ICDL Arabia

تقرير الجاهزية الإلكترونية لعامي 2018\2017

ما هو مدى جاهزية دول مجلس التعاون الخليجي للأمن الإلكتروني؟

المحتوى

الاختصارات

ADSIC - مركز أبو ظبي للأنظمة الإلكترونية والمعلومات

CERT - فريق الاستجابة لحالات الطوارئ

CSIRT - فريق الاستجابة لحالات الأمن الحاسوبي

CPC – مركز حماية الطفل

GCC – مجلس التعاون الخليجي

GCI - مؤشر الأمن الإلكتروني العالمي

ICDL – الرخصة الدولية لقيادة الحاسب الآلي

ICT - تكنولوجيا الاتصالات والمعلومات

ITU - الاتحاد الدولي للاتصالات السلكية و اللاسلكية

MoI – وزارة الداخلية

NGO - المنظمات غير الحكومية

VGT - القوة العالمية الافتراضية

مؤسسة أي سي دي إل العربية، رائدة فكر في مجال السلامة على الإنترنت

مؤسسة "أي سي دي إل العربية – ICDL Arabia " المعروفة سابقا باسم "مؤسسة الرخصة الدولية لقيادة الحاسوب لمجلس مجلس التعاون الخليجي – ICDL GCC Foundation "، هي الذراع الإقليمي لمؤسسة " الرخصة الأوروبية لقيادة الحاسوب – ECDL Foundation"، وهي مؤسسة غير ربحية مقرها دبلن - إيرلندا أنشئت في عام 1995 من قبل أعضاء اتحاد جمعيات الحاسوب الأوروبية العضو في الاتحاد الأوروبي وبتمويل من مفوضية الاتحاد الأوروبي، بغرض رفع مستوى المهارات الإلكترونية للقوى العاملة وقطاع التعليم وفئات المجتمع في جميع أنحاء أوروبا في ذلك الحين.

واستنادا إلى الدور الريادي لليونسكو في عام 2001 في تقديمها شهادة ICDL للثقافة المعلوماتية للدول العربية حيث قام مكتب اليونسكو في القاهرة بالإشراف المباشر على تشغيل البرنامج في الدول العربية، تم في عام 2004 إنشاء مؤسسة "أي سي دي إل العربية – ICDL Arabia " كمشغل وحيد لبرامج ICDL في جميع دول مجلس التعاون الخليجي (المملكة العربية السعودية، وسلطنة عمان، وقطر، والامارات العربية المتحدة، والكويت والبحرين) و العراق ومصر.

تم تصميم شهادات ICDL لتكنولوجيا الاتصالات والمعلومات اعتماداً على خبرات واسعة من مئات المنظمات الدولية، بما في ذلك جمعيات الحاسوب الوطنية، وهيئات حكومية، بالإضافة لمؤسسات تعليمية وتدريبية؛ وسلطات محلية وإقليمية من حول العالم. نحن نعمل بتعاون منتظم ومستمر مع الجهات السابق ذكرها لتحديد المهارات والمعارف المطلوبة لاستمرارية مواكبة استخدام عناصر التكنولوجيا الإلكترونية على مستوى المستخدم العادي بفعالية وكفاءة، وإمداد الجماهير بأحدث الاتجاهات فيما يتعلق بمهارات تكنولوجيا الاتصالات والمعلومات المطلوبة في مجال العمل اليوم، فيما يغطي ما يتعدى التطبيقات المكتبية الشائعة الإستخدام إلى مواضيع متخصصة موجهة للأفراد وفق أدوارهم واهتماماتهم مثل برامج الأمن الإلكتروني، وأساسيات استخدام وسائل التواصل الاجتماعي، والتسويق الإلكتروني، وتخطيط المشاريع، واستخدام النظم المعلوماتية الصحية، والحوسبة ،وتكنولوجيا الاتصالات والمعلومات في مجال التعليم وغيرها.

على مدى السنوات الخمس الماضية، سخَّرت مؤسسة "أي سي دي إل العربية " العديد من مواردها لرفع مستوى الوعي بأمور السلامة على الإنترنت، مستهدفة المعلمين والطلبة وأولياء الأمر. ومن خلال مسؤوليتها الاجتماعية للشركات استثمرت المؤسسة في تطوير برامج تعليمية لمواجهة المخاطر التي تواجه أطفالنا على الإنترنت ومنها التسلط عبر الإنترنت وإدمان الإنترنت والاستغلال عبر الإنترنت وغيرها.

قامت مؤسسة "أي سي دي إل العربية " بإطلاق مبادرة خدمة مجتمعية ممولة ذاتيا تحت مسمى Onliensense.org للفت انتباه أصحاب القرار وواضعي السياسات والأوصياء والمعنيين الآخرين إلى الحاجة الماسة لاتخاذ الإجراءات اللازمة لخلق عالم أكثر أمانا لأطفالنا عبر الإنترنت، تضمنت العديد من برامج التوعية، والإعلانات ذات الرسائل التوعوية الموجهة عبر المجلات الاجتماعية، وتوزيع الهدايا التي تحمل رسائل توعية بالسلامة على الإنترنت، وتوزيع الملصقات، والنشرات، والمناهج التعليمية.

كما تضمنت المبادرة إطلاق موقع إلكتروني توعوي تحت مسمَى"Onliensense.org" كبادرة خدمة مجتمعية ممولَة ذاتيا من قبل المؤسسة، حيث تحتوي هذه البوابة على أحدث النصائح والإرشادات والمقالات والمواد التعليمية حول كل ما يتعلق بأمور السلامة على الإنترنت وكلها متاحة للجميع بشكل مجاني. كما وأطلقت المؤسسة حديثا قناة يوتيوب جديدة متاحة باللغة العربية عبر Onliensense.org/videos-ar وباللغة الإنجليزية عبر Onliensense.org/videos، تم تحميلها بموسوعة من مقاطع الفيديو التوعوية التي تغطي مواضيع متنوعة متعلقة بسلامة النشء على الإنترنت. كما قامت بتنفيذ ما زاد عن مئة ورشة توعوية في المدارس، ونظمت عشرات المخيمات الصيفية، ونشرت دراسات بحثية سنويا حول مواضيع استخدام وسائل التواصل الاجتماعي والسلامة على الإنترنت - وهذا التقرير هو الأحدث في سلسلة من أربعة تقارير " تقرير الجاهزية الإلكترونية 2017 / 2018".

ويستند نجاح مؤسسة "أي سي دي إل العربية " على الثقة والمسؤولية التي منحنا إياها صانعو السياسات والحكومات والمؤسسات التعليمية في المنطقة ومن جميع أنحاء العالم. ونحن نعمل عن كثب مع سلطات إنفاذ القانون والهيئات التنظيمية لاعتماد أفضل الممارسات في مجال السلامة على الإنترنت من جميع أنحاء العالم مع أخذ الإعتبارات المحلية في الحسبان. هذا وتعتبر مؤسسة "أي سي دي إل العربية " اليوم رائدة فكر وخبيرة موضوعية في مجال السلامة على الإنترنت، وهي ملتزمة تماما بالمساهمة في خدمة المجتمعات التي تعمل فيها، وبتوفير أحدث المعلومات وأفضل الممارسات حول موضوع الأمن الإلكتروني، ودعم جهات إنفاذ القانون والدفاع والتعليم والحكومة والمجتمع ككل.

شكر و تقدير

تود مؤسسة آي سي دي إل-العربية أن تتوجه بالشكر إلى جميع المنظمات التي شاركت في تقديم المعلومات والدراسات المذكورة في هذا التقرير، وتشمل هذه المنظمات الكيانات الحكومية والمنظمات في مختلف الصناعات وأصحاب المصلحة الآخرين، وتستحق المنظمات التالية اهتماماً خاصاً لمساهمتها:

- البنك الدولي
- الأمم المتحدة والاتحاد الدولي للاتصالات السلكية و اللاسلكية (ITU)
- معهد بوتوماك للدراسات السياسية
- وزارة المواصلات والاتصالات - قطر
- هيئة تقنية المعلومات - سلطنة عمان
- شركة HISCOX
- دائرة أبو ظبي للتعليم والمعرفة
- مركز دبي للأمن الإلكتروني
- هيئة تنظيم قطاع الإتصالات - الإمارات
- شرطة عمان

ملخص تنفيذي

تم البدء في استخدام الإنترنت في الدول الأعضاء الست في مجلس التعاون الخليجي بين عامي 1993 و 1997. وبعد أكثر من عقدين من إعداد الأنظمة والاستثمارات من قبل حكومات المنطقة وشركات الاتصالات الوطنية وقيام الشراكات بين القطاعين العام والخاص على هذا الصعيد، اتسعت وسائل الاتصال بشكل كبير، مما أدى إلى نمو سريع في عدد المستخدمين وفي خدمات الحكومة الإلكترونية، والتعليم الإلكتروني، والتجارة الإلكترونية، والخدمات المصرفية الإلكترونية، فضلا عن انتشار استخدام وسائل التواصل الاجتماعي.

مع أكثر من 35 مليون مستخدم للإنترنت في دول مجلس التعاون الخليجي، أصبح معظمنا اليوم يعتمد على الإنترنت بطريقة أو بأخرى. سواء من خلال استخدام وسائل التواصل الاجتماعي أو التطبيقات عبر الإنترنت، كما تزايد اعتماد الأفراد على التكنولوجيا، مما خلق فرص عمل جديدة وحفَز النمو الاقتصادي بمعدلات لم يسبق لها مثيل. ونتيجة لذلك، شهد كل ركن من أركان هذه المنطقة تحسينات كبيرة في تقديم الخدمات، وزيادة الإنتاجية، وغيرها من أشكال الابتكار.

وكما هو الحال في العديد من البلدان الأخرى، يشكل الاستخدام الواسع للإنترنت تحديا كبيرا للحكومة فيما يتعلق بالأمن الإلكتروني. يدرك صناع السياسات إدراكا تاما أن زيادة سرعة الاتصال بشبكة الإنترنت يؤدي إلى التنوع الاقتصادي طالما كانت البنية الأساسية والأجهزة المتصلة بها آمنة نسبيا. وإذا كانت لدى الحكومات رؤى اقتصادية تتضمن اتجاهات إلكترونية ضمن مبادراتها، فمن الضروري النظر في التدابير الوقائية ومواءمتها مع الأهداف الرامية إلى بناء أساس متين للأمن الإلكتروني.

ولأن التكنولوجيا والعالم الإلكتروني يتطوران بسرعة كبيرة، يحتاج واضعو السياسات إلى قياس جاهزية أمنهم الإلكتروني في بلدانهم بانتظام. ويتعين عليهم أن يضعوا نهجا شاملا لضمان حماية مواطنيهم من الاحتيال المالي عبر الإنترنت وغيره من أشكال الانتهاكات. ويجب أن تترجم استراتيجيات الجاهزية الإلكترونية إلى خطط عمل محددة.

ويسعى التقرير السنوي "لمؤسسة أي سي دي إل العربية" ، المعنون باسم "جاهزية الأمن الإلكتروني لدول مجلس التعاون الخليجي لعام 2017" إلى طرح منظور حديث حول استعداد دول مجلس التعاون الخليجي لحماية نفسها من المخاطر الإلكترونية. ويهدف التقرير كذلك إلى إبراز أصحاب المصلحة المعنيين وأهمية مشاركتهم في التطوير الجاري للأطر الخاصة بتحسين إدارة الأمن اللإكتروني، مع العمل في المجالات التي تتطلَب الاستثمار؛ ليس فقط لامتلاك شبكة بنية تحتية قوية ولكن أيضا لخلق مساحة إلكترونية أكثر أمنا وأكثر ثقة.

والاشتراطات التالية هي الاعتبارات الرئيسية التي ينبغي مراعاتها عند وضع استراتيجية وطنية للاستعداد للأمن الإلكتروني:

• توسيع الاستراتيجية الوطنية للأمن الإلكتروني لتشمل التدريب القانوني والتقني والتنظيمي وبناء القدرات [التعليم والتدريب والتوعية]، فضلا عن التعاون [الشراكة بين القطاعين العام والخاص، والتعاون بين الحكومات، والتعاون مع الحكومات الأجنبية، ومشاركة عامة الجمهور] .

• تحديد ومعالجة نقاط المخاوف الحالية التي يحتمل أن تبطئ من معدل استهلاك الإنترنت بسبب عدم الثقة؛

• تحديد أحدث الاتجاهات العالمية على الانترنت التي من المحتمل أن تسبب ضررا للمجتمع من سوء الاستخدام، والثغرات الأمنية، والاختراقات الإلكترونية؛

• مراقبة ودراسة ومقارنة تدابير الأمن الإلكتروني للحكومات الأخرى، بما في ذلك تبادل المعلومات المتعلقة بالاهتمامات والآراء والخبرات الجديدة في حماية المواطنين؛

• وأخيرا اعتماد المعايير العالمية وأفضل الممارسات التي أثبتت فعاليتها لتعزيز ثقافة الأمن الإلكتروني العالمي وتكثيف الدفاعات لمواجهة التهديدات الجديدة الناتجة عن التطور الإلكتروني المستمر.

نبذة عن دول مجلس التعاون الخليجي

الوصف	البحرين	الكويت	سلطنة عمان	قطر	المملكة العربية السعودية	الإمارات العربية المتحدة
						
عدد سكان الدولة (مليون)	1.425	4.053	4.425	2.57	32.28	9.27
نسبة الزيادة السكانية (السنوية)	3.80%	2.90%	5.20%	3.50%	2.20%	1.20%
إجمالي قيمة الناتج المحلي بأسعار السوق (بليون دولار)	31.86	114	66.29	152.5	646.4	348.7
نسبة زيادة إجمالي الناتج المحلي(السنوية)	2.90%	1.80%	5.70%	2.20%	1.70%	3.00%
عام إدخال شبكات الإنترنت	1995	1993	1997	1995	1995	1995
الإستراتيجية القومية للأمن الإلكتروني	لم تنشر	لم تنشر	لم تنشر	http://bit.ly/2vpnypv	http://bit.ly/2ij8zbq	لم تنشر
نطاق الإنترنت	.bh	.kw	.om	.qa	.sa	.ae
مستخدمو الإنترنت لكل 100 شخص	93.5	82.1	74.2	92.9	69.6	91.2
الاشتراكات وشبكات النطاق العريض الثابت لكل 100 مستخدم	18.61	1.535	5.61	10.116	11.924	12.89
اشتراكات الهواتف الخلوية المحمولة لكل 100 مستخدم	185.262	231.763	159.861	159.132	179.589	187.348

منهجية هذا البحث

في بحثها حول جاهزية الأمن الإلكتروني في منطقة دول مجلس التعاون الخليجي، قامت مؤسسة أي سي دي إل العربية بالنظر في خمسة معايير رئيسية الى جانب الإشارة إلى المصادر المحلية والدولية في هذه العملية. واعتمد هذا التقرير على بيانات من "تقرير مؤشر الأمن الإلكتروني العالمي لعام 2017" و "ملامح الصحة الإلكترونية" الصادران عن الاتحاد الدولي للاتصالات، وهي وكالة متخصصة تابعة للأمم المتحدة ومسؤولة عن المسائل المتعلقة بتكنولوجيا الاتصالات والمعلومات.

يحدد هذا البحث عددا من الأهداف من خلال معايير قابلة للقياس ويقيم مدى النتائج المحققة. وقد قام الاتحاد الدولي للاتصالات بتقييم كل بلد في تقريره من خلال خمسة عناصر أساسية تقيس مدى الاستعداد للأمن الإلكتروني على النحو التالي.

التعاون بناء القدرات التدابير التنظيمية التدابير التقنية التدابير القانونية

واعتمادا على أبحاثها واكتشافاتها على الانترنت من خلال مراجعة التفاعلات والمعلومات التي تقدمها السلطات الحكومية المعنية، سوف تقدم مؤسسة أي سي دي إل العربية نتائجها في هذا التقرير من خلال المعايير الخمسة المذكورة أعلاه لتبيان تقييمها الخاص بها لكل دولة من دول مجلس التعاون الخليجي من ناحية جاهزية الأمن الإلكتروني والتدابير التي اتخذتها كل دولة لتعزيز أفضل الممارسات.

وسيوصي التقرير أيضا بتوسيع نطاق المبادرات الحكومية الرامية إلى تعزيز الوعي بالأمن الإلكتروني من خلال تعظيم مشاركة عامة الجمهور والقطاع الخاص.

الأهداف المنشودة

حتى الآن، كان هناك القليل جدا من البحوث التي تركز على استعداد دول مجلس التعاون الخليجي للأمن الإلكتروني. تهدف مؤسسة أي سي دي ال العربية إلى جذب المزيد من الاهتمام إلى هذا الموضوع ودفع اعتماد أفضل الممارسات والابتكار في مجال الأمن الإلكتروني في المنطقة في وقت مبكر.

سيسعى هذا التقرير أيضا إلى الكشف عن الأسباب الكامنة وراء تبوؤ بعض البلدان التي مراتب عالية على هذا الصعيد والجوانب التي تحتاج فيها دول مجلس التعاون الخليجي إلى قدر كبير من التحسن.

نحن على ثقة من أن هذا التقرير سوف يقنع صنَاع السياسات في دول مجلس التعاون الخليجي بإعادة تقييم جاهزية بلدانهم للأمن الإلكتروني والنظر في تخصيص ميزانيات خاصة لتعزيز الأمن الإلكتروني.

ويشمل ذلك أيضا إدخال الإصلاحات اللازمة لتمكين أصحاب المصلحة من بناء بنية تحتية أفضل للأمن الإلكتروني لإبقاء سكان تلك الدول آمنين في عالم الإنترنت.

قوة الأمن الإلكتروني في منطقة مجلس التعاون الخليجي

على مدى السنوات ال 25 الماضية، كانت تكنولوجيا الاتصالات والمعلومات والإنترنت في طليعة التطور التكنولوجي. وقد ساعدت على تحويل المجتمع إلى ما نشير إليه الآن باسم العصر الإلكتروني. وتعد مبادرات مثل الحوكمة الإلكترونية والتجارة الإلكترونية والخدمات المصرفية الإلكترونية والصحة الإلكترونية والتعلم الإلكتروني من بين العديد من المجالات التي ظهرت مع وجود الإنترنت والتي تعتبرها دول المجلس عوامل حاسمة في جدول أعمالها الاقتصادي.

وتواصل الحكومات تطويرها في هذه المجالات بسبب فوائد كبيرة مثل الكفاءة والشفافية مما يسفر عن نمو اقتصادي أسرع وزيادة ثقة الجمهور. وأشار المنتدى الاقتصادي العالمي إلى دراسة أجريت في عام 2009 تشير إلى أن الناتج المحلي الإجمالي للبلد سيزداد بنسبة تصل إلى 2% في حالة ارتفاع معدل انتشار الإنترنت بنسبة 10%.

وبعد مرور عقد تقريبا، وصلت منطقة الخليج إلى نقطة تحول في العصر الإلكتروني. وقد مكن التحول الجوهري في انتشار الإنترنت في دول مجلس التعاون الخليجي بين عامي 2000 و 2015 غالبية الأشخاص في هذه المناطق من الوصول إلى شبكة الإنترنت. وسيتم تسجيل نحو 226 مليون مستخدم في الدول العربية على شبكة الإنترنت بحلول عام 2018[2].

أصبح الاتصال بالإنترنت من أقل المشكلات التي يمكن أن تواجهها في هذا الجزء من العالم. ومع ذلك، نجد أن عدد التهديدات الإلكترونية هو الذي يتزايد باستمرار. **في عام 2016، كان 0.7٪ من إجمالي الأشخاص الذين أصيبوا بفيروس الفدية العالمي في المملكة العربية السعودية، في حين كان 0.5٪ في الإمارات العربية المتحدة.** [3]

كلما تطور الإنترنت أصبح يحوي كميات أكبر من المعلومات الحساسة مما يسبب ارتفاع معدل الوصول والأنشطة على الانترنت، وبذلك تزداد فرص مجرمي الإنترنت المتربصين للحصول على هذه المعلومات. ولذلك، يتحتم على صانعي السياسات مواءمة رؤيتهم الاقتصادية وأولويات الأمن القومي بالتوازي مع الأمن الإلكتروني. وليس فقط من شأن ذلك أن يساعد البلدان على حماية المعلومات الحساسة، بل أيضا يساعد ذلك في منع النشاط الإلكتروني الذي يتعارض مع القيم الثقافية لدول مجلس التعاون الخليجي.

تكلفة الهجوم الإلكتروني

التهديدات الإلكترونية يمكن أن تأتي في أشكال مختلفة مثل البرمجيات الخبيثة، وبرامج التجسس، و فيروسات الفدية، وفي الأوقات الحالية ترتبط معظم هذه الأشكال مع تسرب البيانات والابتزاز النقدي. وهذا الاتجاه واضح في بعض أكبر الهجمات التي نفذت حتى الآن هذا العام 2017 [4]. كل هجوم يمكن أن يكون مكلفا للغاية للحكومات والشركات والأفراد.

أنواع الأضرار التي يمكن أن تسببها الهجمات الإلكترونية:

خسارة النفقات: وفقا لتقرير Hiscox لعام 2017، كلفت الجريمة الإلكترونية الاقتصاد العالمي أكثر من 450 مليار دولار في2016 [5]

فقدان البيانات الحساسة: تم سرقة أكثر من ملياري سجل شخصي في عام 2016، بما في ذلك ملايين السجلات الطبية [6]

أضرار تلحق بالمعدات: الأضرار التي لحقت بالمعدات الإلكترونية المتصلة بالإنترنت من خلال شبكة داخلية

حظر وتوقف في الخدمات الإلكترونية: عدم توفر المواقع الإلكترونية أو غيرها من الخدمات الإلكترونية بسبب البرامج الضارة التي تمنع الخوادم

انقطاع في الاتصال بالشبكة : إغلاق / تباطؤ الشبكات المحلية أو منع الوصول إلى الإنترنت

مقدمة عن استعدادات الأمن الإلكتروني

يؤكد العديد من الخبراء حقيقة إنه لا يوجد أحد مستعد للأمن الإلكتروني تماما. وهناك عدة أسباب لعدم تمام الاستعداد؛ والسبب الرئيسي واضح - التطور التكنولوجي السريع. مع تحسُن الإجراءات الأمنية؛ ومواكبة ذلك بتحسين خطط المواجهة من قبل مجرمي الإنترنت". وقد أثبتت هجمات فيروس الفدية مثل Wannacry و Petya هذا الأمر.

