تجزئة الإنترنت والأمن الإلكتروني:

دليل تمهيدي

صامويل دومينيوني، متحصل على شهادة الدكتوراه

ملخص النقاط الرئيسية

- يُعد النهوض ببيئة منفتحة وآمنة ومستقرة وميسرة وسلمية لتكنولوجيا المعلومات والاتصالات هدفًا ثابتًا في العمليات المتعددة الأطراف المتعلقة بالأمن الدولي وأمن تكنولوجيا المعلومات والاتصالات في الأمم المتحدة. ويمثل الفريق العامل المفتوح العضوية علامة فارقة في التعاون الدولي الرامي لإرساء مثل هذه البيئة.
- لا يزال الإنترنت في جوهره مستقرًا ومنفتحًا وآمنًا بشكل عام. ومع ذلك، يشكل تنامي ظاهرة تجزئة الإنترنت مصدرًا للقلق. قد تختلف مفاهيم التجزئة باختلاف الأطراف المعنية لكن يمكن تحديد بعد تقني لها. وفي هذا السياق، قد تؤثر التجزئة على العناصر الأساسية التي تضمن قابلية التشغيل البيني للشبكات والأجهزة.
- إذ يوجد ثلاثة مجالات رئيسية مثيرة للقلق في البعد التقني لتجزئة الإنترنت تتعلق بالعنونة والتسمية والتوجيه. بعض هذه المخاوف نابعة من الابتكارات الضرورية التي كان على مجتمع أصحاب المصلحة المتعددين تطويرها لمعالجة الاستخدام المتزايد لتكنولوجيا المعلومات والاتصالات ولكنها لم تنفذ بالكامل بعد (مثل بروتوكول الإنترنت الإصدار 4 وبروتوكول الإنترنت الإصدار 6)؛ والبعض الآخر ناتج عن الاتجاهات الناشئة في تطوير المكونات التقنية الحرجة التي تنحرف عن المعايير والبروتوكولات الدولية الحالية (على سبيل المثال، في نظام أسماء النطاقات)؛ وأخيراً، يتعلق البعض الآخر بالعيوب أو القيود التقنية في تصميم وتطوير المكونات الأساسية للإنترنت (مثل التوجيه).
- تؤدي هذه المجالات من التجزئة إلى إضعاف الإنترنت العالمي وانفتاحه واستقراره وإمكانية الوصول إليه، ولها أيضًا آثار على الأمن الإلكتروني. وتتعلق بعض هذه الآثار بمعايير وبروتوكولات الأمن الإلكتروني في حد ذاتها (مثل بروتوكولات التوجيه) والتي قد تتأثر بأشكال متنوعة من الأنشطة الضارة لتكنولوجيا المعلومات والاتصالات. والبعض الآخر يتعلق بإمكانية الوصول إلى البيانات وتوافره وأمنه لخطر متزايد (كما هو الحال مع أنظمة التسمية البديلة). بشكل عام، وبالنظر إلى التعقيد الشديد والترابط الوثيق الذي يكتنف بنية الإنترنت، يمكن أن تؤدي تجزئة البعد التقني إلى ظهور مخاطر معقدة ومتعددة الأوجه (ما يعرف "بالمشكلات الشائكة") تؤثر على الأمن الإلكتروني.
- وتسعى الأبحاث المستقبلية إلى استكشاف كيفية تأثير هذه المخاطر والاتجاهات المحددة في هذا الدليل التمهيدي على تطبيق إطار السلوك المسؤول للدول في الفضاء الإلكتروني، وما يترتب على ذلك من تداعيات على السلام والأمن الدوليين.

مقدمة

يُعد النهوض ببيئة منفتحة وآمنة ومستقرة وميسرة وسلمية لتكنولوجيا المعلومات والاتصالات هدفًا ثابتًا في العمليات المتعددة الأطراف المتعلقة بالأمن الدولي وأمن تكنولوجيا المعلومات والاتصالات في الأمم المتحدة. فعلى سبيل المثال، أكد التقرير النهائي لفريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي لعام 2021، أن "الحفاظ على بيئة منفتحة وآمنة ومستقرة ومتاحة وسلمية لتكنولوجيا المعلومات والاتصالات يُعد ضرورة أساسية للجميع، ويتطلب تعاوناً فعالاً بين الدول للحد من المخاطر التي تهدد السلم والأمن الدوليين".[1] وأشار التقرير النهائي للفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي إلى أن "الفريق العامل المفتوح العضوية يمثل علامة فارقة في التعاون الدولي من أجل إنشاء بيئة منفتحة وآمنة ومستقرة وميسرة وسلمية لتكنولوجيا المعلومات والاتصالات".[2] علاوة على ذلك، شدد كلا التقريرين على أهمية حماية البنية التحتية التقنية اللازمة لتوافر وسلامة الإنترنت بشكل عام.[3] وقد أكد قرار الجمعية العامة الذي نشأ بموجبه الفريق العامل المفتوح العضوية الحالي (2021-2025): "ما خلص إليه فريق الخبراء الحكوميين، في تقريريه لعامي 2013 و2015، من أن القانون الدولي، وعلى وجه الخصوص ميثاق الأمم المتحدة، ينطبق على استخدام الدول لتكنولوجيا المعلومات والاتصالات وهو عنصر لا بد منه

---

[1] الجمعية العامة، 2021، A/76/135، https://undocs.org/Home/Mobile?FinalSymbol=A%2F76%2F135.

[2] الجمعية العامة، 2021، A/75/816، https://undocs.org/Home/Mobile?FinalSymbol=A%2F75%2F816

[3] يطالب تقرير فريق الخبراء الحكوميين لعام 2021، "بتوافر أو سلامة الإنترنت بشكل عام". انظر الجمعية العامة، 2021، A/76/135، الفقرة 10.

لصون السلام والاستقرار وتهيئة بيئة لتكنولوجيا المعلومات والاتصالات تكون منفتحة وآمنة ومستقرة وميسرة وسلمية".[4] ومع ذلك، أصبحت تجزئة بيئة تكنولوجيا المعلومات والاتصالات، ولا سيما الإنترنت مصدر قلق متزايد، وقد بدأت بالظهور في بعض السياقات. في الواقع، يمكن أن تؤثر تجزئة الإنترنت على مستويات مختلفة وأحياناً متداخلة، بما في ذلك السياسية والتجارية والتكنولوجية.[5] ويزداد عدد الدول وأصحاب المصلحة الآخرين الذين يعربون عن قلقهم حيال سيناريو تجزئة الإنترنت. وفي هذا السياق، أدرج تقرير الأمين العام المعنون "خطتنا المشتركة" تجنب تجزئة الإنترنت كإجراء يجب النظر فيه، فضلًا عن أنه أحد الموضوعات الرئيسية التي سيتم تناولها في الاتفاق الرقمي العالمي القادم.

