Signifikansi Perang Siber dalam Konflik Modern Rusia-Ukraina Studi Kasus: Wizard Spider - It Army

Imma Karisma[1], Agussalim Burhanuddin[2]

Universitas Hasanuddin, Indonesia

Immakharisma7@gmail.com[1], agus.unhas@gmail.com[2]

Abstract

The escalation of the conflict between Russia - Ukraine began to experience significant changes to a broad scope and no longer only emphasized the security system on the use of military aspects. Both Russia and Ukraine have made cyberspace important as another part of modern conflicts in the form of cyber wars by focusing on cyber security defense strategies. The significance of this conflict then prompted the creation of the Wizard Spider and the IT Army as cyber-specific organizations as well as supporting actors who play a direct role in the conflict realm. This study uses a qualitative descriptive research method by collecting data from literature studies. The results of the study found that the cyber security system as an attack strategy in the Russia – Ukraine conflict has encouraged the creation of a more modern conflict through confrontational actions in cyberspace carried out by Wizard Spider and the IT Army. This organization has indirectly become a dominant actor through its role in carrying out cyber threats and attacks as well as being a determining actor in the direction of the Russia-Ukraine cyber war conflict.

Keywords: *Russia – Ukraine conflict, Cyber Security, Cyber War, Wizard Spider, IT Army.*

1. PENDAHULUAN

Penggunaan teknologi dalam lingkup internasional telah berkembang pada taraf kemajuan pesat yang menjadikan setiap informasi memegang peranan penting dalam sistem pemerintahan. Setiap negara tidak lagi menjadikan kecanggihan teknologi sebagai ajang pengklarifikasian negara maju, tetapi sebagai bagian dalam mengontrol hubungan antar negara, termasuk konflik dan perang yang secara substansial telah beralih ke cara yang lebih modern. Dalam hal ini, teknologi dan informasi secara tidak langsung telah menciptakan era peperangan yang baru. Akibatnya, perang yang terjadi tidak hanya lagi menggunakan kekuatan militer saja, namun setiap negara kini mampu menciptakan ancaman dan kekacauan bagi kedaulatan negara lain melalui sabotase dan spionase informasi, utamanya dalam hal pertahanan dan keamanan.

Sistem pertahanan dan keamanan negara pun kini menjadi area yang cukup sensitive, utamanya dalam hal perang jaringan dan informasi yang dikenal sebagai *cyber war*. Pada

dasarnya, pembaruan terhadap sistem keamanan berbasis militer dapat dengan mudah untuk dilakukan melalui transformasi anggaran kemiliteran, akan tetapi sistem keamanan yang justru lebih berbasis kepada penggunaan teknologi, informasi dan jaringan akan lebih rentang untuk diterobos, khususnya oleh negara yang memiliki tingkat kecanggihan keamanan yang jauh lebih tinggi. Dengan kata lain, penggunaan dan peningkatan *cyber security* oleh setiap negara dinilai menjadi benteng pertahanan yang strategis dalam menghadapi situasi *cyber war*.

Pada dasarnya, istilah *cyber security* muncul pada tahun 1970 di Amerika Serikat yang kemudian menyebar ke berbagai negara hingga tahun 1990. Istilah *cyber security* sendiri diciptakan oleh pemerintah Amerika Serikat dalam membentuk wacana sebagai ancaman di berbagai entitas negara yang dikenal sebagai "revolusi informasi" dimana teknologi dan informasi dapat berimplikasi terhadap keamanan di lingkup hubungan internasional (Gua Myriam Dunn, 2015 : 402). Dengan demikian, *cyber security* telah menjadi bagian khusus dalam sistem keamanan, khususnya keamanan informasi negara yang meliputi strategi keamanan, kebijakan luar negeri, diplomasi hingga kerahasiaan pemerintahan terhadap penerobosan data dan *hackers* (Rossouw von Solms & Johan van Niekerk, 2012 : 99)

Dalam hal ini juga, informasi menjadi aspek penting dalam strategi *cyber security*. Pada umumnya, peranan sebuah informasi dalam sistem keamanan telah ada pada tahun 1990 sebagai bagian diplomasi dan politik dalam urusan hubungan internasional. Informasi tersebut dinilai mampu mengontrol dan memanajemen sumber daya yang dibutuhkan oleh negara, namun dalam penggunaannya mengalami perubahan signifikan dengan terciptanya berbagai ancaman seperti pengontrolan konflik bersenjata, penggunaan kemiliteran, fenomena *cyber-espionage*, *cyber-crime*, *cyber-attack* hingga *cyber-war*. Oleh karena itu, sebagai bentuk respons pencegahan atas ancaman tersebut, setiap negara mulai menciptakan berbagai aturan terkait *cyber security*.

Akan tetapi, negara yang memiliki sistem *cyber security* yang lebih lemah justru dapat dengan mudah terjebak dalam ancaman tersebut. Hal ini disebabkan karena negara yang memiliki *cyber security* yang jauh lebih canggih dapat dengan mudah mengontrol seluruh informasi rahasia dengan tujuan mengganggu keseimbangan dan merugikan negara lain. Hal tersebut dapat dilihat pada kasus *cyber-war* Estonia oleh Rusia pada 2007 yang diserang oleh gelombang *Distributed Denial of Service* (DDoS) terhadap situs web pemerintahan, parlemen, kementerian, bank dan penyiaran. Penyerangan *cyber security* model DDoS juga terjadi di Georgia yang meliputi situs komersial, media dan pemerintahan. Penyerangan tersebut berdampak cukup besar bagi Georgia karena mampu memicu terjadinya konflik bersenjata pada tahun 2008 dengan Rusia (Mary Ellen O'Connell, 2012:192-193)

Berdasarkan pada kedua kasus sebelumnya, dapat menunjukkan bahwa Rusia termasuk negara yang seringkali melakukan penyerangan *cyber* ke berbagai negara. Selain Estonia dan Georgia, penyerangan *cyber* juga dilakukan terhadap Ukraina. Beberapa dekade terakhir, pembahasan dunia terhadap perang antara Rusia-Ukraina tidak terlepas terhadap bentuk peperangan secara kemiliteran, namun baik Rusia maupun Ukraina juga terlibat langsung dalam *cyber-war*. Rusia yang didukung oleh Kremlin sejak Krimea dicap oleh Moskow, Ukraina mendapatkan serangan *cyber-war* berupa peretasan jaringan yang mengakibatkan gangguan server dan data, spionase, fasilitas sumber energi dan komunikasi di beberapa wilayah hingga disinformasi konflik Rusia-Ukraina (Ahmad Mohee, 2022:1).

Akan tetapi, meski kemampuan *cyber security* yang dimiliki tidak sepenuhnya optimal dalam pengelolaan teknologi dan informasi, Ukraina tetap memberikan serangan perlawanan. Sebagai strategi pertahanan, pemerintah Ukraina membentuk organisasi khusus yang bertugas dalam menangani *cyber security* dan mengintai segala bentuk serangan *cyber-war* dari Rusia. Organisasi tersebut dikenal sebagai "IT Army" yang terdiri atas sukarelawan Ukraina dan masyarakat internasional dari berbagai dunia yang memiliki kemampuan *hacker Underground* dan bersedia untuk menjaga infrastruktur negara Ukraina (cnbc Indonesia).

Sedangkan dari sisi Rusia sendiri juga telah lama memiliki organisasi hacker yang mendukung *cyber security* Rusia secara penuh. Organisasi tersebut bertugas untuk memberikan perlawanan terhadap negara yang dianggap sebagai musuh Rusia yang dikenal dengan nama "Wizard Spider" (cnbcIndonesia). Dengan kata lain, pembentukan Wizard Spider tersebut akan mengambil bagian penting dalam melakukan penyerangan dan menyabotase seluruh siber, melumpuhkan sistem *cyber security* dan memudahkan pemerintahan Rusia dalam mengontrol pertahanan negara lain.

Konflik dan perang antara Rusia – Ukraina, khususnya dalam menargetkan pertahanan melalui *cyber security*, baik organisasi IT Army maupun Wizard Spider akan saling konfrontasi satu sama lain. Meski bentuk konflik yang terjadi melalui dunia maya, akan tetapi peranan dan hasil dari *cyber-war* dari kedua non-aktor tersebut akan sangat menguntungkan bagi masing-masing negara yang berkonflik, utamanya dalam hal menyusun strategi dan melakukan penyerangan balik. Kemudian di sisi lain, keterlibatan IT Army dan Wizard Spider dalam konflik ini juga akan berpengaruh besar pada imbasnya penyalahgunaan informasi dan pengubahan sudut pandang negara lain terhadap konflik Rusia – Ukraina.

Oleh karena itu, dalam mempertahankan *cyber security* kedua negara di tengah konfrontasi cyber-war, maka organisasi tersebut harus terlibat secara proaktif dalam mengelola teknologi dan jaringan. Karenanya peranan "IT Army" dan "Wizard Spider" dalam *cyber security* terhadap konflik Rusia-Ukraina menjadi tujuan penting sebagai bagian topik pembahasan dalam

penelitian ini. Dalam hal ini, dengan mengetahui seberapa besar peranan dan otoritas yang dimiliki dalam mengelolah *cyber security*, maka baik IT Army maupun Wizard Spider akan menjadi aktor yang menentukan dan memegang bagian lain dari keberlangsungan konflik.

2. METODE PENELITIAN

Metode pendekatan penelitian yang digunakan dalam penelitian ini adalah pendekatan kualitatif dengan menggunakan metode deskriptif. Pada umumnya, metode deskriptif merupakan metode penelitian yang objeknya berfokus pada sekelompok manusia, kondisi, pemikiran atau bahkan peristiwa yang terjadi pada masa kini (Nazir, 2017). Untuk memperoleh data penelitian, maka digunakan teknik pengumpulan data primer yang berupa situs resmi dari pemerintah dan surat kabar baik secara nasional maupun internasional dan teknik pengumpulan data sekunder dalam bentuk *library research* yakni teknik memperoleh informasi dengan menggunakan literatur yang relevan dengan topik penelitian yang diperoleh dari berbagai kajian penelitian seperti dokumen resmi, artikel, jurnal hingga buku dan berita yang didapatkan dari berbagai referensi.

Objek yang dikaji dalam penelitian ini berfokus pada peranan penting dari organisasi khusus yang dibentuk oleh Rusia-Ukraina dalam menghadapi dan membendung berbagai bentuk penyerangan dan ancaman terhadap *cyber security*. Penelitian menggunakan konsep pertahanan dan keamanan yang berfokus pada penggunaan teknologi dan jaringan (*cyber security*) sebagai kerangka untuk menggambarkan strategi yang digunakan oleh organisasi IT Army-Ukraina dan Wizard Spider-Rusia sebagai salah satu aktor yang berperan penting dalam membendung konfrontasi konflik Rusia-Ukraina, khususnya *cyber-war*.

3. PEMBAHASAN

3.1. Ancaman Cyber Security Dalam Dilematis Cyber War

Esensial keamanan bagi negara terus mengalami transformasi di setiap periodenya. Pada umumnya, setiap negara selalu menggunakan pendekatan kemiliteran sebagai hal utama dalam melindungi negara dari berbagai bentuk ancaman. Akibatnya, kapabilitas militer mulai diagungkan sebagai power yang harus dimiliki oleh setiap negara dalam tatanan internasional. Selain militer, keberadaan politik, ekonomi dan sosial budaya dalam sistem internasional juga berperan penting untuk meningkatkan esensial keamanan tersebut. Dalam bukunya "Security: A New Framework of Analysis", Barry Buzan (1998) menyatakan bahwa perkembangan sistem keamanan negara pada era perang dingin hanya berfokus pada peningkatan militer dan politik, namun pada dasarnya, sistem keamanan tersebut memiliki cakupan yang jauh lebih luas yang meliputi ekonomi, lingkungan dan sosial budaya (Iqbal Ramadhan, 182).

Akan tetapi, di tengah pusat perkembangan globalisasi yang semakin terdigitalisasi menjadikan tatanan sistem internasional turut mengubah esensial keamanan itu sendiri. Berdasarkan buku yang ditulisnya "*The Future of Power*", Joseph S. Nye (2011) menyatakan bahwa sistem keamanan tidak hanya terdiri atas lima sektor, akan tetapi terdapat enam sektor penting yang mendukung keamanan suatu negara yakni militer, politik, ekonomi, lingkungan, sosial dan siber (Iqbal Ramadhan, 2019:182). Dalam hal ini, keberlangsungan tatanan sosial termasuk negara telah menjadi bagian penting yang diatur dalam peranan dunia maya (*cyberspace*).

Asumsi tersebut juga disampaikan oleh Nir Kshetri (2011) melalui tulisannya yang berjudul "*Cyber Security and International Relations: The US Engagement with China and Russia*" bahwa esensial siber dalam *cyberspace* merupakan bagian lain dari keamanan negara yang mencakupi keamanan militer, udara, air dan darat. Lebih lanjut, Kshetri juga menyatakan bahwa hubungan yang terbentuk antar negara akan sangat memungkinkan dipengaruhi oleh tindakan aktor lain dalam lingkup *cyberspace* (Iqbal Ramadhan, 2019:182). Dengan demikian, kehadiran negara dalam tatanan sistem internasional mulai terdigitalisasi dan dikelola dalam *cyberspace*. Namun keberadaan siber dalam sistem keamanan juga memiliki kelemahan berupa ancaman dan penyerangan yang bisa saja terjadi.

Seperti halnya ancaman keamanan pada sektor lainnya, ancaman terhadap *cyber security* lebih kepada serangan melalui *cyberspace*. Dalam hal ini, *cyberspace* merupakan domain dimana seluruh negara mulai berlomba-lomba untuk saling menyerang informasi satu sama lainnya untuk menjatuhkan. Berdasarkan pengertian *International Telecommunication Union United Nation* (ITU UN) bahwa *cyberspac*e merupakan *terrain* yang tercipta oleh adanya hubungan antar sistem komputer, jaringan, dan data baik secara fisik maupun non-fisik. Kemudian, *US Military Document* juga mendeskripsikan *cyberspace* sebagai regional global yang didalamnya terdiri antar jaringan, teknologi informasi, telekomunikasi, komputer hingga prosesor (Miko Aditiya Suharto, dkk 2021:99). Oleh karena itu, *cyberspace* menjadi medan yang sangat rentan untuk terjadinya ancaman seperti *cyber-attack*, *cyber-crime*, *cyber-warfare*, *cyber-espionage* hingga *cyber-war*.

Ancaman dan serangan terhadap *cyber security* tentunya tidak hanya dilakukan oleh negara saja, melainkan berbagai entitas juga mampu menjadi aktor lain dalam penyerangan tersebut seperti kelompok, individu, organisasi, hingga golongan. Sumber dari ancaman itu sendiri dapat berupa ancaman eksternal – internal, investigasi, kegiatan intelijen, organisasi ektrim, kelompok kejahatan terorganisir seperti terrorism, hingga aktivitas *hacker* (Bram R. Sanjaya, dkk 2022:25). Akibatnya, ancaman terhadap *cyber security* juga memiliki berbagai tingkatan dengan konsekuensi dampak yang buruk. Menurut Myriam Dunn Cavelty (2010), tipologi

ancaman terdiri atas tiga tingkatan yakni *cyber-crime*, *cyber-war* dan *cyber-terrorism*. Selain itu, Aronson (2005) juga turut memaparkan tiga tipologi ancaman lainnya yakni *intelligence gathering*, *hacking* dan *cyber-war* (Iqbal Ramadhan, 2019:182-183)

Diantaran tipologi ancaman tersebut, *cyber-war* termasuk bentuk ancaman yang sering digunakan oleh setiap negara dalam menyerang negara lainnya. Pada dasarnya, negara merupakan objek utama dalam *cyber-war* dan kedaulatan menjadi target sasaran dalam negara tersebut. *Cyber-war* memungkinkan sebuah negara untuk mengancam kedaulatan negara lainnya baik secara politik maupun keamanan. Jika seluruh aspek pertahanan yang dimiliki oleh sebuah negara terintegrasi sebagai informasi rahasia maka peretasan keamanan tersebut akan sangat memungkinkan terjadi dan berakibat pada terancamnya kedaulatan negara. Serangan terhadap *cyber security* dalam *cyber-war* dilakukan melalui media informasi untuk menciptakan kerentanan keamanan seperti propaganda, manipulasi dan distorsi informasi untuk menciptakan ancaman perang. Selain itu, spionase dan sabotase juga sering dilakukan melalui penggunaan kode jaringan untuk meretas jaringan keamanan.

Sehingga dalam lingkup hubungan internasional, konflik *cyber-war* yang melibatkan berbagai negara dan entitas aktor lainnya dalam ancaman *cyber security* seringkali terjadi, salah satunya yakni peristiwa *cyberspace-war* pada tahun 2001 yang merupakan konflik ancaman *cyber security* berskala besar yang melibatkan banyak negara saling berperang informasi dalam *cyberspace*. Dalam peristiwa ini, Amerika Serikat dan Cina merupakan negara yang menjadi target penyerangan siber. Baik Amerika Serikat maupun Cina mengalami kerusakan terhadap situs web nasional mereka akibat serangan peretasan jaringan oleh gelombang DDoS. Selain itu, pesawat pengintai milik Amerika Serikat juga menjadi sasaran sehingga terpaksa melakukan pendaratan di daratan Cina. Diketahui bahwa negara yang menjadi aktor penyerang dalam peristiwa tersebut meliputi Jepang, Korea, Arab Saudi, India, Malaysia, Argentina, Pakistan dan Brazil.

Akan tetapi, Ancaman terhadap *cyber security* yang pertama kali sebenarnya terjadi pada peristiwa Perang Teluk di tahun 1991 yang melibatkan negara-negara Middle East dan Amerika Serikat. Dalam Perang Teluk tersebut, kemiliteran Amerika Serikat merupakan aktor yang melakukan penyerangan siber dan menjadikan kemampuan perang informasi mulai memegang peranan strategis dalam menentukan arah peperangan sehingga ketergantungan penggunaan kemampuan fisik seperti kemiliteran oleh negara Middle East hanya memiliki peranan dalam skala kecil (Gua Myriam Dunn, 2015:409)

Oleh karena itu, dalam *cyber-war*, setiap negara akan lebih cenderung memprioritaskan penggunaan digital, termasuk meningkatkan kemajuan teknologi dan jaringan sehingga dinilai mampu menjadi benteng pertahanan dalam *cyberspace*. Akan tetapi, jika sebuah negara tidak

mampu mengamankan *cyber security* yang dimilikinya, maka akan dengan sangat mudah untuk dimanfaatkan oleh negara lain. Akibatnya, ketika terjadinya *cyber-war*, negara tersebut tidak akan bisa melakukan serangan balik dan tingkat pertahanan diri yang lemah akan menjadikan keamanannya sendiri terancam oleh pihak musuh. Dengan kata lain, negara yang memiliki *cyber security* yang lemah akan berakhir dikuasai oleh negara lain dan hal inilah yang kemudian menjadikan kekalahan telak bagi sebuah negara dalam *cyber-war*.

3.2. Konfrontasi Cyber Security Konflik Rusia – Ukraina

Eskalasi konflik dan perang antara Rusia dan Ukraina pada dekade terakhir ini mengantarkan tatanan hubungan internasional pada situasi yang rumit. Pada tahun 1991, Ukraina menyatakan kemerdekaannya terhadap Uni Soviet dan hubungannya dengan Rusia tetap terjalin dengan sangat baik yang dapat dilihat dari rumpun budayanya dan letak kedua negara tersebut bahkan Rusia merupakan negara yang paling dekat dengan Ukraina dibandingkan negara pecahan Uni Soviet lainnya. Namun, kedekatan tersebut pecah menjadi sebuah konflik saat Rusia mulai menginvasi kawasan Krimea pada tahun 2014 (Ujang Priyono, 2022:44-45). Konflik tersebut terus membesar hingga menciptakan peperangan yang besar antara Rusia – Ukraina sampai saat ini.

Dalam perang antara Rusia – Ukraina, penggunaan kekuatan kemiliteran menjadi power yang mutlak harus ada. Akan tetapi, selain perang militer yang dapat terlihat secara objektif, perang Rusia – Ukraina juga telah meluas hingga ke ranah *cyberspace* yang dalam hal ini baik Rusia maupun Ukraina menggunakan siber sebagai strategi lain untuk mengincar dan meruntuhkan keamanan dari internal negara masing-masing. Perang yang menggunakan siber sebagai persenjataan kemudian dikenal sebagai *cyber-war* dan sistem *cyber security* menjadi target sekaligus benteng pertahanan terkuat untuk kedua negara saat ini.

Pada dasarnya, *cyber-war* Rusia – Ukraina telah terjadi pada tahun 2014 hingga 2015 yang kemudian meningkat hingga tahun 2022 dan menjadi bagian tersendiri dalam konflik yang terjadi. Jika dilihat berdasarkan perbandingan kecanggihan teknologi dan sarana informasi, Rusia menunjukkan kekuatan *cyber security* yang dominan dibandingkan Ukraina. Kemampuan siber Rusia sendiri merupakan salah satu aspek yang dinilai sangat penting utamanya pada sistem keamanan sejak 15 tahun lalu dan mengembangkannya sebagai *cyber security offensive* dalam menjatuhkan negara lain yang dianggap sebagai musuh melalui pengelolaan informasi *cyberspace*. Dalam hal ini, Rusia mengembangkan strategi kampanye informasi dan spektrum militer untuk menciptakan propaganda sebagai ancaman disinformasi sehingga infrastruktur dan kemampuan kekuatan militer musuh terganggu (Marcus Willet, 2022:9).

Dalam melakukan ancaman siber, Rusia menggunakan berbagai perangkat yang kemudian melakukan penyerangan pada sistem informasi dan jaringan yang dianggap bernilai strategis bagi negara lain seperti situs pemerintahan hingga penyiaran. Berdasarkan informasi artikel yang ditulis oleh Joe Robinson yang merupakan seorang pakar invasi dan keamanan siber menyatakan bahwa Rusia telah melakukan berbagai serangan *cyberspace* kepada 19 negara dan menghasilkan sebanyak 75 serangan dalam rentang waktu 2009 hingga 2019. Dalam serangan siber tersebut, Amerika Serikat dan negara Eropa menjadi target sasaran yang utama, khususnya Ukraina sebagai negara yang paling sering mendapatkan serangan siber dalam kurun waktu yang singkat yakni antara tahun 2017 – 2019 terdapat 9 total serangan (Ujang Priyono, 2022:48).

Selain sistematika dan strategi *cyber security offensive*, Pemerintahan Rusia juga didukung oleh peranan beberapa aktor penting baik yang berada dibawah naungan kementerian pertahanan maupun kelompok pro-Rusia. Dalam menanggapi operasi *cyberspace* dan sistem *cyber security*, Rusia membentuk empat lembaga resmi yang bertugas dalam menunjang pertahanan dan keamanan Rusia yakni *The Russian Federal Security Service* (FSB), *Main Directorate of the General Staff of the Armed Forces* (GU), *Russian Foreign Intelligence Service* (SVR) dan *Central Scientific Institute of Chemistry and Mechanics*. Dalam melakukan penyerangan, masing-masing lembaga tersebut memiliki target yang berbeda seperti sektor bisnis, ekonomi, dan sebagainya. Selain itu, lembaga-lembaga tersebut juga sering melakukan serangkaian bentuk kerja sama seperti kelompok gabungan *Fancy Bear* (GRU), *Cozy Bear* (SVR) dan *Multiple Specialized Units* (PSYOPS).

Berdasarkan karya tulisnya yang bertulis *Cyber Warfare: A Part of the Russo-Ukrainian War in 2022*, Jari Juutilainen (2022) menyatakan bahwa dalam menjalankan tugas dan menunjang sistem keamanan Rusia, lembaga-lembaga tersebut membentuk beberapa unit tertentu dengan target penyerangan masin-masing, yakni :

1. *The Russian Federal Security Service* (FSB)
    a. *Berserk Bear*: Menargetkan penyerangan terhadap perusahaan energi barat.
    b. *Primitive Bear*: Melakukan serangan siber melalui penggunaan operasi malware ke berbagai negara.
    c. *Venomous Bear*: Menargetkan keamanan NATO, Badan Intelijen dan Kontraktor Sistem Pertahanan melalui kampanye spionase dan pembajakan komunikasi satelit.
2. *Russian Foreign Intelligence Service (SVR)*

    Dalam SVR, hanya terdiri atas satu unit yang dikenal dengan *Cozy Bear*. Kemampuan dari Cozy Bear lebih kepada penghapusan dan pembatasan jejak digital Rusia dan

menargetkan beberapa organisasi infrastruktur penting, salah satunya organisasi milik Amerika Serikat.

3. *Main Directorate of the General Staff of the Armed Forces (GU)*
   a. *Fancy Bear*: Menargetkan penyerangan siber terhadap NATO, organisasi pemerintahan, kemiliteran, organisasi infrastruktur penting, lembaga penelitian dan pendidikan.
   b. *Voodoo Bear*: Menargetkan organisasi infrastruktur kritis, seperti sektor energi, sektor keuangan dan sistem transportasi dengan cara yang lebih merusak dan mengganggu menggunakan malware jika dibandingkan unit lainnya.
   c. *Ember Bear*: Meski tidak ada target khusus yang menjadi sasaran penyerangan siber namun targetnya kurang lebih seperti Fancy Bear dan Voodoos' Bear
4. *Central Scientific Institute of Chemistry and Mechanics (TsNIIKhM)*

   Dalam menjalankan tugasnya, lembaga ini tidak memiliki unit khusus yang berada dibawah naungannya. Akan tetapi, lembaga tersebut merupakan pusat penelitian penting yang di berada langsung dibawah naungan Kementerian Pertahanan Rusia dalam menciptakan serangkaian malware yang bersifat merusak *cyberspace* negara target seperti malware Triton.
5. *Organized-Crime Groups & Other*
   a. *Wizard Spider*: Kelompok terorganisir dan melakukan penyerangan siber melalui serangan malware dan ransomware yang dikenal dengan Conti atau TrickBot
   b. *Invisi Mole*: Kelompok yang berkaitan dengan unit Primitive Bear dalam hal penyerangan siber. Dalam melakukan aksi penyerangan biasanya melalui aksi spionase cyberspace dengan penggunaan senjata kompleks dan canggih.

Pada dasarnya, semua bentuk serangan dan ancaman terhadap *cyber security* ini tentunya mulai memicu tindakan serangan balasan dari pihak Ukraina sendiri. Jika dibandingkan dengan sistem *cyber security* Rusia yang lebih dominan, sistem *cyber security* milik Ukraina tergolong sangatlah rentang untuk diterobos bahkan serangan tersebut sudah menjadi sebuah teror bagi Ukraina. Akan tetapi, hal tersebut tidak menutup kemungkinan bagi Ukraina memberikan serangan dan ancaman balasan. Serangan *cyber security* oleh Rusia terhadap Ukraina termasuk serangan yang frontal dan bukan hanya mengancam keamanan Ukraina saja, namun NATO, Uni Eropa dan Amerika Serikat turut mengambil andil dalam menangani *cyber-war* tersebut.

Dalam hal ini, jika Rusia memiliki kecanggihan teknologi dan siber yang meningkat, maka Ukraina justru mendapatkan dukungan penuh dari pihak NATO, Uni Eropa dan Amerika Serikat. Dengan kata lain, keberpihakan NATO, Uni Eropa dan Amerika Serikat secara tidak langsung telah memfasilitasi *cyber security* Ukraina. keikutsertaan NATO, Uni

Eropa dan Amerika Serikat dalam konflik *cyber-war* Rusia-Ukraina dinilai sebagai hal yang penting untuk dilakukan karena serangan siber Rusia dinilai mampu merusak dan mempropaganda situs yang dinilai strategis dan kemungkinan bahayanya yang sangat besar perlu untuk dicegah.

Selain dukungan dan keikutsertaan beberapa aktor eksternal dalam penyerangan siber tersebut, pemerintahan Ukraina sendiri juga memiliki beberapa lembaga resmi yang berperan strategis dalam membendung aktivitas serangan siber Rusia. Lebih lanjutnya, Jari Juutilainen (2022) menyatakan dalam penelitiannya bahwa lembaga-lembaga tersebut tidak memiliki unit lainnya namun lebih kepada penugasan secara langsung, diantaranya:

1. *State Service of Special Communication and Information Protection of Ukraine (SSSCIP)*

   SSSCIP merupakan Badan Pertahanan sekaligus lembaga khusus yang bertugas dalam melindungi dan meningkatkan keamanan *cyberspace* Ukraina. Dalam menjalankan tugasnya, SSSCIP menyediakan beberapa layanan diantaranya menjalankan analisis ancamanan *cyberspace*, operasi nasional investigasi, mengeluarkan maklumat perilisan data serta membantu organisasi swasta dalam menghadapi ancaman *cyberspace.*
2. *Security Service of Ukraine (SSU/SBU)*

   jika SSSCIP bertugas dalam meningkatkan keamanan cyberspace, maka SSU lebih kepada melindungi tatanan kenegaraan bangsa Ukraina, kegiatan kontra terorisme dan kontra-intelijen serta melakukan perlawan terhadap berbagai ancaman cyberspace Ukraina seperti *cyber-attack* dan *cyber-terror*.
3. *Cyber Police of Ukraine*

   Merupakan unit kepolisian nasional Ukraina dimana tugas dan wewenangnya telah diatur dalam ketentuan Kementerian Dalam Negeri Ukraina. Sesuai dengan namanya, *cyber police* milik Ukraina bertugas dalam menegakkan hukum, memberikan sanksi terhadap penjahat siber dan memberikan peringatan kejahatan *cyberspace* terhadap warga masyarakat Ukraina.
4. *Defense Intelligence of Ukraine (GUR)*

   Badan Intelijen Pertahanan merupakan salah satu unit dibawah naungan Kementerian Pertahanan Ukraina. Badan Intelijen ini bertugas dalam mengumpulkan dan menganalisis berbagai informasi penting yang berkaitan dengan pengembangan kemampuan militer, pertahanan bidang militer dan teknis militer dalam menjaga keamanan *cyberspace*. Selain itu, juga terdapat unit lainnya yakni *Ukraine's Defense Intelligence Service* (GURMO) yang

dijalankan oleh unit khusus siber. Namun tugas dan peranannya hampir berkaitan dengan *Defense Intelligence of Ukraine*.

5. *IT Army of Ukraine*

Tentara TI Ukraina merupakan kelompok aktivis Ukraina yang pada awal pendiriannya didirikan melalui penggabungan beberapa perusahaan keamanan *cyberspace* Ukraina yang kemudian meluas melalui penggunaan sukarelawan yang berbasis pada terciptanya tentara *cyber security* melalui Kementerian Transformasi Digital Ukraina. Tentara Teknologi Informasi ini berfokus pada partisipasinya dalam operasi siber dengan menjadikan Rusia sebagai target penyerangan. Dalam hal ini, IT Army Ukraine bisa mengeksploitasi peralatan canggih untuk melawan serangan siber Rusia termasuk DDoS.

Serangan *cyber security* yang mampu menciptakan konflik *cyber-war* antara Rusia-Ukraina sebenarnya juga tidak terlepas dari partisipasi beberapa aktor yang handal di bidang siber. Selain lembaga-lembaga resmi yang menangani permasalahan siber di masing-masing negara, *cyber-war* juga tercipta karena adanya keikutsertaan aktor seperti Perusahaan Swasta dan *Hacktivism*. Dalam hal ini, baik Rusia maupun Ukraina membentuk kerja sama dengan beberapa perusahaan swasta yang mampu menyediakan layanan siber yang tentunya menguntungkan. Perusahaan Swasta tersebut dapat berupa Microsoft, ESET dan Starlink.

Selain itu, *cyber-war* Rusia-Ukraina juga telah menjadi domain bagi peningkatan penggunaan Hacktivism di dunia. Dengan kata lain, keikutsertaan Hacktivism dalam konflik Rusia-Ukraina sama halnya dengan keikutsertaan bagi seluruh masyarakat internasional dalam konflik tersebut. Dalam hal ini, masyarakat internasional mendedikasikan dirinya sebagai Hacktivism untuk ikut terlibat secara tidak langsung melalui ancaman dan serangan siber. Kehadiran Hacktivism ini dalam konflik Rusia-Ukraina dapat dilihat pada kehadiran Wizard Spider di Rusia dan IT Army di Ukraina. Meski keterlibatannya secara tidak spesifik namun hasil dari serangan tersebut akan menguntungkan dan merugikan bagi Rusia dan Ukraina. Hacktivism tersebut dapat berupa Anonymous, Belarusian Cyber Partisans, Network Battalion65 dan Cyber Defence.

3.3. *IT Army* vs *Wizard Spider* Dalam Cyber War Konflik Rusia – Ukraina

Dalam dekade terakhir ini, konflik yang terjadi antara Rusia – Ukraina mulai berkembang hingga ke ranah lingkup yang luas. Dalam hal ini, berbagai strategi mulai diciptakan oleh kedua negara baik dalam hal kemiliteran maupun *cyberspace*. Tentunya, jika *cyberspace* mulai digunakan sebagai domain dalam konflik ini, maka kapasitas *cyber security* menjadi benteng pertahanan yang strategis dalam menghadapi potensi terjadinya

cyber-war. berbeda halnya dengan pasukan keamanan militer, *cyber security* lebih mengandalkan individu atau perusahaan yang bergerak dalam bidang hacker dan siber sehingga tingkat keterlibatan aktor lain dalam konflik Rusia-Ukraina semakin meluas.

Demi menunjang kemampuan dan kapasitas *cyber security* dan mencegah berbagai ancaman dan serangan siber, baik Rusia maupun Ukraina memiliki organisasi khusus yang diberikan tugas dan wewenang secara langsung dibawah Kementerian Pertahanan masing-masing negara. Dengan kata lain, konfrontasi Rusia-Ukraina dalam *cyberspace* secara tidak langsung dilakukan oleh organisasi tersebut dengan tujuan mengendalikan dan meretas sistem siber untuk melemahkan pertahanan internal negara. Melalui *Federal Bureau of Investigation* (FBI), pemerintahan Rusia membuat organisasi terorganisir yang berasal dari kelompok intelijen militer Rusia yang dikenal sebagai Wizard Spider. Sedangkan dari pihak pemerintahan Ukraina, melalui *Minister of Digital Transformation* merekrut masyarakat internasional untuk menjadi volunteer dalam organisasi khusus yang bernama IT Army.

Dalam pertahanan sistem *cyber security*, Rusia termasuk negara dengan kemampuan siber yang tinggi dan hal tersebut dibuktikan melalui berbagai serangan dan ancaman yang diberikan ke berbagai negara. Oleh karena itu, untuk lebih mengembangkan kapasitas siber yang dimilikinya, pemerintahan Rusia mulai membentuk organisasi terorganisir Wizard Spider sebagai lembaga yang bertugas untuk melakukan penyerangan ke berbagai negara yang merupakan target dari Wizard Spider tersebut. Wizard Spider sendiri terdiri atas individu yang tergabung dalam kelompok militer intelijen Rusia yang kemudian diberikan perlengkapan khusus dalam melakukan serangan siber dan struktur organisasinya beroperasi seperti *Saint Petersburg* yang merupakan sub-bagian dari lembaga *Central Scientific Institute of Chemistry and Mechanics* (Jari Juutilainen, 2022:51**)**

Oleh karena itu, Wizard Spider seringkali menggunakan malware atau ransomware dalam melakukan operasi penyerangan siber yang dikenal dengan Trickbot, Ryuk dan Conti. Kemampuan serangannya pun dikenal sangat merugikan dan bersifat merusak karena mampu meretas siber beberapa negara sekaligus dalam cakupannya yang luas. Menurut Jeff Burt yang dikutip melalui theregister, bahwa Wizard Spider memiliki kemampuan kontrol hingga ribuan situs web perangkat klien yang tersebar di berbagai negara di dunia dengan menggunakan koneksi server seperti malware proxy SystemBC. Dalam tulisannya juga menyatakan bahwa sebanyak 128.036 server yang diretas oleh SystemBC.

Sedangkan berdasarkan data *Federal Bureau of Investigation* (FBI), Wizard Spider telah melakukan penyerangan setidaknya sebanyak 400 serangan sukses di seluruh dunia sejak awal dibentuknya dan 290 serangan tersebut diantaranya ditargetkan kepada Amerika

Serikat. Namun pada dasarnya, target penyerangan siber Wizard Spider tidak jauh berbeda dari lembaga keamanan siber Rusia lainnya. Dalam hal ini, Wizard Spider menargetkan organisasi pemerintah, lembaga hukum, pelayanan kesehatan dan berbagai infrastruktur lainnya. Kemudian, berdasarkan penelitian keamanan Ukraina, bahwa selain menggunakan ransomware, Wizard Spider juga mulai mengembangkan versi eksploitasi firmware melalui kerja sama dengan *The Russian Federal Security Service* (FSB) dalam penciptaannya (Jari Juutilainen, 2022:51**).**

Dengan kemampuan serangan siber yang canggih menjadikan keterlibatan Wizard Spider dalam konflik Rusia-Ukraina sebagai salah satu aktor yang memiliki peranan strategis. Dalam hal ini, serangan dan ancaman siber yang diberikan mampu membuat sistem *cyber security* Ukraina melemah. Bukan hanya itu, pengaruh dan dampak dari serangan tersebut tidak hanya berpengaruh terhadap Ukraina saja, akan tetapi negara-negara lainnya turut mengecam tindakan tersebut seperti negara keanggotaan NATO, Uni Eropa hingga Amerika Serikat bahkan pihak Amerika Serikat sendiri membentuk *Cybersecurity Advisory* (CSA) bersama dengan Australia, Kanada, New Zealand dan Inggris dalam menanggapi tindakan ancaman siber Rusia (CISA.gov)

Sedangkan serangan dan ancaman *cyber security* yang seringkali dilakukan oleh Wizard Spider terhadap Ukraina yakni berupa *cyber-espionage* dan wacana propaganda. Ancaman ini terus menerus di dapatkan Ukraina sejak peristiwa Euromaidan, yakni penggulingan Presiden Ukraina, Viktor Yanukovych dan intervensi Rusia di Krimea (Greg Simons, dkk, 2020:2). Serangan *cyber security* terhadap Ukraina menjelang pemilihan umum di tahun 2014 merupakan serangan *cyber security* pertama yang dilancarkan oleh Rusia dengan menerobos *cyberspace* Ukraina dan masuk kedalam akses perhitungan suara untuk menghancurkan dan menghapus seluruh catatan elektronik hasil perhitungan suara (Ahmad Mohee, 2022:2)

Selain menghancurkan dan menghapuskan seluruh catatan elektronik pemungutan suara, Wizard Spider juga merusak seluruh sistem telekomunikasi milik Krimea melalui penyerangan situs dan pesan-pesan yang mengandung dukungan terhadap Ukraina mengalami pemblokiran secara permanen (Alika Gachua dan Thorndike Zedelashvili 2020:24). Kemudian, pada 2015, Wizard Spider kembali melakukan serangan siber dengan mengincar fasilitas listrik yang merupakan sarana penting di Ukraina. Akibatnya, sebagian besar wilayah barat Ukraina dan sebagian lagi wilayah kiev mengalami pemadaman listrik selama beberapa jam (Ahmad Mohee, 2022:3).

Berbeda dengan bentuk penyerangan sebelumnya, serangan siber yang juga terjadi di tahun 2017 justru memiliki pengaruh dan cakupan yang jauh lebih besar yang

tidak hanya mencakup wilayah Ukraina saja, namun beberapa negara seperti Italia, Perancis, Jerman dan negara Uni Eropa lainnya juga terdampak serangan tersebut. Peristiwa ini dikenal sebagai serangan NotPetya dengan menggunakan sistem malware yang menyebar ke seluruh dunia. Serangan siber ini termasuk serangan malware yang terbesar dalam sejarah berdasarkan dampak kerugian dan kekacauan yang diakibatkannya mampu melumpuhkan keuangan seluruh dunia Selain itu, beberapa perangkat lunak perusahaan multinasional seperti Merck, FedEx, Maersk, dan perusahaan pengiriman Denmark yang mencakup seperlima dari keseluruhan kapasitas pengiriman dunia juga ikut terancam.

Berdasarkan hasil penyelidikan Amerika Serikat, total kerugian finansial global yang diakibatkan serangan NotPetya tersebut mencakup $10 miliar. Bagi Ukraina sendiri, serangan NotPetya tersebut menjangkit dan meretas hampir keseluruhan situs internal Kabinet kementerian di Ukraina yang menjadi target sasaran. Namun, beberapa server lainnya seperti perusahaan energi, Bank Nasional, Metro Kyiv hingga Bandara Boryspil juga ikut terpengaruh. Beberapa aktor di bidang siber dan IT Army memperkirakan bahwa sebanyak 10% dari keseluruhan komputer di Ukraina terpengaruh bahkan perusahaan independent di Kyiv, Mitra Keamanan Sistem Informasi menyatakan bahwa sekitar 300 perusahaan juga mendapatkan dampak yang sama.

Serangan siber Wizard Spider berlanjut hingga tahun 2022 dan sekaligus merupakan serangan terakhir dalam catatan *cyber-war* oleh pemerintahan Rusia di Ukraina. Pada tahun tersebut, sebanyak 3 serangan siber berturut-turut yang dilakukan oleh kelompok intelijen tersebut. Serangan pertama, pada 15 Januari 2022 berupa penyerangan gelombang ransomware dengan istilah whisper Gate. Target sasarannya yakni nirlaba, organisasi pemerintah, lembaga teknologi informasi Ukraina. Serangan kedua, pada 19 Januari 2022 terhadap *cyberspace* yang bertujuan untuk mengganggu dan mengalihkan fungsi *Global Affairs Canada* setelah pemerintahan Kanada memberikan dukungan kepada Ukraina terkait konflik Rusia – Ukraina yang terjadi. Terakhir pada Februari 2022, Wizard Spider menargetkan peneroran siber terhadap kantor pusat kemiliteran Ukraina beserta jaringan pemerintahan yang bertugas dalam memberikan pelayanan keamanan informasi Rusia.

Sebagai bentuk konfrontasi dengan Wizard Spider dalam mempertahankan *cyber security* Ukraina, IT Army tentunya melakukan berbagai bentuk serangan dan ancaman balasan terhadap *cyber security* Rusia. Akan tetapi, serangan dan ancaman tersebut berbeda jauh terkait dampak dan pengaruh yang diakibatkan oleh Wizard Spider. Namun, meski cakupan yang sempit yakni hanya berfokus pada *cyber security* Rusia dan dampak

yang terbatas, serangan tersebut mampu menghentikan berbagai jenis gelombang jaringan dan malware yang dilakukan oleh Wizard Spider bahkan cukup kuat untuk melawan beberapa serangan siber Wizard Spider di tahun-tahun tertentu yang bisa menciptakan *cyber-war* di kedua negara.

IT Army merupakan kelompok khusus yang beranggotakan masyarakat Ukraina dan masyarakat internasional pro-Ukraina secara keseluruhan yang bergabung sebagai volunteer dalam menciptakan dan melindungi *cyber security* Ukraina. Diantara lembaga pertahanan *cyber security* Ukraina, IT Army termasuk organisasi yang baru terbentuk yakni pada tahun 2020 oleh Yegor Aushey, seorang pengusaha teknologi informasi Ukraina sekaligus pendiri perusahaan Cyber Tech, Hacken.io dan Cyber School. Awal penggagasan pendirian IT Army dilakukan pada tanggal 24-26 Februari yang diajukan oleh Yegor Aushey kepada Mykhailo Federov yang merupakan Menteri Transformasi Digital Ukraina. Diwaktu yang sama, Aushey juga mengumpulkan sebanyak 1.000 individu sukarelawan *cyber security* atas dukungan penuh salah satu pejabat senior di Kementerian Pertahanan Ukraina (Soesanto, 2020:6)

Melalui gagasan tersebut, Fedorov mulai melakukan pemberitahuan secara luas kepada masyarakat melalui penggunaan media sosial seperti facebook, twitter dan telegram pada tahun 2020 mengenai keikutsertaan masyarakat internasional sebagai sukarelawan dalam mendukung cyberspace Ukraina yang terdiri atas keahlian bidang digital, ahli dunia maya, copywriter, desainer, ahli penargetan dan pemasaran. Hasilnya, pada tanggal 26 Februari 2020 hanya sebanyak 175.000 sukarelawan yang tergabung lalu meningkat sebanyak 307.165 sejak tanggal 26 Maret hingga 10 Juni 2020 berdasarkan informasi TAGStat yang merupakan platform analitik saluran obrolan telegram (Soesanto, 2020:8).

Kemudian, tugas dan peranan IT Army hanya difokuskan pada bidang siber dengan tujuan untuk meningkatkan strategis *cyber security*, melindungi *cyberspace* Ukraina dari berbagai gelombang asing dan menangani *cyber-war* dari Rusia. Pada dasarnya, IT Army dibagi dua kelompok besar yakni kelompok defensive dan kelompok offensive. Kelompok defensive bertugas dalam melindungi dan mempertahankan infrastruktur penting milik Ukraina seperti sistem air dan sistem saluran pembangkitan listrik sedangkan kelompok offensive bertugas dalam melakukan perlawanan terhadap serangan siber Rusia melalui pelaksanaan operasi *cyber-espionage*.

Oleh karena itu, untuk melihat peranan IT Army termasuk konfrontasinya terhadap Wizard Spider dalam konflik Rusia-Ukraina utamanya sebagai bentuk serangan balasan, IT Army menjalankan serangan siber yang dikenal sebagai Operasi Prikormka. Dalam operasi ini, IT Army menanamkan sebuah malware ke dalam perangkat lunak. Namun dampak yang

diakibatkan belum sepenuhnya sempurna. Kemudian, masih ditahun yang sama, IT Army kembali melakukan serangan siber dengan dampak kerusakan dan target yang jauh lebih luas yang dikenal sebagai Operasi 9 Mei 2016. Dalam hal tersebut, IT Army memasang 9 peretasan dan keseluruhannya berhasil untuk meretas jaringan siber Rusia. Melalui peretasan tersebut, IT Army berhasil meretas situs propaganda yang anti-Ukraina, menyabotase situs kelompok yang diduga sebagai kelompok separatisme Republik Rakyat Donetsk serta mengacak jaringan penting perusahaan militer swasta milik Rusia.

Serangan siber berikutnya yakni pada Juni 2016 yang dikenal sebagai Operasi Peretasan Saluran Satu. Melalui operasi peretasan tersebut, IT Army berhasil mempropaganda saluran satu milik Rusia melalui Aliansi peretasan yang dibentuk di Ukraina yang terdiri atas Falcon Flame, Rukh dan Trinity. Selanjutnya pada Oktober 2016, IT Army membocorkan Surkov yang merupakan dokumen rahasia milik Rusia. Dalam peretasan tersebut tercatat sebanyak 2.337 email beserta ratusan lampiran mengalami kebocoran ke public, khususnya lampiran dokumen yang berisikan rencana dan strategi Rusia untuk menginvasi wilayah Krimea. Akibatnya yang ditimbulkan juga cukup luas yakni mampu memicu kerusuhan separatis yang besar di wilayah Donbas.

Meski kebanyakan serangan yang dilakukan pada tahun 2016. Akan tetapi hal tersebut mampu memicu berbagai kerusakan fatal bagi Rusia hingga pada akhirnya serangan siber Rusia pada tahun 2017 melalui penanaman malware NotPetya mulai menyerang dan melumpuhkan *cyber security* Ukraina hingga tahun 2022. Akan tetapi, Hal tersebut tidak menutup kemungkinan bagi IT Army untuk bangkit dan melakukan serangan balik. Faktanya, pada Januari 2022, IT Army bahkan berhasil melakukan serangan siber terhadap *cyberspace* Rusia. Dalam konflik Rusia-Ukraina ini, IT Army berhasil melakukan peretasan dan mengganggu proses operasi sistem keamanan di stasiun kereta api Belarusia yang merupakan salah satu jalur alternatif bagi pasukan keamanan Rusia. Dengan meretas operasi sistem keamanan stasiun tersebut, IT Army berhasil memperlambat bahkan menghentikan sementara pergerakan pasukan keamanan Rusia ke perbatasan Ukraina melalui Republik Belarusia.

4. KESIMPULAN

Konflik Rusia – Ukraina dalam tatanan dunia internasional pada dekade terakhir ini tidak terlepas terhadap bentuk peperangan secara kemiliteran. Akan tetapi, esensial keamanan dalam konflik tersebut juga turut mengalami perubahan dan menciptakan bagian eskalasi konflik tersendiri dalam konflik Rusia - Ukraina. Konflik yang pada umumnya menitikberatkan sistem keamanan pada penggunaan aspek kemiliteran kemudian beralih kepada penggunaan sistem *cyber security* dengan menggunakan *cyberspace* sebagai kawasan

perang modern yang dikenal sebagai *cyber-war* sehingga meskipun tidak melakukan konfrontasi secara langsung, Rusia – Ukraina sudah mampu menciptakan ancaman dan serangan satu sama lainnya.

Dalam konflik *cyber-war*, baik Rusia maupun Ukraina membentuk organisasi yang secara khusus berperan dalam melindungi dan meningkatkan *cyber security* yang dimilikinya yakni Wizard Spider oleh Rusia dan IT Army oleh Ukraina yang kemudian menjadi aktor yang berperan strategis dalam menentukan arah konflik *cyber-war*. Wizard Spider yang beranggotakan kelompok militer intelijen menargetkan serangan siber secara luas ke berbagai negara dengan tujuan mengancam kedaulatan dan keamanan melalui penggunaan malware sedangkan IT Army yang dibentuk melalui keanggotaan yang bersifat sukarelawan lebih memfokuskan pada perlindungan siber Ukraina dan penyerangan siber terhadap Rusia sehingga dalam konflik ini, Wizard Spider dan IT Army akan menjadi aktor yang berperan strategis dalam menentukan arah konflik *cyber-war* yang terjadi antara Rusia – Ukraina.

REFERENSI

Burt, J. (2022, Mei 18). *Meet Wizard Spider, the multimillion-dollar gang behind Conti, Ryuk malware*. Theregister, url : https://www-theregister-com.translate.goog/2022/05/18/wizard-spider-ransomware-conti/?_x_tr_sl=en&_x_tr_tl=id&_x_tr_hl=id&_x_tr_pto=sc

CISA.G. (2022, Mei 9). *Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*. CISA.gov url : https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a

Collins, Alan. (2015). *Contemporary Security Studies*. Third Editions, United Kingdom: Oxford University Press

Gachua, A. dan Zedelashvili, T. (2020). Cyber Threats and Asymmetric Military Challenges in the Context of Nuclear Security: Ukrainian and International Cases Analysis. *Ukrainian Policymaker*, 7(1), 20-27. doi:10.29202/up/7/3

Juutilainen, J. (2022). *Cyber Warfare: A Part of the Russo-Ukrainian War in 2022*. (Master's thesis, University of Applied Sciences, Technology, Information and Communications) Julkaisun pysyvä osoite on https://urn.fi/URN:NBN:fi:amk-2022092620438

Mohee, A. (2022, 20 February). Cyber war: The hidden side of the Russian-Ukrainian crisis.https://www.researchgate.net/publication/358736710_Cyber_war_the_hidden_side_of_the_Russian-Ukrainian_crisis

O'Connell, Mary Ellen. (2012). Cyber Security Without Cyber War. *Journal of Conflict & Security*

Law, 17(2),187–209. doi:10.1093/jcsl/krs017

Priyono, U. (2022). Cyber Warfare as Part of Russia and Ukraine Conflict. *Jurnal Diplomasi Pertahanan*, 8(2), 44-59. E-ISSN 2746-8496

Ramadhan, I. (2022). Strategi Keamanan Cyber Security di Kawasan Asia Tenggara: Self-Help atau Multilateralism. *Jurnal Asia Pacific Studies*, 3(2), 181-192. doi: http://dx.doi.org/10.33541/japs.v3i1.1081

Roy. (2022, March 3). *Bukan Dunia Nyata, Perang Rusia-Ukraina Ngeri di Dunia Maya" CNBC Indonesia*, url: https://www.cnbcindonesia.com/tech/20220303100401-37-319748/bukan-dunia-nyata-perang-rusia-ukraina-ngeri-di-dunia-maya

Salt, A.dan May, S.2021). Russian Cyber-Operations in Ukraine and the Implications for NATO. *Canadian Global Affairs Institute*. 1-5. ISBN: 978-1-77397-208-4

Sanjaya, B.N, et.al. (2022). Pengembangan Cyber Security dalam Menghadapi Cyber Warfare di Indonesia. *Journal of Advanced Research in Defense and Security Studies*, 1(1), 19-34. doi: https://ejournal.hakhara-institute.org/index.php/JARDS

Simons, G.et.al. (2020). Hybrid War and Cyber-attacks: Creating Legal and Operational Dilemmas.", *Global Change, Peace & Security*. 1-6. doi: https://doi.org/10.1080/14781158.2020.1732899

Soesanto, S.(2022). The IT Army of Ukraine: Structure, Tasking, and Eco-System.", *Center for Security Studies (CSS), ETH Zürich*, Juni 2022. doi: https://doi.org/10.3929/ethz-b-000552293

Suharto, M.A. & Apriyani. M.N. (2021). Konsep Cyber Attack, Cyber Crime, dan Cyber Warfare Dalam Aspek Hukum Internasional. *Risalah Hukum*, 17(2), 98-107

Supruniuk, I. (2022). *ETH Zürich CSS report: "The IT Army of Ukraine: Structure, Tasking, and Ecosystem*" Techukraine.org, url : https://techukraine.org/2022/06/28/eth-zurich-css-report-the-it-army-of-ukraine-structure-tasking-and-ecosystem/

Willet, M. (2022). The Cyber Dimension of the Russia–Ukraine War.", *Survival: Global Politics and Strategy*, 64(5), 7-26. doi: https://doi.org/10.1080/00396338.2022.2126193