# BAB I
# PENDAHULUAN

## 1.1 Latar Belakang

Di awal proses perkembangan disiplin ilmu hubungan internasional telah diasumsikan bahwa disiplin ini merupakan segala sesuatu yang berkaitan dengan cakupan seluruh relasi antar negara, seperti yang dilansir oleh Schawarzenberger yang menyatakan bahwa disiplin ilmu hubungan internasional adalah bagian asal ilmu sosiologi yang khusus mengkaji masyarakat internasional (*sociology of international relation*). Dewasa ini disiplin ilmu hubungan internasional merupakan pengetahuan yang sedang tumbuh, yakni tengah dalam proses perkembangan, akibatnya belum mencapai titik akhir dalam penggarapan disiplin ilmu itu sendiri. Meski demikian pada realita sekarang ini hubungan internasional kini telah menjadi suatu elemen kebutuhan pokok bagi suatu negara bahkan menjadi faktor penentu keberadaan dari sebuah negara.

Keberadaan suatu negara dalam panggung internasional kekinian mendesak akan adanya suatu ikatan hubungan kerjasama yang saling mendukung demi tercapainya kebutuhan antar masing - masing negara yang terlibat. Kodrat dan keberadaan dari masing – masing negara berbeda satu sama lain, ditinjau dari kepemilikan sumber daya alam, teknologi, sumber daya tenaga kerja, angkatan militer dan semacamnya. Kini ilmu hubungan internasional hadir dari landasan kebutuhan tersebut yang kini semakin berkembang dan jauh lebih kompleks dari sebelumnya.

Alat yang kemudian dipakai dalam berhubungan internasional dikenal dengan penyebutan diplomasi, yakni bentuk aktivitas yang memediasi antara aktor – aktor hubungan internasional. Diplomasi merupakan suatu alat yang membawa kepentingan negara dalam level tertentu. Dari diplomasi tersebut, sebuah negara akan menghasilkan keputusan kerja sama antar negara untuk menyelesaikan konflik yang terjadi. Diplomasi adalah tindakan damai dalam hubungan antar negara.

Dengan kata lain, itu adalah seni melakukan Hubungan Internasional (Kodaman & Akçay, 2010).

Selama dua dekade terakhir, kemajuan pesat dalam komputer, perangkat lunak, komunikasi, dan teknologi penginderaan telah menghubungkan miliaran individu di seluruh dunia, ekonomi terintegrasi melalui rantai pasokan yang terhubung, dan mendorong efisiensi baru melalui *Internet of Things* (Lete, 2021). Merebaknya pandemi virus corona telah mempercepat transformasi digital ini. Namun kemajuan ini juga membawa tantangan, termasuk ketergantungan hampir mutlak semua negara maju dan banyak negara berkembang pada integritas jaringan dan sistem digital. Terlepas dari ketahanan umum sistem berbasis jaringan, integrasi digital yang mendalam juga telah menciptakan kerentanan terhadap serangan *cyber* oleh peretas individu, kejahatan terorganisir, kelompok teroris, dan bahkan negara.

Dimulai dengan serangan *denial-of-service* Rusia terhadap pemerintah Estonia dan sistem keuangan pada tahun 2007, mereka menjadi lebih banyak dan lebih merusak. Misalnya, serangan *ransomware Wanna Cry* pada 2017 memengaruhi ratusan ribu komputer di 150 negara. Peretasan *SolarWinds* 2020 yang menargetkan lembaga pemerintah dan perusahaan swasta dianggap sebagai salah satu serangan *cyber* terbesar dalam sejarah Amerika Serikat. Dengan satu perkiraan, dunia mengalami 43 insiden *cyber* yang signifikan pada kuartal terakhir tahun 2020. Kekhawatiran tentang keamanan *cyber* telah meroket. Meningkatnya perpecahan Internet di sepanjang batas geografis dan komersial, dan kurangnya konsensus internasional tentang norma-norma dunia maya memudahkan pemerintah untuk terlibat dalam operasi digital yang berbahaya. Menetapkan aturan main di dunia maya karena itu lebih penting dari sebelumnya (Lete, 2021).

Secara alami, dunia maya terdesentralisasi dan sebagian besar tidak diatur. Andre Barrinha dan Thomas Renard telah membandingkannya dengan “laut lepas, wilayah udara, dan luar angkasa.” Diplomasi adalah inti dari penggunaan “kesamaan global”, termasuk dunia maya. Tindakan di dunia maya, termasuk

serangan dunia maya, sering kali bersifat transnasional dan dengan demikian dapat mengamanatkan tanggapan transnasional. Untuk merespon terhadap "serangan *cyber* lintas negara", misalnya, negara harus bekerja sama dalam "berbagi informasi, pengumpulan bukti, dan penuntutan pidana" terhadap pelaku serangan. Memang tidak ada negara bagian dapat melindungi dirinya sendiri dari ancaman dunia maya (Khabbaz, 2020).

Seiring dengan meningkatnya ketergantungan pada internet dan teknologi komputer, kepentingan negara semakin meningkat menyatu dengan ranah dunia maya. Internet dan teknologi jaringan telah memungkinkan kemajuan sosial dan ekonomi yang menakjubkan di seluruh dunia. Ketika teknologi baru datang online dan lebih banyak orang terhubung di seluruh dunia, manfaat potensial dari dunia maya tampaknya tidak terbatas. Pengintaian dunia maya, serangan dunia maya, peretasan, sensor internet, dan bahkan masalah teknis seperti netralitas internet sekarang menjadi berita utama secara teratur. *Cyberspace* telah menjadi ruang politik yang diperebutkan, dibentuk oleh kepentingan, norma, dan nilai yang berbeda. Diplomasi *cyber* dapat berfungsi sebagai alat penting di mana negara-negara dapat bekerja sama untuk menetapkan norma *cyber* dan menanggapi ancaman dan kerentanan *cyber*. Namun, untuk memanfaatkan sepenuhnya alat ini, negara harus merangkul diplomasi dunia maya, mengintegrasikannya ke dalam struktur birokrasi mereka, dan berupaya mengatasi tantangan baru yang ditimbulkannya.

Diplomasi *cyber* adalah diplomasi "untuk mengamankan kepentingan nasional terkait dengan dunia maya." Sebagai praktik, diplomasi *cyber* adalah respons alami terhadap relevansi dunia *cyber* yang semakin meningkat secara global. Melalui diplomasi *cyber*, negara-negara berkolaborasi untuk menanggapi dan menangani dimensi *cyber* dari konflik internasional, kejahatan, dan keamanan informasi (Khabbaz, 2020).

Barrinha dan Renard mencatat isu-isu dominan dalam agenda diplomasi *cyber* diantaranya keamanan *cyber* (*cyber security*), kejahatan *cyber* (*cybercrime*),

pembangunan kepercayaan (*confidencebuilding*), kebebasan internet (*internet freedom*), dan tata kelola internet (*internet governance*). Oleh karena itu, menurut mereka, diplomasi *cyber* dilakukan sebagian atau sepenuhnya oleh diplomat, yang bertemu dalam format bilateral (seperti dialog Amerika Serikat - China) atau dalam forum multilateral (seperti di PBB) (Barrinha & Renard, 2017).

