مجلة جامعة الانبار للعلوم الانسانية
University of Anbar Journal for Humanities
P. ISSN: 1995-8463 E.ISSN: 2706-6673
Volume 17- Issue 3- September 2020 | المجلد ١٧- العدد ٣ – ايلول ٢٠٢٠

الأمن السيبراني في دول مجلس التعاون لدول الخليج العربية بمنظور جيوبولتيكي معاصر

أ.م.د احمد حامد علي
كلية التربية – جامعة الموصل
م.د سعاد عبدالله محمد
كلية العلوم الانسانية / جامعة دهوك
Dr.ahmed.h.ali@uomosul.edu.iq

DOI
10.37653/juah.2020.170960

تم الاستلام: ٢٠٢٠/٤/١٨
قبل للنشر: ٢٠٢٠/٦/٢١
تم النشر: ٢٠٢٠/٩/١

الكلمات المفتاحية
الامن السيبراني
الهجمات السيبرانية
استراتيجية الردع السيبراني

الملخص:

يعد الامن السيبراني جزءاً اساسيا في السياسية الامنية الوطنية للدول ، كما ان الكثير من الدول تستخدم قدراتها التي يتيحها الفضاء السيبراني لاعتبارات الامن والقوة العسكرية بشكل يجعلها تدخله ضمن حساباتها الاستراتيجية ، ان الهدف من هذه الورقة البحثية هي دراسة جيوبوليتيكية الامن السيبراني لدول مجلس التعاون لدول الخليج العربية واهم مرتكزات القوة السيبرانية التي تمتلكها هذه الدول ، وتتمحور مشكلة البحث في سؤال يطرحه البحث وهو: هل تمتلك دول مجلس التعاون مرتكزات القوة السيبرانية التي تؤهلها لتبني استراتيجيات الردع السيبراني في مواجهة الهجمات السيبرانية ، وقد توصل البحث الى جملة من الاستنتاجات اهمها ان قضية الامن السيبراني اصبحت على راس اولويات قضايا الامن الوطني لدول مجلس التعاون في محاولة لمواجهة تصاعد التهديدات السيبرانية كما ان ارتفاع وتيرة الهجمات السيبرانية وتوسع رقعة الحرب ضد دول مجلس التعاون لدول الخليج العربية عبر شبكات المعلومات الدولية يجعلها تشكل تهديدا لأمنها الاقتصادي والسياسي والعسكري .

Cyber security in the Gulf Cooperation Council states From a Contemporary geopolitical perspective

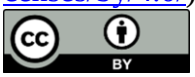
Assistant Prof.Ahmed.H.A
College of Education for Humanities
University of Mosul,

Dr.Suad.A.M
College of Humanities
Duhok University

Abstract:
One of the national security policy of countries is Cyber security, many countries utilize their capacities that cyberspace provides for the considerations of security and military strength in which makes it to be included in its strategic calculations, the aim of this research is to study the geopolitics of cyber security for the Gulf Cooperation Council states as well as the most important owned pillars of cyber power by these countries. The problem of this study is; do the GCC countries possess the cyber power foundations that qualify them to adopt cyber deterrence strategies in the face of cyber-attacks. The outcomes of this research illustrate that the issue of cyber security has become a top priority for the national security issues for the Cooperation Council countries due to be safe from cyber threats, as can be realized that the high frequency of cyber-attacks in addition to the enlarged war against the Gulf Cooperation Council states through international information networks, this lets it to face threat to their economic, political and military security

Submitted: 18/04/2020
Accepted: 21/06/2020
Published: 01/09/2020

Keywords:
cyber security,
cyber attacks
deterrence strategy cyber.



المقدمة:

يعد موضوع الامن السيبراني في أي وحدة سياسية حجر الزاوية في استقلالها الاقتصادي والسياسي والعسكري طالما انه يشكل العمود الفقري في معادلة قياس قوة الدولة طبقا لمنهج الجغرافية السياسية.

لقد نجم عن التطور السريع لتكنلوجيا المعلومات والاتصالات تحولا كبيرا في مفهوم الامن ،اذا ادت علاقة الفضاء الالكتروني بأنشطة الحكومات والافراد وبعمل المنشأة الحيوية سواء كانت مدنية او عسكرية لإمكانية عرضها لهجوم من خلاله يؤثر على عمل انظمتها المعلوماتية ومن ثم فان التحكم في تنفيذ هذا الهجوم يعد اداة سيطرة ونفوذ استراتيجي بالغ الاهمية في وقت السلم والحرب .

وعليه فقد بات الامن السيبراني يشكل جزءاً اساسياً في السياسة الامنية الوطنية، وتستخدم العديد من الدول القدرات التي تتيحها الفضاء السيبراني لاعتبارات الامن والقوة العسكرية بشكل يجعلها تدخله ضمن حساباتها الاستراتيجية وامنها القومي، كما ان صناع القرار في الدول العظمى كالولايات المتحدة والصين و روسيا وغيرها من الدول اصحبوا يضعون مسائل الدفاع السيبراني والامن السيبراني كأولوية في سياساتهم الدفاعية الوطنية وبالتالي تعزيز عناصر القوة الشاملة بمنظور الجغرافية السياسية .

هدف البحث:

يهدف البحث الى دراسة جيوبوليتك الامن السيبراني ومعرفة مرتكزات القوة السيبرانية لدول مجلس التعاون لدول الخليج العربية واستراتيجيات الروع التي تمتلكها هذه الدول في مواجهة اخطار الهجمات السيبرانية.

مشكلة البحث:

تتحدد مشكلة البحث في السؤال الاتي: هل تمتلك دول مجلس التعاون الخليجي مرتكزات القوة السيبرانية التي تؤهلها الى تبني استراتيجيات الردع في مواجهة الهجمات السيبرانية.

فرضية البحث:

ينطلق البحث من فرضية مفادها تباين مرتكزات الامن السيبراني في دول مجلس التعاون مما انعكس على تباين استراتيجيات الردع المعتمدة من قبل هذه الدول تجاه عمليات الاختراق والقرصنة للفضاء السيبراني.

منهجية البحث

اتخذ البحث من منهج تحليل القوة في الجغرافية السياسية منهجا لدراسة مشكلة البحث متخذين من البيانات المتاحة الصادرة من الامم المتحدة وغيرها من المصادر المادة الخام الرئيسة المعتمدة في معالجة التحليل والقياسات الكمية .

هيكلية البحث

تأسيساً على ما تقدم انقسم البحث الى ثلاث محاور رئيسة، ناقش المحور الأول الأمن السيبراني المفهوم والفواعل، فيما خصص المحور الثاني لاستعراض مرتكزات القوة السيبرانية لدول مجلس التعاون لدول الخليج العربية، أما المحور الثالث فقد ناقش استراتيجيات الردع السيبراني لدول المجلس التعاون لدول الخليج العربية.

اولا: الأمن السيبراني المفهوم والفواعل

١- **مفهوم الأمن السيبراني** : الأمن السيبراني مشتق من كلمتين وكلمة سيبر لاتينية الأصل و معناها الفضاء المعلوماتي فيصبح المقصود بالأمن السيبراني أمن الفضاء المعلوماتي وهو تعبير أشمل من أمن المعلومات.

يعرف الأمن السيبراني : بأنه عبارة عن مجموعة الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لحماية الشبكات والأجهزة والبرامج والبيانات من الهجمات أو الأضرار أو الوصول غير المصرح به وسوء الاستغلال [١]. ويعرف ريتشارد تمرر الأمن السيبراني بأنه عبارة عن وسائل دفاعية من شأنها كشف واحباط المحاولات التي يقوم بها القراصنة [٢].

بينما عرفه ادوارد مورسو على أنه: وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة و كشف الفيروسات ووقفها [٣]. وبحسب تعريف الاتحاد الدولي للاتصالات في تقريره حول (اتجاهات الإصلاح في الاتصالات للعام ٢٠١٠-٢٠١١) هو (مجموعة من المهمات مثل تجميع وسائل و سياسات وإجراءات أمنية و مبادئ توجيهية لحماية البيئة السيبرانية و موجودات المؤسسات والمستخدمين) [٤].

٢- الأبعاد والفواعل

يهدف الأمن السيبراني إلى تعزيز حماية جميع ما يتعلق بالدولة الكترونياً وأفراداً لحماية هذه الأنظمة الإلكترونية وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية و جميع مكوناتها المحيطة بالمجتمع من أجهزة و برمجيات و معدات و جميع ما يؤثر على تقدم هذه الخدمات [٥]. و يرتبط الأمن السيبراني بمجالات مختلفة سياسية و عسكرية واقتصادية و قانونية واجتماعية ، بهدف تحقيق منظومة أمن متكاملة تعمل على الحفاظ على الأمن القومي للدولة من أي تهديدات سيبيرية محتملة .

ومن اهم الابعاد الاستراتيجية التي تعمل الدولة على تحصينها من الهجمات و الحروب السيبرانية هي :

١. **البعد العسكري:** تكمن الميزة النسبية للقوة السيبرانية في قدرتها على ربط الوحدات العسكرية ببعضها البعض بما يسمح بتبادل المعلومات والأوامر و تدفقها و إصابة الأهداف عن بعد و تدميرها، و قد تتحول هذه الميزة إلى نقطة ضعف إن لم تكن الشبكة الإلكترونية المستخدمة مؤمنة من الاختراق الذي قد يؤدي إلى تدمير قواعد البيانات العسكرية أو قطع الاتصالات بين القيادة والوحدات العسكرية ، و تعطيل قدرة الدولة على النشر السريع لقدراتها و قواتها، فضلاً عن إمكانية التحكم في بعض الأسلحة و خروجها عن السيطرة (كالطائرات بدون طيار ، أو الصواريخ، أو الأقمار الصناعية ...) كما يمكن التحكم في أنظمة الدفاع الجوي أو التوجيه الإلكتروني للخصم [٦].

٢. **البعد الاقتصادي:** يرتبط الأمن السيبراني ارتباطا وثيقاً بالاقتصاد، فالتلازم واضح بين المعرفة و توسع استخدام تقنيات المعلومات والاتصالات كماً بالقيمة التي تمثلها البيانات والمعلومات المتداولة والمخزونة والمستخدمة عل كل المستويات، كذلك تتيح تقنيات المعلومات والاتصالات تعزيز التنمية الاقتصادية لبلدان كثيرة، عبر إفادتها من فرص الاستخدام التي تقدمها الشركات الدولية والشركات الكبرى، التي تبحث عن إدارة كلفة إنتاجها بأفضل الشروط، إلا أن هذا الواقع المشرق يطرح مسائل مختلفة سواء منها ما يتعلق بحماية الخدمة والعمل أو بحماية المستهلك على الإنترنيت [٧].

كما أن هناك ارتباط بين شبكات البنوك والبورصات و شركات الأسواق المالية من خلال نظم و شبكات الكترونية فأصبحت شبكات الإنترنيت هي أساس المعاملات المالية

والاقتصادية وباتت تشكل محوراً رئيسياً للتطور الاقتصادي وهو ما أثار الحديث عن أهمية تحقيق الأمن السيبري في المجال الاقتصادي [٨].

٣. البعد الاجتماعي: تسمح طبيعة الإنترنيت المفتوحة، عبر المدونات و شبكات التواصل الاجتماعي لكل مواطن أن يعبر عن تطلعاته الثقافية والسياسية والاجتماعية ، كما يمكن مشاركة جميع شرائح المجتمع، أن عدد مستخدمي الإنترنيت في العالم بلغ أكثر من ٤ مليار شخص عام ٢٠١٧، يستخدم أكثر من ٢,٦ مليار منهم مواقع التواصل الاجتماعي، مما يجعلها أكبر تجمع بشري و يتيح فرص الاطلاع عن الأفكار و المعلومات والثقافات الأخرى، وبالتالي تبادل الخبرات وتكون حاجات جديدة، و فتح آفاق للتعاون والتكامل، ولكن بالمقابل قد يعرض أخلاقيات المجتمع للخطر نظراً لصعوبة مراقبة محتوى الإنترنيت كما يعرض الهويات لعمليات اختراق قد تتسبب في تهديد السلم الاجتماعي للدولة و عليه يجب توعية المواطن بهذه المخاطر لتحقيق الأمن السيبراني في بعده الاجتماعي.

٤. **البعد السياسي:** تتمثل الأبعاد السياسية للأمن السيبراني بشكل أساسي في حق الدولة في حماية نظامها السياسي و كيانها و مصالحها الاقتصادية التي تعني حقها وواجبها في تحقيق رفاه شعبها، في وقت تؤثر التقنيات في موازين القوى داخل المجتمع نفسه، حيث أصبح بإمكان المواطن أن يتحول إلى لاعب سياسي في اللعبة السياسية، كما أصبح بالإمكان الاطلاع على خلفيات و مبررات القرارات السياسية التي تتخذها حكومته، عبر الكم الهائل من المعلومات التي يمكن الوصول اليها [٩].

كما أن لشبكات التواصل الاجتماعي دور في تحقيق أهداف سياسية ، كتنظيم حملات انتخابية أو تظاهرات افتراضية، وحركات احتجاجية الكترونية، ويعد التدخل الروسي السيبراني في الانتخابات الأمريكية أبرز دليل على ضرورة وأهمية الأمن السيبراني في بعده السياسي إضافة إلى التسربات لوثائق حساسة والاختراقات التي غالباً ما تؤدي إلى أزمات دبلوماسية بين الدول [١٠].

٥. **البعد القانوني:** ان العلاقة بين القانون والتكنولوجيا علاقة متبادلة فالتطورات التكنولوجية المختلفة تفترض مواكبة التشريعات القانونية لها، من خلال وضع اطر و تشريعات للأعمال القانونية و غير القانونية منها، ولكن الملاحظ بصورة عامة أن الجريمة السيبرانية تفتقد في معظم الحالات والبلدان للأطر القانونية الصارمة للتعامل معها و هذا يعود

إلى طبيعة الجريمة الالكترونية ذاتها، وصعوبة تحديد هوية مرتكبي هذه الجرائم و مرونة التعريفات المرتبطة بتكنولوجيا المعلومات إلى جانب كون الجرائم السيبرية غير مقيدة بحدود الدول الأمر الذي يقضي تفعيل التعاون الدولي المشترك لمكافحتها [١١].

أما الفواعل في الأمن السيبراني فان جوزيف. ناي [*] يحدد أنواع من الفاعلين الذين يمتلكون القوة السيبرانية وهم [١٢] :

١-**الدول** : والتي لديها قدرة كبيرة على تنفيذ هجمات سيبرانية و تطوير البنية التحتية وممارسة السلطات داخل حدودها.

٢-**الفاعلون من غير الدول:** ويستخدم هؤلاء الفاعلون القوة السيبرانية لأغراض هجومية بالأساس، إلا أن قدرتهم على تنفيذ أي هجوم سيبراني مؤثر تتطلب مشاركة و مساعدة أجهزة استخباراتية متطورة، ولكن يمكن اختراق المواقع الالكترونية واستهداف الأنظمة الدفاعية. ويشمل هذا النوع من الفاعلين:

ا- **الأفراد (القراصنة)** الذين يمتلكون معرفة تكنولوجية عالية و القدرة على توظيفها و عادة ما تكون هناك صعوبة في الكشف عن هوياتهم ومن الصعب ملاحقتهم.

ب- **الشركات المتعددة الجنسية** : تمتلك شركات التكنولوجيا موارد للقوة تفوق قدرة بعض الدول ،فخوادم شركات مثل كوكل وفيسبوك ومايكروسوفت وغيرها تسمح لها بامتلاك قواعد البيانات العملاقة التي من خلالها تؤثر في اقتصاديات الدول وفي ثقافة المجتمعات وتوجيهاتها.

ج- المنظمات الاجرامية: تقوم هذه المنظمات بعمليات القرصنة السيبرانية او سرقة المعلومات واختراق الحسابات البنكية وتحويل الاموال ، كما توجد سوق سوداء على الانترنيت المظلم لتجارة المخدرات والاسلحة والبشر .

ء- **الجماعات الارهابية** : تعد ضمن ابرز الفواعل خاصة بعد احداث ١١ سيبتمبر حيث تستغل الفضاء السيبراني في عملياتها رغم انها لم تصل بعد الى مرحلة القيام بهجوم سيبراني حقيقي على منشاءت البنية التحتية للدول .

ثانيا : مرتكزات القوة السيبرانية لدول مجلس التعاون لدول الخليج العربي

تشمل مرتكزات القوة السيبرانية على وجود نظام متماسك يعظم من القوة الناتجة عن التناغم بين القدرات التكنلوجية والسكان والاقتصاد والصناعة والقوة العسكرية وارادة الدولة

وغيرها من العوامل التي تساهم في دعم امكانيات الدولة على ممارسة الاكراه والاقناع او ممارسة التأثير السياسي على اعمال الدول الاخرى او على الحكام في العالم بغرض الوصول للأهداف الوطنية من خلال قدرات التحكم والسيطرة على الفضاء السيبراني ، ويعد جوزيف ناي من ابرز المهتمين بالقوة السيبرانية حيث عرفها بانها القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني أي انها القدرة على استخدام الفضاء السيبراني لإيجاد مزايا للدولة والتأثير على الاحداث المتعلقة بالبيئات التشغيلية الاخرى وذلك عبر ادوات سيبرانية (١٣).

وبغية الكشف عن واقع الامن السيبراني في دول مجلس التعاون لدول الخليج العربية اعتمدت الدراسة على مؤشرات الدليل العالمي للأمن السيبراني الذي تصدره وحدة الاتصالات العالمية في الأمم المتحدة International telecommunication union(ITU) والذي يقيس مستوى التزام الدول المختلفة بالأمن السيبراني ويوفر المعلومات الأساسية لتحليل و مقارنة أداء الدول العالمية من خلال خمسة ركائز رئيسية وهي العوامل القانونية والفنية والترتيبات التنظيمية وبناء القدرات والتعاون (١٤).

ومن الجدول (١) نلاحظ أن هناك تعاون بين دول المجلس في هذه الركائز، حيث يظهر أن دولة عمان حققت نتائج عالية في ركيزتي التقنية والتنظيمية إذ بلغت الأولى ٠,١٨٤ والثانية بلغت ٠,١٩٧ وهذا يدل على أن عمان تتمتع بهيكل تنظيمي قوي و وجود استراتيجية عالية المستوى للأمن السيبراني، وتأتي المملكة العربية السعودية في المرتبة الأولى من بين دول المجلس بأعلى الدرجات في ركيزة القدرات حيث بلغت ٠,١٩٧ إذ تظهر المملكة التزاماً قوياً ببناء القدرات من خلال العديد من المبادرات بما في ذلك برنامج حاضنة التكنولوجيا والشبكة السعودية للبحث والابتكار والاتحاد السعودي للأمن السيبراني والبرمجة، وسجلت السعودية و عمان نقاط متساوية بلغت ٠,١٦٠ في ركيزة التعاون، واحتلت قطر المرتبة الثالثة باطار قانوني قوي وهيكل تنظيمي قوي من خلال الشركة الوطنية لخدمات الكومبيوتر المحدودة التي تركز بشكل رئيسي على تأمين البنية التحتية الحيوية للمعلومات والأمن السيبراني الوطني ،اما بقية دول المجلس فلم يتم الحصول على بيانات بقيم رقمية ولكن تم الحصول عليها بتقدير اما عالي او متوسط او منخفض وكانت لعام ٢٠١٧ ، على سبيل المثال حصلت الامارات على تقدير منخفض في المؤشر القانوني وتقدير متوسط في

بقية المؤشرات التقني والتنظيمي وبناء القدرات والتعاون والبحرين حصلت على تقدير منخفض في المؤشر القانوني ومتوسط في المؤشر التقني والتنظيمي والتعاون وتقدير عالي في مؤشر بناء القدرات .

الجدول (١) مستوى أداء دول مجلس التعاون لدول الخليج العربية في دليل الأمن السيبراني العالمي حسب الركائز الخمسة لعام ٢٠١٨

دول المجلس	مؤشر دليل الأمن السيبراني	القانوني	التقني	التنظيمي	بناء القدرات	التعاون
المملكة العربية السعودية	٠.٨٨١	٠.١٨٧	٠.١٧٩	٠.١٥٨	٠.١٩٨	٠.١٦
عمان	٠.٨٦٨	٠.١٣٣	٠.١٨٤	٠.١٩٧	٠.١٩٥	٠.١٦
قطر	٠.٨٦	٠.٩٣	٠.١٥٤	٠.١٩٢	٠.١٧١	٠.١٥١

المصدر : ITU. Global cyber security index, 2018,P.26,27,57,58,61,62

ومن خلال دليل الأمن السيبراني يظهر لنا درجة التزام دول المجلس وترتيبها عربياً وعالمياً (الجدول ٢) حيث نلاحظ أن السعودية احتلت المرتبة الأولى عربياً والأولى على دول مجلس التعاون بمؤشر بلغ ٠,٨٨١ بينما احتلت المرتبة ١٣ عالمياً، تليها عمان حيث احتلت المرتبة الثانية عربياً وضمن دول المجلس بمؤشر بلغ ٠,٨٦٨ و ترتيبها العالمي هو ١٦، في حين سجلت قطر المرتبة الثالثة ضمن دول المجلس وعربياً أيضاً بمؤشر بلغ ٠,٨٦٠ وترتيبها العالمي ١٧، ، أما الإمارات فقد سجلت المرتبة الرابعة ضمن قائمة دول مجلس التعاون والخامسة عربياً بمؤشر بلغ ٠,٨٠٧ و ترتيبها العالمي كان ٣٣ ، في حين سجلت الكويت المرتبة الخامسة في قائمة دول المجلس بمؤشر بلغ ٠,٦٠٠ والمرتبة ٦ عربياً و ٦٧ عالمياً وسجلت البحرين المرتبة الأخيرة ضمن دول المجلس بمؤشر بلغ ٠,٥٨٥ وعربياً كان ترتيبها ٧ وعالمياً ٦٨ ، وبالنظر إلى هذا الترتيب نستنتج أن دول مجلس التعاون تأتي في مقدمة جميع الدول العربية (ماعدا مصر التي تأتي في المرتبة الرابعة عربياً) في دليل الأمن السيبراني وهذا يعني التزام هذه الدول باستراتيجيات أمنية جيدة في مجال الأمن

السيبراني ، كما أن ترتيب دول المجلس عالمياَ أيضاَ يعد ذو قيمة كبيرة فالسعودية بالمرتبة ١٣ وعمان ١٦ وقطر ١٧ فهذا الترتيب يأتي ضمن ترتيب ١٨٠ دولة على مستوى العلم كذلك مقارنة دول المجلس بدول المقارنة الثلاث (تركيا وإسرائيل و أمريكا) يظهر لنا أن ترتيب إسرائيل هو ٣٩ عالمياَ، كما أن نسبة مؤشرها البالغ ٠,٧٨٣ هو أقل من مؤشر أربع دول في مجلس التعاون وهي السعودية، عمان ، قطر، الإمارات أما تركيا فقد بلغ نسبة المؤشر ٠,٨٥٣ وهو أقل من مؤشر ثلاث دول في المجلس هي (السعودية ، عمان، قطر) وترتيبها العالمي ٢٠ وهذا يجعلها أقل مرتبة في دليل الأمن السيبراني العلمي من ثلاث دول مجلس التعاون وهي (السعودية، عمان، قطر) أما الولايات المتحدة الأمريكية فأن مؤشر دليل الأمن السيبراني بلغ ٠،٩٢٦ وتأتي في المرتبة الثانية عالمياَ بعد المملكة المتحدة البريطانية.

الجدول (٢) ترتيب دول مجلس التعاون لدول الخليج العربية ودول المقارنة وفق دليل الأمن السيبراني العالمي ٢٠١٨

الدول	مؤشر دليل الأمن السيبراني العالمي	ترتيب دول المجلس عربيا	الترتيب العالمي
المملكة العربية السعودية	٠,٨٨١	١	١٣
عمان	٠,٨٦٨	٢	١٦
قطر	٠,٨٦٠	٣	١٧
الإمارات المتحدة	٠,٨٠٧	٥	٣٣
الكويت	٠,٦٠٠	٦	٦٧
البحرين	٠,٥٨٥	٧	٦٨
الولايات المتحدة الأمريكية	٠,٩٢٦	_	٢
إسرائيل	٠,٧٨٣	_	٣٩
تركيا	٠،٨٥٣	_	٢٠

المصدر: U.N .Global cyber security index, 2018,P.27

يمكن اعتماد عدد من مرتكزات القوة السيبرانية في دول مجلس التعاون لدول الخليج العربية وهي :

١- الحكومة الالكترونية و تطبيقاتها في دول مجلس التعاون لدول الخليج العربية:

في دراسة للحكومة الالكترونية لعام ٢٠١٤ عرفت الأمم المتحدة الحكومة الالكترونية على أنها استخدام وتطبيقَ المعلومات في الإدارة العامة لتنظيم و دمج سير العمل

والعمليات بغرض إدارة البيانات والمعلومات بفعالية و تعزيز تقديم الخدمات العامة فضلاً عن توسعة قنوات الاتصال لتضمين وتمكين الأشخاص [١٥].

وفي مجال تطبيقات الحكومة الالكترونية فأن هناك ثلاث معايير يتم من خلالها تقييم دول العالم من حيث مدى كفاءة الحكومة في تقديم الخدمات الالكترونية لمواطنيها وهذه المعايير الثلاث هي (مؤشر خدمة الانترنيت، ومؤشر البنية التحتية للاتصالات اللاسلكية، ومؤشر رأس المال البشري) ومن خلال بيانات الجدول (٣) يظهر لنا مستوى أداء الحكومة الالكترونية ودول المقارنة، حيث احتلت الإمارات العربية المتحدة المرتبة الأولى على مستوى دول المجلس وحققت الترتيب ٢١ على مستوى العالم بقيمة مؤشر بلغ ٠,٨٢٩٥ تليها البحرين في المرتبة الثانية على مستوى دول المجلس والمرتبة ٢٦ على مستوى العالم وبقيمة مؤشر عالي جداً بلغ ٠,٨١١٦ وبالنظر إلى دول المقارنة الثلاثة نجد أن الولايات المتحدة الأمريكية فقط هي الدولة الأكثر كفاءة في تطبيقات الحكومة الإلكترونية بالمقارنة مع دور المجلس و ترتيبها عالمياً هو ١١وبمؤشر بلغ ٠,٨٧٦٩، أما إسرائيل فإنها أقل كفاءة في هذا المجال من إثنين من دول المجلس وهي الإمارات والبحرين بمؤشر يبلغ ٠,٧٩٩٨ و ترتيب عالمي بلغ ٣١وهي أكثر كفاءة من بقية دول المجلس حسب هذا المؤشر ينظر الخريطة (١).

أما تركيا فنلاحظ إنها أقل كفاءة في خدمة الحكومة الإلكترونية ، حيث ان جميع دول المجلس اكثر منها كفاءة ماعدا دولة عمان كما أن ترتيبها أقل من هذه الدول إذ بلغ ٥٣ عالمياً، ومن الجدول يظهر لنا أيضاً أن خمسة دول من دول المجلس وهي (الإمارات، السعودية، الكويت، البحرين، قطر)تقع ضمن المراكز الخمسين الأولى على مستوى العالم في مؤشر تطور الحكومة الإلكترونية، وهذا دليل على قوة تطبيقات الحكومة الإلكترونية في هذه الدول. ومن بين العلامات البارزة على أهمية الحكومة الإلكترونية في دول المنطقة، جوائز الحكومة الإلكترونية لدول المجلس التعاون الخليجي التي تمنح كل عامين إلى الهيئات الحكومية التي تثبت تفوقها في تقديم خدمات الحكومة الإلكترونية في مختلف القطاعات.

وعليه يمكن القول بان هناك علاقة طردية بين الانكشاف الامني للدول وبين اعتمادها المتزايد على الفضاء السيبراني كبرنامج الحكومات الالكترونية والتي تصبح عرضة للاختراق والهجوم بالفيروسات وسرقة المعلومات او اتلافها وبالتالي استخدام الفضاء السيبراني

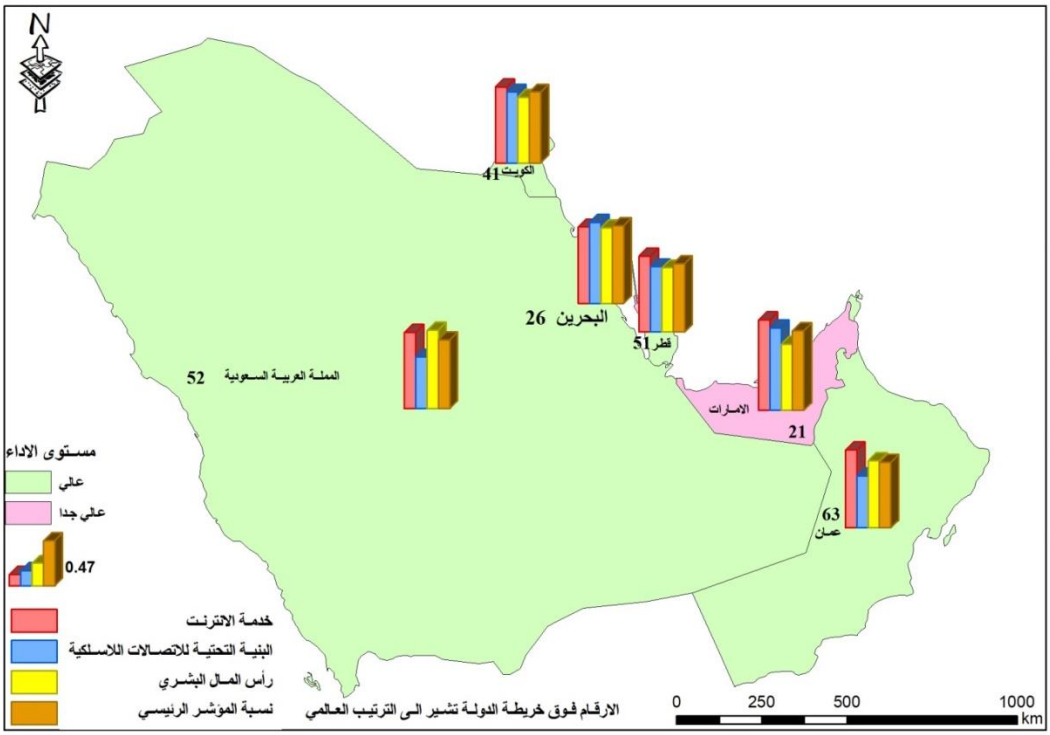
كنمط في استخدام القوة في التأثير على انظمة التشغيل و تدفق المعلومات وهو ما يشكل نقطة ضعف في جسم الدولة طبقا لمنهج تحليل القوة في الجغرافية السياسية .

الجدول (٣) مؤشرات تطور أداء الحكومة الإلكترونية لدول مجلس التعاون ودول المقارنة ٢٠١٨

الدول	معايير المؤشر			نسبة المؤشر الرئيسي	مستوى الأداء	الترتيب العالمي
	خدمة الانترنيت	البنية التحتية للاتصالات اللاسلكية	رأس المال البشري			
المملكة العربية السعودية	٠,٧٩١٧	٠,٥٣٣٩	٠,٨١٥١	٠,٧١١٩	عالي	٥٢
عمان	٠,٨١٢٥	٠,٥٣٩٩	٠,٧٠١٣	٠,٦٨٤٦	عالي	٦٣
قطر	٠,٧٩١٧	٠,٦٧٩٧	٠,٦٦٨٣	٠,٧١٣٢	عالي	٥١
الإمارات العربية المتحدة	٠,٩٤٤٤	٠,٨٥٦٤	٠,٦٨٧٧	٠,٨٢٩٥	عالي جداً	٢١
الكويت	٠,٧٩١٧	٠,٧٣٩٤	٠,٦٨٥٢	٠,٧٣٨٨	عالي	٤١
البحرين	٠,٧٩٨٦	٠,٨٤٦٦	٠,٧٨٩٧	٠,٨١١٦	عالي جداً	٢٦
الولايات المتحدة الأمريكية	٠,٩٨٦١	٠,٧٥٦٤	٠,٨٨٨٣	٠,٨٧٦٩	عالي جداً	١١
إسرائيل	٠,٨٢٦٤	٠,٧٠٩٥	٠,٨٨٨٣	٠,٧٩٩٧	عالي جداً	٣١
تركيا	٠,٨٨٨٩	٠,٤٢٩٨	٠,٨١٤٨	٠,٧١١٢	عالي	٥٣

المصدر:.U.N.E.Government survey,Newyork,2018,P.228-232

الخريطة (١) تباين مؤشرات تطور أداء الحكومة الإلكترونية لدول مجلس التعاون



٢- نسبة المشتركين بخدمة الانترنيت في دول مجلس التعاون

إن نسبة كبيرة من سكان دول مجلس التعاون يستخدمون الانترنيت الجدول (٤) حيث نلاحظ أن هذه النسبة بلغت أعلاها في البحرين حيث بلغت ٩٨% من السكان، وتأتي قطر بالمرتبة الثانية بين دول المجلس بنسبة بلغت ٩٤,٢٩% من السكان وتليها دولة عمان حيث سجلت نسبة مستخدمي الانترنيت ٩٣,٦٩% ثم الإمارات بنسبة بلغت ٩٠,٦% من السكان و تأتي الكويت في المرتبة الخامسة بين دول المجلس من حيث نسبة مستخدمي الانترنيت من السكان بلغت ٧٨,٣٧% ، وتأتي السعودية في المرتبة الأخيرة بنسبة بلغت ٧٣,٧٥% من السكان، وهذه النسب مرتفعة جداً مقارنة بالولايات المتحدة الأمريكية حيث بلغ نسبة مستخدمي الانترنيت إلى جملة السكان ٧٦,١٨% وفي إسرائيل بلغت النسبة ٧٩,٦٥% وفي تركيا بلغت ٥٨,٣٥% من السكان من الواضح أن للمستوى المعاشي المرتفع لسكان دول مجلس التعاون دور كبير في استخدام نسبة كبيرة من السكان للأنترنيت مقارنة مع الدول الأخرى وارتفاع هذه النسب يدل على تواصل سكان هذه الدول مع العالم ومستجداته ، كما ان توظيف الانترنيت في النواحي الاقتصادية والسياسية والاجتماعية يسهم في تعزيز عناصر القوة في الدولة .

٣-البنية التحتية للاتصالات اللاسلكية:

أن من مؤشرات القوة الإلكترونية لأي دولة هي تنمية و تطوير البنية التحتية لتكنولوجيا المعلومات والاتصالات والتكنولوجيا الرخيصة، وقد اعتمد المؤشر العالمي لتنمية الاتصالات لعام (٢٠١٧) (WIDC-المنعقد في بوينس آيرس (الأرجنتين) الهدف رقم ٢ و هو بنية تحتية حديثة وآمنة للاتصالات و تكنولوجيا المعلومات و تعزيز وتنمية البنية التحتية والخدمات بما في ذلك بناء الثقة والأمن في استخدام الاتصالات وتكنولوجيا المعلومات.

والبنى التحتية للاتصالات هو نظام النقل والإرسال مثل أسلاك الهواتف وأسلاك الألياف الضوئية والعوائل ،والموجات الدقيقة والوحدات اللاسلكية ، ويمكن بناءَ عليه تقديم خدمات الاتصال. ومن ثم تيسير الاندماج بين خدمات الإنترنيت والاتصال عن بعد و تكنولوجيا الوسائط المتعددة وتطبيقاتها [١٦] .

تفصح البيانات المتاحة في الجدول (٤) أن أفضل خدمة للاتصالات اللاسلكية تقدمها دول مجلس التعاون لسكانها هي خدمة الهاتف الخلوي وأن هذه الخدمة في جميع دول المجلس تفوق دول المقارنة وأعلى خدمة للهاتف الخلوي سجلت في الإمارات العربية بدرجة قدرت ب ٢١٤,٧ خدمة لكل ١٠٠ نسمة من السكان تليها البحرين ب ٢١٠,١٤ خدمة لكل ١٠٠ نسمة، أما في دول المقارنة فإن إسرائيل كانت أفضل هذه الدول بكفاءة بلغت ١٢٩,٠٣ خدمة لكل ١٠٠ نسمة وأقل من خدمة جميع دول المجلس تليها الولايات المتحدة الأمريكية بدرجة خدمة بلغت ١٢٢,٨٨ خدمة لكل ١٠٠ نسمة من السكان، وفي الجدول (٤) يظهر لنا تفوق أربع دول من دول المجلس وهي حسب الترتيب (الكويت، الإمارات، البحرين، قطر) على الولايات المتحدة الأمريكية ، وسجلت تركيا أيضاً نسب أقل من جميع دول المجلس في هذا الحقل ينظر الخريطة (٢) .

أما إسرائيل فقد سجلت كفاءة أقل من أربع دول في هذا الحقل وتساوت مع عمان بدرجة بلغت ٩١,٥ وتفوقت على السعودية أما بالنسبة لخدمات الهاتف الثابت لكل ١٠٠ نسمة من السكان و خدمة الثابت السلكي موجة عريضة لكل ١٠٠ نسمة فنلاحظ تفوق كل من الولايات المتحدة الأمريكية وإسرائيل على جميع دول المجلس في هاتين الخدمتين.

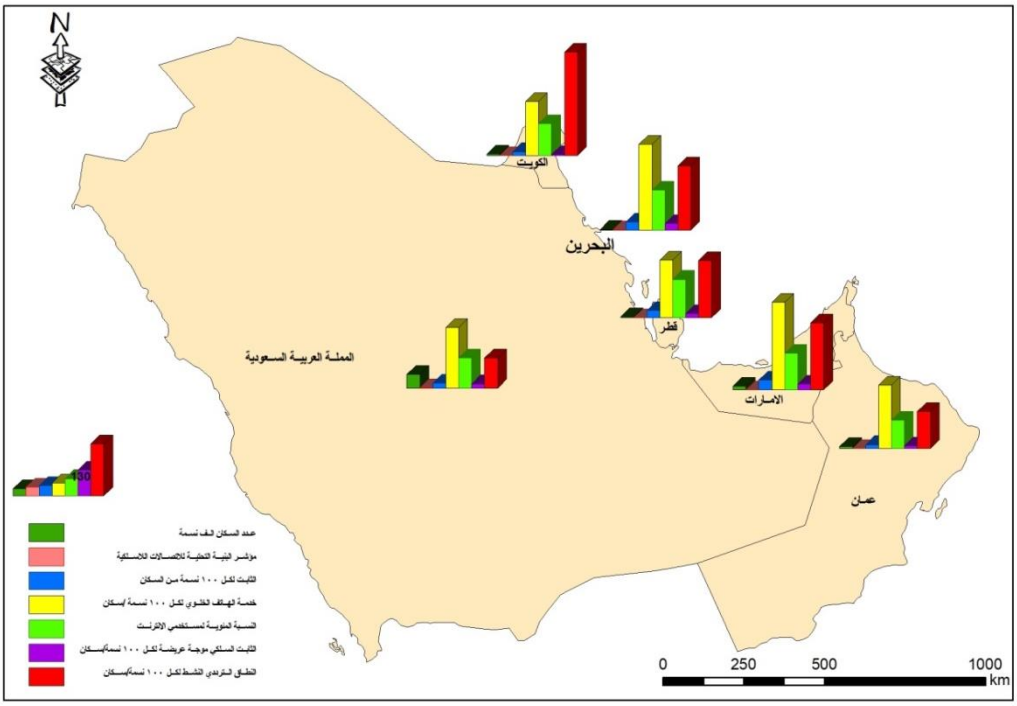
الدول			مكونات المؤشر

	عدد السكان الف نسمة	مؤشر البنية التحتية للاتصالات اللاسلكية	الهاتف الثابت لكل ١٠٠ نسمة من السكان	خدمة الهاتف الخلوي لكل ١٠٠ نسمة/سكان	النسبة المئوية لمستخدمي الإنترنيت	الثابت السلكي موجة عريضة لكل ١٠٠نسمة /سكان	النطاق الترددي النشط لكل ١٠٠ نسمة /سكان
المملكة العربية السعودية	٣٣,٧٠	٠,٥٣٣٤	١١,٨٦	١٤٨,٥١	٧٣،٧٥	١٠,١٩	٧٤
عمان	٤,٨٣	٠,٥٣١	٩,٥٥	١٥٥,١٨	٦٩,٩٣	٦,٤٣	٩١,٤٦
قطر	٢,٧٨	٠,٦٧٩٧	١٨,١٨	١٤٢,١٣	٩٤،٢٩	٩,٨٧	١٣٩,٩٢
الكويت	٤,١٤	٠,٧٣٩٤	٩,٩٥	١٣٣,٠٧	٧٨,٣٧	٢,٥	٢٥٤,٤٢
الإمارات العربية المتحدة	٩,٦٣	٠,٥٨٦٤	٢٤,٦٦	٢١٤,٧٣	٩٠,٦	١٤	١٦٤,٨٩
البحرين	١,٥٧	٠,٨٤٦٦	١٩,٤٦	٢١٠،١٤	٩٨	١٦,٢٩	١٥٧,٣٤
الولايات المتحدة الأمريكية	٣٢٨,٦٧٣	٠,٧٥٦٤	٣٧,٧٢	١٢٢,٨٨	٧٦,١٨	٣٣	١٢٧
إسرائيل	٨,٨٨٤	٠,٧٠٩٥	٤٠,٧٨	١٢٩,٣	٧٩,٦٥	٢٧,٥٦	٩١,٥٥
تركيا	١٨,٣٣٩	٠,٤٢٩٨	١٣,٩٣	٩٤,٤	٥٨,٣٥	١٣,٢١	٦٥,٠٧

الجدول (٤) مؤشر البنية التحتية للاتصالات اللاسلكية و مكوناته لدول مجلس التعاون الخليجي و دول المقارنة ٢٠١٨

1-U.N.E.Government survey ,New york,2018,P.251-255.
2-U.N.Statistical year book, New York,2019,P.114.

الخريطة (٢) التباين المكاني مؤشر البنية التحتية للاتصالات اللاسلكية و مكوناته لدول مجلس التعاون الخليجي



٤- نسبة الإنفاق على برامج الكومبيوتر من الناتج المحلي الإجمالي:

كلما زاد الإنفاق من الناتج المحلي على برامج الكومبيوتر والحاسوب كلما كان مؤشر قوة بالنسبة للدولة، لأنه كلما زاد نسبة الإنفاق على هذه البرامج كلما تحقق للدولة حماية أكثر في مجال أمنها السيبراني فمن خلال هذه البرامج تستطيع الدولة السيطرة أكثر على الخروقات والقرصنة ومنعها والتي تؤدي بدورها إلى تهديد مجالها السيبراني الجدول (٥) يظهر لنا نسبة الإنفاق من الناتج المحلي الإجمالي لدول المجلس على برامج الكومبيوتر فبالرغم من امتلاك بعض دول المجلس ناتج محلي كبير إلا أن نسبة ما ينفق على هذه البرمجيات لا يصل إلى ١% مثال السعودية التي تمتلك أكبر ناتج محلي إجمالي على مستوى دول مجلس التعاون يقدر ب ١,٨٥٦،٦ مليار دولار و نسبة ما تنفقه على برامج الكومبيوتر لا تتعدى ٤% من الناتج المحلي الإجمالي.

ولكن وبالمقارنة مع دولة عظمى كالولايات المتحدة الأمريكية التي يبلغ قيمة الناتج المحلي لها ٢٠,٥١٣،٠ مليار دولار ونسبة الإنفاق يبلغ فقط ١,١% فإن نسبة الإنفاق في السعودية وبقيمة دول المجلس جيدة، كما ونلاحظ أن الناتج المحلي الإجمالي لتركيا أيضاَ يبلغ ٢,٣١٤,٤ مليار دولار وهي تنفق نسبة ٠,٥% فقط على برامج الكومبيوتر وحالها ليس

بأفضل من حال دول مجلس التعاون و قريبة منها حيث أن الكويت التي تمتلك فقط ٣٠٣,٣ مليار دولار ناتج محلي سجلت نسبة انفاق ٠,٤%.

واجمالا للقول فان منظومة الفضاء السيبراني هي اليات يمكن من خلالها تحويل القدرات العلمية والثقافية الى مخرجات اقتصادية وعلمية وسياسية وعسكرية بما يسهم في بناء وتعزيز القوة في دول مجلس التعاون لدول الخليج العربية طبق للاطار النظري في الجغرافية السياسية وهذا الهدف لا يتحقق الا في الاقتصاديات التي تبنى على اساس المعرفة.

الجدول (٥) نسبة الإنفاق على برامج الكومبيوتر من الناتج المحلي الإجمالي لدول مجلس التعاون ودول المقارنة ٢٠١٩

الدول	الناتج المحلي الإجمالي دولار	نسبة الإنفاق على برامج الكمبيوتر
المملكة العربية السعودية	١.٨٥٦.٩	٠.٤
عمان	١٩٨.٢	٠.١
قطر	٣٥٦٥٧	٠.٣
الإمارات المتحدة	٧٣٢.٩	٠.٣
الكويت	٣٠٣.٣	٠.٤
البحرين	٧٥.٢	٠.٣
الولايات المتحدة الأمريكية	٢٠.٥١٣.٠	١.١
إسرائيل	٣٣٦.١	٠
تركيا	٢.٣١٤.٤	٠.٥

المصدر:

WIPO .Global innovation index,2019,P.220,272,279,313,319,335,338,341

ثالثا: الهجمات السيبرانية واستراتيجيات الردع المعتمدة في دول مجلس التعاون لدول الخليج العربية

الردع السيبراني هو منع الأعمال الضارة ضد الأحوال الوطنية في الفضاء [١٧]، و يرتكز على ثلاث ركائز هي : مصداقية الدفاع، والقدرة على الانتقام والرغبة في الانتقام . وفي ظل تعدد التهديدات السيبرانية التي تشمل الحرب الرقمية والإرهاب الرقمي والتجسس الرقمي، بجانب التزايد المفرط في أعداد الهجمات السيبرانية في السنوات القليلة الماضية، تتزايد أهمية الردع السيبراني لتأمين أجهزة الحاسب الآلي، وأنظمة المعلومات والبنى التحتية

من ناحية والحيلولة دون تكرار تلك الهجمات من خلال تحديد الخصم على نحو دقيق و توعده بالانتقام رداً على هجومه من ناحية ثانية و حماية الأمن القومي للدول الذي بات رهناً بالفضاء السيبراني من ناحية الثالثة [١٨] .

ويتم تحقيق الردع السيبراني من خلال رفع تكلفة الهجوم الإلكتروني للدولة المعتدية، عبر إنشاء نظم دفاعية الكترونية صعبة الاختراق تحتاج إلى وقت وجهد كبيرين لاختراقها مع تطوير قدرات تتبع الهجمات السيبرانية واكتشاف مصدرها بما يؤدي إلى التأثير على قرارات الخصم وردعه عن شن هجمات سيبرانية على الدولة في النهاية [١٩]. وقد شهد الفضاء السيبراني الخليجي في السنوات الأخيرة تزايد

الهجمات السيبرانية بشكل حاد نظراً لتعدد التهديدات السيبرانية لتشمل الحروب والإرهاب والتجسس الرقمي وغيرها، وبالرغم من اختلاف غرض وأهداف كل منها إلا أن القاسم المشترك بينها هو استغلال ثغرات ونقاط الضعف في المجال السيبراني بهدف اختراق الكومبيوتر و شبكات الحاسوب والجدول (٦) يبين لنا أهم التهديدات والهجمات السيبرانية في فضاء دول الخليج العربي منها دول مجلس التعاون.

وتوكد التقارير الدولية أن ما يزيد على مئة دولة قد طورت أو تعمل على تطوير قدراتها الهجومية الإلكترونية، فمن المتوقع أن تشكل حرب الفضاء السيبراني جزءاً هاماً من كافة الصراعات المستقبلية، كما ستطلب الأسلحة الإلكترونية الافتراضية دوراً قد يكون حاسماً في الحرب الفعلية و ستكون الغلبة للدولة التي تتفوق في حماية فضاءها السيبراني و تعطيل فضاء أعدائها بعد أن تضمن قدرة جيشها على استخدام تقنية المعلومات و شن هجمات في الفضاء السيبراني الافتراضي بما يحدث أثاراً ملموسة [٢٠].

الجدول (٦) التهديدات والهجمات السيبرانية في فضاء دول الخليج العربي

السنة	التهديد أو الهجمة	الدولة المستهدفة	القطاع المستهدف	الوصف
٢٠١٢	شمعون Shamoon	السعودية	شركة أرامكو	قام فريق من القراصنة السيبرانين الإيرانيين أطلق على نفسه اسم(سيف العدالة القاطع)

				في شهر آب من عام ٢٠١٢ بإقحام فيروس خبيث أطلق عليه اسم Shamoonفي شبكة المعلومات الداخلية لشركة أرامكو السعودية النفطية والذي باشر على الفور نشاطه التخريبي فقام بإلغاء بيانات مهمة في أكثر من ٣٠,٠٠٠حاسب من حواسيب الشركة بالإضافة إلى أدراج صورة لعلم الولايات المتحدة الأمريكية الذي التهمته النيران.
٢٠١٤	Rocket Kitten	دول خليجية ودول عربية أخرى	شبكات الاتصالات والمعلومات	قامت هذه المجموعة من قراصنة المعلومات باختراق شبكات المعلومات والاتصالات في دول خليجية و أصابتها بأضرار جسيمة.
	عملية كليفر Operation Cleaver	قطر ،الكويت، السعودية االإمارات	النفط والغاز ،المطارات مواقع حكومية حساسة شركات الاتصالات	تعد من أشد الهجمات السبيرانية تأثراَ وقد قامت بها مجاميع متعددة من القراصنة السيبرانين الإيرانيين على دول متعددة من الخليج بالإضافة إلى الولايات المتحدة الأمريكية ودول أوروبية وقد خطط لأن تكون ذات تأثيرات جسيمة على قطاعات حيوية في دول الخليج العربي و دول أخرى.
٢٠١٦	شمعون Shamoon	السعودية	شركة أرامكو	بعد هذا البرنامج الخبيث نسخة مطورة من البرنامج الذي استهدف شركة أرامكو السعودية عام ٢٠١٢ وقد توسعت قطاعات تأثيره إلى قطاعات مضافة إلى قطاعي النفط والغاز.
٢٠١٧	الصخرة الدوارة Stone DRILL فيروس صاحبا للغدية Mamba Ransomware	السعودية دول خليجية متعددة	الطيران والبتروكيمياويات القطاع المالي	أحدث هذا البرنامج الخبيث تأثيرات كبيرة على شركات الطيران و شركات البتروكيمياويات في السعودية. يعد من برمجيات الغدية الخبيثة أحكمت قيضتها على حواسيب موجودة في القطاع المالي لدول خليجية متعددة أورثتها خللاَ

				كبيراَ
٢٠١٨	تريتون Triton	دول خليجية متعددة	قطاع النفط والغاز والصناعات البتروكيمياوية	يعد هذا البرنامج الخبيث من الانسال الجديدة التي حملت أثاراَ خطيرة على قطاعي النفط والغاز والصناعات البتروكيمياوية في دول خليجية مع وجود تهديدات باتجاه أحداث تفجيرات ممنهجة يمكن أن تؤدي بحياة العاملين في مواقع العمل.
٢٠١٩	التهديدات السيبرانية المتقدمة المستمرة APT	قطر، الكويت السعودية الإمارات البحرين	البنى التحتية المهمة	هجمات سيبرانية بالغة التأثير مارسها القراصنة الإيرانيون السيبرانيون لاستهداف شبكات المعلومات و بنيتها التحتية و خلال مدد زمنية متطاولة لضمان بلوغ أهدافها و تعميق مستويات تأثيرها.

المصدر: حسن مظفر الرزو ، النزاعات والمواجهات السيبرانية في فضاء منطقة الخليج العربي ، تقارير، ٢٠١٩، على الموقع: http://studies.aljazeera.ne

وقد أدت الهجمات التي وقعت خلال السنوات القليلة الماضية في الفضاء السيبراني لدول الخليج العربي إلى قيام نشاط ملحوظ بين دول مجلس التعاون الخليجي لبناء قدرات الأمن السيبراني وإنشاء المؤسسات المتخصصة بهذا الشأن ووضع الاستراتيجيات اللازمة للحد من هذه الهجمات كما تم سن قوانين خاصة بمكافحة الجرائم السيبرانية. ولردع الهجمات السيبرانية في فضاء دول مجلس التعاون تم تأسيس مراكز وطنية لحماية الأمن السيبراني و فرق الاستجابة لطوارئ الحاسب الآلي والمركز الإقليمي للأمن الإلكتروني للمنطقة العربية و هذه المراكز هي :-

١-مركز الاستجابة لطوارئ الحاسب الآلي: أنشأت هيئة تنظيم الاتصالات بدولة الإمارات العربية المتحدة مركز الاستجابة لطوارئ الحاسب الآلي عام ٢٠٠٧، لتحسين معايير و ممارسات أمن المعلومات و حماية البيئة التحتية التقنية والمعلومات من مخاطر اختراقات الإنترنيت [٢١].

٢-فرقة الاستجابة لطوارئ الحاسب الآلي القطري؛ تم إنشاء المركز الوطني لأمن المعلومات من قبل المجلس الأعلى لهيئة تقنية المعلومات والاتصالات القطرية عام ٢٠٠٥ [٢٢] .

٣-المركز الوطني الإرشادي لأمن المعلومات: فرقة الاستجابة لطوارئ الحاسب الآلي تم إنشاء هذا المركز بواسطة هيئة الاتصالات و تقنية المعلومات السعودية و يهدف للكشف عن التهديدات و المخاطر ومنع الاختراقات والانتهاك للأمن السيبراني والتنسيق والاستجابة للمعلومات عن حوادث الأمن السيبراني على مستوى المملكة [٢٣] .

وفي عام ٢٠١٣ وهو العام الذي أعقب هجوم شمعون على أرامكو، اعتمدت المملكة السعودية أول استراتيجية وطنية لأمن المعلومات وفي عام ٢٠١٧ افتتحت الرياض مركزها الوطني للأمن السيبراني التابع لوزارة الداخلية كمركز تنسيق فني وطني للدفاع الإلكتروني[٢٤].

٤-مركز الاستجابة لطوارئ الحاسب الآلي و فرقة الاستجابة لطوارئ الحاسب الآلي في دولة البحرين عام ٢٠١٢.

٥- المركز الوطني للاستجابة لطوارئ الحاسب الآلي في دولة الكويت والذي سيرتبط بالمراكز المماثلة المنتشرة حول العالم الذي تم افتتاحه خلال معرض الكويت لأمن المعلومات عام ٢٠١٢[٢٥].

وقامت دولة الكويت أيضاَ بوضع الاستراتيجية الوطنية للأمن السيبراني للفترة (٢٠١٧-٢٠٢٠) و تتمثل رؤية الاستراتيجية في ضمان فضاء الكتروني أمن و مرن لحماية المصالح الوطنية لدولة الكويت من المخاطر والتهديدات السيبرانية و تحقيق أكبر قيمة اقتصادية واجتماعية من استخدام الفضاء الإلكتروني و تسعى الاستراتيجية إلى تحقيق ثلاث أهداف رئيسية هي [٢٦]:

١. تعزيز ثقافة الأمن السيبراني التي تدعم الاستخدام الأمن والصحيح للفضاء الإلكتروني.
٢. حماية ومراقبة الأصول والبنى التحتية الحيوية والمعلومات الوطنية والشبكة المعلوماتية في الدولة.
٣. إتاحة سبل التعاون والتنسيق وتبادل المعلومات بين مختلف الجهات المحلية والدولية في مجال الأمن السيبراني.

واتخذت دول مجلس التعاون لدول الخليج العربية عدة خطوات أيضاَ لسن قوانين تتعلق بالجرائم الإلكترونية وأنشأت أنظمة خاصة بذلك الهدف منها حماية المعاملات الإلكترونية وملاحقة مجرمي الأنترنيت ومن هذه القوانين [٢٧].

١. الإمارات العربية المتحدة: القانون الاتحادي رقم ٥ لسنة ٢٠١٢ في شأن مكافحة جرائم تقنية المعلومات.

٢. المملكة العربية السعودية: نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم ١٧

٣. سلطنة عمان: قانون مكافحة جرائم تقنية المعلومات بالرقم ٢٠١١/١٢.

٤. دولة الكويت: قانون رقم ٦٣ لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات.

٥. دولة قطر: قانون مكافحة الجرائم الإلكترونية رقم ١٤ لسنة ٢٠١٤.

٦. مملكة البحرين: قانون رقم (٦٠) لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات.

الاستنتاجات:

١. اصبحت قضية الأمن السيبراني على رأس أولويات قضايا الأمن القومي لدول مجلس التعاون في محاولة لمواجهة تصاعد التهديدات السيبرانية اذا باتت العلاقة بين الامن والتكنولوجيا علاقة متزايدة مع امكانية تعرض المصالح الاستراتيجية ذات الطبيعة الالكترونية الى اخطار الكترونية

٢. حققت دول مجلس التعاون لدول الخليج العربية تقدماَ في مجال الأمن السيبراني و يظهر ذلك من خلال دليل الأمن السيبراني العالمي والمؤشرات العالمية لتطور واداء الحكومة الالكترونية حيث سجلت دول المجلس مراتب متقدمة على مستوى العالم فقد احتلت السعودية المرتبة ١٣ عالميا واحتلت قطر المرتبة ١٦ عالميا في حين سجلت قطر المرتبة١٧ على مستوى العالم.

٣. ارتفاع وتيرة الهجمات السيبرانية وتوسع رقعة الحرب ضد دول مجلس التعاون لدول الخليج العربية عبر شبكات المعلومات الدولية يجعلها تشكل تهديدا لأمنها الاقتصادي والسياسي والعسكري طالما ان هذه الهجمات تتسبب في ضرب وشلل المنظومات الالكترونية التي تشكل العمود الفقري للأنشطة المدنية والعسكرية في دول المجلس .

٤. تتبنى دول مجلس التعاون استراتيجيات وطنية تعمل على محوري الدفاع والهجوم بهدف تحقيق الردع السيبراني وذلك من خلال تعظيم معايير الامن للشبكات الالكترونية فضلا عن اعتماد سياسة الدفاع الالكتروني المشترك مما يساهم في بناء قوة الدولة طبقا للاطار النظري في الجغرافية السياسية.

المصادر

١. ITU .Global cyber security index, Switzerland, 2018.p, 26,27,57 ,58, 61,62.،

٢. U.N .Statistical year book, new York,2019,p,114.

٣. U.N.E .Government survey, New york,2018,p, 228-232, 251-255.

٤. WIPO .Global innovation index,2019, ,P.220 ,272,279 ,313,319 ,335 ,338,341

٥. حسن مظفر الرزو ، النزاعات والمواجهات السيبرانية في فضاء منطقة الخليج العربي ، تقارير، ٢٠١٩، على الموقع: http://studies.aljazeera.net

الاحالات:

(١) أنور ماجد عشقي، الأمن السيبراني والقمة الخليجية الأمريكية، مجلة الأمن والحياة، جامعة نايف العربية للعلوم الأمنية،العدد ٤٠٩، ٢٠١٦، ص٢٦.

(2) Richard A.tomerere, Cyber security, university of California Santa Barbara, Department of computer science,2003,P.3.

(3) Edward Amoroso, cyber security, silicon press,2007,P.1.

(4) ITU ,cyber security ,Geneva: International Telecommunication union (ITU), 2008.

(٥) محمد بن أحمد علي المقصودي، الجرائم المعلوماتية خصائصها و كيفية مواجهتها قانونياً، المجلة العربية للدراسات الأمنية، جامعة نايف العربية للعلوم الأمنية المجلد ٣٣، العدد ٧٠، ٢٠١٧، ص١٣.

(٦) سليم دحماني، أثر التهديدات السيبرانية على الأمن القومي، الولايات المتحدة نموذجا (٢٠٠١-٢٠١٧) رسالة ماجستير، غير منشورة، جامعة محمد بو ضيافه-المسلة، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية، ٢٠١٨، ص٣٣.

(٧) منى الأشقر جبور، السيبرانية هاجس العصر، جامعة الدول العربية، المركز العربي للبحوث القانونية والقضاء، ص٣١.

(٨) عبدالفتاح بيومي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والأنترنيت ، دار الكتب القانونية، مصر، ٢٠٠٧، ص١٩٨.

(٩) منى الأشقر جبور، مصدر سابق، ص٣٠.

(١٠) اسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية، جامعة ديالى، المجلد ١٠، العدد ١، ٢٠١٩، ص ١٠٢٢.

(١١) سليم دحماني، مصدر سابق، ص٣٢.

(*) **جوزيف .س ناي:** من أبرز المهتمين بالقوة السيبرانية، استاذ العلوم السياسية في جامعة هارفارد، وهو من أبتكر مصطلح القوة الناعمة والقوة الذكية.

(12) Joseph S.Nye JR, Cyber Power ,Hardwar Kennedy School,2010.P.

(١٣) علاء الدين فرحات ، الفضاء السيبراني ، تشكيل ساحة المعركة في القرن الواحد والعشرين ، مجلة العلوم القانونية والسياسية ، المجلد ١٠ ، العدد ٣ ، ٢٠١٩، ص ص ٨٨-١٠٧

(١٤)علم الدين بانقا، مخاطر الهجمات الإلكترونية (السيبرانية) وآثارها الاقتصادية دراسة حالة دول مجلس التعاون الخليجي، المعهد العربي للتخطيط، مجلة دراسات تنموية، الكويت ، العدد ٦٣، ٢٠١٩، ص ٤٢.

(١٥) خالد دهلز، خالد لبد، مقومات نجاح تطبيق الحكومة الإلكترونية في فلسطين: دراسة استكشافية، مجلة جامعة النجاح للأبحاث (العلوم الإنسانية) المجلد ٣١، العدد ٧، ٢٠١٧، ص ١١١٧.

(١٦) منظمة الأمم المتحدة للتربية والتعليم، اليونسكو، على الموقع : Ar.unesco.org

(17)Michael krepon ,Julia Thompson ,deterrence and Sino-American relations, united states,stimson-center,2013,P.15.

(١٨) رغدة البهي، الردع السيبراني، المفهوم والإشكاليات والمتطلبات، مجلة العلوم السياسية والقانون، المركز الديمقراطي العربي ، برلين ، المانية ، العدد١، ٢٠١٧، ص١٧.

(١٩) إيهاب خليفة، تنامي التهديدات السيبرانية للمؤسسات العسكرية، مجلة اتجاهات الأحداث، ابو ظبي ، العدد٢٢، ٢٠١٧، ص٥٥.

(٢٠) ريتشارد كلارك، روبرت نيك، حماية الفضاء الإلكتروني في دول مجلس التعاون لدول الخليج العربية، مركز الآمرات للدراسات والبحوث الاستراتيجية، أبوظبي، ٢٠١٠، ص ٩.

(٢١)الاستراتيجية الوطنية للأمن السيبراني، البيئة الوطنية للأمن السيبراني، الإمارات، ٢٠١٩، على الموقع U.ae<ar-ae<national-cyber security-strategy – 2019.

(٢٢) الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، مجلس التعاون لدول الخليج العربية الأمانة العامة، مسابقة جائزة الأمير نايف بن عبدالعزيز للبحوث الأمنية لعام ٢٠١٥، مجمع البحوث والدراسات ، أكاديمية السلطان قابوس لعلوم الشرطة، نزوي – سلطنة عمان، ٢٠١٦، ص ٨٧.

(٢٣) ليلى الجنابي، فعالية القوانين الوطنية والدولية في مكافحة الجرائم السيبرانية الحوار المتمدن، العدد ٥٦٣٤، ٢٠١٧، ص ١٢. على الموقع http://www.ahewar.org

(٢٤)عادل رفيق، الجيوبوليتكس السيبرانية والاستقرار في الشرق، المعهد المصري للدراسات ، ٢٠١٨،على الموقع .www.EIPSS.E.G.ORG

(٢٥) ليلى الجنابي، مصدر سابق، ص ١٣

(٢٦) علم الدين بانقا، مصدر سابق، ص٤٦.

(٢٧) ليلى الجنابي، مصدر سابق ، ص ١١.