UDC 355; DOI 10.18551/rjoas.2023-12.01

STRATEGY MODEL OF CYBER INTELLIGENCE STAKEHOLDERS FOR STRENGTHENING CYBER DEFENSE TO ACHIEVE NATIONAL RESILIENCE

Purnomo Widyanto Pudyo*
Doctoral Program of Resilience Studies, University of Brawijaya, Malang, Indonesia

Moeljadi
Faculty of Economics and Business, University of Brawijaya, Malang, Indonesia

Kusumaningrum Adi
Faculty of Law, University of Brawijaya, Malang, Indonesia

Aminuddin M. Faishal
Faculty of Social and Political Sciences, University of Brawijaya, Malang, Indonesia

*E-mail: widhi9843al@gmail.com

ABSTRACT

This research aims to analyze the stakeholders of cyber intelligence for strengthening cyber defense to achieve national resilience. This research is important because cyber intelligence stakeholders play a role as policymakers, coordinators, facilitators, implementers, and policy accelerators in the field of cyber security and defense, influencing the realization of national resilience. This research was conducted using a qualitative descriptive approach to cyber intelligence stakeholders consisting of the Indonesian Armed Forces Intelligence Agency (BAIS TNI), the State Intelligence Agency (BIN), the Ministry of Communication and Information Technology (Kominfo), the Indonesian National Police Intelligence and Security Agency (Baintelkam Polri), and the National Cyber and Encryption Agency (BSSN), using SWOT analysis. Research data were obtained from interviews and surveys with stakeholders related to the cyber field, who have direct involvement and contribution to cyber defense policy. It is expected that this research can provide a model strategy for stakeholders who have influence and interests in cyber security, as well as the interconnection between the roles of Cyber Intelligence actors in strengthening Indonesia's cyber security measures. The results of the research show that cyber intelligence stakeholders as policymakers and implementers of cyber defense policies can provide significant benefits and influence on strengthening national resilience through the formulation of national policies in the field of cyber defense.

KEY WORDS
Cyber intelligence, Indonesia, Intelligence stakeholders, national resilience, SWOT analysis.

In the 21st century, when humans began to enter the information era which utilizes information and communication technology, at that moment new threats emerged. The threat is not only persistent conflict between countries. Rather, there is the threat of conflict between states and proto-states, state actors and non-state actors, even between states and individuals who have sufficient resource capabilities. The American Defense Department defines cyberspace as: A global domain within the information environment consisting of the independent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers (Murphy 2010). Meanwhile, according to Minister of Defense Regulation No. 82 of 2014 about Cyber Defense, a cyberspace is defined as: "A space where communities are connected using networks (for example the internet) to carry out various daily activities." Electronic systems, including internet networks, are currently used to support various activities in the business, trade, health services, communications and government sectors.

The increasingly widespread and increasing use of information and communication technology via the internet network is also accompanied by increased threat activity. The emergence of social media allows internet users to create content rather than just consuming material in cyberspace. The cyberspace that includes social media is no longer just a tool for sharing photos of family vacations and food. Social media devices and applications are available to everyone with a computer or smartphone. Both are increasingly used as effective weapons by many people on different sides of the conflict. Militaries and civilian organizations increasingly feel the need to increase their effectiveness in monitoring their adversaries by using cyber space, defending themselves against ongoing social media attacks, and using cyber media as a weapon in pursuing their own goals.

Indonesia has made significant progress in the digital field in recent years. Indonesia's position in the current progress of the digital world can be explained in several aspects, first, internet penetration. The number of internet users in Indonesia continues to increase rapidly. According to the latest data, more than 70% of Indonesia's population is connected to the internet. This illustrates the high adoption of digital technology in the country. Second, E-commerce Growth. E-commerce has grown rapidly in Indonesia. Platforms such as Tokopedia, Bukalapak, and Shopee have achieved great success in the Indonesian market. Third, Start-ups and Technological Innovation: Indonesia has seen extraordinary growth in the start-up ecosystem and technological innovation. Technology companies such as Go-jek, Tokopedia, and Traveloka have succeeded in achieving "unicorn" status with valuations of billions of US dollars. Fourth, Digital Finance: Digital financial services such as digital wallets and online payments have become widespread in Indonesia. Platforms such as GoPay, OVO, and Dana have become an integral part of the daily lives of many people in Indonesia. Fifth, Government Transformation: The Indonesian government has also been active in encouraging digital transformation in various sectors. Initiatives such as digital payments for public services, online services, and smart city development have been introduced to improve the efficiency and accessibility of public services.

As a country with rapid digital progress, Indonesia also faces the increase of cyber-attacks. Some of the most up-to-date cyber-attack threats in Indonesia such as Ransomware attacks, DDoS attacks, Phishing attacks, Malware and Botnet attacks also targeted attacks. A ransomware attack is an attack in which hackers encrypt user data or a computer system, then demand a ransom payment to obtain the decryption key. Ransomware attacks such as WannaCry and Petya have hit Indonesia in previous years, disrupting business and organizational operations. DDoS Attack: A Distributed Denial of Service (DDoS) attack is an attack in which hackers use a network of infected computers to attack a target system with very high internet traffic, thereby making the system inaccessible to legitimate users. DDoS attacks can cause significant downtime and harm online businesses and services. A phishing attack is an attempt to obtain sensitive information such as passwords, credit card numbers, or personal data by impersonating a trusted entity via email, instant messaging, or a fake website. Phishing attacks are often used for identity theft and financial fraud. Malware and Botnet Attacks: Malware attacks involve sending malicious software to a target system to damage or steal data. A botnet is a network of computers infected with malware that hackers can control remotely. Botnets are often used to launch DDoS attacks or for other illegal activities. A targeting attack is attack that aimed at a specific individual, organization or infrastructure. These attacks can involve high-target attacks such as financial institutions, large corporations, or governments, and often involve sophisticated techniques such as spear-phishing, identity spoofing, or zero-day attacks.

As long as increasing digital progress in Indonesia, the existence of threats in cyber space is also increase and requires comprehensive handling. In this situation, security institutions/agencies, including intelligence agencies, require a multidimensional approach to carry out their duties in cyberspace. Multi-dimensional aspects in handling cyber security and defense such as policy, institutions (governance), technology and infrastructure, and Human Resources. In the case of cyber threats in Indonesia, the most vulnerable factors are cyber intelligence policy and institutional factors which involve the role of cyber intelligence stakeholders (Darmawan, Poniman, and Gultom, 2021). Therefore, intelligence agencies have specific characteristics that are visible in their relationships with other government organizations that will shape their approach to stakeholders.

The originality and novelty presented in this research is the formulation of a strategy model for intelligence stakeholders involved in cyber defense in Indonesia involving a number of agencies or institutions. This certainly has a very significant impact on handling cyber security. This research aims to understand what strategy models are being implemented by cyber intelligence stakeholders as well as analyzing cyber intelligence governance in the defense and security landscape of cyber space, as well as understanding whether government policy products in the field of cyber security are able to strengthen Indonesia's cyber resilience from various threats and challenges that come.

METHODS OF RESEARCH

This research uses a qualitative descriptive research method. The qualitative research method according to (Moleong, 2012) was chosen because it is aimed at describing and analyzing phenomena, events, social activities, attitudes, beliefs, perceptions, thoughts of people individually and in groups. The data that will be used in this research are 1) primary data, were obtained from the first data source at the research location or research object; 2) Secondary data, were obtained from a second source or secondary source of the data needed (Bungin, 2017). In this research, literature studies were collected to complete the information as material for analysis. This research was carried out in government agencies that have cyber intelligence and cyber counterintelligence functions such as the Indonesian Ministry of Defense, BIN, BAIS, BSSN, and Baintelkam POLRI. SWOT analysis as a tool for understanding problems. (Duvenage, 2010) in his thesis said that SWOT analysis is generally used by various organizations to evaluate the Strengths, Weaknesses, Opportunities and Threats involved in a project or plan of action.

RESULTS AND DISCUSSION

Cyber Intelligence stakeholders in Indonesia who play a role in carrying out cyber defense and security governance include five (5) main stakeholders, namely BIN, BSSN, National Police Cybercrime, TNI Cyber Unit and Ministry of Defense Cyber Security. Cyber intelligence stakeholders carry out their functions and roles as part of the cyber defense system to support National Resilience. Indonesian National Resilience is the dynamic condition of the Indonesian nation which covers all aspects of integrated national life, contains tenacity and toughness which contains the ability to develop national strength, in facing and overcoming all challenges, threats, obstacles and disturbances both coming from outside and from within, to guaranteeing the identity, integrity, survival of the nation and state as well as the struggle to achieve national goals (Lemhanas RI, 2016). Meanwhile, the special tasks of the intelligence agency are: (1) Providing analysis in areas relevant to national security, (2) Providing early warning of threatening crises, (3) Assisting in the management of national and international crises by detecting the desires of opposing parties or other parties which have potential opposing parties, (4) Providing information for national security planning needs, (5) Protecting classified information, and (6) Carrying out counter-intelligence operations (Asri, S., Juniarto.D.,Irianto, I. 2008).

The following are the positions and roles of cyber intelligence stakeholders in Indonesia: (a.) BIN as the national intelligence coordinator acts as the primary stakeholder carrying out the role of coordinator; (b.) BSSN as a key stakeholder, carries out the role of policy creator and facilitator; (c.) Central Defense Cyber of the Ministry of Defense as a key stakeholder, carrying out the role of policy creator; (d.) Cybercrime Police as a supporting stakeholder/secondary stakeholder, carries out the role of facilitator; and (e.) TNI Cyber Unit as a supporting stakeholder/secondary stakeholder, carries out the role of facilitator.

Factors that influence in strengthening cyber defense for national resilience are including five things. These five things are legal certainty (legal measures), technical and procedural aspects, organizational structure, capacity building and international cooperation.

If the five pillars are further elaborated in the context of the national interests of each jurisdiction, they can be explained as follows: (a.) Legal certainty means the need for a country to have national legislation starting from national cyber security policy and strategy documents which contain details of cyber security implementation planning to various laws and regulations that support it; (b.) Technical and procedural aspects that focus on elaborating on standardization, protocol accreditation and focusing on finding vulnerabilities in software for cyber security; (c.) Organizational structure created in order to create strategies and implementation to prevent, detect and respond to all forms of attacks on critical information infrastructure; (d.) Capacity building, namely focusing on increasing the understanding and expertise of cyber security personnel to further encourage the success of the goals of the national cyber security policy agenda; (e.) International cooperation, namely the urgency of each country to involve itself in cooperation, dialogue and coordination in responding to the latest dynamic issues of cyber security.

National cyber resilience is an increasingly important issue in this digital era. Cyber threats were increasingly complex mean that every country must strengthen their cyber defenses. One way to do this is to build a robust cyber intelligence stakeholder strategy model. The cyber intelligence stakeholder strategy model integrates various parties who have an important role in securing the country's cyber space, such as government, the private sector, academics and civil society. In this model, stakeholders work together to analyze and predict potential cyber threats, as well as respond to cyber-attacks that occur. One of the advantages of the cyber intelligence stakeholder strategy model is that it allows stakeholders to share information and resources effectively. To build an effective cyber intelligence stakeholder strategy model, there are several steps that can be taken. First, stakeholders must recognize and understand each other's roles in national cyber defense. Second, they need to develop secure and trusted information and communication platforms to facilitate the exchange of information and coordination of actions. Third, they must have strong analytical and predictive capabilities to monitor and identify potential cyber threats. Fourth, they must have rapid and effective response and recovery capabilities in responding to cyber-attacks.

As an example of the cyber intelligence stakeholder strategy model implementation in Indonesia, the Indonesian government could hold a national cyber stakeholder forum involving various related parties, such as government institutions, private companies, academics and civil society. These forums can be used to share information, identify cyber threats, and develop coordinated response plans.

Besides, Indonesia can also build a national cyber intelligence center to monitor cyber threats in real-time and respond quickly to cyber-attacks. This cyber intelligence center can be equipped with sophisticated technology and a team of experts trained in cyber threat analysis and prediction.

In this increasingly complex and rapidly developing digital era, national cyber resilience is becoming increasingly important. The cyber intelligence stakeholder strategy model can be an effective way to build a strong national cyber defense. By building strong collaboration between stakeholders, Indonesia can strengthen national cyber defense and protect national interests from increasingly complex and increasing cyber threats. Through the cyber intelligence stakeholder strategy model, Indonesia can build an effective and coordinated national cyber defense between the government, private sector, academics and civil society.

Collaboration between stakeholders in this strategy model allows them to share information and resources to identify and respond to cyber threats that occur. In the Indonesian context, this is very important considering that Indonesia is the country with the largest number of internet users in the world, so its vulnerability to cyber-attacks is even greater.

However, the cyber intelligence stakeholder strategy model also has challenges and obstacles that need to be overcome. One of the main challenges is the lack of awareness and understanding of the importance of cyber security among the public. Therefore, education and outreach regarding cyber security needs to be improved so that people can better understand the importance of protecting personal data and cyber security in everyday life. Besides, there is also a need for support from the government in building cooperation and collaboration between stakeholders. The government needs to demonstrate clear policies and regulations to strengthen cooperation between stakeholders in building national cyber defense.

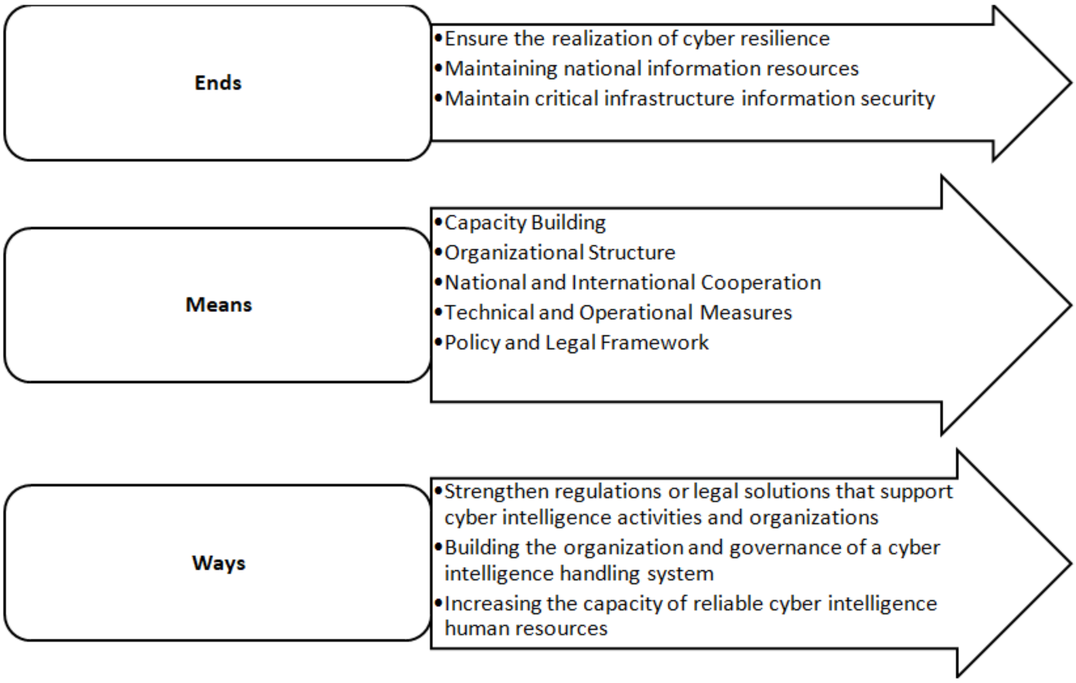

Ends
•Ensure the realization of cyber resilience
•Maintaining national information resources
•Maintain critical infrastructure information security
Means
•Capacity Building
•Organizational Structure
•National and International Cooperation
•Technical and Operational Measures
•Policy and Legal Framework
Ways
•Strengthen regulations or legal solutions that support cyber intelligence activities and organizations
•Building the organization and governance of a cyber intelligence handling system
•Increasing the capacity of reliable cyber intelligence human resources

Figure 1 – National Cyber Intelligence Stakeholder Strategy (Source: Research Data, 2023)

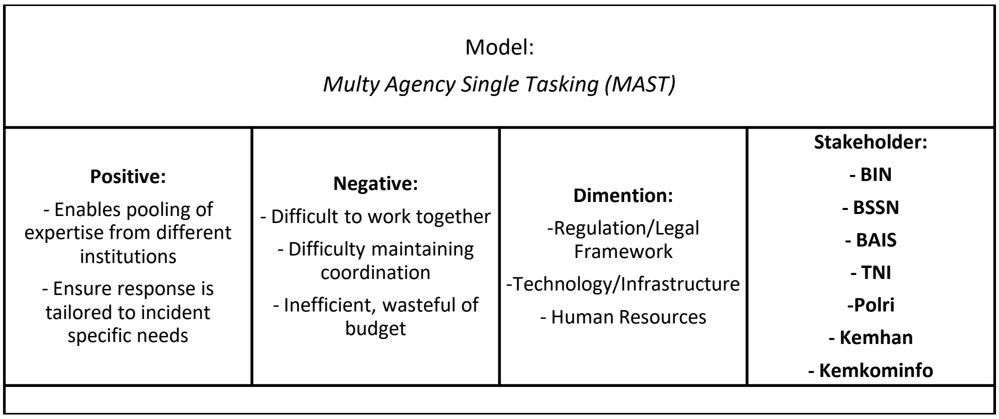
Overall, the cyber intelligence stakeholder strategy model can be an effective way for Indonesia to build a strong national cyber defense. By building collaboration between stakeholders and strengthening public awareness regarding cyber security, Indonesia can protect national interests from increasingly complex and increasing cyber threats.

In explaining the interaction patterns that exist between authorized institutions about cyber security issues in Indonesia, Arthur Himmelman's inter-agency working theory perspective can be applied in the context of interoperability strategies between cyber intelligence stakeholders. According to Himmelman, there are four patterns of interaction implemented between institutions, there are: networking, coordination, cooperation and collaboration. Networking means that interactions occur solely in the form of exchanging information. Meanwhile, coordination is networking but is accompanied by a change as a result of the exchange of information. Furthermore, cooperation is defined as networking and coordination accompanied by the sharing of resources between related institutions. Finally, collaboration is considered the most perfect interaction pattern because it is a combination of the three previous elements and is added to by increasing the activities of certain agencies which mutually benefit other agencies (Himmelman, 2002). From this theory, it can be identified what kind of interaction patterns exist between the institutions mentioned above.

The existence of a number of institutions or ministries that have similar authority as if the case in the context of cyber security in Indonesia is usually referred to as Multi Agency Single Task (MAST). This governance concept means that there are more than two institutions that have the same authority in a country. The magnitude of the task and scope of authority are usually the main reasons why this concept is chosen by the country. In contrast to MAST, the Single Agency Multi Task (SAMT) concept means that there is only one agency that is given overall authority within a bureaucratic scope.

Both concepts have advantages and disadvantages. SAMT has advantages over MAST in terms of effectiveness because there is unity of command and there will be no conflicts of interest between institutions. Besides, SAMT is also more cost efficient because the allocated budget will only be concentrated in one institution. However, SAMT requires comprehensive training and development of human resource capacity so that they can carry out various types of tasks. Things like this are not found in the MAST concept, the responsibility for developing human resource capacity is handed over to each institution and is only focused on and only focuses on one particular aspect of expertise. Based on an organizational point of view, SAMT will also give birth to a fatter bureaucracy because of its wide territorial coverage and work authority. There is no certainty which concept is better. The choice between these concepts will depend greatly on the conditions of each country.

Table 1 – Current National Cyber Intelligence Strategy Approach (Existing Condition)



Model: *Multy Agency Single Tasking (MAST)*			
Positive: - Enables pooling of expertise from different institutions - Ensure response is tailored to incident specific needs	**Negative:** - Difficult to work together - Difficulty maintaining coordination - Inefficient, wasteful of budget	**Dimention:** -Regulation/Legal Framework -Technology/Infrastructure - Human Resources	**Stakeholder:** **- BIN** **- BSSN** **- BAIS** **- TNI** **-Polri** **- Kemhan** **- Kemkominfo**

Source: Processed by researchers (2023).

If looking at the current state of cyber intelligence governance, the Indonesian government is implementing a Multi-Agency Single Task (MAST) strategy, with a number of stakeholders playing the most prominent roles, including BIN, BSSN, BAIS, TNI, Ministry of Defense and Ministry of Communication and Information. With this kind of pattern, there are actually several benefits that can be achieved, one of which is that the MAST pattern can enable the pooling of resources and expertise from various institutions. This pattern can also help improve communication and coordination between various agencies and can help to ensure that the response is tailored to the specific needs of the incident.

However, the MAST pattern also has several disadvantages, one of which is that with the MAST approach it will be difficult to get different agencies to work together. This has been proven in accordance to data from a number of sources who revealed that the pattern of synergy and coordination between institutions did not run smoothly, and some institutions even did not have written cooperation agreements between cyber institutions in Indonesia. Difficulty in maintaining coordination between different institutions is often a classic problem in national defense and security discourse. For this reason, currently the DPR is still working on the Cyber Security Bill which will regulate the synergy and governance of cyber security which will cover the area of national cyber security authority in Indonesia, covering 6 (six) areas, such as: cyber defense, cybercrime, cyber intelligence, cyber security, cyber resilience and cyber diplomacy. Finally, a crucial problem with the MAST pattern is that budget waste often occurs, because these many institutions require large budgets, and are often not on target. The problem becomes more complicated when there is a change in structure, then there are policy changes which often annul previous policies, so that budget swelling continues to occur, while policy strategies always change and never work consistently.

Based on field data, the issue of coordination and synergy between cyber institutions that have intelligence divisions and intelligence institutions that have cyber divisions is only carried out to the extent of synergy in policies and strategies at the top level. Synergy has not been implemented in carrying out investigations or exchanging information. Overall cooperation has not occurred between the ministry and cyber intelligence agencies.

The State Intelligence Agency stated that there has been no overlap between institutions in dealing with cyber threats this time. The implementation of the duties of each institution is in accordance with applicable laws. The resource person explained that if there was no overlap then the search for information related to cyber handling would have been carried out effectively and precisely.

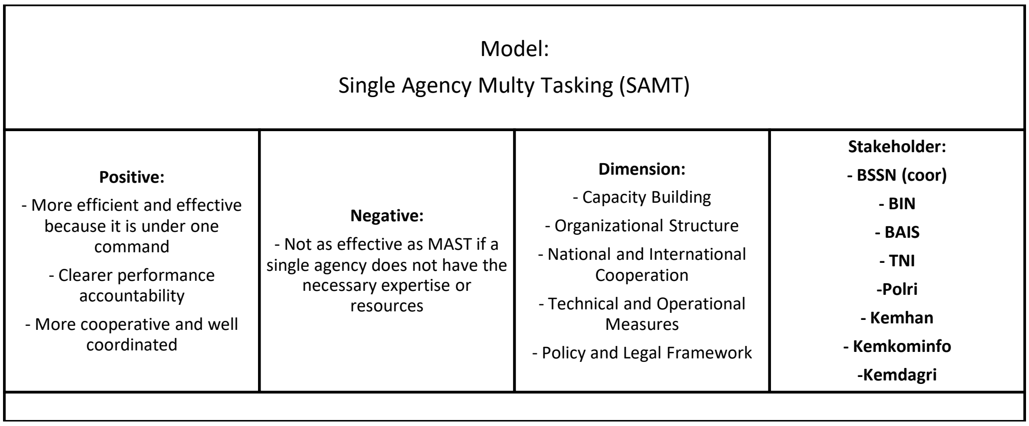
The National Cyber and Crypto Agency said that synergy had also been carried out well. Collaboration has been established between ministries and institutions that handle cyber intelligence. The National Cyber and Crypto Agency itself has entered into formal and unofficial cooperation agreements with other institutions. The National Cyber and Crypto Agency always involves other agencies in every meeting, training, seminar or other cyber event.

The Ministry of Defense's Cyber Defense Center, the TNI Cyber Unit and the National Police's Cyber Crime Unit stated that the synergy that exists is not very effective when viewed at this time. This is because the synergy that carried out is only limited to the top level, was through mergers or cooperation in policies and strategies or work programs, there is no synergy for cyber intelligence operations. beside from secret intelligence, each ministry and agency has its own goals, objectives and programs. Cyber threats are currently still considered to be able to be handled by each agency without cooperation.

Based on explanations from sources at the State Intelligence Agency, the effectiveness of the synergy of these cyber intelligence institutions, if it measured, it has a scale value of 7-8 out of 10. Because cyber intelligence institutions such as the National Cyber and Crypto Agency are already open in handling cyber threats. and has invited other institutions such as the State Intelligence Agency to discuss and communicate together towards cyber threats.

The following is a table of SAMT (Single Agency Multi Task) strategies, which can be applied in intelligence and cyber security governance in Indonesia:

Table 2 – SAMT Pattern National Cyber Intelligence Strategy Approach



Model: Single Agency Multy Tasking (SAMT)			
Positive: - More efficient and effective because it is under one command - Clearer performance accountability - More cooperative and well coordinated	**Negative:** - Not as effective as MAST if a single agency does not have the necessary expertise or resources	**Dimension:** - Capacity Building - Organizational Structure - National and International Cooperation - Technical and Operational Measures - Policy and Legal Framework	**Stakeholder:** **- BSSN (coor)** **- BIN** **- BAIS** **- TNI** **-Polri** **- Kemhan** **- Kemkominfo** **-Kemdagri**

Source: Processed by researchers (2023).

By adopting the SAMT pattern, there are a number of advantages that can be achieved, including: (a) It can be more efficient and effective than MAST, because it allows one institution to lead the response; (b) It can be easier to get different agencies to agree to the SAMT approach; (c) and can reduce the budget more effectively, because all needs can be centralized and adjusted to priority needs and national strategies. The downside of this approach may not be as effective as MAST if a single agency does not have the necessary expertise or resources. Additionally, the strategy pattern with the SAMT approach may not be as coordinated as MAST, as there may be little communication and cooperation between different agencies.

The transition from MAST to SAMT can be a complex process, as it requires a change in mindset and culture among the institutions involved. However, there are a number of benefits to making the transition from MAST to SAMT:

1. Efficiency: The SAMT approach can be more efficient than the MAST approach, as it allows one agency to take the lead in the response. This can help avoid duplication of

effort and ensure that resources are used more effectively;

2. Effectiveness: The SAMT approach can be more effective than the MAST approach, as it allows one agency to have a better understanding of the incident and the resources needed to respond. This can help to ensure that the response is tailored to the specific needs of the incident;
3. Coordination: The SAMT approach can be more coordinated than the MAST approach, as the need for communication and cooperation between different agencies is reduced. This can help ensure that responses are in time and effective.

However, there are definitely challenges that will be faced if the transition is carried out from the MAST strategy model as has been going on for a long time, to the new approach towards unification adopted in the SAMT strategy model. These are the following:

1. Mindset: The transition from MAST to SAMT requires a change in mindset among the agencies involved. Agencies must be willing to give up some of their control and authority for the transition to be successful;
2. Culture: The transition from MAST to SAMT also requires a cultural change among the institutions involved. Agencies must be more collaborative and less territorial for the transition to be successful;
3. Resources: Transitioning from MAST to SAMT may require additional resources, such as training and funding. Agencies need to be prepared to invest in these resources for a successful transition.

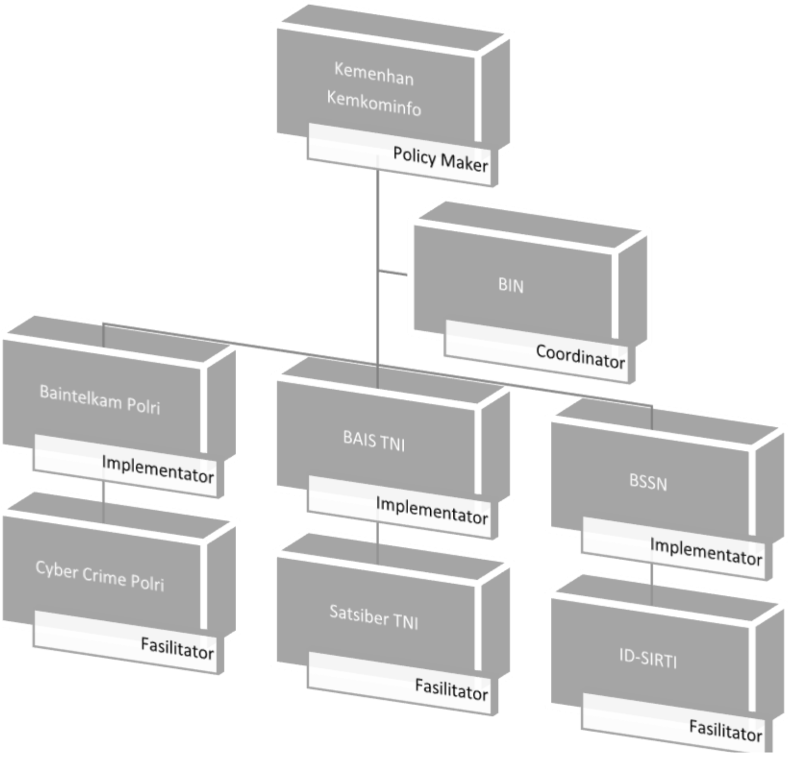


Figure 2 – Cyber Intelligence Stakeholder Strategy Model (National Cyber Intelligence Center)
Source: Data Researchers' Process (2023)

In order for the transition process to run smoothly, beside from strengthening regulations and legal frameworks, a number of efforts are needed so that the transition process from the MAST pattern to the new strategy pattern can be successful. The first step can be taken by starting to build relationships between the institutions involved. This will help create a foundation of trust and cooperation that is essential for a successful transition. The second step, it is necessary to prepare a clear transition plan. This plan should include a timeline, milestones, and necessary resources.

The third step, by providing training to related agencies. This training will help build an understanding of the SAMT approach and how it works. Fourth step, Providing a budget for the transition. These funds will be needed to cover training, development, infrastructure and other resource costs. The fifth step requires monitoring the transition process objectively and thoroughly and making adjustments as needed. The transition from MAST to SAMT is a complex process, and it is important to monitor progress and make adjustments as needed. Transitioning from MAST to SAMT can be a challenging process, but it can also be a rewarding one. By following the steps above, it is hoped that the chances of making the transition successful will be greater.

With the SAMT (Single Agency Model Task) approach, the cyber intelligence stakeholder structure model will be depicted as above. Furthermore, based on the orders of the law, by being included in the Cyber Security Bill, a National Cyber Intelligence Center was formed under the coordination of two ministries, there are the Ministry of Communication and Information and the Ministry of Defense as supervisors and policy makers. The two ministries will collaborate with other ministries/institutions. will become the leading sector by assigning the State Intelligence Agency (BIN) as Coordinator, as mandated by the applicable law. BIN is the coordinator and implementer in cyber intelligence governance. BIN carries out investigations, security, mobilization, monitoring, covert action and analysis of cyber threats. In collaboration with the National Police's intelligence unit which handles intelligence issues that focus on state security. Meanwhile, BAIS TNI, which has authority over national defense intelligence matters, will carry out its main duties and functions as combat/military intelligence and handle cyber warfare. BSSN, which manages the national cyber security system, is tasked with implementing cyber security effectively and efficiently by utilizing, developing and consolidating all elements related to cyber security. Meanwhile, under the next line of coordination, National Police's intelligence unit is also assisted by Cyber Crime Police as a facilitator/supporter. Cybercrime The National Police is tasked with preventing all forms of crime in cyberspace that could occur, such as the spread of hoax news, hate speech, and even the security of personal information data. Meanwhile, the TNI BAIS is strengthened by the TNI Cyber Unit. The TNI Cyber Unit is tasked with carrying out cyber activities and operations in military environment in order to support the main tasks of the TNI.

BSSN is supported by Id-SIRTII/CC (Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center). Id-SIRTII which will help organize Cyber Incident Response Team services in accordance with the needs for handling National Cyber Incidents; Become a national level coordination center for handling Cyber Incidents; Formulate technical guidelines for handling National Cyber Incidents; Carry out registration of the Cyber Incident Response Team; and build and manage a Cyber Incident database from all registered Cyber Incident Response Teams and information regarding Cyber Incidents at the national level; as well as being a national contact person and representing the country at regional and international levels.

The National Cyber Intelligence Center is directly under the control of the president, as a holistic user and covers all areas of national defense, security and intelligence. The cyber security context is related to national defense and security. The Internet basically brings fundamental changes in the interaction of society, government in providing services, business expansion and individual transactions. While the internet brings enormous benefits, saves costs, and brings efficiency there are great threats. For this reason, it is hoped that the National Cyber Intelligence Center will be able to carry out its duties of detecting and deterring all potential threats.

Cyber threats can damage national interests, endanger the functioning of industry and harm individual users or end users. This will create a position of cyber security as an important element of national security. This can be translated into state policy through regulatory initiatives aimed at protecting public, private and individual property rights.

Cyber intelligence governance with reference to national security aspects must be able to accommodate the needs and beliefs of the community. Handling problems in the cyber domain in Indonesia is currently still not integrated and integrated, so governance is still partial. Seeing these conditions, the vulnerability gaps in the cyber domain are still clearly visible. This will be a threat to cyber resilience and security for society, corporations and public service providers which of course can have a strategic or systemic impact, so that in itself it will affect the stability of the nation, the consequences of which are also threats to aspects of ideology, politics, economics, socio-culture, defense and security. In the era of internet-based information and social media, cyber security is closely related to ideological, political, economic, social, cultural, defense and security stability, and even state sovereignty. For example, cyber-attacks on Iran's nuclear reactors (stuxnet case) and crypto ransom attacks on the transportation and health sectors (wannacry case). However, one of the most dangerous types of cyber-attacks that can disrupt national stability is often not direct cyber-attacks on system installations or computer equipment, but rather through social engineering propaganda via internet media.

Therefore, the presence of the state to integrate the management of the cyber domain is absolutely necessary to prevent threats to aspects of national and state life. The presence of the state in order to protect its citizens and maintain state sovereignty, especially in the cyber domain, is with a more effective strategic model and is strengthened by the formation of a bill in the field of cyber security as a legal umbrella in the cyber sector and functions to determine national cyber policy with the role and cooperation of the government, the private sector, and also Indonesian people.

CONCLUSION

The Cyber Intelligence stakeholder strategy model in the current efforts to implement cyber defense in strengthening National Resilience is still based on the Multi Agency Single Task (MAST) pattern by developing on three main sides, such as the people, process and technology sides. This MAST approach means that many institutions/agencies have similar or even overlapping authority in the governance of national cyber intelligence. The current strategy model using the MAST approach has a number of prominent weaknesses, such as weak coordination and wasteful budgeting. The strategy model currently adopted also occurs because there is no regulation or legal framework that can ensure that all cyber intelligence elements or stakeholders can work in a structured and well-organized manner. Based on current conditions, it is necessary to formulate a new approach that is more functional and effective in accordance with the global cyber security agenda, by adopting a strategy model with a Single Agency Multi Task (SAMT) approach. The transition from the MAST pattern to the SAMT pattern can be carried out according to a number of stages. This strategy model can work well if the Cyber Security Bill as a legal framework has been passed as a form of strengthening national cyber resilience.

REFERENCES

1. Asri, S., Juniarto. D., Irianto, I. 2008. Singapore's International Political Economic Policy Strategy towards Hong Kong (In Indonesian). Pekanbaru: ISDP.
2. Bungin. 2017. Qualitative Research Methods (In Indonesian). Depok: PT. Raja Grafindo.
3. Darmawan, N., Poniman, A., Gultom, R.A.G. 2021. The concept of developing cyber security defense technology based on the six ware framework at the command headquarters of the Indonesian National Army Navy base in Palu (In Indonesian). Jurnal Teknologi Penginderaan, 3(2), 48-49.
4. Duvenage, D. 2012. Analyst Strategic Indicators. Foreknowledge. February 2012.
5. Himmelman, A. T. 2002. Collaboration for A Change, Definitions, Decision Making Models, Roles And Collaboration Process Guide.
6. Lemhannas RI. 2016. Lemhannas RI study April 2016 (In Indonesian). Jurnal Kajian Lemhannas RI, 26, 1–83.
7. Murphy, E.,Gibson, J.W.,Greenwood, R. 2010. Analyzing Generational Values among Managers and Non Managers for Sustainable Organizational Effectiveness. SAM Advanced Management Journal, 75(1), 33-35.
8. Moleong, L. J. 2012. Qualitative Research Methods. PT Remaja Rosdakarya.
9. Minister of Defense Regulation No. 82 of 2014 Concerning Cyber Defense.