IMPLEMENTASI KERJA SAMA CISA DAN CSA DALAM MENANGANI ANCAMAN SIBER TAHUN 2019-2022

Farras Putri Nabila¹, Frentika Wahyu R²

Program Studi Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Mulawarman

Abstrak

Penelitian ini membahas implementasi kerja sama antara *Cybersecurity and Infrastructure Security Agency* (CISA) dari Amerika Serikat dan *Cyber Security Agency* (CSA) dari Singapura dalam merespons ancaman siber selama periode 2019-2022. Kerja sama ini dilatarbelakangi oleh peningkatan serangan siber lintas negara, seperti *phishing* dan *ransomware*, yang mengancam infrastruktur digital dan keamanan informasi nasional. Penelitian menggunakan metode kualitatif dengan pendekatan deskriptif-eksplanatif serta memanfaatkan data sekunder dari dokumen resmi, laporan lembaga, dan literatur akademik. Dengan menggunakan teori keamanan non-tradisional dari Copenhagen School, penelitian ini menganalisis bagaimana isu siber dikonstruksikan sebagai ancaman eksistensial yang membutuhkan respons luar biasa. Di sisi lain, konsep cybersecurity digunakan untuk menjelaskan jenis serangan serta strategi pertahanan digital. Hasil penelitian menunjukkan bahwa kerja sama CISA-CSA diwujudkan melalui pertukaran informasi teknis, pelatihan bersama, dan peningkatan kapasitas SDM di bidang keamanan digital. Kolaborasi ini memperkuat ketahanan digital nasional serta mempercepat penanganan insiden, meskipun terkendala oleh perbedaan regulasi dan isu sensitivitas data. Studi ini menegaskan pentingnya pendekatan keamanan non-tradisional dan kerja sama internasional dalam menghadapi ancaman siber yang semakin kompleks.

Kata Kunci: CISA, CSA, Ancaman Siber.

Abstract

This study examines the implementation of cybersecurity cooperation between the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and Singapore's Cyber Security Agency (CSA) from 2019 to 2022. Triggered by increasing cross-border cyber threats such as phishing and ransomware, the collaboration aims to protect national digital infrastructure and information security. Using a qualitative, descriptive-explanatory method and secondary data, the study applies the Copenhagen School's non-traditional security theory to analyze how cyber threats are securitized as existential threats, and cybersecurity concepts to explain attack types and defense strategies. The findings show that the CISA-CSA cooperation is realized through technical information sharing, joint training, and human resource capacity-building in digital security. Despite challenges like regulatory differences and data sensitivity, the partnership enhances national cyber resilience and accelerates incident response. This study highlights the significance of non-traditional security approaches and international collaboration in addressing complex cyber threats.

Keywords: CISA, CSA, Cyber Threats.

1. PENDAHULUAN

Cybercrime dapat didefinisikan sebagai segala bentuk tindak kriminal yang melibatkan penggunaan komputer, jaringan komputer, atau perangkat digital lainnya. Kejahatan ini dapat terjadi baik dengan menyerang sistem dan data (*offences against computer systems*), maupun menggunakan sistem

komputer sebagai sarana melakukan kejahatan (*offences by means of computer systems*). *United Nations Office on Drugs and Crime* (UNODC) menyatakan bahwa *cybercrime* adalah bentuk kejahatan transnasional yang terus berkembang, terjadi dalam ruang siber yang tidak mengenal batas geografis, sehingga memerlukan respons yang cepat, dinamis, dan bersifat internasional. Kejahatan siber yang terja phishing dan *ransomware*.

Laporan *Global Cybersecurity Index* (GCI) 2020 yang dirilis oleh *International Telecommunication Union* (ITU) mencerminkan seberapa serius negara-negara di dunia memandang isu keamanan siber dan bagaimana mereka mengembangkan kapabilitasnya untuk merespons ancaman tersebut. Hasil laporan tersebut menunjukkan bahwa meskipun sebagian besar negara telah memiliki kerangka kerja hukum dan teknis untuk menangani ancaman siber, masih terdapat kesenjangan besar dalam hal kemampuan nyata menghadapi serangan yang terus berkembang. Negara seperti Amerika Serikat dan Singapura memiliki skor tinggi, yang menunjukkan kemajuan signifikan dalam membangun strategi nasional dan pusat operasi keamanan siber (ITU, 2020).

Meskipun menempati peringkat atas dalam *Global Cybersecurity Index* 2020, negara-negara seperti Amerika Serikat dan Singapura tetap menghadapi berbagai tantangan serius dalam menghadapi kejahatan siber yang semakin meningkat terutama saat Covid-19. Untuk menghadapi ancaman siber yang semakin kompleks, berbagai negara membentuk lembaga khusus yang menangani isu keamanan digital secara terstruktur dan strategis. Di Amerika Serikat, lembaga tersebut dikenal dengan nama *Cybersecurity and Infrastructure Security Agency* (CISA), sedangkan di Singapura dikenal sebagai *Cyber Security Agency of Singapore* (CSA). Kedua institusi ini memiliki tugas penting dalam menjaga ketahanan siber nasional dan memperkuat respons terhadap berbagai bentuk serangan digital.

Pada tahun 2021, CISA dan CSA secara resmi mempererat hubungan bilateral dalam bidang keamanan siber dengan menandatangani Memorandum of Understanding tentang kerja sama strategis dalam pertukaran informasi, pelatihan, serta penanganan insiden siber. Kerja sama ini lahir dari kesadaran

bersama bahwa pelaku serangan siber seringkali beroperasi secara global dan memanfaatkan kelemahan di berbagai titik jaringan internasional. Oleh karena itu, respons yang efektif menuntut koordinasi lintas batas, pertukaran intelijen siber secara real-time, serta pengembangan kapasitas bersama untuk deteksi dan mitigasi ancaman.

2. METODE

Dalam penelitian ini, jenis penelitian yang dipergunakan adalah penelitian eksplanatif. Penelitian eksplanatif bertujuan menjelaskan alasan dari suatu fenomena pada peristiwa yang akan diteliti oleh penulis (Neuman,2016). Dalam penelitian ini, Penulis berusaha menjelaskan mengenaiimplementasi kerja sama Amerika Serikat-Singapura dalam menangani ancaman siber melalui CISA dan CSA tahun 2019-2022. Penelitian ini berfokus pada bagaimana implementasi kerja sama Amerika Serikat-Singapura dalam menangani ancaman siber melalui CISA dan CSA tahun 2019-2022. Jenis data yang dipergunakan dalam penelitian ini terdiri atas data sekunder. Data sekunder yang digunakan penulis dalam penelitian ini tentunya mempunyai kredibilitas dan memiliki kesesuaian dengan objek penelitian yang buku, jurnal, artikel bersumber dari arsip, dokumentasi, naskah perjanjian dimana data sekunder didapatkan dari lembaga pemerintah maupun data yang bukan berasal dari dokumen pemerintahan. Pada penelitian ini, penulis menggunakan teknik pengumpulan data studi pustaka (*Library Research*). Studi pustaka merupakan teknik pengumpulan data yang didapatkan dari data sekunder sehingga penulis tidak langsung melakukan proses penelitian di lapangan (Zed, 2004).

Pada penelitian ini, penulis menggunakan teori teori keamanan non-tradisional milik Barry Buzan, Ole Wæver, dan Jaap de Wilde dari Copenhagen School. Selain itu, penulis juga menggunakan konsep keamanan siber.

a. Teori Keamanan Non-Tadisional

Menurut teori ini, keamanan tidak hanya soal menjaga kedaulatan negara dari serangan militer, tetapi juga melibatkan perlindungan terhadap lima

sektor penting kehidupan: militer, politik, ekonomi, sosial, dan lingkungan (Buzan et al., 1998). Dengan membagi keamanan ke dalam sektor-sektor ini, pendekatan non-tradisional memberikan ruang bagi isu-isu yang sebelumnya tidak dianggap sebagai ancaman keamanan, salah satunya adalah keamanan siber.

Konsep inti dari teori ini adalah sekuritisasi (*securitization*). Sekuritisasi adalah proses di mana suatu isu dikonstruksikan atau dibentuk sebagai ancaman serius dan mendesak. Proses ini biasanya dilakukan oleh aktor seperti pemerintah atau lembaga resmi melalui wacana publik atau pernyataan politik. Ketika isu tersebut berhasil dipersepsikan sebagai ancaman eksistensial, yang artinya dianggap dapat membahayakan kelangsungan negara atau masyarakat sehingga perlu tindakan khusus atau luar biasa dapat dilakukan untuk menghadapinya, meskipun cara-cara tersebut di luar kebijakan normal.

Dalam konteks keamanan siber, teori keamanan non-tradisional ini sangat relevan. Ancaman di dunia digital seperti serangan terhadap sistem informasi, pencurian data, dan gangguan terhadap infrastruktur penting tidak bersifat fisik, tetapi dapat berdampak besar terhadap stabilitas nasional dan keamanan ekonomi. Oleh karena itu, banyak negara telah menyekuritisasi isu ini, menjadikannya bagian dari agenda strategis nasional. Artinya, negara menganggap ancaman siber sebagai masalah keamanan serius yang harus ditangani secara prioritas.

b. Konsep Keamanan Siber

Cybersecurity atau keamanan siber merupakan konsep yang mengacu pada perlindungan sistem informasi, jaringan, dan data dari berbagai ancaman digital yang dapat merusak, mencuri, atau mengganggu integritas dan ketersediaannya. Menurut William Stallings (2012), keamanan siber adalah perlindungan terhadap sistem informasi dari pencurian atau kerusakan, baik terhadap perangkat keras, perangkat lunak, maupun informasi yang dikandungnya, serta perlindungan dari gangguan layanan yang disediakan sistem tersebut..

3. IMPLEMENTASI KERJA SAMA CISA DAN CSA DALAM MENANGANI ANCAMAN SIBER TAHUN 2019-2022

Cybercrime di Amerika Serikat

Sebelum tahun 2019, Amerika Serikat telah mengalami peningkatan ancaman kejahatan siber, khususnya *phishing* dan *ransomware*. Berdasarkan laporan *Internet Crime Complaint Center (IC3) FBI*, sejak 2017 jumlah serangan dan kerugian finansial akibat kejahatan siber menunjukkan tren yang meningkat. Tahun 2017 mencatat lebih dari 25.000 kasus *phishing* dan kerugian sekitar 29 juta dolar AS, serta 1.783 laporan *ransomware* dengan kerugian lebih dari 2,3 juta dolar AS. Tren ini berlanjut pada 2018, di mana kasus *phishing* naik menjadi lebih dari 26.000 laporan dengan kerugian melebihi 48 juta dolar AS.

Memasuki tahun 2019, jumlah laporan *phishing* melonjak drastis menjadi lebih dari 114.000 kasus, dengan pola serangan yang meniru institusi resmi guna mencuri data sensitif. Serangan *ransomware* juga meningkat menjadi 2.047 kasus, menargetkan sektor-sektor penting seperti layanan kesehatan, pendidikan, dan pemerintahan.

Puncak eskalasi terjadi pada 2020 ketika pandemi Covid-19 mempercepat digitalisasi. Peralihan kegiatan ke ranah daring memperluas permukaan serangan. Dalam satu tahun, laporan *phishing* meningkat lebih dari dua kali lipat menjadi 241.342 kasus, banyak di antaranya mengeksploitasi isu pandemi. *Ransomware* juga melonjak menjadi 2.474 laporan, dengan korban berasal dari institusi yang tidak siap menghadapi transisi digital mendadak.

Perkembangan ini menunjukkan bahwa pandemi tidak hanya menciptakan krisis kesehatan global, tetapi juga memperdalam krisis keamanan digital. Lonjakan serangan menunjukkan lemahnya kesiapan sistem dalam menghadapi ancaman siber yang terus berkembang. Oleh karena itu, diperlukan sistem pertahanan siber yang lebih kuat, peningkatan deteksi dini, serta kerja sama internasional yang lebih luas. Pengalaman Amerika Serikat selama 2017–2020 menjadi cerminan penting bahwa keamanan siber harus menjadi prioritas dalam pembangunan nasional dan kerja sama global.

Cybercrime di Singapura

Sebelum tahun 2019, Singapura telah mengidentifikasi kejahatan siber sebagai isu strategis yang perlu ditangani secara serius, mengingat tingginya konektivitas digital negara tersebut. Ancaman seperti *phishing* dan *ransomware* telah direspons sejak dini melalui pembentukan *Cyber Security Agency of Singapore* (CSA) pada 2015. CSA bertugas mengoordinasikan keamanan digital nasional, melindungi *Critical Information Infrastructure* (CII), serta menjalin kerja sama regional dan internasional, termasuk melalui forum tahunan *Singapore International Cyber Week* (SICW). Upaya ini diperkuat oleh pengesahan *Cybersecurity Act* pada 2018, yang memberikan dasar hukum bagi intervensi negara dalam menjaga keamanan siber.

Pada 2019, lonjakan serangan siber mulai terlihat. CSA mencatat lebih dari 47.000 situs *phishing* berbahaya yang memanfaatkan domain “.sg” untuk menyamar sebagai entitas resmi. Sementara itu, terdapat 35 serangan *ransomware* yang sebagian besar menargetkan sektor UKM, khususnya di bidang manufaktur dan jasa profesional. Hal ini menandakan bahwa meskipun memiliki infrastruktur keamanan yang mapan, Singapura tetap menghadapi celah yang dimanfaatkan oleh pelaku siber.

Situasi memburuk pada 2020 ketika pandemi Covid-19 mempercepat digitalisasi dan memperluas permukaan serangan. Meskipun jumlah situs *phishing* tetap tinggi (sekitar 47.000 situs), pola serangan menjadi lebih kompleks dengan memanfaatkan tema pandemi seperti vaksinasi dan bantuan pemerintah. Serangan *ransomware* meningkat drastis menjadi 89 kasus, dengan taktik baru seperti *Big Game Hunting* dan *leak and shame*, yang menargetkan organisasi besar dan mengancam publikasi data jika tebusan tidak dibayar.

Pengalaman ini menunjukkan bahwa kesiapan kelembagaan dan teknologis tidak cukup untuk sepenuhnya mengeliminasi risiko siber. Peningkatan jumlah dan kompleksitas serangan menegaskan pentingnya literasi digital publik, ketahanan sistem yang adaptif, serta kolaborasi lintas sektor dan antarnegara. Ancaman siber yang bersifat lintas batas memerlukan respons kolektif dan kerja sama internasional yang lebih erat.

Upaya Penanganan Kejahatan Siber di Amerika Serikat dan Singapura

Sebelum penandatanganan *Memorandum of Understanding* (MoU) pada tahun 2021, Amerika Serikat dan Singapura telah lebih dahulu mengembangkan berbagai kebijakan strategis untuk memperkuat pertahanan siber nasional mereka. Kedua negara menghadapi peningkatan serangan siber lintas negara, termasuk *phishing*, *ransomware*, dan eksploitasi kerentanan infrastruktur digital. Untuk merespons ancaman ini, lembaga utama di bidang keamanan siber, *Cybersecurity and Infrastructure Security Agency* (CISA) di Amerika Serikat dan *Cyber Security Agency* (CSA) di Singapura untuk menjalankan sejumlah inisiatif penting.

Di Amerika Serikat, CISA mengeluarkan kebijakan seperti *Emergency Directive* 19-01 dan *Binding Operational Directive* 19-02 untuk memperkuat sistem DNS dan mempercepat penanganan kerentanan. Selain itu, CISA aktif menyebarluaskan indikator kompromi (IoCs), membentuk forum kolaboratif seperti *Industrial Control Systems Joint Working Group*, serta meluncurkan kampanye nasional seperti “#StopRansomware.” Di masa pandemi 2020, CISA meningkatkan layanannya melalui CISA Central, menyediakan simulasi serangan *phishing*, alat evaluasi kesiapan *ransomware*, dan layanan pemindaian kerentanan secara gratis bagi instansi publik dan sektor penting lainnya.

Sementara itu, Singapura melalui CSA menginisiasi *Cybersecurity Labelling Scheme* (CLS) untuk meningkatkan transparansi keamanan produk IoT, serta mendirikan *ASEAN-Singapore Cybersecurity Centre of Excellence* (ASCCE) sebagai pusat pelatihan dan kerja sama regional. Program *Vulnerability Disclosure* dan *Bug Bounty* turut melibatkan komunitas keamanan siber dalam memperkuat ekosistem digital. Menyadari peningkatan risiko selama pandemi, CSA meluncurkan *Safer Cyberspace Masterplan 2020*, yang menargetkan perlindungan infrastruktur penting, peningkatan kesadaran publik, dan penguatan kapabilitas teknis nasional. Kolaborasi internasional juga terjalin, seperti dengan *National Cyber Security Centre* (NCSC) Inggris dalam pengembangan alat simulasi *Exercise-in-a-Box*. CSA juga mengembangkan

platform deteksi siber berbasis kecerdasan buatan untuk mempercepat respons terhadap insiden.

Langkah-langkah strategis yang dilakukan oleh CISA dan CSA menunjukkan pendekatan yang komprehensif, responsif, dan terkoordinasi dalam menghadapi tantangan keamanan siber modern. Upaya ini menjadi fondasi penting bagi kerja sama bilateral yang lebih erat, serta mencerminkan pentingnya kolaborasi internasional dalam mengelola risiko siber yang terus berkembang.

Kerja Sama Antara CISA dan CSA pada Tahun 2021

Kerja sama antara *Cybersecurity and Infrastructure Security Agency* (CISA) dari Amerika Serikat dan *Cyber Security Agency* (CSA) dari Singapura diperkuat melalui penandatanganan *Memorandum of Understanding* (MoU) pada Agustus 2021. MoU ini merupakan pembaruan dari kesepakatan sebelumnya yang telah dimulai sejak 2016, dan ditandatangani langsung oleh Direktur CISA, Jen Easterly, serta Kepala Eksekutif CSA, David Koh. Pembaruan ini menegaskan komitmen kedua negara untuk mempererat kemitraan dalam menghadapi eskalasi ancaman siber transnasional yang semakin kompleks dan tidak mengenal batas negara.

Peningkatan kerja sama ini dilatarbelakangi oleh semakin seringnya serangan siber yang dilakukan oleh aktor-aktor dengan kapabilitas tinggi, baik dari kelompok kriminal terorganisir maupun aktor negara. Serangan tersebut berpotensi merusak infrastruktur kritis dan mengguncang stabilitas ekonomi global. Oleh karena itu, dibutuhkan respons kolektif yang terkoordinasi secara internasional. Dalam hal ini, pertukaran informasi dan intelijen teknis secara real-time dipandang sebagai komponen utama dalam membangun ketahanan digital yang efektif. Direktur CISA menekankan pentingnya kolaborasi lintas negara sebagai bagian dari strategi nasional keamanan siber, sedangkan pihak CSA menyoroti pentingnya menciptakan ruang digital yang aman, stabil, dan dapat dioperasikan bersama.

Melalui MoU 2021, CISA dan CSA menyepakati enam lingkup utama kerja sama. Pertama, pertukaran informasi secara rutin mengenai ancaman dan tren serangan siber terkini. Kedua, koordinasi respons terhadap insiden siber

yang memiliki potensi dampak besar. Ketiga, berbagi panduan, pengetahuan, serta praktik-praktik terbaik dalam menghadapi berbagai tantangan keamanan digital. Keempat, pelaksanaan pelatihan dan latihan bersama guna meningkatkan kapasitas teknis dan kesiapsiagaan personel. Kelima, penguatan kesadaran publik terhadap pentingnya keamanan siber, dan keenam, pengembangan kapasitas sumber daya manusia yang kompeten di bidang ini.

Selain poin-poin tersebut, MoU juga membuka jalan bagi kerja sama di sektor strategis lainnya yang berkaitan dengan masa depan keamanan siber, termasuk teknologi kritis (*critical technologies*) dan kegiatan penelitian serta pengembangan (R&D). Kedua negara sepakat bahwa kemajuan teknologi harus diimbangi dengan peningkatan ketahanan terhadap potensi ancaman digital yang semakin canggih.

Tujuan keseluruhan dari kerja sama ini adalah untuk membangun mekanisme koordinasi yang lebih efektif antara lembaga-lembaga terkait, menetapkan jalur komunikasi yang aman dalam pertukaran informasi sensitif, serta menyusun kerangka kerja teknis dan operasional yang dapat mendukung respons cepat terhadap insiden siber. Dengan fondasi ini, Amerika Serikat dan Singapura berkomitmen untuk memperkuat ketahanan digital nasional sekaligus memberikan kontribusi nyata bagi stabilitas dan keamanan ruang siber global.

Implementasi Kerja Sama CISA-CSA Berdasarkan MoU 2021

Setelah penandatanganan MoU pada Agustus 2021, kerja sama bilateral antara *Cybersecurity and Infrastructure Security Agency* (CISA) dari Amerika Serikat dan *Cyber Security Agency* (CSA) dari Singapura memasuki fase implementatif yang lebih konkret. MoU ini memperbarui kolaborasi sejak 2016 dan memperluas cakupan kerja sama melalui pilar strategis untuk memperkuat ketahanan digital, meningkatkan koordinasi respons, interoperabilitas teknis, dan pertukaran informasi di tengah meningkatnya kompleksitas ancaman siber global.

Salah satu pencapaian utama adalah penguatan mekanisme pertukaran informasi melalui forum seperti Dialog Siber AS-Singapura, yang membahas lanskap ancaman regional dan global. Inisiatif seperti *Joint Cyber Defense*

Collaborative (JCDC) dan kontribusi Singapura dalam pembaruan panduan keamanan siber global menunjukkan pendekatan berbagi pengetahuan dan praktik terbaik secara lintas batas.

Dalam hal respons insiden, meskipun tidak banyak dipublikasikan secara teknis, kedua lembaga telah memperkuat jalur komunikasi tetap, berbagi indikator kompromi (IoCs), dan taktik serangan untuk deteksi dini dan respons cepat. Upaya ini diperkuat dengan platform pelaporan insiden yang lebih terintegrasi.

Kemajuan juga terlihat dalam pengembangan kapasitas teknis, terutama melalui peluncuran kursus SG-ICS301 oleh CSA dan CISA pada 2023. Kursus ini fokus pada sistem *Operational Technology* (OT) dan *Critical Information Infrastructure* (CII), dengan pelatihan berbasis simulasi insiden nyata. Kegiatan ini dikaitkan dengan forum regional seperti OTCEP, memperluas dampak kerja sama ke tingkat kawasan.

Meskipun belum ada kampanye kesadaran publik berskala besar secara bersama, program nasional seperti *GoSafeOnline* (CSA) dan *Cybersecurity Awareness Program* (CISA) menunjukkan arah sinergi. Harmonisasi pesan edukatif membuka peluang kerja sama kampanye global di masa depan. Statistik tahun 2022 menunjukkan penurunan kasus *phishing* dan *ransomware* di kedua negara, mengindikasikan efektivitas kolaborasi dalam memperkuat ekosistem keamanan siber, meskipun tidak sepenuhnya dapat diatribusikan pada MoU.

Secara keseluruhan, kerja sama CISA-CSA telah berkembang menjadi kemitraan strategis yang dinamis, dengan kontribusi nyata tidak hanya pada tingkat nasional, tetapi juga dalam membentuk arsitektur keamanan siber global. Keberhasilan awal ini menjadi landasan bagi perluasan kerja sama ke sektor-sektor baru, seperti pengamanan teknologi kritis dan riset bersama di bidang keamanan digital dan terintegrasi.

4. KESIMPULAN

Berdasarkan hasil penelitian ini, dapat disimpulkan bahwa kerja sama antara CISA Amerika Serikat dan CSA Singapura yang diformalkan melalui

MoU tahun 2021 merupakan langkah strategis dalam memperkuat ketahanan siber menghadapi ancaman lintas negara. Kolaborasi ini mencakup pertukaran informasi, pelatihan bersama, simulasi penanganan insiden, serta pengembangan teknologi keamanan, yang secara nyata telah meningkatkan efektivitas respons terhadap insiden siber. Selain membangun mekanisme koordinasi yang efisien, kerja sama ini juga menumbuhkan kesadaran akan pentingnya kolaborasi internasional di era digital. Meski demikian, tantangan seperti perbedaan regulasi, sensitivitas pertukaran data intelijen, dan dinamika politik global tetap menjadi hambatan. Namun secara keseluruhan, pendekatan bilateral ini terbukti efektif dalam mendukung pertahanan siber yang tangguh, khususnya bagi keberlanjutan ekonomi digital Singapura yang sangat bergantung pada teknologi.

DAFTAR PUSTAKA

Barry Buzan, J. d. (1998). *Security: A New Framework for Analysis*. Lynne Rienner Publishers Inc.

Cybersecurity and Infrastructure Security Agency, CISA 2019 Highlights. Tersedia di https://www.cisa.gov/sites/default/files/publications/19_1222_cisa_2019_cisa_highlights.pdf

Cybersecurity and Infrastructure Security Agency, CISA 2020 Year in Review, tersedia di <https://www.cisa.gov/resources-tools/resources/cisa-2020-year-review>

Cybersecurity and Infrastructure Security Agency, CISA 2021 Year in Review, tersedia di https://www.cisa.gov/sites/default/files/publications/21-0860_EOY_REPORT_508c.pdf

Cybersecurity and Infrastructure Security Agency, CISA 2022 Year in Review, tersedia di <https://www.cisa.gov/2022-year-review>

Cybersecurity and Infrastructure Security Agency, United States and Singapore Expand Cooperation on Cybersecurity, tersedia di <https://www.cisa.gov/news-events/news/united-states-and-singapore-expand-cooperation-cybersecurity>

- Cyber Security Agency of Singapore, Singapore Cyber Landscape 2019, tersedia di <https://www.csa.gov.sg/resources/publications/singapore-cyber-landscape-2019>
- Cyber Security Agency of Singapore, Singapore Cyber Landscape 2020, tersedia di <https://www.csa.gov.sg/resources/publications/singapore-cyber-landscape-2020>
- Cyber Security Agency of Singapore, Singapore Cyber Landscape 2021, tersedia di <https://www.csa.gov.sg/resources/publications/singapore-cyber-landscape-2021>
- Cyber Security Agency of Singapore, Singapore Cyber Landscape 2022, tersedia di <https://www.csa.gov.sg/resources/publications/singapore-cyber-landscape-2022>
- Europol, Internet Organised Crime Threat Assessment (IOCTA) 2021, tersedia di <https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021>
- Internet Crime Complaint Centre, IC3 2019 Crime Report, tersedia di https://www.ic3.gov/AnnualReport/Reports/2019_ic3Report.pdf
- Internet Crime Complaint Centre, IC3 2020 Crime Report, tersedia di https://www.ic3.gov/AnnualReport/Reports/2020_ic3report.pdf
- Internet Crime Complaint Centre, IC3 2021 Crime Report, tersedia di https://www.ic3.gov/AnnualReport/Reports/2021_ic3report.pdf
- Internet Crime Complaint Centre, IC3 2019 Crime Report, tersedia di https://www.ic3.gov/AnnualReport/Reports/2022_ic3report.pdf
- United Nations Office on Drugs and Crime, Cybercrime, tersedia di <https://www.unodc.org/romena/en/cybercrime.html>
- Stallings, W. dan Brown, L. (2012). *Computer Security Principles and Practices*. Boston: Microsoft Corporation United States of America.
- Zed. Mestika. (2004). *Metodologi Penelitian Kepustakaan*. Jakarta: Yayasan Pustaka Obor Indonesia.