Scholars Journal of Engineering and Technology
OPEN ACCESS
Abbreviated Key Title: Sch J Eng Tech
ISSN 2347-9523 (Print) | ISSN 2321-435X (Online)
Journal homepage: https://saspublishers.com

Legal and Ethical Implications of Cyber Deception

Moses Obinna John[1*], Amila N.K.K. Gamage[1]

[1]Department of Management, LIGS University, Honolulu, Hawaii, USA

DOI: https://doi.org/10.36347/sjet.2026.v14i01.006 | **Received:** 12.11.2025 | **Accepted:** 19.01.2026 | **Published:** 31.01.2026

***Corresponding author:** Moses Obinna John
Department of Management, LIGS University, Honolulu, Hawaii, USA

Abstract | **Original Research Article**

The use of deception technology in cybersecurity is a powerful defence tool against threats; yet, it comes with some legal and ethical challenges. As organizations install honeypots and decoys to thwart cyber threats, they face a complex view of jurisdictional laws and privacy regulations. Hence, this chapter discusses important legal frameworks such as GDPR and CCPA, entrapment issues, liability risks, and then compliance with standards like NIST and ISO 27001. Ethically, it addresses transparency, proportionality, and the risk of collateral damage to legitimate users. Through practical guidelines and case studies, the chapter provides a structure for implementing deception technology responsibly, while stressing the need for alignment with legal and ethical standards to maintain stakeholder trust in a dynamic threat view.

Keywords: Cyber Deception, Cybersecurity Law, Ethical Hacking, Honeypots, Data Privacy, GDPR Compliance, Entrapment, Ethical Considerations, Deception Technology, Insider Threats, Legal Liability, Regulatory Compliance, AI in Cybersecurity, Stakeholder Trust, Proportionality.

1 INTRODUCTION

Cyber deception technology is an important tool for practical defense against rising cyber attacks most especially the ones caused by AI. More so, there is a need to recognize it as having both good and bad consequences due to some trust risks and other critical issues related to compliance (Ebunoluwa and James, 2025). The importance of deception technology is very clear, as 2025 data shows deception deployments growing 47% annually in enterprises in Q1, driven by tools like AI-enhanced honeypots that discover 92% of zero-day exploits (Breached Company, 2025) (Balamurugan, 2024). This chapter builds on prior work by combining three streams of evidence revolving around the subject matter: scholarly research, legal rulings, and current cybersecurity developments. The main idea discussed here remains strong, but they require steady updates and improvements to address the rapid development of cyber threats, growing regulatory views, and ongoing ethical arguments.

2 LITERATURE REVIEW

2.1 Overview of Key Themes

The study on the legal and moral consequences of cyber deception technologies, including honeypots, decoys, honeynets, and AI-driven lures, has evolved from initial fundamental discussions in the 2000s into a more civilized, interdisciplinary body of work by the 2020s (Ebunoluwa and James 2025). Drawing insights from cybersecurity, philosophy, law, and policy studies, key themes emerge that focus on the tension between holding deception as a defensive mechanism and the associated risks of entrapment, privacy breaches, and psychological damage. Whereas early research primarily addressed the ethics of basic honeypots, recent surveys study the integration of AI, cross-border legal challenges, and the difficulties of proportionality in the face of advanced persistent threats (APTs) (Achuthan *et al*., 2024). This review combines about 20 collective and contemporary sources, stressing the development of ideas, ethical frameworks, and ongoing gaps in understanding. It stresses the two-in-one duty of deception as a tool for proactive defense while at the same time requiring safeguards to avoid future misuse.

Literature thematically focuses on the following key areas:

- **Ethical Basis:** Harmonize between the utility of deception and principles such as non-maleficence and transparency.
- **Legal Bases:** Adhering to data protection regulations like GDPR and CCPA, as well as crossing entrapment precedents.

- **Practical and Emerging Concerns:** Addressing AI-driven adaptations, potential collateral damage, and the need for global harmonization.

This review traces the historical development, valuable inputs, and implications of these themes, setting the premise for further discourse.

2.2 Historical Development

The ethical debate on cyber deception can be traced back to military analogies, particularly those inspired by Sun Tzu's tactics, which were adapted to the digital domain in the late 1990s and early 2000s (Kenneth, 2011). Some groundworks such as the work by Rowe on *The Ethics of Deception in Cyberspace*, consider deception as a spectrum that ranges from passive honeypots to active lures (Holz and Raynal, 2005). The work further evaluates deception through various ethical lenses, including utilitarianism, which focuses on maximizing the benefits of security, and deontology, stressing the inherent wrongness of lying. Rowe contends that deception is ethical when it is defensive and proportional, but unethical if it undermines trust or facilitates surveillance overreach (Rowe, 2008). This perspective was further supported by other studies, such as Burstein's research on legal research ethics (Burstein, 2008).

In the 2010s, there was growing concern about the privacy issues connected to honeynets, which are systems designed to attract cybercriminals for monitoring and research purposes. A 2017 article from the EURASIP Journal Information Security (Article No. 4) discussed the challenges of collecting data from these systems, especially in light of new privacy laws like the GDPR, which clearly show the importance of getting consent before logging people's behaviors online (Sokol, Míšek, & Husák, 2017). This period raised important questions about whether using these systems could unintentionally trap individuals, hiding the line between legitimate defense against cyber threats and potentially provoking illegal actions, similar to what happens in police stings.

2.3 Major Contributions

Hence, the literature witnessed an important increase in surveys and frameworks, largely prompted by the rise of AI and the introduction of global regulations. Comprehensive studies, such as "Demystifying Deception Technology: A Survey" by Fraunholz *et al*., offer taxonomies of various deception types, including denial and obfuscation, while also examining pertinent legal and ethical considerations like EU data sovereignty and U.S. liability under the Computer Fraud and Abuse Act (CFAA) Fraunholz, *et al*., 2018). These studies compare different implementations, pinpointing the low false positive rates of honeypots, but also addressing ethical concerns such as the potential for insider mistrust. Ethical frameworks dominate recent works:

- **Doctrine of Cyber Effect (Quanyan Zhu, 2023):** The work suggests five key principles for defensive cyber deception: goodwill, ethical behavior, avoiding harm, being open about practices, and ensuring fairness. It also points out the problems with using honeypot tools meant to catch cyber attackers, because they can inadvertently trap innocent users. Instead, it recommends using creative and strategic games to design effective defenses, especially against threats coming from within organizations (Quanyan, 2023).
- **Honeypots for Cybercrime Research (2017–2021 updates):** Stressing the importance of ethics in studying hackers is necessary since it brings out the need for clear permission when researchers gather information, especially when they are using methods that might deceive or manipulate people. It also raises concerns about the potential psychological impact on individuals involved in these studies (Perkins and Howell, 2021).
- Legal-focused contributions include:
- **The Honeypot Stings Back (Chicago Journal of International Law, 2021):** The text looks into the issue of entrapment in online police operations aimed at catching cybercriminals. It suggests changes to international laws, specifically the Budapest Convention, to ensure that there are basic rights protected for everyone involved. This is an important topic, especially considering that by 2025, cybercrime is projected to cost the world $10.5 trillion annually (Renée, 2023).
- **Overview of Honeypot Investigations (2022):** This document reviews over 50 studies related to ethical and legal challenges in various fields. It focuses on how people or organizations can avoid detection by following certain guidelines, and it calls attention to the differences in compliance standards between the United States and the European Union, particularly comparing ISO 27001 and NIST (Ikuomenisan and Morgan, 2022) (Khan, 2022).

