الأثر العسكري للأمن السيبراني في الجغرافيا السياسية للدولة

The Military Impact of Cyber security in the Political Geography of the State

Taghreed Moeen Hassan ALmashhadi

المدرس الدكتورة
تغريد معين حسن المشهدي
جامعة الكوفة – كلية الآداب
قسم الجغرافيا

ملخص البحث :

يهدف البحث في التعرف على الاثر العسكري للأمن السيبراني في الجغرافية السياسية للدولة لكونه موضوع حديث يتعلق بالمفاهيم الجغرافية السياسية كالدولة والسيادة والقوة والحرب والامن فقد قسم البحث لعدة مباحث تناول الاول منها مفاهيم تخص الامن السيبراني والقوة السيبرانية وما يتعلق بها ولاسيما بالبعد العسكري ،اما المبحث الثاني تناولت تحليل علاقة الامن السيبراني بالجغرافية السياسية فضلاً عن تحليل كل عنصر جغرافي سياسي على حدة كالدولة والقوة والامن القومي بما يتلاءم مع هدف البحث، اما المبحث الثالث فكان عن الاثر العسكري للامن السيبراني والذي تطرق الباحثة فيه فيه لمفهوم الحرب السيبرانية فضلاً عن قياس الامن السيبراني للدول العالم والدول العربية ،اما المبحث الرابع فتم فيه بناء نظرية جيوبولتيكية جديدة من خلال تحليل النظريات القديمة البرية والبحرية والجوية وختم البحث باستنتاجات وتوصيات

الكلمات المفتاحية : الامن السيبراني –الاثر العسكري –الجغرافية السياسية –الدولة –القوة –السيادة

المقدمة

الجغرافيا السياسية والمفاهيم التابعة لها لاسيما السيادة قد تغيرت ويجب اعادة تعريفها ،بسبب ان قدرة كل دولة لم تعد مؤكدة في الحفاظ على اتصالاتها وقيادتها وسيطرتها وقدراتها الحاسوبية ضد التهديدات الجديدة من الانترنيت التي تواجه العالم بأكمله ، كالهجمات الارهابية وعصابات الجريمة المنظمة وغير ذلك من الدول ،فالمساحة الافتراضية التي يشغلها الانترنيت يمكن ان تهدد سيادة ومصالح الدول بسبب نطاقها العالمي وامكانية نقل المعلومات خارج نطاق سيطرة الدول في ضوء ذلك تتمثل **اهمية البحث** في تزايد البعد العسكري للقوة السيبرانية على الجغرافيا السياسية لكثير من البلدان في اطار ما اطلق عليه الفضاء الالكتروني ومجال الحرب الجديدة وما يتصل بها من تهديدات لسيادة الدول وامنها القومي .

هدف البحث معرفة الاثر العسكري للأمن السيبراني في الجغرافيا السياسية للدولة.

مشكلة البحث ما هو أثر الفضاء السيبراني على مفاهيم القوة ، الحرب ، الأمن ؟

كمفاهيم متعلقة بالجغرافيا السياسية للدولة لاسيما ببعدها العسكري .وكيف اثر الفضاء السيبراني على تلك المفاهيم

فرضية البحث للأنترنيت والامن السيبراني تأثير كبير على الدول بكل مفاهيم الجغرافية السياسية لاسيما القوة والحرب والامن التي تتعلق بالبعد العسكري

المبحث الاول : المفاهيم العلمية

١-الامن السيبراني : هو مفهوم ظهر بعد الحرب الباردة استجابة للمزيد من الابتكارات التكنولوجية والظروف الجيوسياسية المتغيرة ، تم استخدامه لأول مرة من قبل علماء الكمبيوتر في اوائل التسعينات للتأكيد عل سلسلة من حالات عدم الامان المرتبطة بأجهزة الكمبيوتر لكنه تجاوز مفهومه التقني لأمن الكمبيوتر عندما حث المؤيدين على ان التهديدات الناشئة عن التقنيات الرقمية يمكن ان يكون لها اثار اجتماعية مدمرة .[١] يعرف الامن السيبراني هو العملية او قدرة الدولة التي يتم بموجبها حماية انظمة الاتصالات والمعلومات الواردة اليها و الدفاع عنها ضد الضرر او الاستخدام غير المصرح به او التعديل او الاستغلال . ويعرف ايضاً بانه امن الشبكات والانظمة المعلوماتية والبيانات والمعلومات والاجهزة المتصلة بالأنترنيت وعليه فهو المجال الذي يتعلق بإجراءات مقايس ومعايير الحماية المفروض اتخاذها والالتزام بها لمواجهة التهديدات ومنع التعديات او للحد من اثارها في اقسى واسوأ الاحوال . [٢]

ويعرف الامن السيبراني انطلاقاً من أهدافه بانه النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات ويضمن امكانات الحد من الخسائر والاضرار التي تترتب في

حال تحقق المخاطر والتهديدات، كما يتيح اعادة الوضع الى ما كان عليه بأسرع وقت ممكن بحيث لا تتوقف عجلة الانتاج، ولا تتحول الاضرار الى خسائر دائمة. (٣)

٢- الفضاء السيبراني : هو مجال عالمي في بيئة المعلومات الذي يتميز من خلال استخدام الإلكترونيات والطيف الكهرومغناطيسي لإنشاء وتخزين وتعديل وتبادل واستغلال المعلومات عبر شبكات مترابطة باستخدام تقنيات الاتصالات المعلوماتية . (٤) والفضاء السيبراني كبيئة افتراضية عالمية لأنظمة المعلومات العامة والخاصة المترابطة فيما بينها الذي يتم فيه إنشاء أنواع مختلفة من المعلومات وتخزينها ونقلها داخل الفضاء السيبراني ، بما في ذلك أنواع معينة من المعلومات التي تهيمن على متطلبات أمن المعلومات بشكل عام ، وكذلك القوانين واللوائح الوطنية والدولية المختلفة. (٥)

وهو عالم افتراضي يتشابك مع عالمنا المادي يتأثر به ويؤثر فيه بشكل معقد أذ تقوم العلاقة بين العالمين على نظرة تكاملية تحمل في طياتها مزايا ومخاطر لا تتوقف . بيد أن طبيعة ذلك الفضاء كساحة عالمية عابرة لحدود الدول جعل الأمن السيبراني يمتد من داخل الدولة إلى النظام الدولي ليشكل نوعاً من الأمن الجماعي العالمي لاسيما مع وجود مخاطر تهدد جميع الفاعلين في مجتمع المعلومات العالمي .(٦)ومنهم من يعرفه المجال المادي وغير المادي الذي يتكون من عناصر هي أجهزة الكومبيوتر والشبكات والبرمجيات وحوسبة المعلومات ومعطيات النقل والتحكم ومستخدمو كل هذه العناصر، أذ تعد كل هذه العناصر العامل المشترك في جميع محاور استخدام الفضاء السيبراني، سواء أكانت الجهات المستخدمة قادرة على تعظيم قيمتها وقدراتها بما في ذلك رفع كفاءة العنصر البشري(٧)

٣- الفضاء الجيوسيبراني العلاقة بين الانترنيت والجغرافيا والديمغرافيا والاقتصاد والسياسة للدولة وسياستها الخارجية .

٤- الاستقرار الجيو سيبراني : قدرة جميع البلدان على الاستفادة من الانترنيت لتحقيق فوائد اقتصادية وسياسية وديمغرافية مع الامتناع عن انشطة يمكن ان تسبب معاناة ودمار لهما .

٥- القوة السيبرانية : وهي القدرة على استخدام الفضاء السيبراني لخلق المزايا والتأثير على الأحداث في البيئات التشغيلية الأخرى وعبر أدوات القوة وهي مجموعة الوسائل، والطاقات، والإمكانيات المادية وغير المادية، المنظورة وغير المنظورة التي بحوزة الدولة وتمثل الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات، والشبكات الإلكترونية، والبنية التحتية المعلوماتية، والمهارات البشرية المدربة للتعامل مع هذه الوسائل ، ويستخدمها صانع القرار في فعل مؤثر يحقق مصالح الدولة، وتؤثر في سلوك الوحدات السياسية الأخرى"(٨)

٦- **الإرهاب السيبراني** :هو الهجوم ذي الدوافع السياسية أو التهديد بالهجوم على أجهزة الكمبيوتر أو الشبكات أو أنظمة المعلومات من أجل تدمير البنية التحتية وترهيب الحكومة أو المواطنين وإجبارهم على تحقيق أهداف سياسية واجتماعية بعيدة المدى، بمعنى أوسع فإن الإرهاب السيبراني يعني استخدام الإنترنت للتواصل والدعاية والتضليل من قبل المنظمات الإرهابية . [٩]

٧- **الاستراتيجية السيبرانية** : تعني تطوير وتوظيف قدرات متكاملة ومتناسقة مع المجالات التشغيلية الاخرى للعمل في الفضاء السيبراني ، لدعم تحقيق الأهداف عبر عناصر السلطة الوطنية وتتناول القضايا الرئيسية المرتبطة بالاستراتيجية السيبرانية التحدي المتمثل في ابتكار "ردع مخصص" للتأثير على سلوك الكيانات الرئيسية التي تدعمها التطورات في الفضاء السيبراني.

٨- **الصراع السيبراني** :إنه مصطلح أكثر ملاءمة لأنه يؤكد على وجود التكنولوجيا الإلكترونية في كل مجال من مجالات النشاط ، بما في ذلك النزاع ويعد الصراع الالكتروني أحد أوجه الصراع الدولي، أذ يستطيع أحد أطراف الصراع أن يوقع خسائر فادحة بالطرف الاخر، وأن يتسبب في فشل البنية المعلوماتية والاتصالاتية الخاصة به وهو ما يسبب خسائر عسكرية واقتصادية فادحة من خلال قطع أنظمة الاتصال بين الوحدات العسكرية بعضها ببعض أو تضليل معلوماتها أو سرقة معلومات سرية عنها [١٠].

٩-**الجريمة السيبرانية** :نشاطاً غير مشروع موجهاً إلى نسخ أو تغيير أو حذف أو الوصول إلى المعلومات المُخزنة داخل الحاسوب أو التي تُنقل عن طريقه كما تُعرف بأنها سلوك غير مشروع فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات[١١].

١٠-**الدفاع السيبراني** :مجال فرعي وظيفي للأمن السيبراني ، ويتم التعامل معه على أنه جزء من عقيدة عسكرية ، ينبغي أن تعتمد على الموارد والممارسات التي وضعها الأمن الإلكتروني الوطني المعني. [١٢]

المبحث الثاني / الجغرافيا السياسية والامن السيبراني

أصبحت مساحة المعلومات مجالًا جديدًا للجغرافيا السياسية وغيرت توازن القوى بين الجغرافيا السياسية للدول وقد أوجد الإنترنت فضاءً عامًا جديدًا بالكامل ، اذ يتجاوز فضاء المعلومات المساحة الجغرافية المكانية التقليدية ويغير العلاقة المكانية للجغرافيا السياسية ، ويؤثر بعمق في الفضاء الجغرافي المكاني التقليدي [١٣].

ففضاء المعلومات يجعل الجغرافيا السياسية لها ميزات بنية مكانية جديدة أذ كان التحدي السابق يتمثل في الدفاع عن حدود الدولة في حين ساهمت تقنيات المعلومات والشبكات في إضعاف الحدود الجغرافية التقليدية بين الدول وأصبح من السهل للغاية اختراقها ويصعب اكتشافها من خلال الشبكة داخل أراضي

بلد ما كما توسعت السيادة الوطنية من المناطق والمجال الجوي إلى "حدود المعلومات" وتغير التفكير الجيوسياسي التقليدي القائم على العوامل الطبيعية للجغرافيا مما جعل الشبكة جزءًا جديدًا مهمًا من السيادة الوطنية ، كما أصبح أمن حدود المعلومات جزءًا مهمًا من الأمن القومي(١٤)

ولا يشكل فضاء المعلومات نوعًا جديدًا من الفضاء الجغرافي السياسي فقط ، بل يغير أيضًا توازن القوى بين الهيئات الجيوسياسية الأصلية ، مما يجعل القوى المختلفة المشاركة في السياسة الدولية من خلال الشبكة تتمتع بالمساواة النسبية في الوضع فلم تعد السياسة الدولية منطقة حصرية للحكومة وانما تشارك الحكومة التقليدية المنظمات غير الحكومية والشركات متعددة الجنسيات باعتبارها الموضوعات السياسية الدولية الرائدة إلى جانب تقدم تكنولوجيا شبكة المعلومات وصعود موجة التحول الديمقراطي سيصبح الأفراد بعد الحكومة والمنظمات غير الحكومية والشركات متعددة الجنسيات. وقد أظهرت الشبكة تأثيرات سياسية وعسكرية وثقافية قوية أذ بدأت الحرب الإلكترونية السيبرانية مثل حرب الرأي العام والحرب الثقافية والأيديولوجية وحرب المعلومات والاستخبارات التي حدثت على الإنترنت في عالم المعلومات الجغرافية الجديد مراراً وتكراراً(١٥) .

كما إن قوة المعلومات غيرت طبيعة وسلوك لبنة البناء الأساسية للعلاقات الدولية فقد ادركت الحكومات الأهمية الاستراتيجية للمعلومات أذ قامت بتطبيق استراتيجيات معلومات محلية ودولية فهم يكثفون بيئات معلوماتهم المحلية ويوقفون مواطنيهم عن تدفق المعلومات العالمية ، اذ تعتقد الصين وروسيا أن المنافسة الاستراتيجية في القرن الحادي والعشرين تتميز بمسابقة للسيطرة على البيانات ، فضلاً عن التكنولوجيا والمواهب اللازمة لتحويل البيانات إلى معلومات مفيدة. (١٦)

- **عناصر الجغرافيا السياسية وعلاقتها بالامن السيبراني**

اولا :الدولة والامن السيبراني في ظل العولمة

منذ نهاية الحرب الباردة كانت هناك العديد من الحجج التي تشير الى انه بسبب ترابط الانسانية عبر الانترنيت فان مفهوم الدولة والمفاهيم الجغرافية السياسية قد تم تجاوزها كظاهرة موازية لعولمة السلع والافكار المادية فضلاً عن ان العولمة قد اثرت في الامن القومي للدولة بطرق مختلفة الا ان الجغرافيا السياسية للدولة لها اهمية لاسيما في مواجهة التهديدات المتعلقة بالأمن السيبراني لعدة اسباب منها : (١٧)

١- ان البنى التحتية للأنترنيت من الاقمار الصناعية الى الموجهات والكوابل توضع في نقاط جغرافية محددة (معظمها تم وضعها من قبل شركات خاصة)ويؤخذ بوضعها الاعتبارات الجغرافية السياسية .

٢- تحدث عملية التبادل السيبراني في مناطق توجد فيها منافسات وتوترات جيوبوليتيكية .

٣- الاستخدام السيبراني له بعد جيوبوليتيكي.

٤- ان الفضاء السيبراني يعمل كمساحة افتراضية للعديد من الجهات الفاعلة لاستغلال استراتيجيتهم الجيوسياسية المتأصلة في العالم المادي ثلاثي الابعاد الذي نعيش فيه [١٨].

مع كل هذه الاسباب تبقى الدولة جزء من بنية الامن السيبراني التي تهدف الى تخفيف المخاطر السياسية الناشئة عبر الانترنيت ، اما النقطة الاهم هي **سيادة الدولة** وبما ان البنية التحتية لتقنية المعلومات والاتصالات اسست لحركة تدفق المعلومات عبر الحدود الجغرافية بين الدول محولة العالم الى قرية كونية لذا فرض ذلك واقعاً جديداً على السيادة الوطنية ، الامر الذي جعل الدولة تعاني من مشاكل اشد واخطر من تلك التي واجهتها من قبل ، فألى مسائل الامن عبر الحدود ومسائل الامن التقليدية برزت مشكلة السيادة على الفضاء السيبراني وعلى العلاقات التي تحاك عبر الانترنيت بين اشخاص موجودين على اراضي مختلفة خاضعة لعدد من السيادات اذ يختلف بلد مصدر العمل وبلد تحقق نتائجه والبلاد التي تمر عبرها البيانات فالفضاء السيبراني مكان مختلف لكنه شديد الارتباط بالعالم المادي وليس مستقلا عنه . [١٩]وهذا يعني ان الامن السيبراني اثر في سيادة الدولة ولم يلغيها وانما غير وظيفتها ومعناها يعني فرض وظيفة جديدة على سيادة الدول .

ثانيا : الامن السيبراني والامن القومي

نتيجة للتقدم العلمي والتقني السريع في مجال تطوير تكنولوجيا المعلومات والاتصالات والعولمة الديناميكية ظهر بالفعل نوع جديد من التهديدات لأمن الدولة والأمن الدولي في العقد الأخير من القرن العشرين تهديدات تكنولوجيا المعلومات تسمى أيضا تهديدات الإنترنت إنها تشكل تهديدًا بسرقة أو استخدام التكنولوجيا الحديثة أو بيانات تكنولوجيا المعلومات والاتصالات أو الحد من الجهات الفاعلة الأخرى (الكيانات أو الشركات عبر الوطنية أو مؤسسات الدولة أو المؤسسات الدولية) للوصول إلى بياناتهم الخاصة أو الشبكة العالمية ، أشكالها الرئيسية هي: الجريمة الإلكترونية والإرهاب الإلكتروني إنها نوع من القرصنة المستخدمة في ارتكاب جرائم الكمبيوتر وفي شبكة إنترنت عالمية (الفضاء الإلكتروني) ضد محتوى حقوق الطبع والنشر تعد الجرائم الموجهة ضد الأمن العام (في الدول) والمؤسسات التي تضمن الأمن القومي للدول والأمن الدولي خطيرة بشكل خاص وأخطر أشكال تهديد تكنولوجيا المعلومات هو الإرهاب السيبراني [٢٠].

وقد تطور مفهوم الأمن القومي تجاه التهديدات الجديدة غير التقليدية واتسع مجاله ليمتد من الجانب العسكري الى مجالات أخرى عديدة ، واذ أن أجهزة الحكومة الإلكترونية فى العالم في فضاء مفتوح ، ولعدم وجود حدود جغرافية لذا اصبحت أجهزتها عرضة للعديد من الاخطار تحت دوافع مختلفة ، ومن الممكن أن يتم مهاجمة أنظمة الحكومة الإلكترونية من داخلها أو من خارجها عن طريق الهاكرز أو أجهزة الاستخبارات في بلدان معادية عبر تنفيذ الهجمات الإلكترونية بهدف اختراق النظام الأمني المعلوماتي للحكومة ، ولذلك تغير مفهوم الأمن القومي إلى الأمن السيبرانى التي تسعى الدول إلى حمايته[٢١]

ثالثاً: الامن السيبراني وقوة الدولة

بفضل ثورة التكنولوجيا والاتصالات وظهور الفضاء الإلكتروني طرأت تحولات جديدة على مفهوم القوة وظهر مفهوم جديد أطلق عليه(القوة الإلكترونية)والتي أدت إلى توزيع القوة بين عدد أكبر من الفاعلين من غير الدول بما فيهم الفاعلين العنيفين والأفراد وذلك بعد أن كانت الدولة هي المحتكر الوحيد للقوة مما جعل قدرة الدولة على الهيمنة في هذا المجال موضع شك لاسيما مع زيادة تأثير الفاعلين غير الدوليين على المستوى السياسي الداخلي والدولي وتستخدم الدول الفضاء الالكتروني لاعتبارات الامن والقوة العسكرية بشكل جعل عديدًا من الدول تدخل الفضاء الالكتروني ضمن حسابتها الاستراتيجية و أمنها القومي[٢٢]

فالقوة السيبرانية هي القدرة على استخدام الفضاء الإلكتروني لخلق مزايا والتأثير على الأحداث في بيئات التشغيل الأخرى وعبر أدوات السلطة لذا يجب أن تركز مناقشات القوة السيبرانية على التكامل العميق والمعقد للتكنولوجيا الإلكترونية عبر الأنظمة العامة والخاصة وعبر القطاعات من وسائل الإعلام والاقتصاد إلى الدفاع وفي جميع الوظائف الاجتماعية الرئيسة. [٢٣]

اذاً للأمن السيبراني اثره في قوة الدولة من خلال ظهور شكل جديد للقوة وهو القوة الافتراضية والتي تعرف "القدرة على الحصول على النتائج المرجوة من خلال مصادر المعلومات المرتبطة إلكترونياً بالميدان المعلوماتي"عبر أدوات القوة المختلفة، سواء كانت عسكرية أو اقتصادية أو دبلوماسية أو معلوماتية ، وأيضاً تعدد شكل علاقات القوى فأصبح ما تسمى علاقات القوى الافتراضية، كما تعدد الفاعلون وقوتهم النسبية، وظهر ثلاثة أنواع من الفاعلين الذين يمتلكون القوة الإلكترونية .يتمثل النوع الاول في الدولة، والنوع الثاني في الفاعلين من غير الدول، والنوع الثالث يتمثل في الأفراد وقد ظهرت أنماطًا لاستخدام موارد القوة الافتراضية، وميز بين الاستخدام الناعم لها والاستخدام الصلب. [٢٤]

في العالم الافتراضي يكون الفاعلون متنوعين مجهولين في بعض الأحيان والمسافة غير مادية و جريمة افتراضية واحدة تكاد تكون خالية من التكلفة والدفاع قد لا يبقى كما هو الحال على المدى الطويل مع تطور التكنولوجيا بما في ذلك الجهود الرامية إلى إعادة هندسة بعض الأنظمة لمزيد من الأمان لكنها تظل كذلك في هذه المرحلة ويتمتع من يمتلك القوة الأكبر بقدرة محدودة على نزع سلاح العدو أو تدميره أو احتلال الأراضي أو استخدام استراتيجيات القوة المضادة بفعالية فإن الردع ممكن لكنه يختلف بسبب مشاكل إسناد مصدر الهجوم. [٢٥] .

المبحث الثالث : الاثر العسكري للأمن السيبراني في الجغرافيا السياسية للدولة

يأتي تأثير الامن السيبراني في بعده العسكري على الجغرافيا السياسية للدولة من خلال التطرق للحرب السيبرانية ، فالحروب المعلوماتية قديمة قدم النزاع البشري وظلت الدوافع الكامنة وراء هذه الحروب على حالها عموماً وتشمل هذه الدوافع السعي لتقويض ثقة الخصم وتعطيل خطوط اتصالاته وإرباكها وخلق الأوهام في نفسه بشأن طبيعة النزاع ومسرحه ولم تزل مثل هذه الدوافع قائمة في عالم اليوم أما مستجد في القرن الحادي والعشرين الذي شاعت فيها البنى التحتية المعلوماتية الإلكترونية بصلاتها الرقمية ذات النطاق الواسع أكثر فأكثر الآتي: [٢٦]

أ) شراسة الهجمات المعلوماتية التي يمكن أن تمزق النسيج الاجتماعي للبلد المستهدف . ب) القدرة البالغة على إلحاق أضرار مادية واسعة.

ج) الطاقات والقدرات الوبائية للهجمات المعلوماتية المتواصلة والمتاحة للجهات الفاعلة غير الحكومية القادرة على المشاركة في الحروب غير المتناظرة.

د) نشوء حالة متفشية من النزاع الدائم منخفض المستوى، وهو ما يمكن أن يُطلق عليه اسم الحرب الباردة السيبرانية او النزاع السيبراني[٢٧]

وأدى الاستخدام المكثف لتكنولوجيا المعلومات الجديدة إلى تعزيز القدرات القتالية للأسلحة التقليدية والتكنولوجيات العسكرية الأخرى ولهذا السبب فإن العسكريين ينظرون إلى تكنولوجيا المعلومات والاتصالات على أنها سلاح وهدف في آن واحد ففي المجال العسكري ، تقع العمليات التي تتم للحصول على تفوق المعلومات في نطاق حرب المعلومات ففي هذا النطاق تُشن عمليات المعلومات الهجومية والدفاعية عن طريق التدخل المسلح ، والحرب الإلكترونية وما إلى ذلك [٢٨]

وتنقسم حرب المعلومات إلى:

الحرب الإلكترونية التقليدية و القرصنة الإلكترونية وحرب المعلومات الاقتصادية

اما العمليات العسكرية في الفضاء الإلكتروني تنقسم إلى أربع مستويات:

جمع المعلومات الاستخباراتية وعمليات تستهدف المعنويات "الحرب النفسية" وعمليات هجومية وعمليات دفاعية . [٢٩]

اذاً مفهوم الحرب السيبرانية :قيام دولة أو فواعل من غير الدول بشن هجوم إلكتروني في إطار متبادل أو من قبل طرف واحد ، فوفقاً للمفهوم التقليدي للحرب فإنها تنطوي على استخدام الجيوش النظامية ويسبقها إعلان واضح لحالة الحرب وميدان قتال محدد ، بينما تبدو هجمات الفضاء الإلكتروني غير محددة المجال وغامضة الأهداف كونها تتحرك عبر شبكات المعلومات والاتصالات المتعدية للحدود الدولية فضلاً عن اعتمادها على أسلحة إلكترونية جديدة تلائم طبيعة السياق التكنولوجي لعصر المعلومات أذ يتم توجيهها ضد المنشآت الحيوية أو دسها عن طريق عملاء لأجهزة الاستخبارات. [٣٠]

كما تتميز الحروب السيبرانية بعدم الاعتراف بها على مستوى الحكومة وان الحكومات غير راغبة في الاعتراف بهذا الواقع علانية خشية ان يتطلب الاعتراف الانتقام والخوف ويمكن ان تتصاعد الى حرب حركية ويمكن ان نلخص اهم مزايا الحرب السيبرانية بما يلي : [٣١]

١- الاسناد : أي عدم القدرة على اسناد المشكلة في دولة اذ يمكن للمهاجمين اختراق الخوادم في أي جزء من العالم ويمكنهم تحديد انشطتهم في أي منطقة جغرافية ويمكن ان يكتبوا باي لغة .

٢- الانكار : عندما يكون من المستحيل اثبات الجاني علنا يكون من السهل على المشتبه ان ينكر ، ففي اعقاب النفي المتكرر للانخراط في خروقات الانتخابات الامريكية لعام ٢٠١٦ اقترح فلاديمير بوتين في النهاية انه كان من المكن ان يكونوا قراصنة روسيين لكن اوكد انه ليس له علاقة بالحكومة الروسية وهذا يفسر (انت تعلم اننا فعلناها لكنك لا تستطيع اثبات ذلك وهذا هو الانكار .

٣- التصعيد : من خلال الادعائيات والاخبار المزيفة والتشويش وغيرها .

وتعد الحروب السيبرانية ساحة المعركة الخامسة نوع جديد من الحروب بحاجة إلى مزيد من التعريف بالنسبة للآخرين ، إنه مجرد سلاح جديد يمكن دمجه في الصراع التقليدي فالحرب السيبرانية" يمكن أن تُفهم بصورة واسعة على أنها حرب تجري في الفضاء السيبراني باستعمال واستهداف تكنولوجيا المعلومات والاتصالات والاعتماد المتزايد بسرعة على الشبكات الذكية وغيرها من أنظمة المراقبة والرصد عن طريق الإنترنت تضع مركز موارد الطاقة والنقل والدفاع في متناول هؤلاء الذين يسعون إلى إحداث الفوضى في الحكومة وبين السكان المدنيين . [٣٢]

ويمكن تقسيم الهجمات السيبرانية إلى أربع فئات هي:

الإرهاب الإلكتروني والحرب السيبرانية والجريمة السيبرانية والتجسس الإلكتروني فضلاً عن أن كل مجموعة إرهابية لها وجود على شبكة الإنترنت إلا أن الإرهاب السيبراني الحقيقي لا يزال نادراً ولم تكن هناك حرب سيبرانية حقيقية ويعتقد أن المشاكل الأكثر إلحاحًا هي الجريمة السيبرانية والتجسس الإلكتروني فضلاً عن أي شكل من أشكال الهجوم السيبراني هو نوع من التسلل عبر الإنترنت ولا ينبغي التقليل من خطر التطفّل السيبراني [٣٣]

لذا يمكن اثبات تأثير الامن السيبراني في بعده العسكري على الجغرافيا السياسية ،هو السبب الرئيس للحرب السيبرانية هو عدم الثقة السياسية الدولية مع تصاعد هذا الامر تزداد الحوادث الالكترونية الدولية وكمثال على ارتفاع عدم الثقة السياسية التوترات بين الصين والولايات المتحدة الامريكية وكذلك الحرب على الارهاب وظهور ايران في الفضاء السيبراني.

المبحث الثالث :قياس القوة السيبرانية العسكرية

اعتمدت الدول القومية على امتلاك أفضل فهم ممكن لقدرات الأعداء المحتملين على إبراز القوة لاسيما في المجال العسكري الذي يُنظر إليه دائمًا كأداة حيوية في فن الحكم أذ كان الاتجاه السائد بالنسبة للدول هو الحفاظ على سرية هذه القدرات ولا يزال ذلك أمرًا ضروريًا لكن التجربة التاريخية الحديثة لا سيما الحرب الباردة أدت إلى ظهور ثقافة الردع الاستراتيجية القائمة على الوعي المتبادل بالقدرات[٣٤]

أدى تطور المجال السيبراني إلى تعقيد هذه الصورة بشكل كبير ، ليس فقط من حيث كيفية تبني القوات المسلحة للتكنولوجيا الجديدة والتكييف معها ، وإثارة أسئلة حول ما يشكله الاستخدام العسكري في مجال يكون فيه المستخدمون المدنيون والعسكريون متشابكاً بشكل لا ينفصم ، لذا اتبعت الدول مقاربات تنظيمية مختلفة إما عن طريق إنشاء فرع منفصل من قواتها المسلحة كما في حالة قوة الدعم الاستراتيجي في الصين أو عن طريق توزيع القدرات عبر أسلحة الخدمة المختلفة كما هو الحال مع القيادة السيبرانية للولايات المتحدةالامريكية.

السؤال هنا كيف يمكن للمرء قياس القوة السيبرانية؟ فضلاً عن وجود العديد من الطرق الثابتة لقياس القوة ، إلا أنه لا يمكن تطبيق أي من هذه الطرق بشكل مرض على المجال السيبراني وقد استمرت المقاييس التقليدية للقوة العسكرية : الناتج القومي الإجمالي ، والسكان ، والطاقة ، والأرض ، والمعادن في الهيمنة على المناقشات حول ميزان القوى ولا تزال موارد الطاقة هذه مهمة ، وما زالت الولايات المتحدة الامريكية تعتمد عليها وكذلك على المعلومات ، كما يصعب تصنيف قوة المعلومات أيضًا لأنها تشمل

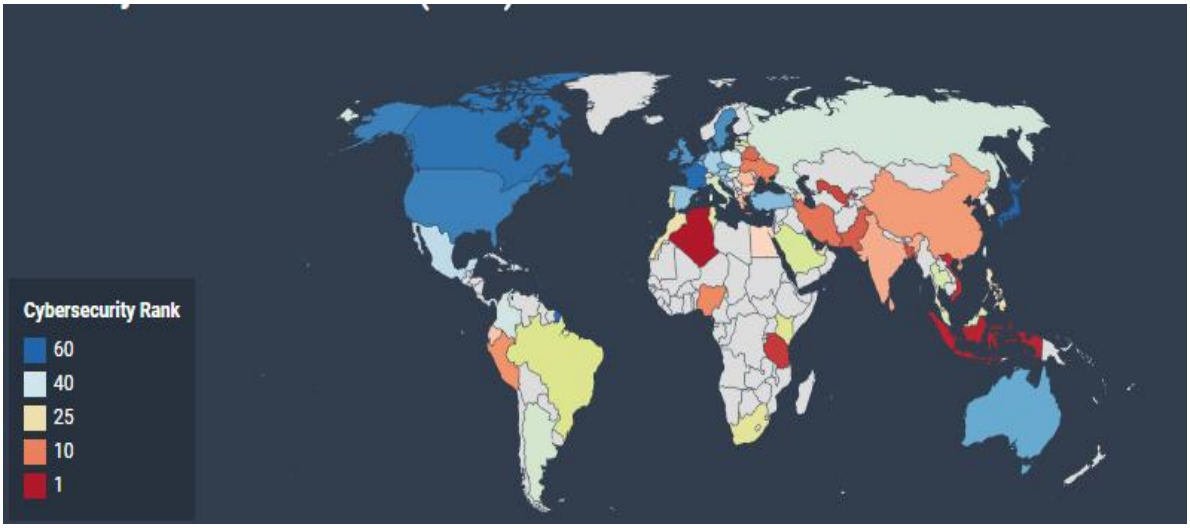
جميع موارد القوة العسكرية والاقتصادية والاجتماعية والسياسية وفي بعض الحالات تقلل من قوتها وفي حالات أخرى تضاعفها .[٣٥]ونحاول تحديد مؤشر الأمن السيبراني العالمي (GCI) هو مرجع موثوق به يقيس التزام البلدان بالأمن السيبراني على المستوى العالمي لرفع مستوى الوعي لأهميته وأبعاده المختلفة لأن للأمن السيبراني مجالًا واسعًا للتطبيق يشمل العديد من الصناعات والقطاعات المختلفة ولاختيار أفضل البلدان استعدادًا لمواجهة الهجمات الإلكترونية هو استخدام مؤشر الأمن السيبراني العالمي يتم تقييم مستوى التنمية أو المشاركة في كل دولة على خمس ركائز (١)التدابير القانونية (٢) التدابير الفنية (٣) التدابير التنظيمية (٤) بناء القدرات (٥) التعاون ، ثم تجميعها في النتيجة الإجمالية كعوامل نجاح رئيسة.[٣٦]وكما يوضحه الجدول (١) والخريطة (١).

جدول (١) الدول العشر الاكثر قدرة على مواجهة التهديدات السيبرانية

الدولة	التدابير القانونية	التدابير الفنية	التدابير التنظيمية	بناء القدرات	التعاون	عوامل النجاح الرئيسة
سنغافورة	0.95	0.96	0.88	0.97	0.87	0.92
الولايات المتحدة الامريكية	1	0.96	0.92	1	0.73	0.91
ماليزيا	0.87	0.96	0.77	1	0.87	0.89
سلطة عمان	0.98	0.82	0.85	0.95	0.75	0.87
استونيا	0.99	0.82	0.85	0.94	0.64	0.84
موريشيوس	0.85	0.96	0.74	0.91	0.70	0.82
استراليا	0.94	0.96	0.86	0.94	0.44	0.82
جورجيا	0.91	0.77	0.82	0.90	0.70	0.81
فرنسا	0.94	0.96	0.60	1	0.61	0.81
كندا	0.94	0.93	0.71	0.82	0.70	0.81

الاتحاد الدولي للاتصالات ، مؤشر الامن السيبراني العالمي ، ٢٠١٧ ، ص١٧.

خريطة (١) الدول الاكثر مواجهة للخطر السيبراني في العالم



Global Cyber security, Index ,2017 .

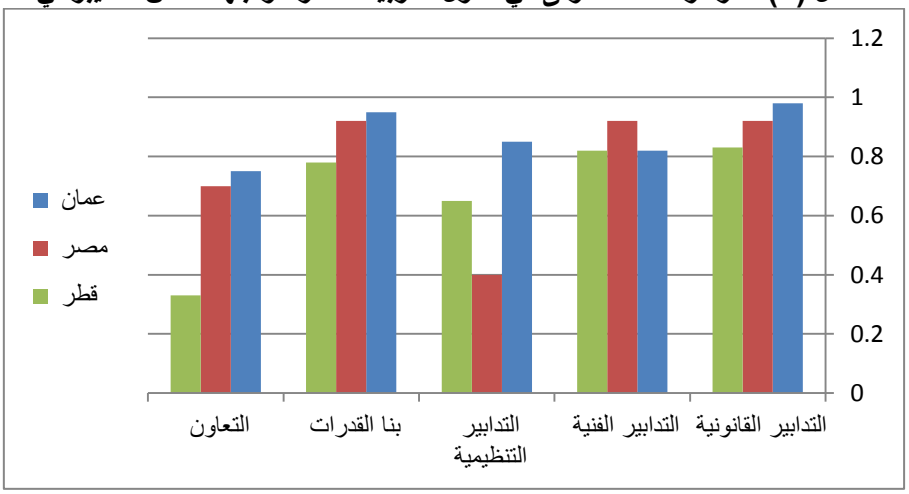
وتم قياس مستوى الامن السيبراني للدول العربية لعام ٢٠١٧ اعتماداً على نفس المؤشر (GCI) وتقييم الدول على أساس الركائز الخمس (التدابير القانونية والتدابير الفنية والتدابير التنظيمية وبناء القدرات والتعاون والنتيجة التي أظهرت عوامل النجاح الرئيسة)كان لدولة عمان المركز الأول عربياً ومصر في المركز الثاني ودولة قطر بالمركز الثالث كما موضح في الجدول (٢) والشكل (١).

جدول(٢) المراكز الثلاث الاولى في الدول العربية الاكثر مواجهة للامن السيبراني

الدولة	التدابير القانونية	التدابير الفنية	التدابير التنظيمية	بناء القدرات	التعاون	عوامل النجاح الرئيسة
عمان	0.98	0.82	0.85	0.95	0.75	0.87
مصر	0.92	0.92	0.4	0.92	0.7	0.77
قطر	0.83	0.82	0.65	0.78	0.33	0.67

الاتحاد الدولي للاتصالات ، مؤشر الامن السيبراني العالمي ، ٢٠١٧ ، ص٢٩.

الشكل (١) المراكز الثلاث الاولى في الدول العربية الاكثر مواجهة للأمن السيبراني



المصدر : بالاعتماد على الجدول (٢)

يوضح الشكل (١) أعلى الدرجات في منطقة الدول العربية بالنسبة إلى الركائز الخمس لـ GCI يُظهر أن سلطنة عمان تحرز أعلى نسبة في بناء القدرات وفي التدابير القانونية والفنية والتنظيمية والتعاون تليها مصر اما في المرتبة الثالثة تاتي قطر [٣٧]

المبحث الرابع /بناء نظرية جيوبولتيكية جديدة (نظرية القوة السيبرانية)

للتشابه القوي بين النظريات الجيوبولتيكية القوة الجوية والبحرية والفضاء الخارجي والفضاء الإلكتروني وتماثل تلك التشبيهات نفسها لمفهوم القوة السيبرانية المستمدة من القوة البرية والقوة البحرية أوالقوة الجوية يمكن وضع نظرية للقوة السيبرانية وذلك من خلال تحليل النظريات السابقة

فقد كتب ماهان على نطاق واسع حول العوامل التي أدت إلى تفوق القوى البحرية وكيف يمكن للحكومة أن تحفز المواقف الوطنية تجاه السلطة في البحار لكنه لم يحدد بوضوح وببساطة ما يعنيه المصطلح اما تعريف القوة البحرية الذي نشر من قبل الأكاديمية البحرية الأمريكية بعد فترة وجيزة من الحرب العالمية الأولى "قدرة أمة على فرض إرادتها على البحر" تأثرت بوضوح بفكر ماهان وأكدت الآثار بدلاً من الوسائل ، فضلاً عن أنها تتجاهل علاقة القوة البحرية بجوانب القوة الأخرى ، مثل القوة الاقتصادية الوطنية . [٣٨] ومن الواضح أنهم لم يكونوا يشيرون إلى التحكم في البحر نفسه ، بل إلى التحكم في الأنشطة البشرية والوطنية في البحر وكيفية استخدام هذه الوسيلة المادية للتأثير على الأحداث والعمليات ولم يحدد دي سيفرسكي، الرجل الأكثر ارتباطًا بمفهوم القوة الجوية ، تعريفًا واضحًا له فضلاً عن أنه أنشأ سيناريوهات تفصيلية لإظهار تأثيره على الحرب المستقبلية.

كما أن بيلي ميتشل ، أحد رواد سلاح الجو الأمريكي لم يحدد المفهوم بالتفصيل ، فضلاً عن تصريحه بأن "القوة الجوية هي القدرة على فعل شيء ما في الجو ومع ذلك فهو يعاني أيضًا من نفس المنظور الضيق الذي يتسم به تعريف ماهان ويتجاهل على سبيل المثال التأثير الاقتصادي الضخم للهيمنة الأمريكية على سوق الطائرات المدنية لسنوات عديدة ولكن جميع هؤلاء الرواد كادوا أن يتفقوا مع نهج يركز على القدرة على استخدام البيئات المادية واستغلالها أو "القدرة على استخدام البحر للاستفادة" أو "القدرة على استخدام الجو لنفس الغرض". (٣٩)

وهذا يؤدي إلى تعريف القوة السيبرانية بأنها " القدرة على استخدام الفضاء الإلكتروني لخلق مزايا والتأثير على الأحداث في جميع البيئات التشغيلية وعبر أدوات السلطةهذا التعريف أوسع من تعريف ماهان او دي سيفرسكي في استخدام القوة البحرية أو القوة الجوية لأنه يتضمن إشارة واضحة إلى أشكال أخرى من القوة وهو المقصود التأكيد على تأثير تآزر القوة الإلكترونية على أشكال وأدوات القوة الأخرى والتكامل معها. (٤٠)

وبعد اجراء تقييم للنظريات الجيوبولتيكية تم التوصل إلى أن نظرية القوة السيبرانية يجب أن تركز على **أربعة عوامل رئيسية: التقدم التكنولوجي وسرعة نطاق العمليات والسيطرة على السمات الرئيسية والتعبئة الوطنية** تماشياً مع كل من هذه الميزات تم رسم الآثار التالية لنظرية القوة السيبرانية فيما يتعلق بالتطورات التكنولوجية لوحظ أن الاعتماد على الفضاء الإلكتروني أدى إلى نقاط ضعف استراتيجية جديدة تم تحسين مشكلة عدم الحصانة هذه بواسطة شبح "cyber Pearl Harbour" وإدراك أن الفضاء الإلكتروني الحالي عرضة لمجموعة متنوعة من الهجمات العدوانية على سبيل المثال هجمات رفض الخدمة والتسلل من المعلومات الحساسة والفساد المحتمل للبيانات الحساسة ونظرًا لانتشار تكنولوجيا الفضاء الإلكتروني المنخفضة التكلفة تعززت سرعة ونطاق العمليات ويتجلى ذلك في السرعة التي يمكن بها إجراء العمليات العالمية على سبيل المثال القدرة على إشراك أهداف حساسة بنجاح في أي مكان في العالم وقد أدى ذلك إلى تحسينات في القدرة والقيادة والتحكم ، مما يقلل بشكل كبير من عملية مراقبة الأزمنة الكلاسيكية ففي النظريات البيئية للسلطة تم التركيز على التحكم في الميزات الرئيسية على سبيل المثال في النظريات البحرية التزام ذلك التحكم في "نقاط الاختناق" الرئيسية (مثل مضيق ملقا) ، بينما كان هناك اهتمام في القوة الفضائية بالتحكم في مواقع المدارات الجيولوجية المتزامنة الرئيسة وفي حالة الفضاء الإلكتروني فإن السمات الرئيسة المثيرة للاهتمام هي من صنع الإنسان. (٤١)

الاستنتاجات

١-اثر الامن السيبراني في الجغرافية السياسية للدولة من خلال ظهور معنى جديد لها وفرض وظيفة جديدة على كل مفاهيمها الامن والسيادة والقوة

٢-أوجد الإنترنت فضاءً عامًا جديدًا بالكامل ، يتجاوز المساحة الجغرافيا المكانية التقليدية

٣-ان الجغرافيا السياسية للدولة لها اهمية خاصة في مواجهة التهديدات المتعلقة بالأمن السيبراني .

٤-تطور مفهوم الأمن القومي تجاه التهديدات الجديدة غير التقليدية واتسع مجاله ليمتد من الجانب العسكري لمجالات أخرى عديدة أذ أن أجهزة الحكومة الإلكترونية للعالم فى فضاء مفتوح ولعدم وجود حدود جغرافية لذا اصبحت أجهزتها عرضة للعديد من الاخطار تحت دوافع مختلفة.

٥-للأمن السيبراني اثره في قوة الدولة من خلال ظهور شكل جديد للقوة وهو القوة الافتراضية والتي تعرف القدرة على الحصول على النتائج المرجوة من خلال مصادر المعلومات المرتبطة إلكترونياً بالميدان المعلوماتي.

٦-تتميز الحروب السيبرانية في عدم الاعتراف بها على مستوى الحكومة وان الحكومات غير راغبة في الاعتراف بهذا الواقع علانية خشية ان يتطلب الاعتراف الانتقام والخوف ويمكن ان تتصاعد الى حرب حركية.

٧-تعد الحروب السيبرانية ساحة المعركة الخامسة – نوع جديد من الحروب بحاجة إلى مزيد من التعريف بالنسبة للآخرين إنه مجرد سلاح جديد يمكن دمجه في الصراع التقليدي.

٨-يمكن اثبات تأثير الامن السيبراني في بعده العسكري على الجغرافيا السياسية هو ان السبب الرئيس للحرب السيبرانية هو عدم الثقة السياسية الدولية مع تصاعد هذا الامر تزداد الحوادث الالكترونية الدولية.

التوصيات

أدخلت التطورات التكنولوجية للمعلومات الجغرافيا السياسية في حقبة جديدة مما فرض على الدول تغيير كيفية تفاعلها مع مواطنيها ومع الدول الاخرى وتحديد مصالحهم الوطنية وأولوياتهم الاستراتيجية لذا من المهم أن يكون لدى الدول قوانين وأنظمة مناسبة للجرائم الإلكترونية من اجل :

١-حماية سرية وسلامة وتوافر البيانات والشبكات الخاصة بما في ذلك البنية التحتية المهمة.

٢-حماية سلامة الحكومة وسمعة البلد.

٣-تساعد على منع بلد من أن يصبح ملاذاً للجهات الفاعلة السيئة بما في ذلك الأعمال الإرهابية التي تستخدم أو تهاجم أنظمة تكنولوجيا المعلومات.

٤-تساعد في منع أي بلد من أن يصبح مستودعًا للبيانات الجنائية الإلكترونية.

٥-توفر الحماية للمعلومات السرية وبيانات العدالة الجنائية والمعلومات الشخصية والبيانات العامة المحمية.

٦-حماية المستهلكين ومساعدة إنفاذ القانون وجمع المعلومات الاستخباراتية.

٧-تردع الفساد.

٨-تزيد من الأمن القومي وتقلل من مواطن الضعف لدى الإرهابيين وغيرهم من الجهات المارقة.

الهوامش

(1) Lene Hansen- Helen Nissenbaum, Digital Disaster, Cyber Security, and the Copenhagen School, International Studies Quarterly (2009) 53, 1155–1175

(٢) نسرين الشحات الصباحى على –الأبعاد العسكرية للقوة السيبرانية على الأمن القومى للدول دراسة حالة " إسرائيل منذ عام ٢٠١٠ "المركز الديمقراطي العربي، ٢٩ ابريل ٢٠١٦

(٣) منى الأشقر جبور، الأمن السيبراني: التحديات ومستلزمات المواجهة، **المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية ،اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني، بيروت ٢٧ ــ ٢٨ أغسطس (آب) ٢٠١٢،ص٣.**

(٤) عادل عبد الصادق ، " الفضاء الإلكترونى والرأي العام : تغير المجتمع والأدوات والتأثير " ، المركز العربي لأبحاث الفضاء الإلكترونى : قضايا استراتيجية ، العدد ٢٤٥٩ ، (٢٠١٣)

(5)Aleksandar KLAIC, A Method for the Development of Cyber Security Strategies, Information & Security: An International Journal, I&S Volume 34, (2015) ,p86.

(٦) ايهاب خليفة ،القوة الالكترونية كيف يمكن ان تدير الدول شؤنها في عصر الانترنيت ،مطبعة العربي ، القاهرة ، ٢٠١٧

(7) RON DEIBER ,The Geopolitics of Cyberspace After Snowden , Current History,15 January 2015

(٨) ايهاب خليفة ،القوة الالكترونية كيف يمكن ان تدير الدول شؤنها في عصر الانترنيت،المصدرالسابق،ص٢٤.

(9) Ryszard Zi□ba, Wspó□czesne wyzwania i zagro□enia dla bezpiecze□stwa mi□dzynarodowego, Stosunki Mi□dzynarodowe – International Relations, nr 3 (t. 52) 2016,p19

(١٠) ايهاب خليفة ، القوة الالكترونية وابعاد التحول في خصائص القوة ، مطبعة الاسكندرية ، ٢٠١٤،ص٢٣.

(١١)ربيع محمد يحيى، إسرائيل وخطوات الهيمنة على ساحة الفضاء السيبراني في الشرق الأوسط دراسة حول استعدادات ومحاور عمل الدولة العبرية في عصر الإنترنت (٢٠٠٢ – ٢٠١٣)، روى استراتيجية يونيو ٢٠١٣ ،ص٧٥

(١٢) ايهاب خليفة ،القوة الالكترونية كيف يمكن ان تدير الدول شؤنها في عصر الانترنيت ،المصدر السابق،ص٢٨.

(13)WANG Limao, M. Changes in driving forces of geopolitical evolution and the new trends in geopolitics studies[J]. Geographical Research, 2016 , 35 (1): 3-13.

(14)Michael Sentonas, Cybercrime, the new tool in geopolitics VP Technology Strategy at Crowd Strike, Michael Sentonas (CSO Online) on 01 February, 2018 16:50

(15).Michael Sentonas, Cybercrime, the new tool in geopolitics VP Technology Strategy at Crowd Strike,opcit.

(16)John B. Sheldon, Geopolitics and Cyber Power: Why Geography Still Matters, The Journal of the National Committee on American Foreign Policy, Volume 36, Issue 5-2014.p290

(17)Irene Poetranto, The Geopolitics of Cyberspace After Snowden, Current History, January 2015.

(18)Irene Poetranto, The Geopolitics of Cyberspace After Snowden, op.cit,p4.

(19)Iulian F. Popa, CYBER GEOPOLITICS AND SOVEREIGNTY. AN INTRODUCTORY OVERVIEW ,Conference Paper, Conference: 5th International scientific conference „National and International Security", At Armed Forces Academy of Genera

(20) Ryszard Zi□ba, Wspó□czesne wyzwania i zagro□enia dla bezpiecze□stwa mi□dzynarodowego, Stosunki Mi□dzynarodowe – International Relations, nr 3 (t. 52) 2016.

(٢١)نسرين الشحات الصباحى على –،الأبعاد العسكرية للقوة السيبرانية على الأمن القومى للدول دراسة حالة " إسرائيل منذ عام ٢٠١٠ "، المصدر السابق،ص٤.

(22) Joseph S. Nye, Jr. Cyber Power, Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010.

(23) Joseph S. Nye, Jr. Cyber Power, ibd,p.

(24)Nye, Soft Power: The Means To Success In World Politics(New York: Public Affairs, 2004)

(25)Franklin D. Kramer, Stuart H. Starr, Larry K. Wentz, Cyber power and National Security, National Defense University Press,2009.p180

(26)https://www.vifindia.org/.../07/dimensions-of-cyber-security-in-india Lt Gen Gautam Banerjee, February 7,2014

(٢٧) جانكارلو أ. بارليتا، ووليام أ. بارليتا، وفيتالي تسيجيشكو، النزاع السيبراني والاستقرار الجيوسيبراني ،البحث عن السلام السيبراني ،الاتحاد الدولي للاتصلات ،٢٠١١،ص٤٩ .

(٢٨) حمدون إ. توريه، البحث عن السلام السيبراني ،الاتحاد الدولي للاتصالات ،٢٠١١،ص٤٨.

(٢٩) الحروب المستقبلية فى القرن الحادي والعشرين ، (تصوير : أحمد ياسين) ، (مركز الامارات للبحوث الاستراتيجية)،ط١ ،٢٠١٤،ص٥٧.

(30) Robert Mandel, Global Security Upheaval: Armed Non-State Groups Usurping State Stability ,Functions,(California: Stanford University Press, 2013)

(31)Simon Dalby, Critical Geopolitics and Security , Carlton university-novembr 3rd 2008.

(32)Mohan B. Gazula, Cyber Warfare Conflict Analysis and Case Studies, M.S., Computer Science, Boston University, June 2017,p13.

(٣٣) الحروب المستقبلية فى القرن الحادي والعشرين ، (تصوير : أحمد ياسين)، المصدر السابق ، ص62.

(34)Nigel Inkster, Measuring Military Cyber Power, Global Politics and, Strategy Volume 59,Issue 4-2017, p30.

(35)Jelle van Haaster, Assessing Cyber Power, 2016 8th International Conference on Cyber Conflict Cyber Power, NATO CCD COE Publications.

(36)Global Cybersecurity Index 2018, report, International Telecommunication Union

(37) Global Cyber security Index 2017, report, International Telecommunication Union

(38)Stuart H. STARR., Towards an Evolving Theory of Cyber power, a Center for Technology and National Security Policy (CTNSP) National Defense University (NDU), Cryptology and Information Security Series, Volume 3: The Virtual Battlefield: Perspectives on Cyber Warfare,2009

(39)Sean Charles Gaines Kern, Expanding Combat Power Through Military Cyber Power Theory, Center for 21st Century Security and Intelligence, in Washington, DC, June 2013

(40)K R I S E . B A R C O M B, From Sea Power to Cyber Power Learning from the Past to Craft a Strategy for the Future, JFQ / issue 69, 2nd quarter 2013.

(41)Sean Charles Gaines Kern, Expanding Combat Power Through Military Cyber Power Theory,opcit.

المصادر العربية:

١- ايهاب خليفة ،القوة الالكترونية كيف يمكن ان تدير الدول شؤنها في عصر الانترنيت ،مطبعة العربي ، القاهرة ،٢٠١٧.

٢- ايهاب خليفة ، القوة الالكترونية وابعاد التحول في خصائص القوة ، مطبعة الاسكندرية ، ٢٠١٤ .

٣-جانكارلو أ. باراليتا، ووليام أ. باراليتا، وفيتالي تسيجيشكو، النزاع السيبراني والاستقرار الجيوسيبراني،البحث عن السلام السيبراني ،الاتحاد الدولي للاتصلات ،٢٠١١ .

٤-حمدون إ. توريه، البحث عن السلام السيبراني ،الاتحاد الدولي للاتصالات ،٢٠١١.

٥-الحروب المستقبلية فى القرن الحادي والعشرين ، (تصوير : أحمد ياسين) ، (مركز الامارات للبحوث الاستراتيجية)،ط١ ،٢٠١٤.

٦-ربيع محمد يحيى، إسرائيل وخطوات الهيمنة على ساحة الفضاء السيبراني في الشرق الأوسط دراسة حول استعدادات ومحاور عمل الدولة العبرية في عصر الإنترنت (٢٠٠٢ – ٢٠١٣)، روى استراتيجية يونيو ٢٠١٣.

٧-عادل عبد الصادق ، " الفضاء الإلكترونى والرأي العام : تغير المجتمع والأدوات والتأثير " ، المركز العربي لأبحاث الفضاء الإلكترونى : قضايا استراتيجية ، العدد ٢٤٥٩ ، (٢٠١٣)

٨- منى الأشقر جبور، الأمن السيبراني: التحديات ومستلزمات المواجهة، المركز العربي للبحوث القانونية والقضائية،جامعة الدول العربية ،اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني، بيروت ٢٧ – ٢٨ أغسطس (آب) ٢٠١٢.

٩- نسرين الشحات الصباحى على –الأبعاد العسكرية للقوة السيبرانية على الأمن القومى للدول دراسة حالة " إسرائيل منذ عام ٢٠١٠ "المركز الديمقراطي العربي، ٢٩ ابريل ٢٠١٦

English Reference

1-Aleksandar KLAIC, A Method for the Development of Cyber Security Strategies, Information & Security: An International Journal, I&S Volume 34, (2015) .

2-Franklin D. Kramer, Stuart H. Starr, Larry K. Wentz, Cyber power and National Security, National Defense University Press,2009.

3-Global Cybersecurity Index 2018, report, International Telecommunication Union

4-Global Cyber security Index 2017, report, International Telecommunication Union

5-Joseph S. Nye, Jr. Cyber Power, Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010.

6-John B. Sheldon, Geopolitics and Cyber Power: Why Geography Still Matters, The Journal of the National Committee on American Foreign Policy, Volume 36, Issue 5-2014.p290.

7-K R I S E . B A R C O M B, From Sea Power to Cyber Power Learning from the Past to Craft a Strategy for the Future, JFQ / issue 69, 2nd quarter 2013.

8-Lena Hansen- Helen Nissenbaum, Digital Disaster, Cyber Security, and the Copenhagen School, International Studies Quarterly (2009).

9-Irene Poetranto, The Geopolitics of Cyberspace After Snowden, Current History, January 2015.

10-Iulian F. Popa, CYBER GEOPOLITICS AND SOVEREIGNTY. AN INTRODUCTORY OVERVIEW ,Conference Paper, Conference: 5th International scientific conference „National and International Security", At Armed Forces Academy of Genera.

11-Michael Sentonas, Cybercrime, the new tool in geopolitics VP Technology Strategy at Crowd Strike, Michael Sentonas (CSO Online) on 01 February, 2018 16:50

12-Mohan B. Gazula, Cyber Warfare Conflict Analysis and Case Studies, M.S., Computer Science, Boston University, June 2017.

13-Nye, Soft Power: The Means To Success In World Politics(New York: Public Affairs, 2004).

13-Robert Mandel, Global Security Upheaval: Armed Non-State Groups Usurping State Stability ,Functions,(California: Stanford University Press, 2013.

14-Ryszard Zi□ba, Wspó□czesne wyzwania i zagro□enia dla bezpiecze□stwa mi□dzynarodowego, Stosunki Mi□dzynarodowe – International Relations, nr 3 (t. 52) 2016.

15-Sean Charles Gaines Kern, Expanding Combat Power Through Military Cyber Power Theory, Center for 21st Century Security and Intelligence, in Washington, DC, June 2013.

16-Simon Dalby, Critical Geopolitics and Security , Carlton university-novembr 3rd 2008.

17-Stuart H. STARR., Towards an Evolving Theory of Cyber power, a Center for Technology and National Security Policy (CTNSP) National Defense University (NDU), Cryptology and Information Security Series, Volume 3: The Virtual Battlefield: Perspectives on Cyber Warfare,2009

18-WANG Limao, M. Changes in driving forces of geopolitical evolution and the new trends in geopolitics studies[J]. Geographical Research, 2016.

19-https://www.vifindia.org/.../07/dimensions-of-cyber-security-in-india Lt Gen Gautam Banerjee, February 7,2014

Abstract

The research aims to identify the military impact of cybersecurity on the political geographyl state of the being A recent topic related to political geography concepts such as state, sovereignty, power, war and security has been the research section of several topics, The first dealt with concepts pertaining to cyber security, cyberspace and related issues, especially the military dimension ,The second topic analyzed the relationship between cyber security and political geography with the analysis of each political geography element separately, such as the state, power and national security, in line with the objective of the research ,The third topic was on the military impact of cyber security, which dealt with the concept of cyber warfare, The last topic was the construction of a new political geography theory by analyzing the old land, sea and air theories and concluding the research with conclusions and recommendations.

Keywords: cyber security – military impact- political geography- state – power – sovereignt