اللجنة العالمية
المعنية باستقرار الفضاء السيبراني

تعزيز استقرار الفضاء السيبراني

التقرير النهائي
نوفمبر 2019

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

تعزيز الاستقرار في الفضاء السيبراني من أجل بناء السلام والازدهار

ستضع اللجنة العالمية المعنية باستقرار الفضاء السيبراني (GCSC) مقترحات بشأن القواعد والسياسات لكي يتم تعزيز الأمن والاستقرار الدوليين وتوجيه السلوكيات المسؤولة الحكومية وغير الحكومية المتبعة في الفضاء السيبراني.

www.cyberstability.org
info@cyberstability.org | cyber@hcss.nl
theGCSC@

تعزيز
استقرار الفضاء السيبراني

التقرير النهائي
نوفمبر 2019

معهد إيست ويست
نيويورك | بروكسل
موسكو | سان فرانسيسكو

cyber@eastwest.ngo
www.eastwest.ngo

مركز لاهاي للدراسات الاستراتيجية
Lange Voorhout 1
2514 EA The Hague

info@hcss.nl
www.hcss.nl

الرؤساء

مايكل تشيرتوف الولايات المتحدة الأمريكية
لاتا ريدي الهند
مارينا كالجوراند إستونيا *(الرئيس السابق)*

المفوضون

عبد الحكيم أجيجولا نيجيريا
فيرجيليو
ألميدا البرازيل
إسحاق بن إسرائيل إسرائيل
سكوت تشارني الولايات المتحدة الأمريكية
فريديريك دوزيت فرنسا
أنرييت إسترهويسن جنوب أفريقيا
جين هول لوت الولايات المتحدة الأمريكية
نايجل إنكستر المملكة المتحدة
خو بوون هوي سنغافورة
وولفجانج كلانفيجتر ألمانيا
أولاف كولكمان هولندا
لي شياو دونغ الصين
جيمس لويس الولايات المتحدة الأمريكية
جيف موس الولايات المتحدة الأمريكية
إلينا نور ماليزيا
جوزيف صمونيل ناي، الابن الولايات المتحدة الأمريكية
كريستوفر بينتر الولايات المتحدة الأمريكية
أور روزنتال هولندا

إيليا ساتشكوف روسيا
سمير ساران الهند
ماريبيت شاك هولندا
موتوهيرو توشيا اليابان
بيل ودكوك الولايات المتحدة الأمريكية
زهانغ لي الصين
جوناثان زيتراين الولايات المتحدة الأمريكية

الممثلون والمستشارون الخاصون

كارل بيلت السويد
فينت سيرف الولايات المتحدة الأمريكية
سورين دوكارو رومانيا
مارثا فينيمور الولايات المتحدة الأمريكية

المديرون

ألكسندر كليمبورغ النمسا
بروس دبليو ماكونيل الولايات المتحدة الأمريكية

رؤساء مجموعة البحوث الاستشارية

شون كانوك الولايات المتحدة الأمريكية
كويتيرو كوميامـا اليابان
ماريليا ماسيل البرازيل
ليز فيهول إستونيا
هوغو زيلبرج فرنسا

الأمانة العامة

The Hague Centre for Strategic Studies

EastWest INSTITUTE

الشركاء

CSA SINGAPORE

Ministry of Foreign Affairs of the Netherlands

Internet Society

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

Afilias

Microsoft

الجهات الراعية

الإدارة الاتحادية للشؤون الخارجية السويسرية
منظمة جلوبسيك
وزارة الخارجية الإستونية
وزارة الشؤون الداخلية والاتصالات اليابانية

الجهات الداعمة

مفوضية الاتحاد الأفريقي
بلاك هات أمريكا
ديف كون
وفد الاتحاد الأوروبي إلى الأمم المتحدة بجنيف
المنتدى العالمي للخبرات السيبرانية
Google
بلدية لاهاي
منظمة باكيت كليرينج هاوس
جامعة تل أبيب
معهد الأمم المتحدة لبحوث نزع السلاح

المحتويات

رسالة موجهة من الرؤساء

يمثل الفضاء السيبراني أحد أكبر الاختراعات للبشرية، إذ أنه يعيد صياغة العلاقات الشخصية والاجتماعية والتجارية والسياسية. ولسوء الحظ، فإن هناك حاجة إلى اتخاذ إجراء عاجل لضمان استقرار الفضاء السيبراني وذلك بسبب الهجمات التي تُشن عليه ومن خلاله. ويتطلب مفهوم استقرار الفضاء السيبراني، مثله مثل الاستقرار الدولي، صياغة رؤية مشتركة تدرك من خلالها جميع الأطراف أنه يجب إدارة الخلافات والتغيرات الجيوسياسية التي تؤثر على الفضاء السيبراني بسلام نسبي، وأنه يجب ضمان استقرار الفضاء السيبراني.

بدأت اللجنة العالمية المعنية باستقرار الفضاء السيبراني عملها على اقتناع بأنه لم يعد من الممكن معالجة قضية كانت في العادة حكرًا على بعض الدول - السلم والأمن الدوليين - دون إشراك الجهات المعنية الأخرى. فالفضاء السيبراني هو بيئة متعددة الجهات المعنية: من المرجح أن تكون الجهات التي تبني الفضاء السيبراني وتديره، والجهات التي تتصدى للهجمات التي تُشن على الفضاء السيبراني ومن خلاله، جهات فاعلة غير حكومية وليس فقط مسؤولين حكوميين. وجرى اختيار المفوضين لدينا للتعبير عن هذه الميزة، حيث تضمنت صفوفنا، إلى جانب كبار المسؤولين الحكوميين السابقين من ذوي الخبرة في قضايا الأمن الدولي، قادة معترف بهم في مجالات إدارة الإنترنت ومجتمعات حقوق الإنسان والتنمية والتكنولوجيا والصناعة. وقام مفوضونا البالغ عددهم 28 مفوضًا من 16 دولة بتوفير مجموعة واسعة من الخبرات والآراء، وقد استفادوا من التعليقات العامة التي وردت استجابة لأنشطة التوعية التي قامت بها اللجنة.

يعد التقرير النهائي ثمرة جهد متواصل للجنة دام لمدة ثلاث سنوات. لذا، فإننا نعرب عن امتناننا للأشخاص الذين جعلوا هذا الأمر ممكنًا: المفوضون والمستشارون والباحثون لدينا (العديد منهم متطوعون أيضًا)، وجهات الدعم المالي، ومجلس الإدارة لدينا. وأخيرًا، نعرب عن تقديرنا للأمانة العامة، التي لم تدير العملية بحذاقة فحسب، بل كانت تلعب دورًا جوهريًا في إنشاء اللجنة كمبادرة للمجتمع المدني.

ظلت اللجنة طيلة عملها مدركة لمبادرات الفضاء الإلكتروني الأخرى، سواء في الماضي أو الحاضر. يُعد تقريرنا—*تعزيز استقرار الفضاء الإلكتروني*—جزءًا مكملًا لعمل الآخرين ومعززًا له، بالإضافة إلى تقديم أفكار جديدة لتعزيز استقرار الفضاء السيبراني.

مايكل تشيرتوف
الرئيس المشارك
اللجنة العالمية المعنية باستقرار
الفضاء السيبراني

لاثا ريدي
الرئيس المشارك
اللجنة العالمية المعنية باستقرار
الفضاء السيبراني

الملخص التنفيذي

لقد استكملنا فترة خمس وعشرين سنة من الاستقرار الإستراتيجي والسلام النسبي بين القوى الكبرى، وقد اتخذ الصراع بين الدول أشكالًا جديدة، ومن المرجح أن تلعب الأنشطة السيبرانية دورًا رائدًا في هذه البيئة الجديدة المضطربة. فعلى مدى العقد الماضي، ازداد عدد الهجمات السيبرانية التي شنتها الجهات الحكومية وغير الحكومية كما ازدادت درجة تطورها، الأمر الذي يهدد استقرار الفضاء السيبراني. وببساطة، ربما لم يعد الأشخاص والمنظمات على ثقةمن قدرتهم على استخدام الفضاء السيبراني بطريقة آمنة ومأمونة، أو ربما لا يشعرون بالطمأنينة إزاء توفر الخدمات والمعلومات وتكاملها.

وانطلاقًا من هذه الخلفية، أُنشئت اللجنة العالمية المعنية باستقرار الفضاء السيبراني (GCSC) لتقديم توصيات لتعزيز استقرار الفضاء السيبراني. وقد بدأنا بتحديد إطار عمل استقرار الفضاء السيبراني المكون من سبعة عناصر. ويشمل هذا الإطار ما يلي: (1) إشراك الجهات المعنية المتعددة؛ (2) ومبادئ استقرار الفضاء السيبراني؛ (3) ووضع القواعد الطوعية وتنفيذها؛ (4) والالتزام بالقانون الدولي؛ (5) وتدابير بناء الثقة؛ (6) وبناء القدرات؛ (7) وإصدار المعايير التقنية التي تضمن مرونة الفضاء السيبراني واستخدامها على نطاق واسع. وقامت اللجنة بعد تحديد هذا الإطار بإجراء دراسة متعمقة لثلاثة من عناصره، ألا وهي إشراك الجهات المعنية المتعددة والمبادئ والقواعد.

هناك حاجة إلى إشراك الجهات المعنية المتعددة في العديد من الاتفاقيات الدولية، ورغم هذا فإن الأمر لا يزال موضع نزاع، حيث يواصل البعض الاعتقاد بأن ضمان الأمن والاستقرار الدوليين يقع على عاتق الدول بشكل شبه تام. ومع ذلك، من الناحية العملية، جرى تصميم ساحة المعركة السيبرانية (أي الفضاء السيبراني) ونشرها وتشغيلها بشكل أساسي من قبل الجهات الفاعلة غير الحكومية، ونعتقد أن مشاركتهم ضرورية لضمان استقرار الفضاء السيبراني. وعلاوة على ذلك، فإن مشاركتهم أمر حتمي، إذ أنه غالبًا ما تكون الجهات الفاعلة غير الحكومية أول من يرد على الهجمات السيبرانية - بل ويعزوها إلى فاعلها.

خلصت اللجنة إلى أن هذه الجهات الفاعلة غير الحكومية لم تلعب دورًا بالغ الأهمية لضمان استقرار الفضاء السيبراني فحسب، بل لا بد أيضًا أن تسترشد بالمبادئ وأن تلتزم بالقواعد. وتعكس المبادئ الأربعة التالية وجهة النظر المذكورة، حيث تناشد جميع الأطراف لتحمل المسؤولية والتقييد واتخاذ الإجراءات واحترام حقوق الإنسان:

- المسؤولية: كل فرد مسؤول عن ضمان استقرار الفضاء السيبراني.
- التقييد: يجب على الجهات الحكومية وغير الحكومية عدم اتخاذ إجراءات من شأنها أن تضعف استقرار الفضاء السيبراني.
- الحاجة إلى التصرف: يجب على الجهات الحكومية وغير الحكومية اتخاذ خطوات معقولة ومناسبة لضمان استقرار الفضاء السيبراني.
- احترام حقوق الإنسان: يجب أن تراعي الجهود المبذولة لضمان استقرار الفضاء السيبراني حقوق الإنسان وسيادة القانون.

استنادًا إلى هذه المبادئ، والسعي إلى تكملة عمل الآخرين وعدم تكراره، وضعت اللجنة ثمانية قواعد مصممة لضمان استقرار الفضاء السيبراني بشكل أفضل ومعالجة المخاوف أو الثغرات التقنية في القواعد المعلنة سابقًا:

1. تلتزم الجهات الحكومية وغير الحكومية بعدم القيام بأي نشاط من شأنه أن يضر التوافر العام أو الأساس العام للإنترنت، وبالتالي استقرار الفضاء السيبراني، عن قصد أو بشكل ملموس أو السماح بذلك عن علم.
2. تلتزم الجهات الحكومية وغير الحكومية بعدم السعي إلى العمليات السيبرانية التي تهدف إلى تعطيل البنية التحتية التقنية اللازمة لإجراء الانتخابات أو الاستفتاءات أو دعمها أو السماح بها.
3. تلتزم الجهات الحكومية وغير الحكومية بعدم العبث بالمنتجات والخدمات في التطوير والإنتاج، أو السماح بالعبث بها، إذا كان القيام بذلك قد يضعف استقرار الفضاء الإلكتروني على نحوٍ كبير.

4. تلتزم الجهات الحكومية وغير الحكومية بعدم الاستحواذ على موارد تقنية المعلومات والاتصالات الخاصة بعامة الجمهور من أجل استخدامها كشبكات روبوت أو لأغراض مماثلة.

5. تلتزم الدول بإنشاء أطر عمل شفافة من الناحية الإجرائية لتقييم ما إذا كان ينبغي الكشف عن مواطن الضعف أو العيوب غير المعروفة علنًا التي تدركها في نظم وتكنولوجيا المعلومات ومتى ينبغي ذلك. وينبغي أن يكون الافتراض الوارد مؤيدًا لقرار الإفصاح.

6. تلتزم الجهات المطورة والجهات المنتجة للمنتجات والخدمات التي يعتمد عليها استقرار الفضاء السيبراني (1) بإعطاء الأولوية للأمن والاستقرار، (2) واتخاذ خطوات معقولة لضمان خلو منتجاتها أو خدماتها من مواطن الضعف الكبيرة، (3) واتخاذ التدابير اللازمة في الوقت المناسب للتخفيف من مواطن الضعف التي تم اكتشافها لاحقًا والتحلي بالشفافية بشأن عملياتها. وتلتزم جميع الجهات الفاعلة بمشاركة المعلومات المتعلقة بمواطن الضعف بهدف المساعدة في منع النشاط السيبراني الخبيث أو الحد منه.

7. تلتزم الدول باتخاذ التدابير المناسبة، بما في ذلك القوانين واللوائح، لضمان السلامة السيبرانية الأساسية.

8. تلتزم الجهات غير الحكومية بعدم المشاركة في العمليات السيبرانية الهجومية وتلتزم الجهات الحكومية بمنع مثل هذه الأنشطة والاستجابة لها في حالة حدوثها.

التوصيات

تقوم اللجنة في نهاية المطاف بتقديم ست توصيات تركز على تعزيز نموذج الجهات المعنية المتعددة، والتشجيع على اعتماد القواعد وتنفيذها، وضمان خضوع الجهات التي تنتهك القواعد والمعايير للمساءلة، وذلك إدراكًا منها لأهمية إشراك الجهات المعنية المتعددة وحقيقة أن مجرد الإعلان عن القواعد السلوكية لا يجدي النفع المفترض به.

وتوصي اللجنة على وجه التحديد بما يلي:

1. تتبنى الجهات الحكومية وغير الحكومية وتنفذ القواعد التي تعزز استقرار الفضاء السيبراني من خلال تعزيز مبدأ التقييد وتشجيع العمل.

2. تتصدى الجهات الحكومية وغير الحكومية، بما يتفق مع مسؤولياتها وحدودها، لانتهاكات القواعد على النحو المناسب، مما يضمن تلقي الجهات التي تنتهك القواعد لعواقب وخيمة يمكن التنبؤ بها.

3. تبذل الجهات الحكومية وغير الحكومية، بما في ذلك المؤسسات الدولية، المزيد من الجهود الرامية إلى تدريب الموظفين، وبناء القدرات والإمكانيات، وتعزيز الفهم المتبادل لأهمية استقرار الفضاء السيبراني، ومراعاة الاحتياجات المتباينة لمختلف الأطراف.

4. تعمل الجهات الحكومية وغير الحكومية على جمع المعلومات المتعلقة بانتهاكات القواعد وتأثير هذه الأنشطة ومشاركتها ومراجعتها ونشرها.

5. تحرص الجهات الحكومية وغير الحكومية على تأسيس المجتمعات ذات المصالح ودعمها للمساعدة في ضمان استقرار الفضاء السيبراني.

6. يتم إنشاء آلية مشاركة متعددة الجهات المعنية الدائمة لمعالجة القضايا المتعلقة بالاستقرار، حيث يتم إشراك الدول والقطاع الخاص (بما في ذلك كالمجتمع التقني) والمجتمع المدني والتشاور معها على نحوٍ ملائم.

يمثل نشر هذا التقرير نهاية مرحلة الكتابة والتخطيط وبداية مرحلة السعي والتنفيذ. وقد أنجزت اللجنة المهام المسندة إليها. لذا، يتعين على أعضاء اللجنة العالمية المعنية باستقرار الفضاء السيبراني ومؤيديها، بالإضافة إلى جميع الجهات التي تدعم أهدافها بدء مرحلة العمل الشاق المطلوب لتنفيذ هذه المبادئ والقواعد والتوصيات للتو، إذ يعد بدء التنفيذ أمرًا بالغ الأهمية، حيث ستضيع فوائد الفضاء السيبراني في حالة عدم ضمان استقراره.

1. مقدمة

لقد أدى التطور الرقمي والفضاء السيبراني إلى تغيير العالم المعاصر للبشر تغييرًا كبيرًا،[1] لقد كان للقدرة على رقمنة البيانات وتخزينها وتحليلها ونقلها حول العالم تأثيرات عميقة في كل قطاع من قطاعات المجتمع، الأمر الذي أدى إلى تغيير الطريقة التي ندير بها الشؤون الشخصية والتجارية والسياسية. اليوم، أصبح أكثر من ما يقرب من نصف سكان العالم يستخدمون الإنترنت[2] وهذا الرقم في تزايد مستمر. ولكن حتى الأشخاص الذين لا يستخدمون الفضاء السيبراني بشكل شخصي يتأثرون بمدى وصوله، نظرًا لأن الكيانات التي يعتمدون عليها لتوفير السلع والخدمات غالبًا ما تستخدم الفضاء السيبراني للاتصالات والخدمات اللوجستية والتمويل.

غالبًا ما تمت مناقشة الأمور المتعلقة بمزايا الفضاء السيبراني - والحاجة إلى ضمان استقراره - وكذلك تحدياته. وعلى رأس هذه الأمور دعم الفضاء السيبراني للأهداف النبيلة والخسيسة على حدٍ سواء. فعلى سبيل المثال، يسمح الاتصال العالمي، وعدم الإفصاح عن الهوية، وعدم إمكانية التتبع للأفراد والآلات بالاتصال بالبيانات والأنظمة دون تأكيد الهوية، وهذا يمكن المجرمين أيضًا من الاستفادة من هذه السمات لارتكاب الجرائم والإفلات من العقاب. ونتيجة لذلك، تواجه الحكومات والشركات والأشخاص في جميع أنحاء العالم الكثير من المعضلات، حيث تهتم الحكومات بحماية الفضاء السيبراني وتقديم الخدمات العامة وتعزيز الأنشطة المهمة الأخرى (مثل التعليم والخدمات المصرفية عبر الإنترنت) وكذلك تعزيز مصالح الأمن القومي، بما في ذلك إنفاذ القانون والاستخبارات والقدرات العسكرية، كما تجد الشركات، المهتمة بحماية عملائها وسمعتها وأرباحها، نفسها تتعرض للهجوم و/أو التحقيق في الأنشطة الخبيثة و/أو الخضوع لطلبات البيانات الحكومية. ويعتمد الأشخاص بشكل متزايد على التكنولوجيا الرقمية وتبنيها - سواء بشكل مباشر أو غير مباشر، لكنهم يشعرون بالقلق إزاء استمرار توفرها وسلامتها. وعلى مدى العقد الماضي، ازداد عدد الهجمات السيبرانية ودرجة تعقيدها، بما في ذلك الهجمات على الأنظمة الحكومية والبنى التحتية الحيوية.[3] وعلى هذا النحو، فإن الوضع الراهن والاتجاهات الملحوظة لا تبعث على التفاؤل.

توضح الهجمات السيبرانية، التي تشنها الجهات الحكومية وغير الحكومية، أن العالم يحتاج إلى إطار استقرار سيبراني، إذ سيعمل مثل هذا الإطار على تقليل احتمالات حدوث اضطرابات كبيرة في الفضاء السيبراني من شأنها تقويض فوائده وتقليل رفاهية الأشخاص، بما في ذلك حقوقهم وحرياتهم. وبات من الواضح أن المنتجات والخدمات جيدة التصميم وقوية البنية، والتي تدار بشكل جيد من قِبَل المهنيين العاملين في مجال تقنية المعلومات ومستخدمي الكمبيوتر، ستزيد من الأمن والاستقرار، ولكن، على الجانب الآخر، ستعمل المنتجات والخدمات سيئة التصميم، أو الممارسات

1 عُرِّف "الفضاء السيبراني" بطرق مختلفة. https://ar.wikipedia.org/wiki/Cyberspace. ينص تعريف القاموس على أنه "نظام إلكتروني يسمح لمستخدمي الكمبيوتر حول العالم بالتواصل مع بعضهم البعض أو الوصول إلى المعلومات لأي غرض." https://dictionary.cambridge.org/us/dictionary/arabic/cyberspace. وفقًا للمملكة المتحدة، "الفضاء السيبراني هو المصطلح المستخدم لوصف الوسيط الإلكتروني للشبكات الرقمية المستخدمة في تخزين المعلومات وتعديلها وإيصالها. وهو يشمل الإنترنت ولكن أنظمة المعلومات الأخرى التي تدعم الأعمال التجارية والبنية التحتية والخدمات كذلك". https://www.cpni.gov.uk/cyber. على هذا النحو، يمكن القول أنه مصطلح أوسع من الإنترنت، الذي يوصف بمصطلحات شائعة بأنه "نظام عالمي لشبكات الكمبيوتر المترابطة التي تستخدم مجموعة بروتوكول الإنترنت (TCP/IP) لربط الأجهزة في جميع أنحاء العالم." انظر https://en.wikipedia.org/wiki/Internet. انظر أيضًا ورقة نقاش الاتحاد الدولي للاتصالات، بعنوان "تعريف الإنترنت"، (مايو 2013)، https://www.itu.int/dms_pub/itu-s/md/13/wtpf13/inf/S13-WTPF13-INF-0008%21%21MSW-E.docx.

2 "إحصائيات استخدام الإنترنت"، إحصائيات عالم الإنترنت، آخر تعديل في 4 أكتوبر 2019، https://internetworldstats.com/stats.htm.

3 مركز الدراسات الدولية والإستراتيجية (CSIS)، *الحوادث السيبرانية الكبرى منذ عام 2006*، https://csis-prod.s3.amazonaws.com/s3fs-public/190904_Significant_Cyber_Events_List.pdf؛ المحرران لويس مارينوس وماركو لورينسو، *تقرير وكالة الاتحاد الأوروبي للأمن السيبراني بشأن ساحة التهديدات لعام 2018*, ENISA (يناير 2019)، https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018؛ أبهيشيك أغراوال وآخرون، *تقرير التحليل الذكي لخدمات الأمان من مايكروسوفت*، المجلد 24 (ديسمبر 2018)، https://clouddamcdnprodep.azureedge.net/gdc/gdc09FrGq/original؛ الجمعية العامة للأمم المتحدة *التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي: تقرير الأمين العام*، A/74/120 (24 يونيو 2019)، https://undocs.org/A/74/120.

التشغيلية السيئة أو المتهاونة، على تقويضهما. لكن تعزيز التطوير وتحسين العمليات لن يكون أمرًا كافيًا، خاصةً مع رؤية الجهات الحكومية وغير الحكومية للفضاء الإلكتروني على أنه ساحة معركة يمكن للمرء فيها تحقيق ميزة سياسية أو عسكرية أو اقتصادية. ويمكن للمهاجم المثابر إحباط التدابير الأمنية والعمل بالمثل السائر القائل "الهجوم خير وسيلة للدفاع على الإنترنت" وخلق عدم الاستقرار[4] وبالتالي، يجب عدم التركيز على التكنولوجيا فحسب ولكن على السلوكيات أيضًا: كيف نشجع جميع الجهات الفاعلة على التصرف بطرق مسؤولة تعزز استقرار الفضاء السيبراني - ولا تهدده؟

للمساعدة في الإجابة عن هذا السؤال، قدمت العديد من الكيانات الحكومية وغير الحكومية الدعم اللازم لإنشاء اللجنة العالمية المعنية باستقرار الفضاء السيبراني (GCSC)،[5] مشيرة إلى ما يلي:

> لقد استكملنا فترة خمس وعشرين سنة من الاستقرار الإستراتيجي والسلام النسبي بين القوى الكبرى، حيث سيتخذ الصراع بين الدول أشكالًا جديدة، ومن المرجح أن تلعب الأنشطة السيبرانية دورًا رائدًا في هذه البيئة الجديدة المضطربة، مما يزيد من خطر تقويض الاستخدام السلمي للفضاء السيبراني لتسهيل النمو الاقتصادي وتوسيع نطاق الحريات الفردية.

