TECHNIUM
SOCIAL SCIENCES JOURNAL

Vol. 38, 2022

A new decade for social changes

www.techniumscience.com

ISSN 2668-7798

TECHNIUM SOCIAL SCIENCES JOURNAL

Technium Social Sciences Journal
Vol. 38, 87-102, December, 2022
ISSN: 2668-7798
www.techniumscience.com

Collaboration of ministries/institutions and the private sector in handling cyber threats through the establishment of *Computer Security Incident Response Team* (CSIRT)

Husni Rohman[1], Sumarna[2], Suwanda[3] , Widya Leksmanawati[4]

[123]Student in Magister Program, Faculty of Administrative Science, Universitas Indonesia, [4]Doctor of Faculty of Administrative Science, Universitas Indonesia

husnirohman86@gmail.com , sumarna.amar@gmail.com , wandachb@gmail.com , widyal@ui.ac.id

Abstract. The writing of this article aims to describe how the coordination efforts of Ministries / Institutions and the Private Sector in handling cyber threats through the formation of a *Computer Securtiy Incident Response Team* (CSIRT). The research method used is a qualitative method through the study of literature from various reference sources and other documents. The writing of this article is descriptive and explanatory to obtain facts and describe a comparative analysis of cyber threat handling policies through CSIRT in various countries with Indonesia. The secondary data used are obtained not from direct observation but rather obtained from several previous studies such as research reports and other important documents. The result of this research is how collaboration is carried out by Ministries/Institutions and the Private Sector in handling cyber threats through the formation of a Cyber Incident Response Team organization.

Keywords. Cyber threats, *CSIRT*, Cyber Incidents, Cyber Incident Response Team

I. Introduction

1.1 Indonesian Internet Users

The Covid-19 pandemic that occurred in the world and in Indonesia had an impact on various economies around the world, including Indonesia. This also has an impact on adapting people's activities to often carry out online activities both for work, study, buying and selling transactions, socializing and so on so that during the Covid-19 period there was an increase in activities carried out using the internet or online activities. According to data from the Indonesian Internet Service Providers Association (APJII) in 2022, the number of internet users is around 210.02 million people or around 77.02% of the total population of Indonesia in 2021 around 272.68 million people.(APJII, 2022)

Based on this data, it indicates that the development of technology and communication has become inseparable from the activities of the Indonesian people who use cellular / internet network technology in the current era of the industrial revolution. Internet speed test application development company Ookla noted an increase in the need for average internet connection speed in Indonesia in 2022, for cellular networks by 15.82 Mbps or an increase of 3.40 Mbps

Technium Social Sciences Journal
Vol. 38, 87-102, December, 2022
ISSN: 2668-7798
www.techniumscience.com

(27.4 %), while for networks there remained an increase of 20.13 Mbps or an increase of 4. 04 Mbps (25.1%) . The use of the internet in Indonesia is generally used for daily community activities such as work, social interaction, access to public services, (Ookla, 2022)trade, banking, education to entertainment. Based on research conducted by Hootsuite, one of the content management service companies in Indonesia, it is noted that Indonesia is ranked 8th as a country that uses social media to support work activities. (Hootsuite, 2022) From the description of this explanation, it can be interpreted that most of the activities of people in Indonesia rely on the internet or commonly known as the *Internet of Thing* (IOT).

1.2 Data leakage cases in Indonesia

The phenomenon of increasing internet use in Indonesia, in fact, is also balanced by the large number of cyber incidents that occur such as data leaks, *web defacement* and several other cyber incidents. Data leakage cases in Indonesia throughout 2022 are in the spotlight in the world, such as data leaks from PLN, BRI, Pertamina, Ministry of Health, Dukcapil, Online Shop and others. The Dutch cybersecurity company *Surfshark*, stated that Indonesia is the 3rd country in the world with the highest number of data leakage cases. In September 2022, 12.74 million accounts were monitored for data leaks. While the first and second ranks in the world are occupied by the countries of Russia and France with the number of data leakage cases of 14.78 and 12.94 million accounts. Furthermore, according to the monthly report on cybersecurity monitoring results published by the Directorate of Cybersecurity Operations of BSSN for the September 2022 period, there were 33,133 million traffic anomalies with traffic anomalies classified including (https://databoks.katadata.co.id, 2022) *Advance Persistent Threat* (APT), *Denial of Service* (DOS), Information *Gathering, Exploit, Information Leak, Malware, Trojan Activity, Web Application Attack,* and others. (Diropskamsiber BSSN, 2022)

Cyber threats are threats that have an impact on a country's defense. Strategists predict that future warfare will be more *hybrid*, that is, a war that combines conventional and non-conventional warfare (threats of cyber warfare, chemical weapons, biology, radiology, nuclear attacks, and explosive devices and information warfare). Oneof the current growing threats to the country's defense is the threat of *5th Generation Warfare (5GW).* Ada four elements that are the main strengths of the *5GW*, namely multi-domain *battle, fusion warfare,* based on the internet network (*network),* and the *battle virtual server* center *(combat cloud).* (Liang, 1999) Furthermore, according to President Joko Widodo in his statement at the 2019 MPR annual session, said Data is a new type of wealth for our nation, now data is more valuable than oil. The government must be prepared to face the threat of cybercrime including the crime of misuse of data.

