مجلة الدراسات القانونية المقارنة
المجلد 11/ العـــدد02 (2025)، ص.ص.275-301. ISSN:2478-0022 EISSN:2600-6154

القانون الدولي ومعايير الفضاء السيبراني، بين الفراغ القانوني والاستغلال الجيوسياسي

International law and Norms for cyberspace

Between legal vacuum and geopolitical exploitation

طيب كامش

Tayeb KAMECHE

أستاذ محاضر قسم "أ"، قانون دولي عام، كلية الحقوق والعلوم السياسية، جامعة حسيبة بن بوعلي، الشلف (الجزائر)

Lecturer Class A, Specialization: International Public Law, faculty of Law and political science,Hassiba Ben Bouali University, Chlef, ALGERIA

t. kameche@univ-chlef.dz

تاريخ إرسال المقال:2025/11/05 تاريخ القبول:2025/12/17 تاريخ النشر:2025/12/25

ملخّص:

الفضاء السيبراني هو أحد أبرز المجالات الحديثة التي أثارت نقاشًا واسعًا في القانون الدولي نظرًا لتطورها السريع وتداخلها مع مفاهيم السيادة والأمن القومي وحقوق الإنسان. ورغم أهمية هذا الفضاء في الحياة السياسية والاقتصادية والعسكرية، إلا أنّ المنظومة القانونية الدولية ما تزال تعاني من فراغٍ قانونيٍ واضح، في تنظيمه وضبط سلوك الدول والفاعلين فيه، وتتمثل الإشكالية المركزية في غياب معايير دولية مُلزمة تُحدّد القواعد القانونية لاستخدام الفضاء السيبراني، مما أتاح لبعض القوى الكبرى استغلال هذا الفراغ لخدمة مصالحها الجيوسياسية. ويهدف هذا المقال إلى تحليل مكانة القانون الدولي وكيفية استخدامه في العمليات الدائرة تحت مظلة الأمم المتحدة مثل" مجموعة الخبراء الحكوميين" و"مجموعة العمل المفتوحة العضوية" التي تهدف إلى وضع معايير طوعية لتنظيم السلوك المسئول في الفضاء السيبراني،كما يناقش الدور المشترك لهذه المعايير والقانون الدولي في تنظيم الفضاء الإلكتروني والدوافع الجيوسياسية الكامنة وراء ذلك.

كلمات مفتاحية:

القانون الدولي، معايير الفضاء السيبراني، الأمم المتحدة، مجموعة الخبراء الحكوميين الدوليين.

Abstract:

Cyberspace is one of the most prominent modern fields that has sparked extensive debate in international law due to its rapid development and its overlap

المؤلف المرسل: طيب كامش **Email**: t.kameche@univ-chlef.dz

with concepts of sovereignty, national security, and human rights. Despite its importance in political, economic, and military life, the international legal system still suffers from a clear legal vacuum in regulating it and controlling the behavior of states and actors within it. The central problem lies in the absence of binding international standards that define the legal rules for the use of cyberspace, which has allowed some major powers to exploit this vacuum to serve their geopolitical interests.

This article aims to analyze the role of international law and how it is applied in processes under the auspices of the United Nations, such as the Group of Governmental Experts and the Open-ended Working Group, which aim to develop voluntary standards for regulating responsible behavior in cyberspace. It also discusses the role of these standards and international law together in regulating cyberspace and the underlying geopolitical motivations.

***Keywords**:*
International law, cyberspace standards, United Nations, Group of Governmental Experts.

مـــقدمة

يشكل الفضاء السيبراني أحد أبرز ميادين التفاعل الإنساني الذي أفرزته التطورات التكنولوجية المتسارعة، وهو الآن يشمل الشبكات الرقمية والبنية التحتية للاتصالات والأنظمة الحاسوبية التي تربط الأفراد والدول على مستوى عالمي، وقد وأصبح هذا الفضاء مجالاً مفتوحا للتبادل المعلوماتي والاقتصادي والثقافي، وبالقدر نفسه أصبح ميداناً جديدا للصراعات السياسية والعسكرية والاستخباراتية بين الدول، غير أن هذا التطور المتسارع تجاوز الإطار القانوني التقليدي الذي تأسس لخدمة العلاقات الدولية في عالم مادي وحدودي، أوجد فراغاً قانونيا واضحا في تنظيم استخدام هذا الفضاء، وتحديد المسؤوليات والالتزامات الناشئة عنه.

وفي ظل هذا الفراغ، برزت محاولات متباينة لتأويل قواعد القانون الدولي الكلاسيكية بما يتناسب مع الطبيعة الفريدة للفضاء السيبراني، وسعت بعض القوى الدولية إلى استغلال هذا الفراغ لتحقيق مصالحها الجيوسياسية، عبر فرض رؤى ومعايير تقنية وأمنية تخدم نفوذها الاستراتيجي، بينما يسعى القانون الدولي إلى وضع معايير استخدام الفضاء السيبراني وتحديد القواعد التي تحكم سلوك الدول والجهات الفاعلة غير الحكومية، حيث تشمل هذه المعايير اتفاقيات دولية، ومبادئ مستمدة من القانون الدولي العام مثل ميثاق الأمم المتحدة وقوانين النزاعات المسلحة وحقوق الإنسان، كما تبرز جهود دولية لوضع إطار قانوني ملزم يهدف إلى منع الاعتداءات السيبرانية وحماية البنى التحتية الحيوية، وتعزيز التعاون الدولي في مكافحة الجرائم الالكترونية

وهكذا أصبح تطبيق القانون الدولي على الفضاء السيبراني مصدر ارتباك وخلاف بين الدول، ويخضع لتفسيرات جيوسياسية دولية متناقضة تعقّد المفاوضات حول الوسائل الفعالة لضمان أمن واستقرار الفضاء لسيبراني. لارتباط هذا الفضاء بتصورين الأول: ينظر إليه على أنه فضاء يجب غزوه والسيطرة عليه (لا يخضع لسيادة الدول) وبالتالي هناك

حاجة إلى وضع قواعد جديدة تحدد السلوك المسئول فيه، والثاني ينظر إلى هذا الفضاء على أنه إقليم تُمارس عليه سيادة الدول، وهو بالتالي وسيلة عمل جديدة للتصرف.

وقد يلاحظ المراقب الواعي أن الخلاف حول تطبيق قواعد القانون الدولي على الفضاء السيبراني، كان مع أول قرار صادر عن الجمعية العامة للأمم المتحدة في عام 1998 (وهو أول مبادرة رسمية لتنظيم السلوك في الفضاء الالكتروني) وصولا الى اللقاءات والمؤتمرات التي نظمت فيما بعد في أعمال مجموعات العمل الحكومية الدولية التابعة للأمم المتحدة فمجموعتا العمل الحكوميتان الدوليتان لعامي 2004 و2017 (وهما مجموعتا عمل أنشأتهما الأمم المتحدة بقرار من الجمعية العامة لدراسة التطورات في مجال تكنولوجيا المعلومات) لم يتوصلا التوصل إلى توافق في الآراء لاعتماد تقرير نهائي، وكان سبب هذا الفشل يتعلق أساساً بتطبيق قواعد القانون الدولي.

ورغم اعتماد قرارين من قبل الأمم المتحدة في ديسمبر 2018 (القرار 7327 تحت عنوان "تقدم تكنولوجيا المعلومات والاتصالات والأمن الدولي"، والقرار 266/73 تحت عنوان "تشجيع السلوك المسؤول للدول في الفضاء السيبراني في سياق الأمن الدولي)، اللذين تم بموجبهما إنشاء فريقين للعمل: الفريق العامل المفتوح العضوية(OEWG)[1] وفريق الخبراء الحكوميين السادس (GGE)[2]. إلا أن عمل هذين الفريقين طغت عليهما خلافات شديدة حول الوسائل التي يجب استخدامها لضمان أمن واستقرار الفضاء السيبراني.

ويهدف هذا المقال إلى تقديم تحليل منهجي لمدى قدرة القانون الدولي على مواكبة هذا التحول، والكشف عن أوجه القصور في المعايير الحالية، حيث يكشف هذا المقال أبعاد وخلفيات هذا التوتر الحاصل في تطبيق قواعد القانون الدولي على الفضاء السيبراني، وحول الآثار الجيوسياسية المترتبة على استمرار غياب إطار قانوني موحّد، في عالم يتزايد فيه اعتماد الدول على الفضاء الرقمي كأداة للهيمنة والتأثير وذلك في تساؤل رئيسي نصوغه كالآتي:

هل يمكن للقانون الدولي التقليدي المبني على السيادة الإقليمية والقوة المادية أن ينظم فضاءاً سيبرانياً غير إقليمي وغير مادي، أم أن المعايير السلوكية هي البديل الوحيد في سياق تنافس جيوسياسي يستغل الفراغ القانوني؟.

وللاجابة عن هذا التساؤل وتحليل مكانة القانون الدولي وأدواته في إطار عمليتي التفاوض الرئيسيتين في الأمم المتحدة. سنحاول أن نشرح السياق الجيوسياسي الذي نشأت فيه هاتان العمليتان وكيف تترابط وتتداخل ولاياتهما وهذا في المبحث الأول، أما في المبحث الثاني؛ سنناقش فيه الغموض والتردد الذي يكتنف دور المعايير والقانون الدولي في تنظيم الفضاء السيبراني والدوافع الجيوسياسية الكامنة وراء ذلك، مما يثير الجدل حول ضرورة إبرام معاهدة دولية في هذا المجال.

المبحث الأول: الأمن السيبراني في منظومة الأمم المتحدة وإشكالية انطباق القانون الدولي

تعد المناقشات حول تنظيم الأمن السيبراني تحت رعاية الأمم المتحدة جزءاً من الجهود المستمرة لتعزيز الأمن السيبراني العالمي، ووضع قواعد ومعايير طوعية تحكم سلوك الدول في هذا المجال، وبناء آليات تعاون دولي رغم وجود

اختلافات بين الدول حول السيادة الرقمية والحقوق الإنسانية، وقد شهدت منظومة الأمم المتحدة في السنوات الأخيرة فهما متزايدا لكون الفضاء السيبراني يتطلب الاهتمام بالعواقب المحتملة الناتجة عن ضعف حالة الأمن السيبراني، فهي تتجاوز فعلا تعطيل البنية التحتية لتكنولوجيا المعلومات والاتصالات وأنظمتها وحجم البيانات التي تتعرض للاختراق في نهاية الأمر[3].

وتعمل الأمم المتحدة على تعزيز التعاون الدولي في مجال الأمن السيبراني من خلال عدة آليات مثل القرارات الأممية، واللجان المتخصصة، ولعل وجود هذه الأخيرة كان بفعل العديد من المبادرات الرامية إلى وضع قواعد سلوك دولية في الفضاء السيبراني، وعلية يناقش هذا المحور من الدراسة المبادرات التي دارت في صميم الأمم المتحدة حول تنظيم السلوك في هذا الفضاء منذ نشوئها وتطورها وفيما يلي تقسيم وتقييم لمراحل هذه المبادرات:

المطلب الأول : المبادرات الرئيسية للأمن السيبراني في منظمة الأمم المتحدة

مع التطور التدريجي لاستخدام التكنولوجيا وشيوعها منذ أواخر التسعينات كانت أول مبادرة رسمية لتنظيم السلوك في الفضاء السيبراني من طرف روسيا، حين اقترحت ولأول مرة في سنة 1998 مناقشة الأمن السيبراني في الأمم المتحدة من خلال وثيقة بعنوان "تطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي"[4]، وكانت هذه الوثيقة الأساس لمناقشات لاحقة مما أدى الى اعتماد القرار رقم 70/53 [5] داخل الأمم المتحدة، حيث دعت روسيا من خلالها إلى وضع إطار قانوني لمنع استخدام الفضاء السيبراني في الأعمال العدائية مثل الهجمات على البنية التحتية الحيوية.

لاقت الوثيقة الروسية تحفظات نظراً للاعتراضات التي سُجلت عليها من قبل الولايات المتحدة الأمريكية والدول العربية بحجة أنها تؤدي إلى قيود على حرية الانترنت، إلا أنها أدت فيما بعد إلى مناقشات أوسع وذلك بقرار سنوي حول موضوع الأمن السيبراني من الجمعية العامة للأمم المتحدة في دوراتها اللاحقة أعوام 2004، 2009، 2013 و 2014 و أخيرا 2016 أدت في مجملها إلى التوصل لتوافقات مهمة حول تطبيق القانون الدولي على الفضاء السيبراني ووضع معايير لسلوك الدول في هذا المجال [6].

الفرع الأول: المجموعة الحكومية للخبراء (GGE) بشأن الأمن السيبراني لعام 2004.

استجابة للمبادرة الروسية لعام 1998 التي دعت إلى مناقشة التحديات الأمنية الناشئة عن التطورات في مجال المعلومات والاتصالات، أنشأت الأمم المتحدة أول مجموعة حكومية للخبراء سنة 2004[7] ، وتعتبر هذه المجموعة جزءا من جهود الأمم المتحدة الواسعة لتعزيز الأمن السيبراني ومنع الاستخدامات العدائية لتكنولوجيا المعلومات حيث كان من أهدافها:

- تقييم التحديات والفرص التي يفرضها الأمن السيبراني على الأمن الدولي
- مناقشة سبل تطبيق القانون الدولي على الفضاء السيبراني.
- محاولة وضع إجراءات لبناء الثقة بين الدول للحد من التهديدات السيبرانية، ووضع سياسات يمكن أن تعتمد عليها الدول في أمن واستقرار هذا الفضاء.

استمرت هذه المجموعة في عقد اجتماعات سنوية، ولم يتمكن فريق الخبراء الحكوميين لسنة 2004 في البداية من التوصل إلى توافق في الآراء، ونتيجة لذلك لم يتم اعتماد أي تقرير نهائي[8]،وكان تطبيق قواعد القانون الدولي في ذلك الوقت بالفعل محور الخلافات بين الخبراء الحكوميين.

غير أن اجتماعات فريق الخبراء الحكوميين الثلاثة التالية كانت حاسمة واعتمدت تقارير توافقية، في عام 2010 بالتقرير رقم (65/201) وعام 2013 بالتقرير رقم (68/98) وعام 2015 بالتقرير رقم (70/174)، قدمها الأمين العام إلى الجمعية العامة، التي اكتفت بالإحاطة علماً بها، وأوصت الدول الاسترشاد بها؛ حيث تضمنت هذه التقارير الثلاثة توصيات بشأن تدابير بناء الثقة التي من شأنها تعزيز أمن واستقرار الفضاء السيبراني، وبشأن تدابير التعاون والمساعدة الدولية التي يمكن أن تنفذها الدول، وأخيراً، معايير السلوك المسئول التي تهدف إلى تحديد أفضل لما يشكل سلوكاً مسئولا في الفضاء السيبراني.

وبالفعل، ففي الاجتماع السنوي لفريق الخبراء الحكوميين عام 2013، تم الاعتراف، ولأول مرة، بانطباق القانون الدولي في التقرير النهائي للاجتماع حيث جاء في التقرير ما نصه "إن القانون الدولي، ولاسيما ميثاق الأمم المتحدة، قابل للتطبيق وضروري لصون السلام والاستقرار وتعزيز بيئة معلوماتية مفتوحة وآمنة وسلمية وسهلة المنال"[9].

وقد ذهب تقرير فريق الخبراء الحكوميين لعام 2015، الذي كان له هو الأخير ولاية صريحة للتعامل مع القانون إلى أبعد من ذلك؛ بتخصيص الجزء السادس من التقرير للقانون الدولي، حيث أدرجت فيه الدول الأعضاء عددًا من قواعد القانون الدولي، بما في ذلك مبدأ السيادة وعدم التدخل وحظر استخدام القوة. ومنذ ذلك الحين، أكدت العديد من الدول أنها تتشاطر هذا النهج في مساهماتها الطوعية المقدمة إلى الأمين العام للأمم المتحدة[10]، الأمر الذي سمح بوضع إحدى عشرة قاعدة قانونية طوعية تخص حماية البنى التحتية الحيوية وعدم استهداف الدول الأخرى بعمليات سيبرانية ضارة.

ورغم التقدم المحرز في هذه العملية إلا أن الجولة الخامسة من المفاوضات لفريق العمل انتهت بالفشل في يونيو 2017، إذ لم يتوصل الخبراء الحكوميون المشاركون إلى اتفاق لاعتماد تقرير نهائي توافقي. ويعزى هذا الفشل بشكل خاص إلى رفض ثلاث دول إدراج قابلية تطبيق بعض فروع القانون الدولي في التقرير النهائي، فقد عارضت الصين وكوبا وروسيا ذكر وتطوير "قابلية تطبيق حق الدفاع عن النفس والتدابير المضادة وقانون النزاعات المسلحة " في تقرير مجموعة الخبراء الحكوميين. وأوضح الخبراء الحكوميون الكوبيون والروس أن مثل هذه الإشارة يمكن استخدامها لتبرير عسكرة الفضاء السيبراني وثارت خلافات عميقة في التفسير، وفي ضوء هذه الخلفية تم إنشاء الفريق العامل المفتوح العضوية وفريق الخبراء الحكوميين السادس.

الفرع الثاني: فريق العمل المفتوح العضوية (OEWG) وفريق الخبراء الحكوميين السادس(GGE6)

أنشئ فريق العمل المفتوح العضوية، وفريق الخبراء الحكوميين السادس بموجب القرارين: 27 والقرار 266 في الدورة 73 للجمعية العامة للامم المتحدة [11] على التوالي، واللذين تم اعتمادهما بفارق بضعة أيام بين 5 و 22 ديسمبر 2018، في سياق متوتر بشكل خاص بين الدول، وللمرة الأولى منذ بدء المناقشات في عام 1998 اعتمدت الجمعية العامة قرارين (بدلاً من قرار واحد) بشأن تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي، مما يدل على الانقسام الواضح بين الدول حول هذا الموضوع ويعطي انطباعًا بوجود كتلتين متعارضتين من الدول.

أولاً: خلفيات إنشاء فريقا العمل لسنة 2018 وردود فعل الدول اتجاههما

القرارات التي أدت إلى إنشاء فريق العمل مفتوح العضوية، وفريق الخبراء الحكوميين السادس كانت مقترحة من قبل مجموعتين من الدول تشكلان في الواقع كتلتين متعارضتين؛ فروسيا وبدعم من الصين ودول أخرى اقترحت مشروع قرار أول في أكتوبر 2018[12]، تضمن مشروع القرار هذا فقرة تنص على إنشاء فريق عمل مفتوح العضوية، كما تضمّن قائمة بالمعايير التي اعتمدها الفريق الحكومي الدولي في عام 2015، بالإضافة إلى معايير مدونة السلوك الدولية لأمن المعلومات التي اقترحتها الدول الأعضاء في منظمة شنغهاي للتعاون في عام 2015، والتي رفضتها الدول الغربية آنذاك جملة وتفصيلا (الولايات المتحدة، بدعم من العديد من الدول الأوروبية على وجه الخصوص).

وردًا على ذلك، قدمت الولايات المتحدة الأمريكية، بدعم من عدد من الدول الأوروبية مشروع قرار منافس ينشئ مجموعة خبراء حكوميين سادسة، ويوصي الدول بتنفيذ تقارير مجموعة الخبراء الحكوميين السابقة (تقريري 2013 و2015)[13]، وفي مواجهة الانتقادات العديدة، قامت روسيا والدول الراعية (الجهات المانحة) لمشروع القرار الأول بتعديل مشروعهم. ومع ذلك، لم تسحب الولايات المتحدة والدول الراعية مشروع القرار الخاص بها.

فبالنسبة للولايات المتحدة والدول الأوروبية، كانت النسخة الثانية من مشروع قرار مجموعة العمل المعنية بالتكنولوجيا الحيوية لا تزال تحتوي على أحكام غير مقبولة ولا تعكس بشكل صحيح تقرير عام 2015 الصادر عن مجموعة العمل الحكومية المعنية بالتكنولوجيا والأمن السيبراني. وعلى هذا الأساس نوقشت في اللجنة الأولى للأمم المتحدة مسودتا قرارين متنافسين بشأن تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي، إحداهما مقدمة من روسيا والأخرى من الولايات المتحدة.

وقد جرت هذه المناقشات على خلفية توتر شديد بين مختلف الدول. ووفقًا للبيانات التي أوردت تفاصيل المناقشات، فإن إيران هاجمت الدول التي قدمت مشروع قرار منافس بهدف فرض الأمر الواقع، واتهمت الولايات المتحدة والدول الغربية بأنها تعتبر الفضاء الإلكتروني ساحة معركة وتعمل بنشاط على تطوير أسلحة إلكترونية[14].

أما ممثل جمهورية الصين الشعبية، من جانبه تساءل عما إذا كان تصويت دولة ما ضد مشروع القرار الذي اقترحته روسيا سيسمح لها بالحصول على "تذكرة" للمشاركة في مجموعة الخبراء الحكوميين، وهكذا تعززت صورة وجود كتلتين

متعارضتين من الدول، سواء من قبل الدول التي قدمت القرارين أو من خلال سياق اعتماد هذين القرارين ومضمون المناقشات.

ثانيا: ردود فعل الدول اتجاه انشاء فريقا العمل

يدور عمل هذين الكتلتين حول نهجين غالباً ما يُحللان على أنهما متعارضان تماماً، نهج اتبعته الولايات المتحدة والدول الغربية، التي تصف نفسها بشكل عام بأنها دول متشابهة في التفكير، ونهج اتبعته الصين وروسيا، ومع ذلك ينبغي التمييز بين تجانس هذين الكتلتين من الدول وتعارض مواقفهما[15] في النقاط التالية:

1/ بغض النظر عن التكتل، يتعلق الأمر بمجموعات من الدول التي تشترك في تصور نهج تنظيم الفضاء الالكتروني دون أن تكون متطابقة، فهناك اختلافات كبيرة بين نهج الصين ونهج روسيا[16] رغم أنهما متفقتان، كما توجد اختلافات بين النهج الفرنسي والنهج الأمريكي.

2/ لم تكن غالبية الدول الأعضاء في الأمم المتحدة جزءاً من أي من المجموعتين اللتين قامتا بوضع مشروع هذين القرارين، مما يحد من مفهوم وجود كتلتين من الدول تشكلان طرفي النقيض في المفاوضات الدولية، والأهم من ذلك، أن الغالبية العظمى من الدول الأعضاء في الأمم المتحدة صوتت لصالح القرارين. وقد تم تبني القرار المعنون "تقدم تكنولوجيا المعلومات والاتصالات والسلام والأمن الدوليين" في 5 ديسمبر 2018[17]. أما القرار المعنون بـ :"تشجيع السلوك المسئول للدول في الفضاء السيبراني في سياق الأمن الدولي" تم تبنيه في 22 ديسمبر 2018[18].

يبدو أن هاتين العمليتين متنافستان بالنسبة لكثير من الدول، فالعضوية المحدودة في فريق الخبراء الحكوميين تتيح إحراز تقدم حقيقي في جوهر القضايا، في حين أن العضوية المفتوحة في فريق الخبراء الحكوميين تتيح نهجًا أكثر شمولاً، مما يفتح المجال لسماع أصوات وتوقعات جميع الدول [19].

وقد أظهرت الجلسة الأولى للعمل في مجموعة العمل مفتوحة العضوية التي عقدت في نيويورك في سبتمبر 2019 اهتمام عدد كبير من الدول بالمشاركة في هذه المناقشات وإسماع صوتها، وهو ما تأكد خلال الجلسة الرسمية الثانية التي عقدت في فبراير 2020. وبالتالي، فإن العمليتين الجاريتين لا تضعان كتلتين متجانستين من الدول في مواجهة بعضهما البعض بل إنهما، بحكم تكوينهما، توفران نوعًا من التكامل.

أما الدول الأوروبية فدخلت إلى المناقشات بشكل متفرق، على الرغم من وجود رغبة فيما بينها لتبني نهج مشترك، فقد أثبتت فرنسا نفسها كدولة محركة للمناقشات الدولية في هذا المجال، من خلال إطلاقها لنداء باريس بدعم الدول الأعضاء في الاتحاد الأوروبي[20]، الذي يمثل أوسع مبادرة متعددة الأطراف في مجال أمن الفضاء الإلكتروني تحظى بدعم أكثر من 1200 جهة داعمة من جميع قارات العالم تلتزم هذه الجهات بالعمل يدًا واحدةً من أجل تنفيذ مبادئ نداء باريس واتّباع سلوك مسؤول في مجال الفضاء الإلكترون، إلا أن ذلك بقي مبادرة فرنسية في المقام الأول وليست مبادرة أوروبية مشتركة.

كما اعتمد الاتحاد الأوروبي لـ "صندوق أدوات الدبلوماسية الإلكترونية" الذي تم تنفيذه لأول مرة في يوليو 2020، لكن يبدو أن بعض الدول الأوروبية تميل أكثر إلى العمل في إطار تحالفات أخرى وبالتنسيق مع دول غير أوروبية، ومما يضاعف من صعوبة أوروبا في تأكيد نفسها كقوة موحدة لها تأثير حقيقة أنه خلال عمليات اعتماد القرارات السابقة والتفاوض بشأنها، غالبًا ما كان يُنظر إليها على أنها تتبع الولايات المتحدة.

ومع ذلك، هناك الآن تصميم أوروبي حقيقي على العمل بطريقة متضافرة وإثبات نفسها كقوة دافعة في المناقشات الدولية حيث تمتلك أوروبا، من خلال دولها الأعضاء، ما يلزم لتكون قوة اقتراح حقيقية في المناقشات الدولية وتأكيد مصالحها إذا تمكنت الدول الأوروبية من العمل بشكل متضافر[21]، لا سيما من خلال إبراز خبرتها ونجاحها في تنفيذ التزاماتها الدولية في هذا المجال، فعلى سبيل المثال، يساهم نظام المعلومات الوطنية (المعتمد بتوجيه الاتحاد الأوروبي 1148/2016) واللائحة العامة لحماية البيانات (لائحة الاتحاد الأوروبي 679/2016) في تنفيذ التزامات العناية الواجبة و"خلق ثقافة عالمية للأمن السيبراني"من قبل الدول الأوروبية[22]، وهو ما يؤكد على أن الدول الأوروبية قادرة على تقديم نهج أقل انقسامًا وبالتالي قادرة على التوفيق بين المواقف المختلفة.

على العكس من ذلك، أعلنت الولايات المتحدة، التي تنتقد بشدة الهيئات المتعددة الأطراف منذ تولي دونالد ترامب منصبه كرئيس، منذ البداية عن عدم رغبتها في اعتماد معايير جديدة، مما يثير شكوك المراقبين في استعدادها لاتخاذ نهج بناء وتقديم تنازلات.

ستوفر المناقشات الجارية في إطار الأمم المتحدة والقرارات التي قد يتم اعتمادها معلومات قيّمة عن نهج الدول ومستقبل المناقشات. وقد أبرزت عدة دول التكامل بين العمليتين، ففريق العمل المفتوح العضوية مفتوح لجميع الدول الأعضاء في الأمم المتحدة. وبالتالي، يمكن للدول التي ترغب في المشاركة تقديم اقتراحات، مما يسمح بمراعاة جميع وجهات النظر، على العكس من ذلك، يقتصر تكوين مجموعة الخبراء العالمية على خمسة وعشرين دولة عضواً فقط يتم تعيينهم وفقاً لمبدأ التمثيل الجغرافي [23]، ويكون فيها أعضاء مجلس الأمن أعضاء دائمون بحكم عضويتهم. وبذلك، تبدو مجموعة الخبراء العالمية كهيئة مختصة في هذا الشأن .

المطلب الثاني: إشكالية اختصاصات وولاية فريقا العمل في صياغة معايير وقواعد السلوك السيبراني

يشكّل الفضاء السيبراني أحد أكثر المجالات تعقيداً في النظام القانوني الدولي المعاصر، خصوصاً في ظل بروز مبادرات دولية متعددة تهدف إلى وضع معايير وقواعد سلوك تضبط استخدامه، ضمن هذا السياق، برزت فرق العمل الدولية التابعة للأمم المتحدة و التي أشرنا اليها في المطلب الأول من هذه الدراسة، باعتبارها الجهات الرئيسية المكلفة بصياغة المبادئ القانونية والمعايير غير الملزمة التي توجه سلوك الدول في الفضاء السيبراني. غير أن تعدد هذه اللجان وتباين ولاياتها القانونية أثار إشكاليات تتعلق بتداخل الاختصاصات، حدود الولاية، مدى الشرعية التمثيلية، وإشكاليات التوافق السياسي.

الفرع الأول: إشكالية تداخل الاختصاص وتعدد الولايات

في سياق عمل الأمم المتحدة مجال الأمن السيبراني، يُشار عادةً إلى هذين الهيكلين الرئيسيين، مما يثير أحياناً نقاشات حول تداخل اختصاصاتهما وتعدد ولاياتهما، بالإضافة إلى الإطار الزمني لكل منهما، ففريق العمل المفترح العضوية يختص بصفة رئيسية بإجراء دراسة شاملة عن مشكلة الجريمة السيبرانية، واستعراض الردود عليها من الدول الأعضاء والمجتمع الدولي، والقطاع الخاص بما يشمل ذلك من تبادل المعلومات حول التشريعات الوطنية، وأفضل الممارسات و المساعدة الفنية والتعاون الدولي، مع اقتراح خيارات لتعزيز الردود الوطنية والدولية.

أما فريق الخبراء الحكوميين باعتباره هيئة مؤقتة تنشئها الجمعية العامة، ويعمل في إطار ولايات محددة من الجمعية العامة فيختص بإعداد التقارير التي تمثل توافقاً تاريخياً للآراء حول كيفية تطبيق القانون الدولي على الفضاء السيبراني ووضع قواعد السلوك المسؤول للدول ، وتركز مهامه بصورة رئيسية على سيادة الدول وسلوكها في سياق الأمن الدولي ونزع السلاح، والأساس القانوني للانطباق الكامل للقانون الدولي، بما في ذلك ميثاق الأمم المتحدة، على الفضاء السيبراني.

ويوضح الجدول التالي المهام الرئيسية و العملية و الجدول الزمني لكل من فريقي العمل الرئيسيين في الأمم المتحدة و اللذان يخصان بالأمن في الفضاء السيبراني:

الجدول رقم 01: يوضح الجدول التالي المهام الرئيسية والإطار الزمني لكل فريق

الفريق / الجانب	فريق العمل المفتوح العضوية (OEWG)	فريق الخبراء الحكومي (GGE)
الولاية والتركيز	حوار شامل ومفتوح لجميع الدول الأعضاء في الأمم المتحدة والجهات الفاعلة التركيز على التنفيذ العملي للمعايير الحالية، وبناء الثقة، وبناء القدرات	فريق أصغر يركز على الجوانب الفنية والقانونية العميقة، مثل كيفية تطبيق القانون الدولي في الفضاء السيبراني
الاختصاصات الرئيسية	– مناقشة التهديدات الناشئة في مجال الأمن السيبراني – تعزيز تنفيذ معايير السلوك المسؤول للدول – تعزيز تدابير بناء الثقة بين الدول – تعزيز جهود بناء القدرات، خاصة للدول النامية .	– دراسة كيفية انطباق القانون الدولي على استخدام تكنولوجيا المعلومات والاتصالات في السياق الأمني – تحديد معايير جديدة للسلوك المسؤول للدول في الفضاء السيبراني.
العضوية والمشاركة	مفتوح لجميع الدول الأعضاء في الأمم المتحدة، مما يجعله أكثر شمولية	عضويته محدودة، حيث يتكون من خبراء من عدد مختار من الدول
المدة / المرحلة	2021 – 2025. تم الاتفاق على	عمل عبر عدة دورات (مثل 2016–2017

	استمرار العمل من خلال "الآلية العالمية" التي ستبدأ عملها في عام 2026	2018، 2021 .

المصدر : من اعداد الباحث بناءا على المراجع المتوفرة

ويتضح من خلال هذا الجدول أن اختصاصات وصلاحيات فريقا العمل الرئيسيان تبدو متشابهة لدرجة أنها تتداخل إلى حد كبير، وتشمل ولاية المجموعتين العمل على تطوير المعايير غير الملزمة ووضع القواعد والمبادئ الخاصة بالسلوك المسؤول للدول في الفضاء السيبراني، وتدابير بناء الثقة وتعزيز القدرات، وتطبيق قواعد القانون الدولي فيها، ومع ذلك هناك تفسيرات وقراءات مختلفة لولايتهما تعكس انقسامات جيوسياسية بين الدول الغربية (مثل الولايات المتحدة وأوروبا) والدول مثل روسيا والصين، خاصة حول التوازن بين السيادة الدولية، حقوق الإنسان، والسيطرة على الإنترنت .

كما يوضح الجدول أنه يمكن لمجموعة العمل الحكومية إجراء مشاورات مع الدول غير المشاركة في المجموعة والمنظمات الإقليمية المختصة، أما الفريق التقني لمجموعة العمل المقتوحة العضوية والمعنية بالاتفاقية (OEWG) فسيعقد جلسات استشارية غير رسمية مع القطاع الخاص والمنظمات غير الحكومية، كما يُسمح للجهات الفاعلة غير الحكومية بالمشاركة في الجلسات الرسمية، وتجدر الإشارة هنا إلى أنه بعد رفض الصين، لم يُسمح إلا للمنظمات المعتمدة لدى المجلس الاقتصادي والاجتماعي للأمم المتحدة (Ecosoc) بحضور الجلسات الرسمية.

ينص القرار رقم 266 الذي يحدد ولاية الفريق الحكومي الدولي على أن التقرير الذي يقدم إلى الجمعية العامة يكون "مصحوباً بملحق يحتوي على المساهمات الوطنية للخبراء الحكوميين حول كيفية تطبيق القانون الدولي على استخدام الدول لتكنولوجيات المعلومات والاتصالات" (الفقرة 3)، وبالتالي يتعين على الدول الخمس والعشرين المشاركة في مجموعة الخبراء الحكومية توضيح موقفها بشأن القانون الدولي المطبق على العمليات الإلكترونية، هذا ما قامت به فرنسا وهولندا على وجه الخصوص من خلال نشر تقريرين: الأول من قبل وزارة الدفاع الفرنسية بعنوان "القانون الدولي المطبق على العمليات في الفضاء الإلكتروني"[24] ووثيقة رسمية من وزارة الخارجية الهولندية بعنوان "القانون الدولي في الفضاء الإلكتروني" [25]. وستكون هاتان الوثيقتان اللتان نُشرتا في 9 سبتمبر و14 أكتوبر 2019، بمثابة مساهمة وطنية في أعمال مجموعة الخبراء الحكومية.

وأخيرًا، سيكلف الفريق العامل المعني بالاتصالات الإلكترونية بدراسة إمكانية إقامة حوار مؤسسي منتظم على أوسع نطاق ممكن تحت رعاية الأمم المتحدة[26] بما في ذلك إجراء مناقشات حول إنشاء هيئة أو عملية دائمة لمعالجة مسألة تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي.

الفرع الثاني: خلافات الرأي بين الدول بشأن الجدول الزمني ومضمون الولاية:

هناك تفسيرات وقراءات مختلفة لولاية فريق العمل المفتوح العضوية وفريق الخبراء الحكوميين تعكس انقسامات جيوسياسية بين الدول الغربية (مثل الولايات المتحدة وأوروبا) والدول مثل روسيا والصين، ومن الاختلافات التي تثير القلق ما يتعلق بالعنصر الأول منها بالجدول الزمني للعملية، حيث كان من المقرر أن ينتهي الفريق العامل المفتوح العضوية من أعماله في عام 2020، خلال الدورة الخامسة والسبعين للجمعية العامة للأمم المتحدة، أي قبل عام من انتهاء ولاية الفريق الحكومي الدولي (الذي كان من المقرر أن ينتهي في عام 2021 خلال الدورة السادسة والسبعين) وأتاح تمديد الدورة الخامسة والسبعين حتى مارس 2021 تمديد أعمال الفريق الحكومي الدولي المعني بالاتفاقية الشاملة للحد من التسليح الزائد للفضاء السيبراني، مما يمكّن من تقديم التقرير خلال الدورة السادسة والسبعين. لكن سيظل هناك فارق زمني (بضعة أشهر) بين تقديم التقريرين المحتملين. وتخشى بعض الدول أن يؤدي هذا الفارق الزمني إلى تغيير موقف الدول التي كانت وراء قرار إنشاء الفريق العامل المفتوح العضوية بعد انتهاء أعماله.

العنصر الثاني من الخلافات يتعلق بمضمون الولاية؛ حيث سيتم مناقشة القانون الدولي في إطار العمليتين، وهو موضوع محوري في أعمالهما. ويمثل هذا الوضع فرصة ومخاطرة في آن واحد؛ فرصة للدول لإجراء مناقشات معمقة حول هذه القضايا والقدرة على مناقشة تفسير القانون الدولي في هذا السياق الجديد للسلام والأمن الدوليين؛ ومخاطرة بأن تسلك العمليتان اتجاهين متباينين، مما يخلق وضعًا غير مستقر للنظام القانوني الدولي، نفس الأمر ينطبق على معايير السلوك المسئول للدول، التي يذكرها القرار 27/73 مرتين في تعريف ولاية الفريق الحكومي الدولي المعني بمعايير السلوك المسئول نفس الأمر ينطبق على معايير السلوك المسؤول للدول وبالتالي، فإن الوضع حساس من ناحيتين:

الناحية الأولى، ترد الإشارة إلى المعايير في القرار 27/73 في بداية تعريف الولاية حيث جاء في الفقرة 5 من القرار "تقرر الجمعية العامة في أن تكلف الفريق الحكومي الدولي، على أساس التوافق في الآراء، بمواصلة وضع القواعد والمعايير والمبادئ الخاصة بالسلوك المسئول للدول المشار إليها في الفقرة 1من هذا القرار، على سبيل الأولوية، وتحديد سبل تطبيقها؛ وإدخال تغييرات عليها أو وضع قواعد جديدة، حسب الاقتضاء" [(27)]. وبالتالي فإن المعايير الواردة في قرار الجمعية العامة هي التي ينبغي أن تشكل أساس عمل الفريق العامل المختلط. وبما أن هذه المعايير تختلف قليلاً عن تلك الواردة في تقرير الفريق الحكومي الدولي لعام 2015[(28)] فإن ذلك يعني أن أساس عمل المجموعتين قد يختلف، وسيؤدي ذلك في الواقع إلى زيادة خطر حدوث تناقضات أو اختلافات في التوصيات التي سيتم اعتمادها في مختلف العمليات[(29)].

لكن في ضوء الممارسات التي اتبعتها الدول حتى الآن، يلاحظ أنه قد زال خطر حدوث هذه التناقضات إذ أن الغالبية العظمى من الدول أشارت، خلال الدورتين الأوليين للفريق العامل المفتوح العضوية إلى أنها تسترشد بقواعد المجموعة الحكومية للخبراء وليس بالقواعد الواردة في القرار 27/73، وهذا يوضح عدم وجود توافق في الآراء بشأن

المعايير المنصوص عليها في القرار 27/73، ولكنه يؤدي أيضاً إلى وجود تباين بين التطبيق الحرفي للولاية والممارسة المتبعة في إجراء المفاوضات.

كما أن مسألة قاعدة العمل هي الأخرى تؤثر في المفاوضات الدائرة في إطار العمليتين، حيث ينص القرار 73/27 أن مجموعة العمل الحكومية الدولية المعنية بالمعايير مفوضة بأن"...تحدد وسائل تطبيق هذه المعايير" وبذلك، سيكون على الدول الأعضاء أن تحدد تفاصيل تفعيل المعايير المتفق عليها، وبما أن العديد من هذه المعايير إعلانية الطابع، فإنها تحتاج إلى توضيح من أجل تنفيذها.

الناحية الثانية: ترد الإشارة الثانية إلى المعايير في الجزء الثاني من تعريف الولاية في القرار 27/73، حيث لم يتم تحديد هذه المرة المعايير المقصودة، مما يثير التساؤل حول المعايير المرجعية. هل هي المعايير المنصوص عليها في القرار أم تلك التي اعتمدتها مجموعة الخبراء الحكومية التابعة للأمم المتحدة في عامي 2013 و2015؟.

ويبدو أن هذه التساؤلات قد حُسمت في الوقت الحالي من خلال الممارسة حيث تفضل الدول اعتماد معايير المجموعة الحكومية كأساس للمناقشة. ومع ذلك، قد تكون هذه التساؤلات مصدراً للتناقضات بين العمليتين، حيث أن المجموعة الحكومية والمجموعة التقنية غير الحكومية مكلفتان بالعمل على هذه الأحكام.

وبما أن كلا العمليتين تشملان في ولايتهما مسألة القانون الدولي ومعايير السلوك المسئول، فإن السؤال الذي يطرح نفسه هو مسألة توزيع العمل؛ ففي كلمته خلال الجلسة الأولى للفريق العامل المفتوح العضوية في يونيو 2019، اقترح الممثل الخاص لرئيس الاتحاد الروسي للتعاون الدولي في مجال أمن المعلومات أن يتناول الفريق العامل المفتوح العضوية مسألة معايير السلوك المسئول، وتدابير بناء الثقة، وتدابير التعاون والمساعدة الدولية، تاركاً مسألة القانون الدولي للفريق العامل المحدود العضوية [30]. لكن هذا الاقتراح لم يتم العمل به، وبالتالي تعمل العمليتان بالتوازي على جميع هذه القضايا.

المبحث الثاني: التردد والخلاف حول الوسائل التي يجب استخدامها لأمن واستقرار الفضاء السيبراني

يحكم النقاش حول الوسائل المثلى لضمان أمن الفضاء السيبراني حالة من الارتباك والخلاف العميق، ينبع من صعوبة التوفيق بين السيادة الوطنية والحاجة إلى تعاون دولي فعال، وسط بيئة تكنولوجية سريعة التغير، ومع تزايد الهجمات السيبرانية، مثل تلك التي استهدفت البنى التحتية الحيوية خاصة خلال جائحة كوفيد-19، أصبح تطبيق القانون الدولي في هذا الفضاء مصدر ارتباك وخلاف بين الدول، خاصة حول الوسائل الفعالة لضمان أمنه واستقراره، ويناقش هذا المحور من البحث محاور الخلاف الرئيسية حول الوسائل المناسبة التي تعكس التناقض والخلاف بين الدول في سبيل تطبيق القانون الدولي على الفضاء السيبراني أو تطبيق معايير السلوك المسئول في هذا الفضاء وذلك فيما يلي:

المطلب الأول: الإطار المعياري والقانوني الحالي وأوجه القصور فيه

مع الاعتماد المتزايد على الفضاء السيبراني أصبح هذا الأخير ساحة للتنافس والصراع، مما يهدد استقرار الدول والأفراد على حد سواء، وتكمن الإشكالية المحورية في أن البيئة التنظيمية الحالية لهذا الفضاء لا تواكب خطورة التهديدات وسرعة تطورها، مما يخلق حالة من "التردد والخلاف" حول الوسائل المثلى لتحقيق الأمن والاستقرار. ويستند الجدل الدائر إلى فجوة عميقة بين واقعين: الأول، واقع الإطار المعياري والقانوني الدولي الحالي الذي يوصف بأنه مجزأ، طوعي، وغير ملزم في معظمه، ويعتمد على مبادئ عامة يصعب ترجمتها إلى مساءلة فعلية. والثاني، واقع التهديدات السيبرانية المتطورة والمستمرة، والتي تتسم بطابعها العابر للحدود وتعقيدها التقني، مما يجعل المواجهة الفردية للدول غير كافية بل وقد تزيد من حالة عدم الاستقرار.

لذا، فإن هذا المطلب يسعى إلى دراسة هذه الإشكالية من خلال تحليل نقدي لمكونات الإطار الحالي، واستقراء الخلافات الجوهرية حول أدوات تنفيذه، حيث يمثل الإطار الحالي للمعايير والقانون الدولي نقطة التقاء وخلاف في الوقت ذاته، ويمكن حصر هذه الخلافات في النقاط التالية:

الفرع الأول: طبيعة معايير السلوك المسئول غير الملزمة

تعتمد المعايير الدولية الحالية، التي أوصت بها المجموعات الحكومية للخبراء الدوليين والتي تم الاتفاق عليها في منظمة الأمم المتحدة، على الطوعية وعدم الالزامية القانونية، حيث يتضمن تقرير المجموعة الحكومية للخبراء الدوليين في مجال الأمن السيبراني لعام 2013 جزءًا مخصصًا للمعايير والقواعد والمبادئ الخاصة بالسلوك المسئول للدول، ولم تعترف الدول الأعضاء في هذه المجموعة بانطباق القانون الدولي على الفضاء السيبراني فحسب، بل اعتمدت أيضًا عدّة معايير من أجل تعزيز أمن واستقرار البيئة المعلوماتية العالمية (احترام الحريات الأساسية في استخدام تكنولوجيا المعلومات والاتصالات، وتكثيف التعاون لمكافحة استخدام الأدوات المعلوماتية لأغراض إجرامية، واحترام القانون الدولي...). ويظهر من تحليل تقرير المجموعة أن العديد من هذه المعايير تستند إلى الاعتراف بانطباق القانون الدولي على الفضاء السيبراني، وتعيد صياغة الالتزامات الدولية القائمة في سياق الرقمية[31].

لكن في تقرير مجموعة الخبراء الحكوميين لعام 2015 (الذي وضع إحدى عشر قاعدة طوعية) اختارت الدول الأعضاء التمييز بين معايير السلوك المسئول من جهة، والقانون الدولي من جهة أخرى، إلا أن هذا التمييز يغفل الروابط التي قد توجد بين معايير السلوك المسئول، التي تندرج في إطار القانون غير الملزم (أي أنها غير ملزمة قانونًا) والقانون الدولي، الذي تذكر المجموعة بعض قواعده، وقد أدى هذا التمييز إلى تعقيد تعريف حقوق وواجبات الدول في الفضاء السيبراني من خلال إدخال التباس حول طبيعة القواعد وتعقيد سير المفاوضات.

إن هذا التمييز (الذي جاء جزأين منفصلين من التقرير) بين المعايير غير الملزمة للسلوك المسئول للدول من جهة، والقانون الدولي من جهة أخرى، ينطوي على ثلاثة قيود:

أولا: القيد المرتبط بعدم الزامية معايير السلوك المسئول

يرتبط هذا القيد بحقيقة أن طبيعة الأحكام المذكورة في الجزء المتعلق بالمعايير القانونية الاختيارية وغير الملزمة التي لا تُحظر الأفعال التي تحترم القانون الدولي"[32]، لذا فانتهاكها لا يرتب على الدولة المنتهكة المسؤولية الدولية، ولعل التساؤل المطروح هنا هو ما فائدة ذكر ذلك في تقرير فريق الخبراء الحكومي الدولي، ما دام ذلك مجرد تقرير خبراء ولا يمكنه بأي حال من الأحوال أن يفرض معايير ملزمة للدول. هذا القيد ورد في الجزء المخصص للقانون الدولي، حيث أن الأحكام الواردة في الجزء المخصص للقانون الدولي في تقرير عام 2015 الصادر عن مجموعة الخبراء الحكومية الدولية ليست أكثر إلزامية من تلك الواردة في الجزء المخصص للمعايير، فهي تظل مجرد توصيات، وبالتالي يمكن القول معايير السلوك المسئول ليس لها أي طابع الزامي ويجب التمييز بينها و بين الالتزامات المنصوص عليها في القانون الدولي والتي تمت دراستها في جزء آخر من التقرير [33].

ثانياً: القيد المرتبط بالتمييز بين معايير السلوك المسئول والتزامات القانون الدولي

تُعد الصلة بين معايير السلوك المسؤول في الفضاء السيبراني والتزامات القانون الدولي صلة تكاملية وتدعيمية، حيث تبني هذه المعايير على القانون الدولي القائم وتكمله دون أن تكون ملزمة قانونيًا في حد ذاتها. وفقًا للأمم المتحدة والمنظمات الدولية مثل اللجنة الدولية للصليب الأحمر، يُعترف بأن القانون الدولي ينطبق على الفضاء السيبراني، وتشمل التزاماته مبادئ مثل احترام السيادة الدولية، وحظر استخدام القوة، وحق الدفاع عن النفس بموجب المادة 51 من ميثاق الأمم المتحدة، بالإضافة إلى قواعد القانون الإنساني الدولي أثناء النزاعات المسلحة[34]

وتشكل معايير السلوك المسؤول، التي تم تطويرها من خلال مجموعات خبراء حكوميين في الأمم المتحدة (مثل تقرير مجموعة الخبراء الحكوميين لعام 2015)، إرشادات طوعية غير ملزمة تهدف إلى تعزيز الاستقرار والأمن في الفضاء السيبراني من خلال تحديد سلوكيات متوقعة للدول. هذه المعايير تركز على جوانب مثل عدم إجراء أو دعم عمليات سيبرانية تؤدي إلى سرقة الملكية الفكرية لأغراض تجارية، أو إلحاق الضرر بالبنية التحتية الحيوية، أو عرقلة فرق الاستجابة للحوادث الأمنية السيبرانية بالإضافة إلى التعاون الدولي في التحقيق في الجرائم السيبرانية

غير أن التمييز بينها وبين التزامات القانون الدولي يغفل هذه الصلة، فلا يمكن وصف الالتزامات غير ملزمة على أنها غير قانونية مقارنة بقواعد القانون التي تعتبر القواعد الوحيدة الملزمة، بل إنها تندرج في إطار "التدرج المعياري" بين القانوني وغير القانوني[35]،هذه الأحكام غير الملزمة، التي غالباً ما يشار إليها باسم "القانون اللّين"، يمكن أن تساهم في

تفسير الالتزامات القائمة بموجب القانون الدولي، بل وحتى في تشكيل التزامات دولية جديدة، فغياب الطابع الملزم لا يعني غياب الأثر القانوني[36].

ثالثاً: القيد المرتبط بواجب الرعاية وواجب حماية حقوق الإنسان واحترامها

يرتبط هذا القيد بالإشارة، سواء في الجزء المخصص للمعايير في التقرير أو في الجزء الذي يتناول القانون الدولي، إلى واجب الرعاية وواجب حماية حقوق الإنسان واحترامها [37] ويُظهر هذه التكرار وجود صلة بينهما، وأن الدول غير قادرة تماماً على التمييز بينهما، بل وأن هذا التمييز يبدو مصطنعاً أيضا من الناحيتين الشكلية والموضوعية. ويُظهر تحليل محتوى معايير السلوك المسئول أنه يمكن تصنيفها إلى فئتين: معايير تحدّد الممارسات الجيدة التي تسمح بتعزيز أمن واستقرار بيئة المعلومات العالمية؛ ومعايير أخرى تستند إلى التزامات القانون الدولي المطبقة على سلوك الدول في الفضاء السيبراني، وعليه فان الفئة الثانية من المعايير تحافظ على ارتباط مادي وثيق بالقانون الدولي. ونظراً لارتباطهما، فان الفصل القائم بين الالتزامات بموجب القانون الدولي الواردة في التقرير والمعايير من شأنه أن يثير مشكلتين:

الأولى: من شأن هذا التمييز أن يطرح مشكلة فيما يتعلق بتحديد حقوق الدول والتزاماتها، فعندما يعيد معيار السلوك المسئول صياغة التزام دولي، يطرح التساؤل حول ما إذا كان المقصود هنا الحفاظ على الصلة القائمة بين المعيار والالتزام الدولي نفسه، وماهي العواقب التي يمكن استخلاصها من هذا الفصل مادام المحتوى واحد؟ هل يعني هذا الفصل أن تنفيذ الالتزام الدولي الوارد في المعيار في الفضاء السيبراني سيكون مجرد توصية منفصلة عن الالتزام الدولي الذي يستند إليه ؟.والراجح أن الدولة ملزمة في جميع الأحوال باحترام الالتزامات الدولية. ومع ذلك، قد تكون الرسالة التي تنقلها هذه العبارة تسبب بعض الالتباس. فقد تعطي انطباعًا بأن المعيار منفصل عن القانون الدولي ليصبح مستقلاً، وإذا لزم الأمر، فان السلوك المتبع في الفضاء السيبراني لن يكون قائما على التزام دولي (أي ملزم) بل على حسن نية الدولة.

علاوة على ذلك، تميل بعض المعايير إلى تفسير الالتزامات المنصوص عليها في القانون الدولي، بينما تكتفي أخرى بإعادة صياغتها فقط، كما تميل بعض الأحكام الواردة في القسم المخصص للقانون الدولي إلى تفسير الالتزامات الدولية، بينما تكتفي أحكام أخرى بإعادة ذكرها. فكيف يمكننا إذن التمييز بين ما هو مجرد تكرار لأحكام القانون الدولي وبين ما هو تفسير لالتزام دولي في الفضاء السيبراني.

على سبيل المثال، عندما تفسر الأحكام الواردة في الجزء المتعلق بالقانون الدولي باعتبارها التزامًا دوليًا تفسيرًا ضيقًا، في حين أن الأحكام الواردة في الجزء المخصص للمعايير تكتفي بإعادة صياغته، فهل يعني ذلك أن الحكم الأول له وزن أكبر لأنه يقع في قسم القانون الدولي، وإذا كان الأمر كذلك، فهل يعني أن التفسير الذي يجب اعتماده للالتزام الدولي يكون أكثر تقييدًا في مضمونه عند تطبيقه على الفضاء السيبراني.

المشكلة الثانية، قد يشكل هذا التمييز مشكلة فيما يتعلق بإجراء المفاوضات الدولية، سواء في إطار مجموعة العمل المفتوحة العضوية أو مجموعة الخبراء الحكوميين؛ حيث ستناقش الدول المعايير والقانون الدولي في وقتين مختلفين (ما يعني أن المعايير والقانون الدولي يتم تناولهما بشكل منفصل) لأن جلسات العمل تنظم حسب الموضوعات، وبما أن هاتين المسألتين مرتبطتان، لا سيما من حيث المضمون، فهناك خطر أن تتناول الدول المسألة نفسها مرتين وتتخذ مواقف مختلفة، بل ومتناقضة.

فضلا عن ذلك، بما أن المناقشات الجارية حول المعايير تركز بشكل أساسي على تفعيلها (أي تنفيذها بشكل ملموس) فإن الأحكام التي يتم اعتمادها ستساهم في تفسير الالتزامات الدولية. غير أن مسألة المحتوى تشمل أيضاً الجوانب التي لا تتناولها الأحكام التي تحدد تنفيذ المعايير وبالتالي (تفسر الالتزامات الدولية). فهل ينبغي اعتبار أن عدم إدراج بعض التفاصيل يرجع إلى أنها لا تنبع من تنفيذ الالتزام الدولي الذي تم تحديد تطبيقه على الفضاء الإلكتروني؟ أم ينبغي اعتبار أن العناصر غير المذكورة لا تؤثر على تفسير الالتزام الدولي؟

وعليه، فإن التمييز بين معايير السلوك المسئول والأحكام المتعلقة بالقانون الدولي ليس واضحاً وصارماً كما يوحي التقرير. وفي نهاية المطاف، فإن مفهوم معيار السلوك المسئول ذاته في علاقته بالقانون الدولي هو الذي يمكن أن يكون موضع تساؤل من وجهة نظر موضوعية. والتساؤل هنا عما إذا كانت المعايير "تهدف بالفعل إلى تعزيز القانون الدولي وتقويته أو ما إذا كان إطار "السلوك المسؤول للدولة" هو طريقة ملتوية للقانون الدولي[38]

وخلاصة القول، أن المعايير لا تُلغي أو تُعدل القانون الدولي؛ بل تكمله. على سبيل المثال، أقر تقرير فريق الخبراء الحكوميين التابع للأمم المتحدة بشأن الأمن السيبراني في تعريفه لمعيار التزام بالعناية الواجبة بأن "توقع عام للدول لاتخاذ إجراءات معقولة لمنع استخدام أراضيها في أعمال ضارة" أي يجب على الدولة عدم السماح عمدا باستخدام أراضيها لأعمال غير مشروعة دوليا باستخدام تقنيات المعلومات والاتصالات[39]، وهذا يقع في قاعدة الواجب الاجتهادي، لكنه يظل غير ملزم كقاعدة قانونية. مما يساعد في تجنب التصعيد، لكن الانتهاكات القانونية تُثير مسؤولية دولية كاملة.

كما يؤكد التقرير أن هذه المعايير ضرورية لسد الفجوات في القانون الدولي، خاصة في ظل التهديدات السيبرانية المتزايدة، لكنها لا تحل محله. هذا التمييز يعكس التوازن بين الالتزام الطوعي والإلزام القانوني لتعزيز الأمن السيبراني العالمي من الناحية الموضوعية، أما من الناحية الشكلية فيمكن استخدامه كنقطة انطلاق لتبرير صياغة معاهدة.

الفرع الثاني: معضلة الإسناد القانوني للهجمات السيبرانية:

تعد مسألة الإسناد أي، تحديد وتوثيق مصدر الهجوم السيبراني بدقة مقبولة قانونياً، واحدة من أعقد المعضلات التي تواجه المجتمع الدولي في مواجهة الجرائم السيبرانية، وتشكل حجر عثرة أمام المساءلة والردع، وثغرة استراتيجية يستغلها المهاجمون للتملص من العقاب. ومعضلة الإسناد القانوني للهجمات السيبرانية هي عقبة أساسية تواجه كذلك تطبيق القانون الدولي وتطوير معايير أمن الفضاء السيبراني. تعود الصعوبات الرئيسية إلى العوائق التقنية والسياسية المترابطة، مما يؤدي إلى حالة من "التردد والخلاف" حول الاستجابة المناسبة، وفيما يلي بيان أبعاد ومستويات هذه المعضلة .

أولاً: التحديات التقنية

تعد عملية الإسناد التقني في إثبات هوية المهاجم ونسب الهجوم إليه بدقة التحدي الأكبر في طريق المساءلة، فالمهاجم يستخدم عادة سلاسل طويلة من الخوادم المخترقة في دول متعددة ويستخدم برمجيات خبيثة معاد توظيفها بواسطة وسائل تقنية متطورة، فضلاً عن التجاء بعض الدول إلى استخدام "الوكلاء" (الجماعات غير الحكومية) الذي يضيف طبقة من الغموض، ويصعب التمييز بين هجوم من دولة أو جماعة مستقلة. وعليه فالإسناد ليس مجرد مسألة تقنية بحتة، بل هو عملية سياسية بالدرجة الأولى تحتاج إلى معلومات كافية لإقناع صناع القرار والرأي العام العالمي، و في ظل غياب وكالة دولية محايدة ومتفق عليها للتحقيق في الهجمات الإلكترونية – على غرار الوكالة الدولية للطاقة الذرية – يُصعب عملية الإسناد ويسمح للدول الكبرى باعتراض إنشاء مثل هذه الآليات حفاظاً على سيادتها .

وأمام غياب معيار دولي موحد للإسناد بحيث فشلت حتى الآن مجموعة الخبراء الحكوميين ومجموعة العمل مفتوحة العضوية في الأمم المتحدة (كما تطرقنا في المبحث الأول) في التوافق على قواعد إسناد ملزمة وموحدة تبقى هذه المعضلة قائمة خاصة في ظل الفجوة الكبيرة بين الإسناد التقني والإسناد القانوني بحيث حتى لو تأكدت دولة ما تقنيا أن جهة معينة هي المسئولة فان هذا لا يكفي من الناحية القانونية لاتخاذ اجراءات (عقوبات، رد عسكري أو ملاحقة جنائية) ضد هذه الجهة لأن القانون الدولي يطالب بمستوى اثبات في أحسن الاحوال وهذا مستحيل تقريبا من الفضاء السيبراني

ثانياً: التحديات القانونية

أمام غياب معيار دولي موحد للإسناد يصعب جمع الأدلة الرقمية القابلة للاعتماد أمام القضاء، فهي معرضة للتلف أو التعديل، كما أن الاختلاف بين القوانين الوطنية وعدم وجود اتفاقية دولية شاملة حول إجراءات التحقيق في الجرائم السيبرانية يحد من التعاون. بالإضافة إلى ذلك، يسأل القانون الدولي عن نطاق الاستجابة المسموح بها للهجوم السيبراني.

3/ التحديات الجيوسياسية:

غالباً ما يكون الإسناد النهائي قراراً سياسياً وليس مجرد نتيجة فنية. هذا يخلق مجالاً للإنكار المتبادل، حيث تنفي الدول التورط، كما حدث في هجمات التبت عام 2024 المنسوبة للصين. كما أن نقص الإرادة السياسية أو الصراع الجيوسياسي بين الدول قد يعيق عملية المساءلة.

تظهر معضلة الإسناد أن "التردد والخلاف" حول الوسائل ليس ضعفاً، بل هو انعكاس لتعقيد الفضاء السيبراني، إن غياب اليقين القانوني والفني يجعل من الصعب الاتفاق على قواعد ملزمة وآليات مساءلة فعالة، بينما الحل الفعال يتطلب نهجاً متكاملاً يجمع بين التقدم التقني (مثل الذكاء الاصطناعي للتحليل)، وتطوير الأطر القانونية، والإرادة السياسية لبناء الثقة والتعاون الدولي.

وفي الاخير يمكن القول ان الخلاف والارتباك حول وسائل ضمان أمن الفضاء السيبراني يعكس واقعاً أكثر تعقيداً من مجرد نقص في التنظيم، إنه انعكاس للتنافس الجيوسياسي والتصورات المختلفة للسيادة في العصر الرقمي. بينما تشكل المعايير الحالية والقانون الدولي أساساً لا غنى عنه، فإن ضمان الاستقرار على المدى الطويل يتطلب الانتقال من مرحلة وضع المعايير إلى مرحلة بناء آليات فعالة للمساءلة والثقة تجعل من انتهاك هذه المعايير عملاً مكلفاً سياسياً واقتصادياً.

المطلب الثاني: مناقشة الحاجة إلى معاهدة دولية لتنظيم السلوك في الفضاء السيبراني

شهد العقدان الأخيران تصاعدًا في الهجمات السيبرانية متعددة الأهداف مثل تعطيل الخدمات العامة، استهداف بنيات تحتية حيوية، وهجمات على الاقتصاد الوطني. في الوقت نفسه، ظهرت مبادرات دولية ولا سيما داخل إطار الأمم المتحدة (مثل مجموعات الخبراء GGE ومجموعة العمل الفتوحة العضوية . OEWG لبلورة معايير سلوك مسؤول للدول في الفضاء السيبراني، لذا يتكرر السؤال حول: كفاية المعايير الغير ملزمة للتحول إلى معاهدة دولية ملزمة وظهرت مع هذا السؤال الاشكالية الجدلية حول ما إذا كانت هناك حاجة إلى معاهدة دولية ملزمة لتنظيم سلوك الدول والجهات الفاعلة في الفضاء السيبراني أم تبقى المعايير غير الملزمة هي الاطار المعياري المناسب الذي يحكم بهذا الفضاء.

الفرع الأول: الحجج المؤيدة والمعارضة لوضع معاهدة دولية

نظراً للطبيعة الخاصة للفضاء الإلكتروني، نشأت مسألة الحاجة الملحة إلى وضع قواعد ملزمة قانونا تنظم الفضاء السيبراني. ففي وقت مبكر يعود إلى عام 2000، دافعت روسيا عن ضرورة وضع معاهدة جديدة تتناول على وجه التحديد تكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي، موضحة أن القانون الدولي الوضعي لا يمكنه أن يواجه التحديات المتسارعة والمتطورة للفضاء السيبراني ويوفر إطاراً لسلوك الدول[40]

وعلى العكس من ذلك، رأت العديد من الدول الغربية أنه ليس من الضروري وضع قواعد جديدة (الولايات المتحدة، المملكة المتحدة)[41]. وكان من الممكن أن ينهي الإقرار بانطباق القانون الدولي هذا الجدل. وبما أن القانون الدولي ينطبق على سلوك الدول في الفضاء السيبراني، فلا يوجد فراغ قانوني واضح، فسلوك الدول يخضع للقانون الدولي القائم، وبالتالي لا حاجة لاعتماد قواعد جديدة. ويمكن لمعايير سلوك المسئول للدول أن تكمل الالتزامات الدولية وتوضحها (دون معالجة المسائل العملية المتعلقة بالمحتوى المحتمل للقواعد الدقيقة) على أن تأخذ في الاعتبار خصائص الفضاء الإلكتروني[42].

وعلى الرغم من التوافق الظاهر حول تطبيق القانون الدولي، عادت مسألة طرح معاهدة للظهور في عام 2019، مدعومة بالتمييز بين المعايير والقانون الدولي. وهي توضح اختلاف في وجهات النظر حول سبل ضمان أمن الفضاء السيبراني.

من جهة، ترغب بعض الدول مثل: روسيا في وضع التزامات دولية جديدة يؤدي انتهاكها إلى تحميل الدولة المسؤولية الدولية للدولة، دون الطعن في تطبيق القانون الدولي الذي أصبحت قواعده لا تستوعب جميع خصوصيات الفضاء الإلكتروني، وبالتالي فمن الضروري وضع قواعد جديدة. ومن جهة أخرى، تفضل بعض الدول مثل الولايات المتحدة استخدام قواعد القانون غير الملزمة، وهي قواعد طوعية ولا يمكن أن تؤدي مخالفتها إلى تحميل الدولة المسؤولية، وبالنسبة لأصحاب هذا الاتجاه، يتسم القانون الدولي الوضعي بالمرونة الكافية لتوفير إطار لسلوك الدول. ومع ذلك، ونظراً للطبيعة الخاصة للفضاء الإلكتروني، هناك حاجة إلى معايير سلوك تكميلية من أجل توضيح توقعات المجتمع الدولي.

الجدولين التاليين يوضحان بالحجج الآراء المؤيدة والآراء المعارضة لوضع معاهدة دولية لتنظيم الفضاء السيبراني:

1/ الدول المؤيدة لوضع معاهدة ملزمة تنظم السلوك في الفضاء السيبراني: يوضح هذا الجدول جملة من الآراء المؤيدة بالحجج للدول التي تبنت موقف ضرورة وضع معاهدة دولية لتنظيم السلوك في الفضاء السيبراني والتي تعترف بالسيادة السيبرانية للدولة

الرأي (التفصيل)	الحجة
لا توجد معاهدة تحظر استخدام الأسلحة السيبرانية كما في الأسلحة النووية أو الكيميائية، صعوبة تحديد مصدر الهجمات السيبرانية مما يشجع على الإفلات من العقاب.	غياب آليات الردع القانوني
تقرير مايكروسوفت للدفاع الرقمي2023: أكثر من 120 دولة طورت قدرات هجومية سيبرانية، تقرير فريق الخبراء الحكوميين التابع للأمم المتحدة لسنة 2021: يحذر من "سباق تسلح سيبراني."	تصعيد التهديدات الاستراتيجية
حدوث أخطر هجمات سيبرانية في التاريخ مثل هجمات 2017 "Notpetya " (برمجية خبيثة تدميرية تهدف الى تعطيل الأنظمة بشكل دائم) تسببت بخسائر 10 مليارات دولار، الحاجة الى معاهدة يمكن أن تحظر استهداف المستشفيات، الشبكات الكهربائية، وأنظمة التحكم الصناعي.	حماية البنية التحتية الحرجة
وجود قواعد مثل "قواعد تالين" 2017 (وهي وثيقة غير ملزمة) توضح تطبيق القانون الدولي، لكنها غير كافية، الحاجة معاهدة تحول هذه القواعد إلى التزامات قانونية.	توحيد القواعد القانونية
معاهدة عدم انتشار الأسلحة النووية (NPT)، ومعادة حظر الأسلحة الكيميائية نجحتا في الحد من التسلح. إقتراح نموذج مشابه للأسلحة السيبرانية.	نماذج سابقة ناجحة

2/ **الدول المعارضة لوضع معاهدة ملزمة تنظم السلوك في الفضاء السيبراني:** ويوضح الجدول التالي حجج الدول المعارضة لوضع معاهدة ملزمة (الو م أ وبعض الدول الاوروبية) بصفة رسمية في الأمم المتحدة اثناء المناقشات الدائرة حول الأمن السيبراني

الأسلحة السيبرانية برمجية، سهلة الإخفاء والنسخ، لا توجد "مفتشون دوليون" يمكنهم فحص الشيفرات البرمجية.	صعوبة التحقق والمراقبة
التقنيات تتطور يوميًا، معاهدة قد تصبح قديمة خلال 5 سنوات فقط	الطبيعة المتغيرة للفضاء السيبراني
–الولايات المتحدة وأوروبا :تفضل المعايير الطوعية (مثل إطار باريس	الانقسامات الجيوسياسية

للسلوك المسؤول 2018 – (روسيا والصين تدعمان معاهدة، لكن مع رقابة على المحتوى، مكافحة "التطرف)، مما يثير مخاوف من قمع الحريات.	
الفريق الحكومي للخبراء(GGE) وفريق العمل المفتوح العضوية (OEWG) التابعين للأمم المتحدة حققا إجماعًا على 11 معيارًا طوعيًا. أكثر من 50 دولة أنشأت نقاط اتصال وطنية	النجاح النسبي للمعايير الطوعية
شركات مثل:Google Microsoft، CrowdStrike تلعب دورًا أكبر من الدول في كشف الهجمات (مثل كشف شركة "SolarWinds " وهي شركة أمريكية متخصصة في تطوير البرمجيات إدارة تكنولوجيا المعلومات، عن هجوم الكتروني كبير استهدف برمجية "orion" التابعة للشركة، المعاهدة قد تُقيد هذا التعاون.	دور وفعالية القطاع الخاص

المصدر: من إعداد الباحث بناءا على المراجع المتوفرة.

و يتضح من خلال هذين الجدولين يمكن تفسير هذا التعارض بعدة أسباب: أولها، يعود هذا التعارض إلى أصول مناقشات الأمم المتحدة حول الأمن السيبراني، حيث كانت هذه المناقشات تُوضح استخدام القانون الدولي في محاولة للحد من قدرات الدول الأكثر تقدماً، وفي هذه الحالة الولايات المتحدة. وثانيا، تعبر هذه المعارضة عن رؤى مختلفة للشرعية الدولية[43] فمن وجهة نظر العقيدة الروسية، فإن هذه المعايير تهدف إلى أن تصبح التزامات دولية، وفقًا لرؤية قانونية قائمة على تطوير واحترام الالتزامات بموجب القانون الدولي.

ودون التشكيك في أحكام القانون الدولي، فان الدول الغربية، ورغم وجود اختلافات جوهرية بينها، فان لديها رؤية سياسية أكثر تكاملًا بين الالتزامات السياسية والالتزامات القانونية، ويمكن تفسير هذا التفضيل أيضًا بحقيقة أن هذه الدول لا ترغب في إلزام نفسها قانونيًا في سياق لا يكون فيه ميزان القوى أثناء التفاوض على معاهدة ما في صالحها، وحيث توجد معارضة قوية بشأن جوهر القضايا، لذلك ركزت المعارضة هنا على مسألة الحاجة إلى المعاهدة وقيمة أحكامها، دون أي مناقشة لمضمونها المحتمل.

الفرع الثاني: التحديات الرئيسية أمام التوصل إلى معاهدة دولية تنظم السلوك في الفضاء السيبراني

مناقشة مضمون معاهدة مستقبلية للأمن السيبراني تتطلب التركيز على نقاط التوافق التي يمكن أن تشكل أساسها، وتحليل التحديات الجوهرية التي تعيق تحقيقها، واستشراف المسارات الممكنة للتقدم. أما فيما يتعلق بالمضمون، فالسؤال المطروح هو:

– ما إذا كان ينبغي لمعاهدة مستقبلية أن تنشئ التزامات دولية جديدة– على سبيل المثال، عن طريق تحويل الممارسات الجيدة المنصوص عليها كمعايير للسلوك المسؤول إلى التزامات دولية؟؛

– أو ما إذا كان ينبغي أن تحدد الطريقة التي ستنفذ بها الالتزامات المنصوص عليها في المعاهدة كمعايير للسلوك المسؤول إلى التزامات دولية ؟؛

– أو ما إذا كان ينبغي أن توضح كيفية تفسير الالتزامات الدولية القائمة، من أجل تحديد حقوق والتزامات الدول في الفضاء السيبراني بشكل أفضل؟.

أولاً، ليس من الضروري أن تحل مسألة تفسير القانون الدولي في السياق المحدد الذي نتناوله باعتماد معاهدة. فلكل دولة الحرية– في حدود ما يسمح به القانون الدولي– في تبني تفسيراتها الخاصة، ومع ذلك فإن إبلاغ الدول عن نهجها في تطبيق معايير القانون الدولي يمكن أن يلعب دوراً هاماً في تحديد الممارسات المتبعة للدول [44].

في هذا الصدد، فإن الطلب الموجه إلى الدول الأطراف في الدورة السادسة للفريق الحكومي الدولي للخبراء (GGE) بشأن مسألة" كيفية تطبيق القانون الدولي على استخدام تكنولوجيات المعلومات والاتصالات"[45] يمكن يوفر عناصر الإجابة ذات صلة للاستجابة. في الوقت الحالي، لم تقم سوى أقل من عشرة دول في العالم بالإبلاغ بشكل جوهري عن نهجها.

ثانياً، لا يمكن تحديد الالتزامات الدولية الجديدة إلا من خلال عمل تفسيري معمّق، وممارسة الدول لتطبيق القانون الدولي في الفضاء السيبراني. إذ كيف يمكن تحديد القواعد الجديدة اللازمة إذا لم يتم تحديد السلوكيات التي يغطيها القانون الوضعي مسبقاً؟ من ناحية أخرى، فإن وضع قواعد دقيقة للغاية وتقييد المجال المادي للقواعد العرفية للقانون الدولي قد يوفر الوضوح على المدى القصير، ولكنه ينطوي أيضًا على خطر تقادم أو إضعاف هذه القواعد العرفية التي يُعتزم تطبيقها في السياق الرقمي[46].كما لا ينبغي نتجاهل المرونة والقدرة على التكيف التي توفرها المبادئ العامة لمجرد ظهور تطورات تكنولوجية جديدة.

أخيرًا، التمييز بين معايير السلوك والقانون الدولي يقدم حجة لصالح وضع التزامات دولية جديدة. وفي هذه المرحلة تحديداً يمكن رصد تناقض في حجج الدول التي ترفض أي نقاش حول وضع معاهدة، ولكنها تدافع عن معايير السلوك بل وتؤيد اعتماد معايير جديدة، ويمكن أن يُنظر إلى اعتماد هذه المعايير على أنه مؤشر على وجود فراغ قانوني ينبغي ملؤه، ومن ثم استخدامه لتبرير فتح مناقشات حول معاهدة دولية، وفي هذا الصدد فإن الاقتراح الروسي بإحالة موضوع معايير السلوك إلى مجموعة العمل المفتوحة العضوية المعنية بالقواعد الدولية للسلوك يشير إلى تجدد اهتمام روسيا باعتماد معاهدة دولية في هذا المجال.

وفي الواقع، قد توفر صيغة "مجموعة العمل المفتوحة العضوية" إطارًا مثاليًا للمضي قدمًا نحو صياغة معاهدة بما أنها مفتوحة لجميع الدول لتقديم اقتراحاتها، لكن لا يمكن إغفال أن الرغبة في إبرام معاهدة لا تحظى بإجماع الدول، ويمكن أن يتم رفضها صراحة حتى من قبل بعض الدول التي ترتبط عادة بروسيا (باعتبارها صاحبة الموقف بتبني معاهدة)[47]، كما

جرى ذلك خلال جلسات مجموعة العمل المفتوحة العضوية، لذلك فإن الموقف الصيني يعتبر الأكثر حذرًا ويكشف عن الرغبة في مواصلة دراسة تفسير القانون الدولي والنتائج المترتبة عند تطبيقه على سلوك الدول في الفضاء السيبراني.

وبتمييزها بين معايير السلوك والقانون الدولي، لم تقم الدول الأعضاء في مجموعة الخبراء الحكوميين فقط بإدخال تمييز مصطنع إلى حد كبير يتنافى جزئياً محتوى المعايير نفسها، بل أعادت أيضاً إحياء التوترات حول مسألة المعاهدة التي تفاقمت بسبب السياق الجيوسياسي.

وتشكل قضية المعاهدة الآن نقطة خلاف أساسية، مما يعرقل أي تقدم جوهري بشأن مضمون حقوق الدول والتزاماتها في الفضاء الإلكتروني. ويتفاقم هذا الوضع بسبب وجهات النظر المتعارضة حول مضمون قواعد القانون الدولي التي ستتم مناقشتها، وتبقى الحاجة إلى معاهدة رغبة طويلة الأمد في ظل الظروف الحالية، والحل الأمثل الآن هو تعزيز المعايير الطوعية وبناء الثقة، دون إغفال تعاون القطاع الخاص في مجال الأمن السيبراني مع إبقاء الباب مفتوحًا لمعاهدة مستقبلية.

وعلى الرغم من عدم وجود "معاهدة" شاملة الآن، إلا أن جهود المجتمع الدولي ترسم معالم الطريق نحوها، ويتمحور الحوار الدولي الحالي حول مجموعة من المبادئ والإجراءات التي يحتمل أن تشكل جوهر أي اتفاقية مستقبلية تتمثل في العناصر التالية:

1/حظر استهداف البنية التحتية الحيوية، وهي مبدأ أساسي لحماية المجتمع. يتفق المجتمع الدولي على أن المستشفيات وشبكات الطاقة والمياه والأنظمة المالية يجب أن تكون محمية.

2/ منع الأنشطة الضارة من الأراضي الوطنية، حيث تلتزم الدول بمنع جهات خبيثة من استخدام أراضيها قاعدة لهجمات سيبرانية.

3/ تعزيز التعاون والمساعدة، خاصة في بناء قدرات الدول النامية. هذه ضرورة لمواجهة التهديدات العابرة للحدود احترام حقوق الإنسان والقانون الدولي، كالالتزام بتطبيق أي تدابير أمنية مع الحفاظ على الخصوصية وحرية التعبير.

تعزيز الشفافية والثقة، التي يمكن أن تتضمن إجراءات مثل الإبلاغ عن الثغرات الأمنية الكبرى أو التباحث حول الحوادث.

رغم التحديات، تتجه الجهود الدولية نحو آليات متعددة قد تؤدي إلى أطر تنظيمية أكثر قوة تطوير المعايير والثقة (نهج تدريجي): بدلاً من انتظار معاهدة شاملة، يتركز العمل على تعزيز القواعد الطوعية المتفق عليها دولياً، مثل معايير الأمم المتحدة لعامي 2015 و2021. وقد تكون "معاهدة الجرائم السيبرانية" التي دعا إليها الأمين العام للأمم المتحدة خطوة عملية أولى.

الخـاتمة

أصبح القانون الدولي، باعتباره أداة للسياسة الخارجية للدول، عقدة غوردية (عقبة مستعصية) في المفاوضات الدولية حول أمن واستقرار الفضاء الإلكتروني، ويوضح هذا المقال مكانته المركزية في أعمال العمليتين الجاريتين في إطار الأمم المتحدة وهما: فريق الخبراء الحكوميين، وفريق العمل المفتوح العضوية المعنيين بالقانون الدولي والأمن والاستقرار في الفضاء الإلكتروني.

على الصعيد السياسي، لا شك أن لمعايير السلوك المسئول تلعب دورا هاماً. فهي ترشد الدول في تحديد ما يشكل سلوكاً مسئولا، وترسي أسس قانون دولي مستقبلي للفضاء الإلكتروني. ومع ذلك، لا بد من التأكيد على الطابع المصطنع نسبياً للتمييز بين المعايير غير الملزمة قانوناً والقانون الدولي، ومن خلال تحليل عميق للتمييز الذي تم إجراؤه في هذه الأعمال، سلط مقالنا الضوء على الصلة الوثيقة بين بعض المعايير والالتزامات بموجب القانون الدولي، فبعض المعايير تنبع مباشرة من الالتزامات بموجب القانون الدولي مثل الالتزام "بواجب العناية" حيث أن بعض المعايير تستخدم في المقام الأول لتفسير هذه الالتزامات، وفي ظل هذه الظروف، يبدو من الصعب إجراء تمييز صارم بينهما، بل من الناحية القانونية سيكون بالخطورة أن يتطور معيار قائم على التزام بموجب القانون الدولي والمعيار المذكور بشكل منفصل في اتجاهين متعارضين.

وفي السياق الدولي الراهن، تبدو المعايير غير الملزمة (المعايير الطوعية) بمثابة حل مؤقت للقانون الدولي لسببين رئيسيين: أولهما؛ لأنها تتيح للدول إمكانية الاتفاق على تفسير بعض الالتزامات بموجب القانون الدولي، والاتفاق على عناصر أخرى تشكل سلوكاً فاضلاً في الفضاء الإلكتروني، دون أن تكون هذه الالتزامات والسلوكيات مكتوبة على حجر وبالتالي، تحدد هذه المعايير السلوك الذي ينبغي أن تتبناه الدول في الفضاء الإلكتروني، سواء من منظور القانون الدولي القائم أو من منظور الإجماع السياسي الذي توصلت إليه الدول، دون أن تفرض قيوداً جديدة. وثانيهما؛ يمكن أن تشكل هذه المعايير في نهاية المطاف أساساً لتطوير قواعد ومبادئ القانون الدولي القائمة، أو حتى لصياغة قواعد جديدة اتفاقية أو عرفية، وهذه عملية طويلة وغير مؤكدة، ولكن لا ينبغي إغفالها لأنها مصدر العديد من الالتزامات القائمة بموجب القانون الدولي.

تبرز هاتان الملاحظتان بشكل أوضح التمييز المصطنع في الكثير من الأحيان بين معايير السلوك المسئول والقانون الدولي، وتنبع من هذه الملاحظات ضرورة مراعاة الصلة بين المعايير المعتمدة على أساس توافق سياسي والقانون الدولي، وكذلك آثارها المحتملة على تطور هذا القانون.

في النهاية، يبدو أن التمييز بين المعايير غير الملزمة والقانون الدولي هو في المقام الأول نتيجة لعلاقات القوة بين الدول التي شاركت في الجولات السابقة من مفاوضات في المجموعات الحكومية للخبراء، أو نتيجة لاستقطاب نسبي حول مواقف الولايات المتحدة والدول الغربية من جهة، ومواقف روسيا والصين من جهة أخرى.

لقد أظهر بحثنا، أن هذا الاستقطاب النسبي هو في الواقع خيال، وأن هناك فسيفساء من المناهج المختلفة التي تشترك في العديد من الأوجه التشابه تتجاوز "الكتلتين" الموصوفتين ، وتبرز في الواقع تنوع المناهج المتبعة لتطبيق القانون

الدولي بشكل عام، ولاسيما عندما يتعلق الأمر بالقانون الدولي المطبق على العمليات السيبرانية، ويؤكد هذا الوضع الحاجة إلى أن تقوم الدول بالتواصل بشكل جوهري بشأن نهجها وتفسيرها لقواعد ومبادئ القانون الدولي، وهو ما لم تقم به سوى حفنة من الدول حتى الآن.

الهوامش:

(1) اختصار "OEWG " باللغة الانجليزية يعني: (Open- Ended Working Group) ويُترجم إلى العربية بـ "مجموعة عمل مفتوحة العضوية " أو"مجموعة عمل ذات تركيبة غير محدودة" وستخدم هذا الاختصار بشكل شائع في سياقات الأمم المتحدة والاتفاقيات الدولي في مجال الأمن السيبراني حيث يشير إلى "مجموعة العمل المفتوحة العضوية" حول التطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي .

(2) اختصار" GGE" يعني باللغة الإنجليزية: (Group of Governmental Experts) ويُترجم إلى العربية بـ "فريق الخبراء الحكوميين "أو " مجموعة الخبراء الحكوميين" ويُستخدم هذا الاختصار في سياقات متعددة داخل الأمم المتحدة، لكن الأكثر شيوعاً في السنوات الأخيرة (خاصة في مجال الأمن الدولي) هو: في مجال الأمن السيبراني والتكنولوجيا :يشير إلى Responsible State Behaviour in Cyberspace in the Context of International Security" " أي فريق الخبراء الحكوميين المعني بتعزيز السلوك المسؤول للدول في الفضاء السيبراني في سياق الأمن الدولي، حيث كانت هناك ست مجموعات GGE رئيسية منذ 2004 حتى 2021، ساهمت في تطوير إطار للسلوك المسؤول للدول في الفضاء السيبراني، بما في ذلك تأكيد تطبيق القانون الدولي (مثل ميثاق الأمم المتحدة) على الأنشطة السيبرانية، واقتراح قواعد طوعية غير ملزمة لتجنب التصعيد.

(3) خورخي فلوريس كاييخاس، عائشة عفيفي، تقرير وحدة التفتيش المشتركة " الأمن السيبراني في مؤسسات منظومة الأمم المتحدة" وثائق الأمم المتحدة jiu/rep/2021/3 الأمم المتحدة ، جنيف 2021 .
.https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_arabic.pdf

(4) يمكن الاطلاع على نص الوثيقة كاملا عبر مكتبة الأمم المتحدة من خلال الموقع : digilibrary.un.org

(5) القرار رقم A/RES /53/70 المعتمد من طرف اللجنة الأولى التابعة للجمعية العامة للأمم المتحدة بناءا على التقرير الصادر عن مكتب الأمم المتحدة انزع السلاح https://disarmament.unoda.org.

(6) أنظر تقرير وحدة التفتيش المشتركة لعام 2021 حول الأمن السيبراني في مؤسسات منظومة الأمم المتحدة

(7) وهو فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات و الاتصالات السلكية و اللاسكلية في سياق الامن الدولي المعروف اختصاراً بـ: (GEG) أنشأ عملاً بالفقرة 4 من قرار الجمعية العامة 24/66، بقرار رقم :(A / RES / 58/32) سنة 2004 وذلك لدراسة التهديدات السيبرانية وتطوير معايير السلوك المسئول في الفضاء الالكتروني، وتضم من 20 إلى 25 دولة.

(8) كانت العقبات الرئيسية في عدم اعتماد أي تقرير نهائي تتمثل في عدم وجود وكفاية قواعد القانون الدولي والقانون الدولي الإنساني تطبق في حالة الاستخدام العدائي لتكنولوجيا المعلومات والاتصالات لأغراض سياسية وعسكرية.

(9) الفقرة 19 من التقرير :(2013) A/68/98).

(10)
United nations General Assembly report of the group of Governemental experts on Advancing Responsible State Behaviour incyberspace in the contextof international Security « A/76/174(2015) https:// undocs.org/A/76/135 .

(11) أطلقت بقرار الجمعية العامةA/RES/73/27 في سنة 2018 كمنصة مفتوحة لجميع الدول لمناقشة الأمن السيبراني.

(12) مشروع القرار رقم:A/C.1/C.1/L.27/Rev.1

(13) مشروع القرار رقم :A/C.1/73/L.37.

(14) جاء في الرد الإيراني ما نصه" إن أولئك الذين يسعون إلى فرض تفوقهم يريدون بطبيعة الحال الحفاظ على الوضع الراهن ويرفضون وضع قواعد دولية من شأنها أن تحد من قدرتهم على التصرف في الفضاء الإلكتروني."من المرجح أن إيران تشير هنا – من بين أمور أخرى إلى" Stuxnet" وهو اسم فيروس

حاسوبي يُفترض أن الولايات المتحدة وإسرائيل طورتاه في عام 2010 لاستهداف محطات "ناتنز" النووية الإيرانية بهدف تخريب البرنامج النووي الإيراني(/DSI/3613AG).

(15)

Grigsby Alex, « The un Doubles Its Workload on Cyber Norms, And Not Everyone is Pleased , Councilof Foreign Relations, blogue, 15 novembre. Consulté sur Internet (https://www.cfr.org/blog/united-nations-doubles-itsworkload-cyber-norms-and-not-le 03 septembre 2024

(16)

Broeders Dennis, Liisi Adamson et RogierCreemers, A Coalition of the Unwilling ?Chinese and Russian Perspectives on Cyberspace, Leyde, The Hague Program, LeidenAsia Center et Université de Leyde. Consulté sur Internet (https://scholarlypublications.universiteitleiden.nl/access/item%3A2967052/ view) le novembre 2024.

(17) القرار رقم: A/RES/73/27) الصادر عن الجمعية العامة للأمم المتحدة تم تبنيه بأغلبية 119 صوتًا مقابل 46 صوتًا، مع امتناع 14 دولة عن التصويت.

(18) وهو القرار الصادر عن الجمعية العامة للأمم المتحدة رقم A/RES/73/266)تم تبنيه بأغلبية 138 صوتًا مقابل 12 صوتًا، مع امتناع 16 دولة عن التصويت.

(19)

De Tomas ColatinSamuele, 2019, «A Surprising Turn of Events : un Creates Two Working Groups on Cyberspace », ccdcoe. Consultésur Internet (https:// ccdcoe.org/incyder-articles/a-surprising-turn-of-events-un-creates-twoworking-groups-on-cyberspace/) le 25 mars2025 .

(20) نداء باريس من أجل الثقة والأمن في الفضاء الإلكتروني في 12 تشرين الثاني/نوفمبر 2017. يمثّل نداء باريس أوسع مبادرة متعددة الأطراف في مجال أمن الفضاء الإلكتروني، فهي تحظى بدعم أكثر من 1200 جهة داعمة من جميع قارات العالم تنبثق من القطاعَين العام والخاص ومن المجتمع المدني، وتضمّ المبادرة من بين مجمل الجهات الداعمة 80 دولة وأكثر من 700 منشأة وجمعية مهنية وأكثر من 390 منظمة من المجتمع المدني، فضلًا عن مجموعة من السلطات العامة والسلطات المحلية. وتلتزم الجهات الداعمة بالعمل يدًا واحدةً من أجل تنفيذ مبادئ نداء باريس واتّباع سلوك مسؤول في مجال الفضاء الإلكترونيhttps: Pariscall.international/fr . 2018

(21)

PawlakPatryk, «Rebooting the eu’s Cyber Diplomacy», eu Cyber Direct Ideas in Focus. Consulté sur Internet (https://eucyberdirect.eu/content_research/ rebooting-the-eus-cyberdiplomacy/) le 14 avril 2025.

(22)

Delerue François, Joanna Kulesza et PatrykPawlak, 2019, « The Application of International Law in Cyberspace : Is There a European Way ? » eu Cyber Direct – Policy in Focus. Consultésur Internet (https://eucyberdirect.eu/ content_research/application-of-international-law-european-way/) le 15 avril 2025

(23) الفقرة 3 من القرار: A/RES/73/266 السالف الذكر.

(24)

Ministère des Armées (France), 2019, Le droit international appliqué aux opérations dans le cyberespace, 4 octobre. Consulté sur Internet (https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit+interna +appliqué+aux+opérations+Cyberespace.pdf) /) le 25 /09/ 2025

(25)

Royaume des Pays-Bas, 2019, 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, renduepublique le 15 octobre 2019, Annexe « International Law in Cyberspace» 27/09/2025

(26) الفقرة الخامسة من القرار :A/RES/73/27

(27) الفقرة الخامسة من القرار :A/RES/73/27.

(28) القرار 266/73 يشير فقط إلى تقريرالفريق الحكومي الدولي لعام 2015)، باعتباره القرار الذي أنشأ فريق العمل الحكومي السادس.

(29) على سبيل المثال، تم تضمين التوصية المتعلقة بمنع التقنيات والأدوات الحاسوبيةالخبيثة في فقرة عن سلامة سلسلة التوريد في تقرير مجموعة الخبراء الحكومية التابعة لمجلس الأمن لعام 2015، في حين أنها موضوع بند مستقل في القرار 27/73.

(30)

The Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland, 2019, « Statement by Amb.AndreyKrutskikh, 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 juin. Consulté sur Internet (https://rusemb.org.uk/ article/541) le 13 septembre 2025.

(31)

Adamson Liisi, 2020, « International Law and International Cyber Norms : A Continuum ? dans Dennis Broeders et Bibi van den Berg (dir.), Governing Cyberspace: Behavior, Power and Diplomacy, Lanham, Rowman& Littlefield: 19-44. 13 septembre 2025

(32) الفقرة العاشرة من القرار A./RES 70/774

(33)

Adamson Liisi, 2020 opcit, p25.

(34)

Brian J. Egan, International Law and Stability in Cyberspace, 35 Berkeley J. Int'l Law. 169 (2017). Available at: http://scholarship.law.berkeley.edu/bjil/vol35/iss1/5 p p 170,171.

(35)

Pellet Alain, 1984, «Le “bon droit” et l’ivraie – Plaidoyer pour l’ivraie (Remarques sur quelques problèmes de méthode en droit international du développement) », dans Le droit des peuples à disposer d’eux-mêmes: méthodes d’analyse du droit international. Mélanges offerts à Charles Chaumon, Paris, Pedone :p 488.

(36)

Combacau Jean et Serge Sur, 2014, Droit international public, Paris, l.g.d.j. Cour internationale de Justice, 1950, Affaire du Détroit de Corfou, arrêt, 9 avril 1950, c.i.j. Recueil 1950.

(37) الفقرتان 13 و 28 من التقرير A/70/174.

(38)

Tikk Eneken.2020 « internayional law in cyberspace : Mind the Gap » eu cyber Direct. Consulté sur internet (https://eucyberdirect.eu/content_research/international -law-in- cyberspace-mind-thegap/) le 27/09/2025.

(39) أنظر: تقرير فريق الخبراء الحكوميين التابع للأمم المتحدة بشأن الأمن السيبراني (الوثيقة الرسمية A/76/135)

(40) مشروع القرار رقم A/54/213 ص 8-10.

(41) مشروع القرار رقم A/54/213 ص 6-8.

(42) Tikk Eneken et Mika Kerttunen, 2018, Parabasis: Cyber-Diplomacy in Stalemate, Nupi Report

(43) Roberts Anthea, 2017, Is International Law International? Oxford, Oxford University Press.

(44) Delerue François, Joanna Kulesza et Patryk Pawlak, « The Application of International Law in Cyberspace : Is There a European Way ? » eu Cyber Direct – Policy in Focus. Consulté sur Internet 2019(https://eucyberdirect.eu/content_research/application-of-international-law-european-way/) le 14er septembre 2025

(45) قرار الجمعية العامة للأمم المتحدة A/RES/73/266 هو قرار يتعلق بإنشاء فريق خبراء حكوميين (GGE) بهدف الارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدول، تمت الموافقة على هذا القرار في عام 2019 ويدعو إلى مواصلة عمل فريق الخبراء الحكوميين في الفترة 2019-2021 بالتعاون مع فريق العمل مفتوح العضوية.

(46) Grange Maryline et Anne-Thida Norodom, « Propos Introductifs », dans Maryline Grange et Anne-Thida Norodom (dir.), Cyberattaques et droit international. Problèmes choisis, Paris 2019, Pedone : 11-20.

(47) للاطلاع على مواقف الدول بشأن هذا الموضوع، انظر المساهمات المقدمة من الدول في إطار الفريق العامل المعني بالقانون العام لنزع السلاح (الأمم المتحدة، مكتب شؤون نزع السلاح، بدون تاريخ) https://disarmament.unoda.org/ar.