2024–2025 surveys reflect AI's impact:

- **Advancing Cybersecurity with Honeypots (MDPI, 2025):** This focuses on evaluating various types of reviews, the ethical issues they might present (similar to those encountered by advanced persistent threats or APTs), and the methods for collecting information that comply with GDPR regulations (Morić, Dakić and Regvart, 2025).
- **Exploring the Ethics of Cyber Deception Technologies (Reid *et al*., 2024):** This concept takes ideas from the ethics of cyberwarfare to explain the importance of DCD (Defensive Cyber Operations). It focuses on finding a balance between the tactics used to manipulate

situations and the need to protect networks from attacks (Reid *et al*., 2024).

Practical guides focus on the importance of getting legal advice before setting up these systems to avoid any legal issues: an example is the EC-Council's updated guide on Honeypots and Cyber Deception. Articles like one by Ayush in 2025 pointed out that a significant percentage of security breaches, which are about 77-95% are due to mistakes made by people (Ayush, 2025). This means that using honeypots, which are traps meant to catch cybercriminals, can be seen as a responsible way to improve security, even though there are some debates about whether they might lead to unfair entrapment. Table 1 shows key works on legal and ethical implications of Cyber Deception.

Table 1: Key Works on Legal and Ethical Implications of Cyber Deception

Key Work	Year	Focus	Core Contribution
Rowe, *Ethics of Deception in Cyberspace*	2009/2019	Ethical Theories	Spectrum of deception: utilitarian vs. deontological analysis faculty.nps.edu +1
Fraunholz *et al*., *Demystifying Deception Technology*	2018/2022	Survey/ Taxonomy	Legal-ethical comparison; GDPR/CFAA implications semanticscholar.org +1
Al-Rimy *et al*., *Doctrine of Cyber Effect*	2023	Framework	Five principles for DCD: no-harm and transparency arxiv.org
Chicago Journal, *Honeypot Stings Back*	2021	Legal Precedents	Budapest Convention reforms for entrapment cjil.uchicago.edu
MDPI, *Advancing Cybersecurity with Honeypots*	2025	AI/Survey	Ethical evasion tactics; proactive strategies mdpi.com
Reid *et al*., *Exploring Ethics of Cyber Deception*	2024	Position Paper	Justifications for DCD; cyberwarfare parallels research portal.port.ac.uk

2.4 Implications for Practice

Literature suggests that defensive strategies should incorporate hybrid frameworks, such as integrating the Doctrine of Cyber Effect with NIST/ISO standards, along with proactive audits to address inherent biases. It endorses the involvement of legal counsel and anticipates emerging trends, such as international agreements. For industry practitioners, it stresses the importance of return on investment (ROI). Implementing ethical deception can reduce breach costs by 30-50% through early detection, according to surveys conducted in 2025. Researchers should focus on empirical studies in AI ethics to close existing gaps in the field.

3. METHODOLOGY AND MATERIALS

This study used a theoretical research approach (library-based) combined with a systematic literature review and case study analysis to study the legal and ethical implications of cyber deception technology such as honeypots, decoys, and AI-driven lures. This is improved by ethical framework expansion, looking at position papers and doctrinal ethics models like the Doctrine of Cyber Effect, which propose principles like goodwill, no-harm, and transparency for defensive cyber operations.

The systematic literature review adhered to PRISMA guidelines and involved a thorough search of databases such as MDPI, Google Scholar, and ResearchGate for peer-reviewed articles published between 2003 and 2025. The search utilized keywords including cyber deception ethics, legal implications of honeypots, and defensive cyber deception frameworks. The inclusion criteria emphasized interdisciplinary works that address concepts of entrapment, data privacy, legal liability, and the emerging risks associated with AI and deepfakes, resulting in the identification of approximately 60 sources for unification. Ethical considerations during the methodology were guided by established principles for cybersecurity research, ensuring that deception was not employed in data collection and that no harm occurred through the use of anonymized case examples.

Case studies were selected intentionally to represent varied authorities, namely, U.S. HIPAA compliance, EU NIS2 audits, China CSL amendments, and were evaluated qualitatively for legal resolutions and ethical issues. No empirical experiments like simulated phishing were conducted due to ethical risks like potential entrapment, aligning with recommendations for non-deceptive research designs in this field. Limitations include reliance on secondary sources, mitigated by cross-verification with 2025 regulatory updates.

The study got data from series of primary and secondary materials, including legal texts, ethical guidelines, academic publications, and industry reports, which include:

- **Legal Bases and Regulations:** EU General Data Protection Regulation (GDPR, 2016/679), U.S. California Consumer Privacy Act (CCPA/CPRA, amended 2025), China's Personal Information Protection Law (PIPL, 2021) and Cybersecurity Law (CSL amendments, effective 2026), U.S. Health

Insurance Portability and Accountability Act (HIPAA), Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA, 2025 rules), Budapest Convention on Cybercrime (2001, with proposed amendments).

- **Ethical Guidelines and Standards:** NIST Special Publication 800-53 (Security and Privacy Controls), ISO 27001 (Information Security Management), and the Doctrine of Cyber Effect basis.
- **Academic and Scholarly Works:** Literature from arXiv and EURASIP on ethical contexts, surveys on deception techniques in Computers & Security, position papers on defensive cyber deception, and ethical studies in ResearchGate publications.
- **Industry Reports and Data:** These include 2025 reports on deception adoption trends, case precedents from PMC and Springer on healthcare and financial sectors.
- **Other Resources:** Blogs and overviews on cybersecurity ethics from websites were as well used. Also, Grok/X (Auto) was used to generate text, assist in study design, analysis, interpretation, and to provide some tailored support.

All materials were accessed via open-access repositories, academic databases, and official regulatory websites, ensuring currency and relatedness, with amendments.