Based on the phenomenon of cyber threats, who is responsible for cybersecurity? Cybersecurity is our shared responsibility, because of the need for involvement through the coordination of all authorities ranging from the Government, Ministries / Institutions to private parties in handling cyber threats with the establishment of *Computer Security Incicent Response Teams* (CSIRT), which will further be described in the writing of this study.

II. Research Methods

The method used in this study is a qualitative method through the study of literature from various reference sources and other documents. Researchers compare the handling of incident insiber through the Incident Response Team or Team *Cert* in various countries with Indonesia. The writing of this article is descriptive and explanatory to obtain facts and describe a comparative analysis of cyber threat handling policies through CSIRT in various countries

Technium Social Sciences Journal
Vol. 38, 87-102, December, 2022
ISSN: 2668-7798
www.techniumscience.com

with Indonesia. Researchers also presented data on how the process of forming CSIRT in Indonesia and various other countries.

The data used in this study is in the form of secondary data, which means that the source of the data is obtained not from direct observation but obtained from several previous studies such as research reports and other important documents. The literature search strategy uses *searches through Google Scholar, Elsevier* and several other journal searches nationally and internationally.

III. Review Of Literature

3.1 Computer Security Incident Response Team (CSIRT)

3.1.1 Definition of *CSIRT*

CSIRT is an Organization or capability or capability that provides services and support to specific constituents in order to prevent, handle, and respond to cybersecurity incidents. The existence of an organization that has duties and responsibilities as a cyber incident response team has existed since 1988, starting when the first *Worm* virus called Morris spread on all computers in the world. As a result of the spread of the virus, an agency in the United States DARPA (Defence Advanced Research Projects Agency) formed the SEI (Software Engineering Institute) then formed the CERT/CC (Computer Emergency Response Team / Coordination Center) at Carnegie Mellon University under a US government contract. The following is a table of nomenclature used for naming cyber incident response teams as below:(wikipedia.org, 2016)

Table 3.1.1 Nomenclature of Cyber Incident Response Teams

No	Acronym	Information
1	TRUE	Computer Emergency Response Team
2	TRUE	Computer Emergency Readiness Team
3	CIRCUS	Computer Incident Response Capability
4	IRC	Computer Incident Response Team
5	IRC	Incident Response Center
6	IRT	Incident Response Capability
7	SERVES	Incident Response Team
8	SIRT	Security Emergency Response Team
9	CSIRT	Computer Security Incident Response Team

Source : processed by the author

3.1.2 Role and Activity of CSIRT

CSIRT organizations have a role and activity in handling cyber incidents, along with the roles and activities of CSIRT;

Role of CSIRT :

a. Computer security incident response has become an important component of information technology (IT) programs.

b. Cybersecurity-related attacks are not only becoming more numerous and diverse, but also more destructive and disruptive

c. New types of security-related incidents are emerging more frequently

d. Preventive activities resulting from risk assessments can reduce the number of incidents, but not all incidents can be prevented

Technium Social Sciences Journal
Vol. 38, 87-102, December, 2022
ISSN: 2668-7798
www.techniumscience.com

e. Incident response capabilities are needed to detect incidents quickly, minimize losses and damages, reduce exploitation of vulnerabilities, and restore IT services.

Aktiftas CSIRT :

a. Provide SINGLE POINT OF CONTACT in every local issue
b. Identify, analyze, the impact of treatment and or incidents
c. Research, solutions, mitigation, strategy, planning, training
d. Share experiences, feedback information, learning, etc.
e. Awareness, capacity building, networking (within the community)

f.Incident response, and damage control, recovery/repair, minimizing risk to management, preventing incident and repetition expansion, preparedness, defense, and resilience.

3.1.3 CSIRT Types

Thedefinition of CSIRT in each country is tailored to the type of service provided in terms of cyber incident management. The following types of CSIRT are in accordance with the services it provides;

a. Internal CSIRT:

Providing incident handling services to its parent organizations, e.g. CSIRT Bank, CSIRT Government, CSIRT Academic.

b. National CSIRT :

Provide incident handling services in the country. Maintaining national security and interests is to carry out Critical Infrastructure Protection (CIP's) for example CISA (US), ENISA (EU).

c. Coordination Center :

Coordinate and facilitate incident handling centers in various CSIRTs, eg. JP-CERT/CC, My-CERT/CC, sectors.

d. Intelligence Analysis :

Focus on the synthesis of data from various sources to determine trends and patterns of activity within incidents (research and development) e.g. Security Operations Center (SOC) Team, security in-depth analysis

e. Vendor Teams :

Handle software or hardware product (solution) vulnerability reports such as social media security teams.

f. Incident Response Providers :

Provide services for handling commercial incidents or not for profit, for example outsourcing security managed services.

3.1.4 Regional CSIRT Organization

a. FIRST The Forum of Incident Response and Security Teams – Global Community :

1) CSIRT Teams
2) Security Teams
3) Technology Vendors
4) Expert and Academia

Technium Social Sciences Journal
Vol. 38, 87-102, December, 2022
ISSN: 2668-7798
www.techniumscience.com

b. EU CSIRTs Network, ANSAC The ASEAN Network Security Action Council
   1) European National CSIRT
   2) European CIP/CIIP Agencies
   3) ASEAN National CSIRT
c. APCERT The Asia Pacific CERT, OIC CERT The OIC CERT
   1) Asia Pacific National CSIRT
   2) Organization of Islamic Cooperation
   3) Organizational Members
   4) Expert and Academia

3.2 *Wicked Problems*

Wicked problems are public problems characterized by complex, uncertain characteristics, and are colored by differences in values among stakeholders. The word '*wicked*' is used to mark that problems in this categorization cannot be solved by conventional solutions, and at the same time demand fundamental changes at the level of government and society. The higher the degree of complexity, uncertainty, and difference in the value of a problem, the higher the '*wickedness*' of the problem will be (Brian, 2022). One example of '*wicked problems*' is the problem of cyberattacks. Attacks targeting the public and private sectors caused a variety of panics not only by the public but also strategic policy makers, which has the potential to strengthen people's sentiments of dissatisfaction with the State.

Since the introduction of digital information and communication technology, there has also been a rise in security crimes (Castells, 2000). As a result, pressure is increasing to find alternatives to traditional methods and instruments previously applied in tackling crimes in the field of information security (Klijn, 2012). Subsequently, a growing debate arose about forms of coordination from the originally hierarchical towards the centralized pattern (Bisschop & Verhage, 2012) or network-oriented (Yar , 2011). The transition of governance patterns from *government* to *governance* refers to the existence of several police partners (public and private) or 'security networks' (Dupont, 2004).

3.3 Coordination

Coordination is a fast, adaptive response, and relying on cooperation between stakeholders is needed to unravel '*wicked problems*' so that they can be intervened immediately. The plurality of actors with interaction and collaboration is the key to the concept of governance, with five distinctive characteristics, namely (i) the use of a set of institutions and actors inside and outside the government; (ii) the convergence of the power of government, the private sector, and society; (iii) the establishment of interdependent relations between the three forces; (iv) the establishment of autonomous networks across the boundaries of actors; and (v) the government does not only play the role of the main actor, simply as a catalyst (Sanusi, Putra, 2020).

In the opinion of other experts, coordination is an effort to provide direction for all organizational units to align activities optimally in order to achieve the desired organization . (Manullang , 2008) . Furthermore, according to Manullang (2008) coordination can be done in various ways, including the following; Secondly , appoint a person or a team or coordinating committee in charge of explaining what should be coordinated. Third, create a manual that contains the duties and responsibilities of each element / party involved in coordination. Fourth, there are regular meetings of leaders and subordinates in the context of guidance, consultation and direction.

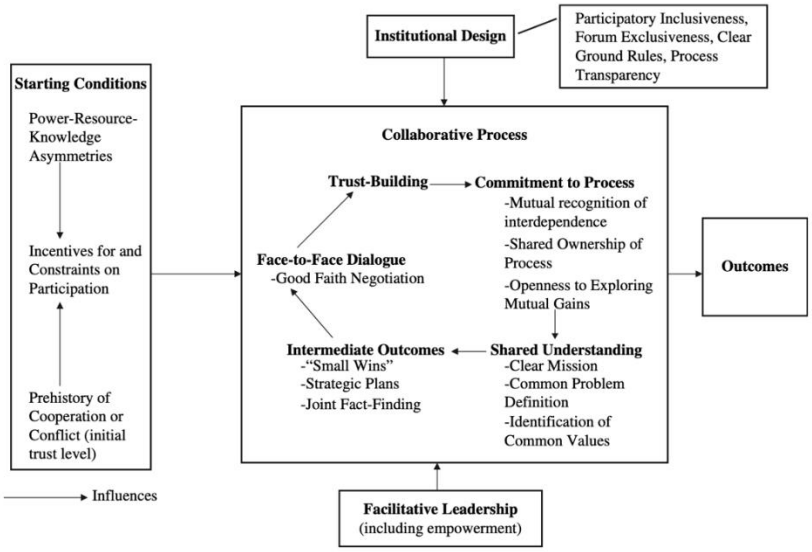
Technium Social Sciences Journal
Vol. 38, 87-102, December, 2022
ISSN: 2668-7798
www.techniumscience.com

When referring to the pattern of coordination between its members, it is divided into three types of networks which include, first, *self-governed networks*, where there is no organ that plays a formal role in coordinating members in the network. Roles and responsibilities are exercised by each member, which relies heavily on the active participation of the members. Second, l*ead organization-governed* network, that is, there is one member who plays the role of leading the network and facilitates other members in playing their roles and responsibilities. Third, network *administrative organizations*, where the key to network strength is outside the network, are driven by external units that are able to facilitate and circulate the resources needed by members to carry out their roles and responsibilities (Rondelez, 2018).

3.4 *Collaborative Governance*

Ansell and Gash (2007) define collaborative governance as an arrangement that governs one or more public institutions directly by engaging non-public stakeholders in a formal, consensus-oriented, and deliberative collective decision-making process and aims to implement public policies, manage public programs and assets. Stakeholders can find opportunities for mutual benefit, increase understanding, increase stakeholder trust, gather knowledge and information, improve efficient and effective coordination and improve decision legitimacy. Collaborative Governance arises because of cross-sectoral policy issues that demand administrative changes in overcoming these problems (Trein, 2020).

The application of the collaborative governance model is influenced by several factors/variables, as described in the following figure:



Source: Ansell and Gash, 2007.

Eight characteristics in collaboration according to (Carpenter, 1990): 1) Participation is unrestricted and not hierarchical, 2) Participants are responsible for ensuring the achievement of success. 3) the desired goal makes sense. 4) There isa definition of the problem. 5) Participants educate or teach each other. 6) Identification and testing of sharing options. 7) The implementation of the solution is shared with several participants involved. 8) Participants are always up to date with the development of the situation.

From some of the explanations above, it can be concluded that collaboration is a collaboration between two more people to achieve the goals that have been set. The benefits of collaboration are 1) providingquality service by combining unique professional expertise.

Technium Social Sciences Journal
Vol. 38, 87-102, December, 2022
ISSN: 2668-7798
www.techniumscience.com

2) maximizethe productivity, effectiveness and efficiency of resources. 3) To increase professionalism, loyalty, and job satisfaction. 4) Increased cohesiveness between related parties. 5) provideclarity role as a form of duty and responsibility of each party involved.

IV. Results and Discussion

4.1 Collaboration in the Early Days of CSIRT

The CSIRT embryo is a CERT ID which is a community-based coordination team. This organization was founded by Budi Raharjo, then together with JP-CERT (Japan) and AUS-CERT (Australia) established the APCERT (*Asia Pacific Computer Emergency Response Team*) forum. The background to the establishment of CERT ID is the need to respond to internet security problems in Indonesia. The purpose of establishing CERT ID is to (i) coordinate the handling of incidents involving Indonesians and foreign parties, (ii) Inform various complaints about internet security network incidents, (iii) Build the CERT Indonesia community, (iv) Socialize the importance of internet security in Indonesia, and (v) Conduct various research in the field of Internet security needed by the Indonesian Internet community (Alkazimy, 2017).

Based on the collaborative governance model, ID CERT as a collaborative effort is based, one of which is due to concerns from non-state actors who have expertise / knowledge about internet security in Indonesia. The starting *condition* that is the background of CERT ID is the variety of knowledge/information and ability to respond to cyber threats. Furthermore, ID CERT collaborates with various other institutions, both from the government and non-government in carrying out information/knowledge dissemination activities about cybersecurity. ID CERT collaborates with regional CERT (Malaysia, Australia, Japan), technology companies (facebook, yahoo, google) and ministries/agencies (Kemenkominfo, Kemenkopolhukam, BPPT). The collaboration is based on shared understanding among stakeholders regarding cyber threats.

4.2 Coordination and Collaboration of Ministries/Institutions as a solution to problems in handling cyber threats through the Establishment of CSIRT.

Based on the problems described earlier, to solve these problems, it is necessary to collaborate or involve stakeholder elements between Ministries/Institutions and Swaswa with the formation of an organization formed by CSIRT, meaning that it needs a fast, adaptive response, and relying on cooperation between stakeholders is needed to unravel public problems (*wicked problems)* In order to intervene immediately, in this case it is the handling of cyber threats.

To solve the problems described earlier, the coordination type solution suggested by Rondelez (2018) is the net type **l*ead organization-governed*** network, meaning that there is one member who plays the role of leading the network and facilitates other members in playing their roles and responsibilities. In this case, the Government through the State Cyber and Cipher Agency (BSSN) as the *leader* with *Nat-CSIRT* while the Ministry/Institution and the Private Sector are members with the Sectoral *CSIRT*. The *governance* of the network is the key to the success of the government, considering that in governantion, there is not one '*center*' that plays an absolute role, but many points with a diversity of roles and responsibilities. Gathering various perspectives, technical knowledge, and resources owned by actors into network mechanisms can trigger the resolution of thorny public problems by utilizing resources as effectively as possible. The traffic of information and resources that was never imagined before because it was considered an 'asset' of the actors' private property, was then able to be exchanged

Technium Social Sciences Journal
Vol. 38, 87-102, December, 2022
ISSN: 2668-7798
www.techniumscience.com

quickly. However, the key word that is important to pay attention to is the existence of clear rules of the game and the accommodation of the interests of each actor, where consensus is the determinant for each direction the network takes. The art of managing power through negotiations, strategies, and *resource trade-offs* is a way to build relationships between actors in the network to remain solid and sustainable (Pratikno, 2007).

Furthermore, what is the role of each Ministry /agency in the collaborative process of handling cyber threats. The government through BSSN issued a BSSN Regulation on CSIRT, then its implementation formed a Cyber Incident Response Team Organization (Nat CSIRT / Gov CSIRT) as the Central Coordinator in charge of the organization CSIRT in Ministries/Institutions, Provincial Government/District as a member of CSIRT. Then where the role of the Private Sector, in addition to the Private sector can form a Private Sector CSIRT Organization, can also provide the capability of its resources to organize *sharing knowledge* about *cyber* security, implementation of certification in the field of information and cyber security. The Private Sector such as APJII (Indonesian Internet Providers Services Association) plays a role "to be a partner of the Government in building national and international information and communication facilities, so that all existing resources can be mobilized in an integrated, efficient and effective manner". (APJII, 2022)

Governance issues within ministries/institutions can also be linked to bureaucratic reform efforts. As mentioned in the *Grand Design of* Bureaucratic Reform, Bureaucratic Reform aims to create a bureaucracy that is professional, serving, neutral, prosperous and upholds the basic values and codes of ethics of the state apparatus. To realize this goal, there are several areas in government management that must be improved, which include (i) change management, (ii) structuring laws and regulations, (iii) structuring and strengthening organizations, (iv) structuring governance, (v) structuring human resources, (vi) strengthening performance accountability, (vii) strengthening supervision, and (viii) improving the quality of public services. One of these areas is the management area which is expected to create aclear, effective, efficient, measurable work process and procedure and in accordance with the principles of *good governance.*

It can be concluded that coordination and collaboration are one of the important activities in organizing so that the achievement of organizational goals can be carried out effectively and efficiently. Coordinationand collaboration between parts of the organization or with other organizations, will facilitate the resolution of each individual's problems for a common purpose. After the solutions found to overcome the existing problems, then how to implement in the formation of CSIRT, in the next sub-chapter will be explained how the legal basis, overview and stages in the formation of CSIRT in Indonesia.

