IRSEM
INSTITUT DE RECHERCHE STRATÉGIQUE DE L'ÉCOLE MILITAIRE

EU CYBER DIRECT

November 2020

THE GEOPOLITICAL REPRESENTATIONS OF INTERNATIONAL LAW IN THE INTERNATIONAL NEGOTIATIONS ON THE SECURITY AND STABILITY OF CYBERSPACE

François Delerue, Frédérick Douzet and Aude Géry

REPORT – No. 75

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

The EU Cyber Direct project supports EU cyber diplomacy efforts and consequently contributes to the development of a secure, stable and rules-based international order in cyberspace through extensive dialogues with strategic partner countries and regional/international organisations. The EU Cyber Direct project is funded by the European Commission under the Partnership Instrument, International Digital Cooperation project: Trust and Security in Cyberspace.

Website: https://eucyberdirect.eu

Twitter: @EUCyberDirect

THE GEOPOLITICAL REPRESENTATIONS OF INTERNATIONAL LAW IN THE INTERNATIONAL NEGOTIATIONS ON THE SECURITY AND STABILITY OF CYBERSPACE

François Delerue

Research Fellow in Cyberdefence and International Law at IRSEM

Frédérick Douzet

Professor, French Institute of Geopolitics, Director of GEODE

Aude Géry

Post-doctoral researcher, GEODE

To quote this publication

François Delerue, Frédérick Douzet and Aude Géry, *The geopolitical representations of international law in the international negotiations on the security and stability of cyberspace*, Report No. 75, IRSEM/EU Cyber Direct, November 2020.

Dépôt légal

ISSN : 2268-3194

ISBN : 978-2-11-152716-4

RECENTLY PUBLISHED

74. *Réalités opérationnelles de l'environnement arctique. Approches transdisciplinaires et transsectorielles des impacts du changement climatique dans les sous-régions arctiques*

Magali VULLIERME (dir.)

73. *La Diplomatie des garde-côtes en Asie du Sud-Est*

Benoît de TRÉGLODÉ et Éric FRÉCON (dir.)

72. *La Criticité des matières premières stratégiques pour l'industrie de défense*

Raphaël DANINO-PERRAUD

71. *Le Sri Lanka, l'Inde et le Pakistan face à la* Belt and Road Initiative *chinoise*

Raphaëlle KHAN

70. *Risques géopolitiques, crises et ressources naturelles. Approches transversales et apport des sciences humaines*

Sarah ADJEL, Angélique PALLE et Noémie REBIÈRE (dir.)

69. *Contemporary Society-centric Warfare: Insights from the Israeli experience*

Jonathan (Yoni) SHIMSHONI and Ariel (Eli) LEVITE

68. *Les États-Unis divisés : la démocratie américaine à l'épreuve de la présidence Trump*

Frédérick GAGNON, Frédéric HEURTEBIZE et Maud QUESSARD (dir.)

67. *Le Financement chinois dans le secteur des transports en Afrique : un risque maîtrisé*

Juliette GENEVAZ et Denis TULL

66. *L'Expérience militaire dans les médias (2008-2018). Une diversification des formes de récits*

Bénédicte CHÉRON

TEAM

Director
Jean-Baptiste JEANGÈNE VILMER

Scientific Director
Jean-Vincent HOLEINDRE

General Secretary
CRG1 (2S) Étienne VUILLERMET

Head of Support Staff
Caroline VERSTAPPEN

Editor
Chantal DUKERS

Find IRSEM on social medias:

@ https//www.irsem.fr

@IRSEM1

DISCLAIMER: One of IRSEM's missions is to contribute to public debate on issues relating to defence and security. The views expressed in IRSEM's publications are the authors' alone and are in no way representative of an official Ministry of the Armed Forces stance.

ABOUT IRSEM

Founded in 2009, the Institute for Strategic Research (IRSEM) is a research institute attached to the Ministry of the Armed Forces' General Directorate for International Relations and Strategy (DGRIS). The institute employs a staff of forty-five civilian and military personnel, and its primary aim is to further French research on defense and security stakes.
The research team is divided into six departments:
• The 'Transatlantic Studies' department analyses strategic and geopolitical developments in North America, Europe, Russia and the Eurasian areas which include Eastern Europe (Moldova, Ukraine, Belarus), the South Caucasus (Armenia, Georgia, Azerbaijan) and the five Central Asian countries. The department's research team analyzes competition for power in that region, the evolving role of NATO, maritime safety, and strategies of influence.
• The 'Africa – Asia – Middle East' department analyses strategic and geopolitical developments in those regions through the following themes: political authoritarianism and economic liberalization in emerging countries; the role of the army and the security apparatus in the way states and societies function; strategic and regional security challenges; ideologies, nationalisms and the redefining of regional interstate balances.
• The 'Weaponry and Defense Economics' department's team focuses on economic issues related to defense. More broadly, it includes strategic issues resulting from technological developments, problems of access to natural resources and those related the environment. The department's research is based on an interdisciplinary approach, both qualitative and quantitative, which mobilizes various scientific fields: defense economics, history of technologies, and geography.
• The 'Defense and Society' department is at the crossroad of issues specific to military circles and of the social evolutions they face. The following aspects are put forward in particular: the link between civilian society and the armed forces, sociology of military personnel, integration of women in armed conflicts, relations between political power and the Army as an institution, renewal in the forms of commitment, socialization and integration of the youth, rise of

radicalisms. Beyond its research activities the Defense and Society department also promotes defense issues within civilian society, towards all its constituents, including those in the academia.

• The 'Strategies, Norms and Doctrines' department is dedicated to the study of contemporary armed conflicts, particularly in their political, military, legal and philosophical dimensions. The main threads of research developed in its publications and the events it arranges relate to international law, in particular from a technological standpoint (cyber, artificial intelligence, robotics), deterrence doctrines, arms control, including nuclear disarmament and the fight against such proliferation. The transformations of international relations and in their stakes in terms of power and security, as well as the philosophy of war and peace are also part of its field of study.

• The 'Intelligence, Anticipation and Hybrid Threats' department conducts research on the «knowledge and anticipation» strategic function put forward by the Defense White Paper since 2008. This programme therefore aims at contributing to a more subtle understanding of intelligence in its broadest sense (i.e. as information, process, activity and organization); secondly, it aims at contributing to the consolidation of analytical approaches, particularly in the field of anticipation; finally, it works on the different dimensions of so-called "hybrid" warfare, particularly on information manipulation. The field also contributes to strengthening the hybrid nature of the IRSEM by publishing notes which are halfway between academic research and open source intelligence analysis.

BIOGRAPHIES

Dr François Delerue is a research fellow in cyberdefense and international law at the Institute for Strategic Research (Institut de Recherche Stratégique de l'École Militaire – IRSEM) and a lecturer at Sciences Po Paris. François is also rapporteur for international law in the EU Cyber Direct project. François' research concerns cyberdefense and cybersecurity, specifically their legal, policy and strategic dimensions. His research focuses on international law obligations, norms and international cooperation, as well as on the various actors involved in this area, including States, private companies, non-governmental organisations. More broadly, he is interested in how new technologies and activities (space activities, cyber, robotics and artificial intelligence) challenge international law and international relations. His book titled *Cyber Operations and International Law* has been published by Cambridge University Press in March 2020.

Contact: francois.delerue@irsem.fr
Twitter: @francoisdelerue

Frédérick Douzet is a Professor of geopolitics at the French Institute of Geopolitics at University Paris 8 and the director of GEODE. She works on the strategic and geopolitical aspects of the digital revolution. She is a member of the Global Commission on the Stability of Cyberspace since February 2017 and of the Ethics Committee of the French Ministry of the Armed Forces since January 2020. In 2017, she was a member of the drafting committee of the *Strategic Review for Defense and National Security*. From 2013 to 2018 she was the chairwoman of the Castex Chair of Cyberstrategy (IHEDN). She was nominated as a junior member of the Institut Universitaire de France et she received several prizes for her research. In 2020, she edited the issue "Geopolitics of the Datasphere" of the academic journal *Hérodote*.

Contact: fdouzet@gmail.com
Twitter: @geode_science

Aude Géry is a post-doctoral researcher at GEODE, a multisciplinary research and teaching center on the geopolitics of the datasphere. Her PhD was on international law and the counter-proliferation of cyberweapons. She works on the international regulation of information and communication technologies both from a legal and geopolitical aspect. She works on States' legal strategies, international negotiations and international cooperation on these issues.

Contact: gery.aude@gmail.com
Twitter: @AudeGery

SOMMAIRE

ABSTRACT

International law and norms of responsible behaviour are at the heart of the discussions at the United Nations (UN) on Developments in the Field of Information and Telecommunications in the Context of International Security. The purpose of the present study is, therefore, to analyse – and provide food for thought on – the place of international law within the framework of the two processes underway at the UN, the Open-Ended Working Group (OEWG) and the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE). It will also explain how international law is being instrumentalised in the present negotiations.

The study is comprised of three parts. First, it sets out the context in which these two processes arose, their respective mandates, and the place of international law in their work. Secondly, it examines the ambiguities and consequences associated with the distinction between norms of responsible behaviour and international law. Finally, the last part focuses on the interpretation of certain rules of international law, such as, on the one hand, the responses authorised by international law in reaction to a cyber operation and, on the other hand, the principle of sovereignty. The study then analyses the geopolitical motivations behind this.

INTRODUCTION

Almost two years ago, on 12 November 2018, the French president, Emmanuel Macron, launched the Paris Call for Trust and Security in Cyberspace during his speech at the Internet Governance Forum, at the UNESCO headquarters.[1] The shared aspirations of the French authorities and of the private sector led to this unique document. Indeed, for the first time, state and non-state actors – including French and foreign companies – agreed on a common declaration on the security and stability of cyberspace. The supporters of the Paris Call reaffirmed their attachment to "an open, secure, stable, accessible, and peaceful cyberspace, which has become an integral component of life in all its social, economic, cultural, and political aspects" and to the principle that "international law, including the United Nations Charter in its entirety, international humanitarian law and customary international law is applicable to the use of information and communication technologies (ICT) by states".

France's ambition was to reopen international discussions on the regulation of cyberspace, which had ended in stalemate after the failure in June 2017 of the fifth Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE). This failure and the disagreements it underscored led international negotiations into a period of uncertainty and instability. With the Paris Call, France hoped to impose itself as a driving force on those questions, federating the so-called "like-minded states" and pushing for the resumption of the negotiations. That said, power rivalries never stopped prevailing, and it led to the adoption of two competing resolutions by the United Nations General Assembly (UNGA) in December 2018 and to the implementation of two competing negotiation processes. In that context, international law is a central element in the state-level discussions on peace and stability in cyberspace. But international

1. Paris Call for Trust and Security in Cyberspace, 12 November 2018.

law is exposed to contradictory geopolitical representations that complicates these negotiations – for two main reasons.

First, contradictory representations of cyberspace coexist – sometimes within the same state – depending on whether it is described as falling within the purview of state sovereignty or not. On the one hand, cyberspace is perceived as a conquerable space, which would thus not be submitted to state sovereignty, and, for that reason, would require the elaboration of new guidelines to rule behaviours. This representation explains why the applicability of international law on cyberspace is being debated. But, on the other hand, cyberspace is also described as a territory where state sovereignty is exerted, a new way to act.[2] For that reason, the only question worth asking is how existing international law can be applied to cyberspace. Yet, the characteristics of cyberspace complicate the implementation of rules of international law and lead to many debates about their interpretation, their limits, and the means that can be employed to ensure the security and stability of cyberspace.

