Jurnal Trends. Volume 01 Nomor 01 Tahun 2023

CYBER WAR: ANCAMAN PADA KEAMANAN NASIONAL

Dewi Chirzah[1]*, Rizqy Akbar Ramadhan[2]
[1] Program Studi Sains Data, Institut Teknologi Bisnis dan Kesehatan Bhakti Putra Bangsa Indonesia, Indonesia.
[2] Program Studi Informatika, Universitas Perwira Purbalingga, Indonesia..
[1]dewi.chirzah@ibisa.ac.id
[2]ramadhanrizqy72@gmail.com

ABSTRAK

Internet sebagai salah satu bentuk perkembangan teknologi di zaman keuniversalan yang telah menciptakan suatu bentuk korelasi; interdependensi dan interkoneksi yang menimbulkan konsekuensi *cyberwar. Cyberwar* merupakan jenis tindakan agresi yang dilakukan oleh negara, individu, kelompok atau organisasi yang menargetkan sistem informasi komputer, infrastruktur, jaringan komputer dan atau perangkat komputer pribadi melalui berbagai tindakan berbahaya dengan maksud mencuri, mengubah atau menghancurkan dengan menerobos konstelasi yang rawan. Analisis berpusat pada berbagai bentuk ancaman dan serangan serta dampak yang ditimbulkan dari *cyberwar* dalam skala nasional. Analisis menggunakan metode kualitatif non interaktif yang beracuan pada sumber sekunder dari beberapa dokumen sehingga dapat dipertanggungjawabkan. Jadi, penelitian ini dirasa cukup penting untuk meningkatkan pemikiran, kognisi dan pendangan terkait kondisi *cyberspaces* dalam negeri dan ancaman *cyberwar* dimasa mendatang.

Kata Kunci: Cyberwar, Interdependensi, Interkoneksi.

ABSTRACT

The internet as a form of technological development in the age of universality has created a form of correlation; interdependence and interconnection that has led to the consequences of cyberwar. Cyberwar is a type of aggression committed by a state, individual, group or organisation that targets computer information systems, infrastructure, computer networks and or personal computer devices through various malicious actions with the intention of stealing, altering or destroying by breaking through vulnerable constellations. The analysis centred on the various forms of threats and attacks as well as the impacts of cyberwar on a national scale. The analysis uses a non-interactive qualitative method that refers to secondary sources from several documents so that it can be accounted for. Thus, this research is considered important enough to improve thinking, cognition and views related to the condition of domestic cyberspaces and the threat of cyberwar in the future.

Keywords: *Cyberwar, Interdependence, Interconnection.*

PENDAHULUAN

Pada abad ke-21, era globalisasi semakin meningkat dan berkembang secara pesat sebagai efek dari kemajuan teknologi informasi salah satunya internet. Era globalisasi telah menciptakan suatu bentuk korelasi yang saling bergantung (*interdependence*) dan saling terhubung (*interconnection*) antar negara dan pelaku internasional secara global. Akibat globalisasi, interdependensi dan interkoneksi menciptakan 2 konsekuensi utama yaitu, identik dengan integrasi globalisasi menimbulkan fenomena permasalahan baru yang tidak dapat diselesaikan oleh tiap-tiap masyarakat suatu negara, melainkan harus diselesaikan secara bersama-sama sebagai komunitas warga dunia. Konsekuensi kedua, globalisasi dicirikan oleh menipisnya batas negara atau dapat di katakan tidak ada sekat dan batas lagi antarnegara dan pelaku internasional mengenai isu-isu permasalahan internasional yang telah melebar tidak lagi semata-mata menangkut ancaman terhadap stabilitas nasional dan regional tapi juga dunia seperti ancaman *cyberwar*, persaingan ideologi antara komunisme dan kapitalisme, perang nuklir, krisis diplomasi dan masalah lainnya.

Dari konsekuensi kedua, hal itu menyebabkan meluasnya isu politik dan ancaman dari internasional seiring meningkatnya penggunaan internet di seluruh dunia yang sejalan dengan meningkatnya penyalahgunaan melalui internet atau biasa disebut dengan perang siber (*cyberwar*). *Cyberwar* atau *cybercrime* adalah setiap aktivitas yang dilakukan seseorang, sekelompok orang, badan hukum atau entitas yang menggunakan komputer untuk melakukan kejahatan atau menjadia komputer sebagai objek kejahatan. Semua kejahatan tersebut merupakan perbuatan melawan hukum dan peraturan perundang-undangan, baik secara material maupun secara formal.

