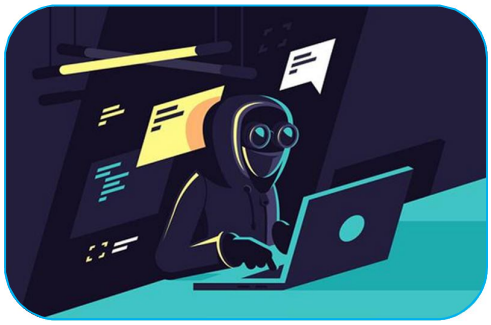
REVIEW OF RESEARCH
ISSN: 2249-894X
IMPACT FACTOR : 5.7631(UIF)
VOLUME - 15 | ISSUE - 7 | APRIL - 2026

ENTRAPMENT TO EXPLOITATION: A SOCIO- LEGAL STUDY OF HONEY TRAPPING CRIMES IN THE DIGITAL AGE IN INDIA

Dr. Pravin Kumar Chauhan
Associate Proffesor, Supervisor, Law Department, Monad University, Hapur, U.P.

Parmod Kumar
Research Scholar, Law Department, Monad University, Hapur, U.P.

ABSTRACT :



Honey-trapping has existed in various forms since the time of ancient kings and empires, and it entails using romantic or personal connections to gain information or power. Honey-trapping crimes have taken on new dimensions in the modern era, particularly in cyberspace, where profiles on social media sites such as Facebook and Twitter are used to befriend and subsequently entice individuals into providing sensitive information. This attitude has escalated into a major issue, endangering both personal and national security. This study examines honey-trapping Crime Cases to investigate the tactics and implications of honey-trapping, focusing on the move from physical seduction to digital manipulation. It also examines the legal and ethical issues raised by honey-trapping, highlighting the lack of strong legal procedures to combat these crimes. Furthermore, the study discusses preventive ways to protect individuals and organisations from such dangers.

KEYWORDS: *Crime prevention, criminal law, cyber espionage, cybersecurity, digital manipulation, honey trapping.*

INTRODUCTION:

Honey trapping is a dishonest strategy in which a person utilises romantic or sexual interactions to manipulate a target into a compromising position for personal, political, or financial advantage. The word "honey trap" or "honey pot" comes from the idea of employing a sweet substance to attract and catch insects; in this case, the "sweetness" is a beautiful person acting as bait.

The term "honey trap" also refers to using dating services to get access to a victim.

Private investigators are frequently hired by wives, husbands, and other partners to set up a honey pot when an illicit romantic affair is suspected of the "target," or subject of the investigation. Occasionally, the term may be used to refer to the practice of staging an affair in order to obtain incriminating photos for blackmail purposes. A honey trap is primarily used to gather evidence about its subject. Honey trapping is also used to get new users addicted to illegal substances, as well as for drug smuggling.[1]

The success of a honey trap operation is dependent on exploiting human psychology and emotions. The target may form a strong emotional bond, making it difficult for them to evaluate the motivations underlying the relationship. This emotional attachment can impair judgement, enabling the target to reveal secret information or engage in compromising behaviour.

It is worth noting that, while honey traps exist, they are not the primary technique of intelligence collecting used by most intelligence agencies. More complex measures, such as technical surveillance, cyber operations, and human intelligence networks, are generally preferred due to their dependability and legal standing.[2]

Honey-trapping crimes have expanded to social media platforms like Facebook and Twitter, where personas (typically bots) are utilised to befriend and attract individuals into disclosing sensitive information. Innefu warns that this conduct jeopardises both individual and national security. Using romantic connections to gain information or influence is a long-standing practice in India and other countries, dating back to ancient kings and empires. Honey-trapping is a very efficient method for collecting sensitive information from unwary persons due to its attraction of romantic connection and personal gain.

Honey-trapping has evolved into a sophisticated and often lethal tactic used by both domestic and foreign intelligence organisations. Indian intelligence agencies use honey-trapping techniques to obtain information on potential risks to national security, including terrorist groups and international espionage rings. However, these technologies have been exploited for malevolent ends, including blackmail and political influence. Honey-trapping in India has created privacy and security concerns, as well as the risk of exploitation. Honey-trapping methods have resulted in high-profile examples of blackmail and damage. Honey-trapping research is critical for understanding the impact on modern cybersecurity, exploitable human vulnerability, and espionage.

Honey-trapping has evolved from physical interactions to digital platforms, utilising misleading profiles and AI for data collection. The usage of AI will pose significant challenges in the future years. Targeting defence personnel poses serious concerns to national security due to their access to sensitive information. Recent incidents, such as the kidnapping of Indian Army personnel by Pakistani agents and Iranian soldiers by Hamas, highlight the worldwide impact and serious implications of this tactic. Researching honey-trapping aids in developing counter-strategies for detecting and preventing such espionage activities. suggests using advanced models and algorithms to discover probable honey trap profiles using forensic network research, such as Complex Event.[3]

Background of Honey Trap

Honey trapping has a long history of application in espionage.

During the Cold War, the Soviet Union's KGB deployed female agents known as "Mozhno girls" or "Mozhnos" to spy on foreign leaders by seducing them.The name Mozhno derives from the Russian word "mozhno" meaning "it is permitted" as these agents were allowed to flout restrictions banning Russian communication with outsiders.

In 2009, the British MI5 sent a 14-page dossier to hundreds of British banks, corporations, and financial organisations titled "The Threat from Chinese Espionage." It alleged a large-scale Chinese operation to bribe Western businesspeople over sexual relationships.

Despite their ancient origins, honey traps continue to work in both the real and virtual worlds, and digital honey traps offer practitioners several benefits over their physical counterparts. Let's see how they operate. The memo expressly warns that Chinese intelligence agencies are attempting to build "long-term relationships" and have been known to "exploit vulnerabilities such as sexual relationships [...] to compel individuals to cooperate with them."[4]

Honey Trap Squad is an expanded unofficial wing of RAW made up of female agents who have been declared dead in official records. Mitra, known by the code name Honey, leads this group. The way of functioning for this team is synonymous with its name. These are highly trained agents with killer looks that can lure their victim into their traps. Right now, HTS is behind the counterfeit network in India, which is run by Abdul Hameed from Dubai. Abdul Hameed is an absconding criminal from India who is plotting against the country with the support of ISI. This story follows HTS as he cuts the wings of this counterfeit network one by one, as well as Hameed's efforts to rescue his empire from an unforeseen threat. To accomplish this, he has resort to hiring an assassin known as "Mirage," who is a myth to the rest of the world. Will the girls be able to take down the assassin and disable Hameed's network. [5]

Honey trapping in cybersecurity

In the world of cybersecurity, a "honey trap" is a strategy that hackers employ to lure victims into dangerous situations. Although honey traps can take numerous forms, they typically involve creating a false identity or online presence in order to entice an unwary victim. After convincing the victim to disclose sensitive information or download malware, the hacker can use that information to execute a variety of cyberattacks.

A honey trap is a type of social engineering attack that employs psychological persuasion to gain a victim's trust by impersonating a trustworthy source, such as a friend or coworker, and then exploiting that trust to obtain valuable information or other benefits. Honey traps can take many forms, such as:

1. fraudulent social media profiles: To contact with potential victims, a hacker may create a fraudulent profile on a social media platform.
2. Dating scams: A hacker may create a phoney profile on a dating website and use it to deceive unsuspecting victims into paying money or giving private information.
3. False employment offers: A hacker may approach a target while posing as a recruiter or hiring manager. They might then use that connection to steal confidential information or get access to the victim's network or system.
4. Email phishing: A hacker may send a target a phishing email while posing as a legitimate company or service. The victim may unintentionally disclose private information by inputting it on the bogus website after clicking on a link in the email that takes them to a fake website that looks like the real one.
5. Physical honey traps: A hacker may use a bogus USB drive or phone charger to get access to a victim's PC or mobile device. These devices may include malware or other malicious software, which might be used to launch a cyberattack.

How to Avoid Honey trap:

Be wary of suspicious or unsolicited communications: Avoid strangers or unknown people who approach you with unsolicited texts, phone calls, or social media requests.

Limit the amount of personal information you share online. Be cautious about the personal information you disclose online, especially on social media, dating apps, and other platforms. Only share information with reputable individuals or organisations.

Be wary of romantic advances from strangers: If someone you don't know well exhibits romantic interest in you or attempts to establish a relationship, use caution and take the time to get to know the individual before providing personal information or agreeing to meet in person.

Protect your online accounts by using strong, unique passwords and turning on two-factor authentication whenever possible.

Stay informed: Keep up with the most recent strategies and trends in honey traps and other social engineering attacks. This can help you recognise suspicious behaviour and avoid falling prey to such techniques.

Be cautious of the risks of social engineering: Honey traps are a type of social engineering that includes tricking people into disclosing sensitive information or doing potentially damaging acts.

