الفضاء الالكتروني وأثره علي مفاهيم القوة والأمن والصراع في العلاقات الدولية

Cyberspace and its impact on the concepts of power, security and conflict in international relations

محمود علي عبدالرحمن

طالب ماجستير – كلية السياسة والاقتصاد – جامعة بني سويف

اسامة فاروق مخيمر

استاذ مساعد – كلية السياسة والاقتصاد – جامعة بني سويف

المستخلص:

يشهد العالم الآن في ظل الطفرة الكبيرة فى استخدام التكنولوجيا ثورة تعتمد على المعلومات والمعرفة ألا وهى الثورة التكنولوجية وانتشارها بشكل كبير حيث تم التزاوج بين التكنولوجيا والارهاب، وظهور الارهاب الالكترونى الذي أثر بدوره علي مفاهيم الأمن والقوة وأضفي البعد الالكتروني عليها، فالقوة لم تعد مقتصرة على القوة الصلبة والتى تتمثل فى القوة العسكرية والاقتصادية، والتى تحتكرها الدول بشكل عام، وليس كل الدول وانما الدول الكبرى، وأن هذا النوع لم يعد يقتصر على الدول فقط وانما كل من له القدرة على امتلاك المعرفة التكنولوجية والقدرة على استخدامها وتوظيفها لتحقيق أهدافه، سواء كان دولة أو أفراد أو فاعلين من غير الدول، ومن ثم انتهاء عصر احتكار القوة، ومن ناحية أخري ظهور الفضاء الالكتروني الذي اختصر حاجز الزمان والمكان وخلق مساحات للتفاعلات الداخلية والدولية في الواقع الافتراضي ومن ثم برزت فضاءات جديدة للصراع

بأدوات مختلفة وأنماط جديدة تختلف عن الصراعات التقليدية كما أسهمت الثورة التكنولوجية في تغير مفهوم الأمن القومي بعد أن كان يركز على القوة العسكرية وقدرتها على حماية الدولة، وأدت الي ظهور مفهوم الأمن الالكتروني حيث تغير هذا المفهوم مؤخراً بتغير مصادر تهديدات النظام الدولى التي تؤثر على الأمن القومي للدولة.

الكلمات المفتاحية: القوة الالكترونية؛ الفضاء الالكتروني؛ الأمن الالكتروني؛ الصراع الالكتروني؛ العلاقات الدولية.

Abstract:

The world is now witnessing a revolution based on information and knowledge, namely, the technological revolution and its widespread spread, where technology and terrorism have been combined, and the emergence of cyber-terrorism, which in turn has affected the concepts of security and power and added the electronic dimension to it. But all those who have the ability to possess technological knowledge and the ability to use it and employ it to achieve its objectives, whether it be a State, individuals or non-State actors, and then the end of the era of monopoly of power, and on the other hand the emergence of cyberspace, which shortened the barrier of time and space and created spaces for internal and international interactions in virtual reality and thus emerged new spaces of conflict with different tools and new patterns different from traditional conflicts, and the technological revolution contributed to the change of the concept of national security after He was focused on military power and its ability to protect the state, It has led to the emergence of the concept of cyber security, which has recently changed with

the changing sources of threats to the international system affecting the national security of the state.

Keywords: Electronic Power; Cyberspace; Cyber security; Cyber Conflict; International Relations.

مقدمة:

أفرزت ثورة المعلومات والتكنولوجيا تحولات عميقة في مفهوم الأمن ومضامينه وأبعاده، وايضا أحدثت تغيرات في مفاهيم القوة والصراع من حيث طبيعة المفهوم وملامح الفاعلين، حيث ظلت الصراعات التقليدية والقوة العسكرية تحددان لفترة طويلة طبيعة الخطابات السياسية، وحدود وهيكل النظام العالمي، وموقع القوي الكبري منه، إلا أن اتساع تأثيرات التقدم التقني والعامل التكنولوجي في السياسات الدولية، وخاصة بعد انتهاء الحرب الباردة، أضاف أبعادا أخري للمفاهيم التقليدية كالأمن والقوة العسكرية والصراع، حيث تلاشت الفواصل والحدود بين ماهو مدني وعسكري، ومن ثم أخذت تلك المفاهيم أبعاد وسمات غير تقليدية، سواء من حيث الفاعلون، أو القضايا، أو ديناميات التفاعل في عالمنا الراهن، وذلك نتيجة التغير في طبيعة التهديدات في ظل التزاوج بين التكنولوجيا والارهاب وظهور الارهاب الالكتروني ومع بروز الفضاء الالكتروني، كأحد أسباب التغير في مفاهيم القوة والأمن والصراع في العلاقات الدولية، حيث ساهمت ثورة المعلومات والتكنولوجيا في تحول عدد من الظواهر والتهديدات وفي مقدمتها الإرهاب، مما يجعله يشكل تأثيرا سلبيا متناميا على الأمن القومي للدول[1]، حيث أصبح العالم أمام ما يمكن أن يطلق علية العصر الجديد للارهاب وذلك بالمقارنة بتغير طبيعة الصراعات وملامح الفاعلين وأبعاد الامن القومي وظهور الأمن الالكتروني والفضاء الالكتروني الذي

اختصر حاجز الزمان والمكان وخلق مساحات للتفاعلات الداخلية والدولية في الواقع الافتراضي ومن ثم برزت فضاءات جديدة للصراع بأدوات مختلفة وأنماط جديدة تختلف عن الصراعات التقليدية.

المشكلة البحثيه:

مع بروز الفضاء الالكتروني كساحة للصراع العالمي واجهت المفاهيم التقليدية مثل الأمن والقوة والصراع تحديات واضحة خاصة لجهة مدي ملائمتها أو حتي تكيفها مع طبيعة التفاعلات في الواقع الافتراضي، لذا برزت الحاجة الي معرفة وتفسير طبيعة التغيرات التي ألحقتها الحقائق التكنولوجية بهذه المفاهيم ومن هنا تدور المشكلة البحثيه حول **التساؤل الرئيسي** وهو: **كيف أثر الفضاء الالكتروني علي مفاهيم القوة والأمن والصراع في العلاقات الدولية؟**

وتأتي **أهمية الدراسة** في معرفة التحولات التي طرأت علي مفاهيم الامن والقوة والصراع في ظل التقدم الملحوظ والانتشار المتزايد لثورة التكنولوجيا والمعلومات فضلا عن توضيح أبرز التغيرات في الفواعل وطبيعة الصراعات في العلاقات الدولية، بينما **تهدف الدراسة** الي ابراز وتوضيح البعد الالكتروني لمفاهيم القوة والأمن والصراع وتأثير ذلك علي طبيعة وشكل النظام الدولي وموازين القوي في العلاقات الدولية، مع توضيح العلاقة بين الأمن الالكتروني والأمن القومي وتمثل **منهج البحث وأدواته** من خلال منهج التحليلي الوصفي والذي يمكن من خلاله تفسير طبيعة التغيرات التي لحقت بمفاهيم الامن والقوة والصراع من خلال جمع البيانات الوصفية حول واقع التحولات والتحديات التي واجهتها من حيث تكيفها مع طبيعة التفاعلات في الواقع الافتراضي وصولا الي تحليل وتفسير هذه البيانات. **وسوف تتناول الدراسة المحاور التاليه:**

- **المحور الأول: أثر الفضاء الإلكتروني علي مفهوم القوة في العلاقات الدولية.**

- **المحور الثاني: أثر الفضاء الالكتروني علي طبيعة الصراعات في العلاقات الدولية.**
- **المحور الثالث: أثر الفضاء الالكتروني علي مفهوم الأمن في العلاقات الدولية.**

- **أولا: أثر الفضاء الإلكتروني علي مفهوم القوة في العلاقات الدولية:**

كانت ثورة المعلومات وظهور الانترنت إيذانا ببزوغ العصر الإلكتروني، وخلق بيئة جديدة هي الفضاء الإلكتروني (Cyber space) الذي يمثل بعدا خامسا للحرب والارهاب إلي جانب الأبعاد الأربعة الأخري التقليدية المتمثلة في البر والبحر والجو والفضاء الخارجي حيث أصبح يؤثر في النظام الدولي، خاصة مع بروز شكل جديد من القوة وهي القوة الإلكترونية (Cyber power) التي توزعت وانتشرت بين عدد أكبر من الفاعلين على المستوى الدولي والمحلي، ما جعل الفضاء الإلكتروني مجالا جديدا للصراع بين الدول[2].

وقد جاء دور الفضاء الإلكتروني في تحول الجماعات الإرهابية من الطابع القومي الى طابع عابر للقوميات حيث أصبحت لا تتقيد بحدود الدولة بل أنها تعمل على نطاق عالمي وتسعى إلى التأثير الكوني لاعمالها ومخاطبة الرأي العام، كما وفر التقدم التكنولوجي من وجود افاقا جديدة للعمليات السرية، وتميزت بتعدد الجنسيات المنضوية تحت عمل تلك المنظمات، كما أن تلك المنظمات تعمل من خلال بنيان شبكي لا مركزي، كما أن هناك إمكانية للتنسيق والتجنيد والتعبئة والتمويل عبر شبكات تكنولوجيا الاتصال والمعلومات والهاتف المحمول وأجهزة الكمبيوتر المحمولة والبريد الالكتروني ومواقع الانترنت[3] .

يعتبر الفضاء الإلكتروني مجال افتراضي من صنع الإنسان يعتمد على نظم الكمبيوتر وشبكات الانترنت وكم هائل من البيانات والمعلومات والأجهزة، وهناك من عرف الفضاء الإلكتروني بوصفه الذراع الرابعة للجيوش الحديثة، وهناك من يرى أنه البعد الخامس للحرب، وهذا التعريف يحصر الفضاء الإلكتروني في المجال

العسكري فقط دون التطرق للمجالات الأخرى، وهذا التعريف يركز على الجانب التقني كما يغفل العامل البشري، والذي يعد جزءا أساسيا في فهم الفضاء الإلكتروني[4].

كما جاء تعريف الاتحاد الدولي للاتصالات للفضاء الإلكتروني بأنه: " المجال المادي وغير المادي الذي يتكون وينتج عن عناصر هي: أجهزة الكمبيوتر، الشبكات، البرمجيات، حوسبة المعلومات، المحتوى، معطيات النقل والتحكم، ومستخدمي كل هذه العناصر"[5].

وعليه يمكننا القول بأن: "الفضاء الإلكتروني هو بيئة تفاعلية حديثة، تشمل عناصر مادية وغير مادية، مكون من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشغلين أو مستعملين"[6].

وتجدر الإشارة إلى أن مسألة تحديد مفهوم "الفضاء الإلكتروني"، هي مسألة نسبية تتوقف على طبيعة إدارك وفهم كل من الدول والهيئات كلاً علي حسب رؤيته واستراتيجيته وقدرته على استغلال المزايا المتاحة ومواجهة المخاطر الكامنة في هذا الفضاء.

- **دور الفضاء الالكتروني في تغير مفهوم القوة:**

أصبح الفضاء الإلكتروني أحد 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 جليا أن من يمتلك آليات توظيف البيئة الالكترونية يصبح أكثر قدرة على تحقيق أهدافه والتأثير في سلوك الفاعلين المستخدمين لهذه البيئة[7].

حيث لعب الفضاء الإلكتروني دورا أساسيا في تعظيم القوة، أو الاستحواذ على عناصرها الأساسية في العلاقات الدولية، حيث أصبح التفوق في ذلك المجال عنصرا حيويا في تنفيذ عمليات ذات فاعلية في الأرض، والبحر، والجو، والفضاء، واعتماد القدرة القتالية في الفضاء الإلكتروني على نظم التحكم والسيطرة التكنولوجية[8]

وأدى ذلك الأمر إلى تغيير في مفهوم القوة الوطنية للدولة، فبات بالإمكان تعريفها بأنها مجموعة الوسائل، والطاقات، والإمكانيات المادية وغير المادية، المنظورة وغير المنظورة التي بحوزة الدولة، ويستخدمها صانع القرار في فعل مؤثر يحقق مصالح الدولة، وتؤثر في سلوك الوحدات السياسية الأخرى[9].

- **تحولات القوة وظهور القوة الإلكترونية:**

من الأمور المستقرة في العلاقات الدولية أن 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 والإقناع، ومع ثورة المعلومات ظهر شكل جديد من أشكال القوة وهي القوة الإلكترونية (Cyber power)، التي لها تأثير كبير على المستوى الدولي والمحلي، فمن ناحية أدت إلى توزيع وانتشار القوة بين عدد أكبر من الفاعلين مما جعل قدرة الدولة على السيطرة موضع شك، ومن ناحية أخرى منحت الفاعلين الأصغر قدرة أكبر على ممارسة كل من القوة الصلبة والقوة الناعمة عبر الفضاء الإلكتروني، وهو ما يعني تغيرا في علاقات القوى في السياسة الدولية[10].

وفي غمار هذا التحول، برزت "القوة الالكترونية"، حيث يعرفها **جوزيف ناي** (Joseph S.Nye) بأنها:" القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء الإلكتروني، أي أنها القدرة على استخدام الفضاء الإلكتروني لإيجاد مزايا للدولة، والتأثير على الأحداث المتعلقة بالبيئات

التشغيلية الأخرى وذلك عبر أدوات إلكترونية"، كما يوضح جوزيف ناي أن مفهوم القوة الإلكترونية يشير إلى "مجموعة الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات والشبكات الالكترونية والبنية التحتية المعلوماتية والمهارات البشرية المدربة للتعامل مع هذه الوسائل"[11].

ويتناول مفهوم القوة الإلكترونية مجمل القضايا التي تتعلق بالتفاعلات الدولية الاقتصادية العسكرية والسياسية والثقافية والإعلامية وغيرها.

وترتكز عناصر تلك القوة على وجود نظام متماسك يعظم القوة المتحصلة من التناغم بين القدرات التكنولوجية، والسكانية، والاقتصادية، والصناعية، والقوة العسكرية، وإرادة الدولة، وغيرها بما يسهم في دعم إمكانات الدول على ممارسة الإكراه، أو الإقناع، وممارسة التأثير السياسي في أعمال الدول الأخرى بغرض الوصول للأهداف الوطنية، من خلال قدرات التحكم، والسيطرة على الفضاء الالكترونى[12].

فقد أعطت القوة الالكترونية دفعا رئيسيا في اتجاهين الأول: تدعيم القوة الناعمة للدول حيث بات الفضاء الإلكتروني مسرحا لشن هجمات تخريبية ترتبط بنشر المعلومات المضللة، والحرب النفسية، والتأثير في توجهات الرأي العام، والنشاط السري والاستخباراتي، أما الاتجاه الآخر، فيتعلق بتبني الدول لزيادة الإنفاق في سياسات الدفاع الإلكتروني، وحماية شبكاتها الوطنية من خطر التهديدات، وبناء مؤسسات وطنية للحماية الإلكترونية[13].

- **الفواعل في مجال القوة الإلكترونية:**

يحدد **جوزيف ناي** ثلاثة أنواع من الفاعلين الذين يمتلكون القوة الإلكترونية[14]:

1- **الدول:** والتي لديها قدرة كبيرة على تنفيذ هجمات إلكترونية وتطوير البنية التحتية وممارسة السلطات داخل حدودها.

2- **الفاعلون من غير الدول:** ويستخدم هؤلاء الفاعلون القوة الإلكترونية لأغراض هجومية بالأساس، إلا أن قدرتهم على تنفيذ أي هجوم إلكتروني مؤثر تتطلب مشاركة ومساعدة أجهزة استخباراتية متطورة، ولكن يمكنهم اختراق المواقع الالكترونية واستهداف الانظمة الدفاعية.

3- **الأفراد (القراصنة)** : 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 كالتالي[15]:

- **الشركات متعددة الجنسيات:**

تمتلك بعض شركات التكنولوجيا موارد للقوة تفوق قدرة بعض الدول، ولا تنقصها سوى شرعية ممارسة القوة التي مازالت حكرا على الدول، فخوادم شركات مثل: **جوجل**Google **وفيسبوك** Facebook ، **وميكروسوفت** Microsoft تسمح لها بامتلاك قواعد البيانات العملاقة التي من خلالها تستكشف وتستغل الأسواق، وتؤثر في اقتصاديات الدول وفي ثقافة المجتمعات وتوجهاتها، وهذا ما حدث في الأزمة بين شركة جوجل والصين حول المحتوى، أو فضيحة تسريب بيانات مستخدمي فيسبوك لصالح شركة" كامبردج أناليتيكا" التي تم الاستعانة بها لصالح حملة المرشح الجمهوري ترامب.

- **المنظمات الإجرامية :**

تقوم هذه المنظمات الإجرامية بعمليات القرصنة الإلكترونية، وسرقة المعلومات واختراق الحسابات البنكية وتحويل الأموال، كما توجد سوق سوداء على الانترنت المظلم Dark internet لتجارة المخدرات والأسلحة والبشر، حيث تكلف هذه الجرائم الإلكترونية مليارات الدولارات سنويا.

- **الجماعات الإرهابية**[16]

تعد من أبرز الفواعل الدولية، خاصة بعد أحداث 11سبتمبر، حيث تستغل الفضاء الإلكتروني 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 إلكتروني حقيقي على منشآت البنية التحتية للدول.

- **الأفراد:**

أصبح الفرد بفضل الفضاء الإلكتروني فاعلا مؤثرا في العلاقات الدولية، ومن أبرز النماذج ظاهرة **الويكيليكس** Wikileaks" "الذي نجح في نشر ملايين الوثائق السرية وقنصلياتها للإدارة الأمريكية، مما خلق مشاكل دبلوماسية بين الولايات المتحدة الأمريكية وحلفائها.[17]

ثانيا: أثر الفضاء الالكتروني علي طبيعة الصراعات في العلاقات الدولية:

تعرضت ظاهرة الصراع إلى تغيرات مع بروز الفضاء الإلكترونى، كمجال تنشأ فيه نزاعات بين الفاعلين المختلفين، خاصة مع الاعتماد الكثيف على تكنولوجيا الاتصال والمعلومات، وهنا ظهر الصراع الإلكتروني كحالة من التعارض في المصالح والقيم بين الفاعلين، سواء أكانوا دولا أم غير دول في الفضاء الإلكترونى.

وبرغم الآثار المدمرة لهذا النمط من الصراعات، فلا يرافقه دماء، وقد يتضمن التجسس والتسلل إلى مواقع الخصوم الإلكترونية وقرصنتها دون أنقاض، أو غبار، كما أن أطرافه يتسمون بعدم الوضوح، وتنطوي كذلك تداعياته على مخاطر عدة على أمن الدول، سواء عن طريق التخريب، أو استخدام أسلحة الفضاء الإلكتروني المتعددة[18].

ومع انتشار الفضاء الإلكتروني وسهولة الدخول إليه، اتسعت دائرة الصراعات الإلكترونية، وزاد عدد المهاجمين، وباتت هناك حالة من الكر والفر في الهجمات الإلكترونية لتعبر عن الصراع الممتد، ولذا صار الصراع بين الفاعلين المختلفين حول امتلاك أدوات الحماية والدفاع، وتطوير القدرات الهجومية الإلكترونية يستهدف حيازة القوة، والتفوق، والهيمنة، وتعزيز التنافس حول السيطرة والابتكار، والتحكم في المعلومات، وتعظيم القدرات القادرة على زيادة النفوذ والتأثير في المستويين المحلي والدولي[19].

وبما أن المتنازعين يلجئون في الصراعات التقليدية إلى استخدام شتى أنواع أسلحة التدمير الممكنة، فقد انتقلت جبهات القتال بشكل مواز الي ساحة الفضاء الالكتروني، وكان هذا التغيير سببا في اعادة التفكير في حركية وديناميكية الصراع وظهور مايعرف بعصر القوة النسبية والتي أثبتت أن القوة العسكرية قد لا تكفي وحدها لتأمين البنية التحتية للدول، الأمر الذي يخلف اثارا استراتيجية هائلة علي مستوي تركيبة وتوازنات النظام الدولي.[20]

حيث اختصر الفضاء الإلكتروني حاجز الزمان والمكان، وخلق مساحات للتفاعلات الداخلية والدولية في الواقع الافتراضي، ومن ثم، برزت فضاءات جديدة للصراع بأدوات مختلفة، وأنماط جديدة تختلف عن الصراعات التقليدية، بعد أحداث 11سبتمبر 2001 كان الفضاء الإلكتروني ساحة الصراع والقتال بين تنظيم القاعدة والولايات المتحدة، وفي عام2007 جرت العمليات العدائية بين استونيا وروسيا، وهو ما حدث أيضا في 2008 في الحرب بين روسيا وجورجيا، وجاء الهجوم الإلكتروني بفيروس" **ستاكسنت** "على برنامج إيران النووي عام 2010 ليبرز قوة الأسلحة الإلكترونية في الصراعات الدولية.[21]

برزت فضاءات جديدة للصراع بأدوات مختلفة، وأنماط جديدة تختلف عن الصراعات التقليدية وتعود أسباب اهتمام الفاعلين، سواء كانوا من الدول، أم غيرها، بهذا الفضاء، كمجال لتحقيق البيئة، وتنفيذ الأهداف، وإدارة الصراعات، إلى امتلاكه عدة **سمات أساسية، من أبرزها مايأتي**[22]:

1- **ساحة صراع افتراضية:** أي أنه ليس له مساحة جغرافية، لذلك يتخطى الفضاء الإلكتروني العديد من الثنائيات التي تظهر في الصراعات التقليدية، حيث يشارك في الصراعات ذات الطبيعة الإلكترونية المدنيون والعسكريون، كما ترتبط أيضا بالتطورات المادية السياسية والعسكرية على الأرض، كما أنها أقل تكلفة، من حيث الخسائر المادية، وأكثر تحديدا للهدف، مقارنة بنظيراتها التقليدية.

2- **زيادة الاعتماد الإلكتروني:** إذ باتت الدول الحديثة تربط بنيتها التحتية بالفضاء الإلكتروني، خاصة شبكات الكهرباء والمياه، والبنوك، والبورصة، والاتصالات، وغيرها بالإضافة إلى أنظمة السيطرة والتحكم العسكرية، وجمع المعلومات، مثل الأقمار الصناعية والطائرات دون طيار في الحروب للدولة ذات الطابع الإلكتروني أحد عوامل الصراع الإلكترونى[23].

3- **تماهي حدود الداخل والخارج:** اي وجود حالة من التأثير الشبكي المتزايد داخل الدول وخارجها، حيث أن الصراع يجري في بيئة متحركة قد تغير من طبيعته واتجاهاته، خاصة مع اتساع استخدام الافراد والجماعات والدول للتكنولوجيا الحديثة المرتبطة بالفضاء الإلكتروني سواء كانت مواقع تواصل اجتماعي ام هواتف ذكيه ام مواقع عامة للتعاملات المالية والتجارية والخدمية، ويتصل كل ذلك بشبكة الانترنت مما يجعل الخدمات والمعلومات متاحة للجميع، الأمر الذي قد يعرضها للاستهداف.

4- **صعوبة الردع الالكتروني:** كون الفضاء الإلكتروني ساحة افتراضية بالتالي يصعب علي الدول وضع حدود لسيادتها عليه ومع ضعف القوانين الدولية للسيطرة علي هذا الفضاء، يغيب الردع في ظل

امكانية التنكر علي شبكة الانترنت ومجهولية مصدر الهجمات الالكترونية وسهولة ان يقوم بها الأفراد وليس الدول فقط[24].

5- **غياب الشفافية الالكترونية:** فمع عدم القدرة علي معرفة هويات القائمين علي هجمات القرصنة، نشبت معضلة غياب الشفافية والقوانين المقيدة للصراعات في المجال الالكتروني، بالاضافة الي صعوبة التمييز بين طبيعة الأطراف المتنازعة.

ولعل أبرز ما يعزز انتشار الأنشطة غير السلمية في الفضاء الإلكتروني ما يلي) [25]:

1- ارتباط العالم المتزايد بالفضاء الإلكتروني وزيادة خطر تعرض البنية التحية الكونية للمعلومات لهجمات إلكترونية.

2- استخدام الفاعلين من غير الدول للفضاء الإلكتروني لتحقيق أهدافهم وتأثير ذلك على سيادة الدولة.

3- انسحاب الدولة من قطاعات إستراتيجية لصالح القطاع الخاص.

4- اشكالية تعامل الدول مع الشركات التكنولوجية متعدية الجنسيات، والتي أصبحت تفوق قدراتها، مثل مواقع التواصل الاجتماعي كالفيسبوك وتويتر واليويتوب الذين أصبحوا فاعلين دوليين بامتياز.

وبالتالي أصبح الفضاء الإلكتروني ساحة جديدة للصراع بشكله التقليدي ولكنه ذو طابع إلكترونى يعكس النزاعات التي تخوضها الدول أو الفاعلين من غير الدول على خلفيات دينية أو يديولوجية أواقتصادية أو عرقية أو سياسية، ويتمدد الصراع الإلكتروني بداخل شبكات الاتصال والمعلومات متجاوزا الحدود التقليدية وسيادة الدول.

وكشف استخدام الفضاء الإلكتروني 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 **أنواع للصراع الإلكتروني منها**[26]:

- **صراع إلكترونى تحركه دوافع سياسية**، ويأخذ شكلا عسكريا، ويتم فيه استخدام قدرات هجومية ودفاعية عبر الفضاء الإلكتروني بهدف افساد النظم المعلوماتية والشبكات والبنية التحتية.
- **ويوجد صراع إلكتروني ذو طبيعة ناعمة**، حول الحصول على المعلومات والتأثير في المشاعر والأفكار وشن حرب نفسية واعلامية.
- **كما يأخذ الصراع الإلكتروني طابعا تنافسيا** حول الاستحواذ على سبق التقدم التكنولوجي وسرقة الأسرار الاقتصادية والعلمية، والتحكم بالمعلومات، والعمل على اختراق الأمن القومى للدول، كهجمات قراصنة الكمبيوتر والتجسس بما يكون له من تأثير على تدمير الاقتصاد والبنية التحتية بنفس القوة التي قد يسببها تفجير تقليدي مدمر.

ويمكن أن يستخدم الفضاء الإلكتروني كوسيلة من وسائل الصراع داخل الدولة بين مكوناتها، على أساس طائفي أو اقتصادي أو ديني ونتيجة زيادة التهديدات والمخاطر في الفضاء الإلكتروني التي تواجه الدول ظهر مفهوم الأمن الإلكتروني[27].

- **ثالثا: أثر الفضاء الالكتروني علي مفهوم الأمن في العلاقات الدولية:**

فقد ارتبط ظهور الأمن الإلكتروني بظهور الهجمات الإلكترونية والتي حدثت بسبب عاملين أساسين:

- **الأول:** باستحداث أجهزة الكمبيوتر في منتصف الخمسينيات من القرن المنصرم كأداة لمعالجة وحفظ المعلومات رقمياً(Digital) ، رافقه تضافر جهود عدد من الشركات الخاصة والعامة، توج بتطوير وحدة المعالجة المركزية(CPU) ، وذلك لتسهيل المهام الموكلة له، وقد تطور ذلك بصورة جذرية في العقود اللاحقة، حتى أصبح جهاز الكمبيوتر أساساً في عمل الكثير من المؤسسات الخاصة والعامة، فضلاً عن الحياة اليومية.
- أما **الثاني:** فهو ظهور الشبكة العنكبوتية(الإنترنت)، الذي أحدث انقلاباً مثيراً في حياة البشرية من خلال التواصل ونقل المعلومات بسرعة فائقة، وقد سارعت الدول في وتيرة استخدام الكمبيوتر لتحقيق قفزات نوعية في المجال الأمني والعسكري في مطلع التسعينيات من القرن المنصرم، وذلك حتى أطلق البعض عليها مصطلح الحرب الإلكترونية الباردة (Cyber Cold War) أو سباق التسلح الإلكتروني[28](Cyber arms race).

ويعرف الأمن الإلكتروني بأنه أمن الشبكات والأنظمة المعلوماتية، والبيانات، والمعلومات، والأجهزة المتصلة بالانترنت، وعليه فهو المجال الذي يتعلق بإجراءات، ومقاييس، ومعايير الحماية المفروض اتخاذها، أو الالتزام بها، لمواجهة التهديدات، ومنع التعديات، او على الأقل الحد من آثارها[29].

- **طبيعة العلاقة بين الأمن والتكنولوجيا:**

تزايدت العلاقة بين الأمن والتكنولوجيا، خاصة مع إمكانية تعرض المصالح الاستراتيجية للدول إلى أخطار وتهديدات، الأمر الذي حول الفضاء الإلكتروني لوسيط ومصدر لأدوات جديدة للصراع الدولي وفرضت تلك التطورات إعادة التفكير في مفهوم الأمن القومي للدولة، والذي يعنى بحماية قيم المجتمع الأساسية، وإبعاد

مصادر التهديد عنها، وغياب الخوف من خطر تعرض هذه القيم الهجوم، وبات توافر أمن الفضاء الإلكتروني يتحقق حال وجود إجراءات الحماية ضد التعرض للأعمال العدائية، والاستخدام السيئ لتكنولوجيا الاتصال والمعلومات[30].

وعنى ذلك الأمن الإلكتروني بعملية وضع المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى ايدى أشخاص غير مخولين بها عبر الاتصالات، ولضمان أصالة وصحة هذه الاتصالات[31].

بيد أن طبيعة ذلك الفضاء، كساحة عالمية عابرة لحدود الدول، جعل الأمن الالكتروني يمتد من داخل الدولة إلى النظام الدولي ليشكل نوعا من الأمن الجماعي العالمي، خاصة مع وجود مخاطر تهدد جميع الفاعلين في مجتمع المعلومات العالمي لذا، أصبحت هناك مصلحة قطرية، وكذلك دولية، في الحفاظ على أمن الفضاء الإلكتروني، على أساس أن الأخير صار جزءا من الأمن القومي، ودعم ذلك الطبيعة المتغيرة للتفاعلات الإلكترونية، خاصة مع تطور القدرات البشرية على إنتاج تقنيات جديدة، فضلا عن تصاعد مخاطر التهديدات الإلكترونية على البنية التحتية الكونية للمعلومات[32].

- **أبعاد الأمن الإلكتروني:**

يطال الأمن الإلكتروني جميع المسائل العسكرية، الاقتصادية، والاجتماعية، والسياسية، والإنسانية، بهدف تحقيق منظومة أمن متكاملة تعمل على الحفاظ على الأمن القومي للدولة من كل التهديدات الإلكترونية، وعليه لابد من توضيح أبعاد الأمن الإلكتروني، والتي نوردها كالآتي[33]:

– **البعد العسكري:** يكمن في الحفاظ على قدرة الوحدات العسكرية على التواصل عبر الشبكات العسكرية، مما يسمح بتبادل المعلومات والأوامر وتدفقها ، وإصابة الأهداف عن بعد، إلا أنها تمثل

كذلك نقطة ضعف، خاصة إذا لم تكن مؤمنة جيدا من الاختراق، الذي قد يؤدي إلى تدمير قواعد البيانات العسكرية، أو قطع الاتصال بين القيادة والوحدات العسكرية، فضلا عن إمكانية التحكم في بعض الأسلحة وخروجها عن السيطرة (طائرات بدون طيار، صواريخ موجهة، أقمار صناعية...إلخ)، ويعتبر فيروس ستاكسنت Stuxnet بداية لاستعمال القوة الإلكترونية لتدمير البنية المادية (هاجم حواسيب أجهزة الطرد المركزي الإيرانية).[34]

– **البعد الاقتصادي:** أصبح الانترنت أساسا للمعاملات التجارية والمالية والاقتصادية، كما تستعمل الحواسيب في تسيير وتطوير الصناعات وتحريك الاقتصاد، وأصبح الكل مترابطا عبر شبكات الكمبيوتر، مما يستدعي الحديث عن أهمية تحقيق الأمن الإلكتروني في المجال الاقتصادي.

– **البعد الاجتماعي** [35]تسمح طبيعة الإنترنت المفتوحة عبر المدونات والشبكات الاجتماعية بشكل خاص لكل مواطن بأن يعبر عن تطلعاته السياسية وطموحاته الاجتماعية، حيث تمثل مشاركة جميع شرائح المجتمع فرصة للاطلاع على الأفكار والمعلومات المختلفة وبما تكونه من حاجة لدى المجتمع في الحفاظ على استقرار الفضاء الإلكتروني والمجتمع الذي يرتكز إليه، لكن في المقابل يعرض أخلاقيات المجتمع للخطر، نظراً لصعوبة مراقبة محتوى الإنترنت، كما يعرض الهويات لعمليات اختراق خارجي مما قد يتسبب في تهديد السلم الاجتماعي للدولة، وعليه فلابد من العمل على توعية المواطن بهذه المخاطر لتحقيق الأمن الإلكتروني في بعده الاجتماعي.

– **البعد السياسي:** يعد التدخل الروسي الإلكتروني في الانتخابات الأمريكية أبرز دليل على ضرورة وأهمية الأمن الإلكتروني في بعده السياسي، إضافة إلى التسريبات للوثائق الحساسة والاختراقات التي

غالبا ما تؤدي إلى أزمات دبلوماسية بين الدول، كما أن الفضاء الإلكتروني أصبح بيئة خصبة للحملات الانتخابية والدعاية لمختلف الفاعلين الدوليين.[36]

– **البعد القانوني:** إن التطورات التكنولوجية المتسارعة، تفرض مواكبة التشريعات القانونية لها، من خلال وضع أطر وتشريعات للأعمال القانونية وغير القانونية في الفضاء الإلكتروني، فالملاحظ أن الجريمة الإلكترونية تفتقد في معظم الحالات والبلدان أطرا قانونية صارمة للتعامل معها، إضافة إلى ضرورة تفعيل التعاون الدولي المشترك لمكافحتها.[37]

ويتميز الأمن الإلكتروني بمجموعة من **الخصائص منها:**

- طابع متعدد التخصصات الاجتماعية والتقنية.
- كونه شبكة خالية من الحجم، اضافة الي أن قدرات الفاعلين يمكن أن تكون مماثلة على نطاق واسع.
- درجة عالية من التغيير والترابط وسرعة التفاعل[38].

كما أن تراجع سيادة الدولة مع تصاعد دور الفاعلين من غير الدول في العلاقات الدولية (مثل الشركات التكنولوجية العابرة للحدود، وشبكات الجريمة، والقرصنة الإلكترونية، والجماعات الإرهابية وغيرها) فرض تحديات عديدة في الحفاظ على الأمن الالكتروني العالمي، ودفع ذلك إلى بروز اتجاهات تعددية لتحقيق ذلك الأمن عبر التنسيق بين أصحاب المصلحة من الحكومات والمجتمع المدني، والشركات التكنولوجية، ووسائل الإعلام، وغيرها.

الخاتمة:

يمكن القول أن ثورة المعلومات وما صاحبها من التطور في التكنولوجيا والتقنيات الحديثة في ظل العصر الرقمي أدت الي ظهور تحولات في طبيعة التهديدات للأمن القومي أبرزها الارهاب الالكتروني

واستغلاله لبعض الثغرات الموجودة في الفضاء الإلكتروني، ويعتبر من بين التهديدات التي لا تقل خطورة ومساسا بالأمن القومي للدول، الذي قد طرأ عليه الكثير من التعديل والتغيير، على مستوى التهديدات، الفاعلين، والقطاعات، فبعد أن بدأ عند الواقعيين محصورا في الدولة والقوة العسكرية، توسع في مفهومه الشامل، ليعم جميع مجالات الحياة، مركزا على أمن الافراد والمجتمعات، وظهور العصر الرقمي بفضل ثورة المعلومات والاتصالات، فالكل مرتبط بالشبكة، مما خلق فضاء جديدا للتفاعل، هو الفضاء الإلكتروني، الذي بدوره أحدث تغييرا في مفاهيم العلاقات الدولية، كمفهوم القوة والصراع والحرب، حيث انتشرت القوة بين الفاعلين، وتحول الصراع من المادي الى الافتراضي، وأصبحت الحروب تخاض بالاصفار والآحاد، وبدا واضحا أن الدول تتجه نحو عسكرة الفضاء الإلكتروني، مما نتج عنه ظهور فكلما زاد التشابك، زادت تهديدات جديدة تتزايد في الحجم والشدة، وتشكل تهديدا خطيرا للأمن القومي، التهديدات الإلكترونية، وأثر ذلك على الأمن القومي، مما عجل بظهور مفهوم جديد هو الامن الإلكتروني، بأبعاده المختلفة، والذي تحاول الدول من خلاله الحد من المخاطر والتهديدات في الفضاء الإلكتروني، فالجريمة والارهاب والحرب في الفضاء الإلكتروني تعد من بين التحديات الأمنية الجديدة أمام الدول.

ولذا فقد خلصت الدراسة لعدة نتائج:

1- أصبح الفضاء الالكتروني أحد العناصر الأساسية التي تؤثر في النظام الدولي، بما يتيحه من أدوات تكنولوجية مهمة لعمليات الحشد والتعبئة في العالم، فضلا عن التأثير في القيم السياسية.

2- الفضاء الالكتروني أصبح مجالا للتفاعلات الصراعية الدولية، حتي في ادارة الأسلحة التقليدية، التي تستهدف البنية التحتية المدنية المرتبطة بالفضاء الالكتروني، والذي يربط الشبكات الحيوية للدولة عبر

نظم اتصال قد تستهدفها الهجمات الالكترونية، بجانب تهديد البني التحتية العسكرية، وسرقة المعلومات العسكرية أو التلاعب بها، واختراق أنظمة التحكم والسيطرة والحرب النفسية الالكترونية علي العدو.

3- أن من يمتلك آليات توظيف البيئة الالكترونية يصبح أكثر قدرة على تحقيق أهدافه والتأثير في سلوك الفاعلين المستخدمين لهذه البيئة.

4- ظهور القوة الالكترونية منحت الفاعلين الأصغر قدرة أكبر على ممارسة كل من القوة الصلبة والقوة الناعمة عبر الفضاء الالكتروني، وهو ما يعني تغيرا في علاقات القوى في السياسة الدولية.

5- يأخذ الصراع الالكتروني طابعا تنافسيا حول الاستحواذ على سبق التقدم التكنولوجي وسرقة الأسرار الاقتصادية والعلمية، والتحكم بالمعلومات، والعمل على اختراق الأمن القومى للدول، كهجمات قراصنة الكمبيوتر والتجسس بما يكون له من تأثير على تدمير الاقتصاد والبنية التحتية بنفس القوة التي قد يسببها تفجير تقليدي مدمر.

6- مفهوم الأمن القومي قد طرأ عليه الكثير من التعديل والتغيير، على مستوى التهديدات، الفاعلين، والقطاعات، فبعد أن كان محصورا عند الواقعيين في الدولة والقوة العسكرية، توسع في مفهومه الشامل، ليعم جميع مجالات الحياة.

الهوامش:

1) عبد القادر جعيجع،زهرة تيغزة، تطور الإرهاب وانعكاسه على استقرار المجتمعات: قراءة في ظاهرة الإرهاب الإلكتروني وإستراتيجيات المواجهة، **دفاتر السياسة والقانون**، جامعة الجزائر، الجزائر، المجلد 13، العدد 1 ،2021، ص ص 544-556.
2) سليم دحماني، "أثر التهديدات "السيبرانية" على الأمن القومي الولايات المتحدة الأمريكية – أنموذجا –(2001-2017)"، **رسالة ماجيستير**، كلية الحقوق والعلوم السياسة، جامعة محمد بو ضياف، المسيلة، 2018م، ، ص22.
3) عادل عبد الصادق، "أثر الارهاب الالكتروني علي مبدأ استخدام القوة في العلاقات الدولية2001-2007"، **رسالة ماجيستير**، كلية الاقتصاد والعلوم السياسية، جامعة القاهرة،2009م، ص 70.
4) عباس بدران، الحروب الالكترونية: الاشتباك في عالم متغير، **مركز دراسات الحكومة الالكترونية**، بيروت،2010، ص4.
5) The International Télécommunication Union, **ITU Toolkit for CybercrimeLégislation**, Geneva, 2010, P 12

6) سليم دحماني، **مرجع سابق ذكره**، ص23.
7) اسماعيل زروقة، الفضاء الإلكتروني والتحول في مفاهيم القوة والصراع"، **مجلة العلوم القانونية والسياسية**, المجلد 10، العدد1، ص1016-1031، 2019م
8) Arsenio T. Gumahad, **Cyber Troops and Net War: The Profession of Arms in the Information Age**, War College Series, United States, 2015, pp 57-156.
9) عادل عبد الصادق، أنماط الحرب السيبرانية وتداعياتها علي الأمن العالمي، **مجلة السياسة الدولية**، العدد 208، أبريل2017.
10) اسماعيل زروقة، **المرجع سابق** ، ص 1018.
11) Joseph S.Nye JR , **Cyber Power**, Harvard Kennedy School, 2010, P 03, 04.
12) عادل عبد الصادق، الفضاء الإلكتروني والتحول في سياسات أجهزة الاستخبارات الدولية، **دراسات استراتيجية**، العدد ٢٤٧، 2013، ص ص 10- 12.
13) عادل عبد الصادق، "أنماط الحرب السيبرانية وتداعيتها علي الأمن العالمي"، **مرجع سابق.**
14) سليم دحماني، **مرجع سابق ذكره**، ص25.
15) ايهاب خليفة،**القوة الالكترونية وأبعاد النحول في خصائص القوة**، مكتبة الاسكندرية،مصر، ،2014ص33-42.
16) ايهاب خليفة،القوة الالكترونية وأبعاد النحول في خصائص القوة، **المرجع السابق ذكره**،ص35
17) اسماعيل زروقة، **مرجع سابق** ، ص 1020.
18) عادل عبد الصادق، "أنماط الحرب السيبرانية وتداعيتها علي الأمن العالمي" ، **مجلة السياسة الدولية**، العدد 208 ، ابريل، 2017م
19) عادل عبد الصادق، "أنماط الحرب السيبرانية وتداعيتها علي الامن العالمي"،**المرجع السابق**، ص33.
20) عادل عبد الصادق، "هل يمثل الارهاب الالكتروني شكلا جديدا من أشكال الصراع الدولي"،ملف الاهرام الاستراتيجي، **مركز الدراسات السياسية والاستراتيجية**، جريدة الأهرام، العدد 156، ديسمبر 2007.
21) سليم دحماني، **مرجع سابق ذكره**، ص27.
22) سماح عبد الصبور، " الصراع السيبراني.. طبيعة المفهوم وملامح الفاعلين، **مجلة السياسة الدولية**، العدد 208، المجلد 52، ابريل، 2017م.
23) سماح عبد الصبور، ،**المرجع السابق** ،ص5.
24) ايهاب خليفة، إمكانيات تحقيق الردع في صراعات الفضاء الالكتروني ، **دورية اتجاهات الأحداث**، العدد 13، 2015م.
25) عادل عبد الصادق، **أسلحة الفضاء الالكتروني في ضوء القانون الدولي**، سلسلة أوراق، العدد 23، مكتبة الاسكندرية، القاهرة، 2016، ص17-18
26) عادل عبد الصادق، أنماط الحرب السيبرانية وتداعيتها علي الأمن العالمي"، **مرجع سابق ذكره**.ص34.
27) اسماعيل زروقة، **مرجع سابق ذكره**، ص 1021.
28) فارس قرة ، الأمن السيبراني، **الموسوعة السياسية**، تاريخ الدخول 2021/9/23م، علي الرابط: https://political-encyclopedia.org/dictionary/
29) منى الأشقر جبور، **السيبرانية هاجس العصر**، المركز العربي للبحوث القانونية والقضائية، بيروت،2017، ص25.
30) مصطفى علوى، مفهوم الأمن في مرحلة ما بعد الحرب الباردة، **مركز الدراسات الأسيوية**، كلية الاقتصاد والعلوم السياسية، القاهرة ٢٠٠٤،ص١٤.
31) Martin C. Libicki, **Conquest in Cyberspace: National Security and Information Warfare**, Cambridge University Press, New York, 2007, pp 1-14
32) Morgane Fouch, Robert Macrae and Jon Danielsson, "Could a Cyber Attack Cause a Financial Crisis?" **World Economic Forum** (13 June 2016), online e-article, https://www.weforum.org/agenda/06/2016/could-a-cyber-attack-cause-a-financial-crisis
33) عادل عبد الصادق، القوة الالكترونية: اسلحة الانتشار الشامل في عصر الفضاء الالكتروني، **مجلة السياسة الدولية**، العدد 188، مؤسسة الأهرام، مصر، 2012 ،ص 32
34) محمد مختار،"الأمن السيبراني "، **مفاهيم المستقبل**، اتجاهات الأحداث ، العدد2015،6، ص6.
35) فارس قرة ، الأمن السيبراني، **مرجع سابق ذكره**.
36) اسماعيل زروقة، **مرجع سابق ذكره**، ص 1023.
37) سليم دحماني، **مرجع سبق ذكره**،ص32,
38) فارس قرة ، الأمن الإلكتروني، **مرجع سابق ذكره**.