The second reason is linked to the very nature of international law as it organises the coexistence of states. Any debate on the international regulation of the digital space, and more particularly on international law, fits within existing power rivalries between states. International law is a tool of states' diplomacy, a "strategic object, used and sometimes manipulated by a state based on its perception of a national interest".[3] Hence, states' "external legal policies"[4] vary depending on perceived geopolitical threats. Now, due to exacerbated tensions in cyberspace

2. Alix Desforges, *Approche géopolitique du cyberespace, enjeux pour la défense et la sécurité nationale, l'exemple de la France*, PhD. Dissertation, Université Paris 8 Vincennes-Saint-Denis, 2018, 398 p.; Alix Desforges and Frédérick Douzet, "Du cyberespace à la datasphère. Le nouveau front pionnier de la géographie," *NETCOM*, 32:1-2, 2018, 87-108.

3. Julian Fernandez, "Un enjeu et un moyen de la diplomatie des Etats," *Questions Internationales, A quoi sert le droit international ?*, 49, May-June 2011, 14, (our translation) "*est donc un objet de stratégie, utilisé voire manipulé en fonction de la perception qu'un État se fait de son intérêt national*".

4. Guy Ladreit de Lacharrière, *La politique juridique extérieure*, Economica, 1983, 236 p., (our translation) "*politique juridique extérieure*".

– and in the world at large – international law has become an object of disputes. Incidentally, an analysis of states' positions on international law, and more generally on the international regulation of the digital space, reveals different representations of these threats. It also translates in legal terms states' strategies on these issues and delineates the competing visions of the international legal order.

International law has always been the subject of intense debates between states and has long been used by some of them to counter the technological development of others. Any shrewd observer would note that, within the larger theme of the regulation of the digital space, this has always been a topic of disagreement – since the first resolution of the UNGA in 1998. However, the consensus reached by the GGEs in 2010, 2013, and 2015, as well as the notable progress made back then, have eclipsed the fundamental disagreements on international law.

From the start, international law has been both an important topic and an important source of tensions in the work of the GGEs. The failure of two GGEs, in 2004 and 2017, was partly due to matters of international law. Following the last failure, in 2017, dual dynamics took shape: International law obtained a more central role in states' diplomatic strategies and its instrumentalisation in the discourses opposing those respecting and those not respecting international law, i.e. those defending it and those questioning it.[5] Because it is a natural by-product of power rivalries, it has become a privileged tool in the negotiations on ICTs in the context of international security. Considering the context surrounding the adoption of the resolutions 73/27 "Developments in the field of information and telecommunications in the context of international security" and 73/266 "Advancing responsible state behaviour in cyberspace in the context of international security" in 2018, which respectively created the Open-Ended Working Group (OEWG) and the sixth GGE, as well as the preceding GGE reports on which they base their work, the treat-

5. See, for example: *Joint Statement on Advancing Responsible State Behavior in Cyberspace*, 23 September 2019.

ment of international law has revealed strong oppositions. These disagreements focus, on the one hand, on the necessary means to ensure security and stability in the digital space and, on the other hand, on the content of the negotiations that illustrate the perception of the risk of militarisation of cyberspace associated with the possible forms of responses authorised by international law in reaction to internationally wrongful acts. For all that, negotiating on protective principles, such as the principle of sovereignty, which may limit states' actions on the territory of other states, is not exempt of difficulties because of the entanglement of the issues at stake.

This article aims to analyse and provide food for thought on the role played by international law in the two ongoing processes at the UN, and eventually to present how it has been instrumentalised in the present negotiations. First, we will describe the context during which these two processes were born and what are their mandates. Then, we will focus on the ambiguous (sometimes confusing) role played by norms and international law in the regulation of cyberspace and on the geopolitical motivations underpinning it. Finally, we will examine the geopolitical representations associated with the interpretation of several rules of international law.

I. ELEMENTS OF CONTEXT ON THE GGE AND THE OEWG

The two processes launched by the United Nations General Assembly reflect current geopolitical tensions. If their composition and calendar differ, their mandates are largely similar. A brief reminder of the preceding GGEs and of UN-level discussions on progress in information and telecommunication in the context of international security allows us to measure the progress made and the depth of the work that remains to be done on the matter.

THE PRECEDING GGES AND THE UN-LEVEL DISCUSSIONS ON PROGRESS IN INFORMATION AND TELECOMMUNICATIONS IN THE CONTEXT OF INTERNATIONAL SECURITY

When the Russian Federation introduced the theme of "progress in information and telecommunication in the context of international security" at the United Nations General Assembly in 1998, it started a discussion on the consequences of the development of states' cyber capacities on the security and stability of the world. It led to the adoption of the resolution 53/70 on 4 December 1998. The General Assembly has passed a resolution on the matter every year since.

These resolutions have led to the creation of five successive GGEs: in 2004, 2009, 2012, 2014, and 2016. But they only became truly effective in the 2010s. For example, the participants in the 2004 GGE weren't able to reach a consensus and no final report was adopted. As one of the experts in the Russian delegation later testified: "whether humanitarian international law and international law provided a sufficient regulation of security in international relations in case of a 'hostile' use of information and communication technologies for politico-military reasons was the main stumbling block".[1] Hence, international law was

1. A. A. Streltsov, "International information security: description and legal aspects," *ICTs and International Security,* Disarmament Forum, 2007, 8.

already at the heart of the disagreements among governmental experts. The following three GGEs proved conclusive and led to the adoption of consensual reports in 2010 (document UN A/65/201), 2013 (document UN 1/68/98) and 2015 (document UN A/70/174), which the Secretary General submitted to the General Assembly. The UNGA took note of the three and suggested that member states draw from them. The three reports contain recommendations on confidence building measures susceptible to upholding security and stability of cyberspace, on measures of international cooperation and assistance that could be implemented by the states, and finally norms of responsible behaviour meant to better define what responsible behaviour in cyberspace should be.

Furthermore, the applicability of international law to cyberspace was first recognised in the 2013 final report:

> International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful, and accessible ICT environment.[2]

The 2015 report of the GGE, which was instructed to deal with international law for the first time,[3] went further and dedicated its sixth part to international law, listing several rules. Since then, numerous states have endorsed this approach in their voluntary contributions to the Secretary General of the United Nations.[4]

2. UN, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 24 June 2013, UN Document A/68/98, paragraph 19.

3. UN, Developments in the field of information and telecommunications in the context of international security, Resolution of the UN General Assembly, 27 December 2014, A/RES/68/243.

4. See, among others: UN, Developments in the field of information and telecommunications in the context of international security, Report to the Secretary General, 9 September 2013, UN Document 1/68/156/Add.1; UN, Developments in the field of information and telecommunications in the context of international security, Report to the Secretary General, 30 June 2014, UN Document A/69/112; UN, Developments in the field of information and telecommunications in the context of international security, Report to the Secretary General, 18 September 2014, UN Document 1/69/112/Add.1.

The fifth GGE ended in failure in June 2017. The governmental experts weren't able to come to an agreement leading to the adoption of a consensual final report. Three states refused the inscription in the final report of the applicability of certain branches of international law. Indeed, China, Cuba, and Russia refused to mention and further elaborate on the applicability of the right of self-defence, of the law of countermeasures, and of the law of armed conflicts in the final report. Cuban and Russian governmental experts explained that the endorsement of the applicability of these branches of international law in cyberspace could serve to justify the militarisation of cyberspace,[5] and they pointed at profound divergences in interpreting the law. It is in this very tense context that, eventually, the Open-Ended Working Group and the sixth Group of Governmental Experts were created.

THE OPEN-ENDED WORKING GROUP (OEWG) AND THE SIXTH GROUP OF GOVERNMENTAL EXPERTS (GGE)

The Open-Ended Working Group and the sixth Group of Governmental Experts were created by the resolutions 73/27 and 73/266, adopted within a few days, on 5 and 22 December 2018, respectively, in a context of heightened tensions between the states. For the first time since the discussion started in 1998, two resolutions on ICTs in the context of international security – instead of the usual one – were adopted by the General Assembly, which testified to an apparent rupture between member states and gave the impression that two blocks of states were fighting each other on this topic.

5. Cuba, *71 UNGA: Cuba at the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Representaciones Diplomáticas de Cuba en El Exterior, 23 June 2017; Russia, *Response of the Special Representative of the President of the Russian Federation for International Cooperation on Information Security Andrey Krutskikh to TASS' Question Concerning the State of International Dialogue in this Sphere*, Ministry of Foreign Affairs of the Russian Federation, 29 June 2017.

The context of the creation of two negotiation processes

The resolutions creating the Open-Ended Working Group (OEWG) and the Group of Governmental Experts (GGE) were introduced by two groups of states forming seemingly adversarial blocs. But the reality is more complex and nuanced.

Russia, supported by China and other states,[6] proposed a first draft of resolution in October 2018. It contained a paragraph creating an OEWG and listed not only norms adopted by the GGE in 2015 but also norms taken from the International Code of Conduct for Information Security proposed by the member states of the Shanghai Cooperation Organization in 2015 – and rejected by Western governments. As a response, the United States submitted an alternative draft for a resolution creating a sixth GGE, which was supported by many European countries.[7] Eventually, Russian and co-sponsoring states modified their project to account for the many criticisms they received. But the United States and their co-sponsors didn't retract their own draft. They asserted that the modified Russian draft paving the way for an OEWG still contained unacceptable dispositions and didn't reflect the 2015 GGE final report as well as it claimed. For that reason, two competing resolutions on ICTs in the context of international security were debated in the First Committee of the UNGA, one promoted by Russia, the other by the United States.

Heightened tensions between the states surrounded the debates. Hence, according to the press communiqué describing

6. Algeria, Angola, Azerbaijan, Belarus, Bolivia, Burundi, Cambodia, China, Cuba, Eritrea, the Russian Federation, Kazakhstan, Madagascar, Malawi, Namibia, Nepal, Nicaragua, Uzbekistan, Pakistan, the Syrian Arab Republic, the Democratic Republic of Congo, Samoa, Sierra Leone, Surinam, Tajikistan, Turkmenistan, Venezuela and Zimbabwe. See: UN Document A/C.1/73/L.27/Rev.1.

7. Germany, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Georgia, Greece, Hungary, Ireland, Israel, Italy, Japan, Latvia, Lithuania, Luxembourg, Malawi, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Ukraine, the United Kingdom, the United States of America. See: UN Document A/C.1/73/L.37.

the debates, Iran, "[a]s a victim of cyber weapons, [...] rejects the status quo and supports the establishment of international legal norms and rules aimed at preventing the malicious use of cyberspace and information and communications technology. Condemning those seeking dominance and superiority in cyberspace and their attempts to maintain the status quo, [the Iranian representative] pointed to a certain state [the United States] which, in collaboration with Israel, used the computer worm Stuxnet against Iran's critical infrastructure, and yet has tabled a draft resolution regarding responsible state behaviour in cyberspace".[8] The representative of the People's Republic of China asked whether a negative vote on the Russian resolution would bring a "ticket" for the country to take part in the GGE.[9] The impression of two competing blocs of states was then reinforced by the sponsoring states of each resolution but also by the context of their adoption and the contents of the debates. These two "blocs" articulated themselves around two approaches often analysed as diametrically opposed: On the one side, there was the United States and European countries, usually described as the "like-minded states", whereas on the other side, China and Russia advertised a different approach. That said, we need to nuance both the homogeneity of the two blocs of states and the antagonism underlaying their respective positions.