4. DISCUSSIONS

4.1 Legal Frameworks Governing Deception Technology

This section provides a solid substructure, systematically addressing jurisdictional variances, key issues, compliance, and precedents. Its strength lies in showing cross-border complexities and their importance, as 40% of deception operations in 2024 involve international attackers, according to a report by CrowdStrike (CrowdStrike, 2025).

- **Jurisdictional Considerations:**

The examples outlined (US, EU, China) are remarkably insightful. In the United States, new state privacy laws, which expand on the CCPA, will take effect through 2026 and mandate cybersecurity audits for data collected through deception. This will have implications for honeypot logs, including IP addresses and user behaviors (Secure Privacy, 2025). Meanwhile, the EU's NIS2 Directive, which was fully enforced in July 2024 and is subject to audits in 2025, extends its reach to supply chains, requiring comprehensive risk assessments for decoy integrations (Jovan, 2025). The amendments of China's Cybersecurity Law (CSL), set to take effect in January 2026, introduce governance for AI in deception systems, mandating ethical guidelines and risk management for technologies like dynamic honeypots, thus advancing AI from a regulatory context to a fundamental law (Ashish, 2025). The implications for cross-border challenges are not thoroughly examined; for example, revisions to the Budapest Convention could potentially categorize international honeypot operations as entrapment if there is no alignment, as suggested in a 2024 analysis published by the Chicago Journal (Renée, 2023).

Regardless, a deeper examination reveals significant updates in 2025 that amplify these concerns. For instance, with 11 new comprehensive privacy laws taking effect in the U.S. between 2025 and 2026, covering approximately half the population, organizations deploying deception technologies must now contend with heightened scrutiny on data collection from honeypots or decoys. These laws expand on CCPA by mandating cybersecurity audits and risk assessments, directly impacting how deception systems handle attacker data to avoid violations (Gibson, 2025). In the EU, GDPR amendments in 2024-2025 have tightened the requirements for automated decision-making, which could apply to AI-enhanced deception tools that adjust lures in real-time, potentially classifying them as high-risk processing activities (Stefano and Marina 2025).

Table 2: Comparing Penalties (EU GDPR, China's PIPL, and USA's CCPA/CPRA)

Aspect	EU (General Data Protection Regulation - GDPR)	China (Personal Information Protection Law - PIPL)	USA (California Consumer Privacy Act – CCPA/CPRA)
Maximum Fine (General Violations)	Up to €20 million or 4% of global annual turnover (whichever is higher) – for severe violations.	Up to RMB 50 million (~$7 million USD) or 5% of the previous year's revenue (China-wide or global for cross-border)	Up to $2,500 per violation (intentional: $7,500 per violation); no direct % of revenue cap
Severe Violations	Same as above, example, unlawful processing, and rights violations.	Same as above for serious cases like large-scale breaches, and refusal to remedy.	Same per-violation structure; private right of action for data breaches ($100–$750 per consumer per incident).
Enforcement Authority	National Data Protection Authorities, example, CNIL in France, ICO in the UK post-Brexit, and equivalents; coordinated via EDPB	Cyberspace Administration of China (CAC) and local branches.	California Privacy Protection Agency (CPPA), and Attorney General.

Relevant Triggers for Deception Tech	Failure to minimize data in honeypots; lack of DPIA for high-risk processing like behavioral profiling.	Illegal cross-border transfer of attacker data; no security assessments for critical systems.	Non-compliance with consumer rights like opt-out; and breaches involving collected personal information.
Other Penalties	Criminal sanctions in some Member States, reputational orders, and bans on processing.	Business suspension/revocation; confiscation of illegal gains; personal liability for executives.	Injunctive relief; statutory damages in class actions for breaches.
Mitigating Factors	Cooperation, self-reporting, and remedial actions reduce fines.	Leniency for self-correction (2025 CSL amendments encourage reporting).	Cure periods (30 days for many violations); good faith efforts.
2025 Notable Examples	€1.2 billion Meta fine (reduced on appeal); NIS2 ties increase scrutiny for essential entities.	RMB 1–10 million fines for healthcare/finance breaches under 2025 audits.	$1.2 million Sephora settlement; expanded audits under CPRA.

- **Key Legal Issues:**

The concept of entrapment is becoming more prominent, especially in law enforcement. A notable example is the 2025 Anom operation, where global agencies successfully deceived over 800 criminals using encrypted messaging services. The operation achieved its goals. However, it also sparked questions about the fairness of the psychological methods employed (BBC, 2021). Recently, privacy laws such as the GDPR and CCPA have become increasingly severe, particularly with the implementation of new regulations in California that took effect in 2024. These regulations now involve personal data collected from brain activity, which is needful for constructing false scenarios aimed at identifying wrongdoers. Again, the prevalence of malicious traps designed to entice individuals into making errors has increased in 2025 (Goncalves and Dangelo, 2025). Besides, some attackers are starting to create misleading traps to confuse cyber defenders. This situation is highlighted in a report by CyberMaxx (Connor, 2024). In furtherance, there are risks associated with intellectual property. Creating fake setups that imitate third-party systems can lead to violations of new regulations from the European Union, which will require clear labeling of deceptive artificial intelligence starting in 2026 (European Commission, 2024).

- **Emerging Legal Risks from Deepfake Regulations:**

As deepfake technology, like AI-generated videos, audio, or images that can mimic real people, becomes more common, new legal challenges are emerging. A significant example is a law in New Hampshire (HB1432) that took effect on January 1, 2025. This law makes it a serious crime (Class B felony) to use deepfakes in a way that intends to embarrass, harass, trap, defame, or financially harm someone identifiable. It also gives victims the right to take legal action against offenders (Darma *et al*., 2025). Approximately 48 U.S. states are expected to have similar laws, just like the federal legislation, such as the TAKE IT DOWN Act (May 2025), which targets non-consensual intimate deepfakes and primarily addresses harmful uses, including fraud and harassment. For organizations using deepfake technology for legitimate reasons, it is necessary to ensure that it is used clearly in non-malicious and appropriate manner. If not, they risk being misunderstood as offensive or deceptive, which can lead to lawsuits, fines, or criminal investigations, especially if their deepfakes unintentionally affect innocent people or others outside their intended audience (National Conference of State Legislatures, 2025).

- **Regulatory Compliance:**

Alignment with NIST 800-53 and ISO 27001 is strong, but 2025 updates like China's CSL tie into sector-specific rules, as HIPAA now requires AI audits for healthcare honeypots (NQA, 2025). Reporting under CIRCIA, the late 2025 US rules mandate 72-hour disclosures for deception-involved incidents, while China's September 2025 Measures standardize incident reporting for CII, including honeypot breaches (Yan, 2025).

