القرصنة الالكترونية في الفضاء السيبراني "التهديد المتصاعد لأمن الدول"

د.نورة شلوش

أستاذة محاضرة صنف" أ "بجامعة الجزائر ٠٣

البريد الإلكتروني Email : Mahmoudiche@hotmail.fr

الهاتف: ٠٥,٥٤,٠٤,٠٢,٧١

الكلمات المفتاحية: القرصنة الالكترونية، الفضاء السيبراني، التهديد، أمن الدول.

كيفية اقتباس البحث

شلوش ، نورة، القرصنة الالكترونية في الفضاء السيبراني "التهديد المتصاعد لأمن الدول"، مجلة مركز بابل للدراسات الانسانية،٢٠١٨، المجلد:٨ ،العدد: ٢.

Cyber piracy in cyberspace "The growing threat to state security

Dr. Noura Shalouch
Professor of Class A Lecture at the University of Algiers 03

Keywords: Cyber piracy, Cyberspace, Threat, State Security .

How To Cite This Article
Shalouch, Noura, Cyber piracy in cyberspace "The growing threat to state security, Journal Of Babylon Center For Humanities Studies, Year :2018,Volume:8, Issue: 2.

Abstract :

The importance of this research paper on electronic piracy in cyberspace is the growing threat to the security of countries, from the importance of virtual cyberspace and the various cyber attacks received by cyberspace , which today is the first threatened entity of any country with destruction and collapse and the creation of international conflicts among them, for the purpose of the strategies and mechanisms that can be activeated by international systems for the embodiment of cybersecurity international and to know the relationship of electronic piracy to make changes in the security environment, and the identification of the impact of cyber attachs,including electronic piracy in the emergence of new patterns of international conflict the most prominent of these attacks in addition to the nature of these cyber attacks and to the identification of most of the new electronic weapons this paper aims to identify the electronic race that the world is witnessing today by international regimes in the extent to which cybercrime can be reduce in cyberspace.

الملخص:

تأتي أهمية هذه الورقة البحثية الموسومة ب **القرصنة الالكترونية في الفضاء السيبراني "التهديد المتصاعد لأمن الدول"** من أهمية موضوع الفضاء السيبراني الافتراضي ومختلف الهجمات السيبرانية التي يتلقاها الفضاء الالكتروني والتي أصبحت اليوم المهدد الأول لكيان أي دولة بالدمار والانهيار وخلق صراعات دولية فيما بينها، ولهذا جاءت هذه الورقة البحثية تجسيدا لأهداف البحث والتي منها: التعرف على الاستراتيجيات والآليات التي يمكن تفعيلها من قبل الأنظمة الدولية لتجسيد الأمن السيبراني الدولي ومعرفة مدى علاقة القرصنة الالكترونية بإحداث تغييرات في البيئة الأمنية السيبرانية الدولية، والتعرف على تأثير الهجمات السيبرانية ومنها القرصنة الالكترونية في بروز أنماط جديدة للصراع الدولي مع التقرب من طبيعة هذه الهجمات السيبرانية، بالإضافة إلى التعرف على أغلب الأسلحة الالكترونية الجديدة، وتهدف هذه الورقة البحثية أيضا إلى التعرف على السباق الالكتروني الذي يشهده العالم اليوم من طرف الأنظمة الدولية في مدى إمكانية الحد من هذه الهجمات السيبرانية في الفضاء السيبراني.

مقدمة:

شهدت البشرية منذ سنوات تقدما تقنيا وتكنولوجيا، قلما عرفه عصر من العصور السابقة من قبل، حتى بات هذا التقدم ثورة قائمة بذاتها في عالم الاتصالات والعلاقات الدولية، كما أصبح العالم بفضلها بمثابة قرية كونية فعلا، بحيث أصبح للفضاء السيبراني الافتراضي دور في حركة التفاعلات والتحولات البنيوية كمجال جديد في العلاقات الدولية وبدأ ينتقل تأثيره من تغييرات هيكلية وتحتية إلى إحداث تغييرات كيفية في النظام الدولي حتى أصبح العالم اليوم يشهد تطورا في المخاطر الأمنية مع تطور مراحل النضج التكنولوجي مع الانتقال من مرحلة النمو السريع إلى مرحلة الاستخدام الكثيف، وبذلك أصبحت قضية أمن الفضاء الالكتروني من عمليات القرصنة الالكترونية والهجمات السيبرانية والتي بدوها تؤثر على أمن الدول تلقى اهتماما متصاعدا على أجندة الأمن الدولي وذلك في محاولة لمواجهة تصاعد التهديدات الالكترونية ودورها في التأثير على الطابع السلمي للفضاء الالكتروني، وباتت العلاقة بين والتكنولوجيا وامن الدول علاقة طردية فبتطور التكنولوجيا تتزايد إمكانية تعرض المصالح الإستراتيجية ذات الطبيعة الالكترونية إلى أخطار الكترونية منها القرصنة الالكترونية في الفضاء السيبراني الذي يمثل التهديد الأكبر لأمن الدول خاصة وان الفضاء الالكتروني غدا وسيط ومصدر لأدوات جديدة للصراع الدولي المتعدد الأطراف والمزود الأول لتغذية التوترات الدولية.

إشكالية البحث: من خلال ما سبق تتضح الإشكالية الرئيسية للبحث وهي:

Journal Of Babylon Center For Humanities Studies2018 Volume: 8 Issue : 2
(ISSN): 2227-2895 (Print) (E-ISSN):2313-0059 (Online)

ما هي الاستراتيجيات والآليات التي يمكن تفعيلها من قبل الأنظمة الدولية لتجسيد الأمن السيبراني الدولي من القرصنة الالكترونية؟

وتندرج ضمن هذه الإشكالية الرئيسية مجموعة من الأسئلة الفرعية تتمثل أساسا في:

- ✓ ما مدى علاقة القرصنة الالكترونية بإحداث تغييرات في البيئة الأمنية السيبرانية الدولية؟
- ✓ ما هي أبرز الهجمات السيبرانية؟
- ✓ كيف أثرت الهجمات السيبرانية ومنها القرصنة الالكترونية في بروز أنماط جديدة للصراع الدولي؟
- ✓ هل يشهد العالم اليوم سباق الكتروني؟ وما هي أغلب الأسلحة الالكترونية الجديدة؟
- ✓ هل يمكن الحد من هذه الهجمات السيبرانية في الفضاء السيبراني؟

فرضيات البحث: للإحاطة بحيثيات البحث اعتمدنا الفرضيات التالية:

- يشهد العصر الحالي تغيرات سريعة وكثيفة في ظل التكنولوجيا منها الايجابية والسلبية، فكانت التغيرات السلبية لها أقوى درجة من التأثير خاصة في مجال المساس بأمن الدول وذلك نتيجة انتشار الهجمات السيبرانية في الفضاء السيبراني، مما توجب على الأنظمة الدولية التفطن لوضع استراتيجيات جديدة للحد من هذه الهجمات السيبرانية.
- تتجسد علاقة القرصنة الالكترونية بإحداث تغييرات عميقة ومؤثره سلبا على امن البيئة السيبرانية الأمنية للدول.
- تبرز أغلب الهجمات السيبرانية في الفضاء السيبراني في الهجمات السرية المتعلقة باستخدام التجسس بوسائل تكنولوجية فائقة الجودة وعمليات الاختراق للأنظمة الالكترونية والبيانات المختلفة.
- تؤثر الهجمات السيبرانية ومنها القرصنة الالكترونية في بروز أنماط جديدة من الصراع الدولي.
- يشهد العالم اليوم سباق الكتروني في ظهور أسلحة الكترونية جديدة وذلك في إطار التصدي للهجمات السيبرانية وذلك بالوصول إلى عسكرة الفضاء الالكتروني.