First, more than homogeneous blocs, the countries in each group share certain characteristics in their approach that are not completely alike either. There are, for example, important divergences between the Chinese approach and the Russian one,[10] as well as between France's and the United States'. Second,

8. UN, *First Committee Delegates Exchange Views on Best Tools for Shielding Cyberspace from Global Security Threats Triggered by Dual-Use Technologies, Innovations*, 30 October 2018..

9. UN, "First Committee Approves 27 Texts, Including 2 Proposing New Groups to Develop Rules for States on Responsible Cyberspace Conduct," 8 November 2018, Meetings Coverage, UN Document GA/DIS/3619.

10. Dennis Broeders, Liisi Adamson, Rogier Creemers, *A coalition of the unwilling? Chinese and Russian perspectives on cyberspace*, Policy Brief, November 2019, 16 p.

the majority of UN member states did not adhere to any of the groups that offered the resolutions, which limits the notion that two blocs of states structured the oppositions in international negotiations. More importantly still, the vast majority of the members voted in favour of the two resolutions.[11] If, for a number of countries, these two processes are effectively competing, they each advanced different sets of interests. The limited composition and the focus on expertise in the GGE make concrete progress possible on the core of the questions debated, whereas the non-limited composition of the OEWG offers a more inclusive approach that allows each state to have its positions and interests heard. The first session of the OEWG, which took place in New York in September 2019, actually highlighted the interests that many states have in taking an active part in the discussions – something confirmed during the second formal session in February 2020. Hence, the two ongoing processes don't oppose two homogenous blocs of states and, based on their respective composition, they are somewhat complementary. Despite the hostile climate that surrounded their creation, which reveal strong geopolitical tensions, they offer – in theory at the least – a possibility for the states to go beyond their inherent divisions to a smooth parallel functioning or even synergy. The ambassadors Guilherme de Aguiar Patriota and Jürg Lauber, which preside over the GGE and the OEWG, respectively, actually advertised this constructive ambition from the moment they were nominated in those roles.

In the negotiations, European countries have given the impression that they are working independently from each other, although there is a willingness to adopt a common position nowadays. France has positioned itself as a driving force

11. The resolution "Developments in the field of information and telecommunications in the context of international security" (5 December 2018, UNGA Resolution A/RES/73/27) was adopted with 119 votes against 46 and 14 abstentions (UN Document A/73/PV.45) and the resolution "Advancing responsible State behaviour in cyberspace in the context of international security" (22 December 2018, UNGA resolution A/RES/73/266) was adopted with 138 votes against 12 and 16 abstentions (UN Document A/73/PV.65).

in the international discussions on this topic with the launch of the Paris Call. If it has been endorsed by European states, it remains a French initiative and not a common European initiative. Similarly, despite the adoption of the "Cyber Diplomacy Toolbox" by the European Union, some states have been more inclined to side with other coalitions and with non-European countries. This European inability to offer a unified voice has been reinforced by the fact that, during the adoption and negotiation of the previous resolutions, they have been portrayed as simply following the United States. That said, there is a genuine European willingness to act in a more united manner and to position itself as a major actor in international discussions.

Through its member states, the EU has the necessary assets to affirm itself as a leading voice in international discussions and defend its own interests. If European countries succeed in working together, the EU could become a formidable force of propositions as it lays out its expertise and its past successes in the implementation of its international obligations on this matter. For example, the NIS directive[12] and the General Data Protection Regulation[13] participate in the implementation of the obligation of due diligence and to the "creation of a global culture of cybersecurity"[14] among European states. Furthermore, Europe is often described as able to provide a less divisive approach to the issue, one that could reconcile different positions. The United States, on the other hand, has been very critical of multilateral organisations since Donald Trump was inaugurated and they have shown their contempt for the adoption of new norms, which makes observers think they won't be able to adopt a construc-

12. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS).

13. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

14. Resolution of the General Assembly of the United Nations, 30 January 2003, A/RES/55/239.

tive approach and make concessions. The ongoing discussions at the General Assembly of the United Nations and the resolutions it potentially adopts will provide valuable insights into the approach of states and the future of the discussions. The complementarity of the two processes has been highlighted by several states. The OEWG is open to all the member states, taking all the points of view into account. But, on the contrary, the composition of the GGE is limited to 25 member states designated "on the basis of equitable geographical distribution",[15] and the permanent members of the Security Council are ex officio members. Hence, the GGE appears as a more specialised entity. However, an analysis of their respective mandates shows that, if they can be complementary, their mandates overlap to a certain extent which does not facilitate the search for consensus and coherence in the negotiations.

The mandates of the two negotiation processes

At first glance, the mandates of the two groups are so similar that they overlap to a large extent, with the risk of encroaching on each other. Indeed, both groups are mandated to work on the norms, rules, and principles of responsible behaviour of the states, on confidence building measures, on capacity building, and international law. A careful reading, in fact, reveals several differences.

First, the GGE will be able to consult states that aren't members of the GGE and with the competent regional organisations (African Union, Organization of American States, Organization for Security and Co-operation in Europe, and the Regional Forum of the Association of Southeast Asian Nations). For its part, the OEWG will hold informal sessions to consult private actors and non-governmental organisations. Furthermore, non-state actors are authorised to attend the formal sessions, but that only applies to the organisations accredited to the United Nations Economic

15. Resolution of the General Assembly of the United Nations, A/RES/73/266, paragraph 3.

and Social Council (ECOSOC), following the Chinese refusal to enlarge the pool further. Second, the resolution 73/266, defining the mandate of the GGE, states that its report will be presented to the General Assembly with "an annex containing national contributions of participating governmental experts on the subject of how international law applies to the use of information and communications technologies by states".[16] For that reason, the 25 countries participating in the GGE will have to clarify their position on the international law applicable to cyber operations. France and the Netherlands are already set to do that with the publication of a report on *International Law Applied to Cyberoperations* by the French Ministry of Armed Forces,[17] and with an official document untitled *International Law in Cyberspace* by the Dutch Ministry of Foreign Affairs.[18] These two documents, published on 9 September and 14 October 2019, are probably meant to be the two countries' national contributions to the GGE.[19] Finally, the OEWG will be tasked with studying "the possibility of establishing regular institutional dialogue with broad participation under the auspices of the United Nations",[20] which implies the possibility of creating a permanent body or process to deal with ICTs in the context of international security.

Some differences have raised concerns, starting with the respective timelines. The OEWG was supposed to end its work in 2020, during the 75th session of the UNGA, a year before the GGE which mandates last until 2021 and the 76th session of the

16. Ibid.

17. France, International Law applied to Operations in Cyberspace, Ministry of Armed Forces, 4 October 2019.

18. The Netherlands, *Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace*, made public on 15 October 2019, Annex: "International Law in Cyberspace."

19. For a compared study of the states' positions on international law applied to cyberoperations, see: Przemyslaw Roguski, *Application of International Law to Cyber Operations: A Comparative Analysis of States' Views*, The Hague Program on Cyber Norms, Policy Brief, 2020, 48 p.

20. Resolution of the General Assembly of the United Nations, A/RES/73/27, paragraph 5.

UNGA. The extension of the 75th session until March 2021, due to the COVID-19 crisis, will allow the OEWG's work to continue so it can present its report by March to the 75th session of the UNGA. The deadlines for the two reports will be preserved. Some observers are worried that several states behind the resolution creating the OEWG might change course after the end of its sessions. In other words, they would be adopting a constructive approach up to the end of the OEWG's work, in order to achieve a consensus on its conclusions, before turning less cooperative during the remaining time of the GGE sessions, to push for a failure and boast of the superior achievements of the OEWG.

The second concern comes from the content of the mandates. International law is being discussed in the two processes and constitutes a central topic in their proceedings. This is both an opportunity and a risk: States are able to have in-depth discussions about these questions and debate the interpretation of international law in this new context of international peace and security, but they risk adopting diverging directions in the two processes, leading to a certain level of instability for the international legal order.

The same can be said about the norms of responsible state behaviour, mentioned twice in the resolution 73/27 that defined the mandate of the OEWG. The situation here is delicate for two reasons.

The first mention of the norms in the resolution 73/27 appears early on in the definition of the mandate in paragraph 5. The General Assembly decided to convene an OEWG that shall strive,

> acting on a consensus basis, to continue, as a priority, to further develop the rules, norms and principles of responsible behaviour of states listed in paragraph 1 above, and the ways for their implementation; if necessary, to introduce changes to them or elaborate additional rules of behaviour;[21]

Hence, norms – as stated in the resolution – constitute the working base of the OEWG. If the resolution 73/266 only refers to the 2015 GGE report, the resolution 73/27 acknowledges it too but slightly differs from the norms defined in it, which

21. Ibid.

means that the working base of the two processes could differ. It would increase the risks of contradictions and divergence in the meaning of the recommendations adopted by each process. For example, the recommendation on the prevention of malicious computer tools or technologies is included in a paragraph on supply chain integrity in the 2015 GGE report, whereas it is the subject of a stand-alone provision in resolution 73/27. In the latter case, the autonomisation of the problematic could indicate a desire to work more extensively on the issue of proliferation.

That said, an observation of the practice of the states shows that this risk remains limited at this point. During the first two sessions of the OEWG, the large majority of states opted for the norms as stated in the GGE report instead of the ones written in resolution 73/27. It illustrates the lack of consensus on the norms stated in the provisions of the resolution 73/27 but it also highlights a gap between a strict application of the mandate and the practice adopted during the negotiations.

The uncertainty around the working base can also affect other aspects of the negotiations. The mandate states that the OEWG ought to "develop… the ways for their implementation".[22] Hence, the member states are tasked with detailing the operationalisation of the norms. Indeed, as several of them are purely declaratory, they need to be specified to be implemented. Finally, the mandate paves the ground for a reappraisal of the conclusions of the 2013 and 2015 GGEs as states are able to "introduce changes",[23] including establishing new norms. If elaborating new norms – which is authorised by resolution 73/27 – could mean creating new norms that better define what responsible behaviour is, it could also imply the creation of norms susceptible to limit the open nature of cyberspace – hence reassessing what was decided in 2013 and 2015 to guarantee it.

The second mention of norms in the resolution 73/27 can be found in the second part of the definition of the mandate. But it isn't explained if this mention refers to the norms stated in the

22. Ibid.
23. Ibid.

resolution 73/27 or the ones adopted by the GGEs in 2013 and 2015.

A close reading of the mandate thus highlights a number of questions related to the working base on which the negotiations will be conducted. The practice of using the GGE norms seems to prevail so far but contradictions could emerge as both the GGE and the OEWG are tasked with working on these provisions.

The fact that international law and the norms of responsible behaviour are mentioned in both mandates raises the question of the division of labour between the two. In his speech during the first session of the OEWG in June 2019, the special representative of the President of the Russian Federation for international cooperation in information security proposed that the OEWG deals with norms of responsible behaviour, confidence building measures, and measures of international cooperation and assistance, hence leaving the issue of international law to the GGE.[24] This proposal wasn't taken on, and the two processes work concomitantly on the whole set of issues.

Two comments need to be made at this point. On the one hand, treating these issues of international law and norms of responsible state behaviour indiscriminately can be justified by the difficulty to dissociate them completely. Indeed, these topics are intrinsically linked, as we shall see. On the other hand, this situation reinforces the risk of repetitions in the content of the negotiations but also of contradictions in the formulate recommendations made by the two groups on the rights and obligations of the states in the digital space. Moreover, the refusal to dissociate them highlights disagreements on the necessary means to ensure security and stability of cyberspace.

24. Russia, *Statement by Amb. Andrey Krutskikh*, Special Representative of the President of the Russian Federation for International Cooperation in the Field of Information Security at the First Session of the UN Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, New York, 3-4 June 2019, Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland, 7 June 2019.

II. NORMS AND INTERNATIONAL LAW: BETWEEN CONFUSION AND DISAGREEMENT ON THE MEANS NECESSARY TO ENSURE SECURITY AND STABILITY OF CYBERSPACE

In the *International Strategy for Cyberspace* published by the White House in 2011,[1] the United States called for the elaboration of norms of responsible state behaviour in cyberspace. The 2013 GGE report contains a part dedicated to norms, rules and principles of responsible state behaviour in which the member states of the GGE recognised the applicability of international law in cyberspace but also adopted several norms meant to strengthen the security and stability of the global computer environment. Analysing them shows that several norms build on the recognition of the applicability of international law in cyberspace, and paraphrase existing international obligations to be applied in cyberspace. In the 2015 report, the member states opted to list the norms of responsible behaviour and international law provisions in two different parts. But this distinction disregards the links that exist between the first, which are *soft law* provisions that are usually non-binding, and the second, including some rules restated by the GGE. Furthermore, this distinction complexifies the definition of rights and obligations for the states in cyberspace as it introduces a confusion on the nature of the rules and complicates the conduct of the negotiations. Finally, there is no division of work in the two mandates, which mostly highlights disagreements on the means necessary to ensure the stability and security of cyberspace.

1. United States, *International Strategy for Cyberspace*, White House, May 2011, 9. See also: Frédérick Douzet and Aude Géry, "War and Peace in Cyberspace: Obama's Multifaceted Legacy," in François Vergniolle de Chantal (ed.), *Obama's Fractured Presidency. Policies and Politics*, Edinburgh University Press, 2020.

A DISTINCTION PARTLY ARTIFICIAL IN ITS FORMAL AND MATERIAL DIMENSIONS

The formal separation – in two distinct parts of the report – of non-binding provisions on responsible state behaviour on the one side, and international law on the other, bears three limits.

The first limit has to do with the mentioned nature of the dispositions listed in the part dedicated to – legally non-binding – norms. There is no comparable mention in the part dedicated to international law. It states that

Voluntary, non-binding norms of responsible state behaviour can reduce risks to international peace, security and stability. Accordingly, norms do not seek to limit or prohibit action that is otherwise consistent with international law.[2]

Incidentally, the state cannot be held liable for a violation of these norms.

But, as the 2015 GGE report is an expert report and not a treaty of international law, all the provisions it contains, including the ones in the part dedicated to international law, are legally non-binding by nature. The same can be said about the resolutions of the General Assembly which, even though they can participate in the formulation of international law,[3] are absolutely non-binding. Hence, the mention raises a number of questions.

The mention of the non-binding character of the norms can effectively be read as introducing a distinction between them and the obligations pertaining to international law that are addressed in another part of the report. It implies that these provisions are not linked to international law, reinforcing their distinctiveness from the obligations of international law listed in another part of the report.[4]

2. UN, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 22 July 2015, United Nation Documents 1/70/174, 8, paragraph 10.

3. Gérard Cahin, *La coutume internationale et les organisations internationales. L'incidence de la dimension institutionnelle sur le processus coutumier*, Publication de la R.G.D.I.P., Nouvelle Série, 52, Pedone, 2001, 782 p.

4. Liisi Adamson, "International Law and International Cyber Norms. A Continuum?," in Dennis Broeders, Bibi van den Berg (eds.), *Governing Cyberspace. Behavior, Power and Diplomacy*, Rowman & Littlefield, 2020, 25.

But this distinction between norms of responsible behaviour and obligations of international law disregards the link that exists between certain non-binding provisions and some binding obligations. This is the second limit. Indeed, if these provisions are non-binding, they cannot be qualified as outside of the boundaries of the law, in comparison to the legal rules that would be the only binding ones. They are both part of the so-called "normative gradation"[5] between law and lawlessness. The non-binding provisions, often called soft law, can contribute to the interpretation of existing obligations in international law, or to the formation of new international obligations,[6] as their non-binding character doesn't imply an absence of legal effects.[7] Indeed, "states opt out from a binding legal commitment when they make a statement of *soft law*, but they do not altogether refuse to engage".[8]

Finally, the third limit deals with the mention, in the part dedicated to norms and in the one dedicated to international law, of the obligation of diligence[9] and the obligation to protect and respect human rights.[10] These repetitions highlight a link

5. Alain Pellet, "Le "bon droit" et l'ivraie – Plaidoyer pour l'ivraie (Remarques sur quelques problèmes de méthode en droit international du développement)," in *Le droit des peuples à disposer d'eux-mêmes : méthodes d'analyse du droit international. Mélanges offerts à Charles Chaumon*, Pedone, 1984, 488, (our translation) "*dégradé normatif*".

6. Christine Chinkin, "Normative Development in the International Legal System," in Dinah Shelton (ed.), *Commitment and Compliance. The Role of Non-Binding Norms in The International Legal Systems*, Oxford University Press, 2000, 30-31.

7. Jean Combacau, Serge Sur, *Droit international public*, 11th edition, L.G.D.J., Domat, 2014, 53.

8. Julien Cazala, "Le *soft law* international entre inspiration et aspiration," *Revue interdisciplinaire d'études juridiques*, 2011/1, volume 66, p. 47 (our translation) "*Les États refusent, en recourant* à *un énoncé de soft law, un engagement juridique contraignant, mais ne renoncent pas* à *toute forme d'engagement*".

9. UN, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 22 July 2015, United Nation Documents 1/70/174, 9, paragraph 13(c), and 15, paragraph 28(e).

10. Ibid., paragraph 13(e) and 28(b).

between the two and the fact that the states haven't been able to distinguish the two completely.

Hence, the present analysis shows the limits of the formal distinction between non-binding norms and provisions paraphrasing obligations of international law. And this distinction is all the more artificial on the material level, i.e. in terms of the content.

Analysing the content of the norms of responsible behaviour show that they can be divided into two categories. Some identify good practices to strengthen the security and stability of the global cyber environment whereas others are built on obligations of international law applied to state behaviours in cyberspace.[11] As such, this second category of norms is tightly linked to international law on the material level.

The separation between obligations in international law stated in the report and the norms creates two problems, as they are both linked: one pertains to the identification of the rights and obligations of the states, and the other the conduct of the negotiations.

First, this distinction raises a problem in identifying the rights and obligations of the states. As soon as a norm of responsible behaviour paraphrases an international obligation, we can question the desire to maintain the link that exists between the two. What consequences can we draw from this distinction when the content is the same? Does it imply that the implementation and the respect of the obligation stated in the norm is a simple recommendation, distinct from the international obligation on which it has been built? We don't think it is, as the state ought to respect international obligations in all cases. The message hence carried could imply that the norm is detached from international law to be made autonomous and, in as such, that the behaviour to be adopted in cyberspace wouldn't be built upon an international obligation but on the goodwill of the states.

11. François Delerue and Aude Géry, *Etat des lieux et perspectives sur les normes de comportement responsable des Etats et mesures de confiance dans le domaine numérique*, Note Stratégique, CEIS 2017.

Furthermore, some norms and provisions contained in the part dedicated to international law seem to interpret the obligations of international law whereas others are only paraphrasing them. As such, it is difficult to differentiate a simple reminder of a rule of international law from the specific interpretation of an international obligation applied to cyberspace.

When the same obligation is cited in both parts of the report, should the provision set out in the part dealing with international law be considered to be of greater value than that cited in the part dealing with norms, since it is specified that norms are not intended to limit the rights and obligations of states? Depending on the statement of the paraphrased obligation or the one on which the provision is laid out, and on the retained response, the consequences in terms of the rights and obligations of the states could differ. For example, when the provision in the part dealing with international law narrowly interprets an international obligation, whereas the provision in the part dealing with norms simply paraphrases, does it mean that the first disposition carries more weight – because it comes from the part dealing with international law – and, if that's the case, that the retained interpretation of an international obligation is more restrictive in its content when it is applied to cyberspace?

Second, this distinction risks being problematic in the conduct of international negotiations in the OEWG and in the GGE. The states will discuss norms and international law at two different moments because the working sessions are organised by themes, with one dedicated to norms and another to international law. Yet, because they are both linked, the risk is that states treat this issue twice and adopt two different, or even contradictory, positions. Furthermore, as the ongoing negotiations on norms focus mainly on their operationalisation, i.e. on their practical implementation, future provisions will have a part in the interpretation of international obligations. However, the question of content also encompasses aspects not covered by the provisions specifying the implementation of the norms and thus interpreting international obligations. Should it be considered that if certain clarifications are not made it is because they do not result

from the implementation of the concerned international obligation? Or should the elements not mentioned be said to have no consequences on the interpretation of the international obligation?

The problems in the negotiations risk being even more complex depending on whether they are conducted based on the norms stated in resolution 73/27 (OEWG) or on the norms previously adopted in the GGE reports, as most states do. Indeed, the operationalisation of the norms necessitates a prior identification of the accepted basic norms. The norm on the obligation of due diligence from the resolution 73/27 is a good illustration.[12] It is made of the GGE norm on the obligation of due diligence[13] and of the paragraph relative to the same obligation in the part dealing with international law.[14] The GGE norm paraphrases the famous *dictum* of the International Court of Justice in the Corfu Channel case stating an obligation to every state not to allow willingly its territory to be used for acts contrary to the rights of other states.[15] The corresponding paragraph in the international law section of the report contains a provision focusing on the use of intermediaries by states and on not allowing their territory to be used by non-state actors to commit internationally wrongful acts. This paragraph seems to interpret the obligation of due diligence by specifying its implications as regards the conduct to be adopted vis-à-vis intermediaries and non-state actors, questioning the willingness of states to limit its application in the digital context to these two cases. Depending on the interpretation of this paragraph, the obligation of due diligence is therefore more precise or more limited than the obligation set forth by the International Court of Justice and reproduced in the section dealing with norms. However, in so far as these two provisions are combined in resolution 73/27 but not in the GGE report, depending on which text is taken as a reference for the definition of its operationalisation, the provisions adopted will not be the same, leading to a risk of confusion as to what is expected of the states.

12. UN, Developments in the field of information and telecommunications in the context of international security, Resolution of the General Assembly, A/RES/73/27, 5 December 2018, paragraph 1.3.

13. Document of the United Nations, A/70/174, paragraph 13(c).

14. Ibid., paragraph 28(e).

15. International Court of Justice, *Corfu Channel case,* order, 9 April 1950.

The established distinction between the norms of responsible behaviour and the provisions of international law isn't as clear-cut as the report suggests. *In fine*, the very notion of a norm of responsible behaviour, in its relation to international law, is potentially questioned on a material level. But it questions whether norms "are indeed intended to promote and enhance international law or whether 'responsible state behaviour' is a deflected route around international law".[16] On a formal level, the distinction between norms and provisions of international law will be a springboard to justify the elaboration of a treaty.

THE DISTINCTION FURTHERS THE CASE FOR A TREATY

Due to the specificities of cyberspace, the need for new rules emerged early on. Hence, Russia had already argued in favour of a new treaty in 2000, explaining that positive international law wasn't able to respond to the specific challenges pertaining to cyberspace or set guidelines for the behaviours of states.[17] On the contrary, many Western countries believed that new rules weren't necessary. The recognition that international law applies to the behaviour of the states in cyberspace could have ended the debate and signified the absence of a manifest legal gap. Existing rules of international law regulate states' behaviours in cyberspace and thus it seems unnecessary to adopt new rules. Additionally, the norms of responsible state behaviour could complete and specify international obligations. That being said, and despite an apparent consensus, the possibility of a treaty re-emerged in 2019, facilitated by the distinction established

16. Eneken Tikk, *International Law in Cyberspace: Mind the gap*, Research Focus, 2020, 7.

17. United Nations, Developments in the field of information and telecommunications in the context of international security, A/54/213, Russia, 8-10.

between norms and international law. It illustrates diverging points of view on the means required to secure cyberspace.

The opposition focuses on the value of the instrument

The proponents of a treaty want to elaborate a binding legal instrument to define explicitly the rights and obligations of the states in cyberspace. They don't challenge the applicability of positive international law, but consider it insufficient to take hold of all the specificities of cyberspace. This position highlights an exceptionalist vision of international law, built on the inability of general international law to regulate certain phenomena, and it implies the development of a *lex specialis*, i.e. specific rules of law aimed at regulating these phenomena. For their opponents, positive international law is flexible enough to regulate the behaviours of the states. However, due to the specificities of cyberspace, additional norms of behaviour are necessary on some aspects. But these norms aren't meant to become international obligations, in the short or medium range at the least. This interpretation is confirmed by the very notion of the norm of behaviour, as "norms do not seek to limit or prohibit action that is otherwise consistent with international law".[18] Hence, the value of the rules is questioned more than their contents. On one side, some states, such as Russia, wish to elaborate new international obligations that would find states internationally responsible in case of violation. On the other side, different states, such as the United States, prefer to go on with the non-binding rules of soft law, which means that a violation, as such, cannot engage the responsibility of a state. The opposition between the groups has thus crystalised on the necessity of a treaty and on the value of its provisions, without discussing its eventual content.

It can be explained by various reasons. On the one side, this antagonism can be traced back to the early stages of the

18. UN, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 22 July 2015, United Nations document A/70/174, 8, paragraph 10.

discussions on cybersecurity at the UN. It illustrates the use of international law to try and limit the capabilities of the most advanced states and highlights a geopolitical power struggle. On the other side, it expresses different visions of international legality. From the perspective of the Russian doctrine, these norms are meant to become international obligations, following a legalist vision built on the development and respect of international law. Without questioning international law, and even though there are important differences between them, Western countries have a more political vision in which political and legal commitments are complementary. They don't necessarily try to develop binding rules and opt for non-binding commitments.[19]

This preference can also be explained by the fact that they don't want to be legally constrained when the power balance in the negotiations over a treaty wouldn't necessarily be in their favour. If this element can be overcome by the different steps of the signing and ratification of the treaty, which they would be free to proceed with after the treaty is open for signature, the very existence of this treaty could put them in an uneasy situation. The lack of a signature and ratification could be instrumentalised to point at a refusal to ensure peace and stability of cyberspace. More largely, it is important to note that the present period is inauspicious to the development of new multilateral treaties and of international law at large, as several states are particularly critical of the international legal system and of the potential constraints coming from it.[20]

However, two important distinctions must be made. First, the *instrumentum* – the choice of a specific legal instrument – versus its content. Then, the distinction between the notions of binding and obligatory. A treaty is a binding legal instrument. It is an "agreement concluded between two or more subjects of international

19. Anthea Roberts, *Is International Law International?*, Oxford University Press, 2017, 432 p.

20. Heike Krieger and Georg Nolte, *The International Rule of Law – Rise or Decline? – Points of Departure*, KFG Working Paper Series No 1, 2016; François Delerue, "Reinterpretation or Contestation of International Law in Cyberspace?", *Israel Law Review*, 52:3, 2019, 295-298.

law, intended to have legal effects and to be governed by international law".[21] It creates international obligations that ought to be implemented by the states according to the principle of *pacta sunt servanda*. That said, a binding instrument can contain general provisions that gives some leeway to the states to implement them. Their decision to respect these provisions could be materialised in different ways. This is, for example, the case of the UN Framework Convention on Climate Change, which was open to signature after the Rio Conference of 1992. Alan Boyle explains that "[t]his treaty does impose some commitments on the parties, but its core articles, dealing with policies and measures to tackle greenhouse gas emissions, are so cautiously and obscurely worded and so weak that it is uncertain whether any real obligations are created".[22] On the contrary, non-binding provisions can have an obligatory character due to the vocabulary used, to their exactness – which leads to a uniform implementation – or to the existence of strong monitoring mechanisms. Hence, "the technique or conventional mould doesn't solely confer a given intensity to the obligations".[23] For that reason, legal formalism cannot presume of the obligatory character of the provisions.[24] In other words, we need to go beyond the type of instrument dealt with in this case to study its practical content.

Beyond the instrument, what could be in the treaty?

In terms of its content, it remains to be decided whether a treaty should create new international obligations – transforming norms of responsible behaviour into international obligations, for

21. Patrick Daillier, Mathias Forteau, Alain Pellet, *Droit international public*, 8th edition, L.G.D.J., 2009, 132.

22. Alan E. Boyle, "Some Reflections on the Relationship of Treaties and Soft Law," *The International and Comparative Law Quarterly*, 48:4, 1999, 907.

23. Jean Combacau and Serge Sur, *Droit international public*, *op. cit.*, 150, (our translation) "*La technique ou le moule conventionnel ne confèrent pas à eux seuls à ces obligations une intensité donnée*".

24. R. R. Baxter, "International Law in "Her Infinite Variety"," *The International and Comparative Law Quarterly*, 29:5, 1980, 549-566.

example – or if it should specify the way existing international obligations ought to be interpreted, in order to better define the rights and obligations of the states in cyberspace.

First of all, the problematic interpretation of international law in this context wouldn't necessarily be settled with the adoption of a treaty. We need to remember that each state is free – within the limits granted by international law – to retain its own interpretations. However, the communication of each state's approach on the implementation of rules of international law could play an important role in identifying their practices.[25] The requirement for the countries participating to the sixth GGE to submit national contributions "on the subject of how international law applies to the use of information and communications technologies"[26] could bring relevant elements to that end. Indeed, if the 25 countries – and especially the five permanent members of the Security Council (China, United States, France, United Kingdom, Russia) – oblige, it will be possible to assess the points of divergence and convergence in their approach of international law applied to cyber operations. At the moment, less than a dozen countries have substantially communicated about their approach.[27] Furthermore, the norms of responsible state behaviour are useful for agreeing on the interpretation of sev-

25. The exchange of information on legal strategies for cyberoperations is an important step in the development of state practice. But the existence of a sufficient practice is essential for the International Law Commission to be able to consider this issue in the future. Its referral, which would aim at codifying international law in this field, could then, to a certain extent, constitute an alternative path to the adoption of a treaty. It would not, however, resolve the question of possible new international obligations that might be adopted. This hypothesis is not, however, conceivable at present, both for political reasons and for reasons relating to the conditions under which the matter could be referred to the International Law Commission. François Delerue, "The Codification of the International Law Applicable to Cyber Operations: A Matter for the ILC?," *ESIL Reflections* 7, 2018.

26. Resolution of the General Assembly of the United Nations, A/RES/3/266, paragraph 3.

27. Przemyslaw Roguski, *Application of International Law to Cyber Operations: A Comparative Analysis of States' Views*, The Hague Program on Cyber Norms, Policy Brief, 2020.

eral rules of international law in specific contexts. In that sense, several norms adopted by the previous GGEs participate in the interpretation of international law.

Second, the identification of new international obligations should only come from a deeper work of interpretation and from the practice of the states on the application of international law to cyberspace. Indeed, how can we identify whether new rules are necessary if the behaviours already covered by positive law haven't been previously identified? As such, the example of the protection of electoral infrastructures from computer attacks aimed at interfering with the election is significant. This proposal's relevance from the Global Commission on the Stability of Cyberspace (GCSC),[28] also stated in the Paris Call, raises a number of questions as the principle of non-intervention is already evidently applicable to electoral infrastructures. If it can be perceived as an implementation of this principle, could it also be seen as weakening it – and, as a consequence, the implied protection of electoral processes – with its non-binding character and the language employed? Beyond this example, we need to identify the relevance and the risk of obsolescence of international law when choosing too restrictive or precise norms that impede on the customary rules of international law. The flexibility and the adaptability offered by general principles shouldn't be discarded simply because of new technological developments.

Finally, the distinction made between norms of behaviour and international law offers an argument in favour of the elaboration of new international obligations. Indeed, we can already see a contradiction in the arguments deployed by states that refuse to debate the elaboration of a treaty yet defend existing norms of responsible behaviour – or even endorse the adoption of new norms. Hence, the official French position provides that the existence of legal gaps justifies the adoption of new international

28. The Global Commission on the Stability of Cyberspace (GCSC) is an international group bringing experts from academia, the private sector, government and civil society who work on the elaboration of norms to ensures the stability of cyberspace.

obligations, though these gaps haven't been established.[29] That said, France actively defends the norms adopted in 2013 and 2015 and the Paris Call also contains new norms. These positions can be perceived as contradictory as the elaboration of these norms should be interpreted as the marker of a legal gap that requires filling, and could be used to justify the opening of discussions on an international treaty. The Russian proposal to put the OEWG in charge of norms of behaviour signals a renewed interest in Russia for an international treaty on this matter. Indeed, the OEWG's format – open to all member states – could constitute a favourable framework to that end. It is thus probable that Russia uses the process to bring back the topic and defend the necessity of a treaty. This is what the Russian delegation has already done during the formal sessions of the OEWG. If so, it is all the more understandable that the provision on the handling of evidence when making accusations of cyber operations, which was originally in the section on international law in the 2015 GGE report, was referred to as a norm of responsible behaviour in resolution 73/27, since it would be a matter of transforming it into a genuine international obligation. This disposition, present in section IV of the 2015 report, has been explicitly rejected by the United States and France who refused to interpret it as creating a new international obligation. But, as they qualify the provision as a norm, and according to the objective of the elaboration of a treaty, it could eventually become a new international obligation.

It is important to note, however, that many states don't support a new treaty, even among the ones often associated with Russia. Hence, the Chinese position is more prudent and focuses on the need to continue studying the interpretation of international law and the consequences of its application on state behaviours in cyberspace. Without rejecting the eventual need for new rules of law in the future, it doesn't subscribe to the exceptionalist vision.

29. France, France's response to Resolution 73/27 "Developments in the field of information and telecommunications in the context of international security" and Resolution 73/266 "Advancing responsible state behaviour in cyberspace, Ministry of Europe and Foreign Affairs, 13 May 2019.

Whatever the Russian strategy on an eventual treaty may be, analysing the normative character and the legal effects of the adopted provisions now constitutes a major challenge in an attempt to find our way through the meanders of state rights and obligations in cyberspace. The states' practice in terms of international law and norms of behaviour remains embryonic. And yet, it is fundamental due to its role in forming international law. Besides, even though these instruments aren't binding, the states that adopted them are required to behave in good faith. The implementation of a declaratory monitoring mechanism, based on the model proposed by France during the G7,[30] or by Australia and Mexico during the OEWG,[31] and which could be built upon states' voluntary contributions to the Secretary General of the United Nations, would constitute a tool to reinforce these norms, on the same level as the confidence building measures and the measures of international cooperation and assistance that have been adopted.

As they separated norms of behaviour and international law, the member states of the fifth GGE not only introduced a largely artificial distinction that was partially contradicted by the very content of these norms, but they also revived tensions around the adoption of a new treaty that have been exacerbated in the current geopolitical context. The issue of a treaty now represents a major point of divergence that blocks substantive progress on the content of the rights and obligations of the states in cyberspace. And this situation has been reinforced by the oppositions on the content of the rules of international law that need to be discussed.

30. G7, Ministerial Foreign Affairs Meeting, Dinard Declaration on Cyber Norm Initiative, Dinard, 5 April 2019.

31. https://front.un-arm.org/wp-content/uploads/2020/04/final-joint-oewg-proposal-survey-of-national-implementation-16-april-2020.pdf.

III. INTERPRETING INTERNATIONAL LAW: AN ENTANGLEMENT OF ISSUES AND THE RISK OF A MILITARISATION OF CYBERSPACE

The principle of the applicability of international law is now consensual. But there is no agreement on what it entails, leading to serious risks of deadlock. The 2017 GGE failed because several states refused the applicability of certain branches of international law to cyberspace to be detailed in the report. This opposition was presented in some commentaries[1] as an overall questioning of the applicability of international law in cyberspace. But this wasn't the case.

Contrary to what has been said, neither China nor Russia question the principle of the applicability of international law or of the Charter of the United Nations, in its entirety, to cyberspace. Their positions are somewhat similar, but with a few nuances. The two states have expressed a desire to focus on protecting principles of international law, such as principles of sovereignty and non-intervention, and on the clarification of the primary rights and obligations of the states rather than to discuss the reactions to violations of international law, such as self-defence and countermeasures. Their refusal to debate the applicability of Article 51 of the UN Charter (right to self-defence) in cyberspace isn't a challenge to the applicability of the rule. Their attitude lays on political and legal arguments, such as the difficult attribution and the weak standards of proof. According to their analysis, these legal obstacles hinder the right to self-defence – and yet not questioning its existence. This subtilty in their reasoning has often been dismissed by other state actors, either due to a simple thinking or to political interests. But it is all the more important as, politically speaking, it doesn't make any sense for

1. United States, Michele G. Markoff, *Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security*, U.S. Department of State, 23 June 2017.

a state to renounce its right to self-defence. Interestingly, if the Russian discourse on this right has been overly critical, the country has never renounced it.

Furthermore, several months after the failure of the fifth GGE, the heads of states of the BRICS (Brazil, Russia, India, China, and South Africa) adopted the Xiamen Declaration, on 5 September 2017, which stated their commitment to the applicability of international law to information and communication technologies:

> We consider the UN has a central role in developing universally accepted norms of responsible state behaviour in the use of ICTs to ensure a peaceful, secure, open, cooperative, stable, orderly, accessible, and equitable ICT environment. We emphasise the paramount importance of the principles of international law enshrined in the Charter of the United Nations, particularly the state sovereignty, the political independence, territorial integrity and sovereign equality of states, non-interference in internal affairs of other states and respect for human rights and fundamental freedoms. We emphasise the need to enhance international cooperation against terrorist and criminal misuse of ICTs, reaffirm the general approach laid in the eThekwini, Fortaleza, Ufa, and Goa declarations in this regard, and recognise the need for a universal regulatory binding instrument on combatting the criminal use of ICTs under the UN auspices as stated in the Ufa Declaration.[2]

This opposition on the interpretation of international law has crystalised tensions between states and it is rooted in disagreements on the representations associated with the interpretation of several rules of international law. Certainly, states adopt interpretations that may differ depending on the threats they prioritise or on their strategic interests. In other words, the debates aren't about the rules of international law themselves, but their interpretation. These rules are relatively flexible and make different interpretations possible and, as such, states differ on them. The legal translation of the various representations of the threats is bound to be notably marked in cases dealing with the responses authorised by international law to acts defined as internationally wrongful. But it will also be complicated by the entanglement of issues, thus illustrating the difficulty for a state

2. BRICS, *BRICS Leaders Xiamen Declaration*, 2017 BRICS Summit, 4 September 2017, paragraph 56.

to position itself on the interpretation of international law when it considers all its strategic interests.

THE RESPONSES AUTHORISED BY INTERNATIONAL LAW: THE CASE OF THE MILITARISATION OF CYBERSPACE

The discussion at the 2017 GGE stalled on the paragraph dealing with international law. Several states refused to mention[3] the law of armed conflicts, countermeasures, and self-defence[4] because they believed it could lead to the militarisation of cyberspace. These points of disagreement between the states highlight the absence of consensus on the implementation of the modalities of response to cyber operations as laid out by international law. To respond to an unfriendly act, a state can adopt measures of retorsion, whereas it can adopt measures of retorsion and countermeasures[5] in reaction to an act recognised as wrongful internationally; self-defence, meanwhile, is only invokable in response to an armed attack.[6]

The various responses that a state can invoke and implement in reaction to a cyber operation will probably be the subject of further disagreements, or tensions, in the GGE and the OEWG. This issue is crucial as we've seen a multiplication of public

3. They were mentioned in the 2015 GGE report (United Nation document 4/70/174).

4. Even though they had been mentioned in the 2015 GGE report (United Nation document 4/70/174).

5. Counter-measures designate the actions, otherwise wrongful, that a state can adopt to respond to a wrongful action from another state. The fact that an action has been adopted as a counter-measure means that the circumstances exclude its wrongfulness. See, for example: François Delerue and Aude Géry, "Le droit international et la cyberdéfense," in Didier Danet, Amaël Cattaruzza and Stéphane Taillat, *La Cyberdéfense – Politique de l'espace numérique*, Armand Colin, 2018, 68.

6. See, for example: François Delerue, *Cyber Operations and International Law*, Cambridge University Press, 2020, chapter 10. Also, the flowchart on the legal process of attribution, characterisation and response to cyberoperations under international law, in François Delerue, *International Law in Cyberspace Matters: This Is How and Why*, EU Cyber Direct, Policy in Focus, 2019.

political attributions and/or imputations.[7] Since the hacking of Sony Pictures in November 2014, attributed to North Korea by the United States, we have seen a change in the strategy of several states as they decided to denounce certain computer hacks publicly, even in a coordinated (semi-collective attribution) or joint (collective attribution) manner. An analysis of the discourses of attribution shows three dynamics. First, they often fall within power struggles that oppose the "Five Eyes"[8] to Russia, China, and some of their allies. Second, it shows that, if the states shy away from legally qualifying the behaviours they denounce, they do at least invoke the international legal order and the norms of responsible behaviour adopted by the 2013 and 2015 GGEs. According to its proponents, the "naming and shaming" strategy aims at establishing the political responsibility of the attacking states and reinforcing the security and stability of cyberspace. It materialised in the adoption on the sidelines of the General Assembly of the United Stations, by 27 states including France, of a "Joint Statement on Advancing Responsible State Behavior in Cyberspace" on 23 September 2019, also known as the "New York Call".[9] Third, these discourses are often accompanied by sanctions.[10]

7. The willingness of states to invoke the political or legal responsibility of the state actors to which they attribute the concerned cyberoperations is not always clear. The vagueness surrounding this practice is not likely to clarify and appease the debate on how to respond to violations of international law or unfriendly acts.

8. "Five Eyes" refers to the alliance between the intelligence services of five English-speaking countries (Australia, Canada, United States, New Zealand, United Kingdom).

9. *Joint Statement on Advancing Responsible State Behavior in Cyberspace*, 23 September 2019.

10. See, for example: United States, *Treasury Imposes Sanctions Against the Government of the Democratic People's Republic of Korea*, Treasury Department, 2 January 2015, (hacking of Sony Pictures); United States, *Press Call on the Administration Responses to Russian Malicious Cyber Activity and Harassment*, White House, 29 December 2016 (election interferences); United States, *Treasury Targets Supporters of Iran's Islamic Revolutionary Guard Corps and Networks Responsible for Cyber-Attacks Against the United States*, Treasury Department, 14 September 2017; United States, *Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks*, Treasury Department, 15 March 2018 (election interferences and NotPetya).

Contextual elements are important to understand why, politically, there is opposition on the issue of how to respond to state-sponsored cyber operations. Existing frictions between groups of states are important, and so are uncertainties over the non-explicit legal qualification used by states to adopt undefined measures to respond to targeted computer attacks. In other words, the relative uncertainty over the interpretation of international law by states creates legal insecurity over the justifications invoked to justify a response. This new context of relative legal insecurity explains, in part, some states' reluctance to codify the interpretation of certain branches of international law applicable in cyberspace.

From the perspective of international law, these uncertainties come from diverging interpretations, including between so-called "like-minded" states, and some of these uncertainties tend to favour the use of military force. The first divergence rests on the existence of a threshold between the use of force (article 2§4 of the UN Charter) and an armed attack (article 51). The first opens the right to adopt countermeasures, whereas the second triggers the right to self-defence. But the United States doesn't recognise this distinction, the right to self-defence being, according to them, triggered as soon as a state violates article 2§4.[11] This interpretation does lower the threshold on the use of self-defence and, as such, the potential use of force to respond to an internationally wrongful act.

The second point of divergence pertains to the theory of armed countermeasures. Contrary to self-defence, countermeasures cannot be a use of force. It has been confirmed by the *Articles of the International Law Commission on the Responsibility of States for Internationally Wrongful Acts*.[12] A minority group in

11. See, for example: Harold Hongju Koh, "International Law in Cyberspace," *Harvard International Law Journal,* Vol. 54, 1-12, based on his speech delivered at the 2012 USCYBERCOM Inter-Agency Legal Conference.

12. International Law Commission of the UN, Responsibility of States for Internationally Wrongful Acts, annexed to the resolution 56/83 adopted by

the literature suggests that, while we should maintain the distinction between the threshold for the use of force and an armed attack, a state victim of the use of force that doesn't amount to an armed attack could opt for armed countermeasures.[13] In that case, they should respect a double criteria of necessity and proportionality, which apply to both countermeasures and self-defence. This theory questions the balance between the two forms of response as it authorises the states to adopt, in response to an act below the threshold of an armed attack, measures that could imply the use of force. Knowing the uncertainties when identifying the different qualifying thresholds, these interpretations could favour the conduct of cyber operations with potentially destabilising effects.

The third point of divergence deals with the adoption of collective countermeasures to support the state victim of a cyber operation. The possibility to adopt collective countermeasures in response to cyber operations has been defended by the Estonian president in her opening speech at CyCon.[14] Even though it contains several ambiguities, the regime of collective countermeasures is defined by the *Articles of the International Law Commission on the Responsibility of States for Internationally Wrongful Acts*. But the Estonian proposal wants to broaden them.[15] As several states

the General Assembly on 12 December 2001, and modified by the document A/56/49 (Vol. I)/Corr. 3, article 50(1)(a).

13. This theory has been pushed by Judge Bruno Simmar in his separate opinion in the Oil Platforms case (Islamic Republic of Iran v. United States of America) (International Court of Justice, Oil Platforms case (Islamic Republic of Iran v. United States of America), decision, 6 November 2003, C.I.J. Rec. 2003, Separate Opinion, p. 331-334, paragraphs 12-16. It has been largely developed and supported by some experts of the *Tallinn Manual 2.0*, in the commentary to rule 22. See: Michael N Schmitt and Liis Vihul (dir.), *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd edition, Cambridge University Press, 2017, 123-125.

14. Estonia, *President of the Republic at the opening of CyCon 2019*, 29 May 2019: "[a]mong other options for collective response, Estonia is furthering the position that states which are not directly injured may apply countermeasures to support the state directly affected by the malicious cyber operation."

15. Przemyslaw Roguski, "Collective Countermeasures in Cyberspace – Lex Lata, Progressive Development or a Bad Idea," *in 12th International*

attribute to certain states cyber operations suffered by third countries,[16] including through collective and semi-collective attributions, this proposal has been perceived as destabilising and a future source of divisions and tensions that could represent an important point of stalemate. France, for instance, has expressed its opposition to such an evolution of the law on collective countermeasures.[17]

Finally, the last point of divergence rests on the assimilation, and sometimes confusion, between the obligation of due diligence, and the theory of unable or unwilling. The non-respect of the obligation of due diligence by a state allows the victim state to adopt, under certain conditions, measures of retorsion or countermeasures without being able to use the right to self-defence.[18] On the contrary, the theory of unable or unwilling has been used by the United States to justify the use of force on the territory of states, without their consent, because they were unwilling or unable to adopt the necessary measures to end the use of their territory by armed groups. This principle is highly controversial; the United States has been the only one to invoke it, and it seems to be distancing itself from it nowadays. Believing that the theory of unable or unwilling and the obligation of due diligence are identical legitimises the use of force in situations proscribed by current international law. Any mention of this principle in a section dedicated to international regulation or to threats would be perceived as a way to facilitate the use of mili-

Conference on Cyber Conflict 20/20 Vision: The Next Decade, NATO CCD COE Publication, 2020, 43-62.

16. This is the case of New Zealand, that attributed NotPeya and the attempted breaking in the OPCW to Russia even though it stated it wasn't a victim of it. New Zealand, National Cyber Security Centre, *New Zealand joins international condemnation of NotPetya cyber-attack*, 16 February 2018; New Zealand Government Communications Security Bureau, *Malicious cyber activity attributed to Russia*, 4 October 2018.

17. France, International Law applied to Operations in Cyberspace, Ministry of Armed Forces, 4 October 2019.

18. This position has been forcefully recalled by France in its white paper on the applicability of international law to operations in cyberspace, hence unambiguously rejecting the theory of unable or unwilling (*idem*, 10).

tary force against a state whose territory has been used to launch cyber operations against another state.

These four points expose the legal arguments behind the reluctance of some states in the discussions on the forms of responses to internationally wrongful cyber operations under international law. As they facilitate the conduct of cyber operations in response to an unfriendly act or an internationally wrongful act, their opponents believe that they lead to the militarisation of cyberspace at the expense of an open, secure, accessible, and peaceful cyberspace. However, and despite the predictable difficulties of the endeavour, these countries think that the negotiations should focus on protecting and stabilising principles, such as the principles of sovereignty and non-intervention.

THE PRINCIPLE OF SOVEREIGNTY: AN INTERPRETATION COMPLICATED BY THE ENTANGLEMENT OF ISSUES

Sovereignty, an attribute of the state, is at the basis of international law.[19] Several corollaries emerged from this principle, including the sovereignty equality of the states, their freedom to act within the perimeter of their sovereignty, and the non-intervention in the internal or external matters of a state. This implies limits on the right for a state to conduct cyber operations against another state. For that reason, these corollaries are deemed protecting and stabilising. Determining which cyber operations constitute a violation of sovereignty and of the territorial integrity of a state, or of the principle of non-intervention, is a true challenge. Indeed, because the issues are entangled – a legal question can be led out differently in different contexts and provoke different interpretations depending on competing strategic interests – and because the states have chosen not to address certain types of cyber operations or topics, including cyber espionage, it is

19. International Court of Justice, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), decision of 27 June 1986, C.I.J. Rec. 1986, paragraph 263, 133.

difficult to reach a consensus on the interpretation of these principles in the digital context.

With regard to respect for the sovereignty and territorial integrity of a state, the territorial criterion serves as a cornerstone for defining the contours of states' rights and obligations. However, in the digital context, it can be abused by a phenomenon that disregards borders. We are therefore witnessing a two-fold movement. On the one hand, all the states recognise that their sovereignty can be exerted over all the infrastructures present on their territories,[20] leading to a territorialisation of cyberspace based on its physical layer[21] but they also use other mechanisms, such as the theory of effects.[22] On the other hand, parts of the doctrine and several states have partly reassessed this territoriality based on techno-political arguments,[23] on an unreasonable

20. See, for example: UN, Report of the Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 24 June 2013, United Nations document A/68/98; UN, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 22 July 2015, United Nations document A/70/174.

21. This is the case in France: "Any cyberattack against French digital systems or any production of effects on French territory via digital means by a state body, person or entity exercising the prerogatives of public powers or by a person or persons acting on the instructions or directives or under the control of a state constitutes a violation of sovereignty." France, International Law applied to Operations in Cyberspace, Ministry of Armed Forces, 4 October 2019.

22. The theory of effects has been used by the states to identify a credential enabling them to act in a given domain. Hence, states could invoke that a digital activity had some effects on their territory to identify a credential. See: Edouard Treppoz, « Jurisdiction in the Cyberspace », *Swiss Review of International and European Law*, 26:2, 2016, 273-288.

23. An analysis of the position of the states is available in Przemyslaw Roguski, *Application of International Law to Cyber Operations: A Comparative Analysis of States' Views*, The Hague Program on Cyber Norms, Policy Brief, 2020, 4-7.

interpretation of the territorial criteria[24] and on other credentials to establish their jurisdiction.[25]

This is a fundamental issue when dealing with two problems in particular. The first one deals with the exercise of extraterritorial enforcement jurisdiction,[26] especially in criminal matters. It has generally been accepted that a state cannot collect evidence on the territory of another state without a permissive rule, be it a conventional one – the authorisation comes from a pre-existing treaty between the concerned states – or an agreement from the state territorially competent.[27] The second deals with espionage and whether or not an intrusion in a computer system can be considered equal to an intrusion on the territory of a

24. United States, United States District Court, Southern District of New-York, In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation (Microsoft Corporation vs. United States of America), 25 April 2014, 15 F, Supp. 3d, 475-476; United States, Court of Appeals for the Second Circuit, In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation (Microsoft Corporation vs. United States of America), 14 July 2016, case 14-2985. For official reactions on the affair, see, for example: "Letter of Viviane Reding to an MEP," 24 June 2013; United States, Court of Appeals for the Second Circuit, "Brief of Amicus Curiae Ireland," 23 December 2014, case 14-2985, document 164, 1; United States, Supreme Court, "Brief Amicus Curiae of the U.N. Special Rapporteur on the Right to privacy Joseph Cannataci in Support of Neither Party," 13 December 2017, case 17-2, 29-36; United States, Supreme Court, "Brief of Amicus Curiae Jan Philipp Albrecht, Siphie In'T Veld, Viviane Reding, Birgit Sippel, and Axel Voss, Members of the European Parliament in Support of Respondent Microsoft Corporation," 18 January 2018, case 17-2, 6.

25. Cloud Act H.R.4943; H. R. 1625, Pub. L. 115- 141; Patrick Jacob, "La compétence des Etats à l'égard des données numériques," *Revue critique de droit international privé*, 3, 2019, 665-679.

26. "An implementing power is the power of a state to implement a general rule or an individual decision by material acts of enforcement which may go as far as the implementation of state coercion." Brigitte Stern, "Quelques observations sur les règles internationales relatives à l'application extraterritoriale du droit," *A.F.D.I.*, Vol. 32, 1986, 11.

27. Permanent Court of International Justice, "Lotus" case, decision delivered on 7 September 1927, *Series A., n° 10,* 18-19. See also: Jonathan Bourguignon, "La recherche de preuves informatiques et l'exercice extraterritorial des compétences de l'Etat," in S.F.D.I., *Internet et le droit international*, Colloque de Rouen, Pedone, 2014, 357-372.

state.[28] The first issue falls within the scope of the discussions on cybercrime and should therefore not be addressed by the GGE or the OEWG. The second is a matter of international peace and security and, although it is not addressed for political reasons, it should have its place in the ongoing negotiations. This is all the more the case since most state-led cyber operations are carried out by intelligence services. Moreover, any exploitation of a vulnerability for intelligence purposes creates a broader risk, as the vulnerability can also be exploited for other purposes by other malicious actors. Moreover, offensive tools developed by states for intelligence purposes can be stolen and reused, thus directly contributing to their proliferation and international instability. Viewed from two different angles, this subject amounts to asking the following question: Does an unauthorised penetration of the information systems[29] located on the territory of a state undermine its territorial integrity and constitute a violation of its sovereignty?[30] From the answer to this question, however, comes

28. On the applicability of international law on activities of espionage in cyberspace, see, for example: Russell Buchan, *Cyber Espionage and International Law*, Bloomsbury Publishing, 2018.

29. A distinction is made here between the case of direct collection of evidence and that of an order to transmit data issued by a judge in the case of a criminal investigation. In the latter case, the criterion of the territoriality of the data has been reduced in favor of the criterion of personal connection. See: Jennifer Daskal, "Borders and Bits," *Vanderbilt Law Review,* 71, 2018, 179-240; Patrick Jacob, "La compétence des États à l'égard des données numériques : du nuage au brouillard... en attendant l'éclaircie ?," *Revue critique de droit international privé*, 3, 2019, 665-680.

30. On the lawfulness of espionage, it should be recalled that nothing in international law prohibits states from engaging in espionage activities. In other words, espionage in peacetime does not in itself constitute an internationally wrongful act. There is consensus on this analysis. Nevertheless, there are two opposing schools of thought on the lawfulness of espionage. The majority view is that espionage is not in itself unlawful and that no norm of international law limits the ability of states to engage in espionage, but that such activities may constitute violations of international law if they breach specific rules or principles of international law. For example, it is perfectly legal for a state to spy on another state, but sending its agents to the territory of another state would constitute a violation of that state's sovereignty. The minority stream takes what can be described as a functional approach. It considers that espionage is not

the implementation of the secondary rules on the responsibility of the states for internationally wrongful acts, determining in particular the measures that the injured state may take to induce the responsible state to comply with its international obligations.

This situation illustrates the difficulty in setting apart topics of negotiation when they all come back to the same issue and, ultimately, the risk of producing contradictory conclusions. To avoid that problem, it would be necessary to take into account the finality of the act. Here, setting a distinction would without a doubt be interpreted – and rightly so – as an attempt to instrumentalise the principle of sovereignty to make cyber operations lawful when conducted for espionage. This situation also highlights the limits faced by the negotiations on the interpretation of international law applied to cyberspace. In view of the conflicting positions on this subject, it seems unlikely that a consensus can be reached on a principle which is at the basis of the international legal order and from which other principles of international law and the definition of many rights and obligations derive. That raises the question of the delimitation between what should be the subject of a consensus in international negotiations and what should be left to the interpretation of each state.

Thus, the points of divergence between the states on the interpretation of international law remain numerous, whether they pertain to primary norms – such as sovereignty – or on secondary norms – the response to internationally wrongful acts. Identical positions on specific points can be adopted by states usually perceived as antagonistic (this is the case with the French and Russian approach on sovereignty) whereas these same states can fight each other forcefully on other issues. Likewise, the notion of "like-minded" is fictitious and doesn't stand up to a careful

illegal under international law and that this reflects on the acts of espionage. Thus, those acts which should normally constitute internationally wrongful acts, such as the violation of the sovereignty of a state, would not be wrongful because they are carried out for the purpose of espionage and espionage is lawful under international law. For an analysis of the role of espionage in international law, see Fabien Lafouasse, *L'espionnage dans le droit international*, Editions Nouveau Monde, 2012, 492 p.

examination of states' international legal policies. And yet, these divergences risk being accentuated, as we've seen before, by the artificial distinction established between norms of responsible behaviour and international law.

CONCLUSION

As it is an instrument of the foreign policy of the states, international law has become a Gordian knot in international negotiations on the security and stability of cyberspace. This article has demonstrated the role it plays nowadays in the work of two ongoing processes at the UN on peace and stability of cyberspace: the GGE and the OEWG.

Politically speaking, the norms of responsible behaviour unquestionably have a role to play. They can orient the states in the identification of what constitutes responsible behaviour and pave the way for future international law in cyberspace. Yet, we need to underline the relatively artificial nature of the distinction between non-binding legal norms and international law. After analysing in depth this distinction operated in the reports, our study shows that there is a strong link between certain norms and some obligations of international law. Some norms directly derive from obligations of international law, such as the obligation of due diligence, for example, and are primarily there to help interpreting them. In such a context, it seems difficult to operate a strict distinction. It would be counterproductive, or even legally dangerous, for a norm based on an obligation of international law to evolve in a different, or even opposite, direction from the said obligation.

In the current international context, non-binding norms appear as a palliative to international law for two main reasons. First, because they provide an opportunity for states to agree on the interpretation of certain obligations under international law and other elements of responsible behaviour in cyberspace, without setting them in stone. Secondly, these norms could eventually serve as a basis for the transformation of existing rules and principles of international law or even for the formation of new conventional or customary rules. This is a long and uncertain process that should not be neglected, however, as it is at the origin of many existing obligations under international law. Again, these two remarks further underline the often artificial nature of

the distinction between norms and international law. The adoption of norms based on political consensus must therefore take into account their relationship with international law and their potential consequences for its development.

Finally, the operated distinction seems to be the product of power struggles observed during the previous GGEs, or even of a relative polarisation around the positions defended by the United States and Western countries on the one side, and Russia and China on the other. In reality, this relative polarisation is fictitious and there is a mosaic of different approaches sharing many similarities beyond the two "blocs" often described. This diversity of approaches exists on the application of international law in general, but also on its implementation when dealing with cyber operations in particular. The overall situation reaffirms the need for the states to substantially communicate about their approach and their interpretation of the rules and principles of international law, something that only a minority of them has done thus far.

Our study focused on the norms of behaviour and international law in the negotiations at the UN. States, as the main subjects of international law and members of the United Nations, are the primary protagonists. However, it is necessary to note the growing power of new actors, especially on issues related to ICTs. Indeed, some non-state actors are now particularly active in the discussion of norms.[1] They are behind some initiatives proposing or promoting new norms of responsible behaviour. With the multiplication of initiatives from non-state actors and with the development of non-binding norms, we can see that inter-

1. It is no longer possible to study these issues and ongoing state processes, including at the United Nations, without looking at the actions of non-state actors, be they private companies such as Microsoft or expert groups such as the Global Commission for the Stability of Cyberspace (GCSC). In particular, attention should be paid to the influence of these actors on the GGE and the OEWG. For example, consideration could be given to the possible influence of the draft Digital Geneva Convention proposed by Microsoft on the proposal made by some states to open negotiations for the adoption of a legally binding treaty.

national law remains the pillar of the international legal order, even with the need to define the rights and obligations of states in cyberspace. Through the debates and oppositions it entails, its overall usefulness as law organising the peaceful coexistence of states has been reaffirmed. Nevertheless, it is certainly not a panacea[2] and remains the result of power struggles in a context of heightened geopolitical tensions.

2. François Delerue, *Cyber Operations and International Law*, Cambridge University Press, 2020, 493-498.

BIBLIOGRAPHY

ADAMSON Liisi, "International Law and International Cyber Norms. A Continuum?," in Broeders Dennis, van den Berg Bibi (eds.), *Governing Cyberspace. Behavior, Power and Diplomacy*, Rowman & Littlefield, 2020, 25.

BAXTER R. R., "International Law in 'Her Infinite Variety'," *The International and Comparative Law Quarterly*, 29:5, 1980.

BOURGUIGNON Jonathan, "La recherche de preuves informatiques et l'exercice extraterritorial des compétences de l'Etat," in S.F.D.I., *Internet et le droit international*, Colloque de Rouen, Pedone, 2014.

BOYLE Alan E., "Some Reflections on the Relationship of Treaties and Soft Law," *The International and Comparative Law Quarterly*, 48:4, 1999.

BROEDERS Dennis, ADAMSON Liisi and CREEMERS Rogier, *A coalition of the unwilling? Chinese and Russian perspectives on cyberspace*, Policy Brief, November 2019.

BUCHAN Russell, *Cyber Espionage and International Law*, Bloomsbury Publishing, 2018.

CAHIN Gérard, *La coutume internationale et les organisations internationales. L'incidence de la dimension institutionnelle sur le processus coutumier*, Publication de la R.G.D.I.P., Nouvelle Série, 52, Pedone, 2001.

CAZALA Julien, "Le *soft law* international entre inspiration et aspiration ," *Revue interdisciplinaire d'études juridiques*, Vol. 66, 2011/1.

CHINKIN Christine, "Normative Development in the International Legal System," in Dinah Shelton (ed.), *Commitment and Compliance. The Role of Non-Binding Norms in The International Legal Systems*, Oxford University Press, 2000.

COMBACAU Jean and SUR Serge, *Droit international public*, 11th edition, L.G.D.J., Domat, 2014.

DAILLIER Patrick, FORTEAU Mathias and PELLET Alain, *Droit international public*, 8th edition, L.G.D.J., 2009.

DASKAL Jennifer, "Borders and Bits," *Vanderbilt Law Review*, 71, 2018.

DELERUE François, *Cyber Operations and International Law*, Cambridge University Press, 2020.

DELERUE François, *International Law in Cyberspace Matters: This Is How and Why*, EU Cyber Direct, Policy in Focus 2019.

DELERUE François, "Reinterpretation or Contestation of International Law in Cyberspace?" *Israel Law Review*, 52:3, 2019.

DELERUE François, "The Codification of the International Law Applicable to Cyber Operations: A Matter for the ILC?", *ESIL Reflections* 7, 2018.

DELERUE François and GÉRY Aude, "Le droit international et la cyberdefense," in Didier Danet, Amaël Cattaruzza and Stéphane Taillat, *La Cyberdéfense – Politique de l'espace numérique*, Armand Colin, 2018.

DELERUE François and GÉRY Aude, *Etat des lieux et perspectives sur les normes de comportement responsable des Etats et mesures de confiance dans le domaine numérique*, Note Stratégique, CEIS 2017.

DESFORGES Alix, *Approche géopolitique du cyberespace, enjeux pour la défense et la sécurité nationale, l'exemple de la France*, Ph.D. thesis, University Paris 8 Vincennes-Saint-Denis, 2018.

DESFORGES Alix and DOUZET Frédérick, "Du cyberespace à la datasphère. Le nouveau front pionnier de la géographie," *NETCOM*, 32:1-2, 2018.

DOUZET Frédérick and GÉRY Aude, "War and Peace in Cyberspace: Obama's Multifaceted Legacy," in François Vergniolle de Chantal (dir.), *Obama's Fractured Presidency. Policies and Politics*, Edinburgh University Press, 2020.

FERNANDEZ Julian, "Un enjeu et un moyen de la diplomatie des Etats," *Questions Internationales, A quoi sert le droit international ?*, 49, mai-juin 2011.

JACOB Patrick, "La compétence des États à l'égard des données numériques : du nuage au brouillard... en attendant l'éclaircie ?," *Revue critique de droit international privé,* 3, 2019.

KOH Harold Hongju, "International Law in Cyberspace," *Harvard International Law Journal,* Vol. 54, from a speech given to the 2012 USCYBERCOM Inter-Agency Legal Conference.

KRIEGER Heike and NOLTE Georg, *The International Rule of Law – Rise or Decline? – Points of Departure*, KFG Working Paper Series No 1, 2016.

LADREIT DE LACHARRIÈRE Guy, *La politique juridique extérieure*, Economica, 1983.

LAFOUASSE Fabien, *L'espionnage dans le droit international*, Editions Nouveau Monde, 2012.

PELLET Alain, "Le 'bon droit' et l'ivraie – Plaidoyer pour l'ivraie (Remarques sur quelques problèmes de méthode en droit international du développement)," in *Le droit des peuples à disposer d'eux-mêmes : méthodes d'analyse du droit international. Mélanges offerts à Charles Chaumon*, Pedone, 1984.

ROBERTS Anthea, *Is International Law International?*, Oxford University Press, 2017, 432 p.

ROGUSKI Przemyslaw, *Application of International Law to Cyber Operations: A Comparative Analysis of States' Views*, The Hague Program on Cyber Norms, Policy Brief, 2020.

SCHMITT Michael N. and Vihul Liis (eds.), *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2th edition, Cambridge University Press, 2017.

STERN Brigitte, "Quelques observations sur les règles internationales relatives à l'application extraterritoriale du droit," *A.F.D.I.*, Vol. 32, 1986.

STRELTSOV A. A., "La Sécurité de l'information au niveau international : description et aspects juridiques," *Les technologies de l'information et la sécurité internationale, Forum du désarmement,* 2007.

TIKK Eneken, *International Law in Cyberspace: Mind the gap*, Research in Focus, 2020.

TREPPOZ Edouard, "Jurisdiction in the Cyberspace," *Swiss Review of International and European Law*, 26:2, 2016.

REPORT – No. 75

THE GEOPOLITICAL REPRESENTATIONS OF INTERNATIONAL LAW IN THE INTERNATIONAL NEGOTIATIONS ON THE SECURITY AND STABILITY OF CYBERSPACE

François Delerue, Frédérick Douzet and Aude Géry

International law and norms of responsible behaviour are at the heart of the discussions at the United Nations (UN) on Developments in the Field of Information and Telecommunications in the Context of International Security. The purpose of the present study is, therefore, to analyse – and provide food for thought on – the place of international law within the framework of the two processes underway at the UN, the Open-Ended Working Group (OEWG) and the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE). It will also explain how international law is being instrumentalised in the present negotiations.

The study is comprised of three parts. First, it sets out the context in which these two processes arose, their respective mandates, and the place of international law in their work. Secondly, it examines the ambiguities and consequences associated with the distinction between norms of responsible behaviour and international law. Finally, the last part focuses on the interpretation of certain rules of international law, such as, on the one hand, the responses authorised by international law in reaction to a cyber operation and, on the other hand, the principle of sovereignty. The study then analyses the geopolitical motivations behind this.

IRSEM, École militaire
1, place Joffre, case 38 - 75700 Paris SP 07
irsem.fr

IRSEM
INSTITUT DE RECHERCHE STRATÉGIQUE DE L'ÉCOLE MILITAIRE