جيوبولتيك المخاطر السيبرانية للفضاء الالكتروني على الامن القومي لدول المشرق العربي

أ.م.د نبهان زمبور السعدي

جامعة كركوك –كلية التربية للعلوم الانسانية

البريد الإلكتروني Email : nabhanza@uokirkuk.edu.iq

الكلمات المفتاحية: الامن السيبراني ، الجغرافية الالكترونية ، المخاطر السيبرانية ، الهجمات الالكترونية.

كيفية اقتباس البحث

السعدي ، نبهان زمبور، جيوبولتيك المخاطر السيبرانية للفضاء الالكتروني على الامن القومي لدول المشرق العربي، مجلة مركز بابل للدراسات الانسانية، نيسان ٢٠٢٤،المجلد:١٤ ،العدد:٢.

هذا البحث من نوع الوصول المفتوح مرخص بموجب رخصة المشاع الإبداعي لحقوق التأليف والنشر (Creative Commons Attribution) تتيح فقط للآخرين تحميل البحث ومشاركته مع الآخرين بشرط نَسب العمل الأصلي للمؤلف، ودون القيام بأي تعديل أو استخدامه لأغراض تجارية.

مفهرسة في Indexed
IASJ

مسجلة في Registered
ROAD

Geopolitics of Cyber Threats of Cyberspace on the National Security of the Mashriq Countries

Prof. Dr. Nabhan Zambour Al-Saadi
Kirkuk University - College of Education for Human Sciences

Keywords : cybersecurity, cyber geography, cyber risks, cyber attacks.

How To Cite This Article
Al-Saadi, Nabhan Zambour, Geopolitics of Cyber Threats of Cyberspace on the National Security of the Mashriq Countries, Journal Of Babylon Center For Humanities Studies, April 2024,Volume:14,Issue 2.

This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.

Abstract

The world today is still in the information technology revolution. The Internet, big data, artificial intelligence, cloud technology, and even many new improvements will continue to develop, and the meaning and extension of cyberspace will continue to develop. Many security conflicts facing cyberspace have emerged and are expanding at all levels of technology, politics, and prior education, which Odera geopolitically competes around the fabric of vital tissues such as energy, public transportation and manufacturing.

The research aims to reveal the concept of cybersecurity in cyberspace as a field of political geography, and to identify the reality of the strength of cybersecurity in the region of the Arab Levant countries, and to deal effectively with the hidden dangers that threaten Internet security, and to ensure interconnection between networks. The problem revolves around the questions raised by the research, which are: What is the concept and risks of cybersecurity from a geopolitical perspective? What are the levels of cybersecurity in the Arab Levant countries? What is the geopolitical weight of the cybersecurity force of the Arab Levant countries? The research reached several results, the most important of

which are: Digital geopolitics represents the mapping of traditional geostrategic thinking in the digital space, and then strengthening and expanding control in the physical space. Some countries of the Arab Levant (Saudi Arabia and the Emirates) were also able to achieve a safe and secure environment by obtaining a classification Very high on the overall cybersecurity strength scale. Most of the countries of the Arab Levant face geopolitical risks to their cybersecurity and therefore their economic, political and social security, such as Iraq, Syria, Lebanon, Yemen and Jordan from the perspective of cybersecurity standards.

المستخلص

لا يزال العالم اليوم في موجة ثورة تكنولوجيا المعلومات، فالإنترنت والبيانات الضخمة والذكاء الاصطناعي وتكنولوجيا السحابة وحتى العديد من التقنيات الجديدة ستستمر في الظهور، وسيستمر توسع مدلول الفضاء السيبراني وامتداده ، وستظهر المخاطر والصراعات الأمنية التي يواجهها الفضاء الإلكتروني وتمتد على جميع مستويات التكنولوجيا والسياسة والاقتصاد والأمن، والتي تأخذ تنافسا جيوسياسيا دوليا والذي يتركز حول قطاعات البنية التحتية الحيوية مثل الطاقة والنقل العام والتصنيع.

ويهدف البحث الى الكشف عن مفهوم الامن السيبراني للفضاء الالكتروني كمجال للجغرافية السياسية ، والتعرف على واقع قوة الامن السيبراني لإقليم دول المشرق العربي ،والتعامل الفعال مع الأخطار الخفية التي تهدد أمن الإنترنت ، وضمان الترابط بين الشبكات ، وتتمحور المشكلة في التساؤلات التي طرحها البحث وهي : ما هو مفهوم ومخاطر الامن السيبراني من منظور الجغرافية السياسية ؟ وما هي مستويات الامن السيبراني لدول المشرق العربي ؟ و ما هو الوزن الجيوبولتيكي لقوة الامن السيبراني لدول المشرق العربي ؟ وتوصل البحث الى عدة نتائج اهمها : تمثل الجغرافيا السياسية الرقمية بكونها رسم لخرائط التفكير الجيوستراتيجي التقليدي في الفضاء الرقمي ، ومن ثم تعزيز وتوسيع السيطرة في الفضاء المادي ، كما استطاعت بعض دول المشرق العربي (السعودية والامارات) ان تحقق بيئة آمنة ومأمونة من خلال حصولها على تصنيف عالي جدا ضمن مقياس القوة الشاملة للأمن السيبراني. وأن معظم دول المشرق العربي تواجه مخاطر جيوبولتيكية لأمنها السيبراني وبالتالي امنها الاقتصادي والسياسي والاجتماعي كالعراق وسوريا ولبنان واليمن والاردن من منظور مقاييس الامن السيبراني.

المقدمة

مع ثورة تكنولوجيا المعلومات ظهر فضاء جديد وهو الفضاء السيبراني أو الالكتروني الرقمي الذي بدأ من الانترنت (الشبكة العنكبوتية) وما أحدثته من انقلاب في مختلف مجالات الحياة ، بما فيها المجال السياسي والدولي لما أتاحه من قوة جديدة بيد الدول الأكثر قدرة على توظيفه ، وفي نفس الوقت ما يشكل من مخاطر غير مسبوقة نتيجة سهولة اختراق المجال والأمن القومي وخصوصيات الناس ، بأدوات خارج ما متعارف عليه فيما يخص السيادة التقليدية.

نظرا لقوة تأثير مخاطر الفضاء السيبراني على مفهوم وواقع القوة والسيادة والأمن والحرب والإرهاب والجيوسياسة والاقتصاد والحريات الشخصية اشتق المختصون في هذا المجال مصطلحات جديدة مثل الأمن السيبرانيCyber-Security والذي اصبح نقطة الارتكاز لحماية واستقلال الدول من المنظور الاقتصادي والسياسي والاجتماعي والعسكري ، لذا اصبح من اولويات الدول للحفاظ على امنها السيبراني من خلال تعزيز دفاعاتهم الوطنية لردع التهديدات والهجمات الالكترونية المستقبلية .

ويهدف البحث الى دراسة مفهوم الامن السيبراني للفضاء الالكتروني كمجال للجغرافية السياسية ، والتعرف على واقع قوة الامن السيبراني لدول المشرق العربي ، ولغرض تقييم المخاطر الجيوبولتيكية المحتملة تم تحديد اهداف تكتيكية اقليمية ودولية لغرض المقارنة.

وتتمثل مشكلة البحث في التساؤلات التالية :

١-ما هو مفهوم ومخاطر الامن السيبراني من منظور الجغرافية السياسية ؟

٢-ما هي مستويات الامن السيبراني لدول المشرق العربي ؟

٣-ما هو الوزن الجيوبولتيكي لقوة الامن السيبراني لدول المشرق العربي ؟

جاءت فرضية كإجابة لسؤال مشكلة البحث ، وهي:

- ان ظهور قضايا الأمن السيبراني من خلال التهديدات والهجمات الإلكترونية بين الدول ، قد اصبحت شكلاً جديدًا من أشكال الصراع الدولي وتشكل تحديًا للاستقرار الاستراتيجي للفضاء السيبراني الدولي.

- تباينت مستويات الامن السيبراني لدول المشرق العربي ما بين التصنيف العالي جدا والعالي والمتوسط والمنخفض ، تبعا للاستراتيجيات والسياسات السيبرانية المتبعة .

- كشفت مقاييس قوة الامن السيبراني ان بعض لدول المشرق العربي تواجه انحدار جيوبولتيكي كبير في مسالة امنها السيبراني .

قسم البحث الى اربعة محاور تناول المحور الاول مفهوم الامن السيبراني كمجال للجغرافية السياسية ، بينما تطرق المحور الثاني تقييم الامن السيبراني لدول المشرق العربي ، والمحور الثالث تطرق الى مؤشر القياس العالمي للأمن السيبراني (GCI) لإقليم دول المشرق العربي ، في حين بين المحور الرابع مؤشر القوة السيبرانية الشاملة لدول المشرق العربي.

اعتمد البحث على منهج تحليل القوة في الجغرافية السياسية لغرض تحقيق الهدف من خلال الاعتماد بيانات منظمة الامم المتحدة المتمثلة بالرقم القياسي العالمي للأمن السيبراني، وتقرير مسح الحكومة الالكترونية وتقرير التنمية البشرية.

الاول : مفهوم الامن السيبراني كمجال جديد للجغرافية السياسية

ينبع ظهور مفهوم الأمن السيبراني من النزاعات الإلكترونية المتكررة بين الدول ، والتي أصبحت شكلاً جديدًا من أشكال الصراع الدولي وتشكل تحديًا للاستقرار الاستراتيجي للفضاء السيبراني الدولي ، من خلال أدواتها العسكرية أو الاقتصادية أو النفسية وفي سباق التسلح ، ومن الامثلة على اثارها التوترات الأخيرة بين الولايات المتحدة والصين ، وكذلك بين الولايات المتحدة وروسيا بخصوص التأثير على الانتخابات الأمريكية ، فضلا عن استعمال المجال السيبراني في المواجهة بين أمريكا وإيران ، وفي الجدل الدائر بين أنظمة الحكم ومستعملي وسائط التواصل الاجتماعي وخصوصا أثناء التظاهرات والثورات الشعبية ، والتي سيكون تأثيرها ودورها حاسما في الحروب والمواجهات المستقبلية حيث من غير المستبعد أن تحل القنابل الالكترونية محل القنابل التقليدية والذرية ، وبذلك يعتقد ريتشارد كلارك ، المستشار الخاص لرئيس الولايات المتحدة بشأن الأمن السيبراني ، أن النزاعات السيبرانية لديها القدرة على تغيير التوازن العسكري في العالم ، وبالتالي تغيير العلاقات السياسية والاقتصادية بشكل جذري[١].

يقول جون ستون إن الحرب الإلكترونية موجودة وأن الأعمال الحربية تستخدم القوة لإحداث تأثيرات عنيفة، هذه الآثار العنيفة ليست بالضرورة قاتلة بطبيعتها ، ولكن لا يزال من الممكن أن يكون لها آثار تدميرية ولا تزال تندرج ضمن فئة الحرب ، كون أنظمة المعلومات التي تتحكم في البنية التحتية الحيوية معرضة بشكل كبير للهجمات السيبرانية ، وبالتالي ما لم يتم تحسين الدفاعات الإلكترونية وتحسين الثغرات الأمنية النظامية في الأنظمة التابعة ، فإن الحروب الإلكترونية أمر لا مفر منه [٢].

وبذلك يعرف الامن السيبراني بأنه عبارة عن مجموعة من الوسائل التقنية التنظيمية والإدارية التي يتم استخدامها لحماية الشبكات والأجهزة والبرامج والبيانات من الهجمات والمخاطر

والتهديدات من طرف ثاني ، او هو استخدام الوسائل والدفاعات لغرض مواجهة الهجمات على البرامج والبيانات والشبكات وتجنب اثارها [٣].

ومن وجهة نظر ستيفن والت ، فإن التهديدات للدول هي نتيجة عدة عناصر كالقوة ، والقرب الجغرافي ، والقدرات ، والنوايا العدوانية ، كما ساهمت مشاكل عدم الكشف عن الهوية ومصادر الهجمات الإلكترونية إلى تفاقم الطبيعة الفوضوية والمعضلة الأمنية للفضاء الإلكتروني الدولي ، مما يشكل تهديدًا خطيرًا على الدول [٤].

ما تم ذكره جعل الخوف من المجهول والشعور بانعدام الأمن الناجم عن الخصائص التقنية للفضاء السيبراني ، دفع الدول الى تعزيز بناء القدرات الهجومية والدفاعية السيبرانية ، وحتى اتخاذ استراتيجيات وقائية لحماية أمنها، وبالنسبة لبعض القوى السيبرانية أصبحت صياغة استراتيجية إلكترونية وطنية اهم اولوياتها ، وتطورت الى القوة الإلكترونية كخدمة جديدة أخرى بعد القوة البرية والبحرية والقوة الجوية ، وهي القوة المهمة لتحقيق الامن السيبراني .

وتأكيدا على اهمية القوة السيبرانية فقد عرفها جوزيف.س ناي ، وهو أبرز المهتمين بالقوة السيبرانية بأنها القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني [٥]، لذلك من المتوقع أن يكون هناك المزيد من المهاجمين والمخربين ، لان الهجمات الإلكترونية اصبحت تزيد من فرص مهاجمة الدولة الأصلية للهدف المطلوب وإلحاق الضرر به ، مع تقليل المخاطر التي تتحملها الدولة الأصلية لأنه من السهل إرسال رمز برمجة خاص بدلاً من إرسال قوات خاصة ومعدات عسكرية تقليدية .

يشير كل من كينيث كناب وويليام بولتون إلى أن الأسلحة السيبرانية واسعة النطاق والقوية منها أصبحت أرخص وأكثر توفرا ، بحيث يمكن للمهاجمين صنع قنبلة كهرومغناطيسية مقابل أقل من ٤٠٠ دولار ، لتتضمن أساليب الهجوم على الشبكة بشكل أساسي التخريب ، وحرمان وتعطيل الموزع للخدمة ، والاختراق ، و يمكن تقسيم اختراق الشبكة إلى الفيروسات ، والديدان ، والمراقبة ، مما يعني ان تكلفة هذه الهجمات الإلكترونية لا تكاد تذكر بالنسبة للدولة ، ولا تؤدي إلى تحمل أي مخاطر او وقوع إصابات، بالتالي مهما كانت تكلفة الهجمات الإلكترونية عالية ، فإنها أقل من الأنواع الأخرى من الأسلحة [٦].

وكحالة مؤكدة لتأثير الخطر السيبراني، تعد عملية شمعون الإيرانية ضد شركة أرامكو السعودية عام ٢٠١٢ من خلال هجوم الكتروني خطير بواسطة اختراق فايروس ضار للشبكة ، ففي غضون ساعات قليلة تم مسح أكثر من ٣٥٠٠٠ جهاز كمبيوتر جزئيًا أو تدمير أجهزة الكمبيوتر كليا بحيث قضى الفيروس على ٨٥ في المائة من بيانات الكمبيوتر لشركة أرامكو

السعودية واستبدلها بصورة لعلم أمريكي محترق، وتوصل خبراء الكمبيوتر الى ان هذا النوع الجديد من الفيروسات (شامون)، المعروف أيضًا باسم (W32.DisTrack) تحتوي على البرامج الضارة كتأثير قنبلة منطقية تؤدي إلى تشغيل مسح البيانات وتجعل أجهزة الكمبيوتر المتصلة بالشبكة غير قابلة للاستخدام [٧].

والحالة الثانية ، هي عملية الولايات المتحدة ستوكسنت (Stuxnet) ضد إيران وهي عبارة عن دودة كمبيوتر تم اكتشافها في يونيو ٢٠١٠، الهدف الرئيسي للفيروس هو المنشأة النووية لمحطة تخصيب اليورانيوم في إيران من خلال استهداف وحدات التحكم المنطقية القابلة للبرمجة (PLCs) ، والتي تسمح بهكر العمليات الكهروميكانيكية ، مثل تلك المستخدمة للتحكم في الآلات على خط تجميع المصنع أو أجهزة الطرد المركزي المستخدمة لفصل المواد النووية ، حيث دمر فيروس (Stuxnet) نظام التحكم المنطقي القابل للبرمجة في إيران ، وجمع معلومات عن الأنظمة الصناعية ، وتسبب في تفكك أجهزة الطرد المركزي سريعة الدوران ، فقد دمر الفيروس ما يقرب خمس أجهزة الطرد المركزي الإيرانية ، وأصاب أكثر من ٢٠٠ ألف جهاز كمبيوتر ، وتسبب في تدهور مادي لألف جهاز ، وعطل البرنامج النووي الإيراني لمدة عامين[٨].

الفضاء السيبراني كمجال جديد للجغرافيا السياسية

كسر الفضاء الالكتروني حدود الفضاء الجغرافي التقليدي الأرض والبحر والجو ، فهو لا يمثل نتاجًا للطبيعة ، بل هو مساحة مبنية بشكل مصطنع ، استطاع تغيير التفكير الجيوسياسي التقليدي القائم على الفضاء الجغرافي الطبيعي من خلال الغاء الحدود الجغرافية التقليدية بين البلدان.

تعد ولادة الإنترنت هي نتاج الجغرافيا السياسية ، نتيجة الصراع الجيوسياسي بين الولايات المتحدة والاتحاد السوفيتي خلال الحرب الباردة، ففي ١٩٦٩ أطلقت وزارة الدفاع الأمريكية مشروع بحث عسكري يسمى ARPAnet لتوفير أنظمة اتصالات لمساعدة الولايات المتحدة في الدفاع ضد الهجوم النووي.[٩]

منذ ذلك الحين وبجهود العديد من العلماء ، تم تشكيل الإنترنت لأول مرة في الولايات المتحدة وأوربا ، فبعد انتهاء الحرب الباردة هدأت البيئة الدولية ، ودخل الإنترنت حيز التشغيل التجاري وبدأ ينتشر بسرعة حول العالم ، مكون من ثلاثة مستويات: الأول هو طبقة البنية التحتية للكيانات المادية ، بما في ذلك مرافق أجهزة الإنترنت مثل الكابلات الضوئية البحرية والخوادم وأجهزة الكمبيوتر الشخصية والأجهزة المحمولة ، الثاني يمثل الطبقة المنطقية المكونة

من المعايير التي تستخدم أنشطة مستخدمي الإنترنت كوسيلة للتوسع في المجالات السياسية والاقتصادية والاجتماعية ، والثالث هو طبقة المحتوى المكونة من مواقع الويب والخدمات والتطبيقات والبيانات المختلفة . ، وبالتالي تكوين فضاء إلكتروني متعدد الأبعاد.

في وقتنا الحاضر اصبح يطلق على الإنترنت اسم طفل الحرب الباردة ، على الرغم من اختلاف الفضاء الإلكتروني عن Arpanet الأصلي ، إلا أنه لا يزال يتمتع بسمات جيوسياسية ، فهو يمثل مجال جديد للجغرافيا السياسية استنادا الى العديد من الروابط فمكونات الفضاء السيبراني لها سمات جغرافية ، و أيضًا الموضوعات النشطة للفضاء السيبراني لها سمات جغرافية فاستخدام القوة السيبرانية يرتبط بالخلفية الجغرافية ، لأنه غالبًا ما يمكن استخدام السمات الجغرافية السياسية لتحليل هوية ودوافع ونوايا الجهات الفاعلة في الفضاء السيبراني ، كما يعتمد المشغلون والمستخدمون والمديرون والمستفيدون من مرافق الفضاء الإلكتروني على المساحة الجيوسياسية الفعلية المنفصلة ماديًا.

ويعتقد ديفيد كلارك ، الأستاذ في معهد ماساتشوستس للتكنولوجيا ، أنه يمكن تقسيم الفضاء الإلكتروني إلى أربعة مستويات بترتيب تنازلي من حيث الأهمية ، أحدهما المشاركون في نشاط الشبكة ، الذين يشاركون في الاتصال ، ويولدون المعلومات ، ويتخذون القرارات ، وينفذون الخطط ، والآخر هو تخزين الفضاء الإلكتروني للمعلومات التي يتم نقلها وتغييرها ، والثالث هو الهياكل المنطقية المختلفة التي تحافظ على خدمات وعمليات الفضاء الإلكتروني ، والرابع هو المرافق المادية التي تدعم الهياكل المنطقية.(١٠)

فالمشاركون في أنشطة الشبكة ، أي الأشخاص هم الأكثر أهمية كمستوى بشري وأيضًا كمستوى الاجتماعي ، ولا يمكن للناس في المجتمع الحقيقي الابتعاد عن الجغرافيا السياسية التقليدية ، حتى الإرهابيون استفادوا بالكامل من الخصائص الجيوسياسية للفضاء السيبراني لجمع الأموال أو تجنيد الأعضاء ، لذا لا يغير وصول عصر البيانات الضخمة السمات الجغرافية لأنشطة الفضاء الإلكتروني ، فهي جزء مهم من البيانات الضخمة في وسائل التواصل الاجتماعي والحوسبة السحابية والإنترنت عبر الهاتف المحمول ، كما إن الموضوعات النشطة لوسائل التواصل الاجتماعي والإنترنت عبر الهاتف المحمول تعود لأشخاص ينتمون إلى فضاء جغرافي سياسي معين(١١).

ومن السمات الجغرافية السياسية للفضاء السيبراني أيضًا من القوة الصاعدة للدول ذات السيادة في الفضاء السيبراني، فعلى الرغم من أنه في الأيام الأولى لتطوير الإنترنت ، تبنت الحكومات الوطنية بشكل أساسي موقف عدم التدخل ، على اعتبار انها تقنية خاصة خالية من

القرارات الحكومية ، لكن أي شيء له تأثير كبير على حياة الناس يجب أن تنظمه الحكومة في نهاية المطاف ، فعلى الرغم من أن العولمة التي أحدثها الإنترنت قد تكون قد غيرت أدوات الأمن القومي في بعض الجوانب ، إلا أن الدولة في الواقع تحافظ على سيادتها الداخلية والخارجية بل وتعززها ، لأنها فقط هي التي ستكون أكثر اهتمامًا بالمخاطر السياسية الناجمة عن تطور الفضاء السيبراني ، والاستقرار السياسي هو الشرط الأساسي لاستقرار اجتماعي[١٢].

وبما ان التنمية الاقتصادية تعد جزء وظائف الحدود الوطنية في المفهوم المادي هو تقسيم الحدود بين الاستقرار الداخلي و عوامل الاضطراب الخارجي من هذا المنظور ، فإن حدود المعلومات هي أيضًا منطقة وطنية جديدة تلتزم فيها الدولة بالأمن ، لذلك ستستخدم الدول القوة الوطنية للتعامل مع التهديدات السيبرانية ، وتظهر الحروب الإلكترونية تدريجياً ، وهي إحدى الاتجاهات التي تعكس بشكل أفضل الجغرافيا السياسية للفضاء السيبراني[١٣].

نستنتج مما تقدم ان البيئة الجغرافية هي مرتكز الاطار النظري الجغرافي السياسي على الرغم من أن الفضاء الإلكتروني ليس له موقع جغرافي ومادي ثابت ، إلا انه قد يستطيع أن يغير مركز ثقل القوة الجغرافية السياسية من خلال تأثيره على المجالات الأخرى ، لذلك أصبحت الشبكة العنكبوتية مساحة جديدة ، وليست ملحقًا بالمجالات الأربعة التقليدية ، بل هي مثل القائد غير المرئي ، الذي يربط المجالات المكانية الأربعة السابقة لتشكيل بنية ديناميكية للتفاعل متعدد الأبعاد والتكامل .

فالفضاء الإلكتروني الجديد غير مادي وافتراضي ، لكنه موجود في كل مكان في العالم المادي ولم يعد الفضاء الإلكتروني منطقة مثالية يتم فيها تبادل المعلومات بحرية ، ولكن مجالًا جديدًا للجغرافيا السياسية ، فالتنافس في الفضاء الإلكتروني لا يمكن فصله عن الجغرافيا السياسية ، كونه يعد مجالًا عالميًا لا تؤثر الخصائص الجغرافية السياسية للفضاء السيبراني على الوصول إلى الشبكة وسرعة الشبكة والموثوقية فقط ، بل تؤثر أيضًا على الحوكمة العالمية للفضاء السيبراني ، كما تؤثر أيضًا على طبيعة التنافس والصراع السيبراني بين الدول والذي يتركز حول قطاعات البنية التحتية الحيوية مثل الطاقة والنقل العام والتصنيع.

الثاني : تقييم الامن السيبراني لدول المشرق العربي

تعكس قوة الامن السيبراني قوة الدولة من الناحية الاقتصادية والسياسية والاجتماعية والعسكرية ، لذلك يعد قياسه ليس بالأمر اليسير ، لارتباطه بعدة جوانب منها اقتصادية واجتماعية وسياسية وعسكرية [١٤]. وفي هذا الاطار سنحاول الكشف عن وزن الامن السيبراني

لدول المشرق العربي بالاعتماد على ثلاثة مقاييس عالمية رئيسة ، ومقارنة ذلك بأهداف تكتيكية تركيا وايران والكيان الصهيوني كجوار جغرافي اقليمي ، والولايات المتحدة الامريكية دوليا .

١: مؤشر الحكومة الالكترونية(*) لدول المشرق العربي

ويقيم المؤشر مدى تطور الحكومة الإلكترونية لدول المشرق العربي على المستوى الوطني، وهو مؤشر مركب يعتمد على المتوسط المرجح لثلاثة مؤشرات موحدة ، الثلث الأول مستمد من مؤشر البنية التحتية للاتصالات ، والثلث الثاني من مؤشر رأس المال البشري والثلث الأخير من مؤشر الخدمة عبر الإنترنت والتي تقيم التواجد الوطني عبر الإنترنت .

أ : مؤشر البنية التحتية للاتصالات

هو مؤشر مركب يمثل المتوسط الحسابي لأربع مؤشرات فرعية ، وهي الاول مؤشر اشتراك الهاتف الخلوي لكل ١٠٠ نسمة ، ويشمل أي هاتف محمول مشترك في خدمة هاتف نقال عامة باستخدام تكنولوجيا الهاتف الخلوي، و التي توفر الوصول إلى شبكة هاتف أرضية عامة والثاني الافراد المستخدمين للأنترنيت لكل ١٠٠نسمة ، يشير إلى نسبة الأفراد الذين استخدموا الإنترنت من أي مكان في الأشهر الثلاثة الماضية، اما الثالث ، هو اشتراك النطاق الثابت العريض السلكي لكل ١٠٠نسمة إلى مجموعة الاشتراكات والنطاق العريض النقال لنقل البيانات والصوت واشتراكات النطاق العريض النقال وهو يغطي الاشتراكات المستخدمة للوصول إلى الإنترنت بسرعات النطاق العريض، وليس اشتراكات إمكانية الوصول المحتمل، والرابع اشتراك النطاق الثابت العريض اللاسلكي النشط لكل ١٠٠نسمة إلى الاشتراكات الثابتة للوصول عالي السرعة إلى الإنترنت العام أو الاتصال ببروتوكول نقل البيانات / بروتوكول البيانات) TCP/IP،(بسرعات استلام بيانات تساوي أو تزيد عن 256 كيلو بايت / ثانية ، وهذا يشمل مودم ذو كابل، وخط المشترك الرقمي (DCI) توصيل كبل الألياف إلى المنزل / المبنى، واشتراكات النطاق العريض الثابتة / السلكية الأخرى، والنطاق العريض للأقمار الصناعية (الساتلي) والنطاق العريض اللاسلكي الثابت الأرضي(١٥).

ومن بيانات الجدول (١) وخريطة (١) نلاحظ تطورا ملحوظا في قيمة المؤشر لعام ٢٠٢٢ مقارنة لعام ٢٠٢٠ بالنسبة لدول المشرق العربي ، حيث شهدت دول مجلس التعاون الخليجي عدا (قطر والكويت) ارتفاعا في قيم المؤشر فقد حصلت الامارات العربية على المرتبة ١٣ عالميا ، حيث بلغت قيمة المؤشر ٠.٨ الى ٠,٩ وذلك لقيامها بإنشاء بنية تحتية أساسية من النظم الرقمية المشتركة والتكنولوجيات والعمليات والنماذج التنظيمية التي وفرت إطارًا قويًا يتسم بالمرونة في نفس الوقت، بهدف تنمية وتقديم الخدمات الحكومية التي تركز على المستخدمين

وترتكز على البيانات ، والعربية السعودية المرتبة ٣١ عالميا لتصبح قيمة المؤشر ٠,٨ بعد ان كانت ٠,٧ وهذا يدل على قوة البنية التحتية لتكنلوجيا الاتصالات والمعلومات والاتصال الموثوق والمتاح وبخاصة الانترنيت عريض النطاق والذي يلعب دور مهم في تحقيق القوة السيبرانية .

اما بقية دول الاقليم فقد حصلت عمان على ٠,٧٨ لتحتل المرتبة ٥٠ والبحرين ٠,٧٧ بالمرتبة ٥٤ والكويت ٠,٧٤ بالمرتبة ٦١ عالميا ، اما بالنسبة لبقية دول الاقليم فقد حصلت على مستويات متدنية تعكس خطورة امنها السيبراني فالأردن بلغت قيمة المؤشر ٠,٦ لتحتل المرتبة ١٠٠ عالميا ولبنان ٠,٥ بالمرتبة ١٢٢ والعراق ٠,٤ بالمرتبة ١٤٦ عالميا وسوريا واليمن ٠,٣ و ٠,٢ بالمرتبة ١٥٦ و١٧٨ عالميا لكل منهما على التوالي .

وبالمقارنة مع دول الجوار الاقليمي والدولي نجد ان الولايات المتحدة الامريكية تقدمت على دول المشرق العربي وبلغت قيمة المؤشر ٠,٩٢ لتحتل المرتبة ١٠ عالميا في حين ان الكيان الصهيوني ظهرت قيمة المؤشر ٠,٨٨ لحتل المرتبة ١٦ عالميا وهو اعلى من جميع دول الاقليم العربي عدا الامارات العربية والسعودية ، كذلك الحال بالنسبة لتركيا وايران فقد ظهرت بمستويات مقاربة مع دول المشرق العربي وبخاصة مع دول مجلس التعاون الخليجي ، وافضل حالا من بقية دول الاقليم وبخاصة العراق وسوريا والاردن واليمن وهذا يعد نقطة ضعف وخلل من منظور الامن السيبراني .

خلاصة ما تقدم ان جميع دول مجلس التعاون الخليجي استطاعت ان تنتقل من مستويات منخفضة الى مستويات عالية وعالية جدا وهذا يرتبط بمستوى الدخل القومي للدولة فبما انها ذات دخل مرتفع ساهم في إحراز قيم مؤشر تطور الحكومة الإلكترونية أعلى من الدول ذات الدخل المنخفض ، مما يعني الدقة والموثوقية في الاتصال بالأنترنيت عريض النطاق ، فضلا عن وجود تشريعات ولوائح وتدابير وسياسات ملائمة وحديثة لتكنلوجيا المعلومات والاتصالات والرقمنة ، اضافة الى الاستثمار الكبير في بنية التكنلوجيا والمعلومات والاتصالات مما يسهم في بناء قوة في البنية التحتية وبما يعزز قوة الامن السيبراني .

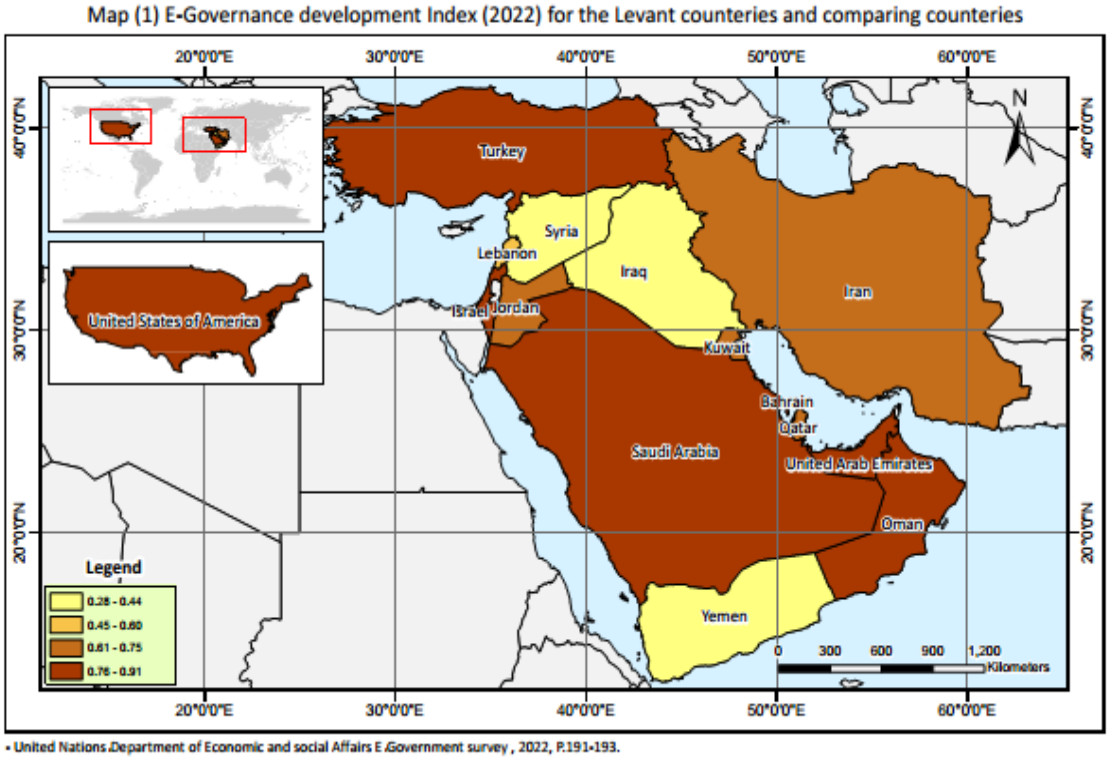
جدول (١) مؤشر تطور الحكومة الإلكترونية لدول المشرق العربي ودول المقارنة ٢٠٢٠-٢٠٢٢

الدولة	التصنيف	المرتبة عالميا	مؤشر الخدمة عبر الانترنيت	مؤشر راس المال البشري	مؤشر البنية التحتية للاتصالات	مؤشر تطور الحكومة ٢٠٢٢	مؤشر تطور الحكومة ٢٠٢٠
العراق	MH	١٤٦	٠.٢٠٦	٠.٥٨٨٨	٠.٥٢٠١	٠.٤٣٨٣	غير متوفر
العربية السعود	V2	٣١	٠.٨٢٢٠	٠.٨٦٦٢	٠.٨٧٣٥	٠.٨٥٣٩	٠.٧٩٩١

ية							
الامارات العربية	VH	١٣	٠.٩٠١٤	٠.٨٧١١	٠.٩٣٠٦	٠.٩٠١٠	٠,٨٥٥٥
قطر	VH	٧٨	٠.٦٠٩٤	٠.٧١٥٠	٠.٨٢٠٣	٠.٧١٤٩	٠.٧١٧٣
البحرين	V1	٥٤	٠.٧٥٢٣	٠.٨١٥٤	٠.٧٤٤٤	٠.٧٧٠٧	٠.٨٢١٣
عمان	V1	٥٠	٠.٧٤٢٣	٠.٨٠٦٧	٠.٨٠١٢	٠.٧٨٣٤	٠.٧٧٤٩
سوريا	M3	١٥٦	٠.٣٠٥٣	٠.٤٩٨٣	٠.٣٥٨١	٠.٣٨٧٢	غير متوفر
الكويت	VH	٦١	٠.٦٩٧٣	٠.٧٧٠٦	٠.٧٧٧٤	٠.٧٤٨٤	٠.٧٩١٣
لبنان	H1	١٢٢	٠.٤٢٥٧	٠.٦٦٥٦	٠.٤٩٠٧	٠.٥٢٧٣	غير متوفر
اليمن	M1	١٧٨	٠.٣٣٩٣	٠.٣٦٣٣	٠.١٦٧١	٠.٢٨٩٩	غير متوفر
ايران	H3	٩١	٠.٤١٩٦	٠.٧٨٠٤	٠.٧٣	٠.٦٤٣٣	غير متوفر
الاردن	H2	١٠٠	٠.٦٥٩٤	٠.٦٩٦٧	٠.٤٦٨١	٠.٦٠٨١	غير متوفر
تركيا	V1	٤٨	٠.٨٦٠٠	٠.٨٧٢٢	٠.٦٦٢٦	٠.٧٩٨٣	٠.٧٧١٨
الكيـــان الصـــهيو ني	V3	١٦	٠.٨٧٤٥	٠.٨٩٩٤	٠.٨٩١٥	٠.٨٨٨٥	٠.٨٣٦١
امريكا	VH	١٠	٠,٩٣٠٤	٠,٩٢٧٦	٠,٨٨٧٤	٠,٩١٥١	٠,٩٢٩٧

United nations , department of economic and social affairs , E – Government survey , 2022 , P.191-193.

خريطة (١) مؤشر الحكومة الالكترونية لدول المشرق العربي ودول المقارنة



• United Nations ,Department of Economic and social Affairs E ,Government survey , 2022, P.191-193.

ب : مؤشر رأس المال البشري (HCI)

يعد راس المال البشري من اهم عوامل النجاح الرئيسة لأي مبادرة للأمن والقوة السيبرانية كون ان المهارات والمعلومات والتدريب والتعليم اصبحت سلعا لها اهمية كبيرة .

يقيس المؤشر مدى نجاح او اخفاق السياسات الرامية الى تنمية الموارد البشرية والاهتمام براس المال البشري من اجل النهوض بواقعها السياسي والاقتصادي والاجتماعي ، من خلال أربع مكونات هي نسبة الإلمام بالقراءة والكتابة لدى الكبار، هو نسبة مئوية من السكان تبلغ اعمارهم ١٥ سنة فاكثر والذين يمكنهم القراءة والكتابة لعبارة بسيطة لحياتهم اليومية [١٦].

والنسبة الإجمالية للالتحاق بالمدارس الابتدائية والثانوية والجامعية ، هي نسبة الطلاب الملتحقين بالمرحلة الابتدائية والثانوية و الجامعة بغض النظر عن العمر من (٤-١٧) سنة[١٧].

و سنوات الدراسة المتوقعة ، وهي اجمالي عدد السنوات المتوقعة التي من المتوقع لطفل ان يكملها ببلوغه ١٨ سنة ، و متوسط سنوات الدراسة هو متوسط عدد سنوات التعلّم التي اكملها السكان البالغين في دولة ما ٢٥ سنة او اكثر [١٨].

ومن الجدول (٢) نجد ان جميع دول المشرق العربي قد حصلت على مستويات عالية وعالية جدا عدا سوريا واليمن فقد حصلا على مستوى منخفض لقيم المؤشر ، وقد احتلت العربية

السعودية المرتبة الاولى عربيا والثانية والعشرون عالميا وبلغت قيم المؤشر ٠,٩٦ ، ضمن فئة التصنيف العالي جدا ، وحصلت كل من الكويت والبحرين وعمان على مراتب متقدمة ضمن المستوى العالي جدا حيث بلغت قيم المؤشر ٠,٨٨ و٠,٨٧و٠,٨٧ لكل منهم وعلى التوالي.

كما حصلت الامارات العربية على قيمة مؤشر ٠,٨٢ ضمن المستوى العالي جدا والكويت ٠,٧١ وفي نفس المستوى ، لكن بفئة V2 و V3 لكل منهما على التوالي ، في حين حصل العراق على قيمة ٠,٦٥ ضمن المستوى العالي ، في حين انخفضت قيم المؤشر لكل من سوريا واليمن الى مستويات خطيرة لتبلغ ٠,٤٩ و ٠,٣٦ لكل منهما على التوالي .

ومن خلال المقارنة مع الاهداف الاقليمية والدولية يظهر ان الولايات المتحدة قد تفوقت على جميع دول اقليم المشرق العربي ، لتحتل المرتبة ١٥ عالميا بقيمة مؤشر ٠,٩٧ ، وفيما يخص اهداف المقارنة الاخرى ، تقدمت كل من تركيا والكيان الصهيوني على جميع دول المشرق العربي عدا العربية السعودية حيث بلغت قيمة المؤشر ٠,٩٥ لكل واحدة منهما ، كما حققت ايران تقدم على بعض دول الاقليم وبخاصة الامارات العربية وقطر.

يكمن القول ان معظم دول المشرق العربي هي واقعة ضمن المستويات العالية جدا والتي تقع ضمنها الاهداف المقارنة لكن بفئات متباينة مما يعني ارتفاع مستويات التعليم وزيادة ميزانيات الانفاق الخاصة بالتعليم ، في حين يمكن تعليل انخفاض مستويات مؤشر راس المال البشري في العراق وسوريا واليمن الى الصراعات الداخلية والحروب التي عملت على اضعاف راس المال البشري من خلال عدم الاستقرار وانعدام الامن لدى السكان والتي اثرت على مستويات التعليم .

جدول (٢) مؤشر راس المال البشري لدول المشرق العربي

الدولة	مؤشـــر راس المال البشري	**مستوى** مؤشر راس المال البشري	فئة التصنيف	الترتيب العالمي
العراق	٠.٦٥	عالي	H3	١٤١
العربية السعودية	٠.٩٦	عالي جدا	VH	٢٢
الامارات العربية	٠.٨٢	عالي جدا	V2	٩٣
قطر	٠.٧١	عالي جدا	V1	١١٩
البحرين	٠.٨٧	عالي جدا	V2	٥٤
عمان	٠.٨٧	عالي جدا	V2	٦٢
سوريا	٠.٤٩	متوسط	M	١٥٣
الكويت	٠.٨٨	عالي جدا	V3	٥٨
لبنان	٠.٦٦	عالي	H3	١٣١
اليمن	٠.٣٦	متوسط	M	١٧٧

ايران	٠.٨٣	عالي جدا	V2	٧٤
الاردن	٠.٦٩	عالي	H 3	١٣٥
تركيا	٠.٩٥	عالي جدا	VH	٢٤
الكيان الصهيوني	٠.٩٥	عالي جدا	VH	٣٢
امريكا	٠,٩٧	عالي جدا	VH	١٥

الامم المتحدة ، دائرة الشؤون الاقتصادية والاجتماعية ، مسح الحكومة الالكترونية ٢٠٢٢، مستقبل الحكومة الرقمية ، جدول ٢-٣ص٦٩و٢-٩ ص٨٣.

ج : مؤشر الخدمة عبر الانترنيت (OSI)

يعد مكون مؤشر الخدمة عبر الإنترنت الخاص بمؤشر تطور الحكومة الإلكترونية مؤشرًا مركبًا يقيس استخدام تكنولوجيا المعلومات والاتصالات من قبل الحكومات لتقديم الخدمات العامة على المستوى الوطني.

ومن الجدول (٣) نلاحظ ان الامارات العربية حصلت على المرتبة الاولى ضمن دول المشرق العربي وبلغت قيمة المؤشر ٠,٩ وبتصنيف عالي جدا ضمن الفئة V2 وهذا ينبع إلى حد كبير من المستويات المرتفعة أو المرتفعة جدًا من مؤشر رأس المال البشري و مؤشر البنية التحتية للاتصالات ، وحصلت العربية السعودية على المرتبة الثانية بقيمة مؤشر ٠,٨٢ لتحتل المرتبة ١٤ عالميا ، في حين جاءت كل من البحرين وعمان والاردن والكويت وقطر ضمن التصنيف العالي وبقيم ٠,٧٥ ، ٠,٧٤ ، ٠,٦٩ ، ٠,٦٥، ٠,٦ على التوالي ، بينما ظهرت كل من لبنان وسوريا بمستوى متوسط في قيم المؤشر ، ويبرز مكمن الخطر لقيم المؤشر في العراق واليمن حيث بلغت قيمته ٠,٢ و ٠,٣ على التوالي وبمستوى منخفض ، مما يعني التخلف في توفير الخدمات عبر الإنترنت نتيجة التأخر في البنية التحتية وتنمية رأس المال البشري بالرغم من ان الاولى هي من الدول ذات الدخل القومي جيد .

وبالنظر مع دول المقارنة نجد ان الولايات المتحدة تقدمت على دول المشرق العربي حيث بلغت قيمة المؤشر ٠,٩٣ وبالمرتبة الخامسة عالميا ، كما تجاوزت قيم المؤشر لكل من الكيان الصهيوني وتركيا جميع دول الاقليم باستثناء الامارات العربية والسعودية .

نستنتج من ذلك ان معظم دول المشرق العربي احرزت تقدم في الميزات التقنية للبوابات والمنصات الالكترونية التي تقدم الخدمات عبر الانترنيت والتي تساعد المواطن على الاستخدام الصحيح للأنترنيت وبالتالي تساهم في التوجه الى اليات التقدم لاكتساب قوة الدولة ، فضلا عن انها تعكس تطورا في البنية التحتية للاتصالات وراس المال البشري ، اما بالنسبة للدول التي

انفضت فيها قيم المؤشر كالعراق واليمن فهي تعكس ضعف السياسات و الاستراتيجيات للحكومة الالكترونية المطبقة مما يعني تهديد البنية التحتية المادية وغير المادية للفضاء السيبراني.

جدول (٣) مؤشر الخدمة عبر الانترنيت (OSI) لدول المشرق العربي ودول المقارن ٢٠٢٢

الدولة	قيمة (OSI)	التصنيف	الفئة	الترتيب المحلي	الترتيب العالمي
العراق	٠.٢٠٦	منخفض	LM	١٠	٦٩
العربية السعودية	٠.٨٢٢٠	عالي جدا	V3	٢	١٤
الامارات العربية	٠.٩٠١٤	عالي جدا	V2	١	٧
قطر	٠.٦٠٩٤	عالي	H2	٧	٣٤
البحرين	٠.٧٥٢٣	عالي	H2	٣	٢١
عمان	٠.٧٤٢٣	عالي	V1	٤	٢٢
سوريا	٠.٣٠٥٣	متوسط	M3	٩	١٥٦
الكويت	٠.٦٩٧٣	عالي	VH	٥	٢٦
لبنان	٠.٤٢٥٧	متوسط	H1	٧	١٢٢
اليمن	٠.٣٣٩٣	منخفض	M1	٨	١٧٨
ايران	٠.٤١٩٦	متوسط	H3		٥١
الاردن	٠.٦٥٩٤	عالي	H2	٦	١٠٠
تركيا	٠.٨٦٠٠	عالي جدا	V1		١١
الكيان الصهيوني	٠.٨٧٤٥	عالي جدا	V3		١٠
امريكا	٠,٩٣٠٤	عالي جدا	VH		٥

الامم المتحدة ، دائرة الشؤون الاقتصادية والاجتماعية ، مسح الحكومة الالكترونية ٢٠٢٢، مستقبل الحكومة الرقمية ، جدول ٢-٣ص٦٩و٢-٩ ص٨٣.

الثالث : مؤشر القياس العالمي للأمن السيبراني (GCI) لدول المشرق العربي

يقيس هذا المؤشر مستوى تطور دول المشرق العربي في هذا المجال، وهو مؤشر مركب لخمسة من المؤشرات، يتطور لكل تكرار، مهمته قياس مدى التزام دول الاقليم بالأمن السيبراني من خلال خمسة ركائز استراتيجية وهي (التدابير التعاونية)، من خلال معالجة إجراءات الأمن السيبراني الجماعية كونه يمثل أداة أساسية لمواجهة تحديات الأمن السيبراني ، و(التدابير التقنية)والتي تقوم على وضع آليات، وهياكل مؤسسية، فعالة للتعامل مع التهديدات والحوادث السيبرانية على نحو موثوق، اما (التدابير التنظيمية) ، فهي تدرس آليات الإدارة والتنسيق داخل البلدان المعنية بالأمن السيبراني، وتشمل ضمان استدامة الأمن السيبراني ، في حين تقوم (

تدابير بناء القدرات) ، تطوير وتنفيذ الفرق الوطنية المعنية بالاستجابة للحوادث الحاسوبية وفقاً للتشريعات والسياسات الوطنية. ويمكن أن تكون هذه الفرق جزءاً من مؤسسة حكومية أو تحت مظلة وزارة معينة أو كيان آخر، كما تهدف (التدابير القانونية)على وضع تشريعات تحدد ما يشكل الأنشطة غير المشروعة في الفضاء لسيبراني، بالإضافة إلى تعريف الأدوات الإجرائية اللازمة للتحقيق والمقاضاة وتطبيق هذه التشريعات ، وإنشاء خطوط أساسية للأمن السيبراني[١٩].

تتمثل أهداف المؤشر الرئيسة في حساب نوع ومستوى وتطور الالتزام بالأمن السيبراني بمرور الوقت داخل دول الاقليم العربي ومقارنته بالدول الأخرى ، وكذلك قياس مدى التقدم والفجوة بالأمن السيبراني من منظور عالمي واقليمي ، ومساعدة دول الاقليم لتحديد مجالات التحسين ، واتخاذ تدابير خاصة لتقوية تلك المجالات ، ورفع المستوى العام للالتزام بالأمن السيبراني.

كما يهدف ايضا الى الكشف عن الامثلة الناجحة في الأمن السيبراني والتي تكون بمثابة ممارسة جيدة وارشادات لدول المشرق العربي التي لديها بيئات وطنية مماثلة ، كما يضمن امكانات الحد من الخسائر والاضرار التي تنجم في حال تحقق التهديدات والمخاطر، ويضمن إعادة الوضع الى ما كان عليه بأسرع وقت ممكن، ولا تتحول الاضرار الى خسائر دائمة [٢٠].

من الجدول (٤) وخريطة (٢) نجد ان ركائز الامن السيبراني لدول المشرق العربي تواجه انحدار جيوبولتيكي لبعض اجزائه حيث يلاحظ ان دول مجلس التعاون الخليجي عدا اليمن قد حققت معدلات عالية وهذا يرتبط بالإمكانيات المالية العالية فالمملكة العربية السعودية حققت نتائج عالية جدا بقيمة (١) في اربعة ركائز وهي القانونية والتنظيمية وتنمية القدرات والتعاون ، فضلا عن انها حققت المرتبة الاولى على الدول العربية في ركيزة التقنيات بقيمة (٠.٩٨) وحصلت على المرتبة الاولى عربيا والثانية عالميا حيث بلغ اجمالي مؤشر القوة السيبراني فيها (٠.٩٩).

جدول (٤) قياس قوة الامن السيبراني لدول المشرق العربي ودول المقارن ٢٠٢٠

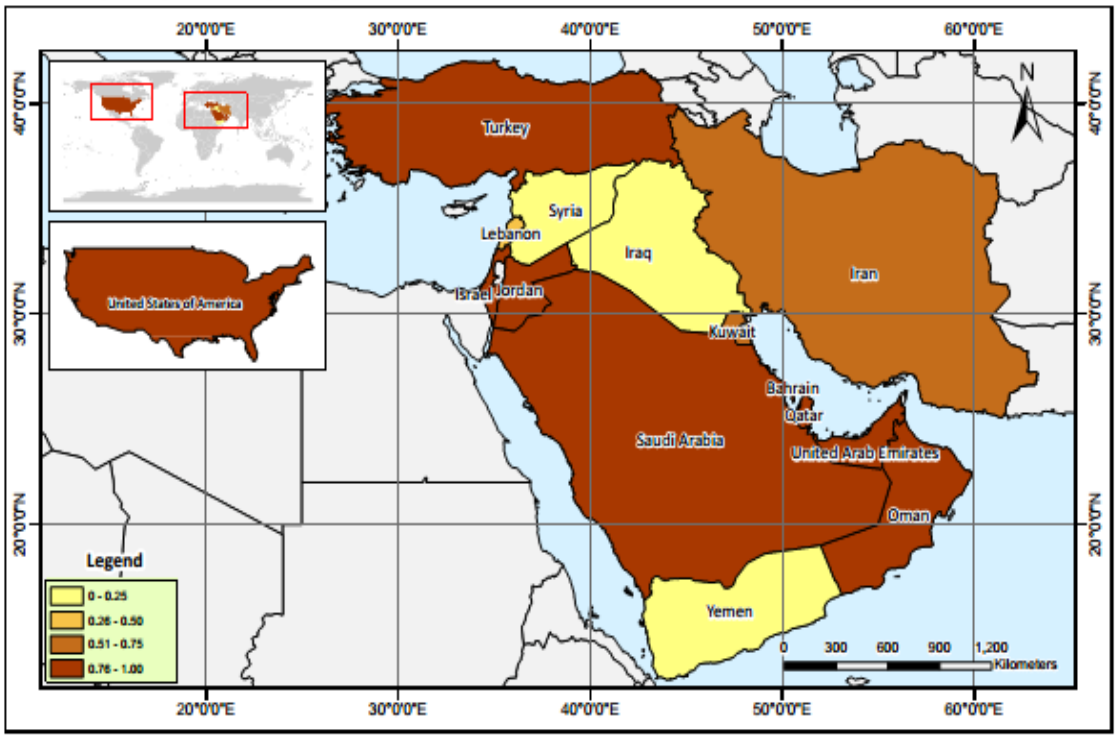
الدولة	قيمة المؤشر ٢٠٢٢	الترتيب	التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية
العراق	٠.٢٠	١٢٩	٠,٠٠	٠.٣٢	٠.٣٨	٠.١٠	٠.٢١
العربية السعودية	٠.٩٩	٢	١	٠.٩٨	١	١	١
الامارات	٠.٩٨	٥	١	٠,٩٥	٠,٩٥	١	١

العربية							
قطر	٠.٩٤	٢٧	١	٠.٨٣	٠.٩٢	١	٠.٩٧
البحرين	٠.٧٨	٦٠	١	٠.٦١	٠.٧٦	٠.٨٤	٠.٦٩
عمان	٠.٩٦	٢١	١	٠.٨٣	١	١	٠.٩٧
سوريا	٠.٢٢	١٢٦	٠.٤٩	٠.٣٩	٠.٢٢	٠,٠٠	٠,٠٠
الكويت	٠.٧٥	٦٥	٠.٨٩	٠.٧١	٠.٥٦	٠.٨٠	٠.٨٠
لبنان	٠.٣٠	١٠٩	٠.٥١	٠.١٦	٠.٢٨	٠.٤١	٠.١٤
اليمن	٠	١٨٢	٠	٠	٠	٠	٠
الاردن	٠.٧١	٧١	٠.٩٢	٠.٥٣	٠.٧٨	٠.٥٧	٠.٧٢
ايران	٠.٨١	٥٤	٠,٨٢	٠.٧٣	٠.٨٤	٠.٨٩	٠.٧٧
تركيا	٠.٩٧	١١	١	٠.٩٨	٠.٩٠	١	١
الكيـــــان الصهيوني	٠.٩١	٣٦	٠.٩٨	٠.٨٥	٠.٧٥	٠.٩٦	١
امريكا	١	١	١	١	١	١	١

International Telecommunication Union (ITU) ,Global cybersecurity Index,2020,P.70,72,74,75,78,79,82,88,116,128

خريطة (٢) مؤشر قوة الامن السيبراني لدول المشرق العربي ودول المقارنة (٢٠٢٠)

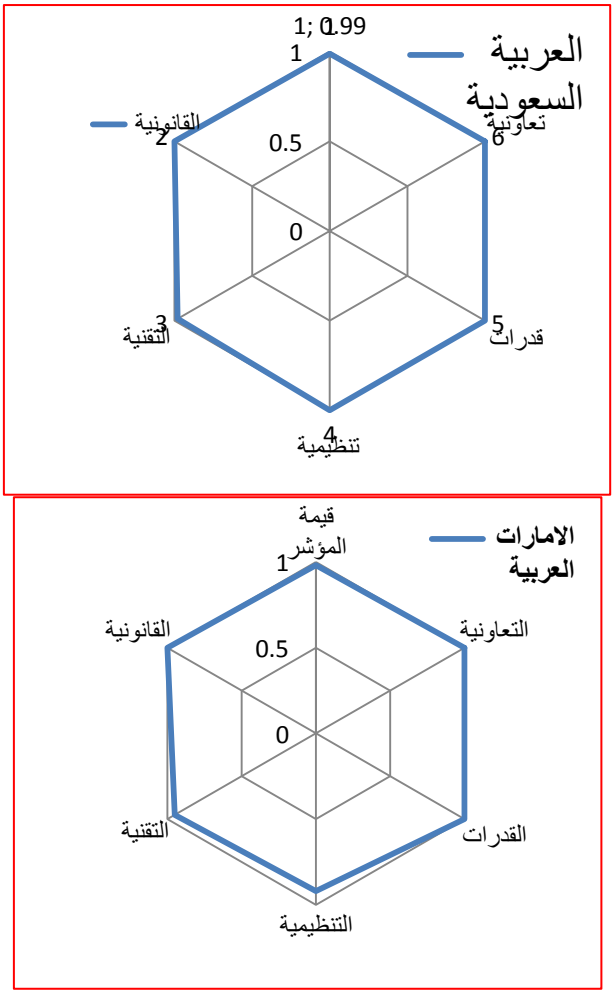
Map (2) Cybersecurity Strength Index (2020) for the Levant counteries and comparing to other counteries



• International Telecommunication Union (ITU) ,Global cybersecurity Index,2020,P.70,72,74,75, 78,79,82,88,116,128

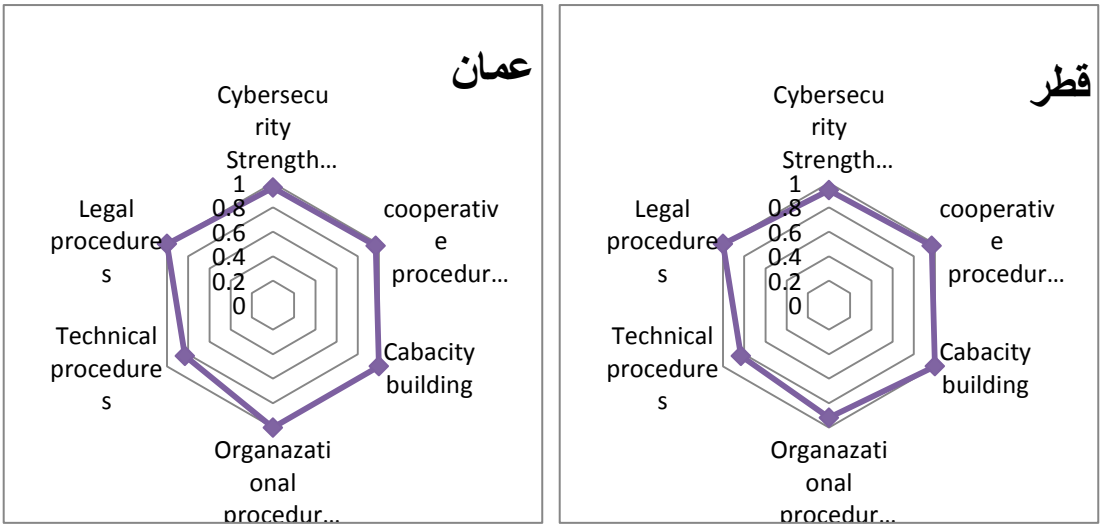
وحصلت الامارات العربية على المرتبة الثانية على مستوى الاقليم والخامسة عالميا ليبلغ مؤشر القوة السيبراني فيها (٠.٩٨) لتتساوى مع المملكة العربية السعودية في قيم الركائز القانونية والتعاونية وتنمية القدرات ، في حين حصلت على قيمة (٠.٩٥) لركيزتي التقنية و التنظيمية.شكل (١) .

شكل (١) قوة الامن السيبراني وركائزه للمملكة العربية السعودية والامارات العربية ٢٠٢٠



اما بالنسبة لبقية دول المجلس والمتمثلة بدولة عمان وقطر فقد حصلت على مستويات اقل حيث بلغت قيمة مؤشر القوة السيبراني لهما (٠.٩٦ و ٠.٩٤) على التوالي ، وبلغت قيم الركائز (١) للتدابير القانونية والتنظيمية والقدرات بالنسبة للأولى ، و الركيزة القانونية وتنمية القدرات للثانية، ليحصلا على المرتبة (٢١ و ٢٧) عالميا . شكل (٢)

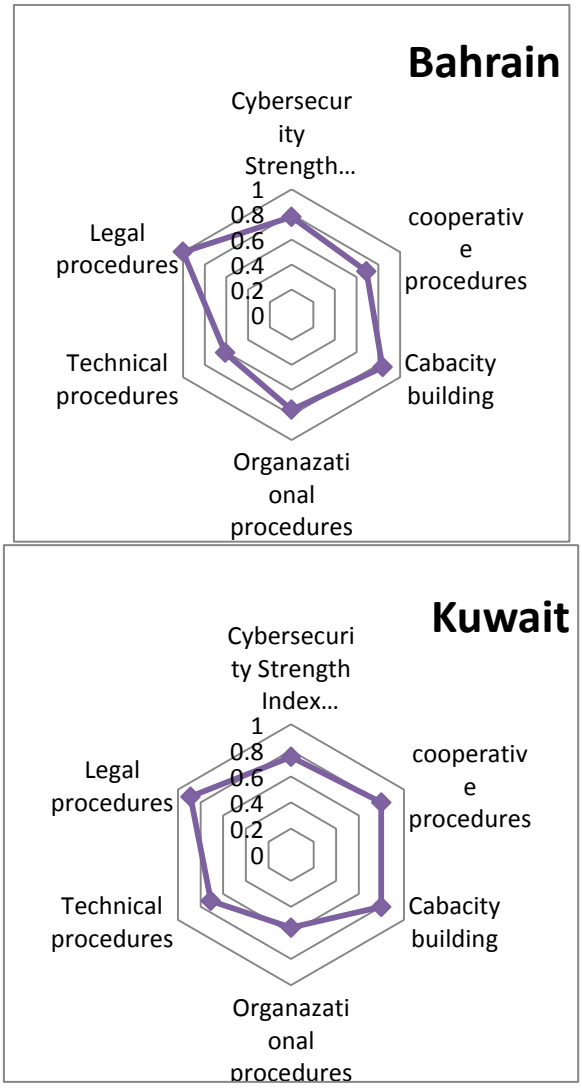
شكل (٢) مؤشر قوة الامن السيبراني وركائزه لدولتي قطر وعمان ٢٠٢٠



المصدر : بالاعتماد على جدول (٤)

وظهر مؤشر مقياس القوة السيبرانية بمستوى اقل بالنسبة لدولتي البحرين والكويت ليبلغ (٠.٧٨ و٠.٧٥) على التوالي بالمرتبة الخامسة والسادسة عربيا والمرتبة ٦٠ و ٦٥ عالميا ، وقد حصلا على قيمة (١) لمؤشر التدابير القانونية ، وقيمة منخفضة للتدابير التقنية للأولى والتنظيمية للثانية مما يعني انهما بحاجة الى استراتيجية وطنية عالية المستوى للأمن السيبراني. شكل (٣)

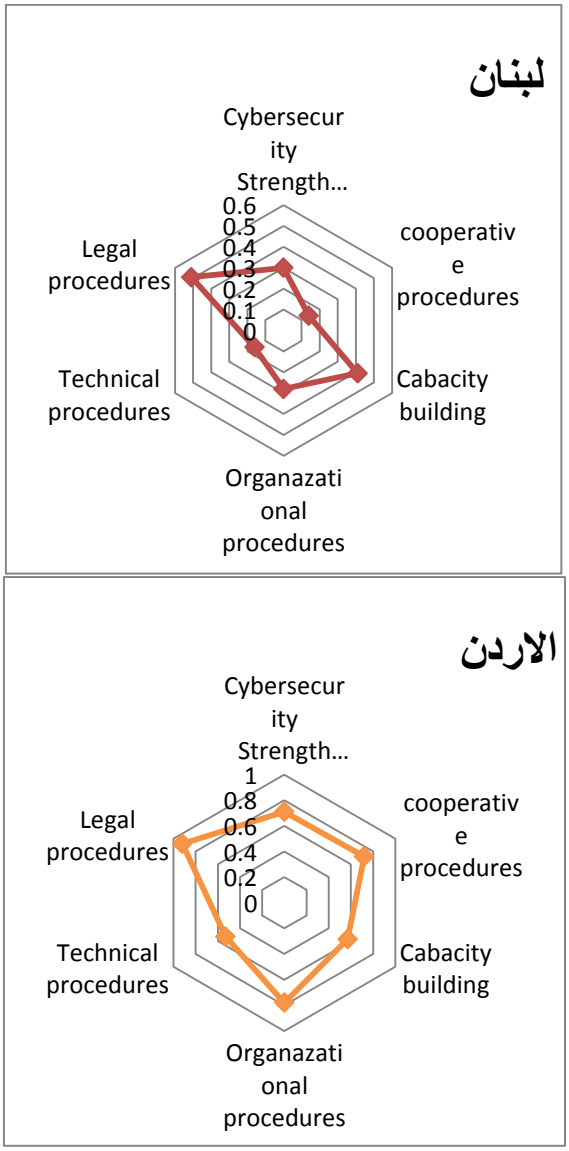
شكل (٣) قوة الامن السيبراني وركائزه لدولتي البحرين والكويت ٢٠٢٠

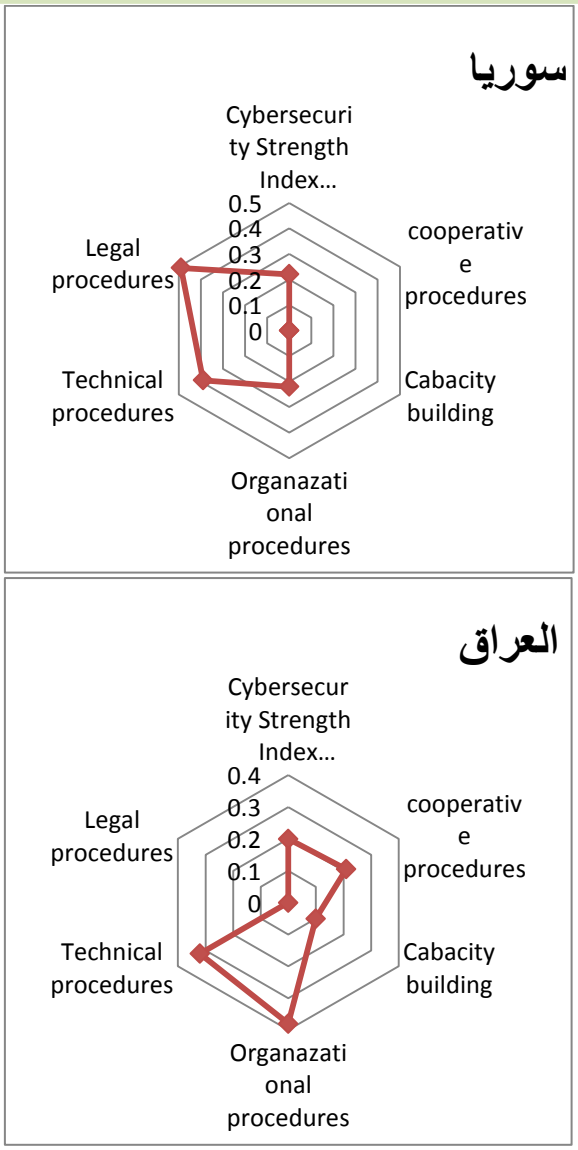


المصدر :جدول (٤)

اما بالنسبة لبقية دول المشرق العربي فقد حصلت الاردن على قيمة مؤشر متدنية ٠.٧١ وهي افضل حالا من بقية دول الاقليم كالعراق وسوريا بقيم (٠.٢٠ و ٠.٢٢) على التوالي ، والذي عكس خطورة امنهما السيبراني من ناحية تعرضهما للتهديدات والهجمات السيبرانية بسبب التراجع الكبير في جميع الركائز ، لتحتل سوريا المرتبة ١٢٦ والعراق ١٢٩ عالميا .شكل (٤)

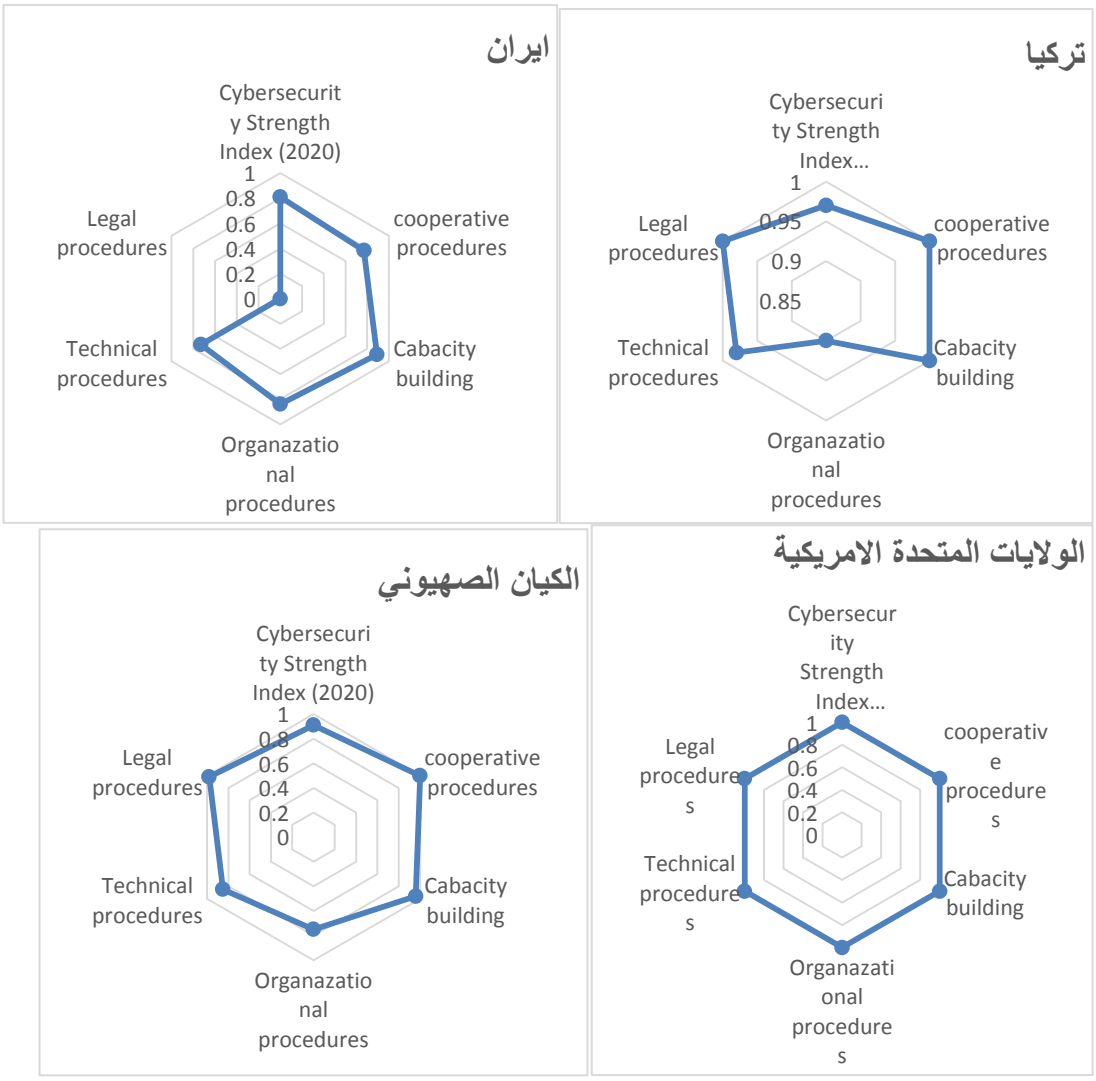
شكل (٤) مؤشر قوة الامن السيبراني وركائزه لدول الاردن و لبنان وسوريا والعراق ٢٠٢٠





وبالمقارنة مع دول الجوار الجغرافي الاقليمي والدولي نجد ان المملكة العربية السعودية تساوت مع الولايات المتحدة الامريكية والتي حصلت على المرتبة الاولى في اربعة ركائز وهي (التعاونية ، وتنمية القدرات ، والتدابير التنظيمية ، والإجراءات القانونية) ، اما ايران التي بلغت قيمة قوتها السيبرانية (٠.٨١) فقد استطاعت ان تحقق كفاءة اعلى من بقية دول دول اقليم المشرق العربي عدا الدول الخليجية (السعودية ، الامارات ، قطر ، عمان) وتحصل على المرتبة (٥٤) عالميا . اما تركيا فقد بلغت قيمة مؤشر قوة الامن السيبراني لها (٠.٩٧) لتحتل المرتبة (١١) عالميا متجاوزة جميع دول الاقليم ماعدا بعض دول مجلس التعاون السعودية والامارات وتساوت معها في الركائز القانونية و التنظيمية و التعاونية ، في حين حقق مؤشر قياس قوة الامن السيبراني الكيان الصهيوني قيمة (٠.٩١) متجاوزا معظم دول اقليم المشرق العربي عدا (السعودية والامارات وقطر وعمان) ليحصل على المرتبة (٣٦) عالميا. شكل (٥)

شكل (٥) مؤشر قوة الامن السيبراني وركائزه لدول المقارنة تركيا وايران والكيان الصهيوني وامريكا ٢٠٢٠



المصدر : بالاعتماد على جدول (٤)

حاصل ما تقدم ان بعض دول المشرق العربي تتمتع بكفاءة ومستوى عالي في جميع ركائز امنها السيبراني، وهذا يعد مصدر قوة للحفاظ على امنها السيبراني ، بينما يواجه البعض الاخر انحدارا جيوبولتيكيا في امنها السيبراني مما يؤثر على تعزيز قوتها من النواحي الاقتصادية والسياسية والاجتماعية والعسكرية ضد التهديدات والهجمات السيبرانية.

الرابع : مؤشر القوة السيبرانية الشاملة لدول المشرق العربي

يعد مؤشر القوة السيبرانية الشاملة (Overall cyber power Index (OCPI اداة قياس يتم من خلالها الكشف عن محددات القوة السيبرانية للدولة ، ونقاط الضعف لفجوة الامن السيبراني والناتجة عن السياسات والاستراتيجيات التي تتبعها الدولة بقصد تعزيز امنها السيبراني ضد التهديدات الخارجية .

تم صياغة معادلة المؤشر بالاعتماد على المتوسط المرجح لمؤشرات الحكومة الالكترونية وهي مؤشر البنية التحتية للاتصالات (TII) ومؤشر راس المال البشري (HCI) ومؤشر الخدمة عبر الانترنيت (OSI) مضروبا بالمتوسط المرجح لركائز الامن السيبراني GCI، وهي التدابير والتدابير القانونية والتدابير التنظيمية والتدابير التقنية والتدابير التعاونية وتدابير بناء القدرات . من خلال المعادلة التالية[٢١]:

OCPI =1/3 (TII normalized + HCI normalized + OSI normalized) × GCI normalized

تتراوح قيمة المؤشر بين (٠و١) تعني قيمة (١) ان الدولة تمتلك اليات تكنلوجية وكوادر بشرية واستراتيجية وطنية دفاعية تؤهلها لمواجهة التهديدات السيبرانية ، ومن ثم تنظيم قيم المؤشر بمستويات رياضية تتراوح ما بين المنخفض ٠ – ٠,٢٥ و المتوسط ٠,٢٥ – ٠,٥٠ ، و العالي ٠,٥٠ – ٠,٧٥ ، والعالي جدا ٠,٧٥ – ١، ومن ثم تصنف قيم المؤشر الى اربعة فئات لكل مستوى ، جدول (٥) .

جدول (٥) مستويات التصنيف والفئات لمؤشر القوة السيبرانية الشاملة[٢٢]

مؤشرالقوة السيبرانية لشاملة (OCPI) العالّي جدا				مؤشرالقوةالسيبرانية الشاملة (OCPI) العالّي				مؤشرالقوةالسيبرانيةالشاملة (OCPI) المتوسط				مؤشرالقوةالسيبرانيةالشام لة (OCPI) المنخفض			
VH	V3	V2	V1	HV	H3	H1	H1	MH	M3	M2	M1	LM	L3	L2	L1

United nations , department of economic and social affairs , E – Government survey , 2022 , P. 5.

من خلال جدول (٦) وخريطة (٣) وحساب مؤشر القوة الشاملة للأمن السيبراني لدول المشرق العربي تبين ان المملكة العربية السعودية حصلت على قيمة مؤشر ٠,٨٧ وتصدرت المرتبة الاولى عربيا والسابعة عالميا ، والامارات العربية المتحدة ٠,٨٦ في المرتبة الثانية والثامنة محليا وعالميا على التوالي ، وضمن التصنيف العالي جدا في الفئة V2 ، في حين حصلت عمان على قيمة مؤشر ٠,٧٧ واحتلت المرتبة الثالثة محليا ضمن التصنيف العالي جدا في الفئة V1 .

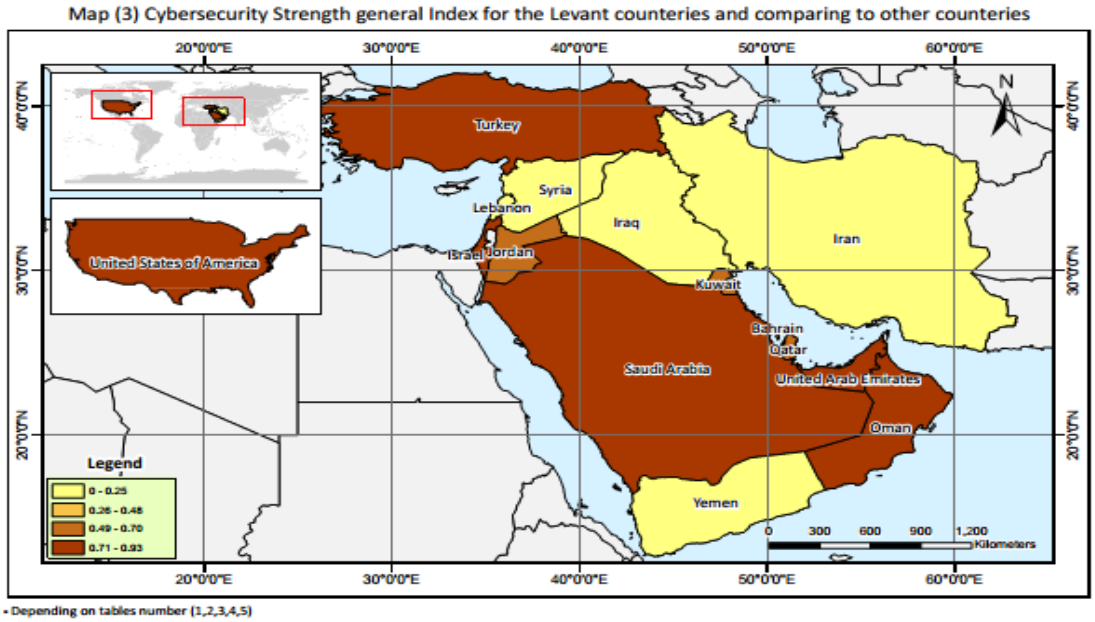
جدول (٦) مؤشر القوة السيبرانية الشاملة لدول المشرق العربي ودول المقارنة لسنة ٢٠٢٢

الدولة	قيمة (OCPI)	التصنيف	الفئة	الترتيب المحلي	الترتيب العالمي
العراق	٠.٠٠٩	منخفض	L1	١٢	٦٧
العربية السعودية	٠.٨٧	عالي جدا	V2	١	٧

الامارات العربية	٠.٨٦	عالي جدا	V2	٢	٨
قطر	٠.٧٠	عالي	H3	٤	١٩
البحرين	٠.٦٢	عالي	H2	٥	٢٤
عمان	٠.٧٧	عالي جدا	V1	٣	١٤
سوريا	٠.٠٧	منخفض	L1	١٣	٧٣
الكويت	٠.٥٩	عالي	H2	٦	٢٧
لبنان	٠.١١	منخفض	L1	١٠	٦٠
اليمن	٠.٠٣	منخفض	L1	١٦	٧١
الاردن	٠.٢٣	منخفض	L1	٨	٤٧
ايران	٠.٥٣	متوسط	H1		٣١
تركيا	٠.٨٠	عالي جدا	V1		١٢
الكيان الصهيوني	٠.٨٢	عالي جدا	V2		١١
امريكا	٠,٩٣	عالي جدا	VH		٢

اعتمادا على الجداول (١) ، (٢) ، (٣) ، (٤) ، (٥)

خريطة (٣) مؤشر القوة السيبرانية الشاملة لدول المشرق العربي ودول المقارنة



بالاعتماد على الجداول (١,٢,٣,٤,٥)

فيما يخص بقية دول الاقليم صنف بعضها ضمن المستوى العالي وهي كل من قطر والبحرين والكويت فبلغت قيم المؤشر لهما ٠,٧٠ و ٠,٦٢ و ٠,٥٩ لكل منهم وعلى التوالي ، بينما حصلت قطر على الفئة H3 والبحرين والكويت ضمن الفئة H2 ، في حين تعكس بقية مؤشرات

دول الاقليم خطورة امنها السيبراني على ضوء مؤشرات القوة ، فقد اوضحت قيم مؤشر الاردن ولبنان والعراق وسوريا واليمن والتي بلغت ٠,٢٣ و ٠,١١ و ٠,٠٩ و ٠,٠٧ و ٠,٠٣لكل منهم على التوالي انها تفتقر الى السياسات والاستراتيجيات الوطنية التي تهدف الى ضمات وحماية امنها السيبراني ضد التهديدات الخارجية والتي تنعكس على بنيتها الاقتصادية والسياسية والاجتماعية ، بالتالي فانها صنفت ضمن المستوى المنخفض في الفئة L1.

وبالمقارنة مع الاهداف المحددة ، نجد ان الولايات المتحدة الامريكية تفوقت على جميع دول المشرق العربي حيث بلغت قيمة مؤشرها ٠,٩٣ لتحتل المرتبة الثانية عالميا ضمن المستوى العالي جدا للفئة VH ، وتقدمت مؤشرات دول المقارنة (الكيان الصهيوني وتركيا) على جميع مؤشرات دول الاقليم العربي باستثناء العربية السعودي والامارات ، وهذا يعد نقطة ضعف جيوبولتيكية للأمن السيبراني لدول المشرق العربي ، وفيما يخص ايران فقد بلغت قيمة مؤشرها ٠,٥٣ ضمن المستوى المتوسط فهي اقل من مستويات دول مجلس التعاون الخليجي لكن افضل من العراق وسوريا والاردن ولبنان واليمن .

خلاصة ذلك ان بعض دول المشرق العربي اعطت اهمية واولوية لمسالة الحفاظ على امنها السيبراني من خلال السياسات والاستراتيجيات الوطنية القائمة الاطر المؤسسية والقانونية لتطور الحكومة الإلكترونية من خلال تكنولوجيا المعلومات والاتصالات بهدف تحقيق امنها السيبراني في شكل حماية متعددة المستويات تغطي أجهزة الكومبيوتر والشبكات والبرامج او البيانات التي تحتاج الى حماية ، في حين واجه البعض الاخر ، تحديات تتعلق بالموارد لسد الفجوة في قدراتها السيبرانية، بما في ذلك نقص المعرفة المؤسسية والقيود على السياسات ونقص المهارات وعدم الاستقرار الامني لحماية أنظمتها في مجال تكنولوجيا المعلومات والاتصالات، بالتالي فإنها تواجه مخاطر كبيرة لأمنها السيبراني ، فهي ليست مستعدة بشكل كافٍ لتهديد الهجمات الإلكترونية.

النتائج

١-تمثل الجغرافيا السياسية الرقمية بكونها رسم لخرائط التفكير الجيوستراتيجي التقليدي في الفضاء الرقمي ، بهدف التنافس على الهيمنة في الفضاء الرقمي ، ومن ثم تعزيز وتوسيع السيطرة في الفضاء المادي .

٢-استطاعت بعض دول المشرق العربي (السعودية والامارات) ان تحقق بيئة آمنة ومأمونة لاعتمادها على شبكة سلسلة التوريد العالمية الجديرة بالثقة للمنتجات والخدمات المتعلقة

بتكنولوجيا المعلومات والاتصالات من خلال حصولها على تصنيف عالي جدا ضمن مقياس القوة الشاملة للأمن السيبراني.

٣-أن معظم دول المشرق العربي ليست مستعدة بشكل كافٍ لتهديد الهجمات الإلكترونية وتواجه مخاطر جيوبولتيكية لأمنها السيبراني وبالتالي امنها الاقتصادي والسياسي والاجتماعي كالعراق وسوريا ولبنان واليمن والاردن من منظور مقاييس الامن السيبراني.

٤-بفضل التخطيط والقرارات الصحيحة ،حققت كل من العربية السعودية والامارات العربية تقدما على جميع دول المقارنة الاقليمية عدا الولايات المتحدة الامريكية ولجميع مقاييس البحث مما يؤكد نضج امنها السيبراني من خلال تعظيم امن الشبكات مما يساهم في تقليل مخاطر الفضاء الالكتروني وبما يعزز قوتها من منظور الجغرافية .

التوصيات

١- ضرورة حماية البنية التحتية الحيوية لدول المشرق العربي من خلال توسيع نطاق القطاعات الحيوية التي يغطيها الحد الأدنى من متطلبات الأمن السيبراني بالتأكيد على الاستثمار في القدرات أكثر من الأدوات .

٢- تفعيل دور القطاع الخاص كقوة ضاربة من خلال آليات قابلة للتطوير لمكافحة الجهات الفاعلة في التهديد وتعطيلها ، وتعزيز الخصوصية وأمن البيانات الشخصية لمنع المتسللين من استغلال الثغرات الأمنية.

٣- الحد من نقاط الضعف التكنولوجية النظامية في الانترنيت لدول المشرق العربي من خلال إعطاء الأولوية للبحث والتطوير في تكنولوجيات الجيل التالي من الأمن السيبراني ، مثل التشفير اللاحق للكم ، وخطط الهوية الرقمية ، والبنية التحتية للطاقة النظيفة و تعزيز التنوع وقوى عاملة وطنية قوية على الإنترنت .

٤- تعزيز التعاون العربي والدولي ومن خلال التعاون لتحقيق الأهداف المشتركة لمكافحة التهديدات التي يتعرض لها النظام البيئي الرقمي لدول المشرق العربي من خلال الإعداد المشترك والاستجابة والتمويل وتحسين قدرة الشركاء على مقاومة التهديدات الإلكترونية في أوقات السلم والأزمات.

الهوامش

(١) Richard A. Clark and Robert K. Cyberwar: The Coming Threat to National Security and What to Do About It (New York: HarperCollins Publishers, 2012), p. 32.

(٢) Gary McGraw, "Cyberwar is inevitable (unless we build security in it)," Journal of Strategic Studies, Volume 36, Number 1, 2013, pp. 109-119.

(٣) احمد حامد علي ، سعاد عبدالله محمد، الامن السيبراني في دول مجلس التعاون الخليجي بمنظور جيوبولتيكي معاصر ،مجلة جامعة الانبار للعلوم الانسانية ، العدد٣ مج ١، ايلول ٢٠٢٠ ، ص ٣٧٣.
(٤)Stephen M. Walt, The Origins of Alliances (Ithaca: Cornell University Press, 1987), p. 33
(٥). Joseph S.Nye JR, Cyber Power ,Hardwar Kennedy School,2010.P.77
(٦) Kenneth Knapp and William Bolton, "Cyberwarfare Threatens Businesses: The Expansion of Business Environments," Journal of Information Systems Management 23, p. 2, 2006, p. 76.
(٧) Nicole Perlroth, "In Cyberattack on Saudi Company, US Sees Iran Pull Back," The New York Times, Oct. 23, 2012, https://www.nytimes.com/2012/10/24/business/global/cyberattack -on - saudi-oil-firm-disquiets-us.html accessed December 13, 2018.
(٨) Yaakov Katz, "Stuxnet virus set back Iran's nuclear program for two years," The Jerusalem Post Dec. 15, 2010, https://www.jpost.com/Iranian-Threat/News/Stuxnet-virus-set-back- Irans-nuclear-program-by-2-years, accessed December 13, 2018
(٩)RonDeibert, "The Geopolitics of Cyberspace After Snowden," Current History, January2015.p10
(١٠)David Clark, "Characterizing Cyberspace: Past, Present and Future," MIT/CSAIL Working Paper, March12, 2010, p.1
(١١) Gabriel Weimann, Terroron the Internet: The New Arena ,the New Challenges, Washington, D C: United States Institute of Peace Press, 2006
(١٢) Norrin M. RipsmanandT. V. Paul, "Globalization and the National Security State: A Framework For Analysis ,"International Studies Review, Vol. 7 , No .2, June 2005 p 199 .
(١٣) John B. Sheldon, "Geopolitics and Cyber Power: Why Geography Still Matters," p . 278 .
(١٤) حسن هادي جاهل و آخرون، تقانة المعلومات و دورها في رفع كفاءة أداء الجهاز المصرفي .مجلة جامعة كركوك للعلوم الإدارية و الاقتصادية مج. ١١، ع. ١ ،٢٠٢١، ص ١٢٣– ١٢٧.
(*) المزيد من التفاصيل: الامم المتحدة ، دائرة الشؤون الاقتصادية والاجتماعية ، مسح الحكومة الالكترونية ٢٠٢٢، مستقبل الحكومة الرقمية https://publicadministration.un.org/en/
(١٥) United nations ,department of Economic and social Affairs ,E Government survey ,2022 P. 196.
(١٦) وزارة التخطيط التنموي والاحصاء ، دليل للمؤشرات المستخدمة في التعليم والتدريب والبحث والتطويرفي دولة قطر، اكتوبر ، ٢٠١٦ ،ص ١٤.
(١٧) مركز الإحصاء ، دليل المؤشرات الاحصائية ، أبو ظبي٢٠٢١، ص ٢٣ .
(١٨) United nations , Department of Economic and social Affairs , E p.137-Government survey , 2016،
(١٩) International Telecommunications Union (ITU) , Global Cybersecurity Index , 2020 , P.132 , 133 ينظر : نبهان زمبور السعدي ، الابعاد الجيوسياسية لتجارة الصادرات في اقطار مجلس التعاون الخليجي ،مجلة جامعة تكريت للعلوم الانسانية ،مجلد ٢٢،العدد ٨،تشرين الثاني ،٢٠١٥ ،ص٣٤٦.
(٢٠) تغريد معين حسن المشهدي ، الأثر العسكري للأمن السيبراني في الجغرافية السياسية للدولة ، مجلة البحوث الجغرافية ، العدد ٣٠،ص ٢٤٠.
(٢١) United nations , department of economic and social affairs , E – Government survey , 2022 , P. 189, 190

(٢٢) United nations , department of economic and social affairs , E – Government survey , 2022 , P. 5 .

المصادر

١-احمد حامد علي ، سعاد عبدالله محمد، الامن السيبراني في دول مجلس التعاون الخليجي بمنظور جيوبولتيكي معاصر ،مجلة جامعة الانبار للعلوم الانسانية ، العدد٣ مج ١، ايلول ٢٠٢٠.

٢-تغريد معين حسن المشهدي ، الأثر العسكري للأمن السيبراني في الجغرافية السياسية للدولة ، مجلة البحوث الجغرافية ، العدد ٣٠.

٣-حسن هادي جاهل و آخرون، تقانة المعلومات و دورها في رفع كفاءة أداء الجهاز المصرفي. مجلة جامعة كركوك للعلوم الإدارية و الاقتصادية مج. ١١، ع. ١ ،٢٠٢١.

٤-نبهان زمبور السعدي ، الابعاد الجيوسياسية لتجارة الصادرات في اقطار مجلس التعاون الخليجي ،مجلة جامعة تكريت للعلوم الانسانية ،مجلد ٢٢،العدد ٨،تشرين الثاني ،٢٠١٥.

٥-مركز الإحصاء ، دليل المؤشرات الاحصائية ، أبو ظبي٢٠٢١.

٦-وزارة التخطيط التنموي والاحصاء ، دليل للمؤشرات المستخدمة في التعليم والتدريب والبحث والتطويرفي دولة قطر، اكتوبر ، ٢٠١٦.

7-David Clark, "Characterizing Cyberspace: Past, Present and Future," MIT/CSAIL Working Paper, March12, 2010.

8- Gary McGraw, "Cyberwar is inevitable (unless we build security in it)," Journal of Strategic Studies, Volume 36, Number 1, 2013.

9- Gabriel Weimann, Terroron the Internet: The New Arena ,the New Challenges, Washington, D C: United States Institute of Peace Press, 2006 .

10- International Telecommunications Union (ITU) , Global Cybersecurity Index , 2020 .

11-Joseph S.Nye JR, Cyber Power ,Hardwar Kennedy School,2010.

12- Kenneth Knapp and William Bolton, "Cyberwarfare Threatens Businesses: The Expansion of Business Environments," Journal of Information Systems Management 23, 2006.

13- Norrin M. RipsmanandT. V. Paul, "Globalization and the National Security State: A Framework For Analysis ,"International Studies Review, Vol. 7 , No .2, June 2005.

14- Nicole Perlroth, "In Cyberattack on Saudi Company, US Sees Iran Pull Back," The New York Times, Oct. 23, 2012, https://www.nytimes.com/2012/10/24/business/global/cyberattack -on - saudi-oil-firm-disquiets-us.html accessed December 13, 2018.

15- Ron Deibert, "The Geopolitics of Cyberspace After Snowden," Current History , January2015 .

16- United nations ,department of Economic and social Affairs ,E Government survey ,2022 .

17- United nations , department of economic and social affairs , E – Government survey , 2022

18-Yaakov Katz, "Stuxnet virus set back Iran's nuclear program for two years," The Jerusalem Post Dec. 15, 2010, https://www.jpost.com/Iranian-Threat/News/Stuxnet-virus-set-back- Irans-nuclear-program-by-2-years, accessed December 13, 2018
19- United nations , Department of Economic and social Affairs , E Government survey , 2016.

المصادر العربية المترجمة

1 -Ahmed Hamid Ali, Souad Abdullah Muhammad, Cybersecurity in the Gulf Cooperation Council countries from a contemporary geopolitical perspective, Anbar University Journal for the Humanities, Issue 3, Volume 1, September 2020.
2-Taghreed Moin Hassan Al-Mashhadi, The Military Impact of Cybersecurity on the Political Geography of the State, Journal of Geographical Research, No. 30.
3-Hassan Hadi Jahl and others, information technology and its role in raising the efficiency of the banking system's performance. Kirkuk University Journal of Administrative and Economic Sciences Vol. 11, p. 1, 2021.
4 -Nabhan Zambour Al-Saadi, Geopolitical Dimensions of Export Trade in Gulf Cooperation Council Countries, Tikrit University Journal of Human Sciences, Volume 22, Issue 8, November, 2015.
5 -Statistics Center, Statistical Indicators Guide, Abu Dhabi 2021.
6-Ministry of Development Planning and Statistics, a guide to indicators used in education, training, research and development in the State of Qatar, October, 2016.