A Double-Edged Sword: How Lab Cameras may Enable Some Cyber Deception in Biosecurity

Rachid Soro[1], Lucas Potter[2], Xavier Palmer[2] and Michaela Barnett[3]
[1]Independent Security Researcher, Virginia, USA
[2]BiosView Labs, Ohio, USA
[3]Blacks In Cybersecurity Headquarters, Inc., Virginia, USA

nowireless@proton.me
biosview1@proton.me

Abstract: Cameras keep individuals and assets safe by monitoring behavior, configurations or indications of concern. Cameras are utilized throughout daily life; supporting lifestyles, greater domestic, civil, industrial or and laboratory infrastructure. Cameras monitor plants in controlled experiments, capturing images analyzed by AI to decide when to provide water or nutrients. This setup sounds efficient and reliable but introduces new risks. Internet-connected cameras can be hacked. If that happens, an attacker could fake the footage, hiding an intruder entering a high-security lab or tricking an automated system, like the AI-powered machine, into damaging crops. A tool meant to protect can easily turn into a threat. This paper explores how lab cameras act as both protectors and sources of risk in biosecurity laboratories. We combine research papers and real-world examples in a narrative review to understand how these systems are used and where they fail. We classify risks ranging from weak software and unprotected networks to tampered camera feeds and flawed security updates. Alongside this taxonomy, we discuss solutions such as better network isolation, automated checks for altered footage, and stronger device verification protocols. This review reveals that current research often treats cybersecurity and biosecurity as separate fields, leaving a critical gap where these domains overlap. Relatively few studies have examined how deceptive camera data could disrupt lab operations, cause security breaches, or lead to worse outcomes. Furthermore, few have examined the intersection of biosecurity, cyber-physical security, and cybersecurity. By connecting these domains, this paper highlights the necessity for an integrated approach to improve camera safety and reliability in laboratories. Implementing stronger standards and security practices is essential to prevent these vital devices from becoming vulnerabilities rather than assets. Integrated security efforts can benefit from closer inclusion of camera functions, uses, and forensics.

Keywords: Cyberbiosecurity, Cameras, Laboratory, Deception, Forensics

1. Introduction

Surveillance cameras are ubiquitous, monitoring areas from residences to high-security environments. These devices increasingly rely on internet connectivity, offering real-time and remote monitoring for critical security functionality (ECAM Technologies Corp., 2025). Cameras are categorized as Analog or Digital (Internet Protocol (IP)) where data is transmitted over a network and remotely managed (ECAM Technologies Corp., 2025). Analog cameras transmit video through coaxial cables with separate power lines, producing lower resolution.

An IP camera, or Internet Protocol camera as referenced above, is a type of digital video camera that transmits and receives data over a network or the internet, allowing for remote surveillance and monitoring. Modern IP cameras use a single Ethernet cable for both power and data transmission via Power over Ethernet (PoE) technology and now dominate Biosecurity Laboratories due to their high-resolution imaging performance, functional reliability, and features that align with the unique needs of facilities. However, as Blancaflor et al. (2023) highlight, these devices are often vulnerable to cyberattacks due to issues like unencrypted RTSP streams and weak authentication, which can lead to data theft and unauthorized access. The device's additional connectivity features facilitate seamless integration within networked environments. In relation to operational security, cameras with this capability are able to provide remote monitoring functionality. As they are used across various environments and integrated with other IoT (Internet of Things) devices, their reliance on network connectivity introduces potential cybersecurity vulnerabilities, making them susceptible to unauthorized access or data interception if not properly secured (Affia et al., 2023; Kalbo et al., 2020).

Many labs utilize remote-controlled cameras to monitor personnel in maximum-containment areas, where; the highest level of controlled isolation is applied to a system, facility or environment. This is designed to prevent any form of leakage, exposure or unauthorized interaction by employing the most stringent safeguards available (Diederich & Eschbaumer, 2025). This allows external observers to rapidly identify and respond to incidents or "security breaches" (CDC Emerging Infectious Diseases, 2011), to examine a practical use case. These cameras are increasingly integrated into networked, cyber-physical systems, forming part of broader IoT environments and reflecting the convergence of digital and physical infrastructures (NuAire, Inc.,

2015; Kalbo et al., 2020; National Institute of Standards and Technology, 2024). However, this dependence creates vulnerabilities. Cyberbiosecurity frameworks treat security systems and networked devices as critical assets in the laboratory, whose compromise undermines both required safety oversight and the active scientific activity (George, 2019; Reed & Dunaway 2019). While IP cameras enhance oversight, they also act as an entry point to a given attack surface. Attackers can utilize unauthenticated access or access retrieved from exploitation to manipulate video feeds, disrupt monitoring or interfere with emergency protocols. This introduces risk that undermines the intended safety guarantees.

This paper addresses this double-edged sword. While IP cameras in this current landscape act as essential tooling with multiple applications, they are also potential vectors for cyber deception, defined in this work as the intentional manipulation, falsification or withholding of information using technology. It is significant to acknowledge this concept of Cybersecurity throughout this work in contrast to the general understanding or holistic idea of deception; "Deliberately inducing erroneous sensemaking to gain an advantage" (Defused Cyber, n.d.).

This analysis intends to highlight the critical overlap of cybersecurity and biosecurity in reference to the related surveillance with the intention to propose practical solutions to enhance the security and reliability of camera systems (IP Cameras) in biosecurity environments.

2. Case Studies in Relation to Threat Landscape

Internet-connected IoT (Internet of Things) enabled cameras in biosecurity labs to introduce multiple vulnerabilities. The interconnectivity via the internet enables constant communication between devices, exposing them to actors with varying motives. In the current age, motives have moved away from amusement or sport to the acquisition of resources such as intelligence or information about a target, data or monetary gain, for an ultimate goal of leverage (Prasad et al., 2025). The healthcare sector remains a prime target for cyber threats and a candidate for examination as a case study. In this instance a cause for consideration in adapting or appropriating new technology would be for the purpose of inter-communication, treating patients or the translation of results. Many Life Sciences Laboratories would also share this same use case and concern, especially around delicate environments unique to these facilities. (Affia et al, 2023).

IP Cameras can enable deception, espionage or additonal resulting factors (Cunliffe, 2021; Herodotou and Hao, 2023; Singh and Dhumane, 2025). IP Cameras can serve as powerful tools for deception and espionage by enabling the covert collection and manipulation of visual input. In the contextual use of an abusive actor or offensive security practitioner, IP Cameras may be used to observe user behavior, capture sensitive data (such as credentials or screen activity) or possibly build intelligence for targeted attacks (Cunliffe, 2021; Herodotou and Hao, 2023; Singh and Dhumane, 2025). IP Cameras can also support nefarious operations by creating false perceptions. Placing/replacing physical cameras and/or their feed to suggest surveillance while the actual monitoring occurs elsewhere. IP Cameras can also be manipulated to produce footage to mislead viewers. Deception research provides a useful vocabulary for understanding how compromised IP Camera systems can shape an environment.

IP Cameras in biosecurity laboratories are especially vulnerable to these dynamics because they can be treated as authoritative windows into these restricted spaces or diagnostic tools. When attackers can pause (jam), freeze (stop), or loop (repeat) feeds, they are directly manipulating the perceptual channel that underpins safety decisions and incident reconstructions or recounts (Clark and Mitchell, 2019; Reed and Dunaway, 2019).

2.1 Case Study: Cloud-Connected, Remotely Controllable Cameras

Work by Kalbo et al. (2020) supports that Cloud-connected, remotely controllable cameras can introduce attack surfaces. A notable, related application involved Flock Safety exposing livestreams and administrative interfaces for at least sixty of its AI-enabled Condor cameras to the open internet without authentication, enabling access to live feeds, archived footage (up to thirty days), and camera configuration controls (Koebler, 2025). Threat actors can leverage tools such as Shodan, a specialized search engine that indexes internet-connected devices (e.g., servers, webcams, and IoT systems), to discover and exploit exposed systems, significantly expanding the attack surface of networked infrastructure (Kalbo et al, 2020; Herodotou and Hao, 2023; Koebler, 2025). High-containment laboratories are specialized facilities designed to safely handle and study hazardous biological agents under strict security and safety controls (Crawford et al., 2023). High-containment laboratories trend toward adopting integrated cyber-physical architectures managing security and containment (Crawford et al., 2023). These laboratories increasingly rely on networked camera systems, where visual surveillance is conducted through integrated digital monitoring infrastructures that operators

may utilize to conduct reviews and make critical decisions *(Crawford et al., 2023)*. Poorly secured systems enable external adversaries to silently monitor lab routines, download historical footage or modify settings. Cyber intrusions targeting equipment can facilitate "malicious access to or alteration of security-relevant digital records," making it difficult to distinguish between accidental and deliberate acts (Reed and Dunaway, 2019). These weaknesses directly intersect with Cyberbiosecurity concerns as laboratories become more "smart" and seek to interconnect their systems for efficiency or automation.

Exposure in this case primarily enables intelligence gathering and preparation of attempted deception. An actor who can silently watch, archive, configure or set up persistence toward cameras can gain a detailed picture of routines and blind spots that can later support more active activity, such as concealment or simulation. In terms of deception, this positioning work or staging shapes what exists authentically, stored in archives or changed; thereby pre-structuring how practitioners will later make sense of activity and illustrating how deception targets "sensemaking" and downstream behavior rather than isolated perceptions alone (Clark and Mitchell, 2019; Henderson, 2023). Connecting systems increases the attack surface, risking cascading consequences across multiple safety and security functions from a single cyber-attack (Crawford et al., 2023). Concurrently, camera feeds are evolving from passive recording to the infrastructure to include "smart" safety systems. Computer-vision-based technology would be an applicable use case to reflect upon in this environment as many organizations or institutions move toward automated auditing of compliance auditing and enforcement. A case to review would be the use and retention of personal protective equipment (PPE) compliance systems that use video analytics for automatic detection and supervision in real time (Vukicevic et al., 2024). This integration means camera streams directly influence compliance assessments and operational responses.

