UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

التعاون الدولي للتخفيف من العمليات الإلكترونية التي تمس البنية التحتية الحيوية

التوقعات المعيارية والممارسات الجيدة الناشئة

أندراز كاستيليك

شكر وتقدير

يشَكّل الدعم المالي الأساسي المقدم من مختلف الجهات لمعهد الأمم المتحدة لبحوث نزع السلاح الأساس لجميع أنشطته. وقد أُجريت هذه الدراسة من قبل برنامج الأمن والتكنولوجيا، الذي تموله حكومة كلٍّ من فرنسا، وألمانيا، وهولندا، والنرويج، وسويسرا، وكذلك شركة مايكروسوفت. هذا ويتقدم المؤلف بالشكر إلى الأفراد التالية أسماؤهم على مشورتهم القيّمة ومساعدتهم في هذا التقرير: كيري آن باريت (منظمة الدول الأمريكية)؛ جياكومو بيرسي باولي (معهد الأمم المتحدة لبحوث نزع السلاح)؛ والمشاركون في جلستنا الحوارية مع أصحاب المصلحة المتعددين بعنوان «تفعيل المعايير الإلكترونية: حماية البنية التحتية الحيوية»، التي عقدت في 3 يوليو 2020: أوليغ عبدوراشيتوف (كاسبيرسكي لاب)، وكاجا سيغليك (مايكروسوفت)، ومارك هيناور (المركز الوطني للأمن الإلكتروني، سويسرا)، وولفارم فون هاينز (المكتب الفيدرالي الألماني)، ودانيال كلينجيل (الإدارة الفيدرالية للشؤون الخارجية، سويسرا)، وتيمو إس كوستر وزارة الخارجية، هولندا)، وكريس كوبيكا (HypaSec)،وأندريه سالغادو (مجموعة CITI). الشكر موصول أيضًا لـ إيفغيني غونشاروف، وغليب جريستال، وأناستازيا كازانوفا من «كاسبرسكي لاب» على مساهمتهم بمعرفتهم المتعمقة في هذه الصناعة.

تصميم وتخطيط المنشور: إريك إم شولز
الرسوم البيانية: يوروس بودجوريليك

ملاحظة

لا تعني التسميات المستخدمة وطريقة عرض المواد في هذا المنشور التعبير عن أي رأي مهما كان من جانب الأمانة العامة للأمم المتحدة بشأن الوضع القانوني لأي بلد أو إقليم أو مدينة أو منطقة أو لسلطاتها، أو بشأن ترسيم حدودها أو قيودها الجغرافية. هذا وتُعتبر الآراء المُعبر عنها في هذا المنشور مسؤولية المؤلفين الفردية، وهي لا تعكس بالضرورة وجهات نظر أو آراء الأمم المتحدة، أو معهد الأمم المتحدة لبحوث نزع السلاح، أو موظفيه، أو الجهات الراعية.

قائمة المحتويات

	الملخص التنفيذي	**vi**
1	**فهم المشكلة والسيا**	**1**
1.1	انتشار الحوادث الإلكترونية التي تؤثر على البنية التحتية الحيوية	1
2.1	الآثار المترتبة على تعطُّل البنية التحتية الحيوية	3
3.1	تحديات إدارة العمليات الإلكترونية التي تستهدف البنية التحتية الحيوية	4
4.1	حماية البنية التحتية الحيوية: اعتماد المعايير	6
5.1	اتحديد النطاق في هذا التقرير	7
2	**تنفيذ المعايير: الأعمال التحضيرية الوطنية**	**9**
1.2	ما هي البنية التحتية التي تُعتبر حيوية بالفعل؟	9
2.2	تحديد القطاعات والقطاعات الفرعية ذات الصلة	10
3.2	تجميع قائمة بالأصول الحيوية والاحتفاظ بها	10
4.2	بناء شبكات محلية لحل الأزمات	12
3	**التنفيذ من خلال إشراك المجتمع الدولي**	**13**
1.3	الشفافية ومشاركة المعلومات	13
2.3	نقاط الاتصال الموحدة	14
3.3	(إجراء تمرينات الأمن الإلكتروني الوطنية (الدولية	15
4	**الاستجابة للحوادث الإلكترونية في سياق المعيار**	**17**
1.4	أفضل الممارسات التي توجه الاتصالات الدولية	17
2.4	نهج الاستجابة الشامل الذي يضم أصحاب المصلحة المتعددين	17
3.4	الفرق بين المساعدة والتخفيف	18
5	**الخاتمة**	**21**
	المراجع	**22**

نبذة حول المؤلف

أندراز كاستيليك هو الباحث الرئيسي في مجال الاستقرار الإلكتروني في برنامج الأمن والتكنولوجيا المُمول من معهد الأمم المتحدة لبحوث نزع السلاح. وقد شغل قبل انضمامه للمعهد العديد من المناصب البحثية في المنظمات الدولية والمؤسسات البحثية حول العالم.

نبذة عن معهد الأمم المتحدة لبحوث نزع السلاح

معهد الأمم المتحدة لبحوث نزع السلاح هو معهد مستقل ومُمول من التبرعات داخل الأمم المتحدة, وهو أحد معاهد السياسة القليلة في العالم التي تركز على نزع السلاح, ويعمل على إنتاج المعرفة وتعزيز الحوار والعمل بشأن نزع السلاح والأمن. كما يساعد المعهد, الذي مقره جنيف, المجتمع الدولي على تطوير الأفكار العَملية والمبتكرة الضرورية لإيجاد الحلول للمشاكل الأمنية الحرجة والمهمة.

الاختصارات والتسميات المختصرة

GGE	فريق الخبراء الحكوميين
ICT	تكنولوجيا المعلومات والاتصالات
OEWG	الفريق العامل مفتوح العضوية
UN	الأمم المتحدة
UNIDIR	معهد الأمم المتحدة لبحوث نزع السلاح

الملخص التنفيذي

زعزعة استقرار الدول وتهديد السلم والأمن على المستوى الدولي.

للتصدي لخطر التهديدات الإلكترونية المعقدة والفعالة بشكل متزايد، والتي تستهدف البنية التحتية الحيوية، يستخدم المجتمع الدولي معايير السلوك المتوقع للدول في الفضاء الإلكتروني لتعزيز التعاون. ويبحث هذا التقرير في المعايير –على النحو الذي اقترحه فريق الخبراء الحكوميين (GGE) التابع للأمم المتحدة والمعني بالتطورات. في مجال تكنولوجيا المعلومات والاتصالات (ICT) في سياق الأمن الدولي عام 2015– والذي يحث الدول على الاستجابة لطلبات الدول الأخرى للمساعدة أو التخفيف في حال حدوث أنشطة الجرائم الإلكترونية ضد البنية التحتية الحيوية.[1]

يطرح هذا التقرير الإجراءات والتدابير التالية التي يمكن للدول والمجتمع الدولي اتخاذها لتنفيذ هذه المعايير:

- يتعين على الدول تعريف البنية التحتية الحيوية الوطنية والدولية الخاصة بها بشكل واضح، وتحديد القطاعات التي تُصنَف منتجاتها أو خدماتها على أنّها بُنية تحتية حيوية ومهمة، والاحتفاظ بقائمة الأصول الحيوية. كما يجب مشاركة هذه التعريفات والتعيينات مع المجتمع الدولي كإجراء لبناء الثقة.

- يتعين على الدول بناء شبكات لحل الأزمات تضم الجهات الفاعلة المحلية ذات الصلة.

- يتعين على المجتمع الدولي بناء شبكة من نقاط الاتصال الموحدة بين الجهات الوطنية المؤهلة وتفويض نقاط الاتصال هذه للتواصل مع نظيراتها الدولية.

- يتعين على الدول فحص واختبار قدرتها على الاتصال مع الدول الأخرى بشكل منتظم وكذلك قدرتها على الاستجابة لطلبات المساعدة والتخفيف (وأن تفحص بالتحديد قنوات الاتصال، والبروتوكولات والإجراءات)، عن طريق التمرينات الدولية على الأمن الإلكتروني.

1 UNGA (2015b, III: para. 13(h)).

- ينبغي أن تتبع أفضل الممارسات الحالية المتعلقة بالإبلاغ عن الحوادث في السياقات الوطنية والدولية ذات الصلة.

- يتعين على جميع الدول التي قد تشارك في جهود تعاونية للاستجابة لأنشطة الجرائم الإلكترونية ضد البنية التحتية الحيوية استخدام شبكات حل الأزمات المحلية المنشأة مسبقًا لأصحاب المصلحة المتعددين, وأن تعتمد على خبرة التخفيف المقدمة من الدولة والجهات الفاعلة غير التابعة للدولة في حال حدوث أنشطة إلكترونية من هذا النوع.

- تجدر الملاحظة أنّ التوقعات المعيارية للمساعدة والتخفيف تعتمد على السياق؛ فعندما تحدث أنشطة الجرائم الإلكترونية ضد البنية التحتية الحيوية, يتعين على الدولة التي يصدر عنها النشاط (دولة المصدر بعبارة أخرى) اتخاذ تدابير وإجراءات معقولة إمّا لإنهاء تلك الأنشطة الحاصلة أو للتقليل من انتشار الرموز البرمجية الخبيثة المركزية للأنشطة ذاتها.

- يتعين على أي دولة تتلقى طلبًا للمساعدة أن تبذل قصارى جهدها لتقديم المساعدة بالشكل الذي تطلبه الدولة المتضررة. ولا يقتصر مفهوم المساعدة على الإجراءات المباشرة المتخذة ضد أنشطة الجرائم الإلكترونية, بل يمكن أن يستلزم أي شكل من أشكال المساعدة التي تقلل من التبعات والآثار المترتبة على تلك الأنشطة ضد البنية التحتية الحيوية.

1. فهم السياق والمشكلة

لا تُشكل أنشطة الجرائم الإلكترونية ضد البنية التحتية الحيوية –أي جميع الأصول الضرورية واللازمة للحفاظ على الوظائف الحيوية والمهمة لرفاه مجتمع معين[2]– تهديدًا لرفاه الدولة المستهدفة فحسب، بل للسلم والأمن على المستوى الدولي أيضًا[3]. وتضم القطاعات التي تقع عادةً ضمن تعريفات البنية التحتية الحيوية: قطاع الطاقة، والنقل، والرعاية الصحية، والحكومة، وإنتاج الغذاء وإمداداته، وإمدادات المياه، والخدمات المالية، والاتصالات، والتصنيع الحيوي[4].

وعلى الرغم من أنّ مدى الحوادث الإلكترونية التي تصيب البنية التحتية الحيوية والآثار الدقيقة لها لا يمكن تحديدها بشكل موثوق، إلّا أنّ الحوادث المسجلة تشهد على إمكاناتها المدمرة. ونظرًا إلى المكانة الجوهرية للبنية التحتية الحيوية، فقد يكون للحوادث الإلكترونية عواقب وتأثيرات وخيمة على مجتمعاتنا، بما في ذلك التداعيات الاقتصادية، والأَضرار المادية، وحتى الإصابات البشرية.

ففي عام 2015، اقترح فريق الخبراء الحكوميين (GGE) التابع للأمم المتحدة والمعني بمجال تكنولوجيا المعلومات والاتصالات (ICT) في سياق الأمن الدولي معيارًا دوليًا يهدف إلى تسهيل التعاون الدولي في حال حدوث أنشطة جرائم إلكترونية ضد البنية التحتية. ويهدف هذا التقرير الذي بين أيديكم إلى المساعدة في فهم كيفية تفعيل هذا المعيار، كما أنّه مُنظم وفق البنية التالية:

- يُفصّل الجزء المتبقي من القسم الأول التحديات التي تقترن بحماية البنيةالتحتية من التهديدات الإلكترونية، ويوضح المعيار المذكور أعلاه
- يُعدِّد القسم الثاني الخطوات التحضيرية التي يتعين على الدول النظر في تنفيذها قبل وقوع الحوادث الإلكترونية
- يُقدم القسم الثالث توصيات بشأن الإجراءات التي يتعين تنفيذها على المستوى الدولي
- يقترح القسم الرابع تدابير وإجراءات خاصة بتنفيذ معيار فريق الخبراء الدوليين (GGE) بعد وقوع الحادث الإلكتروني
- يُشير القسم الخامس إلى بعض التساؤلات التي لم تتم معالجتها، ويقترح بعض التوجهات للمناقشات أو البحوث الدولية المستقبلية

1.1 انتشار الحوادث الإلكترونية التي تؤثر على البنية التحتية الحيوية

في الآونة الأخيرة، أعاقت العديد من الحوادث الإلكترونية الكيدية عمل عدد كبير من البنى التحتية الحيوية وشلّت حركتها[5]. إلّا أنّه لا يزال من الصعب التأكد من عددها بشكل دقيق وبالتالي الحكم بأنّها أصبحت أكثر، شيوعًا أو تدميرًا. هذا وتكمن الصعوبة والتحدي في العوامل التالية:

2 لا يوجد تعريف مُتفق عليه دوليًا للبنية التحتية الحيوية. ويعتمد هذا التقرير تعريفًا عمليًا مستوحى من مجلس الاتحاد الأوروبي (2008، الفقرة 2(أ))، بالرغم من تقديم بعض الأمثلة البديلة (انظر البند 2.1).

3 (OEWG (2021, para. 18.

4 تعتمد القطاعات التي تعتبر حيوية على السياق. (انظر البند 2.2).

5 انظر، على سبيل المثال، Steffen (2016) لسلسلة من الأنشطة الإلكترونية ضد المستشفيات الألمانية؛ و Gallagher (2020) للأنشطة الإلكترونية ضد مؤسسات الرعاية الصحية حول العالم؛ ووكالة الأمن الإلكتروني وأمن البنية التحتية الأمريكية (2020) بشأن الأنشطة الإلكترونية التي تتسبب في خسارة الإنتاجية والعائدات في منشأة ضغط الغاز الطبيعي؛ و Statt (2021) بشأن الأنشطة الإلكترونية التي تتدخل في عمل محطة معالجة المياه.

- اختلاف التعريفات بين القطاعات والدول
- النُهج المختلفة المستخدمة لقياس وتيرة وتأثير العمليات والأنشطة الإلكترونية
- درجة عالية من عدم اليقين بشأن العدد الحقيقي والفعلي للعمليات والأنشطة الإلكترونية

يكمن السبب الأول لصعوبة تحديد كمّ وعدد الأنشطة والعمليات الإلكترونية في أنّ مفهوم البنية التحتية ليس مُعرفًا بشكل واضح أو عالمي؛ إذ يعتمد تعريفها بشكل كبير على السياق الوطني. على سبيل المثال، في الوقت الذي تعتمد فيه بعض الدول على قطاع السياحة في جزء كبير من ناتجها المحلي الإجمالي، وقد تُصنِّف بالتالي البنيةَ التحتيةَ التي يعتمد عليها القطاع بأنّها حيوية وبالغة الأهمية[6]، قد لا يكون القطاع نفسه حيويًا ومهمًا بنفس الدرجة للدول الأخرى. لذا، ينبغي قراءة أي إحصائيات حول اتجاهات الحوادث الإلكترونية ضد ما يُعرف بشكل عام على أنّه «بنية تحتية حيوية» بنوع من الحذر.

فضلًا عن ذلك، يُشكل مصطلح البنية التحتية مفهومًا متعدد الأوجه، كما تشهد القطاعات المختلفة اتجاهات مختلفة للحوادث الإلكترونية. وقد يكون من التعميم بمكان القول بأنّ أنشطة الجرائم الإلكترونية التي تستهدف كل قطاع من قطاعات البنية التحتية الحيوية آخذة في التزايد أو النقصان: فهناك حاجة لإجراء تحليل تفصيليٍ ومخصص للقطاع لتقييم تطور مشهد التهديدات بشكل كامل.

أخيرًا، قد تكون العديد من أنشطة الجرائم الإلكترونية التي تؤثر على البنية التحتية غير مُكتشفة، أو لا يتم الإبلاغ عنها. وعليه، فقد يكون عدد الحوادث الإلكترونية التي تُصيب البنية التحتية أعلى مما قد تُشير إليه الإحصائيات والتقارير المتوفرة. ويُشير تقرير شركة «كاسبرسكي لاب» إلى أنّ معظم الحوادث الإلكترونية التي تصيب البنية التحتية لا تزال غير مُعلنة وغير معروفة للجمهور، سواء كان ذلك نتيجة مطالب صريحة من مشغلي البنية التحتية أو بسبب منع مشغلي البنية التحتية من الكشف عن مثل هذه الحوادث من خلال التشريعات المحلية[7]. وعلى نحو مماثل، تؤكد اللجنة الدولية للصليب الأحمر على «صعوبة تقييم عدد العمليات والأنشطة غير اختراقها، أو ما إذا كانت «منافذالمكتشفة، ومدى قدرة المهاجمين على الوصول الفعلي للبنية التحتية و التمرير الخفية» قد تم بناؤها للاستخدامات المستقبلية، مثل زرع «مفاتيح الإيقاف المؤقت» على سبيل المثال».[8]

بالتالي، قد لا يكون من المستغرب أن تعكس البحوث التي أجرتها شركات أمنية مختلفة اتجاهاتٍ مختلفة ومتناقضةً في بعض الأحيان. على سبيل المثال:

- أبلغت شركة «آي بي إم» (IBM) أنّ عدد الحوادث الإلكترونية التي تؤثر على أنظمة التحكم الصناعي وشبكات التكنولوجيا التشغيلية –المستخدمة بشكل متكرر من البنية التحتية الحيوية– كانت أعلى في 2019 بالمقارنة مع السنوات الثلاثة السابقة مجتمعة.[9]

- تُشير الأبحاث التي أجرتها شركة «كاسبرسكي لاب» إلى أنّ نسبة أجهزة الحاسوب المستخدمة في نظام التحكم الصناعي والمستهدفة بالرموز البرمجية الخبيثة قد تراجعت بالفعل في النصف الثاني من 2019 والنصف الأول من 2020. وأنّ هذا الاتجاه لم ينعكس إلا في النصف الثاني من 2020.[10]

---

6 انظر على سبيل المثال جمهورية موريشيوس (2014).
7 مراسلات شخصية مع Evgeny Goncharov رئيس فريق الاستجابة لطوارئ الأنظمة الحاسوبية في شركة «كاسبرسكي لاب»، أكتوبر 2020.
8 Gisel & Olejnik (2019, 25).
9 «منصة «إكس فورس» لخدمات الاستخبارات والاستجابة للحوادث في شركة «آي بي إم» (6, 2020).
10 فريق «كاسبرسكي» للاستجابة لطوارئ الأنظمة الحاسوبية (2020b, 15, 13)،فريق «كاسبرسكي» للاستجابة لطوارئ الأنظمة الحاسوبية (2021).

2.1 الآثار المترتبة على تعطُّل البنية التحتية الحيوية

بغض النظر عن العدد الدقيق للأنشطة والعمليات الإلكترونية للهجوم على البنية التحتية الحيوية, فقد وقع عدد كافٍ من الحوادث الفعلية /التي تُبرر القلق الكبير بشأن المحافظة على أمن البنية التحتية الحيوية التي تُصبح مترابطة بشكل متزايد. ففي أوائل عام 2020, على سبيل المثال, أجبرت أنشطة الجرائم الإلكترونية التي استهدفت مستشفى جامعة برنو في التشيك المنشأةَ على تعليق العمليات الجراحية المجدولة وتحويل المرضى إلى المرافق القريبة[11]. وقبل أربع سنوات, أبلغت شركة توزيع الكهرباء الأوكرانية عن انقطاع الشبكة لعدة ساعات نتيجة لعملية إلكترونية استهدفت أجهزة الحاسوب فيها وأنظمة التحكم الإشرافي وجمع البيانات. مما جعل 225,000 عميل تقريبًا يعانون من انقطاع في التيار الكهربائي.[12]

لا تتسبب جميع الأنشطة والعمليات الإلكترونية التي تقع ضد البنية التحتية الحيوية في انقطاع الخدمات المهمة والحيوية, مع أنّها تُعطي فكرة عن العواقب الوخيمة والمحتملة لذلك. على سبيل المثال, أبلغت السلطات الإسرائيلية في إبريل 2020 عن عمليات إلكترونية ضد أنظمة معالجة المياه في الدولة, والتي حاولت إفساد الممرات المائية الإقليمية[13]. كما تم الإبلاغ عن حادثة مماثلة في أوائل 2021 في محطة لمعالجة المياه في فلوريدا.[14]

وخلال العقد الماضي, انضم عدد متزايد من الحكومات الوطنية للشركات الخاصة[15] والمهنيين المتخصصين في الأمن[16] في اعتبار هذه الأنواع من الحوادث من بين أبرز مشاكل الأمن الإلكتروني. وفي عام 2015, أشارت مجموعة الخبراء الدوليين (GGE) في تقريرها إلى أنّ «مخاطر الهجمات الضارة على [تكنولوجيا المعلومات والاتصالات (ICT) التي تمس البنية التحتية الحيوية حقيقية وخطيرة في نفس الوقت.[17]

وبحكم التعريف, قد يكون لتعطُّل البنية التحتية تبعاتُه وآثارُه واسعة النطاق, كما يمكنه أن يُقوض الوظائف الحيوية التي تعتمد عليها المجتمعات إلى حدٍّ خطير, ومن المحتمل أيضًا أن يتسبب في أضرار مادية وإصابات بشرية أو حتى الموت[18]. على سبيل المثال, يمكن لعملية إلكترونية مُنفذة بشكل جيد ضد العناصر الرئيسية لتوزيع الطاقة, من الناحية النظرية على الأقل, أن تحرم بلدًا بأكمله من الكهرباء[19]. وبالرغم من أنّ التبعات والآثار الفعلية والدقيقة للعملية الإلكترونية المذكورة آنفًا والتي أثّرت على نظام الإمداد بالكهرباء في أوكرانيا ما زالت غير معروفة, إلا أنه تم توثيق التداعيات الاقتصادية التي حدثت عقب حوادث مماثلة سابقة لانقطاع الطاقة على المستوى المحلي[20] والوطني[21] بشكل جيد. كما ثَبَتَ أنّ حالات انقطاع الطاقة تتسبب في زيادة مستويات الوفيات غير العرضية.[22]

قد لا تؤدي العمليات الإلكترونية التي تستهدف البنية التحتية الأخرى بشكل مباشر إلى إلحاق الأذى بالبشر, ولكنها يمكن أن تعيق حركة المجتمع إلى درجة كبيرة. على سبيل المثال, إذا استُخدمت العمليات لاستهداف النظم المالية الوطنية والدولية, فقد يهدد الاستخدام الضار لتكنولوجيا المعلومات والاتصالات (ICT) «الاستقرار المالي»[23], وبالتالي جميع جوانب المجتمع الفعال الذي يعتمد على التدفقات النقدية المستقرة.

---

11 Khalili (2020).
12 Lee et al. (2016).
13 Cimpanu (2020).
14 Statt (2021).
15 Siemens Gas & Power (2019).
16 ENISA (2019, 109); Security Magazine (2020).
17 UNGA (2015b, II: para. 4).
18 أثناء اجتماع الفريق العامل مفتوح العضوية (OEWG) لعام 2020 المعني بالتطورات في مجال المعلومات والاتصالات في سياق اجتماع الأمن الدولي, أكدت الدول أنّ الهجمات على البنية التحتية الحيوية «تشكل تهديدًا ليس فقط للأمن, ولكن أيضًا للتنمية الاقتصادية وسبل العيش, وفي نهاية المطاف لسلامة ورفاهية الأفراد ». (OEWG, 2020, para. 22).
19 Smith et al. (2019).
20 Shuaia et al. (2018).
21 Schmidthaler & Reichl (2016).
22 Anderson & Bell (2012).
23 G-20 (2017, para. 7).

فالعملية الإلكترونية عام 2007 التي استهدفت القطاع المصرفي في إستونيا، ضمن قطاعات أخرى، منعت السكان من استخدام الخدمات المصرفية عبر الإنترنت. وعلى الرغم من أنّ البنية التحتية لشبكة الحاسوب الإستونية لم تتكبد أي ضرر مادي، إلا أن الدولة التي تحدث 97% من المعاملات المصرفية فيها عبر الإنترنت[24] وُصفت بأنها أصيبت بشلل مؤقت».[25]

3.1 تحديات إدارة العمليات الإلكترونية التي تستهدف البنية التحتية الحيوية

قد تتفاقم العواقب والآثار الوخيمة التي تعقب الحوادث الإلكترونية الموجهة للبنية التحتية الحيوية بفعل التهديدات الإلكترونية الناشئة، والتي تنطوي على مجموعة عوامل هي:

- هجمات جديدة ومتزايدة التعقيد[26]. إذ تعمل الجهات الفاعلة الكيدية باستمرار على ابتكار نواقل هجمات جديدة وتطوير عمليات استغلال مقابلها. في الوقت الحاضر، أصبحت البرمجيات الخبيثة التي تستهدف البنية التحتية الحيوية مخصصة على نحو أكثر فعالية للتركيز على الهدف والنيل منه، وأصبحت بالتالي أكثر تعقيدًا

- التوسع السريع في سطح الهجوم[27]. يُعزى هذا في الغالب إلى الترابط المتزايد لأنظمة تكنولوجيا المعلومات (ICT) والاتصالات المستخدمة في أصول البنية التحتية الحيوية. وقد أدّت ترتيبات العمل عن بُعد التي اتُخذتاستجابة لجائحة فيروس كورونا (كوفيد-19) إلى تسريع هذه المشكلة أو .تعقيدها[28]

- الأنظمة التشريعية القديمة التي لا تتمتع بالمرونة الكافية لمواجهة التحديات الجديدة والتي تساهم في زيادة المخاطر الواقعة على البنية التحتية ونقاط الضعف فيها. على سبيل المثال، ووفقًا لتقرير صادر عن الكونغرس الأمريكي، تُعد أنظمة الحاسوب للتحكم الصناعي، والتي هي جزء مكمل وأصيل في البنية التحتية الحيوية، بمثابة «نقاط ضعف محددة، حيث أنّه لم يُنظر إلى الأمن الإلكتروني لهذه الأنظمة سابقًا على أنّه أولوية كبرى».[29]. كما تمخضت تقارير وتقييمات مماثلة على سبيل المثال من شركة مايركوسوفت[30] والمساهمات العلمية[31]

- تخصيص موارد غير كافية لجهود الوقاية[32]. حيث كان من الممكن، على سبيل المثال، منع العملية الإلكترونية عام 2018، والتي استهدفت بشكل كبير قدرة الخدمات الصحية الوطنية في المملكة المتحدة على

24 Herzog (2011, 51).

25 Ilves (2007).

26 أصبح من الصعب جدًا رسم وتحديد مشهد التهديدات، إذ لا يُطور المهاجمون تقنيات وأساليب جديدة لاختراق الأنظمة الأمنية فحسب، بل إنّ التهديدات تزداد من حيث التعقيد والدقة في إصابة الأهداف المرجوة أيضًا" (ENISA, 2020c). كما تُشير شركة "كاسبرسكي لاب" إلى أنّ "التهديدات أصبحت أنجع من حيث الاستهداف والتركيز، وبالتالي أكثر تنوعًا وتعقيدًا " (Kaspersky ICS CERT, 2020b).

27 على سبيل المثال، ووفقًا لـ Bhunia & Tehranipoor (2019, ch.1) "فإنّ سطح الهجوم هو مجموع كل الثغرات أو مخاطر التعرض الأمنية المحتملة". بعبارة أخرى، يمثل سطح الهجوم مجموعة نقاط الوصول المحتملة التي يمكن أن تستغلها الجهات الفاعلة الكيدية خلال التحضير للعملية أو الأنشطة الإلكترونية. انظر أيضًا التنبؤات التي قام بها ENISA (2020c, 10).

28 انظر، على سبيل المثال US CISA (2020b).

29 Shea (2004).

30 "عادة ما تكون شبكات التكنولوجيا التشغيلية المستخدمة في بيئات البنية التحتية الصناعية والحيوية معزولة بشكل تام عن شبكات تكنولوجيا المعلومات" الخاصة بالشركات والإنترنت، إلّا أنّ التحوُّل الرقمي زاد من الترابط والاتصال بين هذه البيئات، فضلًا عن عدد الأجهزة فيها، مما شكل خطرًا أكبر. ومما زاد من إنترنت الأشياء]/بروتوكولات التكنولوجيا التشغيلية والأجهزة المتضمنة في هذه البيئات تم تصميمها منذ سنوات] IoT المخاطر أيضًا أنّ العديد من تشريعات "عديدة – وتفتقر إلى آليات وتقنيات الضبط الحديثة مثل التشفير، ومتطلبات التوثيق المتشددة، وبُنية البرمجيات المحصنة " (Microsoft, 2020, 31).

31 على سبيل المثال، "تفتقر منظمات الرعاية الصحية والجامعات عادة إلى الموارد اللازمة للحماية من الهجمات الإلكترونية"، بحسب ما أشار إليه Muthuppalaniappan & Stevenson (2020).

32 BBC (2017); Maglaras et al. (2018, 42).

توفير الرعاية[33]، لو أنّ المُشغلين قاموا بتخصيص الموارد الكافية وتصحيح (وبالتالي تحصين) أنظمة الحاسوب قبل وقوع الحادثة[34]. ولا يقتصر عدم بذل إجراءات العناية الواجبة على هذه الحادثة فقط، إذ يمكن ملاحظة ذلك أيضًا في الولايات القضائية الأخرى، وقطاعات البنية التحتية الحيوية أيضًا[35]. ووفقًا لشركة مايكروسوفت، تعتمد 71% من أنظمة التحكم الصناعية على إصدارات قديمة من نظام التشغيل ويندوز، والتي لم يعد من الممكن تحديثها بشكل منتظم باستخدام برامج التصحيح الأمني من مايكروسوفت».[36]

عدم القدرة على التنبؤ بالآثار، بما في ذلك مدى الوصول والانتشار أيضًا. الاعتماد المتبادل بين البنى التحتية الحيوية ظاهرةً مُوثقة بشكل جيد، وقد يترتب على الحوادث الإلكترونية عواقب وآثار سلبية غير متوقعة وواسعة النطاق، ويمكن أن تخرج عن إطار الحدود الإقليمية لبلد ما. ,قد يتجلّى أثر مثل هذا الاعتماد المتبادل في فشل عنصر الشبكة الكهربائية في ألمانيا عام 2006، الذي تسبب في انقطاع التيار الكهربائي عن 20 دولة في أوروبا وما خارجها، مما أثر على حوالي 15 مليون أسرة[37]. وبالرغم من أنّ تلك الحادثة لم تنتج عن عملية إلكترونية، إلّا أنّها توضح مدى الانتشار الواسع والمحتمل الذي يمكن أن تُحدثه أنشطة الجرائم الإلكترونية الواقعة على البنية التحتية الحيوية.

33 Ghafur et al. (2019).
34 Morse (2017).
35 انظر أيضًا على سبيل المثال، US DOE (2019).
36 Microsoft (2020, 31).
37 Van der Vleuten & Lagendijk (2010).

4.1 حماية البنية التحتية الحيوية: اعتماد المعايير

تُشير جميع العوامل التي تمت مناقشتها في القسم السابق إلى الحاجة إلى التعاون الدولي لمنع أنشطة الجرائم الإلكترونية التي تستهدف البنية التحتية الحيوية أو التخفيف منها. وتتمحور إحدى النُهج التي اتبعها المجتمع الدولي خلال العقد الماضي لتأمين البنية التحتية الحيوية، ورفع مستوى الأمن الوطني (الدولي)، ومنع الدمار والأذى الذي قد يلحق بالبشر، حول معايير السلوك المسؤول في الفضاء الإلكتروني.[38]

للتقليل من المخاطر والتهديدات التي تستهدف السلم والأمن والاستقرار على المستوى الدولي»[39]، والتقليل» بشكل خاص من تأثير أنشطة الجرائم الإلكترونية التي تستهدف البنية التحتية، اقترحت مجموعة الخبراء الدوليين ثلاثة معايير محددة لسلوك الدولة المسؤول في الفضاء الإلكتروني، وفصّلت التوقعات لسلوك الدولة فيما (GGE) يتعلق بأمن البنية التحتية في العصر الإلكتروني. وتُشير هذه المعايير إلى أنّ الدول ينبغي أن:

- تمتنع عن القيام بالأنشطة والعمليات الإلكترونية التي تستهدف البنية التحتية الحيوية الواقعة تحت سلطة قضائية أجنبية
- تحمي البنية التحتية الحيوية الخاصة بها من أنشطة الجرائم الإلكترونية
- تتعاون على المستوى الدولي في حال حدوث أنشطة جرائم إلكترونية ضد البنية التحتية الحيوية الخاصة بها[40]

معايير أخرى لسلوك الدولة المسؤول في سياق البنية التحتية الحيوية

تتجلى حقيقة أنّ المجتمع الدولي يضع حماية البنية التحتية الحيوية على رأس قائمة مخاوف الأمن الإلكتروني الدولي أيضًا في ظهور معايير مماثلة أو ذات صلة تسعى إليها مختلف الاتحادات وتعززها. على سبيل المثال، تَعهّد الأعضاء في مبادرة نداء باريس من أجل الثقة والأمن في الفضاء الإلكتروني بالعمل معًا، وذلك في المنتديات القائمة ومن خلال المنظمات والمؤسسات والآليات والعمليات ذات الصلة، تعهدوا لمساعدة بعضهم البعض وتنفيذ تدابير تعاونية، ولا سيما للوقاية والتعافي من أنشطة الجرائم الإلكترونية التي تهدد أو تسبب ضررًا جسيمًا أو عشوائيًا أو منهجيًا للأفراد والبنية التحتية الحيوية[41]. ستساعد هذه المعايير في سد الفجوة الرقمية، وتجسيد المثال الجيد لمعنى الجيرة الحسنة، وزيادة فعالية الاستجابة للحوادث[42]، والمساهمة بشكل عام في استقرار وأمن العالم المترابط. يكون ذلك صحيحًا بشكل خاص إذا كان العنصر الحيوي للبنية التحتية يتجاوز حدود الدولة الواحدة، كما هو الحال في البنية التحتية الحيوية الدولية أو فوق الوطنية[43]، مثل النواة العامة للإنترنت.[44]

---

38 كما تؤدي أيضًا الحلول التكنولوجية والقانون الدولي وبناء القدرة وتدابير بناء الثقة وغيرها دورًا مهمًا، بالرغم من أنّ البحث في ذلك يقع خارج نطاق هذا التقرير. انظر على سبيل المثال، UNGA (2015b, V); Gusev (2020, 314); Baker et al. (2020, 503).

39 UNGA (2015b, para. 10).

40 UNGA (2015b, para. 12(f)–(h)).

41 وزارة الشؤون الخارجية والأوروبية، فرنسا (2018).

42 NIST (2012, 45).

43 OEWG (2020, 17).

44 الحكومة الهولندية (2017; 2020, 2).

5.1 تحديد النطاق في هذا التقرير

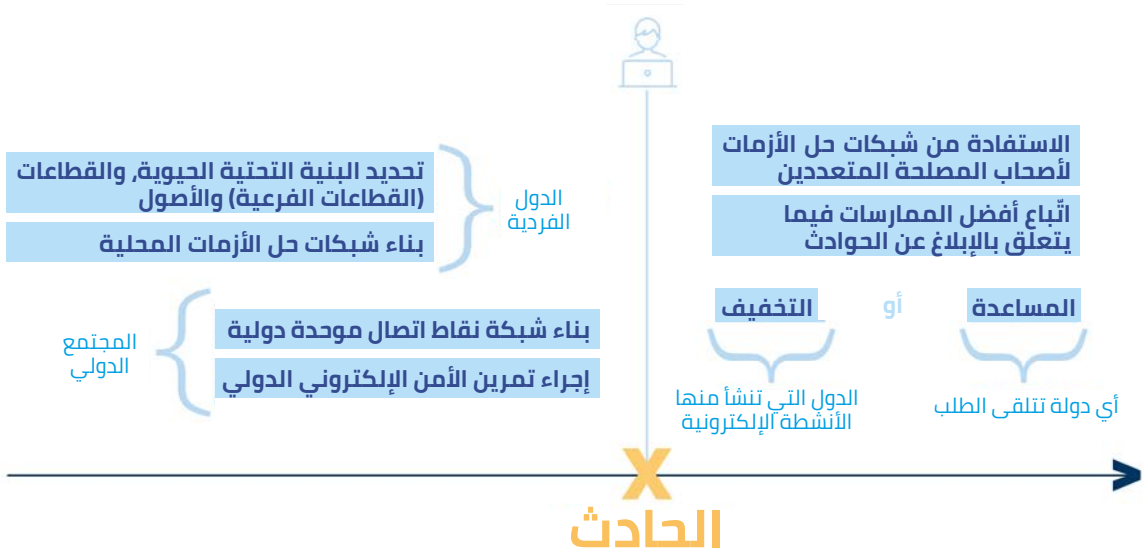
في حين أنّ المعايير الثلاثة الواردة في تقرير فريق الخبراء الحكوميين (GGE), والموصوفة أعلاه, معايير مترابطة ويعزز بعضها بعضًا, إلّا أنّ **هذا التقرير يركز على جانب المساعدة الدولية**, وبشكل أكثر تحديدًا على كيفية إعداد الدول بشكل أفضل لطلب تلك المساعدة أو الاستجابة لها عند الضرورة.

وبالرغم من وجود ثروة من الأبحاث حول حماية البنية التحتية الحيوية[45], إلّا أنّه لم يتم تسجيل متطلبات المساعدة والتخفيف الدولية في سياق حماية البنية التحتية الحيوية, لا سيما في سياق معيار مجموعة الخبراء الدوليين (GGE) ذي الصلة. وبينما ينصب تركيز هذا المعيار على الاستجابة لأنشطة الجرائم الإلكترونية التي تستخدم مكوِّنات (ICT) تكنولوجيا المعلومات والاتصالات للمساس بالبنية التحتية الحيوية, إلّا أنّ تنفيذ تلك المعايير يعتمد على سلسلة من الإجراءات والأنشطة على المستوى الوطني والإقليمي والدولي, والمتخذة قبل وبعد وقوع الحادث. وقد تم تلخيص تلك الإجراءات, التي ستُناقش بشكل تفصيلي خلال هذا التقرير, في الشكل 1.

ترتبط الكثير من الإجراءات والأنشطة التي تمت مناقشتها في هذا التقرير بتحسين القدرة الوطنية لمنع أنشطة الجرائم الإلكترونية ضد البنية التحتية الحيوية, أو التخفيف من حدتها والاستجابة لها, أو التعافي منها. غير أنّ التركيز في هذا التقرير يظل منصبًا على طرائق التعاون الدولي, مع أنّ التدابير المُوضحة لا تغطي جميع العوامل التي تجب مراعاتها في السياق الأوسع لتطوير القدرات الإلكترونية, كما لا يناقش التقرير التدابير الوقائية التي يمكن للدول أن تتخذها لتفادي وقوع الحوادث الإلكترونية في المقام الأول.

الشكل 1:

الإجراءات المقترحة في هذا التقرير لضمان تفعيل معيار فريق الخبراء الحكوميين (GGE) الذي تم تحليله



45 انظر على سبيل المثال, ENISA (2020a).

2. تنفيذ المعايير: الأعمال التحضيرية الوطنية

يتطلب تفعيل معيار فريق الخبراء الحكوميين (GGE) تطويرَ أطر هيكلية وطنية تمكينية بشكل مسبق وقبل أي حدوث محتمل لأنشطة الجرائم الإلكترونية، لضمان مستوى كاف من الجاهزية والاستعداد. وعلى هذا النحو، **يتعين على الدول أن تعتمد تعريفًا عامًا وموحدًا للبنية التحتية الوطنية الحيوية، وتحدد القطاعات (القطاعات الفرعية) المؤهلة، وتُجَمِّع قائمة بالأصول ذات الصلة؛ ويتعين عليهم أيضًا بناء شبكات حل الأزمات المحلية.**

هذا ويمكن للدول التي تحتاج إلى توجيه في عملية تعريف البنية التحتية الوطنية الحيوية والقطاعات والأصول الاستفادة من برامج المساعدة المتعددة[46]، بالإضافة إلى الوثائق الإرشادية[47]، ومجموعات الممارسات الوطنية الجيدة[48] التي جمعتها المنظمات الدولية.

1.2 ما هي البنية التحتية التي تعتبر حيوية بالفعل؟

يقع تحديد نطاق البنية التحتية ضمن الحقوق السيادية لكل دولة. وهذا لا يتماشى مع مبدأ السيادة في القانون الدولي فحسب، بل تم تأكيده أيضًا صراحةً في قرار مجلس الأمن التابع للأمم المتحدة رقم 2341، الذي أكد أنّ «كل دولة تحدد ما يشكل بنيتها التحتية الحيوية».[49]

بالرغم من ذلك، قد تُصنّف البنية التحتية على أنّها حيوية على أساس الغرض منها، أو على أساس تعطُّل الأصول أو الخدمات التي تتيحها البنية التحتية، أو على أساس مزيج من المبدأين[50]. هذا وقد تم طرح عدة محاولات إقليمية لتحديد نطاق البنية التحتية الحيوية والتي يمكنها تقديم المشورة للدول في هذا الصدد. على سبيل المثال، تُعرّف اتفاقية التعاون لضمان أمن المعلومات الدولي بين الدول الأعضاء في منظمة شنغهاي للتعاون البنية التحتية الحيوية بأنّها تشمل «مرافق وأنظمة ومؤسسات الدولة، التي قد يكون للتأثير عليها عواقب يمكنها المساس بالأمن الوطني بشكل مباشر، بما في ذلك أمن الأفراد والمجتمع والدولة»[51]. وتُقدم أطر دولية وإقليمية أخرى تعريفات عامة مماثلة لهذا المفهوم، مثل إعلان منظمة الدول الأمريكية بشأن حماية البنية التحتية الحيوية من التهديدات الناشئة[52] واتفاقية الاتحاد الأفريقي بشأن الأمن الإلكتروني وحماية البيانات الشخصية.[53]

46 انظر على سبيل المثال، CICTE (2015, para. 9).
47 OECD (2008b); Suter (2007).
48 UNCTED & UNOCT (2018).
49 UNSC (2017, 2)، تم اعتماد الحقوق الوطنية من قبل بعض الأطر الإقليمية مثل الاتحاد الإفريقي. انظر أيضًا على سبيل المثال ITU (2010)، (2014, art. 24).
50 UNCTED & UNOCT (2018, 58).
51 منظمة شنغهاي للتعاون (2009, 10).
52 CICTE (2015, para. 11).
53 الاتحاد الإفريقي (2014, art. 1).

2.2 تحديد القطاعات والقطاعات الفرعية ذات الصلة

يتعين على الدول، بعد اعتماد التعريف، أن تقوم بتحديد القطاعات المُؤهلة (وربما القطاعات الفرعية) التي ستُعتبر بنيةً تحتيةً وطنيةً حيويةً. وفي حين أنّ تعريفات البنية التحتية ستتسم بشيء من التوافق والاتساق على الأرجح، إلّا أنّ قوائم القطاعات التي تُصنف على أنّها بنية تحتية حيوية ستكون مختلفة بلا شك .

في كثير من الأحيان تكون القطاعات التي تُصنَّف على أنّها حيوية هي القطاعات التي يُحتَمل أن يُسبب تعطُّلها الضرر البشري والضرر المادي على نطاق واسع، بالإضافة إلى عدم الاستقرار الاقتصادي والاجتماعي. وفي هذا السياق، يُحتمل اعتبار قطاعات مثل الطاقة، والتمويل، وإمدادات المياه والغذاء، والنقل، وتكنولوجيا المعلومات (ICT)، والاتصالات والحكومة، على أنّها قطاعات حيوية في معظم الدول[54]. غير أنّه يمكن تصنيف قطاعات أخرى مثل السياحة على أنّها حيوية فقط لدى مجموعة مختارة من الدول التي يعتمد اقتصادها بشكل كبير على تلك القطاعات.[55]

3.2 تجميع قائمة بالأصول الحيوية والاحتفاظ بها

يتعين على الدول تجميع قائمة بالأصول الحيوية الوطنية والاحتفاظ بها. ويجب أن تتضمن هذه القائمة الجهات أو الأصول المحددة التي تُمَكِن قطاعات (قطاعات فرعية) حيوية تم تحديدها مسبقًا من القيام بوظيفتها. ومع مراعاة الطبيعة الحساسة لمثل تلك القائمة نظرًا لتأثيرها المحتمل على الأمن الوطني المحلي، يجب على الدول أن تضمن التواصل بشكل سليم ومناسب، فضلًا عن مشاركة المعلومات مع الجهات ذات الصلة، بما في ذلك مالكو الأصول أو مديروها. كما ينبغي تنظيم القائمة في مجموعات مختلفة من حيث الأولوية بناءً على الثغرات الموجودة في الأصول، وعلى مدى التأثير الذي سيُحدثه تَعطُّل أحد تلك الأصول. يمكن أيضًا أن تتضمن القائمة الأصولَ المُصنفة على أنّها بنية تحتية حيوية دولية، وتقع خارج الولاية القضائية لدولة معينة، إلّا أنّها تعتبر حيوية بسبب الوظيفة التي تؤديها لمجتمع تلك الدولة. هذا ويتحتم على الدول مراجعة قوائم الأصول الحيوية الخاصة بها بانتظام، إلى جانب مجموعات الأولوية، لتبقى دائمًا على علم بالظروف الوطنية المتغيرة، وبمشهد التهديدات الناشئة كذلك.[56]

الشكل 2:

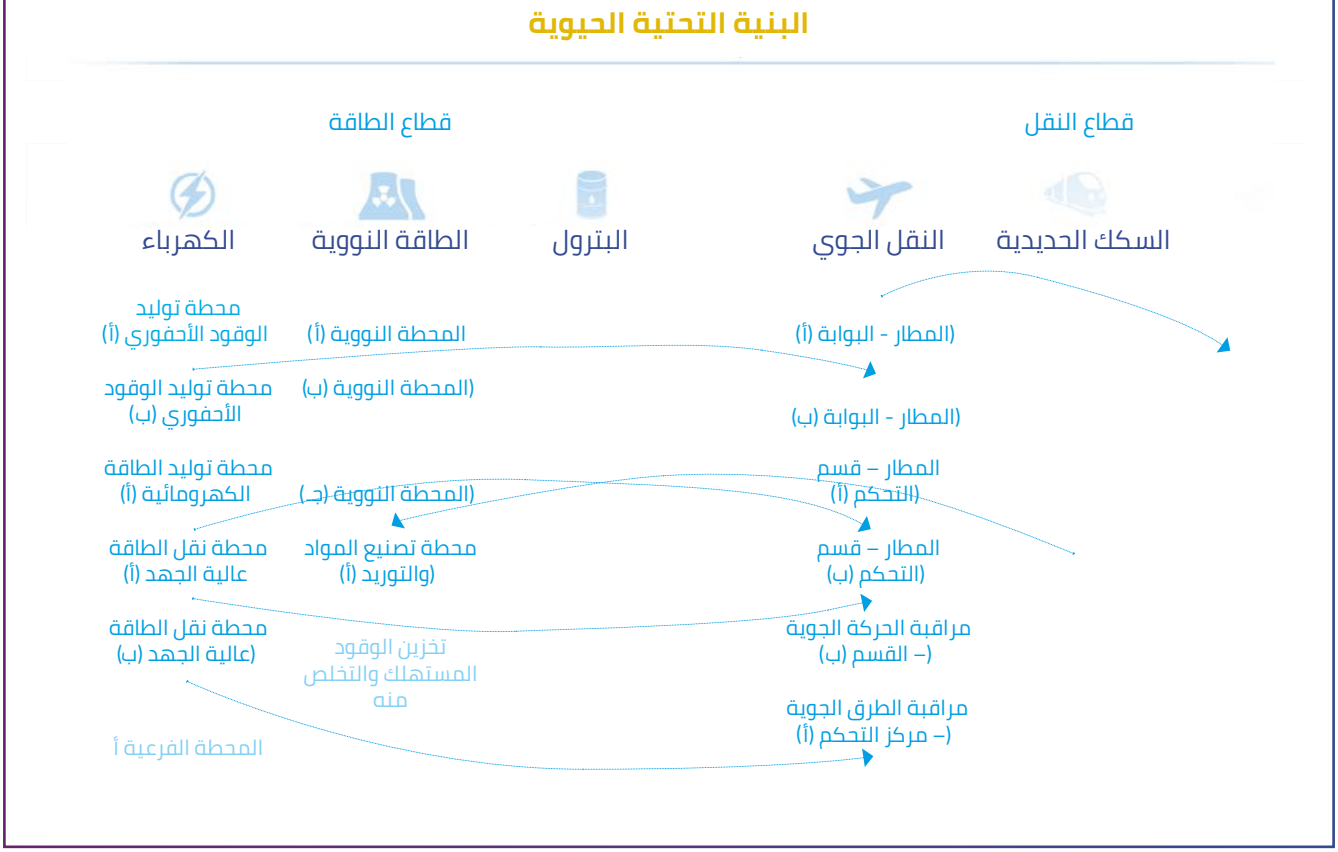
الهيكل النظري للبنية التحتية الحيوية الوطنية (القطاعات، القطاعات الفرعية، الأصول) وإظهار مدى الاعتماد المتبادل

54 انظر على سبيل المثال المكتب الفيدرالي للحماية المدنية، سويسرا (2020).
55 انظر على سبيل المثال جمهورية موريشيوس ((2014, 11).
56 المركز العالمي للقدرات الأمنية الإلكترونية (2016).

وقد يكون هناك ترابط بين بعض الأصول، فإذا عطّلت عملية إلكترونية على سبيل المثال محطة معينة لنقل الطاقة عالية الجهد، فمن المحتمل أن تتأثر الأصول التي تنتمي إلى قطاع مختلف بدرجة بالغة، وربما تتعطل، في حالة عدم وجود محطات نقل احتياطية مناسبة.

الشكل 3:

هيكل نموذجي للبنية التحتية الحيوية الوطنية،
يوضح القطاعات والأصول والترابط بينها



إن طبيعة التقدُّم الأصيلة وما يترتب عليها من انخفاض أسعار التكنولوجيا، بالإضافة إلى عمليات الرقمنة السريعة والتي ساهمت جائحة فيروس كورونا (كوفيد–19) في تسريعها أيضًا، كل ذلك يؤدي إلى الزيادةَ الحاصلةَ في عدد الأصول الحيوية، مما يُوسع نطاق البنية التحتية الحيوية أيضًا. إلّا أنّه لا ينبغي للدول أن تنساق وراء الرغبة في توسيع مفهوم البنية الحيوية التحتية الوطنية الحيوية إلى أكثر من حدوده اللازمة: فكلما زاد نطاق البنية التحتية الحيوية المُعرفة، كلما زاد حجم الاستثمار الاستراتيجي المترتب على الحكومة بشكل عام، وكذلك على مُشغلي تلك البنية، بغرض حمايتها[57]. ولهذا السبب، يتعين على الدول تقييد مفهوم البنية التحتية الحيوية بالأصول والقطاعات التي تُعتبر حيوية بالفعل لرفاه المجتمع.

57 لا يتناول هذا التقرير تفعيل المعيار الذي يقترح أن تستثمر الدول في حماية بنيتها التحتية الحيوية. إلّا أنّه توجد العديد من المحاولات للإشارة إلى حماية البنية التحتية الحيوية. انظر، على سبيل المثال وزارة الداخلية الاتحادية، ألمانيا (2008a). ;OECD (2009).

4.2 بناء شبكات محلية لحل الأزماتالفرعية ذات الصلة

بالإضافة إلى تحديد مفهوم البنية التحتية الحيوية, يتعين على **الدول النظر في إنشاء شبكات حل الأزمات لأصحاب المصلحة المتعددين بحيث تضم الجهات الفاعلة المحلية ذات الصلة**. هذا ويجب أن تكون هذه الشبكات شموليةً بطبيعتها, وأن تُشرك بشكل فعال كلًا من جهات الدولة وممثلي القطاع الخاص, وأن تضم -بين جهات أخرى- مُشغلي البنية التحتية الحيوية, وفريق الاستجابة للطوارئ الحاسوبية, وغيرهم من الجهات الفاعلة المؤهلة المستعدة والقادرة على المساهمة في تقديم الحلول الناجحة للحوادث الإلكترونية التي تمس البنية التحتية الحيوية الوطنية أو الخارجية. كما أنّ هذا النوع من الشبكات يمكنه المساهمة أيضًا في جهود الوقاية من تلك الحوادث.

وإلى جانب قنوات الاتصال القائمة, فإنّ البروتوكولات والإجراءات المحلية الدقيقة والموثقة التي تسمح بالتدفق السريع للمعلومات من مُشغلي البنية التحتية الحيوية أو السلطة الوطنية المؤهلة (مثل فريق الاستجابة للطوارئ الحاسوبية) إلى نقطة الاتصال الوطنية, كلاهما ضروري للمساعدة في إرسال طلب فعال للحصول على المساعدة أو التخفيف الدولي. هذا ويجب أن يكون أصحاب المصلحة المحليون على دراية بالبروتوكولات والعمليات المتفق عليها, كما هو الحال لدى الجهات التعاونية في الساحة الدولية.[58]

58 صدرت نفس الاقتراحات من UNCTED & UNOCT (2018, 58).

3. التنفيذ من خلال إشراك المجتمع الدولي

إضافة إلى الجهود الداخلية لبناء شبكات محلية لحل الأزمات, يُمكن أن تكون الإجراءات التالية مفيدة لكفاءة وفعالية التعاون الدولي وحسن توقيته في الاستجابة لأنشطة الجرائم الإلكترونية التي تستخدم مُكونات تكنولوجيا المعلومات والاتصالات للمساس بالبنية التحتية الحيوية, على المستويين الإقليمي والدولي:

- زيادة الشفافية وتبادل المعلومات حول موضوع البنية التحتية الحيوية, بما في ذلك التعريفات والنطاق
- بناء قنوات مخصصة للاتصال بين نقاط التواصل المحددة بشكل واضح
- تطوير البروتوكولات والإجراءات لدعم تدفق المعلومات عبر قنوات الاتصال الوطنية والدولية,
- إجراء تمرينات إقليمية ودولية منتظمة لفحص واختبار الإداء الصحيح لشبكات نقاط الاتصال والبروتوكولات والإجراءات

1.3 الشفافية ومشاركة المعلومات

يتعين على الدول ممارسة الشفافية وتعزيز التبادل المنتظم للمعلومات ذات الصلة بالمفاهيم الوطنية للبنية التحتية الحيوية. ولتحقيق هذه الغاية, حثّ فريق الخبراء الحكوميين (GGE) لعام 2015 الدولَ للمشاركة في «تقديم الدول طوعيًا لآرائها الوطنية حول فئات البنية التحتية التي تعتبرها حيوية, بالإضافة إلى الجهود الوطنية لحمايتها, بما في ذلك المعلومات المتعلقة بالقوانين والسياسات الوطنية لحماية البنية التحتية القائمة على البيانات وتكنولوجيا المعلومات والاتصالات (ICT)».[59] ويُعد تبادل المعلومات أحد عوامل التمكين الرئيسية للتعاون الدولي والمساعدة والتخفيف في سياق تعطُّل البنية التحتية الحيوية نتيجة أنشطة الجرائم الإلكترونية, إذ لا يدعم ذلك الدول في الإبلاغ بشكل أفضل عن احتياجاتها في أوقات الأزمات فحسب, بل يهيئ الفرصة أيضًا لإجراء تقييم أفضل للاستجابة اللازمة والمطلوبة من الدول التي تتلقى طلبات المساعدة (أو التخفيف).

تتوفر العديد من المستودعات الإقليمية والدولية لتسهيل تبادل المعلومات هذا, وأحد هذه المشاريع هو بوابة السياسة الإلكترونية لمعهد الأمم المتحدة لبحوث نزع السلاح[60], وهو مستودع رقمي يحتوي على مجموعة سياسات الأمن الإلكتروني الوطنية لجميع الدول الأعضاء في مجلس الأمن, بالإضافة إلى أطر عمل المنظمات الحكومية الدولية الإقليمية أو متعددة الأطراف. ومن الأمثلة الأخرى على ذلك, مستودع استراتيجيات الأمن الإلكتروني الوطني الذي يتعهده الاتحاد الدولي للاتصالات.[61]

59 UNGA (2015b, para. IV(d)).
60 www.cyberpolicyportal.org.
61 ITU (2020).

2.3 نقاط الاتصال الموحدة

والسريع للمعلومات في حال تعطُّل البنية التحتية الحيوية لأحد الأعضاء. هذا ويتعين على المجتمع الدولي السعي إلى إنشاء شبكة عالمية من نقاط الاتصال الموحدة بين الجهات الوطنية المؤهلة، والمُفوضة بالتواصل مع نظيراتها الدولية عندما يستدعي الوضع ذلك[62]. وأحد الأمثلة على تلك الشبكات هي قائمة نقاط الاتصال الموحدة التي طورها قسم توجيه أمن الشبكة والمعلومات في الأمم المتحدة[63]، والتي يتم تحديثها بانتظام، وهي متاحه مجانًا عبر الإنترنت.[64]

وقد أوصى تقرير فريق الخبراء الحكوميين (CGE) في 2015 بأن تنظر الدول في إنشاء دليل لنقاط الاتصال الموحدة «على المستويين التكنولوجي والسياسي»[65]. وخلال النقاش الذي أجراه الفريق العامل مفتوح العضوية (OEWG) حول التطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي في فبراير 2020، أيدت عدة وفود وضع قائمة نقاط اتصال عالمية، إلّا أنّها لم تتخذ موقفًا موحدًا حول طبيعة وأهلية الجهات المتضمنة في هذا الدليل. وقد أيدت بعض الوفود[66] تحديد نقاط اتصال سياسية؛ بينما فضلت أخرى وضع قائمة بنقاط اتصال متعددة تمثل جهات الاستجابة للطوارئ الحاسوبية، وجهات إنفاذ القانون، وغيرهم من أصحاب المصلحة ذوي الصلة[67]. هذا وتضمن التقرير الموضوعي النهائي للفريق العامل مفتوح العضوية (OEWG) توصيات بأن تُنشئ الدول الأعضاء دليلًا عالميًا بنقاط الاتصال.[68]

يمكن أن تتخذ المساعدة والتخفيف العديد من الأشكال الأخرى غير الفنية[69]، إلّا أنّه للتقليل من مخاطر الارتباك وعدم اليقين في أوقات الأزمات، يُقترح أن تشمل أي قائمة مستقبلية لنقاط الاتصال الجهاتِ الوطنية المعتمدة رسميًا فقط، التي تمتلك المعرفة الفنية والتشغيلية الكافية لطلب أو تسهيل المساعدة والتخفيف الدوليين.

62 وقائع حوار أصحاب المصلحة المتعددين حول تفعيل المعايير الإلكترونية: حماية البنية التحتية الحيوية، 3 يوليو 2020 [في ملف لدى المؤلف]. تم تطوير الفكرة أيضًا في تقرير فريق الخبراء الحكوميين (GGE) لعام 2015: انظر UNGA (2015b, IV (a)).

63 EU (2016, art. 8).

64 EC (2020) انظر أيضًا G-7 (2019); OSCE Permanent Council (2013, art. 8). على الرغم من أنّ الاتفاقية المتعلقة بالجرائم الإلكترونية في سياق مختلف وأضيق، تتطلب من الدول تعيين نقاط اتصال وطنية لتسهيل مكافحة الجرائم الإلكترونية. انظر أيضًا CoE (2004, art. 35).

65 UNGA (2015b, para. 16(a)).

66 الأرجنتين وأستراليا والبرازيل وكندا وتشيلي وكولومبيا وإكوادور وإستونيا وفرنسا وغانا وملاوي وماليزيا والمكسيك ونيوزيلندا والاتحاد الروسي وسلوفينيا وسويسرا والجمهورية العربية السورية (2020) Gavrilović.

67 Gavrilović (2020).

68 OEWG (2021, para. 51).

69 انظر البند 4.3.

3.3 إجراء تمرينات الأمن الإلكتروني الوطنية (والدولية)

يكون التعاون الدولي الناجح مشروطًا بتوفُّر الشبكات الوظيفية لحل الأزمات، بالإضافة إلى البروتوكولات وقنوات الاتصال الفعالة. لذا، يُقترح أن تُجري الدول بانتظام **تمرينات الأمن الإلكتروني الوطنية والدولية** التي ستختبر وتفحص قدراتها على التواصل، أو الاستجابة لطلبات المساعدة أو التخفيف.

ستعمل تمرينات الأمن الإلكتروني الوطنية على تقييم وتعزيز جاهزية واستعداد الشبكات المحلية لحل الأزمات، وقدرتها على نقل وترحيل طلبات المساعدة والتخفيف المناسبة إلى الدول الأخرى، كما أنّها ستعزز القدرة على مساعدة دولة أخرى في حال مساس أنشطة الجرائم الإلكترونية ببنيتها المحلية الحيوية[70].

وتساعد تمرينات الأمن الإلكتروني الدولية أيضًا في بناء قدرة الدول على توصيل طلب المساعدة أو التخفيف بشكل فعال، لكّنها تساعد على وجه التحديد في تعزيز قنوات الاتصال بين نقاط الاتصال، فضلًا عن البروتوكولات والإجراءات الدولية المستخدمة. عطفًا على كل ذلك، تسهل تمرينات الأمن الإلكتروني الدولية بناء الثقة بين الدول. على سبيل المثال، يساعد الاتحاد الدولي للاتصالات بشكل منتظم الدول في إجراء تمرينات الأمن الإلكتروني الإقليمية[71].

70 على سبيل المثال، تدعم OAS (2021) و OSCE (2018) الدولَ في إجراء تمارين الأمن الإلكتروني الوطنية.
71 ITU (2021).


NEW YORK
SYDNEY

4. الاستجابة للحوادث الإلكترونية في سياق المعيار

لا يتضمن معيار فريق الخبراء الحكوميين (GGE) الذي يدعو إلى التعاون الدولي في محاولة لوقف أنشطة الجرائم الإلكترونية ضد البنية التحتية الحيوية بصيغته الحالية أي توقعات ببذل العناية الواجبة أو يُشير إلى الحاجة لتواصل المجتمع الدولي بشكل استباقي مع الدولة المتضررة. وبحسب نص المعيار، تتحمل الدولة التي تم استهداف بنيتها التحتية الحيوية من خلال الأنشطة والعمليات الإلكترونية مسؤولية إصدار طلب مناسب للمساعدة أو التخفيف.

في هذا السياق، ولضمان تفعيل المعيار، يجب تحديد ماهية الطلبات التي تُعتبر «طلبات معتمدة للمساعدة [أو التخفيف] من قبل دولة أخرى تخضع بنيتها التحتية الحيوية لأنشطة الجرائم الإلكترونية التي تستخدم مُكونات تكنولوجيا المعلومات والاتصالات (ICT)».[72]

1.4 أفضل الممارسات التي توجِه الاتصالات الدولية

لا بد أن تتبَع نقاط الاتصال في تفاعلاتها البروتوكولاتِ والعملياتِ المعترف بها بشكل عام. ونظرًا للتحديات والصعوبات التي تتشكل لدى إنشاء وتطوير بروتوكولات وعمليات عالمية للاتصال، **يتعين على الدول أن تتبع أفضل الممارسات القائمة والمتعلقة بالإبلاغ عن الحوادث في السياقات الدولية والوطنية**، الأمر الذي يُهيئ الفُرص للتواصل الأمثل بين الأطراف المعنية وبالتالي يُسهل التعامل الفعال مع الحادث.

ويُعد كل من دليل الممارسات الجيدة للإبلاغ عن الحوادث الصادر عن وكالة الاتحاد الأوروبي للأمن الإلكتروني[73]، والمبادئ الإرشادية الفيدرالية للإبلاغ عن الحوادث والصادرة عن فريق الاستعداد للطوارئ الحاسوبية في الولايات المتحدة الأمريكية[74]، مثالًا على أطر الإبلاغ عن الحوادث التي يمكن استخدامها لهذا الغرض. هذا وتشمل الأمثلة على البروتوكولات الفنية التي يمكن استخدامها في هذا الصدد سياسة تبادل المعلومات 2.0، وبروتوكول إشارات المرور، وكلاهما تم نشره من قبل منتدى الاستجابة للحوادث وفِرق الأمن[75].

إضافة إلى كل ما سبق، يجب ألّا يتضمن الطلب المعتمد للمساعدة أو التخفيف المعلومات حول الحادثة فحسب، بل ينبغي أن يشمل أيضًا الإجراءات المحددة المقترحة التي يلزم اتخاذها من قبل الدولة التي يُوجَّه إليها الطلب.

2.4 نهج الاستجابة الشامل الذي يضم أصحاب المصلحة المتعددين

يتعين على جميع الدول المشاركة في العملية التعاونية للتصدي لأنشطة الجرائم الإلكترونية ضد البنية التحتية الحيوية أن تستخدم الشبكات **المحلية لحل الأزمات المذكورة سابقًا والتي تضم أصحاب المصلحة المتعددين، وأن تعتمد على خبرات التخفيف المتوفرة لدى الدولة والجهات الفاعلة غير التابعة للدولة ذات الصلة**؛ إذ يمتلك القطاع الخاص ثروة هائلة من الخبرة في مجال الأمن الإلكتروني، وغالبًا ما يتحكم في تقنيات البنية التحتية الحيوية ذات الصلة. وعليه، من المرجح أن تحقق أي محاولات لحل الأزمات.

72 UNGA (2015b, III: para. 13 (h)).
73 ENISA (2009).
74 US-CERT (2015).
75 FIRST (2019).

دون إشراك القطاع الخاص نتائج دون المستوى[76]. نعيد ونكرر مرة أخرى أنّه من المهم أن تستثمر الدول في بناء الشبكات التعاونية وشبكات حل الأزمات الوطنية، إلى جانب قنوات الاتصال المُحددة بدقة ووضوح، والأدوار والمسؤوليات الواضحة لأعضاء الشبكة.

3.4 الفرق بين المساعدة والتخفيف

وفقًا لما ينص عليه المعيار قيد الدراسة والنقاش، يتعين على الدول الاستجابة لـ«الطلبات المعتمدة للمساعدة» أو «الطلبات المعتمدة للتخفيف من أنشطة الجرائم الإلكترونية التي تستخدم مُكونات تكنولوجيا المعلومات والاتصالات (ICT) لاستهداف البنية التحتية الحيوية لدولة آخرى»[77]. ولا يُتوقع من الدول التي تتلقى طلبات المساعدة أو التخفيف أن تتصرف بأكثر من إمكانياتها؛ بل يُتوقع منها ببساطة أن تبذل قصارى جهدها للمساعدة ضمن الموارد المتوفرة في ذلك الوقت. لكن ما هو الفرق بين المساعدة والتخفيف؟

أولًا، عندما يتعذر تحديد مصدر العملية الإلكترونية أو عندما تصدر من البنية التحتية لدولة غير تلك التي تلقّت الطلب، **تُوصى الدولة التي طُلبت منها المساعدة بتقديم أي مساعدة أو دعم ممكن لتخفيف أي تبعات أو آثار تترتب على أنشطة الجرائم الإلكترونية الواقعة ضد البنية التحتية الحيوية. يمكن أيضًا للدول تقديم المساعدة بإنهاء العملية الإلكترونية أو تقوية وتعزيز أنظمة شبكة الحاسوب للبنية التحتية** الحيوية المتضررة؛ إذ يمكن تقديم المساعدة بأشكال مختلفة ولا تقتصر فقط على المساعدة التقنية. فإذا أعاقت العملية الإلكترونية إنتاج الكهرباء في دولة معينة على سبيل المثال، يمكن لهذه الدولة أن تطلب المساعدة على شكل إمدادات إضافية من الكهرباء. فعندما يتم طلب المساعدة، يُتوقع من الدولة المتأثرة بالعملية الإلكترونية تحديد الاحتياجات أو الطلب، بما في ذلك مدى المساعدة والأدوات المستخدمة في ذلك. ومن المهم أن تتواصل الدول المتفاعلة والمتعاونة في هذا الصدد، وأن تتصرف بحسن نية، وضمن حدود مبدأ حق السيادة الذي ينص عليه القانون الدولي وما ينتج عنه من التزامات.

ثانيًا، إذا تم تسليم الطلب للدولة التي يُعتقد أن أنشطة الجرائم الإلكترونية صادرة عنها (دولة المصدر)، يتعين على الدول الاستجابة عن طريق تخفيف العملية الإلكترونية ذاتها. يبدو أنّ التخفيف مفهوم أضيق بالمقارنة مع المساعدة، ويُشير إلى تقييد العملية الإلكترونية ضد البنية التحتية الحيوية أو الحد منها. على هذا النحو، يقتصر التخفيف إلى حد كبير على الإجراءات التي تكون تقنية بطبيعتها، والمتعلقة بالعملية الإلكترونية ذاتها. وفي هذا السياق، **يُتوقع من دوُل المصدر أن تتخذ إجراءات وتدابير معقولة لإيقاف أو التقليل من انتشار الرموز البرمجية الخبيثة المتضمنة**. وعلى الرغم من أنّ التخفيف يتسم بنطاق أضيق من المساعدة، إلّا أنّه يُشير إلى أهمية الدور الذي تؤديه دُول المصدر في الحد من انتشار العملية الإلكترونية والدمار الناتج عنها. ويجدر بالذكر أن التخفيف والمساعدة لا يستبعد أي منهما الآخر؛ إذ يمكن للدولة التي يُطلب منها تخفيف العملية الإلكترونية الناشئة من أراضيها أن تُقدم المساعدة أيضًا

مع كل ذلك، لا ينظر المعيار في الدور المنوط بدول العبور التي قد تكون البنية التحتية فيها حلقة تمكين مهمة لسلسلة العمليات أو الأنشطة الإلكترونية الكيدية، والتي من المحتمل.

76 انظر على سبيل المثال، ITU et al. (2018, 44).
77 UNGA (2015b, para. 13(h)).
78 ICJ (1997, para. 80).

أن تكون في وضع يُمكنها من التخفيف من العملية الإلكترونية ضد البنية التحتية الحيوية لدولة أُخرى. هذا ويمكن للمجتمع الدولي أن يُجري مزيدًا من التحليلات لدور دول العبور بينما يُواصل الدفع قُدمًا بالمناقشات حول معايير سلوك الدولة المسؤول في المنتديات متعددة الجوانب.

ثالثًا, لا ينبغي أن تتركز جهود المساعدة والتخفيف حول مسألة الإسناد الفني؛ ففي إطار الاستجابة الفورية للعمليات الإلكترونية التي تحدث ضد البنية التحتية الحيوية, يجب أن تُنفّذ أنشطة وإجراءات الكشف عن المجرمين ومقاضاتهم إلى الدرجة التي تحد من الضرر الناجم عن العملية الإلكترونية. ولا يعني هذا أن تتجاهل الجهات التي تشترك في هذه الاستجابة التعاونية أي دليل رقمي يتم اكتشافه خلال مرحلة محاولة حل الحادث؛ إذ أنّ مثل ذلك الدليل قد يكون مفيدًا في مرحلة لاحقة, ويُمَكِّنها من اتخاذ الإجراءات والتدابير التي تتوافق مع القانون الجنائي المحلي أو القانون الدولي المتعلق بمسؤولية الدولة. وعلى الرغم من ذلك, لا ينبغي بأي حال من الأحوال أن يتمحور الجهد الرئيسي للأطراف المتعاونة حول الإسناد الفني للمشكلة فحسب, إذ أنّه قد يحيدهم عن الهدف الأساسي للتعاون – وهو وقف انتشار العملية الإلكترونية وتقليل عواقبها غير المرغوب فيها.

الخاتمة

للمعايير المتعلقة بسلوك الدولة المسؤول في الفضاء الإلكتروني. ففي عام 2015, اعتمدت الجمعية العامة للأمم المتحدة مجموعة من المعايير التي طورها فريق الخبراء الحكوميين (GGE) والتي تُعزز -ضمن أمور أخرى- التعاون بين الدول في حال حدوث عمليات إلكترونية تخريبية ضد البنية التحتية الحيوية, وتنص على أنّ الدول يجب أن تستجيب لطلبات المساعدة المعتمدة أو طلبات التخفيف المعتمدة في بعض الأحيان, التي تُرسل من قبل دولة أخرى تتعرض البنية التحتية الحيوية فيها لأنشطة الجرائم الإلكترونية التي تستخدم مُكونات تكنولوجيا المعلومات والاتصالات (ICT) للمساس بها.

ولتيسير تنفيذ تلك المعايير ودعم الدول في ذلك, حدد هذا التقرير بالتفصيل نطاق المعيار ومضمونه, موضحًا التوقعات المعيارية, وممارسات الدول, والممارسات الجيدة الناشئة المتعلقة المعيار. ويُشير التقرير على وجه التحديد, إلى ما يتعين على الدول القيام به, وهو:

- تعريف البنية التحتية الحيوية, بما في ذلك القطاعات (والقطاعات الفرعية) بالإضافة إلى قاعدة بيانات بالأصول المؤهلة
- بناء وتأسيس آليات محلية لحل الأزمات بحيث تضم أصحاب المصلحة المتعددين
- مشاركة وتبادل المعلومات حول مفهوم البنية التحتية الحيوية مع المجتمع الدولي
- السعي إلى بناء وتأسيس شبكة عالمية من نقاط الاتصال الموحدة
- إجراء تمرينات الأمن الإلكتروني الوطنية (والدولية) بشكل منتظم
- .اتّباع أفضل الممارسات في التواصل عند تقديم طلب المساعدة أو التخفيف أو الاستجابة له
- بذل ما في وسعها لتقديم المساعدة للدولة المتضررة بأي شكل من الأشكال اللازمة, وإذا تم تحديدها بأنّها دولة المصدر لأنشطة الجرائم الإلكترونية, يتعين عليها أن تبذل ما في وسعها للتخفيف من العملية ذاتها

إلّا أنّه ومع كل ذلك, لا تزال هناك العديد من جوانب المعيار التي تحتاج إلى المزيد من التفصيل من قِبل المجتمع الدولي؛ ولذلك ينبغي للدول أن تستمر في شرح وجهات نظرها وآرائها حول تفعيل المعايير أو تقديم مستويات فهم إضافية عبر مشاركة أفضل الممارسات والتجارب المتعلقة بتطبيق المعيار.

إضافة إلى ذلك, يتعين على المجتمع الدولي النظر في استكشاف دور دول العبور, إلى جانب التفكير في تنفيذ الأطر المعيارية الحالية, مع إيلاء اهتمام خاص لإمكانية مساهمة دُول العبور في جهود التخفيف في حال حدوث عمليات إلكترونية ضد البنية التحتية الحيوية.

يتعين أيضًا على المجتمع الدولي النظر في وضع وصياغة مفهوم البنية التحتية الحيوية الدولية أو عبر الوطنية, وتحديد التوقعات من مختلف الدول بشأن التخفيف من أنشطة الجرائم الإلكترونية التي تستهدف مثل تلك البُنى التحتية.

أخيرًا, ينبغي للمجتمع الدولي النظر في كيفية الاستفادة من جهود بناء القدرات الحالية والمستقبلية[79] من أجل تعزيز القدرات الوطنية للدول الفردية, وتمكينها من حماية البنية التحتية الحيوية لديها, بالإضافة إلى التخفيف من أنشطة الجرائم الإلكترونية التي تستهدف البنية التحتية الحيوية لدولة أخرى, أو مساعدة الدول التي تحتاج إلى ذلك.

---

79 UNGA (2015b, para. 23).

المراجع

الاتحاد الإفريقي, 2014. (اتفاقية الأمن الإلكتروني وحماية البيانات الشخصية)

African Union. 2014. Convention on Cyber Security and Personal Data Protection. 27 June.

(إطفاء الأضواء: تأثير انقطاع التيار الكهربائي في 2003 على معدل الوفيات في نيويورك)

Anderson, Brooke G., & Michelle L. Bell. 2012. 'Lights Out: Impact of the August 2003 Power Outage on Mortality in New York, NY.' *Epidemiology* 193–189 :(2) 23. As of 24 October 2020: https://journals.lww.com/epidem/Fulltext/03000/2012/ Lights_Out Impact_of_the_August_2003_Power.3.aspx

(تطوُّر التعاون)

Axelrod, Robert. 1984. *The Evolution of Cooperation*. New York: Basic Books.

منصة آمنة قائمة على الحوسبة الضبابية لبُنية إنترنت الأشياء التحتية الحيوية القائمة على «نظام التحكم الإشرافي وتحصيل البيانات (سكادا)»)

Baker, Thar, Muhammad Asim, Áine MacDermott, Farkhund Iqbal, Faouzi Kamoun, Babar Shah, Omar Alfandi & Mohammad Hammoudeh. 2020. 'A Secure Fog 'Based Platform for SCADA. Based IoT Critical Infrastructure.' *Special Issue: Software Tools and Techniques for Fog and Edge Computing* 50 (5): 503. As of 21 October 2020: https://onlinelibrary.wiley.com/doi/ abs/10.1002/spe.2688

(كان من الممكن لنظام الرعاية الصحية الوطني «أن يمنع» هجمة WannaCry Ransomware)

BBC. 2017. 'NHS "Could Have Prevented" WannaCry Ransomware Attack.' *BBC News*, 27 October. As of 25 October 2020: https://www.bbc.com/news/technology41753022

(أمن الأجهزة: نهج التعلم العَملي)

Bhunia, Swarup, & Mark Tehranipoor. 2019. *Hardware Security: A Hands-on Learning Approach*. Cambridge: Elsevier.

(نظريات الامتثال للقانون الدولي)

Burgstaller, Markus. 2005. *Theories of Compliance with International Law*. Leiden: Brill Academic.

(ضرب هجومان إلكترونيان آخران شبكة المياه الإسرائيلية)

Cimpanu, Catalin. 2020. 'Two More Cyber-Attacks Hit Israel's Water System.' ZDNet, 20 July. As of 21 October 2020: https://www.zdnet.com/article/two-more-cyber-attacks-hit-israels-water-system

المجلس الأوروبي. 2004. (اتفاقية الجرائم الإلكترونية)

Council of Europe (CoE). 2004. Convention on Cybercrime, ETS 185.

مجلس الاتحاد الأوروبي. 2008. (توجيه المجلس EC 114/2008 / الصادر في 8 ديسمبر 2008 بشأن تحديد وتعيين البنى التحتية الحيوية الأوروبية وتقييم الحاجة إلى تحسين حمايتها)

Council of the European Union. 2008. *Council Directive 114/2008/EC of 8 December 2008 on the identification and designation of European Critical infrastructures and the assessment of the need to improve their protection.*

2017. (دليل تبادل المعلومات لإنفاذ القانون)

——— . 2017. *The Manual on Law Enforcement Information Exchange*. 4 ,17/6261 July. As of 6 March 2021: https://data.consilium.europa.eu/doc/document/ST-2017-6261-INIT/en/pdf

(السمعة, والامتثال, والقانون الدولي)

Downs, George W., & Michael A. Jones. 2002. 'Reputation, Compliance, and International Law.' *Journal of Legal Studies* 31 (S1): S96.

معهد أديسون للكهرباء. 2018. (يعد الأمن الإلكتروني لنظام توزيع الكهرباء مسألة بالغة الأهمية في المجتمع المترابط اليوم)

Edison Electric Institute. 2018. 'Electric Distribution System Cybersecurity Is Critical in Today's Interconnected Society.' April. As of 25 October 2020: https://www.eei.org/issuesandpolicy/Documents/EEI_Cybersecurity_Considerations_Distribution.pdf

المفوضية الأوروبية. 2020. (قائمة بنظام نقاط الاتصال الموحدة والسلطات المؤهلة – قسم توجيه أمن الشبكة والمعلومات)

European Commission (EC). 2020. 'List of SPOCS & Competent authorities – NIS Directive.' As of 21 October 2020: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53682

الاتحاد الأوروبي. 2016. (توجيه (الاتحاد الأوروبي) 1148/2016 الصادر عن البرلمان الأوروبي والمجلس بتاريخ 6 يوليو 2016 بشأن التدابير الخاصة بمستوى عالٍ من أمن الشبكات وأنظمة المعلومات عبر الاتحاد)

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

الوكالة الأوروبية للأمن الإلكتروني. 2009. (الممارسات الجيدة للإبلاغ عن الحوادث الأمنية)

European Union Agency for Cybersecurity (ENISA). 2009. 'Good Practices on Reporting Security Incidents.' December. As of 21 December 2020: https://www.enisa.europa.eu/publications/ good-practice-guide-on-incident-reporting1-/at_download/fullReport

2019. (تقرير وكالة الاتحاد الأوروبي للأمن الإلكتروني حول مشهد التهديدات في 2018)

——— . 2019. *ENISA Threat Landscape Report 2018*. Athens: ENISA. As of 21 October 2020: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report2018

2020أ. (البنى التحتية الحيوية والخدمات)

——— . 2020a. 'Critical Infrastructures and Services.' As of 21 October 2020: https://www. enisa.europa.eu/topics/critical-information-infrastructures-and-services?tab=publications

2020ب. (الاستعراض السنوي: مشهد التهديدات من وكالة الاتحاد الأوروبي للأمن الإلكتروني).

——— . 2020b. *Sectoral/Thematic Threat Analysis: ENISA Threat Landscape*. Athens: ENISA. As of 21 October 2020: https://www.enisa.europa.eu/publications/ sectoral-thematic-threat-analysis

2020 ج. (الاستعراض السنوي: مشهد التهديدات من وكالة الاتحاد الأوروبي للأمن الإلكتروني).

——— . 2020c. The Year in Review: *ENISA Threat Landscape*. Athens: ENISA. As of 24 October: https://www.enisa.europa.eu/publications/year-in-review/at_download/fullReport

وزارة الداخلية الاتحادية, ألمانيا, 2009. (الاستراتيجية الوطنية لحماية البنية التحتية الحيوية)

Federal Ministry of the Interior, Germany. 2009. *National Strategy for Critical Infrastructure Protection (CIP Strategy)*. Berlin: Government of Germany. As of 25 October: https://www.bmi. bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis_englisch.html

المكتب الاتحادي للحماية المدنية, سويسرا. 2020. (البُنى التحتية الحيوية)

Federal Office for Civil Protection, Switzerland. 2020. 'Critical Infrastructures.' As of 21 October 2020: https://www.babs.admin.ch/en/aufgabenbabs/ski/kritisch.html

(منتدى الاستجابة للحوادث والفرق الأمنية. 2019. (تعريف إطار سياسة تبادل المعلومات 2.0)

Forum of Incident Response and Security Teams (FIRST). 2019. 'Information Exchange Policy 2.0 Framework Definition.' As of 21 October 2020: https://www.first.org/iep/ iep_framework_2_0

2020 بروتوكول إشارة المرور: تعريفات معايير منتدى الاستجابة للحوادث وفِرق الأمن وإرشادات الاستخدام – الإصدار 1.0)

———. 2020. 'Traffic Light Protocol (TLP): FIRST Standards Definitions and Usage Guidance– Version 1.0.' As of 21 October 2020: https://www.first.org/tlp

مجموعة العشرين, 2017. (اجتماع وزراء مالية ومحافظي البنوك المركزية لمجموعة العشرين)

G-20. 2017. 'Communiqué – G20 Finance Ministers and Central Bank Governors Meeting.' Baden-Baden, Germany, 17–18 March 2017.

(تجميع مبادرة المعايير الإلكترونية للدروس المستفادة وأفضل الممارسات)

G-7. 2019. 'Cyber Norm Initiative Synthesis of Lessons Learned and Best Practices.' 26 August. As of 21 October 2020: https://www.diplomatie.gouv.fr/IMG/pdf/_eng_synthesis_ cyber_norm_initiative_cle44136e.pdf

(قراصنة» بلا ضمير» يطالبون بفدية من عشرات المستشفيات والمختبرات العاملة في مجال فيروس كورونا)

Gallagher, Ryan. 2020. 'Hackers "Without Conscience" Demand Ransom from Dozens of Hos- pitals and Labs Working on Coronavirus.' *Fortune*, 1 April. As of 21 October: https://fortune. com/01/04/2020/hackers-ransomware-hospitals-labs-coronavirus

(تدابير بناء الثقة)

Gavrilović, Andrijana. 2020. 'Confidence-Building Measures.' Geneva Internet Platform, February 2020. As of 21 October 2020: https://dig.watch/sessions/confidence-building-measures

(التحليل بأثر رجعي لهجمة WannaCry على نظام الرعاية الصحي الوطني)

Ghafur, Saira S. Kristensen, K. Honeyford, G. Martin, A. Darzi & P. Aylin. 2019. 'A Retrospective Impact Analysis of the WannaCry Cyberattack on the NHS.' *NPJ Digital Medicine*

(التكلفة البشرية المحتملة المترتبة على العمليات والأنشطة الإلكترونية)

Gisel, Laurent, & Lukasz Olejnik. 2019. *The Potential Human Cost of Cyber Operations*.

(جنيف: اللجنة الدولية للصليب الأحمر)

Geneva: International Committee of the Red Cross. As of 21 October 2020: https://www.icrc. org/en/download/file/97346/the-potential-human-cost-of-cyber-operations.pdf

اللجنة الدولية للاستقرار في الفضاء الإلكتروني. 2019. (تعزيز الاستقرار الإلكتروني). التقرير النهائي. نوفمبر.

Global Commission on the Stability of Cyberspace. 2019. *Advancing Cyberstability*. Final Report, November. As of 21 October 2020: https://cyberstability.org/wp-content/ uploads/02/2020/GCSC-Advancing-Cyberstability.pdf

المركز العالمي للإمكانيات في مجال الأمن الإلكتروني . 2016. (نموذج نضج قدرات الأمن الإلكتروني للدول) – الإصدار المنقح)

Global Cyber Security Capacity Centre. 2016. *Cybersecurity Capacity Maturity Model for Nations (CMM)* – Revised Edition. Oxford: University of Oxford. As of 21 October 2020: https:// gcscc.ox.ac.uk/files/cmmrevisededition090220171pdf

الحكومة الأسترالية, 2019. (التنفيذ الأسترالي لمعايير سلوك الدولة المسؤول في الفضاء الإلكتروني)

Government of Australia. 2019. 'Australian Implementation of Norms of Responsible State Behaviour in Cyberspace.' As of 21 October 2020: https://www.dfat.gov.au/sites/default/files/how-australia-implements-the-ungge-norms.pdf

(الحكومة الكندية, 2019. (تنفيذ كندا لمعايير فريق الخبراء الحكوميين 2015)

Government of Canada. 2019. 'Canada's Implementation of the 2015 GGE Norms.' As of 21 October 2020: https://unoda-web.s3.amazonaws.com/wp-content/uploads/11/2019/canada- implementation-2015-gge-norms-nov-16-en.pdf

الحكومة الهولندية, 2017. (بناء الجسور الرقمية: الاستراتيجية الإلكترونية (السيبرانية) الدولية). 2 فبراير .

Government of the Netherlands. 2017. 'Building Digital Bridges: International Cyber Strategy.' 2 February. As of 21 October 2020: https://www.government.nl/documents/ parliamentary-documents/12/02/2017/international-cyber-strategy

2020. (ورقة موقف هولندا حول الفريق العامل مفتوح العضوية (OEWG) التابع للأمم المتحدة حول «التطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي»، وفريق الخبراء الحكوميين (GGE) التابع للأمم المتحدة بشأن «تعزيز سلوك الدولة المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي)»

———. 2020. 'The Netherlands' Position Paper on the UN Open-ended Working Group "on Developments in the Field of Information and Telecommunications in the Context of International Security" and the UN Group of Governmental Experts "on Advancing responsible State behavior in cyberspace in the context of international security."' February. As of 21 October 2020: https://unoda-web.s3.amazonaws.com/wp-content/uploads/02/2020/letter-to-chair-of-oewg-kingdom-of-the-netherlands.pdf

(نواقل الهجمات الإلكترونية الجديدة للبنية التحتية الحيوية للشركات الروسية: نظرة على القطاع المصرفي الخاص المحلي في إطار طرق حماية الذكاء الاصطناعي)

Gusev, Alexey. 2020. 'New Cyberattacks Vectors of Russian Critical Infrastructure Enterprises: Domestic Private Banking Sector View within AI Protection Methods.' *Procedia Computer Science* 314 :169. As of 21 October 2020: https://www.sciencedirect.com/science/article/pii/S1877050920303124

(نظرية الامتثال للقانون الدولي)

Guzman, Andrew T. 2002. 'A Compliance Based Theory of International Law.' *California Law Review* 1823 :(6)90. As of 21 October 2020: https://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=1216&context=gjicl

(إعادة النظر في الهجمات الإلكترونية الإستونية: التهديدات الرقمية والاستجابات متعددة الجنسيات)

Herzog, Stephen. 2011. 'Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses.' *Journal of Strategic Security* 49 :(2)4.

منصة «إكس فورس» لخدمات الاستخبارات والاستجابة للحوادث في شركة «آي بي إم» 2020. (تقرير Threat Intelligence Index لعام 2000). فبراير.

IBM X-Force Incident Response and Intelligence Services. 2020. 'X-Force Threat Intelligence Index 2020'. February. As of 21 October 2020: https://www.ibm.com/security/digital-assets/xforce-threat-intelligence-index-map

(خطاب رئيس جمهورية إستونيا, توماس هندريك إلفيس, أمام الدورة الثانية والستين للجمعية العامة للأمم المتحدة 25 أيلول/سبتمبر 2007))

Ilves, Toomas Hendrik. 2007. 'Address by Toomas Hendrik Ilves President of the Republic of Estonia to the 62nd Session of the United Nations General Assembly (25 September 2007)'. As of 17 January 2021: https://www.un.org/webcast/ga/2007/62/pdfs/estonia-eng.pdf

(لجنة البلدان الأمريكية لمكافحة الإرهاب. 2015. (إعلان: حماية البنية التحتية الحيوية من التهديدات الناشئة)

Inter-American Committee Against Terrorism (CICTE). 2015. *Declaration: Protection of Critical Infrastructure from Emerging Threats*. CICTE document CICTE/doc.23 ,15/1 March 2015. As of 21 October 2020: https://www.sites.oas.org/cyber/Documents/CICTE20%DOC20%201%DECLARATION20%CICTE00955E04.pdf

(محكمة العدل الدولية. 1997. (مشروع Gabčíkovo-Nagymaros (المجر/سلوفاكيا)

International Court of Justice (ICJ). 1997. *Gabčíkovo-Nagymaros Project (Hungary/Slovakia), Judgment, ICJ Reports 1997*, p. 7.

الاتحاد الدولي للاتصالات. 2010. (السؤال 22–2: تأمين شبكات المعلومات والاتصالات: أفضل الممارسات لتطوير ثقافة الأمن الإلكتروني (التقرير النهائي))

International Telecommunication Union (ITU). 2010. *Question 1-22: Securing Information and Communication Networks: Best Practices for Developing a Culture of Cybersecurity* (Final Report). Geneva: ITU. As of 25 October 2020: https://www.itu.int/pub/D-STG-SG2010-01.22

2020. (مستودع استراتيجيات الأمن الإلكتروني الوطني)

———. 2020. 'National Cybersecurity Strategies Repository.' As of 17 December 2020: https:// www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx

2021. (التمرينات الإلكترونية)

———. 2021. 'CyberDrills.' As of 11 February 2021: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx

الاتحاد الدولي للاتصالات, البنك الدولي, أمانة الكومنولث, منظمة الكومنولث للاتصالات, المركز التعاوني للدفاع السيبراني التابع لمنظمة حلف شمال الأطلسي. 2018. (دليل تطوير استراتيجية الأمن الإلكتروني الوطني – المشاركة الاستراتيجية في الأمن الإلكتروني). جنيف: الاتحاد الدولي للاتصالات.

ITU, The World Bank, Commonwealth Secretariat, the Commonwealth Telecommunications Organisation, NATO Cooperative Cyber Defence Centre of Excellence. 2018. *Guide to Developing a National Cybersecurity Strategy – Strategic Engagement in Cybersecurity*. Geneva: ITU

الإنتربول. 2020. (منع الجريمة وحماية الشرطة: تقييم الإنتربول للتهديد العالمي لجائحة فيروس كورونا (كوفيد–19)) 6 إبريل.

INTERPOL. 2020. 'Preventing Crime and Protecting Police: INTERPOL's COVID19- Global Threat Assessment.' April 6. As of 21 October 2020: https://www.interpol.int/en/News-and-Events/News/2020Preventing-crime-and-protecting-police-INTERPOL's-COVID-19-global-threat-assessment

فريق «كاسبرسكي» للاستجابة لطوارئ الأنظمة الحاسوبية. 2020أ. (التهديدات الإلكترونية لأنظمة التحكم الصناعي بالطاقة في أوروبا. الربع الأول من عام 2020)

Kaspersky ICS CERT. 2020a. 'Cyberthreats for ICS in Energy in Europe. Q2020 1.' As of 21 October 2020: https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT2020-Q-1Threats- to-energy-industry-in-Europe.pdf

2020ب. (مشهد التهديدات لأنظمة الأتمتة الصناعية في النصف الأول من عام 2020)

———. 2020b. 'Threat landscape for industrial automation systems H2020 1'. September 24. As of 21 October 2020: https://ics-cert.kaspersky.com/media/ KASPERSKY_H2020_1_ICS_REPORT_EN.pdf

2021. (مشهد التهديدات لأنظمة الأتمتة الصناعية. الإحصائيات للنصف الأول من عام 2020) 25 مارس.

———. 2021. 'Threat landscape for industrial automation systems. Statis- tics for H2020 2'. March 25. As of 28 March 2021: https://securelist.com/threat-landscape-for-industrial-automation-systems-statistics-for-h10129/2020-2

(مشهد التهديدات لأنظمة التحكم الصناعية المستخدمة في صناعة إدارة المياه)

———. Forthcoming. 'Threat Landscape for ICS in Water Management Industry.'

(مستشفى فيروس كورونا يُعلق نشاطه على إثر الهجمات الإلكترونية)

Khalili, Joel. 2020. 'Coronavirus Hospital Suspends Activity over Cyberattack.' *Techradar.Pro*, 16 March. As of 21 October 2020: https://www.techradar.com/news/ coronavirus-hospital-suspends-activity-over-cyberattack

(مُلخص الرئيس: اجتماع استشاري غير رسمي لفريق الخبراء الحكوميين (GGE) حول تعزيز سلوك الدولة المسؤول في الفضاء الإلكتروني في سياق الأمن الدولي)

Lauber, Jurg. 2019. 'Chair's Summary: Informal Consultative Meeting of the Group of Governmental Experts (GGE) on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security.' 6–5 December. As of 21 October 2020: https://www.un.org/ disarmament/wp-content/uploads/12/2019/gge-chair-summary-informal-consultative-meet- ing-6-5-dec20191-.pdf

(تحليل الهجمة الإلكترونية على شبكة الطاقة الأوكرانية)

Lee, Robert M., Michael J. Assante & Tim Conway. 2016. 'Analysis of the Cyber Attack on the Ukrainian Power Grid.' SANS & E-ISAC, 18 March. As of 21 October 2020: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

(الأمن الإلكتروني للبُنى التحتية الحيوية)

Maglaras, Leandros A., Ki-Hyung Kim, Helge Janicke, Mohamed Amine Ferrag, Stylianos Rallis, Pavlina Fragkou, Athanasios Maglaras & Tiago J. Cruz. 2018. 'Cyber Security of Critical Infrastructures.' *ICT Express* 4: 42–45.

ميكروسوفت. 2020. (تقرير الدفاع الإلكتروني لمايكروسوفت)

Microsoft. 2020. 'Microsoft Digital Defense Report' September. As of 21 October 2020: https://www.microsoft.com/en-us/download/details.aspx?id=101738

وزارة الشؤون الخارجية والأوروبية, فرنسا. 2018. (نداء باريس من أجل الثقة والأمن في الفضاء الإلكتروني). 11 ديسمبر.

Ministry of Europe and Foreign Affairs, France. 2018. 'Paris Call for Trust & Security in Cyberspace.' 11 December. As of 21 October 2020: https://pariscall.international/assets/files/paris-call.pdf

(التحقيق: الهجمة الإلكترونية WannaCry ونظام الرعاية الصحي الوطني)

Morse, Amyas. 2017. *Investigation: WannaCry Cyber Attack and the NHS*. London: National Audit Office. As of 21 October 2020: https://www.nao.org.uk/report/ investigation-wannacry-cyber-attack-and-the-nhs

(الهجمات الإلكترونية على نظام الرعاية الصحي وجائحة فيروس كورونا (كوفيد–19): تهديد عاجل للصحة العالمية)

Muthuppalaniappan, Menaka, & Kerrie Stevenson. 2020. 'Healthcare Cyber-Attacks and the COVID-19 Pandemic: An Urgent Threat to Global Health.' *International Journal for Quality in Health Care* 33 (1). As of 25 October 2020: https://academic.oup.com/intqhc/article/33/1/mzaa117/5912483

(بيان من فاسيلي نيبينزيا, الممثل الدائم للاتحاد الروسي لدى الأمم المتحدة, في اجتماع «غير رسمي» عبر الفيديو لأعضاء مجلس الأمن التابع للأمم المتحدة حول الهجمات الإلكترونية ضد البنية التحتية الحيوية

Nebenzia, Vassily. 2020. 'Statement by Vassily Nebenzia, Permanent Representative of the Russian Federation to the United Nations, at the "Arria-formula" VTC of the UNSC Members on Cyber-Attacks against Critical Infrastructure.' Permanent Mission of the Russian Feder- ation to the United Nations, 26 August. As of 21 October 2020: https://russiaun.ru/en/news/ arria_260820

الفريق العامل مفتوح العضوية حول التطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي. 2020. (المسودة الثانية لتقرير الفريق العامل مفتوح العضوية (OEWG) حول التطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي). 27 مايو .

Open-ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security. 2020. 'Second "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security.' 27 May. As of 21 October 2020: https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-revised-pre-draft.pdf

2021. (التقرير الموضوعي النهائي). 10 مارس 2021, وثيقة للأمم المتحدة.

———. 2021. 'Final Substantive Report.' 10 March 2021, UN Document A/AC.290/2021/ CRP.2. As of 12 March 2021: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

منظمة التعاون والتنمية الاقتصادية. 2008أ. (حماية «البنية التحتية الحيوية» ودور سياسات الاستثمار المتعلقة بالأمن القومي)

Organisation for Economic Co-operation and Development (OECD). 2008a. 'Protection of "Critical Infrastructure" and the Role of Investment Policies Relating to National Security.' May. As of 21 October 2020: https://www.oecd.org/daf/inv/investment-policy/40700392.pdf

2008ب. توصيات منظمة التعاون الاقتصادي والتنمية الصادرة عن المجلس بشأن حماية البنى التحتية الحيوية للمعلومات)

———. 2008b. *OECD Recommendation of the Council on the Protection of Critical Information Infrastructures*. OECD Document C(2008)35. Paris: OECD. As of 21 October 2020: http://www. oecd.org/sti/40825404.pdf

المجلس الدائم لمنظمة الأمن والتعاون في أوروبا. (القرار رقم 1106: مجموعة أولية من تدابير بناء الثقة لمنظمة الأمن والتعاون في أوروبا لتقليل مخاطر الصراع الناشئة عن استخدام تكنولوجيا المعلومات والاتصالات)

Organization for Security and Co-operation in Europe (OSCE) Permanent Council. 2013. 'Decision No. 1106: Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies.' OSCE Document PC.DEC/1106, 3 December 2013.

2018. (تعقد منظمة الأمن والتعاون في أوروبا جلسات نقاشية تدريبية في كازاخستان حول حماية البنية التحتية الحيوية للطاقة من الهجمات الإرهابية الإلكترونية)

———. 2018. 'OSCE Holds National Table Top Exercise in Kazakhstan on Protecting Critical Energy Infrastructure from Cyber-Related Terrorist Attacks.' 29 November. As of 10 February 2021: https://www.osce.org/programme-office-in-astana/404594

منظمة الولايات الأمريكية. 2021. (برنامج الأمن الإلكتروني). اعتبارًا من 10 فبراير 2021:

Organization of American States (OAS). 2021. 'Cybersecurity Program.' As of 10 February 2021: http://www.oas.org/en/sms/cicte/prog-cybersecurity.asp

البعثة الدائمة لجمهورية إندونيسيا في الأمم المتحدة, نيويورك. 2020. (بيان من سعادة الدكتور السفير ديان تريانسياه دجاني الممثل الدائم لجمهورية إندونيسيا: في الاجتماع غير الرسمي لمجلس الأمن التابع للأمم المتحدة حول «الاستقرار الإلكتروني, ومنع النزاعات, وبناء القدرات). نيويورك, 22 مايو. اعتبارًا من 21 أكتوبر 2020)

Permanent Mission of the Republic of Indonesia to the United Nations, New York. 2020. 'Statement by H.E. Ambassador Dian Triansyah Djani Permanent Representative of the Republic of Indonesia: United Nations Security Council Arria-formula Meeting "Cyber Stability, Conflict Prevention, and Capacity Building."' New York, 22 May. As of 21 October 2020: https://kemlu.go.id/newyork-un/en/read/united-nations-security-council-arria-formula-meeting-cyber-stability-conflict-prevention-and-capacity-building/3645/ etc-menu

مجلس الرئيس الاستشاري حول البنية التحتية الوطنية, 2017. (أصول الأمن الإلكتروني: معالجة التهديدات الإلكترونية العاجلة التي تمس البنية التحتية الحيوية). أغسطس. اعتبارًا من 21 أكتوبر 2020:

President's National Infrastructure Advisory Council (NIAC). 2017. 'Security Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure.' August. As of 21 October 2020: https://www.cisa.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf

جمهورية موريشيوس 2014. (استراتيجية الأمن الإلكتروني الوطني 2014–2019) اعتبارًا من 21 أكتوبر 2020.

Republic of Mauritius. 2014. 'National Cyber Security Strategy 2014 – 2019.' As of 21 October 2020: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Mauritius_2014_National%20Cyber%20Security%20Strategy%20-%202014%20-%20 EN.pdf

(تقييم الآثار الاجتماعية والاقتصادية لانقطاع التيار الكهربائي الناتج عن هجمات مخصصة لهذا الغرض)

Schmidthaler, Michael, & Johannes Reichl. 2016. 'Assessing the Socio-Economic Effects of Power Outages Ad Hoc.' *Computer Science – Research and Development* 31: 157–61. As of 21 October 2020: https://link.springer.com/article/10.1007/s00450-014-0281-9

(تُشكل الهجمات الإلكترونية على البنية التحتية الحيوية مصدر قلق أكبر من عمليات اختراق البيانات للشركات)

Security Magazine. 2020. 'Critical Infrastructure Cyberattacks a Greater Concern Than Enterprise Data Breaches.' *Security Magazine*, 26 March. As of 25 October 2020: https://www. securitymagazine.com/articles/91992-critical-infrastructure-cyberattacks-a-greater-con- cern-than-enterprise-data-breaches

منظمة شنغهاي للتعاون، 2009. (اتفاقية التعاون لضمان أمن المعلومات الدولي بين الدول الأعضاء في منظمة شنغهاي للتعاون) 16 يونيو. اعتبارًا من أكتوبر 2020.

Shanghai Cooperation Organization. 2009. 'Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization.' 16 June. As of 21 October 2020: http://eng.sectsco.org/load/207508

(البنية التحتية الحيوية: أنظمة التحكم والهجمات الإرهابية)

Shea, Dana A. 2004. 'Critical Infrastructure: Control Systems and the Terrorist Threat.' CRS Report for Congress, RL20 ,31534 January. As of 21 October 2020: https://apps.dtic.mil/sti/pdfs/ADA467307.pdf

(مراجعة تقييم الخسارة الاقتصادية لانقطاع التيار الكهربائي)

Shuaia, Mao, Wang Chengzhib, Yu Shiwena, Gen Haoa, Yu Jufanga & Hou Hui. 2018. 'Review on Economic Loss Assessment of Power Outages.' *Procedia Computer Science* 130: 1158–63. As of 25 October 2020: https://www.sciencedirect.com/science/article/pii/S1877050918305131

(كونهم في مرمى الهدف: هل تواكب الخدمات التهديدات الإلكترونية الصناعية؟)

Siemens Gas & Power. 2019. *Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat?* Houston: Siemens. As of 21 October 2020: https://assets.new. siemens.com/siemens/assets/api/uuid:35089d45-e1c2-4b8b-b4e9-7ce8cae81eaa/ version:1572434569/siemens-cybersecurity.pdf

(فنزويلا ترزح تحت انقطاع هائل في التيار الكهربائي والاتصالات)

Smith, Scott, Fabiola Sanchez & Christopher Torchia. 2019. 'Venezuela Buckles under Massive Power, Communications Outage.' *Associated Press*, 9 March. As of 21 October 2020: https:// apnews.com/6ba2f69b77e2457da64593a7b8eced16

(يعبث المهاجمون بمحطة معالجة المياه في فلوريدا عن طريق تغيير المستويات الكيميائية)

Statt, Nick. 2021. 'Hackers Tampered with a Water Treatment Facility in Florida by Changing Chemical Levels.' The Verge, 8 February. As of 8 February 2021: https://www.theverge.com/2021/2/8/22273170/hackers-water-treatment-facility-florida-hacked-chemical-levels-changed

(المهاجمون الإلكترونيون يحتجزون بيانات المستشفيات الألمانية كرهينة)

Steffen, Sarah. 2016. 'Hackers Hold German Hospital Data Hostage.' DW, February 25. As of 21 October 2020: https://www.dw.com/en/hackers-hold-german-hospital-data-hostage/a-19076030

(إطار وطني عام لحماية البنية التحتية الحيوية للمعلومات)

Suter, Manuel. 2007. *A Generic National Framework for Critical Information Infrastructure Pro- tection (CIIP*). Zurich: Center for Security Studies. As of 25 October 2020: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf

مؤتمر الأمم المتحدة حول التنظيم الدولي. 1945. (ميثاق الأمم المتحدة والنظام الأساسي لمحكمة العدل الدولية). سان فرانسيسكو, 26 يونيو.

United Nations Conference on International Organization. 1945. *Charter of the United Nations and Statute of the International Court of Justice.* San Francisco, 26 June.

المديرية التنفيذية للجنة الأمم المتحدة لمكافحة الإرهاب ومكتب الأمم المتحدة لمناهضة الإرهاب. 2018. (حماية البنى التحتية الحيوية ضد الهجمات الإرهابية: خلاصة الممارسات الجيدة) يونيو.

United Nations Counter-Terrorism Committee Executive Directorate (UNCTED) & UN Office on Counter-Terrorism (UNOCT). 2018. *The Protection of Critical Infrastructures against Terrorist Attacks: Compendium of Good Practices*. June. As of 21 October 2020: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_eng.pdf

الجمعية العامة للأمم المتحدة. 1970. (إعلان مبادئ القانون الدولي المتعلقة بالعلاقات الصديقة والتعاون بين الدول وفقًا لميثاق الأمم المتحدة), 24 أكتوبر 1970

United Nations General Assembly (UNGA). 1970. *Declaration on principles of international law concerning friendly relations and co-operation among States in accordance with the Charter of the United Nation*, UN Document A/PV.1883, 24 October 1970.

1999. (مراجعة تنفيذ التوصيات والقرارات التي تبنتها الجمعية العامة في دورتها الاستثنائية العاشرة: تقرير هيئة نزع السلاح.

———. 1999. *Review of the implementations of the recommendations and decisions adopted by the General Assembly at its tenth special session: Report of the Disarmament Commission*, UN Document A/182/51/Rev.9 ,1 June 1999. As of 21 October 2020: https://www.un.org/disarmament/wp-content/uploads/09/2019/A-182-51-Rev.-1E.pdf page=53

2001. (مسؤولية الدول تجاه الأفعال غير المشروعة دوليًا), 28 يناير 2001)

———. 2001. *Responsibility of States for internationally wrongful acts*, UN Document A/RES/56/83, 28 January 2001.

2010. (فريق الخبراء الحكوميين المعني بالتطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي), 10 يوليو 2010.

———. 2010. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Document A/65/201, 10 July 2010.

2015أ. (التطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي), 23 ديسمبر 2015.

———. 2015a. *Developments in the field of information and telecommunications in the context of international security*, UN Document A/RES/70/237, 23 December 2015.

2015أ. (فريق الخبراء الحكوميين المعني بالتطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي), وثيقة للأمم المتحدة, 22 يوليو 2015.

———. 2015b. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN document A/70/174, 22 July 2015.

2341 (2017)), 13 فبراير S/RES/2017 مجلس الأمن التابع للأمم المتحدة. 2017. (وثيقة الأمم المتحدة.

United Nations Security Council (UNSC). 2017. UN document S/RES/2341 (2017), 13 February 2017.

فريق الاستجابة للطوارئ الحاسوبية التابع للولايات المتحدة الأمريكية. 2015. (المبادئ الإرشادية للإبلاغ عن الحوادث الفيدرالية لفريق الاستجابة للطوارئ الحاسوبية التابع للولايات المتحدة الأمريكية.

United States Computer Emergency Readiness Team (US-CERT). 2015. 'US-CERT Federal Incident Notification Guidelines.' As of 6 March 2021: https://www.cisa.gov/uscert/sites/default/files/publications/Federal_Incident_Notification_Guidelines_2015.pdf

الوكالة الأمريكية للأمن الإلكتروني وأمن البنية التحتية. 2020أ. (التنبيه (AA049-20A) حول فيروس الذي Ransomware يؤثر على تشغيل خطوط الأنابيب الرئيسية), 18 فبراير

United States Cybersecurity and Infrastructure Security Agency (CISA). 2020a. 'Alert (AA20- 049A) Ransomware Impacting Pipeline Operations.' Department of Homeland Security, 18 February. As of 21 October 2020: https://us-cert.cisa.gov/ncas/alerts/aa20-049a

2020ب. (الإرشادات حول القوى الأساسية العاملة في البنية التحتية الحيوية: ضمان المرونة المجتمعية والوطنية في الاستجابة لفيروس كورونا (كوفيد-19)), الإصدار 4.0, 18 أغسطس.

———. 2020b. 'Guidance on the Essential Critical Infrastructure Workforce: Ensuring Community and National Resilience in COVID-19 Response.' Version 4.0, 18 August. As of 11 February 2021: https://www.cisa.gov/sites/default/files/publications/ECIW_4.0_Guidance_on_Essential_Critical_Infrastructure_Workers_Final3_508_0.pdf

وزارة الطاقة الأمريكية. 2019. (تقرير التقييم).

United States Department of Energy (DOE). 2019. *Evaluation Report*. DOE-OIG-20-12, 19 November. Washington, DC: US DOE. As of 25 October 2020: https://www.energy.gov/sites/default/files/2019/11/f68/DOE-OIG-20-12.pdf

وزارة الأمن القومي الأمريكية. 2020. (القضايا الدولية الخاصة بالخطة الوطنية لحماية البنية التحتية لحماية CI/K).

United States Department of Homeland Security. 2020. 'National Infrastructure Protection Plan International Issues for CI/KR Protection.' As of 25 October 2020: https://www.dhs.gov/ xlibrary/assets/nipp_international.pdf

المعهد الوطني الأمريكي للمعايير والتكنولوجيا. 2012. (دليل التعامل مع حوادث أمن الحاسوب: توصيات المعهد الوطني للمعايير والتكنولوجيا). نشرة خاصة 880-61, المراجعة الثانية).

United States National Institute of Standards and Technology (NIST). 2012. *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology*. Special Publication 800-61, Revision 2. Gaithersburg: US NIST. As of 25 October 2020: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

(الثغرات في البنية التحتية عبر الوطنية: التهيئة التي أدت إلى انقطاع التيار الكهربائي عن أوروبا عام 2006 عبر التاريخ)

Van der Vleuten, Erik, & Vincent Lagendijk. 2010. 'Transnational infrastructure vulnerability: The historical shaping of the 2006 European "Blackout."' Energy Policy 38 (4): 2042–2052.

(ما الذي يمكن أن يتعلمه صناع سياسات الأمن الإلكتروني من المبادئ المعيارية في الحوكمة العالمية), سبتمبر 2020)

Vidyarthi, Apratim, & Anastasiya Kazakova. 2020. 'What Cybersecurity Policymaking Can Learn from Normative Principles in Global Governance,' background paper, *IGF 2020 Best Practice Forum on Cybersecurity*, September 2020.

التعاون الدولي للتخفيف من العمليات الإلكترونية التي تمس البنية التحتية الحيوية

التوقعات المعيارية والممارسات الجيدة الناشئة

تمثل أنشطة الجرائم الإلكترونية تهديدًا للبنية التحتية الحيوية وبالتالي لرفاه مجتمعاتنا, إذ يمكن أن تؤدي الحوادث الكبرى إلى زعزعة استقرار الدول وتهديد السلم والأمن على المستوى الدولي. وللتصدي لخطر التهديدات الإلكترونية المعقدة والفعالة بشكل متزايد, والتي تستهدف البنية التحتية الحيوية, يستخدم المجتمع الدولي معايير السلوك المتوقع للدول في الفضاء الإلكتروني لتعزيز التعاون. يبحث هذا التقرير في المعايير – على النحو الذي اقترحه فريق الخبراء الحكوميين التابع للأمم المتحدة عام ٢٠١٥ والمعني بالتطورات في مجال تكنولوجيا المعلومات والاتصالات في سياق الأمن الدولي –والذي يحث الدول على الاستجابة لطلبات (ICT) الدول الأخرى للمساعدة أو التخفيف في حال حدوث أنشطة الجرائم الإلكترونية ضد البنية التحتية الحيوية.

UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH