مركز دراسات الخليج والجزيرة العربية
تأسس عام ١٩٩٤م. جامعة الكويت

تحديات الأمن السيبراني وتأثيراته على مؤسسات وهيئات دول مجلس التعاون لدول الخليج العربية

د. صفاء عبدالخالق زمان
أ. آمنة عبدالله عيادة

التقرير الاستراتيجي
العدد (٣٦)

الكويت. ٢٠٢٤م

مركز دراسات الخليج والجزيرة العربية
تأسس عام ١٩٩٤م. جامعة الكويت

تحديات الأمن السيبراني وتأثيراته على مؤسسات وهيئات دول مجلس التعاون لدول الخليج العربية

إعداد

د. صفاء عبدالخالق زمان

عضو الهيئة الأكاديمية ـ جامعة الكويت
رئيس الجمعية الكويتية لأمن المعلومات

أ. آمنة عبدالله عيادة

مركز دراسات الخليج والجزيرة العربية

التقرير الاستراتيجي

العدد (٣٦)

الكويت ـ ٢٠٢٤م

أُسس **مركز دراسات الخليج والجزيرة العربية بجامعة الكويت** في عام ١٩٩٤م، بوصفه مركزاً بحثياً يهتم بالبحوث والدراسات العلمية ذات الصلة بالقضايا التي تهم دولة الكويت ومنطقة الخليج والجزيرة العربية على وجه التحديد، ومنطقة الشرق الأوسط والقضايا الدولية عموماً.

ومن هذا المنطلق يقوم المركز بشكل دوري بإصدار «**التقرير الاستراتيجي**» الذي يتناول القضايا الاستراتيجية التي تهم دولة الكويت والمنطقة. ويهدف المركز من خلال هذا التقرير إلى تقديم تحليل استراتيجي للقضايا والمستجدات المتعلقة بأمن المنطقة، ما يمكن أن يساهم في خدمة الباحثين والمهتمين في الشؤون الاستراتيجية. كما يسعى المركز من خلال هذا التقرير إلى تقديم الرؤى والتوصيات اللازمة لصناع القرار السياسي بما يخدم تحقيق المصلحة الاستراتيجية لدولة الكويت.

أعضاء مجلس إدارة
مركز دراسات الخليج والجزيرة العربية

أ. د. عثمان حمود الخضر
القائم بأعمال نائب مدير جامعة الكويت للأبحاث (رئيس مجلس الإدارة)

أ. د. يعقوب يوسف الكندري
القائم بأعمال مدير المركز ـ نائب رئيس مجلس الإدارة

داخل جامعة الكويت

أ. د. عبدالله عقله الهاشم
قسم المناهج وطرق التدريس
كلية التربية ـ جامعة الكويت

أ. د. عبيد سرور العتيبي
القائم بأعمال رئيس قسم الجغرافيا
كلية العلوم الاجتماعية ـ جامعة الكويت

أ. د. غانم حمد النجار
قسم العلوم السياسية
كلية العلوم الاجتماعية ـ جامعة الكويت

أ. د. فايز منشر الظفيري
قسم المناهج وطرق التدريس
كلية التربية ـ جامعة الكويت

خارج جامعة الكويت

د. بدر عثمان مال الله
المدير العام للمعهد العربي للتخطيط السابق
دولة الكويت

سعادة السفير / سميح عيسى جوهر حيات
مساعد وزير الخارجية لشؤون آسيا
وزارة الخارجية ـ دولة الكويت

سعادة السفير / عبد العزيز الشارخ
المدير العام السابق لمعهد سعود الناصر الدبلوماسي الكويتي ـ دولة الكويت

د. ناصر جاسم الصانع
الهيئة العامة للتعليم التطبيقي والتدريب
دولة الكويت

الناشر

مركز دراسات الخليج والجزيرة العربية

جامعة الكويت

ص.ب: ٦٤٩٨٦ الشويخ (ب)

الرمز البريدي: ٧٠٤٦٠، الكويت

هاتف : ٢٤٩٨٤٦٣٩ ـ ٢٤٩٨٤٦٥٨ (٩٦٥+)

البريد الإلكتروني **cgaps@ku.edu.kw**

الموقع الإلكتروني **www.cgaps.ku.edu.kw**

الآراء الواردة في هذه الدراسة لا تعبّر بالضرورة عن اتجاهات يتبناها مركز دراسات الخليج والجزيرة العربية بجامعة الكويت

الطبعة الأولى . الكويت ـ ٢٠٢٤م

تمهيد:

يعد الأمن السيبراني مجالاً من أهم المجالات في العصر الحالي، حيث إنه يقوم على ممارسات الدفاعات الإلكترونية، وبناء هياكل دفاعية تقوم على صد الهجمات الإلكترونية، وهو الحماية الشاملة للأنظمة الإلكترونية والشبكات والبيانات والبرمجيات والأجهزة الإلكترونية من الهجمات الإلكترونية والاختراقات السيبرانية والتهديدات الأمنية الأخرى.

كما أنه يهدف إلى الحفاظ على سرية وسلامة وتوافر المعلومات والبيانات الحيوية والحسَّاسة في الأنظمة الإلكترونية، والتأكد من عدم تعرّضها للسرقة أو التغيير أو الاستخدام غير المصرّح به.

لذلك يتطلّب الأمن السيبراني تنفيذ استراتيجيات شاملة ومنهجية للحماية من التهديدات السيبرانية، حيث يجب أن تكون موجَّهة نحو تحقيق أهداف محدَّدة للأمن السيبراني في وزارات ومؤسسات وهيئات الدول الخليجية.

كما يشمل ذلك تقييم الأخطار الأمنية، وتطوير خطط الاستجابة للأزمات السيبرانية، وتحديث التقنيات الأمنية بشكل دوري، وتطوير قدرات الحماية والردع والتعافي من الهجمات السيبرانية.

وبما أن الأمن السيبراني يتعلَّق بالحماية من التهديدات الإلكترونية، فإنه يعتبر مجالاً متطوراً ومتغيراً باستمرار، ويتطلّب متابعة دائمة للتطورات التقنية والتهديدات الأمنية الجديدة، وتحديث الإجراءات والأدوات الأمنية بشكل دوري لتلبية التحديات الجديدة.

كما أن تحقيق الأمن السيبراني يتطلّب التعاون بين الجهات المختلفة بما في ذلك الوزارات والمؤسسات والهيئات الحكومية منها والخاصة للدول الخليجية، وتوجيه الجهود الجماعية الدولية نحو تحقيق الأهداف الأمنية المشتركة.

في ضوء ذلك، فقد خصَّص مركز دراسات الخليج والجزيرة العربية هذا التقرير الاستراتيجي لعرض أبرز التهديدات السيبرانية التي تواجه منطقة الخليج العربي، وأهم إنجازات الهيئات الخليجية في مجال الأمن السيبراني، مدعوماً بدور الأمانة العامة لمجلس التعاون الخليجي؛ لخلق منظومة التعاون في مجال الأمن السيبراني، ومعززاً بمؤشرات نضوج جاهزية الأمن السيبراني لدول مجلس التعاون الخليجي، وصولاً إلى التوصيات نحو التكامل الخليجي في منظومة الأمن السيبراني سواء على مستوي الدولة أو على مستوى دول مجلس التعاون.

إدارة المركز

مركز دراسات الخليج والجزيرة العربية

المحتويات	رقم الصفحة

المحتويات	رقم الصفحة

مركز دراسات الخليج والجزيرة العربية

ملخص:

يعتبر الأمن السيبراني من الموضوعات المهمة والحيوية في العالم وبالأخص في منطقة الخليج العربي، لما تتميّز به هذه المنطقة من خصائص قد جعلتها في صدارة الدول المستهدفة للاختراقات والهجمات الإلكترونية؛ حيث تتمتع منطقة الخليج بثروات اقتصادية نفطية، كما تعتبر موطناً للشركات والمؤسسات العالمية، بالإضافة إلى التطور الكبير والازدهار الذي تشهده المنطقة مؤخراً، فضلاً عن تطور البنيات التحتية للمعلوماتية والاتصالات وانفتاحها على العالم الرقمي بأبعاد مختلفة، واعتمادها على التقنية والفضاء الإلكتروني.

وتتركّز هذه الدراسة على تسليط الضوء على أبرز التهديدات والهجمات السيبرانية التي تواجه منطقة الخليج العربي، وأهم الخسائر التي ترتبت عليها هذه الهجمات، حيث تعتبر منطقة الخليج العربي بيئة خصبة للهجمات الإلكترونية بجميع أنواعها؛ ولهذه الأسباب، من المهم الاجتهاد في تحسين البنية الأمنية لدول مجلس التعاون الخليجي، والذي سيكون موضوع الفصل الثاني لهذه الدراسة من خلال سرد أهم إنجازات الهيئات والمؤسسات الخليجية في مجال الأمن السيبراني؛ كذلك ستتطرق الدراسة إلى

دور الأمانة العامة لمجلس التعاون الخليجي لخلق منظومة التعاون في مجال الأمن السيبراني في الفصل الذي يليه.

وبما أن أبعاد التكنولوجيا تتطور باستمرار؛ فسوف يتناول الفصل الرابع من هذه الدراسة مستقبل المنظومة الأمنية لدول المنطقة الخليجية في ظل الطفرات المتتابعة للتقنية، وما أهم الاستعدادات والمتطلبات التي يجب اتخاذها.

وختاماً، ذكر أهم المقترحات والتوصيات نحو التكامل الخليجي في منظومة الأمن السيبراني، والطموحات التي نأمل في تحقيقها من أجل منظومة خليجية متطورة وآمنة.

مقدمة :

بسبب تضخم التقنيات الرقمية واقتحام تقنيات الذكاء الاصطناعي وثورة تضخم البيانات وبرمجة الروبوتات وغيرها من طفرات التقنية التي قد فاقت القدرات البشرية الاعتيادية؛ إلى جانب الإمكانيات الفائقة لهذه التقنيات، إذ تعد تقنية الحوسبة الكمية على سبيل المثال لا الحصر (نموذجاً حاسبياً نظرياً يتم من خلاله معالجة البيانات وعمليات الحوسبة من خلال قوانين "الكم") من التقنيات التي تفوق سرعتها ١٠٠ مليون مرة من أجهزة الحاسوب الحالية، حيث توفر قوة حوسبة عالية جداً وخطيرة إذا استخدمت في عمليات الاختراق، حيث إنها تمكّن القراصنة من الاختراق بطرق أسرع، وبالتالي يصعب ملاحظتها وملاحقتها، وهذا قد يغيّر ديناميكية الفضاء السيبراني إلى حد كبير، الأمر الذي يتطلّب تقييم مجالات للإستراتيجيات السيبرانية الوطنية للعديد من الدول، بالإضافة إلى أن اعتماد الشعوب على التقنيات أصبح أكثر تشعباً، كما أن انخراط تلك التقنيات في مجتمعاتنا أصبح أكبر عُمقاً، حيث تواجه الحكومات تحديًا كبيراً لاحتواء تلك التقنية من ناحية، ومن ناحية أخرى معضلة حماية شعوبها والحد من استنزاف البيانات وحماية الخصوصية، وبسبب الطفرات التكنولوجية السريعة وظهور الأفكار المبتكرة وتغيير التقنيات باستمرار الأمر الذي

يجعل العالم الافتراضي متغيراً ومتقلّباً بصورة سريعة وغير متزن، وهذا ما يجعل صياغة الإستراتيجيات السيبرانية للدول تعتبر تحدياً كبيراً لأسباب كثيرة أهمها ما يلي:

١ ـ الافتقار إلى رؤية واضحة للشؤون الإلكترونية والأنظمة الرقمية المستخدمة على المستوى الوطني، بحيث لا تمتلك معظم الدول النامية سياسات وطنية واضحة ومتماسكة فيما يتعلق بفضائها الإلكتروني.

ـ الاعتماد الكبير على الأجهزة والبرامج المستوردة دون فهم تفاصيل تلك البرمجيات والخوارزميات وتأثيراتها المختلفة على الخصوصية والبيانات، إذ تعتمد العديد من الدول على استيراد التقنيات والتكنولوجيات الحاسوبية من دول متقدّمة دون إدراك طبيعة وطريقة عملها بالرغم من أنه يتم استخدامها في قطاعاتها الحيوية مثل: الدفاع والمؤسسات الأمنية والمؤسسات المالية الاقتصادية والحكومية، وبالتالي فإن هذه التبعية تشكّل تهديداً خطيراً لأمن الدولة القومي.

٢ ـ مع ظهور تقنيات الخدمات السحابية والتي ساهمت في زيادة التبعية بصورة واضحة من خلال تخزين بيانات وأنظمة بعض الدول المستخدمة لهذه التقنيات والخدمات السحابية في سيرفرات وكيانات الدول المنتجة والمصدّرة لها، وهذا يعتبر استيلاءً غير مباشر على مقدّرات الدول المستخدمة للتقنيات والخدمات السحابية.

ـ تخصيص ميزانية غير كافية للعمليات السيبرانية نتيجة إحجام بعض الحكومات عن عدم منح الأموال الكافية للمنظمات والهيئات والمؤسسات

ذات الصلة بالقضايا السيبرانية، وذلك بسبب عدم فهم، أو ربما عدم وجود إدراك كافٍ لجدية وأهمية هذا المجال على المستوى الوطني الحيوي، ودور الأمن السيبراني في عملية حماية الأنظمة والشبكات والبرامج ضد الهجمات الرقمية، في ظل بزوغ مشهد رقمي يعزِّز التعاون المتواصل لرصد الأخطار الجديدة.

٣ ـ عدم وجود هيكل وطني مناسب للتعامل مع الصراعات السيبرانية لدى بعض الدول، وافتقارها إلى وجود استراتيجيات لإدارة الأخطار، أو جيوش دفاعية رقمية تحمي مقدَّرات الدولة؛ فبعض الدول ليس لديها أي هيئة أو مركز وطني متخصص ومتكامل يمكن أن يدير ويشرف على القضايا السيبرانية ويستجيب لأمن الفضاء الإلكتروني ويعزِّز أمن المعلومات بأشكالها كافة، ناهيكم عن غياب ثقافة الأمن السيبراني المستمرة داخل الهيئات الحكومية البيروقراطية المترهّلة في بعض دول العالم الثالث، إذ لا تمتلك معظم تلك الدول النامية سياسة ناظمة لرصد التهديدات على بنيتها التحتية الحيوية، مثل: البنوك وشبكات الاتصالات السلكية واللاسلكية ومعاملاتها المالية وقطاعاتها الحيوية المختلفة.

٤ ـ عدم وجود نظام موثوق وقوي لضمان أمن الدولة وفضائها السيبراني، وهذا ما يجعل بعض حكومات الدول النامية مترددة في بدء أي تغيير جذري في السياسة الحالية والجهاز الحكومي، ومما يعزّز هذا التوجّه وجود صعوبة في تبنّي التقنيات المتغيّرة بسرعة في الوقت المناسب، والافتقار إلى مبادرات البحث والتطوير للمنتجات الرقمية المحلية، مع غياب مراكز

البحث والدراسات والتطوير في كثير من دولنا المصنَّفة من العالم الثالث دون وجود استفادة من الخبرات المتاحة.

وبسبب الهجمات السيبرانية المتعاقبة والمستمرة على الدول الخليجية مؤخراً والتي قد تهدد اقتصادياتها واستقرارها؛ حيث ترتبط تلك الهجمات الإلكترونية بأهداف سياسية، أو القيام بأعمال تخريبية، أو التجسس وضرب الأمن القومي للدول، أو تحقيق فوائد مالية، وتعد دول مجلس التعاون الخليجي بين أبرز مناطق العالم التي زاد استهدافها من قِبل الهجمات السيبرانية سواء بدافع الاحتيال وجني المال، أو بدافع أيديولوجي لتبرير الأضرار المتعمدة، أو بمبرر سياسي قصد التخريب، لما لمنطقة الخليج العربي من مميزات تجعلها عُرضة لتلك التهديدات والهجمات السيبرانية، وأهمها ما تملكه من ثروات اقتصادية ونفطية كبيرة، الأمر الذي يجعلها مطمعاً للكثيرين، إلى جانب أنها تعتبر مركزاً رائجاً للعديد من الشركات والمؤسسات العالمية.

من جانب آخر، تعد زيادة أهمية منطقة الخليج العالمية وانفتاح ازدهار مؤسساتها وأفرادها على استخدام الفضاء الإلكتروني أكبر دافع للمخرّبين والمجرمين لتبرير هجماتهم؛ بالإضافة إلى أن سكان منطقة الخليج العربي يعتبرون الأكثر اتصالاً بالإنترنت مقارنة بشعوب العالم الثالث، وفي الوقت ذاته، عدم وعيهم الكافي للتعامل مع التقنيات الحديثة والعوالم المفتوحة، الأمر الذي أدى أيضاً إلى ارتفاع عدد التهديدات والهجمات السيبرانية على المنطقة الخليجية.

لذا اجتهدت الحكومات في دول الخليج العربي للحد من تلك الهجمات السيبرانية، ومحاولات الاختراق المتكررة من خلال جهود حفيفة كان هدفها بناء سور رقمي يصد تلك الهجمات، أو يحدّها عبر دعم مراكز الأمن السيبراني؛ فقد نجحت الإمارات العربية المتحدة في منع حدوث أكثر من ٨٧ ألف هجمة إلكترونية، خلال الربع الأول من عام ٢٠٢٠، التي تنوّعت ما بين "خبيثة"، و"ثغرات أمنية"، و"محاولات احتيال ونصب".

من جانبها، استحدثت سلطنة عُمان، في ١٠ يونيو ٢٠٢٠، مركزاً للدفاع الإلكتروني يستهدف المعاملات الإلكترونية ومكافحة جرائم تقنية المعلومات، ويتماشى المركز الأمني الجديد مع تصنيف السلطنة بالمركز الثاني عربياً والـ١٦ عالمياً في مؤشر الأمن السيبراني العالمي لعام ٢٠١٨-٢٠١٩، الصادر عن الاتحاد الدولي للاتصالات، وشمل ١٧٥ دولة، كما حصلت السلطنة على جائزة القمة العالمية لمجتمع المعلومات والتي تحتضنها مدينة جنيف السويسرية، ويأتي هذا الدور الريادي لسلطنة عُمان تقديراً لجهودها المميزة والكبيرة في مجال الأمن السيبراني، وإدراكها بأهميته في ظل التطورات المتلاحقة للتكنولوجيا، وضرورة التعامل مع الأخطار والتهديدات الأمنية الإلكترونية ومع الجرائم الإلكترونية ليس على المستوى الوطني فحسب، بل على المستويات الإقليمية والدولية.

أما المملكة العربية السعودية، فإنها كانت من أكثر دول الخليج عُرضة للهجمات الإلكترونية الخبيثة عام ٢٠١٩، وفق تقرير لشركة «ترينـد مايكرو» العالمية المتخصصة بأمن المعلومات، ففي ٣١ مارس ٢٠٢٠ تعرّضت المملكة

لمليونين و٣٥٢ ألفاً و٥٧٠ هجمة إلكترونية خبيثة على مؤسساتها؛ وهذا الذي ألزمها الاهتمام جداً بهذا المجال، حيث أبدت المملكة في ذلك دوراً بارزاً من خلال إطلاق ٥ مراكز متخصصة، هم: مركز المعلومات الوطني، ومركز التصديق الرقمي، والمركز الوطني الإرشادي للأمن السيبراني، ومركز التميّز لأمن المعلومات، والمركز الوطني للأمن الإلكتروني؛ الأمر الذي جعلها تخطو بخطوات كبيرة في مجال تحسين البنية التحتية الرقمية، وتحقيق الريادة في مجال الأمن السيبراني، فقد حصدت المركز الثاني عالمياً لسنة ٢٠٢٠ في مؤشر الأمن السيبراني (GCI) من بين ١٧٥ دولة.

بدورها عملت دولة قطر بشكل مكثّف أيضاً في السنوات الأخيرة على تعزيز وتطوير جهودها في مجال الأمن السيبراني ومكافحة القرصنة؛ حيث وقَّعت اتفاقيات عدة تصبّ في تأمين هذا القطاع وتطوير القدرات الوطنية للارتقاء بأنظمته وإمكاناته التكنولوجية؛ إلى جانب إطلاق وكالة تُسمَّى «الوكالة الوطنية للأمن السيبراني» بقرار أميري رقم (١) لسنة ٢٠٢١ وتتبع رئيس مجلس الوزراء، كبادرة على جدّية اهتمام الدولة وأولوياتها لقيام دولة تواكب تطورات وطفرات التكنولوجيا العالمية.

أما مملكة البحرين، فقد حرصت على جعل الأمن السيبراني وحماية أنظمتها الرقمية من أولوياتها من خلال إطلاق إدارات متنوّعة أهمها هيئة المعلومات والحكومة الإلكترونية، وهيئة تنظيم الاتصالات، وهيئة حماية البيانات الشخصية، وغيرها من القطاعات المهمة؛ إلى جانب أنها حرصت على إطلاق الاستراتيجية الوطنية للأمن السيبراني، وتشريعات

الجرائم الإلكترونية، واستخدام آليات وبرامج متطورة للحد من الهجمات الإلكترونية المستمرة.

من جانب آخر، تعرَّضت دولة الكويت مؤخراً لهجمات إلكترونية كثيرة استهدفت مؤسساتها الحيوية والمهمة الأمر الذي ألزمها بالعمل الدؤوب للحد من تلك الهجمات من خلال إطلاق المركز الوطني للأمن السيبراني بتاريخ ٥ فبراير ٢٠٢٢، والذي يهدف إلى بناء منظومة فعَّالة للأمن السيبراني على المستوى الوطني وتطويرها وتنظيمها لحماية الدولة من تهديدات الفضاء السيبراني ومواجهتها بكفاءة وفاعلية بما يضمن استدامة العمل والحفاظ على الأمن السيبراني الوطني، إلى جانب حرص دولة الكويت على توقيع اتفاقيات دولية تهدف إلى تأمين هذه القطاعات المختلفة لديها، وتطوير القدرات الوطنية في مجال الأمن السيبراني.

إن الفضاء السيبراني سلاح ذو حدين لما يتضمنه من إيجابيات من جهة، ومن تحديات وتهديدات من جهة أخرى، ولا سيما أن الهجمات والجرائم السيبرانية أصبحت معقّدة ومتسارعة وخطيرة، ويصعب على الكثير من المؤسسات التغلّب والدفاع عن أمنها السيبراني دون وجود إستراتيجيات عمل وطنية واقتناء تقنيات وتطبيقات متطورة، إلى جانب وجود توعية وممارسات سليمة تأخذ بعين الاعتبار كل الاحتمالات للوقاية من أخطار وتهديدات هذا الفضاء العالمي المتسع الذي أصبح دون شك ميدان الحرب الجديدة بين أطراف القوى العالمية العظمى، لذا أصبح من المهم الاهتمام بهذا المجال وجعله من أولويات الدولة باعتباره أنه أصبح الركيزة الأساسية التي تقوم عليها الدولة ومؤسساتها.

وتهدف هذه الدراسة إلى إبراز أهم تحديات الأمن السيبراني وتأثيراته على مؤسسات وهيئات الدول الخليجية، من خلال التركيز على خمسة فصول رئيسة؛ الفصل الأول يركّز على أهم التهديدات والهجمات السيبرانية التي تواجه منطقة الخليج العربي، وأحدث الاختراقات التي تعرَّضت لها مؤخراً، وأهم الخسائر التي ترتبت على هذه الهجمات، بعدها يعرض أهم التجارب الناجحة لدول مجلس التعاون الخليجي، سعياً لمحاربة الهجمات الإلكترونية والحد منها، وهذا ما تناوله الفصل الثاني من الدراسة من خلال ذكر أهم إنجازات الهيئات والمؤسسات الخليجية في مجال الأمن السيبراني.

أما الفصل الثالث فقد سلّط الضوء على جهود الأمانة العامة لمجلس التعاون الخليجي الساعية لتحقيق بنية موحّدة آمنة لدول مجلس التعاون الخليجي وحماية مقدّراته، بعدها ارتكز الفصل الرابع على مستقبل المنظومة الأمنية لدول المنطقة الخليجية في ظل الطفرات المتتابعة للتقنية، وأهم الاستعدادات والمتطلّبات التي يجب اتخاذها.

وختاماً تم ذكر أهم المقترحات والتوصيات والطموحات التي تسعى دول مجلس التعاون الخليجي لتحقيقها من أجل بناء منظومة رقمية موحَّدة وآمنة، تحقق الطموحات وترتقي بمساعي دول المنطقة.

أولاً ـ أبرز التهديدات السيبرانية التي تواجه منطقة الخليج العربي:

تعتبر الهجمات الإلكترونية بمنزلة اعتداء شبه مباشر على السيادة الوطنية الإلكترونية لما تحمله من أخطار على الأفراد والمجتمعات والدول بصورة عامة، إلى جانب أن القدرات السيبرانية تشكّل مجالاً مهماً لممارسة النفوذ وتحقيق التفوق والتنافس الدولي، ولهذا يدعو الباحثون بمجال أمن المعلومات الدول إلى بذل جهود كبرى لتمتين حصانتها الإلكترونية وأمنها السيبراني، ونظراً إلى أن منطقة الخليج تعتبر منطقة اقتصادية غنية ومليئة بالثروات المالية والنفطية، وموطناً للمقرّات الإقليمية للعديد من الشركات والمؤسسات العالمية، بالإضافة إلى كونها قاعدة للعمليات العسكرية الحيوية؛ فإنها تمثّل هدفاً لأنشطة الجرائم الإلكترونية.

ومن المرجّح أن المنصَّات الرقمية الحكومية والتابعة لمؤسسات حسّاسة، أو عاملة في القطاع الخاص باتت عُرضة أكثر لهجمات محتملة من قراصنة مجهولين أو موظفين من قِبل دول تربطها مع دول الخليج نزاعات علنية أو خفية أو حتى أطماع للسيطرة والاستحواذ، من جانب آخر، الخسائر الناجمة عن الهجمات الإلكترونية في دول مجلس التعاون تفوق المتوسطَ العالمي، ولا يمكن استرداد معظم الخسائر المالية الناجمة عن هذه الهجمات، وأثبتت نماذج الهجمات الإلكترونية السابقة على دول المجلس إمكانية إلحاق الضرر بالمرافق الحيوية والبنيات التحتية بهذه الدول، مما يحتم بذل المزيد من الجهود لسد الثغرات في الأمن الإلكتروني بهذه الدول.

ووفقاً لما توصّلت إليه تحريات بعض الباحثين والخبراء، فإن الإمارات العربية المتحدة تعتبر في صدارة الدولة الأكثر تعرّضاً لتلك الهجمات السَيبرانِيّة على مستوى العالم، وتلتها السعودية والكويت، ثم سلطنة عُمان وقطر في المرتبة الثالثة، وأن أكثر القطاعات عُرضة للاختراق هو القطاع النفطي والمالي والعسكري، وفي فبراير ٢٠٢٠، حذّر خبراء في مجال الأمن السيبراني، في تقرير نشره موقع «cisomag.com»، من أن دول الخليج ستشهد ارتفاعاً في الهجمات الإلكترونية المدعومة في الأعوام المقبلة - ما يُعرف بـ«التهديدات المستمرة المتطورة»، مقارنة بالأنشطة الإجرامية الأخرى.

ووفقاً للتقرير، أوضح مدير المرونة الرقمية والأمن السيبراني في شركة «PwC» الشرق الأوسط، سيمون فيرناشيا، أن التوترات الجيوسياسية نتج عنها ارتفاع في التهديدات السيبرانية المحتملة التي تستهدف بنى تحتية حساسة؛ وتوقع أن تكون هناك تهديدات من جهات فاعلة عالمياً تهدف إلى تخريب خطوط الإمداد الرئيسة في المنطقة، مثل: النفط والغاز والبتروكيماويات، إضافة إلى شبكات الكهرباء، مبيناً أن أنشطة الجرائم الإلكترونية ستستمر في النمو بالمراكز المالية في دول الخليج.

وحسب تقرير نشرته «Honeywell»، أنه من المتوقع أن ينمو سوق الأمن السيبراني في الشرق الأوسط بمعدل سنوي مركب ٢٢,٥٪، وذلك بين عامي ٢٠١٨ و٢٠٢٤، ووفق تقرير نشره موقع "مودرن دبلوماسي" الأمريكي، فإن المجال السيبراني بات المجالَ العملياتي

الخامس، إلى جانب الجو والفضاء والبر والبحر، وإن أكثر من ٤٠ دولةً الآن تمتلك إمكانات عسكرية في هذا المجال، منها ١٢ دولة تتمتع بقدرات سيبرانية هجومية صريحة، وفي ١٦ يونيو ٢٠٢٠، كشف باحثون بشركة "كاسبرسكي" المتخصصة بالأمن الإلكتروني، أن دول الخليج الست تعرّضت لقرابة ٢٨٢ ألف هجمة على مستخدمي الهواتف الذكية فيها؛ من يناير حتى يونيو ٢٠٢٠.

وكشفت إحصاءات شبكة "كاسبرسكي" الأمنية (KSN)، في أكتوبر ٢٠٢٠، أن البرمجيات المالية الخبيثة التي شوهدت في جميع أنحاء دول الخليج، زادت بنسبة ٤٥٪ في النصف الأول من عام ٢٠٢٠، مقارنة بالفترة نفسها من العام الماضي، وبحسب المنصة المتخصصة التي صُمّمت لمعالجة المعلومات المتعلّقة بالتهديدات وتحويلها إلى رؤى متعمقة قابلة للتنفيذ، فقد جاءت سلطنة عُمان في القائمة الأعلى بالمنطقة بنسبة بلغت ٧٢٪، تلتها السعودية بـ٥٥٪، وتبعتها الإمارات بـ٥ , ٤٢٪، وفي هذا السياق، قالت وزارة الخارجية البحرينية في تقرير لجنة الشؤون الخارجية والدفاع والأمن الوطني بمجلس النواب: إن الاتفاقية الأمنية الخليجية لعام ١٩٩٤ جُددت بموجب الاتفاقية الأمنية بين دول المجلس لعام ٢٠١٢، بغية المساهمة في محاربة الجريمة بأنواعها كافة، وعلى الأخص الجرائم السيبرانية.

وفي ديسمبر ٢٠٢٠، كشفت شركة "بروف بوينت" للأمن السيبراني، أن ما يصل إلى ٨٢٪ من المؤسسات في الإمارات استهدفت بهجمات إلكترونية،

من جانب آخر، صرَّحت شركة "كاسبرسكاي" في عام ٢٠٢٣ بأن الكويت تتعرَّض لأكثر من ٥٣٠٠ هجوم يومياً باستخدام ١٠ أنواع مختلفة من الفيروسات والملفات الملغّمة بشفرات معقدة تساعد على اختراق الأجهزة والحواسيب، إلى جانب تعرض مؤسسات دولة الكويت إلى برامج الفدية بصورة كبيرة الأمر الذي سبب عطلاً لبعض أنظمتها، وفقدان للبيانات للبعض الآخر.

وقد نصح خبراء كاسبرسكي الشركات والمؤسسات المالية في الكويت لتعزيز دفاعاتها في عام ٢٠٢٤ تحسباً للازدياد المتوقع للتهديدات السيبرانية المدفوعة بقدرات الذكاء الاصطناعي والأتمتة العالية التطور، كما كشفت شركة "ترينـد مايكرو" التقنية في تقرير لها لعام ٢٠٢٠، عن صد أكثر من ١٠ ملايين هجمة إلكترونية في دولة قطر، ما يدفع الدولة لاستنفار كل إمكانياتها لمواجهة هذا الخطر، فقد تعرّضت دولة قطر لأكثر من ٤,٧ ملايين تهديد عبر البريد الإلكتروني، و٤,٧ ملايين هجمة باستخدام الروابط الضارة، إضافة إلى ما يُقارب نحو ٢٠ ألف هجمة عبر الروابط المضيفة.

وبحسب تقرير الشركة، فإن الشبكات المنزلية في قطر شكَّلت المصدر الرئيس لاستقطاب مجرمي الإنترنت الذين يستهدفون الأنظمة والأجهزة والشبكات، ومن جانب آخر، أظهرت الدراسة التي أجرتها شركة «إن جي إن» العالمية لأنظمة المعلومات المتكاملة بالتعاون مع شركة «جروب أي بي» العالمية تعرض ٦٠٪ من المؤسسات والشركات والمنظمات العاملة في مملكة

البحرين لهجمات سيبرانية كانت تستهدف سرقة البيانات الحساسة والابتزاز والتخريب؛ كما أشارت أيضاً الدراسة إلى أن ٥١٪ من المؤسسات المستهدفة «لا تملك إطار عمل مناسباً للحماية من الأخطار السيبرانية المرتفعة».

وفي السعودية تضمنت أبرز الحوادث الرئيسة في هجماتٍ استهدفت في البداية شركة أرامكو السعودية المملوكة للدولة في عام ٢٠١٢، وعطّلت نشاط الشركة لمدة شهر، فيما يُشار إليه بأكبر اختراق في التاريخ، وقد تسببت هذه البرمجيات الخبيثة في حدوث خلل في حركة الشركة مرة أخرى في نوفمبر ٢٠١٦ ويناير ٢٠١٧، كذلك أوضح تقرير Over Security Advisory Council والصادر في عام ٢٠١٦ أن الهجوم على شركة أرامكو السعودية قد كلّفها تغيير ٥٠ ألف قرص صلب لأجهزتها الحاسوبية، ولم تستطع استخدام الإنترنت لمدة خمسة أشهر تقريباً، وهذا يعتبر زمنًا قياسيًا في الإصلاح، خاصة إذا ما أخذ في الاعتبار إمكانات أرامكو المالية والتقنية، وأعلنت الهيئة الوطنية للأمن السيبراني السعودي في عام ٢٠٢٠ أن المملكة تواجه نحو ٢٢٤٤ هجمة إلكترونية يومياً، بمعدل ٥ , ٩٣ هجمة كل ساعة.

وأعلنت شركة «كاسبرسكي» أن المملكة العربية السعودية تواجه ارتفاعاً ملحوظاً في الهجمات في معدل الهجمات الإلكترونية وصل إلى ١٩٪ في ٢٠٢١، وفي سلطنة عُمان، تم حظر أنواع مختلفة من البرمجيات الخبيثة على ١ , ٣٣٪ من أجهزة الحاسوب المتصلة بنظم الرقابة الصناعية، بين يناير وسبتمبر ٢٠٢٢، وفقاً لإحصاءات فريق الاستجابة للطوارئ الرقمية في نظم الرقابة الصناعية لدى كاسبرسكي المتخصصة في الأمن

الإلكتروني، حيث إن تلك الأجهزة متصلة بنظم الرقابة الصناعية في قطاعات النفط والغاز والطاقة وصناعة السيارات وأتمتة المباني وغيرها، وتُستخدم لأداء مجموعة من الوظائف القائمة على التقنيات التشغيلية، من محطات عمل المهندسين والمشغّلين إلى خوادم التحكّم الإشرافي وتحصيل البيانات (SCADA) وواجهات التفاعل بين الإنسان والآلة.

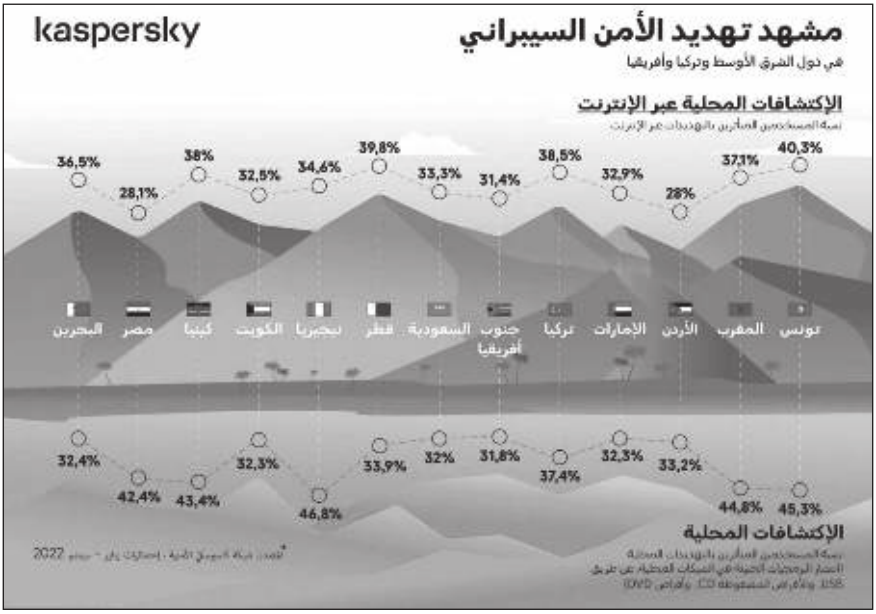
وتُعدّ الهجمات الرقمية على هذه الأجهزة شديدة الخطورة؛ لأنها قد تسبب خسائر مادية وتعطلاً في الإنتاج وحتى في عمل المنشأة كلها، وذلك نظراً لطبيعة استخدامات تلك الأجهزة والأنظمة المتصلة بها، كذلك فإن توقّف المؤسسات الصناعية والمرافق الحيوية عن الخدمة يمكن أن يُحدث خللاً في المنظومات الاجتماعية والبيئية وحتى في الاقتصاد الكلي للمنطقة.

وفي دراسة أخرى أجرتها شركة كاسبرسكي الأمنية Kaspersky Security Network لعام ٢٠٢٣ عن أرقام التهديدات الواردة في المنطقة (١) والتي تؤكد على تأثّر نحو ثلث المستخدمين في منطقة الشرق الأوسط وتركيا وإفريقيا بالتهديدات القادمة عبر الإنترنت وعبر غيرها من نواقل الهجوم المادية (غير المتصلة بالإنترنت) بدءاً من Metador، أحدث العصابات في الفضاء الرقمي، والتي استهدفت شركات الاتصالات، كذلك وسّعت عصابة HotCousin عملياتها إلى هذه المنطقة التي شهدت عدداً من الحملات التي تنشر العديد من منافذ IIS الخلفية، تنفيذ Death-Stalker و Lazarus هجمات على قطاعات متعدّدة، فيما اكتُشف منفذ خلفي لدى جهات حكومية ومنظمات غير ربحية، كما هو موضح

بالشكل (١) ؛ ففي الشرق الأوسط تحديداً، كان أكبر عدد من المستخدمين تأثراً بالتهديدات القادمة عبر الإنترنت في قطر، وذلك بواقع ٣٩,٨٪ من المستخدمين في الدولة، التي تلتها البحرين بنسبة ٣٦,٥٪، فالمملكة العربية السعودية بنسبة (٣٣,٣٪)، ودولة الإمارات بنسبة (٣٢,٩٪)، والكويت بنسبة (٣٢,٥٪)، فيما كانت مصر والأردن الأقلّ تأثراً بالتهديدات، بنسبة (٢٨,١٪) و(٢٨٪)على التوالي.

وكان أكبر عدد من التهديدات غير المتصلة بالإنترنت في الشرق الأوسط في مصر بنسبة (٤٢,٤٪) من المستخدمين في البلاد، ثمّ قطر بنسبة (٣٣,٩٪)، فالأردن بنسبة (٣٣,٢٪)، فيما سجّلت البحرين نسبة (٣٢,٤٪) والإمارات نسبة (٣٢,٣٪) والكويت نسبة (٣٢,٣٪)، وسجّلت السعودية أقلّ نسبة من المستخدمين المتضررين في الشرق الأوسط من التهديدات المحلية بنسبة (٣٢٪).

وشهد العام ٢٠٢٢ زيادة في عدد الهجمات المستمرة والمعقّدة التي تستهدف مختلف الدول في منطقة الشرق الأوسط وتركيا وبالأخص إفريقيا، أما في العام الماضي فشهدت المنطقة العديد من التهديدات الجديدة النشطة.



● الشكل (١): مشهد تهديد الأمن السيبراني في دول الشرق الأوسط وتركيا وأفريقيا

وتشمل التوقعات بالتهديدات المتقدمة الأخرى للعام ٢٠٢٤ ما يلي:

- يتوقع خبراء كاسبرسكي أن تزيد الهجمات السيبرانية المدفوعة بقدرات الذكاء الاصطناعي والتي تتنكّر على هيئة قنوات اتصال مشروعة، مما يؤدي إلى انتشار الحملات الأقل جودة بسرعة.

- علاوة على ذلك، يتنبأ الخبراء أن يستغل المجرمون السيبرانيون شعبية أنظمة الدفع المباشر، وبالتالي ظهور برمجيات خبيثة تستهدف حافظات النسخ واللصق، وبرمجيات حصان طروادة وتستهدف العمليات المصرفية التي تتم عبر الهاتف المحمول، فمنذ الآن، قد توسعت

عائلات برمجيات خبيثة مثل Grandoreiro إلى خارج البرازيل التي ظهرت فيها أولاً، مستهدفة أكثر من ٩٠٠ بنك في ٤٠ دولة.

- يتمثّل اتجاه آخر مقلق في عام ٢٠٢٤ في زيادة عدد الحزم البرمجية الخبيثة التي تستخدم أبوابًا خلفية لاختراق برامج مفتوحة المصدر، هذا الاستغلال للثغرات في البرامج مفتوحة المصدر واسعة الانتشار سيهدد أمن الكثيرين، وربما يؤدي إلى انتهاك بيانات شخصية وخسائر مالية.
- انخفاض استغلال ثغرات اليوم صفر (Zero Vulnerabilities)، وارتفاع استغلال ثغرات اليوم واحد (one Vulnerabilities)، بهدف زيادة إمكانية الوصول، ستنتقل مصادر هجمات برمجيات الجريمة إلى استغلال ثغرات اليوم واحد بسبب موثوقيتها الأكبر وندرة ثغرات اليوم صفر.

ومن جانب آخر، وبحسب ما ورد من رئيس مجلس الأمن السيبراني لحكومة دولة الإمارات العربية المتحدة، عن أن المجلس بالتعاون مع شركائه تصدّى لأكثر من ٧١ مليون هجمة سيبرانية استهدفت قطاعات استراتيجية في الدولة، منذ بداية ٢٠٢٣، وحتى الربع الثالث منه، ولفت إلى أن القطاعات المصرفية والمالية والصحية والنفط والغاز هي الأكثر استهدافاً، وتوقع أن تتزايد هذه الهجمات في ظل التطور التكنولوجي المتسارع، وتشكّل هذه الجرائم الإلكترونية جزءاً من اتجاه أوسع، حيث بدأ المهاجمون على المستويين الفردي والجماعي، في استهداف البنى التحتية الرئيسة كوسيلة لإثارة ذعر المواطنين وابتزاز الشركات أو السلطات مقابل الحصول على المال.

وفي هذا الصدد، أوضحت شركة «ترينـد مايكرو» للأمن السيبراني، أن «الجهات الفاعلة ذات النوايا الخبيثة في الوقت الحالي قد اختارت المطالبة بفدية أكبر من الأهداف التي من المرجّح أن تدفع لها، مثل شركات الرعاية الصحية والحكومات المحلية والأعمال التجارية»، وكتب كل من غاي مينز وروكسان فارمانفرمايان، في مجلة «فورين بوليسي» أن «الخليج أصبح بشكل سريع مختبراً لأخلاقيات وممارسات الحرب الهجينة، وهي استراتيجية عسكرية تجمع بين الحرب التقليدية والحرب غير النظامية والحرب السيبرانية».

وبالعودة لعام ٢٠١٤، خلص جيمس أندريه، من مركز الدراسات الدولية والاستراتيجية - CSIS، إلى أن "منطقة الخليج فريدة من نوعها، حيث إن استخدام الحكومات تقنيات الإنترنت من أجل العمل السري أكثر انتشاراً من أية منطقة أخرى ما عدا شبه الجزيرة الكورية، وفي تقرير حديث لـ "المعهد الملكي للشؤون الدولية"، أشار كل من جيمس شايرس وجويس حكمة، إلى أن "جميع دول مجلس التعاون الخليجي تواجه تهديدات تقليدية كبيرة في الفضاء الإلكتروني، مثل برامج الفدية والاحتيال الإلكتروني والقرصنة؛ ولكن هذه الدول بشكل خاص تستهدف التهديدات المستمرة المتقدمة - APT، أو الحملات التي ترعاها دول، والتي تشمل عمليات التجسس السيبراني".

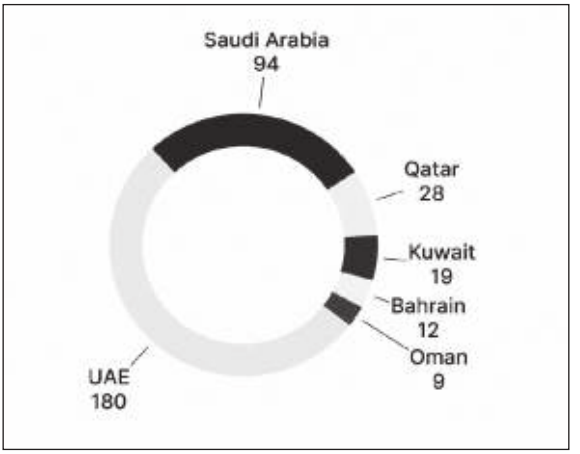
وبعد التوجّه العالمي بالتحول الرقمي والخدمات السحابية، والتي أثّرت بصورة مباشرة في ازدياد الجرائم الإلكترونية والمحاولات المتكررة

للاختراقات، تم استهداف الأنظمة الإلكترونية للقطاعين الحكومي والخاص بمختلف البرمجيات الخبيثة أهمها برامج الفدية، وهجمات تدميرية مثل الفيروسات والديدان الإلكترونية، ناهيك عن الاحتيالات الإلكترونية المستمرة، ويعد هذا الأمر مصدر قلق بالنسبة لدول مجلس التعاون، خاصةً أنها تركّز على استقطاب الاستثمارات وتطوير بيئة عمل شفافة بعد انخفاض أسعار النفط عام ٢٠١٤، وللمحافظة على مواردها واقتصاداتها وتحقيق أهدافها الاستثمارية والاقتصادية، وجب على دول الخليج العربي الاهتمام بمجال الأمن السيبراني وجعله من أهم أولوياتها، وإضعاف أي محاولة قد تسبب في انهيار أنظمتها واستثماراتها.

من جانب آخر، باتت القدرات السيبرانية مجالاً مهماً لممارسة النفوذ وتحقيق التفوق والتنافس الدولي، فلم تعد ترسانات الأسلحة التقليدية هي المعيار الأساسي والوحيد لقياس القوة بعد الثورة المعلوماتية، وهذا يتطلّب من الخبراء والدول الاختراع والبحث عن نماذج لقياس مؤشرات القدرات السيبرانية وتصنيفها كما هي الحال في جانب القوة الصلبة؛ لأن بناء أدوات تقيس قدراتها الإلكترونية بات حاجة ملحّة تساهم في فهم هذا المجال البالغ الأهمية لتحسين الاستراتيجيات الوطنية والسياسات الإلكترونية للدول، في ظل تصاعد المواجهة الدولية في فضاء أصبح جزءاً من التفاعلات الدولية بعد أن توسّعت وازدادت معدلات التهديدات وتزايدت الهجمات الإلكترونية بشكل كبير.

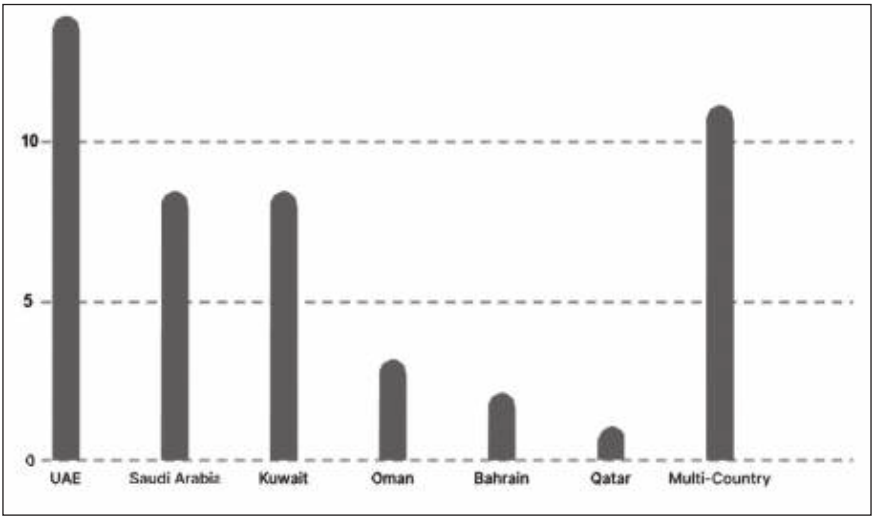
وقد قام فريق SOCRadar dark web [2]، في الفترة الزمنية ما بين مارس ٢٠٢٢ وفبراير ٢٠٢٣، برصد أهم التسريبات والحوادث التي تعرّضت لها منطقة الخليج العربي، وأهم ما جاء في التقرير ما يلي:

- تم الكشف عن ٣٠٩ مشاركة على شبكة الإنترنت المظلم تتعلّق بدول مجلس التعاون الخليجي بين النطاق الزمني من ١ مارس ٢٠٢٢ إلى ٢٨ فبراير ٢٠٢٣، يهدف ٩٨٪ من المنشور إما إلى بيع البيانات أو مشاركتها دون أي تعويض.
- قام الفريق برصد ٤٧ برمجية الفدية (ransomware) أهمها (LockBit3.0. AlphVM/Blackcat) و (Mallox groups) الدول الأكثر استهدافاً من قِبل الجهات الفاعلة في التهديد هي: الإمارات العربية المتحدة والمملكة العربية السعودية والكويت بين النطاق الزمني من ١ مارس ٢٠٢٢ إلى ٢٨ فبراير ٢٠٢٣.



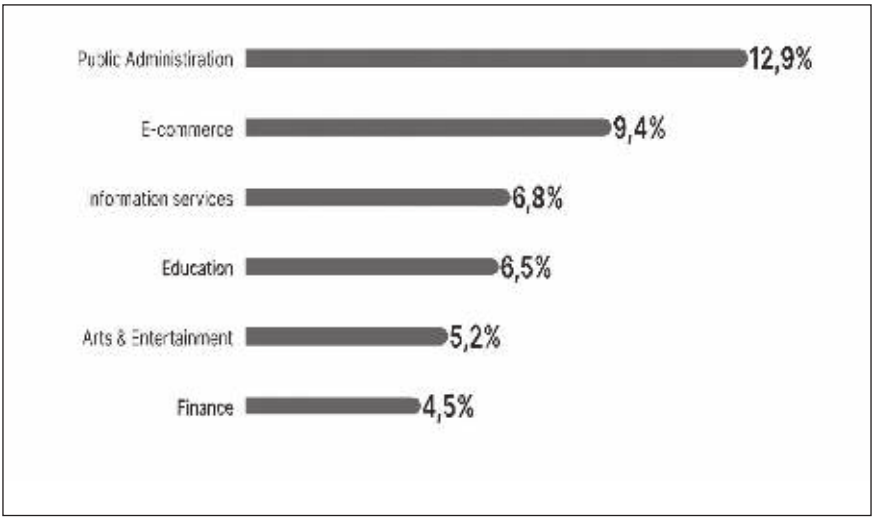
● **الشكل (٢): الدول الأكثر استهدافاً من قبل الجهات الفاعلة في التهديد**

يوضح شكل (٣) أن الدول الأكثر استهدافاً من قِبل الجهات الفاعلة في التهديد كانت الإمارات العربية المتحدة والمملكة العربية السعودية والكويت.



• الشكل (٣): توزيع الدول الخليجية حسب تعرضها لبرنامج الفدية (٤٧ هجوماً)

- أهم المجالات المستهدفة في منطقة دول مجلس التعاون الخليجي هي «الإدارة العامة»، تليها صناعات التجارة الإلكترونية، وخدمات المعلومات (كما هو موضح بالشكل (٤))



• الشكل (٤): تصنيف المجالات المعرّضة للهجوم السيبراني

• تم تسجيل ما مجموعه ٧٥٥ هجمة للتصيد ضد دول مجلس التعاون الخليجي.

وبعد تحليل الهجمات الواقعة على الدول الخليجية، تبيّن أن تعرّض البيانات كان أكثر أنواع منشورات الويب المظلمة شيوعاً، وتشمل البيانات المكشوفة البيانات السرية للشركات الخاصة والمنظمات الحكومية، والموظفين، ومعرفات العملاء، وأكثر من ذلك بكثير، وبعد تسرّب البيانات الحساسة، كانت المشاركات حول بيع الوصول إلى شبكات المؤسسات ولوحات الإدارة هي ثاني أكثر أنواع المنشورات شيوعاً، وتشمل البيانات المكشوفة بيانات الاعتماد لشبكات الشركة، لوحات المشرف، و/ أو بيانات الاعتماد فين ورديب الاتصالات.

● الشكل (٥): تهديدات الويب المظلمة. أنواع منشورات الويب المظلمة

- أما عن أهم وأكثر البرمجيات التي تتعرّض لها منطقة الخليج هي ما يلي :

ـ برمجيات الفدية (LockBit3.0).

ـ التهديد المستعصي المتقدم

(APT) (Turla Group, CHRYSENE, Leviathan, Naikon, HAZY TIGER, El Machete, MAGNALLIUM, RAZOR TIGER, Infy, MuddyWate).

ـ تهديدات التصيد (Phishing Threats).

وقد تعرضت مؤخراً بعض دول الخليج العربي لعدد من الاختراقات كما يلي :

- في ٤ مارس ٢٠٢٣، أوقفت وزارة التجارة والصناعة الكويتية محاولة قرصنة برمجية الفدية Lock bit 3.0 virus والتي تسللت إلى الشبكة من خلال أجهزة الكمبيوتر الشخصية.

- في ٤ مارس ٢٠٢٣، تعرّضت وزارة المالية في دولة الكويت لهجوم الفدية، وحدّد المخترق الفدية المطلوبة بنحو ١٥ بيتكوين بما يعادل نحو ٤٠٠ ألف دولار.
- في ٢ مارس ٢٠٢٣، قاعدة بيانات سكان دبي معروضة للبيع.
- في ٢٥ فبراير ٢٠٢٣، تسريب وثائق حساسة للهيئة الوطنية لمكافحة الفساد في المملكة العربية السعودية.
- في ١٤ فبراير ٢٠٢٣، قراصنة يستهدفون مطار البحرين ومواقع إخبارية للاحتفال بالانتفاضة.
- في ٦ فبراير ٢٠٢٣، تم الكشف عن بيع وصول غير مصرّح به لشركة نفط عربية سعودية.
- في ١ فبراير ٢٠٢٣، بيانات حساسة لحكومة المملكة العربية السعودية معروضة للبيع.
- في ٢٩ يناير ٢٠٢٣، تم الكشف عن بيع الوصول غير المصرّح به إلى الشبكة للخدمات الداخلية لحكومة قطر.
- في ١٥ ـ ٢٥ يناير ٢٠٢٣، تعرّض العديد من عملاء البنوك في الكويت لحملات تصيد عبر البريد الإلكتروني، وتلقى الضحايا رسائل البريد الإلكتروني تبدو وكأنها قادمة من إدارة البريد في وزارة الاتصالات الكويتية، أو من شركات البريد السريع مثل، دي إتش إل، وأرامكس مع وجود صلة خبيثة.

- في ٢١ يناير ٢٠٢٣، تم عرض بيانات المواطنين الإماراتيين للبيع.
- في ٢٢ نوفمبر ٢٠٢٢، استهداف موظفي كأس العالم في قطر بالهجمات الإلكترونية الاحتيالية.
- في ٣ يناير ٢٠٢٣، تسرّبت بيانات شركات النفط والغاز القطرية.
- في ٤ يوليو ٢٠٢٢، تسجيل أكثر من ٢ مليون هجوم إلكتروني خلال شهر خلال موسم الحج.

وستستمر تلك الهجمات السيبرانية ومحاولات الاختراق المتكررة الطامعة على منطقة الخليج العربي باستمرار التطور التكنولوجي، واعتماد دول المنطقة على تلك التقنيات العالمية في رسم مسارات سياساتها الدولية المختلفة، وبناء على دراسات عدة، تبيّن أن أهم النطاقات الرئيسة من الفضاء السيبراني قد تواجه فيها بلدان الخليج هجمات كبيرة في المستقبل هي ما يلي:

١. الهجوم على سلسلة التوريد عبر اختراق المورّدين:

يمكن أن تؤدي عمليات التسلل الناجحة إلى منصات برامج المورّدين في سلاسل التوريد الضخمة إلى أخطار في عدد لا يحصى من الشركات بشكل متزامن، ويعتبر هجوم NotPetya الذي قام فيه القراصنة بتخريب برنامج الضرائب الأوكراني وإرسال تحديثات خاطئة انتشرت عبر الشبكات المخترقة وأصابت نقاط الاستخدام النهائية ببرمجيات خبيثة، المثال الأبرز حتى الآن.

٢ . استهداف أنظمة التحكم الصناعية:

تمثّل أنظمة التحكم الصناعية مجموعة متنوّعة من التقنيات التي تقوم بإدارة وأتمتة أجزاء كبيرة من المجتمع، بما في ذلك شبكات الكهرباء وعمليات النفط والغاز والتصنيع وغيرها، ومن الممكن أن تكون الهجمات على أنظمة التحكّم الصناعية مدمّرة كونها قد تؤدي إلى توقف العمليات وحتى التسبب بأضرار مادية.

٣ . مهاجمة أدوات ومنصات برمجيات تابعة لجهات خارجية:

مع نضوج عمليات تطوير النظم، تهدف منصات البرمجيات إلى توفير أفضل فائدة للمستهلكين والمطورين، كما أن العديد من هذه المنصات سهل الاستخدام ويمكن تعديله وفق الطلب ببساطة، ما يزيد من سهولة تعرّض هذه المنصات للاختراق من قِبل القراصنة الذين يسعون لنشر الشيفرات الخبيثة عبر التطبيقات التي يقومون بإنشائها، ومع تطوّر عملية تطوير النظم في الشرق الأوسط، ينبغي أن تكون المؤسسات حذرة من أخطار قيام القراصنة بتعريض مكتبات البرمجيات وأدوات تطوير النظم التابعة لجهات خارجية لاختراقات من هذا النوع.

٤ . استغلال بيئة العملة المشفّرة:

في وقت سابق من هذا العام، سرق القراصنة نحو ٥٣٢,٦ مليون دولار من مؤسسة لتحويل العملة المشفرة في طوكيو، ما أدّى إلى إعادة إطلاق النقاشات حول الأمن والحماية التنظيمية في السوق الناشئة بالنسبة

للعملات المشفّرة مثل بيتكوين Bitcoin. وفيما يفكّر المشرّعون الماليون في دولة الإمارات بوضع قوانين خاصة بالعملة المشفّرة وتطوير إطار عمل مع شركات القطاع والهيئات المرتبطة بنشاطها، فإن البيئة التي تفتقر إلى معايير حماية أمنية عالمية صارمة تظل هدفاً مربحاً للقراصنة، خصوصاً مع استمرار توسّع عدد فئات العملة المشفّرة وتبادلها.

٥. خرق القواعد الضخمة للبيانات:

فيما تسعى دول الخليج مثل المملكة العربية السعودية والإمارات العربية المتحدة إلى رقمنة اقتصاداتها وقطاعاتها الصناعية بأكملها، كالسجلات الصحية الإلكترونية على سبيل المثال، تشكّل قواعد البيانات المتزايدة بفعل التحوّل الرقمي أهدافاً جديدة للقراصنة.

٦. تطور أدوات الاختراق من خلال استخدام تقنيات الذكاء الاصطناعي:

استخدام تقنيات الذكاء الاصطناعي سيزيد من الهجمات السيبرانية المدفوعة بقدرات قد تكون خارقة من خلال إضافة أساليب تتنكّر على هيئة قنوات اتصال مشروعة، مما يؤدي إلى انتشار الحملات الأقل جودة بسرعة، علاوة على ذلك، فإن تقنيات الذكاء الاصطناعي ساعدت على ظهور تقنيات فائقة الجودة في الاختراق والتسلسل في الأنظمة من خلال كتابة البرامج الضارة واختراق كلمات المرور والبحث عن نقاط الضعف في البرامج، وتحليل البيانات واستخدام برمجيات خبيثة تستهدف حافظات النسخ واللصق، وبرمجيات حصان طروادة وبطرق ذكية ويصعب اصطيادها.

٧. برمجيات الفدية وتطورها بصورة مخيفة:

لا تزال حملات القرصنة بنظام الفدية تحقق خسائر كبيرة قد تؤثر على اقتصاديات الكثير من الدول، لكن ما هو أكثر خطورة يتمثّل في سيناريوهات يهاجم فيها القراصنة شبكات حكومية أو قطاعية يحتمل أن تؤدي إلى تعطيل العمليات، وفي جميع أنحاء منطقة الخليج، يؤدي إطلاق برامج الحكومة الذكية وأنظمة التشغيل الآلي، مثل البوابات الإلكترونية في المطارات وغيرها، إلى استحداث نقاط ضعف محتملة تمكّن الهجمات من استغلالها لإحداث اضطرابات كبيرة.

٨. استهداف الأحداث والمناسبات البارزة:

إن المناسبات والأحداث الكبيرة لا تؤدي فقط إلى جذب الحشود الضخمة، بل أيضاً إلى لفت اهتمام القراصنة، وأبرزها انتشار جائحة كورونا، وكأس العالم في قطر، ومعرض إكسبو في دبي وقطر، وموسم الرياض وغيرها من مناسبات قد تكون جاذبة لأعداد هائلة من الهجمات السيبرانية.

وتتلخّص أبرز الأسباب التي ساعدت على انتشار التهديدات السيبرانية في المنظومة الخليجية فيما يلي:

١ ـ تعتبر دول الخليج العربي دولاً نفطية ذات مستوى معيشي مرتفع، وهذا يجعلها مطمعاً لكثير من المخترقين والمحتالين.

٢ ـ الهجمات السيبرانية المتطورة، تزداد تعقيدات تقنيات الذكاء الاصطناعي وتطورات الهجمات السيبرانية، وأصبحت عملية الكشف والسيطرة

على الهجمات أكثر صعوبة مما يتطلّب تحسين استعداد الدول للتصدي لها والتعامل مع التهديدات المتقدمة.

٣ ـ تراجع دور الدولة في ظل العولمة والانسحاب من بعض القطاعات الاستراتيجية مع تصاعد أدوار الشركات متعددة الجنسيات، خاصة العاملة في مجال التكنولوجيا كفاعل مؤثر في الفضاء السيبراني.

٤ ـ تعتبر دول المنطقة الخليجية من الدول المستهلكة وليس المنتجة للتقنيات والأنظمة المختلفة، وهذا ما يجعل التفاصيل الفنية للتطبيقات المستخدمة والخدمات السحابية تغيب عنها.

٥ ـ تزايد اعتماد الدول على الأنظمة الإلكترونية في جميع منشآتها الحيوية، الأمر الذي جعل من الممكن الإضرار بمصالحها من خلال الهجمات الإلكترونية في حالات العداء.

٦ ـ نقص المهارات والكوادر والكفاءات المؤهّلة والمتخصصة في مجالات الأمن السيبراني على المستوى الوطني، وغياب الكوادر الوطنية والاعتماد على الكوادر الأجنبية في التكنولوجيا.

٧ ـ عدم وجود وحدات تنظيمية متخصصة في الأمن السيبراني ضمن الهياكل التنظيمية في أغلب المؤسسات الحكومية والخاصة.

٨ ـ تزايد حجم البيانات والتشعب التكنولوجي، الأمر الذي يشكّل تحدياً كبيراً يواجه عملية رقابة وإدارة الأمن السيبراني وتأمين هذه البيانات.

٩ ـ تحديات التشريعات والقوانين التي تنظم العلاقات مع التقنيات الرقمية المتغيّرة والمختلفة وضمان امتثالها لمعايير الأمن السيبراني.

١٠ ـ التهديدات السيبرانية المستمرة للبنية التحتية الحيوية، وتشمل التحديات حماية البنية التحتية الحيوية مثل: الكهرباء والماء والنقل من الهجمات السيبرانية التي يمكن أن تؤثّر على حياة السكان واستقرار الدولة.

١١ ـ وجود شركات عالمية وكيانات مسيطرة ومتحكّمة بصورة كبيرة على حماية خصوصية شعوبنا ومقدّراتنا، الأمر الذي يستوجب تقليل حدّة الاعتماد عليها مثل: شركة ميتا فيرس، وشركة إكس (سابقاً تويتر) وغيرها من شركات.

١٢ ـ التحديات الدولية والتعاون الدولي في مجال قضايا التعاون الدولي في مجال مكافحة الجريمة السيبرانية وتبادل المعلومات، حيث يتطلّب الأمن السيبراني جهوداً مشتركة للتصدي للتهديدات عبر الحدود.

١٣ ـ ضعف الوعي بأهمية الالتزام بسياسات الأمن السيبراني لدى معظم فئات المجتمع بمختلف أعمارهم.

إلى جانب ذلك، فإن أهم مواضع القصور التي تعاني منه بعض المؤسسات الخليجية هي ما يلي:

١ ـ وجود ضعف في أنظمة مراقبة العمليات، وبالتالي عدم القدرة على كشف حالات الاختراق منذ وقتٍ مبكر.

٢ ـ وجود قصور كبير جدًا في تتبع الأموال الناتجة عن عمليات الاحتيال وإيقافها قبل خروجها من الدولة.

٣ ـ ضعف في إجراءات تلقي بلاغات الاحتيال، والتعامل معها من حيث الرصد والتحقيقات والتقارير.

٤ ـ ضعف الاستثمار في البنية التحتية لأنظمة مكافحة الاحتيال باستخدام الذكاء الاصطناعي ودراسة سلوك العميل.

٥ ـ قلة الكوادر البشرية المؤهّلة في مجال الأمن السيبراني.

٦ ـ ضعف جودة البرامج التوعوية المقدّمة للعملاء، من حيث المادة والقنوات المستخدمة ووضع مؤشرات لقياس فاعليتها.

٧ ـ امتلاك المجموعات التخريبية قدرات تقنية عالية جدًا في الأمن السيبراني.

ومن المهم أن نعرف أن التعامل مع هذه التحديات تتطلّب تكامل الجهود بين الحكومة والقطاع الخاص والمؤسسات الأكاديمية أيضاً، مما يعزّز القدرة على التصدّي للتهديدات السيبرانية وتعزيز أمان البيئة الرقمية في دول الخليج العربي.

ثانياً ـ أهم إنجازات الهيئات والمؤسسات الخليجية في مجال الأمن السيبراني:

برزت أخطار أمنية وعسكرية واقتصادية من نمط جديد نتيجة لانبساط سطوة الفضاء السيبراني وتكاثر أدواته، وبدأت تلك الأخطار تهدد استقرار وكيانات واقتصاديات الدول التي باتت تخلق هواجس لإحداث أضرار متفاوتة في الكيانات الرقمية التي تقيم في الفضاء السيبراني، ونتيجة لتصعيد التهديدات وتكاثر الهجمات، بدأت الدول بتوجيه جل اهتمامها نحو ترسيخ أمن أنظمتها الرقمية وكياناتها التقنية، مع تطوير آلتها السيبرانية سواء الدفاعية أو الهجومية لضمان بسط سطوتها السيبرانية قبالة التهديدات المتكررة والمؤثّرة، فتحوّلت دائرة النزاع تدريجيًّا، من ساحة المواجهة التقليدية إلى ساحة المواجهة الافتراضية السيبرانية المستحدثة.

وفي منطقة الخليج على وجه الخصوص، تركّزت أهم تلك المواجهات الافتراضية لتخلق تهديداً ملموساً لاقتصاديات واستقرار دول المنطقة الخليجية، وذلك لأسباب عدة أهمها الاستحواذ على الثروات النفطية والاقتصادية التي تنعم بها دول المنطقة، إضافة إلى تحقيق مطامع سياسية لإعادة رسم خريطة المنطقة من خلال فك التحالفات الدولية التي تنعم بها دول الخليج العربي والتي جعلت منها قوى تنافس كبار الدول اقتصادياً وسياسياً، كما أنها تعتبر موطناً للمقرّات الإقليمية للعديد من الشركات والمؤسسات العالمية، بالإضافة إلى كونها قاعدة للعمليات العسكرية الحيوية؛ فإنها تمثّل هدفاً لأنشطة الجرائم الإلكترونية.

إلى جانب ما تعرّضت له دول المنطقة الخليجية من هجمات سيبرانية وتحديات هدّدت كياناتها الاقتصادية والسياسية، وكانت البرمجية الخبيثة Stuxnet الشرارة الأولى التي أوقدت نار تلك النزاعات السيبرانية في منطقة الخليج العربي وتكابدت بعدها الانتهاكات السيبرانية والتي قد نجح البعض منها وفشل الآخر، الأمر الذي كان ناقوس خطر لبداية إطلاق السياج الدفاعي لأنظمتها الرقمية، فبدأت دول الخليج العربي بالسعي جدياً لحماية أنظمتها الرقمية من خلال الممارسات والآليات والاتفاقيات والمعاهدات التي أبرمتها، وهنا نستعرض أهم وأبرز إنجازات دول مجلس التعاون الخليجي في مجال الأمن السيبراني.

جدول (١)
أهم المرتكزات والهيئات الخليجية المتخصصة في مجال الأمن السيبراني

الدولة	اسم الجهة	نوع الجهة
المملكة العربية السعودية	الهيئة الوطنية للأمن السيبراني	هيئة حكومية
	الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز	هيئة حكومية
	مركز المعلومات الوطني	مركز متخصص
	مركز التصديق الرقمي	مركز متخصص
	المركز الوطني الإرشادي للأمن السيبراني	مركز متخصص
	مركز التميز لأمن المعلومات	مركز متخصص
	المركز الوطني للأمن الإلكتروني	مركز متخصص

سلطنة عُمان	المركز الوطني للسلامة المعلوماتية	هيئة حكومية
	المركز العربي الإقليمي للأمن السيبراني	مركز متخصص
	مركز الدفاع الإلكتروني	هيئة حكومية
مملكة البحرين	المركز الوطني للأمن السيبراني	هيئة حكومية
	هيئة تنظيم الاتصالات ـ مبادرة إنترنت آمن	هيئة حكومية
	هيئة حماية البيانات الشخصية	هيئة حكومية
الإمارات العربية المتحدة	مجلس الأمن السيبراني	هيئة حكومية
	هيئة أبوظبي الرقمية	هيئة حكومية
	مركز دبي للأمن السيبراني	هيئة حكومية
	هيئة تنظيم الاتصالات والحكومة الرقمية	هيئة حكومية
دولة قطر	الوكالة الوطنية للأمن السيبراني	هيئة حكومية
دولة الكويت	المركز الوطني للأمن السيبراني	هيئة حكومية
	الهيئة العامة للاتصالات وتقنية المعلومات	هيئة حكومية

ثالثاً ـ أنشطة دول مجلس التعاون لدول الخليج العربية في مجالات الأمن السيبراني:

(١) ـ أنشطة المملكة العربية السعودية في مجال الأمن السيبراني :

تميّزت المملكة العربية السعودية في السنوات الأخيرة في مجالات التقنية المختلفة وخاصة في مجال الأمن السيبراني(٣)، حيث أبدت المملكة في ذلك دوراً بارزاً في المنطقة، وذلك لإدراكها الفعلي بخطورة المجال من ناحية، ومن ناحية أخرى لحرصها على الوصول للريادة دوماً وفي جميع المجالات، وقد مثَّلت المملكة ذلك من خلال الجهود المبذولة طوال مسيرتها العامرة لتعزيز الأمن السيبراني من خلال :

أ- إنشاء ٥ مراكز متخصصة، هي :

- مركز المعلومات الوطني.
- مركز التصديق الرقمي.
- المركز الوطني الإرشادي للأمن السيبراني.
- مركز التميّز لأمن المعلومات.
- المركز الوطني للأمن الإلكتروني.

ب- إنشاء جهتين حكومية ومستقلة، هما :

- الهيئة الوطنية للأمن السيبراني، هي هيئة حكومية مختصة في الأمن السيبراني في السعودية، مهتمة بشؤون الأمن السيبراني، من خلال تهيئة

كـوادر وطنية متخصصـة وطموحة وتمكينها، وبناء الـشراكات مع الجهات العامـة والخاصـة، وتحفيـز الابتكار والاسـتثمار في مجـال الأمـن السـيبراني؛ للإسـهام في تحقيـق نهضـة تقنيـة تخـدم مسـتقبل الاقتصـاد الوطني للمملكـة.

- الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز.

ج - اعتماد أنظمة وقوانين ذات صلة مباشرة بالأمن السيبراني، أهمها:

- أنظمة وتشريعات الأمن السيبراني.
- الضوابط الأساسية للأمن السيبراني.
- نظام مكافحة الجرائم المعلوماتية ٢٠٠٧.
- نظام التعاملات الإلكترونية.
- السياسات (سياسة الاقتصاد الرقمي، سياسة الحكومة الرقمية سبتمبر ٢٠٢١).
- التراخيص (خدمات تقنية المعلومات والوثائق المتعلّقة بها، وخدمات الاتصالات والوثائق المتعلّقة بها).
- وسياسات أخرى أهمها: تصنيف البيانات، والحوسبة السحابية، وحماية البيانات ...إلخ.

د - إطلاق الاستراتيجية الوطنية للأمن السيبراني:

أطلقت الهيئة الوطنية للأمن السيبراني الاستراتيجية الوطنية للأمن السيبراني، والتي تتمثَّل رؤيتها في إيجاد فضاء سيبراني سعودي آمن

وموثوق، يضمن العمل الآمن في ظل التغيرات المتسارعة للتكنولوجيا، من خلال تحقيق أهدافها:

- حوكمة الأمن السيبراني.
- إدارة الأخطار السيبرانية.
- حماية الفضاء السيبراني.
- بناء القدرات البشرية.
- تعزيز الشراكات.
- تعزيز القدرات الوطنية.

هـ - إطلاق المبادرات الوطنية في الأمن السيبراني، وأهمها:

- مبادرة سايبر هب: أطلق الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز مبادرة سايبر هب إلى تهدف إلى تطوير الكفاءات الطلابية المميزة في مجال الأمن السيبراني، بالإضافة إلى دعم إنشاء الأندية الطلابية المتخصصة في الأمن السيبراني؛ وذلك سعيًا منها إلى إيجاد كوادر بشرية وطنية تتمتع بقدر عالٍ من الكفاءة والمهارة.
- معسكر طويق السيبراني: دُشّن هذا المعسكر من قِبل الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز، والذي يهدف من خلاله إلى تأهيل الكفاءات الوطنية في مجال الأمن السيبراني وتمكينهم من فرص العمل في سوق العمل السعودي.

- مؤتمر هاك: نظّم الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز بالتعاون مع الهيئة العامة للترفيه و BlackHat أضخم حدث تقني في مجال الأمن السيبراني في منطقة الشرق الأوسط وشمال إفريقيا.
- معسكر هوماثون: مبادرة أطلقها الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز، لمناقشة التحديات التي واجهت المجتمعات جراء تفشي فيروس كورونا، وطرح حلول ابتكارية تقنية في مجالات محورية في حياة كل فرد، مثل: الصحة، والتعليم، والترفيه، والحكومة الإلكترونية، والتقنية المالية، والعمل عن بُعد، والخدمات اللوجستية.
- منصة مكافأة الثغرات: تعد هذه المنصة الأولى من نوعها بمنطقة الشرق الأوسط، وهي تهدف إلى اكتشاف أكبر قدر ممكن من الثغرات البرمجية وإغلاقها مقابل مكافآت نقدية للمبرمجين المكتشفين.
- الأكاديمية الوطنية للأمن السيبراني: دشنت الهيئة الوطنية للأمن السيبراني الأكاديمية الوطنية للأمن السيبراني لبناء قدرات الكفاءات الوطنية في مجال الأمن السيبراني لسد الاحتياج في سوق العمل السعودي، وتعزيز قوة الأمن السيبراني للمملكة.
- اتفاقية تعاون بين الهيئة الوطنية للأمن السيبراني ووزارة التعليم: جاءت هذه الاتفاقية لتعزيز التعاون المشترك بين وزارة التعليم والهيئة الوطنية للأمن السيبراني في مجالات التعليم والبحث العلمي والتوعية والتدريب في مجال الأمن السيبراني، والتي تسهم بشكل مباشر في تأهيل الكوادر الوطنية وتمكينهم في المجال.

- مهارات المستقبل: أتاحت وزارة الاتصالات وتقنية المعلومات عبر مبادرة مهارات المستقبل عددًا من الدورات التدريبية المتخصصة في الأمن السيبراني، بالإضافة إلى فرص التدريب التعاوني، والتدريب الاحترافي.
- الأكاديمية السعودية الرقمية: إحدى مبادرات وزارة الاتصالات وتقنية المعلومات التي تستهدف بناء قدرات رقمية وطنية في مجالات التقنيات الحديثة المرتبطة بتقنيات الثورة الصناعية الرابعة من خلال برامج نوعية متخصصة، ومعدّة وفق أحدث الأساليب المتبعة في التدريب العملي.
- Virtual internship : برنامج تدريبي عن بُعد يُنفّذ بالشراكة مع الأكاديمية السعودية الرقمية، ويستهدف الخريجين الراغبين في اكتساب خبرات مهنية متميزة في مجال التقنية والأمن السيبراني.
- برنامج روَّاد أمن الاتصالات: يُعد أحد برامج الأكاديمية السعودية الرقمية، ويهدف إلى تأهيل كوادر وطنية في مجال الأمن الرقمي لسد احتياج سوق العمل، وربط مخرجات الأكاديمية مع الكفاءات المهنية، بالإضافة إلى تمكين المرأة وتعزيز مشاركتها في الأمن الرقمي.
- معسكرات الهِمم الرقمية: أحد برامج الأكاديمية السعودية الرقمية يستهدف تدريب وتأهيل حديثي التخرج والباحثين عن عمل عبر معسكرات تدريبية مكثَّفة ونوعية في مجالات التقنية الناشئة والحديثة والمتقدمة.
- قدَّم صندوق الموارد البشرية (هدف) ضمن برنامج دعم الشهادات المهنية الاحترافية عددًا من الشهادات الاحترافية المتخصصة في الأمن

السيبراني؛ وذلك لتعزيز مهارات الكوادر السعودية وزيادة كفاءة سوق الأمن السيبراني بالمملكة، منها:

* أمن نظم المعلومات الاحترافية CISSP.
* شهادة المخترق الأخلاقي المعتمد CEH.
* شهادة محلل الأمن السيبراني من CompTIA.
* شهادة ممارس الأمن السيبراني CSX-P.
* CYSA .

- حصين: بوابة إلكترونية أطلقتها الهيئة الوطنية للأمن السيبراني، حيث تقدّم حصن تقارير تفصيلية حول حالة الأمن السيبراني لدى الجهات والشركات الوطنية، وذلك عبر ٤ منصات:

- منصة مشاركة المعلومات: تقديم معلومات استقصائية وفورية عن التهديدات المحلية والعالمية؛ لمساعدة الجهات على اتخاذ الإجراءات الاستباقية اللازمة.

منصة إدارة الإلزام: معرفة وقياس مدى إلزام الجهات الوطنية بضوابط ومتطلبات الأمن السيبراني التي تصدرها الهيئة.

- منصة توثيق البريد الإلكتروني: توثيق أسماء نطاقات البريد الإلكتروني وحمايتها من الانتحال والاستخدام غير المصرح به.

- منصة فحص الملفات والروابط: التحليل الآمن للملفات والروابط والكشف عن البرمجيات الضارة والحد من الاختراقات السيبرانية.

- برنامج «سايبرك» لتنمية قطاع الأمن السيبراني: برنامج شامل يضم مجموعة من المبادرات النوعية، يعي بتطوير المهارات وتنمية المعرفة في مجالات الأمن السيبراني، بالإضافة إلى توطين تقنيات الأمن السيبراني، وزيادة عدد الشركات في هذا المجال من خلال دعم الشركات الوطنية الناشئة في الأمن السيبراني والمساندة في تأسيسها.

ونتيجة لكل الجهود الكبيرة المبذولة من قِبل المملكة العربية السعودية - والتي سبق ذكرها - لخلق منظومة رقمية آمنة، وبإدارة وتشغيل كوادر وطنية تتمتع بقدرات مهنية متدرّبة ومتميّزة، حققت المملكة في عام ٢٠٢٢ المركز الثاني في مؤشر الأمن السيبراني على المستوى العالمي متفوقة على الكثير من الدول، ومحققة بذلك قفزات سريعة نحو الريادة العالمية في مجال الأمن السيبراني، مقارنة بالسنوات الماضية، ففي ٢٠١٨ حيث تبوأت المركز الـ ٣٩، وفي ٢٠١٩ حصلت على المركز الـ ٢٦، وفي ٢٠٢٠ حققت المركز الـ ٢٤ على مستوى دول العالم.

(٢) ـ أنشطة سلطنة عُمان في مجال الأمن السيبراني:

تعتبر سلطنة عُمان من الدول الريادية التي اهتمت بمجال الأمن السيبراني، حيث حصلت السلطنة ممثلة بالمركز الوطني للسلامة المعلوماتية على المركز الأول في المؤشر العالمي للأمن السيبراني من بين ٢٢ دولة عربية تم تحليلها وفق هذا المؤشر الإقليمي، وذلك حسب أحدث تصنيف للاتحاد الدولي للاتصالات ومركز «إيه بي آي ريسيرش» سنة ٢٠١٣، كما حصلت عام ٢٠٢٠ على المركز الثالث عربيًا والواحد والعشرين عالميًا من أصل

١٩٣ دولة ضمن تقرير المؤشر العالمي للأمن السيبراني ٢٠٢٠ الذي أعلنه الاتحاد الدولي للاتصالات، كما حصلت السلطنة على جائزة القمة العالمية لمجتمع المعلومات والتي تحتضنها مدينة جنيف السويسرية؛ حيث حصل المركز الوطني للسلامة المعلوماتية على جائزة من فئة بناء الثقة والحماية في استخدام تقنية المعلومات والاتصالات، ويأتي هذا الدور الريادي لسلطنة عُمان تقديراً لجهودها المميزة والكبيرة في مجال الأمن السيبراني، وإدراكها بأهميته في ظل التطورات المتلاحقة للتكنولوجيا، وضرورة التعامل مع الأخطار والتهديدات الأمنية الإلكترونية ومع الجرائم الإلكترونية ليس على المستوى الوطني فحسب، بل على المستويات الإقليمية والدولية.

ويتمثّل حرص سلطنة عُمان من خلال إنشاء ثلاثة مراكز ريادية وهي:

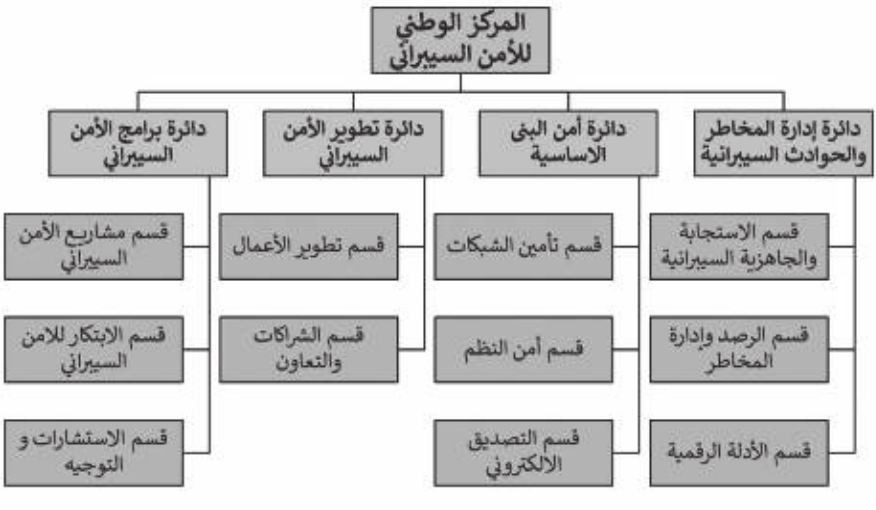
١. المركز الوطني للسلامة المعلوماتية :

تم التدشين الرسمي للمركز الوطني للسلامة المعلوماتية[٤] في شهر أبريل ٢٠١٠ وذلك لتحليل الأخطار والتهديدات الأمنية الموجودة في الفضاء الإلكتروني، ولتوصيل هذه المعلومات لجميع مستخدمي خدمات الإنترنت ووسائل تقنية المعلومات، سواء كانوا من المؤسسات العامة أو الخاصة، أو الأفراد، من خلال تأهيل كوادر وطنية في مجال الأمن السيبراني، ومن أهم مهام المركز هي كشف الحوادث الأمنية، والاستجابة الطارئة لها، وتحليل الأخطار والتهديدات الأمنية في فضاء الإنترنت العُماني لخلق قدرات أمن معلومات بمقاييس عالمية تجعل كل مستخدم للحاسب

الآلي في السلطنة يشعر بالأمن والسلامة، إلى جانب، صناعة متخصصة في الأمن السيبراني تعزز وتنوّع النمو الاقتصادي.

بالإضافة إلى ما يلي:

- العمل كمركز اتصال موثوق للإبلاغ عن أي حوادث أمنية تتعلّق بتقنية المعلومات والاتصالات.
- بناء الثقة في استخدام الخدمات الإلكترونية الحكومية.
- بناء الوعي الأمني في فضاء الإنترنت العُماني.
- بناء القدرات الأمنية للتعامل مع الحوادث الأمنية المتعلّقة بالحاسوب والإنترنت.
- تقديم معلومات دقيقة وآنية عن التهديدات الأمنية ونقاط الضعف الحالية أو الناشئة.
- تحليل التهديدات الأمنية المحتملة وآثارها.
- توفير تدابير استباقية لتقليل الحوادث الأمنية.
- الاستجابة للحوادث الأمنية والحد من آثارها.
- تشجيع البحث والتطوير في مجال أمن المعلومات.
- التنسيق مع مراكز الاستجابة لطوارئ الحاسوب على الصعيدين الإقليمي والدولي.



• الشكل (٦): الهيكل التنظيمي للمركز الوطني للأمن السيبراني

أهم الخدمات التي يقدّمها المركز:

- الاستجابة للحوادث الأمنية.
- التصديق الإلكتروني.
- مختبر الأدلة الرقمية.

كما كان للمركز مبادرات وبرامج متخصصة تميّز بها، ومن أهمها:

• برنامج حداثة، والذي يهدف إلى صناعة متخصصة في الأمن السيبراني تعزّز وتنوّع النمو الاقتصادي من خلال إنشاء صناعة متخصصة في الأمن السيبراني في المنطقة، وتُركّز على رأس المال البشري وتستند إلى الابتكار والإبداع والتميز.

- المؤشر الوطني للأمن السيبراني، وهو برنامج يسعى من خلاله إلى رفع مستوى السلطنة في مجال الجاهزية، وتعزيز الاستمرارية في الأداء، وهذا من خلال قياس مدى التزام المؤسسات بالمقاييس العالمية في مجال الأمن السيبراني ومعرفة مراكز الضعف وتحسينها وفقاً للدعائم الخمس للبرنامج العالمي للأمن السيبراني، وهي: (التدابير القانونية والتقنية والتنظيمية، وبناء القدرات والتعاون الدولي) في جميع الجهات الوطنية، وبالتعاون مع الأطراف ذات العلاقة، ومن هذا المنطلق عمل المركز على إعداد الخطة التنفيذية المفصلة لبرنامج المؤشر الوطني للأمن السيبراني؛ ليتسنى لممثلي الوزارات والمؤسسات الحكومية الشروع بالبرنامج حسب الخطة، بما يكفل إنجاح أهداف البرنامج للحصول على النتائج المرجوّة.
- الأسبوع الإقليمي للأمن السيبراني.
- التمارين السيبرانية، حيث يتم إجراء التمرين الوطني لمحاكاة المشاركين من الفرق الوطنية للاستجابة لحالات الطوارئ (CERTs)، أو فرق الاستجابة للحوادث لمختلف السيناريوهات بناءً على دراسات الحالة ومواقف الحياة الواقعية، والتي توفّر لهم فرصة لاختبار مهاراتهم ومعارفهم في الاستجابة لمثل هذه الهجمات، كما أنه يهدف إلى تعزيز العمل الجماعي، وقدرات الفرق المشاركة في الاستجابة للحوادث؛ لضمان استمرار الجهود الجماعية ضد التهديدات السيبرانية من خلال CIRT في المنطقة.
- برنامج سفراء السلامة المعلوماتية، والهدف من هذا البرنامج هو خلق وصلة دائمة بين المركز والمستفيدين من الخدمات التي يقدمها من

خلال نشر الوعي في مجال أمن المعلومات، ومشاركة المعرفة والثقافة الأمنية الإلكترونية مع الجميع؛ لتوسيع قاعدة نشر هذه المعرفة لتكون مسؤولية الأفراد والدارسين وأخصائيي أمن المعلومات بالسلطنة.

- برنامج حماية الطفل، حيث يقوم هذا البرنامج بطرح أنشطة متنوّعة لتثقيف الأطفال وأولياء الأمور عن كيفية الحفاظ على معلوماتهم الشخصية أثناء استخدامهم الإنترنت بأساليب ترفيهية بسيطة تصل إلى الطفل ويتأثّر بها مثل الألعاب ورسومات للتلوين وغيرها.
- برنامج وعي، برنامج وعي هو برنامج التدريب والتوعية الموحّد لأمن المعلومات للجهات الحكومية ومؤسسات البنية التحتية الوطنية الحرجة في سلطنة عُمان، والذي يهدف من خلال هذا البرنامج إلى الشروع في برنامج موحّد لأمن المعلومات؛ لتعزيز الوعي بأمن المعلومات والكمبيوتر، وتبادل أفضل الممارسات لتخفيف الأخطار الأمنية من أجل ضمان استمرارية الأعمال، وتقليل تأثير الأخطار الأمنية في القطاع الحكومي.

٢. المركز العربي الإقليمي للأمن السيبراني:

تم تأسيس المركز العربي الإقليمي للأمن السيبراني (ITU-ARCC) [٥] من قِبل الاتحاد الدولي للاتصالات (ITU) وسلطنة عُمان في ديسمبر ٢٠١٢ ممثلة في وزارة النقل والاتصالات وتقنية المعلومات، مع رؤية لإنشاء بيئة أكثر أمناً وتعاوناً في مجال الأمن السيبراني في المنطقة العربية، وتعزيز دور الاتحاد الدولي للاتصالات في بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات في المنطقة.

ومن أهم أهداف المركز ما يلي:

- الإشراف على تنفيذ البرنامج العام للأمن السيبراني للاتحاد الدولي للاتصالات في جميع أنحاء المنطقة العربية.
- الاستجابة لمتطلبات الأمن السيبراني لأحدث التطورات.
- خلق مركز للإدارة ومنصة لتنفيذ أهداف الأمن السيبراني.
- توفير مركز موحّد للدول الأعضاء لإدارة برامج مبادرات الأمن السيبراني للدول الأعضاء.
- العمل على وضع الأطر والخطط في مجال الأمن السيبراني، من خلال إجراء الدراسات الإقليمية وعقد ورش العمل، ورفع مستوى الوعي والخبرات في الأمن السيبراني في قطاع البنى التحتية للمعلومات.

وتتلخص مهامه فيما يلي:

- تطوير استراتيجية وحوكمة الأمن السيبراني، من خلال العمل جنباً إلى جنب مع القطاعين العام والخاص من أجل تطوير استراتيجيات الأمن السيبراني الوطني مع وجود مسؤوليات واضحة.
- ضمان التوافقية وتقنيات الأمن السيبراني، والتي تهدف إلى تقديم التدابير التقنية وتدابير الالتزام بالمعايير.
- بناء القدرات في الأمن السيبراني وتطوير حلول وبرامجية فاعلة.
- إدارة الحوادث السيبرانية، من خلال إنشاء فرق وطنية للاستجابة للطوارئ والحوادث الأمنية، حيث تأخذ هذه الفرق مسؤولية وطنية لتكون مركزاً

موثوقاً لتنسيق جهود الأمن السيبراني، كما تساعد هذه الخدمة على تقييم مقدّرات فرق الاستجابة للحوادث الأمنية في الحكومات والقطاع العام، وتحديد الثغرات وتقديم خارطة الطريق لتحسين هذه الفرق.

٣. مركز الدفاع الإلكتروني:

يعتبر مركز الدفاع الإلكتروني[٦] جهة مختصة ومسؤولة عن الدفاع الإلكتروني في السلطنة، والمرجع الوطني لحماية المصالح الحيوية في الفضاء الإلكتروني، والمشرف على بناء القدرات الوطنية المتخصصة في مجال الأمن الإلكتروني.

ويهدف المركز إلى تحقيق ما يلي:

١ ـ تعزيز قدرة الجهات المعنية، والأفراد في التصدي للتهديدات الإلكترونية.

٢ ـ بناء القدرات الوطنية المتخصصة في مجال الأمن الإلكتروني عبر خلق شراكات بين القطاعات المعنية محلياً، ودولياً.

أهم اختصاصاته ما يلي :

١ ـ إعداد الاستراتيجية وآليات تنفيذها، واقتراح تعديلها، والتحقق من تنفيذها بعد اعتمادها من المجلس.

٢ ـ وضع الإطار التنظيمي والقانوني، وآليات الحوكمة لتطبيق الاستراتيجية.

٣ ـ إعداد الخطة الوطنية لمواجهة الأخطار والتهديدات المتعلّقة بالأمن الإلكتروني، ومتابعة الالتزام بها بعد اعتمادها من اللجنة، ورفع مقترحات تعديلها.

٤ ـ إعداد تصنيف وتحديد للبنى الأساسية للأمن الإلكتروني والجهات المرتبطة بها، وتحديد القطاعات والجهات ذات الصلة بالأمن الإلكتروني.

٥ ـ وضع الشروط أو الخصائص أو المعايير الوظيفية أو المواصفات الفنية لأي أجهزة أو أنظمة مرتبطة بمجال الأمن الإلكتروني، والموافقة على استعمالها أو استيرادها أو تداولها في السلطنة.

٦ ـ متابعة تنفيذ الجهات المعنية للاستراتيجية، ومعايير وسياسات الأمن الإلكتروني الصادرة عن المركز.

٧ ـ التدخل التقني المباشر متى ما دعت الضرورة للتصدي لحوادث الأمن الإلكتروني التي تتعرّض لها الجهات المعنية، ويجوز للمركز في سبيل ذلك السماح بالاستعانة بالشركات المعتمدة لتقديم خدمات الأمن الإلكتروني.

٨ ـ وضع الضوابط اللازمة لمنع أي محاولات لإعاقة أو تعطيل أو تخريب شبكات الاتصالات ونظم المعلومات في السلطنة، واتخاذ ما يلزم للتعامل مع شتى أنواع التهديدات الإلكترونية، سواء كانت من داخل السلطنة، أو خارجها.

٩ ـ مراقبة شبكات الجهات المعنية، والتحقيق في أي تهديدات إلكترونية، ويجوز للمركز ـ بعد أخذ موافقة رئيس اللجنة ـ عزلها إن اقتضت الحاجة في حال عدم التقيد بمعايير الأمن الإلكتروني بما يكفل التصدي لأي تهديدات قد تلحق ضرراً بمنظومة الأمن الوطني، أو اقتصاد السلطنة، أو علاقاتها الدولية والإقليمية.

١٠ ـ تقديم المساندة للجهات المختصة، من خلال الاستدلال، والتحقيق في الجرائم المتعلّقة بالأمن الإلكتروني.

١١ ـ إبداء الرأي التقني في الموضوعات المتعلّقة بالأمن الإلكتروني.

١٢ ـ القيام بالفحص الأمني، والتدقيق على الجهات المعنية متى ما اقتضت الحاجة التأكد من التزامها بالمعايير والسياسات التي يصدرها المركز.

١٣ ـ التنسيق، والتعاون مع الجهات ذات العلاقة للعمل وفق بنود إطار الحوكمة الوطنية للدفاع الإلكتروني.

١٤ ـ تنظيم عمل الخبراء، والاستشاريين، والمقاولين وغيرهم، ممن يقدمون خدمات الأمن الإلكتروني، وإعداد سجل يُقيَّد فيه المستوفون للمعايير الأمنية.

١٥ ـ إعداد ودعم الدراسات والبرامج والبحوث العلمية اللازمة لتطوير منظومة الأمن الإلكتروني في السلطنة بالتنسيق مع المؤسسات الأكاديمية والمهنية داخل السلطنة، أو خارجها.

١٦ ـ متابعة تنفيذ الالتزامات الناشئة عن الاتفاقيات الدولية في مجال الأمن الإلكتروني ـ إن وجدت ـ التي تكون السلطنة طرفاً فيها، والقرارات الصادرة من المنظمات الدولية والإقليمية المنضمة إليها السلطنة، وذلك بالتنسيق مع الجهات المعنية.

١٧ ـ دراسة التشريعات ذات الصلة بالأمن الإلكتروني، واقتراح التعديلات المناسبة بشأنها، وذلك بالتنسيق مع الجهات المختصة.

١٨ ـ إعداد التقارير الدورية، والسنوية بشأن تنفيذ الاستراتيجية، وغيرها من الأعمال المرتبطة بمجال الأمن الإلكتروني، ورفعها إلى المجلس.

١٩ ـ إبلاغ ورفع تقارير دورية إلى المجلس حول قضايا الأمن الإلكتروني ذات البُعد الوطني.

٢٠ ـ تبادل المعلومات في مجال الأمن الإلكتروني مع المراكز النظيرة المحلية أو الدولية.

٢١ ـ تمثيل السلطنة بالاشتراك والتنسيق مع الجهات الأخرى ذات العلاقة في المنظمات والمؤتمرات واللجان والاتحادات والاجتماعات الإقليمية والدولية ذات الصلة بالأمن الإلكتروني.

٢٢ ـ أي مهام أو اختصاصات أخرى يعهد بها إلى المركز بموجب القوانين، والمراسيم السلطانية.

علاوة على ذلك، فقد تم اختيار سلطنة عُمان لاستضافة أول مركز إقليمي للأمن السيبراني تابع للوكالة المتخصصة بتكنولوجيا المعلومات والاتصالات التابعة للأمم المتحدة ـ الاتحاد الدولي للاتصالات ـ بهدف تهيئة بيئة أكثر أماناً وتعاوناً للأمن السيبراني في المنطقة العربية، وتعزيز دور الاتحاد الدولي للاتصالات في بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات في المنطقة، كما وقع الاختيار على سلطنة عُمان لتولي رئاسة مجلس فريق الاستجابة للطوارئ الحاسوبية بمنظمة التعاون الإسلامي المعروف (OIC-CERT) وتعد المنظمة ثاني أكبر منظمة بعد

الأمم المتحدة، إذ تضم في عضويتها ٥٧ دولة فضلاً عن تمتعها بصفة المراقب في الأمم المتحدة، كما أنها تشارك في عضوية العديد من المنظمات الإقليمية والدولية، بما في ذلك المنتدى العالمي الرائد لفرق الأمن والاستجابة لحوادث الحاسوب، وفريق الاستجابة للطوارئ الحاسوبية بمنظمة التعاون الإسلامي، والفريق الوطني للاستجابة لطوارئ الحاسب الآلي بمجلس التعاون الخليجي، ومجموعة عمل مكافحة التصيد الاحتيالي، ومنظمة Malware Alliance Organization، ومشروع Honey Net.، ومبادرة Cyber Green العالمية، وغيرها الكثير، إلى جانب تعزيز التعاون والمشاركات في مبادرات الأمن السيبراني مع المنظمات الدولية بما في ذلك الاتحاد الدولي للاتصالات واللجنة الاقتصادية والاجتماعية لغربي آسيا، ومعهد الأمم المتحدة لبحوث نزع السلاح، ومعهد تشاتام هاوس.

(٣) ـ أنشطة مملكة البحرين في مجال الأمن السيبراني:

يُعد الأمن السيبراني ركيزة أساسية للإطار الوطني لتكنولوجيا المعلومات والاتصالات في مملكة البحرين، تحكمه إدارات متنوّعة أهمها هيئة المعلومات والحكومة الإلكترونية، وهيئة تنظيم الاتصالات، وإنترنت آمن، وهيئة حماية البيانات الشخصية، وغيرها من قطاعات جعلت هذا المجال من أولوياتها، حيث تلتزم مملكة البحرين بحماية مصالحها في الفضاء السيبراني من خلال أنشطة ومهام كانت ركيزة لانطلاقها في هذا الفضاء بأمان وحماية أهمها:

- إطلاق الاستراتيجية الوطنية للأمن السيبراني.

- إطلاق تشريعات الجرائم الإلكترونية.
- منع الهجمات الإلكترونية من خلال استخدام آليات وبرامج متطورة.

*** الاستراتيجية الوطنية للأمن السيبراني :**

تسعى الاستراتيجية الوطنية للأمن السيبراني إلى خلق فضاء إلكتروني آمن لحماية المصالح الوطنية، وحماية مملكة البحرين من التهديدات السيبرانية لتقليل الأخطار؛ ومن أهم أهدافها ما يلي:

- حماية البنية التحتية الوطنية الحساسة، من خلال حماية المنظمات التي تقدّم الخدمات الأساسية للأمة مثل: النفط والكهرباء والمياه والخدمات الحكومية والمالية.
- الاستجابة بشكل حاسم للتهديدات السيبرانية، من خلال إنشاء نهج شامل للحوادث التي تواجه كلاً من القطاعين العام والخاص.
- إنشاء إطار تشريعي وتنظيمي، من خلال تطوير قانون إلكتروني يتبع المعايير الدولية لمكافحة الإجرام الإلكتروني.
- تطوير نظام بيئي حيوي للأمن السيبراني، وذلك من أجل ضمان مصدر دائم للخبرة والحلول لدعم خطط البنية التحتية المرنة والفضاء السيبراني الأكثر أمانًا.
- إنشاء فضاء إلكتروني أكثر أمانًا للحفاظ على ثقة المواطنين في الأنظمة الإلكترونية، وبالتالي تشجيع الاستخدام العام للخدمات الإلكترونية.

- التعاون الدولي، من خلال إقامة تعاون دولي لمواجهة التهديدات السيبرانية، وتكييف مبادرات بناء القدرات، وتسهيل التبادلات بشأن القوانين واللوائح السيبرانية.

*** تشريعات الجرائم الإلكترونية :**

أصدرت حكومة مملكة البحرين العديد من القوانين والتشريعات المتعلّقة بالأمن السيبراني وحماية البيانات الشخصية لدعم الإطار الوطني للأمن السيبراني(٧)، أهمها:

- القانون رقم ٣٠ لسنة ٢٠١٨ بشأن إصدار قانون حماية البيانات الشخصية.
- القانون رقم ١٦ لسنة ٢٠١٤ بشأن حماية المعلومات ووثائق الدولة.
- القانون رقم ٢ لسنة ٢٠١٧ بشأن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.
- قانون رقم ٦٠ لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات.
- المرسوم بقانون رقم (٥٤) لسنة ٢٠١٨ بشأن إصدار الخطابات والمعاملات الإلكترونية.
- قرار رئيس مجلس الوزراء رقم ٣٦ لسنة ٢٠١٨ بشأن تنظيم الاشتراطات الفنية لإرسال واستلام وتحديث السجلات والتوقيعات الإلكترونية للهيئات العامة.

*** منع الهجمات الإلكترونية :**

ولتحقيق هدفها في خلق فضاء آمن، ارتأت مملكة البحرين إطلاق مبادرات وبرامج ومشاريع هدفها معالجة هذه الأخطار من أجل تحسين الجاهزية وأمن المعلومات في الجهات الحكومية والبحرين بشكل عام، وأهمها:

- برنامج Cyber Trust: هو برنامج تنافسي بطبيعته ويهدف إلى رفع مستوى أمن المعلومات من خلال الحوكمة ودعم الجوانب الفنية لتحقيق الريادة الإقليمية والعالمية واستدامة بيئة إلكترونية حكومية موثوقة للجهات الحكومية.
- صقور الأمن: هي مبادرة تجمع مجموعة من المتخصصين في الأمن السيبراني من مختلف الجهات الحكومية في البحرين، وتهدف إلى التواصل والتعاون المستمر بشأن قضايا الأمن السيبراني، واكتشاف أي تهديدات للأمن السيبراني والتخفيف من حدتها.
- خدمة الاستشارات المتعلقة بالتهديدات: الاستشارات الخاصة بالتهديدات هي وثيقة يقدمها الفريق التابع لحكومة البحرين لتزويد العملاء بتفاصيل حول البرامج الضارة والتهديدات الجديدة مع التوصيات، والمستند مدعوم برسوم بيانية لتوضيح وتلخيص تفاصيل التهديد.
- إنترنت آمن (Safe Surf): مبادرة أطلقتها هيئة تنظيم الاتصالات مكرّسة لتمكين المواطنين والمقيمين في البحرين وعائلاتهم بالمعرفة والمعلومات من أجل بيئة إلكترونية أكثر أمانًا.

- وجود منظومة واضحة لحوكمة الأمن السيبراني أو الأمن الإلكتروني متمثلة بالإدارة العامة لمكافحة الفساد والأمن الاقتصادي والإلكتروني والمركز الوطني للأمن الإلكتروني التابعين لوزارة الداخلية.

كما أن هناك جهات ساهمت في تعزيز الأمن السيبراني وأهمها:

أ- المركز الوطني للأمن السيبراني:

من أهم مهام المركز الوطني للأمن السيبراني[٨] السعي إلى توفير فضاء إلكتروني آمن في مملكة البحرين عن طريق وضع معايير الحوكمة الفعَّالة لتنفيذها، وتوفير وسائل الدفاع والمراقبة والاستجابة للهجمات الإلكترونية، فضلاً عن نشر الوعي بين الأفراد والمؤسسات في إطار تحقيق الرؤية الاقتصادية ٢٠٣٠، والمساهمة في تعزيز أهداف التنمية المستدامة.

وتتلخّص أهم اختصاصات ومهام المركز فيما يلي:

١ ـ إعداد الاستراتيجية الوطنية للأمن السيبراني والإشراف على تنفيذها، وقد تضمنت الاستراتيجية خمس ركائز وهي: حماية سيبرانية قوية ومرنة، والحوكمة والمعايير الفعّالة للأمن السيبراني، وبناء مجتمع واعٍ بالأمن السيبراني، وتعزيز الحماية من خلال الشراكات والتعاون، وتطوير الكوادر الوطنية.

٢ ـ تحديد القطاعات الحيوية في مجال الأمن السيبراني في المملكة والجهات المنضوية تحتها.

٣ ـ وضع السياسات والمعايير والضوابط والمتطلبات والتعليمات والإجراءات اللازمة؛ لتوفير الحماية السيبرانية على المستوى الوطني من التهديدات والأخطار والحوادث السيبرانية.

٤ ـ وضع أطر وآليات إدارة الأخطار السيبرانية ومتابعة الالتزام بها وتحديثها.

٥ ـ وضع أطر وآليات الاستجابة الوطنية للحوادث السيبرانية على المستوى الوطني وتنفيذها بالتنسيق مع الجهات المعنية.

٦ ـ تنظيم عمليات تدقيق وتقييم الجهات في مجال الأمن السيبراني على المستوى الوطني.

٧ ـ إدارة منصة وطنية موحّدة لرصد التهديدات والأخطار والحوادث السيبرانية، وتحليلها والاستجابة لها واحتوائها في القطاعات الحيوية، وإشعار الجهات المعنية بالأخطار والتهديدات السيبرانية.

٨ ـ تنظيم آلية وضوابط مشاركة المعلومات والبيانات ذات الصلة بالأمن السيبراني بين جهات القطاعات الحيوية، والإشراف على ذلك.

٩ ـ نشر الوعي بالأمن السيبراني بما يساهم في خلق بيئة إلكترونية آمنة.

١٠ ـ بناء القدرات الوطنية في مجال الأمن السيبراني، والمشاركة في إعداد وتوفير برامج تدريبية وتطويرية في الأمن السيبراني بالتنسيق مع الجهات ذات العلاقة، ووضع المعايير المهنية لكوادر الأمن السيبراني والمقاييس والاختبارات القياسية.

١١ ـ اعتماد المؤشرات والقياسات الوطنية للأمن السيبراني في المملكة.

١٢ ـ إعداد التقارير الدورية لتحديد مستوى الأمن السيبراني في المملكة وقطاعاتها الحيوية.

١٣ ـ اقتراح وإبداء الرأي في مشروعات القوانين واللوائح والقرارات المتعلّقة بالأمن السيبراني.

١٤ ـ التعاون والتنسيق مع الدول والمنظمات والهيئات والاتحادات الدولية والإقليمية المتخصصة في الأمن السيبراني.

١٥ ـ تمثيل المملكة في المؤتمرات والاجتماعات والمحافل الإقليمية والدولية ذات الاختصاص في الأمن السيبراني، ومتابعة تنفيذ التزامات المملكة الدولية الخاصة بالأمن السيبراني.

١٦ ـ تبادل الخبرات والتجارب والمعرفة محليًا ودوليًا.

١٧ ـ تعزيز الدراسات والبحوث والتطوير في مجال الأمن السيبراني.

ب. الإدارة العامة لمكافحة الفساد والأمن الاقتصادي والإلكتروني:

استمراراً للجهود المبذولة لسعي مملكة البحرين للحد من الجرائم الإلكترونية وحماية المجتمع من الآثار السلبية لهذه الآفة، تم إنشاء الإدارة العامة لمكافحة الفساد والأمن الاقتصادي والإلكتروني[٩] في ٢٨ من نوفمبر لعام ٢٠١١م بمرسوم رقم (١٠٩) للعام ٢٠١١ بتعديل بعض أحكام المرسوم رقم (٦٩) للعام ٢٠٠٤، والتي تختص بمكافحة جميع الجرائم الإلكترونية بجميع أنواعها والكشف عنها وتعقبها، وذلك لما تشكّله من

خطورة على أمن الفرد والمجتمع، بالإضافة إلى التدريب المستمر للكوادر الفنية وعقد الندوات والمؤتمرات المتخصصة وإقامة الدورات وورش العمل في مجال مكافحة الجرائم، وتختزل أولويات الإدارة فيما يلي:

- الحد من جرائم الشبكة العنكبوتية من خلال العمل على الوقاية من هذه الجرائم.
- تنفيذ الاستراتيجيات في مجال مكافحة جرائم الحاسوب في مملكة البحرين.
- حل المسائل القانونية والتحقيق في الجرائم الإلكترونية وإحالة القضايا للنيابة العامة.
- وضع الاقتراحات التشريعية، والشروع والمشاركة في الجهود الدولية لمكافحة الجريمة الحاسوبية.

ج. إنترنت أمن البحرين:

إنترنت أمن البحرين[١٠] هي مبادرة من هيئة تنظيم الاتصالات في مملكة البحرين لتمكين المواطنين والمقيمين في البحرين بالمعرفة والمعلومات ومن أجل بيئة إنترنت أكثر أماناً، من خلال إطلاق أنشطة توعوية متنوّعة، تساهم بشكل مباشر في خلق ثقافة رقمية آمنة لدى جميع أفراد المجتمع، ومن أهم أنشطتهم:

- إقامة معارض التوعية.
- إقامة ندوات توعوية.
- إقامة أنشطة اجتماعية متنوّعة توعوية.

د . هيئة حماية البيانات الشخصية:

أصدر المشرّع البحريني القانون رقم ٣٠ لسنة ٢٠١٨ بتاريخ ١٩ يوليو ٢٠١٨ هيئة حماية البيانات الشخصية[١١]، والذي تناول فيه موضوع حماية البيانات الشخصية الذي يعنى بحماية الأفراد والبيانات الشخصية العائدة لهم عن طريق وضع إطار قانوني يحدّد طرق وسبل الولوج إلى البيانات والحصول عليها ومعالجتها بطريقة فعّالة، وتمنح الأفراد الثقة في كل ما يتعلّق ببياناتهم التي في حوزة الشركات والمؤسسات، ولكي تتم إدارتها بشكل دقيق وحديث وآمن لضمان حماية بيانات الأفراد الشخصية، ومنع الأطراف الأخرى لمعالجة بياناتهم بطريقة غير مشروعة ومنصفة، وكفل لهم سبل المحافظة على حقوقهم في هذا الشأن، من خلال التالي:

- حماية أية معلومات سواء أكانت صورة تخصُّ فردًا مُعرَّفًا، أم قابلاً بطريق مباشر أم غير مباشر لأن يُعرَّف، وتعتبر بيانات شخصية طبقًا للقانون، وبذلك فإن أي بيان يكون من شأنه التعرف إلى هوية شخص ما، كاسم الشخص أو رقم هويته أو رقم جواز السفر أو الهاتف أو رقم العضوية في أي مؤسسة، أو صورته الشخصية أو صور المستندات المتعلّقة بشخصه أو وظيفته، أو معلوماته المصرفية، أو بريده الإلكتروني، يدخل في نطاق البيانات الشخصية المحمية بموجب القانون؛ بالإضافة إلى أن كل من يقرر طريقة الحصول على البيانات الشخصية وطريقة التصرف فيها – وهو ما يُعرف قانونًا بمعالجة البيانات – يعتبر مديرًا للبيانات وتقع على عاتقه مسؤولية الالتزام بتطبيق الشروط القانونية للحصول على البيانات

والتصرف فيها، وبذلك تلتزم كل مؤسسة أو شركة أو جهة تحصل من خلال تعاملها على معلومات شخصية لعملائها وتقرر طريقة معالجتها بالمعايير المقررة قانونًا لحماية البيانات الشخصية.

- أعطى القانون صاحب البيانات الحق في معرفة ما إذا كانت جهة معينة تعالج بياناته الشخصية، وفرض القانون على هذه الجهة أن تجيب عن كل استيضاح أو سؤال من صاحب البيانات لبيان ما إذا كانت هذه الجهة تقوم بمعالجة بياناته الشخصية وبيان الهدف من هذه المعالجة والجهات التي تسلمتها.
- إعطاء صاحب البيانات الحق في أن يطلب من هذه الجهة تصحيح أو حَجْب أو مسح البيانات الشخصية الخاصة به بحسب الظروف والأحوال والمقتضيات، إذا كان من شأن معالجتها أن يلحق به أو بسواه ضررًا غير مبرر وغير يسير، مهما كان نوع هذا الضرر ماديًا كان أو معنويًا.
- إعطاء صاحب البيانات الحق في الاعتراض على التسويق المباشر، وهو التسويق الذي يتم عن طريق توجيه مادة إعلانية أو دعاية إلى شخص محدَّد، كالإعلانات التي ترسل عن طريق الرسائل النصية أو البريد الإلكتروني، وأوجب القانون على أي جهة أن تتوقف عن هذه المعالجة في حال تسلمها طلبًا بذلك من قِبل صاحب البيانات.
- أتاح القانون لكل ذي مصلحة أو صفة أنْ يتقدّم إلى الهيئة بشكوى، إذا كان لديه ما يحمله على الاعتقاد بوقوع أية مخالفة لأحكام هذا القانون أو بأن شخصًا ما يقوم بمعالجة بياناته الشخصية خلافًا لأحكام القانون.

كذلك شاركت جهات الدولة المختلفة في مملكة البحرين في عملية الحماية وخلق دروع مؤسسة آمنة لحماية المستخدمين مثل:

- **هيئة المعلومات والحكومة الإلكترونية**[١٢]، من خلال وضع السياسات الرقمية الوطنية والتي تنظم إتمام المعاملات الرقمية بصورة آمنة وأهم تلك السياسات هي: سياسات الحكومة الرقمية، وسياسات المشاركة الإلكترونية، وسياسات البيانات المفتوحة، وسياسات الخدمات السحابية.
- **وزارة الاعلام**، من خلال إطلاق الدليل الاسترشادي لاستخدام شبكات التواصل الاجتماعي في الجهات الحكومية.
- **مصرف البحرين المركزي**[١٣]، من خلال إصدار لوائح إرشادات الأمن السيبراني للقطاعات المصرفية للحد من الاحتيالات المالية والهجمات الإلكترونية.

(٤) ـ أنشطة دولة الإمارات العربية المتحدة في مجال الأمن السيبراني:

أصبح الاهتمام بالأمن السيبراني في دولة الإمارات العربية المتحدة من أولويات الدولة، وركيزة مهمة في استراتيجية الأمن الوطني للدولة، وأحد أهم مشاريعها الحالية والمستقبلية، لذلك فإن دولة الإمارات العربية المتحدة تستثمر بشكل كبير في الأمن السيبراني من خلال استخدام التقنيات المتطورة لحماية أصول المعلومات، ومحاربة مجرمي الإنترنت وحماية

خصوصية مواطنيها وبنيتها التحتية والمرافق المهمة، لذا خصصت مراكز وهيئات متخصصة تختص وتتابع هذا الملف المهم والحساس وأهمها:

- مجلس الأمن السيبراني.
- هيئة أبو ظبي الرقمية.
- مركز دبي للأمن الإلكتروني.
- هيئة تنظيم الاتصالات والحكومة الرقمية.

أ- مجلس الأمن السيبراني:

يهدف مجلس الأمن السيبراني[١٤] إلى اقتراح سياسات وتشريعات لتعزيز الأمن السيبراني في الدولة للقطاعات المستهدفة كافة، ورفعها إلى مجلس الوزراء لاعتمادها وتنفيذها بالتنسيق مع الجهات المعنية، ورفع جاهزية القطاعات كافة للاستجابة والتصدي للهجمات الطارئة بكفاءة واحترافية عالية، مما يعزّز مسيرة الإمارات الرائدة نحو مستقبل رقمي فائق التطور، وخلق بيئة سيبرانية آمنة وصلبة، كما يعمل المجلس على تجسيد الرؤية الاستشرافية للقيادة الرشيدة والنهج الاستباقي للدولة، من خلال جهات متخصصة وفاعلة قادرة على توفير الحماية الرقمية، وتأمين البنية التحتية المتطورة بما يضمن استمرارية الأعمال وتقديم الخدمات بشكل منتظم في الأنشطة الاقتصادية والتعليمية والصحية والاجتماعية، ونشر الثقافة السيبرانية من خلال مبادرات موجّهة إلى مختلف الشرائح، وحماية المجتمع من حالات الاختراق والدخول غير المشروع، ويعمل المجلس ضمن استراتيجية تتكون من خمسة محاور رئيسة؛ هي:

- **المحور الأول**: الاستراتيجية في بناء القدرات، والسياسات، والحوكمة، وتأهيل وبناء القدرات الشخصية، والبرامج والمناهج والجامعات، وبناء القدرات التقنية مع الشركاء الاستراتيجيين.
- **المحور الثاني**: الحماية والدفاع من خلال توظيف هذه القدرات.
- **المحور الثالث**: التوعية ونشر ثقافة الأمن السيبراني.
- **المحور الرابع**: يتمثّل في الاستجابة اللازمة للحوادث السيبرانية من قِبل الجهات المختصة.
- **المحور الخامس**: التعاون على جميع المستويات بدءاً من المحيط الخليجي والعربي والعالمي وفق مقررات الأمم المتحدة لمراكز الاستجابة وفرق الاستجابة للطوارئ المعلوماتية.

أهم اختصاصاته ما يلي:

- إعداد وتطوير وتحديث الاستراتيجية الوطنية للأمن السيبراني في المنطقة.
- اقتراح وإعداد التشريعات والسياسات والمعايير لتعزيز الأمن السيبراني لجميع القطاعات الحيوية المستهدفة في الدولة.
- اقتراح وإعداد الخطة الوطنية الكاملة للاستراتيجية السيبرانية بما في ذلك الهجمات والتهديدات، مع تقييم جاهزيتها.

- تطوير الإطار العام والآلية التي يتم من خلالها تبادل وتشارك وإدارة المعلومات المتعلّقة بالأمن السيبراني بين الجهات والقطاعات محلياً ودولياً، بالتنسيق والتعاون مع السلطات ذات الصلة.
- تطوير المعايير والمتطلبات المرتبطة بتطابق الأمن السيبراني في أنظمة وقدرات الحكومة الرقمية، والشبكات، والبنية التحتية الرقمية، والتي من خلالها يتم الاستعداد لحجب الأخطار والتهديدات وردعها، وسيتم تعزيزها بالتنسيق والتعاون مع السلطات والهيئات ذات الصلة.
- اقتراح وإعداد المعايير والضوابط لإنشاء مركز عمليات وطني للأمن السيبراني بجميع أنواعه، حيث يشمل مركز التحكم والاستطلاع والمراقبة وتبادل وتحليل المعلومات.
- اقتراح المعايير وإجراءات الرقابة المتعلّقة باستيراد وتصدير واستخدام المعدّات والأجهزة والبرمجيات العالية الحساسية للأمن السيبراني، بالتعاون مع السلطات والهيئات ذات الصلة.
- وضع الخطط اللازمة لبناء مواهب وقدرات الدولة في مجالات الأمن السيبراني، بالتنسيق مع السلطات والهيئات ذات الصلة، والعمل على رفع الوعي والمشاركة المجتمعية.
- اقتراح وتنفيذ الدراسات والبحوث اللازمة للتطوير في مجالات الأمن السيبراني بالتنسيق مع الهيئات والسلطات ذات الصلة.

- مجلس الأمن السيبراني مكلّف بضمان الامتثال لسياسات المكان والأطر والمبادئ التوجيهية، بعد ذلك، تقديم التقرير نصف السنوي عن وضع الهيئات في جميع أنحاء الإمارات العربية المتحدة إلى مجلس الوزراء للمراجعة.

ب - هيئة أبوظبي الرقمية:

تعمل هيئة أبوظبي الرقمية على دعم مسيرة التحول الرقمي في جميع الجهات الحكومية عبر البرامج الرقمية المُبتكرة والشراكات العالمية والمحلية، بالإضافة إلى دعم التحول الرقمي لأبوظبي عبر الاستراتيجيات والسياسات والمعايير وتطوير البنى الهيكلية المؤسسية الرقمية من أجل تعزيز فاعلية الأداء الحكومي، كما تقدّم خدمات ومنصات وقنوات رقمية بالاستعانة بتقنيات الذكاء الاصطناعي والحلول الحكومية المشتركة، وتوفير حلول الأمن السيبراني للجهات الحكومية؛ حيث تتمحور رؤية الهيئة حول قيادة المستقبل الرقمي لإمارة أبوظبي من خلال أربعة محاور، وهي:

- الاستباقية: تقديم تطبيقات تكنولوجية متطورة تتيح للمتعاملين الحصول على بيانات موثوقة.
- التخصص: توفير منصات وقنوات متكاملة للخدمات الحكومية بشكل سلس وسريع يناسب احتياجات المتعاملين.
- التكامل: تقديم مبادرات مشتركة تعزّز كفاءة الخدمات الحكومية بشكل مبتكر ومتكامل.

- الأمن السيبراني: توفير حلول أمنية تضمن حماية البنية التحتية والبيانات والأنظمة الرقمية الخاصة بالمتعاملين.

ج - مركز دبي للأمن الإلكتروني:

يهدف مركز دبي للأمن الإلكتروني[١٥] إلى حماية المعلومات وشبكة الاتصالات وأنظمة المعلومات الحكومية، ويعمل على تطوير وتعديل واستخدام الوسائل اللازمة في مجال الأمن الإلكتروني، ورفع كفاءة طرق حفظ المعلومات وتبادلها لدى الجهات الحكومية في الإمارة. ويختص المركز بوضع سياسة الإمارة في مجال أمن المعلومات الحكومية وتنفيذها، ووضع المعايير الكفيلة بتوفير الأمن الإلكتروني، وإعداد خطة استراتيجية لمواجهة أية أخطار على المعلومات الحكومية بالتنسيق مع الجهات كافة، والتأكد من فعالية أنظمة أمن شبكة الاتصالات وأنظمة المعلومات لدى الجهات الحكومية.

ومن أهم أهداف المركز ما يلي:

- الحماية: حماية المعلومات وشبكة الاتصالات وأنظمة المعلومات الحكومية في الإمارة.
- التطوير: تطوير وتعديل واستخدام الوسائل اللازمة في مجال الأمن الإلكتروني.
- الكفاءة: رفع كفاءة طرق حفظ المعلومات وتبادلها لدى الجهات الحكومية في الإمارة.

- ومن أهم خدمات المركز ما يلي:
- خدمات الثقة الرقمية.
- الاستراتيجيات والسياسات والقوانين الأمنية.
- الامتثال وتطبيق معايير أمن المعلومات.
- تقديم الاستشارات الأمنية.
- التوعية والتعليم.
- الاستجابة للأحداث.
- اختبار قابلية الاختراق.
- إصدار التراخيص.
- مؤشر مستوى أمن الشبكات.

د - هيئة تنظيم الاتصالات والحكومة الرقمية:

يتمحور دور هيئة تنظيم الاتصالات والحكومة الرقمية[١٦] في مجالين هما: تنظيم قطاع الاتصالات، وتمكين الجهات الحكومية في مجال التحول الرقمي؛ من أجل تمكين وتنظيم قطاع الاتصالات والحكومة الرقمية لتقديم خدمات ذكية تمتاز بالكفاءة والاستدامة، وتعمل على تطوير منظومة متكاملة تشمل بيئة تنظيمية لقطاع الاتصالات والمعلومات تحمي مصالح المستخدمين، وبنية تحتية رقمية متكاملة تسهم في تقديم خدمات حكومية استباقية ومرنة، وتعزّز التنافسية والاستدامة وجودة الحياة، وتهدف هيئة

تنظيم الاتصالات كذلك إلى التنفيذ المستمر للمبادرات الرامية نحو تحقيق مزيد من التعاون بين القطاعين العام والخاص لضمان استعدادهما بشكل مناسب لمواجهة تهديدات الأمن السيبراني المتزايدة، واستدامة خدمات تقنية المعلومات والاتصالات وتوفيرها بشكل آمن يدعم بشكل أساسي تحقيق اقتصاد رقمي قوي.

ويُشار إلى أن دولة الإمارات تمتلك سجلاً حافلاً بالإنجازات في مجال الأمن السيبراني، حيث تم الإشارة إلى أكثر من جهة متخصصة في مجال الأمن السيبراني (تم ذكرهم سابقاً)، وتنفيذ شبكة إلكترونية اتحادية، وإنشاء السحابة الوطنية، وشهادة المواطنة الرقمية، وإطلاق استراتيجيات الأمن السيبراني والإلكتروني، بالإضافة إلى المبادرات المستمرة ومن أهمها إطلاق مبادرات في السلامة الإلكترونية، ومبادرة النبض السيبراني التي تشمل مجموعة من الفعاليات والأنشطة، منها التدريب الذي يهدف إلى تمكين القيادات والكوادر النسائية الوطنية والطلاب، وغيرهم في مجال الأمن السيبراني، من خلال برامج تدريبية مخصصة تسهم في نشر الثقافة الرقمية وكيفية التصدي باحترافية للهجمات الإلكترونية الخبيثة.

(٥) ـ أنشطة دولة قطر في مجال الأمن السيبراني:

تتبوأ دولة قطر مكانة ريادية في مجال الأمن السيبراني، حيث تتبنى سلسلة من الإجراءات والاستراتيجيات لحماية أنظمتها الرقمية ومواطنيها من التهديدات السيبرانية المتزايدة، وتعكس جهود قطر

في هذا المجال التزامها الراسخ بتحقيق مجتمع رقمي آمن ومتقدم من خلال إطلاق وكالة تُسمى «الوكالة الوطنية للأمن السيبراني» بقرار أميري رقم (١) لسنة ٢٠٢١ وتتبع رئيس مجلس الوزراء، كبادرة على جدية اهتمام الدولة وأولوياتها؛ لقيام دولة تواكب تطورات وطفرات التكنولوجيا العالمية، إلى جانب جهود قطر في مجال الأمن السيبراني، وتحديث السياسات والإجراءات بشكل دوري لتعزيز فعالية الحماية الرقمية، وتركز الحكومة على تطوير البنية التحتية السيبرانية للتصدي للهجمات المتطورة، مع التركيز على استخدام تكنولوجيا حديثة لمراقبة وحماية الأنظمة الرقمية، بالإضافة إلى تبني الدولة أيضاً استراتيجية شاملة لتعزيز الوعي الرقمي بين المواطنين والشركات، وتعتبر جهود قطر في تحقيق الحماية والدفاع لمنظومتها الرقمية نموذجاً للتّفاني والابتكار في مجال التكنولوجيا الرقمية، وبفضل هذه الجهود، تظل قطر في موقع قوي لمواجهة التحديات السيبرانية المستقبلية وتحقيق تقدم مستدام في عالم متسارع التطور تكنولوجياً.

* الوكالة الوطنية للأمن السيبراني :

تهدف الوكالة الوطنية للأمن السيبراني[١٧] إلى المحافظة على الأمن الوطني السيبراني وتنظيمه، وتعزيز المصالح الحيوية للدولة وحمايتها في مواجهة تهديدات الفضاء السيبراني، ويكون لها في سبيل تحقيق ذلك ممارسة الاختصاصات والصلاحيات كافة، وبوجه خاص ما يلي:

١ ـ إعداد الاستراتيجية الوطنية للأمن السيبراني وتحديثها بالتنسيق مع الجهات المعنية، والإشراف على تنفيذها.

٢ ـ وضع وتحديث السياسات وآليات الحوكمة والمعايير والضوابط والإرشادات اللازمة لتعزيز الأمن السيبراني بالتنسيق مع الجهات المعنية وتعميمها على الجهات ذات العلاقة ومتابعة الالتزام بها.

٣ ـ وضع وتحديث أطر إدارة الأخطار السيبرانية، ومتابعة الالتزام بها.

٤ ـ تقييم الوضع الأمني السيبراني في الدولة، بالتنسيق مع الجهات المعنية، لرصد الأخطار بصفة استباقية.

٥ ـ إعداد التقارير عن الحالة الأمنية السيبرانية محلياً وإقليمياً ودولياً.

٦ ـ تحديد وتصنيف مؤسسات القطاعات الحيوية في الدولة.

٧ ـ إعداد وتنفيذ الخطة الوطنية للاستجابة والتعافي من الحوادث والهجمات السيبرانية بالتنسيق مع الجهات المعنية.

٨ ـ الإشراف على خطط الطوارئ وضمان استمرارية الأعمال المتعلّقة بالأمن السيبراني لمؤسسات القطاعات الحيوية.

٩ ـ وضع آليات لتبادل ومشاركة ونشر ورصد واستطلاع وتحليل المعلومات المتعلّقة بالأمن السيبراني مع الجهات المحلية والدولية.

١٠ ـ وضع المعايير والآليات اللازمة لفحص واعتماد الأجهزة والأنظمة والتطبيقات المشغلة للبنية التحتية الحيوية في الدولة بالتنسيق مع الجهات المعنية.

١١ ـ إجراء الاختبارات الفنية الأمنية للأنظمة والبرامج والشبكات في مؤسسات القطاعات الحيوية.

١٢ ـ اعتماد أطر ومعايير تقييم الكوادر البشرية العاملة في مجال الأمن السيبراني في مؤسسات القطاعات الحيوية.

١٣ ـ تقييم وتطوير قدرات الأمن السيبراني لمؤسسات القطاعات الحيوية ووضع خطط لرفع المستويات ومتابعة تنفيذها.

١٤ ـ وضع معايير وضوابط الترخيص لمقدمي خدمات الأمن السيبراني وإصدار شهادات الاعتماد.

١٥ ـ رفع مستوى الوعي بالأمن السيبراني، ودعم وتطوير القدرات الوطنية في هذا المجال من خلال البرامج والمبادرات، وتنظيم الفعاليات المتعلّقة بالأمن السيبراني في الدولة.

١٦ ـ اعتماد مشاريع ومبادرات الأمن السيبراني في مؤسسات القطاعات الحيوية.

١٧ ـ تنفيذ تمارين الجاهزية والمناورات السيبرانية على مستوى الدولة.

١٨ ـ إبرام العقود ومذكرات التفاهم والشراكات مع الجهات المحلية والدولية المعنية بالأمن السيبراني.

١٩ ـ متابعة تنفيذ التزامات الدولة المعنية بالأمن السيبراني.

٢٠ ـ تشجيع وتوجيه البحث العلمي والابتكار في مجال الأمن السيبراني، والعمل على توطين صناعة محلية له.

٢١ ـ تنفيذ القوانين واللوائح والقرارات المتعلّقة بحماية خصوصية البيانات الشخصية.

٢٢ ـ اقتراح الأدوات التشريعية ذات الصلة بالأمن السيبراني.

جهود أخرى:

- وكانت أحدث الجهود القطرية في هذا السياق نجاح علماء في معهد قطر لبحوث الحوسبة بجامعة حمد بن خليفة، بالشراكة مع جهات قطرية وتركية أخرى، في بناء منصة دفاع للأمن السيبراني تحت اسم «تحذير»؛ للتنبؤ بالتهديدات الأمنية ضد الشركات والبنى التحتية الحيوية واكتشافها، وتُعد المنصة الجديدة نتاجاً لمشروع يمتد لثلاث سنوات بين معهد قطر لبحوث الحوسبة، ووزارة الداخلية القطرية، واللجنة العُليا للمشاريع والإرث، وجامعة توب التركية للاقتصاد والتكنولوجيا، وجامعة «قادر هاس»، وشركة «إنتربروب» المتخصصة في تقديم خدمات الاستخبارات الإلكترونية والدفاع السيبراني، وتم تمويل المشروع عن طريق منحة بقيمة ١,٦٥ مليون دولار قدَّمها الصندوق القطري لرعاية البحث العلمي بالاشتراك مع مجلس الأبحاث العلمية والتكنولوجية التركي (توبيتاك).
- وفي العام ٢٠١٩، وقعت شركة (BI.ZONE) الروسية المتخصصة في خدمات حماية الأصول وإدارة السمعة على الإنترنت اتفاقية مع

شركة (MANNAI) القطرية، تقوم بموجبها الأخيرة بتسويق منتجات الشركة الروسية في مجال الأمن السيبراني في قطر، وجاء في بيان صدر عن مصرف «سبيربنك» (المالك لشركة BI.ZONE)، أن الشركة القطرية ستصبح وفقاً للاتفاق الموزع الرسمي لمنتجات وخدمات الشركة الروسية في مجال الأمن السيبراني في قطر، وستسمح شراكة الشركتين بزيادة الحماية ضد الهجمات الإلكترونية المغرضة في منطقة الشرق الأوسط، وذلك بمساعدة التكنولوجيات الروسية، ووفقاً للاتفاق ستورّد الشركة الروسية إلى السوق القطرية حلولاً لمكافحة عمليات الاحتيال والنصب في القنوات المصرفية الرقمية، ومنصات إلكترونية لجمع وتحليل ونشر البيانات حول تهديدات الأمن السيبراني، وكذلك سيحصل الجانب القطري على إمكانية استخدام الحلول السحابية للحماية وخوادم لأتمتة عمليات المراقبة وإبداء رد الفعل على الحوادث في مجال الأمن السيبراني.

- كما تتعاون جامعة «تكساس آي آند إم» في قطر مع مركز الدراسات التنفيذية التابع لجامعة حمد بن خليفة، منذ العام ٢٠١٨، من خلال برنامج يمنح شهادة في أساسيات الأمن السيبراني، ويغطي البرنامج موضوعات متعلّقة بالمفاهيم الأساسية لأنظمة التشفير الحديثة، وكيفية استخدامها لحماية البيانات والاتصالات الخاصة، إضافة لطرق جمع وتحليل المعلومات مفتوحة المصدر والمعلومات المتاحة للجمهور، وتقنيات الحوسبة السرّية.

(٦) ـ أنشطة دولة الكويت في مجال الأمن السيبراني:

كمثيلتها من المنظومة الخليجية، اهتمت دولة الكويت بمجال الأمن السيبراني وجعلته مؤخراً من أهم اهتماماتها، إذ خصصت الحكومة الكويتية جهات مختلفة للقيام بمهام الحماية والدفاع عن الأنظمة الرقمية للدولة؛ إلى جانب اجتهاد المؤسسات التعليمية في طرح تخصص الأمن السيبراني سواء كمقررات دراسية أو تخصصات مدرجة لدى المؤسسة التعليمية، ويعتبر المركز الوطني للأمن السيبراني من أبرز الأنشطة التي قامت بها الدولة مؤخراً بغية تحقيق مجتمع أكثر أماناً وسلامة، والهيئة العامة للاتصالات وتقنية المعلومات.

أ . المركز الوطني للأمن السيبراني:

تم إطلاق المركز الوطني للأمن السيبراني بموجب قرار مجلس الوزراء رقم ٣٥٥ في اجتماعه ٢٠١٩/ ١١ بتاريخ ٢٠١٩/ ٣/ ١٨ لتأمين وحماية الشبكات المعلوماتية، وشبكة الاتصالات، ونظم المعلومات، وعمليات جمع وتبادل المعلومات باستخدام أي وسيلة إلكترونية ويهدف إلى ما يلي:

١ ـ بناء منظومة فعّالة للأمن السيبراني على المستوى الوطني وتطويرها وتنظيمها لحماية الدولة من تهديدات الفضاء السيبراني ومواجهتها بكفاءة وفاعلية بما يضمن استدامة العمل والحفاظ على الأمن السيبراني الوطني.

٢ ـ حماية المصالح الحيوية في الفضاء الإلكتروني، والإشراف على بناء القدرات الوطنية المتخصصة في مجال الأمن السيبراني.

٣ ـ تعزيز ثقافة الأمن السيبراني التي تدعم الاستخدام الآمن والصحيح للفضاء الإلكتروني.

٤ ـ حماية ومراقبة الأصول والبنية التحتية الحيوية والمعلومات الوطنية والشبكة المعلوماتية في دولة الكويت.

٥ ـ إتاحة سبل التعاون والتنسيق وتبادل المعلومات فيما بين مختلف الجهات المحلية والدولية في مجال الأمن السيبراني.

وذلك من خلال القيام بالمهام التالية:

١ ـ إعداد استراتيجيات وسياسات ومعايير وآليات تنفيذ الأمن السيبراني واقتراح تعديلها، ومتابعة تنفيذها.

٢ ـ إعداد الخطة الوطنية لمواجهة الأخطار والتهديدات المتعلّقة بالأمن السيبراني وتعديلاتها، ومتابعة تنفيذها.

٣ ـ متابعة تنفيذ الجهات المعنية للاستراتيجية وخطط ومعايير وسياسات الأمن السيبراني الصادرة عن المركز.

٤ ـ تطوير عمليات الأمن السيبراني وتنفيذها وتقديم الدعم والاستشارة اللازمين لبناء فرق عمليات الأمن السيبراني، وتنسيق جهود الاستجابة لها والتدخل عند الحاجة.

٥ ـ وضع الإطار التنظيمي وآليات الحوكمة لتطبيق الاستراتيجية.

٦ ـ إعداد وتصنيف وتحديد البنية الأساسية للأمن السيبراني والجهات المرتبطة بها، وتحديد القطاعات والجهات ذات الصلة بالأمن السيبراني.

٧ ـ تحديد معايير الأمن السيبراني وضوابطه، وتصنيف حوادث الأمن السيبراني.

٨ ـ إنشاء قاعدة بيانات بالتهديدات الإلكترونية بمشاركة الجهات المعنية.

٩ ـ تقييم وتطوير النواحي الأمنية لخدمات الحكومة الإلكترونية.

١٠ ـ تقييم وتطوير فرق الاستجابة لحوادث الأمن السيبراني وإصدار التعليمات للجهات المعنية.

١١ ـ إجراء تدريبات ومسابقات الأمن السيبراني.

١٢ ـ تنظيم عمل الشركات والخبراء والاستشاريين وغيرهم ممن يقدّمون خدمات الأمن السيبراني، ومنح الترخيص وإعداد سجل يقيد فيه المستوفون للمعايير الأمنية.

١٣ ـ تطوير البرامج اللازمة لبناء القدرات والخبرات الوطنية في مجال الأمن السيبراني، وتعزيز الوعي على المستوى الوطني.

١٤ ـ وضع الشروط والمواصفات الفنية لأي أجهزة أو أنظمة مرتبطة بمجال الأمن السيبراني، والموافقة على استعمالها أو استيرادها أو تداولها بالدولة، وإصدار التعاميم والتعليمات المنظمة لحماية الأجهزة والبرامج والشبكات ومواقع غرف الحسابات من أخطار التدخلات والاختراقات، والوصول إلى المعلومات من غير المخوّلين بالوصول إليها.

١٥ ـ وضع الشروط والمعايير الوظيفية لشغل وظائف الأمن السيبراني بالجهات المعنية.

١٦ ـ القيام بالفحص الأمني التقني، والتدقيق على أنظمة وشبكات الجهات المعنية للتأكد من التزامها بالمعايير والسياسات التي يصدرها المركز.

١٧ ـ التدخل التقني إذا ما تطلّب الأمر للتصدّي لحوادث الأمن السيبراني التي تتعرّض لها الشبكات والجهات المعنية.

١٨ ـ وضع الضوابط اللازمة لمنع أي محاولات لإعاقة أو تعطيل أو تخريب شبكات الاتصالات ونظم المعلومات في الدولة، واتخاذ ما يلزم للتعامل لمواجهة التهديدات الإلكترونية كافة، سواء كانت من داخل الدولة أو خارجها.

١٩ ـ مراقبة ورصد التهديدات الإلكترونية لشبكات الجهات المعنية وإجراء التحقيقات اللازمة بشأنها وعزلها إذا اقتضت الحاجة في حالة عدم التقيّد بمعايير الأمن السيبراني بما يكفل التصدي لأي تهديدات قد تلحق ضرراً بمنظومة الأمن الوطني أو اقتصاد الدولة أو علاقاتها الدولية والإقليمية.

٢٠ ـ تقديم المساندة والاستشارة التقنية للجهات المعنية، من خلال الاستدلال، ومساندة التحقيق في الجرائم المتعلّقة بالأمن السيبراني.

٢١ ـ إبداء الرأي التقني في الموضوعات المتعلّقة بالأمن السيبراني.

٢٢ ـ التنسيق والتعاون مع الجهات المعنية للعمل وفق بنود إطار الحوكمة الوطنية للأمن السيبراني.

٢٣ ـ إعداد ودعم الدراسات والبرامج والبحوث العلمية اللازمة لتطوير منظومة الأمن السيبراني في الدولة بالتنسيق مع المؤسسات الأكاديمية والمهنية المحلية والدولية.

٢٤ ـ متابعة تنفيذ الالتزامات الناشئة عن الاتفاقيات الدولية في مجال الأمن السيبراني، والقرارات الصادرة من المنظمات الدولية والإقليمية المنضمة إليها الدولة، وذلك بالتنسيق مع الجهات المعنية.

٢٥ ـ دراسة التشريعات ذات الصلة بالأمن السيبراني، واقتراح تعديلها، وذلك بالتنسيق مع الجهات المعنية.

٢٦ ـ إعداد التقارير الدورية والسنوية بشأن تنفيذ الاستراتيجية، وعن أعمال المركز، ورفعها إلى مجلس الوزراء.

٢٧ ـ إعداد تقارير دورية حول قضايا الأمن السيبراني ذات البُعد الوطني ورفعها إلى مجلس الوزراء لاتخاذ ما يراه.

ب. الهيئة العامة للاتصالات وتقنية المعلومات:

تهدف الهيئة العامة للاتصالات وتقنية المعلومات[١٨] إلى تنظيم وإشراف أمثل على سوق الاتصالات وتقنية المعلومات قائماً على أساس المنافسة الإيجابية، وتعمل على تقديم خدمات متميزة ومتطورة من خلال شبكة اتصالات سريعة وآمنة وموثوقة تعود بالنفع على المشتركين من أفراد وجهات عامة وخاصة وتحافظ على مصالحهم، وخلق مناخ محفّز للاستثمار بقطاعي الاتصالات وتقنية المعلومات، وتشجيع المبادرات الإبداعية للشباب الكويتي من أصحاب المشاريع الصغيرة والمتوسطة، وتطبيق أعلى المعايير العالمية للارتقاء بالخدمات الإلكترونية الحكومية وإتاحتها للمواطنين والمقيمين، وكذلك تعمل الهيئة وفقاً للرؤية الاستراتيجية

الوطنية للأمن السيبراني، حيث تباشر الاختصاص بمهام ومسؤوليات الأمن السيبراني على المستوى الوطني من خلال المهام التالية:

- إطلاق سياسات وضوابط أمنية.
- نشر التوعية الأمنية.
- إطلاق منصة تبادل المعلومات.
- إطلاق خدمات أمنية، مثل حجب المحتوى، ومبادرة تأمين العمل عن بُعد للجهات الحكومية، خدمة أمن تطبيقك.

رابعـــاً ـ دور الأمانـة العامـة لمجلـس التعـاون الخليجـي لخلـق منظومـة التعـاون في مجـال الأمـن السـيبراني:

نتيجة لاهتمام دول منطقة الخليج العربي اهتماماً بالغاً بمجال الأمن السيبراني، الأمر الذي ألزم الأمانة العامة لمجلس التعاون الخليجي بإطلاق اللجنة الوزارية للأمن السيبراني بدول مجلس التعاون سنة ٢٠٢٢، واللجنة التنفيذية للأمن السيبراني بدول مجلس التعاون وتختص كل منها بكل موضوعات الأمن السيبراني.

تضم اللجنة الوزارية للأمن السيبراني في دول مجلس التعاون لدول الخليج العربية في عضويتها أصحاب السعادة وزراء المراكز المعنية بالأمن السيبراني بدول مجلس التعاون، وتعقد اللجنة الوزارية للأمن السيبراني اجتماعًا سنويًا على مستوى وزراء الأمن السيبراني في دول مجلس التعاون الخليجي، وتهدف من خلالها إلى الإسهام في تهيئة فضاء سيبراني آمن، ومواءمة الجهود ورفع كفاءة التنسيق والتعاون بين دول المجلس، وحماية مصالحها في المنظمات الدولية ذات الصلة بمجال الأمن السيبراني، وتم عقد اجتماعين لها؛ الاجتماع الأول كان بمقر الأمانة العامة لمجلس التعاون في ٢٣ أكتوبر ٢٠٢٢، جرى خلال الاجتماع مناقشة العديد من الموضوعات المتعلّقة بالجوانب المشتركة للتعاون بين دول مجلس التعاون في مجال الأمن السيبراني، والتي تشمل وضع الأطر والسياسات والإجراءات المشتركة للتصدي للتهديدات السيبرانية، ومواءمة الجهود بين دول المجلس بمختلف القطاعات، ورفع مستوى التعاون الدولي مع الدول والمنظمات ذات

العلاقة، وتعزيز ونمو صناعة الأمن السيبراني بدول المجلس، إضافة إلى تبادل المعرفة والخبرات والدراسات والتجارب المتعلّقة بالأمن السيبراني، وتهيئة فضاء سيبراني آمن لحماية دول المجلس من التهديدات السيبرانية، كما تم إطلاق التمرين الخليجي الأول للأمن السيبراني، والذي يهدف إلى تعزيز التواصل ومشاركة المعلومات بين دول المجلس، وتبادل الخبرات بين الكوادر الوطنية المختصة بالأمن السيبراني، ورفع مستوى الجاهزية السيبرانية، والاستعداد لمواجهة التهديدات والأخطار السيبرانية، بالإضافة إلى إيجاد حلول مبتكرة لمواجهة التحديات والتهديدات السيبرانية.

أما الاجتماع الثاني فكان في يوم الخميس الموافق ٩ نوفمبر ٢٠٢٣م في مدينة مسقط بسلطنة عُمان؛ حضر الاجتماع رؤساء الجهات المختصة في مجال الأمن السيبراني في دول مجلس التعاون، والأمين العام لمجلس التعاون جاسم بن محمد البديوي، وتطرّق الاجتماع إلى عدد من الموضوعات التي تمثّل ركيزة أساسية لأعمال اللجنة، بالإضافة إلى مناقشة عدد من مشاريع الأمن السيبراني لتعزيز التكامل بين دول مجلس التعاون في هذا القطاع، وتضمنت نتائج الاجتماع الموافقة على مبادرة المملكة العربية السعودية بشأن إعداد استراتيجية شاملة للأمن السيبراني بدول مجلس التعاون، واعتماد هيكلة ونطاق عمل ومهام واختصاصات اللجنة الوزارية للأمن السيبراني واللجان التابعة لها، كما ناقشت اللجنة طلب نقل مهام واختصاصات لجنة المراكز الوطنية للاستجابة لطوارئ الحسابات وفريق عمل خدمات الثقة الرقمية لتكون ضمن اختصاصات اللجنة الوزارية للأمن السيبراني

واللجان التابعة لها، كما اعتمدت اللجنة خلال الاجتماع الخطة التنفيذية لعمل اللجنة الوزارية للأمن السيبراني بدول المجلس، بحيث يتم مراجعتها بعد اعتماد استراتيجية الأمن السيبراني بدول المجلس، واعتماد ما ورد في محاضر الاجتماع الأول والثاني للجنة التنفيذية للأمن السيبراني بدول المجلس.

أما عن اللجنة التنفيذية للأمن السيبراني بدول مجلس التعاون لدول الخليج العربية فقد عقدت اجتماعين حتى الآن، الاجتماع الأول كان في يوم الأحد الموافق ٥ مارس ٢٠٢٣م، عبر الاتصال المرئي، تم فيه مناقشة العديد من الموضوعات المشتركة بين دول المجلس لتعزيز التعاون في مجال الأمن السيبراني، حيث تم استعراض الأطر والسياسات والإجراءات المشتركة، ومواءمة الجهود بين دول المجلس بمختلف القطاعات للتصدي للتهديدات السيبرانية، وبحث التعاون الدولي مع الدول والمنظمات ذات العلاقة، بالإضافة لوضع آليات لتبادل المعرفة والخبرات والدراسات والتجارب المتعلّقة بالأمن السيبراني بين دول المجلس، وتعزيز ودعم صناعة الأمن السيبراني بهدف تهيئة فضاء سيبراني آمن بدول المجلس.

أما الاجتماع الثاني فقد كان عبر الاتصال المرئي في اليوم الخميس الموافق ٢٦ أكتوبر ٢٠٢٣م، وذلك بمشاركة أصحاب السعادة وكلاء الوزارات ونواب الهيئات ورؤساء المراكز المعنية بالأمن السيبراني بدول مجلس التعاون؛ تم خلال الاجتماع مناقشة العديد من الموضوعات المشتركة بين دول المجلس والمتعلّقة بالأمن السيبراني، وشملت الاستراتيجية

الاسترشادية التي سيتم العمل ضمن إطارها خلال الفترة المقبلة، والخطة التنفيذية لعمل اللجنة الوزارية للأمن السيبراني، ومبادرات دول المجلس في هذا المجال، وذلك بهدف مواءمة الجهود بين مختلف القطاعات ورفع مستوى الجاهزية السيبرانية بدول المجلس.

كما تحرص الأمانة العامة لمجلس التعاون لدول الخليج العربية على تأسيس آليات للتعاون وبناء الشراكات مع مختلف الجهات المحلية والإقليمية والدولية على نحو يسهم في تحقيق الغايات المشتركة، حيث وقَّعت مؤخراً مذكرة تفاهم مع الهيئة الوطنية للأمن السيبراني في السعودية، بهدف تعزيز التعاون بين الطرفين في مختلف الموضوعات ذات الصلة بمجال الأمن السيبراني، وتوظيف إمكانياتهما وخبراتهما بما يحقق المصلحة المشتركة، وتهدف إلى إنشاء إطار رفيع المستوى بين الهيئة والأمانة العامة لمجلس التعاون لدول الخليج العربية للتعاون في مختلف الموضوعات ذات الصلة في مجال الأمن السيبراني، ورفع أداء الأمن السيبراني لدى الأمانة العامة للمجلس عبر مجموعة من الأدوات والأنشطة المتبادلة، وتعزيز التكامل المبذول من الجانبين؛ بالإضافة إلى تبادل المعلومات والتنبيهات، وتقديم الدعم اللازم للأمانة العامة لمجلس التعاون لدول الخليج العربية من أجل وضع خطط الاستجابة لحوادث الأمن السيبراني، وتتضمن أيضاً بناء وتدريب الكوادر المتخصصة بالأمن السيبراني لدى الأمانة، وتقديم الإرشادات التوعوية لها وفق أفضل الممارسات الحديثة والمتبعة في المجال، وتنفيذ التوصيات المتعلّقة بالتعامل مع التنبيهات السيبرانية الصادرة عن

الهيئة، كما تم الاتفاق على تدشين منصة تحليل البرمجيات الخبيثة الخاصة بالأمن السيبراني، المشروع الخليجي المشترك، والذي يستهدف ضمان أمن المعلومات وحمايتها في دول الخليج العربي.

خلال الفترة الماضية، تبوأت دول مجلس التعاون الخليجي مراكز متقدمة في المؤشرات الدولية للأمن السيبراني، وهذا بسبب الجهود الواضحة لدول مجلس التعاون الخليجي في هذا المجال، وحرصهم الواضح على تأمين وحماية أنظمتها وسيادة دولها ضد الهجمات والمطامع السيبرانية الكثيرة؛ إلى جانب أن تعاون تلك الجهود والإنجازات التي حققوها في هذا المضمار سيجعلها قوة رادعة للتحديات السيبرانية المستقبلية وقوة سياسية واقتصادية منافسة.

خامساً ـ مؤشرات نضوج جاهزية الأمن السيبراني لدول مجلس التعاون الخليجي:

نتيجة للمجهود الواضح الذي سعت إليه دول مجلس التعاون الخليجي في منظومة الأمن السيبراني ومكافحة الهجمات السيبرانية المتعاقبة عليها، الأمر الذي أوجد كيانات تلك الدول في الخريطة العالمية من بين دول العالم الكبرى، من خلال المؤشرات العالمية التي أثبتت وجوداً واضحاً لدول الخليج العربي، وهنا نستعرض أهم تلك المؤشرات والمراتب التي استحوذتها من بين دول العالم المتنافسة.

فبالنسبة لمؤشر الأمن السيبراني (GCI)[١٩] الصادر عن الاتحاد الدولي للاتصالات (ITU) التابع للأمم المتحدة لعام ٢٠٢٠م، احتلت المملكة العربية السعودية المركز الثاني عالمياً مع بريطانيا على حد سواء بعد الولايات المتحدة التي تصدّرت القائمة عالمياً، فيما حلّت الإمارات أيضاً في مركز متقدم عالمياً عند المرتبة الخامسة بالتساوي مع روسيا وماليزيا، واحتلت سلطنة عُمان المركز الـ ٢١، وبعدها دولة قطر المركز الـ ٢٧، والبحرين المركز الـ ٦٠، أما الكويت فقد حلت المركز الـ ٦٥ عالمياً من بين ١٧٥ دولة.

يبيّن الجدول أدناه ترتيب دول الخليج في مؤشر الأمن السيبراني لعام ٢٠٢٠

جدول (١)
ترتيب دول مجلس التعاون لدول الخليج العربية في مؤشرات الأمن السيبراني لعام ٢٠٢٠م

ترتيب دول الخليج في مؤشر الأمن السيبراني لعام 2020		
الدولة	الترتيب الخليجي	الترتيب العالمي
السعودية	1	2
الامارات	2	5
عمان	3	21
قطر	4	27
البحرين	5	60
الكويت	6	65

وصنّف المؤشر العالمي للأمن السيبراني (GCI) لعام ٢٠٢١ أربع دول عربية فقط في المستوى المرتفع، وتصدَّرت دول السعودية وقطر والإمارات والبحرين وعُمان الجهود في تحقيق الأمن السيبراني عربياً وعالمياً، في حين وقعت باقي الدول في مرتبة متوسطة عالمياً، أو تذيّلت القائمة وفق المؤشر الذي شمل ١٧٥ دولة.

ويعتمد المؤشر العالمي للأمن السيبراني (GCI) على قياس وتحليل التدابير التي تتخذها الدول في خمسة مجالات رئيسة هي: التدابير القانونية والتقنية والتنظيمية وبناء القدرات والتعاون ومدى وجود استراتيجيات وسياسات للأمن السيبراني، ومدى وجود خطط ومعايير وطنية يتم تنفيذها على أرض الواقع، مثل توافر التدريب والتأهيل للكوادر في مجال الأمن السيبراني والجهود والمبادرات المبذولة في هذا الشأن، كما يشير إلى أحد أهم العوامل، وهو وجود بنية تشريعية وقانونية تدعم الأمن السيبراني.

وبناء على المؤشر الوطني للأمن السيبراني أو مؤشر
(NCSI: National Cybersecurity Index)[٢٠]

والـذي يقيـس جاهزيـة الـدول في منـع التهديـدات وتدبـير الحوادث السـيبرانية والـذي تـم رصـده في سـبتمبر ٢٠٢٣، شـمل ١٧٦ دولـة، واحتلـت المملكـة العربيـة السـعودية المركـز الـ ١٤، تلتهـا دولـة قطـر في المركـز الـ ٦٠، وبعدهـا مملكة البحريـن في المركـز الـ ٦٣؛ في حـين احتلـت سـلطنة عُـمان المركـز الـ ٨١ ودولـة الإمـارات العربيـة المتحـدة المركـز الـ ٨٩، وختامـاً دولـة الكويـت في المركـز الـ ٩٨.

أمـا عـن مـؤشر (CEI: Cybersecurity Exposure Index)[21] والـذي يحـدد مسـتوى تعـرّض الدولـة للجرائـم الإلكترونيـة وشـملت ٩٣ دولة، وقد كان آخـر تحديـث لهـا في عـام ٢٠٢٠، فقـد احتلـت فيـه دولـة قطـر المركـز الـ ١٩، وبعدهـا الإمـارات العربيـة المتحـدة المركـز الـ ٣٨، تلتهـا المملكـة العربيـة السـعودية المركـز الـ ٤٠، ولم يكـن لـكل مـن سـلطنة عُـمان ومملكـة البحريـن ودولـة الكويـت وجـود في القائمـة المعلنـة.

وفي تقريـر آخـر والـذي عرض متوسـط ثلاثـة مـؤشرات (GCI,NCSI, CEI)[٢١]، وقـد شـملت ٩٣ دولـة في العـالم، احتلـت فيـه دولـة قطـر المركـز الـ ٣٠، وبعدهـا الإمـارات العربيـة المتحـدة المركـز الـ ٤٣، تلتهـا المملكـة العربيـة السـعودية المركـز الـ ٦٥، ولم يكـن لـكل مـن سـلطنة عُـمان ومملكـة البحريـن ودولـة الكويـت وجـود في القائمـة المعلنـة.

مـن جانـب آخـر، تكشـف النسـخة الخامسـة مـن مـؤشر «Surfshark» الصـادر عـن شركـة سـيرف[٢٢] شـارك المتخصّصـة لهـذا العـام ٢٠٢٣ لجـودة

الحياة الرقمية عن رؤى حول العوامل التي تؤثّر على الرفاهية الرقمية للبلد والمجالات التي ينبغي منحها الأولوية لتحسين جودة الرقمنة مستقبلاً، وتقدّم النسخة الخامسة من هذا المؤشر منظوراً فريداً لجودة الحياة الرقمية في أي بلد وفقاً لخمس ركائز: القدرة على تحمّل تكاليف الإنترنت، وجودة الإنترنت، والبنية التحتية الإلكترونية، والأمن الإلكتروني، والحكومة الإلكترونية، خليجياً، جاءت الإمارات أولاً بالمركز الـ ٣٨ عالمياً، تلتها المملكة العربية السعودية بالمركز الـ ٤٥ عالمياً، ثم قطر المركز الـ ٤٨ عالمياً، ثم البحرين بالمركز الـ ٥٧ عالمياً، ثم عُمان بالمركز الـ ٦١ عالمياً، وحلّت الكويت بالمركز الأخير خليجياً و٦٣ عالمياً.

كما حققت المملكة العربية السعودية المركز الثاني عالمياً في مؤشر الأمن السيبراني، وذلك ضمن تقرير الكتاب السنوي للتنافسية العالمية لعام ٢٠٢٣، الصادر عن مركز التنافسية العالمي التابع للمعهد الدولي للتنمية الإدارية في سويسرا IMD[٢٣]، والذي يهدف إلى تحليل وترتيب قدرة الدول على إيجاد بيئة داعمة ومحفّزة للتنافسية والمحافظة عليها وتطويرها.

وقد أظهرت الدراسات والإحصائيات تفوق دول مجلس التعاون الخليجي بشكل جماعي على العديد من الدول الغربية الأخرى والبلدان الأكثر تقدماً اقتصادياً من حيث قدراتها الأمنية السيبرانية واستدامة البنى التحتية البشرية وغيرها، بالإضافة إلى التدابير التعاونية لخلق بيئة تقنية آمنة؛ وهذا ما يهيئها لإطلاق وحدة اتحادية مشتركة تقاوم تحديات التكنولوجيا المستقبلية ومثالبها.

سادساً ـ مستقبل المنظومة الأمنية لدول المنطقة الخليجية :

لمواجهة التحديات الأمنية في المجال السيبراني تحوّلت دول الخليج إلى تدشين شراكات مع الدول الأخرى وإنشاء بنى تحتية دفاعية جديدة خاصة بها مع مختلف دول العالم، فقد عزَّزت دول مجلس التعاون الخليجي تعاونها الدفاعي في مجال الأمن السيبراني مع المملكة المتحدة، ففي أغسطس ٢٠٢٣ وقّعت دولة الكويت وبريطانيا إعلان نوايا للتعاون في مجال الأمن السيبراني، كما قامت أيضاً دولة الكويت والولايات المتحدة بتوقيع خطاب نوايا لتعزيز التعاون في الأمن السيبراني؛ بالإضافة إلى الاتفاقيات التي أبرمتها دولة الكويت مؤخراً مع دول وقطاعات مختلفة.

من جانب آخر، تتحرك السعودية من أجل التعاون مع بلدان إقليمية ودولية في مجالات الأمن السيبراني؛ ففي ٢٠٢٣ وقّعت الهيئة الوطنية للأمن السيبراني ٤ مذكرات تفاهم مع عدد من الجهات: قطر، والكويت، ورومانيا، وإسبانيا، ومن جانب آخر، وقّعت دولة قطر في عام ٢٠١٨ مع الولايات المتحدة خطابات نوايا في مجالات الأمن السيبراني ومنصة التعاون القطري الأمريكي، وكذلك حرصت دولة قطر في عام ٢٠٢٣ على تعزيز التعاون المشترك مع دولة الكويت في الأمن السيبراني، وفي العام نفسه سعت دولة قطر مع الاتحاد الأوروبي لتعزيز التعاون في الأمن السيبراني؛ كما انضمت مؤخراً إلى منظمة «التعاون الرقمي» بهدف تعزيز التعاون الدولي في مجالات الابتكار والتمكين وتسريع نمو الاقتصاد الرقمي، ودعم استراتيجيات التنمية الاقتصادية في البلاد؛ وسيعزز انضمام قطر للمنظمة من أمنها السيبراني ومكافحة الجرائم الإلكترونية.

أما الإمارات العربية المتحدة، فقد اجتهدت في توثيق العلاقات مع مختلف الحكومات والقطاعات الخاصة، ووقّعت مذكرة تفاهم للتعاون في مجال الأمن السيبراني مع المغرب، وألبانيا وجامايكا وأرمينيا وغيرها من الدول للتعاون في مجال الأمن السيبراني، إلى جانب تعاونها مع القطاعات الخاصة ومنها شركة «مايكروسوفت»، وذلك لتعزيز القدرات السيبرانية وتبادل المعلومات، وإنشاء مجتمع معلومات آمن وعالمي.

كذلك وقّعت اتفاقية تعاون مع شركة «ماندیانت» الأمريكية لتحسين عمليات التنسيق وسرعة الاستجابة للهجمات السيبرانية المحتملة، وتوفير التدريب للكوادر الوطنية في هذا المجال الحيوي في إطار برنامج «نافس» لتأهيل وتدريب المواطنين وتزويدهم بمهارات المستقبل، كما وقّعت أيضاً الإمارات العربية المتحدة مذكرة تفاهم مع شركة هيوليت باكارد إنتربرايز «HPE» لتدريب طلاب المدارس والجامعات على المهارات الإلكترونية والتكنولوجية وإعداد جيل من الشباب الإماراتي لشغل وظائف في مجال التكنولوجيا المتطورة.

وقد أطلق مجلس الأمن السيبراني لحكومة دولة الإمارات مؤخراً تقرير «الـ ٥٠ عاماً المقبلة ... سيبرانياً ـ Cyber next 50» بالتعاون مع شركة «كي بي إم جي لوار جولف« ـ »KPMG» العالمية والذي يشكّل جهداً بحثياً رائداً يستشرف مستقبل الأمن السيبراني والتكنولوجيا المتقدمة والمشهد الرقمي للعقود الخمسة المقبلة.

أما عن سلطنة عُمان، فقد وقّعت السلطنة مذكرات تفاهم للتعاون في مجال الأمن السيبراني مع عدد من البلدان بما فيها مملكة البحرين وكوريا

الجنوبية وماليزيا واستونيا وسنغافورة، إلى جانب ذلك وقّعت سلطنة عُمان أيضاً مع المنظمة العالمية للاستجابة للطوارئ المعلوماتية بهدف تعزيز التعاون الدولي في مجال الأمن السيبراني والتصدي للتهديدات والأخطار الأمنية المعلوماتية، ومقرها الولايات المتحدة الأمريكية، كما وقّعت اتفاقية تعاون أخرى مع مركز الأمن السيبراني التابع للمنتدى الاقتصادي العالمي، وهي منظمة دولية غير حكومية وغير ربحية، وتجمع بين نخبة من رجال الأعمال والسياسيين والأكاديميين وتهدف إلى إيجاد منصة للحوار والتباحث بشأن التحديات الاقتصادية والسياسية التي تواجه العالم وسبل حلها.

ولم تتوانَ مملكة البحرين في بذل المزيد من الجهود والاتفاقيات في مجال الأمن السيبراني، فقد سعت مملكة البحرين إلى تعزيز التعاون المشترك مع الولايات المتحدة في مجالات الأمن السيبراني ومكافحة الجريمة، وقامت أيضاً بتوقيع مذكرة تعاون مع الهند في الأمن السيبراني والذكاء الاصطناعي وغيرها من التقنيات، والتي تهدف إلى بناء أنظمة تكنولوجية قوية، وتطوير البرامج التعليمية والمناهج المتعلّقة بالذكاء الاصطناعي والأمن السيبراني، كما صدر بيان مشترك بين دولة الإمارات العربية المتحدة ومملكة البحرين للتعاون في مجالات عدة أهمها تعزيز التعاون المشترك في المجال الأمني بما يسهم في تطوير المنظومة الأمنية من خلال تبادل الخبرات والتجارب وأفضل الممارسات بين البلدين، بما في ذلك التعاون في مجال الأمن السيبراني.

ودعماً لهذه الخطوات، اتجهت دول الخليج العربي أيضاً إلى إنشاء وكالات أمن إلكتروني مخصصة لإيلاء الاهتمام الكامل لدفاعاتها الإلكترونية،

حيث قامت المملكة العربية السعودية بإنشاء بنية تحتية مؤسسية واسعة للتعامل مع الأمن السيبراني، وفي العام ٢٠١٧، أنشأت الهيئة الوطنية للأمن السيبراني، وهناك أيضاً الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز، بالإضافة إلى مراكز متخصصة تعي بالأمن السيبراني وتطبيقاته، كما دشّنت سلطنة عُمان عام ٢٠١٠ المركز الوطني للسلامة المعلوماتية ومركز الدفاع الإلكتروني، بالإضافة إلى أنها احتوت مقر المركز العربي الإقليمي للأمن السيبراني.

أما مملكة البحرين فقد أطلقت المركز الوطني للأمن السيبراني عام ٢٠٢٠، بالإضافة إلى المبادرات الأخرى، وأيضاً الإمارات العربية المتحدة، فقد كان لها مجهود كبير في تعزيز الأمن السيبراني من خلال مجلس الأمن السيبراني وهيئة أبو ظبي الرقمية، ومركز دبي للأمن السيبراني وهيئة تنظيم الاتصالات والحكومة الرقمية، ولم تتوانَ دولة قطر في الاهتمام بهذا المجال، فقط أطلقت عام ٢٠٢١ الوكالة الوطنية للأمن السيبراني.

وختاماً أطلقت دولة الكويت المركز الوطني للأمن السيبراني عام ٢٠٢٢، بالإضافة إلى إطلاق الاستراتيجية الوطنية للأمن السيبراني من قِبل الهيئة العامة للاتصالات وتقنية المعلومات.

وبالإضافة إلى العمليات الدفاعية التي تقوم بها الدول، كان هناك أيضاً الكثير من الإجراءات على مستوى القطاع الخاص، وهو ما انعكس في النمو الكبير لسوق الأمن السيبراني في الخليج خلال السنوات الأخيرة، ووفقاً لشركة «هانيويل» المتخصصة في مجال التقنيات الإلكترونية المُعقدة،

من المتوقّع أن ينمو سوق الأمن السيبراني العام ٢٠٢٤، بمعدل سنوي يبلغ ٢٢,٥٪، بالإضافة إلى نمو اقتصادي ملحوظ في هذا القطاع من ٤,١١ مليار دولار، العام ٢٠١٧، إلى ١,٢٢ مليار دولار، في عام ٢٠٢٢.

إضافة إلى أن المنظومة الخليجية متجهة في تطوير استراتيجياتها الأمنية المستقبلية من خلال حماية البنية التحتية السيبرانية والتي تتجسّد في تأمين وحماية البنية التحتية التكنولوجية للحكومات والشركات من الهجمات السيبرانية وضمان استمرارية الخدمات، إلى جانب حماية البيانات والخصوصية والتي تشكّل قوى عظمى قد تؤثّر وبصورة مباشرة على أمن واستقرار سيادة الدول، لذا وجب تطوير سياسات فعّالة لحماية البيانات الحساسة، وضمان الامتثال لمعايير الخصوصية الدولية، بالإضافة إلى التصدي للهجمات السيبرانية من خلال إطلاق استراتيجيات للكشف عن الهجمات السيبرانية المستهدفة والتصدي لها، سواء كانت هجمات داخلية أو خارجية، إلى جانب سن التشريعات وسياسات الأمن السيبراني، والتي تتضمَّن إقرار وتحديث التشريعات والسياسات المتعلّقة بالأمن السيبراني لضمان الامتثال والتطور التكنولوجي، ناهيك عن أهمية تعزيز الوعي الرقمي وتطوير قدرات الأمن السيبراني ومهارات المتخصصين في مجال الأمن السيبراني من خلال التدريب وورش العمل.

وختاماً تم تحقيق التعاون الدولي مع المنظمات الدولية والدول الأخرى لتبادل المعلومات حول التهديدات السيبرانية وتعزيز التعاون الدولي في هذا السياق.

سابعاً: مقترحات وتوصيات نحو التكامل الخليجي في منظومة الأمن السيبراني:

تعتبر دول مجلس التعاون الخليجي اليوم مركزاً عالمياً للديناميكية والتطور، مما يحتّم علينا ضرورة العمل الدائم والمستمر لحمايتها وحماية مؤسساتها من التهديدات الرقمية عبر الابتكار في مجال الأمن السيبراني، وتقديم حلول للتحديات كافة، تعزّز الجاهزية والقدرة على استيعاب أية مشكلات محتملة، وفي المقابل تطوّرت تقنيات الاختراقات والجرائم الإلكترونية بصورة مخيفة بعد تضخم حجم البيانات واستخدام تقنيات الاتصال الفائق والحوسبة الكمومية، وتقنيات الذكاء الاصطناعي وغيرها من وسائل؛ لذا وجب العمل الدؤوب لمواجهة الجرائم الإلكترونية والحد من آثارها؛ لأننا بلا محالة مجبرون على الخوض في هذه العوالم الافتراضية الرقمية مجهولة الهوية، فهي الحاضر وهي المستقبل الواعد، ففي مارس ٢٠٢٣ أطلقت الجمعية الكويتية لأمن المعلومات(٢٤) مؤتمرها الثاني تحت عنوان «المؤتمر الخليجي الثاني لتحديات الأمن السيبراني»، والذي ختم بإطلاق توصيات مهمة وضرورية للعوم في تيارات أخطار الأمن السيبراني، وقد صنّفت تلك التوصيات إلى ما يلي:

- توصيات على مستوى الدولة.
- توصيات على مستوى دول مجلس التعاون الخليجي.

أ. توصيات على مستوى الدولة:

• ضرورة إنشاء هيئة مستقلة للأمن السيبراني وتحديد اختصاصاتها التنظيمية والإدارية والتشغيلية في مجال الأمن السيبراني، ووضع فروع لها في جميع مؤسسات

الدولـة، بحيث تكون الإدارة الرئيسـة (والتـي قد تتبع الأمانة العامة لمجلس الوزراء) هـي التـي تشرف مبـاشرة عـلى الإدارات الفرعية الموزّعة في جميـع القطاعات.

• تطويـر وتنفيـذ اسـتراتيجية وطنيـة للأمـن السـيبراني، مـع ضمان أعلى مسـتوى من الدعـم مـن قِبل المسـؤولين في الدولة، والتـي تعتمد على الأطر العالمية للأمن السـيبراني (NIST- the National Institute of Standards and Technology)

وتعمل على خمسة محاور متوازية أهمها:

١ ـ تحديد الأصول الرقمية والأخطار المرتبطة بها.

٢ ـ الحماية والتامين.

٣ ـ اكتشاف الهجمات السيبرانية.

٤ ـ الاستجابة للحوادث السيبرانية.

٥ ـ التعافي من الحوادث السيبرانية.

• ضرورة إعـادة صياغـة القوانـين والتشريعـات المتعلّقـة بأمـن المعلومـات بصـورة تناسـب المتغيـرات السريعـة للتكنولوجيـا، وتعالـج المشـكلات التـي نجمـت عـن القوانـين الحاليـة.

• دعـم البحـث والتطويـر في مجـال الأمـن السـيبراني وتشـجيع الباحثـين والناشـطين في مجـال الأمـن السـيبراني وتقنياتـه.

• تعزيـز أوجـه التعـاون مـع مجموعـات ومراكـز وطنيـة ودوليـة لأبحـاث الأمـن والـوكالات الحكوميـة والـشركات والمؤسسـات الأكاديميـة بهـدف التميـز في نتائـج الحلـول الأمنيـة.

• بناء كوادر وطنية، من خلال ما يلي:

- اعتماد البرامج التعليمية في مجال الأمن المعلوماتي وإدراجها ضمن المناهج التعليمية، بالإضافة إلى وضع خطة ابتعاث واضحة تعكس احتياجات سوق العمل في مجال الأمن السيبراني.

- تشجيع ودعم الشباب في هذا المجال وتبني المواهب والإبداعات في مجال أمن المعلومات.

- إطلاق المبادرات التعليمية والتدريبية المتخصصة للمساعدة على تأهيل وبناء الكفاءات الوطنية المتميزة.

- إقامة وتنظيم المسابقات وتشجيع روح المنافسة (مثال: Bug Bounty Program).

- دعم وتأهيل الشباب للمشاركة في المنافسات المحلية أو العالمية المتخصصة في الأمن السيبراني والبرمجة.

• تطوير معايير وضوابط قياسيه لتحقيق حد أدنى من أهداف ومتطلبات الأمن السيبراني، والتي من الممكن تعزيزها ولكن لا يمكن النزول دونها.

• تطوير معايير ضمان البيانات وخصوصيتها لحماية البنية التحتية للمعلومات في الدول وتحسين أمن المعلومات الوطنية.

• تطوير وتعديل الهياكل الإدارية بالمؤسسات الحكومية والخاصة لتواكب التغيرات في التخصصات والمهن والإجراءات، وذلك لسد بعض الثغرات الإدارية والإجرائية التي قد تشكّل تهديدات أمنية قد تعرّض

الكيانات للخطر، كذلك من الضروري وجود إدارات خاصة بأمن المعلومات ذات مهام واضحة ومحددة في جميع مؤسسات الدولة بما يدعم تفعيل سياسات وأدوات وضوابط الأمن السيبراني وإلزامها على الجميع.

- توفير وتوحيد البنية التحتية والقانونية لمؤسسات الدولة في مجال أمن المعلومات وتطوير الخدمات الإلكترونية وحماية المعلومات.
- تحديد مجال ضيق جداً للنفاذ للمعلومات الحساسة وتقييد مشاركتها ووضع آليات وقوانين تقنن استنزاف البيانات.
- ضمان التعاون داخل الحكومة، حيث يعتبر الالتزام والتنسيق والتعاون داخل الحكومة من المهام الأساسية لبناء منظومة آمنة داخل الدولة.
- ضرورة التعاون بين الحكومة والقطاع الخاص والشركات الصناعية من خلال العمل سوياً، وتبادل المعلومات الضرورية كشركاء حقيقيين سواء من خلال توحيد القوانين وتبادل البيانات والخبرات.
- عمل كشف دوري على الأنظمة المستخدمة في مجال الأمن السيبراني مع ضرورة وجود تدقيق خارجي على أمن المعلومات External Audit وبشكل دوري، ووضع مقاييس لقياس مدى الجودة والأمان لتلك الأنظمة.
- تنظيم عملية إطلاق التطبيقات الحكومية من خلال إلزام الجهات المختلفة لأخذ شهادة رقمية للتطبيقات الحكومية والذي يتم خلالها اختبار التطبيق أمنياً وفنياً قبل إطلاقه للمستخدمين.

- استخدام أنظمة مراقبة سلوك الموظفين وخاصة من لديه صلاحية الدخول إلى الأنظمة المعلوماتية.
- وضع خطة لإدارة الأخطار ومؤشرات للتنبيه في حال احتمال حدوثها من أجل تحديد الآليات التي يجب على المؤسسات اتخاذها لتقليل الأخطار الأمنية.
- استحداث أنظمة موحّدة لإتمام عملية تبادل البيانات وتطويرها بين مختلف قطاعات الدولة المختلفة وهيكلة النظام الإداري والفني القائم بين تلك القطاعات.
- الحصول على اعتمادات عالمية للأنظمة المستخدمة (أيزو وغيرها)، وتطبيق نظم أمن المعلومات وفق أفضل المعايير المعتمدة والممارسات العالمية المعمول بها لتكون أكثر شمولية وإنتاجية.
- العمل على إنشاء مركز لمعالجة البيانات وتحليلها من أجل رسم التوقعات المستقبلية للدولة والتنبؤ بالمتغيرات الرئيسة التي من شأنها قد تؤثر على أمنها واقتصادها، وإيجاد حلول دائمة لأهم الأزمات والصعوبات التي قد تواجهها.
- عقد اتفاقيات دولية مع الشركات أصحاب التطبيقات العالمية من حيث التحكم والحد من استنزاف بيانات المستخدمين (مثل شركة الفيسبوك والتويتر وغيرها)، وفي حال عدم موافقتها يتم حجب تلك التطبيقات، وذلك لتأثيرها الكبير على أمن الشعوب واستقرارها.

- وضع برنامج توعوي مشترك يجمع فيه القطاعات الحكومية والخاصة ومؤسسات المجتمع المدني من أجل تغيير الثقافة المجتمعية وتحسين الاستخدام.
- حجب التطبيقات التي من شأنها قد تؤثّر على أمن وسلامة مواطنيها والإشراف والتدقيق في نوعية التطبيقات المستخدمة.
- تنظيم عملية التعامل مع الإنترنت من خلال تصنيف الاشتراكات بناءً على الفئات العمرية (للأفراد) ومجال العمل (المؤسسات).
- تجهيز جيوش دفاع سيبرانية بأحدث التقنيات والبرامج الذكية الحديثة؛ لتكون حصناً منيعاً لصد أي هجوم سيبراني محتمل.

ب. توصيات على مستوى دول مجلس التعاون الخليجي :

- ضرورة إنشاء وإطلاق اتحاد خليجي موحّد بين دول مجلس التعاون الخليجي يضم نخبة من المتخصصين في مجال الأمن السيبراني، يكون من أهم اختصاصاته:
  - قياس الوضع الراهن للمنطقة في مجال أمن المعلومات وبشكل مستمر، ومعالجة الشائك منها.
  - وضع السياسات والأطر لمنظومة أمن المعلومات.
  - متابعه التطورات التكنولوجية للتنبيه إلى طرق الاختراق المحتملة والمستجدة والعمل للحيلولة دون وقوعها.

- رسم استراتيجية خليجية موحّدة تحميها من المتغيرات القادمة.

• تعديل التشريعات والقوانين من خلال ما يلي:

- العمل على بناء مواصفات قياسية ومتطلبات فنية وقانونية وإدارية وتنظيمية موحّدة في مجال أمن المعلومات لحماية المؤسسات بشكل عام والمعاملات التجارية بشكل خاص.
- توفير وتوحيد البنية التحتية والقانونية لتطوير الخدمات الإلكترونية وحماية أمن المعلومات.
- ضرورة إعادة صياغة القوانين والتشريعات المتعلّقة بالأمن السيبراني بصورة تناسب المتغيرات السريعة للتكنولوجيا وتعالج المشكلات التي نجمت عنها القوانين الحالية.

• تعزيز أوجه التعاون مع مجموعات ومراكز وطنية ودولية لأبحاث الأمن والوكالات الحكومية والشركات والمؤسسات الأكاديمية بهدف التميز في نتائج الحلول الأمنية.

• ربط الدراسات الأكاديمية باحتياجات سوق العمل، وتجهيز كوادر وطنية تكون سياجاً واقياً للدولة.

• إنشاء وتطوير المراكز الخليجية للاستجابة للحوادث السيبرانية، والتعاون فيما بينها، لتكون بمثابة خط الدفاع الأول ووحدات الكشف المبكر عن الهجمات السيبرانية، وتحديد مصادر هذه الهجمات وأهدافها، ومحاولة تحليل أساليب عملها والثغرات المستهدفة بهذه الهجمات السيبرانية.

تشجيع الاستثمار في مجال الأمن السيبراني، وتعاون القطاع الحكومي والخاص في إطلاق مشاريع أمنية مشتركة بين مختلف دول الخليج العربي.

- الدعوة لتأسيس صندوق خليجي لدعم البحوث والتطوير في مجال الأمن السيبراني.
- ضرورة إنشاء مراكز لعمليات أمن المعلومات (Security Operation Centers-SOCs)، لتنفيذ أعمال المراقبة الأمنية المستمرة، وتوفير خدمات أمن المعلومات الاستباقية والتفاعلية، والتنسيق والتواصل المستمر مع مراكز وفرق الاستجابة بقطاعات الدول الخليجية.
- حتمية مشاركة المعلومات والبيانات الأساسية والمهمة بين مختلف الدول الخليجية للحد من عمليات الاحتيال والتزوير.
- عمل اتفاقيات خليجية لتبادل البيانات الأساسية، والعمل على إنشاء مركز مشترك لمعالجتها وتحليلها؛ لإثراء صنع السياسات والاستجابات المناسبة للتحركات المستقبلية.
- خلق كوادر وطنية فنية من خلال :

- تبادل الخبرات الوطنية وعمل مؤتمرات وملتقيات مشتركة لمناقشة أهم الموضوعات ذات الصلة بأمن المعلومات.
- تنظيم وتبادل برامج أكاديمية مشتركة في مجال أمن المعلومات، ودعوة أصحاب الاختصاص من جميع أبناء دول مجلس التعاون الخليجي سواء بالحضور أو المشاركة.

- عمل برامج توعوية مشتركة باستخدام وسائل الإعلام التقليدية أو الرقمية، واستخدام طرق مبتكرة ذات التأثير الأكبر على المجتمع وخاصة في محاكاة الفئة الشبابية، وإطلاقها ضمن برامج مؤسسة الإنتاج البرامجي المشترك لمجلس التعاون لدول الخليج العربية والعمل على تعزيز الثقافة السيبرانية التوعوية.
- إطلاق المبادرات التعليمية والتدريبية المتخصصة للمساعدة على تأهيل وبناء الكفاءات الوطنية المتميزة.
- دعوة المؤسسات التعليمية لإدراج مناهج في مجال الأمن السيبراني ضمن المناهج التعليمية، بالإضافة إلى وضع خطة ابتعاث في مجال الأمن السيبراني.
- العمل على تعزيز التعاون المشترك في الجوانب الأكاديمية بين مختلف مؤسسات التعليم في دول مجلس التعاون الخليجي؛ لبناء رؤى مشتركة تواجه التحديات السيبرانية كافة.
- إقامة وتنظيم المسابقات وتشجيع روح المنافسة (Bug Bounty Program).

• إصدار وثيقة خليجية لتعزيز الأمن السيبراني والتي تحتوي على ضوابط ملزمة للجميع لحماية أمن البيانات الإلكترونية والشبكات والأنظمة، ومتابعة الالتزام بها، وتحديثها.

• اعتماد أنظمة معلوماتية آمنة ومحلية للحفاظ على البيانات، واستبدال التطبيقات الأجنبية المتداولة الآن (مثل الفيسبوك والتويتر وغيرها) بالتطبيقات المحلية لضمان حماية البيانات وخصوصيتها.

- العمل على إيجاد مناخ مناسب يتبنى المبادرات السيبرانية في دول مجلس التعاون الخليجي، ويعمل على تأهيل وبناء الكفاءات الوطنية المتميزة.
- استخدام معايير دولية ومحلية (مستحدثة) لتقييم أخطار العمليات المختلفة (إدارية أو مالية) الإلكترونية بشكل دوري؛ لمعرفة أوجه الضعف ومنافذ الخطر ومعالجتها، ووضع خطة طوارئ.
- العمل المشترك في المشاريع الحكومية ذات الصلة مثل:
  - حوكمة أمن المعلومات.
  - أنظمة المكافحة الذكية للتهديد السيبراني.
  - التعاون مع المؤسسات التعليمية.
  - إدارة الأخطار والبحث والتطوير.
  - وغيرها من مشاريع تخلق قاعدة أمنية قوية.
- الاستفادة من التجارب الدولية الناجحة (سواء من دول المنطقة أو خارجها) في مجال الأمن السيبراني وتعميم معايير النجاح وتطبيقها.
- عمل اتفاقيات خليجية لتبادل البيانات الأساسية والعمل على إنشاء مركز مشترك لمعالجتها وتحليلها؛ لإثراء صنع السياسات والاستجابات المناسبة للتحركات المستقبلية.
- وضع استراتيجية عمل عامة وموحّدة لدول مجلس التعاون الخليجي والحرص على الالتزام بأهم بنودها.

- التوسع في العمل التشاركي في مجال الأمن السيبراني مع الجهات المعنية في دول مجلس التعاون الخليجي لخلق قوة قادرة على مقاومة التحديات السيبرانية المستقبلية المتغيرة.
- إنشاء إدارة للاستجابة للحوادث السيبرانية لدول مجلس التعاون الخليجي، وإنشاء مرصد إلكتروني لرصد الجرائم عبر وسائل التواصل الاجتماعي لحماية الخليج وكذلك إيجاد آلية لتصنيفها.

ومن الثابت أنّه مع استمرار جهود دول الخليج العربي في تطوير دفاعاتها في مجال الأمن السيبراني واتباع الاستراتيجيات الوقائية، فإن هناك تطور هائل يقابله في الهجمات الإلكترونية والبرامج الخبيثة ووسائلها، وخاصة مع دخول أنظمة الذكاء الاصطناعي والبيانات الضخمة وتحليلها وتقنياتها المرعبة في مجال الاختراقات؛ لذا أصبح من الضروري واللازم الاستمرار في خوض هذه المعركة السيبرانية الافتراضية ليس فقط لحماية مقدّرات الدول، بل لأنها أصبحت مكوناً أساسياً للنجاح الاقتصادي والازدهار في هذا العالم.

ومن جانب آخر، أصبحت خريطة العالم تُرسم بناء على مدى إمكانية الدول للبقاء في الواقع الافتراضي الذي تم صياغته من قِبل وسائل التكنولوجيا المختلفة وتقنيات الذكاء الاصطناعي وبرمجة الروبوتات وعالم البيانات الضخمة وغيرها من طفرات جعلت من واقعنا خيالاً ومن خيالنا واقعاً ذا أبعاد لا تنتهي، والمنظومة الخليجية بنشاطها الحالي وجهودها

الكبيرة ستبقى محصنة، فتاريخها المشرّف وحاضرها الزاهي ومستقبلها المبهر وطموحاتها التي تسابق الزمن وتتجاوز كل الحدود كلها مؤشرات مبشّرة وعوامل دافعة للاستمرار والتفاؤل؛ لذا فإنني أختم صفحات هذه الدراسة بأمنيات وتطلعات على يقين أنها ستتحقق قريباً أو بعيداً، لكنها ستكون يوماً ما جزءاً من الواقع، ونختزل تطلعاتنا بما يلي:

- خلق منظومة خليجية محصّنة ومتماسكة وقادرة على حماية المؤسسات الخليجية، وجعلها قادرة على التصدي للتهديدات والحوادث السيبرانية المستقبلية.
- إطلاق مركز خليجي موحَّد معتمدًا محلياً ودولياً؛ لإصدار شهادات التراخيص المتعلّقة بخدمات ومنتجات الأمن السيبراني.
- خلق جيش سيبراني مؤهّل وقادر على الدفاع عن المنظومة الخليجية ضد الهجمات السيبرانية العالمية المستمرة.
- خلق بيئة جاذبة وداعمة للابتكارات الخليجية في مجال الأمن السيبراني؛ لبناء منتجات وخدمات سيبرانية عالية المستوى.
- الاكتفاء الذاتي والاعتماد على البرامج والتطبيقات المحلية الرقمية وتصديرها عالمياً كمنافس للتطبيقات العالمية الأخرى.
- تعزيز التعاون الدولي وإبرام اتفاقيات عالمية للاستفادة من الخبرات والتجارب العالمية في مجالات الأمن السيبراني ومجالات التقنية المبتكرة الحديثة الأخرى.

وختاماً، يمكننا القول بأن تحقيق الحماية المطلوبة لمختلف الأنظمة الرقمية المستخدمة هو أولوية قصوى لا يمكن تجاهلها أو التقليل من آثارها وتداعياتها، سواء كانت اقتصادية أو سياسية أو عسكرية، فقد أضحى الأمن السيبراني جزءًا لا يتجزأ من آليات التعاون الاقتصادي والأمني والتنموي والاستثماري فيما بين دول مجلس التعاون الخليجي، ويستوجب ذلك إيجاد نهج مشترك في السياسة العالمية تجاه الفضاء السيبراني، ولابد من إبرام اتفاقيات بين الكيانات الخليجية والعالمية للمساعدة على الامتثال إلى قواعد في الفضاء السيبراني.

قائمة المراجع

١ ـ مشهد التهديدات الإلكترونية في ٢٠٢٣

(https://me.kaspersky.com/blog/meta-csw10312/22-/)

٢ ـ تقرير شركة SOCRadar

(https://socradar.io/gulf-countries-threat-landscape-report-cyber-security-posture-of-the-gcc-countries/)

٣ ـ تقرير سايبر السعودية ٢٠٢١

٤ ـ المركز الوطني للسلامة المعلوماتية

(https://cert.gov.om//).

٥ ـ المركز العربي الإقليمي للأمن السيبراني

(https://arcc.om/).

٦ ـ مركز الدفاع الإلكتروني

(https://qanoon.om/p/2020/rd2020064/)

٧ ـ هيئة المعلومات والحكومة الإلكترونية

(https://www.iga.gov.bh/category/national-digital-policies)

٨ ـ المركز الوطني للأمن السيبراني

(https://www.ncsc.gov.bh)

٩ ـ إدارة مكافحة الجرائم الإلكترونية - وزارة الداخلية

(https://www.acees.gov.bh/cyber-crime/about-cyber-crime/)

١٠ ـ مبادرة إنترنت آمن
(https://safesurf.bh/ar/)

١١ ـ هيئة حماية البيانات الشخصية
(http://www.pdp.gov.bh/about-PDPA.html)

١٢ ـ هيئة المعلومات والحكومة الإلكترونية
(https://www.iga.gov.bh/)

١٣ ـ مصرف البحرين المركزي
(https://www.cbb.gov.bh/ar/)

١٤ ـ مجلس الأمن السيبراني
(https://www.csc.gov.ae/ar)

١٥ ـ مركز دبي للأمن الإلكتروني
(https://www.desc.gov.ae/about-us-ar/)

١٦ ـ هيئة تنظيم الاتصالات والحكومة الرقمية
(https://tdra.gov.ae)

١٧ ـ الوكالة الوطنية للأمن السيبراني
(https://ncsa.gov.qa/ar)

١٨ ـ الهيئة العامة للاتصالات وتقنية المعلومات
(https://citra.gov.kw)

١٩ ـ مؤشر الأمن السيبراني (GCI) الصادر عن الاتحاد الدولي للاتصالات (ITU)
(https://www.itu.int/epublications/publication/D-STR-GCI.-2021-01HTM-E)

٢٠ ـ مؤشر NCSI
(https://ncsi.ega.ee/ncsi-index/?order=rank&archive=1)

٢١ ـ مؤشرات أمنية لعام ٢٠٢٠
(National Cyber Security Index (NCSI) و Global Cybersecurity Index (GCI) و Cybersecurity Exposure Index (CEI)) (https://resources.cdn.seon.io/uploads/04/2023/Cybersecurity_countries-min.pdf)

٢٢ ـ النسخة الخامسة من مؤشر «Surfshark» الصادر عن شركة سيرف شارك المتخصّصة لهذا العام ٢٠٢٣ لجودة الحياة الرقمية
(https://www.telecomreviewarabia.com/articles/reports-coverage/-3309 gcc-leading-digital-quality-of-life-index)

٢٣ ـ مؤشر الأمن السيبراني الصادر عن مركز التنافسية العالمي التابع للمعهد الدولي للتنمية الإدارية في سويسرا IMD
(https://www.alarabiya.net/aswaq/economy/20/06/2023)

٢٤ ـ الجمعية الكويتية لأمن المعلومات
(https://kaiskw.org/)

٢٥ ـ مركز الخليج للدراسات الاستراتيجية.
https://www.gcssonline.com

٢٦ ـ دليل لوضع استراتيجية وطنية للأمن السيبراني التزام استراتيجي بالأمن السيبراني.
https://www.itu.int

٢٧ ـ دراسة أجرتها شركة كاسبرسكي الأمنية -Kaspersky Security Net work لأهم التهديدات الواردة في منطقة الشرق الأوسط لعام ٢٠٢٤ (https://almalnews.com/)

٢٨ ـ إطار العمل للأمن السيبراني للبنك المركزي السعودي (ساما) (https://dcybersecurity.sa/saudi-arabian-monetary-authority-sama-cyber-security-framework-arabic/).

Abstract:

Cybersecurity is an important and vital topic in the world, particularly in the Arabian Gulf region, because of its characteristics, which have placed it at the forefront of the target countries for cyberattacks. The Gulf region enjoys oil wealth and is home to international companies and institutions, as well as the region›s recent development and prosperity. The development of information and communication infrastructure and its openness to the digital world in different dimensions and its reliance on technology and cyberspace. This study focuses on highlighting the most significant threats and cyberattacks facing the Arabian Gulf region, and the main losses resulting from these attacks. The Arabian Gulf region is a fertile environment for cyberattacks of all kinds. For these reasons, it is important to strive to improve the security structure of GCC countries, which will be the subject of chapter 2 of this study by listing the most important achievements of GCC bodies and institutions in the field of cybersecurity. The study will also address the role of the GCC General Secretariate to create the cybersecurity cooperation system in the next chapter. As the dimensions of technology are constantly evolving, chapter 4 of this study will address the future of security system of the GCC States in the light of the successive advances in technology and what are the most important preparations and requirements to be taken. In conclusion, mentioning the most important proposals and recommendations towards Gulf integration in the cybersecurity system and the aspirations we hope to achieve for a sophisticated and secure Gulf system.

قواعد النشر في
سلسلة (التقرير الاستراتيجي)

١ ـ أن يكون موضوع التقرير معنياً بالقضايا الاستراتيجية التي تهم دولة الكويت في المقام الأول، ودول منطقة الخليج والجزيرة العربية بشكل عام، أو يعالج قضايا دولية واقليمية من زاوية ارتباطها بمنطقة الخليج.

٢ ـ أن يغلب على التقرير التحليل والتفسير مع تقليص مساحة الوصف أو التأريخ.

٣ ـ لا يقل عدد كلمات التقرير عن (**٣٧٥٠** كلمة).

٤ ـ يمنح الباحث مكافأة مالية مقدارها (١٥٠ دينار كويتي).

جامعة الكويت
KUWAIT UNIVERSITY

Center for the Gulf and Arabian Peninsula Studies
Established in 1994 - Kuwait University

The Challenges of Cybersecurity and its Effects on the Institutions and Bodies of the GCC Countries

Dr. Saffa Zaman
Amna Ayadah

Strategic Report
No. (36)

Kuwait - 2024

ISBN: 978-9921-749-59-5