Profesionalisme TNI di Era Keamanan dan Pertahanan Siber Indonesia

Andrea Angeline; Daniel Steve; Gisella Christina; Leony Monica*.

**Bachelor students of Interior Design, Pradita University,
leony.monica@student.pradita.ac.id**

ABSTRACT: Cyber security is increasingly becoming an urgent issue in this digital era. With advances in information technology and a growing reliance on information systems, cyber security has become a top priority for organizations, governments and individuals. This research is used to understand the challenges faced in maintaining cyber security and to analyze the approaches used to protect information systems that are developing rapidly and have an impact on all aspects of life. One of them is the security aspect in the form of cyber crime threats. Therefore cyber security has a vital role to prevent cyber crime. Cyber security strategy in Indonesia and strengthening cyber security in Indonesia in order to realize national security in this era. Various challenges in cybersecurity were identified, including malware attacks, phishing attacks, DDoS (Distributed Denial of Service) attacks, and hacking attacks. The human factor is also a significant risk factor in cybersecurity, such as lack of awareness of good security practices and reluctance to adopt appropriate security measures.

KEYWORDS: Cyber security, Digital era, Information technology progress, Indonesian Society.

ABSTRAK: Keamanan siber menjadi isu yang semakin mendesak dalam era digital ini. Dengan kemajuan teknologi informasi dan ketergantungan yang semakin besar terhadap sistem informasi, keamanan siber telah menjadi prioritas utama bagi organisasi, pemerintah, dan individu. Penelitian ini digunakan untuk memahami tantangan yang dihadapi dalam menjaga keamanan siber dan menganalisis pendekatan yang digunakan untuk melindungi sistem informasi yang sangat berkembang dengan pesat memiliki dampak terhadap seluruh aspek kehidupan. Salah satunya adalah aspek keamanan berupa ancaman cyber crime. Oleh karena itu cyber security mempunyai peran vital untuk mencegah terjadinya cyber crime. Strategi cyber security di Indonesia serta penguatan cyber security di Indonesia dalam rangka mewujudkan keamanan nasional di era ini. Berbagai tantangan dalam keamanan siber diidentifikasi, termasuk serangan malware, serangan phishing, serangan DDoS (Distributed Denial of Service), dan serangan peretasan. Faktor manusia juga menjadi faktor risiko yang signifikan dalam keamanan siber, seperti kurangnya kesadaran akan praktik keamanan yang baik dan keengganan untuk mengadopsi tindakan keamanan yang tepat.

KATA KUNCI: Keamanan siber, Era digital, Kemajuan teknologi informasi, Masyarakat Indonesia.

I. PENDAHULUAN

Keamanan siber telah menjadi isu prioritas bagi semua negara di dunia, karena teknologi informasi dan komunikasi digunakan dalam banyak bidang kehidupan antara lain sosial, ekonomi, hukum, organisasi, kesehatan, pendidikan, budaya, pemerintahan, keamanan, pertahanan, dll. . dalam waktu dekat. Pada. Berbanding lurus dengan tingginya tingkat penggunaan teknologi informasi dan komunikasi, risiko dan ancaman penyalahgunaan teknologi informasi dan komunikasi juga semakin meningkat dan semakin kompleks. Pesatnya perkembangan teknologi informasi saat ini mempengaruhi kehidupan manusia dan hubungan antar negara di dunia. Selain itu, seiring kemajuan teknologi, keberadaan batas-batas negara, yang sebelumnya diamati dan diikuti sebagai konsensus internasional, kini menjadi nyata.

Perang dunia maya merupakan ancaman nyata jika tidak diantisipasi dengan baik. Perang dunia maya, penggunaan jaringan komputer atau internet untuk bersaing satu sama lain, mengontrol komunikasi, mengganggu, mencegat bahkan mengubah informasi dan tindakan yang ditujukan untuk merugikan dan menghancurkan musuh. Hal ini menyebabkan serangan dunia maya yang merugikan tidak hanya individu dalam masyarakat tetapi juga negara. Serangan dunia maya dilakukan di masyarakat untuk mendapatkan informasi pribadi secara ilegal, meretas akun, menyebarkan virus, menguping, bahkan mencemarkan nama baik. Kegiatan ini jelas merugikan masyarakat karena melanggar hak privasi dan mengakibatkan kemungkinan hilangnya kepemilikan informasi pribadi yang dicuri.

Pada saat yang sama, serangan dunia maya berdampak pada negara membongkar strategi keamanan dan pertahanan negara. Lingkungan strategis abad ke-21 merupakan bagian dari zaman horizontal (horizontalization) atau “garis global” di mana keamanan informasi (information: fisik dan elektronik) sangat sulit dikendalikan, mempengaruhi keamanan dunia maya dan nuklir. Dalam Kajian Keamanan Internasional, Adi Rio Arianto, dalam karyanya “*Cyber Security Towards Geometry War Between Nations: Geopolitik dan arsitektur*

keamanan dunia di abad horizontal abad ke-21.” Menurut Arianto, melalui konsep Politik Geometrik, keamanan informasi merupakan bagian dari keamanan siber, karena metode dan cara pengamanan informasi merupakan bagian dari keamanan siber. berdasarkan Studi Keamanan Internasional (KIS). Mengenai ancaman abad 21, perlu diperhatikan pendapat Raden Mas, Jerry Indrawani dan Efriza, bahwa ancaman abad 21 bersifat intangible (tidak kasat mata), misalnya ancaman ideologi berupa terorisme. dan radikalisme. mempengaruhi pertahanan negara dan keamanan nasional, khususnya di Indonesia. Dalam situasi ini, ancaman intangible tumpang tindih dengan ancaman siber karena keduanya tidak terlihat namun dampaknya dapat dirasakan. Branscomb mengasumsikan pengetahuan tentang bagaimana aliran darah bekerja dalam tubuh manusia. Jadi, ancaman data adalah ancaman dunia maya, dan ancaman dunia maya sudah pasti merupakan ancaman keamanan dunia maya nasional diikuti oleh ancaman keamanan dunia maya global. Dengan demikian, ancaman terhadap keamanan dunia maya global merupakan ancaman total terhadap keamanan internasional. Indonesia tidak kalah dalam upayanya mencegah serangan siber.

Namun, penggunaan keamanan siber di Indonesia sangat masif dan tidak terkoordinasi secara sistematis. Hal tersebut dijelaskan oleh Eris Heryanto (Sekjen Kemhan) yang menyatakan bahwa konsep pertahanan siber yang diterapkan Kemhan dan TNI selama ini masih bersifat sektoral dan belum menyeluruh. Tindakan Kementerian Pertahanan meliputi menjaga keamanan dan perlindungan internal (Departemen Pertahanan) dan eksternal (nasional) dari berbagai serangan dunia maya. Selain militer, Kemenkominfo juga turut serta mencegah serangan siber dengan membentuk ID SIRTII (Indonesian Security Incident Response Team on Internet Infrastructure). 29/FR/Senin. COMINFO/12/2010. uti pembentukan kelompok kerja di Pusat Operasi Pertahanan Siber, yang tujuannya adalah untuk menjaga keamanan dan perlindungan internal (Departemen Pertahanan) dan eksternal (nasional) dari berbagai serangan dunia maya. Selain militer, Kemenkominfo juga turut serta mencegah serangan siber dengan membentuk ID SIRTII (Indonesian

Security Incident Response Team on Internet Infrastructure). 29/FR/Senin. COMINFO/12/2010.

Sasaran strategis strategi keamanan siber Indonesia adalah untuk mencapai ketahanan siber, keamanan layanan publik, kontrol hukum siber, budaya keamanan siber dan keamanan siber dalam ekonomi siber. Strategi keamanan informasi Indonesia diharapkan menjadi salah satu tumpuan kepercayaan global terhadap Indonesia di beberapa forum keamanan siber internasional. Strategi keamanan siber Indonesia merupakan kontribusi bangsa Indonesia untuk mendorong perdamaian dunia.

II. METODE

Pada penelitian ini menggunakan metode kualitatif dengan pendekatan deskriptif yang bertujuan untuk mendeskripsikan dan menganalisis suatu fenomena, peristiwa, aktivitas sosial, sikap, kepercayaan, persepsi, pikiran individu maupun kelompok. Penelitian deskriptif dilakukan untuk mengetahui nilai variabel mandiri tanpa membuat perbandingan dengan variabel yang lainnya (Sugiyono, 2018). Informasi yang diperoleh disajikan secara analitis-deskripsi, yaitu dengan teknik analisis yang menggambarkan karakteristik variabel yang menjadi fokus perhatian penelitian. Jenis penelitian ini adalah penelitian kepustakaan yaitu penelitian yang menggunakan literatur seperti buku, catatan, artikel dan laporan hasil penelitian yang sudah ada.

III. HASIL PENELITIAN & PEMBAHASAN

A. Latar Belakang Pentingnya Keamanan Siber di Indonesia

Ada banyak istilah dan interpretasi terkait dengan konsep keamanan siber. Karena cyber adalah ruang virtual yang diciptakan oleh perpaduan manusia dan teknologi, khususnya teknologi informasi dan komunikasi. Oleh karena itu, konsep keamanan siber tidak hanya

berdampak pada bidang teknologi, tetapi juga menjadi ancaman bagi keamanan nasional.

	Global	Indonesia
GDP* :	USD 71,620 bn	USD 895 bn
Percent of global GDP*:		1,20 %
Cost of** :		
Genuine Cyber Crime:	USD 3,457 m	USD 43 m
Transitional Cyber Crime:	USD 46,600 m	USD 582 m
Cyber Criminal Infrastructure:	USD 24,840 m	USD 310 m
Traditional Crimes Becoming Cyber	USD 150,200 m	USD 2,748 m

Cybercrime pertama kali muncul pada tahun 1988 dengan nama Cyber Attack. Kemudian, para pelaku mengembangkan worm dan virus untuk menyerang komputer, mengakibatkan kerusakan sekitar 10 persen dari semua komputer Internet di seluruh dunia. Cybercrime adalah tindakan yang berkaitan dengan teknologi informasi di mana satu orang mendapatkan keuntungan dengan mengorbankan orang lain. Itu juga bisa disebut sebagai penjahat dunia maya atau sekelompok orang yang menyerang sistem keamanan komputer atau data yang disimpan di dalamnya. Motif kejahatan ini berkisar dari masturbasi hingga kerugian finansial atau politik.

Oleh karena itu, pembentukan “Tim Respons Insiden Keamanan Infrastruktur Internet Indonesia (IDSIRTII)” oleh Kementerian Komunikasi dan Informatika Republik Indonesia merupakan langkah untuk memastikan stabilitas informasi, keamanan siber, dan perlindungan terhadap segala ancaman dari penjahat siber.

B. Parameter Pertahanan dan Keamanan Siber Nasional Indonesia: Peran ID-SIRTII dan lembaga siber nasional

Saat ini situasi keamanan siber Indonesia berada pada tahap yang sangat kritis dan berbahaya. Hal ini disebabkan meningkatnya informasi global dalam sistem jaringan informasi nasional Indonesia. Indonesia kini menjadi sasaran utama para peretas dan telah menyalip China, membuat kontrol arus informasi semakin sulit. Keadaan ini dapat memicu kejahatan dunia maya secara global, yang jika tidak dikendalikan dengan baik dapat melumpuhkan sistem informasi nasional. Oleh karena itu, perhatian penting harus diberikan pada situasi ini. Kepastian hukum dalam kebijakan keamanan siber diperlukan untuk mencegah melemahnya pertahanan dan keamanan siber di Indonesia. Pada tahun 2007, Menteri Komunikasi dan Informatika menerbitkan Keputusan No. 26/PER/M.Kominfo/5/2007 tentang Pengamanan Penggunaan Jaringan Komunikasi Berbasis Protokol Internet, yang kemudian diubah dengan Keputusan Menteri Komunikasi dan Informatika. Teknologi Informasi NO. 16/PER/M.KOMINFO/10/2010. Aturan tersebut kembali diperbarui dengan Keputusan Menteri Komunikasi dan Informatika No. 29/PER/M.KOMINFO/12/2010. Aturan ini digunakan sebagai dasar ID-SIRTII. ID-SIRTII. Didefinisikan oleh: Melakukan pemantauan, pendeteksian awal, peringatan dini terhadap ancaman jaringan internet. Peraturan ini digunakan sebagai dasar ID-SIRTII. ID-SIRTII. Ditugaskan untuk: 1) Berkoordinasi dengan pihak dalam dan luar negeri guna meningkatkan keamanan jaringan di internet. 2.) Mengoperasikan dan mengembangkan sistem database ID-SIRTII. 3.) Menyusun katalog pemanfaatan jaringan. 4.) Memberikan layanan atas ancaman dan keamanan telekomunikasi yang berbasis protokol internet. 5.) Menjadi contact point dengan lembaga dalam pemanfaatan jaringan telekomunikasi. 6.) Menyusun program kerja keamanan jaringan telekomunikasi yang berbasis internet. 7.) Menyusun program kerja keamanan jaringan telekomunikasi yang berbasis internet.

Kerangka hukum untuk keamanan Cyber Indonesia saat ini sedang dibangun berdasarkan Undang-Undang Informasi dan Transaksi Elektronik No. 11/2008, Peraturan pemerintah untuk dilaksanakan

Sistem dan Transaksi Elektronik No. 82 2012 dan Surat Edaran Menteri dan peraturan kementerian. Namun, masalah terkait mempromosikan keamanan dunia maya Yang sulit antara lain:

Batasan Layanan Server luar negeri dan dibutuhkan menggunakan sistem yang aman; Belum terhadap adanya legalitas yang cukup menangani serangan dunia maya; Administrasi Institusi Keamanan Cyber yang masih parsial dan tersebar dan tidak ada standar koordinasi dalam menangani masalah keamanan dunia maya. Pemrosesan Keamanan Cyber harus terintegrasi dengan kuat dan Keterlibatan berbagai pihak, seperti: Intelijen, Penegakan Hukum, Pertahanan dan keamanan yang baik adalah layanan pertahanan dan TNI serta pemerintah sebagai regulator, diwakili dalam hal ini Kominfo dan Badan Crypto Nasional yang sekarang telah diubah menjadi Badan Siber dan Sandi Negara (BSSN). Guna melawan kejahatan dunia maya ribet tentunya kalau indonesia. Guna menyikapi kejahatan siber yang semakin kompleks, sudah sewajarnya jika Indonesia menempatkan mata siber dalam konteks “pertahanan dan Keamanan Nasional” dengan cara menghadirkan: (1) pembangunan basis strukturalnya seperti diciptakannya suatu Angkatan Siber melengkapi Angkatan Darat, Angkatan Laut, dan Angkatan Udara; (2) pembangunan basis infrastrukturnya seperti diperkuatnya satelit khusus untuk pertahanan dan keamanan siber, termasuk didalamnya; (3) memantau protokol kerja lalu lintas Siber yang secara hukum masuk dalam wilayah Indonesia, namun secara teknisnya dikontrol oleh sejumlah provider telekomunikasi pemilik kuasa dari teknologi dimana alat tersebut dibeli, teknologi asing.

C. Penataan pertahanan dan keamanan nasional Indonesia di bidang siber:

Keinginan lahirnya Angkatan Siber yang bisa melengkapi Angkatan Darat, Angkatan Laut, dan Angkatan Udara harus disikapi secara baik dan benar. Hal ini adalah tantangan bagi pemerintah Indonesia guna bisa

menghadirkan suatu sistem pertahanan dan keamanan siber yang handal dan berkualitas bagi rakyatnya. Selain dari tantangan struktural, tantangan lain ke depannya dalam mengembangkan kebijakan Keamanan Siber adalah sifat dari ancaman Siber yang “geometris dan tak terbatas” membuat penanganannya tidak hanya menjadi tanggung jawab dari TNI, Polri, Kemhan, serta Kemenkominfo. Adapun Salah satu strategi menarik yang patut diperhatikan untuk menghadapi ancaman siber global diantaranya adalah upaya serius pemerintah dalam menangani keamanan siber secara nasional yang didukung oleh sektor swasta maupun masyarakat untuk siber guna melindungi infrastruktur telekomunikasi dan siber dari situasi kritis. Sektor swasta dan masyarakat juga memiliki tugasnya tersendiri yakni untuk membangun dan memelihara sistem keamanan Siber di Indonesia. Pada akhirnya, berangkat dari dua domain “fungsionalisme siber” di atas digunakan untuk menciptakan suatu strukturalisme Pertahanan dan Keamanan Nasional Indonesia di sektor siber, sekarang saatnya Indonesia membentuk Angkatan Siber sebagai pelengkap dari Angkatan Darat, Angkatan Laut, dan Angkatan Udara. Angkatan Siber ini akan menjadi bagian dari formasi struktural di tubuh Tentara Nasional Indonesia (TNI) dengan mengembangkan strategi nasional dalam membangun Keamanan Siber di Indonesia untuk kedepannya. Selain itu, Angkatan Siber dibagi untuk menyelesaikan masalah dan mendukung perkembangan teknologi informasi Indonesia yang tidak hanya di ranah militer, tetapi juga menjangkau ranah sipil dalam membangun Keamanan Siber nasional dan global yang bisa membantu negara. Tugas-tugas yang diemban oleh Angkatan Siber ini diharapkan bisa menjadi pusat kontrol atas sistem informasi nasional, kompetisi organisasi informasi, pengambilan keputusan organisasi informasi, dan fungsionalisme sistem informasi dalam dua domain dimaksud dengan bekerjasama dengan institusi siber lainnya.

IV. KESIMPULAN

Dengan kemajuan teknologi siber di seluruh dunia, saat ini Indonesia berada di posisi pertama sebagai negara yang berpotensi menjadi target hacker dari seluruh dunia. Hadirnya fungsionalisme siber ini sebagai arena politik internasional, Indonesia harus mulai mempersiapkan agenda besar yang digunakan untuk mendukung pertahanan dan keamanan siber nasional yang bisa mencegah ancaman siber global, baik di bagi sipil maupun militer yang bisa mengarah pada “Perang Siber Global (PSG)” atau lebih dikenal sebagai “Perang Geometri Antarbangsa (PGA).” Selain itu, melanjutkan kajian Geometri Politika yang menghasilkan sebuah kekuasaan siber atas dilibatkannya matra siber dalam kekuasaan dengan istilah “geometrik”, maka kita juga akan bertemu dengan “Negara Maya atau Pemerintahan Siber.” Hal ini bisa menjadi pengingat bahwa kekuasaan juga dapat terbentuk di dunia siber yang dipimpin oleh suatu kedaulatan siber. Setidaknya, dengan adanya “Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII)”, Indonesia telah memberikan jawaban sesuai dengan ketersediaan SDM dan SDA.

Dalam melakukan pencegahan dari ancaman siber global, penelitian ini menemukan bahwa ancaman siber di Indonesia sangat kompleks, terlihat dari adanya variasi aktor, motif, dan targetnya. Kompleksitas ini dijelaskan melalui empat aspek 28 Jurnal Pertahanan & Bela Negara April 2019, Volume 9 Nomor 1 berikut, yaitu: (1) berangkat dari studi Geometri Politika, fungsionalisme siber berada dalam dua domain, yaitu “fungsionalisme siber untuk tujuan politik tingkat tinggi atau yang biasa disebut juga sebagai geometrik militer yang merupakan sebuah formulasi dan aktivasi dari kekuatan Siber guna menghadapi terjadinya Perang Siber Global (PSG), Perang Geometri Antarbangsa (PGA), dan kompleksitas terciptanya “Negara Maya atau Pemerintahan Siber”; dan “fungsionalisme siber untuk tujuan politik tingkat normal (geometrik sipil)” berupa sebuah perlindungan dari segala aktivitas sipil di dunia maya; (2) guna mencegah meluasnya kejahatan siber, dilaksanakan pada kebijakan ID-SIRTII harus terlaksana dengan peran dari institusi siber nasional; (3) guna menghadapi Ancaman Siber Global, pelaksanaan

kebijakan ID-SIRTII perlu diperhatikan oleh institusi siber regional dan global; dan (4) berangkat dari dua “fungsionalisme siber” di atas sekaligus berusaha menciptakan suatu struktur Pertahanan dan Keamanan Siber Nasional Indonesia, sekarang waktunya Indonesia untuk bisa membentuk Angkatan Siber Nasional ini sebagai pelengkap dari Angkatan Darat, Angkatan Laut, dan Angkatan Udara. Angkatan Siber dibagi agar bisa menyelesaikan masalah serta mendukung perkembangan teknologi informasi yang tidak hanya di bagian militer, tetapi juga mencakup sipil dalam pembangunan Keamanan Siber nasional dan global. Keempat hal ini setidaknya dapat menjadi sebuah indikator agar kita bisa memahami kesiapan dari Indonesia dalam menghadapi berbagai macam kemungkinan yang bisa terjadi dengan dunia Internasional Abad ke-21 yang akan mulai didominasi oleh teknologi siber.

DAFTAR REFERENSI

Sugiyono. 2018. Metode Penelitian Kuantitatif, Kualitatif dan R&D. Bandung : Alfabeta

Akamai. 2013. "The State of The Internet Report". Dokumen Americas Highlights. Second Quarter.

Djojonegoro, Ngasiman. 2021. "Profesionalisme TNI pada Era Pertahanan Siber".
<https://www.antaraneews.com/berita/2538541/profesionalisme-tni-pada-era-pertahanan-siber> , diakses pada 15 Mei 2023.

Merdeka. 2021. "Panglima TNI: Profesionalisme dan Pengabdian Bukti Kesetiaan Prajurit untuk Bangsa."
<https://www.merdeka.com/peristiwa/panglima-tni-profesionalisme-dan-pengabdian-bukti-kesetiaan-prajurit-untuk-bangsa.html> , Diakses pada 15 Mei 2023.

Subagyo, Agus. 2017. Mewujudkan Profesionalisme Tni AD Di Era Reformasi.
https://www.researchgate.net/publication/322306489_MEWUJUDKAN_PROFESIONALISME_TNI_AD_DI_ERA_REFORMASI .
Diakses pada tanggal 15 Mei 2023

Kemhan. 2015. "Konsep Pertahanan Indonesia Didasarkan pada Ancaman Nyata dan Tidak Nyata."
<https://www.kemhan.go.id/2015/05/27/konsep-pertahanan-indonesiadidasarkan-pada-ancaman-nyata-dan-tidak-nyata.html>
Diakses tanggal 15 Mei 2023.

Pasal 9 Peraturan Menteri Komunikasi dan Informatika No. 29/PER/M. KOMINFO/12/2010 tentang perubahan kedua Peraturan Menteri Komunikasi dan Informatika No. 26/PER/M. Kominfo/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet.

Arianto, Adi Rio. 2017. "Cyber Security: Geometripolitika dan Dimensi Pembangunan Keamanan Dunia Era Horizontal Abad 21". Jurnal Power In International Relations. Universitas Potensi Utama. Vol. 1. No.2. Februari.

Gautama, Hasyim, "Penerapan Cyber Security", dalam http://kemhubri.dephub.go.id/pusdatin/files/materi/Penerapan_Cybersecurity.pdf , diakses pada 17 Oktober 2018.

"Kemkominfo: Pengguna Internet di Indonesia Capai 82 Juta", dalam http://kominfo.go.id/index.php/content/detail/3980/Kemkominfo%3A+Pengguna+Interet+di+Indonesia+Capai+82+Juta/0/berita_satker#.U9G4o5R_tfs , diakses pada 15 Mei 2023.