*Cyberspace* (Ruang *Cyber*) memberikan peluang besar untuk inovasi, kemajuan ekonomi, pengembangan budaya, dan akses ke informasi. Sementara perkembangannya yang cepat terbukti sangat berguna untuk banyak aktivitas manusia, namun juga membawa ancaman baru. Praktik baru dan berbahaya berkembang di dunia maya: kejahatan dunia maya, manipulasi informasi, spionase politik atau ekonomi, serangan terhadap infrastruktur atau individu penting, pencurian informasi pribadi atau data rahasia, kompromi sistem informasi dan komunikasi yang digunakan oleh warga, perusahaan, dan lembaga. Serangan ini dapat berasal dari kelompok Negara atau non-Negara yang tidak menghormati batas. Serangan-serangan ini menjadi semakin canggih dan intens. Oleh karena itu, penting untuk menyatukan komunitas internasional untuk memastikan perdamaian dan keamanan di ruang digital.

Di saat teknologi modern memberikan banyak kemudahan dan manfaat, ada saja oknum yang menyalahgunakannya sehingga dapat mengancam privasi kita. Kejahatan dunia maya seringkali memiliki dampak yang luar biasa pada perusahaan dan individu. Diperkirakan biaya kejahatan dunia maya dapat mencapai $10,5 triliun pada tahun 2025 (Carter, 2021).

Kejahatan *cyber* terjadi bermula dari kegiatan hacking yang telah ada lebih dari satu abad. Pada tahun 1870-an, beberapa remaja telah merusak sistem telepon baru negara dengan merubah otoritas. Awal 1960 Fasilitas universitas dengan kerangka utama komputer yang besar, seperti laboratorium kepintaran buatan (*artificial intelligence*) MIT, menjadi tahap percobaan bagi para *hacker*. Pada awalnya, kata "*hacker*" berarti positif untuk seorang yang menguasai komputer

yang dapat membuat sebuah program melebihi apa yang dirancang untuk melakukan tugasnya (Sujana, 2018).

Pada tahun 1970 di Amerika Serikat terjadi kasus manipulasi data nilai akademik mahasiswa di *Brooklyn College* New York, kasus penyalahgunaan komputer perusahaan untuk kepentingan karyawan, kasus pengkopian data untuk sarana kejahatan penyelundupan narkotika, kasus penipuan melalui kartu kredit. Selain itu, terjadi pula kasus akses tidak sah terhadap Database *Security Pacific National Bank* yang mengakibatkan kerugian sebesar $10.2 juta US pada tahun 1978. Selanjutnya kejahatan serupa terjadi pula disejumlah negara antara lain Jerman, Australia, Inggris, Finlandia, Swedia, Austria, Jepang, Swiss, Kanada, Belanda dan Indonesia. Kejahatan tersebut menyerang terhadap harta kekayaan, kehormatan, sistem dan jaringan komputer (Sumarwani, 2014).

Awal 1980 Pengarang William Gibson memasukkan istilah "*cyberspace*" dalam sebuah novel fiksi ilmiah yang disebut *Neuromancer*. Dalam satu penangkapan pertama dari para hacker, FBI menggerebek markas 414 di Milwaukee (dinamakan sesuai kode area lokal) setelah para anggotanya meyebabkan pembobolan 60 komputer berjarak dari Memorial Sloan-Kettering Cancer Center ke Los Alamos *National Laboratory*. *Comprehensive Crime Control Act* memberikan yuridiksi *Secret Service* lewat kartu kredit dan penipuan komputer. Dua bentuk kelompok *hacker*, *the Legion of Doom* di Amerika Serikat dan *the Chaos Computer Club* di Jerman (Nahak, 2017).

Salah satu ancaman *cyber* paling awal dan terbesar dimulai oleh *Melissa Virus*. Pada tahun 1999, *Melissa Virus* diluncurkan oleh programmer David Lee Smith dengan mengirimkan file kepada pengguna untuk dibuka oleh *Microsoft Word*. Virus ini menyebabkan kerusakan parah pada ratusan perusahaan, termasuk *Microsoft*. Diperkirakan bahwa perbaikan sistem yang terkena biaya sekitar $80 juta. Di tahun yang sama, James Jonathan yang berusia 15 tahun mampu meretas dan mematikan komputer NASA selama 21 hari. Sekitar 1,7 juta perangkat lunak diunduh selama serangan itu, yang menelan biaya perbaikan sekitar $ 41.000. Pada

bulan April 2007, di negara bagian Eropa tepatnya di Estonia menyaksikan apa yang dianggap sebagai serangan dunia maya pertama di seluruh wilayah, di mana sekitar 58 situs web Estonia offline, termasuk situs web pemerintah, bank, dan media (Carter, 2021).

Pada tahun 2015, sebanyak 19.000 situs web Perancis diretas simpatisan ISIS sejak tragedi Charlie Hebdo pada 7 Januari 2015. Kepala Pertahanan *Cyber* untuk militer Perancis, Adm. Arnaud Coustilliere mengatakan bahwa 19 ribu situs di Perancis telah mengalami serangan *cyber* dalam beberapa hari terakhir. Serangan *cyber* ini dipicu oleh aksi penembakan kantor majalah Charlie Hebdon yang menewaskan belasan orang. Insiden ini disebabkan karena majalah Charlie Hebdon yang kerap membuat kartun Nabi Muhammad. Sebagai pembalasan aksi penembakan ini, sekelompok peretas Anonymous mengatakan bahwa mereka telah menyerang situs web yang menyediakan informasi jihad. Kelompok ini mempublikasi video dan mengatakan bahwa mereka akan merusak situs dan media sosial yang berkaitan dengan aksi terorisme ini (Pratomo, 2015). Menurut Coustilliere, tingkat cakupan dan bentuk serangan dunia maya itu sangat besar dan belum pernah terjadi sebelumnya. Sejumlah situs kalangan bisnis, kelompok agama, perguruan tinggi diretas dengan mengganti tampilannya dan diisi dengan pesan-pesan bernuansa Islam (Oktaveri, 2015).

Coustilliere menambahkan bahwa sebagian besar serangan dilakukan dengan menggunakan teknik *DDoS* dengan membanjiri lalu lintas data. Serangan ini dapat melumpuhkan sistem jaringan pada server target dan menyebabkan kerusakan yang sangat serius. Menurut *Arbor Networks,* perusahaan yang memitoring ancaman internet, dalam waktu 24 jam tercatat sebanyak 1.070 serangan DDoS mengarah pada situs yang berbasis di Perancis. Jumlah ini merupakan seperempat lebih banyak dari jumlah serangan pada Amerika Serikat (Rio, 2015).

Coustilliere menganggap bahwa serangan ini merupakan balasan dari aksi anti-terorisme besar-besaran yang menarik 3,7 juta orang ke jalanan pada hari

Minggu lalu di Perancis. Ia juga menilai kelompok peretas yang melakukan aksi ini memiliki jaringan, organisasi dan pola kerja yang terstruktur. Setelah serangan terhadap kantor majalah Charlie Hebdo di Paris awal tahun ini, sekelompok hacker yang mengaku sebagai pejuang militan membajak ratusan laman situs di Perancis dan menyebarkan propaganda (Asmardika, 2015).

Pada tahun yang sama, serangan *cyber* memotong transmisi dari 11 saluran milik jaringan TV Perancis TV5 MONDE, jaringan televisi Perancis TV5 MONDE mengatakan jika saluran televisi tersebut telah diretas oleh seorang yang mengaku sebagai anggota kelompok yang menamakan dirinya *Cyber Khilafah* yang terkait Negara Islam Irak dan Suriah (ISIS). Ia mengaku telah membajak bukan hanya saluran televisi, tapi juga situs dan halaman *Facebook* stasiun televisi tersebut (Nursalikah, 2017).

Serangan tersebut dimulai pada pukul 10.00 malam waktu setempat, tetapi lembaga penyiar global berbahasa Perancis tersebut tampaknya kembali memiliki kontrol pada halaman *Facebook*-nya saat tengah malam. Tetapi jaringan stasiun televisi masih berada di bawah kendali peretas. Dalam serangan dan terornya, para pembajak (*hacker*) mengunggah dokumen-dokumen pada halaman *Facebook* TV5 MONDE, yang berisikan kartu identitas dan CV (*Curriculum Vitae*) dari kerabat tentara-tentara Perancis yang terlibat dalam operasi anti-ISIS. Posting-an itu juga menuduh Presiden Perancis Francois Hollande telah melakukan kesalahan tak termaafkan dengan terlibat dalam perang yang tidak memiliki tujuan apa pun. Perancis adalah bagian dari koalisi militer pimpinan AS yang melakukan serangan udara terhadap ISIS di Irak dan Suriah. "Khalifah *Cyber* akan terus melakukan upaya '*Jihad Cyber*' terhadap musuh-musuh ISIS," bunyi pesan yang di-posting oleh *hacker* di akun Facebook TV5 MONDE (Silaban, 2015).

Selama 2017 dunia dihebohkan dengan serangan virus *ransomware*. Tepatnya sekitar bulan Mei. Serangan global itu melumpuhkan berbagai perangkat dan jaringan komputer di berbagai negara di dunia. Di antaranya mengganggu produksi pabrik mobil Perancis, Renault, mengusik sistem Bank Sentral Rusia, serta

mengacaukan sistem jaminan kesehatan nasional Inggris. *WannaCry* atau *Wanna Decryptor* (WCRY) itu terdeteksi sebagai Win32/Filecoder.WannaCryptor.D trojan. Bila dibandingkan dengan ransomware lain, *WannaCry* punya keunikan, yakni memilih memanfaatkan eksploitasi Windows yang diperoleh melalui eksploit NSA (*National Security Agent*) yang disebut *EternalBlue* yang sempat digunakan oleh kelompok *Shadow Broker*. Proses penyebaran masif disebabkan juga agresifitas *ransomware* yang terus bekerja secara terstruktur, misal, apabila salah satu komputer perusahaan terinfeksi oleh *WannaCry*, *Worm* pada ransomware akan mencari sendiri komputer yang rentan untuk diinfeksi, sehingga dalam waktu singkat *WannaCry* bisa meruntuhkan sebuah sistem atau jaringan dalam perusahaan (Kertopati, 2017).

Dikutip dari CNN Indonesia, badan kerja sama polisi Uni Eropa, Europol, menyebut serangan *cyber ransomware WannaCry* telah memakan lebih dari 200 ribu korban setidaknya di 150 negara. Perangkat lunak jahat ini telah melumpuhkan ratusan ribu jaringan komputer instansi perusahaan maupun pemerintah secara global. Kepala Badan Kepolisian Uni Eropa (Europol) Rob Wainwright mengatakan jumlah terakhir ada lebih dari 200 ribu korban di setidaknya 150 negara. Banyak dari para korban merupakan pelaku bisnis, termasuk perusahaan besar. *Ransomware WannaCry* merupakan salah satu program jahat yang bisa mengunci data pada komputer terinfeksi dan jaringan terhubung hanya dalam hitungan menit. *Malware* ini disebut sebagai salah satu yang paling canggih dan mulai terdeteksi menyebar secara global sejak 11 Mei 2017. Sejauh ini, belum ada penangkal untuk mendekripsi file yang terjangkit. Pelaku meminta pengguna membayar sebesar US$300 dolar dalam bentuk Bitcoin virtual sebagai tebusan agar dokumen yang disandera atau dikunci bisa dibuka kembali.

Salah satu korban terparah adalah Inggris. Sedikitnya 45 fasilitas kesehatan nasional (NHS) terinfeksi, membuat sejumlah rumah sakit harus membatalkan operasi dan program perawatan pasien. Wainwright mengatakan sejumlah bank di Eropa pun telah terinfeksi. karena itu, lembaganya bersama Biro Investigasi Federal (FBI) bergegas melacak pihak yang bertanggung jawab atas serangan *cyber* masif

yang dianggap belum pernah terjadi sebelumnya ini. Berdasarkan penyelidikan awal, pelaku serangan malware ini diperkirakan berjumlah lebih dari satu orang. Walaupun begitu, dia menuturkan, motivasi pelaku di balik serangan ini masih belum diketahui, meski pada umumnya serangan *cyber* berkedok tebusan biasanya "bersifat kriminal." Wainwright bahkan mengatakan sejumlah korban telah membayar tebusan yang diminta si pelaku agar bisa mendapatkan kembali dokumen yang diblokir (Suastha, 2017).

Presiden Perancis Emmanuel Macron pada November 2018 menyerukan agar semua pelaku dunia maya bersatu untuk menghadapi ancaman digital yang membahayakan warga dan infrastruktur. *Paris Call for Trust and Security in Cyberspace* adalah deklarasi tingkat tinggi yang mendukung pengembangan prinsip-prinsip umum untuk mengamankan dunia maya dan prinsip-prinsip kunci terkait: kepraktisan hukum internasional, perilaku yang bertanggung jawab dari aktor Negara, tanggung jawab khusus pemangku kepentingan swasta, terutama dalam hal mencegah kegagalan keamanan dan mencegah penggunaan praktik-praktik tertentu yang dapat mengganggu stabilitas dunia maya. *Paris Call* mengajak semua pelaku dunia maya untuk bekerja sama dan mendorong negara-negara untuk bekerja sama dengan mitra sektor swasta, akademisi, dan masyarakat sipil. Lebih dari 1.200 pendukung *Paris Call* (81 negara bagian, lebih dari 706 perusahaan, 390 organisasi masyarakat sipil) berkomitmen untuk bekerja sama untuk mengadopsi perilaku yang bertanggung jawab dan menerapkan di dunia maya prinsip-prinsip dasar yang berlaku di dunia fisik. *Paris Call* menegaskan kesediaan untuk bekerja sama, dalam forum yang ada dan melalui organisasi, lembaga, mekanisme, dan proses terkait untuk saling membantu dan menerapkan langkah-langkah kerja sama. Ada sembilan prinsip dalam *Paris Call*, yaitu: (1) Melindungi individu dan infrastruktur; (2) Lindungi internet; (3) Mempertahankan proses pemilu; (4) Mempertahankan kekayaan intelektual; (5) Nonproliferasi perangkat lunak dan praktik berbahaya; (6) Keamanan siklus hidup; (7) Kebersihan dunia maya; (8) Tidak ada peretasan pribadi; (9) Norma Internasional (*Paris Call*, 2018).

Mengingat hal ini, *Paris Call* merupakan upaya besar untuk menciptakan struktur multi-stakeholder yang menarik bagi aktor negara dan non negara, berusaha untuk melengkapi negosiasi antar pemerintah dan inisiatif serupa. *Paris Call* telah mendapat dukungan luas dan mungkin sampai saat ini merupakan alat terbaik yang tersedia untuk berbagai aktor untuk berinteraksi dalam tata kelola dunia maya dan untuk menerapkan norma-norma perilaku.

### 1.2 Rumusan Masalah

Dari uraian yang telah dijelaskan diatas maka rumusan masalah dalam penelitian ini adalah sebagai berikut "Bagaimana dampak *Paris Call* sebagai instrument diplomasi *cyber* bagi kerja sama dan upaya pencegahan serangan *cyber* negara Perancis?"

### 1.3 Tujuan Penelitian

Menjelaskan mengenai dampak *Paris Call* sebagai instrument diplomasi *cyber* bagi kerja sama dan upaya pencegahan serangan *cyber* negara Perancis.

### 1.4 Studi Pustaka

Untuk menjawab pertanyaan mengenai "Dampak *Paris Call* sebagai instrument diplomasi *cyber* bagi negara Perancis?" maka penulis melakukan studi pustaka terkait penelitian-penelitian sebelumnya yang membahas mengenai diplomasi *cyber* dan *Paris Call*. Penulis sedikitnya menemukan beberapa jurnal terkait, adapun tinjauan pustaka sebagai berikut:

Pertama, jurnal berjudul *Cyber Diplomacy: Menuju Masyarakat Internasional Yang Damai Di Era Digital* oleh Iskandar Hamonangan dan Zainab Assegaff (Hamonangan & Assegaff, 2020). Penelitian ini membahas mengenai diplomasi *cyber* (*cyber diplomacy*) dan apa yang bisa dijanjikannya untuk menuju masyarakat internasional yang damai di era digital. Penulis dalam penelitian ini berpendapat perlunya dilakukan diplomasi *cyber* untuk menyelaraskan kepentingan negara-negara dan agar tidak terjadi perang *cyber* yang terbuka. Diplomasi *cyber* adalah implementasi internasional yang muncul atas upaya untuk membentuk

masyarakat *cyber* internasional, dengan menjembatani antara kepentingan nasional negara dan dinamika masyarakat dunia. Oleh karena itu, tujuan dari diplomasi *cyber* adalah untuk mengisi fungsi-fungsi tradisional diplomasi, seperti melindungi perdamaian serta membentuk rasa saling percaya di antara para pemangku kepentingan, di ruang *cyber*.

Diplomasi harus berperan sebagai alat komunikasi internasional untuk membangun norma bersama dan sebagai upaya mengelola politik internasional yang bertujuan untuk meminimalkan gesekan dalam hubungan internasional agar terciptanya perdamaian dalam masyarakat internasional. Jika dikaitkan dengan diplomasi dalam ruang *cyber*, diplomasi *cyber* harus berperan menjadi alat komunikasi internasional untuk membentuk norma *cyber* bersama dan cara untuk mengelola ruang *cyber* yang bertujuan untuk meminimalkan gesekan di ruang *cyber*. Upaya untuk membentuk norma *cyber* bersama sudah digagas oleh berbagai negara, organisasi internasional, dan perusahaan teknologi swasta, diantaranya adalah NATO Talinn Manual, *Microsoft Norms Paper*, *Code of Conduct*–yang digagas oleh China, Rusia serta negara lainnya–*US Government Policy*, dan *United Nations group of Governmental Expert on Information Security* (UN GGE). Selain pembangunan norma, upaya untuk meminimalkan gesekan pada ruang *cyber* dapat dilakukan menggunakan kebijakan ruang *cyber* internasional.

Kedua, dalam jurnal yang berjudul *Cyber Diplomacy: The Making of an International Society in the digital age* oleh Andre Barrinha dan Thomas Renard (Barrinha & Renard, 2017). Jurnal ini mengusulkan untuk mengeksplorasi konsep diplomasi *cyber*, dengan menganalisis evolusinya dan menghubungkannya dengan diskusi yang lebih luas tentang diplomasi sebagai institusi fundamental masyarakat internasional, seperti yang didefinisikan oleh *English School of International Relations*. Penulis berpendapat bahwa *cyber*-diplomasi adalah praktik internasional yang muncul yang mencoba untuk membangun masyarakat internasional *cyber*, menjembatani kepentingan nasional negara-negara dengan dinamika masyarakat dunia – ranah utama di mana dunia maya telah berkembang dalam empat dekade terakhir.

Kegiatan dunia maya sebagian besar telah dilakukan mengikuti alasan masyarakat dunia yang paling baik ditangkap oleh apa yang disebut model multi-stakeholder yang mengatur internet, meskipun negara-negara sekarang mencoba untuk menerima pentingnya bidang tersebut dengan memasukkannya ke dalam ranah masyarakat internasional. Semua ini, tanpa mengecualikan sistem internasional realis, ruang di mana negara-negara hidup berdampingan dan berinteraksi tanpa memperhatikan nilai atau norma bersama. Padahal kasus seperti peretasan Komite Nasional Demokrat Juli 2016 bukti bahwa aktivitas negara di dunia maya masih sangat ditentukan oleh pertimbangan-pertimbangan strategis (bukan normatif) (ranah sistem internasional), maka diplomasi *cyber* bertujuan untuk secara progresif menggeser perilaku dan sikap tersebut ke arah ruang kerjasama yang damai. keberadaan, ditentukan oleh aturan dan prinsip yang jelas: dari sistem unit interaktif ke masyarakat negara. Dalam hal itu, diplomasi *cyber* bagi dunia maya sama dengan diplomasi bagi Hubungan Internasional adalah pilar fundamental masyarakat internasional.

Jurnal ketiga, berjudul *Cyber Diplomacy: Benefits, Developments, and Challenges oleh Dana Khabbaz* (Khabbaz, 2020). Jurnal ini dimulai dengan memberikan gambaran tentang diplomasi *cyber* dan menyoroti kebutuhan penggunaannya. Kemudian, makalah ini menguraikan upaya utama diplomasi *cyber* internasional. Sebagai praktik, diplomasi *cyber* adalah respons alami terhadap relevansi dunia *cyber* yang semakin meningkat secara global. Melalui diplomasi *cyber*, negara-negara berkolaborasi untuk menanggapi dan menangani dimensi *cyber* dari konflik internasional, kejahatan, dan keamanan informasi. Diplomasi *cyber* tidak hanya penting untuk tanggapan internasional yang efektif terhadap ancaman *cyber*, tetapi negara-negara juga perlu terlibat dalam diplomasi untuk mengembangkan norma-norma yang kemudian mengatur kolaborasi internasional ini. Karena penggunaan dan relevansi dunia maya terus berkembang, negara menghadapi kekurangan standar yang ditetapkan yang mengatur interaksi dan tanggapan dunia maya terhadap peristiwa terkait *cyber*. Dalam pengertian ini, hukum dunia maya berbeda secara substansial dari, misalnya, undang-undang

berusia berabad-abad yang mengatur laut lepas. Sementara beberapa norma sudah ada di dunia maya, penciptaan norma dunia maya sedang berlangsung, dan diplomasi internasional dapat menjadi penting dalammembentuk proses. Terakhir, diplomasi *cyber* bukan hanya kebutuhan tetapi juga peluang. *Cyberspace* menyediakan tempat lain untuk keterkaitan global. Diplomasi *cyber* dapat bersinggungan dengan diplomasi mata pelajaran lain dan berimplikasi pada isu-isu penting global lainnya, seperti:hak asasi manusia internasional, kesehatan masyarakat, dan perubahan iklim.

Jurnal ini selanjutnya merangkum perkembangan Amerika Serikat baru-baru ini. Di sini, Amerika Serikat berfungsi sebagai studi kasus perubahan diplomasi *cyber* internal satu negara. Amerika Serikat memiliki pengaruh yang cukup besar pada hukum internasional dan kadang-kadang mendukung diplomasi dunia maya. Pada saat yang sama, Amerika Serikat kadang-kadang menjadi penghambat kemajuan diplomasi *cyber* dan telah berjuang untuk mengintegrasikan diplomasi *cyber* ke dalam kebijakan luar negerinya. Setelah diskusi tentang perkembangan Amerika Serikat, jurnal ini diakhiri dengan mengidentifikasi tujuh tantangan utama diplomasi *cyber*, banyak di antaranya bersinggungan dengan hukum, kebijakan, politik, dan teknologi. Tantangan-tantangan tersebut meliputi (1) keengganan beberapa negara untuk berpartisipasi dalam diplomasi *cyber*; (2) isu atribusi di dunia maya; (3) pesatnya perkembangan diplomasi *cyber*; (4) perpecahan politik antar negara bagian; (5) kesenjangan dalam kapasitas teknologi negara bagian; (6) tumpang tindih diplomasi *cyber* dengan bidang lain; dan (7) sulitnya menjaga kepentingan *cyber* aktor non-negara.

Jurnal keempat, Berjudul *Diplomacy in Change and Transformastion : Cyber Diplomacy* oleh Betul Catal (Çatal, 2015). Dengan pemanfaatan internet sebagai alat komunikasi, masyarakat dapat mengakses informasi dengan cepat, pesatnya penyebaran informasi yang tak terbendung tentu saja membawa dampak positif. Selain sebagai alat komunikasi, internet juga digunakan sebagai layanan infrastruktur. Institusi yang terhubung ke Internet mempercepat komunikasi dengan menghubungkan satu sama lain melalui komputer dan dapat melakukan banyak

transaksi yang memberatkan dalam waktu singkat. Di era pra-internet, transaksi yang dilakukan dengan susah payah dilakukan dengan cara yang sangat sederhana dan cepat. Diplomasi yang merupakan alat pelaksana politik luar negeri telah mengalami perubahan besar sejak dahulu hingga saat ini. Dalam konteks ini, perubahan dalam bidang komunikasi dengan globalisasi, Hal tersebut berdampak signifikan dalam bidang diplomasi dan memunculkan konsep baru yang disebut diplomasi *cyber*. Dalam penelitian ini, konsep diplomasi *cyber*, perbedaannya dengan diplomasi tradisional dan kontribusinya terhadap diplomasi akan dicoba dijelaskan.

Diplomasi *cyber* atau diplomasi generasi baru, atau dengan kata lain diplomasi digital, telah meningkatkan kecepatan penyebaran informasi di seluruh dunia. Ini telah mempengaruhi negara dan struktur sosial kita secara dekat dalam waktu dekat, dan di jauh akan terus mempengaruhi. Ekonomi dan teknologi, pendidikan dan diplomasi budaya akan sangat efektif dalam komunikasi antar negara dan perang kepentingan. Implementasi strategi operasi persepsi yang terkait dengan negara kita seharusnya tidak hanya menjadi tugas publik. Jika akan ada perjuangan untuk hak dan keberadaan total untuk negara kita; dinamika yang dominan ini seharusnya adalah universitas, LSM, media, pers, sinema dan penulis serta generasi baru yang dilengkapi dengan teknologi. Teknologi *cyber* harus merambah ke seluruh negeri kita. Jika tidak, selalu ada risiko menghadapi kerusakan dan sanksi yang tidak dapat diperbaiki. Ketika langkah-langkah dan strategi tersebut di atas diterapkan, kita dapat melanjutkan keberadaan kita sebagai individu terhormat dari suatu negara dengan persepsi positif di seluruh dunia.

Kelima, jurnal berjudul *International Cybersecurity Norms and Responsible Cyber Sovereigty* oleh Tuba Eldem (Eldem, 2021). Jurnal ini bertujuan untuk menjelaskan munculnya norma-norma keamanan *cyber* internasional dengan berfokus pada negosiasi yang diadakan di Komite Pertama Perserikatan Bangsa-Bangsa selama lebih dari dua puluh tahun. Penulis berpendapat bahwa negosiasi yang diadakan di bawah Komite Pertama yang menangani perlucutan senjata dan masalah keamanan internasional menunjukkan tahap pertama pembentukan aturan

internasional terkait dengan dunia maya, dan negosiasi yang akan diselesaikan di bawah Kelompok Kerja Terbuka PBB (OEWG) pada tahun 2021 sangat penting untuk transisi norma-norma keamanan *cyber* internasional dari tahap pertama ke tahap kedua.

Awalnya dibayangkan sebagai ruang komunikasi yang bebas dan terbuka antara orang-orang, bebas dari regulasi dan intervensi negara, dunia maya telah menjadi subjek fundamental politik nasional dan global selama dekade terakhir. Diduga operasi *cyber* yang disponsori negara terhadap Estonia pada 2007, Georgia pada 2008 dan Iran pada 2010 memainkan peran penting dalam mengubah keamanan *cyber* menjadi masalah keamanan nasional dan internasional. Meskipun perkembangan diplomasi *cyber* dan hukum keamanan *cyber* internasional tertinggal dari militerisasi dunia *cyber*, namun demikian, ada banyak inisiatif internasional untuk mengadopsi norma-norma keamanan *cyber* internasional dalam satu dekade terakhir. Dalam hal kesesuaian negara dengan norma, pengakuan umum atas norma lebih penting daripada validitas resmi. Mengingat keefektifan norma berubah tergantung pada bagaimana dan di mana norma tersebut diterima, dengan aktor mana berinteraksi di mana dan seberapa sering mereka berinteraksi secara internasional, dapat dikatakan bahwa dengan struktur multi-stakeholdernya yang luas, Kelompok Kerja Terbuka PBB pada tahun 2021 berpotensi untuk meningkatkan efektivitas dengan meningkatkan pengakuan sosial dan legitimasi norma-norma ini. Oleh karena itu, negosiasi yang sedang berlangsung di Kelompok Kerja Terbuka akan memungkinkan lebih banyak negara untuk berpartisipasi dalam konseptualisasi norma-norma dunia maya dan bagaimana mereka akan diimplementasikan, sehingga memastikan bahwa mereka adalah bagian dari proses tersebut. Hanya keyakinan bahwa negara-negara berada dalam kepentingan norma-norma ini akan mendorong mereka untuk mengalokasikan sumber daya yang diperlukan untuk menegakkan norma-norma, berbagi pengalaman mereka, dan meminta pertanggung jawaban satu sama lain.

Jurnal keeman, berjudul *Cyber Diplomacy : A Systematic Literature Review* oleh Amel Attatfa, Karen Renaud dan Stefano De Paoli (Attatfa et al., 2020).

Penulis dalam jurnal ini mengeksplorasi dimensi diplomasi dunia maya yang dibuktikan oleh penelitian dan literatur. Tindakan diplomatik dalam hubungan internasional menjadi prioritas karena keamanan negara menjadi taruhannya. Jelas bahwa keamanan ini sangat terkait dengan dunia maya dan kebutuhan untuk melindungi infrastruktur penting, dan populasi yang lebih luas, dari dampak serangan dunia maya negara-bangsa. Hal ini menimbulkan pertanyaan tentang sejauh mana dan jangkauan diplomasi *cyber*, yang dianggap sebagai instrumen penting dalam hubungan internasional, dan pengaruhnya dalam mempertemukan aktor yang berbeda dan beragam.

*Paris Call for Cyber Peace* adalah prakarsa dunia maya yang diluncurkan oleh Perancis, dalam pidato yang disampaikan oleh Presiden Perancis Emmanuel Macron. Panggilan tersebut diadakan di Internet of Trust pada 12 November 2018 di UNESCO, di Paris, di hadapan Sekretaris Jenderal PBB Antonio Guterres. Ini mengikuti inisiatif Group of Governmental Experts (GGE) pada tahun 2017, setelah gagal karena kurangnya konsensus. Inisiatif kunci diplomasi *cyber* ini dikemas dalam *Paris Call*, sebuah upaya diplomatik Perancis, yang menempatkan Perancis di garis depan (mendukung penggunaan kekuatan lembut, atau kekuasaan dengan kooptasi, sebuah gagasan yang dikemukakan oleh Joseph Nye). Keamanan *cyber* adalah masalah utama dalam hubungan diplomatik, seperti yang diidentifikasi oleh Perancis Buku Putih Pertahanan dan Keamanan Nasional sebagai prioritas nasional.

Jurnal ketujuh, berjudul *Cybernorms: Analysis of International Norms in France's Paris Call for Trust and Security in Cyberspace* oleh Diko Catur Novanto, Ika Riswanti Putranti dan Andi Akhmad Basith Dir (Novanto et al., 2021). Penelitian ini berusaha untuk melihat pentingnya *Paris Call* yang telah dilakukan oleh pemerintah Perancis yang bertujuan untuk mengingatkan kembali norma-norma umum dunia maya yang belum populer atau melihat terbentuknya norma-norma internasional di bidang *cyber*. Ruang *cyber* berfungsi untuk mempromosikan demokrasi dan kebebasan berekspresi. Banyaknya aktor yang memiliki kepentingan yang berbeda membuat dunia maya menjadi tidak stabil. Beberapa aktor negara dan non-negara sendiri telah berkolaborasi dan mengadakan konvensi

di ranah *cyber*. Bagi Perancis, di dunia maya, diplomasi tidak lagi hanya soal hubungan negara-negara, tetapi juga hubungan negara-masyarakat sipil. Dalam aksinya, Perancis mendukung kebebasan berekspresi dan hak asasi manusia di semua media. Perancis memiliki nilai demokrasi dan HAM yang tinggi, sehingga dapat dijelaskan bahwa dukungan yang dilakukan terhadap *Paris Call* ini juga merupakan dukungan terhadap HAM di ruang *cyber*. Perancis membuat deklarasi tingkat tinggi yang disebut *Paris Call for Trust and Security in Cyberspace* pada tahun 2018, untuk menjaga stabilitas di dunia maya. Melalui *Paris Call*, Perancis mencoba membangun norma internasional di ranah *cyber* yang dikenal dengan *Cybernorms*. Norma ini telah didukung oleh beberapa aktor negara dan non-negara.

Kedelapan, jurnal yang berjudul *The Paris Call and Activating Global Cyber Norms* oleh Bruno Lete (Lete, 2021). Penulis dalam jurnal ini menyimpulkan bahwa *Paris Call for Trust and Security in Cyberspace* adalah alat terbaik yang tersedia bagi berbagai aktor untuk berinteraksi dalam tata kelola ruang maya yang inklusif. Ini adalah platform yang membantu untuk mengembangkan ide-ide segar tentang norma-norma dunia maya dan memasukkannya ke dalam negosiasi antar pemerintah, seperti proses PBB, bahkan jika itu tidak secara resmi dimasukkan ke dalamnya. Sejauh mana *Paris Call* akan membentuk implementasi norma *cyber* akan ditentukan oleh keragaman dan kredibilitas penandatangannya, bentuk negosiasi norma *cyber* antar pemerintah di masa depan, dan kebangkitan kedaulatan nasional di dunia maya. Ini memiliki potensi nyata untuk melengkapi PBB dengan mampu bertindak di mana PBB tidak bisa, terutama dengan mengoperasionalkan rezim norma yang ada. Meskipun banyak ketidakpastian seputar masa depan negosiasi PBB, norma-norma yang telah diadopsi oleh PBB dan prinsip *Paris Call* memberikan pedoman yang kuat untuk membentuk perilaku negara yang bertanggung jawab di dunia maya. Prioritas *Paris Call* sekarang adalah menemukan kapasitas dan sumber daya yang dibutuhkan untuk mengoperasionalkan kerangka kerja yang ada. Keragaman luas pemangku kepentingan yang terlibat dalam perdebatan tentang norma-norma dunia maya dan proliferasi inisiatif yang berusaha untuk mengoperasionalkan norma-norma ini telah menggerakkan tren yang akan

sulit untuk dibalik. Kekuatannya adalah membangun kapasitas bottom-up untuk menerapkan norma, kebutuhan mendasar saat memberikan jawaban atas banyak masalah di dunia maya, termasuk kekhawatiran seputar kepercayaan, stabilitas, dan keamanan. Pemerintah mungkin masih memiliki hak prerogatif untuk menentukan aturan main, tetapi keputusan yang mereka buat akan memiliki dampak yang jauh lebih besar jika mereka juga melibatkan entitas non-pemerintah. Tanggung jawab bersama di dunia maya bukan lagi konsep asing dan komunitas *Paris Call* berperan dalam mempercepat perubahan ini.

Sejauh ini, sudah banyak berbagai penelitian yang membahas mengenai diplomasi *cyber* dan beberapa penelitian mengenai *Paris Call*, namun masih belum cukup untuk membahas lebih dalam instrument apa yang digunakan serta apa sajakah dampak dari intrument tersebut.

## 1.5 Kerangka Teori

Kerangka teori sangat dibutuhkan untuk melakukan sebuah penelitian dengan menggunakan teori, model dan konsep, terstruktur dan jelas. Untuk menganalisa permasalahan tentang dampak *Paris Call* sebagai instrument diplomasi *cyber* penulis menggunakan konsep rezim keamanan *cyber*, *soft power* dalam diplomasi dan konsep diplomasi *cyber*.

### 1.5.1 Rezim Keamanan *Cyber*

> Institusi dan rezim internasional mulai berkembang sejak Perang Dunia II. Konferensi Bretton Woods yang diadakan pada pertengahan tahun 1944 merupakan cikal bakal terbentuknya institusi dan rezim internasional, khususnya di bidang ekonomi. Sejauh ini, rezim telah meliputi hampir setiap aspek urusan internasional yang memerlukan koordinasi antar pemerintah, mulai dari lingkungan masalah pertahanan (seperti pengembangan senjata dan pembatasan pertahanan kolektif), perdagangan, keuangan dan investasi, telekomunikasi, dan hak asasi manusia dan lingkungan; merupakan contoh dari sekian banyak urusan dalam rezim internasional (Prayuda et al., 2019).

Robert Keohane menyatakan bahwa peran lembaga adalah sebagai berikut: 1. Memberikan aliran informasi dan peluang negosiasi; 2. Meningkatkan kemampuan pemerintah untuk memantau otoritas lain dan melaksanakan komitmennya sendiri, oleh karena itu kemampuan untuk membuat komitmen yang kredibel adalah yang terpenting; 3. Memperkuat harapan (expectation level) yang muncul mengenai kesehatan perjanjian internasional (Keohane, 2020).

Dalam konteks keamanan, rezim terbentuk atas asumsi dasar bahwa hakikat negara hidup pada prinsip "timbal balik". Prinsip resiprositas atau timbal balik memaksa negara-negara berdaulat mengorbankan kepentingan jangka pendek untuk memperoleh keuntungan di masa depan yang lebih besar yang timbul dari sikap timbal balik aktor atau negara lain. Arthur Stein menyatakan bahwa akar dari terbentuknya rezim adalah relasi diantara negara yang berdaulat yang terjadi karena masing-masing negara berupaya memenuhi kebutuhannya, hingga akhirnya negara tersebut dapat bergantung pada diri sendiri dan mampu mengembangkan kemampuannya. Sekalipun dalam perspektif keamanan rezim sangat sulit dicapai, tetapi kebutuhan untuk kelangsungan hidup negara adalah membentuk hubungan yang bertujuan untuk mengelola kompleksitas melalui hubungan yang ada dalam rezim (Novitasari, 2017).

Ketika dunia menjadi lebih saling terhubung, keamanan dan kemakmuran masing-masing negara akan bergantung pada keamanan dan kemakmuran negara-negara lain, mendorong kekuatan-kekuatan besar untuk bekerja sama lebih erat satu sama lain, terutama terkait keamanan *cyber*. Pembentukan rezim internasional untuk mengatur keamanan *cyber* sangat penting untuk masa depan lingkungan keamanan internasional dan keamanan semua negara yang beroperasi di dalamnya.

Untuk mencapai komposisi keamanan *cyber* yang lebih tangguh, Anggota Negara harus mengembangkan dan menerapkan sesegera mungkin mencari kerangka kerja keamanan *cyber* (ditambah rencana aksi) untuk mengoordinasikan regional yang kohesif kerja sama dan secara kolektif

mengatasi tantangan keamanan *cyber* global bersama. Kerangka kerja semacam itu harus dipublikasikan secara terbuka untuk tujuan transparansi dan ketentuan harus dibuat untuk tinjauan berkala dan pemutakhiran tindakan dan rencana yang disepakati untuk menggabungkan prinsip-prinsip fleksibilitas, kemampuan beradaptasi, implementasi tepat waktu, dan strategis tinjauan ke masa depan. Karena sifat dari lingkungan ancaman selalu berubah-ubah, tidak fleksibel kerangka kerja dengan rencana kerja dan program kerja yang tetap mungkin tidak cukup efektif (Heinl, 2013).

Keamanan *cyber* mempengaruhi setiap negara di dunia ini dan merupakan bagian integral dari keberhasilan perdagangan global di era modern. Ancaman dan tantangan terkait arena *cyber* tidak hilang, tetapi akan terus berkembang. Sangat penting bahwa masalah ini dihadapi secara langsung dengan upaya internasional yang gigih untuk mengamankan dunia maya demi kebaikan dan kemakmuran semua yang terlibat. Prosesnya tentu akan rumit dan memakan waktu. Akan ada ketidaksepakatan antara negara-negara mengenai sifat spesifik dari ancaman, tingkat otoritas dan tanggung jawab negara, dan implikasinya terhadap kedaulatan negara. Masalah membangun sarana verifikasi kepatuhan yang layak akan menjadi tantangan. Berbagai tingkat koordinasi perlu dibentuk, termasuk koordinasi antarlembaga di dalam negara, koordinasi antara sekutu dan mitra, serta koordinasi dan kerja sama global (Holdorf, 2015).

Rezim keamanan *cyber* tidak akan menghilangkan semua risiko dan tantangan yang terkait dengan aktivitas *cyber*, namun rezim itu akan memberi negara beberapa cara untuk mengurangi banyak tantangan terkait *cyber*. Seperti rezim kontrol senjata, rezim keamanan *cyber* akan menciptakan aturan dan norma yang akan mengurangi ketidakpastian, memperkuat tanggung jawab hukum, dan mengurangi biaya transaksi terkait penggunaan dunia maya.

*Paris Call* menjadi wadah penghubung bagi banyak negara-negara untuk saling berkontribusi menciptakan keadamaian di segala aspek kehidupan bernegara. Terlebih lagi di tahun pandemi, kedamaian tersebut

diwujudkan dalam ranah keamanan *cyber* yang akan menciptakan rezim keamanan *cyber*.

### 1.5.2 *Soft power* dalam diplomasi

Suatu negara dalam mencapai kepentingan nasionalnya memerlukan adanya kekuatan atau power untuk mewujudkan keinginannya. Joseph Nye mengatakan power sebagai "*the ability to influence the behavior of others to get the outcomes one wants*" yang artinya kemampuan suatu negara untuk mempengaruhi atau merubah perilaku negara lain agar sesuai dengan keinginan negara yang bersangkutan (Winkler & Nye, 2005).

Menurut Nye power juga digolongkan dalam spektrum perilaku yang berbeda. Penggolongan ini dibagi menjadi dua yakni hard power dalam spektrum perilaku command power, command power adalah kemampuan untuk mengubah apa yang pihak lain lakukan (*what others do*) seperti menggunakan kekuatan militer atau ekonomi. Kedua yakni soft power dalam spekrum perilaku *co-optive power* dan *attraction*, yang mana dengan kemampuan untuk dapat mempengaruhi dan membentuk apa yang pihak lain inginkan (*what others want*) berbentuk budaya, ide, nilai, kebijakan ataupun penghargaan yang telah dicapai oleh suatu bangsa. *Co-optive* bekerja melalui agenda setting (manipulasi agenda pilihan politik sehingga pihak lawan gagal dalam mengekspresikan suatu tujuan politik tertentu karena merasa tujuan tersebut tidak lagi realistis/tidak banyak menguntungkan). Sedangkan *attraction*/daya tarik yang bersumber pada budaya, nilai-nilai dan kebijakan yang dimiliki. *Attraction* umumnya sukses bekerja apabila diplomasi publik memiliki daya tarik yang cukup atraktif untuk mempengaruhi preferensi target/pihak lawan yang dituju (Nye, 2019).

*Soft power* adalah kemampuan suatu negara untuk mendapatkan apa yang diinginkan melalui daya tarik bukan melalui sebuah paksaan atau pembayaran dan merupakan sumber daya nasional yang unggul sebagai kemampuan negara yang dapat digunakan untuk mempengaruhi negara lain demi mencapai hasil yang diinginkan atau kepentingannya. Alasan soft

power digunakan dalam hubungan antar negara tak lain adalah untuk mencapai tujuan nasional negara yang bersangkutan.

Penerapan *soft power* ini dapat diimplementasikan dalam berbagai instrumen dan teknik kebijakan luar negeri yang dijalankan oleh suatu negara, seperti progam diplomasi, bantuan ekonomi, pertukaran budaya dan berbagai macam kerjasama lain. Akan tetapi dalam pengimplemetasiannya soft power memiliki batasan yaitu: 1) Adanya imitasi yang dapat mengurangi efek *Soft power*; 2) Ketergantungan *soft power* pada konteks yang lebih besar daripada *hard power*; 3) *Attraction* memiliki efek yang lebih tersebar, sehingga sulit untuk melakukan pengukuran dengan pasti sehingga penggukuran *soft power* tidak dapat dilakukan dengan sempurna; 4) Apabila hanya dikonsentrasikan pada satu negara, *soft power* akan kehilangan daya tarik/ menjadi kurang penting; 5) *Soft power* lebih sering memberikan efek pada tujuan umum suatu negara, hanya sebagian yang berdampak pada tujuan khusus; 6) Pemerintah tidak memiliki kontrol penuh atas daya tarik.

### 1.5.3 Diplomasi *Cyber*

Diplomasi *cyber* adalah diplomasi "untuk mengamankan kepentingan nasional terkait dengan dunia maya." Sebagai praktik, diplomasi *cyber* adalah respons alami terhadap relevansi dunia *cyber* yang semakin meningkat secara global. Melalui diplomasi *cyber*, negara-negara berkolaborasi untuk menanggapi dan menangani dimensi *cyber* dari konflik internasional, kejahatan, dan keamanan informasi (Khabbaz, 2020).

Diplomasi *Cyber* dapat didefinisikan sebagai diplomasi dalam domain *cyber* atau dengan kata lain, penggunaan sumber daya diplomatik dan kinerja fungsi diplomatik untuk mengamankan kepentingan nasional terkait dengan dunia maya. Kepentingan-kepentingan tersebut umumnya diidentifikasi dalam strategi *cyberspace* atau *cybersecurity* nasional, yang sering kali menyertakan referensi ke agenda diplomatik. Isu-isu utama dalam agenda diplomasi *cyber* termasuk keamanan *cyber*, kejahatan *cyber*,

pembangunan kepercayaan, kebebasan internet, dan tata kelola internet. Oleh karena itu, diplomasi dunia maya dilakukan seluruhnya atau sebagian oleh para diplomat, pertemuan dalam format bilateral (seperti dialog AS-China) atau dalam forum multilateral (seperti di PBB). Di luar kewenangan diplomasi tradisional, diplomat juga berinteraksi dengan berbagai aktor non-negara, seperti pemimpin perusahaan internet (seperti Facebook atau Google), pengusaha teknologi, atau organisasi masyarakat sipil. Diplomasi juga dapat melibatkan pemberdayaan suara-suara tertindas di negara lain melalui teknologi. Meskipun hal ini menetapkan jangkauan kegiatan yang cukup luas, hal ini memungkinkan kita untuk secara tegas menempatkan diplomasi *cyber* sebagai lembaga masyarakat internasional, bahkan ketika berinteraksi dengan aktor masyarakat dunia (Barrinha & Renard, 2017).

Ketika mempertimbangkan munculnya diplomasi *cyber*, penting untuk terlebih dahulu memahami logika yang mendasari kerja sama dalam domain kebijakan ini. Dunia maya mengumpulkan sejumlah karakteristik yang membingkai keterlibatan diplomatik di antara para pemangku kepentingan. Pertama-tama, ini adalah domain global yang menghubungkan negara dan warga di seluruh dunia dalam berbagai cara, menghasilkan interaksi dan gesekan di antara mereka. Lebih jauh lagi, dunia maya biasanya dianggap sebagai "global common", yang didefinisikan sebagai "domain sumber daya di mana semua negara memiliki akses hukum" (Buck, 1998).

Prinsip-prinsip masyarakat internasional tersebut berbenturan dengan sifat persaingan dunia maya di mana kekuatan utamanya mempromosikan visi, kepentingan, dan nilai yang bersaing untuk ruang maya. Karakteristik relevan lainnya dari ranah ini termasuk sulitnya atribusi serangan dan penyusupan dunia maya, menghalangi kepercayaan di antara para pemangku kepentingan; keuntungan dari pelanggaran atas kapasitas pertahanan, mendukung perilaku agresif; atau kesenjangan digital antara kekuatan dunia maya utama dan negara berkembang, yang menciptakan kerentanan global. Semua karakteristik ini membuat hubungan *cyber*

internasional dan tata kelola dunia maya menjadi sangat kompleks dan rapuh, tetapi pada saat yang sama membuat diplomasi menjadi semakin diperlukan, terutama yang berkaitan (tetapi tidak terbatas) pada mekanisme pembangunan kepercayaan dan pengembangan norma-norma internasional dan nilai-nilai.

## 1.6 Argumen

*Paris Call* merupakan upaya besar untuk menciptakan struktur multistakeholder yang menarik bagi aktor negara dan non-negara. Dengan adanya *Paris Call* kerja sama dalam penanggulangan upaya pencegahan dan meminimalisir serangan *cyber* negara Perancis dengan negara lainnya semakin berkembang, dan serangan *cyber* walaupun tidak banyak namun berkurang.

## 1.7 Metodelogi Penelitian

### 1.7.1 Jenis Penelitian

Metodologi merupakan suatu ilmu yang mempelajari tentang cara-cara dalam mencari dan menemukan sekumpulan data yang diperlukan untuk memenuhi kepentingan ilmiah dalam suatu rangkaian proses penelitian. Dalam penelitian ini peneliti menggunakan metode penelitian Kualitiatif. Ciri khusus metode kualitatif adalah pengungkapan fenomena tanpa harus menyajikan penjelasan-penjelasan kuantitatif.

Dengan melakukan proses berpikir yang di mulai dari data yang dikumpulkan kemudian diambil kesimpulan secara umum, yang merupakan suatu strategi inquiri yang menekankan pencarian makna, pengertian, konsep, karakteristik, gejala, simbol maupun deskripsi tentang suatu fenomena, kemudian disajikan secara naratif. Setelah mengambil beberapa data dari jurnal online (*Scopus, J-stor, Google Scholar*) penulis akan menyaring informasi yang diperoleh lalu kemudian menuliskannya kembali.

### 1.7.2 Lokasi dan Jangkauan Penelitian

Lokasi penelitian secara kualitatif untuk mendapatkan data sekunder dilaksanakan di Indonesia. sedangkan jangkauan penelitian dari tahun 2019 -2022 untuk membantu proses penelitian.

### 1.7.3 Sumber Data

Untuk sumber data peneliti menggunakan sumber data sekunder berupa informasi dan kajian yang diperoleh dari buku, surat kabar, majalah, jurnal, media internet serta informasi dari instansi-instansi yang terkait dengan penelitian.

### 1.7.4 Metode Pengumpulan Data

Dalam penyusunan naskah ini menggunakan metode penelitian kepustakaan (*library research*) yaitu mengumpulkan semua bahan bacaan yang berkaitan dengan masalah yang dibahas, kemudian memahami secara teliti dan hati-hati sehingga menghasilkan temuan-temuan penelitian.

## 1.8 Sistematika Penulisan

Sistematika penulisan yang digunakan penulis dalam proposal tesis ini akan dibagi dan dijelaskan ke dalam lima bab, yaitu:

Bab satu mendeskripsikan mengenai proposal tesis ini yang terdiri dari latar belakang masalah, rumusan masalah, tujuan penelitian, kontribusi penelitian, studi pustaka, kerangka teori, hipotesis, metode penelitian, dan sistematika penulisan.

Bab dua ini menjelaskan tentang *cyber*, *cybersecurity*, serangan *cyber* global dan Perancis, dan dampak terhadap negara yang terkena.

Bab tiga menjelaskan tentang platform *Paris Call*, negara yang terlibat, tujuan, dan prinsip dari *Paris Call*.

Bab empat adalah bab berisi pembuktian menjabarkan dampak *Paris Call* sebagai diplomasi *cyber* di negara Perancis.

Bab lima merupakan bab yang berisi kesimpulan dari seluruh kajian pada bab-bab sebelumnya.