Jurnal IPTEK-KOM (Jurnal Ilmu Pengetahuan dan Teknologi Komunikasi) eISSN 2527 - 4902
Vol. 24 No. 2, Desember 2022, 135 - 146

Memahami Perang Siber Rusia dan Peran Badan Intelijen Negara dalam Menangkal Ancaman Siber

Understanding Russian Cyber Warfare and the Role of the State Intelligence Agency in Countering Cyber Threats

M. Yusuf Samad[1], Pratama Dahlian Persadha[2]
[1,2]Communication & Information System Security Research Center (CISSReC),
Jl. Moh. Kahfi 1 No. 88D Jagakarsa, Jakarta Selatan, DKI Jakarta, Indonesia
[1]ahmadyusad@gmail.com, [2]pratama@cissrec.org.

Naskah diterima: 28 Oktober 2022 , direvisi: 12 November 2022, disetujui: 23 Desember 2022

Abstract

Cyber attacks that target a country have occurred in Georgia, Estonia and Ukraine, these attacks were able to paralyze vital infrastructure in both countries. Similar attacks have the potential to occur in Indonesia, so it is necessary to understand the mechanism of cyber attacks and how to prevent them. This study uses a qualitative approach with the aim of understanding cyber attacks through the Russian cyber war against Estonia, Georgia, and Ukraine. In addition, this study also aims to understand the role of the State Intelligence Agency in countering cyber threats in Indonesia. The findings of this study are cyber attacks against Giorgia, Estonia and Ukraine through each stage of Cyber Early Warning. In preventing similar attacks, BIN plays a role in preventing cyber attacks by coordinating intelligence, cyber patrols and security assessments.

Keywords: *cyber war, State Intelligence Service, cyber threat*

Abstrak

Serangan siber yang mengarah pada suatu negara telah terjadi di Georgia, Estonia dan Ukraina, serangan tersebut mampu melumpuhkan infrastruktur vital pada kedua negara. Serangan serupa berpotensi terjadi di Indonesia sehingga perlu dipahami bagaimana mekanisme serangan siber dan cara mencegahnya. Penelitian ini menggunakan pendekatan kualitatif dengan tujuan penelitian untuk memahami serangan siber melalui perang siber Rusia terhadap Estonia, Georgia dan Ukraina. Selain itu, penelitian ini juga bertujuan untuk memahami peran Badan Intelijen Negara dalam menangkal ancaman siber di Indonesia. Temuan penelitian ini adalah serangan siber terhadap Giorgia, Estonia, dan Ukraina melalui setiap tahapan pada Cyber Early Warning. Dalam mencegah serangan serupa, BIN berperan menangkal serangan siber dengan cara melakukan koordinasi intelijen, patroli siber dan Security Assessment.

Kata kunci: *perang siber, Badan Intelijen Negara, ancaman siber*

PENDAHULUAN

Perkembangan zaman dari tahun ke tahun terus mengalami perubahan dan hal tersebut juga mempengaruhi tren perang yang terjadi hingga saat ini. Dahulu, perang nuklir Perang Dingin membuat Departemen Pertahanan Amerika Serikat (AS) khawatir akan terjadinya perang nuklir

sehingga memicu dimulainya riset untuk mengubungkan berbagai komputer departemen pertahanan dalam satu instalasi, yang diharapkan dapat saling berkomunikasi dan bertahan jika perang benar-benar terjadi. Para peneliti dan teknisi melakukan riset dan akhirnya menemukan internet yang dapat dijadikan wadah komunikasi dan mengakses data yang diperlukan (Ningsih 2022). Tren perang bergeser dengan mengoptimalkan pemanfaatan ilmu pengetahuan dan teknologi (IPTEK) sehingga perang sebelumnya atau perang konvensional antarnegara hampir tidak lagi ditemukan, tetapi perang yang lebih dominan ditemukan adalah perang siber atau *cyber war*. Keamanan siber menjadi penting karena tidak ada batas kedaulatan dalam siber, serta konflik yang lebih banyak dipelopori oleh aktor nonnegara (Pratiwi 2019).

Setiap negara akan bekerja sama atau berkompetisi dalam memperebutkan sesuatu misalnya wilayah, energi atau lainnya. Bahkan, sejumlah negara menyatakan secara terbuka bahwa mendukung salah satu negara dalam menghadapi serangan siber negara lawan (Suryakusumah 2022). Saat ini *cyber attack* atau serangan siber menjadi metode mutakhir untuk berkompetisi bahkan mengarahkan serangan pada pertahanan suatu negara. Serangan ini merujuk pada pemanfaatan kegiatan yang disengaja untuk mengganggu, mengubah, menurunkan, menipu, atau merusak sistem jaringan/komputer yang digunakan oleh lawan atau informasi dan/atau program penduduk (Lin 2012). Permasalahan timbul tatkala serangan siber mulai dianggap dapat memberikan manfaat militer dan diselaraskan dengan sengketa menggunakan senjata (Yuliantiningsih 2021). Permasalahan tersebut menimbulkan ketegagan laten atau *latent tensions*, kemudian setiap negara melakukan upaya untuk mengumpulkan berbagai macam informasi mengenai lawan (*Cyber Recon*). Tahapan berikutnya, *Initiating Event*, yaitu menyiapkan berbagai macam peralatan, pasukan, metode dan membangun strategi, teknik dan taktik dalam melakukan serangan. Selanjutnya, melakukan mobilisasi siber (*Cyber Mobilization*) dan tahap terakhir adalah bagaimana cara memulai sebuah penyerangan dengan melakukan serangan siber atau *cyber attack* pada infrastruktur siber (rumah sakit, infrastruktur penerbangan, infrastruktur energi, dll) dalam konteks *cyber war*. Kelima tahap tersebut disebut dengan *Cyber Early Warning Model* (Carr 2012).

Berdasarkan Laporan Tahunan Monitoring Keamanan Siber 2021, Badan Siber dan Sandi Negara (BSSN) mencatat sebanyak 1.637.973.022 trafik anomali dengan trafik tertinggi pada Desember sebanyak 242.066.168 anomali, sebanyak 264 kasus *phishing,* sebanyak 5.940 kasus *web defacement* dengan kasus terbanyak terjadi pada Maret yang mencapai 727 kasus, dan sebanyak 1.676.286 aktivitas *Advanced Persistent Threat* (APT) di Indonesia (Direktorat Operasi Keamanan Siber 2021).

Sejak tahun 2019, Kementerian Komunikasi dan Informatika (Kominfo) mencatat sebanyak 29 lembaga dan perusahaan yang menjadi korban kejahatan siber berupa kebocoran data, termasuk diantaranya Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan. Dari puluhan kasus tersebut, 21 kasus diantaranya telah diselesaikan oleh Kominfo. Data Kominfo menunjukkan bahwa 29 kasus kebocoran data disebabkan oleh sistem keamanan yang rawan diretas dan kurangnya integritas Sumber Daya Manusia (SDM) sehingga bekerja sama dengan pelaku peretasan (Burhan 2021).

Kementerian Kominfo telah melakukan berbagai upaya dalam menyikapi kasus dugaan kebocoran data BPJS Kesehatan. Dalam siaran pers Kementerian Kominfo, dijelaskan bahwa Kementerian Kominfo telah melakukan investigasi terhadap 1 juta data sampel yang diklaim oleh pelaku dan hasilnya menunjukkan bahwa sampel data diduga kuat identik dengan data yang dimiliki oleh BPJS Kesehatan karena data yang ada berupa data Noka (Nomor Kartu), Kode Kantor, Data Keluarga/Data Tanggungan, dan status Pembayaran (Permadi 2021). Selain kasus di BPJS

Kesehatan, kasus kebocoran data juga terjadi pada data Daftar Pemilih Tetap (DPT) tahun 2014 yang memuat data pribadi seperti nomor kartu keluarga, nama lengkap, Nomor Induk Kependudukan (NIK), alamat rumah, tempat dan tanggal lahir, dan lain-lain. Komisioner Komisi Pemilihan Umum (KPU) Viryan Aziz mengakui bahwa sebanyak 2,3 juta data yang telah dicuri adalah data DPT Pemilu 2014 yang berformat PDF (Setiawan 2020). Berdasarkan pernyataan Ketua Tim Tata Kelola Pelindungan Data Pribadi Kementerian Kominfo, Hendri Sasmita Yuda menegaskan bahwa data pribadi tidak hanya berkaitan dengan keamanan, tetapi juga pemenuhan hak-hak proporsionalitas untuk mewujudkan tata kelola perlindungan data pribadi (Andreya 2022).

Bentuk serangan siber lainnya juga pernah terjadi pada sejumlah instansi pemerintah, seperti *web defacement* atau pengubahan tampilan halaman situs web tanpa diketahui pemilik sah. Serangan *web defacement* terjadi pada situs web Dewan Perwakilan Rakyat (DPR), kejadian tersebut bertepatan dengan aksi protes tentang Omnibus Law Undang-Undang Cipta Kerja, peretas menyampaikan aspirasinya melalui *web defacement* dengan mengubah tulisan "Dewan Perwakilan Rakyat" menjadi "Dewan Penghianat Rakyat (Persadha 2020). Beragam serangan siber terjadi di Indonesia, tidak hanya menargetkan instansi pemerintah tetapi juga pejabat pemerintah, salah satunya serangan siber yang kemungkinan besar menargetkan para pejabat Badan Usaha Milik Negara (BUMN) dan kementerian. Serangan siber tersebut sangat mungkin merupakan bagian dari operasi intelijen (Persadha 2021).

Perkembangan ancaman siber telah mengalami peningkatan yang pesat sekali dengan aktor siapa saja baik negara maupun nonnegara. Di sisi lain, Indonesia masuk dalam kategori negara yang sangat rentan dan menjadi target paling potensial dalam lingkup Asia. Instrusi ancaman siber yang sangat hebat sudah pernah terjadi, seperti pencurian data dan penyalahgunaan sistem informasi milik pemerintah dan swasta yang bersifat destruktif. Ancaman siber menjadi alternatif karena keunggulannya yang tidak perlu mengeluarkan biaya besar, minim penggunaan personel, anonim, dan mampu dikendalikan dari lokasi berbeda hingga lintas negara dan benua (Suratman 2017).

Eksistensi serangan siber semakin jelas yang dibuktikan dengan keterlibatan negara secara aktif dalam serangan siber. Menyikapi hal tersebut, Indonesia harus aktif dalam melakukan pemetaan terhadap setiap potensi serangan siber dalam rangka menjaga keamanan dan ketahanan nasional, mengingat efek dari perang siber sangat jelas dan bersentuhan langsung dengan kehidupan masyarakat. Serangan siber dapat merusak data konsumen, memadamkan listrik dan saluran air sebuah kota, menimbulkan kericuhan, bahkan memantik munculnya hal-hal yang mengganggu stabilitas nasional (Rofii 2018).

Berdasarkan sejumlah fakta diatas, tulisan ini memberikan gambaran tentang ancaman keamanan nasional di bidang siber dengan memaparkan serangan siber oleh Rusia ke beberapa negara. Rusia merupakan negara penyumbang sebagian besar atau 58 persen peretasan yang disponsori negara selama periode Juli 2020 hingga Juni 2021, serangan yang bersumber dari Rusia mengalami peningkatan efektivitas dari 21 persen menjadi 32 persen (Microsoft 2021). Rusia juga memiliki potensi besar dalam hal perang siber dan beberapa peristiwa membuktikannya, seperti Rusia menggunakan senjata siber melawan Georgia selama perang 2008. Rusia telah berhasil mengadaptasi serangan siber untuk memperluas kepentingannya. Salah satu serangan siber tahun 2007 adalah serangan yang menargetkan Estonia yang berupa serangan DDoS. Hal yang sama terjadi pada tahun 2008 selama perang Rusia-Georgia dan Rusia-Ukraina, serangan siber yang dilakukan oleh Rusia lebih mutakhir dan destruktif (Guchua, Zedelashvili, and Giorgadze 2022). Di tahun 2022, Rusia kembali melakukan serangan siber terhadap Ukraina sebagai bagian dari invasi yang dilakukan Rusia ke Ukraina (Priyono 2022). Selain itu, tulisan ini juga menjabarkan bagaimana

peran Badan Intelijen Negara (BIN) sebagai salah satu aktor keamanan negara dalam menangkal ancaman serangan siber di Indonesia.

METODE

Penelitian ini merupakan penelitian kualitatif, yaitu suatu penelitian yang pada dasarnya menggunakan pendekatan deduktif-induktif. Analisis data dalam penelitian kualitatif dilakukan selama proses dan akhir pengumpulan data. Dalam penelitian kualitatif, teknik analisis data lebih banyak dilakukan bersamaan dengan pengumpulan data (Hardani, et al. 2020). Penulis menggunakan pendekatan deskriptif kualitatif dengan memaparkan hasil-hasil penelitian sebelumnya kemudian disandingkan dengan teori atau konsep yang disajikan, yakni *Cyber Early Warning Model*. Hasil penelitian diperoleh dari sumber seperti internet/berita, jurnal, buku, dan sumber lainnya. Penelitian deskriptif adalah studi yang menggunakan data untuk memberikan solusi terhadap suatu permasalahan. Dalam penelitian ini, proses analisis memerlukan penyajian, evaluasi, dan interpretasi data (Narbuko and Achmadi 2015). Penelitian ini menggunakan studi kasus serangan siber Rusia ke beberapa negara dengan menggunakan *Cyber Early Warning Model* sebagai acuan kemudian memahami dan menjelaskan pola atau kesamaan dari serangan siber tersebut.

HASIL DAN PEMBAHASAN

Rusia vs Estonia Tahun 2007

Kasus kedua negara tersebut dimulai pada 30 April 2007, ketika pemerintah Estonia memindahkan sebuah patung Stalin atau patung perunggu (*Bronze Statue*) dari dari distrik Kota Tua ibu kota ke pemakaman militer. Pergerakan patung ini memicu ketegangan antara warga sipil Estonia dan minoritas Rusia. Bagi warga sipil Estonia, patung tersebut mewakili penindasan Rusia terhadap Estonia, sedangkan bagi minoritas Rusia, pergerakan patung ke pinggiran Tallinn mewakili marginalisasi etnis mereka, ketegangan kemudian diikuti oleh protes besar-besaran di depan Duta Besar Estonia di Rusia oleh *Nashi Youth Group* (Herzog 2011). Perpindahan monumen menyebabkan meningkatnya perlawanan terhadap pemerintah Estonia oleh mereka yang membenci tindakan tersebut sehingga para penyerang meningkatkan keinginan mereka untuk menyerang Estonia. Banyaknya peringatan tentang pergerakan monumen, para penyerang memiliki waktu sekitar enam bulan untuk merencanakan serangan mereka sebagai protes atas peristiwa tersebut. Para penyerang mempersiapkan serangan siber dan kerusuhan, serta memastikannya melalui proses perencanaan bahwa ada penyangkalan yang masuk akal tentang partisipasi penyerang dalam kedua jenis serangan (T. M. K. Roeder et al. 2016).

Nashi Youth Group melakukan serangan siber dengan menggunakan *Distributed-Denial of Service* (DDoS). Serangan siber mulai terstruktur dengan sangat baik, pada tanggal 27 April 2007, dengan menargetkan beberapa situs penting seperti situs presiden, parlemen Estonia, Kepolisian Estonia, Partai Politik, dan media massa yang sangat berpengaruh. Selain itu, email parlemen dinonaktifkan karena serangan siber. Pada tanggal 4 Mei 2007, serangan siber menargetkan sektor perbankan dengan cara yang lebih koordinatif dari sebelumnya, seperti Bank Hansa dan merusak Anjungan Tunai Mandiri (ATM) dan membuat mereka merugi 1.000.000 $USD. Kemudian serangan siber memuncak pada 9 Mei 2007, bersamaan dengan Hari Kemerdekaan Federasi Rusia untuk memperingati kemenangan mereka atas Nazi dalam Perang Patriotik Hebat (NATO StratCom COE, n.d.). Waktu dan koordinasi yang jelas dari serangan siber dan kerusuhan menunjukkan bahwa mereka sangat terorganisir (Tikk, Kaska, and Vihul 2010). Selama serangan siber di Estonia, forum berbahasa Rusia menyediakan pembaruan berita dan tempat perekrutan bagi peretas yang

eISSN 2527 - 4902

tertarik. Hal ini menunjukkan bahwa teknologi digital memungkinkan mobilisasi transnasional yang cepat di saat krisis. Di sisi lain, ada forum bahasa Rusia dengan alat yang diunduh dan instruksi bagaimana melakukan serangan siber (Kozlowski 2013).

Berdasarkan model *Cyber Early Warning* yang dikaitkan dengan perang Rusia vs Estonia*, latent tensions* kedua negara tersebut berupa perpindahan patung Stalin dan rentetannya, kemudian *cyber recon* dengan mengumpulkan informasi melalui forum online dan *initiating event* ditunjukkan dengan adanya persiapan yang dilakukan selama kurang lebih enam bulan. Dalam hal ini, penulis menilai bahwa penyerang terlebih dahulu mencari informasi mengenai target/lawan (Estonia) baik itu melalui grup *online*/forum khusus maupun cara lainnya, kemudian merencanakan serangan DDoS. Untuk memasifkan serangan dan memaksimalkan dampak yang ditimbulkan dari serangan tersebut, penyerang melakukan *cyber mobilization* dengan cara menyediakan tempat perekrutan bagi peretas yang tertarik serta alat khusus dan instruksi melakukan serangan siber.

Gambar 1. Model *Cyber Early Warning* pada Kasus Rusia vs Ukraina (diolah oleh penulis, 2022)

Rusia vs Georgia Tahun 2008

Konflik Rusia vs Georgia adalah salah satu sampel dari serangan siber yang bersamaan dengan invasi suatu negara ke negara lain melalui laut, darat, dan udara. Invasi Rusia dilatarbelakangi oleh serangan Georgia terhadap separatis di Ossetia Selatan (Hollis 2011). Rusia intervensi militer terhadap Georgia dikarenakan Georgia telah melakukan serangan terhadap Ossetia Selatan (Yuliantiningsih 2021). Selain itu, kampanye siber yang dikendalikan dengan baik dengan menargetkan situs web strategis milik pemerintah Georgia termasuk kedutaan Amerika Serikat dan Inggris dengan menggunakan serangan *Distributed Denial of Service (DDoS), SQL injection, dan cross scripting* (XSS)22 (Carr 2012).

Serangan siber pertama terjadi beberapa bulan sebelum pecahnya perang. Pada 19 Juli, Firma keamanan menginformasikan tentang DDoS terhadap situs-situs web Georgia. Skenario serupa dengan serangan dalam skala lebih besar terulang pada 8 Agustus dan bertepatan dengan pasukan Rusia memasuki Ossetia Selatan. Serangan yang dilakukan oleh peretas Rusia dapat dibagi menjadi dua fase. Pada tahap pertama, peretas menyerang terutama pada berita Georgia dan situs web pemerintah. Rusia menggunakan robot berupa *botnet* untuk melakukan serangan DDoS yang brutal. Pada fase kedua serangan siber, daftar target mencakup lembaga keuangan, bisnis, lembaga pendidikan, media, dan situs web peretas Georgia. Selain serangan DDoS, ada juga operasi perusakan situs web yang dilakukan dengan menggunakan injeksi SQL29 dan *spamming* besar-besaran pada email publik. Selama fase kedua operasi, banyak peretas patriotik bergabung dalam kampanye melawan Georgia (Kozlowski 2013).

Pada dasarnya, serangan terjadi beberapa minggu sebelum 'intervensi' yang sebenarnya dilakukan pada situs web Presiden Georgia berupa serangan DDoS dari peretas Rusia. Sebelumnya telah terjadi diskusi aktif di seluruh web Rusia tentang apakah serangan DDoS dan perusakan situs web harus dilakukan atau tidak. Setelah konflik Rusia-Georgia, spekulasi selama seminggu di sekitar forum dalam jaringan (*online*) Rusia akhirnya membuat serangan siber Rusia vs Georgia terwujud menjadi serangan siber terkoordinasi terhadap infrastruktur internet Georgia. Serangan

telah berhasil mengompromikan beberapa situs web pemerintah dengan melanjutkan serangan DDoS terhadap banyak situs pemerintah Georgia lainnya (Danchev 2008).

Situs web Rusia, ruang obrolan, dan jaringan juga membahas serangan yang akan datang selama beberapa minggu ke depan. Diduga penyerang Rusia melakukan gladi bersih untuk serangan siber. Pakar Internet di Amerika Serikat mengatakan serangan terhadap infrastruktur internet Georgia dimulai pada 20 Juli dengan serangan DDOS dan secara efektif mematikan peladen Georgia. Salah satu aspek menarik dari serangan siber di Georgia adalah persiapan perangkat siber, instruksi, situs web khusus untuk melakukan serangan. Hal ini dapat menunjukkan bahwa Rusia mempersiapkan perang siber untuk waktu yang lebih lama karena akses ke alat yang tersedia untuk orang Rusia dan petunjuk cara menggunakannya tidak dapat disiapkan dalam satu hari. Serangan tersebut berasal dari wilayah Rusia dan merupakan gabungan dari tindakan profesional yang dilakukan dengan menggunakan *botnet* dan serangan yang dilakukan oleh peretas patriotik yang sama seperti dalam kasus Estonia dapat menemukan informasi dan program di forum khusus. Pada forum itu, terdapat daftar target yang diprioritaskan dan informasi tentang potensi kerentanan dan cara menghindari *firewall* Georgia pada koneksi Internet dari Rusia. Pusat dari kampanye informasi ini adalah situs StopGeorgia.ru yang didalamnya tersedia alat untuk melakukan serangan DDoS yang dapat digunakan oleh para amatir. (Kozlowski 2013).

Jika model *Cyber Early Warning* dikaitkan dengan perang Rusia vs Georgia, maka *latent tensions* pada perang tersebut berupa adanya serangan Georgia terhadap Ossetia Selatan. *Cyber recon* dilakukan dengan cara mencari informasi di situs web Rusia, ruang obrolan atau forum online seperti informasi tentang daftar target prioritas dan informasi tentang potensi kerentanan, kemudian *initiating event* dilakukan dengan cara persiapan yang matang dan adanya serangan awal atau gladi bersih beberapa waktu sebelum serangan utama dilancarkan, sedangkan *Cyber Mobilization* dilakukan dengan kampanye pada situs StopGeorgia.ru yang menyebabkan adanya keterlibatan pihak lain dalam melakukan serangan DDoS, seperti banyaknya peretas patriotik bergabung dalam kampanye melawan Georgia.

Gambar 2. Model *Cyber Early Warning* pada Kasus Rusia vs Ukraina (diolah oleh penulis, 2022)

Rusia vs Ukraina 2022

Ketegangan Rusia dan Ukraina semakin bergejolak pasca Rusia menginvasi Ukraina pada Februari 2022. Perselisihan antara kedua negara pada dasarnya bukan konflik yang baru karena perselisihan kedua negara mulai dari yang kecil hingga besar beberapa kali setelah Uni Soviet runtuh dan kedua negara menjadi negara merdeka. Sejumlah permasalahan perbatasan seperti serangan siber Rusia ke Ukraina, gerakan-gerakan separatis, hingga aneksasi Rusia atas wilayah Krimea merupakan beberapa permasalahan yang terjadi diantara kedua negara (Najmi and Lestiyaningsih 2022). Selain itu, konflik yang sedang berkembang di Ukraina saat ini merupakan sebuah gejala geopolitik yang dipicu terutama oleh Barat dibawah kendali North Atlantic Treaty Organization/NATO (Ornay and Azizah 2022).

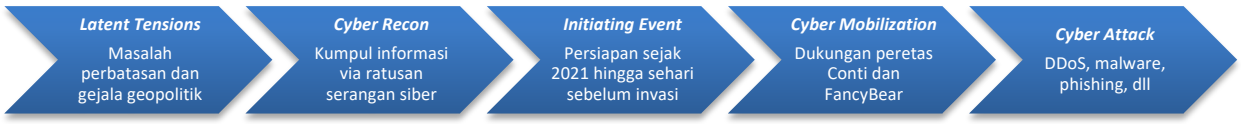
Rusia meluncurkan kampanye siber yang luas sesaat sebelum invasi, sejumlah laporan menunjukkan peningkatan besar dalam eksploitasi pada hari pertama dengan tujuan untuk menciptakan kekacauan dan mengganggu pertahanan Ukraina. Rusia berusaha untuk

mengganggu layanan dan memasang malware yang merusak di jaringan Ukraina termasuk phishing, dan memanfaatkan kerentanan perangkat lunak (Lewis 2022). Laporan Microsoft tentang Laporan Khusus Ukraina mencatat bahwa sejak invasi, beberapa kelompok peretas yang terhubung dengan Rusia melakukan ratusan serangan siber terhadap Ukraina. Kelompok peretas memulai persiapan peretasan pada Maret 2021, sekitar satu tahun sebelum Presiden Rusia menyerang Ukraina. Sehari sebelum invasi militer, operator yang terkait dengan lembaga intelijen militer Rusia, meluncurkan serangan yang mampu merusak ratusan sistem di pemerintahan Ukraina, TI, energi, dan organisasi keuangan. Sejak itu, aktivitas berupa menghancurkan, mengganggu, atau menyusup ke jaringan lembaga pemerintah dan berbagai organisasi infrastruktur vital, yang dalam beberapa kasus menjadi sasaran pasukan militer Rusia dengan serangan darat dan serangan rudal. Serangan siber ini kadang-kadang tidak hanya menurunkan fungsi organisasi yang ditargetkan, tetapi juga berusaha mengganggu akses warga ke informasi penting dan layanan masyarakat, serta bertujuan untuk menurunkan kepercayaan masyarakat kepada pemerintah (Microsoft 2022).

Berdasarkan data dari badan pertahanan dan keamanan siber Ukraina, *State Service of Special Communications and Information Protection* (SSSCIP), tercatat bahwa sejak dimulainya invasi Rusia ke Ukraina, sebanyak 796 serangan siber menargetkan pemerintah Ukraina dan organisasi sektor swasta. Sejumlah sektor industri yang paling terdampak oleh serangan siber Rusia diantaranya sektor energi, telekomunikasi, keuangan, dan infrastruktur. Mayoritas serangan yang teridentifikasi oleh SSSCIP difokuskan pada pengumpulan informasi (242 insiden), dan sisanya bertujuan untuk merusak sistem yang ditarget menggunakan malware. Data SSCIP sesuai dengan laporan Microsoft terkait skala serangan siber yang didukung Rusia terhadap Ukraina sejak invasi Februari. Salah satu temuannya adalah Microsoft Threat Intelligence Center (MSTIC) mendeteksi upaya penyusupan jaringan Rusia pada 128 target di 42 negara di luar Ukraina, Sebagian besar serangan ini terutama difokuskan pada pengumpulan informasi sensitif dari lembaga pemerintah di negara-negara dengan peran penting dalam respon NATO dan Barat terhadap perang Rusia (Gatlan 2022).

Rusia mendapat dukungan dari kelompok peretas Conti yang akan melakukan serangan terhadap musuh-musuh Rusia. Berdasarkan *chat* atau percakapan yang bocor, kelompok ini memiliki rantai komando yang terhubung dengan Pemerintah Rusia. Laman Heimdal Security mengatakan Conti Ransomware berbasis di Rusia dengan nama samaran Wizard Spider. Peretas ini disebut sebagai aktor jahat yang destruktif karena kemampuan mengenkripsi data dan menyebar ke sistem lain secara cepat (Roy 2022). Selain itu, Google Alphabet Inc mendeteksi peretas Rusia yang terkenal dengan penegakan hukum, termasuk FancyBear, berperan dalam kampanye *phishing*, spionase, dan serangan lain yang menyasar pada Ukraina dan sekutunya (Setyowati 2022).

Dalam perspektif model *Cyber Early Warning* yang disandingkan dengan perang siber Rusia vs Ukraina, maka terlihat bahwa Rusia masih menggunakan pola yang sama ketika melakukan serangan siber terhadap Estonia dan Georgia pada beberapa tahun silam. Pada tahap *latent tensions,* masalah yang muncul adalah masalah perbatasan dan gejala geopolitik akibat intervensi NATO. Selanjutnya, tahap *cyber recon* dilakukan dengan cara mengumpukan informasi melalui serangan siber yang mencapai ratusan serangan. Lalu pada tahap *initiating event* dilakukan dengan cara persiapan cukup panjang hampir satu tahun sebelum invasi Rusia ke Ukraina. Tahap selanjutnya adalah tahap *cyber mobilization* dengan cara memperoleh dukungan dari kelompok peretas asal Rusia dengan target serangan siber ke Ukraina.



Gambar 3. Model *Cyber Early Warning* pada Kasus Rusia vs Ukraina (Diolah oleh penulis, 2022)

Intelijen Negara

Menurut Eks Kepala BIN (Badan Intelijen Negara) Prof A. M. Hendropriyono, intelijen (nonmiliter) bekerja mendukung pengguna (*user*) melalui penyajian informasi bersifat intelijen (informasi benar yang sudah diolah), untuk unggul dalam persaingan, kompetisi, atau kehendak. Kekeliruan dalam penentuan kebijakan pemerintahan negara merupakan latar belakang dari permasalahan yang dihadapi oleh intelijen negara di berbagai negara (Hendropriyono 2013).

Penyajian informasi intelijen dilakukan dengan cara menghasilkan produk intelijen yang disampaikan secara lisan dan secara tertulis. Irawan (2014) menyebut produk tersebut sebagai *Intelligence Paper* yang mencakup masa lalu, dimensi masa sekarang, dan dimensi akan datang. Informasi-informasi tersebut terdiri dari 80 persen informasi dari sumber terbuka dan sisanya dari sumber tertutup. *Intelligence Paper* diberikan kepada klien tunggal sebagai bahan masukan untuk pengambilan keputusan. Tugas Intelijen adalah memberikan informasi dan masukan sedini mungkin kepada klien tunggal agar klien tersebut dapat membuat keputusan secepat mungkin. Berdasarkan *The Reason of D' etrer*, intelijen berkaitan langsung dengan kepentingan nasional dan keamanan nasional (Sukarno 2004).

Dalam menjalankan kepentingan dan keamanan nasional, terdapat permasalahan baik dari dalam negeri maupun luar negeri. Permasalahan yang muncul merupakan permasalan strategis berupa ancaman serangan siber yang menargetkan Indonesia. Sugirman dalam bukunya berjudul "Analisis Intelijen", memaknai permasalahan strategis adalah masalah yang memiliki nilai dampak berjangka panjang, cakupan luas, dan ukuran yang besar. Permasalahan yang strategis harus ditangani dengan kebijakan-kebijakan yang trategis juga karena langkah-langkah taktis tidak dapat menyelesaikan permasalahan yang strategis (Sugirman 2009). Permasalahan strategis tersebut merupakan ancaman yang harus ditangani oleh intelijen negara. Dalam Undang-Undang (UU) Nomor 17 Tahun 2011 tentang Intelijen Negara, penjelasan UU tersebut menjelaskan bahwa hakikat ancaman bersifat multidimensional dan mengalami perubahan makna dari simetris menjadi asimetris.

Merujuk pada perang siber, maka ancaman siber merupakan ancaman asimetris dan bersifat strategis karena dampak yang ditimbulkan sangat luas sehingga mampu melumpuhkan infrastruktur vital suatu negara seperti serangan siber terjadi pada Estonia dan Georgia. Antisipasi ancaman siber merupakan salah satu tugas dari intelijen negara sebagai lini pertama keamanan negara sesuai dengan UU No. 17 Tahun 2011. Antisipasi tersebut dilakukan dengan melaksanakan fungsi intelijen berupa penyelidikan, pengamanan, dan penggalangan. Dalam hal antisipasi, fungsi penyelidikan lebih dominan dilakukan dengan cara deteksi dini dan cegah dini baik melalui kegiatan intelijen maupun operasi intelijen. Hasil penyelidikan tersebut kemudian dianalisis sehingga menghasilkan informasi bersifat intelijen kemudian disampaikan kepada *user* agar dijadikan pertimbangan dalam mengambil kebijakan yang berdampak secara nasional.

Peran BIN Dalam Menangkal Ancaman di Bidang Siber

BIN sebagai wujud dari intelijen negara memiliki peran untuk menangkal, mencegah, hingga mengatasi masing-masing ancaman yang merongrong keamanan dan kepentingan nasional (Bahtiar, Purwadianto, and Juwono 2021). BIN memliki peran sangat vital karena menjadi

mata dan telinga Presiden RI. Artinya, BIN mempunyai tanggung jawab dan kewenangan untuk membantu presiden menyusun prioritas pembangunan, termasuk penguatan SDM dan teknologi siber. Salah satu ancaman di bidang siber yang cukup signifikan adalah serangan siber pada infrastruktur strategis negara (Persadha 2021). Ancaman serangan siber berpotensi menimpa hampir setiap aspek kehidupan modern dan dapat mempengaruhi kestabilan negara jika tidak segera diantisipasi (Siburian, Makayasa, and Romika 2021).

BIN sebagai salah satu penyelenggara intelijen negara berdasarkan Undang-Undang Nomor 17 Tahun 2011, berperan dalam mendeteksi ancaman yang dapat mengganggu kepentingan dan keamanan nasional. Khusus di bidang siber, BIN melakukan deteksi ancaman dengan melakukan patroli siber secara berkala untuk memonitoring ancaman siber dan menerapkan pengamanan berlapis untuk menangkal adanya serangan siber yang mengarah pada sistem informasi teknologi (CNBC Indonesia 2021). Selain itu, BIN melalui layanan publik Deputi Bidang Intelijen Siber BIN berupa *Security Assesment* atau penilaian keamanan siber. Layanan ini hanya terbatas pada instansi pemerintah saja sesuai dengan lampiran Standar Pelayanan *Security Assessment* pada Keputusan Kepala Badan Intelijen Negara Nomor 36 Tahun 2019 tentang Standar Pelayanan Badan Intelijen Negara (Samad 2021).

Merujuk pada model *Cyber Early Warning* dan dikaitkan dengan peran BIN, maka patroli siber dan *Security Assessment* memiliki peran penting dalam mendeteksi ancaman pada tahapan model *Cyber Early Warning.* Melalui patroli siber, BIN dapat mendeteksi ketegangan laten sebagai bentuk indikasi adanya pemicu atau potensi ancaman siber. Kemudian, patroli siber dilakuan secara mendalam dan spesifik sesuai dengan temuan pada tahap sebelumnya. Selanjutnya patroli siber mengarah pada forum-forum atau seruan di dunia maya yang mengindikasikan potensi serangan siber guna memastikan apakah ada upaya mobilisasi siber yang berujung pada serangan siber. Sedangkan *Security Assessment* lebih berperan pada tahap celah keamanan siber yang berpotensi dimanfaatkan oleh pihak lain sebagai pintu untuk melakukan serangan siber. Keberadaan *Security Assessment* mampu mendeteksi celah keamanan tersebut sehingga pihak yang ingin melakukan serangan siber tidak dapat mengumpulkan informasi secara utuh sesuai dengan tahap *Cyber Recon* dan pada akhirnya serangan siber dapat diminimalisir bahkan ditiadakan karena tahap selanjutnya sulit dilakukan karena kurangnya informasi yang tersedia. Peran BIN tidak hanya sebatas memberikan layanan publik dan patroli siber, tetapi juga penyelenggaran koordinasi intelijen negara di pusat dan di daerah berdasarkan Peraturan Presiden (Perpres) Nomor 67 Tahun 2013 tentang Koordinasi Intelijen Negara. Dalam persepektif ini, BIN sebagai koordinator dapat melakukan rapat koordinasi melalui forum Komite Intelijen Pusat (Kominpus) dan Komite Intelijen Daerah (Kominda) yang membahas kasus serangan siber yang mengancam Indonesia (Samad and Persadha 2022). Hasil patroli siber, Kominpus/Kominda, dan *Securit Assessment* tertuang dalam *Intelligence Paper* yang mencerminkan sejauh mana ketahanan siber di Indonesia khususnya ketahanan siber pada instansi pemerintah sehingga Presiden RI sebagai *user* dapat mengambil keputusan strategis di bidang siber guna mencegah serangan siber terjadi di Indonesia.

KESIMPULAN

Serangan siber Rusia yang menargetkan sejumlah negara telah melalui berbagai tahap sesuai dengan model *Cyber Early Warning,* mulai dari tahap ketegangan, pengumpulan informasi, persiapan penyerangan, mobilisasi siber, hingga serangan siber. Pola tersebut dilakukan oleh Rusia sejak lama dan hal tersebut digunakan lagi pada serangan siber ke Ukraina sebagai bagian dari rangkaian invasi Rusia ke Ukraina di tahun 2022. Tahap-tahap ini telah dilakukan oleh Rusia ketika

melakukan serangan ke sejumlah negara, seperti Estonia, Georgia dan Ukraina. Untuk menangkal adanya serangan siber serupa oleh negara lain dan menargetkan Indonesia, BIN melakukan koordinasi melalui forum Kominda dan Kominpus dengan agenda yang berkaitan dengan serangan siber, patroli siber dan *Security Assessment* secara spesifik berperan dalam setiap tahapan pada model *Cyber Early Warning.* Dengan demikian, penulis menyarankan aturan tentang layanan *Security Assessment* direvisi agar layanan *Security Assessment* juga dilaksanakan pada sektor swasta terutama yang mengelola data-data krusial. Bagi peneliti selanjutnya, melakukan penelitian terhadap bagaimana peran BIN dalam menangkal ancaman bidang siber di tingkat masyarakat.

UCAPAN TERIMA KASIH

Terima kasih kepada *Communication & Information System Security Research Center* (CISSReC).

DAFTAR PUSTAKA

Bahtiar, Andhi, Agus Purwadianto, and Vishnu Juwono. 2021. "Analisa Kewenangan Badan Intelijen Negara (BIN) DalamPenanganan Pandemi Covid-19." *JIIP: Jurnal Ilmiah Ilmu Pemerintahan* 6 (2). https://doi.org/10.14710/jiip.v6i2.11475.

Burhan, Fahmi Ahmad. 2021. "Kominfo: 29 Lembaga Alami Kebocoran Data Sejak 2019, Termasuk BPJS." *Katadata.Co.Id*, 2021. https://katadata.co.id/desysetyowati/digital/60d2eac6a7826/kominfo-29-lembaga-alami-kebocoran-data-sejak-2019-termasuk-bpjs.

Carr, Jeffrey. 2012. *Inside Cyber Warfare: Mapping the Cyber Underworld*. O'Reilly Media, Inc.

CNBC Indonesia. 2021. "Tangkal Serangan Hacker, BIN Terapkan Keamanan Berlapis." *CNBC Indonesia*, 2021. https://www.cnbcindonesia.com/news/20210927113153-8-279397/tangkal-serangan-hacker-bin-terapkan-keamanan-berlapis.

Danchev, Dancho. 2008. "Coordinated Russia vs Georgia Cyber Attack in Progress." *Zdnet*, 2008. https://www.zdnet.com/article/coordinated-russia-vs-georgia-cyber-attack-in-progress/.

Direktorat Operasi Keamanan Siber. 2021. "Laporan Tahunan Monitoring Keamanan Siber 2021." Jakarta Selatan. https://cloud.bssn.go.id/s/Lyw8E4LxwNiJoNw.

Gatlan, Sergiu. 2022. "Ukraine Targeted by Almost 800 Cyberattacks since the War Started." *Bleepingcomputer*, 2022. https://www.bleepingcomputer.com/news/security/ukraine-targeted-by-almost-800-cyberattacks-since-the-war-started/.

Guchua, Alika, Thornike Zedelashvili, and Gela Giorgadze. 2022. "Geopolitics of the Russia-Ukraine War and Russian Cyber Attacks on Ukraine-Georgia and Expected Threats." *Ukrainian Policymaker* 10: 26–36. https://doi.org/. https://doi.org/10.29202/up/10/4.

Hendropriyono, A. M. 2013. *Filsafat Intelijen Negara Republik Indonesia*. Jakarta: Kompas Media Nusantara.

Herzog, Stephen. 2011. "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses." *Journal of Strategic Security* 4 (2).

Hollis, D. 2011. "Cyberwar Case Study: Georgia 2008." *Small Wars Journal* 7 (1): 1–9.

Kozlowski, Andrzej. 2013. "Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan." In *International Scientific Forum*. Tirana. https://www.researchgate.net/profile/Nnedinma-Umeokafor/publication/260107032_International_Scientific_Forum_ISF_2013vol3/links/02e7e52f964505c201000000/International-Scientific-Forum-ISF-2013vol3.pdf#page=246.

Lin, Herbert. 2012. "Cyber Conflict and International Humanitarian Law." *International Review of The Red Cross* 94 (886): 515–31.

Microsoft. 2021. "Microsoft Digital Defense Report." https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi.

———. 2022. "Special Report: Ukraine." https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

Najmi, Crystalia Shabrina, and Rani Lestiyaningsih. 2022. "No Title." https://www.researchgate.net/profile/Crystalia-Shabrina-Najmi/publication/359505744_UPAYA_RESOLUSI_KONFLIK_DALAM_PERANG_RUSIA_-UKRAINA_2022/links/6241125a8068956f3c539709/UPAYA-RESOLUSI-KONFLIK-DALAM-PERANG-RUSIA-UKRAINA-2022.pdf.

Narbuko, Cholid, and Abu Achmadi. 2015. *Metodologi Penelitian*. Jakarta: Bumi Aksara.

NATO StratCom COE. n.d. "2007 Cyber Attacks on Estonia." https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf.

Ornay, Emanuel Sani de, and Nur Azizah. 2022. "Kepentingan Keamanan Nasional Rusia Dalam Serangan Militer Terhadap Ukraina Tahun 2022." *Jurnal Communitarian* 4 (1).

Permadi, Dedy. 2021. "Update Terkait Dugaan Kebocoran Data Pribadi Penduduk Indonesia." *Kominfo*, 2021. https://www.kominfo.go.id/content/detail/34628/siaran-pers-no-179hmkominfo052021-tentang-update-terkait-dugaan-kebocoran-data-pribadi-penduduk-indonesia/0/siaran_pers.

Persadha, Pratama. 2020. "Hacktivism Sebagai Upaya Menyampaikan Suara Lewat Ruang Siber Di Indonesia." *Jurnal Penelitian Ilmu-Ilmu Sosial* 21 (2): 72–77.

———. 2021. "Membangun Dan Mempersiapkan Sumber Daya Intelijen 5.0 Dalam Menghadapi Ancaman Serta Peluang Di Era Digital." *Jurnal Penelitian Dan Kajian Intelijen* 2 (1): 15–29.

Pratiwi, Ratna Ayu Paramitha. 2019. "Analisis Persepsi Keamanan Nasional India Terhadap Serangan Siber Dari Pakistan 2008-2017." *Journal of International Relations* 5 (4).

Priyono, Ujang. 2022. "Cyber Warfare as Part of Russia and Ukraine Conflict." *Jurnal Diplomasi Pertahanan* 8 (2).

Rofii, Muhammad Syaroni. 2018. "Antisipasi Perang Siber: Postur Ketahanan Nasional Indonesia Merespon Ancaman Perang Siber." *Jurnal Kajian Stratejik Ketahanan Nasional,* 1 (2).

Roy. 2022. "Bukan Dunia Nyata, Perang Rusia-Ukraina Ngeri Di Dunia Maya." *CNBC Indonesia*, 2022. https://www.cnbcindonesia.com/tech/20220303100401-37-319748/bukan-dunia-nyata-perang-rusia-ukraina-ngeri-di-dunia-maya.

Samad, M. Yusuf. 2021. "Optimalisasi Layanan Publik Badan Intelijen Negara Dalam Perspektif Global Cybersecurity Index." *Al Ulum Sains Dan Teknologi* 7 (1).

Samad, M. Yusuf, and Pratama Dahlian Persadha. 2022. "Pendekatan Intelijen Strategis Sebagai Upaya Memberikan Perlindungan Di Ruang Siber Dalam Konteks Kebebasan Menyatakan Pendapat." *Jurnal Kajian* 27 (1): 31–42.

Setiawan, Riyan. 2020. "KPU Membenarkan 2,3 Juta Data Yang Bocor Merupakan DPT Tahun 2014." *Tirto*, 2020. https://tirto.id/kpu-membenarkan-23-juta-data-yang-bocor-merupakan-dpt-tahun-2014-fA5B.

Setyowati, Desy. 2022. "Perang Hacker Rusia Dan Ukraina." *Katadata*, 2022. https://katadata.co.id/desysetyowati/digital/6226ff1f90fb6/perang-hacker-rusia-dan-ukraina.

Siburian, V. N., I. M. W. A. Makayasa, and E. M. Romika. 2021. "Optimalisasi Kesiapan Sumber Daya Manusia Menghadapi Ancaman Siber Dalam Mewujudkan Keamanan Nasional." *Jurnal Penelitian Dan Kajian Intelijen* 2 (1): 111–38.

Sugirman, Supono. 2009. *Analisis Intelijen*. Jakarta: Center for The Study of Intelligence and Counter Intelligence.

Sukarno, Irawan. 2004. *Ilmu Intelijen*. Jakarta: Prenada Media Group.

Suratman, Yosua Praditya. 2017. "Penggunaan Strategi Operasi Kontra Intelijen Dalam Rangka Menghadapi Ancaman Siber Nasional." *Jurnal Pertahanan Dan Bela Negara* 7 (2).

T. M. K. Roeder, P. I. Frazier, R. Szechtman, E. Zhou, T. Huschka, and S. E. Chick. 2016. "Simulating Political and Attack Dynamics of The 2007 Estonian Cyber Attacks." In *Proceedings of the 2016 Winter Simulation Conference*.

Tikk, Eneken, Kadri Kaska, and Liis Vihul. 2010. *International Cyber Incidents: Legal Considerations*. Tallinn: Cooperative Cyber Defence Centre of Excellence (CCD COE). https://ccdcoe.org/uploads/2018/10/legalconsiderations_0.pdf.

Yuliantiningsih, Aryuni. 2021. "Analisis Doktrin Perang Yang Adil (Just War) Dalam Kasus Serangan Siber Rusia Terhadap Georgia Tahun 2008." *Kosmik Hukum* 21 (3): 167–75. https://doi.org/10.30595/kosmikhukum.v21i3.10613.