International Journal of Multicultural and Multireligious Understanding

http://ijmmu.com
editor@ijmmu.com
ISSN 2364-5369
Volume 9, Issue 8
August, 2022
Pages: 442-454

Paris Call as French Diplomacy Instrument

Endah Kurniati; Ahmad Sahide

Master of International Relations, Universitas Muhammadiyah Yogyakarta, Indonesia

http://dx.doi.org/10.18415/ijmmu.v9i8.4070

Abstract

Cyber diplomacy can be defined as diplomacy in the cyber domain or other words, the use of diplomatic resources and the performance of diplomatic functions to secure national interests related to cyberspace. These interests are generally identified in cyberspace or cybersecurity, which often include references to the diplomatic agenda. Cyberspace has become a contested political space, shaped by different interests, norms, and values. In light of this, the Paris Call represents a major effort to create an attractive multi-stakeholder structure for state actors seeking to complement intergovernmental negotiations and similar initiatives. This study uses qualitative research methods, using primary data in the form of journals taken through the website (google scholar, J-Stor, and Scopus). Paris Call for Confidence and Security in Cyberspace testifies to the active role played by France in promoting a safe, stable, and open cyberspace. In practice, the impact of the procedures for implementing the Paris Call principles is not transparently described. However, the Paris Call as an instrument of cyber diplomacy for France has shown success in rebuilding cooperative relations with countries that had previously conflicted with France.

Keywords: *Factors; Immigration; Qur'an, People of the Book; Arabia*

Introduction

Along with the increasing dependence on the internet and computer technology, the interests of the state are increasingly integrated into the realm of cyberspace. The Internet and network technologies have enabled amazing social and economic progress around the world. As new technologies come online and more people connect around the world, the potential benefits of cyberspace seem limitless. Cyber reconnaissance, cyber attacks, hacking, internet censorship, and even technical issues like internet neutrality are now making headlines regularly. Cyberspace has become a contested political space, shaped by different interests, norms, and values.

Over the past two decades, rapid advances in computers, software, communications, and sensing technologies have connected billions of individuals worldwide, integrated economies through connected supply chains, and drive new efficiencies through the Internet of Things (Lete, 2021). The outbreak of the coronavirus pandemic has accelerated this digital transformation. But these advances also bring challenges, including the almost absolute dependence of all developed countries and many developing countries on the integrity of digital networks and systems. Apart from the general resilience of network-based systems, deep digital integration has also created vulnerability to cyberattacks by individual hackers, organized crime, terrorist groups, and even nations.

Starting with denial-of-service attacks against the Estonian government and financial system in 2007, they became more and more destructive. attack Wanna Cry ransomware in 2017 affected hundreds of thousands of computers in 150 countries. hack SolarWinds that targeted government agencies and private companies is considered one of the largest cyberattacks in US history. By one estimate, the world experienced 43 significant cyber incidents in the last quarter of 2020. Cybersecurity concerns have skyrocketed. The increasing division of the Internet along geographic and commercial boundaries and the lack of international consensus on cyber norms make it easier for governments to engage in malicious digital operations. Setting the rules of the game in cyberspace is therefore more important than ever (Lete, 2021).

Cyberspace provides great opportunities for innovation, economic progress, cultural development, and access to information. While its rapid development is proving to be very useful for many human activities, it also brings new threats. New and dangerous practices are developing in cyberspace: cybercrime, manipulation of information, political or economic espionage, attacks on important infrastructure or individuals, theft of personal information or confidential data, and compromise of information and communication systems used by citizens, companies, and institutions. These attacks can come from State or non-State groups that do not respect boundaries. These attacks became increasingly sophisticated and intense. Therefore, it is important to unite the international community to ensure peace and security in the digital space.

Paris Call for trust and security in cyberspace, launched on 12 November 2018 at the Paris Peace Forum, is a call to collectively confront new threats that endanger citizens and infrastructure (Paris Call, 2018). It is based on nine general principles for securing cyberspace. The principles call for protecting individuals and infrastructure, protecting the internet, defending electoral processes, defending intellectual property, preventing the proliferation of malware, ensuring the security of the lifecycle of digital products, ensuring cybersecurity hygiene, avoiding personal hacking, and promoting the acceptance of international norms in the world. virtual.

In light of this, the Paris Call represents a major effort to create a multi-stakeholder structure that is attractive to both state and non-state actors, seeking to complement intergovernmental negotiations and similar initiatives. This paper describes the Paris Call For trust and security in cyberspace in cyber diplomacy for the French state.

Literature Study

In the journal Cyber Diplomacy: Towards a Peaceful International Society in the Digital Age by Iskandar Hamonangan and Zainab Assegaff reveals that diplomacy must act as an international communication tool to build common norms and as an effort to manage international politics which aims to minimize friction in international relations to create peace in the international community. If it is associated with diplomacy in cyberspace, cyber diplomacy must play a role as an international communication tool to form shared cyber norms and ways to manage cyberspace to minimize friction in cyberspace (Hamonangan & Assegaff, 2020).

In the journal Cyber Diplomacy: The Making of an International Society in the digital age by Andre Barrinha and Thomas Renard argue that cyber-diplomacy is an emerging international practice that attempts to build a cyber international community, bridging the national interests of countries with the dynamics of world society – the main realm in which cyberspace has developed in the last four decades (Barrinha & Renard, 2017).

In the journal Cyber Diplomacy: Benefits, Developments, and Challenges by Dana Khabbaz, argues that through cyber diplomacy, countries collaborate to respond to and address the cyber dimensions of international conflict, crime, and information security. Cyber diplomacy is not only essential for an effective international response to cyber threats, but states also need to engage in diplomacy to develop the norms that then govern this international collaboration (Khabbaz, 2020). In the journal entitled Diplomacy in Change and Transformation: Cyber Diplomacy by Betul Catal, Cyber diplomacy has increased the speed of information dissemination around the world, is affecting our countries and social structures shortly and will continue to influence. Cyber technology must spread throughout our country. Otherwise, there is always a risk of facing irreparable damage and sanctions. When the above steps and strategies are implemented, we can continue our existence as respectable individuals from a country with positive perceptions around the world (Çatal, 2015).

In the journal entitled International Cybersecurity Norms and Responsible Cyber Sovereigty by Tuba Eldem describes the emergence of international cybersecurity norms by focusing on negotiations held at the United Nations First Committee for more than twenty years. The author argues that the negotiations held under the First Committee on disarmament and international security issues represent the first stage of establishing international rules relating to cyberspace, and the negotiations to be concluded under the United Nations Open Working Group (OEWG) in 2021 are crucial for the transition. International cybersecurity norms from the first stage to the second stage (Eldem, 2021).

In a journal entitled Cyber Diplomacy: A Systematic Literature Review by Amel Attatfa, Karen Renaud, and Stefano De Paoli argues thatDiplomatic action in international relations is a priority because state security is at stake. This security is closely linked to cyberspace and the need to protect critical infrastructure, and the wider population, from the impact of nation-state cyber attacks. Cybersecurity is a key issue in diplomatic relations, as identified by the French White Paper on Defense and National Security as a national priority (Attatfa et al., 2020).

In the title Cybernorms: Analysis of International Norms in France's Paris Call for Trust and Security in Cyberspace by Diko Catur Novanto, Ika Riswanti Putranti, and Andi Akhmad Basith Dir This study seeks to see the importance of the Paris Call that has been carried out by the French government which aims to remind general norms of cyberspace that is not yet popular or to see the formation of international norms in the cyber field. Cyberspace serves to promote democracy and freedom of expression. France made a high-level declaration called the Paris Call for Trust and Security in Cyberspace in 2018, to maintain stability in cyberspace. Through the Paris Call, France is trying to establish international norms in the cyber realm known as Cybernorms. This norm has been supported by several state and non-state actors (Novanto et al., 2021).

In a journal entitled The Paris Call and Activating Global Cyber Norms by Bruno Lete argues that the Paris Call for Trust and Security in Cyberspace is the best tool available for multiple actors to interact in inclusive cyberspace governance. It is a platform that helps to develop fresh ideas about cyber norms and incorporate them into intergovernmental negotiations, such as UN processes, even if they are not formally incorporated into them. Its strength is building bottom-up capacity to enforce norms, a fundamental need when providing answers to many problems in cyberspace, including concerns around trust, stability, and security. Governments may still have the prerogative to determine the rules of the game, but the decisions they make will have a far greater impact if they also involve non-governmental entities. Shared responsibility in cyberspace is no longer a foreign concept and the Paris Call community plays a role in accelerating this change (Lete, 2021).

So far, there have been many studies that discuss cyber diplomacy and several studies on Paris Call, but it is still not enough to discuss more deeply what instruments are used and what are the impacts of these instruments.

Theoretical Framework

Cyber diplomacy be defined as diplomacy in the cyber or in other words, the use of diplomacy resources and the performance of diplomacy functions to secure national interests related to cyberspace. These interests are generally identified in cyberspace or cybersecurity, which often include references to the diplomatic agenda. Key issues on the cyber diplomacy agenda include cyber security, cyber crime, trust building, internet freedom, and internet governance. Therefore, cyber diplomacy is carried out in whole or in part by diplomats, meetings in a bilateral format (such as the US-China dialogue) or in multilateral forums (such as at the United Nations). Outside of traditional diplomacy powers, diplomats also interact with various non-state actors, such as leaders of internet companies (such as Facebook or Google), technology entrepreneurs, or civil society organizations. Diplomacy can also involve empowering oppressed voices in other countries through technology. Although this establishes a fairly broad range of activities, it allows us to firmly place cyber diplomacy as an institution of the international community, even when interacting with actors from the world community (Barrinha & Renard, 2017).

When considering the emergence of cyber diplomacy, it is important to first understand the logic underlying cooperation in this policy domain. Cyberspace collects several characteristics that frame diplomatic engagement among stakeholders. First of all, it is a global domain that connects countries and citizens around the world in various ways, generating interactions and friction between them. Furthermore, cyberspace is usually considered a “global common”, defined as “a resource domain to which all countries have legal access” (Buck, 1998).