لمواجهة هذه التطورات، ستضع اللجنة العالمية المعنية باستقرار الفضاء السيبراني مقترحات بشأن القواعد والسياسات بهدف تعزيز الأمن والاستقرار الدوليين وتوجيه السلوكيات المسؤولة الحكومية وغير الحكومية المتبعة في الفضاء السيبراني. وستعمل اللجنة العالمية المعنية باستقرار الفضاء السيبراني على إشراك المجموعة الكاملة من الجهات المعنية للتوصل إلى فهم مشترك، وسيساعد عملها على تعزيز الاستقرار السيبراني من خلال دعم تبادل المعلومات وبناء القدرات والبحوث الأساسية والدعوة.[6]

تجدر الإشارة إلى أن اللجنة نفسها متعددة الجهات المعنية وعالمية لأنها تتألف من أفراد ينتمون إلى خلفيات مختلفة ويتمتعون بخبرات متنوعة. وقد شغل بعض المفوضين مناصب حكومية وشاركوا في مفاوضات ثنائية ومتعددة الأطراف حول قضايا الإنترنت، بينما يتمتع البعض الآخر بخبرة في بناء شبكة الإنترنت وصيانتها وحمايتها. وقد عمل آخرون كممثلين في المجتمع المدني.

إن اللجنة لا تعمل بمعزل عمن حولها، وقد سعت اللجنة العالمية المعنية باستقرار الفضاء السيبراني من منطلق إدراكها أن العديد من المؤسسات والعمليات الأخرى (الماضية والحالية) تشاركها اهتمامها باستقرار الفضاء السيبراني، إلى عدم تكرار العمل الذي ينجزه الآخرون. وبدلًا من ذلك، تحاول اللجنة العالمية المعنية باستقرار الفضاء السيبراني الاستناد إلى العمليات الأخرى للجهات المعنية المتعددة والحكومة والتأثير على الأعمال المستقبلية. وتشمل هذه العمليات العمل التأسيسي والمستمر لفريق الخبراء

4 راجع، على سبيل المثال، بي دبليو سنغر وألان فريدمان، "طائفة الهجوم السيبراني،" *فورين بوليسي* (15 يناير 2014)، https:// foreignpolicy.com/2014/01/15/cult-of-the-cyber-offensive/؛ المنتدى الاقتصادي العالمي (WEF)، *تقرير المخاطر العالمية لعام 2019*، (2019)، http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf.

5 لمزيد من المعلومات حول اللجنة العالمية المعنية باستقرار الفضاء السيبراني، راجع الملحق ج: تاريخ اللجنة العالمية المعنية باستقرار الفضاء السيبراني وأهدافها والعمليات الخاصة بها.

6 اللجنة العالمية المعنية باستقرار الفضاء السيبراني، https:// cyberstability.org/.

7 في قرار مهم، في عام 2015 أكدت الجمعية العامة للأمم المتحدة بالإجماع على استنتاج فريق الخبراء الحكوميين التابع للأمم المتحدة. راجع قرار الجمعية العامة 70/237، *القرار المعتمد من الجمعية العامة في 23 ديسمبر 2015 [بشأن تقرير اللجنة الأولى (A/70/455)]*، https://undocs.org/ar/A/RES/70/237. وهكذا، يضع القانون الدولي وعلى وجه الخصوص، ميثاق الأمم المتحدة إطارًا حصريًا للتصدي على المستوى الدولي للأفعال العدائية ينطبق أيضًا على العمليات التشغيلية السيبرانية. يستند عملنا إلى اتفاق جميع الدول في الجمعية العامة للأمم المتحدة لعام 2015 على الاسترشاد بقواعد السلوك المسؤول لزيادة الاستقرار والأمن في استخدام تقنيات المعلومات والاتصالات والوفاء بالتزاماتها بموجب القانون الدولي بشأن العناية الواجبة والتعاون.

الحكوميين التابع للأمم المتحدة (UN GGE)[7]، وعمل الفريق العامل المفتوح العضوية (UN OEWG)، بالإضافة إلى المنتدى العالمي للخبرات السيبرانية (GFCE)،[8] والقمة العالمية لمجتمع المعلومات (WSIS)، واللجنة العالمية المعنية بحوكمة الإنترنت (لجنة بيليت)، ومنتدى حوكمة الإنترنت (IGF)، المؤتمر العالمي المعني بالفضاء السيبراني (GCCS/ عملية لندن)، ومبادرة NETmundial، ومنظمة الأمن والتعاون في أوروبا (OSCE)، ومفوضية الاتحاد الأفريقي (AUC)، وميثاق الثقة، واتفاقية Cybersecurity Tech Accord، وبرنامج لاهاي بشأن القواعد السيبرانية، ومعهد الأمم المتحدة لبحوث نزع السلاح (UNIDIR)، ودعوة باريس من أجل الثقة والأمن في الفضاء السيبراني ("دعوة باريس")، والفريق الرفيع المستوى المعني بالتعاون الرقمي التابع للأمين العام للأمم المتحدة. كذلك يسترشد عمل اللجنة بالبحوث المكلف بها وطلبات التعليقات العامة.

ركزت بعض الجهود المذكورة، بشكل جزئي، على استقرار الفضاء السيبراني، وأعربت عن قلقها بشأن الارتباط الوثيق بين استقرار الفضاء السيبراني والحوكمة. مما يعني أنه في غياب نموذج حوكمة قوي، يفتقر المجتمع إلى التفاعلات وعمليات صنع القرار اللازمة لضمان الاستقرار. على سبيل المثال، اقترحت لجنة بيلت ميثاقًا اجتماعيًا للجهات المعنية المتعددة فيما يتعلق بالخصوصية والأمن الرقميين "بين المواطنين وممثليهم المنتخبين، والسلطة القضائية، ووكالات إنفاذ القانون والاستخبارات، والأعمال التجارية، والمجتمع المدني، والمجتمع التقني على الإنترنت، بهدف استعادة الطمأنينة وتعزيز الثقة بشأن الإنترنت".[9]

ونحن نشيد بهذه الجهود السابقة في صياغة المبادئ والقواعد والأعراف لتطبيقها على السلوك في المجال الجديد المضطرب للفضاء السيبراني ونعتقد أن يلزم وجود إطار شامل لزيادة استقرار الفضاء السيبراني. يُظهر السجل التاريخي أن المجتمعات والحكومات قد تستغرق في بعض الحالات عقودًا لتطوير هياكل حوكمة دولية رسمية واسعة النطاق لتقنيات كاسحة جديدة مهمة.[10] ويرجع ظهور الفضاء السيبراني كبُعد حاسم للاعتماد المتبادل الاقتصادي والاجتماعي والأمني العالمي إلى أواخر التسعينات، عندما بدأ الاستخدام الواسع لشبكة الويب العالمية. وبالتالي، فإن عمليات الحوكمة المتطورة لا تزال في مرحلة مبكرة حيث تتواجد مجالات الاتساق وعدم الاتساق المعياري بجانب بعضها البعض.[11] على سبيل المثال، بينما تكون القواعد والقوانين ذات الصلة بنظام أسماء النطاقات متطورة جيدًا، هناك مجالات خلاف كبرى بين الدول وبين الشركات ذات الصلة بتنظيم المحتوى. في بعض الأحيان، تطبق الجهات الفاعلة الرسمية وغير الرسمية قواعد من أنظمة أخرى مثل الملكية الفكرية والتجارة وبشكل متزايد تضع الشركات الخاصة بنفسها القواعد.[12] ولا يتمثل الغرض من لجنتنا في تدبر هذه المسائل المختلفة بشأن الحوكمة، لكن في وضعها داخل إطار عام لضمان استقرار الفضاء السيبراني.

كذلك نلاحظ أن أولئك المعنيين باستقرار الفضاء السيبراني كافحوا لمواكبة أولئك الذين يسعون إلى تقويضه، بالإضافة إلى مواكبة التطورات التقنية وتطور الصراعات الجيوسياسية. ويكون جزء من التحدي هو أن الفضاء السيبراني قد غيّر الطريقة التي تسعى بها الجهات الفاعلة إلى تحقيق أهداف سياسية وعسكرية؛ فمع انخفاض حواجز الدخول، تقل صعوبة التحول إلى قوة سيبرانية عن قوة عسكرية تقليدية. بالإضافة إلى ذلك، مع وجود التقنية الجديدة في مجموعات الأدوات الخاصة بها، يتردد البعض في اعتماد قيود، خاصة إذا لم يتم احترام هذه القيود على نطاق واسع. والمطلوب هو إطار شامل للاستقرار السيبراني من أجل المجتمع الدولي، إطار يعزز من استقرار الفضاء السيبراني ولكنه يظل مفيدًا مع استمرار وتيرة التغير التقني في الازدياد. لذلك نبدأ بتحديد الهدف الأساسي: حماية استقرار الفضاء السيبراني.

8 كان المنتدى العالمي للخبرات السيبرانية فعالًا بشكل خاص في بناء القدرات. راجع، على سبيل المثال، "بيان دلهي حول برنامج عالمي لبناء القدرات السيبرانية للمنتدى العالمي للخبرات السيبرانية"، المنتدى العالمي للخبرات السيبرانية (24 نوفمبر 2017)، https://www.thegfce.com/delhi-communique/documents/publications/2017/11/24/delhi-communique.

9 اللجنة العالمية لحوكمة الإنترنت، تقرير *إنترنت واحد (One Internet)* (2016)، ص. IX، https://www.cigionline.org/sites/default/files/gcig_ final_ report_-_with_cover.pdf. "إننا ندعو الحكومات والشركات الخاصة والمجتمع المدني والمجتمع التقني والأفراد إلى وضع ميثاق اجتماعي جديد للعصر الرقمي".

10 ولعل المثال الأكثر صلة بهيكل حوكمة من هذا القبيل يرتبط بالأسلحة النووية، والذي استغرق وقتًا وجهدًا كبيرًا لإنشائه. وحتى الآن، بعد مرور 60 سنة على معاهدة عدم انتشار الأسلحة النووية (NPT)، ما زالت حوكمة الأسلحة النووية تشكل مصدر قلق أمني.

11 لقد أُطلق على هذه المرحلة المبكرة مصطلح "مجموعة الأنظمة". راجع جوزيف ناي، "مجموعة أنظمة إدارة الأنشطة السيبرانية العالمية المعقدة،" اللجنة العالمية لحوكمة الإنترنت، رقم (1) (مايو 2014)، https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf.

12 راجع، على سبيل المثال، القواعد التي وضعتها جمعية الإنترنت (ISOC) ومايكروسوفت: "القواعد المتفق عليها بشكل متبادل لأمن التوجيه (MANRS)"، جمعية الإنترنت (2014)، https://www.manrs.org/؛ وأنجيلا ماكاي وآخرون، *القواعد الدولية للأمن السيبراني التي تحد من الصراع في عالم يعتمد على الإنترنت*، Microsoft (ديسمبر 2014)، https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVroA؛ وسكوت تشارني وآخرون، *من الصياغة إلى التنفيذ: تمكين إحراز التقدم بشأن قواعد الأمن السيبراني*، مايكروسوفت (يونيو 2016)، https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc8.

2. ما المقصود باستقرار الفضاء السيبراني؟

التعريف:

يعني استقرار الفضاء السيبراني أن الجميع يمكن أن يكونوا واثقين بشكل معقول في قدرتهم على استخدام الفضاء السيبراني بطريقة آمنة ومأمونة، حيث يتم ضمان توافر ونزاهة الخدمات والمعلومات المقدمة في الفضاء السيبراني وعبره بشكل عام، وحيث يُدار التغيير بأسلوب يتسم بالسلام النسبي، وحيث يتم حل التوترات بطريقة غير تصعيدية.

بينما يستند تعريف اللجنة على التعريف المعياري لـ "الاستقرار"،[13] إلا أنه يختلف قليلًا من ناحيتين: الأولى، هناك إشارة إلى ثقة المستخدم. تكون الثقة مهمة لأن القرارات البشرية قد تكون مبنية على التصورات وليس الحقائق فقط، وإذا تصور أحد الأشخاص وجود حالة من عدم الاستقرار، فقد يكون مترددًا في استخدام الفضاء السيبراني والحصول على مزاياه. على سبيل المثال، قد يؤدي استخدام الفضاء السيبراني إلى تبسيط العمليات وجعلها أكثر كفاءة، مما يشير إلى أن وظائف معينة (مثل الوصول إلى الخدمات الحكومية، الخدمات المصرفية عبر الإنترنت) يمكن أن تستفيد من استغلال الفضاء السيبراني. ولكن إذا كانت مثل هذه الأنظمة غير موثوقة، أو كان هناك تصور بأن هذه الأنظمة غير موثوق بها، فسيكون استخدامها محدودًا وستهدر فوائد التقنية.

الثانية، يجب تذكر أن الفضاء السيبراني هو مجال من التغير المستمر. هناك تغيرات في التقنية، وفي نماذج الأعمال، وفي الوظائف، وفي التوقعات المجتمعية بشأن دور التقنية في الحياة اليومية. وبالتالي، على عكس تعريف القاموس لـ "الاستقرار" الذي يتضمن "العودة إلى حالة أصلية"، ما نحتاج إليه هو آليات مرنة لضمان استقرار الفضاء السيبراني مع تطور التقنيات. فبتعبير بسيط، يجب أن يظل الجميع واثقين من توافر ونزاهة الفضاء السيبراني حتى مع تغيره هو والعالم من حوله.

13 يُعرّف "الاستقرار" بأنه "حالة التحلي بالاستقرار". https://www.lexico.com/ar/definition/stability. يعني التحلي بالاستقرار (1) عدم احتمالية التراجع أو الانقلاب؛ الثبات بقوة و(2) عدم احتمالية التغير أو الفشل؛ الرسوخ؛ و(3) عدم القابلية للخضوع لتغييرات مادية. راجع https://en.oxforddictionaries.com/definition/stable. في العلاقات الدولية، كان أحد أكثر التعريفات اتساقًا لمصطلح الاستقرار الدولي هو "احتمالية احتفاظ النظام [الدولي] بجميع خصائصه الأساسية؛ وألا تصبح دولة واحدة مهيمنة؛ وأن يستمر معظم أعضائها في البقاء؛ وأن تلك الحرب واسعة النطاق لا تحدث." كارل دبليو دويتش وجيه ديفيد سينغر، "أنظمة الطاقة متعددة الأقطاب والاستقرار الدولي"، *وورلد بوليتكس*، المجلد. 16، رقم 3 (أبريل 1964): 390-406، http://users.metu.edu.tr/utuba/Deutsch.pdf.

3. إطار الاستقرار السيبراني للجنة العالمية بشأن استقرار الفضاء السيبراني

لمواجهة التحديات الموضحة أعلاه، فإن اللجنة العالمية المعنية باستقرار الفضاء السيبراني، كما فعل الآخرون،[14] تقترح إطارًا شاملًا للاستقرار السيبراني. يشتمل هذا الإطار على (1) مشاركة الجهات المعنية المتعددة؛ و(2) مبادئ للاستقرار السيبراني؛ و(3) وضع قواعد طوعية وتنفيذها؛ و(4) الالتزام بالقانون الدولي. و(5) تدابير لبناء الثقة؛ و(6) بناء القدرات؛ و(7) تعميم المعايير التقنية التي تضمن مرونة الفضاء السيبراني واستخدامها على نطاق واسع. ركزت جهود اللجنة العالمية المعنية باستقرار الفضاء السيبراني في المقام الأول على ثلاثة من هذه العناصر، نهج الجهات المعنية المتعددة والمبادئ والقواعد، ويتم تناولها في الأقسام 4 و5 و6 على التوالي. وفيما يتعلق بالقواعد، إننا لم نركز فقط على صياغتها، ولكن على المسائل الأكثر صعوبة التي تتمثل في اعتمادها وتنفيذها ومساءلة منتهكيها.

نلاحظ أن هناك العديد من الجهود الحالية التي تتناول عناصر فردية من إطار الاستقرار السيبراني هذا وتكون هذا الجهود، مثل الفضاء السيبراني نفسه، لا مركزية. لإحراز تقدم، تؤمن اللجنة العالمية المعنية باستقرار الفضاء السيبراني بأنه يلزم بذل جهد عالمي مشترك من الجهات المعنية المتعددة. لذلك، تقدم اللجنة العالمية المعنية باستقرار الفضاء السيبراني، بالإضافة إلى تناول المسائل الجوهرية، توصيات بشأن العملية تحاول الاستفادة من الجهود الحالية وتكملها وربما منحها قدرة جديدة.

14 راجع، على سبيل المثال، عصر *الترابط الرقمي: تقرير الفريق الرفيع المستوى المعني بالتعاون الرقمي التابع للأمين العام للأمم المتحدة* (يونيو 2019)، ص 39، https://digitalcooperation.org/wp-content/uploads/2019/06/DigitalCooperation-report-web-FINAL-1.pdf. "نحن نوصي بإرساء التزام عالمي بشأن الثقة والأمن الرقميين لتشكيل رؤية مشتركة، وتحديد سمات الاستقرار الرقمي، وتوضيح وتعزيز تنفيذ قواعد للاستخدامات المسؤولة للتقنية، واقتراح أولويات العمل".

4. مشاركة الجهات المعنية المتعددة

على الرغم من وجود عدد كبير من الاتفاقات الدولية بين الدول تشير إلى أهمية اتباع نهج من الجهات المعنية المتعدة، إلا أن الأمر لا يزال محلًا للجدل. فبالنسبة للبعض، يكون النقاش فلسفيًا ويركز على الأدوار النسبية للجهات الرسمية وغير الرسمية في سياسة التقنية والشؤون الدولية. وبالنسبة للآخرين، تكون عمليات الجهات المعنية المتعددة عملية، من خلال التأكيد على أن عمل الدول بمفردها أو مع حد أدنى فقط من المساهمات غير الرسمية لا يمكن أن يضمن استقرار الفضاء السيبراني.[15] ونحن نتفق مع هذا الرأي الأخير.

إن هذا النقاش حول مزايا مشاركة الجهات المعنية المتعددة مستمر لعقود. وفي كثير من الأحيان، ظهرت المشكلة في سياق إدارة موارد الإنترنت، ولكن أثيرت أيضًا مسألة القواعد والأمن القومي. على سبيل المثال، خلال المرحلة الثانية من القمة العالمية لمجتمع المعلومات التابعة للأمم المتحدة، رفض فريق الأمم المتحدة العامل المعني بحوكمة الإنترنت (WGIG) مفهوم القيادة الفردية لجهة معنية. وبدلًا من ذلك، خلص إلى أن الإنترنت أكبر من أن تتم إدارته من قِبل مجموعة واحدة من الجهات المعنية أو مؤسسة واحدة بمفردها واقترح نهجًا من الجهات المعنية المتعددة. وهكذا، في عام 2005، أعلن رؤساء الدول في أجندة تونس بالقمة العالمية لمجتمع المعلومات أن "التعريف العملي لحوكمة الإنترنت هو تطوير وتطبيق الحكومات والقطاع الخاص والمجتمع المدني، كل في دوره الخاص، للمبادئ والمعايير والقواعد المشتركة وإجراءات اتخاذ القرارات والبرامج التي تشكل تطور واستخدام الإنترنت".[16]

وقد أعاد الاجتماع الرفيع المستوى للجمعية العامة للأمم المتحدة بشأن الاستعراض الشامل لتنفيذ نواتج القمة العالمية لمجتمع المعلومات تأكيد وجهة النظر هذه بعد مرور عشر سنوات، والذي صرح أيضًا في قرار الأمم المتحدة 70/125 (2015):

> علاوة على ذلك، نحن نعيد التأكيد على قيمة ومبادئ تعاون ومشاركة الجهات المعنية المتعددة التي اتسمت بها عملية القمة العالمية لمجتمع المعلومات منذ بدايتها، مع الإقرار بأن المشاركة الفعالة والشراكة والتعاون بين الحكومات والقطاع الخاص والمجتمع المدني والمنظمات الدولية والأوساط التقنية والأكاديمية وجميع الجهات المعنية الأخرى، في إطار أدوارها ومسؤولياتها الخاصة، ولا سيما مع التمثيل المتوازن من البلدان النامية، كانت ولا تزال حيوية في تطوير مجتمع المعلومات.[17]

15 "قدم تعريف القمة العالمية لمجتمع المعلومات (2005) مفهوم" الأدوار الخاصة" وفلسفة "المشاركة". وعرف إعلان NETmundial (2014) العناصر الأساسية على أنها قائمة على نهج تصاعدي والانفتاح والشفافية والشمولية وحقوق الانسان. بعبارة أخرى، لدينا بعض الإرشادات العامة لنهج من الجهات المعنية المتعددة، ولكن ليس لدينا نموذج واحد للجهات المعنية المتعددة. وحتى الآن، ظهر نموذجان مختلفان للجهات المعنية المتعددة: النموذج الاستشاري والنموذج التعاوني. " وولف غانغ كلينفيكتر، "نحو نهج شامل لصنع السياسات العامة المتعلقة بالإنترنت"، اللجنة العالمية المعنية باستقرار الفضاء السيبراني (يناير 2018)، https://cyberstability.org/wp-content/uploads/2018/02/GCSC_Kleinwachter-Thought-Piece-2018-1.pdf. لمزيد من المناقشة حول نماذج الجهات المعنية المتعددة، راجع فيرجيليو ألميدا وآخرون، "منشأ وتطور نماذج الجهات المعنية المتعددة،" *IEEE Internet Computing*، المجلد 19 (يناير - فبراير 2015): 74-79، https://doi.ieee-computersociety.org/10.1109/MIC.2015.15.

16 "أجندة تونس لمجتمع المعلومات"، القمة العالمية لمجتمع المعلومات (18 نوفمبر 2005)، الفقرة 34، https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html.

17 راجع قرار الجمعية العامة للأمم المتحدة 70/125، *الوثيقة الختامية للاجتماع الرفيع المستوى للجمعية العامة بشأن الاستعراض الشامل لتنفيذ نتائج القمة العالمية لمجتمع المعلومات*، A/RES/70/125 (16 ديسمبر 2015)، الفقرة 3، https://undocs.org/en/A/RES/70/125.