أهمية البحث:

تأتي أهمية هذه الورقة البحثية الموسومة ب **القرصنة الالكترونية في الفضاء السيبراني "التهديد المتصاعد لأمن الدول"** من أهمية موضوع الفضاء السيبراني الافتراضي ومختلف الهجمات السيبرانية التي يتلقاها الفضاء الالكتروني والتي أصبحت اليوم المهدد الأول لكيان أي

دولة بالدمار والانهيار وخلق صراعات دولية فيما بينها، خاصة وان جل المجتمعات الحديثة أصبحت تعتمد بشكل متنامي على التكنولوجيات مما باتت القرصنة الالكترونية تهدد الأمن السيبراني الذي يشكل جزء أساسيا من أي سياسة أمنية دفاعية دولية، لاسيما وان أكثر من ١٣٠ دولة حول العالم تخصص أقساما ومرافق خاصة بالحرب السيبرانية ضمن فرق الأمن الوطني لأي دولة والتي تضاف جميع هذه الجهود إلى الجهود الأمنية التقليدية لمحاربة الجرائم الالكترونية، القرصنة الالكترونية والاحتيال الالكتروني والأوجه الأخرى للمخاطر السيبرانية.

أهداف البحث:

- التعرف على الآليات التي يمكن تفعيلها من قبل الأنظمة الدولية لتجسيد الأمن السيبراني الدولي.
- معرفة علاقة القرصنة الالكترونية بإحداث تغييرات في البيئة الأمنية السيبرانية الدولية.
- التعرف على تأثير الهجمات السيبرانية ومنها القرصنة الالكترونية في بروز أنماط جديدة للصراع الدولي.
- التعرف على أغلب الأسلحة الالكترونية الجديدة.
- التعرف على السباق الالكتروني الذي يشهده العالم من طرف الأنظمة الدولية.
- التعرف على إمكانية الحد من هذه الهجمات السيبرانية في الفضاء السيبراني.

هيكل البحث:

للإجابة على الإشكالية المطروحة تم تقسيم البحث إلى المحاور التالية:

المحور الأول: ماهية الفضاء السيبراني، مفهومه، أنواعه، خصائصه، هجماته السيبرانية.

المحور الثاني: جدلية الصراع الالكتروني في الفضاء السيبراني وبزوغ القوة الالكترونية للدول.

المحور الثالث: القرصنة الالكترونية وتحديات الأمن العالمي أمام الخطر،المواجهة والمسؤولية.

المحور الرابع: استراتيجيات الردع السيبراني من الهجمات السيبرانية " المتطلبات والحلول".

المحور الأول: ماهية الفضاء السيبراني، مفهومه ،خصائصه، هجماته السيبرانية:

١/ مفهوم الفضاء السيبراني:

تختلف التعريفات حول الفضاء السيبراني على حسب طبيعة كل دولة أو كيان وعلى مدى قدرته على تحديد رؤيته وإستراتيجيته للتعامل مع مجال الفضاء السيبراني بشقيه المدني والعسكري وكذلك مدى قدرته على استغلال المزايا ومواجهة المخاطر الكامنة في هذا المجال

فهناك من عرفه على: بأنه عالم افتراضي يتشابك مع عالمنا المادي ، يتأثر به ويؤثر فيه بشكل معقد، حيث تقوم العلاقة بين العالمين على نظرة تكاملية تحمل بين طياتها مزايا ومخاطر لا تتوقف **وهناك من وصفه** بالذراع الرابعة للجيوش الحديثة إلى جوار القوات الجوية والبحرية والبرية وخاصة أن الانترنت شهد بداية الحديث عن معارك حقيقية تدور في هذا العالم الافتراضي.[١]

وهناك من يرى أنه يمثل البعد الخامس للحرب، **كما يعرف على أنه:** المجال المادي وغير المادي الذي يتكون من عناصر هي أجهزة الكومبيوتر، والشبكات والبرمجيات وحوسبة المعلومات والمحتوى ومعطيات النقل والتحكم ومستخدمو كل هذه العناصر، حيث تعد كل هذه العناصر العامل المشترك في جميع محاور استخدام الفضاء السيبراني، سواء أكانت الجهات المستخدمة قادرة على تعظيم قيمتها وقدراتها بما في ذلك رفع كفاءة العنصر البشري أم كانت في مرحلة متأخرة.[٢]

خصائص الفضاء السيبراني:

يعتمد الفضاء السيبراني كمجال افتراضي على نظم الكمبيوتر وشبكات الانترنت ومخزون هائل من البيانات والمعلومات، بحيث يتم الاتصال بالشبكات غير الحواسيب أو الهواتف أو غيرها من دون تقيد بالحدود الجغرافية، وقد ظهر مصطلح الفضاء السيبراني في ثمانينات القرن الماضي في إحدى روايات الخيال العلمي للكتاب الأمريكي الكندي ويليام جيبسون [١]، ويوصف العصر الحالي بأنه العصر الرقمي، فهو يتضمن تطورات تكنولوجية هائلة تخدم جميع مناحي الحياة العامة والخاصة، وتنعكس على خدمة المجتمع الدولي بأكمله، حيث بات العصر يتحرك من خلال تكنولوجيا المعلومات والاتصالات التي واكبتها حركة إجرامية كبيرة، فانتشرت الجرائم المعلوماتية بشكل خطير في جميع دول العالم التي أصبحت عرضة للوقوع تحت تهديد هذه الجرائم باستخدام الفيروسات وبرامج التجسس وغيرها وهي أدوات يمكن وصفها مجازا بالجراثيم المستحدثة أو المختلفة. [٢]

وتكمن مخاطر هذا المجال في صعوبة تحديد هوية الكيان الذي نفذ الهجمات السيبرانية في الكثير من الحالات، وكذلك غياب التشريعات الدولية التي تضع الدول أو المؤسسات التي تقوم بمثل هذه الأنشطة تحت طائلة القانون الدولي، ما يعني عدم القدرة على ملاحقتها قانونيا على خلاف مجالات الحرب التقليدية. [٣]

أنواع الهجمات السيبرانية:

تعرف الهجمات السيبرانية على أنها فعل يقوض من قدرات وظائف شبكة الكومبيوتر لغرض قومي أو سياسي، من خلال استغلال نقطة ضعف ما تمكن المهاجم من التلاعب بالنظام ومن بين الهجمات السيبرانية ما يلي:

سرقة كلمات المرور للمستخدمين للتسلل في النظام: مثل التخمين والخداع والبرمجيات الخبيثة والنفاذ إلى ملف تخزين كلمة المرور والسطو على كلمات المرور السرية والتجسس على المستخدمين.

- **هجمات رفض أداء الخدمة** "إنكار الخدمة" (هجمات دوس DDOS) [١]

تستخدم لزيادة التحميل على الانترنت والبنية التحتية للشبكات والخدمات وهو يزعج الشركات والمنظمات، وهو على العكس من التقنيات التي يستخدمها مجرمو الانترنت، فهي تمنع المستخدمين الشرعيين من الوصول إلى المنتجات والخدمات ويمكن أن يرتكبها فرد أو جماعة.

وهي تعتمد على العديد من الروبوتات وهي نوعين:

- **القائم على اتصال:** يحدث عندما يكون هناك تبادل بين الخادم والعميل باستخدام طرق معينة.
- **منقطع الاتصال:** القائمة على غير اتصال.
- وتأثير هجمات دوس على الشركات ، باعتبارها قادرة على شن هجمات من حيث الحجم والمدة والتعقيد التكنولوجي وهذه الهجمات تطورت باستمرار.
- **الهجمات الطمسية:** هي عن طريق استبدال الصفحات بغيرها بهدف الشك والتقلب.
- **هجمات البنية التحتية:** والتي تستهدف شبكات الكهرباء والاتصالات والأغذية والصرافة والمالية والمهام الحكومية .....
- **قراصنة المعلومات:** يتمثل ذلك في الهاكرز والأنونميوس والكراكرز، فالهاكرز: هما المبرمجين القادرين على التعامل مع الكمبيوتر ومشاكله بدراية احتراف ويقدمون حلولاً لمشاكل البرمجة بشكل تطوعي وهما نوعين:

✓ **المحترفين:** والذين يستخدمون برامج أو تقنيات في محاولات للاختراق الأنظمة والأجهزة للحصول على معلومات سرية أو للتخريب.

✓ **المبتدئين:** يتسللون عبر الشبكات الهاتفية اعتمادا على تقنية غير قانونية وهما من أخطر أنواع الهاكرز. [٢]

Journal Of Babylon Center For Humanities Studies2018 Volume: 8 Issue : 2
(ISSN): 2227-2895 (Print) (E-ISSN):2313-0059 (Online)

المحور الثاني: جدلية الصراع الالكتروني في الفضاء السيبراني وبزوغ القوة الالكترونية للدول.

١/ عصر الصراع الالكتروني في الفضاء السيبراني:

بعد أحداث ١١ سبتمبر ٢٠٠١ بدأ التركيز على الفضاء الإلكتروني كتهديد أمني جديد بفعل أحداث دولية كان أبرزها استخدام تنظيم القاعدة له كساحة قتال ضد الولايات المتحدة ، وفي عام ٢٠٠٧ برز بوضوح دور الفضاء الإلكتروني كمجال جديد في العمليات العدائية في الصراع بين استونيا وروسيا وفي ٢٠٠٨ في الحرب بين روسيا و جورجيا،وجاء الهجوم الإلكتروني بفيروس "ستاكسنت" على برنامج إيران النووي عام ٢٠١٠ ليمثل نقلة هامة بالتطور في مجال الأسلحة الإلكترونية . وعلى الرغم من الدور السياسي الذي لعبته شبكات التواصل الاجتماعي في حالة الثورات العربية في مطلع عام ٢٠١١ إلا أنها مثلت نقطة هامة لدعم الاهتمام الدولي بأمن الفضاء الإلكتروني ، وبرزت محاولات للسيطرة عليها بعد تصاعد الاحتجاجات في أكثر البلدان ديمقراطية وهي بريطانيا والولايات المتحدة.

وخلال العقد الأخير شهد المجتمع الدولي صعود قضايا الأمن الإنساني المشترك والتغير في المجال الاقتصادي والاعتماد المتبادل وضعف دور الدولة وبروز الفاعلين من غير الدول[١]. وصاحب ذلك التغير موجة انتشار هائلة لتكنولوجيا الاتصال والمعلومات والتي انتشرت من حيث الكم بمعدلات غير مسبوقة ، ومن الناحية الوظيفية دخلت بكثافة في عمل العديد من المرافق الحيوية ، وسرعت من انتقال الأفكار والأموال والأفراد بين دول العالم.ومن أهم مظاهر كثافة التفاعلات الدولية وصول عدد مستخدمي الإنترنت لـ٢,١ مليار مستخدم ،و٢,٤ مليار يستخدم الشبكات الاجتماعية ، و٣,١٤٦ مليار حساب بريد إلكتروني ،و ٥,٩ مليار مستخدم للمحمول ، و بليار فيديو تم فتحه من اليوتيوب.

وهو ما يعزز في ذات الوقت من انتشار الأنشطة غير السلمية للفضاء الإلكتروني، الذي يتجاوز الحدود الدولية، أصبح الفضاء الإلكتروني يواجه بتهديدات متصاعدة نتيجة البيئة الأمنية الجديدة بسبب أولا:ارتباط العالم المتزايد بالفضاء الإلكتروني بما عمل على زيادة خطر تعرض البنية التحية الكونية للمعلومات لهجمات إلكترونية. وثانيا: استخدام الفاعلين من غير الدول للفضاء الإلكتروني لتحقيق أهدافهم وتأثير ذلك على سيادة الدولة. وثالثا: انسحاب الدولة من قطاعات إستراتيجية لصالح القطاع الخاص وخاصة بالمنشآت الحيوية ، ورابعا: تأثير مواجهة الحرب الإلكترونية على حرية استخدام الفضاء الإلكتروني وخامسا : إشكالية تعامل الدول مع الشركات

التكنولوجية متعدية الجنسيات والتي أصبحت تفوق قدراتها مثل مواقع الشبكات الاجتماعية كالفيس بوك وتويتر واليويتوب الذين أصبحوا فاعلين دوليين.

وساهمت تلك المتغيرات في بروز وعي عالمي بما يحدث و درجة عالية من التأثير والتأثر في أرجاء العالم المختلفة،وأفرز الفضاء الإلكتروني بيئة دولية جديدة تمثلت في إعطاء دفعة قوية لزيادة المعرفة في عمليات الإنتاج والابتكار، والأهمية المتزايدة للاتصالات وهي أحد أوجه الأمن مما جعل هذه البيئة الإلكترونية حقيقة غير مسبوقة ،بالإضافة إلى عدم كفاية الاعتماد على القوة العسكرية، وإعادة النظر في تعريف الأمن؛ مع ظهور أوجه غير عسكرية له ، واتجه الصراع الدولي حول الموارد والمصالح والقيم نحو الاعتماد على تكنولوجيا الاتصال والمعلومات فيما يعرف بصراع "عصر المعلومات" والتنافس في ساحة الإنجازات ذات الطبيعة المادية وصراع آخر حول الأفكار والقيم [١]

وتتأثر حالة الصراع وانعدام الأمن في الفضاء الإلكتروني بكل أنواع البيئات الأخرى غير المتصلة بالفضاء الإلكتروني كالنزاعات بين الأفراد والصراع بين الجماعات والصراع بين الدول أو صراع بين الشركات الدولية ، وتعددت أنماط الصراع ما بين صراع ذي طابع قانوني وتجاري أو صناعي وعسكري وسياسي وامتد تأثير ذلك ليشمل كافة المجالات الأخرى **التي تدور على ارض الواقع.**

وأصبح الفضاء الإلكتروني ساحة جديدة للصراع بشكله التقليدي ولكنه ذو طابع إلكتروني يعكس النزاعات التي تخوضها الدول أو الفاعلين من غير الدول على خلفيات دينية أو عرقية أو إيديولوجية أواقتصادية أو سياسية . ويتمدد الصراع الإلكتروني بداخل شبكات الاتصال والمعلومات متجاوزا الحدود التقليدية وسيادة الدول، ويؤثر ذلك في امتداد مجاله وتداعياته أو آثاره، وأضافت عملية تعدد الاستخدام والفاعلين والمصالح لتنوع أشكال الصراع وأهدافه.

ولأن الصراعات "الفعلية" تستعمل شتى أنواع أسلحة التدمير الاقتصادية والإلكترونية والسياسية والإعلامية، فإنها لم تتوان عن استخدام الفضاء الإلكتروني، بما له من تأثير نفسيً ومعنويً وإعلامي ثم أصبح له تأثير أمني وعسكري لتزحف جبهات القتال التقليدية بشكل مواز لها إلى ساحة الفضاء الإلكتروني [1]

وكشف استخدام الفضاء الإلكتروني **عن حالة التعارض الحقيقي أو المتخيل للاحتياجات والقيم والمصالح بين العديد من الفرقاء سواء أكانوا دولا أو أفرادا أو جماعات** أو شركات ، وبما ساعد على بلورة أساليب للصراع الدولي ذات الطابع التقني والتجاري والاقتصادي والعسكري ،

إلى جانب ظهور طرق بديلة عن الحرب المباشرة بين الدول أو بين الخصوم عبر شبكات الاتصال والمعلومات[2]

وكان لتلك التغييرات دور في إعادة التفكير في حركية وديناميكية الصراع والأمن على نحو يعكس التطور الذي فرضه الفضاء الإلكتروني على المجتمع الدولي ، وخاصة في ظل تزايد حالة الاعتماد المتبادل ،وهو ما ساعد في ظهور ما يعرف بـ "عصر القوة النسبية" الذي يعني بعجز " القوة العسكرية" عن تأمين الأهداف السياسية المترتبة عليها، مما يخلف آثارا إستراتيجية هائلة على مستوى تركيبة وتوازنات النظام الدولي.

وذلك بعد أن تغير "براديم" الحرب جذريا بانتقاله من نسق "الحروب الصناعية بين الدول" إلى نسق "الحرب في وسط الشعوب". ففي الحروب القديمة كان الغرض هو تدمير الخصم ، إما باحتلال أرضه أو الاستيلاء على موارده ، بينما أصبح في الحرب الجديدة هو التحكم في إرادته وخياراته ، ومن ثم كان الدور المحوري للشعوب في هذا الصنف الجديد من الحروب، سواء تعلق الأمر بالسكان المستهدفين في أرضية المواجهة، أو بالرأي العام في الدولة التي تشن الحرب ، أو بالرأي العام الإقليمي والدولي . وأصبحت أهداف الحرب أقل مادية ، يؤدي فيها العامل النفسي والدعائي دورا محوريا ، وسببه تنامي التغطية الإخبارية السمعية البصرية المباشرة للأحداث لحظة وقوعها عبر مواقع الإنترنت والفضائيات إلى جانب ضعف سيطرة أنظمة الحكم على توجهات مواطنيها.

وعلى الرغم من سعى الجيوش النظامية لاستغلال تفوقها التقني العسكري . الإعلامي الكاسح، لحسم حرب نظيفة سريعة تجنب السكان فظائع وآلام المواجهة، فان إستراتيجية الشبكات الإلكترونية المسلحة المقاومة لها هي الاستخدام المعاكس لهذه الميزات التقنية ، إلى جانب اتباع إستراتيجية مواجهة متدرجة تؤدي إلى إنهاك الخصم للتغلب عليه بالتسلل إلى وسط السكان والاحتماء بهم وزعزعه ثقتهم في مؤسسات الدولة وبالتالي تحويلهم إلى أرضية مواجهة بديلة عن المواجهة المباشرة بين دول ، ويتم في ذلك توجيه سلاح الصورة إلى مآسي الحرب وجرائمها الإنسانية بما يعمل على شحن الرأي العام ، وهو ما برز بظهور فكرة "إسقاط النظام من الداخل" بدلا من استخدام القوة العسكرية الخارجية كحالة العراق.

وفي هذا المشهد تنمحي الفروق التقليدية بين الحرب والسلم ، ففي الوقت الذي يغدو فيه الصدام السمة الغالبة على الوضع الاستراتيجي الدولي فإنه أفرز تعاونا متبادلا ، وإن كان نادرا ما

يتطور إلى حالة مواجهة مسلحة للوعي المتزايد بعدم قدرة الحسم العسكري في إطفاء بؤر التوتر القائمة. وتم توظيف التطرف ذي الخلفيات الدينية أو القومية لتحويل استخدام التكنولوجيا من أداة مدنية إلى أداة عسكرية وذات أبعاد تخريبية [1]

ومن أهم أشكال الصراع في عصر المعلومات هما حرب الشبكات وحرب الفضاء الإلكتروني Cyber war & Net war، وعلى الرغم من زيادة معدلات استخدام تلك الأشكال إلا إن ذلك لا يعني بالضرورة اعتمادها فقط وسائل تكنولوجيا الاتصال والمعلومات بل تأتي مواكبة أو معبرة عن استخدام الآليات التقليدية للصراع ولكن بوجه تكنولوجي يتواكب مع عصر المعلومات [2] .

ويتميز الصراع الإلكتروني Cyber Conflict بأن به تدمير لا تصاحبه دماء وأشلاء بالضرورة ، يتضمن التجسس والتسلل ثم النسف لكن لا دخان ولا أنقاض ولا غبار ، ويتميز أطرافه بعدم الوضوح وتكون تداعياته خطيرة سواء عن طريق تدمير المواقع على الإنترنت ونسفها وقصفها بوابل من الفيروسات أو العمل على استخدام أسلحة الفضاء الإلكتروني المتعددة ، للنيل من سلامة تلك المواقع ، وهي أسلحة يسهل الحصول عليها من خلال مواقع الإنترنت أيضا وتعلم كيفية استخدامها كما إن انتشار الفضاء الإلكتروني وسهولة الدخول إليه يمكن أن يوسع دائرة استهداف المواقع بالإضافة إلى زيادة عدد المهاجمين، ولتدور تلك الهجمات المتبادلة على نحو من الكر والفر ليعبر عن حالة صراع ممتد يرتبط بطبيعة الفضاء الإلكتروني المختلفة3

وهناك صراع إلكتروني تحركه دوافع سياسية ويأخذ شكلا عسكريا ويتم فيه استخدام قدرات هجومية ودفاعية عبر الفضاء الإلكتروني وذلك بهدف إفساد النظم المعلوماتية والشبكات والبنية التحتية وبما يتضمن استخدام أسلحة وأدوات إلكترونية من قبل فاعلين داخل المجتمع المعلوماتي أو من خلال التعاون ما بين قوى أخرى لتحقيق أهداف سياسية [1]

وهناك صراع إلكتروني ذو طبيعة ناعمة عن طريق الصراع حول الحصول على المعلومات والتأثير في المشاعر والأفكار وشن حرب نفسية وإعلامية، ويتم أيضا من خلال تسريب المعلومات واستخدامها عبر منصات إعلامية بما يؤثر على طبيعة العلاقات الدولية كالدور الذي لعبه موقع ويكيليكس في الدبلوماسية الدولية [2]

ويأخذ الصراع الإلكتروني طابعا تنافسيا حول الاستحواذ على سبق التقدم التكنولوجي وسرقة الأسرار الاقتصادية والعلمية إلى أن يمتد ذلك الصراع إلى محاولة السيطرة على الإنترنت من خلال السعي للسيطرة على أسماء النطاقات وعناوين المواقع ، والتحكم بالمعلومات ، والعمل

على اختراق الأمن القومي للدول بدون استخدام طائرات أو متفجرات أو حتى انتهاك للحدود السيادية كهجمات قراصنة الكمبيوتر وتدمير المواقع والتجسس بما يكون له من تأثير على تدمير الاقتصاد والبنية التحتية بنفس القوة التي قد يسببها تفجير تقليدي مدمر.

وخاصة مع صعوبة الفصل بين النشاط الذي يتعلق بالاستخبارات وجمع المعلومات وحرب الفضاء الإلكتروني أو التمييز بين الاستخدام السياسي والإجرامي، وتساهم البيئة المثالية تلك للفضاء الإلكتروني في عمل الجماعات المختلفة ودعم القدرة على تشكيل شبكة عالمية بدون سيطرة مباشرة بالإضافة إلى رخص التكلفة وسهولة الاتصال وضعف الرقابة التقليدية عليه ومثل ذلك عنصر جذب لاستخدامها وتوظيفها لتحقيق أهداف سياسية وعسكرية. وساعدت البيئة المحلية والسياق الدولي للفضاء الإلكتروني على بروز الصراعات ذات البعد المحلي– الدولي من خلال توفير بيئة مناسبة لدمج الفئات والقوى المهمشة في السياسة الدولية وخلق شبكة تحالفات مؤيدة أو معارضة ذات نطاق دولي عريض إما على أساس قيم حقوقية أو انتماءات عرقية أو دينية [3]

وساهم الفضاء الإلكتروني في دعم الهيكل التنظيمي والاتصالي للحركات والجماعات والمنظمات المدنية إلى جانب بروز ظاهرة الفاعلين من غير الدول في عمليات التجنيد والحشد والتعبئة والتمويل

وتنتقل الصراعات الممتدة عبر الفضاء الإلكتروني وتتميز بحدوث حالات متكررة للقرصنة المتبادلة دون أن تسفر عن حرب تقليدية بالضرورة وخاصة مع صعود دور "الفرد" في العلاقات الدولية مثل حالة الصراع العربي الإسرائيلي أو ما بين باكستان والهند أو ما بين الصين والولايات المتحدة أو ما بين الصين وتايوان أو كوسوفا أو غيرها من مناطق الصراعات.

ويمكن أن يستخدم الفضاء الإلكتروني كوسيلة من وسائل الصراع داخل الدولة Inte–State Conflict، بين مكوناتها على أساس طائفي أو اقتصادي أو ديني ، وهو ما يساعد على كشف ديناميكيات التفاعل الداخلي إلى الخارج بما يسهل من عملية الاختراق الخارجي عبر شبكات الاتصال بدعم أحد أطراف الصراع بأدوات غير قتالية.

وكان لتكنولوجيا الاتصال والمعلومات دور في وجود أهداف ووسائل جديدة ، وأوجدت قابلية التعرض للهجوم ، وهو ما أوجد نوعاً جديداً من الضرر دون الحاجة للدخول الطبيعي والمادي

لإقليم الدولة ، وذلك لاعتماد الدول على الأنظمة الإلكترونية في كافة منشأتها الحيوية بما يجعل من تلك الأنظمة هدفا للهجوم، وخاصة أن تلك الأنظمة تحمل طابعا مدنياً وعسكريا مزدوجا. وذلك بعد أن تمخض عن الثورة التكنولوجية ثورة أخرى هي الثورة في الشؤون العسكرية وتطور تقنيات الحرب .

القوة الالكترونية للدول:

أدت علاقة الفضاء الإلكتروني بعمل المنشآت الحيوية سواء أكانت مدنية أو عسكرية لقابلية تعرضها لهجوم من خلاله إما يستهدفه كوسيط وحامل للخدمات أو بشلل عمل أنظمتها المعلوماتية ، ويكون من شأنه التأثير علي القيام بوظيفتها ومن ثم فإن التحكم في تنفيذ هذا الهجوم يعد أداة سيطرة ونفوذ إستراتيجية بالغة الأهمية سواء في زمن السلم أو الحرب.وأحدث التطور السريع لتكنولوجيا الكمبيوتر وخاصة في الشبكات تحولا كبيرا في مفهوم القوة ترتب عليه دخول المجتمع الدولي في مرحلة جديدة تلعب فيها هجمات الفضاء الإلكتروني دورا أساسيا سواء في تعظيم القوة أو الاستحواذ على عناصرها الأساسية.وأصبح التفوق في مجال الفضاء الإلكتروني عنصرا حيويا في تنفيذ عمليات ذات فاعلية في الأرض وفي البحر والجو والفضاء. واعتماد القدرة القتالية في الفضاء الإلكتروني على نظم التحكم والسيطرة.[١]

وقد أوجدت ملايين أجهزة الكمبيوتر المنتشرة في كل مكان عالما افتراضيا نشأ نتيجة عملية الاتصال، ومثل وسيطا جديدا للقوة حيث يمكن للقراصنة دخول الفضاء الإلكتروني بهدف محاوله السيطرة على الأجهزة وسرقة المعلومات وإفسادها أو تعطيلها .[٢]

وإذا كان الأمن القومي يعني بحماية وغياب التهديد لقيم المجتمع الأساسية وغياب الخوف من خطر تعرض هذه القيم للهجوم فإن الفضاء الإلكتروني قد فرض إعادة التفكير في مفهوم الأمن والذي يتعلق بتلك الدرجة التي تمكن الدولة من أن تصبح في مأمن من خطر التعرض للهجوم العسكري أو الإرهابي، وإجراءات الحماية ضد تعرض المنشآت الحيوية للبنية التحتية للأعمال العدائية من خلال الاستخدام السيئ لتكنولوجيا الاتصال والمعلومات.

وأصبحت قضية امن الفضاء الإلكتروني تدخل في استراتيجيات الأمن القومي للعديد من الدول من اجل الاستحواذ على مصادر القوة داخل الفضاء الإلكتروني ، للعمل على الحيلولة دون تعرض بنيتها التحتية الحيوية للخطر الذي ينجم جراء قطع خدمة الإنترنت أو ضرب مواقعها أو توقف رسائل البث الإذاعي أو التلفزيوني أو توقف موجات الراديو أو سقوط

شبكات المحمول أو البث الفضائي ، وأصبح لها تأثير عميق على المجتمع والاقتصاد على النطاق الدولي .[٣]

وبذلك دخل المجال الإلكتروني ضمن المحددات الجديدة للقوة وأبعادها الجديدة من حيث طبيعتها وأنماط استخدامها بل وأيضا طبيعة الفاعلين وهو ما كان له انعكاس على قدرات الدول وعلاقاتها الخارجية ، وهو ما أضفي خصائص جديدة للقوة والتي تعني "بأنها مجموعة الوسائل والطاقات والإمكانيات المادية وغير المادية، المنظورة وغير المنظورة التي بحوزة الدولة، يستخدمها صانع القرار في فعل مؤثر يحقق مصالح الدولة، وتؤثر في سلوك الوحدات السياسية الأخرى [٤]

ويتضمن مفهوم " **القوة الإلكترونية** " أو cyber power تغطية كافة القضايا التي تندرج تحت إطار الصراع الإلكتروني بشكل يختلف عن مسمى " الحرب الإلكترونية cyber warr " والذي يشير إلى التطبيقات العسكرية للفضاء الإلكتروني ويتم الإشارة إليه بالهجوم الإلكتروني عندما يتم اعتباره نمطا من الهجوم يتم شنه من قبل الدولة أو الفاعلين من غير الدول والتي يكون لها تداعيات على الأمن القومي للدول والأمن العالمي.

ويقدم "جوزيف ناي" مصطلح" **القوة الإلكترونية** "لفهم الدور الذي تلعبه الإنترنت في تشكيل قدرة الأطراف المؤثرة، والتي يعد من أبرزها الأطراف الدولية والدول الناشئة، لتحقيق أهدافها.وبأن العصر الإلكتروني قد قلل من صعوبات الدخول وأعطى الأطراف القدرة والقوة ولكن القوة الإلكترونية في الوقت نفسه فرضت تحديات كبرى على هؤلاء الأطراف، وخاصة بالنسبة لأطراف ذات تاريخ مثل الولايات المتحدة.التي كان لديها ما يشبه الاحتكار لمصادر القوة منذ نهاية الحرب الباردة ،ولتظهر عملية انتقال القوة وانتشارها بين أطراف متعددة سواء أكانت دولا أو من غير الدول [١]

ويمكن القول أن عناصر القوة الإلكترونية ترتكز على وجود نظام متماسك يعظم من القوة المتحصلة من التناغم بين القدرات التكنولوجية ، والسكان، والاقتصاد، والصناعة، والقوة العسكرية، وإرادة الدولة وغيرها من العوامل التي تسهم في دعم إمكانيات الدولة علي ممارسة الإكراه، أو الإقناع أو ممارسة التأثير السياسي علي أعمال الدول الأخرى، أو علي الحكام في العالم بغرض الوصول للأهداف الوطنية من خلال قدرات التحكم والسيطرة على الفضاء الإلكتروني. وعكست عملية تغيير طبيعة القوة في العلاقات الدولية طبيعة التغيرات الأفقية والرأسية في النظام الدولي ، والتي كان فيها للبعد التكنولوجي والاتصالي دور هام سواء على مستوى الثورة في الشئون العسكرية أو فيما يتعلق ببروز مجال جديد للصراع الدولي أو ما يتعلق بانتشار القوة الاقتصادية وانتقال معايير القوة القومية من خصائص السكان والمساحة

وعدد الجيش والموارد إلى أبعاد جديدة تتعلق بدور الدولة في الابتكار والإنتاج التكنولوجي حيث أصبحت دولة مثل سنغافورة لديها ناتج محلي إجمالي يفوق دول لديها القوة القومية بالمعايير القديمة، ولم تعد القوى الكبرى تحتكر القوة وحدها مع بروز ظاهرة الاعتماد المتبادل وتعدي الشبكات للحدود الدولية بما فتح المجال أمام لاعبين دوليين جدد ، فضلا عن أن تكلفة الحصول على القوة أصبحت متدنية مع ثورة المعرفة والاتصالات وهو ما مكن أطرافا جديدة من الدخول ببساطة للشؤون الدولية والتأثير فيها.وزادت حالة الانكشاف الأمني للدول وذلك باعتمادها المتزايد على الفضاء الإلكتروني كبرنامج الحكومات الإلكترونية والتي تصبح عرضة للاختراق والهجوم بالفيروسات وسرقة المعلومات أو إتلافها والتي أصبحت معضلة جديدة للأمن بتحوله إلى نوع جديد يعتمد على الشبكات والإنترنت ،ولبروز مخاوف من ممارسة الدول لمثل تلك المعطيات إلى إمكانية اتجاه الجماعات الإرهابية في التأثير على أمن الفضاء الإلكتروني[١]

وجاء استخدام الفضاء الإلكتروني كنمط من استخدام القوة عن طريق التأثير على عمل مصادر المعلومات وإتلافها وأنظمة الاتصالات عن طريق الهجوم الإلكتروني أو هجوم المعلومات من خلال الأدوات والوسائل الإلكترونية بما يؤدي إلى شلل هذه الأنظمة وتدمير أنظمة التشغيل الخاصة بها والتأثير على تدفق المعلومات بما يؤدي إلى إرباك عمل البنية التحتية الحيوية.

وهناك محاولة السيطرة الواسعة على المؤسسات الحيوية للدول الأخرى عن طريق استخدام أسلحة تكنولوجيا الاتصال والمعلومات ضد المنشآت المدنية والعسكرية وأنظمة الدولة والمؤسسات السياسية وإفساد عملها بما يمثل تهديدا مباشرا للأمن القومي الذي يتمثل في الدخول غير المشروع في المؤسسات المالية والاقتصادية والتدمير الواسع للبنية التحتية للاتصالات من خلال استخدام تكنولوجيا الاتصال والمعلومات بما يعد هجوماً على أنظمة صنع القرار والسيطرة والهجوم على الأنظمة الدفاعية للدولة الأخرى بما يمثل إمكانية تعرضها لهجوم محتمل بما يمكن أن يأتي في شكل رد فعل يتمثل في الحق الشرعي للدفاع عن النفس، ويؤدي استهداف الاتصالات وأنظمة المواصلات وخدمات الطوارئ والخدمات الحكومية إلى الأضرار بالحياة والممتلكات والمرافق الحيوية.

وتعد روسيا والصين والولايات المتحدة من أكبر القوى في مجال الاستحواذ على القوة الإلكترونية القادرة على توفير أقصى درجات الأمن الإلكتروني cyber security ، وهو

ما فرض على الدول وجود إجراءات حماية عبر تبني **سياسات دفاعية** تتضمن عمليات الحماية والتطوير لإجراءات الدفاع ضد الأخطار المحتملة وحماية نظم المعلومات ومنع تعرضها لعمليات هجومية معادية، وتعزيز الأمن الاليكتروني بأبعاده المتعلقة بالبرمجيات والبنية التحتية. ومنع استغلاله في الحرب النفسية. من أجل ضمان امن وسلامة الفضاء الالكتروني ، إلى جانب تبني **سياسات هجومية** في الفضاء الإلكتروني عبر اتخاذ إجراءات لمهاجمة مصادر التهديد وتعقب الفاعليين في الهجوم على منشآت البنية التحية الحيوية ويتم استخدام نظم إلكترونية متقدمة كتطوير استخدام أسلحة إلكترونية في الحروب . ويشهد العالم تطورا حذرا وسريا في هذا الشأن.

ومن ابرز أنماط ممارسة القوة عبر الفضاء الإلكتروني" **نمط القوة الصلبة** " عبر استخدام مقدراته وأدواته في عمل تخريبي عبر قطع كابلات الاتصالات أو تدمير أنظمة الاتصالات أو الأقمار الصناعية أو استخدام الأسلحة الإلكترونية المتقدمة كالفيروسات في تدمير الأنظمة المعلوماتية لمنشآت حيوية بشكل يؤثر على وظيفتها ويهدد امن الدولة والسكان.

وهناك نمط آخر لاستخدام القوة عبر الفضاء الإلكتروني فيما يمكن أن يطلق علية" **نمط القوة الناعمة** "وذلك بدعم دوره في إدارة العمليات النفسية والتأثير في الرأي العام وتكوين التحالفات الدولية وفي عمل أجهزة الاستخبارات الدولية بما وفره من سيل عالمي للمعلومات لا يقتصر علي وجهة النظر الرسمية للدول والحكومات، بل تعدي ذلك لدور الأفراد في إنتاج المعلومات وترويجها،وفي توافر كم هائل للتحليلات السياسية والاقتصادية مع تعدي الحدود الدولية وشكل ذلك ثورة معلوماتية هائلة لا حدود لها، مادامت عكفت عليها أجهزة الاستخبارات الكبري للحصول عليها أولا، والبحث فيها ثانيا وتوظيف نتائجها ثالثا[١] .

وتنتقل عملية التأثير والتأثر من وإلى الفضاء الإلكتروني عبر مسارات القوة أو اتجاهات سيطرت على المجال العام الدولي ، وأصبح **المسار الأول** يتعلق بعملية الانتقال للأحداث من ارض الواقع إلى الفضاء الإلكتروني إما لتصفية الصراعات أو استخدامه كوسيلة إعلام في التحريض أو العنف أو بث الكراهية مثل حالة انتقال الصراع بين الكوريتين إلى الفضاء الإلكتروني أو ما بين الصين وتايوان أو ما بين تنظيم القاعدة والولايات المتحدة .أما **المسار الثاني** فتعلق بانتقال وتصدير الفضاء الإلكتروني لعناصر تهديد إلى ارض الواقع عن طريق ما يتم الاستجابة له من نشر معلومات أو صور أو فيديو وهو ما يكون له تأثير في تكسير شبكة العلاقات القائمة ونشر شائعات تضر بالسلام من خلال ما ينشر من خطابات والتضليل بالمعلومات.

وأدى الفضاء الإلكتروني إلى تصاعد دور الصورة في تحريك الأحداث الدولية ومثال على ذلك حالة نشر الرسوم الكاريكاتورية المسيئة للرسول وهو ما أثر في احتجاجات دولية واعتداءات وعلى طبيعة العلاقات الدولية. وفيما يتعلق **بالمسار الثالث** فتعلق بدور الفضاء الإلكتروني كوسيلة إعلام يتم استخدامها كنشاط مواز للحوادث على أرض الواقع مثل أحداث القتل أو التدمير أو الكوارث أو الطبيعية أو الحروب بما يساهم في خلق ردود أفعال عالمية رسمية وغير رسمية ومؤيدة ومعارضة .وتلعب شركات تكنولوجية كبرى دور في صياغة الرأي العام الدولي.

أما **المسار الرابع** فتعلق بما يتم نشره عبر الفضاء الإلكتروني ولا يتعدى تأثيره عن نطاق الفضاء الإلكتروني ويعد هذا المسار من أنشط المسارات وذلك يرجع إلى اقتصار تأثيره على الطابع الإلكتروني فقط وهو ما يجعله أكثر تأثيرا على المصالح الإلكترونية وخاصة إذا كان من أنماطه إطلاق الفيروسات أو القرصنة أو سرقة المعلومات أو التجسس وغيرها.

المحور الثالث: القرصنة الالكترونية وتحديات الأمن العالمي أمام الخطر،المواجهة والمسؤولية:

لقد أصبحت الهجمات الالكترونية مصدر تهديد حقيقيا لاقتصاديات الدول، ولم تعد هذه الجرائم تقتصر على سرقة أموال البنوك أو الأفراد، بل اجتاحت قطاعات جديدة على غرار امن الموانئ، التي قد تتعرض لهجمات خطيرة من عصابات الجريمة المنظمة أو الإرهابيين أو حتى الدول المعادية وذكر بعض الخبراء أن الأرباح الضخمة التي تحققها الجرائم الالكترونية تجاوزت أرباح تجارة المخدرات، وذكر الخبراء أيضا أن الجرائم الالكترونية أصبحت اليوم واقعا في دولة الإمارات بوقوع نحو مليوني شخص من سكان الدولة ضحية للجرائم الالكترونية خلال سنة ٢٠١٥م، ومنذ عام ٢٠١٤م ارتفعت معدلات ما يطلق عليه قانونا اسم الجريمة الالكترونية في الوطن العربي، حيث بلغ عدد عمليات القرصنة الالكترونية التي تعرضت بعض دول الوطن العربي إلى نحو ٢٦ مليون عملية من القرصنة الالكترونية، والجزائر كغيرها من الدول التي لم تسلم هي الأخرى من ما يسمى بالقرصنة الالكترونية، أو من الجرائم الالكترونية ككل، حيث لم تسلم مواقع التواصل الاجتماعي وفضاءات تبادل المعلومات من عملية السطو على الصور والبيانات الشخصية واستعمالها كوسيلة للابتزاز والمساومة والتشهير وناهيك عن استغلال بيانات الحسابات الشخصية بالإضافة الاعتداء على أنظمة المعلومات، وحسب مصدر موثوق لجريدة الفجر، فقد تم تسجيل أكثر من ٥٠٠ جريمة الكترونية في الجزائر خلال ٢٠١٦م وهذا مما يستدعي تضافر الجهود من اجل التصدي لهذا الخطر والمتمثل في الردع السيبراني. [١]

المحور الرابع: استراتيجيات الردع السيبراني من الهجمات السيبرانية " المتطلبات والحلول":

مقومات الردع السيبراني: تتمثل في مصداقية الدفاع، القدرة على الانتقام، الرغبة في الانتقام.

متطلبات الردع السيبراني:

إن الردع السيبراني صعب التنفيذ، كما أن هناك العديد من العوامل التي يجب أن تحدث لضمان تحقيق النتائج المرجوة منها[٢]:

يتطلب الردع السيبراني تطبيق طرق وأساليب جديدة، وإعادة تكييف مفاهيم الردع التقليدية لتتناسب مع هذا المجال الجديد، فلا يمكن معرفة الهدف من الهجمات دون معرفة من شنها ودون معرفة الخصم وهدفه، لا يمكن للردع أن ينجح وسرقة المعلومات قد تتكرر مستقبلا، من هذه المتطلبات ما يلي:

الردع السلبي، الاحتجاجات الدبلوماسية، التدابير القانونية، العقوبات الاقتصادية، الانتقام في الفضاء الافتراضي، الانتقام العسكري.

استراتيجيات الردع السيبراني: تتمثل في:

الأنظمة البديلة، إعادة التأسيس.

خاتمة:

من خلال عرض الدراسة البحثية السابقة نستنتج أن العصر الذي نعيش فيه بات عصر رقمي تتحكم فيه المعرفة والمعلومات ووسائل الاتصالات، فمن يملك المعرفة يتحكم في كل شيء، وأصبح الفضاء السيبراني واقعي والحروب السيبرانية حقيقة لا مفر منها والتي تعتبر الجيل الخامس من الحروب ويرى الكثير من الأكاديميين أنها نهاية الحروب في المستقبل، وأصبحت الرقمنة هي الصياغة السائدة في العصر الحالي من نقود وحكومات وسيادة سيبرانية وأمن سيبراني ودبلوماسية سيبرانية، كل شيء يتعامل عبر الفضاء الإلكتروني، ولذلك يتوجب على الدول والأفراد الحذر والحيطة عند استخدام البيانات والمعلومات في المجال الافتراضي، لتجنب الوقوع في مخاطر التصيد الشبكي والهاكرز والجماعات الإرهابية.

الهوامش

[١]: عباس بدران، الحرب الالكترونية، الاشتباك في عالم المعلومات، بيروت، مركز دراسات الحكومة الالكترونية، ٢٠١٠، ص٤.

: يائير كوهين، الفضاء الالكتروني والبعد الخامس للحرب، القدس، ٢٠١٢، ص٢٢. [٢]

[١]: للتعرف إلى مجالات عمل وأعمال ويليام جيبسون انظر http://www.williamgibsonbooks.com

[٢]:دويب حسين صابر، القوانين العربية وتشريعات تجريم الجرائم السيبرانية وحماية المجتمع، الرياض،٢٠٠٩، ص٢.

[٣]:شمويل ايفين ودافييد سيمان توف، حرب الفضاء الالكتروني، المفاهيم والاتجاهات، برلين، ٢٠١١،ص٢٠.

[١] The cost Of DDOS Attacks and building The business case for protection, : CoGEco peer (2017)

[٢]: خالد وليد محمود، " الهجمات عبر الانترنت ساحة الصراع الإلكتروني الجديد" ، المركز العربى للأبحاث ودراسة السياسات ، 2013 ، ص ١١.

[١]: مصطفى علوي، مفهوم الأمن في مرحلة ما بعد الحرب الباردة، القاهرة، ٢٠٠٤، ص.١٤

[١] .Myriam Dunn ,information age conflicts,issue64 ,2002,p202:

[١]: عادل عبد الصادق، هل يمثل الإرهاب الالكتروني شكلا جديدا من أشكال الصراع الدولي، مركز الدراسات السياسية والإستراتيجية، القاهرة،٢٠١٧، ص٥

[2]:Myriam and Dunn, the internet and the changing face of international relations and security,edit7,bulgaria,p52.

[1:] Martin libicki, conquest in cyberspace,national security and information ٧warfare,cambridge university press,2007,p

[2]:Athina karatzogianni,cyberconflicts and global politics, routeledge and taylor fancis group,edit 11,2008,pp240-٢٤٢.

[3]:Jennie and williamson,information operation,computer network attacks in the 21st century,u.s,2002,pp15-22.

[1]:Myriam and Dunn,information age conflicts:a study of the information revolution and a changing operation environment,center for security studies,edit 6, 2002,p25.

[٢]: عادل عبد الصادق، موقع ويكيليكس وتحدي عالم الاستخبارات الامريكي، مركز الاهرام للدراسات، القاهرة،٢٠١٠، ص٨٨.

[٣]: عادل عبد الصادق، مرجع سبق ذكره، ص٧٢.

[1:]Arsenio gumhad ,cyber troops and net war, the profession of arms in the information age, 1996,pp55-57.

[٢]: عادل عبد الصادق، امريكا وتشكيل قيادة عسكرية في الفضاء الالكتروني، القاهرة، مركز الاهرام، ٢٠٠٩، ص٢٢.

[٣] :Ttim jordan, cyber power,the culture and politics of cyberspace and the internet,routledge,2000,pp160-163.

[٤]: جوزيف ناي، المنازعات الدولية ترجمة احمد امين ومجدي كامل، القاهرة، ١٩٩٧، ص٨٢.

[١]: عادل عبد الصادق، الانترنت والاتصالات، ساحة جديدة للتجسس الدولي، القاهرة، المركز العربي لأبحاث الفضاء الالكتروني،٢٠٠١،ص١٠.

[١]: عادل عبد الصادق، الإرهاب الالكتروني القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة، القاهرة، مركز الدراسات السياسية، ٢٠٠٩،ص١٥٠.

[١]: علي حسين باكير، الحروب الالكترونية في القرن الواحد والعشرين، قطر، مركز الجزيرة للدراسات، ٢٠١٠،ص٢٣.

[١]: رونيتتيروش، إسرائيل مستعدة لهجمات قراصنة الكومبيوتر بعد القرصنة عل بطاقات الائتمان من قبل قراصنة السعودية ترجمة منير القحطاني، قطر، مركز العلوم والتكنولوجيا، ٢٠١٢، ص١١٦.

[٢]: ايهاب خليفة ، القوة الالكترونية وأبعاد التحول في خصائص القوة، القاهرة، وحدة الدراسات المستقبلية، ٢٠٠٤، ص١٢.

قائمة المراجع:

١-عباس بدران، الحرب الالكترونية، الاشتباك في عالم المعلومات، بيروت، مركز دراسات الحكومة الالكترونية، ٢٠١٠.

يائير كوهين، الفضاء الالكتروني والبعد الخامس للحرب، القدس، ٢٠١٢. ٢-

٣-دويب حسين صابر، القوانين العربية وتشريعات تجريم الجرائم السيبرانية وحماية المجتمع، الرياض،٢٠٠٩.

٤-شمويل أيفين ودافييد سيمان توف، حرب الفضاء الالكتروني، المفاهيم والاتجاهات، برلين، ٢٠١١.

٥-رونيتتيروش، إسرائيل مستعدة لهجمات قراصنة الكومبيوتر بعد القرصنة عل بطاقات الائتمان من قبل قراصنة السعودية ترجمة منير القحطاني، قطر، مركز العلوم والتكنولوجيا، ٢٠١٢،.

٦-ايهاب خليفة ، القوة الالكترونية وأبعاد التحول في خصائص القوة، القاهرة، وحدة الدراسات المستقبلية، ٢٠٠٤.

٧-علي حسين باكير، الحروب الالكترونية في القرن الواحد والعشرين، قطر، مركز الجزيرة للدراسات، ٢٠١٠.

٨-عادل عبد الصادق، الإرهاب الالكتروني القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة، القاهرة، مركز الدراسات السياسية، ٢٠٠٩.

٩-عادل عبد الصادق، الانترنت والاتصالات، ساحة جديدة للتجسس الدولي، القاهرة، المركز العربي لأبحاث الفضاء الالكتروني،٢٠٠١.

١٠-عادل عبد الصادق، أمريكا وتشكيل قيادة عسكرية في الفضاء الالكتروني، القاهرة، مركز الأهرام، ٢٠٠٩.

١١-جوزيف ناي، المنازعات الدولية ترجمة احمد أمين ومجدي كامل، القاهرة، ١٩٩٧.

١٢-عادل عبد الصادق، موقع ويكيليكس وتحدي عالم الاستخبارات الأمريكي، مركز الأهرام للدراسات، القاهرة،٢٠١٠.

١٣-خالد وليد محمود، " الهجمات عبر الانترنت ساحة الصراع الإلكتروني الجديد" ، المركز العربى للأبحاث ودراسة السياسات ، 2013 .

١٤-عادل عبد الصادق، هل يمثل الإرهاب الالكتروني شكلا جديدا من أشكال الصراع الدولي، مركز الدراسات السياسية والإستراتيجية، القاهرة،٢٠١٧.

١٥-مصطفى علوي، مفهوم الأمن في مرحلة ما بعد الحرب الباردة، القاهرة، ٢٠٠٤.

١٦-للتعرف إلى مجالات عمل وأعمال ويليام جيبسون انظرhttp://www.williamgibsonbooks.com

17-Arsenio gumhad ,cyber troops and net war, the profession of arms in the information age, 1996.

18-Ttim jordan, cyber power,the culture and politics of cyberspace and the internet, routledge,2000.

19-Myriam and Dunn,information age conflicts:a study of the information revolution and a changing operation environment,center for security studies,edit 6, 2002.

20-Martin libicki, conquest in cyberspace,national security and information warfare,cambridge university press,2007.

List of references:

1 - Abbas Badran, Electronic Warfare, The World of Information, Beirut, Center for eGovernment Studies, 2010.

Yair Cohen, The Electronic Space and the Fifth Dimension of War, Jerusalem, 2012. 2 -

3 - Dawib Hussein Saber, Arab Laws and Legislation Criminalizing Cybercrime and Community Protection, Riyadh, 2009.

4 - Samuel Avin and David Seaman, The Space Warfare, Concepts and Trends, Berlin, 2011.

5-Runitreroch, Israel is ready for hacker attacks after hacking credit cards by Saudi hackers Translated by Munir Al-Qahtani, Qatar, Science and Technology Center, 2012 ,.

6. Ehab Khalifa, The Power of Electronic and the Dimensions of Transformations in Force Characteristics, Cairo, Future Studies Unit, 2004.

7 Ali Hussein Bakir, Electronic Warfare in the 21st Century, Qatar, Al Jazeera Center for Studies, 2010.

8-Adel Abdel-Sadiq, Electronic Terrorism Force in International Relations, New Pattern and Different Challenges, Cairo, Center for Political Studies, 2009.

9- Adel Abdel-Sadiq, Internet and Communications, New International Espionage Square, Cairo, Arab Center for Space Research, 2001.

10-Adel Abdul-Sadiq, America and the formation of a military command in electronic space, Cairo, Al-Ahram Center, 2009.

11. Joseph Nay, International Disputes, Ahmed Amin and Magdy Kamel, Cairo, 1997.

12-Adel Abdul-Sadiq, WikiLeaks and the Challenge of American Intelligence, Al-Ahram Center for Studies, Cairo, 2010.

13- Khaled Waleed Mahmoud, "Attacks via the Internet The new electronic conflict arena", Arab Center for Research and Policy Studies, 2013.
14- Adel Abdel Sadeq, Is Electronic Terrorism a New Form of International Conflict, Center for Political and Strategic Studies, Cairo, 2017.
15. Mustafa Alawi, The Concept of Security in the Post-Cold War, Cairo, 2004.