# Cybernorms: Analysis of International Norms in France's Paris Call for Trust and Security in Cyberspace

**Diko Catur Novanto**

*Students in Department of International Relations*
*Diponegoro University*
*Email : dikocn@students.undip.ac.aid*

**Ika Riswanti Putranti**

*Lecturer in Department of International Relations*
*Diponegoro University*

**Andi Akhmad Basith Dir**

*Lecturer in Department of International Relations*
*Diponegoro University*

**Abstract**

Cybercrime is a crime involving computers and networks that began to develop after the Cold War. International politics also have developed through computer networks or cyberspace, especially in communication and diplomacy. Many actors who have different interests make the cyber sphere unstable. Several state and non-state actors themselves have collaborated and conventions in the cyber realm. In 2018, France made a high-level declaration called the Paris Call for Trust and Security in Cyberspace to maintain stability in cyberspace. Through the Paris Call, France tries to establish an international norm in the cyber domain known as Cybernorms. This norm has been supported by several state and non-state actors. This study seeks to see the importance of the Paris Call that has been made by the French government which aims to remind the general norms of cyber that are not popular or see the formation of international norms in the cyber sphere. This study uses a qualitative method with the process-tracing data analysis method used to explain change and cause-and-effect. This research argues that cyber norms are very important for state or non-state actors in

maintaining the stability of the cyber world.

***Key Words :*** *France, Cybercrime, Cybernorms, Cyber, Cybersecurity, Norms*

**Abstrak**

*Kejahatan Siber (Cybercrime) adalah kejahatan yang melibatkan komputer dan jaringan yang mulai berkembang pasca Perang Dingin. Politik Internasional juga telah berkembang melalui jaringan komputer atau ranah siber (cyberspace) khususnya dalam komunikasi maupun diplomasi. Banyaknya aktor yang mempunyai kepentingan yang berbeda-beda membuat ranah siber tidak stabil. Beberapa aktor negara maupun non-negara sendiri telah melakukan kerjasama dan konvensi atas ranah siber. Pada tahun 2018, Prancis membuat deklarasi tingkat tinggi bernama Paris Call for Trust and Security in Cyberspace untuk menjaga kestabilan didalam ranah siber. Melalui Paris Call, Prancis mencoba untuk menetapkan sebuah Norma Internasional dalam ranah siber yang disebut sebagai Cybernorms. Norma ini sendiri telah didukung oleh beberapa aktor negara dan non-negara. Penelitian ini berusaha untuk melihat pentingnya Paris Call yang telah dibuat oleh pemerintah Prancis yang bertujuan untuk mengingatkan kembali norma-norma umum siber yang tidak populer maupun melihat tentang terbentuknya norma Internasional di ranah siber. Penelitian ini menggunakan metode kualitatif dengan metode analisis data process-tracing yang digunakan untuk menjelaskan perubahan dan sebab-akibat. Penelitian ini berargumen bahwasannya norma siber ini sangat penting bagi aktor-aktor negara maupun non-negara dalam menjaga kestabilan dunia siber.*

***Kata Kunci :*** *Prancis, Cybercrime, Cybernorms, Cyber, Cybersecurity, Norma*

## INTRODUCTION

In the development of the globalization era, technology is one aspect that is developing rapidly. One of the developments that occurred is the development in the field of internet or cyberspace. Cyberspace was originally developed for military technology that is used as a distribution network for sending information (Buzan & Hansen, 2009). Over time, the internet has begun to be widely used by several countries in the world.

The Paris Call for Trust and Security in Cyberspace is a high-level declaration supporting the development of general principles for securing cyberspace and related key principles: the practicality of international law, the responsible behavior of State actors, the specific responsibilities of private stakeholders, especially in terms of preventing security failures and preventing the use of certain practices that could destabilize cyberspace. There are nine principles in the Paris Call, namely: (1) Protecting individuals and infrastructure; (2) Protect the internet; (3) Defend electoral process; (4) Defend intellectual property; (5) Non-proliferation; (6) Lifecycle security; (7) Cyber hygiene; (8) No private hack back; (9) International Norms (Paris Call, 2018). In the Paris Call, the ninth principle, international norms, contains two norms, namely the norms of resilience and trust which was made by French Foreign Minister Jean-Yves le Drian.

