BAB II

LATAR BELAKANG KEAMANAN SIBER PRANCIS HINGGA PEMBUATAN *PARIS CALL*

Seiring perkembangan zaman, ranah siber menjadi sangat penting. Semuanya terdigitalisasi dalam semua sudut perkembangan negara dari politik, ekonomi, budaya, maupun sosial. Negara-negara telah mengintegrasikan infrastruktur mereka dengan teknologi yang digital, munculnya *e-commerce, e-diplomacy, e-business, e-voting* dan lainnya. Perkembangan ini juga membuat ancaman bagi para pengguna internet, bukan hanya individu saja, akan tetapi aktor seperti negara maupun non-negara juga terkena dampaknya. Ancaman *cyberattack* menjadi rawan di ranah siber terutama bagi negara-negara yang telah mendigitaslisasikan infrastruktur mereka. Tanpa adanya regulasi atau norma yang mengatur aktor-aktor negara maupun non-negara bisa melakukan semau mereka di ranah siber, seperti *cyberattack* terhadap pemerintahan Estonia, Georgia, Meksiko, Kenya, dan lainnya. Pembuatan norma internasional menjadi topik yang populer didalam ranah siber, terutama terhadap akademisi Hubungan Internasional maupun Hukum Internasional. *Paris Call For Trust And Security In Cyberspace* merupakan deklarasi tingkat tinggi yang dibuat oleh Prancis dalam upaya mereka merespon ancaman di ranah siber saat ini.

Dalam Bab 2, penulis menjelaskan tentang latar belakang keamanan siber secara domestik hingga internasional di Prancis, yang melatarbelakangi pembuatan

Paris Call. Bab ini akan dibagi menjadi lima sub-bab. Bagian pertama, membahas tentang doktrin keamanan digital di Prancis dari level domestik hingga internasional. Bagian kedua, membahas tentang kesembilan prinsip didalam *Paris Call*. Bagian ketiga, membahas tentang norma umum siber dan membandingkannya dengan *Paris Call*. Disini, penulis mengambil lima studi kasus konvensi dan kerjasama yang mempunyai kaitan dengan siber, seperti ENISA, Konvensi Budapest, *Tech Accord*, *Charter of Trust*, dan *For the Web*. Bagian keempat, menjelaskan tentang pentingnya *Paris Call* dan menjelaskan betapa pentingnya ke-sembilan prinsip didalamnya. Bab kelima, melihat siapa saja aktor pendukung dari *Paris Call* dan menjelaskan mengapa mereka mendukung *Paris Call*. Bab terakhir, memberikan kesimpulan dari Bab 2 yang menjelaskan tentang pentingnya *Paris Call*.

2.1 Doktrin *Cybersecurity* Prancis

Keamanan siber menjadi sangat penting bagi negara dalam menjaga data warga negara, infrastruktur, maupun militer. Hal ini tentunya membuat banyak negara memposisikan diri mereka untuk membuat kebijakan dan arahan baru. Kemunculan kebijakan siber di Prancis terbentuk pertama kali dari kekhawatiran Stuxnet pada tahun 2010. Hal ini dikarenakan kejadian tersebut dapat menyerang sektor perindustrian dan di buat oleh negara Amerika Serikat dan Israel (Falliere, Murchu and Chien, 2011; Baumard, 2017). Permasalahan ini membuat Prancis untuk bertindak dalam membuat kebijakan didalamnya.

Pada bab ini menjelaskan doktrin keamanan siber Prancis di level domestik dan internasional. Mengenal doktrin dalam kedua level ini penting untuk mengetahui kedepannya dalam pembuatan *Paris Call*.

2.1.1 Level Domestik

Awal mula kemunculan sejarah kebijakan keamanan siber berasal pada evolusi sejarah intelijennya. Inisiatif pertama adalah pada tahun 1942 ketika sekutu mengambil kembali Afrika Utara, Jendral De Gaulle meminta Kolonel Jean Joubert de Ouches untuk membuat organisasi terdesentralisasi yang mempu mencegat dan mengurai komunikasi lawan. Pada Agustus 1943, terbuatlah organisasi antar kementerian yang disebut *Direction Technique du Chiffre* (Direktorat Teknis Cipher) (Baumard, 2017).

Pada tahun 1986, Prancis membuat kebijakan untuk keamanan sistem informasi, dan membentuk komisi dan delegasi antar-administrasi, serta layanan pusat untuk keamanan sistem informasi. Organisasi ini direvisi dengan penugasan pada tahun 1996 untuk Sekretariat Jenderal Pertahanan Nasional (SGDN) pada tanggung jawab khusus dalam identifikasi dan pemantauan risiko yang mempengaruhi keamanan sistem informasi. Pada keputusan Juli 2001, keamanan layanan informasi menjadi arahan utama bagi Pertahanan Nasional (ibid., hal 55).

Pada 13 Januari 2006, ada laporan dari Pierre Lasbordes yang menjelaskan bahwa keamanan sistem informasi Prancis tertinggal yang di beri judul "*The security of information systems—A major issue for France"*[1].

Pada 2008 Februari, kebijakan Prancis melihat ada permasalahan baru di dalam sistem informasi ini, sehingga buku putih Prancis mengarah ke keamanan siber. Buku putih ini melihat bahwa "tingkat serangan harian terhadap sistem informasi, baik yang berasal dari negara atau non-negara, menunjukkan potensi yang sangat tinggi untuk destabilisasi kehidupan sehari-hari, kelumpuhan jaringan yang penting bagi kehidupan bangsa, atau fungsi kemampuan militer tertentu" (ibid., hal 56)

Pada 7 Juli 2009 ada keputusan dalam pembuatan *Agence nationale de la sécurité des systèmes d'information* (ANSSI), yang melayani dalam membantu Perdana menteri dalam tanggung jawabnya di bagian pertahanan dan keamanan nasional terutama dalam bidang sistem informasi (Agence nationale de la sécurité des systèmes d'information, no date).

Dengan berkembangnya dunia siber, pemerintahan Prancis mengetahui bahwa dunia ini menjadi sangat penting. Mereka

[1] http://www.senat.fr/rap/r11-681/r11-68117.html

membuat “strategi nasional” yang bertujuan untuk memposisikan negara dan kepentingan mereka ke arah dunia siber. April 2011, terbuatnya *Digital National Council (Conseil national du numérique)* oleh Pemerintah Prancis yang bertujuan untuk menjaga netralitas internet, dan menjaga kebebasan berekspresi maupun data pribadi warga negara di dalam “French Internet” (Intenet Prancis) (Baumard, 2017; Numérique, 2017)

Tahun 2013, buku putih Prancis juga menyoroti permasalahan siber, yang dimana pada poin ke-9 dan ke-10 tentang keamanan siber. Mereka tahu bahwa pentingnya dunia siber ini kedepannya sehingga perlu menjaga keamanan siber.

Tahun 2016, terjadi revisi kebijakan keamanan siber dibawah pemerintahan Manuel Valls. Strategi nasional ini tidak lepas dari kepentingan keamanan yang bertujuan melawan *cybercrime*. Keamanan sebagai rangkaian dari perlindungan rakyat termasuk infrastruktur dan pertahanan militer. Adanya penambahan yang baru ini dikarenakan serangan teroris terhadap warga negara Prancis pada tahun 2015-2016 (Chow and Kostov, 2015). Strategi Digital Nasional 2016 juga sangat memperkuat keamanan sistem informasi "*Operator of Vital Importance*" (OVI). Prancis tidak akan membiarkan perusahaan internasional besar dan negara asing memata-matai rakyatnya. Dalam laporan nasional Prancis:

"Pengembangan teknologi digital tidak dapat berkelanjutan di dunia maya yang di mana Negara tidak menghormati praktik baik yang diperlukan untuk transisi digital yang bermanfaat bagi semua negara dan di mana beberapa pemain ekonomi memonopoli kekayaan yang merupakan data digital, terutama data pribadi, dan sumber daya untuk generasi masa depan." (Baumard, 2017).

2.1.2 Level Internasional

Kerjasama dalam penanganan dunia siber diperlukan, Prancis sendiri telah melakukan beberapa kerjasama. *European Union Agency for Cybersecurity* (ENISA) yang telah bekerja untuk membuat keamanan dunia maya Eropa sejak 2004 (ENISA, no date), merupakan salah satu kerja sama yang dilakukan Prancis di level internasional. Perdana Menteri Prancis pada saat itu, Manuel Valls, berkomitmen untuk transisi yang dibawa Prancis ke arah digital. Valls juga mengetahui tentang ancaman dan konfrontasi di dunia siber seperti kompetisi dan spionase, disinformasi dan propaganda, terorisme dan kriminalitas, maupun menjadi kepentingan bagi negara-negara lain[2].

Pendekatan ENISA mempresentasikan kegiatannya di berbagai bidang (1) Rekomendasi mengenai keamanan siber dan saran

[2] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf

independen; (2) Kegiatan yang mendukung pembuatan dan implementasi kebijakan; (3) Pekerjaan *'Hands On'*, di mana ENISA bekerjasama secara langsung dengan tim operasional di seluruh UE; (4) Menyatukan Komunitas Uni Eropa dan mengoordinasikan respons terhadap insiden *cybersecurity* lintas batas berskala besar, (5) Menyusun skema sertifikasi *cybersecurity* (ENISA, n.d).

Konvensi yang diikuti Prancis seperti Konvensi Budapest juga diikuti. Konvensi ini menangani pelanggaran hak cipta, penipuan terkait komputer, pornografi anak dan pelanggaran keamanan jaringan. Ini juga berisi serangkaian kekuatan dan prosedur seperti pencarian jaringan komputer dan penyangkalan (Council of Europe, no date). Tujuan utamanya adalah untuk mengejar kebijakan terhadap kriminal bersama yang sama, yang bertujuan melindungi masyarakat terhadap kejahatan dunia siber, terutama dengan mengadopsi undang-undang yang tepat dan membina kerja sama internasional. Konvensi ini juga di tanda tangan oleh negara lain seperti Amerika Serikat, Kanada, Jepang, dan Afrika Selatan. Beberapa negara juga telah meratifikasi seperti Australia, Kanada, Republik Dominika, Israel, Jepang, Mauritius, Panama, Sri Lanka, dan Amerika Serikat.

2.2 Ke-Sembilan Prinsip *Paris Call*

Ada sembilan prinsip didalam *Paris Call*, 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)*; dan (9) Norma internasional.

Prinsip-prinsip ini merupakan prinsip-prinsip umum yang sering diterapkan dalam perjanjian multilateral terhadap keamanan siber. Akan tetapi, beberapa prinsip ini kadang terlupakan, bahkan hanya difokuskan pada sektor-sektor tertentu, seperti sektor industri, tanpa adanya pertimbangan terhadap prinsip lainnya, inilah yang membuat *cybernorms* ter-fragmentasi. Ke-sembilan prinsip ini mempunyai dukungan aktor negara yang kuat, yang mencoba untuk menggaet banyak aktor.

Prinsip pertama, menjelaskan tentang adanya hubungan antara individu dan infrastruktur. Sebagai contoh; ketika pusat panggilan darurat mengalami serangan siber, gangguan pada panggilan darurat dari organisasi penyelamat dapat mengakibatkan kematian individu. Prinsip kedua, merupakan prinsip yang mencoba untuk melindungi ketersediaan dan integritas inti publik internet. Hal ini untuk menanggulangi permasalahan apabila adanya *error* dalam website maupun serangan DDoS dari luar.

Prinsip ketiga, mempunyai peran yang berfokus kepada aktor negara. Prinsip ini berperan untuk menjaga demokrasi dalam pemilihan umum. Ini adalah fenomena global, dengan contoh gangguan pemilu terlihat di negara-negara seperti Estonia pada tahun 2007, Georgia pada tahun 2008, Meksiko pada tahun 2018, Kenya pada tahun 2017, dan lainnya (Crabtree, 2018; Nye, 2018; Rozak, 2018). Bukan dari negara lain

saja yang bermain peran, aktor domestik juga mencoba menabur perpecahan dan polarisasi dalam konteks otoriter dan demokratis. Kejadian-kejadian tersebut merupakan serangan terhadap demokrasi yang terjadi saat ini.

Prinsip keempat, merupakan prinsip dalam menjaga Hak Cipta *(intellectual property)*, seiring berjalannya teknologi, perlu juga adanya keseimbangan antara Hak Cipta maupun akses terhadap informasi, *Paris Call* mencoba untuk mengatasi keseimbangan ini. Prinsip kelima, adalah non-proliferasi, yang mencoba untuk mengembangkan cara untuk mencegah penyebaran perangkat lunak berbahaya dan praktik yang dimaksudkan untuk menyebabkan kerusakan. Prinsip keenam adalah keamanan *lifecycle* yang mencoba untuk memperkuat keamanan proses, produk, dan layanan digital, di sepanjang siklus hidup dan rantai pasokannya. Memperkuat keamanan produk dan layanan digital di seluruh rantai pasokan adalah prinsip dari *Paris Call* karena pelaku jahat dapat mengancam pemerintah, industri, dan individu dengan menyerang titik terlemah dalam rantai tersebut, dengan konsekuensi negatif dalam hal geopolitik, spionase, perdagangan , dan perlindungan konsumen. Prinsip ke tujuh, dalam *Paris Call* merupakan *cyberhygiene* yaitu, memberikan edukasi tentang pentingnya dan tanggung jawab dalam dunia siber terhadap semua aktor. Prinsip kedelapan adalah tidak ada retasan kembali secara pribadi *(no private hack back)*, prinsip ini mencegah aktor non-negara, termasuk sektor swasta, melakukan *hacking-back*, untuk tujuan mereka sendiri atau untuk kepentingan aktor non-negara lainnya.

Prinsip terakhir yang penulis *highlight* merupakan norma internasional dengan cara mempromosikan penerimaan luas dan penerapan norma-norma internasional

tentang perilaku yang bertanggung jawab serta langkah-langkah membangun kepercayaan di dunia maya. Pembuatan *cybernorms* diharapkan dapat membuat aktor-aktor yang terlibat untuk bertanggung jawab di dalam ranah siber. Walaupun sudah ada norma-norma umum di dalam ranah siber, akan tetapi, beberapa dari norma-norma tersebut berfokus pada kepentingan aktor maupun berfokus pada suatu industri.

2.3 Norma Umum Siber dan *Paris Call*

Kerjasama yang dilakukan oleh Prancis terhadap keamanan siber seperti organisasi ENISA maupun Konvensi Budapest merupakan bukti konkrit bahwa keamanan siber sangat di perlukan. Permasalahan dari kedua organisasi tersebut adalah bagaimana kerjasama ini hanya memfokuskan dan bertujuan untuk menangani keamanan siber di dalam organisasi itu saja. ENISA yang muncul dari Uni Eropa, berfokus pada *Critical Infrastructures* yang ada di Uni Eropa dan terutama pada penetapan praktik, kebijakan, organisasi, dan kapasitas keamanan jaringan dan informasi yang tepat[3]. Konvensi Budapest mempunyai jangkauan aktor yang lebih luas, hal ini dapat terlihat dari beberpa aktor yang mengikutinya seperti Amerika Serikat, Kanada, Jepang, dan Afrika Selatan. Budapest juga berfokus pada penanganan pelanggaran hak cipta, penipuan terkait komputer, pornografi anak dan pelanggaran keamanan jaringan. Kedua hal tersebut lebih bertujuan untuk menjaga keamanan nasional bagi negara masing-masing dan menjaga kejahatan *cybercrime* yang dilakukan oleh individu.

[3] https://www.enisa.europa.eu/publications/corporate/enisa-strategy

Pembuatan *cybernorms* juga bukan berasal dari aktor negara saja, aktor *non-states* seperti Microsoft yang membuat "*Tech Accord*" yang bertujuan agar internet dan industri teknologi melindungi privasi dan keamanan pelanggan mereka dengan lebih baik dari serangan *cyberattacks*. Begitu pula, pembuatan dari perusahaan Siemens tentang "Charter of Trust" mencoba membuat norma siber yang berupaya mengembangkan kepatuhan pada prinsip dan proses keamanan, dengan tujuan mengembangkan "standar global" untuk keamanan siber. Akan tetapi Prancis memandang bahwa *cybernorms* tersebut terlalu sempit dan berorientasi pada industri. Terakhir, *For the Web* yang berfokus terhadap hak individu untuk mempunyai akses terhadap internet, dan menjaga internet untuk lebih terbuka.

Name	Nine principles								
	Melindungi individu dan infrastruktur	Melindungi Internet	Menjaga proses pemilihan umum	menjaga *intellectual property*	Non-proliferasi	Keamanan siklus hidup *(lifecycle)*	*cyberhygiene*	*No private hack back*	Norma Internasional
Paris Call	✓	✓	✓	✓	✓	✓	✓	✓	✓
ENISA	✓	✓	✓	✓	✗	✓	✓	✗	✗
Budapest Convention	✓	✓	✓	✓	✗	✗	✓	✗	✗
Charter of Trust	✓	✓	✗	✓	✗	✓	✓	✗	✗
Tech Accord	✓	✓	✓	✓	✓	✓	✓	✗	✗
For The Web	✓	✓	✗	✓	✓	✗	✗	✗	✗

Tabel 2.1 Perbandingan Kelima Perjanjian *Cybersecurity* terhadap *Paris Call*

Pembuatan *Paris Call* dengan sembilan poin, terutama dalam poin ke-9 tentang norma internasional. Dimana Paris ingin membuat norma di dalam ranah baru. Hal ini berbeda dari kedua kerjasama tersebut yang hanya meningkatkan keamanan siber dan penanggulangan *cybercrime*. *Paris Call* bertujuan untuk mengumpulkan semua

pemangku kepentingan, negara dan non-negara, swasta dan publik, agar mereka memainkan peran mereka dalam menjaga ranah siber yang aman.

2.4 Pentingnya Sembilan Prinsip *Paris Call*

Kemunculan teknologi dan internet yang sangat pesat membuat manusia tidak luput dari informasi yang dibawakan teknologi dan internet. Komunikasi dan informasi menjadi vital di masa-masa dunia yang globalisasi. Begitu pula dengan aktor negara maupun non-negara yang mengintegrasikan infrastruktur mereka ke dalam sistem teknologi. Integrasi ini dinamakan *Critical Infrastructure* yang dimana sektor-sektor negara terintegrasi satu sama lain melalui jalannya teknologi. Karena mereka berkontribusi pada produksi dan distribusi barang dan jasa yang penting bagi Negara Prancis untuk menjalankan wewenangnya, agar ekonomi berjalan, dan juga untuk kelanjutan keamanan dan pertahanan nasional. Konsep baru mulai bermunculan dengan integrasi infrastruktur dan teknologi, seperti *e-commerce, e-voting, e-diplomacy, e-business* dan lainnya. Tentunya *critical infrastructure* yang terintegrasi membantu negara dalam memonitor perekonomian dan menjadi sangat penting juga bagi aktor-aktor negara maupun non-negara lainnya, yang ikut serta mengintegrasikan teknologi dan infrastruktur mereka.

Kejadian seperti Stuxnet yang menyerang infrastruktur nuklir Iran membuat negara-negara khawatir. Virus ini juga menargetkan sistem kontrol industri. Amerika Serikat dan Israel yang membuat virus ini tentunya untuk melumpuhkan kekuatan nuklir Iran, yang menjadi kekhawatiran adalah bagaimana AS-Israel bisa menargetkan

sistem tersebut dari jarak jauh (Falliere, Murchu and Chien, 2011; Baumard, 2017). Hal serupa terjadi terhadap Estonia pada tahun 2007, dan Georgia 2008, dimana kedua negara tersebut di retas dan terkena *Distributed Denial of Service* (DDoS) yang di

asumsikan adalah peretas yang di bantu oleh pemerintah Russia (Nye, 2018). *Cyberattack* menjadi kekhawatiran bagi masa depan negara, hal ini dikarenakan peretas yang melakukan hal tersebut akan susah untuk dilacak. Penyerangan yang terjadi juga akan mengganggu ke stabilan sistem pemerintah dari sektor-sektor ekonomi, bisnis, kesehatan, dan lainnya. Adanya gangguan pemilu juga terlihat, seperti 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).

Ranah siber menjadi ranah yang terkontestasi oleh beberapa negara yang mencoba untuk mengedepankan kepentingan mereka untuk tujuan mereka masing-masing, hal ini membuat ranah siber tidak teregulasi sama sekali. Perlombaan untuk mendapatkan keuatan dan kekuasaan di siber menjadi penting bagi negara-negara besar, konsep *cyberpower* yang muncul menjelaskan bahwa kekuatan dunia siber dapat digunakan untuk menghasilkan hasil yang diinginkan di dalam dunia siber atau dapat menggunakannya sebagai instrumen untuk menghasilkan hasil yang lebih diinginkan di luar ruang siber (Nye, 2018).

	Di dalam ruang siber (intra)	Di luar ruang siber (ekstra)
Instrumen Informasi	***Hard*** : *Distributed Denial of Service* (DDoS) ***Soft*** : Menetapkan norma dan standar	***Hard*** : Penyerangan sistem kontrol dan akuisisi data (SCADA) ***Soft*** : Kampanye diplomasi publik untuk mempengaruhi opini
Instrumen Fisik	***Hard*** : Kontrol pemerintah terhadap perusahaan ***Soft*** : Infrastruktur untuk membantu aktivis HAM	***Hard*** : Membom router atau memotong kabel ***Soft*** : Protes dan demonstrasi

Tabel 2.2 Sumber: Diadaptasi dari Tabel Joseph Nye (Cyber Power, 2018)

Menurut Fabrizio Hochschild Asisten Sekretaris Jenderal untuk Koordinasi Strategis PBB, ada dua bahaya dalam perkembangan dunia siber: (1) Manipulasi kebenaran dan perilaku sosial yang datang dengan media sosial, yang "menciptakan kondisi yang memungkinkan terjadinya konflik" menurutnya kroban pertama dalam konflik adalah kebenaran. Penggunaan propaganda di sosial media membawa dampak disinformasi yang tinggi. Kampanye yang bersifat politik juga dapat menargetkan lebih dari satu sistem komputer akibat penggunaan propaganda yang ada. Manipulasi perilaku yang terjadi sekarang secara bebas di media sosial menjadi dasar dari masalah; (2) Ancaman AI dan *lethal autonomus weapon* (LAW), yang 'dapat membunuh tanpa agen/aktor manusia', menururutnya walaupun penetapan norma adalah langkah pertama yang krusial, kerangka kerja penahan diperlukan, yang dimana mampu mengubah dan beradaptasi cukup cepat agar sesuai dengan tingkat perubahan teknologi dan transformasi sosial yang terjadi sebagai akibatnya (Paris Peace Forum, 2018).

Sehingga dibutuhkan kerjasama dan tanggung jawab global dalam menjaga kestabilan *cyberspace.* Inilah mengapa *Paris Call* terbuat. *Paris Call* bertujuan untuk

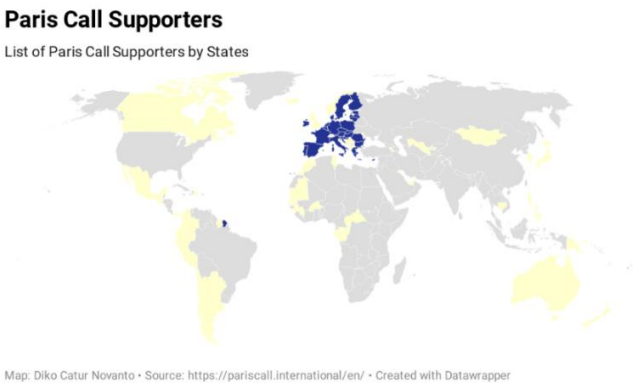
menjadikan arena internasional sebagai satu kesatuan yang bekerja menuju *'digital peace'* atau 'perdamaian digital'. Konsep ini dimunculkan oleh Presiden Microsoft Brad Smith dan Menteri Luar Negeri Prancis Jean-Yves le Drian. Dalam mencapai *'la paix digitale'*, Le Drian menekankan pada norma kepercayaan dan ketahanan. Dia menyerukan baik di tingkat nasional dan internasional untuk memperkuat sistem kepercayaan global. Negara harus membuktikan bahwa mereka dapat menerapkan *'le droite national'* ke dunia maya dan di tingkat internasional, dimana entitas seperti UE, NATO maupun G7 dapat mengembangkan dan memajukan praktik dan norma yang baik di dalam dunia maya (Paris Peace Forum, 2018).

Prancis percaya juga bahwa Hukum Humaniter Internasional ter aplikasikan di dalam penggunaan Teknologi Informasi dan Komunikasi (TIK), terutama di dalam ranah siber. Norma kepercayaan dan ketahanan yang di jelaskan oleh Le Drian menjadi sebuah acuan *Paris Call.* Dengan menggabungkan suara lebih dari 70 negara dan banyak entitas non-pemerintah, ini menggambarkan pentingnya menangani ancaman ini secara kolektif terhadap komunitas global. Prinsip-prinsip tersebut menunjukkan mengapa *Paris Call* itu penting, karena tidak hanya karena skala globalnya, tetapi karena pada akhirnya ini adalah upaya besar untuk dalam menempatkan perlindungan warga negara di garis depan.

2.5 Aktor Pendukung *Paris Call*

Aktor-aktor yang mendukung *Paris Call* dibagi menjadi dua, yakni aktor negara, dan juga aktor non-Negara.

2.5.1 Aktor Negara



Gambar 2.1
Sumber: Map Data dibuat oleh Penulis sendiri[4]

Di antara 79 negara, negara-negara Eropa adalah yang paling banyak hadir. Namun, hampir setiap benua terwakili: di antaranya kita temukan Qatar, Korea Selatan, Meksiko, Jepang, Kanada, Kolombia, Maroko, Senegal, dan Selandia Baru. Ada beberapa negara seperti India dan Brasil tidak ada dalam daftar. Ketiadaan negara-negara seperti itu dapat menjadi masalah. Sementara AS (setidaknya untuk saat ini), Tiongkok dan Rusia tidak mungkin untuk bergabung, seruan tersebut akan bergantung pada dukungan dari negara-negara seperti India dan Brasil untuk mendapatkan daya tarik di dalam lembaga internasional, terutama Perserikatan Bangsa-Bangsa. Macron, yang menyadari tantangan ini, menyarankan, *Internet Governance Forum* sebuah acara yang diselenggarakan oleh PBB untuk bertanggung jawab dalam memantau implementasi yang efektif dari *Paris Call* dan dipindahkan di bawah pengawasan langsung Sekretaris Jenderal PBB (Internet Governance Forum, 2018).

[4] Data berasal dari https://pariscall.international/en/supporters, diakses pada 18 Januari 2021

Prancis juga tetap mengacu kepada kerjasama siber sebelumnya dengan aktor negara lain, di dalam dokumen *Paris Call* menjelaskan bahwa dibutuhkan kerjasama antar negara dalam meningkatkan keamanan TIK yang digunakan bagi individu, oleh karena itu Konvensi Budapest juga menjadi salah satu kunci utama dalam menjaga kestabilan dunia siber.

2.5.2 Aktor *Non-States*

Dokumen tersebut telah mendapat dukungan dari kelompok non-pemerintah yang berpengaruh. Seperti *World Leadership Alliance, Chatham House, Carnegie Endowment for International Peace, World Wide Web Foundation* dan *Internet Society* telah berkomitmen pada prinsip-prinsipnya. Badan tata kelola teknis, seperti *Number Resource Organization* juga menyatakan minatnya. Dalam perusahaan yang berfokus pada sektor bisnis, seperti *Indian Chambers of Commerce & Industry, the Internet and Mobile Association of India* dan *U.S.-India Strategic Partnership Forum*, telah mendukung *Paris Call*. Secara total, sebanyak 300 universitas, LSM, dan asosiasi profesi telah berkomitmen pada himbauan tersebut.

Dalam lanskap industri, Prancis berhasil menarik kedua inisiatif utama: *The Tech Accord* dan *Charter of Trust* mewakili bagian signifikan dari penandatangan sektor swasta, karena bersama-sama mereka mewakili 85 perusahaan kuat seperti Airbus, Cisco, dan Facebook. Pendatang baru terkemuka termasuk Google, Samsung Electronics, Intel Corporation, Kaspersky Lab, Thales dan banyak perusahaan lainnya, mulai dari industri perbankan dan asuransi, hingga hukum, perdagangan dan pertahanan.

2.6 Kesimpulan

Dunia siber yang berkembang dengan cepatnya membuat mudahnya pertukaran informasi data dari aktor negara maupun non-negara. Sektor-sektor perekonomian, industri, dan lainnya terintegrasi satu sama lain untuk melakukan supervisi melalui teknologi. Walaupun sudah ada beberapa norma umum di dalam ranah siber, akan tetapi fokus sektor yang dilakukan masih ter-fragmentasi. Sehingga melalui pembentukan *Paris Call* ini, Prancis bertujuan untuk menjaga kestabilan ranah siber dengan menggaet aktor-aktor negara dan non-negara.

Dokumen tersebut mendorong regulasi dunia maya yang lebih luas dan terkoordinasi dengan lebih baik dalam semangat prinsip-prinsip dasar Piagam PBB, terutama pemeliharaan perdamaian dan keamanan internasional. Dengan kata lain *Paris Call* bertujuan untuk menjadi apa yang Konvensi Jenewa lakukan pada Perang Dunia 2. Bahkan jika Konvensi Jenewa menyatukan negara-negara menentang perang, *Paris Call* melakukan lebih dari sekadar menerjemahkan norma ke dunia maya. Ini adalah mengumpulkan semua pemangku kepentingan, negara dan non-negara, swasta dan publik, untuk benar-benar membuat semua orang memainkan peran mereka (Paris Peace Forum, 2018).