يُعد هذا الدليل التمهيدي أولى ثمار مشروع أشمل حول تجزئة الإنترنت والأمن الدولي، ويهدف إلى تقديم موضوع تجزئة الإنترنت وتحديد أبرز التحديات التي قد تطرأ على الأمن الإلكتروني بمفهومه الواسع. واستناداً إلى هذه الثمرة الأولى، سيستعرض الجزء الثاني من المشروع البحثي تأثير تجزئة الإنترنت على الأمن الدولي، مع التركيز بشكل خاص على تطبيق إطار السلوك المسؤول للدول في الفضاء الإلكتروني (يشار إليه لاحقًا بالإطار). يهدف هذا الدليل التمهيدي إلى تقديم لمحة عامة تمهيدية عن تطورات تجزئة الإنترنت وتداعياتها على الأمن الإلكتروني لصانعي السياسات والدبلوماسيين وغيرهم من الأطراف غير التقنية المهتمة بالموضوع. وقد استندت المادة المعروضة هنا إلى مصادر متاحة للجمهور، ومقابلات الخبراء (أُجريت بين سبتمبر ونوفمبر 2023)، بالإضافة إلى حوارات متعددة الأطراف شارك فيها ممثلون عن القطاع الخاص والأوساط الأكاديمية والمجتمع المدني وعُقدت عبر الإنترنت في 17 أكتوبر 2023.

مفهوم تجزئة الإنترنت

يعد مفهوم تجزئة الإنترنت موضع خلاف حيث تختلف تفسيراته باختلاف صاحب المصلحة. ومع ذلك، تشير بعض الدراسات العلمية إلى إمكانية تحديد اتجاه ثلاثي الأبعاد لفهم تجزئة الإنترنت، يتمثل في التجزئة التقنية والتجزئة التجارية والتجزئة الحكومية.[6] بينما يطرح آخرون تصورًا آخر للتجزئة الثلاثية مع اختلافات طفيفة في الفهم.[7] ونظرًا لأن هذا الدليل التمهيدي يُعنى بتأثير تجزئة الإنترنت على الأمن الإلكتروني، فإنه يولي اهتمامًا خاصًا لتحليل البعد التقني لهذه الظاهرة.[8]

وفقًا للكتاب الأبيض الصادر عن المنتدى الاقتصادي العالمي حول تجزئة الإنترنت، تحدث التجزئة التقنية عندما تظهر "ظروف في البنية التحتية الأساسية [أي طبقات الإنترنت] تعيق قدرة الأنظمة على التفاعل الكامل وتبادل حزم البيانات وقدرة الإنترنت على العمل باستمرار عبر جميع النقاط الطرفية".[9] يقدم الإطار 1 لمحة موجزة عن طبقات الإنترنت ووظائفها.

الإطار 1: طبقات الإنترنت

تعتبر نماذج الربط البيني للأنظمة المفتوحة (OSI) وبروتوكول مراقبة الإرسال/بروتوكول الإنترنت (TCP/IP) من بين أكثر الطرق استخداماً لتصنيف الهيكل الطبقي للإنترنت. وعادة ما يتم تمثيل هذه النماذج على شكل كومة عمودية. وتضطلع كل طبقة بوظيفة مختلفة لكنها مترابطة، تقوم بتحويل المعلومات (مثلا استعلام نصي في متصفح) إلى حزم بيانات مما يتيح الاتصال بين جهازين (أو أكثر).

يتألف **نموذج الربط البيني للأنظمة المفتوحة** من سبع طبقات وهي: التطبيق، والعرض، والجلسة، والنقل، والشبكة، والرابط البياني، والطبقة المادية.

1. توفر **طبقة التطبيق** خدمات لتطبيقات الشبكة التي تستخدم الإنترنت، مثل المتصفحات والبريد الإلكتروني وتطبيقات الاتصالات.
2. في **طبقة العرض**، يتم تنسيق المعلومات الواردة من طبقة التطبيق لعرضها (في حالة الاستقبال) أو لمزيد من المعالجة (في حالة الإرسال).

---

[4] الجمعية العامة، 2020، A/RES/75/240، https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/000/25/PDF/N2100025.pdf

[5] William J. Drake, Vinton G. Cerf, and Wolfgang Kleinwächter, 2016, "Internet Fragmentation: An Overview", Future of the Internet Initiative White Paper, World Economic Forum, https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf.

[6] المصدر نفسه.

[7] على سبيل المثال، تستخدم ورقة مناقشة شبكة سياسات منتدى حوكمة الإنترنت بشأن تجزئة الإنترنت الأبعاد التالية: تجزئة تجربة المستخدم، وتجزئة الطبقة التقنية للإنترنت، وتجزئة حوكمة الإنترنت والتنسيق؛ شبكة سياسات تجزئة الإنترنت، 2023، ورقة مناقشة شبكة سياسات تجزئة الإنترنت (مدخلات لمنتدى حوكمة الإنترنت 2023)، 15 سبتمبر، https://www.intgovforum.org/en/filedepot_download/256/26218.

[8] ستتناول المنشورات القادمة تأثيرات التجزئة السياسية والتجارية على الأمن الإلكتروني.

[9] William J. Drake, Vinton G. Cerf, and Wolfgang Kleinwächter, 2016, "Internet Fragmentation: An Overview", Future of the Internet Initiative White Paper, World Economic Forum, https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf, p. 14.

