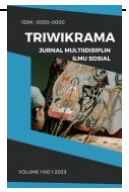
Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Vol. 9 No. 4 (2025)
E-ISSN: 2988-1986
Open Access:



PENGARUH CYBER SECURITY DALAM KAMPANYE MALWARE KOREA UTARA: KETEGANGAN KOREA UTARA DAN KOREA SELATAN

Aqila Neva Aulia[1], Wira Atman[2]

[123] Program Studi Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Hasanuddin

ARTICLE INFO

Article history:
Received Juni, 2025
Revised Juni, 2025
Accepted Juni, 2025
Available online Juni , 2025

Aqilneva15@gmail.com
wiraatman@unhas.ac.id

A B S T R A K

Penelitian ini mengkaji cyber security dalam ketegangan Korea Utara dengan Korea Selatan dalam belakangan ini, penulis menganalisa bahwa kejahatan siber termasuk dalam permasalahan keamanan dan kepentingan internasional. Penulis menggunakan metode kualitatif deskriptif melalui analisis data sekunder dari jurnal, berita, dan laporan resmi. Penelitian ini mengungkap bahwa Korea Utara telah melakukan serangan cyber kepada Korea Selatan 3 kali dalam waktu 15 Tahun yang dapat menyebabkan kerusakan khusunya di dunia digital. permintaannya. Korea Utara dapat menggunakan perang siber untuk memanfaatkan kelemahan dalam sistem musuh-musuhnya atau barang apa pun yang dapat memenuhi permintaannya. Korea Selatan merespon keadaan perang siber tidak dapat dan tidak boleh dilihat secara terpisah dari sistem keamanan yang lebih besar. Perlu digarisbawahi bahwa meskipun Korea Selatan memutuskan untuk merespons

Kata Kunci: Korea Selatan,Korea Utara, Siber

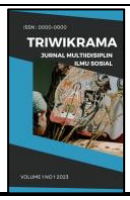
A B S T R A C T

This research examines cyber security in the recent tensions between North Korea and South Korea, the author analyses that cybercrime is included in international security and interest issues. The author uses descriptive qualitative methods through secondary data analysis from journals, news, and official reports. This research reveals that North Korea has conducted cyber attacks on South Korea 3 times within 15 years which can cause damage especially in the digital world. his request. North Korea can use cyber warfare to exploit weaknesses in its enemies' systems or any item that can fulfil its demands. South Korea's response to the state of cyber warfare cannot and should not be seen in isolation from the larger security system. It should be underlined that even if South Korea decides to respond to a cyber warfare situation, it should not be seen in isolation from the larger security system.

Keywords: *South Korea, North Korea, Cyber*

*Corresponding author
E-mail addresses: Aqilneva15@gmail.com

Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Volume 8 No 6, 2025
E-ISSN: 2988-1986
Open Access:



PENDAHULUAN

Teknologi berkembang dengan cepat setiap saat. Teknologi informasi dan komunikasi adalah salah satunya. Cara orang berperilaku di seluruh dunia dipengaruhi oleh teknologi informasi dan komunikasi ini. Selain itu, penyebaran pengetahuan yang cepat telah membuat dunia menjadi tanpa batas (Angel & Andini, 2024). Tidak diragukan lagi, kemajuan teknologi berdampak pada dunia baik positif maupun negatif. Internet memiliki pengaruh yang menguntungkan karena memungkinkan orang di seluruh dunia untuk dengan cepat dan mudah mendapatkan semua informasi yang mereka butuhkan. (Barrinha & Renard, 2017)

Ketergantungan negara-negara yang berkembang pada infrastruktur siber telah menyebabkan peningkatan bahaya siber. Menurut Heffter & Goel (2018) kemajuan siber telah memungkinkan terobosan teknologi saat ini menyentuh setiap aspek kehidupan, membuat pemerintah, individu, dan organisasi semakin bergantung pada dunia digital untuk menjalankan fungsinya sehari-hari. Pada saat yang sama, seiring dengan kemajuan inovasi siber, lingkungan bahaya tumbuh, dan dampak serangan meningkat, mulai dari kehilangan informasi hingga kerugian finansial hingga kerusakan properti dan manusia (Heffter & Goel, 2018) Mereka berpendapat bahwa negara-negara secara aktif membangun persenjataan digital mereka sebagai pengakuan atas potensi penggunaan serangan siber oleh militer, yang dapat memicu perlombaan senjata siber.

Dalam waktu belakangan ini konflik di ruang siber semakin rumit. Kim (2014) menyatakan bahwa hal ini disebabkan oleh adanya dua faktor. Aliansi negara-negara bersaing untuk mendominasi keamanan siber global: aliansi negara-negara Barat mengadvokasi internet yang lebih terbuka dan bebas, sementara aliansi yang terdiri dari Rusia, China, dan negara-negara berkembang lainnya berpendapat bahwa internet harus terstruktur, jelas didefinisikan, dan lebih dikendalikan oleh negara. Sebaliknya, Amerika Serikat dan China, dua kekuatan global dominan abad ke-21, bersaing untuk supremasi dalam keamanan siber (Kim, 2014, hlm. 346). Metode yang berbeda dalam standar teknologi, undang-undang regulasi, dan retorika keamanan siber antara kedua negara terkadang memperburuk ketegangan di antara mereka.

Di kawasan Asia Timur, kepentingan negara-negara besar secara strategis selaras. Cina, Jepang, Korea Utara, dan Korea Selatan bersaing untuk mendapatkan dominasi politik dan ekonomi di kawasan ini. Skenario ini semakin tidak jelas ketika Amerika Serikat secara aktif berpartisipasi dalam pengaturan keamanan Asia Timur. Salah satunya adalah penggunaan senjata nuklir dalam konflik Semenanjung Korea, sengketa teritorial antara Cina dan Jepang di Kepulauan Senkaku/Diaoyu dan konflik Cina dengan Taiwan, serta isu Cina dan Jepang yang memodernisasi militer dan meningkatkan anggaran pertahanan mereka. Ini adalah masalah keamanan utama di Asia Timur yang berdampak pada negara-negara di kawasan ini. Selain kekhawatiran ini, penting untuk melihat bagaimana aktor-aktor regional eksternal terutama antara Korea Utara dan Korea Selatan (Paozi, 2024).

Konflik cyber juga merujuk kepada masyarakat fanatik. Menurut sumber berita online Kpopchart.net, Kim Garam menghadapi tuduhan perundungan selama masa sekolahnya setelah debutnya sebagai anggota LE SSERAFIM. Setelah hiatus dari aktivitas grup, Hybe Labels dan Source Music secara resmi menyatakan bahwa Kim Garam telah meninggalkan grup, dan LE SSERAFIM akan melanjutkan aktivitasnya dengan lima anggota. Pengumuman ini membagi pendukung menjadi dua kubu yang berbeda. Hal itu juga terjadi dalam serangan siber yang dilakukan oleh entitas negara, termasuk serangan yang dilancarkan oleh Korea Utara terhadap Sony Pictures dan SWIFT.

Analisis jaringan menunjukkan bahwa serangan semacam itu dapat menimbulkan

Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Volume 8, Number 6 2025
E-ISSN: 2988-1986
Open Access:

konsekuensi strategis yang signifikan jika dilakukan secara luas oleh badan intelijen negara. Penelitian ini menunjukkan bahwa mengevaluasi kemampuan siber negara-negara tertentu, seperti Korea Utara, menghadapi tantangan yang signifikan karena struktur masyarakat mereka yang tertutup, yang membatasi akses terhadap informasi. Sumber dari negara pesaing, seperti Korea Selatan, seringkali tidak dapat dipercaya.

Keamanan siber sangat penting karena keamanan digital merupakan unsur esensial dari kebijakan keamanan nasional. Perang siber, yang ditunjukkan oleh serangan Korea Utara, menunjukkan bahwa keamanan digital telah beralih dari masalah sampingan menjadi komponen fundamental dari pertahanan nasional. Oleh karena itu, meningkatkan kemampuan pertahanan siber, meningkatkan kesadaran digital, dan memperkuat kerja sama internasional merupakan hal yang esensial.

Mengingat betapa rumitnya keamanan Asia Timur khusunya antara Korea Utara dan Korea Selatan serta berbagai variabel yang berkontribusi terhadapnya, tidak dapat dipungkiri bahwa kerumitan ini akan mempengaruhi bagaimana negara-negara di kawasan ini memandang dan memprioritaskan keamanan nasional. Kawasan Asia Tinur juga merupakan tempat dimana kepentingan keamanan nasional dan keamanan global bersinggungan dan dipengaruhi satu sama lain, maka tidak dapat disangkal bahwa keamanan nasional dan hubungannya dengan dinamika tatanan keamanan global dan regional saling terkait erat.

TINJAUAN PUSTAKA

A. Cyber Security

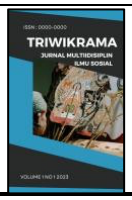
Keamanan siber adalah kegiatan yang dilakukan oleh suatu sistem atau seseorang untuk mempertahankan sistem komputer dari serangan siber yang dilakukan secara tidak sah. International Telecommucation Unit (ITU) mendefinisikan keamanan siber sebagai sebuah konsep dan strategi keamanan yang dapat digunakan untuk melindungi sumber daya organisasi nasional atau internasional (Paozi, 2024). Perlu diketahui bahwa ada tiga gagasan dalam keamanan siber:

1. **Kerahasiaan**, di mana ide ini hanya membatasi akses untuk orang-orang tertentu. Hal ini dilakukan untuk menghentikan pencurian atau kebocoran data. Elemen kunci dari konsep kerahasiaan adalah mengaktifkan autentikasi dua faktor (2FA), yang mengharuskan pengguna untuk menyelesaikan dua langkah untuk mengakses akun tertentu. Langkah-langkah ini termasuk menggunakan kata sandi dan kode khusus yang dikirim langsung ke perangkat tertentu untuk masuk.
2. **Integritas**, ide ini memberikan informasi yang akurat dan benar kepada publik. Selain itu, data pengguna harus dilindungi dari akses yang tidak sah oleh pihak ketiga.
3. **Ketersediaan**, di mana ide ini harus menjamin bahwa pengguna dapat mengoperasikan sistem dengan benar dan kesalahan sistem tidak terjadi.

Konsep keamanan siber dalam penelitian ini berfungsi sebagai landasan analisis terhadap ketegangan antara negara Korea Selatan dengan Korea Utara dengan tujuan melihat ketahanan keamanan siber di kawasan kedua negara dengan menggunakan keahlian keamanan siber dan mengintegrasikannya dengan kebutuhan dan kondisi setempat.

Tim Riset Ancaman Securonix telah menemukan kampanye yang persisten, yang diberi kode SHROUDED#SLEEP, yang diduga terkait dengan APT37 Korea Utara (kadang-kadang disebut

*Corresponding author
E-mail addresses: zukhruufii@gmail.com



sebagai Reaper atau Group123. Sel ancaman persisten yang canggih ini diyakini berasal dari Korea Utara dan menyebarkan malware tersembunyi ke target di Asia Tenggara.

APT37, berbeda dengan organisasi APT regional lain seperti Kimsuky, memiliki sejarah panjang dalam menargetkan negara-negara di luar fokus utamanya di Korea Selatan. Hal ini mencakup beberapa iklan terbaru yang menargetkan negara-negara di Asia Tenggara. Ini bukan kali pertama Korea Utara fokus di wilayah ini. Data operasional sebelumnya menunjukkan adanya malware yang serupa dengan aktivitas ini. Tampaknya aktor ancaman telah mengubah dan mempertahankan operasinya sejak identifikasi awal pada 2023, atau sebagian besar tetap tidak terdeteksi dalam aksinya sejak saat itu. Korban diduga ditargetkan menggunakan email phishing yang menyertakan lampiran berkas ZIP sebagai muatan awal. Meskipun menunjukkan semua karakteristik lampiran email phishing konvensional, tim kami tidak dapat menentukan email awal yang mengirimkan virus, hanya lampiran itu sendiri. Kamboja tampaknya menjadi fokus utama upaya ini, namun mungkin juga meluas ke negara-negara Asia Tenggara lainnya. Analisis ini didasarkan pada bahasa dan negara yang disebutkan dalam umpan phishing, serta data telemetri geografis dari sampel terkait.

Keamanan siber sangat penting karena keamanan digital merupakan unsur esensial dari kebijakan keamanan nasional. Perang siber, yang ditunjukkan oleh serangan Korea Utara, menunjukkan bahwa keamanan digital telah beralih dari masalah sampingan menjadi komponen fundamental dari pertahanan nasional. Oleh karena itu, meningkatkan kemampuan pertahanan siber, meningkatkan kesadaran digital, dan memperkuat kerja sama internasional merupakan hal yang esensial.

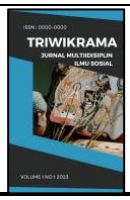
Bedasarkan kasus diatas kondisi cyber security antara korea utara dan korea Selatan dalam kampanye malware ini akan menggunakan tiga gagasan cyber security dalam hasil analisisnya dengan memperhatikan indikator gagasan kerahasiaan,integritas serta ketersediaan.

B. Perang Siber Sebagai Bentuk Peperangan Asimetris

Perang siber merupakan varian penting dari perang asimetris, karena aktor non-negara memanfaatkan teknologi untuk mengeksploitasi kelemahan pemerintah yang lebih kuat. Hal ini khususnya efektif ketika entitas yang lebih lemah menggunakan strategi yang menumbangkan sistem kekuasaan memperoleh manfaat strategis yang cukup besar meskipun sumber daya mereka terbatas. Karakteristik dunia maya, yang sangat bergantung pada infrastruktur dan sistem jaringan, menghadirkan peluang besar untuk mengganggu jaringan penting, sistem komunikasi, dan infrastruktur penting lainnya . Serangan serupa ini berupaya menimbulkan gangguan yang luas tanpa memerlukan keterlibatan militer langsung, sehingga dapat dipindahkan.

Dengan demikian, cybercalling menumbangkan konsep perang dan kekuasaan tradisional sebagaimana didefinisikan oleh Clausewitz, yang melihat perang sebagai perluasan wacana politik melalui cara lain. Perang saudara, tidak seperti peperangan konvensional yang menggunakan kekuatan militer untuk terlibat langsung dan menghancurkan lawan, menggunakan teknik non-kinetik yang dirancang untuk melemahkan komponen penting keamanan nasional sekaligus mengurangi kerusakan pada kehidupan manusia. Hal ini tidak hanya menyamakan peluang bagi entitas asimetris tetapi juga menggarisbawahi hubungan antara keterlibatan dunia militer modern

Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Volume 8, Number 6 2025
E-ISSN: 2988-1986
Open Access:



C. Penelitian Terdahulu

Pertama, Yulinda (2021) menulis penelitian berjudul Implementasi Kerangka Kerja ASEAN untuk Perlindungan Data Pribadi di Asia Tenggara 2016-2020. Jenis penelitian, jenis data, teknik pengumpulan data, teknik analisis data, dan jadwal penelitian, semuanya termasuk dalam bentuk metodologi penelitian deskriptif. Peneliti bertujuan untuk menjelaskan bagaimana ASEAN beroperasi sebagai organisasi internasional regional dalam mengimplementasikan Kerangka Kerja ASEAN tentang Perlindungan Data Pribadi untuk negara-negara anggotanya melalui berbagai upaya dan tindakan yang dilakukan oleh ASEAN dalam mempraktikkan ketiga kerangka kerja tersebut. Tiga poin implementasi tersebut adalah (1) pertukaran dan pembagian informasi; (2) lokakarya, seminar, dan kegiatan pengembangan kepribadian lainnya; dan (3) penelitian umum di bidang terkait. Perlindungan data ini akan memberikan pengaruh yang signifikan terhadap iklim investasi dan ekonomi suatu negara. Persamaan dan perbedaan penelitian ditentukan oleh metode yang digunakan dalam setiap penelitian. Peneliti sebelumnya meneliti tiga kerangka kerja perlindungan data pribadi pengguna internet di Asia Tenggara. Sementara itu, persamaannya terletak pada cara menganalisis data kerangka kerja ASEAN dengan menggunakan kerangka kerja yang mengoptimalkan keamanan data pengguna internet di Asia Tenggara.

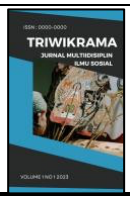
Kedua, penelitian sebelumnya, "*Cyber Diplomacy*: Kebijakan Jepang dalam Mendukung Peningkatan Kapasitas Keamanan Siber Negara-Negara ASEAN," yang ditulis oleh Fathma Ilmi Anindita Iskandar, Ferry Rustam, M. Mossadeq Bahri, dan Dhini Afiatanti. Dengan teknik pengolahan data yang berkaitan dengan kebijakan Jepang dalam menghadapi tantangan keamanan siber di kawasan ASEAN, penelitian ini menggunakan metode analisis deskriptif. Berdasarkan hasil penelitian, bantuan Jepang terhadap tantangan keamanan siber di ASEAN merupakan salah satu contoh diplomasi siber yang dilakukan untuk melindungi keamanan nasional Jepang. Topik penelitian ini berbeda dengan penelitian sebelumnya yang berkonsentrasi pada kebijakan Jepang yang mendukung pertumbuhan AJCCBC. Studi ini mencakup kegiatan kerja sama AJCCBC yang bertujuan untuk meningkatkan keamanan siber di Asia Tenggara. Penelitian ini dan penelitian sebelumnya memiliki kesamaan yaitu sama-sama menggunakan paradigma yang berfokus pada diplomasi keamanan siber dalam kaitannya dengan pertumbuhan AJCCBC.

METODE

Analisis artikel ini didasarkan pada pendekatan penelitian kualitatif deskriptif. Studi artikel ini mencakup data primer dan sekunder. Data sekunder diperoleh dari penelitian sebelumnya dan laporan media tentang subjek terkait, sedangkan data primer berasal dari publikasi atau dokumen resmi yang dikeluarkan oleh lembaga terkait. Sebuah studi komprehensif terhadap data dan informasi yang diperoleh kemudian dilakukan untuk menghasilkan temuan-temuan mengenai masalah yang diteliti (Moleong, 2014). Artikel ini menganalisis cybe security dalam ketegangan Korea Utara dengan Korea Selatan. Namun demikian, analisis ini juga tidak akan terpisahkan dari negara lain dan juga menggarisbawahi dimensi internasional. Artikel ini terutama akan membahas pentingnya *cyber security* dalam ketegangan Korea Utara dan Korea Selatan.

*Corresponding author
E-mail addresses: zukhruufii@gmail.com

Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Volume 8 No 6, 2025
E-ISSN: 2988-1986
Open Access:



HASIL DAN PEMBAHASAN

Korea Utara dan Korea Selatan telah berperang sejak lama. Korea Utara dan Selatan bersatu di bawah Dinasti Choson, yang berkuasa dari tahun 1392 hingga 1910. Pada tanggal 6 dan 9 Agustus 1945, Amerika Serikat menjatuhkan bom atom di kota Nagasaki dan Hiroshima, yang menghancurkan Jepang dan membuatnya mengakui kekalahan dalam Perang Dunia II. Jepang adalah negara terkuat di Asia pada saat itu, dan terus berkembang, bahkan merambah ke Korea. Korea adalah salah satu negara yang diduduki Jepang yang mendeklarasikan kemerdekaannya setelah Amerika Serikat dan Sekutunya mengalahkan Jepang.

Meskipun hubungan kedua negara semakin memburuk, Korea Selatan juga mengalami transisi kepemimpinan pada tahun 2022 ketika masa jabatan Moon Jae In berakhir dan Presiden Yoon Suk Yeol mulai menjabat. Yoon Suk Yeol telah berjanji untuk bertindak lebih agresif terhadap Korea Utara pada tahun 2022 dibandingkan Moon Jae In yang menurutnya kurang agresif terhadap RRDK. 19. Selain segera menanggapi provokasi yang sering dilakukan Korea Utara, Yoon Suk Yeol juga membentuk departemen baru untuk menciptakan pertahanan terhadap ancaman nuklir negara itu. Presiden Korea Selatan menyatakan bahwa negaranya sedang berdiskusi dengan Amerika Serikat mengenai kemungkinan melakukan latihan nuklir bersama untuk menanggapi ancaman dan provokasi Korea Utara.

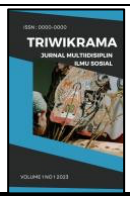
Peretas yang dipekerjakan oleh Biro Umum Pengintaian Korea Utara yang terkenal kejam berusaha menargetkan dan mencuri data dari perusahaan Korea Selatan yang terkait dengan militer, kebijakan luar negeri, dan penyatuan Semenanjung Korea pada tahun 2021, menurut laporan tahunan NCSC yang dirilis pada bulan Desember tahun itu. Serangan Ransomware terhadap infrastruktur vital dan penyedia TI diantisipasi pada tahun 2022, bersama dengan operasi canggih terhadap bisnis swasta di sektor pertahanan, perawatan kesehatan, dan sektor lainnya.

Menurut laporan tersebut, reaksi NCSC adalah meneliti serangan dan menilai manajemen keamanan informasi ratusan perusahaan Korea Selatan. Perusahaan-perusahaan ini, bersama dengan organisasi pemerintah dan sektor swasta penting lainnya, menerima intelijen ancaman siber dari pusat tersebut.

NCSC telah memberikan intelijen ancaman kepada 14 bisnis pertahanan utama sejak Oktober 2020, bersama dengan "berbagai perusahaan teknologi inti." Sistem Intelijen Ancaman Siber Nasional NCSC sekarang memiliki 351 entitas yang berpartisipasi. "Untuk menghentikan penyebaran bahaya, NCSC membagikan informasi ancaman (kode berbahaya, alamat IP, dan data komando dan kontrol) kepada entitas pemerintah dan swasta," demikian menurut studi itu. "Rapat Evaluasi Krisis Siber diadakan untuk menentukan tahap siaga krisis di sektor publik ketika kasus-kasus mendesak muncul, masalah siber global muncul, atau nilai indeks ancaman siber melebihi ambang batas.

NCSC juga berkolaborasi dengan dua tim internasional, yaitu Tim Tanggap Darurat Komputer Asia Pasifik dan Tim Forum Keamanan dan Respons Insiden, untuk memerangi ancaman siber. Selain itu, pada Juli 2021, Seoul memprakarsai program Digital New Deal untuk menciptakan infrastruktur *e-government* yang tahan terhadap serangan siber. Menurut Kementerian Ilmu Pengetahuan dan Teknologi Informasi dan Komunikasi Korea Selatan, rencana tersebut menyerukan kepada pemerintah untuk menggelar jaringan nirkabel 5G yang aman di semua gedung pemerintah dan beralih ke komputasi awan untuk sistem informasi publik pada tahun 2025.

Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Volume 8, Number 6 2025
E-ISSN: 2988-1986
Open Access:



Konflik antara kedua negara masih berlangsung sampai hingga sekarang melalui *cyber attack*. Perang siber menawarkan tantangan unik dibandingkan dengan konfrontasi kinetik (fisik), terutama dalam hal menghalangi musuh. Dalam perang asimetris, ketika perbedaan sumber daya antara dua pihak yang berlawanan terlihat jelas, perang siber memberikan keuntungan strategis tambahan yang dapat membantu pihak yang lebih lemah. Tujuan melakukan serangan siber adalah untuk mengurangi kerentanan pihak yang lebih lemah, karena serangan dapat dilakukan dengan menggunakan alat dan pola yang tidak beraturan untuk melukai lawan dan meningkatkan permainan mereka. Namun, hal ini tidak membuktikan bahwa perang siber harus dipelajari terpisah dari kerangka kerja keamanan yang lebih besar atau bahwa perang tradisional tidak lagi penting. Di sisi lain, komplikasi konflik yang lebih umum, di sisi lain, diberikan makna oleh perang siber yang hanya dapat dipahami sepenuhnya dengan menempatkannya dalam logika militer yang lebih besar.

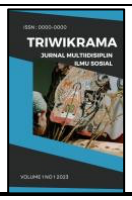
Serangan siber telah menjadi topik yang populer di kalangan akademis sejak serangan tersebut dilakukan. Ketegangan yang meningkat antara Korea Utara dan Korea Selatan terkait perang siber juga berkontribusi pada peningkatan serangan siber. Dapat diperkirakan bahwa pola yang sama akan ditemukan dalam penelitian-penelitian selanjutnya. Sebagai pemain internasional yang kontroversial dan terkenal karena sikap politiknya yang berani dan aktivitas kekuatan globalnya dalam konfigurasi keamanan internasional.

Menentukan apa yang sebenarnya merupakan perang siber tentu saja sulit karena, tidak seperti konflik (non) internasional konvensional, yang telah didefinisikan oleh hukum humaniter internasional, saat ini tidak ada instrumen hukum yang diakui secara global untuk perang siber. Akan tetapi, kurangnya standar hukum seharusnya tidak menjadi penghalang bagi diskusi yang bermanfaat tentang perang siber. Oleh karena itu, untuk memfasilitasi pemeriksaan penelitian ini, penulis akan mengacu pada penelitian ilmiah sebelumnya. Tiga faktor yang harus dipertimbangkan ketika memeriksa perang siber: 1) awal dan sumber serangan; 2) jumlah korban dan kerusakan; dan 3) kecanggihan serangan. Perang siber harus memenuhi kriteria berikut: 1) Tujuannya adalah untuk memaksa dan meyakinkan musuh untuk bekerja sama.

Berikut daftar cyber attack yang dilakukan oleh Korea Utara terhadap Korea Selatan Kim. (2014) :

Nama Serangan	Tahun	Target	Perbuatan yang dilakukan
Serangan Denial of service terhadap Korea Selatan	2011	Korea Selatan	Perusakan layanan perbankan
Serangan Denial of service terhadap Korea Selatan	2013	Korea Selatan	Perusakan layanan perbankan dan xi sabotase operasi penyiaran

*Corresponding author
E-mail addresses: zukhruufii@gmail.com



Peretasan pada Rencana Operasi 5027 (sebuah operasi militer rahasia antara Korea Selatan dan Amerika Serikat)	2016	Korea Selatan	Virus Malware, menginfeksi ribuan komputer dari komando militer siber, xii termasuk Kementrian Pertahanan.

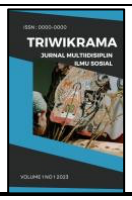
Serangan-serangan dalam tabel di atas memenuhi kriteria berikut: 1) gangguan tersebut menargetkan infrastruktur penting, menyebabkan dampak yang signifikan dan bukan dampak yang dapat diabaikan; 2) negara secara aktif dan strategis terlibat dalam serangan tersebut; 3) kemampuan siber digunakan untuk mencapai proyeksi kekuatan dan kelangsungan hidup rezim, sebuah upaya untuk menjadikan Korea Utara sebagai negara yang diakui dan kuat dalam konstelasi keamanan global, di samping kepemilikan perangkat militer lainnya, seperti enjata nuklir dan pembangunan kekuatan militer.

Dengan demikian, perang siber mirip dengan perang asimetris; tujuannya adalah untuk mengganggu infrastruktur militer dan sipil. Dengan menggunakan perang siber, Korea Utara dapat mengeksploitasi kelemahan dalam sistem musuh-musuhnya atau produk apa pun yang dapat memenuhi kebutuhannya. Dengan menggunakan perang siber, Korea Utara dapat mengeksploitasi kelemahan dalam sistem musuh-musuhnya atau produk apa pun yang dapat memenuhi kebutuhannya. Perang siber berhasil karena memungkinkan Korea Utara mendapatkan sumber daya yang diperlukan untuk kelangsungan hidup militer, cepat dan tak terduga, lebih murah daripada senjata kinetik, dan sekarang tidak dapat ditiru karena membutuhkan waktu untuk melacak pelakunya. Beberapa serangan, seperti virus ransomware WannaCry dan perampokan bank SWIFT Network, tidak hanya didorong oleh motivasi politik; mereka juga berusaha memenuhi tujuan penting lainnya, termasuk keinginan untuk mendapatkan uang dalam jumlah besar. Karena pembatasan ekonomi yang diberlakukan pada negara tersebut, Korea Utara mungkin meningkatkan operasi sibernya untuk mendapatkan uang yang dibutuhkan untuk mempertahankan kediktatorannya, yang memperparah keputusasaan ekonomi.

Korea Utara maupun Korea Selatan belum menanggapi serangkaian serangan yang dilaporkan ke Korea Utara. Jika situasi ini terus berlanjut, masuk akal untuk mengantisipasi bahwa Korea Utara akan terus menggunakan kemampuan sibernya untuk mencapai tujuannya. Hal ini memberikan nilai tambah dunia maya yang signifikan untuk mendukung tujuan militernya.

Pencegahan “terutama berkaitan dengan pesan, atau kemampuan yang secara jelas mengkomunikasikan batasan dan konsekuensi,” menurut Buchanan dan Libicky. Ungkapan “jika Anda melakukan satu hal, saya akan melakukan hal lain sebagai balasannya” merangkum pencegahan. Sebagai hasilnya, jelas terlihat seberapa besar serangan, misalnya, yang dapat diterima dan apa yang akan terjadi jika suatu bahaya dinilai telah melampaui batas-batas tersebut. Ada empat faktor penting yang perlu dipertimbangkan dalam menciptakan pencegahan yang efektif: 3) kredibilitas (kemungkinan negara untuk melakukan pembalasan); 2) ambang batas (secara teratur membedakan antara tindakan yang memerlukan pembalasan dan tindakan yang tidak memerlukan pembalasan); 4) kapasitas (negara harus dapat merespons secara tepat); dan 5) atribusi (identifikasi untuk menelusuri motivasi dan identitas penyerang).

Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Volume 8, Number 6 2025
E-ISSN: 2988-1986
Open Access:



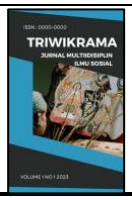
Penangkalan yang efektif mengabaikan analisis biaya-manfaat dari serangan siber Korea Utara karena mengabaikan legitimasi dan kemampuan respons Korea Selatan/ Pertama, kemampuan Korea Selatan untuk membalas di dunia maya dipertanyakan. Korea Utara mengklaim bahwa karena tidak ada cukup banyak situs web yang memiliki dampak signifikan terhadap pihak Korea Utara, maka target-targetnya tidak akan mengambil risiko pembalasan. Infrastruktur dan masyarakat Korea Utara yang terisolasi di dunia maya tentu saja berbeda dengan Korea Selatan, yang memiliki jaringan yang luas dan bergantung pada ruang digital. Pada kenyataannya, pertahanan siber Korea Selatan jauh lebih kuat daripada Korea Utara. Mengingat kompleksitas ruang siber dan bahaya serta kelemahannya yang terus berubah, mereka akan lebih baik membiarkan Korea Utara lolos dalam perang siber, yang mungkin menjadi bumerang karena dapat mengakibatkan kerusakan tambahan yang lebih besar bagi Korea Selatan.

Kedua, karena tidak ada kerangka kerja yang diakui secara global atau seperangkat kriteria yang dapat diterima, Korea Utara didorong untuk percaya bahwa menyerang lebih baik daripada diserang. Mengapa norma dan kerangka kerja internasional penting dalam konteks perang siber? Sistem internasional membantu memprediksi maksud dan kemungkinan tindakan negara lain; sistem ini memberikan tingkat kepastian yang lebih tinggi dalam memprediksi tindakan negara lain, selain membatasi ruang lingkup konflik atau mengatur perilaku negara. Akibatnya, ketiadaan rezim seperti itu dipandang sebagai keadaan ambiguitas dalam memprediksi tindakan negara lain. Karena hal itu memberikan keuntungan yang lebih besar bagi Korea Utara daripada berdiam diri, maka Korea Utara membentuk pemikirannya dengan cara ini: menyerang lebih baik daripada diserang.

Orang mungkin berpendapat bahwa karena perang siber bukanlah satu-satunya senjata yang tersedia bagi mereka,dan Korea Selatan tidak perlu bereaksi di dunia maya. Mereka mungkin, pada kenyataannya, menggunakan senjata konvensional, yang akan membuat postur militer Korea Utara menjadi lebih lemah. Namun, alasan ini mendukung poin pertama, yaitu bahwa perang siber tidak dapat dan tidak boleh dilihat secara terpisah dari sistem keamanan yang lebih besar. Perlu digarisbawahi bahwa meskipun Korea Selatan memutuskan untuk merespons, Korea Utara memiliki jaring pengaman dalam bentuk senjata nuklirnya. Terlepas dari manfaatnya, perang siber tidak ada gunanya jika digunakan sebagai taktik militer yang berdiri sendiri. Data empiris terbaru mendukung klaim kami bahwa negara-negara yang memiliki senjata nuklir jauh lebih mungkin untuk meluncurkan dan berpartisipasi dalam serangan siber:

*Corresponding author
E-mail addresses: zukhruufii@gmail.com

Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Volume 8 No 6, 2025
E-ISSN: 2988-1986
Open Access:

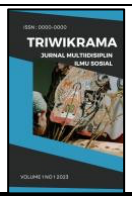


SIMPULAN

Tinggal di negara dengan teknologi dan konektivitas internet yang canggih memiliki konsekuensi. Negara-negara ini dapat menjadi ancaman karena dapat membuka celah yang lebih luas untuk dieksploitasi oleh musuh. Menurut contoh sebelumnya, pemerintah target serangan siber Korea Utara dan Korea Selatan, telah menunjukkan keengganan untuk menyatakan perang terhadap serangan siber karena mereka takut kerusakan yang terjadi di negara mereka sendiri akan bertambah. Karena mereka tidak dapat meramalkan aktivitas pihak lawan di masa depan karena kurangnya kerangka kerja dan standar internasional bersama tentang perang siber, serangan siber, dan kejadian serupa lainnya, pihak yang menyerang, Korea Utara, memutuskan bahwa yang terbaik adalah menyerang selagi masih memungkinkan. Dalam upaya untuk meningkatkan keamanan siber, negara-negara lain juga harus mengambil langkah untuk menetapkan standar serangan siber atau sikap terhadap situasi berisiko yang memerlukan pembalasan. Jika hal ini tidak dilakukan, ketidakpastian situasi yang ada akan memungkinkan penyerang untuk terus menikmati hak-hak hukum yang memungkinkan mereka untuk melakukan kejahatan tanpa dimintai pertanggungjawaban. Menetapkan ambang batas yang lebih akurat akan memberikan dasar yang kuat untuk melindungi dunia digital.

.

Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Volume 8, Number 6 2025
E-ISSN: 2988-1986
Open Access:



DAFTAR PUSTAKA

Angel, A., & Andini, E. M. S. (2024). ANALISIS PENGIMPLEMENTASIAN "ASEAN CYBER SECURITY FRAMEWORK" DI SINGAPURA TAHUN 2020. *Journal of Social and Economics Research*, *6*(1), 2168–2179. https://doi.org/10.54783/jser.v6i1.587

Barrinha, A., & Renard, T. (2017). Cyber-diplomacy: the making of an international society in the digital age. *Global Affairs*, *3*(4–5), 353–364. https://doi.org/10.1080/23340460.2017.1414924

Heffter, A., & Goel, S. (2018). Mitigating Cyber Warfare through Deterrence and Diplomacy. *The 13th Pre-ICIS Workshop on Information Security and Privacy*.

Kim. (2014). Cyber Security and Middle Power Diplomacy: A Network Perspective. *The Korean Journal of International Studie*, *12*(2).

Moleong. (2014). *Metode Penelitian Kualitatif*. Remaja Rosdakarya.

Paozi, A. (2024). Perubahan Kebijakan Jepang Dalam Bidang Pertahanan dan Implikasinya Terhadap Keamanan Kawasan Asia Timur. *Universita Mataram Repository*.

Yulinda, L. P. (2021). *Implementasi Kerangka Kerja ASEAN Dalam Perlindungan Data Pribadi dI Asia Tenggara 2016-2020*. Universita Pembangunan Nasional "Veteran" Jaka

*Corresponding author
E-mail addresses: zukhruufii@gmail.com

Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Volume 8 No 6, 2025
E-ISSN: 2988-1986
Open Access: