قدرات المملكة العربية السعودية السيبرانية

The Kingdom of Saudi Arabia's Cyber Capabilities

أ.د. باسم علي خريسان

مركز الاستراتيجية والدراسات الدولية – جامعة بغداد

alibasim6493@gmail.com

تاريخ استلام البحث: ٢٠٢٥/٢/٥ تاريخ قبول النشر: ٢٠٢٥/٥/١٩

الملخص:

يعد الأمن السيبراني تحديًا رئيسًا يواجه الدول في العصر الحديث، إذ أصبح بناء القدرات السيبرانية ضرورة استراتيجية لحماية الأمن القومي وضمان التفاعل المؤثر في الفضاء السيبراني. وقد أدركت العديد من الدول، مثل إيران، الإمارات العربية المتحدة، وتركيا والمملكة العربية السعودية، أهمية هذا المجال وسعت إلى تطوير سياساتها واستراتيجياتها لتعزيز أمنها السيبراني. برزت المملكة العربية السعودية كإحدى الدول الرائدة في هذا المجال، حيث جعلت من بناء قدراتها السيبرانية أولوية استراتيجية، خاصة بعد الهجوم السيبراني الكبير الذي استهدف شركة أرامكو في العام ٢٠١٢ وألحق أضرارًا مادية جسيمة. دفعها ذلك إلى تعزيز بنيتها التحتية الرقمية والاستثمار في التقنيات الحديثة، مما مكّنها من تحقيق المرتبة الأولى عالميًا في مؤشر الأمن السيبراني لعام ٢٠٢٤.إن تجربة السعودية في تطوير قدراتها السيبرانية تعد أنموذجًا مهمًا يستحق الدراسة، لا سيما بالنسبة للعراق، الذي يحتاج إلى الاستفادة من هذه التجربة لبناء بنية سيبرانية قوية تحميه من التهديدات المتزايدة، وتعزز دوره الفاعل في الفضاء السيبراني الدولي.

الكلمات المفتاحية: المملكة العربية السعودية، الهجوم السيبراني، شركة.

Abstract:

Cybersecurity is a major challenge facing nations in the modern era. Building cyber capabilities has become a strategic necessity to protect national security and ensure effective engagement in cyberspace. Many countries, including Iran, the United Arab Emirates, Turkey, and Saudi Arabia, have recognized the importance of this field and have worked to develop policies and strategies to enhance their cybersecurity. Saudi Arabia has emerged as one of the leading countries in this domain, making the development of its cyber capabilities a strategic priority, especially after the major cyberattack that targeted Saudi Aramco in 2012, causing significant material damage. This incident prompted the kingdom to strengthen its digital infrastructure and invest in modern technologies, enabling it to achieve first place globally in the Cybersecurity Index for 2024.Saudi Arabia's experience in developing its cyber capabilities serves as a significant model worthy of study, particularly for Iraq, which needs to benefit from this experience to build a strong cyber infrastructure that can protect it from increasing threats and enhance its active role in the global cyberspace.

Keywords: Saudi Arabia, cyber-attack, company.

المقدمة:

شكّل التطور الكبير في مجال الأمن السيبراني تحديًا جديدًا فرض على المجتمعات والدول ضرورة السعي لبناء القدرات اللازمة للتكيف مع هذا التطور. وتُعدّ المملكة العربية السعودية من بين الدول التي حققت إنجازًا بارزًا في هذا المجال، حيث احتلت المرتبة الأولى عالميًا في مؤشر الأمن السيبراني لعام ٢٠٢٤. يُبرز هذا الإنجاز أهمية التجربة السعودية في بناء القدرات السيبرانية، ما يجعلها موضوعًا مهمًا للبحث والدراسة، بهدف فهم طبيعة هذه القدرات ومدى تأثيرها في الفضاء السيبراني، وهو ما يسعى هذا البحث إلى استكشافه وتحليله.

اولا: اهتمامات المملكة السيبرانية: تشهد المملكة العربية السعودية تطورات كبيرة في مجال الأمن السيبراني، وفي إطار **رؤية السعودية ٢٠٣٠**، تبنّت المملكة استراتيجية لتقليل الاعتماد على النفط، وتنويع الاقتصاد، وتطوير القطاعات الخدمية، مع التركيز على التكنولوجيا والتحول الرقمي.مع بداية جائحة كورونا، شهدت دول الشرق الأوسط ارتفاعًا في الهجمات السيبرانية، حيث زادت هجمات البرامج الضارة بنسبة(٢٢٪)، وهجمات البريد العشوائي بنسبة (٣٦٪)، مما أثر على الشركات السعودية التي كانت في طور التحول إلى العمل عن بُعد. وقد شكّلت هذه التهديدات تحديًا للبنية التحتية الرقمية، ما أدى إلى تأثيرات اقتصادية وأمنية، بما في ذلك تراجع ثقة المواطنين في الخدمات الحكومية واحتمال حدوث اضطرابات سياسية.فرضت الجائحة تحديات على المؤسسات العامة والخاصة، حيث أدى الانتقال السريع إلى العمل عن بُعد إلى ضرورة إعادة هيكلة قطاع **تكنولوجيا المعلومات**، وتحويل جميع أشكال التواصل إلى الإنترنت، مثل الاجتماعات الافتراضية عبر تطبيق(Zoom)، والتعليم عن بُعد، والتجارة الإلكترونية. دفع هذا التغيير الشركات إلى تبني استراتيجيات تضمن استمرار الإنتاجية، من خلال **نقل البيانات إلى الحوسبة السحابية**، وتوفير الوصول إلى موارد تكنولوجيا المعلومات عن بُعد.ونتيجة لذلك، أصبح الاستثمار في **الأمن السيبراني** ضرورة ملحّة لمواجهة التهديدات المتزايدة، من خلال اعتماد تقنيات حديثة وتدابير أمان قوية. كما برزت الحاجة إلى تدريب الموظفين على تحليل التهديدات الناشئة واتباع معايير الأمن السيبراني. يرىّ أكثر من نصف مديري تكنولوجيا المعلومات السعوديين أن **إدارة الأمن** هي التحدي التكنولوجي الأكبر، وأصبح **الاستثمار في الأمن السيبراني** من الأولويات الاستراتيجية، مما يعزز التحول الرقمي ويدفع إلى زيادة الإنفاق على **حماية البيانات والتقنيات الحديثة** في السنوات المقبلة [١].

ثانياً: استراتيجية المملكة لبناء قدراتها السيبرانية: في ظل التحديات المتزايدة للأمن السيبراني، أنشأت السعودية **الهيئة الوطنية للأمن السيبراني (NCA)** بموجب مرسوم ملكي في ٣١ تشرين الاول ٢٠١٧، بهدف تعزيز أمن الدولة من خلال إعداد التحليلات الداخلية ووضع الحلول القانونية. تتألف الهيئة من كبار المسؤولين الأمنيين، مثل **رئيس رئاسة أمن الدولة، ورئيس المخابرات العامة، ونائبي وزيري الداخلية والدفاع**، وتعمل على **تنظيم العمليات السيبرانية** والتعاون مع الجهات العامة والخاصة

لحماية البنية التحتية الرقمية وتحقيق أهداف **رؤية ٢٠٣٠**. وضعت **(NCA)** استراتيجية وطنية للأمن السيبراني تتضمن ستة محاور رئيسة: **تنسيق الأمن السيبراني على المستوى الوطني، إدارة المخاطر، تحسين الأداء في الفضاء السيبراني، تطوير الدفاع الديناميكي، تعزيز الشراكات الدولية، وتوسيع القدرات الوطنية في المجال السيبراني**، وتشمل هذه الجهود **الاستثمار في التعليم والتدريب**، ودعم **الصناعة والبحث العلمي** لتعزيز الابتكار.

وسعّت المملكة جهودها في المجال الرقمي بإنشاء **الهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA)** عام ٢٠١٩، والتي تُعنى بوضع استراتيجيات **تخزين البيانات وتطوير الذكاء الاصطناعي**، إلى جانب **المركز الوطني للذكاء الاصطناعي**. تهدف هذه المؤسسات إلى زيادة الإنتاجية، وتحسين عمليات صنع القرار، وتوفير خدمات مبتكرة للمواطنين، ودعم نمو الشركات. سعياً لتعزيز الأمن السيبراني، عملت المملكة على تحديث **قانون الجرائم الإلكترونية لعام ٢٠٠٧**، كما وقّعت وزارة التعليم اتفاقية مع **(NCA)** في اذار ٢٠٢١ لإطلاق برامج تدريبية وبحثية في مجال الأمن السيبراني. وتشمل هذه المبادرات **المنح الدراسية، وتطوير التعليم العالي، وتنفيذ مشاريع بحثية مشتركة**، مما يعزز الاستثمار في هذا المجال ضمن إطار **رؤية ٢٠٣٠**.منذ الهجوم السيبراني على **أرامكو السعودية**، تبنت المملكة استراتيجيات لتعزيز قدراتها الدفاعية، حيث زادت ميزانية الأمن السيبراني من **(7.8) مليار دولار في ٢٠١٢ إلى (27.2) مليار دولار في ٢٠٢٠**. كما أنشأت **المركز الوطني لتكنولوجيا الأمن السيبراني** عام ٢٠١٤ للبحث في أمن الشبكات والبرمجيات.على الصعيد الدولي، تتعاون السعودية مع منظمة **الأمم المتحدة، وجامعة الدول العربية، والولايات المتحدة الامريكية، وبريطانيا، والإمارات** لتعزيز الأمن السيبراني. وبسبب التوترات مع **إيران** وارتفاع الهجمات السيبرانية، أصبحت المملكة **الطرف الأكثر نشاطًا في مجلس التعاون الخليجي**، حيث تقود جهود توسيع التعاون الإقليمي في هذا المجال [٢].

من جهة اخرى ومن أجل تقليل المخاطر السيبرانية على الأصول المعلوماتية والتقنية على مستوى داخلي أو خارجي، عملت الهيئة الوطنية للأمن السيبراني على(١١٤) ضابط أساس للأمن السيبراني مقسم على خمسة مكونات رئيسة:

١. حوكمة الأمن السيبراني.

٢. تعزيز الأمن السيبراني.

٣. صمود الأمن السيبراني.

٤. الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية.

٥. الأمن السيبراني لأنظمة التحكم الصناعي [٣].

ثالثاً: أهمية الأمن السيبراني في سياق رؤية ٢٠٣٠ وبرنامج التحول الوطني: على الرغم من أن رؤية المملكة العربية السعودية ٢٠٣٠ من المتوقع أن تخلق سبلًا جديدة للنمو الاقتصادي والتنوع، لا تزال المملكة تواجه تحديات أمنية. ففي السنوات الأخيرة، تعرضت بنيتها التحتية الوطنية الحيوية لعدة هجمات، مما أثار مخاوف متزايدة بشأن الأمن السيبراني. وقد دفعت هذه التحديات المملكة إلى تعزيز أمنها السيبراني، وأصبح مستوى الجاهزية السيبرانية أحد مؤشرات الأداء الرئيسة لمبادرات التحول في جميع أنحاء البلاد.اتخذت المملكة العربية السعودية خطوات رئيسة للحد من التعرض المستقبلي لتهديدات الإنترنت، كما تبذل جهودًا متضافرة لمكافحة الإرهاب السيبراني. ووفقًا لاستطلاع في المملكة عام ٢٠١٩، أفاد(٨٥٪) من الرؤساء التنفيذيين المشاركين بأن الاستثمارات في الأمن السيبراني وحماية الخصوصية ستكون من التقنيات الحاسمة لدفع مبادرات التحول الرقمي في مؤسساتهم.تعترف خطط التنمية الوطنية ومبادرات التنويع بأن التقنيات الناشئة تُعدّ عاملاً أساسيًا في تحقيق التحول الشامل للصناعة. ومع ذلك، فإن تبني هذه التقنيات أدى إلى ظهور موجة جديدة من التهديدات السيبرانية التي تستهدف كلًا من القطاعين العام والخاص. ولذلك، تسعى المملكة إلى توجيه جهود إضافية نحو بناء القدرات السيبرانية وتعزيز قدرتها على تأمين التقنيات الداعمة لمبادرات التنويع، والتي تمثل القوة الدافعة وراء برنامج التحول الوطني [٤].

رابعاً: مستوى الامن السيبراني للمملكة: على الصعيد العالمي، من المتوقع أن تصل صناعة الأمن السيبراني إلى ما يقرب من (٣٦٦,١٠) مليار دولار بحلول عام ٢٠٢٨، ومن المتوقع أن تتبع الاتجاهات داخل المملكة العربية السعودية هذا النمط. من المتوقع أن ينمو سوق الأمن السيبراني في المملكة العربية السعودية بمعدل نمو سنوي مركب نسبته(١٢,٤٪) بين عامي ٢٠٢٠ و٢٠٢٦، مع وصول حجم السوق إلى(٢١) مليار ريال سعودي (٥,٦ مليار دولار أمريكي) بحلول نهاية عام ٢٠٢٣. احتلت المملكة بين العامين ٢٠١٦ و٢٠١٨، المرتبة السادسة على مستوى العالم باعتبارها الأكثر تضرراً من الهجمات السيبرانية. في العام ٢٠١٩، سجلت المملكة العربية السعودية والإمارات العربية المتحدة ثاني أعلى متوسط تكلفة لخرق البيانات بقيمة(٢٢,٤) مليون ريال سعودي (٥,٩٧ مليون دولار أمريكي)، وفقاً لتقرير صادر عن شركة (IBM)، في نفس العام، شهدت هاتان الدولتان الخليجيتان أيضاً أعلى متوسط لعدد السجلات المخالفة (٣٨٨٠٠) لكل حادثة مقارنة بالمعدل العالمي البالغ(٢٥٥٠٠) سجل لكل حادث [٥]. وفي مقابل ذلك سعت المملكة نحو تطوير قدراتها الامنية في المجال السيبراني حيث استطاعت وفقا لمؤشر الامن السيبراني للعام ٢٠٢٠ ان تحتل المرتبة الثانية بدرجة (٩٩,٥٤) بعد الولايات المتحدة الامريكية التي جاءت بالمرتبة الاولى عالمياً [٦]. والمرتبة الاولى في مؤشر الامن السيبراني للعام ٢٠٢٤[٧].

خامساً: مؤسسات الامن السيبراني في المملكة:

١. فريق الاستجابة لطوارئ الحاسوب(CERT): تأسس الفريق في العام ٢٠٠٦ باعتباره جهة رسمية ومرجع لأمن المعلومات بموجب هيئة الاتصالات وتقنية المعلومات. بدأ (CERT) بتقديم استشارات إدارة الحوادث الخدمات المقدمة للقطاعين العام والخاص لنشر الوعي بتأثير الهجمات الإلكترونية وأهمية الإبلاغ عن مثل هذه الحوادث. كان الهدف الأساس لمبادرة التوعية التابعة لفريق (CERT) تزويد المؤسسات بقدرات الكشف عن الحوادث السيبرانية والوقاية منها مع الوظائف التعليمية والتدريبية. تشمل خدمات (CERT) ما يلي: (١) تمكين المنظمات مع المهارات اللازمة للتخفيف من التهديدات الأمنية، وتضخيم الوعي بالأمن السيبراني من خلال حملات التدريب وضع مناهج جديدة للأمن السيبراني وبرامج تمكين للحكومة المنظمات من خلال التعاون مع الجامعات، ونشر المعلومات عن الحوادث السيبرانية.

٢. مركز التميز لأمن المعلومات(COEIA) – جامعة الملك سعود: تأسس المركز في العام ٢٠٠٩ كمركز غير ربحي يساهم في التنمية حلول الأمن السيبراني وتطبيق معايير الأمن السيبراني والاستشارات والتمكينات للصناعة والأكاديمية والقطاعات العامة. بصرف النظر عن الخدمات الاستشارية، فإن (COEIA) يشارك على نطاق واسع في البحث في مجال الأمن السيبراني ويتمتع بشهرة مبتكرة ومؤثرة حول المعلومات المتعلقة بالأمن السيبراني وحملات التوعية وبراءات الاختراع.

٣. المركز الوطني لتكنولوجيا الأمن السيبراني(KACST) –مدينة الملك عبدالعزيز للعلوم والتقنية: تأسس المركز في العام ٢٠١٤، في إطار مدينة الملك عبد العزيز للعلوم والتقنية مؤسسة بحثية مكثفة في مجالات أمن الشبكات وأمن التطبيقات، أمن المعلومات وحوكمة الأمن. يهدف المركز إلى تسخير إمكانات رأس المال البشري الوطني ويكون بمثابة محفز لإعداد أسس نجاح المملكة العربية السعودية وفقاً لرؤية ٢٠٣٠ من خلال مساهمة المهنيين الأكفاء في أبحاث الأمن السيبراني وقدرات التطبيق.

٤. المركز الوطني للأمن السيبراني (NCSC): تأسس المركز في العام ٢٠١٦، حيث عمل على تطوير حزمة من التقييمات التي تساعد المنظمات في تحديد مستوى الأمن وتحديد القضايا الأمنية وفقاً لمعايير الأمن السيبراني الدولية. هذا التقييم يمكن المنظمات من تحديد والتحقق من صحة وتقييم نقاط الضعف التقنية وتمكين فهم أعمق لتحسين الوضع الأمني للبنية التحتية لتكنولوجيا المعلومات. يوفر (NCSC) التوصيات الفنية والإرشادات بناءً على التقييم المذكور.

٥. الاتحاد العربي السعودي للأمن السيبراني والبرمجة والطائرات بدون طيار(SAFCSPD): تأسس الاتحاد في العام ٢٠١٨ كمؤسسة وطنية تحت مظلة المملكة العربية السعودية اللجنة الأولمبية تسعى لبناء القدرات الوطنية والمهنية في مجالات الأمن السيبراني والبرمجة وتقنيات الطائرات بدون طيار بما يتماشى مع التقنيات المعمول بها دولياً والممارسات والمعايير المعترف بها، لتسريع صعود المملكة العربية السعودية إلى مصاف الدول المتقدمة في مجال الابتكار التكنولوجي.

٦. **الهيئة الوطنية للأمن السيبراني(NCSA):** تم تأسيس الهيئة الوطنية للأمن السيبراني عام ٢٠١٧ بموجب توجيه ملكي، بهدف تعزيز الأمن السيبراني للدولة وحماية بنيتها التحتية الوطنية. وتماشياً مع رؤية المملكة العربية السعودية ٢٠٣٠ وبرنامج التحول الوطني (NTP)، تسعى الهيئة الوطنية للأمن السيبراني إلى تطوير وتعزيز القدرات السيبرانية الوطنية، مما يساهم على المدى الطويل في تحقيق النهضة التقنية المنشودة. بعد سلسلة من هجمات برامج الفدية التي استهدفت المنشآت السعودية عام ٢٠١٦، وأثرت على البنية التحتية والملكية الفكرية، إلى جانب تأثيرها على آلاف الأنظمة في القطاعات الحكومية، أدركت حكومة المملكة العربية السعودية الحاجة الملحة إلى تعزيز قدراتها في مجال الأمن السيبراني. لذلك، تم تفويض الجهود والمبادرات الخاصة بالأمن السيبراني الوطني إلى جهة مركزية لضمان تنظيمها وإدارتها بفعالية.يتمثل الهدف الأساس للهيئة الوطنية للأمن السيبراني في تحليل وصياغة وتنظيم وتفويض السياسات والأطر والمعايير والإرشادات المتعلقة بالأمن السيبراني، لضمان حماية الفضاء السيبراني الوطني وتعزيز جاهزيته لمواجهة التهديدات المستقبلية.

٧. **كلية (MBS) للأمن السيبراني والذكاء الاصطناعي والتقنيات المتقدمة:** تعكس الكلية رؤية القيادة الحالية للمملكة العربية السعودية، بقيادة **ولي العهد الأمير محمد بن سلمان**، لتعزيز **التدريب المهني** وبناء **القدرات الوطنية** في المجالات الأساسية مثل **الذكاء الاصطناعي، الأمن السيبراني، والتقنيات المتقدمة** وقد بدأت الكلية في تطوير برامج أكاديمية **وتعاون بحثي** مع **أرقى المؤسسات العالمية**، بهدف **تكثيف التدريب العلمي** وتعزيز **برامج البحث** لصقل **رأس المال البشري المحلي**. وتعد **كلية (MBS)** ثمرةً لهذه المبادرة الطموحة، حيث تسهم في **إعداد كوادر مؤهلة** تواكب التطورات التقنية الحديثة [٨].

سادساً: المؤسسات التعليمية للامن السيبراني في المملكة: يعد التعليم ركيزة اساسية لبناء قاعدة معرفية حول الامن السيبراني لذلك سعت المملكة كغيرها من الدول نحو بناء قاعدة تعلمية سيبرانية لتكون رافد اساس لها في بناء قدراتها السيبرانية البشرية والمعرفية، وفي هذا الإطار نجد العديد من المؤسسات البحثية والتعليمية التي تم تأسيسها لتحقيق هذه الهدف وهي كالتالي:

١. **الاكاديمية السعودية الرقمية:** إحدى مبادرات وزارة الاتصالات وتقنية المعلومات تهدف لبناء القدرات الرقمية الوطنية في مجالات التقنيات الحديثة المرتبطة بتقنيات الثورة الصناعية الرابعة ولتواكب متطلبات التحول الرقمي تنمية رأس المال البشري في القدرات الرقمية وربطه بمهن المستقبل في قطاع الاتصالات وتقنية المعلومات لإعداد جيل وقيادة شابة لمواكبة التطورات التقنية المرتبطة بالثورة الصناعية الرابعة، من خلال برامج نوعية متخصصة معدة وفق أحدث أساليب التدريب العملية والتطبيقي [٩].

٢. **الجامعات والكليات السيبرانية:** تخصص الامن السيبراني في جامعة الملك سعود وجامعة الامير سلطات وجامعة دار الحكمة، وكلية جدة الخاصة للامن السيبراني، وكلية الامن السيبراني والبرمجة والذكاء الاصطناعي [١٠]. وتمنح هذه الجامعات درجات علمية دبلوم وبكالوريوس في ثمانية تخصصات وهي [١١].

١) بكالوريوس العمليات السيبرانية.

٢) بكالوريوس الجرائم السيبرانية.

٣) بكالوريوس الذكاء الاصطناعي.

٤) دبلوم التحقيق في الجرائم السيبرانية.

٥) دبلوم الدفاع السيبراني.

٦) دبلوم البيانات الضخمة.

٧) دبلوم الاستجابة للحوادث السبرانية.

٨) دبلوم حوكمة الامن السيبراني.

ولم تكتفِ المملكة في تأسيس العديد من المؤسسات التعلمية السيبرانية وأنما نجدها قد عمدت الى انشاء وحدات للامن السيبراني داخل الجامعات تعمل على التثقيف بالأمن السيبراني وتقديم استشارات ورش تدريبة للطلاب والتدريسين حول مخاطر الجرائم السيبرانية فضلاً عن تقديم حلول لمعالجة الاختراقات السيبرانية وتسجيل براءات الاختراع في مجال الامن السيبراني [١٢].

سابعاً: التنظيم القانوني للامن السيبراني في المملكة: مع التوسع الكبير في الأنشطة الحياتية المختلفة داخل الفضاء السيبراني، وما يترتب عليها من جرائم سيبرانية تهدد الأمن الداخلي للأفراد والمجتمعات، أدركت الدول، سواء المتقدمة أو النامية، خطورة هذا التحدي وأهميته. لذلك، سعت إلى وضع القوانين والتشريعات اللازمة لحماية أمنها الداخلي وتعزيز السلامة المجتمعية وفي هذا الإطار سعت المملكة العربية السعودية على وضع قانون جرائم المعلومات في العام ٢٠٠٧. والذي يهدف إلى الحد من انتشار جرائم المعلوماتية عبر الإنترنت، ومعاقبة المجرمين السيبرانين لحماية الأفراد والمؤسسات. حيث فرض النظام المقر من مجلس الوزراء، عقوبة بالسجن لمدة لا تزيد عن سنة، وغرامة مالية لا تزيد على(٥٠٠) ألف ريال سعودي على كل شخص يرتكب أياً من الجرائم المنصوص عليها في النظام، والتي جاءت كالآتي [١٣]:

١. التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي – دون مسوغ نظامي صحيح – أو التقاطه أو اعتراضه.

٢. الدخول غير المشروع لتهديد شخص أو ابتزازه؛ لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعًا.

٣. الدخول غير المشروع إلى موقع إلكتروني، أو الدخول إلى موقع الكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه.

٤. المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا، أو ما في حكمها

٥. التشهير بالآخرين وإلحاق الضرر بهم، عبر وسائل تقنيات المعلومات المختلفة.

وفرض النظام عقوبة السجن مدة لا تزيد على (١٠) سنوات وبغرامة لا تزيد على (٥) ملايين ريال أو بإحداهما على كل شخص يقوم بالآتي:

١. نشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره؛ لتسهيل الاتصال بقيادات تلك المنظمات، أو أي من أعضائها أو ترويج أفكارها أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرات، أو أي أداة تستخدم في الأعمال الإرهابية.

٢. الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني.

ومع صدور هذا النظام الذي يسعى إلى تحقيق توازن ضروري بين مصلحة المجتمع في الاستعانة بالتقنية الحديثة ومصلحة الإنسان في حماية حياته الخاصة والحفاظ على أسراره، والمساعدة على تحقيق النظام المعلوماتي وحفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية، كما يهدف إلى حماية المصلحة العامة والأخلاق والآداب العامة وكذلك حماية الاقتصاد الوطني [١٤].

الخاتمة:

بناء القدرات السيبرانية يمثل تحديًا أساسيًا لأي دولة تسعى إلى أن تكون فاعلة ومؤثرة في الفضاء السيبراني. ومن هذا المنطلق، سعت العديد من الدول إلى تبني السياسات ووضع الاستراتيجيات اللازمة لتطوير قدراتها السيبرانية. وفي منطقة الشرق الأوسط، هناك العديد من الدول التي تعمل على تعزيز أمنها السيبراني، مثل إيران وتركيا والإمارات العربية المتحدة، بالإضافة إلى المملكة العربية السعودية، التي جعلت من بناء قدراتها السيبرانية أولوية استراتيجية.

وقد ازدادت هذه الجهود بشكل ملحوظ بعد الهجمات السيبرانية التي تعرضت لها المملكة، وأبرزها الهجوم الذي استهدف شركة أرامكو في العام ٢٠١٢، والذي تسبب في أضرار مادية كبيرة. دفع ذلك المملكة إلى توفير البنية التحتية المعرفية والمادية المطلوبة لتعزيز أمنها السيبراني، مما مكّنها من تحقيق تقدم ملحوظ واحتلال المرتبة الاولى عالميًا في مؤشر الأمن السيبراني.

وفي هذا السياق، فإن العراق بحاجة ماسة إلى الاستفادة من التجربة السعودية في بناء بنية سيبرانية متطورة، تمكنه من تعزيز حضوره في الفضاء السيبراني وحماية أمنه الوطني من التهديدات المتزايدة.

الهوامش:

(1) ALEKsandER OLech Cybersecurity in Saudi Arabia, September 3, 2021,https://www.cyber-insights.org/cybersecurity-in-saudi-arabia/-12-9-2022.
(2) Dr. Aleksander Olech, Cybersecurity in Saudi Arabia, Op, Cit.
(3) https://www.my.gov.sa/wps/portal/snp/content/cybersecurity.12-9-2022.
(4)Cybersecurity and its impact on digital Saudi, https://resources.trendmicro.com/rs/945-CXD-062/images/Cybersecurity-and-its-Impact-on-Digital-Saudi.pdf.
(5) Ahmad Al Zoubi, The Future Of Cyber Security In Saudi Arabia, 21 Mar 2022, https://www.grantthornton.sa/en/insights/articles-and-publications/future_cybersecurity/
(6) Global cybersecurity index 2020, International telecommunication union,2020,p25.
(7) Global cybersecurity index 2024, International telecommunication union,2024.p77.
(8) Amanullah Quadri &Muhmmad Khurram Khan, CYBERSECURITY CHALLENGES OF THE KINGDOM OF SAUDI ARABIA, Past, Present Future, Global Foundation for Cyber Studies and Research, JANUARY, 2019, PP4-5.
(9) https://sda.edu.sa/#features,18-9-2022.
(10) https://www.almnsa.com/post/58370,18-9-2022.
(11) https://www.almuheet.net/post/366997,18-9-2022.

(١٢) د. الجوهرة بنت عبد الرحمن ابراهيم المنيع متطلبات تحقيق الامن السيبراني في الجامعات السعودية... في ضوء رؤية ٢٠٢٣، المجلة العلمية لكلية التربية، جامعة اسيوط –كلية التربية، المجلد ٣٣، العدد الاول، يناير ٢٠٢٢، ص١٦٥.

(١٣) نظام مكافحة جرائم المعلوماتية،
https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/25df73d6-0f49-4dc5-b010-a9a700f2ec1d/

(١٤) سارة سمير، (كل ما تريد معرفته حول) الجرائم الإلكترونية أو الجرائم المعلوماتية،
https://www.alroeya.com/9-34/2186157

المصادر:

١) د. الجوهرة بنت عبد الرحمن ابراهيم المنيع، متطلبات تحقيق الامن السيبراني في الجامعات السعودية... في ضوء رؤية ٢٠٢٣، المجلة العلمية لكلية التربية، جامعة اسيوط –كلية التربية، المجلد ٣٣، العدد الاول، يناير ٢٠٢٢، ص ١٦٥.
٢) سارة سمير، (كل ما تريد معرفته حول) الجرائم الإلكترونية أو الجرائم المعلوماتية،
https://www.alroeya.com/9-34/2186157
٣) نظام مكافحة جرائم المعلوماتية:
https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/25df73d6-0f49-4dc5-b010-a9a700f2ec1d/1
4) Almuheet. (2022, September 18). [Article title]. https://www.almuheet.net/post/366997

5) Almnsa. (2022, September 18). [Article title]. https://www.almnsa.com/post/58370
6) Al Zoubi, A. (2022, March 21). The future of cyber security in Saudi Arabia. Grant Thornton. https://www.grantthornton.sa/en/insights/articles-and-publications/future_cybersecurity/
7) Cybersecurity and its impact on digital Saudi. (n.d). Trend Micro. https://resources.trendmicro.com/rs/945-CXD-062/images/Cybersecurity-and-its-Impact-on-Digital-Saudi.pdf
8) Global cybersecurity index 2020. (2020). International Telecommunication Union.
9) Global cybersecurity index 2024. (2024). International Telecommunication Union.
10) Olech, A. (2021, September 3). Cybersecurity in Saudi Arabia. Cyber Insights. https://www.cyber-insights.org/cybersecurity-in-saudi-arabia/
11) Quadri, A., & Khan, M. K. (2019). Cybersecurity challenges of the Kingdom of Saudi Arabia: Past, present, and future. Global Foundation for Cyber Studies and Research.
12) Saudi Digital Academy. (n.d.). https://sda.edu.sa/#features
13) Saudi Government Portal. (n.d). Cybersecurity. https://www.my.gov.sa/wps/portal/snp/content/cybersecurity