When lab cameras serve the dual role of auditing and compliance partners within organizations, manipulating their streams or archived data becomes a potent vector for the goal of deception (Reed & Dunaway, 2019; Crawford et al., 2023). Adversaries and actors who interfere with the integrity or availability of these feeds can shape what automated systems "see" and alter what personnel are able to review.

2.2 Case Study: Wireless Camera Jamming

Wireless IP camera performance may be influenced by frequency band choice; this boasts another illustrative example. The 2.4 GHz band generally offers greater range and wall penetration but is more susceptible to congestion, whereas 5 GHz provides higher throughput with reduced congestion over shorter distances (Intel, n.d.). This distinction is relevant for security considerations because the camera's operational band affects how its wireless communications behave under interference or disruption. Non-peer-reviewed technical reporting has described proof-of-concept devices capable of generating interference across these bands, with demonstrations suggesting that Wi-Fi camera video streams may be disrupted under interference conditions, for example through packet loss (Skyforest, 2025). Prior research on hidden and network-connected surveillance devices indicates that such systems can be detected and analyzed through methods such as network traffic monitoring, signal analysis, and device fingerprinting (Pravin et al., 2022; Ju et al., 2025). At the same time, more recent work suggests that no single detection method is consistently reliable, and that combining multiple approaches may improve identification accuracy in complex environments (Kumar et al., 2026). In tandem, these findings highlight that wireless surveillance devices introduce measurable security considerations, although the effectiveness of detection and interference techniques may vary depending on the environment and device characteristics. Practical demonstrations further illustrate the feasibility of disrupting wireless camera systems.

For example, a prototype device has been suggested to have the capability to interfere with 2.4 GHz wireless cameras, disrupting live video feeds during testing (CiferTech, 2025). As many surveillance devices operate on the 2.4 GHz band due to its extended range and compatibility, systems configured to use this frequency may be particularly susceptible to such interference, highlighting a potential vulnerability in real-world deployments (Herodotou and Hao, 2023). In modern "Wi-Fi-enabled" laboratories, where cameras, instruments, and building systems share a networked infrastructure, a device modeled after the RF-Clown v2 could pose a tangible threat. Cyberbiosecurity analyses of high-containment laboratories suggest that the increasing integration of interconnected cyber-physical systems (such as building automation, biosafety cabinets and networked access controls) may expand the overall attack surface.

Under certain conditions, this interconnectivity could allow a compromise in one component to affect other systems, potentially weakening multiple layers of safety and security. However, the extent to which such effects propagate depends on system architecture, configuration, segmentation and operational controls

(Pravin et al., 2022; Ju et al., 2025). When wireless cameras monitor critical procedures or access, a brief, well-timed freeze of a 2.4 GHz video feed can create an opportunity for deception "blind window" that is invisible to downstream auditing, yet sufficient enough to obscure an unauthorized action. Targeted wireless interference tools such as RF-Clown v2 demonstrate how disruption can degrade the availability of visual monitoring systems by interrupting or freezing live camera feeds (CiferTech, 2025; Skyforest, 2025). The resulting loss or delay of real-time information may still influence decision-making, as operators and automated systems depend on timely data to interpret events (Clark and Mitchell, 2019; Henderson, 2023).

2.3 Case Study: Looping and Spoofing Lab Camera Feeds

In “Cyber War: The Next Threat to National Security and What to Do About It”, Richard A. Clarke and Robert K. Knake (2010) describe the Stuxnet operation targeting Iran’s Natanz facility, noting that it involved both process disruption and manipulation of monitoring outputs. They report that compromised Supervisory Control and Data Acquisition (SCADA) systems could present data consistent with normal operation despite underlying anomalies (Clarke and Knake, 2010). More generally, industrial control system incidents have been understood to involve interactions between physical processes and digital monitoring systems. In environments that rely on such systems for situational awareness, especially laboratory settings, compromise of monitoring outputs could affect how system conditions are perceived. The relevance and impact of such scenarios depend on system design and implementation.

IP cameras may also be susceptible to network-layer manipulation under certain conditions. For example, a Forescout demonstration showed that, where video streams are transmitted using unencrypted protocols, it is possible to intercept traffic and replay previously recorded footage in place of a live feed (dos Santos, 2019). Such scenarios depend on specific configuration weaknesses but suggest that, in some deployments, visual monitoring systems may not reliably reflect real-time conditions if compromised.

In examining the intersection of the stuxnet’s modus operandi and IP camera-replay we can illustrate the technique of deception in which attackers present convincing but false views to operators while damaging or unsafe processes unfold behind the scenes. Analyses of deception stress that such operations work not because they are visually spectacular, but because they are boringly plausible and align with what the audience already expects to see, thereby nudging them toward inaction when intervention is needed (Clark and Mitchell, 2019; Henderson, 2023).

2.4 Case Study: “Dance-coding”, “Vogue-coding” and Vision Challenges

Laboratory camera systems are increasingly embedded in biosecurity workflows, supporting monitoring, compliance, and incident reconstruction. As networked, cyber-physical assets, they fall within the scope of cyberbiosecurity (Reed and Dunaway, 2019). Prior work shows that IP-based surveillance systems can be manipulated at the network or device level, including disruption or replay of video streams under certain conditions (Kalbo et al., 2020; dos Santos, 2019). In parallel, advances in vision-language models, such as representation-learning approaches exemplified by Meta AI (FAIR)’s VL-JEPA, demonstrate increasing capability to extract structured information from video data (Chen et al., 2025). While primarily developed for perception tasks, their integration into camera systems may extend functionality from passive recording toward automated interpretation. Together, these strands suggest that camera systems may present a more complex security consideration than is reflected in current cyberbiosecurity literature, which has largely treated them as generic IoT devices. However, empirical evidence specific to high-containment laboratory environments remains limited, and this work therefore focuses on plausible risks rather than demonstrated prevalence.

Hypothetical Path 1: Visual Coding To Trigger Malicious Action

A hypothetical scenario for discussion involves a future IP camera system integrated with a multimodal vision–language model responsive to visual inputs. In principle, if such systems interpret human movement as input, structured motion patterns could influence outputs in unintended ways. The concept of “vogue-coding” is used here as a metaphor for encoding signals through movement, drawing on the technique of vogueing which draws on Ballroom culture from the 20th Century (Winsor, 2023; Ray, 2025). The use of this term does not imply a yet practical programming method, but illustrates how visual inputs, if systematically interpreted, might carry implicit instructions. Under adversarial conditions, carefully constructed movements could potentially bias or disrupt model interpretation. This remains speculative. There is no clear evidence that current systems can be intentionally controlled through unconstrained movement, particularly in operational settings. However, research on adversarial inputs shows that machine learning systems can be influenced by

crafted signals. Accordingly, “vogue-coding” is best understood as a conceptual lens for anticipating how future vision-enabled systems may require safeguards against unintended or adversarial visual inputs.

Hypothetical Path 2: Generating Fabricated or Fraudulent Visual Artifacts

This path considers an adversarial scenario in which a vision system generates misleading or fabricated visual outputs, conceptually similar to demonstrated manipulation of medical imagery using generative models (e.g., CT-GAN) (Mirsky et al., 2019). In principle, sufficiently advanced and well-integrated camera systems incorporating generative capabilities could introduce ambiguity or doubt into visual records, potentially complicating evidentiary interpretation in legal or investigative contexts (Zhao et al., 2019; Apolo and Michael, 2024; Tayfor et al., 2025; Guo, 2025).

The motivations for such manipulation may include both inducing false beliefs in system users and shaping the behavior of downstream observers or decision-makers. While proposed applications span a wide range of domains, including agriculture, life sciences, healthcare, and critical infrastructure, these uses are best understood as context-dependent and largely speculative, rather than established attack patterns (Mo et al., 2022; Elgabry, 2023; Kaufman et al., 2023; Potter and Palmer, 2023; Stephen et al., 2023; Potter and Palmer, 2024; Stephen et al., 2024).

System effectiveness could, in principle, be enhanced by integrating additional data sources such as biometric tracking or IoT-linked devices. However, the coordinated exploitation of such multimodal inputs for deception remains an area of ongoing research, rather than a demonstrated capability (Affia et al., 2023; James et al., 2025; Potter et al., 2025; Purnell et al., 2025). Increased data aggregation may also expand the attack surface, particularly where data leakage or weak integration controls are present. Mitigation is necessarily multi-layered. Techniques such as watermarking and data integrity controls may contribute to detection and resilience, but they do not constitute comprehensive solutions (Morrison, 2018; Korada, 2024; Naik et al., 2025). More broadly, reducing risk requires a combination of secure system design, provenance verification, and ongoing monitoring of visual data pipelines.

Both Path 1 and Path 2 highlight emerging challenges in adversarial vision systems, likely requiring interdisciplinary responses. The scenarios point to a speculative future where camera-driven systems could be influenced by structured visual inputs, shaping behaviour in unintended ways. In this context, deception operates by introducing plausible but misleading signals into perception, affecting both human and machine interpretation in line with established principles of plausibility and expectation (Clark and Mitchell, 2019; Henderson, 2023).

3. Integrated Security and Best Practices

Defenders must counter adversaries who blend digital and physical domains, employing a vast library of tools particularly against laboratory cameras. Countering these threats requires uniting experts in cybersecurity, biosecurity, cyber-physical engineering, and policy via practical mechanisms like cross-sector partnerships, and routine information-sharing (Powell et al., 2021; Adeoye et al., 2023; Haley and Burrell, 2025). Laboratory cameras must be treated as integral safety and security infrastructure, not peripherals. This means joint risk assessments considering how camera compromise affects biosafety, physical security, and digital records; standardized video tampering response plans; and involving both IT security and laboratory safety officers in system design (Reed and Dunaway, 2019; Cyberbiosecurity in High-Containment Laboratories, 2023; ASPR, n.d.).

Given their centrality, cameras are critical systems demanding systematic pre-deployment security testing of hardware, firmware, and network configurations. This testing must verify basic hygiene, such as changing default passwords, enforcing strong authentication, and disabling unauthenticated access. An internal testing team is beneficial, reducing exposure of sensitive network details, though external expertise should still be utilized. These checks determine camera appropriateness and the necessity for "compensating controls or patches." Continuous vulnerability monitoring is also essential. In the examination of the October 2025 Louvre jewel heist, it can be derived that high-profile institutions despite the most sophisticated security consideration and planning can exhibit poor camera security; weak authentication enables exploitation (Leath, 2025; Seipel, 2025).

Technical practices beyond testing form a baseline for securing lab camera systems. Network segmentation and isolation are central: placing cameras on dedicated, access-controlled segments separate from "unrelated internal systems" like instruments or administrative workstations, a critical concern in high-containment

facilities (Reed and Dunaway, 2019; Crawford et al., 2023). Strong device authentication and access control, avoiding default credentials and unauthenticated web interfaces, as seen with exposed "Flock Condor cameras" and the "Louvre's CCTV password", reduces silent external monitoring (Koebler, 2025; Reyes, 2025; Leath, 2025; Seipel, 2025). Regular security updates, prompt patching and explicit decommissioning prevent cameras from becoming "long-lived footholds" (ASPR, n.d.; Reed and Dunaway, 2019).

Finally, forensic-readiness measures, including "tamper-evident logging, redundant storage," and mechanisms to validate "archived footage," are necessary to detect deceptive attacks which can otherwise make operations appeared to proceed without anomaly (Clarke and Knake, 2010; (Johns Hopkins University Applied Physics Laboratory, 2003; Tayfor et al., 2025).

4. Discussion, Limitations and Conclusion

Laboratory camera systems are increasingly used for monitoring, compliance, and retrospective review, particularly in controlled environments (NuAire, Inc., 2015). As these systems contribute to situational awareness and documentation, their reliability may influence how events are interpreted within a facility. Existing research and reporting indicate that such systems can exhibit a range of vulnerabilities, including weak authentication (Leath, 2025), unencrypted video transmission (dos Santos, 2019), and susceptibility to wireless interference (Skyforest, 2025).

More broadly, studies of cyber-physical systems show that manipulation or disruption of monitoring data can affect perception by presenting incomplete or misleading information (Clarke and Knake, 2010; Clark and Mitchell, 2019). While these findings derive from varied contexts, they suggest that monitoring systems may be vulnerable to both disruption and misrepresentation. Cyberbiosecurity literature has not consistently examined camera systems as distinct components of laboratory security, often treating them as general IoT infrastructure (Reed and Dunaway, 2019; Racicot et al., 2022; Cyberbiosecurity in High-Containment Laboratories, 2023).

This indicates a need for further study of their role in safety oversight and evidentiary use. This exploration is limited by its narrative scope and reliance on examples drawn largely from outside laboratory settings. Accordingly, it emphasizes potential vulnerabilities and design considerations rather than the prevalence of such incidents in biosecurity environments. In the future, a focus topic is to examine defense in depth as a strategy for defending against cyber deception.

Despite these limitations, the analysis confirms that laboratory cameras hold a critical yet under-examined role in Cyberbiosecurity. Cameras mediate operational visibility, safety enforcement, and incident reconstruction; vulnerability to unauthorized access, jamming, looping, or adversarial manipulation transforms them from protective tools into enablers of cyber deception. Future work should convene operators, biosafety/biosecurity professionals, cybersecurity/cyber-physical engineers, and legal/policy experts to experimentally evaluate camera architectures, adversarial attacks, and mitigation strategies in realistic lab settings, translating these findings into integrated standards and training.

Ethics Statement: No experimental subjects were performed upon in this work.

AI Ethics Statement: To organize and format parts of the paper, AI tools within ChatGPT, Grammarly and Google Docs were used.

References

Adeoye, S.O., Lindberg, H., Bagby, B., Brown, A.M., Batarseh, F.A. and Kaufman, E.K., 2023. Cyberbiosecurity Workforce Preparation: Education at the Convergence of Cybersecurity and Biosecurity. NACTA Journal, 67, pp.341-351.

Affia, A.A.O., Finch, H., Jung, W., Samori, I.A., Potter, L. and Palmer, X.L., 2023. IoT health devices: exploring security risks in the connected landscape. *IoT*, *4*(2), pp.150-182.

Apolo, Y. and Michael, K., 2024. Beyond a reasonable doubt? Audiovisual evidence, AI manipulation, deepfakes, and the law. *IEEE Transactions on Technology and Society*, *5*(2), pp.156-168.

ASPR (Assistant Secretary for Preparedness and Response) (n.d.) Physical security. U.S. Department of Health and Human Services. Available at:https://aspr.hhs.gov/S3/Pages/Physical-Security.aspx (Accessed: 6 January 2026).

Blancaflor, E., Ong, A., Navarro, A., Sudo, K. and Villasor, D. (2023) 'Exploring the Attacks, Impacts, and Mitigations in a Real-Time Streaming Protocol Service of IP Cameras', in 2023 9th International Conference on Computer Technology Applications (ICCTA 2023), May 10-12, 2023, Vienna, Austria. New York, NY: ACM. doi: 10.1145/3605423.3605447

Centers for Disease Control and Prevention (CDC) (2009) Emerging infectious diseases, 15(7). Available at:https://wwwnc.cdc.gov/eid/article/15/7/08-1523_article (Accessed: 6 January 2026).

Chen, D., Shukor, M., Moutakanni, T., Chung, W., Yu, J., Kasarla, T., Bolourchi, A., LeCun, Y. and Fung, P. (2025) 'VL-JEPA: Joint embedding predictive architecture for vision-language', arXiv preprint, arXiv:2512.10942. Available at:https://arxiv.org/abs/2512.10942 (Accessed: 6 January 2026).

CiferTech (2025) 'RF-Clown v2: The wireless beast just got a turbo boost', 27 October. Available at: https://cifertech.net/rf-clown-v2 (Accessed: 15 April 2026).

Clark, R.M. and Mitchell, W.L. (2019) Deception: counterdeception and counterintelligence. 1st edn. Los Angeles; London; New Delhi: SAGE / CQ Press. Available at: https://us.sagepub.com/sites/default/files/upm-binaries/93027_Chapter_1_Deception_The_Basics.pdf

Clarke, R. A. and Knake, R. (2010) Cyber War: The Next Threat to National Security and What to Do About It. New York: Ecco.

Crawford, E., Bobrow, A., Sun, L., Joshi, S., Vijayan, V., Blacksell, S., Venugopalan, G. and Tensmeyer, N. (2023) 'Cyberbiosecurity in high-containment laboratories', Frontiers in Bioengineering and Biotechnology, 11, p. 1240281. Available at: https://doi.org/10.3389/fbioe.2023.1240281

Cunliffe, K.S. (2021) 'Hard target espionage in the information era: New challenges for the second oldest profession', Intelligence and National Security, 36(7), pp. 1018–1034. Available at: https://doi.org/10.1080/02684527.2021.1947555

Diederich, S., & Eschbaumer, M. (2025). More similar than different: A comparison of human and veterinary maximum containment facilities. Advances in Virus Research, 122, 61–77. https://doi.org/10.1016/bs.aivir.2025.05.001

dos Santos, D. (2019) Sabotaging common IoT devices in smart buildings by exploiting unencrypted protocols. Forescout Research Blog, 30 July. Available at: https://www.forescout.com/blog/sabotaging-smart-building-iot-devices-using-unencrypted-protocols/ (Accessed: 15 April 2026).

ECAM Technologies Corp. (2025) *Define surveillance camera: A complete guide*. Available at:https://ecam.com/security-blog/define-surveillance-camera-a-complete-guide (Accessed: 15 April 2026).

Elgabry, M., 2023. Biocrime, the Internet-of-Ingestible-Things and Cyber-Biosecurity. In Cyberbiosecurity: A New Field to Deal with Emerging Threats (pp. 135-146). Cham: Springer International Publishing.

Flock exposed its AI-powered cameras to the internet. We tracked ourselves', *404 Media*, 22 December. Available at: https://www.404media.co/flock-exposed-its-ai-powered-cameras-to-the-internet/ (Accessed: 15 April 2026).

Frontiers in Ecology and Evolution (2024) 'Article 1359201', Frontiers in Ecology and Evolution. Available at:https://www.frontiersin.org/journals/ecology-and-evolution/articles/10.3389/fevo.2024.1359201/full (Accessed: 6 January 2026).

George, A.M. (2019) 'The national security implications of cyberbiosecurity', Frontiers in Bioengineering and Biotechnology, 7, p. 51. Available at: https://doi.org/10.3389/fbioe.2019.00051

Guo, Z., 2025. *Building trustworthy computer vision: adversarial techniques for robustness assessment and misuse prevention* (Doctoral dissertation, The University of St Andrews).

Haley, P. and Burrell, D.N. (2025) 'Artificial intelligence driven criminal and national security threats in biosecurity, biotechnology, and bio-cybersecurity', RAIS Journal for Social Sciences, 9(1), pp. 52–72.

Henderson, S. (2023). Creativity and morality in deception. In H. Kapoor & J. C. Kaufman (Eds.), Creativity and Morality (pp. 101–124). https://deceptionbydesign.com/wp-content/uploads/2023/11/Henderson-2023-Creativty-and-Morality-in-Deception-Preprint.pdf

Herodotou, S. and Hao, F. (2023) 'Spying on the Spy: Security Analysis of Hidden Cameras', in Li, S., Manulis, M. and Miyaji, A. (eds.) Network and System Security: 17th International Conference, NSS 2023, Canterbury, UK, August 14–16, 2023, Proceedings. Cham: Springer, pp. 345–362. doi: 10.1007/978-3-031-39828-5_19.

Intel (n.d.) 2.4 GHz vs 5 GHz wireless. Available at:https://www.intel.com/content/www/us/en/products/docs/wireless/2-4-vs-5ghz.html (Accessed: 6 January 2026).

James, A., Potter, L. and Palmer, X.L., 2025, June. Understanding Cybersecurity Threats to Implantable Medical Devices: A Review. In *European Conference on Cyber Warfare and Security* (pp. 230-240). Academic Conferences International Limited.

Johns Hopkins Applied Physics Laboratory (n.d.) APL creates system to detect digital video tampering. Available at:https://www.jhuapl.edu/news/news-releases/030926-johns-hopkins-apl-creates-system-detect-digital-video-tampering (Accessed: 6 January 2026).

Ju, X., Chen, Y., Li, Z. and Han, B. (2025) 'Detection and localization of hidden IoT devices in unknown environments based on channel fingerprints', Big Data and Cognitive Computing, 9(8), p. 214. Available at: https://doi.org/10.3390/bdcc9080214.

Kalbo, N., Mirsky, Y., Shabtai, A. and Elovici, Y. (2020), *The security of IP-based video surveillance systems*, Sensors, 20(17), p. 4806. Available at:https://doi.org/10.3390/s20174806

Kaufman, E.K., Adeoye, S. and Batarseh, F.A., 2023. Leadership for cyberbiosecurity: The case of Oldsmar water.

Korada, L., 2024. Data Poisoning-What Is It and How It Is Being Addressed by the Leading Gen AI Providers. *European Journal of Advances in Engineering and Technology*, *11*(5), pp.105-109.

Kumar, H., Mishra, K., Awasthi, K., Gautam, K. and Kumar, R. (2026) 'Trinetra: A three-tier multi-modal detection system for hidden spy cameras and microphones using IR sensing, computer vision, and network traffic analysis', in 2026 International Conference on Computing, Sciences and Communications (ICCSC). IEEE. Available at: https://doi.org/10.1109/ICCSC67078.2026.11468605 .

Leath, M. (2025) Password to Louvre's video surveillance system was 'Louvre', according to employee. ABC News, 5 November. Available at: https://abcnews.com/International/password-louvres-video-surveillance-system-louvre-employee/story?id=127236297

Mirsky, Y., Mahler, T., Shelef, I. and Elovici, Y., 2019. {CT-GAN}: Malicious tampering of 3d medical imagery using deep learning. In *28th USENIX Security Symposium (USENIX Security 19)* (pp. 461-478).

Mo, Y., Wu, D., Wang, Y., Guo, Y. and Wang, Y., 2022. When adversarial training meets vision transformers: Recipes from training to architecture. *Advances in Neural Information Processing Systems*, *35*, pp.18599-18611.

Morrison, M.I., 2018. Info-topia: Postcolonial cyberspace and artificial intelligence in TRON: Legacy and Nalo Hopkinson's Midnight Robber. *Journal of Postcolonial Writing*, *54*(2), pp.161-173.

Naik, D., Naik, I. and Naik, N., 2025. Weaponising Generative AI Through Data Poisoning: Analysing Various Data Poisoning Attacks on Large Language Models (LLMs) and Their Countermeasures. *Authorea Preprints*.

National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg, MD: NIST. Available at: https://doi.org/10.6028/NIST.CSWP.29

NuAire, Inc. (2015) General camera information and use for NuAire biological safety cabinets (BSC) and isolators. Technical Bulletin GTB00276. Available at: https://nuaire.com/resources/general-camera-information-and-use-with-isolators-and-biosafety-cabinets-bulletin-general

Potter, L. and Palmer, X.L., 2023. Mission-aware differences in cyberbiosecurity and biocybersecurity policies: Prevention, detection, and elimination. In Cyberbiosecurity: A new field to deal with emerging threats (pp. 37-69). Cham: Springer International Publishing.

Potter, L. and Palmer, X.L., 2024. Social Murder in Another Century: Technologies That Enable Misinformation to Instigate Assault. Journal of Information Warfare, 23(4).

Potter, L., Ayala, O. and Palmer, X.L., 2021, February. Biocybersecurity: A converging threat as an auxiliary to war. In *ICCWS 2021 16th international conference on cyber warfare and security* (p. 291).

Potter, L., Shetty, S., Karahan, S. and Palmer, X.L., 2024. Biocybersecurity and applications of predictive physiological modelling. *International Journal of System of Systems Engineering*, *14*(4), pp.349-361.

Potter, L., Westberry, C. and Palmer, X.L., 2025, March. An Overview of Video Game Biometrics Collection and Considerations for Cyberbiosecurity. In *Proceedings of the 19th International Conference on Cyber Warfare and Security*. Academic Conferences and publishing limited.

Powell, E., Akogo, D., Potter, L. and Palmer, X.L., 2021, October. Co-leadership and cross-pollination of university and DIY bio spaces: an exploration in consideration of Biocybersecurity. In Proceedings of the Future Technologies Conference (pp. 610-621). Cham: Springer International Publishing.

Prasad, N., Diro, A., Warren, M. and Fernando, M. (2025) 'A survey of cyber threat attribution: Challenges, techniques, and future directions', Computers & Security, 157, p. 104606. Available at: https://doi.org/10.1016/j.cose.2025.104606

Pravin, A., Jacob, T.P., Prasad, K.M., Judgi, T. and Srinivasan, N. (2022) 'Efficient framework for hidden camera detection & jamming using IoT', in 2022 6th International Conference on Trends in Electronics and Informatics (ICOEI). IEEE. Available at: https://doi.org/10.1109/ICOEI53556.2022.9776943.

Purnell, A., Barnett, M., Potter, L. and Lewis-Palmer, X., 2025, June. Wearable Smart Devices: Innovations Through AI and Cyberbiosecurity Threats. In *European Conference on Cyber Warfare and Security* (pp. 538-546). Academic Conferences International Limited.

Qualia Bio (n.d.) BSL-4 security: Safeguarding high-containment labs. Available at:https://qualia-bio.com/blog/bsl-4-security-safeguarding-high-containment-labs/ (Accessed: 6 January 2026).

Racicot, M., Cardinal, A.M., Tremblay, D. and Vaillancourt, J.P. (2022) 'Technologies monitoring and improving biosecurity compliance in barn anterooms', Frontiers in Veterinary Science, 9, 1005144. Available at:https://www.frontiersin.org/journals/veterinary-science/articles/10.3389/fvets.2022.1005144/full (Accessed: 6 January 2026).

Ray, P.P., 2025. A Review on Vibe Coding: Fundamentals, State-of-the-art, Challenges and Future Directions. *Authorea Preprints*.

Reed, J.C. and Dunaway, N., 2019. Cyberbiosecurity implications for the laboratory of the future. *Frontiers in bioengineering and biotechnology*, *7*, p.182.

Reyes, F. (2025) 'Ben Jordan exposes severe security vulnerabilities in Flock surveillance cameras', Privacy Guides, 17 November. Available at: https://www.privacyguides.org/news/2025/11/17/ben-jordan-exposes-severe-security-vulnerabilities-in-flock-surveillance-cameras/

Researchers replace IP camera feed with fake footage. Available at:https://www.securityweek.com/researchers-replace-ip-camera-feed-fake-footage/ (Accessed: 6 January 2026).

Seipel, B. (2025) The Louvre used its own name as a password. Here's what to learn from it. McAfee Blog, 5 November. Available at: https://www.mcafee.com/blogs/security-news/the-louvre-used-its-own-name-as-a-password-heres-what-to-learn-from-it/ (Accessed: 15 April 2026)

Singh, S. and Dhumane, A. (2025) 'Unmasking digital deceptions: An integrative review of deepfake detection, multimedia forensics, and cybersecurity challenges', *MethodsX*, 15, p. 103632. Available at:https://doi.org/10.1016/j.mex.2025.103632

Skyforest, Z. (2025) Simple device can freeze Wi-Fi camera feeds. Hackaday, 1 November. Available at: https://hackaday.com/2025/11/01/simple-device-can-freeze-wi-fi-camera-feeds/ (Accessed: 15 April 2026).

Stephen, S., Alexander, K., Potter, L. and Palmer, X.L., 2023. Implications of cyberbiosecurity in advanced agriculture.

Stephen, S., Palmer, X., Potter, L. and Ruffin, D., 2024. Securing agricultural systems against the threat of misinformation. Journal of the ASABE, p.0.

Tayfor, N.B., Rashid, T.A., Qader, S.M., Hassan, B.A., Abdalla, M.H., Majidpour, J., Ahmed, A.M., Ali, H.M., Aladdin, A.M., Abdullah, A.A. and Shamsaldin, A.S. (2025) 'Video forgery detection for surveillance cameras: A review', arXiv preprint, arXiv:2505.03832. Available at:https://arxiv.org/abs/2505.03832 (Accessed: 6 January 2026).

Vukicevic, A.M., Petrovic, M., Milosevic, P., Peulic, A., Jovanovic, K. and Novakovic, A. (2024) 'A systematic review of computer vision-based personal protective equipment compliance in industry practice: Advancements, challenges and future directions', Artificial Intelligence Review, 57(12), p. 319.

Winsor, A., 2023. Ballroom Refuses to Burn: Exploitation versus Community Education in Documentaries about Voguing and the Ballroom Community. *Nota Bene: Canadian Undergraduate Journal of Musicology*, *16*(1), pp.74-92.

Zhao, Y., Zhu, H., Liang, R., Shen, Q., Zhang, S. and Chen, K., 2019, November. Seeing isn't believing: Towards more robust adversarial attack against real world object detectors. In *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security* (pp. 1989-2004).