وبينما نشير في الغالب إلى مؤشر الأمن الإلكتروني العالمي [8] في بحثنا، فإن مؤشر الاستعداد للأمن الإلكتروني(CRI) الذي أصدره معهد بوتوماك للدراسات السياسية، جدير بالذكر هنا أيضا، لأنه يدعم ما توصل إليه مؤشر الأمن الإلكتروني العالمي فيما يتعلق بحالة الاستعداد للأمن الإلكتروني. كما ساعدت مبادرة الاستعداد للأمن الإلكتروني على إثارة النقاش الدولي وأثارت أنشطة عالمية ضد ما يسمى "انعدام الأمن الإلكتروني".

أخذ مؤشر الاستعداد للأمن الإلكتروني في الاعتبار نقاط الضعف الإلكترونية والأثر السلبي المحتمل لعدم وجود استعداد للأمن الإلكتروني على الاقتصادات، وقيَم موضوعيا نضج كل بلد والتزامه والتأهب للأمن الإلكتروني والقدرة على الصمود. وأوصى بالتدابير التي يمكن أن تتخذها البلدان لحماية اقتصاداتها ذات الصلة العالية والحفاظ على نموها المحتمل في الناتج المحلي الإجمالي عن طريق توفير الأمن الإلكتروني. ويشار أدناه إلى الركائز الخمسة لأهلية الأمن الإلكتروني التي تركز عليها البحوث المقدمة من مؤشر الأمن الإلكتروني العالمي بشكل قاطع، وتتطرق إلى ذلك بشكل عام[9].

التدابير القانونية: هل أظهر بلد ما الالتزام بالحماية من الجرائم الإلكترونية؟

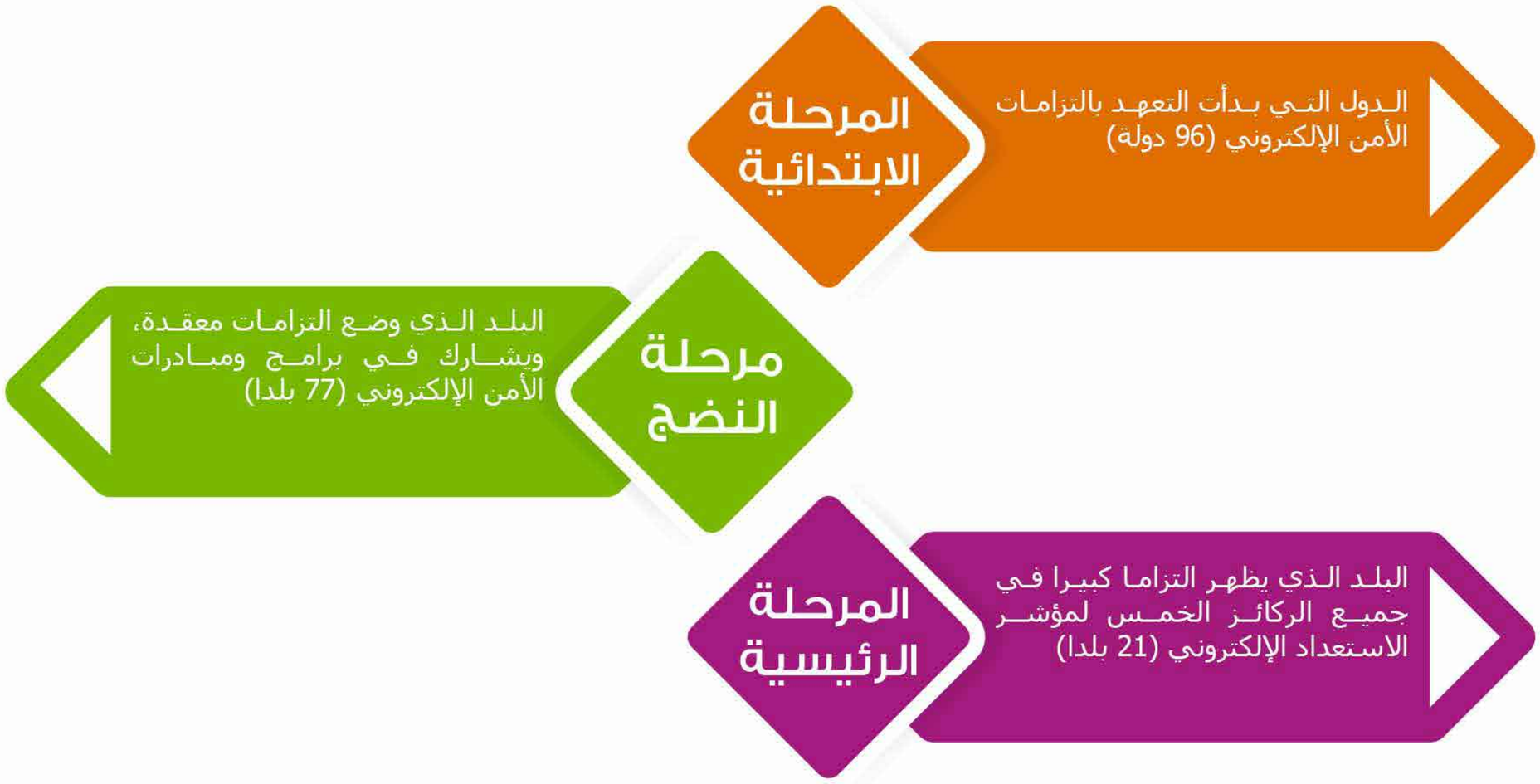
التدابير التقنية: هل لدى أي بلد فريق استجابة لحالات الطوارئ في مجال الكمبيوتر أو فريق استجابة لحالات أمن الكمبيوتر؟

التدابير التنظيمية: هل قدمت الحكومة استراتيجية للأمن الإلكتروني تستلزم جهة تنسيقية ومؤشرات محددة جيدا لتتبع الجرائم الإلكترونية؟

بناء القدرات: هل أظهر بلد ما أنه يستثمر في أبحاث الأمن الإلكتروني، وأنه يقدم حوافز للقطاع الخاص لتعزيز الأمن الإلكتروني، و / أو تمويل مبادرات الأمن الإلكتروني؟

التعاون: هل أظهر بلد ما جهودا تعاونية عبر المجالات الوطنية والدولية وبين القطاعين العام والخاص؟

وتوجد ضمن هذه الركائز الخمسة مؤشرات مختلفة قام مؤشر الأمن الإلكتروني العالمي من خلالها بتقييم كل بلد. كانت إجابات الأسئلة إما "نعم" أو "لا" وتم تصنيف البلدان إلى ما يلي:



وفيما يلي مقارنة بين الدرجات الكلية لدول مجلس التعاون الخليجي والمراتب العالمية:

الدولة	البحرين	الكويت	سلطنة عمان	قطر	المملكة العربية السعودية	الإمارات العربية المتحدة
التصنيف العالمي	65	139	4	25	46	47
مستوي الأمن الإلكتروني	عالي	بدائي	متقدم	عالي	عالي	عالي
درجة المؤشر العالمي للأمن الإلكتروني	0.57	0.1	0.87	0.68	0.57	0.57

سلطنة عُمان هي الدولة الوحيدة في مرحلة الريادة

قطر، الإمارات العربية المتحدة، والبحرين (ومرتبتها 65) في مرحلة النضج

الكويت هي الدولة الوحيدة في مرحلة البدء

وبعد وضع سياق للاستجابة العاجلة للأمن الإلكتروني في دول مجلس التعاون الخليجي، فإن هذا التحليل هو تحليل الاستعداد الإلكتروني في دول مجلس التعاون الخليجي، استنادا إلى الركائز الخمسة التي يستخدمها مؤشر الأمن الإلكتروني العالمي كمعايير رئيسية.

التدابير القانونية

تشكل التشريعات تدبيرا حاسما لتوفير إطار منسق في جميع قطاعات المجتمع. ولكي تكون مستعداً إلكترونياً، فإن توفير إطار قانوني يتعين على الجمهور الالتزام به أمر ضروري. كما أنه يساعد على وضع تدابير قابلة للتشغيل المتبادل لتسهيل مكافحة الجريمة الإلكترونية على الصعيد الدولي ويضع المعايير الدنيا للسلوك بشأن الكيفية التي ينبغي بها بناء المزيد من قدرات الأمن الإلكتروني. ويقيس مؤشر الأمن الإلكتروني العالمي البيئة القانونية استناداً على الوجود والعدد الخاص بالمؤسسات والأطر القانونية التي تتناول الأمن الإلكتروني والجريمة الإلكترونية. و تشمل المؤشرات الثلاثة التالية:

ا) قانون الجرائم الإلكترونية

في عالم مترابط للغاية، يمكن أن تنشأ الجرائم الإلكترونية من أي مكان وتؤثر على بلدان متعددة. أيضا، وعلى عكس الجريمة التقليدية، فإن الجريمة الإلكترونية ليست محددة جيداً حتى الآن. ولذلك، من المهم أن تكون قوانين الجرائم الإلكترونية شاملة. ويجب أن تدرج هذه القوانين جميع الأعمال غير القانونية الممكنة،وأن تبقى على علم بأنواع جديدة من الجرائم وان يكون لديها إطار تحقيق قادر على تحديد أنواع جديدة من الأدلة وتوثيقها وتحليلها. وينبغي دعم القوانين بإطار التعاون الدولي القوي الذي يمكن أن يقدم الجناة من أي جزء من العالم إلى العدالة. في هذا القسم، قمنا بإدراج التشريعات الحالية المتعلقة بالجريمة الإلكترونية وفحص مدى فعالية إطارها.

فيما يلي التشريعات الخاصة بالجريمة الإلكترونية التي أعدتها أو صاغتها دول مجلس التعاون الخليجي (مثلما تم مناقشتها في مؤتمر الأمم المتحدة للتجارة والتنمية [10]:

الدولة	عنوان التشريع / قانون التشريع	روابط القوانين
البحرين	المرسوم التشريعى رقم 28 لسنة 2002 بشأن التعاملات الإلكترونية (باللغة العربية)	http://bit.ly/ICDL2017a
الكويت	مشروع قانون مكافحة جرائم الإنترنت	No Link Available
سلطنة عمان	المرسوم الملكي رقم 2011/12 (باللغة الإنجليزية)	http://bit.ly/ICDL2017B
قطر	قانون الإتصالات (رقم 34) 2006 (باللغتين الإنجليزية والعربية)	http://bit.ly/ICDL2017C
المملكة العربية السعودية	القانون رقم 79 بشأن جرائم تكنولوجيا المعلومات لعام 2007 (بالإنجليزية)	http://bit.ly/ICDL2017D
الإمارات العربية المتحدة	القانون الاتحادي رقم 2 بشأن مكافحة جرائم الإنترنت (باللغة الإنجليزية)	http://bit.ly/ICDL2017E

إن جميع دول مجلس التعاون الخليجي باستثناء الكويت لديها تشريعات لمكافحة الجرائم الإلكترونية، إلا أن هذه التشريعات يجب أن تكون أشمل بكثير، كما هو موضح في البحث الذي أجراه مركز Chatham House [11].

وفيما يلي مقارنة بين قوانين الجريمة الإلكترونية في دول مجلس التعاون الخليجي، من حيث شمولها، (وفقا للبحث المقدم من مركز (Chatham House):

الدولة	البحرين	الكويت	سلطنة عمان	قطر	المملكة العربية السعودية	الإمارات العربية المتحدة
التعريفات	✓	✓	✓	✓	✓	✓
التجريم	✓	✓	✓	✓	✓	✓
الصلاحيات الإجرائية	✓			✓		
الأدلة الإلكترونية						
التعاون الدولي						

ملاحظات عامة استناداً إلى بحث Chatham House

- **التعريفات:** تقوم جميع البلدان بتعريف قوانين الجريمة الإلكترونية بوضوح مع الاخذ بالاعتبار الجريمة الإلكترونية.

- **التجريم:** تحدد جميع البلدان قوانين الجريمة الإلكترونية بوضوح والأفعال التي تعتبر إجرامية وتذكر العقوبة المقابلة لها

- **الصلاحيات الإجرائية:** تحدد كل من البحرين وقطر فقط عملية يتم من خلالها ممارسة الصلاحيات القانونية مع الحكم على الجرائم الإلكترونية

- **الدليل الإلكتروني:** لا تنظر أي من البلدان بشكل شامل في الأدلة الإلكترونية كجزء من التحقيق في الجرائم االإلكترونية

ب) اللائحة الإلكترونية

يشـير مؤشـر الأمـن الإلكترونـي العالمـي إلـى أن سـلطنة عُمـان هـي الدولـة الوحيـدة فـي دول مجلـس التعـاون الخليجـي التـي لديهـا أنظمـة راسـخة للجريمـة الإلكترونيـة. فـي حيـن أن 80٪ مـن دول مجلـس التعـاون الخليجـي قـد وضعـت تشـريعات للحـد مـن الجريمـة الإلكترونيـة، فـإن نتائـج مؤشـر الأمـن الإلكترونـي العالمـي تشـير بوضـوح إلـى أن القوانين وحدها لن تكون فعالة في المنطقة، ما لم يتم وضع اللوائح اللازمة لإنفاذ القوانين.

ويستشـهد مؤشـر الأمـن الإلكترونـي العالمـي بـأن تنظيـم سـلطنة عُمـان للأمـن الإلكترونـي هـو أفضـل مثـال بيـن جميـع البلـدان علـى الصعيـد العالمي.**ويمكـن لدول مجلس التعـاون الخليجي اختيار أفضل الممارسـات من إطار الحكومـة الإلكترونيـة فـي سـلطنة عُمـان،** والـذي يحدد القواعـد والإجـراءات التي تضمـن أن تكون مشـاريع ونظم تكنولوجيـا المعلومـات الحكوميـة مسـتدامة ومتوافقـة مـع اسـتراتيجياتها وأهدافهـا المتعلقـة بتكنولوجيـا الاتصـالات والمعلومات. وهذا يسـهل الإدارة الفعالة للمخاطر المتعلقة بتكنولوجيا الاتصالات والمعلومات.

ج) التدريب الإلكتروني:

يحتـاج موظفـو إنفـاذ القانـون والأعضـاء القضائيـون إلـى التدريـب المناسـب علـى سياسـات الأمـن الإلكترونـي، فضـلا عـن تنفيـذ تلـك القوانيـن. ويحتـاج المحامـون أيضـا إلـى تلقـي تدريـب متكـرر - ويفضـل أن يكـون ذلـك عـن طريـق شـهادات معرفية عندما يتلقون التدريب - نظرا لأن الجرائم الإلكترونية تتطور باستمرار.

لـم تتلـق مؤسسـة أي سـي دي ال العربيـة أيـة إشـارات مـن السـلطات الحكوميـة فيمـا يتعلـق بتدريـب المشـرعين والمحاميـن، ولذلـك تـم بحـث هـذا الجانـب فـي الغالـب مـن خـلال البحـث فـي الأخبـار عبـر الإنترنـت والإعلانـات الصـادرة عن هيئات الأمن الإلكتروني الحكومية [12و 13و 14 و15].

وفـي الوقـت الـذي أعلنـت الجهـات الحكوميـة والخاصـة عـن ورش عمـل حـول القانـون الإلكترونـي، فإنـه لا يوجـد هنـاك أيـة أنبـاء مـن أو عـن مراكـز تدريـب متخصصـة للتدريـب علـى القانـون الإلكترونـي. تتطلـب الوتيـرة التـي تـزداد بهـا الجرائـم الإلكترونيـة إنشـاء مراكـز تدريـب متخصصـة فـي مجـال القانـون الإلكترونـي وترعاهـا الحكومـة بحيـث لا يتـم تثقيـف المحامين فحسـب بل أيضا المسؤولين الحكوميين.

التدابير التقنية

بـدون التدابيـر التقنيـة الكافيـة والقـدرات اللازمـة للكشـف عـن الهجمـات الإلكترونيـة والاسـتجابة لهـا، سـتظل الحكومـات عرضـة للتهديـدات الإلكترونيـة. ويركـز الاتحـاد الدولـي للاتصـالات السـلكية واللاسـلكية بشـكل كبيـر علـى التدابيـر التقنيـة، مشـيرا إلـى أنـه "خـط الدفـاع الأول ضـد التهديـدات الإلكترونيـة والبرمجيـات الضـارة علـى الإنترنـت"[16]. يقـاس هـذا العنصـر اسـتنادا إلـى وجـود مؤسسـات وأطـر تقنيـة تتنـاول برمجيـات الأمـن الإلكترونـي التـي أقرهـا بلـد مـا. ويشـمل ذلـك فـرق الاسـتجابة الحكوميـة والخاصـة فـي حـالات الطـوارئ لتحديـد التهديـدات الإلكترونيـة والدفـاع عنهـا وإدارتها وتعزيز الأمن.

ومـن الضـروري زيـادة مخصصـات الميزانيـة لتعزيـز فـرق الاسـتجابة للأمـن الإلكترونـي وتزويدهـا بالوسـائل اللازمـة لمواجهـة الهجمـات الجديـدة. **ويعتقد الخبـراء أن هناك حاجة إلى المزيد من الاسـتثمارات في مجال أمن البنيـة التحتيـة فـي دول مجلس التعاون الخليجي،** مما يسـلط الضوء على تهديـد الأمن الإلكتروني في أعقاب الهجمات التي وقعت في الماضي [17].

بالإضافـة إلـى فـرق الاسـتجابة، تحتـاج البلـدان إلـى الالتـزام بمعاييـر الأمـن الإلكترونـي المعتـرف بهـا دوليـا لممارسـات تكنولوجيـا الاتصـالات والمعلومـات والبرمجيـات. وسـوف يسـتفيد مجلـس التعـاون الخليجـي أيضـا إذا كان يوفـر برامـج شـهادة الأمن الإلكتروني لموظفي الحكومة والقطاع الخاص للتحقق من مهاراتهم.

التدابير التنظيمية

فيما يلي معايير الاتحاد الدولي للاتصالات التي تقيس مدى فعالية تعامل الحكومة مع التهديدات الإلكترونية:

أ) الإستراتيجية الوطنية

يحتاج البلد إلى إعطاء الأولوية للأمن الإلكتروني ووضع مجموعة شاملة من الأهداف والسياسات والتدابير الإجرائية لتعزيز الأمن. وينبغي أن تصادق جميع قطاعات الحكومة على السياسات وأن تكون مدفوعة بمؤشرات أداء رئيسية واضحة.

وتعد الاستراتيجية الوطنية للأمن الرقمي في المملكة المتحدة[18] مثالا جديرا بالذكر، فهو يوفر سياقا للاتجاهات والفرص التي يعترف بها البلد إزاء التكنولوجيا في إطار زمني مدته خمس سنوات. كما أنه يفسر كيف سيغير السلوكيات العامة والتجارية على حد سواء في معالجة التهديدات بثقة في المجال الرقمي. وقد ضاعفت المملكة المتحدة استثماراتها في مجال الأمن الرقمي مقارنة بخطتها السابقة (1.9 مليار جنيه إسترليني).

وثمة مثال مماثل لنهج مدروس جيدا تجاه الأمن الإلكتروني هو مبادرة أعلنتها حكومة دبي مؤخرا. وتركز استراتيجية دبي للأمن الإلكتروني [19] على ما يلي:

- زيادة الوعي العام بأهمية الأمن الإلكتروني، وضمان بناء مجتمع يدرك تماما مخاطر الجريمة الإلكترونية، فضلا عن تطوير المهارات والقدرات اللازمة لإدارة مخاطر الأمن الإلكتروني بين المؤسسات الحكومية والخاصة والأفراد
- ابتكار وإنشاء فضاء إلكتروني آمن يتسم بالحرية والعدالة
- بناء فضاء إلكتروني آمن من خلال وضع ضوابط لحماية سرية البيانات وسلامتها وتوفرها وخصوصيتها
- الحفاظ على مرونة الفضاء الإلكتروني (المرونة الإلكترونية) وضمان استمرارية وتوافر نظم تكنولوجيا الاتصالات والمعلومات في الفضاء الإلكتروني

سنغافورة هي مثال جيد أيضا. فقد تم تصنيفها من قبل الاتحاد الدولي للاتصالات في المرتبة رقم 1 في الاستعداد الإلكتروني [20] . 60 في المائة من سكان سنغافورة واثقون من قدرتهم على مواجهة أية اختراقات إلكترونية. وهذا أعلى بكثير من المتوسط العالمي البالغ 47 في المائة [21]. **ويمكن لدول مجلس التعاون الخليجي أيضا أن تجتذب المزيد من المشاركة في بناء اقتصاد إلكتروني أقوى من خلال تعزيز ثقة القطاع الخاص والمواطنين في حماية أنفسهم عبر الإنترنت.** ويتعين على وزارات الداخلية ووزارات التربية والتعليم العمل على تحقيق ذلك.

ب) نموذج الحوكمة

يجب وضع استراتيجية وطنية متينة من خلال وضع خارطة طريق للحوكمة من أجل التصدي للتحديات وإظهار كيفية تطبيق السياسات. كما يجب أن تأخذ في الحسبان إجراءات تبادل المعلومات السرية، سواء في القطاع العام أو بين القطاعين العام والخاص.

أجرت الحكومة الكندية في مدينة أوتاوا مؤتمرات نقاشية عامة لمدة ثلاثة أشهر [22] حول تحديث استراتيجية الأمن الإلكتروني. وطلبت من المهنيين الأمنيين داخل القطاع الخاص تقديم مدخلاتهم الأساسية للحفاظ على الاقتصاد الإلكتروني للبلاد قوي وآمن.

وقدمت هذه المبادرة أفكارا جديدة وساعدت كندا على تحديد الثغرات والفرص لتشكيل نهجها في مجال الأمن الإلكتروني. وقد عزز هذا أيضا ثقة الجمهور في الحكومة مع منحهم شعورا بالمشاركة.

ج)الوكالة/الوكالات المسؤولة

ذكر الاتحاد الدولي للاتصالات أن إدارة الأمن الإلكتروني تحتاج إلى أن تضطلع بها هيئات إشرافية متماسكة مثل اللجان الدائمة والمجالس الاستشارية أو المراكز متعددة التخصصات.

ينبغي أن تكون معظم هذه المراكز مسؤولة عن نظم المراقبة، والاستجابات للحوادث الإلكترونية، والإشراف على تنفيذ الاستراتيجيات، وتحسين الهياكل التنظيمية اللازمة لتنسيق الاستجابات للهجمات الإلكترونية.

في دول مجلس التعاون الخليجي، يمكن إنشاء وكالات (مجالس للأمن الإلكتروني) على غرار الوكالات التي أوصى بها الاتحاد وتعيينها من قبل وزارات الداخلية في البلدان الأعضاء.

ولا تزال غالبية دول مجلس التعاون الخليجي في المرحلة الأولى من تشكيل هيئات مستقلة مكرسة للأمن الإلكتروني. وفي حين أن البحرين والكويت وسلطنة عمان قد كلفت هيئات تكنولوجيا الإتصالات والمعلومات أو هيئات الإتصالات بمسؤولية إضافية ألا وهي الأمن الإلكتروني، أنشأت الإمارات العربية المتحدة والمملكة العربية السعودية هيئات حكومية مخصصة للأمن الإلكتروني.

وفي عام 2012، أنشأت دولة الإمارات جهاز استخبارات الإشارة (NESA) للعمل على توسيع نطاق التعليم الإلكتروني وخلق ثقافة تعاونية متجذرة في تكنولوجيا الاتصالات والمعلومات والابتكار. وفي نوفمبر 2017، أعلنت المملكة العربية السعودية عن تشكيل هيئة وطنية للأمن الإلكتروني بهدف <تعزيز الأمن الإلكتروني في البلاد لحماية مصالحها الحيوية والأمن القومي والبنية التحتية الحساسة>

تحدثت مؤسسة أي سي دي إل العربية إلى ممثلين حكوميين من جميع دول مجلس التعاون الخليجي وخلصت إلى أن محاولات إنشاء وكالات لمكافحة جرائم الإنترنت في هذه الدول تحتاج إلى قوة دفع أكبر بكثير. إن أعضاء مجلس التعاون الخليجي إما في طور إنشاء مراكز للجرائم الإلكترونية، أو أنهم شكلوا مراكز تحتاج إلى بذل جهود أكبر من أجل تحقيق إنصاف أفضل أمام الجمهور.

د) مقاييس الأمن الإلكتروني

من الضروري إجراء قياس مستمر لمبادرات الأمن الإلكتروني، لا سيما في جو من التهديدات الإلكترونية المتطورة بسرعة. وسيساعد الحفاظ على مقاييس الأمن الإلكتروني البلدان على الالتزام بمعايير محددة، سواء في القطاعين العام والخاص. وستساعد هذه المقاييس في تحديد ما يحتاجه المتخصصون في تكنولوجيا الاتصالات والمعلومات ليكونوا على دراية بكيفية تحسين تكنولوجياتهم، وكيف يمكن أن تحفز بشكل أفضل الاقتصاد الإلكتروني ككل.

أحد البلدان التي تفعل ذلك جيدا هي هولندا. وفي التقرير السنوي لتقييم الأمن الإلكتروني التابع لمركز الأمن الإلكتروني الوطني، جمع التقرير تقارير الإفصاح والتقارير الأمنية والحوادث باستخدام نظام التسجيل[23].

بناء القدرات

في الاقتصادات التي تعتمد على المعرفة العالية، يمكن تعزيز الأمن الإلكتروني من خلال تحسين التعليم في مجال تكنولوجيا الاتصالات والمعلومات. ولذلك، تحتاج البلدان إلى تطوير وتعزيز المهارات الإلكترونية للجمهور. وقام الاتحاد الدولي للاتصالات بتقييم بناء القدرات من خلال ما يلي: برامج البحث والتطوير، وحملات التوعية العامة، والدورات التدريبية التعليمية والمهنية، والشهادات (بموجب المعايير المعترف بها دوليا)، وآليات الحوافز للشركات لتدريب موظفيها.

وتحدثت مؤسسة أي سي دي ال العربية مع ممثلي حكومات دول مجلس التعاون الخليجي فيما يتعلق بهذا الجانب من بناء القدرات. وفيما يلي نظرة عامة على البرامج والمبادرات في دول مجلس التعاون الخليجي.

أ) حملات التوعية العامة

تشجع الحكومات المحلية الأشخاص على أن يصبحوا أكثر وعيا عبر الإنترنت من خلال الحملات التي تعزز الوعي بقضايا معينة. وقد استثمرت كل دول مجلس التعاون الخليجي تقريبا في مشاريع مختلفة لإشراك الجمهور في موضوعات تتعلق بالأمن الإلكتروني والسلامة الإلكترونية. حتى أن بعض المواقع الإلكترونية التي تمولها الحكومات في هذه الدول مكرسة لرفع مستوى الوعي (راجع قسم الوجود على الإنترنت).

يهدف برنامج أقدر المقدم من "وزارة الداخلية في دولة الإمارات العربية المتحدة" إلى زيادة الوعي الوطني بمنع الجريمة وتثقيف الطلبة حول قضايا الصحة والسلامة. ومنذ عام 2013، تعاون مع وزارة التربية والتعليم ومجلس أبوظبي للتعليم في تنفيذ ورش التوعية بالسلامة الإلكترونية موجَهة لجميع المعلمين والطلبة.

OnlineSense هو مبادرة المسؤولية الاجتماعية للشركات من مؤسسة اي سي دي ال العربية، وهي الذراع الإقليمي لمؤسسة إي سي دي ال، التي أنشئت في عام 2001 بشراكة مع اليونسكو لتعزيز محو الأمية الإلكترونية في المنطقة. وتهدف OnlineSense لبناء أساس قوي للوعي بالأمن الإلكتروني من خلال نشر أحدث التقارير والبحوث والمقالات والأخبار عن السلامة على الانترنت، وتوفير الموارد التعليمية الأساسية للمدارس من خلال بوابة OnlineSense.org.

وقد نفذت مؤسسة أي سي دي ال العربية برامج واسعة النطاق من خلال إصدار الشهادات والبرامج التوعوية التي تركز على الأمن الإلكتروني والسلامة الإلكترونية والاستخدام الفعال والآمن والمسؤول والأخلاقي لوسائل التواصل الاجتماعي. ومن بين برامج التوعية المختلفة التي أطلقتها مؤسسة أي سي دي ال العربية منذ عام 2014 جلسات تثقيفية في المدارس ومخيمات السلامة على الإنترنت.

إن سلطنة عمان نشطة جدا في مجال الأمن الإلكتروني والتوعية بالسلامة على الإنترنت. يوفر المركز العماني الوطني للسلامة المعلوماتية (OCERT) خدمات توعية ومعلومات عن أمن المجتمع للهيئات الحكومية وللمنظمات الخاصة للبقاء في أمان من الاختراقات الأمنية. ويذكر المركز العماني الوطني للسلامة المعلوماتية (OCERT) على موقعه على الإنترنت أنه يقدم دورات تدريبية وورش عمل وينشئ مناسبات على أساس منتظم لبناء ثقافة أقوى للأمن الإلكتروني[25]. وفي مطلع هذا العام، أطلقت وزارة التربية والتعليم حملة لمكافحة التسلط عبر الإنترنت بين المدارس والمجتمع؛ وأجرت حملة ترويجية في جميع أنحاء البلاد لنشر حملاتها.

شكلت حكومة المملكة العربية السعودية مؤسسة غير هادفة للربح هي المركز الوطني الإرشادي لأمن المعلومات (CERT)، بهدف زيادة الوعي والتوعية والوقاية والإدارة والتنسيق والكشف والاستجابة لحالات أمن المعلومات على المستوى الوطني. ويذكر المركز على موقعه على شبكة الإنترنت أنه يعزز الوعي بالأمن الإلكتروني من خلال البوابة، ومن خلال تنظيم الحملات والندوات. كما ينشر المركز الوطني الإرشادي لأمن المعلومات (CERT) أحدث التنبيهات الأمنية، ويدعم ضحايا الهجمات الإلكترونية من خلال تحليل الحوادث وتقديم استراتيجيات الاصلاح.

الفريق الوطني القطري للاستجابة لطوارئ الحاسب الآلي (Q-CERT) هو جهة مفوضة من قبل حكومة قطر لحماية نظم الاتصالات والمعلومات في البلاد. يعمل الفريق الوطني القطري للاستجابة لطوارئ الحاسب الآلي مع الوكالات الحكومية والشركات والمواطنين لمعالجة مخاطر الأمن الإلكتروني، وحماية المعلومات الحساسة، وضمان سلامة الأطفال على شبكة الإنترنت. وأكبر مبادرة للتوعية بالسلامة الإلكترونية في قطر هي "أبقهم آمنين، أبقهم يقظين"، فضلا عن حملات تسلط الضوء على مسؤوليات الأسرة فيما يتعلق بسلامة الأطفال على الإنترنت.

أنشأ الجهاز البحريني المركزي للمعلومات (CIO) الفريق البحريني للاستجابة لطوارئ الحاسب الآلي في البحرين للتعامل مع الوعي والدفاع عن الأمن الإلكتروني. وبالرغم من تعيين اسم النطاق cert.bh لهذا الفريق في البحرين، ولكنه غير مُفعَل. ووفقا لموقع وزارة شؤون الإعلام في البحرين، فلقد عقدت دورات توعية للجهات الحكومية وللمعلمين بشأن قواعد أمن الإنترنت العامة استضافتها الحكومة الإلكترونية، وهو برنامج تموله وزارة التربية والتعليم في البحرين. كما تقدم وزارة شؤون الإعلام في البحرين دورات تدريبية على شبكة الإنترنت لموظفي أمن تكنولوجيا المعلومات.

لا تقدم حكومة الكويت أي جلسات توعوية لموظفيها. وقد قامت وزارة التربية والتعليم التابعة لها بتنظيم دورات تثقيفية للمعلمين حول سلامة الإنترنت بشكل منفصل، ولكن وفقا لممثلي الحكومة، فإنها لم تقدم أي جلسات منذ عام 2016.

الحاجة إلى تحسين مبادرات التوعية

على الرغم من أن رفع الوعي الإلكتروني هو واحد من التقنيات الأكثر بروزا واستخداما في دول مجلس التعاون الخليجي لإشراك الجمهور، إلا أن الإستثمار فيها وفعاليةأدائها كان محدودا. وتوفر معظم الحملات التوعوية معلومات عامة ولا تبني على أو تسوق أو تنسِق مع المبادرات التوعوية الشبيهة الأخرى.

معظم دول مجلس التعاون الخليجي لا تقوم بحملات توعية حول التطرف عبر الإنترنت، وهو موضوع أكثر انتشارا في المنطقة مقارنة بالدول الأخرى. ووفقا للمرصد العالمي للتطرف العالمي للدين والجغرافيا السياسية، فقد حوالي 10000 شخص حياتهم بسبب العنف الديني المتطرف (وبسبب الجهود المبذولة لمواجهة ذلك التطرف) خلال كل ربع من العام 2016. [26]

ويتيح الموقع الإلكتروني للخدمات الحكومية في المملكة المتحدة استراتيجية لمكافحة التطرف تقدم معلومات متعمقة عن مكافحة الأيديولوجية المتطرفة وبناء مجتمعات متماسكة تعطل القيم المتطرفة وتقللها. [27]

ب) شهادات الأمن الإلكتروني

يناقش الاتحاد الدولي للاتصالات، في تقريره عن المبادرة العالمية للتصنيف العالمي، أهمية التصديق على المهنيين والوكالات في القطاع العام في إطار برامج إصدار شهادات الأمن الإلكتروني. وينبغي أن تكون الشهادات معترف بها دوليا ولها معايير عالمية.

وقد بدأت الإمارات العربية المتحدة للتو في التصديق على المهنيين الحكوميين في كل من الأمن الإلكتروني والبرامج المتعلقة بالسلامة على الإنترنت. وفي عام 2013، كشفت بلدية دبي عن موافقتها على شهادة أمن تكنولوجيا المعلومات من الرخصة الدولية لقيادة الحاسب الآلي لموظفيها. وفي عام 2012،أطلق تعاون ما بين "مركز أبوظبي للأنظمة الإلكترونية والمعلومات" ومؤسسة أي سي دي إل العربية تضمن تنفيذ شهادة أمن تكنولوجيا المعلومات من الرخصة الدولية لقيادة الحاسب الآلي استفاد منه حتى تاريخ هذا التقرير الآلاف من موظفي حكومة إمارة أبوظبي المحلية، بما في ذلك كوادر تابعة لجهاز الشرطة.[28]

الحاجة إلى التطوير في الحصول على الشهادات

بالنظر إلى أن دول مجلس التعاون الخليجي لا تزال في المرحلة الأولى من بناء إطار تدريبي لتزويد المهنيين بالأمن الإلكتروني، فهناك الكثير الذي يمكن تعلمه من بلدان أخرى. وتقوم وزارة التربية والتعليم والأبحاث في ألمانيا بتمويل مركز KASTEL للكفاءة، الذي يقدم التدريب مع شهادة تعادل درجة الماجستير في أمن تكنولوجيا الاتصالات والمعلومات [29] . من خلال مقارنة الشهادات المهنية إلى درجة أكاديمية، فإنه يضمن أن موظفي القطاع الحكومي لديهم المهارات اللازمة للنجاح في أي مكان في قطاع تكنولوجيا الاتصالات والمعلومات.

وبالإضافة إلى الحصول على شهادات معترف بها دوليا في مجال الأمن الإلكتروني، يتعين على الحكومات في دول مجلس التعاون الخليجي توفير آليات تحفيزية يمكنها إنشاء وتوسيع أسس الشبكات في القطاع الخاص. ومن شأن ذلك أن يعزز القدرة التنافسية في مجال تكنولوجيا الاتصالات المعلومات وبالتالي يحسن الاقتصاد الإلكتروني لكل بلد من بلدان مجلس التعاون الخليجي. ويمكن للمبادرات الحكومية أن توفر أيضا المزيد من فرص العمل المتعلقة بالقرصنة الأخلاقية والعديد من المجالات الأخرى في سوق الأمن الإلكتروني المزدهر.

ج) الوجود على الإنترنت

بصرف النظر عن البرامج التدريبية للمهنيين، فإنه ينبغي ان يكون لدى الحكومات مواقع إلكترونية ديناميكية لا تحدد فقط مهمة الأمن الإلكتروني وأهدافه ومبادراته ولكن أيضا أقسام أكثر أهمية مثل تنبيهات الأمن الإلكتروني والموارد المخصصة للمهنيين والجمهور.

لذلك، قامت مؤسسة أي سي دي إل العربية بمقارنة مواقع الأمن الإلكتروني في دول مجلس التعاون الخليجي. وفي سلطنة عمان، التي صنفها الاتحاد الدولي للاتصالات السلكية واللاسلكية في المرتبة الرابعة من ناحية مراتب الدول الأكثر أمانا في العالم، فهي تمتلك موقعا على شبكة الإنترنت يحتوي على أقسام مهمة. لذا فقد استخدمت مؤسسة أي سي دي ال العربية الموقع الإلكتروني لسلطنة عُمان كمعيار للمقارنة مع المواقع الإلكترونية (أو وثائق الويب في غياب المواقع الإلكترونية) لدول مجلس التعاون الخليجي الأخرى.

الدولة (الموقع يحتو علي رابط)	البحرين	الكويت	سلطنة عمان	قطر	المملكة العربية السعودية	الإمارات العربية المتحدة
الرسالة والرؤية والأهداف	✓		✓	✓	✓	✓
مبادرات التدريب	✓		✓	✓	✓	
مبادرات توعوية			✓	✓	✓	✓
الإبلاغ عن حوادث			✓	✓	✓	✓
خدمات استباقية أو تفاعلية			✓	✓	✓	✓
تقييم الثغرات مجاناً			✓	✓	✓	
قائمة بأحدث الإشعارات			✓	✓	✓	✓
أخبار وأحداث	✓		✓	✓	✓	✓
الأدب التقني حول الأمن الإلكتروني			✓	✓	✓	✓
ذكر التعاون الدولي والشراكات بين القطاعين العام والخاص	✓		✓	✓	✓	

ملاحظة: على الرغم من أن بعض البلدان لديها عدد قليل من هذه الأقسام بشكل منفصل من خلال مختلف المواقع الحكومية، فقد حصلنا على موقع واحد على اتصال وثيق مع الأمن الإلكتروني في البلد للتحقق مما إذا كان هذا الموقع لديه أقسام. والفكرة هي إبراز أهمية أن يكون لدى البلدان مستودع واحد لجميع جوانب الأمن الإلكتروني.

ملاحظات عامة

1. سلطنة عُمان، والمملكة العربية السعودية، وقطر لديها المواقع الأكثر شمولا والتي تغطي جميع الجوانب الحيوية للأمن الإلكتروني
2. الموقع الإلكتروني الخاص بدولة الإمارات العربية المتحدة لديه نطاق معتدل ليكون أكثر شمولية، في حين أن الموقع الإلكتروني للبحرين لديه نطاق واسع ليكون أكثر شمولية
3. الكويت ليس لديها موقع على شبكة الإنترنت مخصص للأمن الإلكتروني
4. يحتوي الموقع الإلكتروني للبحرين على المحتوى الأكثر إثارة للاهتمام حيث أنه يتضمن مقاطع فيديو ورسوم توضيحية ومقالات

التعاون

يتعلـق العنصـر الأخيـر المذكـور أنفـاً فـي مؤشـر الأمـن الإلكترونـي العالمـي بالشـراكة الفعالـة بيـن مؤسسـات القطاعيـن العـام والخـاص. ويتطلـب الأمـن الإلكترونـي مدخـلات مـن جميـع القطاعـات والتخصصـات، ولهـذا السـبب ينبغـي معالجـة هـذه المسـألة مـن نهـج أصحـاب المصلحـة المتعدديـن. والتعـاون لا يتطلـب الحـوار فحسـب، بـل يفضـل أن يتـم التنسـيق بيـن القطاعـات والعمـل علـى اتاحـة وضـع اسـتراتيجية أكثـر شـمولا وفعاليـة داخـل الدولـة الواحـدة. ويمكـن أن يسـاعد أيضـا فـي تحسـين تطويـر القـدرات المتصلـة بالفضـاء الإلكترونـي والسـماح بتحقيـق أفضـل فـي الجرائم الإلكترونية.

إن دول مجلـس التعـاون الخليجـي لهـا شـوط طويـل فـي التعـاون بشـكل أفضـل مـن أجـل الأمـن الإلكترونـي [30]. وفيما يلي بعض الجهود التعاونية التي يمكن أن تقوم بها حكومات دول مجلس التعاون الخليجي، عبر النطاقات الوطنية والدولية، وبين القطاعين العام والخاص.

أ) الاتفاقات متعددة الأطراف:

إن إقامـة شـراكات رسـمية مـع الـدول الأعضـاء فـي مجلـس التعـاون الخليجـي مـن شـأنه أن ييسـر التعـاون بيـن البلـدان ويسـاعد فـي الحفـاظ علـى المعاييـر المعتـرف بهـا دوليـا للمنطقـة بأسـرها. فعلـى سـبيل المثـال، تتعـاون منطقـة الشـمال الأوروبـي (الدانمـارك وفنلنـدا وآيسـلندا والنرويـج والسـويد) مـن خـلال التعـاون الوطنـي فـي بلـدان الشـمال الأوروبـي. ويشـمل ذلـك التعـاون التقنـي[31] وممارسـات الأمـن الإلكترونـي لتقييـم وتعزيـز الجاهزيـة الحاسـوبية، ودراسـة عمليـات الاسـتجابة للحـوادث، وتعزيـز تقاسـم المعلومـات بصـورة آمنـة فـي المنطقـة. وستسـتفيد دول مجلـس التعـاون الخليجـي كثيـرا مـن التعـاون فيمـا بينهـا. ولـن يقتصـر الأمـر علـى تعزيـز العلاقـات القائمـة داخـل المجتمـع فحسـب، بـل سـيعزز جهـود الاتصـال بشـأن التهديـدات الإلكترونيـة. مـع البنيـة التحتيـة المناسـبة للفـرق الوطنيـة للاسـتجابة لطـوارئ الحاسـب الآلـي، فـإن البلـدان داخـل المجلـس سـتكون قـادرة علـى الاسـتجابة للهجمـات الإلكترونيـة أسـرع مـع التقليـل مـن الأضـرار. وفـي الواقـع، أكـدت هيئـة الطـوارئ المدنيـة السـويدية " أن الحاجـة لتبـادل المعلومـات والتعـاون، والتوعيـة بالحالـة المشـتركة أثنـاء الحـوادث الإلكترونيـة يعـد أمـراً بالـغ الأهميـة ويؤثـر علـى دول الشـمال".[32]

إذا تأثـرت دولـة مـن دول مجلـس التعـاون الخليجـي بهجمـات فيروسـات الفديـة مثـل WannaCry أو NotPetya، فمـن المؤكد أنه سيكون من الأسهل تحذير الآخرين في المنطقة وتحقيق شفافية أكثر فعالية مع الجمهور.

ب) الشراكات بين القطاعين العام والخاص:

تشير الشراكات بين القطاعين العام والخاص إلى تبادل المعلومات بين القطاعين العام والخاص. وتساعد هذه الجهود على تعزيز مكافحة الاحتيال الإلكتروني، ومكافحة التصيد على الإنترنت، واختبار القدرة على صد الاختراقات الخارجية.

ومن الضروري لمعالجات البيانات الكبيرة مثل Facebook و Google العمل مع الجهات الحكومية، وخاصة وزارة الداخلية. وكجزء من التحقيقات، يطلب المسؤولون الحكوميون بيانات عن الأشخاص الذين يستخدمون خدماتهم. وتتعلق الغالبية العظمى من هذه الطلبات بالقضايا الجنائية، ولكن يمكن للسلطات أيضا أن تطلب من شركات خاصة تقييد الوصول إلى المحتوى في محاولة للقضاء على أي شيء ينتهك القوانين المحلية.[33]

شركات مثل Facebook قدمت معلومات عن عدد من الطلبات الحكومية لمعرفة البيانات ذات الصلة الخاصة بالجمهور المستخدم. وارتفعت الطلبات الحكومية للبيانات الخاصة بحسابات Facebook بنسبة 9٪ على الصعيد العالمي [34] مقارنة بالنصف الأول من عام 2016، من 59.229 إلى 64,279 طلبا. حققت الإمارات العربية المتحدة أكبر عدد من طلبات بيانات مستخدمي Facebook منذ عام 2013، تليها الكويت. أما بلدان مجلس التعاون الخليجي الأخرى فتقدم عددا أقل نسبيا من الطلبات. وقدمت جميع هذه الطلبات للتحقيق الحكومي في الجرائم (الجرائم الإلكترونية وغيرها من الجرائم).

ج) المؤسسات الدولية "غير الحكومية" (NGO's):

تظهر المؤسسات الدولية "غير الحكومية" (NGO's) كحليف مهم لحكومات الدول في مجال الأمن الإلكتروني. وتشجع هذه الهيئات البلدان على المشاركة في المشاريع الدولية والأحداث المتصلة بالإنترنت، وجمع خبراء من جميع أنحاء العالم للمساعدة في تدريب المسؤولين الحكوميين على تبادل المعلومات الحيوية.

وسعت بضعة بلدان في المنطقة إلى إقامة شراكات عالمية مع المنظمات المتخصصة في موضوع السلامة على الإنترنت. وقد انضم مركز حماية الطفل في دولة الإمارات العربية المتحدة، وهو هيئة تعمل في وزارة الداخلية، إلى فريق القوة العالمية الافتراضية (VGT) للاستفادة من الخبرات والممارسات الدولية في مكافحة الاعتداء الجنسي على الأطفال على الإنترنت. في أوائل عام 2014، تضافرت جهود مركز حماية الطفل مع مؤسسة أي سي دي ال العربية لبناء بيئة أكثر أمانا للأطفال وحمايتهم من أن يصبحوا ضحايا للإساءة عبر الإنترنت. ويهدف مركز حماية الطفل إلى تحقيق هدفه من خلال السعي إلى الامتثال لمعايير حماية الطفل المقبولة دوليا، وتعزيز الوعي من خلال برامج التوعية المجتمعية، وتقديم الخدمات القانونية.

وقد أتاح مركز حماية الطفل خطا ساخنا (111 116) يمكن الاتصال به للإبلاغ عن أية إساءة يتعرض لها الأطفال [35] المقيمون في الإمارات العربية المتحدة على الإنترنت وخارجها.

القوة العالمية الافتراضية (VGT) هي مؤسسة دولية غير حكومية تسعى إلى بناء شراكة دولية فعالة بين سلطات إنفاذ القانون والمنظمات غير الحكومية والقطاع الخاص للمساعدة في حماية الأطفال من الاعتداء على الإنترنت وغير ذلك من أشكال الاستغلال الجنسي للأطفال. انضمت دولة الإمارات العربية المتحدة إلى القوة العالمية الافتراضية (VGT) في عام 2010، وكانت عضوة منذ عام 2015 [36].

لمحة عن مؤشر الأمن الإلكتروني العالمي

على الرغم من أن مؤشر الأمن الإلكتروني العالمي التابع للاتحاد الدولي للاتصالات السلكية واللاسلكية يتطرق إلى العديد من الجوانب الهامة لاستعداد الأمن الإلكتروني، إلا أن هناك بعض المجالات التي يمكن أن يكون لها تأثير على دقة النتائج التي توصل إليها في منطقة مجلس التعاون الخليجي.

أ) التحقق من ممارسات الأمن الإلكتروني:

أشار مؤشر الأمن الإلكتروني العالمي إلى أن قطر لديها مركز للتحقيق في الجرائم الإلكترونية من أجل "حماية الجمهور والقضاء على أولئك الذين يستخدمون التكنولوجيا للقيام بأنشطة إجرامية". هناك جزء من البيان الصحفي الذي صدر في مطلع عام 2016 لمناقشة الموقع الجديد [37]، وقد كتبت معلومات قليلة جداً عن ما يفعله المركز لمنع الجرائم الإلكترونية. في الواقع، هناك القليل جدا من الأدلة على أن المركز نشط. وبعد التحدث مع ممثلي الحكومة في قطر، وجدت مؤسسة أي سي دي إل العربية أن قانون الجرائم الإلكترونية الذي تم اعتماده لم يتم تنفيذه بعد. وظل تقرير الاتحاد الدولي للاتصالات السلكية واللاسلكية يسلط الضوء على هذا الأمر باعتباره أحد الأسباب التي جعلت قطر واحدة من أفضل ثلاث دول ذات جاهزية إلكترونية في المنطقة.

ب) السلامة الإلكترونية للأطفال:

بالإضافة إلى عدم وجود قياس نوعي، فإن مناقشة قليلة جدا بشأن السلامة على الإنترنت تم دمجها في تحليلات الاتحاد الدولي للاتصالات السلكية واللاسلكية. على الرغم من أن الاستبيان يتحدث عن حماية الأطفال على الإنترنت في دعامة قانونية، فإنه لا يحدد تعريفه لحماية الطفل على الانترنت ولا يوفر أي مناقشة لكيفية قياس الاتحاد الدولي للاتصالات السلكية واللاسلكية لما يتعلق بجهود حماية الطفل على الإنترنت. ولم يذكر في أي تقرير من تقارير الاتحاد ما هي الخطوات التي اتخذتها الهيئات الحكومية لزيادة الوعي في المدارس أو داخل الأسرة.

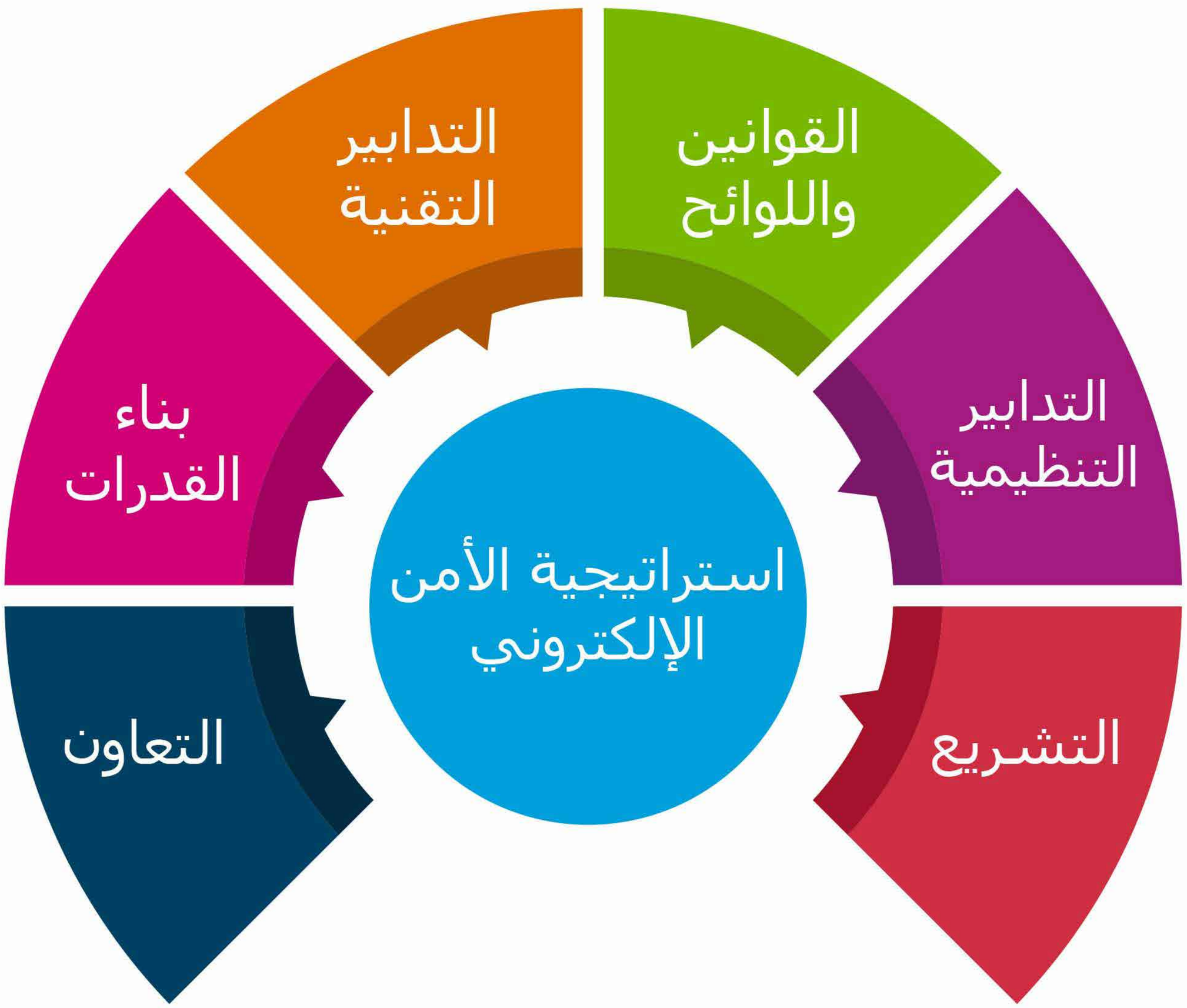
يمكن لمعظم أبحاث الجاهزية الإلكترونية أن تتعمق في الاختلافات بين الأمن الإلكتروني والسلامة على الإنترنت. ومن الناحية المؤسسية، كلاهما مهم للغاية للحفاظ على اقتصاد آمن ومزدهر. في حين يشير الأمن الإلكتروني في المقام الأول إلى حالة الحماية من الاستخدام الإجرامي أو غير المصرح به للبيانات عبر الإنترنت، فإن السلامة على الإنترنت تشير أكثر إلى كيفية استخدام تكنولوجيا الاتصالات والمعلومات بأمان ومسؤولية. وبعبارة أخرى، يتضمن الأمن الإلكتروني جوانب تقنية أكثر والسلامة على الإنترنت تحتوي على المزيد من الجوانب التعليمية والاجتماعية مثل التسلط عبر الإنترنت، والاستغلال الإلكتروني، وتطرف الأطفال عبر الإنترنت.

وقد تم تجاهل هذه المواضيع في تقرير الاتحاد الدولي للاتصالات السلكية واللاسلكية، وبالتالي أثرت على التصنيف العام للبلدان وترتيبها داخل المنطقة. هناك العديد من الطرق التي يجب على الحكومات أن تدرج فيها السلامة الإلكترونية في تقرير الاستعداد للأمن الإلكتروني. فعلى سبيل المثال، يمكن أن تسأل وزارات التربية والتعليم في قسم بناء القدرات في تقارير الاتحاد المقبلة عما إذا كانت توفر حملات للتوعية العامة بشأن السلامة على الإنترنت. ويمكن للاتحاد أيضا أن يحقق فيما إذا كانت البلدان توفر التدريب الإلزامي، وحلقات العمل،والجلسات التثقيفية، والدورات، و/أو شهادات للمعلمين بشأن السلامة على الإنترنت.

يمكن للمرء أن يكون قادرا على ترتيب البلدان على أساس مدى أمن النظم، ولكن لا يمكن للمرء أن يحدد حقا كيف يقوم الإنترنت بتجهيز الحكومة أو المجتمع دون إدراج أي توعية بالسلامة الإلكترونية. تم التواصل مع الاتحاد الدولي للاتصالات من قبل مؤسسة أي سي دي ال العربية عدة مرات للرد على الأسئلة التي أثارها مؤشر الأمن الإلكتروني العالمي لعامي 2014 و 2017، ومعرفة المزيد عن النتائج التي توصلوا إليها في التقرير والمعايير المستخدمة لترتيب استعداد الدول العربية، ولكن للأسف لم تتلق مؤسسة أي سي دي ال العربية أي رد حتى وقت نشر هذا التقرير.

التوصيات

يقر هذا التقرير بأن بلدان منطقة مجلس التعاون الخليجي بدأت في اعتبار الأمن الإلكتروني جزءا هاما من الأمن القومي والاقتصاد الإلكتروني. ومع ذلك، **لا يزال هناك تفاوت كبير بين دول مجلس التعاون الخليجي فيما يتعلق باستعدادات الأمن الإلكتروني. على الرغم من أن سلطنة عُمان تحتل المرتبة الرابعة بين أفضل خمس دول في العالم في مجال الأمن الإلكتروني، فإن الكويت هي تقريبا في أسفل القائمة، في المركز 139.** ويكشف هذا التفاوت عن الحاجة الملحة لدول مجلس التعاون الخليجي إلى تبني نهج تعاوني جوهري لتطوير أساس متين للأمن الإلكتروني.



وفيما يلي ملخص للتدابير الفورية التي يوصي هذا التقرير البلدان في البدء بها:

- إعطاء الأولوية للتعاون وتبادل المعرفة على مستوى دول مجلس التعاون الخليجي لوضع استراتيجيات مفصلة للأمن الإلكتروني، ومحاكاة نماذج متطورة مثل استراتيجية الأمن الإلكتروني في المملكة المتحدة، [38] والتعلم من النهج الذي اعتمدته الأمثلة الإقليمية مثل استراتيجية دبي للأمن الإلكتروني. [39]

- تثقيف المحامين حول أحدث التهديدات الإلكترونية، وبناء قانون شامل ضد الاحتيال والانتهاكات على الانترنت. إن اتباع معيار خاص مثل قانون الأمن الإلكتروني الأمريكي [40] ضروري للتعامل مع أحدث الجرائم الإلكترونية.

- إنشاء مختبر للأمن الإلكتروني لمتابعة أحدث التهديدات واستنباط طرق لمعالجتها.

- إنشاء مراكز حكومية للتدريب على الأمن الإلكتروني للموظفين في القطاعين العام والخاص والعاملين على البنية التحتية الحيوية التي تحتاج إلى الحماية. ومن الأمثلة الجيدة على ذلك مبادرات التدريب التي نفذت في مدينة ويلز [41] في المملكة المتحدة.

- إبرام اتفاقات مع البلدان التي تنشأ فيها أغلبية الجرائم الإلكترونية من أجل مقاضاة المجرمين فعلياً من تلك الأماكن. البدء من خلال التعاون مع المنظمات الدولية للأمن الإلكتروني. [42]

- جعل مواقع الإنترنت الحكومية الخاصة بالأمن الإلكتروني أكثر شمولا، مع التحديثات والتنبيهات والموارد وخدمات الأمن، وبرامج التدريب.

وفي ختام هذا التقرير، من المهم النظر فيما يلي:

الجاهزية الإلكترونية أكثر شمولاً من الأمن الإلكتروني

أصبح مصطلح الجاهزية الإلكترونية مرادفا تقريبا لاستعدادات الأمن الإلكتروني، ولكن من المهم التمييز بين الاثنين. إن الاستعداد الإلكتروني له نطاق أوسع بكثير من مجرد الأمن الإلكتروني. فإنه يشير إلى كل الأمور الضرورية لأي بلد حتى يكون جاهزا لعالم الإنترنت. وتشمل هذه الجاهزية في كامل مجالها على البنية التحتية الإلكترونية، ومهارات تكنولوجيا الاتصالات والمعلومات، وانتشار الإنترنت، والتوعية، والأمن الأساسي للبلدان للاستفادة من الفضاء الإلكتروني للتنمية.

الشفافية هي العنصر السادس المخفي من الجاهزية للأمن الإلكتروني

في الفضاء الإلكتروني يمكن أن يحدث خرق أمني في أي مكان، ومشاركة الجمهور يعد أمرا بالغ الأهمية لتحديد الهجمات الإلكترونية واحتواءها في المرحلة الأولى. ولن يشارك الجمهور إلا إذا عززت الحكومة الثقة من خلال الشفافية والحوار. وفي ما يلي بعض الأمثلة على ما ينبغي أن تتقاسمه الحكومات مع الجمهور لبناء بيئة شفافة:

- التدابير التي اتخذتها الحكومة لحماية خصوصية الأشخاص والحريات المدنية في الفضاء الإلكتروني
- الإعلان عن الهجمات الإلكترونية على الشبكات الحكومية / الخاصة والمعلومات الحساسة التي قد تؤثر على مصالح الجمهور
- نهج الحكومة وقدراتها ومبادراتها لتحديد الهجمات الإلكترونية ومكافحتها

مزيد من احتياجات الجاهزية الإلكترونية البحثية التي يتعين القيام بها وجمعها (محليا)

كشفت تفاعلات مؤسسة أي سي دي إل العربية مع ممثلي حكومات دول مجلس التعاون الخليجي أنه ليس لدى دول المجلس بيانات كافية لتحديد جاهزية الأمن الإلكتروني. في حين أبرزت الدراسات التي أجرتها مختبرات كاسبيرسكي [43] والاتحاد الدولي للاتصالات [44] عدم وجود الاستعداد والوعي في مجال الأمن الإلكتروني في دول مجلس التعاون الخليجي.

كمـا لـم تعثـر مؤسسـة أي سـي دي إل العربيـة علـى أي تقريـر حـول الاسـتعداد للأمـن الإلكتروني تم نشره من قبل أي حكومة من حكومات دول المجلس، وهذا يشير إلى احتمال عدم وجود بحـوث تقودهـا الحكومـة بشـأن هـذا الموضـوع الملحـوظ. إن تقييـم التأهـب للأمـن الإلكترونـي هـو الخطـوة الأولـى نحـو اتخـاذ تدابيـر لتصبـح أكثـر أمنـا. لذلـك، ينبغـي علـى بلـدان مجلـس التعـاون الخليجـي إجـراء بحـوث مدعومـة مـن قبـل الدولـة لمعرفـة المزيـد عـن التهديـدات الأخيـرة، والقـدرات للتصـدي لتلـك التهديدات.

لا شـك أن الأمـن الإلكترونـي ضـروري لمسـتقبل الدولـة الإلكترونيـة وأمنهـا القومـي. ويعتمـد نجـاح أو فشـل جاهزيـة الأمـن الإلكترونـي فـي بلـد مـا بشـكل حاسـم علـى المشـاركة المباشـرة المسـتمرة للحكومـة بدعمهـا عبـر التمويـل المناسـب والسياسـات وبرامـج التوعيـة. وفـي الوقـت الـذي تسـعى فيـه حكومـات دول مجلـس التعـاون الخليجـي إلـى تنويـع اقتصاداتهـا، فإنهـا سـتحتاج إلـى تعزيـز حصـول المواطنيـن علـى تكنولوجيـا الاتصـالات والمعلومـات. كمـا يجـب عليهـا أن تلتـزم بزيـادة سـلامة ومرونـة البنيـة التحتيـة للإنترنـت مـن جميـع أنـواع المخاطـر، بمـا فـي ذلـك اختراقـات البيانـات، والأنشـطة الإجراميـة، وانقطـاع الخدمـة، وتدميـر الممتلـكات. وبـكل بسـاطة، فكلمـا زادت الثقـة التـي يضعهـا المواطنـون عنـد التعامـل عبـر الإنترنـت، كلمـا كانـت العوائد أعلى بالنسبة للدولة ككل.

المراجع

1. http://www3.weforum.org/docs/WEF_IT_DynamicEcosystem_Report_2009.pdf
2. http://www.arabianbusiness.com/arab-internet-users-forecast-rise-226m-by-2018--626635.html
3. http://www.itp.net/mobile/612536-in-the-uae,-one-in-136-emails-is-malicious-research
4. https://www.wired.com/story/2017-biggest-hacks-so-far/
5. https://www.hiscox.co.uk/cyber-readiness-report/docs/cyber-readiness-report-2017.pdf
6. https://www.hiscox.co.uk/cyber-readiness-report/docs/cyber-readiness-report-2017.pdf
7. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CyberReadiness_EN.pdf
8. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CyberReadiness_EN.pdf
9. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01--2017-PDF-E.pdf
10. http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx
11. https://www.chathamhouse.org/sites/files/chathamhouse/publications/research/2017-06-30-cybercrime-digital-economy-gcc-hakmeh.pdf
12. http://www.bna.bh/portal/en/news/762914
13. https://www.tra.gov.ae/en/media-hub/press-releases/2017.1.15/tra-hosts-the-first-introductory-workshop-of-the-uae-information-security-awareness-committee-isa.aspx
14. http://marinafox.com/news/training_for_lawyers_on_cyber_law
15. https://www.theknowledgeacademy.com/sa/courses/cyber-security-training/cyber-security-awareness/riyadh/
16. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf
17. http://saudigazette.com.sa/article/152682/?page=1
18. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf
19. http://www.dubai.ae/en/Pages/DCSS.aspx
20. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017PDF-E.pdf
21. https://www.accenture.com/t20170406T010037__w__/sg-en/_acnmedia/PDF-38/Accenture-Facing-Cybersecurity-Conundrum-Singapore.pdf
22. http://www.itworldcanada.com/article/breaking-news-ottawa-announces-public-consultation-on-cyber-security-strategy/385740#ixzz4dm1QjsTu
23. https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessent-netherlands-2016.html
24. http://www.aqdar-uae.com/en/about/
25. http://www.cert.gov.om/services.aspx
26. http://www.religionandgeopolitics.or/global-security/extremism-and-conflict-what-watch-2017
27. http://www.gov.uk/government/publications/counter-extremism-strategy
28. https://icdlarabia.org/uploads/news/english/2012/Sep/ADSIC_Security_Eng.pdf
29. http://www.kastel.kit.edu/
30. https://www.thenational.ae/business/technology/gcc-urged-to-coordinate-cyber-security-following-wannacry-attack-1.90087
31. http://www.msb.se/en/Tools/News/Nordic-cyber-security-exercise-was-conducted-in-Linkoping/
32. http://www.msb.se/en/Tools/News/Nordic-cyber-security-exercise-was-conducted-in-Linkoping/
33. https://govtrequests.facebook.com/about/
34. https://newsroom.fb.com/news/201704//global-government-requests-report-7/
35. https://icdlarabia.org/uploads/news/english/2015/UAE_Welcomes_ICDL_Arabic_to_Virtual_Global_Taskforce. df
36. https://www.moi.gov.ae/en/media.center/News/News4k20151111.aspx
37. https://www.moi.gov.qa/site/english/news/2016/01/-24/-35540.html
38. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf
39. http://www.dubai.ae/en/Pages/DCSS.aspx
40. https://fas.org/sgp/crs/natsec/R42114.pdf
41. http://www.computerweekly.com/feature/How-Wales-has-evolved-into-a-hotspot-for-cyber-security
42. https://www.thebalance.com/leading-information-security-organizations-2071545
43. https://me-en.kaspersky.com/about/press-releases/2017_kaspersky-labs-latest-parental-control-report-shows-uae-kids-online-behavior
44. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf