الممارسات الناشئة في الشراكات والتعاون بين القطاعين العام والخاص المتعلقة بالأمن السيبراني في الدول المشاركة في منظمة الأمن والتعاون في أوروبا

OSCE Organization for Security and Co-operation in Europe

نشرت من قبل منظمة الأمن والتعاون في أوروبا

فيينا، مارس / آذار 2023

© منظمة الأمن والتعاون في أوروبا OSCE 2023

تخطيط وتصميم من ماكسينوفا، بلغراد

كل الحقوق محفوظة. لا يجوز إعادة نشر أو إنتاج أي جزء من هذا المنشور أو تخزينه في نظام استرجاع أو نقله بأي شكل أو بأي وسيلة - إلكترونية أو ميكانيكية أو تصويرية أو تسجيلية أو غيرها دون إذن كتابي مسبق من الناشرين. لا ينطبق هذا القيد على عمل نسخ رقمية أو مطبوعة من هذا المنشور للاستخدام الداخلي في إطار منظمة الأمن والتعاون في أوروبا، وللاستخدام الشخصي أو التعليمي لأغراض غير ربحية وغير تجارية، بشرط أن تكون النسخ مصحوبة بإقرار بأن منظمة الأمن والتعاون في أوروبا هي المصدر.

رقم ISBN 978-92-9271-238-9
إدارة التهديدات عبر الوطنية
أمانة منظمة الأمن والتعاون في أوروبا
شارع Wallnerstrasse 6، A-1010 فيينا، النمسا
https://www.osce.org/secretariat/cyber-ict-security

تم نشر هذا التقرير بفضل المساهمة السخية من الجمهورية الإيطالية. محتوى هذا المنشور، بما فيه وجهات النظر والآراء والنتائج والتفسيرات والاستنتاجات الواردة فيه لا تعكس بالضرورة آراء الجهات المانحة. إنها ليست وثيقة قائمة على الإجماع.

يتم نشر هذا المنشور بما يتماشى مع ولاية إدارة التهديدات عبر الوطنية التابعة لمنظمة الأمن والتعاون في أوروبا. لا تتحمل الأمانة العامة لمنظمة الأمن والتعاون في أوروبا أي مسؤولية عن دقة أو اكتمال أي معلومات، أو عن التعليمات أو المشورة المقدمة، أو عن أخطاء الطباعة. لا يجوز تحميل الأمانة العامة لمنظمة الأمن والتعاون في أوروبا المسؤولية عن أي خسارة أو ضرر قد ينشأ عن استخدام المعلومات الواردة في هذا المنشور، كما أنها غير مسؤولة عن محتوى المصادر الخارجية، بما في ذلك المواقع الخارجية المشار إليها في هذا لمنشور.

جدول المحتويات

شكر وتقدير

تم إعداد هذا التقرير من قبل خلية تنسيق بإدارة التهديدات عبر الوطنية التابعة لمنظمة الأمن والتعاون في أوروبا (TNTD) تحت إشراف السيدة سيلفيا توته، ضابطة الأمن السيبراني.

تود TNTD أن تشكر الدكتورة كامينو كافاناغ على أبحاثها وصياغة التقرير، كما قدم السيد جريجور راموش من خلية التنسيق TNTD دعمه القيم في التقرير.

قائمة مختصرات الأسماء والمصطلحات

BTK	الهيئة التركية لتكنولوجيا المعلومات والاتصالات
CBM	تدابير بناء الثقة
CCB	مركز الأمن السيبراني بلجيكا
CCN-CERT	المركز الإسباني الحكومي الوطني للتشفير - فريق الاستجابة لحوادث أمن الكمبيوتر
CERT	فريق الاستجابة للطوارئ الحاسوبية
C-HUB	مركز الابتكار الرقمي للأمن السيبراني (البرتغال)
CIPAC	المجلس الاستشاري لشراكة البنية التحتية الحرجة (الولايات المتحدة)
CIRCIA	قانون الإبلاغ عن الحوادث السيبرانية للبنية التحتية الحرجة (الولايات المتحدة)
CISA	وكالة الأمن السيبراني والبنية التحتية (الولايات المتحدة)
CSIRT	فريق الاستجابة لحوادث أمن الكمبيوتر
CSN	مؤسسة شبكة الأمن السيبراني (صربيا)
DEG	فريق خبراء أمن تكنولوجيا المعلومات ونظم المعلومات (لاتفيا)
eID	الهوية الإلكترونية
EISA	الجمعية الإستونية لأمن المعلومات

EU	الاتحاد الأوروبي
FINMA	الهيئة السويسرية للإشراف على السوق المالية
FS-CSC	المركز السويسري للأمن السيبراني في القطاع المالي
FS-ISAC	المركز السويسري لتبادل وتحليل معلومات الخدمات المالية
ICT	تكنولوجيا المعلومات والاتصالات
ISAC	مركز تبادل المعلومات وتحليلها
ITS	المعاهد التكنولوجية العليا (إيطاليا)
IWG	الفريق العامل غير الرسمي
NCSC	المركز الوطني للأمن السيبراني
NCSC-FI	المركز الوطني الفنلندي للأمن السيبراني
NICE Framework	إطار القوى العاملة للأمن السيبراني (الولايات المتحدة)
NIS	أمن الشبكات والمعلومات
NIST	المعهد الوطني للمعايير والتكنولوجيا (الولايات المتحدة)
OKTT	المهمة المعروفة موضوعيا (هولندا)
OSCE	منظمة الأمن والتعاون في أوروبا
PPP	شراكة بين القطاعين العام والخاص
R&D	البحث والتطوير
SBOM	قائمة مواد البرمجيات
SME	الشركات الصغيرة والمتوسطة
SOC	مركز العمليات الأمنية
SOW	سيفون ويب (بلجيكا)
TLP	بروتوكول إشارات المرور
UK	المملكة المتحدة
UKC3	تعاون عناقيد الإنترنت في المملكة المتحدة
UN	الأمم المتحدة
USOM	المركز الوطني التركي للاستجابة لطوارئ الكمبيوتر

تمهيد

يسرني أن أقدم بين أيديكم هذا التقرير عن الممارسات الناشئة في الشراكات والتعاون بين القطاعين العام والخاص في مجال الأمن السيبراني بالدول المشاركة في منظمة الأمن والتعاون في أوروبا. التقرير يبين مدى تنفيذ التدبير الرابع عشر لبناء الثقة في الأمن السيبراني / تكنولوجيا المعلومات والاتصالات والتي وضعته منظمة الأمن والتعاون في أوروبا، ومن شأنه تشجيع الدول على إقامة شراكات بين القطاعين العام والخاص بهدف الاستجابة للتحديات الأمنية المشتركة الناشئة عن استخدام تكنولوجيا المعلومات والاتصالات، كما أنه يقدم أمثلة على الممارسات الحالية في منطقة منظمة الأمن والتعاون في أوروبا، بالإضافة إلى توصيات أساسية لدعم الجهود المستقبلية.

ومنذ عام 2013، اعتمدت الدول المشاركة في منظمة الأمن والتعاون في أوروبا 16 تدبيرا لبناء الثقة في مجال الأمن السيبراني / تكنولوجيا المعلومات والاتصالات، مما جعل منظمة الأمن والتعاون في أوروبا أول منظمة إقليمية تضع مثل هذه التدابير. وتواصل منظمة الأمن والتعاون في أوروبا القيام بدورها الرائد في هذا الصدد، حيث تسلم عمليات الأمم المتحدة الأخيرة بشأن الأمن الدولي لتكنولوجيا المعلومات والاتصالات بأهمية المنظمات الإقليمية ودون الإقليمية في وضع وتنفيذ تدابير بناء الثقة في مناطقها.

من خلال التدبير الرابع عشر لبناء الثقة، أكدت الدول المشاركة في منظمة الأمن والتعاون في أوروبا على أهمية اتباع نهج لأصحاب المصلحة المتعددين إزاء أمن الفضاء الحاسوبي / تكنولوجيا المعلومات والاتصالات، ولا سيما عن طريق التعاون المنظم مع القطاع الخاص. هناك اعتراف واسع النطاق بأن هذا التعاون يمكن أن يزيد من القدرة على المرونة السيبرانية وتعزيز التأهب الوطني. وعلى الصعيد الدولي، يشكل تبادل الممارسات الجيدة والدروس المستفادة بشأن هذا الموضوع تمرينا لبناء الثقة والقدرات، وتتشرف إدارة التهديدات عبر الوطنية التابعة لمنظمة الأمن والتعاون في أوروبا بدعمه.

في منظمة الأمن والتعاون في أوروبا، شهدنا بالفعل عددا من هذه التبادلات البناءة. والواقع أن التدبير الرابع عشر لبناء الثقة حظي باهتمام واسع النطاق وبتنفيذ وطني كبير، كما يتضح من الأمثلة الملموسة للشراكات بين القطاعين العام والخاص في هذا التقرير. من خلال مبادرة "اعتماد تدابير بناء الثقة"، التي دشنها في عام 2018 رئيس الفريق العامل غير الرسمي المنشأ بموجب قرار المجلس الدائم رقم 1039، ترعى هذا التدبير مجموعة من ست دول مشاركة، كانت جهودها محورية في وضع هذا التقرير.

ويستند هذا التقرير إلى الدراسات السابقة التي أجرتها الدول المشاركة، والتي جمعت أمثلة على التعاون بين القطاعين العام والخاص في مجال الأمن السيبراني / تكنولوجيا المعلومات والاتصالات. يتناول التقرير هذه النتائج بمزيد من التفصيل من خلال سلسلة من المقابلات التي أجريت مع ممثلي القطاع العام المشاركين بنشاط في التعاون مع القطاع الخاص. ومن خلال تسليط الضوء على أمثلة للممارسات الناشئة ومناقشة الطرائق الملموسة للشراكات بين القطاعين العام والخاص، يأمل التقرير أن يكون بمثابة أداة لبناء قدرات الخبراء وواضعي السياسات وأن يدعم صياغة وتنفيذ السياسات الوطنية المتعلقة بالأمن السيبراني / تكنولوجيا المعلومات والاتصالات.

ألينا كوبتشينا

منسقة الأنشطة الرامية إلى
التصدي للتهديدات عبر الوطنية

أمانة منظمة الأمن والتعاون في أوروبا

موجز تنفيذي

تعتمد مجتمعات اليوم اعتمادا كبيرا على التقنيات الرقمية أو تتحول بطريقة تشير إلى مستويات أعلى من هذا الاعتماد مستقبلا. إن الأمن السيبراني / تكنولوجيا المعلومات والاتصالات والقدرة على المرونة سيظلان حاسمين للرفاه الاقتصادي والاجتماعي للمجتمعات وللأمن الوطني والدولي. في وقتنا الحاضر، قد يكون من الصعب على الحكومات أن تمتلك الوسائل والقدرات على الفهم الكامل للعدد المتزايد من التهديدات والتحديات المتعلقة بالأمن السيبراني التي تواجهها بلدانها والاستجابة لها. وكما هو الحال مع أشكال التبعيات الأخرى، تعتمد الحكومات بشكل متزايد على التعاون والتآزر مع القطاع الخاص والجهات الفاعلة غير الحكومية الأخرى للاستجابة لهذه التهديدات والتحديات، واحتياجات السياسة العامة والشواغل التي تنبع منها.

لقد أدرجت العديد من الحكومات تطلعات ذات صلة بالشراكات بين القطاعين العام والخاص وغيرها من الترتيبات المماثلة في سياساتها واستراتيجياتها الوطنية للأمن السيبراني. وقد ركزت هذه التطلعات في الأصل على مفهوم ضيق للأمن السيبراني ونموذج للعلاقات بين القطاعين العام والخاص تضمن فيه الإدارة الذاتية للسوق والصناعة الأمن السيبراني، في حين تضمن الحكومات الأسواق المفتوحة حتى يزدهر الابتكار. ومع ذلك، أكدت الزيادة في نطاق وحجم التهديدات بالتوازي مع الاعتماد المتزايد على التقنيات الرقمية على مدى العقدين الماضيين أن السوق والآليات الطوعية لا تنتج في حد ذاتها الأمن السيبراني، ناهيك عن القدرة على المرونة، ويمكن أن تتعارض مع الأمن القومي الأوسع والأهداف المجتمعية والمعيارية. وثمة نهج بديل يركز على إنشاء نظم تنظيمية ترتكز على المعايير والقواعد وإجراءات وممارسات الرقابة والإنفاذ. ومع ذلك، من الصعوبة بمكان إقامة مثل هذه الأنظمة في بيئة متغيرة باستمرار. وقد لا يتماشى الإفراط في التنظيم مع التهديدات الأمنية القائمة والناشئة على حد سواء، ويمكن أن يبطئ الابتكار أو يقوضه ويقلل من حوافز إشراك القطاع الخاص، كما يمكن أن يتعارض مع الالتزامات والواجبات الأخرى، بما في ذلك تلك التي تهدف إلى تقليل الضرر الذي يلحق بالجمهور. لذلك، أصبح تحقيق التوازن بين الاثنين أمرا حتميا للعديد من البلدان في سعيها للمشاركة مع القطاع الخاص في القضايا المتعلقة بالأمن السيبراني والقدرة على المرونة في السنوات الأخيرة. مرة أخرى، هذا ليس بالأمر السهل دائما لأن الدوافع والاهتمامات قد تختلف اختلافا كبيرا. وفي هذا الصدد، من الضروري ضمان أن تكون الشراكات بين القطاعين العام والخاص وغيرها من الترتيبات المماثلة مدعومة بمبادئ أساسية مثل الشفافية والمساءلة، ولا سيما عندما تنشأ لحل مشاكل محددة تتعلق بالسياسات العامة، يتوقف عليها الأمن الوطني أيضا.