3. تُعنى **طبقة الجلسة** بعمليات المصادقة والترخيص. على سبيل المثال، تسمح المصادقة (أي تسجيل الدخول إلى تطبيق ما) بإجراء الاتصال بين المستخدم وخادم التطبيق، وبالتالي بدء الجلسة.
4. تضمن **طبقة النقل** موثوقية الاتصال بين الأجهزة والشبكات. وتعتمد على بروتوكولين رئيسيين وهما بروتوكول مراقبة الإرسال (TCP) وبروتوكول مخطط بيانات المستخدم (UDP). يُستخدم البروتوكول الأول لإنشاء اتصالات تضمن نقل المعلومات بين الأجهزة بشكل موثوق، لكنه قد يكون بطيئاً نسبيًا. أما الثاني فيُستخدم للاتصالات التي تتطلب سرعة أكبر ولكن بدقة أقل في نقل البيانات (مثل بث مقاطع الفيديو).
5. تعمل **طبقة الشبكة** على تسهيل نقل البيانات بين الأجهزة في شبكات مختلفة. ومن بين وظائف هذه الطبقة العنونة المنطقية، حيث يتم إرفاق عنوان IP (بروتوكول الإنترنت) الخاص بكل مستخدم بحزمة البيانات لضمان وصولها إلى الوجهة الصحيحة. ثم تُنقل هذه البيانات من خلال أجهزة التوجيه من شبكة إلى أخرى. وتعتمد هذه الطبقة على آلية تحديد المسار من أجل اختيار أفضل مسار ممكن لتسليم البيانات.
6. تساعد **طبقة الربط البياني** في تحضير المعلومات المراد إرسالها بين الشبكات المختلفة كما تعمل على الحد من الأخطاء التي قد تحدث أثناء انتقال البيانات إلى الطبقة التالية.
7. في **الطبقة المادية**، وهي الطبقة الأخيرة في نموذج الربط البيني للأنظمة المفتوحة، تتحول البيانات إلى رموز ثنائية تُحوّل بدورها إلى إشارات تُنقل عبر الوسائط المحلية، وهي الوصلة المادية التي تربط بين الأجهزة (مثل الأسلاك النحاسية أو الألياف الضوئية أو الهواء للإشارات الراديوية). يحدث هذا التحويل في اتجاهين: إما من البيانات إلى الإشارات أثناء الإرسال أو من الإشارات إلى البيانات عند الاستقبال.

نموذج بروتوكول مراقبة الإرسال/بروتوكول الإنترنت مشابه لنموذج الربط البيني للأنظمة المفتوحة، لكنه يجمع طبقات التطبيق والعرض والجلسة في طبقة واحدة تسمى طبقة التطبيق. أما الطبقات المتبقية فتأخذ نفس اسماء الطبقات الموجودة في نموذج الربط البيني للأنظمة المفتوحة، وهي النقل والشبكة والربط البياني والطبقة المادية.

الربط البيني للأنظمة المفتوحة OSI	**بروتوكول مراقبة الإرسال/ بروتوكول الإنترنت TCP**
التطبيق (التفاعل بين الإنسان والحاسوب)	**التطبيق** (عرض البيانات وترميزها والتحكم في الجلسة)
العرض (تمثيل البيانات وتشفيرها)	
الجلسة (الاتصال بين المضيفين)	
النقل (بروتوكول مراقبة الإرسال وبروتوكول مخطط بيانات المستخدم)	**النقل** (بروتوكول مراقبة الإرسال وبروتوكول مخطط بيانات المستخدم)
الشبكة (التوجيه وعناوين بروتوكول الإنترنت IP)	**الشبكة** (التوجيه وعناوين بروتوكول الإنترنت IP)
الربط البياني (تصحيح الأخطاء وإعادة الإرسال)	**الربط البياني** (تصحيح الأخطاء وإعادة الإرسال)
الطبقة المادية (ترسل البيانات إلكترونيًا أو بصريًا أو كموجات راديوية)	**الطبقة المادية** (ترسل البيانات إلكترونيًا أو بصريًا أو كموجات راديوية)

في الواقع، يمكن للإنترنت أن يكون شريانًا حيويًا للمنفعة العامة العالمية بفضل بنيته التحتية وخصائصه التي تتيح مد جسور التواصل وتبادل المعلومات (في شكل حزم بيانات) دون النظر لأي قيود تفرضها الحدود الجغرافية أو الاجتماعية. من بين هذه العناصر، هناك مكونات أساسية تضمن قابلية التشغيل البيني للشبكات والأجهزة (انظر الإطار 2).

الإطار 2: المكونات الأساسية للإنترنت.

ساهمت المبادرات التالية في تسليط الضوء على المكونات الأساسية للإنترنت.

فقد قدمت اللجنة العالمية المعنية باستقرار الفضاء الإلكتروني مفهوم "الجوهر العام للإنترنت"، والذي يشمل:

1. توجيه الحزم وإرسالها
2. أنظمة التسمية والترقيم
3. آليات التشفير الخاصة بالأمن والهوية
4. وسائط الإرسال
5. البرمجيات
6. مراكز البيانات[10]

اقترحت جمعية إنترنت Internet Society خمس خصائص جوهرية تحدد الوظائف الأساسية لشبكات الإنترنت، وهي:

1. البنية التحتية المتاحة التي تعتمد على بروتوكول موحد مفتوح دون حواجز تمنع الوصول.
2. البنية المفتوحة لوحدات البناء القابلة للتشغيل البيني والقابلة لإعادة الاستخدام التي تستند إلى عمليات تطوير مفتوحة المعايير يعتمدها مجتمع المستخدمين طواعية.
3. إدارة لامركزية ونظام توجيه موزع موحد يتميز بالمرونة والقابلية للتوسع.
4. معرّفات عالمية مشتركة لا لبس فيها وشاملة.
5. شبكة محايدة تقنياً وعامة الأغراض بسيطة وقابلة للتكيف.[11]

توضح ورقة المناقشة الصادرة عن شبكة سياسات منتدى حوكمة الإنترنت بشأن تجزئة الإنترنت أن تجزئة البنية التحتية التقنية للإنترنت ترتبط "بمجموعة من التحديات التي تعيق قابلية التشغيل البيني في الطبقة التقنية للنقل، وهي الأساس الذي يجعل الإنترنت يعمل بشكل فعّال".[12] وبالفعل، يعتمد الإنترنت العالمي "أساساً على تصميم طبقة النقل في الإنترنت والاستخدام الموحد لنفس البروتوكولات التقنية (بروتوكول مراقبة الإرسال/بروتوكول الإنترنت TCP/IP، ونظام أسماء النطاقات DNS، وبروتوكول بوابة الحدود BGP، وبروتوكول نقل النصوص المترابطة HTTP، و بروتوكول الإنترنت - الإصدار 4 و6 (IPv4&6) و غيرها)، والتي تستند إلى نظام جذر موحد ولكنه لا مركزي يدعم جميع أشكال الاتصالات عبر الإنترنت".[13] لذلك، ونظرًا للسمات الأساسية المرتبطة بالمكونات الحيوية للإنترنت، فإن أي محاولات لتجزئة هذا البعد التقني ستشكل تهديدًا بالغ الخطورة على انفتاح الإنترنت وقابليته للتشغيل البيني.

مجالات المخاطر المتعلقة بتجزئة الإنترنت على المستوى التقني

تعد التجزئة التقنية مصدر قلق متزايد، خاصة بالنسبة للمجتمع المتعدد الأطراف الذي يُعنى بالمكونات الأساسية للإنترنت. وقد أشار الكتاب الأبيض الصادر عن المنتدى الاقتصادي العالمي في عام 2016 حول تجزئة الإنترنت إلى أن "الإنترنت لا يزال مستقرًا ومنفتحًا وآمنًا بشكل عام في أسسه".[14] وبعد مرور ثماني سنوات تقريبًا، وهي فترة زمنية طويلة في عالم التكنولوجيا، لا تزال هذه الأسس متينة على الرغم من تصاعد نقاط الضعف والمخاطر.[15] وللاستفادة بشكل متسق من الأدبيات الموجودة، لا سيما الكتاب الأبيض للمنتدى الاقتصادي

[10] Global Commission on the Stability of Cyberspace, "Advancing Cyberstability", November 2019, https://hcss.nl/wp-content/uploads/2019/11/GCSC-Final-Report-November-2019.pdf.

[11] Internet Society, "The Internet Way of Networking: Defining the Critical Properties of the Internet", September 2020, https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/critical-properties-of-the-internet/.

[12] PNIF, 2023, PNIF Discussion Paper (input to IGF 2023), 15 September, https://www.intgovforum.org/en/filedepot_download/256/26218, p. 12.

[13] Wolfgang Kleinwächter and Alexander Klimburg, 2023, "Fragment or Not Fragment – Is This the Question? Will the "One World-One Internet" Survive Today's Geopolitical Stress Test?", CircleID, 6 June, https://circleid.com/posts/20230606-fragment-or-not-fragment-is-this-the-question-will-one-world-one-internet-survive-todays-geopolitical-stress-tests.

[14] William J. Drake, Vinton G. Cerf, and Wolfgang Kleinwächter, 2016, "Internet Fragmentation: An Overview", Future of the Internet Initiative White Paper, World Economic Forum, https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf, p. 8.

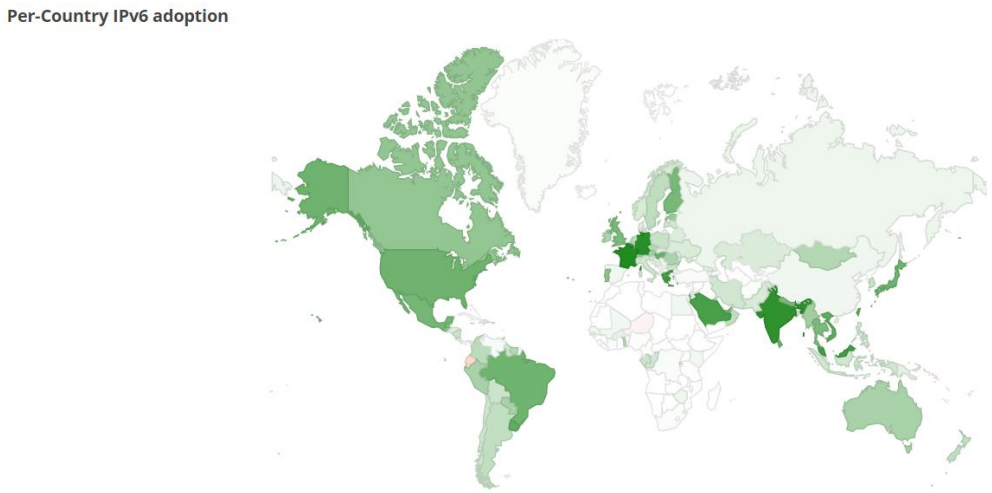
[15] مقابلة أجراها المؤلف مع الدكتور فينتون ج. سيرف، أحد مؤلفي الكتاب الأبيض للمنتدى الاقتصادي العالمي حول تجزئة الإنترنت، 26 أكتوبر 2023.

العالمي، يركز هذا الموجز على مجالات المخاطر نفسها، وهي العنونة والتسمية (نظام أسماء النطاقات) وتوجيه الاتصال (الربط البيني)[16] للإنترنت، بهدف تحديد الاتجاهات القائمة التي تضعف أسس الإنترنت.

العنونة

تتعلق العنونة بالمعرّفات الفريدة، أو ما يسمى بعناوين IP، وهي عبارة عن قيم عشرية تُستخدم لتحدد نقاط فريدة على الإنترنت. وهناك مسألتان رئيسيتان تتعلقان بعناوين IP وتجزئة الإنترنت. تتعلق الأولى باعتماد وتوافق نسختين من بروتوكول الإنترنت IPv4 و IPv6، وترتبط الثانية بإدارة أرقام IP.

حالياً، هناك نسختان رئيسيتان من عناوين بروتوكول الإنترنت: بروتوكول الإنترنت - الإصدار 4 (IPv4) وبروتوكول الإنترنت - الإصدار 6 (IPv6). يعتمد الأول على مساحة عنوان بطول 32 بت، مما يتيح إنشاء ما يصل إلى حوالي 4.3 مليار عنوان. ونتيجة للزيادة الهائلة في عدد الأجهزة المتصلة بالإنترنت خلال العقود الماضية، استُنفدت جميع التوليفات الممكنة لعناوين IPv4. لذلك، واستجابة لهذه الحاجة إلى المزيد من المعرفات الفريدة، تم تقديم إصدار جديد من بروتوكول الإنترنت (IPv6) باستخدام مساحة عنوان 128 بت. ويمكن لهذا الإصدار تغطية ما يصل إلى 340 تريليون تريليون تريليون نقطة نهائية.[17] ومع ذلك، لا يقبل الإصداران IPv4 و IPv6 التشغيل البيني المباشر. وهذا يعني أن الأجهزة الموجودة على شبكات IPv4 لا يمكنها الاتصال بالأجهزة الموجودة على شبكات IPv6.[18] ولا يمكن تحقيق التوافق بينها إلا من خلال تقنيات الانتقال، مثل الشبكات ذات الكومة المزدوجة. ويمكن أن تحدث التجزئة نتيجة للتباين بين إصدارات بروتوكول الإنترنت IP التي لا تدعمها تقنيات الانتقال بين الدول والمناطق حول العالم. وعلى الرغم من أن مستوى اعتماد بروتوكول IPv6 [19] يتزايد باستمرار، إلا أنه يختلف من دولة إلى أخرى.



الشكل 1 اعتماد IPv6 حسب البلد - كلما كان اللون أغمق كلما زادت نسبة الاتصال بهذا البروتوكول (المصدر: إحصائيات غوغل)

[16] من بين الطرق البسيطة لفهم مصطلحات العنونة والتسمية والتوجيه هي النظر إليها على النحو التالي "يشير اسم المورد إلى ما نبحث عنه، ويشير العنوان إلى مكان وجوده، ويحدد التوجيه المسار الذي يجب اتباعه للوصول إليه"، John F. Schoch, 1978, "A Note on Inter-Network Naming, Addressing, and Routing", Internet Experiment Note # 19, Notebook Section 2.3.3.5 https://www.rfc-editor.org/ien/ien19.txt.

[17] William J. Drake, Vinton G. Cerf, and Wolfgang Kleinwächter, 2016, "Internet Fragmentation: An Overview", Future of the Internet Initiative White Paper, World Economic Forum, https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf.

[18] Erik Bais, "IPv4 vs IPv6: What Security Professionals Should Know", Prefix Broker, https://www.prefixbroker.com/news/ipv4-vs-ipv6-what-security-professionals-should-know/.

[19] في وقت نشر الكتاب الأبيض للمنتدى الاقتصادي العالمي، كانت نسبة الاتصال بالإصدار السادس من بروتوكول الإنترنت IPv6 لا تتجاوز 4 في المائة من الإنترنت، في حين أنها في أكتوبر 2023، أصبحت حوالي 40 في المائة (المصدر https://www.google.com/intl/en/ipv6/statistics.html).

لذلك، فمن الممكن حدوث تجزئة على طول هذا الجانب من الفجوة الرقمية، مما يشكل مخاطر على قابلية التشغيل البيني للشبكات والأجهزة عبر البلدان والمناطق.

أما الجانب الثاني من تجزئة بروتوكول الإنترنت IP، فيتعلق بإدارة أرقام بروتوكول الإنترنت المستخدمة في إنشاء عناوين بروتوكول الإنترنت. ففي الوضع الحالي للإنترنت، تُدار هذه المهمة من قبل هيئة الإنترنت للأرقام المخصصة Assigned Number Authority (وهي فرع تابع لمؤسسة الإنترنت للأسماء والأرقام المخصصة Internet Corporation for Assigned Names and Numbers)، بالتعاون مع منظمة سجلات الإنترنت الإقليمية Regional Internet Registers، وتُنفذ على نطاق واسع نظرًا لأن هياكل الإنترنت لا تقتصر على الحدود الوطنية. يعد وجود نظام يضمن التفرد العالمي لبروتوكولات الإنترنت أمرًا بالغ الأهمية؛ إذ أن غياب مثل هذا النظام قد يؤدي إلى إنشاء عناوين بروتوكول الإنترنت البديلة وغير المنسقة مما قد يعقد أو يمنع تحقيق التوافق مع البنية التحتية القائمة التي تعتمد على بروتوكولي IPv4 أو IPv6.[20]

التسمية

تشير التسمية إلى نظام أسماء النطاقات DNS، الذي يترجم الأسماء إلى عناوين بروتوكول الإنترنت (على سبيل المثال، بالنسبة لموقع معهد الأمم المتحدة لبحوث نزع السلاح على الويب فإن اسم النطاق هو https://unidir.org وبروتوكول الإنترنت المقابل له هو 34.107.109.130). ولضمان هذه الخاصية، من الضروري أن تظل إدارة عملية الربط والتطابق الفريدة (التي تقوم بها مؤسسة الإنترنت للأسماء والأرقام المخصصة) مستقرة ومتسقة وشرعية. وأي محاولات لإنشاء أنظمة أسماء بديلة (بما في ذلك إدارة منطقة الجذر[21]) قد تُعد من أسوأ أشكال التجزئة الممكنة[22] لأنها ستؤدي إلى فقدان الترجمات الفريدة لنظام أسماء النطاقات. ويمكن أن تترتب على ذلك تناقضات واحتمال أخطاء في البحث عن نظام أسماء النطاقات؛ فعلى سبيل المثال، قد يؤدي إدخال الرابط https://unidir.org من قبل مستخدمين مختلفين إلى فتح صفحات غير تلك المقصودة.

التوجيه

يُقصد بالتوجيه البروتوكولات التي تضمن أن المعلومات تتبع المسار الصحيح والأمثل عند انتقالها عبر الشبكة. وفي حال كان من الضروري نقل المعلومات من شبكة إلى أخرى (حيث يتكون الإنترنت من العديد من الشبكات المختلفة التي تُدار عادة بشكل منفصل بواسطة مقدم خدمة واحد)، فإنّ بروتوكولات بوابة الحدود (BGP) تعمل على ربط هذه الشبكات، مما يمكّن النظام العالمي للتوجيه في الإنترنت. وكما أشار الكتاب الأبيض للمنتدى الاقتصادي العالمي، "لا يزال من الممكن تقنيًا حدوث تلف متعمد أو عرضي في بيانات التوجيه".[23] إذ لا يزال أمان نظام التوجيه بحاجة إلى تحسينات، على سبيل المثال، من خلال تنفيذ ما يسمى بالبنية التحتية للمفاتيح العامة للموارد Resource Public Key Infrastructure ، وهو إطار البنية التحتية للمفاتيح العامة المصمم لتأمين بروتوكول بوابة الحدود.[24] وبشكل عام، إذا لم يكن بروتوكول بوابة الحدود محميًا بشكل كافٍ، فقد تحدث التجزئة نتيجة لعجز الشبكة عن ضمان سرية البيانات وسلامتها وتوافرها.

المجالات المثيرة للقلق في الأمن الإلكتروني

لا يركز هذا الدليل التمهيدي على فهم تجزئة الإنترنت وحالتها الراهنة فحسب، بل أيضاً على تحديد الآثار المحتملة لها على الأمن الإلكتروني. ويتناول هذا الدليل الأمن الإلكتروني من منظور شامل يعتمد على ما يسمى بمثلث الأمن الإلكتروني[25] والمصداقية. بشكل عام، يمكن أن تؤدي تجزئة الإنترنت إلى العديد من المخاطر في مجال الأمن الإلكتروني التي قد تشمل ما يسمى بـ "المشكلات المستعصية".

---

[20] انظر، على سبيل المثال، النقاش الدائر حول الاقتراح الخاص بـ"بروتوكول الإنترنت الجديد": Alain Durand, 2020, "New IP", ICANN Office of the Chief Technology Officer, https://www.icann.org/en/system/files/files/octo-017-27oct20-en.pdf.

[21] منطقة الجذر هي الجزء العلوي في بنية نظام أسماء النطاقات الهرمية (على سبيل المثال، في https://unidir.org الجزء العلوي هو ".org").

[22] Multi-stakeholder dialogue on Internet Fragmentation and Cybersecurity, 17 October 2023; William J. Drake, Vinton G. Cerf, and Wolfgang Kleinwächter, 2016, "Internet Fragmentation: An Overview", Future of the Internet Initiative White Paper, World Economic Forum, https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf.

[23] المصدر نفسه، ص 23.

[24] مقابلة أجراها المؤلف مع الدكتور فينتون جي. سيرف، أحد مؤلفي الكتاب الأبيض، 26 أكتوبر 2023.

[25] يركز المثلث على ضمان أمن البيانات ويشمل سريتها وتوافرها وسلامتها. يشير التوافر إلى ضرورة أن تكون البيانات متاحة للمستخدمين المصرح لهم في أي وقت يحتاجون إليها؛ وأي حدث قد يؤثر على قدرتهم على الوصول إليها يعد تهديدًا لتوافر البيانات. تشير السرية إلى إمكانية الوصول إلى بيانات محددة بحيث تكون في متناول المستخدمين المصرح لهم فقط، ويجب أن تبقى سرية أو خاصة. تتعلق السلامة بمصداقية واعتمادية وموثوقية البيانات؛ وهذا يعني عدم التلاعب بالبيانات. See Samuele Dominioni and Giacomo Persi Paoli, 2022, "A Taxonomy of Malicious ICT Incidents", UNIDIR, https://unidir.org/publication/a-taxonomy-of-malicious-ict-incidents/.

وتظهر هذه المشكلات خاصة في المجالات أو الميادين المركبة والمترابطة والتي تضم أطرافًا متعددة (مثل الإنترنت) ويمكن أن تكون شديدة التعقيد ومتعددة الأوجه.[26] وغالبًا ما يكون من الضروري اتباع نهج متعدد الأطراف يشمل التعاون بين مختلف الجهات الفاعلة والقطاعات والدول، للتعامل مع هذه المشكلات المستعصية (انظر الى الجدول 1).[27] ولذلك، فإن "تجزئة الإنترنت تعيق أي محاولة لمعالجة القضايا المتعلقة بالأمن الإلكتروني لأنها تتجاهل العوامل المتشابكة وتغلق المجال أمام أي تعاون محتمل".[28] وعلاوة على ذلك، فإن تجزئة الإنترنت إلى شبكات أصغر قد تؤدي إلى تقليص قدرة الشبكات العامة على الصمود، ذلك لأن قوة الإنترنت تكمن في كونه لا مركزي ومبني على مكونات قابلة للتشغيل البيني (مثل المعايير والبروتوكولات والأجهزة وغيرها)، مما يتيح للمجتمع التقني، عند الحاجة، معالجة المشكلات دون المساس بالشبكة ككل.[29]

النوع	الخصائص	حلول محتملة
بسيطة	الحلول، أو مناهج تصميم الحلول، معروفة	*التعاون*: زيادة الوعي وتبادل المعلومات، عادةً من خلال مجموعات مشغلي الشبكات
معقدة	لا توجد حلول معروفة؛ تمتد المشكلة عبر أجزاء متعددة من الإنترنت	*التوافق*: وضع معايير مفتوحة قائمة على توافق الآراء
مستعصية	لا يوجد حل في أي ميدان؛ عدم وجود اتفاق عام على وجود المشكلة أو كيفية توصيفها	*التآزر*: تجاوز الحدود القائمة بين الميادين والمؤسسات ووضع عمليات جديدة لتحديد المشكلات وصياغة حلول ملائمة لها

الجدول 1: أنواع المشكلات (المصدر: Leslie Daigle, Konstantinos Komaitis and Phil Roberts "Keys to Successful Collaboration (and Solving Wicked Problems", Internet Society, 2016

تسلط العناوين التالية الضوء على المخاوف الأمنية المرتبطة بكل مجال من مجالات التجزئة المحددة.

العنونة

هناك تأثيران رئيسيان مرتبطان بتجزئة العناوين على الأمن الإلكتروني. أولاً، قد يؤدي الاعتماد المتناثر للبروتوكول IPv6 حول العالم إلى تعزيز التجزئة، وذلك بسبب عدم التوافق المباشر بين نموذجي بروتوكول الإنترنت، بالإضافة إلى التناقضات في مستويات التعرض لتهديدات تكنولوجيا المعلومات والاتصالات. يتميز الإصدار السادس من بروتوكول الإنترنت IPv6 بخصائص رئيسية، مثل دمج أمن بروتوكول الانترنت (IPsec)[30]، مما يوفر أماناً أفضل.[31] ومع ذلك، فإن تنفيذ وإعداد IPv6 قد يكون أكثر تعقيدًا من IPv4 ويتطلب معارف ومهارات تقنية متخصصة. والأخطاء في إعداد الأجهزة التي تدعم IPv6 قد تحدث ثغرات أمنية مما يجعل الأجهزة أكثر عرضة للاختراق.[32] علاوة على ذلك، قد تثير الأجهزة والشبكات ذات الكومة المزدوجة (أي التي تعمل على IPv4 و IPv6 في الوقت نفسه) مخاوف أمنية إضافية بسبب توسع المساحة المعرضة للهجوم.[33]

---

[26] تحمل معظم حوادث تكنولوجيا المعلومات والاتصالات الخبيثة الخطيرة لها طابعًا عابرًا للحدود، حيث تشمل العديد من الأصول والجهات الفاعلة من قطاعات ومناطق جغرافية مختلفة.

[27] Leslie Daigle, Konstantinos Komaitis, and Phil Roberts, 2016, "Keys to Successful Collaboration and Solving Wicked Internet Problems", Internet Society, https://www.internetsociety.org/resources/doc/2017/keys-to-successful-collaboration-and-solving-wicked-internet-problems/.

[28] Konstantinos Komaitis, 2023, "Internet Fragmentation: Why It Matters for Europe", Research in Focus, EU Cyber Direct – EU Cyber Diplomacy Initiative, https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/ioyLip9O/internet-fragmentation-why-it-matters-for-europe.pdf, p. 8.

[29] مقابلة المؤلف مع كونستانتينوس كومايتيس، 9 نوفمبر 2023.

[30] أمن بروتوكول الانترنت هو معيار يوفر أمان القنوات في طبقات الإنترنت. أمن بروتوكول الانترنت إلزامي في IPv6، في حين كان اختياريًا في IPv4. See Internet Engineering Task Force (IETF), 2011, "IPv6 Node Requirements, Request for Comment 6434", https://www.rfc-editor.org/rfc/pdfrfc/rfc6434.txt.pdf.

https://www.rfc-editor.org/rfc/pdfrfc/rfc6434.txt.pdf

[31] Emre Durda and Ali Buldu, 2010, "IPV4/IPV6 Security and Threat Comparisons", *Procedia—Social and Behavioral Sciences*, 2, pp. 5285–5291. www.sciencedirect.com/science/article/pii/S187704281000902X

[32] National Security Agency, 2023, "IPV6 Security Guidance", U/OO/105622-23 | PP-22-1805 , ver. 1.0, https://media.defense.gov/2023/Jan/18/2003145994/-1/-1/0/CSI_IPV6_SECURITY_GUIDANCE.PDF

[33] المصدر نفسه.

ثانياً، إن وضع بروتوكولات الإنترنت بدون تنسيق أو بما يتناقض مع النظام القائم قد يعطل بشكل خطير إمكانية الوصول العالمي وأمن الشبكات الوطنية، مع أن حدوث ذلك بعيد الاحتمال ولكنه ممكن. وفي هذه الحالة، ستحتاج الدول إلى العمل على إبرام اتفاقات ثنائية مع مقدمي خدمات الإنترنت وضمان تطبيق معايير وبروتوكولات الأمان لشبكاتها المحلية. لكن ليست كل الدول تتمتع بنفس القدرات لتحقيق نفس مستوى الأمان. وفي الوقت الحالي، يمكن لكل دولة الاعتماد على مجتمع مفتوح متعدد الأطراف مكرس لوضع ومناقشة وتحديث المعايير والبروتوكولات التي تخدم الجميع.

التسمية

إن التجزئة على مستوى التسمية، والتي تحدث في الغالب من خلال وضع أنظمة أسماء بديلة، قد تؤدي إلى إخفاقات جسيمة في مجال الأمن الإلكتروني. وفي هذا السيناريو، على سبيل المثال، قد يواجه المستخدم صعوبة في الوصول إلى الموقع المقصود عند كتابة اسم الموقع وقد ينتهي به الأمر في موقع مختلف. بشكل عام، في حالة وجود أنظمة أسماء بديلة، لن يتمكن المستخدمون من الوصول إلى البيانات، مما يعني أن هذه البيانات ستكون غير متاحة. وعلاوة على ذلك، قد تؤدي الجهود التي يبذلها المجتمع المتعدد الأطراف لربط نظام أسماء النطاقات بأنظمة أسماء بديلة إلى "نتائج غير متوقعة وإحباط المستخدم وارتفاع تكاليف الدعم، وفي النهاية، إلى إنترنت أقل أمانًا واستقرارًا".[34]

التوجيه

بروتوكولات الحدود معرضة للاختراقات التي تعبث بتدفقات البيانات. وفي الواقع، يحتوي بروتوكول بوابة الحدود على آليات داخلية محدودة للحماية ضد الأفعال الخبيثة التي قد تغير البيانات أو حتى تحذفها، مما يشوش على سلوك التوجيه في الشبكة بشكل عام.[35] وبالفعل فإن بروتوكول بوابة الحدود عرضة لتهديدات خطيرة ومختلفة متعلقة بتكنولوجيا المعلومات والاتصالات، بما في ذلك اختطاف التوجيه،[36] مما قد يؤدي إلى تجزئة الإنترنت وآثار تخريبية أو استغلالية.[37] وفي معظم الحالات، تكون هذه الآثار محدودة النطاق والتأثير؛ ولكن، في حالات أخرى، قد تؤدي إلى فشل كارثي في الاتصالات.[38] ويمكن أن يكون تنفيذ البنية التحتية للمفاتيح العامة للموارد RPKI بمثابة إجراء فعال للأمن الإلكتروني.

الخلاصة والخطوات التالية

لا يزال الإنترنت في جوهره مستقرًا ومنفتحًا وآمنًا بشكل عام، ولكنه يواجه تحديات متزايدة مع تفاقم نقاط الضعف والمخاطر على جميع الأصعدة. وقد تؤدي تجزئة الإنترنت على المستوى التقني إلى زعزعة أسس البيئة المنفتحة والآمنة والمستقرة والميسرة والسلمية لتكنولوجيا المعلومات والاتصالات، ما ينذر بعواقب وخيمة على الأمن الإلكتروني.

تشير الاتجاهات المقلقة إلى زيادة محتملة في الممارسات والسياسات التي تتعارض مع المعايير والبروتوكولات التقنية الدولية في المقام الأول، مما يخلق تحديات أمنية عديدة للأمن الإلكتروني. لذلك، فإن أي محاولات تعسفية وأحادية الجانب للتلاعب بالمكونات الحيوية للإنترنت قد تؤدي إلى تفاقم التجزئة القائمة بالفعل وافقار الأمن العام لشبكة الشبكات وتمتد آثارها لأبعد من ذلك. في الواقع، لا تقتصر خطورة تجزئة الإنترنت على الأمن الإلكتروني فحسب، بل تتجاوز ذلك إلى زعزعة الأمن الدولي. وستركز الأبحاث المستقبلية على كيفية تأثير مجالات واتجاهات المخاطر المحددة في هذا الدليل التمهيدي على تنفيذ الإطار، وبالتالي على السلام والأمن الدوليين.

---

[34] Alain Durand, 2022, "Challenges with Alternative Name Systems", OCTO-034, ICANN, https://www.icann.org/en/system/files/files/octo-034-27apr22-en.pdf.

[35] IETF, 2006, RFC#4272, "BGP Security Vulnerabilities Analysis", https://datatracker.ietf.org/doc/html/rfc4272.

[36] يحدث هذا السيناريو عندما يقوم المهاجمون بإعادة توجيه حركة تدفق البيانات عبرالإنترنت بشكل خبيث عن طريق الإعلان الزائف عن عنوان IP، مما يؤدي في الواقع إلى توجيه البيانات إلى عنوان آخر. بعبارة أخرى، "تشبه عملية اختطاف بروتوكول بوابة الحدود إلى حد كبير قيام شخص ما بتغيير جميع اللوحات الإرشادية الموجودة على جزء من الطريق السريع وإعادة توجيه حركة المرور إلى مخارج غير صحيحة"؛ Cloudflare, "What is BGP Hijacking", https://www.cloudflare.com/learning/security/glossary/bgp-hijacking/

[37] يترك كل حادث إلكتروني تأثيرًا على الهدف، ويمكن تصنيفه إلى نوعين رئيسيين من التأثيرات الأولية: التخريبية، والتي تشير إلى التدخل في وظائف تكنولوجيا المعلومات والاتصالات، والاستغلالية، والتي تتعلق بسرقة المعلومات. See Samuele Dominioni and Giacomo Persi Paoli, 2022, "A Taxonomy of Malicious ICT Incidents", UNIDIR, https://unidir.org/files/2022-08/UNIDIR_Taxonomy_of_Malicious_ICT_Incidents.pdf; Charles Harry and Nancy Gallagher, 2018, "Classifying Cyber Events", *Journal of Information Warfare*, vol. 17, no. 3, https://www.jstor.org/stable/26633163, pp. 17–31.

[38] "على سبيل المثال، تعتمد التطبيقات الحيوية مثل المعاملات الإلكترونية المصرفية، وتداول الأسهم، والتطبيب عن بعد بشكل أساسي على الإنترنت"، Kevin Butler et al., 2010, "A Survey of BGP Security Issues and Solutions", *Proceedings of the IEEE*, Vol. 98, No. 1, https://ieeexplore.ieee.org/abstract/document/5357585, pp. 100–122..

وفي الختام، لضمان بيئة منفتحة وآمنة ومستقرة وميسرة وسلمية لتكنولوجيا المعلومات والاتصالات، يجب على مجتمع أصحاب المصلحة المتعددين - بما في ذلك الدول الأعضاء - أن يعمل على حماية سلامة المكونات الحيوية للإنترنت وتوافرها وترابطها. ولتحقيق ذلك، من الضروري فهم الترابط بين هذه المكونات والتأثيرات المتسلسلة التي قد تنشأ عن العبث بهذه الأنظمة المعقدة والمتشابكة، وتبعات ذلك على هذا المجال المشترك العالمي الذي أنشأه الإنسان. ويعد هذا الدليل التمهيدي جزءًا من الجهود الرامية لتحقيق هذه الغاية.

شكر وتقدير

يشكل الدعم الذي تقدمه الجهات المانحة الرئيسية لمعهد الأمم المتحدة لبحوث نزع السلاح الأساس لجميع أنشطته. وقد موّل الاتحاد الأوروبي هذا المنشور كجزء من برنامج الأمن والتكنولوجيا التابع لمعهد الأمم المتحدة لبحوث نزع السلاح، والذي تدعمه حكومات كل من تشيكيا وألمانيا وإيطاليا وهولندا وسويسرا، وكذلك شركة مايكروسوفت. هذا ويتقدم المؤلف بالشكر لمجموعة متنوعة من الخبراء من قطاع الصناعة والحكومة والأوساط الأكاديمية الذين أسهموا بتقديم ملاحظات قيمة على النسخ المختلفة وأقسام محددة من هذه الورقة وشاركوا في حلقة عمل أصحاب المصلحة المتعددين، بما في ذلك أنج بنيامين، جايا بالو، فينتون سيرف، آلان دوراند، ماري هومو، كونستانتينوس كوميتيس، أليسون مانكين، كيفن ريفستيك، روب سبيجر، بيل وودكوك، مايكل زابا. كما ساهمت إيليا سميث، وهي خريجة متخصصة في برنامج الأمن والتكنولوجيا، في المشروع البحثي.

نبذة عن معهد الأمم المتحدة لبحوث نزع السلاح

معهد الأمم المتحدة لبحوث نزع السلاح هو معهد مستقل ممول طوعيًا تابع للأمم المتحدة. يعد معهد الأمم المتحدة لبحوث نزع السلاح أحد المعاهد السياسية القليلة في العالم التي تركز على نزع السلاح، ويعمل على إنتاج المعرفة وتعزيز الحوار والعمل بشأن نزع السلاح والأمن. يقع مقر معهد الأمم المتحدة لبحوث نزع السلاح في جنيف، ويساعد المجتمع الدولي على تطوير الأفكار العملية والمبتكرة اللازمة لإيجاد حلول للمشكلات الأمنية الحرجة.

الاقتباس

ص. دومينيوني. Internet Fragmentation and International Security. Exploring the Cybersecurity Implications. جنيف، سويسرا: معهد الأمم المتحدة لبحوث نزع السلاح، 2023.

ملاحظة

إن التسميات المستخدمة في هذا المنشور وطريقة تقديم المادة فيه لا تعبر عن أي رأي مهما كان من جانب الأمانة العامة للأمم المتحدة فيما يتعلق بالوضع القانوني لأي بلد أو إقليم أو مدينة أو منطقة، أو لسلطات أي منها، أو فيما يتعلق بتعيين حدودها أو تخومها. الآراء الواردة في المنشور تقع ضمن مسؤولية مؤلفيها فقط. إنها لا تعكس بالضرورة آراء أو وجهات نظر الأمم المتحدة أو معهد الأمم المتحدة لبحوث نزع السلاح أو موظفيها أو الجهات الراعية لها.