



إيمان عبد القادر

باحثة بمركز المعلومات ودعم اتخاذ القرار - مجلس الوزراء - مصر

أثر الفضاء السيبراني

على الأمن القومي العربي خلال الفترة من ٢٠١١ حتى ٢٠٢٣

مقدمة :

الفضاء السيبراني "Cyber Space" أحد الأشكال الجديدة لمفهوم القوة والتعبير عن مفرداتها، بما يُمكن المقتدرفيه من استخدامه بطريقة تضمن مصالحه وأمنه القومي (١)، ونتيجة هذه الاستخدامات وتحول الإنترنت إلى بنية تحتية عالمية للنشاطات المدنية، وإلى وسيلة جديدة للضغط السياسي والتجسس، بالإضافة إلى تأثير الفضاء السيبراني على الأمن القومي في كل مجالاته، تصدر الأمن السيبراني المراكز الأولى في سياسات واستراتيجيات الدول للحفاظ على نظامها وأمنها القومي (٢).

- التعرف على الموقف الحالي للأمن السيبراني في الدول العربية.

منهج الدراسة :

تم الاعتماد على المنهج الوصفي للتعرف على تأثير الفضاء السيبراني على الأمن القومي العربي في مجالاته السياسية والأمنية والاقتصادية والاجتماعية، وتوضيح الوضع الحالي للدول العربية في مؤشرات الأمن السيبراني.

محتويات الدراسة :

- ١- العلاقة النظرية بين الفضاء السيبراني والأمن القومي.
- ٢- تأثير الفضاء السيبراني على مجالات الأمن القومي العربي.
- ٣- الموقف الحالي للأمن السيبراني في الدول العربية.
- ٤- نتائج الدراسة.

أولاً: العلاقة النظرية بين الفضاء السيبراني والأمن القومي:

أدى ظهور الفضاء السيبراني بما يحمل من أدوات تكنولوجية تلعب دوراً مهماً في عملية التعبئة والحشد، إلى التأثير في القيم السياسية مثل القوة، والحرب، والأمن (٥)،

برز دور الفضاء السيبراني عبر مواقع التواصل الاجتماعي في إدارة الصراع السياسي في الدول العربية، وظهر تفاوت في استخدام الفضاء السيبراني وفق طبيعة التطور التقني وقدرة النظام على إدارة الصراع الإعلامي، والتأثير في الرأي العام وتعبئة وحشد الجمهور (٣)، فضلاً عن أن مواقع التواصل الاجتماعي كانت وسيلة جيدة للجماعات الإرهابية من أجل تجنيد أعضاء جدد وجمع التمويل ونشر آرائهم المتطرفة وتنفيذ عملياتهم في المنطقة العربية، أيضاً تعرضت العديد من المواقع الخاصة بجهات أمنية عربية، ووزارات وشركات مهمة إلى هجمات سيبرانية وتوقف العمل فيها لعدة ساعات (٤).

أهداف الدراسة :

- التعرف على العلاقة النظرية بين مفهومى الفضاء السيبراني، والأمن القومي.
- تناول دور الفضاء السيبراني في التأثير على الأمن القومي العربي في جميع مجالاته (السياسية والعسكرية والاقتصادية والاجتماعية).



إيمان عبد القادر

كذلك اتسع مجال الأمن ليمتد من الجانب العسكري لمجالات أخرى عديدة (٦).

١- مفهوم الفضاء السيبراني:

كلمة *Cyper* مشتقة من الفعل اليوناني *Kubernao* الذى يعنى يقود، ويُعد وليام جيبسون أول من استخدم كلمة *Cyper* مقترنة بكلمة *Space* ليتكون مفهوم الفضاء السيبراني *Cyper Space* فى كتابه الكلاسيكى عام ١٩٨٤، وجاءت جهود نيل ستيفسون عام ١٩٨٩ ليرسما معاً صورة تكاد تكون شاملة عن ماهية ذلك المفهوم التى تحددت فى أنه ذلك الفضاء أو المحتوى والبديل الكونى الذى يمكن من خلاله للناس أن تشارك فيه (٧).

تعددت تعريفات الفضاء السيبراني وسيتم الاستناد إلى تعريف وزارة الدفاع الأمريكية للفضاء السيبراني بأنه «مجال يتميز باستخدام الإلكترونيات والطيف الكهرومغناطيسى لتخزين وتعديل وتبادل البيانات عبر أنظمة الإنترنت والبنى التحتية المادية المرتبطة بها» (٨).

تتكون تركيبة الفواعل فى الفضاء السيبراني من الدول التى تُعدُّ فاعلاً محورياً فى تسيير الفضاء السيبراني، انطلاقاً من إمكاناتها المادية والبنوية والبشرية والقانونية، إلى جانب فواعل أخرى أبرزها المنظمات الحكومية، والمنظمات غير الحكومية التى تعتمد بشكل كبير على الإنترنت فى تعبئة الرأي العام، والضغط على الحكومات (٩). كذلك المنظمات الإجرامية التى تقوم بعمليات القرصنة السيبرانية، وسرقة المعلومات، والجماعات الإرهابية التى تستغل الفضاء السيبراني فى عمليات التجنيد والدعاية وجمع الأموال (١٠).

٢- مفهوم الأمن القومى:

تقليدياً كان يُعرّف الأمن القومى على أنه دفاعات عسكرية فى مواجهة تهديدات عسكرية، وثبت أن هذه الرؤية ضيقة، وأدى ذلك إلى ضرورة صياغة تعريف أوسع للأمن القومى، ومن ثمَّ تعددت تعريفات الأمن القومى، وفى دراسة لمؤسسة *Heritage* وهى مؤسسة فكرية أمريكية محافظة مقرها واشنطن، وتُعدُّ من أكثر منظمات السياسة العامة تأثيراً فى الولايات المتحدة، قامت بتعريف الأمن القومى بأنه «حفظ الأمة من أى هجوم أو أخطار خارجية وحماية القوات المسلحة وحماية أسرار الدولة، وحماية الأمن الداخلى وسلسلة من المصالح الجيوسياسية والاقتصادية وغيرها».

تعددت مجالات الأمن القومى، فهناك المجال السياسى الذى يتمثل فى الحفاظ على وحدة وسلامة أراضى الدولة من أى تهديدات داخلية أو خارجية، والمجال الاقتصادى الذى يتمثل فى تنمية الموارد الاقتصادية للدولة وتحقيق التنمية الاقتصادية المستدامة (١١)، والمجال الاجتماعى يتمثل فى قدرة الدولة على حماية قيمها الأيديولوجية (١٢)، والمجال العسكرى/ الأمنى ويتمثل فى تقوية القدرات العسكرية للدولة، أيضاً المجال السيبراني الذى يتمثل فى الإجراءات والتقنيات التى تستخدمها الدولة بهدف حماية أنظمتها الإلكترونية المختلفة من الهجمات الإلكترونية (١٣).

• مفهوم الأمن القومى العربى:

هناك فجوة كبيرة بين مفهوم الأمن القومى فى النظام العربى الرسمى وبين الممارسة الفعلية (١٤)، إلا أن الأمانة العامة لجامعة الدول العربية قامت بتعريفه فى دراسة أعدتها عام ١٩٩٢ بأنه «قدرة الأمة على الدفاع عن أمنها، وحقوقها، وصياغة استقلالها، وسيادتها على أراضيها، وتنمية القدرات والامكانات العربية، فى مختلف المجالات السياسية والاقتصادية والثقافية والاجتماعية، مستندة إلى القدرة العسكرية والدبلوماسية، أخذة فى الاعتبار الاحتياجات الأمنية الوطنية لكل دولة، والامكانات المتاحة، والمتغيرات الداخلىة والإقليمية والدولية، التى تؤثر على الأمن القومى العربى» (١٥).

• مفهوم الأمن السيبراني:

أدى الاعتماد على الفضاء السيبراني، وتأثيره على الأمن القومى إلى ظهور مفهوم الأمن السيبراني *Cyper Security* (١٦)، وتعرّفه وزارة الدفاع الأمريكية بأنه «جميع الإجراءات التنظيمية المطلوبة لضمان حماية أمن المعلومات بجميع أشكالها (الإلكترونية والمادية)، وأمن الأنظمة والشبكات حيث يتم تخزين المعلومات والوصول إليها ومعالجتها ونقلها، بما فى ذلك الاحتياطات المُتخذة للوقاية من الجريمة والهجوم والتخريب والتجسس والحوادث» (١٧).

٣. العلاقة بين الفضاء السيبراني والأمن القومى

هناك تأثير كبير للفضاء السيبراني على مجالات الأمن القومى المختلفة وسيتم تناول كل منها كالتالى:

أ- تأثير الفضاء السيبراني على المجال السياسى يكون ذلك من خلال إدارة العمليات النفسية والتأثير فى رأى العام وتكوين التحالفات الدولية (١٨)، وتُعدُّ مواقع التواصل الاجتماعى من أبرز الأدوات المستخدمة

استخدامها امتد ليشمل أنشطة ومجالات أخرى كالنشاط السياسي وعسكرية وغيرها من المجالات (٢٧)، كذلك برزت مخاطر أمنية وعسكرية من نمط جديد نتيجة انتشار الفضاء السيبراني وتكاثر أدواته (٢٨)، حيث تعرضت العديد من الدول العربية إلى هجمات سيبرانية (٢٩).

١- تأثير الفضاء السيبراني

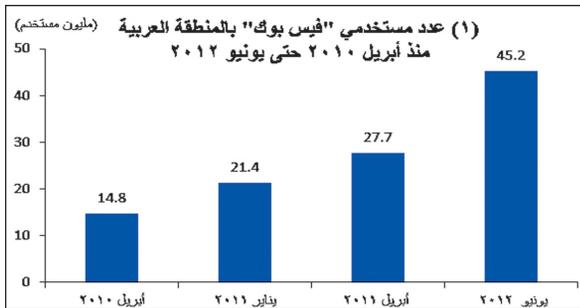
على المجال السياسي العربي

برز التأثير السياسي للفضاء السيبراني في الثورات العربية عبر مواقع التواصل الاجتماعي، حيث ازداد استخدامها في التأثير على الرأي العام وتعبئة وحشد الجمهور (٣٠)، ولم يقتصر دورها خلال الثورات العربية، وإنما ما بعد الثورات من عدم وجود استقرار سياسي لهذه الدول (٣١).

أ- دور مواقع التواصل الاجتماعي في الثورات العربية
النمو الذي شهدته مواقع التواصل الاجتماعي في المنطقة كان له الدور الأكبر والفاعل في تكوين وجهات النظر والأفكار لنشوء الثورات العربية، كذلك لعبت تلك المواقع دوراً كبيراً في تغيير نمطية تفكير الشعوب وتمكينهم من تكوين أفكار ومعتقدات فاعلة، نتيجة لوفرة المعلومات (٣٢).

الدعوة إلى المظاهرات والاحتجاجات التي شهدتها العديد من الدول العربية، منذ نهاية عام ٢٠١٠ كانت تتم عبر مواقع التواصل الاجتماعي، وبخاصة «فيس بوك» و«تويتر»، وكذلك من خلال المدونات التي كان لها دور كبير في كشف العديد من أوجه الخلل ومظاهر القصور في أداء بعض الحكومات العربية، وبخاصة قضايا الفساد السياسي وغياب الشفافية والعدالة الاجتماعية (٣٣).

زاد عدد مستخدمي الإنترنت في الوطن العربي عام ٢٠١١ بنسبة ٩، ١٢٪ ليصل إلى ٩٦ مليون مستخدم مقارنة بـ ٨٥ مليون مستخدم عام ٢٠١٠ (٣٤)، وتضاعف عدد مستخدمي «فيس بوك» خلال فترة الثورات في المنطقة العربية.



(١) عدد مستخدمي «فيس بوك» بالمنطقة العربية منذ أبريل ٢٠١٠ حتى يونيو ٢٠١٢ (٣٥)

في الفضاء السيبراني لإدارة العمليات النفسية والتأثير في الرأي العام، وتنقسم إلى شبكة الإنترنت وتطبيقاتها، مثل «فيس بوك» و«تويتر» و«اليوتيوب» والمدونات، ومواقع الدردشة، وتطبيقات قائمة على الأدوات المحمولة المختلفة ومنها أجهزة الهاتف الذكية، ومواقع التواصل الاجتماعي للقنوات والإذاعات (١٩).

ب- تأثير الفضاء السيبراني على المجال العسكري / الأمن

أحدث عصر المعلومات تحولاً كبيراً في مفهوم القوة ترتب عليه دخول الفضاء السيبراني ضمن المحددات الجديدة للقوة (٢٠)، وتحول إلى بيئة جديدة للنزاع وتحولت الحروب من تقليدية إلى سيبرانية (٢١). يمكن تحديد أهداف استخدام الفضاء السيبراني في النزاع في تأثير فاعل على سلوكيات فاعل آخر ودفعه للقيام بأعمال لم يكن ليقوم بها كما في حالة استهداف البنية التحتية للدولة من خلال نشر فيروسات تدمر أجهزة الدولة، كذلك قدرة الفاعل على التحكم في أجندة الآخرين، وترتيب أولويات الفواعل الأخرى (٢٢).

ج- تأثير الفضاء السيبراني على المجال الاجتماعي

قد يتحول الفضاء السيبراني في بعض الأحيان إلى وسيلة أيديولوجية تسعى إلى دفع الأفراد للتفكير بطريقة محددة، ومسيرة معايير وقيم ومعتقدات جديدة (٢٣). ويظهر ذلك في استخدام مواقع التواصل الاجتماعي من قبل الجماعات الإرهابية لنشر وإدارة الدعاية الإرهابية لتوصيل رسالتهم وتبرير أفعالهم، في سياق حرب المعلومات وإدارة العمليات النفسية (٢٤).

د- تأثير الفضاء السيبراني على المجال الاقتصادي

تعرض المؤسسات الكبرى لهجمات سيبرانية يكون له آثار اقتصادية خطيرة؛ لأن تكلفة استعادة السيطرة على النظم الإلكترونية عالية جداً (٢٥)، كذلك فإن أي هجمة ناجحة على مؤسسة مالية كبرى أو خدمة يستخدمها الكثير يمكن أن تنتشر تداعياتها سريعاً في النظام المالي بأسره، مما يؤدي إلى اضطراب واسع الانتشار ويتسبب في فقدان الثقة، ومن الممكن أن تقشل المعاملات نظراً لحبس السيولة (٢٦).

ثانياً: تأثير الفضاء السيبراني على مجالات الأمن القومي العربي؛

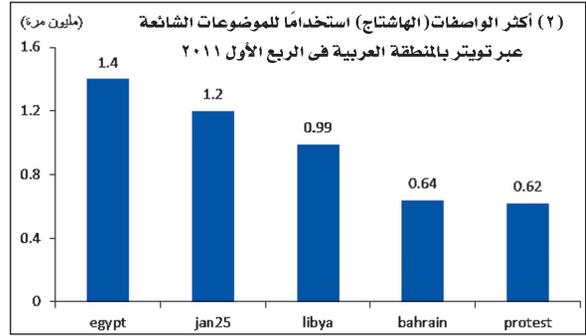
أكدت الثورات العربية أهمية تقنيات الاتصال الحديثة، لاسيما مواقع التواصل الاجتماعي، فعلى الرغم من أن هذه المواقع أنشئت بالأساس للتواصل بين الأفراد، فإن



أثر الفضاء السيبراني على الأمن القومي العربي خلال الفترة من ٢٠١١ حتى نوفمبر ٢٠٢٣

إيمان عبد القادر

بينما قُدِّر عدد مستخدمي «تويتر» النشطين في المنطقة العربية في نهاية مارس ٢٠١١ بـ ٢,١ مليون مستخدم، وكان عدد التغريدات التي أنتجها هؤلاء المستخدمون النشطون ٨,٢٢ مليون رسالة تويت في الربع الأول عام ٢٠١١.



أكثر الوصفات (المهاشاج) استخداماً للموضوعات الشائعة عبر تويتر بالمنطقة العربية في الربع الأول ٢٠١١ (٣٦)

العامة، إلا أنه يساء توظيفها بصورة تهدد الأمن والسلم في الدول العربية، خاصة أنها لا تخضع لأطر أو قوانين تضبط المحتوى الذي يتم نشره عليها، وتحولت في الآونة الأخيرة إلى أداة تساعد التنظيمات المتطرفة في نشر الأفكار الهدامة والتحريض على العنف والكرهية، وفي نشر الشائعات وإثارة الفوضى (٤٠).

٢. تأثير الفضاء السيبراني على المجال الأمني العربي

برزت مخاطر أمنية وعسكرية من نمط جديد نتيجة انتشار الفضاء السيبراني وتكاثر أدواته (٤١)، حيث تعرضت العديد من الدول العربية إلى هجمات سيبرانية، كما قام الموساد الإسرائيلي باختراق نظم الاتصالات في دول عربية والتجسس عبر الإنترنت، كما قامت إيران بشن هجمات سيبرانية على منشآت نفطية في الخليج العربي احتجاجاً على السياسات التمييزية ضد الشيعة ورداً على الهجمات السيبرانية الأمريكية الإسرائيلية التي استهدفتها (٤٢).

كذلك فإن التنظيمات الإرهابية تستخدم الإنترنت في مجموعة واسعة ومتنوعة من الأغراض، تشمل التجنيد، والتدريب، والتحريض على ارتكاب أعمال إرهابية، وجمع المعلومات، وتيسير الاتصال داخل التنظيمات الإرهابية، وتقديم الدعم المالي (٤٣).

ويظهر ذلك في استمرار «الخلافة الافتراضية» لجماعة «داعش»، على الرغم من انهيار الجماعة في العراق، وجزء كبير من سوريا، وصرح المفوض الأوروبي للاتحاد الأمني جوليان كينج بأنه على الرغم من تعرض «داعش» لضربة كبيرة في كل من العراق وسوريا، فإنه لا يزال نشطاً على الإنترنت ويعزز أيديولوجياته (٤٤).

٣- تأثير الفضاء السيبراني

على المجال الاجتماعي العربي

يستخدم الإرهابيون الإنترنت لبت دعايتهم، في شكل تعاليم أيديولوجية أو إرشادات، أو تقدم شروحاتاً للنشطة الإرهابية أو تسوق المبررات لها أو تشجع على القيام بها، وقد تشمل الأهداف الأخرى للدعاية الإرهابية التأثير على نفسية الفرد لإضعاف إيمانه ببعض القيم الاجتماعية، أو لبت الذعر في المجتمع (٤٥).

بدأت حركة الشباب الصومالية في استخدام تويتر باللغة الإنجليزية في وقت مبكر من ٢٠١١ (٤٦)، وفي تونس توجد مؤسسة «القيروان الإعلامية» في شكل صفحة رسمية على

أما المدونات العربية فقد ظهرت في ٢٠٠٤ وزاد انتشارها وتأثيرها عام ٢٠٠٥، وقد لعب المدونون دوراً بارزاً في الدفع نحو التغيير وزيادة الوعي السياسي، خاصة بين الشباب في دول مثل مصر وتونس وسوريا، كذلك أسهم «اليوتيوب» في الكشف عن ممارسات الحكومات وفضح وقائع القمع والتعذيب وترويع المتظاهرين خلال الثورات العربية وقبلها، ما أسهم في تأجيج الجماهير وتعبئتهم، وتزويد المحطات التلفزيونية بالأحداث اليومية في الميدان (٣٧).

ب- تأثير مواقع التواصل الاجتماعي

في مرحلة ما بعد الثورات

استمر دور مواقع التواصل الاجتماعي في مرحلة ما بعد الثورات نتيجة التزايد المستمر في أعداد مستخدمي الإنترنت، ووفقاً للاتحاد الدولي للاتصالات ارتفع عدد المستخدمين العرب بنسبة ٦,٢٤٠% عام ٢٠٢٢ مقارنة بعام ٢٠١١، ليصل إجمالي المستخدمين إلى ٢٢٧ مليون مستخدم (٣٨)، والتزايد المستمر في أعداد مستخدمي مواقع التواصل الاجتماعي، حيث وصل عدد المستخدمين في الوطن العربي إلى أكثر من ٥٠% من عدد سكان الدول العربية عام ٢٠١٩، حسب مؤسسة «هوتسويت الكندية» (٣٩).

في الوقت الذي تلعب فيه مواقع التواصل الاجتماعي العديد من الأدوار الإيجابية، سواء فيما يتعلق بتسمية الوعي والتأثير في الرأي العام والدفاع عن قضايا الحريات

ثالثاً: الموقف الحالي للأمن السيبراني في الدول العربية

سيتم تناول وضع الدول العربية في المؤشرات الدولية للأمن السيبراني وجاهزية الشبكات، وذلك لتوضيح الوضع الحالي والتهديدات التي تواجه الدول العربية في هذا المجال ومحاولة إيجاد حلول لها.

١- وضع الدول العربية في المؤشرات الدولية الخاصة بالأمن السيبراني

صمّمت العديد من المؤسسات العالمية مؤشرات لقياس الأمن السيبراني ومدى جاهزية واستعداد الدول لاستخدام الفضاء السيبراني، وسيتم عرض وضع الدول العربية في مجموعة من هذه المؤشرات.

أ- ترتيب الدول العربية

في مؤشر الأمن السيبراني عام ٢٠٢٠

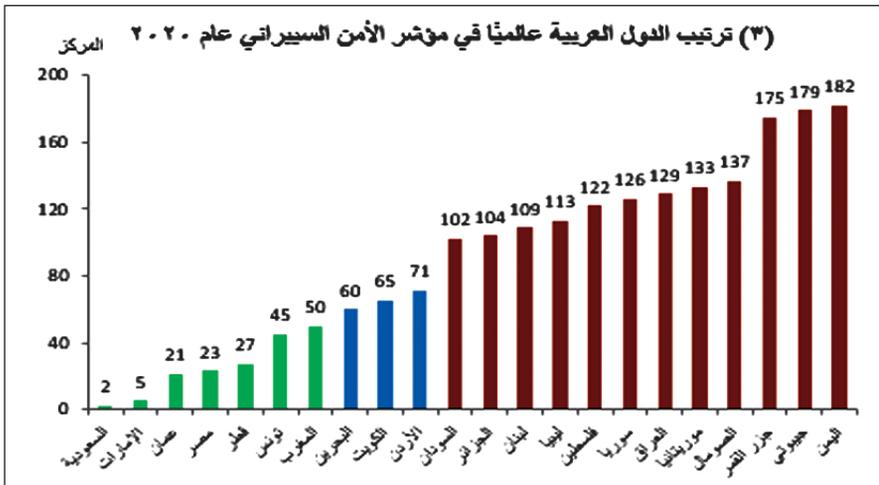
يقيس مستوى التزام الدول بالأمن السيبراني، من خلال خمس ركائز هي العوامل القانونية والفنية والترتيبات التنظيمية وبناء القدرات والتعاون، ويمكن تصنيف الدول العربية وفقاً للمؤشر إلى دول أظهرت مستويات عالية من الالتزام إزاء جميع الركائز وهي (السعودية والإمارات وعمان ومصر وقطر وتونس والمغرب)، وهي من أفضل ٥٠ دولة عالمياً في المؤشر، ودول طوّرت التزامات معقدة ومنخرطة في برامج ومبادرات للأمن السيبراني وهي (البحرين والكويت والأردن)، وأخيراً دول بدأت في تنفيذ التزامات في مجال الأمن السيبراني وهي (السودان والجزائر وليبيا وفلسطين وسوريا والعراق وموريتانيا والصومال وجزر القمر وجيبوتي واليمن).

«فيس بوك»، تقوم ببث ونشر بيانات تنظيم «أنصار الشريعة»، الذي يضم شباب التيار الجهادي التونسي، وفي العراق وسوريا، نشط تنظيم داعش اعتماداً على مواقع التواصل الاجتماعي (٤٧)، حيث أدار من خلالها حملة متعددة اللغات غيرت النظرة للتنظيم من منظمة جهادية صغيرة ووحشية لعلامة تجارية مرادفة للعالمية والإسلام السلفي، وأصبح معروفاً لدى كل بيت (٤٨).

٤. تأثير الفضاء السيبراني على المجال الاقتصادي العربي

تعرضت الشركات العربية والبنى التحتية الحيوية مثل شبكات الكهرباء إلى العديد من الهجمات السيبرانية، ما أدى إلى خسائر مالية وشكلت ضربة قوية لاقتصادات المنطقة (٤٩). ولعل أبرزها تمكن مجرمي الإنترنت من القرصنة على أحد البنوك الإماراتية ومطالبتهم بدفع الفدية بالعملة الرقمية "Bit Coin" في مقابل عدم تسريب المعاملات المالية السرية وتفاصيل العميل عام ٢٠١٥، كذلك تمكن متسللون من سرقة بيانات من حسابات بنك "QNB" القطري ونشرها على الإنترنت (٥٠).

أيضاً شهدت شركة أرامكو السعودية أكبر هجوم سيبراني لها في ٢٠١٢، عطل غالبية عمليات الشركة التجارية، واستغرق الأمر ما يقرب من خمسة أشهر لإعادة تشغيل أنظمة الشركة (٥١). وفي عام ٢٠١٧، تكرر الهجوم على الشركة (٥٢)، وكان المنتدى الاقتصادي العالمي حذر من الاحتمال المتزايد للهجمات السيبرانية في منطقة الخليج خاصة السعودية والإمارات وقطر (٥٣).



ترتيب الدول العربية
عالمياً في مؤشر الأمن
السيبراني عام ٢٠٢٠ (٥٤)

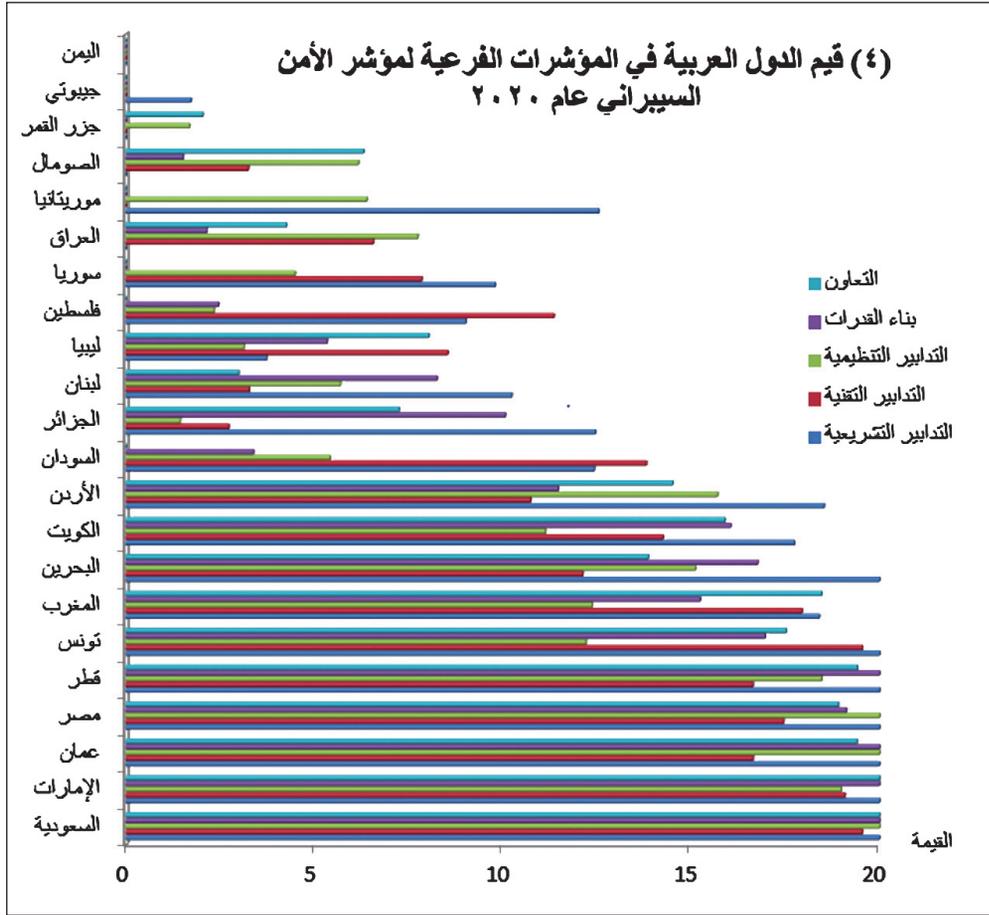


أثر القضاء السيبراني على الأمن القومي العربي خلال الفترة من ٢٠١١ حتى نوفمبر ٢٠٢٣

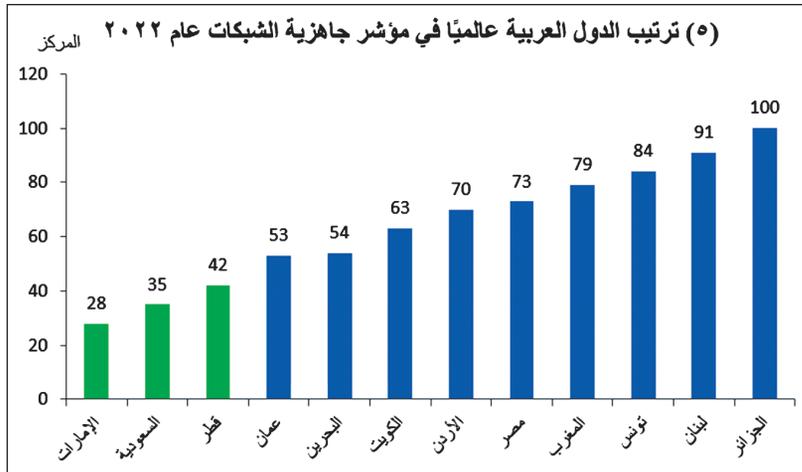
إيمان عبد القادر

القسم الأول

دراسات استراتيجية



قيم الدول العربية في المؤشرات الفرعية لمؤشر الأمن السيبراني عام ٢٠٢٠ (٥٥)

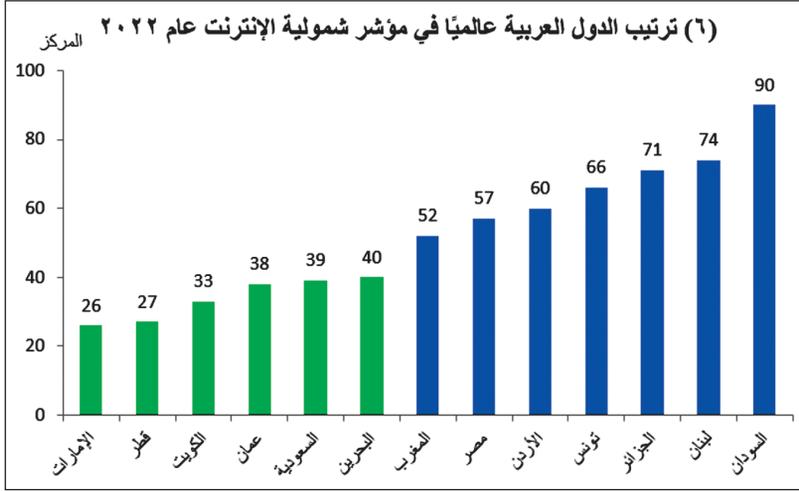


ترتيب الدول العربية عالمياً في مؤشر جاهزية الشبكات عام ٢٠٢٢ (٥٦)

ب- ترتيب الدول العربية في مؤشر

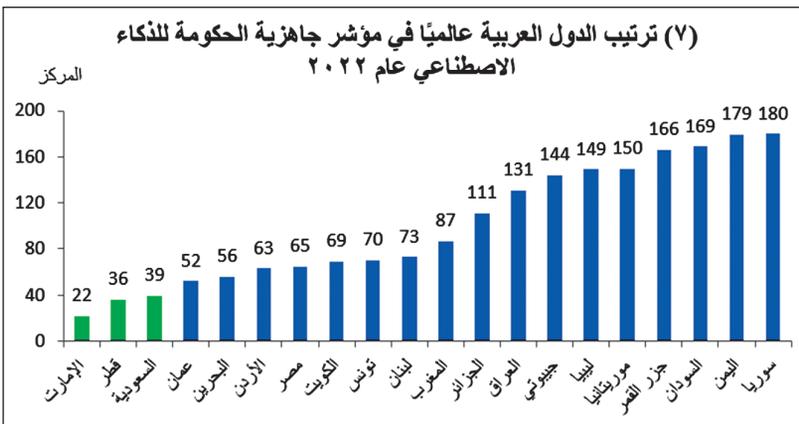
جاهزية الشبكات عام ٢٠٢٢

يقيم مدى استعداد الدول للاستفادة من تقنيات المعلومات وفقاً لـ ٤ جوانب هي التكنولوجيا والأشخاص والحوكمة والتأثير.



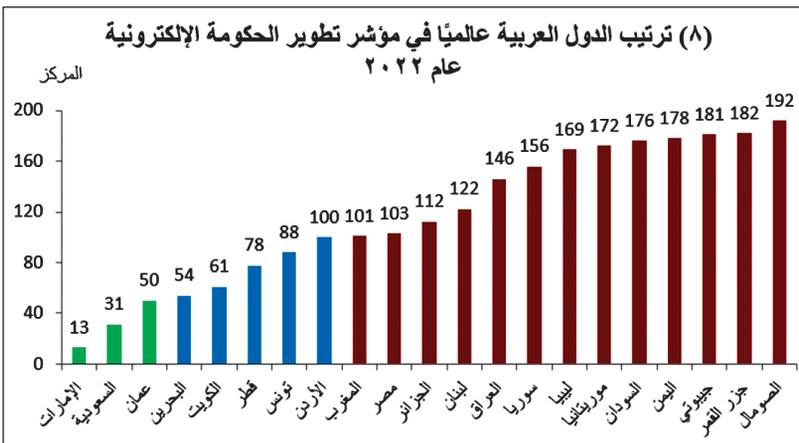
ترتيب الدول العربية عالمياً في مؤشر شمولية الإنترنت عام ٢٠٢٢ (٥٧)

ج- ترتيب الدول العربية في مؤشر شمولية الإنترنت عام ٢٠٢٢ يقيّم مدى توافر الإنترنت، والقدرة على تحمل تكاليفه، ومدى ملاءمة المحتوى، وتوافره باللغة المحلية وجاهزية الأفراد لاستخدامه.



ترتيب الدول العربية عالمياً في مؤشر جاهزية الحكومة للذكاء الاصطناعي عام ٢٠٢٢ (٥٨)

د- ترتيب الدول العربية في مؤشر جاهزية الحكومة للذكاء الاصطناعي عام ٢٠٢٢ يقيس مدى استعداد الحكومات لاستخدام تقنيات الذكاء الاصطناعي في تقديم الخدمات لمواطنيها، من خلال ٣٣ مؤشراً، أبرزها وجود استراتيجية وطنية للذكاء الاصطناعي، والبنية التحتية للاتصالات، وتوافر المهارات الرقمية.



ترتيب الدول العربية عالمياً في مؤشر تطوير الحكومة الإلكترونية عام ٢٠٢٢ (٥٩)

هـ- ترتيب الدول العربية في مؤشر تطوير الحكومة الإلكترونية عام ٢٠٢٢ يقيس مدى استعداد الحكومات لاستخدام تقنيات الذكاء الاصطناعي في تقديم الخدمات لمواطنيها، من خلال ٣٣ مؤشراً، أبرزها وجود استراتيجية وطنية للذكاء الاصطناعي، والبنية التحتية للاتصالات، وتوافر المهارات الرقمية.



أثر القضاء السيبراني على الأمن القومي العربي خلال الفترة من ٢٠١١ حتى نوفمبر ٢٠٢٣

إيمان عبد القادر

٢- أبرز جهود التعاون السيبراني على المستوى الإقليمي العربي

تمثلت أبرز الجهود الإقليمية في إنشاء «المنظمة العربية لتكنولوجيات الاتصال والمعلومات» عام ٢٠٠٥، وتم تعديلها عام ٢٠١٨ بموجب قرار المجلس الاقتصادي والاجتماعي لجامعة الدول العربية، وهي منظمة حكومية عربية متخصصة تابعة لجامعة الدول العربية تهدف إلى الإسهام في تطوير تكنولوجيات المعلومات والاتصال في البلدان العربية وتوفير الآليات الضرورية لدعم التعاون والتكامل في المجال بين أعضاء المنظمة وتطوير سياسات واستراتيجيات مشتركة لنشر النفاذ العادل المستدام إلى التكنولوجيا وتطويعها لخدمة أهداف التنمية الاقتصادية وتحقيق الرقي الاجتماعي في المنطقة العربية (٦٠).

كذلك قامت الإسكوا منذ عام ٢٠٠٩ بإطلاق مشروع «تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية»، وهدفت إلى تعزيز وتنسيق التشريعات السيبرانية في المنطقة العربية بعبء بناء قطاع متين ومستدام لتكنولوجيا المعلومات والاتصالات عبر وضع الأطر التشريعية والقانونية الملائمة (٦١).

أيضاً تم إقرار الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في ديسمبر ٢٠١٠ (٦٢)، ثم أقر البرلمان العربي أول قانون عربي استرشادي في مجال حماية وتعزيز الأمن السيبراني في الدول العربية في نوفمبر ٢٠٢٢، وذلك في إطار دعم الجهود العربية لوضع إطار قانوني شامل لمواجهة الجرائم السيبرانية، وتعزيز حماية الأنظمة التقنية ومكوناتها، وتأمين ما تقدمه من خدمات وما تحويه من بيانات، من أي أعمال غير مشروعة (٦٣).

كما قامت المنظمة العربية لتكنولوجيات الاتصال والمعلومات بإطلاق «الاستراتيجية العربية للأمن السيبراني» (٢٠٢٢-٢٠٢٧) وهي خطة من الإجراءات مقدّمة للحكومات العربية لتنفيذها خلال السنوات الخمس المقبلة لتشجيع تبني وتطوير ضوابط خاصة بالأمن السيبراني على مستوى عالمي، وتشتمل على مجموعة من الممارسات مقسّمة إلى وضع استراتيجيات وطنية للأمن السيبراني، دعم البحث والتطوير، التدريب والتوعية، التعاون العربي المشترك، إنشاء مراكز وطنية للاستجابة للحوادث، تعزيز مناهج للأمن السيبراني الموجهة نحو سوق العمل، وأخيراً تحديث أطر حوكمة للأمن السيبراني (٦٤).

أنشأت جامعة الدول العربية في سبتمبر ٢٠٢٢ «مجلس وزراء الأمن السيبراني العرب»، بناء على مقترح من المملكة العربية السعودية، ويهدف المجلس إلى تعزيز التعاون العربي في مجال الأمن السيبراني، ورفع كفاءة التنسيق بين الدول العربية لمعالجة التهديدات السيبرانية (٦٥).

رابعاً: نتائج الدراسة

سيتم في هذا الجزء توضيح التحديات التي تواجه الأمن السيبراني في الدول العربية، والركائز التي يمكن الاعتماد عليها لمواجهة هذه التحديات، ثم وضع مجموعة من التوصيات التي يمكن من خلالها تحقيق الأمن السيبراني في الدول العربية.

١- التحديات والركائز

تم الاعتماد على تحليل (SWOT) لتوضيح التحديات التي تواجه تحقيق الأمن السيبراني في الدول العربية والتي تتمثل في نقاط الضعف والتهديدات، والتعرف على الركائز التي يمكن الاستناد إليها لمواجهة هذه التحديات التي تتمثل في نقاط القوة والفرص، كالتالي:

أ- نقاط القوة:

- إقرار أول قانون عربي استرشادي في مجال حماية وتعزيز الأمن السيبراني في الدول العربية في نوفمبر ٢٠٢٢.
- قامت المنظمة العربية لتكنولوجيات الاتصال والمعلومات بإطلاق الاستراتيجية العربية للأمن السيبراني (٢٠٢٣ - ٢٠٢٧).
- قامت جامعة الدول العربية بإنشاء «مجلس وزراء الأمن السيبراني العرب» في سبتمبر ٢٠٢٢.
- جاءت ٧ دول عربية ضمن أفضل ٥٠ دولة عالمياً في مؤشر الأمن السيبراني (السعودية، الإمارات، عمان، مصر، قطر، تونس، المغرب).
- اتخذت ١٠ دول عربية تدابير تشريعية قوية لحماية الأمن السيبراني (السعودية، الإمارات، عمان، مصر، قطر، تونس، البحرين، الأردن، المغرب، الكويت).
- اتخذت ٧ دول عربية تدابير تقنية قوية، متمثلة في وجود فرق وطنية للاستجابة للحوادث الحاسوبية، ومعايير للأمن السيبراني (السعودية، تونس، الإمارات، المغرب، مصر، عمان، قطر).

- لم تتخذ ٤ دول عربية تدابير تنظيمية قوية خاصة (موريتانيا، جزر القمر، جيبوتي، اليمن).
- لم تتخذ دولتان عربيتان تدابير تنظيمية (جيبوتي، اليمن).
- لم تتخذ ٥ دول عربية إجراءات فى مجال التوعية بالأمن السيبرانى وبناء القدرات (سوريا، موريتانيا، جزر القمر، جيبوتي، اليمن).
- لم تتخذ ٦ دول عربية إجراءات فى مجال الانخراط فى اتفاقيات ثنائية ومتعددة الأطراف للأمن السيبرانى، ووجود شراكات بين القطاعين العام والخاص (السودان، فلسطين، سوريا، موريتانيا، جيبوتي، اليمن).

ج- الفرص :

- اتخذت ٣ دول عربية إجراءات متوسطة فى مجال الأمن السيبرانى (البحرين، الكويت، الأردن).
- اتخذت ٨ دول عربية إجراءات تشريعية تراوحت ما بين متوسطة أو ضعيفة (موريتانيا، الجزائر، السودان، لبنان، سوريا، فلسطين، ليبيا، جيبوتي).
- اتخذت ١١ دولة عربية تدابير تقنية تراوحت ما بين متوسطة أو ضعيفة (الكويت، السودان، البحرين، فلسطين، الأردن، ليبيا، سوريا، العراق، لبنان، الصومال، الجزائر).
- اتخذت ١٢ دول عربية تدابير تنظيمية تراوحت ما بين متوسطة أو ضعيفة (المغرب، تونس، الكويت، العراق، موريتانيا، الصومال، لبنان، السودان، سوريا، ليبيا، فلسطين، جزر القمر، الجزائر).
- اتخذت ٨ دول عربية إجراءات فى مجال التوعية بالأمن السيبرانى وبناء القدرات تراوحت ما بين متوسطة أو ضعيفة (الأردن، الجزائر، لبنان، ليبيا، السودان، فلسطين، العراق، الصومال).
- اتخذت ٨ دول عربية إجراءات فى مجال الانخراط فى اتفاقيات ثنائية ومتعددة الأطراف للأمن السيبرانى، ووجود شراكات بين القطاعين العام والخاص تراوحت ما بين متوسطة أو ضعيفة (الأردن، البحرين، ليبيا، الجزائر، الصومال، العراق، لبنان، جزر القمر).
- إمكان استفادة الدول الضعيفة فى الأمن السيبرانى من الدول التى اتخذت إجراءات قوية.

- اتخذت ٧ دول عربية تدابير تنظيمية قوية خاصة بإطلاق استراتيجيات وطنية للأمن السيبرانى وإنشاء هيئات للأمن السيبرانى (السعودية، عمان، مصر، الإمارات، قطر، الأردن، البحرين).
- اتخذت ٩ دول عربية إجراءات قوية فى مجال التوعية بالأمن السيبرانى وبناء القدرات (السعودية، الإمارات، عمان، قطر، مصر، تونس، البحرين، الكويت، المغرب).
- قامت ٨ دول عربية بالانخراط فى اتفاقيات ثنائية ومتعددة الأطراف للأمن السيبرانى، وقامت بإيجاد شراكات بين القطاعين العام والخاص (السعودية، الإمارات، عمان، قطر، مصر، المغرب، تونس، الكويت).
- شهدت الدول العربية نموًا متواصلًا فى معظم المجالات المتعلقة بالبنية التحتية لتكنولوجيا المعلومات والاتصالات والنفوذ إليها واستعمالها.
- احتلت ٣ دول عربية مراكز متقدمة فى مؤشر جاهزية الشبكات (الإمارات، السعودية، قطر).
- احتلت ٣ دول عربية مراكز متقدمة فى مؤشر جاهزية الحكومة للذكاء الاصطناعى (الإمارات، قطر، السعودية).
- احتلت ٦ دول عربية مراكز متقدمة فى مؤشر «شمولية الإنترنت» (الإمارات، قطر، الكويت، عمان، السعودية، البحرين).
- احتلت ٣ دول عربية مراكز متقدمة فى مؤشر «تطوير الحكومة الإلكترونية» (الإمارات، السعودية، عمان).
- قامت العديد من الدول العربية بإطلاق أقمار اصطناعية.
- أتجهت بعض الدول إلى إنشاء مدن ذكية، وتأسيس حكومة إلكترونية.

ب- نقاط الضعف :

- تعاني ١٢ دولة عربية ضعف إجراءات الأمن السيبرانى (السودان، الجزائر، لبنان، ليبيا، فلسطين، سوريا، العراق، موريتانيا، الصومال، جزر القمر، جيبوتي، اليمن).
- لم تتخذ ٤ دول عربية إجراءات تشريعية (العراق، الصومال، جزر القمر، اليمن).



أثر الفضاء السيبراني على الأمن القومي العربي خلال الفترة من ٢٠١١ حتى نوفمبر ٢٠٢٣

إيمان عبد القادر

القسم الأول

دراسات استراتيجية

تعاونى بين الدول العربية وتحقيق مزيد من الشراكات التعاونية بين القطاعين العام والخاص، وتوفير التدريب للكوادر العربية فى مجال الأمن السيبرانى، ومساعدة الدول التى اتخذت إجراءات متوسطة فى مجال الأمن السيبرانى، بما يمكنها من اتخاذ إجراءات أقوى.

ب- يُقترح قيام الدول العربية السبع (السعودية، الإمارات، عمان، مصر، قطر، تونس، المغرب) التى تُعد من أفضل ٥٠ دولة عالمياً فى مؤشر الأمن السيبرانى بتقديم الدعم للدول التى لم تتخذ إجراءات فى ركائز الأمن السيبرانى وذلك من خلال:

- تقديم المساعدة لدول (العراق، الصومال، جزر القمر، اليمن) فى وضع إجراءات تشريعية.
- تقديم الدعم التقنى لـ (موريتانيا، جزر القمر، جيبوتى، اليمن).
- تقديم المعلومات لدولتى (جيبوتى، اليمن) التى تمكنهما من اتخاذ تدابير تنظيمية قوية.
- تقديم المساعدة لـ (سوريا، موريتانيا، جزر القمر، جيبوتى، اليمن) فى اتخاذ إجراءات فى مجال التوعية بالأمن السيبرانى وبناء القدرات.
- عقد اتفاقيات بين الدول العربية التى اتخذت إجراءات قوية فى مجال الانخراط فى اتفاقيات ثنائية ومتعددة الأطراف للأمن السيبرانى، ووجود شراكات بين القطاعين العام والخاص مع (السودان، فلسطين، سوريا، موريتانيا، جيبوتى، اليمن) ومساعدتهم فى الانخراط فى اتفاقيات متعددة الأطراف للأمن السيبرانى.

ج- يمكن الاستعانة بالقانون العربى الاسترشادى للأمن السيبرانى فى مساعدة الدول العربية التى تعانى من عقبات تمنعها من صياغة وإقرار القوانين السيبرانية.

د- يمكن الاستفادة من إنشاء « مجلس وزراء الأمن السيبرانى العرب » فى حل المشكلات السياسية والمالية التى تعانى منها بعض الدول العربية والتى تعوق تنفيذها استراتيجيات تمكنها من حماية أمنها السيبرانى.

هـ- يُقترح قيام (الإمارات، قطر، السعودية) التى تُعد من أفضل الدول عالمياً فى مجال جاهزية الشبكات

- بدأت ٩ دول عربية فى اتخاذ إجراءات فى مجال جاهزية الشبكات (عمان، البحرين، الكويت، الأردن، مصر، المغرب، تونس، لبنان، الجزائر).
- اتخذت ١٧ دولة عربية إجراءات ما بين متوسطة أو ضعيفة فى مجال جاهزية الحكومة للذكاء الاصطناعى (عمان، البحرين، الأردن، مصر، الكويت، تونس، لبنان، المغرب، الجزائر، العراق، جيبوتى، ليبيا، موريتانيا، جزر القمر، السودان، اليمن، سوريا).
- اتخذت ٧ دول عربية إجراءات متوسطة فى مجال « شمولية الإنترنت » (المغرب، مصر، الأردن، تونس، الجزائر، لبنان، السودان).
- اتخذت ١٨ دول عربية إجراءات تراوحت ما بين متوسطة أو ضعيفة لتطوير الحكومة الإلكترونية (البحرين، الكويت، قطر، تونس، الأردن، المغرب، مصر، الجزائر، لبنان، العراق، سوريا، ليبيا، موريتانيا، السودان، اليمن، جيبوتى، جزر القمر، الصومال).
- هناك فرص متاحة لإيجاد منهج تعاونى وتحقيق مزيد من الشراكات التعاونية بين القطاعين العام والخاص.

د- التهديدات :

- وجود عقبات فى صياغة وإقرار القوانين السيبرانية فى بعض الدول العربية.
- تراجع أمن ومرونة البنية التحتية للإنترنت فى بعض الدول العربية.
- ضعف الكوادر المدربة فى مجال الأمن السيبرانى.
- ضعف الموارد المالية اللازمة فى معظم الدول العربية.
- تعانى بعض الدول العربية أزمات سياسية.

٢- التوصيات :

بناءً على ما توصلت إليه الدراسة من نتائج سيتم وضع مجموعة من التوصيات والمقترحات التى تساعد فى معالجة التحديات التى تواجه الأمن السيبرانى العربى المتمثلة فى نقاط الضعف والتهديدات، وذلك بالاعتماد على الركائز المتمثلة فى نقاط القوة والفرص كالتالى:

أ- يمكن الاستفادة من إطلاق الاستراتيجية العربية للأمن السيبرانى (٢٠٢٢ - ٢٠٢٧) فى إيجاد منهج

والتكيف، وتكون قادرة على توظيف عمليات الفضاء الإلكتروني في جميع أنحاء نطاق الصراع. ز- توفير منح دراسية في مجال الأمن السيبراني للدول التي تعاني عدم وجود كوادر مُدرّبة لحين إنشاء مؤسسات تعليمية متخصصة في مجال الأمن السيبراني في تلك الدول. ح- نشر الوعي بالاستخدامات السلبية للفضاء السيبراني التي تهدف إلى زعزعة أمن واستقرار الدول العربية.

وجاهزية الحكومة للذكاء الاصطناعي بمساعدة الدول العربية التي تعاني تراجع أمن ومرونة البنية التحتية للإنترنت بها. و- إيلاء مزيد من الاهتمام للحماية وتعزيز الأمن السيبراني لأجهزة الدولة من خلال بناء وحدات سيبرانية داخل الجيوش العربية يكون لديها القدرة الاستباقية للردع ومواجهة الهجمات السيبرانية، وأن تمتلك تلك الوحدات قدرات قابلة للتطوير

الخلاصة:

أدى الاعتماد على الفضاء السيبراني إلى تغييرات في مجالات الأمن القومي، ففي المجال السياسي يظهر تأثيره من خلال إدارة العمليات النفسية، أما في المجال العسكري فقد أدى ظهوره إلى تحوّل في مفهوم القوة، وتحوّل الحروب من تقليدية إلى سيبرانية، وفي المجال الاجتماعي، أصبح أداة للصراع الأيديولوجي، أما في المجال الاقتصادي فإن الهجمات السيبرانية ينتج عنها تعطيل الخدمات وخسائر مالية كبيرة.

كما ثبت أن للفضاء السيبراني تأثيراً كبيراً على الأمن القومي العربي، ففي المجال السياسي، كان لمواقع التواصل الاجتماعي دور بارز خلال الثورات التي انطلقت عام ٢٠١١، وما زالت تلعب دوراً كبيراً، وفي المجال الأمني، ازداد استخدام الفضاء السيبراني في الصراع بين إيران ودول الخليج، كذلك نجحت الجماعات الإرهابية في استخدام مواقع التواصل الاجتماعي لتجنيد أعضاء جدد وجمع التمويل والمعلومات، أما في المجال الاجتماعي، فقد استخدمت الجماعات الإرهابية تلك المواقع لنشر أفكارها المتطرفة، وفي المجال الاقتصادي، أدت الهجمات السيبرانية المتزايدة إلى تكبد الدول العربية خسائر اقتصادية كبيرة.

وتجدر الإشارة إلى أن التأثير الكبير للفضاء السيبراني على الأمن القومي العربي أدى إلى قيام الدول العربية باتخاذ سياسات في مجال الأمن السيبراني، وعلى الرغم من ذلك فإن الهجمات في ازدياد، مما كشف ضرورة خلق أطر من التعاون بين الدول العربية لوضع إجراءات لحماية الأمن السيبراني، الذي يمكن تحقيقه من خلال الاستراتيجية العربية للأمن السيبراني (٢٠٢٣ - ٢٠٢٧). كذلك ضرورة قيام الدول العربية التي تُعد من أفضل ٥٠ دولة عالمياً في مؤشر الأمن السيبراني بتقديم الدعم للدول التي تعاني ضعف إجراءات الأمن السيبراني، فضلاً عن ضرورة نشر الوعي بالاستخدامات السلبية للفضاء السيبراني التي تهدف إلى زعزعة أمن واستقرار الدول العربية.



أثر الفضاء السيبراني على الأمن القومي العربي خلال الفترة من ٢٠١١ حتى نوفمبر ٢٠٢٣

إيمان عبد القادر

المراجع :

- (١) نورة شلوش، القرصنة الإلكترونية في الفضاء المتصاعد لأمن الدول، مجلة مركز بابل للدراسات الإنسانية، المجلد ٨، العدد ٢، عام ٢٠١٨، ص ١٨٧.
- (٢) منى الأشقر جبور، أهمية الاتفاقية العربية للأمن السيبراني، ورقة عمل مقدمة إلى اللقاء السنوي الرابع للمختصين في أمن وسلامة الفضاء السيبراني، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، ١٩ أغسطس ٢٠١٥، ص ٢.
- (٣) عادل عبد الصادق، الفضاء الإلكتروني وأسلحة الانتشار الشامل بين الردع وسباق التسليح: (١ نوفمبر ٢٠١٩) <https://seconf.wordpress.com/2015/05/15/%D8%A7>.
- (٤) منى الأشقر جبور، مرجع سبق ذكره، ص ٣.
- (٥) نسرین الشحات الصباحي على، الأبعاد العسكرية للقوة السيبرانية على الأمن القومي للدول « دراسة حالة إسرائيل »: <https://democraticac.de/?p=30962> (٢ أكتوبر ٢٠٢٠).
- (6) PW Singer, Allan Friedman, (2014), Cyber security and Cyberwar: What everyone needs to know, New York, Oxford University Press, p. 11.
- (7) Martti Lehto (2014), Phenomena in the Cyper World, in Martti Lehto & Pekka Neittaanmaki (eds.) Cyper Security: Analytics, Technology and Automation, Finland: Springer, p.3-p.4.
- (8) James E. Cartwright, Joint Terminology for Cyberspace Operations, Memorandum for Chiefs of the Military Services, Washington, D.C. 20318-9999, p. 7.
- (9) Alex Tanchev (2018) The strategic dimensions of cyber security an interdisciplinary approach, Austria Institut für Europa und Sicherheitspolitik, p. 4
- (١٠) إيهاب خليفة، القوة الإلكترونية وأبعاد التحول في خصائص القوة، مكتبة الإسكندرية، وحدة الدراسات المستقبلية، ٢٠١٤، ص ٣٢-٤٢
- (11) Kim R. Holmes, (2015), What is national Security, Washington, The Heritage Foundation, p. 23- p. 19
- (12) Jude Blanchette (2020), Ideological Security as National Security, Washington, Center for Strategic and International Studies, p. 4
- (13) Kim R. Holmes, op.cit, p. 19
- (١٤) أحمد يوسف أحمد، التوجهات العربية للأمن القومي بين المفهوم والخبرة، بحث مقدم إلى المؤتمر السنوي لمركز البحوث والدراسات السياسية، كلية الاقتصاد والعلوم السياسية بجامعة القاهرة، ديسمبر ٢٠٠٥، ص ٦٤.
- (١٥) منى الأشقر جبور، الأمن السيبراني- التحديات ومستلزمات المواجهة، ورقة عمل مقدمة إلى اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني، المركز العربي للبحوث القانونية والقضائية بجامعة الدول العربية ٢٧-٢٨ أغسطس ٢٠١٢، ص ٣-٤.
- (16) ITU, Introduction to Security Cyberspace, Cybercrime and Cybersecurity, <https://www.itu.int/en/ITU/Cybersecurity/Documents/Introduction%20to%20the%20Concept%20of%20IT%20Security.pdf> (30 october 2021)
- (17) James E. Cartwright, op.cit, p. 7.
- (١٨) نورة شلوش، مرجع سبق ذكره، ص ٢٠٠.
- (١٩) الحسين، أثر وسائل التواصل الاجتماعي على سلوكيات وقيم الشباب من منظور التربية الإسلامية، مجلة كلية التربية بجامعة الأزهر، العدد ١٦٩، الجزء الثالث، يوليو ٢٠١٦، ص ٣٣٦.
- (٢٠) سليم دحمانى، أثر التهديدات السيبرانية على الأمن القومي، الولايات المتحدة الأمريكية نموذجًا (٢٠٠١-٢٠١٧)، رسالة ماجستير، جامعة محمد بوضياف الجزائرية، كلية الحقوق والعلوم السياسية، عام ٢٠١٨، ص ٢٥.
- (21) James E. Cartwright, op.cit, p. 8.
- (٢٢) إيهاب عبد الحميد خليفة عبد العال، استخدام القوة الإلكترونية في إدارة التفاعلات الدولية « الولايات المتحدة نموذجًا خلال الفترة من ٢٠٠١ إلى ٢٠١٢ »، رسالة ماجستير، جامعة القاهرة، كلية الاقتصاد والعلوم السياسية، ٢٠١٤، ص ٢١-٢٢.
- (٢٣) أحمد إسماعيل، أيديولوجيا الإعلام الجديد والوعي الزائف مقارنة في استراتيجيات الإقناع وصناعة الواقع، مجلة الدراسات الإعلامية، المركز الديمقراطي العربي ببرلين، العدد ٨، أغسطس ٢٠١٩، ص ٦٩.
- (٢٤) رغدة البهي، الإرهاب السيبراني: المفهوم، السمات، الأنماط، (١١ سبتمبر ٢٠٢٠) <https://www.ecsstudies.com/7141/>.

المراجع :

- (٢٥) ماركو لويس أونسو، الأمن السيبراني.. كيف يمكن الحد من الآثار الاقتصادية للهجمات الإلكترونية المنظمة؟، ترجمة محمد عويس، جريدة الجرائد العالمية، العدد ٦٠٩، ٢٦ مايو ٢٠٢١، ص٢٨.
- (26) Jennifer Elliott and Nigel Jenkinson, Cyber Risk is the New Threat to Financial Stability, <https://imf.org/2020/12/07/cyber-risk-is-the-new-threat-to-financial-stability/> (13 september 2020)
- (٢٧) عبد الجبار أحمد عبد الله، دور شبكات التواصل الاجتماعي في ثورات الربيع العربي، مجلة العلوم السياسية، العدد ٤٤، ٢٠١٢، ص٢٠٠.
- (٢٨) حسن مظفر الرزق، النزاعات والمواجهات السيبرانية في فضاء منطقة الخليج العربي، مركز الجزيرة للدراسات، ١٥ سبتمبر ٢٠١٩، ص٣.
- (٢٩) عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، سلسلة أوراق، وحدة الدراسات المستقبلية، مكتبة الإسكندرية، العدد ٢٣، ٢٠١٦، ص٣١.
- (٣٠) عادل عبد الصادق، الفضاء الإلكتروني وأسلحة الانتشار الشامل بين الردع وسباق التسلح، مرجع سبق ذكره.
- (٣١) سنان صلاح رشيد الصالحى، دور مواقع التواصل الاجتماعي في السياسة الدولية، <https://democraticac.de/?p=50855> (١١ سبتمبر ٢٠٢٠).
- (32) Sabiha Gire, The Role of Social Media in the Arab Spring, <https://sites.stedwards.edu/pangaea/the-role-of-social-media-in-the-arab-spring/> (14 september 2020)
- (٣٣) أشرف العيسوى، وسائل التواصل الاجتماعي: تأثيرات متنامية وأدوار شائكة في العالم العربي، <https://trendsresearch.org/ar/insight/> (٣ أكتوبر ٢٠٢٠).
- (34) International Telecommunication Unit, <https://www.itu.int/en/ITU-D/Statistics/Pages/stat/> (30 august 2023)
- (35) Arab Social Media Report, Social Media in the Arab World, Influencing Societal and Cultural Change?, Dubai School of Government, Vol. 2, No. 1, July 2012, p.7.
- (٣٦) تقرير الإعلام الاجتماعي العربي، الإعلام الاجتماعي والحراك المدني: تأثير فيسبوك وتويتر، كلية دبي للإدارة الحكومية، الإصدار الثاني، مايو ٢٠١١، ص٩-١٦.
- (٣٧) نديم منصورى، دور الإعلام التواصلى الجديد فى تحريك الثورات العربية، <https://al-akhbar.com/Opinion/67495> (٥ أكتوبر ٢٠٢٠).
- (38) International Telecommunication Unit, op.cit.
- (39) Hootsuite, <https://hootsuite.com/resources/digital-2020> (7 october 2020)
- (٤٠) أشرف العيسوى، مرجع سبق ذكره.
- (٤١) حسن مظفر الرزق، مرجع سبق ذكره، ص٣.
- (٤٢) عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، مرجع سبق ذكره، ص٣١-٤٢.
- (٤٣) مكتب الأمم المتحدة المعنى بالمخدرات والجريمة، استخدام الإنترنت فى أغراض إرهابية، نيويورك، الأمم المتحدة، ٢٠١٢، ص١.
- (44) Anne Speckhard and Ardian Shajkovci, Is ISIS Still Alive and Well on the Internet?, <https://www.hstoday.us/subject-matter-areas/cybersecurity/is-isis-still-alive-and-well-on-the-internet/> (26 june 2021)
- (٤٥) مكتب الأمم المتحدة المعنى بالمخدرات والجريمة، مرجع سبق ذكره، ص٢-٥.
- (46) Adam Hoffman, The Islamic State's Use of Social Media, Terrorism's Siren Song in the Digital Age, p. 99, <https://www.inss.org.il/he/wp-content/uploads/sites/%20Adam%20Hoffman.pdf>, (26 june 2021)
- (٤٧) سماح عبد الصبور، الإرهاب الرقمة: أنماط استخدام الإرهاب الشبكي، <https://futureuae.com/ar-AE/Mainpage/Item/227/> (12 فبراير 2021).
- (48) Adam Hoffman, op.cit, p. 99.
- (49) Joyce Hakmeh, (June 2017), Cybercrime and the Digital Economy in the GCC Countries, Chatham House, p. 6.



أثر القضاء السيبراني على الأمن القومي العربي خلال الفترة من ٢٠١١ حتى نوفمبر ٢٠٢٣

إيمان عبد القادر

المراجع :

- (٥٠) عبد الرحمن عاطف أبو زيد، الأمن السيبراني في الوطن العربي... دراسة حالة المملكة العربية السعودية، <http://www.acrseg.org/41356> (٢٩ أكتوبر ٢٠٢٠).
- (51) Annie Fixler (February 2020), The Cyber Threat from Iran after the Death of Soleimani, Combating Terrorism Center At west point, Volume 13, Issue 2, p. 22.
- (52) Aman Quadri & Muhammad Khurram Khan (January, 2019), Cyper Security Challenges of the Kingdom of Saudia Arabia, Global Foundation for Cyber Studies and Research, p. 8.
- (٥٣) محمد مصباح محمد، تأمين البنية التحتية للدول.. المخاطر والتحديات، مجلة عالم التكنولوجيا بمركز المعلومات ودعم اتخاذ القرار، مجلس الوزراء، العدد ١، مارس ٢٠٢٠، ص ١٩
- (54) International Telecommunication Unit, Cyper security index report, <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx> (30 june 2021)
- (55) Ibid.
- (56) Soumitra Dutta and Bruno Lanvin, The Network Readiness Index 2022, https://networkreadinessindex.org/wp-content/uploads/reports/nri_2022.pdf (29 august 2023)
- (57) The economist, <https://impact.economist.com/projects/inclusive-internet-index/> (29 august 2023)
- (58) Oxford Insights, https://static1.squarespace.com/static/58b2e92c1e5b6c828058484e/t/639b495cc6b59c620c3ecde5/1671121299433/Government_AI_Readiness_2022_FV.pdf (29 august 2023)
- (59) United Nation, <https://publicadministration.un.org/egovkb/Data-Center> (29 august 2023)
- (٦٠) المنظمة العربية لتكنولوجيات الاتصال والمعلومات، http://www.aicto.org/ar/%d8%b9%d9%86- / (٢٠ سبتمبر ٢٠٢٢).
- (٦١) ليلي الجنابي، فعالية القوانين الوطنية والدولية في مكافحة الجرائم السيبرانية <https://www.ssraw.org/ar/print.art.asp?aid=571423&ac=2> (٢٠ سبتمبر ٢٠٢٢).
- (٦٢) العشاش إسحاق، الإرهاب السيبراني وتحديات الدول.. دراسة مقارنة مع الاتفاقيات الدولية، مجلة بحوث بجامعة الجزائر، العدد ١٢، الجزء الأول، ٢٠١٨، ص ١٩٦.
- (٦٣) سوزان عاطف، إقرار أول قانون عربي لحماية وتعزيز الأمن السيبراني في الدول العربية <https://www.almasryalyoum.com/news/details/2453786> (٢٠ سبتمبر ٢٠٢٢).
- (٦٤) الاستراتيجية العربية للأمن السيبراني (٢٠٢٣ - ٢٠٢٧) <http://www.aicto.org/ar/%d8%a7%d9%84%d8%a5%d8%b5%d8%af%d8%a7%d8%b1%d8%a7%d8%aa/%d8%a7%d9%84%d8%af%d8%b1%d8%a7%d8%b3%d8%a7%d8%aa/> (٢٠ سبتمبر ٢٠٢٢).
- (٦٥) ياسمين السيد، جامعة الدول العربية تتشئ مجلس وزراء الأمن السيبراني العرب <https://www.forbesmiddleeast.com/ar/industry/economy/establishment-of-the-council-of-arab-ministers-of-cybersecurity-at-the-league-of-arab-states> (٢٠ سبتمبر ٢٠٢٢).

أثر الفضاء السيبراني على الأمن القومي العربي خلال الفترة من ٢٠١١ حتى ٢٠٢٣

■ إيمان عبد القادر

باحثة بمركز المعلومات ودعم اتخاذ القرار- مجلس الوزراء - مصر

مستخلص:

يُعتبر الفضاء السيبراني "Cyber Space" أحد الأشكال الجديدة لمفهوم القوة والتعبير عن مفرداتها، بما يمكن المقتدر فيه من استخدامه بطريقة تضمن مصالحه وأمنه القومي، ونتيجة هذه الاستخدامات وتحول الإنترنت إلى بنية أساسية عالمية للنشاطات المدنية، وإلى وسيلة جديدة للضغط السياسي والتجسس، بالإضافة إلى تأثير الفضاء السيبراني على الأمن القومي في كل مجالاته، تصدر الأمن السيبراني المراكز الأولى في سياسات واستراتيجيات الدول للحفاظ على نظامها وأمنها القومي.

برز أيضا دور الفضاء السيبراني عبر مواقع التواصل الاجتماعي في إدارة الصراع السياسي في الدول العربية، وظهر تفاوت في استخدام الفضاء السيبراني وفق طبيعة التطور التقني وقدرة النظام على إدارة الصراع الإعلامي، والتأثير في الرأي العام وتعبئة وحشد الجمهور، فضلا عن أن مواقع التواصل الاجتماعي كانت وسيلة جيدة للجماعات الإرهابية من أجل تجنيد أعضاء جدد وجمع التمويل ونشر آرائهم المتطرفة وتنفيذ عملياتهم في المنطقة العربية، أيضا تعرضت العديد من المواقع الخاصة بجهات أمنية عربية، ووزارات وشركات مهمة إلى هجمات سيبرانية وتوقف العمل فيها لعدة ساعات، لذلك من الأهمية التعرف على العلاقة بين مفهومى الفضاء السيبراني، والأمن القومي، ودراسة دور الفضاء السيبراني في التأثير على الأمن القومي العربي في جميع مجالاته (السياسية والعسكرية والاقتصادية والاجتماعية)، والتعرف على الموقف الحالي للأمن السيبراني في الدول العربية، ووضع مقترحات لمواجهة هذه التحديات.

الكلمات المفتاحية: الفضاء السيبراني، الأمن السيبراني، الأمن القومي العربي

The impact of cyberspace on Arab national security during the period from 2011 to 2023

■ Iman Abdul Qader

Researcher at the Information and Decision Support Center – Cabinet - Egypt

Abstract:

Cyberspace is considered one of the new forms of the concept of power and the expression of its vocabulary, enabling those with power to use it in a way that guarantees their interests and national security. The role of cyberspace has emerged through social media sites in managing political conflict in Arab countries, and disparities have emerged in the use of cyberspace. According to the nature of technical development and the regime's ability to manage the media conflict, influence public opinion and mobilize the public, in addition to the fact that social networking sites were a good way for terrorist groups to recruit new members, it is therefore important to recognize the relationship between the concepts of cyberspace and national security. Studying the role of cyberspace in influencing Arab national security in all its fields (political, military, economic, and social), identifying the current position of cyber security in Arab countries, and developing proposals to confront these challenges.

Keywords: cyberspace, cyber security, Arab national security