**ANALISIS PENGARUH ANCAMAN *CYBER WAR* RUSIA DAN UKRAINA SEBAGAI URGENSI *CYBER DEFENCE* INDONESIA**

Anjelina, Dina1 dan Agussalim, SIP., MIRAP2

PROGRAM ILMU HUBUNGAN INTERNASIONAL UNIVERSITAS HASANUDDIN, INDONESIA

**ABSTRAK**

Rusia dan Ukraina hingga kini masih dilanda konflik yang berhasil menyita perhatian dunia termasuk negara Indonesia karena semakin memanas dan belum menemukan titik terang penyelesaian. Terlebih ketika mengetahui bahwa tidak hanya perang militer yang terjadi, melainkan juga ancaman perang siber dari Rusia yang belum tersorot oleh publik, mengingat Rusia merupakan negara *great power*. Perang siber tidak bolehdiabaikan sebab eksistensinya menjadi biang keladi runtuhnya stabilitas dan keamanan internasional yang berdampak pada kedaulatan suatu negara. Maka melalui tulisan ini, penulis hendak menganalisis terlebih dahulu perihal serangan siber yang telah dilakukan oleh Rusia terhadap Ukraina dan bagaimana respon Indonesia dalam meningkatkan kewaspadaan akan ancaman perang siber dari kedua negara melalui upaya pertahanan dan keamanan siber. Upaya yang dilakukan juga tidak hanya terpusat pada aktivitas negara namun aktivitas individu sebagai dasar perilaku. Adapun metode penelitian yang digunakan oleh penulis adalah metode deskriptif dengan pendekatan kualitatif melalui studi kepustakaan yang bersumber dari buku, website resmi nasional maupun internasional, jurnal, dan artikel.

Kata Kunci : Perang Siber, Pertahanan Keamanan

***ABSTRACT***

*Russia and Ukraine are still being hit by conflicts that have managed to grab the world's attention, including the Indonesian countries, because they are getting hotter and have not yet found a clear resolution point. Especially when you know that it's not just a military war that's going on, but also the threat of cyber war from Russia that hasn't been highlighted by the public, considering that Russia is a great power country. Cyber war should not be ignored because its existence is the root cause of the collapse of international stability and security which has an impact on the leadership of a country. So through this paper, the author wants to analyze in advance regarding the cyber attack that has been carried out by Russia against Ukraine and how Indonesia's response is in increasing awareness of the threat of cyber war from the two countries through cyber defense and security efforts. The efforts made are not only limited to state activities but individual activities as a basis for behavior. The research method used by the author is a descriptive method with a qualitative approach through literature studies sourced from books, official national and international websites, journals and articles.*

*Keywords : Cyber War, Cyber Defence*

**PENDAHULUAN**

Keamanan adalah keadaan bebas dari rasa takut akan bahaya. Secara kompleks, definisi keamanan cukup beragam sesuai dengan lingkupnya. Sebagai contoh, pendapat dari Patrick J. Garrity, yang mengemukakan keamanan saling berkaitan dengan pembelaan negara atas kepentingan berdaulat melalui pendekatan militer. Sederhananya, keamanan yang dimaksud ini mengarah pada lingkup nasional sebagai upaya untuk melindungi populasi dan wilayah dengan perilaku kompetitif dari kejahatan transnasional. Pendapat lain berasal dari penulis literatur kepolisian bernama Awaloedin Djamin yang secara umum melihat keamanan mengarah pada lingkup individu, yaitu kebebasan dari gangguan jasmani dan rohani, serta terlindunginya keselamatan jiwa dan harta benda dari segala macam bahaya. Paham realisme, konstruktivisme, dan liberalisme juga menanggapi pengertian keamanan dalam hubungan internasional sesuai dengan karakteristik nilai masing-masing.

Pertama, perspektif realisme. Realisme menganggap kehidupan negara-negara di dunia berada dalam kondisi yang anarkis, cenderung saling curiga satu sama lain dan saling bersaing demi meningkatkan kekuatan masing-masing tanpa adanya otoritas tertinggi untuk memberikan batasan aturan dalam menciptakan ketertiban. Sebagai aktor utama, negara berkewajiban untuk melindungi kepentingan nasional dan kelangsungan hidup masyarakatnya demi menciptakan keamanan. Bagi kaum realis, keamanan didasarkan pada kemampuan militer sebagai senjata pertahanan dan perlawanan negara jika hendak menyerang. Negara berupaya untuk mencapai keamanan melalui keseimbangan kekuatan atau aliansi dengan negara lain untuk melindungi diri mereka dari ancaman. Keamanan juga menyinggung konsep ketergantungan keamanan yang tidak hanya dipengaruhi oleh kebijakan negara sendiri melainkan kebijakan negara lain. Sehingga jika terjadi dominasi kekuatan dari negara besar, maka dapat melemahkan keamanan negara yang lain.

Kedua, perspektif konstruktivisme. Konstruktivisme menekankan bahwa keamanan tidak hanya bergantung pada faktor material seperti kekuatan militer, tetapi juga dipengaruhi oleh aspek ideasional, seperti identitas, norma, dan kepercayaan yang dianut oleh para aktor tersebut. Aspek ideasional ini menjadi penentu bagaimana perilaku para aktor negara dalam mengatur suatu kebijakan. Konstruktivisme juga melihat keamanan sebagai hasil dari proses para aktor berinteraksi, membentuk identitas dan norma, serta menciptakan konstruksi bersama perihal ancaman dan pengendalian keamanan. Bagi konstruktivisme, keamanan memang merupakan kebutuhan dasar untuk menjaga kepentingan nasional ketika menghadapi ancaman dari dalam maupun dari luar. Eksistensi keamanan berasal dari adanya pengakuan dan rasa saling percaya antar-aktor dalam sistem internasional.

Ketiga, perspektif liberalisme. Berbeda dengan perspektif realisme yang lebih mengutamakan kekuatan militer dalam penanganan keamanan, liberalisme memusatkan pada kerjasama yang diperkenalkan melalui lembaga, diplomasi, dan negosiasi internasional di bidang ekonomi, sosial, politik, hingga lingkungan guna mencegah peperangan. Meskipun demikian, pada konteks kebijakan luar negeri, liberalisme tidak secara mutlak menolak penggunaan militer dan menggarisbawahi penggunaan militer dengan bijak dan bertanggung jawab. Liberalisme memandang keamanan sebagai kondisi negara yang aman sehingga masyarakat memiliki kesempatan untuk menggapai tujuan tanpa adanya ancaman. Keamanan tersebut didasari oleh hak asasi manusia, kebebasan berindividu, dan nilai demokrasi. Contohnya pada bidang ekonomi, kondisi tercapainya keamanan mencakup kemudahan akses lapangan kerja, perlindungan sosial, serta pendapatan dan perekonomian yang tersebar merata.

Melihat dari begitu banyaknya pemahaman umum tentang keamanan, secara tidak langsung dapat disimpulkan bahwa keamanan merupakan elemen penting pondasi suatu negara. Tentu setiap negara seringkali menghadapi ancaman. Ancaman tersebut bisa bersifat alami seperti bencana alam atau penyebaran penyakit, maupun bersifat psikologi yang berasal dari ulah manusia, baik yang terjadi di dalam negeri maupun di luar negeri. Pada dasarnya, segala bentuk ancaman tetap membahayakan otoritas negara yang berpengaruh pada stabilitas perdamaian dunia.

Dalam pembukaan Undang-Undang Dasar 1945 tepatnya Alinea ke-IV, dituliskan bahwa kemerdekaan Indonesia didasari oleh tujuan, “… *melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia, memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa dan ikut melaksanakan ketertiban dunia yang berdasarkan kemerdekaan* …” Sebagaimana dengan tujuan tersebut, tersirat beberapa amanat yang harus dipenuhi oleh pemerintah Indonesia selaku penggerak masyarakat, antara lain menjamin terselenggaranya pembangunan nasional sebagai proses untuk mewujudkan kepentingan nasional seperti menciptakan masyarakat yang adil dan makmur atau bebas dari kemiskinan, mencerdaskan kehidupan bangsa melalui pendidikan intelektual dan moral, serta berkomitmen dalam menjaga perdamaian dunia dengan menjunjung tinggi nilai kemanusiaan. Secara implisit, makna amanat ini memiliki keterkaitan dengan keamanan dalam arti luas, yaitu menjaga stabilitas dan mencapai kesejahteraan yang mencakup pekerjaan, pangan, sandang, papan, kesehatan, dan pendidikan dalam masyarakat. Penilaian keamanan pada masyarakat diukur dari seberapa besar terpenuhinya kebutuhan cakupan kesejahteraan tersebut. Selain itu, kondisi keamanan suatu bangsa juga tidak terlepas dari faktor geografi, demografi, sumber daya alam, ideologi, kekayaan budaya, dan pertahanan keamanan.

Jika keamanan nasional mengalami kegoyahan akibat kurang terpenuhinya kebutuhan di dalam negeri, maka negara berada dalam posisi ambang kejatuhan, mengalami berbagai gangguan yang membahayakan kedaulatan dan keselamatan negara sebagai konsekuensi dari kurangnya menjaga keamanan nasional. Konsekuensi tersebut dapat berupa ancaman internal hingga ancaman eksternal. Ancaman internal yang datang dari dalam negeri, seperti radikalisme, narkoba, separatisme, dan korupsi. Ketidakstabilan keamanan berpengaruh pada kepercaaan masyarakat terhadap pemerintah beserta jajarannya sebagai aktor negara. Sedangkan ancaman eksternal merupakan kondisi dimana negara rentan diserang oleh pihak luar dari negara lain seperti invasi, terorisme, juga terjadi gangguan maritim pada wilayah perbatasan seperti pencurian sumber daya perikanan dan masuknya kapal asing melewati batas kedaulatan negara.

Jika keamanan nasional goyah atau terganggu, negara dapat menghadapi berbagai konsekuensi yang serius. Hal ini dapat mencakup kerentanan terhadap ancaman militer atau serangan teroris, kerentanan terhadap kejahatan terorganisir yang dapat mengancam kehidupan masyarakat, kerusakan infrastruktur penting, kekacauan sosial dan politik, dan kerugian ekonomi yang signifikan. Selain itu, ketidakstabilan keamanan nasional dapat mengganggu kepercayaan rakyat terhadap pemerintah dan lembaga negara. Maka dari itu, untuk menjaga keamanan nasional agar menjadi kokoh, secara komprehensif, pemerintah harus mempunyai upaya membentuk kebijakan keamanan yang efektif, memperkuat sistem keamanan melalui kerja sama internasional dan peningkatan kapasistas intelijen serta militer, serta melibatkan partisipasi masyarakat dalam aktivitas pemerintahan.

Tulisan ini akan membahas tentang salah satu studi kasus yang sedang hangat diperbincangkan yaitu kasus Rusia dengan Ukraina, dimana diketahui kini penyerangan yang dilakukan juga memanfaatkan teknologi atau disebut sebagai serangan siber. Dari fenomena penyerangan tersebut, penulis jadikan sebagai hal yang harus diwaspadai oleh negara Indonesia dengan meningkatkan pertahanan siber sebab ditakutkan akan terjadi dampak yang mengancam keamanan nasional.

**METODE PENELITIAN**

Tulisan berjudul “Analisis Pengaruh Ancaman *Cyber War* Rusia dan Ukraina sebagai Urgensi *Cyber Defence* Indonesia” ini termasuk jenis penelitian yang menggunakan metode kualitatif. Metode penelitian kualitatif berfokus pada penggambaran secara mendalam dan mendeskripsikan realita dari fenomena yang dikaji dengan mengumpulkan data informasi sebanyak mungkin. Jenis data yang digunakan dalam tulisan ini adalah data sekunder yang diperoleh melalui publikasi, dokumen resmi, dan basis data seperti Publikasi Badan Pusat Statistik Indonesia. Teknik pengumpulan data dilakukan melalui pendekatan studi kepustakaan atau *library research* dari berbagai sumber yang relevan dan tersedia. Studi kepustakaan atau *library research* adalah proses mempelajari literatur tertulis melalui membaca yang dijadikan sebagai referensi untuk karya ilmiah. Penulis mengolah data yang didapatkan melalui teknik analisis data yang kemudian menghasilkan pernyataan untuk menjawab rumusan masalah yang telah ditetapkan. Berikutnya, data penelitian tersebut diinterpretasikan dalam bentuk deskripsi sesuai dengan hasil dari teknik analisis secara deskriptif. Juga secara eksplanatif yang menganalisis hubungan sebab akibat pada variabel dalam data sesuai dengan konsep yang digunakan.

**HASIL DAN PEMBAHASAN**

1. **SERANGAN SIBER RUSIA KE UKRAINA**

Pada awal tahun 2022 tepatnya tanggal 24 Februari, melalui pidato Presiden Vladimir Putin sebagai pemimpin Rusia, dunia digemparkan oleh penyampaian aksi penyerangan besar yang akan dilakukan Rusia terhadap Ukraina, dan benar saja seusai pidato tersebut, terdengar bunyi ledakan di Ukraina. Perlu diketahui bahwa sebelumnya sejak bulan Desember 2021, Rusia juga melakukan persiapan dengan mengerahkan sebanyak 100.000 angkatan militer di perbatasan Ukraina. Hingga saat ini, belum juga ditemukan hilal atas penyelesaian fenomena konflik tersebut. Lalu muncul banyak pertanyaan, apa yang menyebabkan fenomena ini bisa terjadi? Apa yang dilakukan oleh Ukraina sehingga termasuk dalam masalah besar yang membuat Rusia murka?

Menjawab kedua pertanyaan tersebut, berdasarkan informasi yang dianalisis oleh penulis, konflik bermula dari sikap Presiden Viktor Yanukovych selaku presiden Ukraina ke-4 yang dicap sebagai pengkhianat karena tindakannya kepada pihak Barat yang berubah keberpihakan dengan menolak untuk menandatangani European Association Agreement (EAA) pada bulan November 2013 sebagai bentuk kerja sama antarnegara timur dan Uni Eropa dalam bidang ekonomi dan politik. Diduga bahwa Presiden Yanukovych berbalik mendukung Rusia. Apa yang dilakukan olehnya sudah pasti mengundang amarah warga Ukraina yang anti-Rusia sehingga terjadilah aksi demonstrasi dan melalui aksi tersebut, kedudukan Presiden Yanukovych berhasil dilengserkan. Namun di sisi lain, Rusia juga tidak mau kalah dan ikut mengintervensi Ukraina untuk mencegat bergabungnya Ukraina ke Uni Eropa

Hubungan antara Rusia dan Ukraina kian memanas ketika muncul informasi yang menyebutkan bahwa Ukraina berencana untuk bergabung dalam NATO dengan alasan agar Ukraina dapat meningkatkan kekuatan militernya sehingga memudahkan melakukan perlawanan atas tindakan agresi yang dilakukan Rusia. Disinilah penulis menetapkan inti pembahasan dari studi kasus yang diangkat, yakni apa yang menjadi kepentingan nasional Ukraina begitu pun dengan apa yang menjadi kepentingan nasional Rusia dengan menjalankan strategi berupa invasi ke Ukraina. Rusia berasumsi bahwa dengan masuknya Ukraina dalam NATO, dikhawatirkan perbatasan Ukraina dan Rusia akan dimanfaatkan oleh NATO sebagai front depan yang nantinya bisa saja NATO akan membangun pangkalan militer untuk menghancurkan Rusia. Rusia pun meluncurkan aksinya dengan menyerang beberapa kota besar di Ukraina dan bala tentara, menggunakan senjata kimia, menutup akses bantuan, serta menuntut Ukraina untuk menarik permohonan bergabungnya sebagai negara anggota Uni Eropa dan NATO.

Sejak diumumkannya invasi militer Rusia ke Ukraina oleh Vladimir Putin selaku Presiden Rusia, Ukraina mengalami krisis yang cukup hebat. Terjadi begitu banyak penyerangan yang mengancam dan merenggut nyawa warga tidak bersalah. Hebatnya penyerangan tersebut tidak hanya melalui operasi militer saja, melainkan juga dengan memanfaatkan teknologi digital yang telah menjadi ancaman global. Dampak dari serangan siber tidak boleh disepelehkan karena dapat menimbulkan kekacauan yang lebih besar di berbagai sektor dibandingkan serangan militer. Tercatat Rusia melakukan serangan siber terhadap Ukraina sejak tahun 2014 yang ditandai dengan konflik di Krimea.

Krimea merupakan sebuah semenanjung dengan letak yang strategis sebagai jalur perdagangan, berada di antara dua perairan, yaitu Laut Azov dan Laut Hitam. Dulunya, Uni Soviet memiliki hak kuasa atas Krimea, kemudian Uni Soviet mengalami keruntuhan dan Krimea diberikan sebagai hadiah kepada Ukraina. Awalnya, konflik di Krimea hanya sebatas krisis domestik saja, akan tetapi, krisis ini justru semakin buruk hingga berhasil mengundang keterlibatan Rusia dan menarik perhatian internasional dalam tindakan aneksasi Rusia ke Ukraina. Krisis Krimea dilatarbelakangi oleh perubahan politik di Ukraina melalui peristiwa terlengsernya Viktor Yanukovych sebagai Presiden Ukraina pada Februari 2014. Pelengseran tersebut disebabkan oleh ketidakpuasan masyarakat terhadap kinerja kepemimpinan Yanukovych dan ketidaksenangan akan sikap Yanukovych yang cenderung keras dalam menanggapi aksi unjuk rasa masyarakat untuk menuangkan aspirasinya. Alhasil setelah penggulingan rezim Yanukovych, terjadi kekosongan kekuasaan di Ukraina yang memicu ketidakstabilan politik. Melihat situasi di Ukraina, Rusia memilih untuk ikut campur sesuai dengan persetujuan dari Perdana Menteri Krimea. Perdana Menteri Krimea mengirim permohonan kepada Rusia untuk membantu menyelesaikan konflik domestik Ukraina. Permohonan tersebut sebenarnya didukung oleh latar belakang etnis, dimana mayoritas penduduk Krimea berasal dari etnis Rusia serta terjalinnya ikatan historis dan budaya yang erat dengan Rusia. Di sisi lain, Rusia juga tidak melakukannya dengan percuma, melainkan didasari oleh kepentingan nasional Rusia. Hal itu dapat dilihat dari bagaimana ketidakpuasan Rusia ketika mengetahui bahwa rencana pemerintah Ukraina yang baru akan mengadopsi kebijakan yang bersifat pro-Barat dan pro-integrasi dengan Uni Eropa. Rencana tersebut justru menjadi ancaman bagi Rusia dikarenakan Rusia telah menjadikan Ukraina sebagai zona kekuasaan yang menghadirkan momentum dalam mencapai kepentingan nasionalnya terutama pada aspek perekonomian dan pertahanan keamanan. Rusia pun melakukan upaya militerisasi untuk menganeksasi wilayah Ukraina yang menewaskan hingga$ \pm $14.000 orang.

Rusia yang dikenal dengan sebutan negara *great power* dapat memenuhi ketidakpuasannya dengan kemampuan yang dimiliki. Sebagai pemimpin Rusia, Vladimir Putin memandang kemampuan merupakan kunci utama dalam realisasi tercapainya politik luar negeri Rusia. Tidak hanya secara kasat mata saja, kemampuan tanpa kasat mata juga telah dilakukan oleh Rusia. Terbukti pada tahun 2014 hinga 2016, Rusia mencatat sejarah awal penyerangan siber terhadap Ukraina. Penggunaan kekuatan siber ini tentu tidak terlepas dari komando rezim Putin yang melihat peluang besar keberhasilan di Ukraina sebab Ukraina belum mumpuni dalam bidang teknologi

Melalui kekuatan sibernya, Rusia melakukan serangan terhadap infrastruktur internet Ukraina untuk mengacaukan situasi menjelang pemilihan umum dengan menjatuhkan kandidat nasionalis dan mengangkat kandidat pro-Rusia. Dalam serangan tersebut, para peretas asal Rusia mencuri informasi penting milik para pemimpin Jerman, NATO, dan para pejabat Demokrat yang hendak disebarluaskan. Mereka juga diduga meretas jaringan komputer milik Belanda guna mengamankan informasi rahasia tentang peristiwa jatuhnya pesawat Malaysia Airlines MH17 tahun 2014 di Ukraina. Selain itu, Rusia menyerang infrastruktur energi yaitu menutup jalur pipa yang ditanam dalam tanah sebagai penyaluran minyak gas Ukraina yang menyebabkan krisis energi negara anggota Uni Eropa dan infrastruktur publik seperti pemadaman jaringan listrik untuk menciptakan ketidakstabilan aktivitas negara, dimana masyarakat mulai kehilangan rasa percaya terhadap pemerintah dan mengganggu operasi angkatan militer Ukraina.

Akibat dari serangan siber tersebut, beberapa koalisi internasional seperti NATO dan PBB memberikan kecaman agar Rusia menghormati kedaulatan Ukraina dengan mengakhiri serangannya. Bahkan Uni Eropa dan negara Amerika Serikat menjatuhkan sanksi ekonomi karena aneksasi Rusia ke Ukraina dipandang bersifat ilegal. Sanksi ekonomi ini berupa pembekuan aset dan larangan untuk bertransaksi pada entitas tertentu, pembatasan ekspor dan layanan spesifik tertentu terutama yang menyinggung minyak gas Ukraina ke Rusia, serta pengimbangan sanksi yang ada untuk direalisasikan sesuai isi perjanjian Minsk. Perjanjian Minsk adalah upaya perdamaian yang ditandatangani pada tahun 2014 dan 2015, bertujuan untuk mengamankan konflik bersenjata antara sekelompok separatis yang didukung oleh Rusia dengan pasukan pemerintah Ukraina di Ukraina Timur. Perjanjian Minsk berisikan sejumlah persyaratan yang harus dipatuhi, antara lain yang pertama, menegaskan bahwa kedaulatan dan integritas teritorial Ukraina harus dipertahankan, dimana para pihak diharapkan untuk menghormati batas teritorial Ukraina dengan tidak melakukan sejenis perilaku ancaman yang membahayakan kedaulatan Ukraina. Kedua, menekankan pentingnya prinsip non-intervensi atau penghentian kekerasan dari pihak asing. Tidak diperkenankan adanya campur tangan pada urusan dalam negeri Ukraina, baik yang berkaitan dengan hukum dan wilayah teritorial Ukraina. Ketiga, mengarahkan perhatian pada perlindungan hak asasi manusia dan keadilan yang menjamin kehidupan masyarakat di Ukraina. Misalnya pemberian bantuan kemanusiaan yang harus disalurkan secara merata dan tidak memiliki motif tersendiri, serta implementasi program kerja pemerintah secara transparan sehingga mempermudah akses masyarakat untuk menilai dan berpartisipasi, seperti dalam proses pemilihan umum. Terakhir, menegaskan kepada para pihak yang terlibat dalam Perjanjian Minsk agar berkomitmen dan bekerja sama dalam merealisasikan persyaratan pada perjanjian tersebut guna tercapainya perdamaian dan stabilitas di Ukraina dan wilayah sekitar. Para pihak juga dimohon untuk bantu menyerukan perintah gencatan senjata teristimewa di kawasan konflik yakni Ukraina Timur.

Meskipun mendapat kecaman di ranah internasional, namun kecaman itu tidak mampu menghentikan langkah Rusia untuk tetap menjalankan aksi serangan sibernya. Rusia kembali menyerang Ukraina yang mencapai puncaknya pada tahun 2022. Serangan siber Rusia berlangsung sejak tanggal 13 Januari setelah kurang lebih 6 tahun semenjak kejadian serangan siber pertama kali di Ukraina yang diidentifikasi oleh Microsoft Threat Intelligence Center (MSTIC) dan dilaporkan sebagai jenis serangan *malware* bernama WhisperGate atau DEV-0586. Sifat dari *malware* tersebut dirancang terlihat seperti catatan tebusan tanpa memiliki fitur pemulihan dengan niat menghancurkan file alih-alih mengenkripsinya untuk tebusan dan akan beroperasi ketika perangkat elektronik yang menjadi target dalam keadaan *power off*.

Serangan siber ini terus berlanjut dan mencapai sekitar 2.194 serangan yang menyebabkan sekitar 70 situs web pemerintahan mengalami kelumpuhan, seperti web Kementerian Pertahanan dan Angkatan Bersenjata Ukraina dan situs web bank besar Ukraina yaitu PrivatBank dan Oschadbank mengalami kelumpuhan. Bahkan terjadi pula peretasan Viasat terhadap salah satu perusahaan satelit komersial terbesar di dunia dengan tujuan untuk menyerang komando dan kontrol militer Ukraina. Akibatnya, ribuan modem broadband satelit Viasat KA-SAT tidak dapat dioperasikan di Ukraina, termasuk yang digunakan oleh militer dan lembaga pemerintah lainnya, menyebabkan kerugian besar dalam komunikasi internet.

Ukraina mulai mengalami kebangkitan pada tanggal 26 Februari, melalui adanya pengumuman pembentukan pasukan yang mahir dalam bidang teknologi informasi komunikasi untuk balas dendam terhadap Rusia. Dampak dari kebangkitan tersebut dimulai dari adanya penyerangan pada situs web dan bank pemerintah Rusia dan acara Ukraina di saluran televisi kembali berjalan lancar. Dari berbagai serangan siber yang dilakukan, Rusia cenderung menggunakan 4 teknik. Pertama, serangan DDoS (Distributed Denial of Service) adalah serangan yang menargetkan situs web dengan melakukan banyak permintaan secara bersamaan sehingga sistem mengalami penurunan kinerja yang tidak dapat menampilkan hasil valid hingga menyebabkan offline sama sekali. Kedua, serangan *malware* adalah serangan yang dilakukan oleh jenis perangkat lunak berbahaya seperti virus terhadap perangkat elektronik jaringan internet. BlackEnergy juga termasuk dalam serangan *malware* yang menargetkan infrastruktur komputer untuk menimbulkan kerusakan di dunia nyata. Contohnya pada kasus pemadaman listrik pada tahun 2015. Ketiga, serangan ransomware adalah serangan yang bertujuan untuk mengenkripsi data pada sistem target kemudian meminta uang tebusan agar data tersebut dapat digunakan kembali. Contoh kasusnya yakni pada awal serangan siber dijalankan pada Januari 2022. Keempat, serangan phising adalah serangan yang dirancang untuk mendapatkan informasi sensitif seperti nama pengguna, kata sandi, dan nomor kartu kredit dengan menyamar sebagai entitas terpercaya.

Melihat dari kasus serangan siber Rusia terhadap Ukraina yang terjadi sejak tahun 2022 ini, Uni Eropa mengutuk serangan tersebut dan menegaskan kesiapan untuk memberikan bantuan tambahan teknis ke Ukraina untuk melawan serangan dan mendukung Ukraina melawan aktivitas destabilisasi lebih lanjut, termasuk meningkatkan ketahanannya terhadap ancaman hibrida dan dunia maya. Sekretaris Jenderal NATO Jens Stoltenberg mengatakan pakar dunia maya di Brussel akan bertukar informasi tentang aktivitas dunia maya yang berbahaya dengan mitra Ukraina mereka dan menandatangani perjanjian untuk meningkatkan kerja sama dunia maya. Selain itu Badan-badan A.S. mengeluarkan Penasihat Keamanan Siber bersama CISA, FBI, dan NSA mengeluarkan Penasihat Keamanan Siber bersama berjudul, "Aktor Siber yang Disponsori Negara Rusia Menargetkan Jaringan Kontraktor Pertahanan yang Dihapus untuk Memperoleh Informasi dan Teknologi Pertahanan A.S. yang Sensitif." CISA mengatakan entitas yang dikompromikan telah mencakup kontraktor pertahanan (CDC) yang mendukung program Angkatan Darat AS, Angkatan Udara AS, Angkatan Laut AS, Angkatan Luar Angkasa AS, dan Komunitas Intelijen selama dua tahun terakhir.

1. **RESPON NEGARA INDONESIA DALAM MENJADIKAN FENOMENA SERANGAN SIBER RUSIA DAN UKRAINA SEBAGAI PEMBELAJARAN UNTUK PERTAHANAN SIBER (CYBER DEFENCE)**

Seiring dengan kebudayaan dan kemajuan peradaban umat manusia, teknologi mengalami perkembangan yang cukup pesat. Semakin maju kebudayaannya, semakin berkembang teknologinya. Perkembangan teknologi bertumbuh semakin cepat dari hari ke hari dan membuat banyak perubahan terhadap seluruh negara tidak terkecuali negara Indonesia. Penggunaan teknologi meningkat tajam hingga menjadi kebutuhan dasar bagi setiap orang. Sesuai dengan fungsinya, teknologi dapat mempermudah pekerjaan manusia terutama dalam berkomunikasi antar-masyarakat. Akan tetapi, teknologi juga bagaikan pisau bermata dua jika tidak dengan bijak dikendalikan ketika munculnya tantangan baru yang saling bersinggungan perihal keamanan siber. Salah satu fenomena yang menjadi perhatian karena menyangkut keamanan siber atau keamanan data adalah Rusia dan Ukraina.

Tidak hanya berdampak pada keamanan nasional kedua negara yang saling bertikai, namun juga berdampak pada stabilitas global, sehingga menjadi pelajaran berharga bagi negara Indonesia untuk menjaga dan memperkuat pertahanan sibernya. Adapun pelajaran berharga yang dimaksud ialah menggarisbawahi pentingnya negara Indonesia untuk meningkatkan kesadaran akan ancaman siber. Langkah yang dapat diambil dimulai dari diri sendiri melalui teknik penyandian atau kriptografi dengan menyembunyikan informasi secara rahasia sehingga data yang ditransmisikan hanya untuk pihak yang berkepentingan saja (Iskandar 2016). Langkah ini dinilai mampu menjamin keamanan dari infastruktur teknologi dengan jaminan komunikasi. Komunikasi yang aman ditujukan untuk melindungi data maupun informasi yang sedang disampaikan sehingga data tersebut tidak dapat disadap oleh pihak yang tidak bertanggungjawab.

Langkah selanjutnya yang harus dilakukan oleh negara Indonesia yaitu membentuk tentara *cyber*. Dalam era modern ini, tentara cyber berperan penting dalam pertahanan keamanan negara, seperti pengumpulan informasi intelijen melalui aktivitas siber dengan menyusup ke pihak musuh dan mencegah terjadinya serangan siber melalui perlindungan sistem, jaringan, dan infrastruktur negara agar tidak terjadi perusakan atau pencurian terhadap data sensitif milik negara, kelompok, atau individu. Pembentukan tentara *cyber* perlu dipersiapkan secara matang agar tidak terjadi kesalahpahaman atas persiapan seputar anggaran. Untuk merealisasikan peresmian terbentuknya tentara *cyber*, dapat dilakukan dalam kerja sama dan koordinasi antara Kementerian Pertahanan (Kemhan) dan Kementerian Infomasi dan Komunikasi (Kominfo). Keduanya juga perlu menjalin hubungan komunikasi dengan operator seperti Telkomsel, Indosat dan sebagainya untuk mencegah serangan siber yang mengancam kerahasiaan informasi berupa penyadapan, serta para aktor keamanan seperti POLRI, BIN, lembaga negara untuk menyelaraskan posisi dan pendapat terhadap ancaman siber serta pembagian tugas dan langkah penanganannya. Terakhir, memberikan kuasa kepada komunitas *hacker, cracker*, dan penjahat IT untuk berpartisipasi dan menginformasikan Kemhan tentang potensi ancaman siber. Indonesia juga harus menekankan kepada Kemhan agar dapat bekerjasama dengan berbagai instansi pemerintah tingkat tinggi, sehingga koordinasi dan pertukaran pengalaman selalu dibicarakan saat bertukar pandangan mengenai inovasi keilmuan teknologi yang baru. Dan terakhir, Kemhan RI harus dapat menjalin kerjasama internasional dengan negara-negara bilateral, trilateral dan multilateral melalui mekanisme atau proses yang berhubungan dengan negara-negara lain di dunia (Subagyo 2018).

**KESIMPULAN**

Seperti yang kita ketahui, dunia internasional masih dihebohkan oleh kasus konflik antara Rusia dan Ukraina, yang tidak hanya menyerang secara kasat mata, namun juga dengan tidak kasat mata. Dalam tulisan ini, penulis telah menjawab rumusan masalah yang telah ditetapkan, yaitu bagaimana kasus serangan siber oleh Rusia dan bagaimana respon negara Indonesia dalam menjadikan serangan siber antara Rusia dan Ukraina sebagai pembelajaran keamanan dan pertahanan siber. Terhitung hingga kini, total serangan siber yang diluncurkan sebanyak 2.194 serangan yang menyebabkan sekitar 70 situs web pemerintahan mengalami kelumpuhan. Meskipun serangan siber Rusia dan Ukraina tersebut secara langsung dampaknya tidak mengenai negara Indonesia, akan tetapi juga mempengaruhi stabilitas nasional. Adapun langkah yang dilakukan oleh negara Indonesia demi mencegah serangan siber sebenarnya dimulai dari niat diri sendiri melalui teknik penyandian secara individu dan terbentuknya tentara *cyber.*

**DAFTAR PUSTAKA**

Adriyanto, S. Dian. (2022). *Sebulan Rusia Serang Ukraina, Begini Kronologis Sejak 24 Februari 2022*. <https://dunia.tempo.co/read/1576379/sebulan-rusia-serang-ukraina-begini-kronologis-sejak-24-februari-2022>

Adryamarthanino, Verelladevanka. (2022). *Sejarah Hubungan Rusia dan Ukraina.* https://www.kompas.com/stori/read/2022/01/31/100000979/sejarah-hubungan-rusia-dan-ukraina?page=all

Anggraini, Aliffah. *Realisme dalam Studi Keamanan dan Pertahanan.* https://www.academia.edu/43828692/Realisme\_Dalam\_Studi\_Keamanan\_Dan\_Pertahanan

Apriyani, Suharto dan. 2021. “Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional.” *Risalah Hukum* 98-107.

BBC News. (2022). *Mengapa Ukraina ingin bergabung dengan Uni Eropa, apakah akan terwujud ketika perang belum usai?* <https://www.bbc.com/indonesia/dunia-61133424>

Darmono. (2010). KONSEP DAN SISTEM KETAHANAN NASIONAL INDONESIA. *Jurnal Ketahanan Nasional,* 15(1): 1-39. https://jurnal.ugm.ac.id/jkn/article/view/22307/14890

Donnelly, Jack. (2009). *Realism and International Relations*. Cambridge University Press. file:///C:/Users/LENOVO/OneDrive/Documents/Kuliah/Semester%202/E-book%20dan%20materi%20pembelajaran/Teori%20HI/Realisme.pdf

Fanasafa, Irfan. (2022). *Waspada! Kejahatan Phising Mengintai Anda.* https://www.djkn.kemenkeu.go.id/kpknl-purwakarta/baca-artikel/14851/Waspada-Kehajatan-Phising-Mengintai-Anda.html

Hidayat, Muhammad Nizar. (2022). Konstruktivisme dalam Diskursus Kebangkitan Cina di Asia Timur. *INTERDEPENDENCE JOURNAL OF INTERNATIONAL STUDIES*, 3(1): 55-62. https://www.ijis.fisip-unmul.ac.id/site/index.php/ijis/article/download/52/45

Iskandar, Darmanto dan. 2016. “PENERAPAN ALGORITMA DATA ENCRYPTION STANDARD PADA PERANCANGAN APLIKASI KRIPTOGRAFI BERBASIS WEB PADA CYBER DEFENCE.” *INTEKSIS* 3 (2).

Iswara, Aditya Jaya. (2022). Rusia Umumkan 1.351 Tentaranya Tewas, Sedangkan Ukraina 14.000. <https://www.kompas.com/global/read/2022/03/25/221208970/rusia-umumkan-1351-tentaranya-tewas-sedangkan-ukraina-14000>

KEMENTERIAN KOMUNIKASI DDAN INFORMATIKA REPUBLIK INDONESIA. (2017). *Kemenkominfo Siapkan Tentara Cyber.* https://www.kominfo.go.id/content/detail/9089/kemenkominfo-siapkan-tentara-cyber/0/sorotan\_media

Manggala, Pandu Utama. (2016). Strategi Pertahanan dan Keamanan Nasional Indonesia. *Jurnal Kajian Lemhannas RI,* edisi 26: 68-77. https://www.lemhannas.go.id/images/Publikasi\_Humas/Jurnal/Jurnal\_Edisi\_26\_Juni\_2016.pdf

Microsoft Security. *Apa itu serangan DDoS? https://www.microsoft.com/id-id/security/business/security-101/what-is-a-ddos-attack*

Microsoft Security. *Apa itu ransomware? https://www.microsoft.com/id-idsecurity/business/security-101/what-is-ransomware*

Mukhtar, Sidratahta. (2011). KEAMANAN NASIONAL: ANTARA TEORI DAN PRAKTEKNYA DI INDONESIA. *Sociae Polites*, edisi khusus. http://ejournal.uki.ac.id/index.php/sp/article/view/466/353

Ramadhan, Iqbal. (2019). STRATEGI KEAMANAN CYBER SECURITY DI KAWASAN ASIA TENGGARA. *Jurnal Asia Pasific Studies,* 3(2): 182-191. http://ejournal.uki.ac.id/index.php/japs/article/view/1081/1110

Security Encyclopedia. (2023). *BlackEnergy*. <https://www.hypr.com/security-encyclopedia/blackenergy>

Subagyo. 2018. “Sinergi Dalam Menghadapi Ancaman Cyber Warfare.” *Jurnal Pertahanan & Bela Negara* 89-108.

Tribata News. (2019, 15 Jan). *Memahami Konsep Keamanan.* https://tribratanews.kepri.polri.go.id/2019/01/15/memahami-konsep-keamanan/

Triandi, Budi. (2019). Keamanan Informasi secara Aksiologi dalam Menghadapi Era Revolusi Industri 4.0. *Jurnal Riset Komputer,* 6(5): 477-478. http://ejurnal.stmik-budidarma.ac.id/index.php/jurikom/article/view/1556/1243

Wikipedia. (2022). *2022 Ukraine Cyberattacks.* <https://en.wikipedia.org/wiki/2022_Ukraine_cyberattacks>

Wikipedia. (2022). *Invasi Rusia ke Ukraina 2022.* <https://id.wikipedia.org/wiki/Invasi_Rusia_ke_Ukraina_2022>