IMPLIKASI *CYBERATTACK* DALAM KONFLIK RUSIA-UKRAINA TERHADAP STRATEGI PERTAHANAN UKRAINA

Oleh : Kanjeng Ayu Siti Rahmah
Pembimbing: Irwan Iskandar, S.IP, MA
Jurusan Hubungan Internasional
Fakultas Ilmu Sosial dan Ilmu Politik
Universitas Riau
Kampus Bina Widya, Jl. H.R. Soebrantas Km 12,5 Simp. Baru, Pekanbaru 28293
Telp/Fax. 0761-63277

ABSTRACT

More than a hundred countries are developing cyber military capacity to strengthen security even attack other countries. On 2-24, 2022, Russia launched an invasion of Ukraine in every area of warfare including cyberspace. Russian hackers have initiated attacks on many Ukrainian websites since the beginning of the invasion making government web pages and online banking services inaccessible to the public.

This research is a descriptive qualitative with data sources coming from Ukrainian government websites, international organizations and related publications. This paper uses a neorealist perspective with the concept of the Global Cybersecurity Agenda at the country level of analysis within the scope of 2016-2022.

The changes can be seen from the renewal of Ukraine's defense strategy which also focuses on the realm of cybersecurity, Ukraine established a special institution that works in the realm of cybersecurity and Ukraine formed international cooperation with NATO in building a national cyber defense system. Ukraine already has several frameworks in place related to cybersecurity. In early 2016, the government approved the first Cybersecurity Strategy of Ukraine. It later issued a second version (Strategy 2020), after which both regulations were canceled with the adoption of Presidential Decree No. 447/2021.

Keywords: *Cyberattack, Cybersecurity, Cyberweapon and Ukraine Defence Strateg*

PENDAHULUAN

Cyber-attack (serangan *cyber*) dan konsekuensinya telah menjadi agenda utama dalam pembahasan dunia. Salah satu yang menjadi perhatian penting adalah operasi militer *cyber* di tengah konflik bersenjata dengan kemampuan menghancurkan fungsi dari insfrastruktur serta pelayanan vital bagi populasi penduduk. Lebih dari seratus negara diperkirakan sudah dan sedang mengembangkan kapasitas militer *cyber*.[1]

Cyber-attack sendiri terdiri dari berbagai bentuk dan telah terjadi dalam operasi yang tidak terhitung seperti *cybercrime, cyberespionage* serta *state-sponsored operations*. Pembahasan terkait *cyber warefare* di kancah internasional serta hukum yang dapat diimplementasikan dalam memandang limitasi pelaksanaan *cyber-attack* menjadi indikasi urgensi kesadaran akan ancaman dari serangan *cyber* tersebut. Dari berbagai bentuk operasi, hanya operasi dalam konteks konflik bersenjatalah yang dinaungi Hukum *cyber-attack* Humanitarian Internasional.[2]

Perkembangan penggunaan *cyberweapon* sebagai permulaan maupun dalam menghadapi konflik terus meluas. *Tepatnya* pada 24 Februari 2022, Rusia- Ukraina mulai tercatat menjadi aktor utama perang terbuka selain perang Tigray (Ethiopia-Sudan) yang terjadi dalam 10 tahun terakhir.[3] Menariknya, kedua belah pihak tidak hanya mengandalkan operasi militer langsung tetapi juga melancarkan rangkaian *cyber-attack*. Hal ini menandakan intensnya penggunaan *cyberweapon* dimana realita tersebut dapat diartikan terindikasinya peningkatan aktivitas konflik antar negara dalam *cyberspace*.

Sepanjang konflik Rusia-Ukraina berlangsung, terdapat beberapa peristiwa besar yang menandai eskistensi *cyber-attack*. Salah satunya adalah Operasi Garmageddon atau Armageddon. Dinas Keamanan Ukraina mengklasifikasikan kelompok peretas "Armageddon" sebagai APT (*Advanced Persistent Threat*), dan secara jelas mengidentifikasinya sebagai unit struktural yang dibuat khusus dari Dinas Keamanan Federal Federasi Rusia, yang tugasnya adalah kegiatan intelijen dan subversif terhadap Ukraina di dunia maya. Dinas Keamanan Ukraina percaya bahwa Armageddon dibentuk dan telah beroperasi sejak 2014. Tujuan utama dari kegiatannya adalah untuk melakukan operasi intelijen *cyber* yang ditargetkan terhadap badan-badan negara Ukraina, terutama badan-badan keamanan, pertahanan dan penegak hukum, untuk mendapatkan informasi intelijen. Aktivitas dan perkembangan kelompok peretas "Armageddon" selama 2014-2021 telah menyebabkan adanya ancaman dunia maya baru yang nyata.

Pada 24 Februari 2022, Rusia melancarkan invasi ke Ukraina di setiap wilayah peperangan termasuk dunia maya. Peretas Rusia telah memulai serangan di banyak situs web Ukraina sejak awal invasi,

[1] ICRC. 2021. *Cyber Warfare: does International Humanitarian Law apply?* 2 25. Accessed 12 04, 2022. https://www.icrc.org/en/document/cyber-warfare-and-international-humanitarian-law.

[2] Ibid.

[3] *ICRC. 01April 2022. ICRC statement on International Law in the Second session of the OEWG on security of and in the use of information and communications technologies. statement on* . 04 01. Accessed 12 04, 2022. https://www.icrc.org/en/document/international-humanitarian-law-limi

membuat halaman web pemerintah dan layanan perbankan online tidak dapat diakses oleh publik. Wakil perdana menteri Ukraina dan menteri untuk transformasi digital menanggapi serangan Rusia dengan menciptakan pasukan teknologi informasi (TI) yang terdiri dari spesialis keamanan dunia maya pada 22 Februari 2022. Sebelumnya situs web beberapa bank Ukraina dan departemen pemerintah menjadi tidak dapat diakses. Pada saat yang sama serangan "penghapus" baru, yang menghancurkan data pada mesin computer yang terinfeksi. Serangan ini digunakan untuk menyerang organisasi Ukraina. Pada bulan Januari, pemerintah Ukraina menuduh Rusia berada di balik gelombang DDoS lainnya, dan gelombang serangan penhapusan (*wiper*) yang lebih kecil dan kurang canggih. Beberapa situs web yang terpengaruh diganti dengan peringatan kepada warga Ukraina untuk "bersiap menghadapi yang terburuk". Akses ke sebagian besar situs dipulihkan dalam beberapa jam.[4]

Meluasnya penggunaan *cyberweapon* dan dipilihnya *cyber-attack* sebagai salah satu strategi keamanan dan bahkan alat mencapai kepentingan negara, menjadikan dunia global bergerak ke arah elemen baru dalam menimbang kekuatan yang dikenal sebagai *cyberpower*. Kekuatan *cyber* adalah kemampuan untuk melakukan sesuatu yang berguna di dunia maya, atau kemampuan untuk menggunakan dunia maya dengan tujuan menghasilkan keuntungan dan memengaruhi peristiwa di semua lingkungan operasional dan semua sarana kekuasaan.[5]

Topik *cyber-attack* pada konflik Rusia-Ukraina ini sangat menarik untuk diteliti karena kita dapat melihat bagaimana *cyberweapon* diintegrasikan dengan strategi militer serta digunakan dalam periode konflik bersenjata. Selain itu, pembahasan ini juga menarik karena secara mutlak kekuatan militer Rusia jauh lebih baik dari Ukraina. Sebanyak 12.420 tank dimiliki oleh Rusia yang menjadi peringkat satu dunia, sedangkan Ukraina menduduki urutan 13 dunia dalam hal jumlah tank. Baik dari aspek personel, pesawat tempur, kendaraan lapis baja, armada laut dan lainnya Rusia masih cukup jauh lebih unggul. Bagaimana Ukraina membentuk strategi pertahanan dalam menghalau berbagai kekuatan militer Rusia yang lebih unggul khususnya pada rangkaian *cyber-attack* Rusia akan dibahas dalam tulisan ini.

KERANGKA TEORI

Perspektif: Neorealis

Untuk menjabarkan situasi konflik serta perkembangan motif penggunaan *cyber*weapon dalam kebijakan *cyber-attack* oleh negara-negara terlibat, akan digunakan perspektif neorealis. Bagi pendekatan realis peperangan merupakan sesuatu yang abadi dan mustahil untuk ditiadakan. Realisme politik ketika menganalisis hubungan internasional selalu mendasarkan pandangan mereka pada realitas, pada apa yang ada, dan bukan pada apa yang seharusnya, seperti yang diklaim oleh kaum idealisme politik.[6]

Perspektif neorealisme pertama kali

[4] BBC, Joe Tidy. 2022. *Ukraine crisis: 'Wiper' discovered in latest cyber-attacks* . 02 24. Accessed12 05, 2022. https://www.bbc.com/news/technology-60500618.

[5] Bebber, Robert Jake. 2017. *Cyber Power and Cyber Effectiveness. Comparative Strategy* Vol 36Hlm 427.

[6] Asrudin, Azwar. Desember 2014. *Thomas Kuhn dan Teori Hubungan Internasional: Realismesebagai Paradigma.* Indonesian Journal of International Studies *(IJIS)* Vol.1, No.2

diperkenalkan oleh Kenneth N. Waltz dengan nama *structural realism*. Istilah neorealisme kemudian dipopulerkan oleh Richard Ashley dalam bukunya "The Poverty of Neorealism." Berbeda dengan kaum realis klasik yang memandang kekuasaan sebagai totalitas kekuatan militer, kaum neorealis berpendapat bahwa kekuasaan adalah agregasi seluruh aspek dan sumber daya suatu negara untuk memaksa dan mendominasi negara lain dalam sistem internasional. Kenneth N. Waltz dalam bukunya mengemukakan bahwa "*...apa yang seharusnya menjadi perhatian suatu negara bukanlah untuk memaksimalkan power, melainkan mengamankan posisinya di dalam sistem internasional"* Neorealis menurut Waltz, masih melihat power sebagai faktor yang paling penting dalam hubungan internasional. Power akan membantu suatu negara untuk mencapai posisi yang aman dalam sistem anarki yang berjalan di dunia.[7]

Level Analisis : Negara

Tingkat analisa negara berfokus pada pemaparan terkait perilaku negara yang ditentukan oleh tiap faktor internal negara bersangkutan. Merujuk pada Rourke, penelitian yang menerapkan level analisis ini harus memiliki pemahaman tentang peran berbagai aktor termasuk birokrat, kelompok kepentingan serta badan legislatif di dalam negara tersebut dengan kaitannya pada pengambilan kebijakan luar negri. Pada akhirnya, penggunaan tingkat analisis negara akan menghasilkan penjelasan menengah. Dalam artian tidak terlalu mikro dari yang dihasilkan level analisis individu serta tidak lebih terlalu makro sebagaimana pemaparan yang dihasilkan oleh tingkat analisis sistem.[8]

***Konsep: Global Cybersecurity Agenda* (GCA)**

Konsep ini merupakan kerangka kerja internasional yang dikeluarkan oleh ITU (*International Telecmmunication Union*).[9] ITU adalah badan khusus PBB terkemuka untuk teknologi informasi dan komunikasi (TIK). Didirikan pada tahun 1865, ITU merupakan badankhusus tertua dalam sistem PBB. Titik fokus global untuk pemerintah dan sektor swasta dengan 191 Negara Anggota, 900+ Anggota Sektor dan Rekanan. ITU berkantor pusat di Jenewa, Swiss; 11 kantor regional/area dan staf dari hampir100 negara.

Pertumbuhan dan potensi masa depan masyarakat informasi online berada dalam bahaya dari ancaman siber yang terus meningkat. Selain itu, dunia maya tidak memiliki batas, serangan siber dapat menimbulkan kerusakan yang tak terukur di berbagai negara dalam hitungan menit. Ancaman siber adalah masalah global dan membutuhkan solusi global, yang melibatkan semua pemangku kepentingan. Pada Konferensi Tingkat Tinggi Dunia tentang Masyarakat Informasi (WSIS), para pemimpin pemerintah mengakui risiko nyata dan signifikan yang ditimbulkan oleh kejahatan siber dan mempercayakan ITU untuk mengambil peran utama dalam mengoordinasikan upaya internasional dalam hal keamanan siber, sebagai Moderator/Fasilitator tunggal untuk Bidang Aksi WSIS C5, "Membangun Kepercayaan Diri dan Keamanan dalam Penggunaan

[7] Suryanti, Budhi Tri. 2021. *Pendekatan Neorealis terhadap Studi Keamanan Nasional. JurnalDiplomasi Pertahanan* Volume 7, Nomor 1

[8] Rourke, John T. 1995. *International Politics on the World Stage, 5th ed* . Connecticut: DushkingPublishing Group

[9] Dr. Hamadoun I. Touré, 2007. *ITU Global Cybersecurity Agenda*

Teknologi Informasi dan Komunikasi (TIK)"

Menanggapi mandat ini, Sekretaris Jenderal ITU, Dr. Hamadoun I. Touré, meluncurkan Agenda Keamanan Siber Global pada tanggal 17 Mei 2007 sebagai kerangka kerja untuk kerja sama internasional yang bertujuan untuk mengajukan strategi solusi untuk meningkatkan kepercayaan dan keamanan dalam masyarakat informasi. GCA berusaha untuk membangun inisiatif nasional dan regional yang ada untuk menghindari duplikasi pekerjaan dan mendorong kolaborasi di antara semua mitra yang relevan. GCA dibangun di atas lima Area Kerja (WA-*Working Area*) utama:

- Langkah-langkah hukum,
  berupaya mengembangkan saran tentang bagaimana kegiatan kriminal yang dilakukan melalui TIK dapat ditangani melalui legislasi dengan cara yang kompatibel secara internasional. Berupaya mempromosikan kerja sama dan memberikan saran strategis kepada Sekretaris Jenderal ITU tentang tanggapan legislatif untuk mengatasi masalah hukum yang berkembang di bidang keamanan siber. Beberapa anggota HLEG (*High Level Expert Group*) menganggap bahwa ruang lingkup WA1 mencakup penuntutan terhadap kejahatan siber.
- Langkah-langkah Teknis dan Prosedural,
  berfokus pada langkah-langkah utama untuk mengatasi kerentanan pada produk perangkat lunak, termasuk skema akreditasi, protokol, dan standar. Diskusi mencakup bagaimana membangun pekerjaan yang sudah ada di bidang ini, termasuk di antaranya, Kriteria Umum dan pekerjaan ITU-T dan organisasi standardisasi lainnya.
- Struktur Organisasi
  mempertimbangkan kerangka kerja umum dan strategi respons untuk pencegahan, deteksi, respons, dan manajemen krisis serangan siber, termasuk perlindungan sistem infrastruktur informasi penting negara. Konsensus umum dicapai pada rekomendasi untuk WA3, tanpa ada oposisi yang disuarakan untuk menghapus salah satu rekomendasi. Diskusi difokuskan pada kerangka kerja potensial untuk evaluasi dan penilaian kesiapan keamanan siber.
- Pengembangan Kapasitas, mencakup upaya-upaya peningkatan kesadaran akan keamanan siber di Tengah Masyarakat dan kemampuan berbagai elemenn Masyarakat termasuk industry guna peningkatan kemanan siber sehingga meminimalisir pengambilan kendali oleh musuh dari aspek sipil.
- Kerja Sama Internasional, berusaha mengembangkan strategi kerja sama internasional, dialog, dan koordinasi dalam menghadapi ancaman siber.

METODE PENELITIAN

Penelitian merupakan jenis penelitian kualitatif deskriptif. Dalam Metode Penelitian Hubungan Internasional, deskriptif adalah sebuah jenis penelitian dimana mengambarkan sekaligus menjelaskan mengenai fenomena, gejala, peristiwa, atau kejadian yang terjadi saat ini.

Sumber data pada penelitian ini berasal dari sumber primer dan sekunder contohnya dokumen-dokumen penting seperti peraturan perundan-undangan dari institusi internasional dan masing-masing negara terlibat serta sumber sekunder.

Ruang lingkup penelitian adalah

cyber-attack selama konflik Rusia- Ukraina serta implikasinya bagi strategi pertahanan Ukraina tahun 2016-2022.

HASIL DAN PEMBAHASAN

Dalam '*The Rise of Cyberspace Power*' John Sheldon menyebutkan, beberapa ahli percaya bahwa kemudahan serangan dunia maya "*...menandai era*

gangguan yang terus-menerus." Ada yang berpendapat bahwa keberhasilan internet juga merupakan domain potensial untuk peperangan dan ketika ruang dunia maya menjadi lebih penting bagi ekonomi, kemakmuran, dan keamanan nasional suatu negara, semakin menarik bagi musuh untuk mencoba melumpuhkannya dengan melakukan serangkaian *cyberattack.*[10] Melalui penggunaan sarana siber, telah terjadi berbagai macam tindakan jahat yang berlarut-larut termasuk tindakan kriminal hingga spionase serta *cyberattack* yang dapat dilakukan oleh negara, organisasi, ataupun individu.

Daniel Kuehl mendefinisikan *cyberpower* sebagai, "*kemampuan dalam menggunakan ruang siber untuk menciptakan keuntungan dan mempengaruhi peristiwa di semua lingkungan operasional dan di seluruh instrumen kekuasaan*" dan digunakan untuk mencapai tujuan kebijakan pelaku yang dapat berupa individu, organisasi, atau negara.[11] Oleh karena itu, kekuatan siber (*cyberpower*) didasarkan pada penciptaan, kontrol, dan komunikasi informasi digital melalui internet dan sarana digital lainnya. Informasi merupakan elemen kunci dalam *cyberpower* dan membentuk dimensi dari instrumen kekuasaan. Dengan meningkatnya penggunaan *cyberpower* secara militer, kita sekarang menjadi saksi bahwa *cyberpower* juga menjadi bagian dari instrumen kekuatan militer.[12]

a. Rangkaian cyberattack oleh Rusia terhadap Ukraina

Latar belakang sejarah dan kronologi konflik Ukraina penting dalam memahami konteks di mana konflik itu berkembang. Ukraina memperoleh kemerdekaannya pada saat runtuhnya Uni Soviet, tetapi Rusia masih berusaha untuk mempertahankan kontrol atau pengaruhnya terhadap bekas republik- republik Soviet. Hubungan antara Rusia dan Ukraina telah diwarnai dengan perselisihan, termasuk *Revolusi Oranye* selama pemilihan umum Ukraina pada tahun 2004 dan perselisihan mengenai pasokan gas alam.

[10] Daniel T. Kuehl. Franklin D. Kramer. Stuart Starr. and Larry K. Wentz. 2009. *From Cyberspaceto Cyber power: Defining the problem.*" Cyberpower and National Security. eds. Washington. D.C.: National Defence UP

[11] Ibid.

[12] Calvin Seah Ser Thong. 2014. *Cyber Power – An Age of Perpetual Disruption*. Journ al of the singapore armed fores Vol.42 No.4

Ukraina pertama kali memulai pemulihan hubungan dengan Uni Eropa dengan perjanjian asosiasi, tetapi kemudian berbalik kembali ke Rusia. Keputusan ini memicu protes Euromaidan dan memprovokasi kepergian Presiden Ukraina Yanukovych.[13] Rusia telah mengembangkan dan menggunakan kemampuan siber ofensif (*cyber offensive*) untuk melawan negara-negara yang dianggap sebagai musuh.

Aktivitas siber Rusia, terutama yang terkait dengan konflik baru-baru ini di Ukraina dan aneksasi Krimea, merupakan salah satu contoh terbaik penggunaan *cyberattack* untuk membentuk arah politik secara keseluruhan dari sebuah perselisihan. Menurut David J. Smith, budaya politik dan strategis menghasilkan gaya dan preferensi nasional di dunia maya. Rusia memiliki konsep perang informasi yang luas, yang mencakup intelijen, kontra intelijen, penipuan, disinformasi, perang elektronik, pelemahan komunikasi, degradasi dukungan navigasi, tekanan psikologis, degradasi sistem informasi, dan propaganda.[14]

b. Implikasi Cyberattack Rusia terhadap Ukraina

- Sosial dan Politik

Di tingkat sosial, orang-orang dari Ukraina Timur dan Krimea, yang sebagian besar merupakan wilayah berbahasa Rusia, benar-benar terisolasi dari informasi luar. Mereka hanya dapat mendengarkan radio Rusia atau menonton televisi Rusia dan oleh karena itu memiliki akses yang sangat terbatas ke bentuk media lain, yang secara efektif mencegah mereka untuk membentuk opini lain selain yang dipromosikan oleh media Rusia.

Di sisi lain, orang-orang dari bagian barat Ukraina memiliki akses terbatas ke media berbahasa Rusia.[15] Mempertahankan isolasi ini adalah bagian penting dari perang informasi Rusia, di mana tujuannya adalah untuk mengendalikan opini publik dan secara tidak langsung membentuk keputusan yang menguntungkan Rusia.[16]

- Ekonomi

Dampak ekonomi dari *cyberattack* dalam konteks konflik Ukraina sebagian besar berkaitan dengan konsekuensi dari serangan DDoS dan *defacement*. Serangan DDoS biasanya menimbulkan biaya langsung bagi bisnis dalam bentuk hilangnya pendapatan dan hilangnya produktivitas. Kerugian ekonomi rata-rata diperkirakan mencapai US$22.000 per menit dari tidak tersedianya situs web, dan perkiraan rata-rata durasi serangan ini adalah 54 menit.[17]

- Teknologi

Dalam konteks konflik di Ukraina, terdapat serangan fisik

[13] Marie Baezner. 2018. *Cyber and Information warfare in the Ukrainian Conflict*. Edidi ke-2.Risk and Resilience Team Center for Security Studies (CSS). ETH Zürich. Hal, 7

[14] David J. Smith. 2012. *How Russia Harnesses Cyberwarfare*. Defense Dossier No. 4,7-8

[15] Lange-Ionatamishvili, E., Svetoka, S. 2015. *Strategic Communications and Social Media in the Russia Ukraine Conflict*. Cyber War in Perspective: Russian Aggression against Ukraine. Kenneth Geers, Tallinn. Hal, 103–112

[16] Ibid.

[17] Marie Baezner. 2018. *Cyber and Information warfare in the Ukrainian Conflict*. Edidi ke-2.Risk and Resilience Team Center for Security Studies (CSS). ETH Zürich. Hal, 14-15

terhadap infrastruktur telekomunikasi dan juga *cyberattack* terhadap infrastruktur penting. Secara khusus, ketika Ukraina diinvasi pada bulan Maret 2014, pasukan khusus Rusia yang disebut "orang hijau kecil" menyerbu infrastruktur Krimea dari penyedia telekomunikasi Ukraina, UkrTelecom.

Mereka merusak titik pertukaran internet Krimea untuk mengisolasi semenanjung tersebut dari seluruh dunia dan mencegahnya untuk mengkomunikasikan berbagai peristiwa. Dalam hal ini, kerusakan fisik yang terjadi bukanlah hasil dari *cyberattack*, melainkan gangguan material terhadap fungsi internet di Krimea. Rusia, yang mengakui bahwa "orang hijau kecil" itu sebenarnya adalah pasukan Rusia pada bulan April 2014, tidak mencoba untuk mematikan internet di Ukraina sepenuhnya karena dua alasan.[18]

Pertama, hal itu akan terlalu sulit karena Ukraina memiliki enam titik akses internet, yang semuanya melalui Kiev. Kedua, Rusia telah memiliki perusahaan telekomunikasi utama di Ukraina, yang juga sebagian besar bergantung pada perangkat keras Rusia untuk infrastruktur telekomunikasi mereka. Selain itu, banyak orang Ukraina menggunakan media sosial Rusia seperti vKontakte dan sumber daya internet Rusia seperti alamat email, yang memungkinkan pihak berwenang Rusia untuk menyadap dan membaca atau mendengarkan semua percakapan yang dilakukan melalui platform ini[19]

- Internasional

Di tingkat internasional, Ukraina mendapati dirinya terisolasi dari bantuan apa pun dan berada di bawah kendali perang informasi Rusia yang efisien setelah aneksasi Krimea. Pada Desember 1994, Amerika Serikat, Inggris, Prancis, dan Cina berjanji kepada Ukraina, dalam Memorandum tentang Jaminan Keamanan, bahwa mereka akan meminta bantuan dari Dewan Keamanan PBB jika ada agresi dari Rusia.[114] Pada kenyataannya, bekas Republik Soviet ini secara geografis terlalu dekat dengan Rusia dan terlalu jauh dari Eropa Barat untuk mendapatkan keuntungan dari dukungan militer yang signifikan dari negara-negara Barat. Terlepas dari beberapa bantuan materi dan pendidikan, tentara negara-negara Barat tidak melakukan banyak hal untuk mencegah Rusia mencaplok Krimea atau menghentikan konflik di Ukraina Timur.[20]

Namun, negara-negara Barat menjatuhkan sanksi ekonomi terhadap Rusia setelah aneksasi Krimea. Sanksi-sanksi ini tidak dipaksakan kepada Rusia secara khusus karena *cyberattack* di

[18] Karmanau dan Isachenkov, 2014

[19] Pakharenko, G. 2015. *Cyber Operations at Maidan: A First-Hand Account, in: Cyber War inPerspective: Russian Aggression against Ukraine*.Tallinn. Hal, 59–66

[20] Marie Baezner. 2018. *Cyber and Information warfare in the Ukrainian Conflict*. Edidi ke-2.Risk and Resilience Team Center for Security Studies (CSS). ETH Zürich. Hal, 15-16

Ukraina.

c. Implikasi Krisis 2014 terhadap Pemikiran Keamanan Nasional Ukraina

Aneksasi Rusia atas Krimea dan perang siber serta invasi di Ukraina timur menghancurkan ilusi yang dipegang oleh orang-orang Ukraina timur mengenai hubungan 'persaudaraan' antara kedua bangsa, sebuah konsep yang telah menjadi pokok kebijakan kebangsaan Soviet sejak akhir 1930-an.[21] Ancaman Rusia terhadap Ukraina menjadi nyata. Para politisi Euromaidanu harus berurusan dengan ancaman Rusia yang baru, yang untungnya lebih mudah bagi mereka karena Partai Daerah telah bubar dan Partai Komunis tak bisa lagi berpartisipasi dalam pemilihan umum setelah pengesahan empat undang-undang dekomunisai pada 2015.

Memasukkan ancaman Rusia ke dalam pemikiran keamanan nasional dilakukan bersamaan dengan memperbaiki kondisi angkatan bersenjata yang sangat buruk, yang telah hancur selama masa kepresidenan Yanukovych ketika Rusia diizinkan untuk menyusup dan menguasai wilayah-wilayah penting.[22] Selain itu, Ukraina harus membuat undang-undang untuk memerangi berbagai ancaman keamanan baru yang digambarkan oleh Oscar Jonsson dan Robert Seely sebagai 'konflik spektrum penuh'.[23]

Selain doktrin keamanan nasional Ukraina tahun 2015, banyak undang-undang yang diadopsi untuk: memerangi perang informasi dan perang siber; kontrol perbatasan; badan keamanan Ukraina (SBU); memerangi terorisme; melindungi institusi negara, pejabat dan rahasia negara; dan mempertahankan zona maritim eksklusif.[24]

Sejumlah undang-undang juga mengatur tentang: menghidupkan kembali sektor industri militer dan memastikan perceraian sepenuhnya dengan Rusia; memperkuat angkatan bersenjata; mengadopsi doktrin militer baru; dan mengubah Pasukan Internal Kementerian Dalam Negeri menjadi penjaga nasional dan Militsiya menjadi pasukan polisi. Pada Januari 2018, format Operasi Anti-Teroris (ATO-*Anti Terrorism Operation*) untuk memerangi perang Rusia-Ukraina yang dipimpin oleh SBU diubah dengan undang-undang baru menjadi Operasi Pasukan Gabungan (JFO-*Join Force Operation*) yang dipimpin oleh militer. Banyak dari reformasi ini dilakukan dengan dukungan NATO, Uni Eropa, dan pemerintah Barat.[25]

Ukraina sendiri telah memiliki konsep keamanan nasional pasca *cyberattack* yang dilancarkan oleh Rusia, pertama konsep keamanan nasional Poroshenko tahun 2015 dan konsep keamanan nasional Zelensky tahun 2020 yang tidak banyak yang membedakan dalam hal menyatakan Rusia sebagai ancaman bagi Ukraina dan tujuan mengembalikan wilayah yang diduduki. Bedanya, dalam konsep 2020, Rusia didefinisikan sebagai 'negara agresor' dalam delapan kesempatan yang sesuai dengan pandangan 72% warga Ukraina.

Konsep 2020 memiliki manfaat dari tujuh tahun perang spektrum penuh Rusia untuk lebih memahami ancaman

[21] Taras Kuzio. National University of Kyiv-Mohyla Academy dalam https://rusi.org/explore- our-research/publications/commentary/long-and-arduous-road-ukraine-updates-its-national-security-strategy
[22] Ibid.
[23] Ibid.
[24] Centre for Global Studies. 2019. *Ukraine – EU – NATO Cooperation for Countering HybridThreats in the Cyber Sphere.* "Strategy XXI
[25] Ibid.

yang ditimbulkannya.[26] Konsep 2015 dan 2020 terus menguraikan tujuan NATO, yang telah dimasukkan ke dalam setiap dokumen keamanan nasional, kecuali di masa kepemimpinan Yanukovych, dan Uni Eropa. Pada bulan Februari 2019, konstitusi Ukraina diubah untuk memasukkan tujuan keanggotaan NATO dan Uni Eropa, sehingga hal ini menjadi lebih menantang untuk diubah.

d. Pembentukan Regulasi sebagai Langkah Hukum
   - Strategi Keamanan Nasional (Keputusan Presiden Ukraina No. 287/2015 dari 26-05-2015
   - Strategi Keamanan Siber Ukraina 15 Maret 2016, № 96/2016[129]
   - Undang-Undang Ukraina "Terhadap Prinsip-prinsip Dasar Penyediaan Keamanan Siber Ukraina." 05-10-2017
   - Keputusan Presiden Ukraina No. 392/2020
   - Keputusan Presiden No. 447/2021

e. Peningkatan Kesadaran Masyarakat dan Kapasitas Sistem *Cybersecurity* sebagai Langkah Pengembangan Kapasitas dan Teknis Prosedural

   Serangan siber terhadap infrastruktur penting Ukraina merupakan inti dari perang hibrida besar-besaran yang dilakukan pemerintah Rusia terhadap negara tersebut. Sektor energi Ukraina nuklir, listrik, pembangkit listrik tenaga air, serta minyak dan gas adalah target yang sangat berharga. Ukraina harus bertindak cepat untuk merespons serangan-serangan terhadap infrastruktur penting ini, menerapkan solusi yang efisien, dan membangun pertahanan baru terhadap serangan-serangan di masa depan yang mungkin dilakukan oleh berbagai pelaku jahat, baik domestik maupun eksternal.

   Mengurangi kerentanan keamanan siber di infrastruktur penting adalah tujuan dari Keamanan Siber untuk Aktivitas Infrastruktur Kritis (*Cybersecurity for Critical Infrastructure Activity/USAID*) yang didanai oleh Badan Pembangunan Internasional AS (USAID), yang juga bertujuan untuk mengubah Ukraina dari aktor keamanan siber yang reaktif dan mudah dikompromikan menjadi pemimpin keamanan siber yang proaktif.[27] Lebih dari 20 organisasi, termasuk Kementerian Transformasi Digital, Kementerian Luar Negeri, Dewan Keamanan dan Pertahanan Nasional Ukraina, Layanan Negara untuk Komunikasi Khusus dan Perlindungan Informasi, dan institusi pendidikan tinggi di seluruh Ukraina, mendapat manfaat dari kegiatan ini, yang mana memperkuat postur keamanan siber Ukraina di infrastruktur penting.

   Prioritas Kegiatan ini mencakup penguatan kapasitas organisasi dan teknis di lembaga-lembaga penting dan memastikan generasi pakar keamanan siber generasi mendatang mampu menangani tantangan-tantangan ini.

[26] Ibid.

[27] Pemerintah Ukraina, https://www.rnbo.gov.ua/en/Diialnist/4838.html

Selain itu, Kegiatan ini bertujuan untuk meletakkan dasar bagi peningkatan kesiapan dengan membangun kerangka hukum dan peraturan yang efisien, membina komunikasi pemangku kepentingan yang efektif, dan berkolaborasi dengan sektor swasta

f. Pembentukan Badan Organisasi yang Menangani Cybersecurity
   - Koordinator Dewan Keamanan dan Pertahanan Nasional
   - Dinas Keamanan Nasional
   - Kementrian Pertahanan dan Staf Umum Angkatan Bersenjata
   - Kepolisian Nasional Ukraina
   - Layanan Negara Perlindungan Komunikasi dan Informasi Khusus
   - CERT-UA (Tim Tanggap Darurat Komputer Ukraina)

g. Kerjasama Internasional Ukraina untuk Keamanan Siber
   - Uni Eropa

   Ukraina mengembangkan keamanan sibernya sendiri di bidang perlindungan jaringan komputer dan penanggulangan kejahatan siber, yang berorientasi pada model Uni Eropa, dan memperkuat pertahanan sibernya seperti yang dilakukan oleh Aliansi.[28] Relevansi mereka dikonfirmasi pada tahun 2018 ketika spesialis keamanan siber Ukraina berhasil memblokir sekitar 400 serangan siber. Beberapa di antaranya, menurut SSU (Dinas Keamanan Ukraina), dapat menimbulkan konsekuensi yang tidak kalah dengan akibat virus Petya-A.

Pada bulan Desember 2018, Parlemen Eropa, Dewan Eropa, dan Komisi Eropa mencapai kesepakatan politik tentang Undang-Undang Keamanan Siber yang juga memperkuat mandat Badan Uni Eropa untuk Keamanan Siber (Badan Uni Eropa untuk Jaringan dan Informasi dan Keamanan, ENISA), menetapkan kerangka kerja Uni Eropa untuk sertifikasi keamanan siber, yang meningkatkan keamanan siber layanan online.[29] Pada saat yang sama, Komisi Eropa mengusulkan pembentukan Dana Tanggap Darurat Keamanan Siber, yang dapat diikuti oleh negara-negara anggota Uni Eropa jika diinginkan.

Lembaga keamanan siber Ukraina menandatangani Pengaturan Kerja dengan Badan Uni Eropa untuk Keamanan Siber. Badan Uni Eropa untuk Keamanan Siber (ENISA) telah meresmikan Pengaturan Kerja dengan mitra Ukraina yang berfokus pada peningkatan kapasitas, pertukaran praktik terbaik, dan meningkatkan kesadaran situasional.

Uni Eropa sendiri telah membantu Ukraina melalui Misi Penasihat Uni Eropa untuk Ukraina (EUAM), yang antara lain, memberikan bantuan di bidang penanggulangan ancaman siber di seluruh Ukraina. Lebih dari 2,5 juta euro dialokasikan oleh EUAM untuk berbagai proyek yang membantu Ukraina dibidang keamanan siber. Misi ini mendorong peningkatan peralatan teknis lembaga penegak hukum

[28] László Kovács. *Cyber Security Policy and Strategy in The European Union and Nato*. LandForces Academy Review Vol. Xxiii. No 1(89). 2018

[29] Ibid.

Ukraina, mengadakan pelatihan, pertukaran pengalaman, dan diskusi panel. Acara-acara tersebut melibatkan para ahli dari Europol dan lembaga-lembaga Uni Eropa lainnya.[30]

- NATO

Berbeda dengan UE, di NATO, penanggulangan ancaman siber didefinisikan dengan gagasan pertahanan siber, yang termasuk dalam daftar tugas inti pertahanan kolektif, yang menekankan pada orientasi pertahanan, dan bukan keamanan internal, seperti halnya UE. Konsep Strategis NATO-2030 yang baru, yang disetujui pada 29 Juni di KTT Madrid, menggaris bawahi keamanan siber sebagai hal yang penting untuk pencegahan dan pertahanan Aliansi yang koheren.[31] Salah satu lembaga utama Aliansi dalam pertahanan siber adalah *NATO Cooperative Cyber Defense Center of Excellence* (NATO CCDCOE), yang terletak di Tallinn.

Pusat ini merupakan pusat pertahanan siber terakreditasi yang didedikasikan untuk mendukung negara-negara anggota NATO dengan keahlian interdisipliner yang unik dalam penelitian, pelatihan, dan latihan pertahanan siber yang mencakup bidang fokus teknologi, strategi, operasi, dan hukum.[32] Pusat Pertahanan Siber setiap tahun menyelenggarakan latihan pertahanan siber langsung yang menjadi pelatihan internasional terbesar dan paling kompleks di dunia. Agustus lalu, Ukraina menyetujui versi baru dari Strategi Keamanan Siber, yang salah satu elemen pentingnya adalah integrasi dengan sistem pertahanan siber NATO. Badan Komunikasi dan Informasi NATO (NCIA) dan Ukraina menandatangani Nota Perjanjian yang diperbarui pada 17 Januari 2022, untuk melanjutkan kerja sama mereka dalam proyek-proyek terkait teknologi.

Di antara proyek-proyek utama lainnya adalah mentransfer peralatan untuk komunikasi yang aman ke Ukraina, yang telah dimulai pada Desember 2018.[33] Komponen penting dari kerja sama antara Ukraina dan NATO telah menjadi acara tahunan National Hackathon on Cyber Defense. NATO TIDE Hackathon berlangsung dua kali setahun.

Ukraina telah mencoba menjadi anggota CCDCOE sejak 2021, tetapi baru mengalami kemajuan setelah invasi skala penuh Rusia. Maret lalu, Ukraina diberikan peran formal sebagai "peserta yang berkontribusi." Pusat siber NATO mencakup 29 negara sponsor dan sembilan peserta yang berkontribusi, termasuk Ukraina. Hanya anggota NATO yang dapat memberikan suara pada keputusan CCDCOE. Menurut Tkachuk, keanggotaan dalam badan siber ini merupakan langkah penting dalam perjalanan Ukraina menuju NATO. Ukraina telah secara aktif bekerja sama dengan pusat siber NATO sepanjang tahun ini, menurut Yurii Shchyhol, kepala Layanan Negara untuk

[30] Euro News, https://www.eurointegration.com.ua/eng/news/2022/07/6/7142685/

[31] Ukraine – EU – NATO Cooperation for Countering Hybrid Threats in the Cyber Sphere Centre for Global Studies “Strategy XXI” 2019 Kyiv

[32] Ibid.

[33] Ibid.

Komunikasi Khusus dan Perlindungan Informasi Ukraina.[34]

SIMPULAN

Ukraina telah memiliki beberapa kerangka kerja yang terkait dengan bidang keamanan siber; namun, tantangan yang terus tumbuh dan berkembang membutuhkan revisi dan peningkatan yang cepat dan komprehensif dari sisi teknis dan operasional keamanan siber (kerangka kerja hukum, pemangku kepentingan utama, mekanisme kerja sama, pengaturan teknis). Pada awal 2016, pemerintah menyetujui Strategi Keamanan Siber Ukraina yang pertama, dengan tujuan "menciptakan kondisi untuk berfungsinya dunia maya dengan aman, penerapan dunia maya untuk memberi manfaat bagi individu, masyarakat, dan Negara". Kemudian mengeluarkan versi kedua (Strategi 2020), yang setelahnya kedua regulasi tersebut dibatalkan bersamaan disahkannya Keputusan Presiden No. 447/2021.

Ukraina tidak memiliki insentif keuangan untuk menarik spesialis terbaik untuk bekerja bagi pemerintah, dan ada masalah yang cukup besar dalam hal kerja sama antara sektor publik dan swasta, yang sangat penting untuk keberhasilan keamanan siber. Sebagian besar peningkatan pertahanan siber Ukraina tidak akan mungkin terjadi tanpa bantuan keuangan dan pelatihan dari mitra Barat. Untuk mencapai keamanan siber yang kuat di negara ini, Ukraina harus memastikan rentang pengembangan yang sama antara sektor TIK dan infrastruktur keamanan siber. Sayangnya, area kemitraan publik-swasta masih dalam tahap awal pengembangan.

[34] Volodymyr Shypovskyi A. Volodymyr Cherneha B. Serhiy Marchenkov C. 2020. *Analysis of the Ways of Improvement of Ukraine – NATO Cooperation on Cybersecurity Issues.* Social development & Security. Vol. 10, No. 2,

REFERENSI

Asrudin, Azwar. Desember 2014. *Thomas Kuhn dan Teori Hubungan Internasional: Realisme sebagai Paradigma.* Indonesian Journal of International Studies *(IJIS)* Vol.1, No.2

BBC, Joe Tidy. 2022. *Ukraine crisis: 'Wiper' discovered in latest cyber-attacks* . 02 24. Accessed 12 05, 2022. https://www.bbc.com/news/technology-60500618.

Bebber, Robert Jake. 2017. *Cyber Power and Cyber Effectiveness. Comparative Strategy* Vol 36

Calvin Seah Ser Thong. 2014. *Cyber Power – An Age of Perpetual Disruption.* Journ al of the singapore armed fores Vol.42 No.4

Centre for Global Studies. 2019. *Ukraine – EU – NATO Cooperation for Countering Hybrid Threats in the Cyber Sphere.* "Strategy XXI

Daniel T. Kuehl. Franklin D. Kramer. Stuart Starr. and Larry K. Wentz. 2009. *From Cyberspace to Cyber power: Defining the problem.*" Cyberpower and National Security. eds. Washington. D.C.: National Defence UP

David J. Smith. 2012. *How Russia Harnesses Cyberwarfare*. Defense Dossier No. 4

Dr. Hamadoun I. Touré, 2007. *ITU Global Cybersecurity Agenda*

EuroNews, https://www.eurointegration.com.ua/eng/news/2022/07/6/7142685/

ICRC. 01April 2022. ICRC statement on International Law in the Second session of the OEWG on security of and in the use of information and communications technologies. statement on . 04 01. Diakses pada 12 04, 2022. https://www.icrc.org/en/document/international- humanitarian-law-limi

ICRC. 2021. *Cyber Warfare: does International Humanitarian Law apply?* 2 25. Accessed 12 04, 2022. https://www.icrc.org/en/document/cyber-warfare-and-international-humanitarian-law.

International Cooperation on Cybersecurity. (t.thn.). Diambil kembali dari https://sherloc.unodc.org/cld/en/education/tertiary/cybercrime/module- 8/key-issues/international-cooperation-on-cybersecurity-matters.htm

International Telecommunication Union. (2011). *Statistics*. Diambil kembali dari http://www.itu.int/en/ITUD/Statistics/pages/stat/default.aspx

International Telecommunication Union. (2017). *Global Cybersecurity Index.* Diambil kembali dari https://www.itu.int/dms_pub/itu-d/opb/str/D-STR- GCI.01-2017-PDF-E.pdf

International Telecommunication Union. (9-10 November 2017). Ikhtisar Indeks Keamanan Siber Global. *Pertemuan Tahunan ke-2 Komunitas Praktik tentang Indikator Komposit dan Papan Skor*. Ispra, Italia.

ITU Regional Workshop for Europe and CIS on Cybersecurity and Child Online Protection. (t.thn.).

Karmanau dan Isachenkov, 2014

Lange-Ionatamishvili, E., Svetoka, S. 2015. *Strategic Communications and Social Media in the Russia Ukraine Conflict*. Cyber War in Perspective: Russian Aggression against Ukraine. Kenneth Geers, Tallinn.

László Kovács. *Cyber Security Policy and Strategy in The European Union and Nato*. Land Forces Academy Review Vol. Xxiii. No 1(89). 2018

Marie Baezner. 2018. *Cyber and Information warfare in the Ukrainian Conflict*. Edidi ke-2. Risk and Resilience Team Center for Security Studies (CSS). ETH Zürich.

Marie Baezner. 2018. *Cyber and Information warfare in the Ukrainian Conflict*. Edidi ke-2. Risk and Resilience Team Center for Security Studies (CSS). ETH Zürich.

Marie Baezner. 2018. *Cyber and Information warfare in the Ukrainian Conflict.* Edidi ke-2. Risk and Resilience Team Center for Security Studies (CSS). ETH Zürich.

National Cybersecurity Cluster. (2021). *Facing the Cybersecurity Strategy's Goals, Cyber Leaders Promote the Implementation of Cybersecurity Strategy of Ukraine 2021-2025.*

NATO. (2001). *Policy in the Age of Computer Network Attacks Conference.* Berlin.

Pakharenko, G. 2015. *Cyber Operations at Maidan: A First-Hand Account, in: Cyber War in Perspective: Russian Aggression against Ukraine*.Tallinn.

Pemerintah Ukraina, https://www.rnbo.gov.ua/en/Diialnist/4838.html

Pemerintah Ukraina https:// cybersecuritycluster.org.ua/en/news/facing-the-cybersecurity-strategys- goals-c

Presiden Ukraina. (2020). *Strategi Keamanan Nasional Ukraina.* Retrieved from https://www.president.gov.ua/documents/3922020-35037

Presidential Decree of Ukraine. (2018, October). *Cybersecurity Strategy of ukraine.* Diambil kembali dari https://ccdcoe.org/uploads/2018/10/NationalCyberSecurityStrategy_Ukraine.pdf

Rourke, John T. 1995. *International Politics on the World Stage, 5th ed* . Connecticut: Dushking Publishing Group

Suryanti, Budhi Tri. 2021. *Pendekatan Neorealis terhadap Studi Keamanan Nasional. Jurnal Diplomasi Pertahanan* Volume 7, Nomor 1

Taras Kuzio. National University of Kyiv-Mohyla Academy dalam https://rusi.org/explore-our-research/publications/commentary/long-and-arduous-road-ukraine-updates-its-national-security-strategy

Ukraine – EU – NATO Cooperation for Countering Hybrid Threats in the Cyber Sphere Centre for Global Studies "Strategy XXI" 2019 Kyiv

Volodymyr Shypovskyi A. Volodymyr Cherneha B. Serhiy Marchenkov C. 2020. *Analysis of the Ways of Improvement of Ukraine – NATO Cooperation on Cybersecurity Issues.* Social development & Security. Vol. 10, No. 2,