حروب الفضاء الإلكترونية وتأثيرها في الصراعات الدولية

Cyberspace Wars and their Impact on International Conflicts

https://aif-doi.org/AJHSS/106605

الباحث: د. حسين حسين صالح سميع*

*باحث سياسي في مركز الدراسات والبحوث اليمني

نائب رئيس دائرة البحوث السياسية

الملخص

هدفت الدراسة إلى معرفة طبيعة الفضاء الإلكتروني ومكوناته وتأثيره في الصراعات الدولية والذي يُعد ميداناً شاملاً للحروب الإلكترونية والتعرف على الحروب الإلكترونية، وأنواعها وآليات عملها وأثرها في الصراعات الدولية، ومعرفة النماذج التطبيقية لتلك الصراعات الإلكترونية، وقد اعتمدت الدراسة علي التكامل المنهجي فقد اعتمد ت علي اكثر من منهج كمنهج دراسة الحالة والمنهج التحليلي والمنهج القانوني، وقد تضمنت الدراسة ثلاثة مباحث: الأول منها : طبيعة الفضاء الإلكتروني ومكوناته ودوره في تغيير مفاهيم القوة، **والثاني:** الحروب الإلكترونية وآليات عملها وأنواعها وخصائصها، والأخير منها: أثر الحروب الإلكترونية في الصراعات الدولية، وقد خلصت الدراسة إلى عدة نتائج أهمها:

- الفضاء الإلكتروني فرض نفسه كبعد استراتيجي جديد في الصراعات الدولية، والذي بدوره أحدث تغييرات في مفاهيم العلاقات الدولية، كمفهوم القوة والصراع والأمن.
- الفضاء الإلكتروني أصبح أحد العناصر المهمة التي تؤثر في النظام الدولي بما ينتجه من أدوات تكنولوجية مهمة لعملية الحشد والتعبئة في العالم والتأثير في القيم السياسية.
- أخذ الصراع الإلكتروني طابعاً تنافسياً وهو ما يطلق عليه (سباق التسلح الإلكتروني والمعلوماتي) وفي شتى الميادين (السياسية والاقتصادية والعسكرية) وغيرها بين دول العالم.
- ظهور مراكز قيادة عالية التكاليف تهتم بالجيوش الإلكترونية على مستوى العالم تقيم فيها المناورات والتدريبات على هذا النوع الجديد من الصراعات، وكيفية مواجهاتها والاستعداد لها من خلال تطوير الإجراءات المضادة.

الكلمات المفتاحية: الفضاء الإلكتروني- الصراعات الدولية - القوة الإلكترونية - الحروب الإلكترونية - الجيوش الإلكترونية.

Abstract

The study aimed to find out the nature of cyberspace, its components and its impact on international conflicts, which is a comprehensive field of

ISSN : 2410-1818

electronic warfare, and to identify electronic wars, their types, mechanisms of action and their impact on international conflicts, and to know the applied models of those electronic conflicts, the study relied on methodological integration, it relied on more than one approach such as the case study method, the analytical method and the legal method. The study included three topics: the first of them: the nature of cyberspace, its components and its role in changing the concepts of power, the second: electronic wars, their mechanisms, types and characteristics, and the last of them: the impact of wars study has concluded several results, the most important of which are:

- Cyberspace has imposed itself as a new strategic dimension in international conflicts, which in turn has brought about changes in the concepts of international relations, such as the concept of power, conflict and security.

-Cyberspace has become one of the important elements that affect the international system by producing important technological tools for the process of mobilization and mobilization in the world and influencing political values.

-The electronic conflict has taken on a competitive character, which is called the (electronic and information arms race) and in various fields (political, economic, military) and others between the countries of the world.

-The emergence of high-cost command centers that are interested in electronic armies worldwide, where maneuvers and trainings are held on this new type of conflict, how to confront them and prepare for them
the development of countermeasures.

***Keywords*:** Cyberspace-International Conflicts-Electronic power - Electronic warfare-Electronic armies.

أولاً: المقدمة

شهد العالم العديد من التحولات ومن أبرز هذه التحولات ثورة التكنولوجيا وثورة المعلومات والقدرة على استخدام التكنولوجيا الحديثة، والتي تعد من أهم الركائز الأساسية للمجتمع في جميع المجالات تحولاً ديناميكياً سريعاً عن طريق الاختراع والإبداع والإنتاج، وأصبح العصر الحالي هو عصر الثورة الرقمية والإلكترونية التي تمارس نشاطها في الفضاء الإلكتروني، وبرزت عدة أشكال جديدة ومتنوعة من القوة الإلكترونية والتي أصبح لها انعكاسات مباشرة على المستوى الدولي والمحلي، وأصبح الفضاء الإلكتروني متغير أساسي وعنصر مؤثر في النظام الدولي، نظرا لما يحمله من أدوات تكنولوجية متطورة جعلت منه أداة مهمة في التأثير على أنماط القوة والأمن والحرب والتي يتم إداراتها عن بعد في الفضاء الإلكتروني مثل الحروب الإلكترونية، والهجمات السيبرانية، والإرهاب الإلكتروني (1).

ISSN : 2410-1818

ومن ناحية أخرى مكنت القوة الإلكترونية بعض الدول الصغرى في السياسة الدولية من قدرة أكبر على ممارسة القوة الصلبة والناعمة عبر استراتيجية جديدة تمثل "القوة الإلكترونية "مصدرها، وهذا أدى إلى تغيير في العلاقات الدولية، واتسمت الحروب الإلكترونية بصفة تدميرية كبرى حيث يستطيع أحد أطراف الصراع أن يوقع خسائر فادحه بالطرف الآخر قد لا تصاحبه دماء أو أشلاء بالضرورة، وقد يتضمن التجسس والتسلل ثم النسف لكن لا دخان ولا أنقاض ولا غبار، وتكون تداعياتها خطيرة سواء عن طريق تدمير المواقع على الانترنت ونسفها وقصفها بوابل من الفيروسات والعمل على استخدام أسلحة الفضاء الإلكتروني المختلفة والمتعددة للنيل من تلك المواقع وهي أسلحة يسهل الحصول عليها من خلال مواقع الإنترنت، وبهذا أفسح الفضاء الإلكتروني عن محاور جديدة للصراع في الصراعات الدولية(2).

ثانياً: المشكلة البحثية.

تنطلق الدراسة من إشكالية مفادها أن حروب الفضاء الإلكتروني نقلت علاقات القوى الدولية والصراعات الدولية إلى مرحلة جديدة تستهدف أهداف معينة التي يمثل الفضاء الإلكتروني ميدانها بنوع أسلحة جديدة تختلف عن الأسلحة التقليدية.

وتكمن المشكلة البحثية للدراسة في الإجابة على السؤال الرئيس وهو إلى أي مدى تتأثر الصراعات الدولية بالحروب الإلكترونية التي يمثل الفضاء الإلكتروني ميدانها؟ ويتفرع من السؤال الرئيس الأسئلة الفرعية الآتية:

- ما طبيعة الفضاء الإلكتروني ومدى تأثيره على مفاهيم القوة؟
- ما هي الحروب الإلكترونية وأهم خصائصها وآليات عملها وأنواعها ومصادرها؟
- هل غيرت الحروب الإلكترونية في وسائل الصراعات الدولية؟
- ما هي النماذج التطبيقية الدولية على الحروب الإلكترونية؟

ثالثاً: فرضية الدراسة.

كلما زاد التطور التكنولوجي كلما زادت الحروب الإلكترونية وقل دور العامل البشرى في إدارة الصراعات الدولية.

ISSN : 2410-1818

رابعاً: أهداف الدراسة:

تهدف الدراسة إلى:

1- التعرف على ماهية الفضاء الإلكتروني ومكوناته الأساسية.
2- معرفة أثر القضاء الإلكتروني في تغيير مفاهيم القوة.
3- ما هي الحروب الإلكترونية وأهم خصائصها وآليات عملها.
4- معرفة أثر الحروب الإلكترونية في الصراعات الدولية.
5- التعرف على الدراسات والنماذج التطبيقية في الصراعات الدولية.

خامساً: أهمية الدراسة.

أ. الأهمية العلمية/ النظرية

تكمن الأهمية العلمية للدراسة فيما تقدمه من معرفة شاملة حول الدراسة على مستوى الدولة أو الفرد أما بالنسبة على مستوى الدولة تكون في تعريف الدولة بخطورة الحروب الإلكترونية وكيفية مواجهاتها والحفاظ على فضاءها الإلكتروني وضرورة تحقيق القوة الإلكترونية في استراتيجيتها.

أما على مستوى الفرد: تكمن الأهمية في توعية الأفراد بأساليب هذه الحروب وخطورتها لأن منها ما يستهدف الشباب من أجل إفسادهم وتغيير هويتهم ومعرفة خطورة هذا النوع من الحروب على الفرد والمجتمع والبحث عن أساليب مواجهتها حتى لا يكون الأفراد الضحية لهذه الحروب.

ب. الأهمية العملية/ التطبيقية

تعد دراسة وفهم الحروب الإلكترونية ذات أهمية بالغة لأن الدول تسعى بطرق متسارعة لامتلاك واعتماد الهجمات الإلكترونية في استراتيجيتها وتكتيكاتها فيما يخص علاقاتها بالدول الأخرى، وبالتالي يجب على الباحثين وصناع القرار العمل من أجل تطوير استراتيجيات تتبنى و توظف الأساليب الحديثة لمواجهة أي هجمات متوقعه في المستقبل.

ساساً – منهج الدراسة

اعتمدت الدراسة على التكامل المنهجي حيث اعتمدت على أكثر من منهج هي:

- منهج دراسة الحالة: وذلك باعتماد الحروب الإلكترونية لتوضيح مدى تأثير هذه الحروب باستراتيجياتها المختلفة ورصد أبرز نماذج هذه الحروب.

- المنهج التحليلي: حيث يقوم هذا المنهج بتحليل البيانات الوصفية موضحا أهم استراتيجيات الحروب الإلكترونية وتفسير دور الحروب الإلكترونية في إدارات التفاعلات والصراعات على الساحة العالمية.

ISSN : 2410-1818

- المنهج القانوني: من خلال توضيح الآليات القانونية الدولية لمجابهة الحروب الإلكترونية.

سابعاً: تقسيم محتويات هذه الدراسة

تحتوي الدراسة على المباحث الآتية:

المبحث الأول: طبيعة ومفهوم الفضاء الإلكتروني ومكوناته وأثره على تغيير مفاهيم القوة.

المبحث الثاني: الحروب الإلكترونية وآليات عملها وأنواعها ومصادرها وشروط استخدامها.

المبحث الثالث: أثر الحروب الإلكترونية في الصراعات الدولية.

المبحث الرابع: الدراسات التطبيقية والنماذج على الحروب الإلكترونية وإمكانات مواجهاتها.

المبحث الأول

الفضاء الإلكتروني مفهومه ومكوناته وأثره في تغيير مفاهيم القوة

مدخل

أفضت الثورة المعلوماتية عن ظهور بيئة جديدة وهي الفضاء الإلكتروني، وهي تختلف عن البيئيات الأخرى سواء البري، البحري، الجوي أو الفضاء الخارجي كونها من صنع الإنسان ولكنها تشترك في بعض السمات والخصائص مع البيئات الأخرى، وأضحي الفضاء الإلكتروني عنصراً مؤثراً في النظام الدولي وفي إدارة التفاعلات الدولية بين الدول وأصبح يلعب دوراً مهماً في الصراعات الدولية وفي موازين القوي وتستخدم العديد من الدول القدرات التي يوفرها الفضاء الإلكتروني لاعتبارات في مقدمتها الأمن والقوة العسكرية، وسيتناول هذا المبحث المطالب الآتية:

المطلب الأول

مفهوم الفضاء الإلكتروني

كان بدء الثورة المعلوماتية في العالم بداية ظهور العالم السيبراني الكبير، والتي ساهمت في إنشاء بيئة للفضاء الإلكتروني بوجود ما يمكن تسميته بالقوة السيبرانية أو القوة الإلكترونية في العالم وذات تأثير مميز، حيث أصبح الفضاء الإلكتروني محل ونقطة الصراع بين الدول، بدلاً عن الأرض مما جعل للفضاء الإلكتروني دوراً فاعلاً على الصعيد المحلي والدولي. وأصبح مجالاً حيوياً يتم من خلاله إدارة التفاعلات الدولية، وتخاض فيه العديد من الحروب والهجمات الرقمية، كما أنه ليس فضاءً حقيقيا بل هو مكانا خياليا وهميا ينشأ من خلال النقر على لوحة مفاتيح الحاسب الآلي(3).

ISSN : 2410-1818

ويعتبر الفضاء الإلكتروني مجالاً افتراضياً من صنع الإنسان يعتمد على نظام الكمبيوتر وشبكات الإنترنت، وكماً هائلاً من البيانات والمعلومات والأجهزة، وهناك من عرف الفضاء الإلكتروني بوصفه الذراع الرابع للجيوش الحديثة، وهناك من يرى أنه يمثل البعد الخامس للحرب، وهذا التعريف يحصر الفضاء الإلكتروني في المجال العسكري وهذا التعريف يركز على الجانب التقني كما يغفل العامل البشري، الذي يعد جزءاً أساسياً في فهم الفضاء الإلكتروني (4).

ويعرف الاتحاد الدولي للاتصالات الفضاء الإلكتروني بأنه: المجال المادي وغير المادي الذي يتكون وينتج عن عناصر هي أجهزة الكمبيوتر، الشبكات، البرمجيات، حوسبت المعلومات، المحتوى، معطيات النقل والتحكم، ومستخدمي كل هذه العناصر وعليه يمكن القول بأن: الفضاء الإلكتروني هو بيئة تفاعلية حديثة، تشمل عناصر مادية وغير مادية مكون من مجموعة من الأجهزة الرقمية، وأنظمة البرمجيات، والشبكات، والمستخدمين سواء مشغلين أو مستعملين. ويمكن تحديد مفهوم **الفضاء الإلكتروني** بأنه: مسالة نسبية تتوقف على طبيعة إدراك وفهم كل من الدول والهيئات كلاً على حسب رؤيته واستراتيجيته وقدراته على استغلال المزايا المتاحة ومواجهة المخاطر الكامنة في هذا الفضاء وبالتالي أصبح الفضاء الإلكتروني يمثل الجيل الرابع من الجيوش الحديثة (5).

المطلب الثاني

مكونات الفضاء الإلكتروني

بعد أن أصبح الفضاء الإلكتروني بما يحمله من أدوات تكنولوجية تلعب دوراً مهماً في الصراعات الدولية فضلاً عن التأثير في القيم السياسية كان لابد من معرفة أهم المكونات الأساسية التي تلعب الدور المهم في مفهوم الفضاء الإلكتروني وهي:

أولاً: الطبقة المادية أو الطبيعية.

- وتشمل البنية التحتية المعلوماتية من معدات الحواسيب والبرمجيات والمعدات الضرورية لعملية الربط بين الفاعلين الدوليين باستخدام تكنولوجيا المعلومات.
- الطبقة المنطقية أو الطبيعية أو المحتوي: وتشمل مجموعة البرامج المترجمة للمعلومات على شكل معطيات رقمية بحيث يتم الانتقال من لغة الإنسان إلى لغة الآلة.
- الطبقة الإعلامية: وتشمل عملية الاتصال بحيث يكون لكل إنسان عدة هوايات رقمية ابتداءً بالعنوان والبريد الإلكتروني وغيره.

ISSN : 2410-1818

ثانياً: مجموعة الفواعل الدولية في مجال القوة الإلكترونية: تعتبر الدولة فاعل أساسي في الفضاء الإلكتروني، ويمكنها اتخاذ الإجراءات القانونية لحماية فضاءها الإلكتروني والتحكم فيه وقد حددّ جوزيف ناي، ثلاثة أنواع من الفاعلين الذين يمتلكون القوة الإلكترونية وهم (6).

1- الدول والتي لديها قدرة كبيرة على تنفيذ هجمات إلكترونية وتطوير البنية التحتية لممارسة الحروب الإلكترونية من داخل حدودها.
2- الفاعلين من غير الدول: ويستخدم هؤلاء القوة الإلكترونية لأغراض هجومية بالأساس، إلا أن قدرتهم على تنفيذ أي هجوم إلكتروني مؤثر تتطلب مشاركة ومساعدة أجهزة استخبارية متطورة، يمكنهم من اختراق المواقع الإلكترونية واستهداف الأنظمة الدفاعية.
3- الأفراد القراصنة: الذين يمتلكون معرفة تكنولوجية والقدرة على توظيفها، وعادة ما تكون هناك صعوبات في الكشف عن هويتهم، ومن الصعب تتبعهم.

الفاعلين من غير الدول: فقد أصبح هناك من يزاحم الدولة في الفضاء الإلكتروني في توجهاتها وإدارتها وفق سياسة معينة وهم.

1- الشركات متعددة الجنسيات: تمتلك بعض شركات التكنولوجيا موارد للقوة تفوق قدرة بعض الدول، ولا تنقصها سواء شرعية ممارسة القوة التي ما زالت حكراً على الدول، مثل شركة جوجل وشركة فيسبوك تسمح لها امتلاك قواعد البيانات العملاقة التي من خلالها تستكشف وتستغل الأسواق، وتؤثر في اقتصاد الدول وفي ثقافة المجتمعات وتوجهاتها، وهذا ما حدث بين شركة جوجل والصين حول المحتوى، أو فضيحة تسريب بيانات مستخدمي فيسبوك، لصالح شركة كمبردج انالتيكا، ، التي تم الاستعانة بها لصالح حملة المرشح الجمهوري ترامب.(7).

2- المنظمات الإجرامية: تقوم هذه المنظمات بعملية القرصنة الإلكترونية، وسرقة المعلومات واختراق الحسابات البنكية وتحويل الأموال، كما توجد سوق سواد على الانترنت المظلم لتجار المخدرات والأسلحة والبشر، حيث تكلف هذه الجرائم الإلكترونية مليارات الدولارات سنويا.

الجماعات الإرهابية (8)

تعد من أبرز الفواعل الدولية، خاصة بعد أحداث 11 سبتمبر2001م، حيث تستغل الفضاء الإلكتروني في عملية التجنيد والتعبئة والدعاية وجمع الأموال والمتطوعين، كما تحاول جمع المعلومات حول الأهداف العسكرية، وكيفية التعامل مع الأسلحة وتدريب المجندين الجدد رغم أنها لم تصل إلى مرحلة القيام بهجوم الكتروني حقيقي على منشأة البنية التحتية للدول.

ISSN : 2410-1818

الأفراد: أصبح الفرد بفضل الفضاء الإلكتروني فاعلاً مؤثراً في العلاقات الدولية، ومن أبرز النماذج ظاهرة (الويكي ليكس) الذي نجح في نشر ملايين الوثائق السرية وقنصلياتها للإدارة الأمريكية، مما خلق مشاكل دبلوماسية بين الولايات المتحدة الأمريكية وحلفائها (9).

ونتيجة تطور التعامل مع الفضاء الإلكتروني من الفواعل الدولية وغير الدولية، أدى ذلك التعامل للاستخدام المفرط من جانب الدول أو غيرها للفضاء الإلكتروني، في أعمال تخدم مصالح المستخدمين وتضر بمصالح الآخرين مما جعله أداة مهمة وفعالة في إدارات التفاعلات بين الفواعل المختلفة وبأشكال **مختلفة سواءً كان إرهاب الكتروني أو حروب إلكترونية.**

المطلب الثالث

دور الفضاء الإلكتروني في تغيير مفهوم القوة الإلكترونية

أصبح الفضاء الإلكتروني أحد العناصر الأساسية التي تؤثر في النظام الدولي، بما يتيحه من أدوات تكنولوجية مهمة لعملية الحشد والتعبئة في العالم، فضلا عن التأثير في القيم السياسية، فسهولة الاستخدام ورخص التكلفة زاد من قدراته على التأثير في مختلف مجالات الحياة، سواء السياسية، والاقتصادية والعسكرية، والاجتماعية وحتى الأيديولوجية وبات جلياً أن من يمتلك آليات توظيف البيئة الإلكترونية يصبح أكثر قدرة على تحقيق أهدافه والتأثير في سلوك الفاعلين المستخدمين لهذه البيئة.

فقد لعب الفضاء الإلكتروني دوراً أساسياً في تعظيم القوة، أو الاستحواذ على عناصرها الأساسية في العلاقات الدولية، حيث أصبح التفوق في مجال الفضاء الإلكتروني عنصراً حيوياً في تنفيذ عمليات ذات فاعلية في الأرض، والبحر، والجو، والفضاء، واعتماد القدرة القتالية في الفضاء الإلكتروني على نظام التحكم والسيطرة التكنولوجية (10).

وأدى ذلك الأمر إلى تغيير مفهوم القوة الوطنية للدولة، فبات بالإمكان تعريفها بأنها (مجموعة الوسائل، والطاقات، والإمكانات المادية وغير المادية المنظورة وغير المنظورة التي بحوزة الدولة، ويستخدمها صانع القرار في فعل مؤثر يحقق مصالح الدولة، وتؤثر في سلوك الوحدات السياسية الأخرى (11).

التحولات في القوة الإلكترونية:

من الأمور المستقرة في العلاقات الدولية أن مصادر قوة الدولة وأشكالها تتغير، فإلى جانب القوة الصلبة ممثلة في القوة العسكرية والاقتصادية، تزايد الاهتمام بالأبعاد غير المادية للقوة، ومن ثم برزت القوة الناعمة التي تعتمد على جاذبية النموذج والإقناع، ومع ثورة المعلومات ظهر شكل جديد من أشكال القوة هي القوة الإلكترونية التي لها تأثير كبير على المستوى الدولي والمحلي، ومن ناحية أدت

ISSN : 2410-1818

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 مما يعني تغير في علاقات القوي في السياسة الدولية. وفي غمار هذا التحول، برزت القوة الإلكترونية حيث يعرفها جوزيف ناي (12)

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 بالبيئة التشغيلية الأخرى وذلك عبر أدوات إلكترونية، كما يوضح جوزيف ناي أن مفهوم القوة الإلكترونية يشير إلى مجموع الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات والشبكات الإلكترونية والبنية التحتية المعلوماتية والمهارات البشرية المدربة للعمال مع هذه الوسائل (13).

ويتناول مفهوم القوة الإلكترونية مجمل القضايا التي تتعلق بالتفاعلات الدولية الاقتصادية العسكرية والسياسية والثقافية والإعلامية وغيرها. وتتركز عناصر تلك القوة على وجود نظام متماسك يعظم القوة المتحصلة من التناغم بين القدرات التكنولوجية، والسكانية، والاقتصادية، والصناعية، والقوة العسكرية، وإدارات الدولة، وغيرها بما يسهم في دعم إمكانات الدولة على ممارسات الإكراه، أو الإقناع وممارسات التأثير السياسي في أعمال الدول الأخرى، بغرض الوصول للأهداف الوطنية، من خلال قدرات التحكم والسيطرة على الفضاء الإلكتروني(14).

فقد أعطت القوة الإلكترونية دافعاً رئيسياً في اتجاهين، الأول: تدعيم القوة الناعمة للدول؛ حيث بات الفضاء الإلكتروني مسرحاً لنشر 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 سياسة الدفاع الإلكتروني، وحماية شبكاتها الوطنية من خطر التهديد، وبناء مؤسسات وطنية للحماية الإلكترونية (15).

المبحث الثاني

الحروب الإلكترونية مفهومها وأنواعها وآليات عملها

مدخل

بفضل ما أحدثته الثورة المعلوماتية من ثورة هائلة في مجال الفضاء الإلكتروني، فقد أصبح الفضاء الإلكتروني يُدار من خلاله التفاعلات الدولية بأسلحة وأدوات مختلفة تماماً عن الأسلحة والأدوات التقليدية، وهنا ظهر مُسمى جديد يُطلق عليه (حروب الفضاء الإلكتروني)، وقد غيرت حروب

ISSN : 2410-1818

الفضاء الإلكتروني من مفهوم وطبيعة الحروب؛ فهي لا تستهدف تدمير الآلات والمعدات العسكرية للعدو أو احتلال الأرض وإنما إلحاق الضرر البالغ بالبنية التحتية للدولة بأقل كُلفة ممكنة. وعليه سيتناول هذا المبحث المطالب الآتية:

المطلب الأول

مفهوم حروب الفضاء الإلكترونية

شكل التطور الإلكتروني الذي شهده عالم التكنولوجيا الرقمية والإلكترونية الكونية تنافسات شديدة بين دول العالم، أدخلتها بما يعرف بالحروب الإلكترونية إذ تتسم هذه الحروب بالصمت والظلام وسرعة الأداء وقوة التأثير وشبهة انعدام معرفة هوية المهاجم والخلفيات الأيديولوجية، والوقت وغيرها من الصفات التي تجعل منها حرباً شديدة الخطورة حرب تخيلية افتراضية ذات طبيعة غير ملموسة تحاكي الواقع، وتعرف الحروب الإلكترونية بأنها: حرب قد تكون بلا دماء، إذ تتلخص أدوات الصراع فيها بالمواجهات الإلكترونية والبرمجيات التقنية وجنود من برامج التخريب المحوسب وطلقاتها لوحة المفاتيح ونقرات المبرمجين في بيئة اصطناعية تحاول ما أمكن الوصول إلى صورة حقيقية لملامح الحياة المادية والملموسة (16).

ويُمكن تعريف الحروب الإلكترونية من النظرة القانونية بأنها: نظام قائم على الرعب المُنتشر في الشبكة العنكبوتية تهدف إلى تنفيذ العديد من الأعمال لترويع أمن الأفراد والجماعات والمؤسسات والدول وإرهاقهم اقتصاديا وإدخالهم في أزمات نفسية واجتماعية ناتجة عما يعرف بالإرهاب الصامت، وينطلق هذا المفهوم من الواقع الغربي، وهي حرب ناعمة صامتة تأخذ أشكالاً عدة كشكل الاتصالات بين الجيوش وقاداتها وإضعاف شبكات النقل والإمدادات اللوجستية وضرب المعلومات الاقتصادية وإحراج الساسة والعبث بالمحتوى الفني والتقني (17).

وقد عرفتها ماريا تاديو، الباحثة في معهد أكسفورد للإنترنت بأنها: حرب تُركز على استخدامات معينة لتكنولوجيا المعلومات والاتصالات ضمن استراتيجية عسكرية هجومية أو دفاعية أقرتها الدولة، وتهدف إلى التعطيل الفوري أو السيطرة على موارد العدو والتي تُشن داخل بيئة المعلومات مع أهداف تتراوح بين الصعيد المادي والمجالات غير المادية، والتي قد يختلف مستوى الدمار فيها حسب طبيعة وحجم الهجوم (18).

فيما عرفت وزارة الدفاع الأمريكية حروب الفضاء الإلكترونية: أنها توظيف القدرات السيبرانية وذلك بهدف تحقيق غرض أساسي، يتمثل في تحقيق الأهداف أو الآثار العسكرية في الفضاء

ISSN : 2410-1818

الإلكتروني أو من خلاله، وبالتالي يُمكن تلخيص مفهوم الحروب الإلكترونية في معناها الإجرائي بأنها:

هي الهجمات التي تشنها بعض الدول ويكون مسرحها هو الفضاء الإلكتروني، بغرض إلحاق الضرر بالمنشآت والبنى التحتية والأهداف العسكرية للدولة التي تعرضت للهجوم، وتتميز حروب الفضاء الإلكتروني بأنها يُمكن أن تكون من فاعلين غير الدول فيكون هناك صعوبة في تحديد العدو والجهة المُهاجمة (19).

وكذلك تعرف الحروب الإلكترونية بأنها: المشهد الصراعي والمستقبلي والقادم للبشرية ولكن بصورة رقمية وتكنولوجية، وهي صراعات قديمة جديدة بدأت منذ الوقت الذي ابتكر فيه الإنسان أدوات تواصله الأولى، كالأصوات والتلغراف والهواتف اللاسلكية، وأنظمة البرق الصوتي وأنظمة الترميز وآلة الطباعة وغيرها التي تم استخدامها في الحربين العالميتين الأولى والثانية (20).

وهناك من يربط مفهوم الحرب الإلكترونية ببيئة الإنترنت فقط؛ كونها ساعدت على انتشار المعلومات في مختلف أرجاء العالم بشكل كبير وسهلت الوصول إليها بشكل سريع بحيث يمكن تعريف الحروب الإلكترونية بناء على ذلك بأنها: الحرب التي تستهدف المعلومات، وهي تعبر عن الاعتداءات التي تطال مواقع البيانات الموجودة على الانترنت وتحاول الاستيلاء على معطياتها بين أطراف متناقضة الأهداف ومتعارضة المصالح ومختلفة المواقف (21).

وقد شهد العقد الأخير تطورات سريعة في مجال الحوسبة وتكنولوجيا المعلومات، بما أفضى إلى تغيرات بعيدة المدى في جميع مجالات الحياة ولا سيما في المجالين الأمني والعسكري، الذين أدخل فيهما العديد من التغييرات التي تتعلق بطريقة القتال وتفعيل القدرات للجيوش الإلكترونية، ويعزى ذلك إلى المستجدات التي طرأت على أنماط التفكير الاستراتيجي وعلى بلورة عقيدة قتالية تتلاءم مع الواقع الإلكتروني، لذلك تعد المجالات العسكرية من أكثر البيئات تجانساً والتصاقاً بالحروب الإلكترونية (22).

وتعرف الحروب الإلكترونية تبعاً لترابطها بالقوة العسكرية بأنها: الحروب التي تتسم بالتعاون مع الحرب العسكرية؛ إذ أنها تصوب نيرانها نحو الأهداف الإلكترونية والرقمية والمعلوماتية كالتجسس على المعلومات والإشارات الصادرة من الأجهزة الإلكترونية التابعة إلى الأهداف المستهدفة، وكذلك تتبع الموجات المطلقة من الاتصالات اللاسلكية وغيرها، إذ تستهدف هذه النيران الإلكترونية المصالح القومية والسياسية والعسكرية والأمنية للدول المستهدفة متخذة شكل هجمات إلكترونية أو اختراقات إلكترونية الهادفة لتعطيل البنية المعلوماتية للدولة المستهدفة (23).

ISSN : 2410-1818

وتقوم الحروب الإلكترونية على عنصرين مهمين في أي صراع الكتروني قد ينشب في الفضاء الإلكتروني هما:

1- توفر المعلومات التي ترتكز عليها الحروب التكنولوجية بشكل كبير حيث إن توفر عنصر المعلومات هو أول آليات عمل الحروب الإلكترونية.

2- القدرات العقلية والذهنية والتي تكون مسؤولة عن تخطيط وتوجيه الضربات الإلكترونية في عالم رقمي شديد التعقيد يتبع توفر عنصري المعلوماتية والقدرات العقلية البشرية والتي تستند إليها آلية عمل الحروب الإلكترونية، الإجراءات الفنية والتقنية القائمة على أساس تنفيذ خطوات وآليات الحروب الإلكترونية عبر الفضاء الرقمي.

المطلب الثاني

أشكال وأنواع الحروب الإلكترونية

لقد غيرت ثورة المعلومات والإنترنت من طبيعة الصراعات والحروب وأضافت أساليب جديدة ومختلفة ومنها الحروب الموجهة، وحرب الشبكات، والحرب التجسسية، والحرب الفضائية، والنفسية، والإعلامية وسيتم مناقشة هذه الحروب بشيء من التفصيل في هذا المطلب على النحو الآتي:

الحروب الموجهة: استند هذا النوع من الحروب على المعلوماتية؛ إذ أنه يكفي لقهر العدو ويتم النجاح باستخدام هياكل القيادة ولديه وسائل الاتصال مع المؤسسات الفكرية، وكذلك تستند هذه الحروب على القنابل الذكية التي استخدمت في حرب الخليج الثانية عام 1991م، وقنابل الغرانيت القادرة على تصفير دوائر المراكز الكهربائية والتي استخدمت أخيراً ضد الصرب في حرب كوسوفو وكذلك القنابل التي استخدمت في الحرب الأمريكية على العراق عام 2003م، إذ أنه في حالة الصراع تصبح المعارك هدفاً للمواجهة وليس فقط ما يتيح الهجوم أو الصدام في الظرف الملائم (24).

وقد كان آخر تطبيق لهذه الحرب عام 2003م في العراق من خلال اعتماد الولايات المتحدة على استراتيجية (الصدمة والترويع)، التي تقوم على قدرة تكنولوجية متطورة ومنظمة تسليحية متكاملة وقادرة على تطبيق التأثير المستهدف من أجل التأثير في إرادة الخصم وإدراكه، وتتطلب هذه الاستراتيجية عدة عناصر لنجاحها هي: المعرفة الكاملة بالذات والخصم والبيئة، ويشمل ذلك معرفة كاملة بالعمليات الذهنية والمنظومات التقنية لقادة الخصم وجماهيره والسرعة في جميع مراحل العمل العسكري سواء في المناورات أو التحركات داخل الميدان وضمان السيطرة على العمليات سواء على الأرض أو في مجال الإشارات اللاسلكية والبنية الأساسية للاتصالات بما يضطر الخصم إلى الاستسلام

ISSN : 2410-1818

خوفا لتعرضه لدمار واسع كما أن الحرب الموجهة تستخدم أكثر الأسلحة ذكاء وتتطلب وجود قوات ووحدات صغيرة ومترابطة لكي تتمكن من تنسيق هجماتها بشكل متكرر، ومن أبرز الدول التي تمتلك هذه القوات هي الولايات المتحدة الأمريكية وفرنسا وكندا وبريطانيا (25).

الحروب التجسسية

أصبح التقدم التقني واحد من أهم مفاتيح المستقبل وعامل حاسم للسيطرة في النظام العلمي الجديد فقد أصبحت المنافسة شديدة في الميدان التكنولوجي والسياسي والاستراتيجي، لأن من يحصل على التكنولوجيا فإنه سيسيطر في المجالات الأخرى؛ لذا يري بعض المحللين الامنين بأن جزاء كبيرا من الاتصالات العالمية تسيطر عليها أجهزة الأمن والأجهزة المخابراتية، إذ أن هذه الأجهزة تراقب كل شيء تقريبا وينتشر وكلاء متخصصون في كل بلدان العالم مدعومون بأقمار صناعية تجسسية لجمع المعلومات والعمل مع الآلاف من الإذاعات والقنوات، وكل ذلك يتجه لهدف واحد ألا وهو التجسس على العالم، فالوكالات الأمنية تنتشر في كل بلدان العالم وتسعي وتتنافس وبكل الطرق للحصول على المعلومات مستخدمة كل الوسائل المتاحة بعملية تصارع أشبه بالحرب ذاتها من هنا انطلقت حرب التجسس هذه، فالدول تسعى لإنفاق ثرواتها على قواعدها التنصتية ونصب وسائل ذات تقنية عالية الكفاءة للتجسس على العالم (26).

حروب الشبكات: وهو شكل جديد من أشكال الحروب التي تمكن من التأثير على نشاطات وأعمال الخصم.

إذا كان مجتمع الخصم متطورا ويعتمد بدرجة كبيرة على وسائل المواصلات والاتصالات، أما إذا كان أقل تطورا في اعتماده بالتقنيات الحديثة فإن أساليب حروب الشبكات كالفعاليات التقنية والتشويش لم يكن مؤثر بالدرجة المطلوبة، ومن ثم سيتم الاعتماد على الأسلحة التقليدية والتي تعتمد على الدقة في الإصابة والسرعة في الاستجابة؛ لذا فإن حروب الشبكات موجهة بشكل أساسي نحو تحجيم العدو، ومن ثم هي تختلف عن الحرب الموجهة التي تكون نحو شل قدرات العدو(27).

الحروب الفضائية:

سعت الولايات المتحدة الأمريكية في عام 1983م لتطوير برنامج حرب النجوم أو منظومة الدفاع الاستراتيجي وامتلاك القدرات المطلقة على صد أي هجوم صاروخي، ومن ذلك الوقت طور الفضاء العمليات العسكرية الأرضية في مجال المراقبة والاتصالات والملاحة والرصد الجوي بحيث عمقت التكنولوجيا مفهوما جديدا يخص الميدان والجبهة على كل الأبعاد يدعى بالجبهة متعددة الأبعاد (28).

ISSN : 2410-1818

وأن ظهور ما سمي بحرب النجوم التي ما هي إلا حرب أوسع تتضمن فقط البدء بوضع أسلحة في مدارات حول الأرض تمكنها من تدمير القاذفات الاستراتيجية والصواريخ النووية خلال ثوان معدودة من إطلاقها، ومثل هذا الاحتمال إذا ما قدر له أن يتحول إلى حقيقة فإنه سيغير مشهد الحرب عامة، فتفتقد الصواريخ العابرة للقارات فعاليتها وجدواها وبذلك نكون قد انتقلنا إلى مرحلة من الأسلحة الاستراتيجية مصممه لتدمير المجتمعات، أسلحة قادرة على تدمير أسلحة الدمار الشامل، وعلى الرغم من انتهاء الحرب الباردة قاد إلى تراجع أهمية هذا المشروع للمؤسسة العسكرية – الصناعية الأمريكية إلى أنه سرعان ما أن تصاعد وتيرة العودة للحديث عن هذا المشروع والبدء في عملية تطورية، وكذلك الكتمان الذي يحيط بالأبحاث الفضائية والمبالغ الضخمة التي تنفق على غزو الفضاء كافية لتثبت أن الأمر ليس بحثا علميا خالصا لمنفعة الإنسان (29).

وبذلك فإن التكنولوجيا المتقدمة قد بدلت من منظومة القيادة والسيطرة والحاسبات والاتصالات والمراقبة والاستطلاع والاستخبارات في الحروب والعمليات العسكرية فضلا عن ذلك أصبحت المسافة التي تفصل بين المستوى التكتيكي والاستراتيجي قليلة جدا؛ إذ يمكن للمستوى الاستراتيجي قيادة العمليات التكتيكية مباشرة وعن بعد، وتعد عملية قتل زعيم تنظيم القاعدة أسامة ابن لادن في عام 2011م مثالا حيا على ذلك فقد كانت فرقة صغيرة من القوات الخاصة تقوم بالعملية والرئيس الأمريكي بارك أوباما مع طاقم مجلس الأمن القومي الأمريكي يتابعون العملية مباشرة (30).

وقد أحدث استخدام معدات الحرب الإلكترونية في الحروب الحديثة تطوراً هائلاً في مجالات هذه الحروب ومراحلها، وأصبح الحسم في المعارك الحديثة لصالح الجيوش والقوات التي تستخدم الحديث منها، وبقدر ما يمتلكه كل طرف من الأطراف المتصارعة، بعد أن كانت تحسم لمصلحة الطرف الذي يمتلك التفوق العددي، أو النوعي، أو يمتلك الأسلحة بعيدة المدى والدليل على ذلك أن معدات الحرب الإلكترونية المستخدمة في الطائرات المقاتلة يقترب ثمنها من نصف قيمة الطائرة بدون طيار(31).

الحرب النفسية والإعلامية

تعد الحرب النفسية أحد أسلحة الحرب الحديثة التي توجه ضد الفكر والعقيدة والتقاليد والشجاعة والثقة وصناعة القرار وضد الرغبة في القتال، وهي حروب دفاعية وهجومية لأنها تحاول بناء معنويات الشعب والمقاتلين بينما تحطم معنويات العدو في الوقت نفسه باستخدام كل وسائل التشويش وتحطيم الصور المثالية في تفكير الناس وهي جزء من الحرب الشاملة لأنها تشن قبل الحرب وأثناء الحرب وفي أعقابها (32).

ISSN : 2410-1818

المطلب الثالث

خصائص الحروب الإلكترونية

تتميز حروب الفضاء الإلكتروني بالعديد من الخصائص، التي كانت الدافع وراء اعتماد العديد من الفاعلين الدوليين عليها وكذلك الفاعلين من غير الدول ومن أهم تلك الخصائص:

انخفاض تكلفة الحروب الإلكترونية:

فهي لا تحتاج إلى معدات أو جيوش مُجهزة وبالتالي لا يكون هناك إراقة للدماء، كما أن احتمالية إلحاق الخسائر من الجهة المُهاجمة تكون مُنعدمة مع إلحاق ضرر بالعدو.

مبدأ إخلاء المسئولية:

كون حروب الفضاء الإلكتروني يكون فيها صعوبة تحديد الجهة المُهاجمة مما يُساعد على إمكانية التلاعب والتمويه العالية فيما يتعلق بمصدر ومكان شن الهجوم الإلكتروني (33).

تعدد الأهداف: هذه الحروب تستهدف مجموعة من الأهداف ولا تقتصر على الأهداف العسكرية فقط بل قد يكون الهدف منها طمس هوية الدولة، وقد يكون هدفها ثقافي، وقد يكون الهدف منها هو تدمير أجهزة المعلومات لمجموعة من المؤسسات المالية في الدولة، وقد يكون هدفها اقتصادي خاصةً بعد تحول مُعظم قطاعات الدولة للرقمنة، أي أنها تستهدف البنى التحتية للدولة.

- **يُمكن أن تكون الحروب الإلكترونية من فاعلين من غير الدول:**

حيث أن الأسلحة المُستخدمة في هذه الحروب ليست حكراً في يد الدولة، وبالتالي يُمكن وصفها بأنها حروب غير تناظرية، فنتيجة لتكلفتها المُتدنية وأنها لا تحتاج لمقاتلات متطورة أو امتلاك أسلحة مُكلفة وإنما يكفي للقيام بها أن يكون هناك تطوير للبرمجيات وامتلاك أجهزة الحاسوب وكيفية التعامل معها، جعل فاعلين أيضاً من غير الدول تقوم بها.

فشل إمكانية تطبيق مبدأ الردع: والتي عادةً ما يُستخدم من دولة ضد أخرى في الحروب التقليدية أو النووية، ولكن في الحروب الإلكترونية بسبب صعوبة تحديد الجهة المُهاجمة يكون من الصعب تتبع الهدف وبالتالي يكون من الصعب ردعه. يتم فيها استخدام أساليب متنوعة ولا تعتمد على أسلوب معين، كل هذه الخصائص جعلت الحروب الإلكترونية هي وجهة العديد من الدول في العصر الحديث وبالتالي أصبحت ركناً أساسياً في الصراعات العالمية، فهي لا تعرف الحدود الجغرافية والمكانية ومن المتعذر فيها تحديد الضربات وخط سيرها، كل ذلك جعلها نوعا جديدا من المواجهات مغايرا لما عرفته البشرية في تاريخها(34).

ISSN : 2410-1818

المطلب الثالث

آليات عمل الحروب الإلكترونية

تقوم آلية عمل الحروب الإلكترونية بالدرجة الأولى على توفر عنصرين أساسيين يكونا في أي صراع ينشب في الفضاء الإلكتروني؛ أول هذه العناصر هي توفر المعلومات والتي ترتكز عليها الحروب التكنولوجية بشكل كبير، أما ثاني هذه العناصر هي القدرات العقلية والذهنية؛ فتتمثل القدرات العقلية في القدرة على الاستحواذ على المعلومة وتوظيفها توظيفاً دقيقاً للتأثير في الطرف الآخر بينما توفر المعلومات تعني امتلاك المعلومات المهمة عن الجهة المستهدفة تُساعد في تحقيق الهدف فالمعلومة قوة، ولا يتم الاكتفاء بامتلاك المعلومات فقط بل امتلاك الاتصالات الحديثة والمتطورة من برمجيات وشبكات الإنترنت وأجهزة اتصالات وحواسيب تتسم بأعلى معايير الكفاءة (35).

يتوقف نجاح عمل الوسائل الحديثة وتوفر المعلومات بتزويدهما ببنية معلوماتية صحيحة نابعة من عقل بشري يعي أهدافه بشكل سليم؛ لكي تتمكن من تصويب أهدافها الرقمية بشكل دقيق، فبدون ذلك لن تستطيع أي حرب إلكترونية تحقيق أهدافها ولن تتمكن أدواتها من القيام بعملها بكفاءة وفاعلية.

ويُمكن الدخول للحرب الإلكترونية من خلال العمليات الآتية:

عملية الهجوم الإلكتروني: تهدف للسيطرة على معلومات الخصم وضرب معلوماته السياسية والاقتصادية والعسكرية؛ لإلحاق الأضرار المعنوية والمادية بالخصم عن طريق التشويش على مصادر المعلومات وتدميرها وحرمان العدو من استخدامها.

عملية الدفاع الإلكتروني: هي الإجراءات الوقائية التي تهدف للحد من رد فعل الخصم من خلال وضع الخطط الاستباقية ومنع أي اختراق بالدفاع عن أنظمة مؤسسات الدولة.

عملية الدعم الإلكتروني: هي عملية مُكملة للعمليتين السابقتين وتهدف للتعرف على التهديدات المباشرة من خلال تحديد الأهداف والتخطيط لإدارة العمليات في المستقبل (36).

تنفيذ الثلاث عمليات السابقة يتطلب أيضاً آليات عمل لتحقيق الأهداف المنشودة، وبالتالي يتم تنفيذ تلك العمليات من خلال **التجسس المعلوماتي، الاختراق الإلكتروني، القرصنة الإلكترونية** من خلال تجنيد العديد من الأشخاص المؤهلين لاقتحام الوسائل الاتصالية والنظم التكنولوجية وهناك وسائل أخرى أيضاً مثل: التضليل الإلكتروني عبر التقليد الصوتي ونشر الشائعات وانتحال الشخصيات

ISSN : 2410-1818

وكذلك الطائرات الإلكترونية وهي طائرات بدون طيار أو طائرات مسيرة وتملك قدرة عالية على الدقة في تحديد الهدف والمراقبة والقصف.

تتميز أسلحة الفضاء الإلكتروني بالتنوع وتفاوت تأثيرها وفقاً للتقدم العلمي والتقني الذي تواكبه الدولة، أما خسائرها فتكون مادية ومعنوية ولا تقف عند حدود معينة.

المطلب الرابع

استراتيجيات الحروب الإلكترونية

تتنوع استراتيجيات الحروب الإلكترونية وفقاً لأهمية الهدف الذي تُوضع من أجله والمجال الذي تنوي استهدافه وبالتالي يُمكن توضيح استراتيجيات الحروب الإلكترونية في ثلاث استراتيجيات رئيسية وهي

أولا: استراتيجية عسكرة التكنولوجيا: يُعد الهدف الأساسي لهذه الاستراتيجية هو تعطيل وإفساد المعلومات بغرض زرع وسائل التجسس وتوجيهها ضد الطرف المقصود بالهجوم، وتتخذ هذه الاستراتيجية ثلاث أساليب تتمثل في:

- **الهجوم الإلكتروني**، وهو يعني استخدام الطاقة الكهرومغناطيسية أو الأسلحة المضادة للإشعاع؛ لمهاجمة الأفراد والمرافق بقصد إضعاف القدرة القتالية للعدو والحد من الاستخدام الفعال للطيف المغناطيسي من العدو والتي تشمل التشويش والتضليل الكهرومغناطيسي، وتكون الخسائر الناتجة عن الهجوم الإلكتروني خسائر مادية ضخمة ولا تكون بشرية مثل الحروب التقليدية.

- **الحماية الإلكترونية**، وتعني الإجراءات المُتخذة لحماية الموظفين والمنظمات من أي هجمات إلكترونية وذلك من خلال التأكد بأن النظام الإلكتروني محمي من الهجمات الإلكترونية من خلال التدريبات قبل التحكم في البرامج الخاصة بهذه المنظمات أو الدول أو الأفراد، ويلعب العامل العسكري دوراً مهماً في نجاح الحماية الإلكترونية، ومثالاً على ذلك الولايات المتحدة الأمريكية ونظراً لما خاضته من حروب عسكرية عدة في العقود الأخيرة أكسبها ذلك مهارات العمل العسكري والإلكتروني؛ لذلك تُعد من أهم الدول الحريصة على الحماية الإلكترونية (37).

- **دعم الحرب الإلكترونية**، وهي الإجراءات التي يقوم بها قائد العمليات لتحديد مصادر أشعة الطاقة الكهرومغناطيسية والتعرف على الأهداف المباشرة والتخطيط لإدارة العمليات مُستقبلاً، ويُعد هذا النظام مصدرا أساسيا لاتخاذ الإجراءات الفورية للقيام بالهجوم الإلكتروني وتجنب الاستهداف، ويتم ذلك من خلال الأمن الإلكتروني والاستخبارات الإلكترونية.

ISSN : 2410-1818

وبالتالي يبقى نجاح عمليتي الهجوم والحماية الإلكترونيين مرهونين بتوجيه الاهتمام على نُظم دعم الحرب الإلكترونية.

ثانيا: استراتيجية اختراق المنظومة الاقتصادية

أصبح ضرب القطاع الاقتصادي إلكترونياً عملاً استراتيجياً لتحقيق أهداف معينة؛ لأن المنظومة الاقتصادية باتت تستند في عملها على الوسائل التكنولوجية المتطورة، ومن أخطر صور هذه الاستراتيجية:

- **التجسس الصناعي:** حيث أن القطاع الصناعي يُمثل عاملا وركيزة أساسية من ركائز التنمية الاقتصادية بل وسبباً للنزاع بين العديد من الدول، فتلجأ الدول للتجسس على أهم الأدوات والركائز في هذا القطاع بالطرق الإلكترونية، ومن أهم عمليات التجسس التي حدثت ضد الدول هي عمليات التجسس على القطاع الصناعي التي تعرضت لها ألمانيا عام 2010 من روسيا والصين نتيجة المنافسة الاقتصادية بين هذه الدول (38).

- **تعطيل قطاعي التجارة والخدمات:** يُسهم قطاعي التجارة والخدمات في الدول إلى تلبية احتياجات السكان، فالهجوم على مثل هذه القطاعات يُمثل شلل اقتصادي للدولة في تلبية الخدمات وكذلك تذمر من الشعب من الخدمات المُقدمة، وقد يتم ذلك من خلال قرصنة المواقع الإلكترونية وتُعد المواقع الاقتصادية الإسرائيلية الأكثر استهدافاً خاصةً مواقع البورصة والبنوك، وتُكبد هذه العمليات الدول أموالاً طائلة تصل لمليارات الدولارات سنويا(39).

ثالثاً: استراتيجية الهيمنة الفكرية الثقافية

هي ما يُطلق عليها الغزو الثقافي أو الفكري والتي تهدف إلى سلخ الخصم عن هويته من خلال التسلل لأفكاره عن طريق إرسال رسائل لاستدراجه للوصول للنتيجة المطلوبة وهي تطبيع هوية الخصم على طبع المُهاجم وتتم بأشكال مختلفة أهمها وسائل التواصل الاجتماعي ونتيجة للعولمة والثورة المعلوماتية أدى ذلك للانحلال في القيم العميقة للبنية الاجتماعية.

يتم تحقيق أهداف هذه الاستراتيجية باتخاذ السُبل الآتية:

- **نشر القيم الاستهلاكية وتفتيت هوية الأفراد:** ويظهر ذلك في أشكال التبعية لدول العالم النامي بالتدريج بالتبعية الاقتصادية التي أدت لتبعية سياسية ثم تبعية تكنولوجية تقنية، وبوصف الدول العربية نموذجاً؛ حيث اعتمدت على التكنولوجيا الغربية في الصنع والنشأة والمؤسسة من أجل غرس العدمية القومية واللامبالاة وهدم اللغة والثقافة عن طريق البرامج المعلوماتية الترفيهية الاستهلاكية والتي تمثل

ISSN : 2410-1818

خطراً على العلاقات الاجتماعية وقللت فرص التواصل على مستوى الأسرة العربية، حيث أنها تضع الأفراد بين ثقافتين متناقضتين، واحدة متطورة والأخرى متخلفة مما يُسهم في التقليد.

- **التأثير في التعددية الثقافية:** ويتم التأثير عليها بطرق مختلفة أهمها عولمة الإعلام، خاصةً في نهاية ثمانينات القرن الماضي؛ فعلى سبيل المثال صدرت الولايات المتحدة الأمريكية أفلاماً سينمائية ومواد إعلامية إلى أوروبا عام 1993 بقيمة 4 مليار دولار وفي مقابل ذلك استوردت من أوروبا نحو 336 مليون دولار، بما يعني بأن خطر هذه الاستراتيجية على الدول النامية والمتقدمة، كما قد تُفرض ثقافة واحدة مهيمنة من خلال السيطرة على وسائل الإعلام وجعلها أداة تخدم أجندتها الخاصة، وبالتالي يكون التأثير على ثقافة الأفراد والعبث بمعتقداتها(40).

تُعد استراتيجية الهيمنة الفكرية الثقافية طمس للهوية الحضارية والثقافية والوطنية للشعوب من خلال تركيزها على محاولة القضاء على التعددية الثقافية وتشجيع ثقافة الاستهلاك وقتل روح الإبداع وإدخالها في دوامة التقليد؛ لجعلها مجتمعات فارغة من الهوية والقيم.

المبحث الثالث

الحروب الإلكترونية وتأثيرها في الصراعات الدولية

لقد أدى إدخال أدوات وتقنيات التكنولوجيا إلى ساحة الصراعات المتعددة والتي تعتبر امتداداً للحروب الإلكترونية، وكذلك استخدام التكنولوجيا الحديثة والمتطورة إلى التغيير في شكل الصراعات الدولية، والتي تطورت واتسعت خلال الحرب الباردة وقد أحدث استخدام معدات الحرب الإلكترونية في الحروب الحديثة تطوراً هائلاً في مجالات هذه الحروب ومراحلها، وأصبحت الشبكة أساسية في أغلب الاتصالات والتعاملات وأجهزة التحكم كما شكلت وسيلة للتجسس للبعض، وتحولت إلى أداة للحرب بمختلف صورها وأصبح الحسم في المعارك الحديثة للجيوش التي تستخدم الحديث منها وعليه سيتناول هذا المبحث المطالب الآتية:

المطلب الأول

أثر التحولات في الصراعات الدولية.

شكلت ثورة المعلومات أهمية قصوى فيما بعد الحرب الباردة إذ دخل العالم مرحلة متطورة من التقدم من حيث ثورة المعلومات الشاملة وثورة وسائل الاتصالات الحديثة، التي بلغت الأقمار الصناعية وثورات الحاسبات الإلكترونية التي امتزجت مع وسائل الاتصال والثورة المعرفية الشاملة باندماج الحاسبات الإلكترونية مع التلفزيون والاتصالات السلكية واللاسلكية، وأدى الخوف من شبح الحروب النووية بالدول المالكة لهذا السلاح بالتفكير بوسائل صراع تستثني المواجهة المباشرة. هذا ما شهده العالم خلال الحرب الباردة طوال 45عاما، ظهر خلال ذلك مصطلحات عدة، مثل الحرب

ISSN : 2410-1818

بالوكالة والحرب الاقتصادية والحرب الإلكترونية وغيرها ، فإن عدم استخدام السلاح النووي لا يعني توقف الدول عن التفكير بوسائل جديدة للمواجهة، وآخر هذه الوسائل هو التركيز الكبير على تكنولوجيا الحرب الإلكترونية ، والتي تُعد أهم وأحدث تطور في عالم الصراعات والتنافس الدولي، هذه الحرب تعتمد بشكل أساسي على مدى التطور التكنولوجي العسكري للدول المعنية، كما أن وسائل الحرب تتمايز فيما بينها ، فمنها الدفاعي لصد الهجمات الإلكترونية المعادية وإبطال الصواريخ المعادية وتعطيلها والبعض الآخر هجومي يعتمد على السيطرة والضبط والوسيلة الثالثة تندرج في مجال الأقمار الصناعية وأنظمة الملاحة وأجهزة الرصد والإنذار المبكر، ويدور الحديث عن بدء استخدام تكنولوجيا أسلحة الليزر بشكل موسع منذ عام 2020م والتي تستخدم في تدمير الصواريخ وتفتيتها وإبطال أجهزة الطائرات بدون طيار (41).

وعليه فقد تعرضت ظاهرة الصراع إلى تغييرات مع بروز الفضاء الإلكتروني، كمجال تنشأ فيه نزاعات بين المتصارعين المختلفين، خاصة مع الاعتماد الكثيف على تكنولوجيا الاتصال والمعلومات، وهنا ظهر الصراع الإلكتروني كحالة من التعارض في المصالح والقيم بين المتصارعين سواء كانوا دولاً أم غير ذلك في الفضاء الإلكتروني.

وبالرغم من 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 (42).

وبما أن المتصارعين يلجأون في الصراعات التقليدية إلى استخدام شتى أنواع أسلحة التدمير الممكنة، فقد انتقلت جبهات القتال إلى ساحة الفضاء الإلكتروني، وكان هذا التغيير سببا في إعادة التفكير في حركية وديناميكية الصراع وظهور ما يعرف بعصر القوة الإلكترونية، والتي أثبتت أن القوة العسكرية قد لا تكفي وحدها لتحقيق الأمن القومي للدول، الأمر الذي يخلف آثاراً استراتيجية هائلة على مستوي تركيبة وتوازنات النظام الدولي.

فقد أصبح من السهل تصور قيام شبكات مسلحة وتنظيمات للقيام بشن كثير من الهجمات بدون أجهزة الحكومة ويرجع ذلك في أن أدوات التدمير أصغر وأرخص وأسهل للوصول إلى سلسلة من الأفراد والشبكات والتنظيمات المسلحة أوسع بكثير من ذي قبل وبينما كانت القنابل وأجهزة توقيتها ثقيلة وغالية الثمن فان المتفجرات، البلاستيكية وأجهزة توقيتها الرقمية غدت رخيصة وخفيفة (43).

ISSN : 2410-1818

ولقد صاحب التطور التكنولوجي تطورا في أدوات الحروب الحديثة بتسارع، بنحو يتعين على الجيوش الحديثة أن تلاحقه، وهذا كان سبب تطور أساليب الصراع بما يسمي الجيل الأول للحرب، ثم الجيل الثاني ثم الجيل الثالث، ومع القفزة التكنولوجية الهائلة التي ظهر تأثيرها على العلاقات الدولية، وعلى رأسها أدوات الصراع العسكري ظهرت فكرة الجيل الرابع للحرب، التي كانت بعد ذلك جزء من الحروب اللامتماثلة (غير النمطية)، في الجيش الأمريكي باعتباره أكثر جيوش العالم امتلاكا للتكنولوجيا الحديثة والفائقة (44).

المطلب الثاني

الحروب الإلكترونية و أثرها في الصراعات الدولية.

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، التي لها تأثير كبير على المستوي الدولي والمحلي، ومن 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 في السياسة الدولية قدرة اكبر على ممارسة كل من القوة الصلبة والقوة الناعمة عبر الفضاء الإلكتروني، وهو ما يعني تغيرا في علاقات القوي في السياسة الدولية (45).

ومع ظهور الانترنت ومواقع الويب أصبح الفضاء الإلكتروني أحد العناصر الرئيسية التي تؤثر في النظام الدولي بما يحمل من أدوات تكنولوجيا تلعب دورا مهما في عملية التعبئة والحشد في العالم، فضلا عن التأثير في القيم السياسية وأشكال القوة المختلفة سواء كانت صلبة أو ناعمة.

كما تُعد الحروب الإلكترونية أحد أوجه الصراعات الدولية، إذ يستطيع أحد أطراف الصراع أن يوقع خسائر فادحة بالطرف الآخر، وأن يتسبب في شل البنية المعلوماتية والاتصالاتية الخاصة به، وهو ما يسبب خسائر عسكرية واقتصادية فادحة، من خلال قطع أنظمة الاتصال بين الوحدات العسكرية بعضها البعض أو تضليل معلوماتها أو سرقة معلومات سرية عنها، أو التلاعب بالبيانات الاقتصادية والمالية وتزييفها، أو مسحها من أجهزة الحواسيب. وبالرغم من الخسائر الفادحة، إلا أن الأسلحة بسيطة لا تتعدى (الكيلو بايت)، تتمثل في فيروسات الكترونية تخترق شبكة الحاسب الآلي وتنتشر بسرعة بين الأجهزة، وتبدأ عملها في سرية تامة وبكفاءة عالية، وهي في ذلك لا تفرق بين المقاتل والمدني وبين العام والخاص وبين السري والمعلوم (46).

ISSN : 2410-1818

فقد اختصر الفضاء الإلكتروني حاجز الزمان والمكان، وخلق مساحات للتفاعلات الدولية والداخلية في الواقع الافتراضي، ومن ثم برزت فضاءات جديدة للصراع بأدوات مختلفة، وأنماط جديدة تختلف عن الصراعات التقليدية، خاصة بعد أحداث 11سبتمبر 2001م، فقد كان الفضاء الإلكتروني ساحة الصراع والقتال بين تنظيم القاعدة والولايات المتحدة الأمريكية، وهو ما حدث نفس الشيء عام 2008م في الحرب بين روسيا وجورجيا، وجاء الهجوم الإلكتروني بفيروس (ستاكس نت) والذي يعتبر نقطة تحول هامة في مجال الأسلحة الإلكترونية، وذلك بانتقال الفيروس من مرحلة تدمير أو سرقة البيانات إلى إصابة المكون المادي نفسه حيث قام بتعطيل ما يقرب من 1000 جهاز طرد مركزي في برنامج إيران النووي عام 2010م، لتبرز قوة الأسلحة الإلكترونية في الصراعات الدولية (47).

وعلى المستوى العالمي، تنظر الولايات المتحدة الأمريكية إلى الفضاء الإلكتروني كحيز يجب أن تعمم فيه معايير ومقاييس سياسية وأيديولوجية مختلفة حسب مفهومها، وفي ربيع العام 2010م تم إنشاء مؤسسة تابعة للبنتاغون في القيادة الإلكترونية. وفي عام 2010م أعلنت وزارة الدفاع أنها شرعت في التحكم بالشبكات الاجتماعية من أجل تحسين الصور، والتأثير على الدول الأخرى، وقد أشارت أن جهودا إضافية ستبذل لإنشاء (مديرة وكالة الدفاع الأمريكية للتقنيات الواعدة) ريغينا دوغان- سلاح الكتروني هجومي يشكل عنصراً جوهرياً في الآلات العسكرية. مع ضرورة معرفة الإمكانات الإلكترونية للدول الأخرى بهدف التحصن ضدها، وهذا يعني أن الولايات المتحدة الأمريكية تمارس التجسس الإلكتروني بنفسها (48).

إن الاهتمام بموضع الحرب على الشبكة العنكبوتية قد تزايد بشكل ملحوظ وعلى مستوى أكثر عمقاً وشمولاً. وانعكس ذلك على إعداد ما ينشر عنه من ورش عمل ومؤتمرات. ولم يقتصر ذلك على الجانب العسكري، فحسب بل اتسع ليشمل المؤسسات الاقتصادية والمجتمع المدني، وكما هو واضح للعيان قد تمكن في كثير من الدول جعل هذا العالم الافتراضي مسرحاً له، وميدانا لحروبه الأيدلوجية والسياسية، من دون أن يكون للعاملين على هذا المسرح مقر حقيقي ملموس؛ إذ يكفيهم أن يدير معاركهم على ساحة العالم الافتراضي الممتد بلا حدود، وعلى مشهد من العالم كله، وذلك تطور خطير يحتاج إلى إعادة نظر في كثير من الأفكار القديمة، كما أن العديد من الدول بدأت تعد العدة للتصدي لهذه الهجمات ولشن أخرى مضادة عبر الانترنت، وقد (سرح جريغ داي) أحد المحللين الأمنيين بقوله: هناك على الأقل خمسة بلدان من المعروف أنها تسلح نفسها استعدادا لهذا الصنف من الصراعات التابعين للفرع الأوربي مشيرا بالقول هذه البلدان بريطانيا وفرنسا وألمانيا والصين وكوريا الشمالية. مشيرا إلى أن الولايات المتحدة الأمريكية استخدمت أساليب قرصنة أثناء حملتها في العراق، وهي الأساليب نفسها التي تنتهجها من أجل إحكام رقابتها على أمنها القومي (49).

ISSN : 2410-1818

وقد تمكنت الدول الكبرى من إنشاء جيوش الكترونية عظمى تستطيع فيها تغيير وجه العالم وابرز الجيوش الالكترونية في العالم هي (50):

1- الوحدات الست في الولايات المتحدة: تعتمد الولايات المتحدة في الحروب الإلكترونية على ست عناصر هي الوحدة الأمريكية لقيادة "الفضاء الإلكتروني" ، وهي المختصة بالتخطيط والتنسيق وإدارة عمليات الحروب الإلكترونية مع باقي الفروع التي تتبعها.

2- كوريا الشمالية: تمتلك كوريا الشمالية وحدة خاصة بالحروب الإلكترونية هي المكتب 121 وأهدافه الرئيسية هي كوريا الجنوبية والولايات المتحدة واليابان وأنشئ عام (1998).

3- اللواء77 البريطاني: انضمت بريطانيا للحروب الإلكترونية باللواء (77) في أوائل(2015) ويركز في الأساس على الحسابات المؤيدة للإرهابيين على "توتير" حيث يعمل اللواء البريطاني على شن الحروب النفسية ويتكون من (2000) جندي.

4- مخابرات الإشارة الروسية: أن مجموعات من الهاكرز يعملون لصالح استخبارات الإشارة الروسية, وكان أحدث الهجمات التي يشنها هاكر روس بحسب " سي إن إن" هو اختراق وزارة الخارجية الأمريكية واختراق أنظمة البيت الأبيض لدرجة تسريب جدول أعمال الرئيس الأمريكي باراك أوباما.

5- الوحدة (61398) الصينية: تشتهر الصين بامتلاكها أحد أفضل الجيوش في الحروب الإلكترونية في العالم ورغم عدم الكشف رسميا عن الوحدة المسؤولة عن عمليات الاختراقات الصينية إلا أن وزارة العدل الأمريكية قالت أن الوحدة هي مصدر حروب الصين الالكترونية.

6- كوماندوز الجيش الإسرائيلي: اشتهرت إسرائيل باستخدام وحدة عسكرية من أجل الحرب النفسية على الانترنت حيث توجد وحدة كوماندوس إسرائيلية تركز على 30 موقع بالإضافة إلى العديد من مواقع التواصل الاجتماعي وتبث رسائلها بعدة لغات منها العربية والإنجليزية والعبرية والفرنسية والإسبانية.

7- جيش إيران الإلكتروني: وفي السنوات الأخيرة برزت إيران كقوة في الحروب الإلكترونية من خلال جيش إيران الإلكتروني والذي أظهر القدرة على اختراق أهدافه ببراعة على حد قول معهد الدراسات الاستراتيجية الأمريكي.

ISSN : 2410-1818

المبحث الرابع

صراع الحـــروب الالكتـــرونيـــة

بعض النماذج التطبيقية للصراعات الإلكترونية:

لقد انتقلت قطاعات واسعة من الحروب والمعارك والصراعات والثورات في العالم إلى العالم الافتراضي الذي أوجده الإنسان من حين اختراع الكمبيوتر والذاكرات الإلكترونية وشبكات المعلومات فأنشأت جغرافية افتراضية جديدة وانتقلت إلى عالم الفضاء الإلكتروني، من خلال وسائل السيطرة والتحكم بمعظم العمليات الحيوية الموجودة على الأرض، وأخذ الصراع الإلكتروني حيزا واسعا من خرائط الصراعات الدولية، لأنها حروب غير مكلفة، وتلحق أضرارا كبيرة في الخصم ويصعب تحديد هوية المهاجم وتجنب الدول الإدانات والتبعات القانونية وتجنبها الردود العسكرية، ولها آثار مدمرة على الدول المستهدفة ولذلك سعت كثيرا من الدول إلى استخدام الهجمات الإلكترونية التي تتم عبر الفضاء الإلكتروني، وكان لها تأثيرا كبيرا في الصراعات الدولية، ومن أبرز هذه الحروب والهجمات في الآونة الأخيرة الآتي:

أولاً: الهجمات الإلكترونية بين روسيا وأوكرانيا

- حيث تعرضت وزارة الكهرباء الأوكرانية عام 2015م لهجمات الكترونية على شبكة الكهرباء الأوكرانية وأوضحت المصادر أن متسللين استخدموا شبكة الانترنت مقرها روسيا قاموا بهذا الهجوم مما تسبب بانقطاع الكهرباء وكانت أول هجوم ناجم عن هجوم اكتروني.
- سلسلة الهجمات الإلكترونية التي وقعت من روسيا ضد أوكرانيا حول شبه جزيرة القرم استهدفت البنوك والوزارات وشركة الكهرباء وتم فيها استخدام برمجيات خبيثة من نوع بيتا مما نتج عنه تعطيل أنظمة المعلومات وتعطيل أعمال الشركات الحكومية والخاصة (51).

ثانياً: الهجمات الإلكترونية بين إيران وإسرائيل

في العام 2010م ومع ظهور فيروس ستاكس نت، والذي يعتبر نقطة تحول هامة في مجال الأسلحة الإلكترونية ، وذلك بانتقال الفيروس من مرحلة تدمير أو سرقة البيانات إلى إصابة المكون المادي نفسه حيث قام بتعطيل ما يقرب من 1000 طرد مركزي، وهو ما أثر على عملية تخصيب اليورانيوم للمفاعل النووي الإيراني وقد تبنت إسرائيل المسؤولية عن شن هجماتً ستاكس نت بالتعاون مع الولايات المتحدة الأمريكية (52).

ISSN : 2410-1818

وفي عام 2019م تطورت الحرب الإلكترونية بين الدولتين حيث أعلنت وحدة الدفاع الإلكترونية الإسرائيلية أنها أحبطت عملية اختراق إيرانية استهدفت نظام التنبيه ضد الصواريخ الإسرائيلية، في العام التالي 2020م أعلن جهاز الأمن الوطني الإلكتروني في إسرائيل أنه أحبط هجوم الكتروني على منظومة المياه في إسرائيل كما تضمن الهجوم الأنظمة الحاسوبية لست منشآت مياه في إسرائيل ورجعت إسرائيل وقوف إيران وراء هذا الهجوم وذلك لأن من الصعب التحقق من هوية المعتدي، ففي 2020 م تعرضت إيران لتفجيرات غامضة استهدفت مواقع عدة أهمها منشأة نطنز النووية وهي المبني الرئيسي لتخصيب اليورانيوم بإيران (53).

ثالثاً: الصراع بين الولايات المتحدة الأمريكية – وإيران.

يعد برنامج إيران للحرب الإلكترونية أحد أجنحة النظام الإيراني لمواجهة الولايات المتحدة الأمريكية، الذي بدأ تشكيله عام (2012) ويشرف على إدارته المجلس الأعلى للفضاء الإلكتروني، وقد أشار الضابط السابق في الحرس الثوري والباحث الفيزياوي (محسن فخري زاده) بقوله: إن إيران عملت على تطوير قدراتها الإلكترونية منذ تأسيس المجلس الأعلى للفضاء الالكتروني، واستغل النظام الإيراني البرنامج لشن هجمات إلكترونية وتنفيذ عمليات تجسس إلكترونية في محاولة لإلحاق الضرر بالبنى الأساسية المالية والأمنية والسياسية الخاصة بالدول لمعادية لإيران (54).

وقبيل أعوام من توصل المجتمع الدولي إلى الاتفاق النووي مع طهران، شنّت الولايات المتحدة الأمريكية حربها الالكترونية على مشروع إيران النووي، بهدف إضعاف قدرة طهران النووية، وإجبارها على التنازل على طاولة المفاوضات، وهو ما تم وفق خبراء، وقد وضح (جورج ميد)، خبير فيروسات يعمل في الجيش الأمريكي: أنه تم إرسال الفيروسات الخبيثة لتخريب المنشآت النووية الإيرانية، الأمر الذي أضعف قدرتها على تخصيب اليورانيوم.

وفي الوقت نفسه لم تكن واشنطن بمأمن من الهجمات الالكترونية، ففي يوم الجمعة 23 مارس(2018) وجهت وزارة العدل الأمريكية اتهامات جنائية وفرضت عقوبات على شركة إيرانية وعلى(9) ناشطين إيرانيين، لاختراقهم أنظمة مئات الجامعات والشركات وضحايا آخرين لسرقة البحوث والبيانات الأكاديمية والملكية الفكرية، ووصفت وزارة العدل الأمريكية القراصنة بأنهم عصابة تسلل إلكتروني، حاول أفرادها اختراق مئات الجامعات حول العالم، وهم أفراد تابعين للحرس الثوري الإيراني، فضلاً عن اختراقهم عشرات من الشركات وقطاعات من الحكومة الأمريكية لحساب الحكومة الإيرانية، وحسب ما صدر من تقارير صادرة عن الوزارة وضحت فيه:"إن الهجوم الذي وصفته بإحدى كبرى الهجمات الإلكترونية التي ترعاها دولة إيران، بدأ منذ 2013 على الأقل وبه تمت سرقة أكثر من 31 تيرابايت من البيانات الأكاديمية وحقوق الملكية الفكرية من 144 جامعة أمريكية و176 جامعة في 21 دولة أخرى(39).

ISSN : 2410-1818

كما أوضح المحلل السياسي مجيد رفيع زاده:

أن النظام الإيراني شن هجمات إلكترونية ضد الولايات المتحدة وغيرها من الدول، والمثال على ذلك، تعرضت الأنظمة المصرفية الأمريكية لهجوم بمستوى غير مسبوق فضلًا عن مواقع عدد من البنوك، مثل: بنك أوف أمريكا، وسيتي جروب، وأوضح مسؤولون أمريكيين: أن مستوى تلك الهجمات يشير إلى أن الفاعل الحكومة الإيرانية، واتهمت مؤخراً وزارة العدل الأمريكية (7) إيرانيين بشن هجمات تعطيل الخدمة على 46 شركة، وتستهدف بصورة أساسية القطاع المصرفي والمالي.

وأشارت الاستخبارات الأمريكية: أن إيران وراء (فيروس شمعون)، الذي استهدف شركة – أرامكو- السعودية, وأوضح زاده بقوله: أن القادة الإيرانيين مدركون لحقيقة أن شن هجمات إلكترونية أقل تكلفة عن الانخراط في مواجهة عسكرية مباشرة مع خصومها، خاصة وأن قدراتها العسكرية أقل من أعدائها، لافتا إلى أنه من وجهة نظر القادة الإيرانيين البديل للحرب الفعلية هي الافتراضية التي تقدم ميزة إخفاء الهوية كما تصعب للغاية إمكانية محاسبتهم، ورأى زاده أن إيران على الأرجح ستحاول تصدير تلك القدرات المتعلقة بالحرب الإلكترونية إلى وكلائها إقليمياً، وقد يكون لهذا عواقب وخيمة بالنسبة لمصالح الأمن القومي الأمريكي، وكذلك أشار إلى أن برنامج الحرب الإلكترونية الإيراني أصبح مسألة أمن قومي بالنسبة للنظام؛ خاصة وأنه يساعد النظام في تحقيق أهداف سياستهم الخارجية ومطامعهم في الهيمنة الإقليمية(55).

رابعاً: الصراع بين الولايات المتحدة- وروسيا.

لقد أدى ظهور الجيوش الالكترونية إلى كشف عن نوايا الحروب الالكترونية جديدة، وهذا ما كشف عنه وزير الدفاع الروسي سيرغي شويغو: أن بلاده أنشأت بالفعل جيشا إلكترونياً تابعاً لوزارة الدفاع، ويتوقع أن يقوم هذا الجيش بردع الدعاية المغرضة ضد بلاده وأن يكون أداة فعالة ذكية وكفؤة، ورغم أن مهام هذا الجيش ستكون سرية ولن تقف عند مجال الدعاية، فإن أهمية هذه التصريحات التي أدلى بها وزير الدفاع الروسي أنها جاءت في أعقاب إعلان مدير الاستخبارات الألمانية هانس جورج ما سن (أن الهجمات الإلكترونية يمكن أن تقوم بتركيع الدول المتقدمة بما فيها ألمانيا) (56).

ولا شك أن الحرب الإلكترونية التي أعلنها الرئيس الروسي، (فلاديمير بوتين)، على الانتخابات الرئاسية الأمريكية في عام 2016، والتي تهدف للتأثير فيها لمصلحة الرئيس (دونالد ترامب) شكلت عهداً جديداً في الحروب الالكترونية وباتت بوابة حروب المعلوماتية، انعكست آثارها على الأرض في الولايات المتحدة فللمرة الأولى تنتقل الحرب الإلكترونية بين الدول إلى الساحة الديمقراطية بعد أن كانت تقتصر على استهداف المنشآت العسكرية والاستخبارية (57).

ISSN : 2410-1818

كما أن الخطورة التي تشكلها أجهزة التشويش الروسية على القوات الأمريكية المتواجدة في سوريا، وذلك نقلاً عن مصادر عسكرية أمريكية وبحسب التقارير فإن القوات الأمريكية المنتشرة في سوريا تضطر بشكل متزايد إلى الدفاع عن نفسها أمام هجمات إلكترونية روسية التي لها عواقب مميتة. وذكر ضباط أمريكيون اختبروا التشويش المعروف باسم (الحرب الإلكترونية)، إنه لا يقل عن الهجمات التقليدية بالقنابل والمدفعية وقد أشار الخبير في قضايا الأمن القومي والقضايا العسكرية في (معهد ليكسينغتون) دانيال غور بقوله: إن تطور أنظمة الحرب الإلكترونية الجديدة في روسيا والتي يمكن تركيبها على المركبات الكبيرة أو الطائرات وبإمكانها التشويش على أهداف تقع على بعد مئات الأميال.

وكشفت صحيفة (الواشنطن بوست) عن توسع عمليات التجسس الأمريكية على روسيا، مشيرة إلى أنها وصلت إلى أوسع نطاق لها منذ نهاية الحرب الباردة، والتجسس الأمريكي على روسيا شمل العديد من المفاصل الحيوية، بالإضافة إلى أنظمة الأقمار الصناعية، وهو ما أدى إلى تخصيص ميزانيات كبيرة لهذه الأعمال، وهي المبالغ التي خصصت سابقاً لمكافحة الإرهاب وتغطية الحروب الأمريكية، وأن الأنشطة التجسسية الأمريكية التي تم إخفاؤها عن الرأي العام، تعتبر جزءاً من الصراع والمنافسة بين الولايات المتحدة الأمريكية وروسيا في أعقاب عقدين من الهدوء، هدوء لن يستمر في أعقاب التوترات المتصاعدة بين البلدين على خليفة العديد من القضايا (58).

لذلك أصبح للحروب الالكترونية تأثيراً عالمياً كبيراً، إذ قد تؤدي إلى تدمير بنية تحتية لدولة ما، بما في ذلك سدودها المائية ومفاعلاتها النووية, فالحرب الالكترونية هي تطور طبيعي في مفهوم الحروب، نقلتها إلى جيل جديد يعتمد على التحكم والسيطرة عن بعد.

وعليه يمكن القول بأن مزايا الحروب الإلكترونية التي تفوق مزايا الدفاع , ستدفع العالم إلى مزيد من الصراعات وخاصة مع تطور آليات الهجوم الالكتروني بشكل متسارع مما يضفي عليها مزايا إضافية في المراحل المختلفة لهذه التطورات، فغياب الأطر القانونية الدولية الرادعة في الحروب الالكترونية وانتفاء القيود الشرعية الدولية كنتيجة لعدم إمكانية التعرف على هوية المهاجم على عكس الهجوم التقليدي, كل هذه العوامل تجعل من الفضاء الالكتروني ساحة جاذبة للقوى الكبرى لإدارة صراعاتها مع بعضها البعض, فاستبدال الحرب العسكرية بتلك الالكترونية وانتقال الصراع ما بين القوى الكبرى من المساحات التقليدية إلى الفضاء الالكتروني قد يسمح للقوى الدولية الدخول في مواجهات الكترونية.

ISSN : 2410-1818

وهنا يطرح سؤال ما هي الآليات والأساليب لمواجهة الحروب الإلكترونية ؟

هناك أساليب وآليات للتصدي للهجمات الإلكترونية وتتمثل في الآتي:

1- **الجهود الوطنية:** وهي جهود الدول لحماية فضاءها الإلكتروني من خلال:

- بناء الجيوش السيبرانية: ورصد ميزانيات للتطوير في مجال الهجوم والدفاع والحماية وتتصدر الولايات المتحدة الأمريكية العالم في بناء الجيوش السيبرانية حيث تنفق سنوياً نحو 7مليارات دولار للأمن السيبراني وتأتي كوريا الشمالية في المرتبة الثانية حيث تنفق 20% من الميزانية العسكرية للأمن (59).
- تشكيل هيئات وطنية للأمن السيبراني: تكون مهمتها رفع الوعي بالأمن السيبراني، وإعداد الاستراتيجيات الوطنية، وسن التشريعات القانونية الوطنية للأمن السيبراني، مثل قانون مكافحة الجرائم السيبرانية.

2- **تفعيل الآلية التقنية:** ويأتي في مقدمتها جدران الحماية أو الجدران النارية التي تعد من أهم الوسائل التقنية لصد الهجمات الإلكترونية.

3- **استخدام مضادات الفيروسات:** والتي يتم استخدامها لاكتشاف البرمجيات الضارة ومنعها من إلحاق الضرر بالحاسوب أو سرقة المعلومات كما يمكنها التصدي لبرامج التجسس الإلكتروني.

الخاتمة

إن الفضاء الإلكتروني قد فرض نفسه كبعد استراتيجي جديد في الصراعات الدولية، والذي بدوره أحدث تغييرات في مفاهيم العلاقات الدولية، كمفهوم القوة والصراع والأمن حيث انتشرت القوة بين الفاعلين وتحول الصراع من المادي إلى الافتراضي، وأصبحت الحروب تخاض بالأصفار والآحاد وبدا واضحا أن الدول تتجه نحو عسكرة الفضاء الإلكتروني، مما نتج عنه ظهور تهديدات جديدة تتزايد في الحجم والشدة وتشكل تهديدا خطيرا للأمن القومي، فكلما زاد التشابك زادت التهديدات الإلكترونية وأثر ذلك على الصراعات الدولية.

وأضحى الفضاء الإلكتروني عنصراً مؤثراً في النظام الدولي وفي الصراعات الدولية، نظراً لما يحمله من أدوات تكنولوجية متطورة تلعب دوراً مهماً في عمليات الحشد والتعبئة في العالم برمته، فضلاً عن التأثير في القيم السياسية، وتستخدم العديد من الدول القدرات التي يوفرها الفضاء الإلكتروني لاعتبارات في مقدمتها الأمن والقوة العسكرية، وهذا جعل تلك الدول تدخل الفضاء الإلكتروني ضمن حساباتها الاستراتيجية وأمنها القومي.

ISSN : 2410-1818

وظهر بعد جديد في الصراعات الدولية وهو صراع الفضاء الإلكتروني، مكن أحد أطراف الصراع أن يوقع خسائر فادحة بالطرف الآخر، وأن يتسبب في شل البنية المعلوماتية والاتصالية الخاصة به، وهو ما يسبب خسائر عسكرية واقتصادية فادحة، من خلال قطع أنظمة الاتصال بين الوحدات العسكرية وبعضها البعض، أو تضليل معلوماتها، أو سرقة معلومات سرية عنها، أو من خلال التلاعب بالبيانات الاقتصادية والمالية وتزييفها أو مسحها من أجهزة الحواسيب. وحرب الفضاء الإلكتروني لا توجد بها أي أراقة للدماء ولكنها أخطر من الحروب العسكرية لأنها تستطيع تدمير الأنظمة والأجهزة مما يمنعها عن العمل بشكل تام وإتلافها.

لقد تغيرت الحروب التقليدية، وأصبحت الجيوش الالكترونية العسكرية في كافة أنحاء العالم، تهتم بحرب المعلومات ودورها في حروب المستقبل والتي يتوقع الكثير حدوثها في الفضاء الإلكتروني، وأصبح هناك مراكز قيادة عالية التكاليف تقام فيها المناورات والتدريب على هذا النوع الجديد من الصراع وكيفية مواجهته والاستعداد له، وطبيعة الحرب لا تتغير ولكن سمات الحرب تتغير مع تطور أدوات الحرب، والحرب الإلكترونية هي حرب من دون نار أو دخان أو قصف ولكن لها جانب عنيف من حيث الاختراقات والقرصنة ونشر الفيروسات وغيرها من الأساليب، وبالرغم من فداحة الخسائر، فإن الأسلحة بسيطة لا تتعدى في أغلب الأحوال (الكيلو بايت) التي تتمثل في فيروسات إلكترونية تخترق شبكة الحاسب الآلي، وتنتشر بسرعة بين الأجهزة وتبدأ عملها في سرية تامة وبكفاءة عالية، وبات من الصعب تخيل صراعاً عسكرياً اليوم دون أن يكون لهذا الصراع العسكري أبعاداً إلكترونية، وأصبحت في صلب اهتمامات الأنظمة الدفاعية لأي صراع يمكن أن يحدث في المستقبل.

إن الثورة المعلوماتية قد غيرت من طبيعة الصراعات والحروب وابتكرت أساليب جديدة فمنها الحروب الموجهة، وحروب الشبكية، والحروب التجسسية، والحروب الفضائية، والحرب النفسية والحرب الإعلامية، والحرب الاقتصادية، وإن نجاح الحروب التي تشن اليوم ومستقبلاً سوف يفوز بها الجانب الذي يتقن حرب المعلوماتية والتجسس على الاتصالات.

وقد خلصت الدراسة إلى النتائج الآتية:

1- فرض الفضاء الإلكتروني نفسه كبعد استراتيجي جديد في الصراعات الدولية، والذي بدوره أحدث تغييرات في مفاهيم العلاقات الدولية، كمفهوم القوة والصراع والأمن، حيث انتشرت القوة بين الفاعلين وتحول الصراع من المادي إلى الافتراضي.

ISSN : 2410-1818

2- أصبح الفضاء الإلكتروني أحد العناصر التي تؤثر في النظام الدولي بما ينتجه من أدوات تكنولوجية مهمة لعملية الحشد والتعبئة في العالم والتأثير في القيم السياسية.

3- أصبح الفضاء الإلكتروني مجالا للتفاعلات الصراعية الدولية، والذي يربط الشبكات الحيوية للدولة عبر نظم اتصال قد تستهدفها الهجمات الإلكترونية، بجانب تهديد البني التحتية العسكرية، وسرقة المعلومات العسكرية أو التلاعب بها، واختراق أنظمة التحكم والسيطرة والحرب النفسية الإلكترونية على العدو.

4- أخذ الصراع الإلكتروني طابعا تنافسيا وهو ما يطلق عليه (سباق التسلح الالكتروني والمعلوماتي) وفي شتى الميادين (السياسية والاقتصادية والعسكرية) وغيرها بين دول العالم.

5- إن ظهور القوة الإلكترونية قد منحت الفواعل الدولية الأصغر قدرة على ممارسة كل من القوة الصلبة والناعمة عبر الفضاء الإلكتروني، كونها تراها حروب قليلة التكلفة وذات حجم تدميري كبير.

6- إن الحروب الإلكترونية أخذت مجالا تفاعليا في العلاقات الدولية، كعامل مهم ومؤثر في الصراعات الدولية، وأن من يمتلك آليات البنية الإلكترونية يصبح أكثر قدرة على تحقيق أهدافه والتأثير في سلوك العدو المستخدم لهذه البنية.

7- الحروب التقليدية قد تغيرت وأصبحت الجيوش الإلكترونية العسكرية في كافة أنحاء العالم تهتم بحروب المعلومات ودورها في الحروب المستقبلية، التي يتوقع الكثير حدوثها في الفضاء الإلكتروني.

8- أصبح هناك مراكز قيادة عالية التكاليف تهتم بالجيوش الإلكترونية على مستوى العالم تقام فيها المناورات والتدريبات على هذا النوع الجديد من الصراعات، وكيفية مواجهاتها والاستعداد لها من خلال تطوير الإجراءات المضادة.

9- إن الترابط بين التكنولوجيا المعلوماتية والحروب الإلكترونية أدى إلى طفرة نوعية مؤثرة جدا في مجال الحروب، فحروب الفضاء الإلكتروني لا توجد بها أي إراقة للدماء ولكنها أخطر من الحروب العسكرية لأنها تستطيع تدمير الأنظمة والأجهزة الإلكترونية وإتلافها مما يمنعها عن العمل بشكل تام.

10- إن دخول العالم في عصر الحروب الهجينة ذات الأشكال والأساليب والموارد البشرية المتعددة، جعل الجيوش الإلكترونية ركنا أساسيا غير مرئية وغير عضوية وكذلك خلاياها القاتلة التي لا يمكن مواجهتها في معزل عن التوعية وتحديث قوانين الإرهاب.

ISSN : 2410-1818

المراجع

1- محمد عاطف إمام، الفضاء الإلكتروني وأثره على الأمن القومي للدول، دراسة منشورة على الانترنت، تاريخ النشر، 23 ابريل 2022م، المركز الديمقراطي العربي، متوفر على الرابط https//democraticac.de.

2- نفس المرجع السابق.

3- قاسم خضير عباس العزاوي، ديناميكية الحروب الإلكترونية وأثرها في العلاقات الدولية. متاح علي الرابط التالي https//democraticac.de

4- محمد عاطف إمام، مرجع سابق.

5- عادل عبد الصادق، أثر الإرهاب الإلكتروني: القوة في العلاقات الدولية، 2001-2007م، رسالة ماجستير، كلية الاقتصاد والعلوم السياسية جامعة القاهرة، 2009م،

6- إيهاب خليفة، القوة الإلكترونية وأبعاد التحول في خصائص القوة، مكتبة الإسكندرية، مصر، 2015م، ص 35-45.

7- الموسعة الجزائرية للدراسات السياسية والاستراتيجية، الجيوش السيبرانية والإلكترونية في العالم، تاريخ النشر 2021/7/30م متاح على الرابط .https://www.politics-dz.com

8- إيهاب خليفة، إمكانيات تحقيق الردع في صراع الفضاء الإلكتروني، دورية اتجاهات الأحداث، العدد13، 2015م.

9- عادل عبد الصادق، القوة الإلكترونية، أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني، مجلة السياسة الدولية، العدد188، مؤسسة الأهرام المصرية، 2012م، ص33.

10- عادل عبد الصادق، القوة الإلكترونية، أسلحة الانتشار الشامل، المرجع السابق، ص45.

11- نفس المرجع السابق.

12- إيهاب خليفة، القوة، كيف تدير الدول شؤونها في عصر الأنترنت (الولايات المتحدة الأمريكية نموذجاً)، العربي للنشر والتوزيع، القاهرة، ط1، 2017م، ص 55.

13- قاسم خضير عباس العزاوي، ديناميكية الحروب الإلكترونية وأثرها في العلاقات الدولية، مرجع سابق.

14- جوزيف ناي، الحرب الناعمة، وسيلة النجاح في السياسة الدولية، متاح على الرابط post- https;alkhanadeg.com.

15- عباس بدران، الحرب الإلكترونية، الاشتباك في عالم المعلومات، مركز دراسات الحكومة الإلكترونية، للنشر والتوزيع، بيروت، 2010م، ص 53.
16- عباس بدران، الحرب الإلكترونية، نفس المرجع السابق، ص 55.
17- نفس المرجع السابق، ص 77.
18- قاسم خضير، مرجع سابق.
19- رياض مهدي عبد الكاظم خلف، المعلوماتية والحروب الحديثة،(دراسة حالة الحرب الأمريكية على العراق عام 2003م، تاريخ النشر 9 أغسطس /2021م، متاح على الرابط https.adhwaa.net
20- نفس المرجع السابق.
21- قاسم خضير عباس، ديناميكية الحروب الإلكترونية، مرجع سابق.
22- رياض مهدي خلف، المعلوماتية والحروب الحديثة، مرجع سابق.
23- الحرب الإلكترونية في مستقبل الصراع الدولي، موقع ارتي عربية، تاريخ النشر2017/10/3م.متاح على الرابط .htt// Arabic.rt.com/world/902434
24- نفس المصدر السابق.
25- رياض مهدي، مصدر سابق.
26- رياض مهدي، مصدر سابق.
27- الحرب الإلكترونية في مستقبل الصراع الدولي، مرجع سابق.
28- الحروب الإلكترونية: معارك العالم الافتراضي تنتقل إلى الميدان، مقال منشور على النت، تاريخ النشر 2018/3/24م، متاح على الرابط .https://orient-news.net/ar/news-show
29- الحرب النفسية والانقلابات في الاستراتيجية الأمريكية، دراسة منشورة على الانترنت، متاح على الرابط التالي .www.nostakbaiat.com.ndex2-htmal
30- الحرب الإلكترونية في مستقبل الصراع الدولي، مرجع سابق.
31- محمد عاطف إمام، الفضاء الإلكتروني وأثره على الأمن القومي للدول، مرجع سابق.
32- صلاح حيدر عبد الواحد، حروب الفضاء الإلكتروني، دراسة في مفهومها وسبل مواجهتها جامعة الشرق الأوسط، 2021م، ص145.
33- نفس المرجع السابق، ص 155.

ISSN : 2410-1818

34- محمد عاطف أمام، الفضاء الإلكتروني وأثره على الأمن القومي، مرجع سابق.

35- جوزيف ناي، مرجع سابق.

36- نسرين الشحات الصباحي، الأبعاد العسكرية للقوة السيبرانية على الأمن القومي للدول (دراسة حالة إسرائيل) دراسة منشورة على النت، متاح على الرابط .https.democrticac.de

37- ورقة بحثية، الفضاء الإلكتروني وأثره على مفاهيم القوة والأمن والصراع في العلاقات الدولية، .متاح على الربط التالي .jocu.journal2.ekb.eg

38- الحرب الإلكترونية في مستقبل الصراع الدولي، مرجع سابق.

39- الفضاء الإلكتروني وأثره على مفاهيم القوة والصراع في العلاقات الدولية مرجع سابق.

40- نقلا عن قاسم خضير ديناميكية الحروب الإلكترونية مرجع سابق

41- نقلا عن المصدر نفسه

42- الفضاء الإلكتروني وأثره على مفاهيم القوة، مرجع سابق.

43- قاسم خضير، مرجع سابق.

44- تداعيات الحرب الإلكترونية على العلاقات الدولية، (دراسة في الهجوم الإلكتروني على إيران)،(فيروس ستاكس نت) دراسة منشورة على النت بتاريخ 2020/6/1م. متاح على الرابط التالي.asjp.cerist.dz/enartide

45- الحروب الإلكترونية : معارك العالم الافتراضي تنتقل إلى الميدان، مرجع سابق.

46- نفس المرجع السابق.

47- نقلاً عن الموسوعة السياسية الجزائرية للدراسات الاستراتيجية، الجيوش السيبرانية والإلكترونية في العالم، تاريخ النشر 2021/7/30م. مرجع سابق.

48- محمد عاطف إمام، مرجع سابق.

49- نسرين الشحات الصباحي، الأبعاد العسكرية للقوة السيبرانية على الأمن القومي للدول، مرجع سابق.

50- نفس المرجع السابق.

51- عصر الجيوش الإلكترونية مالا تعرفه عن الجيوش غير المرئية، شبكة النبأ المعلوماتية، دراسة منشور على الانترنت بتاريخ 92017/28م.

ISSN : 2410-1818

52- الفضاء السيبراني ساحة حروب جديدة قد تشعل العالم، دراسة منشورة على النت بتاريخ 2016/9/27م. متاح على الرابط .www.aljazeera.net

53- د ، محمد عاطف إمام، مرجع سابق.

54- عصر الجيوش الإلكترونية مالا تعرفه عن الجيوش غير المرئية ، مرجع سابق.

55- تداعيات الحرب الإلكترونية على العلاقات الدولية ، دراسة في الهجوم الإلكتروني على إيران، مرجع سابق.

56- نفس المرجع السابق.

57- عصر الجيوش الإلكترونية مالا تعرفه عن الجيوش غير المرئية ، مرجع سابق.

58- الفضاء السيبراني ساحة حروب جديدة قد تشعل العالم،مرجع سابق.

59- عصر الجيوش الإلكترونية مالا تعرفه عن الجيوش غير المرئية ، مرجع سابق.