The American Journal of Political Science Law and Criminology
ISSN 2693-0803 | Open Access

TYPE Original Research
PAGE NO. 206-215
DOI 10.37547/tajpslc/Volume07Issue05-22

Integrated Policing in Critical Infrastructure Protection: Bridging Intelligence and Field Operations

Ahmed Abuelfadl Ahmed Haridy

Police Officer, The Ministry of Interior of Egypt New Brunswick, NJ

OPEN ACCESS

SUBMITTED 11 March 2025
ACCEPTED 05 April 2025
PUBLISHED 24 May 2025
VOLUME Vol.07 Issue05 2025

CITATION

Ahmed Abuelfadl Ahmed Haridy. (2025). Integrated Policing in Critical Infrastructure Protection: Bridging Intelligence and Field Operations. The American Journal of Political Science Law and Criminology, 7(05), 206–215. https://doi.org/10.37547/tajpslc/Volume07Issue05-22.

Abstract: This article examines contemporary challenges in protecting critical infrastructure, driven by the rapid growth of "hybrid" cyber-physical attacks and chronic gaps in intelligence sharing between strategic analysts and field response teams. The study aims to analyze existing legal and regulatory frameworks in the United States and the European Union, assess the technological capabilities of a "digital twin" of CNI assets, and identify key barriers to translating threat analyses into on-site operational actions. The relevance of this work is underscored by statistics from Europol, KnowBe4, Check Point, and NERC reporting hundreds of millions of cyberattacks and thousands of physical incidents per year, as well as high-profile cases such as Colonial Pipeline and Moore County, which exposed critical communication failures between the intelligence community and asset operators. The novelty of the research lies in an interdisciplinary comparison of the paradigms of problem-oriented policing, intelligence-led policing, and the all-hazards approach with current technological and regulatory realities, including ISA/IEC 62443 standards, the Zero Trust protocol, and the STIX 2.1 format for alert exchange. Thus, the main technical and legal barriers to bringing intelligence data into field operations have been pinpointed, and the efficacy of a sync exchange approach has been demonstrated

through cases from the Port of Rotterdam, Capital Shield program, and Cyberabwehr Bayern, where timely delivery of analytics saw average response times go from days to hours. It proposes unifying procedures and exchange protocols as a foundation for increased coordination among varied services in critical infrastructure protection. This work will benefit developers of state security infrastructure, cyber and physical protection specialists, and fusion-center analysts.

Keywords: critical infrastructure, hybrid threats, intelligence data, field response, legal and regulatory frameworks, digital twin, Zero Trust, STIX 2.1, intelligence-led policing.

Introduction: Hybrid threats are not simply a combination of a cyberattack and sabotage; today, they constitute a resilient ecosystem in which state intelligence services employ criminal networks as proxies to sabotage pipelines, ports, and power grids, while formally denying involvement. In its annual threat assessment, Europol highlights a sharp rise in such "tandem" operations: by 2025, the number of sabotage-type incidents in the EU had grown so significantly that the agency speaks, for the first time, of a "shadow coalition" between criminal groups and foreign intelligence services targeting critical infrastructure [1].

The magnitude of the problem is measured in hundreds of millions of intrusion attempts. Analysis [2] records more than 420 million attacks on CNI assets over just 12 months (January 2023–January 2024)—equivalent to 13 attacks per second and representing a 30% increase over 2022; since 2020, the weekly number of attacks on energy companies has quadrupled. Check Point Research reports a 70% surge in the United States alone: in 2024, the average reached 1,162 attacks per utility company versus 689 the previous year [3]. Meanwhile, the NERC regulator logs roughly 60 new vulnerabilities in the power system each day: by the end of 2024 there were 23–24 thousand, up from 21–22 thousand a year earlier, while physical attacks on substations remain at about 2 800 cases, of which 3% result in actual outages [4]. Tactically, a cyber penetration into SCADA enables precise targeting, and a subsequent physical strike ensures disconnection.

Against this backdrop, the gap between strategic intelligence and tactical response is especially acute. A textbook example is the attack on Colonial Pipeline [5]. Within hours, the FBI forwarded data to CISA. Yet, the company did not liaise directly with the agency: analysts obtained technical details only via third-party channels, forcing field teams to operate blindly, lengthening the pipeline's downtime, and triggering a fuel crisis on the US East Coast. This information vacuum between the federal level and the asset operator demonstrates that gathering intelligence does not automatically translate into actionable instructions for first responders.

