International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.
© 2025 Scholar AI LLC.
https://ijpsat.org/ Vol. 51 No. 2 July 2025, pp. 265-275

Strategic Integration Of Signal Intelligence Technologies For Cyber Threat Attribution In Indonesian Government Systems: A Policy And Legal Framework For IMSI Catcher Deployment

Mohammad Rayhan Syahman*[1], Ni Luh Meliana Liberty*[2], H.A. Danang Rimbawa*[3], Bisyron Wahyudi*[4]

[1, 2]Master Programee of Cyber Defense Engineering's Department, Republic of Indonesia Defense University, Bogor, Indonesia

[3, 4]Lecturer of Cyber Defense Engineering's Department, Republic of Indonesia Defense University, Bogor, Indonesia

[1]mohammad.syahman@tp.idu.ac.id, [2]lub.liberty@tp.idu.ac.id, [3] danang.rimbawa@idu.ac.id, [4]bisyron.wahyudi@idu.ac.id

Corresponding Author: Mohammad Rayhan Syahman. E-mail: mohammad.syahman@tp.idu.ac.id

Abstract - Indonesia's increasing digital dependency has exposed its government systems to sophisticated cyber threats, including the hijacking of official domains by transnational cybercriminals (Singh & Krishnan, 2021). Traditional cybersecurity defences often struggle with attribution and proactive mitigation due to anonymization, jurisdictional complexity, and the technical evasions used by threat actors (Rid & Buchanan, 2015). To address this critical capability gap, this study explores the strategic integration of signal intelligence (SIGINT) technologies—specifically International Mobile Subscriber Identity (IMSI) catchers—into Indonesia's cyber defence framework.Using a policy-oriented qualitative methodology, this paper examines the operational potential, legal limitations, and ethical risks of deploying IMSI catchers to enhance threat attribution capabilities. It evaluates Indonesia's existing cybersecurity governance structure—including regulatory anchors such as UU ITE and Perpres No. 82/2022—and compares policy benchmarks from Singapore, Estonia, and Israel, which have successfully embedded SIGINT into broader cyber strategies (Chong & Hall, 2022).Findings suggest that while IMSI catchers offer actionable intelligence-gathering capabilities, their deployment must be constrained by clear legal mandates, inter-agency protocols, and civil rights safeguards (Deibert, 2020; UN Special Rapporteur, 2019). This study proposes a strategic policy framework that enables lawful use of SIGINT tools to detect and attribute cyber threats against public digital infrastructure.The research contributes to global discourse on responsible surveillance in cybersecurity, offering actionable guidance for policymakers and intelligence stakeholders in emerging digital democracies seeking to secure state systems without compromising democratic values.

Keywords: Signal Intelligence, IMSI Catcher, Cyber Threat Attribution, Government Systems, Surveillance Policy, National Cyber Defence, Legal Oversight, Ethical Surveillance

I. INTRODUCTION

Cybersecurity has become an integral dimension of national defense policy in the digital era. As state functions increasingly rely on interconnected systems, the threats targeting government digital infrastructure have evolved in both scale and sophistication. In this context, cyberattacks that target public sector websites, networks, and data systems are no longer isolated technical events but strategic disruptions with national security implications.

A central challenge in modern cybersecurity is attribution—the ability to accurately identify the perpetrators behind cyber incidents. While conventional tools such as digital forensics and IP tracing provide partial insights, advanced threat actors often exploit anonymization techniques, encryption, and cross-border infrastructure to obscure their identities (Rid & Buchanan, 2015). This results in a significant gap between detection and response, making it difficult for authorities to act with confidence or legal authority.

One potential solution lies in the application of signal intelligence (SIGINT) technologies, particularly International Mobile Subscriber Identity (IMSI) catchers. These tools, commonly used in law enforcement and counterterrorism, allow for the real- time identification and location of cellular devices. When deployed within a tightly controlled legal and operational framework, IMSI catchers could support cyber threat attribution efforts by linking suspicious digital activity to physical actors.

This study proposes a strategic approach for integrating SIGINT tools into national cybersecurity policy. By drawing from international best practices— such as those implemented in Singapore, Israel, and Estonia (Chong & Hall, 2022)—the paper seeks to contribute to the development of an ethical, legal, and operationally effective cyber defense model for Indonesia.

1.1 Background

Indonesia's growing dependence on digital systems for governance and service delivery has made its public infrastructure an attractive target for cybercriminals. A surge in domain hijackings—where official government websites are redirected to illicit sites, particularly online gambling platforms—has exposed critical vulnerabilities in the state's cyber infrastructure (Singh & Krishnan, 2021). These incidents not only disrupt state services but also diminish public trust and national credibility.

Despite regulatory advancements such as UU ITE and Perpres No. 82/2022 on critical infrastructure protection, existing cybersecurity mechanisms remain largely reactive and technologically limited. Tools like firewalls, anti-malware systems, and conventional forensic methods are frequently bypassed by attackers employing encrypted channels, decentralized infrastructures, and anonymization protocols.

The attribution gap remains the most severe obstacle. Without the ability to confidently trace malicious activities to their sources, legal enforcement, incident response, and deterrence become ineffective (Rid & Buchanan, 2015). This limitation is compounded by the jurisdictional complexity of cybercrimes and the absence of inter-agency coordination on real-time intelligence gathering.

Signal intelligence (SIGINT)—specifically the use of IMSI catchers—presents an underutilized opportunity. When ethically deployed, these tools can assist in bridging the attribution gap by linking cyber activity to real-world actors, a strategy already applied in countries like Israel and Singapore with promising results (Chong & Hall, 2022). However, their integration into Indonesia's cyber policy must navigate legal, ethical, and governance challenges to avoid misuse.

1.2 Research Objectives

This paper seeks to explore how signal intelligence tools, especially IMSI catchers, can be strategically and lawfully deployed to enhance Indonesia's cybersecurity posture. The core objectives are:

1. To evaluate the strategic and technical potential of IMSI catchers as tools for cyber threat attribution in cases involving government system hijackings. To assess the legal, ethical, and operational conditions necessary for deploying SIGINT technologies in alignment with Indonesia's cybersecurity and privacy laws.
2. To develop a policy framework that supports the regulated integration of SIGINT into Indonesia's national cyber incident response system, emphasizing both effectiveness and rights protection.

1.3 Scope

This study is focused on examining the strategic, legal, and ethical feasibility of integrating signal intelligence technologies, particularly IMSI catchers, into Indonesia's national cybersecurity framework. The scope is deliberately narrowed to address cyber threats targeting government digital infrastructure, such as domain hijackings and unauthorized redirections of public sector websites.

Key aspects within the scope include:

- Technological Assessment: Analyzing the functionality, capabilities, and limitations of IMSI catchers as tools for cyber threat attribution.
- Policy and Legal Review: Evaluating Indonesian legal instruments—such as UU ITE and Perpres No.

82/2022—in the context of SIGINT deployment, along with ethical considerations related to privacy and civil liberties.

- Comparative Benchmarking: Reviewing practices in countries such as Singapore, Estonia, and Israel, where SIGINT technologies have been integrated into national cybersecurity strategies under regulatory oversight.
- Strategic Recommendations: Proposing a policy framework tailored for Indonesian stakeholders (e.g., BSSN, Kominfo, law enforcement agencies) that balances operational effectiveness with democratic accountability.

Excluded from this study are the technical engineering details of IMSI catcher construction, private-sector cybersecurity deployments, and SIGINT applications unrelated to cyber attribution (e.g., kinetic military or counterinsurgency operations).

II. Literature Review

2.1 Cyber Threats Targeting Government Systems

In the digital age, government information systems have become strategic targets for a range of threat actors, including hacktivists, cybercriminal syndicates, and state-sponsored groups. The shift from isolated attacks to persistent and high-impact breaches has escalated concerns regarding the resilience of public digital infrastructure.

In Southeast Asia, there has been a noticeable uptick in domain hijackings where official government websites are redirected to unauthorized destinations, such as online gambling portals. These hijackings are not merely embarrassing or disruptive—they represent an attack on the symbolic and functional legitimacy of the state (Singh & Krishnan, 2021). Such attacks exploit technical vulnerabilities in DNS servers, outdated web platforms, and weak access controls.

The Indonesian National Cyber and Crypto Agency (BSSN) has reported numerous cyber incidents involving defaced public portals, manipulated DNS entries, and spoofed e-Government systems (BSSN, 2022). However, despite increasing investment in perimeter security, response times remain slow, and investigations are often inconclusive due to limited attribution capacity.

2.2 The Attribution Challenge in Cybersecurity

Attribution is the process of identifying the source or actor behind a cyberattack. In practice, this is notoriously difficult. Threat actors often employ a variety of tactics to obscure their identities, such as using botnets, virtual private networks (VPNs), anonymous relays (e.g., Tor), and compromised servers located in foreign jurisdictions. These methods make it nearly impossible to trace a single digital fingerprint back to a human perpetrator without auxiliary intelligence (Rid & Buchanan, 2015).

Technically, attribution involves collecting and correlating log data, behavioral indicators, malware signatures, and infrastructure connections. However, these data points are often unreliable or deliberately manipulated. As Rid and Buchanan (2015) argue, attribution must be understood not just as a technical exercise, but as a process that combines evidence from cyber forensics, human intelligence (HUMINT), signal intelligence (SIGINT), and open-source intelligence (OSINT).

The lack of attribution capacity in countries like Indonesia leads to impunity for cyber actors and weakens deterrence. This is especially concerning when government systems are compromised without any legal or diplomatic consequence for the attackers.

2.3 Signal Intelligence and IMSI Catchers

Signal Intelligence (SIGINT) refers to the interception and analysis of signals—primarily electronic communications—to gather intelligence. It is traditionally employed by military and law enforcement agencies for surveillance, counterterrorism, and national security missions. One specialized SIGINT tool is the International Mobile Subscriber Identity (IMSI) catcher, also known colloquially as a “cell site simulator” or “stingray.”

IMSI catchers operate by posing as a fake mobile base station. They prompt nearby mobile phones to connect, revealing unique identifiers (IMSI numbers) and, in some cases, enabling geolocation or interception of metadata and communications. These devices have been used to locate suspects, monitor large protests, and conduct covert operations (Müller-Maguhn, 2018).

In cybersecurity, the value of IMSI catchers lies in their potential to bridge the gap between cyber activity and physical identity. For instance, if a threat actor accesses a hijacked server or uploads malicious code from a mobile-connected hotspot, an IMSI catcher in the vicinity could detect and log the associated device. When used in tandem with cyber forensics, this physical-digital correlation can significantly enhance attribution efforts (Schneier, 2019).

However, this integration remains underutilized. Most national cybersecurity agencies still separate digital and physical surveillance capabilities due to bureaucratic silos or legal limitations.

2.4 Legal and Ethical Considerations

The deployment of IMSI catchers and other SIGINT tools is controversial due to their invasive nature. They indiscriminately collect data from all nearby mobile devices, not just those belonging to a suspect. This raises major privacy concerns, particularly in democratic societies governed by constitutional rights and data protection laws.

According to Deibert (2020), the unregulated use of surveillance technologies can erode civil liberties, chill dissent, and enable authoritarian practices under the guise of cybersecurity. The UN Special Rapporteur on the Right to Privacy has emphasized that states must adhere to the principles of necessity, proportionality, and judicial oversight when authorizing surveillance (UN Special Rapporteur, 2019).

For Indonesia, these concerns are amplified by the absence of a comprehensive personal data protection law (though a draft bill exists), as well as unclear inter- agency protocols regarding cyber surveillance. Without legal safeguards, the use of SIGINT tools could result in overreach, abuse, or public backlash— especially if used outside of critical incident contexts.

Therefore, the ethical integration of IMSI catchers requires a multi-layered framework involving:

2.4.1 Strict access control and judicial warranting

2.4.2 Data minimization and retention limits

2.4.3 Independent auditing and reporting mechanisms

2.4.4 Public transparency and parliamentary oversight

2.5 Comparative Policy Approaches

International best practices show that SIGINT tools can be integrated into cyber defense strategies when paired with legal constraints and strategic clarity.

2.5.1 Singapore maintains a strong cybersecurity architecture where SIGINT tools are employed under the oversight of a centralized cybersecurity agency (CSA), guided by the Cybersecurity Act of 2018. The legal framework allows surveillance in critical infrastructure sectors while requiring authorization at the ministerial level (Chong & Hall, 2022).

2.5.2 Estonia, often cited as a global digital leader, balances state security with civil rights through strong constitutional protections. Surveillance is permitted under court supervision, and intelligence agencies must report annually to a parliamentary committee. Estonia's integration of SIGINT into cyber threat response has been linked to its effective deterrence posture (ENISA, 2020).

2.5.3 Israel takes a more securitized approach, embedding SIGINT capabilities within its broader counterintelligence and cyber command ecosystem. While effective operationally, Israel has faced criticism for a lack of transparency, prompting debates around legislative reform (Chong & Hall, 2022).

These cases demonstrate that technical capability alone is insufficient. The legitimacy and success of SIGINT in cybersecurity depend on how well it is embedded into a lawful, accountable, and interoperable governance model.

Table 1. Comparative Overview of SIGINT Integration in National Cybersecurity Strategies

Aspect	Singapore	Estonia	Israel
Legal Framework	Cybersecurity Act (2018)	Surveillance Act (2001); Constitution	Internal Security Agency Law (2002); classified military regulations
Primary Use Case	Protection of Critical Information Infrastructure (CII); threat monitoring	Attribution and surveillance for national cyber threats	Integrated cyber- SIGINT operations for national defense and counterterrorism
Oversight Mechanism	Ministerial approval through Cyber Security Agency (CSA)	Court-supervised surveillance; parliamentary oversight	Internal agency review; limited public or judicial oversight
Key Strengths	Centralized command, operational speed, and sector-specific response	Strong legal safeguards; EU-aligned privacy protections	High operational capacity; effective in real-time Attribution
Main Challenges	Limited public transparency; centralization risks	Bureaucratic limitations; potential latency in decision- making	Weak civilian oversight; potential for human rights concerns

III. Research Methodology

This study employs a qualitative, policy-oriented research approach, emphasizing in-depth analysis, legal and ethical evaluation, and strategic recommendations. Given the sensitive and complex nature of signal intelligence technologies, particularly IMSI catchers, qualitative research provides the necessary depth for comprehensive policy evaluation and normative guidance, going beyond quantitative assessments that are typically confined to purely technical evaluations.

3.1 Research Design

The research employs a descriptive-analytical and normative-legal design that integrates multiple qualitative techniques to thoroughly evaluate the feasibility, legality, and strategic effectiveness of integrating SIGINT technologies into Indonesia's cybersecurity framework.

The research design encompasses four critical dimensions:

1. Contextual Descriptive Analysis

- Describes the current state of cybersecurity threats targeting government infrastructure in Indonesia, especially the domain hijacking phenomenon, to establish the urgency and relevance of the study.
- Reviews government documents, national cybersecurity strategies, and publicly available incident reports, providing contextual evidence to frame the policy challenges.

2. Comparative Policy Analysis

- Conducts a structured comparative analysis of SIGINT integration frameworks in countries with advanced cybersecurity strategies: specifically Singapore, Estonia, and Israel.

- Identifies critical success factors, legal mechanisms, oversight structures, and governance models that inform policy adaptations applicable to Indonesia's context.

3. Normative-Legal Analysis

- Critically examines Indonesia's existing legal framework governing cybersecurity and electronic surveillance, including laws such as UU ITE, Perpres No. 82/2022, and proposed legislation like the Personal Data Protection Bill.
- Reviews international legal standards and human rights principles (e.g., proportionality, necessity, legality, transparency) established by bodies such as the United Nations Human Rights Council (UNHRC) and comparative national jurisprudence.

4. Prescriptive Policy Recommendations

- Integrates insights from the descriptive, comparative, and legal analyses to develop strategic policy recommendations tailored specifically to Indonesia's institutional and legal landscape.
- Proposes concrete governance models, operational guidelines, oversight structures, and ethical safeguards for deploying IMSI catchers within Indonesian cybersecurity policy.

3.2 Data Collection Methods

To ensure comprehensive and robust findings, the study integrates multiple qualitative data collection methods:

a. Document and Literature Review

- Primary Documents:
  - National cybersecurity strategies (BSSN annual reports).
  - Indonesian legal texts: UU ITE, Perpres No. 82/2022, and pending data protection bills.
  - International reports: ENISA threat landscape reports (ENISA, 2020), UN Human Rights Council reports on digital surveillance (UN Special Rapporteur, 2019), Freedom House reports on internet governance.
- Scholarly Literature:
  - Peer-reviewed journals and books addressing SIGINT tools, cyber attribution methods, surveillance law, and ethics (e.g., Rid & Buchanan, 2015; Müller-Maguhn, 2018; Schneier, 2019; Deibert, 2020).

b. Comparative Policy Analysis

- Examination of secondary sources detailing SIGINT policies, legislation, oversight mechanisms, and operational integration in Singapore, Estonia, and Israel (Chong & Hall, 2022; ENISA, 2020).
- Evaluation of policy documents, legislation texts, annual cybersecurity reports, and academic analyses.

c. Expert Consultation

- Semi-structured interviews or structured expert consultations with cybersecurity practitioners,policy analysts, and legal experts in Indonesia (e.g., from BSSN, Kominfo, legal academia).
- Consultation aims to validate findings from literature and comparative analysis and to contextualize policy recommendations within local institutional realities.
- In cases where direct interviews were infeasible due to access limitations, secondary expert

commentaries and published interviews from credible media and institutional reports were synthesized.

3.3. Data Analysis Techniques

The data collected from these sources were systematically analyzed using three complementary qualitative methods:

a. Thematic Analysis

- Qualitative coding was performed on policy documents, expert opinions, and literature to identify central themes regarding:
  - Cyber threat trends and attribution challenges.
  - Technical capabilities and limitations of IMSI catchers.
  - Legal and ethical concerns surrounding surveillance technologies.
  - Effective governance models and oversight mechanisms.

b. SWOT Analysis

- Conducted to systematically assess:
  - Strengths: Technological capability, attribution accuracy, potential effectiveness in threat mitigation.
  - Weaknesses: Risks of misuse, civil liberties infringement, regulatory uncertainties.
  - Opportunities: Integration with existing cybersecurity frameworks, potential for international cooperation, enhancement of cyber sovereignty.
  - Threats: Public backlash, misuse by authorities, negative international reputation impacts.

c. Gap Analysis

- Conducted to clearly define the existing policy and regulatory shortfalls in Indonesia's cyber attribution capacity.
- Identified key legal and institutional gaps impeding the effective and ethical deployment of IMSI catchers.

3.4 Ethical Considerations

Given the sensitive nature of SIGINT technologies, ethical considerations have been explicitly integrated into the research design:

- Ensured compliance with international ethical research standards on digital surveillance, privacy protection, and human rights.
- Recommendations are developed within frameworks of necessity, proportionality, legality, and include explicit calls for judicial oversight and public transparency mechanisms to protect against potential misuse of IMSI catchers.

3.5 Limitations

The study acknowledges certain methodological limitations inherent in policy-oriented qualitative research:

3.5.1 No direct empirical testing or field experiments of IMSI catcher devices were conducted.

3.5.2 Limitations exist regarding the accessibility of classified or sensitive government cybersecurity strategies, restricting the depth of institutional analysis.

3.5.3 Reliance on secondary literature and document reviews may limit insights into practical implementation challenges.

IV. FINDING AND DISCUSSION

The findings of this study are organized around three central pillars: (1) strategic and technical feasibility, (2) legal and ethical challenges, and (3) policy integration pathways. The discussion critically examines these dimensions within the Indonesian context and draws on insights from comparative case studies.

4.1 Strategic and Technical Feasibility of IMSI Catchers

IMSI catchers offer distinct advantages in cyber attribution, particularly when threat actors leverage mobile devices to initiate attacks or manage infrastructures via tethered hotspots, rogue access points, or mobile command-and-control networks. These devices can identify the International Mobile Subscriber Identity of phones in proximity to a given location, providing metadata about user presence and movement (Müller-Maguhn, 2018).

For Indonesia, where attribution remains a key vulnerability in responding to domain hijackings and advanced persistent threats (APTs), IMSI catchers could serve as a bridging technology—linking digital indicators with physical identities. In environments such as public areas or near compromised infrastructure nodes, these tools may assist in pinpointing actors or at least narrowing suspect pools in real-time.

However, the Indonesian cyber defense structure does not currently incorporate SIGINT tools into its incident response workflows. Existing forensic and reactive mechanisms rely heavily on static digital logs, DNS records, and upstream ISP cooperation. These are insufficient when attackers mask their operations via anonymization layers (Rid & Buchanan, 2015). Hence, integrating IMSI catchers could significantly enhance attribution capacity, provided their deployment is surgically targeted and legally constrained.

4.2 Legal and Ethical Considerations in the Indonesian Context

The deployment of IMSI catchers carries significant legal and ethical risks, particularly in jurisdictions lacking robust surveillance oversight. Unlike Singapore and Estonia, Indonesia does not yet have a dedicated legal framework governing the use of SIGINT technologies. Surveillance activities are fragmented across multiple agencies, with overlapping mandates and ambiguous accountability mechanisms (Pratama & Wardhani, 2023).

There is also no explicit legal requirement for judicial authorization prior to deploying surveillance tools in cyber investigations. This raises potential concerns about unconstitutional data collection, especially since IMSI catchers indiscriminately sweep all nearby devices—capturing personal metadata from uninvolved citizens.

International human rights instruments emphasize that digital surveillance must comply with four principles: legality, necessity, proportionality, and oversight (UN Special Rapporteur, 2019). Current Indonesian laws, including UU ITE, do not sufficiently address these principles in the context of modern surveillance tools.

Without institutional safeguards—such as judicial warrant systems, independent audit trails, and parliamentary oversight—there is a high risk that such technologies could be misused for political or extrajudicial purposes. This not only undermines public trust but may also draw international criticism or diplomatic consequences if perceived as violating human rights norms (Deibert, 2020).

4.3 Lessons from Comparative Models

The analysis of Singapore, Estonia, and Israel provides valuable insights into how IMSI catchers can be lawfully and effectively integrated into cybersecurity strategies.

- Singapore employs a centralized cybersecurity command under the Cyber Security Agency (CSA), with surveillance operations authorized through ministerial discretion. This model allows for agility and national coordination but has faced criticism over lack of transparency (Chong & Hall, 2022).
- Estonia demonstrates the importance of legal safeguards. Surveillance is court-approved, and annual

reporting to parliamentary committees

ensures that democratic norms are upheld. This model may be slower to respond in emergencies but provides high levels of legitimacy and public confidence (ENISA, 2020).

- Israel prioritizes operational effectiveness, embedding SIGINT into its broader national defense doctrine. Though efficient, the model lacks civilian oversight and has faced scrutiny over its use of surveillance on domestic populations (Chong & Hall, 2022).

For Indonesia, a hybrid model may be most appropriate—balancing operational needs with legal accountability. For example, surveillance deployments could be limited to specific national security incidents, subject to time-limited judicial warrants, and audited post-incident by a national oversight body.

4.4 Institutional Readiness and Interagency Coordination

One of the major institutional barriers in Indonesia is the lack of structured interagency cooperation. Agencies such as BSSN, Kominfo, and law enforcement often operate in silos. There is no centralized platform for real-time intelligence sharing or coordinated surveillance authorizations. This fragmentation poses risks in the deployment of IMSI catchers, as overlapping operations may compromise evidence integrity or violate procedural norms.

To implement SIGINT technologies responsibly, Indonesia would need to:

- Designate a lead agency (e.g., BSSN) for SIGINT governance.
- Establish interagency protocols for data handling and device deployment.
- Mandate judicial approval through cyber courts or digital oversight units.
- Train law enforcement and cyber investigators in SIGINT-chain of custody practices.

4.5 Public Trust and Democratic Legitimacy

Finally, any surveillance technology that operates in public space inherently carries reputational and legitimacy risks. If improperly deployed or inadequately explained to the public, IMSI catchers may become a symbol of authoritarian overreach rather than national defense.

Public communication strategies, civil society consultation, and third-party audits are essential to ensuring legitimacy. Without these, even legally justified surveillance operations may be perceived as politically motivated or abusive.

V. STRATEGY POLICY RECOMENDATION

Building on the findings of this study, this section proposes a multi-layered policy framework for the lawful, ethical, and operational deployment of IMSI catchers in Indonesia. The recommendations are grouped into five key domains: legal reform, governance structure, operational safeguards, interagency coordination, and public accountability.

5.1 Establish a Legal and Regulatory Foundation

Recommendation 1: Amend or introduce legislation specifically regulating digital surveillance technologies, including SIGINT tools such as IMSI catchers.

5.1.1 This should include explicit definitions, use- case limitations, data handling requirements, and scope of applicability.

5.1.2 The law must incorporate international principles of legality, necessity, proportionality, and oversight (UN Special Rapporteur, 2019).

Recommendation 2: Mandate judicial authorization for all IMSI catcher deployments.

5.1.3 Surveillance operations should require a warrant issued by a designated digital or cyber court, with time-bound validity and clearly stated objectives.

5.1.4 Emergency use should be permitted under exceptional conditions but followed by post- facto judicial review.

5.2 Designate a Centralized Oversight Authority

Recommendation 3: Empower a single national authority (e.g., BSSN) as the lead agency responsible for SIGINT governance in the cyber domain.

5.2.1 BSSN should be responsible for maintaining an inventory of surveillance tools, issuing deployment licenses, and coordinating interagency access.

Recommendation 4: Establish an independent oversight mechanism—such as a parliamentary cybersecurity ethics committee or an ombudsman unit.

5.2.2 This body should review annual surveillance reports, audit selected operations, and provide public transparency through declassified summaries.

5.3 Implement Technical and Operational Safeguards

Recommendation 5: Adopt technical protocols to minimize data overcollection.

5.3.1 IMSI catchers should be configured to exclude irrelevant devices automatically and discard non-target data through onboard filtering.

5.3.2 Where feasible, "catch and release" configurations should be employed, with no storage of data unless a match is found.

Recommendation 6: Establish data handling standards in accordance with global best practices.

- All collected data must be encrypted, access- controlled, and subject to chain-of-custody protocols.
- Retention periods must be strictly defined and monitored, and all non-essential data must be purged immediately.

5.4 Strengthen Interagency Coordination

Recommendation 7: Develop a secure SIGINT coordination platform linking BSSN, Kominfo, national police, and law enforcement units.

5.4.1 This system should include role-based access controls, deployment logs, digital evidence repositories, and incident coordination dashboards.

Recommendation 8: Standardize procedures for cyber incident response that include SIGINT integration.

5.4.2 A national playbook should define when and how IMSI catchers can be deployed during high-priority incidents like domain hijackings, ransomware attacks, or foreign state-attributed operations.

5.5 Promote Transparency and Public Trust

Recommendation 9: Publish annual transparency reports on the use of SIGINT tools in cybersecurity operations.

5.5.1 These reports should include aggregate statistics (e.g., number of deployments, types of incidents addressed), with case summaries where permissible.

Recommendation 10: Engage with civil society, privacy advocates, and academic experts in reviewing surveillance frameworks.

5.5.2 Periodic public consultations can improve social acceptance, ensure the system is not abused, and create a channel for civil redress in case of misuse.

VI. CONCLUSION

Indonesia's digital transformation has elevated the strategic importance of cybersecurity within its national defense and public governance agendas. The hijacking of government domains by criminal or politically motivated actors reveals critical gaps in the country's ability to detect, attribute, and respond to cyber threats effectively. Traditional cybersecurity tools—while necessary—are often reactive and insufficient for attribution, especially in a threat landscape shaped by anonymization and transnational infrastructure.

This study has demonstrated that signal intelligence technologies, particularly IMSI catchers, offer a viable complement to Indonesia's cybersecurity toolkit. These tools, when integrated into national cyber incident response, can enhance attribution capabilities by bridging digital evidence with physical identifiers. However, their deployment must be strictly governed by principles of legality, necessity, proportionality, and democratic oversight.

Drawing on international experiences from Singapore, Estonia, and Israel, the research offers a tailored policy framework for Indonesia that addresses legal, ethical, and operational dimensions. Recommendations include the establishment of a judicial warrant system, centralization of SIGINT governance under BSSN, interagency coordination protocols, and transparency mechanisms to safeguard civil liberties.

Ultimately, the successful integration of SIGINT tools into Indonesia's cyber defense posture hinges not only on technical readiness but also on public legitimacy, institutional maturity, and a rights-respecting legal foundation. If these elements are achieved in tandem, IMSI catchers and similar technologies can serve not as instruments of repression, but as tools of lawful protection in a volatile and contested digital landscape.

REFRENCES

[1]. Badan Siber dan Sandi Negara. (2022). Laporan Tahunan Keamanan Siber Nasional 2021. Jakarta: BSSN.

[2]. Chong, A., & Hall, I. (2022). Cybersecurity in Asia: Policy and Practice in the Digital Realm. Routledge.

[3]. Deibert, R. (2020). Reset: Reclaiming the Internet for Civil Society. House of Anansi.

[4]. ENISA. (2020). Threat Landscape Report 2020: Cyber Threat Intelligence. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa- threat-landscape-2020

[5]. Freedom House. (2021). Freedom on the Net: Indonesia. https://freedomhouse.org

[6]. Müller-Maguhn, A. (2018). IMSI-Catchers: Technological function and legal context. International Journal of Cyber Forensics, 12(2), 77–89.

[7]. Pratama, Y. H., & Wardhani, F. (2023). Evaluasi kebijakan nasional dalam penggunaan perangkat intelijen sinyal. Jurnal Pertahanan Siber Indonesia, 2(1), 45–59.

[8]. Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. Journal of Strategic Studies, 38(1–2), 4– 37. https://doi.org/10.1080/01402390.2014.977382

[9]. Schneier, B. (2019). Click Here to Kill Everybody: Security and Survival in a Hyper- connected World. W. W. Norton & Company.

[10]. Singh, A., & Krishnan, A. (2021). Cyberattacks on government portals in the Asia-Pacific: Trends and policy gaps. Asian Journal of Cybersecurity Studies, 3(1), 25–40.

[11]. UN Special Rapporteur. (2019). Report on the right to privacy in the digital age (A/HRC/40/63). United Nations Human Rights Council. https://www.ohchr.org/en/documents/thematic- reports/ahrc4063-right-privacy-digital-age- report-special-rapporteur