AALCO/59/HONG KONG/2021/SD/S17

للاستخدام الرسمي فقط

المنظمة الاستشارية القانونية الآسيوية – الإفريقية

القانون الدولي في الفضاء السيبراني

الأمانة العامة لمنظمة آلكو
29- سي، ريزال مارغ،
ديبلوماتيك انكليف، تشاناكيابوري،
نيودلهي - 110021
(الهند)

القانون الدولي في الفضاء السيبراني

المحتويات

أولاً. مقدمة

أ. خلفية

1. تم تقديم موضوع "القانون الدولي في الفضاء السيبراني" كبند من بنود جدول الأعمال التي ستتم مناقشتها في الدورة السنوية الثالثة والخمسين لآلكو التي عقدت في طهران إيران في 2014 بناءً على توصية من جمهورية الصين الشعبية. تمت مناقشة جدول الأعمال لاحقاً كموضوع ثابت مرة أخرى في العام التالي في عام 2015 في الدورة السنوية الرابعة والخمسين التي عُقدت في بكين في الصين. وجّه القرار بشأن بند جدول الأعمال المعتمد في تلك الجلسة الأمانة إلى "دراسة هذا الموضوع بناءً على المداولات والتقدم المحرز في إطار الأمم المتحدة والمنتديات الأخرى مع إيلاء اهتمام خاص للقانون الدولي المتعلق بسيادة الدول والاستخدام السلمي في الفضاء السيبراني وقواعد التعاون الدولي في مكافحة الجرائم الإلكترونية وتحديد الأحكام ذات الصلة من ميثاق الأمم المتحدة والصكوك الدولية الأخرى المتعلقة بالفضاء السيبرانية".[1] كما تقرر بموجب القرار المذكور إنشاء "مجموعة العمل المفتوحة العضوية (OEWG) المعنية بالقانون الدولي في الفضاء السيبراني لمواصلة مناقشة القضايا المحددة أعلاه من خلال الاجتماعات أو ورش العمل التي تشارك في رعايتها مع حكومات الدول الأعضاء أو المنظمات الدولية ذات الصلة."[2]

2. اجتمعت بناءً على ذلك مجموعة العمل المفتوحة العضوية الأولى المعنية بالقانون الدولي في الفضاء السيبراني خلال الدورة السنوية الخامسة والخمسين في نيودلهي الهند في عام 2016. تم انتخاب البروفيسور هوانغ تشي تشونغ كمقرر والسيد حسين بناهي عازار رئيساً لمجموعة العمل المفتوحة العضوية. وجه القرار الذي تم تبنيه بشأن بند جدول الأعمال في الدورة السنوية الخامسة والخمسين الأمانة إلى "... متابعة التطورات في المنتديات الدولية عن كثب المتعلقة بحوكمة الفضاء والأمن الالكتروني ومواصلة دراستها حول القانون الدولي في الفضاء السيبراني وفقاً للقرار ذي الصلة المعتمد في الدورة السنوية الرابعة والخمسون..."، ومجموعة العمل المفتوحة العضوية"... لعقد اجتماعات بين الدورات... مع الأخذ في الاعتبار حاجة الدول الأعضاء في آلكو في مكافحة جرائم الإنترنت. "[3] انعقد الاجتماع الثاني لمجموعة العمل المفتوحة العضوية المعنية بالقانون الدولي في الفضاء السيبراني في الفترة من 9 إلى 10 شباط/ فبراير 2017 في مقر منظمة آلكو في نيودلهي. تمت مناقشة الموضوعات التالية التي حددتها الدول الأعضاء بالفعل منذ البداية باعتبارها ذات أهمية قصوى في الاجتماع الثاني لمجموعة العمل المفتوح العضوية وهي: أ) السيادة في الفضاء السيبراني: موازنة الحقوق والالتزامات ب) القانون وحوكمة الفضاء السيبراني ج) الحرب الالكترونية: الآثار القانونية د) الجرائم الإلكترونية والقانون الدولي. كما نوقش

[1] AALCO/RES/54/SP2، بكين، 17 نيسان/ أبريل لعام 2015.
[2] AALCO/RES/54/SP2، بكين، 17 نيسان / أبريل لعام 2015.
[3] AALCO/RES/55/S17، نيودلهي، 20 أيار/ مايو لعام 2016.

مشروع الدراسة الخاصة الذي أعدته الأمانة والذي يحتوي بشكل عام على نفس الموضوعات المذكورة أعلاه خلال الاجتماع الثاني لمجموعة العمل المفتوحة العضوية.

3. تم تناول موضوع القانون الدولي في الفضاء السيبراني مرة أخرى كبند موضوعي في جدول الأعمال في الدورة السنوية السادسة والخمسين في نيروبي، كينيا في عام 2017. وصدرت فيه الدراسة الخاصة التي أعدتها الأمانة بشأن القانون الدولي في الفضاء السيبراني. وجه القرار الذي تم اعتماده خلال الدورة الأمانة إلى "...متابعة التطورات في المنتديات الدولية عن كثب المتعلقة بحوكمة الفضاء والأمن الالكتروني وتنظيم اجتماعات مجموعة العمل المفتوحة العضوية، عند الضرورة" والمقرر لإعداد "...تقرير على أساس المناقشات التي جرت حتى الآن بين الدول الأعضاء والدراسة الخاصة التي أعدتها الأمانة والتي تضع خطة عمل مستقبلية لمجموعة العمل المفتوحة العضوية ".[4]

4. تم إرسال التقرير الذي أعده مقرر مجموعة العمل المفتوحة العضوية المعنية بالقانون الدولي في الفضاء السيبراني بشأن خطة العمل المستقبلية لمجوعة العمل المفتوحة العضوية بشكل أولي إلى جميع الدول الأعضاء من خلال أمانة آلكو لإبداء تعليقاتهم وملاحظاتهم. تلقت الأمانة تعليقات من عدد من الدول الأعضاء وبناءً على ذلك أعد المقرر تقريراً منقحاً تم توزيعه على جميع الدول الأعضاء. تمت مناقشة التقرير المنقح بعد ذلك في الاجتماع الثالث لمجموعة العمل المفتوحة العضوية المعنية بالقانون الدولي في الفضاء السيبراني الذي انعقد على هامش الدورة السنوية السابعة والخمسين في طوكيو اليابان في عام 2018.

5. كان الإجماع الواسع في الدورة السنوية السابعة والخمسين الذي تم التوصل إليه بشأن خطة العمل المستقبلية لمجموعة العمل المفتوحة العضوية على النحو التالي: أ) تواصل مجموعة العمل المفتوحة العضوية مناقشة مسألة القانون الدولي في الفضاء السيبراني بهدف: من بين أمور أخرى تعزيز التعاون في مكافحة الجريمة الالكترونية والبحث في بعض القضايا الرئيسية للقانون الدولي في الفضاء السيبراني وتحديد مجالات بناء القدرات حسب الاقتضاء ب) يعد المقرر تقريراً عن آخر التطورات في القانون الدولي في الفضاء السيبراني؛ وبشأن الحاجة الخاصة للدول الأعضاء إلى التعاون الدولي ضد الجريمة الالكترونية ج) يظل بند جدول الأعمال "القانون الدولي في الفضاء السيبراني" على جدول أعمال المنظمة والدورة السنوية القادمة أيضاً، وتواصل مجموعة العمل المفتوحة العضوية عملها بشأن هذا الموضوع د) تنظر مجموعة العمل المفتوحة العضوية في عقد اجتماع واحد على الأقل قبل أو أثناء الدورة السنوية التالية لتلقي آراء الدول الأعضاء وتعزيز المزيد من المشاورات حول هذا البند، رهناً بتوافر الموارد المالية.

[4] AALCO/RES/56/S17، نيروبي، 5 أيار/ مايو لعام 2017.

6. تم توزيع استبيان أعده المقرر على الدول الأعضاء في إطار إعداد تقرير المقرر حول "الحاجة الخاصة للدول الأعضاء للتعاون الدولي ضد الجرائم الإلكترونية"، وفقًا لما نصت عليه الدورة السنوية السابعة والخمسون والذي تم تلقي ردود عليه من قبل 11 دولة عضو. يتكون الاستبيان من 38 سؤالاً ويتضمن أربعة أجزاء وهي: أ) القانون المحلي، ب) التعاون الدولي، ج) بناء القدرات والمساعدة الفنية، د) الشراكة بين القطاعين العام والخاص. عُقد الاجتماع الرابع لمجموعة العمل المفتوحة العضوية المعنية بالقانون الدولي في الفضاء السيبراني في الفترة من 2 إلى 4 أيلول/ سبتمبر 2019 في هانغتشو، جمهورية الصين الشعبية برئاسة سعادة الدكتور عباس باقربور أردكاني. قدم المقرر تقريره عن نتيجة رد الدول الأعضاء على الاستبيان. اختتم الرئيس المناقشة بإبراز أهمية وجود إطار مناسب يعالج الموضوع على وجه التحديد. إن الحاجة إلى مواجهة التحديات بشكل جماعي تظل الشغل الشاغل للدول الأعضاء في آلكو على الرغم من بعض وجهات النظر المتباينة. قالت إن الحاجة إلى إيجاد أرضية مشتركة بين الدول الأعضاء هي أهم جانب في الموضوع ويمكن أن تشكل الأساس للدورة السنوية المقبلة لآلكو. كما طلب التوجيه والمساعدة من أمانة آلكو تحت قيادة الأمين العام لاستكشاف إعداد ورقة غير رسمية و/ أو مشروع صفري تعكس المبادئ الأساسية التوافقية للقانون الدولي المطبق في الفضاء السيبراني. تمت بعد ذلك مناقشة القضايا الصعبة للقانون الدولي في الفضاء السيبراني وهي: أ) تطبيق مبدأ عدم التدخل في الفضاء السيبراني ب) سيادة البيانات وتدفقات البيانات عبر الحدود وأمن البيانات ج) تنظيم المحتوى الضار عبر الإنترنت. ناقش المشاركون أخيراً موضوع "الاستخدام السلمي للفضاء السيبراني".

7. تمت في هذا الصدد صياغة وتعميم اقتراح الأمين العام بشأن "المبادئ الأساسية التوافقية للقانون الدولي المنطبقة في الفضاء السيبراني" (كما نصت على ذلك مجموعة العمل المفتوحة العضوية) على الدول الأعضاء. وردت من خمس دول أعضاء تعليقات بشأن المشروع الأول. تمت مراجعة المبادئ بناءً على هذه التعليقات والمراجعة الداخلية لهذه المبادئ. يتألف المشروع المنقح لشهر تموز/ يوليو 2021 من مجموعة من 14 مبدأ صيغت بعناية وإسهاب ومذكرة تفسيرية لنفس المبادئ. وقد وردت تعليقات على هذا المشروع المنقح من قبل ثلاث دول أعضاء حتى الآن. سيتم تقديم المشروع المنقح والتعليقات الواردة إلى الاجتماع الخامس لمجموعة العمل المفتوحة العضوية المعنية بالقانون الدولي في الفضاء السيبراني لإجراء مزيد من المناقشات المتعمقة وإمكانية اعتماده.

8. أعربت الدول الأعضاء في الدورة السنوية الثامنة والخمسين التي انعقدت في دار السلام في جمهورية تنزانيا المتحدة في تشرين الأول / أكتوبر 2019 عن آرائها بشكل عام بشأن استخدام الفضاء السيبراني مع التركيز بشكل خاص على مواضيع مثل مبدأ عدم التدخل في الفضاء السيبراني وقضايا الخصوصية والقانون الدولي المطبق على الهجمات الإلكترونية وتنظيم المحتوى عبر الإنترنت والاتفاقية متعددة الأطراف التي قد تنظم الأنشطة داخل الفضاء السيبراني وتعزيز التعاون في مكافحة الجرائم الإلكترونية

فضلاً عن أهمية وثيقة عامة غير ملزمة بموجب آلكو توضح المبادئ الأساسية التوافقية للقانون الدولي المطبق في الفضاء السيبراني.

9. تجدر الإشارة إلى أن رد الدول الأعضاء على الاستبيان الذي قدمه المقرر عند إعداد تقريره عن "الحاجة الخاصة للدول الأعضاء للتعاون الدولي ضد الجرائم الإلكترونية"، وكذلك اقتراح الأمين العام بشأن "اقتراح المبادئ الأساسية التوافقية للقانون الدولي المطبقة في الفضاء السيبراني" والتعليقات الواردة سيتم مناقشتها في الاجتماع الخامس لمجموعة العمل المفتوحة العضوية المعنية بالقانون الدولي في الفضاء السيبراني الذي سيعقد على هامش الدورة السنوية التاسعة والخمسين وفقاً للولايات المذكورة أعلاه. ولذلك فإن هذا الملخص يقتصر في نطاقه على موضوعات مناقشة الاجتماع العام في الدورة السنوية التاسعة والخمسين.

ب. قضايا للمداولات المركزة في الدورة السنوية الحالية

1) تطبيق مبدأ عدم التدخل في الفضاء السيبراني
2) سيادة البيانات وتدفق البيانات عبر الحدود وأمن البيانات
3) تنظيم المحتوى الضار عبر الإنترنت
4) الاستخدام السلمي للفضاء السيبراني

ثانياً. مداولات الدورة السنوية الثامنة والخمسين لآلكو (دار السلام، جمهورية تنزانيا المتحدة، 21-25 تشرين الأول/ أكتوبر 2019م)

10. أدلى الأمين العام لآلكو البيان الاستهلالي حول هذا الموضوع. أوضح بإيجاز كيف تعاملت آلكو مع موضوع "القانون الدولي في الفضاء السيبراني" منذ أن تمت إضافته كبند ثابت في جدول الأعمال عام 2014. أشار كذلك إلى أن المناقشات حول القانون الدولي في الفضاء السيبراني في إطار الاجتماع العام الرابع للدورة السنوية الثامنة والخمسين كانت تجري على خلفية الاجتماع الرابع لمجموعة العمل المفتوحة العضوية المعنية بالقانون الدولي في الفضاء السيبراني الذي اختتم في هانغتشو، الصين في الفترة من 2-4 أيلول/ سبتمبر 2019. هنأ البروفيسور بعد ذلك تشي تشونغ هوانغ من كلية الحقوق بجامعة ووهان، جمهورية الصين الشعبية لعمله كمقرر لمجموعة العمل المفتوح العضوية المعنية بالقانون الدولي في الفضاء السيبراني وكذلك جمهورية الصين الشعبية وكل من الدول الأعضاء الأخرى على اهتمامها النشط بالموضوع. ودعا المقرر البروفيسور تشي تشونغ هوانغ لتقديم عرض عن عمله الجاري وكذلك البروفيسور زاكايو ن. لوكوماي لبدء ومساعدة المداولات بصفته الفردية كخبير في هذا الموضوع.