The two main functions of diplomacy are to create peace in the international community, namely as an international communication tool to build common norms and as an effort to minimize friction in international relations. If it is associated with diplomacy in cyberspace, cyber diplomacy must function as an international communication tool to build shared cyber norms and as an effort to minimize friction in cyberspace. By carrying out the governance and communication functions in global cyberspace, the peaceful use of cyberspace can be realized (Hamonangan & Assegaff, 2020).

The principles of the international community clash with the competitive nature of cyberspace where the main force is to promote competing visions, interests, and values for cyberspace. Other relevant characteristics of this realm include the difficulty of attribution of cyber attacks and intrusions, hindering trust among stakeholders; gains from offense over defense capacity, favors aggressive behavior; or the digital divide between major cyber powers and developing countries, creating global vulnerabilities. All of these characteristics make international cyber relations and cyber governance extremely complex and fragile, but at the same time make diplomacy even more necessary, especially concerning (but not limited to) trust-building mechanisms and the development of international norms and values. score.

Research Method

In this research, the method used is the descriptive qualitative method. Collecting data using literature study (library study) by collecting secondary data related to topics related to the research title, then understanding carefully. For secondary data sources, researchers used data taken online from Google Scholar, J-Stor, and Scopus. The data that has been obtained is analyzed by reading, studying, analyzing, and comparing various library sources, so that conclusions can be drawn from the problems discussed using descriptive writing.

Discussion

Cyberspace

In general, the concept of space in "Cyberspace" tends to be abstract and mathematical without the duality of volume. Therefore, cyberspace in the conventional sense is just cyberspace, digitally created based on various infrastructures such as computers, networks, data and information, hardware and software, etc. On the other hand, it is a general term in computer technology that is conceptualized as a virtual environment with which humans can interact. Unsurprisingly, the term cyberspace has been inconsistently understood in various dictionaries, official government sources, and literature. Multiple definitions of cyberspace have evolved for different purposes or emphases over the years.

Barrinha explains that cyber information was initially claimed to be purely a technical issue, then became an external aspect of domestic policy, until it was finally recognized as the main topic of foreign policy. They further argue that at the turn of the first decade of the twenty-first century, several countries using major cyber powers issued their first cybersecurity strategies, at a time when cyberspace and infrastructure were increasingly considered strategic assets (Barrinha & Renard, 2017).

In international relations, cyberspace has now become a significant focus. This topic has become mainstream because most of the world's actors have outlined their foreign policies and adopted various steps to pursue their strategic goals in cyberspace. In addition, there are also concerns about national security in cyberspace, so that cyberspace becomes a contested political space, shaped by unequal interests, norms, and values. The politicization of cyberspace has made diplomats have an important role in analyzing and mediating existing cases.

It is foreseeable that the common cyberspace should be a diversified future world characterized by explosive digitization, holistic internalization, ubiquitous intelligence, and incremental virtualization. Therefore, taking into account the features and the three main components (existence, interaction, and application/services) of cyberspace in general, the main issues become increasingly serious, such as:

1. Existence: Identification, naming, representation, modeling, expression of various types of existence; spacetime consistency of existence in different spaces.
2. Interaction: Heterogeneous transformation of data/information exchange and communication between existences; language/linguistic variations and protocols.
3. Applications/Services: Sensing, capturing, processing, and computing big data; request discovery; resource storage and management; maintenance and update; energy consumption and management; security and privacy for applications and services. (Ning et al., 2018).

Cyberspace can be seen as the infrastructure of all data stored, analyzed, and streamed. All of the above scenarios are based on cyberspace. It includes all computing, communication, and storage technologies like IoT (Internet of Things), cloud computing, big data, etc.

Cyber Security

Cybersecurity was first used by computer scientists in the early 1990s to emphasize a range of insecurity associated with computer networks but later moved beyond the technical concept of computer security when proponents argued that threats posed by technology digital can have devastating social effects (Hansen & Nissenbaum, 2009).

Cybersecurity issues have been largely the domain of computer experts and specialists since the Internet started as a small community where layers of authentication codes were not required and the development of norms was simple. But the growth of the Internet changed everything. Cyberspace is not only an arena for business and social activity, but also an environment for crime, hacking, and terrorism.

Governments, private companies, and non-state actors are making efforts to develop the much-needed capabilities to secure their resources and activities in cyberspace. Foreign policymakers and International Relations (IR) scholars struggle to understand the technological and structural characteristics of cyberspace, which differ from traditional security concerns. Among them, the key to understanding the magnitude of the potential cyber threat is the character of the Internet as a complex network. Cyber threats are constantly evolving, and increasingly blurring the distinctions between the civil and military domains, non-state and state actors, and even human and non-human actors (Sangbae, 2014).

Overall, cybersecurity issues with understanding various cyber attacks and designing appropriate defense strategies that maintain several properties are defined as follows:

- Confidentiality is a property used to prevent access and disclosure of information to individuals, entities, or unauthorized systems.
- Integrity is a property used to prevent unauthorized modification or destruction of information.
- Availability is a property used to ensure timely and reliable access to information systems and assets to authorized entities (Sarker et al., 2020).