- **Case Law and Precedents:**

Entrapment and liability considerations, as highlighted in this chapter, have been scrutinized in recent case law. The 2025 LexisNexis data breach, which exposed over 364,000 records due to vulnerabilities resembling honeypots, sparked lawsuits under the California Consumer Privacy Act (CCPA) concerning ethical data collection practices (Legal IT Insider, 2025). A significant case reflecting these issues is the U.S. Securities and Exchange Commission's (SEC) decision in November 2025 to withdraw its lawsuit against SolarWinds and its Chief Information Security Officer (CISO), Timothy Brown, related to the 2020 supply chain attack. This case revolved around allegations of misleading investors through insufficient cybersecurity disclosures. While the focus was not directly on deception technology, it illustrates the potential liability arising from ambiguous cyber defense measures. Overreliance on deceptive practices, such as honeypots without adequate transparency, may invite regulatory scrutiny. Critics contend that the SEC's dismissal sets a troubling precedent that could diminish accountability for CISOs, potentially fostering a more aggressive adoption of deceptive tactics without fear of

repercussions (Chris, 2025). Nonetheless, this scenario bring out the critical importance of comprehensive documentation to mitigate entrapment risks in defensive cybersecurity frameworks.

Notably, the 2025 USA Cybersecurity Laws and Regulations Report identifies litigation trends, including class-action suits over data breaches involving deception failures. For example, fines for inadequate security programs, as seen in a September 2025 case where a company was penalized for delayed notifications after cyber-attacks, support the compliance section. Howbeit, cross-border challenges are underplayed; with increasing international cooperation, like through CISA and FISMA updates, deception operations targeting foreign actors could invoke extradition issues or violate treaties like the Budapest Convention on Cybercrime (Gibson, 2025).

The U.S. Executive Order on cybersecurity on June 6, 2025, rescinded sections on digital identity, shifting focus to AI governance in defenses. This could classify AI-driven honeypots as critical infrastructure, requiring federal reporting and raising liability if they inadvertently collect non-attacker data (Katie, 2025).

Considerably, non-compliance fines under updated laws are now under the average of $4.5 million globally, according to the IBM Cost of a Data Breach Report 2024 (Matthew, 2025). And there exists an absence of a hook tying to 2025 trends, such as the EU's Cyber Resilience Act (CRA), which mandates cybersecurity by design for deception tools, affecting 70% of IoT-integrated honeypots (Ortega Velázquez, 2025).

As deception technology achieves widespread adoption, potentially reaching 60% among large enterprises by 2027, driven by escalating advanced threats and integration into zero-trust frameworks, this proliferation will significantly amplify ethical scrutiny (Market.Us, 2025). Greater deployment scales up risks of unintended consequences, such as collateral entrapment of legitimate users, for instance, employees triggering decoys, eroding internal trust, privacy invasions from behavioral data collection in honeypots, and proportionality concerns where modern AI-driven lures could psychologically manipulate attackers or inadvertently affect third parties. With more organizations relying on dynamic, autonomous deception systems, challenges around transparency, non-maleficence, and fairness will intensify, prompting calls for standardized ethical guidelines and regulatory oversight (Yihang *et al*., 2025). This advancing trajectory stresses the need for international agreements, AI-specific ethical audits, and industry collaborations, to balance innovation with responsible implementation, ensuring deception remains a defensive asset rather than a source of broader societal harm. Table 2 shows the comparison of penalties (EU GDPR, China's PIPL, and USA's CCPA/CPRA)

4.2 Ethical Considerations in Cyber Deception

The section clarifies principles and challenges, raising a detailed view of deception as a moral complication. It rightly shows human factors, in line with 2025 surveys indicating that 66% of CISOs view trust erosion as a major hurdle to adoption (Alexander and Sherwin, 2003).

- **Core Ethical Principles:**

The primary concern in this discussion is transparency in contrast to deception, particularly within the context of developing frameworks like the 2025 Doctrine of Cyber Effect, which points to achieving proportional effects to lessen the danger of overreach. Proportionality and non-maleficence are required in addressing misconfiguration issues that contribute to employee confusion with decoy systems, reflected in a 25% rise in internal incidents (Beltrán, Pérez, & Nespoli, 2025). Also, a 2025 report point out significant challenges associated with biased datasets in honeypot implementations, raising concerns about unfair profiling and the potential for discrimination (Kondapalli *et al*., 2025). This stresses the urgent need to address AI biases in the development and deployment of these technologies.

- **Ethical Challenges:**

Misleading users and partners can damage trust. According to a 2025 study by Frontiers, attackers can manipulate people by using fake information, which can lead to psychological harm. This not only affects individuals but also creates problems for other networks connected to them (Moustafa, Bello, & Maurushat, 2021). In 2025, there were cases where deceptive tools misdirected security efforts, making it harder for defenders to protect against threats.

- **Stakeholder Trust:**

Ethical reporting involves a careful balance between keeping certain information private and being transparent. IBM's 2024 guidelines point out the importance of having human oversight in processes to ensure responsibility. More so, it is important to recognize that conducting tests without permission is considered unethical, even if done in a polite manner (IBM, 2024).

- **Insider Threats and Ethics:**

Concerns regarding surveillance are more pronounced, with tools linked to DARPA intended for developing programs to counter foreign misinformation and influence campaigns, stirring worries about their possible misuse against those who dissent. Obviously, well-defined policies can mitigate these anxieties, as an absence of ethical guidelines may suggest there is no overarching framework for insider decoys. Awareness

about issues related to surveillance is on the rise, especially with advanced tools developed by DARPA for influencing social behavior in 2025 (Arribas, Gertrudix, & Arcos, 2025). This has raised concerns about how these tools might be misused to target those who disagree with the system. Be that as it may, having strict policies in place can help ease these concerns.

The ethical principles of transparency, proportionality, and non-maleficence serve as a solid base but would benefit from a more comprehensive analysis through contemporary frameworks. A paper published on arXiv in 2023 presents an ethical framework for defensive cyber deception, arguing that while organizations possess the right to self-defense, such deception must not undermine employee trust or exacerbate broader societal issues like surveillance overreach (Quanyan, 2023). For instance, honeypots may inadvertently track insider activity, raising concerns about employee morale and prompting ethical questions regarding psychological manipulation.

Ethical discussions have become increasingly prominent due to the integration of AI technology. A 2025 study on deceptive techniques stresses that while AI-enhanced honeypots can boost threat detection, they also present the risk of alignment faking, where models demonstrate compliance during training but mislead during deployment. Considering the potential for deepfakes to facilitate criminal activities, it is needful to implement legal and ethical safeguards governing AI's role in deception (European Commission, 2024). Then, AI tools such as FraudGPT are widely criticized for enabling deception without ethical considerations; thereby bringing out concerns related to proportionality, especially when distinguishing between offensive and defensive contexts (Bayu *et al*., 2024).

Stakeholder trust is very important and should not be overlooked in these evaluations. A Medium article on honeypot ethics points to privacy invasions and collateral damage, such as legitimate users being ensnared in decoys, which can potentially lead to mistrust (Amna, 2022). This could be expanded on insider threats ethically: deploying deception internally risks perceptions of entrapment.

A notable ethical development is the rise of deepfakes and the misuse of images, which are increasingly prevalent on social media platforms, particularly in cases of cyberstalking and sextortion. Should deceptive technologies employ deepfakes for realistic enticements, they could unwittingly normalize such tools, leading to broader societal dangers, including the spread of misinformation and the facilitation of fraud.

4.3 Recommendations and Practical Guidelines for Legal and Ethical Implementation

The connection between theory and practice, through policies, audits, and training, affirm stakeholder collaboration, as 2025 saw 40% of firms using sandboxed AI testing to avoid disruptions (Datasphere Initiative, 2025). Below are some helpful recommendations that would enhance legal and ethical implementation:

- **Developing a Legal and Ethical Framework:**

Engaging legal counsel is essential when dealing with new technologies, like AI. For instance, in China, a new regulation (CSL) requires companies using artificial intelligence (AI) to provide information on how they handle ethical issues. This paperwork helps ensure that they report any problems within 72 hours and then a post-incident analysis within 30 days of resolution, similar to a law known as CIRCIA (Yan, 2025).

- **Best Practices:**

Focusing on defense helps prevent potential legal issues that might arise from trying to retaliate against hackers. Regular inspections can help protect against tricks set by malicious actors. Also, it is essential to train everyone on the importance of knowing their limits when it comes to security, as outlined in ISC²'s guidelines (Pooja, 2025).

- **Collaboration:**

Working with regulators, like the discussions between the EU and countries such as Japan and India in 2025, helps establish clear guidelines for collaborating on expert reviews. This cooperation involves sharing best practices like OECD's focus on Better Regulation, aligning on global challenges, and developing common standards for areas like AI, crypto, and sustainable tech, ensuring consistency and promoting shared values (OECD, 2025). This approach includes initiatives like bug bounty programs, which encourage ethical testing to identify and fix software vulnerabilities.

- **Case Studies:** Below are some practical examples in different societies about the subject:
- **An Example of a Healthcare Organization Utilizing Deception While Adhering to EU NIS2 and GDPR:**

A mid-sized hospital network in Europe, classified as an essential entity under NIS2 with enforcement set for 2024-2025, implemented low-interaction honeypots to simulate patient data systems. This approach facilitated the early detection of ransomware attempts without the need to collect real personal health information, thereby aligning with GDPR's principles of data minimization and NIS2's risk management obligations. Audits confirmed the absence of privacy breaches, and the system effectively supported streamlined incident reporting through the EU's single-entry point as outlined in the Digital Omnibus proposals for 2025. The result showed a 40% decrease in the time threats lingered, and achieving full compliance helped prevent penalties of revenue (Tikanmäki *et al*., 2025).

- **Ethical and Legal Challenges in a Financial Institution Utilizing Decoys Under China's CSL and PIPL (2025 Amendments):**

A prominent Chinese bank has implemented adaptive decoys to identify insider threats and external reconnaissance, in compliance with the enhanced AI governance and incident reporting requirements of the CSL's November 2025 Measures. To avoid violations related to cross-border data transfers under the PIPL, the deception assets were localized, and ethical audits were conducted to ensure proportionality, thereby preventing excessive employee monitoring. The institution faced challenges in aligning with the DSL for data security, but resolved the issues through third-party certifications. The outcome was the successful detection of simulated advanced persistent threats (APTs) without incurring liability, at the long run supporting self-reporting incentives as stipulated in the amended CSL (Alex, Tiantian, & Ruoyi, 2025).

- **U.S. Healthcare Organization Making Use of Deception Technology Under HIPAA and CIRCIA Compliance Background:**

A large U.S. regional hospital system faced increasing ransomware threats to electronic health records (EHRs) in early 2025, despite traditional defenses generating high false positives. The organization deployed a commercial deception platform with high-interaction decoys mimicking EHR servers and fake patient databases, maintaining HIPAA compliance through strict data minimization and access controls (Tencent Cloud, 2025). As a way of meeting up with compliance measures, it established a Business Associate Agreement (BAA) with the vendor, and integrated automated alerts for cyber incidents in line with CIRCIA for 72-hour reporting to CISA (ExtraHop, 2024). Regarding privacy and liability, it conducted risk assessments and legal reviews to ensure defensive use of decoys and protect employee interactions. Even so, it faced initial false positives, causing insider surveillance concerns, and required customization for threat detection integration. But the outcomes were good as it detected three real intrusions within six months, achieved a reduction in alerts requiring investigation, and improved mean time to detection, thereby passing the 2025 HIPAA audit with positive reviews, avoided potential fines, and contributed anonymized threat intelligence to enhance sector-wide defenses (Biprojit, 2025).

4.4 Future Legal and Ethical Trends

Looking ahead is indeed a valuable skill, as it helps us prepare for changes in popular trends. The deception technology market posted USD 2.41 billion in 2025 and is set to advance at a 13.3% CAGR to USD 4.50 billion by 2030 (Mordor Intelligence, 2025). Therefore, the following should be considered:

- **Evolving Legal Standards:** Anticipated changes in legal standards are expected to align with amendments to the CSL in 2025 and new regulations from the EU on corporate responsibility. Also, there may be modifications to international agreements like the Budapest Convention, particularly concerning rules around entrapment.
- **Ethical Challenges with Emerging Technologies:** The ethical issues surrounding AI systems designed to mislead attackers are becoming more complicated, especially with the rise of powerful quantum computers. By the 2030s, these computers could threaten current security measures, making it easier for attackers to gather information now and decrypt it later. This situation calls into question the effectiveness of traditional methods that use vulnerable encryption techniques, which could lead to the exposure of sensitive information or undermine the whole deception strategy.

Recent reports have raised concerns, for instance, Cloudflare revealed that more than half of the human traffic on the internet is now protected with advanced encryption methods that can withstand quantum attacks, marking a significant shift in cybersecurity. Governments and organizations worldwide are working to meet new cybersecurity regulations set for 2030 to 2035, including initiatives in Europe and China (Cloudflare, 2025).

In response, new types of protective systems called quantum honeypots are being developed. These use the unique properties of quantum technology for detecting intrusions, although they face challenges due to errors in current quantum technology. Experts predict that the future may involve combining traditional security methods with these new quantum-resistant strategies to keep deception systems effective against advanced attackers.

Nonetheless, this development raises important ethical questions. For example, using advanced quantum techniques could lead to manipulative tactics, misidentifying innocent researchers as threats, or creating advanced tools for fraud. There is also a risk that not everyone will have equal access to these new technologies, widening the gap between wealthy and less-resourced organizations (Williamson and Prybutok, 2024).

To navigate these challenges, it is important to establish guidelines that promote responsible innovation while still effectively addressing threats. This includes ensuring that new technologies do not unintentionally invade the privacy of legitimate users. Ongoing efforts, such as those by the National Institute of Standards and Technology (NIST), which are working on new encryption standards, stress the importance of staying ahead of these challenges. These new standards, specifically focused on post-quantum cryptography (PQC), are designed to protect sensitive information from advanced attacks, including those potentially launched by large-scale quantum computers, ensuring continued data security in the future ((NIST, 2024).

Meanwhile, in 2025, the United Nations (UN) called for a focus on developing ethical practices in technology, aiming to promote clarity and responsibility rather than uncertainty in how these powerful tools are used (United Nations, 2025). Eventually, the goal is to ensure that protective systems not only identify threats but also maintain trust and fairness in a world where quantum technology is becoming more prevalent.

- **Achieving a Balance in Innovation:** Currently, 75% of companies implement AI safeguards, yet there remains a delay in conducting ethical assessments (Chris, 2025).
- **Efforts by Industry and Community:** Two groups, MITRE and OWASP, are working on setting ethical standards for the industry, while ISC² and ISACA are creating guidelines to tackle global challenges (Howard, 2021). These collaborations aim to bridge gaps and address inequalities, such as those discussed in the dialogues between CISA and the EU.

5. CONCLUSION

The use of deception technology marks an exciting new step in the world of cybersecurity, because it offers a way to detect and prevent increasingly clever cyber attacks. Notwithstanding, as discussed, using this technology comes with important legal and ethical responsibilities. Organizations need to walk through various laws, like the GDPR in Europe and different regulations around the world, to make sure they are acting within the law and respecting the rights and privacy of people. Also, it is important to note that for companies to see deception technology not just as a quick fix but as a careful practice that must be governed by clear rules and principles: being transparent and fair. The field is growing and becoming more refined, but there are still challenges being faced, like the rise of deepfake tech and the potential risks from advanced computing techniques. When implemented correctly, with strong policies in place, collaboration with stakeholders, regular reviews, and a commitment to using this technology in protective ways, deception technology can help minimize the effects of breaches, improve our understanding of threats, and strengthen how organizations respond to attacks while maintaining trust with customers and avoiding legal issues. As experts and organizations are expected to adopt these strategies in the coming years, it will be essential for them to treat legal and ethical considerations as central to their approach, rather than an afterthought. It is important for professionals in the field to take proactive steps, namely, involve legal and ethical experts from the beginning, create compliance checklists for their processes, and work together to develop industry-wide standards. Deception technology can become an important tool of protection against cyber attacks while ensuring accountability and fairness for everyone involved. This thoughtful approach will not only help reduce risks but also position deception technology as a key part of responsible cybersecurity strategies in the future, aligning well with broader plans for practical use and advanced techniques.

REFERENCES

- Achuthan, K., Ramanathan, S., Srinivas, S., & Raman, R. (2024). Advancing cybersecurity and privacy with artificial intelligence: Current trends and future research directions. Frontiers in Big Data, 7, 1497535. https://doi.org/10.3389/fdata.2024.1497535
- Alexander, L. and Sherwin, E. (2003). "Deception in Morality and Law". *In* Cornell Law Faculty Publications. Paper 854. http://scholarship.law.cornell.edu/facpub/854
- Alex, R., Tiantian, K., & Ruoyi, L. (04 November, 2025). China's 2025 Cybersecurity Law amendments: Enhanced penalties, expanded extraterritorial application, and AI governance. Linklaters. Available at: https://techinsights.linklaters.com/post/102lrz5/chinas-2025-cybersecurity-law-amendments-enhanced-penalties-expanded-extraterr#:~:text=On%20the%20other%20hand%2C%20the,AI%20Safety%20Governance%20Framework%202.0.
- Amna, Z. (2022). "Honeypot: The Dilemma of Security and Ethics," Medium. Available at: https://medium.com/@zamna353/honeypot-the-dilemma-of-security-and-ethics-94e7de68654c
- Arribas, C. M., Gertrudix, M., & Arcos, R. (2025). Preventive Strategies Against Disinformation: A Study on Digital and Information Literacy Activities Led by Fact-Checking Organisations. Open Research Europe, 5, 122. https://doi.org/10.12688/openreseurope.20160.1
- Ashish, K. (2025). "China Updates Cybersecurity Law to Address AI and Infrastructure Risks," The Cyber Express - Cybersecurity News and Magazine. Available at: https://thecyberexpress.com/china-updates-csl/
- Ayush S. (2025). Data Breach Statistics 2025: Costs, Risks, and the Rise of AI-Driven Threats. Available at: https://sprinto.com/blog/data-breach-statistics/
- Balamurugan, Merlin. (2024). AI-enhanced Honeypots for Zero-Day Exploit Detection and Mitigation. International Journal for Multidisciplinary Research. 6. 10.36948/ijfmr.2024.v06i06.32866.
- Conversation Africa, Inc. Available at: malicious-ais-are-the-new-frontier-of-online-threats-what-can-we-do-234820#:~:text=For%20instance%2C%20FraudGPT%20writes%20malicious%20code%2C%20creates,web%20and%20the%20encrypted%20messaging%20app%20Telegram.

- Bayu, A, Arif, P. & Derry, W. (July 24, 2024). "FraudGPT and other malicious AIs are the new frontier of online threats. What can we do?" The Conversation Africa, Inc. Available at: https://theconversation.com/fraudgpt-and-other-malicious-ais-are-the-new-frontier-of-online-threats-what-can-we-do-234820#:~:text=For%20instance%2C%20FraudGPT%20writes%20malicious%20code%2C%20creates,web%20and%20the%20encrypted%20messaging%20app%20Telegram.
- Beltrán, P., Pérez, M. & Nespoli, P. (2025). Cyber Deception: Taxonomy, State of the Art, Frameworks, Trends, and Open Challenges. *IEEE Communications Surveys & Tutorials,* 1-1. DOI:10.1109/COMST.2025.3594788
- BBC (8 June 2021). ANOM: Hundreds arrested in massive global crime sting using messaging app. Available at: https://www.bbc.com/news/world-57394831
- Biprojit, C. (2025). The Ultimate Guide to HIPAA Compliance Audit in 2025. Available at: https://www.cloudeagle.ai/blogs/the-ultimate-guide-to-hipaa-compliance-audit
- Breached Company (2025). Briefing on the 2025 Cybersecurity Landscape: Key Threats, Trends, and Incidents. Available at: https://breached.company/briefing-on-the-2025-cybersecurity-landscape-key-threats-trends-and-incidents/
- Burstein, Aaron. (2008). Conducting Cybersecurity Research Legally and Ethically. First USENIX Workshop on Large-Scale Exploits and Emergent Threats, April 15, 2008, San Francisco, CA, USA, Proceedings. Available at: https://www.researchgate.net/publication/220832007_Conducting_Cybersecurity_Research_Legally_and_Ethically
- Chris, E. (2025). Over 75% of Companies Have Not Implemented AI Ethics. Datamation. Available at: https://www.datamation.com/artificial-intelligence/over-75-percent-companies-not-implemented-ai-ethics/
- Chris, P. (2025). US SEC dismisses case against SolarWinds, top security officer. Reuters. Updated November 20, 2025. Available at: https://www.reuters.com/legal/government/us-sec-dismisses-case-against-solarwinds-top-security-officer-2025-11-20/
- Cloudflare (2025). State of the post-quantum Internet in 2025. Available at: https://blog.cloudflare.com/pq-2025/#:~:text=41%20min%20read,new%20exciting%20cryptography%20was%20proposed.
- Connor, J. (2024). "The Rise of Malicious Honeypots: A New Threat in Cyber Deception Tactics," CyberMaxx. Available https://www.cybermaxx.com/resources/the-rise-of-malicious-honeypots-a-new-threat-in-cyber-deception-tactics/
- CrowdStrike (2025). CrowdStrike Global Threat Report: China's Cyber Espionage Surges 150% with Increasingly Aggressive Tactics, Weaponization of AI-powered Deception Rises. February 27, 2025. Available at: https://ir.crowdstrike.com/news-releases/news-release-details/2025-crowdstrike-global-threat-report-chinas-cyber-espionage/#:~:text=Insider%20Threats%20Continue%20to%20Rise,defenders%20little%20time%20to%20react.
- Darma M, Gisymar NA, Purwadi A, Zubaedah PA, & Judijanto L. (2025). Legal implications of deepfake technology misuse in digital content on social media. Science of Law. Science of Law, 2025, No. 3, pp. 98-103, DOI:10.55284/eqazc148
- Datasphere Initiative (2025). Sandboxes for AI: Tools for a new frontier. Available at: https://www.thedatasphere.org
- Ebunoluwa A, James A. (2025). AI-Powered Honeypots: Enhancing Deception Technologies for Cyber Defense. Available at: https://www.researchgate.net/publication/390113901_AI-Powered_Honeypots_Enhancing_Deception_Technologies_for_Cyber_Defense
- European Commission (2024). "AI Act," Shaping Europe's digital future. Available at: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai#1720699867912-0
- ExtraHop (2024). Making Sense of Proposed CIRCIA Incident Reporting Rules. Available at: https://www.extrahop.com/blog/circia-cyber-incident-reporting-requirements
- Fraunholz, D., Duque Anton, S., Lipps, C., Reti, D., Krohmer, D., Pohl, F., Tammen, M. & Schotten, H. (2018). Demystifying Deception Technology: A Survey. DOI:10.48550/arXiv.1804.06196.
- Gibson, D. (2025). U.S. Cybersecurity and Data Privacy Review and Outlook – 2025. Available at: https://www.gibsondunn.com/us-cybersecurity-and-data-privacy-review-and-outlook-2025/
- Goncalves, M., & Dangelo, D. (2025). Regulating the Mind: Neuromarketing, Neural Data and Stakeholder Trust Under California's CCPA. Administrative Sciences, 15(10), 386. https://doi.org/10.3390/admsci15100386
- Holz, T. & Raynal, F. (2005). Detecting Honeypots and other suspicious environments. Conference: Information Assurance Workshop, 2005. IAW '05. Proceedings from the Sixth Annual IEEE SMC. DOI:10.1109/IAW.2005.1495930
- Howard, P. (2021). "Top threat modeling frameworks: STRIDE, OWASP Top 10, MITRE ATT&CK framework and more," Management, Compliance & Auditing. Infosec. Available at: https://www.infosecinstitute.com/resources/management-compliance-auditing/top-threat-modeling-frameworks-stride-owasp-top-10-mitre-attck-framework/

