Lizut, R. (2025). Security challenges of IoT integration in national and state critical infrastructures. *Politics & Security, 13*(3), 82–94. Doi: 10.54658/ps.28153324.2025.13.3.pp.82-94

SECURITY CHALLENGES OF IOT INTEGRATION IN NATIONAL AND STATE CRITICAL INFRASTRUCTURES

Rafał Lizut
John Paul II Catholic University
Lublin, Poland
rafal.lizut@kul.pl
https://orcid.org/0000-0002-6067-1469

Abstract. *This investigation scrutinizes the incorporation of Internet of Things (IoT) systems within national infrastructures, accentuating both operational advantages and notable security challenges. It delves into the stratified architecture of IoT, underscoring vulnerabilities that emerge from device constraints, varied deployment environments, and inadequate cybersecurity practices. The examination addresses external threats such as distributed denial-of-service attacks, malware, and data manipulation, in conjunction with internal risks including insider threats and misconfigurations. The ramifications of these threats on critical infrastructure sectors, such as energy, transportation, and healthcare, are evaluated, with a focus on operational disruptions and economic impacts. Emergent defense strategies involving Software-Defined Networking and machine learning-based anomaly detection are assessed for their capability to bolster security posture. Furthermore, the role of national cybersecurity strategies and regulatory frameworks is analyzed, concentrating on multi-stakeholder coordination, legal measures, and adaptive governance to manage evolving risks. The findings highlight the imperative of integrating technical, organizational, and policy approaches to protect IoT-enabled critical systems and sustain national security resilience.*

Keywords: Internet of Things (IoT), Critical Infrastructure Protection, Cybersecurity, Distributed Denial-of-Service (DDoS), Malware and Data Manipulation.

1. INTRODUCTION

The progressive incorporation of Internet of Things (IoT) systems into national infrastructures presents considerable advantages in terms of both operational efficiency and situational awareness. By harnessing real-time data streams from an increasing array of connected devices, decision-makers are able to conduct more precise monitoring of environments such as transportation systems, energy grids, healthcare facilities, and industrial control systems.

These capabilities enhance the potential for early detection of incidents like equipment failures or environmental hazards, thus providing opportunities for intervention before issues escalate into significant crises. However, alongside these benefits comes a notable expansion of the attack surface accessible to adversaries. A major concern is that IoT devices, despite their functional and deployment diversity, frequently exhibit systemic security weaknesses. They are often developed under stringent cost and time-to-market constraints, prompting manufacturers to prioritize usability and compatibility features over stringent cybersecurity engineering (Group, 2018). Default configurations, inadequate integrity checks, and the absence of prompt firmware updates create persistent vulnerabilities, rendering these devices attractive targets for exploitation (Kudini, 2024).

In practice, these weaknesses not only jeopardize individual devices but also potentially serve as entry points into broader networks that vital services rely on. Threats manifest through various vectors. Externally, attacks encompass distributed denial-of-service (DDoS) campaigns using botnets composed of compromised IoT nodes, unauthorized access attempts by exploiting insecure APIs or interfaces, and targeted malware deployments intended to disrupt specific operational processes (Buiya et al., 2024). Data interception and manipulation may also occur when communications between IoT endpoints are neither properly encrypted nor authenticated.

Concurrently, internal risks, such as malicious insiders possessing extensive system knowledge or negligent administrative practices, can compromise even robust security architectures (Garcia-Morchon et al., 2019). This duality, characterized by external hostility coupled with internal vulnerability, renders the cybersecurity challenge particularly intricate. Connected IoT infrastructures supporting smart buildings or municipal services further exemplify these vulnerabilities. A compromised subsystem, such as an HVAC controller or alarm mechanism, can instigate cascading operational repercussions: triggering false alarms to divert responders, altering environmental controls to disrupt occupancy comfort, or compromising physical access management systems (Group, 2018).

When such systems become integrated with other critical assets such as data centers or emergency services networks, the potential exists for an attack to propagate across domains previously isolated from one another. In conjunction with technical vulnerabilities, privacy considerations add an additional layer of complexity. The aggregation of personally identifiable information (PII), including location records from connected vehicles or biometric data from medical wearables, constitutes a significant target for espionage or criminal exploitation (Al-Garadi et al., 2020). A breach involving these datasets poses risks of both direct harm to individuals and the erosion of public confidence in IoT-enabled services.

Concerns are particularly pronounced in healthcare contexts, where sensitive medical information flows between patient-facing devices and cloud platforms. For national security stakeholders, these scenarios concerning the exploitation of information cannot be disregarded. Strategic adversaries might leverage compromised IoT deployments for purposes of surveillance or disinformation. Information extracted from industrial sensors could disclose production patterns in sectors crucial to defense supply chains. Disruptions to grid-connected sensors or distributed generation units could result in significant impacts on the energy sector (Mohamed et al., 2023). These implications underscore the critical intersection between defending IoT systems and safeguarding broader critical infrastructure sectors. Emerging solutions such as Software-Defined Networking (SDN), when integrated into IoT architectures, show promise for enhancing control over dynamic network configurations and enabling automated policy enforcement to counteract specific threats (Oredola & Ashraf, 2024).

The centralization of control logic within SDN allows administrators to apply granular traffic filtering rules across diverse device fleets with greater agility compared to static configurations. Nonetheless, SDN controllers themselves remain valuable targets for attackers; absent appropriate protection measures, such as secure channel protocols and monitoring frameworks incorporating anomaly detection algorithms, adversaries could potentially manipulate them to orchestrate detrimental actions on a large scale. Furthermore, artificial intelligence-driven telemetry analysis represents another promising avenue for advancing threat detection within complex IoT ecosystems.

Machine learning pipelines trained on varied attack signatures can assist in distinguishing benign traffic anomalies from authentic intrusion attempts (El-Sofany et al., 2024). These models, which continuously adapt by utilizing streaming inputs from deployed IoT environments, may discern new patterns indicative of evolving attacker strategies. However, researchers emphasize that the accuracy of these models is significantly contingent upon the quality and comprehensiveness of the training datasets (Al-Garadi et al., 2020). The generation of datasets accurately reflecting real-world attacks presents significant challenges due to the diversity of incidents and the rapid emergence of new exploits. Systematically organized vulnerability reporting mechanisms serve as a crucial adjunct to automated defense systems. Facilitating the submission of detailed incident evidence by both internal teams and external actors, such as white-hat researchers, ensures that organizations can quickly triage credible threats and implement mitigations before incidents escalate further (Group, 2018).

This collaborative methodology enhances collective readiness, mitigating the risk of undetected vulnerabilities persisting due to prolonged detection cycles. Any discourse regarding the security of IoT deployments must integrate comprehensive risk assessments alongside privacy impact evaluations. Risk assessments categorize threats based on their likelihood and potential operational impact to prioritize mitigation efforts towards the most severe risks, while privacy impact evaluations ensure adherence to legal mandates concerning the handling of personally identifiable information (PII) and identify areas susceptible to data misuse (Garcia-Morchon et al., 2019).

Both evaluations provide structured foundations for the effective allocation of resources between preventative engineering measures and responsive capabilities. It is plausible that without enhanced standardization concerning secure development practices—such as default encryption for communication channels, secure boot processes for firmware integrity validation, and authentication protocols resistant to replay and spoofing attempts—the gap between deployment velocity and security assurances will broaden. Given the rapid evolution of functionalities in this domain, adaptive security strategies, capable of learning from both historical attack patterns and real-time monitoring outputs, will be particularly critical in balancing the benefits of innovation against the exposure to national-level threats.

2 FOUNDATIONS OF IOT IN THE CONTEXT OF NATIONAL AND STATE SECURITY

2.1 Definition and Scope of IoT

The Internet of Things (IoT) can be understood as an expansive network architecture comprising diverse physical devices, ranging from basic sensor nodes to sophisticated autonomous machines, interconnected through both wired and wireless communication technologies to facilitate bidirectional interaction between the physical environment and digital systems.

These interconnected entities are distinguished by their embedded sensing and actuation functionalities, enabling them to gather environmental data, process information either locally or remotely, and execute actions contingent upon pre-defined instructions or algorithmic triggers. Their implementation spans a variety of settings, including industrial facilities, healthcare environments, transportation infrastructure, agricultural operations, and domestic living spaces, thereby enhancing both operational utility and the potential attack surface. A salient characteristic of IoT systems is their layered architecture, typically divided into layers such as the perception layer (consisting of physical devices and sensors), the network layer (responsible for data transmission), and the application layer (providing functional outputs to end users) (Al-Garadi et al., 2020).

Each of these layers presents unique security challenges due to variations in protocols, computational resources, and exposure to external interfaces. At the foundational level of the perception layer, physical devices are frequently constrained in processing power and memory capacity. This limitation can hinder the incorporation of advanced cryptographic algorithms that would otherwise enhance their robustness against attacks (Voronko, 2024).

Moreover, design decisions made at this layer significantly impact the overall risk profile of the system. From a conceptual perspective, IoT is not confined to static deployments but includes highly dynamic configurations where devices may spontaneously join or leave networks, and connections might be transient. Such dynamism permits versatility but also influences the security landscape by augmenting vectors for unauthorized access or malicious manipulation (Ani et al., 2019).

For instance, devices integrated into supply chains within critical infrastructure sectors such as energy or transportation may exhibit intermittent connectivity during maintenance or operational cycles. In these contexts, the transient nature of these connections can conceal ongoing threats until they intensify. A critical viewpoint in defining the Internet of Things (IoT) involves acknowledging its integration with existing communication technologies and emerging computational paradigms, including cloud computing and machine learning.

Numerous IoT applications depend on cloud infrastructure to provide scalable storage, facilitate remote computation, and enable service orchestration (Kudini, 2024). Moreover, some applications incorporate machine learning models at various junctures within the architecture to facilitate adaptive decision-making based on real-time sensor data (El-Sofany et al., 2024). This combination allows for advanced functionalities such as predictive maintenance in manufacturing operations or contextually aware automation within smart cities.

Nevertheless, it also obscures the conventional demarcations between cyber infrastructures and physical systems, which is a significant consideration when evaluating risks at the national level. From a pragmatic standpoint, IoT subsumes a broad array of device categories: industrial control sensors assessing flow rates in pipelines, wearable health monitors transmitting biometric data, environmental probes monitoring air quality, logistics tags with embedded GPS for asset tracking, and consumer devices like smart refrigerators interfacing with energy demand-response systems. Each operates under distinct regulatory requirements, network conditions, and protocols for lifecycle management.

Consequently, defining IoT must accommodate this diversity while recognizing shared foundational features, such as persistent connectivity, data generation aligned with sensing functions, and the capacity for autonomous or semi-autonomous operation. An additional scope-related dimension surfaces when considering the interaction between IoT systems and broader digital ecosystems. They are not isolated entities; rather, they engage with enterprise IT assets, operational technology systems that control physical processes, mobile endpoints borne by individuals, and even other IoT networks managed by third parties (Group, 2018).

These interconnections augment overall system complexity and foster interdependence across various domains. Disruption in one segment, whether induced by technical failure or a targeted attack, may propagate through software dependencies, shared communication channels, or misconfigured interfaces. The extensive scope of IoT necessitates a reevaluation of traditional threat modeling methodologies, which were predominantly optimized for discrete software applications. As noted in previous studies (Aufner, 2020), many established frameworks inadequately anticipate hardware-based threat vectors unique to IoT deployments because these frameworks were developed under assumptions that treated hardware as either trusted or immutable during analysis.

Consequently, a comprehensive approach necessitates the incorporation of artifacts from the device design stages alongside conventional software lifecycle inputs to accurately enumerate systemic vulnerabilities. In the context of national security discourse, defining IoT surpasses the mere listing of device types or communication protocols. Instead, it necessitates an understanding of their role within critical infrastructures, such as emergency response services, food distribution networks, dam monitoring systems, military operations centers, educational campuses with connected laboratories, and hospital systems equipped with remote diagnostic tools (Ani et al., 2019).

The interconnectivity across these sectors implies that IoT's operational boundaries often misalign with the jurisdictional or organizational boundaries employed in governance frameworks. Additionally, scope determination must encompass privacy as a core parameter, alongside considerations of reliability and resilience. Each connected node, capable of generating detailed telemetry—whether through the recording of geolocation trails via GPS-enabled units or the scanning of thermal signatures via infrared sensors—carries potential implications for individual privacy rights and corporate intellectual property protection (Al-Garadi et al., 2020).

Addressing these implications requires embedding privacy-preserving principles not as sporadic afterthoughts, but as integral components within the core architectural definitions utilized during procurement and standardization phases. Therefore, the definition and scope of IoT comprise a complex matrix: it spans layers from sensing hardware to analytics-rich applications; encompasses industries from civilian retail environments to mission-critical defense logistics; navigates constraints imposed by the minimal capability of embedded systems alongside complexities introduced by integration into global cloud infrastructures; and encompasses both operational safety margins and normative discussions regarding data sovereignty. By comprehending this vastness early in strategic planning processes centered on national interests, stakeholders are better equipped to manage both the immediate security issues elucidated in Section 1 and the enduring sustainability challenges inherent in extensive, connected ecosystems.

2.2 Relevance of IoT to Critical Infrastructure

The convergence of Internet of Things (IoT) implementations with critical infrastructure systems is particularly noteworthy due to the provision of indispensable services by these sectors, where disruptions

can lead to cascading societal and economic impacts. Systems such as energy grids, water distribution networks, transportation mechanisms, and emergency communication frameworks necessitate real-time operational insight to maintain effective functioning under varying conditions of load and stress. IoT technologies enable this level of awareness by delivering continuous data streams from widely distributed assets, thereby allowing system operators to identify anomalies, foresee maintenance requirements, and manage distributed resources more efficiently.

This degree of connectivity enhances the adaptive and responsive nature of infrastructure while simultaneously exposing it to novel attack vectors that were previously confined to isolated information technology environments. From a national security standpoint, critical infrastructure is viewed both as a strategic asset and as a potential point of vulnerability. The European Union's classification of pivotal sectors at both the supranational and state levels underscores the importance of domains such as energy and transport to societal stability (P0103tra0219cu, 2021). Integrating IoT devices into these systems augments capabilities; for instance, smart metering can optimize electricity distribution, and connected sensors can manage traffic flows in real-time. However, these devices may also become points of weakness if their firmware integrity is compromised or if communication channels are intercepted.

When operational technology closely integrates with information technology layers via IoT, threats originating in the digital realm can quickly extend into the physical world, a scenario not anticipated in previous engineering designs. An additional perspective arises in the defense sector's utilization of IoT-enabled infrastructures, where real-time situational updates from remote sensors can guide tactical decisions or logistical coordination. Yet, the sophistication of adversaries in cyberspace, as evidenced by instances where state actors employ coordinated information confrontation strategies, indicates that IoT assets will be targeted for intelligence gathering or disruption.

The amalgamation of AI-enhanced analytics with extensive sensory data volumes could produce unprecedented predictive capabilities for asset management and threat anticipation but might equally be manipulated to mislead decision-makers through data tampering or sensor deception. Cybersecurity considerations significantly influence the discourse surrounding the integration of IoT into critical infrastructure. As systems become progressively interconnected across borders and administrative boundaries, any deviation or malfunction holds the potential for rapid escalation beyond its initial point of origin (Ahmed et al., 2023). The impact of new paradigms such as IoT combined with cloud services heightens this dynamic: while centralization enhances orchestration efficiency, it also forms high-value targets whose compromise could simultaneously affect multiple dependent systems. Distributed denial-of-service attacks on services crucial to operational continuity have already illustrated the swift manner in which vulnerabilities within consumer-centric IoT ecosystems can extend into core infrastructure operations (Group, 2018).

The advancement of industrial control environments to include machine learning-based monitoring systems for IoT security represents an opportunity to manage these threats proactively. The process of learning normative patterns of device-to-device interactions within intricate infrastructure networks enables models to identify anomalies indicative of intrusion efforts prior to the occurrence of significant damage (Al-Garadi et al., 2020). For instance, an unexpected increase in command signals transmitted to remote grid components outside standard operational hours may be recognized as abnormal and subsequently activate automated containment protocols.

However, reliance on machine learning and deep learning methodologies introduces new dependencies concerning the quality of training data; biases or deficiencies in the data could undermine detection accuracy, particularly in confronting emergent attack vectors (El-Sofany et al., 2024). Policy implications hold considerable significance as well. Emphasized in scholarly examinations of resilience modeling for critical national infrastructure (CNI), evolving threat landscapes necessitate not merely incremental enhancements but occasionally comprehensive transformations of established protection strategies (Ani et al., 2019). Current critical infrastructure protection (CIP) strategies frequently exhibit deficiencies in covering a broad range of attributes pertinent to contemporary threats, notably those associated with human-mediated cyber intrusions rather than environmental hazards.

Integrating IoT-specific elements into these frameworks is crucial due to the increasing convergence between cyber threats and physical operational repercussions with each successive iteration of device

integration. An often-overlooked yet vital component in sustaining resilient IoT-enhanced critical infrastructures is effective key management within heterogeneous network configurations (Attkan & Ranga, 2022).

Energy distribution nodes that are interconnected through decentralized IoT architectures possess distinct fault tolerance characteristics compared to localized centralized structures; the selection of appropriate key management systems (KMS) for encryption directly influences whether an attacker exploiting a single node can freely infiltrate others. Privacy-related risks are intrinsically linked to security concerns. IoT deployments integrated into infrastructure routinely gather sensitive data sets, from passenger movement patterns within public transit systems to industrial production statistics, which, if compromised, could produce competitive intelligence or facilitate hostile reconnaissance activities.

In transportation sectors such as railways, robust encryption protocols like SSL/TLS are employed to secure communications between embedded control units and supervisory platforms, while layered authentication regulates access rights to individual device interactions. Although this mitigates certain classes of exploitation, consistent vigilance against approaches such as distributed denial-of-service aimed at disrupting operational accessibility is essential (Voronko, 2024).

Furthermore, the progression toward advanced multi-layered architectures incorporating virtualized network functions (VNFs) alongside conventional physical network functions (PNFs) adds complexity for defenders responsible for safeguarding the interfaces between devices and users (El-Sofany et al., 2024). Internal threats from compromised on-domain devices must be approached distinctly from external penetrations arising from wide-area networks, neglecting either poses risks of systemic destabilization. Bearing in mind incidents like the Mirai botnet's exploitation of unsecured IoT components to destabilize major internet services indirectly leveraged by infrastructure operators (Group, 2018), it is apparent that the security of these devices cannot be dismissed as secondary.

Threat assessments must contemplate how vulnerabilities within ostensibly peripheral assets could trigger national-scale disruptions if foundational services, such as DNS resolution, are compromised during coordinated attacks. Ultimately, the significance of IoT integration within critical infrastructure is encapsulated in a paradox: while it provides transformative enhancements in efficiency, adaptability, and foresight for systems crucial to national welfare, it concurrently expands potential pathways for adversaries to inflict large-scale damage.

Addressing this duality necessitates not only technical fortification through encryption-by-default policies, anomaly detection systems, and decentralized fault-tolerant structures, but also adaptive governance frameworks that harmonize policy evolution with technological advancements (P0̈103tra0̈219cu, 2021). Only through these measures can nations fully actualize the potential of interconnected infrastructure without jeopardizing its fundamental resilience.

3. THREAT LANDSCAPE FOR IOT IN NATIONAL SECURITY

3.1 External Threats and Internal Threats Overview

The incorporation of IoT components into critical systems poses a bifurcated security challenge, influenced by threats arising both externally and internally within the operational surroundings. External threats predominantly originate from malicious entities exploiting vulnerabilities inherent in device design, communication protocols, or network configurations. Such threats may encompass distributed denial-of-service (DDoS) campaigns, which target the availability of essential services, to more targeted invasions leveraging compromised credentials or vulnerabilities in exposed interfaces (Hadi et al., 2023).

The deployment of botnets comprised of unsecured IoT devices has already illustrated how economically viable, internet-connected endpoints can be transformed into potent attack platforms, capable of disrupting not only the intended target but also ancillary systems dependent on shared infrastructure (Group, 2018). Adversities posed by external adversaries seeking operational disruption may utilize spoofing techniques to introduce falsified sensor data into automated control loops or instigate man-in-the-middle attacks to intercept and alter communications between nodes. Such manipulations can

provoke unpredictable physical-world behaviors, such as erroneous actuator responses in industrial environments, thereby diminishing safety and reliability (Chen et al., 2022). In segments where instantaneous response is indispensable, as in vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) communications, any latency introduced by such interference may undermine decision-making processes vital for safety (Group, 2018).

Cyber-espionage constitutes a related category of external threats, wherein strategic actors endeavor to extract sensitive operational data without activating alerts. In contexts concerning national defense, these infiltrations might target sensor networks established for perimeter surveillance or logistic coordination, thereby mapping asset locations and activity patterns over time. Manipulations of this nature can transpire without immediate overt damage, yet they pave the way for subsequent sabotage or disinformation campaigns. Equally troubling is the potential for external attackers to exploit firmware vulnerabilities uncovered through public vulnerability feeds or reverse engineering; once a defect is comprehended, extensive automated scanning tools can identify susceptible devices across global networks in a matter of minutes (El-Sofany et al., 2024).

The heightened complexity and heterogeneity of IoT networks augment exposure due to the challenge of enforcing standardized defenses across diverse hardware architectures and software stacks (Garcia-Morchon et al., 2019). The internal threat landscape exhibits distinct characteristics but remains equally severe. Insider threats may emerge from individuals with legitimate access who engage in malicious or negligent activities.

This could entail altering configuration files to bypass authentication protocols, installing unauthorized software modules that establish backdoors, or disabling logging services to evade detection during unauthorized activities (Hadi et al., 2023).

In contexts where IoT devices function autonomously within critical infrastructure frameworks, even ostensibly minor modifications at the device level, such as adjusting calibration parameters, can propagate through dependent processes due to the tight coupling between sensors and control mechanisms (Ani et al., 2019). Users possessing privileged administrative rights pose particular risks if their accounts are compromised, as these credentials often provide comprehensive control over device behavior and connectivity pathways. Internal risks also include latent vulnerabilities inherent in the devices themselves. Many IoT endpoints have limited processing capabilities, resulting in constrained adoption of robust encryption algorithms or sophisticated anomaly detection mechanisms locally (Al-Garadi et al., 2020).

Firmware may be distributed with hardcoded default passwords or outdated protocol implementations that are never patched due to inadequate lifecycle maintenance policies. These weaknesses constitute primary internal threats when they offer footholds for adversaries already present within a segmented network, enabling lateral movement towards higher-value targets undetected. There is also the dimension of accidental insider threats, prompted by misconfiguration or insufficient security awareness among operational personnel. For instance, connecting a maintenance laptop infected with malware to a supposedly isolated industrial IoT subnet can inadvertently bridge air-gapped protections.

Similarly, activating unsecured remote-access features on field devices for convenience can expose them to unsolicited internet connections (Garcia-Morchon et al., 2019). Such unintentional exposure is exacerbated in scenarios where operational teams underestimate the interconnectedness of modern systems; what appears to be an isolated endpoint may indeed interface with multiple subsystems via machine-to-machine protocols.

A complicating factor in the analysis of both external and internal threats is the convergence of cyber layers with physical process control. Attacks initiated externally may swiftly manifest as internal disruptions once malware propagates within trusted perimeters through compromised update servers or supply chain insertions. Likewise, malicious insiders could secrete authentication tokens externally or collaborate with foreign entities, transforming an internal breach into a broader coordinated offensive (Group, 2018).

In industrial control system contexts superimposed upon IoT frameworks, these composite attacks hinder attribution efforts while reducing available response times before critical thresholds are surpassed. Addressing these multifaceted threats necessitates incorporating proactive monitoring capable of detecting anomalies associated with both categories. Machine learning-based models offer early detection

potential by observing deviations from established behavioral baselines for devices and applications (El-Sofany et al., 2024). However, their efficacy can be compromised if internal actors manipulate training datasets or if novel external attack methodologies generate traffic patterns indistinguishable from legitimate surges caused by irregular operating conditions.

Accordingly, effective defenses require the amalgamation of automated pattern recognition with traditional rule-based controls informed by comprehensive risk management frameworks, such as those derived from National Infrastructure Protection Plan methodologies (Ani et al., 2019). This synthesis ensures that mitigation strategies address not only known vectors but also evolving hybrid tactics bridging external penetration attempts with internal exploitation opportunities. Ultimately, the examination of external versus internal threats in IoT-centric national security contexts elucidates that these domains cannot be regarded as mutually exclusive silos; rather, they constitute an interdependent continuum where compromise in one domain facilitates action in the other.

Safeguarding critical systems necessitates strategies cognizant of this interplay, reinforced through multi-layered authentication regimes, encrypted communication channels impervious to spoofing attempts, rigorous patch management schedules across heterogeneous fleets, and continuous education aimed at reducing risky behaviors among personnel granted operational access rights (Hadi et al., 2023). Without concurrent attention to both aspects of this equation, defenses will remain susceptible to exploitation by adversaries skilled at traversing categorical boundaries between outsider intrusion and insider facilitation.

4 IMPACT OF IOT THREATS ON NATIONAL AND STATE SECURITY

4.1 Operational Disruption and Economic Consequences

Interruptions to operational continuity instigated by IoT-associated security incidents can materialize abruptly, extending significantly beyond the immediate technical confines of the compromised system. In numerous critical infrastructure contexts, the integration of network-linked control and monitoring devices has established an operational dependence on the accuracy, timeliness, and integrity of data.

The degradation of these elements through malicious interference—via data manipulation, denial-of-service attacks, or direct sabotage of control logic—provokes consequential effects upon safety-critical processes and essential public services. In rail transport networks, for instance, cyberattacks possess the potential to manipulate or incapacitate train speed regulation systems or sensor-driven signaling mechanisms. Such interference not only temporarily stalls operations; it also heightens immediate risks to passenger safety and could precipitate accidents resulting in casualties.

Similar disruptions in cargo tracking or routing systems may hinder supply chains, disrupt just-in-time manufacturing pipelines, and induce costly delays in the transport of high-value goods (Voronko, 2024). The economic implications manifest from both direct remediation costs and indirect market impacts. Direct expenditures encompass the restoration of impacted hardware and software components, the deployment of forensic teams for incident investigations, and the maintenance of operational downtime as systems are resecured. Indirect repercussions, albeit more challenging to quantify, frequently exceed the immediate repair costs.

These include reputational damage leading to customer attrition, contractual penalties for unfulfilled service-level agreements, and diminutions in investor confidence. Media coverage that amplifies public perceptions of insecurity in the systems of a transportation operator or energy provider can perpetuate a credibility deficit long after technical faults have been rectified. Within sectors such as industrial control environments supplemented with IoT sensors and actuators, disruptions can propagate rapidly from a single vulnerable point to entire production lines interconnected through shared controllers. If attackers capitalize on firmware vulnerabilities to introduce erroneous readings or impede actuator commands during critical production phases, entire batches may be rendered defective prior to the detection of the issue (Chen et al., 2022). The economic ramifications extend significantly beyond the mere wastage of raw materials, encompassing legal disputes over breach-of-contract if defective products penetrate the market, as well as regulatory fines when safety standards are not met. Economic repercussions also materialize

from cascading failures that traverse multiple infrastructure domains. For instance, a cyberattack targeting IoT-based monitoring within the energy grid may destabilize electricity supply in specific areas. Such instability can subsequently jeopardize water distribution facilities that rely on electrically powered pumps or affect hospitals that operate without adequate backup capacity in their medical device networks. Each subsequent disruption amplifies societal costs while diluting accountability across numerous stakeholders (Group, 2018).

Attack campaigns, such as those driven by large-scale IoT botnets, illustrate how adversaries can exert economic pressure on entire sectors without necessarily breaching their core control systems. By incapacitating domain name resolution services or cloud-based application interfaces essential to traffic management platforms or logistics coordination tools, malevolent actors induce widespread degradation of services (Hadi et al., 2023). Even in the absence of physical asset damage, sustained outages diminish trust in the continuity of digital services within supply chains that increasingly depend on IoT interlinks. Beyond adversarial engineered disruptions, inadvertent device mismanagement can yield effects of equivalent operational severity.

Misconfigurations that disrupt encryption between distributed IoT sensors within a manufacturing environment may allow unsophisticated intrusions that precipitate incorrect system behaviors, leading to a complete production halt. As downtime extends over several days awaiting full recovery, partly due to frequent shortages of replacement parts for specialized embedded IoT devices, consequent revenue losses can be substantial (Al-Garadi et al., 2020). The cost structures associated with these incidents increasingly encompass expenditures aimed at compliance restoration under international cybersecurity regulations governing critical infrastructure sectors.

Post-incident investigations often uncover inadequacies such as a lack of encrypted communications or failures to authenticate update packages for IoT endpoints, deficiencies frequently highlighted in regulatory reviews following incidents (Group, 2018). Mandatory system upgrades mandated by such reviews impose capital burdens that are particularly challenging for operators handling heterogeneous fleets of legacy devices (Amro, 2024). Operational disruptions also manifest through long-term performance degradation when persistent threats remain undetected within IoT environments. A state-sponsored intrusion illicitly extracting minor amounts of proprietary industrial telemetry over an extended period may evade detection while skewing predictive maintenance algorithms utilized for asset management (Al-Garadi et al., 2020). The eventual decline in decision quality, exemplified by inaccurate predictions of component fatigue, could precipitate premature machinery failures during peak demand periods when replacements cannot be scheduled without interrupting core services. From a strategic economic vantage point, states must consider how adversarial exploitation of IoT vulnerabilities could afford asymmetrical advantages, undermining public confidence in the provision of national infrastructure without necessitating physical attacks. This undermining effect imposes pressures on government budgets through contingencies such as emergency procurement programs and heightened defense allocations to replace compromised technologies before their natural replacement cycles. Moreover, some disruptions entail geopolitical spillover effects.

Targeted interference with international freight transit systems utilizing IoT-enabled logistics coordination can divert trade flow competitiveness from targeted nations to rivals perceived as more secure channels for goods movement. The cumulative impact of market share losses across strategic industries, such as energy exports impeded by compromised pipeline monitoring systems, heightens economic vulnerability far beyond the accounting of directly affected firms. Ensuring availability and proper functionality across such interconnected ecosystems is therefore not solely an engineering challenge but a socio-economic imperative closely linked to national security planning priorities.

Effective mitigation of these disruptions necessitates proactive technical protective measures, such as segmentation between high-trust operational sub-networks and lower-trust external connections, complemented by incident response playbooks that address both rapid failover capabilities and public communication strategies during crises (Ani et al., 2019). In the absence of integrating technical resilience with coordinated economic risk containment strategies, individual attack occurrences will persist in threatening disproportionate systemic economic consequences relative to their initial access point vector within an IoT deployment architecture.

5 SECURITY GOVERNANCE AND POLICY FRAMEWORKS

5.1 National Cybersecurity Strategies and Regulatory Frameworks

National cybersecurity strategies fundamentally represent multi-layered frameworks that synthesize technological protections, legal measures, institutional coordination mechanisms, and strategic policies into a unified defense posture against both domestic and transnational cyber threats. The development of these strategies often mirrors the unique geopolitical and socio-economic environments of the nation adopting them, as well as the variety and sophistication of its critical infrastructure sectors. Nations with substantial IoT penetration in essential services are required to address not only the immediate technical concerns of device and network security but also the systemic interdependencies that give rise to cascading vulnerabilities.

A comprehensive national strategy generally commences with an evaluation of existing capacities in cyber defense. This involves an audit of physical and digital assets, assessment of human capital readiness, mapping of inter-agency coordination mechanisms, and identification of legal deficiencies in prosecuting cybercrime. Enhancing these foundations often necessitates the expansion of specialized law enforcement units and the streamlining of institutional responsibilities across government bodies. The Indonesian government, for instance, expanded its cyber defense framework to include total defense principles, increased personnel in its police cybercrime divisions from 40 to 100, restructured the National Crypto Agency into the National Cyber and Crypto Agency (BSSN), and enacted a national cybersecurity strategy that emphasizes resilience across public services, law enforcement, cultural awareness programs, and protection of the digital economy (Rizky et al., 2023).

These strategies seldom function independently; they depend on integration between government entities and private stakeholders. Numerous states formally incorporate multi-stakeholder engagement models into their policy design processes to leverage expertise from industry consortia, academia, civil society organizations, and standards development bodies (Group, 2018). This collaboration is particularly crucial in countries where standards-setting activities predominantly occur within organizations led by the private sector rather than state-run technical committees.

By integrating public-private partnerships into national frameworks, governments enhance situational awareness and expedite the remediation of identified vulnerabilities through coordinated updates or patch management campaigns on a large scale. Beyond domestic coordination mechanisms, robust strategies incorporate the international dimensions of cybersecurity policy. Governments acknowledge that digital threats readily cross jurisdictions without impediment. Consequently, bilateral agreements, engagement in multilateral cyber norms discussions, joint exercises with foreign CERTs (Computer Emergency Response Teams), and participation in global or regional security forums are integral components of proactive frameworks (Rizky et al., 2023).

This external focus enables nations to compare their capabilities with those of their peers while benefitting from intelligence-sharing arrangements that function as early-warning systems for emerging threat patterns. The development process must also account for structural challenges, such as a lack of comprehension among policymakers or stakeholders regarding specific technical requirements for secure operations, like limiting reliance on overseas-hosted critical services or enforcing encryption standards (Budiman, 2022).

Explicit procedural mandates reduce ambiguities during incidents; for instance, defining legal jurisdiction for data breaches involving servers located abroad ensures more rapid prosecution and clarity regarding notification duties. Strategic leadership is pivotal in translating high-level policies into operational practice. Leaders not only approve resource allocation but also define risk tolerance levels across sectors. They bear the responsibility of monitoring the threat horizon to identify trends, such as increases in IoT-based distributed denial-of-service attacks, and adjusting defenses accordingly (Rizky et al., 2023). Effective implementation requires detailed policy documents that delineate roles during crisis response phases; this correlates with contemporary resilience theories that advocate adaptive planning cycles devoid of fixed endpoints (Ahmed et al., 2023). For IoT-intensive national infrastructure sectors, as previously discussed in Section 4.1, strategies should encompass sector-specific annexes that address

unique protocols or operational environments. For example, industrial control systems may necessitate mandatory air-gapping for certain functions, whereas public transportation systems might focus on intrusion detection tuned for vehicular communication networks.

The integration of cryptographic requirements, addressing confidentiality, integrity verification, authentication mechanisms such as digital signatures, and robust key management protocols, ensures foundational interoperability across devices while mitigating the risk of trivial exploitation during cross-system communication (Group, 2018). Certain jurisdictions explicitly include regulatory compliance audits within their frameworks to evaluate operator conformity with security standards comparable to those instituted under directives such as the EU NIS Directive. These audits serve dual purposes as enforcement instruments and capacity-building exercises by identifying systemic vulnerabilities before adversaries do (Schaberreiter et al.).

Provisions might require regular penetration testing for operators of critical services or mandate the adoption of certified secure hardware modules in new IoT deployments targeted for vital industry applications. Furthermore, governance frameworks increasingly recognize that achieving perfect prevention against sophisticated adversaries is unattainable. They incorporate resilience-focused objectives to minimize service degradation when incidents occur. Measures in this context may range from pre-negotiated mutual assistance agreements among infrastructure proprietors ensuring spare capacity during outages (Ahmed et al., 2023), to continuous monitoring systems that supply threat intelligence platforms capable of correlating anomalies across diverse networks in real time.

Another characteristic of mature strategies is embodied in a structured regulatory environment that maintains accountability while avoiding the stifling of innovation. In developing nations, which are constructing foundational digital economies alongside critical infrastructures, regulations sometimes encounter resistance if perceived as onerous by emerging industries dependent on rapid deployment cycles for IoT solutions. Constructing proportionate regulations that balance economic incentives with stringent minimum-security assessments helps prevent scenarios where insecure consumer-grade IoT products inadvertently infiltrate industrial contexts due to ambiguous applicability scopes. Ultimately, national strategies, supported by adaptive legal frameworks, establish not merely compliance architectures but dynamic systems capable of evolving in conjunction with shifting threat landscapes. They institutionalize periodic review cycles, typically every two to five years, that accommodate the integration of lessons learned from domestic and global incidents (Rizky et al., 2023).

By embedding this reflexivity within governance structures and ensuring that each cycle includes multi-sectoral consultation along with opportunities for cross-border dialogue, states position themselves more effectively to respond decisively whether disruptions originate within their jurisdictional boundaries or beyond.

6 CONCLUSION

The incorporation of Internet of Things (IoT) technologies into national infrastructures presents a dual-faceted scenario, offering significant enhancements in operational efficiency and situational awareness, while simultaneously introducing considerable security challenges. The diverse and resource-constrained nature of IoT devices, coupled with their extensive deployment across critical sectors such as energy, transportation, healthcare, and industrial control, creates a complex attack surface that is susceptible to both external and internal threats.

These vulnerabilities arise from design trade-offs that prioritize usability and cost over security, resulting in persistent weaknesses such as default credentials, insufficient firmware updates, and inadequate encryption. External adversaries exploit these gaps through tactics including distributed denial-of-service attacks, unauthorized access, data manipulation, and cyber-espionage, often leveraging botnets comprising compromised IoT nodes. Internal threats, whether from malicious insiders or inadvertent misconfigurations, further complicate defense efforts by facilitating lateral movement within networks and undermining trust in system integrity. The convergence of cyber and physical domains magnifies the potential impact of attacks, as disruptions in digital layers can cascade into physical operational failures with severe safety and economic consequences. The economic ramifications extend

beyond immediate remediation costs to include reputational damage, regulatory penalties, and long-term degradation of system performance.

Cascading failures across interconnected infrastructure sectors underscore the systemic risks posed by insecure IoT deployments. Addressing these challenges necessitates a comprehensive approach that combines technical safeguards, such as encryption by default, anomaly detection, and secure key management, with adaptive governance frameworks capable of aligning policy with technological advancements.

National cybersecurity strategies must integrate multi-stakeholder collaboration, international cooperation, and sector-specific considerations to build resilience and ensure the continuity of essential services. Furthermore, the dynamic nature of IoT ecosystems demands continuous monitoring and incident response capabilities that can promptly detect and mitigate emerging threats. Machine learning and artificial intelligence offer promising avenues for enhancing threat detection, though their effectiveness heavily relies on the quality of training data and the ability to counter adversarial manipulation.

Regulatory frameworks should balance security requirements with innovation incentives, ensuring that minimum-security standards are met without stifling technological progress. Ultimately, safeguarding IoT-enabled critical infrastructures is a complex endeavor that intersects technical, organizational, legal, and socio-economic dimensions. Success depends on recognizing the interdependence of external and internal threat vectors and implementing layered defenses that address vulnerabilities across device lifecycles and network architectures. By embedding privacy and security considerations into the foundational design and operational phases, states can better protect national interests, maintain public trust, and harness the benefits of connected technologies without compromising resilience or safety.

REFERENCES

Ahmed, M. F., Molla, A. H., Uddin, M. R., & Chowdhury, T. R. (2023). Advancing cyber resilience: Bridging the divide between cyber security and cyber defense. International Journal for Multidisciplinary Research (IJFMR), 5(6), 1. http://www.ijfmr.com

Al-Garadi, M. A., Mohamed, A., Al-Ali, A., Du, X., & Guizani, M. (2020). A survey of machine and deep learning methods for internet of things (IoT) security.

Amro, A. (2024). IoT vulnerability scanning: A state of the art.

Ani, U. D., Watson, J. D. McK., Nurse, J. R. C., Cook, A., & Maple, C. (2019). A review of critical infrastructure protection approaches: improving security through responsiveness to the dynamic modelling landscape.

Attkan, A., & Ranga, V. (2022). Cyber-physical security for IoT networks: A comprehensive review on traditional, blockchain and artificial intelligence based key-security. Complex & Intelligent Systems, 8, 3559–3591. https://doi.org/10.1007/s40747-022-00667-z

Aufner, P. (2020). The IoT security gap: A look down into the valley between threat models and their implementation. International Journal of Information Security, 19(1), 3–14. https://doi.org/10.1007/s10207-019-00445-y

Budiman, I. (2022). National cyber defense of the indonesian government in protecting the society. MANDALA: Jurnal Ilmu Hubungan Interna Sional, 5(2), 231.

Buiya, M. R., Laskar, A. K. M. N., Islam, M. R., Shil, S. K., Chowdhury, M. S. R., Shawon, R. E. R., & Sumsuzoha, M. (2024). Detecting IoT cyberattacks: Advanced machine learning models for enhanced security in network traffic. Journal of Computer Science and Technology Studies, 6(4), 142. https://doi.org/10.32996/jcsts.2024.6.4.16

Chen, Z., Liu, J., Shen, Y., Simsek, M., Kantarci, B., Mouftah, H. T., & Djukic, P. (2022). Machine learning-enabled IoT security: Open issues and challenges under advanced persistent threats. ACM Computing Surveys, 35.

El-Sofany, H., El-Seoud, S. A., Karam, O. H., & Bouallegue, B. (2024). Using machine learning algorithms to enhance IoT system security. Scientific Reports, 14, 12077. https://doi.org/10.1038/s41598-024-62861-y

Garcia-Morchon, O., Kumar, S., & Sethi, M. (2019). Internet of things (IoT) security: State of the art and challenges. In Internet Research Task Force (IRTF) Request for Comments (8576; p. 1).

Group, I. I. C. S. W. (2018). Interagency report on the status of international cybersecurity standardization for the internet of things (IoT). https://doi.org/10.6028/NIST.IR.8200

Hadi, Q. A., Alfoudi, A. S., & Mahdi, A. M. (2023). IoT cybersecurity threats and detection mechanisms: A review. Wasit Journal for Pure Sciences, 2(2), 231.

Kudini, A. A. (2024). Internet of things based data integration ontology in cyber security. International Journal of Engineering Research and Applications, 14(11), 01–04. https://doi.org/10.9790/9622-14110104

Mohamed, N., Oubelaid, A., & Almazrouei, S. K. (2023). Staying ahead of threats: A review of AI and cyber security in power generation and distribution. International Journal of Electrical and Electronics Research (IJ EER), 11(1), 143–147. https://doi.org/10.37391/IJEER.110120

Oredola, C., & Ashraf, A. (2024). A systematic mapping study on SDN controllers for enhancing security in IoT networks. https://arxiv.org/abs/2408.01303v1

P0̈103tra0̈219cu, P. (2021). EMERGING TECHNOLOGIES AND NATIONAL SECURITY: THE IMPACT OF IoT IN CRITICAL INFRASTRUCTURES PROTECTION AND DEFENCE SECTOR. Land Forces Academy Review, XXVI(4(104)), 423. https://doi.org/10.2478/raft-2021-0055

Petrişor, P. (2021). Emerging technologies and national security: The impact of IoT in critical infrastructures protection and defence sector. Land Forces Academy Review, XXVI(4(104)), 423. https://doi.org/10.2478/raft-2021-0055

Rizky, R., Samuel, L. T. T., Handayani, K. S. N., & Zakky, A. H. (2023). Analysis of presidential regulations concerning cyber security to bolster defense policy management. Defense and Security Studies, 4, 84–93. https://doi.org/10.37868/dss.v4.id244

Schaberreiter, T., Röning, J., Quirchmayr, G., Kupfersberger, V., Wills, C., Bregonzio, M., Koumpis, A., Sales, J. E., Vasiliu, L., Gammelgaard, K., Papanikolaou, A., Rantos, K., & Spyros, A. A cybersecurity situational awareness and information-sharing solution for local public administrations based on advanced big data analysis: The CS-AWARE project.

Voronko, I. (2024). The security of IoT systems in railway transport. Transport Systems and Technologies, 4(3), 90. https://doi.org/10.32703/2617-9059-2024-43-7