Jurnal Surya Kencana Satu:
Dinamika Masalah Hukum dan Keadilan

ISSN Print: 2085-2339
ISSN Online: 2654-7252

Editorial Office: Fakultas Hukum, Universitas Pamulang,
Jalan Surya Kencana No. 1, Pamulang Barat, Tangerang Selatan 15417, Indonesia.
Phone/ Fax: +6221-7412566
E-mail: dinamikahukum_fh@unpam.ac.id
Website: http://openjournal.unpam.ac.id/index.php/sks

Penolakan *European Convention On Cybercrime* Oleh Rusia Dalam Mempertahankan Kepentingan Nasional

Muhammad Granit Ady Wirasisya[a] Tulus Warsito[b]

[a] *Fakultas Hukum Universitas Muhammadiyah Yogyakarta.* E-mail: granit.wirasisya@gmail.com
[b] *Fakultas Hukum Universitas Muhammadiyah Yogyakarta*

Article

Received: Nov 26, 2020;
Reviewed: Dec 01, 2020;
Accepted: Dec 15, 2020;
Published: Mar 31, 2021

Abstract

Cepatnya perkembangan teknologi dan komunikasi memunculkan sebuah dunia baru, yaitu dunia *cyber* atau *cyberspace*. Hal ini memiliki dampak kepada pembuatan kebijakan negara. Cepatnya perkembangan teknologi dan informasi tidak dapat diikuti oleh negara-negara menyebabkan diperlukannya kerjasama antar negara untuk memperkokoh dan mengharmonisasikan kebijakan didalam dunia *cyber*. Kejahatan yang terjadi didalam dunia *cyber* termasuk kedalam kejahatan internasional karena tempat pelaku melakukan kejahatan tidak sama dengan target yang dituju. Penelitian ini dilakukan untuk melihat bagaimana kebijakan Rusia didalam menangani ancaman dunia *cyber* dan menolak menandatangani *European Convention on Cybercrime.* Rusia memiliki perbedaan pendapat terhadap dunia *cyber* dimana Rusia melihat dunia ini adalah sebuah ancaman negara. Rusia tidak mengikuti penandatanganan *Convention on Cybercrime* yang membuat Rusia melakukan kerjasama dengan negara yang memiliki pemikiran yang sama dalam dunia cyber Selain itu Rusia juga ikut didalam *Shanghai Cooperation Organization* dan *Collective Security Treaty Organization* didalam pertahanan Cyber untuk melakukan harmonisasi kebijakan dunia cyber di wilayah regional. Dengan melihat hal ini, Rusia meskipun memiliki pandangan yang berbeda dengan negara lain, memiliki kebijakan *cyber* dalam negeri dan luar negeri yang mumpuni dalam mempertahankan negara dalam ancaman yang berada dari dunia *cyber*.

Kata kunci: kebijakan *cyber*; organisasi regional; kepentingan nasional.

The fast development of technology and communication gave rise to a new world, namely the cyberspace. This has implications for state policy making. The rapid development of technology and information cannot be followed by countries causing the need for cooperation between countries to strengthen and harmonize policies in the cyberspace. Crimes that occur in the cyberspace are included in international crimes because the place where the perpetrator commits the crime is not the same as the target. This research conducted to see how Russian policy in dealing with cyber threats and refuse to sign the European Convention on Cybercrime. Russia has differences of opinion on the cyberspace where Russia sees that world as a threat. Russia did not participate in the signing of the Convention on Cybercrime which

made Russia cooperate with countries that had the same thoughts in the cyberspace. In addition, Russia also participating in the Shanghai Cooperation Organization and Collective Security Treaty Organization in cyber defense to harmonize cyberspace's policies in regional areas. By looking at this, Russia, despite having a different view from other countries, has a domestic and foreign cyber policy that is capable of defending the country under threats from the cyberspace.

Keywords: *cyber policy; regional organization; national interest.*

PENDAHULUAN

Dunia telah masuk kedalam zaman digital dimana semua orang memiliki ketergantungan terhadap internet. Internet sendiri adalah sebuah tepat dimana suatu data dari barang elektronik disimpan, diperbarui, dan dibagikan melewati jaraingan yang tidak dibatasi oleh geografi.

Perkembangan teknologi informasi dan komunikasi yang pesat menyebabkan tatanan kehidupan keseharian masyarakat berubah, mudahnya berkomunikasi dan cepatnya sebuah berita sampai kepada masyarakat membuat teknologi sebelumnya menjadi tidak efisisen. Meskipun kemudahan didalam komunikasi dan cepatnya perkembangan teknologi membantu negara dan masyarakat, muncul tantangan-tantangan didalam bagaimana mengatur wilayah internet, sebuah wilayah yang terbentuk dikarenakan kemajuan teknologi informasi dan komunikasi.

Majunya teknologi informasi dan komunikasi, pelaku kejahatan mengikuti trend didalam melakukan kejahatan, yaitu kejahtan *cyber*, menjadi sebuah isu pemerintah dan negara. Didalam hukum, kasus yang dilakukan oleh pelaku kejahatan *cyber* tidak mudah untuk diselesaikan dikarenakan untuk melacak pelaku sangat susah dan bukti yang diterima dan diberikan kepada penegak hukum sangatlah teknis, yaitu bukti berupa perangkat lunak dan perangkat keras. Rusia sebagai negara dengan penduduk terbesar dengan peringkat kesembilan denganjumlah penduduk 145,953,700 (Worldometer, 2020) berusaha untuk melindungi masyarakat dan negara dari ancaman dunia *cyber*.

Kejadian kejahatan *cyber* di Rusia terjadi karena adanya ekspansi pasar pada kebutuhan jasa *hacker* dikarenakan semakin maju teknologi informasi dan komunikasi dan masyarakat diberbagai tingkatan masyarakat memakai dunia *cyber*. Semakin luasnya ekspansi pasar dan kemampuan pelaku kejahatan *cyber* membuat Rusia kesusahan didalam melawan kejahatan *cyber*. Ini membuat Rusia sebagai salah satu *hotspot* dalam kejahatan *cyber* (Noah, Rayman, 2020)

Di dalam dunia *cyber*, pelaku dari kelompok kejahatan yang terjadi sering melibatkan anggota-anggota yang berbeda negara. Karakteristik ini menjadi salah satu bukti bahwa kejahatan dunia *cyber* termasuk dari kejahatan transnasional. Selain itu kegiatan kelompk yang bersifat global dan tidak menghiraukan batas geografis juga menjadi bukti lain yang menunjukan bahwa kejahatan yang terjadi didunia *cyber* termasuk kejahatan transnasional. (Ionel, Stioca, 2006)

Pemerintah Rusia menanggapi secara serius kejahatan-kejahatan yang terjadi didalam dunia internet dan pemerintah melihat bahwa kebebasan didalam internet dapat membuat para pelaku melakukan kejahatan denga mudah dan dapat menimbulkan ketidakstabilan negara.

Konsep fundamental negara Rusia dalam masalah dunia *cyber* adalah adanya kemampuan pemerintah untuk memiliki sebuah kendali terhadap dunia *cyber*. Hal ini didukung oleh negara Cina, Tajikistan, dan Uzbekistan. (Giles, Keir, 2020) Meski menjadi *hotspot* kejahatan dunia *cyber*, Rusia tidak ikut menandatangani *European Convention on Cybercrime*. Sebuah konvensi pertama dalam menghadapi kejahatan internet dan komputer dengan melakukan harmonisasi hukum negara.

Hal ini menarik dikarenakan meskipun Rusia tidak ikut menandatangani *European Convention on Cybercrime*, Rusia memiliki kebijakan hukum yang mirip dengan konvensi itu. Selain itu, Rusia juga ikut serta melakukan harmonisasi kebijakan *cyber* di Asia Tengah bersama Cina dibawah organisasi Shanghai Cooperation Organization.

PERMASALAHAN

Dari latar belakang yang telah dipaparkan di atas penulis menemukan fokus permasalahan yang akan di analisis yaitu *pertama*, Mengapa Rusia tidak menandatangani konvensi *European Convention on Cyber Crime* ? dan *kedua*, bagaimana kerjasama yang dilakukan Rusia dalam mempertahankan dunia *cyber* ?

METODOLOGI

Penelitian ini menggunakan metode kualitatif. Teknik pengumpulan data penelitian ini dilakukan melalui studi kepustakaan (*library research*) yang kemudian disusun secara sistematis sehingga memperlihatkan korelasi antara fakta satu dan fakta yang lain. Data dan fakta yang didapat dari berbagai sumber tertulis seperti buku-buku yang relevan, jurnal, dan media massa cetak maupun elektronik yang berkaitan dengan subyek penelitianTeknik analisis data yang digunakan dalam penelitian ini adalah teknik deskriptif-eksplanatif, yaitu dengan menjelaskan dan menafsirkan data yang berkaitan dengan situasi yang terjadi. Pada penelitian ini analisis data bertujuan untuk menjelaskan dan menerangkan kebijakan pemerintah Rusia dan Amerika Serikat dalam kebijakan *Cybercrime* berikut faktor-faktor yang mempengaruhi kebijakan. Selain itu juga melihat Kebijakan dari Organisasi Internasional yang dimana masing-masing negara menjadi anggota tersebut sebagai objek penelitian secara sistematis, faktual, dan akurat.

PEMBAHASAN

Kajian Rusia Tidak Menandatangani *European Convention On Cybercrime*

Diperlukan sebuah perspektif dan konsep dalam hubungan internasional. Yaitu Teori rasionalitas dan konsep dari kejahatan *cyber* atau *cybercrime*. Menurut Max Webber, tindakan sosial terbagi menjadi 4 rasionalitas yaitu rasionalitas berdasarkan tujuan tertentu atau rasionalitas instrumental(*zwecrational*), rasionalitas berdasarkan keyakinan yang dimana berdasarkan pada alas an intrinsik seperti etika, estetika, agama, atau alasan lain(*Wertrational*), rasionalitas yang berdasarkan pada emosi dan perasaan aktor(*Affectual*), dan rasionalitas berdasarkan pada nilai-nilai kebiasan yang terbentuk disuatu lingkungan atau individu(Tradisonal).

Kejahatan *cyber* atau *cybercrime* merupakan salah satu kejahatan asimetris yang menjadi ancaman banyak negara. *Cybercrime* menurut Dr. K. Jaishankar, Kejahatan *cyber* adalah suatu pelanggaran yang dilakukan oleh suatu kelompok atau individu yang memiliki motif criminal untuk merusak suatu reputasi korban atau yang menyebabkan kerugian secara fisik ataupun mental terhadap korban secara langsung ataupun secara tidak langsung, yang menggunakan telekomunikasi modern seperti internet(*Chatrooms, E-mails,* atau forum internet) dan telepon genggam(SMS/MMS). (D, Halder, K, Jaishankar, 2011)

Dalam kasus ini, Rusia mengikuti rasionalitas berdasarkan tujuan tertentu(*Zwecrational*) yaitu dimana pemerintah Rusia menjaga rezim politik yang sekarang dan mengurangi kesempatan aktor-aktor barat untuk melakukan intervensi dalam kebijakan domestik Rusia. Banyak dari petinggi pemerintah Rusia berpikir bahwa revolusi warna yang terjadi di Eropa dikarenakan hasil dari campur tangan pihak barat. Hal ini membuat pemerintah Rusia berkerjasama dengan Shanghai Cooperation Organization untuk melakukan Harmonisasi kebijakan *cyber* didalam wilayah asia tengah.

Rusia memiliki 3 kepentingan nasional didalam melaksanakan kebijakan-kebijakan negara. Yang pertama adalah menjaga rezim politik yang sekarang dan mengurangi kesempatan aktor-aktor barat untuk melakukan interfensi dalam kebijakan domestik Rusia. Banyak dari petinggi dipemerintahan Rusia berpikiran bahwa pihak barat ingin melakukan revolusi didalam pemerintahan Rusia dimana banyak yang berpikir revolusi warna yang terjadi di Eropa adalah dikarenakan buah tangan barat.

Kepentingan nasional yang kedua adalah sebuah perjalanan perjuangan-perjuangan Rusia didalam mendapatkan kehormatan negara, dimana didalam artikel dari Andrei Kortunov, adalah sebuah figur unik didalam kultur Rusia. (Kortunov, Andrey, 2020) Rusia sampai sekarang masih berpikiran bahwa mereka sebuah negara besar dan kuat dimana didalam pengertian tradisional adalah sebuah negara yang memiliki status kuat memiliki kemampuan untuk mendominasi negara lain. Tetapi negara-negara barat tidak mengakui hal ini menyebabkan negara Rusia merasa tidak diakui. Mereka masih melihat Rusia adalah sebuah pecahan dari Uni Soviet.

Kepentingan Nasional Rusia yang ketiga adalah Rusia ingin mendapatkan status yang sama didalam dunia internasional. Meskipun pihak barat telah memberikan Rusia tempat yang sama didalam institusi (contohnya *Council of Europe*), Rusia masih merasa tidak setara. Kesamaan yang diinginkan oleh Rusia adalah dimana Rusia dapat mendorong kepentingan dia didalam dunia internasional dan memiliki hak veto didalam wilayah dia. Ini dapat dilihat didalam organisasi pertahanan Eropa yag dipegang oleh NATO(*North Atlantic Treaty Organization*) yang menyebabkan Rusia melihat bahwa sejarah-sejarah ketika mereka membantu wilayah Eropa tidak diingat oleh Eropa.

Banyak kasus-kasus kejahatan *cyber* yang terjadi di Rusia. Hukum Rusia dalam menangani kejahatan *cyber* paling awal pada 1 Januari 1997didalam Kode Kriminal Federasi Rusia (*Criminal Code of the Russian Federation*). Meski Rusia menyatakan tidak akan menandatangani *European Convention on Cybercrime*, Rusia sendiri sudah memiliki Artikel hukum tentang kejahatan *cyber* dimana Artikel yang paling menonjol ada di bab 28 tentang *Crimes in a computer information sphere*. Bab ini terbagi menjadi 3 artikel yaitu 272 tentang akses informasi ilegal pada komputer, 273 tentang pembuatan, dan pembuatan program

merusak, dan 274 tentang penyebaran program yang dapat merusak, dan penyalahgunaan dalam operasi komputer, sistem komputer, atau jaringan komputer. Artikel 28 ini juga telah direvisi oleh pemerintah Rusia untuk memberi hukuman yang lebih berat kepada para pelaku agar memiliki efek jera dan untuk mereda keinginan calon pelaku untuk melakukan kegiatan *hacking* didalam wilayah pemerintah Rusia.

Selain itu, didalam *Law of the Russian Federation of 27.07.2006 Number 149-FL "On Information, Information Technologies and Protection of Information"*, menjelaskan tentang regulasi legal dalam hal informasi dikarenakan adanya hak untuk mencari, mendapatkan, melakukan pengiriman, produksi, dan distribusi informasi. Informasi dapat menjadi sebuah objek dimana informasi terbagi menjadi dua, yaitu informasi yang dapat diakses oleh individu itu sendiri atau dan inforasi yang dapat diakses oleh siapapun. Kepemilikan informasi harus dimiliki oleh penduduk asli Rusia atau individu legal yang berada diwilayah Rusia. Kepemilikan informasi dapat mengatur informasi apakah informasi itu dapat diakses, dipakai, atau diberikan kepada orang lain. Pemilik informasi juga harus menghormati kebijakan dari pemilik informasi lain, melakukan tindakan,-tindakan dalam melindungi informasi, dan dapat melakukan liitasi akses pada informasi itu. (WIPO, 2020)

Jika diketahui adanya sebuah informasi dalam objek yang mempunyai paten atau sejenisnya atau sebuah informasi yang seharusnya ilegal terdistribusikan tanpa ada konsen dan berdasarkan hukum. Badan pemerintah dapat mengontrol dan akan melakukan monito pada media yang tersebar untuk tidak dapat mengakses informasi itu dimana badan eksekutif akan melakukan kontrol pada informasi itu.

Dalam pertahanan negara dalam dunia *cyber*, Rusia melihat dunia *cyber* dengan memerhatikan sangat dalam pada pertukaran informasi yang tidak bisa dibendung didalam dunia *cyber*. Pertukaran informasi yang sangat massif ini memberikan sebuah ancaman kepada masyarakat dan negara Rusia.

Munculnya sebuah kebijakan pemerintah tentang keamanan informasi pada Rusia yang menjadi pedoman untuk badan eksekutif dan badan pemerintah untuk bergerak dalam mempertahankan kepentingan Rusia dalam lingkup informasi, badan-badan pemerintah juga bergerak dalam dasar untuk menjaga keseimbangan kepentingan individu, sosial, dan negara didalam lingkup informasi.

Kebijakan pemerintah tentang doktrin keamanan informasi berdasarkan pada prinsip Memantau konstitusi dan legislative Rusia didalam kegiatan untuk memberikan keaman informasi yang diterima secara norma dari hukum internasional negara Rusia. Selain itu, prinsip tentang keamanan informasi juga berdasarkn pada prinsi keterbukaan dalam menerapkan kebijakan dari pemerintah kepada public dan memberikan informasi kepada masyarakat tentang aktifitas yang mereka lakukan yang dibatasi oleh legislative Rusia dan adanya kesetaraan semua partisipan didalam interaksi informasi tanpa memandang kedudukan politik, sosial, dan ekonomi. Yang dalam hal ini berdasarkan kepada hak konstitusional warga negara untuk bebas mencari, melakukan transmisi, dan membuat informasi secara legal.

Prinsip kemanan informasi ini juga melakukan prioritas pembangunan informasi dan teknologi informasi dalam negeri didalam menghadapi globalisasi dengan tujuan mempertahankan kepentingan nasional negara Rusia dan melakukan komprehensi didalam analisisi dan meramalkan adanya bahaya dalam keamanan informasi Rusia.

Kerjasama Rusia dalam Upaya Mempertahankan Dunia *Cyber* Melalui Kebijakan Luar Negeri Rusia dan Dalam Negeri

Dunia *cyber* sudah sangat menyebar dan tidak terbendung, tidak adanya batasan terhadap perkembangan teknologi komunikasi membuat dunia *cyber* semakin meluas dengan pemakaian yang semakin banyak didalam dunia ini. Tetapi kejahatan didalam dunia ini juga ikut berkembang mengikuti teknologi dan dengan pandangan dasar dari dunia *cyber* tentang tidak adanya batasan maka kejahatan dapat dilakukan diluar dari negara target. Maka dari itu, perlunya sebuah kebijakan yang sama antar negara gar pelaku dapat terjaring ketika dia berada diluar negara target.

Pemerintah Rusia menanggapi secara serius kejahatan-kejahatan yang terjadi didalam dunia internet dan pemerintahmelihat bahwa kebebasan dalam internet dapat membuat para pelaku melakukan kejahatan dengan mudah dan dapat menimbulkan ketidakstabilan negara. Bahwa dengan mudahnya seseorang menyebarkan informasi yang dapat menimbulkanmasalah secara luas. Maka dari itu, negara Rusia perlu berkerjasama dengan negara lain untuk mempertahankan kepentingan nasional dia. Organisasi yang berpengaruh didalam pertahanan dan keamanan negara rusia adalah *Collective Security Treaty Organization* dan *Shanghai Cooperation Organization*.

Collective Security Treaty Organization atau CSTO adalah sebuah aliansi militer yang terbentuk pada tahun 15 mei 1992 dimana enam negara awal organisasi ini, Rusia, Armenia, Kazakhstan, Kyrgystan, Tajikistan, dan Uzbekistan, menandatangani aliansi ini dengan ditambah 3 negara, Azerbaijan, Georgia, dan Belarusia pada tahun 1994. CSTO dalam hal ini dalam menjaga kestabilan dan keamanan wiayah pada anggota CSTO, maka semua agresi akan kepada 1 anggota akan menjadi agresi kepada seluruh anggota CSTO. (Collective Secuirty Treaty Organization, 2020). Di dalam pertahanan dunia *cyber*, negara anggota didalam artikel delapan didalam piagam CSTO mengatakan bahwa akan berkerjasama didalam mempertahankan perbatasan negara, pertukaran informasi, pertahanan informasi, pertahanan populasi dan wilayah dari keadaaan darurat.

Kerjasama anggota CSTO yang merupakan salah satu kerjasama yang berhasil adalah Operasi PROKSI dimana tujuan utama dari operasi ini adalah untuk mengungkapkan dan menahan informasi didalam bagian internet nasional yang dimana informasi dapat merusak kestabilan negara ataupun negara anggota. (Ruben, Elamiryan, Radomir, Bolgov, 2018). *Shanghai Cooperation Organization* atau SCO adalah sebuah organisasi yang dibentuk pada tahun 15 Juni 2001 oleh negara Cina, Rusia, Kazakstan, Kyrgyztan, Tajikistan, dan Uzbekistan, yang berdasarkan pada deklarasi *Shanghai Cooperation Organization*. Organisasi ini berkerja dala topik politik, ekonomi, dan keamanan. Isi dari konvensi *Shanghai Cooperation Organization* adalah tentang melawan terorisme, separatism, dan ekstrimis.

Pada tahun 2007 diadakan pertemuan pemimpin *SCO* yang menandatangani sebuah dokumen tentang "Perencanaan anggota *SCO* dalam melindungi keamanan informasi internasional". Dokumen ini ditandangani oleh Rusia, Kazakhstan, Kyrgyzstan, Tajikistan, Uzbekistan, dan Cina. Pada pertemuan tahun 2010, SCO memberi pernyataan dalam meningkatkan dan meneruskan dalam melawan terorisme, separatisme dan ekstrimis, dan melawan perdagangan gelap dalam obat-obatan terlarang. Dalam hal ini, topik *cyber* masuk

kedalam terorisme. Pada 11 dan 12 september 2014 diadakan konferensi Dushanbe yang berada di Tajikistan. Topik dari konferensi ini adalah melawan terrorisme, ekstrimis, separatisme, dan juga situasi Afghanistan, non-proliferasi nuklir, kerjasama ekonomi, dan pertahanan informasi. Pada deklarasi konferensi Dushanbe, topik pertahanan informasi berada di seksi 5 yang menyatakan bahwa :

"Anggota SCO melakukan usaha bersama untuk dapat menciptakan ruang informasi yang aman, damai, setara, dan terbuka, yang berdasarkan pada prinsip menghormati kedaulatan nasional dan tidak melakukan intervensi di dalam peristiwa internal negara lain. Anggota SCO akan berkerja sama dalam melakukan pencegahan pada teknologi informasi dan komunikasi yang bertujuan untuk mengacaukan politik, ekonomi, dan keamanan public dan kestabilitasan negara. Selain itu juga untuk menghentikan penyebaran ide pada terorisme, ekstrimis, separatisme, radikalisme, fasisme dan patrotisme terlalu tinggi yang terjadi di dalam internet".

Para anggota mendukung hak bersama pada semua negara di dalam mengurus internet dan kedaulatan negara di dalam perspektif segmen nasional, termasuk salah satunya adalah ketetapan pertahanan. Anggota SCO juga melakukan bantuan dalam pembangunan peraturan universal, norma, dan prinsip didalam tanggung jawab negara di dalam ruang informasi dan melihat. Dalam melihat dunia *cyber*, pihak Rusia dan pihak barat memiliki perbedaan pendapat dalam melihat isu-isu yang berada didalam ruang *cyber*. Meski kedua belah pihak melihat bahwa adanya ancaman didunia *cyber*, perbedaan terhadap persepsi ancaman terhadap konten internet menjadi pembeda kedua belah pihak. Dimana pihak Rusia mempunyai perspesi bahwa konten didalam internet merupakan suatu ancaman.

Hal ini bertolak belakang pada persepsi oleh pihak barat dimana pihak barat melihat isu ini masuk ekdalam hukum saja. Pihak barat menyatakan bahwa ruang *cyber* adalah sebuah tempat dimana kebebasan didalam informasi dan pengetahuan, kebebasan didalam berekspresi, berasosiasi dan berkumpul, yang dimana hal ini menjadi komponen penting didalam demokrasi sosial dan budaya. (OECD, 2020)

Rusia menerima bahwa didalam ruang *cyber* adala sebuah tempat yang bebas. Tetapi Rusia dan negara-negara yang medukung ide didalam kontrol nasional dunia *cyber*, yaitu negara yang menjadi anggota *Commonwealth of Independent States, Collective Security Treaty Organization,* dan *Shanghai Cooperation Organization*, dimana perangkat-perangkat lunak ruang *cyber* yang berada didalam wilayah nasional negara masuk kedalam legislative negara.

Pemerintah Rusia menolak menandatangani *European Convention on Cybercrime* dimana poin-poin konvensi ini sudah masuk kedalam kode kriminal dalam negeri negara Rusia. Selain itu, hal utama yang membuat pihak Rusia tidak ingin menandatangani konvensi ini adalah adanya sebuah Artikel, tepatnya Artikel ke-32 didalam European *Convention on Cybercrime*, yang berisikan "sebuah subjek boleh dengan atau tanpa izin dari subjek lain mengakses atau menerima suatu objek didalam sistem komputer, ataupun didalam data local komputer. Dimana objek didapat secara legal dan subjek tidak merahasiakan objek tersebut."

Pemerintah Rusia melihat dalam artikel bahwa hal ini melanggar kedaulatan negara dimana subjek atau negara lain dapat mengakses dengan tanpa izin objek yang berada didalam wilayah *cyber* kedaulatan Rusia.

PENUTUP

Melihat didalam kebijakan dalam dan luar negeri Rusia, dan dengan melihat bagaimana kepentingan nasional Rusia dalam menjaga negara maka dapat dilihat bahwa penolakan didalam menandatangani *European Convention on Cybercrime* tidak menjadikan negara Rusia sebuah negara tanpa kebijakan *cyber*. Rusia dengan penolakan ini menjadikan kebijakan *cyber* Rusia didalam mempertahankan kepentingan nasional Rusia semakin kuat. Dan dengan kerjasama dengan organisasi regional seperti *Collective Security Treaty Organization* dan *Shanghai Cooperation Organization* menjadikan harmonisasi kebijakan dalam menangani ancaman dunia *cyber* semakin kuat.

DAFTAR PUSTAKA

Andrey, Kortunov,"How not to talk with Russia", https://www.ecfr.eu/article/commentary_how_not_to_talk_with_russia_6053. Diakses tangal 19 Oktober 2020

Collective Secuirty Treaty Organization,"COLLECTIVE SECURITY TREATY, Dated May 15,1992", dalam https://en.odkb-csto.org/documents/documents/dogovor_o_kollektivnoy_bezopasnosti/. Diakses 21 Oktober 2020

D, Halder, K, Jaishankar, Cyber crime and the Victimization of Women: Laws, Rights, and Regulations (pp. 12), Hersey, IGI Global, 2011

Elamiryan, Ruben, Radomir, Bolgov, Cybersecurity in NATO and CSTO: Comparative Analysis of Legal and Political Frameworks, dalam Proceeding 17th European Conference on Cyber Warfare and Security ECCWS (2018), Halaman 146-155

Keir, Giles,"Russian Cyber Security: Concepts and Current Activity", dalam https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/Russia%20and%20Eurasia/060912summary.pdf. Diakses 17 Oktober 2020

OECD, "OECD Council Recommendation on Principles for Internet Policy Making", dalam http://www.oecd.org/dataoecd/11/58/49258588.pdf. Diakses 17 Oktober 2020

Rayman, Noah, " The World's Top 5 Cybercrime Hotspot", dalam http://time.com/3087767/the-worlds-5-cybercrime-hotspots/. 20 Oktober 2020

Stioca, Ionel, "Transnational Organized Crime", dalam Journal of Defense Resources Management, Vol 7 No. 2 (2006), Halaman 13-30.

WIPO," Federal'nyy zakon ot 27.07.2006 goda № 149-FZ 'Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii' (s izmeneniyami, vnesennymi v sootvetstvii s Federal'nym zakonom ot 18.06.2017 g. № 127-FZ)", dalam http://www.wipo.int/wipolex/en/text.jsp?file_id=443109. Diakses 20 Oktober 2020

Worldometer, "Russia Population 2020", dalam https://www.worldometers.info/world-population/russia-population/. Diakses 21 Oktober 2020