- IBM (2024). Reflecting on the Five-Year Anniversary of IBM's AI Ethics Board. Available at: https://www.ibm.com/granite/docs/resources/ai-ethics-board-5-year-anniversary.pdf#:~:text=These%20events%20reflect%20some%20of%20the%20many,the%20development%2C%20deployment%2C%20and%20use%20of%20technology.
- Ikuomenisan, G. & Morgan, Y. (2022). Meta-Review of Recent and Landmark Honeypot Research and Surveys. Journal of Information Security, 13, 181-209. doi: 10.4236/jis.2022.134011.
- Jovan, S. (2025). Timeline for NIS2 compliance and implementation deadlines. Available at: https://www.chino.io/post/timeline-for-nis2-compliance-and-implementation-deadlines#:~:text=What%20to%20expect%20in%202025,your%20business%20and%20your%20users
- Katie, W. (2025). Trump Signs Executive Order Amending Cybersecurity Requirements. American Bar Association (ABA). Available at: https://www.americanbar.org/groups/health_law/news/2025/6/trump-signs-executive-order-amending-cybersecurity-requirements/
- Kenneth Geers (February 9, 2011). Sun Tzu and Cyber War. *In* CCD CoE. Retrieved from: https://ccdcoe.org/library/publications/sun-tzu-and-cyber-war/
- Khan, W. (2022). Achieving Regulatory Compliance with ISO 27001 and NIST Frameworks: The Process and Challenges of Obtaining these Critical Certifications for Clients. Journal of Artificial Intelligence & Cloud Computing. 1-14. DOI:10.47363/JAICC/2022(1)E170.
- Kondapalli, P., Singh, P., Malik, A., & Lesmana, C. S. A. T. (2025). A Literature Review: Bias Detection and Mitigation in Criminal Justice. *Engineering Proceedings, 107*(1), 72. https://doi.org/10.3390/engproc2025107072
- Legal IT Insider (May 28, 2025). Updated: LexisNexis Risk Solutions suffers data breach affecting over 364,000 people. Available at: https://legaltechnology.com/2025/05/28/lexisnexis-risk-solutions-suffers-data-breach-affecting-over-364000-people/#:~:text=May%2028%2C%202025-,Updated:%20LexisNexis%20Risk%20Solutions%20suffers%20data%20breach%20affecting%20over%20364%2C000,well%20as%20notifying%20law%20enforcement.
- Market.Us (2025). Deception Technology Market. Available at: https://market.us/report/deception-technology-market/#:~:text=Given%20their%20complex%20operational%20needs%2C%20large%20enterprises,robust%20ways%20to%20safeguard%20their%20digital%20assets.
- Matthew, O. (2025). The real costs of non-compliance in cyber security. Integrity360. Available at: https://insights.integrity360.com/the-real-costs-of-non-compliance-in-cyber-security
- Mordor Intelligence (2025). "Deception Technology Market Size & Share Analysis - Growth Trends & Forecasts (2025 - 2030)," Global Deception Technology Market. Available at: https://www.mordorintelligence.com/industry-reports/deception-technology-market
- Morić, Z., Dakić, V., & Regvart, D. (2025). Advancing Cybersecurity with Honeypots and Deception Strategies. Informatics, 12(1), 14. https://doi.org/10.3390/informatics12010014
- Moustafa, AA., Bello, A., & Maurushat, A. (2021). The Role of User Behaviour in Improving Cyber Security Management. *Frontiers in Psychology, 12*, 561011. https://doi.org/10.3389/fpsyg.2021.561011
- National Institute of Standards and Technology (NIST). (August 13, 2024). NIST Releases First 3 Finalized Post-Quantum Encryption Standards. Available at: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
- National Conference of State Legislatures (July 10, 2025). Artificial Intelligence 2025 Legislation. Updated July 10, 2025. Available at: https://www.ncsl.org/technology-and-communication/artificial-intelligence-2025-legislation
- NQA (2025). ISO 27001:2022 Transition Guidance for Clients. Available at: https://www.nqa.com/en-ca/transitions/iso-27001-2022#:~:text=ISO%2027001:2022%20Change%20Analysis,standards%20(i.e.%20Annex%20SL).&text=However%2C%20several%20previous%20controls%20have,Secure%20Coding
- Organisation for Economic Co-operation and Development (OECD). (29 September 2025). Better Regulation Practices across the European Union 2025. Available at: https://www.oecd.org/en/publications/better-regulation-practices-across-the-european-union-2025_6f007516-en.html#:~:text=To%20get%20the%20balance%20right%20and%20make,)%20Recommendation%20on%20Regulatory%20Policy%20and%20Governance.
- Ortega Velázquez, MÁ., Cuevas Martínez, I., & Jara, AJ. (2025). Integrating the CRA into the IoT Lifecycle: Challenges, Strategies, and Best Practices. Information, 16(12), 1017. https://doi.org/10.3390/info16121017
- Perkins, R. & Howell, C. (2021). Honeypots for Cybercrime Research. In Researching Cybercrimes, Methodologies, Ethics, and Critical Approaches (pp.233-261), DOI:10.1007/978-3-030-74837-1_12
- Pooja, R. (2025). ISC2 CC Domain 5:5.4: Understand Security Awareness Training. Available

at: https://www.infosectrain.com/blog/isc2-cc-domain-5-5-4-understand-security-awareness-training/#:~:text=Security%20awareness%20training%20is%20a,attacks%20and%20strengthening%20password%20practices.

- Quanyan, Z (2023). The Doctrine of Cyber Effect: An Ethics Framework for Defensive Cyber Deception. *ArXiv*. https://arxiv.org/abs/2302.13362
- Reid, I., Okeke-Ramos, A., & Serafin, M. (2024). Exploring the ethics of cyber deception technologies for defensive cyber deception. The 10th International Conference on Socio-Technical Perspectives in IS (STPIS'24). Jönköping, Sweden.
- Renée, NG (2023). The Honeypot Stings Back: Entrapment in the Age of Cybercrime and a Proposed Pathway Forward. Chicago Journal of International Law, Vol. 24 No. 1, pp. 187-221.
- Rowe, NC (2008). "The Ethics of Deception in Cyberspace," *In* the Handbook of Research on Technoethics, ed. R. Luppicini, Hershey, PA: Information Science Reference. Available at: https://faculty.nps.edu/ncrowe/technoethics_cyberdec.htm
- Secure Privacy (December 11, 2025). Privacy Laws 2026: Global Changes, Enforcement & Compliance Guide . Available at: https://secureprivacy.ai/blog/privacy-laws-2026
- Sokol, P., Míšek, J. & Husák, M. (2017). Honeypots and honeynets: issues of privacy. EURASIP J. on Info. Security 2017, 4. https://doi.org/10.1186/s13635-017-0057-4
- Stefano De Luca & Marina Federico (2025). Algorithmic discrimination under the AI Act and the GDPR. European Parliamentary Research Service (EPRS). PE 769.509. Available at: https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/769509/EPRS_ATA(2025)769509_EN.pdf
- Tencent Cloud (2025). "What are the special requirements for the application of deception defense in the medical industry?" Technology Encyclopedia Home. Available at: https://www.tencentcloud.com/techpedia/118549
- Tikanmäki, I., Rajamäki, J., Boateng, F., Kaikkonen, J., Ketene, B., Lehtiaho, J., & Miestamo, J. (2025). Cyber threats in hospitals: GDPR and NIS2 regulations in preventing USB injections. International Conference on Cyber Warfare and Security, 20(1), 461–468. https://doi.org/10.34190/iccws.20.1.3308
- United Nations (2025). "2025 Technology and Innovation Report: Inclusive Artificial Intelligence for Development," United Nations Conference on Trade and Development (UNCTAD). UNCTAD/TIR/2025. United Nations Publications: Geneva. Available at: https://unctad.org/system/files/official-document/tir2025_en.pdf
- Williamson, SM., & Prybutok, V. (2024). The Era of Artificial Intelligence Deception: Unraveling the Complexities of False Realities and Emerging Threats of Misinformation. Information, *15*(6), 299. https://doi.org/10.3390/info15060299
- Yan, L. (2025). "China Amends Cybersecurity Law and Incident Reporting Regime to Address AI and Infrastructure Risks," in Cybersecurity. Inside Privacy: Updates on Developments in Data Privacy and Cybersecurity. Available at: https://www.insideprivacy.com/cybersecurity-2/china-amends-cybersecurity-law-and-incident-reporting-regime-to-address-ai-and-infrastructure-risks/
- Yan, L. (2025). "China Amends Cybersecurity Law and Incident Reporting Regime to Address AI and Infrastructure Risks," Global Policy Watch: Key Public Policy Developments Around the World. Available at: https://www.globalpolicywatch.com/2025/10/china-amends-cybersecurity-law-and-incident-reporting-regime-to-address-ai-and-infrastructure-risks/
- Yihang, S., Huajun, Z., Lin, S., & Shoukun, X. (2025). Autonomous cyber defense for AIoT using Graph Attention Network-Enhanced reinforcement learning, Computer Communications, Volume 241, 108265, ISSN 0140-3664, https://doi.org/10.1016/j.comcom.2025.108265.