Report suspicious activity: If you believe you have been targeted by a honey trap or other social engineering attack, notify police enforcement or the appropriate authorities immediately.[6]

Legal Framework: Gaps and Provisions in Indian Law: There is no law in India that particularly addresses honey trapping. Several parts of the IPC and IT Act are regularly invoked.

BNS Section 308: This section of the BNS addresses the offence of extortion. This applies when individuals are threatened or coerced into handing over money, precious items, or sensitive information. This rule applies to honey trap cases where victims are blackmailed or intimidated into paying monetary compensation or divulging confidential information under threat of damage.

Section 319 of the BNS concerns the crime of defrauding by impersonation. Deception occurs when someone pretends to be someone else in order to acquire an illegal advantage. This section is sometimes utilised in honeytrap scenarios when the perpetrator creates a false persona, whether online or offline.

In person, the victim may be lured into a relationship or trap, leading to exploitation, deception, or financial fraud.

BNS Section 294: Section 292 addresses obscenity-related offences. Obscene materials are prohibited from being sold, distributed, exhibited, or circulated in public. This rule applies to honey traps, which use sexually explicit photographs, videos, or communications to attract or blackmail victims. Sharing such content without consent may lead to legal consequences.

Section 66E of the Information Technology Act addresses the invasion of individuals' privacy. It is illegal to intentionally capture, publish, or transfer photos of someone's private **parts without their agreement. Section 66E addresses privacy violations in honey trap cases,** where private images or videos are secretly taken or transmitted.

Sections 67 and 67A of the IT Act regulate the electronic publication and transmission of sexually explicit content. Section 67 penalises online distribution of obscene material, while Section 67A focuses on sexually explicit information. Honey trap operations using electronic communication, such as social media, messaging apps, or email, often use these sections to prevent the spread of inappropriate content and hold offenders accountable under cyber law.

Although these clauses provide some coverage, they do not clearly identify honey traps as a crime in itself. This legal vacuum leads to inconsistent investigations, poor deterrence, and difficulty in prosecution. Digital evidence is susceptible to alteration and removal, complicating the evidentiary process.[7]

Cases Related to Honey Trap:

Noida Honey Trap Extortion Case (2024)

In January 2024, Surajpur police in Greater Noida arrested four people, including two women, for operating a honey trap. In 2023, the group utilised children to befriend men online and extorted almost ₹10 lakh from its victims.[8]

Bengaluru Honey Trap Racket (2024)

In August 2024, Bengaluru police detained three people, including a woman named Njma Kausar, for running a honey trap operation. The organization used phone calls to entice guys, then threatened them with bogus rape claims to extract money.[9]

Meerut Honeytrap Gang (2024)

A seven-member gang, including two women, was detained in Meerut, Uttar Pradesh, for honey-trapping men. Women would entice males to engage in sexual activities, videotape the interactions, and then extort money by threatening to reveal the videos or file fake rape claims.[10]

DRDO Espionage Case (2023)

Pradeep Kurulkar, a top scientist at the Defence Research and Development Organisation (DRDO), was detained for allegedly sharing secret material with a Pakistani intelligence operator.[11] Investigations found that he communicated with a female Pakistani intelligence worker via WhatsApp, voice, and video chats.

Sonipat Honey Trap Gang Involves Lawyers (2023)

In August 2023, Sonipat police arrested two lawyers and a woman for running a honey trap ring.

They allegedly filed fraudulent rape cases to extract money from victims, with allegations of perhaps 12-15 such incidents.[12]

CONCLUSION:

Honey traps constitute a significant and evolving threat that leverages human emotions—such as loneliness, vanity, and the desire for romantic connection—to facilitate espionage, extortion, and blackmail. In the digital age, this tactic has shifted from purely physical encounters to sophisticated cyber-social engineering, utilizing fake profiles, AI, and social media to target individuals across various sectors, including defense, corporate, and private life. Ultimately, the conclusion is that honey trapping is a "human firewall" issue, where emotional vulnerabilities bypass technological defenses. Preventing such traps requires combining technical security with psychological readiness and a heightened awareness that "real love doesn't ask for passwords".

REFERANCES:

1. https://en.wikipedia.org
2. https://www.staysafeonline.in
3. www.kriminologie.de
4. https://en.wikipedia.org
5. https://www.imdb.com/title/tt28477916
6. https://www.staysafeonline.in
7. https://theacademic.in
8. Noida Honey Trap Extortion Case (2024)
9. Bengaluru Honey Trap Racket (2024)
10. Meerut Honeytrap Gang (2024)
11. DRDO Espionage Case (2023)
12. Sonipat Honey Trap Gang Involves Lawyers (2023)