ومرة أخرى، تجاوز البيان إدارة موارد الإنترنت المهمة وتعمق بشكل مباشر في قلب قضايا الأمن القومي:

> نحن ندرك الدور الرائد للحكومات في مسائل الأمن السيبراني المتعلقة بالأمن القومي. كما ندرك الأدوار والمساهمات المهمة لجميع الجهات المعنية، في أدوارها ومسؤولياتها ذات الصلة.[18]

أعلنت مجموعة الثمانية (G8) في عام 2011، فيما يتعلق بالقواعد على وجه التحديد، ما يلي:

> يعد أمن الشبكات والخدمات على الإنترنت مشكلة لجهات معنية متعددة. ويتطلب التنسيق بين الحكومات والمؤسسات الإقليمية والدولية، والقطاع الخاص، [و]المجتمع المدني...فللحكومات دور تؤديه، مستنيرة في ذلك بمجموعة كاملة من الجهات المعنية، في المساعدة على وضع قواعد السلوك والنهج المشتركة في استخدام الفضاء السيبراني.[19]

أصدر فريق الخبراء الحكوميين التابع للأمم المتحدة بعد ذلك بعامين، في عام 2013، *تقريره عن التطورات في مجال المعلومات والاتصالات عن بُعد في سياق الأمن الدولي*. أشار فريق الخبراء الحكوميين التابع للأمم المتحدة في قسم بعنوان "إقامة التعاون بهدف الحصول على بيئة سلمية وآمنة ومرنة ومنفتحة لتقنية المعلومات والاتصالات"، إلى أنه "على الرغم من أنه يجب على الدول القيادة في مواجهة هذه التحديات، فإن التعاون الفعال سيستفيد من المشاركة المناسبة للقطاع الخاص والمجتمع المدني."[20] وتابع التقرير في قسم بعنوان "توصيات بشأن قواعد وقواعد ومبادئ السلوك المسؤول للدول،" بما أفاد أنه:

> ينبغي للدول الأعضاء النظر في أفضل السبل للتعاون في تنفيذ قواعد ومبادئ السلوك المسؤول المذكورة أعلاه، بما في ذلك الدور الذي يمكن أن يلعبه القطاع الخاص ومنظمات المجتمع المدني.[21]

وقد أعيد تأكيد هذه المواقف في تقرير فريق الخبراء الحكوميين التابع للأمم المتحدة لعام 2015، حيث أُعلن ما يلي:

> وبينما تتحمل الدول مسؤولية أساسية عن الحفاظ على بيئة آمنة وسلمية لتقنية المعلومات والاتصالات، فإن التعاون الدولي الفعال سيستفيد من تحديد آليات للمشاركة، حسب الاقتضاء، من القطاع الخاص والأوساط الأكاديمية ومنظمات المجتمع المدني.[22]

تكرر هذا البيان في قرار الجمعية العامة لعام 2018 بشأن *تعزيز سلوك الدولة المسؤول في مجال الفضاء السيبراني في سياق الأمن الدولي*..[23]وتعبر الاتفاقيات الدولية الأخرى بوضوح عن نفس الشعور؛ على سبيل المثال، ذكرت دعوة باريس، "نحن ندرك ضرورة اتباع نهج معزز متعدد الجهات المعنية وبذل جهود إضافية للحد من المخاطر التي تهدد استقرار الفضاء الإلكتروني وبناء الثقة والقدرة والائتمان."[24]

18 المرجع نفسه، الفقرة 50.

19 مجموعة الثمانية، "إعلان مجموعة الثمانية: الالتزام المتجدد من أجل الحرية والديمقراطية،" قمة مجموعة الثمانية بدوفيل (27 مايو 2011)، الفقرة 17، http://www.g8.utoronto.ca/summit/2011deau-ville/2011-declaration-en.html.

20 الجمعية العامة للأمم المتحدة، *تقرير فريق الخبراء الحكوميين المعني بالتطورات في مجال المعلومات والاتصالات عن بُعد في سياق الأمن الدولي*، A/68/98 (24 يونيو 2013)، صفحة 7، الفقرة 12، https://undocs.org/A/68/98، (المُشار إليه فيما يلي بعبارة "تقرير فريق الخبراء الحكوميين التابع للأمم المتحدة لعام 2013).

21 المرجع نفسه، صفحة 8، الفقرة 25.

22 الجمعية العامة للأمم المتحدة، *تقرير فريق الخبراء الحكوميين المعني بالتطورات في مجال المعلومات والاتصالات عن بُعد في سياق الأمن الدولي*، A/70/174 (22 يوليو 2015)، صفحة 13، الفقرة 31، https://undocs.org/A/70/174، (المُشار إليه فيما يلي بعبارة "تقرير فريق الخبراء الحكوميين التابع للأمم المتحدة لعام 2015).

23 قرار الجمعية العامة للأمم المتحدة رقم 73/266، *تعزيز سلوك الدولة المسؤول في مجال الفضاء السيبراني في سياق الأمن الدولي*، A/RES/73/266 (22 ديسمبر 2018)، https://undocs.org/ar/A/RES/73/266.

24 وزارة الثقة والأمن في الفضاء السيبراني" (11 نوفمبر 2018)، https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf. راجع أيضًا، NETmundial، "بيان NETmundial للجهات المعنية المتعددة" (24 أبريل 2014)، http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf.

وذكر الفريق الرفيع المستوى المعني بالتعاون الرقمي التابع للأمين العام للأمم المتحدة مؤخرًا، في يونيو 2019، في تقريره، *عصر الترابط الرقمي*، ما يلي:

> يتطلب التعاون الرقمي الفعال تعزيز تعددية الأطراف، على الرغم من الضغوط الحالية. كما يتطلب الأمر أن يتم استكمال تعددية الأطراف بتعددية الجهات المعنية - وهو تعاون لا يقتصر على الحكومات فحسب، بل يشمل طيفًا أكثر تنوعًا بكثير من الجهات المعنية الأخرى مثل المجتمع المدني والأكاديميين والتقنيين والقطاع الخاص.[25]

وفي حين أثبتت فكرة النهج متعدد الجهات المعنية نجاحه، إلا أنه غير مدعوم عالميًا. لازالت بعض الحكومات تعتقد بأن ضمان الأمن والاستقرار الدوليين يقع على عاتق الدول بشكل حصري تقريبًا. تنبع هذه النظرة الأكثر تقليدية للأمن من فكرة أن الدول تتحمل مسؤولية حماية مواطنيها من الهجمات من الوسائل القوية، وهي فكرة تنعكس في مسؤوليات مجلس الأمن التابع للأمم المتحدة على النحو المدون في المادة 24 من ميثاق الأمم المتحدة.[26] قد يتم تعزيز هذا الاتجاه من التفكير أيضًا من خلال الخبرة السابقة لأنه في المجال المادي، لم تتمتع الحكومات فقط باحتكار الاستخدام المشروع للقوة، بل كانت تسيطر كذلك على الأسلحة العسكرية (مثل الطائرات والدبابات) المستخدمة في مهاجمة هذا المجال والدفاع عنه.

ومن الناحية العملية، تم تصميم ساحة المعركة السيبرانية (أي الفضاء السيبراني) ونشرها وتشغيلها بشكل أساسي من قبل القطاع الخاص. لا تعتبر الحكومات، على الرغم من مسؤولياتها الفريدة، الجهة الحامية الحصرية لهذا المجال. حتى لو حافظت الحكومات على *احتكار قانوني* للاستخدام الشرعي للقوة في الفضاء السيبراني، فلم يعد لديها احتكار عملي في مهاجمة هذا المجال وحمايته، ولا يمكنها منع انتشار واستخدام الأسلحة السيبرانية القوية.

وبدلًا من ذلك، يلعب المجتمع التقني والمجتمع المدني والأفراد دورًا رئيسيًا كذلك في حماية الفضاء السيبراني، بما في ذلك تعميم المعايير. ولذلك، فإن النهج متعدد الجهات المعنية ضروري لتحسين النتائج وضمان كون القواعد والسياسات التي تدعم استقرار الفضاء السيبراني جيدة التكوين وتتجنب العواقب غير المرغوب فيها.

وهو على نفس القدر من الأهمية، حتى لو كانت الدول ترغب في القيام بذلك بمفردها، فلا يمكنها ذلك. فمشاركة الجهات الفاعلة من غير الدول في الأمور التي تؤثر على استقرار الفضاء السيبراني تعتبر أمرًا لا مفر منه. على سبيل المثال، قد يكون العديد من أعضاء القطاع الخاص والمجتمع التقني مسؤولين عن البروتوكولات والخدمات المهمة، وقد يقدمون الحماية للدول التي تستخدم منتجاتها التجارية مفتوحة المصدر. وبالإضافة إلى ذلك، حتى التحقيقات وإسناد الهجمات، وهو دور تقليدي وامتياز سياسي للحكومات، لم يعد مجال المعرفة والمسؤولية الوحيد بالنسبة لها؛ وقد تم تحديد بعض هجمات الدول البارزة ونشرها من قبل هيئات غير حكومية. باختصار، على الرغم من أن للدول دورًا فريدًا تؤديه أثناء الهجوم وبعده (بما في ذلك نشاط إنفاذ القانون و/أو اتخاذ إجراءات دبلوماسية أو غيرها من الإجراءات الحكومية)، فإنها لا تحتكر عمليات التحقيق والإسناد، ولا يمكنها استبعاد الجهات الفاعلة من غير الدول بشكل فعال. ونتيجة لذلك، يتطلب وضع قواعد وسياسات ناجحة للفضاء السيبراني، وضمان الالتزام بها، مشاركة من قبل جميع الجهات المعنية ويعد مسؤوليتها، ويجب على الحكومات التركيز على إنشاء آليات تدمج مشاركة القطاع الخاص والمجتمع التقني والأوساط الأكاديمية وممثلي المجتمع المدني الآخرين بشكل فعال. وهذا بالضبط ما دعت إليه العديد من الحكومات.

25 *عصر الترابط الرقمي*، صفحة 7، https://digitalcooper-ation.org/wp-content/uploads/2019/06/DigitalCooperation-re-port-web-FINAL-1.pdf.

26 ميثاق الأمم المتحدة، "الفصل الخامس - مجلس الأمن"، مرجع ممارسات هيئات الأمم المتحدة، http://legal. un.org/repertory/art24.shtml.

5. المبادئ

ينشق السلوك المعياري من القيم. لذلك يجب أن يكون إعلان هذه القيم، سواء كانت تتعلق بالمسؤوليات الفردية أو مسؤوليات الدولة أو حقوق الإنسان الأساسية، هو نقطة انطلاقنا. والواقع أن القيم المختلفة يمكن أن تجعل تحقيق توافق الآراء أمرًا صعبًا، فضلًا عن أنها تؤدي إلى اختلاف التفسيرات وعمليات التنفيذ القطرية أو الإقليمية للاتفاقيات الدولية. ولا يعني هذا أن الاتفاق على المبادئ مطلوب لإحراز التقدم؛ فأحيانًا تتفق الأطراف على السلوكيات المقبولة حتى إذا اختلفت دوافعها للقيام بذلك. لكن المبادئ المشتركة والترابط يمكن أن يؤدي إلى التزامات أكثر عمقًا ويقلل مخاطر نشوب الخلافات أو النزاعات في المستقبل. لذلك من المهم أن تجري الأطراف مناقشات صريحة حول المبادئ رفيعة المستوى التي توجه طريقة تفكيرهم والتي تنبثق منها القواعد.

تعد المبادئ الأربعة التالية حاسمة لضمان استقرار الفضاء السيبراني:

1. **المسؤولية:** كل فرد مسؤول عن ضمان استقرار الفضاء السيبراني.
2. **التقييد:** يجب على الجهات الحكومية وغير الحكومية عدم اتخاذ إجراءات من شأنها أن تضعف استقرار الفضاء السيبراني.
3. **شرط العمل:** يجب على الجهات الحكومية وغير الحكومية اتخاذ خطوات معقولة ومناسبة لضمان استقرار الفضاء السيبراني.
4. **احترام حقوق الإنسان:** يجب أن تراعي الجهود المبذولة لضمان استقرار الفضاء السيبراني حقوق الإنسان وسيادة القانون.

أ. مبدأ المسؤولية

يتحدث المبدأ الأول عن الطبيعة اللامركزية والموزعة للفضاء السيبراني. ويؤكد من جديد الحاجة إلى نهج متعدد الجهات المعنية لضمان استقرار الفضاء السيبراني، ولا سيما توسيع نطاق "الجهات المعنية" ليشمل كل فرد. يتحمل كل فرد مسؤوليات، بصفته الشخصية و/أو المهنية، لضمان استقرار الفضاء السيبراني. وفي حين أنه قد يكون من الواضح أن أولئك المسؤولين عن السياسات الحكومية السيبرانية والموظفين الذين يديرون الخدمات السحابية لديهم دور يلعبونه، حيث يجب على كل فرد متصل بالفضاء السيبراني بذل جهود معقولة لضمان عدم تعرض أجهزتهم الخاصة للاختراق، وربما استخدامها في الهجمات. وحتى أولئك الذين ليسوا متصلين بالإنترنت قد يعتمدون على قدراته على استلام السلع والخدمات، ولديهم مصلحة كذلك في ضمان معالجة سياسة الفضاء السيبراني بشكل مناسب في مجتمعاتهم.

ب. مبدأ التقييد

يشمل المبدأ الثاني متطلبًا عامًا للتقييد. يتماشى هذا بالنسبة للدول مع قرارات عام 2018 الصادرة عن الجمعية العامة للأمم المتحدة (UNGA) بشأن سلوك الدولة المسؤول في مجال الفضاء السيبراني[27] وتقرير فريق الخبراء الحكوميين التابع للأمم المتحدة لعام 2015 الذي يشير إلى أنه "ينبغي على الدول، بما يتفق مع أغراض الأمم المتحدة، بما في ذلك الحفاظ على السلام والأمن الدوليين، ... منع ممارسات تقنية المعلومات والاتصالات التي يُعترف بكونها ضارة أو التي قد تشكل تهديدات للسلام والأمن الدوليين ..."[28] ولكن الأمر لا يتعلق فقط بالدول، حيث يمكن للجهات الفاعلة من غير الدول المشاركة أيضًا في اتخاذ الإجراءات، مثل قرصنة مهاجميها، مما قد يقوض كذلك استقرار الفضاء السيبراني.

27 قرار الجمعية العامة للأمم المتحدة رقم 73/27، *التطورات في مجال المعلومات والاتصالات عن بُعد في سياق الأمن الدولي*، A/RES/73/27 (5 ديسمبر 2018)، https://undocs.org/ar/A/RES/73/27؛ وقرار الجمعية العامة للأمم المتحدة رقم 73/266، https://undocs.org/ar/A/RES/73/266.

28 تقرير فريق الخبراء الحكوميين التابع للأمم المتحدة لعام 2015، صفحة 7، الفقرة 13(أ)، https://undocs. org/A/70/174.

ج. مبدأ شرط العمل

يشمل المبدأ الثالث متطلبًا عامًا لاتخاذ إجراء إيجابي للحفاظ على استقرار الفضاء السيبراني. ينبغي على الدول توخي الحذر عند العمل لتجنب تصاعد التوترات أو زيادة عدم الاستقرار عن غير قصد. ويتسق هذا مع الالتزام المشار إليه في تقرير فريق الخبراء الحكوميين التابع للأمم المتحدة لعام 2015 بـ "التعاون في وضع وتطبيق تدابير لزيادة الاستقرار والأمن في استخدام تقنية المعلومات والاتصالات".[29] ولكن مرة أخرى، لا يقتصر الأمر على الدول فقط، حيث يمكن للشركات الخاصة والأفراد أيضًا اتخاذ خطوات تعاونية للمساعدة في ضمان استقرار الفضاء السيبراني. فعلى سبيل المثال، يمكن للشركات الخاصة العمل معًا للتخفيف من التهديدات السيبرانية، ويمكن للأفراد التأكد من أنهم يستخدمون أفضل الممارسات، مثل الترقية والبرامج التصحيحية واستخدام المصادقة متعددة العوامل، للحد من مخاطر سيطرة شبكات الروبوت على أجهزتهم ومن ثم استخدامها لشن هجمات واسعة النطاق تهدد استقرار الفضاء السيبراني.

د. مبدأ حقوق الإنسان

يقر المبدأ الرابع بأهمية حماية حقوق الإنسان كعنصر مهم في استقرار الفضاء السيبراني. ومع تزايد اعتماد الأفراد على تقنية المعلومات والاتصالات، يتضخم التأثير المدمر على النشاط البشري الناجم عن التهديدات على توافره أو سلامته. وبالتالي، من الضروري أنه بينما تسعى الدول لتحقيق مصالحها الاستراتيجية الوطنية في الفضاء السيبراني، فإنها يجب أن تولي الاعتبار الواجب للتأثير الناتج على الأفراد، ولا سيما حقوقهم الإنسانية. وعلى نفس المنوال، ينبغي على الجهات الفاعلة من غير الدول النظر في المخاطر التي تشكلها أنشطتها على تمتع الأفراد بحقوقهم على شبكة الإنترنت وخارجها وتقليل هذه المخاطر. يتطلب الامتثال لمبدأ حقوق الإنسان أن تلتزم الدول بالتزاماتها في مجال حقوق الإنسان كحد أدنى بموجب القانون الدولي أثناء مشاركتها في أنشطة في الفضاء السيبراني.

29 المرجع نفسه.

تم إدراج حقوق الإنسان المقبولة عالميًا في الإعلان العالمي لحقوق الإنسان.[30] بالإضافة إلى ذلك، تم اعتماد عدد كبير من الاتفاقيات الدولية التي تنص على مجموعة متنوعة من حقوق الإنسان المحددة وتنشئ التزامات قانونية ملزمة للدول الأطراف. تم تأكيد قابلية تطبيق القانون الدولي لحقوق الإنسان بشكل صريح، في سياق الفضاء السيبراني، في عدة مناسبات من قبل الجمعية العامة للأمم المتحدة،[31] ومجلس حقوق الإنسان التابع للأمم المتحدة (HRC)[32]، وكذلك تقارير فريق الخبراء الحكوميين التابع للأمم المتحدة لعامي 2013 و 2015.[33] ويعتبر التمسك بحقوق المستخدمين وضمان ثقتهم في احترام حقوقهم أمرًا بالغ الأهمية لضمان استقرار الفضاء السيبراني.

نلاحظ أن المبادئ الأربعة لا يُقصد بها أن تكون شاملة أو تغطي كل جانب من جوانب سياسة الفضاء السيبراني، وهناك العديد من المؤسسات التي أنتجت مجموعات واسعة النطاق من المبادئ التي تغطي مجموعة متنوعة من القضايا. توجد كذلك مؤسسات أخرى تركز على القضايا المتعلقة بإدارة شبكة الإنترنت وحقوق الإنسان عبر الإنترنت (بما في ذلك الخصوصية وحرية التعبير وحرية تكوين الجمعيات). إن هدفنا هو تحقيق قبول واسع النطاق للمبادئ التي تدعم استقرار الفضاء السيبراني، خاصةً في عصر النشاط العدائي غير المسبوق والمعقد حيث قد تكون القواعد غير واضحة أو، حتى لو كانت واضحة، قد لا يتم تبنيها أو فرضها.

30 قرار الجمعية العامة للأمم المتحدة رقم 217 أ (3)، *الإعلان العالمي لحقوق الإنسان* (10 ديسمبر 1948)، https://www.un.org/ar/universal-declaration-human-rights/.

31 راجع قرار الجمعية العامة للأمم المتحدة رقم 68/167، *الحق في الخصوصية في العصر الرقمي*، A/RES/68/167 (18 ديسمبر 2013)، https://undocs.org/A/RES/68/167؛ وقرار الجمعية العامة للأمم المتحدة رقم 69/166، *الحق في الخصوصية في العصر الرقمي*، A/RES/69/166 (18 ديسمبر 2014)، https://undocs.org/A/RES/69/166.

32 مجلس حقوق الإنسان التابع للأمم المتحدة، *تعزيز حقوق الإنسان وحمايتها والتمتع بها على شبكة الإنترنت*، A/HRC/20/L.13 (29 يونيو 2012)، https://undocs.org/A/HRC/20/L.13.

33 تقرير فريق الخبراء الحكوميين التابع للأمم المتحدة لعام 2013، https://undocs.org/A/68/98 وتقرير فريق الخبراء الحكوميين التابع للأمم المتحدة لعام 2015، https://undocs.org/A/70/174.

6. القواعد

في حين تكون المبادئ هي نقطة البداية الرئيسية لوضع السياسات وتوجيه الإجراءات التكتيكية، إلا أن مستوى تجريدها العالي يتطلب أن يتم استكمالها باتفاقيات أكثر دقة تحدد السلوك المقبول. وهذا يعني أن المبادئ يجب أن تكملها القواعد. تمثل القواعد سلوكيات اجتماعية متوقعة ومناسبة.[34] فمن المستحيل مناقشة القواعد دون الرجوع إلى أعمال المؤسسات الأخرى، لا سيما فريق الخبراء الحكوميين التابع للأمم المتحدة وتقريره لعام 2015.[35] وقد أقر فريق الخبراء الحكوميين التابع للأمم المتحدة بأنه "بالنظر إلى السمات الفريدة لتقنية المعلومات والاتصالات، يمكن وضع قواعد إضافية بمرور الوقت،"[36] وكان تفويض اللجنة العالمية المعنية باستقرار الفضاء السيبراني، في الواقع، هو "طرح مقترحات لقواعد وسياسات لتعزيز الأمن والاستقرار الدوليين." "من الأهمية بمكان، للبناء على العمل المسبق وتحديد أين قد تكون هناك حاجة إلى قواعد إضافية، البدء بالقواعد المتفق عليها في عام 2015 والتي يمكن العثور عليها بالكامل في الملحق أ.

وكما أشار فريق الخبراء الحكوميين التابع للأمم المتحدة في عام 2015، فقد تم تكليفه، من بين أمور أخرى، "بتحديد مواضع حاجة القواعد الإضافية التي تأخذ في الاعتبار التعقيد والسمات الفريدة لتقنية المعلومات والاتصالات إلى التطوير."[37] ومنذ ذلك الوقت، استمرت منتجات وخدمات تقنية المعلومات والاتصالات، وكذلك سوء استخدامها، في التغيير. ركزت اللجنة العالمية المعنية باستقرار الفضاء السيبراني على سد الثغرات في مجموعة القواعد الحالية، لمعالجة هذا الأمر، وإضافة الخاصية التقنية إلى مناقشة القواعد، ومعالجة قضايا التنفيذ. وفيما يتعلق بسد الثغرات، على سبيل المثال، أقرت اللجنة العالمية المعنية باستقرار الفضاء السيبراني معيارًا لحماية النواة العامة للإنترنت[38] ومعيارًا لحماية النظم الانتخابية.[39] وبالمثل، بينما يشير معيار فريق الخبراء الحكوميين التابع للأمم المتحدة إلى "سلامة سلسلة التوريد"،[40] يتماشى معيار اللجنة العالمية المعنية باستقرار الفضاء السيبراني بشكل أكثر تحديدًا مع أنواع الهجمات على سلسلة التوريد التي يجب تناولها.[41]

34 https://en.oxforddictionaries.com/definition/norm.

35 تقرير مجموعة الخبراء الحكوميين التابعين للأمم المتحدة 2015، https://undocs.org/A/70/174.

36 نفس المرجع، ص 8، الفقرة 15.

37 نفس المرجع، ص 7، الفقرة 11.

38 اللجنة العالمية المعنية باستقرار الفضاء السيبراني (GCSC)، *دعوة إلى حماية النواة العامة للإنترنت* (نيودلهي، نوفمبر 2017)، https://cyberstability.org/wp-content/uploads/2018/07/call-to-protect-the-public-core-of-the-internet.pdf. كان الباحث الهولندي دينيس برودرز من أوائل مؤيدي تحديد النواة العامة للإنترنت من أجل الحماية الخاصة. راجع دينيس برودرز، *النواة العامة للإنترنت: جدول الأعمال الدولي لحوكمة الإنترنت* (أمستردام: مطبعة جامعة أمستردام، 2015)، http://www.oapen.org/download?type=document&docid=610631.

39 اللجنة العالمية لاستقرار الفضاء السيبراني (GCSC)، *دعوة لحماية البنية التحتية الانتخابية* (براتيسلافا، مايو 2018)، https://cyberstability.org/wp-content/uploads/2018/05/GCSC-Call-to-Protect-Electoral-Infrastructure.pdf.

40 تقرير مجموعة الخبراء الحكوميين التابعين للأمم المتحدة 2015، ص 8، الفقرة 13(i). "يجب أن تتخذ الدول خطوات معقولة لضمان سلامة سلسلة الإمداد حتى يتمكن المستخدمين النهائيين من الثقة في أمن منتجات تكنولوجيا المعلومات والاتصالات (ICT). ويجب أن تسعى الدول لمنع انتشار أدوات وتقنيات تكنولوجيا المعلومات والاتصالات الخبيثة واستخدام الوظائف المخفية".

41 اللجنة العالمية لاستقرار الفضاء السيبراني (GCSC)، *المعايير بجميع أنحاء سنغافورة* (نوفمبر 2018)، https://cyberstabil-ity.org/wp-content/uploads/2019/04/singaporenew-digital.pdf. "يجب على الجهات الفاعلة الحكومية وغير الحكومية عدم التلاعب بالمنتجات والخدمات عند التطوير والإنتاج، أو السماح بالتلاعب بها، إذا كان من شأن القيام بذلك أن يضر باستقرار الفضاء السيبراني بشكل كبير".

ويتمثل الفارق الرئيسي الآخر بين القواعد التي حددها فريق الخبراء الحكوميين التابع للأمم المتحدة وتلك التي اقترحتها اللجنة العالمية المعنية باستقرار الفضاء السيبراني في أن اللجنة العالمية المعنية باستقرار الفضاء السيبراني تعتقد أنه يجب فرض المسؤوليات على الجهات الفاعلة غير الحكومية أيضًا، كما يتعين عليها تحمل المسؤولية أو اتخاذ خطوات إيجابية لضمان استقرار الفضاء السيبراني. ونحن لا نشير هنا إلى الهجمات السيبرانية التي يشنها المجرمون؛ فالمجرمين الذين لا تردعهم الإجراءات الحكومية لن تردعهم القوانين. ولكن بما أن التكنولوجيا تتغير بشكل سريع والقوانين لا تتغير، فمن المفيد أن نتعامل بشكل دقيق فيما يتعلق بالسلوكيات غير الحكومية التي يجب تشجيعها أو تثبيطها حتى في غياب القوانين. على سبيل المثال، يدعو البعض إلى ضرورة السماح لضحايا عمليات القرصنة "بالقرصنة الارتجاعية". وحتى في غياب القوانين التي تسمح بمثل هذا السلوك أو تمنعه، تعتقد اللجنة العالمية المعنية باستقرار الفضاء السيبراني أنه من غير المستحسن القيام بذلك لعدة أسباب، بما في ذلك أن المهاجم الأولي قد يقوم بشن هجماته عبر أنظمة تابعة لجهات خارجية (مثل مزود سحابة أو مستشفى) وبالتالي فإن القرصنة الارتجاعية قد تؤثر على المستخدمين الأبرياء (على سبيل المثال، عملاء الخدمة السحابية أو المرضى). بالإضافة إلى ذلك، وبسبب هذه الهجمات على الضحايا الأبرياء، يمكن اعتبار القرصنة الارتجاعية تصعيدًا للمشكلة أو إثارة لها. باختصار، ونظرًا للتعقيدات التي أُثيرت، حتى في غياب القوانين، فإن القاعدة التي تقيد الجهات الفاعلة في القطاع الخاص قد تؤثر على السلوكيات المتبعة وبالتالي تخدم غرضًا فعالًا.

أ. القواعد التي اقترحتها اللجنة العالمية المعنية باستقرار الفضاء السيبراني

مع مراعاة النقاط الواردة أعلاه، وضعت اللجنة العالمية المعنية باستقرار الفضاء السيبراني المعايير التالية المقترحة:

1. تلتزم الجهات الحكومية وغير الحكومية بعدم القيام بأي نشاط من شأنه أن يضر التوافر العام أو الأساس العام للإنترنت، وبالتالي استقرار الفضاء السيبراني، عن قصد أو بشكل ملموس أو السماح بذلك عن علم.

2. تلتزم الجهات الحكومية وغير الحكومية بعدم السعي إلى العمليات السيبرانية التي تهدف إلى تعطيل البنية التحتية التقنية اللازمة لإجراء الانتخابات أو الاستفتاءات أو دعمها أو السماح بها.

3. تلتزم الجهات الحكومية وغير الحكومية بعدم العبث بالمنتجات والخدمات في التطوير والإنتاج، أو السماح بالعبث بها، إذا كان القيام بذلك قد يضعف استقرار الفضاء الإلكتروني على نحوٍ كبير.

4. تلتزم الجهات الحكومية وغير الحكومية بعدم الاستحواذ على موارد تقنية المعلومات والاتصالات الخاصة بعامة الجمهور من أجل استخدامها كشبكات روبوت أو لأغراض مماثلة.

5. تلتزم الدول بإنشاء أطر عمل شفافة من الناحية الإجرائية لتقييم ما إذا كان ينبغي الكشف عن مواطن الضعف أو العيوب غير المعروفة علنًا التي تدركها في نظم وتكنولوجيا المعلومات ومتى ينبغي ذلك. وينبغي أن يكون الافتراض الوارد مؤيدًا لقرار الإفصاح.

6. تلتزم الجهات المطورة والجهات المنتجة للمنتجات والخدمات التي يعتمد عليها استقرار الفضاء السيبراني (1) بإعطاء الأولوية للأمن والاستقرار، و(2) اتخاذ خطوات معقولة لضمان خلو

منتجاتها أو خدماتها من مواطن الضعف الكبيرة، و(3) اتخاذ التدابير اللازمة في الوقت المناسب للتخفيف من مواطن الضعف التي تم اكتشافها لاحقًا والتحلي بالشفافية بشأن عملياتها. وتلتزم جميع الجهات الفاعلة بمشاركة المعلومات المتعلقة بمواطن الضعف من أجل المساعدة في منع النشاط السيبراني الخبيث أو الحد منه.

7. تلتزم الدول باتخاذ التدابير المناسبة، بما في ذلك القوانين واللوائح، لضمان السلامة السيبرانية الأساسية.

8. تلتزم الجهات غير الحكومية بعدم المشاركة في العمليات السيبرانية الهجومية وتلتزم الجهات الحكومية بمنع مثل هذه الأنشطة والاستجابة لها في حالة حدوثها.

تجدر الإشارة إلى أن إيجاد أنسب لغة للتعبير عن قاعدة ما قد يشكل تحديًا كبيرًا. وإذا كانت المعايير دقيقة للغاية ولم تترك مجالًا للتفسير، فقد يكون من الصعب تحقيق توافق في الآراء وقد تكون هناك ثغرات كبيرة في التغطية. ومن ناحية أخرى، إذا كانت القواعد غامضة للغاية، فإنها لا تقدم نوع التوجيه اللازم لتوجيه السلوكيات وتحديد توقعات واضحة لمجموعة محددة من الجهات الفاعلة. والهدف من ذلك تحقيق التوازن الصحيح ووضع المزيد من القواعد، عند الضرورة، لضمان معالجة السلوكيات غير المرغوب فيها. على سبيل المثال، عملت القواعد التي اعتمدها فريق الخبراء الحكوميين التابع للأمم المتحدة في 2015 على حماية البنى التحتية الحيوية، ولكن ليس من الواضح أن الأساس العام للإنترنت مشمول بهذا المصطلح؛ ويعتقد الكثيرون أن البنى التحتية الحيوية هي المرافق والخدمات (مثل الطاقة والاتصالات والخدمات المصرفية).[42] فضلاً عن ذلك، لم يشير فريق الخبراء الحكوميين التابع للأمم المتحدة على وجه التحديد إلى الأنظمة الانتخابية، وهو من المخاوف التي أصبحت أكثر حدة بعد عام 2015.[43] وعلى الرغم من أن الأنظمة الانتخابية قد تكون مشمولة في بعض البلدان من خلال الإشارة إليها (على سبيل المثال، تعتبر بعض الولايات الآن أن الأنظمة الانتخابية هي بنية تحتية حيوية، مما يجعلها تدخل في نطاق قواعد البنية التحتية الحيوية),[44] إلا أن بعض البلدان لا تتبع هذا النهج. وبالتالي، بينما يُعد الفضاء السيبراني عالميًا، فإن تدابير الحماية المعيارية قد لا تكون كذلك. وللمساعدة في معالجة قضايا التفسير المتعلقة بقواعد اللجنة العالمية المعنية باستقرار الفضاء السيبراني، قررت اللجنة تقديم نص يتضمن معلومات أساسية لكل قاعدة من القواعد المذكورة أعلاه (انظر الملحق ب).

وأخيرًا، لا يمكن أن تكون قواعد السلوكيات في الفضاء السيبراني ثابتة. تعكس قواعد اللجنة العالمية المعنية باستقرار الفضاء السيبراني لحظة من الزمن في مشهد تكنولوجي متغير بشكل مستمر. يجب على الجهات الفاعلة الحكومية وغير الحكومية أن تكون على أتم الاستعداد لوضع قواعد جديدة تتوافق مع تقدم التقنيات، ومع فهمنا للآثار المترتبة على تغير التقنيات الحالية.

سواء ركزت على القواعد التي حددها فريق الخبراء الحكوميين التابع للأمم المتحدة، أو قواعد اللجنة العالمية المعنية باستقرار الفضاء السيبراني، أو مقترحات أخرى، ينبغي الإقرار بأنه لكي تكون القواعد فعّالة، فمن الضروري اعتمادها وتنفيذها، ويجب أن يخضع منتهكي القواعد للمساءلة. والآن نعالج هذه القضايا، قبل أن ننتقل إلى الكيفية التي يمكن بها للجهات الفاعلة غير الحكومية، واللامركزية والتي يتم توزيعها في مختلف أنحاء العالم، أن تتحد معًا للعمل مع الحكومات للتوصل إلى حلول عملية لتحديات الاستقرار السيبراني.

ب. اعتماد القواعد

لكي تكون القاعدة فعّالة، يجب أن تحظى بقبول واسع النطاق. يعزز هذا القبول، حتى من جانب الجهات الفاعلة التي يعتقد البعض أنها من منتهكي

42 تم تحديد البنية التحتية الحرجة على أنها تتضمن "النظم والأصول، سواء المادية أو الافتراضية، الحيوية لدرجة أن ضعف أو تلف هذه الأنظمة والأصول سيكون له أثر موهن على الأمن، الأمن الاقتصادي الوطني، الصحة أو السلامة العامة الوطنية، أو أي مزيج من هذه الأمور". *قانون حماية البنية التحتية الحرجة لسنة 2001*، 42 القانون الأمريكي (2001) ،5195c(e) §. كما تم تحديدها على أنها" الأصول أو النظم الحيوية للحفاظ على الوظائف المجتمعية، صحة الأشخاص أو سلامتهم أو أمنهم أو اقتصادهم أو رفاهيتهم الاجتماعية". مجلس الاتحاد الأوروبي، *توجيهات المجلس 2008/114/EC بتاريخ 8 ديسمبر 2008 بخصوص تحديد وتسمية البنية التحتية الأوروبية الحرجة وتقييم الحاجة الى تحسين حمايتها*، الصحيفة الرسمية للاتحاد الأوروبي، (8 ديسمبر 2008)، https://eur-lex.europa.eu/legal-content/EN/TXT/ PDF/?uri=CELEX:32008L0114.

43 إيريك براتيبرغ وتيم موريز، *التدخل في الانتخابات الأوروبية: مواجهة أوروبا للأخبار الزائفة والهجمات السيبرانية*، مؤسسة كارنيغي للسلام الدولي (23 مايو 2018)، https://carn-egieendowment.org/2018/05/23/russian-election-int europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435. انظر أيضًا مايكل ماكفول، *تأمين الانتخابات الأمريكية*، مركز ستانفورد للسياسة السيبرانية (يونيو 2019)، https://cyber.fsi.stanford.edu/securing-our-cyber-future.

44 انظر، على سبيل المثال، وزارة الأمن الداخلي الأمريكية "بيان الوزير جيه جونسون بخصوص تسمية البنية التحتية الانتخابية على أنها قطاع فرعي للبنية التحتية الحرجة (6 يناير 2017)، https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastruc-ture-critical.

القواعد المحتملة، من شرعية الإجراءات التي تلقي الضوء على انتهاكات القواعد والإجراءات الجماعية المناسبة التي يتم اتخاذها للتصدي لهذه الانتهاكات. وعلى الرغم من أن اعتماد هذه القواعد على نطاق واسع هو الخيار الأفضل، إلا أن هناك مكانًا لمجموعات أصغر من الدول التي تتشاطر نفس الآراء أو الكيانات الأخرى للاتفاق على قواعد محددة وإنفاذها. ولمعالجة هذه المسألة، تقترح اللجنة العالمية المعنية باستقرار الفضاء السيبراني نهجًا مرنًا وقابل للامتداد على نطاق واسع يسمح للدول والجهات المعنية الأخرى بتبني بعض القواعد في حالة رفض أو امتناع الآخرين. وهذا النهج لا يعمل فقط على توضيح القواعد من خلال تسليط الضوء على مجالات محددة من الاتفاق والاختلاف، بل يسمح أيضاً بتبني قواعد معينة وتحسينها وتنفيذها، حتى إذا كانت هناك حاجة لمزيد من الوقت لتقييم مجالات أخرى. على أية حال، سيتطلب اعتماد القواعد على نطاق واسع جهودًا طويلة الأجل.

توجد أيضاً بعض التحديات الفريدة والعملية التي تواجه عملية تعزيز اعتماد القواعد. يتمثل التحدي الفريد في أننا نحاول معالجة السلوكيات الجديدة نسبياً والمزعزعة للاستقرار. ووصولًا إلى الحد الذي تكون فيه القاعدة "شيئًا معتادًا أو نموذجيًا أو قياسيًا،"[45] تُعد صياغة القواعد المتعلقة بالسلوكيات المستقبلية ممارسة مثيرة للاهتمام. وإذا كان الجميع يتصرف بالفعل بطريقة معينة، إذًا، تُعد القاعدة المكتوبة ببساطة تدوينًا للممارسة القائمة. ولكن إذا لم تكن هناك "سلوكيات نموذجية"، فإن صياغة قاعدة ما هي محاولة لتشجيع السلوكيات المشتركة في المستقبل، حتى في الحالات التي لا يوجد فيها سلوكيات مشتركة اليوم. فمجرد الإعلان عن شيء مرغوب لن يجعله سلوكًا معيارياً، وبالتالي، يجب تعزيز الاعتماد.

ثانياً، لابد من زيادة الوعي بالقواعد المقترحة من قِبل الكيانات القادرة على تنفيذها، فضلاً عن تلك الكيانات التي تهدف القواعد إلى حمايتها. وحتى مع النشاط الكبير الذي تقوم به الأمم المتحدة ومجموعة من المحافل الأخرى، لا يزال اعتماد القواعد في مراحله الأولى نسبيًا، ولابد من بذل الكثير من الجهود لتعزيز القواعد المقترحة وضمان القبول، وخاصة في أجزاء معينة من العالم. ولهذا السبب تُعد جهود بناء القدرات في هذا المجال بالغة الأهمية؛ فمن المرجح أن تدعم المنظمات ذات القدرات الأكبر اعتماد القواعد بشكل فعال ويُعد الحصول على جهات ملتزمة إضافية أمرًا أساسيًا لأي هيكل معياري عالمي. بالإضافة إلى ذلك، يجب إجراء أنشطة التوعية مع أولئك الذين تحميهم القواعد، إذ أنهم قد لا يدركون تأثيرها المحتمل. على سبيل المثال، لا يبدو أن هناك وعيًا واسع النطاق بين فرق الاستجابة لحوادث أمن الفضاء الإلكتروني (CSIRTs/CERTs) بالقواعد التي حددها فريق الخبراء الحكوميين التابع للأمم المتحدة فيما يتعلق بالدول التي لا تهاجم فرق الاستجابة لحوادث أمن الفضاء الإلكتروني وتستخدم هذه الفرق لأغراض دفاعية فقط. ووفقًا للمناقشة الواردة أدناه، غالبًا ما يكون للكيانات المحمية دورًا في التنفيذ والمساءلة (فضلاً عن تصميم القاعدة المقترحة)، ولكن لا يمكنها الاضطلاع بهذه الأدوار إذا لم يكن لديها أي وعي أو رؤية للمقترحات التي تقدمها الجهات الفاعلة الحكومية وغير الحكومية. فمن الواضح أنه ينبغي على الحكومات والمنظمات الدولية بذل المزيد من الجهود للوصول إلى تلك المجتمعات التي تهدف القواعد المقترحة لمساعدتها.

ج. تنفيذ القواعد

بعد اعتماد هذه القواعد، يتعين على الجهات الفاعلة الحكومية وغير الحكومية اتخاذ خطوات ملموسة لتنفيذ قاعدة ما. يبدو أن هناك توافقًا في الآراء في عمليات الأمم المتحدة الجارية (الفريق العامل المفتوح العضوية وفريق الخبراء الحكوميين) وفي الجهود الإقليمية التي تعتبر عملية تنفيذ القواعد ذات أولوية.[46] وبالنسبة للبعض، يشير التنفيذ إلى اعتماد القاعدة، أو المشاركة في جهود بناء القدرات وتدابير بناء الثقة، أو التوصل إلى توافق أكثر دقة في الآراء حول معنى القاعدة المتفق عليه.[47] وعلى الرغم من أن هذه الخطوات تشكل متطلبات أساسية لتنفيذ القواعد، إلا أنها لا تساعد في تنفيذ القواعد ذاتها. على سبيل المثال، في حين أن بناء القدرات يُعد ضرورة أساسية لضمان قدرة البلدان على تأمين نفسها وضمان تمتعها بالقدرة على المشاركة على الصعيد الدولي، يمكن للمرء بناء القدرات دون اعتماد القواعد أو تنفيذها. وعلى غرار ذلك، في حين أن تدابير بناء الثقة يمكن أن تساعد في الحفاظ على استقرار الفضاء السيبراني من خلال تيسير تبادل وجهات النظر الوطنية حول العقيدة السيبرانية، وإنشاء خطوط ساخنة للتواصل السريع بين الخبراء السيبرانيين الوطنيين، وتشجيع تبادل أفضل الممارسات والمعايير الأمنية، إلا أنه يمكن القيام بذلك أيضًا بدون تنفيذ القواعد. في الواقع، يتطلب تنفيذ قاعدة ما اتخاذ خطوات ملموسة لمنحها القوة اللازمة. وعلى الصعيد المحلي، قد يتضمن ذلك دمج القواعد المقترحة

45 انظر https://www.lexico.com/en/definition/norm.

46 قرار الجمعية العمومية 73/266، ص 3، الفقرة 1(b)، https://undocs.org/ar/A/RES/73/266؛ قرار الجمعية العمومية 73/27، ص 5، الفقرة 5، https://undocs.org/ar/A/ RES/73/27. انظر أيضًا منظمة الأمن والتعاون في أوروبا (OSCE)، *ملاحظات افتتاحية من الأمين العام توماس غريمنغر*، رئاسة مؤتمر الأمن السيبراني/أمن تكنولوجيا المعلومات والاتصالات على مستوى منظمة الأمن والتعاون في أوروبا عام 2019 (براتيسلافا، 2019). "المنظمات الإقليمية... قد تكون حاضنات لأفكار جديدة وجهود عملية تتعلق بـCBMs فضلاً عن كونها منفذ للاتفاقيات المقبولة على الصعيد العالمي، مثل تقارير مجموعة الخبراء الحكوميين (GGE). وبالتالي، فالمنظمات الإقليمية عبارة عن حاضنات وجهات منفذة".

47 تدعو الجمعية العمومية للأمم المتحد جميع الدول الأعضاء، مع الأخذ في الاعتبار التقييمات والتوصيات المضمنة في تقارير مجموعة الخبراء الحكوميين ومجموعة العمل المفتوحة (OEWG)، إلى مواصلة إخبار الأمين العام بوجهات نظرهم وتقييمهم بخصوص *من بين أمور أخرى* "الجهود المبذولة على المستوى الوطني لتعزيز أمن المعلومات والتشجيع على التعاون الدولي في هذا المجال" و"الإجراءات المحتملة التي قد يتخذها المجتمع الدولي لتعزيز أمن المعلومات على الصعيد العالمي". انظر تقرير الأمين العام للأمم المتحدة 74/120، https://undocs.org/A/74/120. لمزيد من وجهات النظر الوطنية للدول الأعضاء، انظر، https://www.un.org/disarmament/ict-security/.

في السياسة الوطنية، والتشريعات، والعقيدة العسكرية. وعلى الصعيد الدولي، قد يتضمن ذلك الاستشهاد بأحكام قاعدة ما عند عزو الهجمات السيبرانية إلى مصادرها الحقيقية أو اتخاذ إجراءات دبلوماسية. كما أن تفعيل قاعدة بهذه الطريقة من شأنه أن يمنحها تعريفًا أكثر دقة.

د. المساءلة

بمجرد اعتماد القواعد وتنفيذها، يجب خضوع أولئك الذين ينتهكون هذه القواعد للمساءلة. ويثير ذلك القضايا المعقدة المرتبطة بتحديد المسؤولية والاستجابة، وقد أثبت كل منهما أنه يمثل تحديًا في التعامل مع الهجمات السيبرانية.

إن دعم الادعاء بأن جهة فاعلة حكومية أو غير حكومية تتصرف بشكل خاطئ يتطلب إسناد المسؤولية بشكل جدير بالثقة. ويبدأ ذلك بجمع الأدلة وتحليلها، ويوجد أيضًا عمل تقني وإجرائي يمكن القيام به الآن لتحسين جودة إسناد المسؤولية وتوقيتها. وبشكل أكثر تحديدًا، كما هو الحال مع التخصصات التقنية الأخرى، يُعد وجود بروتوكولات مقبولة جيدًا لجمع الأدلة وتحليلها أمرًا هامًا لتحسين جودة التحقيقات. وبالتالي، يُعد توحيد أساليب التحقيق أمرًا هامًا لأنه قد يقلل من المخاوف المتعلقة بسلامة الأدلة، حتى وإن كان يجب تحديد الإسناد على أساس كل حالة على حدة. وبالإضافة إلى تحسين عملية إسناد المسؤولية كمسألة تقنية، هناك الكثير الذي يمكن القيام به لتقصير العمليات البيروقراطية المرتبطة باتخاذ قرارات الإسناد، ثم الكشف عنها عند الاقتضاء. ويرجع سبب التأخير الطويل في كثير من الأحيان بين الحدث وإعلان المسؤولية، بشكل كبير، إلى العمليات غير الواضحة أو غير العملية التي يتم إجرائها للتوصل إلى مثل هذه القرارات على المستوى الوطني، ويتفاقم هذا الوضع عند مشاركة عدة بلدان في إصدار بيانات جماعية عن إسناد المسؤولية. وقد يؤدي تصميم العمليات وممارستها للوصول إلى الإسناد على المستوى الوطني والمستوى الدولي، وتحسين تبادل المعلومات بين البلدان، إلى تحسين توقيت بيانات الإسناد وفعاليتها بشكل كبير وتيسير اتخاذ أي إجراء آخر مناسب.

وحتى بعد أن تشير الأدلة إلى جهة فاعلة معينة، قد تظل الخطوة التالية (الإسناد) تشكل تحدياً كبيرًا. في الماضي، أكدت بعض الجهات الفاعلة الحكومية وغير الحكومية على أن الإسناد أمرًا مستحيلًا أو يتطلب دليلًا مطلقًا. ولكن الدليل المطلق ليس مطلوبًا، وعلى الرغم من أن الإسناد قد يكون صعبًا، إلا أنه ليس مستحيلًا كما اقترح البعض. في سياق الدولة القومية، غالبًا ما يكون الإسناد عملًا سياسيًا، سواء في المجال السيبراني أو المادي، وعلى الرغم من عدم الاتفاق على معيار الإثبات بشكل خاص، لا تزال الدول لديها حافز قوي لعدم تقديم ادعاءات زائفة خشية أن تفقد مصداقيتها. باختصار، يجب أن يكون الإسناد مقنعًا للدول الأخرى وللجمهور.

حتى إذا اقتنع الطرف المتضرر بمسؤولية جهة فاعلة معينة (وقد حدث الإسناد في حالات دولية)، فقد تم إثبات أن مساءلة الجهات الفاعلة الحقيقية تُشكل تحديًا صعبًا أيضًا، مما يقلل من قيمة القواعد. وفي النهاية، إذا لم تكن هناك عواقب سلبية على أولئك الذين ينتهكون القواعد المقبولة، تصبح هذه القواعد مجرد كلمات على الورق ومن غير المرجح أن تثبط الأنشطة المزعزعة للاستقرار.

تُعد المساءلة عن الهجمات السيبرانية التي تشنها الجهات الفاعلة غير الحكومية واضحة نسبياً ويتم تحقيقها بشكل سائد من خلال فرض المسؤولية المدنية أو الجنائية بموجب القوانين المحلية للدول المعنية. ولا شك أن القيام بذلك ينطوي على العديد من التحديات، حيث أن الطبيعة الدولية للعديد من الهجمات السيبرانية والتحديات الفنية في جمع الأدلة قد تشكل عقبات تحول دون إجراءات الدولة. ولكن تعتبر سبل المضي قدمًا واضحة من الناحية النظرية: فهي تتمثل في تبسيط عمليات فرض القانون الدولي والعمل على ضمان تحديد المجرمين السيبرانيين ومحاكمتهم.

تُشكل مساءلة الدول عن انتهاكات القواعد تحديًا أكثر صعوبة.[48] وذلك لأن الرد على الهجمات في الفضاء السيبراني يعتمد بشكل كبير على السياق. وفيما يتعلق بما إذا كانت المساءلة مطلوبة، سوف تنظر الجهات الفاعلة الحكومية وغير الحكومية في أربعة عوامل مختلفة؛ على سبيل المثال، قد تنظر الدولة التي تستجيب لانتهاكات القواعد في العواقب السياسية بينما قد تنظر شركة من القطاع الخاص في العواقب المترتبة على الأعمال التجارية أو الإضرار بالسمعة. أما عن كيفية معالجة انتهاكات القواعد، فيمكن اعتبار إجراءات الدولة المتاحة استجابة لانتهاكات القواعد في مسار متواصل، حيث إن الاستجابة قد تكون بسيطة (على سبيل المثال، شكوى خاصة) أو مهمة (على سبيل المثال، العقوبات الاقتصادية) أو درامية (على سبيل المثال، استجابة حركية مرئية بشكل كبير). وعلى الرغم من أن حجم الاستجابة لهذه الانتهاكات غير ملائم ولن يكون كذلك، فمن الواضح أنه يجب أن تكون هناك عواقب مجدية على انتهاكات القواعد والقانون الدولي. وبما أن الجهود السابقة التي تهدف إلى إنفاذ القواعد قد حققت نجاحًا محدودًا، هناك حاجة إلى استجابات أكثر فعالية في الوقت المناسب، مع التسليم بأن هذه الاستجابات يجب أن تسعى إلى تقليل المزيد من عدم الاستقرار إلى أدنى حد.

48 قد تتحمل الدول المسؤولية عن العمليات السيبرانية التي تنفذها أو توجهها أو تسمح بها. كما قد يثبت مبدأ العناية الواجبة فائدته في تحديد مستوى العناية المطلوبة من الدول في الفضاء السيبراني. جوانا كوليزا، *العناية الواجبة في القانون الدولي*، (ليدن: بريل نيجوف، 2016)، https://doi.org/10.1163/9789004325197. انظر أيضًا، *مقالات حول مسؤولية الدول عن الأفعال غير المشروعة دوليًا*، المتبناة من قبل لجنة القانون الدولي في جلستها الثالثة والخمسين في 2001، الملحقة بقرار الجمعية العمومية 56/83 بتاريخ 12 ديسمبر 2001، والمصححة بموجب المستند A/56/49(Vol I)/Corr4، المواد 4 و11، http://legal.un.org/ilc/texts/instruments/draft_arti-cles/9_6_2001.pdf.

وتعمل الجهات الفاعلة غير الحكومية أيضاً على ضمان مساءلة منتهكي القواعد على أفعالهم. على سبيل المثال، يجمع المنتدى العالمي للخبرات السيبرانية[49] بين الحكومة والمجتمع المدني وأعضاء القطاع الخاص للمساعدة في تنسيق الجهود الرامية إلى بناء القدرات، وهو شرط أساسي ضروري لاعتماد القواعد وتنفيذها والمساءلة. فضلًا عن ذلك، اضطلع القطاع الخاص بدور موسع في عزو الهجمات، باستخدام كل من المعلومات الخاصة والعامة لكشف الجهات الفاعلة ووصف الأضرار التي أحدثتها. وأخيرًا، اقترحت بعض كيانات القطاع الخاص أو أطلقت جهودًا، مثل "معهد سايبر بيس (معهد السلام السيبراني)"[50] الذي تم تصميمه لمراقبة الأحداث السيبرانية الضخمة وكشف هذه الأحداث بطريقة أكثر منهجية وربما على نطاق أوسع.

يجب على الجهات الفاعلة غير الحكومية لعب دور أكبر في محاسبة المخالفين عن الانتهاكات. تجدر الإشارة إلى أن فكرة إنفاذ معايير القطاع الخاص ليست جديدة: ففي 1977، على سبيل المثال، وخلال النضال ضد الفصل العنصري في جنوب أفريقيا، روجت جنرال موتورز لمجموعة من المبادئ المعتمدة على نطاق واسع لتنفيذ العمل (وعدم تنفيذ العمل) في هذه البلد، مما أدى إلى سحب استثمارات ما يزيد عن 125 شركة أجنبية.[51] ومؤخرًا، وبطريقة أكثر رمزية، استجابت العديد من الشركات (والحكومات) لقتل السعودية للصحفي المعارض جمال خاشقجي عن طريق مقاطعة مبادرة الاستثمار المستقبلية كرسالة للرفض.[52]هذه الأنواع من الجهود بحاجة لمزيد من الفحص.

هـ- مجتمعات المصالح

بالرغم من أهمية نهج أصحاب المصالح المتعددين المتعلق بتبني المعايير وتنفيذها والمحاسبة عنها، إلا أن تضافر طاقات وقدرات هذه المجموعات يشكل تحديًا. فكثيرًا ما تستخدم الحكومات المصطلح "الأمم ذات التفكير المتماثل" للإشارة إلى مجموعة من الدول لها وجهات نظر مماثلة، إلا أنه لا يوجد مصطلح مرادف يشمل مجموعة من الدول، الشركات الخاصة، المنظمات غير الربحية (بما في ذلك منظمات المعايير)، المجتمعات المدنية، والشخصيات التي تتشارك وجهات نظر بخصوص موضوع معين. وهذا ضروري لأن المعايير التي اقترحت من قبل مجموعة الخبراء الحكوميين التابعين للأمم المتحدة (UN GGE) واللجنة العالمية لاستقرار الفضاء السيبراني (GCSC) قد تؤثر على الدوائر الانتخابية المختلفة، وقد تهتم منظمات مختلفة وأفراد بالمجتمع بالدعوة إلى معايير معينة أكثر من غيرها.

بما أن الحكومات، القطاع الخاص، المجتمع الفني، الأوساط الأكاديمية، والمجتمع المدني ليست كيانات متجانسة، فمن الضروري التفكير في كيفية إيجاد جهد منسق في مقابل الجهد المركز، الجهد الذي يشرك المجتمعات المتنوعة في مشاكل ذات صلة بالمعايير.[53] يعمل إيجاد مجتمعات المصالح على السماح لمن يمتلكون الخبرة في معايير معينة بالعمل على مواصلة التطوير والتنفيذ. على سبيل المثال، قد تهتم فرق الاستجابة لطوارئ الكمبيوتر (CERTs/CSIRTs) تحديدًا بتنفيذ معيار مجموعة الخبراء الحكوميين التابعين للأمم المتحدة الموجه نحو حماية المجتمع ومراقبته، كما قد يهتم المسؤولون عن النظم الانتخابية تحديدًا بمعيار اللجنة العالمية لاستقرار الفضاء السيبراني الخاص بالنظم الانتخابية. بالمثل، قد تساعد سحابة مجتمع الإنترنت على تقدم، تنفيذ، ومراقبة المعيار المقترح من اللجنة لحماية النواة العامة للإنترنت، وقد يهتم المطورون أكثر بالمعيار المتضمن للتلاعب بالمنتج.

قد يكون تكوين مجتمع المصالح موجهًا أو مخصصًا، عملية تصاعدية. حقيقة أن الأعضاء أنفسهم قد يشكلون مجتمعًا لا تشير إلى ضرورة ترك تطورهم ونجاحهم للصدفة. بل من الضروري التركيز على ما يجعل المجتمع ناجحًا: (1) المبادئ المشتركة؛ (2) التركيز على المشكلة؛ (3) الخبرة بالموضوع؛ (4) الدعم المالي والإداري؛ و(5) شفافية العملية. في الحقيقة، من الممكن تحديد قالب أفضل ممارسة لكيفية إيجاد وتنفيذ المجتمعات، مما يسمح بعمليات تحديد المعايير المختلفة لتحسين نموذج مجتمع مماثل. وهذا من شأنه أن يساعد في تسوية مسارات العمل المختلفة لضمان الكفاءة والتركيز، فضلاً عن تحسين أفضل الممارسات لتبني المعايير، وتنفيذها، والمحاسبة عليها.

49 المنتدى العالمي للخبرة السيبرانية، https://www.thegfce.com/.
50 معهد سايبر بيس، https://cyberpeaceinstitute.org/.
51 انظر، بشكل عام، "مبادئ سوليفان"، ويكيبيديا، 12 أغسطس 2018، https://en.wikipedia.org/wiki/Sullivan_principles.
52 انظر "المقاطعة الغربية لمبادرة الاستثمار المستقبلي 2018"، *رويال نيوز*، 16 أكتوبر 2018، https://en.royanews.tv/news/15500/2018-10-16.
53 انظر، بشكل عام، *عصر الاستقلال الرقمي*، https://digitalcooperation.org/wp-content/uploads/2019/06/DigitalCo-operation-report-for-web.pdf.

7. التوصيات

تتدفق توصياتنا الست الخاصة بضمان استقرار الفضاء السيبراني من مبادئنا المتعلقة بالمسؤولية، التقيد، شرط العمل، واحترام حقوق الإنسان. وبما أن الجميع مسؤولون عن، ونهج أصحاب المصالح المتعددين هام، ضمان استقرار الفضاء السيبراني، فإن توصياتنا تسعى أيضًا لتحسين قدرات الجهات الفاعلة الحكومية وغير الحكومية، بشكل جزئي من خلال مجتمعات المصالح. باختصار، نحن نركز على مت يجب القيام به وكيف يمكن القيام به.

1. **يجب على الجهات الفاعلة الحكومية وغير الحكومية تبني وتنفيذ معايير تزيد من استقرار الفضاء السيبراني عن طريق تعزيز التقيد وتشجيع العمل.** يجب على الجهات الفاعلة الحكومية التي وافقت في السابق على المعايير أن تكون أكثر وضوحًا في تحديد المصطلحات المستخدمة، والنتيجة التي يمكن تحقيقها من خلال المزيد من المفاوضات ومن خلال الخبرة العملية في تنفيذ المعايير الحالية. ويجب على الجهات الفاعلة الحكومية وغير الحكومية تقديم دليل واضح على تبني وتنفيذ المعايير من خلال البيانات العامة، ومن خلال التغييرات في السياسة والفعل.

2. **يجب أن تستجيب الجهات الفاعلة الحكومية وغير الحكومية، بما يتسق مع مسؤولياتها وقيودها، بشكل مناسب لانتهاكات المعايير، لضمان مواجهة من ينتهكون المعايير لعواقب متوقعة وذات مغزى.** لن يكون تطوير وتنفيذ المعايير فعالاً في حال معرفة من ينتهكون هذه المعايير بعدم وجود ثمن للقيام بذلك. لذا، يجب على الجهات الفاعلة الحكومية وغير الحكومية تطوير القدرات الداخلية لتقييم الانتهاكات وتحديد واتخاذ الاستجابات الفردية والجماعية المناسبة على وجه السرعة، بما يتسق مع مبدأ شرط العمل.

3. **يجب على الجهات الفاعلة الحكومية وغير الحكومية، بما في ذلك المؤسسات الدولية، زيادة الجهود لتدريب الموظفين، بناء القدرات والإمكانيات، تعزيز الفهم المشترك لأهمية استقرار الفضاء السيبراني، والأخذ في الاعتبار الاحتياجات المتباينة للأطراف المختلفة.** زيادة القدرات والإمكانيات والفهم من شأنه أن يزيد من قدرة العالم على تنفيذ القوانين الدولية، والمعايير، وغيرها من إجراءات بناء الثقة المُصممة لتحسين استقرار الأمن السيبراني مع احترام حقوق الإنسان. ويجب على جميع الأطراف تحسين المنظمات الحالية، بما في ذلك المنتدى العالمي لأصحاب المصالح المتعددين بخصوص الخبرة السيبرانية، التي تركز على بناء القدرات لكونه متطلب أساسي لتبني وتنفيذ المعايير، مما يضمن المساءلة، اتخاذ إجراءات الاستقرار الأخرى، واحترام حقوق الإنسان.

4. **يجب على الجهات الفاعلة الحكومية وغير الحكومية جمع، مشاركة، مراجعة، ونشر المعلومات المتعلقة بانتهاكات المعايير وأثر هذه الأنشطة.** بالرغم من أن العالم شهد إجراءات تشكل انتهاكًا للمعايير الواردة في الأمم المتحدة والمقترحة من قبل اللجنة العالمية لاستقرار الفضاء السيبراني، إلا أن التقارير تميل إلى كونها سردية وليست شاملة. ويجب على المنظمات، لاسيما تلك المستقلة عن أي مصلحة حكومية أو تجارية، جمع ونشر المعلومات المتعلقة بانتهاكات المعايير وآثارها بشكل منهجي. فمن شأن القيام بذلك أن يحفز الاستجابات من قبل الجهات الفاعلة الحكومية وغير الحكومية لانتهاكات المعايير وأن يحسّن الامتثال للمعايير.

5. **يجب على الجهات الفاعلة الحكومية وغير الحكومية تأسيس ودعم مجتمعات المصالح للمساعدة على ضمان استقرار الفضاء السيبراني.** من شأن تأسيس ودعم المجتمعات أن يضمن تلبية كل الأطراف المهتمة ومنها الحكومات، القطاع الخاص، المجتمع الفني، الأوساط الأكاديمية، والمجتمع المدني لكل مسؤولياتها لضمان استقرار الفضاء السيبراني. ويمكن لهذه المجتمعات التركيز، من بين أمور أخرى، على تفسير، تبني، وتنفيذ معايير الأمن السيبراني المنصوص عليها في هذا التقرير وفي أي مكان آخر، سواء كانت معايير الإثبات الخاصة بالإسناد قوية أم لا، وسواء كان منتهكو المعايير يحاسبون في الوقت المناسب وبطريقة فعالة أم لا.

6. **توصي اللجنة العالمية لاستقرار الفضاء السيبراني بتحديد آلية دائمة لمشاركة أصحاب المصالح المتعددين لمعالجة مشاكل الاستقرار، آلية تتم فيها الحكومات، القطاع الخاص (بما في ذلك المجتمع الفني)، والمجتمع المدني بالمشاركة والتشاور كما ينبغي.** يسلّم مبدأ المسؤولية بأن للجميع دور يلعبه في ضمان استقرار الفضاء السيبراني كما يعزز الحاجة لطرق أصحاب المصلحة المتعددين. من 2011-17، وفر المؤتمر العالمي للفضاء السيبراني (GCCS) منصة واحدة لهذه المشاركة جذبت مشاركين على المستوى الوزاري من وزارات أجنبية وأمنية كُلفت بتحقيق الاستقرار العالمي في سياقات أخرى، كما كان بمثاب نقطة الانطلاق للمنتدى العالمي للخبرة السيبرانية، محاولة هامة لبناء القدرات. كما وفر منتدى حوكمة الإنترنت (IGF) منصة هامة لمناقشة أصحاب المصلحة المتعددين. ومؤخرًا، جمعت دعوة باريس بين أكبر مجتمع لأصحاب المصلحة المتعددين على الإطلاق من الداعمين لمعايير الأمن السيبراني. تشير هذه المحاولات إلى أن الوقت قد حان لتطوير مجتمع أصحاب مصلحة متعددين عالمي وشامل وموجه نحو العمل يركز على التنفيذ العملي لمعايير الأمن السيبراني الواردة في هذا التقرير وأي مكان آخر. ويجب دعم الآلية من قبل كيان دائم لضمان استدامة واستمرار المحاولة.

الملحق أ:
المعايير المتبناة من قبل مجموعة الخبراء الحكوميين التابعين للأمم المتحدة[54]

أ- بما يتسق مع أغراض الأمم المتحدة، ومنها الحفاظ على السلام والأمن الدولي، يجب على الولايات التعاون لإعداد وتطبيق إجراءات لزيادة الاستقرار والأمن عند استخدام تكنولوجيا المعلومات والاتصالات ولمنع ممارسات تكنولوجيا المعلومات والاتصالات المعترف بكونها ضارة أو التي قد تفرض تهديدات على السلام والأمن الدولي؛

ب- في حالة حوادث تكنولوجيا المعلومات والاتصالات، يجب على الدول النظر في كل المعلومات ذات الصلة، ومنها السياق الأكبر للحدث، وتحديثات الإسناد إلى بيئة تكنولوجيا المعلومات والاتصالات وطبيعة ومدى العواقب؛

ج- يجب على الدول عدم السماح عن علم باستخدام أراضيها لأفعال غير مشروعة دوليًا باستخدام تكنولوجيا المعلومات والاتصالات؛

د- يجب على الدول التفكير في أفضل طريقة للتعاون من أجل تبادل المعلومات، ومساعدة بعضها البعض، وملاحقة الإرهابيين والاستخدام الجنائي لتكنولوجيا المعلومات والاتصالات وتنفيذ الإجراءات التعاونية الأخرى لمعالجة هذه التهديدات. وقد تحتاج الدول إلى التفكير في إذا ما كانت الإجراءات الجديدة بحاجة إلى التطوير في هذا الصدد أم لا؛

هـ- لضمان أمن استخدام تكنولوجيا المعلومات والاتصالات، يجب على الدول احترام قرارات مجلس حقوق الإنسان 20/8 و26/13 عند الترويج لحقوق الإنسان على الإنترنت وحمايتها والاستمتاع بها، فضلاً عن قرارات الجمعية العمومية 68/167 و69/166 المتعلقة بحق الخصوصية في العصر الرقمي، لضمان الاحترام التام لحقوق الإنسان، ومنها الحق في حرية التعبير؛

و- يجب على الدولة ألا تقوم بتنفيذ أو دعم نشاط من أنشطة تكنولوجيا المعلومات والاتصالات مخالف لالتزاماتها بموجب القانون الدولي من شأنه أن يضر عمدًا بالبنية التحتية الحرجة أو يعيق استخدام وتشغيل البنية التحتية الحرجة لتوفير خدمات للعامة؛

ز- يجب على الدول اتخاذ الإجراءات المناسبة لحماية بنيتها التحتية الحرجة من تهديدات تكنولوجيا المعلومات والاتصالات، مع الأخذ في الاعتبار قرار الجمعية العمومية 58/199 بخصوص تكوين ثقافة عالمية عن الأمن السيبراني وحماية بنية المعلومات الحرجة، وغيرها من القرارات ذات الصلة؛

ح- يجب على الدول الاستجابة لطلبات المساعدة المناسبة من قبل دولة أخرى تتعرض بنيتها التحتية الحرجة لأفعال تكنولوجيا المعلومات والاتصالات الخبيثة. كما يجب على الدول الاستجابة للطلبات المناسبة لتقليل نشاط تكنولوجيا المعلومات والاتصالات الخبيث الموجه للبنية التحتية الحرجة لدولة أخرى الصادر من أراضيها، مع الأخذ في الاعتبار الاحترام الواجب للسيادة؛

ط- يجب أن تتخذ الدول خطوات معقولة لضمان سلامة سلسلة الإمداد حتى يتمكن المستخدمين النهائيين من الثقة في أمن منتجات تكنولوجيا المعلومات والاتصالات. ويجب أن تسعى الدول لمنع انتشار أدوات وتقنيات تكنولوجيا المعلومات والاتصالات الخبيثة واستخدام الوظائف المخفية؛

ي- يجب أن تشجع الدول الإبلاغ عن نقاط ضعف تكنولوجيا المعلومات والاتصالات المسؤولة وأن تشارك المعلومات ذات الصلة المتعلقة بسبل الانتصاف المتوفرة لنقاط الضعف هذه للحد وربما التخلص من التهديدات المحتملة لتكنولوجيا المعلومات والاتصالات والبنية المعتمدة على تكنولوجيا المعلومات والاتصالات؛

ك- يجب ألا تقوم الدول بتنفيذ أو دعم نشاط للإضرار بنظم المعلومات الخاصة بالفرق المعتمدة للاستجابة للطوارئ (تُعرف في بعض الأحيان بفرق الاستجابة لطوارئ الكمبيوتر أو فرق الاستجابة لحوادث الأمن السيبراني) بدولة أخرى. ويجب ألا تقوم الدولة باستخدام الفرق المعتمدة للاستجابة للطوارئ للمشاركة في نشاط دولي خبيث.

54 انظر الجمعية العمومية للأمم المتحدة، *تقرير مجموعة الخبراء الحكوميين عن التطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي*، A/70/174 (22 يوليو 2015)، https://undocs.org/A/70/174.

الملحق ب:
معايير اللجنة العالمية لاستقرار الفضاء السيبراني

1. عدم التدخل في النواة العامة

المعيار:

يجب على الجهات الفاعلة الحكومية وغير الحكومية عدم تنفيذ أو السماح عن علم بنشاط يضر عمدًا وبشكل كبير بالتوافر العام أو سلامة النواة العامة للإنترنت، ومن ثم استقرار الفضاء السيبراني.

نبذة

يُشكل تعريف النواة العامة للإنترنت تحديًا وذلك لأن العديد من أنواع الهجمات المختلفة قد يؤدي في النهاية إلى إعاقة التوافر العام أو سلامة الإنترنت بشكل عام (النتيجة التي يجب تجنبها). وقد تكون هناك مكونات معينة بشكل واضح يستهدفها المرء إذا أراد إحداث هذا التأثير الكبير ومن الممكن على الأقل توفير قائمة غير حصرية بهذه العناصر الحرجة. تُعرف اللجنة، عند أعلى مستوياتها، القصد من عبارة "التوافر العام" بأن سلوك الجهات الفاعلة له تأثير جوهري على عامة السكان. لذا، يسلّم هذا المعيار بأن تلك الدول الداعمة لهذا المعيار قد تستمر في الانخراط في الأنشطة الأكثر محدودية في الغرض والنطاق وليس لها تأثير جوهري على عامة السكان.

وتُعرّف اللجنة عبارة "النواة العامة للإنترنت" لتتضمن هذه العناصر الحرجة للبنية التحتية للإنترنت مثل توجيه وإعادة توجيه الحزمة، نظم التسمية والترقيم، آليات تشفير الأمن والهوية، وسائط الإرسال، ومراكز البيانات.

تتضمن عناصر توجيه وإعادة توجيه الحزمة، على سبيل المثال لا الحصر، (1) المعدات، والمرافق، والمعلومات، والبروتوكولات، والنظم التي تيسر إرسال الاتصالات المجمعة في حزمة من مصادرها إلى وجهاتها؛ (2) ونقاط تبادل الإنترنت (المواقع المادية حيث يتم إنتاج عرض النطاق الترددي للإنترنت)؛ (3) وموجهات الإقران والنواة للشبكات الرئيسية التي تنقل عرض النطاق الترددي هذا إلى المستخدمين؛ (4) والنظم اللازمة لضمان أصالة التوجيه والدفاع عن الشبكة ضد السلوك المسيء؛ (5) وتصميم وإنتاج وسلسلة إمداد المعدات المستخدمة للأغراض أعلاه؛ (6) وسلامة بروتوكولات التوجيه ذاتها وعمليات تطويرها وتوحيدها وصيانتها.

تتضمن نظم التسمية والترقيم، على سبيل المثال لا الحصر، (1) النظم والمعلومات المستخدمة في عملية نظام اسم نطاق الإنترنت (بما في ذلك السجلات، خوادم الاسم، محتوى المنطقة، البنية التحتية والعمليات مثل الامتدادات الأمنية لنظام اسم النطاق (DNSSEC) المستخدمة لتسجيل السجلات بطريقة مشفرة)؛ (2) وخدمات معلومات WHOIS لمنطقة الجذر، تسلسل العنوان المعكوس، كود البلد، الجغرافية، ونطاقات المستوى الأعلى الدولية ونطاقات المستوى الأعلى العامة الجديدة والعامة غير العسكرية؛ (3) ومحللات DNS المتكرر العام المستخدم بشكل متكرر؛ (4) ونظم هيئة الأرقام المخصصة للإنترنت وسجلات الإنترنت الإقليمية التي توفر وتحافظ على التوزيع الفريد لعناوين بروتوكول الإنترنت، وأرقام النظام المستقل، ومعرفات بروتوكول الإنترنت؛ (5) وبروتوكولات التسمية والترقيم ذاتها وسلامة العمليات والنتائج الموحدة لتطوير وصيانة البروتوكول.

تتضمن آليات تشفير الأمن والهوية، على سبيل المثال لا الحصر، (1) مفاتيح التشفير المستخدمة لمصادقة المستخدمين والأجهزة وتأمين معاملات الإنترنت؛ (2) المعدات، والمرافق، والمعلومات، والبروتوكولات، والنظم التي تمكن من إنتاج، نقل، استخدام، وإلغاء هذه المفاتيح؛ (3) خوادم PGP الرئيسية، هيئات التصديق والبنية التحتية الرئيسية العامة الخاصة بها؛ (4) DANE والبروتوكولات والبنية التحتية الداعمة له؛ (5) وآليات إلغاء الشهادة وسجلات الشفافية؛ (6) مديري كلمة المرور؛ (7) وموثقي الوصول إلى التجوال؛ (8) وآليات الوقت الدقيق وتأكيد الأسبقية الزمنية، مثل بروتوكول وقت الشبكة وبنيته التحتية؛ (9) وسلامة عمليات ونتائج التوحيد بالنسبة لخوارزمية التشفير وتطوير وصيانة البروتوكول؛ و(10) وتصميم وإنتاج وسلسلة إمداد المعدات المستخدمة لتنفيذ عمليات التشفير.

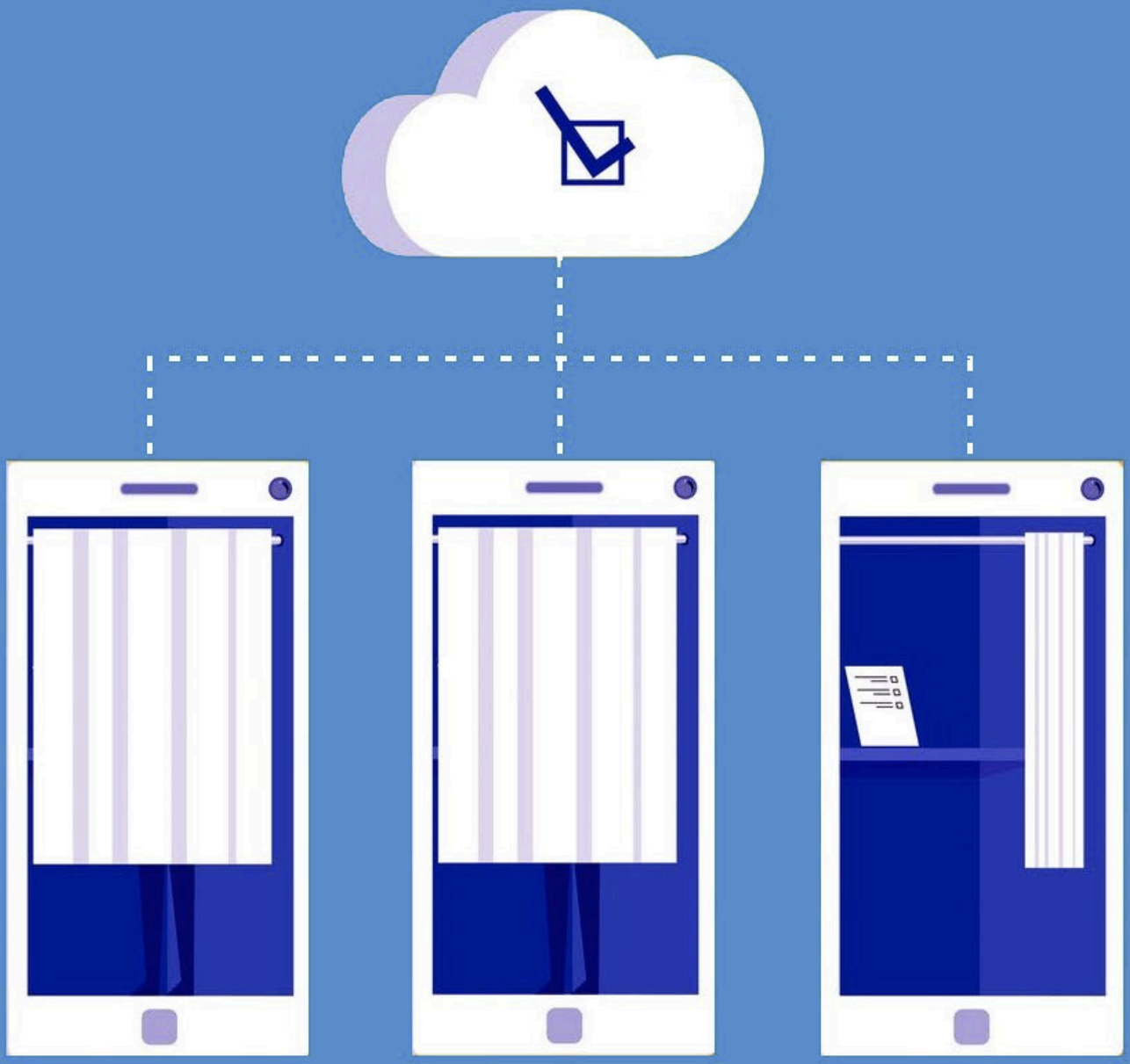
تتضمن وسائط الإرسال، على سبيل المثال لا الحصر، (1) البنية التحتية، النظم والتجهيزات الخاصة بالاتصالات التي تخدم العامة، سواء كانت ألياف أو نحاس أو لاسلكية؛ (2) والكابلات الأرضية أو الموجودة تحت سطح البحر والمحطات البرية، مراكز البيانات، وغيرها من المرافق المادية التي تدعمها؛ (3) واتصالات الصوت والبيانات الخلوية واللاسلكية الأخرى؛ (4) والاتصالات البث المنظمة وغير المنظمة؛ (5) ونظم الدعم الخاصة بالإرسال، إعادة توليد الإشارة، والتفريع، والمضاعفة، وتمييز الإشارة من الضوضاء؛ (6) ونظم الكابلات التي تخدم المناطق أو السكان، وليس التي تخدم عملاء الشركات الفردية.

تتضمن البرامج، على سبيل المثال لا الحصر، توافر وسلامة عمليات التطوير، والتعليمة البرمجية وتصحيح البنية التحتية للتوزيع بالنسبة للبرامج المستخدمة في نواة الإنترنت وبواسطة أجزاء كبيرة من العامة المستخدمين للإنترنت.

تتضمن مراكز البيانات، على سبيل المثال لا الحصر، (1) المرافق المادية التي تضم الخوادم، المحتوى، والبنية التحتية للإنترنت؛ (2) والنظام المستخدم لضمان سلامة مركز البيانات وأمنه ومراقبة الوصول المادي إليه وعملياته وإدارته وصيانته ووفرة أنظمته؛ و(3) نظم الاتصالات المستخدمة لإرسال الاتصالات إلى، من وداخل مراكز البيانات.

يعتقد الخبراء أن فئات أكثر بكثير من البنية التحتية المدعومة بالإنترنت وتكنولوجيا المعلومات والاتصالات تستحق الحماية، وبالتالي فقد يتسع هذا التعريف في المستقبل.

2. حماية البنية التحتية الانتخابية



المعيار:

تلتزم الجهات الحكومية وغير الحكومية بعدم السعي إلى العمليات السيبرانية التي تهدف إلى تعطيل البنية التحتية التقنية اللازمة لإجراء الانتخابات أو الاستفتاءات أو دعمها أو السماح بها.

نبذة

من جميع القواعد والتعاليم والمبادئ التي توجه سلوك الدول في مجاملة الأمم، ربما يكون مبدأ عدم التدخل هو الأكثر قداسة. فالمادة 2 (4) من ميثاق الأمم المتحدة تتكلم عن هذا المعيار بوضوح وترفعه إلى مبدأ الصفة القانونية، وبالتالي، الملزمة:

> يجب على جميع الأعضاء الكف في علاقاتهم الدولية عن التهديد بالقوة أو استخدامها ضد السلامة الإقليمية أو الاستقلالية السياسية لأي دولة، أو بأي طريقة أخرى لا تتسق مع أغراض الأمم المتحدة.

من خلال هذا النص، أقر معدو الميثاق بأن أخط التهديدات لمبدأ عدد التدخل يأتي من الإجراءات القسرية الموجهة إلى استقلالية الدولة المادية أو السياسية، لأن كلاهما، في الحقيقة، ضروري لسيادة الدولة. فالأراضي الخاضعة لسيطرة الدولة قد تعبر عن قدرتها السيادية، إلا أنه لا قيمة لها بدون الاستمتاع بالوكالة والاستقلالية السياسية. كما أنه لا شيء يعكس الاستقلالية السياسية الحقيقية أكثر من العمليات التشاركية الوطنية، مثل الانتخابات، التي تتم بحرية ونزاهة. سعى ميثاق الأمم المتحدة لمنح حماية قوية من التدخل الخارجي غير المقبول.

وتتعرض هذه الإجراءات الوقائية الآن للتحديات مرةً أخرى في العصر الرقمي.

ناقش الخبراء إذا ما كان يُنظر إلى نوع التدخل في الانتخابات ذي الصلة بالإنترنت مؤخرًا على أنه يرقى إلى كونه انتهاكًا غير قانوني للسيادة أم لا (لأنه يتدخل في ممارسة وظيفة حكومية متأصلة).[55] وسواء حدث انتهاكًا للقانون الدولي أم لا، فهناك احتمال واضح يشير إلى أن الجهات الفاعلة الخبيثة—سواء كانت تعمل بمفردها أو معًا أو بالنيابة عند دول—ستتلاعب بالانتخابات بطرق رقمية. بتزايد تعقيد العمليات التشاركية الوطنية من حيث النطاق والتطور، حدث ازدهار في البيانات، المؤسسات والبنية التحتية لإدارتها. حيث تنشر العديد من البلدان الآن قوائمها الانتخابية—ضمان أساسي وتقليدي ضد التلاعب بالتصويت أو الاحتيال—على الإنترنت، مما يعرض قواعد البيانات هذه للهجمات السيبرانية والاستغلال. بالمثل، تُستخدم أدوات التصويت الانتخابي في المناطق النائية والبعيدة من البلد، حيث لا يكون مشغليها على علم تام بالمخاطر والمشاكل ذات الصلة بالتلاعب الرقمي بها. كما أن موردي برامج التصويت ونظم الحاسب على المستوى المحلي أو مستوى "مقصورة التصويت" عرضة لهذه التدخلات.

لتقييد العدد المتزايد من التهديدات الموجهة نحو العمليات التشاركية وللحد من شدتها، واعترافًا بأن هذه الهجمات غير مقبولة، توصي اللجنة العالمية لاستقرار الفضاء السيبراني بتدابير وطنية أقوى وتعاون دولي فعال لمنع التدخلات السيبرانية ضد البنية التحتية الانتخابية الفنية والتخفيف من آثارها والاستجابة لها. تقر اللجنة بأن السلوك الفعلي للانتخابات أو العمليات التشاركية على المستوى الإقليمي أو المحلي أو الفيدرالي من الاختصاصات المتأصلة للدول، التي يجب تنفيذها وفقًا لقوانينها الوطنية ذات الصلة. مع ذلك، قد تنشأ الهجمات السيبرانية على بنيتها التحتية الانتخابية من خارج الحدود، مما يستوجب قرار تعاون متعدد الأطراف. باختيار المزيد من البلدان رقمنة أجهزتها الانتخابية، تزدد وتتعدد المخاطر ونقاط الضعف ذات الصلة بهذه البنية التحتية، وكذلك احتمالية حدوث عملية سيبرانية هجومية كبيرة. لذا، يجب على الحكومات الالتزام بالامتناع عن المشاركة في العمليات السيبرانية ضد البنية التحتية الانتخابية الفنية لدولة أخرى. للتوصية بهذا المعيار، تؤكد اللجنة على أن التدخل في الانتخابات غير مقبول سواء كان ذا صلة بانتهاك القانون الدولي أم لا.

55 انظر مايكل ن. شميت، "الحرمان الافتراضي: التدخل في الانتخابات السيبرانية في المناطق الرمادية من القانون الدولي،" *صحيفة شيكاغو للقانون الدولي*، مجلد 19، رقم 1، ونيكولاس تساجورياس، "التدخل السيبراني في الانتخابات، تقرير المصير ومبدأ عدم التدخل في الفضاء السيبراني"، https://www.ejiltalk.org/electoral-cyber-interfer ence-self-determination-and-the-princi-ple-of-non-intervention-in-cyberspace/.

3. معيار تجنب التلاعب

المعيار:

تلتزم الجهات الحكومية وغير الحكومية بعدم العبث بالمنتجات والخدمات في التطوير والإنتاج، أو السماح بالعبث بها، إذا كان القيام بذلك قد يضعف استقرار الفضاء الإلكتروني على نحوٍ كبير.

نبذة

في معيار يركز على "عدم التدخل في النواة العامة للإنترنت"، دعت اللجنة العالمية لاستقرار الفضاء السيبراني الجهات الفاعلة الحكومية وغير الحكومية إلى عدم الإضرار المتعمد والعرضي بالتوافر العام أو السلامة العامة للنواة العامة للإنترنت. ولدعم هذا المعيار، ذكرت اللجنة الاعتماد المتزايد للبنى التحتية الأخرى على الإنترنت المستقر والآمن والعواقب الوخيمة المحتملة لتعطله. فبالرغم من أن معيار النواة العامة ركز على "نواة الإنترنت"، إلا أن الأفراد والمنظمات يعتمدون بشدة على منتجات تجارية معينة للوصول إلى هذه النواة العامة وتحسين الاتصال الذي توفره. لذلك فإن التلاعب بالمكونات الرئيسية في البرامج ومنتجات تكنولوجيا المعلومات للأجهزة (بما في ذلك، وعلى سبيل المثال لا الحصر، أنظمة التشغيل، ونظم المراقبة الصناعية، والمحولات، الموجهات وغيرها من معدات الشبكة الحرجة، ومنتجات ومعايير التشفير الحرجة، وتصميم الرقاقة وتطبيقات المستهلك الخاصة بالمستخدم النهائي المستخدمة على نطاق واسع) قد يحرم المجتمع كذلك من القدرة على استخدام وتحسين الإنترنت بشكل آمن، وقد يضعف إجمالي الثقة في وظيفته المناسبة. وبالرغم من أن هذه الهجمات ترد كثيرًا في الأخبار، إلا أن ما يحظى باهتمام أقل هو حقيقة أن الهجوم قد يحدث حتى قبل طرح أحد المنتجات أو تحديثه في الأسواق. على سبيل المثال، قد يتعرض أحد المنتجات للهجوم عن طريق إدخال نقطة ضعف—أو حذف ميزة أمنية على نحو سري—خلال مرحلة التصميم والتصنيع أو أثناء إحدى عمليات تحديثه. بعبارة أخرى، قد يتم التلاعب بالمنتج قبل طرحه أو إنتاج، مع عواقب للعامة. قد تختلف الفترة الزمنية بين إدخال نقطة ضعف، وتنشيط نقطة الضعف من أجل الاستخدام الخبيث.

تواجه الدول تعارضًا في المصالح والمسؤوليات عند التعامل مع منتجات تكنولوجيا المعلومات. فمن ناحية، تلتزم الدول بتعزيز مرونة وسلامة البنية التحتية السيبرانية للمساعدة في إحباط الهجمات السيبرانية المستقبلية من قبل الجهات الفاعلة الخبيثة وجعل النظام البيئي الرقمي ككل أكثر أمنًا. ومن ناحية أخرى، تلتزم الدول تجاه مواطنيها بحماية الأمن القومي ومكافحة المجرمين وغيرهم من الجهات الفاعلة الخبيثة الأخرى في الفضاء السيبراني. عززت الدول الاستفادة من نقاط الضعف في المنتجات والخدمات الرقمية المستخدمة من قبل الأعداء لتحقيق النجاح في مهمتها المتعلقة بالأمن القومي والسلامة العامة. وبالتالي، قد تجد الدول أيضًا أنه من المفيد، بقدر اعتبارها الاستفادة من نقاط الضعف نهجًا فعالاً للوفاء بمسؤولياتها، إدخال نقاط ضعف أو أبواب خلفية عند عمد في المنتجات والخدمات المستخدمة من قبل الأعداء. قد تتلاعب الجهات الفاعلة غير الحكومية بدورها بالمنتجات والخدمات، لأن أهدافها قد تكون مدعومة بقدرتها على تعطيل استقرار الفضاء السيبراني. وجدير بالذكر أن المعيار يمنع التلاعب بخط المنتج أو الخدمة، الأمر الذي يعرض استقرار الفضاء السيبراني للخطر. هذا المعيار لن يمنع إجراء الدولة المستهدفة الذي يفرض القليل من الخطر على مجمل استقرار الفضاء السيبراني؛ على سبيل المثال، الاعتراض المستهدف والتلاعب بعدد محدود من أجهزة المستخدم النهائي لتيسير التجسس العسكري أو التحقيقات الجنائية. ومن غير المرجع أن يعمل هذا النوع من الأنشطة، ما لم يحدث داخل البنية التحتية الأساسية للنواة العامة ذاتها، أو يضعف ثقة المستخدم بشكل كبير في الإنترنت على الصعيد العالمي، على إضعاف إجمالي الثقة في الفضاء السيبراني وهو شرط في استقرار الفضاء السيبراني. بالرغم من أن الجهة الفاعلة غير الحكومية قد تستهدف الأنظمة أيضًا بطريقة محدودة، إلا أن هذا النشاط قد ينتهك القوانين الجنائية والمدنية الحالية.

وبالرغم من عدم ثبوت تلاعب الجهات الفاعلة الحكومية وغير الحكومية بالمنتجات في مرحلة التطوير أو الإنتاج، إلا أن الجهات العاملة في الصناعة تقع على عاتقها مسؤولية منع هذه الأسئلة. لذا، يجب على مصنعي المنتجات والخدمات الالتزام بمستوى معقول من العناية لتصميم وتطوير وتسليم منتجات وخدمات تولي الأمن الأولوية وتعمل بدورها على تقليل احتمال نقاط الضعف وتكرارها وإمكانية استغلالها وخطورتها. كما يجب على المعنيين رفض أي محاولات حكومية أو غير حكومية واضحة لتعريض المنتجات والخدمات للخطر، بالإضافة إلى تبني ممارسات تقلل من خطر التلاعب وتسمح لهم بالاستجابة في حال اكتشاف التلاعب.

4. معيار ضد الاستيلاء على الأجهزة في شبكات الروبوت

المعيار:

تلتزم الجهات الحكومية وغير الحكومية بعدم الاستحواذ على موارد تقنية المعلومات والاتصالات الخاصة بعامة الجمهور من أجل استخدامها كشبكات روبوت أو لأغراض مماثلة.

نبذة

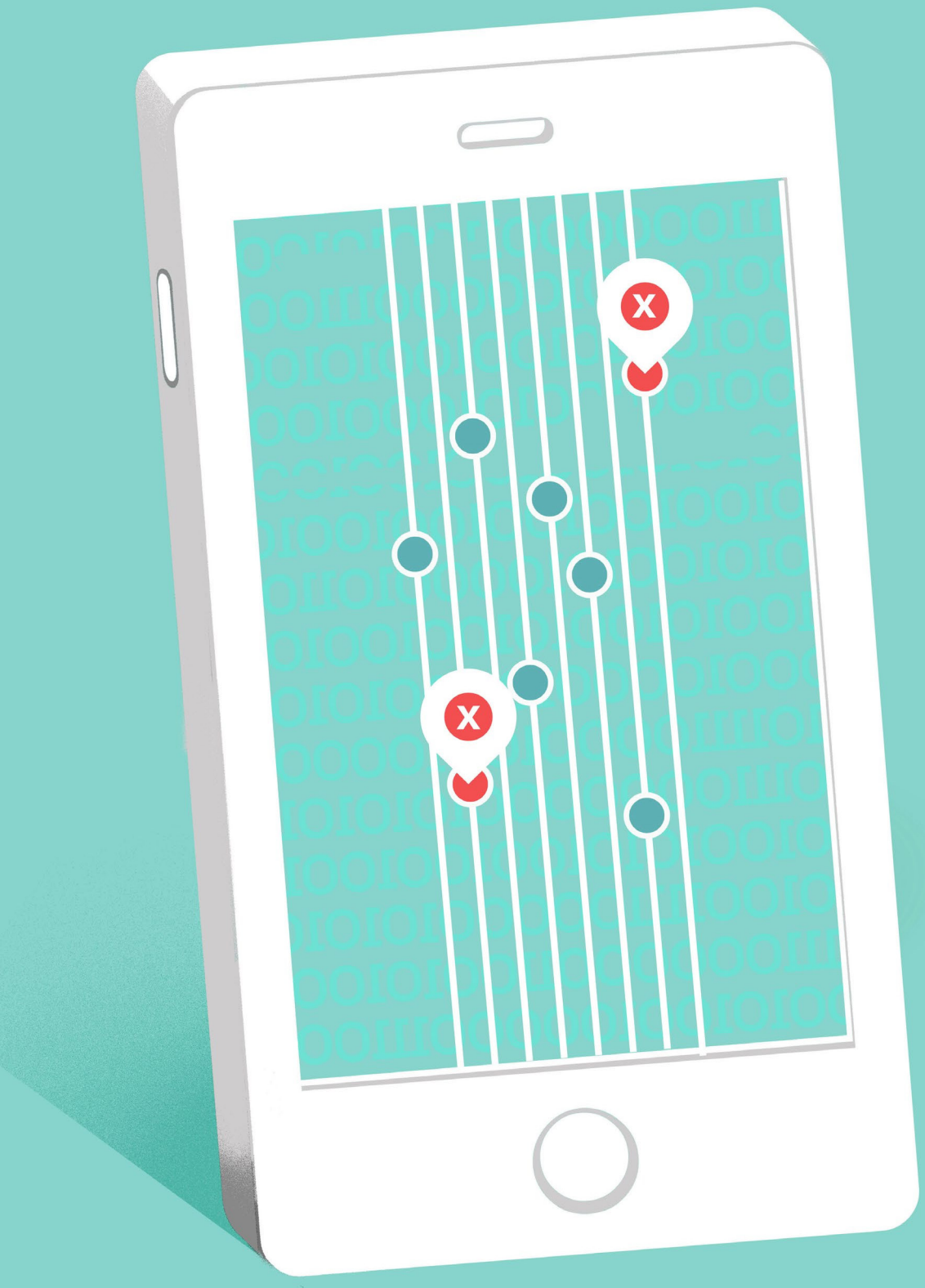
أصبحت الأجهزة المتصلة بالإنترنت جزءًا لا يتجزأ من حياة الناس بجميع أنحاء العالم. فنحن محاطون بأجهزة متعددة القدرات الحسابية والشبكية والحسية والتشغيلية. ومنظمات الحرارة، أجهزة التلفزيون، الأجهزة الطبية، ساعات التنبيه والسيارات تحتوي قدرات خاصة بالحوسبة والتخزين والشبكات يمكن الاستيلاء عليها أو إساءة استخدامها. قد يؤدي استغلال نقاط الضعف في الرمز الأساسي لها إلى مشاكل في السلامة المادية بالنسبة للأفراد المستخدمين للجهاز: جهاز يعمل خارج معايير تصميمه قد يشتعل أو يوجد ظروف أخرى غير آمنة، مثل الأبواب غير المقفلة بشكل غير متوقع، بث فيديو من داخل المنزل أو التسبب في تعدل الأجهزة (الطبية).

نشير إلى شبكات الروبوت عند تثبيت وكلاء البرنامج، بشكل جماعي ودون موافقة، لاستخدام المصادر الحسابية أو التخزينية أو الشبكية للجهاز. ثم يمكن استخدام شبكات الروبوت هذه لممارسة التأثيرات المباشرة على نظام مستهدف مختلف قد يتضمن التأثير على سرية وتوافر وسلامة بيانات الأهداف النهائية. وبالتالي، يصبح جهاز "الطرف الثالث" غير المتورط، ومالكه/مشغله، طرفًا في نشاط سيبراني خبيث دون معرفته. لا يؤدي اختراق الأجهزة لتثبيت وكلاء البرامج الخبيثة إلى إضعاف دفاع الجهاز ضد الهجمات الأخرى فحسب—ضد المجرمين على سبيل المثال—أو انتهاك وظائف الجهاز العادية، وإنما يعتبر المالك/المشغل مسؤولاً محتملاً عن الأضرار التي تلحق بالهدف النهائي. وهذا أمر خطير تحديدًا للحالات التي قد يعتبر اختراق الجهاز فيها الجهاز ومالكه/مشغله محاربًا غير مقصود في الأعمال العدائية بين الدول، ومن ثم يدعو إلى الانتقام أو المساءلة.

كلما زاد اعتمادنا على التكنولوجيا في بيئتنا الشخصية، وكلمات زاد دخول الأجهزة المتصلة إلى الأسواق، أدى استغلال أجهزة المستهلك واستخدامها كشبكات روبوت إلى ضعف الثقة وزعزعة المجتمع بشكل كبير. تقر اللجنة بوجود حالات—لأغراض إنفاذ القانون على سبيل المثال—قد تجد الجهات الفاعلة الحكومية المعتمدة ضرورة لتثبيت وكلاء البرامج على أجهزة عدو واحد مستهدف على وجه التحديد، أو مجموعة من الأعداء. إلا أنه يجب على الجهات الفاعلة الحكومية وغير الحكومية عدم الاستيلاء على أجهزة المدنيين من عامة الناس (بشكل جماعي) لتيسير أو تنفيذ عمليات سيبرانية هجومية مباشرة، بغض النظر عن الحافز.[56]

56 هذا المعيار مكمّل للمعيار المقترح السابق للجهات الفاعلة الحكومية وغير الحكومية لتجنب التلاعب بالمنتجات قبل طرحها، الذي يركز على جوانب سلسلة الإمداد، بينما يتناول هذا المعيار الأجهزة المنتشرة بالفعل.

5. معيار للدول لإيجاد عملية حقوق نقطة الضعف



المعيار:

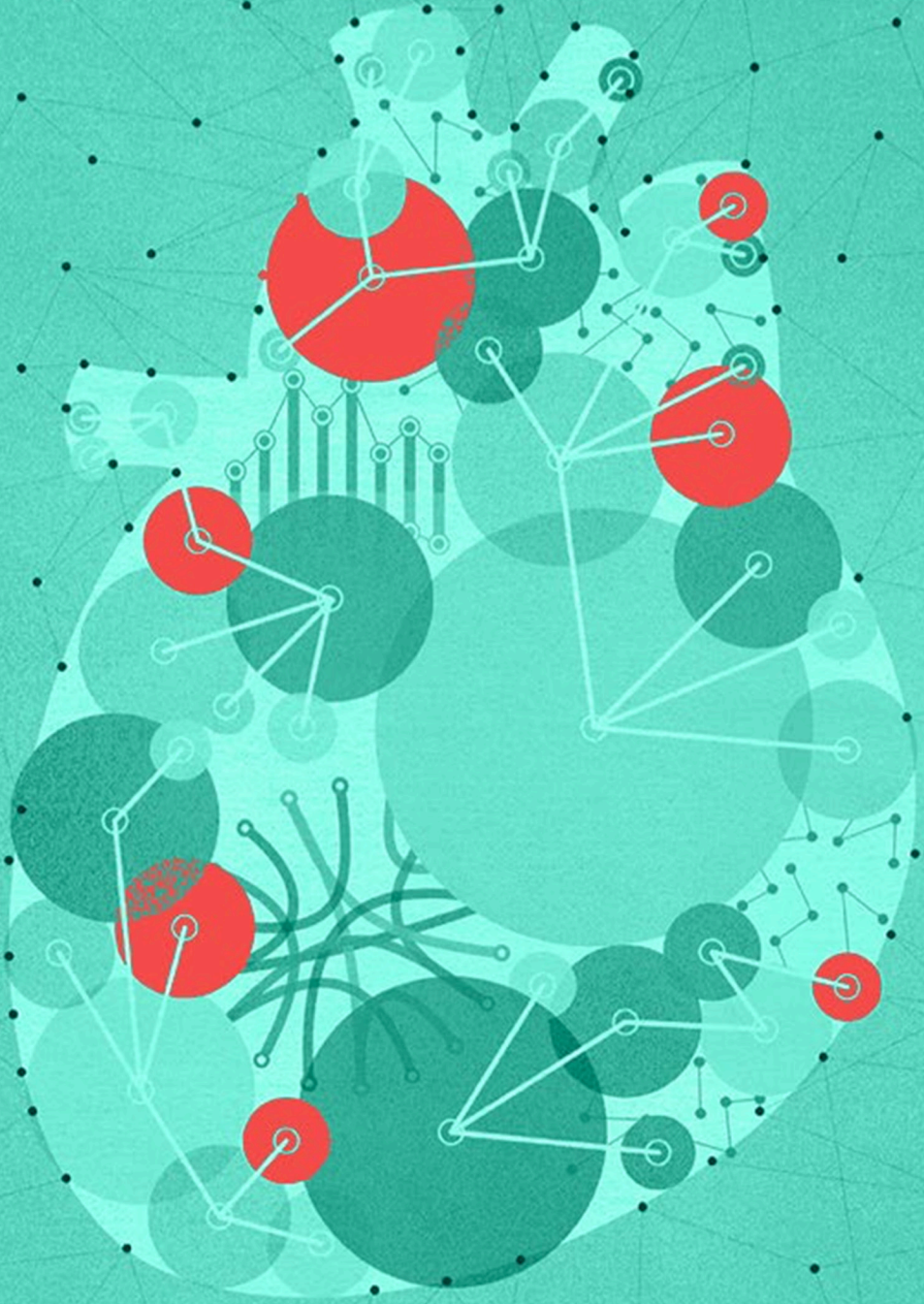
تلتزم الدول بإنشاء أطر عمل شفافة من الناحية الإجرائية لتقييم ما إذا كان ينبغي الكشف عن مواطن الضعف أو العيوب غير المعروفة علنًا التي تدركها في نظم وتكنولوجيا المعلومات ومتى ينبغي ذلك. وينبغي أن يكون الافتراض الوارد مؤيدًا لقرار الإفصاح.

نبذة

بسبب تعقيد أنظمة التشغيل، تنمو البرامج الحرجة وأجهزة الكمبيوتر، وتحتوي بشكل كبير على نقاط ضعف. ويمكن استغلال نقاط الضعف هذه من قبل الجهات الفاعلة الحكومية وغير الحكومية. تواجه الدول في بعض الأحيان تعارضًا في المصالح والمسؤوليات عند التعامل مع نقاط الضعف المكتشفة حديثًا. فمن ناحية، تلتزم الدول بتعزيز مرونة وسلامة البنية التحتية الضرورية لاستقرار الفضاء السيبراني وجعل النظام البيئي الرقمي ككل أكثر أمنًا لجميع المستخدمين وذلك بالمساعدة في إحباط النشاط السيبراني الخبيث. وهذا من شأنه أن يحث الدولة على الإفصاح سريعًا عن نقاط الضعف المكتشفة حديثًا للموردين وجهات التصنيع لتصحيحها، فضلاً عن تقديم إقرارات علنية أوسع، عند الاقتضاء، لحماية العامة. من ناحية أخرى، تلتزم الدول بحماية مواطنيها من المجرمين، بالتحقيق في الجرائم السيبرانية وملاحقتها قضائيًا، والاحتفاظ بحق فرض عقوبات تكون بمثابة رادع خاص وعام للنشاط الخبيث المستقبلي. ويُعتبر اعتماد الدول على استغلال نقاط الضعف في البنية التحتية الرقمية أداة ضرورية لملاحقة الجهات الفاعلة الخبيثة، ولاسيما الجهات الفاعلة المتطورة مثل الدول المارقة. لذا، كثيرًا ما تقول الدول بوجوب احتفاظها ببعض القدرات المحددة على الأقل، ومنها استخدام نقاط الضعف غير المفصح عنها، وإلا فقد تمضي الجهات الفاعلة الخبيثة ذات القدرات العالية دون اكتشافها وتحديدها.

وبالرغم من عدم احتمال إفصاح الدول طواعيةً عن كل نقطة ضعف تكتشفها، إلا أن خطوة حديثة اتخذتها عدة دول بعيدًا عن افتراض أنه سيتم الاحتفاظ بكل نقاط الضعف غير المفصح عنها، إلى افتراض في صالح الإفصاح من أجل تعزيز الأمن السيبراني النظامي. يتمثل جزءً رئيسي من هذا في قيام الدول بإيجاد عملية موصوفة علنًا لتقييم إيجابيات وسلبيات الإفصاح الذي يأخذ في الاعتبار النطاق الكامل للحقوق السياسية والاقتصادية والاجتماعية الفنية. وبشكل أكثر تحديدًا، يجب أن تكون هذه العملية شفافة من الناحية الإجرائية وأن تأخذ في الاعتبار النطاق الكامل لوجهات النظر ومنها العوامل مثل: أمن ومرونة الشبكة، أمن المستخدمين وبياناتهم، خدمة إنفاذ القانون والأمن القومي، والآثار الدبلوماسية والتجارية. نشرت الولايات المتحدة مؤخرًا إصدارًا جديدًا من هذه العملية وتدرس بلدان أخرى إيجاد سياسات عملية حقوق نقطة الضعف (VEP) الخاصة بها. وبفرض أن اكتشاف نقطة الضعف والإفصاح عنها أكبر من أي دولة واحدة، ولتعزيز مرونة الشبكة مع حماية الأمن الوطني في نفس الوقت، سيكون ذلك في صالح استقرار الفضاء السيبراني على المدى الطويل بالنسبة لكل دولة تمتلك هذه العملية. بالإضافة إلى أنه يجب على الدول العمل من أجل عمليات متوافقة ومتوقعة. قد يكون وجود هذه العمليات بمثابة إجراء لبناء الثقة بين الدول لأنها توفر بعض التأكيد على أنه تم النظر في الحقوق ذات الصلة والمصالح المتضاربة بشكل تام. لا شك في أن لكل دولة قدرات مختلفة وهياكل فريدة بين الوكالات، مع ذلك، يجب تصميم أي عملية من عمليات حقوق نقطة الضعف لأخذ مجموعة كبيرة من وجهات النظر والحقوق في الاعتبار. بالإضافة إلى أن القرارات الفعلية التي يتم التوصل إليها في حالات فردية قد تظل سرية، بدافع الضرورة، وبالتالي يجب أن تكون هناك شفافية في الإجراءات العامة وإطار العمل الخاص بالتوصل لهذه القرارات. أخيرًا، لا يتعامل هذا المعيار إلا مع تحديد عملية يتم من خلالها اتخاذ قرارات الإفصاح. وفي حال اتخاذ حكومة أو أي كيان آخر لقرار الإفصاح، فيجب أن يتم هذا الإفصاح بطريقة مسؤولة تعزز السلامة العامة ولا تؤدي إلى استغلال نقطة الضعف هذه.

6. معيار لتقليل نقاط الضعف الخطيرة والتخفيف من آثارها



المعيار:

يجب على مطوري ومنتجي المنتجات والخدمات التي يعتمد عليها استقرار الفضاء السيبراني (1) ترتيب أولويات الأمن والاستقرار، (2) واتخاذ خطوات معقولة لضمان خلو منتجاتهم وخدماتهم من نقاط الضعف الخطيرة، (3) واتخاذ إجراءات للتخفيف من آثار نقاط الضعف المكتشفة لاحقًا في الوقت المناسب والامتثال بالشفافية فيما يتعلق بمعالجتها. وتلتزم جميع الجهات الفاعلة بمشاركة المعلومات المتعلقة بمواطن الضعف من أجل المساعدة في منع النشاط السيبراني الخبيث أو الحد منه.

نبذة

هناك منتجات وخدمات محددة في قطاع تكنولوجيا المعلومات ضرورية لاستقرار الفضاء السيبراني بسبب استخدامها في البنية التحتية الفنية الأساسية، كما هو الحال في دقة أو توجيه الاسم الأساسي، أو بسبب تسهيلها لتجربة المستخدم للإنترنت على نطاق واسع، أو بسبب استخدامها داخل البني التحتية الحرجة. ويجب على مصنعي المنتجات والخدمات الالتزام بمستوى معقول من العناية لتصميم وتطوير وتسليم منتجات وخدمات تولي الأمن الأولوية وتعمل بدورها على تقليل احتمال نقاط الضعف وتكرارها وإمكانية استغلالها وخطورتها.

بسبب زيادة تعقيد البرامج والأجهزة، تُعتبر نقاط الضعف في هذه المنتجات حقيقة من حقائق الحياة. وبالرغم من أن نقاط الضعف هذه عادة ما تكون غير متعمدة، إلا أن الجهات الفاعلة الحكومية وغير الحكومية الخبيثة كثيرًا ما تستغل نقاط الضعف هذه عند اكتشافها بطرق تزعزع استقرار الفضاء السيبراني.

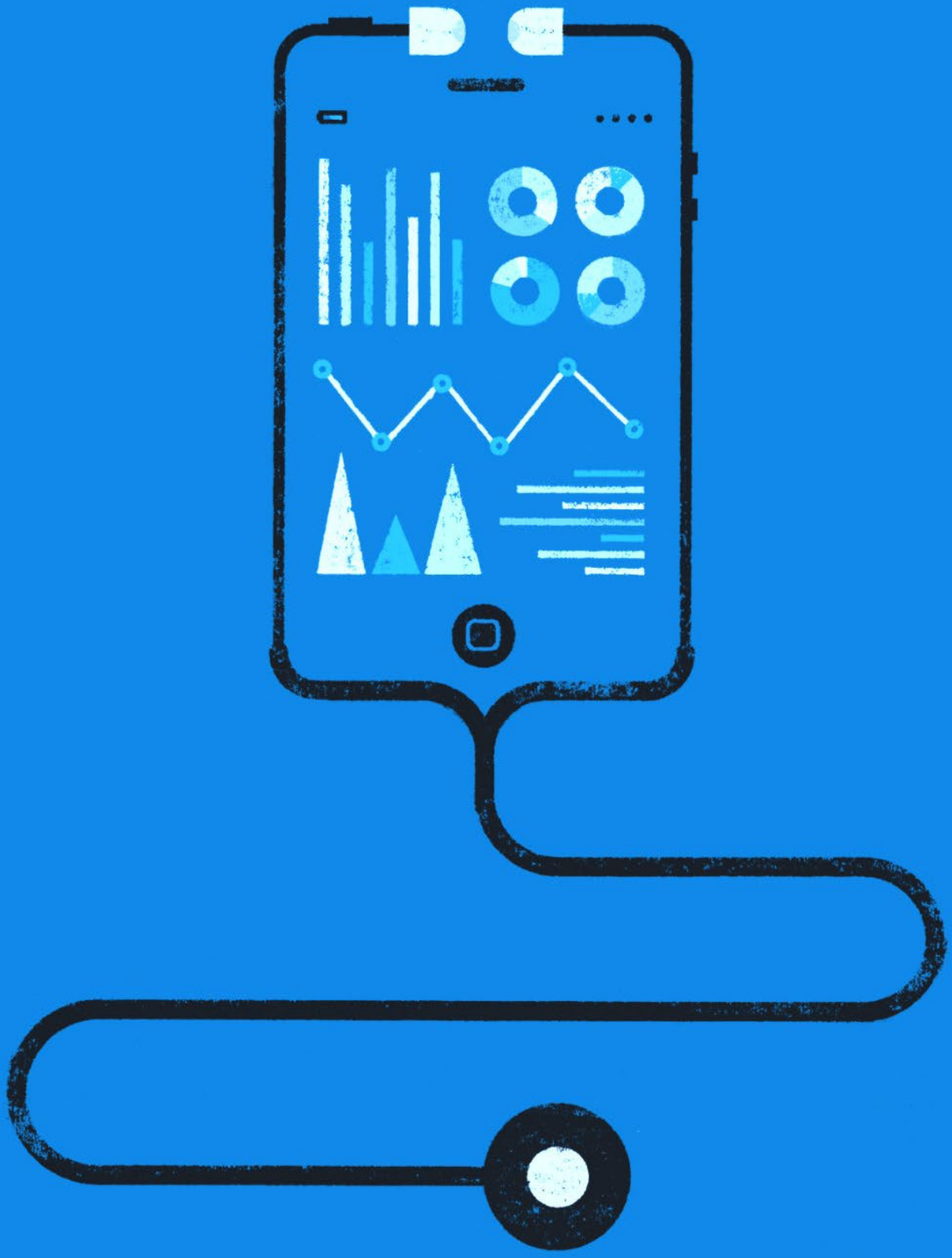
كما أنه في عالم شديد الترابط وشديد التبعية، قد تؤثر نقطة الضعف المكتشفة على عدة منتجات وخدمات من منتجين مختلفين وفي بيئات مختلفة. تجدر الإشارة إلى أن تصحيح منتج واحد دون الإفصاح عن نقطة الضعف الأساسية للآخرين قد يحمي هذا المنتج إلا أنه لن يحمي استقرار الفضاء السيبراني بشكل عام. والمتواجدون في وضع أفضل لتقييم أثر نقطة ضعف معينة كثيرًا ما يكونون هم المطورون، المنتجون، المثبتون أو المشغلون للمنتجات المتضررة بنقاط الضعف. لذا، فمن الضروري مشاركة المعلومات التي تساعد في إصلاح نقاط الضعف الأمنية أو المساعدة في منع الهجوم أو تقييده أو التخفيف من أثره.[57]

بالرغم من شدة صعوبة ضمان عدم وجود نقاط ضعف في المنتجات المطروحة أو المحدثة مؤخرًا، إلا أن هذا المعيار المقترح يشير إلى اتخاذ المشاركين في تطوير وإنتاج هذه المنتجات "لخطوات معقولة" من شأنها أن تقلل تكرار وخطورة ما يحدث.

كما يعالج معيار "عدم التلاعب" الإدخال الدولي لنقاط الضعف في المنتجات والخدمات الحرجة، ومعيار النظافة يعالج في نهاية المطاف واجبات المستخدمين النهائيين، فإن هذا المعيار المقترح يسعى إلى اتخاذ من يقومون بتطوير أو إنتاج المنتجات الحرجة لإجراءات معقولة لضمان تقليل عدد ونطاق نقاط الضعف الحرجة والتخفيف من آثارها بشكل فعال ومناسب والإفصاح عنها، عند الاقتضاء، عند اكتشافها. ويجب أن تكون العملية المستخدمة شفافة لإيجاد بيئة متوقعة ومستقرة.

57 أحد معايير السلوك المسؤول للدول في تقرير 2015 الخاص بمجموعة الخبراء الحكوميين التابعين للأمم المتحدة (A/70/174) يؤكد على أن "الدول يجب أن تحث على الإبلاغ المسؤول عن نقاط ضعف تكنولوجيا المعلومات والاتصالات ومشاركة المعلومات ذات الصلة المتعلقة بطرق معالجة نقاط الضعف هذه لتقييد أو التخلص من التهديدات المحتمل أن تواجهها تكنولوجيا المعلومات والاتصالات والبنية القائمة على تكنولوجيا المعلومات والاتصالات".

7. معيار خاص بالنظافة السيبرانية الأساسية كدفاع مؤسسي



المعيار:

تلتزم الدول باتخاذ التدابير المناسبة، بما في ذلك القوانين واللوائح، لضمان السلامة السيبرانية الأساسية.

نبذة

مع اجتياح الاتصال بالإنترنت المنتشر في جميع أنحاء العالم لكل جوانب الحياة العصرية، يزداد اعتماد المستخدمين من جميع الأنواع—الأفراد، المنظمات، الشركات، والحكومات—على التكنولوجيا والوصول إلى المعلومات المتوفرة على الإنترنت. فالسياسة والاقتصاد والمعلومات العامة والتعليم والتطوير وكل طريقة أخرى من طرق التفاعل الاجتماعي تعتمد بشكل كبير على الإنترنت والتقنيات ذات الصلة. مع ذلك، تظل هذه العجيبة الحديثة غير آمنة على نطاق واسع، ولا أحد محصن من مخاطرها.

ولم يظهر بعد الإجماع على الطرق الأكثر فاعلية لتحسين تقنيات الفضاء السيبراني الواعدة بجانب حماية العامة. حتى الآن، تتفق الأغلبية على تعذر استمرار فوائد حياتنا المتصلة رقميًا دون معايير متفق عليها للأمن الأساسي في الفضاء السيبراني. ولتحقيق هذه الغاية، تؤيد اللجنة بشدة التبني واسع الانتشار والتنفيذ المؤكد للنظافة السيبرانية الأساسية—نظام من التدابير التأسيسية تمثل المهام الأساسية ذات الأولوية التي يجب تنفيذها للدفاع ضد المخاطر التي يمكن تجنبها في الفضاء السيبراني ومنعها والتخفيف سريعًا من آثارها.

في الواقع، ونظرًا لشمولية الاتصال البيني على الإنترنت، تشكل هذه التدابير واجب عناية أساسي يجب طلبه من جميع المستخدمين. ويجب أن تتضمن نظم النظافة تدابير تنفيذ موثوقة، وأن تنص على المشاركة واسعة الانتشار للمعلومات الفنية وأفضل الممارسات، وأن تخضع للإشراف المناسب. فالأجهزة والعمليات الذكية بشكل كبير تتطلب قوانين ولوائح ذكية. ولإيجاد المزيد من المساءلة فيما يتعلق بواجب العناية السيبرانية الأساسي هذا، يجب ألا تقوم الحكومات بتقليص الابتكار أو تعديل الخصائص الأساسية للإنترنت.

توجد معايير النظافة السيبرانية بالفعل في أشكال متعددة.[58] وقد لاقت قبولاً دوليًا أوسع، بسبب زيادة فهم الحكومات والشركات لأهمية اتخاذ خطوات موضحة للمساعدة في منع مخاطر البرامج الخبيثة المعروفة والتخفيف بسرعة من آثارها. بالإضافة إلى أن هذه المعايير تمثل أفضل الممارسات، وتبرز أهمية الإشراف الملموس والمنتظم وتؤكد على أهمية المشاركة التلقائية للمعلومات متى أمكن لتنبيه المستخدمين الآخرين إلى المشكلة. تعتمد هذه الدفاعات السيبرانية الأساسية كما وردت في هذه الطرق على حقيقة أنه لا يمكن لأي حكومة أو منظمة أو مجموعة من المستخدمين العمل على نحو منفرد لتخفيف المخاطر ذات الصلة بالإنترنت. كما تقر بأن للمستخدمين على جميع المستويات أدوار هامة يجب عليهم لعبها لتعزيز الأمن السيبراني.

تؤمن اللجنة العالمية لاستقرار الفضاء السيبراني بأن دفاع الأمن السيبراني الأساسي من خلال التبني واسع الانتشار للنظافة السيبرانية قد أصبح أساسيًا للاستخدام المسؤول والنمو المفيد للإنترنت. ويجب أن يُنظر إلى الأمن على أنه عملية مستمرة متضمنة لمسؤوليات موزعة بين كل الجهات الفاعلة بالإضافة إلى وجود آليات موضوعة في مكانها، مثل إعداد التقارير ومشاركة المعلومات بشكل تلقائي، لضمان المحاسبة الصحيحة.

كما تقر اللجنة بمواجهة العديد من المجتمعات بجميع أنحاء العالم لتحديات كبيرة تتعلق باستخدام تكنولوجيا المعلومات والاتصالات وتدعو الدول لمشاركة المعرفة وتوفير بناء القدرات للعمليات الفورية من أجل التنفيذ الفعال لأنظمة النظافة السيبرانية الأساسية لزيادة تأثير هذا المعيار.

58 يتضمن ذلك، على سبيل المثال، المعهد الأوروبي لمعايير الاتصالات السلكية واللاسلكية (ETSI)، مركز أمن الإنترنت غير الربحي (CIS) ومديرية الإشارات الأسترالية (ASD)، من بين مؤسسات أخرى.

8. معيار ضد العمليات السيبرانية الهجومية من قبل الجهات الفاعلة غير الحكومية

المعيار:

تلتزم الجهات غير الحكومية بعدم المشاركة في العمليات السيبرانية الهجومية وتلتزم الجهات الحكومية بمنع مثل هذه الأنشطة والاستجابة لها في حالة حدوثها.

نبذة

بالرغم من أن تكنولوجيا المعلومات والاتصالات حولت المجتمعات بشكل إيجابي، إلا أنها تفرض أيضًا تحديات أمنية جديدة. فكثيرًا ما تفرض سرعة العمليات السيبرانية ووجودها في كل مكان صعوبات بالغة على النظم القضائية للدول والتعاون الدولي لإنفاذ القانون. وبالرغم من هذه الصعوبات، يجب التذكير بأن سيادة الدولة هي حجر الزاوية لنظام الأمن والسلام الدولي القائم على القواعد. فالدول المحتكرة للاستخدام الشرعي للقوة، ملزمة تمامًا بالقانون الدولي. وبعض الجهات الفاعلة غير الحكومية، الشركات الخاصة تحديدًا، تدافع عن حق تنفيذ عمليات سيبرانية هجومية عبر الحدود الوطنية، مدعية أنها تشكل إجراء دفاعي ضروري لأن الدول لا تملك القدرة في حمايتها بالقدر الكافي من الهجمات السيبرانية. يُشار إلى تلك العمليات السيبرانية الهجومية التي تقوم بها الجهات الفاعلة غير الحكومية في بعض الأحيان بالتعبير اللطيف "الدفاع السيبراني النشط"،[59] بما في ذلك، وعلى سبيل المثال لا الحصر، ما يُسمى بـ "الاختراق"، لأنها تُنفذ لأغراض دفاعية.

لا تملك بعض الدول الرقابة على هذه الممارسات وقد تتجاهلها فعليًا، بالرغم من الخطر الذي تفرضه على استقرار وأمن الفضاء السيبراني. غير أن هذه الممارسات تُعتبر غير قانونية في العديد من الدول، إن لم تُجرم، في حين تبدو في دول أخرى إما محظورة أو معتمدة بشكل صريح. ومع ذلك، تنظر بعض الدول في إضفاء الصفة الشرعية على العمليات السيبرانية الهجومية التي تقوم بها الجهات الفاعلة غير الحكومية. في الواقع، قامت بعض الدول بتقرير أو اقتراح قوانين محلية للسماح بالعمليات الهجومية من قبل الجهات الفاعلة غير الحكومية.

وتؤمن اللجنة العالمية لاستقرار الفضاء السيبراني بأن هذه الممارسات تزعزع استقرار الفضاء السيبراني. فقد تؤدي إلى حدوث عطل كبير أو وقوع أضرار بالغة، منها ما يتعلق بالجهات الخارجية، ومن المحتمل أن تؤدي إلى نشوب نزاعات قانونية معقدة وتصاعد النزاعات. والدول التي تمنح الجهات الفاعلة غير الحكومية الإذن الصريح أو تسمح لها عن علم بتنفيذ العمليات الهجومية، لأغراض خاصة بها أو لأغراض خاصة بجهات خارجية، ستقرر سابقة خطيرة وستخاطر بانتهاك القانون الدولي. تؤمن اللجنة بأنه يجب على الدول فقط الاحتفاظ بهذه التدابير الدفاعية وتُذكر بأن القانون الدولي يضع إطار عمل صارم وشامل لاستجابات الدول للأعمال العدائية ينطبق أيضًا على العمليات السيبرانية. بالمثل، وبموجب القانون الدولي، يجب اعتبار الجهات الفاعلة غير الحكومية التي تتصرف بالنيابة عن الدول وكلاء لها ومن ثم تُعتبر امتداد للدولة.[60]

وإذا سمحت الدول بهذا التصرف، فقد تتحمل المسؤولية بموجب القانون الدولي.[61] فيجب على الدول التصرف، على الصعيد المحلي والدولي، لمنع العمليات السيبرانية الهجومية التي تقوم بها الجهات الفاعلة غير الحكومية.

59 يجب فهم الدفاع السيبراني النشط على أنه مجموعة من الإجراءات التي تتراوح من الدفاع الذاتي على شبكة الضحية إلى النشاط المدمر على شبكة المهاجم. والعمليات السيبرانية الهجومية ضمن هذه السلسلة تعني تصرف المدافع خارج شبكته بغض النظر عن نيته (الهجوم أو الدفاع) والأهلية القانونية لأفعاله. ينبغي العمل بشكل أكبر على تعريف العمليات السيبرانية الهجومية والدفاع السيبراني النشط.

60 انظر "ملاحظة إضافية" لمعالجة القضية بشكل أوسع في إطار القانون الدولي، تتوفر هنا: https://cybersta-bility.org/wp-content/uploads/2018/11/Additional-Note-to-the-Norm-Against-Of-fensive-Cyber-Operations-by-Non-state-Actors-Norm-Package-Singapore.pdf.

61 نفس المرجع

الملحق ج:
تاريخ، وأهداف، وعمليات اللجنة العالمية المعنية باستقرار الفضاء السيبراني

منذ انطلاقها في مؤتمر ميونيخ للأمن في فبراير 2017 تحت رعاية وزير الخارجية الهولندي بيرت كوندرز، اعتبرت اللجنة العالمية المعنية باستقرار الفضاء السيبراني إحدى أولى مبادرات أصحاب الملحة المتعددين من نوعها التي تركز تحديدًا على استقرار الفضاء السيبراني. وبرئاسة مايكل شيرتوف، الوزير السابق للأمن الداخلي الأمريكي؛ لاثا ريدي، النائب السابق لمستشار الأمن القومي بالهند؛ ومارينا كالجوراند من قبل، عضو البرلمان الأوروبي ووزيرة خارجية إستونيا، تكونت اللجنة من 28 شخصية بارزة من مناطق جغرافية مختلفة فضلاً عن خلفيات مختلفة ذات صلة بالفضاء السيبراني الدولي.[62] وحصلت اللجنة على الدعم من مستشارين خاصين، أمانة، تألفت من مركز *لاهاي* للدراسات الإستراتيجية ومعهد إيست ويست، مجموعة استشارية للبحوث، فضلاً عن عدد من الشركاء والرعاة، منهم وزارة الخارجية الهولندية والفرنسية، وكالة الأمن السيبراني بسنغافورة، مايكروسوفت، مجتمع الإنترنت، أفيلياس.

ولدت اللجنة من الرغبة في مواصلة عمل لجان المجتمع المدني السابقة، ومنها اللجنة العالمية لحوكمة الإنترنت، والارتباط بعمل المؤتمر العالمي للفضاء السيبراني. في 2015، طُلب من مركز *لاهاي* للدراسات الإستراتيجية (HCSS) تنظيم جلسة تمهيدية لاجتماع لاهاي بالمؤتمر العالمي للفضاء السيبراني، المخصص للسلام والأمن الدولي. اعتمد الكثير من إعلان المؤتمر العالمي للفضاء السيبراني اللاحق على عمل الاجتماعي التمهيدي، الذي حدد بوضوح الحاجة إلى تنسيق أحاب المصلحة المتعددين لمناقشة مشاكل الفضاء السيبراني الدولية. بناءً عليه، اجتمع مركز لاهاي للدراسات الإستراتيجية بمجموعة رئيسية من الداعمين والممولين (مايكروسوفت، مجتمع الإنترنت، ووزارة الخارجية الهولندية في الأصل) وأعد خطة إستراتيجية. في أغسطس 2016، وبعد اكتساب معهد إيست ويست (EWI) كشريك في الأمانة، عقد مركز لاهاي للدراسات الإستراتيجية اجتماعًا لمجموعة تأسيس اللجنة العالمية لاستقرار الفضاء السيبراني في كلية كينيدي بجامعة هارفارد، نتج عنه صياغة المتطلبات الرئيسية لعمل اللجنة العالمية المعنية باستقرار الفضاء السيبراني، وعضويتها، وهيكلها، وأهدافها، فضلاً عن بيان مهمتها.

وفيما يلي بيان مهمة اللجنة:

> ستضع اللجنة العالمية المعنية باستقرار الفضاء السيبراني (GCSC) مقترحات بشأن القواعد والسياسات من أجل تعزيز الأمن والاستقرار الدوليين وتوجيه السلوكيات المسؤولة الحكومية وغير الحكومية المتبعة في الفضاء السيبراني. وستشرك اللجنة العالمية لاستقرار الأمن السيبراني مجموعة أصحاب المصلحة المتعددين بالكامل في إعداد تفاهمات مشتركة، وسيسهم عملها في تحسين الاستقرار السيبراني من خلال دعم البحث وتبادل المعلومات وبناء القدرات.

62 انظر القائمة الكاملة لأعضاء اللجنة في الصفحة 4.

منذ بدايتها، كان القصد من اللجنة العالمية لاستقرار الفضاء السيبراني هو التأثير على جدول أعمال السلام والأمن الدولي ذي الصلة بالفضاء السيبراني، المُشار إليه بشكل عام باسم "الأمن السيبراني الدولي". وقد حددت مجموعة التأسيس الحاجة إلى التماس وجهات نظر متنوعة في مناقضات الأمن السيبراني الدولي المستمرة، لاسيما من إدارة الإنترنت والمجتمعات الفنية. كان الهدف من ذلك هو تحسين نقل المداولات في مجتمعات مراقبة الأسلحة والسلام والأمن، حيث اعتبر الكثير من العمل الجيد، لاسيما فيما يتعلق بالمعايير، معاقًا بسبب نقص المدخلات والقبول من الجهات الفاعلة بالمجتمع المدني والقطاع الخاص. لذا، اعتبر نهج أصحاب المصلحة المتعددين عمليًا وليس مشكلة أيديولوجية.

تناولت اللجنة العالمية لاستقرار الفضاء السيبراني مداولاتها بطريقة "تصاعدية إلى تنازلية". أولاً، قامت اللجنة بتحديد المعايير التشغيلية التي تلبي احتياجات الأمن السيبراني الدولي الأكثر إلحاحًا كما عبر عن ذلك أعضائها والتي لم تُعالج في أي مكان آخر. ثانيًا، استنتجت من هذه المعايير والمعايير الموجودة بالفعل تعريف عامل للأمن السيبراني ومبادئه الأساسية. ثالثًا، تم إعداد إطار عمل الاستقرار لفهم ما يجب على هيكل السلام والأمن الدولي فعله لتلبية هذا التعريف بشكل أوضح. أخيرًا، أعدت اللجنة التوصيات الموجهة إلى أصحاب المصلحة الحكوميين وغير الحكوميين حول كيفية تحقيق ذلك.

عُقدت مداولات أعضاء اللجنة لتحقيق هذه الأهداف عبر الحدود الجغرافية وعبر مجموعات أصحاب المصلحة. ومنذ البداية، أكدت اللجنة على عقد اجتماعاتها على هوامش المؤتمرات ذات الصلة لتيسير المدخلات من مجموعة كبيرة من أصحاب المصلحة.[63] كما التمست المدخلات على نحوٍ نشطٍ من خلال البحث ومن المجتمع الأوسع. لربط عمل اللجنة العالمية لاستقرار الفضاء السيبراني بالمجتمع الأكاديمي الأوسع، تم دفع المجموعة الاستشارية للبحوث إلى كرسي الرئاسة وأربعة نواب للرئيس[64] مسؤولين عن إدارة قائمة البريد الإلكتروني لما يزيد عن 200 خبير. كما أنها كانت الأساس لبرنامج بحثي واسع النطاق، كلف في النهاية المؤسسات البحثية والأفراد في جميع أنحاء العالم بإجراء ما يزيد عن 20 دراسة.[65] وتم تقديم الجزء الأكبر من هذا العمل إلى أعضاء اللجنة بشكل مباشر في "جلسات استماع الاستقرار السيبراني" المخصصة.

قبل نشر هذا التقرير والمعايير الصادرة في السابق، سعت اللجنة باستمرار للحصول على مدخلات من مجموعة كبيرة من أصحاب المصلحة بالحكومة والمجتمع المدني والصناعة. وبجدولة التسليم على مدار فترة عمل اللجنة، فقد كان من الممكن دعوة المدخلات والتعليقات الخارجية باستمرار. صدرت طلبات الاستشارة على الإنترنت بخصوص معايير اللجنة العالمية لاستقرار الفضاء السيبراني وتعريف الاستقرار السيبراني. ورد ما يزيد عن 23 طلب من جهات فاعلة بجميع أنحاء العالم توجهت نحو نقل مداولات أعضاء اللجنة. كما شاركت اللجنة على نحو فعال في ما يزيد عن 70 مؤتمر وفعالية، وعقد اجتماعات المائدة المستديرة، فعاليات جانبية، جلسات استماع الاستقرار السيبراني المخصصة مع مجموعة كبيرة من أصحاب المصلحة الحكوميين وغير الحكوميين.

أخيرًا، بقي أعضاء اللجنة أنفسهم على اتصال نشط بمجتمعاتهم المعنية. ومثلت المدخلات والتعليقات من هذه المجموعات حجر الأساس للتفاعلات مع المجتمع الأوسع من الخبراء الحكوميين وغير الحكوميين وستشكل الأساس للدعوة إلى المضي قدمًا في التقرير.

63 عقدت الاجتماعات الرسمية للجنة في الفعاليات التالية: 2017 مؤتمر ميونيخ للأمن (ميونيخ، ألمانيا)؛ CyCon (تالين، إستونيا)؛ BlackHat الولايات المتحدة الأمريكية (لاس فيغاس، الولايات المتحدة الأمريكية)؛ المؤتمر العالمي للفضاء السيبراني (نيودلهي، الهند)؛ FIC 2018 المنتدى الدولي للأمن السيبراني (ليل، فرنسا)؛ 2018 مؤتمر ميونيخ للأمن (ميونيخ، ألمانيا - منح)؛ منظمة جلوبسيك (براتيسلافا، سلوفاكيا)؛ أسبوع الإنترنت بإسرائيل (تل أبيب، إسرائيل - منح)؛ أسبوع الإنترنت الدولي بسنغافورة (سنغافورة)؛ منتدى باريس للسلام وIGF (باريس، فرنسا - منح)؛ 2019 معهد الأمم المتحدة لبحوث نزع السلاح (جنيف، سويسرا)؛ منتدى مجتمع ICANN 64 (كوبه، اليابان)؛ EuroDIG (لاهاي، هولندا)؛ اجتماع GFCE السنوي (أديس أبابا، إثيوبيا).

64 يشمل أربعة مجالات بالموضوع، منها السلام والأمن الدولي، القانون الدولي، حوكمة الإنترنت، والتكنولوجيا.

65 انظر فقرة الشكر والتقدير.

شكر وتقدير

ترغب اللجنة العالمية لاستقرار الفضاء السيبراني في شكر العديد من المؤسسات والأفراد الذين دعموا عمل اللجنة وساهموا فيه ويسروه ومنهم، على سبيل المثال لا الحصر، رعاتنا، والمجموعة الاستشارية للبحوث، ومؤلفو أوراق البحث والمراجعين من الأقران، وفريق الدعم. وفيما يلي بعضًا ممن ساهموا في نجاح اللجنة.

الأمانة العامة

مركز *لاهاي* للدراسات الإستراتيجية (HCSS)

ألكسندر كليمبورغ، مدير، مبادرة وأمانة اللجنة العالمية المعنية باستقرار الفضاء السيبراني
لوك فايزن، مدير المشروع، أمانة اللجنة العالمية المعنية باستقرار الفضاء السيبراني
إليوت مايهيو، مساعد المشروع، أمانة اللجنة العالمية المعنية باستقرار السيبراني

بدعم إضافي من: **تيمون دوليما نيونيوس نيجارد، كوين فان دين دول، نيلس رينسن**، و**كاجا كارلسون**.

معهد إيست ويست (EWI)

بروس دبليو ماكونيل، المدير المساعد، أمانة اللجنة العالمية المعنية باستقرار الفضاء السيبراني
أنيلين روجمان، مدير المشروع، أمانة اللجنة العالمية المعنية باستقرار الفضاء السيبراني

بدعم إضافي من: **أباجيل لاوسن، دراغون ستوجانوفسكي**، و **كونارد جارزيبوسكي**.

الشركاء، والجهات الراعية، والجهات الداعمة

مركز *لاهاي* للدراسات الإستراتيجية، معهد إيست ويست، وأعضاء اللجنة يتقدمون بالشكر والتقدير للمنظمات التالية من أجل دعمها:

الشركاء:

- **وزارة الخارجية الهولندية**، **تيمو كوستر** و **ديمتري فوجيلار**
- **مايكروسوفت**، **جان نيوتز** و **كاجا سيجليك**
- **وكالة الأمن السيبراني بسنغافورة**، **ديفيد كو** و **سيثوراج بونراج**
- **مجتمع الإنترنت (ISOC)**
- **وزارة الخارجية الفرنسية**، **هنري فيردر** و **ديفيد مارتينون**
- **أفيلياس**، **رام موان** و **فيليب جرابنسي**

الجهات الراعية:

- **الإدارة الفيدرالية للشؤون الخارجية بسويسرا**
- **منظمة جلوبسيك**
- **وزارة الخارجية الإستونية**
- **وزارة الشؤون الداخلية والاتصالات اليابانية**

الجهات الداعمة:

- **مفوضية الاتحاد الأفريقي**
- **Black Hat الولايات المتحدة الأمريكية**
- **ديف كون**
- **وفد الاتحاد الأوروبي إلى الأمم المتحدة بجنيف**
- **المنتدى العالمي للخبرات السيبرانية**
- **جوجل**
- **بلدية لاهاي**
- **غرفة مقاصة الحزم**
- **جامعة تل أبيب**
- **معهد الأمم المتحدة لنزع السلاح**

تلتزم هذه المنظمات والمؤسسات بتحسين النقاش ووضع حلول إبداعية لبعض التحديات الأكثر إلحاحًا التي تواجه استقرار الفضاء السيبراني.

الباحثون

تود اللجنة تقديم الشكر لأعضاء المجموعة الاستشارية للبحوث التابعة لها، مجموعة مكونة مما يزيد عن 200 عضو على الإنترنت تصل اللجنة العالمية لاستقرار الفضاء السيبراني بالمجتمع الأكاديمي الأوسع. ونود أن نشكر تحديدًا الباحثون الذين كُلفوا بكتابة الإحاطات والمذكرات لنقل مداولات أعضاء اللجنة.

الموجز الإعلامي الأول للجنة العالمية المعنية باستقرار الفضاء السيبراني (نوفمبر 2017)

أليكس جريجسبي، من مجلس العلاقات الخارجية (CFR) سابقًا
ديبوره هاوسن كوريل، شركة Konfidas Digital Ltd.
جونا كوليزا، جامعة لودز و **رولف إتش ويبر**، جامعة زيورخ
أولوافيمي أوشو، **جوزيف أيه أوجيني**، و **شافعي إم عبد الحميد**، الجامعة الفيدرالية للتكنولوجيا، مينا
أناليا أسبيس، جامعة بوينس آيرس **روبرت مورجاس**، من أمريكا الجديدة سابقًا، **ماكس سميتس**، من مركز الأمن والتعاون الدولي سابقًا، جامعة ستانفورد، و **تري هير**، كلية كينيد بجامعة هارفارد
أرون موان سوكومار، **مادوليكا سريكومار**، و **بادافيازا موانتي**، مؤسسة أوبزيرفر للبحوث (ORF)

الموجز الإعلامي الثاني للجنة العالمية المعنية باستقرار الفضاء السيبراني (مايو 2018)

سين يي، **جيانغ تيانجياو**، **ووانغ لي**، مركز بحوث حوكمة الفضاء السيبراني، جامعة فودان
إيلانا بروينتمان، **مايلان فيدلر**، و**روبرت مورجوس**، من أمريكا الجديدة سابقًا
إلوناي هيكوك و**أريندراجيت باسو**، مركز الإنترنت والمجتمع
توماس أورين، **بارت هوجيفين**، و**فيرجاس هانسون**، المعهد الأسترالي للسياسة الإستراتيجية (ASPI)
دراغون مالدينوفيتش و**فلاديمير رادونوفيتش**، DiploFoundation
توماس رينهولد، معهد بحوث السلام والسياسة الأمنية، جامعة هامبورغ

الاستشارات

تود اللجنة تقديم الشكر للأفراد التالين والمنظمات التالية لتقديم تعليقات شاملة استجابة لطلب الاستشارات في حزمة معيار سنغافورة (من 17 ديسمبر 2018 وحتى 17 يناير 2019) وتعريف استقرار الفضاء السيبراني (من 14 أغسطس 2019 وحتى 6 سبتمبر 2019):

حسين أبو العينين، Access Partnership
كايودي أكاني، DesignIT
جوناثان دي أرونسون، جامعة كاليفورنيا الجنوبية (USC)
أفيرام أتزابا، إسرائيل مديرية الإنترنت القومية
أريندراجيت باسو، **جورشاباد غروفر**، **إلوناي هيكوك**، **وكاران ساييني**، مركز الإنترنت والمجتمع
فيتوتاس بوتريماس، مركز امتياز أمن الطاقة بحلف شمال الأطلسي (NATO)
Cybersecurity Tech Accord
مايكل دانيال، تحالف التهديدات السيبرانية
Global Partners Digital
أرفيند جوبتا و**ديكي كومار**، مؤسسة Vivekananda International Foundation
تارا هاريستون و**أناستاسيا كازاكوفا**، Kaspersky
سفين هيربج، Stiftung Neue Verantwortung
درو ميتنك، Access Now
جورج إم مور، مركز جيمس مارتن لدراسات عدم الانتشار
بريت فان نيكيرك و**تريشانا راملوكان**، جامعة كوازولو-ناتال
بيتر سواير، **جاستن هيمينغز**، و**سرينيدي سرينيفازان**، كلية جورجيا تك شيلر للأعمال
جوان دي ويت، Siemens/TU Delft

وأخيرًا، تود اللجنة تقديم الشكر للخبراء التالين، الذين ساهموا بعملهم وخبرتهم في توجيه مداولات اللجنة وتثقيفها:

دينيس برودرز، جامعة ليدن
يبورا براون و**فيرونيكا فيراري**، جمعية الاتصالات التقدمية
مايكل دانيال، تحالف التهديدات السيبرانية
فرانسوا ديليرو، Institut de Recherche Stratégique de l'École Militaire – IRSEM
أخيل ديو و **أرون موان سوكومار**، مؤسسة أوبزيرفر للبحوث (ORF)
مارثا فينمور، جامعة جورج واشنطن
أودي جيري، جامعة روان
دنكان هوليس، كلية الحقوق بجامعة تمبل
جوانا كوليزا، جامعة لودز
بيتر رولاند، غرفة مقاصة الحزم
مايكل شميت، كلية الحقوق بجامعة إكسيت

Patra Kongsirimongkolchai / EyeEm / Getty Images

الأمانة العامة

الشركاء

الجهات الراعية

الإدارة الفيدرالية للشؤون الخارجية بسويسرا

منظمة جلوبسيك

وزارة الخارجية الإستونية

وزارة الشؤون الداخلية والاتصالات اليابانية

الجهات الداعمة

مفوضية الاتحاد الأفريقي

بلاك هات أمريكا

ديف كون

وفد الاتحاد الأوروبي إلى الأمم المتحدة بجينيف

المنتدى العالمي للخبرة السيبرانية

Google

بلدية لاهاي

منظمة باكيت كليرينج هاوس

جامعة تل أبيب

معهد الأمم المتحدة لبحوث نزع السلاح

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE