



**Universitas Katolik Parahyangan**  
**Fakultas Ilmu Sosial dan Ilmu Politik**  
**Program Studi Hubungan Internasional Program Sarjana**

*Terakreditasi Unggul*

*SK BAN-PT No. 2579/SK/BAN-PT/AK-ISK/S/VI/2022*

**Analisis Kerja Sama *Comprehensive Security* di Bidang  
*Cybersecurity* antara Jepang dan Amerika  
Serikat 2011 – 2019**

Skripsi

Oleh

Maria Christina Septania Anis Putri

2017330189

**Bandung**

**2022**



**Universitas Katolik Parahyangan**  
**Fakultas Ilmu Sosial dan Ilmu Politik**  
**Program Studi Hubungan Internasional Program Sarjana**

*Terakreditasi Unggul*

*SK BAN-PT No. 2579/SK/BAN-PT/AK-ISK/S/VI/2022*

**An Analysis of Comprehensive Security Alliances in  
Cybersecurity Between Japan and the United States  
2011 - 2019**

Thesis

By

Maria Christina Septania Anis Putri

2017330189

**Bandung**

**2022**



**Universitas Katolik Parahyangan**  
**Fakultas Ilmu Sosial dan Ilmu Politik**  
**Program Studi Hubungan Internasional Program Sarjana**

*Terakreditasi Unggul*

*SK BAN-PT No. 2579/SK/BAN-PT/AK-ISK/S/VI/2022*

**Analisis Kerja Sama *Comprehensive Security* di Bidang  
*Cybersecurity* antara Jepang dan Amerika**  
**Serikat2011 – 2019**

Skripsi

Oleh

Maria Christina Septania Anis Putri

2017330189

Pembimbing

Idil Syawfi, S.IP., M.Si.

**Bandung**

**2022**



**Universitas Katolik Parahyangan**  
**Fakultas Ilmu Sosial dan Ilmu Politik**  
**Program Studi Hubungan Internasional Program Sarjana**

*Terakreditasi Unggul*

*SK BAN-PT No. 2579/SK/BAN-PT/AK-ISK/S/VI/2022*

**An Analysis of Comprehensive Security Alliances in  
Cybersecurity Between Japan and the United States  
2011 - 2019**

Thesis

By

Maria Christina Septania Anis Putri

2017330189

Pembimbing

Idil Syawfi, S.IP., M.Si.

**Bandung**

**2022**

Fakultas Ilmu Sosial dan Ilmu Politik  
Jurusan Hubungan Internasional  
Program Studi Hubungan Internasional Program Sarjana



**Tanda Pengesahan Skripsi**

Nama : Maria Christina Septania Anis Putri  
Nomor Pokok : 2017330189  
Judul : Analisis Kerja Sama *Comprehensive Security* di Bidang  
*Cybersecurity* antara Jepang dan Amerika Serikat  
2011 – 2019

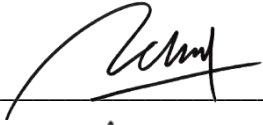
Telah diuji dalam Ujian Sidang jenjang Sarjana  
Pada Kamis, 23 Juni 2022  
Dan dinyatakan **LULUS**

**Tim Penguji**

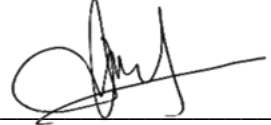
**Ketua sidang merangkap anggota**

Putu Agung Nara Indra Prima Satya, S.IP., M.Sc : 

**Sekretaris**

Idil Syawfi, S.IP., M.Si. : 

**Anggota**

Dr. I Nyoman Sudira, Drs., M.Si. : 

Mengesahkan,  
Dekan Fakultas Ilmu Sosial dan Ilmu Politik



Dr. Pius Sugeng Prasetyo, M.Si

## Lembar Pernyataan Orisinalitas

---

### Pernyataan

Saya yang bertandatangan dibawah ini:

Nama : Maria Christina Septania Anis Putri

NPM : 2017330189

Program Studi : Hubungan Internasional

Judul : Analisis Kerja Sama *Comprehensive Security* di Bidang  
*Cybersecurity* antara Jepang dan Amerika Serikat  
2011 – 2019

Dengan ini menyatakan bahwa skripsi ini merupakan hasil karya tulis ilmiah sendiri dan bukanlah merupakan karya yang pernah diajukan untuk memperoleh gelar akademik oleh pihak lain. Adapun karya atau pendapat lain yang dikutip, ditulis sesuai dengan kaidah penulisan ilmiah yang berlaku.

Pernyataan ini saya buat dengan penuh tanggung jawab dan bersedia menerima konsekuensi apa pun sesuai aturan yang berlaku apabila di kemudian hari diketahui bahwa pernyataan ini tidak benar.

Bandung, 15 Juni 2022



Maria Christina Septania Anis Putri



## ABSTRAK

Nama : Maria Christina Septania Anis Putri  
NPM : 2017330189  
Judul : Analisis Kerja Sama *Comprehensive Security* di Bidang  
*Cybersecurity* antara Jepang dan Amerika Serikat 2011 - 2019

---

Penelitian ini bertujuan untuk mengetahui alasan kerja sama antara Jepang dan Amerika Serikat di bidang *cybersecurity*. Jepang dikenal sebagai salah satu negara yang memiliki penguasaan teknologi tinggi. Berbagai pengembangan dan penemuan teknologi yang Jepang lakukan telah menghasilkan prestasi hingga meningkatkan pertumbuhan sektor perekonomian mereka. Meskipun Jepang memiliki kapabilitas yang tinggi di bidang teknologi, Jepang masih harus menjalin kerja sama di bidang *cybersecurity* dengan Amerika Serikat. Penelitian ini ditujukan untuk menjelaskan alasan Jepang sebagai negara dengan penguasaan teknologi tinggi hingga harus melakukan kerja sama secara komprehensif dengan Amerika Serikat dalam menanggulangi isu *cybersecurity*. Metode kualitatif induktif digunakan untuk memperoleh alasan terjadinya kerja sama Jepang dan Amerika Serikat. Analisis dilakukan dengan melihat beberapa perjanjian hukum di mana menjadi dasar terjadinya kerja sama *cybersecurity* secara *collective self-defense* antar kedua negara yang selanjutnya mengalami perluasan di bidang yang lebih komprehensif. Penggunaan metode dan konsep *comprehensive security* dalam analisis penelitian ini kemudian menghasilkan jawaban bahwa terdapat faktor internal dan eksternal yang membatasi kapabilitas Jepang untuk menghadapi ancaman tinggi di bidang *cybersecurity* pada sektor politik, militer, dan ekonomi.

**Kata kunci:** *cybersecurity*, *cyberattack*, *comprehensive security*, *collective self-defense*, Jepang, Amerika Serikat.



## **ABSTRACT**

Name : Maria Christina Septania Anis Putri  
NPM : 2017330189  
Title : An Analysis of Comprehensive Security Alliances in  
Cybersecurity Between Japan and the United States 2011 - 2019

---

The objective of this research is to understand the cause of cooperation between Japan and the United States in cybersecurity. Japan is known as one of the countries with expertise in advanced technologies. Many technological development and discoveries made by Japan have gained success in increasing the rate of their economic sectors. Although Japan is highly capable of technology, they must still form an alliance in cybersecurity with the US. This will be the base of the research to analyze various reasons for Japan as a highly advanced country in technology to conduct an alliance with the US towards handling cybersecurity issues. An inductive, qualitative method is used to gather references in supporting the research objective of understanding the alliance between Japan and the US. The analysis is conducted by observing several law agreements where a collective self-defense cybersecurity alliance between two countries is expanding in a comprehensive security field. The use of comprehensive security methods and concepts in the research analysis are able to provide answers that internal and external factors which restrain Japan's capability to face critical threats in cybersecurity towards politics, military, and economic sectors.

**Keywords:** cybersecurity, cyberattack, comprehensive security, collective self-defense, Japan, United States.

## KATA PENGANTAR

Puji dan syukur penulis ucapkan kepada Allah Bapa Yang Maha Kuasa karena melalui perantaraan Putera-Nya Tuhan Yesus Kristus telah memberikan segala kasih, berkat, karunia dan kuasa-Nya untuk menguatkan dan membimbing penulis dalam menyelesaikan penelitian berjudul “Analisis Kerja Sama *Comprehensive Security* di Bidang *Cybersecurity* antara Jepang dan Amerika Serikat 2011 – 2019”. Penulisan skripsi ini ditujukan guna memenuhi persyaratan dalam menyelesaikan pendidikan tingkat Sarjana pada jurusan Ilmu Hubungan Internasional Universitas Katolik Parahyangan, Bandung. Selain itu juga ditujukan untuk menambah penelitian hubungan internasional terkait topik kerja sama *cybersecurity* antara Jepang dan Amerika Serikat.

Penelitian ini berada jauh di luar kesempurnaan yang disebabkan oleh keterbatasan penulis di dalam proses penulisan. Namun dengan kuasa Tuhan, doa, dan bantuan berbagai pihak dapat membantu penulis untuk menyelesaikan penelitian ini. Dengan berbagai kekurangan yang ada di dalam penelitian ini, maka penulis memohon segala kritik dan saran yang sekiranya dapat menjadi pembelajaran untuk mengembangkan pengetahuan serta kemampuan penulis di masa mendatang.

Bandung, 15 Juni 2022

Penulis

## DAFTAR ISI

ABSTRAK.....	i
ABSTRACT.....	ii
KATA PENGANTAR.....	iii
UCAPAN TERIMA KASIH.....	iv
DAFTAR ISI.....	x
DAFTAR SINGKATAN.....	xii
BAB I.....	1
Pendahuluan.....	1
1.1. Latar Belakang Masalah.....	1
1.2. Identifikasi Masalah.....	5
1.2.1. Pembatasan Masalah.....	7
1.2.2. Perumusan Masalah.....	8
1.3. Tujuan dan Kegunaan Penelitian.....	8
1.3.1. Tujuan Penelitian.....	8
1.3.2. Kegunaan Penelitian.....	9
1.4. Kajian Literatur.....	9
1.5. Kerangka Pemikiran.....	13
1.6. Metode Penelitian dan Teknik Pengumpulan.....	19
1.7. Sistematika Pembahasan.....	21
BAB II.....	23
Kebijakan Pemerintah Jepang Bersama AS Sebagai Negara Aliansi Terhadap Kasus <i>Cyberattack</i> yang Menyerang Jepang.....	23
2.1. Kebijakan <i>Cybersecurity</i> Jepang.....	23

2.2.	Kasus – Kasus <i>Cyberattack</i> yang Pernah Menyerang Jepang.....	31
2.3.	Forum Kerja Sama <i>Cybersecurity</i> AS dan Jepang.....	35
BAB III.....		42
Alasan Jepang Melakukan Kerja Sama <i>Cybersecurity</i> Bersama Dengan Amerika Serikat.....		42
3.1.	Batasan – Batasan Pada <i>Cybersecurity</i> Jepang.....	42
3.1.1.	Batasan Pada Faktor Internal Jepang.....	43
3.1.2.	Batasan Pada Faktor Eksternal Jepang.....	47
3.2.	Peralihan <i>Individual Self-Defense</i> Jepang Kepada <i>Collective Self-Defense</i> di Bidang <i>Cybersecurity</i> Bersama Amerika Serikat.....	49
3.3.	Perluasan <i>Collective Self-Defense</i> Jepang-AS Pada Sektor Politik, Militer, dan Ekonomi.....	54
3.3.1.	Politik.....	58
3.3.2.	Militer.....	60
3.3.3.	Ekonomi.....	63
BAB IV.....		67
Kesimpulan.....		67
REFERENCES.....		71

## DAFTAR SINGKATAN

APTs	Advanced Persistent Threats
CDPWG	Cyber Defense Policy Working Group
DDoS	Distributed Denial of Service
IHI	Ishikawajima-Harima Heavy Industries
ISPC	Information Security Policy Council
JAEA	Japan Atomic Energy Agency
JAXA	Japan Aerospace Exploration Agency
JASDF	Japan Air Self-Defense Force
JNES	Japan Nuclear Energy Safety Organization
JPS	Japan Pension Service
JSDF	Japan Self-Defense Force
JGSDF	Japan Ground Self-Defense Force
JMSDF	Japan Maritime Self-Defense Force
KHI	Kawasaki Heavy Industries
MAFF	Ministry of Agriculture, Forestry and Fishery
METI	Ministry of Economy, Trade and Industries
MHI	Mitsubishi Heavy Industries
MIC	Ministry of Internal Affairs and Communications
NISC	National Information Security Center
WoG	Whole-of-Government

## **BAB I**

### **Pendahuluan**

#### **1.1. Latar Belakang Masalah**

Penemuan dan kemajuan Jepang pada teknologi menjadi sebuah prestasi bagi Jepang, mengingat negara ini pernah mengalami kehancuran di bidang industri setelah mengalami kekalahan pada Perang Dunia Kedua.<sup>1</sup> Setelah berakhirnya perang tersebut, Jepang menyadari bahwa bidang industri merupakan hal yang dapat menguatkan perekonomian mereka.<sup>2</sup> Inilah penyebab mengapa Jepang berupaya meningkatkan kekuatan mereka kembali di bidang industri. Cara yang dilakukan oleh Jepang, yaitu dengan mempelajari pengetahuan seputar pengembangan teknologi yang didapatkan dari negara – negara barat dan berupaya untuk mengembangkan pengetahuan tersebut.<sup>3</sup>

Adanya upaya untuk melakukan inovasi pada bidang teknologi telah mendukung bidang perindustrian Jepang pada tahun 1960.<sup>4</sup> Banyaknya penemuan yang dilakukan telah mendorong pemasaran produk teknologi hingga ranah internasional sehingga menjadikan Jepang sebagai salah satu negara paling inovatif

---

<sup>1</sup> Keichi Oshima, "Technological Innovation and Industrial Research in Japan," *Research Policy* 13, no.5 (1984): 287, [https://doi.org/10.1016/0048-7333\(84\)90012-X](https://doi.org/10.1016/0048-7333(84)90012-X).

<sup>2</sup> *Ibid.*, 285 - 286.

<sup>3</sup> Tom Forester, "How Japan Became No.1 in It: (Part One) Japan's Information Technology Strategy," *Policy and Society* 6, 1(1993): 25, doi: <https://doi.org/10.1080/10349952.1993.11876784>.

<sup>4</sup> Keichi Oshima, *Technological Innovation and Industrial Research in Japan*, 289.

di bidang teknologi.<sup>5</sup> Mulai dari pengembangan mesin, bahan kimia, baja dan besi pada bidang industri berat,<sup>6</sup> peralatan seputar teknologi informasi dan komunikasi (IT) dan produk elektronik hingga pengembangan teknologi robot serta berbagai bidang lain.<sup>7</sup> Oleh karena itu produk teknologi buatan Jepang dapat sangat dikenal oleh berbagai pihak di dunia.

Meskipun Jepang telah menciptakan berbagai penemuan di bidang teknologi, mereka masih memiliki tujuan lain memperkuat bidang tersebut. Sebelumnya pun Jepang juga telah berhasil memasarkan produk – produk digital di bidang keuangan dan komputer seperti *big data* serta produk hiburan, seperti industri film dan animasi yang disebut sebagai *anime* hingga *video game*. Namun, adanya perkembangan teknologi informasi dan komunikasi (internet) menjadi alasan Jepang untuk mengembangkan rencana *Super Smart Society* dan *Japan Model*.<sup>8</sup>

*Super Smart Society* dimaksudkan sebagai upaya Jepang untuk memajukan dan memenuhi kebutuhan hidup sosial masyarakat dengan menggunakan kemajuan teknologi. Keberadaan kemajuan teknologi ini diharapkan dapat menghubungkan antara teknologi di dunia siber atau *cyberspace* seperti *cybersecurity*, *artificial intelligence*, *big data* dan *internet of things* dengan teknologi di dunia nyata yang

---

<sup>5</sup> Carin Holroyd, *Innovation: 'Japan Inc.' in the 21<sup>st</sup> Century: Technological Development in Contemporary Japan: Possibility and Challenges* (Osaka: Suntory Foundation, 2017) hlm. 5, <https://www.suntory.com/sfnd/jgc/forum/011/pdf/011.pdf>.

<sup>6</sup> Keichi Oshima, *Technological Innovation and Industrial Research in Japan*, 286.

<sup>7</sup> Tom Forester, *How Japan Became No.1 in It: (Part One) Japan's Information Technology Strategy*, 25 dan 28.

<sup>8</sup> Carin Holroyd, *Innovation: 'Japan Inc.' in the 21<sup>st</sup> Century: Technological Development in Contemporary Japan: Possibility and Challenges*, 6-7.

berhubungan dengan kebutuhan logistik, layanan publik, transportasi, keuangan, manufaktur, dan energi. Kemudian Jepang diharuskan untuk meningkatkan kemampuan pada hal – hal seputar *cybersecurity*, *internet of things*, analisis *big data*, *artificial intelligence* serta berbagai teknologi supercomputer lain guna mendukung implementasi *Super Smart Society*.<sup>9</sup> Lalu, *Japan Model* dimaksudkan sebagai upaya Jepang untuk menjadi negara yang dapat dipercaya, termasuk juga dalam bidang keamanan informasi di mana memiliki kualitas tinggi untuk menjamin keamanan dan keselamatan masyarakat. Jepang juga berharap agar *Japan Model* ini dapat diterapkan pada ranah global<sup>10</sup> sehingga juga dapat mendukung kerja sama secara internasional, khususnya pada bidang *cybersecurity*.<sup>11</sup>

Guna mencapai tujuan tersebut, Jepang perlu menguasai teknologi *supercomputer* yang berkaitan dengan keamanan data dan informasi. Teknologi pada bidang ini tentunya merupakan hal baru bagi Jepang karena berbeda dengan industri yang mereka kembangkan sejak akhir Perang Dunia Kedua. Mengingat bahwa teknologi yang dikembangkan oleh Jepang sejak setelah masa Perang Dunia Kedua belum diarahkan pada teknologi *super computer*. Hal ini disebabkan karena

---

<sup>9</sup> Carin Holyroyd, “Technological innovation and building a ‘super smart’ society: Japan’s vision of society 5.0,” *Journal of Asian Public Policy* 15, No. 1 (2022):3-4, <https://doi.org/10.1080/17516234.2020.1749340>.

<sup>10</sup> Information Security Policy Council, *First National Strategy on Information Security: Toward the Realization of A Trustworthy Society*, 2 Februari 2006, Tokyo: National center of Incident readiness and Strategy for Cybersecurity, hlm.5.

<sup>11</sup> Paul Kallender & Christopher W. Hughes, “Japan’s Emerging Trajectory as a “Cyber Power” : From Securitization to Militarization of Cyber Space,” *Journal of Strategic Studies* 40 (2016): 14-15, doi : <https://doi.org/10.1080/01402390.2016.1233493>



Jepang baru mengikuti perkembangan di bidang *cybersecurity* pada tahun 2013.<sup>12</sup> Dengan ini, Jepang masih memiliki batasan pada penguasaan bidang *cybersecurity* sehingga mudah menjadi target dari tingginya ancaman *cyberattack* dari banyak aktor eksternal (internasional), seperti kasus – kasus pada penelitian ini. Tujuan Jepang untuk mengembangkan *Super Smart Society* dan *Japan Model* tentunya perlu didukung oleh kapabilitas *cybersecurity* yang tinggi. Oleh karena itu, hal ini juga menjadi alasan pendorong mengapa Jepang perlu meningkatkan *cybersecurity* karena memiliki program – program yang membutuhkan keahlian tinggi pada *cybersecurity* di mana hal tersebut terlihat masih menghadapi berbagai keterbatasan.

Oleh karena itu, topik kerja sama *cybersecurity* antara Jepang dan AS penting dibahas. Alasan mengapa topik ini penting untuk dibahas secara mendalam karena isu *cybersecurity* dapat mempersulit kehidupan negara dan segala isinya pada berbagai bidang. Terlebih lagi bila negara tidak memiliki kapabilitas pada bidang ini. Hal ini dapat menimbulkan kesulitan bagi negara jika terjadi kasus pencurian data sebagai dampak dari adanya *cyberattack*. Khususnya di dalam penelitian ini, penguasaan kapabilitas di bidang *cybersecurity* akan sangat membantu Jepang dalam melindungi informasi dan data sehingga meningkatkan kehidupan masyarakat dapat menjalin hubungan baik dengan negara lain.

Selain itu juga karena mengingat posisi penting yang dipegang oleh Jepang sebagai aliansi militer dan diplomasi pada kawasan Asia Pasifik. Adanya

---

<sup>12</sup> Franz-Stefan Gady, “Japan: The Reluctant Cyberpower,” *Ifri Center For Asian Studies*, No. 91(2017): 5, diakses pada 24 April 2022, [https://www.ifri.org/sites/default/files/atoms/files/gady\\_japan\\_cyberpower\\_2017.pdf](https://www.ifri.org/sites/default/files/atoms/files/gady_japan_cyberpower_2017.pdf).

pertentangan yang terjadi di antara AS terhadap China dan Korea Utara memaksa AS untuk memperkuat kapabilitas militer dan *cybersecurity* mereka. Dengan adanya hal ini, tentunya mengharuskan Jepang sebagai negara aliansi AS untuk ikut meningkatkan kapabilitas *cybersecurity* guna mendukung hubungan aliansi AS dan Jepang dan juga mendukung upaya “*rebalance*” AS di kawasan Asia Pasifik.<sup>13</sup> Tingginya *cyberattack* yang dialami Jepang sudah memberikan dampak secara komprehensif sehingga membuat Jepang perlu menjalin kerja sama bilateral secara komprehensif bersama dengan AS sebagai negara aliansi Jepang dalam menanggulangi isu *cybersecurity* yang dialami oleh Jepang. Hal – hal inilah yang dilihat dapat mendorong kerja sama bilateral *cybersecurity* secara komprehensif antara Jepang dan AS.

## **1.2. Identifikasi Masalah**

Meskipun Jepang telah menjadi salah satu negara yang menjadi pelopor pengembangan teknologi, tetapi belum dapat membantu Jepang untuk menghadapi *cyberattack*. Batasan yang Jepang hadapi di bidang *cybersecurity* membuatnya menjadi sasaran *cyberattack* dari negara lain, seperti China, Rusia, dan Korea Utara.<sup>14</sup> Kelemahan ini tentunya sangat berpotensi menjadi ancaman terhadap keamanan informasi dan data – data rahasia milik negara, pemerintah, perusahaan hingga data milik masyarakat sehingga dapat mengganggu kestabilan negara pada

---

<sup>13</sup> Paul Kallender dan Christopher W. Hughes, *Japan's Emerging Trajectory as a 'Cyber Power': From Securitization to Militarization of Cyberspace*, 17.

<sup>14</sup> James Andrew Lewis, *U.S.-Japan Cooperation in Cybersecurity*, (Washington: Center for Strategic Studies & International Studies, 2015) hlm. 1, [https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy\\_files/files/publication/151105\\_Lewis\\_USJapanCyber\\_Web.pdf](https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151105_Lewis_USJapanCyber_Web.pdf).

berbagai sektor. Contohnya adalah kasus penyerangan *Advanced Persistent Threats* (APT) yang dialami oleh Mitsubishi Heavy Industries (MHI) serta berbagai kasus *cyberattack* lain yang akan dijelaskan pada bab berikutnya. *Cyberattack* tipe ini menggunakan fasilitas *email* untuk mengirimkan *file* berisikan virus yang sulit untuk dideteksi oleh perangkat lunak (*software*) anti virus. Virus ini akan mengakses seluruh data di dalam komputer korban sehingga pelaku dapat mengambil berbagai data penting dari komputer tersebut.<sup>15</sup>

Kembali diingat, Jepang merupakan salah satu negara pelopor dari penemuan dan pengembangan teknologi hingga dapat memberikan keberhasilan dalam bidang ekonomi, baik pada tingkat produktivitas industri hingga pendapatan individu masyarakat.<sup>16</sup> Meskipun demikian, Jepang masih harus menjalin kerja sama dengan Amerika Serikat (AS) sebagai negara aliansinya untuk dapat membantu Jepang di bidang *cybersecurity*. Hal inilah yang dipertanyakan melalui tulisan ini, yakni alasan mengapa Jepang perlu menjalin kerja sama dengan AS terkait *cybersecurity* untuk menanggulangi ancaman *cyberattack* walaupun, Jepang memiliki kapabilitas besar dalam penguasaan teknologi.

Berdasarkan segi historis, Jepang telah memiliki hubungan bilateral yang dekat dengan AS sejak terjadi penandatanganan perjanjian keamanan bilateral negara tahun 1960 sehingga memudahkan terjalinnya kerja sama antar kedua negara.<sup>17</sup> Hubungan ini dapat membantu Jepang untuk menghadapi ancaman

---

<sup>15</sup> Motohiro Tsuchiya, "Japan's Response to Cyber Threats in the Surveillance Age," *Seton Hall Journal of Diplomacy and International Relations* 17, no. 1-2 (2015-2016): 10-11, diakses pada 30 April 2022, <https://www.proquest.com/docview/1904774776>.

<sup>16</sup> Carin Holroyd, *Innovation: 'Japan Inc.' in the 21<sup>st</sup> Century*, 5.

<sup>17</sup> Japan-U.S. Security Treaty 1960.

*cyberattack* melalui aksi *collective self-defense* yang dilakukan bersama AS. Terlebih dengan adanya deklarasi yang disampaikan oleh pemerintah Jepang melalui rapat Information Security Policy Council (ISPC) terkait hak Jepang untuk melakukan aksi *self-defense* di bawah naungan hukum internasional terhadap *cyberattack* yang mengancam negara tersebut.<sup>18</sup>

Dalam upaya menanggulangi isu *cybersecurity*, Jepang dan AS telah mengadakan forum diskusi dan kerja sama bilateral, seperti *Japan-U.S. Cyber Dialogue*, *Japan-U.S. Policy Cooperation on the Internet Economy*, *2+2 Meeting*, *U.S.-Japan Cyber Defense Policy Working Group (CDPWG)*, *Japan-US IT Forum*, dan *U.S.- Japan Business Dialogue on the Internet Economy* serta berbagai forum lain. Pada bulan April 2006, Amerika Serikat bersama Jepang telah menandatangani kerja sama melalui *Memorandum of Understanding Concerning Cooperation Regarding Information Assurance and Computer Network Defense*.<sup>19</sup>

### **1.2.1. Pembatasan Masalah**

Penelitian ini memfokuskan pembahasan pada kasus – kasus besar *cyberattack* pada awal tahun 2011 di Jepang yang mana turut mendatangkan banyak isu *cybersecurity* baru. Kasus ini juga memunculkan kerja sama antara Jepang dan Amerika Serikat sebagai negara aliansi dalam menanggulangi ancaman *cyberattack*. Penelitian ini juga akan lebih difokuskan pada posisi Jepang sebagai korban dari kasus *cyberattack* yang telah terjadi secara besar – besaran hingga merugikan

---

<sup>18</sup> Paul Kallender, “Japan, The Ministry of Defense and Cyber-Security,” *The RUSI Journal* 159, no.1(2014): 98, <https://doi.org/10.1080/03071847.2014.895264>.

<sup>19</sup> Paul Kallender & Christopher W. Hughes, *Japan’s Emerging Trajectory as a Cyber Power” : From Securitization to Militarization of Cyber Space*, 16-17.

banyak badan pemerintahan, perusahaan serta masyarakat. Jarak waktu penelitian akan dibatasi dari tahun 2011 sampai dengan tahun 2019. Tahun 2011 dipilih sebagai tahun awal pembatasan masalah karena marak terjadi *cyberattack* yang dialami oleh Jepang di mana juga menjadi tahap awal pada kesadaran Jepang terhadap *cybersecurity*. Kemudian tahun 2019 dipilih sebagai batasan tahun terakhir untuk membatasi pembahasan *cybersecurity* Jepang sebelum adanya pandemi COVID-19. Adanya pandemi mengakibatkan negara lebih memprioritaskan untuk berfokus pada isu keamanan kesehatan sehingga terdapat pertemuan – pertemuan terkait pembahasan *cybersecurity* yang harus ditunda atau hanya dilakukan secara *virtual*.

### **1.2.2. Perumusan Masalah**

Berdasarkan bagian latar belakang, identifikasi dan pembatasan masalah, maka pertanyaan pada penelitian ini **“Mengapa Jepang sebagai negara dengan penguasaan teknologi tinggi harus melakukan kerja sama secara komprehensif dengan Amerika Serikat terkait penanggulangan isu *cybersecurity*?”**

## **1.3. Tujuan dan Kegunaan Penelitian**

### **1.3.1. Tujuan Penelitian**

Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis faktor – faktor yang menyebabkan terjadinya perluasan kerja sama *cybersecurity* secara komprehensif pada sektor politik, militer, dan ekonomi antara Jepang dan Amerika Serikat dalam menanggulangi ancaman *cyberattack* yang semulanya hanya berada pada ranah *collective self-defense* di bidang pertahanan militer.

### **1.3.2. Kegunaan Penelitian**

Penelitian ini diharapkan dapat memberikan informasi dan pandangan baru terkait alasan yang menjadi penyebab Jepang melakukan kerja sama *cybersecurity* secara komprehensif bersama dengan AS dalam menghadapi ancaman *cyberattack* yang ditunjukkan terhadap Jepang. Dengan melihat perluasan kerja sama dari *collective self-defense* kedua negara kepada keamanan komprehensif di bidang *cybersecurity* ini diharapkan dapat menambah literatur terkait *cybersecurity* di ranah Hubungan Internasional. Oleh karena itu, pembuatan penelitian ini juga diharapkan dapat membuka jalan bagi penelitian selanjutnya terkait kerja sama *cybersecurity* antara Jepang dan AS.