GLOBAL INSIGHTS JOURNAL
Jurnal Mahasiswa Program Studi
Ilmu Hubungan Internasional - FISIP - UNJANI
https:/ejournal.fisip.unjani.ac.id/index.php/GIJ
DOI : https://doi.org/10.36859/gij.v2i2.3365
Vol. 02 No. 02 Tahun 2025

Article Informations
Received: 18/02/2025; *Accepted*: 28/02/2025; *Published*: 30/06/2025
Corresponding Email:
afinalayalia17@gmail.com

KEPENTINGAN INGGRIS DALAM KERJA SAMA CYBER SECURITY DENGAN INDONESIA TAHUN 2016-2023

Afina Layalia Khoirunnisa[1)], Jusmalia Oktaviani[2)], Taufan Herdansyah Akbar[3)]

[1,2,3)]Program Studi Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Jenderal Achmad Yani, Indonesia

Abstract

Technological developments cannot stem the increasing diversity of threats to a country, one of which is cybercrime which can have an impact on aspects of defense, economy, ideology and even world order. Such as the case of the Wannacry ransomware attack in 2017 which caused quite large losses for the affected country. Therefore, this study aims to analyze in depth the national interests of the United Kingdom in cooperating with Indonesia as a country that excels in the field of cybersecurity. This analysis is based on a framework of thought, namely neo-realism, national interests and the concept of cybersecurity. This study was conducted using a qualitative approach and data collection techniques where the data sources used were supported by secondary data in the form of books, journals, articles and official documents related to the research being raised. The analysis in this study found that the national interests of a country greatly influence the behavior of that country.

Keywords: *Cyber Security, National Interests, UK, Indonesia*

PENDAHULUAN

Seiring berkembangannya realitas baru yaitu *cyber space* memudahkan aktivitas karena keterbatasan antara waktu dan juga jarak tidak lagi menjadi hambatan. Kemajuan teknologi yang ada memberikan banyak kontribusi terhadap keberlangsungan hidup manusia. Dalam hubungan internasional perkembangan teknologi yang terus berkembang pesat digunakan juga sebagai alat untuk bertahan dan bersaing dalam era globalisasi baik oleh negara maju maupun negara berkembang. Bahkan saat

ini keberlangsungan hidup suatu negara dapat bergantung pada *cyber security* yang mereka kembangkan. Disisi lain kemajuan teknologi dan kemudahan akses transformasi digital dapat menjadi dampak negatif.

Serangan terhadap sistem informasi seperti peretasan dan pencurian data menjadi suatu ancaman dalam *cyber space* karena adanya celah pada keamanan *cyber* yang dimanfaatkan oleh suatu individu maupun kelompok untuk mendapatkan keuntungan pribadi dengan menyalahgunakannya. Salah satu contohnya yaitu *ransomware Wannacry* tahun 2017 yang menyebabkan kerugian besar. Meningkatanya ancaman keamanan siber membuat Inggris menyadari pentingnya kerjasama siber untuk memperluas keamanan siber baik diluar yuridiksi maupun yang langsung berdampak langsung pada keamanan nasional Inggris. Penyelahgunaan seperti itu selain berdampak pada aspek keamanan nasional juga akan berdampak pada aspek ekonomi, ideologi dan juga sosial budaya.

Untuk mengatasi hal tersebut Inggris bekerjasama dengan negara lain yaitu Indonesia sebagai mitra kerjasama yang memiliki potensial di kawasan Asia Tenggara untuk memperkuat keamanan siber. Negara Inggris menandatangani nota kesepahaman (MoU) tentang *Cybersecurity* dengan Indonesia pada tahun 2018 yang saat ini telah diperpanjang. Indonesia dipilih oleh Inggris karena kedua negara sebelumnya miliki banyak histori baik dalam hubungan kerjasama di berbagai bidang. Selain itu kerjasama ini dilakukan dengan upaya untuk menjaga keamanan serta kepentingan nasional Inggris sebagai negara yang memiliki reputasi yang kuat, dan posisi Inggris pasca *Brexit* membuat Inggris perlu memperkuat hubungan bilateral. Dengan adanya kolaborasi ini dapat meningkatkan pentingnya kerjasama internasional dalam mengatasi kejahatan siber dengan memperkuat kapasitas keamanan siber.

METODE PENELITIAN

Metode penelitian adalah cara ilmiah untuk mendapatkan data yang valid dengan tujuan menemukan, membuktikan, dan mengembangkan data baru yang berguna untuk memahami, memecahkan, dan mengantisipasi masalah. Metode penelitian merupakan strategi sistematis yang digunakan untuk memperoleh informasi dan data guna menjawab pertanyaan penelitian. Dalam penelitian ini, digunakan metode kualitatif deskriptif berdasarkan studi literatur dengan pendekatan neorealisme, kepentingan nasional dan konsep *cybersecurity*.

PEMBAHASAN

A. Kasus Ransomware Wannacry

Kasus kejahatan *cyber* yang berwujud *cyber attack* yaitu serangan *ransomware WannaCry* pada tahun 2017. *Wannacry* menjadi serangan *cyber* terbesar di dunia karena seratus lima puluh negara terkena dampak dari serangan ini dua diantaranya yaitu negara Inggris dan Indonesia. Dimana penyebaran serangan *ransomware* ini berbeda dengan serangan lainnya, karena mengunci sistem komputer dengan memanfaatkan senjata *cyber intel* milik negara Amerika Serikat yaitu NSA (*National Security Agency*) yang dicuri dan disebarluaskan di internet oleh hacker. Hal tersebut yang menjadikan serangan *ransomware* ini menyebar luas untuk menginfeksi ribuan sistem

komputer di negara-negara terdampak dalam waktu yang relatif singkat.

Dampak yang dialami oleh Inggris akibat serangan *ransomware* ini adalah data-data pasien di komputer rumah sakit dalam jaringan (NHS) *National Health Service* dicuri dan dikunci sehingga diperlukan tebusan untuk mendapatkan kembali data-data tersebut dalam bentuk *cryptocurrency bitcoin*. Hal ini mengakibatkan pihak (NCSC) *National Cyber Security Center* bertindak untuk memperbaiki sistem komputer yang terinfeksi dan tertundanya pelayanan medis yang pada akhirnya terpaksa dipindahkan ke rumah sakit lain yang tidak terdampak. Sama halnya dengan Inggris, beberapa rumah sakit di Indonesia terkena serangan *ransomware WannaCry* tersebut hingga puluhan unit sistem komputer yang berisi data pasien terdampak serangan ini. Pada akhirnya untuk menebus data tersebut pihak rumah sakit yang terdampak harus mengeluarkan biaya setara dengan $17 ribu dolar.

Kasus kejahatan *cyber* seperti kasus *ransomware wannacry* ini memiliki dampak yang cukup mempengaruhi suatu negara termasuk Inggris, karena sebagai negara yang selalu terhubung dengan dunia *cyber* pemerintah Inggris harus mengeluarkan biaya tinggi untuk meningkatkan perlindungan dan pertahanan keamanan *cyber* negaranya. Untuk meminimalisir kejadian serupa di masa mendatang pemerintah Inggris menginisiasi kepentingan nasionalnya melalui *National Cyber Security Strategy* untuk menjalin kerja sama secara internasional, dalam menjaga keamanan *cyber* dan menjadi negara yang aman dalam dunia *cyber* serta dapat mengamankan kepentingan Inggris baik diluar yuridiksi ataupun yang langsung berdampak pada keamanan nasional Inggris.

Pemerintah Inggris memulai kerja sama dengan pemerintah Indonesia di bidang keamanan *cyber* melalui kunjungan menteri muda Inggris urusan Asia Pasifik untuk membahas hubungan bilaterar serta penandatanganan (MoU) Memorandum of Understanding terkait cyber security kedua negara pada tahun 2018 oleh kepala BSSN yaitu Dr. Djoko Setiadi dan Menteri Muda Inggris urusan Asia Pasifik The Rt. Hon. Mark Field, MP. Melalui (MoU) kerja sama ini Inggris dapat meningkatkan kapasitas keamanan pada bidang cyber serta keuntungan untuk mencapai kepentingan nasionalnya.

Meskipun kerja sama ini disepakati pada tahun 2018 yaitu setahun setelah kasus *ransomware* tersebut terjadi namun pembahasan mengenai kerja sama ini telah dilakukan sebelumnya namun, kedua pihak tidak mempublikasikan arsip untuk menjaga kerahasiaan dan isu sensitif yang dibahas didalamnya. Dengan menduduki rangking ke lima dalam keamanan *cyber global*, Inggris dapat menjadi mitra kerja sama strategis bagi Indonesia. Ditambah dengan adanya kasus serangan *ransomware Wannacry* yang berdampak pada kedua negara tersebut menjadi latar belakang kerja sama ini, melalui kerja sama tersebut sebagai pertahanan dan pencegahan di ruang *cyber* dengan tujuan untuk mencegah kasus serupa terjadi di masa depan.

Bagi pemerintah Inggris keamanan siber merupakan salah satu prioritas dalam Strategi Nasional Inggris. Memiliki tujuan untuk menjadikan Inggris sebagai negara yang amana untuk melakukan bisnis di ruang siber. Dengan kerja sama ini Inggris melalui *Goverment Communications Headquarters* (GCHQ) dapat memberikan informasi bagaimana mengolah manajemen

keamanan siber di sektor pemerintahan. Inggris dapat memberikan panduan untuk meningkatkan kapasitas akdemik dalam bidang keamanan siber dan diharapkan dapat membantu memperkuat kolaborasi antara pemerintah, industri dan masyarakat dalam menerapkan strategi keamanan siber. Kerja sama bilateral ini diperlukan sebagai upaya pencegahan dan penanggulangan serangan siber, untuk itu diperlukannya pendekatan global untuk melindungi keamanan dan kepentingan nasionalnya.

B. Implementasi Kerjasama Keamanan Siber Inggris dengan Indonesia

Pada kegiatan tersebut penandatanganan kerja sama di bidang keamanan siber tersebut meliputi implementasi dan pengembangan strategi keamanan siber nasional, pengelolaan insiden siber, kejahatan siber, pelatihan dan kampanye kesadaran keamanan siber dan peningkatan kapasitas. Inggris dan Indonesia sepakat untuk melakukan pertukaran informasi dalam suatu penyusunan kebijakan keamanan siber nasional dan penerapannya. Dimana kolaborasi ini diharapkan dapat berkontribusi pada pembentukan standar perilaku global di bidang siber yang saat ini menjadi perhatian global.

Selama periode kerja sama MoU, diselenggarakan forum dialog siber dengan mengundang entitas siber terkait masalah yang dibahas. Forum ini berfungsi sebagai alat untuk mengatur pelaksanaan substansi kerja sama MoU. Dalam pelaksanaannya, *National Cyber Security Center* (NCSC) dan BSSN bekerja sama dalam dua program. Pertama, program pengembangan siber dan sandi negara, juga dikenal sebagai program teknis. Kedua, program generik, juga dikenal sebagai program dukungan manajemen dan pelaksanaan tugas teknis lainnya.

Dalam pengembangan kapasitas pemerintah Indonesia membuat *Computer Security Incident Response Team* (CSIRT) yang bertujuan untuk menangani Insiden serangan siber. BSSN bertanggung jawab untuk menerima, meninjau dan menghadapi laporan dan aktivitas insiden keamanan siber yang terus disempurnakan melalui bantuan dari NCSC agar terciptanya keamanan siber di Indonesia. Pembentukan CSIRT ini dilakuka dalam instansi pemerintah disetiap wilayah Indonesia. Selain itu NCSC melakukan pengembangan terhadap SDM di Indonesia yang juga menjadi salah satu prioritas BSSN, karena dengan adanya perkembangan teknologi maka kebutuhan peningkatan sumber daya manusia juga diperlukan untuk dapat memahami perkembangan teknologi tersebut.

C. Hambatan dalam Inplementasi Kerja Sama *Cybersecurity* Inggris dengan Indonesia

Dalam implementasi kerja sama ini memiliki beberapa hambatan diantaranya sejak tahun 2018 hingga tahun 2020 kerja sama ini disepakati dan berjalan namun hanya tiga dari lima program yang disepakati. Program pengelolaan manajemen insiden tidak berjalan baik dikarenakan pengelolaan manajemen tersebut masih termasuk kedalam strategi nasional Indonesia. Alasan yang menghambat berjalnnya program kerja sam tersebut diantaranya, pergantian kepemimpinan dalam BSSN yang menyebabkan perlunya penyesuaian ulang jadwal pelaksanaan kerja sama yang sebelumnya telah di tetapkan. Indonesia belum memiliki kesempatan untuk mengirimkan delegasi untuk mengikuti join exercise dalam upaya penguatan

kapasitas dibidang *cyber forensic.* Kemunculan virus covid-19 yang menjadi hambatan terbesar pad kerja sama tersebut. Perbedaan kebijakan di negara masing-masingyang mempengaruhi pemahaman dan koordinasi kedua negara menjadi suatu tantangan. Perbedaan regulasi dan sistem hukum. Perbedaan tingkat kemajuan teknologi dan keahlian dibidang keamanan siber. Keterbatasan sumber daya dan anggaran terutama dari pihak Indonesia dan lain sebagainya. Namun kerja sama ini diperpanjang per tahun 2023, dengan didorong kepentingan nasionalnya Inggris tetap melakukan kerja sama keamanan siber dengan Indonesia.

KESIMPULAN

Berdasarkan hasil penelitian, dapat disimpulkan bahwa kerja sama keamanan siber antara Inggris dengan Indonesia berdasarkan kepentingan nasional Inggris sesuai dengan klasifikasi Nuectherlein yaitu kepentingan pertahanan, kepentingan ekonomi, kepentingan tatanan negara dan kepentingan ideologi. Pada kepentingan pertahanan, Inggris melihat Indonesia sebagai mitra strategis dalam menjadi partner kerja sama keamanan *cyber* selain karena politik luar negeri Indonesia yang bebas aktif menjadikan Indonesia sebagai negara yang berperan aktif dalam menjaga keamanan terutama pada bidang *cyber*. Pada kepentingan ekonomi, suatu negara dilakukan dengan menjalin hubungan dengan negara lain untuk meningkatkan kesejahteraan nasional dari negara tersebut. pada kepentingan tatanan dunia, Inggris sebagai aktor utama melakukan kerja sama ini untuk mendapatkan keuntungan absolut diantaranya sebagai cara untuk memperkuat posisinya sebagai pemimpin *cyber security* dalam menghadapi ancaman siber dan untuk menjaga stabilitas dari aktor lainnya. Pada kepentingan ideologi, Inggris mendorong konsep *rule of law* dalam tata kelola *cyber* global, dimana hal tersebut sejalan dengan kepentingan Inggris untuk memastikan bahwa *cyber space* tetap terbuka, dan aman.

D. Kepentingan Inggris dalam Kerja Sama *Cybersecurity* dengan Indonesia

Keputusan Inggris untuk keluar dari Uni Eropa membuat Inggris harus mencari pasar yang aman pada saat terjadi turbulensi. Namun hal ini masih merupakan hal umum dan Indonesia menjadi salah satu tujuan dari exodus dana. Selain itu, Indonesia dapat menjadi gerbang untuk memperluas pengaruhnya di kawasan Asia Tenggara. Dengan diambilnya kebijakan *referendum Brexit*, Inggris juga mengambil langkah awal untuk mencapai visi *Global Britain*. Keputusan pengambilan kebijakan *referendum Brexit* membawa perubahan yang signifikan termasuk implikasi bagi negara-negara di kawasan Asia Tenggara diantaranya, Inggris lebih fleksibel dalam menjalin hubungan bilateral yang lebih mendalam dengan negara-negara di kawasan Asia Tenggara. Inggris dapat memperkuat posisinya sebagai pemimpin global dalam bidang keamanan siber.

Inggris dan Indonesia juga telah banyak melakukan kerja sama pada sektor teknologi baik pada bidang pendidikan maupun pertahanan keamanan dan kerja sama dalam mengatasi kejahatan lintas batas. Hingga saat ini posisis strategis Indonesia menjadi pertimbangan utama untuk menjadikan Indonesia sebagai mitra yang memiliki potensi sehingga kerjasama bilateral keamanan siber dibutuhkan. Serangan siber seringkali menargetkan Asia Tenggara oleh karena itu kerjasama dengan Indonesia

dapat mengurangi resiko ancaman terhadap kepentingan Inggris dikawasan tersebut. selain itu, kerjasama keamanan siber memungkinkan Inggris memperkenalkan teknologi dan solusi keamanan buatan Inggris dan mendukung perusahaan-perusahaan yang berinvestasi di sektor teknologi Indonesia.

KESIMPULAN

Pada kerja sama keamanan siber yang dilakukan oleh Inggris dengan Indonesia terlihat bahwa Inggris mengedepankan kepentingan survival dan kepentingan vital negaranya dikarenakan kondisi Inggris pasca *Brexit* dan juga pengalaman Inggris saat mengatasi permasalahan serangan *ransomware Wannacry*. Oleh karena itu Inggris lebih memilih untuk mengedepankan kepentingan nasionalnya, karena negara Indonesia tidak hanya menjadi pihak penerima karena pertukaran informasi mempermudah Inggris dalam melindungi kepentingan Inggris dikawasan tersebut, meningkatkan posisi bisnis Inggris di pasar global pada bidang siber, memperluas pengaruh Inggris di kawasan sebagai pemimpin siber, mempromosikan ruang siber yang bebas dan damai sesuai dengan ideologi Inggris. Disisi lain kerja sama ini juga memberikan keuntungan terhadap negara Indonesia yang dimana, negara Indonesia terbantu oleh pertukaran informasi, transfer teknologi serta peningkatan keamanan siber negaranya.

DAFTAR PUSTAKA

Amer Ababakr. “Understanding Neorealism Theory in Light of Kenneth Waltz’s Thoughts.” International Relations and Diplomacy 9.12 (2021).

Badan Siber dan Sandi Negara. “BSSN Luncurkan Government – Computer Security Incident Response Team (Gov-CSIRT) Indonesia,” 2019. Available: https://surl.li/hbvhkc.

———. “Tandatangani Nota Kesepahaman Kerjasama di Bidang Keamanan Siber Dengan Pemerintah Inggris Raya.” BSSN. Biro Hukum dan Humas, BSSN, 2018. Available: http://surl.li/tjqjrh.

Barry, et al., Buzan. Security - A New Framework For Analysis. Vol. 11. London: Lynne Rienner, 1998.

BBC. “Brexit: What you need to know about the UK leaving the EU - BBC News,” 2020. Available: https://www.bbc.com/news/uk-politics-32810887.

C, Chotimah Hidayat. “Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara.” JURNAL POLITICA 10.2 (2019): 113–128.

Collier, Roger. “NHS ransomware attack spreads worldwide.” PMC 189.22 (2017): 786–787. Available: https://pmc.ncbi.nlm.nih.gov/articles/PMC5461132/.

Craigen, Dan, Nadia Diakun-thibault, and Randy Purse. “Defining Cybersecurity”October (2014): 13–21.

Creswell, John. W, and J. David Creswell. Qualitative, Quantitative, and Mixed Methods Approaches. Asia-Pacific Pte. Ltd. Sage Publication, 2018.

Dhiyanka, Magrisa. “Kerja Sama Badan Siber Dan Sandi Negara (BSSN) Indonesia Dengan Department of Foreign Affairs and Trade (DFAT)

Australia Dalam Pengembangan CyberSecurity." JOM FISIP Vol. 7: Edisi II Juli-Desember 2020 7 (2020): 1–11.
Digital, Emerge. "The WannaCry attack and the NHS," 2017. Available: https://emerge.digital/resources/the-wannacry-attack-and-the-nhs/.
Dugis, Vinsensio. Teori Hubungan Internasional ; Perspektif-Perspektif Klasik. Surabaya: PT Revka Petra Media, 2016.
Etania, Rebeca Bernike, and Tri Indriawati. "Brexit Latar Belakang dan Proses Keluarnya Inggris dari Uni Eropa," 2023. Available: https://www.kompas.com/stori/read/2023/09/12/170000479/brexit--latar-belakang-dan-proses-keluarnya-inggris-dari-uni-eropa.
Fitzgerald, Oonagh E. "Brexit Deal Defeated: What's Next?," 2019. Available: https://surl.li/ontnkl.
Grieco, Joseph M. "Anarchy and the limits of cooperation: A realist critique of the newest liberal institutionalism." International Organization 42.3 (1988): 485–507.
Hadfield, Amelia, and Richard G. Whitman. "The diplomacy of 'Global Britain': settling, safeguarding and seeking status." International Politics (2023).
Hélie, Ghernaouti. Cybersecurity Guide for Developing Countries. Enlarged. Geneva ITU, 2009. Available: http://surl.li/vkajoo.
Hirdaramani, Yogesh. "The United Kingdom commits to cyber capacity building in Southeast Asia." GovInsider, 2023. Available: https://surl.li/vincfh.
HM Government. "Global Britain in a Competitive Age." GOV.UK, 2021. Available: https://surl.li/hbsxrw.
———. "National Cyber Security Strategy 2016-2021." National Cyber Security Strategy (2016). Available: http://surl.li/dqrhab.
Indonesia, Republik. "Indonesia Law No.37/1999 about Foreign Affairs." Lembaran Negara RI1 (1999): 1–11.
Jackson, Robert, and George Sorensen. Introduction to Relations International Theories and Approaches. Multi-modality Cardiac Imaging: Processing and Analysis. 5th ed. United Kingdom Oxford University Press, 2013.
Josh, Fruhlinger. "WannaCry explained: A perfect ransomware storm," 2022. Available: http://surl.li/ysichw.
Kementerian Perdagangan RI. "Tingkatkan Hubungan Dagang, Indonesia-Inggris Senggol Sektor Ekonomi Digital dan Energi Terbarukan Via JETCO," 2023.
Lewis, James A. "Cybersecurity and Critical Infrastructure Protection." Center for Strategic and International StudiesJanuary (2016): 1–23. Available: https://surl.li/jqhozz.
Macroeconomic Dasboard. "Brexit dan Kita," 2014. Available: https://surl.li/jjqjht.
Mahkamah Konstitusi RI. "Undang-undang Dasar Negara Republik Indonesia 1945," 1945. Available: https://surl.li/lsishx.
Mcmillan, Richard. The British Occupation of Indonesia 1945–1946. Taylor & Francis e-Library, 2006.
Menhan. "Inggris Berkeinginan Tingkatkan Kerjasama Pertahanan dengan Indonesia." Jakarta: Kementerian Pertahanan Republik Indonesia, 2018. Available: http://surl.li/poqpcl.

Miles, Matthew B., and A Michael Huberman. Qualitative Data Analysis. 2nd ed. SAGE Publications,Inc, 1994.
Murdiyanto Eko. Metode Penelitian Kualitatif. Vol. 5. 1st ed. Yogyakarta Press, 2020.
N., Waltz Kenneth. Theory of International Politics. Addison-Wesley, 1979.
Nassaji, Hossein. "Qualitative and descriptive research: Data type versus data analysis." Language Teaching Research 19.2 (2015): 129–132.
Nazli, Choucri. Cyberpolitics in International Relations. Cyberpolitics in International Relations, 2019.
NCSC. "National Cyber Security Centre," n.d.
Ningsih, Widya Lestari, and Nibras Nada Nailufar T. "Traktat London-Latar Belakang, Isi, dan Dampaknya," 2021. Available: http://surl.li/vpmohc.
NSA. "National Security Agency Generating foreign intelligence insights. Applying cybersecurity expertise. Securing the future.," n.d.
Nuechterlein, Donald E. "National interests and foreign policy: A conceptual framework for analysis and decision-making." British Journal of International Studies 2.3 (1976): 246–266.
Nurdiyanto, Ridwan Adi. "KERJASAMA KEAMANAN SIBER INDONESIA-INGGRIS PADA PERIODE 2018-2028." Jurnal Mahasiswa Magister Hubungan Internasional 1.1 (2024): 339–349.
Papp, Daniel S. "Contemporary International Relations: Framework for Understanding." New York: Macmillan College Pub. Co., 1994.
Peter, Reynolds. "Britain's foreign and defence policy shake-up focuses on technology." The Economist, 2021. Available: https://surl.li/jkhrrw.
Pratama, Rizky. "Kerjasama Indonesia-Inggris dalam mengatasi kejahatan siber di Indonesia tahun 2018-2020." Journal Ilmu Hubungan Internasional 8.4 (2020): 688–700.
Rizki, et al., Hapizon. "Analisis Kerjasama Cyber Security Indonesia-Australia dalam Menangani Kejahatan Siber di Indonesia." Jurnal political Science International Relation (2022).
Rosenau, James N, Kenneth W Thompson ., and Gavin T A Boyd. World politics : an introduction. NV-1 o. New York: Free Press, 1976.
Sanceau, Elaine. Good Hope: the voyage of Vasco da Gama. Academia Internacional da Cultura Portuguesa, 1967.
Sardiman, AM, and Lestariningsih Dwi Amurwani. Sejarah Indonesia. 2nd ed. Kemendikbud, 2017.
Saviar, Yulyan Maharta. "Mengapa Brexit ? Faktor-Faktor Di Balik Penarikan Inggris Dari Keanggotaan Uni Eropa" (2016): 1–14.
Schmitt, Michael N. "Tallinn Manual 2.0." Cambridge University Press, 2017., 2017.
The Health Foundation. "WannaCry Ransomware Cyberattack," 2018. Available: https://surl.li/smxaej.
TNI AD. "Kedubes Inggris Bersama Pussansiad Selenggarakan Army Cyber Commander Training Course," 2023. Available: tniad.mil.id.
Tuxworth, S. "UK ranks fifth in global cyber security rankings," 2015. Available: http://surl.li/zqaauv.
UN. "Group of Governmental Experts – UNODA." UN.org, 2019. Available: https://www.un.org/disarmament/group-of-governmental-experts/.
Usman, Bobby F. "Faktor-Faktor yang Melatarbelakangi Kerja Sama

Indonesia dengan Inggris di Bidang Keamanan Siber Tahun 2018." Moestopo Journal International Relations 1.2 (2021): 107–114.
Widiastutie, Sophiana. "Kebijakan Luar Negeri Inggris Keluar dari Keanggotaan Uni Eropa Tahun 2017" (2021): 1–17. Available: https://surl.li/dldbfy.
Yuniarti, Siti. "Cyber Operation: Tallin manual 2.0." Binus University, 2017. Available: https://surl.li/dpyzmb.
"BSSN Jalin Kerja Sama Keamanan Siber dengan Pemerintah Inggris," 2023. Available: https://surl.li/gwhamb.