BAB I

PENDAHULUAN

A. LATAR BELAKANG MASALAH

Negara-negara pada masa Perang Dunia Dua dan sebelumnya sangatlah memikirkan bahwa keamanan dan pertahanan negara hanyalah sebatas kekuatan militer. Dapat dilihat pada Perang Dunia Satu dan Perang Dunia Dua terbagi menjadi dua kubu. Hal ini sangatlah terlihat bahwa negara-negara besar mempunyai kekuatan militer yang besar juga dimana negara-negara yang memiliki kekuatan militer yang kecil sangat tergantung kepada negara-negara besar untuk menjaga keamanan dan pertahanan negara mereka.

Tetapi setelah terjadi perang dingin yang dilakukan Amerika Serikat dengan Uni Soviet, munculnya banyak konflik-konflik baru yang pada saat itu tidak umum seperti konflik sosial dan konflik budaya. Juga terjadinya perubahan konflik secara garis besar dari yang awalnya adalah konflik vertikal menjadi konflik horizontal. Dari aktor yang awalnya adalah sebuah negara menjadi aktor-aktor organisasi masyarakat sampai pada individu.

Setelah Uni Soviet bubar, munculnya negara baru yang menggantikan Uni Soviet yaitu Rusia. Rusia merupakan negara yang menempati nomor 1 di dalam luas wilayah dengan luas 17,125.200 km^2. Rusia berbatasan langsung dengan Norwegia, Finlandia, Estonia, Latvia, Lithuania, Polandia, Belarusia, Ukraina, Georgia, Azerbaijan, Kazakhstan, Cina, Mongolia, dan Korea Utara. Selain itu, pemasukan

utama dari negera Rusia adalah dari penjualan minyak dan gas yang membuat negara Rusia dapat bertahan dari keruntuhan ekonomi pada tahun 1998.[1] Rusia memiliki bentuk pemerintah berupa Federasi *dual executive system* republik dimana adanya presiden dan perdana menteri di dalam 1 sistem. Dalam hal ini, Vladimir Putin sangat mendominasi system politik dan selalu menjadi antara presiden atau perdana menteri.[2]

Dunia telah masuk ke dalam zaman digital dimana semua orang memiliki ketergantungan terhadap ruang *cyber*. Ruang *cyber* sendiri adalah sebuah tempat dimana suatu data dari barang elektronik disimpan, diperbarui, dan dibagikan melewati jaringan-jaringan yang tidak dibatasi dengan batasan geografi. Banyak manfaat yang muncul dari munculnya teknologi teknologi ini seperti berita, komunikasi, dan bisnis.

Dengan perkembangan teknologi yang sangat pesat merubah banyak tatanan di dalam kehidupan sehari-hari, dengan meningkatnya teknologi maka semakin mudah suatu masalah untuk diselesaikan. Dimana dalam hal ini seperti komunikasi dan transportasi. Dua aspek yang disebutkan dalam 10 tahun ini sangat berkembang pesat dibuktikan dengan munculnya teknologi komunikasi yang sangat maju, yaitu *Smartphone*. Kemudahan ini memberikan perkembangan yang positif di dalam berkomunikasi. *Smartphone* ini tersambung ke dalam sebuah jaringan yang sangat luas dimana kita sebut Internet atau dunia maya. Internet atau dunia maya ini menurut Joseph S. Nye, JR. Adalah

[1] BBC News, "*Russia Country Profile*", https://www.bbc.com/news/world-europe-17839672, 19 Februari 2020.
[2] Reuters,"*Putin says Russia has to be strong presidential republic*", https://uk.reuters.com/article/uk-russia-putin-future/putin-says-russia-has-to-be-strong-presidential-republic-idUKKBN1ZL2DI, 25 February 2020

sebuah domain di dalam jaringan, dimana tersambung dengan Internet dari komputer, teknologi telepon selular, kabel fiber, ataupun komunikasi yang berbasis dalam dunia maya. Domain ini pasti mempunyai sebuah infrastrukur fisik yang terkontrol dalam hukum ekonomi dan hukum politik yang masuk di dalam kekuasaan jurisdikasi.[3]

Meskipun dengan banyak kemudahan-kemudahan yang didapat dari perkembangan teknologi, munculnya sebuah tantangan kepada pembuat kebijakan untuk melihat ke dunia maya. Dimana menurut Joseph S. Nye, JR. domain ini masuk ke dalam jurisidkasi politik dan ekonomi yang mengharuskan pemerintah untuk mengatur dan mempertahankan domain ini agar tidak ada munculnya sebuah ketidakstabilan di dalam sebuah negara.[4]

Cybercrime menjadi sebuah isu yang menjadi perhatian kalangan bawah sampai dengan kalangan petinggi negara. Dalam hukum, sebuah kasus *Cybercrime* tidak mudah diselesaikan dikarenakan untuk melacak pelaku tidak begitu mudah dan bukti-bukti yang diberikan kepada penegak hukum sangatlah teknis dimana diperlukan pengetahuan khusus untuk mengerti barang bukti yang diberikan. Selain itu, perbandingan terjadinya kasus yang berhubungan dengan *Cyber* dengan sumber daya manusia yang ada masih tidak terlalu banyak.

Pelaku-pelaku *Cybercrime* telah banyak muncul dikarenakan mudahnya mendapatkan program-program untuk melakukannya pada era digital ini. Dimana dengan mencari sedikit melalui mesin pencari

[3] Joseph S. Nye Jr, *Nuclear Lessons for Cyber Security*, dash.harvard.edu/bitstream/handle/1/8052146/Nye-NuclearLessons.pdf, 20 Juni 2020
[4] Ibid

dapat menemukan apa yang mereka cari. Dari latihan-latihan dasar untuk melakukan *hacking* dan membuat program-program ilegal dan berbahaya hingga dapat mencari kelompok yang ingin berkerja sama dengan para pelaku-pelaku yang lebih profesional dimana orang-orang baru mendapatkan pengalaman langsung dari para pakar kejahatan.

Dalam dunia *cyber*, kelompok kejahatan-kejahatan yang terjadi melibatkan beberapa pelaku dari luar negeri. Para peneliti yang meneliti tentang kejadian tentang organisasi kejahatan transnasional menyepakati tentang karakteristik-karakterisitik dalam organisasi kejahatan transnasional, yaitu pelaku, objek dari organisasi kejahatan, subjek dari organisasi kejahatan, motif dari organisasi kejahatan, dan sinyal digital. Dari kelima karakteristik itu, dapat dilihat bahwa organisasi kejahatan transnasional memiliki 3 karakteristik yang paling menonjol. Yaitu, mereka melakukan kegiatan secara regional dan global, mereka mempunyai hubungan antar negara yang menghiraukan perbatasan, dan mereka mempunyai kapasitas dalam menantang otoritas nasional dan internasional.[5]

Rusia pada dunia kejahatan *cyber* menjadi sebuah pasar besar dimana wilayah Rusia sangat banyak program-program untuk melakukan kejahatan dikarenakan memang dasar dari pembuatan program-program itu terdapat di Rusia. Selain program-program, mereka juga bisa memesan program-program ilegal itu disana karena banyaknya para pelaku yang berdomisili diwilayah Rusia.

[5] Ionel, Stoica, "Transnational Organized Crime. An International Security Perspective", Journal of Defense Resources Management, edisi 2, volume 7, tahun 2016, halaman 13-30.

Kemajuan dalam era informasi menjadikan para pelaku bisa saja berasal dari negara-negara lain. Para pelaku mencari mangsa ke dalam wilayah-wilayah negara yang jauh dari pelaku agar sulit dilakukannya penangkapan dan penyelidikan dikarenakan perbedaan hukum dan perbedaan sudut pandang kejahatan dalam internet.

Pemerintah Rusia menanggapi secara serius kejahatan-kejahatan yang terjadi ke dalam dunia internet dan pemerintah melihat 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 menimbulkan masalah secara luas. Konsep fundamental Rusia dalam urusan dunia *cyber* adalah adanya kemampuan pemerintah untuk memiliki sebuah kendali terhadap dunia *cyber*. Hal ini didukung oleh negara Cina, Tajikistan, dan Uzbekistan.[6]

Berbeda dengan negara-negara barat dimana mereka menyatakan bahwa informasi harus mengalir dengan bebas tanpa adanya hambatan dari pemerintah sekalipun dikarenakan ini termasuk sebagai kebebasan dalam menyatakan pendapat. Bahkan dalam deklarasi Perserikatan Bangsa-Bangsa (PBB) menyatakan bahwa, “Semua orang mempunyai hak dalam berpendapat dan berekspresi; dalam hal ini termasuk kebebasan dalam menyampaikan opini tanpa ada interfensi dari pihak lain dan kebebasan dalam mencari, mendapatkan, dan memberikan sebuah informasi dan pendapat melalui media apapun tanpa ada

[6] Giles, Keir, 6 september 2012*, “Russian Cyber Security: Concepts and Current Activity”,* https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/Russia%20and%20Eurasia/060912summary.pdf, 21 November 2019

batas".[7] Rusia mempunyai cara pandang yang berbeda dalam hal dunia *cyber* ini dimana Amerika Serikat dan Uni Eropa berpendapat bahwa *cyber* tidak boleh dibataskan tetapi Rusia melihat bahwa dunia baru ini adalah sebuah ancaman negara. Saya ingin melakukan penelitian dimana perbedaan kedua negara ini dalam melakukan pembuatan hukum dan kebijakan, dan kerja sama yang dilakukan negara-negara Amerika Serikat dan Rusia dikarenakan bedanya pandangan dan dimana Rusia tidak ikut menandatangani *Budapest Convention of Cybercrime*.

Dunia *cyber* sendiri sudah menjadi perbincangan di dunia internasional 1997. Munculnya internet awalnya hanyalah digunakan untuk mempercepat berita dan ilmu pengetahuan antar universitas dan laboratorium dan sebagai *platform* dalam ilmu pengetahuan. Tetapi sekarang menjadi sebuah kebutuhan di dalam segala bidang dari sosial sampai dengan pemerintahan. Maka dari itu perlunya sebuah jala pengaman untuk menahan kejahatan-kejahatan yang sedang terjadi dan akan terjadi di dunia *cyber*. Munculnya *European Convention on Cyber Crime* menjadi sebuah jawaban dari hal ini, sebuah konveksi untuk mendasari kejahatan *cyber* untuk melindungi tatanan sosial dengan mengadopsi hukum yang diterima oleh badan legislasi dan dengan bantuan luar negeri. *Council of Europe* adalah sebuah forum yang dibentuk pada tahun 1949 dengan jumlah anggota sebanyak 44 negara dimana semua anggota dari Uni Eropa ikut sebagai penandatangan. Forum ini dibentuk dengan tujuan memperkuat hak asasi manusia dan mempromosikan demokrasi dan aturan hukum di Eropa.

[4] United, Nation, "*Universal Declaration of Human Rights"*, https://www.un.org/en/universal-declaration-human-rights/, 22 November 2019

Convention on Cybercrime, atau *Budapest Convention* adalah sebuah perjanjian internasional yang pertama dalam menghadapi internet dan kejahatan komputer dengan melakukan harmonisasi hukum nasional, meningkatkan teknik investigasi, dan menaikan kerja sama antar negara.[8] Konvensi ini ditandangani pada 23 November 2001 dan mulai berlaku pada 1 Juli 2004.

Konvensi ini mewajibkan negara yang menandatangani untuk memasukan beberapa list ke dalam kejahatan. Yaitu, kejahatan dalam aktifitas *Hacking*(dalam hal ini menjual, mendistribusikan, dan memproduksi alat bantuan *hack*), Kejahatan dalam pornografi yang melibatkan anak dibawah umur, dan memperluas *scope* dalam pelanggaran hak cipta. Penandatangan juga diharuskan untuk melakukan implimentasi bebrapa mekanise prosedur untuk hukum, contohnya dengan memberikan autoritas kepada penegak hukum unutk mempunyai kemampuan atau kekuatan untuk menyuruh *provider internet* memonitor aktifitas internet seseorang. Terakhir, penandatangan konvensi ini diharuskan untuk melakukan kerja sama sebisa mungkin dalam investigasi dan menghukum pelaku kejahatan yang berafiliasi dengan sistem komputer dan data, atau memiliki bukti-bukti dalam bentuk elektronik/*software* bahwa dia adalah pelaku dari kejahatan. Penegak hukum akan membantu penegak hukum negara lain yang berpartisipasi dalam konvensi ini.[9]

Tujuan dari konvensi ini adalah :

[8] Council of Europe, "*Details of Treaty No*. 185", https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185, 28 November 2019.
[9] Electronic Privacy Information Center, *The Council of Europe's Convention on Cybercrime*, https://epic.org/privacy/intl/ccc.html, 23 November 2019

1. Mengharmonisasikan kejahatan-kejahatan hukum dan membantu menghubungkan kepada area *cybercrime*
2. Memberikan penegak hukum domestik kekuatan yang dibutuhkan untuk melakukan investigasi dan penangkapan pada kejahatan-kejahatan dengan menggunakan sistem komputer atau barang bukti yang berhubungan dengan itu dalam bentuk elektronik
3. Menyiapkan rezim yang cepat dan efektif dalam kerja sama internasional.

Banyak negara menyetujui penandatanganan *European Convention on Cyber Crime* dikarenakan konvensi ini adalah sebuah konvensi pertama internasional yang mencakup dunia *cyber* dan menjadi panduan dalam pembuatan kebijakan di dalam dunia *cyber*. Selain itu, konvensi ini juga membuat Negara-negara anggota dapat menyamakan pandangan dalam kejahatan dalam dunia *cyber* dengan negara lain.

Tetapi Pada tahun 2005, Presiden Rusia Vladimir Putin menolak untuk menandatangani dalam *European Convention on Cyber Crime*. Banyak hal yang tidak sesuai dengan kebijakan dari pemerintah Rusia sendiri. Yang pertama adalah dimana aliran informasi berjalan dengan mudah. Pemerintah Rusia berpendapat bahwa itu dapat menyebabkan mudahnya persebaran terror-teror terhadap negara Rusia sendiri yang dapat menghasut masyarakat untuk ikut serta dalam melakukan kejahatan-kejahatan yang dapat merugikan negara dan dimana dengan mudahnya aliran informasi pihak-pihak yang tidak bertanggung jawab dapat menyebar topik dan berita palsu yang dapat menyebabkan perpecahan dan ketidak stabilan pemerintah. Kedua adalah dimana pemerintah Rusia ingin mendapatkan kontrol data-data internet yang

data fisik itu berada di dalam wilayah Rusia. Dalam hal ini adalah server dari data-data itu. Dimana pemerintah Rusia dapat melihat aliran-aliran informasi yang berada diwilayah Rusia agar tidak adanya informasi-informasi yang dapat menimbulkan kerusakan dan ketidakstabilan pemerintah Rusia. Pemerintah Rusia mempunyai kontrol terhadap data yang berada diwilayah Rusia dimana data itu dapat dilihat oleh para penyidik untuk keperluan persidangan. Selain itu, pemerintah Rusia juga dapat dengan mudah menutup halaman website yang bermasalah tanpa menunggu surat izin menutup halaman *website* yang bermasalah itu. Yang ketiga adalah Presiden Rusia Vladimir Putin menanggapi bahwa Rusia bisa menandatangani konvensi siber itu jika adanya revisi pada isi konvensi di Artikel 32 bagian 'b' yang mengatakan bahwa "*Party may, without the authorisation of another Party access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the party through that computer system*" atau ditranslasikan ke dalam bahasa indonesia menjadi "sebuah subjek boleh dengan atau tanpa izin dari subjek lain mengakses atau menerima suatu objek di sistem komputer, ataupun di dalam data lokal komputer. Dimana objek didapat secara legal dan subjek tidak merahasiakan objek tersebut". Presiden Vladimir Putin menyatakan bahwa artikel ini dapat membahayakan dan merusak kedaulatan negara dan keamanan negara anggota pada hak-hak masyarakat.[10]

[10] eng.cnews.ru, "*Putin defies convention on Cybercrime*", http://www.crime-research.org/news/28.03.2008/3277/, 27 November 2019

Meskipun Rusia tidak ikut menandatangani konvensi itu. Pada tahun 2011, dikeluarkan sebuah statemen kebijakan tentang ruang *cyber* oleh Rusia yaitu ”*Conceptual Views on the Activity of the Russian Federation Armed Forces in Information Space*”. Statemen ini dipresentasikan pada tahun 14 desember 2011 di Berlin pada pertemuan keamanan informasi.[11] Isi dari statemen ini adalah adalah Rusia melihat potensi dalam operasi di dalam ruang informasi, asumsi dan definisi tantangan ruang informasi, dan dimana konsep keamanan informasi negara lain, termasuk dalam hal ini militer, sangat berbeda dengan Rusia.

Terbentuknya *Shanghai Cooperation Organization* yang adalah sebuah organisasi yang terbentuk dengan tujuan melawan terorisme, separatisme dan ektrimis. Sesuai dengan deklarasi *Shanghai Cooperation Organization*, anggota dari organisasi ini berkerja sama untuk mengatasi masalah politik, ekonomi, dan keamanan. Organisasi ini terbentuk pada 15 Juni 2001 dan menjadi jembatan dan wadah diwilayah Asia dan Rusia.[12]

Dengan naiknya penggunaan dunia *cyber* oleh masyarakat di dalam wilayah Rusia, ini menjadi sebuah wadah masyarakat dalam menyampaikan pendapat dalam opini politik dan berdiskusi bersama. Ini menjadi sebuah permasalahan ketika hal ini salah satu cara masyarakat Rusia untuk mengangkat isu-isu politik seperti pemalsuan

---

[11] *Russian Ministry of Defense,* 22 Desember 2011, “*Russian Federation Armed Forces' Information Space Activities Concept*”, http://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle, 22 November 2019.

[12] CCDCOE, “*Information Security Discussed at the Dushanbe Summit if the Shanghai Cooperation Organisation*”, https://ccdcoe.org/incyder-articles/information-security-discussed-at-the-dushanbe-summit-of-the-shanghai-cooperation-organisation/, 27 November 2019.

hasil pemilihan anggota *Duma* pad tahun 2011, diskusi tentang *Arab spring* atau kebangkitan dunia arab, dan protes pembuatan jalan sambung yang menghubungkan kota Moskow dan kota St. Petersburg.[13]

Negara-negara anggota dari *Euroepan Convention on Cybercrime* menekan Rusia di dalam pertahanan ruang *cyber* dikarenakan Rusia melakukan serangan-serangan kearah negara anggota konvensi ini tanpa mendapatkan hukuman sama sekali. Tanpa ada nya konvensi yang mengikat, Rusia dapat masuk ke dalam ruang *cyber* tanpa terganggu oleh negara lain. Selain itu, dengan kasus Snowden, seorang *whistleblower* tentang bagaimana Amerika Serikat mengawasi semua orang, Amerika melakukan protes dan tekanan kearah Rusia untuk memberikan kekuatan penegak hukum untuk masuk dan melakukan penahan kepada Snowden.

Dengan tekanan-tekanan itu dan dengan adanya klausa tentang bagaimana negara lain dapat mengakses informasi pada negara lain, Rusia tidak tertarik untuk melakukan kerja sama pertahanan *cyber* kearah Eropa dan mengalihkan pandangan kearah Asia. Dimana Rusia dapat mendorong kerja sama dengan negara-negara lain tanpa takut negara yang ikut berkerja sama masuk ke dalam negeri Rusia dan Rusia juga dapat memajukan kepantingan dia dalam penguatan pertahanan *cyber* global nya.

[13] Karina, Alexanyan, Vladimir, Barash," Exploring Russian Cyberspace: Digitally-Mediated Collective Action and the Networked Public Sphere", Research Publication No. 2012-2 March 2012, The Berkman Center of Internet & Society, Harvard Unversity.

B. Rumusan Masalah

Dengan melihat dari latar belakang dan alasan pemilihan judul, muncul sebuah pertanyaan yaitu Mengapa Rusia tidak menandatangani konvensi *European Convention on Cyber Crime* ?

C. LITERATURE REVIEW

Dalam Jurnal berjudul *Contest and Conquest: Russia and Global Internet Governance* karya Julien Nocetti pada Jurnal International Affair Volume 91 Issue 1 pada halaman 111 sampai 130 menjelaskan bahwa dunia *cyber* adalah sebuah arena dimana negara-negara berkompetisi untuk mendapatkan kekuasan dalam mengatur dunia *cyber*. Julien Nocetti memberikan contoh dimana adanya sebuah eksistensi Negara-negara besar seperti Cina dan Amerika yang melakukan *cyber-spying*, melakukan kegiatan mata-mata di dalam dunia *cyber*, di dalam dunia *cyber* yang menargetkan Negara lain untuk mendapatkan informasi-informasi. Selain itu Julian Nocetti juga menjelaskan tentang 3 trend yang dilakukan pemerintah Negara besar,

Yang pertama adalah banyak pemerintah melakukan kebijakan mereka di dalam dunia *cyber* sama dengan dunia nyata. Tetapi hal ini menjadi sebuah hambatan dimana banyak perusahaan swasta memegang peran di dalam dunia *cyber* dan pemakai dari dunia *cyber* adalah masyarakat luas.

Yang kedua adalah pemerintah masih berjuang untuk mengejar ketinggalan dalam perubahaan teknologi. Kecepatan berkembangnya teknologi tidak dapat diikuti oleh perkembangan pembuatan kebijakan.

Yang ketiga adalah dunia *cyber* berkembang dengan cepat dan merata keseluruh dunia dan mulai menjadi internasional dan tidak mengikuti wilayah barat, tempat asal dunia *cyber*. Dan mulai menantang dominasi oleh Amerika dalam dunia *cyber*.

Jurnal ini mengeksplorasi kebijakan dalam negeri dan luar negeri internet pemerintah Rusia dalam menghadapi dunia *cyber* dimana memberikan konklusi bahwa Rusia berusaha untuk mendapatkan kedaulatan di dalam dunia *cyber* dimana kebijakan Rusia bersinggungan dengan pemerintah karena teknologi digital dapat digunakan sebagai penyebab perpecahan di dalam masyarakat yang dapat memicu ketidakstabilan negara. Selain itu, Rusia juga ingin menghentikan pergerakan Amerika di dalam wilayah kedaulatan Negara Rusia.

Dalam Paper Konverensi Internasional berjudul *Russia's Public Stance on Cyberspace Issues* Karya Keir Giles dalam *2012 4th International Conference on Cyber Conflict* yang dilakukan oleh NATO Cooperative Cyber Defence Centre of Excellence menjelaskan bahwa dasar dari pendangan Rusia oleh ancaman dunia *cyber* sangat berbeda dengan Negara barat. Dimana Rusia sangat berpikir bahwa prinsip pertukaran informasi yang tidak terkontrol di dunia *cyber* yang tidak mempunyai batas wilayah sangat mengkhawatirkan pemerintah Rusia dimana Rusia mempunyai "Kedaulatan Internet". Hal ini yang ingin dibagikan oleh pemerintah Rusia dalam menyamakan pemikiran dalam prinsip umum di dalam dunia *cyber*. Dalam paper yang ditulis oleh Keir Giles ini melihat 2 aspek yang dikeluarkan oleh pemerintah Rusia dalam kebijakan dunia *cyber*. Yaitu, *Draft Convention on International Information Security*

dan *Conceptual Views on the Activity of the Russian Federation Armed Forces in Information Space*. Aspek pertama adalah dimana Rusia memberikan Draft Konvensi untuk menyamakan dasar dari dunia *cyber* kepada PBB dan Aspek kedua adalah dunia *cyber* juga menjadi sebuah kedaulatan Negara Rusia dimana militer akan ikut mempertahankan kedaulatan negara Rusia.

Dalam Jurnal yang berjudul *A World of Difference: The Budapest Convention On Cybercrime and the Challenges of Harmonisation* Karya Jonathan Clough dalam Monash University Law Review Volume 40 Nomor 1 Halaman 698 sampai 736 menjelaskan tentang bagaimana teknologi informasi dan komunikasi menjadi pusat dari interaksi untuk bersosialisasi dan berdagang dimana hal ini menjadi umpan untuk melakukan kejahatan. Terhubungnya seorang individu di dunia luas menjadi sebuah permasalahan global dimana hal ini menjadikan perhatian khusus di dunia internasional. *Convention on Cybercrime* yang dibuat oleh *Council of Europe* menjadi sebuah konvensi pertama yang bersifat multilateral dalam meregulasi *cybercrime*. Pentingnya harmonisasi kebijakan dalam melawan *cybercrime* dikarenakan adanya sebuah tantangan unik dimana *cybercrime* sudah pasti menjadi sebuah masalah transnasional karena sifat dasar dari dari *cybercrime* adalah mengikuti dari perkembangan teknologi. Dengan mengharmonisasikan kebijakan ini, tidak ada negara atau wilayah yang menjadi tempat aman dari pelaku kejahatan *cyber*. Dikarenakan tidak adanya hukum yang mencakup itu. Jurnal ini juga menuliskan tentang pangangan umum tentang *Convention on Cybercrime*. Selain itu, dalam jurnal ini juga menjelaskan tentang adanya sebuah lawan dari konvensi ini. Yaitu yang dibuat oleh *Shanghai Cooperation Organisation* dan Liga Arab.

Dimana *Shanghai Cooperation Organisation* lebih mengarah kepada terorisme dan ancaman informasi. Sedangkan Liga Arab lebih mengarah kepada hukum dan kestabilan dalam negeri.

Dalam Artikel yang berjudul *Russia and the Council of Europe Convention on Cybercrime* Karya Orji Uchenna Jerome dalam Computer and Telecommunication Law Review menjelaskan tentang Rusia sebagai member dari *Council of Europe* atau Dewan Eropa tidak ikut menandatangani dikarenakan adanya klausa kedaulatan dan menginginkan klausa itu dihapus. Tetapi, dalam *Convention on Cybercrime* sendiri juga sudah ada sebuah pengaman agar negara lain tidak ikut serta terlalu jauh dalam penegakan negara. Negara yang diminta boleh menolak untuk melakukan ekstradisi pelaku kejahatan jika pelaku masih menjadi penduduk negara. Selain itu, negara juga boleh menolak memberikan barang bukti berupa perangkat keras jika itu mengandung rahasia negara. Dalam tulisan ini, pemerintah Rusia menekankan bahwa ancaman criminal, teroris, dan militer atau politik menjadi sebuah isu di dalam keamanan dunia *cyber*. Dengan memajukan kebijakan dalam negeri, pemerintah Rusia membantu mengamankan dunia *cyber* dikarenakan banyak perangkat lunak yang berasal dari negara Rusia.

Dalam Tesis yang berjudul *Offense-defense theory analysis of Russian cyber capability* Karya Sergei A. Medvedev dari Naval Postgraduate School, Monterey, California menjelaskan bahwa kemampuan *cyber* Rusia dalam pertahanan *cyber* sangat mumpuni dimana di dalam tulisan ini mengatakan bahwa Pemerintah Rusia dapat melakukan serangan balik dan melakukan pertahanan awal dalam dunia *cyber*. Dengan ter integrasi nya kebijakan dunia *cyber* dengan militer,

Rusia dapat melakukan penanganan yang cepat untuk menindaklanjuti masalah dunia *cyber*. Perbedaan dalam melihat pertahanan *cyber* sangat menguntungkan pemerintah Rusia dikarenakan di dalam kebijakan-kebijakan nya memiliki konsiderasi jika pelaku adalah sebuah organisasi non-pemerintah yang memiliki potensi untuk mengganggu kestabilan negara. Dikarenakan ini, kebijakan pemerintah Rusia lebih melihat bagaimana kedaulatan negara dapat dijaga. Pemerintah Rusia juga mengirimkan draft untuk Pemerintah Bangsa-Bangsa untuk menyamakan persepsi dalam melihat ancaman dunia *cyber*.

Tabel 1.1: Mengenai Isi Pokok dari Keseluruhan *Literature Review*

No	Nama Penulis	Judul	Tempat Publikasi	Argumen Penulis
1	Julien Nocetti	Jurnal > *Contest and conquest: Russia and global internet governance*	International Affair Volume 91 Issue 1 pada halaman 111 sampai 130	• Negara berkompetisi untuk mendapatkan kekuasaan. • Masyarakat sebagai pengguna nomor 1 di dunia *cyber*. • Dunia *cyber* akan menjadi permasalahan global dikarenakan perkembangan teknologi
2	Keir Giles	Paper > *Russia's Public Stance on Cyberspace Issues*	*4th International Conference on Cyber Conflict* oleh NATO	• Perbedaan pandangan oleh pemerintah Rusia dengan pihak barat • Rusia memiliki sebuah pengertian tentang Kedaulatan Internet dimana negara dapat ikut campur ke dalam dunia *cyber*. • Rusia mengirimkan draft kepada PBB untuk

				menyamakan pandangan dalam ancaman dunia *cyber*.
3	Jonathan Clough	Jurnal > *A WORLD OF DIFFERENCE: THE BUDAPEST CONVENTION ON CYBERCRIME AND THE CHALLENGES OF HARMONISATION*	Monash University Law Review Volume 40 Nomor 1 Halaman 698 sampai 736	• Perkembangan Teknologi adalah pemicu munculnya kejahatan *cyber*. • Perlunya harmonisasi di dalam kebijakan negara-negara agar tidak adanya *safe haven* atau tempat aman untuk pelaku kejahatan *cyber*. • Adanya Konvensi lain yang membicarakan dunia *cyber* tetapi memiliki perbedaan pandangan terhadap ancaman *cyber*.
4	Orji Uchenna Jerome	Artikel > Russia and the Council of Europe Convention on Cybercrime	Computer and Telecommunication Law Review	• Penolakan Rusia untuk menandatangani *Convention on Cybercrime* dikarenakan ada klausa kedaulata dan akan menandatangani jika klausa itu dihilangkan. • Dengan meningkatkan kebijakan dalam

				negeri, pemerintah Rusia juga ikut membantu meningkatkan pertahanan *cyber* global
5	Sergei A. Medvedev	Tesis > Offense-defense Theory analysis of Russian cyber capability	Naval Postgraduate School, Monterey, California.	• Rusia sebagai actor kunci di dalam dunia *cyber*. • Kemampuan *cyber* Rusia untuk melakukan pertahanan sangat kuat.

D. KERANGKA TEORI

1. Teori Rasionalitas

Teori rasionalitas diperkenalkan pertama kali oleh Max Webber, seorang sosiolog dari Jerman dengan intepretasi tindakan sosial yang dibedakan dalam empat jenis rasionalitas, pertama adalah *zwecrational* atau rasionalitas berdasarkan tujuan tertentu atau rasionalitas instrumental, yaitu dengan harapan tingkah laku orang lain atau objek lain dalam lingkungan sekitra yang diperhitungkan secara rasional. Kedua adalah *Wertrational* atau rasional berbasis nilai keyakinan. Rasional ini didasarkan pada alasan intrinsik seperti etika, estetika, agama, atau alasan lain, yang langsung maupun tidak diyakini akan membawa keberhasilan. Ketiga adalah *Affectual*, nilai-nilai yang dipakai di dalam ini adalah emosi dan perasaan dari aktor. Keempat adalah tradisional, dimana nilai-nilai yang dilihat adalah kebiasaan yang terbentuk disuatu lingkungan atau individu.[14]

2. Kebijakan Nasional

Kebijakan nasional menurut Arnold Wolfers adalah sebuah simbol pengertian yang dilihat oleh suatu orang berbeda-beda, dimana secara objektif keamanan nasional adalah hilangnya sebuah gangguan untuk

[14] Tulus Warsito, Nasionalitas Politik, Program S3 Ilmu Politik Direktorat Pasca Sarjana UMY, halaman 60.

mendapatkan sesuatu dan hilangnya ketakutan pada saat objek itu diambil.[15]

Kebijakan nasional Rusia ialah bagaimana pemerintah Rusia untuk mempertahankan individu, masyarakat, dan negara dari ancaman dalam atau luar negeri. Kepentingan nasional Rusia adalah bagaimana pemerintah menjaga banyaknya kepentingan domsetik dengan cara organisasi publik yang beroperasi dibawah pemerintah Rusia secara konstitusional dan hukum. Dalam hal domestik, kepentingan nasional Rusia menitik beratkan pada stabilitas sistem konstitusional negara yang dimana membuat adanya harmoni, menjaga perdamaian publik, dan menghilangkan faktor-faktor yang dapat membuat pemerintah tidak stabil.

3. Konsep *Cybercrime*

Cybercrime merupakan salah satu kejahatan asimetris yang menghantui banyak negara dikarenakan susahnya para penegak hukum untuk melaksanakan tugasnya. Amerika sendiri yang merupakan negara yang sudah menandatangani konvensi Budapest dan memiliki badan hukum yang bagus tetap tidak bisa menghindari dari serangan para hacker yang menginginkan ada nya kebebasan dalam berpendapat di dunia *cyber*. Dalam kasus megaupload, Amerika menghilangkan website file sharing dikarenakan adanya berkurangnya tingkat perekonomian dari hak-hak cipta seperti software, musik, film, dan barang-barang lain yang berkaitan dengan soft file. Amerika menangkap pemilik dari situs file sharing, yaitu Kim Dotcom. Meski setelah itu Anonymous yang merupakan suatu kelompok penjahat

[15] Arnold, Wolfers. "National Security", *Political Science Quarterly*, edisi 4, volume 67, tahun 1952, halaman 483.

melakukan serangan kepada situs FBI (*Federal Bureu of Investigation*), Universal Music Group, dan situs department hukum Amerika yang membuat situs-situs itu tidak bisa dibuka untuk beberapa saat.[16]

Berkembangnya teknologi internet adalah suatu anugerah dan malapetaka di dalam negara dan masyarakat. Dengan tidak adanya sebuah halangan untuk mengakses sesuatu dan mudahnya dalam melakukan kegiatan di dalam internet mampu menjadikan sebuah teknologi yang awalnya untuk kegiatan ilmu pengetahuan menjadi sebuah konsumsu umum. Tetapi, kejahatan juga terjadi di dalam internet. Banyak kasus yang terjadi di dunia *cyber* yang contohnya adalah kegiatan *hacking*, situs pornografi, dan penjualan barang-barang ilegal yang memaksa pemerintah negara masuk menjadi badan yang bertujuan untuk menjaga masyarakat dan khususnya pemerintahan agar tidak terkena dan menangkal hal-hal yang nantinya akan terjadi.

Dalam era globalisasi teknologi ini, telah banyak juga penggunaan dalam internet yang dampaknya adalah banyak juga bermunculan kriminal-kriminal yang berada diruang internet. Dalam hal ini disebut sebagai kejahatan *Cyber* (*Cybercrime*). *Cybercrime* sendiri adalah suatu kejahatan yang dilakukan melalui komputer dan jaringan. [17] Komputer itu dapat menjadi alat untuk melakukan kejahatan atau menjadi target dari kejahatan itu. Menurut Dr. K. jaishankar. Kejahatan *Cyber* "adalah suatu pelanggaran yang dilakukan suatu kelompok atau individu yang memiliki motif kriminal untuk merusak suatu reputasi

---

[16] Christopher, Williams, 20 januari 2012, "Anonymous attacks FBI website over Megaupload raids", http://www.telegraph.co.uk/technology/news/9027246/Anonymous-attacks-FBI-website-over-Megaupload-raids.html, 22 November 2019.

[17] R,Moore, *Cyber crime: Investigating High-Technology Computer Crime*, Anderson Publishing, Cleveland, Mississippi, 2005, Halaman 2

korban serangan atau yang menyebabkan merugikan secara fisik ataupun mental terhadap korban secara langsung ataupun secara tidak langsung, yang menggunakan telekomunikasi modern seperti internet(Chat rooms, Emails, papan pengumuman disuatu forum) dan telepon Genggam (SMS/MMS)".[18] Kejahatan itu dapat mengganggu keamanan dan finansial suatu negara. Isu tentang jenis kejahatan ini akan menjadi suatu isu yang diperhatikan jika dalam kasus *Cracking* dan pelanggaran hak cipta, pornografi yang melibatkan anak kecil. Selain itu, ada juga suatu permasalahan tentang Privasi dalam suatu informasi yang rahasia bocor. Dalam level global, aktor pemerintah dan non-pemerintah semakin besar kepentingannya dikarenakan sekarang dapat melakukan suatu aktifitas espionage dan serangan-serangan dari tempat yang tidak mengenal batas negara.

E. ARGUMEN PENELITIAN

Berdasarkan uraian penulis diatas, argument utama dari penulis adalah pemerintah Rusia tidak ingin menandatangani *European Convention on Cybercrime* dikarenakan Rusia tidak ingin gerakan-gerakan nya di dalam dunia *cyber* terbatasi oleh negara lain. Pemerintah Rusia memiliki pemikiran bahwa konvensi ini adalah sebuah cara kekuatan barat masuk ke dalam pemerintah Rusia melalui informasi-informasi di dalam dunia *cyber*. Dengan tekanan-tekanan yang diberikan oleh negara Eropa dan Amerika, Rusia mengalihkan pandangan kearah Asia dengan tujuan meningkatkan pertahanan *cyber* negara Rusia tanpa adanya campur tangan dari negara lain.

[18] D, Halder, K, Jaishankar, *Cyber crime and the Victimization of Women: Laws, Rights, and Regulations*, IGI Global, Hershey, 2011, Halaman 12

F. TUJUAN PENELITIAN

Ada beberapa tujuan yang memberikan peneliti melakukan penelitian mengapa Rusia tidak ikut menandatangani *European Convention on Cybercrime* adalah :

1. Untuk mengetahui pandangan Rusia terhadap ancaman di dalam dunia *cyber.*
2. Untuk mengetahui upaya Rusia dalam mempertahankan kedaulatan dalam dunia *cyber*.
3. Untuk melihat perkembangan kebijakan dalam menghadapi dunia *cyber*.
4. Untuk mengetahui kerja sama-kerja sama yang dilakukan Rusia dalam mempertahankan dunia *cyber*.

G. METODOLOGI PENELITIAN

1) Jenis Penelitian

Penelitian tesis ini menggunakan metode kualitatif. Metode kualitatif adalah metode yang lebih menekankan pada aspek pemahaman secara mendalam terhadap suatu masalah. Metode ini lebih menggunakan teknik analisis mendalam, yaitu mengkaji masalah secara kasus per kasus. Metode kualitatif meyakini bahwa sifat suatu masalah yang satu akan berbeda dengan sifat dari masalah lainnya. Tujuan dari metode ini lebih kepada pemahaman secara mendalam terhadap suatu masalah.

2) Teknik Pengumpulan Data.

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 penelitian

3) Teknik Analisis Data

Teknik analisis data yang digunakan dalam penelitian ini adalah teknik deskriptif-eksplanatif, yaitu dengan menjelaskan dan menafsirkan data yang berkaitan dengan situasi yang terjadi. Pada penlitian ini analisis data bertujuan untuk menjelaskan dan menerangkan kebijakan pemerintah Rusia 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.

H. BATASAN MASALAH

Jangkauan Penelitian ini dimulai pada tahun 2005 dimana negara Rusia menolak menandatangani *European Convention on Cyber Crime* sampai dengan 2015 dimana *Shanghai Cooperation Organization* mengusulkan revisi dari *International Code of Conduct for Information Security*.

I. SISTEMATIKA PENULISAN

Penulisan tesis ini akan terdiri atas 5 bab, yaitu :

Bab 1 PENDAHULUAN : Akan menjelaskan tentang pendahuluan yang terdiri atas alasan pemilihan judul, latar belakang masalah, rumusan masah, kerangka teori, asumsi dasar, metodologi peneltian,

tujuan dan manfaat penelitian, jangkauan penelitian, dan sistematika penulisan

Bab 2 PERKEMBANGAN DUNIA CYBER DAN MUNCULNYA EUROPEAN CONVENTION ON CYBERCRIME : Akan membahas tentang perkembangan dunia *cyber* rezim internasional dan akan membahas tentang *European Convention on Cybercrime*.

Bab 3 KEBIJAKAN CYBER RUSIA DAN KERJA SAMA SHANGHAI COOPERATION ORGANIZATION DALAM MEMPERKUAT PERTAHANAN REGIONAL : Akan membahas tentang penjelasan terhadap kebijakan-kebijakan *cyber* pemerintah Rusia dalam menghadapi dunia *cyber* dan kerja sama di dalam *Shanghai Cooperation Organization* dalam rangka memperkuat pertahanan *cyber* regional.

Bab 4 PENOLAKAN PEMERINTAH RUSIA DALAM MENANDATANGANI EUROPEAN CONVENTION ON CYBERCRIME : Akan membahas tentang alasan dan faktor pemerintah Rusia tidak menyetujui dalam menandatangani *European Convention on Cybercrime*.

Bab 5 KESIMPULAN DAN SARAN : akan memuat kesimpulan dari keseluruhan bab-bab sebelumnya yang akan melihat dari secara luas sampai dengan aktor negara dalam dunia *cyber*.