A similar failure occurred in the physical domain. In December 2022, unknown assailants shot two distribution nodes in Moore County, North Carolina, leaving 45,000 households without power. The local sheriff acknowledged that the perpetrators "knew exactly where to shoot," while federal agencies joined the investigation only post hoc. As experts probed the attackers' motivations, repair crews spent five days restoring equipment, and the state governor spoke of a "qualitatively new level of threat" [6]. Again, the intelligence community collected extensive data on potential radicalization and target selection, yet transferring this analysis to district patrols and substation guards remained unregulated.

Thus, the quantitative surge in cyber-physical attacks and breakdown of qualitative information exchange constitute a dual challenge. The following sections examine the US and EU regulatory frameworks, the technological architecture of the CNI "digital twin," and propose an integrated IP-CIP model designed to "stitch" intelligence and field operations into a seamless cycle of detection, assessment, and immediate response.

MATERIALS AND METHODOLOGY

The study of an integrated policing approach to critical infrastructure protection is grounded in an interdisciplinary analysis of twenty-seven sources. The primary empirical foundation comprised Europol's annual reports on hybrid threats [1], the KnowBe4 report on cyberattacks against CNI assets [2], Check Point Research studies on the escalation of attacks on US utility networks [3], and NERC statistics on new vulnerabilities and physical incidents in the power system [4]. To illustrate practical rifts between analytics

and response, the case studies of Colonial Pipeline [5] and the Moore County, North Carolina incident [6] were examined.

Methodologically, the research proceeded through several complementary stages. First, a comparative analysis of quantitative data—from the number and growth rates of CNI attacks to grid vulnerability metrics—was conducted to gauge the scale of current risks and trace the dynamics of cyber-physical attack integration. Second, a systematic review of classical policing paradigms was performed: problem-oriented policing [8], intelligence-led policing and the evolution of the fusion center network in the United States [9], and the all-hazards approach to civil protection [10], aiming to compare their strengths and limitations in addressing novel threat types. The third stage entailed a legal and regulatory examination: analysis of National Security Memorandum NSM-CIP and the updated DHS "Fusion Center Foundational Guidance" on intelligence sharing with CNI operators [11,9], JCDC priorities for joint cyber- and physical defense [12], EU Directive 2022/2557 and the ProtectEU strategy [13,14], as well as Europol's programme documents on expedited interstate data exchange [14]. Special attention was given to safety standards (ISA/IEC 62443) and Zero Trust protocols for secure alert delivery in STIX 2.1 format [16,17].

Finally, a cross-analysis was performed to assess the integrated IP-CIP model: juxtaposing digital-twin characteristics (market size, growth trajectories, and architectural requirements [15]) with the analytical, tactical, and regulatory components outlined above. This enabled the formulation of a closed loop—Detect, Assess, Respond, Feedback—where protocol efficacy is measured by reducing mean time to detect (MTTD) and mean time to respond (MTTR) from days to hours.

RESULTS AND DISCUSSION

The perimeter security model, which coalesced in the 1960s around nuclear facilities and large power plants, consisted of high fences, low-resolution video cameras, and guard posts. Reliance was placed on physical isolation and, as the U.S. Department of Energy report acknowledges, on "security through obscurity": each plant employed a proprietary SCADA stack, so it was assumed attackers would find it challenging to prepare an effective strike [7]. This approach was sufficient while threats remained linear and localized, but it offered no solution when an attack unfolded simultaneously in both the cyber and physical domains.

In the 1970s, the problem of "blind" security prompted law enforcement to reevaluate analytically. The concept of problem-oriented policing (POP), articulated by Herman Goldstein, proposed viewing each incident as a symptom of offender behavior and seeking the "root cause," rather than merely patrolling a perimeter. While this method yielded strong results in combating street crime, it lacked the tools to integrate with CNI technological systems: officers received statistics only retrospectively and seldom exchanged data with facility technical staff.

After the September 11, 2001, attacks, focus shifted to intelligence-led policing (ILP). First institutionalized in the United Kingdom and detailed in the BJA guide "The New Intelligence Architecture," ILP advocated building operations around analytical products rather than patrol schedules [8]. In the U.S., ILP's development was accompanied by creating a network of fusion centers: by 2008, about fifty nodes had been deployed, funded with over USD 130 million from the federal budget [9].

Concurrently, the all-hazards approach took hold in civil protection, requiring preparedness for any threat, from hurricanes to cyberattacks. This doctrine broadened the threat spectrum but was criticized for excessive generality, complicating prioritization and increasing the risk of overreach in citizens' data collection [10]. Thus, by mid-2010s, a triadic landscape had emerged: POP provided qualitative local analysis, ILP delivered a strategic overview, and the all-hazards approach enabled comprehensive planning—yet none offered a streamlined channel capable of providing real-time intelligence to a mobile response team at the asset.

The rationale for transitioning to an integrated IP-CIP model arises from this unfilled gap. IP-CIP adopts ILP's centralized risk-assessment system, POP's focus on a specific asset and its socio-technical context, and the all-hazards approach's capacity to address a broad threat spectrum. Its novel layer is the digital twin of the CNI, into which SCADA telemetry, fusion-center data, and patrol reports converge. This architecture enables two-way communication: strategy is informed by big data, while tactics update strategy via a feedback channel

within minutes, thus eliminating the historical disconnect between analysts and first responders.

In the United States, a unified critical-infrastructure protection framework was established by the National Security Memorandum on Critical Infrastructure Protection (NSM-CIP), signed on 30 April 2024; the document for the first time obligates the intelligence community to transmit relevant data directly to asset owners and operators, and requires each of the 16 CNI sectors to submit annual risk-management plans compatible with DHS assessment matrices [11]. Further to the memorandum, the Department of Homeland Security in the same year updated its "Fusion Center Foundational Guidance": annexes now describe a dedicated analytical module for CNI protection and a minimum set of procedures that states must implement to ensure end-to-end alarm transmission from fusion centers to field officers. Simultaneously, CISA elevated the Joint Cyber Defense Collaborative (JCDC) to "operational hub" status; its 2024 priorities explicitly mandate that all joint-defense scenarios cover OT segments and account for "new risks arising from the deployment of cloud-based SCADA solutions" [12]. Thus, the U.S. regulatory continuum from strategic to tactical levels establishes a single line of authority, while imposing stringent requirements on the data-recipient systems' technical compatibility—a challenge for regional operators managing heterogeneous device portfolios.

Within the European Union, Directive (EU) 2022/2557 (CER) occupies the central role, obligating Member States by October 2024 to adopt national resilience strategies and conduct periodic stress tests across energy, transport, water, and digital infrastructure sectors [13]. Politically, the directive is supplemented by the ProtectEU strategy, presented on 1 April 2025, which ranks CNI protection and hybrid-threat countermeasures as the EU's second most crucial internal-security priority. Europol serves as the practical "node" for these efforts: in its 2024–2026 programme document, the agency announced the expansion of its analytical platform for accelerated intelligence sharing with national centers and sectoral SOCs, particularly in energy and maritime port domains [14]. This configuration enables horizontal exchange between Member States but burdens incident-classification standardization, as each country may introduce additional secrecy levels.

Legal conflicts impede synchronization of the U.S. and EU schemes. The EU's General Data Protection Regulation (GDPR) mandates minimization and localization of personal data. In contrast, the U.S. CLOUD Act grants American authorities the right to request data from cloud providers irrespective of physical storage location. Both regimes apply concurrently when a CNI operator employs a transnational cloud SOC, creating legal uncertainty and potential delays in log transmission, which are critical for rapid response. In light of the growing number of cyber-physical attacks, this "jurisdictional interface" becomes not merely a legal debate but a recovery-time risk factor. The integrated IP-CIP model proposed herein assumes that technical data-exchange protocols must be complemented by transparent bilateral agreements on jurisdiction and data-classification schemes, so that strategic intelligence in the U.S. can interface without delay with tactical response in Europe, and vice versa.

The digital twin underpins the integrated architecture: a synchronous model of SCADA equipment and the field-sensor layer, overlaid on a 3D-GIS site map. According to [15], the global market for such solutions reached USD 24.97 billion in 2024, with a compound annual growth rate of 34.2%, as illustrated in Figure 1.

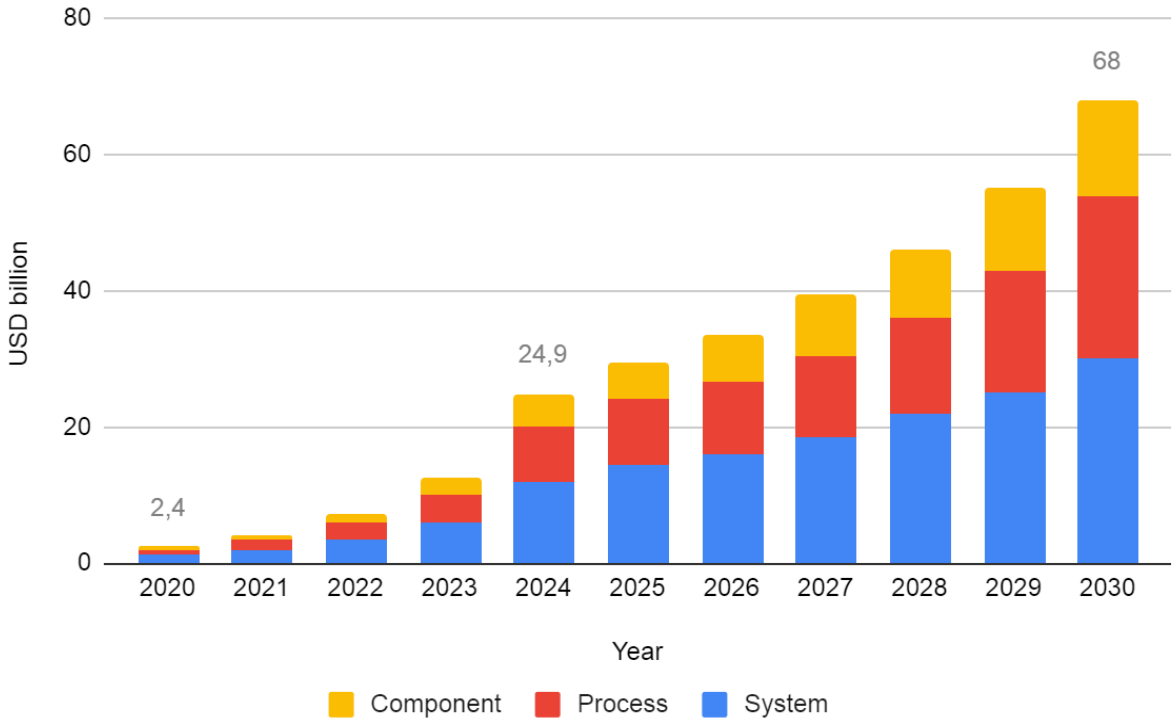

Fig. 1. Digital Twin Market Growth [15]

Data streams converge in the fusion center. The updated "Fusion Center Foundational Guidance" requires each state to deploy a specialized analytical module for critical infrastructure and issue alerts in STIX 2.1 format via an MQ bus directly to officers' mobile terminals. Transmission follows a Zero Trust architecture codified in ISA/IEC 62443, which prescribes zone-conduit segmentation of OT networks and device-authentication procedures [16].

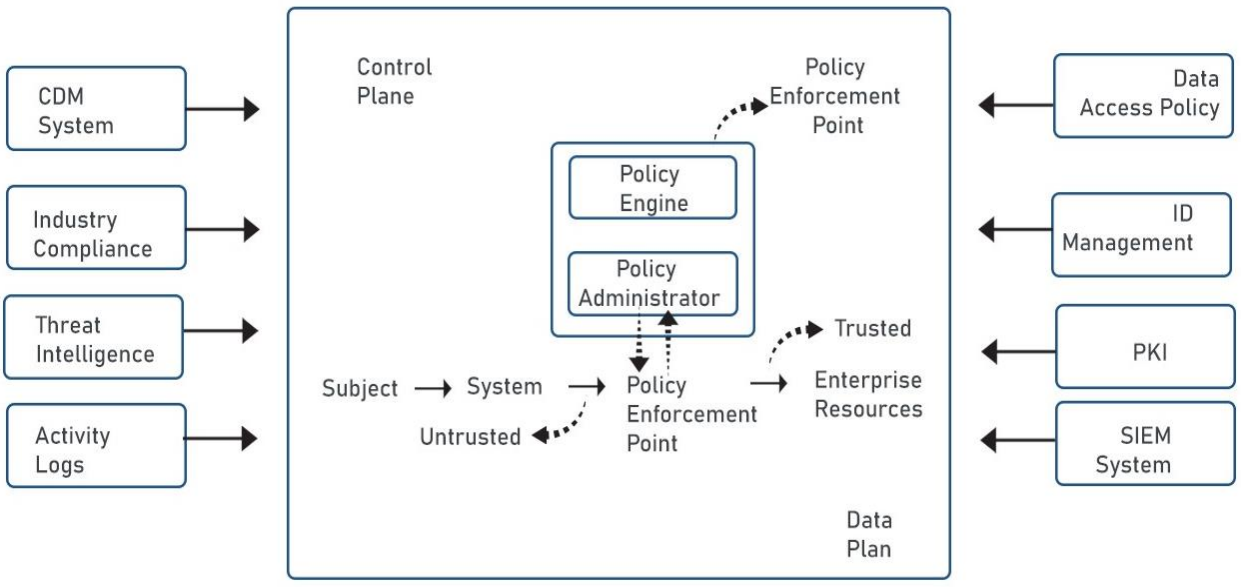

Fig. 2. Zero Trust Framework [17]

The "Secure-by-Design" principle reinforces the security layer, an initiative supported by major vendors and coordinated by CISA. Concurrently, the JCDC-2024 program prioritizes OT segments and small operators to "raise the baseline cybersecurity level of critical infrastructure."

The IP-CIP conceptual framework organizes technologies into a Detect–Assess–Respond–Feedback cycle. The digital twin detects an anomaly; the fusion center enriches it with external intelligence in seconds and, via 5G MEC or a backup satellite link, forwards an alert package to the response team, comprising a "twin" officer, the facility engineer, and private security if required. After incident resolution, video and action logs return to analytics to refine the detection models. Core metrics are mean time to detect (MTTD) and mean time to respond (MTTR). For comparison, median dwell time remains nine days according to [18], dropping to five days in internally discovered cases. IP-CIP's objective is to shift MTTD and MTTR from days to hours by creating a closed loop in which intelligence and field operations continuously feed one another, thereby closing the historical gap between strategic analysis and on-site tactics.

The sharp increase in cyber-physical load on operational networks renders algorithmic speed a critical resource: a report [19] indicates that ransomware incidents targeting the industrial sector rose to 1,693, an 87% year-over-year increase (Figure 3).

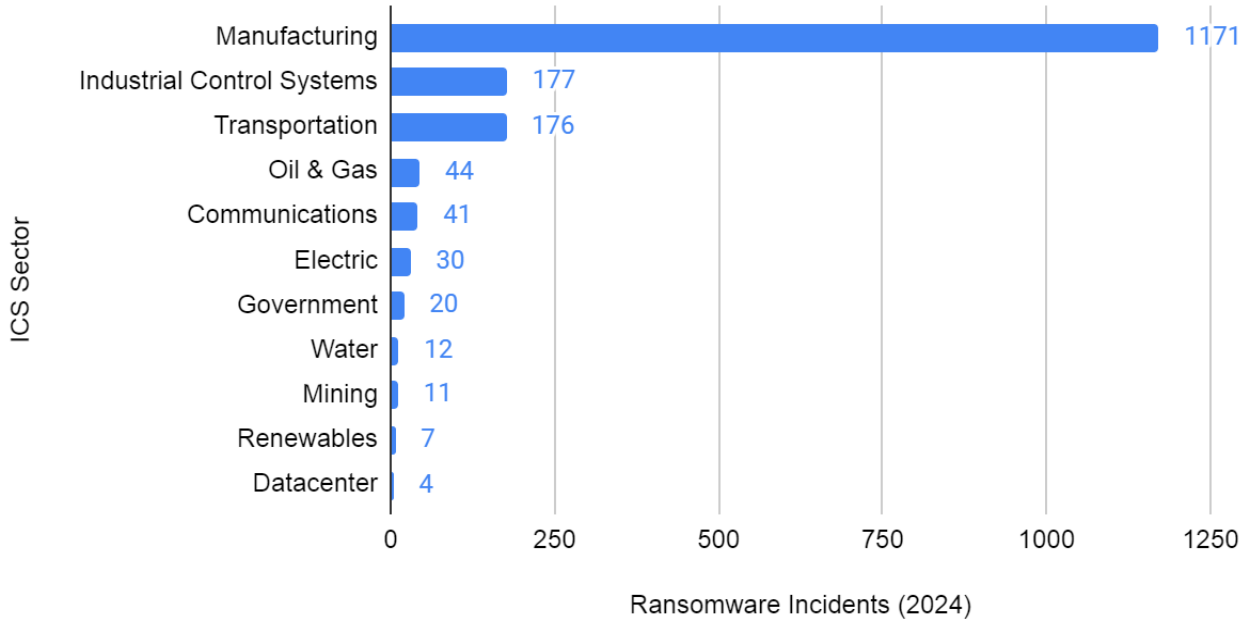

Fig. 3. Ransomware Incidents in Different Sectors [19]

To avoid being overwhelmed by telemetry, major operators are adopting machine-learning ensembles that detect deviations in Modbus or DNP3 traffic and immediately cross-check them against physical-sensor readings; in pilot projects, these models reduce average detection time to seconds and yield graph-NLP data capable of forecasting near-term attacks by linking APT-group TTPs with vulnerable assets.

The practical utility of AI depends directly on human trust in the field. A study on explainable AI in cybersecurity demonstrates that adding interpretable layers to detectors reduces false alarms and increases operators' willingness to act on system recommendations, because the precise features driving an algorithm's conclusion become visible [20]. Transparency, rather than maximum accuracy, thus becomes the principal condition for fusion-center intelligence to translate into patrol-level action within minutes. Even with ideal protocols, personnel training remains decisive. The concept of the "twin officer," combining cyber-analyst and tactical-team skills, receives financial support via the State & Local

Cybersecurity Grant Program. In 2024 alone, USD 279.9 million was allocated for training and VR simulators, and applications submitted by CNI-operator consortia receive priority [21]. Thus, predictive analytics, standardized exchange channels, and skilled human resources converge into a unified operational fabric, eliminating the longstanding divide between intelligence and on-site response.

Three case studies illustrate how the intelligence–field principle functions across CNI scales. In the Port of Rotterdam, the adoption of unmanned aerial patrols served as a catalyst: a U-Space prototype enables the port dispatcher to task UAVs in real time to coordinates obtained from SCADA sensors and AIS messages, reducing the incident detection–confirmation cycle almost to flight time—the Avy Aera network automatically launches 30 seconds after trigger and provides high-resolution stabilized video to the inspector before a patrol boat can cast off [22]. A by-product was logistical optimization: by integrating telemetry streams with the PortXchange platform, average container-ship idle time at berth fell by 30%, indicating that a unified digital picture benefits security and efficiency [23].

"Capital Shield," the District of Columbia's upgraded fusion-center configuration, illustrates how DHS regulations become a technical bus. Operating 24/7, the center integrates situational analysts, the transport-dispatch node, and federal officers, enabling immediate correlation of cyber and physical anomalies at the capital's energy and transport assets [24]. Since 2024, most cyber indicators arrive via CISA's AIS-2.0 service, and the routing algorithm automatically packages them into machine-readable formats for police mobile terminals, eliminating prior information loss when over half of the 55,609 active HSIN accounts went unused for months [25].

The Bavarian power grid demonstrates a regional integration variant. The Cyberabwehr Bayern platform unites the police directorate, the Office for the Protection of the Constitution, the Landesamt für Sicherheit in der IT, and network operators to form a unified cyber "Lagebild," which automatically feeds duty shifts in the NOCs and SOCs of the state's largest distribution networks [26]. The BSI report confirms relevance: in the 12 months to June 2023, one-third of Germany's 99 energy-sector incidents occurred in Bavaria, prompting the region to accelerate end-to-end event handling from substation detector to Landeskriminalamt response team [27]. The outcome was the establishment of standard procedures. After the SOC's automated anomaly correlator generates an electronic "Steckbrief," it is transmitted promptly to the Vorgangsbearbeitung police system and technical telemetry, which only NOC engineers can mitigate. This regime minimizes coordination delays and cements the police's role as coordinator rather than network-equipment operator.

Comparison reveals the typical benefits and constraints of the integrated model. The Dutch port achieved the most tremendous responsiveness gains through "sensor–drone" automation, but practice transferability is limited by airspace regulation and capital intensity. The U.S. case underscores that, without a uniform data format, even the most advanced federated infrastructure stalls: the principal barrier proved not to be technology but user habits. The Bavarian example highlights the importance of a legal framework: platform-based intelligence exchange is feasible only where police, regulators, and private operators have pre-agreed on real-time decision-making responsibilities.

These observations confirm the article's thesis: an integrated policing model becomes viable when tactical communication channels, legal regulations, and data architecture are designed as a cohesive whole, rather than retrofitted onto one another post hoc.

CONCLUSION

This study has demonstrated the pressing need to bridge the historical gap between strategic intelligence and tactical response in critical-infrastructure protection. Combining cyberattacks with physical sabotage, contemporary hybrid threats create a complex ecosystem in which criminal networks and state intelligence services may coordinate as "shadow coalitions." The scale of these threats is evidenced by statistics reporting hundreds of millions of intrusion attempts and the daily emergence of dozens of new vulnerabilities, underscoring the limited efficacy of traditional perimeter security models and fragmented analytical and data-exchange approaches.

The integrated IP-CIP model proposed herein merges the strengths of problem-oriented policing, intelligence-led policing, and the all-hazards approach, augmenting them with a digital twin of the asset. This architecture delivers a continuous Detect–Assess–Respond–Feedback cycle. SCADA telemetry, fusion-center analytical products, and field-team reports converge into a single system and are instantly relayed to operational units. Using the Zero Trust protocol and ISA/IEC 62443 standard ensures secure STIX 2.1 alert exchange; machine learning and explainable AI technologies will minimize detection time and false positives.

One significant factor for successful IP-CIP implementation is having a strong regulatory body and harmonizing steps at the international level. The U.S. NSM-CIP and up-to-date Fusion Center Foundational Guidance ensure intelligence is sent straight to CNI owners. Similarly, EU Directive 2022/2557 and the ProtectEU strategy facilitate horizontal information sharing among Member States. Yet differences between GDPR and CLOUD Act laws clearly show the need for bilateral agreements on matters of jurisdiction and data-classification schemes to ensure operational agility and legal clarity when working cross-border.

The real-world examples—from drone flights in the Rotterdam port to linking Capital Shield with the Cyberabwehr Bayern platform at a regional level—show that combining tech, clear comms channels, and expert people can reduce the time taken to find out about an issue and act on it from days to hours. Thus, the IP-CIP integrated policing model constitutes a viable operational framework for critical-infrastructure protection, wherein strategic analytics and field operations function as interconnected links in a unified process.

REFERENCES

L. O'Carroll, "Russia using criminal networks to drive increase in sabotage acts, says Europol," *The Guardian*, Mar. 18, 2025. https://www.theguardian.com/technology/2025/mar/18/russia-criminal-networks-drive-increase-sabotage-europol (accessed Apr. 10, 2025).

A. Ribeiro and A. Ribeiro, "Critical infrastructure faces 30 percent surge in cyber attacks, KnowBe4 report highlights," *Industrial Cyber*, Aug. 28, 2024. https://industrialcyber.co/critical-infrastructure/critical-infrastructure-faces-30-percent-surge-in-cyber-attacks-knowbe4-report-highlights/ (accessed Apr. 11, 2025).

S. Dareen and S. Vallari, "Cyberattacks on US utilities surged 70% this year, says Check Point," *Reuters*, Sep. 11, 2024. Accessed: Apr. 12, 2025. [Online]. Available: https://www.reuters.com/technology/cybersecurity/cyberattacks-us-utilities-surged-70-this-year-says-check-point-2024-09-11/

L. Kearney, "US electric grid growing more vulnerable to cyberattacks, regulator says," *Reuters*, Apr. 04, 2024. Accessed: Apr. 14, 2025. [Online]. Available: https://www.reuters.com/technology/cybersecurity/us-electric-grid-growing-more-vulnerable-cyberattacks-regulator-says-2024-04-04/

S. Schwartz, "CISA left in the dark during Colonial Pipeline's initial response," *Cybersecurity Dive*, May 12, 2021. https://www.cybersecuritydive.com/news/colonial-pipeline-ransomware-cisa-senate-hearing/600029/ (accessed Apr. 15, 2025).

S. Bernstein, "North Carolina electric grid shooter 'knew exactly what they were doing,' sheriff says," *Reuters*, Dec. 06, 2022. Accessed: Apr. 16, 2025. [Online]. Available: https://www.reuters.com/world/us/attack-north-carolina-electric-grid-new-level-threat-governor-says-2022-12-05/

"Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats," 2016. Available: https://www.energy.gov/sites/prod/files/2017/01/f34/Electric%20Grid%20Security%20and%20Resilience--Establishing%20a%20Baseline%20for%20Adversarial%20Threats.pdf

M. Peterson, "Intelligence-Led Policing: The New Intelligence Architecture," Bureau of Justice Assistance. Accessed: Apr. 17, 2025. [Online]. Available: https://www.ojp.gov/pdffiles1/bja/210681.pdf

R. Singel, "Feds Tout New Domestic Intelligence Centers," *Wired*, Mar. 20, 2008.

https://www.wired.com/2008/03/feds-tout-new-d/ (accessed Apr. 19, 2025).

A. Allen, "The All Hazards Approach To Emergency Planning, Explained" *AlertMedia*, Jan. 09, 2019. https://www.alertmedia.com/blog/all-hazards-approach/ (accessed Apr. 20, 2025).

"National Security Memorandum on Critical Infrastructure Security and Resilience | CISA," *CISA*. https://www.cisa.gov/national-security-memorandum-critical-infrastructure-security-and-resilience (accessed Apr. 21, 2025).

"2024 JCDC Priorities," *CISA*. https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative/2024-jcdc-priorities (accessed Apr. 21, 2025).

Directive - 2022/2557. 2022. Accessed: Apr. 22, 2025. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng

"Europol Programming Document," Europol, 2024. Accessed: Apr. 24, 2025. [Online]. Available: https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Programming_Document_2024-2026.pdf

"Global Digital Twin Market Size & Share Report," *Grand View Research*, 2023. https://www.grandviewresearch.com/industry-analysis/digital-twin-market (accessed Apr. 26, 2025).

International Society of Automation, "ISA/IEC 62443 Series of Standards," *ISA*, 2024. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards (accessed Apr. 27, 2025).

"What Is Zero Trust Security?" *Spiceworks*, Oct. 22, 2021. https://www.spiceworks.com/it-security/network-security/articles/zero-trust-security/#lg=1&slide=0 (accessed Apr. 28, 2025).

A. Chuvakin, "Reading the Mandiant M-Trends 2024," *Medium*, May 2024. https://medium.com/anton-on-security/reading-the-mandiant-m-trends-2024-acb3208add80 (accessed Apr. 30, 2025).

"Dragos's 8th Annual OT Cybersecurity Year in Review Is Now Available," *Dragos*, Feb. 25, 2025. https://www.dragos.com/blog/dragos-8th-annual-ot-cybersecurity-year-in-review-is-now-available/ (accessed May 01, 2025).

I. H. Sarker, H. Janicke, A. Mohsin, A. Gill, and L. Maglaras, "Explainable AI for cybersecurity automation, intelligence and trustworthiness in digital twin: Methods, taxonomy, challenges and prospects," *ICT express*, vol. 10, no. 4, May 2024, doi: https://doi.org/10.1016/j.icte.2024.05.007.

"State and Local Cybersecurity Grant Program," *CISA*. https://www.cisa.gov/cybergrants/slcgp (accessed May 02, 2025).

"Avy's VTOL-in-a-box," *Avy*, 2024. https://avy.eu/technology (accessed May 02, 2025).

R. O'Dwyer, "Digital port data exchange trial reduces Rotterdam idle time by 30%," *Smart Maritime Network*, Jun. 03, 2020. https://smartmaritimenetwork.com/2020/06/03/digital-port-data-exchange-trial-reduces-rotterdam-idle-time-by-30 (accessed May 03, 2025).

"National Capital Region Threat Intelligence Consortium," *HSEMA*. https://hsema.dc.gov/DCFC (accessed May 05, 2025).

J. V. Cuffar, "OIG-24-62," Office of Inspector General, Sep. 2024. Accessed: May 06, 2025. [Online]. Available: https://www.oig.dhs.gov/sites/default/files/assets/2024-09/OIG-24-62-Sep24.pdf

J. Herrmann, "Cybersicherheit in Bayern 2022," Bayern, 2023. Accessed: May 06, 2025. [Online]. Available: https://www.stmi.bayern.de/assets/stmi/sus/datensicherheit/brosch%C3%BCre_cybersicherheit_in_bayern_2022.pdf

"Cybersecurity situation is tense to critical," *Bayern Innovativ*, 2024. https://www.bayern-innovativ.de/en/emagazine/detail/en/page/cybersecurity-situation-is-tense-to-critical (accessed May 07, 2025).