POLITEIA: Jurnal Ilmu Politik
Politeia, 14 (1) (2022): 54-62
ISSN 0216-9290 (Print), ISSN 2549-175X (Online)
Available online https://talenta.usu.ac.id/politeia

Perkembangan Sistem Pertahanan/Keamanan Siber Indonesia dalam Menghadapi Tantangan Perkembangan Teknologi dan Informasi

Makbull Rizki*

Program Pascasarjana Departemen Ilmu Politik, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Padjadjaran, Bandung, Indonesia, 45363

Submitted : 11 Juni 2021 Revision : 18 Desember 2021 Accepted : 10 Januari 2022

Abstrak

Tantangan dunia pertahanan dan keamanan selalu bersifat dinamis, selalu mengalami perubahan baik bentuk, sifat, maupun sumber dari ancaman itu sendiri. Pada era sebelumnya tantangan pertahanan keamanan masih berupa penyerangan langsung dengan peralatan perang dan melibatkan kontak fisik yang lebih intens, sementara di era teknologi dan informasi yang berkembang cepat tantangan keamanan dan pertahanan memunculkan satu dimensi baru yaitu keamanan siber. Artikel ini akan menggambarkan bagaimana ancaman dan serangan siber itu menjadi tantangan bagi dunia pertahanan di era sekarang dan bagaimana perkembangan sistem pertahanan dan keamanan siber yang dimiliki oleh Indonesia saat ini

Kata Kunci: Pertahanan, Keamanan, Teknologi dan Informasi, Siber.

Abstract

The challenges in the world of defense and security are always dynamic, always changing in form, nature, and source of the threat itself. In the previous era, the challenges of defense and security were form by direct attacks with war equipment and involving more intense physical contact, while in the era of technology and information which is developing rapidly, security and defense challenges have created a new dimension, namely cyber security. This article will describe how cyber threats and attacks are a challenge for the world of defense in this current era, and how is the development of Indonesia's current cyber defense and security system.

***Keyword**: Defence, Security, technology and information, Cyber.*

How to Cite: **Rizki, M. (2021).** Perkembangan Sistem Pertahanan/ Keamanan Siber Indonesia dalam Menghadapi Tantangan Perkembangan Teknologi dan Informasi. *Politeia : Jurnal Ilmu Politik*, 14 (1): 54-62.

*Corresponding author:
E-mail: rizkimaqbul@gmail.com

PENDAHULUAN

Perkembangan teknologi dan informasi adalah sebuah peluang sekaligus tantangan yang melahirkan perubahan dalam segala aspek kehidupan mulai dari ruang lingkup terkecil yaitu individu, sampai pada ruang yang begitu luas yaitu negara bahkan dunia.

Pesatnya kemajuan di bidang teknologi dan informasi juga telah memberikan pengaruh besar terhadap seluruh komponen kehidupan, mulai dari ekonomi, politik, sosial serta keamanan.

Sifat alamiah dari ancaman dan keamanan adalah dinamis, terbukti bahwa ancaman dan keamanan bukanlah hal yang dapat selesai untuk diperbincangkan, di diskusikan dan berhenti untuk diperbaharui.

Pada abad ke-21, ancaman yang sering terjadi adalah ancaman yang bersifat tidak terlihat *(intangible),* minsal-nya ancaman ideologi berupa terorisme dan radikalisme yang berpengaruh pada keamanan nasional khususnya di Indonesia. Perubahan bentuk, sifat dan model dari ancaman tersebut yang kemudian menjadi pemicu bagi setiap negara untuk terus melakukan evaluasi dan pengembangan sistem dan alternatif cara untuk menangkal ancaman tersebut.

Perkembangan teknologi dan informasi di era sekarang ini telah membentuk ruang kehidupan baru untuk manusia saling berinteraksi, ruang tersebut disebut dengan *cyber space.* Secara singkat *cyber space* merupakan sebuah tempat maya dimana komunikasi antar pengguna terjadi.

Kemunculan dan meningkatnya penggunaan *cyber space* ini menghadirkan kemudahan bagi para penggunanya untuk berhubungan dengan orang lain, namun hal tersebut juga bersamaan dengan dampak negatif yang berupa ancaman keamanan dari dan untuk individu, organisasi dan pemerintahan.[1]

Berdasarkan data dari Kementerian Komunikasi dan Informasi (Kominfo) republik Indonesia. Terdapat sekitar 82 juta penduduk Indonesia yang berada di ruang internet dan aktif menggunakan internet. Dan hal tersebut membuat Indonesia berada di peringkat ke delapan sebagai negara dengan pengguna internet aktif terbanyak di dunia.

Tingginya angka pengguna aktif internet seharusnya juga dibarengi dengan tingkat keamanan siber yang terjamin, sehingga lalu lintas informasi dan aktivitas masyarakat maupun pemerintahan Indonesia dalam dunia internet tersebut dapat terjamin keamanan dan kerahasiaannya.

Sementara kondisi di Indonesia masih dalam keamanan siber yang rendah dan lemah, hal tersebut yang mendorong terjadi banyak peretasan data pribadi individu, seperti alamat, identitas sampai kartu debit nasabah bank, selain daripada menyasar data individu, kelemehan keamanan siber Indonesia juga turut diwarnai dengan kasus-kasus spionase, intelehen, hacking dan lain-lain.

Kasus kasus seperti peretasan, spionase dan kebocoran informasi, merupakan pertanda bagi ketidaksiapan keamanan Indonesia

[1] M. Smith (205). Research Handbook on Internasional Law and Cyberspace. Massachusetts: Elgar Publishing Limited.

dalam menghadapi ancaman keamanan era baru yaitu ancaman siber.

Berdasarkan hasil riset sebelumnya yang dilakukan oleh lembaga perusahaan dalam bidang internet dan cyber space, Akamai technologies. Pada tahun 2013 lalu Indonesia menjadi negara paling berpotensi menjadi target *hacker.* Pada tahun tersebut juga kejahatan internet di Indonesia meningkat dua kali lipat.[2]

Data lain menunjukan bahwa perkiraan kerugian akibat kejahatan siber yang terjadi di Indonesia mencapai angka USD 895 Milyar, angka tersebut adalah 1,20% dari total kerugian akibat kejahatan siber di dunia. Merujuk pada data *United Nations Institute for Disarmament research* (UNIDIR). Pada tahun 2021 terjadi pelonjakan peningkatan jumlah negara anggota PBB yang telah memiliki sistem pertahanan dan keamanan siber yang secara umum dikenal dengan istilah *cyber security programs.* Jumlah negara yang telah memiliki sistem tersebut meningkat dari 68 negara pada tahun 2011 menjadi 114 negara di tahun 2012 dari total 193 negara anggota PBB.

Terkait dengan hal tersebut, dunia keamanan dan pertahanan juga telah melahirkan suatu persepektif baru, jika sebelumnya negara ditempatkan sebagai unsur terpenting untuk dilindungi, maka persepktif baru yang muncul menempatkan manusia sebgai unsur paling penting. Persfektif tersebut dikenal dengan nama *"human security".*

Perisitiwa-peristiwa penyerangan lewat media internet terhadap lembaga-lembaga pemerintahan di berbagai negara termasuk di Indonesia menunjukan bahwa ancaman dan bentuk perang yang terjadi antar negara saat ini berbeda bentuk dari perang generasi sebelumnya. Perang yang bersifat konvensional melibatkan kontak fisik tidak terlalu dominan, namun telah berganti kepada ancaman dan perang dalam dunia teknologi dan informasi.[3]

Sudah seharusnya negara memberikan perlindungan dan keamanan bagi seluruh masyarakatnya terkhusus dalam ruang siber. Negara dalam hal ini harus bekerja untuk menangkal seluruh ancaman terhadap negara, baik ancaman terhadap individu warga negara, perusahaan negara, lembaga pemerintahan, dan keutuhan seluruh wilayah negara Indonesia.

Berdasarkan permasalahan-permasalahan di atas, maka artikel ini akan mencoba memberikan penjelasan terkait sistem pertahanan siber yang dimiliki oleh Indonesia serta bagaimana perkembangan sistem pertahanan Indonesia saat ini.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan penelitian kualitatif dengan metode studi kasus. Penelitian ini menggunakan sumber data sekunder. Data yang diperoleh melalui hasil studi literasi atau studi kepustakaan. Sumber

[2] Akamai (2013). The State of The Internet Report. Dalam, Adi Rio Arianto dan Gesti (2019). Membangun Pertahanan Keamanan Siber Nasional, dst. Jurnal Pertahanan dan Bela Negara. Vol. 9 (1).

[3] David Putra Setyawan dan Arwin Datumaya, (2016). Diplomasi Pertahanan Indonesia dalam Pencapaian Cybersecurity melalui ASEAN Regional Forum on Cybersecurity Initiatives, Jurnal Penelitian Politik, Vol. 13 (1).

data adalah buku maupun jurnal yang melalui proses penelitian dengan topik penelitian yang serupa dengan penelitian ini.

HASIL DAN PEMBAHASAN

Ancaman dan Serangan Siber

Ancaman Siber

Ancaman siber adalah potensi kemunculan pelanggaran keamanan, izin, hukum ataupun aturan, yang dilakukan oleh oknum yang tidak memiliki hak atas informasi atau akses pada teknologi milik negara dengan tujuan materil maupun immateril.

Ancaman siber dapat difahami berdasarkan pada empat kategori ancaman siber yaitu: sumber ancaman, jenis ancaman, bentuk ancaman dan aspek ancaman.[4]

Sumber ancaman dapat berupa aktor yang mewakili pemerintah *(State Actor)* atau non pemerintah *(non-state actor),* sehingga pelaku bisa bersifat perorangan, kelompok, golongan, organisasi atau bahkan sebuah negara.

Jenis ancaman terdiri dari tiga kelompok diantaranya yaitu, Ancaman perangkat keras *(hardware threat),* Ancaman Perangkat Lunak *(software threat),* dan Ancaman Data/informasi *(data/information threat).*

Adapun bentuk-bentuk ancaman siber yang dapat terjadi terhadap negara diantaranya adalah serangan terhadap website lembaga negara atau pemerintahan dengan berbagai pola cara seperti, defacement, phising, malware, *Advance Persistent Threats (APT).* Kemudian ada bentuk ancaman siber berupa penyusupan, spam dan Penyalahgunaan protokol komunikasi.

Sementara aspek ancaman merupakan semua hal terkait yang melatarbelakangi terjadinya ancaman dan serangan siber, yang termasuk di dalamnya aspek-aspek politik, ideologi, ekonomi, budaya, sosial, militer, teknologi serta aspek lain yang berhubungan dengan kehidupan berbangsa dan bernegara termasuk kepentingan individual.

Serangan Siber (cyber attack)

Serangan Siber (CyberAttack) terjadi ketika intensitas dan skala ancaman siber meningkat dan berubah dari ancaman yang bersifat potensial menjadi factual seperti tindakan yang bertujuan untuk memasuki, menguasai, mengubah, mencuri, menghilangkan, menghancurkan, dan melumpuhkan sistem atau aset informasi.

Serangan siber terdiri dari perang siber dan gangguan siber. Perang siber adalah semua tindakan yang dilakukan secara sengaja dan terkoordinir untuk menggangu kedaulatan negara, sedangkan gangguan siber adalah tindakan yang dilakukan dengan tidak disengaja, kegiatan bersifat pasif dan dalam skala kegiatan, ancaman dan gangguan kecil.

Pertahanan/Keamanan Siber

Keamanan atau pertahanan siber adalah sebagian bagian dari cara-cara atau mekanisme yang dilaksanakan dan digunakan untuk melindungi dan meminimalisir gangguan terhadap kerahasiaan data, integritas, serta ketersediaan informasi.

[4] Kementerian Pertahanan Republik Indonesia (2014). Pedoman Pertahan Siber. Jakarta: Indonesia.

Negara-negara yang telah melakukan pembaharuan di bidang pertahanan dan keamanan, telah banyak melakukan gerakan-gerakan pembangunan kapasitas pertahanan keamanan siber masing-masing, mulai dari langkah-langkah dasar seperti merancang dan mengesahkan peraturan atau undang-undang tentang cybercrime, meningkatkan sumber daya manusia bidang teknologi dan informasi, meningkatkan kemampuan penegakan hukum sampai pada membentuk tim khusus tanggap darurat khusus yang biasa disebut *Computer Emergency Response Team (CERT).*

Lebih dari badan tanggap darurat, beberapa negara telah membentuk lembaga negara atau organisasi yang secara khusus bekerja dalam membidangi pertahanan siber atau keamanan siber di negaranya masing-masing.

Salah satu contoh negara yang sejak lama telah memberikan perhatian khusus terhadap masalah keamanan dan pertahanan siber ini adalah brunei Darussalam, yang pada tahun 2004 membentuk lembaga bernama *Brunei Computer Emergency Response Team (BruCERT)* dibawah *Information Technology Protective Security Services (ITPSS),* sebuah perusahaan yang bekerja sama dengan Kementrian Komunikasi Pemerintah Brunei Darussalam yang khusus menangani masalah ancaman dan serangan siber.

Mekanisme pertahanan dan keamanan siber sendiri memiliki elemen-elemen pokok yang menjadi karakteristik negara yang memiliki *cyber security* yang baik, diantara elemen-elemen tersebut adalah:

1. *Dokumen security policy,* Sebuah dokumen yang berisi aturan sebagai standar dan panduan dalam menjalankan proses pengamanan informasi.
2. *Information infrastructure,* merupakan wadah atau media yang berperan sebagai penyebar informasi seperti perangkat keras dan perangkat lunak.
3. *Perimeter defense* sebagai media yang menjadi komponen pertahanan pada information infrastructure.
4. *Network Monitoring System* ialah media yang berperan untuk melakukan pengawasan kelayakan, utilisasi serta performance infrastruktur informasi.
5. System Information and Event Management ialah media yang berperan dalam melakukan pengawasan terhadap berbagai macam kejadian pada jaringan.
6. *Network Security Assesment* merupakan elemen dari *cyber security* yang memiliki peran dalam melakukan mekanisme control dan memberikan measurement level keamanan informasi.
7. *Human resource dan security awareness* yang berkaitan dengan sumber daya manusia serta kewaspadaannya terhadap keamanan informasi.[5]

[5] I Wayan Midhio, Reksoprodjo dan Zaelani (2018). Pembangunan Kapasitas *Cyber security* Di Negara Asean: Analisis Komparatif Terhadap Brunei Dan Indonesia. Jurnal Prodi Perang Asimetris. Vol 4 (2).

Pertahanan/Keamanan Siber Indonesia

Merujuk pada bagian awal artikel ini, bahwa keamanan pertahanan siber dibentuk atas lima bidang kerja, yaitu kepastian hukum, tindakan procedural, struktur organisasi, capacity building dan kerjasama internasional.

Jika membedah satu persatu aspek tersebut maka Indonesia dapat dikatakan masih sebagai negara yang berproses dalam pembentukan dan penguatan sistem keamanan dan pertahanan siber sampai saat ini.

Dalam aspek kepastian hukum, Indonesia telah beberapa kali merancang dan melakukan perubahan terhadap aturan yang mengatur tentang bidang keamanan dan pertahanan siber republic Indonesia.

Catatan dokumen menyebutkan bahwa kebijakan *cyber security* Indonesia mulai telihat saat pengesahan aturan hukum dalam Peraturan Menteri Komunikasi dan Informatik No. 26 / PER / M.Kominfo /5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet.

Aturan lainya tentang *cyber security* Indonesia tertuang dalam pedoman pertahanan siber yang dikeluarkan oleh kementerian pertahanan Indonesia pada tahun 2014 yaitu peraturan menteri pertahanan republik Indonesia Nomor 82 Tahun 2014.

Aturan lainya berkaitan dengan pendirian lembaga negara khusus yang mengatur dan mengurusi masalah siber di Indonesia yang diberi nama Badan Siber dan Sandi Negara (BSSN) lewat peraturan Presiden Nomor 53 Tahun 2017.

Aspek Lainya yaitu struktur organisasi, pemerintahan Indonesia membentuk lembaga negara khusus sandi siber BSSN seperti yang disebutkan pada bagian sebelumnya, pembentukan lembaga tersebut dapat diidentifikasi menjadi bentuk keseriusan pemerintah dalam membentengi negara dari ancaman siber dari aktor dalam maupun luar negara.

Badan Siber dan Sandi Negara (BSSN) sendiri merupakan alat pemerintahan yang didirikan atas dasar tumpeng tindihnya kewenangan, tugas dan fungsi dari beberapa lembaga yang membidangi masalah siber sebelumnya seperti Kementerian Komunikasi dan Informasi (Kominfo), Badan Intelegen Negara (BIN), Kementerian Pertahanan (Kemhan), Polri dan institusi lainya.

Pada aspek tindakan procedural dalam hal pertahanan atau keamanan siber Indonesia masih semerawut dan saling tumpeng tindih lembaga, khususnya pada bagian keamanan, sering kali badan siber dan sandi negara tidak lebih eksis dari lembaga Polri atau TNI dalam hal siber.

Aspek lainya pada bagian capacity building Indonesia terlihat mulai memberikan perhatian khusus terhadap penanganan masalah siber di Indonesia, seperti penggagasan aturan undang-undang ITE sebagai upaya pencegahan perbuatan yang dapat membahayakan persatuan dan keamanan dan pertahanan negara.

Dalam dunia pendidikan pemerintah juga telak memasukan pendidikan teknologi terhadap pelajar Indonesia, dengan tujuan melek teknologi dan memiliki kesadaraan

untuk memanfaatkan teknologi dengan baik dan benar.

Aspek terakhir yang dapat dilihat dalam pembangunan kapasitas *cyber security* adalah aspek kerjasama internasional. Dalam aspek ini Indonesia memiliki beberapa kerjasama internasional dalam hal keamanan siber diantaranya seperti kerjasama antara pemerintahan Indonesia dan Australia (Indonesia-Australia Cyber Copperation), ikut dalam Asean Regional Forum (ARF). Menurut Zaenali Hamzah (2019). Indonesia mengikuti empat forum kerjasama internasional terkait *cyber security*.

Indonesia Saat Ini

Data serangan siber indonesia periode waktu 1 januari sampai 12 April 2020.

Periode/bulan	Jumlah Serangan
Januari	25,224,811
Februari	29,188,645
Maret	26,423,989

Data Diolah dari laporan Pusat Operasi Keamanan Siber Nasional Indonesia.

Berdasarkan data tersebut dapat diketahui bahwa indonesia merupakan salah satu negara yang mengalami ancaman serangan siber yang cukup tinggi. Ancaman siber yang diterima memiliki bermacam-macam pola mulai dari peretasan website sampai pada penyebaran berita bohong.

Perlu adanya penangkalan dan sistem pendeteksian diri bagi ancaman serangan siber yang lebih baik dari pihak berwajib yaitu pemerintah indonesia melalui lembaga-lembaga terkait.

Serangan siber akan memberikan dampak yang buruk bagi keberlangsungan negara, karena dapat menciptakan instabilitas politik di masyarakat, yang biasanya melalui penyebaran hoax, maupun terganggu nya pelaksanaan agenda negara melalui peretasan website.

Sebagai saran dan rekomendasi dari penulis artikel ini, maka ada beberapa hal yang harus dan dapat dilakukan oleh pemerintah indonesia, diantaranya adalah:

Menciptakan dan mengembangkan infrastruktur digital milik negara, hal tersebut dapat mengurangi resiko pemanfaatan data pengguna dalam hal ini adalah masyarakat indonesia oleh oknum-oknum yang dapat membahayakan keselamatan dan kerahasiaan data.

Selanjutnya pihak terkait dapat melakukan peningkatan kafasitas personil dalam bidang pemetaan dan prediksi ancaman, dengan harapan badan keamanan siber memiliki kemampuan pemetaan dan pencegahan sedini mungkin terhadap upaya serangan siber dari pihak manapun,

Ketiga, pemerintah indonesia harus membentuk sistem pertahanan keamanan yang lebih mandiri, baik dalam hal pengadaan alat keamanan maupun bidang teknologi informasi, dan tetap terlibat dalam kerjasama internasional dalam bidang keamanan.

Terakhir adalah membuat rencana strategi nasional yang tepat dalam bidang keamanan siber dan pertahanan siber.

SIMPULAN

Pembangunan dan penguatan sistem keamanan siber di Indonesia

sudah merupakan suatu keharusan yang dilakukan oleh pemerintahan Republik Indonesia. Hal tersebut karena berkaitan langsung dengan keamanan, stabilitas dan persatuan negara Indonesia.

Serangan siber secara nyata telah memberikan dampak yang besar bagi negara terserang, terkhusus Indonesia, berdasarkan data yang ada telah menjadi negara dengan urutan tertinggi menjadi sasaran penyerangan siber oleh para hacktivist. Total kerugian yang sangat besar patut menjadi sebuah bahan evaluasi bagi bidang keamanan dan pertahanan terkhsusus pada bagian *cyberspace.*

Perlu adanya aturan hukum yang lebih tegas dan jelas tentang sistem pertahanan dan keamanan siber republic Indonesia yang membagi garis kerja yang jelas antara banyaknya lembaga negara yang bertugas menjaga keamanan dan pertahanan negara kesatuan republik Indonesia seperti antara BSSN, TNI, POLRI, PUS HAN SIBER KEMHAN RI, Kominfo, serta lain-lain.

Pengembangan sistem pertahanan siber Indonesia perlu melakukan perluasan pemahaman tentang penggunaan teknologi dan informasi kepada masyarakat, sehingga konflik-konflik horizontal yang akhir-akhir ini terjadi di masyarakat karena kesalahan penyebaran informasi dan banyaknya penyebaran informasi bohong yang dengan mudah dipublikasi-kan oleh pihak yang tidak bertanggung jawab.

Selain itu upaya-upaya kerjasama antar banyak negara lewat forum, maupun antara Indonesia dengan negara lain dalam hal pertahanan dan keamanan siber harus terus dilakukan dan diperbanyak dengan harapan bahwa kerjasama tersebut akan melahirkan keuntungan bagi pihak-pihak yang ikut bekerjasama.

DAFTAR PUSTAKA

Arianto A., Anggraini G, (2019). Building Indonesia's National Cyber Defense and Security To Face The Global Cyber Threats Through Indonesia Security Incident Response Team On Internet Infrastructure (ID-SIRTII). Jurnal Pertahanan dan Bela Negara. Vol.9 (1)

Badan Siber dan Sandi Negara (2020). Rekapitulasi Insiden Web Defacement, Januari-April 2020.

Ardiyanti, Handrini. (2014). *Cyber security* dan Tantangan Pengembangannya di Indonesia. Jurnal.dpr.go.id

Center for Strategic and International Studies. (2013). The Cyber Index: International Security Trends and Realities. UNIDIR

Kementerian Pertahanan Republik Indonesia (2014). Pedoman Pertahan Siber. Jakarta: Indonesia.

M. Smith (2015). Research Handbook on Internasional Law and Cyberspace. Massachusetts: Edwar Elgar Publishing Limited.

Raden dan Efriza (2017). Bela Negara Sebagai Metode Pencegahan Ancaman Radikalisme di Indonesia. Jurnal Pertahanan dan Bela Negara. No. 3 (7).

Setyawan David dan Datumaya A. (2016). Diplomasi Pertahanan Indonesia dalam Pencapaian Cybersecurity melalui ASEAN Regional Forum on Cybersecurity Initiatives, Jurnal Penelitian Politik, Vol. 13 (1).

Wayan Midhio, Reksoprodjo dan Zaelani (2018). Pembangunan Kapasitas *Cyber security* di Negara Asean: Analisis Komparatif Terhadap Brunei Dan Indonesia. Jurnal Prodi Perang Asimetris. Vol 4 (2).