The term cybersecurity applies in a variety of contexts, from business to mobile computing, and can be divided into several general categories. It is -network security which mainly focuses on securing computer networks from cyber attackers or intruders; application security which takes into account keeping software and devices free from cyber risks or threats; information security which mainly considers the security and privacy of relevant data; operational security which includes the process of handling and protecting data assets. A typical cybersecurity system consists of a network security system and a computer security system that contains a firewall, antivirus software, or intrusion detection system (Mukkamala et al., 2005).

Cyber Crime

Cybercrime is the latest and perhaps the most complex problem in cyberspace. "Cybercrime can be said to be a species, which belongs to the conventional crime class, and where the computer is the object or subject of an act that constitutes a crime" "Any criminal activity that uses a computer either as a tool, target, or means to perpetuate further crime including within the scope of cybercrime" (Dashora & Patel, 2011).

Cybercrime is closely related to the existence of security in cyberspace which must always experience the development of a security system so that it can prevent leakage of digital security systems. Cybercrime (or 'pure' cybercrime) is an offense that can only be committed using a computer, computer network, or other forms of information communication technology (ICT). This includes the spread of viruses or other malware, hacking, and distributed denial of service (DDoS) attacks (McGuire & Dowling, 2013).

The target actors are devices, hardware, software, and victims' personal information. The nature of these cybercrimes is that the perpetrators and victims are invisible, adding a unique complexity to this type of cybercrime. The advantage of perpetrators in cybercrime activity is anonymity of perpetrators, which makes it easier to hide their identities. There is also a time lag where if the perpetrator commits a crime in cyberspace, the perpetrator can more freely eliminate evidence by deceiving and preventing responses from efforts made by law enforcement agencies.

A general definition of cybercrime may be "an unlawful act in which the computer is the tool or the target or both." Computers can be used as a tool in the act of cybercrime. Cybercrime itself most often occurs through malware attacks.

Malware is software created to enter and sometimes damage computer systems, networks, or servers without the owner knowing. The term malware is a combination of two words, namely malicious "meaning intent" and software "software". Of course, the goal is to damage or steal data from the device that is entered. For example, stealing data, spying on the victim's online behavior to deleting the desired data (Yasin, 2018).

The first example of the most destructive and deadly malware attack is the spyware attack called WannaCry 2017. These spyware attacks hospitals and factories around the world. The WannaCry attack is also huge. In the four days following the spread of the WannaCry attack, more than 200,000 computers in 150 countries, including the airline company Boeing, have been disabled. If the total losses due to the WannaCry ransomware itself range from USD 4-8 billion or Rp. 112.9 billion (Mamduh, 2021).

The next and no less exciting example of a Malware case is the Pegasus Spyware attack case in November 2019, where around 1,400 smartphones were targeted by Pegasus attacks via WhatsApp calls. Pegasus is known to be used to spy on politicians, activists, journalists, and governments in several countries around the world. This spyware, which was developed by an Israeli technology company, NSO Group, has a reliable ability to spy on smartphone users (Android and iOS) and steal their data. When the phone rings, Pegasus will then be installed on the victim's smartphone without having to be picked up by the owner. In addition to web links and application security vulnerabilities, this spyware can also be installed on devices that can send signals to smartphones, one of which is a wireless transceiver (Clinten, 2021).

The next example of malware is RottenSys, which was discovered by security researchers from Check Point Mobile Security in 2018. This malware has infected nearly 5 million smartphones from several well-known brands. RottenSys is a high-level malware that disguises itself as a device to help manage Wi-Fi connections. After that, this malware immediately downloads and installs the codes using the "DOWNLOAD_WITHOUT_NOTIFICATION" permission which does not require user interaction at all. As a result, the infected device will receive advertisements and provide a loophole for hackers to take over the device (Mamduh, 2021).

The Petya malware attack took place in June 2017. This Petya attack initially attacked a company in Ukraine. Then Petya spread to several countries such as France, Germany, Italy, Poland, the United Kingdom, and the United States. In Europe and America, the most impacted country is Ukraine. While WannaCry has taken a major toll on the healthcare infrastructure of Britain's National Health Service (NHS), Petya has claimed the lives of several port operators in New York, Rotterdam, and Argentina, as well as the government system in Kiev, as well as some large companies such as Rosneft, Maersk. , WPP Plc. Even the Petya infection has forced operators of the Chernobyl nuclear facility to follow manual procedures in carrying out activities within the Chernobyl nuclear facility (Prayudi, 2017).

Paris Call

Cybersecurity concerns have skyrocketed increasing the division of the Internet along geographic and commercial boundaries, and the lack of international consensus on cyber norms makes it easier for governments to engage in malicious digital operations. Setting the rules of the game in cyberspace is, therefore, more important than ever. The list of national, bilateral, or multilateral initiatives to find solutions to these problems continues to grow. Last December, the European Union adopted a new cybersecurity strategy aimed at making critical physical and digital entities more resilient. In January, the United States Department of State launched a new Bureau for Cybersecurity and Emerging Technologies to help lead diplomatic efforts around the issue, while China and Indonesia signed a memorandum of understanding on capacity-building development for Internet security.

However, the United Nations remains the most significant body for determining the rules of behavior in cyberspace at the global level. Within the United Nations First Committee, countries entrusted two entities to lead the negotiations: a Group of Governmental Experts (GGE) established in 2004, and an Open-Ended Parallel Working Group (OEWG) established in 2018. norms and standards of state behavior in cyberspace, especially when countries agreed to adopt two groundbreaking GGE reports in 2013 and 2015. But the volatile relationship on cybersecurity between major powers such as China, the European Union, Russia, and the United States makes compromises and consensus increasingly difficult to find; the boundaries of the intergovernmental process for establishing or implementing norms are being exposed. In 2013, GGE recognized the need to think about new cyber governance practices that included a multi-stakeholder model rather than relying solely on an intergovernmental approach. Cyberspace and the state behavior associated with it is a complex and interdisciplinary area. This demands policy development that is inclusive and expertise-driven, and that engages a wide range of stakeholders (Lete, 2021).

Initiatives extending cybersecurity responsibilities to non-state actors have proliferated over the past few years. Examples include the Global Commission on the Stability of Cyberspace, Cybersecurity Tech Accord, and Paris Call.

The making Paris Call occurred because of a threat that occurred in cyberspace. Where attacks are carried out by individuals or even supported by state actors or under the influence of non-state actors. Awareness by France emerged in June 2010, as evidenced by the emergence of Stuxnet at the time, which attacked the system of uranium enrichment sites. Stuxnet's ultimate goal is to sabotage the facility by reprogramming its programmable logic controllers. External intervention in elections is also a threat to democracy, as happened in Kenya in 2017, where there was influence from Cambridge Analytica during elections, and in 2018 in Mexico, as seen in a large number of registrants on voting sites, especially from Russia. Then attacks on critical infrastructures, such as the attack on French TV network TV5 Monde in 2015 (Melvin & Botelho, 2015). This cyber threat to France has made cyberspace unstable and insecure, not only threatening state actors and the industrial sector but also threatening democracy and human rights (Novanto et al., 2021).

The Paris Call For trust and security in cyberspace testifies to the active role played by France in promoting a safe, stable, and open cyberspace. A high-level political declaration, this text marks a new mobilization on the fundamental issue of stability in cyberspace. Presented on 12 November 2018, at the Paris Peace Forum and endorsed by the President of the Republic at UNESCO before the Internet Governance Forum, it testifies to France's ability to mobilize broadly around its vision of regulation in cyberspace. Since 2018, 80 states have joined this partnership along with many nonprofits and universities. Hundreds of technology companies, including major industry players such as Microsoft Corp, Google LLC, and Hewlett Packard Enterprise Co, have also supported Paris Call (Deutscher, 2021).

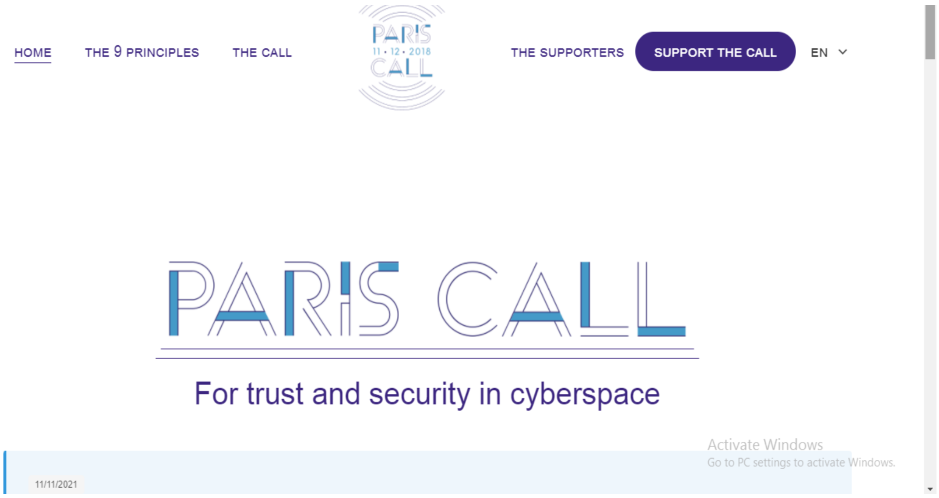
HOME
THE 9 PRINCIPLES
THE CALL
PARIS 11 · 12 · 2018 CALL
THE SUPPORTERS
SUPPORT THE CALL
EN
PARIS CALL
For trust and security in cyberspace
Activate Windows
Go to PC settings to activate Windows.
11/11/2021

Figure 1: PlatformParis Call

(*source: https://pariscall.international/en/*)

The inclusive approach of the Paris Call underscores the need for a multi-stakeholder approach to develop standards and good practices that will enable us to take advantage of a reliable and secure way of the possibilities offered by the digital revolution. France now intends to reflect, with its country partners but also with the private sector and civil society, on the specific roles and responsibilities of private actors in strengthening international cyber stability and security.

The Paris Call sets out nine general principles for securing cyberspace. The principles call for protecting individuals and infrastructure (preventing and recovering from malicious cyber activity that threatens or causes significant, indiscriminate, or systemic harm to individuals and critical infrastructure.), protecting the internet (preventing activity that intentionally and substantially impairs availability). or the public core integrity of the Internet.), defending electoral processes (strengthening our capacity to prevent malicious interference by foreign actors aimed at undermining the electoral process through malicious cyber activity), protecting intellectual property (preventing theft of ICT-enabled intellectual property, including confidential trade or other confidential business information, with the intent of giving a company or commercial sector a competitive advantage), preventing the proliferation of malware (developing ways to prevent the proliferation of malicious software and practices intended to harm.), ensuring digital product lifecycle security (strengthening the security of digital processes, products and services, throughout their lifecycle and supply chain), ensuring cybersecurity cleanliness (strengthening the security of digital processes, products and services, throughout their lifecycle and supply chain.), avoiding personal hacking (taking steps to prevent non-State actors, including the private sector, from hacking, for their own purposes or those of other non-State actors.) and promoting the acceptance of international norms in cyberspace (promoting broad acceptance and application of international norms of responsible behavior and trust-building measures in cyberspace.).

Implementation of the Paris Call

One year since the launch of the Paris Call for Trust and Security in Cyberspace, Jean-Baptiste Lemoyne, French Minister of State in collaboration with the Ministers of Europe and Foreign Affairs, announced remarkable progress in securing cyberspace. The Paris Call signatory community is growing and taking new initiatives to thwart attacks that threaten democracy, the economy, and public services. This commitment to the Paris Call from around the world demonstrates a widespread, global multi-stakeholder consensus on what is acceptable behavior in the world (Frank, 2019).

Two years since the Paris Call for Trust and Security in Cyberspace was launched, it has brought government, industry, civil society, and academia together on a common path to greater stability in cyberspace. The Cybersecurity Tech Accord was one of the initial backers of the initiative. Since then, Paris Call's backers have grown to include more than 1,000 entities, including nearly 80 governments, more than 700 companies, and more than 350 civil society organizations, 79 of which are non-governmental organizations. government. During that time, the Cybersecurity Technology Agreement also expanded to include more than 150 signatories who are committed to advancing and complying with the nine principles enshrined in the Paris Call (TechAccord, 2021).

In November 2020, the French government announced the formation of six working groups, to advance international norms and cooperate on concrete initiatives that build on the principles of the Call and improve overall cybersecurity. The working group will look at 1) fostering community, 2) engaging developing countries, 3) supporting continued UN negotiations with a strong multi-stakeholder approach, 4) advancing international norms, 5) building a stability index and 6) offering tools concrete to supporters (Letstalkcyber, 2021).

Quoted from statista.com the annual number of worldwide malware attacks from 2015-2021.

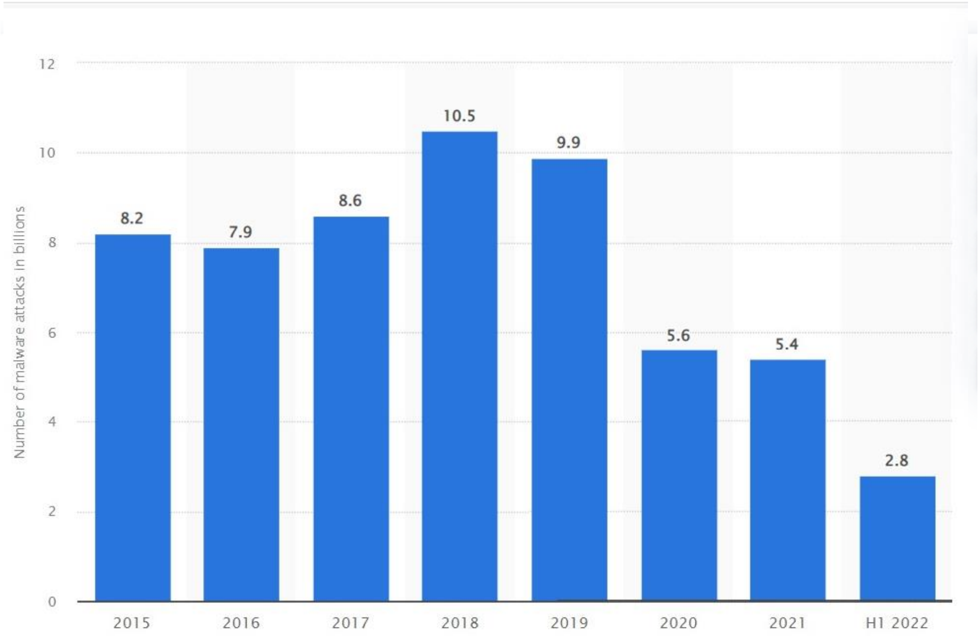

Figure 2 Annual number of malware attacks worldwide from 2016 to 2022
(sumber: https://www.statista.com/statistics/873097/malware-attacks-per-year-worldwide/)

From the above, it can be seen from 2018 when the new Paris Call was launched. around 10.5 Billion Malware attacks in 2019 were reduced by at least 0.6. In 2021 attacks saw a reduction in the number of Malware attacks to 5.4 billion, a decrease of about 4.4 billion from the previous year.

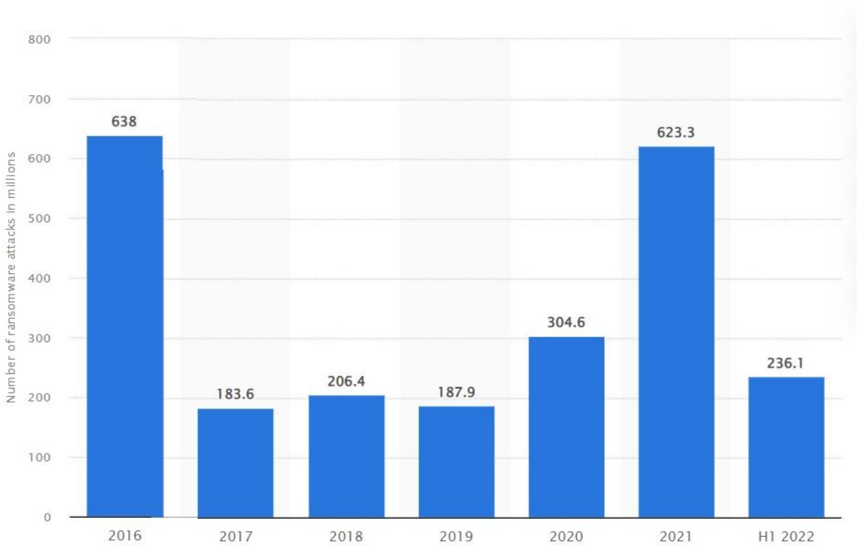

Figure 3 Annual number of ransomware attacks worldwide from 2016 to 2022
(sumber: https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/)

The figure above shows the number of Ransomware attacks worldwide starting from 2016 until 2020. From 2018 to 2019 there was a decrease, although only slightly, in 2020 Ransomware attacks increased more than in the previous year. Attacks increased in number in 2020 and 2021 because cyber took advantage of the situation where the Covid-19 virus began to spread, and attacks were infiltrated through applications under the guise of Covid-19 information services. They take advantage of the public's curiosity about Covid-19, for example, the Covidlock platform (Burhan, 2021).

Since 2021 the United States has signed up for The Paris Call for Trust and Security in Cyberspace – an international effort to ensure the internet remains free and open, and an agreement to limit critical infrastructure from electronic attacks by sovereign states and other actors.

A White House statement explained that the United States' decision to adopt the Paris Call reflects the Biden-Harris Administration's priority to renew and strengthen America's engagement with the international community on cyber matters. The statement added that this announcement builds on the United States' ongoing efforts to improve cybersecurity for its citizens and businesses (Sharwood, 2021).

The United States of America (USA) strongly promotes peacetime norms which are expressed primarily in terms of the exercise of the innate right to self-defense and the legal responsibilities of states, including cyber precautions. With ransomware rampant in the United States and the Biden administration having made several calls for international cooperation to stop it, the White House sees and supports the Paris Call that can provide several advantages. One of the goals of the Paris Call effort is to isolate and criticize those who choose not to participate.

The call is also a signature diplomatic initiative for French President Emmanuel Macron, and the United States needs it back after the creation of the US/UK/Australia AUKUS pact that cost France its $65 billion submarine-building contract with Australia. Therefore, US support for the Call was announced alongside a deeper collaboration with France in space. America is committed to joining the Space Climate Observatory (SCO) – an effort to collect data in space to help with the terrestrial response to climate change. The two countries will also collaborate on security issues related to space (Sharwood, 2021).

Conclusion

Paris Call For trust and security in cyberspace is the best tool available for multiple actors to interact in inclusive cyberspace governance. It is a platform that helps to develop fresh ideas about cyber norms and incorporate them into intergovernmental negotiations, such as the UN process, although not formally incorporated into them.

Reaching out to stakeholders in developing and non-democratic countries remains a challenge. More capacity building and resources are needed to reach them. The more and more diverse the signatories, the better the Paris Call can credibly engage with the UN or other groups on cyber norms. In this sense, the Paris Call's value beyond these nine principles also has the potential to bind its diverse community members to universal values around human rights or the rule of law.

In its development, Paris Call has received a lot of support from various countries, both from companies and individuals. The impact of the procedures for implementing the Paris Call principles is not transparently described. The Paris Call as an instrument of cyber diplomacy for France has shown success in re-establishing cooperation with countries that had previously conflicted with France. Such as the United States which left the Paris agreement in the Trump era, which considered the Paris agreement to have been shackled and did not produce any action to reduce greenhouse gas emissions, and the conflict after the formation of the US/UK/Australia AUKUS pact which made France lose its contract to build a submarine worth Rp. $65 billion with Australia.

Reference

Attatfa, A., Renaud, K., & de Paoli, S. (2020). Cyber diplomacy: A systematic literature review. *Procedia Computer Science*, *176*, 60–69. https://doi.org/10.1016/j.procs.2020.08.007.

Barrinha, A., & Renard, T. (2017). Cyber-diplomacy: the making of an international society in the digital age. *Global Affairs*, *3*(4–5), 353–364. https://doi.org/10.1080/23340460.2017.1414924.

Buck, S. J. (1998). *The Global Commons : An Introduction*.

Burhan, F. A. (2021). *Serangan Ransomware Melonjak 752% Selama 2020, Memicu Tindak Kriminal - Teknologi Katadata.co.id*. https://katadata.co.id/safrezifitra/digital/60ad3d6ef2fa1/serangan-ransomware-melonjak-752-selama-2020-memicu-tindak-kriminal.

Çatal, B. (2015). *DIPLOMACY IN CHANGE AND TRANSFORMATION: CYBER DIPLOMACY*. *February 2018*, 43–54.

Clinten, B. (2021). *Apa Itu Spyware Pegasus dan Bagaimana Cara Kerjanya? Halaman all - Kompas.com*. https://tekno.kompas.com/read/2021/07/26/13120047/apa-itu-spyware-pegasus-dan-bagaimana-cara-kerjanya?page=all.

Dashora, K., & Patel, P. P. (2011). Cyber Crime in the Society: Problems and Preventions. *Journal of Alternative Perspectives in the Social Sciences*, *3*(1), 240–259.

Deutscher, M. (2021). *US joins the Paris Call for Trust and Security in Cyberspace - SiliconANGLE*. https://siliconangle.com/2021/11/11/us-joins-paris-call-trust-security-cyberspace/.

Eldem, T. (2021). International Cybersecurity Norms and Responsible Cyber Sovereignty. *İstanbul Hukuk Mecmuası*, *79*(1), 347–378.

Frank, J. (2019). *Paris Call: Growing Consensus on Cyberspace - Microsoft On the Issues*. https://blogs.microsoft.com/on-the-issues/2019/11/12/paris-call-consensus-cyberspace/.

Hamonangan, I., & Assegaff, Z. (2020). CYBER DIPLOMACY: MENUJU MASYARAKAT INTERNASIONAL YANG DAMAI DI ERA DIGITAL. *Padjadjaran Journal of International Relations (PADJIR)*, *1*(3), 311–333. https://doi.org/10.24198/padjir.v1i3.26246.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the copenhagen school. *International Studies Quarterly*, *53*(4), 1155–1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x.

Khabbaz, D. (2020). *Cyber Diplomacy: Benefits, Developments, and Challenges*. https://static1.squarespace.com/static/58011083197aea95712e1bf4/t/5ed5230bb568f07c9647c189/1591026443959/Cyber+Diplomacy+Benefits%2C+Developments%2C+and+Challenges.pdf.

Lete, B. (2021). *The Paris Call and Activating Global Cyber Norms*. 1–14. https://www.gmfus.org/news/paris-call-and-activating-global-cyber-norms.

Letstalkcyber. (2021). *Six Paris Call Working Groups Announced :: Let's Talk Cyber*. https://letstalkcyber.org/news/six-paris-call-working-groups-announced.

Mamduh, N. (2021). *7 Contoh Kasus Malware Paling Merusak dan Mematikan*. https://telset.id/ngehits/serangan-malware-paling-merusak-dan-mematikan/.

McGuire, D. M., & Dowling, S. (2013). Cyber crime: A review of the evidence Summary of key findings and implications. *Mercenaries in Asymmetric Conflicts*, *October 2013*, 273–308. https://doi.org/10.1017/cbo9781139208727.008.

Mukkamala, S., Sung, A., & Abraham, A. (2005). Cyber security challenges: Designing efficient intrusion detection systems and antivirus tools. *Enhancing Computer Security with Smart Technology.*, 125–188.

Ning, H., Ye, X., Bouras, M. A., Wei, D., & Daneshmand, M. (2018). General cyberspace: Cyberspace and cyber-enabled spaces. *IEEE Internet of Things Journal*, *5*(3), 1843–1856. https://doi.org/10.1109/JIOT.2018.2815535.

Novanto, D. C., Putranti, I. R., & Basith Dir, A. A. (2021). Cybernorms: Analysis of International Norms in France's Paris Call for Trust and Security in Cyberspace. *Journal of Islamic World and Politics*, *5*(2), 326–342. https://doi.org/10.18196/jiwp.v5i2.11656.

Paris Call. (2018). *PARIS CALL FOR TRUST AND SECURITY IN CYBERSPACE*. *November*, 1–4. https://pariscall.international/en/call.

Prayudi, Y. (2017). *Habis WannaCry, Terbitlah Petya – PUSFID*. https://forensics.uii.ac.id/habis-wannacry-terbitlah-petya/.

Sangbae, K. (2014). Cyber Security and Middle Power Diplomacy: A Network Perspective. *The Korean Journal of International Studies*, *12*(2), 323–352.

Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. *Journal of Big Data*, *7*(1). https://doi.org/10.1186/s40537-020-00318-5.

Sharwood, S. (2021). *USA agrees to Paris Call for Trust & Security in Cyberspace • The Register*. https://www.theregister.com/2021/11/11/usa_supports_paris_call/.

TechAccord. (2021). *Paris Call for Trust and Security in Cyberspace: Six Working Groups Launched to Advance Global Cybersecurity | Cybersecurity Tech Accord*. https://cybertechaccord.org/paris-call-for-trust-and-security-in-cyberspace-six-working-groups-launched-to-advance-global-cybersecurity/.

Yasin. (2018). *Apa itu Malware? Pengertian dan Cara Mengatasinya - Niagahoster*. https://www.niagahoster.co.id/blog/apa-itu-malware/.

Copyrights