11. ذكر المتحدث الأول تشي تشونغ هوانغ مقرر مجموعة العمل المفتوحة العضوية المعنية بالقانون الدولي في الفضاء السيبراني في بادئ الأمر البروفيسور أنه قدم تقريراً عن كيفية استجابة الدول الأعضاء للاستبيان المتعلق بجرائم الإنترنت الذي أعده في الاجتماع الرابع لمجموعة العمل المفتوحة العضوية المعنية بالقانون الدولي في الفضاء السيبراني المقام في هانغتشو. وذكر أن بيانه الحالي سيكون تقريراً محدثاً. أبلغ الدول الأعضاء أن الاستبيان الذي أعده كان تعزيزاً للتفويض التي تم تلقيه في الدورة السنوية السابعة والخمسين في عام 2018 والتي كانت تهدف إلى "إعداد تقرير عن آخر التطورات في القانون الدولي في الفضاء السيبراني وحول الحاجة الخاصة إلى الدول الأعضاء من أجل التعاون الدولي ضد الجريمة الالكترونية". لخص الردود الواردة من الدول الأعضاء التي أوضحت فيها احتياجاتها الخاصة للتعاون الدولي ضد الجرائم الإلكترونية، وأشار إلى أن الردود تشير بشكل عام إلى حاجة الدول الأعضاء إلى تعزيز التعاون الدولي في مكافحة الجريمة الالكترونية وإلى تعزيز بناء القدرات والمساعدة التقنية في هذا الصدد. كما رحب بالمدخلات من الدول الأعضاء الأخرى في آلكو حتى يتمكن من استكمال تقريره عن الحاجة الخاصة للدول الأعضاء للتعاون الدولي ضد الجرائم الإلكترونية وفقاً للتفويض المذكور أعلاه.

12. تناول المتحدث التالي البروفيسور زاكايو ن. لوكوماي كبير المحاضرين والقائم بأعمال مدير كلية الحقوق في تنزانيا في عرضه بشكل موسع إمكانية تطبيق مبادئ القانون الدولي على الفضاء السيبراني أي التعاون الدول والسيادة والاختصاص وقانون الصراعات المسلحة. ذكر أن الأمر نفسه قد مكّن المجرمين أيضاً من الانخراط في مجموعة متنوعة من الأنشطة الإجرامية في الفضاء السيبراني بعد شرح الطبيعة العالمية والمجهولة للفضاء السيبراني. أضاف أن الفضاء السيبراني أصبح أيضاً مجالاً للنزاعات بين الدول حيث أصبحت الهجمات الإلكترونية عبر الإنترنت أكثر شيوعاً. أشار إلى أن هذا استلزم إنشاء نظام من القوانين واللوائح يعرف باسم قوانين الإنترنت المعمول بها بالفعل بدرجات متفاوتة في دول مختلفة. ذكر كذلك وفيما يتعلق بالجرائم الإلكترونية أنه لا يوجد اتفاق بين الدول فيما يتعلق بما يمكن أن يشكل تعريفاً مشتركاً للجريمة الإلكترونية حتى يتم حظرها. لذلك من أجل تحديد الأنشطة التي يمكن أن تشكل جرائم إلكترونية يعاقب عليها القانون بشكل عام اقترح تطبيق القانون الدولي - من خلال اعتماد صكوك قانونية دولية ملزمة - من أجل الطبيعة العالمية للإنترنت.

13. اقترح أنه يجوز للدولة ممارسة اختصاصها خارج الإقليم عملاً بالمادة 19 من العهد الدولي الخاص بالحقوق المدنية والسياسية (ICCPR) لأن الدولة لها الحق بموجب القانون الدولي في الدفاع عن نفسها ضد أي هجوم إلكتروني يهدد الأمن القومي أو النظام العام أو الحقوق والحريات القانونية للآخرين بما في ذلك حقوق الخصوصية والملكية الفكرية. اقترح كذلك فيما يتعلق بالجرائم الإلكترونية أنه نظراً لأن للجريمة طابع دولي يجب على الدولة الاحتجاج بنظرية الاختصاص القضائي العالمي التي تتطلب بعض الإجماع بين الدول. ذكر أنها قد لا تكون أداة مناسبة لحل جميع القضايا لأنها تعتمد على حسن نية البلد

الذي تسعى إلى التعاون معه فيما يتعلق باتفاقية بودابست كأداة لتكوين تعاون دولي لمكافحة جرائم الإنترنت. تفتقر الاتفاقية أيضاً إلى منح الدول الأسلحة اللازمة لمكافحة هذا النوع من الجريمة.

14. أقترح فيما يتعلق بالإرهاب الالكتروني استخدام اتفاقية روما لعام 1988 لقمع الأعمال غير المشروعة الموجهة ضد سلامة الملاحة البحرية والتي يمكن تفسيرها أيضاً على أنها تغطي الأنشطة الإلكترونية. ناقش العديد من القضايا المرتبطة بتطبيق المادتين 2(4) و51 من ميثاق الأمم المتحدة فيما يتعلق بمسألة القانون الدولي المطبق على الحرب الإلكترونية. ذكر في الختام أنه من أجل حل القضايا المتعلقة بالجرائم الإلكترونية هناك حاجة إلى صك قانوني دولي ملزم تحت رعاية الأمم المتحدة.

15. أقر **مندوب من جمهورية كينيا** أثناء تقديره الطبيعة الفريدة للفضاء السيبراني الذي يوفر فرصاً كبيرةً للمجتمع العالمي ككل بالتحديات الهائلة التي ظهرت، واعترف بالحاجة الملحة لمواجهة تلك التحديات. أعرب في هذا الصدد عن تقديره للعمل الجاري في مجموعة العمل مفتوحة العضوية التابعة لآلكو المعنية بالقانون الدولي في الفضاء السيبراني. أقر على وجه الخصوص بالمسائل القانونية الناشئة المحيطة بإساءة استخدام أجهزة الحاسوب والفضاء السيبراني بشكل عام والحاجة إلى إطار قانوني دولي بالإضافة إلى الأطر الإقليمية القائمة لتعزيز التعاون في مكافحة الجريمة الالكترونية. أوضح أيضاً بإيجاز الإطار القانوني المحلي في كينيا للتصدي لتهديد الأمن الالكتروني بموجب "قانون إساءة استخدام أجهزة الحاسوب والجرائم الإلكترونية لعام 2018 ". تحدث أيضاً عن قانون المعلومات والاتصالات الكيني لعام 2015 الذي قطع شوطاً طويلاً في تعزيز إطار التعاون متعدد الوكالات من بين الجوانب الرئيسية الأخرى التي تدعم مرونة الأمن الالكتروني الوطني. قدم في الختام تأكيدات بأن كينيا بصدد إعداد ردود مفصلة على الاستبيان الذي سيتم تقديمه إلى أمانة آلكو.

16. أشار **مندوب جمهورية تنزانيا المتحدة** أولاً إلى أن الفضاء السيبراني لا ينبغي أن يكون منطقة خارجة عن القانون، يجب أن يخضع في الواقع لمبادئ السيادة والولاية القضائية وكذلك حظر التدخل في شؤون الدول الأخرى واستخدام القوة. أوصى إضافةً لذلك فيما يتعلق بالتنظيم الدولي للفضاء السيبراني بما يلي: أ) ينبغي أن يكون هناك صك دولي ملزم قانوناً لتنظيم الفضاء السيبراني. هناك حاجة إضافةً لذلك إلى توضيح دور القانون الدولي في الفضاء السيبراني حيث بدأت بعض الدول في نشر تفسيراتها الخاصة للقانون الدولي فيما يتعلق بالفضاء السيبراني. ب) هناك حاجة لتحديد ما إذا كان القانون الحالي كافياً أو مرضياً لتوفير إرشادات وضمانات كافية للعلاقات المتبادلة بين الدول داخل الفضاء السيبراني. ج) هناك حاجة لتصنيف الهجمات الإلكترونية عبر الإنترنت التي تعتبر انتهاكات للقانون الدولي. د) يجب معالجة القوى الالكترونية الكبرى لمناقشة الخطوط الحمراء للنشاط الالكتروني الهجومي. هـ) يجب أن يكون تطبيق القانون الدولي على الفضاء السيبراني واضحاً فيما يتعلق بالتكاليف الإنسانية للهجمات الإلكترونية خاصةً عندما تستخدم بعض المنظمات الفضاء السيبراني للاتصالات والخدمات اللوجستية التي تعرضت

لهجمات إلكترونية. و) يجب أن تكون هناك استجابات متعددة الأطراف للتهديدات الناشئة القائمة في الفضاء السيبراني.

17. أعرب **مندوب جمهورية نيبال الديمقراطية الفيدرالية** أولاً عن تقديره لمجموعة العمل مفتوحة العضوية المعنية بالقانون الدولي في الفضاء السيبراني لمساهمته في تطوير القانون الدولي للفضاء السيبراني. أعرب عن أن القانون الدولي قد انتقل الآن من تطبيق القانون الدولي على الفضاء السيبراني إلى كيفية تطبيق القانون الدولي في الفضاء السيبراني، الأمر الذي يحتاج بدوره إلى إجماع دولي. صرح في هذا الصدد أن وجود وثيقة عامة غير ملزمة بموجب مقدمات آلكو توضح المبادئ الأساسية التوافقية للقانون الدولي المعمول به في الفضاء السيبراني سيكون أمراً حيوياً. أشار إلى أن حكومة نيبال أقرت مشروع قانون بشأن المعلومات والتكنولوجيا إلى مجلس النواب من أجل مواجهة تحديات الأمن الالكتروني وقضايا الفضاء السيبراني. ذكر كذلك أنه يجب وضع تدابير خاصة لمعالجة الإدماج والتعاون بين الدول الأعضاء لتعزيز التعاون في بناء القدرات ووضع معايير موحدة لمكافحة الجريمة الالكترونية نظراً لأن الأمن الالكتروني ليس مجرد صفقة محلية. حث آلكو في هذا الصدد على الشروع في تطوير قواعد مناسبة وفعالة للقانون الدولي لمكافحة الجرائم الإلكترونية ونظام دولي يساعد المجتمع الدولي في بناء آلية وطريقة قوية وتحقيق التوازن بين مجال الدولة والمجال العام في مواجهة تطوير فضاء إلكتروني آمن وشامل. أشار في الختام إلى أن نيبال تخضع لعملية تشاور مع السلطات المسؤولة للمساهمة في تقرير المقرر بشأن "الحاجة الخاصة للدول الأعضاء للتعاون الدولي ضد الجرائم الالكترونية".

18. اعترف **مندوب جمهورية الهند** أولاً بالفضاء السيبراني كمجال معقد حيث يتم باستمرار تحدي المفاهيم التقليدية للسيادة والاختصاص والخصوصية. ذكر أنه في هذا الصدد من الضروري أن تفهم الدول وتنفذ المعايير المهمة المتفق عليها بالفعل في مجموعات الخبراء الحكوميين التابعة للأمم المتحدة في مجال المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي (UNGGEs). أشار أيضاً إلى أن هناك حاجة إلى تطوير فهم أفضل لتطبيق القانون الدولي في الفضاء السيبراني. تنطبق التزامات الدول بموجب ميثاق الأمم المتحدة والقانون الدولي الآخر على سلوكها في الفضاء السيبراني.

19. ذكر أن الطابع الجديد للفضاء السيبراني وضعف البنية التحتية الإلكترونية أدى مع ذلك إلى طرح تساؤلات حول ما إذا كان القانون الدولي الحالي يمكن أن يقدم إجابات كافية على المخاوف الناشئة في الفضاء السيبراني على سبيل المثال لا يعترف العمل في تقارير مجموعة الخبراء الحكوميين التابعة للأمم المتحدة حتى الآن بوضوح أن القانون الدولي الإنساني (IHL) ينطبق على تصرفات الدولة في الفضاء السيبراني. ذكر أيضاً أنه يتعين على المجتمع الدولي الاتفاق على تعريفات مشتركة للسيادة الالكترونية والاختصاص والصراع المسلح والجريمة والردع والهجمات وما إلى ذلك. أبلغ الجلسة بأن الهند شاركت في مناقشات مجموعة الخبراء الحكوميين التابعة للأمم المتحدة الخامسة التي أدت إلى اعتماد قرارين في

اللجنة الأولى للجمعية العامة للأمم المتحدة في تشرين الثاني / نوفمبر 2018 وفي الاجتماع الموضوعي الأول لمجموعة العمل مفتوحة العضوية في الفترة من 9 إلى 13 أيلول / سبتمبر 2019 في نيويورك وأنها تؤيد الحاجة إلى وجود فهم مشترك حول كيفية تطبيق القانون الدولي على الدولة وهو أمر ممكن في إطار الأمم المتحدة وغيرها من المنتديات المتعددة الأطراف. أشار أيضاً أنه يجب أن يكون تطوير وتنفيذ قوانين وسياسات وممارسات الأمن الالكتروني متسقة مع القانون الدولي بما في ذلك القانون الدولي لحقوق الإنسان. ذكر في الختام أن المداولات حول القضايا المذكورة أعلاه في آلكو ينبغي بالتالي أن تأخذ في الاعتبار العمل حول الموضوع الذي يتم إجراؤه تحت رعاية الأمم المتحدة بهدف تجنب ازدواجية العمل.

20. أشار **مندوب جمهورية كوريا** أولاً إلى أن تكنولوجيا المعلومات والاتصالات (ICT) بالإضافة إلى توفير فرص لا حدود لها ومزايا اقتصادية واجتماعية غير مسبوقة، قد تسببت في نفس الوقت في تهديدات أمنية جديدة وهي الهجمات الإلكترونية. أشار إلى أن الأمن الالكتروني يتطلب تعاوناً دولياً أو حتى تعددية. ذكر لذلك أن التعاون المتبادل والمساعدة وتبادل المعلومات أمر مطلوب بناءً على العناصر الحاسمة التالية: أ) تتمتع المناقشات في آلكو بالقدرة على تعميق فهم الدول للمشهد الحالي للإطار المعياري للفضاء السيبراني والتحديات المقبلة. ب) تلعب التدابير العملية المصممة لبناء القدرات على المستويات الوطنية والإقليمية والعالمية دوراً حاسماً في تعزيز الشفافية والمرونة في الفضاء السيبراني. أشار إلى أن كوريا تشارك بنشاط أيضاً في المناقشات حول معايير الفضاء السيبراني في إعداد فريق الخبراء الحكوميين التابع للأمم المتحدة بالإضافة إلى عقد مشاورات ثنائية حول السياسة الإلكترونية مع عشرات البلدان. أضاف في الختام أن جمهورية كوريا قد قدمت بالفعل إجاباتها على استبيان مجموعة العمل مفتوحة العضوية التابعة لآلكو المعنية بالقانون الدولي في الفضاء السيبراني والذي يأمل أن يعمق فهم الجهات الفاعلة في مجال الفضاء السيبراني حول قضايا الفضاء السيبراني وتعزيز التعاون بين الدول.

21. أعرب **مندوب جمهورية إيران الإسلامية** أولاً عن تقدير لعمل آلكو ومقرر مجموعة العمل مفتوحة العضوية المعنية بالفضاء السيبراني حول هذا الموضوع وخاصةً لإعداد الاستبيان بشأن التعاون الدولي في التعامل مع الجرائم الإلكترونية. ذكر أن جمهورية إيران الإسلامية تتابع باهتمام عمل آلكو ومجموعة العمل مفتوحة العضوية المعنية بالقانون الدولي في الفضاء السيبراني حول هذا الموضوع، وأنها تعتبر مجموعة العمل مفتوحة العضوية منصة مناسبة للدول الأعضاء لتبادل الأفكار في سياق قانوني والمساهمة في التطوير المناسب للقانون الدولي بشأن الجرائم الإلكترونية. أشار إلى أن الاجتماع الرابع لمجموعة العمل مفتوحة العضوية الذي عقد في هانغتشو بالصين ناقش بعض القضايا وثيقة الصلة مثل التعاون الدولي في مكافحة الجرائم الإلكترونية وتطبيق مبدأ عدم التدخل وكذلك القضايا المتعلقة بسيادة البيانات، حيث لعبت إيران دوراً نشطاً فيها.

22. أفاد فيما يتعلق بمكافحة جرائم الفضاء السيبراني بأن إيران تواصل المشاركة في المناقشات ذات الصلة في سياق الأمم المتحدة من أجل التوصل إلى صك يتم التفاوض بشأنه واعتماده عالمياً بشأن مكافحة الجريمة الالكترونية. ذكر أيضاً أن جمهورية إيران الإسلامية اتخذت على الصعيد المحلي بعض الخطوات المهمة بما في ذلك التصديق على قانون الجرائم الإلكترونية (2009) وقانون التجارة الإلكترونية (2003) وقانون نشر البيانات والوصول إليها (2010) (LPAD) التي وفرت الأساس القانوني في الفضاء السيبراني. أشار إلى أن حكومة جمهورية إيران الإسلامية أنشأت فيما يتعلق بالتدبير التنفيذي في مكافحة الجرائم الإلكترونية الشرطة الالكترونية في عام 2011 كجهاز نشط في مكافحة الجريمة الإلكترونية. أفاد أيضاً بأن جمهورية إيران الإسلامية قد وقعت اتفاقيات ومذكرات تفاهم مع دول مختلفة خاصةً في مناطق غرب ووسط آسيا.

23. ذكر فيما يتعلق بمبدأ عدم التدخل أنه على الرغم من الأهمية والحالة العامة لهذا المبدأ التي لا جدل فيها، فإن الأبعاد والملامح الدقيقة لتطبيق هذا المبدأ على الفضاء السيبراني ليست واضحة وتحتاج إلى مزيد من العمل والمداولات. أعرب في الختام عن تقديره لعمل الأمين العام في صياغة المبادئ الأساسية التوافقية للقانون الدولي المنطبقة في الفضاء السيبراني، وأشار إلى أن جمهورية إيران الإسلامية ستقدم تعليقاتها على هذا المشروع في الوقت المناسب.

24. دعا **مندوب جمهورية الصين الشعبية** أولاً إلى مبادئ السلام والسيادة والحكم المشترك والفوائد المشتركة في التبادل والتعاون الدوليين في الفضاء السيبراني. ذكر أن التحدي الحقيقي يكمن اليوم في تحديد كيفية تطبيق مبادئ القانون الدولي في الفضاء السيبراني. أشار إلى أن الصين تؤيد صياغة قواعد دولية مقبولة عالمياً في الفضاء السيبراني من خلال مفاوضات ديمقراطية متعددة الأطراف وعادلة في إطار الأمم المتحدة، ومن المتوقع في هذا الصدد أن يسفر فريق الخبراء الحكوميين الجديد ومجموعة العمل مفتوحة العضوية تحت رعاية الأمم المتحدة عن نتائج إيجابية.

25. ذكر فيما يتعلق بمسألة مكافحة جرائم الفضاء السيبراني أنه نظراً للاختلافات في القوانين والممارسات بين الدول، لا يمكن حل تحديات مكافحة الجريمة الالكترونية عن طريق بضع اتفاقيات إقليمية، بما في ذلك اتفاقية بودابست المبرمة منذ 18 عاماً - وأن الحل الوحيد الفعال هو وضع صك قانوني دولي بشكل جماعي يتم التفاوض عليه من قبل جميع الدول ويكون مفتوحاً لجميع الدول. أشار كذلك إلى أن روسيا والصين وعدد من الدول الأخرى شاركت في تقديم مشروع قرار للجمعية العامة للأمم المتحدة في نيويورك يطلب من الجمعية العامة إنشاء لجنة حكومية دولية مفتوحة العضوية لوضع اتفاقية دولية شاملة بشأن مكافحة الجريمة الالكترونية، والتي إذا تم اعتمادها سيوفر منصة مهمة للبلدان النامية للمشاركة في عملية صنع القواعد الدولية لمكافحة الجريمة الالكترونية.

26. ذكر فيما يتعلق بمسألة الحرب الإلكترونية أن الصين تعارض بشدة الحرب الإلكترونية أو سباق التسلح الالكتروني، ويحث جميع الدول الأعضاء في آلكو على دعم الاستخدام السلمي للفضاء السيبراني، وستكون البلدان بشكل عام بالنظر إلى "الفجوة الرقمية" بين البلدان النامية والبلدان المتقدمة في وضع غير مؤات في مناقشة وتطوير هذه القواعد، وسيكون من الصعب ضمان أن القواعد عادلة ومنصفة. أشاد بعد ذلك بمجموعة العمل مفتوحة العضوية التابعة لآلكو المعنية بالقانون الدولي في الفضاء السيبراني باعتبارها منصة مهمة غطت مجموعة واسعة من القضايا الجديدة والمهمة في القانون الدولي في الفضاء السيبراني بما في ذلك مكافحة الجرائم الإلكترونية وتنظيم المحتوى الضار عبر الإنترنت والقضايا المتعلقة بتدفق البيانات عبر الحدود - والتي يمكن أن تساعد الدول الأعضاء على الاستعداد لعمليات وضع القواعد الدولية المحتملة في ظل الأمم المتحدة.

27. أثنى كذلك على توافق الآراء بشأن استكشاف صياغة وثيقة عامة غير ملزمة توضح المبادئ الأساسية التوافقية للقانون الدولي المطبق في الفضاء السيبراني كنتيجة مهمة لاجتماع مجموعة العمل مفتوحة العضوية. أشار تقديراً لمشروع المبادئ الذي أعده الأمين العام إلى أن المبادئ المتعلقة بتدفق البيانات عبر الحدود وتنظيم المحتوى الضار عبر الإنترنت مفقودة في مسودة الأمين العام على أمل أن يتم تضمينها في التكرار القادم لمشاريع المبادئ. أعرب أيضاً عن سروره لاستضافة الصين للاجتماع الرابع لمجموعة العمل مفتوحة العضوية في أيلول / سبتمبر 2019. حث جميع الدول الأعضاء في آلكو في الختام على المشاركة بنشاط في مناقشة مجموعة العمل مفتوحة العضوية وبالتالي تعزيز قدرتها على إدارة الفضاء السيبراني ووضع القواعد.

28. تطرق **مندوب جمهورية اندونيسيا** أولاً إلى مختلف الخطوات التنظيمية التي اتخذتها حكومة إندونيسيا لتعزيز الاستخدام السلمي للفضاء السيبراني والنمو الاقتصادي من خلاله بما في ذلك القانون رقم 11 لعام 2008 بشأن المعلومات والمعاملات الإلكترونية والذي تم تعديله بعد ذلك بموجب القانون رقم 19 لعام 2016 واللائحة الحكومية رقم 71 لسنة 2019 بشأن استخدام النظام والمعاملات الإلكترونية واللوائح الجديدة التي يجري إعدادها وهي مشروع قانون الأمن الالكتروني والمرونة ومشروع قانون حماية البيانات الشخصية والاستراتيجية الوطنية للأمن الالكتروني. أضاف أنه تم أيضاً إعداد عدد من اللوائح لمكافحة الجرائم التقليدية باستخدام الفضاء السيبراني على سبيل المثال الجرائم المتعلقة بالمخدرات وانتهاكات حقوق الإنسان (خاصةً تلك التي تشمل الأطفال والتمييز ضد الأطفال والاستغلال والعنف) وكذلك مكافحة الإرهاب والتطرف العنيف بما في ذلك خطة العمل الوطنية لمكافحة التطرف الذي يؤدي إلى الإرهاب.

29. ذُكر أن إندونيسيا توافق من حيث المبدأ على اعتماد 11 معياراً إلكترونياً بشأن سلوك الدولة المسؤولة بما يتماشى مع تقرير فريق الخبراء الحكوميين للأمم المتحدة لعام 2015. أكد كذلك على المبادئ التوجيهية التالية للفضاء السيبراني: أ) المبادئ والمعايير العالمية لتطوير الهيكل العالمي للفضاء السيبراني في

مختلف المنتديات بما في ذلك كل من الأمم المتحدة وآلكو من خلال نهج أصحاب المصلحة المتعددين لتطوير فضاء إلكتروني متسامح وشامل، ب) تطوير فضاء إلكتروني مفتوح وحر وآمن للأغراض السلمية فيما يتعلق بسيادة الدولة وحقوق الإنسان من خلال المشاركة الشاملة، ج) استخدام الحلول الدبلوماسية وتجنب القوة العسكرية في حل نزاعات الفضاء السيبراني. أعرب أيضاً عن تقديره لعمل مجموعة العمل مفتوحة العضوية الرابعة المعنية بالقانون الدولي في الفضاء السيبراني ولا سيما نتيجة المبادئ الأساسية التوافقية للقانون الدولي المطبق في الفضاء السيبراني. أشار إلى أن جمهورية إندونيسيا وافقت بشكل أساسي على المبادئ من (أ) إلى (ز) من مشروع الأمين العام "للمبادئ الأساسية التوافقية للقانون الدولي في الفضاء السيبراني"، مع ملاحظة أن المبدأ (ح) يحتاج إلى مزيد من المناقشات كما هو أساساً في المجال العسكري ويجب مناقشته من خلال منتديات مثل الحوار الدفاعي وما إلى ذلك.

30. شجعت أمانة آلكو على ما يلي: أ) إنشاء دليل نقطة اتصال لآلكو يتألف من مستويات عالية وعملية. يجب أن تنسق نقطة الاتصال وتؤكد وقت وقوع الحوادث الإلكترونية، ب) لدعم شركات وسائل التواصل الاجتماعي لمساعدة حكومات الدول الأعضاء في آلكو في تصفية انتشار المحتويات السلبية عن الإرهاب والمواد الإباحية (بما في ذلك حماية الأطفال عبر الإنترنت من التمييز والاستغلال والعنف) وغيرها من المسائل المتعلقة بالجرائم الإلكترونية، ج) تعزيز الشراكة بين القطاعين العام والخاص من خلال بناء التعاون لمنع إساءة استخدام الإنترنت.

31. أعرب **مندوب جمهورية فيتنام الاشتراكية** أولاً عن مخاوفه بشأن تطبيق القانون الدولي في الفضاء السيبراني حيث أصبح الأمن الإلكتروني بشكل متزايد قضية عالمية مما يشكل مخاطر أمنية غير متوقعة. ذكر أن فيتنام عانت كثيراً في الماضي من قضايا "الأخبار الكاذبة" وغيرها من أشكال الهجمات الإلكترونية، مما يهدد الأمن القومي ويتسبب في خسارة كيانات الدولة والمواطنين. إن عدم وجود مجموعة من القواعد المقبولة عالمياً لتنظيم الأنشطة في الفضاء السيبراني بما في ذلك تطبيق المبادئ الراسخة للقانون الدولي في الفضاء السيبراني، يستدعي اتخاذ إجراءات فورية من جانب الدول. أشار فيما يتعلق بالقوانين الوطنية لتعزيز الأمن الإلكتروني إلى أنه تم سن القانون التالي داخل فيتنام، وهو القانون الشامل للأمن الإلكتروني الذي سُن في حزيران / يونيو 2018، وأن هناك مرسوماً حكومياً يفصل تنفيذ القانون قيد الإنشاء الآن ليحكم بشكل كبير الأمن الإلكتروني للأمة.

32. أشار إلى أنه يصعب الحصول على فهم مشترك لكيفية تطبيق القانون الدولي في الفضاء السيبراني فيما يتعلق بالتعاون الدولي في مجال الأمن الإلكتروني إلى أنه دون هذا التعاون. ذكر في هذا الصدد أنه على الرغم من أن فيتنام لم تصبح بعد طرفاً في أي اتفاقية دولية في هذا الصدد فإنها تعمل تدريجياً على تحسين إطارها القانوني الوطني في هذا المجال بهدف ضمان توافقه مع القواعد والمعايير الدولية الحالية ذات الصلة بما في ذلك تبادل الآراء مع أعضاء رابطة أمم جنوب شرق آسيا الآخرين بشأن مكافحة الجرائم

الإلكترونية على أساس أن القانون الدولي وخاصةً المبادئ المنصوص عليها في ميثاق الأمم المتحدة يجب أن تنطبق على الفضاء السيبراني.

33. أضاف في هذا الصدد أنه ينبغي أن يستخلص الدروس من مجالات أخرى مثل الفضاء الخارجي وقانون البحار بما أن الفضاء السيبراني ظاهرة آخذة في التطور. بينما أعرب عن تقديره لعمل آلكو كمنصة للتعاون الإقليمي الفعال لمكافحة الجرائم الإلكترونية، أشار بشكل خاص إلى العمل المفيد الذي قام به مقرر مجموعة العمل مفتوحة العضوية المعنية بالقانون الدولي في الفضاء السيبراني بما في ذلك المساهمات التي قدمتها مختلف الدول الأعضاء. أعرب أيضاً عن تقديره للعمل الذي أنجزه الأمين العام في مشروعه حول "المبادئ الأساسية التوافقية للقانون الدولي في الفضاء السيبراني"، بينما أشار أيضاً إلى أن الموضوع يتطلب مزيداً من الدراسة ولا ينبغي التعجيل به لغرض اعتماد وثيقة ختامية. ذكر في الختام أن تبادل الآراء هو السبيل الوحيد للدول لتعميق التفاهم المتبادل والتوصل إلى قرارات على الرغم من صعوبة توصل الدول الأعضاء إلى اتفاق خلال الاجتماع الرابع لمجموعة العمل مفتوحة العضوية.

34. فتح بعد ذلك نائب الرئيس باب التعليقات من الوفود المراقبة.

35. أدلى **مندوب اللجنة الدولية للصليب الأحمر (ICRC)** بتصريحه حول القيود التي يفرضها القانون الإنساني الدولي أو (IHL) على استخدام العمليات الإلكترونية أثناء النزاعات المسلحة. ذكر أن اللجنة الدولية للصليب الأحمر مهتمة بالتكلفة البشرية المحتملة نظراً لاستخدام العمليات الإلكترونية في النزاعات المسلحة الجارية، وفي هذا الصدد من الأهمية بمكان أن تؤكد الدول أن القانون الإنساني الدولي يحد من استخدام العمليات الإلكترونية أثناء النزاع المسلح ويحمي المدنيين والأعيان المدنية، كما هو الحال مع أي وسائل وأساليب حرب أخرى. شدد أيضاً في نفس الوقت على أن تطبيق القانون الإنساني الدولي لا يعني إضفاء الشرعية على النزاعات، لا في المجالات التقليدية للحرب ولا في الفضاء السيبراني. يخضع ذلك لميثاق الأمم المتحدة والقانون الدولي العرفي ذي الصلة. أشار أيضاً أن القانون الإنساني الدولي يوفر طبقة إضافية من الحماية والشعور بالإنسانية وسط هذه المعاناة.

36. رحب في هذا الصدد بمشروع الأمين العام بشأن "المبادئ الأساسية التوافقية بشأن القانون الدولي المطبق في الفضاء السيبراني" كنتيجة ملموسة لمجموعة العمل مفتوحة العضوية الرابعة المعنية بالقانون الدولي في الفضاء السيبراني ولا سيما المبدأ 2(ح)، وهو حكم يتناول الاستخدام العسكري للفضاء السيبراني ويهدف إلى ضمان احترام القانون الإنساني الدولي. أشار إلى أنه من خلال تبني مبدأ بهذا المعنى فإن آلكو ستساهم بشكل كبير في تقدم المحادثات الدولية حول هذه القضية. شجع الدول الأعضاء في آلكو على مواصلة دراسة كيفية تقييد القانون الإنساني الدولي لاستخدام العمليات الإلكترونية أثناء النزاعات المسلحة. أشار في الختام إلى أنه في حين أنه من الصحيح أن تطوير القدرات الإلكترونية العسكرية واستخدامها أثناء النزاع المسلح لا يمكن أن يحدث في فراغ قانوني ومقيد بالقانون الدولي القائم بما في ذلك

القانون الإنساني الدولي في الوقت نفسه، ليس هناك شك في أنه كما هو الحال مع تطوير أي طريقة جديدة للحرب، قد تتفق الدول على قواعد إضافية لحظر أو تقييد قدرات أو عمليات إلكترونية عسكرية محددة لمجموعة من الأسباب بما في ذلك الأسباب الإنسانية والتي ينبغي أن تستند إلى القانون القائم وتعززه.

37. ذكر **مندوب الاتحاد الروسي** أولاً أن تطبيق القانون الدولي ليس بهذه البساطة كما قد يبدو منذ اعتماد التقرير الأخير لمجموعة الخبراء الحكوميين في عام 2015، لم تتقدم المناقشة بشكل ملحوظ. ذكر أن أحد الأسباب الرئيسية لذلك هو الاختلاف في وجهات نظر الدول فيما يتعلق بطبيعة استخدام هذا المجال. تحاول إحدى المجموعات التي تنتمي إليها روسيا تطوير الجوانب القانونية للاستخدام السلمي لتكنولوجيا المعلومات والاتصالات بما في ذلك القضايا العملية المتعلقة بحماية المساواة في السيادة بين الدول وعدم التدخل والتعاون، بينما من ناحية أخرى تضع مجموعة الدول الأخرى في مقدمة التحليل الاستخدام العسكري لتكنولوجيا المعلومات والاتصالات بما في ذلك قابلية تطبيق المادة 51 من ميثاق الأمم المتحدة وحق الدفاع عن النفس.

38. أشار كذلك إلى أن الرأي الأخير يهدف إلى ضمان الحق في تطبيق تدابير مضادة رداً على الهجمات الإلكترونية مع تجنب أو رفض مباشر لمناقشة مشكلة تأسيس العلاقة بين الهجوم والحالة المقابلة وكذلك مشكلة وضع معايير إثبات لمثل هذا الاتصال والضرر الناجم عنه. تعتبر روسيا مع ذلك أن مسألة معيار الإثبات وإسناد الهجوم الحاسوبي إلى الدولة من أجل إثبات مسؤوليتها القانونية الدولية ينبغي أن تسبق أي استنتاجات لتعميم غير هام وما إذا كان يمكن اتخاذ أي تدابير مضادة استجابةً أكثر من ذلك في ضوء المادة 51 من ميثاق الأمم المتحدة. أضاف أن الاعتراف بأنواع معينة من استخدام تكنولوجيا المعلومات والاتصالات كهجوم مسلح يعطي الحق في الاستخدام المتبادل للقوة التي يمكن أن تغرق العالم في الفوضى وعواقب لا يمكن التنبؤ بها. أشار في نفس السياق إلى أن التطبيق العام للقانون الإنساني الدولي هو مسألة صعبة. ذكر أن التطبيق العملي لمبدأ التعاون السلمي في مجال تكنولوجيا المعلومات والاتصالات هو المبدأ الأساسي لتطبيق القانون الدولي في الفضاء السيبراني والذي تدعمه مختلف قرارات الجمعية العامة للأمم المتحدة. أشار كذلك إلى أن النزعة الإقليمية في هذه المسألة قد تكون خطيرة.

39. ذكر فيما يتعلق بمسألة الجرائم الإلكترونية أن الدول بغض النظر عن مستوى تطورها لا يمكنها أن تتعامل بفعالية مع الجرائم الإلكترونية دون تعاون دولي مناسب، وأن هناك بالفعل في هذا الصدد حاجة إلى صك دولي ملزم تحت رعاية الأمم المتحدة. لاحظ أنه يجب أن يقوم هذا الصك على مبادئ المساواة في السيادة وعدم التدخل لتحقيق الأهداف التالية: أ) تعزيز وتقوية التدابير لمنع الجرائم وغيرها من الأعمال غير القانونية، ب) ضمان الملاحقة القضائية لمرتكبي هذه الأفعال وتسهيل التعرف على هذه الأعمال والتحقيق فيها، ج) زيادة كفاءة التعاون الدولي بما في ذلك التدريب والمساعدة التقنية. ذكر في الختام أنه في هذا الصدد صاغت روسيا والصين وعدد من الدول الأخرى قرار الجمعية العامة للأمم المتحدة بعنوان

"مكافحة استخدام المحكمة الجنائية الدولية للتجارة الدولية لأغراض إجرامية" والذي جعل من الممكن من ناحية البناء على المناقشات حول هذه القضية التي عقدت في الجمعية العامة للأمم المتحدة هذا العام ومن ناحية أخرى تخلق منصة تفاوضية يمكن استخدامها على المدى الطويل.

40. طلب **مندوب سلطنة عمان** الكلمة بعد تصريحات المندوبين المراقبين. أعرب أولاً عن تقديره ووافق على النتائج التي توصلت لها مجموعة العمل مفتوحة العضوية المعنية بالقانون الدولي في الفضاء السيبراني في اجتماعه الرابع الذي عقد في هانغتشو بالصين في الفترة من 2 إلى 4 أيلول / سبتمبر 2019 حول أهمية التعاون بين الدول الأعضاء في مجال مكافحة الجريمة الإلكترونية، وكذلك المشروع الذي أعده الأمين العام بشأن مبادئ القانون الدولي المنطبقة على الفضاء السيبراني. ذكر أنه بما أن التهديدات الإلكترونية تؤثر بشدة على سيادة الدول وأمنها واستقرارها الاقتصادي والاجتماعي، فليس لديها خيارات سوى التعاون مع بعضها البعض لصياغة التنظيم القانوني الذي يحكم العبور والمحتوى والاستخدام الضار للفضاء السيبراني. أشاد في هذا الصدد بعمل مجموعة العمل مفتوحة العضوية المعنية بالقانون الدولي في الفضاء السيبراني لآلكو والذي كان بمثابة نقطة انطلاق يمكن للدول الأعضاء أن تبني عليها من أجل تبني موقف موحد وواضح يمكن طرحه في المحافل الدولية الأخرى.

ثالثاً. المناقشات العامة والتطورات الأخيرة

(أ) تطبيق مبدأ عدم التدخل في الفضاء السيبراني

41. تشير السيادة في القانون الدولي العام المعاصر إلى الوضع القانوني الدولي الأساسي لدولة لا تخضع ضمن اختصاصها الإقليمي للاختصاص القضائي الحكومي أو التنفيذي أو التشريعي أو القضائي لدولة أجنبية أو للقانون الأجنبي بخلاف القانون الدولي العام.[5]

42. ونظراً لخصائصه الفريدة - التي توصف عادة بأنها "لا مكان" عظيم أو مجال دون حدود حقيقية تتجاوز الفضاء المادي - فإن تطبيق السيادة في الفضاء السيبراني مع ذلك بعيد كل البعد عن أن يكون مباشراً. بينما يبدو أن الإجراءات في المجال الإلكتروني تحدث خارج الحدود المادية لأي دولة في عالم افتراضي فإن آثارها مع ذلك لها آثار في العالم الحقيقي غالباً ما يتم الشعور بها داخل الدول. إن البنية التحتية لتكنولوجيا المعلومات والاتصالات علاوة على ذلك مملوكة للحكومة أو الشركات وهي متصلة بشبكة الإنترنت الوطنية. يستلزم علاوةً على ذلك امتياز الدولة للسيطرة على الأحداث داخل أراضيها القدرة على تنظيم الآثار المحلية للأعمال التي تتجاوز الحدود الإقليمية. لذا في حين أنه من الصحيح أن البنية الفريدة للفضاء السيبراني تجعل من الصعب على الدول ممارسة سيادتها، فإن المشاكل التقنية التي ينطوي عليها

[5] اتش. ستينبرغر، *السيادة*، (معهد ماكس بلانك للقانون العام المقارن والقانون الدولي، موسوعة القانون الدولي العام، المجلد 10 (1987))، صفحة 414.

الأمر لا تمنع ولا يمكن أن تمنع الدولة من ممارسة سيادتها. قامت إحدى الدول الأعضاء في آلكو بتلخيصها بشكل مثالي في بيانها في الدورة السنوية الرابعة والخمسين لآلكو - "السمة المراوغة لهذا النوع من الاختصاص القضائي تتطلب أن تكون خاضعة لسيطرة جميع الدول".[6]

43. أعلن فريق الخبراء الحكوميين التابع للأمم المتحدة في نسختي 2013[7] و2015 أن القانون الدولي ولا سيما ميثاق الأمم المتحدة ينطبق على الفضاء السيبراني. فإن الأسئلة مع ذلك حول كيفية تطبيقه لا تزال دون حل. أكد دليل تالين 1.0 و2.0 أيضاً على تطبيق القانون الدولي في الفضاء السيبراني. توضح القاعدتان 1 و2 من دليل تالين 1.0 الأساس القانوني لممارسة الاختصاص القضائي هذا.[8] تنص القاعدة 1 بوضوح على أنه يجوز لدولة ما أن تمارس سيطرتها على البنية التحتية الإلكترونية والأنشطة الواقعة داخل أراضيها السيادية والتي تشمل الأراضي البرية والمياه الداخلية والبحر الإقليمي والمياه الأرخبيلية والمجال الجوي الوطني. هذا الحق هو الامتداد الطبيعي للسيادة التي تتمتع بها الدولة على أراضيها. توضح القاعدة 2 أنه يجوز للدولة ممارسة اختصاصها القضائي دون المساس بالالتزامات الدولية السارية: أ) على الأشخاص المنخرطين في أنشطة إلكترونية على أراضيها، ب) على البنية التحتية الإلكترونية الموجودة على أراضيها، ج) خارج الحدود الإقليمية وفقاً للقانون الدولي.

44. ازداد حجم وتواتر الهجمات الإلكترونية باستمرار منذ إنشاء شبكة الويب العالمية. استجابت الحكومات لهذه الهجمات بدءاً من إزعاج المتسللين الأفراد في السنوات الأولى إلى العدوان الالكتروني الشديد ضد الدول بإنشاء العديد من وكالات الأمن الالكتروني العسكرية والحكومية وبتشريعات تتناول الأهمية الحاسمة لأمن الفضاء السيبراني بشكل مباشر.

45. يفرض ميثاق الأمم المتحدة قيوداً أساسية على الحرب الإلكترونية من خلال حظر التهديد أو استخدام القوة بموجب المادة 2(4) باعتباره الركيزة الأساسية لقانون الحرب. اعتبرت محكمة العدل الدولية أن المادتين 2(4) و51 من ميثاق الأمم المتحدة فيما يتعلق بحظر التهديد أو استخدام القوة والدفاع عن النفس على التوالي تنطبقان على "أي استخدام للقوة بغض النظر عن الأسلحة المستخدمة".[9] يفرض القانون الدولي الإنساني قيوداً على استخدام العمليات الإلكترونية أثناء النزاعات المسلحة، حيث تؤكد اللجنة الدولية للصليب الأحمر (ICRC) أن القانون الدولي الإنساني يحد من استخدام العمليات الإلكترونية أثناء النزاع المسلح ويحمي المدنيين والممتلكات المدنية كما يفعل مع أي وسائل وطرق أخرى للحرب وأن مضمونه

[6] بيان من جمهورية إيران الإسلامية، بند جدول الأعمال: القانون الدولي في الفضاء السيبراني، الدورة السنوية الرابعة والخمسون لآلكو، بكين، عام 2015.

[7] يعلن فريق الخبراء الحكوميين التابع للأمم المتحدة في تقريره لعام 2013 أن "سيادة الدولة والمعايير والمبادئ الدولية التي تنبع من السيادة تنطبق على سلوك الدولة للأنشطة المتعلقة بتكنولوجيا المعلومات والاتصالات وعلى اختصاصها القضائي على البنية التحتية لتكنولوجيا المعلومات والاتصالات داخل أراضيها". انظر "التطورات في مجال المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي"، تقرير الأمين العام لعام A/68/156، 2013.

[8] انظر *دليل تالين للقانون الدولي المطبق على الحرب الإلكترونية*، (مطبعة جامعة كامبريدج، 2013)، الصفحات 25-30.

[9] رأي استشاري بشأن الأسلحة النووية، *مشروعية التهديد بالأسلحة النووية أو استخدامها*، رأي استشاري، 1996 محكمة العدل الدولية رقم 226 (8 تموز / يوليو)، الفقرة 39.

ليس لإضفاء الشرعية على النزاعات. تؤكد بعض الدول ومع ذلك أن قبول تطبيق المادة 51 من ميثاق الأمم المتحدة على الفضاء السيبراني يرقى إلى مستوى إضفاء الطابع العسكري للفضاء السيبراني وينفي المفهوم الأوسع للاستخدام السلمي للفضاء السيبراني. يوفر المبدأ الواسع لعدم التدخل بموجب القانون الدولي إرشادات محدودة في مجال الفضاء السيبراني لأن الغالبية العظمى من العمليات الالكترونية لا تطلق العتبات الحركية لاستخدام القوة وبالتالي لا تتناسب تماماً مع العناصر المعترف بها تقليدياً في قاعدة عدم التدخل.

46. يُفهم التدخل تقليدياً على أنه تدخل قسري في أمور تقع ضمن الشؤون السيادية للدولة مثل اختيار النظام السياسي والاقتصادي والاجتماعي والثقافي وصياغة السياسة الخارجية. يوفر الفضاء السيبراني بيئة سهلة حيث يمكن أن يحدث التدخل، وينوع وسائله وأساليبه ولكنه يعزز قابليته للتوسع والوصول والتأثيرات أيضاً. تضاعف استخدام الفضاء السيبراني في الماضي القريب للتدخل الانتخابي وكان له عواقب وخيمة وبعيدة المدى. يتكون هذا التدخل بشكل أساسي من الهجمات على البنية التحتية الانتخابية وعمليات التلاعب بالسلوك الانتخابي. كافح المعلقون في القانون الدولي لتأهيل مثل هذه العمليات. خلصوا إلى أنهم لا يستوفون شروطه وخاصة شروط الإكراه على الرغم من أن الأغلبية وضعتهم في إطار مبدأ عدم التدخل.[10] يؤكد بعض المؤلفين مع ذلك أن التدخل الالكتروني الانتخابي يمكن أن ينتهك مبدأ عدم التدخل من خلال القول بأن التلاعب بالناخبين قد يصل إلى حد "الإكراه".[11]

47. أُنشئ فريق الخبراء الحكوميين التابع للأمم المتحدة (UNGGEs) في ست مناسبات منذ عام 2003 لدراسة التهديدات القائمة والمحتملة في مجال أمن المعلومات والتدابير التعاونية الممكنة لمواجهتها بما في ذلك فريق الخبراء الحكوميين للفترة 2019-2021. أكدت هذه المجموعات من جديد من خلال تقاريرها الثلاثة التي تحظى بتوافق الآراء (2010 و2013 و2015) وهي تقارير تراكمية بطبيعتها أن القانون الدولي ولا سيما ميثاق الأمم المتحدة قابل للتطبيق وضروري للحفاظ على السلام والاستقرار في بيئة تكنولوجيا المعلومات والاتصالات. أوصوا أيضاً بإحدى عشرة قاعدة طوعية غير ملزمة لسلوك الدولة المسؤولة وأقروا بإمكانية وضع قواعد إضافية بمرور الوقت. تمت التوصية باتخاذ تدابير محددة لبناء الثقة وبناء القدرات والتعاون. وافقت الدول الأعضاء بتوافق الآراء في قرار الجمعية العامة 237/70على أن تسترشد في استخدامها لتكنولوجيا المعلومات والاتصالات بتقرير فريق الخبراء الحكوميين لعام 2015 وبالتالي توحيد إطار عمل أولي لسلوك الدولة المسؤولة في استخدام تكنولوجيا المعلومات والاتصالات.

48. فشل فريق الخبراء الحكوميين الخامس والمكلف التابع للأمم المتحدة بتطوير "فهم مشترك" لكيفية تصرف الدول في الفضاء السيبراني في التوصل إلى نتيجة في عام 2017 مع عدم موافقة العديد من الدول على

[10] انظر على سبيل المثال، جينس ديفيد اولين، "هل ينتهك التدخل الروسي الإلكتروني في انتخابات 2016 القانون الدولي؟"، كلية الحقوق بجامعة كورنيل، 2017.

[11] نيكولاس تساغورياس، "التدخل الالكتروني الانتخابي وتقرير المصير ومبدأ عدم التدخل في الفضاء السيبراني"، *المجلة الأوروبية للقانون الدولي: مباشر!*، (2019)

المسودة النهائية للتقرير. حقق فريق الخبراء الحكوميين التابع للأمم المتحدة للفترة 2016-2017 تقدماً ملموساً في توضيح قواعد سلوك معينة للجهات الفاعلة الحكومية وغير الحكومية، ومع ذلك لم تتمكن الدول من الاتفاق على مشروع الفقرة 34 التي توضح بالتفصيل كيفية تطبيق القانون الدولي على استخدام تكنولوجيا المعلومات والاتصالات.

49. أُنشئت في عام 2018 مجموعة عمل أخرى مفوضة من الأمم المتحدة - مجموعة العمل مفتوحة العضوية المعنية بالتطورات في مجال تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي (OEWG) بالتوازي مع فريق الخبراء الحكوميين وبمشاركة "جميع الدول المهتمة". ناقشت مجموعة العمل مفتوحة العضوية وفقاً لتفويضها التهديدات القائمة والمحتملة في مجال أمن المعلومات والتدابير التعاونية الممكنة لمواجهتها وزيادة تطوير قواعد ومعايير ومبادئ السلوك المسؤول للدول وكيف ينطبق القانون الدولي على استخدام الدول لتكنولوجيا المعلومات والاتصالات وتدابير بناء الثقة وإمكانية إقامة حوار مؤسسي منتظم بمشاركة واسعة تحت رعاية الأمم المتحدة. جُدد تفويض مجموعة العمل مفتوحة العضوية لعام 2025/2021 في كانون الأول / ديسمبر 2020. اعتمدت تقريرها النهائي بالإجماع في آذار / مارس 2021.[12] اعتُمد التقرير النهائي بالإجماع من قبل 68 دولة مشاركة ليصبح التقرير الأول عن الأمن الالكتروني بهذا الحجم الذي تم اعتماده بمشاركة حكومية مباشرة.

50. يؤكد التقرير من جديد بيان فريق الخبراء الحكوميين السابق بانطباق القانون الدولي بما في ذلك ميثاق الأمم المتحدة على الفضاء السيبراني. تعترف مجموعة العمل مفتوحة العضوية صراحةً بآليات تسوية النزاعات المقدمة في ميثاق الأمم المتحدة التي تشجع الدول على "السعي إلى تسوية النزاعات بالوسائل السلمية مثل التفاوض والاستفهام والوساطة والتوفيق والتحكيم والتسوية القضائية واللجوء إلى الوكالات أو الترتيبات الإقليمية أو غيرها من الوسائل السلمية التي تختارها". يخلص التقرير إلى أن الطريقة الأكثر فعالية للتوصل إلى أرضية مشتركة بشأن التطبيق الملموس للقانون الدولي على بيئة تكنولوجيا المعلومات والاتصالات هي من خلال التبادل المنتظم لوجهات النظر والممارسات وتحديد قضايا القانون الدولي المحددة التي تتطلب محادثات متعمقة تحت رعاية الأمم المتحدة والأمين العام.[13] يمتنع التقرير عامةً عن تحديد فروع محددة للقانون الدولي يمكن تطبيقها والتي أثار احتمال حدوثها توقعات عالية.

51. طُلب إلى الأمين العام في قرار الجمعية العامة 266/73 إنشاء فريق الخبراء الحكوميين المعني بتعزيز السلوك المسؤول للدولة في الفضاء السيبراني في سياق الأمن الدولي. عقد فريق الخبراء الحكوميين اجتماعه الأول في عام 2019 وقدم تقريره النهائي إلى الجمعية العامة في عام 2021. تتألف المجموعة من 25 عضواً وسيجري رئيسها بين دوراتها مشاورتين غير رسميتين مع جميع الدول الأعضاء في الأمم المتحدة. يشمل التفويض أيضاً إجراء مشاورات حول الموضوع مع المنظمات الإقليمية مثل الاتحاد

[12] "مجموعة العمل مفتوحة العضوية المعنية بالتطورات في مجال المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي - التقرير الموضوعي النهائي"، الجمعية العامة للأمم المتحدة، A/AC.290/2021/CRP.2، 10 آذار / مارس 2021.
[13] *المرجع ذاته*.

الأفريقي والاتحاد الأوروبي ومنظمة الدول الأمريكية ومنظمة الأمن والتعاون في أوروبا والمنتدى الإقليمي لرابطة أمم جنوب شرق آسيا.

52. أعيد التأكيد أثناء المناقشات التي جرت في فريق الخبراء الحكوميين لعام 2019 على العناصر المتعلقة بالقانون الدولي الواردة في تقريري 2013 و2015 ولا سيما أن القانون الدولي وبالتحديد ميثاق الأمم المتحدة ينطبق على استخدامات الدول لتكنولوجيا المعلومات والاتصالات على الرغم من وجود أسئلة حول كيفية تطبيقه. ذُكر علاوة على ذلك أن انطباق القانون الإنساني الدولي على العمليات الالكترونية أثناء النزاع المسلح لا يشجع إضفاء طابع عسكري على الفضاء السيبراني أو الشرعية على الحرب الإلكترونية كما أنه لا يضفي الشرعية على أي شكل آخر من أشكال الحرب. أشير فيما يتعلق بقابلية تطبيق القانون الدولي الإنساني إلى قابلية تطبيقه على استخدام أسلحة ووسائل وأساليب حرب جديدة أثناء النزاعات المسلحة بما في ذلك تلك التي تعتمد على تكنولوجيا المعلومات والاتصالات.[14]

53. اختتم فريق الخبراء الحكوميين عمله باعتماد تقرير توافقي في 28 أيار / مايو 2021.[15] تمثل جهود مجموعة العمل للتوصل إلى توافق في الآراء وحلول وسط بشأن القضايا الرئيسية تقدماً مهماً نظراً لفشل فريق الخبراء الحكوميين الأخير بما في ذلك تداعيات العمليات الإلكترونية العدائية الشديدة ضد أعضاء فريق الخبراء الحكوميين. تتداخل العديد من جوانب التقرير مع تلك الواردة في تقرير مجموعة العمل مفتوحة العضوية نظراً للتشابه في تفويضات كل منهما، ربما تكون الخطوة الأكثر جوهرية إلى الأمام بالنسبة لفريق الخبراء الحكوميين هي إقراره بأن القانون الدولي الإنساني ينطبق على العمليات الإلكترونية أثناء النزاع المسلح بما في ذلك من خلال استحضار المبادئ الأساسية الإنسانية والضرورة والتناسب والتميز. أقر فريق الخبراء الحكوميين بالحاجة إلى مزيد من الحوار حول تأهيل المصطلحات الرئيسية في السياق الالكتروني مع استمرار الخلاف حول التفسير الملموس لمبادئ القانون الدولي الإنساني. يتوسع تقرير فريق الخبراء الحكوميين لعام 2021 في مبادئ القانون الدولي التي قد تكون ذات صلة بالفضاء السيبراني على عكس تقرير مجموعة العمل مفتوحة العضوية. يتضمن تقرير عام 2021 الصادر عن فريق الخبراء الحكوميين حظراً للتهديد باستخدام القوة أو استخدامها ضد السلامة الإقليمية أو الاستقلال السياسي لدولة أخرى واحترام حقوق الإنسان والحريات الأساسية وعدم التدخل في الشؤون الداخلية للدول الأخرى بناءً على تقرير عام 2015 الذي يشير إلى التزام الدولة بالمساواة في السيادة. هو يؤكد على ضعف البنية التحتية الحيوية في مواجهة العمليات الالكترونية العدائية مثل تقرير مجموعة العمل مفتوحة العضوية.[16]

[14] ملخص الرئيس، الاجتماع الاستشاري غير الرسمي لفريق الخبراء الحكوميين (GGE) بشأن تعزيز سلوك الدولة المسؤول في الفضاء السيبراني في سياق الأمن الدولي، 5-6 كانون الأول / ديسمبر 2019، متاح على: https://www.un.org/disarmament/group-of-governmental-experts/

[15] "تقرير مجموعة الخبراء الحكوميين حول تعزيز سلوك الدولة المسؤول في الفضاء السيبراني في سياق الأمن الدولي"، نسخة مسبقة، 28 أيار / مايو 2021.

[16] *المرجع ذاته*.

54. يطور تقرير فريق الخبراء الحكوميين كذلك وسائل الامتثال للمعايير الطوعية غير الملزمة لسلوك الدولة المسؤول المتفق عليها في عام 2015. هو يؤكد على أهمية التعاون الدولي وقيمة تدابير بناء القدرات مثل مجموعة العمل مفتوحة العضوية. برز فريق الخبراء الحكوميين كعملية شاملة لتطبيق القانون الدولي على الفضاء السيبراني وأظهر تقدماً كبيراً من دوراته السابقة لا سيما فيما يتعلق بتطبيق القانون الدولي الإنساني على الفضاء السيبراني على الرغم من أن عدداً من القضايا لا يزال يستحق اهتماماً وثيقاً. لا يزال نطاق مساءلة الدولة والتدابير المضادة غير مستقرة أي قضايا مثل السيادة والعناية الواجبة والتدخل ومعنى الهجوم في عالم الإنترنت كما هو الحال مع الدعوات إلى آلية شفافة لتقييم وتتبع التقدم المحرز في تنفيذ المعايير.[17]

(ب) سيادة البيانات وتدفق البيانات عبر الحدود وأمن البيانات

55. نحن نعيش اليوم في "عصر رقمي" حيث أصبحت البيانات أكثر قيمة من أي وقت مضى. مثلما تعلمت الصناعة التحويلية العالمية قبل نصف قرن التكيف مع عصر الأتمتة تتعلم الشركات اليوم التكيف مع عصر الرقمنة. كان أنصار عولمة البيانات في السنوات الأخيرة على خلاف مع مؤيدي توطين البيانات. كان السابقون يشجعون التدفق الحر والمفتوح للبيانات عبر الحدود بينما اعتمد الأخير تدابير تحد من تدفق البيانات عبر الحدود مشيراً إلى مخاوف تتعلق بالخصوصية والأمن.

56. "سيادة البيانات" هي فكرة خضوع البيانات للقوانين وهياكل الحوكمة في البلد الذي يتم جمعها فيه أو ضد الدولة التي يتم تخزينها أو معالجتها فيها أو حيث يتم دمج الشركة التي تخزن البيانات. قد يكون لسرقة ونقل بيانات المستخدمين خلسة بطريقة غير مصرح بها إلى الخوادم الموجودة خارج البلد الذي نشأت فيه البيانات والتجميع اللاحق لهذه البيانات والتنقيب عنها وتنميطها من قبل عناصر معادية للأمن القومي للدولة المذكورة عواقب شديدة على سيادة وسلامة هذه الدولة. ترى العديد من الدول اليوم أن البيانات هي أصل سيادي وأن القيود الحكومية على تدفقات البيانات ستسمح للدول بأن تكون قادرة على استخدام "البيانات الشخصية والمجتمعية والعامة" المولدة في البلد من أجل رفاهية وتطوير شعبها. هناك حجة مؤيدة للخصوصية أيضاً مفادها أن التعامل مع البيانات كأصل سيادي يبتعد عن الحقوق الفردية على البيانات ويتبادلها مقابل رقم إجمالي للناتج المحلي (GDP) أعلى وسيطرة أكبر للدولة. هناك أيضاً مفاهيم بديلة تدعو إلى مسار وسطي للسيادة يهدف إلى إعادة السيطرة والاستقلالية للناس. توفر هذه المفاهيم إطاراً يمكن من خلاله صياغة أسئلة حول وكالة الفرد والمصلحة الجماعية.

[17] *المرجع ذاته.*

57. يعود تاريخ قوانين حماية البيانات إلى السبعينيات مما يعكس المخاوف بشأن ظهور تكنولوجيات الكمبيوتر والاتصالات مع قدرتها على معالجة كميات كبيرة من البيانات عن بعد. أدرك المشرعون بشكل متزايد أن الإنترنت "بنية تحتية وطنية حيوية" يتم من خلالها تنفيذ نسبة متزايدة من الأنشطة الاقتصادية والاجتماعية اليومية وكمصدر للضعف والتهديد. إن معالجة هذه الازدواجية ووضع تدابير كافية لأمن البيانات هو عنصر أساسي في الاستجابة القانونية والسياسية. دور أمن البيانات أساسي. يجب أن تحمي التدابير الأمنية البيانات من سوء الاستخدام المتعمد وكذلك الفقد العرضي أو تدمير البيانات سواء كانت مادية أو منطقية أو تنظيمية.

58. أصبح تحديد الاختصاص مسألة بارزة للغاية في تنظيم حماية البيانات وذلك فيما يتعلق بمسألة سيادة البيانات، ويرجع ذلك جزئياً إلى التدفق الواسع النطاق للبيانات عبر الحدود ومن ناحية أخرى إلى عدم وجود اتفاق عالمي واحد بشأن حماية البيانات (وما يترتب على ذلك من تجزئة التنظيم). يكون قانون الاختصاص معقداً في غياب اتفاق دولي. إن إرساء السيادة هو مصدر قلق مهم بشكل خاص وسط القيود القانونية والسياسية عندما تكون البيانات والموارد افتراضية ويتم توزيعها على نطاق واسع. أدى النمو الهائل للبيانات الإلكترونية إلى قيام المنظمات الخاصة والوكالات الحكومية ذات التخزين المحدود وموارد تكنولوجيا المعلومات بالاستعانة بمصادر خارجية لتخزين البيانات لمقدمي الخدمات المستندة إلى السحابة. يعد التحقق من أن موفري خدمات التخزين السحابي يوفون بالتزاماتهم الجغرافية التعاقدية يمثل مشكلة صعبة وقد ظهرت كمشكلة حرجة. هناك لذلك حاجة لتطوير خوارزميات جديدة لإثبات سلامة البيانات المخزنة في السحابة ومصداقيتها وموقعها الجغرافي.

59. أدى النقل الدولي للبيانات الشخصية إلى نمو اقتصادي وكفاءات كان لها تأثير إيجابي في جميع أنحاء العالم وفي الوقت نفسه تعرض خصوصية الأفراد لمخاطر جديدة ومتزايدة. إن تطبيق مثل هذه الضوابط في عالم مترابط بشكل متزايد يمثل تحدياً كبيراً في حين أن الحاجة المحتملة للسيطرة على تدفقات البيانات عبر الحدود لأغراض الخصوصية واضحة. تجعل تطورات تكنولوجيا المعلومات والاتصالات مثل الخدمات السحابية الأمور أكثر تعقيداً حيث لا تدرك كيانات المعالجة بالضرورة مكان وجود البيانات. إن من شأن التنسيق المتزايد للقوانين والأنظمة أن يقلل بشكل كبير من احتمالية الاحتكاك بشأن تدفقات البيانات عبر الحدود على الرغم من أن الإجابة قد تكون في النهاية إجابة تكنولوجية. يحدث تطور نظام قانوني جديد له حقوق ومسؤوليات معينة تتعلق بتدفقات البيانات عبر الحدود في وقت زادت فيه فرص إساءة استخدام البيانات المعالجة أو المخزنة بشكل كبير. أصبحت الحاجة إلى مبادئ حاكمة منسقة في معالجة البيانات التي تعبر الحدود الوطنية ملحة.

60. لا تشترك الدول دائماً في مصالح متطابقة على الرغم من النهج العالمي الحالي لتنظيم تدفقات البيانات عبر الحدود. يختلف نمط تدفقات البيانات عبر الحدود بين البلدان المتقدمة والبلدان النامية، حيث تتدفق البيانات

المعالجة إلى البلدان النامية وتتدفق البيانات الخام إلى البلدان المتقدمة. إن الدعوة إلى تنظيم تدفقات البيانات عبر الحدود بالتالي تضع الدول المتقدمة - الدول التي تستفيد أكثر من غيرها من تدفقات البيانات عبر الحدود - في مواجهة الدول النامية. تكمن المشكلة التي تبرز في كيفية التحكم في تدفق البيانات الشخصية عبر الحدود الوطنية أو تنظيمها بطريقة منظمة لا تضع حقوق خصوصية البيانات في مخاطر غير مبررة أو غير مقبولة. أصبح من الضروري لذلك اعتماد نهج عالمي لحل هذه المشاكل. لا توجد اتفاقية أو معاهدة عالمية تتناول حقاً خصوصية البيانات على وجه التحديد - فهناك معاهدات أسفرت حتى الآن عن تعاون وتنسيق دوليين، وإن كان ذلك على المستويين الثنائي والإقليمي.

61. احتل أمن البيانات مكانة مهمة في المناقشات الجارية في المحافل القانونية الدولية. كان للأمم المتحدة أولاً وقبل كل شيء تاريخ طويل في تعزيز الحق في الخصوصية من خلال معاهدات حقوق الإنسان الخاصة بها، لا سيما من خلال المادة 12 من الإعلان العالمي لحقوق الإنسان (UDHR) والمادة 17 من العهد الدولي الخاص بالحقوق المدنية والسياسية (ICCPR). لقد عززت دورها في حماية الخصوصية من خلال مقياسين بارزين - أحدهما نشر بيان حول الحقوق الرقمية، والثاني تعيين مقرر خاص معني بالحق في الخصوصية. تبنت الأمم المتحدة في عام 2013 القرار 167/68 الذي أعرب عن قلقه العميق بشأن التأثير السلبي الذي قد تحدثه مراقبة واعتراض الاتصالات على حقوق الإنسان مع التأكيد على أن الحقوق التي يحتفظ بها الأشخاص خارج الإنترنت يجب أن تكون محمية أيضاً عبر الإنترنت ودعت جميع الدول إلى احترام وحماية الحق في خصوصية الاتصالات الرقمية.[18] تبع القرار تقرير مفصل في عام 2014 بعنوان "دراسة المفوض السامي لحقوق الإنسان حول الحق في الخصوصية في العصر الرقمي"، والتي خلصت إلى أن الممارسات في العديد من الدول كشفت عن عدم وجود تشريعات وطنية كافية و / أو إنفاذ، وضعف الضمانات الإجرائية والرقابة غير الفعالة وكلها ساهمت في انعدام المساءلة عن التدخل التعسفي أو غير القانوني في الحق في الخصوصية".[19]

62. يقدم المقرر الخاص للأمم المتحدة المعني بالحق في الخصوصية في كل عام تقريراً سنوياً إلى مجلس حقوق الإنسان والجمعية العامة للأمم المتحدة. درس المقرر في تقرير 2020 للمقرر الخاص لمجلس حقوق الإنسان المعني بالحق في الخصوصية المقدم إلى الجمعية العامة للأمم المتحدة، جانبين معينين لتأثير كوفيد - 19 على الحق في الخصوصية: حماية ومراقبة البيانات. إن استخدام المعلومات والتكنولوجيا ليس بجديد في إدارة حالات الطوارئ الصحية العامة. اهتم التقرير مع ذلك بالطبيعة الغازية لخصوصية الأدوات التي تتبع جهات الاتصال التي تستخدمها كيانات الصحة العامة بشكل متزايد من أجل تتبع انتشار الأمراض المعدية. يعني هذا أنه سيناريو معقد عندما يتم اقتراح أجهزة المراقبة المستخدمة تقليدياً لأغراض أمن الدولة أو نشرها على عجل لغرض الصحة العامة مثل مكافحة كوفيد - 19. أشار

[18] الأمم المتحدة، "الحق في الخصوصية في العصر الرقمي"، قرار اعتمدته الجمعية العامة في 18 كانون الأول / ديسمبر 2013، 167/68، متاح على: https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167

[19] مفوض الأمم المتحدة السامي لحقوق الإنسان، "الحق في الخصوصية في العصر الرقمي (نظرة عامة)"، متاح على: https://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx

المقرر إلى أنه عندما يكون للدولة قانون ينص على سلطات استثنائية وحيث يبدو أن أي تدابير يتم تطبيقها عند ممارسة هذه الصلاحيات تنتهك الخصوصية بما في ذلك أي شكل من أشكال المراقبة (على سبيل المثال تحديد الموقع الجغرافي ومراقبة القرب والبرامج الضارة والتنصت على الهاتف والتنميط)، يجب أن تتطلب الإشراف المسبق واللاحق لإثبات أنها ضرورية ومتناسبة مع الهدف المنشود. سيكون مضموناً بهذه الطريقة أن أسلوب المراقبة المناسبة فقط هو الذي ينفذ من قبل الأشخاص المناسبين للغرض المناسب وللمدة الزمنية المناسبة.[20]

63. تعد اتفاقية حماية البيانات الصادرة عن مجلس أوروبا لعام 1981 (التي يشار إليها عادةً باسم الاتفاقية 108 أو اتفاقية مجلس أوروبا) أبرز اتفاقية دولية ملزمة بشأن حماية البيانات. إن عضوية هذه الاتفاقية مفتوحة لأي دولة على الرغم من أنه قد تم تأسيسها من قبل مجلس أوروبا، وقد وقعت العديد من الدول غير الأوروبية على هذه الاتفاقية. تم تطوير المبادئ التوجيهية لمنظمة التعاون الاقتصادي والتنمية لعام 1980 بشأن حماية الخصوصية وتدفقات البيانات الشخصية عبر الحدود (تمت مراجعتها في عام 2013) من قبل الدول الأعضاء في منظمة التعاون الاقتصادي والتنمية بالتشاور مع مجموعة واسعة من أصحاب المصلحة. إن التأثير الحقيقي لإرشادات منظمة التعاون الاقتصادي والتنمية هو تأثيرها على محتوى قوانين الخصوصية في جميع أنحاء العالم - بما يتجاوز قاعدة أعضاء منظمة التعاون الاقتصادي والتنمية. تحتوي الإرشادات على ثمانية مبادئ للخصوصية تشكل العمود الفقري للمبادئ المدرجة في معظم قوانين الخصوصية الوطنية. هناك أيضاً إطار الخصوصية التابع لمنظمة التعاون الاقتصادي لآسيا والمحيط الهادئ (2005) (APEC) والقانون التكميلي للمجموعة الاقتصادية لدول غرب أفريقيا (ECOWAS) بشأن حماية البيانات الشخصية داخل المجموعة الاقتصادية لدول غرب أفريقيا 2010 والتي حققت نجاحاً كبيراً على المستوى الإقليمي.

64. من المهم فيما يتعلق بالآثار التجارية لحماية البيانات، ملاحظة أن المادة 14(ج) (ثانياً) من الاتفاقية العامة لمنظمة التجارة العالمية بشأن التجارة في الخدمات (GATS) تسمح بالقيود التجارية الضرورية لحماية خصوصية الأفراد فيما يتعلق بمعالجة ونشر البيانات الشخصية وحماية سرية السجلات والحسابات الفردية"، مع تحديد أن "مثل هذه التدابير لا تطبق بطريقة من شأنها أن تشكل وسيلة للتمييز التعسفي أو غير المبرر بين البلدان التي تسود فيها مثل هذه الظروف، أو تقييد مقنع للتجارة في الخدمات". تزداد أهميتها في التجارة الدولية مع انتقال المزيد من نماذج وممارسات الأعمال إلى المنصة الرقمية وزيادة مشاركة البيانات وتبادلها على نطاق دولي. تؤثر القيود واللوائح المتعلقة بالبيانات بشكل مباشر على التجارة العالمية نظراً لأن البيانات يتم جمعها ورقمنتها وتخزينها ونقلها على نطاق عالمي حقيقي من قبل العديد من الأطراف. ترتبط حماية البيانات ارتباطاً مباشراً بالتجارة في السلع والخدمات في الاقتصاد

[20] جوزيف أ. كاناتشي، تقرير المقرر الخاص المعني بالحق في الخصوصية، الدورة الخامسة والسبعون للجمعية العامة للأمم المتحدة، A/75/147، في 27 تموز / يوليو 2020.

الرقمي - حيث إن الحماية القليلة للغاية يمكن أن تخلق آثاراً سلبيةً على السوق من خلال التأثير على ثقة المستهلك والكثير يمكن أن يقيد الأنشطة التجارية والتجارة بشكل مفرط.

65. يشمل توفير الخدمات الرقمية عبر الحدود حتماً تدفق البيانات عبر الحدود المطلوبة للخدمة مثل بيانات المستهلك أو بيانات الأعمال. يمكن بالتالي تقييم تدابير توطين البيانات التي تقيد أو تحظر فعلياً التجارة عبر الحدود في إطار الاتفاقية العامة لتجارة الخدمات (GATS)، وقد تثير تساؤلات حول ما إذا كانت تدابير توطين البيانات تنتهك المبادئ الأساسية للاتفاقية العامة لتجارة الخدمات. أصبحت الأحكام التي تحظر توطين البيانات شائعة بشكل متزايد في اتفاقيات التجارة الحرة الأخيرة. المزيد والمزيد من البلدان على استعداد لقبول مثل هذه الأحكام في اتفاقيات التجارة الإقليمية والثنائية. إن اتفاقيات التجارة الحرة فقط بالتالي لديها حتى الآن التزامات ملزمة تحظر تدابير توطين البيانات مع عدم اعتبار تدابير توطين البيانات صراحةً مقيدة للتجارة بموجب الاتفاقية العامة لتجارة الخدمات.

(ج) تنظيم المحتوى الضار عبر الإنترنت

66. يحمل الإنترنت مثل أي تكنولوجيات اتصال أخرى كمية من المحتويات التي قد تكون ضارة أو غير قانونية يمكن إساءة استخدامها كوسيلة لأنشطة إجرامية.

67. تعني الطبيعة المختلفة جداً للمحتوى أنه من غير المحتمل أن تكون استجابة واحدة فعالة على الرغم من أن العديد من الأشكال المختلفة للمحتوى يمكن أن تندرج تحت المصطلح الشامل "محتوى غير قانوني أو ضار". قد يُحظر عدد من الأشكال المختلفة للمحتوى بموجب القانون الدولي لحقوق الإنسان (الذي نطلق عليه "محتوى غير قانوني") على سبيل المثال أو قد يكون محظوراً بموجب الاستثناءات المحدودة للحق في حرية التعبير (والتي نطلق عليها "المحتوى الضار")، بما في ذلك المحتوى المرتبط بالإرهاب والمتطرف والكلام الذي يحرض على الكراهية والعنف القائم على النوع الاجتماعي عبر الإنترنت و"الأخبار المزيفة" والمعلومات المضللة والإشاعات. هناك العديد من الأشياء الأخرى: الاعتداء الجنسي على الأطفال وأشكال معينة من المواد الإباحية والتحريض على العنف أو الكراهية والمواد المحمية بحقوق النشر. تختلف الأضرار التي تنتج عن هذه الأشكال من المحتوى اختلافاً كبيراً وبينما يمكن تحديد بعض هذه الأشكال من المحتوى بوضوح نسبياً (مثل الاعتداء الجنسي على الأطفال)، فإن البعض الآخر - مثل المحتوى المتطرف أو الكلام الذي يحض على الكراهية - يصعب تحديده.

68. تعني هذه الاختلافات أنه قد تكون هناك حاجة إلى ردود مختلفة من الدول والمنصات على حد سواء. قد يحتاج أصحاب المصلحة المختلفون إلى المشاركة وقد يلزم النظر في المناهج المختلفة من حيث ربط المسؤولية. قد تختلف باختصار درجة استخدام الخوارزميات أو الأتمتة في تنظيم المحتوى. مثلما توجد

ردود مختلفة على سبيل المثال على المواد المحمية بحقوق الطبع والنشر والكلام الذي يحرض على الكراهية عندما تظهر في وضع عدم الاتصال فإن الردود المختلفة مطلوبة عند ظهورها عبر الإنترنت. قد تحتاج هذه الاستجابات إلى تجاوز مجرد تقييد المحتوى أو إزالته ومعالجة أسباب المشكلة المعينة بما في ذلك من خلال التدخلات غير المتصلة بالإنترنت مثل التعليم المناسب وتحسين محو الأمية الرقمية وتمويل البرامج التي تعالج السلوك الضار.

69. من حيث المحتوى غير القانوني والضار، من الضروري أيضاً التمييز بين المحتوى غير القانوني والمحتوى الضار الآخر. سيكون من الخطر على سبيل المثال دمج قضايا منفصلة مثل وصول الأطفال إلى محتوى إباحي للبالغين وحصول البالغين على مواد إباحية عن الأطفال. يجب تحديد الأولويات بشكل واضح وحشد الموارد لمعالجة أهم القضايا وهي مكافحة المحتوى الإجرامي - مثل تضييق الخناق على استغلال الأطفال في المواد الإباحية أو استخدام الإنترنت كتقنية جديدة للمجرمين.