Dikutip dari jurnal (Yanuar, 2021) sebuah lembaga pencegahan kejahatan di Havana, Kuba pada tahun 1999 dan di Wina, Austria pada tahun 2000, menyebutkan terdapat dua (2) pengertian *cybercrime* secara garis sempit luas. *Cybercrime* dalam arti sempit, yaitu aktivitas mencurigakan ilegal atau melanggar hukum secara langsung menyerang sistem keamanan komputer dan data yang diproses oleh komputer. Adapun *cybercrime* dalam arti luas, yaitu aktivitas mencurigakan, ilegal atau melanggar hukum terkait dengan sistem atau jaringan komputer.

Cybercrime atau kejahatan siber memiliki beberapa jenis antara lain *unauthorized access, illegal contents*, penyebaran virus dengan sengaja, *data forgery, cyber espionage, sabotage and extortion, cyberstalking, hacking and cracking, carding, cybersquatting and typosquatting, hijacking, cyber terorism, cyber attack, spywar* dan sebagainya. Dari semua bentuk kejahatan tersebut dapat mengancam keamanan nasional sewaktu-waktu sehingga Indonesia harus memiliki sistem *cyber security* sebagai pelindung dan pertahanan dalam menanggulangi serta mengatasi *cybercrime.*

Untuk mengatasi *cybercrime* yang telah menjadi ancaman komunitas warga internasional, tiap-tiap negara perlu untuk berkolaborasi dalam mengatasi dan mencegah tindakan *cybercrime* serta melibatkan institusi Internasional yang memiliki wewenang pada *cyber security* yang bertujuan untuk menyiapkan segala aspek dalam menghadapi ancaman *cybercrime* pada saat-saat tertentu.

Penulisan ini memiliki matlamat untuk menjabarkan ancaman terhadap keamanan dalam negeri Indonesia saat ini dan masa depan dengan salah satunya adalah ancaman *cyberwar* atau *cybercrime* serta menguji sejauh mana ancaman dan bahaya tersebut mengancam keamanan

dalam negeri dan masyarakat Indonesia. Penulis menyadari sangat banyak kekurangan pada penulisan ini, namun penulis akan terus berusaha menampung saran dan kritik yang membangun sembari meerbaiki kekurangan-kekurangan pada penulisan ini. Penulis berharap semoga jurnal ini dapat berguna bagi semua yang akan melakukan penelitian mengenai *cyberwar* atau *cybercrime* dan ancaman dunia internasional bagi keamanan dalam negeri Indonesia.

TINJAUAN PUSTAKA

A. Teori Sekuritisasi

Barry Guzan menjelaskan teori sekuritisasi dalam bukunya yang berjudul "*Security : A Framework for Analysis*" bahwa suatu isu dapat menjadi masalah keamanan karena adanya aktor-aktor yang merencanakannya dengan mengatakan bahwa isu tersebut merupakan ancaman terhadap suatu objek. Teori sekuritisasi memiliki 3 model untuk menguji sektor *cyber* secara spesifik, yaitu:

a. *Hyper Securitization*, model ini digunakan untuk menggambarkan ancaman dan bahaya serangan melalui jaringan di sebuah negara dengan level di atas normal dimana jaringan yang rusak menyebabkan kerugian yang sangat besar di berbagai sektor terutama militer dan keuangan.
b. *Everyday Security Practice*, model ini bertujuan untuk mengamankan aktor, memobilisasi individu "normal" untuk mengamankan kemitraan individu dan membuat skenario *hypersecuritization* menjadi lebih masuk akal dengan strategi yang menggabungkan alat dan pengalaman skenario ancaman.
c. *Technification*, model ini memanfaatkan pakar teknologi *cyber* yang berperan penting dalam *hypersecuritization.*

B. Cyberspaces

Istilah *Cyberspaces* pertama kali diperkenalkan oleh William Gibson dalam bukunya yang berjudul "*Neuromancer*" sementara masyarakat Indonesia lebih akrab dengan sebutan dunia maya. *Cyberspace* sendiri adalah sebuah gambaran besar informasi yang berasal dari dunia realitas sebagai suatu bentuk kesadaran tanpa tubuh dengan masuk ke dalam sebuah jaringan (Tampubolon, 2019). Kemudian dalam buku *Cyberculture Theorists*, David Bale menyebut *cyberspaces* sebagai alam semesta paralel, sebab tersusun atas berbagai jaringan listrik berbeda yang berjalan dan setiap jaringan mewakili tingkat *artificial intellegence* yang berbeda.

Dengan kemajuan teknologi seperti saat ini, *cyberspaces* telah menjadi wadah aktivitas yang terjadi di dunia nyata yang bertransformasi ke dalam dunia maya salah satunya adalah peperangan (Afrinata, 2012). Peperangan yang terjadi bukan lagi peperangan fisik melainkan peperangan dunia maya yang dapat menjadi ancaman keamanan nasional. Akibatnya, konsep keamanan nasional telah bergeser dan bertransformasi dari keamanan tradisional ke keamanan non-tradisional yang berfokus pada *human security*. *Human security* meliputi pelbagai sektor keamanan seperti keamanan ekonomi, keamanan kesehatan hingga keamanan politik.

METODE PENELITIAN

Penelitian ini berfokus pada berbagai bentuk ancaman dan serangan *cyber* dari internasional ke dalam negeri Indonesia dari dulu hingga saat ini. Dari objek penelitian, akan dianalisis tentang jenis, bahaya serta kemungkinan besar dampak serangan *cyber* dalam menganggu keamanan dalam negeri atau nasional Indonesia.

Penelitian ini menggunakan metode kualitatif non interaktif. Metode kualitatif sering disebut dengan metode baru, *pospositivistik, artistik,* dan *interpretive research* yang digunakan untuk meneliti pada kondisi obyek alamiah dimana peneliti sebagai instrumen kunci (Sugiyono, 2019). Metode

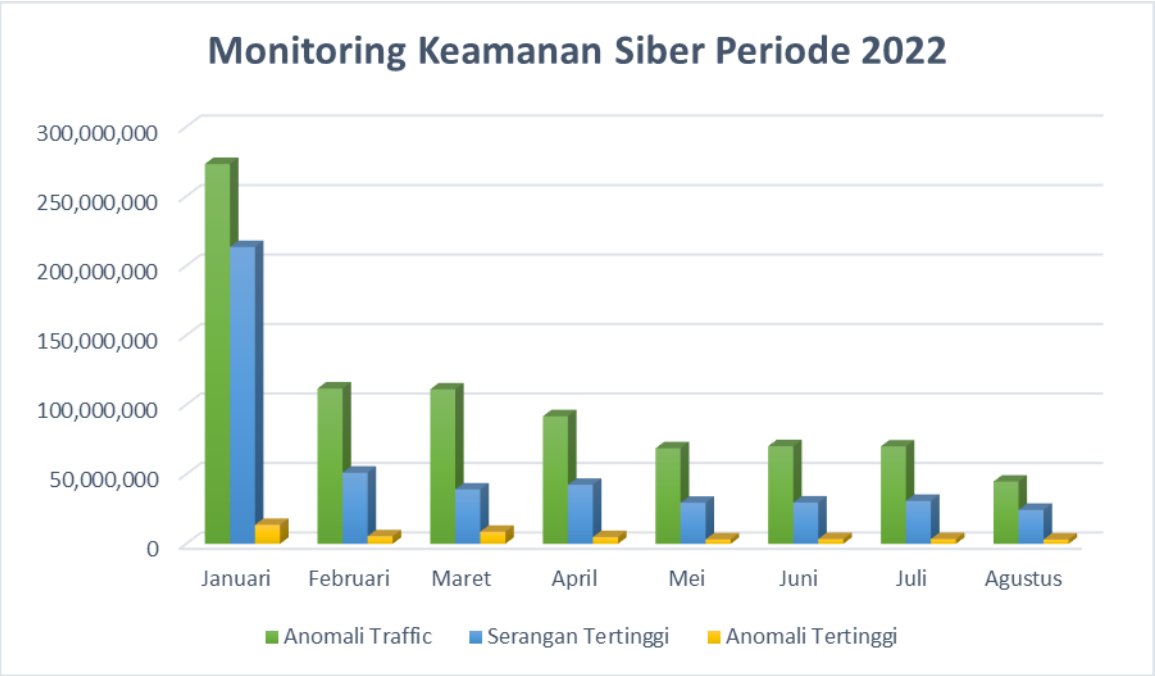
kualitatif non interaktif sendiri disebut juga sebagai penelitian analisis dengan mengadakan pengkajian berdasarkan analisis dokumen. Penelitian ini beracuan pada sumber-sumber sekunder dari beberapa dokumen seperti jurnal, portal berita, *website*, dan *e-book* yang membahas mengenai *cyberwar* dan keamanan nasional.

HASIL DAN PEMBAHASAN

Pada era teknologi yang berkembang pesat seperti masa sekarang, internet merupakan hal yang sangat vital di tengah-tengah masyarakat. Internet sudah menjadi salah satu kebutuhan manusia pada masa sekarang selain 3 kebutuhan pokok manusia; kebutuhan papan, kebutuhan pangan dan kebutuhan sandang. Dengan demikian setiap negara harus mampu menguasai, mengontrol dan mengendalikan pergerakan internet setiap warganya. Bagaimana tidak, khusus di Indonesia menurut data dari *Hootsuite (We Are Social)* pengguna internet di Indonesia pada tahun 2022 mencapai angka 204,7 juta atau naik 1 persen dari tahun 2021 yang mencapai 202,6 juta. Jumlah tersebut menunjukkan bahwa pengguna internet di Indonesia mencapai 74 persen dari populasi penduduk Indonesia. Dari jumlah pengguna internet tersebut, sebanyak 191,4 juta merupakan pengguna media sosial aktif atau naik sebesar 12,6 persen dari tahun 2021 yang mencapai 170 juta. Berdasarkan data yang diambil menggambarkan bahwa masyarakat khususnya masyarakat Indonesia telah menciptakan dunia baru yang berdampingan dengan dunia nyata.

Apalagi pada kondisi *pandemic covid-19* seperti saat ini yang mengharuskan di setiap sektor bertransformasi dengan menggunakan media *online* dalam aktivitasnya. Beberapa sektor vital yang menggunakan media online dalam aktivitasnya yaitu: (1) Sektor Pendidikan, sektor pendidikan menjadi yang paling pertama terkena dampaknya dimana mengharuskan setiap institusi pendidikan mulai dari sekolah dasar hingga perguruan tinggi mengalihkan pembelajaran mereka menjadi *e-learning*. (2) Sektor Bisnis dan Pekerjaan, selain pendidikan, sektor bisnis dan pekerjaan juga menerapkan hal yang sama dengan membatasi setiap karyawan yang datang ke kantor atau bahkan memberlakukan kerja dari rumah (*Work From Home*/WFH) secara menyeluruh dan (3) Sektor Perbankan dan Perdagangan, yang terakhir adalah sektor perbankan dan jual beli yang menggunakan media *online* sebagai *platform* aktivitas jual beli dengan maraknya aplikasi toko *online* dan perbankan yang saling berkolaborasi. Akibatnya permintaan pemasangan *wifi* untuk akses internet dari rumah mengalami peningkatan.

Namun, peningkatan pengguna internet memiliki sisi negatif terhadap keamanan individu dan keamanan nasional. Beberapa dampak negatif yang ditimbulkan dari hal tersebut adalah pencurian data, maraknya penyebaran *hoax* atau berita palsu, penyebaran konten provokatif dan lainnya. Badan Siber dan Sandi Negara (BSSN) mencatat selama periode Januari – Agustus 2022 telah terjadi sebanyak 841.920.975 anomali *traffic* (BSSN, 2022).



Gambar 1. Diagram Monitoring Keamanan Siber 2022

Serangan pada bulan Januari tercatat oleh BSSN sebanyak 273.313.399 anomali *traffic* dengan serangan tertinggi terjadi pada 20 Januari 2022 sebanyak 13.664.793 yang didominasi oleh serangan *malware*, aktivitas *trojan*, *exploit* dan *information leakage*. Terjadi penurunan serangan berturut-turut pada bulan Februari hingga Mei yaitu turun dari 111.773.819 serangan pada bulan Februari ke angka 68.732.476 serangan. Serangan masih didominasi dengan serangan *malware*, aktivitas *trojan*, *exploit* dan *information leakage*. Namun, pada periode ini kasus *information leakage* mengalami peningkatan yang cukup signifikan. Serangan mengalami peningkatan pada bulan Juni dengan total 70.257.042 serangan. Puncaknya pada tanggal 10 Juni 2022 terjadi sebanyak 3.435.259 serangan dengan serangan *malware* dan *information leakage* menjadi dua serangan paling sering terjadi pada bulan ini. Pada bulan Juli hingga Agustus terjadi penurunan kasus yang cukup signifikan sebanyak 25.316.015 serangan. Lihat pada Tabel 1

Bulan	**Anomali Traffic**		
	Jumlah	**Anomali Tertinggi**	**Dominasi Serangan**
Januari	273.313.399	20 Januari 2022	Malware
Februari	111.773.819	7 Februari 2022	Malware
Maret	111,160.791	25 Maret 2022	Trojan
April	91.795.651	21 April 2022	Malware
Mei	68.732.476	6 Mei 2022	Malware
Juni	70.257,042	10 Juni 2022	Malware
Juli	70.092.906	19 Juli 2022	Malware
Agustus	44.776.891	3 Agustus 2022	Malware

Tabel 1. Tabel Monitoring Keamanan Siber 2022

Hingga Oktober 2022, terdapat 893.952.873 anomali *traffic* dengan rincian kasus dimana sebagian besar serangan datang dalam bentuk aktivitas serangan *malware* yang mencapai 55,83 persen, kemudian *information leakage* dengan 14,99 persen dan aktivitas *trojan* sebesar 10,45 persen.

Hal ini membuktikan bahwa dari adanya peningkatan penggunaan internet berdampak pada peningkatan terjadinya serangan siber. Lebih dari itu, hal tersebut akan lebih memperbesar potensi terjadinya perang siber antar negara maupun serangan siber dengan aktor bukan negara. Menurut data (Kompas, 2021) terdapat beberapa contoh efek dari penggunaan internet terhadap stabilitas keamanan dalam negeri Indonesia, antara lain:

a. Kasus BPJS Kesehatan

Pada akhir Mei 2021, situs Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan, yakni bpjs-kesehatan.go.id diduga diretas. Alhasil, data milik 279 juta warga Indonesia diduga bocor dan dijual pada Raid Forums. Data yang dijual seharga 0,15 bitcoin atau sekitar Rp 84,4 juta (kurs 20 Mei 2021) termasuk data NIK, nomor ponsel, *e-mail*, alamat hingga gaji.

Demikian menurut kajian mendalam Kementerian Komunikasi dan Informatika, menyimpulkan bahwa sampel dataset tersebut diduga kuat identik dengan data milik BPJS Kesehatan. Kementerian Komunikasi dan Informatika akhirnya mengusulkan untuk menghentikan akses penggunaan tautan (*link*) untuk mengunduh data pribadi, termasuk memblokir Raid Forums sebagai langkah antisipatif dan proaktif untuk mencegah penyebaran data lebih lanjut.

b. Kasus Asuransi BRI Life

Perusahaan asuransi BRI Life diretas pada 27 Juli 2021. Dalam kasus ini, diduga sekitar 2 juta data nasabah BRI Life bocor dan dijual seharga U$D 7.000 atau sekitar Rp 101,6 juta (kurs 21 Juli 2021) di dunia maya. Kobocoran data pertama kali diungkap oleh akun Twitter *@UnderTheBreach* yang mengklaim bahwa *hacker* berhasil mendapatkan data sebesar 250 GB data dari BRI Life termasuk 2 juta file data nasabah dalam format PDF dan sekitar 463 ribu dokumen lainnya. Data nasabah yang bocor tersebut meliputi informasi gambar KTP, rekening, nomor wajib pajak, akte kelahiran hingga rekam medis. Kebocoran data diduga karena adanya celah keamanan pada sistem elektronik internal pihak BRI Life yang dimanfaatkan oleh pihak yang tidak bertanggung jawab.

c. Situs Sekretariat Kabinet Republik Indonesia

Beberapa hari kemudian, situs web Sekretariat Kabinet Republik Indonesia (Setkab RI) setkab.go.id diretas dengan metode *deface*. Secara sederhana dengan menggunakan metode ini, peretas (*hacker*) dapat mengubah tampilan halaman web target sesuai dengan keinginannya. Pada 30 Juli 2022, situs setkab.go.id diretas dan tidak bisa diakses serta berubah tampilan menjadi hitam dengan foto yang menampilkan demonstran membawa bendera merah putih yang dibawahnya tertulis keterangan "Padang Blackhat || Anon Illusion Team Owned By Zyy Ft Luthfifake". Polisi menduga peretasan ini dilakukan karena alasan keuangan, dengan maksud untuk menjual *script backdoor* dari *website* target kepada yang membutuhkan. Menurut penyelidikan sementara Polisi, peretasan tersebut disebabkan oleh lemahnya sistem keamanan dan kelalaian operator. Pihak Setkab memastikan tidak ada dokumen rahasia pada situs Setkab.

d. Kasus e-HAC Kementerian Kesehatan

Agustus 2021, muncul kabar peretasan pada aplikasi Electronic Health Alert (e-HAC) buatan Kementerian Kesehatan (Kemenkes) yang buntutnya data milik 1,3 juta masyarakat Indonesia yang tersimpan dalam aplikasi tersebut bocor. Aplikasi e-HAC adalah versi modern dari kartu peringatan kesehatan dan merupakan persyaratan wajib bagi mereka yang

ingin berpergian di dalam maupun luar negeri. Kebocoran data pertama kali ditemukan oleh peneliti keamanan siber VPNMentor pada 15 Juli 2021. VPNMentor mengklaim bahwa aplikasi e-HAC tidak memiliki protokol keamanan aplikasi yang tepat sehingga rentan terhadap peretasan dan penyusupan serta pengembang dilaporkan menggunakan basis data Elasticsearch yang kurang aman digunakan untuk penyimpanan data. Kasus ini tidak hanya mengungkap data pengguna e-HAC tetapi juga seluruh infrastruktur terkait e-HAC seperti data tes Covid-19 yang dilakukan penumpang, data pribadi penumpang, data rumah sakit hingga data staff e-HAC. Pihak Kementerian Kesehatan mengumumkan bahwa sumber aliran data berasal dari mitra aplikasi e-HAC yang lama. Namun, pemerintah telah menghentikan penggunaan aplikasi ini sejak 2 Juli 2021.

e. Badan Intelijen Nasional dan 10 Jaringan Kementerian

Pada September 2021, Sistem jaringan internal milik 10 kementerian dan lembaga negara Indonesia termasuk milik Badan Intelijen Negara (BIN) dilaporkan telah diretas berdasarkan laporan terbaru dari sekelompok peneliti keamanan siber yang berafiliasi dengan media massa internasional *TheRecord*, Insikt Group. Insikt Group hanya mengungkapkan bahwa insiden peretasan terkait dengan Mustang Panda, kelompok *hacker* asal China yang biasanya memata-matai dunia maya dan aktivitasnya menargetkan kawasan Asia Tenggara. Insikt Group menemukan server *Command and Control* (C&C) grup Mustang Panda menggunakan *malware* tipe PlugX. Server tersebut berkomunikasi dengan beberapa *host* yang berpotensi terinfeksi di jaringan internal pemerintah Indonesia.

f. Situs Pusmanas Badan Siber Sandi Negara

Situs milik Badan Siber dan Sandi Negara (BSSN) menjadi korban peretasan *hacker* dengan teknik *deface* pada Oktober 2021. Situs yang berhasil dibobol adalah Pusat Malware Nasional (Pusmanas) yang menurut BSSN, situs tersebut tercantum informasi mengenai laporan (repositori) *malware*. Serangan terhadap situs BSSN diunggah oleh akun Twitter @son1x777 yang memperlihatkan situs Pusmanas BSSN yang sudah di-*hack* dengan teknik *deface*, dimana pada halaman muka situs menampilkan tulisan "Hacked by theMx0nday (diretas oleh theMx0nday)". Terkait insiden tersebut, BSSN segera melakukan penanganan yang dilakukan oleh *Computer Security Incident Response Team* (CSIRT) BSSN.

g. Database Polri

Pada November 2021, *hacker* mengklaim telah membobol database Polri, informasi ini dilaporkan pada 17 November 2021 oleh akun Twitter @son1x666. Dalam tweetnya, *hacker* mengatakan bahwa 28.000 kredensial pribadi dan *log in* telah dicuri. Dia juga menyertakan 3 tautan yang tercantum spesimen informasi yang diduga berasal dari *database* Polri yang berisi informasi sensitif seperti nama lengkap, tempat tanggal lahir, nomor registrasi pokok, alamat rumah, pangkat, golongan darah, satuan kerja, suku, email hingga pelanggaran yang pernah dilakukan oleh anggota. Ada pula data tentang rehab putusan, rehab putusan sidang, rehab keterangan, id propam dan beberapa lainnya. Data ini bisa diakses dan diunduh secara bebas.

h. Bjorka

Tahun 2022 dikejutkan dengan sosok Bjorka. Bjorka diduga *hacker* yang meretas situs Kementerian Komunikasi dan Informatika. Nama Bjorka muncul dalam komentarnya di situs forum brached.to terkait peretasan data dari Indonesia sejak Agustus lalu. Bjorka mengklaim telah menjual sebanyak 105 juta data milik warga Indonesia yang diperoleh dari

Komisi Pemilihan Umum (KPU) serta mengklaim telah mempunyai 1,3 milyar data pendaftaran kartu SIM prabayar yang terdiri atas NIK, nomor telepon, operator seluler hingga tanggal registrasi (Bineksari, 2022).

Dari beberapa contoh diatas merupakan bukti bahwa potensi meningkatnya *cyberwar* di era globalisasi dan pandemi *covid-19* semakin besar ditunjang dengan penggunaan internet yang semakin meningkat tanpa dibarengi dengan edukasi para penggunanya. Berdasarkan hal itu, pemerintah Indonesia perlu untuk mencari elemen perlindungan diri dengan berbasis *cyber* sehingga pemerintah Indonesia memiliki *cyber security* yang bertujuan untuk memberikan rasa aman dari ancaman serangan *cyber*.

Cyber Security

Menurut ISO/IEC 27032:2012 *Cybersecurity* merupakan upaya yang dilakukan dalam menjaga kerahasiaan (*confidentiality*), integritas (*integrity*) dan ketersediaan (*availability*) dari informasi di *cyberspace*. Sedangkan menurut CISCO, *cybersecurity* adalah praktik melindungi sistem, jaringan dan program dari serangan digital. Dari sini dapat disimpulkan bahwa *cybersecurity* atau keamanan siber adalah suatu tindakan untuk melindungi sistem komputer terhadap serangan atau akses ilegal (Permatasari, 2022).

Dikutip dari jurnal yang ditulis oleh (Yanuar, 2021) mengatakan bahwa dalam lingkup internasional terdapat konsep bersama dalam menanggulangi adanya serangan siber, yaitu Global *cyber-security*. Global *cyber-security* didasarkan pada 5 bidang kerja; Pertama, elemen kepastian hukum (undang-undang *cybercrime*). Kedua, elemen teknis dan tindakan prosedural (sebuah aksi konkrit dalam menanggulangi *cyber attack*). Ketiga, elemen struktur organisasi (struktur organisasi yang berperan dalam *cyber security*). Keempat, elemen *capacity building* dan pendidikan pengguna (kampanye publik dan edukasi terhadap *cyber security*). Kelima, elemen kerjasama internasional (termasuk kolaborasi resiprokal dalam upaya mengatasi ancaman *cyber*).

Elemen-elemen tersebut merupakan elemen yang telah dilakukan pemerintah Indonesia hingga saat ini. Dikutip dari jurnal (Ardiyanti, 2014) strategi Indonesia dalam menghadapi ancaman *cyber security*, antara lain:

1. Kepastian Hukum

   Kebijakan *cyber-security* secara khusus di Indonesia telah diinisiasi sejak tahun 2007 dengan dikeluarkannya Peraturan Menteri Komunikasi dan Informatika No. 26/PER/M.Kominfo/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet yang kemudian direvisi dengan Peraturan Menteri Komunikasi dan Informatika No.16/PER/M.KOMINFO/2010 yang kemudian diperbaharui lagi dengan Peraturan Menteri Komunikasi dan Informatika No.29/PER/M.KOMIFO/2010. Salah satu yang diatur dalam peraturan tersebut adalah pembentukan ID-SIRTII (*Indonesia Security Incident Response Team on Internet Infrastructure*) yang ditugaskan oleh Menteri Komunikasi dan Informatika (Kominfo) untuk membantu pemantauan keamanan jaringan telekomunikasi berbasis protokol internet.

   Menurut Hasyim Gautama, payung hukum *cyber-security* Indonesia saat ini berdasarkan atas dasar Undang-Undang Informasi dan Transaksi Elektronik No. 11 Tahun 2008, Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik No. 82 Tahun 2012 serta Surat Edaran Menteri dan Peraturan Menteri.

2. Teknis dan Tindakan Prosedural

   Untuk elemen teknis dan tindakan prosedural, butuh adanya aksi nyata dari setiap aktor *cyber-security* yang terkait dengan keamanan informasi, standar infrastruktur yang wajib dipenuhi sesuai dengan standar internasional dalam menghadapi *cyberwar* termasuk didalamnya adanya perlindungan perimeter yang memadai, adanya sistem pemantauan jaringan, adanya sistem manajemen informasi dan manajemen insiden yang dirancang untuk memantau berbagai peristiwa jaringan yang terkait dengan kegagalan keamanan informasi, *network security assesment* yang berperan sebagai kontrol dan pemelihara keamanan.
3. Struktur Organisasi

   Guna mengatasi *cybercrime* dengan *cyber security*, Kementerian Pertahanan dan Keamanan membentuk Tim Kerja Pusat Operasi Dunia Maya (*Cyber Defence Operation Centre*) yang bertujuan menjaga keamanan dan perlindungan internal Kementerian Pertahanan dan Keamanan maupun keamanan dan perlindungan eksternal yaitu negara Indonesia itu sendiri. *Cyber Defence Operation Centre* dalam tataran kebijakan *cyber-security* nasional pembentukannya ditujukan untuk membangun sistem pertahanan universal pada tingkat kebijakan keamanan siber nasional yang mencakup semua warga negara, wilayah dam sumber daya nasional lainnya untuk mendukung kedaulatan negara, integritas wilayah dan keselamatan bangsa dari ancaman *cyber*.
4. Capacity Building

   Guna meningkatkan kualitas Sumber Daya Manusia, Program pelatihan dan peningkatan keahlian *cyber-security* dilakukan dalam koordinasi *Cyber Defence Operation Centre* dengan melakukan pembinaan tentang arti pentingnya *cyber-security* guna meningkatkan pemahaman langkah-langkah preventif dalam menangkal segala tindak *cybercrime.* Selain itu, dalam tubuh TNI telah melakukan kerjasama dengan *stakeholder* yang memiliki kemamuan di bidang Informasi Teknologi seperti yang dilakukan TNI AD dengan Institut Del (IT Del), Sumatera Utara yang berlangsung dari tahun 2014 hingga 2017 dalam 3 program, antara lain: penyiapan model perang *cyber,* seminar *military cyber intellegence and cyber operation*, serta *cyber camp* atau pekan *cyber* (Badri, 2012).
5. Kerjasama Internasional

   Langkah kerjasama Internasional yang dilakukan oleh Indonesia dalam rangka penanggulangan *cybercrime* diantaranya dengan melakukan kerjasama bilateral dibidang *cyber-security* dengan Jepang, Inggris, Amerika Serikat dan beberapa negara lain serta menjadi anggota berbagai komunitas, organisasi dan forum internasional, diantaranya:

   a. ASEAN *Network Security Action Council*
   b. *International Telecommunication Union* (ITU)
   c. *Forum of Incident Response and Security* (FIRST
   d. Serta menjadi *steering committee Asia Pacific Computer Emergency Response Team* (APCERT)

   Indonesia juga berperan aktif dalam program *Global Cyber Security Agenda* (GCSA) yang diluncurkan pada *World Telecommunication and Information Society Day* 2007 yang merupakan program kerjasama internasional yang bertujuan untuk menciptakan kepercayaan dan keamanan di tengah masyarakat informasi.

Lima hal tersebut telah dijalankan oleh Badan Siber dan Sandi Negara (BSSN). Namun, selama tahun 2021 hasil monitoring BSSN dengan melakukan pemantauan dan indentifikasi potensi serangan siber selama 24 jam penuh setiap hari tercatat terdapat 1,6 milyar serangan siber (Kompas, 2022). Hal ini menandakan Indonesia masih termasuk ke dalam negara yang rentan akan serangan siber.

KESIMPULAN

Kemajuan teknologi informasi khususnya internet telah menciptakan 2 korelasi yaitu interdependensi dan interkoneksi yang memiliki konsekuensi yaitu *cyberwar*. *Cyberwar* sendiri merupakan ancaman masa kini dan masa depan keamanan nasional seiring dengan meningkatnya penggunaan internet dan era globalisasi. Indonesia telah memiliki strategi untuk menghadapi dan menanggulangi dampak *cyberwar* dengan membentuk kepastian hukum, aksi nyata dari tindakan teknis dan tindakan prosedural, struktur organisasi *cyber-security*, meningkatkan kapasitas sumberdaya manusia melalui *capacity building* hingga kerjasama internasional dengan berbagai forum, organisasi dan menjalin hubungan bilateral dibidang *cyber* dengan berbagai negara. Namun demikian, masih kurang efektif dan efisien karena Indonesia masih termasuk ke dalam kategori negara rentan terhadap serangan siber dengan data 1,6 milyar serangan siber selama tahun 2021.

DAFTAR PUSTAKA

Afrinata, H. (2012). *Teknologi Cyber, Cyberspace*. Diakses pada 22 November 2022, dari https://www.kompasiana.com/lamigos/557217f3307a614e38ad23ca/teknologi-cyber-cyberspace

Ardiyanti, H. (2014). Cyber-security dan Tantangan Pengembangannya Di Indonesia. *Politica*, *5*(1), 95–110.

Badri, M. (2012). *Komunikasi Militer*. Jakarta: ASPIKOM.

Bineksari, R. (2022). *Siapakah Bjorka Hacker Yang Bikin Pemerintah RI Ketar Ketir?* Diakses pada 21 November 2022, dari https://www.cnbcindonesia.com/news/20220911063631-4-371044/siapakah-bjorka-hacker-yang-bikin-pemerintah-ri-ketar-ketir/

BSSN, Badan Siber dan Sandi Negara. (2022). *Laporan Bulanan Publik Hasil Monitoring Keamanan Siber Bulan Januari - Agustus 2022*. Jakarta.

Kompas. (2021). *8 Kasus Peretasan Yang Terjadi Di Indonesia Sepanjang 2021*. Diakses pada 23 November 2022, dari https://tekno.kompas.com/read/2021/12/21/06540017/8-kasus-peretasan-yang-terjadi-di-indonesia-sepanjang-2021/

Kompas. (2022). *BSSN Sebut Ada 1,6 Milyar Serangan Siber Selama 2021*. Diakses pada 20 November 2022, dari https://www.kompas.com/nasional/read/2022/03/07/20162321/bssn-sebut-ada-16-miliar-serangan-siber-selama-2021

Permatasari, D. (2022). *Tantangan Cyber Security Di Era Revolusi Industri 4.0*. Diakses pada 22 November 2022, dari https://www.djkn.kemenkeu.go.id/kanwil-sulseltrabar/baca-artikel/14190/Tantangan-Cyber-Security-di-era-Revolusi-Industri-40.html

Sugiyono, S. (2019). *Metode Penelitian Kuantitatif, Kualitatif dan R&D*. Bandung: Penerbit Alfabet.

Tampubolon, K. E. A. (2019). Perbedaan Cyber Attack, Cybercrime, dan Cyber Warfare. *Jurist-Diction*, *2*(2), 539. https://doi.org/10.20473/jd.v2i2.14250

Yanuar, A. P. (2021). Cyber War : Ancaman Baru Keamanan Nasional dan Internasional (Cyber War : New National and International Security. *Keamanan Nasional*, *VII*(1), 23–35.