

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Pada perkembangan era globalisasi, teknologi merupakan salah satu aspek yang berkembang dengan pesat. Salah satu perkembangan yang terjadi adalah perkembangan dalam bidang internet atau dunia siber (*cyberspace*). Hal ini terlihat pada saat jatuhnya bom nuklir pada Perang Dunia II, dimana pada awal mulanya *cyberspace* dikembangkan untuk teknologi militer yang digunakan sebagai jaringan distribusi dalam mengirim informasi (Buzan and Hansen, 2009). Seiring berjalanya waktu, internet mulai banyak digunakan oleh beberapa negara di dunia.

Paris Call for Trust and Security in Cyberspace adalah deklarasi tingkat tinggi yang mendukung pengembangan prinsip-prinsip umum untuk mengamankan ruang siber dan prinsip-prinsip utama yang terkait: kepraktisan hukum internasional, perilaku yang bertanggung jawab dari aktor Negara, tanggung jawab spesifik dari pemangku kepentingan swasta, terutama dalam hal mencegah kegagalan keamanan dan mencegah penggunaan praktik tertentu yang dapat merusak stabilitas di dunia maya (France Diplomatie, 2018). Pembuatan deklarasi ini menunjukkan peran aktif Prancis dalam mempromosikan ruang siber yang aman, stabil, dan terbuka. Deklarasi politik tingkat tinggi ini menandai komitmen baru terhadap masalah mendasar stabilitas di ruang siber. *Paris Call* dipresentasikan di *Paris Peace Forum* pada 12 November 2018 dan dipromosikan oleh Presiden Prancis di UNESCO sebelum *Internet Governance Forum*.

Ini menunjukkan kemampuan Prancis untuk secara luas mendukung visinya dalam hal pengaturan ruang siber (France Diplomatie, 2018). Ada sembilan (9) poin yang ada di dalam *Paris Call* ini, yakni: (1) Melindungi individu dan infrastruktur; (2) Melindungi internet; (3) Menjaga proses pemilihan umum; (4) Menjaga *intellectual property*; (5) Non-proliferasi; (6) Keamanan siklus hidup (*lifecycle*); (7) *Cyberhygiene*; (8) Tidak ada retasan kembali secara pribadi (*No private hack back*); (9) Norma Internasional (*Paris Call*, 2018). Presiden Emmanuel Macron melihat adanya ancaman yang hadir dalam ranah siber ini, seperti yang dinyatakannya di *Internet Governance Forum* bahwa:

“I would first like to say that I believe that the Internet we take for granted is under threat.”¹

Prancis memandang bahwa kejahatan siber itu nyata dan ada. Bahkan hal ini terlihat pada sejarah Prancis yang memiliki peraturan dalam menjaga keamanan Internet, beberapa contoh peraturan dari Prancis merupakan: buku putih Prancis tahun 2008, *Agence nationale de la sécurité des systèmes d’information* (ANSSI) tahun 2009, *The 2011 National Digital Strategy* (Baumard, 2017), hingga buku putih yang dikeluarkan oleh Prancis, dalam poin ke-9 dan poin ke-10 buku putih Prancis tentang ‘..., *Cyber defence: a new strategic context*, dan *Giving priority to intelligence*,...’ (Ministere de la Defense, 2013), yang di dalamnya mereka merasa bahwa dunia siber merupakan hal yang harus di jaga keamanan stabilitasnya, aman dan terbuka.

¹ Dikutip dari transkrip pidato Emmanuel Macron di dalam *International Governance Forum* pada tahun 2018. <https://www.intgovforum.org/multilingual/content/igf-2018-speech-by-french-president-emmanuel-macron>. Diakses pada 7 November 2019

Pembuatan *Paris Call* terjadi di karena adanya ancaman yang terjadi di dalam ranah siber. Di mana serangan tersebut di-lakukan oleh individu atau bahkan di dukung oleh suatu aktor negara maupun influensi suatu aktor non-negara. Kesadaran oleh Prancis muncul pada Juni 2010, yang terlihat dari kemuculan Stuxnet pada saat itu, kode berbahaya ini diperkenalkan dalam perangkat lunak di dalam komponen perangkat keras perusahaan Jerman Siemens yang dimaksudkan untuk menargetkan dan mengintegrasikan sistem kontrol dan akuisisi data (*SCADA*) dari situs pengayaan uranium di Natanz, Iran (Falliere, Murchu and Chien, 2011; Baumard, 2017) yang di buat oleh Amerika Serikat dan Israel. Beberapa contoh lainnya merupakan kejadian di Estonia tahun 2007, di mana terjadinya *Distributed Denial of Service* (DDoS) yang di lakukan oleh “peretas patriotik” dari Russia yang tersinggung karena monumen Perang Dunia II terhadap Soviet. Hal serupa terjadi pada tahun 2008 di Georgia, yang terkena DDoS dalam sistem informasinya sebelum tentara Russia melakukan invasi. Asumsi yang terjadi adalah pemerintah Russia telah bersekongkol dengan peretas, dan menolak kaitan mereka terhadap peretasan (Nye, 2018). Interfensi luar terhadap pemilu juga merupakan ancaman terhadap demokrasi, seperti kasus di negara Meksiko pada tahun 2018, yang di lihat dari banyaknya pendatang ke dalam website *voting*, terutama dari Russia (Rozak, 2018). Lalu pada tahun 2017, di Kenya yang terdapat influensi dari *Cambridge Analytica* pada saat pemilu (Crabtree, 2018). Lalu serangan terhadap *critical infrastructure*, seperti serangannya terhadap jaringan TV Prancis TV5 Monde pada tahun 2015 (ssMelvin & Botelho, 2015). Ancaman-ancaman siber ini bagi Prancis, membuat ranah siber menjadi tidak stabil, dan tidak aman, bukan hanya mengancam

aktor negara maupun sektor industri saja, akan tetapi ancaman bagi demokrasi dan Hak Asasi Manusia (HAM).

Menurut Fabrizio Hochschild selaku Asisten Sekretaris Jenderal untuk Koordinasi Strategis PBB, penetapan sebuah norma merupakan tahapan yang krusial. Norma di dalam ranah siber ini di namakan *cybernorms* (norma siber). Akan tetapi, perlu dilihat lagi bahwa beberapa prinsip yang dibuat oleh Prancis merupakan prinsip-prinsip umum yang telah ada dalam beberapa perjanjian keamanan siber, seperti ENISA yang berfokus pada dunia siber di Uni Eropa, dan Konvensi Internasional Budapest yang telah mereka tanda tangani. Bahkan konvensi Budapest telah ditandatangani oleh pelbagai negara dari Uni Eropa, maupun bukan non-member Uni Eropa². Selain itu, terdapat juga kerangka pembuatan norma siber sebelum-sebelumnya seperti *Cybersecurity Tech Accord*, *Charter of Trust*, dan *For the Web*. Lalu apa yang membedakan *Paris Call* dari yang lainnya, dan yang menjadi sebuah *puzzle* adalah bagaimana Prancis menciptakan norma baru dan mengingatkan norma umum melalui *Paris Call*?

Seiring dengan perkembangan Hubungan Internasional, penelitian di dalam *cyberspace* minim sekali, terutama terhadap norma internasional di ranah siber. Sebagai contoh, tesis Hubungan Internasional yang memfokuskan sekuritisasi *cyber laundering* (pencucian siber) yang terjadi di Internet dan lebih memfokuskan kepada sekuritisasi pencucian uang di dalam *game online* (Kaloka, 2017). Penelitian yang di

² Sumber dapat dilihat melalui halaman web *Council of Europe* : https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=XFjffPQ4

lakukan cenderung hanya berfokus terhadap *cybercrime*, sekuritisasi siber, dan kerjasama siber. Akan tetapi minimnya penjelasan tentang pembuatan *cybern norms* oleh suatu aktor.

Berdasarkan permasalahan di atas, penelitian ini berusaha menyajikan analisis tentang pembuatan *cybern norms* dan menjelaskan proses penyebarannya terhadap cara menggaet aktor-aktor lainnya.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang di jabarkan di atas, penulis akan menarik sebuah rumusan masalah yang akan di teliti lebih lanjut, yaitu:

- a. Bagaimana Prancis menciptakan norma baru dan mengingatkan norma umum melalui *Paris Call*?

1.3 Tujuan Penelitian

Tujuan penelitian ini untuk memberikan pengetahuan mengenai gambaran umum *Cybern norms* yang dilakukan oleh Prancis melalui *Paris Call for Trust and Security in Cyberspace*, bagaimana proses terbentuknya serta penyebarannya oleh negara Prancis. Penelitian ini memfokuskan bahwa *Paris Call for Trust and Security in Cyberspace* ini merupakan prinsip-prinsip umum yang ada di dalam dunia siber yang mempunyai cakupan aktor yang luas.

1.4 Manfaat Penelitian

Dari penelitian yang dilakukan oleh penulis melalui studi literatur, manfaat yang diberikan merupakan:

1.4.1 Manfaat Praktis

Penelitian ini diharapkan dapat memberikan pengetahuan dalam hal yang berada dalam ranah siber, khususnya dalam menjelaskan *cybernorms*.

1.4.2 Manfaat Akademis

Memberikan pengetahuan tentang kerjasama *Paris Call*, dan mencoba untuk memperkaya penelitian dalam lingkup domestik maupun global dalam pengaruh siber di dunia.

1.4.3 Manfaat Sosial

Penelitian ini diharapkan dapat memberi informasi bagi masyarakat untuk mengetahui seberapa pentingnya norma internasional, dan bagaimana proses terbentuknya dan peyengarannya terhadap aktor-aktor.

1.5 Kerangka Pemikiran

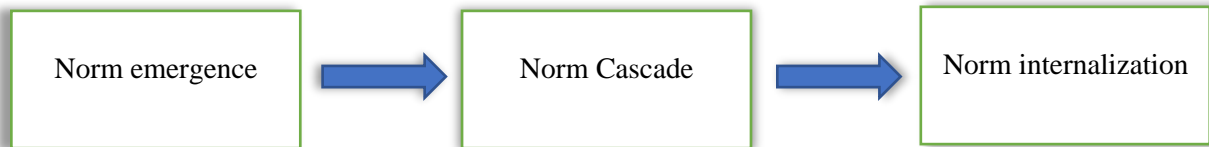
1.5.1 Konstruktivisme berbasis Norma

Konstruktivisme adalah teori yang memandang bidang hubungan internasional sebagai konstruksi sosial. Secara ontologis, konstruktivisme berbeda dengan rasionalisme yang dijelaskan melalui tiga poin. (1) *pertama*, konstruktivisme lebih bersifat idealis dibanding materialis, dimana konstruktivis memandang secara intersubjektif satu sama lain; (2) *kedua*, menempatkan pada hubungan *agents* dan *structures*, dimana sistem internasional

merupakan ranah yang konstitutif; (3) *ketiga*, kaum rasionalis berbeda dengan kaum konstruktivis dalam konsepsi mereka terhadap logika dominan yang mengatur tindakan *agents*, dimana negara-negara lebih ke arah logika kepantasan (*logic of appropriateness*) di banding logika kepatuhan (*logic of consequences*). (Bakry, 2017).

Berbeda dari realis yang menjelaskan bahwa norma sebagai suatu kepentingan, dan liberalisme yang menjelaskan bahwa norma merupakan sebuah landasan. Konstruktivisme menjelaskan tentang bagaimana suatu norma menyebar dan diadopsi negara (Rosyidin, 2020). Norma mempunyai siklus atau '*life cycle*' (Finnemore and Sikkink, 1998). Finnemore dan Sikkink telah mengembangkan gagasan norma, bagaimana norma itu muncul, disetujui, dan pengadopsian di ranah domestik yang terjadi. Perluasan konsep norma mempunyai tiga bentuk utama. Pertama, konsep munculnya norma baru yaitu *norm emergence* dari sebuah isu atau masalah yang terjadi di sebuah negara secara internasional atau domestik, kemunculan norma berasal dari *norm entrepreneur*. Lalu tahap kedua yakni *norm cascade* yaitu perdebatan tentang norma di jelaskan dalam ranah politik untuk mendapatkan persetujuan bersama. Terakhir, *norm internalization* yakni bagaimana

pengadopsian yang terjadi dalam ranah domestik di negara-negara lain.



Gambar 1.1

Sumber: Diadaptasi dari Finnemore dan Sikkink (1998)

Fokus utama penelitian penulis membahas tentang konsep munculnya sebuah norma (*norm emergence*). Para peneliti, cenderung memandang *norm emergence* sebagai hasil persuasi, tanpa karakteristik formal atau hal yang biasa terjadi. Akan tetapi, pembuatan norma ini terbuat atas beberapa dasar seperti individu, ketidakpastian, kejadian kebetulan, dan peristiwa yang menguntungkan. Pembuatan norma ini menggunakan *process-tracing* sebagai metode untuk mencari sebab akibat pembuatan norma (Kowert and Legro, 1996; Finnemore and Sikkink, 1998). Contoh pembuatan norma dapat dilihat dari Henry Dunant yang merupakan bankir di Swiss Genevese. Dunant memiliki pengalaman pribadi yang transformatif pada pertempuran Solferino pada tahun 1859 dan membantu mendirikan sebuah organisasi untuk mempromosikan tujuan ini. Organisasi ini kemudian disebut Komite Palang Merah Internasional atau *International Committee*

of the Red Cross (ICRC) melalui perjanjian internasional (Konvensi Jenewa pertama) (Finnemore and Sikkink, 1998).

<i>Stage 1 Norm Emergence</i>
<i>Actors</i> <i>Norm Entrepreneurs with Organizational Platforms</i>
<i>Motives</i> <i>Altruism, empathy, ideational commitment</i>
<i>Dominant Mechanism</i> <i>Persuasion</i>

Gambar 1.2

Sumber : Diadaptasi dari Finnemore dan Sikkink (1998)

Dalam prosesnya, ada “pembingkai” sebuah isu atau masalah dari *norm entrepreneur* (Snow *et al.*, 1986). *Norm entrepreneur* sangat penting untuk kemunculan norma karena mereka memperhatikan masalah atau bahkan "menciptakan" masalah dengan menggunakan bahasa yang menyebut, menafsirkan, dan mendramatisirnya. *Norm entrepreneur* dapat berupa individu yang mendorong perubahan normatif ke depan dan mampu meyakinkan para pembuat keputusan untuk menempatkan isu-isu atau permasalahan dalam agenda politik (Nadelmann, 1990). Beberapa peneliti juga melihat peran lainnya yang berpengaruh pada norma. Norma internasional dapat berkembang karena beresonansi dengan

audiensi domestik atau karena norma domestik dinaikkan ke tingkat internasional (Cortell and Davis, 1996; Price and Tannenwald, 1996). Atau, norma dapat dilembagakan di tingkat internasional dalam organisasi yang ada (Cortell and Davis, 1996). Penjelasan tingkat sistemik untuk pengembangan norma yang sukses juga telah disajikan. Norma dapat muncul sebagai respons terhadap sebuah masalah (Keohane, 2005). Negara hegemonik mungkin juga bisa memperkenalkan norma baru (Ikenberry and Kupchan, 1990), atau keberhasilan pembentukan norma dapat dikaitkan dengan seberapa baik hal itu menyatu dengan norma internasional yang ada (Price, 1998). Lalu identitas pelaku, kekuatan persaingan, dan kekuatan politik juga dapat membantu perkembangan norma (Florini, 1996).

Dalam menjelaskan *norm entrepreneur*, penulis menggunakan konsep '*Transnational moral entrepreneurs*' yang terlibat dalam "proselitisme moral" menurut Nadelmann. Grup ini memobilisasi opini populer dan dukungan politik baik di dalam maupun di luar negeri; mereka merangsang dan membantu pembentukan organisasi yang berpikiran sama di negara lain; dan mereka memainkan peran penting dalam meningkatkan tujuan mereka melampaui kepentingan nasional pemerintah mereka (Nadelmann, 1990).

Upaya untuk mempromosikan norma baru berlangsung dalam standar "kepantasan" yang ditentukan oleh norma sebelum-

sebelumnya. Proses ini dikenal sebagai 'logika kepantasan', di mana aktor berperilaku dengan cara tertentu karena mereka percaya bahwa perilaku ini sesuai (March and Olsen, 2009).

Untuk motivasi yang dilakukan oleh *norm entrepreneur* tentunya ada banyak, akan tetapi bagi para peneliti norma, akan sangat sulit untuk menjelaskan motivasi *norm entrepreneur* tanpa mengacu pada empati, altruisme, dan komitmen ideasional. Empati muncul ketika aktor memiliki kapasitas untuk berpartisipasi dalam perasaan atau gagasan orang lain. Empati seperti itu dapat mengarah pada saling ketergantungan empati, di mana aktor "tertarik pada kesejahteraan orang lain demi kepentingannya sendiri, bahkan jika hal ini tidak berpengaruh pada kesejahteraan atau keamanan material mereka sendiri" (Keohane, 2005). Altruisme ada ketika aktor benar-benar mengambil "tindakan yang dirancang untuk menguntungkan orang lain bahkan dengan risiko bahaya yang signifikan bagi kesejahteraan aktor itu sendiri" (Monroe, 2014). Komitmen ideasional menjadi motivasi utama ketika *entrepreneur* mengedepankan norma atau gagasan karena mereka percaya pada cita-cita dan nilai-nilai yang terkandung dalam norma, meskipun mengejar norma tersebut mungkin tidak berpengaruh pada kesejahteraan mereka. (Monroe, 2014)

Dalam mekanismenya, *norm entrepreneur* tidak melawan kepentingan aktor lain, akan tetapi mereka bertindak dengan pemahaman yang didefinisikan ulang tentang kepentingan aktor lain. Seperti halnya bagaimana Palang Merah (*Red Cross*) harus meyakinkan para pemimpin militer bahwa melindungi yang terluka sejalan dengan tujuan perang mereka (Finnemore and Sikkink, 1998).

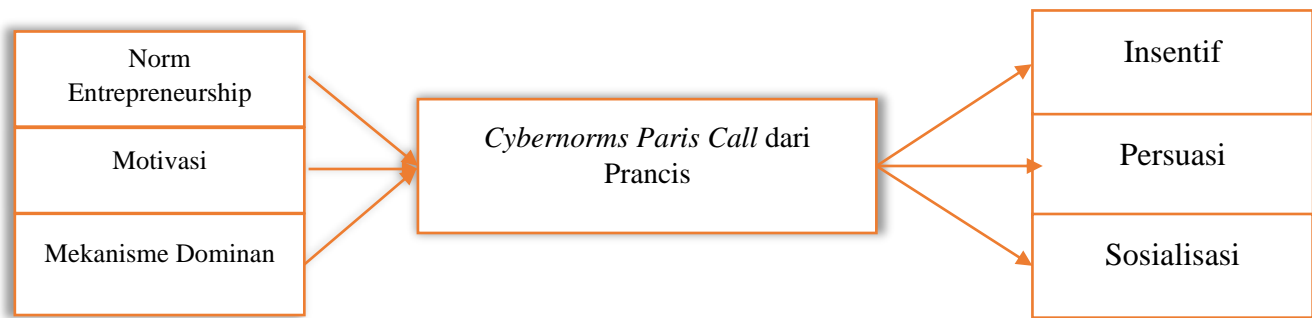
Semua *norm entrepreneur* di tingkat internasional membutuhkan semacam platform organisasi untuk mempromosikan norma mereka. Apa pun platform mereka, *norm entrepreneur* dan organisasi yang mereka tempati perlu mendapatkan dukungan dari aktor negara untuk mendukung norma mereka dan menjadikan sosialisasi norma sebagai bagian dari agenda mereka, dan platform organisasi yang berbeda menyediakan berbagai jenis alat bagi *norm entrepreneur* untuk melakukannya.

Terbentuknya sebuah norma yang sudah terjadi, norma tersebut akan di sebar, norma memiliki tiga alat strategis utama untuk membangun norma lebih lanjut: Insentif, persuasi, dan sosialisasi (Goodman and Jinks, 2014; Finnemore and Hollis, 2016). Para akademisi hukum internasional dan hubungan internasional telah mempelajari mekanisme penciptaan dan pengoperasian norma-norma internasional. Baik muncul dari kebiasaan atau dari *norm*

entrepreneur, setidaknya ada tiga alat untuk menganalisa perkembangan progresif dan penyebaran norma: (1) insentif, (2) persuasi, dan (3) sosialisasi (Goodman and Jinks, 2014; Finnemore and Hollis, 2016).

- a. Insentif, aktor yang kuat, atau lebih tepatnya negara yang kuat sering kali memiliki sumber daya yang sangat banyak untuk menyebarkan norma yang mereka sukai melalui berbagai insentif. Mereka dapat menawarkan bujukan positif.
- b. Persuasi atau pembujukan, persuasi yang berarti menyebabkan seseorang melakukan atau mempercayai sesuatu dengan bertanya, berdebat, atau memberikan alasan. Ini terutama merupakan proses kognitif dari pertukaran informasi dan argumentasi yang mengubah pikiran, pendapat, dan sikap tentang kausalitas dan efek tanpa adanya paksaan (Ratner, 2011).
- c. Sosialisasi, yaitu mengacu pada proses di mana pendatang baru dimasukkan atau diintegrasikan ke dalam pola interaksi sosial yang terorganisir (Stryker and Statham, 1977).

Sehingga penulis akan menganalisis tentang apa saja faktor dan tahapan pembuatan sebuah norma internasional yakni *Paris Call*. Penulis juga menganalisa tentang apa saja yang mendorong atau menyebarkan perkembangan *Paris Call for Trust and Security in Cyberspace* sebagai suatu norma di ranah internasional.



Gambar 1.3

Sumber: Pembuatan sistematika dari penulis.

1.6 Metode Penelitian

1.6.1 Definisi Konseptual

1.6.1.1 *Cyber* (Siber)

Cyber atau siber merupakan jaringan yang berkaitan atau melibatkan komputer atau jaringan komputer (termasuk internet) (Mirriam-Webster, 2015) yang di mana menjadi awalan yang mengacu pada teknologi berbasis elektronik dan komputer (Eriksson and Giacomello, 2007).

1.6.1.2 *Cyberspace* (Dunia Maya/Siber)

Cyberspace (dunia siber) pertama kali di ciptakan oleh William Gibson pada tahun 1980-an dalam cerita pendeknya di *Burning Chrome* (1982),

yang di definisikan sebagai “teknologi digital yang luas dan saling berhubungan” dan di populerkan di novelnya *Neuromancer* (1984).

Dalam menjelaskan pendekatan yang di lakukan negara dunia siber didefinisikan sebagai domain global dalam lingkungan informasi yang terdiri dari jaringan infrastruktur teknologi informasi yang saling tergantung, termasuk Internet, jaringan telekomunikasi, sistem komputer, dan prosesor serta pengontrol yang tertanam (US Joint Staff, 2010). Yang dapat di ambil kesimpulan bahwa bukan hanya teknologi yang saling berkaitan akan tetapi informasi, komunikasi, dan lainnya.

1.6.1.3 Cyberattack (Serangan Siber)

Cyberattacks (serangan siber), yang sebagaimana di definisikan oleh P.W Singer dan Allan Friedman (2014), “...an attack can literally move at the speed of light, unlimited by geography and the political boundaries. Being delinked from physics also means it can be in multiple places at the same time, meaning the same attack can hit multiple targets at once.” Atau bagaimana serangan yang dapat terjadi di beberapa tempat sekaligus tanpa dibatasi faktor geografis maupun politik. Bahkan definisi ini di perluas lagi yang di mana “...targets another computer and the information within it. The intended results of the attack may be to damage something physical, but that damage always first results from an incident in the digital realm.” (Singer and

Friedman, 2014) Yang menjadi fokus serangan adalah sistem komputer dan informasi-informasi yang ada didalamnya.

1.6.1.4 *Cybersecurity* (Keamanan Siber)

Cybersecurity (Keamanan Siber) berasal dalam artikel ilmuwan komputer pada tahun 1990-an dalam menggarisbawahi ketidakamanan yang terkait dengan jaringan komputer, lalu secara lambat laun melampaui konsep teknis keamanan komputer saja, di mana munculnya ancaman-ancaman dari teknologi digital yang berdampak pada efek sosial (Nissenbaum, 2005).

International Telecommunication Union (ITU) dari Perserikatan Bangsa-Bangsa (PBB) mendefinisikan keamanan siber sebagai "kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk melindungi lingkungan siber dan organisasi serta aset pengguna" (International Telecommunication Union (ITU), 2008)

1.6.1.5 *Cyberpower* (Kekuatan Siber)

Cyberpower adalah "*the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power.*" Atau penggunaan dunia siber untuk mendapatkan keuntungan dalam memberi pengaruh pada peristiwa di dalam maupun di luar dunia siber (Kuehl, 2011).

1.6.1.6 Norm Emergence

Norm Emergence merupakan konsep proses terbentuknya atau munculnya sebuah norma. Kemunculan norma ini berasal dari sebuah isu atau masalah yang di bingkai oleh *norm entrepreneur* (Finnemore and Sikkink, 1998).

1.6.1.7 Norm Entrepreneur

Norm Entrepreneur merupakan aktor yang membingkai sebuah isu atau masalah, dan mendorong sebuah pembuatan norma. *Norm Entrepreneur* dapat berupa aktor domestik maupun *transnational moral actors* (Nadelmann, 1990).

1.6.1.8 Norma

Norma adalah standar perilaku yang baik atau buruk, pantas atau tidak pantas. Norma sebagai standar perilaku yang sesuai untuk aktor dengan identitas tertentu merupakan standar untuk perilaku negara yang sesuai, Banyak norma internasional dimulai sebagai norma domestik dan menjadi internasional melalui upaya dari aktor *entrepreneur* dari berbagai jenis (Finnemore and Sikkink, 1998).

1.6.2 Definisi Operasional

1.6.2.1 Ancaman Ranah Siber

Ancaman yang mampu mengganggu ke-stabilan di dalam maupun di luar ranah siber. Ancaman ini di bingkai dan di hubungkan dengan

sektor-sektor lainnya yang membuat persepsi tentang pentingnya pembuatan sebuah norma

1.6.2.2 *Cyberspace* (Dunia siber)

Cyberspace (dunia siber) merupakan sebuah dunia yang dimana komunikasi, informasi, maupun data yang saling berhubungan satu dengan yang lainnya, yang menggunakan teknologi (termasuk internet). Ranah dunia ini juga digunakan oleh aktor-aktor negara maupun aktor non-negara dalam melakukan komunikasi ataupun diplomasi (*e-diplomacy*), dan juga memberi informasi antara aktor yang satu dengan aktor yang lainnya.

1.6.2.3 *Cyberattack* (Serangan Siber)

Serangan siber adalah serangan yang menyerang komputer maupun teknologi, yang dapat melumpuhkan sistem tersebut. Penyerangan bisa dilakukan melalui individu, kelompok, maupun sebuah negara.

Dalam praktiknya, penyerangan dilakukan oleh satu aktor saja tanpa adanya timbal balik dari aktor lainnya.

1.6.2.4 *Cyberpower* (Kekuatan Siber)

Kekuatan siber adalah kekuatan yang dipegang oleh aktor maupun non-aktor untuk mempengaruhi di dalam (intra) maupun di luar (ekstra) ranah siber. Kekuatan ini dipegang oleh aktor yang mempunyai teknologi maju.

1.6.2.5 *Cyber security* (Keamanan Siber)

Keamanan siber adalah keamanan yang berfokus pada jaringan di dalam komputer atau teknologi yang dilakukan oleh aktor untuk mencegah adanya sebuah serangan siber kepada aktor tersebut. Keamanan siber mencoba untuk menjaga informasi, data, maupun jaringan yang di punyai oleh aktor.

1.6.2.6 *Cybernorms* (Norma Siber)

Dalam pengertian penulis, norma siber merupakan sebuah seperangkat aturan yang diikuti oleh aktor sesuai dengan hal yang telah disepakati di forum terhadap regulasi di ranah atau dunia siber.

Hal ini menyangkut dengan sembilan hal yang ada di *Paris Call* seperti (1) Melindungi individu dan infrastruktur; (2) Melindungi Internet; (3) Menjaga proses pemilihan umum; (4) Menjaga *intellectual property*; (5) Non-proliferasi; (6) Keamanan siklus hidup (*lifecycle*); (7) *cyberhygiene*; (8) Tidak ada retasan kembali secara pribadi (*No private hack back*); (9) Norma Internasional. Terkhususnya poin ke sembilan dalam *Paris Call*.

1.6.2.7 Norma

Norma merupakan standar perilaku yang baik atau buruk, pantas atau tidak pantas. Norma ini menjadi sebuah pedoman untuk aktor-aktor internasional dalam berperilaku.

Penulis menggunakan pendekatan konstruktivis berbasis norma yang menjelaskan bahwa norma bukanlah alat kepentingan seperti

pandangan realis ataupun pandangan liberalis yang memandang norma sebagai sebuah landasan negara. Akan tetapi, norma juga mempengaruhi dan memberitahu negara tentang apa tujuan yang ingin dicapai.

1.6.2.8 Norma Internasional

Norma internasional merupakan produk kesepakatan antarnegara dalam forum multilateral misalnya konvensi, perjanjian, dokumen dan lainnya. Norma internasional dibuat oleh aktor internasional untuk tujuan bersama dalam hubungan internasional. Norma internasional juga dapat digunakan sebagai pedoman bagi aktor-aktor internasional dalam berperilaku.

Didalam *Paris Call*, prinsip ke-sembilan (9), norma internasional, didalamnya terkandung dua norma, yaitu norma ketahanan dan kepercayaan.

1.6.3 Tipe Penelitian

Pada penelitian ini, penulis menggunakan tipe penelitian secara eksplanatif yang bertujuan untuk menemukan suatu penjelasan dengan cara menjelaskan hubungan antara dua atau lebih gejala atau variabel. Pada penelitian ini, penulis mencoba untuk menjelaskan bagaimana Prancis membuat norma internasional yang baru dan mengingat ulang norma umum sebelumnya dengan menggunakan Teori Konstruktivisme, khususnya dalam studi keamanan.

1.6.4 Jangkauan Penelitian

Penelitian ini dimulai pada awal Januari 2020 hingga Maret 2021, yaitu menganalisis terhadap pembuatan *Paris Call* pada tahun 2018 yang lampau.

1.6.5 Teknik Pengumpulan Data

a. Data Primer

Teknik pengumpulan data yang digunakan dalam penelitian ini adalah teknik studi kepustakaan di mana informasi yang didapat berdasarkan penelaahan literatur dan referensi dari berbagai sumber.

b. Data Sekunder

Data sekunder yang diambil bersumber dari literatur-literatur yang relevan seperti artikel, jurnal internasional, surat kabar, media massa, dokumen, situs-situs website dan berbagai hal lainnya yang berhubungan dengan kasus yang diteliti.

1.6.6 Teknik Analisis Data

Penelitian ini menggunakan teknik analisis kualitatif. Metode kualitatif memungkinkan spontanitas dan adaptasi yang lebih besar dari interaksi antara peneliti dan penelitian (Mears, 2017). Penulis mencari sebuah sebab-akibat dari suatu kasus dan mengidentifikasi faktor-faktor primer dan sekunder di balik fenomena tersebut (Rosyidin, 2019).

1.6.7 Sistematika Penulisan

Penelitian ini terbagi menjadi 4 bab. Bab 1 merupakan pendahuluan yang menjadi desain sebuah penelitian ke depannya. Lalu, Bab 2 merupakan gambaran umum yang mendeskripsikan *Paris Call for Trust and security in cyberspace* dan bagaimana program tersebut di jalankan oleh Prancis.

Bab 2 juga akan mendeskripsikan tentang proses doktrin keamanan siber di Prancis dan melihat dari level domestik hingga internasional. Di dalam bab 2 ini juga akan menjelaskan tentang *Paris Call*, terutama 9 prinsip didalamnya. Penulis juga mencari data serta aktor siapa saja yang mendukung dalam pembuatan *Paris Call*. Selain itu juga menjelaskan tentang ancaman di-ranah siber saat ini yang menampilkan betapa pentingnya *Paris Call*. Penulis juga membandingkan kerjasama multilateral lainnya dengan *Paris Call*, serta apa saja keunggulan dan kekurangannya.

Bab 3 menjelaskan tentang proses pembuatan dan penyebaran dari teori konstruktivis yang berbasis norma. Penulis menggunakan teori *life cycle* oleh Finnemore dan Sikkink, dengan berfokus pada konsep *norm emergence*. Lalu menggunakan alat analisis Goodman dan Jinks dalam penjelasan penyebaran norma internasional terhadap aktor lainnya.

Bab 4 merupakan penutup yang berisi kesimpulan dan saran bagi peneliti selanjutnya. Bab ini mengemukakan hasil temuan

penelitian. Kemudian, penulis juga menyampaikan kelebihan dan kelemahan dari penelitian ini. Kelebihan dari penelitian ini diharapkan dapat memberikan pengetahuan kepada pembaca dan memberi sumbangsih bagi penelitian di bidang Hubungan Internasional, khususnya pada ranah siber. Sementara, kekurangan dari penelitian ini dapat dijadikan pembelajaran bagi penelitian selanjutnya.