70. من الواضح لذلك يمكن أن يكون تنظيم المحتوى على الإنترنت بما في ذلك تنظيم المحتوى غير القانوني والضار صعباً للغاية لأن جزءاً من هذا المحتوى قد يكون أكثر وضوحاً أو يمكن التعرف عليه بسهولة مثل الدعاية التي تحرض على العنصرية ونظريات المؤامرة والعنف والتطرف، وقد يكون الكثير من هذا المحتوى أكثر دقة مع ذلك. ركزت المناقشات على المنصة العالمية، وخاصةً الأمم المتحدة[21] ركز إلى حد كبير على تنظيم الدولة للمحتوى عبر الإنترنت حيث لم تعد الآراء المعارضة مسموعة مع استنتاج مفاده أنه بمرور الوقت يمكن أن يقوض هذا الأمر أساس القيم المشتركة والتسامح في المجتمع، ويمزق نسيج الديمقراطية نفسها وذلك نظراً لأن الحكومات في جميع أنحاء العالم تعمل على توطين البيانات بشكل متزايد وتلجأ إلى مراقبة المحتوى الذي ينشئه المستخدمون أو حتى إزالته.

71. وجهت اللجنة العالمية لأخلاقيات المعرفة العلمية والتكنولوجيا (COMEST) الانتباه إلى دور الذكاء الاصطناعي (AI) في اختيار المعلومات والأخبار التي يقرأها الناس والموسيقى التي يستمعون إليها والقرارات التي يتخذونها فضلاً عن تفاعلهم السياسي ومشاركتهم. يكمن وراء هذه النقطة قلق من أن أنظمة الذكاء الاصطناعي التي تستخدمها شركات التكنولوجيا هي "صناديق سوداء" تفتح هوة المعلومات بين شركات التكنولوجيا وأي شخص آخر بما في ذلك صناع السياسات والمنظمون.[22] كان على منظمة الصحة العالمية على سبيل المثال ونتيجةً للاعتماد المتزايد على الموضوعات الشائعة التي يولدها الذكاء

[21] انظر *عصر التبادل الرقمي المتبادل، تقرير الفريق الرفيع المستوى للأمين العام للأمم المتحدة بشأن التعاون الرقمي* (نيويورك، 2019)، الصفحة 17. متاح على: https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf إي سي راتراي، "محو الأمية الإعلامية والمعلوماتية في عصر عدم اليقين"، *وقائع الأمم المتحدة*، 3 كانون الأول / ديسمبر 2020، متاح على: https://www.un.org/en/un-chronicle/media-and-information-literacy-age-uncertainty و"تقرير المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير"، الجمعية العامة للأمم المتحدة، A/HRC/38/35 في 6 نيسان / أبريل 2018.

[22] أورس جاسر وفيرجيليو ايه اف أليميدا، "نموذج متعدد الطبقات لحوكمة الذكاء الاصطناعي"، *معهد مهندسي الكهرباء والإلكترونيات لحوسبة الإنترنت*، المجلد 21، العدد 6 (تشرين الثاني / نوفمبر، كانون الأول / ديسمبر 2017)، الصفحة 58-62، متاح على https://dash.harvard.edu/handle/1/34390353

الاصطناعي محاربة "وباء المعلومات" إلى جانب كوفيد - 19 لأن العديد من الأشخاص المعرضين لخطر الإصابة بالفيروس لم يكونوا على دراية بكمية المعلومات حول الوباء التي كانت غير صحيحة أو مضللة عمداً أو ضارة.

72. أفاد مكتب التحقيقات الفيدرالي في الولايات المتحدة في مثال آخر بحدوث زيادة بمقدار أربعة أضعاف في حجم الاحتيال الالكتروني حيث استفاد المحتالون من الأزمة وقدموا نصائح مزيفة بشأن كوفيد - 19 لحث المستلمين على النقر فوق روابطهم مما سمح لهم بتنزيل البرامج الضارة والوصول إلى المعلومات الشخصية والمالية. تشمل الاهتمامات الأخرى الملحة بشكل متزايد تركيز ملكية المنصات وملايين الأشخاص المتخلفين غير المتصلين أو يفتقرون إلى المهارات الرقمية ليكونوا قادرين على المنافسة وحقيقة أن معظم الأطر التنظيمية لوسائل الإعلام متخلفة الآن كثيراً في العالم الجديد لتسريع التغيير التكنولوجي. لا تزال معظم اللوائح التنظيمية على سبيل المثال تعمل حصرياً على المستوى الوطني على الرغم من أن الشركات المحلية تتنافس الآن مع مزودين أجانب أكبر بكثير وغير منظمين إلى حد كبير. يحتاج المنظمون إلى تبني دور جديد في ضمان أن المواطنين يمكن أن يكتسبوا المعرفة والمهارات اللازمة للاستفادة الكاملة من الموارد الرقمية مع الحماية من المحتوى الخبيث والضار وغير المناسب.[23]

73. يعتبر تقرير عام 2018 للمقرر الخاص للأمم المتحدة المعني بتعزيز وحماية الحق في حرية الرأي والتعبير - الذي الدول والشركات إلى تطبيق القانون الدولي لحقوق الإنسان في جميع مراحل تنظيم المحتوى على الإنترنت: بدءاً من وضع قواعد بشأن المحتوى الذي يجب التخلص منه إلى إجراء العناية الواجبة حول كيفية تأثير التغييرات على المنصات على حقوق الإنسان وتوفير سبل الانتصاف للأشخاص المتضررين من قرارات الاعتدال - أول تقرير للأمم المتحدة لفحص تنظيم المحتوى عبر الإنترنت الذي ينشئه المستخدمون. تأتي هذه الخطوة في مواجهة الزيادة العالمية في الالتزامات التي تفرضها الحكومة لمراقبة وإزالة المحتوى الذي ينشئه المستخدمون. يوصي المقرر الخاص في تقريره بأنه يجب على الدول أن تعتمد تدابير تنظيمية ذكية على الإنترنت وليس تنظيماً صارماً قائماً على وجهة النظر، ويركز على ضمان شفافية الشركة وعلاجها لتمكين الجمهور من اتخاذ خيارات بشأن كيفية المشاركة في المنتديات عبر الإنترنت وما إذا كان ينبغي ذلك أم لا، وأن عليهم الامتناع عن فرض عقوبات غير متناسبة سواءً كانت غرامات باهظة أو سجناً على وسطاء الإنترنت نظراً لتأثيرها المروع على حرية التعبير.[24]

74. الأمر الراسخ والمقبول أن حقوق الإنسان تنطبق على الإنترنت وخارجه. قالت الجمعية العامة للأمم المتحدة إن "نفس الحقوق التي يتمتع بها الأشخاص خارج الإنترنت يجب أن تكون محمية أيضاً على

[23] إي سي راتراي، "محو الأمية الإعلامية والمعلوماتية في عصر عدم اليقين"، *وقائع الأمم المتحدة*، 3 كانون الأول / ديسمبر 2020، متاح على: https://www.un.org/en/un-chronicle/media-and-information-literacy-age-uncertainty

[24] تقرير المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير، الجمعية العامة للأمم المتحدة، A/HRC/38/35 في 6 نيسان / أبريل 2018.

الإنترنت" (وثيقة الأمم المتحدة A/RES/68/167، الفقرة 3) وقد ذكر المقررون الخاصون المعنيون بتعزيز وحماية الحق في حرية الرأي والتعبير بانتظام أن نفس المعايير الدولية لحقوق الإنسان التي تنطبق على أشكال حرية التعبير غير المتصلة بالإنترنت تنطبق بشكل متساوٍ على تقنيات الاتصال الجديدة مثل الإنترنت (راجع، على سبيل المثال، وثيقة الأمم المتحدة A/HRC/17/27، الفقرة 21). لكن هذه البيانات العامة لا تأخذنا حتى الآن إلا عندما يتعلق الأمر بمسألة نطاق الحق في حرية التعبير عبر الإنترنت لا سيما عندما يتعلق الأمر بالمنصات الاجتماعية. تتيح هذه المنصات مجموعة واسعة من أشكال التعبير عبر الإنترنت تتراوح من المحتوى الذي يمكن الوصول إليه عالمياً (مثل التغريدات على تويتر) إلى المحتوى الذي يمكن الوصول إليه فقط لأفراد معينين مسموح لهم (مثل المنشورات على فيسبوك التي يمكن الوصول إليها فقط "للأصدقاء"). هناك أيضاً فرص للمستخدمين الفرديين أنفسهم لتنظيم المحتوى في حين أن المحتوى المنشور عبر هذه الأمثلة يتم تنظيمه من خلال شروط خدمة الشركة (أو معايير المجتمع أو على أي حال). يمكّن فيسبوك الأفراد على سبيل المثال من إنشاء كل من المجموعات المفتوحة والمغلقة والإشراف على المشاركات التي يقوم بها الأعضاء داخل هذه المجموعات، إما عن طريق طلب الموافقة من المسؤول قبل نشر المنشور أو من خلال القدرة على حذف المشاركات التي تم نشرها بالفعل.

75. إذا كانت جميع أشكال التعبير على الإنترنت هذه محمية بموجب الحق في حرية التعبير فإن هذا يثير أسئلة صعبة حول المسؤولية عن ضمان عدم تقييد هذا الحق بطريقة تتعارض مع القانون الدولي لحقوق الإنسان. بما أن الالتزام النهائي بضمان حماية حقوق الإنسان على سبيل المثال يقع على عاتق الدولة، فهل من الضروري أن تشرع الحكومات أو تشرك نفسها بطريقة أخرى في مسائل تنظيم المحتوى من قبل الأفراد الذين يديرون مجموعات وسائل التواصل الاجتماعي الخاصة؟ كما يطرح سؤالاً آخر حول مسؤولية الفرد الذي يمارس حرية التعبير عبر الإنترنت في احترام حقوق الإنسان للآخرين والالتزام بالقوانين واللوائح ذات الصلة. يجب على الحكومات بصفتها جهات تنظيمية للأنشطة عبر الإنترنت ضمان التوازن بين حرية التعبير عبر الإنترنت والمسؤوليات المقابلة للأفراد الذين يمارسون حرية التعبير عبر الإنترنت.

76. بما أنه لا توجد في الوقت الحاضر اتفاقية دولية تنظم المحتوى الضار عبر الإنترنت فإنه يتم التعامل معها على نطاق واسع بموجب التشريعات الوطنية. يعتبر الاختصاص القضائي تحد كبير آخر في تنظيم المحتوى الضار عبر الإنترنت لأن مجرمي الإنترنت ينشئون محتوى على خوادم في الاختصاصات القضائية يكون فيها هذا المحتوى خارج نطاق التنظيم حيث تظل الدول منقسمة بشأن نهج تنظيم المحتوى الضار عبر الإنترنت. هناك حاجة ملحة لوجود لوائح دولية للحد من المحتوى الضار عبر الإنترنت واحتوائه، كما هو الحال مع ظهور التقنيات الجديدة التي تحكم حياتنا اليومية مثل الذكاء الاصطناعي والبلوكتشين فإن تهديد المحتوى الضار عبر الإنترنت يشكل تهديداً للمجتمع الدولي بأسره أكثر من أي

وقت مضى. يعتبر من الضروري أيضاً أثناء ذلك أن تمتنع الدول عن كبح حرية الرأي والتعبير عبر الإنترنت مع تنظيم المحتوى الضار عبر الإنترنت.[25]

(د) الاستخدام السلمي للفضاء السيبراني

77. يجب على المجتمع الدولي أن يراعي المقاصد والمبادئ المنصوص عليها في ميثاق الأمم المتحدة بشكل جدي ولا سيما حظر التهديد أو استخدام القوة والتسوية السلمية للنزاعات من أجل ضمان السلام والأمن في الفضاء السيبراني.

78. تخضع شرعية أي لجوء للدول إلى القوة سواءً من خلال الوسائل الإلكترونية أو الحركية، أولاً لقانون استخدام القوة (أو قانون الحرب) على النحو المبين في ميثاق الأمم المتحدة. يتطلب هذا الأمر من الدول الامتناع عن التهديد أو استخدام القوة مع الحفاظ على حق الدفاع الفردي أو الجماعي عن النفس رداً على هجوم مسلح. يسمح لمجلس الأمن الدولي أيضاً بالموافقة على استخدام القوة للحفاظ على السلم والأمن الدوليين. إن الهدف من القانون الدولي الإنساني أو قانون الحرب الذي ينطبق أثناء نزاع مسلح، من ناحية أخرى هو التخفيف من المعاناة من خلال حماية أولئك الذين لم يشاركوا أو لم يعودوا يشاركون في الأعمال العدائية وعن طريق تقييد وسائل وأساليب الحرب التي قد تستخدمها أطراف النزاعات المسلحة.

79. اعتبرت محكمة العدل الدولية (ICJ) أن المادتين 2(4) و51 من ميثاق الأمم المتحدة فيما يتعلق بحظر التهديد أو استخدام القوة والدفاع عن النفس على التوالي، تنطبقان على "أي استخدام للقوة بغض النظر عن الأسلحة المستخدمة".[26] هناك مع ذلك عدد من القضايا القانونية المرتبطة بتطبيق القانون الدولي على استخدام القوة على الهجمات الإلكترونية.

80. تنص المادة 8 من المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً التي اعتمدتها لجنة القانون الدولي في عام 2001 على أن "سلوك شخص أو مجموعة من الأشخاص يعتبر فعلاً من أعمال

[25] اقترح مكتب المفوض السامي لحقوق الإنسان التابع للأمم المتحدة (OHCHR) لمعالجة معضلات تنظيم وتعديل المحتوى على الإنترنت خمسة إجراءات للدول والشركات للنظر فيها:
أولاً. يحث مكتب المفوض السامي لحقوق الانسان التابع للأمم المتحدة على أن يكون تركيز التنظيم على تحسين عمليات تعديل المحتوى بدلاً من إضافة قيود خاصة بالمحتوى.
يجب أن يتخذ الأشخاص القرارات وليس الخوارزميات عند مواجهة مشكلات معقدة على سبيل المثال.
ثانياً. يجب أن تستند القيود التي تفرضها الدول على القوانين ويجب أن تكون واضحة وضرورية ومتناسبة وغير تمييزية.
ثالثًا. يجب أن تتحلى الشركات بالشفافية بشأن كيفية إنشاء المحتوى وإدارته وكيفية مشاركتهم المعلومات، كما يجب أن تتحلى الدول بالشفافية بشأن طلباتها لتقييد المحتوى أو الوصول إلى بيانات المستخدمين.
رابعاً. يجب أن تتاح للمستخدمين فرص فعالة للطعن في القرارات التي يعتبرونها غير عادلة، ويجب أن يكون للمحاكم المستقلة القول الفصل في قانونية المحتوى.
ينبغي أخيراً إشراك المجتمع المدني والخبراء في تصميم اللوائح وتقييمها.
انظر "الإشراف على المحتوى عبر الإنترنت: محاربة الأذى أو إسكات المعارضة"، مكتب المفوض السامي لحقوق الانسان التابع للمتحدة المتحدة، 23 تموز / يوليو 2021.

[26] رأي استشاري بشأن *الأسلحة النووية، شرعية التهديد بالأسلحة النووية أو استخدامها*، رأي استشاري، 1996 محكمة العدل الدولية 226 (8 تموز / يوليو)، الفقرة 39.

الدولة بموجب القانون الدولي إذا كان الشخص أو مجموعة الأشخاص يتصرفون في الواقع بناءً على تعليمات تلك الدولة أو تحت إشرافها أو سيطرتها في تنفيذ السلوك". عتبة أقل صرامة - تم وضع "السيطرة الشاملة" من قبل المحكمة الجنائية الدولية ليوغوسلافيا السابقة (ICTY) في قضية تاديتش، حيث نصت على أنه يكفي أن يكون للدولة من أجل الإسناد "دور تلعبه في تنظيم أو تنسيق أو تخطيط أعمال المجموعة العسكرية بالإضافة إلى التمويل والتدريب والتجهيز أو تقديم الدعم التشغيلي لتلك المجموعة... بغض النظر عن أي تعليمات محددة من قبل الدولة المسيطرة فيما يتعلق بارتكاب كل من هذه الأفعال".[27] دعا القليل من المعلقين إلى اعتماد اختبار تاديتش في حالات الهجوم الالكتروني نظراً لطبيعته السرية والصعوبة التقنية في تحديد منفذي الهجوم.[28] تنص القاعدة 6 من دليل تالين 1.0 على أن "الدولة تتحمل المسؤولية القانونية الدولية عن العملية الإلكترونية المنسوبة إليها والتي تشكل انتهاكاً لالتزام دولي".[29]

81. هناك مسألة أخرى تتعلق بالطرائق الدقيقة التي تحكم استخدام القوة في حالات الدفاع عن النفس. يجب في هذا السياق التحقق من أنه في ظل أي ظرف يمكن أن ترقى العمليات الالكترونية إلى: أ) فعل غير مشروع دولياً من التهديد أو استخدام القوة. ب) "هجوم مسلح" يبرر اللجوء إلى القوة الضرورية والمتناسبة في "الدفاع عن النفس". تشير القاعدة 11 من دليل تالين 1.0 في هذا الصدد إلى أن "العملية الإلكترونية تشكل استخداماً للقوة عندما يكون نطاقها وتأثيراتها قابلة للمقارنة مع العمليات غير الإلكترونية التي ترتفع إلى مستوى استخدام القوة". من الواضح لذلك أن تطبيق القانون الدولي بشأن استخدام القوة في الفضاء السيبراني ليس بأي حال من الأحوال مهمة مباشرة، ويتطلب المزيد من المداولات بين الدول للتوصل إلى أي توافق في الآراء.

82. تهتم اللجنة الدولية للصليب الأحمر بأي سلاح جديد والعواقب الإنسانية لاستخدامه وتوافقه مع القانون الدولي الإنساني. لقد كانت الهجمات الإلكترونية ضد الأنظمة الانتخابية وأنظمة النقل وشبكات الكهرباء والسدود والمصانع الكيماوية أو النووية ممكنة تقنياً في حين أن الإمكانات العسكرية للفضاء السيبراني ليست مفهومة بالكامل بعد. كان لمثل هذه الهجمات عواقب إنسانية واسعة النطاق. من الضروري لذلك اتخاذ خطوات عملية بهدف توضيح الحدود التي يفرضها القانون الدولي الإنساني بالفعل على اللجوء إلى العمليات الإلكترونية كطريقة أو وسيلة حرب، وكذلك النظر في خطط الطوارئ الإنسانية في حال وقوع مثل هذه الهجمات. تُعرّف اللجنة الدولية للصليب الأحمر الحرب الإلكترونية بأنها عمليات ضد جهاز الحاسوب أو نظام الحاسوب من خلال تدفق بيانات أو رمز حاسوب عند استخدامها كطريقة أو وسيلة حرب في نزاع مسلح.

---

[27] *المدعي العام الخامس*. تاديتش المحكمة الجنائية الدولية الخاصة بيوغوسلافيا السابقة، القضية رقم IT-94-1-A، حكم دائرة الاستئناف، 15 تموز / يوليو 1999، الفقرة 117.

[28] إس. جيه. شاكلفورد، "من الحرب النووية إلى الحرب الشبكية: مقارنة الهجمات الإلكترونية عبر الإنترنت في القانون الدولي"، *مجلة بيركلي للقانون الدولي*، 27 (2009)، الصفحة 192.

[29] دليل تالين 1.0، (صحافة جامعة كامبردج، 2013)، الصفحات 37-38.

83. هناك قيود بموجب القانون الدولي الإنساني عندما تلجأ أطراف النزاع إلى العمليات الالكترونية في حين أن معاهدات القانون الدولي الإنساني لا تحظر صراحةً الحرب الإلكترونية أو تنظمها. تم توضيح هذا الأمر في الالتزام بإجراء مراجعة قانونية للأسلحة الجديدة، لتحديد ما إذا كان استخدامها محظور بموجب القانون الدولي كما هو منصوص عليه في المادة 36 من البروتوكول الإضافي الأول لعام 1977 الملحق باتفاقيات جنيف. تعتبر مثل هذه المراجعات ضرورية بالفعل لضمان امتثال الأسلحة الجديدة للقانون الحالي بما في ذلك قواعد القانون الدولي الإنساني وهذا الأمر على وجه التحديد لأن هذه القواعد تنطبق على الأسلحة الجديدة. لجميع الدول مصلحة في تقييم شرعية الأسلحة الجديدة بغض النظر عما إذا كانت أطرافاً في البروتوكول الإضافي الأول.

84. هناك قلق متزايد في العديد من البلدان بشأن حماية البنية التحتية المدنية الأساسية من الهجمات الإلكترونية. تعتبر المرافق التي توفر مياه الشرب وشبكات الكهرباء التي تخدم السكان المدنيين والبنية التحتية للصحة العامة والسدود والمحطات النووية أهداف مدنية وتتمتع بحماية خاصة بموجب القانون الدولي الإنساني. إن تطبيق القانون الدولي الإنساني على الحرب الإلكترونية يعني أن الهجمات ضد هذه الأمور محظورة.

85. إن تطبيق القانون الدولي الإنساني على الحرب الإلكترونية لا يخلو مع ذلك من التحديات. يتعلق التحدي الأول بربط الفضاء السيبراني بمبادئ التمييز والتناسب المتعلقة بسير الأعمال العدائية. يجب مع ذلك تقييمه لتلبية حظر الهجمات العشوائية وغير المتناسبة وهو التزام بموجب القانون الدولي الإنساني. ثانياً، يشكل مفهوم "الهجوم" وهو أمر أساسي لتطبيق قواعد سير الأعمال العدائية تحدياً كبيراً. تنطبق معظم القواعد المذكورة سابقاً في الواقع على "الهجمات" التي تم تعريفها في البروتوكول الإضافي الأول لعام 1977 على أنها "أعمال عنف ضد الخصم سواءً في الهجوم أو الدفاع". يكمن السؤال في قلب هذه القضية - ما الذي يرقى إلى "عمل من أعمال العنف" في الفضاء السيبراني؟ التحدي الأخير هو إخفاء الهوية في الفضاء السيبراني مما يُعقّد القدرة على عزو الأنشطة العدوانية إلى الجناة. إذا تعذر التعرف على مرتكب الهجوم الالكتروني قد يكون من الصعب تحديد ما إذا كان القانون الدولي الإنساني ينطبق حتى على العملية. يتطلب الأمر بذل المزيد والمزيد من الجهود المتضافرة من قبل الدول للتأكد من انطباق القانون الدولي الإنساني على الفضاء السيبراني وتحديده.

86. ترى دول كثيرة اليوم أن الغرض من دراسة الحرب الإلكترونية هو محاولة وقفها، بما في ذلك سبل ووسائل زيادة الوعي وبناء القدرات داخل الدول ولا سيما في مسألة تحديد التهديدات الالكترونية مقدماً، وليس تشجيع سباق التسلح. إن حقيقة الأمر مع ذلك هي أنه لا يمكن ولا ينبغي السماح بتنفيذ العمليات الإلكترونية في فراغ قانوني. يمكننا ضمان أن يظل الالتزام باحترام القانون الدولي الإنساني متماشياً مع التطورات في تكنولوجيا الحرب فقط من خلال الجهود الجماعية.

رابعاً. ملاحظات وتعليقات الأمانة العامة لمنظمة آلكو

87. تعمل التكنولوجيات الرقمية على إحداث تحولات سريعة في المجتمعات والاقتصادات، حيث تعمل في نفس الوقت على النهوض بالظروف البشرية وخلق تحديات عميقة وغير مسبوقة. إن الهدف النهائي لتطبيق القانون الدولي لتنظيم الفضاء السيبراني في هذا السيناريو هو بلا شك توجيه استخدام التقنيات الرقمية بطريقة يمكن أن تسهم في تحقيق أهداف التنمية المستدامة داخل الدول[30]، من أجل تعظيم الفوائد للمجتمع وتقليل الأضرار.

88. إن التحديات التي يثيرها "العصر الرقمي" الحالي متعددة الأوجه وتتطور بسرعة. يمكن أن تقوض الاتجاهات السلبية في المجال الرقمي الأمن والاستقرار الدوليين، وتضع ضغوطاً على النمو الاقتصادي والتنمية المستدامة وتعوق التمتع الكامل بحقوق الإنسان والحريات الأساسية. تشمل هذه الاتجاهات الاستغلال المتزايد لتكنولوجيا المعلومات والاتصالات لأغراض خبيثة. أبرزت الأزمة الصحية العالمية الحالية الفوائد الأساسية لتكنولوجيا المعلومات والاتصالات واعتمادنا عليها بما في ذلك توفير الخدمات الحكومية الحيوية وإيصال رسائل السلامة العامة الأساسية وتطوير حلول مبتكرة لضمان استمرارية الأعمال وتسريع البحث والمساعدة في الحفاظ على التماسك الاجتماعي من خلال الوسائل الافتراضية. أظهرت جائحة كوفيد - 19 في الوقت نفسه مخاطر وعواقب الأنشطة الخبيثة التي تسعى إلى استغلال نقاط الضعف في الأوقات التي تتعرض فيها المجتمعات لضغوط هائلة. سلطت الضوء أيضاً على ضرورة سد الفجوات الرقمية وبناء المرونة في كل مجتمع وقطاع والحفاظ على نهج محوره الإنسان.

89. هناك حاجة ملحة إلى أن يعمل المواطنون والمجتمع المدني والحكومات والأوساط الأكاديمية والقطاع الخاص معاً بطرق أكثر فعالية وشمولية لمواجهة هذه التحديات. نحن بحاجة ماسة إلى أشكال جديدة من التعاون الرقمي لضمان بناء التقنيات الرقمية على أساس احترام حقوق الإنسان وتوفير فرصة مجدية لجميع الناس والدول.

90. إن معظم الآليات الحالية للتعاون الرقمي هي آليات محلية أو وطنية أو إقليمية في المقام الأول. يستلزم الترابط الرقمي أيضاً مع ذلك أن نعزز آليات التعاون الرقمي العالمي لمواجهة التحديات وتوفير الفرص للجميع. يُعد منتدى إدارة الإنترنت أو IGF حالياً المجال العالمي الرئيسي الذي عقدته الأمم المتحدة لمعالجة قضايا حوكمة الإنترنت والسياسة الرقمية. استضافت الأمم المتحدة الاجتماع السنوي الخامس عشر لمنتدى إدارة الإنترنت في عام 2020 عبر الإنترنت في إطار الموضوع الشامل "الإنترنت من أجل

[30] للحصول على حساب أكثر تفصيلاً للعلاقة المتبادلة بين التعاون الرقمي وتحقيق أهداف التنمية المستدامة، راجع "تعزيز التحول الرقمي والشراكات العالمية: خطوط عمل القمة العالمية لمجتمع المعلومات لتحقيق أهداف التنمية المستدامة"، وثيقة نتائج منتدى القمة العالمية لمجتمع المعلومات 2020، 29 تشرين الأول/ أكتوبر 2020، متاح على:
https://www.itu.int/net4/wsis/forum/2020/Files/outcomes/draft/WSISForum2020_OutcomeDocument_DRAFT-20201204.pdf

صمود الإنسان وتضامنه". تم بناء البرنامج حول أربع مسارات مواضيعية رئيسية: (1) البيانات و(2) البيئة و(3) الشمول و(4) الثقة. كانت إحدى النتائج الرئيسية للاجتماع أن جائحة كوفيد - 19 كشفت أنه على الرغم من أن العديد من الحكومات وكيانات القطاع الخاص لديها أطر عمل وسياسات للبيانات، إلا أنها لم تكن كافية أثناء الأزمة عندما كانت هناك حاجة لمشاركة البيانات في الوقت الفعلي وبحاجة إلى درجة عالية من الدقة. ذكر أيضاً أن الدقة في جمع البيانات لا سيما في أوقات الأزمات لا يجب أن تمس الخصوصية، سواءً كانت الخصوصية الشخصية أو الخصوصية الجماعية للمجتمع. يعد إنشاء الأطر القانونية والأخلاقية لمعالجة المعلومات أمراً حيوياً لتحقيق الشفافية والمساءلة ولمنع التقنيات القائمة على البيانات من تعميق أوجه عدم المساواة القائمة. تدعم هذه الأطر فكرة الموافقة المستنيرة حيث يمكن للأفراد اتخاذ قرارات ذات مغزى بشأن مشاركة البيانات مع العلم أن بياناتهم لن تستخدم لأغراض أخرى غير الأغراض المذكورة. يجب أن تكون فوائد التقنيات القائمة على البيانات إضافةً لذلك في متناول الجميع، ليس فقط للحكومات والقطاع الخاص ولكن أيضاً للمجتمعات والأفراد. يحتاج الناس لتمكين ذلك إلى الوصول إلى الأجهزة الرقمية والاتصال فضلاً عن مهارات محو الأمية الرقمية للاستفادة الكاملة من التقنيات القائمة على البيانات.[31] ستستضيف حكومة بولندا الاجتماع السنوي السادس عشر لمنتدى إدارة الإنترنت في كاتوفيتشي في الفترة من 6 إلى 10 كانون الأول / ديسمبر 2021، تحت الموضوع الشامل: اتحاد الانترنت.

91. أخذت آلكو والدول الأعضاء فيها هذا الموضوع بمنتهى الجدية وذلك اعترافاً بالطبيعة عبر الوطنية للفضاء السيبراني وأهمية إنشاء إطار للحوكمة الالكترونية بما يتفق مع مبادئ القانون الدولي. ركز نهج آلكو بشأن هذا الموضوع على الحاجة إلى توضيح قواعد القانون الدولي بشأن هذا الموضوع مع استكشاف إمكانية زيادة توسيع هذه المعايير في ضوء التطورات التكنولوجية الجديدة مع التشجيع القوي لسلوك الدولة المسؤولة في الفضاء السيبرانية.

92. تحث أمانة آلكو الدول الأعضاء في هذا الصدد على تقديم ردودها على استبيان المقرر في إعداد تقرير المقرر حول "الحاجة الخاصة للدول الأعضاء للتعاون الدولي ضد الجرائم الإلكترونية"، إضافةً إلى "اقتراح الأمين العام للمبادئ الأساسية التوافقية للقانون الدولي المطبقة في الفضاء السيبراني" بحيث تظهر نتيجة ملموسة لمداولات آلكو حول هذا الموضوع.

[31] "مسودة ملخص منتدى حوكمة الانترنت 2020"، منتدى حوكمة الإنترنت - الاجتماع الخامس عشر، 17 تشرين الثاني / نوفمبر 2020، متاح على: https://www.intgovforum.org/multilingual/filedepot_download/10794/2357