PEMAKSIMALAN KEKUATAN MILITER RUSIA MELALUI SERANGAN SIBER DALAM KRISIS UKRAINA TAHUN 2014

Said M. Rezza Vahlefy

FISIP Universitas Riau, Kampus Bina Widya Km. 12,5 Simpang Baru Panam, Pekanbaru 28293

Abstract: In 2014, Russia involves a cyber in Ukraineian crisis as an effort to maximize its military power. The involvement of cyber attacks in the maximization of military power is related to military and technological factors, both Russia and Ukraine. This study aims to get an overview and explanation of why Russia uses cyber attacks in the Ukraine crisis of 2014 while its military strength is far superior and the availability of other potentials. To analyze it, researchers use the perspective of offensive realism, the theory of great power with the concept of "power", "cyber power" and "cyber warfare" to manage conflict in a transformative way.

Abstrak: Pada tahun 2014, Rusia melibatkan siber dalam krisis Ukraina sebagai upaya memaksimalkan kekuatan militer. Pelibatan serangan siber dalam pemaksimalan kekuatan militer ini berkaitan dengan faktor militer dan faktor teknologi, baik Rusia maupun Ukraina. Penelitian ini bertujuan untuk mendapatkan gambaran dan penjelasan mengapa Rusia menggunakan serangan siber dalam krisis Ukraina tahun 2014 sementara kekuatan militernya sudah jauh lebih unggul dan ketersediaan potensi lain. Untuk menganalisisnya, peneliti menggunakan perspektif realisme ofensif, teori great power dengan konsep "power", "cyber power" dan "cyber warfare" untuk mengelola konflik secara transformatif.

Kata Kunci: serangan siber, *great power*, pemaksimalan kekuatan, realisme ofensif

PENDAHULUAN

Hubungan antara Rusia dan Ukraina pra krisis Ukraina mengalami tren kedekatan yang dinamis. Diantara semua negara-negara yang berbatasan dengan Ukraina, Rusia merupakan negara yang memiliki posisi dominan karena nilai strategis dan situasi geopolitik serta geoekonomi Ukraina[1]. Namun hubungan kedua negara mengalami penurunan yang disebabkan oleh beberapa isu, seperti isu batas wilayah, politik identitas, perdagangan dan ekonomi, serta interdependensi energi, bahkan potensi militer Ukraina yang mencemaskan Rusia dalam upaya perimbangannya. Hal tersebut tidak terlepas dari kebijakan luar negeri Rusia yang tersusun dari beberapa isu kunci yaitu untuk menjaga Kiev dalam pengaruh Rusia dan menggabungkan Ukraina ke dalam kawasan Rusia atau minimal beberapa bagian Ukraina[2].

Kepentingan luar negeri Rusia terhadap Ukraina cenderung berakhir konflik. Konflik terbaru yang terjadi adalah krisis Ukraina tahun 2014. Krisis Ukraina dimulai dengan kompetisi antara Uni Eropa dan Rusia untuk orientasi geoekonomi masa depan Ukraina[3]. Hubungan Rusia dan Ukraina ditandai dengan perselisihan, termasuk revolusi Oranye selama pemilihan presiden Ukraina tahun 2004 dan juga terkait persediaan gas alam. Ukraina mulai mendekati Uni Eropa dengan perjanjian kerjasama, namun berbelok ke Rusia pada akhirnya. Keputusan ini menimbulkan protes *Euromaidan*[4] dan memprovokasi Presiden Ukraina Yanukovich me-

[1] Tadesuz Andrzej Olszanski, "Ukraine and Russia: Mutual relations and the Conditions that Determine Them". _____. *CES Studies*. Tersedia di: <http://pdc.ceu.hu/archive/00002222/01/uk_ru_mutual_rel.pdf> [Internet] (diakses pada tanggal 16 April 2018 WIB)

[2] Robert Nalbandov, "Not by Bread Alone: Russian Foreign Policy under Putin" (Nebraska: University of Nebraska Press, 2016), halaman 214.

[3] Dmitri Trenin, "The Ukraine Crisis and the Resumption of Great-Power Rivalry", (Moskwa: Carnegie Moscow Center, 2015), halaman 4

[4] *Euromaidan* ialah gelombang demonstrasi dan revolusi di Ukraina. Pada awalnya, krisis politik dan pergolakan sosial di Ukraina yang menyebabkan terjadinya protes di Maidan Nezalezhnosti atau Lapangan Kemerdekaan di pusat kota Kyev untuk bergabung dengan Eropa – atau dikenal *Euromaidan*, sebuah istilah yang muncul merujuk pada simpati para demonstran. Diuk, Nadia. Fokus: "Euromaidan: Ukraine's Self-Organizing Revolution". *World Affairs*. 2014. Tersedia di:<http://www.worldaffairsjournal.org/article/euromaidan-ukraine%E2%80%99s-self-organizing-revolution> [Internet] (diakses pada tanggal 14 Desember 2017 pukul 16.24 WIB).

larikan diri ke Rusia. Hal ini disebabkan penolakan Yanukovich terhadap perjanjian kerjasama atau asosiasi Ukraina dengan Uni Eropa. Bersamaan dengan ini, situs internet in-stitusi Ukraina terkena serangan DDoS[5]. Setelah peristiwa tersebut, perang siber semakin ikut berperan dalam krisis Ukraina meskipun invasi militer juga dilakukan. Serangan siber yang dilakukan Rusia dimulai pada tahun 2013 namun mengalami puncak pada tahun 2014.

Munculnya serangan siber dalam krisis Ukraina tersebut ikut mendukung pemaksimalan upaya militer Rusia. Perang siber merupakan *domain* (wilayah) baru dalam kajian hubungan internasional di era informasi ini. Perang siber merupakan istilah umum yang mendefinisikan serangan siber akibat dari tindakan saling balas antarnegara atau kelompok terorganisir sebagai respon terhadap situasi konflik[6]. Adapun target serangan siber ialah menyerang keamanan publik dengan manipulasi sistem informasi, sistem pertahanan nasional, sistem elektronik pemerintah, manipulasi informasi atau *cyberpropaganda*, dan dalam kejahatan keuangan[7].

Sejak awal 1990-an, para analis telah memprediksikan bahwa serangan siber di abad XXI akan menjadi wadah peperangan yang sangat menonjol[8]. Perang siber akan memiliki dampak pada dunia kinetik. Maksudnya ialah perang siber akan menyebabkan kerusakan baik langsung maupun tidak terhadap infrastruktur fisik. Perang di era informasi ini bersifat steril atau tanpa menghasilkan korban jiwa yang dihadapkan pada infrastruktur digital dan kapabilitas fisik yang diintegrasikan untuk memungkinkan terjadinya perang modern[9]. Menurut para pakar strategi militer, saat ini arena siber menjadi arena pertempuran baru. Meskipun perang siber masih dalam fase pertumbuhan, generasi baru dari pasukan dan persenjataan siber akan membentuk kembali bagaimana berlangsungnya perang di abad XXI[10]. Banyak negara di dunia ini secara aktif telah membentuk dan mengembangkan divisi perang siber dalam angkatan bersenjata tradisional mereka[11].

Dominasi serangan siber selama krisis Ukraina dilakukan oleh Rusia meskipun mendapat perlawanan dari Ukraina pada tahun-tahun setelahnya. Rusia mengembangkan operasi siber untuk tujuan atau berfungsi sebagai pengali atau *multiplier* kekuatan dari komponen angkatan bersenjata yang lebih tradisional dan kinetis[12]. Dalam panggung internasional, Rusia adalah negara *heavyweight* atau kelas berat dalam kemajuan kapabilitas siber. Rusia tidak semaju Amerika Serikat secara teknologi, namun dalam kapabilitas siber, Rusia merupakan kekuatan yang diperhitungkan. Adapun diantara beberapa negara dengan kapabilitas siber terbesar (AS, Cina, Iran, Korea Selatan dan Utara, Britania Raya, Jerman dan Israel), Rusia merupakan negara dengan kapabilitas siber yang paling berbahaya.[13] Rusia pernah terlibat perang siber dengan negara-negara kawasan Eropa Timur lainnya yaitu Estonia (2007) dan Georgia (2008). Sumber lain juga menyebutkan beberapa negara kawasan ex-Soviet lainnya seperti Lithuania (2008) dan Kyrgyzstan (2009)[14]. Hal ini menunjukkan telah terjadi pergeseran kekuatan

[5] Serangan DdoS atau A Distributed Denial of Service adalah upaya menghilangkan pelayanan *online* yang membanjirinya dengan jaringan yang sibuk dari sumber beragam. Pelaku menargetkan sumber-sumber penting, dari situs bank hingga berita. Digital Attack Map. Fokus: "What is a DdoS Attack?". *Digital Attack Map.* 2013. Tersedia di: <http://www.digitalattackmap.com/understanding-ddos/> [Internet] (diakses pada 25 Juni 2017, pukul 20:16 WIB)

[6] Solange Ghernaouti. "Cyber Power, Crime, Conflict and Security in Cyberspace" (Lausanne: EPFL Press. 2013), halaman 146.

[7] *Ibid.*, halaman 144.

[8] Derek Reveron (Ed.). "Cyber Challenges and National Security: Threats, Opportunities, and Power in a Virtual World" (Washington DC: Georgetown University Press. 2012), halaman 3.

[9] Andrew Colarik dan Lech Janczewski, "Establishing Cyber Warfare Doctrine", *Journal of Strategic Security*, Vol. 5 No. 1 (Musim Semi, 2012) halaman 39.

[10] Rex Hughes, "A Treaty for Cyberspace", *International Affairs (Royal Institute of Internatonal Affairs 1944-)*, Vol. 86 No. 2 (Maret 2010), halaman 523.

[11] Philip Pool, "War of the Cyber World: The Law of Cyber Warfare", *The International Lawyer.* Vol. 47 No. 2 (Musim Gugur 2013), halaman 203

[12] *Op. Cit*., Philip Pool, halaman 203

[13] Ryan Maness dan Brandon Valeriano, "Russia's Coercive Diplomacy: Energy, Cyber and Maritime Policy as New Sources of Power" (New York: Palgrave Macmillan, 2015) halaman 92.

[14] William C. Ashmore, "Impact of Alleged Russian Cyber Attacks", (Kansas: School of Advance Military Studies US Army Command and General Staff College Fort Leavenworth, 2009), halaman 13

Rusia dari kekuatan tradisional (militer) menjadi integrasi militer dan siber.

Pemaksimalan kekuatan siber ini tidak lepas dari sosok pemimpin Rusia, Vladimir Putin. Banyak para ahli pertahanan Rusia kontemporer menyatakan bahwa Uni Soviet tidak memiliki kapabilitas siber yang mumpuni pada tahun 1980an. Oleh karena itu, hal ini menjadi faktor keruntuhannya. Administrasi Putin tidak ingin melakukan kesalahan yang sama. Ia memberikan FSB atau Badan Intelijen Federal Rusia dana untuk memonitor internet di Rusia dan membiarkannya untuk mengembangkan kapabilitas ofensif atau serangan[15]. Selain itu, Rusia juga memiliki sejumlah peretas yang dikenal dengan *hacktivis*. Secara politis, mereka aktif dan secara teknologi mereka merupakan individu-individu yang cerdas dengan tingkat patriotisme yang besar dan loyal pada Rusia[16].

Integrasi antara militer dan siber Rusia tidak kali ini terjadi. Pada tahun 2008, Rusia menggunakan operasi siber untuk mendukung invasi militer di Georgia. Pada 2014, Rusia menggunakan upaya yang sama terhadap Ukraina. Vladimir Putin mengatakan bahwa *Rusia bisa saja menduduki Kiev (Ibukota Ukraina) serta ibukota negara-negara Baltik dalam dua hari dengan kekuatan militernya*[17]. Namun praktiknya, Rusia melibatkan serangan siber dalam konflik tersebut dan tanpa memanfaatkan kemampuan kolektif militer yang, secara kuantitas, lebih unggul dari Ukraina.

Penelitian ini bertujuan untuk mendapatkan gambaran dan penjelasan mengapa Rusia menggunakan serangan siber dalam krisis Ukraina tahun 2014 sementara kekuatan militernya sudah jauh lebih unggul dan ketersediaan potensi lain.

METODE

Berdasarkan penjelasan permasalahan penelitian dan kerangka pemikiran, maka untuk mengetahui keadaan sebenarnya secara rinci dan aktual mengenai permasalahan penelitian ini dengan melihat masalah dan tujuan penelitian seperti yang telah disampaikan sebelumnya, maka pendekatan yang digunakan dalam penelitian ini adalah pendekatan historis. Pendekatan historis (sejarah) cenderung menganalisis perkembangan yang ada dengan pola *ex pose facto (after the fact)*. Artinya, penelitian yang dilakukan setelah suatu kejadian itu terjadi.[18]

Model analisis yang digunakan dalam penelitian ini lebih mengarah pada penggunaan model penelitian kualitatif-deskriptif. Model penelitian kualitatif adalah strategi penelitian yang menekankan kedekatan dengan data, partisipasi dan pengalaman.[19] Penelitian ini menekankan pengumpulan fakta dan identifikasi data. Komponen metode dalam penelitian ini adalah mendeskripsi, menganalisa, dan menafsirkan temuan dalam istilah yang jelas dan tepat.[20]

HASIL DAN PEMBAHASAN

Krisis di Ukraina didasarkan pada kebangkitan nasionalisme terhadap Rusia. Hal ini dikarenakan aktor-aktor yang menjadi penyebab dan terlibat merupakan aktor yang pro-Rusia. Melalui fenomena tersebut, Ukraina dilanda oleh kabut nasionalisme Rusia yang berkembang di negaranya sehingga isu-isu separatisme atau pemisahan diri menjadi isu yang sangat sensitif. Hal ini tentu saja tidak terlepas dari intervensi Rusia yang membantu kelompok-kelompok tersebut dan memberi dukungan atas aksi yang terjadi. Berdasarkan faktanya, tidak hanya invasi militer yang terlibat dalam konflik tersebut. Kekuatan tidak tampak namun memiliki pengaruh yang besar ialah pelibatan perang siber[21] antara Rusia dan Ukraina.

---

[15] *Ibid*., halaman 90

[16] *Ibid*.

[17] Huggler, Putin Privately Threatened to Invade Poland, Romania and the Baltic States, *Daily Telegraph, 19*. 18 September, 2014. Dikutip dari: http://www.telegraph.co.uk/news/worldnews/europe/russia/11106195/Putin-privately-threatened-to-invade-Poland-Romania-and-the-Baltic-states.html (Diakses pada tanggal 2 Februari 2018, pukul 14.00 WIB)

[18] Arif Furchan. *Pengantar Penelitian dalam Pendidikan*. Pustaka Pelajar, Yogyakarta, 2004, hal. 383.

[19] Bruce A. Chadwick, Howard M. Bahr, & Stan L. Albrecht. *Metode Penelitian Ilmu Pengetahuan Sosial*. Edisi Terjemahan. Diterjemahkan oleh Sulistia, Yan Mujianto, Ahmad Sofwan dan Suhardjito, Prentice Hall International Inc., New Jersey, 2007, hal. 488.

[20] Lexy Moleong. *Metode Penelitian Kualitatif*. Remaja Rosdakarya, Bandung, 2000, hal. 112.

[21] Pelibatan kekuatan lain (non-militer) dan militer di bawah satu komando terpusat dan diarahkan untuk tujuan politik yang sama disebut juga Konflik *Full-Spectrum.* Konsep

Rusia sebagai negara *Great Power* di kawasan Eropa Timur memiliki keunggulan terutama *power* yang diwakilkan dengan kekuatan militer. Bila dibandingkan dengan negara-negara di sekitarnya, Rusia memiliki kapabilitas militer yang lebih mumpuni dan ditakuti secara kolektif. Sebagai negara *Great Power,* ketidakpuasan akan kemampuan sendiri menjadi sesuatu yang pasti terjadi mengingat negara-negara di sekitarnya melakukan perimbangan, baik dengan improvisasi kekuatan domestik serta ikut dalam aliansi-aliansi guna tujuan keamanan dan perlindungan dari negara agresor yang mengancam kedaulatannya.

Hubungan antara Rusia dan Ukraina sejak runtuhnya Uni Soviet mengalami kemerosotan namun tetap interdependensi. Isu-isu mengenai perbatasan, kaum minoritas Rusia di Ukraina, energi dan perdagangan menjadi faktor yang ikut mewarnai konflik antara kedua belah pihak terutama dalam krisis Ukraina tahun 2014. Krisis Ukraina diwarnai dengan upaya militerisasi Rusia untuk menganeksasi wilayah Ukraina Timur dan Krimea yang terkait dengan isu politik identitas. Beberapa warga Rusia ingin bersatu dengan Rusia dan menolak asosiasi dengan Barat karena dikhawatirkan tidak adanya keberpihakan kepada mereka.

Krisis Ukraina diwarnai dengan perpecahan oleh kaum separatis Rusia di Ukraina yang dibantu oleh militer Rusia. Upaya militerisasi tersebut melibatkan perang tak kasat mata namun memiliki dampak yang signifikan yaitu perang siber. Perang siber dalam krisis ini berlangsung selama empat tahun selama krisis Ukraina (2014). Pada tahun 2014, terjadi serangan siber besar-besaran oleh Rusia terhadap Ukraina yang menargetkan infrastruktur publik dan semakin melemahkan Ukraina sehingga aneksasi berhasil dilakukan di kedua kawasan tersebut. Serangan searah dari Rusia mendapatkan perlawanan dari para peretas Ukraina yang menyebabkan perang siber.

Dalam perspektif realisme ofensif oleh Mearsheimer, negara *Great Power* terus berjuang untuk memaksimalkan kekuatannya. Rusia sebagai *Great Power* memaksimalkan kekuatan, secara strategis, melihat krisis Ukraina sebagai arena dan momentum yang tepat untuk melancarkan serangan siber. Momen siber yang tepat ini merupakan upaya taktis dan strategis oleh Rusia karena sektor siber memiliki perkembangan yang pesat serta potensi dan celah Ukraina yang belum mengembangkan sektor ini di negaranya. Pemaksimalan kekuatan Rusia di ranah siber tidak terlepas dari sosok Vladimir Putin sebagai Presiden Rusia terutama di masa kepresidenan ketiga yang membangun sektor siber dan didukung oleh sumber daya manusia yang mumpuni di bidang tersebut.

Asumsi perspektif realisme ofensif mensyaratkan bahwa negara *Great Power* memiliki sifat selalu ofensif dengan kekuatan militernya. Secara kuantitas, kemampuan militer Rusia lebih unggul dibandingkan Ukraina. Namun dari segi taktis dan potensi, Ukraina lebih unggul karena aliansinya dengan NATO serta potensi tersembunyi berkaitan dengan persediaan persenjataan yang diwarisi di era Uni Soviet. Menurut perspektif ini, potensi ofensif negara *Great Power* tidak bisa dibendung. Dengan kata lain, meskipun Rusia tidak mampu secara kolektif mengerahkan kapabilitas militernya, kapabilitas sektor siber yang baik bisa digunakan sebagai upaya memaksimalkan kekuatan dan berintegrasi dengan militer dalam krisis Ukraina selama tahun 2014. Berdasarkan asumsi tersebut, Mearsheimer menyimpulkan bahwa negara *Great Power* mengalami kekhawatiran karena Rusia berpegang pada kekuatan sendiri dan bertumpu pada strategi terbaik untuk tetap bertahan atau *survive* dalam merebut status hegemon regional khususnya kawasan Eropa Timur.

Pemaksimalan kekuatan melalui sektor siber oleh Rusia menjadi tepat dikarenakan beberapa hal berikut. Pertama, sejak runtuhnya Uni

perang Rusia telah berada pada generasi keenam. Menurut Slipchenko, perang generasi keempat melibatkan persenjataan otomatis, tank dan pertempuran udara; kelima melibatkan senjata Nuklir; dan keenam melibatkan persenjataan yang lebih presisi yaitu perang elektronik dan informasi atau siber tanpa adanya kontak. Tujuannya ialah (a) mengalahkan secara total angkatan bersenjata musuh; (b) menghancurkan potensi ekonomi musuh dan menggulingkan dan mengganti sistem politik musuh. Dikutip dari: Oscar Jonsson dan Robert Seely, "Russian Full-Spectrum Conflict: An Appraisal after Ukraine", The Journal of Slavic Military Studies, Vol. 28 No. 1 (2015), halaman 3.

Soviet literasi masyarakat dan pemerintah Rusia terhadap sektor siber meningkat. Peningkatan ini sejalan dengan arah kebijakan luar negeri dan doktrin militer yang diterapkan di masa kepresidenan ketiga Vladimir Putin. Pemaksimalan kekuatan terjadi dalam pemerintahan (FSB) dan sipil (Hacktivis). Hal ini bertepatan dengan menurunnya kemampuan militer Rusia sehingga dilakukan reformasi militer pasca konflik 2008 di Georgia. Hal ini sejalan dengan doktrin militer Rusia yang dirancang setelahnya.

Kedua, dalam upaya strategi menghadapi perimbangan militer Ukraina, kapabilitas siber dapat digunakan karena literasi Ukraina dalam sektor tersebut belum terlihat. Namun setelah terjadinya serangan siber besar-besaran oleh Rusia terutama tahun 2014, Ukraina memiliki dua dasar hukum pertahanan dan keamanan siber dalam bentuk Strategi Keamanan Nasional dan Strategi Keamanan Siber Ukraina tahun 2015 dan 2016 serta dukungan NATO menyebabkan perang atau aksi saling serang antara Rusia dan Ukraina dengan ketegangan yang lebih rendah.

Ketiga, terjadinya perang siber secara tidak langsung menyelamatkan asset Rusia yang ada di Ukraina. Aset tersebut berupa jalur pipa dan para *Russophone* yang ada di Ukraina. Dampak perang siber tidak menyebabkan kelumpuhan total pada infrastruktur seperti perang konvensional. Dampak perang siber pada Ukraina bersifat melemahkan kekuatan pemerintah untuk melawan invasi militer Rusia ke wilayah Donbass dan Krimea. Pemaksimalan Rusia akan siber tidak berhenti pada ranah alat teknologi dan informasi. Peningkatan kemampuan siber dilakukan dengan mematikan aliran listrik Ukraina sehingga, dalam beberapa jam, Ukraina mengalami pelemahan dalam suasana pemerolehan kekuatan baru dalam sektor siber. Dalam perspektif realisme ofensif, Rusia tepat dikatakan sebagai *Great Power* karena tidak berhenti melakukan pemaksimalan kekuatan demi mencapai tujuan menjadi hegemon kawasan Eropa Timur.

Krisis Ukraina tahun 2014 menjadi kemunculan dan lahirnya bentuk perang jenis baru di era digital saat ini. Kemunculan perang siber adalah respon terhadap situasi konflik terutama dalam krisis di Ukraina. Seperti operasi militer, fenomena perang siber tidak dapat dielakkan sehingga terus berlangsung dan meningkat. Dari tiga tahun terjadinya upaya saling balas antara Rusia dan Ukraina di arena siber, maka tahun 2014 merupakan puncak terjadinya perang siber yang didominasi oleh Rusia. Hal ini berkaitan langsung dengan tiga peristiwa yang meliputinya yaitu *Euromaidan*, aneksasi Krimea dan konflik Donbass yang melibatkan juga operasi militer dan pemberontakan kelompok separatis pro-Rusia.

Selama tahun 2014, serangan siber Rusia tidak hanya menyertai konflik, namun dalam kehidupan tata negara Ukraina. Serangan tersebut mulai dari penyerangan/penyadapan telepon seluler anggota parlemen dan mempengaruhi pemilihan presiden Ukraina. **U**paya tersebut dilakukan peretas Rusia agar Ukraina tetap dalam koridor Rusia atau menganut hukum dan mencari pemimpin yang tetap pro-Rusia, seperti Viktor Yanukovich. Alhasil, dengan terpilihnya Poroshenko sebagai presiden Ukraina, upaya separatis pro-Rusia dan para peretas terhenti.

Berdasarkan penjelasan di atas, hal ini memperlihatkan dominasi Rusia dalam melakukan serangan siber tanpa adanya perlawanan dari Ukraina. Rusia terus melancarkan upaya serangan siber dalam upaya-upaya aneksasi terhadap Krimea dan Donbass. Hal ini menunjukkan bahwa Rusia sebagai *Great Power* dalam perspektif realisme ofensif akan terus memaksimalkan kekuatannya demi tercapainya tujuan menjadi negara hegemon di kawasan.

SIMPULAN

Pelibatan serangan siber Rusia terhadap Ukraina dilakukan karena pertimbangan akan potensi militer Ukraina. Pertimbangan lain juga diperhitungkan Rusia yaitu kedekatan geografis antara Ukraina dengan negara-negara anggota NATO. Keseluruhan kekuatan militer Rusia tidak dapat digunakan dalam krisis Ukraina karena Rusia perlu menempatkannya dalam posisi defensif. Selain itu, kekuatan militer NATO jauh lebih unggul ketimbang Rusia. Kemunduran ini dirasakan oleh Rusia pasca invasi Abkhazia dan Osetia Selatan di Georgia tahun 2008 meskipun mengalami kemenangan. Untuk memperbaiki kapabilitas militer, Rusia melakukan reformasi

militer dengan memasukkan unsur teknologi dalam milterisasi. Selain itu, penguatan dari dalam dilakukan oleh Rusia dalam bentuk doktrin militer tahun 2010 sebelum terjadinya krisis Ukraina. Doktrin ini berbentuk dekrit presiden yang berisi tentang penguatan kekuatan militer Rusia dan integrasinya dengan sektor teknologi (informasi-siber).

Penurunan kemampuan militer Rusia ternyata tidak berbanding lurus dengan perkembangan dan kemampuan teknologi dan informasi di Rusia. Kondisi ini menyebabkan Rusia memanfaatkan kemampuan tersebut untuk tetap menginterasikan kemampuan militer dengan kekuatan siber yang dilancarkan oleh tiga aktor siber yaitu Institusi Negara (FSS), dan sipil (hacktivis). Hal tersebut diejawantahkan ke dalam doktrin militer Rusia sebagai koridor pelaksanaan operasi militer Rusia dan invasi ke negara-negara sasarannya. Rusia tidak bisa mengerahkan kemampuan militer secara kolektif untuk menaklukkan Ukraina. Hal ini dikarenakan potensi dan perimbangan militer Ukraina yang dapat diperhitungkan Rusia. Namun demikian, Rusia melihat bahwa faktor siber masih lemah dalam sektor keamanan Ukraina terutama pada tahun 2014. Dengan kesiapan Rusia dalam ranah siber, Ukraina menjadi sasaran yang mudah dimasuki dan dirusak sehingga serangan siber secara besar-besaran terjadi yang tidak hanya diderita oleh masyarakat sipil, tapi juga pemerintah. Alhasil pada tahun 2015, Ukraina memiliki strategi keamanan nasional dan tahun 2016, strategi keamanan siber serta diikuti dengan dukungan NATO terutama dibidang pertahanan siber. Dekrit presiden tersebut kemudian mengintegrasikan siber Ukraina dengan pemerintah seperti yang lebih dulu dilakukan oleh Rusia yang semula hanya dilakukan oleh para peretas Ukraina.

DAFTAR RUJUKAN

Ashmore, William. 2009. *Impact of Alleged Russian Cyber Attacks*. Kansas: School of Advance Military Studies US Army Command and General Staff College Fort Leavenworth.

Chadwick, Bruce, dkk. 2007. *Metode Penelitian Ilmu Pengetahuan Sosial*. Diterjemahkan oleh Sulistia, Yan Mujianto, Ahmad Sofwan dan Suhardjito, Prentice Hall International Inc., New Jersey.

Colarik, Andrew dan Lech Janczewski, "Establishing Cyber Warfare Doctrine", *Journal of Strategic Security*, Vol. 5 No. 1 (Musim Semi, 2012).

Furchan, Arif. 2004. *Pengantar Penelitian dalam Pendidikan*. Pustaka Pelajar, Yogyakarta.

Ghernaouti, Solange. 2013. *Cyber Power, Crime, Conflict and Security in Cyberspace*. Lausanne: EPFL Press.

Hughes, Rex. "A Treaty for Cyberspace", *International Affairs (Royal Institute of Internatonal Affairs 1944-)*, Vol. 86 No. 2 Maret 2010.

Jonsson, Oscar dan Robert Seely, "Russian Full-Spectrum Conflict: An Appraisal after Ukraine", The Journal of Slavic Military Studies, Vol. 28 No. 1 2015.

Maness, Ryan dan Brandon Valeriano. 2015. *Russia's Coercive Diplomacy: Energy, Cyber and Maritime Policy as New Sources of Power*. New York: Palgrave Macmillan.

Moleong, Lexy. 2000. *Metode Penelitian Kualitatif*. Remaja Rosdakarya, Bandung.

Nalbandov, Robert. 2016. *Not by Bread Alone: Russian Foreign Policy under Putin*. Nebraska: University of Nebraska Press.

Pool, Philip. "War of the Cyber World: The Law of Cyber Warfare", *The International Lawyer* Vol. 47 No. 2 Musim Gugur 2013.

Presiden Federasi Rusia. *The Military Doctrine of Russian Federation.* A Presidential Edict by Russian Presidential Website on 5th February , 2010

Reveron, Derek. (Ed.). 2012. *Cyber Challenges and National Security: Threats, Opportunities, and Power in a Virtual World*. Washington DC: Georgetown University Press.

Trenin, Dmitri. 2015. *The Ukraine Crisis and the Resumption of Great-Power Rivalry*. Moskwa: Carnegie Moscow Center.