أمن سلسلة التوريد في عصر الإنترنت

اتجاهات القطاع، والتهديدات الحالية، واستجابات أصحاب المصلحة المتعددين

أولج ديميدوف وجياكومو بيرسي باولي

40 | UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

شكر وتقدير

يحظى برنامج الأمن والتكنولوجيا التابع لمعهد الأمم المتحدة لبحوث نزع السلاح بدعم من حكومة ألمانيا, وهولندا, والنرويج وسويسرا. ويتقدم المؤلفون بالشكر إلى السيد كريس نيسن, مدير الاستجابة للتهديد غير المتماثل وأمن سلسلة التوريد في منظمة ميتري؛ والسيد دونالد أ. (آندي) بوردي الابن, كبير مسؤولي الأمن في شركة هواوي (الولايات المتحدة الأمريكية)؛ والسيد كاي مايكل هيرمسن, المنسق العالمي لميثاق الثقة في شركة سيمنز؛ والسيدة كيرستن فيغنارد, رئيسة فريق دعم عمليات الجمعية العامة عملاً بالقرارين 27/73 و266/73 في معهد الأمم المتحدة لبحوث نزع السلاح, لمناقشة محتوى التقرير وتقديم الملاحظات والتوصيات.

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, المجتمعَ الدولي على تطوير الأفكار العَملية والمبتكرة الضرورية لإيجاد الحلول للمشاكل الأمنية الحرجة والمهمة.

ملاحظة

لا تعني التسميات المستخدمة وطريقة عرض المواد في هذا المنشور التعبيرَ 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.

قائمة المحتويات

نبذة عن المؤلفين

أولج ديميدوف باحث في مجال الفضاء الإلكتروني ضمن برنامج الأمن والتكنولوجيا التابع لمعهد الأمم المتحدة لبحوث نزع السلاح. تخرج من جامعة لومونوسوف الحكومية في موسكو، وأجرى منذ عام 2011 أبحاثًا حول سياسة الأمن الإلكتروني، والحوكمة الإلكترونية وحوكمة الإنترنت العالمية، وحماية البنية التحتية للمعلومات المهمة والحساسة، بالإضافة إلى التأثيرات الأمنية الدولية للتقنيات التكنولوجية الناشئة. وقبل الانضمام إلى معهد الأمم المتحدة لبحوث نزع السلاح، قاد أولج برنامج الأمن السيبراني الدولي وحوكمة الإنترنت العالمية في مركز الفكر غير الحكومي PIR.

جياكومو بيرسي باولي هو قائد برنامج الأمن والتكنولوجيا التابع لمعهد الأمم المتحدة لبحوث نزع السلاح. تمتد خبرته لتشمل مجاليْ العلوم والتكنولوجيا، مع التركيز على تأثيرات التكنولوجيات الناشئة في الأمن والدفاع. وقبل أن ينضم إلى معهد الأمم المتحدة لبحوث نزع السلاح، كان مديرًا مُشاركًا في معهد RAND Europe، حيث تولى ملف الأمن القومي والسيبراني والمرونة، مع العمل مؤخرًا على الاستحواذ الإلكتروني، والسياسة والاستراتيجية الإلكترونية، وتطوير القدرات الإلكترونية.

الاختصارات والتسميات المختصرة

3GPP	مشروع شراكة الجيل الثالث
BSI	المكتب الفيدرالي لأمن المعلومات في ألمانيا
CBM	تدابير بناء الثقة
CEN	اللجنة الأوروبية للتقييس
CENELEC	اللجنة الأوروبية للتقييس الكهروتقني
CNSS	لجنة أنظمة الأمن القومي
CPNI	مركز حماية البنية التحتية الوطنية
C-SCRM	إدارة مخاطر سلسلة التوريد الإلكترونية
ETSI	المعهد الأوروبي لمعايير الاتصالات
G7	مجموعة الدول الصناعية السبعة
GCSC	اللجنة العالمية لاستقرار الفضاء الإلكتروني
GGE	فريق الخبراء الحكوميين
ICT	تكنولوجيا المعلومات والاتصالات
IEC	اللجنة الكهروتقنية الدولية
IGO	منظمة حكومية دولية
IoT	إنترنت الأشياء
ISO	المنظمة الدولية للتوحيد القياسي
ITU	الاتحاد الدولي للاتصالات
NCSC	المركز القومي للأمن الإلكتروني
NESAS	مشروع ضمان أمن معدات الشبكة
NIST	المعهد الوطني للمعايير والتقنية
OEWG	الفريق العامل مفتوح العضوية
OSCE	منظمة الأمن والتعاون في أوروبا

O-TTPS	معيار مُزود التكنولوجيا الموثوقة المُصادق عليه من منتدى المجموعة المفتوحة
SCO	منظمة شنغهاي للتعاون
SCRM	إدارة مخاطر سلسلة التوريد
SME(s)	الشركات الصغيرة والمتوسطة
(T)CBMs	الشفافية وتدابير بناء الثقة
TSC(s)	سلاسل التوريد التكنولوجية
UNGA	الجمعية العامة للأمم المتحدة

الملخص التنفيذي

ينطوي المفهوم التقليدي لسلسلة التوريد على اعتبارها نظامًا يضم المؤسسات، والأشخاص، والتكنولوجيا، والأنشطة، والمعلومات، والمصادر المعنية بنقل المنتَج أو الخدمة من المُورد (المُنتِج) إلى العميل. اليوم، ومع ظهور التحوُّل الرقمي العالمي، نجد أنّ سلاسل التوريد وطرق إداراتها تتغير وتتحول، مع زيادة المخاطر والتهديدات لأمنها وسلامتها. وتُسلط هذه الاتجاهات الضوء على زيادة الحاجة إلى حلول عالمية مشتركة وقابلة للتبني وقابلة للتطوير والتوسع ويمكنها عكس مسار التهديدات الإلكترونية لسلاسل التوريد أو كبحها من خلال الجهود التعاونية للحكومات، والصناعة، ومجتمع التكنولوجيا، وأصحاب المصلحة الآخرين.

هذا ويُعد أمن سلسلة التوريد أحد القضايا الرئيسية لعمليات تطوير المعايير المتعددة الأطراف المتعلقة بتكنولوجيا المعلومات والاتصالات (ICT)، ولا يزال النقطة الرئيسية للنقاش في إطار عمليتيْن إلكترونيتيْن جديدتيْن متعددتي الأطراف تم إطلاقهما في 2018 تحت رعاية الجمعية العامة للأمم المتحدة (UNGA): فريق الخبراء الحكوميين الجديد التابع للأمم المتحدة (GGE)، والفريق العامل مفتوح العضوية (OEWG) اللذان يركزان على التطورات في مجال تكنولوجيا المعلومات والاتصالات (ICT) في سياق الأمن الدولي.

يهدف هذا التقرير إلى تقييم الكيفية التي يمكن من خلالها تحسين وتفعيل الاستجابة المعيارية لتحديات تكنولوجيا المعلومات والاتصالات (ICT)، ذات الصلة بأمن سلسلة التوريد، وحيث أنّ المعايير تعكس التوقعات أو المعايير المشتركة للسلوك المناسب، فإنّ إيجاد الفرص لتحسينها وتفعيلها يلزمُه النظرُ فيما وراء القواعد والمعايير ذاتها، ووضعها في سياق منظومة الاستجابات الأوسع لتحديات أمن سلسلة التوريد لتحديد الفجوات ومواطن التحسين.

تطوُّر مشهد التهديدات الرقمية لسلاسل التوريد

بات زيادة حجم أنشطة الجرائم الإلكترونية التي تستهدف سلاسل التوريد أمرًا ملاحظًا من قبل الشركات الخاصة والوكالات الحكومية وخبراء الأمن الإلكتروني في جميع أنحاء العالم. وعلى نحو أكثر تحديدًا، فقد أصبحت الهجمات على برامج سلسلة التوريد أحد التهديدات الإلكترونية الرئيسية للصناعة ولأصحاب المصالح الآخرين، حيث أدى الوعي المتزايد بالأمن الإلكتروني والتدابير المضادة المحددة إلى تقليل فعالية الهجمات الإلكترونية الشائعة وزيادة تكلفتها.

وقد أصبحت المخاطر التي تتعرض لها مكونات الأجهزة والبرامج الثابتة في سلاسل التوريد مصدر قلق متزايد بين الحكومات والشركات الخاصة وخبراء الأمن الإلكتروني، وهذا يتضمن التقارير حول عمليات مخصصة من قبل جهات كيدية تهدف إلى الإضرار بسلاسل التوريد عبر إدخال وظائف وبرامج وأجهزة بطريقة مخفية «منافذ تمرير خفية».

الاستجابة لتحديات تكنولوجيا المعلومات والاتصالات التي تواجه أمن سلسلة التوريد وسلامتها

تستند منظومة الاستجابات الحالية لتحديات سلاسل التوريد القائمة على تكنولوجيا المعلومات والاتصالات (ICT) إلى خمس ركائز مترابطة ومتداعمة:

1. أطر التقييس الفني
2. الأطر التشريعية والتنظيمية الوطنية
3. إدارة أمن سلسلة التوريد للشركات وسياسات ضمان أمن سلسلة التوريد
4. أدوات وموارد بناء القدرات
5. الأطر المعيارية

المعايير الفنية تُشكل «اللغة المشتركة» المستخدمة في التواصل حول مستويات الأداء المتوقعة للمنتجات والخدمات، وهي من بين الركائز الأساسية للنظم البيئية المعقدة القائمة على التكنولوجيا، وسلاسل التوريد العالمية ليست استثناءً منها.

السياسات والأطر التنظيمية الوطنية تُكمل تطوير وإنفاذ المعايير الفنية، وتسمح للحكومات بتطوير وتنفيذ إدارة مخاطر سلسلة التوريد الإلكترونية (C-SCRM) على نحو أكثر شمولية وكليةً وفعالية بين مؤسسات القطاعيْن العام والخاص.

الممارسات وأطر العمل للشركات تتضمن مجموعة أدوات شاملة تنطوي على متطلبات البائعين، والإجراءات التفصيلية، والمبادئ الإرشادية وأفضل الممارسات التي تهدف إلى التقليل من مخاطر تكنولوجيا المعلومات والاتصالات (ICT) والتخفيف منها في سلاسل التوريد للشركات.

أدوات وموارد بناء القدرات من الخيارات لأصحاب المصالح المهمتين بتقييم وتحسين الممارسات الحالية. وتتضمن هذه الخيارات أدوات وخدمات التقييم (الذاتي) والتدقيق لإدارة مخاطر سلسلة التوريد الإلكترونية (C-SCRM), وحلول المنصات الرقمية للتعاون الآمن ومشاركة المعلومات بين بائعي التكنولوجيا, وأطر عمل إدارة مخاطر سلسلة التوريد الإلكترونية (C-SCRM) التطوعية, والطرق التي طورتها الصناعة ومجتمع التكنولوجيا لمساعدة المؤسسات على إدارة مخاطر سلاسل التوريد الخاصة بهم.

أطر ومبادرات تطوير المعايير

تمثل المعايير المستوى الأعلى ضمن منظومة الاستجابات لأمن سلسلة التوريد, وتُشكل في العادة الأطرَ المفاهيمية للعناصر التي تميل أكثر إلى الطابع التشغيلي (مثل المعايير, والسياسات, واللوائح, والمبادئ الإرشادية). كما يمكن تقسيم مبادرات تطوير المعايير للتعامل مع تحديات تكنولوجيا المعلومات والاتصالات (ICT) الخاصة بأمن سلسلة التوريد وسلامتها إلى ثلاث فئات:

1. العمليات متعددة الأطراف التي تقودها الأمم المتحدة فريق الخبراء الحكوميين (GGE) الإلكترون/السيبراني الحالي والفريق العامل مفتوح العضوية (OEWG – وكلاهما يستند إلى تقرير فريق الخبراء الحكوميين (GGE) عام 2015 ومجموعة المعايير المتضمنة فيه.
2. مبادرات المنظمات الوطنية أو الحكومية الدولية الأخرى التي تعالج أيضًا قضايا سلسلة التوريد في سياق أمن تكنولوجيا المعلومات والاتصالات (ICT) والتعاون الدولي (مثل منظمة شنغهاي للتعاون (SCO) ومجموعة الدول الصناعية السبعة G7).
3. مبادرات بناء المعايير لأصحاب المصلحة المتعددين, وذلك من خلال مجموعة مُوسعة من «رواد تغيير المعايير» (مثل تعهد حماية الأمن الإلكتروني, واللجنة العالمية لاستقرار الفضاء الإلكتروني).

وباستخدام التحليل المقارن بين المبادرات المختلفة, يمكن التوصل إلى الملاحظات التالية:

1. لقد ازداد العدد الإجمالي للأطر المعيارية التي تعالج قضية أمن سلسلة التوريد وسلامتها بسرعة متزايدة على مدى السنوات السبع السابقة – بدءًا من المبادرة الفعلية الوحيدة لفريق الخبراء الحكوميين(GGE) في 2013, إلى ثماني مبادرات في عام 2019.
2. العديد من هذه المبادرات (خمسة من أصل ثمانية) هي أطر عمل لأصحاب المصلحة المتعددين تم تطويرها وقيادتها إمّا من قِبل الجهات الفاعلة في صناعة التكنولوجيا (مثل شركة مايكروسوفت وسيمنز) أو من مزيج من مجموعات أصحاب المصلحة, بما في ذلك الدول والجهات الفاعلة في قطاع التكنولوجيا (مثل نداء باريس من أجل الثقة والأمن في الفضاء الإلكتروني).
3. يبدو أنّ المنظمات الإقليمية هي أقل فئة مُمثلة من الجهات الفاعلة التي تتصدى لتحديات تكنولوجيا المعلومات والاتصالات (ICT) المتعلقة بقضايا أمن سلسلة التوريد وسلامتها من منظور المعايير.
4. غالبية المعايير المقترحة (خمسة منها) تعد «إيجابية», وهي التي تشجع أو تُلزم الدول والجهات الفاعلة الأخرى باتخاذ إجراءات معينة للتخفيف من تهديدات تكنولوجيا المعلومات والاتصالات (ICT) لأمن سلسلة التوريد وسلامتها. كما أنّ هناك معياران «سلبيَّيْن», والآخر يتضمن مزيجًا من العناصر «الإيجابية» و«السلبية».

الفجوات في المعايير ذات الصلة بأمن سلسلة التوريد وإجراءات التخفيف المُوصى بها

تقدم هذه الدراسة عرضًا أوليًا «للفجوات» في الأطر المعيارية المقترحة أو المُطورة. وفي هذا السياق, لا يُنظر إلى الفجوات والقيود على أنّها «أوجه قصور», إنما تُعامَل على أنّها الفرصة التي قد يُساهم إجراء المزيد من التفصيل على المبادرات المعيارية (أو بشأن مسارات العمل الداعمة لها) في تفعيل الأطر المعيارية بشكل أفضل.

هذا وتم تصميم مجموعة من التوصيات الممكنة لسد تلك الفجوات والتعامل مع تلك القيود, بهدف إثارة النقاش بين صناع السياسات, والدبلوماسيين, وغيرهم من الخبراء الوطنيين المعنيين بجهود بناء القدرات, وكذلك بين الصناعة ومجتمع التكنولوجيا الأوسع ومجموعات أصحاب المصلحة الآخرين

وفيما يلي ملخص للفجوات والقيود والتوصيات ذات الصلة في الجدول أدناه, بالإضافة إلى المزيد من التفصيل حول ذلك في التقرير .

الفجوات والقيود والتوصيات

الفجوات والقيود

1

افتقار المعايير «السلبية» لآليات المراقبة والتحفيز والتنفيذ

تواجه مبادرات تطوير المعايير هذه تحديات نظرًا لافتقارها للدوافع والحوافز المناسبة التي تدعو الجهات الفاعلة المستهدفة للامتثال بها. كما أنّ إمكانية المراقبة الفعالة للمعايير السلبية محدودة بسبب التحدي المعروف والمتمثل في القدرة على الإسناد الموثوق به لأنشطة الجرائم الإلكترونية.

2

طبيعة التعامُل «المُجزأة» للمبادرات التي تركز على الوظائف المخفية الضارة

تتعامل المعايير التي يقتصر نطاقها على التعامل مع الطرق المخفية لتعطيل الوظائف الإلكترونية مع مخاطر الوظائف المخفية بمنأىً عن بقية مخاطر تكنولوجيا المعلومات والاتصالات (ICT) لسلاسل التوريد, وعليه فهي تُقوّض النموذج القائم على نهج إدارة المخاطر الشامل والمتكامل.

التوصيات

مواءمة نطاق المعايير المقترحة مع نهج إدارة مخاطر سلسلة التوريد (SCRM) الشامل وممارسات الصناعة

الاستفادة من تفويض الفريق العامل مفتوح العضوية (OEWG) لتطوير المزيد من المعايير, والقواعد والمبادئ – ويمكن أن تتضمن الإجراءات المحددة ما يلي:

- ضمان توازن أفضل بين المعايير «السلبية» والإيجابية»
- توسيع نطاق تركيز المعايير (الجديدة والمعتمدة) للتعامل مع السلسلة الكاملة لمخاطر تكنولوجيا المعلومات والاتصالات (ICT) ومواءمة محتوى المعايير المقترحة مع النُهج المستخدمة في الصناعة ومجتمع التكنولوجيا

3

الفجوات والقيود

تداخل وازدواجية الجهود ضمن مبادرات أصحاب المصلحة المتعددين

في حين أنّ التنوع في الأطر والمبادرات، وحتى التنافس فيما بينها، يعزز أجندة بناء معايير الأمن الإلكتروني العالمية، فقد يؤدي أيضًا
إلى تشتت الجهود. ويؤدي هذا الاتجاه على وجه الخصوص إلى خطر وجود أطر إدارة مخاطر (SCRM) سلسلة التوريد المتعددة والمتوازية التي تتنافس على وضع الممارسة المعيارية العالمية الواقعية.

التوصيات

تعزيز التنسيق والتآزر بين مبادرات تطوير المعايير من قبل أصحاب المصلحة المتعددين، وتعزيز الشروط الدُنيا الموحدة والقابلة للتشغيل المتبادل لموردي التكنولوجيا

ويمكن أن تتضمن الإجراءات المحددة ما يلي:

- استكشاف الفرص لتوفير تدفق الاتصال ومشاركة المعلومات بشكل منظم ومنهجي بين عمليات تطوير المعايير لدى أصحاب المصلحة االمتعددين والتي تعالج قضايا سلسلة التوريد العالمية في سياق تكنولوجيا المعلومات والاتصالات (ICT).
- إطلاق عملية لمناقشة وتفصيل مجموعة موحدة أو على الأقل مُنسقة وقابلة للتشغيل المتبادل من الشروط الدنيا لمعايير الأمن وإصدار الشهادات (الاعتماد)، بحيث تكون مشتركة ومدعومة ومعززة بشكل مشترك من قِبل المنتديات الرئيسية لأصحاب المصلحة المتعددين.

4

الفجوات والقيود

عدم وجود أطر عمل موحدة للتعامل مع بائعي التكنولوجيا العالميين في الأسواق الوطنية

في ظل عدم تَوفُّر معايير دولية لضمان أمن سلسلة التوريد لدى التعامل مع مزودي التكنولوجيا الأجانب، يقوم عدد متزايد من الدول الأعضاء بإنشاء ووضع قواعد ومتطلبات على المستوى الوطني. وقد يؤدي ذلك إلى الإضرار بتماسك (وفعالية) الجهود المبذولة على المستوى الدولي، وإلى زيادة تكلفة الامتثال بالنسبة للبائعين.

التوصيات

مواءمة العمليات الوطنية للعمل مع بائعي التكنولوجيا العابرين للحدود

استكشاف فرص التنسيق والمواءمة للنُهج والعمليات المُتبعة العابرين للحدود لإدارة بائعي التكنولوجيا عبر الدول، لتصبح أكثر شفافية ومواءمة مع إدارة مخاطر سلسلة التوريد (SCRM) العالمية ومعايير تقييم أمن البائعين.

5

الفجوات والقيود

عدم التنسيق والتآزر بين المبادرات المعيارية الحكومية الدولية والصناعة العالمية ومجتمع التكنولوجيا

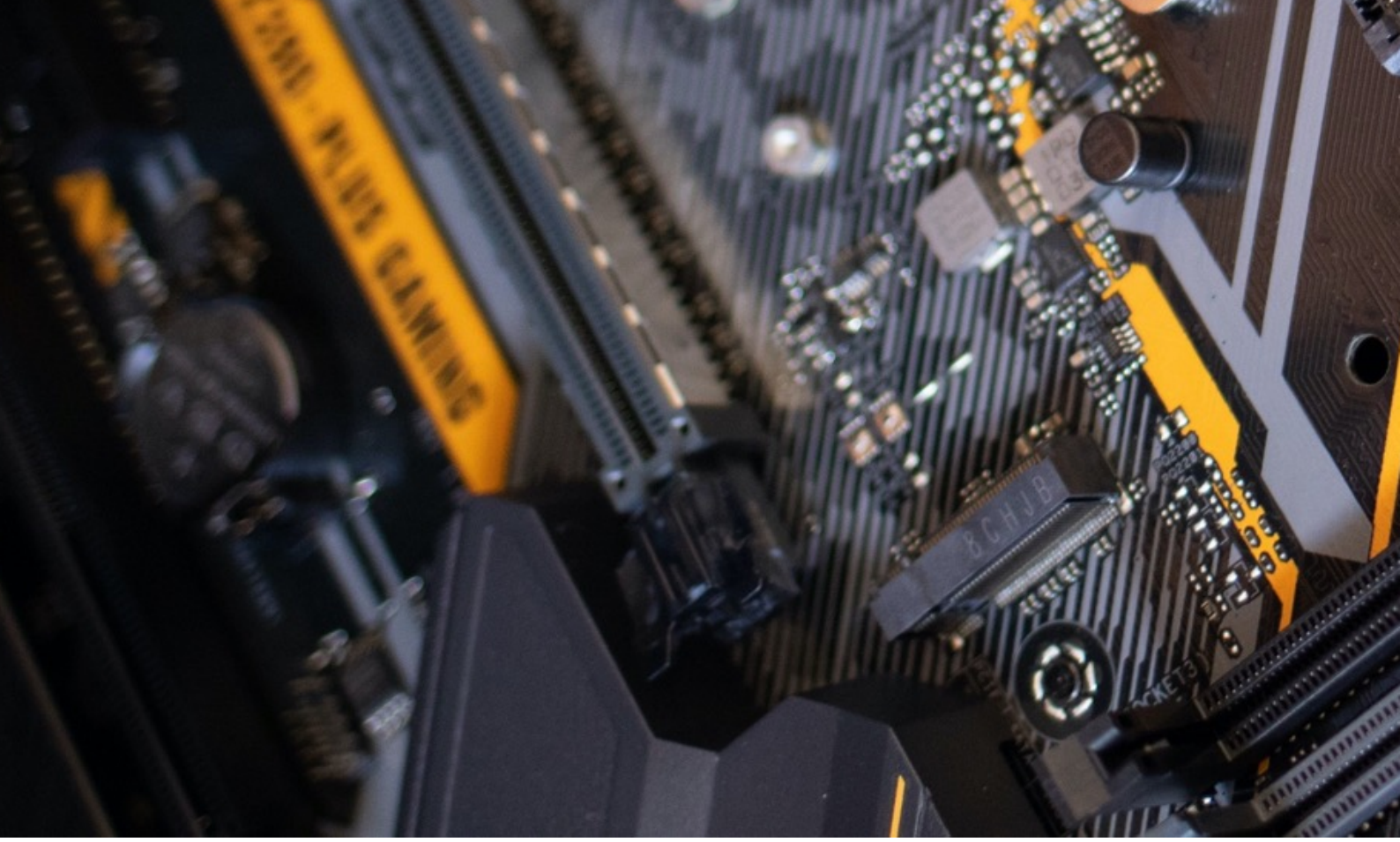
تقدم جهود بناء المعايير التي تبذلها مختلف الجهات الفاعلة (مثل الأمم المتحدة, والصناعة, ومجموعات أصحاب المصلحة المتعددين) مستويات مختلفة من النضج والتركيز على المواضيع وطرق التمثيل. وبما أنّ هذه الجهود لا تسعى بشكل متعمد لتحقيق عمليات تكميلية أو إضافية, فإنّ تأثير مجموعة المبادرات الشاملة يبدو دون المستوى الأمثل والمطلوب.

التوصيات

النظر في إنشاء منصة مخصصة لدعم العمليات التي تقودها الأمم المتحدة للتعامل مع الصناعة ومجتمع التكنولوجيا ومجموعات أصحاب المصلحة الآخرين والمبادرات النشطة في مجال أمن سلسلة التوريد وسلامتها

في إطار تفويض الفريق العامل مفتوح العضوية (OEWG) لإقامة حوار مؤسسي منتظم بمشاركة واسعة, بما في ذلك مشاركة القطاع الخاص, يتعين النظر في إنشاء منصة مخصصة (على سبيل المثال لجنة أو فريق عمل) لدعم تفعيل معايير الأمن الإلكتروني الدولية ذات الصلة بسلامة وأمن سلاسل التوريد.

ليس الهدف من المنصة المقترحة تأدية دور مكافئ أو بديل لعمليات تطوير المعايير الإلكترونية الحكومية الدولية, بل لتقدم الدعم الضروري والأساسي لتلك العمليات في المجالات التي يكون للقطاع الخاص فيها دور رئيسي متأصل في تنفيذ المعايير المقترحة.



6

الفجوات والقيود

عدم التركيز على معالجة مخاطر تكنولوجيا المعلومات والاتصالات (ICT) لسلسلة التوريد من خلال بناء القدرات

باعتبار أنّ النظام البيئي لموردي التكنولوجيا مشتت حول العالم, وأنّ العديد من الموردين يتواجدون في ولايات قضائية تفتقر إلى السياسات التنظيمية وأطر التقييس الناضجة, يمكن لجهود بناء القدرات الدولية أن تُحسن بشكل كبير بيئة المخاطر ككل في سلاسل التوريد العالمية.

التوصيات

زيادة التركيز على جهود بناء القدرات

يتعين على الدول أن تُجري وبشكل مستقل أو بدعم من جهة خارجية تقييمًا للقدرات الوطنية لتحديد الفجوات واحتياجات بناء القدرات ذات الصلة بتخفيف مخاطر تكنولوجيا المعلوما والاتصالات (ICT) لسلاسل التوريد.

كما يتعين على المنظمات الإقليمية القيام بالشيء ذاته, ويجب أن تُوفرَ البياناتِ والمعلوماتِ والمواردَ الأوسع لدعم الدولة وبائعي التكنولوجيا المستعدين لإنشاء الأعمال في مناطق أو دول المحددة

هذا ويجب تطوير مبادرات بناء القدرات متعددة الأطراف للتركيز بشكل محدد على مخاطر سلاسل التوريد.

7

الفجوات والقيود

عدم التركيز على استخدام مجموعة أدوات تدابير بناء الثقة (CBM) لمعالجة مخاطر تكنولوجيا المعلومات والاتصالات (ICT) التي تمس سلسلة التوريد

كما هو الحال في بناء القدرات, لم يتم البحث بشكل كافٍ في الدور الذي تُؤديه الشفافية وتدابير بناء الثقة (TCBM) في معالجة مخاطر تكنولوجيا المعلومات والاتصالات (ICT) لسلاسل التوريد التكنولوجية (TSCs). النجاح النسبي في اعتماد تدابير بناء الثقة (CBM) على المستوى الإقليمي (منظمة الأمن والتعاون (OSCE) في 2021 و 2016), وعلى المستوى الثنائي (الاتفاقيات بين روسيا والولايات المتحدة في 2013),للتخفيف من مخاطر تكنولوجيا المعلومات والاتصالات (ICT) العابرة للحدود, كل ذلك يعطي سببًا لاستكشاف المزيد حول إمكانية اعتماد مجموعة أدوات تدابير بناء الثقة (CBM) لإدارة تحديات الأمن الإلكتروني لسلاسل التوريد التكنولوجية (TSCs).

التوصيات

تقييم وتحديد فرص استخدام مجموعة أدوات الشفافية وتدابير بناء الثقة T)CBM) لضمان أمن وسلامة سلاسل التوريد التكنولوجية تقييم وتحديد فرص استخدام مجموعة أدوات الشفافية وتدابير بناء الثقةلضمان أمن وسلامة سلاسل التوريد التكنولوجية (TSCs)

كجزء من أعمال الفريق العامل المفتوح عضوية (OEWG), دراسة مدى الحاجة إلى توسيع قائمة الشفافية وتدابير بناء الثقة (T)CBMs) للأمن الإلكتروني بإضافة التدابير التي تخص بالتحديد التخفيف من المخاطر الإلكترونية على سلاسل التوريد التكنولوجية (TSCs), أو الحاجة إلى صياغة تفسير سياقي للتدابير المعتمدة فعليًا لتعكس القضايا ذات الصلة بسلسلة التوريد. إضافة إلى ذلك, يتعين على الدول النظر في مشاركة طوعية للمعلومات من جانب واحد حول تهديدات تكنولوجيا المعلومات والاتصالات (ICT), فضلًا عن التعزيز ثنائي الجوانب لتدابير الثقة والشفافية التي تستهدف أمن سلاسل التوريد وسلامتها على وجه الخصوص.

8

الفجوات والقيود

انخفاض مستوى نضج الأطر والمبادرات الوطنية لضمان أمن وسلامة سلاسل التوريد التكنولوجية (TSCs) على المستوى الوطني بشكل عام

تتركز غالبية الاستجابات الحديثة على المستوى الوطني لمعالجة مخاطر تكنولوجيا المعلومات والاتصالات (ICT) لسلاسل التوريد التكنولوجية (TSCs) في عدد محدود من الدول؛ إذ تكشف النظرة على الدول المتبقية مستويات أقل بكثير من النضج في الاستجابات الاستراتيجية والسياساتية والتنظيمية لمثل تلك التحديات.

التوصيات

تعزيز التنسيق المؤسسي والاستراتيجي والسياساتي للجهود المبذولة لمعالجة تحديات تكنولوجيا المعلومات والاتصالات (ICT) لسلاسل التوريد التكنولوجية (TSCs) على المستوى الوطني

تم طرح هذه التوصية على النطاق الوطني, كما تُركز على الحاجة إلى تحسين التنسيق (الداخلي) لجهود الدول للتخفيف من تحديات تكنولوجيا المعلومات والاتصالات (ICT) لسلاسل التوريد على المستوى المحلي.


COM-A
COM-B
LINE-O
VID-O

المقدمة

1.1 السياق

غالبًا ما ينطوي نقل منتج أو خدمة على نظام من المنظمات والأشخاص والتكنولوجيا والمعلومات والأنشطة، والذي يُشار إليه في العادة بـ «سلسلة التوريد».[1]

وقد كانت التحديات الإلكترونية المتعلقة بسلامة وأمن سلاسل التوريد العالمية محور التركيز لمبادرات تطوير المعايير الدولية لعدة سنوات. ويشير هذا التقرير، وفقًا لما جاء في الدراسة التي أجراها البنك الدولي، إلى المعايير العالمية على أنّها «توقعات أو معايير السلوك المناسب المشتركة التي تقبلها الدول والمنظمات الحكومية الدولية، والتي يمكن تطبيقها على الدول، والمنظمات الحكومية الدولية، و/أو الجهات الفاعلة [غير التابعة للدول] بمختلف أنواعها».[2]

على مستوى الجمعية العامة للأمم المتحدة (UNGA)، تم ذكر المعايير التي تركز على تكنولوجيا المعلومات والاتصالات (ICT) وسلاسل التوريد بشكل مباشر وصريح للمرة الأولى عام 2013، في تقرير فريق الخبراء الحكوميين حول التطورات في مجال المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي (الذي أعده فريق الخبراء الحكوميين (GGE) للأمن الإلكتروني التابع للأمم المتحدة). وقد حدد التقرير المخاطر التي تهدد «الاستخدام الآمن والموثوق لتكنولوجيا المعلومات والاتصالات (ICT)، وسلاسل التوريد القائمة على تكنولوجيا المعلومات والاتصالات (ICT)، للمنتجات والخدمات»، مع التركيز بشكل خاص على الوظائف المخفية المُضمنة فيها (المُسمّاة «منافذ التمرير الخفية»).[3] هذا ودعا تقرير فريق الخبراء الحكوميين (GGE) في 2013 الدولَ أيضًا إلى تشجيع القطاع الخاص والمجتمع المدني عل تأدية دورهم المناسب في تحسين أمن تكنولوجيا المعلومات والاتصالات (ICT)، بما في ذلك أمن سلسلة التوريد.[4] كما تم تكرار هذه التوصية وتوسيعها في تقرير 2015 لفريق الخبراء الحكوميين (GGE) اللاحق (الرابع) من بين المعايير والقواعد والمبادئ الأخرى المقترحة للسلوك المسؤول من الدول.

بالرغم من ذلك، وعلى مدى السنوات العديدة الماضية، فقد تَلقّت جهود تطوير المعايير التي تهدف إلى تعزيز الأمن الإلكتروني والاستقرار العالمي للفضاء الإلكتروني مساهمات كبيرة من أصحاب المصلحة المتعددين وأطر القطاع الخاص، وتضمنت مجموعة من المبادرات التي تقودها شركات التكنولوجيا الكبرى، مثل اتفاقية جنيف الرقمية لحماية الفضاء الإلكتروني من قبل مايكروسوفت، أو ميثاق الثقة للأمن الإلكتروني من سيمنز، والجهود التي أطلقتها الحكومة لأصحاب المصلحة المتعددين مثل نداء باريس من أجل الثقة والأمن في الفضاء الإلكتروني.

1 للمزيد من التعريفات، يرجى الرجوع إلى . ISO (2014, part I) ; ENISA (2015).
2 Martinsson (2011).
3 UNGA (2013).
4 UNGA (2013).

انضمت هذه الجهات الفاعلة من قطاع الصناعة الخاص، والمجتمع المدني ومجتمع التكنولوجيا، التي تُوصف أحيانًا بـ «رواد تغيير المعايير»[5]، إلى الجهات الفاعلة الحكومية والجهات الحكومية الدولية في النقاش حول معايير الأمن الإلكتروني، كما ساهمت في مجموعة واسعة من المبادرات والجهود لتطوير وتعزيز متطلبات إلزامية جديدة لأمن سلسلة التوريد وسلامتها وشفافيتها على المستوى العالمي، بالإضافة إلى أفضل الممارسات المقننة، والمعايير ومعايير الاعتماد المرجعية.

وفي هذا السياق، فإن حقيقة أنّ غالبية المعايير والتوصيات المقترحة والتي طورها «رواد تغيير المعايير» الإلكترونية كانت تُركز على أمن وسلامة سلاسل التوريد توضّح مدى أهمية وحجم التحديات القائمة على تكنولوجيا المعلومات والاتصالات (ICT) . كما أنّ هذا التركيز ناتج عن زيادة تكلفة الهجمات وأنشطة الجرائم الإلكترونية التي تؤثر على أمن وسلامة سلاسل التوريد العالمية والتي تواجه القطاع الخاص.[6]

تُشكل الجهات الحكومية الكبيرة والمنظمات الحكومية، ولا سيما في قطاع الدفاع، حصة كبيرة في سوق مُشتري التكنولوجيا العالمية[7]، ومن ثمّ فهم يعتمدون على مُكونات تكنولوجيا المعلومات والاتصالات (ICT)، وعلى المنتجات والخدمات، بما في ذلك المنتجات التجارية الجاهزة التي تُورَّد لهم من الشركات الخاصة. وهذا يُحدد بشكل مُسبق دور الصناعة الخاصة كخط الدفاع الأول ضد التهديدات التي تمس أمن وسلامة سلاسل التوريد العالمية الناشئة عن الاستخدام الكيدي لتكنولوجيا المعلومات والاتصالات (ICT)، بما في ذلك الهجمات على البرامج وأنواع أخرى من استغلال الأجهزة والبرمجيات.

اليوم، أصبح القيام بهذا الدور أمرًا أكثر صعوبة؛ إذ أفاد خبراء الأمن بحدوث زيادة مفاجئة وسريعة في استغلال سلاسل التوريد التكنولوجية (TSCs)، باعتبارها ناقلًا مُفضلًا وشائعًا للهجمات الإلكترونية والتجسس التكنولوجي، وغيرها من الأنشطة التي تقوم بها مجموعة متنوعة من الجهات الفاعلة، بدءًا من مجرمي الإنترنت إلى وكلاء الدولة المزعومين. إضافة إلى كل ذلك، عبّر عدد متزايد من الدول عن مخاوفها من اعتمادية صناعاتها والوكالات الحكومية فيها على بائعي التكنولوجيا الأجانب في القطاعات الحساسة والحرجة مثل التكنولوجيا ذات الاستخدام المزدوج وتكنولوجيا الدفاع، وكذلك التكنولوجيات الاستراتيجية الرقمية مثل اتصالات الجيل الخامس.[8]

أما فيما يتعلق بعمليات تطوير المعايير الدولية، فتشدد هذه الاتجاهات بقدر أكبر على الحاجة إلى ضمان التشغيل الفعال للمعايير (والمعدات الداعمة مثل مجموعة أدوات التكنولوجيا وأفضل الممارسات) لتحسين إدارة المخاطر وزيادة المرونة في التصدي لتهديدات تكنولوجيا المعلومات والاتصالات (ICT)، الخاصة بسلاسل التوريد التكنولوجية (TSCs).

بالنسبة للأمم المتحدة والدول الأعضاء فيها، فإنّ فرصة التّقدُّم في هذا الاتجاه مفتوحة الآن، مع إطلاق عمليتيْن متوازيتيْن لمعالجة تحديات الأمن الإلكتروني: فريق الخبراء الحكوميين (GGE) السادس والفريق العامل المفتوح عضوية الجديد (OEWG)، اللذين تم تكوينهما بموجب قرار الجمعية العامة للأمم المتحدة (UNGA) A / RES / 73/27 في أواخر عام 2018.[9]

5 Hurel & Lobato (2018).
6 CrowdStrike (2018).
7 Evermann (2014).
8 EC (2019a); Feinstein (2019); US White House (2019b); Wright (2019).
9 UNGA (2018).

2.1 نطاق التقرير والغرض منه

يهدف هذا التقرير إلى تقييم كيفية تحسين وتعزيز وتفعيل الاستجابات المعيارية لتحديات تكنولوجيا المعلومات والاتصالات (ICT) التي تؤثر على أمن سلسلة التوريد.

كما أنّ الغرض من هذا التقرير هو دعم السياسة وصانعي القرار المشاركين في العمليات متعددة الأطراف والإقليمية والوطنية المتعلقة بتطوير المعايير الإلكترونية. إضافة إلى ذلك، يمكن أن يحقق هذا التقرير الفائدة لمجموعات أصحاب المصلحة الأخرى، مثل شركات القطاع الخاص، والمجتمع المدني، ومجتمعات التكنولوجيا.

3.1 هيكل التقرير

تم تنظيم هذا التقرير ضمن عدة مواضيع، وهي مفصلة بشكل محدد فيما يلي:

- الفصل الثاني يقدم نبذة حول الاتجاهات الرئيسية الحالية المتعلقة بالتكنولوجيا الرقمية التي تؤثر على سلاسل التوريد العالمية، بما في ذلك مدى التقارب أو التلاقي بين سلاسل التوريد المادية والرقمية، والانتشار السريع لمخاطر الأمن الإلكتروني في علاقات سلسلة التوريد، وغيرها من الاتجاهات ذات الصلة.
- الفصل الثالث يقدم نبذة أساسية حول تحديات ومخاطر وتهديدات تكنولوجيا المعلومات والاتصالات (ICT) التي تمس أمن وسلامة سلاسل التوريد عبر القطاعات والولايات القضائية. ويتضمن ذلك تصنيفًا أساسيًا لمخاطر الأمن الإلكتروني التي تواجه سلاسل التوريد، بالإضافة إلى نبذة حول مجموعة من حوادث وهجمات الأمن الإلكتروني التي تؤثر على سلاسل التوريد في السنوات الأخيرة.
- الفصل الرابع يقدم نبذة عن منظومة الاستجابات لتحديات تكنولوجيا المعلومات والاتصالات (ICT) التي تمس أمن سلاسل التوريد، بما في ذلك التقييس الفني والأطر القانونية والتنظيمية الوطنية، وممارسات الشركات، ومبادرات بناء القدرات
- الفصل الخامس يتناول مبادرات تطوير المعايير العالمية التي تركز على ضمان الأمن والسلامة لسلاسل التوريد في سياق تحديات تكنولوجيا المعلومات والاتصالات (ICT)، بما في ذلك معايير فريق الخبراء الحكوميين (GGE) والأطر المعيارية الأخرى.
- الفصل السادس يحدد ويبحث في الفجوات بين مبادرات تطوير المعايير وآليات تنفيذها، إضافة إلى الآليات العَملية (الفنية والتنظيمية) والأدوات المُطورة والمستخدمة حاليًا من الجهات الفاعلة في الصناعة وأصحاب المصلحة الآخرين لضمان الأمن والسلامة والشفافية في سلاسل التوريد الخاصة بهم .
- الفصل السابع يبني على تحليل الفجوات هذا، ويحدد التوصيات المقترحة للتدخلات المتعددة الأطراف والإقليمية والوطنية لتعزيز أمن وسلامة سلسلة التوريد في سياق تحديات تكنولوجيا المعلومات والاتصالات (ICT).

نظرًا إلى الطبيعة الفنية لموضوع هذا التقرير, تتضمن وثيقة منفصلة ملحقة بهذا التقرير بعنوان «الخلاصة الفنية» معلومات داعمة إضافية مقدمة ضمن ثمانية ملاحق فنية, وتغطي معلومات مثل:

- التعريفات الموحدة للمصطلحات الرئيسية المتعلقة بأمن وسلامة سلسلة التوريد (ICT) (ا الملحق).
- حالات مختارة للهجمات الواقعة على سلسلة التوريد (الملحق II).
- أطر التقييس الفني التي تعالج قضية أمن وسلامة سلسلة التوريد في سياق مخاطر وتهديدات تكنولوجيا المعلومات والاتصالات (ICT) (والملحق III الملحق IV).
- نبذة عامة حول المبادئ الإرشادية الحكومية والمتعلقة بالصناعة وأفضل الممارسات غير القياسية لإدارة مخاطر تكنولوجيا المعلومات والاتصالات (ICT) المتعلقة بأمن سلاسل التوريد (الملحق V).
- حالات مختارة لإدارة مخاطر سلسلة التوريد (SCRM) في الشركات, وأطر ضمان الأمن (الملحق VI).
- أدوات التقييم الذاتي والتدقيق لإدارة مخاطر سلسلة التوريد الإلكترونية (الملحق VII).
- ملخص مبادرات تطوير المعايير الدولية ومبادرات أصحاب المصلحة المتعددين في هذا الشأن والتي تعالج أمن وسلامة سلاسل التوريد فيما يتعلق بمخاطر تكنولوجيا المعلومات والاتصالات (ICT) (الملحق VIII).

اتجاهات التكنولوجيا عبر سلاسل التوريد العالمية

1.2 سلاسل التوريد في عصر التحوُّل الرقمي

تؤدي تكنولوجيا المعلومات والاتصالات (ICT) – أو التكنولوجيات الرقمية – دورًا مهيمنًا بشكل متزايد في تنظيم وتشغيل سلاسل التوريد العالمية، وكذلك المحلية للمؤسسات التجارية والمنظمات الحكومية. لذا، فإنّ أمن وسلامة سلسلة التوريد من حيث منتجات وخدمات تكنولوجيا المعلومات والاتصالات (ICT) يعد أمرًا مهمًا عبر القطاعات المتعددة؛ والسبب هو أنّ التحوُّل الرقمي العالمي للصناعات وقطاعات الاقتصاد، الذي يجعل مكون تكنولوجيا المعلومات والاتصالات (ICT) منتشرًا في كل مكان وعبر القطاعات، يستحدث أيضًا التحوُّل العالمي في إدارة أمن سلسلة التوريد والعلاقات بين الموردين والمُشتَرين. وعلى الرغم من أنّ سلاسل التوريد لمكونات تكنولوجيا المعلومات والاتصالات (ICT) نفسها (مثل سلاسل التوريد للبرامج ومكونات الأجهزة ذات الصلة منتجات وخدمات تكنولوجيا المعلومات والاتصالات (ICT) تقع في مقدمة التطورات التكنولوجية، إلّا أنّ تحديات تكنولوجيا المعلومات والاتصالات التي تمس أمن وسلامة سلسلة التوريد تمتد في الوقت الحاضر إلى ما هو أبعد من قطاع تكنولوجيا المعلومات والاتصالات (ICT)، وهي متقاطعة بطبيعتها.

الاعتماد العالمي المتزايد لسلاسل التوريد على تكنولوجيا المعلومات والاتصالات (ICT) له العديد من «الأسماء التجارية». وتصفُها منظمة التجارة العالمية بـ «سلسلة التوريد 4.0»: وهي إعادة تنظيم سلاسل التوريد (من حيث التصميم والتخطيط والإنتاج والتوزيع والاستهلاك واللوجستيات العكسية) باستخدام التكنولوجيات المعروفة بـ «الصناعة 4.0»[10]. هذا الاتجاه العالمي الذي نشأ الآن نشأ بين الشركات التجارية الكبيرة في قطاعات التكنولوجيا للدول ذات الدخل المرتفع في محاولة لتحسين كفاءة إدارة سلسلة التوريد من خلال استخدام التكنولوجيات الرقمية المبتكرة (مثل الحوسبة السحابية، والذكاء الاصطناعي، وتقنية دفتر الحسابات الموزع).

10 البنك الدولي و WTO (2019).

إضافة إلى ذلك، يُتوقع مع ظهور تقنية الجيل الخامس، وإنترنت الأشياء، وإنترنت الأشياء في الصناعة، وكذلك رقمنة «الصناعات العمودية»، زيادة تغلغُل تكنولوجيا المعلومات والاتصالات (ICT) في صميم الأعمال والعمليات التكنولوجية عبر القطاعات المتعددة، مما يزيد من الاعتماد على تكنولوجيا المعلومات والاتصالات (ICT) عبر كل تلك القطاعات. وكما ذكر مايكل سبنس، الحائز على جائزة نوبل في الاقتصاد: «ثمة رسالة واضحة مفادها أنّه عندما يصبح الاقتصاد مبنيًا بشكل جزئي على أساسات رقمية، فلا يمكن فصل التجارة، [سلاسل القيمة العالمية] والتكنولوجيا الرقمية والتعامل معها على أنّها اتجاهات وقوى منفصلة»[11].

تم تقديم إحدى الأفكار المدروسة حول هذا التحوُّل من وزارة الاقتصاد والتجارة والصناعة في اليابان، ضمن مسودة إطار الأمن الإلكتروني/المادي، الصادرة عام 2017[12]. وتؤكد الوثيقة على زيادة التقارب والتلاقي بين الفضاء الإلكتروني والمجال المادي ضمن التكنولوجيات الرقمية، بما في ذلك الأنظمة الإلكترونية – المادية والواجهات، والتحوُّل المصاحب لطبيعة العلاقات والتفاعلات بين المورد – العميل.

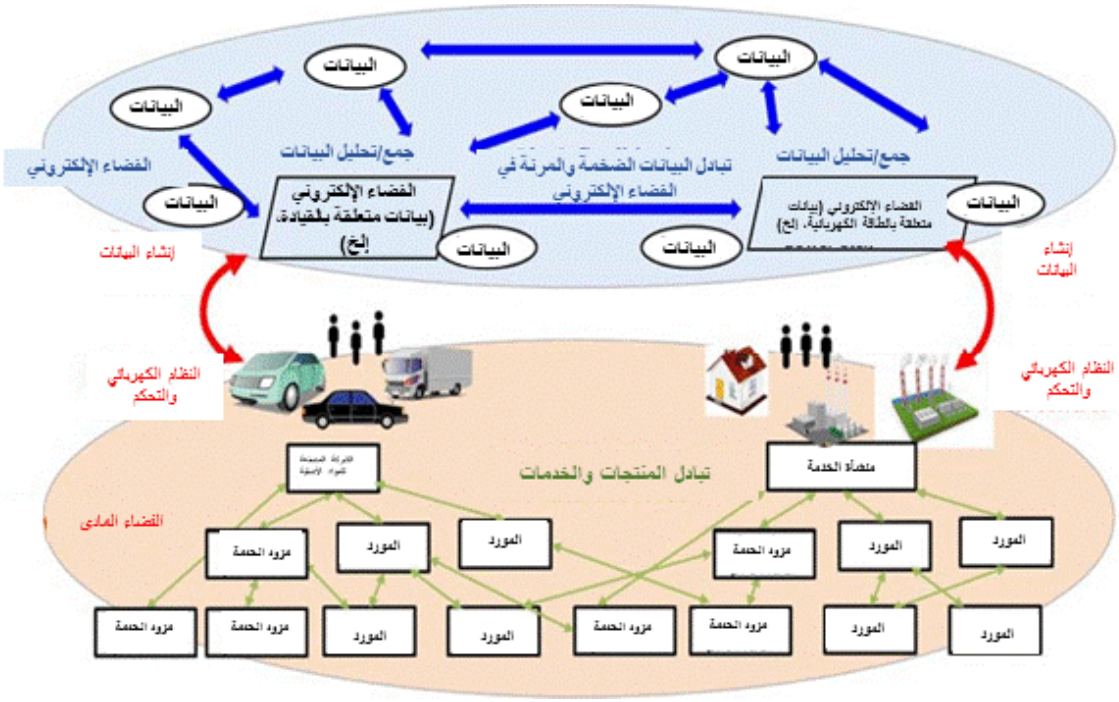
وعلى النقيض من نموذج سلسلة التوريد الخطية التقليدية، ومع ظهور التكنولوجيات الرقمية والعمليات التجارية القائمة على تكنولوجيا المعلومات والاتصالات (ICT) عبر الصناعات والقطاعات المختلفة، فقد نشأ هيكل ومنطق جديدان فيما يتعلق بسلسلة التوريد العالمية. يعتمد هذا النموذج الجديد لسلسلة التوريد (والذي إلى جانب الإشارة إليه بـ «سلسلة التوريد 4.0»، تم وصفه بـ «سلسلة توريد المجتمع 5.0»[13]) على الخصائص التالية:

- **التقارب والتكامل الكبيرين بين العمليات غير المتصلة بالإنترنت والعمليات عبر الإنترنت على طول دورة حياة سلسلة التوريد:** أصبحت التكنولوجيات الرقمية متأصلة ولا يمكن الاستغناء عنها في سلسلة التوريد ذاتها ولإدارتها، بما في ذلك المراقبة المستمرة لسلامة سلسلة التوريد والمخاطر لجميع العمليات التي تعتمد على البيانات
- **سلسلة التوريد حسب الطلب:** يتم توفير العناصر والخدمات للأشخاص الذين يحتاجونها في الوقت المناسب؛ حيث أصبحت عمليات سلسلة التوريد تعتمد على العميل بشكل متزايد.
- **المرونة:** نقطة البداية لسلسلة الأنشطة التي تتم بهدف إضفاء قيمة مضافة لا تكون ثابتة
- **الإدارة وصناعة القرارات القائمة على البيانات:** قد تختلف العمليات والأنشطة لسلسلة التوريد خلال دورة حياة السلسلة إذا تم تحديد حلول أو منهجيات أو طلبات جديدة خلال عملية تحليل البيانات الرقمية المُجمعة
- **تفكيك التسلسل الهرمي:** أدى دمج التكنولوجيات والبنى التحتية التشغيلية والمتعلقة بالمعلومات، وزيادة مرونة العلاقات في السوق واعتمادها على العميل، فضلًا عن زيادة المعرفة القائمة على البيانات لدى المدراء، إلى إمكانية الاستغناء عن الهرم التسلسلي الجامد والمُصمت لاتخاذ القرارات ذات الصلة بإدارة سلسلة التوريد والعلاقات مع البائعين والعملاء. وعلى عكس النموذج الخطي الذي تتدفق فيه التعليمات على طول السلسلة وبالعكس، أي عبر «المورد – المُنتِج – المُوزع – المستهلك» ثم بالعكس، قدمت سلسلة التوريد 4.0 نموذجًا متكاملًا تتدفق فيه المعلومات في اتجاهات متعددة[14].

11 البنك الدولي و WTO (2019).
12 METI (2019a).
13 انظر: METI (2019a).
14 انظر: METI (2019a, 2–4).

يوضح الشكل 4.0 نبذة عامة تخطيطية حول سلسلة التوريد 4.0 الجديدة هذه, والصلات بين الموردين المتعددين والجهات الأخرى التي تعتمد على سلسلة التوريد وتدفقات البيانات الرقمية.

الشكل 1.2 – الصلات بين الموردين, والجهات الأخرى, وتدفقات البيانات الرقمية في سلسلة التوريد 4.0



الرمز OEM = المصنع الأصلي للمعدات, المصدر METI (2019a,2).

2.2 خصائص سلسلة التوريد 4.0

يكتسب ظهور سلسلة التوريد 4.0 – أو سلسلة توريد المجتمع 5.0 – زخمًا كبيرًا عبر مختلف القطاعات والسلطات والأقاليم. ووفقًا لدراسات السوق التي تغطي الشركات عبر الأقاليم والقطاعات, حققت 33% من الشركات بالفعل مستويات عالية من الرقمنة في إدارة سلسلة التوريد الخاصة بها, كما يُتوقع لهذه النسبة أن تزيد لتصل إلى 72% بحلول 2021[15].

وفي هذا السياق, يمكن ملاحظة اتجاهات عالية المستوى وعبر القطاعات, والتي قد يكون لها تأثيرات مثيرة للجدل فيما يتعلق بأمن سلسلة التوريد, ومرونتها وشفافيتها, وكذلك إدارة مخاطرها (SCRM):

- زيادة التعقيد والعولمة
- زيادة الاعتماد المُتبادل وعبر الحدود
- زيادة الإدارة الرقمية لسلاسل التوريد
- توسيع نطاق التأثيرات الأمنية

وقد تمت مناقشة هذه الاتجاهات بإيجاز فيما يلي:

1.2.2 هيكل التقرير

أصبحت سلاسل التوريد التي تحتوي على مُكوِّن رئيسي لتكنولوجيا المعلومات والاتصالات(ICT) أكثر عَولمة وتعقيدًا. وفي حين أشارت العديد من الدراسات والتقارير إلى هذا الاتجاه[16], إلّا أنّه يتضح بشكل أفضل من خلال حجم سلاسل : التوريد الخاصة بشركات التكنولوجيا الكبرى وتعقيدها الهيكلي :

- تشمل قائمة موردي شركة أبل لعام 2018 حوالي 200 مورد من أكثر من اثني عشر ولاية قضائية, وهي ليست قائمة شاملة.[17]
- تعمل سلسلة التوريد لشركة سامسونج مع أكثر من 2,000 مورد في جميع أنحاء العالم[18].
- تعمل شركة جوجل مع أكثر من 500 مورد نشط في أكثر من 60 دولة تُوفر الأجهزة للمستهلكين ومراكز البيانات, وكذلك الخدمات لدعم عمليات الشركة[19].
- تضمنت قائمة موردي شركة هواوي, والتي تمثل مجتمعة 90% من نفقات المشتريات للشركة, 1183 بائعًا من دول متعددة اعتبارًا من عام 2018[20].
- اعتبارًا من 2017, تعمل سلسلة التوريد العالمية لشركة آي بي إم مع 13,000 مورد من الدرجة الأولى في أكثر من 100 دولة[21].

15 PwC (2016, 11)
16 ResearchMoz (2019); Khan (2018); البنك الدولي و WTO (2019) .
17 Apple Inc. (2019).
18 Samsung (2019).
19 Google (2018).
20 Huawei (2019).
21 IBM (2017a).

يقدم الشكل 2.2 تمثيلًا مُصورًا للطبيعة المعقدة والعابرة للقارات لسلسلة التوريد التكنولوجية (TSC) العالمية، والمتعلقة في هذه الحالة بشركة هواوي.

الشكل 2.2 – سلسلة التوريد العالمية لشركة هواوي (اعتبارًا من يونيو 2016)

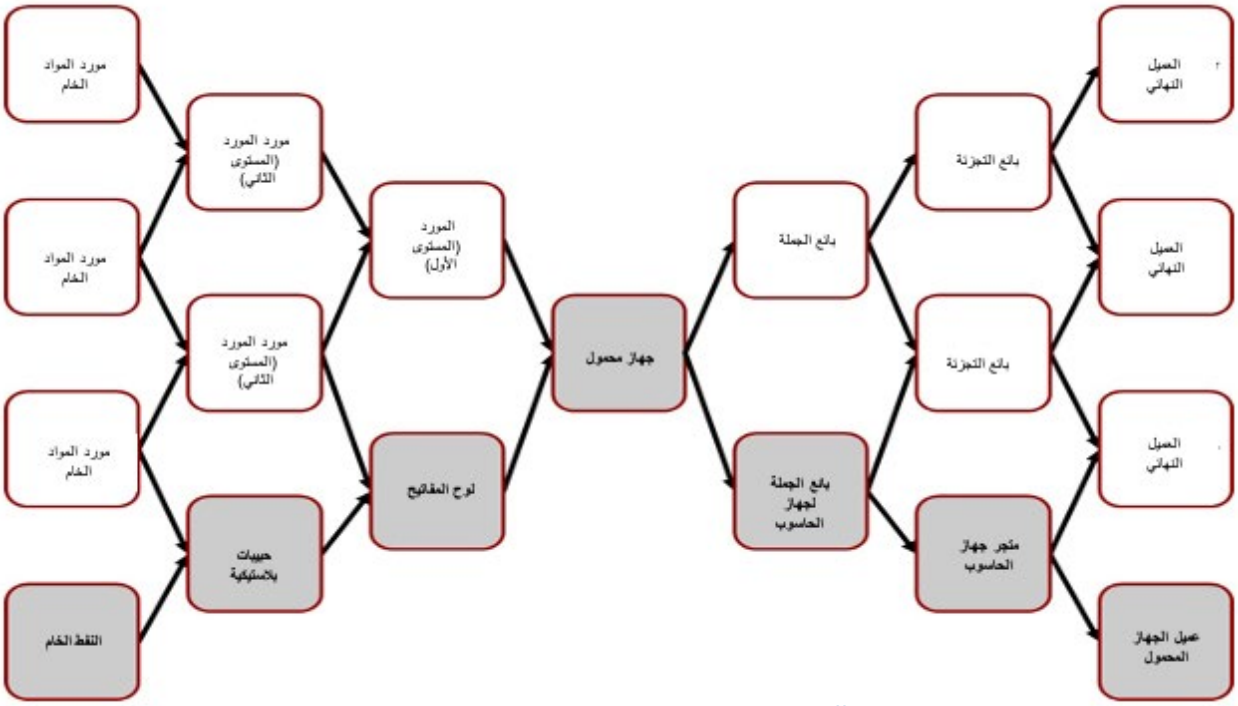
المصدر: Purdy (2016)

بصرف النظر عن النطاق العالمي والتنوع الجغرافي، يساهم العدد الكبير من الموردين أيضًا في التعقيد الهيكلي لسلاسل التوريد في الشركات والمنظمات الحكومية الكبيرة (على سبيل المثال، يُقدر أنّ سلسلة التوريد التابعة لوزارة الدفاع الأمريكية تعمل مع أكثر من 100,000 مورد مباشر والعديد غيرهم من الموردين غير المباشرين)[22]. ويعود هذا التعقيد في المقام الأول إلى الطبيعة المتشابكة لسلاسل التوريد: إذ أنّ الموردين الذي يُوردون المكونات أو المنتجات أو الخدمات للمنظمات لديهم سلاسل التوريد الخاصة بهم، فضلًا عن شبكة الاتصالات وعلاقات الموردين والمشترين مع البائعين الآخرين. ومن وجهة نظر المنظمة، فإنّ مورديها المباشرين هم ما يسمى «بائعو المستوى الأول»، وأولئك الذين يقدمون المنتجات والخدمات إلى «البائعين من المستوى الأول» هم «بائعو المستوى الثاني». بالنسبة إلى الجهات الأكبر، والتي قد تضم آلاف الكيانات في شبكة مورديها، يصبح التتبع الفعال لمكونات سلسلة التوريد أمرًا بالغ الأهمية لإدارة الثغرات الإلكترونية على نحو سريع.

وفيما يلي تمثيل تخطيطي لهذه المنظومة الشبكية في الشكل 3.2.

22 Defense Business Board (2017).

الشكل 3.2 – مفهوم سلسلة التوريد متعددة المستويا



المصدر: Wieland & Wallenburg (2011)

يتمثل أحد المخاوف الرئيسية لدى خبراء الأمن ومنظمي الحكومات في عدم القدرة على تحديد وتتبُّع سلسلة التوريد الكاملة التي تتعدى «بائعي المستوى الأول» بشكل فعال، على الرغم من أنّ الصناعة والمنظمين قد اتخذوا بعض المبادرات لمعالجة هذه القضية بشكل مباشر[23, 24]. على سبيل المثال، ووفقًا للتقرير المعد في 2016 من قبل المعهد الوطني للمعايير والتقنية (NIST) في الولايات المتحدة، فإنّ 72% من الشركات في الولايات المتحدة لم تطّلع بشكل كامل على سلاسل التوريد الخاصة بها، و 50% ليس لديها عمليات لتقييم الأمن الإلكتروني لمزودي المستوى الثالث[25] وبالنسبة إلى مجموعات معينة من الموردين (مثل المتعاقدين مع هيئات الدفاع والأمن الوطنية)، قد تختلف هذه النسب والأرقام نظرًا إلى المتطلبات الإضافية وإجراءات الامتثال التي يفرضها المُشترون[26].

غير أنّ عدم القدرة على الكشف عن سلاسل التوريد الخاصة بالمنظمات ومتابعتها شَكّل تحديًا رئيسيًا لإدارة مخاطر سلسلة التوريد (SCRM) في كلا القطاعيْن، العام والخاص[27]. فعند دخول منتج أو مُكون مشوب أو تم التلاعب به في بداية سلسلة التوريد، يمكنه أن يُعرض سلاسل التوريد لمنظمات العملاء للخطر في أي مستوى. وعليه، يتعين على المنظمة النظر في المخاطر الأمنية عبر جميع مراحل منظومة سلسلة التوريد متعددة المستويات والمعقدة. لهذا السبب، تم إيلاء اهتمام خاص لفرض متطلبات إلزامية على بائعي المستوى الأول تتمثل باستخدام ضمانات الأمان عند التعامل مع مورديهم.

23 مكتب وكيل وزارة الدفاع للاستحواذ والاستدامة، ومكتب نائب مساعد وزير الدفاع للسياسة الصناعية (2018).
23 المكتب البرلماني للعلوم والتكنولوجيا (2017).
25 Weatherford (2018, 24).
26 مكتب وكيل وزارة الدفاع للاستحواذ والاستدامة (2019).
27 اللجنة المشتركة لاستراتيجية الأمن القومي (2018, 33).

2.2.2 الاعتماد المتبادل عبر الحدود

جعلت الرقمنةُ والعولمةُ المستمرة لسلاسل التوريد الجهاتِ الفاعلةَ من الولايات القضائية والأقاليم المختلفة أكثر ارتباطًا واعتمادًا على بعضهم البعض من حيث العلاقات بين المشتري والمورد. ولربما يتضح هذا الاتجاه على نحو أفضل من خلال الممارسة الشائعة للاستعانة بمصادر خارجية لتطوير البرمجيات: فحتى الشركات الصغيرة والمتوسطة (SMEs) عبر العالم تُعيِّن طرفًا ثالثًا من المنظمات أو المبرمجين لتطوير البرامج[28]. وفي في كثير من الحالات، يكون موردو خدمات تطوير البرمجيات من الأطراف الثالثة في ولاية قضائية أو منطقة مختلفة؛ مثل الهند، ومؤخرًا أصبحت دول جنوب شرق آسيا وأمريكا اللاتينية تُعرف كمصانع عالمية لتعهيد البرمجيات لشركات من الولايات المتحدة وغيرها من دول شمال شرق أوراسيا وأوروبا الغربية[29].

وقد أثار اعتماد شركات التكنولوجيا العالمية على الموردين الأجانب في بعض الحالات مخاوف أمنية تتراوح من الأمن الإلكتروني إلى الأمن الوطني. وقد تم تحديد بعض أبرز الأمثلة في هذا الصدد من خلال المراجعات والتقييمات للمخاطر المقترنة بسلاسل التوريد عبر الحدود لقطاع الدفاع. ففي الولايات المتحدة، كشف التقييم الأخير لقاعدة صناعة الدفاع وسلامة سلسلة التوريد عن مستوى مفاجئ من الاعتمادية على الموردين الأجانب، بما في ذلك بعض تكنولوجيات الدفاع الحساسة مثل تصنيع لوحات الدوائر المطبوعة لاحتياجات قطاع الدفاع[30]. وقد شاركت حكومات أخرى مخاوف مماثلة وأجرت التقييمات ذاتها، مما كشف عن التوجُّه نحو اعتبار الاعتماد المتبادل على سلاسل التوريد التكنولوجية عبر الحدود خطرًا استراتيجيًا [31].

3.2.2 الإدارة الرقمية لسلاسل التوريد

سلك التحوُّل الرقمي طريقه إلى إدارة سلسلة التوريد حتى في الأسواق والصناعات التي لا تتضمن سلسلة التوريد للمنظمة فيها مُكونات لتكنولوجيا المعلومات والاتصالات (ICT) مثل البرمجيات والأجهزة. ظهر هذا التخصص الجديد بالكامل لإدارة سلسلة التوريد الرقمية بالإضافة إلى مفهوم «سلسلة التوريد الرقمية» خلال العقد الماضي. كما شهد سوق برمجيات إدارة سلسلة التوريد العالمي نموًا سريعًا، ويُتوقع أن يصل إلى 22.7 مليار دولار أمريكي بحلول 2024[32].

تتضمن هذه القطاعات السوقية، والتي تعتمد على كبرى الشركات في صناعة تكنولوجيا المعلومات (ICT) مثل شركة آي بي إم، وأوراكل، ساب، وفانغارد سوفتوير، مجموعة من الخدمات القائمة على التكنولوجيات الرقمية الناشئة، وتهدف إلى زيادة الكفاءة والمرونة في إدارة سلسلة التوريد[33]. وفيما يلي سرد لتلك الخدمات:

28 Computaris (2016); PwC (2015).
29 Designveloper (2019); BairesDev (2019).
30 مكتب وكيل وزارة الدفاع للاستحواذ والاستدامة، ومكتب نائب مساعد وزير الدفاع للسياسة الصناعية (2018).
31 CISA (2019); EC (2019d).
32 PRNewswire (2018).
33 Bhargava et al. (2019); IBM (2017b); McKinsey & Company (2016); ResearchMoz (2019); SAP (2019).

- الاتصالات المُؤتمتة والرقمية, وتدفق الوثائق والتعامُلات مع الموردين والمُشتَرين بمساعدة المنصات والخدمات الرقمية فيما بين الشركات.
- إدارة سلسلة التوريد ودعم صناعة القرارات بمساعدة التعلم الآلي والتحليلات التنبؤية القائمة على الذكاء الاصطناعي.
- الكشف والمتابعة المتكاملان لسلاسل التوريد للمنظمات –بدءًا من مواقع التصنيع إلى الخدمات اللوجستية وشبكات التوصيل– من خلال تجميع البيانات وتحليلها وعرضها بشكل مرئي.
- الخدمات القائمة على السحابة ومنصات السحابة التي تهدف إلى تمكين الوصول إلى أنظمة إدارة سلسلة التوريد الرقمية للمنظمات الأصغر في ظل محدودية موارد تكنولوجيا المعلومات والاتصالات (ICT) وقد تتضمن مثل هذه الحلول الوصول القائم على السحابة إلى منصات الحوسبة المعرفية القوية, مثل نظام واتسون من شركة آي بي إم.
- إدارة المستودعات والمخزون المؤتمتة كجزء من إدارة الخدمات اللوجستية في سلسلة التوريد: تبدأ التكنولوجيات القابلة للتطبيق من الخدمات القائمة على إنترنت الأشياء التي تُتيح التتّبُّع في الوقت الفعلي وتحليل البيانات للقدرة المستخدمة في المستودعات, وصولًا إلى الطباعة ثلاثية الأبعاد لمعدات المستودعات.
- حلول إدارة المخاطر لسلسلة التوريد للتعامل مع التحديات, بما فيها تلك القائمة على تجميع البيانات الضخمة ومعالجتها وتحليلها.

المفارقة هنا هي أنّه في حين تجلب هذه التطورات التكنولوجية كمًّا هائلًا من الفوائد من خلال تزويد المنظمات بالوسائل الفعالة والقوية لزيادة كفاءة تشغيل سلسلة التوريد الخاصة بها, إلّا أنّها تُولد في نفس الوقت مخاطر جديدة فيما يتعلق بالأمن الإلكتروني للمنظمات.

4.2.2 الآثار الأمنية

يتجلى التأثير التراكمي لهذه التطورات في الانتشار السريع وغير المسبوق لمخاطر الأمن الإلكتروني عبر سلاسل التوريد التكنولوجية (TSCs) العالمية والمشاركين فيها؛ إذ أنّ سطح الهجوم المُوسع[34], ونقاط الدخول الجديدة للجهات الفاعلة الكيدية, وخطر تعطيل العمليات التكنولوجية وعمليات التشغيل, كلها تتأتى للمنظمات كأثر جانبي سلبي لسلسلة التوريد 4.0. وفي حين تُؤكد الشركات التجارية والمنظمات العامة بشكل عام على فوائد منظومة سلسلة التوريد التكنولوجية العالمية (TSCs), إلّا أنّها ليست جميعها قادرة على مواجهة هذه المخاطر وتخفيفها, ولا حتى على عِلمٍ بها. هذا وتم وصف تصنيفات وخصائص التهديدات الإلكترونية التي تنطوي على استخدام سلاسل التوريد التكنولوجية (TSCs) بمزيد من التفصيل في الفصل التالي.

34 Howard et al. (2003); Newman (2017).

1.3 ديناميات هجمات تكنولوجيا المعلومات والاتصالات (ICT) التي تمس سلاسل التوريد

لا بد وأن تؤثر اتجاهات التكنولوجيا التي غيّرت سلاسل التوريد العالمية القائمة على تكنولوجيا المعلومات والاتصالات (ICT) على أمنها وسلامتها، فضلًا عن تأثيرها على مشهد التهديدات والمخاطر العالمية التي تتعرض لها أيضًا، إذ أنّ زيادة تعقيد سلاسل التوريد الرقمية وطبيعة تعدُّد المستويات فيها، بالإضافة إلى عدم وضوح الحدود بين المعلومات وعمليات التشغيل وعلاقات البائعين ذات الصلة، والانتشار السريع لإنترنت الأشياء والأنظمة الإلكترونية المادية، كل ذلك يخلق تحديات جديدة أمام إدارة أمن سلاسل التوريد التكنولوجية (TSCs). والدليل الرئيسي على ذلك هو التزايد الدائم في عدد وحجم الحوادث الأمنية التي تستهدف سلاسل التوريد التكنولوجية، المُبلغ عنها من الشركات الخاصة والوكالات الحكومية وخبراء الأمن الإلكتروني في جميع أنحاء العالم. وقد تضمنت الدراسات التي أجريت في مجال الصناعة، وكذلك التقارير حول الهجمات الإلكترونية على سلسلة التوريد في السنوات الثلاثة الماضية، على سبيل المثال ما يلي.

- أبلغت شركة سيمانتيك عن زيادة بنسبة 78% في هجمات سلسلة التوريد في عام 2018 [35].
- حددت مايكروسوفت في تقريرها الأخير للاستخبارات الأمنية الهجماتِ على برامج سلسلة التوريد باعتبارها أحد عوامل التهديد الرئيسية للصناعة ولأصحاب المصلحة الآخرين، مُشددة على أنّ العدد المتزايد من الهجمات على برامج سلسلة التوريد في السنوات القليلة الماضية أصبح إحدى المخاوف الرئيسية في صناعة التكنولوجيا ومجتمع الأمن[36]. وأخيرًا، أشار التقرير المنشور إلى انتشار هجمات سلسلة التوريد في السحابة باعتباره مصدر قلق خاص، إذ أنّ نطاق أنشطة الجرائم الإلكترونية قد خرج عن البرامج ليطال العمليات والخدمات والبنى التحتية القائمة على السحابة[37].
- أجرَت شركة الأمن الإلكتروني كراود سترايك، والتي مقرها في الولايات المتحدة، مسحًا عالميًا عام 2019، والذي أشار إلى أنّ 66% من المشاركين في المسح قد تعرضوا لشكل من أشكال الهجوم المضاد على سلسلة التوريد في شركاتهم؛ كما أنّ 45% من تلك الحوادث وقعت خلال الاثني عشر شهرًا التي سبقت المسح[38].
- ذُكرت الزيادة المستمرة في عدد الهجمات الإلكترونية على سلسلة التوريد، وانتشار عوامل التهديد هذه، التي يتركز معظمها على برامج سلسلة التوريد، بالإضافة إلى تزايُد وتيرة وتعقيد هذه الهجمات، ضمن اتجاهات التهديدات الإلكترونية الرئيسية وتوقعاتها لعام 2019 من عدد من شركات الأمن الإلكتروني، بما في ذلك شركة تشيك بوينت، وسيسكو وكاسبيرسكي[39].

35 Symantec (2019).
36 Microsoft (2018b).
37 Microsoft (2018b).
38 Bourne (2018); CrowdStrike (2018).
39 Check Point Research (2019); Cisco (2018); Kaspersky (2019).

- عبّرت الوكالات الحكومية أيضًا عن مخاوفها تجاه المخاطر المطردة التي يتعرض لها المستخدمون والمنظمات جرّاء العدد المتزايد من هجمات تكنولوجيا المعلومات والاتصالات (ICT) البارزة التي تمس سلاسل التوريد. ووفقًا لمركز مصادر أمن الحاسوب التابع للمعهد الوطني للمعايير والتقنية (NIST) في الولايات المتحدة، فقد أصبحت الهجمات على برامج سلسلة التوريد «طريقة فاعلة لتجاوُز الدفاعات التقليدية والإضرار بعدد كبير من أجهزة الحاسوب». ففي عام 2017، تم الإبلاغ عن سبعة حوادث بارزة على الأقل، بالمقارنة مع أربعة حوادث مماثلة في الفترة ما بين 2014–2016[40].

- ذكر المعهد الوطني للمعايير والتقنية (NIST) في الولايات المتحدة سببيْن على الأقل للارتفاع المتوقع في الهجمات على برامج سلسلة التوريد:

  – عدم توفر وسائل الحماية الإلكترونية (عبر الإنترنت) المناسبة والخاصة بالعمليات خلال جميع قنوات التطوير والتوزيع لدى بائعي البرمجيات.

  – زيادة الوعي بالأمن الإلكتروني، والنضج وتعزيز وضع الأمن الإلكتروني لشبكات المنظمات، والمُكونات وأجهزة الحاسوب، الأمر الذي جعل ناقلات وأساليب الهجمات الشائعة الأخرى أقل فعالية أو أكثر تكلفة وأصعب من حيث التنفيذ[41]. ويعكس هذا الآراء التي تُشاركها كبرى الشركات الخاصة؛ على سبيل المثال، وبحسب مايكروسوفت، قد تكون موجة الهجمات على برامج سلسلة التوريد التي تستفيد من نقاط الضعف في أدوات تحديث البرامج ناتجة عن حماية أفضل للمنصات الرقمية وأنظمة التشغيل الحديثة، بالإضافة إلى ضعف نواقل العدوى التقليدية مثل الثغرات الموجودة في برامج التصفح[42].

ومنذ عام 2017، حدثت الزيادة العالمية في هجمات تكنولوجيا المعلومات والاتصالات (ICT) الخاصة بسلاسل التوريد في الغالب عبر برامج سلاسل التوريد. هذا وتم وصف بعض الحوادث المهمة من هذا النوع، والتي تم الإبلاغ عنها في السنوات الأخيرة، في الملحق II ضمن وثيقة الخلاصة الفنية.

ثمة عامل آخر يجب أخذه بعين الاعتبار، وهو أنّ بعض أنشطة الجرائم الإلكترونية التي تستهدف سلاسل التوريد قد تكون سرية ولا يتم الكشف عنها لفترة زمنية طويلة. وأحد الأمثلة على أنشطة الجرائم الإلكترونية تلك هي الدّس بوظائف مخفية في المنتجات أو المُكونات عبر سلسلة التوريد، بحيث يمكن تشغيلها عن بُعد في الوقت والطريقة التي تختارها الجهات الفاعلة الكيدية. وتُعد هذه الوظائف التي تُسمى «القنابل المنطقية» أحد أنواع الوظائف المخفية، والتي تُعرَّف بأنّها «جزء (أو أجزاء) من التعليمات البرمجية المُدخلة عمدًا في نظام برمجي، بحيث يقوم بإطلاق وتشغيل وظيفة ضارة في حال استيفاء الشروط المحددة لذلك»[43].

40 US NIST-CSRC (2017).
41 US NIST-CSRC (2017).
42 Microsoft (2018b).
43 US NIST-CSRC (n.d.b).

2.3 طبيعة وتصنيف تهديدات تكنولوجيا المعلومات والاتصالات (ICT) التي تمس سلاسل التوريد

يمكن فهم نطاق التهديدات وطبيعتها، بالإضافة إلى التصنيفات والخصائص الرئيسية لهجمات تكنولوجيا المعلومات والاتصالات (ICT) التي تمس سلسلة التوريد، على نحو أفضل بالرجوع إلى التعريفات الموحدة ونماذج التصنيف المستخدمة من قبل الصناعة والوكالات الحكومية. وتُستخدم التعريفات المُدرجة في الجدول 1.3 لتعريف وتوضيح الهجمات على سلسلة التوريد؛ إلّا أنّها لا تقتصر بالضرورة على هجمات تكنولوجيا المعلومات والاتصالات (ICT) على سلاسل التوريد أو نواقل الهجمات الإلكترونية.

الجدول 1.3 – تعريفات الهجمات على سلسة التوريد

التعريف	المؤلف (الجهة	المصدر
الهجمات التي تسمح للخصم باستخدام الأجهزة المزروعة أو الثغرات الأمنية الأخرى التي تم إدخالها قبل تثبيت البرنامج لاختراق البيانات أو التلاعب بأجهزة أو برمجيات أو أنظمة تشغيل تكنولوجيا المعلومات والاتصالات (ICT) أو الأجهزة الطرفية (منتجات تكنولوجيا المعلومات) أو الخدمات خلال أي وقت عبر دورة الحياة الخاصة بها	لجنة أنظمة الأمن القومي في الولايات المتحدة (CNSS) (الحكومة)	مسرد مصطلحات لجنة أنظمة الأمن القومي في الولايات المتحدة الأمريكية (CNSS) CNSSI 4009-2015
محاولة تخريب عملية إنشاء البضائع وذلك بتخريب الأجهزة، أو البرمجيات أو مُكونات المنتج التجاري قبل التسليم للعميل (خلال التصنيع، أو الطلب، أو التوزيع) بغرض تضمين ثغرة قابلة للاستغلال	منتدى التكنولوجيا الموثوقة للمجموعة المفتوحة (القطاع الخاص/مجتمع التكنولوجيا)	معيار مُزود التكنولوجيا الموثوقة المُصادق عليه من منتدى المجموعة المفتوحة (O-TTPS) الإصدار 1.1 التخفيف من المنتجات المزيفة والملوثة بشكل كيدي، يوليو 2014
إجراء كيدي متعمّد (مثل الإدخال، أو الاستبدال، أو التعديل) يتم اتخاذه لإحداث ثغرة في مُكونات تكنولوجيا المعلومات والاتصالات (ICT) واستغلالها في نهاية الأمر (مثل الأجهزة، البرمجيات، أو البرامج الثابتة) في أي نقطة على طول سلسلة التوريد، بهدف أساسي هو تعطيل أو اختراق المهمة باستخدام الموارد الإلكترونية	معهد ماساتشوستس لبحوث التكنولوجيا والهندسة (MITRE) (القطاع الخاص/ مجتمع التكنولوجيا)	الهجمات على سلسلة التوريد وإجراءات التخفيف ذات الصلة بالمرونة الإلكترونية – دليل لمهندسي أمان النظام، 2017

تقدم التقارير والمبادئ الإرشادية التنظيمية الأخرى تعريفات تركز بشكل أوضح على تكنولوجيا المعلومات والاتصالات (ICT) أو على تصنيفات مخاطر سلسلة التوريد الإلكترونية ونواقل الهجمات. على سبيل المثال، ووفقًا للمعهد الوطني للمعايير والتقنية (NIST) في الولايات المتحدة، فإنّ خطر تكنولوجيا المعلومات والاتصالات الذي يمس سلسلة التوريد هو «حدث ضمن سلسلة التوريد القائمة على تكنولوجيا المعلومات والاتصالات(ICT)، بحيث يهددُ خصمٌ ما سرية أو سلامة أو تَوفُّر النظام أو المعلومات التي يعالجها النظام أو يخزنها أو ينقلها. هذا ويمكن أن يتحقق هذا الخطر أو الضرر في أي مرحلة ضمن دورة حياة تطوير النظام للمنتج أو الخدمة»[44].

وبالاعتماد على التعريفات والتصنيفات الموضحة أعلاه، نقترح تصنيفًا أساسيًا لتهديدات تكنولوجيا المعلومات والاتصالات (ICT) التي تمس سلاسل التوريدات استنادًا إلى المعايير الآتية[45]:

- **هدف الجهة الفاعلة الكيدية:** تهدف هجمات تكنولوجيا المعلومات والاتصالات (ICT) الواقعة على سلسلة التوريد في العادة للوصول غير المُصرح به إلى مُكوّنات أو أنظمة تكنولوجيا المعلومات والاتصالات (ICT) الموثوقة (مثل الأجهزة، البرامج الثابتة، البرمجيات أو العمليات القائمة على تكنولوجيا المعلومات) خلال بعض مراحل دورة حياتها، وذلك قبل أن يتم شحن المنتج أو تأدية الخدمة للعميل النهائي، كما تهدف إلى تعديل هذه المكوِّنات أو الأنظمة إما لاستغلال الثغرات الموجودة أو لزرع ثغرات أو برمجيات خبيثة جديدة[46].ويمكن تحقيق ذلك بعدة طرق. ويقدم معهد ماساتشوستس لبحوث التكنولوجيا والهندسة (MITRE) مثالاً على تصنيف الأساليب المستخدمة من قبل الجهات الفاعلة الكيدية على أساس 41 دراسة حالة للهجمات على سلسلة التوريد[47].

الإدخال: الدّس بمعلومات إضافية، أو رموز برمجية أو وظيفة في إحدى وحدات أو مُكوّنات تكنولوجيا المعلومات والاتصالات (ICT) بحيث يؤدي وظيفة جديدة كيدية أو يُفسد وظائف النظام المقصودة. على سبيل المثال، إضافة رموز برمجية خبيثة إلى مكتبة البرامج. يمكن تطبيق معظم الهجمات من هذا النوع على الأنظمة قيد التنفيذ أو خلال إجراء التحسينات أو التحديثات أو إضافة وظيفة جديدة إلى النظام أو وحداته.

- **الاستبدال:** الاستبدال الكامل لوحدة أو مُكوّن (الأجهزة، أو البرمجيات، أو البرامج الثابتة) ليتم دمجه في نظام مع ذلك الذي تم التلاعب به فعليًا بهدف تغيير وظيفته المقصودة منه في الأصل أو طريقة تشغيله بشكل كيدي وضار.

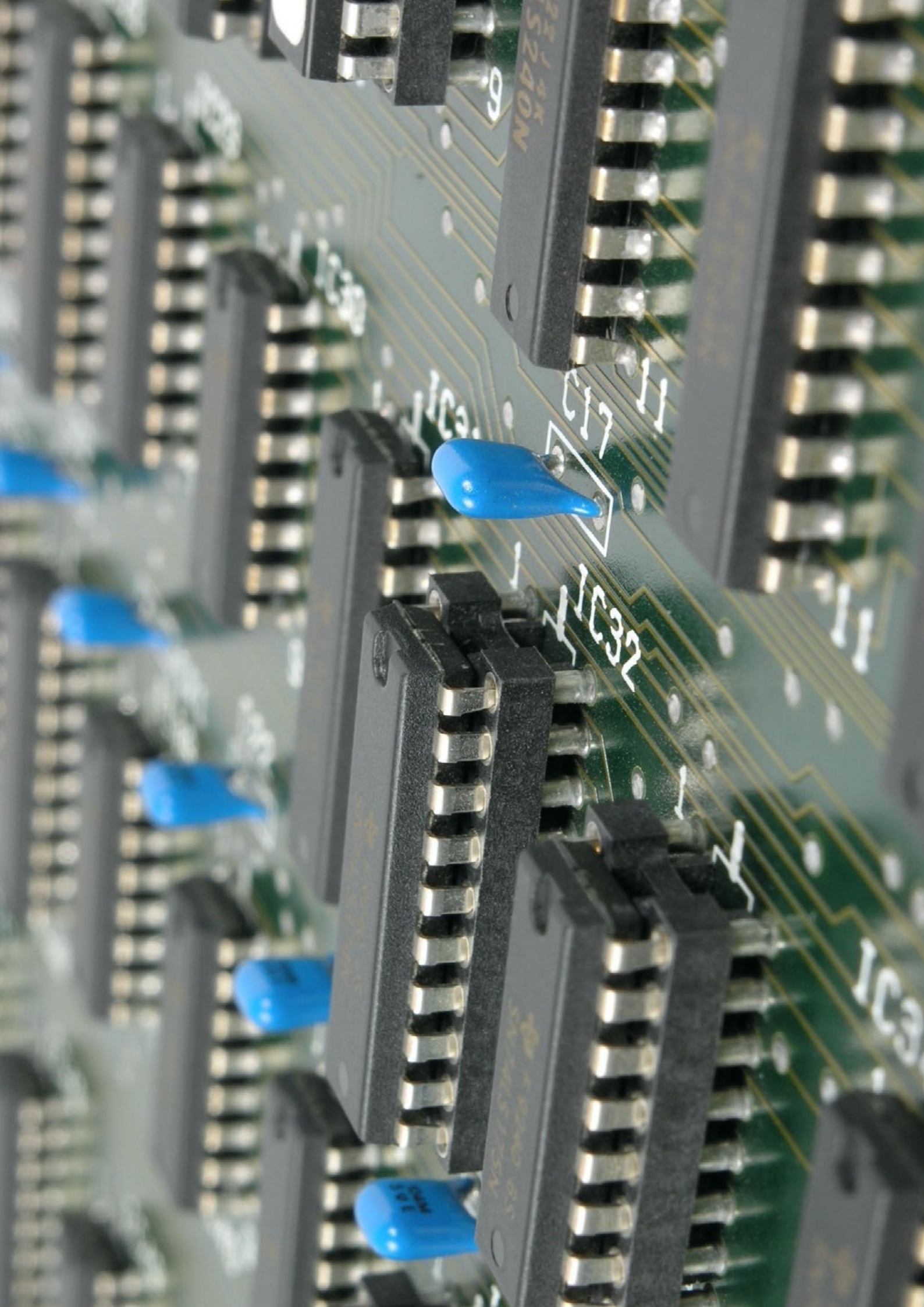
- **التعديل:** أي تغيير على التصميم الحالي أو المعلومات الأخرى التي تُعرّف النظام قيد التنفيذ. في الكثير من الحالات، سيتسبب التغيير في إحداث تدهور أو ضعف في التطويرات التي تُجرَى على النظام أو على الإنتاج.

44 Boyens et al. (2015).
45 Paulsen (2013).
46 انظر أيضًا: Kavanagh (2019).
47 Heinbockel et al. (2017).

- الجزء من سلسلة التوريد للمنظمة والمرحلة من دورة حياة منتجات أو خدمات تكنولوجيا المعلومات والاتصالات (ICT) المستهدفة من قبل الجهة الفاعلة الكيدية: يمكن للمهاجمين الاستفادة من الثغرات داخل كل جزء من سلسلة التوريد تقريبًا، الأمر الذي يزيد الحاجة إلى تقديم ضمانات أمن شاملة ومتكاملة من قبل المنظمات وشبكات البائعين ذات الصلة بسلسلة التوريد تلك.
- نوع أصول تكنولوجيا المعلومات والاتصالات (ICT) التي تستهدفها الهجمات على سلسلة التوريد:
  - البرمجيات.
  - الأجهزة أو البرامج الثابتة.
  - العمليات أو الخدمات القائمة على تكنولوجيا المعلومات والاتصالات (ICT).

- دور البائعين من الطرف الثالث في الحادثة الأمنية التي تؤثر سلسلة التوريد في المنظمة والقائمة على تكنولوجيا المعلومات والاتصالات (ICT): يمكن تمييز طبيعة الجهة الفاعلة التي تقف وراء هجمات سلسلة التوريد القائمة على تكنولوجيا المعلومات والاتصالات (ICT) وفقًا لهذا المعيار المخصص لهذا الغرض. وهناك اثنان من السيناريوهات الممكنة هنا؛
  - أحدث الحوادث المهمة (مثل Floxif, Kingslayer, NotPetya, ShadowHammer: لمزيد من التفصيل، انظر الملحق VI في وثيقة الخلاصة الفنية)، وهي أمثلة على سلاسل التوريد التي تم استهدافها واختراقها من قبل المهاجمين الخارجيين. عندما تمكّنت الجهة الفاعلة الكيدية من استغلال الثغرات الأمنية في سلسلة التوريد للبائع بنجاح، أدّى عدم قدرة البائع على تحديد الحادث والتخفيف منه على الفور إلى انتشار الهجوم إلى شبكة العملاء الخاصة بالبائع، بحيث تم توريد منتجات تكنولوجيا المعلومات والاتصالات (ICT) التي تم العبث بها أو تعديلها.
  - غير أنّ البائعين يمكنهم تأدية دور مختلف في الحالات التي يكونون فيها على دراية بالثغرات الأمنية أو البرمجيات الخبيثة أو الوظائف المخفية ضمن منتجات أو خدمات البرامج أو الأجهزة، ويقومون عن قصد بشحن هذه المنتجات أو تقديم مثل هذه الخدمات إلى مؤسسات تابعة لجهات خارجية. وفي هذه الحالات، يتحول البائعون أنفسهم إلى الجهات الفاعلة الكيدية، ويخترقون أمن سلاسل التوريد القائمة على تكنولوجيا المعلومات والاتصالات (ICT) الخاصة بعملائهم بمنتجات أو خدمات مشوبة وملوثة. وقد تكون هناك صلة وثيقة بين سيناريو البائع الكيدي هذا ومعيار فريق الخبراء الحكوميينGGE لعام 2015، والذي يتناول بشكل خاص الحاجة إلى منع استخدام الوظائف المخفية الضارة في منتجات تكنولوجيا المعلومات والاتصالات (ICT).

لقد تحوّلت هجمات سلاسل التوريد، والتي كانت في السابق وسيلة غريبة وغير مألوفة نسبيًا للهجوم الإلكتروني، إلى وسيلة عامة في صناعة الأمن الإلكتروني – وفي عالم الجريمة الإلكترونية. ويمكن أن يكون تزايد عدد وحجم الحوادث التي تُسببها مثل تلك الهجمات مؤشرًا على أنّه بالرغم من الجهود المبذولة من صناعة التكنولوجيا، إلّا أنّ هناك فجوة بين سرعة وقدرة الجهات الفاعلة الكيدية التي تستهدف بشكل مطرد ومتزايد سلاسل التوريد التي تقوم على تكنولوجيا المعلومات والاتصالات (ICT) وبين الخيارات والاستراتيجيات المتاحة لأولئك الذين يدافعون عن أنفسهم، وعن شركائهم ومستخدميهم ضد مثل هذه الأنشطة الإجرامية.


C17
IC32
IC30
IC31
IC33

1.4 النظام البيئي لاستجابات أصحاب المصلحة

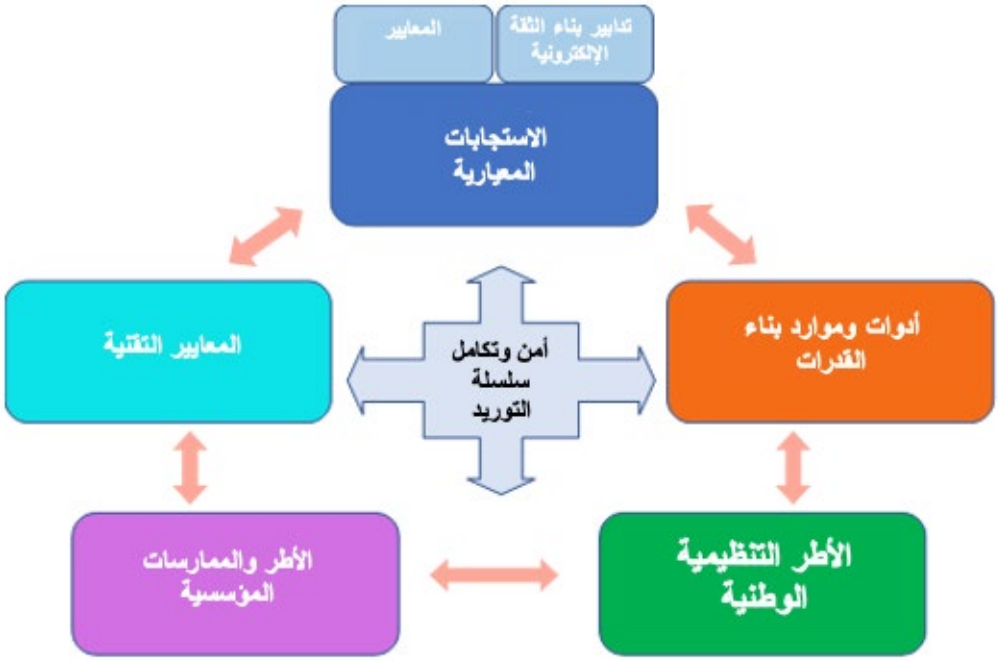
عندما تكون المعايير الدولية قيد التطوير والصياغة أو تكون موجودة بصورة أولية وناشئة، فقد يلجأ أصحاب المصلحة -مثل الجهات الفاعلة في الصناعة ومجتمع التكنولوجيا والحكومات- إما للاعتماد على الأدوات والاستراتيجيات المتاحة لتخفيف التهديدات لسلسلة التوريد الخاصة بهم، أو لتطوير مثل هذه الأدوات بأنفسهم.
وتتسم منظومة الاستجابة لدى الدول والصناعات وأصحاب المصلحة الآخرين بتعدُّد المستويات والتعقيد، مع تَوفُّر العديد من الاستجابات والأطر التي تهدف إلى إحداث تأثير وخلق التزام على مستوى العالم. ويمكن في إطار هذه المنظومة تحديد خمس فئات لمستويات الاستجابة:

- المعايير
- أطر التقييس الفني
- الأطر التشريعية والتنظيمية الوطنية
- إدارة أمن سلسلة التوريد للشركات وسياسات ضمان أمن سلسلة التوريد
- أدوات التقييم (الذاتي)، والمبادئ الإرشادية، وخلاصة أفضل الممارسات وغيرها من أدوات وموارد بناء القدرات

بالإضافة إلى هذه العناصر، هناك أدوات وحوافز أخرى لمختلف أصحاب المصلحة –مثل الحوافز الاقتصادية التي يمكن استخدامها من قبل المنظمين لحثّ الجهات الفاعلة في القطاع الخاص على تغيير سلوكهم والانتقال إلى سياسات أكثر نضجًا وشمولًا لإدارة مخاطر سلاسل التوريد الإلكترونية (cyber–SCRM)(على سبيل المثال، شهادة نموذج نضج الأمن الإلكتروني التي تمنحها وزارة الدفاع في الولايات المتحدة للمتعاقدين في مجال الدفاع.

لا يتم العمل ضمن هذه المنظومة وفقًا لتسلسل هرمي صارم؛ بل يُمكن تصورُّها كمجموعة من العناصر المترابطة والمتآزرة التي تحدث تأثيرًا متبادلًا (انظر الشكل 1.4).

الشكل 1.4 – منظومة عناصر تخفيف المخاطر لسلسلة التوريد



المصدر: CBM(T) (الشفافية و) تدابير بناء الثقة

- تستمد الأطر التنظيمية الوطنية معاييرها من المعايير الدولية المعتمدة على نطاق واسع, كما تُساهم أيضًا في تشكيلها وصياغتها. أحد الأمثلة ذات الصلة بأمن وسلامة سلسلة التوريد هو المعايير المشتركة التي اعتمدتها المنظمة الدولية للتوحيد القياسي (ISO) والتي وُلدت تاريخيًا من ثلاثة معايير وطنية وإقليمية لأمن المعلومات: الكندية والأوروبية والأمريكية [48].
- يمكن تطوير أطر التقييس التي تقودها الصناعة إلى معايير دولية أيضًا, مثل معيار مُزود التكنولوجيا الموثوق المُصادق عليه من منتدى المجموعة المفتوحة (O-TTPS) المعتمد أيضًا من المنظمة الدولية للتوحيد في القياسي (ISO) واللجنة الكهروتقنية الدولية (IEC) في (2015) [49].
- لا تُطور هيئات التقييس الدولية مثل المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهروتقنية (IEC) الدولية المعايير بنفسها, إذ أنّ عمليات تطوير المعايير, بما فيها تلك المتعلقة بأمن وسلامة سلسلة التوريد, يقودها ويُوجهها الخبراء في اللجان الفنية وفِرق العمل لهيئات التقييس. ويأتي معظم هؤلاء الخبراء من الصناعة ومجتمع التكنولوجيا ليتابعوا ويعززوا المنهجيات والرؤى ومبادرات التقييس لمنظماتهم.

48 في وثيقة الخلاصة الفنية المرفقة مع هذا التقرير III للمزيد من التفاصيل: انظر الملحق .
49 في وثيقة الخلاصة الفنية المرفقة مع هذا التقرير III للمزيد من التفاصيل: انظر الملحق .

- وكما يتضح من مبادرات تطوير المعايير لأصحاب المصلحة المتعددين التي تقودها اللجنة العالمية لاستقرار الفضاء الإلكتروني (GCSC)، وشركة مايكروسوفت وسيمنز والجهات الفاعلة في القطاع الخاص، فإنّه يمكن للجهات الفاعلة في مجال الصناعة ومجتمع التكنولوجيا أيضًا الدخول في مجال تطوير المعايير وقيادة المبادرات التي تستهدف أصحاب المصلحة المتعددين، بما في ذلك الدول.

بدأت المعايير في الظهور في مجال أمن وسلامة سلسلة التوريد في وقت متأخر جدًا، وقد اكتسبت حتى الآن نضجًا بدرجة أقل من العناصر والمعايير الأخرى. وهذه عملية طبيعية للعديد من القطاعات ذات الصلة بتكنولوجيا المعلومات والاتصالات (ICT)، ولأمن المعلومات بشكل عام[50]. هذا وسيرد وصف تفصيلي لطبيعة ونطاق التي الاستجابات المعيارية لتحديات تكنولوجيا المعلومات والاتصالات (ICT) تمس سلسلة التوريد في الفصل الخامس من هذا التقرير، كما تُقدم الأقسام التالية في هذا الفصل نبذة حول جميع العناصر الأخرى: التقييس الفني، والسياسات التنظيمية الوطنية، وممارسات الشركات، وبناء القدرات. ويمكن اعتبار هذه العناصر بمثابة ركائز مهمة لتفعيل المعايير الإلكترونية ذات الصلة بأمن سلسلة التوريد.

2.4 التقييس الفني

باستخدام أبسط التعابير والمصطلحات، يمكن أن نصف المعايير التقنية بأنّها اللغة المشتركة التي تُستخدَم للتعبير عن مستويات الأداء المتوقعة للمنتجات والخدمات ووصفها. وفي سياق هذا التقرير، تقع هذه المنتجات والخدمات ضمن تدفق سلسلة التوريد[51]. كما تُعد المعايير والأطر المؤسسية التي تقف وراء مستويات الأداء المتوقعة تلك بمثابة الركائز الأساسية للأنظمة البيئية المعقدة القائمة على التكنولوجيا، وسلسلة التوريد العالمية ليست استثناءً من ذلك، فالنظام البيئي لتقييس سلسلة التوريد معقد وغير متجانس، إذ يضم الأطر الدولية والإقليمية والوطنية، والمعايير ذات الصلة المُعتمدة من الحكومة، فضلًا عن الأطر والمبادرات التي تقودها الصناعة، والتي تم اعتماد بعضها واستخدامها دوليًا أو حتى عالميًا [52].

غير أنّ المعايير التقنية لا تقف معلّقة في الفراغ بلا دعامة، ولا تُحدث تغييرات في الممارسات والعمليات المتعلقة بسلسلة التوريد للمنظمات بنفسها؛ إذ يتم دعم وتعزيز التقييس من خلال الامتثال والاعتماد (إصدار الشهادة) – للممارسات الموجودة التي تتطور في إطار الصلة بين التقييس، والسياسات التنظيمية الوطنية، واللوائح والممارسات الداخلية للشركات.

والسمة الرئيسية التي تخص أمن وسلامة سلسلة التوريد تحديدًا كقطاع تقييس فني هي أنّه تم تطوير هذه المعايير منذ البداية بطريقة مخصصة، وأنّها تتقاطع مع مجالات تقييس أكبر[53]. ويتضمن ذلك :

50 UNGA (1999); UNODA (2019b).
51 Bartol (2011).
52 Davidson (2014).
53 انظر: Bartol (2011)؛ الرئيسان المشاركان للفريق العامل المتخصص JTC/CS1-ICT التابع للمعهد الوطني الأمريكي للتقييس لإدارة مخاطر سلسلة التوريد.

- التقييس الفني لأمن المعلومات ضمن مفهومه الواسع الذي يغطي المبادئ الإرشادية لضمان أمن المعلومات والأمن الإلكتروني للمنظمات والأنظمة والعمليات
- معايير تقييم المخاطر وإدارة المخاطر (مع التركيز على أمن المعلومات وإدارة مخاطر الأمن الإلكتروني وحوكمة المخاطر)
- معايير دورة الحياة للمنتجات والخدمات
- معايير هندسة الأنظمة التي تغطي جوانب مختلفة لأنظمة تكنولوجيا المعلومات (مثل البرمجيات، وتطبيقات الحاسوب وأجهزة ومعدات تكنولوجيا المعلومات)

غير أنّه وعلى مدى السنين، ومع تزايُد تحديات تكنولوجيا المعلومات والاتصالا (ICT) لأمن وسلامة سلسلة التوريد العالمية، شكّل ذلك دفعة لوضع معايير محددة، مما أدى إلى تطوير العديد من أطر التقييس التي تركز بالتحديد على إدارة أمن سلسلة التوريد في سياق تكنولوجيا المعلومات والاتصالات (ICT). وتم تقديم مساهمات كبيرة لهذه العملية من خبراء الصناعة والحكومات عبر إطار عمل المنظمة الدولية للتوحيد القياسي (ISO)، وبالأخص اللجنة الفنية الأولى (تكنولوجيا المعلومات) التابعة لها، واللجنة الفرعية رقم 27 (تقنيات أمن تكنولوجيا المعلومات)، بالإضافة إلى مبادرات التقييس الرئيسية الأخرى، مثل معيار مُزود التكنولوجيا الموثوقة المُصادق عليه من منتدى المجموعة المفتوحة (O-TTPS)، ومعيار المنظمة الدولية للتوحيد القياسي/اللجنة الكهروتقنية الدولية (ISO/IEC 20243) للمزيد من التفاصيل يرجى الرجوع إلى الملحق III في الخلاصة الفنية المرفقة مع هذا التقرير)[54].

وقد تم تقديم لمحة سريعة حول مشهد أطر التقييس الفني التي تعالج قضية أمن وسلامة سلسلة التوريد التكنولوجية TSC في الملحق IV من وثيقة الخلاصة الفنية.

خلاصة القول، يمكن تحديد العديد من التحديات التي تواجه التقييس كعنصر أساسي في النظام البيئي لأمن وسلامة سلسلة التوريد فيما يلي.

- معظم المعايير، حتى تلك التي تركز بشكل محدد على أمن سلسلة التوريد في سياق تكنولوجيا المعلومات والاتصالات (ICT)، ليست أدوات جاهزة يمكن اعتمادها واستخدامها على الفور من قبل المنظمات. فالمبادئ الإرشادية والمتطلبات، ولاسيما التي تخص معايير المنظمة الدولية للتوحيد القياسي (ISO)، هي في الغالب في المستوى الأساسي وعامة بطبيعتها. وذلك أمر حتمي، إذ أنّه لا يمكن لأي معيار دولي أن يشمل ويعكس تفاصيل العمليات التجارية عبر العدد الهائل من القطاعات والصناعات والأسواق والولايات القضائية المعنية في سلسلة التوريد التكنولوجية (TSC). وعليه، يعتمد التطبيق العَملي للمعيار لدى المُورد أو المشتري على إمكانية تكييف المعيار ليتوافق مع العمليات ومجال تخصص الأعمال للمورد أو المشتري – وعلى مدى تحفيز الجهات الفاعلة.
- فيما يتعلق بالتقييس، فإن الأداة الرئيسية التي تساعد على تحقيق الأثر العَملي المُتوخى على ممارسات المنظمات هي الاعتماد (إصدار الشهادة). والتحدي الرئيسي هنا هو أنّه في العديد من أطر التقييس، لا تزال هذه الشهادة غير مفروضة كمتطلب إلزامي من قبل المُشترين، سواء في القطاعات التجارية أو الحكومية. أما في بعض القطاعات ذات اللوائح الحكومية الصارمة، مثل الدفاع والفضاء الجوي، قد يكون الوضع مختلفًا، إلّا أنّ اعتماد الموردين في مثل هذه القطاعات يقوم في الغالب على المعايير والمتطلبات التنظيمية الوطنية الخاصة بالقطاع، ولا تكون بالضرورة متوافقة مع المعايير العالمية.

54 ISO (2019).

- سرعة العمليات تحديًا آخر لكفاءة وفاعلية التقييس الدولي، إذ تستغرق الدورة الكاملة لتطوير واعتماد المعيار في المنظمة الدولية للتوحيد القياسي (ISO) مدة تتراوح بين سنتين وخمس سنوات[55]. وقد لا يكون ذلك سريعًا بما فيه الكفاية، مع اعتبار الديناميات والطبيعة المتغيرة لتهديدات تكنولوجيا المعلومات والاتصالات (ICT) التي تمس أمن وسلامة سلسلة التوريد. ويمكن موازنة ذلك إلى حدٍّ ما بالجهود التي تبذلها أطر تطوير المعايير الأخرى، مثل مشروع شراكة الجيل الثالث (3GPP) [56]، ومشروع ضمان أمن معدات الشبكة (NESAS)[57]، والمكتب الفيدرالي لأمن المعلومات في ألمانيا (German BSI) وهيئات التقييس في الاتحاد الأوروبي اللجنة الأوروبية للتقييس CEN، واللجنة الأوروبية للتقييس الكهروتقني CENELEC والمعهد الأوروبي لمعايير الاتصالات IEC)[58]. إلاّ أنّه يمكن اعتبار الدور الذي تؤديه تلك الأطر وتأثيرها على مشهد التقييس ذي الصلة بأمن وسلامة سلسلة التوريد القائمة على تكنولوجيا المعلومات والاتصالات (ICT) دورًا تكميليًا للأطر التي تم تطويرها من قبل هيئات التقييس الدولية والعالمية، ولا يحل محلها أو يستبدلها.

3.4 السياسات والأطر التنظيمية الوطنية

تشمل النظم البيئية التنظيمية الحكومية التشريعاتِ وأحكام إنفاذ القانون؛ والإجراءات والأنشطة التنظيمية الفنية التي تهدف إلى تكييف المعايير الدولية وتوطينها؛ فضلًا عن متطلبات الجهات الفاعلة المعنية بتفعيل وسلامة وأمن سلسلة التوريد التكنولوجية (TSC)؛ وأطر الامتثال .

هذا وتؤدي الحكومات، إلى جانب كونها جهات مُنظمة، دورًا مهمًا في النظام البيئي لسلسلة التوريد الذي يضم أصحاب المصلحة المتعددين بصفتها «المشتري الأكبر»: وهي الجهة الفاعلة التي تتحكم بحصة كبيرة من النظام البيئي لسوق سلسلة التوريد من جهة المُشتري. ويظهر هذا الدور بشكل خاص في قطاع الدفاع وبعض الصناعات الأخرى مع زيادة مستوى وحجم الأصول المملوكة للدولة والاستحواذ والمشتريات الحكومية على نطاق واسع. ويمكن للوكالات الحكومية في بعض الأحيان استخدام هذا الدور كأداة تأثير على السوق لتحفيز شبكات موردي التكنولوجيا التجارية الخاصة بهم على تَبنّي أفضل الممارسات في مجال إدارة مخاطر سلسلة التوريد (SCRM)، وضمان الأمن والأمن الإلكتروني وذلك لتمكينهم من التنافس بنجاح مع عقود الاستحواذ الحكومية. وكما تُشير بعض الدراسات وخبراء مجتمع التكنولوجيا، يمكن للجهات العامة (الحكومية) الكبيرة التي تعد من بين أكبر المستحوذين في أسواقها الوطنية أن تؤدي دور «النجم القطبي» للبائعين في السوق[59].

غير أنّه يجب استكمال هذا الدور بالتعاون مع القطاع الخاص على نطاق أوسع، من أجل تطوير متطلبات مشتريات مشتركة لمكونات تكنولوجيا المعلومات والاتصالات (ICTs) على سبيل المثال. عطفًا على كل ذلك، فإنّ سلطة الحكومات بصفتها جهات تنظيمية وجهات مشترية رئيسية في سوق التكنولوجيا، تسمح لها بالتصرف بشكل غير مباشر (مثلًا بالضغط على مجموعات الموردين) لتطوير ممارساتهم الموصى بها في الصناعة، وتعزيزها وإصدار الشهادات بشكل ذاتي (بما في ذلك اختبارات منتجاتهم الخاصة ومعالجة العيوب ونقاط الضعف).

55 Bartol (2011).
56 See: 3GPP (2019).
57 GSMA (2019).
58 EC (2019b); EC (2019c).
59 Nissen et al. (2018).

تم عرض أمثلة توضيحية حول الأطر والسياسات التنظيمية الناضجة لإدارة مخاطر سلسلة التوريد الإلكترونية (cyber – SCRM) بالإضافة إلى استعراض السياسات التنظيمية المحلية والجهود الحكومية لمعالجة تحديات تكنولوجيا المعلومات والاتصالات (ICT) التي تواجه سلاسل التوريد في اليابان، والمملكة المتحدة والولايات المتحدة الأمريكية، في الملحق V من وثيقة الخلاصة الفنية المرفقة في هذا التقرير. وإليكم فيما يلي بعض الأمثلة البارزة المختارة:

1.3.4 الولايات المتحدة الأمريكية

- الولايات المتحدة الأمريكية هي إحدى الدول القليلة التي عالجت مخاطر سلاسل التوريد العالمية على مستوى الاستراتيجيات الوطنية، مع التركيز المتزايد على المخاطر القائمة على تكنولوجيا المعلومات والاتصالات (ICT)[60].
- طور المعهد الوطني للمعايير والتقنية (NIST) في الولايات المتحدة الأمريكية إطاره لتحسين الأمن الإلكتروني للبنية التحتية الحرجة (إطار الأمن الإلكتروني للمعهد الوطني للمعايير والتقنية). وقد تم توسيع نسخته ١,١ التي تم إصدارها في 2018[61] نطاق التركيز بشكل كبير ليشمل إدارة مخاطر الأمن الإلكتروني لسلسلة التوريد[62].
- اليوم، يعمل الإطار .الذي تستخدمه 30% من منظمات الولايات المتحدة الأمريكية، إلى جانب منظمات في أكثر من 20 دولة أخرى، كأداة فعلية لمعالجة المخاطر العالمية، إذ يسمح لمستخدميه بتحديد وتخطيط معايير الأمن الإلكتروني، وأفضل الممارسات، والأدوات الأخرى ذات الصلة بنوعها، والقطاع والعملية المحددين، بحيث تُغطي مجال إدارة مخاطر سلسلة التوريد الإلكترونية (C-SCRM)[63].
- كما تم أيضًا تطوير أطر مخصصة لإدارة مخاطر سلسلة التوريد الإلكترونية (C-SCRM). وتم إطلاق برنامج إدارة مخاطر سلسلة التوريد الإلكترونية (C-SCRM). من المعهد الوطني للمعايير والتقنية (NIST) في الولايات المتحدة الأمريكية[64] في 2008 استجابة لمبادرة الأمن الإلكتروني الوطنية الشاملة رقم 11، وهي «تطوير نهج متعدد الجوانب لإدارة مخاطر سلسلة التوريد العالمية»[65]. كما تم مؤخرًا التركيز بشكل خاص على تحديد المتطلبات للتخفيف من مخاطر سلسلة التوريد للأنظمة والوظائف الحساسة والحرجة في وزارة الدفاع الأمريكية[66].

60 US White House (2018).
61 US NIST (2018b).
62 للاطلاع على نبذة مفصلة حول منهجية الأطر، انظر الملحق المرفق مع هذا التقرير، النقطة 1.
63 US NIST (2018a).
64 US NIST (2018c).
65 US White House (2019a).
66 وكيل وزارة الدفاع للاستحواذ والاستدامة (2019)؛ وزارة الدفاع الأمريكية (2018).

2.3.4 الولايات المتحدة الأمريكية

- يقدم مركز حماية البنية التحتية الوطنية (CPNI) والمركز القومي للأمن السيبراني (NCSC) التوجيه فيما يتعلق بمخاطر تكنولوجيا المعلومات والاتصالات (ICT) التي ترتبط بالعلاقات بين المتعاقدين والموردين (مثل مبادئ أمن السحابة، ودارسة التهديدات الداخلية)[67]. هذا وتهدف توصيات المركزين آنفي الذكر إلى مساعدة المنظمات على تأمين أنظمتهم بأنفسهم، بدلًا من ضمان المسؤولية المباشرة والسيطرة الشاملة من الحكومة فيما يتعلق بإدارة مخاطر سلسلة التوريد (SCRM) في القطاعين الخاص وغير الحكومي.
- إنّ معظم الأدوات والموارد التي تُعالج أمن سلسلة التوريد القائمة على تكنولوجيا المعلومات (ICT) والاتصالات في المملكة المتحدة ليست أدوات حكومية أو تنظيمية بحتة، لكنها نتاج شراكات بين القطاعين العام والخاص، على سبيل المثال:
- أداة CyberEssentials[68] وهي مجموعة من الضوابط التقنية لمساعدة المنظمات على حماية أنفسهم ضد التهديدات الأمنية عبر الإنترنت، والتي طورتها حكومة المملكة المتحدة بالتعاون مع القطاع الخاص الشركات الصغيرة والمتوسطة (SMEs)وجمعيات الأمن الإلكتروني.
- مبادرة البرمجيات الموثوقة[69] المدعومة من برنامج الأمن الإلكتروني القومي لحكومة المملكة المتحدة، والذي يهدف إلى المساعدة في تعزيز البرمجيات الموثوقة بين مجتمع العرض والطلب والتعليم في إطار عملية دورة حياة كاملة قائمة على المخاطر.

67 CPNI (2019).
68 NCSC (2019).
69 مؤسسة البرمجيات الموثوقة (2019).

3.3.4 اليابان

- تَشكّل نهج التخفيف من المخاطر المتعلقة بالتحوُّل التكنولوجي لسلسلة التوريد العالمية وقطاع تكنولوجيا المعلومات بأكمله على المستوى الاستراتيجي والمفاهيمي من خلال مشروع إطار الأمن الإلكتروني/المادي الصادر في عام 2019 من وزارة الاقتصاد والتجارة والصناعة[70]. ويُمثل هذا الإطار دعامة الأمن الإلكتروني الرئيسية لبرنامج «الصناعات المترابطة»، الذي أطلقته الحكومة اليابانية لخلق قيمة عبر بناء الروابط والعلاقات بين البيانات الصناعية المتفرقة[71].

قد يكون تحليل المنهجيات الوطنية المُتّبعة بمثابة نقطة انطلاق مفيدة للحكومات الأخرى التي ترغب في تعزيز أطرها التنظيمية، وسيكون من المفيد أيضًا وبشكل خاص تقديم لمحة عامة حول الدول التي ليس لديها أطر استراتيجية سياسية وتنظيمية مفصلة بشكل جيد في هذا المجال. إلّا أنّ اللمحة العامة عن هذه الأطر لجميع الدول الأعضاء في الأمم المتحدة تتعدى نطاق هذا التقرير، ولم يتم تحديد مثل هذه المعلومات الشاملة في المؤلفات المتضمنة فيه.

4.4 الممارسات والأطر في الشركات

تتضمن أنشطة قطاع الشركات مجموعة أدوات شاملة من المتطلبات للبائعين، بالإضافة إلى الإجراءات والمبادئ الإرشادية وأفضل الممارسات المُفصلة والتي تهدف إلى الحد والتخفيف من مخاطر تكنولوجيا المعلومات والاتصالات (ICT) في سلاسل التوريد للشركات. هذا وتركز أطر ضمان أمن سلسلة التوريد التكنولوجية التي طورتها الشركات التجارية والجهات الفاعلة الأخرى في القطاع الخاص على أجزاء مختلفة ضمن النظام البيئي لسلسلة التوريد:

- **ضمان أمن سلسلة التوريد في المستويات الأولية:** يشمل إطار الضمان هذا المستوى الأولَ من البائعين الذين يُوردون المنتجات أو المُكونات أو الخدمات للمنظمة، وللمستويات الأخرى من الموردين.
- **ضمان أمن سلسلة التوريد في المستويات النهائية:** في هذا النموذج، تهدف المنظمة إلى تقديم الضمان لعملائها أو المُشترَين منها، وإلى تطوير إطار سيُمكنها من أن تُثبِت أنّ سلسلة التوريد الخاصة بها لم تتعرض للخطر ولم يتم اختراقها.
- **ضمان أمن وسلامة سلسلة التوريد الشامل أو المتكامل:** تغطي هذه الأطر الأجزاء والمستويات الأولية والنهائية لسلاسل التوريد للشركات على حد سواء. غير أنّ تطوير مثل تلك الأطر وصيانتها بات مهمة صعبة بشكل متزايد، ويتطلب كمًّا هائلًا من الموارد والمهارات من المؤسسات؛ ففي الشركات الكبيرة، يزيد تعقيد ضمان سلسلة التوريد الشامل والمتكامل على نحو يتناسب مع عدد الموردين في المستويات الأولى والمُشتَرين في المستويات النهائية.

70 METI (2019a).
71 METI (2019b).

وتُعد أفضل طريقة لمراجعة وتلخيص الأمثلة المتوفرة حول تلك الممارسات التي نشرتها الصناعة هي النظر إلى الشركات الكبيرة في قطاع التكنولوجيا التي تملك سلاسل توريد ضخمة وعابرة للحدود، بالإضافة إلى عدد كبير من الموردين والعملاء (المستويات الأولى والنهائية من سلاسل التوريد). وكمثال توضيحي، سنعرض في هذا القسم نبذة حول المبادرات التي قامت بها ثلاث شركات تكنولوجية كبرى، إحداها شركة (هواوي) في شرق آسيا، والثانية شركة (مايكروسوفت) في شمال أمريكا، والأخيرة شركة (كاسبرسكي لاب) في شمال أوراسيا. هذا وقد تم تقديم المزيد في الملحق VI من وثيقة الخلاصة الفنية المرفق مع هذا التقرير.

لا تقدم هذه النبذة العامة فهمًا شاملًا لضمان سلسلة التوريد الذي يركز على تكنولوجيا المعلومات والاتصالات وممارسات إدارة المخاطر عبر صناعة التكنولوجيا العالمية، إلّا أنّه، وبالنظر إلى حجم هذه الشركات ومكانتها (ICT) الرائدة في مجالات السوق الخاصة بها، سيتسنى التعرف على بعض الاتجاهات والمنهجيات الرئيسية على الأقل تجاه إدارة مخاطر سلسلة التوريد التكنولوجية (TSC)، بالإضافة إلى تعزيز أمنها وسلامتها وشفافيتها.

هذا وقد أعدّ المعهد الوطني للمعايير والتقنية (NIST) في الولايات المتحدة خلاصة جيدة حول ممارسات القطاع الخاص الأخرى من خلال مشروعه «أفضل ممارسات الصناعة في إدارة مخاطر سلسلة التوريد الإلكترونية الذي يقدم نبذة تفصيلية حول منهجيات إدارة مخاطر سلسلة التوريد التي تتّبعها شركة « (Cyber-SCRM)[72]، سيسكو، وداو دوبونت، وفاير آي، وفوجيتسو، وإنتل، وجونيبر للشبكات، ونورثروب غرومان[73]، وغيرهم من الجهات الفاعلة في الصناعة.

1.4.4 هواوي

طورت هواوي نهجًا شاملًا على مستوى الشركة يشمل ضمان الأمن لمنتجاتها وعملياتها[74]، بالإضافة إلى مُكوناتها ودعائمها الرئيسية:

- **التنسيق وتقسيم المسؤوليات على مستوى الشركة فيما يخص ضمان الأمن**، مع وجود هيئة مركزية لجنة الأمن الإلكتروني العالمي في هواوي– التي تتحمل المسؤولية عن برنامج ضمان الأمن في هواوي، بما في ذلك المصادقة عليه، والتخطيط الاستراتيجي، والسياسات، وخارطة الطريق، والاستثمار والتنفيذ[75]
- **دمج برنامج ضمان الأمن على مستوى جميع العمليات في الشركة**، بما في ذلك البحث والتطوير، وسلسلة التوريد، والمبيعات والتسويق، والتسليم والخدمات الفنية.

72 US NIST-CSRC (2019a).
73 US NIST-CSRC (2019b). انظر أيضًا: US NIST-CSRC (2019a); US NIST-CSRC (2019b); US NIST-CSRC (2019c); US NIST-CSRC (2019d); US NIST-CSRC (2019e); US NIST-CSRC (2019f); US NIST-CSRC (2019g).
74 Suffolk (2013).
75 Suffolk (2013, 11).

- **التركيز بشكل رئيسي على أطر التقييس والاعتماد (إصدار الشهادات) على المستويَيْن الوطني والدولي**، بما في ذلك الامتثال لمعايير التدقيق الداخلي، والحصول على الشهادات الخارجية والتدقيق من السلطات الأمنية ووكالات الطرف الثالث المستقلة (يشمل ذلك استخدام معايير دولية مثل ISO-9001, وISO-14001, وISO-27001, وISO-1540, والامتثال لها)[76].
- **آليات أخرى لمعالجة مخاطر أمن سلسلة التوريد**، بما في ذلك معيار تأهيل نظام الأمن الإلكتروني للمُورِّد الداخلي، استنادًا إلى المعيار ISO-28000[77] ؛ وإطار خط الأساس للأمن الإلكتروني لسلسلة التوريد للشركة، والذي يغطي متطلبات الأمن المادي، وأمن تنفيذ البرمجيات، والعمليات التنظيمية، والوعي الأمني للفرد[78]؛ بالإضافة إلى التتبُّع الشامل للسلسلة ضمن نظام تنفيذ البرمجيات، والقائمة على استخدام مُعرفات الباركود لجميع المنتجات والمُكونات التي تأتي عبر سلسلة التوريد الخاصة بالشركة[79].

بالتوازي مع تطوير آليات ضبط الجودة وإدارة مخاطر سلسلة التوريد، انصبّت الجهود الرئيسية في الشركة منذ أوائل الألفية الثالثة على إنشاء أطر لتوفير ضمانات الأمن على المستويات النهائية، إلى جانب ضمان الثقة في منتجاتها بين المستخدمين، والشركاء، والسلطات الحكومية في أسواق الشركة[80].

2.4.4 مايكروسوفت[81]

يستخدم برنامج تقييم المُوِّردين في مايكروسوفت[82] مزيجًا من آليات تصنيف مخاطر المُورِّدين والتقييمات المبنية على الضوابط، بما في ذلك النظام الذي يشمل مؤشرات المخاطر، وتحديد علامة لكل منها، وتصنيفها وتقديم الإجراءات الموصى بها. ويضم ذلك:

- **السياسات، والمعايير، وإجراءات الضبط والتحكم:** تنطبق هذه الإجراءات على البرمجيات والبضائع والخدمات من موردي الطرف الثالث.
- **نموذج تصنيف مخاطر المُورِّدين:** لقد طورت مايكروسوفت نظامًا من لوحات المعلومات التي تشمل معلومات سريعة حول كل مُورِّد وصحة المنتجات أو الخدمات التي توفرها الشركة.
- **دمج الضمان في دورة حياة المشتريات:** يدمج البرنامج[83] التصعيدات الأمنية ليضمن أنّ مايكروسوفت تختار برمجيات وبضائع وخدمات الطرف الثالث من مُورِّدين موثوقين.

76 انظر: (Purdy 2016): النقطة رقم 10، في وثيقة الخلاصة الفنية الملحقة بهذا التقرير للمزيد من التفاصيل ,III ارجع أيضًا إلى الملحق.
77 ISO (2007a); ISO (2007b).
78 ISO (2007b, 22–23).
79 ISO (2007b).
80 انظر: Huawei Cyber Security Evaluation Centre Oversight Board (2019, part I).
81 في سياق هذا التقرير، يجب تحليل ممارسات شركة مايكروسوفت الداخلية لإدارة أمن سلسلة التوريد بشكل منفصل عن جهود الشركة لإطلاق -أو المساهمة في- مبادرات تطوير المعايير والحلول عبر القطاعات للأمن الإلكتروني. وعلى الرغم من أنّ بعض هذه المبادرات (مثل تعهد حماية الأمن الإلكتروني، واتفاقية جنيف الرقمية) تتناول بشكل مباشر أو غير مباشر أمن وسلامة سلسلة التوريد، إلّا أنّها تختلف عن الممارسات الداخلية ونهج الإدارة المنتشر عبر سلسلة التوريد الخاصة بالشركة.
82 Microsoft (2017).

3.4.4 كاسبرسكي لاب

تم إطلاق مبادرة الشفافية العالمية[84] في 2017 ردًا على الاتهامات الموجهة ضد الشركة بالتجسس الإلكتروني ونشر وظائف مخفية لاستخراج وتصدير البيانات (سرقتها) ضمن منتجات وخدمات الشركة للأمن الإلكتروني القائمة على السحابة التي يتم بيعها للأسواق الغربية, ولا سيما الولايات المتحدة[85] والمملكة المتحدة[86].

- على الرغم من أنّ مبادرة الشفافية العالمية لا تركز بشكل حصري على إدارة مخاطر سلسلة التوريد (SCRM) أو تذكرها بشكل صريح, إلّا أنّها تعمل كأداة فعلية لضمان سلسلة التوريد في المستويات النهائية, مما يُمكّن كاسبرسكي لاب من إثبات عدم وجود أي وظائف مخفية ضمن منتجاتها لعملائها والجهات المنظمة في الأسواق الوطنية.
- تهدف مبادرة الشركة إلى إشراك مجتمع أمن المعلومات الأوسع وأصحاب المصلحة الآخرين في التحقق من صحة ومصداقية منتجاتها, وعملياتها الداخلية والتجارية. هذا وتضمنت الإجراءات والتدابير الرئيسية المنفذة في إطار المبادرة ما يلي[87] :
  - السماح بإجراء مراجعة مستقلة للتعليمات البرمجية المصدرية (الشفرة المصدرية) للشركة, وتحديثات البرامج وقواعد اكتشاف وصد التهديدات من قبل الحكومات والخبراء المُعتمدين عند الطلب.
  - السماح بإجراء مراجعة مستقلة للعمليات ضمن دورة حياة التطوير الآمن للشركة وبرمجياتها واستراتيجيات تخفيف مخاطر سلسلة التوريد الخاصة بها.
  - نشر مراكز الشفافية للشركات التابعة لكاسبرسكي لاب على مستوى العالم لمعالجة أي مخاوف أمنية بالاشتراك مع عملائها وشركائها الموثوقين وأصحاب المصلحة الحكوميين[88].

83 Microsoft (2017); Microsoft (2019).
84 Kaspersky (2019).
85 الكونغرس الأمريكي الـ 115 (2017) مكتب السكرتير الصحفي (2017), DoD, GSA & NASA (2019).
86 Martin (2018).
87 Kaspersky (2019).
88 تم افتتاح أول مركز للشفافية في زيورخ - سويسرا في نوفمبر 2018, ويعمل كمقر لمثل هؤلاء الشركاء لإجراء المراجعات للتعليمات البرمجية (رموز البرامج) الخاصة بالشركة, بالإضافة إلى تحديثات البرامج وقواعد الكشف عن التهديدات, إلى جانب الأنشطة الأخرى. تم إطلاق مركز الشفافية الثاني في مدريد في يونيو 2019, وبحلول أوائل عام 2020, تخطط الشركة لافتتاح مركز الشفافية الثالث في كوالالمبور, لتوسيع مبادرتها إلى منطقة آسيا والمحيط الهادئ.

فيما يلي عرض لبعض النتائج العامة التي تم التوصل إليها من مراجعة أفضل الممارسات للشركات:

- طورت معظم الشركات الرائدة أطرًا داخلية شاملة ومفصلة لمعالجة المخاطر المحتملة الناشئة عن المُورِّدين في المستويات الأولى. وتجمع هذه الأطر بين طرق إدارة المخاطر, وأدوات تقييم البائعين واعتمادهم (إصدار الشهادات), وأنظمة تتبُّع سلسلة التوريد في المستويات الأولى, بالإضافة إلى عناصر أخرى. وفي حين أنّ هذا المستوى من النضج بين كبار الفاعلين في الصناعة هو بالتأكيد اتجاه إيجابي, إلّا أنّه قد يفرض أيضًا بعض التحديات. على سبيل المثال, إذا لم يتم تنسيق المتطلبات عبر الجهات الفاعلة, فسيواجه الموردون زيادة في التكاليف الإدارية الناتجة عن التزامات الامتثال المختلفة. وبالنسبة للشركات الصغيرة والمتوسطة (SMEs) فقد يكون عبء هذا الامتثال أكبر من قدرتها التنظيمية. بعبارة أعم, تحدد هذه الملاحظة الحاجة إلى مزيد من التنسيق والمواءمة بين أطر إدارة مخاطر سلسلة التوريد (SCRM) القائمة على تكنولوجيا المعلومات والاتصالات (ICT) عبر الصناعات المختلفة, ولا سيما في الجزء الأول منها, والذي يضم المجتمع المتناثر من مُوردي التكنولوجيا الذي يشمل حصة كبيرة من الشركات الصغيرة والمتوسطة (SMEs).
- أصبحت إدارة مخاطر سلسلة التوريد والضمان في المستويات النهائية مصدر قلق رئيسي, مع قيام المزيد والمزيد من الحكومات بالنظر في الإجراءات القانونية واتخاذها للتخفيف من المخاطر المحتملة الناجمة عن منتجات تكنولوجيا المعلومات والاتصالات (ICT) التي يتم شحنها إلى أسواقهم الوطنية من مُورِّدي التكنولوجيا العالميين. وفي هذا الصدد, تعمل حتى الشركات الكبرى على تطوير أطر ضمان مخصصة لمعالجة وحل المشكلات الحكومية عبر الأسواق الوطنية (مثل هواوي وكاسبيرسكي لاب).
- قد تستفيد الحكومات وبائعو التكنولوجيا العالميون من نوع من «أطر الأطر» لتقييس نطاق ومنهجية متطلبات (شروط) موردي التكنولوجيا العالميين والمبادئ الداعمة لهم, بهدف تمكينهم من ضمان الأمن عبر الولايات القضائية الوطنية باستخدام منهج موحد .

5.4 أدوات بناء الثقة والموارد والمبادئ الإرشادية وأفضل الممارسات

تم تحديد مفهوم بناء الثقة لأغراض كتابة هذا التقرير على أنّه تطوير الموارد البشرية والمؤسسية وتعزيزها[89]. وغالبًا ما تتم الإشارة مؤخرًا إلى أدوات وموارد بناء الثقة في مناقشات فريق الخبراء الحكوميين (GGE), والفريق العامل مفتوح العضوية (OSWG).

لا يتطلب تطوير القدرات أساسًا معياريًا بحد ذاته, ويمكن تنفيذه من جهات فاعلة متعددة دون أي توافق في الآراء حول المعايير الأساسية الداعمة له. وتتضمن الأمثلة أنشطة بناء القدرات التي تُجريها الجهات الفاعلة في القطاع الخاص بين شبكات مُورِّديهم في إطار جهودهم لضمان الإدارة والحوكمة المسؤولة لسلسلة التوريد.

ثمة العديد من الموارد المفيدة, وأدوات بناء القدرات, إلى جانب خلاصة أفضل الممارسات والمبادئ الإرشادية لمساعدة المؤسسات على فهم مخاطر سلسلة التوريد القائمة على تكنولوجيا المعلومات (ICT) والاتصالات وإدارتها, وفيما يلي بعض الأمثلة ذات الصلة :

89 OECD (2018).

- **أدوات وخدمات التقييم (الذاتي) والتدقيق لإدارة مخاطر سلسلة التوريد الإلكترونية (cyber-SCRM):** تساعد هذه الأدوات المؤسساتِ على التعرف على المتطلبات القانونية والتنظيمية لإدارة مخاطر سلسلة التوريد (SCRM) وضمان أمن سلسلة التوريد, والسعي للتوافق مع المعايير الوطنية والدولية الأساسية, وفهم فعالية ممارسات إدارة مخاطر سلسلة التوريد الإلكترونية (cyber-SCRM) الخاصة بهم بشكل أفضل, بالإضافة إلى تحديد فرص التحسين. وقد تم تطوير سلسلة من هذه الأدوات بمختلف التخصصات من قبل الصناعة, ومجتمع التكنولوجيا والجهات المنظمة لمساعدة المؤسسات على فهم إطار الأمن الإلكتروني للمعهد الوطني للمعايير والتقنية (NIST) في الولايات المتحدة (ارجع إلى الملحق VII من وثيقة الخلاصة الفنية للاطلاع على تفاصيل مجموعة مختارة من هذه الأدوات).

حلول المنصات الرقمية للتعاون الآمن ومشاركة المعلومات بين البائعين: تُمكّن هذه المنصات المؤسساتِ من تقييم وقياس وتخفيف المخاطر في الوقت الفعلي عبر شبكات الشركاء والموردين متعددة المستويات, مع التركيز على مخاطر الأمن الإلكتروني (على سبيل المثال, انظر حل إدارة المخاطر لشركة إكسوستار, المُوضح في الملحق VII في الخلاصة الفنية).

- **الأطر التطوعية لإدارة مخاطر سلسلة التوريد (SCRM) وضمان الأمن:** الأطر والطرق التطوعية التي طورتها الصناعة ومجتمع التكنولوجيا لمساعدة المؤسسات على إدارة مخاطر سلسلة التوريد الخاصة بهم (على سبيل المثال, ارجع إلى إطار سلامة سلسة التوريد للبرامج[90] الذي طوره منتدى ضمان البرامج للتميز في الرموز البرمجية (SAFECode), وهو منظمة عالمية غير ربحية تقودها الصناعة وتعمل على زيادة الثقة في منتجات وخدمات تكنولوجيا المعلومات والاتصالات (ICT) مع التركيز على مجالات رئيسية تشمل تطوير البرامج, وضوابط السلامة وأمن سلسلة التوريد).

- **المنشورات والأدلة والخلاصات البحثية حول أفضل الممارسات في إدارة مخاطر سلسلة التوريد (SCRM) وأمن سلسلة التوريد:** توجد مجموعة واسعة من المنشورات التي ليس لها وضع تشريعي أو تنظيمي, إلّا أنّ القصد منها هو تقديم المشورة والتوصيات لمختلف الجهات الفاعلة حول كيفية تحسين وتعزيز ممارساتهم وتخفيف مخاطر تكنولوجيا المعلومات والاتصالات (ICT) التي تمس سلاسل التوريد بشكل أَفضل. وفيما يلي بعض الأمثلة البارزة في هذا الصدد:

  - **دليل إدارة مخاطر سلسلة التوريد (SCRM) والأمن الإلكتروني لمنتدى التحوُّل الشمال أمريكي[91]:** يهدف هذا المنشور إلى تلخيص أفضل الممارسات لبناء وتنفيذ خطة إدارة مخاطر سلسلة التوريد الإلكترونية (cyber-SCRM).

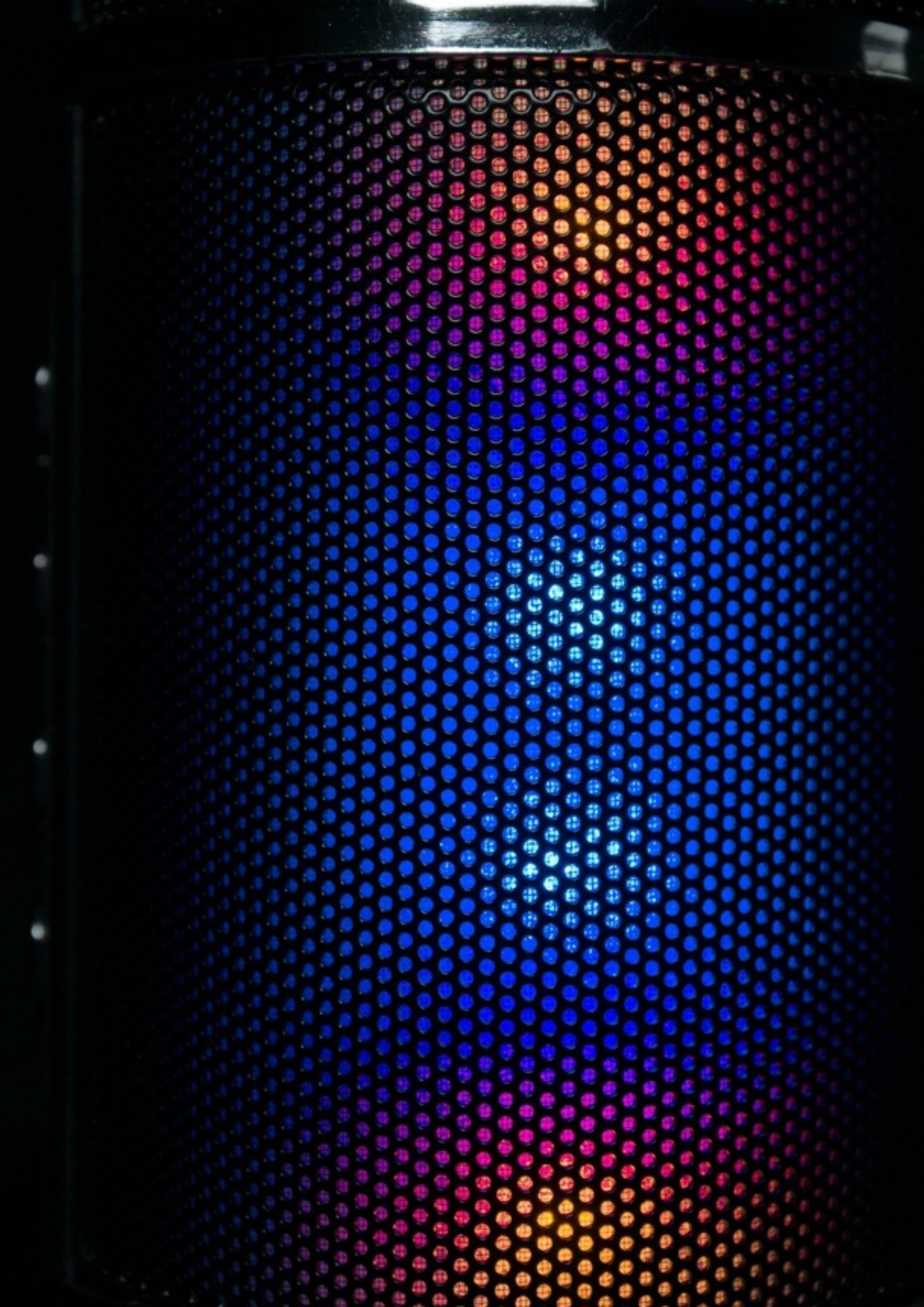
90 SAFECode (2009).
91 NATF (2009).

- **تقرير "Deliver Uncompromised"[92]:** يقدم هذا التقرير الذي أعده معهد ماساتشوستس لبحوث التكنولوجيا والهندسة (MITRE) فكرة متعمقة وتقييمًا للتحديات التي تواجه وزارة الدفاع الأمريكية ومجتمع الاستخبارات فيما يتعلق بضمان سلامة وأمن سلاسل التوريد الإلكتروني الخاصة بهم.
- **مبادرة هيئة التصديق الدولية للمنتجات الإلكترونية[93]:** التي طورها مجلس أمن البنية التحتية الكهربائية، وتهدف إلى تزويد مُشغلي البنية التحتية الكهربائية في الولايات المتحدة بالعمليات الشاملة، والمُوجهة من الصناعة وأصحاب المصلحة الآخرين، للمصادقة على أنّ المنتجات من الأجهزة والبرامج المهمة تم تنظيفها من البرمجيات الخبيثة وغيرها من وسائل الاستغلال العدائية.
- **شراء منتجات وخدمات تكنولوجيا المعلومات والاتصالات (ICT) الآمنة:** الإصدار 1.0 من دليل المُشترين[94]: يهدف هذا الدليل الذي أصدره معهد شرق-غرب، بدعم من عدد من الشركات في قطاع التكنولوجيا، يهدف إلى تقديم خلاصة أفضل الممارسات والمبادئ الإرشادية للمنظمات، وكذلك المستخدمين الأفراد، لمساعدتهم على فهم ومعالجة مخاطر الأمن الإلكتروني والخصوصية المتعلقة بمنتجات وخدمات تكنولوجيا المعلومات والاتصالات (ICT) وسلاسل التوريد الخاصة بهم بشكل أفضل.

تُعد هذه الأدوات والمنشورات، بكل أشكالها المتنوعة، مُكوناتٍ مهمةً للتّبنّي والتعزيز الفعالين لممارسات إدارة المخاطر الإلكترونية لسلسلة التوريد من الجهات الجارية، وكذلك الوكالات الحكومية والجهات التنظيمية. هذا ويمكن تحديد ثلاث فجوات فيما يتعلق بالاتجاهات الحالية لتطوير واستخدام مثل تلك الأدوات والموارد:

- تتناول غالبية هذه المواد والموارد أسواقًا وطنية وأطرًا تنظيمية ومعايير وطنية معينة، وتقودها بشكل مطلق الولايات المتحدة الأمريكية وإطار الأمن الإلكتروني الذي وضعه المعهد الوطني للمعايير والتقنية (NIST). ومهما يكن الأمر إيجابياً بالنسبة لأكبر أسواق التكنولوجيا في العالم، إلّا أنّه يترك معظم الدول الأخرى، لا سيما ذات القدرات المتدنية، معزولة عن أفضل الممارسات والمعرفة والأدوات التي قد تحتاج إليها صناعاتها والجهات المنظمة فيها للتخفيف من مخاطر تكنولوجيا المعلومات والاتصالات (ICT) الواقعة على سلاسل التوريد.
- تركز حصة كبيرة من هذه الأدوات والموارد على قطاعات معينة ذات تنظيم حكومي عالٍ وعمليات ومتطلبات أمنية معقدة (على سبيل المثال، قطاع الدفاع، والمشتريات الفيدرالية). وفي حين أنّ ذلك ليس مفاجئًا على الإطلاق، إلّا أنّه قد يؤدي بشكل متزايد إلى تطور غير منتظم وغير متسق لأطر إدارة مخاطر سلسلة التوريد الإ لكترونية (cyber-SCRM) المُعتمدة عبر القطاعات وربما على المستوى الدولي.
- يلزم التحقق من الكفاءة والفعالية والموثوقية الفعلية والقيمة الإجمالية لمثل هذه الأدوات وتأكيدها، وذلك من خلال التقييمات والاختبارات المستقلة لضمان عدم تحولها بشكل خاطئ إلى بدائل لعمليات أكثر فاعلية لكنها كثيفة الاستخدام للموارد في نفس الوقت.

92 Nissen et al. (2018).
93 Stockton (2018).
94 EastWest Institute (2016).



العنصر الأخير في النظام البيئي للتخفيف من مخاطر سلسلة التوريد هو الاستجابات الدولية، والتي يمكن تصنيفها إلى ثلاثة أنواع، بحسب ما جاء في تقرير فريق الخبراء الحكوميين (GGE) حول الأمن الإلكتروني، وفي الدراسات التي أجراها خبراء المعايير الإلكترونية[95].

- **المعايير:** وفقًا لتعريف البنك الدولي (انظر البند 1.1)، المعايير هي التوقعات أو المعايير المشتركة للسلوك المناسب الذي تقبله الدول والمنظمات الحكومية الدولية (IGOs) والتي يمكن تطبيقها على الدول والمنظمات الحكومية الدولية (IGOs) والجهات الفاعلة غير التابعة للدولة بمختلف أنواعها[96].
- **الشفافية وتدابير بناء الثقة (T)CBMs:** تم تكييف فكرة الشفافية وتدابير بناء الثقة (T)CBMs مع سياق المفاوضات الدولية بشأن أمن تكنولوجيا المعلومات والاتصالات (ICT) من ممارسات منظمة الأمن والتعاون في أوروبا (OSCE)، حيث يتم استخدامها في سياق منع النزاعات. على هذا النحو، لا يوجد لتدابير بناء الثقة (CBM) تعريف مقبول بشكل عام[97]، على الرغم من تصنيفها إلى تدابير بناء الثقة العسكرية وغير العسكرية[98]. ومع ذلك، لا تشير صناعة التكنولوجيا العالمية ولا الجهات المنظمة إلى هذا المفهوم عند مناقشة الممارسات والآليات المُطبقة لمعالجة تحديات تكنولوجيا المعلومات والاتصالات (ICT) التي تمس أمن وسلامة سلسلة التوريد. سيتم طرح هذه المشكلة بمزيد من التفصيل في الفصل السادس (انظر الفجوة السابعة.
- **بناء القدرات:** كما تمت مناقشة ذلك بالفعل في البند 4.5، يُعد بناء القدرات ركيزة منفصلة في النظام البيئي، بالرغم من أنّها مُكملة للاستجابات المعيارية.

1.5 نبذة عامة حول مبادرات تطوير المعايير التي تعالج أمن وسلامة سلسلة التوريد

تنبثق مبادرات تطوير المعايير التي تهدف إلى تعزيز أمن وسلامة سلسلة التوريد، والتخفيف من تهديدات تكنولوجيا المعلومات والاتصالات (ICT) من مختلف العمليات وأصحاب المصلحة.

تجري مناقشات حكومية دولية رئيسية تحت رعاية الأمم المتحدة لمواصلة عمل فِرق الخبراء الحكوميين (GGE) الخمسة في الأمن الإلكتروني. وقد تمت مناقشة قضايا سلسلة التوريد في سياق تهديدات تكنولوجيا المعلومات والاتصالات (ICT) لأول مرة في التقرير الثالث لفريق الخبراء الحكوميين (GGE) في 2013، وهي اليوم واضحة في مناقشات فريق الخبراء الحكوميين (GGE) والفريق العامل مفتوح العضوية (OEWG) على حد سواء.

95 Osula & Rõigas (2018).
96 Martinsson (2011).
97 OSCE (2012, 9).
98 OSCE (2012, 9).

على سبيل المثال، ذكرت اليابان في بيانها المقدم للدورة الموضوعية للفريق العامل المفتوح العضوي (OEWG) التي أُجريت في نيويورك من 3–4 سبتمبر 2019، أنّ أمن سلسلة التوريد أمر حاسم وبالغ الأهمية لتعزيز ثق المستخدم، والترويج للاقتصاد الرقمي، كما اقترحت بعض المعايير المحددة ذات الصلة بأمن سلسلة التوري[99].

أولت المنظمات الإقليمية والتجمعات المتعددة الجنسيات الأخرى أيضًا اهتمامًا بقضايا سلسلة التوريد في سياق أمن تكنولوجيا المعلومات والاتصالات (ICT) والتعاون الدولي، وتشمل الأمثلة على ذلك ما يلي:

- دعت منظمة شنغهاي للتعاون (SCO) الدولَ للسعي إلى ضمان أمن سلسلة التوريد لسِلع وخدمات تكنولوجيا المعلومات والاتصالات (ICT) ضمن نسختها المنقحة لمدونة قواعد السلوك العالمية لأمن المعلومات، بتاريخ 2015[100].
- دعمت مجموعة الدول الصناعية السبعة (G7) مجموعةَ المعايير في تقرير فريق الخبراء الحكوميين (GGE) لعام 2015، وأعلنت التزامها بتنفيذها في بيان دينارد حول مبادرة المعايير الإلكترونية المُتبنّى في 2019[101]، ويتضمن ذلك المعايير ذات الصلة بسلاسل التوريد، على الرغم من عدم ذكرها بشكل صريح في النص. إضافة إلى ذلك، اعتمدت مجموعة الدول الصناعية السبع أيضًا وثيقة العناصر الأساسية لإدارة (G7) المخاطر الإلكترونية للطرف الثالث في القطاع المالي في أكتوبر 2018[102]. ومع أنّ هذا الجهد خاص بالقطاع، ويركز على مفهوم إدارة المخاطر للطرف الثالث، فهو يغطي معظم قضايا إدارة أمن سلسلة التوريد ضمن القطاع المالي.

أخيرًا، ثمة عدد متزايد من مبادرات تطوير المعايير التي تعالج أمن وسلامة سلسلة التوريد في سياق مخاطر تكنولوجيا المعلومات والاتصالات (ICT) تأتي من مبادرات أصحاب المصلحة المتعددين – «رواد تغيير المعايير». وتتضمن مثل تلك المبادرات.

- مبادرة مايكروسوفت، المتمثلة في اتفاقية جنيف الرقمية لحماية الفضاء الإلكتروني، والتي تدعو الدول إلى الامتناع عن إدخال الوظائف المخفية عبر «منافذ تمرير خفية» أو طلب ذلك في المنتجات التجارية الجاهزة[103].
- مبادرة تعهُّد الأمن الإلكتروني، التي أطلقتها أيضًا مايكروسوفت وشركات التكنولوجيا الكبرى، والتي تُعد مؤشرًا على التزام المشاركين فيها بحماية المستخدمين والمنظمات من التلاعب والعبث بالمنتجات والخدمات التقنية[104].

99 UNODA (2019a).
100 UNGA (2015).
101 G7/8 (2019).
102 G7 (2018).
103 Microsoft (2018a).
104 Cybersecurity Tech Accord (2019).

- ميثاق الأمن الإلكتروني، وهو إطار عالمي تقوده الصناعة تم إطلاقه من شركة سيمنز، ويهدف إلى ضمان المسؤولية في جميع أجزاء سلسلة التوريد الرقمية، وتعزيز الاعتماد (إصدار الشهادات) الأمني، كما يضع الحد الأدنى من متطلبات الأمن المُلزمة للموردين[105].
- مقترح حزمة المعايير في سنغافورة الذي أعدته اللجنة العالمية لاستقرار الفضاء الإلكتروني (GCSC) في 2018، والذي تدعو فيه الدولَ والجهات الفاعلة غير التابعة للدولة إلى الامتناع عن العبث والتلاعب بالمنتجات والخدمات أثناء التطوير والإنتاج[106].
- نداء باريس من أجل الثقة والأمن في الفضاء الإلكتروني، الذي أطلقته الحكومة الفرنسية في 2018، بدعم من شركات قطاع التكنولوجيا، والذي ينطوي على التزام بتعزيز أمن العمليات والمنتجات والخدمات الرقمية عبر دورة حياتها وعبر جميع أجزاء سلسلة التوريد[107].
- تم تقديم المزيد من التفاصيل حول هذه الأطر ومبادراتها المعيارية التي تتناول قضية سلاسل التوريد في الملحق VIII من وثيقة الخلاصة الفنية المرفقة مع هذا التقرير.

2.5 التحليل المُقارَن لجهود تطوير معايير سلسلة التوريد

فيما يلي سرد لبعض العوامل الرئيسية التي تم تحديدها لدى مقارنة حجم ونطاق مبادرات تطوير المعايير المذكورة آنفًا:

- في المجمل، عززت ثماني جهات فاعلة عابرة للحدود مبادرات تطوير المعايير الدولية التي تعالج بشكل صريح أمن وسلامة سلاسل التوريد القائمة على تكنولوجيا المعلومات والاتصالات (ICT)، أو التخفيف من المخاطر التي تُشكلها الوظائف المخفية و»منافذ التمرير الخفية» ضمن منتجات تكنولوجيا المعلومات والاتصالات (ICT).
- معظمها (خمسة من أصل ثمانية) عبارة عن أطر معيارية للأمن الإلكتروني لأصحاب المصلحة المتعددين طورتها أو قادتها الجهات الفاعلة في صناعة التكنولوجيا (مايكروسوفت وسيمنز) أو مزيج من مجموعات أصحاب المصلحة، بما في ذلك الدول والجهات الفاعلة في قطاع التكنولوجيا (نداء باريس). ويعكس هذا توجهًا رئيسيًا نحو الصناعة ومجتمع التكنولوجيا للمساهمة بشكل استباقي في الأجندة المعيارية للأمن الإلكتروني في مختلف التخصصات، وأخذ زمام المبادرة لتعزيز وتنفيذ تلك المبادرات.

يبدو أنّ المنظمات الإقليمية هي أقل فئة تمثل الجهات الفاعلة التي تتصدى لتحديات تكنولوجيا المعلومات والاتصالات (ICT) المتعلقة بقضايا أمن سلسلة التوريد وسلامتها من منظور المعايير. فالمنظمة الإقليمية الوحيدة التي تعالج قضية سلاسل التوريد في سياق أمن المعلومات هي منظمة شنغهاي للتعاون (SCO)، ضمن نسختها المنقحة من مدونة قواعد السلوك الدولية لأمن المعلومات.

105 Siemens (2019).
106 GCSC (2018).
107 France Diplomatie (2018).

- معظم المبادرات هي معايير «إيجابية» في أسلوب صياغتها (أي عبارة عن أحكام تُشجع أو تُلزم الدول للقيام بعمل ما)؛ وهناك مبادرتان هما مثال على المعايير «السلبية»، والتي تدعو الدول أو الجهات الفاعلة الأخرى إلى تجنُب أفعال معينة أو الامتناع عنها. ومن الأحكام المعيارية التي يصعب تصنيفها كإيجابية أو سلبية، المعيار المقترح حول ضمان أمن سلسلة التوريد القائمة على تكنولوجيا المعلومات والاتصالات (ICT) ضمن مدونة قواعد السلوك الخاصة بمنظمة شنغهاي للتعاون (SCO).
- يمكن تقسيم المبادرات المقترحة أو المنفذة من الدول ومنتديات أصحاب المصلحة المتعددين على حد سواء إلى أربع فئات بحسب نطاق سلسلة التوريد ذي الصلة بالمخاطر الأمنية، أو أنشطة تخفيف المخاطر التي تتضمنها.
  - **المبادرات التي تهدف إلى التخفيف من الوظائف المخفية[108] الضارة أو منافذ التمرير الخفية[109]:** تركز مثل هذه المعايير بشكل صريح على نوع واحد فقط من الأنشطة الكيدية التي تؤثر على سلسلة التوريد القائمة على تكنولوجيا المعلومات والاتصالات (ICT).
  - **المبادرات التي تهدف إلى تفادي العبث والتلاعب بمنتجات تكنولوجيا المعلومات والاتصالات (ICT):** تُعد فئة المعايير هذه أوسع من تلك المذكورة سابقًا؛ فقد يتضمن العبث والتلاعب تقريبًا في جميع أساليب وطرق الهجوم التي تنطبق على منتجات ومُكونات وخدمات تكنولوجيا المعلومات والاتصالات (ICT) ضمن سلسلة التوريد.
  - **المبادرات التي تهدف إلى ضمان أمن وسلامة سلاسل التوريد القائمة على تكنولوجيا المعلومات والاتصالات (ICT):** يمكن اعتبار هذه الفئة بمثابة تلك التي تغطي وتشمل جميع أنواع الأنشطة ذات الصلة بإدارة مخاطر سلسلة التوريد (SCRM) القائمة على تكنولوجيا المعلومات والاتصالات (ICT)، ولا تقتصر على منع أساليب أو نواقل هجوم معينة أو التخفيف منها.
  - **المبادرات التي تهدف إلى التخفيف من الوظائف المخفية الضارة أو منافذ التمرير الخفية وضمان أمن وسلامة سلاسل التوريد القائمة على تكنولوجيا المعلومات والاتصالات (ICT) على حد سواء:** تعالج هذه الفئة، والتي تتضمن المعايير المستقاة من تقرير فريق الخبراء الحكوميين (GGE) المعد في 2015، قضايا أمن وسلامة سلسلة التوريد القائمة على تكنولوجيا المعلومات والاتصالات (ICT) بطريقة شاملة نسبيًا، مع الإشارة إلى أمن سلسلة التوريد القائمة على تكنولوجيا المعلومات والاتصالات (ICT) بشكل عام وتحديد أولوية المخاطر بالنسبة إليها.
- المبادرة الوحيدة ذات الطابع المُلزم هي ميثاق الأمن الإلكتروني، والذي يتضمن الحد الأدنى من متطلبات الأمن المُلزمة للمُوردين، بالإضافة أحكام الحصول على شهادة إلزامية من طرف ثالث مستقل في حالات البنية التحتية الحيوية وحلول إنترنت الأشياء المهمة.

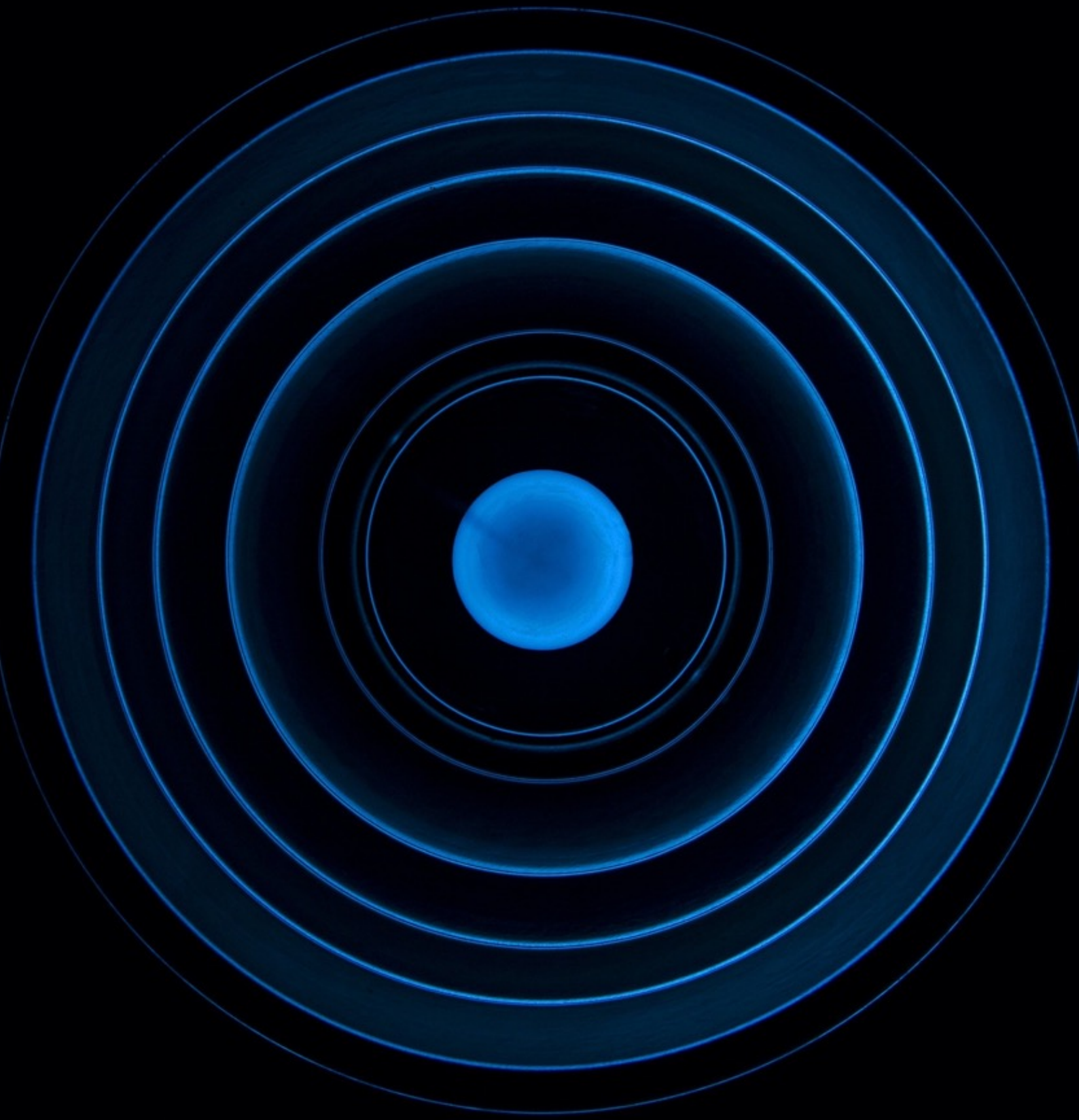
يتوفر تمثيل بياني لهذا التصنيف الأساسي في الجدول 5.1.

108 بالنسبة إلى "الوظائف المخفية الضارة"، لم يتم تحديد تعريف صريح موحد أو مقبول بشكل عام. سياقيًا، يُستخدم هذا المصطلح في وثائق الجمعية العامة للأمم المتحدة، مثل تقارير فِرق الخبراء الحكوميين الإلكترونية والقرارات المتعلقة بالتطورات في مجال المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي كمرادف لـ "منافذ التمرير الخفية".

109 US NIST-CSRC (n.d.a).

الشكل 1.5 – تصنيف مبادرات تطوير المعايير التي تتضمن مخاطر سلسلة التوريد القائمة على تكنولوجيا المعلومات والاتصالات (ICT)

المبادرات أو المعايير	أصحاب المصلحة		المعايير الإيجابية مقابل السلبية		أمن وسلامة			
	المنظمات الحكومية الدولية (IGO)	المتعددين	الإيجابية	السلبية	الوظائف المخفية الضارة (HHF)/منافذ التمرير الخفية	العبث	أمن وسلامة سلسلة التوريد (SC S&I)	أمن وسلامة سلسلة التوريد + الوظائف المخفية الضارة/منافذ التمرير الخفية
فريق الخبراء الحكوميين (GGE)	✓		✓	✓				✓
مجموعة الدول الصناعية السبعة (G7)	✓		✓	✓				✓
منظمة شنغهاي للتعاون (SCO)	✓		✓	✓			✓	
اتفاقية جنيف الرقمية		✓		✓	✓			
تعهد حماية الأمن الإلكتروني		✓		✓		✓		
ميثاق الثقة للأمن الإلكتروني		✓	✓				✓	
اللجنة العالمية لاستقرار الفضاء الإلكتروني		✓		✓		✓		
نداء باريس للثقة والأمن في الفضاء الإلكتروني		✓	✓			✓		



الفجوات في جهود تطوير المعايير لسلسة التوريد

يركز هذا الفصل على الفجوات –أو مواطن التحسين– في المبادرات المعيارية أو في مجموعة الإجراءات التي تدعم تنفيذها.

وفيما يلي سرد للفجوات المستخلصة من مراجعة جهود تطوير المعايير لسلسلة التوريد، والتي ستتم مناقشتها في هذا التقرير:

1. افتقار المعايير «السلبية» إلى آليات المراقبة والتحفيز والتنفيذ.
2. طبيعة التعامُل «المُجزأة» للمبادرات التي تركز على الوظائف المخفية الضارة.
3. تداخل وازدواجية الجهود ضمن مبادرات أصحاب المصلحة المتعددين.
4. عدم وجود أطر عمل موحدة للتعامل مع بائعي التكنولوجيا العالميين في الأسواق الوطنية.
5. عدم التنسيق والتآزر بين المبادرات المعيارية الحكومية الدولية والصناعة العالمية ومجتمع التكنولوجيا.
6. عدم التركيز على معالجة مخاطر تكنولوجيا المعلومات والاتصالات (ICT) لسلسلة التوريد من خلال بناء القدرات.
7. عدم التركيز على استخدام مجموعة أدوات تدابير بناء الثقة (CBM) لمعالجة مخاطر تكنولوجيا المعلومات والاتصالات (ICT) التي تمس سلسلة التوريد.
8. انخفاض مستوى نضج الأطر والمبادرات الوطنية لضمان أمن وسلامة سلاسل التوريد التكنولوجية (TSCs) على المستوى الوطني بشكل عام.

ويرد أدناه وصف موجز لهذه الفجوات؛ كما تمثل تلك الفجوات الأساس للتوصيات الواردة في الفصل السابع.

- تواجه مبادرات تطوير المعايير هذه تحديات نظرًا إلى افتقارها للدوافع والحوافز المناسبة التي تدعو الجهات الفاعلة المستهدفة للامتثال لها. كما أشارت العديد من التقارير إلى أنّه لغرس وتعزيز المعايير العالمية, فلا بد من الالتزام طويل الأمد والتعاون بين مجموعة كبيرة من أصحاب المصلحة المعنيين والمشاركين بفعالية كبيرة[110]. وتعتمد المعايير التي تعالج الوظائف المخفية الضارة, فضلًا عن منافذ التمرير الخفية والعبث بمنتجات وخدمات تكنولوجيا المعلومات والاتصالات (ICT) في سلسلة التوريد التكنولوجية (TSC) من منظور «سلبي» فقط (أي بحظر مثل تلك الأنشطة أو مطالبة الجهات الفاعلة بتجنُّبها أو الامتناع عنها), على التُوقُّع بأنّ الدول والجهات الفاعلة الأخرى ستلتزم طواعية بتلك المعايير وستراقبها. ويتعارض هذا التوقُّع مع ديناميات التهديدات التي تشهدها سلسلة التوريد القائمة على تكنولوجيا المعلومات والاتصالات (ICT). ووفق ما تمت مناقشته آنفًا, تشهد الصناعة والدول زيادة حادة في أنشطة الجرائم الإلكترونية التي تستهدف سلاسل التوريد العالمية.
- لا تزال الفرصة سانحة للمعايير التي تتحدى الممارسات الحالية للنجاح والتمركز في حال كان جدول أعمالها مصحوبًا ومدعومًا بأطر التنفيذ والمراقبة. وبالنسبة إلى سلاسل التوريد, فيمكن رفع مستوى ضمانات الأمن الشاملة وأطر إدارة مخاطر سلسلة التوريد (SCRM) القائمة على تكنولوجيا المعلومات والاتصالات (ICT) لتصل إلى مستوىً عابر للقطاعات وعابر للحدود. غير أنّ المبادرة المعيارية يجب أن تشمل أيضًا ذلك المُكوّن «الإيجابي», وأن تهدف إلى إنشاء مثل تلك الأطر إذا لم تكن موجودة حاليًا. هذا وتعد مبادرات تطوير المعايير التي تجمع بين العناصر السلبية والإيجابية مناسبة أكثر من حيث إمكانية تفعيلها, إذ يمكن للعناصر الإيجابية أن تطلق الآليات اللازمة لتنفيذ المُكوّنات السلبية.
- تكون إمكانية المراقبة الفعالة للمعايير السلبية محدودة نظرًا إلى التحدي المعروف والمتمثل في القدرة على الإسناد الموثوق به للجرائم الإلكترونية. إحدى الأدوات الرئيسية التي يمكن أن تدعم التقيُّد بالمعايير السلبية هي «الحوافز السلبية», مثل أشكال معينة من المسؤولية القانونية أو العقوبات أو أنواع أخرى من الجزاءات المترتبة على انتهاك ومخالفة المعايير والقيام بنشاط ضار.

110 Martinsson (2011).

الفجوة الثانية: طبيعة التعامل «المُجزأة» للمبادرات التي تركز على الوظائف المخفية الضارة

- يمثل الدسُّ بالوظائف المخفية الضارة والبرمجيات ومنافذ التمرير الخفية في الأجهزة تحديًا رئيسيًا وكبيرًا. هذا وتُبيّن التجارب والخبرات عبر الصناعة ومجتمع التكنولوجيا والقطاع العام أنّ معالجة مخاطر تكنولوجيا المعلومات والاتصالات (ICT) التي تمس سلاسل التوريد التكنولوجية (TSCs) يجب أن تتم من خلال إدارة مخاطر سلسلة التوريد الإلكترونية (C-SCRM) الشاملة والمتكاملة، بالإضافة إلى أطر ضمان الأمن الشاملة وبرامج الامتثال أيضًا. ويتضمن ذلك تحديد وتتبُّع مجموعة المخاطر الكاملة وتطوير استراتيجيات لمعالجتها ضمن مجموعة سياسات وممارسات وأدوات شاملة لإدارة مخاطر سلسلة التوريد (SCRM).
- مجموعة سياسات وممارسات وأدوات شاملة لإدارة مخاطر سلسلة التوريد (SCRM). لا تتواءم المعايير التي يقتصر نطاقها فقط على التعامل مع الطرق المخفية لتعطيل الوظائف الإلكترونية مع هذا النوع من النهج الشامل والمتكامل، إذ أنّها تتعامل مع مخاطر الوظائف المخفية بمنأىً عن بقية مخاطر تكنولوجيا المعلومات والاتصالات (ICT) لسلاسل التوريد، وعليه فهي تُقوّض النموذج القائم على نهج إدارة المخاطر الشامل والمتكامل

الفجوة الثالثة: تداخل وازدواجية الجهود ضمن مبادرات أصحاب المصلحة المتعددين

- كما يتضح من مخطط المبادرات المعيارية التي تقودها الصناعة وأصحاب المصلحة المتعددين (انظر الجدول 5.1)، تعالج العديد من هذه المبادرات (مثل تعهّد حماية الأمن الإلكتروني، ومقترح حزمة المعايير من اللجنة العالمية لاستقرار الفضاء الإلكتروني (GCSC)، ونداء باريس) قضايا سلسلة التوريد القائمة على تكنولوجيا المعلومات والاتصالات (ICT) من منظور مماثل، كما تحدد المنهجيات والمعايير المتداخلة. يقترن بذلك عدد كبير من شركات التكنولوجيا الكبيرة، التي تُشكل العمود الفقري لسلاسل التوريد العالمية القائمة على تكنولوجيا المعلومات والاتصالات (ICT)، والمعنية بالعديد من تلك المبادرات بشكل متواز
- في حين أنّ التنوع في الأطر والمبادرات، وحتى التنافس فيما بينها، يعزز أجندة بناء معايير الأمن الإلكتروني العالمية، فقد يؤدي أيضًا إلى تشتت الجهود. ويؤدي هذا الاتجاه على وجه الخصوص إلى خطر وجود أطر إدارة مخاطر سلسلة التوريد (SCRM) المتعددة والمتوازية التي تتنافس على وضع الممارسة المعيارية العالمية في الواقع[111].

111 وقد لوحظت ظواهر مماثلة في بعض قطاعات التقييس الفني للتكنولوجيات الرقمية الناشئة (مثل معايير بروتوكولات الشبكات اللاسلكية للبنى التحتية وخدمات إنترنت الأشياء). أدت المنافسة بين اتحادات التكنولوجيا الرئيسية داخل هيئات التقييس الدولية إلى نشوء نظام بيئي معقد وغير متجانس للغاية يضمن أكوامًا من معايير التقييس في مجال إنترنت الأشياء، ويفتقر إلى قابلية التشغيل البيني ومنهجيات الأمن الشامل.

- وفقًا لما هو موضح في الفصل الرابع، هناك توجّه ناشئ لدى عدد قليل من الحكومات لإنشاء أطر عمل خاصة وواجهات تنظيمية (مراكز تقييم الأمن الإلكتروني، ومراكز الشفافية) باعتبارها «بوابات دخول» إلى الأسواق الوطنية لبائعي التكنولوجيا العالميين. وفي حين أنّ بناء مثل هذه الأطر يمكن أن يبدأ من قبل البائعين استجابة لمتطلبات «الجهات المنظمة» والمخاوف الأمنية، إلّا أنّ الحكومات هي القوى الدافعة التي تقف وراء ذلك.
- فيما يتعلق بالحلول المحتملة الداعمة للمعايير، يكمن التحدي في تفادي الحاجة إلى تطوير مثل هذه الأطر بطريقة مخصصة ومصممة خصيصًا لكل بائع كبير ولكل ولاية قضائية حيث تُمارَس الأعمال. ودون اتّباع نهج معياري (أو مُنسق على الأقل)، قد تكون عملية بناء مثل هذه الأطر عبر الأسواق الوطنية معقدة ومكلفة للغاية، للحكومات والبائعين على حد سواء، فضلًا عن كونها طويلة وبطيئة جدًا ولا تتواءم مع سرعة انتشار تهديدات تكنولوجيا المعلومات والاتصالات (ICT) لسلاسل التوريد العالمية.
- لم تُذكر مثل تلك الأطر بشكل صريح في المبادرات المعيارية وقد لا يتم ربطها بشكل مباشر بأيٍّ منها، إلّا أنّ هذه الممارسة تصبح واسعة الانتشار وسائدة بشكل تدريجي، كما أنّها تدفع طريقة العمل لضمان أمن سلسلة التوريد نحو التعاون بين القطاعين العام والخاص – كأحد أشكال نهج أصحاب المصلحة المتعددين. وعلى عكس المنطق الشائع للعمل من الأعلى إلى الأسفل، حيث تُشكل المعايير الأساسَ المفاهيميَّ لإطار التنفيذ والآليات العَملية الخاصة بها، فقد يتم تعزيز بناء هذا النوع الجديد من أطر العمل لتكون هي الحالة المعيارية، وذلك من خلال نهج العمل من الأسفل للأعلى – باعتباره الحل المشترك الأفضل الذي يُمكّن الجهات المنظمة الوطنية من التعامل مع مخاطر تكنولوجيا المعلومات والاتصالات (ICT) القادمة من موردي التكنولوجيا الأجانب.

- ظهرت المبادرات الحكومية الدولية التي تتعامل مع أمن وسلامة سلسلة التوريد التكنولوجية (TSCs) من خلال تطوير المعايير بعد ممارسات الصناعة والجهود المجتمعية بوقت طويل جدًا (بما في ذلك أطر التقييس والاعتماد «إصدار الشهادات»). وعليه، لم يُشَر إلى مفاهيم أساسية مثل إدارة مخاطر سلسلة التوريد (SCRM) الشاملة وضمان الأمن على طول سلاسل التوريد التكنولوجية (TSCs)، فضلًا عن تعزيز المعايير الدولية ذات الصلة، في تقارير فريق الخبراء الحكوميين (GGE) أو مدونة قواعد السلوك المقترحة من قبل منظمة شنغهاي للتعاون (SCO) عام 2015. في المقابل، يبدو أن نطاق وصياغة المعايير المقترحة في أطر أصحاب المصلحة المتعددين بالمشاركة مع الدول (مثل نداء باريس) يتشكّلان وفقًا لوجهات نظر ونُهُج الصناعة ومجتمع التكنولوجيا وبشكل يراعيها.
- تعكس هذه الفجوة أيضًا العمليات المستخدمة لتطوير المعايير الحكومية الدولية. على سبيل المثال، يعمل فريق الخبراء الحكوميين (GGE)، بحكم تصميمه، وفق أسلوب المشاركة المختارة بحسب الاقتضاء، ولن يقوم بإشراك مجموعة أوسع من أصحاب المصلحة المتعددين خلال اجتماعاته الرسمية. وقد خدم هذا التنسيق أغراضه المنشودة لسنوات عدة، بتهيئة الظروف اللازمة لتحقيق التوافق في الآراء (الذي يصعب الوصول إليه) حول معايير الأمن الإلكتروني في 2013 و 2015. وبينما ينبغي معالجة هذا الافتقار إلى الشمولية جزئيًا على الأقل من خلال الفريق العامل مفتوح العضوية (OEWG)، فإنّ دورته الموضوعية الأولى في سبتمبر 2019[122] لم ينتج عنها مشاركة قوية من الجهات الفاعلة في الصناعة أو مجتمع التكنولوجيا.
- العامل الأخير الذي يساهم في هذه الفجوة هو طرائق العمليات المختلفة للمبادرات والأنشطة الحكومية الدولية التي يقوم بها مجتمع التكنولوجيا والصناعة، ففي حين يُمنَح كلٌّ من فريق الخبراء الحكوميين (GGE) والفريق العامل مفتوح العضوية (OEWG) تفويضات محددة بزمن للتفاوض (والتوصل بشكل مثالي إلى توافق في الآراء بشأن) قضايا محددة في عدد محدود من الجلسات، فإنّ المبادرات في مجتمع التكنولوجيا والصناعة تعتمد على عملية أكثر استمراراً وتتطلب المشاركة والإدارة والحوكمة بشكل دائم (على سبيل المثال، تعهد حماية الأمن الإلكتروني، ميثاق الثقة للأمن الإلكتروني).

112 UN Web TV (2019).

الفجوة السادسة: عدم التركيز على معالجة مخاطر تكنولوجيا المعلومات والاتصالات (ICT) لسلسلة التوريد من خلال بناء القدرات

- باعتبار أنّ النظام البيئي لموردي التكنولوجيا مشتت حول العالم، وأنّ العديد من الموردين يتواجدون في ولايات قضائية تفتقر إلى السياسات التنظيمية وأطر التقييس الناضجة، يمكن لجهود بناء القدرات الدولية أن تُحسن بشكل كبير من بيئة المخاطر ككل في سلاسل التوريد العالمية. إلّا أنّه لا يوجد إطار لتطوير المعايير يتعامل مع إدارة مخاطر سلسلة التوريد (SCRM) القائمة على تكنولوجيا المعلومات والاتصالات (ICT) كبند منفصل وذو أولوية ضمن أجندة بناء القدرات الخاصة به.

الفجوة السابعة: عدم التركيز على استخدام مجموعة أدوات تدابير بناء الثقة(CBM) لمعالجة مخاطر تكنولوجيا المعلومات والاتصالات (ICT) التي تمس سلسلة التوريد

- كما هو الحال في بناء القدرات، لم يتم البحث بشكل كافٍ في الدور الذي تُؤديه الشفافية وتدابير بناء الثقة في (T)CBMs معالجة مخاطر تكنولوجيا المعلومات والاتصالات (ICT) لسلاسل التوريد التكنولوجية (TSCs). وتنمُّ بعض إشارات الخبراء حول هذه الأداة إلى أنّه من الصعب تطبيق الشفافية وتدابير بناء الثقة (T)CBMs والتحقق منها في سياق تنفيذ معايير فريق الخبراء الحكوميين (GGE) بشأن سلسلة التوريد[113]. يرجع ذلك إلى حدٍّ ما إلى أنّ مفهوم تدابير بناء الثقة (CBM) قد تم تشكيله في البداية من أجل منع النزاعات المسلحة والتخفيف من حدتها، ولا يزال يعمل ضمن هذا المنطق واللغة، وهما بعيدان تمامًا عن لغة ومنطق البائعين والمشترين والجهات المنظمة المشارِكة في علاقات سلسلة التوريد.
- النجاح النسبي في اعتماد تدابير بناء الثقة (CBM) على المستوى الإقليمي (منظمة الأمن والتعاون في أوروبا (OSCE) في 2021 و 2016)، وعلى المستوى الثنائي (الاتفاقيات بين روسيا والولايات المتحدة في 2013) للتخفيف من مخاطر تكنولوجيا المعلومات والاتصالات (ICT) العابرة للحدود، ويعطي كل ذلك سببًا لاستكشاف المزيد حول إمكانية اعتماد مجموعة أدوات تدابير بناء الثقة (CBM) لإدارة تحديات الأمن الإلكتروني لسلاسل التوريد التكنولوجية (TSCs).
- فيما يتعلق بالأهداف الرئيسية، هناك الكثير من القواسم المشتركة بين الشفافية وتدابير بناء الثقة (TSCs) وأطر ضمان الأمن – إذ تهدف كلتا الطريقتين إلى توليد الثقة بين الأطراف المتفاعلة في بيئة غير موثوقة. كما أنّ الشفافية هي أحد الأساسات الأخرى المشتركة لهذين النهجين: ففي سياق تدابير بناء الثقة (CBM) هناك حاجة إلى زيادة التفاهم بين الأطراف وتقليل مخاطر التصعيد. وفي شبكات البائعين وفي سلسلة التوريد التكنولوجية (TSC) ذاتها، تعد الشفافية أحد الأهداف الرئيسية لإدارة مخاطر سلسلة التوريد (SCRM) وضمان الأمن.
- المشاركة الطوعية للمعلومات حول التهديدات، والمخاطر ونواقل الثغرات هي أيضًا جزء من الشفافية وتدابير بناء الثقة (T)CBM وطرق إدارة مخاطر سلسلة التوريد (SCRM) الشاملة وطرق ضمان الأمن.
- المشاركة الطوعية للمعلومات حول الاستراتيجيات المعتمدة، والتدابير التنظيمية، وأفضل الممارسات، وغير ذلك، مما يمكن استخدامه في سياق إدارة مخاطر سلسلة التوريد القائمة على تكنولوجيا المعلومات والاتصالات (ICT) من كلٍّ من (الجهات الفاعلة في الشركة (كما يفعل العديد منها بالفعل) والدول.

113 Osula & Rõigas (2018).

- يمكن معالجة القضايا ذات الصلة بضمان أمن وسلامة سلسلة التوريد التكنولوجية (TSC) من خلال مجموعة أدوات الشفافية وتدابير بناء الثقة (T)CBM باعتبارها عنصرًا محددًا لحماية البنية التحتية المهمة – وهو جزء رئيسي من نطاق تدابير بناء الثقة (CBM) المستقاة من ممارسات منظمة الأمن والتعاون في أوروبا (OSCE).
- يجب استكشاف مجموعة من أدوات الشفافية وتدابير بناء الثقة (T)CBMs لتحقيق الأمن الإلكتروني، بما في ذلك تلك المعتمدة من منظمة الأمن والتعاون في أوروبا (OSCE) بالتفصيل لتقييم قدرتها على تعزيز التعاون الحكومي الدولي بشأن معالجة مخاطر تكنولوجيا المعلومات والاتصالات (ICT) التي تمس سلاسل التوريد التكنولوجية (TSCs).

الفجوة الثامنة: انخفاض مستوى نضج الأطر والمبادرات الوطنية لضمان أمن وسلامة سلاسل التوريد التكنولوجية (TSCs) على المستوى الوطني بشكل عام

- كما توضح النبذة العامة حول الاستجابات الحكومية في البند 4.3، فإنّ غالبية الاستجابات الحديثة على المستوى الوطني لمعالجة مخاطر تكنولوجيا المعلومات والاتصالات (ICT) التي تمس سلاسل التوريد التكنولوجية (TSCs) تتركز في عدد محدود من الدول. إذ تكشف النظرة على الدول المتبقية مستويات أقل بكثير من النضج في الاستجابات الاستراتيجية والسياساتية والتنظيمية لمثل تلك التحديات. هذا وتتضمن الفجوات ذات الصلة ما يلي:
  - الافتقار إلى رؤية استراتيجية وعدم تحديد الأهداف بين الجهات المنظمة فيما يتعلق بالتحوُّل التكنولوجي لسلسلة التوريد العالمية وتأثيره على المستوى الوطني، والمتعلقة أيضًا بالاستجابات للمخاطر الأمنية ذات الصلة.
  - الافتقار إلى التنسيق على مستوى الحكومة فيما يتعلق بصناعة السياسة، والتدابير التنظيمية والتعاون مع الصناعة ومجتمع التكنولوجيا بشأن قضايا أمن وسلامة سلسلة التوريد. وفي العديد من الحالات، تكون الأنشطة التنظيمية مُشتتة بين الهياكل والوكالات والأقسام المختلفة.
  - عدم طلب الدعم – وكذلك عدم توفّره – من الصناعة ومجتمعات التكنولوجيا وخبراء السياسة لاستجابات الحكومات لتحديات تكنولوجيا المعلومات والاتصالات (ICT) التي تمس سلاسل التوريد.

114 OSCE (2012).

التوصيات المُقترحة لتفعيل المبادرات المعيارية

عقِب تحليل النتائج الواردة في هذا التقرير، يمكن الخروج بعدد من التوصيات لطرحها للمناقشة مع أصحاب المصلحة المعنيين. وهناك العديد من الملاحظات المتعلقة بهذه التوصيات، والتي ينبغي لقراء هذا التقرير أخذها في الاعتبار:

- تم تصميم التوصيات لمعالجة الفجوات المُدرجة في الفصل السادس.
- تهدف التوصيات إلى إثارة النقاشات بين صناع السياسات والدبلوماسيين وغيرهم من الخبراء الوطنيين المشاركين في جهود تطوير المعايير والصناعة كذلك، فضلًا عن مجتمع التكنولوجيا الأوسع ومجموعات أصحاب المصلحة الأخرى.
- هذه التوصيات مُوجهة إلى الدول، ومنتديات أصحاب المصلحة المتعددين، والأمم المتحدة، بصفتهم الجهات الفاعلة الرئيسية المسؤولة عن العمليات المختلفة ذات الصلة بمعايير الأمن الإلكتروني.
- لا تهدف التوصيات إلى تغطية جميع الاستجابات والحلول لمخاطر تكنولوجيا المعلومات والاتصالات (ICT) التي تمس سلاسل التوريد التكنولوجية (TSCs)؛ إنما تعالج القضايا فقط في سياق تفعيل المعايير الدولية ومبادرات تطوير المعايير.

فيما يلي سرد لمجموعة التوصيات التي خرج بها هذا التقرير.

1. مواءمة نطاق المعايير المقترحة مع نهج إدارة مخاطر سلسلة التوريد (SCRM) الشامل وممارسات الصناعة
2. تعزيز التنسيق والتآزر بين مبادرات تطوير المعايير من قبل أصحاب المصلحة المتعددين، وتعزيز الشروط الدُنيا الموحدة والقابلة للتشغيل المتبادل لموردي التكنولوجيا.
3. مواءمة العمليات الوطنية لإدارة بائعي التكنولوجيا عبر الأوطان:
4. النظر في إنشاء منصة مخصصة لدعم العمليات التي تقودها الأمم المتحدة للتعامل مع الصناعة ومجتمع التكنولوجيا ومجموعات أصحاب المصلحة الآخرين والمبادرات النشطة في مجال أمن وسلامة سلسلة التوريد.
5. زيادة التركيز على جهود بناء القدرات.
6. تقييم وتحديد فرص استخدام مجموعة أدوات الشفافية وتدابير بناء الثقة (T)CBM لضمان أمن وسلامة سلاسل التوريد التكنولوجية (TSCs).
7. تعزيز التنسيق المؤسسي والاستراتيجي والسياساتي للجهود المبذولة لمعالجة تحديات تكنولوجيا المعلومات والاتصالات (ICT) التي تمس سلاسل التوريد التكنولوجية (TSCs) على المستوى الوطني.

تم توضيح كل توصية من هذه التوصيات بمزيد من التفصيل في الأقسام التالية.

التوصية الأولى: مواءمة نطاق المعايير المقترحة مع نهج إدارة مخاطر سلسلة التوريد (SCRM) الشامل وممارسات الصناعة. (تعالج الفجوة الأولى والثانية

مُوجهة إلى: فريق الخبراء الحكوميين (GGE) والفريق العامل مفتوح العضوية (OEWG) في الأمم المتحدة.

في إطار المناقشات ضمن فريق الخبراء الحكوميين (GGE) وبالاستفادة من تفويض الفريق العامل مفتوح العضوية (OEWG) لمواصلة تطوير المعايير والقواعد والمبادئ، قد تتضمن الإجراءات المحددة في هذا الصدد ما يلي:

- توسيع نطاق تركيز المعايير (الجديدة والمعتمدة) للتعامل مع السلسلة الكاملة لمخاطر تكنولوجيا المعلومات والاتصالات (ICT) ومواءمة محتوى المعايير المقترحة مع النُهج المتبعة في الصناعة ومجتمع التكنولوجيا
- تحقيق توازن أفضل بين المعايير «السلبية» و«الإيجابية»، مع مراعاة الطبيعة الأساسية للتحديات التكنولوجية والقانونية والأخرى التي تواجه المعايير السلبية ذات الصلة بسلاسل التوريد (مسألة الإسناد فيما يتعلق بالأمن الإلكتروني، وعدم تَوفُّر أدوات للتحقق والمتابعة الفعالة للامتثال، وما إلى ذلك).

التوصية الثانية: تعزيز التنسيق والتآزر بين مبادرات تطوير المعايير من قبل أصحاب المصلحة المتعددين، وتعزيز الشروط الدُنيا الموحدة والقابلة للتشغيل المتبادل لموردي التكنولوجيا (تعالج الفجوة الثالثة).

مُوجهة إلى: مبادرات تطوير المعايير من أصحاب المصلحة المتعددين ومُساهميهم (الدول، الصناعة، ومجتمع التكنولوجيا).

تتضمن الإجراءات المحددة في هذا الصدد ما يلي:

- استكشاف الفرص لضمان تدفق الاتصال ومشاركة المعلومات بشكل منظم ومنهجي بين عمليات تطوير المعايير لدى أصحاب المصلحة المتعددين، والتي تعالج قضايا سلسلة التوريد العالمية في سياق تكنولوجيا المعلومات والاتصالات (ICT) (مثل اتفاقية جنيف الرقمية، وتعهد حماية الأمن الإلكتروني، وميثاق الثقة، ونداء باريس).
- إطلاق عملية لمناقشة وتفصيل مجموعة موحدة، أو على الأقل مُنسقة، وقابلة للتشغيل المتبادل من الشروط الدنيا لمعايير الأمن والاعتماد (إصدار الشهادات)، بحيث تكون مشتركة ومدعومة ومعززة بشكل مشترك من قبل المنتديات الرئيسية لأصحاب المصلحة المتعددين، وقد تتضمن عناصر المجموعة ما يلي:
  - مجموعة مشتركة من أفضل الممارسات أو مدونات قواعد السلوك المطبقة بين بائعي التكنولوجيا الرئيسيين، والتي تهدف إلى التخفيف من المخاطر التي تمس أمن وسلامة سلاسل التوريد العالمية.
  - مجموعة مشتركة من متطلبات تقييس معايير الأمن ومتطلبات الاعتماد (إصدار الشهادات) لموردي التكنولوجيا. يتجلى أحد الأمثلة الجيدة في مجموعة متطلبات الأمن التي طورتها سيمنز في إطار مبادرة ميثاق الثقة التي أطلقتها.
  - إطار عمل موحد لتقييم مخاطر الطرف الثالث.
  - مجموعة مشتركة من الأدوات التقنية لضمان الأمن والسلامة على طول سلاسل التوريد التكنولوجية (TSCs) العالمية (على سبيل المثال، نظام المُعرفات الرقمية لضمان إمكانية التتبُّع الشامل على طول سلاسل التوريد).

التوصية الثالثة: مواءمة العمليات الوطنية لإدارة بائعي التكنولوجيا العابرين للحدود (تعالج الفجوة الرابعة).

موجهة إلى: الدول الأعضاء.

- استكشاف فرص التنسيق والمواءمة للنُهج والعمليات المُتبعة عبر الدول لإدارة بائعي التكنولوجيا العابرين للحدود، لتصبح أكثر شفافية ومواءمة مع إدارة مخاطر سلسلة التوريد (SCRM) العالمية ومعايير تقييم أمن البائعين.

التوصية الرابعة: النظر في إنشاء منصة مخصصة لدعم العمليات التي تقودها الأمم المتحدة للتعامل مع الصناعة ومجتمع التكنولوجيا ومجموعات أصحاب المصلحة الآخرين والمبادرات النشطة في مجال أمن سلسلة التوريد وسلامتها (تعالج الفجوة الخامسة).

موجهة إلى: الأمم المتحدة.

- في إطار تفويض الفريق العامل مفتوح العضوية (OEWG) بإقامة حوار مؤسسي منتظم بمشاركة واسعة، بما في ذلك مشاركة القطاع الخاص، يتعين النظر في إنشاء منصة مخصصة (على سبيل المثال لجنة، فرقة عمل) لدعم تفعيل معايير الأمن الإلكتروني الدولية ذات الصلة بسلامة وأمن سلاسل التوريد. يمكن لهذه المنصة، التي تركز على قضايا سلسلة التوريد، أن تُجري أنشطتها على أساس مستمر، وأن تجمع المعلومات والمدخلات والمبادرات من الصناعة ومجتمع التكنولوجيا وأصحاب المصلحة الآخرين، وأن تنقل ملاحظاتها إلى العمليات ذات الصلة التي تقودها الأمم المتحدة. كما أنّ بعض المدخلات التي يمكن أن يُوفرها مثل هذاالإطار لفريق الخبراء الحكوميين (GGE)/ والفريق العام مفتوح العضوية (OEWG) والمشاركين معهم قد تشمل:
  - تحديثات ورؤى متعمقة حول ديناميات المشهد العالمي للتهديدات الإلكترونية فيما يتعلق بسلاسل التوريد التكنولوجية (TSCs) العالمية وغيرها من المجالات ذات الصلة.
  - تحديثات من مجتمع التقييس حول التطورات في المجالات ذات الصلة (تقييس إدارة مخاطر سلسلة التوريد (SCRM) وضمان الأمن، وما إلى ذلك.
  - أفضل الممارسات والنُهج لبائعي التكنولوجيا العالميين للتخفيف من مخاطر تكنولوجيا المعلومات والاتصالات (ICT) التي تمس أمن وسلامة سلسلة التوريد.
  - التحديثات، والمقترحات، والتبادل العام للمعلومات بين العمليات التي تقودها الأمم المتحدة ومبادرات أصحاب المصلحة المتعددين التي تعالج أمن وسلامة سلاسل التوريد العالمية.
- ليس الهدف من المنصة المقترحة تأدية دور مكافئ أو بديل لعمليات تطوير المعايير الإلكترونية الحكومية الدولية، بل لتقديم الدعم الضروري والأساسي لتلك العمليات في المجالات التي يكون للقطاع الخاص فيها دور رئيسي متأصل في تنفيذ المعايير المقترحة. ويمكن أن يكون ضمان أمن وسلامة سلاسل التوريد مجالَ نشاط رئيسي لمثل هذه المبادرة بسبب طبيعتها العالمية والتقنية ومشاركة أصحاب المصلحة المتعددين فيها.

التوصية الخامسة: زيادة التركيز على جهود بناء القدرات (تعالج الفجوة السادسة).

موجهة إلى: الأمم المتحدة، والمنظمات الحكومية الدولية الإقليمية، والدول الأعضاء.

- يتعين على الدول:

– إجراء تقييم للقدرات الوطنية لتحديد الفجوات واحتياجات بناء القدرات ذات الصلة بتخفيف مخاطر تكنولوجيا المعلومات والاتصالات (ICT) التي تمس سلاسل التوريد. يمكن إجراء ذلك بشكل مستقل لكل دولة عبر استخدام أدوات التقييم (الذاتي) لإدارة مخاطر سلسلة التوريد الإلكترونية (cyber-SCRM) أو بدعم من جهة خارجية (أي دولة أخرى، أو منظمة إقليمية، أو طرف ثالث مستقل) بهدف تحديد الفجوات واحتياجات بناء القدرات.

- يتعين على المنظمات الإقليمية:

– إجراء تقييم للمعلومات ومدى الوعي بالمخاطر على المستوى الإقليمي، بالإضافة إلى تخطيط مستويات القدرات وفجواتها فيما يتعلق بإدارة مخاطر سلسلة التوريد الإلكترونية (cyber-SCRM) لجميع الدول الأعضاء، إلى جانب تطوير تدخلات تدريب مستهدفة وفقًا لذلك.

– استكشاف فُرص بناء مراكز الموارد أو البيانات التي ستُكلَّف بتجميع المعلومات المفيدة، وكذلك الموارد والتوصيات والأدوات التقنية من الدول الأعضاء والبائعين لمعالجة مخاطر تكنولوجيا المعلومات والاتصالات (ICT) التي تمس سلاسل التوريد التكنولوجية (TSCs).

- يلزم للعمليات متعددة الأطراف التي تقودها الدول ضمن منتديات الأمم المتحدة:

– استكشاف فُرص استخدام أطر بناء القدرات الرقمية الحالية للأمم المتحدة، بالإضافة إلى المنصات والموارد، لتجميع المعلومات المفيدة، وكذلك أدوات التقييم الذاتي وغيرها من الأدوات لمعالجة مخاطر تكنولوجيا المعلومات والاتصالات (ICT) التي تمس سلاسل التوريد والتخفيف منها (مثل مبادرة الخُوذ الزرقاء الرقمية[115]، وركيزة بناء القدرات للبرنامج العالمي المعني بالجريمة الإلكترونية التابع لمكتب الأمم المتحدة المعني بالمخدرات والجريمة[116] ، والركيزة الرابعة في الأجندة العالمية للأمن الإلكتروني التابعة للاتحاد الدولي للاتصالات (ITU)[117]). هذا ويتعين جمع المعلومات والموارد المتاحة لدى مختلف شرائح الجمهور المستهدف: الدول ومنظمات القطاع العام، وكبار البائعين العابرين للحدود، والشركات الصغيرة والمتوسطة (SMEs).

– تشجيع استخدام موارد بناء القدرات للأمم المتحدة (مثل المنشورات، والبوابات، وقواعد البيانات المتاحة من مكتب الأمم المتحدة لشؤون نزع السلاح، ومعهد الأمم المتحدة لبحوث نزع السلاح، والاتحاد الدولي للاتصالات (ITU) كأداة إضافية لتوفير المعلومات والدعم للمشاركين في المناقشات الحكومية الدولية التي تقودها الأمم المتحدة بشأن المعايير التي تعالج أمن وسلامة سلاسل التوريد التكنولوجية (TSCs).

– النظر في إدراج تدابير لضمان أمن وسلامة سلاسل التوريد التكنولوجية (TSCs) في نطاق المسوحات العالمية والإقليمية ذات الصلة، وتصنيفات وتقييمات الدول الأعضاء التي تُجريها الهيئات التابعة للأمم المتحدة (مثل مؤشر الأمن السيبراني العالمي من الاتحاد الدولي للاتصالات (ITU).

115 OICT (2019).
116 UNODC (n.d.).
117 ITU (n.d.).

التوصية السادسة: تقييم وتحديد فرص استخدام مجموعة أدوات الشفافية وتدابير بناء الثقة (T)CBMs لضمان أمن وسلامة سلاسل التوريد التكنولوجية (TSCs) (تعالج الفجوة السابعة).

موجهة إلى: الأمم المتحدة, والمنظمات الحكومية الدولية الإقليمية والدول الأعضاء.

- يتعين على الأمم المتحدة والمنظمات الحكومية الدولية الإقليمية:

– مناقشة أصحاب المصلحة المتعددين حول إمكانية تطبيق الشفافية وتدابير بناء الثقة (T)CBMs لتعزيز تعاون المنظمات الحكومية الدولية بشأن تخفيف مخاطر تكنولوجيا المعلومات والاتصالات (ICT) التي تمس سلاسل التوريد.

– كجزء من أعمال الفريق العامل مفتوح العضوية (OEWG), دراسة مدى الحاجة إلى توسيع قائمة الشفافية وتدابير بناء الثقة (T)CBMs للأمن الإلكتروني، بإضافة التدابير التي تخص بالتحديد التخفيف من المخاطر الإلكترونية على سلاسل التوريد التكنولوجية (TSCs), أو الحاجة إلى صياغة تفسير سياقي للتدابير المعتمدة فعليًا لتعكس القضايا ذات الصلة بسلسلة التوريد.

- يتعين على الدول الأعضاء:

– مشاركة المعلومات, ربما من جانب واحد, مع الدول أو المنظمات الحكومية الدولية الأخرى حول تهديدات تكنولوجيا المعلومات والاتصالات (ICT) التي تمس سلاسل التوريد, والحوادث التي تؤثر على القطاعيْن العام والخاص، والنُهج الوطنية المفصلة, وأفضل الممارسات ذات الصلة بضمان أمن وسلامة سلاسل التوريد التكنولوجية (TSCs).

– بناء الشفافية وتدابير الثقة بشكل ثنائي مع الدول الأخرى، كأن يتم تبادُل المعلومات حول تهديدات الأمن الإلكتروني لسلسلة التوريد, ونواقل المخاطر والثغرات, والنُهج المتّبعة للتخفيف منها.

– وضع الإجراءات التقنية بشكل ثنائي للحد والتخفيف من الحوادث الكبيرة الناجمة عن الأنشطة الكيدية في سلسلة التوريد العالمية (مثل استخدام نظام مشترك للمُعرّفات الرقمية لضمان إمكانية التتبُّع عبر سلاسل التوريد التكنولوجية, وتحديد نقاط الخطر المحتملة).

التوصية السابعة: تعزيز التنسيق المؤسسي والاستراتيجي والسياساتي للجهود المبذولة لمعالجة تحديات تكنولوجيا المعلومات والاتصالات (ICT) التي تمس سلاسل التوريد التكنولوجية (TSCs) على المستوى الوطني (تعالج الفجوة الثامنة).

موجهة إلى: الدول الأعضاء.

- تم طرح هذه التوصية على النطاق الوطني، كما أنّها تُركز على الحاجة إلى تحسين التنسيق الداخلي لجهود الدول للتخفيف من تحديات تكنولوجيا المعلومات والاتصالات (ICT) التي تمس سلاسل التوريد على المستوى المحلي. وتتضمن الإجراءات المحددة ما يلي:

- إجراء تقييم للاستراتيجيات الوطنية والسياسات والأطر التنظيمية والأدوات المستخدمة للتخفيف من تحديات الأمن التي تمس سلاسل التوريد.

  - إذا لم يكن بالإمكان تفويض تنسيق تطوير السياسات والجهود التنظيمية لتخفيف المخاطر الإلكترونية ه على سلاسل التوريد لوكالة حكومية واحدة (كجزء من الوظائف المنوطة بمركز الأمن الإلكتروني الوطني، أو بتأسيس هيئة مخصصة) ، يتعيّن النظر في تأسيس لجان مشتركة بين الوزارات (أو تأسيس عمليات مكافئة). وقد تتضمن بعض المراجع حول أفضل الممارسات الدولية مركز حماية البنية التحتية الوطنية (CPNI) في المملكة المتحدة، والمركز القومي للأمن السيبراني (NCSC)، إضافة إلى تنسيق شبكة أوسع من الموردين لقاعدة الصناعة الدفاعية من قِبل مكتب وكيل وزارة الدفاع للاستحواذ والاستدامة في الولايات المتحدة، ومبادرة مركز أمن سلسلة التوريد الوطني، المقترح مؤخرًا في مشروع قانون MICROCHIPS[118] في الولايات المتحدة.

- النظر في تطوير واعتماد وثيقة السياسة أو الاستراتيجية التي تعالج بشكل خاص المخاطر ذات الصلة بسلاسل التوريد التكنولوجية (TSCs)، بما في ذلك مخاطر تكنولوجيا المعلومات والاتصالات (ICT)، بالإضافة إلى تحديد النواقل الرئيسية، والمراحل الأساسية والأهداف لجهود الحكومات المبذولة في معالجة تلك المخاطر.

- استكشاف فرص إطلاق أداة مؤسسية لتعاون أصحاب المصلحة المتعددين بشأن التخفيف من مخاطر الأمن والتحديات التي تواجه سلاسل التوريد التكنولوجية TSCs على المستوى الوطني. هذا وقد تتضمن التنسيقات العلاقاتِ بين القطاعيْن العام والخاص، ومجموعات أصحاب المصلحة المتعددين التي تعمل في إطار الحكومة أو المنظمين القطاعيين، بالإضافة إلى المجالس والجمعيات في مجال هذه الصناعة، وغير ذلك.

118 Paganini (2019).

الكونغرس الأمريكي الـ115 (2017-2018)، (قانون تفويض الدفاع الوطني للسنة المالية 2018)

115th US Congress (2017 .(2018-2017. *National Defense Authorization Act for Fiscal Year 2018*. As of 10 November 2019: https://www.congress.gov/bill/115th-congress/senate-bill/1519/text

(نبذة حول مشروع شراكة الجيل الثالث (3GPP).

3rd Generation Partnership Project (3GPP). 2019. 'About 3GPP'. As of 10 November 2019: https://www.3gpp.org/about3-gpp

(قائمة المُوردين)

Apple Inc. 2019. 'Supplier List'. As of 10 November 2019: https://www.apple.com/supplier-responsibility/pdf/Apple- Supplier-List.pdf

(اتجاهات الاستعانة بمصادر أخرى للبرمجيات)

BairesDev. 2019. 'Software Outsourcing Trends'. As of 10 November 2019: https://www.bairesdev.com/insights/software-outsourcing-trends

(إدارة مخاطر سلسلة التوريد (SCRM) القائمة على تكنولوجيا المعلومات والاتصالات (ICT) – تحديث معايير المنظمة الدولية للتوحيد القياسي (ISO)

Bartol, Nadya. 2011. 'ICT SCRM – ISO Standards Update'. US National Institute of Standards and Technology. As of 10 November 2019: https://www.nist.gov/document5893-

(سلاسل التوريد الرقمية للهندسة والبناء - كيف يزيد القادة من الرؤية والبصيرة)

Bhargava, Vishal, Raman Chander, José R Favilla, Wilco Kaijim & Spencer Lin. 2019. *Engineering and Construction Digital Supply Chains – How Leaders Are Increasing Visibility and Insight*. IBM. As of 10 November 2019: https://www.ibm.com/downloads/cas/GJOMQOWL

(ممارسات إدارة مخاطر سلسلة التوريد لأنظمة ومنظمات المعلومات الفيدرالية)

Boyens, Jon, Celia Paulsen, Rama Moorthy & Nadya Bartol. 2015. *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*. NIST Special Publication 161-800. US National Institute of Standards and Technology. As of 10 November 2019: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.161-800.pdf

مركز حماية البنية التحتية الوطنية، 2019 (سلسلة التوريد)

Centre for the Protection of National Infrastructure (CPNI). 2019. 'Supply Chain'. As of 10 November 2019: https://www.cpni.gov.uk/supply-chain

(اتجاهات الهجمات الإلكترونية: تقرير منتصف عام 2019)

Check Point Research. 2019. *Cyber Attack Trends: 2019 Mid-Year Report*. Check Point Software Technologies Ltd. As of 10 November 2019: https://research.checkpoint.com/2019/cyber-attack-trends-2019-mid-year-report

(تقرير الأمن الإلكتروني السنوي لعام 2018, لشركة سيسكو)

Cisco. 2018. Cisco 2018 Annual Cybersecurity Report. As of 10 November 2019: https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr2018-.pdf

الرئيسان المشاركان للفريق العامل المتخصص JTC/CS1-ICT التابع للمعهد الوطني الأمريكي للتقييس لإدارة مخاطر سلسلة التوريد, 2017 (المساهمة في طلب المعلومات المقدم من المعهد الوطني للمعايير والتقنية NIST حول تطوير إطار لتحسين الأمن الإلكتروني للبنية التحتية الحيوية)

Co-Chairs of ANSI's JTC/CS-1ICT SCRM AdHoc Working Group. 2017. 'Contribution to the NIST RFI on Developing a Framework to Improve Critical Infrastructure Cybersecurity'. US National Institute of Standards and Technology. As of 10 November 2019: https://www.nist.gov/system/files/documents/040813/06/06/2017_cs1_ict_scrm_ad_hoc.pdf

لجنة أنظمة الأمن القومي, 2015. (مسرد مصطلحات لجنة أنظمة الأمن القومي (CNSS)

Committee on National Security Systems. 2015. Committee on National Security Systems (CNSS) Glossary. CNSSI No. 4009, 5 April 2015. BAI Information Security / RMF Resource Center. As of 10 November 2019: https://rmf.org/wpcontent/uploads/2017/10/CNSSI-4009.pdf

(الاستعانة بمصادر خارجية لتطوير البرمجيات في أوروبا: الاتجاهات والأرقام)

Computaris. 2016. 'Software Development Outsourcing in Europe: Trends and Figures'. As of 10 November 2019: http://eu.rsystems.com/wp-content/uploads/09/2016/Market-research_Software-development-outsourcing.pdf

(تأمين سلسلة التوريد)

CrowdStrike. 2018. 'Securing the Supply Chain'. As of 10 November 2019: https://www.crowdstrike.com/resources/wp- content/brochures/pr/CrowdStrike-Security-Supply-Chain.pdf

وكالة الأمن الإلكتروني وأمن البنية التحتية, 2019 (نبذة حول المخاطر التي تنشأ عن اعتماد شبكة الجيل الخامس (5G) في الولايات المتحدة الأمريكية).

Cybersecurity and Infrastructure Security Agency (CISA). 2019. *Overview of Risks Introduced by 5G Adoption in the United States. US Department of Homeland Security*. As of 10 November 2019: https://www.dhs.gov/sites/default/files/publications/0731_19_cisa_5th-generation-mobile-networks-overview_0.pdf

(تعهد حماية الأمن الإلكتروني, 2019 (تعهد حماية الأمن الإلكتروني – حماية المستخدمين والعملاء في كل مكان)

Cybersecurity Tech Accord. 2019. 'Cybersecurity Tech Accord – Protecting Users and Customers Everywhere'. As of 10 November 2019: https://cybertechaccord.org/accord

(مخاطر إدارة سلسلة التوريد (SCRM): إدارة المخاطر في الشركات أثناء الاستعانة بمصادر خارجية)

Davidson, Don. 2014. 'Supply Chain Risk Management (SCRM): Managing Enterprise Risk when Outsourcing'. US Department of Defense. As of 10 November 2019: https://supplychain.gsfc.nasa.gov/sites/supplychain/files/docs/2014/D.20%Davidson20%-20%SC2014.pptx.pdf

(مجلس أعمال الدفاع, 2017. (الخدمات اللوجستية كميزة تنافسية في القتال الحربي)

Defense Business Board. 2017. *Logistics as a Competitive War Fighting Advantage*. As of 10 November 2019: https://dbb.defense.gov/Portals/35/Documents/Reports/2017/DBB%2017-03%20Logistics%20Study%2020170509%20FINAL.pdf

(لماذا يتعين عليك الشراكة مع شركة تعهيد برامج فيتنامية؟)

Designveloper. 2019. 'Why You Should Partner with a Vietnam Software Outsourcing Company?'. As of 10 November 2019: https://dsvgroup.medium.com/why-you-should-outsource-your-product-to-a-vietnamese-software-company-93b6cd5fdab

(شراء منتجات وخدمات آمنة لتكنولوجيا المعلومات والاتصالات (ICT): دليل المشتري)

EastWest Institute. 2016. *Purchasing Secure ICT Products and Services: A Buyers Guide.* As of 10 November 2019: https://www.eastwest.ngo/idea/purchasing-secure-ict-products-and-services-buyers-guide

(المفوضية الأوروبية, 2019أ. (البحوث والمعايير ذات الصلة بشبكة الجيل الخامس (5G).

European Commission (EC). 2019a. '5G Research & Standards'. As of 10 November 2019: https://digital-strategy.ec.europa.eu/en/policies/5g-research-standards

(توصيات الهيئة في 26 نوفمبر 2019 حول الأمن الإلكتروني لشبكات الجيل الخامس (5G).

———. 2019b. *Commission Recommendation of 26 March 2019 on Cybersecurity of 5G networks, EU Document* C(2019) 2335 final. As of 10 November 2019: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019H0534

(الجهات الفاعلة الرئيسية في التقييس الأوروبي)

———. 2019c. 'Key Players in European Standardisation'. As of 10 November 2019: https://ec.europa.eu/growth/single-market/european-standards/key-players_en

تنشر الدول الأعضاء تقريرًا عن تقييم الاتحاد الأوروبي المنسق للمخاطر لأمن شبكات الجيل الخامس (5G)).

———. 2019d. 'Member States Publish a Report on EU Coordinated Risk Assessment of 5G Networks Security'. As of 10 November 2019: https://ec.europa.eu/commission/presscorner/detail/en/IP_6049_19

وكالة الاتحاد الأوروبي للأمن الإلكتروني, 2015 (سلامة سلسلة التوريد – نبذة عامة حول المخاطر والتحديات الخاصة بسلسلة التوريد القائمة على تكنولوجيا المعلومات والاتصالات (ICT), والرؤية المستقبلية.

European Union Agency for Cybersecurity (ENISA). 2015. *Supply Chain Integrity – An Overview of the ICT Supply Chain Risks and Challenges, and Vision for the Way Forward*. Version 1.1. As of 10 November 2019: https://www.enisa.europa.eu/publications/sci2015-/at_download/fullReport

قطاع تكنولوجيا المعلومات والاتصالات (ICT) في دائرة الضوء – الاستفادة من قرارات المشتريات العامة بشأن ظروف العمل في سلسلة التوريد)

Evermann, Annelie. 2014. *The ICT Sector in the Spotlight - Leverage of Public Procurement Decisions on Working Conditions in the Supply Chain. Electronics Watch Consortium*. As of 10 November 2019: http://electronicswatch.org/the-ict-sector-in-the-spotlight_723519.pdf

(بيان فينشتاين بشأن مخاوف الأمن القومي لشبكات الجيل الخامس (5G)).

Feinstein, Dianne. 2019. 'Feinstein Statement on 5G National Security Concerns'. United States Senator for California Dianne Feinstein, 14 May. As of 10 November 2019: https://www.feinstein.senate.gov/public/index.cfm/press- releases?id=FDC03D-62C40-440DB91-9568-E1103C8B0F

(نداء باريس من أجل الثقة والأمن في الفضاء الإلكتروني)

France Diplomatie (Ministry for Europe and Foreign Affairs). 2018. *Paris Call for Trust and Security in Cyberspace*. As of 10 November 2019: https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf

اللجنة العالمية لاستقرار الفضاء الإلكتروني, 2018 (حزمة معايير سنغافورة)

Global Commission on the Stability of Cyberspace (GCSC). 2018. *Norm Package Singapore*. As of 10 November 2019: https://cyberstability.org/wp-content/uploads/11/2018/GCSC-Singapore-Norm-Package3-MB.pdf

(تقرير سلسلة التوريد المسؤولة لعام 2018)

Google. 2018. *Responsible Supply Chain Report 2018*. As of 10 November 2019: https://storage.googleapis.com/gweb-sustainability.appspot.com/RSC/Google_2018-RSC-Report.pdf

مجموعة السبعة, 2018 (العناصر الأساسية لمجموعة الدول الصناعية السبعة (G-7) لإدارة المخاطر الإلكترونية لدى الطرف الثالث في القطاع المالي)

Group of Seven (G7). 2018. *G-7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector.* Department of Finance Canada. As of 10 November 2019: https://www.fin.gc.ca/activty/G7/pdf/G-7cyber-risk- management-gestion-risques-cybernetiques-eng.pdf

اجتماعات وزراء خارجية مجموعة السبعة/الثمانية, 2019 (إعلان دينارد بشأن مبادرة المعايير الإلكترونية)

Group of Seven/Eight (G8/7) Foreign Ministers Meetings. 2019. 'Dinard Declaration on the Cyber Norm Initiative'. G7 Information Centre. As of 10 November 2019: http://www.g7.utoronto.ca/foreign/-190406cyber.html

مشروع ضمان أمن معدات الشبكة (NESAS).

GSMA. 2019. 'Network Equipment Security Assurance Scheme (NESAS)'. As of 10 November 2019: https://www.gsma.com/security/network-equipment-security-assurance-scheme

(هجمات سلسلة التوريد وتخفيف المرونة إرشادات لمهندسي أمن النظام)

Heinbockel, William J., Ellen R. Laderman & Gloria J. Serrao. 2017. *Supply Chain Attacks and Resiliency Mitigations - Guidance for System Security Engineers.* The MITRE Corporation. As of 10 November 2019: https://www.mitre.org/sites/default/files/pdf/PR_0854-18.pdf

(قياس السطوح النسبية للهجوم)

Howard, Michael, Jon Pincus & Jeannette M. Wing. 2003. 'Measuring Relative Attack Surfaces'. Colorado State University. As of 10 November 2019: https://www.cs.colostate.edu/~malaiya/09/635/Howard03.pdf

(مسؤوليات سلسلة التوريد)

Huawei. 2019. 'Supply Chain Responsibilities'. As of 10 November 2019: https://www.huawei.com/en/about- huawei/sustainability/win-win-development/develop_supplychain

مجلس الرقابة في مركز تقييم الأمن الإلكتروني لشركة هواوي, 2019 (التقرير السنوي لعام 2018 لمجلس الرقابة في مركز تقييم الأمن الإلكتروني لشركة هواوي (HCSEC) – تقرير لمستشار الأمن القومي في المملكة المتحدة)

Huawei Cyber Security Evaluation Centre Oversight Board. 2019. Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board Annual Report 2019 – A Report to the National Security Adviser of the United Kingdom. UK Government. As of 10 November 2019: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf

(«تحليل المعايير الإلكترونية: الشركات الخاصة كرواد في تغيير المعايير»)

Hurel, Louise Marie, & Luisa Cruz Lobato. 2018. 'Unpacking Cyber Norms: Private Companies as Norm Entrepreneurs'. Journal of Cyber Policy 3(1): 61–76. doi:10.1080/23738871.2018.1467942

(سلسلة التوريد – تقرير مسؤولية الشركات لعام 2017)

IBM. 2017a. *Supply Chain – 2017 Corporate Responsibility Report*. As of 10 November 2019: https://www.ibm.com/procurement/openPdf?file=IBM_2017_CRR_SupplyChain.pdf

(مستقبل سلسلة التوريد – التحديات والتكنولوجيات التي تُشكل مستقبل سلسلة التوريد)

———. 2017b. *The Future Supply Chain - The Challenges and Technologies Shaping the Future Supply Chain*. White paper. Watson Customer Engagement. As of 10 November 2019: https://www.ibm.com/downloads/cas/DZKEVME3

المنظمة الدولية للتوحيد القياسي,2007أ. ISO 28000:2007: مواصفات أنظمة إدارة الأمن لسلسلة التوريد)

International Organization for Standardization (ISO). 2007a. *ISO 28000:2007: Specification for Security Management Systems for the Supply Chain.* As of 10 November 2019: https://www.iso.org/standard/44641.html

(أنظمة إدارة الأمن لسلسلة التوريد – أفضل الممارسات لتنفيذ تقييمات وخطط أمن سلسلة التوريد)

———. 2007b. ISO 28001:2007: Security Management Systems for the Supply Chain – Best Practices for Implementing Supply Chain Security, Assessments and Plans – Requirements and Guidance. As of 10 November 2019: https://www.iso.org/standard/45654.html

(ISO/IEC 27036-1:2014:تكنولوجيا المعلومات – تقنيات الأمن – أمن المعلومات لعلاقات الموردين - الجزء الأول: النظرة العامة والمفاهيم)

———. 2014. ISO/IEC 27036-1:2014: Information Technology – Security Techniques – Information Security for Supplier Relationships – Part 1: Overview and Concepts. As of 10 November 2019: https://www.iso.org/standard/59648.html

(ISO/IEC JTC 1/SC27: أمن المعلومات, الأمن الإلكتروني وحماية الخصوصية)

———. 2019. ISO/IEC JTC 1/SC 27: *Information Security, Cybersecurity and Privacy Protection*. As of 10 November 2019: https://www.iso.org/committee/45306.html

الاتحاد الدولي للاتصالات (أجندة الأمن الإلكتروني العالمية)

International Telecommunication Union (ITU). n.d. 'Global Cybersecurity Agenda (GCA)'. As of 10 November 2019: https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx

اللجنة المشتركة حول استراتيجية الأمن الوطنية, 2018 (الأمن الإلكتروني للبنية التحتية الوطنية الحيوية في المملكة المتحدة – التقرير الثالث للدورة 2017–2019)

Joint Committee on the National Security Strategy. 2018. *Cyber Security of the UK's Critical National Infrastructure - Third Report of Session 2017-19*. HL Paper 222, HC 1708. House of Lords, House of Commons. As of 10 November 2019: http://www.dirittoepoliticadeitrasporti.it/wp-content/uploads/2018/12/House-of-Lords-and-House-of- Commons-Cyber-Security-of-the-UKs-Critical-National-Infrastructure-Nov-2018.pdf

(الشفافية)

Kaspersky. 2019. 'Transparency'. As of 10 November 2019: https://www.kaspersky.com/about/transparency?ignoreredirects=true

وقف استغلال التهديدات والثغرات في مجال تكنولوجيا المعلومات والاتصالات (ICT) - نظرة عامة على الاتجاهات الحالية وديناميكيات التمكين واستجابات القطاع الخاص)

Kavanagh, Camino. 2019. Stemming the Exploitation of ICT Threats and Vulnerabilities – An Overview of Current Trends, Enabling Dynamics and Private Sector Responses. United Nations Institute for Disarmament Research. As of 10 November 2019: https://unidir.org/files/publications/pdfs/stemming-the-exploitation-of-ict-threats-and- vulnerabilities-en-805.pdf

(عولمة الخدمات اللوجستية وإدارة سلسلة التوريد)

Khan, Muhammad Arsalan. 2018. 'Globalization of Logistics and Supply Chain Management', conference paper, *Proceedings International Conference on Industrial Engineering and Operations Management*, Kuala Lumpur, 10–8 March 2016. As of 10 November 2019: https://www.researchgate.net/publication/329238875_Globalization_of_Logistics_and_Supply_Chain_Management

(رسالة إلى الأمناء الدائمين بشأن مسألة مخاطر سلسلة التوريد في المنتجات القائمة على السحابة)

Martin, Ciaran. 2018. 'Letter to Permanent Secretaries regarding the Issue of Supply Chain Risk in Cloud-Based Products'. National Cyber Security Centre. As of 10 November 2019: https://www.ncsc.gov.uk/information/letter- permanent-secretaries-regarding-issue-supply-chain-risk-cloud-based-products

(المعايير العالمية: وضع المعايير, والانتشار, والقيود)

Martinsson, Johanna. 2011. Global Norms: Creation, Diffusion, and Limits. The World Bank, Communication for Governance and Accountability Program. As of 10 November 2019: http://siteresources.worldbank.org/EXTGOVACC/Resources/FinalGlobalNormsv1.pdf

(سلسلة التوريد 4.0 – سلسلة التوريد الرقمية للجيل القادم)

McKinsey & Company. 2016. 'Supply Chain 4.0 – The Next-Generation Digital Supply Chain'. As of 10 November 2019: https://www.mckinsey.com/business-functions/operations/our-insights/supply-chain-40--the-next-generation-digital-supply-chain

(تأمين سلسلة التوريد باستخدام تقييمات المخاطر)

Microsoft. 2017. 'Securing the Supply Chain with Risk-Based Assessments'. As of 10 November 2019: https://www.microsoft.com/en-us/itshowcase/securing-the-supply-chain-with-risk-based-assessments

(اتفاقية جنيف الرقمية لحماية الفضاء الإلكتروني)

———. 2018a. 'A Digital Geneva Convention to Protect Cyberspace'. Policy paper. As of 10 November 2019: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH

(بداية الهجوم: تشكل سلسلة التوريد المختَرقة ضمن سلسلة التوريد مخاطر جديدة)

———. 2018b. 'Attack inception: Compromised supply chain within a supply chain poses new risks'. Microsoft Defender ATP Research Team, July 28. As of 10 November 2019: https://www.microsoft.com/security/blog/26/07/2018/attack-inception-compromised-supply-chain-within-a-supply-chain-poses-new-risks

(خصوصية الموردين ومعايير الضمان)

———. 2019. 'Supplier Privacy & Assurance Standards'. As of 10 November 2019: https://www.microsoft.com/en-us/procurement/sspa?activetab=pivot25%3aprimaryr3

(وزارة الاقتصاد والتجارة والصناعة في اليابان، 2019 (إطار الأمن الإلكتروني/المادي (مسودة)

Ministry of Economy, Trade and Industry of Japan (METI). 2019a. *The Cyber/Physical Security Framework (Draft)*. Cyber Security Division, Commerce and Information Policy Bureau. As of 10 November 2019: https://www.meti.go.jp/press/4-20190109001/20190109001/01/2018.pdf

(الصناعات المترابطة)

———. 2019b. 'Connected Industries'. As of 10 November 2019: https://www.meti.go.jp/english/policy/mono_info_service/connected_industries/index.html

(المركز الوطني للأمن الإلكتروني، 2019 (احموا منظماتكم من الهجمات الإلكترونية)

National Cyber Security Centre (NCSC). 2019. 'Protect Your Organisation against Cyber Attack'. As of 10 November 2019: https://www.cyberessentials.ncsc.gov.uk

(معجم المهاجمين: ما هو سطح الهجوم؟)

Newman, Lily Hay. 2017. 'Hacker Lexicon: What Is an Attack Surface?' Wired, 12 March, 08:00 ET. As of 10 November 2019: https://www.wired.com/03/2017/hacker-lexicon-attack-surface

(تقديم استراتيجية صارمة لأمن ومرونة سلسلة التوريد في الاستجابة للطابع المتغير للحرب)

Nissen, Chris, John Gronager, Robert Metzger & Harvey Rishikof. 2018. *Deliver Uncompromised A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War*. The MITRE Corporation. As of 10 November 2019: https://www.mitre.org/sites/default/files/publications/pr-2417-18-deliver-uncompromised- MITRE-study26-AUG2019.pdf

(منتدى التحول الشمال أمريكي, 2018 (دليل إدارة مخاطر سلسلة التوريد الإلكترونية (الإصدار 1.0)

North American Transmission Forum (NATF). 2018. *Cyber Security Supply Chain Risk Management Guidance (Version 1.0).* North American Electric Reliability Corporation. As of 10 November 2019: https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NATF%20Cyber%20Security%20Supply%20Chain%20Risk%20Management%20Guidance.pdf

مكتب السكرتير الصحفي, 2017 (بيان وزارة الأمن الداخلي بشأن إصدار التوجيه التشغيلي الملزم 17-01)

Office of the Press Secretary. 2017. 'DHS Statement on the Issuance of Binding Operational Directive 17-01'. US Department of Homeland Security, 13 September. As of 10 November 2019: https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01

مكتب وكيل وزارة الدفاع للاستحواذ والاستدامة في الولايات المتحدة, 2019 (شهادة نموذج نضج الأمن الإلكتروني)

Office of the Under Secretary of Defense for Acquisition and Sustainment. 2019. *Cybersecurity Maturity Model Certification (CMMC)*, Draft, Version 0.6. As of 10 November 2019: https://www.acq.osd.mil/cmmc/docs/CMMC- V0.6b-20191107.pdf

مكتب وكيل وزارة الدفاع للاستحواذ والاستدامة في الولايات المتحدة, ومكتب نائب مساعد وزير الدفاع للسياسات الصناعية, 2018 (تقييم وتعزيز قاعدة التصنيع والدفاع الصناعية ومرونة سلسلة التوريد في الولايات المتحدة)

Office of the Under Secretary of Defense for Acquisition and Sustainment, & Office of the Deputy Assistant Secretary of Defense for Industrial Policy. 2018. *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States. US Department of Defense*. As of 10 November 2019: https://media.defense.gov/2018/Oct/05/2002048904/-1/-1/1/ASSESSING-AND-STRENGTHENING-THEMANUFACTURING-AND%20DEFENSE-INDUSTRIAL-BASE-AND-SUPPLY-CHAIN-RESILIENCY.PDF

منظمة التعاون الاقتصادي والتنمية, 2018 (النظرة العالمية للنمو المستدام 2019: حان الوقت لمواجهة التحديات)

Organisation for Economic Co-operation and Development (OECD). 2018. *Global Outlook on Financing for Sustainable Development 2019: Time to Face the Challenge*. Paris: OECD Publishing. doi:-9789264307995/10.1787en

منظمة الأمن والتعاون في أوروبا,2012 (دليل منظمة الأمن والتعاون في أوروبا (OSCE) حول تدابير بناء الثقة (CBMs) غير العسكرية)

Organization for Security and Co-operation in Europe (OSCE). 2012. *s*). As of 10 November 2019: https://www.osce.org/secretariat/91082?download=true

(المعايير الدولية الإلكترونية من منظور قانوني وسياسي وصناعي)

Osula, Anna-Maria, & Henry Rõigas, eds. 2016. *International Cyber Norms Legal, Policy and Industry Perspectives.* Tallinn: NATO Cooperative Cyber Defence Centre of Excellence Publications. As of 10 November 2019: https://ccdcoe.org/uploads/10/2018/InternationalCyberNorms_full_book.pdf

(يهدف مشروع قانون (MICROCHIPS) إلى تحسين سلسلة التوريد التكنولوجية (TSC))

Paganini, Pierluigi. 2019. 'MICROCHIPS Act Aims at Improving Tech Supply Chain'. SecurityAffairs, 1 August. As of 10 November 2019: https://securityaffairs.co/wordpress/89224/laws-and-regulations/microchips-supply-chain- security.html

المكتب البرلماني للعلم والتكنولوجيا, 2017 (الأمن الإلكتروني للبنية التحتية في المملكة المتحدة)

Parliamentary Office of Science and Technology. 2017. *Cyber Security of UK Infrastructure*. Postnote Number 554, May 2017. Houses of Parliament. As of 10 November 2019: http://researchbriefings.files.parliament.uk/documents/POST-PN0554-/POST-PN0554-.pdf

إدارة مخاطر سلسلة التوريد القائمة على تكنولوجيا المعلومات والاتصالات) (ICT))

Paulsen, Celia. 2013. 'ICT Supply Chain Risk Management'. US National Institute of Standards and Technology. As of 10 November 2019: https://csrc.nist.gov/CSRC/media//Projects/Forum/documents/june2013_presentations/forum_june2013_cpaulsen.pdf

(إعلان في دائرة الضوء: نماذج أعمال جديدة)

PricewaterhouseCoopers (PwC). 2015. Disclose In the Spotlight: New Business Models. Issue ,2 2015. As of 10 November 2019: https://disclose.pwc.ch/22/media/pdf/pwc_disclose_1502_e.pdf

(بناء المؤسسة الرقمية)

———. 2016. Industry 4.0: Building the Digital Enterprise. As of 10 November 2019: https://www.pwc.com/gx/en/industries/industries-4.0/landing-page/industry-4.0-building-your-digital-enterprise-april-2016.pdf

من المتوقع أن يصل حجم سوق برمجيات إدارة سلسلة التوريد العالمية إلى 22.7 مليار دولار بحلول عام 2024, مرتفعاً بنسبة نمو للسوق تصل إلى 12.1%كمعدل نمو سنوي مركب خلال فترة التنبؤ)

PRNewswire. 2018. 'The Global Supply Chain Management Software Market Size Is Expected to Reach $22.7 Billion by 2024, Rising at a Market Growth of 12.1% CAGR during the Forecast Period'. PRNewswire.com, 22 August, 09:08 ET. As of 10 November 2019: https://www.prnewswire.com/news-releases/the-global-supply-chain-management-software-market-size-is-expected-to-reach-22-7-billion-by-2024--rising-at-a-market-growth-of-12-1-cagr-during-the-forecast-period-300700907.html

(تحديات الأمن الإلكتروني العالمية: حان الوقت لتحقيق تقدُّم فعلي في معالجة مخاطر سلسلة التوريد)

Purdy, Andy. 2016. *The Global Cyber Security Challenge It Is Time for Real Progress in Addressing Supply Chain Risks*. Huawei Technologies. As of 10 November 2019: https://www-file.huawei.com/-/media/corporate/pdf/cyber-security/the-global-cyber-security-challenge-en.pdf

(نمو سوق برمجيات إدارة سلسلة التوريد العالمية, التوقعات وسلسلة القيمة 2019–2025)

ResearchMoz. 2019. 'Global Supply Chain Management Software Market Growth, Forecast and Value Chain 2019- 2025'. Commerce Gazette, 23 September. As of 10 November 2019: https://commercegazette.com/2019/09/23/supply-chain-management-software-market-growth-forecast-and- value-chain-2019-2025

(إطار سلامة سلسلة توريد البرمجيات – تحديد المخاطر والمسؤوليات لتأمين البرمجيات في سلسلة التوريد العالمية)

SAFECode. 2009. The Software Supply Chain Integrity Framework – Defining Risks and Responsibilities for Securing Software in the Global Supply Chain. As of 10 November 2019: http://safecode.org/publication/SAFECode_Supply_Chain0709.pdf

(الإدارة المسؤولة لسلاسل التوريد)

Samsung. 2019. 'Responsible Management of Supply Chain'. As of 10 November 2019: http://safecode.org/publication/SAFECode_Supply_Chain0709.pdf

(سلسلة التوريد الرقمية)

SAP. 2019. 'Digital Supply Chain'. As of 10 November 2019: https://www.sap.com/products/digital-supply-chain.html

(تضع شركة سيمنز متطلبات الأمن الإلكتروني المُلزمة للموردين)

Siemens AG. 2019. 'Siemens Establishes Binding Cybersecurity Requirements for Suppliers'. Press Release. Siemens AG, 15 February. As of 10 November 2019: https://press.siemens.com/global/en/pressrelease/siemens-establishes-binding-cybersecurity-requirements-suppliers?content[]=Corp

(تأمين سلاسل التوريد الحيوية – الفرص الاستراتيجية لمبادرة لجنة الاعتماد الدولي للمنتجات الإلكترونية (CPICTM))

Stockton, Paul. 2018. Securing Critical Supply Chains – Strategic Opportunities for the Cyber Product International Certification (CPICTM) Commission Initiative. EIS Council. As of 10 November 2019: https://www.inss.org.il/wp-content/uploads/2018/10/paul.pdf

(وجهات نظر الأمن الإلكتروني – تحويل الأمن الإلكتروني ليكون جزءًا متأصلًا في الشركة - مجموعة من العمليات والسياسات والمعايير المتكاملة)

Suffolk, John. 2013. Cyber Security Perspectives – Making Cyber Security a Part of a Company's DNA – A Set of Integrated Processes, Policies and Standards. White paper. Huawei Technologies. As of 10 November 2019: https://www-file.huawei.com/-/media/corporate/pdf/cyber-security/hw-cyber-security-wp-2013-en.pdf

(تقرير تهديدات أمن الإنترنت)

Symantec. 2019. *ISTR Internet Security Threat Report*, Vol. 24. As of 10 November 2019: https://docs.broadcom.com/doc/istr-24-2019-en

المجموعة المفتوحة, 2014(معيار مُزود التكنولوجيا الموثوقة المُصادق عليه من منتدى المجموعة (O-TTPS) المفتوحة الإصدار1.1).

The Open Group. 2014. Open Trusted Technology Provider™ Standard (O-TTPS), Version 1.1 (Identical to ISO/IEC 20243:2015). As of 10 November 2019: https://publications.opengroup.org/c147?_ga=2.34603688.806857558.1575029424-72192277.1567443766

مؤسسة البرمجيات الموثوقة (إطار عمل مؤسسة البرمجيات الموثوقة)

Trustworthy Software Foundation. 2019. 'TS Framework'. As of 10 November 2019: http://tsfdn.org/ts-framework

الجمعية العامة للأمم المتحدة, 1999 (التطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي

United Nations General Assembly (UNGA). 1999. *Developments in the field of information and telecommunications in the context of international security,* UN document A/RES/53/70, 4 January 1999. As of 10 November 2019: https://digitallibrary.un.org/record/1655670

(تقرير فريق الخبراء الحكوميين (GGE) حول التطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي)

———. 2013. Report of the Group of Governmental Experts on developments in the field of information and telecommunications in the context of international securityD, UN document A/24 ,98/68 June 2013. As of 10 November 2019: https://digitallibrary.un.org/record/753055

رسالة بتاريخ 9 يناير 2015 من الممثلين الدائمين لكل من الاتحاد الروسي وأوزبكستان وطاجيكستان والصين وكازاخستان

———. 2015. 'Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General. International code of conduct for information security', UN document A/69/723, 13 January 2015. As of 10 November 2019: https://undocs.org/A/69/723

(التطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي)

———. 2018. Developments in the field of information and telecommunications in the context of international security. Resolution adopted by the General Assembly on 5 December 2018. UN document A/RES/73/27, 11 December 2018. As of 10 November 2019: https://undocs.org/A/RES/73/27

مكتب الأمم المتحدة لشؤون نزع السلاح, ٢٠١٩أ. (التقارير المقدمة من الصين إلى الفريق العامل مفتوح المعني بالتطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي (OEWG) العضوية

United Nations Office for Disarmament Affairs (UNODA). 2019a. 'China's Submissions to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security'. As of 10 November 2019: https://s3.amazonaws.com/unoda-web/wp-content/uploads/09/2019/china- submissions-oewg-en.pdf

(التطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي)

———. 2019b. 'Developments in the Field of Information and Telecommunications in the Context of International Security'. As of 10 November 2019: https://www.un.org/disarmament/ict-security

مكتب الأمم المتحدة لتكنولوجيا المعلومات والاتصالات, 2019 (مبادرة الخُوذ الزرقاء الرقمية)

United Nations Office of Information and Communications Technology (OICT). 2019. 'Digital Blue Helmets'. As of 10 November 2019: https://unite.un.org/digitalbluehelmets

مكتب الأمم المتحدة المعني بالمخدرات والجريمة (البرنامج العالمي لمكافحة الجريمة الإلكترونية

United Nations Office on Drugs and Crime (UNODC). n.d. 'Global Programme on Cybercrime'. As of 10 November 2019: https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html

التلفزيون الشبكي للأمم المتحدة, 2019 (الاجتماع الأول للفريق العامل مفتوح العضوية (OEWG) المعني بالتطورات في مجال المعلومات والاتصالات في سياق الأمن العالمي)

UN Web TV. 1)' .2019st Meeting) Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security'. UN Web TV, 9 September. As of 10 November 2019: http://webtv.un.org/search/1st-meeting-open-ended-working-group-on-developments-in-the-field-of- information-and-telecommunications-in-the-context-of-international- security/6084740970001/?term=open20%ended20%information20%group&lan=English&cat=Meetings2%FEvents &sort=date&page=2

وزارة الدفاع الأمريكية, 2018 (حماية الوظائف الحيوية للمهمة للتوصل إلى أنظمة وشبكات الموثوقة

US Department of Defense (DoD). 2018. 'Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)'. Department of Defense Instruction Number 5 ,5200.44 November 2012, incorporating Change 15 ,3 October, 2018. As of 10 November 2019: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520044p.pdf?ver=903-075800-08-11-2018

وزارة الدفاع الأمريكية, وإدارة الخدمات العامة الأمريكية, الإدارة الوطنية الأمريكية للملاحة الجوية والفضاء ((ناسا), 2019 (لائحة الاستحواذ الفيدرالية: استخدام المنتجات والخدمات في شركة كاسبرسكي لاب)

US Department of Defense (DoD), US General Services Administration (GSA) & US National Aeronautics and Space Administration (NASA). 2019. *Federal Acquisition Regulation: Use of Products and Services of Kaspersky Lab*. Federal Register, 10 September. As of 10 November 2019: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520044p.pdf?ver=903-075800-08-11-2018

المعهد الوطني للمعايير والتقنية في الولايات المتحدة, 2018 أ (إطار الأمن الإلكتروني. تأثيرات الصناعة)

US National Institute of Standards and Technology (NIST). 2018a. 'Cybersecurity Framework. Industry Impacts'. As of 10 November 2019: https://www.nist.gov/industry-impacts/cybersecurity

(إطار تحسين الأمن الإلكتروني للبنية التحتية الحيوية. الإصدار 1.1)

———. 2018b. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. As of 10 November 2019: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

(إدارة مخاطر سلسلة التوريد (SCRM) القائمة على تكنولوجيا المعلومات والاتصالات (ICT)

———. 2018c. 'Information and Communications Technology Supply Chain Risk Management (ICT SCRM)'. As of 10 November 2019: https://www.cisa.gov/publication/ict-scrm-fact-sheet

مركز موار الامن الحاسوبي في المعهد الوطني للمعايير والتقنية في الولايات المتحدة (مسرد المصطلحات. منافذ التمرير الخفية

US National Institute of Standards and Technology (US NIST) Computer Security Resource Center (CSRC). n.d.a. 'Glossary. Backdoor'. As of 10 November 2019: https://csrc.nist.gov/glossary/term/backdoor

(مسرد المصطلحات. قنبلة منطقية)

n.d.b. 'Glossary. Logic Bomb'. As of 10 November 2019: https://csrc.nist.gov/glossary/term/logic_bomb
———. 2017. 'Software Supply Chain Attacks'. As of 10 November 2019: https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/ssca/-2017winter/NCSC_Placemat.pdf

أفضل الممارسات في إدارة مخاطر سلسلة التوريد الإلكترونية – شركة سيسكو, إدارة مخاطر سلسلة التوريد المتكاملة)

———. 2019a. *Best Practices in Cyber Supply Chain Risk Management - Cisco, Managing Supply Chain Risks End-to- End*. As of 10 November 2019: https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_Cisco_071515.pdf

أفضل الممارسات في إدارة مخاطر سلسلة التوريد الإلكترونية - حماية المحاصيل في دوبونت, وتخصصات التشغيل لاستدامة سلسلة التوريد وإدارة المخاطر والمرونة)

———. 2019b. Best Practices in Cyber Supply Chain Risk Management – DuPont Crop Protection, Operating Disciplines for Supply Chain Sustainability, Risk Management and Resilience. As of 10 November 2019: https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_DuPont_071315.pdf

(أفضل الممارسات في إدارة مخاطر سلسلة التوريد الإلكترونية – شركة فاير آي, إدارة مخاطر سلسلة التوريد)

———. 2019c. Best Practices in Cyber Supply Chain Risk Management - FireEye, Supply Chain Risk Management. As of 10 November 2019: https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_FireEye_081415.pdf

أفضل الممارسات في إدارة مخاطر سلسلة التوريد الإلكترونية – شركة فوجيتسو, إدارة مخاطر سلسلة التوريد في الشبكات الضوئية واللاسلكية)

———. 2019d. Best Practices in Cyber Supply(Chain Risk Management – Fujitsu Network Communications, Managing Supply Chain Risks in Optical and Wireless Networking. As of 10 November 2019: https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_Fujitsu_091615.pdf

أفضل الممارسات في إدارة مخاطر سلسلة التوريد الإلكترونية – شركة إنتل, إدارة المخاطر المتكاملة في سلسلة التوريد الخاصة بشركة إنتل)

———. 2019e. *Best Practices in Cyber Supply Chain Risk Management - Intel Corporation, Managing Risk End-to-End in Intel's Supply Chain*. As of 10 November 2019: https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_Intel_100715.pdf

(أفضل الممارسات في إدارة سلسلة التوريد الإلكترونية - جونيبر للشبكات, ضمان تجربة عملاء مميزة)

———. 2019f. *Best Practices in Cyber Supply Chain Risk Management – Juniper Networks, Ensuring a Remarkable Customer Experience*. As of 10 November 2019: https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_Juniper_081415.pdf

أفضل الممارسات في إدارة مخاطر سلسلة التوريد الإلكترونية – نورثروب غرومان, سلسلة التوريد الموثوقة, والمبتكرة, وعالمية المستوى)

———. 2019g. *Best Practices in Cyber Supply Chain Risk Management – Northrop Grumman Corporation, Trusted, Innovative, World-Class Supply Chain*. As of 10 November 2019: https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/case_studies/USRP_NIST_Northup_081615.pdf

إدارة مخاطر سلسلة التوريد الإلكترونية – أفضل الممارسات في الصناعة لإدارة مخاطر سلسلة التوريد الإلكترونية (Cyber SCRM))

———. 2019h. 'Cyber Supply Chain Risk Management – Industry Best Practices for Cyber SCRM'. As of 10 November 2019: https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management/Best-Practices

البيت الأبيض الأمريكي, 2018 (الاستراتيجية الإلكترونية الوطنية في الولايات المتحدة الأمريكية

US White House. 2018. *National Cyber Strategy of the United States of America.* As of 10 November 2019: https://www.whitehouse.gov/wp-content/uploads/09/2018/National-Cyber-Strategy.pdf

(مبادرة الأمن الإلكتروني الوطنية الشاملة)

———. 2019a. *The Comprehensive National Cybersecurity Initiative*. As of 10 November 2019: https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative

(أمر تنفيذي بشأن تأمين تكنولوجيا المعلومات والاتصالات وسلسلة توريد الخدمات)

———. 2019b. 'Executive Order on Securing the Information and Communications Technology and Services Supply Chain'. Whitehouse.gov, 15 May. As of 10 November 2019: https://www.whitehouse.gov/presidential- actions/executive-order-securing-information-communications-technology-services-supply-chain

(الأمن الإلكتروني: مخاطر متزايدة لإدارة مخاطر سلسلة التوريد)

Weatherford, Mark. 2018. 'Cybersecurity: A Growing Risk for Supply Chain Risk Management'. US National Aeronautics and Space Administration (NASA) website. As of 10 November 2019: https://supplychain.gsfc.nasa.gov/sites/supplychain/files/docs/2018/weatherford-SC2018.pdf

(إدارة سلسلة التوريد في شركة Stürmischen Zeiten)

Wieland, Andreas, & Carl Marcus Wallenburg. 2011. *Supply-Chain-Management in stürmischen Zeiten*. Berlin: Universitätsverlag der TU.

البنك الدولي ومنظمة التجارة العالمية, 2019 (تقرير تنمية سلسلة القيمة العالمية لعام 2019 – الابتكار التكنولوجي, وتجارة سلسلة التوريد, والعاملين في هذا العالم الذي يتسم بالعولمة

World Bank & World Trade Organization (WTO). 2019. *Global Value Chain Development Report 2019 - Technological Innovation, Supply Chain Trade, and Workers in a Globalized World*. As of 10 November 2019: http://documents.worldbank.org/curated/en/384161555079173489/Global-Value-Chain-Development-Report- -2019Technological-Innovation-Supply-Chain-Trade-and-Workers-in-a-Globalized-World

(البيان الشفوي لجيريمي رايت بشأن مراجعة سلسلة توريد الاتصالات)

Wright, Jeremy. 2019. 'Jeremy Wright's Oral Statement on the Telecoms Supply Chain Review'. Gov.uk, 22 July. As of 10 November 2019: https://www.gov.uk/government/speeches/jeremy-wrights-oral-statement-on-the-telecoms- supply-chain-review

40 | UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH