الفضاء السيبراني ما بين تحول القوة والصراع والأمن القومي للدول

دكتوره

الشيماء فؤاد الدروزي

لعام 2024م

خطة البحث تتكون من :

- المقدمة
- المبحـــث الاول : الفضاء السيبرانى وتحولات القوة
- المبحث الثانـــي : الفواعل في مجال القوة السيبرانية
- المبحث الثالـــث : الصراع السيبرانى
- المبحث الرابـــع : الأمن السيبرانى وأبعاده
- المبحث الخامس : انماط التهديدات السيبرانية
- المبحث السادس : علاقة الأمن السيبرانى بالأمن القومى
- الخاتمة
- الهوامش

الملخص

كانت ثورة المعلومات وظهور الانترنت إيذانا ببزوغ العصر السيبيري ، وخلق بيئة جديدة هي القضاء السبيرانى (Cyber space) – إضافة إلى الأرض والبحر والجو والفضاء . الذى أصبح يؤثر في النظام الدولي ، خاصة مع بروز شكل جديد من القوة هي القوة السيبرانية (Cyberpower) . التي توزعت وانتشرت بين عدد أكبر من الفاعلين على المستوى الدولي والمحلى ، ما جعل الفضاء السيبرانى مجالاً جديداً للصراع بين الدول ، وبالتالي حاولت من خلال هذه الورقة البحثية إظهار الانعكاسات التي احدثها الفضاء السيبرانى على التحولات في مفهوم القوة والصراع ، من خلال التحول من الصراع المادي إلى الصراع الافتراضي ، وهو ما أدى باهتمام الدول إلى أمننة الفضاء السيبراني .

الكلمات المفتاحية : الفضاء السيبرانى ، القوة السيبرانى ، التهديدات السيبرانى ، الأمن السيبرانى

Abstract:

Globalization with the development of the internet mentioned the emergence of the Siberian era and leads to the creation of a new environment, Siberian space in addition to the land, sea, air and space, which became influential in the international system especially with the emergence of a new form of power, the

Siberian power that was distributed and spread among a larger number of international and domestic actors have made Siberian space a new area of conflict between States. Thus, this paper attempts to show the implications of space on the changes in the concept of power and conflict through the transition from physical conflict to virtual conflict, which led to the attention of States to

the security of Cyberspace keywords Siberian space Siberian power Siberian threats Siberian security.

Keys words: cyber space; cyber power; cyber threats; cyber security.

مقدمة:

لقد أحدثت تكنولوجيا المعلومات والاتصالات ثورة شاملة في جميع نواحي الحياة ، إذ تزداد المخاطر السيبرانية في غالب الأحيان كلما ذادت هيمنة تكنولوجيا المعلومات والاتصالات على النسق العام للحياة ، فأصبحنا امام جرائم حقيقية ومتكاملة الأركان تتم عن طريق شبكات الانترنت ، أجهزة الحاسوب وشبكة الانترنت بأشكال كثيرة ، كسرقة الأموال ، النصب والاحتيال ، التخطيط لعمليات إرهابية ، ترويج الأخبار الكاذبة ، وكذلك القرصنة باعتبارها الجريمة الأكثر شيوعاً في العالم الرقمى .

وفى هذا السياق فإن البحث في قضايا التهديدات السيبرانية والتحديات الأمنية يقتضى الغوص في حيثيات العصر الرقمى الجديد وتوصيف بيئة هذه التحديات، حيث إن شبكة الانترنت تتوفر على 30 ترليون موقع الكترونى .

مع انتشار واسع للابتكارات بالشبكة العنكبوتية . ففى تقرير صدر أخيراً عن مؤسسة " سيسكو" سنة 2015. يتبين أن أكثر من 40 مليار جهاز سوف يتحول على الانترنت متمثلة في سيارات ذكية وأجهزة منزلية رقمية ، وبالتالي الإشكالية التي نحاول معالجتها من خلال هذا البحث

هي مدي تأثير الفضاء السيبرانى على التحول في مفاهيم ومضامين القوى والصراع ؟.

اهمية البحث :

للأهمية الكبيرة التي باتت تتمتع بها الانشطة التي تتم من خلال الفضاء السيبراني صار لزاماً علينا معرفة طبيعة هذا الفضاء من خلال الوقوف علي مفهومه وبيان حقيقته كما تتجلي اهمية البحث في وجوب اعادة الحياة للدراسات التي تعني بتحرير المصطلحات وضبط حدودها ليتسني للجهات المعنية التاطي معها علي الوحه المناسب بعد التعرف علي مفهومها بدقة والذي يجب ان يكون موافقاً للواقع علي ماهو عليه فالفضاء السيبراني وامنه من المصطلحات الحديثة التي تحتاج الي مزيد من الدراسات التي تعني به بيانا وتأصيلاً وتمهيداً لوضع النظريات التي يتمن من خلالها مواجهة التحديات التي تطرح في هذه البيئة التواصلية .

اشكالية البحث :

اصبح الفضاء السيبراني اليوم العمود الفقري لمعظم التفاعلات الدولية لسلاسة الاستخدام وانخفاض التكلفة وسهولة الاتصال وهشاشة التنظيمات والقدرات الرقابية مع تزايد اعتماد الدول والحكومات لتبني الحكومة الذكية الامر الذي ادي الي توفير بيئة مناسبة للفاعلين الدوليين من استغلال الفضاء.

فرضية البحث :

دخلت حروب الفضاء السيبراني بقوة في معادلات الصراع والمواجهة بين الدول الكبري حيث وظفت من اجل استخدام القوة في السياسة الدولية والشئون العالمية وتوزيعها بين القوي الكبري ، لذا فان الحروب السيبرانية مجال لاستعراض القوة وممارسة النفوذ وتحقيق التفوق والتنافس .

المنهج :

تعد هذه الدراسة دراسة وصفية تخليلية تعتمد علي منهج التحليل الوصفي والتحليل الثانوية لركائز وممارسات الامن او الفضاء السيبراني خلال الاعوام السابقة مع تطور قواعده وبياناته حتي الان من هنا يمكن صياغة المشكلة البحثية في سؤال رئيسي مفاده :

ما مستوي وطبيعة استغلال الدول وغيرها للفضاء السيبراني في اطار الحروب الغير تقليدية ؟

وبالتالي ينبثق منه عدة تساؤلات هامة محل الدراسة من التحول في مفاهيم القوة والصراع للفضاء السيبراني وخطورته علي الامن القومي للدول وما يحدث من تفاعلات سيبرانية من هجوم ودفاع وردع ، ولماذا يضل الفاعلون الدوليون الفضاء السيبراني عن غيره من مساحات الحروب ؟ مع عرض نموذجين للفضاء السيبراني وهما الارهاب السيبراني و القوة السيبرانية .

المبحث الأول

الفضاء السيبرانى وتحولات القوة

يعتبر الفضاء السيبرانى أحد الأشكال الجديدة لمفهوم القوة والتعبير عن مفرداتها بما يمكن المقتدر فيه من استخدامه بطريقة تضمن مصالحه وامنه القومي . ونتيجة هذه الاستخدامات وتحول الانترنت إلى بنية أساسية عالمية للنشاطات المدنية وإلى وسيلة جديدة للضغط السياسي والتجسس بالإضافة إلى تأثير الفضاء السيبراني على الأمن القومى فى كل مجالاته، كما برز دور الفضاء السيبراني عبر مواقع التواصل الاجتماعي في ادارة الصراع السياسي في الدول العربية وظهر تفاوت في استخدام الفضاء السيبرانى وفق طبيعية التطور التقني وقدرة النظام على إدارة الصراع الإعلامى والتأثير فى الرأى العام فضلاً عن أن مواقع التواصل الاجتماعي كانت وسيلة جيدة للجماعات الإرهابية من أجل تجنيد أعضاء جدد وجمع التمويل ونشر آرائهم المتطرفة وتنفيذ عملياتهم في المنطقة العربية.

وفي غمار هذا القول برزت القوة بمجال الفضاء السيبرانى مما أدى إلى اهمية معرفة مفهوم هذا الفضاء الإلكتروني أو السيبراني كمطلب أول ومعرفة التحولات بين مضامين القوة وظهور القوة السيبرانية كمطلب ثاني بهذا المبحث.

المطلب الاول

مفهوم الفضاء السيبرانى

الفضاء السيبرانى مجال افتراضي من صنع الإنسان يعتمد على نظم الكمبيوتر وشبكات الانترنت وكم هائل من البيانات والمعلومات والأجهزة. كما أن هناك من عرف الفضاء السيبرانى بوصفه الذراع الرابعة للجيوش الحديثة[1]. وهناك من يرى أنه البعد الخامس للحرب. وهذا التعريف يحصر الفضاء السيبرانى في المجال العسكري فقط دون التطرق للمجالات الأخرى .

كما عرفته الوكالة الفرنسية لأمن انظمة الإعلام (ANSSI) على أنه: فضاء التواصل المشكل من خلال الربط البيئي العالمي لمعدات المعالجة الآلية للمعطيات الرقمية [2]. وهذا التعريف يركز على الجانب التقني كما يغفل العامل البشرى، والذى يعد جزءاً اساسياً في فهم الفضاء السيبرانى.

كما يمكن الاعتماد على تعريف الاتحاد الدولي للاتصالات الذى يصف الفضاء السيبرانى بأنه " المجال المادي وغير المادي الذى يتكون وينتج عن عناصر هي : أجهزة الكمبيوتر، الشبكات، البرمجيات، حوسبة المعلومات، المحتوى، معطيات النقل والتحكم، ومستخدمو كل هذه العناصر [3].

وعليه يمكننا القول بأن : "الفضاء السيبرانى هو بيئة تفاعلية حديثة، تشمل عناصر مادية وغير مادية، مكون من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشغلين أو مستعملين" وتجدر الاشارة إلى أن مسألة تحديد مفهوم " الفضاء السيبرانى"، هي مسألة نسبية تتوقف على طبيعة إدراك وفهم كل من الدول والبيئات كل حسب رؤيته واستراتيجيته وقدرته على استغلال المزايا المتاحة ومواجهة المخاطر الكامنة في هذا الفضاء.

المطلب الثاني

التحولات بين مضامين القوة وظهور القوة السيبرانى

أصبح الفضاء السيبرانى احد هذه العناصر الأساسية التي تؤثر في النظام الدولي، بما يتيحه من أدوات تكنولوجية مهمة لعمليات الحشد والتعبئة في العالم، فضلا عن التأثير في القيم السياسية، فسهولة الاستخدام ورخص التكلفة زادا من قدرته على التأثير في مختلف مجالات الحياة، سواء السياسية، الاقتصادية، العسكرية، الاجتماعية وحتى الايديولوجية، وبات جلبا أن من يمتلك آليات توظيف البيئة السيبرانى يصبح أكثر قدرة على تحقيق أهدافه والتأثير في سلوك الفاعلين المستخدمين لهذه البيئة.

- سيسكو شركة امريكية عملاقة متخصصة بعلم الشبكات بشكل عام.
- وكالة حكومية مكلفة بالدفاع السيبرانى الفرنسي أسست في 7 جويلية 2009.

من الأمور المتعارف عليها في العلاقات الدولية ان مصادر قوة الدولة وأشكالها تتغير، فإلى جانب القوة الصلبة ممثلة في القدرات العسكرية والاقتصادية، تزايد الاهتمام بالأبعاد غير المادية للقوة، ومن ثم بروز القوة الناعمة التي تعتمد على جاذبية النموذج والاقناع، ومع ثورة المعلومات ظهر شكل جديد من أشكال القوة هو السيبرانى (Cyber power). التي لها تأثير كبير على المستوى الدولي والمحلى، فمن ناحية ادت إلى توزيع وانتشار القوة بين عدد اكبر من الفاعلين مما جعل قدرة الدولة على السيطرة موضع شك، ومن ناحية اخرى منحت الفاعلين الأصغر قدرة أكبر على ممارسة كل من القوة الصلبة والقوة الناعمة عبر الفضاء السيبرانى، وهو ما يعنى تغيراً في علاقات القوى في السياسة الدولية.

يعد جوزيف س ناى (Josehp S.Nye) من أبرز المهتمين بالقوة السيبرانى، حيث يعرفها بأنها " القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني ، أى انها القدرة على استخدام القضاء السيبراني لايجاد مزايا الدولة ، والتأثير على الأحداث المتعلقة بالبيئات التشغيلية الأخرى وذلك

على أدوات سيبرانية.[4]، كما يوضح جوزيف س ناى أن مفهوم القوة السيبرانى يشير إلى " مجموعة الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات والشبكات الالكترونية والبنية التحتية المعلوماتية والمهارات البشرية المدربة للتعامل مع هذه الوسائل".

ويتناول مفهوم القوة السيبرانية مجمل القضايا التي تتعلق بالتفاعلات الدولية العسكرية والاقتصادية والسياسية والثقافية والاعلامية وغيرها ، وحتى تتمكن الدولة من ممارسة النفوذ داخليا أو خارجياً عبر القوة السيبرانى يجب ان تتوفر على مجموعة عناصر أهمها :

- **وجود بنية تحتية سيبرانية** :

تشمل أجهزة الكمبيوتر، وشبكات الاتصالات ، والبرمجيات ، وقواعد البيانات لمختلف الأنظمة والقطاعات.

- **بنية مؤسسية :**

تتولى مهمة ممارسة القوة السبيرانية وتحقيق الأمن السبيرانى للدولة.

- **بنية تشريعية:**

تكون ضامنة ومحددة لاستعمال القوة السبيرانية.

- استراتيجية بأهداف واضحة تحدد طرق العمل والأهداف المرجوة[5].

المبحث الثاني

الفواعل في مجال القوة السيبرانية

مع تحول الفضاء الإلكتروني إلى ساحة للتفاعلات الدولية ، بزر العديد من الأنماط التوظيفية له، سواء على صعيد الاستخدامات ذات الطبيعة المدنية أو العسكرية، الأمر الذي جعل هذا الفضاء مجالاً للصراعات المختلفة سواء للفاعلين من الدول أو غير الدول لحيازة أكبر قدر من النفوذ و التأثير السيبراني ..

في هذا السياق تبلورت ظاهرة "الحروب السيبرانية" التى اتسمت بخصائص مختلفة عن نظيراتها التقليدية من حيث طبيعة الأنشطة العدائية ، والفواعل، والتأثيرات في بنية الأمن العالمي ، وعبرت تلك الحرب عن نمطين من القوة (الناعمة والصلبة) في عملية توظيف التفاعلات في الفضاء الإلكتروني أو السيبرانى ، مما تعكس تنامى القدرات والتهديدات المتصاعدة لأمن البنية التحتية الكونية للمعلومات وزيارة تأثيرها في البيئات التشغيلية الأخرى كالبحر والبر والفضاء الخارجي .

وعليه فإن المجال السيبراني شهد تنامي مستمر في تحسين الحياه البشرية في مجالات عديدة ، وغدا العالم معتمد على نحو متزايد بهذا الفضاء في جميع المجالات الكونية.

يحدد جوزيف س ناى ثلاثة انواع من الفاعلين الذين يمتلكون القوة السيبرانية :

- الـــــــدول:

والتى لديها قدرة كبيرة على تنفيذ هجمات سيبرانية وتطوير البنية التحتية وممارسة السلطات داخل حدودها.

- الفاعلون من غير الدول :

ويستخدم هؤلاء الفاعلون القوة السيبرانى لأغراض هجومية بالأساس، إلا أن قدرتهم على تنفيذ أى هجوم سيبرانى مؤثر تتطلب مشاركة ومساعدة أجهزة استخباراتية متطورة، ولكن يمكنهم اختراق المواقع الالكترونية واستهداف الأنظمة الدفاعية.

- الأفـــــراد:

الذين يمتلكون معرفة تكنولوجية عالية والقدرة على توظيفها ، وعادة ما تكون هناك صعوبة في الكشف عن هوياتهم، ومن الصعب ملاحقتهم.

كما يمكننا التفصيل أكثر بخصوص الفاعلين من غير الدول كالتالى [6]:

- الشركات متعددة الجنسيات:

تمتلك بعض شركات التكنولوجيا موارد للقوة تفوق قدرة بعض الدول، ولا تنقصها سوى شرعية ممارسة القوة التي مازالت حكراً على الدول، فخوادم شركات مثل : جوجل Google وفيسبوك Facebook وميكروسوفت Microsoft وأبل Apple وأمازون Amazon، تسمح لها بامتلاك قواعد البيانات العملاقة التي من خلالها تستكشف وتستغل الأسواق، وتؤثر في اقتصاديات الدول وفى ثقافة المجتمعات وتوجيهاتها، وهذا ما حدث في الأزمة بين شركة جوجل والصين حول المحتوى، او فضيحة تسريب بيانات مستخدمى فيسبوك لصالح شركة"كامبردج أناليتيكا" التي تم الاستعانة بها لصالح حملة الرئيس الأمريكى ترامب.

- المنظمات الاجرامية:

تقوم هذه المنظمات الإجرامية بعمليات القرصنة السيبرانية ، وسرقة المعلومات واختراق الحسابات البنكية وتحويل الأموال، كما توجد سوق سوداء على الانترنيت العميق Deep Internet لتجارة المخدرات والأسلحة والبشر، حيث تكلف هذه الجرائم السيبرانى مليارات الدولارات سنوياً.

- الجماعات الارهابية:

تعد من أبرز الفواعل الدولية، خاصة بعد احداث 11سبتمبر، حيث تستغل الفضاء السيبرانى في عمليات التجنيد والتعبئة والدعاية وجمع الأموال والمتطوعين، كما تحاول جمع المعلومات حول الأهداف العسكرية، وكيفية التعامل مع الأسلحة وتدريب المجندين الجدد عن بعد، رغم أنها لم تصل بعد إلى مرحلة القيام بهجوم سيبرانى حقيقي على منشآت البنية التحتية للدول.الأفراد:

أصبح الفرد بفضل الفضاء السيبرانى فاعلاً مؤثراً في العلاقات الدولية ومن أبرز النماذج ظاهرة الويكيليكس "Wikileaks" الذى نجح في نشر ملايين الوثائق السرية للإدارة الأمريكية وقنصلياتها، مما خلق مشاكل دبلوماسية بين الولايات المتحدة الأمريكية وحلفائها.

المبحث الثالث

الصراع السيبرانى

اختصر الفضاء السيبرانى حاجزا الزمان والمكان، وخلق مساحات للتفاعلات الداخلية والدولية في الواقع الافتراض ، ومن ثم ، برزت فضاءات جديدة للصراع بأدوات مختلفة، وانماط جديدة تختلف عن الصراعات التقليدية، بعد احداث 11 سبتمبر 2001- التي تعد مفصلية في تاريخ العلاقات الدولية لبداية استعمال الجماعات الارهابية للأنترنت بشكل بارز في الترويج للفكر المتطرف، كان الفضاء السيبرانى ساحة الصراع والقتال بين تنظيم القاعدة والولايات المتحدة، وفى عام 2007 جرت العمليات العدائية بين استونيا وروسيا في الفضاء السيبرانى، وهو ما حدث أيضاً في 2008 في الحرب بين روسيا وجورجيا ، وجاء الهجوم الالكتروني بفيروس" ستاككسنت" على برنامج إيران النووى عام 2012، ليبرز قوة الأسلحة السيبرانى في الصراعات الدولية.

ولعل أبرز ما يعزز انتشار الأنشطة غير السلمية في الفضاء السيبرانى:[7]

(1) ارتباط العالم المتزايد بالفضاء السبيرانى وزيادة خطر تعرض البنية التحتية الكونية للمعلومات لهجمات سيبرانية.

(2) استخدام الفاعلين من غير الدول للفضاء السيبرانى لتحقيق أهدافهم وتأثير ذلك على سيادة الدولة.

(3) انسحاب الدولة من قطاعات استراتيجية لصالح القطاع الخاص.

(4) إشكالية تعامل الدول مع الشركات التكنولوجية متعددة الجنسيات، والتي أصبحت تفوق قدرتها، مثل مواقع الشبكات الاجتماعية كالفيس بوك وتويتر واليوتيوب الذين اصبحوا فاعلين دوليين بامتياز.

وبالتالي أصبح الفضاء السيبرانى ساحة جديدة للصراع بشكلة التقليدي ولكنه ذو طابع سيبرانى يعكس النزاعات التي تخوضها الدول او الفاعلين من غير الدول على خلفيات دينية أو عرقية وأيديولوجية أو اقتصادية أو سياسية، ويتمدد الصراع السيبرانى بداخل شبكات الاتصال والمعلومات متجاوزاً الحدود التقليدية وسيادة الدول.

وكشف استخدام الفضاء السيبرانى عن حالة التعارض الحقيقي للاحتياجات والقيم والمصالح بين العديد من الفاعلين، وساعد ذلك على ظهور أساليب جديدة للصراع الدولي، تباينت بين الطابع التقني والتجاري والاقتصادي والعسكري ، إلى جانب ظهور طرق بديلة عن الحرب المباشرة بين الدول عبر شبكات الاتصال والمعلومات.

فهناك صراع سيبرانى تحركه دوافع سياسية، ويأخذ شكلاً عسكرياً، ويتم فيه استخدام قدرات هجومية ودفاعية عبر الفضاء السيبرانى ، ويوجد صراع سيبرانى ذو طبيعة ناعمة، حول الحصول على المعلومات والتأثير في المشاعر والأفكار وشن حرب نفسية وإعلامية، كما يأخذ الصراع السيبرانى طابعاً تنافسياً حول الاستحواذ على سبق التقدم التكنولوجي وسرقة الأسرار الاقتصادية والعلمية، والتحكم بالمعلومات، والعمل على اخراق الأمن القومى للدول، كهجمات قراصنة الكمبيوتر والتجسس بما يكون له من تأثير على تدمير الاقتصاد والبنية التحتية بنفس القوة التي قد يسببها تفجير تقليدى مدمر، ويمكن أن يستخدم الفضاء السيبرانى كوسيلة من وسائل الصراع داخل الدولة، بين مكوناتها ، على أساس طائفي أو اقتصادي أو ديني.

المبحث الرابع

الأمن السيبرانى وأبعاده

شمولية الأمن تعنى أن له أبعاد متعددة لها خصائص التي تثبت ترابطها وتكاملها كالبعد السياسي والاجتماعي وغيرهما ، ففي بداية الألفية الثانية خرجت العلاقة بين الفضاء السيبراني والعلاقات الدولية من بعدها التكنولوجي لأبعاد أخرى سياسية وأمنية واقتصادية وعسكرية وقانونية، وتحولت لدور وظيفي وحيوي سواء فى الاستحواذ على عناصر القوة أو في تشكيل السياسات الخارجية ، والتأثير فى الرأي العام، وفى اتاحة الفرصة لتشكيل تحالفات دولية .

المطلب الأول

تعريف الأمن السيبرانى

يعرف الأمن السيبرانى بأنه أمن الشبكات والأنظمة المعلوماتية، والبيانات، والمعلومات، والأجهزة المتصلة بالأنترنت، وعليه فهو المجال الذى يتعلق بإجراءات، ومقاييس، ومعايير الحماية المفروض اتخاذها، أو الالتزام بها، لمواجهة التهديدات، ومنع التعديات، أو على الأقل الحد من آثارها.[8]

فريتشارد كمرر Richard A.Kemmerer يعرف الأمن السيبرانى بأنه: عبارة عن وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القراصنة. (9)

بينما عرفه إدوارد أمورسو Edward Amorso على انه : وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القراصنة وكشف الفيروسات ووقفها ..... الخ. (10)

وبحسب تعريف الاتحاد الدولي للاتصالات في تقريره حول (اتجاهات الإصلاح في الاتصالات للعام 2010 – 2011)، هو " مجموعة من المهمات، مثل تجميع وسائل ، وسياسات، واجراءات امنية، ومبادئ توجيهية، ومقاربات لإدارة المخاطر، وتدريبات ،

وممارسات فضلى، وتقنيات، يمكن استخدامها لحماية البيئة السيبرانى، وموجودات المؤسسات والمستخدمين[11]، وتهدف الحماية إلى جعل المعتدين يحجمون عن خططهم، او منعهم من تحقيقها، وإلى ضمان حد مقبول من الأخطار، وذلك عبر وضع خطة تتلاءم والمحيط التقني، البشرى، التنظيمي، والقانوني .

المطلب الثاني

أبعاد الأمن السيبرانى

يطال الأمن السيبرانى جميع المسائل العسكرية، الاقتصادية، والاجتماعية، والسياسية، والإنسانية، يهدف تحقيق منظومة أمن متكاملة تعمل على الحفاظ على الأمن القومى للدولة من كل التهديدات السيبرانى، وعليه لابد من توضيح أبعاد الأمن السيبرانى، التي نوردها كالآتي :[12].

1) **البعد العسكري:**

يكمن في الحفاظ على قدرة الوحدات العسكرية على التواصل عبر الشبكات العسكرية، مما يسمح بتبادل المعلومات والأوامر وتدفقها (هي الفكرة التي خلقت وطورت من أجلها الشبكات ومن بعدها الانترنت)، وإصابة الأهداف عن بعد، إلا انها تمثل كذلك نقطة ضعف، خاصة إذا لم تكن مؤمنة جيداً من الاختراق، الذى قد يؤدى إلى تدمير قواعد البيانات العسكرية، أو قطع الاتصال بين القيادة والوحدات العسكرية، فضلاً عن إمكانية التحكم في بعض الأسلحة وخروجها عن السيطرة(طائرات بدون طيار، صواريخ موجهة، اقمار صناعية..... الخ) ويعتبر فيروس ستاكسنت Staxnet بداية لاستعمال القوة السيبرانى لتدمير البنية المادية (هاجم حواسيب اجهزة الطرد المركزي الإيرانية).

2) **البعد الاقتصادي:**

أصبح الانترنت أساسا للمعاملات التجارية والمادية والاقتصادية، كما تستعمل الحواسب في تسيير وتطوير الصناعات وتحريك الاقتصاد ، وأصبح الكل مترابطاً عبر شبكات الكمبيوتر، مما يستدعى الحديث عن اهمية تحقيق الأمن السيبرانى في المجال الاقتصادي .

3) **البعد الاجتماعي:**

مستعملي الانترنت حول العالم ، مستعملي الانترنت في العالم حسب المناطق الجغرافية

بتاريخ : 31 ديسمبر 2017 و عدد المستعملين :4.165.932.140 مستعمل .

ويفوق مستخدمي الانترنت 4 مليارات شخص في العالم، منهم أكثر من 2.6 مليار يستخدمون مواقع التواصل الاجتماعي، مما يجعلها أكبر تجمع للتفاعل البشرى، ويفتح الباب واسعاً لتبادل الأفكار والخبرات الجيدة، لكن في المقابل يعرض اخلاقيات المجتمع للخطر، نظراً لصعوبة مراقبة محتوى الانترنت، كما يعرض الهويات لعمليات اختراق خارجي قد تتسبب في تهديد السلم الاجتماعي للدولة، وعليه فلابد من العمل على توعية المواطن بهذه المخاطر لتحقيق الأمن السيبرانى في بعده الاجتماعي.

4) **البعد السياسي:**

يعد التدخل الروسي السيبرانى في الانتخابات الأمريكية أبرز دليل على ضرورة وأهمية الأمن السيبرانى في بعده السياسي ، إضافة إلى التسريبات للوثائق الحساسة والاختراقات التي غالباً ما تؤدى إلى أزمات دبلوماسية بين الدول، كما ان الفضاء السيبرانى أصبح بيئة خصبة للحملات الانتخابية والدعاية لمختلف الفاعلين الدوليين.

5) **البعد القانونى:**

إن التطورات التكنولوجية المتسارعة، تفرض مواكبة التشريعات القانونية لها، من خلال وضع أطر وتشريعات للأعمال القانونية وغير القانونية في الفضاء

السيبراني، فالملاحظ ان الجريمة السيبرانى تفتقد في معظم البلدان إلى الأطر القانونية الصارمة للتعامل معها ، إضافة إلى ضرورة تفعيل التعاون الدولي المشترك لمكافحتها.

المبحث الخامس

انماط التهديدات السيبرانية

تنقسم التهديدات السيبرانية التي تواجهها الدول والأفراد إلى أربعة أنماط رئيسية هي: [13]

1) **إتلاف المعلومات او تعديلها :**

ويقصد به الوصول إلى معلومات الضحية عبر شبكة الانترنت أو الشبكات الخاصة، والقيام بعملية تعديل البيانات الهامة دون أن يكشف الضحية ذلك، فالبيانات تبقى موجودة لكنها مضللة قد تؤدى إلى نتائج كارثية خاصة إذا كانت خطط عسكرية أو مواعيد أو خرائط سرية.

2) **التجسس على الشبكات :**

ويقصد به الدخول غير المصرح والتجسس على شبكات الخصم، دون تدمير أو تغيير في البيانات والهدف منه الحصول على معلومات قد تكون خطط عسكرية أو أسرار حربية ، اقتصادية ، مالية ، سياسية ، مما يؤثر سلباً على مهام الخصم.

3) **تدمير المعلومات:**

ويتم في هذه الحالة مسح وتدمير كامل للأصول والمعلومات والبيانات الموجودة على الشبكة يصطلح عليه" تهديد لسلامة المحتوى" ويعنى بها إحداث تغيير في البيانات سواء بالحذف أو التدمير من قبل أشخاص غير مخولين.

وهناك ما يميز بين عدة أنواع لمخاطر التهديدات السيبرانى نذكر منها. [14] :

- التعرض لسرية الاتصالات التي تطال البريد الإلكتروني ، والدخول إلى

الأنظمة والملفات دون إذن، وهذا يعتبر اعتداء على الحريات والحقوق الشخصية.

- التلاعب بالمعلومات الموجودة في نظام معين، وتشويهها أو إتلافها، سواء عبر الاختراق أو نشر الفيروسات.

- الجرائم العادية التي تستخدم الانترنت ، للسرقة والغش وسرقة الهويات، والاعتداء على الملكية الفكرية وغيرها.

المبحث السادس

علاقة الأمن السيبرانى بالأمن القومى

يعد الأمن السيبراني سلاحاً إستراتيجياً بيد الحكومات والأفراد الاسماكين الحرب السيبرانية أصبحت جزء لا يتجزأ من التكتيكات الحديثة للحروب والهجمات بين الدول، ويشمل الأمن السيبرانى أمن المعلومات على أجهزة الحاسوب الآلى وشبكاته ، بما في ذلك العمليات والآليات التي يتم من خلالها حماية معدات الحاسوب الآلى والمعلومات والخدمات من أى تدخل غير مقصود أو غير مصرح به أو تغيير أو إتلاف قد يحدث ويمكن اعتبار تحدى الأمن السيبراني أعلى تحديات الأمن القومى فى القرن الواحد والعشرين مع الإشارة إلى أن الحديث للأمن لا تقتصر فقط على الجوانب العسكرية ، بل يواكب كل التهديدات والتحديات التي يمكن أن تشكل عائقاً أمام الاقتصاد الرقمي وتدفق المعرفة، فقد أسقطت تكنولوجيا المعلومات والاتصالات مفهوم الحدود الجغرافية والسياسية والثقافية بين الدول ، ما يضع السيادة الوطنية على المحك، خاصة مع اختراق المواقع الحكومية الرسمية والتجسس المعلوماتي على الدول.

المطلب الأول

الأمن السيبرانى رافد جديد للأمن القومى

تزايدت العلاقة بين الأمن والتكنولوجيا، ومعها تزايدت امكانية تعرض المصالح الاستراتيجية للدولة للتهديدات السيبرانى ، وتهدد بتحول الفضاء السيبرانى لوسيط ومصدر لأدوات جديدة للصراع الدولي المتعدد الأطراف.

بعد أحداث 11 سبتمبر بدأ التركيز على الفضاء السيبرانى كتهديد امنى جديد، خاصة

مع استخدام تنظيم القاعدة له كساحة قتال ضد الولايات المتحدة الأمريكية، وفى عام 2007 ، 2008 على التوالي كان الأمن القومى لكل من استونيا وجوريجيا مهدداً من طرف روسيا ، حيث استعملت هجمات الحرمان من الخدمة لتقويض العمل في الادارات والمؤسسات الحكومية لكلا الدولتين، وأصبح الفضاء السيبرانى للدولتين مجالاً للعمليات، وجاء الهجوم السيبرانى بفيورس " ستاكسنت" على أجهزة الطرد المركزي الإيرانية، من أجل تعطيل برنامج إيران النووي ، ليمثل نقله نوعية مهمة في تطوير واستخدام الأسلحة السيبرانى [15]، هذا إضافة إلى الدور الكبير الذى لعبته شبكات التواصل الاجتماعي في حالة الثورات العربية في بداية 2011، حيث مثلت نقطة هامة في زيادة الاهتمام الدولي بأمن الفضاء السيبرانى، وبرزت محاولات للسيطرة عليه بعد تصاعد الاحتياجات حتى في الدول الأكثر ديموقراطية كبريطانيا والولايات المتحدة الأمريكية.

إن العلاقة بين الأمن السيبرانى والأمن القومى تزداد كلما زاد نقل المحتوى المعلوماتى والعسكري والأمني والفكري والسياسي والاجتماعي والاقتصادي والخدمي والعلمي والبحثي إلى الفضاء السيبراني ، خاصة مع التسارع في تبنى الحكومات الالكترونية والمدن الذكية في العديد من الدول، واتساع نطاق وعدد مستخدمي الانترنت في العالم، حيث تصبح قواعد البيانات القومية في حالة انكشاف خارجى ، إضافة إلى حملات الدعاية والمعلومات المضللة ونشر الشائعات أو الدعوة لأعمال تحريضية أو دعم المعارضة او الأقليات، مما يساهم في تلاشى سيادة الدولة ويشكك في قدرتها على الحفاظ على أمنها القومى [16].

وعليه فلم يقتصر اهتمام الدول بالأمن السيبرانى على البعد التقني وحسب بل تجاوز إلى أبعاد أخرى مثل الأبعاد الثقافية والاجتماعية والاقتصادية والعسكرية وغيرها وهو ما عمل على دعم حقيقة أن الاستخدام غير السلمى للفضاء الإلكتروني يؤثر على الرخاء الاقتصادي والاستقرار الاجتماعي لجميع الدول التي أصبح تعتمد على البنية التحتية الكونية للمعلومات.

ترتيباً لما سبق فقد أصبحت المصالح القومية التي ترتبط بالبنية التحتية الحيوية عرضة لخطر الهجوم، حيث جعل الفضاء السيبرانى تلك المصالح مرتبطة ببعضها البعض في بيئة عمل واحدة، ومن ثم فإن أى هجوم على إحدى تلك المصالح يكون سبباً لحدوث عدم توازن استراتيجى ومهدد خطر للأمن القومى، وهذا ما دفع العديد من الدول إلى إدخال الأمن السيبراني ضمن استراتيجيتها للأمن القومي.

المطلب الثاني

العقيدة الأمنية الجديدة

إن حالة انعدام الثقة واللايقين في العلاقات الدولية، هو ما يشجع تزايد النزاعات في العالم إضافة إلى التطورات السريعة في الفضاء السيبرانى، مما جعلت الدول تسارع إلى تبنى تغيرات في العقيدة الأمنية، وذلك بإدراج القوة السيبرانى كمحدد رئيس لمدى قوة الدولة، وقدرتها على حسم النزاعات لصالحها.

ووفقاً للعقيدة الروسية الجديدة لأمن المعلومات، التي وقعها الرئيس الروسي فلاديميربوتين ، فإن إحدى التهديدات الرئيسية لروسيا تتمثل " بزيادة عدد الدول الأجنبية التي لديها تأثير على البنية التحتية لمعلومات الأغراض العسكرية في روسياً". أحد الأهداف الرئيسية لواضعي هذه العقيدة للأمن السيبرانى، هو " الردع الاستراتيجى والوقاية من النزاعات العسكرية، والتى يمكن أن تنجم عن استخدام تكنولوجيا المعلومات. (17)

ارتبط تصاعد الصراع بين روسيا والدول القريبة بقيادة الولايات المتحدة، خلال السنوات الماضية، باستدعاء متنام لحرب المعلومات كأحد للمداخل الهامة للتأثير في مسارات الصراع.

كما يعتقد ديفيد سميث David J.smith في دراسة له بعنوان كييف تستخدم روسيا الحرب السيبرانى ؟ " ، ان روسيا تعتمد على مفهوم واسع للحرب المعلوماتية، يشمل : الاستخبارات ، والتجسس المضاد، والخداع، والتضليل، والحرب الالكترونية، وتدمير الاتصالات وأنظمة دعم الملاحة، والضغوط النفسية، بالإضافة إلى الدعاية وإلحاق

الضرر بنظم المعلومات.[18]

ويفترض" بافل أنتونوفيتش" Pavel Antonovich أن " ترسيم الخطوط الفاصلة بين الحرب والسلام يمكن أن يتآكل بسهولة في الفضاء السيبراني، فيمكن أن يتم إلحاق اضرارا، مهما كانت طبيعتها ، بالخصم، وذلك دون تجاوز الخط الفاصل بين الحرب والسلام بشكل رسمى.

وفى الجهة المقابلة، نجد ان منظمة" حلف شمال الأطلسى NATO" سعت بدورها إلى تحديث عقيدته الأمنية، استجابة للتغيرات الحاصلة في طبيعة التهديدات، وطبيعة الحرب، حيث أقر بمجموعة من النقاط الأساسية من بينها:

- **ان الدفاع السيبراني يمثل جزءاً أساسياً من الدفاع الجماعى للحلف.**
- **الفضاء السيبراني يمثل مجالا لعمليات الحلف.**
- **بناء قدرات سيبرانية تعد مهمة اساسية للحلف وحلفائه[19].**

بالإضافة إلى ذلك، نجد كلا من الصين ، اسرائيل، بريطانيا، فرنسا ، والولايات المتحدة الأمريكية، إيران، وكوريا الشمالية، قد طورت كل منها عقديتها الأمنية، وأصبحت تعتبر الفضاء السيبراني مسرحاً للعمليات العسكرية، كما أوجدت قيادة خاصة ومستقلة لقيادة العمليات السيبرانية.

المطلب الثالث

الحروب السيبرانية

تكمن خطورة الحروف السيبرانى في كون العالم أصبح يعتمد أكثر فأكثر على الفضاء السيبرانى ولاسيما في البنية التحتية المعلوماتية، ولا شك أن ازدياد الهجمات السيبرانى يعنى إمكانية تطورها لتصبح سلاحاً حاسماً في النزاعات بين الدول في المستقبل.

أولاً: مفهوم الحرب السيبرانى:

لا يوجد إجماع على تعريف محدد ودقيق لمفهوم الحرب السيبرانى، فيعرفها كل من " ريتشارك كلارك" و " روبرت كناكى" على أنها " أعمال تقوم بها دولة تحاول من خلالها اختراق اجهزة الكمبيوتر والشبكات التابعة لدولة اخرى يهدف تحقيق أضرار

بالغة أو تعطيلها. [20]

ويعرفها " بولوشاكريان" Paulo Shakarian بأنها : امتداد للسياسة من خلال الاجراءات المتخذة في الفضاء السيبراني من قبل دول أو فاعلين غير دوليين، حيث تشكل تهديداً خطيراً للأمن القومى" [21].

يقترح أخرون ان يتم التركيز بدلاً من ذلك على أنواع وأشكال النزاع التي تحصل في الفضاء السبيرانى، ويحددون مستوياتها كالتالى:

- **القرصنة السيبرانية:**

وتقع في المستوى الأول ، ومن أمثلته القيام بعمليات قرصنة المواقع الالكترونية أو بتعطيل الحواسيب الخادمة (Servers) من خلال إغراقها بالبيانات.

- **الجريمة السبيرانية والتجسس السيبرانى:**

ويقعان في المستوى الثاني والثالث وغالباً ما يستهدفان الشركات والمؤسسات وفى حالات نادرة بعض المؤسسات الحكومية.

- **الإرهاب السيبرانى:**

ويقع في المستوى الرابع ويعبر عن الهجمات غير الشرعية التي ينفذها فاعلون غير حكوميون ضد أجهزة الكمبيوتر والشبكات والمعلومات المخزنة.

- **الحرب السيبرانية:**

وهى المستوى الأخطر للنزاع في الفضاء السبيرانى ، وتهدف إلى التأثير على إرادة الطرف المستهدف السياسية وعلى قدرته في عملية صنع القرار، وكذلك التأثير فيما يتعلق بالقيادة العسكرية و/أو توجيهات المدنيين في مسرح العمليات الإلكتروني[22].

ثانيا : خصاص الحروب السيبرانى:

من المتوقع أن تصبح الحرب السبيرانية نموذجاً تسعى إليه العديد من الجهات نظراً للخصائص العديدة التي تنطوى عليها، ومنها:

1) حروب لا تناظرية :

فالتكلفة المتدنية نسبياً للأدوات اللازمة لشن هكذا حروب يعنى أنه ليس هناك حاجة لدولة معينة أ ومنظمة ما لقدرات ضخمة لتشكل تهديداً خطيراً وحقيقها على دولة مثل الولايات المتحدة الأمريكية .

2) تمتع المهاجم بأفضلية واضحة :

فهذه الحروب تتميز بالسرعة والمرونة والمراوغة، وفى بيئة مماثلة يتمتع المهاجم بأفضلية، ومن الصعوبة نجاح عمليات الدفاع.

3) المخاطر تتعدى استهداف المواقع العسكرية :

هناك جهود متزايدة لاستهداف البنية التحتية المدنية والحساسة كاستهداف شبكات الكهرباء والطاقة وشبكات النقل والنظام المالى والمنشآت الحساسة النفطية أو المائية أو الصناعية بواسطة فيروس يمكنه إحداث أضرار مادية حقيقة تؤدى إلى دمار هائل.

ثالثا : تداعيات الحروب السيبرانى على الأمن القومى :

سببت الحروب السبيرانية جملة من المخاطر والتداعيات على تفاعلات السياسة الدولية، يمكن طرح أبرزها على النحو الآتي [23]:

(1)**تصاعد المخاطر الالكترونية**: خاصة مع قابلية المنشآت الحيوية(مدنية وعسكرية) في الدول للهجوم، الأمر الذى يؤثر في وظائف تلك المنشآت، وبالتالي ، فإن التحكم في تنفيذ هذا الهجوم بعد أداة سيطرة استراتيجية.

(2)**تعزيز القوة وانتشارها**: عمل الفضاء السيبرانى على إعادة تشكيل قدرة الأطراف المؤثرة ، وأدى إلى عملية انتشار القوة بين فاعلين متعددين.

(3)**عسكرة الفضاء السيبرانى**: حيث برز في هذا الاطار عدة اتجاهات، مثل التطور في مجال سياسات الدفاع والأمن السيبرانى ، وتصاعدت القدرات في سياق التسلح السيبراني، وتبنى سياسات دفاعية سيبرانية لدى الأجهزة المعنية بالدفاع والأمن في الدول ، وتزايد الاستثمار في مجال تطوير

أدوات الحروب السيبرانى داخل الجيوش الحديثة .

(4)**ادماج الفضاء الالكتروني ضمن الأمن القومي للدول**: وذلك عبر تحديث الجيوش، وتدشين وحدات متخصصة في الحروب الالكترونية، وإقامة هيئات وطنية للأمن والدفاع الالكتروني، والقيام بالتدريب ، وإجراء المناورات لتعزيز الدفاعات الإلكترونية.

(5) **الاستعداد لحروب المستقبل**: حيث تبني العديد من الدول استراتيجية حرب المعلومات باعتبارها حرباً للمستقبل ، حيث ترى الدول الكبرى أن من يحدد مصير تلك المعركة المستقبلية ليس من يملك القوة فقط، وإنما القادر على شل القوة ، والتشويش على المعلومة.

سبب تغلب الطابع السياسي علي الطابع القانوني لهذا البحث

الفضاء السيبراني ليس بيئة ثابتة ولكنه مجال يتيح لنا التفكير في الممارسات الاقليمية لكونه انه يتوسع باستمرار ، مما يجعل من الصعب تحديد الطابع الذي يتضمن سلطة سيادة الدولة حيث ان الدولة القومية هي الاطار السياسي والقانوني لمفهوم الامن السيبراني ويغلب الاطار السياسي بمجال السيبرانية المعلوماتية لحماية وضمان سياسة رقمية امنة للدولة .

الخاتمة

إن الثابت اليوم في العلاقات الدولية وتوازنات القوى ان الحرب الباردة والصراع السياسي والاقتصادي والتجاري بين الأقطاب في العالم تحول إلى حرب سيبرانية صامتة وقد تكون مدمرة في الأعوام المقبلة. من هنا بدأت دول العالم الواحدة تلو الأخرى تستكشف الخيارات المتاحة لتعزيز قدراتها الهجومية في الفضاء السيبرانى وقد أعدت دول كثيرة عدتها للتحول الى مرحلة جديدة لإعادة حساباتها ومراجعة أولويات كي حتى تكون على الاستعداد الكامل للتعامل مع جروب المستقبل التي بالضرورة مبنية على مخرجات تكنولوجيا الجيل الخامس والذكاء الاصطناعي.

باتت السيبرانية مجالاً آخر لاستعراض القوى وممارسة النفوذ وتحقيق التفوق والتنافس الدولي فلم تعد ترسانات الأسلحة ال التقليدية واسلحة الدولة الدمار الشامل هي المعيارالأساسى لقياس مؤشراتها وتصنيفها كما هو الحال للقوة الصلبة لأن بناء أدوات تقيس قدراتها الأساسية في فهم هذا الفضاء البالغ الأهمية لتحسين الاستراتيجية والسياسات الالكترونية للدول ، مع التذكير أن تدفق المعلومات التي تمارسها الدول المتقدمة اليوم تحمل في طياتها تهديدات ومخاطر جديدة على معظم دول عالم الجنوب ومنها العالم العربي الأمر الذي يحتم عليه تحصين أمنه والحفاظ عليه وسط كم هائل من المتغيرات والتطورات المعلوماتية الكبيرة.

وأياً كان الشكل أو المستوى فإن حروب الفضاء السيبرانى أو الالكتروني قداً صبحت واقعاً ليس بإمكان أي دولة التغاضي عنه حيث لا تكاد دولة اليوم تسلم من التعرض لإحدى أشكالها بالأخص من قبل الدول الكبرى وسياستها في الهيمنة والتنافس على موارد وقدرات الدول الأخرى بما في ذلك حرب المعلومات والشائعات أو التجسس والاختراقات وكل ذلك يستدعى المبادرة والأخذ بالتدابير الاحتياطية بداية من تطوير منظومات الدفاع الالكترونية والأمن السيبرانى وحتى المشاركة والدفع باتجاه تطوير منظومات تشريعية دولية تسهم في تحديد وتقييد هذه الحروب بشكل حاسم وفعال .

وفى ضوء ما تقدم من معطيات ، يمكن تأثير النتائج الأتية :

1) أسست القوة السيبرانية رغبة للفواعل من الدول الكبرى وغير الدول بالدخول إلى سباق للتنافس والتفوق السيبرانى كما في العصر النووي سابقاً.

2) أصبحت الحروب السيبرانية دافعاً للدول الكبرى في زيادة قوتها وفاعليتها في النظام الدولي .

3) تفوق الحروب السيبرانية على الحروب التقليدية القديمة بالعمليات العسكرية والحربية والاقتصادية والسياسية والدبلوماسية للوصول لأهدافها بأقل تكلفة.

4) وفرت القوة السيبرانية للدول مجالاً حركياً تتجاوز فيه الحدود الجغرافية للوصول لأهدافها قد يصعب الوصول اليها عن طريقة القوة التقليدية القديمة .

التوصيات:

إن هذا الجيل المعاصر من الحروب يحث على تقديم جملة من التوصيات لصانع القرار كالآتي :

1) الدعوة لتأسيس هيئة عليا في الدولة أو فرع بالقوات المسلحة يرتبط مباشرة بالقيادة العامة للقوات المسلحة يتولى مهمة وضع الخطط الاستراتيجية وإدارة الحرب الالكترونية في الجوانب الدفاعية والهجومية أيضاً .

2) ضرورة عزل المنظومات الأمنية والسيادية الحيوية بشبكة داخلية مستقلة ومحمية من الحاسبات لمنع اختراقها أو التأثير عليها تحت أي ظرف ، مع عمل نسخ احتياطية لكل ملفات المعطيات والبرامج وتجديدها باستمرار و استخدام اتصالات لاسلكية حديثة يصعب إعاقتها .

3) وضع استراتيجية مستقبلية لتشجيع الاستثمار في مجال صناعة الأجهزة والمنظومات الالكترونية لاستقطاب الموهوبين بهذا المجال للاستفادة من خبراتهم في سبيل بناء قوة ردع الكترونية تسمى " بالجيش الالكتروني" .

4) وضع قيود زمنية على تشغيل بعض الوسائل الإلكترونية، لصالح الوسائل الالكترونية الأكثر أهمية مع الحرص على استخدام أقل قدر ممكن من قدرة الإرسال الفترات قصيرة .

الهوامـــش

(1) عباس بدران، الحروب الالكترونية، الاشتباك في عالم متغير، مركز دراسات الحكومة الالكترونية ، بيروت 2010، ص 4

(2) ايهاب خليفة القوة الالكترونية وأبعاد التحول في خصائص القوة، مكتبة الاسكندرية، مصر 2014، ص 33: 42

(3) عادل عبدالصادق أسلحة الفضاء الالكترونى في ضوء القانون الدولي ، سلسلة أوراق، العدد 23، مكتبة الاسكندرية، مصر 2016 ص 17-18

(4) منى الأشقر جبور، السيرانية هامس العصر، المركز العربى للبحوث القانونية والفضائية، بيروت 2017، ص 25

(5) عادل عبدالصادق، القوة الالكترونية، أسلحة الانتشار الشامل في مصر الفضاء الالكترونى، مجلة السياسة الدولية العدد 188 مؤسسة الأهرام، مصر 2012، ص 32

(6) أيهاب خليفة، القوة الالكترونية، كيف يمكن أن تدمر الدول في عصر الانترنيت، دار العربي 2017 ص 54

(7) ما الجديد في عقيدة الأمن السيبراني الروسى، مركز دراسات، على الموقع

(8) حمد بيسونى ، دوافع الاستراتيجية الروسية لحرب المعلومات ضد الدول الغربية، جريدة الصباح الجديد على الرابط.

(9) المجال الخامس، الحروب الالكترونية في القرن الـ21 ، مركز الجزيرة للدراسات على الموقع

(10) عادل عبدالصادق، الحربو السبيرانية : تصاعد القدرات والتحديات للأمن العالمى ، المركز العربي لأبحاث الفضاء الالكترونى على الموقع.

(11) محمد مختار ، الأمن السبيرانى ، مفاهيم المستقبل ، اتجاهات الأحداث، العدد 6 ، 2015 ص 6

(12) محمد مختار، هل يمكن للدول أن تتجنب مخاطر الهجمات الالكترونية، مفاهيم

المستقبل ، العدد 6 مركز المسقبل للأبحاث والتطوير 2015 ، ص 5-6

(13) منى الأشقر جبور، السبيرانية هاجس العصر، مرجع سابق ص 35- 36

14. Olivier KEMPE: introduction à la Cyber stratégie, Paris, Economie,2012,P.g

15. The international telecommunications union, I.T.u too likt for cybercrime legislation, Geneva, 2010, P12.

16. Joseph S. Nye JR: cyber power Harvard Kennedy 2010, P03.

17. Joseph S. Nye JR: I bid, P10.

18. Richard A Kemmere, cyber security. University of California Santa Barabra, Dept. of Computer Science, 2003, P03.

19. Edward Amoro So, Cyber Security. Silicon press, 2007, P01.

20. Rru, Cyber Security Geneva: international telecommunication union (rru) 2008.

21. David Smith, How Russia Hrne SSCS cyber ware fore defense Dossier American foreign policy council (August 2021:Issue 4).

22. Richard A Clarck, Robert Knake: Cyber war the next the national security and what to do about it haper coltins 2010 P.6.

23. Paul, Juna Shakarian, Andrew Ruef: introduction to cyber war fare, Amaltidis plinary Elselver, 2013 p.02.