The making of the Paris Call took place because of a threat that occurred in the cyber space. Where the attack is carried out by individuals or even supported by a state actor or the influence of a non-state actor. The awareness by France arose in June 2010, as evidenced by the emergence of Stuxnet at the time, which attacks the systems of uranium enrichment sites. in Natanz, Iran (Baumard, 2017; Falliere, Murchu, & Chien, 2011)such as a gas pipeline or power plant. The ultimate goal of Stuxnet is to sabotage that facility by reprogramming programmable logic controllers (PLCs created by the United States and Israel. Some other examples are the events in Estonia in 2007, where the Distributed Denial of Service (DDoS) was carried out by "patriotic hackers" from Russia who were offended by the World War II monument to the Soviets. Something similar happened in 2008 in Georgia, which was hit by DDoS in its information system before the Russian army invaded. The assumption is that the Russian government is in cahoots with hackers, and rejects their links to hacking (Nye, 2018). External interference with elections is also a threat to democracy, as was the case in the country of Mexico in 2018, which was seen from the large number of entrants to voting websites, especially from Russia (Rozak, 2018). Then in 2017, in Kenya there was influences from Cambridge Analytica during the election (Crabtree, 2018). Then the attack on critical infrastructure, such as the attack on the French

TV network TV5 Monde in 2015 (Melvin & Botelho, 2015). These cyber threats to France have made the cyber sspace unstable and insecure, not only threatening state actors and the industrial sector, but also threats to democracy and human rights.

According to Fabrizio Hochschild as Assistant Secretary General for UN Strategic Coordination, the establishment of a norm is crucial. Norms in this cyber domain are called cybernorms. However, it needs to be seen again that some of the principles made by France are general principles that have existed in several cybersecurity treaties, such as ENISA which focuses on cyberspace in the European Union, and the Budapest International Convention which they have signed. In addition, there are also previous cyber norm creation frameworks such as the Cybersecurity Tech Accord, Charter of Trust, and For the Web. So what differentiates Paris Call from the others?

Paris Call is not the first in wanting to create cybernorms. In its history, there are several documents on cooperation in the cyber realm. ENISA and the Budapest Convention are one of them. The Budapest Convention is the first international treaty on crimes committed via the Internet and other computer networks, specifically addressing copyright infringement, computer-related fraud, child pornography, hate crimes, and network security breaches. Its main objective is to pursue a common criminal policy to protect the public from cybercrime, particularly by adopting appropriate legislation and encouraging international cooperation (Council of Europe, n.d.). Then, ENISA focuses on dealing with cybersecurity in the European Union. The main objective of ENISA is to strengthen the Cybersecurity Act in the European Union (ENISA, n.d.). Both ENISA and the Budapest Convention have a lot of support including France. However, the problem with the Budapest Convention is that this convention is only a framework to fight cybercrime. This convention does not try to regulate a state actor, but aims to fight and punish individuals who commit cybercrime. Then, ENISA is only trying to improve the Cybersecurity Act in the European Union. According to the authors both agreements are only a framework for cyberspace, and do not try to create a set of norms that try to regulate a country.

The concept of cybernorms also has already been echoed. In April 2018 Microsoft created a "Digital Peace" campaign together with the "Cybersecurity Tech Accord" aimed at the internet and technology industry to better protect the privacy and security of their customers from cyber-attacks. Likewise, Siemens in May 2018 launched a "Charter of Trust" which seeks to develop compliance with security principles and processes, with the aim of developing a "global standard" for cybersecurity. For the Web, focuses on the openness of the Internet to individuals. Even in 2015, the United Nations Group of Governmental Experts (GGE) recognized that international humanitarian law must also be applied in cyberspace, but met a stalemate in 2017. Likewise, two blocks, one led by the United States and the other is led by China and Russia, which have also achieved a stalemate. Macron sees that there are two types of Internet "we are seeing two types of Internet emerge: as I said earlier, there is a Californian form of Internet, and a Chinese Internet." The contestation that is taking place in the cyber space can be seen clearly from the many actors who are trying to get the spotlight. It can be explained that the engagement that occurred also caused the forgetting of norms that should have been common, so that France tried to pave the way and overshadowed many actors in it.

Based on the arguments above, this article will attempt to discuss on how did how France created a new norm and reminded the general norm through the Paris Call. This article will use Constructivism approach regarding the process of making norm and how actors promotes their norm.

The Difference between Paris Call and General Norm

The cooperation carried out by France on cybersecurity such as the ENISA organization and the Budapest Convention is concrete evidence that cybersecurity is urgently needed. The problem of the two organizations is how this collaboration only focuses and aims to deal with cybersecurity within the organization. ENISA, which emerged from the European Union, focuses on Critical Infrastructures in the European Union and especially on establishing appropriate network and information security practices, policies, organizations and capacities. The Budapest Convention has a wider range of actors, this can be seen from several actors who participated in it, such as the United States, Canada, Japan,

and South Africa. Budapest also focuses on dealing with copyright infringement, computer-related fraud, and child pornography and network security breaches. Both of these are more aimed at maintaining national security for each country and protecting cybercrime crimes committed by individuals.

The creation of cybernorms also does not come from state actors alone, non-state actors such as Microsoft created the "Tech Accord" which aims to make the internet and the technology industry better protect the privacy and security of their customers from cyber-attacks. Likewise, the creation of the Siemens Company "Charter of Trust" seeks to establish a cyber-norm that seeks to develop compliance with security principles and processes, with the aim of developing a "global standard" for cybersecurity. However, France views that cybernorms are too narrow and industry-oriented. Finally, For the Web, which focuses on individual rights to have access to the internet and makes the internet more open.

Making the Paris Call with nine points, especially in the 9th point on international norms. Where Paris wants to set the norm in a new realm. This is different from the two collaborations which only improve cybersecurity and tackle cybercrime. Paris Call aims to bring together all stakeholders, state and non-state, private and public, so that they can play their part in maintaining a safe cyber space.

| Charter of Trust | Budapest Convention | ENISA | *Paris Call* | Name | |
|---|---|---|---|---|---|
| ✓ | ✓ | ✓ | ✓ | 1st principle | Nine principles<br>(1) Protecting individuals and infrastructure;<br>(2) Protect the internet;<br>(3) Defend electoral process;<br>(4) Defend intellectual property;<br>(5) Non-proliferation;<br>(6) Lifecycle security;<br>(7) Cyber hygiene;<br>(8) No private hack back;<br>(9) International Norms |
| ✓ | ✓ | ✓ | ✓ | 2nd principle | |
| ✗ | ✓ | ✓ | ✓ | 3rd principle | |
| ✓ | ✓ | ✓ | ✓ | 4th principle | |
| ✗ | ✓ | ✗ | ✓ | 5th principle | |
| ✓ | ✗ | ✓ | ✓ | 6th principle | |
| ✓ | ✓ | ✓ | ✓ | 7th principle | |
| ✗ | ✗ | ✗ | ✓ | 8th principle | |
| ✓ | ✗ | ✗ | ✓ | 9th principle | |

**How Norm is Created and Promoted**

Different from realists who explain that norms as an interest, and liberalism which explain that norms as a basis. Constructivism explains how a norm is spread and adopted by the state (Rosyidin, 2020). Finnemore and Sikkink have developed the idea of norms, how norms emerge, are approved, and the adoption in the domestic realm occurs. The extension of the concept of norms has three main forms. First, the concept of the emergence of new norms, namely norm emergence from an issue or problem that occurs in a country internationally or domestically, the emergence of norms comes from norm entrepreneur. Then the second stage is the norm cascade, in which the debate about norms is explained in the political sphere to get mutual agreement. Finally, norm internalization is how the adoption occurs in the domestic sphere in other countries.

To analyze *Paris Call*, the author focuses on the concept of norm emergence. Researchers tend to view norm emergencies as the result of persuasion, without formal characteristics or things that usually happen. However, this norm-making is made on several bases such as individuals, uncertainties, coincidences, and fortunate events. This norm creation uses process-tracing as a method to find cause and effect of norm creation (Finnemore & Sikkink, 1998; Kowert & Legro, 1996).

| ***Norm Emergence*** |
|---|
| ***Actors***<br>*Norm Entrepreneurs with Organizational Platforms* |
| ***Motives***<br>*Altruism, empathy, ideational commitment* |
| ***Dominant Mechanism***<br>*Persuasion* |

In the process, there is a "framing" of an issue or problem from the norm entrepreneur (Snow, Rochford, Worden, & Benford, 1986). Norm entrepreneurs are very important for the emergence of norms because they pay attention to problems or even "create" problems by using language that mentions, interprets, and dramatizes them. To explain norm entrepreneurship, the author uses the concept of *"Transnational moral entrepreneurs"* who are involved in "moral proselytism" from Nadelmann. This group mobilizes popular opinion and political support both at home and abroad; they stimulate and assist the formation of like-minded

organizations in other countries; and they play an important role in advancing their objectives beyond the national interests of their governments (Nadelmann, 1990).

Of course there are many motivations carried out by norm entrepreneurs, but for norm researchers, it will be very difficult to explain norm entrepreneurial motivations without referring to empathy, altruism, and ideational commitment. Empathy arises when actors have the capacity to participate in other people's feelings or ideas. Such empathy can lead to an interdependence of empathy, in which actors "are attracted to the welfare of others for their own sake, even if this has no effect on their own material well-being or security" (Keohane, 2005). Altruism exists when actors actually take "actions designed to benefit others even at the risk of significant harm to the actor's own well-being" (Monroe, 2014). Ideational commitment becomes the main motivation when entrepreneurs put forward norms or ideas because they believe in the ideals and values contained in the norms, although pursuing these norms may have no effect on their well-being (Monroe, 2014).

In their mechanism, norm entrepreneurs do not oppose the interests of other actors, but they act with a redefined understanding of the interests of other actors (Finnemore & Sikkink, 1998).

| **Development of Promoting the Norm** |
|---|
| **Incentives**<br>Strong Actors mainly States |
| **Persuasion**<br>Encouragement without Coercion |
| **Socialization**<br>Inclusivity |

The process of a norm that has already occurred, the norm will be disseminated, norms have three main strategic tools to further develop norms: incentives, persuasion, and socialization (Finnemore & Hollis, 2016; Goodman & Jinks, 2014). Incentives come from strong actors, or rather strong states often have enormous resources to spread their preferred norms through various incentives. They can offer positive persuasion; Persuasion, which means causing someone to do or believe something by asking, arguing, or giving reasons. This is primarily a cognitive process of exchanging information and arguments that changes thoughts, opinions, and attitudes about causality and effects without coercion (Ratner, 2011) And, Socialization, which refers to the process in which newcomers

are included or integrated into organized patterns of social interaction (Stryker & Statham, 1977).

**The Creation of Paris Call**

One of the main focuses of the author's research is the norm entrepreneurial actor who influences the Paris Call. In the process of forming norms, the entrepreneur's norm is an important actor. There are two actors that will be analyzed, domestic actors and transnational moral entrepreneur actors. According to Nadelmann, what explains moral views, especially foreign policy, comes from the political influence of domestic and transnational moral entrepreneurs as well as strong individual support in government. Moreover, in almost every case the relevant moral outlook is "cosmopolitan", not concerned with how states treat one another, but more about how states and individuals treat their fellow human beings (Nadelmann, 1990).

There are three domestic actors who are analyzed in the process of *Paris Call* by the author, French President Emmanuel Macron and French Foreign Minister, Jean Yves-Le Drian and Microsoft President Brad Smith. In a speech made by Macron at IGF 2018, he explained that the cyber space that is used by us is under threat. He explained that there are three threats, namely the structure itself, as well as the content and services provided, and values. The structural issue explained by Macron, explained that if it does not ensure the stability, trust and security of the cyber system. Then cyberspace security will be questioned. For the second threat, look at the threat to democracy. Which is used for hate speech or the spread of terrorist content than anything else. Finally, values and ideas, Macron explained that the neutral principle of the internet is starting to be questioned, because the content provided tends to be biased (Internet Governance Forum, 2018).

Brad Smith explained that in 2017, there were 1 billion victims of cybercrime worldwide. So that Le Drian, along with Microsoft President Brad Smith, is trying to create an international arena that works towards 'digital peace', this is how the Paris Call initiative emerged. In achieving *'la paix digitale'*, Le Drian emphasizes the norms of trust and resilience. He called on both at the national and international levels to strengthen the global belief system. Explaining, both at the national and international levels, to strengthen the global belief system,

whose security is described as "as strong as its weakest link". Countries must prove that they can apply 'le droite national' to cyberspace and at the international level, where entities such as the EU, NATO and the G7 can develop and promote good practices and norms in cyberspace (Paris Peace Forum, 2018).

The individual actors conducted a framing in which they tried to tell how serious the issue of cyber issues was. They are norm entrepreneurs, which encourages Paris Call as a cybernorms. The invitation made by Macron, Le Drian and Brad Smith, was not only for state actors, but non-actor actors.

Regarding Transnational moral entrepreneurs they tend to have moral views. Their efforts are in the form of framing an issue or problem. The creation of cybernorms is not unique, Microsoft itself has approached France for support for the Tech Accord, however, for France, the Tech Accord is industry-oriented (Untersinger, 2018). Transnational moral entrepreneurs have an important role, especially in providing "framed" issues as a problem. These problems, push the issues in the creation of cybernorms. For example, France is working with Microsoft and the Alliance for Securing Democracy which is building a community of partners to fight election interference, which will bring together representatives from government, industry and civil society to strengthen capacities to prevent malicious interference by foreign actors in the electoral process. Then, Seguros en la red ("Secure on the net") is the 7th principle effort of cyber hygiene which comes from the Equatorian Cybersecurity Association. This group seeks to teach children about the responsible use of technology and information and its risks. France is trying to create a Paris Call to tackle global issues by involving countries, companies and wider civil society in a bottom-up approach.

According to Sikkink, it was explained that norm relations correlate with human rights violations. Sikkink argues that there is human rights prosecution and a 'justice cascade' that can be traced within a norm, which is also supported by an alliance of countries and NGOs that want change (Sikkink, 2011). Motivation for norm entrepreneurs is based on empathy, altruism, and ideational commitment. This motivation could be seen in Macron speech on Paris Peace Forum. The idea of combating illegal content from terrorism to child pornography could be seen

as an empathy; altruistic value could also be seen, which Macron believe that democracy should be upheld. There's no materialistic value for France to help other states in protecting their own general election, which is why this could be seen as altruism of France; Ideational commitments are also on the Paris Call. The principles in the Paris Call are based on the norms of resilience and trust echoed by Le Drian. France believes in this norm, which the Paris Call encourages nationally and internationally. Although there were some actors who didn't follow the Paris Call. This commitment to the idea is what makes France appear ambitious in the creation of cybernorms.

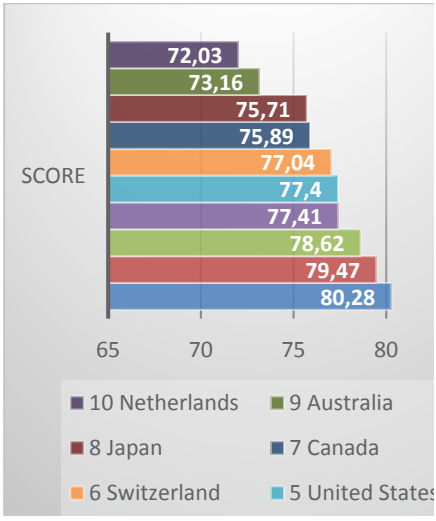
Dominant mechanism that is being used by actors to push the cybernorms is persuasion. The persuasion here is how norm entrepreneur actors see that these issues are an important problem, not only domestically but globally. Persuasion refers to the basic meaning of the term, urging other actors to take action. The European Emergency Number Association (EENA) believes that, for the safety of citizens, it is important to ensure that public safety services remain uninterrupted. To protect critical infrastructure and sensitive information, services must implement appropriate and effective safeguards. The Transatlantic Commission on Election Integrity (TCEI), strives to share best practices between decision-makers and institutions around the world of democracy, raising public awareness of the risks of disruption while applying it in the field to new models and technologies to empower civil society and governments to defend democracy.

The actors' persuasion is needed, because they see, or have even been affected by, a problem in cyberspace. So that this persuasion, urged actors like France to create cybernorms.

## PROMOTING PARIS CALL AND THEIR INTERNATIONAL NORMS

Academics of international law and international relations have studied the mechanisms for the creation and implementation of international norms carefully. Whether emerging from habit or entrepreneurship, there are at least three separate tools for promoting progressive development and norm dissemination: (1) incentives, (2) persuasion, and (3) socialization (Finnemore & Hollis, 2016; Goodman & Jinks, 2014)

Incentives are created based on how strong the actors who carry them are, especially when norm-making is done by strong state actors. Because they can provide positive persuasion, for example trade regulations between actors or arms deals, which allow other countries to like and abide by the norm (Goodman & Jinks, 2014). Incentives by France could be analyzed by their soft power. In 2019, France is one of the strongest countries in the soft power they provide to other countries. Soft power is the ability to encourage collaboration and build networks and relationships, according to Portland Communications, the UK-based public relations agency behind the index. France is in the number 1 position in it (Mcclory, 2019), this shows the strength of France that believes it can create an international norm in cyberspace.




The diplomacy carried out by France is also related to digital aspects, which they call digital diplomacy. Digital diplomacy is one of the priorities for French Ministry for Europe and Foreign Affairs. Soft power is aimed primarily at promoting the image of France and for the benefit of the French economy, language and culture. For France, in cyberspace, diplomacy is no longer just a matter of state-state relations, but also state-civil society relations. The cyber space serves to promote democracy and freedom of expression. In action, France supports freedom of expression and human rights in all media.

Framing is the most important thing in persuading other actors to follow norms (Finnemore & Hollis, 2016). However, framing in

cyberspace is not a single issue. This is due to the emergence of various contexts by various other actors as well. So that when an actor wants to do framing, it must focus on an issue that occurs. An important aspect in framing an issue is linking. Link a cybersecurity issue to a larger problem or global security problem.

Macron persuades state actors, NGOs, transnational companies, and others. Macron uses two tools for persuasion, namely framing and linking. In his speech at the Internet Governance Forum in 2018, Macron explained that "... that the Internet we take for granted is under threat." In his speech. Macron discusses more about cyber issues that are beginning to be threatened. He explained that there are three things that are threatened; the first is the structure on the internet. He saw that if there were no regulations in place, the cyber domain would collapse. Macron sees the need for the formation of trust between actors to maintain the stability of the cyber space. Because not only state actors, but individuals, organizations, companies and NGOs are also integrated with the internet; the second threat comes from the content and services on the internet. Even though the internet has become a matter of climate protests, women's rights, and others, at present the internet also provides hate speech, as well as the spread of terrorist content compared to many others; and finally, the threat that occurs is to values and ideas. Macron explained that the neutral principle of the internet is starting to be questioned, because the content provided tends to be biased. Framing that occurs as if cyber threat is a global threat and requires shared responsibility is something that is needed for this norm to be made. The problems in the frame seem as if the problems in the cyber space are a careful responsibility, and not only for the actors with an interest.

Macron connects cyber issues such as threats to the corporate sector, individuals, to democracy. This reinforces the significance of the issue, much like Macron's speech at the 2018 IGF. Usually the norms propagated also instill a larger 'narrative' about security or identity. Macron uses the word 'we', which suggests that cybersecurity is shared security. This becomes a persuasive force encouragement to invite other actors.

Socialization refers to the process by which newcomers are incorporated into organized patterns of social interaction (Stryker & Statham, 1977). This relationship

rests on social relations and the elemental identity of the concept of norms: an actor who wants to build or maintain a relationship with another actor or group of actors will conform to a norm, not because of its content but because doing so is expected because it is in a valuable relationship between actors. France has high democratic and human rights values, so it can be explained that the support made to the Paris Call is also support for human rights in the cyber space, but it is not only state actors who need to support the Paris Call. Macron explained that *"we need to invent - innovate - new forms of multilateral cooperation that involve not only states, but also all of the stakeholders you represent. This is what I want for us; this is what I want us to work towards. These issues are a huge responsibility for the Internet community, for you and for us."* so this invitation tries to embrace the actors, for universal purposes such as human rights. This universal invitation is also the basis for the actors supporting the Paris Call. The actors believed it was appropriate to follow the Paris Call.

French behavior towards human rights is a reference for actors to follow the norms enforced by France. This is because imitation can occur because actors perceive that this is the way a successful state behaves. According to Finnemore and Hollis, explaining that support for prevailing norms is a socialization process of wanting to imitate, *"To get to where they are now, I have to do what they do,"* but it can also be a more affective response such as *"to be a part of of this group and respected by its members, I have to imitate their behavior."* (Finnemore & Hollis, 2016).

## CONCLUSION

The Paris Call document presented by France should be welcomed by various actors. In cyberspace, companies and other non-governmental organizations are playing a role. But states remain the main regulators in their jurisdictions and in international institutions. The creation of norms in cyberspace is manifold. The initiatives carried out in cybernorm also tend to be fragmented. Macron is trying to get away from the international deadlock in cyberspace. Although Paris Call avoids the most sensitive activities such as espionage and offensive operations, this makes it more likely that Paris Call will receive support from a wider range of actors.

**REFERENCES**

Baumard, P. (2017). Cybersecurity in France. In *Springer*. https://doi.org/10.1007/978-3-319-54308-6

Buzan, B., & Hansen, L. (2009). The evolution of international security studies. In *The Evolution of International Security Studies*. https://doi.org/10.1017/CBO9780511817762

Council of Europe. (n.d.). Convention on Cybercrime. Retrieved May 29, 2020, from https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

Crabtree, justina. (2018, March 23). Cambridge Analytica and its role in Kenya 2017 elections. Retrieved March 18, 2021, from https://www.cnbc.com/2018/03/23/cambridge-analytica-and-its-role-in-kenya-2017-elections.html

ENISA. (n.d.). About ENISA. Retrieved May 29, 2020, from https://www.enisa.europa.eu/about-enisa

Falliere, N., Murchu, L. O., & Chien, E. (2011). W32.Stuxnet Dossier. *Symantec-Security Response*. https://doi.org/20 September 2015

Finnemore, M., & Hollis, D. B. (2016). Constructing Norms for Global Cybersecurity. *American Journal of International Law*. https://doi.org/10.1017/s0002930000016894

Finnemore, M., & Sikkink, K. (1998). International Norm Dynamics and Political Change. *International Organization*. https://doi.org/10.1162/002081898550789

Goodman, R., & Jinks, D. (2014). Socializing States: Promoting Human Rights Through International Law. *The American Journal of International Law*. https://doi.org/10.5305/amerjintelaw.108.3.0576

Internet Governance Forum. (2018). IGF 2018 Speech by French President Emmanuel Macron | Internet Governance Forum. Retrieved November 12, 2020, from https://www.intgovforum.org/multilingual/content/igf-2018-speech-by-french-president-emmanuel-macron

Keohane, R. O. (2005). After hegemony: Cooperation and discord in the world political economy. In *After Hegemony: Cooperation and Discord in the World Political Economy*. https://doi.org/10.2307/40202461

Kowert, P., & Legro, J. (1996). Norms, Identity, and Their Limits: A Theoretical Reprise. *The Culture of National Security: Norms and Identity in World Politics*.

Mcclory, J. (2019). *Methodology of the index The top five American soft power after Trump The soft power of government innovation*.

Melvin, D., & Botelho, G. (2015, April 9). French TV network TV5Monde hit by massive cyberattack - CNN. Retrieved November 9, 2020, from https://edition.cnn.com/2015/04/09/europe/french-tv-network-attack-recovery/index.html

Monroe, K. R. (2014). The Heart of Altruism. In *The Heart of Altruism*. https://doi.org/10.1515/9781400821921

Nadelmann, E. A. (1990). Global prohibition regimes: The evolution of norms in international society. *International Organization*. https://doi.org/10.1017/S0020818300035384

Nye, J. S. (2018). Cyber power. *Routledge Handbook of Russian Foreign Policy*, (May), 182–198. https://doi.org/10.4324/9781315536934

Paris Call. (2018). The call and the 9 principles — Paris Call. Retrieved May 29, 2020, from https://pariscall.international/en/principles

Paris Peace Forum. (2018). Paris Call for Trust and Security in Cyberspace - Paris Peace Forum. Retrieved June 2, 2020, from https://parispeaceforum.org/publication/paris-call-for-trust-and-security-in-cyberspace/

Ratner, S. R. (2011). Law promotion beyond law talk: The Red Cross, persuasion, and the laws of war. *European Journal of International Law*. https://doi.org/10.1093/ejil/chr025

Rosyidin, M. (2020). *Teori Hubungan Internasional: Dari Perspektif Klasik Sampai Non-Barat* (1st ed.; Y. S. Hayati, Ed.). Depok: PT RajaGrafindo Persada.

Rozak, R. (2018, April 16). Who is actually meddling in Mexico's elections? Russia or the U.S.? | Panoramas. Retrieved March 18, 2021, from https://www.panoramas.pitt.edu/news-and-politics/who-actually-meddling-mexicos-elections-russia-or-us

Sikkink, K. (2011). The Justice Cascade: How Human Rights Prosecutions are Changing World Politics by Kathryn Sikkink. In *The Norton Series in World Politics* (0 ed.). https://doi.org/10.1007/s12142-015-0357-3

Snow, D. A., Rochford, E. B., Worden, S. K., & Benford, R. D. (1986). Frame Alignment Processes, Micromobilization, and Movement Participation. *American Sociological Review*. https://doi.org/10.2307/2095581

Stryker, S., & Statham, A. (1977). Symbolic Interaction and Role Theory. In *Symbolic Interactionism*.

Untersinger, P. M. (2018, November 8). La France veut relancer les négociations sur la paix dans le cyberespace. Retrieved February 10, 2021, from https://www.lemonde.fr/pixels/article/2018/11/08/la-france-veut-relancer-les-negociations--sur-la-paix-dans-le-cyber-espace_5380571_4408996.html