4.3 Legal Basis for CSIRT Establishment in Indonesia

As previously explained, that cybersecurity is our shared responsibility of the Government, Ministries/Institutions and the Private Sector. This is emphasized by Government Regulation (PP) Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, article 3 states "Every Electronic Operator must organize an Electronic System reliably and safely and be responsible for the operation of the Electronic System as appropriate". In the PP, it is also stated that an Electronic Operator is "any person, state operator, Business Entity, and society that provides, manages, and/or operates the Electronic System individually or jointly to the Electronic System User for his own and/or other parties' needs. ". From the description of the explanation, it can be concluded that cybersecurity is the responsibility of all of us as organizers of electronic systems.

Technium Social Sciences Journal
Vol. 38, 87-102, December, 2022
ISSN: 2668-7798
www.techniumscience.com

Cybersecurity is defined as an effort that can be used to secure organizational assets in the form of data and information in cyberspace, the effort consists of a group of tools, policies, settings, protection, risk management approaches, security assurance, training, and best practices and technologies. (Khoironi, 2020). Therefore, the Government through the State Cyber and Password Agency (BSSN) as an agency that has the main task in the field of cybersecurity and passwords, issued BSSN Regulation Number 10 of 2020 concerning the *Cyber Security Incident Response Team* (CSIRT), as a form of effort to protect the entire Indonesian nation, including cyberspace as stated in the preamble to the 1945 Constitution paragraph 4. . The establishment of CSIRT is a priority for the Government sector as a vital (Hertianto, M. R., 2021) infrastructure information (IIV) management institution, where many of the information assets are managed that are related not only to the survival of the people but also concern the stability and sovereignty of the country. In line with this, information governance is also currently in digital form after the ratification of Presidential Regulation Number 95 of 2018 concerning Electronic-Based Government Systems (SPBE).

Through the SPBE Presidential Regulation, the Government hopes that the modernization of public service delivery can be realized as well as become one of the *bureaucratic reform tools* that produce quality, professional, transparent and accountable public service output. Security is one of the important aspects to achieve that output. Thus, all data and information processed in the SPBE application become important assets that must be protected by security. According to (Yunas, N. S, 2020) *The Committee on National Security System* (CNSS) information security is the protection of information consisting of systems and hardware to process, store and transmit information from all kinds of cyber disturbances and incidents. Cyber Incidents according to(Romuald H., Jarosław N., Tomasz P., J. S., 2020) Article 1 of BSSN Regulation No.10 of 2020, are "one or a series of events that interfere with or threaten the running of Electronic Systems". Meanwhile, the *Computer Security Incident Response Team* (CSIRT) is "a group of people responsible for handling Cyber Incidents within the scope specified against them".

4.4 Overview of CSIRT in Indonesia

4.4.1 CSIRT Organization

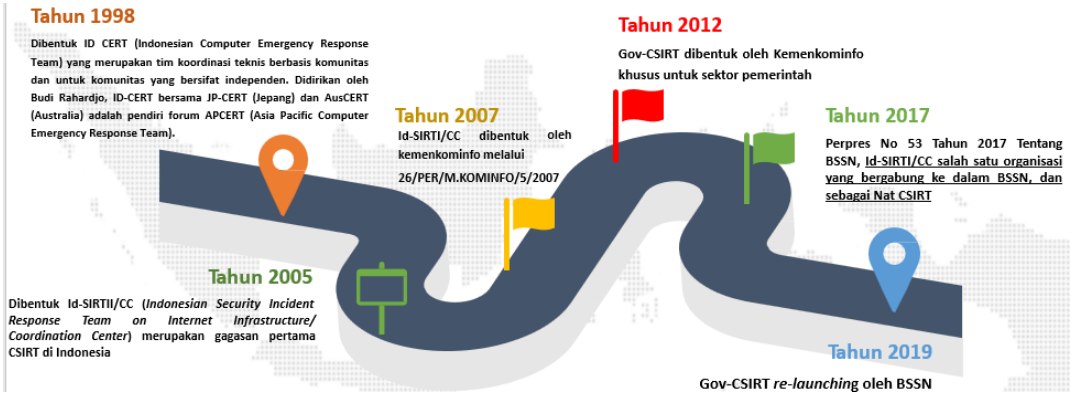
The existence of a Cyber Incident Response Organization or Team in Indonesia has existed since 1998 with a different naming nomenclature, namely ID CERT (*Indonesia Computer Emergency* Response Team) but its duties and functions are the same as the Cyber Incident Response Team. ID CERT is an independent, community-based technical coordination team. This organization was founded by Budi Raharjo, then together with JP-CERT (Japan) and AUS-CERT (Australia) established the APCERT (*Asia Pacific Computer Emergency Response Team*) forum.

Furthermore, in 2005 Id-SIRTII/CC (Indonesia *Security Incident Response Team on Internet Infrastructure Coordination Center*) was formed, which was the first idea of the formation of CSIRT in Indonesia. In 2007 the Id-SIRTII/CC organization was strengthened from a legal point of view by the Government through Kominfo by issuing Minister of Communication and Informatics Regulation Number 26/PER/M.KOMINFO/5/2007. Furthermore, to classify cyber incidents in the government sector, in 2012 the Ministry of Communication and Information formed a CSIRT engaged in the government sector, namely Gov-CSIRT. Departing from the massive escalation of cyber incidents in 2017, the Government

Technium Social Sciences Journal
Vol. 38, 87-102, December, 2022
ISSN: 2668-7798
www.techniumscience.com

issued Presidential Regulation number 53, namely forming BSSN which is a merger of the State Cipher Institute, Directorate of Information Security, Id-SIRTII / CC Directorate General of Applications and Informatics of the Ministry of Communication and Informatics. Id-SIRTII/CC is one of the organizations incorporated in BSSN and is used as National CSIRT (Nat-CSIRT). Furthermore, through BSSN in 2019, the re-inauguration of Gov-CSIRT as a CSIRT organization in the government sector was carried out.

Figure 4. 4.1.1. History of CSIRT Organization in Indonesia



Source : BSSN

On a national scale, BSSN has formed Gov-CSIRT or as Nat-CSIRT which is based on Presidential Regulation Number 28 of 2021 concerning State Cyber and Password Agencies and BSSN Regulation number 6 of 2021 concerning BSSN Organization and Work Procedures. BSSN's Directorate of Cybersecurity Operations was appointed as the manager of the government's Cyber Incident Response Team (TTIS). TTIS government sector is hereinafter referred to as Gov-CSIRT Indonesia and organizes cyber incident response services in the government sector at the request of its constituents covering all central and regional governments. In its implementation, Gov-CSIRT/Nat-CSIRT has the following vision and mission: Gov-CSIRT Indonesia's vision is "the realization of cyber resilience in a reliable and professional government sector". Meanwhile, the mission of Gov-CSIRT Indonesia is to "coordinate and collaborate on cybersecurity services in the government sector; coordinate and collaborate on cyber incident response in the government sector; and building the capacity of cybersecurity resources in the government sector". (BSSN, 2021)

The establishment of CSIRT in the government sector at the central and regional levels is one of the national strategic projects as stated in Presidential Regulation Number 18 of 2020 concerning the 2020-2024 RPJMN. In the national strategic plan, BSSN will form 131 CSIRT by 2024. As of September 2022, the number of CSIRT that has been formed is 118 CSIRT (90.07%), consisting of Ministries/Institutions, Regional Governments, Energy and Mineral Resources, Transportation, Finance, Health, Technology, Food, Defense, Education, and other sectors. (BSSN, 2022)

Technium Social Sciences Journal
Vol. 38, 87-102, December, 2022
ISSN: 2668-7798
www.techniumscience.com

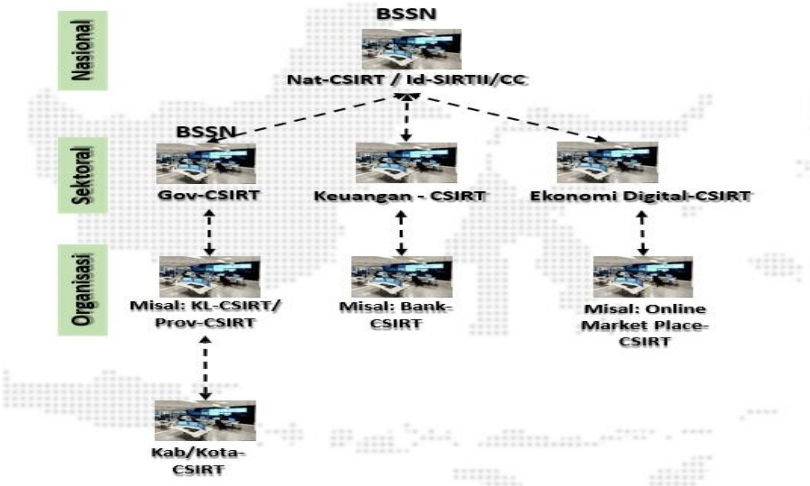
Table 4. 4.1. Table of the Number of CSRIT in Indonesia

No	Sector	Sum	Information
1	Government	92	Ministries/Institutions : 38 Local Government : 54
2	Defence	7	
3	Transportation	1	
4	Finance	7	
5	Health	2	
6	Energy and Mineral Resources	3	
7	Food	1	
8	Other	5	Education, Trade, etc.

Source : BSSN, 2022

Although 90.07% of the formation of CSIRT from the target number of 131 points, this number does not include all government agencies, especially the City Government / District / City Government because problems and obstacles are still found in the field in the implementation process. Through CSIRT, it is hoped that it can help facilitate the resolution of problems in the event of a cyber incident. Furthermore, how is the organizational structure of CSIRT starting from the central level to the regional level.

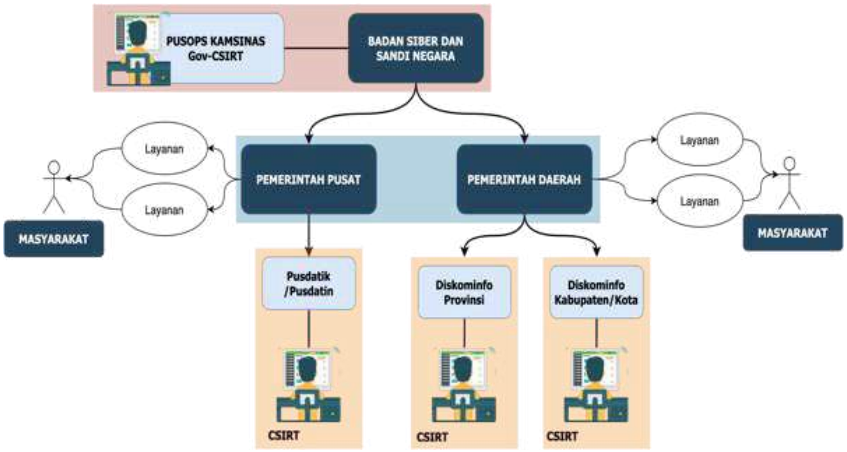
Figure 4. 4.1. 2 Examples of Nat-CSIRT Organizational Collaboration with CSIRT other sectors



Source : BSSN, 2022

Technium Social Sciences Journal
Vol. 38, 87-102, December, 2022
ISSN: 2668-7798
www.techniumscience.com

Figure 4. 4.1. 3 CSIRT Organization Workflow Examples



Source:(Prabaswari, Muhamad Alfikri, Irdam Ahmad, 2022)

4.4.2 Stages of CSIRT Formation

To be able to become a CSIRT organization in Indonesia, there are several stages that must be passed, of course, through coordination and supervision attached to BSSN including the following:

a. Education Stage ; CSIRT Assistance:
   1) Understanding Regulations
   2) Understanding the Purpose
   3) Understanding Models and Mechanisms of action
   4) Understanding Human Resources (HR)
   5) Understanding the Services
   6) Understanding Funding

b. CSIRT Planning Phase:
   1) Vision and Mission Formulation
   2) Formulation of the Organizational Structure
   3) Service Identification
   4) Identify HR Needs
   5) Identify Device Needs / *Tools*
   6) Policy and SOP Formulation
   7) Preparation of Work Plan and Budget

c. Stage of Implementation of CSIRT ;
   1) Team Appointment :

   Appointment of CSIRT Team can be through Decree / Warrant
   2) Fulfillment of Tools / *Tools;*
      (1) Website CSIRT
      (2) Communication Devices (Email, Tel, Fax, etc.)
      (3) Cyber Incident Complaint Ticketing System
      (4) Sistem Monitoring (IDS/SIEM)
      (5) Incident Response Tools

Technium Social Sciences Journal
Vol. 38, 87-102, December, 2022
ISSN: 2668-7798
www.techniumscience.com

3) Implementation of SOP Policy;
   (1) Cyber Incident Reporting SOP
   (2) SOP for Cyber Incident Handling
   (3) Log Storage SOPs
   (4) Other SOPs on Cyber Incidents
4) Declaration; using RFC 2350
5) Registration; send the registration file to BSSN via email

For agencies that have registered for CSIRT, BSSN will provide an increase in CSIRT's HR capabilities in the form of *Cyber Drills,* CSRIT Management Workshops and Trainings.

6) Inauguration

d. CSIRT Operational and Collaboration Phase; CSIRT has experience handling incidents and collaborates with other CSIRTs.

4.4.3 Types of Cyber Contact Services and Workflows

With the establishment of CSIRT, it is hoped that the handling of cyber incidents in the Central and Regional Governments can be more systematic and organized because it has been automated by a system registered in Gov/Nat-CSIRT BSSN. Here are the types of services provided and the Nat-CSIRT BSSN cyber contact workflow.

Types of Nat-CSIRT services:

a. Incident Response ; coordinating, analyzing, technical recommendations, on-site assistance in the context of cyber incident response

b. Security Alerts; provide alerts or notifications about any cyber threats that may have or may occur.

c. International Collaboration ; link/point of contact of CSIRT collaboration between countries.

d. CSIRT Registration; provide CSIRT registration services to become a member of Nat-CSIRT.

e. Security Guidelines; provide services in the form of guidance documents or recommendations in improving cybersecurity.

f.Cybersecurity Monitoring Results Report; providing services in the form of documents that present the recapitulation and analysis of the results of cybersecurity monitoring by BSSN.

Technium Social Sciences Journal
Vol. 38, 87-102, December, 2022
ISSN: 2668-7798
www.techniumscience.com

Cyber Contact Workflow

Figure 4. 4. 3.1 Cyber Contact Workflow

2. - The Cyber Contact Center team verifies the information and relays the information to the relevant Team for follow-up.
   - Koordinasi penanganan insiden (bila diperlukan)
3. - Provide notifications to stakeholders, Mode of communication: email, phone, mail, etc.
   - Providing notifications to Internal BSSN stakeholders
4. Stakeholders can request assistance in handling cyber incidents

V. Conclusion

The Covid-19 pandemic that occurred in the world and in Indonesia had an impact on various economies around the world, including Indonesia. This also has an impact on adapting people's activities to often carry out online activities both for work, study, buying and selling transactions, socializing and so on so that during the Covid-19 period there was an increase in activities carried out using the internet or online activities. The phenomenon of increasing internet use in Indonesia, in fact, is also balanced by the large number of cyber incidents that occur such as data leaks, *web defacement* and several other cyber incidents. Data leakage cases in Indonesia throughout 2022 are in the spotlight in the world, such as data leaks from PLN, BRI, Pertamina, Ministry of Health, Dukcapil, Online Shop and others.

Cyber threats are threats that have an impact on a country's defense. Strategists predict that future warfare will be more *hybrid*, that is, a war that combines conventional and non-conventional warfare (threats of cyber warfare, chemical weapons, biology, radiology, nuclear attacks, and explosive devices and information warfare). One example of '*wicked problems*' is the problem of cyberattacks. Attacks targeting the public and private sectors caused a variety of panics not only by the public but also strategic policy makers, which has the potential to strengthen people's sentiments of dissatisfaction with the State. One of the institutional efforts undertaken by the government to respond to cybersecurity issues is to form CSIRT. The government through the State Cyber and Password Agency (BSSN) as an agency that has the main task in the field of cybersecurity and passwords, issued BSSN Regulation Number 10 of 2020 concerning the *Cyber Security Incident Response Team* (CSIRT), as a form of effort to protect the entire Indonesian nation, including in cyberspace as stated in the preamble to the 1945 Constitution paragraph 4. .(Hertianto, M. R., 2021)

The pattern of cybersecurity policy coordination can be divided into 3 (three) periods. In the first period, the coordination pattern rests on *an all channel / full matrix network* where

the relationship between various stakeholders is consultative and informal. In the second period, the coordination pattern began towards the *hub / star network* where there was an organizational unit that acted as a leading sector, namely the Directorate of Information Security, Ministry of Communication and Information. In the third period, the coordination pattern in the form of *hub/star networks* was strengthened through (i) the establishment of BSSN, and (ii) the establishment of CISRT. BSSN acts as a coordinator at the policy level, while Nat-CISRT acts as a coordinator at the operational level (*lead organization network in the governance network scheme*).

Coordination and collaboration are one of the important activities in organizing so that the achievement of organizational goals can be carried out effectively and efficiently. Coordination and collaboration between parts of the organization or with other organizations, will facilitate the resolution of each individual's problems for a common goal.

References

[1] Alkazimy, Ahmad (2017). The role of ID-CERT in handling cyber incidents in Indonesia

[2] Ansell, C., & Gash, A. (2007). Collaborative Governance in Theory and Practice. *Journal of Public Administration Research and Theory, 18*, 543-571.

[3] Ansel, Christ. 2012. *Collaborative Governance*. DOI: 10.1093/oxfordhb/9780199560530.013.0035.

[4] Oxford University Press

[5] APJII. (2022). *https://apjii.or.id/*. Retrieved from https://apjii.or.id/

[6] BSSN. (2021). Retrieved from https://bssn.go.id/gov-csirt-indonesia/

[7] BSSN. (2022). Retrieved from https://www.idntimes.com/business/economy/vadhia-lidyana-1/bssn-bakal-bangun-131-csirt-sampai-2024-apa-itu

[8] Diropskamsiber BSSN. (2022, didownlod September). Retrieved from https://idsirtii.or.id/halaman/tentang/laporan-hasil-monitoring.html

[9] Hertianto, M. R. (2021). Juridical Review of Child Protection in Cyberspace in Indonesia. *Journal of Law & Development*, 51(3), 555–573.

[10] Hidayat Chusnul Chotimah. (2015). Building National Defense and Security from Cyber Threats in Indonesia. *Journal of Diplomacy*, 60-109.

[11] Hootsuite. (2022). Retrieved from https://datareportal.com/reports/digital-2022-global-overview-report?utm_source=DataReportal&utm_medium=Country_Article_Hyperlink&utm_campaign=Digital_2022&utm_term=Indonesia&utm_content=Global_Promo_Block.

[12] https://databoks.katadata.co.id. (2022). Retrieved from https://databoks.katadata.co.id/datapublish/2022/09/13/indonesia-masuk-3-besar-negara-dengan-kasus-kebocoran-data-terbanyak-dunia

[13] Jason Andreas Steve Winterfeld. (2014). *Cyber Warfare : Technique, Tactics and Tools for Security Practitioners. Second Edition.* Elsevier.

[14] Khoironi, S. (2020). The Influence of Cybersecurity Cultural Training Needs Analysis as an Effort to Develop Competencies for State Civil Apparatus in the Digital Era. *Journal of Communication and Media Studies.* , 24(1), 37.

[15] Liang, Q. (1999). Unrestricted Warfare. *PLA Literature and Arts Publishing House*, 1-7.

[16] Manullang . (2008). *Fundamentals of Management.* Yogyakarta: Ghalia Indonesia (GI).

[17] Ookla. (2022). Retrieved from https://datareportal.com/reports/digital-2022-indonesia
[18] Prabaswari, Muhamad Alfikri, Irdam Ahmad. (2022). Evaluation of Policy Implementation for the Formation of Cyber Incident Response Teams in the Government Sector. *Journal of Policy Innovation: Matra Pembaruan.*
[19] Romuald H., Jarosław N., Tomasz P., J. S. (2020). Measurement Models of Information Security Based on the Principles and Practices for Risk-Based Approach. *Procedia Manufacturing*, 44, 647–654.
[20] wikipedia.org. (2016). Retrieved from https://en.wikipedia.org/wiki/Computer_emergency_response_team
[21] Yunas, N. S. (2020). Implementation of e-Government in Minimizing the Practice of Rent Seeking Behaviour in the Surabaya City Government Bureaucracy. *Renewal Dimension*, 4(1), 13–23.