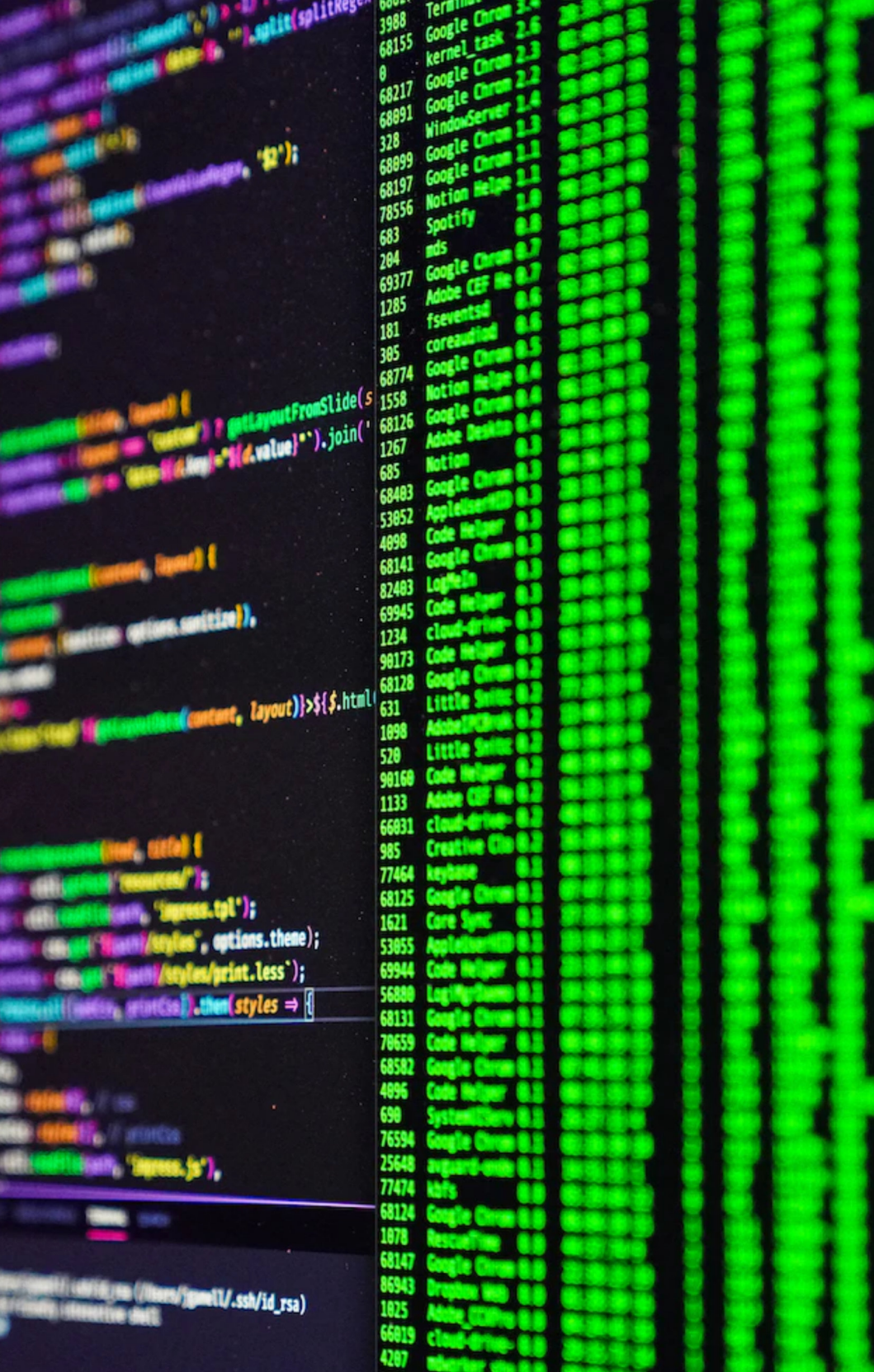
PERANG RUSIA-UKRAINA

DALAM PERSPEKTIF SIBER

PERANG RUSIA - UKRAINA

DALAM PERSPEKTIF SIBER

Sebuah Literasi



TIM PENYUSUN

PEMBINA
MARSMA TNI R. TJAHJO KURNIAWAN
BRIGJEN POL ANTONIUS DWI HENDRO S.

PENGARAH
KOLONEL SUS RIYONO WAHYUDI
KOLONEL CHB SRI ADI TRIO WAHYU P.
KOLONEL SUS HUDI ISTANTO
KOLONEL SUS HENDRA GUNAWAN
KOLONEL LAUT (E) ARNOLDUS TRIONO
KOMBES POL RAHMAD DAMDAMI
LETKOL CHB EKO BAMBANG WIBOWO

PENULIS
LETKOL SUS DWI CAHYO BUDIMAN
LETTU LAUT (E) ROBBY WAHYU
LETTU SUS CAHYO RAMDHANI W
LETTU CHB MUH MUNANDAR
AKP IRKHAMUL KHAKIM
ASEP SETIAWAN
KEVIN YEHEZKIEL GURNING
TEGUH DARMAWANGSA
KONTRIBUTOR TARUNA/TARUNI POLTEK SSN

LAYOUT DAN DESAIN
UCHA
KEVIN YEHEZKIEL GURNING
M. RIFKY
DICKY SAFAAT FUADI

Diterbitkan oleh Politeknik Siber dan Sandi Negara Press
Jl. H. USA Ciseeng, Bogor, Jawa Barat, 16120, Telp. (0251) 8541742
Email: perpustakaan@poltekssn.ac.id

Cetakan I : 2023

ISBN
ISBN

SAMBUTAN KEPALA BSSN

Letjen TNI (Purn) Hinsa Siburian

Bismillahirrahmanirrahim.
Assalamualaikum Warahmatullahi Wabarakatuh.
Salam sejahtera bagi kita sekalian, Syalom, Om Swasyastu, Namo Buddaya, Salam kebajikan.

Salam siber.

Kemajuan teknologi telah mendorong tatanan baru hampir di semua sektor kehidupan, seperti sektor pendidikan, perdagangan, pertanian, transportasi, kesehatan, pemerintahan, industri, termasuk sektor pertahanan dan keamanan. Keberadan negara Republik Indonesia harus bisa menjaga pertahanan dan keamanan penduduknya, sementara ancaman dan serangan keamanan dan pertahanan negara telah terjadi di berbagai sudut, batas laut, udara, darat hingga saat ini sampai kepada perang siber.

Serangan siber sendiri telah mengalami evolusi sesuai dengan perkembangan teknologi. Dari yang sifatnya kejahatan individu, sekarang ini menjadi kejahatan terorganisasi bahkan ada yang didukung oleh negara. Dari yang motifnya pribadi sudah berkembang menjadi motif kelompok, motif ideologi bahkan menjadi bagian dari *cyber-war*.

Selaku Kepala Badan Siber dan Sandi Negara, menyambut gembira dan sangat mengapresiasi terbitnya buku "***Perang Rusia-Ukraina dalam perspektif siber***". Buku hasil karya dari adik-adik saya dari Alumni Sandi Negara yang bertugas di TNI-Polri. Sesuai dengan amanat Presiden RI **Joko Widodo** pada tanggal 16 Agustus 2019, mengingatkan agar kita harus siaga menghadapi ancaman Siber, termasuk kejahatan penyalahgunaan data dan harus siap tanggap dan siap menghadapi serangan siber. Serangan siber dapat dikategorikan menjadi kriminal biasa, kriminal luar biasa, dan perang siber, bergantung dari tujuan dan intensitas serangan tersebut tanpa terbatas pada pembagian spektrum waktu dimasa damai, krisis, atau dalam keadaan perang.

Perang siber pada perang Rusia-Ukraina memiliki dampak yang signifikan di seluruh dunia, termasuk di Indonesia, dampak dari perang siber bisa jauh lebih besar dibandingkan dengan perang konvensional. Kita semua harus siap di bidang pertahanan dan keamanan khususnya menghadapi perang siber.

Saya juga mengajak partisipasi aktif dari seluruh pihak untuk dapat memberikan kontribusi dan sumbangsih dalam bentuk apapun pada usaha dan upaya untuk menjaga kedaulatan siber nasional, karena pada hakikatnya kedaulatan siber nasional hanya dapat diwujudkan dengan kolaborasi dan sinergi dari seluruh komponen bangsa.

Salam siber.

Jakarta, Agustus 2023
Kepala Badan Siber dan Sandi Negara

Letjen TNI (Purn) Hinsa Siburian


SAMSUNG

SAMBUTAN PAKAR SIBER

Dr. Pratama Dahlian Persadha

Bismillahirrahmanirrahim.
Assalamualaikum Warahmatullahi Wabarakatuh.
Salam sejahtera bagi kita sekalian,
Syalom,
Om Swasyastu,
Namo Buddaya,
Salam kebajikan.

Salam siber,

Dengan rasa hormat, saya ingin menghadirkan sambutan untuk buku yang luar biasa ini. Buku ini adalah hasil karya dari senior dan adik-adik saya dari Alumni Sandi Negara di TNI-Polri. Tim Penulis buku ini "Cipherworks" adalah penggiat dan pelaku dunia siber di lingkungannya dengan penugasan dan pengalaman yang beragam.

Dunia siber merupakan sebuah dunia yang semakin kompleks dan cepat berubah. Indonesia saat ini juga tengah menghadapi perang siber yang kondisinya sangat jauh berbeda dengan perang konvensional. Dalam perang konvensional, kita bisa menghitung senjata apa yang dipakai musuh, berapa jumlah pasukan dan berapa banyak tank yang digunakan. Dalam perang siber, tidak dapat diketahui siapa pelaku penyerangan, teknologi apa yang dipergunakan, kekuatannya sebesar apa, berapa orang yang digerakkan, dan infrastruktur apa yang dihancurkan. Efek yang ditimbulkan oleh perang siber pun akan jauh lebih parah daripada perang konvensional.

Sebagai sebuah literasi, buku ini dapat dijadikan sebagai pembelajaran mengenai tahapan dan serangan dalam ranah siber. Buku ini adalah sumber yang tak ternilai bagi siapa pun yang ingin memahami dunia siber dan mengambil langkah-langkah proaktif dalam melindungi diri dan organisasinya dari serangan siber.

Saya ingin mengucapkan penghargaan yang tulus dan sebesar-besarnya kepada tim penulis atas dedikasinya dalam memperkenalkan dunia siber. Buku ini adalah hasil dari pengalaman praktis selama pendidikan dan penugasan, penelitian yang mendalam, dan wawasan yang luas. Saya juga ingin mengucapkan terima kasih kepada penerbit yang telah memberikan platform kepada tim penulis untuk membagikan pengetahuan yang sangat berharga ini kepada dunia.

Akhir kata, saya mendorong setiap pembaca untuk mengeksplorasi buku ini dengan antusiasme dan ketertarikan yang tinggi karena saya yakin bahwa buku ini akan memberikan pemahaman yang mendalam serta menjadi acuan yang berharga dalam menjaga keamanan di dunia siber yang semakin kompleks ini.

Terima kasih dan selamat membaca !

Hormat saya,

Dr. Pratama Dahlian Persadha

Chairman Lembaga Riset Keamanan Siber dan dan Komunikasi CISSReC (Communication and Information System Security Research Center)

“WHY DID I DECIDE TO WRITE CYBER THRILLERS ? BECAUSE WE’VE GONE FROM THE COLD WAR TO THE CODE WAR “

-Thomas Waite-

SANDI NEGARA
TNI - POLRI

FOREWORD

Marsma TNI R. Tjahjo Kurniawan, S.T., M.Si
Direktur Politeknik Siber dan Sandi Negara

Bismillahirrahmanirrahim.
Assalamualaikum Warahmatullahi Wabarakatuh.
Salam sejahtera bagi kita sekalian,
Syalom,
Om Swasyastu,
Namo Buddaya,
Salam kebajikan.

Perkembangan teknologi yang begitu pesat memaksa dunia menghadapi perang generasi kelima yang mengubah tren perang yang semula cold war menjadi code war/cyber war. Perang siber dilakukan dengan memanfaatkan Advanced Persistent Threat (APT) sehingga tak perlu berhadapan secara fisik, namun dampak yang ditimbulkan dari serangan siber ini dapat melumpuhkan sebuah negara dari berbagai sektor. Perang antara Rusia dan Ukraina merupakan salah satu contoh nyata perang siber dengan memanfaatkan malware (malicious software) dan phising. Kondisi tersebut kini tidak lagi bisa dihindari namun harus

dihadapi. Butuh persiapan yang matang bukan hanya dari sisi pemanfaatan teknologi terkini namun juga perlu tersedianya kompetensi personal yang siap menghadapi perang siber.

Buku “Perang Rusia-Ukraina dalam perspektif siber” memberikan gambaran yang komprehensif terkait perubahan metode perang yang beralih dari perang fisik menjadi perang siber. Mengangkat contoh perang Rusia dan Ukraina, buku ini diharapkan dapat membantu pembaca untuk mengidentifikasi ancaman siber sehingga dapat menambah wawasan pembaca sehingga lebih siap dan waspada dalam mempersiapkan diri menghadapi perang siber yang mungkin dihadapi Indonesia.

Apresiasi setinggi-tingginya kepada alumni Akademi Sandi Negara – Sekolah Tinggi Sandi Negara yang saat ini berdinas di TNI/Polri serta Taruna Politeknik Siber dan Sandi Negara yang telah bersinergi untuk menyusun buku ini. Akhirnya, saya mengharapkan semoga buku ini dapat mengubah pandangan kita terkait perang siber sehingga kita semakin siap menghadapi dan menanggulangi perang siber yang mungkin dihadapi Indonesia. Kata terakhir saya kutip dari dr. Roebiono Kertopati “Ingatlah bahwa kechilafan satu orang sahaja tjukup sudah menyebabkan keruntuhan negara”.

Salam Siber.

Wasssalamualaikum Wr. Wb.

R. Tjahjo Khurniawan, S.T., M.Si

Marsekal Pertama TNI

PREFACE

Dalam perang Rusia – Ukrainia terdapat juga perang yang tidak kalah hebatnya, buku ini mencoba untuk membahas secara komprehensif mengenai perang siber yang terjadi pada perang tersebut, tahapan perang siber, serangan siber di perang Rusia-Ukraina, analisa perang siber bagi Indonesia, *lesson learn* dan tantangan menghadapinya bagi Indonesia.

Berawal dari keinginan untuk sama-sama belajar, dari sekedar diskusi melalui grup *whatsapp* kemudian terus berlanjut untuk mewujudkan ide menjadi sebuah karya. ***Buku Perang Rusia-Ukraina dalam perspektif siber*** merupakan karya perdana dari Cipherworks, sebuah tim kecil dari komunitas alumni Akademi Sandi Negara dan Sekolah Tinggi Sandi Negara TNI-Polri.

Puji syukur kepada Allah SWT sang pemilik semua dan ucapan terima kasih kami kepada senior, rekan, Taruna-Taruni Poltek SSN, dan ahli keamanan siber serta semua pihak yang tidak bisa kami sebutkan satu persatu yang telah berkontribusi dalam menyusun buku ini.

Kami menyadari bahwa dalam menulis buku ini masih jauh dari kata sempurna. Oleh karena itu, kritik dan saran yang membangun diharapkan dapat membuat buku ini menjadi lebih baik.

Akhir kata, semoga buku ini dapat memberikan manfaat dan pengetahuan bagi pembaca. Tetaplah berbuat baik. Terima kasih.

Jakarta, Agustus 2023

Cipherworks.

Letkol Sus Dwi Cahyo B., S.Kom., M.I.Pol

DISCLAIMER

Buku berjudul *Perang Rusia-Ukraina dalam perspektif siber* - sebuah literasi adalah buku yang ditulis oleh Cipherworks-tim penulis dari Alumni Sandi Negara TNI-Polri. Apabila di dalam buku ini terdapat skema, logo, gambar, istilah atau bahan persentasi yang mengacu pada suatu negara, institusi, perorangan, produk, merk dagang atau vendor tertentu, HANYA dipergunakan sebagai sarana untuk memudahkan pemahaman dan penjelasan mengenai isi buku ini saja dan TIDAK ADA KEPENTINGAN atau maksud dan tujuan lain atau adanya unsur kesengajaan diluar konteks pembuatan buku ini. Rangkaian kejadian ditulis antara Februari 2022 s.d Februari 2023. Seluruh referensi yang berasal dari sumber terbuka dapat dipastikan aktif pada saat buku ini diterbitkan, namun eksistensi link tersebut bisa saja berubah atau menjadi tidak aktif dikarenakan satu dan lain hal. Kritik dan saran yang membangun dapat disampaikan melalui *email* dengan alamat codenameucha@gmail.com atau cipherworks@gmail.com.

Terima Kasih.

Jakarta, Agustus 2023

Cipherworks

EXECUTIVE SUMMARY

“ Supreme excellence consists of breaking the enemy's resistance without fighting.”

- Sun tzu, The Art of War

Dunia saat ini sedang menghadapi perang generasi kelima. Tren perang telah berubah dengan optimalisasi pemanfaatan ilmu pengetahuan dan teknologi (IPTEK) sehingga perang konvensional antar negara hampir tidak lagi terjadi, namun perang yang lebih dominan adalah *cyber war* atau perang siber. Perang dunia maya telah menjadi medan perang baru di zaman modern.

Perang siber antara Ukraina dan Rusia telah berlangsung sejak 2014, dengan kedua negara meluncurkan serangkaian serangan terhadap satu sama lain. Serangan menargetkan Infrastruktur Informasi Kritis (IIV), organisasi pemerintah, dan individu. Di balik setiap serangan militer fisik dan setiap tindakan agresi militer terdapat operasi yang tidak terlihat. Ketika Presiden Putin mengumumkan "operasi militer" dan militer Ukraina serta warga sipil melawan pasukan Rusia yang menyerang, jenis perang (non-fisik) yang sangat berbeda juga dilancarkan

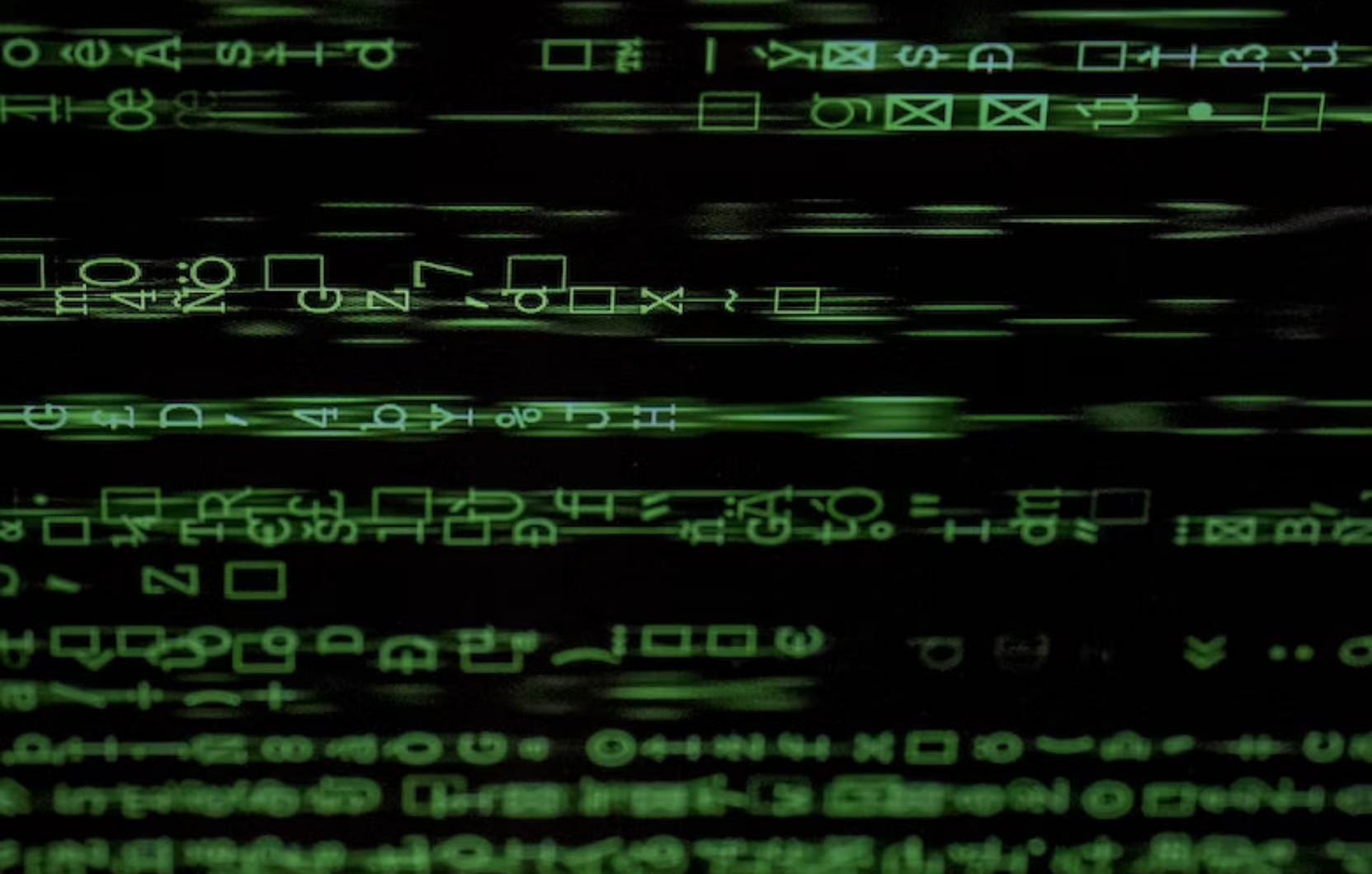
di medan perang lain, yaitu Internet/Dunia maya. Perang Siber menjadi medan perang baru dari Rusia terhadap Ukraina. Aktor negara dan non-negara Rusia melakukan penghancuran IIV, melumpuhkan layanan negara dan ancaman psikologis tanpa kontak fisik yang sebenarnya.

Menurut Cyber Peace Institute, 8 (delapan) ancaman siber yang dominan dalam konteks perang antara lain *Malware, Distributed Denial of Service/DDoS, Defacement, Cyber enabled information operations, Hack and leak, Cyberespionage, Ransomware*, dan *Wiper*. Perang siber di Rusia dan Ukraina menunjukkan semakin pentingnya keamanan siber di zaman modern dan pentingnya kerja sama internasional dalam memerangi ancaman keamanan siber serta menunjukkan betapa pentingnya keamanan siber yang baik bagi suatu negara.

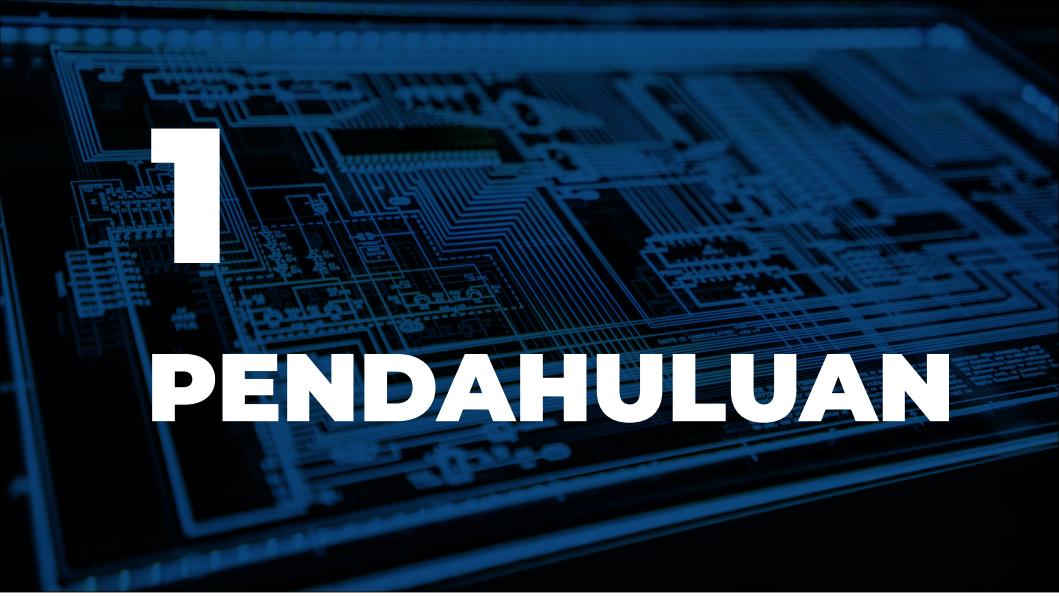
Indonesia dapat mengambil pelajaran dari perang siber yang terjadi di perang Rusia-Ukraina seperti meningkatkan langkah-langkah pencegahan dengan memperkuat infrastruktur keamanan siber, berinvestasi dalam pelatihan dan kesadaran keamanan siber dan mendorong pengembangan industri keamanan siber.

Tantangan dalam mengantisipasi ancaman siber di masa mendatang bagi Indonesia adalah perkembangan dan kecanggihan ancaman siber, belum adanya sistem berbagi intelijen ancaman yang komprehensif dan terkini, serta kurangnya sumber daya manusia yang berpengalaman di bidangnya. Dampak perang siber bisa jauh lebih besar dibandingkan dengan perang konvensional.

DAFTAR ISI



DAFTAR GAMBAR



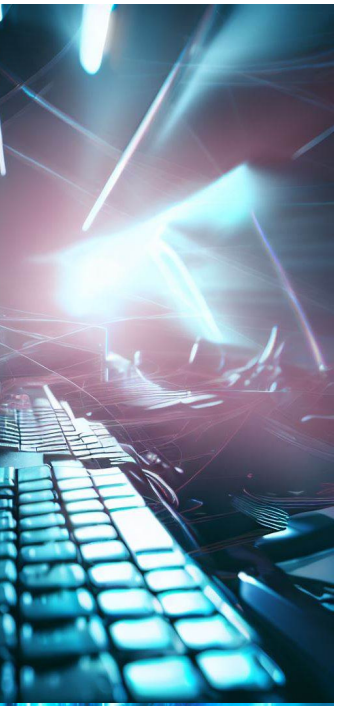
1 PENDAHULUAN

Tren perang telah bergeser dengan mengoptimalkan pemanfaatan Ilmu Pengetahuan dan Teknologi (IPTEK) sehingga perang konvensional antar negara hampir tidak lagi ditemukan, tetapi perang yang lebih dominan adalah perang siber atau *cyber war*. Perang siber mengacu pada penggunaan teknologi digital dan jaringan informasi untuk melakukan tindakan perang atau agresi terhadap lawan. Hal ini dapat mencakup berbagai aktivitas, seperti meretas sistem komputer untuk mencuri informasi sensitif, meluncurkan serangan *denial of service* untuk mengganggu atau melumpuhkan infrastruktur penting, atau menggunakan media sosial dan *platform online* lainnya untuk menyebarkan propaganda atau informasi yang keliru. Perang siber dapat dilakukan oleh aktor negara, seperti pemerintah atau organisasi militer, atau aktor non-negara, seperti kelompok kriminal atau

peretas. 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.

Sejak 24 Februari 2022, Rusia melakukan invasi militer ke Ukraina yang didahului oleh rangkaian *cyber attack*. Perang siber Rusia dan Ukraina telah ditandai dengan berbagai serangan siber dan insiden peretasan serta telah digunakan sebagai alat politik untuk mendukung tujuan politik dan militer yang lebih luas.

"Dunia saat ini sedang menghadapi perang generasi kelima (G-V) berupa peperangan siber dan informasi di dunia digital, yang dikenal juga dengan *cyber warfare*."



PERANG SIBER DI RUSIA - UKRAINA

Perang siber antara Ukraina dan Rusia telah berlangsung sejak 2014 (P.W & Friedman, 2014), dengan kedua negara meluncurkan serangkaian serangan terhadap satu sama lain. Serangan-serangan ini menargetkan Infrastruktur Informasi Vital (IIV), organisasi pemerintah, dan individu (Smith, 2022). Perang siber ini telah memberikan dampak yang signifikan terhadap keamanan siber secara global, termasuk di Indonesia. Salah satu dampak utama perang siber terhadap keamanan siber di Indonesia adalah meningkatnya kesadaran akan potensi serangan siber terhadap IIV. Seiring dengan pesatnya perkembangan dan modernisasi IIV di Indonesia, kebutuhan akan langkah-langkah keamanan siber yang efektif menjadi semakin mendesak. Serangan terhadap jaringan listrik Ukraina, misalnya, menunjukkan potensi serangan siber yang dapat menyebabkan gangguan dan kerusakan yang meluas.

Agresi militer yang dilaksanakan oleh Rusia terhadap Ukraina sejak tanggal 24 Februari

Gambar 1. Perang Rusia Ukraina
https://threatpost.com/ukraine-russia-cyber-warzone-splits-cyber-underground/178693/

2022, secara prespektif geopolitik telah menimbulkan berbagai macam stigma dan dampak terhadap kedua negara tersebut. Namun, dibalik seluruh agresi militer yang dilaksanakan secara fisik dan dampak yang ditimbulkan akibat agresi militer tersebut, terdapat sebuah operasi tak kasat mata, disebut dengan cyber war atau perang siber, yang telah melumpuhkan dan menghancurkan IIV milik Ukraina sehingga Rusia secara leluasa dapat melakukan agresi militer untuk melumpuhkan dan mengambil alih seluruh IIV Ukraina.

Perselisihan antara kedua negara pada dasarnya bukan merupakan konflik yang baru karena perselisihan kedua negara sejatinya sudah dimulai sejak Uni Soviet runtuh dan kedua negara menjadi negara merdeka. Sejumlah permasalahan perbatasan seperti gerakan-gerakan separatis, serangan siber Rusia ke Ukraina, 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 merupakan sebuah gejala geopolitik yang dipicu oleh Barat dibawah kendali North Atlantic Treaty Organization (NATO) (Ornay and Azizah 2022).

Rusia melancarkan invasi militer dengan kombinasi pasukan dan Alutsista, mulai dari tank, pesawat terbang, hingga rudal jelajah. Namun, yang luput dari pandangan masyarakat internasional adalah bahwa yang dilakukan Rusia sebelum melaksanakan invasi ke Ukraina yaitu dengan mengeluarkan cyberweapon yang disebut dengan "Foxblade", yang diluncurkan untuk melumpuhkan IIV di Ukraina melalui serangan siber pada satu hari sebelum pelaksanaan invasi militer secara fisik (Microsoft).

Serangan siber terus berlanjut sejak pengambilan wilayah Krimea (wilayah daratan besar yang terletak di ujung timur Eropa) secara ilegal oleh Rusia pada tahun 2014, dan meningkat tepat sebelum invasi tahun 2022 (EPRS). Selama periode ini baik sektor publik, media, bisnis, keuangan, dan energi di Ukraina mengalami serangan siber secara masif dari Rusia. Tercatat sejak tanggal 24 Februari 2022, serangan siber Rusia telah mengganggu distribusi obat-obatan, makanan, dan pasokan bantuan yang berdampak pada terhambatnya akses ke beberapa layanan dasar hingga terjadinya pencurian data serta propaganda yang menyebabkan disinformasi.

Jika dilihat dari skema invasi yang dilaksanakan oleh Rusia secara menyeluruh, Invasi Rusia sendiri sebagian besar bergantung pada strategi serangan siber yang mencakup setidaknya tiga strategi berbeda dan terkoordinasi dengan tujuan melakukan serangan siber yang merusak di Ukraina,

seperti penetrasi sistem dan jaringan, spionase, serta operasi informasi dan pengaruh (information and psywar) melalui jaringan siber yang menargetkan orang-orang di seluruh dunia (Microsoft). Lebih dari 40% serangan destruktif ditujukan kepada organisasi di sektor IIV yang dapat memiliki efek negatif, khususnya terhadap pemerintah, militer, ekonomi, dan masyarakat. Kemudian, kurang lebih 32% insiden destruktif mempengaruhi organisasi pemerintah Ukraina di tingkat Nasional, Regional, dan pusat-pusat Kota. Adapun aktivitas serangan siber yang dilakukan diantaranya berupa pengiriman email phishing, serangan DDoS, malware, wiper, backdoor, perangkat lunak surveillance, dan pencurian informasi melalui media internet (EPRS).

RUSIA

Rusia memiliki potensi besar dalam hal perang siber dan beberapa peristiwa membuktikannya, seperti Rusia menggunakan senjata siber melawan Georgia selama perang 2008. Negara tersebut telah berhasil mengadaptasi serangan siber untuk memperluas kepentingan negaranya. Pada tahun 2007 serangan siber yang menargetkan Estonia yang berupa serangan Distibuted Denial of Service (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). Tahun 2022, Rusia kembali melakukan serangan siber terhadap Ukraina sebagai bagian dari invasi yang dilakukan Rusia ke Ukraina (Priyono 2022). Rusia merupakan negara penyumbang sebagian

besar (58 %) peretasan yang disponsori negara selama periode Juli 2020 sampai dengan Juni 2021, serangan yang bersumber dari Rusia mengalami peningkatan efektivitas dari 21 % menjadi 32 % (Microsoft 2021).
Serangan siber Rusia pada tanggal 24 Februari 2022 bukanlah yang pertama dilakukan karena Ukraina telah menjadi target permanen serangan siber Rusia sejak tahun 2014. Ribuan serangan terjadi setiap bulan, menjadikan Ukraina sebagai "Sandbox" yang sempurna bagi Rusia dan sebagai tempat untuk melakukan uji coba taktik dan teknik serta peralatan pendukung dalam melaksanakan perang siber (EPRS).

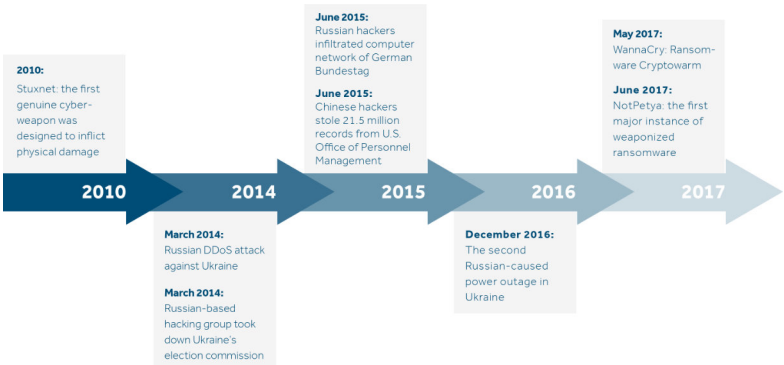
UKRAINA

Ukraina merupakan negara yang berada dekat dengan wilayah inti dari Rusia pada masa kependudukan Uni Soviet

dan dianggap sebagai bagian integral dari Rusia. Hal ini berubah pada tahun 1991 seiring dengan runtuhnya Uni Soviet dan dideklarasikannya kemerdekaan Ukraina dari Uni Soviet. Hubungan antar Rusia dan Ukraina memburuk akibat adanya kepentingan dari kedua belah pihak. Hal ini menyebabkan konflik berkepanjangan yang akhirnya pecah dalam bentuk perang konvensional telah berlangsung sejak bulan Maret 2014, dimana Rusia merebut Crimea dari Ukraina. Sejak saat itu, konflik ini telah diwarnai dengan penggunaan perang fisik dan siber. Di sisi perang siber, Rusia telah dituduh melakukan banyak serangan siber terhadap Ukraina, mulai dari serangan DDoS hingga serangan yang lebih canggih seperti ransomware NotPetya dan kampanye phishing.

2
PERKEMBANGAN KRONOLOGIS PERANG SIBER

Perang siber dapat didefinisikan sebagai penggunaan teknologi komputer untuk menyabotase aset elektronik atau fisik suatu negara atau organisasi. Hal ini terlihat melalui penggunaan virus, worm, malware, ransomware, dan serangan *denial-of-service* (DoS) atau penolakan layanan terdistribusi (DDoS). Pada medio 2010 s.d 2017, Dunia telah melihat berbagai contoh perang siber:



Gambar 2. Visualisasi tahapan perang siber

2010, Stuxnet: Ini adalah senjata siber asli pertama yang dirancang untuk menimbulkan kerusakan fisik. Dilaporkan telah menghancurkan hampir seperlima sentrifugal nuklir Iran. Stuxnet adalah nama yang diberikan untuk malware digital yang sangat kompleks yang menargetkan, dan secara fisik merusak program nuklir rahasia Iran dari tahun 2007 hingga penyamarannya terbongkar pada tahun 2010 oleh para peneliti keamanan komputer. *Malware* ini menargetkan sistem komputer yang mengendalikan infrastruktur fisik seperti sentrifugal dan katup gas.

Maret 2014, serangan DDoS Rusia terhadap Ukraina: Ini adalah kedua kalinya Rusia diduga mengoordinasikan serangan militer dan siber. Serangan DDoS 32 kali lebih besar dari serangan terbesar yang pernah terjadi mengganggu internet di Ukraina ketika pemberontak pro-Rusia

yang bersenjata Rusia menguasai Krimea.

Mei 2014, Rusia vs Komisi Pemilihan Umum Ukraina: Tiga hari sebelum pemilihan presiden Ukraina, kelompok peretas yang berbasis di Rusia melumpuhkan komisi pemilihan umum Ukraina dan sistem cadangannya. Serangan ini merupakan upaya untuk menciptakan kekacauan dan membantu kandidat pro-Rusia.

Juni 2015, Rusia vs parlemen Jerman: Para penyelidik Jerman menemukan bahwa para peretas telah menyusup ke dalam jaringan komputer Bundestag Jerman. Badan intelijen domestik Jerman, BfV, kemudian mengatakan bahwa serangan tersebut dilakukan oleh Rusia dan bahwa mereka mencari informasi tentang cara kerja Bundestag, para pemimpin Jerman, NATO, dan lainnya.

Juni 2015, Kantor Manajemen Personalia Tiongkok vs Amerika Serikat: Data 21,5 juta karyawan dan pelamar yang gagal untuk bekerja di pemerintah Amerika Serikat dicuri dari Kantor Manajemen Personalia AS. Sumber-sumber pemerintah AS meyakini bahwa peretasnya adalah pemerintah Tiongkok.

Desember 2016, pemadaman listrik kedua yang disebabkan oleh Rusia di Ukraina: Diperkirakan bahwa peretas Rusia bersembunyi di jaringan pemasok listrik tanpa terdeteksi selama enam bulan sebelum mematikan listrik. Pemadaman listrik ini menyebabkan sekitar seperlima dari konsumsi listrik di Kiev pada malam itu hilang.

Serangan ini terjadi hampir satu tahun setelah serangan siber pada Desember 2015 yang memutus aliran listrik ke 225.000 orang di Ukraina bagian barat.

Mei 2017, WannaCry: Serangan ini diperkirakan telah memengaruhi lebih dari 200.000 komputer di 150 negara. WannaCry adalah *ransomware cryptoworm* yang menargetkan komputer yang menjalankan Microsoft Windows.

Juni 2017, NotPetya: Ini adalah contoh besar pertama dari ransomware bersenjata. Malware NotPetya menyamar sebagai ransomware tetapi tujuannya adalah untuk menghancurkan file. Meskipun serangan ini berasal dari Ukraina, namun dengan cepat menyebar ke seluruh dunia. Masih belum diketahui secara pasti berapa banyak kerusakan yang ditimbulkan selama serangan ini, tetapi diperkirakan total kerusakannya mencapai lebih dari $10 miliar USD.

PERSIAPAN RUSIA UNTUK PERANG MELAWAN UKRAINA

Rusia telah bersiap secara penuh untuk berkonflik dalam dunia maya sejak Maret 2021, ketika *threat actor* Rusia secara sporadis menargetkan serangan siber terhadap Ukraina serta organisasi dan kelompok lainnya yang diduga dan terbukti mendukung Ukraina. Dalam konflik, threat actor siber Rusia telah diidentifikasi dan diamati oleh *Microsoft Threat Intelligence Center* (MSTIC) saat menjalankan operasi khusus dengan target Ukraina sebelum masa invasi militer. Menjelang invasi militer oleh Russia, Kantor Intelijen Rusia (*Glavnoye Razvedyvatelnoye Upravlenie*) meluncurkan serangan *malware* yang bernama "*Wiper Malware*" yang telah menginfeksi ratusan sistem di pemerintahan Ukraina, baik di sektor

pemerintahan, teknologi informasi, energi, dan organisasi keuangan. Sejak penyebaran *malware* tersebut, aktivitas serangan terpantau meningkat dan telah merusak, mengganggu, dan menginfiltrasi jaringan pada organisasi pemerintahan. Serangan tersebut telah mengakibatkan fungsionalitas jaringan di berbagai layanan pemerintahan tidak dapat diakses oleh penduduk Ukraina dan menyebabkan layanan publik dan IIV di negara tersebut menjadi lumpuh. Serangan tersebut didukung oleh kelompok *Advanced Persistent Threat* (APT) yang secara khusus menargetkan negara Ukraina.

APT sendiri merupakan istilah luas yang mendeskripsikan suatu *campaign* serangan, dimana penyerang melancarkan aksinya secara senyap atau tanpa diketahui dalam jangka waktu yang relatif panjang pada suatu sistem dan jaringan dengan melakukan beberapa serangan yang bervariasi dengan tujuan mendapatkan inforamasi atau data sensitif tingkat tinggi (*Imperva*). Sederhananya, APT adalah suatu ancaman keamanan yang dilakukan

oleh penyerang secara terencana, terstruktur dan berlanjut dalam jangka waktu lama yang dilakukan oleh suatu kelompok organisasi, baik yang berasal dari pemerintahan suatu negara, maupun non pemerintahan atau komunitas. Cara kerja APT sendiri dilakukan dengan sangat matang melalui tahapan-tahapan yang dirancang secara terstruktur menggunakan taktik, teknik dan metode yang berbeda-beda. Berikut merupakan perbedaan antara serangan siber biasa dan serangan APT yang menargetkan suatu sistem (*A Study on Advanced Persistent Threats, Ping Chen et al*).

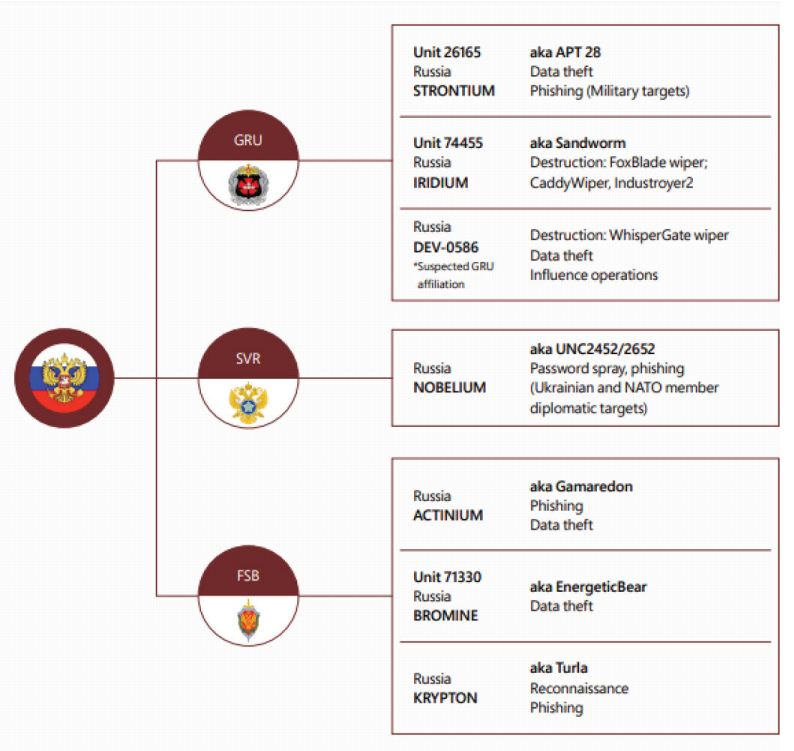
	SERANGAN SIBER BIASA	SERANGAN APT
Penyerang	Kebanyakan adalah perorangan	Kelompok terorganisir, canggih, dan sumber daya lengkap
Target	Tidak tentu dan menyerang secara acak	Organisasi tertentu, institusi pemerintah dan perusahaan komersial
Tujuan	Manfaat finansial dan menunjukkan kemampuan	Keuntungan kompetitif dan manfaat strategis
Pendekatan	Sekali serang dan selesai, jangka waktu pendek	Percobaan dilakukan secara berulang, detail dalam melakukan percobaan dengan melakukan information gathering secara lengkap untuk mengenali sistem pertahanan targetnya, jangka waktu yang dibutuhkan lebih panjang

Gambar 3. Perbedaan serangan siber biasa dan APT.

Berikut merupakan serangan yang dilakukan oleh berbagai APT yang berelasi dengan organisasi intelijen Rusia.

Russia Intelligence Office	Russia's Foreign Intelligence Service	Russia's Federal Security Service
Unit 26165 Russia Strontium (APT 28) APT Rusia yang bertujuan melakukan pencurian data melalui phishing dengan target organisasi militer	APT Russia Nobelium (APT UNC2452/2652) APT yang bertujuan melakukan pencurian password dan phishing yang menargetkan anggota NATO dan anggota diplomatik	APT Russia Actinium (APT Gamaredon) APT yang bertujuan melakukan pencurian data melalui phishing
Unit 74455 Russia Iridium (APT Sandworm) APT Rusia yang bertujuan melakukan penghancuran informasi informasi vital melalui malware FoxBlade iper, CaddyWiper, dan Industroyer2		Unit 71330 Rusia Bromine (APT EnergeticBear) APT yang bertujuan melakukan pencurian data.
APT Group Russia DEV-0586 APT Russia yang bertujuan melakukan pencurian data.		Russia Krypton (APT Turla) APT yang bertujuan melakukan pencarian informasi rahasia melalui phishing

Gambar 4. Tindakan yang dilakukan APT



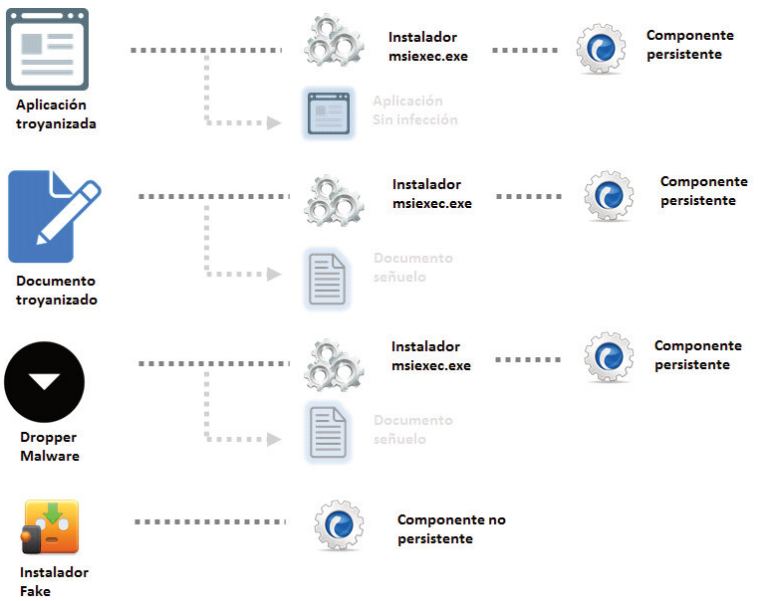
Gambar 5. State actor Rusia yang diidentifikasi oleh Microsoft

SERANGAN PADA PERIODE TAHUN 2014 DAN 2015

Serangan siber terhadap lembaga keuangan di Rusia dan Ukraina menjadi salah satu alat yang digunakan untuk mencapai tujuan Politik. Serangan siber yang terjadi pada sistem perbankan Ukraina oleh kelompok peretas yang didukung oleh Rusia terjadi pada tahun 2014. Serangan tersebut disebut sebagai salah satu serangan siber terbesar yang pernah terjadi di dunia. Serangan tersebut dimulai pada tanggal 24 Februari 2014, ketika *threat actor* Rusia meretas sekitar enam bank Ukraina, termasuk Bank Nadra, Oschad bank, dan Privat Bank. Serangan tersebut dilakukan dengan menggunakan

perangkat lunak berbahaya yang dikenal sebagai *BlackEnergy*, yang mengeksploitasi kelemahan pada jaringan bank (CNN, 2014). Atribusi serangan tersebut tidaklah sederhana, sehingga beberapa perusahaan keamanan di dunia hanya dapat mengidentifikasi bahwa *malware BlackEnergy* berasal dari Rusia dan bahwa Rusia memiliki perselisihan politik dengan Ukraina yang berdampak juga di dunia maya.

Para peretas menggunakan varian *malware BlackEnergy* yang sangat merusak untuk melumpuhkan sistem di tiga otoritas listrik regional di Ukraina sehingga menonaktifkan gardu listrik di negara itu. Serangan siber juga mengganggu penyediaan energi lokal Prykarpattyaoblenergo dan menyebabkan



Gambar 6. Skema infeksi BlackEnergy
(https://www.incibe-cert.es/en/blog/blackenergy-critical-systems)

pemadaman listrik besar-besaran yang membuat setengah populasi di wilayah tersebut tanpa listrik. Kementerian energi Ukraina mengkonfirmasi pemadaman listrik dan mengungkapkan bahwa Pemerintah sedang menyelidiki penyebabnya.

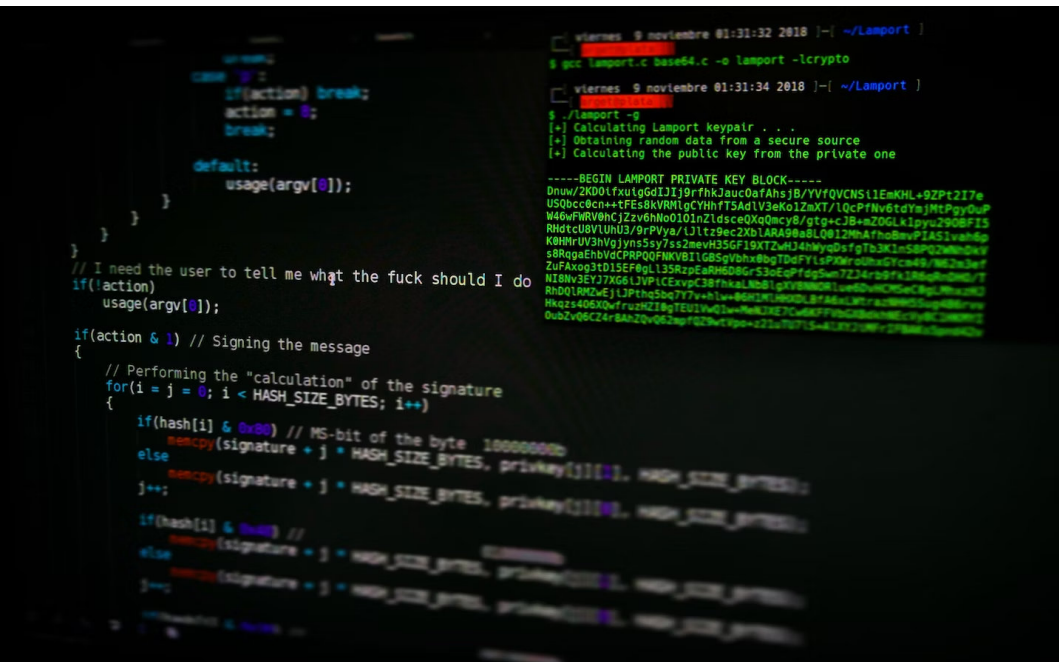
Setelah berhasil masuk ke dalam sistem, peretas menutup akses ke sistem perbankan dan mengirim pesan peringatan yang meminta pembayaran tebusan (*ransomware*). Serangan ini diperkirakan mengakibatkan kerugian mencapai miliaran dolar dan membuat sistem perbankan Ukraina lumpuh dalam beberapa waktu. Serangan tersebut berlanjut hingga beberapa bulan dan meluas ke ratusan bank, perusahaan, serta lembaga pemerintah lainnya di Ukraina (BBC News, 2014).

Perbankan di Ukraina menjadi sasaran utama serangan siber karena bank menyimpan banyak data penting dan sensitif seperti informasi keuangan, nomor kartu kredit, data pribadi, dan informasi transaksi nasabah. Oleh karena itu, peretas sering kali menargetkan bank untuk mencuri informasi ini untuk tujuan keuangan, atau untuk digunakan dalam tindakan penipuan dan aktivitas kriminal lainnya. Dengan mengakses informasi tersebut, Rusia dapat melakukan pencurian identitas dan melakukan penipuan finansial, atau bahkan memindahkan dana ke rekening yang dikontrol oleh Rusia.

Perbankan menjadi kunci dalam infrastruktur keuangan suatu negara. Jika sistem perbankan rusak atau terhenti, akan dapat menyebabkan dampak ekonomi yang signifikan pada negara tersebut. Selain itu, Serangan siber pada sektor perbankan dapat menyebabkan kerusakan sistem perbankan secara keseluruhan yang dapat mempengaruhi kepercayaan nasabah

terhadap bank terdampak. Hal ini dapat memberikan keuntungan politik bagi Rusia. Dengan menargetkan perbankan Ukraina, Rusia dapat merusak roda perekonomian Ukraina dan mengganggu stabilitas politik di negara tersebut. Hal tersebut dapat memperkuat pengaruh Rusia di Ukraina dan mengurangi dukungan warga Ukraina terhadap pemerintahnya. Dengan melakukan serangan siber pada perbankan Ukraina, Rusia dapat memperoleh beberapa keuntungan yang signifikan. Sejauh ini, belum teridentifikasi adanya serangan siber balasan terhadap sektor perbankan Rusia yang dilakukan oleh Ukraina. Ukraina lebih banyak menjadi sasaran serangan siber Rusia.

Pada 13 Maret 2014, tiga hari sebelum referendum tentang status Krimea, Rusia meluncurkan serangan siber berupa serangan DDoS selama delapan menit yang ditujukan untuk mengacaukan jaringan komputer dan komunikasi Ukraina sebagai cara untuk mengalihkan perhatian publik dari



kehadiran pasukan Rusia di Krimea. Pada Mei 2014, sebelum pemilihan presiden Ukraina, kelompok peretas pro-Rusia, CyberBerkut, melakukan serangkaian serangan siber untuk memanipulasi pemungutan suara dengan cara melakukan infeksi malware melalui jaringan dan menghapus file dalam upaya untuk mengubah hasil pemilu dengan target Komisi Pemilihan Umum Pusat. Namun, serangan tersebut gagal karena *malware* telah dihapus 40 menit sebelum pemilihan (25 Mei 2014). Meskipun demikian, para peretas berhasil menunda penghitungan pemilu. Pada 23 Desember 2015, serangan DDoS menargetkan pusat panggilan dan jaringan tiga perusahaan distribusi energi Ukraina yang mengakibatkan lebih dari

230.000 konsumen di Ukraina barat mengalami pemadaman listrik mulai dari satu hingga enam jam. Kemudian, serangan siber serupa juga terjadi pada tahun 2016 dengan menargetkan gardu listrik Kyiv, namun serangan tersebut gagal menonaktifkan peralatan dan sistem listrik sepenuhnya. Meskipun demikian, serangan tersebut mengakibatkan pemadaman listrik selama satu jam.

Selain serangkaian serangan tersebut, pada tahun 2016 bermunculan insiden serangan siber lainnya yang dilaporkan oleh otoritas Ukraina dan diduga dilakukan oleh *threat actor* asal Rusia, termasuk serangan terhadap jaringan pemerintah dan militer Ukraina, serta upaya untuk mengganggu infrastruktur sistem energi dan transportasi. Selain sejumlah serangan siber, konflik ini juga melibatkan kampanye disinformasi dan upaya propaganda yang bertujuan untuk membentuk opini publik dan mempengaruhi hasil politik.

SERANGAN PADA PERIODE TAHUN 2016 SAMPAI 2021

Antara tahun 2016 sampai dengan tahun 2021, serangan siber di Ukraina terus meningkat. Serangan yang paling menonjol melibatkan peluncuran *Malware* NotPetyam yang dianggap sebagai serangan siber yang paling merusak dalam sejarah serangan siber di Ukraina, dimana *malware* disebarkan melalui perangkat lunak akuntansi pada Juni 2017. NotPetyam juga menargetkan pembangkit listrik tenaga nuklir Chernobyl dan hampir 13.000 perangkat yang digunakan oleh lembaga publik, bank, layanan pos, surat kabar, hingga infrastruktur transportasi dan bisnis. NotPetyam bekerja dengan menghapus seluruh data

yang terdapat dalam perangkat penyimpanan komputer kemudian menonaktifkan pemulihan data setelah *malware* melakukan enkripsi terhadap seluruh data. Selain menyerang Ukraina, NotPetyam juga menyerang 65 negara lain dan total sekitar 50.000 sistem, termasuk perusahaan Eropa dan AS FedEx, Maersk dan Merck, yang menimbulkan kerugian lebih dari US$10 miliar. Setelah serangan NotPetyam pada 2017, dua serangan siber besar lainnya terjadi pada tahun 2018 dan 2021. Yang pertama menargetkan stasiun penyulingan klorin Auly, yang beroperasi di 23 provinsi Ukraina. Sedangkan yang terakhir menargetkan *website* layanan keamanan Ukraina. Namun demikian, serangan siber dengan target sistem interaksi elektronik yang digunakan oleh badan eksekutif pemerintah tidak berhasil sepenuhnya dan hanya menimbulkan kegagalan layanan pada sistem tersebut.

FASE SEBELUM INVASI

Pada awal tahun 2022, upaya diplomatik antara Rusia dan Ukraina gagal meraih kesepakatan dan menimbulkan ketegangan pada pangkalan militer Rusia di sepanjang perbatasan antara kedua negara. Hal tersebut menyebabkan Rusia meluncurkan serangan *malware* ke Ukraina yang menandakan bahwa serangan siber Rusia telah memasuki fase destruktif dengan dimulainya upaya pengiriman *malware* Whispergate oleh APT Group Rusia DEV-0586. Berikut merupakan *timeline* serangan siber Rusia dikaitkan dengan isu politik-militer antara kedua negara.

DATE	POLITICAL MILITARY EVENTS	CYBER ATTACKS
13 Januari 2022	Dilakukannya diplomasi secara intensif antara Rusia, US, NATO, dan Ukraina	DEV-0586 mengembangkan *malware* WhisperGate guna menghambat kinerja infrastruktur IT dan pemerintahan di Ukraina
14 Januari 2022	-	DEV-0586 melakukan serangan *deface* dan DDoS ke beberapa *website* milik pemerintah Ukraina
1 Februari 2022	Presiden Putin menyampaikan bahwa US dan NATO menolak tuntutan keamanan Rusia.	-

DATE	POLITICAL MILITARY EVENTS	CYBER ATTACKS
15 – 16 Februari 2022	-	GRU melakukan serangan DDoS ke berbagai institusi keuangan Ukraina.
17 Februari 2022	Kremlin menyatakan akan menanggapi dengan langkah militer jika Amerika Serikat terus mengabaikan tuntutan dari Rusia	-
21 Februari 2022	Presiden Putin mengakui kemerdekaan daerah separatis Ukraina.	-
23 Februari 2022	-	APT Iridium mengembangkan *malware FoxBlade wiper* untuk menyerang ratusan sistem IT Ukraina di berbagai sektor.

Gambar 7. *Timeline* serangan siber saat invasi Rusia

FASE INVASI RUSIA KE UKRAINA

Pada 24 Februari 2022, saat Putin mengumumkan "operasi militer" kepada Ukraina, Serangan militer dilakukan di sejumlah kota sehingga media Barat menyebutnya sebagai invasi militer. Saat militer dan sipil Ukraina terus melawan invasi pasukan Rusia, jenis perang yang sangat berbeda (non fisik) juga terjadi di mandala perang yang berbeda, yakni internet. Perang siber menjadi mandala perang baru dalam invasi militer

Rusia ke Ukraina. Perusakan IIV, penonaktifan layanan pemerintahan, hingga ancaman psikologis dilakukan oleh state actor dan non-state actor Rusia tanpa kontak fisik secara nyata.

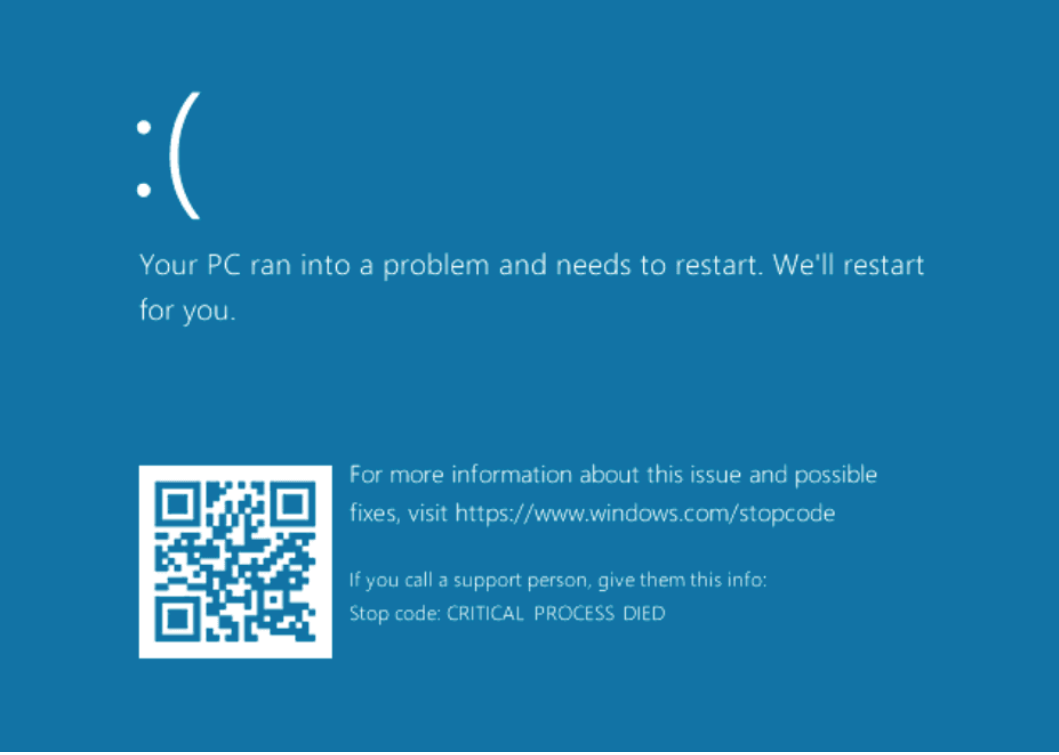
Berikut merupakan *timeline* serangan siber pada awal setelah invasi militer Rusia ke Ukraina:

Waktu	Jenis Serangan
Minggu Pertama (24 Februari - 2 Maret 2022)	*Destructive Malware* : FoxBlade, Lasainraw (Isaac Wiper), DesertBlade, *malicious use of SecureDelete utility*; Jumlah Insiden : 22
Minggu Kedua (3 - 9 Maret 2022)	*Destructive Malware* : - ; Jumlah Insiden : 0
Minggu Ketiga (10 - 16 Maret 2022)	*Destructive Malware* : FoxBlade, *malicious use of SecureDelete utility* ; Jumlah Insiden : 4
Minggu Keempat (17 - 23 Maret 2022)	*Destructive Malware* : DesertBlade, FiberLake, SonicVote, *malicious use of SecureDelete utility* Jumlah Insiden : 6
Minggu Kelima (24 - 30 Maret 2022)	*Destructive Malware* : FoxBlade, SonicVote, *malicious use of SecureDelete utility* Jumlah Insiden : 3
Minggu Keenam (31 Maret - 8 April 2022)	*Destructive Malware* : CaddyWiper, Industroyer2; Jumlah Insiden : 2

Gambar 8. *Timeline* saat awal serangan

Pada saat awal invasi militer Rusia ke Ukraina, terdapat beberapa serangan siber sebagai operasi pendahuluan sebelum operasi militer yang menargetkan Ukraina, diantaranya gangguan layanan sistem komunikasi Kyiv Post dan jaringan satelit KA-SAT satu jam sebelum invasi (24 Februari 2022), serangan IssacWiper terhadap situs web pemerintah (25 Februari 2022), serangan siber yang menargetkan stasiun kontrol perbatasan dengan tujuan mencegah pengungsi memasuki Rumania (25 Februari 2022) dan serangan terhadap infrastruktur digital Ukraina, memblokir akses ke layanan keuangan dan energi (28 Februari). Serangan siber yang menargetkan satelit KA-SAT berhasil mengakibatkan gangguan komunikasi individu dan entitas publik serta swasta Ukraina. Serangan siber berlanjut pada bulan Maret dengan adanya *malware* diluncurkan terhadap *website* pemerintah dan keuangan, serta organisasi non-pemerintah, serta lembaga amal dan bantuan, yang berhasil menghambat distribusi obat-obatan, makanan, dan pasokan bantuan ke Ukraina.

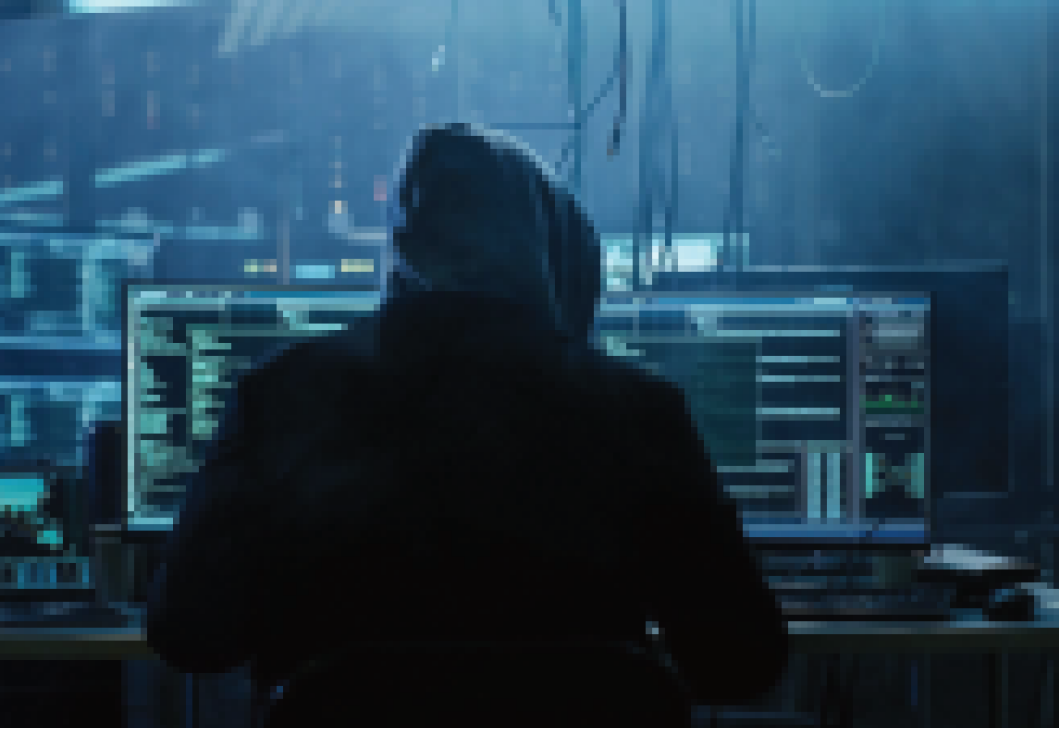
Dalam kasus lain, serangan siber Rusia melibatkan serangan *phishing* terhadap warga dan layanan pemerintah, serta serangan terhadap penyedia layanan telekomunikasi untuk mengganggu jaringan komunikasi Ukraina. Pada 14 Maret 2022, *malware CaddyWiper* menyusup ke sistem milik beberapa organisasi Ukraina, baik di sektor pemerintahan maupun keuangan. *CaddyWiper* adalah perangkat *malware* jenis *wiper* yang dirancang untuk menghapus data yang disimpan pada perangkat yang terinfeksi. Serangan tersebut termasuk serangan bermotif geopolitik yang menargetkan organisasi tertentu di Ukraina.



Gambar 9. Salah satu contoh dampak dari infeksi malware tipe wiper
(https://www.truesec.com/hub/blog/analysis-of-caddywiper-wiper-targeting-ukraine)

Penyebaran dan infeksi *malware* tersebut jelas merupakan elemen lain (siber) yang menjadi bagian dari perang di Ukraina. Infeksi *malware* tipe wiper dibuat untuk merusak sistem sehingga tidak dapat dioperasikan karena menghapus informasi penting dan berpotensi mengganggu ketersediaan layanan sehingga memiliki konsekuensi yang sangat menghancurkan.

Dua hari setelah serangan *CaddyWiper*, sebuah pesan palsu ditayangkan di saluran TV Ukraina, mengklaim bahwa Presiden Ukraina, Volodymyr Zelenskyy, telah meminta penduduk untuk menyerah. Selain itu, Video palsu Zelenskyy juga dibagikan melalui saluran Telegram untuk melengkapi pesan palsu yang ditayangkan melalui saluran TV (EPRS). Hal tersebut merupakan



bentuk upaya serangan siber lain (*hoax*) yang dilancarkan oleh Rusia terhadap Ukraina.

Memasuki kuartal akhir Maret 2022, serangan siber Rusia terhadap Ukraina dilancarkan dalam bentuk *email phishing* yang menargetkan pemerintah dan militer (17 Maret 2022) dan berbagai organisasi (18 Maret 2022), serta penggunaan *backdoor LoadEdge* untuk menginstal perangkat lunak mata-mata atau *spyware* (20 Maret 2022). Selanjutnya, serangan siber menargetkan situs Ukrtelecom dan WordPress yang menyebabkan putusnya konektivitas dan terbatasnya akses ke situs web keuangan dan pemerintah (28 Maret 2022).

Pada 30 Maret 2022, *malware* pencuri informasi, MarsStealer, menyebar di Ukraina dan berhasil mencuri kredensial pengguna milik warga dan organisasi di Ukraina. Serangan siber serupa juga berpotensi

menyebar dengan cepat ke negara lain. Pada 21 Maret 2022, Presiden AS, Joe Biden, mendesak para pemimpin bisnis AS untuk memperkuat kapasitas pertahanan siber mereka, sebagai implikasi risiko serangan siber Rusia terhadap Ukraina yang juga berpotensi menyerang negara maupun organisasi lain yang mendukung Ukraina. AS dan Uni Eropa telah mengambil sejumlah langkah untuk mendukung pertahanan siber Ukraina dan berupaya meningkatkan pertahanan sibernya sendiri. Pada bulan April 2022, peretas mencuri informasi sensitif dan kredensial pengguna dari pemerintah Ukraina (2 dan 7 April 2022) dan entitas media (7 April 2022). Selain itu, mereka juga mengenkripsi data perbankan dan pembayaran warga dengan bantuan *ransomware* (14 April 2022) serta membuat halaman survei media sosial palsu (19 April 2022). Serangan siber selanjutnya yaitu peretas berhasil menghentikan layanan pos Ukraina saat meluncurkan serangkaian surat terkait perang (22 April 2022).

3 Serangan Siber

SERANGAN DDOS RUSIA TERHADAP UKRAINA

Salah satu serangan siber pertama yang dimulai oleh Rusia terhadap Ukraina adalah serangan DDoS yang menyebabkan situs Kementrian Pertahanan Ukraina, PrivateBank, dan Oschadbank tidak berfungsi selama beberapa jam (CYBERINT). Selain itu, serangan DDoS juga menargetkan beberapa IIV Ukraina, memblokir akses ke layanan keuangan, melumpuhkan *website* beberapa departemen pemerintah, seperti Kabinet Menteri dan beberapa Kementerian, stasiun radio, serta stasiun energi selama beberapa jam yang dimulai pada pertengahan bulan Februari (EPRS).

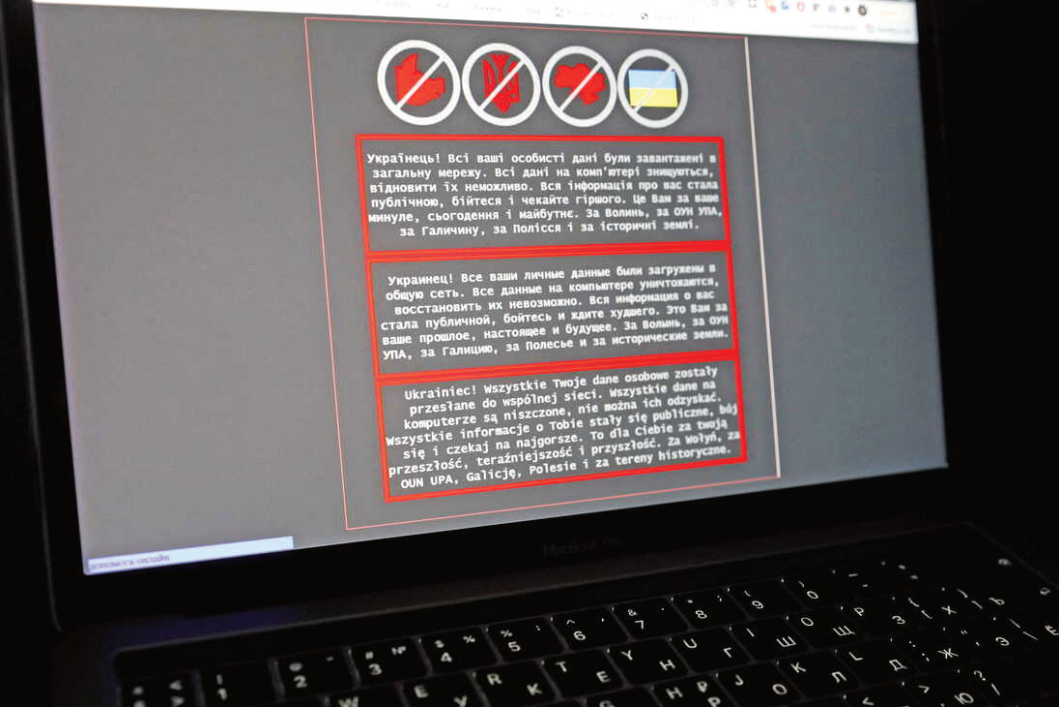
SERANGAN *MALWARE* RUSIA TERHADAP UKRAINA

Serangan *malware* Hermeticwiper yang menargetkan organisasi Ukraina melalui sistem Windows untuk melakukan penghapusan

data atau “wiper” diluncurkan terhadap 100 organisasi pada sektor keuangan, TI, dan penerbangan. Serangan siber ini sudah meningkat pada awal tahun 2022. Seperti pada tanggal 13 Januari 2022, Microsoft melaporkan bahwa malware terdeteksi menargetkan pemerintah Ukraina dan beberapa organisasi nirlaba dan Teknologi Informasi (EPRS). Beberapa *malware* destruktif yang diidentifikasi menargetkan Ukraina yaitu WhisperGate / WhisperKill, FoxBlade, SonicVote, CaddyWiper, DesertBlade, Industroyer2, Lasainraw, dan FiberLake (DoubleZero).

CYBER INFLUENCE OPERATIONS RUSIA TERHADAP UKRAINA

Serangan siber Rusia terhadap Ukraina tidak hanya berbentuk serangan yang bersifat teknis dalam rangka dalam rangka merusak IIV dan melakukan *cyber espionage*, namun juga melakukan serangan dalam bentuk operasi khusus yang disebut dengan cyber influence. Tujuan dari operasi tersebut ialah untuk mendukung operasi dan penyerangan yang telah dilakukan serta memberikan pengaruh kepada pihak lain agar Rusia dapat menciptakan suatu kondisi tertentu yang diharapkan. Pelaksanaan operasi ini dilakukan melalui pemanfaatan teknologi informasi dan media sosial untuk menyebarkan berita dan informasi yang dikehendaki oleh Rusia. Operasi tersebut dapat berupa penyebaran beragam informasi, baik informasi yang dapat dipastikan maupun yang tidak dapat dipastikan kebenarannya (hoax), agar tercipta kondisi yang menguntungkan bagi pihak Rusia yang salah satu tujuannya yaitu untuk menghentikan



Gambar 10. A laptop screen displays a warning message in Ukrainian, Rusian and Polish that appeared on the official website of the Ministry of Foreign Affairs of Ukraine after a massive cyberattack. - Reuter

bantuan negara lain kepada Ukraina.

Operasi cyber influence bukan merupakan hal yang baru, operasi ini telah dilakukan oleh Rusia selama beberapa dekade untuk mempropagandakan informasi guna kepentingan negara. Rusia telah melakukan operasi ini sekitar tahun 1980-an, yang pada saat itu telah tersebar informasi di koran nasional India, The Patriots, yang tertulis bahwa "*AIDS may invade India: Mysterious disease caused by US experiments*". Adanya informasi tersebut dapat mempengaruhi kondisi global sehingga dapat menyebabkan *chaotic situation.* Setelah dilakukan penelusuran, terbukti bahwa informasi tersebut berelasi dan diciptakan oleh KGB, organisasi intelijen Rusia, dimana hal tersebut

membuktikan bahwa adanya operasi cyber influence dapat menjadi operasi yang sangat efektif untuk mempengaruhi kondisi global. Kekuatan informasi yang disebarkan di media massa pada saat itu telah memberikan pengaruh yang cukup besar. Jika dibandingkan dengan kondisi saat ini, maka dengan adanya operasi cyber influence yang memanfaatkan media internet dipastikan dapat memberikan dampak dan pengaruh yang jauh lebih besar jika dibandingkan dengan kondisi masa lalu yang hanya memiliki media penyebaran yang terbatas.

Operasi cyber influence yang dilaksanakan oleh Rusia merupakan kombinasi dari taktik tradisional dengan taktik modern yang memanfaatkan teknologi digital internet untuk memberikan pengaruh ke pihak asing yang lebih luas, baik ditinjau dari jangkauan geografis, target, dan kecepatan penyebaran informasi. *Cyber influence* difokuskan pada empat

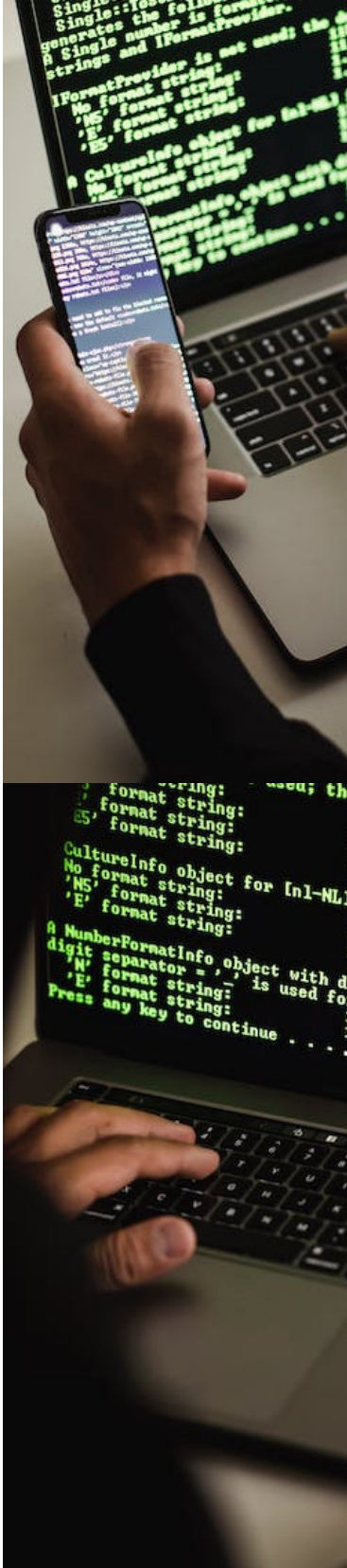
pihak yang berbeda. Pihak yang pertama yaitu internal penduduk Rusia, yang bertujuan untuk membangkitkan semangat nasionalisme dan memberikan kepercayaan bahwa Rusia akan unggul dan dapat meraih kemenangan. Pihak yang kedua yaitu penduduk Ukraina dengan tujuan untuk merusak kepercayaan mereka terhadap negaranya sendiri sehingga dianggap tidak mampu untuk menahan serangan Rusia lebih lama lagi. Pihak yang ketiga yaitu penduduk Amerika dan Eropa, yang bertujuan untuk mengurangi persatuan pihak Barat dalam memberikan bantuan ke Ukraina serta membelokkan kritik atas kejahatan perang yang dilakukan oleh Rusia. Pihak yang keempat yaitu untuk pihak-pihak yang tidak berelasi dengan perang ini (negara-negara Non-blok), agar negara-negara tersebut dapat membela dan lebih mempercayai Rusia di kancah internasional dan di lingkup Perserikatan Bangsa Bangsa (PBB) serta memberikan keyakinan bahwa adanya konflik ini merupakan kesalahan dari pihak Ukraina dan negara-negara barat.

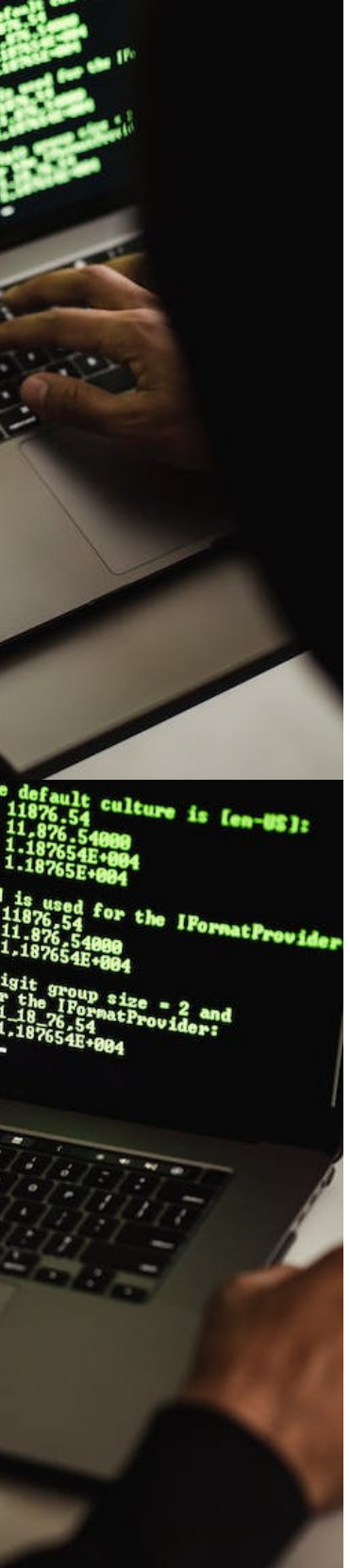
SERANGAN SIBER DENGAN MEDIA SOSIAL

Perang siber tidak hanya sebatas perang antara para peretas dari masing masing negara yang berusaha merebut dan mempertahankan IIV masing masing negara, namun juga merambah ke ranah media sosial. Hal ini dibuktikan dengan banyaknya pengguna media sosial, seperti Twitter, yang berasal dari Rusia dan Ukraina melakukan propaganda dan mencari pembenaran bagi aktivitas yang dilakukan masing-masing negara. Bahkan kepala negara Ukraina Volodymyr Zelenskyy, menggunakan sosial media sebagai salah

satu senjatanya dalam melakukan diplomasi dengan menunjukkan apa yang dia lakukan demi negaranya serta melakukan propaganda untuk mengobarkan semangat warga Ukraina. Hal ini juga diikuti oleh Departemen Pertahanan Ukraina yang selalu melakukan posting setiap kemenangan yang diraih oleh pasukan Ukraina di medan perang. Warga Ukraina juga membantu pasukan negaranya yang sedang berjuang dengan mencari lokasi pasukan Rusia yang melakukan posting saat perang dengan melakukan *tracing* melalui fitur *geotagging* di media sosial VK.

Bagi Ukraina, penggunaan sosial media sebagai media penyebaran informasi dan propaganda berhasil mendapatkan simpati dari dunia dan membantu Ukraina mendapatkan bantuan yang mereka butuhkan. Bantuan yang berhasil disalurkan seperti amunisi, persenjataan, logistik, dan dukungan internasional tersebut tidak terlepas dari strategi perang siber melalui media sosial yang dijalankan oleh pemerintah Ukraina secara efektif. Hal





tersebut memperlihatkan bahwa perang modern saat ini tidak hanya bergantung pada kualitas pasukan, senjata, taktik, ataupun strategi bertempur di medan perang konvensional.

Serangan siber yang dilakukan kedua belah pihak, baik melalui sosial media maupun dengan serangan siber destruktif menggunakan metode *hacking* dan *malware*, memiliki peran yang penting dalam perang antara Rusia dan Ukraina. Bagi Rusia, serangan siber yang terjadi pada Rusia sangatlah menguntungkan di saat Rusia tengah terdesak oleh Ukraina dengan bantuan dari Amerika Serikat dan NATO, entah serangan itu dilakukan oleh Rusia sendiri ataupun oleh pihak lain.

NON-STATE ACTOR

Perang antara Rusia dan Ukraina yang sedang berlangsung saat ini merupakan perang antara dua negara besar yang terjadi setelah perang dingin. Wilayah Rusia dan Ukraina,

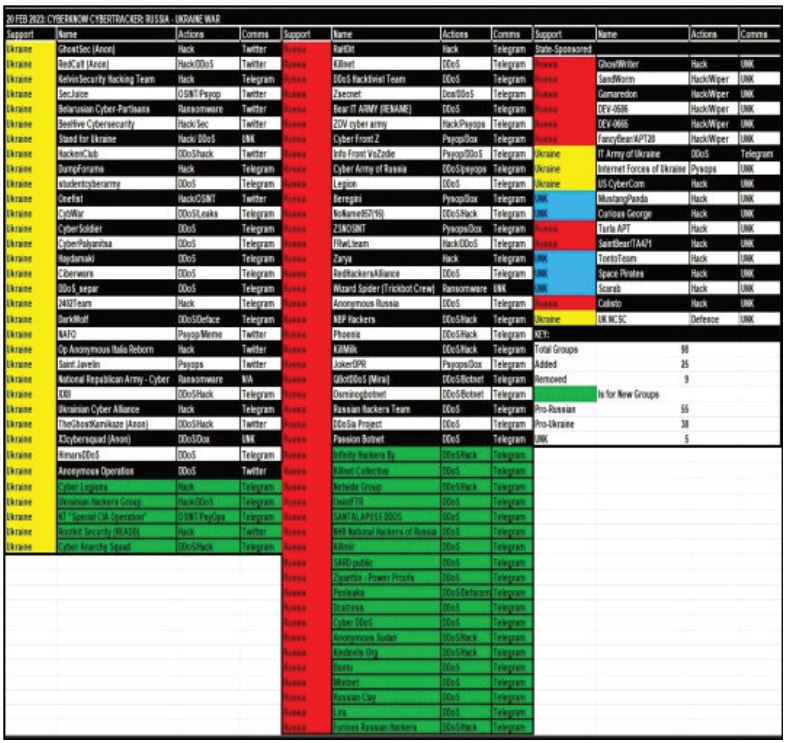
demografi, kekuatan nasional yang komprehensif, dan pengaruh geopolitiknya (dikombinasikan dengan keterlibatan kolektif negara-negara Barat yang luas) memberikan warna yang kental pada konflik Rusia dan Ukraina sebagai pertikaian dan perang antar negara besar. Sementara itu, kelompok kepentingan non-state actor telah memainkan peran penting dalam konflik dan memperumit interaksi dengan aktor-aktor negara. Karakteristik yang mencolok dari jenis konflik internasional yang baru telah muncul, dimana non-state actors telah memainkan peran sebagai pengganggu.

Kapitalis internasional terkemuka, entitas teknologi kecil dan menengah, serta platform internasional yang sedang berkembang, semuanya telah memanfaatkan kekuatan mereka untuk terlibat dalam proses konflik serta permainan diplomatik yang sesuai. Elon Musk, secara terbuka memihak dan mendukung Ukraina pada awal konflik dengan menyediakan layanan internet bagi masyarakat Ukraina menggunakan sistem Starlink miliknya. Oligarki Rusia, Roman Abramovich, bahkan secara langsung memainkan peran sebagai mediator, berpartisipasi dalam negosiasi antara Rusia dan Ukraina dengan bertindak sebagai kurir yang harus melaksanakan perjalanan dari Moskow dan Kyiv dan sebaliknya.

Selama beberapa dekade terakhir, non-state actor telah memainkan peran penting dalam komunitas internasional, namun hanya ada beberapa kasus dimana mereka secara langsung dan mencolok terlibat dalam urusan internasional yang signifikan, seperti dalam perang Rusia-Ukraina. Intervensi non-state actor dalam Perang Rusia-Ukraina, terutama dalam ranah siber, tidak hanya secara signifikan

memperluas ruang pertempuran, tetapi juga telah menciptakan perubahan dalam terminologi perang.

Hingga akhir Februari 2023, baik pihak Rusia maupun Ukraina beserta Non-state Actor terus melakukan cyber attack yang diantaranya adalah melakukan kegiatan Distributed Denial of Services (DDoS), web defacement, hacking activity, Botnet, Ransomware, Doxing, wiper, hingga Operasi Psikologi yang dilakukan oleh total 98 grup atau threat actor dengan rincian 55 threat actors pro Rusia, 55 threat actors pro Ukraina, dan 5 threat actors yang belum



Gambar 11. Daftar Non-state actor pendukung Rusia dan Ukraina

Gambar 12. Threat actor serta kemampuan siber pendukung Rusia - Ukraina

diketahui keberpihakannya (unknown). Dari data, diketahui pula bahwa sebagian besar threat actor yang mendukung Rusia sebagian besar merupakan threat actor yang berafiliasi atau berasal dari negara Cina serta Korea Utara. Sedangkan threat actor yang mendukung Ukraina sebagian besar merupakan threat actor yang berafiliasi atau berasal dari negara-negara yang tergabung dalam NATO.

ANONYMOUS

Anonymous berasal dari komunitas *hacker* yang melakukan kegiatan *hacktivist* dan tersebar di berbagai belahan dunia, dimana sering kali memiliki motif ideologis atau politik. *Anonymous* terkenal karena kerap kali melakukan serangan siber sebagai bentuk protes terhadap kebijakan atau praktik yang dianggap merugikan masyarakat atau kelompok tertentu. Kelompok ini memiliki ciri khas yaitu menggunakan masker *Guy Fawkes* yang

juga dijadikan lambang identitas mereka. Media sosial dan *website defacement* digunakan untuk menyebarkan pesan mereka, serta memobilisasi dukungan publik untuk tujuan mereka. Perang Rusia - Ukraina telah menyebabkan kebangkitan kembali *cyber militancy* dan rekrutan baru untuk Anonymous.

Anonymous "menyatakan perang" terhadap pemerintah Rusia pada tanggal 1 Maret 2022 dan mengklaim telah melumpuhkan situs-situs yang dikelola oleh media milik pemerintah Rusia. *Anonymous* teridentifikasi telah menargetkan outlet media pro-Rusia dan juga mengklaim telah meretas beberapa stasiun penyiaran utama Rusia, termasuk saluran televisi milik pemerintah, yaitu Rusia 24, Channel 1, Moscow 24, dan layanan streaming Wink dan Ivi. Program pada layanan-layanan kantor berita tersebut terganggu oleh klip-klip perang di Ukraina. Pada 10 Maret 2022, Anonymous

mengumumkan bahwa mereka telah membobol sistem Roskomnadzor, lembaga Rusia yang bertanggung jawab untuk memantau dan melakukan sensor terhadap media. Selain itu, *Anonymous* juga mengklaim telah membocorkan lebih dari 360.000 file milik Rusia, termasuk panduan tentang bagaimana strategi melaksanakan invasi ke Ukraina. Perang di Ukraina tidak hanya terjadi di ranah fisik, tetapi juga melibatkan kombinasi ancaman siber yang unik. Dalam konteks perang, menurut Cyber Peace Institute terdapat ada 8 (delapan) ancaman siber dominan yang terkadang digunakan untuk merusak, mengganggu, memberikan informasi yang tidak benar, dan mempersenjatai data:

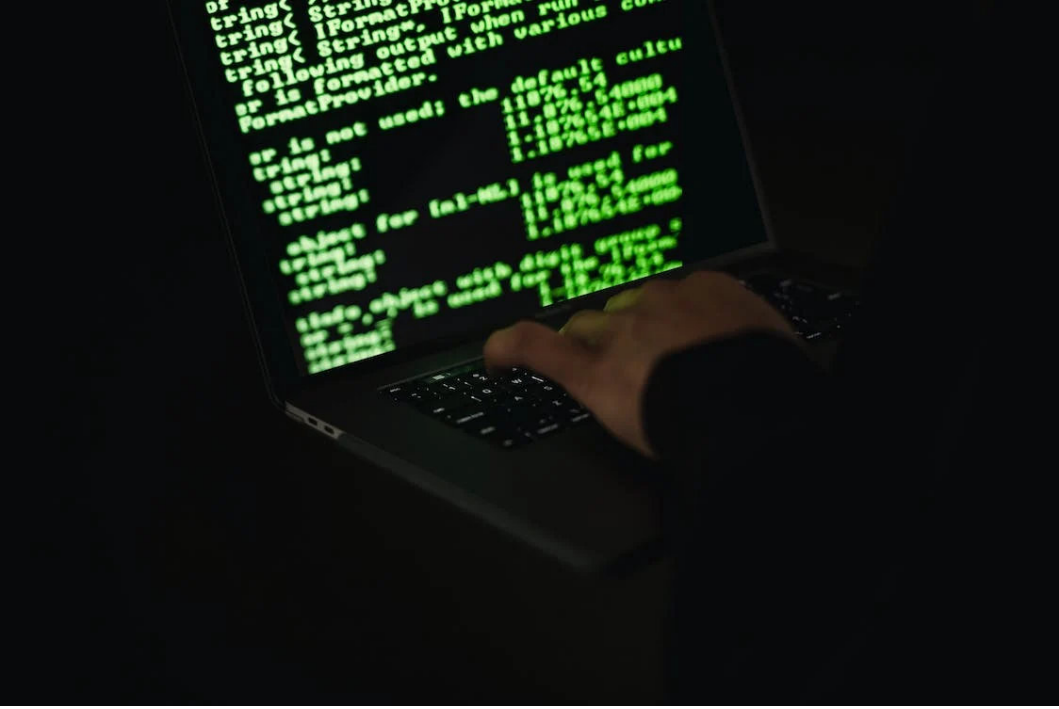
1. *Malware* mencakup segala jenis perangkat lunak yang mengganggu atau berbahaya yang dirancang untuk merusak, menghancurkan, atau menumbangkan sistem komputer. *Wiper*, *ransomware*, dan *spyware* adalah bentuk-bentuk *malware*.

2. *Distributed Denial-of-Service/DDos* - Serangan Penolakan Layanan Terdistribusi terdiri dari membanjiri jaringan, layanan, atau server dengan lalu lintas yang berlebihan untuk mencegahnya berfungsi secara normal. Dikatakan terdistribusi ketika sumber serangan terdiri dari beberapa sistem komputer. Dalam konteks konflik bersenjata, serangan DDoS telah digunakan untuk mengganggu akses ke informasi, keuangan, dan bahkan bantuan kemanusiaan.

3. *Defacement* - Perusakan mencakup modifikasi konten pada sistem internal atau sistem yang berhadapan dengan publik (biasanya situs web). Selama perang, situs web, terutama milik institusi pemerintah sering kali diubah untuk

menampilkan pesan disinformasi atau propaganda. Serangan semacam itu berusaha mempengaruhi dengan mendistorsi atau mengubah informasi, menyebarkan disinformasi dan mempengaruhi opini publik dalam perang.

4. *Cyber enabled information operations* - Operasi informasi yang didukung siber mencakup serangan siber apa pun yang dilakukan untuk menanam/menyebarkan (dis-) informasi atau untuk tujuan informasi lainnya. Serangan peretasan dan pembocoran adalah jenis operasi informasi yang didukung siber. Selama perang, operasi informasi yang diaktifkan di dunia maya sering kali melibatkan kompromi dan penanaman disinformasi atau propaganda. UNC1151 alias GhostWriter adalah aktor ancaman terkemuka yang melakukan serangan semacam itu dalam perang dan telah dikaitkan dengan serangan phishing pada akun personel militer Ukraina dan individu lainnya.



5. *Hack and leak* - Serangan peretasan dan pembocoran mencakup pencurian dan pembocoran data untuk tujuan politik atau ideologis. Data yang bocor sering kali dimanipulasi atau disajikan dengan cara yang menyesatkan. Dalam konteks perang, pencurian dan pembocoran data (termasuk *doxxing*) terutama dilakukan oleh apa yang disebut sebagai kelompok hacktivist. Kebocoran data dan informasi dari institusi dan organisasi menebarkan ketidakpercayaan, menunjukkan ketidakmampuan untuk mengamankan data sensitif, dan berpotensi menempatkan individu dalam risiko.

6. *Cyberespionage* - Spionase siber mencakup infiltrasi sistem dan eksfiltrasi data untuk mendapatkan informasi rahasia dari suatu target. Aktor-aktor negara-bangsa telah terlibat dalam spionase siber sebagai bagian dari konflik, misalnya untuk mengumpulkan informasi

taktis sebelum serangan kinetik.

7. *Ransomware* adalah jenis malware yang digunakan untuk mengenkripsi data dan/atau sistem target untuk memeras uang tebusan sebagai imbalan atas kunci dekripsi. Ransomware telah berkembang menjadi salah satu ancaman kriminal siber yang paling dominan dan canggih. Karena kemampuan dan ketersediaannya yang mengganggu, ransomware telah digunakan sebagai alat untuk mengganggu sistem musuh, termasuk layanan kereta api di Belarus.

8. *Wiper* adalah sebuah bentuk malware yang dikembangkan untuk menghapus atau mengenkripsi data secara permanen pada sistem yang terinfeksi. Serangan wiper sering kali dibuat agar terlihat seperti serangan ransomware yang bermotif finansial, tetapi berbeda karena tidak ada niat untuk mendekripsi atau memulihkan data yang dihancurkan. Jenis malware penghapus data yang signifikan telah diidentifikasi menargetkan entitas dan organisasi Ukraina sesaat sebelum dan selama konflik. Serangan-serangan ini terutama digunakan untuk menyerang lembaga-lembaga publik, perusahaan-perusahaan keuangan dan energi, serta penyedia layanan telekomunikasi dengan tujuan untuk mengganggu kehidupan sehari-hari, dan akses mereka ke layanan-layanan penting.

“Cyber war takes place largely in secret, unknown to the general public on both sides.”

— Noah Feldman

4 ANALISIS PERANG SIBER RUSIA UKRAINA TERHADAP INDONESIA

Dalam buku *Cyber Warfare and Cyber Terrorism; Cyber Warfare* atau perang siber bisa disebut sebagai perang informasi, yang didefinisikan sebagai serangan terencana oleh negara atau agen mereka terhadap informasi dan sistem komputer, program komputer, dan data yang mengakibatkan kerugian musuh. Menurut Peraturan Menteri Pertahanan Republik Indonesia (Permenhan) No. 82 tahun 2014 tentang Pedoman Pertahanan Siber, mendefinisikan perang siber sebagai semua tindakan yang dilakukan dengan tujuan mengganggu kedaulatan negara. Kemudian serangan siber didefinisikan sebagai segala bentuk perbuatan, perkataan, pemikiran baik yang dilakukan dengan sengaja maupun tidak sengaja oleh pihak mana

pun, dengan motif dan tujuan apa pun, yang dilakukan di lokasi mana pun, yang disasarkan pada sistem elektronik atau muatannya (informasi) maupun peralatan yang sangat bergantung pada teknologi dan jaringan dalam skala apa pun, terhadap obyek vital maupun nonvital dalam lingkup militer dan nonmiliter, yang mengancam kedaulatan negara, keutuhan wilayah dan keselamatan bangsa. Serangan siber yang umum terjadi di antaranya menggunakan *malware, SQL Injection, DDoS, defacement, trojan horse, password cracking, phising, spoofing,* dll.

Perang Rusia dan Ukraina sangatlah kompleks dan memiliki banyak aspek karena beberapa alasan. Pertama, konflik ini memiliki konteks sejarah yang panjang, dimana Rusia dan Ukraina memiliki hubungan

yang kompleks dan sering kali bersitegang sejak berabad-abad yang lalu. Konteks historis ini telah berkontribusi pada munculnya identitas nasional yang berbeda, perbedaan bahasa dan budaya, serta sengketa wilayah yang telah memainkan peran dalam konflik saat ini.

Kedua, konflik ini melibatkan berbagai faktor geopolitik, dimana Rusia dan Ukraina saling berusaha untuk menggunakan pengaruhnya atas wilayah tersebut dan sumber dayanya. Hal ini telah menyebabkan perebutan kekuasaan antara kedua negara, dimana Ukraina berusaha untuk menyelaraskan dirinya lebih dekat dengan Eropa Barat dan Rusia berusaha untuk mempertahankan pengaruhnya di wilayah tersebut. Ketiga, konflik ini diperburuk oleh kampanye propaganda dan disinformasi dengan kedua belah pihak menggunakan media dan *platform online* untuk menyebarkan pesan mereka dan memanipulasi opini publik. Hal ini telah berkontribusi pada iklim politik yang terpolarisasi di kedua negara, sehingga sulit untuk menemukan resolusi damai dalam konflik tersebut.

Dampak lain dari perang siber terhadap keamanan siber adalah perlunya peningkatan pembagian informasi dan kolaborasi di antara pemerintah dan pakar keamanan siber. Serangan di Ukraina telah menunjukkan perlunya respons terkoordinasi terhadap ancaman siber, serta pentingnya berbagi informasi dan praktik terbaik dalam konteks keamanan siber di antara negara-negara (Eichensehr, 2022).

Perang siber antara Ukraina dan Rusia telah menyoroti perlunya investasi yang lebih besar dalam penelitian dan pengembangan keamanan siber. Peningkatan investasi

dalam penelitian dan pengembangan keamanan siber dapat membantu meningkatkan ketahanan negara dalam rangka menghadapi kemunungkinan ancaman dan serangan siber. Perang siber antara Ukraina dan Rusia memiliki dampak signifikan terhadap keamanan siber secara global, termasuk di Indonesia. Meningkatnya kesadaran akan potensi serangan siber terhadap IIV, kebutuhan untuk berbagi informasi dan kolaborasi yang lebih baik, serta kebutuhan akan investasi yang lebih besar dalam penelitian dan pengembangan keamanan siber merupakan faktor penting yang perlu dipertimbangkan oleh Indonesia dalam mengembangkan kemampuan keamanan siber.

5 LESSON LEARNED

Perang siber telah memberikan dampak yang signifikan terhadap keamanan siber secara global, termasuk Indonesia. Salah satu dampak utama perang siber terhadap keamanan siber adalah meningkatnya kesadaran akan potensi serangan siber terhadap IIV. Seiring dengan pesatnya perkembangan dan modernisasi teknologi, kebutuhan akan langkah-langkah keamanan siber yang efektif menjadi semakin mendesak. Serangan terhadap jaringan listrik Ukraina, misalnya, menunjukkan potensi serangan siber yang dapat menyebabkan gangguan dan kerusakan secara masif dan meluas. Serangan siber dapat juga menyerang sumber tenaga listrik suatu negara, peretasan akses perbankan, pengalihan isu publik, manipulasi data, maupun seluruh sendi kehidupan lainnya yang berhubungan dengan teknologi.

Perang siber yang terjadi di Rusia dan Ukraina menunjukkan semakin pentingnya keamanan siber pada era modern. Hal tersebut dapat disebabkan oleh

pertama, ketika negara menjadi lebih bergantung pada teknologi dan sistem digital, negara tersebut menjadi semakin rentan terhadap serangan siber yang dapat menyebabkan gangguan secara nyata dan meluas serta dapat merusak informasi sensitif. Kedua, perang siber dalam konflik antara Rusia dan Ukraina menyoroti pentingnya kerja sama internasional dalam mengatasi ancaman keamanan siber. Konflik antara Rusia dan Ukraina bukan hanya masalah bilateral, namun juga harus mendapat perhatian dan memiliki dampak secara global. Penggunaan senjata dalam ruang siber berpotensi menyebabkan kerugian bagi negara dan organisasi lain. Hal yang perlu dilakukan adalah menetapkan kerja sama internasional dalam mengatasi ancaman keamanan siber, termasuk pengembangan pertaturan dan perjanjian umum untuk perilaku negara yang bertanggung jawab di ruang siber.

Terakhir, perang siber dalam konflik antara Rusia dan Ukraina menunjukkan pentingnya pertahanan keamanan siber yang baik dimiliki suatu negara. Hal ini berarti bahwa suatu negara bukan hanya cukup berfokus pada solusi teknis untuk melindungi sistem dan jaringan mereka, namun juga penting untuk mengembangkan strategi dalam mengatasi faktor politik dan ekonomi yang mendasari serangan siber tersebut. Selain itu, adanya peraturan yang mengatur tentang pelanggaran hukum dengan menggunakan peralatan atau senjata siber pada suatu negara maupun internasional juga menjadi hal yang penting dalam rangka mengantisipasi dan mengatasi hal serupa yang terjadi di Ukraina kembali terjadi pada negara lain.

Kemampuan siber mengacu pada kemampuan suatu negara untuk melakukan operasi di dunia maya, yang mencakup segala sesuatu mulai dari bertahan dari serangan siber hingga melakukan operasi siber ofensif. Kemampuan siber dapat mencakup berbagai peralatan dan teknologi yang berbeda, serta personel dengan keterampilan dan pelatihan khusus. Beberapa komponen utama kemampuan siber diantaranya meliputi:

1. Pertahanan siber: Mengacu pada kemampuan suatu negara untuk melindungi IIV dari serangan siber. Hal ini dapat melibatkan kesatuan holistik yang komprehensif, baik teknologi, Sumber Daya Manuasi (SDM), hingga tata kelola pertahanan siber yang baik.

2. Ofensif siber: Mengacu pada kemampuan suatu negara untuk melakukan operasi siber ofensif, seperti meretas jaringan musuh dan mencuri informasi, mengganggu sistem penting, atau melakukan

serangan yang menyebabkan kerusakan dan dampak secara fisik.

3. Intelijen siber: Mengacu pada kemampuan suatu negara untuk mengumpulkan informasi tentang kemampuan dan aktivitas siber negara lain, serta menganalisis data untuk mengidentifikasi potensi ancaman yang berasal dari lawan maupun bakal lawan.

4. Personel siber: Mengacu pada SDM dengan keterampilan dan pelatihan khusus yang diperlukan untuk melaksanakan operasi siber, baik pertahanan siber maupun siber ofensif. Kemampuan SDM tersebut antara lain kemampuan *programming, networking, cybersecurity, ethical hacking, threat intelligence,* maupun kemampuan lainnya yang mendukung operasi siber.

5. Kebijakan dan strategi dalam bidang siber: Mengacu pada pendekatan komprehensif suatu negara terhadap operasi siber, termasuk kebijakan tentang beberapa permasalahan seperti spionase siber, perang siber, serta norma dan standar hukum internasional dalam bidang siber.

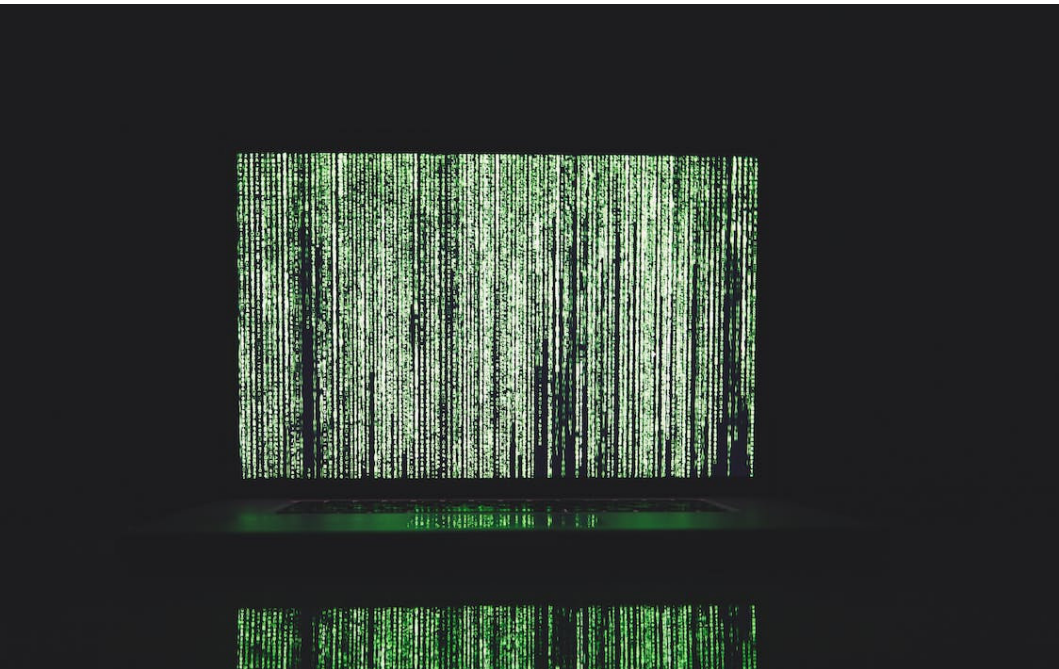
Perang siber antara Rusia dan Ukraina memberikan pelajaran akan pentingnya langkah-langkah keamanan siber yang kuat untuk melindungi keberlangsungan IIV dan keamanan nasional. Indonesia kiranya dapat mengambil beberapa pelajaran dari perang siber yang terjadi pada perang Rusia - Ukraina, dalam rangka meningkatkan langkah-langkah pencegahan terhadap ancaman siber. Beberapa hal yang dapat diambil sebagai pelajaran tersebut antara lain:

1. Indonesia perlu memperkuat infrastruktur keamanan sibernya, termasuk teknologi, SDM, kerangka hukum,

kebijakan, dan peraturan. Indonesia perlu memberlakukan undang-undang keamanan siber yang komprehensif yang mendefinisikan peran dan tanggung jawab lembaga pemerintah, entitas swasta, dan pengguna individu (Putra, 2020). Undang-undang ini harus mencakup ketentuan untuk pelaporan insiden, perlindungan data, dan perlindungan infrastruktur penting.

2. Indonesia perlu berinvestasi dalam pendidikan dan kesadaran keamanan siber. Pendidikan keamanan siber harus diintegrasikan ke dalam sistem pendidikan nasional dan harus menargetkan masyarakat umum, bisnis, dan lembaga pemerintah (Kurniawan, 2019). Hal ini akan membantu mengurangi risiko serangan siber melalui kesalahan manusia dan meningkatkan kesadaran akan pentingnya keamanan siber sehingga semakin banyak warga negara indonesia yang memiliki kesadaran keamanan siber.

3. Indonesia harus mendorong pengembangan industri



keamanan siber lokal. Indonesia harus berinvestasi dalam penelitian dan pengembangan teknologi keamanan siber, termasuk Artificial Intelligence (AI) dan pembelajaran mesin atau machine learning, untuk meningkatkan deteksi dan respons terhadap berbagai macam ancaman siber (Muliawan, 2020). Hal ini akan membantu meningkatkan kemampuan keamanan siber Indonesia serta mengurangi ketergantungan Indonesia terhadap produk keamanan siber asing.

Indonesia harus memperkuat kolaborasi internasional dan berbagi informasi tentang masalah keamanan siber (Reksoprojo, 2020). Hal ini akan memungkinkan Indonesia untuk bertukar dan belajar dari pengalaman negara lain, serta mampu membangun kemitraan yang efektif untuk memerangi ancaman dan serangan siber.

6 TANTANGAN BAGI INDONESIA

Keamanan siber menjadi penting bagi sebuah negara karena tidak ada batas kedaulatan dalam siber dan konflik yang lebih banyak dipelopori oleh aktor non-negara (Pratiwi 2019). Mengantisipasi ancaman siber di masa depan merupakan tugas penting bagi negara dan didukung oleh semua pihak guna memastikan stabilitas IIV dan keamanan negara dapat terwujud. Belajar dari perang siber antara Rusia dan Ukraina, beberapa tantangan dapat diidentifikasi untuk mengantisipasi ancaman siber di masa yang akan datang bagi Indonesia.

Pertama, ancaman siber terus berkembang dan bertransformasi menjadi lebih canggih. Para penyerang sering kali menggunakan taktik, teknik, dan prosedur baru, sehingga sulit untuk memprediksi langkah mereka selanjutnya. Dalam perang Rusia dan Ukraina, para aktor siber Rusia menggunakan berbagai taktik dan teknik, termasuk *spear-phishing, malware*, dan serangan DDoS, yang menyulitkan Ukraina untuk mempertahankan diri (Eichensehr, 2022).

Kedua, kurangnya sistem pembagian intelijen ancaman yang komprehensif dan mutakhir merupakan tantangan signifikan dalam mengantisipasi ancaman siber (Condra, 2019). Indonesia perlu membangun kemitraan antara pemerintah dan sektor swasta yang kuat dan mekanisme pembagian intelijen terpusat untuk menyediakan informasi ancaman yang tepat waktu dan relevan. Sistem semacam itu dapat membantu negara dalam mengantisipasi ancaman siber dan mengambil tindakan pencegahan sebelum terjadinya serangan siber.

Ketiga, kurangnya tenaga profesional di bidang keamanan siber yang terampil merupakan tantangan global yang juga berdampak pada Indonesia. Untuk mengantisipasi dan memitigasi ancaman siber, Indonesia membutuhkan tenaga kerja dengan keterampilan dan pengetahuan yang diperlukan untuk mengatasi ancaman siber.

Indonesia membutuhkan Sumber Daya Manusia (SDM) yang berkualitas, unggul dan maju untuk menjawab tantangan perkembangan teknologi di masa depan. Pada era industri 4.0, SDM harus dilihat sebagai aset (*human capital*) dibandingkan sekedar sumber daya (*human resource*). Sebagai suatu aset, perlu dibangun ekosistem pengembangan SDM yang kondusif, terarah, berkelanjutan dan terukur. Di bidang Keamanan Siber, SDM merupakan aset kunci. Keamanan Siber tidak akan terwujud tanpa adanya SDM yang mumpuni dalam pelaksanaannya. Upaya yang harus dilakukan adalah menyediakan pendidikan dan pelatihan yang relevan untuk membangun tenaga kerja keamanan siber yang terampil dan kompeten

(Rahmani, 2018) serta dengan menerapkan ekosistem pengembangan SDM di bidang Keamanan Siber melalui penyiapan Peta Okupasi dan Standar Kompetensi Kerja.

Keempat, kurangnya kesadaran dan kesiapan di kalangan masyarakat umum dan Usaha Mikro Kecil dan Menengah (UMKM) terkait keamanan siber merupakan tantangan signifikan lainnya dalam mengantisipasi ancaman siber (UNCTAD, 2021). Sebagian besar UMKM di Indonesia tidak memiliki sumber daya manusia yang mumpuni dan berkompetensi dalam bidang keamanan siber sehingga mereka rentan terhadap serangan siber. Untuk itu, diperlukan upaya peningkatan kesadaran keamanan siber sehingga dapat meminimalisir dan membantu UMKM untuk melindungi IIV mereka sendiri.

7
PENUTUP

Dampak perang siber dapat menjadi signifikan, karena dapat mengganggu infrastruktur penting, menyebabkan kerusakan finansial, membahayakan informasi sensitif, bahkan menyebabkan kerusakan fisik atau hilangnya nyawa dalam beberapa kasus. Karena alasan ini, perang siber menjadi perhatian pemerintah, organisasi militer, dan sektor bisnis di seluruh dunia, yang berinvestasi dalam langkah-langkah keamanan siber untuk melindungi dari potensi serangan. Kemampuan siber menjadi aspek yang semakin penting dari keamanan nasional bagi banyak negara, dan kemungkinan akan terus bertambah penting di tahun-tahun mendatang. Berkaca dari konflik Rusia dan Ukraina, perang siber menjadi mandala pertempuran baru di era modern ini, yang mampu memberikan dampak kerugian besar bagi Ukraina. Dampak yang ditimbulkan dari perang siber bisa jauh lebih besar daripada dampak perang konvensional. Oleh karena itu, sudah seharusnya setiap negara termasuk Indonesia mempersiapkan diri serta

membuat infrastruktur keamanan siber yang kuat dan komprehensif untuk menghadapi segala jenis serangan siber.

Perang Rusia dan Ukraina dapat menjadi pengingat bagi negara di seluruh dunia bahwa perang, baik kecil ataupun besar, terdahulu hingga terbaru, konvensional maupun modern (perang siber), tetaplah sebuah perang yang sudah pasti menciptakan kesedihan dan duka mendalam bagi semua pihak. Sun Tzu, seorang jenderal strategi militer dan filsuf yang hidup masa Tiongkok Kuno, pernah mengatakan bahwa "Belum pernah ada perang yang berlarut-larut yang menguntungkan suatu negeri".

DAFTAR PUSTAKA

Kementerian Pertahanan Republik Indonesia. (2014). *PERATURAN MENTERI PERTAHANAN REPUBLIK INDONESIA NOMOR 82 TAHUN 2014 TENTANG PEDOMAN PERTAHANAN SIBER*. Jakarta: Kementerian Pertahanan Republik Indonesia .

CSO. (2022, August 24). *Russia-linked cyberattacks on Ukraine*: A timeline. Retrieved from CSO: https://www.csoonline.com/article/3647072/a-timeline-of-russian-linked-cyberattacks-on-ukraine.html?page=3

Defence of Ukraine. (n.d.). Twitter. Retrieved from Defence of Ukraine(@DefenceU) /https://twitter.com/DefenceU

Priyono, U. (2022). CYBER WARFARE AS PART OF RUSSIA AND UKRAINE CONFLICT. *Jurnal Diplomasi Pertahanan*, 45-59.

Reuters. (2021, July 27). Biden: If U.S. has 'real shooting war' it could be result of cyber attacks. Retrieved from Reuters: https://www.reuters.com/world/biden-warns-cyber-attacks-could- lead-a-real-shooting-war-2021-07-27/

Task & Purpose. (2023, January 3). Russian soldier gave away his position with geotagged social media posts. Retrieved from TaskAndPurpose: https://taskandpurpose.com/news/russian-military-opsec-failure-ukraine/

The Guardian. (2022, January 14). Ukraine hit by ‘massive’ cyber-attack on government websites. (The Guardian) Retrieved February 15, 2023, from The Guardian: https://www.theguardian.com/world/2022/jan/14/ukraine-massive-cyber-attack-government- websites-suspected-russian-hackers

Willet, M. (2022). The Cyber Dimension of the Russia–Ukraine War. Survival, 64(5), 7-26.

Burgess, M. (2022). A Mysterious Satellite Hack Has Victims Far Beyond Ukraine. Wired. https://www.wired.co.uk/article/viasat-internet-hack-ukraine-russia

Cimpanu, C. (2018). Ukraine Says It Stopped a VPNFilter Attack on a Chlorine Distillation Station. https://www.bleepingcomputer.com/news/security/ukraine-says-it-stopped-a- vpnfilter-attack-on-a-chlorine-distillation-station/Insinna, V. (2022).

SpaceX beating Russian jamming attack was “eyewatering.” Breaking Defense. https://breakingdefense.com/2022/04/spacex-beating-russian-jamming-attack-was eyewatering-dod-official/

Kostyuk, N., & Gartzke, E. (2022). Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine. *Texas National Security Review,* 5(3), 113–126. https://tnsr.org/2022/06/why-cyber-dogs-have-yet-to-bark-loudly-in-russias-invasion-of- ukraine/

M. Mcquade. (2018). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Wired, 1–6. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia- code-crashed-the-world/

Massaro, P. (2018). *The Russian Doping Scandal* . 1–20. https://www.csce.gov/international- impact/events/russian-doping-scandal

Michnik, W. (2020). A clash of narratives - Russia, NATO and European Security. *New Eastern Europe*, 1–2(February), 40–48.

Muncaster, P. (2022). *Record-Breaking Year for DDoS Attacks Targeting Russia*. https://www.infosecurity-magazine.com/news/recordbreaking-year-ddos-targeting/

Pearson, J., Satter, R., Bing, C., & Schectman, J. (2022). Exclusive: U . S . spy agency probes sabotage of satellite internet during Russian invasion , sources say. *Reuters*. https://www.reuters.com/world/europe/exclusive-us-spy-agency-probes-sabotage-satellite-internet-during-russian-2022-03-11/

Vicens, A. J. (2022). Top Ukrainian cyber official praises volunteer hacks on Russian targets, offers updates. *Cyberscoop*. https://www.cyberscoop.com/it-army-ukraine-caddywiper- viasat/

Wakefield, J. (2017). Tax software blamed for cyber-attack spread.

BBC. (2022, November 16). *KTT G20 resmi ditutup, deklarasi sepakat "mengecam perang di Ukraina" dan "menuntut Rusia menarik pasukannya."* https://www.bbc.com/indonesia/dunia-63620779

Chen, E. (2022, June 30). As Cyber Threats Grow, Indonesia's Data Protection Efforts Are Falling Short. *The Diplomat*. https://thediplomat.com/2022/06/as-cyber-threats- grow-indonesias-data-protection-efforts-are-falling-short/

Eichensehr, K. E. (2022). Ukraine, Cyberattacks, and the Lessons for International Law.

AJIL Unbound, 116, 145–149. https://doi.org/10.1017/aju.2022.20

Ministry of Foreign Affairs of the Republic of Indonesia. (n.d.). *Statement by the Ministry of Foreign Affairs of the Republic of Indonesia on the Situation in Ukraine*. Retrieved February 16, 2023, from https://kemlu.go.id/portal/en/read/968/berita/statement-by-the-ministry-of- foreign-affairs-of-the-republic-of-indonesia-on-the-situation-in-ukraine

Nardelli, A., Kuznetsov, V., & Krasnolutska, D. (2022). *Cyberattack Hits Ukrainian Websites as Russia Tensions Mount*. https://news.bloomberglaw.com/privacy-and- data-security/cyberattack-hits-ukraine-official-sites-amid-russia-tensions-1

P.W, S., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*.

Roberts, M. (2022). *Indonesia's Cybersecurity Landscape*. https://www.asiapacific.ca/publication/indonesias-cybersecurity-landscape

Smith, M. (2022, February 7). Russia has been at war with Ukraine for years – in cyberspace. *Theconversation*.

Com. https://theconversation.com/russia-has-been- at-war-with-ukraine-for-years-in-cyberspace-176221

VOA. (2022, July 7). *Perang Rusia-Ukraina Dominasi Agenda Pertemuan Menteri Luar Negeri G20.* https://www.voaindonesia.com/a/perang-rusia-ukraina-dominasi-agenda-pertemuan-menteri-luar-negeri-g20-/6648637.html

Aldiansyah Nurrahman. (17. November 2022). *Kemenangan Perang Ditentukan Keberpihakan Negara Lain*. Noudettu osoitteesta validnews.id: https://validnews.id/nasional/kemenangan-perang-ditentukan-keberpihakan-negara-lain

Arbar, T. F. (3. Maret 2022). *Kronologi Perang Rusia-Ukraina, Ini yang Bikin Putin Murka!* https://www.cnbcindonesia.com/news/20220303071704-4-319716/kronologi-perang-rusia-ukraina-ini-yang-bikin-putin-murka

Awaludin, Y. (28. Desember 2022). *Perang Siber Lawan Rusia,Ukraina Klaim PuluhanSerangan/Hari*. https://www.radarbogor.id/2022/12/28/perang-siber-lawan-rusiaukraina- klaim-puluhan-serangan-hari/

Babys, S. A. (2021). Ancaman Perang Siber di Era Digital dan Solusi Keamanan Nasional Indonesia*. JURNAL ORATIO DIRECTA, 425-442*.

Dewi, I. R. (14. Maret 2022). *Serangan Rusia ke Ukraina Picu Perang Hacker Pertama di Dunia*.https://www.cnbcindonesia.com/tech/

20220314153602-37-322617/serangan-rusia-ke-ukraina-picu-perang-hacker-pertama-di-dunia

Hütter, C. L. (20. Januari 2023). *Perang Siber Lumpuhkan Infrastruktur Musuh*. https://www.dw.com/id/perang-siber- infrastruktur/a-64063719

Iskandar. (28. Februari 2022). *Top 3 Tekno: Perang Siber Rusia-Ukraina Jadi Sorotan*. https://www.liputan6.com/tekno/read/4899081/top-3-tekno-perang-siber-rusia-ukraina-jadi-sorotan

Prakoso, J. P. (1. Maret 2022). *Perang Siber Rusia Ukraina: Serangan Hacker dan Misinformasi*. https://kabar24.bisnis.com/read/20220301/19/1505793/perang-siber-rusia- ukraina-serangan-hacker-dan-misinformasi

Wardhana, E. F. (18. Januari 2023). *Ukraina Salahkan Rusia atas 2.000 Serangan Siber pada Tahun Lalu*. Https://international.sindonews.com/read/999195/41/ukraina-salahkan-rusia-atas-2000-serangan-siber-pada-tahun-lalu-1674028889

https://www.chinausfocus.com/peace-security/non-state-actors-new-disruptors

Li Yan Deputy Director of Institute of American Studies, CICIR.

https://www.kompasiana.com/leo1/61ee6a614b660d0d36232082/pengaruh-aktor-non-negara-dalam-lingkup-politik-siber-global

https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war

https://graquantum.com/a-brief-history-of-cyberwarfare/

https://cisac.fsi.stanford.edu/news/stuxnet

https://nordvpn.com/blog/cyber-warfare/

https://www.linkedin.com/pulse/ai-driven-cyber-warfare-preparing-future-conflict-niels-groeneveld

https://www.nasdaq.com/articles/ai-driven-cyberwarfare%3A-the-future-of-conflict

https://www.cybersecurity-insiders.com/artificial-intelligence-to-fuel-cyber-warfare/

https://www.imperva.com/learn/application-security/cyber-warfare/

https://www.bbc.com/news/technology-40428967

UCHA-RAMDANI-MUNANDAR-ROBY-OKTA-TANTO-ADAM-INDRIAN-HENDRY-TAUFIK-KUKUH-KEVIN-ASEP-DKK.