كما يوضح هذا التقرير، لا يوجد هنالك نموذج واحد لكيفية عمل الجهات الفاعلة العامة والخاصة معا على الأمن السيبراني والقضايا المتعلقة بالمرونة. ويتأثر طابع الشراكات بين القطاعين العام والخاص وغيرها من الترتيبات المماثلة، وكيفية نشوئها وتنفيذها، بالنظام السياسي والاقتصادي والاجتماعي، فضلا

عن هيكل الحكم في كل دولة، كما أنها تتشكل من خلال طابع نظام البيئة الرقمية الوطنية للدولة، والذي يتأثر بدوره بمجموعة من القضايا، بما فيها مستوى التنمية الاقتصادية للدولة؛ وسياساتها المالية والتنظيمية والصناعية؛ ومستويات الاستثمار في البحث والتطوير؛ ونظام التعليم في كل دولة؛ والعديد من العوامل الأخرى.

في منطقة منظمة الأمن والتعاون في أوروبا، أقيمت ترتيبات تعاونية وجماعية لتحقيق طائفة واسعة من الأغراض: تبادل المعلومات المتعلقة بقطاعات أو مواضيع محددة أو المعلومات الاستخباراتية المتصلة بالتهديدات؛ كشف عن نقاط الضعف؛ استجابة لنوع معين من مشاكل الأمن السيبراني (على سبيل المثال، لمكافحة برامج الابتزاز، والتصيد الاحتيالي، والقضاء على شبكات البوتات)؛ إذكاء الوعي العام أو القطاعي / الخاص بالموضوع، والنظافة السيبرانية، وبناء القدرات، وللأغراض التعليمية. وتتراوح هذه بين الترتيبات الرسمية أو القائمة على العقود أو المنظمة بين القطاعين العام والخاص والشبكات أو المجموعات التعاونية الطوعية غير الرسمية. وطرائق تنفيذ هذه الترتيبات واسعة النطاق بنفس القدر.

وقد نشأت العديد من الترتيبات الحالية التي تمت مناقشتها في جميع أنحاء التقرير بشكل عضوي استجابة لمشهد تهديد الأمن السيبراني المتغير، وأحيانا بمبادرة من وكالة حكومية أو شركة حددت مشكلة معينة تتطلب حلا. وفي حالات أخرى، توفر الاستراتيجيات الوطنية للأمن السيبراني إطارا للتعاون والتآزر. وفي دول أخرى، تقتضي التشريعات أو اللوائح الوطنية من القطاع الخاص التعاون مع السلطات العامة. وهذه هي الحالة بشكل متزايد عندما يتعلق الأمر بالإبلاغ عن حوادث الأمن السيبراني التي تؤثر على شبكات وأنظمة القطاعات والخدمات الحيوية. وقد برز تحفيز المشاركة وبناء الثقة عبر الجهات الفاعلة والقطاعات كهدف وتحد في هذه العلاقات.

إن الاعتبار أن الشراكات بين القطاعين العام والخاص وغيرها من الترتيبات المماثلة قادرة على تعزيز الأمن السيبراني ومرونته ليس أمرا جديدا. الجديد في الأمر هو التفكير الناشئ في الكيفية التي يمكن بها تحقيق مكاسب إيجابية، ليس فقط لتلبية أهداف الأمن القومي الضيقة لفرادى البلدان، بل وأيضا لتحقيق أهداف أوسع نطاقا للمجتمع بأسره داخل الحدود الوطنية وخارجها.

وأخيرا، لاحظت بعض الدول المشاركة أن الدروس التي تم تبادلها بشأن تنفيذ التدبير الرابع عشر لبناء الثقة في إطار الفريق العامل غير الرسمي التابع لمنظمة الأمن والتعاون في أوروبا والمنشأ بموجب قرار المجلس الدائم رقم 1039، كانت مفيدة للغاية، حيث ساعدتها على صياغة مبادرات مماثلة في بلدانها، وإعادة تصميمها أو إعادة توجيهها. ويبين التقرير أن هناك شهية واضحة لدى معظم الدول المشاركة في مواصلة تبادل الممارسات والدروس الناشئة بشأن الشراكات بين القطاعين العام والخاص المتعلقة بالأمن السيبراني وغيرها من الترتيبات المماثلة في إطار منظمة الأمن والتعاون في أوروبا، طالما أن هذه الأمثلة والدروس تبقى محددة المواضيع، وتركز على النتائج العملية، وتشمل كلا من الجهات الفاعلة العامة والخاصة المشاركة في الأمثلة التي يتم تقاسمها، حسب الاقتضاء.

مع أخذ هذه الملاحظة الأخيرة في الاعتبار، يعرض التقرير الممارسات والدروس الناشئة كتوصيات أساسية وينظمها تحت عناوين الغرض والسياسة والعملية والناس، كما يقترح تناولها في إطار مزيد من عمليات التبادل فيما بين الدول المشاركة في منظمة الأمن والتعاون في أوروبا وبين منظمة الأمن والتعاون في أوروبا والمناطق الأخرى تمشيا مع روح ومقاصد تدابير بناء الثقة في مجال الأمن السيبراني / تكنولوجيا المعلومات والاتصالات التي وضعتها منظمة الأمن والتعاون في أوروبا، ولا سيما التدبير الرابع عشر لبناء الثقة. ويمكن تنظيم هذه المناقشات حول مواضيع حددتها الدول المشاركة في منظمة الأمن والتعاون في أوروبا لمزيد من المناقشة، وهي تشمل التبادل في المجالات التالية.

كيفية قيام الدول المشاركة الأخرى وكذلك الحكومات في المناطق الأخرى بإنشاء علاقات تعاونية مع شركات صغيرة ومتوسطة أو معاهد بحوث أو قطاعات محددة من الهياكل الأساسية الحيوية، والحفاظ عليها؛

منصات موثوقة وآمنة لتبادل المعلومات؛

قدرات الاستجابة السريعة؛

هياكل المساءلة التحفيزية في الشراكات بين القطاعين العام والخاص المتعلقة بالأمن السيبراني؛

رصد هذه الترتيبات والإشراف عليها.

الغرض

ينبغي أن يكون للشراكات بين القطاعين العام والخاص المتعلقة بالأمن السيبراني وغيرها من الترتيبات المماثلة غرض محدد بوضوح.

السياسات

ينبغي تحديد الشراكات بين القطاعين العام والخاص المتعلقة بالأمن السيبراني وغيرها من الترتيبات المماثلة بوضوح في السياسات و/أو التشريعات الوطنية.

العملية

تتطلب الشراكات بين القطاعين العام والخاص المتعلقة بالأمن السيبراني وغيرها من الترتيبات المماثلة طرائق تنفيذ واضحة أو هياكل حوكمة للمساعدة في ضمان تحقيق الأهداف والنظر في هياكل المساءلة التحفيزية المناسبة منذ البداية.

الناس

تتطلب الشراكات بين القطاعين العام والخاص المتعلقة بالأمن السيبراني وغيرها من الترتيبات المماثلة الوضوح بشأن من ينبغي إشراكه ولأي غرض.

خلفية ومقدمة

تمشيا مع التدبير الرابع عشر لبناء الثقة الصادر عن منظمة الأمن والتعاون في أوروبا، "تقوم الدول المشاركة، على أساس طوعي وبما يتسق مع التشريعات الوطنية، بتعزيز الشراكات بين القطاعين العام والخاص ووضع آليات لتبادل أفضل الممارسات في الاستجابات للتحديات الأمنية المشتركة الناشئة عن استخدام تكنولوجيا المعلومات والاتصالات"[1]. وفي عام 2021، أطلق فريق منظمة الأمن والتعاون في أوروبا المعني بالتدبير الرابع عشر لبناء الثقة[2] دراسة لتحديد مستوى انشغال الدول المشاركة في منظمة الأمن والتعاون في أوروبا في هذه الآلية المحددة لبناء الثقة[3].

يستند هذا التقرير إلى تلك الدراسة والتقرير المصاحب الذي تم تقاسمه مع الدول المشاركة لتقديم لمحة عامة عن الممارسات الناشئة في التعاون بين القطاعين العام والخاص فيما يتعلق بالأمن السيبراني في دول منظمة الأمن والتعاون في أوروبا. كما أنه يعتمد على سلسلة إضافية من 23 مقابلة مع الدول المشاركة أجريت بين يوليو / تموز وأكتوبر / تشرين الأول 2022، فضلا عن استعراض الوثائق المتاحة للجمهور المشار إليها خلال المقابلات.

كثيرا ما يُستخدم مصطلح "الترتيبات بين القطاعين العام والخاص" في جميع أجزاء التقرير بدلا من مصطلح "الشراكات بين القطاعين العام والخاص". ويسترشد هذا القرار بالمقابلات التي أجريت مع الدول المشاركة وبتقديماتها بشأن الممارسات الحالية ذات الصلة بالتدبير الرابع عشر لبناء الثقة: ففي حين تفضل بعض الدول استخدام مصطلح "الشراكات بين القطاعين العام والخاص" لأنه منصوص عليه في قوانينها وسياساتها الوطنية، فإن بديله بالنسبة لدول أخرى يجسد بشكل أكثر ملاءمة مجموعة واسعة من النماذج العلائقية التي تشمل الجهات الفاعلة العامة والخاصة المعززة للتعاون والتآزر بهدف التصدي لتهديدات الأمن السيبراني التي تؤثر على الاقتصادات والمجتمعات وأمن الدول المشاركة في منظمة الأمن والتعاون في أوروبا.

وأخيرا، فإن الآراء الواردة في التقرير هي أساسا وجهات نظر أصحاب المصلحة الحكوميين، الذين اعترفوا جميعا بالحاجة إلى إشراك الجهات الفاعلة الخاصة في الأعمال المقبلة على هذا الموضوع، بما في ذلك في عمليات التبادل ذات الصلة بشأن التدبير الرابع عشر لبناء الثقة في منظمة الأمن والتعاون في أوروبا.

1 قرار المجلس الدائم لمنظمة الأمن والتعاون في أوروبا رقم 1202، 10 مارس / آذار 2016: https://www.osce.org/pc/227281

2 يتألف فريق منظمة الأمن والتعاون في أوروبا المعني بالتدبير الرابع عشر لبناء الثقة حاليا من: النمسا وبلجيكا وإستونيا وفنلندا وإيطاليا والسويد. تناصر هذه الدول إدراج التدبير الرابع عشر لبناء الثقة في إطار مبادرة "اعتماد تدابير بناء الثقة". وقد أطلق المبادرة في عام 2018 رئيس الفريق العامل غير الرسمي التابع لمنظمة الأمن والتعاون في أوروبا المنشأ بموجب قرار المجلس الدائم رقم 1039 لتعزيز ملكية فرادى تدابير بناء الثقة من قبل الدول المشاركة المهتمة لاستكشاف طرائق ملموسة لتنفيذها.

3 PC.CBM/3/21 "تقرير بشأن الأفكار الرئيسية المستمدة من استبيان التدبير الرابع عشر لبناء الثقة في مجال الأمن السيبراني / تكنولوجيا المعلومات والاتصالات لمنظمة الأمن والتعاون في أوروبا بشأن الشراكات بين القطاعين العام والخاص"، عُمم في 10 سبتمبر / أيلول 2021.

النتائج الرئيسية

الغرض (العام)

ينبغي أن يكون للشراكات بين القطاعين العام والخاص المتعلقة بالأمن السيبراني وغيرها من الترتيبات المماثلة غرض محدد بوضوح. ويتطلب ذلك الآتي:

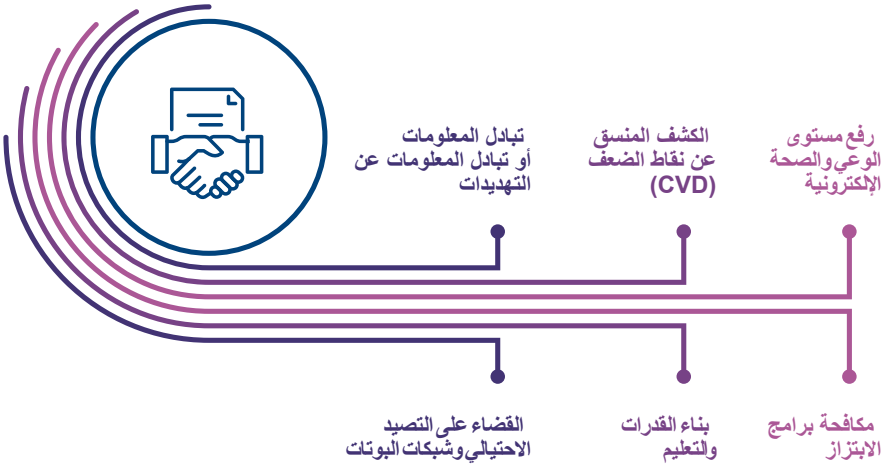
- فهم واضح للنظام البيئي الوطني للأمن السيبراني.
- فهم واضح لنقاط القوة والضعف في كيانات القطاعين العام والخاص ذات الصلة في الدولة مقابل تحديات الأمن السيبراني والقدرة على المرونة والتي تحتاج إلى معالجة.
- تحديد المجالات التي يمكن أن يعالج فيها التعاون بين القطاعين العام والخاص التحديات المحددة.
- تحديد كيفية تحفيز مشاركة القطاع الخاص ذي الصلة والجهات الفاعلة الأخرى.
- تحديد ما إذا كانت هناك حاجة إلى إنشاء منصب حكومي مخصص لتسهيل أو تنسيق العلاقات بين القطاعين العام والخاص.

حاليا، تنطوي الاستجابة لتهديدات الأمن السيبراني على فهم واضح لنطاق وحجم التهديدات والتحديات والمرونة المتصلة بالأمن السيبراني والتي تواجهها البلاد وتحديد أهداف واضحة. يُنظر بشكل متزايد إلى التعاون والتآزر عبر القطاعات على أنهما نهج فعال لتحقيق هذه الأهداف، لأسباب ليس أقلها أن الجهات الفاعلة الخاصة تطور وتمتلك العديد من التقنيات والمنتجات والخدمات التي تعتمد عليها رفاهية المجتمع ولديها رؤى يمكن أن تختلف اختلافا كبيرا عن تلك الخاصة بالوكالات الحكومية.

هناك اعتراف عبر العديد من الدول المشاركة في منظمة الأمن والتعاون في أوروبا بأنه بينما تضع الحكومات السياسة والقانون، فإنها وحدها قد لا تكون قادرة على تحديد نطاق وحجم التحديات المتعلقة بالأمن السيبراني والاهتمام بها، كما لا تغطي تكاليف القيام بذلك. تعد حوادث الأمن السيبراني الكبيرة الأخيرة وآثارها غير المباشرة على الشركات والمجتمعات في جميع أنحاء العالم تذكيرا مهما بالحاجة إلى الشراكات وغيرها من أشكال التعاون مع القطاع الخاص ومع الجهات الفاعلة الأخرى.

ومن الواضح أن كيانات القطاع الخاص لا يمكن أن تحل محل دور السلطات الحكومية فيما يتعلق بالأمن الوطني والسلامة العامة وغيرها من المنافع العمومية، ولكنها تستطيع أن تسهم بشكل إيجابي في تحقيق تلك الأهداف. ومع ذلك، فإن دوافعها وحوافزها لا تتماشى دائما مع دوافع وحوافز الحكومات. وقد تكون هذه الاختلالات إشكالية بشكل خاص عندما يتعلق الأمر بالأمن القومي والسلامة العامة، لأن الجهات الفاعلة في الصناعة غالبا ما تكون مترددة في استثمار الموارد التي تتجاوز احتياجاتها التجارية الفورية أو في مبادرات قد تزيد التكاليف وتقوض أنشطتها التجارية وتشكل مخاطر على سمعتها. ومن جانبها، قد لا تقدم الحكومات الحوافز اللازمة لضمان المشاركة ذات مغزى للجهات الفاعلة الخاصة. ويمثل ذلك إشكالية خاصة عندما يتعلق الأمر بتبادل البيانات أو المعلومات الاستخباراتية المتصلة بالتهديدات. كما هو الحال في مجالات السياسة العامة الأخرى، تأتي هذه العلاقات مع العديد من الفوائد والمقايضات، وقد تستغرق وقتا لرعايتها ويمكن أن تنطلق على أساس الثقة المحدودة.

كما يتضح في جميع أجزاء التقرير، أقيمت في منطقة منظمة الأمن والتعاون في أوروبا شراكات بين القطاعين العام والخاص وغيرها من الترتيبات المماثلة لباقة واسعة من الأغراض: لتبادل البيانات أو المعلومات الاستخباراتية المتعلقة بالتهديدات في قطاع أو موضوع محدد؛ والكشف المنسق عن نقاط



الضعف؛ وللاستجابة لنوع معين من مشاكل الأمن السيبراني (على سبيل المثال، لمكافحة برمجيات الابتزاز، والتصيد الاحتيالي، والقضاء على شبكات البوتات)؛ لزيادة الوعي العام أو القطاعي/الخاص، والنظافة السيبرانية، وبناء القدرات والأغراض التعليمية. وتتراوح شراكات القطاعين العام والخاص هذه بين الرسمية أو القائمة على العقود أو المنظمة وبين غير الرسمية أو التعاونية الطوعية أو القائمة على مجموعات. طرائق تنفيذ هذه الترتيبات واسعة النطاق بنفس القدر[4]. في الفصول التالية، يتناول التقرير أمثلة عملية للشراكات بين القطاعين العام والخاص وغيرها من الترتيبات المماثلة من منطقة منظمة الأمن والتعاون في أوروبا مع الإشارة إلى هذه الأغراض المذكورة.

ينطوي التعامل مع الأمن السيبراني من منظور تعاوني مشترك ومبني على فهم عميق للنظام البيئي للأمن السيبراني في الدولة ونقاط القوة والضعف في كيانات القطاعين العام والخاص ذات الصلة مقابل تحديات الأمن السيبراني والمرونة التي تحتاج إلى معالجة. ويشمل ذلك أيضا فهم كيفية استفادة جميع أصحاب المصلحة المعنيين من التعاون، بطريقة تضمن أن الصالح العام هو في نفس الوقت المحرك والهدف للتعاون. على سبيل المثال، قد تستفيد الحكومات التي تتعامل مع القطاع الخاص من موارد القطاع الخاص وخبراته ورؤيته للتصدي لتهديدات الأمن السيبراني التي تمنعها من تحقيق أهداف السياسة العامة. بالنسبة للدول ذات الموارد المحدودة، قد يغير هذا قواعد اللعبة. وتستفيد كيانات القطاع الخاص من خلال الوصول إلى معلومات التهديدات التي يمكن أن تساعدها على حماية أعمالها. وبالنسبة للشركات الصغيرة والمتوسطة، قد يساعد التعاون مع القطاع العام في تأمين المزيد من الموارد والمهارات والدعم للاستجابة للحوادث والتعافي منها. خلال الجائحة، أثبتت الزيادة في أشكال التعاون هذه قيمتها الهائلة، وفي بعض الحالات، أتاحت للشركات الصغيرة والمتوسطة فرصة للمساعدة في تشكيل السياسات واللوائح المتعلقة بالأمن السيبراني، فضلا عن هياكل الحوافز داخل قطاعاتها.

4 PC.CBM/4/21 "مشاريع التدبير الرابع عشر لبناء الثقة، من الاستيان"، عُمم في 6 ديسمبر / كانون الأول 2021.

السياسات

ينبغي تحديد الشراكات بين القطاعين العام والخاص المتعلقة بالأمن السيبراني وغيرها من الترتيبات المماثلة بوضوح في السياسات و/أو التشريعات الوطنية، ويتطلب ذلك الآتي:

- الإقرار بأهمية الترتيبات بين القطاعين العام والخاص في السياسة والاستراتيجية الوطنية للأمن السيبراني، بما في ذلك من خلال إبراز كيفية مساهمة الترتيب في تحقيق أهداف الأمن الوطني والتنمية الاقتصادية والاجتماعية، التي يمكن إدراج تفاصيلها في خطط العمل ذات الصلة.
- التشاور مع الكيانات الخاصة ذات الصلة في القرارات السياسية والتشريعية والتنظيمية التي ستؤثر عليها.
- الالتزام بإنشاء آليات الشفافية والرقابة للترتيبات بين القطاعين العام والخاص والأنشطة ذات الصلة.

تبرز الدول المشاركة في منظمة الأمن والتعاون في أوروبا بصورة متزايدة أهمية العمل مع كيانات القطاع الخاص بشأن مسائل أمن الفضاء الحاسوبي في التشريعات والسياسات والاستراتيجيات المحلية. وترسخ بعض الدول المشاركة انشغالها مع القطاع الخاص في تشريعاتها الوطنية، وتستخدم الدول الكثيرة الأخرى أدوات السياسة العامة لهذا الغرض. يتضح ذلك في عدد الاستراتيجيات الوطنية للأمن السيبراني التي تتضمن أحكاما بشأن التعاون بين القطاعين العام والخاص، والتي تغطي عموما فرص التعاون مع القطاع الخاص من أجل الاقتصاد والمجتمع والمصلحة الوطنية العامة. توفر هذه الأحكام الأساس المنطقي - القائم على القيمة في بعض الأحيان - لمثل هذا التعاون.

أمثلة على المراجع حول الشراكات بين القطاعين العام والخاص وغيرها من الترتيبات المماثلة في الاستراتيجيات الوطنية للأمن السيبراني للدول المشاركة في منظمة الأمن والتعاون في أوروبا

ألبانيا، الاستراتيجية الوطنية للأمن السيبراني (2020-2025)

"التنسيق والتعاون بين جميع الجهات الفاعلة هما العنصر الأساسي لضمان النجاح. ينبغي تعزيز التعاون مع القطاع الخاص بسبب دينامية التطور السريع لتكنولوجيا المعلومات والاتصالات. لا يمكن تعزيز أمن تكنولوجيا المعلومات والاتصالات وتطويرها في إدارة الدولة إلا بالتعاون الوثيق والاتساق مع التطورات والاتجاهات التكنولوجية".

الجمهورية التشيكية، الاستراتيجية الوطنية للأمن السيبراني (2021-2025)

"ينطوي ضمان الأمن السيبراني على التنسيق بين العديد من الدول والهيئات غير الحكومية لتمكين الجمهورية التشيكية من مواجهة التحديات والتهديدات الأكثر خطورة وتعقيدا بشكل فعال. من الضروري اتباع نهج وطني مشترك ومتكامل لتوفير الأمن في الفضاء السيبراني ومكافحة التهديدات السيبرانية. (...) ومع ذلك، فإن ترك الأمن السيبراني للدولة التشيكية فقط لا يكفي. كل مؤسسة وشركة خاصة وفرد له دوره ويمكنه المساهمة بشكل إيجابي في الأمن السيبراني. لذلك يجب على جمهورية التشيك وضع ودعم سياسة الأمن السيبراني التي ستدمج باستمرار المجتمع بأسره في عمليات الأمن السيبراني وهذا يزيد من قدرتها على المرونة في مواجهة التهديدات السيبرانية".

الدنمارك، الاستراتيجية الوطنية للأمن السيبراني والمعلومات (2022-2024)

"من خلال عدد من الإجراءات الملموسة في الاستراتيجية، تعمل الحكومة على تعزيز التعاون بين القطاعين العام والخاص في مجال الأمن السيبراني وأمن المعلومات. وتضمن المبادرات فرصا أفضل لتبادل المعرفة والخبرات، وتعزز الجهود الاستشارية تجاه السلطات العامة والشركات والمواطنين، وتساهم في القدرة التنافسية للشركات الدنماركية من خلال أدوات ملموسة".

إستونيا، استراتيجية الأمن السيبراني (2019-2022)

"سنحافظ على مجتمع نشط ومتماسك للأمن السيبراني. وللقيام بذلك، سنقدم تدفقات المعلومات التقنية، وننظم تمارين مشتركة، ونشرك القطاع الخاص والكفاءة الأكاديمية في عمليات الصياغة التشريعية والتخطيط الاستراتيجي. (...) سندعم التعاون الفعال بين الدولة والأوساط الأكاديمية والشركاء الرئيسيين للقطاع الخاص. وتحقيقا لهذه الغاية، سنطلق مجموعة تسهل التعاون المحلي والدولي".

استراتيجية فنلندا للأمن السيبراني (2019)

"يتطلب الاستعداد للأمن السيبراني التعاون بين مختلف الجهات الفاعلة في المجتمع والحكومة المركزية ومجتمع الأعمال بالإضافة إلى تعزيز المهارات في مختلف القطاعات. يتطلب الترابط في بيئة التشغيل الرقمية بنية شاملة تأخذ الأمن السيبراني في الاعتبار. وتتطلب استمرارية العمليات والتأهب للحوادث خبرة في المشتريات والمناقصات وتقييم تنفيذ الالتزامات التعاقدية والإدارة الشاملة لشبكة الموردين وسلاسل التوريد. (...) سيتم بناء الأمن السيبراني الوطني بالتعاون بين السلطات ومجتمع الأعمال والمنظمات والمواطنين، عندما يمكن للجميع المساهمة في أمننا السيبراني المشترك".

إيطاليا، الاستراتيجية الوطنية للأمن السيبراني (2022-2026)

"ما يستعرض (...) أهداف الحماية والاستجابة والتنمية، وكذلك العوامل التمكينية للتدريب وتعزيز ثقافة الأمن السيبراني والتعاون، هو الشراكة بين القطاعين العام والخاص (PPP) التي تتخلل تماما هذه الاستراتيجية [التي] تستند (...) إلى نهج "المجتمع بأكمله" الذي يعمل فيه القطاع العام بالتآزر مع الصناعة والمجتمع المدني والأوساط الأكاديمية والبحوث، وكذلك وسائل الإعلام والأسر والأفراد، لتعزيز المرونة السيبرانية للبلد والمجتمع ككل. وعلاوة على ذلك، يتألف الفضاء السيبراني من منتجات وخدمات تكنولوجيا المعلومات والاتصالات التي تنتجها أو تقدمها كيانات خاصة أساسا. ولهذا السبب، لا يمكن لهذه الاستراتيجية أن تستبعد التعاون الوثيق والتشاور المستمر بين القطاعين العام والخاص الذي يترجم إلى سلسلة من الإجراءات المنظمة، مثل مراقبة الفضاء السيبراني من خلال تعاون مراكز العمليات الأمنية (SOC)، والتخفيف من حدة الحوادث من خلال تعاون فرق CSIRT والاستجابة المؤهلة للحوادث، وشبكة مختبرات التجربة، فضلا عن التدريب ونشر الوعي".

سلوفاكيا، الاستراتيجية الوطنية للأمن السيبراني (2021-2025)

"الأمن بشكل عام هو أحد المصالح الأساسية لأي دولة ديمقراطية يسود فيها القانون. مجال الأمن السيبراني ليس استثناء، وهو أكثر عولمة لأن الهجمات الإلكترونية لا تعترف بالحدود الوطنية ولا يلزم أن يكون المهاجمون مواطنين في نفس البلد الذي نشأ منه الهجوم. لذلك، من المهم جدا أن تنشئ الدولة شراكات قوية للغاية على المستوى الدولي، وتتبادل الخبرات والمعرفة والمعلومات، ثم تطبقها بعد ذلك على المستوى الوطني. ويضمن التعاون وبناء الثقة بين كيانات الإدارة العامة والقطاع الخاص والأوساط الأكاديمية تطوير الأمن السيبراني".

جمهورية صربيا، الاستراتيجية الوطنية لمجتمع المعلومات وتنمية الأمن (2021-2026)

"يعد التعاون بين القطاعين العام والخاص أحد العناصر الرئيسية لأمن المعلومات في كل دولة. وعلى وجه التحديد، فإن القيود الموجودة على كلا الجانبين في الاستجابة لتحديات أمن المعلومات تفرض الحاجة إلى إقامة شراكات، لا سيما في حالة تعرض الحوادث أمن المعلومات للخطر بشكل كبير. في إطار الشراكة بين القطاعين العام والخاص، فإن إيجاد آلية مناسبة للتعاون ليس هو القضية الوحيدة؛ بدلا من ذلك، هناك أيضا مسألة خلق الثقة بينهما والتي ستساهم في تعزيز القدرات وزيادة مستوى أمن المعلومات".

تركيا، الاستراتيجية الوطنية للأمن السيبراني (2020-2023)

"من خلال إنشاء شبكة عضوية للأمن السيبراني، تهدف إلى تطوير جهود تعاونية حيث يمكن للأشخاص من جميع الشرائح الذين يعملون أو المهتمين بمجال الأمن السيبراني تبادل المعرفة والخبرات. (...) ومن الأهمية بمكان زيادة تبادل المعرفة بين المؤسسات العامة والقطاع الخاص فيما يتعلق بالتهديدات السيبرانية وتكوين روابط جديدة مع أصحاب المصلحة، وخاصة الجيل الشاب الذي لديه دراسات في مجال الأمن السيبراني".

المملكة المتحدة، الاستراتيجية الوطنية للأمن السيبراني (2022)

"سيكون من الأمور المركزية في استراتيجيتنا اتباع نهج يشمل المجتمع بأسره تجاه الإنترنت. نحن بحاجة إلى بناء شراكة دائمة ومتوازنة عبر القطاعين العام والخاص والقطاع الثالث، حيث يلعب كل منها دورا مهما في جهودنا الوطنية".

وزارة الأمن الداخلي الأمريكية، استراتيجية الأمن السيبراني (2018-2023)

"كان نمو الإنترنت وتطوره مدفوعا في المقام الأول من قبل القطاع الخاص وأمن الفضاء السيبراني هو تحد شامل بطبيعته. لتحقيق أهداف الأمن السيبراني الخاصة بنا، يجب أن نعمل بطريقة تعاونية عبر مكوناتنا ومع الشركاء الفيدراليين وغير الفيدراليين الآخرين.

الاتحاد الأوروبي، توجيه (NIS2 2022)

"تستطيع الشراكات بين القطاعين العام والخاص (PPP) في مجال الأمن السيبراني أن توفر إطارا مناسبا لتبادل المعرفة ومشاركة أفضل الممارسات وإنشاء مستوى مشترك من التفاهم بين أصحاب المصلحة. ينبغي للدول الأعضاء أن تعزز السياسات التي يقوم عليها إنشاء شراكات بين القطاعين العام والخاص بمجال الأمن السيبراني. ويجب أن توضح هذه السياسات، في جملة أمور، النطاق وأصحاب المصلحة المعنيين، ونموذج الإدارة، وخيارات التمويل المتاحة، والتفاعل بين أصحاب المصلحة المشاركين فيما يتعلق بالشراكات بين القطاعين العام والخاص. ويمكن للشراكات بين القطاعين العام والخاص الاستفادة من خبرة كيانات القطاع الخاص لمساعدة السلطات المختصة في تطوير أحدث الخدمات والعمليات، بما في ذلك تبادل المعلومات، والإنذار المبكر، والتهديدات السيبرانية والتدريبات على الحوادث، وإدارة الأزمات والتخطيط للقدرة على المرونة".

غالبا ما تتضمن خطط العمل المرتبطة تفسيرات لكيفية مساهمة هذه التطلعات في زيادة الأمن السيبراني والقدرة على المرونة، وتقدم مزيدا من التفاصيل بشأن المجالات الرئيسية للتعاون مثل تبادل البيانات / المعلومات الاستخباراتية للتهديدات، بما في ذلك:

- حول حماية البنية التحتية الحيوية؛
- الإنذار المبكر؛
- التعليم؛
- تنمية القوى العاملة؛
- الارتقاء بالمهارات والبحث والتطوير المتعلق بالأمن السيبراني؛
- النمو والابتكار.

وفي معظم الحالات، أجرت الدول المشاركة في منظمة الأمن والتعاون في أوروبا مشاورات مع الجهات الفاعلة الخاصة في عملية وضع استراتيجيتها الوطنية لأمن الفضاء الحاسوبي. هذا تطور مهم منذ عقد واحد فقط.

في بعض الأحيان، يمكن أن يحدث هذا التعاون في مرحلة تطوير خطة العمل. ففي كازاخستان، على سبيل المثال، أنشئ فريق عامل يضم مجموعة واسعة من الجهات الفاعلة بما في ذلك الرابطات المهنية والصناعية، ومؤسسات التعليم العالي، والصناعة "لتحليل حالة المعلوماتية في الوكالات الحكومية، وأتمتة الخدمات العامة، وآفاق الاقتصاد الرقمي، وتحديث عمليات الإنتاج، بهدف توسيع نطاق خدمات تكنولوجيا المعلومات والاتصالات"[5]. كما درس التجارب الدولية في حماية البنية التحتية الوطنية لتكنولوجيا المعلومات والاتصالات. ويجري حاليا تنفيذ خطة العمل الناتجة عن ذلك.

وتنشئ بعض الدول المشاركة في منظمة الأمن والتعاون في أوروبا أيضا هيئات محددة مشتركة بين القطاعين العام والخاص لمرافقة تنفيذ استراتيجيتها للأمن الحاسوبي. ويعد **المجلس الاستشاري السيبراني الوطني في المملكة المتحدة** أحد الأمثلة على ذلك، حيث تم إنشاؤه لضمان تعرّف الحكومة على وجهات نظر وشبكات بديلة من جميع أنحاء النظام البيئي السيبراني الوطني، "لدعم التسليم عبر جميع الركائز الخمس للاستراتيجية"[6].

تساعد هذه الجهود الاستشارية على ضمان أن تكون الاستراتيجيات شاملة وأن تعكس تنوع القضايا التي يتعين معالجتها وتنوع أصوات أصحاب المصلحة المعنيين. كما يساعد ذلك على تعزيز شرعية الاستراتيجية وطرائق تنفيذها وإدارة التوقعات.

هناك تطورات أخرى متصلة بالسياسات واضحة في دول منظمة الأمن والتعاون في أوروبا. على سبيل المثال، شهدت السنوات القليلة الماضية تحولا في السياسات في بعض الولايات القضائية فيما يتعلق بما إذا كان التنظيم قادرا على الإسهام في تعزيز الأمن السيبراني والمرونة، وكيفية القيام بذلك. وخلافا لقاعدة ترك الأمن السيبراني لقوى التصحيح الذاتي للسوق وللتدابير الصناعية الطوعية، تتطلع الحكومات بشكل متزايد إلى تنظيم ممارسات الأمن السيبراني للكيانات التي ينظر إليها على أنها حاسمة لتمكين أرباح التحول الرقمي، وللأمن القومي. فعلى سبيل المثال، وبسبب زيادة التهديدات السيبرانية، سنت عدة دول مشاركة أو هي بصدد سن قواعد تتطلب من الكيانات داخل قطاعات معينة الإبلاغ عن حوادث الأمن السيبراني الخطيرة التي تؤثر على شبكاتها وأنظمتها وتبادل المعلومات بانتظام. وقد تواجه هذه الجهود مقاومة. ومع ذلك، فإن العمليات التشاورية الشفافة بشأن القواعد الجديدة، بما في ذلك هياكل المساءلة التحفيزية، والترتيبات بين القطاعين العام والخاص لمرافقة تطوير القواعد الجديدة فضلاً عن تنفيذها، يمكن أن تساعد في تهدئة الشواغل.

5 https://www.itu.int/hub/2022/08/implementing-kazakhstan-cybersecurity/

6 https://www.gov.uk/government/news/cabinet-office-appoints-national-cyber-advisory-board-co-chair

بالنسبة لأعضاء الاتحاد الأوروبي **(EU)**، تم إدخال متطلبات الإبلاغ وتبادل المعلومات في توجيه أمن الشبكات والمعلومات (NIS) لعام 2016. يهدف **التوجيه المنقح (NIS2)** إلى تعزيز تدابير إدارة مخاطر الأمن السيبراني الحالية والتزامات الإبلاغ عبر القطاعات التي تقع ضمن نطاق التوجيه (الطاقة والنقل والخدمات المصرفية والبنى التحتية للأسواق المالية ومياه الشرب والرعاية الصحية والبنية التحتية الرقمية). تحقيقا لهذه الغاية، فإن التوجيه المنقح "(...) ينص على أن تضع الدول الأعضاء التزامات لإدارة مخاطر الأمن السيبراني والإبلاغ عنها للكيانات المشار إليها ككيانات أساسية في المرفق الأول والكيانات المهمة في المرفق الثاني. (ج) ينص على أن تضع الدول الأعضاء التزامات بشأن تقاسم المعلومات المتعلقة بالأمن السيبراني" [7]. وشمل استعراض التوجيه إجراء مشاورات مع طائفة واسعة من أصحاب المصلحة من خلال أشكال مختلفة تشمل المشاورات المفتوحة وحلقات العمل والزيارات المحلية والمقابلات. من المتوقع أن تعمل هيئة التنسيق - مجموعة التعاون - كمنتدى للتواصل مع أصحاب المصلحة من القطاع الخاص من جميع أنحاء الاتحاد الأوروبي حول أنشطة المجموعة والتحديات التي قد تنشأ حول تنفيذ NIS2.

في **الولايات المتحدة، يضع قانون الإبلاغ عن الحوادث السيبرانية للبنية التحتية الحرجة** لعام 2022 (CIRCIA) الأساس للوكالة الوطنية لأمن البنية السيبرانية والتحتية (CISA) "لتطوير وتنفيذ اللوائح التي تتطلب من الكيانات المشمولة الإبلاغ عن الحوادث السيبرانية المغطاة ومدفوعات برامج الابتزاز إلى CISA". والهدف من هذه التقارير هو تمكين الوكالة من نشر الموارد بسرعة وتقديم المساعدة للضحايا الذين يعانون من الهجمات. ومن المتوقع أيضا أن تساعد CISA على تعزيز قدراتها الحالية لتحديد الاتجاهات، وتبادل المعلومات بسرعة مع المدافعين عن الشبكة لتحذير الضحايا المحتملين الآخرين. ويتطلب القانون أيضا من الوكالة أن تتشاور مع مجموعة واسعة من الكيانات العامة طوال عملية وضع القواعد، وقد التزم بتلقي مدخلات من الجهات الفاعلة الخاصة التي ستغطيها اللوائح. وإلى أن يتم الانتهاء من عملية وضع قواعد CIRCIA ودخول متطلبات الإبلاغ حيز التنفيذ، شجعت CISA الإبلاغ الطوعي من قبل الكيانات ذات الصلة، بما في ذلك من خلال الشراكات القائمة في مجال الاستخبارات المتعلقة بالتهديدات وتبادل المعلومات.

7 ينطبق التوجيه على الكيانات الأساسية العامة أو الخاصة العاملة في مجال الطاقة؛ والنقل؛ والخدمات المصرفية؛ والبنى التحتية للأسواق المالية؛ والصحة، ومياه الشرب؛ ومياه الصرف الصحي؛ والبنية التحتية الرقمية؛ والإدارة العامة وقطاعات الفضاء وبعض الكيانات الهامة العاملة في قطاعات أخرى بما في ذلك خدمات البريد والبريد السريع؛ وإدارة النفايات؛ وتصنيع وإنتاج وتوزيع المواد الكيميائية؛ وإنتاج الأغذية وتجهيزها وتوزيعها؛ والتصنيع ومقدمو الخدمات الرقمية:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020PC0823

العملية

تتطلب الشراكات بين القطاعين العام والخاص المتعلقة بالأمن السيبراني وغيرها من الترتيبات المماثلة طرائق تنفيذ واضحة أو هياكل الإدارة للمساعدة في ضمان تحقيق الأهداف والنظر في هياكل المساءلة التحفيزية المناسبة منذ البداية. ويشمل ذلك التأكيد المشترك من قبل الجهات الفاعلة العامة والخاصة المعنية على:

- الأهداف المحددة للترتيب والمشاكل المحددة التي يشرع في حلها.
- الأنشطة التي سيضطلع بها الترتيب لتحقيق الأهداف المتفق عليها.
- العمر الافتراضي ومصادر التمويل.
- متطلبات وبروتوكولات الأمن أو عدم الإفصاح التي يجب وضعها وممارسات النظافة السيبرانية التي يجب الترويج لها بين المشاركين.
- آليات للرصد والإشراف على الأنشطة المضطلع بها.
- آليات لمراجعة وتحديث طرائق التنفيذ أو هياكل الإدارة للشراكة بين القطاعين العام والخاص/الترتيب.
- استراتيجية الاتصالات/التوعية.

وكما سبقت الإشارة، قد تحدد استراتيجية وطنية للأمن السيبراني الخطوط العريضة للتعاون بين القطاعين العام والخاص. وبالإضافة إلى تحديد الغرض من ترتيب معين بين القطاعين العام والخاص، سيحتاج مؤيدوه أيضا إلى اقتراح *الكيفية* التي يعتزم بها تحقيق الأهداف المذكورة.

هيكل الإدارة / طرائق التنفيذ

لا يوجد نموذج إدارة واحد للشراكة بين القطاعين العام والخاص التي تتعلق بالأمن السيبراني أو أي ترتيب آخر من هذا القبيل. ويسترشد النموذج عموما بالسياق، بما في ذلك النظام السياسي والاقتصادي وهيكل الحكم في دولة معينة، فضلا عن طبيعة المشكلة أو المسألة التي يتعين حلها، أي الغرض الفعلي منها. وهذا يجعل من الصعب اقتراح تعريف عام أو مخطط لإنشائها. ومع ذلك، هناك قواسم مشتركة بين معظم الترتيبات بين القطاعين العام والخاص المحددة في التقرير، ولا سيما أن هناك ميلا إلى الوضوح حول نطاقها، وأصحاب المصلحة المعنيين، وطرائق التنفيذ أو هياكل إدارة الترتيبات - التي تتراوح بين الترتيبات العالية التنظيم وتلك غير الرسمية. ويتطلب العديد منها أيضا أشكالا موثوقة وآمنة من المشاركة والتواصل. حيث يبدو أن هناك تركيزا أقل في جميع الأمثلة على كيفية قيام الدول المشاركة برصد وتقييم مساهمة هذه الترتيبات في أهداف الأمن السيبراني والقدرة على المرونة الأوسع نطاقا.

وتشمل النماذج أو الهياكل المشتركة للشراكات بين القطاعين العام والخاص ذات الصلة بالأمن السيبراني وغيرها من الترتيبات المماثلة في الدول المشاركة في منظمة الأمن والتعاون في أوروبا تلك المنظمة تحت مظلة مصطلح "مجموعات الأمن السيبراني" أو "المراكز". وهي نهج ناشئ عموما عن القطاع الخاص و/أو الأوساط الأكاديمية، يجمع بين موارد وقدرات وكفاءات الصناعة والأوساط الأكاديمية والحكومية داخل النظام البيئي للأمن السيبراني في دولة ما. يتم إنشاء الحوافز من خلال تبادل المعلومات، وتجميع المعرفة، وتحديد تحديات القوى العاملة، وخلق فرص التواصل وأنشطة البحث والتطوير، بما في ذلك حلول الأمن السيبراني المطورة محليا والتي يمكن توسيع نطاقها على الصعيدين الوطني والدولي.

تختلف المجموعات أو المحاور السيبرانية في التطور. وقد يكون بعضها ترتيبات بسيطة للغاية، حيث تعمل كمنصات أساسية لتبادل المعلومات والتواصل وتشجيع التعاون حول القضايا الناشئة. وبالنسبة للبلدان أو المناطق داخل دولة ذات نظام بيئي رقمي ناشئ، تعد هذه الأنواع من الترتيبات نقطة انطلاق مهمة للتعاون. وفي بعض هذه الحالات، تم الاتصال بمجموعات أخرى أكثر تفصيلا أو نضجا لإسداء المشورة بشأن إنشائها. وهناك أيضا تفاعل صحي بين مجموعات الأمن السيبراني الوطنية، بما في ذلك من خلال **Global Epic**، وهو اتحاد دولي للمجموعات.

وفيما يتعلق بالأنشطة الملموسة، توفر بعض هذه الترتيبات الخدمات أو تيسر الوصول إلى المعرفة والحلول. هذه هي حالة مركز الابتكار الرقمي في **البرتغال - C-HUB**، الذي يقدم خدمات مبتكرة متعددة التخصصات للأمن السيبراني في جميع أنحاء البلاد، يستهدف على وجه التحديد الشركات الصغيرة والمتوسطة، **أو CyberHub الدنماركي**، الذي يسهل الشراكات بين الشركات الدنماركية الناشئة المبتكرة في مجال الأمن السيبراني والبحث و / أو الخدمة العامة. وبالمثل، تعزز **جمعية أمن المعلومات الإستونية (EISA)** التعاون بين القطاعات بين الأوساط الأكاديمية والقطاع الخاص وكذلك الحكومة وتعتزم تعزيز أنشطة البحث والتطوير في مجال الأمن السيبراني.

تستطيع مجموعات الأمن السيبراني أيضا تحديد وتوفير الفرص للاستجابة لاحتياجات النظام البيئي الوطني للأمن السيبراني، بما في ذلك تحديات القوى العاملة النظامية. ويشمل ذلك تطوير الآليات والأدوات القادرة على تصنيف أعمال وأدوار الأمن السيبراني، مع مساعدة الباحثين عن عمل في مجال الأمن السيبراني من خلال مطابقة مهاراتهم مع احتياجات الصناعة. مثال على هذه الأداة هو **إطار القوى العاملة للمبادرة الوطنية لتعليم الأمن السيبراني لـ Cyber Ireland**، والذي تم تطويره بدوره على أساس **إطار القوى العاملة للمعهد الوطني الأمريكي للمعايير** والتكنولوجيا **(NIST)**[8]. يمكن إدارة مجموعات الأمن السيبراني هذه من قبل أمانة مخصصة يديرها القطاع الخاص، كما في حالة **Hague Security Delta** أو في مراحلها المبكرة، مؤسسة أكاديمية كما في حالة **Cyber Ireland**. وفي حالات أخرى، مثل **مجموعة الأمن السيبراني التركية**، قد تكون الهيئات الحكومية هي المنسقة.

وفي كثير من الأحيان، تضع ترتيبات المجموعات السيبرانية الوطنية إرشادات تشغيلية. على سبيل المثال، عملت **شبكة التعاون العنقودي السيبراني في المملكة المتحدة (UKC3)** مع قادة المجموعات الوطنية من جميع أنحاء البلاد لتطوير إطار تشغيل متفق عليه للمجموعات السيبرانية. ويشتمل **إطار عمل التجمعات السيبرانية**[9] على مجموعة مشتركة من المبادئ والأهداف والنتائج التي توفر تعريفا واضحا لاختصاصات المجموعة وأهدافها، مما يمكن أصحاب المصلحة من فهم ودعم العمل الذي تقوم به المجموعات في تطوير وتنمية نظامها البيئي السيبراني المحلي بشكل أفضل. لتحفيز استخدام إطار العمل، هناك توقع بأن تقوم المجموعات السيبرانية التي تسعى للحصول على اعتراف رسمي وتمويل من UKC3 بتطبيقه.

وتشمل الأنواع الأخرى من الهياكل التي تعزز التعاون بين القطاعين العام والخاص تلك التي تقودها الحكومة، وهي واسعة النطاق عبر الدول المشاركة في منظمة الأمن والتعاون في أوروبا، من بينها **مجلس الأمن السيبراني** السويدي، وهو منتدى تعاون مع تمثيل واسع من القطاعين العام والخاص، وكذلك الأوساط الأكاديمية. يعمل المجلس كمورد استراتيجي لوكالة الطوارئ المدنية السويدية في عملها لدعم وتنسيق الأمن السيبراني وكذلك في تحليل وتقييم التطورات الخارجية داخل المنطقة. يضم **فريق خبراء أمن تكنولوجيا المعلومات ونظم المعلومات في لاتفيا (DEG)** خبراء من مختلف المنظمات الوطنية بما في ذلك من القطاع الخاص. إن هذه المجموعة

8 "إطار القوى العاملة للأمن السيبراني (إطار عمل NICE)، المعهد الوطني للمعايير والتكنولوجيا (NIST)، المنشور الخاص 800-181، المراجعة 1، https://doi.org/10.6028/NIST.SP.800-181r1

9 https://cyberpeaceinstitute.org/compendium-of-multistakeholder-perspectives/

- توفر منصة لتبادل المعلومات حول تهديدات تكنولوجيا المعلومات / نظم المعلومات؛
- تشجع وتدعم النمو المهني لأعضاء المجموعة؛
- تجمّع الموارد لبناء القدرات / الأغراض التعليمية بشأن مواضيع أمن تكنولوجيا المعلومات / نظم المعلومات؛
- تدعم الفريق الوطني للاستجابة للطوارئ الحاسوبية، CERT.LV.

وإلى جانب المجموعات السيبرانية والمحاور والهياكل المماثلة، سلطت عدة دول مشاركة في منظمة الأمن والتعاون في أوروبا الضوء على العمل الجاري مع الجهات الفاعلة الخاصة بشأن مشاكل محددة تتعلق بالأمن السيبراني، مثل

- حماية قطاع الرعاية الصحية؛
- تعزيز خدمات الحكومة الإلكترونية، بما في ذلك حلول الهوية الإلكترونية؛
- الإنذار المبكر؛
- أمن البرمجيات وإدارة مخاطر سلسلة التوريد؛
- التخفيف من التصيد الاحتيالي؛
- الكشف المنسق عن نقاط الضعف;
- القضاء على شبكات البوتات، على سبيل المثال لا الحصر.

للكل مبادرة من هذه المبادرات أهداف وطرائق إدارة مختلفة جدا وتنطوي على جهات فاعلة مختلفة جدا. على سبيل المثال، منذ بداية جائحة كوفيد-19، كانت كيانات قطاع الرعاية الصحية في جميع أنحاء العالم هدفا للهجمات الإلكترونية التي كان لها آثار اقتصادية كبيرة بالإضافة إلى تأثيرات مباشرة وغير مباشرة على المرضى. ويولى الآن اهتمام كبير لتعزيز الجهود المشتركة بين القطاعين العام والخاص لمنع هذه الهجمات والتخفيف من حدتها. أحد هذه الجهود هو التعاون بين **جمهورية التشيك ومايكروسوفت** ومعهد **السلام السيبراني** الذي أدى إلى خلاصة وافية لوجهات نظر أصحاب المصلحة المتعددين حول **حماية قطاع الرعاية الصحية من الأذى السيبراني**[10]. الخلاصة هي نتيجة للعديد من ورش العمل التي شاركت فيها الجهات الفاعلة العامة والخاصة حول مجموعة من الجوانب التقنية والتشغيلية والمعيارية ذات الصلة بحماية قطاع الرعاية الصحية.

ويتعلق مثال آخر بتطوير حلول الهوية الإلكترونية (eID)، التي تشكل حاليا مصدر قلق للبلدان في جميع أنحاء العالم وهي تتحرك نحو الرقمنة وضمان أمن ومرونة الخدمات الحكومية. ففي **إستونيا**، على سبيل المثال، تعاونت الحكومة تعاونا وثيقا مع القطاع الخاص في وضع وتنفيذ هذه الحلول منذ بداية عام 2002. في حين أن **هيئة نظم المعلومات** هي المسؤولة عن تشكيل رؤية واستراتيجية لتطوير مجال الهوية الإلكترونية، فإن شركة القطاع الخاص، **Solutions SK**، تقدم خدمات توثيق موثوقة لكل من القطاعين العام والخاص.

وفيما يتعلق بإذكاء الوعي والإنذار المبكر، تقدم المراكز الوطنية للأمن السيبراني في عدد متزايد من البلدان خدمات جديدة. ففي **فنلندا**، على سبيل المثال، أنشأ المركز الوطني للأمن السيبراني (NCSC-FI) ويدير

10 https://www.cisa.gov/uscert/ncas/current-activity/2022/11/17/cisa-nsa-and-odni-release-guidance-customers-securing-software

نظام Autoreporter الآلي، وهو أداة تجمع معلومات عالمية عن حركة مرور البرامج الضارة الناشئة من فنلندا. يشارك NCSC-FI هذه المعلومات مع مشغلي الاتصالات، الذين يقومون بتوزيعها على عملائهم النهائيين في محاولة لزيادة الوعي ومكافحة انتشار البرامج الضارة.

وتنظر بعض الدول المشاركة أيضا إلى انخراطها مع المجتمع بأسره في القضايا المتعلقة بالأمن السيبراني على أنها شكل من أشكال المشاركة بين القطاعين العام والخاص. ومن الأمثلة على ذلك حملة **بلجيكا** السنوية للتوعية بالأمن السيبراني. تطبيق **Safeonweb (SOW)** الخاص بها هو نتيجة للحملة الأخيرة. يجمع التطبيق أخبارا حول التصيد الاحتيالي ويحذر من التهديدات الإلكترونية والأشكال الجديدة من عمليات الاحتيال عبر الإنترنت. كما يوفر تحديثات منتظمة للمشتركين حول نقاط الضعف والتهديدات عبر تطبيق مخصص. يعمل التطبيق أيضا كمنصة للتعلم الإلكتروني حيث يمكن للمستخدمين تعلم ممارسات الأمن الأساسية والنظافة الإلكترونية واختبار معرفتهم ووعيهم. المشاركة في هذه المبادرة طوعية. وقد انبثقت عن مبادرة سابقة - **حملة BePhish** - التي يقوم من خلالها مستخدمو الإنترنت بتنبيه المركز البلجيكي للأمن السيبراني (CCB) طواعية عندما يتلقون رسالة تصيد مشبوهة. ثم تتحقق العملية التلقائية من الروابط أو المرفقات وتحدد ما إذا كان سيتم حظرها أم لا.

عندما يتعلق الأمر بأمن البرمجيات وإدارة مخاطر سلسلة التوريد، يجري العمل التعاوني بين القطاعين العام والخاص جاريا منذ بعض الوقت. وتشمل المبادرات الأخيرة تأمين **سلسلة توريد البرمجيات: دليل الممارسات الموصى بها للعملاء**[11]، الذي وضعه في **الولايات المتحدة الفريق العامل المعني بالإطار الأمني الدائم** الذي يعمل تحت رعاية المجلس الاستشاري لشراكة البنية التحتية الحرجة، وهو فريق عامل مشترك بين القطاعين العام والخاص. إن منشوره هو الثالث في سلسلة من ثلاثة أجزاء تقدم أفضل الممارسات لعملاء البرمجيات لشراء ونشر البرامج الآمنة. كما يتضمن إرشادات لقائمة مواد البرمجيات (SBOM)، وهي قائمة بجميع "المكونات" التي تشكل عناصر البرامج والتي تبذل بشأنها جهود تعاونية منذ عام 2018.

وفي **الاتحاد الأوروبي**، يعتمد **الإطار الطوعي لإصدار شهادات الأمن السيبراني لمنتجات تكنولوجيا المعلومات والاتصالات وعملياتها وخدماتها** أيضا على التعاون العميق بين القطاعين العام والخاص، بما في ذلك حول منتجات البرمجيات. يعتمد **قانون المرونة السيبرانية** المقترح مؤخرا، والذي يهدف إلى ضمان قدر أكبر من الأمان لمنتجات الأجهزة والبرامج، على تعاون كبير بين القطاعين العام والخاص في تطوير القواعد، وسيتطلب تعاونا مستمرا بين الجهات الفاعلة العامة والخاصة بمجرد اعتماد القواعد الجديدة[12].

تعزيز الشراكات بين القطاعين العام والخاص المتصلة بأمن الفضاء الحاسوبي وغيرها من الترتيبات المماثلة عبر الحدود

لا يمكن التقليل من أهمية التعاون بين القطاعين العام والخاص والتآزر عبر الحدود. وقد كشفت الزيادة في هجمات برامج الابتزاز وتأثيرها على عمل المجتمعات في جميع أنحاء العالم عن الحاجة إلى هذه الأنواع من الترتيبات، بما في ذلك تعزيز قدرات الاستجابة السريعة في جميع البلدان. وتظهر حوادث برامج الابتزاز الأخيرة قيمة ترتيبات الاستجابة بين القطاعين العام والخاص والتعاون عبر المناطق. على سبيل المثال، أرسلت

11 https://www.cisa.gov/uscert/ncas/current-activity/2022/11/17/cisa-nsa-and-odni-release-guidance-customers-securing-software

12 قانون المرونة السيبرانية - قواعد الأمن السيبراني الجديدة للمنتجات الرقمية والخدمات المساعدة. متاح في:
https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services_en

إسبانيا فريقين مختلطين يتألفان من أعضاء المركز الإسباني الحكومي الوطني للتشفير - فريق الاستجابة لحوادث أمن الكمبيوتر (CCN-CERT) وشركات خاصة لدعم جهود الاستجابة للحوادث والتعافي منها في كوستاريكا في أبريل / نيسان ويونيو / حزيران 2022 على التوالي.

كما يستطيع الإعلان الأخير الصادر عن **إسبانيا** و**الولايات المتحدة** بشأن تطوير **أداة لبناء القدرات** لمساعدة الدول على استخدام **الشراكات بين القطاعين العام والخاص لمكافحة برامج الابتزاز** أن يعزز هذه الجهود. يهدف هذا المشروع إلى "توفير التوجيه للدول في جميع أصقاع العالم التي تسعى إلى تطوير أو تعميق الشراكات بين القطاعين العام والخاص"، بما في ذلك من خلال عرض الابتكارات في مكافحة برامج الابتزاز، ومن خلال إنشاء "خطط تمويل" لدعم مثل هذا التعاون بين القطاعين العام والخاص[13].

ضمان الثقة والأمن في الشراكات بين القطاعين العام والخاص وغيرها من الترتيبات المماثلة

في معظم الحالات، يملي الغرض من الترتيب بين القطاعين العام والخاص وطابع الكيانات المعنية مستوى الثقة والأمن اللازمين لتمكين التعاون. العديد من الأمثلة على هذه الترتيبات في الدول المشاركة في منظمة الأمن والتعاون في أوروبا مفتوحة للمشاركة الواسعة ولا تنطوي على أي عملية تدقيق رسمية. وتميل هذه البرامج إلى أن تكون موجهة نحو زيادة الوعي العام أو بناء القدرات أو النظافة السيبرانية.

> ومع ذلك، كلما اقتربت القضية من الأمن القومي، كلما كانت المنصة أكثر انغلاقا، ومن المرجح أن يطلب من المشاركين الحصول على تصريح أمني أو التوقيع على شكل من أشكال اتفاقية السرية أو عدم الإفشاء.

13 https://www.cisa.gov/news/2022/11/10/united-states-and-spain-announce-development-new-capacity-building-tool-combat

ومع ذلك، يمكن لهذه الأنواع من المتطلبات أن تعزز عدم الثقة، بالإضافة إلى أخذ الوقت لتحديدها. وعلى العكس من ذلك، يبين التقرير أن المنصات المغلقة قد تكون مفيدة للطرفين للجمهور وأصحاب المصلحة المعنيين من القطاع الخاص: فهي تساعد في حماية المعلومات السرية والملكية، مع توسيع نطاق المعلومات التي يمكن لأصحاب المصلحة المعنيين الوصول إليها. توفر هذه المنصات أيضا للأعضاء أو المشاركين القدرة على التأثير على السياسة والعمليات داخل مجتمع أو قطاع معين. كما يمكن للعمليات التشاورية التي تؤدي إلى إنشاء ترتيب معين بين القطاعين العام والخاص أن تسهم في تحفيز المشاركة والمساعدة في ضمان استجابة الترتيب لشواغل ومتطلبات الأمن و/أو السرية لجميع المعنيين، وليس فقط شواغل الأمن القومي للحكومة.

وتُبذل الجهود في جميع الدول المشاركة في منظمة الأمن والتعاون في أوروبا لإنشاء منصات آمنة وموثوقة لتعزيز التعاون بين القطاعين العام والخاص، لا سيما عندما يكون الهدف هو تبادل المعلومات الحساسة أو المعلومات الاستخبارية المتعلقة بالتهديدات في الوقت المناسب. تستخدم بعض الدول "بروتوكول إشارات المرور"، "مجموعة من التعيينات المستخدمة لضمان مشاركة المعلومات الحساسة مع الجمهور المناسب"[14]. ويستخدم هذا الأخير، على سبيل المثال، من قبل **تحالف الأمن السيبراني في بلجيكا**، وهي جمعية غير ربحية تعزز التعاون بين الحكومة والقطاع الخاص والأوساط الأكاديمية لتسريع المرونة الرقمية والاستجابة للتهديدات الناشئة.

يمكن لبعض الشركات أيضا أن تلعب دورا موثوقا به في سد الفجوة بين الوكالات الحكومية والقطاع الخاص. على سبيل المثال، في هولندا، يمكن للشركات غير الحيوية الحصول على وضع خاص يسمى **مهمة معروفة موضوعيا (OKTT)**، والتي تسمح لها بالعمل كنوع من جسر تبادل المعلومات والاستشارات بين الوكالة الوطنية للأمن السيبراني والمنظمات في شبكاتها الخاصة.

في بعض الأحيان، تكون الحكومة نفسها هي التي تنشئ منصات آمنة. عند اعتماد استراتيجيتها الوطنية للأمن السيبراني وخطة عملها، أنشأت تركيا **المركز الوطني للاستجابة لطوارئ الكمبيوتر (USOM)** التابع للهيئة الوطنية لتكنولوجيا المعلومات والاتصالات (BTK)، وذلك لتنسيق الاستجابة للحوادث على المستوى التقني. ومنذ ذلك الحين، أقام مركز USOM تعاونا بين مراكز CERT العامة والخاصة. يتم استخدام منصة آمنة - **USOM 7/24** - لجمع ومشاركة البيانات والمعلومات بشأن التهديدات والاستخبارات بين مراكز CERT العامة والخاصة. يساهم USOM أيضا في تنمية النظام البيئي الوطني للأمن السيبراني من خلال تدريب الخبراء ودعم تطوير حلول الأمن السيبراني.

عندما تقود الحكومة مبادرة ما، فإن الوضوح حول متطلبات مثل التصاريح الأمنية وضمان أن تكون مشاركة الصناعة طوعية يمكن أن يساعد في تعزيز الثقة في المبادرة داخل الصناعة والجمهور الأوسع. لنأخذ، على سبيل المثال، **مبادرة الصناعة 100 في المملكة المتحدة**، فإنها تسهل التعاون الوثيق بين المركز الوطني للأمن السيبراني (NCSC) وصناعة المملكة المتحدة. ومن خلال هذا التعاون، يسعى المركز الوطني للأمن السيبراني إلى "تعلم الدروس وتحديد نقاط الضعف النظامية والحد من تأثير الهجمات السيبرانية"[15]. تعمل المبادرة على أساس الإعارة حيث يمكن للجهات الفاعلة في الصناعة البحث عن وظيفة بدوام جزئي في NCSC (تتراوح من يوم واحد في الأسبوع إلى يوم واحد في الشهر). تضع فرق NCSC إعلانات على موقع NCSC عندما يبحثون عن مجموعات مهارات محددة. وحفاظا على الاستقلالية، يتوقع من منظمات المرشحين المختارين أن تدفع مرتب موظفيها أثناء إعارتهم. ولضمان الأمن، يتوقع أن يكون لدى المعارين المختارين تصريحات أمنية.

قد تواجه الدول التي تستضيف شركات أو خدمات متعددة الجنسيات تحديات فريدة في تبادل المعلومات، لا سيما عندما تكون هناك حاجة لتمكين تبادل المعلومات الاستخباراتية عن التهديدات مع الكيانات

14 تعريفات واستخدام بروتوكول إشارات المرور (TLP). متاح في: https://www.cisa.gov/tlp

15 https://www.ncsc.gov.uk/section/industry-100/about

غير الوطنية. في **هولندا**، أنشئت **"دائرة ثقة"** للتعامل مع هذه التحديات وغيرها، وتضم فرق الاستجابة للطوارئ الحاسوبية من 10 شركات متعددة الجنسيات مقرها في البلاد والمركز الوطني للأمن السيبراني، وهي بمثابة مساحة آمنة ومأمونة لتبادل المعلومات، بما في ذلك مخاطر الأمن السيبراني وسلسلة التوريد، وتنمية المواهب. ولا تحل دائرة الثقة محل عمل مراكز تبادل المعلومات وتحليلها (ISAC) الوطنية الخاصة بالقطاعات فهي هيئات مكرسة لجمع وتحليل المعلومات القابلة للتطبيق والمتعلقة بالتهديدات وبتوزيعها على الأعضاء وتزويدهم بأدوات للتخفيف من المخاطر وتحسين القدرة على المرونة.

بما أن الشركات أو الخدمات المتعددة الجنسيات غالبا ما تقع ضمن قطاعات حيوية محددة، فقد يلزم اتخاذ تدابير إضافية لضمان بيئة موثوقة وآمنة لتبادل المعلومات. في **سويسرا**، أنشئ هيكل ذو بنية متقنة لتمكين التعاون داخل القطاع المالي، بما في ذلك الكيانات غير السويسرية، وبين القطاع المالي والسلطات الحكومية. تأسس **المركز السويسري للأمن السيبراني في القطاع المالي (FS-CSC)** في أبريل / نيسان 2022، ويضم أكثر من 50 عضوا مؤسسا، بما في ذلك البنوك وشركات التأمين والجمعيات الصناعية بالإضافة إلى الوكالات الحكومية التابعة مثل الهيئة السويسرية للإشراف على السوق المالية (FINMA) والمركز الوطني للأمن السيبراني وأمانة الدولة للتمويل الدولي. ويتمحور المركز حول مجلس توجيهي يقوم بتنشيط خلية تنسيق الأزمات في حالة وقوع حادث نظامي؛ وفريق خبراء يدير مشاريع تهدف إلى تعزيز المرونة السيبرانية وينظم تمارين استراتيجية وتشغيلية؛ وخلية الأمن السيبراني التشغيلية، التي تدير تبادل المعلومات، وتراقب الأحداث ذات الصلة بالقطاع، وتقدم تقارير خاصة بالقطاع، وتدعم إدارة الأزمات. وهي تعمل كجمعية، والعضوية فيها عبارة عن دفع رسوم للكيانات الخاصة. لضمان بيئة موثوقة وآمنة، تتطلب البنوك وشركات التأمين وشركات الأوراق المالية والبنى التحتية للأسواق المالية التي تسعى للحصول على العضوية إذن FINMA. بالإضافة إلى ذلك، استحوذ FS-CSC مؤخرا على خدمات مركز تبادل وتحليل معلومات الخدمات المالية (FS-ISAC)، وهو مزود عالمي موثوق به لخدمات الأمن السيبراني، لدعم عمليات خلية الأمن السيبراني التشغيلية.

العمر الافتراضي وترتيبات التمويل

قد يختلف عمر أو مدة شراكة أو تعاون معين بين القطاعين العام والخاص اختلافا كبيرا. إن نماذجها المحددة في هذا التقرير هي عموما نماذج دائمة أو مفتوحة العضوية للتعاون (على سبيل المثال، مراكز ISAC لقطاع البنية التحتية الحيوية أو غيرها من منصات تبادل المعلومات الاستخباراتية المتعلقة بالتهديدات). لدى بعضها مدة محددة للغاية، على سبيل المثال، **ترتيبات الاستجابة السريعة، أو أشهر التوعية بالأمن السيبراني** التي تقام سنويا، أو المهرجانات مثل **مهرجان أمن الإنترنت** السنوي في **جمهورية التشيك**. وقد يتحدد عمر المبادرات الأخرى بإلحاح التهديد ونطاقه وحجمه، وبدورات الميزانية وتوافر الموارد عموما.

إن ضمان التمويل الكافي، بطبيعة الحال، هو مفتاح أي شكل من أشكال التعاون، وكما ذكرنا، فإن التمويل المتاح سيحدد عموما مدة أي مبادرة معينة. ويساعد إدراج إشارات إلى هذه الأشكال من التعاون في استراتيجيات الأمن الوطني، فضلا عن تفاصيل أكثر تحديدا في خطط العمل ذات الصلة، على ضمان تخصيص الموارد على نحو كاف، فضلا عن تحديد المجالات التي قد تكون فيها مخصصات إضافية في الميزانية ضرورية والمجالات التي قد يكون فيها تقاسم الأعباء مع الكيانات الخاصة مفيدا للغاية. ومن بين أوجه التعاون بين القطاعين العام والخاص التي حددتها الدول المشاركة، يمول العديد منها من الحكومات من خلال مخصصات محددة في

الميزانية. والبعض الآخر - بشكل عام ذلك التعاون الذي تبدأه الجهات الفاعلة في الصناعة – عادو يُمول من قبل كيانات خاصة أو من خلال العضوية أو الأحداث أو غيرها من الرسوم المماثلة. غير أن البعض الآخر ينطوي على تجميع أنواع مختلفة من الموارد. ويمكن أن تتغير مصادر التمويل هذه بمرور الوقت مع نضوج الترتيب. لنأخذ، على سبيل المثال، مجموعات الأمن السيبراني. وفي بعض الحالات، تنطلق بالتمويل الحكومي، على الرغم من أن الهدف الشامل لمعظم المجموعات هو ضمان الاستقلالية من خلال المساهمات المالية من جميع الكيانات المشاركة ومن خلال أشكال أخرى لجمع الأموال مثل رسوم العضوية وإقامة الأحداث. ويقوم بعضها أيضا بتجميع الموارد، مثل أماكن العمل، غالبا في مواقع أخرى غير العواصم، كما هو الحال في **مجمع دلتا للأمن في لاهاي**، والذي بدوره يمكن أن يساعد في تعزيز قيمة هذه المواقع في تعزيز الأمن السيبراني والقدرة على المرونة، مع ضمان الكفاءة وتعزيز فرص العمل على المستويين الإقليمي أو المحلي وجذب الاستثمار.

في حالة **مؤسسة شبكة الأمن السيبراني (CSN)** في صربيا، قدمت بعثة منظمة الأمن والتعاون في أوروبا إلى صربيا جزءا من التمويل الأولي للمبادرة. كانت CSN تعرف سابقا باسم "Petnica Group"، وهي مؤسسة مستقلة يتمثل هدفها الرئيسي في الجمع بين أصحاب المصلحة من جميع أنحاء المجتمع لتبادل المعلومات وتجميع الأفكار. وسهلت المشاورات التي أدت إلى وضع العديد من الوثائق القانونية في مجال أمن المعلومات في صربيا، بما في ذلك الاستراتيجية الوطنية لمجتمع المعلومات والأمن في الدولة (2021-2026)، التي سلطت الضوء على أهمية التعاون بين القطاعين العام والخاص فيما يتعلق بالأمن السيبراني. بموافقة ودعم من السلطات المختصة، تنفذ مؤسسة شبكة الأمن السيبراني البرنامج التعليمي المعنون "البطل السيبراني" وتنظم مسابقة الأمن السيبراني الوطنية تحت عنوان "تحدي الأمن السيبراني الصربي". وتبذل حاليا جهود لتأمين مصادر تمويل أكثر استدامة، بما في ذلك على الصعيدين الوطني والإقليمي (الاتحاد الأوروبي).

الرصد والرقابة

ويتطلب التركيز المتزايد على أهمية الشراكات بين القطاعين العام والخاص المتصلة بالأمن السيبراني وغيرها من الترتيبات المماثلة للمصالح الوطنية والأمن الوطني، وتزايد الاستثمار في هذه الآليات، تركيزا أكبر على قياس أدائها واستعراضها بانتظام.

يستلزم الرصد التقييم المستمر والمنهجي لمشروع أو مبادرة معينة بناء على الأهداف التي تم الاتفاق عليها، والأنشطة التي تم التخطيط لها وكيفية تنفيذها، والمعلومات التي يتم جمعها على طول الطريق، الأمر الذي يمكّن بذل الجهود في سبيل التقييم بطريقة منهجية وموضوعية من حيث مدى ملاءمتها وأدائها وتأثيرها ونجاحها أو عدمها واستدامتها وفقا للأهداف المعلنة. وتكتسي الرقابة أهمية خاصة عندما تشارك الأموال العامة في التعاون.

بالنسبة لبعض الدول المشاركة في منظمة الأمن والتعاون في أوروبا، غالبا ما يكون الرصد والتقييم جزءا من خطتها الوطنية لتنفيذ استراتيجيتها للأمن السيبراني وينطوي على متطلبات إبلاغ مفصلة. ولا تزال الجهود المبذولة في هذا المجال تنضج. وقد لا تكون أشكال المشاركة الأخرى الأكثر مرونة صارمة للغاية، ولكن القدرة على التعبير عن قيمتها بالمساهمة في الأهداف المتفق عليها أمر مهم مع ذلك. وبغض النظر عن نوع التعاون وما إذا كان ينبع من استراتيجية وطنية للأمن السيبراني، أشارت بعض الدول المشاركة إلى أنها غالبا ما تواجه تحديات في تقييم قيمة مشاركتها مع القطاع الخاص، وقد لا تكون لديها دائما صورة كاملة عما تنطوي عليه وكيف تساهم في تحقيق الأهداف المحددة في استراتيجيتها الوطنية للأمن السيبراني. ونظرا لتزايد الاحتياجات والحاجة إلى تحديد أولويات الجهود والموارد، تقوم بعض الدول المشاركة حاليا باستعراض أوجه التعاون القائمة بين القطاعين العام والخاص، بما في ذلك من خلال إجراء استعراض مستفيض لمذكرات التفاهم أو الاتفاقات المبرمة مع كيانات القطاع الخاص.

وبالنسبة للتعاون التقليدي القائم على الهياكل الأساسية المبنية على العقود بين القطاعين العام والخاص، تستخدم العديد من الأدوات والآليات لأغراض الرصد والرقابة. ويمكن استخلاص الدروس من هذه الشراكات بين القطاعين العام والخاص المتعلقة بالأمن السيبراني وغيرها من الترتيبات المماثلة، لا سيما في غياب التزامات الإبلاغ الرسمية. وهي تشمل أدوات مثل الكشف الاستباقي، وهي عملية يتم من خلالها الكشف عن البيانات غير الحساسة طوال دورة حياة شراكة أو تعاون معين بحيث يكون محتوى التعاون ونطاقه وتقدمه (وليس محتوى ما تتم مناقشته) متاحا للجميع. قد يساعد هذا النوع من الوصول المنظم إلى البيانات في تعزيز الثقة في المشروع، من خلال توفير وسيلة للحكومة والصناعة والجهات الفاعلة غير الحكومية الأخرى لمراقبة الأداء وتحليل نسب التكلفة إلى الفائدة وتحديد فرص جديدة للتعاون، فضلا عن منع الاحتيال والفساد.

وتشمل التطورات الأخرى في هذا المجال نهجا تعاونية لدعم تنفيذ الاستراتيجية الوطنية الحكومية في مجال الأمن السيبراني والإشراف عليها. تلعب **منصة الأمن السيبراني النمساوية** مثل هذا الدور، فتعمل هذه الهيئة كمظلة للتبادل الدائم للمعلومات بين الإدارة العامة وممثلي الاقتصاد والعلوم والبحوث مع جميع أصحاب المصلحة المشاركين على قدم المساواة. وهي تتألف من حوالي 100 فرد من مختلف القطاعات الحيوية الذين ينظمون أنفسهم طواعية في مجموعات فرعية مختلفة للمساعدة وتقديم المشورة لمشاريع متنوعة، مثل صياغة الاستراتيجية الوطنية للأمن السيبراني أو تقديم مدخلات لموقف النمسا قبل الاجتماعات الدولية وعمليات التفاوض ذات الصلة. بالإضافة إلى ذلك، تتمتع هذه المنصة باختصاص تقديم المشورة والدعم **للمجموعة التوجيهية الوطنية للأمن السيبراني**، كما تجتمع مع الحكومة على فترات منتظمة لتقديم تقارير عن مدى تنفيذ الاستراتيجية الوطنية للأمن السيبراني من منظور القطاع الخاص.

الناس

تتطلب الشراكات بين القطاعين العام والخاص المتعلقة بالأمن السيبراني وغيرها من الترتيبات المماثلة الوضوح بشأن من ينبغي إشراكه ولأي غرض. وهذا ينطوي على التعبير الواضح عما يلي:

- أصحاب المصلحة المعنيين وأدوارهم ومسؤولياتهم ضمن الترتيب.
- ما إذا كان الترتيب مفتوحا لجميع الأطراف المعنية أو مقصورا على مجموعة أصغر أو مستهدفة.
- كيف يتوقع من المشاركين المساهمة في تحقيق أهداف الترتيب.
- ما إذا كانت هناك حاجة إلى خبرة محددة أو وظائف مخصصة لتسهيل بناء العلاقات بين الجهات الفاعلة في القطاعين العام والخاص المعنية.

تتوقف المشاركة أو العضوية في شراكة بين القطاعين العام والخاص أو أي ترتيب آخر من هذا القبيل دائما على الغرض من الترتيب الفعلي وهدفه. وفي الدول المشاركة في منظمة الأمن والتعاون في أوروبا، يمكن أن تشمل سلطة عامة واحدة فقط (مثل مركز وطني للأمن السيبراني) أو عدة سلطات. في حالة أكثر من سلطة واحدة، عادة ما تكون هي من وزارات العدل والداخلية والدفاع والتعليم والتحول الرقمي والخزانة / المالية والتخطيط للطوارئ / الكوارث والتعافي (أو من وكالات تابعة لها). وعلى الجانب الخاص، يمكن أن يشمل أصحاب المصلحة الرئيسيون شركات التكنولوجيا المتعددة الجنسيات، وشركات الاتصالات، ومقدمي خدمات الإنترنت، وشركات الأمن السيبراني، ومالكي ومشغلي البنية التحتية الحيوية وغيرها من الأصول والخدمات الأساسية، والشركات الصغيرة والمتوسطة، والخبراء الأفراد، وحتى الأفراد الذين يتصرفون بصفتهم الشخصية.

من المهم ملاحظة أن بعض الدول المشاركة تتبع نهجا أوسع نطاقا إزاء هذه الترتيبات. وقد تشمل المبادرات ذات الصلة الأوساط الأكاديمية أو المعاهد أو الهيئات التقنية أو منظمات المجتمع المدني المتخصصة أو جميع سكان دولة ما. وعادة يكون هو الحال عندما يتعلق الأمر بالتعليم وبناء القدرات. على سبيل المثال، في **إيطاليا**، تمشيا مع الأحكام المحددة المنصوص عليها في الخطة الوطنية للتعافي والقدرة على المرونة، والاستراتيجية الوطنية للأمن السيبراني وقانون تم تبنيه مؤخرا بشأن التعليم ما بعد الثانوي، تبذل الجهود لتطوير **شبكة تنسيق للمعاهد التكنولوجية العليا (ITS - Istituti Tecnologici Superiori)** لتطوير التحول الرقمي والنظام البيئي الوطني لتدريب المهارات الرقمية الجديدة. وسيشمل هذا التعاون العديد من المؤسسات، على الصعيدين الوطني والإقليمي، ويهدف إلى تطوير نظام ITS، الذي يمثل قطاعا للتعليم العالي يدار نتيجة للتعاون بين الإدارات المحلية والمدارس والصناعة، بمشاركة الجامعات. لا يزال نظام ITS، الذي تم إنشاؤه قبل عقد من الزمان، صغيرا في الحجم، فتهدف المبادرة إلى تعزيز نموه، لا سيما في مجال الأمن السيبراني.

كما سيحدد الغرض من هذا الترتيب ما إذا كان النظام مفتوحا لجميع الأطراف المعنية، أو مغلقا، ويتطلب من الكيانات أو الأفراد المشاركين استيفاء معايير معينة. في بعض الأحيان، قد تملي طبيعة الكيان الخاص - سواء كان متعدد الجنسيات أو أجنبيا - ما إذا كان يمكن لموظفيه المشاركة في ترتيب وطني معين أم لا. عادة ما، يتم الاسترشاد بالاعتبارات المتعلقة بالأمن القومي والتشريعات الوطنية على نحو متزايد في توجيه مثل هذه القرارات. ومرة أخرى، تعتبر اتفاقات عدم الكشف والترتيبات المماثلة أدوات هامة لتمكين هذا الشكل من أشكال التعاون.

إن تغير التهديدات والبيئات التنظيمية يدفع العديد من الدول المشاركة إلى تعزيز التنسيق بين السلطات الحكومية واستعراض مذكرات التفاهم القائمة وما يرتبط بها من شراكات وترتيبات مع القطاع الخاص لضمان تحسين تحديد الأولويات واستخدام الموارد. في بعض الحالات، يتم إنشاء مناصب مخصصة داخل الحكومة لتنسيق تعاون الحكومة مع القطاع الخاص على وجه التحديد بشأن القضايا المتعلقة بالأمن السيبراني. هذا هو الحال، على سبيل المثال، في **الجمهورية التشيكية** وهولندا، حيث تجري الاستعدادات للعمل مع مجموعة أوسع بكثير من كيانات القطاع الخاص بموجب توجيه NIS2.

ملاحظات ختامية

كانت نقطة الانطلاق لمشاركة منظمة الأمن والتعاون في أوروبا في مجال الشراكات بين القطاعين العام والخاص المتعلقة بالأمن السيبراني هي نتيجة للتقرير الذي أصدرته في عام 2021 مجموعة التدبير الرابع عشر المعنية ببناء الثقة. ويشكل هذا التقرير بشأن الممارسات الناشئة متابعة له، حيث تم تنظيم توصياته تحت عناوين الغرض والسياسات والعملية والناس، وهي العناوين التي تمثل الخطوط الأساسية الموصى بها لكيفية قيام الجهات الحكومية جنبا إلى جنب مع القطاع الخاص بتحديد الغرض من العلاقة (السؤال لماذا)؛ وما ستركز عليه (السؤال ماذا)؛ وطرائق أو هيكل الترتيب (السؤال كيف) ومن ينبغي إشراكه (السؤال مَن).

يوضح هذا التقرير الطريقة التي تصبح فيها المشاركة مع القطاع الخاص سمة بارزة لتعزيز الأمن السيبراني والقدرة على المرونة عبر منطقة الدول المشاركة في منظمة الأمن والتعاون في أوروبا. كما أنه يبين عددا كبيرا من الترتيبات التعاونية التي قدمتها الدول المشاركة طوال فترة إعداد التقرير حول كيفية تطبيع وإنضاج هذه العلاقات على حد سواء، فضلا عن بناء الثقة داخل المجتمعات المختلفة وفيما بينها أيضا.

وفي الوقت نفسه، كانت الدول المشاركة التي أجريت معها مقابلات طوال العملية صريحة بشأن نطاق وحجم تحديات الأمن السيبراني والمرونة التي تواجهها، وقد أبدت اهتماما كبيرا بمعرفة المزيد عن كيفية تعاون الدول المشاركة الأخرى والمناطق الأخرى المشتركة مع القطاع الخاص للتغلب على التحديات، مثل العمل بشكل تعاوني مع الشركات الصغيرة والمتوسطة أو معاهد البحوث أو قطاعات محددة في البنية الأساسية الحيوية؛ وإنشاء منصات موثوقة وآمنة لتبادل المعلومات والحفاظ عليها؛ وقدرات الاستجابة السريعة؛ وهياكل المساءلة التحفيزية في الشراكات بين القطاعين العام والخاص في مجال الأمن السيبراني؛ ورصد هذه الترتيبات والإشراف عليها. ومن الأهمية بمكان أن تكون الدول المشاركة مهتمة أيضا بالاستماع إلى آراء الشركاء من القطاع الخاص في هذه الترتيبات. بهذا الصدد، تشكل الأمثلة التي قدمتها الدول المشاركة لإثراء هذا التقرير كنزا دفينا لتبادل الآراء في المستقبل على المستويات الثنائية والإقليمية والدولية وذلك عبر العديد من المجالات المختلفة.

المرفق الأول:

الغرض، السياسات، العملية، الناس

الغرض (العام)

ينبغي أن يكون للشراكات بين القطاعين العام والخاص المتعلقة بالأمن السيبراني وغيرها من الترتيبات المماثلة غرض محدد بوضوح. ويتطلب ذلك الآتي:

- فهم واضح للنظام البيئي الوطني للأمن السيبراني.
- فهم واضح لنقاط القوة والضعف في كيانات القطاعين العام والخاص ذات الصلة في الدولة مقابل تحديات الأمن السيبراني والقدرة على المرونة والتي تحتاج إلى معالجة.
- تحديد المجالات التي يمكن أن يعالج فيها التعاون بين القطاعين العام والخاص التحديات المحددة.
- تحديد كيفية تحفيز مشاركة القطاع الخاص ذي الصلة والجهات الفاعلة الأخرى.
- تحديد ما إذا كانت هناك حاجة إلى إنشاء منصب حكومي مخصص لتسهيل أو تنسيق العلاقات بين القطاعين العام والخاص.

السياسات

ينبغي تحديد الشراكات بين القطاعين العام والخاص المتعلقة بالأمن السيبراني وغيرها من الترتيبات المماثلة بوضوح في السياسات و/أو التشريعات الوطنية، ويتطلب ذلك الآتي:

- الإقرار بأهمية الترتيبات بين القطاعين العام والخاص في السياسة والاستراتيجية الوطنية للأمن السيبراني، بما في ذلك من خلال إبراز كيفية مساهمة الترتيب في تحقيق أهداف الأمن الوطني والتنمية الاقتصادية والاجتماعية، التي يمكن إدراج تفاصيلها في خطط العمل ذات الصلة.
- التشاور مع الكيانات الخاصة ذات الصلة في القرارات السياسية والتشريعية والتنظيمية التي ستؤثر عليها.
- الالتزام بإنشاء آليات الشفافية والرقابة للترتيبات بين القطاعين العام والخاص والأنشطة ذات الصلة.

العملية

تتطلب الشراكات بين القطاعين العام والخاص المتعلقة بالأمن السيبراني وغيرها من الترتيبات المماثلة طرائق تنفيذ واضحة أو هياكل الإدارة للمساعدة في ضمان تحقيق الأهداف والنظر في هياكل المساءلة التحفيزية المناسبة منذ البداية. ويشمل ذلك التأكيد المشترك من قبل الجهات الفاعلة العامة والخاصة المعنية على:

- الأهداف المحددة للترتيب والمشاكل المحددة التي يشرع في حلها.
- الأنشطة التي سيضطلع بها الترتيب لتحقيق الأهداف المتفق عليها.
- العمر الافتراضي ومصادر التمويل.
- متطلبات وبروتوكولات الأمن أو عدم الإفصاح التي يجب وضعها وممارسات النظافة السيبرانية التي يجب الترويج لها بين المشاركين.
- آليات للرصد والإشراف على الأنشطة المضطلع بها.
- آليات لمراجعة وتحديث طرائق التنفيذ أو هياكل الإدارة للشراكة بين القطاعين العام والخاص/الترتيب.
- استراتيجية الاتصالات/التوعية.

الناس

تتطلب الشراكات بين القطاعين العام والخاص المتعلقة بالأمن السيبراني وغيرها من الترتيبات المماثلة الوضوح بشأن من ينبغي إشراكه ولأي غرض. وهذا ينطوي على التعبير الواضح عما يلي:

- أصحاب المصلحة المعنيين وأدوارهم ومسؤولياتهم ضمن الترتيب.
- ما إذا كان الترتيب مفتوحا لجميع الأطراف المعنية أو مقصورا على مجموعة أصغر أو مستهدفة.
- كيف يتوقع من المشاركين المساهمة في تحقيق أهداف الترتيب.
- ما إذا كانت هناك حاجة إلى خبرة محددة أو وظائف مخصصة لتسهيل بناء العلاقات بين الجهات الفاعلة في القطاعين العام والخاص المعنية.

المرفق الثاني:

قرار المجلس الدائم لمنظمة الأمن والتعاون في أوروبا رقم 1202

OSCE Organization for Security and Co-operation in Europe

PC.DEC/1202
March 2016 10

Organization for Security and Co-operation in Europe Permanent Council

Original: ENGLISH

1092nd Plenary Meeting
PC Journal No. 1092, Agenda item 1

DECISION No. 1202

OSCE CONFIDENCE-BUILDING MEASURES TO REDUCE THE RISKS OF CONFLICT STEMMING FROM THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES

The OSCE participating States in Permanent Council Decision No. 1039 (26 April 2012) decided to step up individual and collective efforts to address security of and in the use of information and communication technologies (ICTs) in a comprehensive and cross-dimensional manner in accordance with OSCE commitments and in co-operation with relevant international organizations, hereinafter referred to as "security of and in the use of ICTs." They further decided to elaborate a set of draft confidence-building measures (CBMs) to enhance interstate co-operation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs.

The OSCE participating States, recalling the OSCE role as a regional arrangement under Chapter VIII of the UN Charter, confirm that the CBMs being elaborated in the OSCE complement UN efforts to promote CBMs in the field of security of and in the use of ICTs.

The efforts of the OSCE participating States in implementation of the OSCE confidence-building measures in the field of security of and in the use of ICTs will be consistent with: international law, including, inter alia, the UN Charter and the International Covenant on Civil and Political Rights; as well as the Helsinki Final Act; and their responsibilities to respect human rights and fundamental freedoms.

The following CBMs were first adopted through Permanent Council Decision No. 1106 on 3 December 2013:

1. Participating States will voluntarily provide their national views on various aspects of national and transnational threats to and in the use of ICTs. The extent of such information will be determined by the providing Parties.

2. Participating States will voluntarily facilitate co-operation among the competent national bodies and exchange of information in relation with security of and in the use of ICTs.

3. Participating States will on a voluntary basis and at the appropriate level hold consultations in order to reduce the risks of misperception, and of possible emergence of political or military tension or conflict that may stem from the use of ICTs, and to protect critical national and international ICT infrastructures including their integrity.

4. Participating States will voluntarily share information on measures that they have taken to ensure an open, interoperable, secure, and reliable Internet.

5. The participating States will use the OSCE as a platform for dialogue, exchange of best practices, awareness-raising and information on capacity-building regarding security of and in the use of ICTs, including effective responses to related threats. The participating States will explore further developing the OSCE role in this regard.

6. Participating States are encouraged to have in place modern and effective national legislation to facilitate on a voluntary basis bilateral co-operation and effective, time-sensitive information exchange between competent authorities, including law enforcement agencies, of the participating States in order to counter terrorist or criminal use of ICTs. The OSCE participating States agree that the OSCE shall not duplicate the efforts of existing law enforcement channels.

7. Participating States will voluntarily share information on their national organization; strategies; policies and programmes – including on co-operation between the public and the private sector; relevant to the security of and in the use of ICTs; the extent to be determined by the providing parties.

8. Participating States will nominate a contact point to facilitate pertinent communications and dialogue on security of and in the use of ICTs. Participating States will voluntarily provide contact data of existing official national structures that manage ICT-related incidents and co-ordinate responses to enable a direct dialogue and to facilitate interaction among responsible national bodies and experts. Participating States will update contact information annually and notify changes no later than thirty days after a change has occurred. Participating States will voluntarily establish measures to ensure rapid communication at policy levels of authority, to permit concerns to be raised at the national security level.

9. In order to reduce the risk of misunderstandings in the absence of agreed terminology and to further a continuing dialogue, participating States will, as a first step,

voluntarily provide a list of national terminology related to security of and in the use of ICTs accompanied by an explanation or definition of each term. Each participating State will voluntarily select those terms it deems most relevant for sharing. In the longer term, participating States will endeavour to produce a consensus glossary.

10. Participating States will voluntarily exchange views using OSCE platforms and mechanisms inter alia, the OSCE Communications Network, maintained by the OSCE Secretariat's Conflict Prevention Centre, subject to the relevant OSCE decision, to facilitate communications regarding the CBMs.

11. Participating States will, at the level of designated national experts, meet at least three times each year, within the framework of the Security Committee and its Informal Working Group established by Permanent Council Decision No. 1039 to discuss information exchanged and explore appropriate development of CBMs. Candidates for future consideration by the IWG may include inter alia proposals from the Consolidated List circulated by the Chairmanship of the IWG under PC.DEL/682/12 on 9 July 2012, subject to discussion and consensus agreement prior to adoption.

The following CBMs were first adopted through Permanent Council Decision No. 1202 on 10 March 2016:

12. Participating States will, on a voluntary basis, share information and facilitate inter-State exchanges in different formats, including workshops, seminars, and roundtables, including on the regional and/or subregional level; this is to investigate the spectrum of co-operative measures as well as other processes and mechanisms that could enable participating States to reduce the risk of conflict stemming from the use of ICTs. Such activities should be aimed at preventing conflicts stemming from the use of ICTs and at maintaining peaceful use of ICTs.

With respect to such activities participating States are encouraged, inter alia, to:

– Conduct such activities in the spirit of enhancing inter-State co-operation, transparency, predictability and stability;

– Complement, through such activities, UN efforts and avoid duplicating work done by other fora; and

– Take into account the needs and requirements of participating States taking part in such activities.

Participating States are encouraged to invite and engage representatives of the private sector, academia, centres of excellence and civil society in such activities.

PCOEW6464

13. Participating States will, on a voluntary basis, conduct activities for officials and experts to support the facilitation of authorized and protected communication channels to prevent and reduce the risks of misperception, escalation, and conflict; and to clarify technical, legal and diplomatic mechanisms to address ICT-related requests. This does not exclude the use of the channels of communication mentioned in Permanent Council Decision No. 1106.

14. Participating States will, on a voluntary basis and consistent with national legislation, promote public-private partnerships and develop mechanisms to exchange best practices of responses to common security challenges stemming from the use of ICTs.

15. Participating States, on a voluntary basis, will encourage, facilitate and/or participate in regional and subregional collaboration between legally-authorized authorities responsible for securing critical infrastructures to discuss opportunities and address challenges to national as well as trans-border ICT networks, upon which such critical infrastructure relies.

Collaboration may, inter alia, include:

– Sharing information on ICT threats;

– Exchanging best practices;

– Developing, where appropriate, shared responses to common challenges including crisis management procedures in case of widespread or transnational disruption of ICT-enabled critical infrastructure;

– Adopting voluntary national arrangements to classify ICT incidents in terms of the scale and seriousness of the incident;

– Sharing national views of categories of ICT-enabled infrastructure States consider critical;

– Improving the security of national and transnational ICT-enabled critical infrastructure including their integrity at the regional and subregional levels; and

– Raising awareness about the importance of protecting industrial control systems and about issues related to their ICT-related security, and the necessity of developing processes and mechanisms to respond to those issues.

16. Participating States will, on a voluntary basis, encourage responsible reporting of vulnerabilities affecting the security of and in the use of ICTs and share associated

information on available remedies to such vulnerabilities, including with relevant segments of the ICT business and industry, with the goal of increasing co-operation and transparency within the OSCE region. OSCE participating States agree that such information exchange, when occurring between States, should use appropriately authorized and protected communication channels, including the contact points designated in line with CBM 8 of Permanent Council Decision No. 1106, with a view to avoiding duplication.

Practical Considerations[1]

The provisions of these Practical Considerations do not affect the voluntary basis for the activities related to the aforementioned CBMs.

Participating States intend to conduct the first exchange by October 31, 2014, and thereafter the exchange of information described in the aforementioned CBMs shall occur annually. In order to create synergies, the date of the annual exchanges may be synchronized with related initiatives participating States are pursuing in the UN and other fora.

The information exchanged by participating States should be compiled by each of them into one consolidated input before submission. Submissions should be prepared in a manner that maximizes transparency and utility.

Information may be submitted by the participating States in any of the official OSCE languages, accompanied by a translation in English, or only in the English language.

Information will be circulated to participating States using the OSCE Documents Distribution system.

Should a participating State wish to inquire about individual submissions, they are invited to do so during meetings of the Security Committee and its Informal Working Group established by Permanent Council Decision No. 1039 or by direct dialogue with the submitting State making use of established contact mechanisms, including the email contact list and the POLIS discussion forum.

The participating States will pursue the activities in points 9 and 10 above through existing OSCE bodies and mechanisms.

The Transnational Threats Department will, upon request and within available resources, assist participating States in implementing the CBMs set out above.

1 First adopted as part of Permanent Council Decision No. 1106 on 3 December 2013

In implementing the CBMs, participating States may wish to avail themselves of discussions and expertise in other relevant international organizations working on issues related to ICTs.

Considerations[2]

Participating States will, at the level of designated national experts, meet at least three times each year, within the framework of the Security Committee and its Informal Working Group established by Permanent Council Decision No. 1039, to discuss information exchanged and explore appropriate development of CBMs. Candidates for future consideration by the IWG may include inter alia proposals for CBMs aimed at increasing transparency, co-operation, and stability among States in the use of ICTs. Such efforts should, to the extent that they relate to the mandate of the IWG, take into account and seek to complement the expert-level consensus reports of the 2013 and 2015 United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, including their recommendations on voluntary CBMs, and the Group's work in support of voluntary non-binding norms, rules and principles of responsible State behaviour in the use of ICTs.

The Transnational Threats Department of the OSCE Secretariat, through its Cyber Security Officer will, upon request and within available resources, assist participating States in implementing the CBMs set out above, and in developing potential future CBMs.

2 First adopted as part of Permanent Council Decision No. 1202 on 10 March 2016.

تابِع منظمة الأمن والتعاون في أوروبا

أمانة منظمة الأمن والتعاون في أوروبا
إدارة الأخطار العابرة للحدود
6 شارع فالنر، 1010 فيينا، النمسا

cybersec@osce.org
www.osce.org/secretariat/cyber-ict-security

Organization for Security and Co-operation in Europe