# Upaya Indonesia dalam Meningkatkan Strategi Keamanan Siber melalui Kerjasama Indonesia-Inggris

Saat ini dunia sudah semakin canggih dengan segala teknologi yang menjadi bagian dari era globalisasi, terutama internet yang digunakan oleh seluruh penduduk di dunia. Hal tersebut ternyata memiliki dampak yang sangat berpengaruh bagi dunia politik internasional, bukan hanya sekedar kompetisi antara ideologi kapitalisme dan komunisme ataupun ketegangan diplomasi, tetapi lebih dari itu sehingga tidak dapat diatasi hanya dengan satu negara melainkan seluruh negara harus ikut berkontribusi (Winarno, 2014). Pemakaian teknologi yang semakin hari semakin meningkat membuat beberapa oknum yang tidak bertanggung jawab menyahlahgunakan penggunaan internet dan meninmbulkan berbagai kejahatan atau bisa disebut dengan perang siber (*cyber war*). Perang siber merupakan seluruh perbuatan yang dengan sengaja dilakukan untuk memprovokasi kedaulatan suatu negara (INDONESIA, 2014).

Perang siber mempunyai berbagai jenis yang harus diwaspadai seperti *hacking*, *cyber sabotage*, *spywar* yang dapat membahayakan keamanan internasional. Hal tersebut membuat setiap negara dituntun untuk memiliki *cyber security* sebagai alat untuk mempertahankan keamanan nasionalnya masing-masing dari bahayanya cyber crime (Yanuar, 2021). *Cyber security* harus menjadi salah satu fokus utama pemerintah untuk terus ditingkatkan sehingga pengimplementasiannya dapat berjalan secara maksimal terutama dalam segi teknologi. Berdasarkan informasi yang didapatkan dari prosiding seminar akademi angkatan udara, keamanan siber (*cyber security*) ialah tindakan yang ditujukan untuk menjaga suatu informasi atau data-data penting di jagat maya dari berbagai ancaman (Eko Budi, 2021).

Dikarenakan perang siber ini bersifat kejahatan internasional maka diharapkan negara-negara dapat melakukan kerjasama bilateral guna menanggulangi serta memberantas kejahatan siber yang setiap tahunnya semakin meningkat. Salah satu contohnya ialah kerjasama yang dilakukan Indonesia dengan pemerintahan Inggris untuk memerangi kejahatan siber. Ketergantungan yang terjadi dianatara negara Indonesia dan Inggris menjadi salah satu penyebab utama kedua negara tersebut mulai melakukan kerjasama. Diketahui bahwa Indonesia kurang unggul dalam bidang sarana dan prasarana terkait teknologi serta keahilannya untuk memerangi kejahatan siber. Sedangkan Inggris yang sudah sangat unggul dalam pertahanan juga teknologinya mempunyai cita-cita nasional untuk melindungi keamanan nasional dari segala aspek (Weu, 2020).

Pergeseran isu keamanan internasional telah berkembang menuju isu non-tradisional dengan melibatkan manusia sebagai prioritas keamanan utama suatu negara (Krauthammer, 1990). Keberadaan internet sebagai teknologi informasi dan komunikasi selain membawa banyak kemudahan dalam kehidupan, di sisi lain juga menghadirkan faktor ancaman baru berupa munculnya perang siber yang berdampak vital bagi keamanan dan kedaulatan suatu negara, tak terkecuali Indonesia. Ketergantungan yang tumbuh pada jaringan digital telah secara radikal mengubah berapa banyak aspek kehidupan masyarakat yang beroperasi. Transisi ke pekerjaan jarak jauh yang disebabkan oleh COVID-19 telah mempercepat penggunaan platform dan perangkat yang memungkinkan data sensitif dibagikan dengan pihak ketiga, seperti penyedia layanan cloud, agregator data, antarmuka pemrograman aplikasi (API), dan teknologi internet lainnya. Mewajarnya teknologi tingkat tinggi berbasis internet seperti kecerdasan buatan (AI), *blockchain*, 5G, dan *Internet of Things* (IoT) telah membawa peluang kemudahan bagi masyarakat maupun bisnis untuk meningkatkan produktifitas, kualitas, dan efisiensi, namun hal tersebut juga menimbulkan peningkatan jenis ancaman siber yang lebih berbahaya. (World Economic Forum, 2022).

Serangan dunia maya (*cyberattack*) mengancam keamanan nasional dan internasional secara serius. Serangan siber memiliki banyak bentuk, seperti, pencurian dan penyalahgunaan data dan identitas, penyebaran virus dan malware, peretasan website dan akun, penipuan jual-beli, dan kejahatan teroris dalam menyebarkan radikalisme. Kejahatan siber memiliki peluang lebih banyak terjadi dibanding kejahatan konvensional, karena keberadaannya tidak memerlukan pasukan militer, dan tidak terhalang faktor geografis yang memungkinkan jangkauan serangan yang dapat melintasi batas negara. Dengan meningkatnya intensitas ancaman siber seiring berkembangnya teknologi, upaya dilakukan banyak negara-negara di dunia dengan membuat kekuatan khusus angkatan siber untuk menjaga keamanan negaranya. Menyadari hal tersebut, pada 23 Oktober 2012 Menteri Pertahanan membentuk Tim Kerja Pertahanan Dunia Maya yang bertugas merumuskan strategi dan organisasi untuk menghadapi serangan siber. Hingga saat ini, tercatat pada tahun 2021 sendiri di Indonesia terdapat lebih dari 1,6 miliar serangan cyber dengan 44% serangannya berupa malware MytoBot yang menyerang komputer dengan sistem operasi Windows. (BSSN, 2022).

Upaya Indonesia dalam mengatasi ancaman siber selain menerapkan UU ITE, juga tidak terlepas dari kerjasama bilateral dengan negara-negara lain salah satunya Inggris, untuk mencapai kepentingan mutualisme dengan saling memberi bantuan dan informasi, pemantapan pemahaman keamanan siber, dan juga peningkatan sumber daya manusia. Kerjasama antara Indonesia dan Inggris pada sektor keamanan siber mulai dilaksanakan pada 14 Agustus 2018 dengan ditandatanganinya MoU keamanan siber oleh kedua belah pihak. Melalui kerjasama ini, ke dua negara baik Indonesia maupun Inggris mempunyai kepentingan nasionalnya sendiri yang akan dipenuhi melalui kerjasama keamanan siber. Pemerintah Indonesia dapat menata kembali strategi keamanan sibernya dan secara efektif menguatkan sektor lembaga pemerintah, akademisi, dan industri dalam mewujudkan strategi keamanan siber nasional yang kondusif. Adapun kepentingan Inggris menurut Menteri Muda Inggris untuk Asia Pasifik, Mark Field, kerjasama ini selain untuk

menguatkan hubungan antar kedua negara, juga sebagai sarana mempromosikan Inggris sebagai negara yang aman untuk berinvestasi secara digital, dan menjaga keamanan sektor ekonomi Indonesia-Inggris dari kejahatan siber.

Kerjasama ini menguntungkan bagi Indonesia dari bidang pemantapan pemahaman keamanan siber, karena Inggris memiliki keunggulan pada akademik, sumber daya manusia, dan teknologi, menawarkan program akademik dan keterampilan terkait keamanan siber untuk meningkatkan kualitas, pemahaman, dan kemampuan akademisi dan instansi keamanan siber di Indonesia. Kerjasama ini juga berperan pada sektor pemerintahan dan BSSN (Badan Siber dan Sandi Negara) dalam mengelola keamanan siber secara efektif dengan melakukan kooperasi bersama instansi pemerintahan yang lain. Dan terhadap infrastruktur vital nasional yang berbasis internet seperti sektor pertahanan, keuangan, kesehatan, dan pemerintahan, Indonesia dapat menguatkan kemampuannya dalam melindungi dan mengamankan infrastruktur rentan tersebut dari serangan siber. Dalam meningkatkan kemampuan sumber daya manusia, pemerintah Indonesia membentuk *Computer Security Incident Response* Team (CSIRT) pada 20 Desember 2018 dibantu oleh Inggris melalui *National Cyber Security Center* (NCSC), bertujuan untuk mendeteksi dan mengatasi insiden serangan siber dalam rangka menciptakan keamanan siber di Indonesia. Laporan insiden keamanan siber tersebut kemudian diterima, ditinjau, dan ditanggapi oleh BSSN.

Kerjasama ini memberikan kemajuan bagi Indonesia ditunjukkan dari peningkatan Global Cybersecurity Index (GCI) tahun 2021 yang dipublis oleh *International Telecommunication Union* (ITU) yang terus meningkat. Pada tahun 2018 Indonesia berada di peringkat 41 dari 194 negara, dan meningkat menjadi peringkat 24 pada tahun 2020. (ITU, 2021). Hal tersebut menunjukkan kemampuan dan kebijakan Indonesia, dan kesiapan sumber daya manusianya dalam mengatasi ancaman dan kejahatan siber mengalami perkembangan pesat.

Internet membawa pengaruh terhadap perubahan dunia ini, internet sebagai teknologi informasi dan komunikasi serta membawa banyak kemudahan dalam kehidupan kita sehari-hari. Namun pengaruh buruk yang ditimbulkan adalah perang siber, perang siber merupakan ancaman baru bagi keamanan dan kedaulatan suatu negara. Luasnya dunia maya serta tidak terhalang oleh faktor geografis menjadikan serangan siber melintas tanpa batas. Keresahan akibat serangan siber yang di alami setiap negara menyadarkan untuk menjaga keamanan negaranya oleh karena itu pada 23 Oktober 2012 Menteri Pertahanan membentuk Tim Kerja Pertahanan Dunia Maya. Pada 14 Agustus 2018 Indonesia bekerjasama dengan Inggris dalam sektor keamanan siber, tidak hanya untuk mempererat hubungan tetapi juga sebagai ajak promosi Inggris untuk mempromosikan bahwa Inggris negara yang aman untuk berinvestasi secara digital serta menjaga keamanan sektor ekonomi Indonesia-Inggris dari kejahatan siber. Kerja sama yang telah Indonesia dan inggris jalankan membawa kemajuan terutama untuk Indonesia dari peningkatan Global Cybersecurity Index (GCI) yang membuktikan bahwa Indonesia siap menghadapi serta mengatasi ancaman kejahatan siber.

## Referensi


BSSN, D. O. (2022). *Laporan Tahunan Monitoring Keamanan Siber 2021.* Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center.

Eko Budi, D. W. (2021). Strategi Penguatan Cyber Security. *Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia Akademi Angkatan Udara*.

INDONESIA, K. P. (2014). *pedoman pertahanan siber.* Jakarta.

ITU. (2021). *Global Cybersecurity Index 2020.* ITU Publications.

Krauthammer, C. (1990). The Unipolar Moment. *Foreign Affairs*, 23-33.

Weu, M. R. (2020). Kerjasama Pemerintah Indonesia Dan Pemerintah Kerajaan Inggris. *Global Political Studies Journal*.

Winarno, B. (2014). *Dinamika Isu-Isu Global Kontemporer.* Yogyakarta.

World Economic Forum. (2022). *The Global Risk Report 17th Edition.* World Economic Forum.

Yanuar, A. P. (2021). Cyber War : Ancaman Baru Keamanan Nasional dan Internasional.