الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة محمد بوضياف - المسيلة

كلية الحقـــوق و العلـــوم السياسية
قسم العلوم السياسية والعلاقات الدولية
رقم: .....

ميدان: الحقـــوق و العلـــوم السياسية
فرع: العلوم السياسية والعلاقات الدولية
تخصص: علاقات دولية

مذكرة مقدمة لنيل شهادة الماستر أكاديمـــي

إعداد الطالبة: بشلالق ليلى

تحت عنوان

تأثير الحروب الإلكترونية على العلاقات الأمريكية الروسية

لجنة المناقشة:

.....	جامعة المسيلة	رئيســا
د. بوعيسي حسام الدين	جامعة المسيلة	مشرفا ومقررا
.....	جامعة المسيلة	مناقشا

السنة الجامعية: 2019/2018


بسم الله الرحمن الرحيم

شكـــــر وتقديـــــر

قال الله تعالى: ﴿ولئن شكرتم لأزيدنكم﴾ سورة إبراهيم الآية (07)

حمدا لمن أبدع في الكون...وشكرا لصاحب المنة والنعمة...فلا يطيب الليل إلا بشكرك ولا يطيب النهار إلا بطاعتك...ولا تطيب اللحظات إلا بذكرك...ولا تطيب الآخرة إلا بعفوك...ولا تطيب الجنة إلا برؤيتك عز وجل

قدرك...فلك الحمد يا رب العالمين...

أتوجه بخالص الشكر والتقدير لمشرفي الدكتور :" بوعيسي حسام الدين" لتفضله وقبوله الإشراف على هذه المذكرة...حيث كان له الفضل في إثرائها بالمعلومات القيمة ونصائحه...

جزاه الله عنا خير جزاء...

كما لا يفوتني الشكر لمن منحنا الكثير من وقته وجهده ومد لي العون من قريب وبعيد

جزاهم الله عني كل خير...

إهـــــــــــداء

إلى من كلّله الله بالهيبة والوقار...إلى من علمني العطاء دور انتظار...

إلى ملاكي في الحياة... إلى معنى الحب... الى معنى الحنان والتفاني إلى بسمة الحياة وسر الوجود «أمي الحبيبة »... إلى من أحمل اسمه بكل افتخار... أرجو من الله أن يمد في عمرك لترى ثمارا قد حان قطافها بعد طول انتظار... وستبقى كلماتك نجوم اهتدي بها اليوم وغدا... إليك «ابي الغالي» حفظك الله وأدامك عزا وفخرا لنا...

إلى سندي وقوتي وملاذي بعد الله ...إلى أجمل ما في الحياة، أخواتي: هنيدة، سليمة، وإلى أخواي: عبد الوهاب، عبد الكريم

إلى من تحلو بالإخاء وتميزوا بالوفاء والعطاء ...إلى ينابيع الصدق الصافي ومن كانوا معي على طريق الخير والنجاح ...إلى أغلى صديقاتي: سعاد، سارة، سعاد.

إلى كل الأهل والأقارب.

ليـــــــلى

فهرس المحتويات

فهرس المحتويات

مقدمـــــــة

مقدمة:

اتسمت نهاية القرن العشرين بثورة تكنولوجية ومعلوماتية هائلة، أحدثت قفزة غيرت أنماط الحياة وحدود العلاقات، امتدت من فضاء الاتصالات إلى المصارف والأنظمة المالية إلى التجارة والتسويق، إلى التعليم والتكوين وتسيير المواصلات والمطارات والقطارات إلى إدارة المنشآت العسكرية والنووية إلى فضاءات التواصل الاجتماعي وحتى إنشاء الحكومات الإلكترونية .

أنتج هذا التعامل مع الإنترنيت وما توفره من زخم معلوماتي وقدرات اتصال، وخدمات حالة من الارتباط يصعب على الفرد والمؤسسات الاستغناء عنها؛ فأصبحت الانترنيت جزءا من الحياة اليومية للأشخاص والهيئات، كما أفرز هذا التعامل وهذا الارتباط كما هائلا من البيانات والمعلومات، التي تباينت في طبيعتها بين العام والشخصي وبين العلني والسري.

عرفت العلاقات الولية تطورا بارزا من حيث الفواعل والمواضيع والأدوات المستخدمة في إدارة تفاعلاتها، وفي ظل هذه القفزة النوعية التي تزامنت مع ثورة تكنولوجية ورقمية مذهلة، اقتحمت شتى أنماط الحياة الإنسانية والتفاعلات الدولية ظهر نوع جديد من التهديدات المتمثلة في الصراعات الإلكترونية التي وجب على الدولة القومية التعامل معها وبالتالي محاولة مجابهتها، وما زاد ن تعقيد هذا النوع من التهديدات هو ذلك الترابط الذي فرضه هذا التعامل الكثيف في الفضاء الشبكي وحجم الخدمات المتوفر فيه، بالإضافة إلى ذلك الوضع الذي خلقه التطور التكنولوجي على مستوى البناءات الداخلية في الدولة بين السياسة الاقتصاد وقطاع التجارة والمال والثقافة وبالتالي فإن أي هجوم على قطاع من القطاعات من شأنه إحداث أضرار كبيرة من شأنها التأثير على أمن الدول.وبالتالي أصبحت الدول مجبرة على الاهتمام بالفضاء الإلكتروني كونه أضحى ساحة جديدة للتفاعلات الدولية.

فتبلورت ظاهرة الحروب الإلكترونية بوصفها شكلا جديدا من أشكال التفاعلات الدولية وصورة جديدة من صور الحروب، والتي اتسمت بمجموعة خصائص تجعلها مختلفة عن نظيرتها التقليدية من حيث طبيعة الأنشطة العدائية، والفواعل، والتأثير في بنية الأمن العالمي،

وعبرت تلك الحرب بين نمطين من القوة(الناعمة و الصلبة) في عملية توظيف التفاعلات في الفضاء الإلكتروني، مما يعكس تنامي القدرات والتهديدات المتصاعدة لأمن البنية التحتية الكونية للمعلومات.

أهمية الموضوع:

1-الأهمية العلمية: تظهر الأهمية العلمية للدراسة من خلال محاولة الإنارة حول ظاهرة قديمة جديدة في العلاقات الدولية والتي أصبحت تشغل حيزا كبيرا من الاهتمام لدى مراكز البحوث الغربية تتمثل هذه الظاهرة في الحروب الإلكترونية كشكل من أشكال التفاعلات الدولية ، من أجل إزالة الغموض المعرفي وتوضيح الحدود الفاصلة بينها وبين غيرها من مفاهيم مشابهة، ومحاولة إخراجه من مدلوله التقني العلمي إلى مدلول سياسي باعتبار الحرب الإلكترونية تعبر عن واحدة من عمليات التفاعلات في السياسة الدولية؛ بالإضافة إلى محاولة البحث حول إطار نظري من شأنه إعطاء تفسير علمي للظاهرة وخاصة وأن هذه الظاهرة بأبعادها الحالية تعد من مفاهيم الحديثة نسبيا في حقل العلاقات الدولية.

2_ **الأهمية العملية:** استعراض المفاهيم النظرية لظاهرة تعتبر من أحدث التهديدات التي تواجه الدول، وبالتالي أصبح هذا النوع من الحروب أمرا واقعا وربما من أخطر أنواع الحروب حيث توفر ميزة نسبية للدول من حيث الكلفة وصعوبة تحديد الطرف المهاجم وبالتالي إثبات المسؤولية الجزائية؛ هذا ما فرض على الدول أن تأخذ هذه الظاهرة على محمل الجد.

أسباب اختيار الموضوع:

تضافرت مجموعة من الاعتبارات والأسباب لاختيار هذا الموضوع تراوحت بين الذاتية والموضوعية

1_ الأسباب الموضوعية:

محاولة تسليط الضوء على هذا النوع الجديد من الحروب ودورها في تهديد الأمن القومي للدول فنظرا لتصاعد أهمية دور الفضاء الإلكتروني خاصة بعد أحداث11 سبتمبر 2001 أضحت التهديدات الإلكترونية حقيقة واقع ووجب على الدول التعامل معها بكل جدية.

2_الأسباب الذاتية:

شغف معرفي متأصل بالمواضيع المتعلقة بالعلاقات الدولية وخاصة منها تلك الحديثة، وفضول علمي من أجل التعرف على هذا النمط من الحروب التي لم تأخذ حقها في مجال الدراسات العربية على الرغم من اهتمام الكبير الذي توليه لها مراكز البحث الغربية ، وكذلك رغبة منا في إضافة دراسة جادة حول هذا الموضوع أملا في أن تكون إضافة جديدة ومفيدة.

إشكالية الدراسة:

أضحى الفضاء الإلكتروني إلى مجال خامس بعد كل من المجال البري والبحري الجوي والفضاء، وأصبح ساحة جديدة تدور فيها مختلف الصراعات، وما زاد من تعقيد هذا النوع من الصراع هو ذلك الترابط الذي كان نتيجة ظهور هذه الطفرة المعرفية في عصر المعلومات فعلى الرغم من الميزات النوعية التي وفرتها ثورة المعلومات إلى أنها كذلك خلقت مجالا جديدا أصبح يخلق مجموعة من التهديدات التي تتباين وفقا لتباين القدرة المعلوماتية لكل دولة ولعل أكبر تهديد أصبح يمس أمن الدول وأخطر تهديد يكمن في الحروب الإلكترونية

مما سبق فإن التساؤل الرئيسي يدور حول ما هو تأثير الحروب الإلكترونية في العلاقات الأمريكية الروسية؟

منطلقين من الأسئلة الفرعية التالية:

- ما مفهوم الحروب الإلكترونية؟
- كيف أثرت الحروب الإلكترونية في التفاعلات الدولية؟
- هل أصبح الفضاء الإلكتروني ساحة جديدة للصراع الدولي؟
- كيف استفادت الدول الكبرى من الفضاء الإلكتروني من أجل تحقيق مصالحها؟

نطاق الإشكالية:

1-النطاق المكاني :

تراوحت أماكن الدراسة بين الولايات المتحدة الأمريكية والإتحاد السوفياتي سابقا ثم روسيا حاليا بالإضافة إلى الفضاء الإلكتروني باعتباره ساحة انتقل إليها الصراع.

2- النطاق الزماني :

تبدأ الحدود الدراسة من أحداث11سبتمبر إلى الآن، لكن هذا لم يمنع التطرق إلى حقبات زمنية سابقة وذلك من أجل الإحاطة بتطور ظاهرة الحروب الإلكترونية، بالإضافة إلى محاولة تسليط الضوء على تاريخ العلاقات الأمريكية الروسية.

فرضيات الدراسة:

ارتباطا بمضمون المشكلة البحثية المعالجة، فإّن هذه الدراسة تحاول اختبار الفرضية المركزية التالية:

كان لظهور الحروب الإلكترونية تأثير على مسار تطور العلاقات الأمريكية الروسية

والأسئلة الفرعية السابقة تستدعي فرضيات جزئية للإجابة على هذه التساؤلات يستدعي وضع جملة من الفرضيات التي يمكن إخضاعها للاختبار لاكتشاف مدى صحتها أو ضعفها

_الحرب الإلكترونية نوع جديد من الحروب تمتلك مجموعة من المميزات التي تفرقها عن غيرها من الحروب

_ أصبح للحرب الإلكترونية تأثير كبير في التفاعلات الدولية في الوقت الراهن

_ أدى التطور التكنولوجي وظهور عصر المعلومات إلى ظهور الفضاء الّإلكتروني كمجال جديد تدور بين جدرانه الصراعات الدولية

_ سارعت الدول الكبرى ذات الإمكانيات الإلكترونية إلى الاستفادة من ميزات الفضاء الإلكتروني من أجل تحقيق مصالحها.

أدبيات الدراسة:

أثار موضوع الحروب الإلكترونية اهتمام العديد من الكتاب ولعل أهم الدراسات التي اهتمت بتأثير الحروب الإلكترونية في التفاعلات الدولية والتي كانت المعين والسند للقيام بهذه الدراسة مايلي:

يعتبر كل من الدكتور عادل عبد الصادق وإيهاب خليفة من أكثر الباحثين تطرقا لهذا الموضوع سواء من خلال تأليف كتب تتحدث عن موضوع الفضاء الإلكتروني وتأثيره في التفاعلات الدولية، أو من خلال مجموعة من المقالات.

_ **إيهاب خليفة. مجتمع م ابعد المعلومات:** تأثير الثورة الصناعية الرابعة على الأمن القومي : والذي أشار فيه إلى أن الثورة التكنولوجية أو ما أسماها الثورة الصناعية الرابعة من شأنها أن تغير ليس فقط وسائل الإنتاج وخصائص وموازين القوة بل تغير أيضا من المنظور المعرفي للبشر اتجاه الأشياء بصورة عامة. كما رأى أنه مع توجه الدول لتبني نماذج ذكية تعتمد بصورة رئيسية على تكنولوجيا المعلومات والاتصالات لإدارة جميع متطلبات الحياة اليومية فيها واعتماد النظم المالية والمصرفية والإدارية على الإنترنيت تصبح الدول أكثر عرضة للاختراق وتصبح قواعد البيانات والخطط والإستراتيجيات أكثر عرضة للتلاعب بها وتسريبها.

_ إيهاب خليفة القوة الإلكترونية كيف يمكن أن تدير الدول شؤونها في عصر الإنترنيت : والذي أكد فيه أن ظهور الفضاء الإلكتروني والشبكة العنكبوتية كان له أثر مهم في الحياة البشرية فسهولة استخدامها ورخص تكلفتها ساعد على قيامها بأدوار مختلفة في الحياة البشرية سواء تجارية أو اقتصادية أو معلوماتية أو سياسية أو عسكرية أو إيديولوجية، وبالتالي أعادت تعريف المفاهيم التقليدية في العلاقات الدولية مثل الحرب والصراع والردع وظهر لها جميعا جانب إلكتروني فالذي يدير العالم آحاد وأصفار غاية في الصغر وقد أصبح جليا من يمتلك آليات توظيف هذه البيئة الإلكترونية الجديدة فإنه الأكثر قدرة على التأثير في سلوك المستخدمين لهذه البيئة.

_ عادل عبد الصادق في مقال موسوم بـ:الحروب السيبرانية: تصاعد القدرات والتحديات للأمن العالمي أين يرى بأن الفضاء الإلكتروني قد تحول إلى مجال جديد في مجال التفاعلات الدولية بروت حالة توظيفه في الاستخدامات المدنية وأخرى ذات طابع عسكري، وتبلورت الأنشطة العدائية العنيفة في ظاهرة الحرب الإلكترونية، وهو ما يعكس تنامي في القدرات والتهديدات وتعاظم التأثير على أمن البنية التحتية الكونية للمعلومات.

_ مقال: أنماط الحرب السيبرانية وتداعياتها على الأمن العالمي لصاحبه عادل عبد الصادق: والذي ناقش فيه مفهوم الحروب الإلكترونية والأطر المفسرة لنشوء مثل هذه الحروب، وأبرز أنماطها من واقع التفاعلات الدولية وأخيرا تداعيات ومخاطر ذلك على الأمن العالمي.

_ إنمار موسى جواد في دراسته الموسومة بـ: الفضاء الإلكتروني المفهوم _الأدوات والتطبيقات والذي تطرق فيها إلى تعريف الحروب الإلكترونية وميعن غيرها من المفاهيم

بالإضافة إلى استعراض أجيالها، ليتطرق بعد ذلك الى استراتيجيات بعض الدول في التعامل مع الأمن الإلكتروني، وفي الأخير تطرق إلى مستقبل هذا النوع من الحروب.

هذه أهم الدراسات التي تم اعتمادها كمراجع أساسية في عملية البحث.

الإطار المنهجي:

ومن أجل التثبت من صحة الفرضية أعلاه كان لابد من الاعتماد على عدة مناهج، فإذا كانت طريقة البحث العلمي تفرض على الباحث أن يكون ممنهجا في معالجته يكون بالصعوبة الاعتماد على منهج علمي بذاته لتفسير ظاهرة الحروب الإلكترونية ذلك أن الظاهرة تعتمد في تفسيرها على أكثر من منهج وعلى أكثر من طريقة نظرا لما تنطوي عليه هذه الظاهرة من أبعاد وجملة من المتغيرات.

1-المنهج الوصفي التحليلي: يهدف هذا المنهج إلى تحقيق الفهم الدقيق والإحاطة بالأبعاد الواقعية للظواهر والموضوعات، ومن هنا فالقواعد الأساسية التي يقوم عليها المنهج الوصفي تتمثل في تحديد الظواهر المراد بحثها،وجمع المعلومات الدقيقة عنها وفحصها ودراستها ومحاولة الإحاطة بعدد كبير من الأبعاد والعلاقات المرتبطة بالظاهرة من أجل الانتقال من من مستوى الفهم البسيط إلى المستوى المركب، وما يرتبط بذلك من صياغة عدد من النتائج والتعميمات والتوصيات التي ترشد عملية البحث وذلك من خلال محاولة وصف وتحليل مفهوم الحرب الإلكترونية، بالإضافة إلى محاولة وصف وتفسير وتحليل العلاقات الأمريكية الروسية.

2-**المنهج التاريخي:** والذي يستند إلى الأحداث التاريخية في فهم الحاضر المستقبل،فلا يمكن فهم وإدراك حالة سياسية إلا بالعودة إلى جذورها التاريخية، ومن ثمة استنتاج أفكار جديدة أو بناء تصورات وتقديم تعميمات يمكن استخدامها بشكل صحيح، وبالتالي فان هذا المنهج يعنى بدراسة التجارب التاريخية والدقة الموضوعية، ومن أجل فهم أدق لظاهرة الحروب ال}إلكترونية كان لزاما تتبع تاريخ تطور الحروب الإلكترونية، خاصة وأن لها أجيال، بالإضافة إلى أن الصراع الأمريكي الروسي لم يكن وليد اللحظة بل مر بمراحل كان نقل ساحة القتال إلى الفضاء الإلكتروني هي آخر تطور في تاريخ تطور علاقة البلدين في الوقت الراهن.

3- **منهج دراسة حالة:** وفيه يتم التركيز على حالة معينة يقوم الباحث بدراستها، ويتم دراسة هذه الحالة بشكل مستفيض وواف، يتناول كل المتغيرات والظواهر المرتبطة به وتناولها

بالوصف الكامل والتحليلي،وذلك من خلال تسليط الضوء على طبيعة العلاقات الأمريكية الروسية، والانتخابات الرئاسية الأمريكية الأخيرة.

الإطار المفاهيمي:

تم التطرق إلى أهم المفاهيم المحورية في الدراسة:

الحروب الإلكترونية: مجموع الإجراءات العدائية التي تقوم بها الدول ويكون ميدانها العالم الافتراضي.

الفضاء الإلكتروني: هو العالم الرقمي وهو عبارة عن شبكات الكومبيوتر والاتصالات الإلكترونية وهو عبارة عن شبكة خيالية تحتوي كما هائلا من المعلومات التي يمكن الحصول عليها لتحقيق الثروة والسلطة، بل وأصبح عالما مواز للواقع الذي نعيش فيه ويتميز الفضاء الإلكتروني بسقوط الحدود الجغرافية.

القوة الإلكترونية: هي مجموع الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات والشبكات الإلكترونية والبنية التحتية المعلوماتية والمهارات البشرية المدربة للتعامل مع هذه الوسائل.

الإطار النظري:

يستند البحث إلى خلفية نظرية أساسية لمعالجة الموضوع ، ومن أجل ذلك تم اختيار نموذج جوزيف ناي الذي جمع بين القوة الإلكترونية وكل من القوة الصلبة والقوة الناعمة، يرتكز تحليله على مفهوم القوة الإلكترونية، تنوع الفواعل الدولية، بالإضافة إلى مفهوم انتشار القوة

تبرير الخطة:

استنادا إلى الإشكالية المطروحة والفرضيات المقدمة، تم تناول الدراسة وفقا للبناء التالي:

تطرق الفصل الأول إلى الضبط المفاهيمي والإطار النظري للدراسة أين يتم توضيح الحدود الفاصلة بين مفهوم الحروب الإلكترونية وغيرها من المفاهيم التي شاع استخدامها كمرادف لها، والتعرف عن مميزات وأنماط الحروب الإلكترونية، ثم التطرق إلى نموذج جوزيف ناي من أجل تفسير أعمق لظاهرة الحروب في الفضاء الإلكتروني.

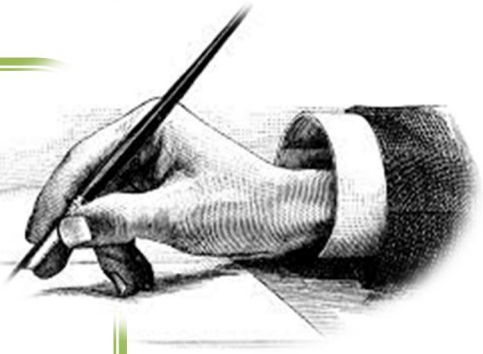
جاء الفصل الثاني من أجل تناول مفهوم القوة الإلكترونية كوافد جديد في العلاقات الدولية، والفضاء الإلكتروني بوصفه ساحة جديدة للقتال وأثره في تحولات القوة، وتسليط الضوء

على أنواع الصراع الإلكتروني وأشكاله وتداعيات الحروب الإلكترونية على الأمن القومي والدولي.

أما في الفصل الثالث فتم عرض الصراع الإلكتروني كجيل جديد من أجيال الصراع الأمريكي الروسي وكيف حاول كل طرف استخدام الفضاء الإلكتروني بطريقة تحقق مصالحه الوطنية، وكيف جسدت حادثة التدخل الروسي في الانتخابات الأمريكية 2016 الصورة الأوضح للحروب الإلكترونية وتداعياتها على العلاقات بين الدول.

الفصل الأول

الإطار المفاهيمي والنظـــــري



تمهيد :

مع نهاية الحرب الباردة عرفت العلاقات الدولية تطورا كبيرا من حيث الفواعل والمواضيع، والأدوات المستخدمة في إدارة مختلف تفاعلاتها؛ وفي سياق هذا التطور الذي صاحب ثورة تكنولوجية ورقمية اقتحمت شتى مجالات الحياة الإنسانية والتفاعلات الدولية ، أين فرض العالم الافتراضي نفسه كساحة جديدة للصراع الدولي، فظهرت مفاهيم جديدة في العلاقات الدولية أهمها الحروب الإلكترونية كنوع جديد من أنواع الحروب.

المبحث الأول: الإطار المفاهيمي

المطلب الأول: تعريف الحرب الإلكترونية

تعريفها لغة: من المبنى اشتقت الحرب من الجذر حرب حربا أي تعب، والحرب اسم جمعه حروب، والحرب قتال ونزال بين طرفين.

ويقال: إذا أخذ جميع ماله فهو حريب، والحرب تعني المقاتلة والمنازلة[1].

وبوصف مقارب حربه يحربه حربا أي أخذ ماله وحرب الرجل ماله وحاربه حرابا أقام عليه الحرب[2]

اصطلاحا: تعرض مفهوم الحرب الإلكترونية إلى جدل أكاديمي واسع عبر عن تقاطع الرؤى والخلفيات المعرفية ، في حين انه هناك اجماع حول تعريف الحرب أنها صراع مسلح أو عنف

1-أحمد بن محمد الفيومي . المصباح المنير في غرب الشرح الكبير للرافعي.ج1.بيروت.المكتبة العلمية.ص127.
2-بطرس البستاني. محيط المحيط. بيروت. مكتبة الناشرون.1979.ص157.

منظم تشنه الدولة لمصلحة الدولة وضد دولة . ومع اقتران الحرب بالتقنيات الالكترونية التي أفضت إليها ثورة المعلومات.[1]

لا يوجد اجماع حول تعريف محدد ودقيق فبالإضافة إلى حداثة هذا المصطلح وضبابيته بالإضافة إلى تداخله مع مفاهيم أخرى ، فعامل الترجمة إلى اللغة العربية زاد من هلامية معناه

لذلك تجدر الإشارة إلى ان الحرب الإلكترونية هي ترجمة لـ Eectronic Warfar

في حين يستعملها البعض الآخر كترجمة لـ Cyber War .في حين يذهب البعض الآخر الى اعتبار أنهما مترادفان مثلما ذهب إليه عادل عبد الصادق حيث يجعل من الإلكتروني مرادفا للسيبراني . وبالتالي فإن الحرب الإلكترونية هي مرادف للحرب السيبرانية ، لذلك سيجري ذكرهما بالتناوب .

يعرفها كل من **ريتشارد كلارك** و **روبرت كنيك** بأنها: « أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكومبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها»[2].

يعرفها **شميت** بالقول:« مجموعة من الإجراءات التي تتخذها الدولة للهجوم على نظام المعلومات المعادية بهدف التأثير والإضرار بها في الوقت نفسه للدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة».[3]

1-Anthony E .Spezio , Member ,LEEE. Electronic Warfar Systems .LEEE TRANSACTIONS ON MICROWAVE THEORY AND TECHNIQUES.VOL.50.NO.03MARCH 2002.P633.

2- ريتشارد أي كلارك. روبرت كي كنيك. حرب الفضاء الإلكتروني التهديد التالي للأمن القومي وكيفية التعامل معه. ط1.الإمارات.مركز الإمارات مركز الإمارات للبحوث والدراسات الإستراتيجية .2012.ص21.

3- أحمد أوبيس الفتلاوي. الهجمات السيبرانية: مفهومها المسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر. مجلة المحقق الحلي للعلوم القانونية والسياسية. ع 04. 2016. ص216.

يعرفها **شين Shin** بأنها استخدام الطيف الإلكتروني أو الكهرومغناطيسي لتخزين وتعديل وتبادل البيانات وجها لوجه مع أنظمة تحكم في بنى تحتية مرتبطة بها.

في حين يعرفها **جوزيف ناي** بأنها:« الأعمال العدائية في الفضاء السيبراني التي لها آثار تفوق العنف الحركي التقليدي».[1]

في حين يعرفها **كينيث جريس** بأنها:« القدرة على الدفاع والهجوم على المعلومات، من خلال شبكات الحاسب الآلي عبر الفضاء الإلكتروني، بالإضافة إلى شل قدرة الخصم على القيام بنفس هذه الهجمات »، وتشمل الحرب السبرانية عند **جريس** خمسة عناصر رئيسية هي التجسس، الدعاية، الحرمان من خدمة الإنترنيت وتعديل البيانات والتلاعب بها.[2]

1- إيهاب خليفة. مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي. مصر. العربي للنشر والتوزيع.2017.ص47.

2- نفس المرجع .

المطلب الثاني: مزايا الحروب الإلكترونية

من خلال التعريفات السابقة يمكن استخلاص بعض المزايا التي تميز هذا النوع من الحروب وهي كالآتي:

1-حروب تقنية متطورة جسدت قمة التطور الذي بلغته ثورة المعلومات وبوابتها الحاسبة الإلكترونية، والتي شكلت بدورها الأداة المحورية لهذا النوع من الحروب والميدان الرئيس لها فكانت نتيجة لذلك عرضة للتطور المستمر والتنوع والابتكار في تقنياتها ووسائلها لارتباطها الرأسي بقمتي الهرم التقني للحضارة الإنسانية، والمصالح الحيوية للدول[1]

2-حرب لا تناظرية بحساب التكلفة المتدنية نسبيا للأدوات اللازمة لشنها، فلا تحتاج الدول في سياق ذلك إلى تخصيص ميزانيات ضخمة من أجل إنتاج أسلحتها مقارنة بالأسلحة المستخدمة في النزاعات العنيفة ذات التكلفة العالية جدا، لذلك تفرض تهديدا خطيرا وحقيقيا على الدول الكبرى.

3-يتمتع فيها المهاجم بأفضلية واضحة على المدافع ،فهذه الحرب تتميز بالسرعة والمرونة والمراوغة وفي بيئة مماثلة يتمتع بها المهاجم بأفضلية من الصعب جدا على عقلية التحصن لوحدها أن تنجح؛ فالتحصين بهذا المعنى سيجعل من هذا الطرف عرضة لمزيد من محاولات الاختراق ، وبالتالي المزيد من الضغط.

4- فشل نماذج الردع المعروفة : يعد مفهوم الردع الذي تم تطبيقه بشكل أساس في الحرب الباردة غير ذي جدوى في هذا النوع من الحروب، فالردع بالانتقام، أو بالعقاب، لا ينطبق عليها؛ فعلى عكس الحروب التقليدية عندما ينطلق الصاروخ من أماكن يتم رصدها والرد عليها

1-أشرف السعيد أحمد .القرصنة الإلكترونية. القاهرة. دار النهضة العربية.2013.ص47.

فإنه من الصعوبة بما كان- بل ومن المستحيل- في كثير من الأحيان تحديد مكان وشخصية القائم بالهجمات الإلكترونية ذات الزخم الكبير، كونها لا تترك أثرا أو دليلا على حصولها، إذ أن معظم الهجمات الإلكترونية يتم اكتشافها بالصدفة، وبعد وقت طويل، وبالاستعانة بخبرة فنية عالية المستوى في كشف مصدر الهجوم؛ وهذا أمر قد يتطلب شهورا أو حتى سنوات، ما يعني إلغاء مفعول الردع بالانتقام، والأكثر من هذا فحتى إذا تم اكتشاف مصدر الهجوم الإلكتروني وتبين أنها تعود لفاعلين غير حكوميين فإنه في هذه الحالة لن يكون لديهم أصول أو قواعد حتى يتم الرد عليها[1]

5- حرب هلامية الشكل والملامح، فهي متعددة بميادينها، متنوعة ومتطورة بوسائلها المرتبطة بأكثر المجالات التقنية تطورا وتبدلا في الحياة المعاصرة للدول، فضلا عن ذلك فهي غير محددة الأهداف والتأثيرات، إذ قد تتعدى مخاطرها ميادين القتال التقليدية، لتطال بدمارها حتى أكثر المواقع السيادية والحساسة والأكثر تحصينا وبعدًا عن دائرة القتال.[2]

1-نفس المرجع. 45 .

2- سامر مؤيد عبد اللطيف. الحرب في الفضاء الرقمي رؤية مستقبلية. مجلة رسالة الحقوق.ع02.2015.العراق.مركز الدراسات القانونية والدستورية. ص79.

المطلب الثالث: الفرق بينها وبين مفاهيم مشابهة[1]

يتم في أحيان استخدام مفهوم الحرب الإلكترونية بدلالة مفاهيم أخرى مقاربة بسبب التداخل الذي قد يحصل بينها من حيث الطبيعة والنطاق والوظيفة مع مفاهيم مقاربة من أهمها (حرب المعلومات والإرهاب الإلكتروني). ولتثبيت الحدود الفاصلة بين تلك المفاهيم جرى تقسيم هذا المحور على عنصرين:

1-تمييزها عن حرب المعلومات:

للوهلة الأولى لا يمكن – بحال من الأحوال- تمييز الفارق النوعي أو فض الاشتباك

والتداخل بين المفهومين، لاسيما وأن العديد من الباحثين قد وظفوا هذين المفهومين بصورة متبادلة. وبتثبيت القاعدة المعرفية لمفهوم حرب المعلومات كمنطلق للتمييز بين المفهومين بصورة متبادلة وبتثبيت القاعدة المعرفية لمفهوم حرب المعلومات كمنطلق للتمييز بين المفهومين، نجد أن أحد الباحثين يعرف حرب المعلومات على أنها أي عمل الغاية منه إرغام الخصم على الخضوع لإرادتنا الوطنية وتنفيذ برامج الغاية منها السيطرة على نظام معلوماته. وعلى الطريق ذاته ذهب آخر في تعريفها بكونها نوع من حرب المعلومات التي تؤدي إلى إحداث خلل في أنظمة معلومات الخصم[2] .

وإن كانت تشترك مع الحرب الإلكترونية بالمعلومات التي يجري توظيفها لتحقيق النصر، فإن حرب المعلومات أكثر اتساعا وشمولا من الحرب الإلكترونية سواء في أدواتها التي تشمل الفضاء الرقمي والكهرومغناطيسي أيضا، أو حتى على الصعيد أهدافها التي تتعدى أبعاد التدمير المادي لتصل إلى المعنويات وما يلحقها من مستلزمات إدارة الحروب بكل أشكالها لتحقيق غاية النصر وإخضاع الخصم ؛ فتكون الحرب الإلكترونية التي يقتصر مضمارها على

1_ نفس المرجع. ص79.

2_ عبد الوهاب جعيجع. الأمن المعلوماتي وإدارة العلاقات الدولية . الجزائر. دار الخلدونية. 2017. ص66.

الشبكة الإلكترونية للمعلومات، وسلاحها وميدانها أيضا الحاسبة الإلكترونية وسيلة من بين الوسائل المتعددة التي توظفها هذه الأخيرة ضد الأعداء فتكون العلاقة بينهما كعلاقة الجزء

الحرب الإلكترونية والكل الذي يتمثل في حرب المعلومات، عبر رابة تتكامل فيها الأدوار بينهما لتتصل فيمل بعد بوحدة الهدف.

2_تمييزها عن الإرهاب الإلكتروني[1]

طبقا لوكالة المباحث الفيدرالية يعد الإرهاب الإلكتروني:« كل هجوم مخطط له بدافع سياسي ضد المعلومات، وأنظمة الحاسب الآلي، وبرنامج الحاسب، والبيانات مما يؤدي إلى العنف ضد أهداف غير حربية من قبل مجموعات وطنية فرعية أو عملاء متخفيين». وفي هذا التعريف يلاحظ أن ورود كلمة الهجوم لم يقتصر على الهجوم المعلوماتي، فقد أطلق بصورة عامة ليشمل حتى الإرهاب بشكله التقليدي، ضد بنية المعلومات، ويمكن القول بأن تعريف الإرهاب الإلكتروني ينبغي أن يشمل أشخاص مرتكبي الأعمال، وأدوات تنفيذ الأعمال الإرهابي، من برامج وأجهزة كما يلزم عند محاولة توصيف هذه الظاهرة التأكد من تحديد وضبط طبيعة الأفعال التي يمكن أن تدخل تحت هدا المصطلح ؛ مما سبق عرضه يمكن التفريق بين المفهومين عند تشخيص أطرافها وأهدافها، فعلى الرغم من اتحاد عنصر الوسيلة المتمثلة في أنظمة الشبكة الإلكترونية للمعلومات إلا أنه على مستوى الفاعلين نجد الإرهاب تقوم به جماعات أو أفراد أو هيئات دون مستوى الدول، ومع دخول الدولة على خط المواجهة الإلكترونية نكون أمام نمط الحرب الإلكترونية، أما على مستوى الأهداف فأهداف الإرهاب تفتقد بالضرورة إلى عنصر المشروعية، في حين تكون فيه أهداف الحرب التي تخوضها الدول في الفضاء الإلكتروني مشروعة.

1_ سامر مؤيد عبد اللطيف . مرجع سابق. ص80.

المبحث الثاني: صور الحروب الإلكترونية وأنماطها

المطلب الأول: صور الحرب الإلكترونية

خضعت أدوات الحرب الإلكترونية لتطورات متسارعة بفعل عوامل عدة، من أهمها الثورة التقنية التي عاشها العالم في القرنين الآخرين، وتنامي الاهتمام الرسمي والعلمي بهذا النوع من التقنيات الحربية بداعي الحاجة لتوظيفها في خدمة أغراض الصراع بين القوى السياسية وتنوع استخداماتها التي أفضتّ إلى تنوع صورها وأساليبّ إدارتها. ومن هذا المنطلق يمكن تحديد أهم صور الحرب الإلكتروني بالاعتماد على عامل التطور التاريخي وظروف الاستخدام في نوعين رئيسيين هما الحرب الإلكترونية التقليدية المصاحب للاشتباك المسلح، والحرب الإلكترونية المعاصرة في الفضاء الرقمي.

1_ الصورة التقليدية للحرب الإلكترونية أثناء الاشتباك المسلح: كانت أساليب الحرب الإلكترونية تستعمل بداية منذ بداية القرن الماضي . بدأ استخدام أجهزة الاتصالات اللاسلكية في الحروب ، وتفيد المصادر أن أول عملية كانت عام 1904م خلال الحرب الروسية [1]عندما كانت سفن الاستطلاع اليابانية تراقب الأسطول الروسي عن كثب وترسل جميع المعلومات بالراديو إلى القيادة ، وفي تلك الأحيان التقط أحد قادة الزوارق الروسية هذا الإرسال فطلب الإذن باستخدام جهاز الإرسال الموجود بزورقه من أجل إعاقة تلك الإرساليات ،لكن رفض طلبه من قبل القيادة الروسية، وبعد فترة وجيزة استطاع أحد قادة الزوارق الروسية دون إذن قيادته التشويش على هذه الإرساليات لكن بعد فوات الأوان ، إذ كانت المعركة قد وقعت وخسرها الروس.

1_ عادل علي خليل. الحرب الإلكترونية من الحرب العالمية الأولى إلى حرب الخليج. مصر دار الهلال.ص08.

أما في الحرب العالمية الأولى فقد استخدمت أجهزة الاتصالات وأجهزة نقل معلومات الاستطلاع بكثرة؛ إذ استطاعت إحدى السفن الإنجليزية سنة1914م أن ترسل بالراديو معلومات عن تحرك بعض القطع الحربية الألمانية في البحر الأبيض المتوسط، لكن بعد أن رصد الألمان تلك الإرساليات تمكنوا من التشويش الكامل عليها.[1]

أما البداية الحقيقية فكانت في الحرب العالمية الثانية لاستخدام لأجهزة الحرب الإلكترونية المتخصصة ففي عام1939م[2]استخدم الألمان طريقة تقاطع الموجات فوق الهدف من أجل قصف المدن الإنجليزية أثناء الليل، فوضع الإنجليز جهاز الإرسال ليقوم بتشويش مخادع ؛ كما استخدم الحلفاء أجهزة التشويش والنصلات للتشويش على الرادارات الألمانية عند الساحل الغربي الفرنسي كما استخدمت المناطيد والبالونات للتنصت والمراقبة والتصوير في عمق أراضي العدو.[3]

وبالتالي ارتبطت بعمليات التشويش والاستطلاع الإلكتروني، فكان ظهورها مقترنا بدخول الطيف الكهرومغناطيسي إلى ساحات المعارك الحربية، تنوعت صور وأساليب استثماره بين تحقيق غايات دفاعية، وأخرى هجومية .وبالاستناد على أساليب استخدام الطيف الكهرومغناطيسي ضمن نطاق الحرب الإلكترونية يمكن تحديد عمليات الدفاع الإلكتروني. وعمليات التشويش الإلكتروني.

فأما عمليات الدفاع والاستطلاع الإلكتروني فهي عبارة عن مجموع الإجراءات المتخذة للبحث عن الانبعاثات الكهرومغناطيسية واعتراضها لغرض تحديد التهديد الفوري سعيا لتقليل

1_ جاسم محمد البصيلي. الحرب الإلكترونية أسسها وأثرها في الحروب. ط2. بيروت. المؤسسة العربية للدراسات والنشر .1989. ص41.

2- صلاح الدين الأثرم. الحرب الإلكترونية من الحرب العالمية الأولى إلى حرب النجوم. ط2. سوريا. دار طلاسم للدراسات والترجمة والنشر .1993. ص47.

3_ كريم حميدة. الحرب الإلكترونية. الألوكة الثقافية.2012/03/20..www.alukah.net// http .2019/05/05.

قدرة العدو على الاستغلال الأمثل للطيف الإلكتروني في شن الهجمات على القوات الصديقة وحماية الأفراد، والمرافق والمعدات للقوات الصديقة من الآثار المدمرة المترتبة على ذلك النشاط المعادي.

وأما عمليات التشويش والهجوم الإلكتروني فهي مجموع الإجراءات المتخذة لمنع الاستخدام الفعال للطيف الكهرومغناطيسي والحد منه من قبل العدو باستخدام القدرات الإلكترونية.

وبالتالي فإنها تعرف بأنها مجموع الإجراءات المتخذة لاستطلاع وكشف المنظومات اللاسلكية الإلكترونية المعادية، وشلها

2_ الصورة المعاصرة للحرب الإلكترونية : ارتبطت بالحاسبات ، ميدانها هو الفضاء الافتراضي أين كشف الواقع الراهن في الفضاء الإلكتروني عن دخول شبكات الاتصال والمعلومات إلى بنية ومجال الاستخدامات الحربية .

ومع تمدد الأعمال العدائية الإلكترونية إلى البنية التحتية المعلوماتية للدول قصد تحقيق أغراض متداخلة (سياسية، اقتصادية، وإجرامية وغيرها)،حمل مفهوم الحرب الإلكترونية أبعادا جديدة، وصار البعض يفضل مصطلح "الحرب السيبرانية" كتعبير عن ذلك التوجه الجديد، وإن ظلت لفظة الحرب ذاتها محل جدل، خاصة وأن هناك مسميات عديدة تطلق على تلك الأنشطة العدائية الإلكترونية منها مثلا الهجمات الإلكترونية، والإرهاب الإلكتروني وغيرهما.[1]

1_ عادل عبد صادق. أنماط "الحرب السيبرانية "وتداعياتها على الأمن العالمي.http://ali;brqtaur.com.2019/05/28.

المطلب الثاني: أنماط الحروب الإلكترونية

1_ نمط الحرب الباردة الإلكترونية والصراع منخفض الشدة:

يتم استخدام الفضاء الإلكتروني كساحة للصراع منخفض الشدة ويعبر عن صراع مستمر بين الفاعلين المتنازعين وقد يكون ذو طبيعة ممتدة، ودائمة النشاط العدائي ،عميق الجذور، متداخل له نواح متعددة ثقافية أو اقتصادية أو اجتماعية ؛عادة ما يتم اللجوء إلى القوة الناعمة في مثل هذه الصراعات .

لها وسائل عدة منها شن الخروب النفسية، الاختراقات المتعددة، التجسس وسرقة المعلومات، وشن حرب الأفكار، والتنافس بين الشركات التكنولوجية العالمية وأجهزة الاستخبارات الدولية .

2_ نمط الحرب الإلكترونية متوسطة الشدة:[1]

يتحول الصراع عبر الفضاء الإلكتروني إلى ساحة موازية لحرب تقليدية قائمة على أرض الواقع، كما يمهد لعمل عسكري؛ هما تدور الحرب الإلكترونية عن طريق اختراق المواقع الإلكترونية وتخريبها وشن حرب نفسية ضد الخصوم.

3_ نمط الحرب الإلكترونية "الساخنة" و الصراع مرتفع الشدة:

عبارة عن نشوء حروب في الفضاء الإلكتروني منفردة، وغير متوازية مع الأعمال العسكرية التقليدية. لم يشهد العالم هذا النوع من الحروب حتى وإن كان احتمال حدوثها وارد في المستقبل مع تطور القدرات التكنولوجية، واتساع الاعتماد المتبادل بين الدول والفواعل من غير الدول على الفضاء الإلكتروني.

1_عادل عبد صادق. الحروب السيبرانية: تصاعد القدرات والتحديات للأمن العالمي. المركز العربي لأبحاث الفضاء الإليكتروني. 2017/03/12. http://accronline.com .2019/05/12.

ينطوي هذا النمط على سيطرة البعد التكنولوجي على إدارة العمليات الحربية أين يتم استخدام الأسلحة الإلكترونية فقط ضد منشآت العدو، وكذا اللجوء إلى الروبوتات الآلية في

الحروب والطائرات دون طيار، وإدارتها عن بعد، بخلاف تطوير القدرات في مجال الدفاع والهجوم الإلكتروني، والاستحواذ على القوة الإلكترونية؛ وفي هذا السياق يتم أيضا استخدام

الفضاء الإلكتروني للاستعداد لحرب المستقبل عبر قيام الدول بتدريبات على توجيه ضربة أولى لحواسيب العدو واختراق العمليات العسكرية عالية التقنية أو حتى استهداف الحياة المدنية والبنية التحتية المعلوماتية والهدف من ذلك تحقيق الهيمنة الإلكترونية الواسعة بشكل أسرع في حالة نشوب صراع.

المبحث الثالث: الإطار النظري

من أجل دراسة ظاهرة الحروب الإلكترونية وتأثيرها على الأمن القومي للدول، يستخدم إطار نظري يرتكز على مفهوم القوة كما توظفه كل من المدرسة الواقعية والمدرسة الليبرالية، حيث أن الاستخدام الفعلي للقوة الإلكترونية في السياسة الدولية يتم في إطار الجمع بينهما وبين كل من القوة الصلبة والقوة الناعمة. لكن قبل ذلك يجب الحديث أولا عن العوامل التي حالت دون إيجاد إطار نظري يستطيع تفسير ظاهرة الحرب الإلكترونية.

المطلب الأول: أسباب الفجوة المعرفية

ترجع صعوبة إيجاد إطار نظري تفسيري مناسب من شأنه تحليل ظاهرة التهديدات الإلكترونية وتأثيرها في ظاهرة الأمن القومي، وبالتالي على الأمن الدولي لمجموعة من الأسباب لعل أهمها:

أن الحروب الإلكترونية غير واضحة المعالم لأنها كانت مختلطة مع الحروب المعلوماتية والنفسية والدعائية، وبالتالي فإن ضبابية وهلامية هذا النوع من الحروب جعل من عملية تفسيره عملية صعبة وشاقة

حداثة التهديدات الإلكترونية، والتطور السريع لهذه التهديدات بشكل أربك حتى التقنيين

النقص في المصطلحات الفنية المتفق عليها لوصف هذه التهديدات، فلا يوجد فهم كامل لهذه التهديدات، فالأمن الإلكتروني غالبا ما يتم تبسيطه كحماية الشبكات وأنظمة البيانات. [1]

وهناك من يذهب إلى القول بأن سبب صعوبة إيجاد إطار نظري مناسب لتحليل هذه الظاهرة يرجع إلى أسباب موضوعية تكمن في تلك الفجوة المعرفية المتعلقة بالأمن الإلكتروني.

أين يرى كل من "**بيتر وارن سينغر**" و "**ألن فريدمان**" بأن أغلب القيادات في الجيوش الدولية أكبر المسؤولين حديثي عهد بالحواسيب، فشباب اليوم يعتبرون مواطنين أصليين في الفضاء الإلكتروني ، كان نشوؤهم في عالم أصبح فيه الحاسوب فيه أمرا طبيعيا؛ لكن مازال العالم يقاد بواسطة من يعتبرون مهاجرين في العالم الافتراضي، ذلك الجيل الذي تظل له الحواسيب ومخاطر الإنترنيت لغزا محيرا وأمرا غير مألوف ، فحتى عام2001 لم يكن هناك جهاز حاسوب في مكتب رئيس التحقيقات الفيدرالية بينما كان وزير الدفاع الأمريكي يطلب من مساعده أن يطبع له البريد الإلكتروني يقرأه ثم يكتب رده بالقلم ويطلب من مساعده طباعة ما كتب على الحاسوب، وبعد عقد كامل من الزمن صرحت وزيرة الأمن القومي في مؤتمر عام2012 صرحت قائلة:« لا تضحكوا...لكنني لا أستخدم البريد الإلكتروني إطلاقا» [2]اعتقادا منها بأنه من غير فائدة وليس موضوع حرص على الأمن.

كما أن الأمن الإلكتروني واحد من المجالات التي تركت لمن هم ميالون للتكنولوجيا للقلق بشأنها، كل ما هو متعلق بالعالم الرقمي ذو الأصفار والآحاد كان مشكلة يحلها فقط علماء الحاسوب وأنظمة المعلومات، وبالتالي فإن غالبية الميالين للتكنولوجيا نجدهم غير مهتمين بعوالم منطق السياسة

---

[1] _ إنمار موسى جواد. حرب الفضاء الإلكتروني المفهوم–الأدوات والتطبيقات. مجلة العلوم القانونية والسياسية. ع:02. العراق.2016.ص129.

[2] _مجاهد فخر الدين قاسم أحمد. ترجمة الصفحات(1–66) من كتاب الأمن الإلكتروني والحرب الإلكترونية ما ينبغي أن يعرفه كل شخص. مذكرة ماجستير. السودان. كلية الدراسات العليا. جامعة السودان للعلوم و التكنولوجيا. السودان.

المطلب الثاني: نموذج جوزيف ناي في توظيف القوة الإلكترونية إلى جانب القوة الصلبة والناعمة

أين يعتمد النموذج الذي قدمه **جوزيف ناي** الذي جمع بين القوة الإلكترونية وكل من القوة الصلبة والقوة الناعمة ،حلل من خلاله كيفية استخدام آليات معلوماتية من أجل توليد قوة صلبة وقوة ناعمة.

و من أجل فهم أدق لهذا النموذج فإن تحليل **ناي** يقوم حول ثلاث مفاهيم مركزية هي: القوة الإلكترونية_ انتشار القوة _ الفواعل الدولية

1_ القوة الإلكترونية: يعرف "**ناي**" القوة الإلكترونية « بأنها القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء الإلكتروني، أي أنها القدرة على استخدام الفضاء الإلكتروني لخلق مزايا، والتأثير في الأحداث المتعلقة بالبيئات الواقعية الأخرى وذلك عبر أدوات إلكترونية»[1].

يجادل "**ناي**" بأن مفهوم القوة الإلكترونية يشير إلى مجموعة الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات والشبكات الإلكترونية والبنية التحتية المعلوماتية والمهارات البشرية المدربة للتعامل مع هذه الوسائل ؛تتعدد أدوات ممارسة القوة في العلاقات الدولية وفقا لقدرات وإمكانيات ورغبات القوى المشاركة فيه، فقد تكون القوة العسكرية من أهم هذه الأدوات، وقد تكون القوة الاقتصادية والحصار الاقتصادي والمالي هما العامل الرئيسي للسيطرة على الخصم وممارسة القوة عليه، وقد تكون الأداة المعلوماتية من خلال وسائل الاتصال والتكنولوجيا الحديثة والإنترنيت هي العامل الرئيسي لحل الصراع بين دولتين.

ويرى "**ناي**" أن الدولة سوف تظل هي الفاعل المهيمن على الفضاء الإلكتروني، و لكن هناك فواعل أخرى سوف تشاركها هذا الفضاء وستجد صعوبة بالغة في السيطرة عليه فالحكومات قلقة من حالة تسرب المعلومات وتدفقها وصعوبة السيطرة عليها[2].

1_ إيهاب خليفة. القوة الإلكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الإنترنيت. القاهرة. العربي للنشر والتوزيع.2017.ص 24.

2_ نفس المرجع. ص 25.

كما يرى بأن الدول الكبرى ليست لها المساحة نفسها التي يمكن من خلالها السيطرة على الفضاء الإلكتروني مقارنة بقدرتها في السيطرة على الإقليم البري والبحري، وأن الكيانات الافتراضية التي تنشأ عبر الإنترنيت تستطيع الالتقاء في إقليم افتراضي جديد خاص بها غير الإنترنيت وتنشأ لها كيانات تنظيمية، ومن ثمة يتراجع دور الدولة المركزية في حياة البشر، ويضيف أن الدول الكبرى التي تمتلك القوة الصلبة أو الناعمة وجدت نفسها تواجه مشاكل في السيطرة على حدودها الإلكترونية. ويؤكد بأن الفضاء الإلكتروني لن يزيل سيادة الدولة أو حدودها الجغرافية ولمن سوف يؤثر على مفاهيم القوة وتحول أدوات القوة.[1]

1_ القوة الإلكترونية وانتشار القوة: يتميز الفضاء الإلكتروني بأن له عدة خصائص ساعدت على انتشاره والاعتماد المتزايد عليه، منها قلة التكلفة الاقتصادية، والسرعة في تبادل المعلومات، وسهولة استخدامه، فضلا عن إمكانية تخفي الفاعلين الذين يستخدمونه وعدم الكشف عن هوياتهم الحقيقية، وهو ما جعل الفضاء الإلكتروني بيئة جاذبة لمستخدميها، ودفعتهم إلى توظيفه في مختلف المجالات السياسية والاقتصادية والاجتماعية والعسكرية.

وكان نتيجة ذلك تنوع وزيادة عدد الفاعلين المستخدمين للفضاء الإلكتروني، وتعدد مجالات استخدامه ووظائفه، فلم يعد يقتصر على تبادل المعلومات؛ حيث باستطاعة أحد مستخدمي الفضاء الإلكتروني أن يوقع خسائر فادحة بالطرف الآخر، وأن يتسبب في شلل البنية

المعلوماتية والاتصالية الخاصة به، وهو ما يسبب خسائر عسكرية واقتصادية، من خلال قطع أنظمة الاتصال بين الوحدات العسكرية بعضها ببعض، أو تضليل معلوماتها أو سرقة معلومات سرية عنها أو من خلال التلاعب بالبيانات الاقتصادية والمالية وتزييفها أو مسحها من أجهزة الحواسيب، وعلى الرغم من فداحة الخسائر إلا أن الأسلحة تتمثل في فيروسات إلكترونية تخترق، شبكة الحاسب الآلي، وتنتشر بسرعة بين الأجهزة وتبدأ عملها في سرية تامة وبكفاءة عالية، وهي بذلك لا تفرق بين المقاتل والمدني، وبين العام والخاص، وبين السري والمعلوم.

---

[1] _ نفس المرجع.

3_ الفواعل الدولية وتوظيف القوة الإلكترونية: يحدد جوزيف ناي ثلاثة أنواع من الفاعلين الذين يمتلكون القوة الإلكترونية [1]

أ_ الدول: التي لديها قدرة كبيرة على تنفيذ هجمات إلكترونية وتطوير البنية التحتية وممارسة السلطات داخل حدودها

ب_ الأفراد(القراصنة): الذين يمتلكون معرفة تكنولوجية عالية والقدرة على توظيفها وعادة ما تكون هناك صعوبة في الكشف عن هوياتهم، ومن الصعب ملاحقتهم.

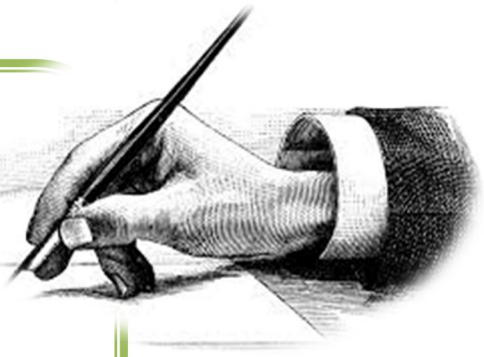
ج_ الفاعلون من غير الدول: يستخدم هؤلاء الفاعلون القوة الإلكترونية لأغراض هجومية بالأساس، إلا أن قدرتهم على تنفيذ أي هجوم سيبراني مؤثر يتطلب مشاركة ومساعدة أجهزة إستخبراتية متطورة، ولكن يمكنهم اختراق المواقع الإلكترونية واستهداف الأنظمة الدفاعية؛ ويمكن حصر الفواعل من غير الدول في(الشركات متعددة الجنسيات– المنظمات الإجرامية– الجماعات الإرهابية).

1_نفس المرجع.

خلاصة الفصل الأول:

مما سبق ذكره نرى بأن الحرب الإلكترونية ظاهرة قديمة جديدة في العلاقات الدولية، ارتبطت في بداياتها بعمليات التشويش الإلكتروني، ومع ظهور شبكة الإنترنيت أخذ هذا المفهوم دلالات جديدة أين أصبحت تعنى بذلك النوع من الصراع الذي ساحته جدران العالم الافتراضي. إلا أنه وحتى الوقت الراهن لم يكن هنالك اتفاق حول تعريف موحد ، بسبب تداخلها مع ظواهر أخرى مشابهة لها لذلك يجب العمل جيدا من أجل الاتفاق حول تعريف موحد من شأنه رسم حدود فاصلة بينها وبين غيرها من المفاهيم؛ كما يجب العمل من أجل إنتاج إطار نظري تفسيري من شأنه تفسير الحرب الإلكترونية تفسيرا علميا.

الفصل الثاني



الحروب الإلكترونية وتفاعلات الدول في الفضاء الإلكتروني

تمهيد:

من أجل الإحاطة بموضوع الحروب الإلكترونية وتأثيرها في التفاعلات الدولية كان لزاما علينا التطرق لمجموعة من المفاهيم ذات الصلة بمفهوم الحرب الإلكترونية هذا إن لم نقل بأنه بدونها لا يمكن فهم الظاهرة فهما دقيقا لذلك سنتطرق لمفهوم الفضاء الإلكتروني، والقوة الإلكترونية، بالإضافة إلى التطرق إلى مفهوم الصراع الإلكتروني.

المبحث الأول: القوة الإلكترونية والتفاعلات الدولية

المطلب الأول: ظهور نمط القوة الإلكترونية

يعتبر مفهوم القوة من المفاهيم المحورية في حقل العلاقات الدولية، حيث تناولته العديد من منظورات العلاقات الدولية التي عكست واقعا دوليا قائما على القوة باختلاف أنواعها وذلك بسبب الطبيعة التنافسية والصراعية والفوضوية للنظام الدولي، أو طبيعة الاعتماد المتبادل والتنافسية للمجتمع الدولي ،فتسعى كل دولة لفرض إرادتها واختياراتها على الآخرين من أجل الحفاظ على مصالحها في ظل عالم صراعي من أجل الحصول على القوة أو تعظيم القوة فالتعارض في المصالح بين وحدات النظام الدولي يؤدي إلى الصراع.

يرتبط مفهوم القوة كباقي مفاهيم العلوم الاجتماعية بالسياق المحيط به، لذا فإن التطور في السياسة الدولية إقليميا و دوليا سيؤدي بالضرورة إلى تغير في معنى القوة وأشكالها والعناصر المكونة لها ومن هنا يمكن القوا بأن مضمون وعناصر القوة تتحدد وفق مصادر التهديد المحتملة والفعلية للأمن وقد يأخذ التغيير في المفهوم أو وضع قواعد جديدة حاكمة للمفهوم، وهو ما يعتبر خطوة أكبر في تطوير المفهوم ومن هنا سيتم التركيز على السياق الفكري الذي صيغ فيه مفهوم القوة وحجم التغير في المفهوم الذي أدخلته مدارس العلاقات الدولية المختلفة ووفقا للتطورات السياسة الدولية.

أدى التطور التكنولوجي وثورة المعلومات إلى التحول في مفاهيم القوة فظهر مفهوم القوة الإلكترونية كوافد جديد في حقل العلاقات الدولية ، والتي يعرفها دانيال كويل على أنها «القدرة على استخدام الإنترنيت لخلق مزايا والتأثير على الأحداث من خلال أدوات القوة».[1]

أما جوزيف ناي فيرى بأنها القوة التي تعتمد على مصادر المعلومات والسيطرة على الأنشطة الإلكترونية والحواسيب والبنية التحتية المعلوماتية ذات الصلة بالفضاء الإلكتروني[2]

وبظهور هذا الشكل الجديد من القوة ترتبت عليه النتائج التالية:

_ تعدد شكل علاقات القوى، وتعدد الفاعلين المستخدمين لها، وتباين قوتهم النسبية.

_ تغير الأدوات المستخدمة في شن الحروب فأضحى الفضاء الإلكتروني بمثابة وسيلة للقيام بحروب غير تقليدية كالهجمات الإلكترونية والتجسس الإلكتروني وإطلاق فيروسات خبيثة على الأجهزة الإلكترونية.

مما أدى إلى نشأة مصادر تهديد غير تقليدية، من تخريب اقتصادي والجريمة والحرب الإلكترونية والإرهاب الإلكتروني؛ تلك التهديدات لها تأثير كبير على القوة الصلبة، نتيجة لصعوبة الردع في المجال الإلكتروني مقارنة بالمجالات الأخرى.

خلقت الثورة المعلوماتية مزايا جديدة ومختلفة بين الدول أهمها المنافسة على إنتاج المعلومات، والتي أصبحت مصدرا جديدا وهاما من مصادر قوة الدول في السياسة الدولية، حيث يرى ناي إنه في عصر المعلومات، الغلبة فيه للدولة أو الجهات الأخرى التي تمتلك الرواية الأفضل للوقائع.[3]

تميز العصر الحالي بانتشار الثورة المعلوماتية والتقنية والتي أدت إلى تحييد وإزاحة التكنولوجيا للعديد من عناصر القوة من موقعها الذي تربعت عليه لفترة طويل وأضحت القوة الإلكترونية

1_ إيهاب خليفة. مرجع سابق.

[2]_ سعاد محمود. دورة القوة: ديناميكيات الانتقال من الصلبة إلى الناعمة إلى الافتراضية، السياسة الدولية . ملحق اتجاهات نظرية.ع:188. 2012. ص16.

[1]-نفس المرجع. ص6.

حقيقة أساسية لا بد من الاعتراف بأهميتها الصلبة والناعمة، مثل دعمها للأعمال الحربية وتأثيرها على تطوير القدرات العسكرية للدول بجانب دعمها للقوة الاقتصادية والسياسية وخاصة في ظل ظهور مجتمع المعلومات الدولي.

المطلب الثاني: أثر الفضاء الإلكتروني على تحولات القوة

ساعدت ثورة المعلومات على إفراز ثلاثة عناصر أساسية هي المعلومة الطابع الإلكتروني والفضاء الإلكتروني هذا الأخير الذي يشتمل على كل الاتصالات والشبكات وقواعد المعلومات والبيانات ومصادر المعلومات ؛وقد أضحى الفضاء الإلكتروني بفضل ثورة المعلومات والإنترنيت أحد العناصر الأساسية المؤثرة في النظام الدولي بما يحمله من أدوات تكنولوجية قادرة على القيام بعمليات الحشد والتعبئة بجانب تأثيره في القيم السياسية وأشكال القوة المختلفة سواء الصلبة أو الناعمة.

فبالنسبة للقوة الصلبة(العسكرية) وعلاقتها بتكنولوجيا المعلومات فإن الأخيرة أدت إلى قيام ثورة في النظم العسكرية، وتطور نظام التسلح، وطبيعة ونوعية الأسلحة، وقدرتها التدميرية وبالتالي التأثير على القوة النسبية للدول وقدرتها على التأثير والنفوذ والهيمنة على هيكل القوة داخل النظام الدولي ولكنها كانت بمثابة سلاح ذو حدين فأدت إلى اختلاف نوعية الأسلحة المستخدمة وزيادة قوتها التدميرية ،لذلك اتجهت الدول للاهتمام بما سيتم فعله فوق إقليم دولة ما من سياسات تجارية ومالية ونفوذ سياسي واقتصادي وثقافي أيضا فكان ذلك أحد أهم التحولات التي أدت إلى ظهور مفهوم القوة الناعمة.

تحول العنصر الرئيسي في بناء القوة من الملكية إلى المعرفة والمعلومات وهو ما نتج عنه زيادة الوعي بأهمية الابتكار والتقدم التكنولوجي كأساس من أجل الاستحواذ على القوة وبالتالي أهمية تطوير مفاهيم استراتيجية ، والتقدم الاستخباراتي في المجال التقني والاقتصادي ونظم الاتصالات ، ومن هنا فقد أثر الفضاء الإلكتروني في التحول في مفهوم القوة على أساس الكم إلى القوة على أساس النتيجة المترتبة عليها والتحول بمفهوم توازن القوى على أساس الثقل المعادل إلى مفهوم الترابط كما يستخدم الفضاء الإلكتروني من قبل الدول لاعتبارات الأمن أين أصبحت تدخله ضمن حساباتهما الاستراتيجية وأمنها القومي فيما يعرف بالأمن الإلكتروني

بالإضافة إلى دور الفضاء الإلكتروني في تحقيق الرفاه الاقتصادي والتفوق السياسي، وزيادة معرفتها وسبقها في مجالات العلم والبحث

ويربط البعض بين الفضاء الإلكتروني والأمن الدولي حيث أن المحتوى المعلوماتي العسكري والفكري والسياسي والاجتماعي والاقتصادي والخدمي والعلمي والبحثي يوجد في الفضاء الإلكتروني ، نتيجة توسع العديد من الدول خاصة المتقدمة منها في تبني الحكومة الإلكترونية مما يجعلها عرضة لخطر الهجوم الإلكتروني، بالإضافة إلى الدعاية والمعلومات المضللة، أو الدعوة إلى أعمال تحريضية أو دعم المعارضين لنظام ما.

المطلب الثالث: عناصر القوة الإلكترونية

تشتمل عناصر القوة الإلكترونية لدولة ما على ستة عناصر أساسية هي[1]:

1_ بنية تحتية تكنولوجية: متمثلة في أجهزة الحاسب وشبكات اتصالات مرتبطة بأجهزة الحواسيب، وعنصر بشري مدرب يمتلك مهارة استخدام هذه الأجهزة وتستطيع من خلالها أن تمارس نوعا من التأثير، وتتضح معالم هذه البنية التحتية في أنظمة الدولة المالية والمصرفية وشبكات الكهرباء والطاقة ونظم إدارة الخدمات حيث تعتمد جميعا على الشبكات الإلكترونية في تقديم الخدمات.

2_الأسلحة الإلكترونية: هي برامج تم تصميمها بشكل معين لإلحاق الضرر وتخريب قواعد البيانات أو سرقتها، أو العمل على قطع الاتصال بالشبكة مع العلم أنه يصعب التعرف أو اكتشاف هذه الأسلحة.

1_ أحمد جلال محمود عبده. صراع القوة المدنية العسكرية وأثره على السياسة الخارجية التركية في منطقة الشرق الأوسط. القاهرة. المكتب العربي للمعارف. ص 49.

3_ العمليات الإلكترونية: وتشمل مهاجمة شبكة البيانات والحواسيب والتي تشمل اختراق هذه الشبكات وتعطيلها ونشر فيروسات تدمرها، أو نشر معلومات محرفة لإرباك العاملين عليها أو قطع قنوات الاتصال ،وشل قدرة الطرف الآخر على النشر السريع لقوته وإمكاناته كما تشمل

قطع أنظمة الاتصال فيما بين الوحدات العسكرية، أو فقد الخصم لقدرته على الاتصال بالأقمار الصناعية التابعة له.

4_ الدفاع عن شبكات الإعلام الآلي: وذلك عن طريق حماية الشبكات والبيانات من أي هجوم بالأسلحة الإلكترونية وما يسببه ذلك من أضرار جسيمة، بحيث يتم تأمين الشبكة والمكون المادي لها مثل الخوادم والشرائح الإلكترونية.

5_ الدفاع عن شبكات الإنترنيت: من خلال القدرة على التجسس على شبكات الخصم بهدف الحصول على معلومات دون أن يصاحب ذلك أي تدمير أو عطل بشبكات الحواسيب وقاعدة البيانات.

6_ الردع الإلكتروني: من خلال خلق مجموعة محفزات المناعة لقيام أحد الأطراف الصراع من القيام باعتداء أو هجوم مستقبلا مع العلم نه لا يستطيع أحد الأطراف تدمير الطرف الآخر كليا.

المبحث الثاني: ظاهرة الصراع في الفضاء الإلكتروني

المطلب الأول: أشكال الصراع الّإلكتروني

تعرضت ظاهرة الصراع إلى تغيرات مع بروز الفضاء الإلكتروني كمجال حيوي تنشأ فيها نزاعات بين الفاعلين المختلفين، خاصة مع الاعتماد الكثيف على تكنولوجيا الاتصال والمعلومات وهنا ظهر الصراع الإلكتروني كحالة من التعارض في المصالح والقيم بين الفاعلين في الفضاء الإلكتروني.

وعلى الرغم من الآثار المدمرة لهذا النمط من الصراعات إلا أنه لا يرافقه دماء؛ فقد يتضمن التجسس والتسلل إلى المواقع الإلكترونية للخصم، وقرصنتها، دون أنقاض أو غبار كما أن أطرافه مجهولين، وتنطوي كذلك تداعياته على مخاطر عدة على أمن الدول سواء على أمن الدول سواء عن طريق التخريب، أو استخدام أسلحة الفضاء الإلكتروني المتعددة.

ومع انتشار الفضاء الإلكتروني، وسهولة الدخول إليه اتسعت دائرة الصراعات السيبرانية، وزاد عدد المهاجمين وباتت هناك حالة الكر والفر في الهجمات الإلكترونية لتعبر عن الصراع الممتد أصبح الصراع بين الفاعلين المختلفين حول امتلاك أدوات الحماية والدفاع وتطوير القدرات الهجومية الإلكترونية يستهدف حيازة القوة والتفوق والهيمنة وتعزيز التنافس حول السيطرة، والابتكار والتحكم في المعلومات وتعظيم القدرات القادرة على زيادة النفوذ والتأثير في المستويين المحلي والدولي.[1]

وبما أن المتنازعين يلجؤون في الصراعات التقليدية إلى استخدام شتى أنواع أسلحة التدمير الممكنة فقد انتقلت جبهات القتال بشكل مواز إلى ساحة الفضاء الإلكتروني، وكان لهذا التغيير دور في إعادة التفكير في حركية وديناميكية الصراع، وبروز "عصر القوة النسبية" التي تعني بأن القوة العسكرية قد لا تكف لوحدها من أجل تأمين البنية التحتية للدول، الأمر الذي يخلف آثارا استراتيجية هائلة على تركيبة النظام الدولي

هناك عوامل ساهمت في انتقال الصراع إلى الفضاء الإلكتروني وبالتالي إفساح المجال لنشوب الحروب الإلكترونية:

أولا/ تغير منظور الحرب جذريا، حيث انتقلت من نسق الحروب بين الدول إلى وسط الشعوب فكان الغرض من الحروب قديما يتمثل في تدمير الخصم، إما باحتلال أرضه، أو بالاستيلاء على موارده؛ أما الحروب الجديدة فأصبحت تستهدف بالأساس التحكم في إرادة وخيارات المجتمعات ومن ثمة بدا للشعوب أهمية محورية سواء تعلق الأمر بالسكان المستهدفين

1-عادل عبد الصادق . أنماط الحرب السيبرانية وتداعياتها على الأمن العالمي. مرجع سابق .

في أرضية المواجهة، أو بالرأي العام في الدولة التي تشن الحرب، أو بالرأي العام على الصعيدين الإقليمي والدولي.

مع هذا التغير أصبحت أهداف الحرب أقل مادية، وتركزت أكثر على العامل النفسي والدعائي، لاسيما مع تنامي التغطية الإخبارية، والسمعية، والبصرية المباشرة للأحداث لحظة وقوعها عبر مواقع الإنترنيت والفضائيات، وضعف سيطرة أنظمة الحكم على توجهات مواطنيها.

ثانيا/ بروز الصراعات ذات الأبعاد المحلية_ الدولية[1] حيث ساعد اشتعال الصراعات الداخلية في مرحلة ما بعد الحرب الباردة، و كذلك طبيعة السياق الدولي للفضاء الإلكتروني في توفير بنيئة 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.

أسهم الفضاء الإلكتروني في دعم الهياكل التنظيمية والاتصالية للحركات والجماعات المحلية، والمنظمات المدنية بما ساعد الفاعلين من غير الدول على ممارسة قوة التجنيد، والحشد، والتعبئة، واستجلاب التمويل.

مما سبق ذكره يرى الأستاذ عادل عبد صادق بأن الحروب الإلكترونية تختلف أهدافها وفقا لطبيعة أهداف الصراعات الإلكترونية على النحو التالي

1_ صراع إلكتروني ذو طبيعة سياسية: تحركه دوافع سياسية، وقد يأخذ شكلا عسكريا يتم فيه استخدام قدرات هجومية ودفاعية عبر الفضاء الإلكتروني بهدف إفساد النظم المعلوماتية، والشبكات والبنية التحتية. ويتضمن هذا النوع من الصراعات توظيف أسلحة إلكترونية من قبل فاعلين داخل المجتمع المعلوماتي، أو من خلال التعاون مع قوى أخرى لتحقيق أهداف سياسية.

1_ نفس المرجع.

2_ صراع إلكتروني ذو طبيعة ناعمة: أي صراع حول الحصول على المعلومات، والتأثير في المشاعر والأفكار، وشن حرب نفسية وإعلامية ويتم ذلك من خلال تسريب

المعلومات، واستخدامها عبر منصات إعلامية، بما يؤثر في طبيعة العلاقات الدولية، كالدور الذي لعبه موقع ويكيليكس في الدبلوماسية الدولية.[1]

3_ صراع إلكتروني على التقدم التكنولوجي والاقتصادي: يأخذ هذا النمط من الصراع طابعا تنافسيا حول الاستحواذ على سبق التقدم التكنولوجي، وسرقة الأسرار الاقتصادية والعلمية. وقد يمتد إلى محاولة السيطرة على الإنترنيت، وأسماء النطاقات، وعناوين المواقع والتحكم بالمعلومات، والعمل على اختراق الأمن القومي للدول، بدون استخدام طائرات أو متفجرات، أو حتى انتهاك حدود الدول، كهجمات قراصنة الكومبيوتر، وتدمير المواقع والتجسس، بما قد يكون له من تأثيرات مدمرة على الاقتصاد والبنية التحتية بذات قوة التفجير التقليدي إن لم يكن أكثر.

4_ صراع إلكتروني على المعلومات والاستخبارات: فمع صعوبة الفصل بين أنشطة الاستخبارات، وجمع المعلومات وحروب الفضاء الإلكتروني أو التمييز بين الاستخدام السياسي والإجرامي، يبدو الفضاء الإلكتروني بيئة أكثر مناسبة للصراعات المعلوماتية. إذ يسهم في بقدرة الأجهزة الأمنية للدول، أو حتى الجماعات المختلفة، على تشكيل شبكة من عالمية من العملاء بدون تورط مباشر، بالإضافة إلى رخص التكلفة، وسهولة الاتصال، وصعوبة الرقابة التقليدية على التفاعلات الإلكترونية، ومثل ذلك عنصر جذب لاستخدام الأسلحة الإلكترونية، وتوظيفها لتحقيق أهداف سياسية وعسكرية.

المطلب الثاني : خصائص الصراع الإلكتروني

يتمتع الصراع الإلكتروني بمجموعة من الخصائص لعل أهمها ما نوجزه فيما يلي:

[1]_نفس المرجع.

1_ أصبح الصراع الإلكتروني حقيقة واقعة وليس مجرد خيال علمي أين نجد العديد من الصراعات قد حدثت فعلا لكن على ساحة العالم الافتراضي .

2_ يحدث هذا النوع من الصراع بسرعة الضوء فعندما تتدفق فوتونات[1] الحزم المهاجمة عبر الألياف الضوئية فإن الوقت المستغرق لشن الهجمة وتأثيرها يكاد يتعذر قياسه مما يسهم في إرباك صناع القرار أثناء الأزمات.

3_ صراع عالمي الطابع فالعدوان الإلكتروني يستشري على مستوى العالم سريعا لأن أجهزة الحاسوب والأجهزة الخادمة المخترقة خفية أو التي تم السيطرة عليها في أنحاء العالم سرعان ما تنظم إلى الهجمات فتجر بلادا كثيرة إلى الصراع سريعا.

4_ أصبحت الدول تتحسب من وقوعه في حالة السلم قبل الحرب، فبدأت تعد الدول ساحة المعركة وذلك من خلال محاولتها اختراق شبكات الدول المعادية وزرع ثغرات التسلل وهذا الطابع للصراع الإلكتروني هو الذي طمس الحدود الفاصلة بين السلم والحرب وخلق بعدا جديدا في حالة انعدام الاستقرار.

5_ الفضاء الإلكتروني لا حدود له حيث يتشارك فيه جميع الفاعلين بما في ذلك الدول من الاستخدام الشخصي إلى البرامج الاقتصادية وحتى العسكرية كلها تعتمد على الفضاء الإلكتروني وعلى العكس من التهديدات التقليدية الملموسة ممكن التنبؤ بها فإن تهديدات الفضاء الإلكتروني يمكن أن تأخذ شكل ومصدر افتراضي وتفرض أخطارا لا يمكن التنبؤ بها.

6_ صعوبة التعرف على هوية المعتدي أو المهاجم فهو صراع يكتنفه الغموض

7_ يمكن استخدام أسلحة الفضاء الإلكتروني بسرعة وسهولة وبدون الفهم الكامل للتفاقم التصاعدي الذي ينجم عنها فعلى الرغم من أن الصراع يبدأ بين جدران العالم الافتراضي بلا جنود ولا أشلاء ومن غير إراقة دماء إلا أنه في بعض الأحيان لا تظل كذلك طويلا فقيام

1_ إنمار موسى جواد. مرجع سابق. ص131.

الدول بزرع أسلحة الفضاء الإلكترونية في شبكات البنية التحتية لغيرها من الدول من شأنه إشعال فتيل الحرب أكثر من أي وقت مضى في تاريخ الحروب.

أما بالنسبة لأثر أسلحة الفضاء الإلكتروني فإنها أثرها يقل خطورة عن الأسلحة النووية لكن استعمالها في ظروف معينة قد يحدث أضرارا بالغة وقد يشعل فتيل حروب واسعة ويمكن قياس القوة في مجال الصراع الإلكتروني من خلال تقييم ثلاثة عوامل

الأول: الهجوم أي قدرة الدولة على شن هجمات إلكترونية على الدول الأخرى.

الثاني: القدرة على الدفاع ويعني قدرة الدولة على اتخاذ القرارات في حال تعرضها لهجوم إلكتروني لصد الهجمة أو التخفيف من آثارها.

الثالث: الاعتماد ويعني مدى اتصال الدولة بالإنترنيت واعتمادها على الشبكات والأنظمة التي قد تكون عرضة للأخطار في حالة وقوع تهديد إلكتروني.[1]

المطلب الثالث: العلاقة بين الأمن الإلكتروني والأمن القومي

تزداد العلاقة بين الأمن الإلكتروني والأمن القومي كلما زاد نقل المحتوى المعلوماتي والعسكري والأمني والفكري والسياسي والاجتماعي والاقتصادي والخدمي والعلمي والبحثي إلى الفضاء الإلكتروني، خاصة مع التسارع في تبني الحكومات الإلكترونية والمدن الذكية في العديد من الدول، واتساع نطاق وعدد مستخدمي الإنترنيت في العالم، والثورة الكبرى في انترنيت الأشياء، حيث أصبحت قواعد البيانات القومية في حالة انكشاف خارجي، إضافة إلى حملات الدعاية والمعلومات المضللة ونشر الشائعات أو الدعوة لأعمال تحريضية أو دعم المعارضة والأقليات، مما يساهم في تلاشي سيادة الدولة ويشكك في قدرتها على الحفاظ على أمنها.

1_ نفس المرجع. ص132.

وعليه فلم يقتصر اهتمام الدول بالأمن الإلكتروني على البعد التقني وحسب، بل تجاوزه إلى أبعاد أخرى مثل الأبعاد الثقافية والاجتماعية والاقتصادية والعسكرية وغيرها وهو ما عمل

على دعم حقيقة أن الاستخدام غير السلمي للفضاء الإلكتروني يؤثر على الرخاء الاقتصادي والاستقرار الاجتماعي لجميع الدول التي أصبحت تعتمد على البنية التحتية الكونية للمعلومات.

إضافة إلى تصاعد دور الفاعلين من غير الدول في العلاقات الدولية قد أثر بدوره على سيادة الدول وخاصة مع بروز دور الشركات التكنولوجية العابرة للحدود، وبروز أخطار القرصنة والجريمة السيبرانية والجماعات الإرهابية.

لقد أصبحت المصالح القومية التي ترتبط بالبنية التحتية الحيوية عرضة لخطر الهجوم، فجعل الفضاء الإلكتروني تلك المصالح مرتبطة ببعضها البعض في بيئة عمل واحدة ومن ثمة فإن أي هجوم على إحدى تلك المصالح من شأنه إحداث خلل في التوازن الاستراتيجي، ومهدد خطير للأمن القومي، وهذا ما دفع بالعديد من الدول إلى إدخال الأمن الإلكتروني ضمن استراتيجياتها للأمن القومي.

المبحث الثالث: تأثير الحرب الإلكترونية على التفاعلات الدولية

المطلب الأول: العوامل التي ساعدت في تصاعد دور الحروب الإلكترونية

تبلورت مصالح قومية للفضاء الإلكتروني إثر تزايد الاعتماد ربط البنى التحتية القومية للمعلومات (قطاع الطاقة و الاتصالات، النقل والخدمات الحكومية والمالية والتجارة الإلكترونية وغيرها) وبالتالي فإن أي تهديد محتمل أو هجوم على إّحدى تلك القطاعات هو تهديد لوجود الدولة، ويؤدي إلى حدوث اختلال في التوازن الاستراتيجي ، وهو ما يكشف عن نمط جديد من التهديدات للأمن القومي

ساعد في تنامي مثل هذه التهديدات الإلكترونية لمصالح الدول، ومن ثمة إمكانية بروز حرب إلكترونية. من بين أهم العوامل التي أدت إلى تصاعد دورها ما يلي:

1_ تزايد ارتباط العالم بالفضاء الإلكتروني مما أدى إلى توسع خطر تعرض البنية التحتية الكونية للمعلومات إلى خطر التعرض لهجمات إلكترونية فضلا عن استخدامه من قبل فاعلين من غير الدول(خاصة المجموعات الإرهابية) لتحقيق أهدافها التي تنال من الأمن القومي للدول.

2_ تراجع دور الدولة في ظل العولمة وانسحابها من بعض القطاعات الاستراتيجية لمصلحة القطاع الخاص وخاصة مع تصاعد دور الشركات متعددة الجنسيات، خاصة العاملة في مجال التكنولوجيا كفاعل مؤثر في الفضاء الإلكتروني، لاسيما مع امتلاكها قدرات تقنية تفوق الحكومات.[1]

3_ نشوء نمط جديد من الضرر على خلفية الهجمات الإلكترونية يمكن أن تسببه دولة إلى أخرى، دون الحاجة للدخول المادي إلى أراضيها؛ ذلك أن تزايد اعتماد الدول على الأنظمة الإلكترونية في جميع منشآتها الحيوية جعل هذه الأخيرة عرضة للهجوم المزدوج، لما لها من

[1]_ عادل عبد الصادق. أنماط "الحرب السيبرانية" وتداعياتها على الأمن العالمي. مرجع سابق.

سمات مدنية وعسكرية متداخلة، خاصة وأن الثورة التكنولوجية الحديثة تمخضت عنها ثورة أخرى في المجالات العسكرية وتطور الحرب.

4_ قلة تكلفة الحروب الإلكترونية مقارنة بنظيراتها التقليدي، فقد يتم شن هجوم إلكتروني بما يعادل تكلفة دبابة من خلال أسلحة إلكترونية جديدة ومهارات بشرية علاوة على أن هذا الهجوم قد يتم في أي وقت سواءً أكان وقت السلم أم الحرب أم أزمة ولا يتطلب تنفيذه سوى وقت محدود.

5_ تحول الحروب الإلكترونية إلى إحدى أدوات التأثير في المعلومات المستخدمة في مستويات ومراحل الصراع المختلفة، سواء على الصعيد الاستراتيجي، أو التكتيكي العملياتي بهدف التأثير بشكل سلبي في هذه المعلومات، ونظم عملها.

6_ توظيف الفضاء الإلكتروني في تعظيم قوة الدول، من خلال إيجاد ميزة أو تفوق أو تأثير في البيئات المختلفة، وبالتالي ظهور ما يسمى "الاستراتيجية الإلكترونية" للدول، والتي تشير إلى القدرة على التنمية وتوظيف القدرات للتشغيل في الفضاء الإلكتروني، وذلك بالاندماج والتنسيق مع المجلات العملياتية لتحقيق أو دعم إنجاز الأهداف، عبر عناصر القوة القومية.

7_ أدى تصاعد المخاطر والتهديدات في الفضاء الإلكتروني إلى بروز تنافس بين الشركات العاملة في مجال الأمن الإلكتروني بغرض تعزيز أسواق الإنفاق العالمي على تأمين البنى التحتية السيبرانية للدول بالإضافة إلى بروز فاعلين آخرين من شبكات الجريمة المنظمة والقراصنة وغيرهم.

8_ اتساع نطاق مخاطر الأنشطة العدائية التي يمارسها الفاعلون، سواء من الدول أو غير الدول في الحروب الإلكترونية، فقد تشن الدول الهجمات الإلكترونية عبر أجهزتها الأمنية والدفاعية، كما قد تلجأ إلى تجنيد قراصنة، أو موالين لشن هجمات ضد الخصوم، دون أي ارتباط رسمي، وبرغم عدم تطوير الجماعات الإرهابية-كفاعل من غير الدول-لقدراتها في الحرب الإلكترونية لنشر الأفكار المتطرفة، فإن هناك مؤشرات على احتمال تطوير تلك الجماعات لقدراتها الهجومية مستقبلا

المطلب الثاني: وسائل وأدوات الحروب الإلكترونية

يتمثل استخدام أدوات حرب الفضاء الإلكتروني في القيام بعمل تخريبي عبر قطع كابلات الاتصالات أو الأقمار الصناعية أو استخدام الأسلحة الإلكترونية المتقدمة كالفيرسات في تدمير الأنظمة المعلوماتية لمنشآت حيوية بشكل يؤثر على وظائفها ويهدد أمن الدولة والسكان.

من أسلحة الحرب الإلكترونية البرامج الخبيثة وهي مجموعة من البرمجيات كالفيروسات والديدان وحيل تصيد المعلومات وتحاول هذه البرامج استغلال العيوب الموجودة في البرامج الأخرى والأخطاء التي يقع فيها مستخدمو الحاسوب قبل الدخول إلى المواقع المصابة بالعدوى الفيروسية أو فتح مرفقات الرسائل البريدية، والفيروسات هي برامج يتم تمريرها من مستخدم إلى آخر عبر الإنترنيت أو الوسائط المحمولة مثل وحدات التخزين الصغيرة؛ أما الديدان فلا تتطلب تمرير برنامج إلى مستخدم آخر لأنها قادرة على نسخ نفسها ذاتيا باستغلال عيوب معروفة ثم تزحف كالديدان عبر الإنترنيت. أما تصيد المعلومات فتقوم على خداع المستعمل للإدلاء بمعلومات مهمة مثل رقم الحسابات المصرفية وشفرات المرور.

وقد يقوم محاربو الفضاء الإلكتروني بإنشاء ثغرة تسلل وهي نفس فكرة حصان طروادة وهي برامج حاسوب غير مرخص يضاف إلى برنامج ما لأغراض خبيثة يسمح بالولوج الغير مرخص إلى شبك أو برنامج حاسوبي فغالبا بعد أن يقوم رجال الفضاء الإلكتروني باختراق الشبكة لأول مرة فإنهم يتركون وراءهم ثغرة تسلل للسماح لهم بالدخول في المستقبل بطريقة أسرع وأسهل؛ وأحيانا تسمح ثغرات التسلل لمحاربي الفضاء الإلكتروني بالدخول إلى أجزاء معينة من الشبكة لا يسمح لهم بالدخول إليها عادة وعند اختراقهم برناماجا ما وهو لا يزال قيد

التطور فإنه لا يسرق نسخة منه فحسب بل قد يضيف إليه شيئا ما وأحيانا تسمح لهم ثغرة التسلل الوصول إلى الجذر فتصبح لديهم السلطات و الصلاحيات التي يتمتع بها مصمم البرنامج وبالتالي يمكنهم إضافة ما يشاؤون من برمجيات ويمحون أي دليل على وجودهم. وقد

يذهبون إلى أبعد من ذلك وذلك من خلال زرع قنبلة منطقية[1]وهي تطبيق من تطبيقات الحاسوب أو برنامج من برامج عمله يسبب إيقاف عمله، أو حذف كل البيانات الموجودة على الشبكة ؛ وهناك أدوات أكثر تقدما من القنابل المنطقية يمكنها توجيه أوامر لمعدات الحاسوب لتقوم بشيء يعمل على تدميرها، كأن تجبر شبكة الكهرباء بتوليد حمل يفوق قدرتها يؤدي إلى حرق دوائر محولاتها أو تجعل لوحات التحكم في الطيران تدفع بالطائرة إلى السقوط المفاجئ وبعد ذلك تمحو كل شيء وتمحو نفسها.

ومن أدوات الحرب الإلكترونية إنشاء شبكات تجبيرية مسلوبة الإرادة زهي شبكة من الحواسيب التي تجبر على العمل وفقا لأوامر مستخدم بعيد غير مرخص له باستخدامها وتستغل هذه الشبكة في الهجوم على أنظمة أخرى.

ومن الأدوات الأخرى منصات التواصل الاجتماعي التي تضم باقة من المواقع ذات النفوذ القوي عبر العالم وتعد هذه المواقع أكثر البيئات تناسيا وتناغما مع الحروب الإلكترونية بل قد تكون هي وجه الصراع القائم الآن في عقدنا التقني هذا كونها سهلة الوصول والاستخدام تفاعلية وشعبية بشكل كبير ومتطورة بوتيرة مرتفعة من عيوبها أنها ذات طابع اصطيادي أي يمكن من خلالها الإيقاع بضحايا إلكترونيين إلا أنها أصبحت منبرا حاشدا للتغيير السياسي.[2]

1_ إنمار موسى جواد. مرجع سابق. ص134.

1_ مصعب قتلوني. دور مواقع التواصل الاجتماعي "الفايسبوك" في عملية التغيير السياسي مصر أنموذجا .رسالة ماجستير (غير منشورة). كلية الدراسات العليا. جامعة النجاح. نابلس. فلسطين. 2012.ص 89.

المطلب الثالث: مخاطر وتداعيات الحروب الإلكترونية

باتت العلاقة بين الأمن والتكنولوجيا علاقة متزايدة مع إمكانية تعرض المصالح الاستراتيجية –ذات الطبيعة الإلكترونية–إلى أخطار إلكترونية، وتهدد بتحول الفضاء الإلكتروني لساحة لتغذية للتوترات الدولية، ما أدى إلى جملة من المخاطر والتداعيات على تفاعلات السياسة الدولية، يمكن طرح أبرزها على النحو التالي:

1_ تصاعد المخاطر الإلكترونية، خاصة مع قابلية المنشآت الحيوية (مدنية و عسكرية) في الدول للهجوم الإلكتروني عبر وسيط وحامل للخدمات، أو شل عمل أنظمتها المعلوماتية، الأمر الذي يؤثر في وظائف تلك المنشآت، وبالتالي فإن التحكم في تنفيذ هذا الهجوم يعد أداة سيطرة استراتيجية بالغة الأهمية، سواء في زمن السلم أو الحرب.

2_ تعزيز القوة وانتشارها، فمن جهة عزز الفضاء الإلكتروني ما سمي بالقوة المؤسسية في السياسة الدولية، ويقصد بها أن يكون لها دور في قوة الفاعلين، وتحقيق أهدافهم وقيمهم في ظل التنافس التنافس مع الآخرين، والإسهام في تشكل الفعل الاجتماعي في ظل المعرفة والمحددات المتاحة والتي تؤثر في تشكيل السياسة العالمية .

ومن جهة أخرى، عمل الفضاء الإلكتروني على إعادة تشكيل قدرة الأطراف المؤثرة–مثل الولايات المتحدة الأمريكية– فبعدما كانت تملك ما يشبه الاحتكار لمصادر القوة بعد انتهاء الحرب الباردة، ظهرت عملية انتشار القوة بين أطراف متعددة سواء كانت دولا أم من غير الدول.[1]

3_ عسكرة الفضاء الإلكتروني سعيا لدرء تهديداته على أمن الفضاء الإلكتروني، وبرز في هذا الإطار اتجاهات، مثل التطور في مجال سياسات الدفاع والأمن الإلكتروني، وتصاعد القدرات في سباق التسلح السيبراني، وتبني سياسات دفاعية سيبرانية لدى الأجهزة المعنية

[1]_ إيهاب خليفة. القوة الإلكترونية وأبعاد التحول في خصائص القوة. مصر. مكتبة الإسكندرية. 2014. ص 29.

بالدفاع والأمن في الدول، وتزايد الاستثمار في مجال تطوير أدوات الحرب الإلكترونية داخل الجيوش الحديثة.

4- إدماج الفضاء الإلكتروني ضمن الأمن القومي لدول، وذلك عن طريق تحديث الجيوش، وإنشاء وحدات متخصصة في الحروب الإلكترونية، وإقامة هيئات وطنية للأمن والدفاع الإلكتروني، والقيام بالتدريب، وإجراء المناورات لتعزيز الدفاعات الإلكترونية، والعمل على تعزيز التعاون الدولي في مجالات تأمين الفضاء الإلكتروني، والقيام بمشروعات وطنية للأمن الإلكتروني.

5- الاستعداد لحروب المستقبل، حيث تبني العديد من الدول استراتيجية حرب المعلومات بحسبانها حربا للمستقبل، والتي يتم خوضها بهدف التشتيت، وإثارة الاضطرابات في عملية صناعة القار لدى الخصوم، عبر اختراق أنظمتهم، واستخدام ونقل معلوماتهم وهنا ترى الدول الكبرى أن من يحدد مصير تلك المعركة المستقبلية ليس من يملك القوة فقط، وإنما من يمتلك القدرة على شل القوة والتشويش على المعلومة.

6- تحديث القدرات الهجومية والدفاعية والهجومية، فسعت الدول إلى تحديث النشاط الدفاعي لمواجهة مخاطر الحرب الإلكترونية، والاستثمار في البنية التحتية المعلوماتية، وتأمينها، وتحديث القدرات العسكرية ورفع كفاءة الجاهزية لمثل هذه الحرب عن طريق التدريب، والمشاركة الدولية في حماية البنية المعلوماتية، والاستثمار في رفع القدرات البشرية داخل الأجهزة الوطنية المعنية وهنا يتعلق التوجه الأخطر بنقل تلك القدرات من الدفاع إلى الهجوم عن طريق استخدام تلك الهجمات في إطار إدارة الصراع والتوتر مع دول أخرى.

خلاصة الفصل الثاني:

مما سبق ذكره نجد أن الفضاء الإلكتروني أصبح مجالا خامسا تدور فيها أحداث الصراع الدولي وفيه يتم قيام الحروب، وما زاد من أهمية هذا الميدان ظهور القوة الإلكترونية كشكل جديد من أشكال القوة، وما زاد من خطورة التهديدات الإلكترونية هو حجم المخاطر التي تنتج عن هذا النوع من الصراع.

الفصل الثالث

الصراع الإلكتروني الأمريكي الروسي وتداعياته

تمهيد:

أدى التطور التكنولوجي الذي شهده العالم، وهذه الثورة المعلوماتية إلى التغير في طبيعة الصراع الدولي وخاصة في ظل هذا الترابط المعلوماتي أين أصبح العالم قرية صغيرة، وأضحت المعلومة متاحة نظرا لسهولة الحصول عليها، وبما خلقه الفضاء الإلكتروني من ميزات نسبية خاصة للطرف المهاجم، فقد دخل تاريخ الصراع الأمريكي الروسي مرحلة جديدة حاول فيها كل طرف تسخير الفضاء الإلكتروني بطريقة تمكنه من تحقيق مصالحه مع تجنب المواجهة المباشرة.

المبحث الأول: تطور العلاقات الأمريكية الروسية

المطلب الأول: العلاقات الأمريكية السوفياتية قبل وأثناء الحرب الباردة

مرت العلاقات الأمريكية الروسية بمراحل عديدة متقلبة ومتفاوتة حسب الظروف وحسب ما تقتضيه المصالح والأهداف، ففي مطلع الثلاثينيات من القرن الماضي كانت الولايات المتحدة الأمريكية الوحيدة التي لم تعترف بالاتحاد السوفياتي على الرغم من التعاون الاقتصادي الذي كان قائما بينهما في ظل عدم وجود علاقات دبلوماسية بين البلدين، وعلى الرغم من احتلال الاتحاد السوفياتي المرتبة الأولى سنة1931 [1]في استيراد السيارات والمعدات من أمريكا، فرضت عليه هذه الأخيرة قيودا صارمة على الصادرات بعد اتهامه بالتدخل في شؤونها الداخلية.

التعاون فترة الحرب العالمية الثانية: بلغ التعاون بين الدولتين أوجه أثناء الحرب العالمية الثانية، من أجل مجابهة الخطر النازي، فأعلنت الولايات المتحدة دعمها للاتحاد السوفياتي عن طريق تقديم المساعدات على اختلافها، متجنبة المخاطر التي كانت تتعرض لها سفنها بفعل ملاحقة البوارج والغواصات الألمانية.

1_ منصور زغيب. تجدد الصراع الأمريكي الروسي في ضوء الأزمات المتجددة. مجلة الدفاع الوطني. ع:99. 2014. http:www.leberny.gov.lb/ ar/ com.05/05/2019.

الصراع أثناء الحرب الباردة: بدأت حالة الصراع والاختلاف في وجهات النظر بين البلدين حول تحديد المستقبل السياسي للقارة الأوربية عموما ومسألة وحدة ألمانيا على وجه الخصوص، إلا أن هناك واقعة تعتبر الأكثر إثارة في هذه المرحلة تتمثل في اكتشاف السلطات الروسية قيام المعسكر الغربي بحفر نفق تحت أرض برلين بهدف التنصت على الاتصالات السوفياتية مما دفعهم إلى تزويدهم بمعلومات مزيفة.

مما أدى إلى التوتر في العلاقات خاصة بعد إنشاء حلف شمال الأطلسي الذي سعى إلى مواجهة المد الشيوعي، وتمثلت رد فعل الاتحاد السوفياتي بإنشاء حلف وارسو سنة1955.

والجدير بالذكر أن امتلاك الجانبين لأسلحة الدمار الشامل أثار الذعر والقلق من

حصول مجابهة عسكرية لم يمنع من حصولها إلا حالة الشعور بالخوف المتبادل ، فما كان

منهما إلا الاحتكام إلى حل وسط يجنب العالم حربا فتاكة تكون نتائجها أكبر من سابقاتها، فكان نتيجة ذلك الانفراج في العلاقات الأمريكية السوفياتية وذلك مع وصول كل من "ريتشارد نيكسون" إلى سدة الحكم بالولايات المتحدة الأمريكية ، باعترافه بأن الاتحاد السوفياتي قوة عظمى لها مصالحها ووزنها الدولي، فتمخض عن ذلك توقيع العديد من الاتفاقيات المشتركة، والمعاهدات أهمها اتفاقيات الحد من التسلح وحظر التجارب النووية في الجو والفضاء وتحت الماء، كذلك تم التوصل إلى معاهدة تقتضي الحد من منظومات الدرع الصاروخية، وأخرى تنص على الإجراءات الرامية إلى الحد من الأسلحة الاستراتيجية الهجومية، بالإضافة إلى التدابير الرامية إلى تطوير التجارة وغيرها من العلاقات الاقتصادية، بالإضافة إلى تبادل العديد من الزيارات من قبل رؤساء ومسؤولين ووفود من أرفع المستويات، من أجل تأكيد النهج الجديد في العلاقات وإرساء قواعد على أسس ومرتكزات جديدة.

اتسمت الحرب الباردة بجملة من الخصائص من أبرزها المستوى العالي من الصراع الذي تخللته بعض مظاهر التعاون النسبي الذي تقتضيها مصلحة كل منهما، فحتى في أوج الحرب الباردة كان هناك انفراج في العلاقات لوحظت عودة إلى الحرب الباردة بأخطر مظاهرها وذلك بسبب تعاقب الأحداث وتداخلها في جميع المراحل وقد أظهرت كل من الولايات المتحدة والاتحاد السوفياتي الحرص الشديد على تجنب وقوع مواجهة مباشرة بينهما.

المطلب الثاني: العلاقات الأمريكية الروسية بعد نهاية الحرب الباردة[1]

بسقوط الاتحاد السوفياتي ظهرت إلى الوجود معطيات جديدة في السياسة الدولية، أين تغير نسق النظام الدولي إلى أحادية قطبية بزعامة الولايات المتحدة الأمريكية، وأدى ذلك إلى حدوث تغير في مفاهيم العلاقات الدولية ومسلماتها، فبالإضافة إلى العامل العسكري أصبح العامل الاقتصادي والاجتماعي وحتى التكنولوجي والثقافي يحتل مكانة مهمة في تصنيف الدول في النظام العالمي الجديد؛ فحاولت روسيا الاتحادية انتهاج سياسة جديدة قوامها الاتجاه نحو الغرب بصفة الشراكة بهدف الخروج من الضائقة الاقتصادية، عبرت عن ذلك من خلا مجموعة من الخطوات التي اتخذتها، من بينها الانضمام إلى المؤسسات الاقتصادية الغربية والسياسية والتوافق مع الغرب في القضايا ذات الاهتمام المشترك في محاولة لجعل الغرب يتقبل روسيا بوصفها دولة صديقة بعد الحرب الباردة، بالإضافة إلى المضي قدما في محادثات نزع السلاح، بعد إدراكها عدم إمكانية استمرار إنتاجه وتحمل تكاليف لتحديثه، بالإضافة إلى سياسة الانفتاح على المستوى الدبلوماسي والسياسي في اتجاهات أكثر واقعية مع المتغيرات الدولية .

في فبراير 1992 تم التوقيع على وثيقة التعاون بين جورج بوش و بوريس يلتسين حيث تم الاتفاق على الميثاق الروسي للشراكة والصداقة، إلا أن ظهور متغيرات جديدة في آسيا الوسطى دعا روسيا إلى إعادة التفكير في توجه سياساتها الخارجية أين ظهر للوجود التنافس التركي الإيراني على آسيا الوسطى، مما اعتبرته روسيا تهديدا لمصالحها بتلك المنطقة، بالإضافة إلى تدفق أعداد كبيرة من الروس من دول الجوار الغربية الأمر الذي هدد الاقتصاد الروسي مع صعود التيارات الأصولية المتطرفة في آسيا الوسطى مما شكل تهديدا للأمن القومي الروسي ووحدة الأراضي الروسية.

في المقابل فإن الولايات المتحدة الأمريكية لم تساند روسيا في توجهها الجديد، بل عمدت إلى إضعاف الخصم الروسي عبر تعزيز الدعم الاستخباراتي للمقاتلين الشيشان في

1_ نفس المرجع.

معركتهم للانفصال عن روسيا، ومن هنا يقال أن علاقة البلدين لم تتعد حدود العلاقات السياسية الودية لإنهاء مظاهر الحرب الباردة.

وهكذا ظلت العلاقات الأمريكية الروسية خلال العقد الأخير من القرن العشرين بين مد وجزر، سعت الولايات المتحدة الأمريكية إلى الحفاظ على تفوقها العسكري عن طريق تحديث قوتها زيادة قدراتها العسكرية، والعمل على منع ظهور قطب منافس لها.

وبغض النظر عن العولمة والتطور الاقتصادي تحولت أولويات السياسة الخارجية الروسية الى التشدد في المحافظة على المصالح القومية الروسية، وتعميق التوجه الأوراسي لكبح جماح الولايات المتحدة الأمريكية التي تحاول تهديد الأمن القومي الروسي عن طريق إثارة الأزمات، ودعم الحروب الدائرة بالقرب من الحدود الروسية، والعمل على توسيع دائرة حلف شمال الأطلسي شرقا وجنوبا، بالإضافة إلى نشر الصواريخ وإقامة القواعد العسكرية.

المطلب الثالث: العلاقات الأمريكية الروسية بعد أحداث 11سبتمبر 2001

مع دخول الألفية الجديدة شهدت العلاقات بين البلدين توجها جديدا نتيجة التحول الذي طرأ على نوعية القيادة على مستوى الطرفين، بالإضافة إلى رواسب الحرب الباردة وتداعياتها التي أثرت في نظرة البلدين أو أحدهما إلى الآخر، ومن الواضح وجود تعارض دائم ين القيادتين ولم يحدث التقارب إلا في نقاط قليلة ونادرة، فكان التنافس والتوتر السمة المميزة للعلاقة بينهما، الأمر الذي دفع أطراف أخرى للاستفادة من هذا الوضع وقد تكون إيران ربما أكبر المستفيدين إذ أدت الحاجة الروسية إلى ممارسة الضغط من خلال توسيع تعاونها مع إيران في برنامجها النووي.

هذا وتميزت هذه الحقبة بأحداث قلبت النظام الدولي وكان لها الأثر المباشر في نمط العلاقة بين الطرفين، فانطلاقا من أحداث11سبتمبر2001 دخل العالم مرحلة جديدة تختلف كليا عن المراحل السابقة ما دفع بالولايات المتحدة لإكمال سياستها الكونية الرامية إلى السيطرة

والهيمنة على العالم من خلال المضي قدما في محاربة الإرهاب مع ما يستوجب ذلك من أفعال وقائية وحروب استباقية، وفي إطار هذا التوجه أيدت روسيا الغزو الأمريكي لأفغانستان سنة2001[1] وسهلت عملية إنشاء قاعدة عسكرية في أوزباكستان، وبالمقابل اعترفت واشنطن لموسكو بأن منطقة آسيا والقوقاز هي منطقة نفوذ روسي، كما تم إبرام اتفاقيات ولقاءات على أرفع المستويات بشكل غير مسبوق وذلك في إطار بلورة العلاقات بين الدولتين في مجال الاستقرار الاستراتيجي والتعاون وحل النزاعات القائمة.

هذا وقد ناقش كلا الطرفين مستقبل العلاقات بينهما في ضوء طرح العديد من الأزمات الدولية التي تشكل بؤر التوتر بين البلدين بسبب اختلاف وجهات النظر والمصالح المتحكمة بمواقفهما إزاء تلك القضايا، فروسيا عارضت غزو العراق من دون موافقة مجلس الأمن، ومن

ثمة طالب الرئيس الروسي بأن تستكمل لجان التفتيش والبحث عن أسلحة الدمار الشامل وأن تعلن النتائج، الأمر الذي رفضته الولايات المتحدة وعملت على إنهاء عمل تلك اللجان.

كذلك ساءت العلاقات حيال العديد من القضايا الدولية أهمها مسألة جورجيا2008،[2] ونشر الولايات المتحدة الدرع الصاروخي في بولندا وتشيكيا، الأمر الذي رأت فيه موسكو تهديدا مباشرا لأمنها القومي يضاف إلى ذلك سعي الإدارة الأمريكية إلى تحقيق استقلال إقليم كوسوفو عن جمهورية صيربيا المقربة من روسيا، فضلا عن الملف النووي الإيراني الذي أثارته الإدارة الأمريكية مع روسيا التي تعدها أمريكا الحليف العسكري لإيران في سعي منها إلى فك ذلك الحلف ومنع تصدير التكنولوجيا النووية لإيران لما في ذلك من تهديد للمصالح الأمريكية في كل من الخليج العربي والصراع العربي الإسرائيلي.

ومن القضايا التي شكلت مؤخرا بؤرة جديدة للتوتر في الدولتين مسألة الربيع العربي وبصورة خاصة الأزمة السورية لما لها من خصوصية إقليمية ودولية ومحط حسابات فعال، حيث تحولت هذه الأزمة إلى صراع دولي من الطراز الرفيع يشبه إلى حد ما الحرب الباردة بين

---

[1]_ نفس المرجع.

2_ نفس المرجع

الشرق والغرب ودخلت أحداث هذا البلد بازار التجاذبات والمساومات بين الدولتين وفق المصالح السياسية والاقتصادية والعسكرية.

مما سبق نرى بأن العلاقات الروسية الأمريكية لطالما كانت في تغير وتطور، غير أن السمة الغالبة لهذه العلاقات كانت الطابع الصراعي الذي تباينت وتنوعت أسبابه بين إيديولوجية واقتصادية وحتى سياسة. إلا أن الثابت في العلاقات الروسية الأمريكية هو الابتعاد كل البعد عن المواجهة المباشرة لذلك نجد أن كلا من الطرفين عمد إلى إيجاد وسائل استراتيجية من شأنها تحقيق مصالحه الحيوية دون الحاجة إلى الاشتباك مع الطرف الآخر، وبالتالي فرض الفضاء الإلكتروني نفسه كساحة جديدة للصراع بين الطرفين بطريقة يعمد فيها كل طرف إلى تحقق المصالح الاستراتيجية .

المبحث الثاني: الصراع الإلكتروني الروسي الأمريكي

المطلب الأول: الاستراتيجية الروسية في الأمن الإلكتروني

تشترك كل من روسيا والولايات المتحدة الأمريكية في كونهما من أكثر الدول اعتمادا على الفضاء الإلكتروني والأكثر عرضة للهجمات الإلكترونية [1]. كما تعتبر من أكثر الدول وضوحا في الإعلان عن استراتيجيات الأمن الإلكتروني الخاصة بها، إما بالإعلان عنها صراحة أو من خلال مسؤولين مطلعين على ما يتم في إطار تطوير سياسة أمنية إلكترونية أو ممن عملوا في إحدى المؤسسات الموكل إليها بمهمة الدفاع الإلكتروني داخل الدولة[2]،بالإضافة إلى أنها كانت من أكثر الدول بروزا كطرف في الهجمات الإلكترونية في السنوات الأخيرة.

بدأ الاهتمام الروسي بالأبعاد السياسية للأمن الإلكتروني بعد تأسيس مجلس الأمن الروسي عام1992 وإضافة إلى المؤسسات الأمنية الروسية، تم إنشاء مؤسسات أخرى تختص فقط بالقضايا الإلكترونية وبحماية الأمن الإلكتروني الروسي، ومن أهم المؤسسات المسؤولة عن الأمن الإلكتروني في روسيا هي مجلس الأمن، وجهاز الأمن الفدرالي للتحكم التقني ووزارة الاتصالات وتكنولوجيا المعلومات، تتقسم المهام بين الإدارات المختلفة في الأنشطة المتعلقة بالأمن الإلكتروني كالآتي: وزارة الداخلية بمواجهة الجرائم الإلكترونية؛ وزارة الدفاع كل ما يتعلق بأخطار الحروب الإلكترونية وتطوير القدرات الإلكترونية الهجومية للجيش الروسي، ويهتم جهاز الأمن الفدرالي بالإرهاب الإلكتروني[3]

تبلور الاهتمام الروسي بقضايا المن الإلكتروني سنة2000 أين قامت روسيا بتطوير استراتيجية أمنية تبنى على أساس الإيمان الكامل بالدور الذي يلعبه الأمن الإلكتروني في تحقيق المصالح القومية وتعزيز الاستقرار الاجتماعي والسياسي، وتتصدر روسيا الدول الساعية

---

[1] _ نوران شقيق. أثر التهديدات الإلكترونية على العلاقات الدولية دراسة في أبعاد الأمن الإلكتروني. القاهرة. المكتب العربي للمعارف.2018.ص 66.

[2] _نفس المرجع. ص67.

3_ نفس المرجع. ص69.

لتطوير اتفاقية دولية لمواجهة المخاطر الإلكترونية نتيجة لتزايد التنافس التكنولوجي ما بين الفواعل على المستوى الدولي.

كما تعتمد الاستراتيجية الروسية الخاصة بالحروب الإلكترونية على استخدام الأسلحة الإلكترونية الهجومية باعتبار أنها قوة مضاعفة في الحروب، فهي تزيد من القدرات القتالية للدولة إذا ما تم استخدامها إلى جانب قدرات عسكرية أخرى كما تعتمد الاستراتيجية الروسية على محاولة تعطيل البنية التحتية المعلوماتية للخصم والاتصالات المدنية والعسكرية له قبل البدء في العمليات العسكرية.

القدرات الإلكترونية الروسية: يرى المنظرون الروس بأن الحرب الإلكترونية تشير إلى كيفية استخدام الكرملين لقدرته على الإنترنيت لتحقيق الأهداف القومية لروسيا، ففي نظرهم أن موسكو تخوض صراع وجودي مستمر مع قوى داخلية وأخرى خارجية تسعى إلى تحدي أمنها في عالم المعلومات ، ويرون أن في الفضاء الإلكتروني تهديدا وفرصا يمكن استغلالها بصورة إيجابية لخدمة أهدافها القومية على حد سواء.

أنشأت روسيا ما يعرف بجيش المتصدين تابع لوكالة الأمن الاتحادي الروسي يضم الآلاف من الموظفين، يخصص له سنويا حوالي 300 مليون دولار من ميزانية الدفاع الروسية[1] ويعد خامس أقوى جيوش العالم الإلكترونية بعد كل من الولايات المتحدة الأمريكية ، الصين، بريطانيا، وكوريا الشمالية على التوالي؛ تتلخص مهامه فيما يلي:

-القيام بعمليات التجسس على الخصوم

-شن الهجمات الإلكترونية التي تسبب الضرر بالبنى التحتية والاقتصادية والمواقع الحكومية في الدول المعادية.

-شن حروب معلوماتية في وسائل الإعلام والشبكات الاجتماعية عن طريق القيام بعمليات اختراق الحسابات والبريد الإلكتروني وإنشاء حسابات وهمية على شبكة المعلومات

1_أحمد يوسف الجميلي. القدرات السيبرانية سلاح روسيا ضد الخصوم. مركز صنع السياسات للدراسات الدولية الإستراتيجية. 2019/05/26http://www.making policies.org..2018/06/19.

الدولية، وفتح الآلاف من الحسابات المزيفة على مواقع التواصل الاجتماعي للرد على الآلاف من التعليقات والمقالات ونشر الشائعات وتضليل الحقائق في محاولة لدعم الموقف الروسي وتوجيه الرأي العام ضد الخصوم.

وتتمثل الميزة الأساسية للجيش الإلكتروني الروسي في عنصر المباغتة فلطالما اعتمد على عنصر الهجوم لإرباك الخصم، فالسيبرانية الهجومية تلعب دورا كبيرا في العمليات العسكرية ،وربما ستلعب دورا أكبر في المستقبل في إطار استراتيجية الردع الروسية، وعلى الرغم من أن الجيش الروسي كان بطيئا في اعتناق العقيدة السيبرانية لأسباب هيكلية وعقيدية على حد سواء فقد أشار الكرملين إلى أنه يعتزم تعزيز القدرات الهجومية الإلكترونية بحروبها المختلفة.

المطلب الثاني: الإستراتيجية الأمريكية في الأمن الإلكتروني

تتمتع الولايات المتحدة الأمريكية بمخزون ثوراتي تكنولوجي ضخم، فهي رائدة الابتكار الاتصالي السحري (الإنترنيت) علاوة عن امتلاكها قاعدة بيانات تحتوي العديد من أنظمة التشغيل وبروتوكولات التواصل واسترجاع المعلومات والأرشيف المعلوماتي المشفر.

التفتت الولايات المتحدة إلى أهمية حماية معلوماتها الإلكترونية القومية في وقت مبكر، والاستفادة من توفير منظومة أمنية لمعلوماتها الرقمية لتشرع بتطبيق سلسلة من الإجراءات القانونية والتقنية والرقابية التي تتناسب وحجم محتواها المعلوماتي، واتساع رقعتها الجغرافية وتوجهاتها السياسية والاقتصادية والاجتماعية والثقافة الداخلية والخارجية نحو جعلها أكثر البلاد أمنا في العالم، وأضخمها احتمالا للمعلومات الإلكترونية، لذلك تعمد الخطة الأمريكية لحماية أمنها الإلكتروني على ثلاث منظومات سياسية وبنائية بشكل متسلسل ومتداخلة بطريقة أكثر متانة على النحو التالي:

1_ المنظومة القانونية: تضم سلسلة من القوانين الفدرالية التي تنظم التعامل مع المعلومات الإلكترونية من منظور أمني وقومي، وقانون إصلاح وإدارة قطاع تكنولوجيا المعلومات، وقانون الحرية الإلكترونية وغيرها من القوانين الأخرى.[1]

2_ المنظومة الفنية: وهي التي تقوم بوضع المعايير الفنية والتقنية الموحدة للتعامل مع الأمن الإلكتروني ، تتشكل هذه المنظومة من عدة جهات مختصة كالمعهد القومي للتكنولوجيا والمعايير ،ولجنة السياسة القومية لتشفير المعلومات والتي عملها تشفير وترميز المعلومات والبيانات المتداولة إلكترونيا وحفظها من الاندثار أو التداول اللاسلمي

3_ المنظومة التنفيذية والتطبيقية والرقابية: هي عبارة عن مجموعة من الهيئات والوكالات الفدرالية المسؤولة عن تطبيق وتنفيذ سياسات الأمن الإلكتروني، والتي لها ارتباطات مع باقي المؤسسات والوزارات القومية في الداخل الأمريكي حيث تقدم لها الاستشارات

والتطبيقات المعلوماتية والأمنية الإلكترونية تقوم هذه المنظومة بالتنسيق مع العشرات من الوكالات على رأسها وكالة المخابرات ووكالة الأمن القومي وزارة الدفاع، المكاتب المعنية بالشؤون الاجتماعية والاقتصادية، بهدف إبقاء الأمن المعلوماتي متزن مع جميع الجهات والحصول على قدر كاف من المعلومات المتعلقة بالأمن المعلوماتي الأمريكي[2]

مما سبق نرى بأن الأمن الإلكتروني قد أصبح على قمة أولويات الأمن القومي، حتى أن التهديدات الإلكترونية من الممكن أن تحل محل خطر الإرهاب في السنوات القادمة، فأغلب التقارير والدراسات التي تناقش موضوع التهديدات الإلكترونية والتي تتوقع حدوث حروب إلكترونية في السنوات القادمة هي دراسات أمريكية بالأساس وبعضها صادر عن مؤسسات أمريكية رسمية.

وبداية من سنة 2010 قامت الولايات المتحدة بإصدار استراتيجية الأمن القومي التي أشارت إلى دور الفواعل من الدول في الفضاء الإلكتروني وما يمكن أن يمثلوه من تهديد

[1]_وليد غسان سعيد جلعود. دور الحرب الإلكترونية في الصراع العربي الإسرائيلي. مذكرة ماجستير. كلية الدراسات العليا. جامعة النجاح الوطنية. نابلس. فلسطين. 2013. ص64.

[2]_ نفس المرجع. ص 65.

المصالح الأمريكية بل أكثر من ذلك فبعد أن كان الاهتمام الأمريكي الأكبر بالأبعاد السياسية للهجمات الإلكترونية أصبح هناك اهتمام كبير بالأبعاد الاقتصادية وتداعيات أي هجوم محتمل على الاقتصاد القومي الأمريكي، حتى أنها أصبحت ترى في الفضاء الإلكتروني أنه المجال الخامس[1] الذي تمارس فيه العمليات العسكرية ولابد أن تهتم به للحفاظ على أمنها وذلك عبر استراتيجيتها الأمنية والتي تقوم على أربع ركائز هي:

1_تعزيز الأمن القومي الأمريكي من خلال تبادل المعلومات عبر الوكالات المتخصصة من أجل حماية شبكات الكومبيوتر وتأمين البنية التحتية الحيوية للبلاد، وذلك من خلال إعطاء وزارة الأمن الوطني مزيدا من الصلاحيات لرقابة جهود الأمن السيبراني المدنية، ومكافحة الجرائم السيبرانية من خلال التعاون مع الدول الأخرى لتعقب منفذيها

2_ تعزيز الاقتصاد الرقمي بتشجيع الابتكار في مجال التكنولوجيا، وذلك من خلال العمل مع شركات التكنولوجيا لتعزيز اختبارات الأمن الإلكتروني في المنتجات الجديدة، بالإضافة إلى بناء قوة عاملة حكومية في مجال الأمن الإلكتروني من خلال توظيف المتخصصين من ذوي الكفاءات في مجال الأمن الإلكتروني في المؤسسات والوكالات الأمريكية.

3_ مكافحة التهديدات الإلكترونية من خلال استخدام كافة أدوات القوة الأمريكية لردع أي هجمات وتعزيز المعايير الدولية في الفضاء الإلكتروني.

4_ الدعوة إلى حرية الإنترنيت في جميع أنحاء العالم وتزويد حلفاء الولايات المتحدة الأمريكية بقدرات إلكترونية–من أجل التعامل مع هذا النوع من التهديدات–والتي تستهدف المصالح المشتركة. [2]

---

[1]– نوران شفيق. مرجع سابق. ص72

[2]_ عمرو عبد العاطي. استراتيجية أمريكية هجومية ضد التهديدات السيبرانية المركز المصري للفكر والدراسات الاستراتيجية. .2019/05/23. http:www. Ecsstudies.com.2018/10/31

المبحث الثالث: الانتخابات الأمريكية ومستقبل الحروب الإلكترونية

المطلب الأول: التدخل الروسي في الانتخابات الأمريكية2016

تعود حيثيات هذه الحادثة إلى عام2012 أين ادعت روسيا بأن **هيلاري كلينتون** – عندما كانت تشغل منصب وزيرة الخارجية الأمريكية– شجعت الاحتجاجات التي انطلقت بعد انتهاء الانتخابات الروسية في مارس2012، والتي أتت بفلاديمير **بوتين** رئيسا لروسيا الاتحادية ، الأمر الذي دفع المعارضة الروسية والمنافسين الأربعة **لبوتين** من التشكيك في نزاهة الانتخابات فانطلقت المظاهرات والاحتجاجات، وفي المقابل قامت حملة اعتقالات طالت قادة المعارضة في روسيا من قبل السلطات، فأعربت الخارجية الأمريكية عن قلقها من حركات القمع والمعارضة أكثر من مرة، وهو ما اعتبرته القيادة الروسية محاولة من كلينتون لخلق حالة من الفوضى السياسية في البلاد.[1]

أصبحت الدول في الوقت الراهن تعمل جاهدة من أجل حماية الحسابات الإلكترونية والبريدية التابعة للدولة، من أجل تجنيب أمنها القومي خطر الحروب الإلكترونية، لذلك فقد أصبحت تمنح المسؤولين حسابات بريدية رسمية ولكن في بداية سنة2015، وقبل أن تعلن كلينتون عن نيتها في الترشح للانتخابات الرئاسية الأمريكية، كشفت تقارير صحفية عن استخدام **هيلاري** بريدا إلكترونيا خاصا تستخدمه بدلا من البريد الرسمي وهو ما أثار المخاوف الأمريكية حول تعرضه لعمليات قرصنة مما يهدد الأمن القومي.

اتهمت الولايات المتحدة الأمريكية روسيا بالقيام بهجمات إلكترونية وذلك باختراق البريد الإلكتروني للحزب الديمقراطي الأمريكي ومدير حملة المترشحة **هيلاري كلينتون، جون بوديشا** وقامت بتسريب رسائل البريد الإلكتروني إلى موقع **ويكيليكس** لنشرها كما استخدمت حسابات روسية [1]شبه معلنة وأخرى خفية على مواقع التواصل الاجتماعي هاشتاغات وعبارات منتشرة

1_ عمرو صبحي. تكتيك الدرع والسيف في استخدام القوة السيبرانية. المركز العربي للبحوث والدراسات.2018/04/26. http://www.qcrrseg.org/40716. 02/06/2019 .

لإظهار ما يبدو أنهم مؤيدو المرشح الجمهوري **دونالد ترامب** المحافظون أو مشجعون يمينيون متطرفون على وسائل التواصل الاجتماعي والتي تمتلئ تعريفاتهم الشخصية بكلمات مثل الدولة

المسيحية[1]، أمريكا، الجيش ثم يدفعون بهاشتاغات مؤيدة **لترامب** مع أخبار كاذبة ومضللة إلى الجمهور الأمريكي الأمر الذي ساعد على إحداث حالة التأييد **لترامب** والتشكيك في الحكومة الأمريكية.

المطلب الثاني: الآفاق المستقبلية للحروب الإلكترونية

أضحى للفضاء الإلكتروني دور أساسي في تعظيم القوة الإلكتروني ، أو الاستحواذ على عناصرها الأساسية، وأضحى التطور في هذا المجال عنصرا حيويا في العلاقات الدولية ؛ يكشف الكثير من الخبراء والكثير من الدراسات الاستراتيجية عن القوة الإلكترونية وروافدها، إذ أن الكثير من الدول تسعى لتحديث قدراتها السيبرانية الدفاعية والهجومية والاستثمار في البنية التحتية المعلوماتية وتأمينها وذلك مع اتساع نطاق المخاطر في الفضاء الإلكتروني في مقدمتها الولايات المتحدة وروسيا والصين يليها قوى إقليمية مثل كوريا وإسرائيل وإيران والبرازيل بالإضافة إلى شركات البرمجيات العالمية الأكثر إنتاجا لبرامج وتطبيقات القوة السيبرانية الفاعلة ويرصد موقع" world Atlas10 " شركات كبرى منها 7 شركات أمريكية تهيمن على الإنتاج ومبيعا وإدارة شبكات المعلومات الدولية[2]، وتمتلك هذه الشركات الكثير من المعلومات الخطرة ذات الحساسية البالغة.

عزز الصراع الإلكتروني دور وأهمية الأمن السيبراني والعامل الأخطر هو عدم كفاءة التأهب واستعداد الحكومات والمؤسسات الدولية للتعامل مع هذه التهديدات وطبيعتها غير

1_ أحمد يوسف الجميلي، مرجع سابق.

2_عبد الغفار عفيفي الدويك فجوة القوة السيبرانية والحاجة إلى مبادرة أممية .الحياة. 2018/02/12 .http://www.qlhqyqt.com. 2019/05/25.

المتماثلة وهناك دلائل تشير إلى أن الدول المتقدمة تستفيد من نقاط الضعف في الفضاء الإلكتروني .

إن معدلات التهديدات وفرص الحروب الإلكترونية تتزايد مع توظيف القدرات الإلكترونية في تحقيق المصالح، بخاصة مع اتساع مخاطر العدائيات السيبرانية وزيادة عدد الأطراف في هذا المجال .وفي هذا الإطار صاغت الدول استراتيجياتها للأمن الإلكتروني لسد الفجوة بين عالمين الأول متقدم يمتلك منظومة للردع السيبراني (أمريكا روسيا والصين) وهي دول قامت فعليا بعمليات سيبيرانية هجومية ضد خصومها والثاني نامي يحاول بناء منظومة دفاعية على

المستوى الوطني أو على مستوى التحالفات الإقليمية مثل الإتحاد الأوربي والناتو وفق أجندة سياسية تحقق مصالحهم.

بعد إيقان الدول الكبرى لخطورة الاعتماد على الفضاء الإلكتروني قامت بإجراءات احترازية مثلما قامت به روسيا حينما أعلنت في يناير 2018 أن الجيش الروسي سوف يستغني عن نظام التشغيل ويندوز ويعتمد كليا على نظام التشغيل **آسترا لينوكس** باعتباره برنامجا استوفى كل الشروط الخاصة بالحماية الأمنية للمعلومات، بالشكل الكافي للقدرة على حماية الملفات المصنفة في أعلى درجات السرية ثم محاولة إدخاله في المؤسسات لتبنيه، خاصة بعد "**فيروس الفدية**" و "**أنا كراي**" الذي أصاب معظم حواسيب الكرة الأرضية صيف2017 والتي تعمل بنظام "**ويندوز إكس بي**" وهو ما جعل شركة مايكروسوفت تتوقف عن إمداد هذا النظام بتجديدات أمنية لحمايته [1].

[1]_ عمرو صبحي. مرجع سابق

على ضوء ما تقدم سيشهد العالم مزيدا من الهجمات السيبرانية في الأعوام القليلة القادمة وستصبح الأسلحة الهجومية أكثر ضراوة، وبخاصة وأن هذا النوع من الهجمات يمكنها أن تحقق أهدافا لا يمكن للهجمات التقليدية والنجاح في المجال الإلكتروني لا يتطلب الدفاع فحسب، فالردع لن يكون فعالا ما لم يتم تبني قدرات هجومية، والمأمول أن تتبنى الأمم المتحدة طرح مبادرة تدعو دول العالم للالتزام بميثاق شرف للحد من انتشار الأسلحة الإلكترونية كخطوة أولى تمهيدا لتوقيع معاهدة دولية لتحقيق الأمن الإلكتروني.

خلاصة الفصل الثالث:

مما سبق ذكره نرى بأنه ومع ظهور القوة الإلكترونية كشكل جديد من أشكال القوة التي تراوحت استعمالاتها بين نمط القوة الصلبة والقوة الناعمة في الفضاء الإلكتروني فإننا نجد بأن كلا من الولايات المتحدة الأمريكية وروسيا الاتحادية قد حاولا الاستفادة من الميزات التي وفرها الفضاء الإلكتروني باعتباره مجالا يختصر الجيوبوليتيك وبالتالي تم نقل الصراع الأزلي إلى جدران الفضاء الافتراضي وكانت بالتالي حادثة التدخل الروسي في الانتخابات الأمريكية أوضح صورة للحروب الإلكترونية وتجسيدا واقعيا لها.

الخاتمـــــة

الخاتمة:

وظف الإنسان التكنولوجيا الحديثة في صراعاته وخصوماته، فأحدثت الحواسيب وشبكة الإنترنيت طفرة نوعية في أساليب ووسائل الصراع والرد والهجوم، فقديما كانت التحركات والقرارات وردات الفعل تتسم بالبطء والتأخر وعدم الدقة خلافا لردود الفعل الفورية والدقيقة اليوم، والتي تستغرق أقل من دقائق وبشكل أكثر ليونة ونعومة وأكثر خطرا وأشد قوة .

ومع تصاعد دور العامل التكنولوجي وتسارع وتيرة التحول العالمي نحو بناء مجتمع المعلومات والاندماج في البنية الكونية للمعلومات وتكثيف الاعتماد على أدوات التكنولوجيا والاتصال في مختلف مناحي الحياة أدركت البشرية ضرورة التأمين عليها لأن تداولها وإدارتها إلكترونيا خاصة ضمن هذا الترابط الذي خلقته شبكة الإنترنيت أصبح خطرا يهدد أمن الدول وشعوبها.

على الرغم من الميزات التي وفرتها ثورة المعلومات للمجتمعات الإنسانية إلى أن هذا لم يمنع أن تفرز معها نوعا جديدا من التهديدات التي أصبح على الفاعلين الدوليين العمل على مجابهتها، خاصة وأن بعض الفواعل قد استغلت هذه الثورة المعلوماتية وعملت على تسخيرها من أجل تحقيق مصالحها، فتحولت أدوات الإنترنيت ووسائل الاتصال ومواقع التواصل الاجتماعي إلى ساحات قتال جديدة وأدوات قتال جندتها بعض الدول من أجل خوض حروبها الإلكترونية ولعل التدخل الروسي في الانتخابات الرئاسية الأمريكية الأخيرة تعتبر الإسقاط الواقعي والفعلي لهذا النوع الجديد من حروب الجيل الجديد.

في ضوء ما تقدم يمكن توصيف النتائج التالية:

_ كان تأثير العامل التكنولوجي في التفاعلات الدولية واضحا ومتسارعا

_ تعقدت مهمة إيجاد تعريف موحد كامل وشامل لمصطلح الحروب الإلكترونية نظرا لتعدد استخداماته والتطورات المعرفية التي مر بها واستخدامه من الباحثين بدلالة عدد غير محدود من المفاهيم المقاربة

_ يمكن التمييز بين صورتين من الحروب الإلكترونية تقليدية ارتبطت بعمليات التشويش الإلكتروني وكان استعمالها في ميدان القتال، وأخرى حديثة ارتبطت بظهور الحواسيب وشبكة الانترنيت ميدانها هو الفضاء الإلكتروني.

_ اكتسبت الدول بفعل هذا النوع من الحروب ميزة نسبية كونها غير مكلفة ماديا ولا يصاحبها خسائر بشرية إلا أنه يمكن أن تحقق نتائج أكبر من تلك التي تحققها نظيرتها التقليدية

_ أصبح الفضاء الإلكتروني ساحة جديدة للصراع الدولي خاصة في ظل تغير أنماط القوة وظهور القوة الإلكترونية والتي تتباين طرق استخدامها بين نمط القوة الناعمة ونمط القوة الصلبة نمط القوة الصلبة: من خلال استخدام الفضاء الإلكتروني في أعمال تدميرية وتخريبية مثل تدمير الأنظمة المعلوماتية والشبكات لمناطق حيوية بما يهدد أمن الأفراد والدول

نمط القوة الناعمة: من خلال دعم دور الفضاء الإلكتروني من خلال التأثير في الرأي العام والعمليات النفسية وتكوين التحالفات الدولية في عملية الاستخبارات الدولية من خلال توفيره للمعلومات والتي لا تقتصر على وجهة نظر الجهات الرسمية وانما أأيضا يمتد لدور الأفراد في انتاج المعلومات مع قدرته على التأثير على أفكار الأفراد من خلال نشر المعلومات والأفكار.

_ أثر انتقال الصراع الدولي إلى الفضاء الإلكتروني على مفهوم الأمن القومي وبالتالي وجدت الدول نفسها أمام نوع جديد من التهديدات وفرض عليها تبني استراتيجيات دفاعية شأنها تقويض خطر الحروب الإلكترونية خاصة في ظل امتلاك لبعض الفواعل الدولية القدرة الهجومية في المجال الإلكتروني.

_ انتقلت فعاليات الحرب الباردة بين الولايات المتحدة وروسيا إلى مجال الفضاء الإلكتروني حيث اعتبر البعض من المحللين بأن حادثة التدخل الروسي في الانتخابات الأمريكية2016 كان بمثابة إعلان عن حرب باردة جديدة انتقلت ساحتها إلى جدران العالم الافتراضي كونها تجنب الطرفين التصادم المباشر في الوقت الذي يحقق فيه هذا النوع من الصراع مصالح كل طرف.

_ يصعب التنبؤ بمستقبل هذا النوع من الحروب نظرا لتسارع وتيرة التغيرات والتطورات في المجال التكنولوجي.

التوصيات:

_ ضرورة الاتفاق حول تعريف موحد لمفهوم الحروب الإلكترونية

_ على الدول التفطن إلى هذا النوع الجديد من التهديدات

_ يجب على الدول أن تتعاون من أجل الحد من مخاطر التهديدات الإلكترونية

_ضرورة عقد اتفاقيات ملزمة من شأنها الحد من انتشار السلاح الإلكتروني

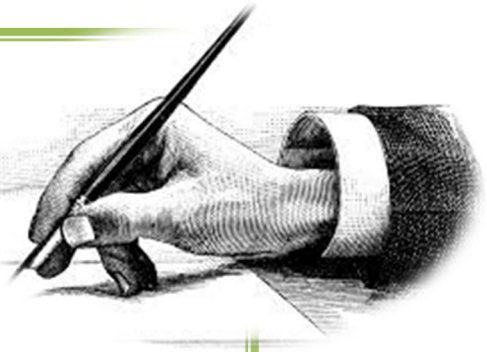
العمل على إنشاء منظمات أو هيئات تعنى بمسؤولية تنظيم الفضاء الإلكتروني ذات قرارات ملزمة، تكون لها من الصلاحيات ما يمكنها من معاقبة الأطراف التي ثبت قيامها بأعمال عدائية

_ضرورة بناء جيوش تعنى بمهام الدفاع في الفضاء الإلكتروني.

_محاولة تقويض من صلاحيات الشركات المتعددة الجنسيات خاصة منها تلك العاملة في مجال تكنولوجيا المعلومات والتي تعاظم دورها وأصبحت ذات تأثير كبير في هذا المجال.

_تشجيع تبادل الخبرات في مجال تكنولوجيا المعلومات بين الدول المتقدمة ودول العالم الثالث.

_تنظيم مؤتمرات وندوات علمية في الجامعات ومراكز البحوث في مختلف دول العالم تضم خبراء وباحثين ومختصين من مختلف التخصصات لدراسة المشكلة واقتراح الحلول الناجعة لمعالجتها.



قائمة المراجع

قائمة المراجع المعتمدة:

أولا/باللغة العربية

01_ الكتب:

1. الأثرم صلاح الدين. الحرب الإلكترونية من الحرب العالمية الأولى إلى حرب النجوم. ط2. سوريا. دار الطلاسم الدراسات و الترجمة والنشر.
2. أحمد أشرف السعيد. القرصنة الإلكترونية. القاهرة. دار النهضة العربية .2013.
3. البصيلي جاسم محمد. الحرب الإلكترونية أسسها وأثرها في الحروب. ط2. بيروت. المؤسسة العربية للنشر. 1989.
4. جعيجع عبد الوهاب. الأمن المعلوماتي وإدارة العلاقات الدولية. الجزائر. دار الخلدونية. 2017.
5. خليفة إيهاب. القوة الإلكترونية كيف يمكن أن تدير الدول شؤونها في عصر الإنترنيت. القاهرة. العربي للنشر.2017.
6. خليفة إيهاب. القوة الإلكترونية وأبعاد التحول في خصائص القوة. مصر. مكتبة الإسكندرية.2014.
7. خليفة إيهاب. مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي.مصر. العربي للنشر والتوزيع.2017.
8. خليل عادل علي . الحرب الإلكترونية من الحرب العالمية الأولى إلى حرب الخليج. مصر. دار الهلال.
9. شفيق نوران. أثر التهديدات الإلكترونية على العلاقات الدولية دراسة في أبعاد الأمن الإلكتروني. المكتب العربي للمعارف.2018.
10. عبده أحمد جلال محمود. صراع القوة المدنية وأثره على السياسة الخارجية التركي في منطقة الشرق الأوسط. القاهرة. المكتب العربي للمعارف .
11. كلارك أي ريتشارد. كنيك روبرت كي. حرب الفضاء الإلكتروني التهديد التالي للأمن القومي وكيفية التعامل معه.ط1. الإمارات. مركز الإمارات للبحوث والدراسات الإستراتيجية . 2012.

02_القواميس والمعاجم:

1. البستاني بطرس. بيروت. مكتبة الناشرون.1979.
2. الفيومي أحمد بن محمد. المصباح المنير في غرب الشرح الكبير للرافعي. ج1. بيروت. المكتبة العلمية.

03_المجلات والدوريات:

1. جواد إنمار موسى. حرب الفضاء الإلكتروني المفهوم–الأدوات والتطبيقات. مجلة العلوم القانونية والسياسية. ع:02. 2016.
2. عبد اللطيف سامر مؤيد. الحرب في الفضاء الرقمي رؤية مستقبلية. العراق. مجلة رسالة الحقوق.ع:02.مركز الدراسات القانونية والدستورية.2015.
3. الفتلاوي أحمد أويس. الهجمات السيبرانية : مفهومها المسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية.ع:04. 2016.
4. محمود سعاد. دورة القوة: دينامية الانتقال من الصلبة إلى الناعمة إلى الافتراضية. السياسة الدولية. ملحق اتجاهات نظرية. ع:188.

04_ الرسائل والمذكرات الجامعية:

1. أحمد مجاهد فخر الدين قاسم. ترجمة الصفحات(01–66) من كتاب الأمن الإلكتروني والحرب الإلكترونية ما ينبغي أن يعرفه كل شخص. مذكرة ماجستير(غير منشورة). كلية الدراسات العليا. جامعة السودان للعلوم و التكنولوجيا. السودان .
2. جلعود وليد غسان سعيد. الحرب الإلكترونية في الصراع العربي الإسرائيلي. مذكرة ماجستير غير منشورة. كلية الدراسات العليا. جامعة النجاح الوطنية. فلسطين. 2013.
3. قتلوني مصعب. دور مواقع التواصل الاجتماعي "الفايسبوك" في عملية التغيير السياسي مصر أنموذجا. رسالة ماجستير(غير منشورة). كلية الدراسات العليا. جامعة النجاح. فلسطين. 2012.

4. مهني محمد. تأثير الإرهاب الإلكتروني على تغير مفهوم القوة في العلاقات الدولية _ توظيف المنظمات الإرهابية لمواقع التواصل الاجتماعي-أنموذجا-. مذكرة ماستر (غير منشورة).قسم العلوم السياسية والعلاقات الدولية. كلية الحقوق. جامعة المسيلة.2017.

المواقع الإلكترونية:

1. كريم حميدة. الحرب الإلكترونية.الألوكة الثقافية.2012/03/20.

.2019/05/05. http// www.alukah.net.

2. عادل عبد صادق. أنماط "الحرب السيبرانية "وتداعياتها على الأمن العالمي.

.2019/05/28.http://ali;brqtaur.com.

3. عادل عبد صادق. الحروب السيبرانية: تصاعد القدرات والتحديات للأمن العالمي.المركز العربي لأبحاث الفضاء الإليكتروني. 2017/03/12.

.2019/05/12. http://accronline.com.

4. منصور زغيب. تجدد الصراع الأمريكي الروسي في ضوء الأزمات المتجددة. مجلة الدفاع الوطني.ع:99. 2014.

05/05/2019. http:www.leberny.gov.lb/ ar/ com.

5. أحمد يوسف الجميلي. القدرات السيبرانية سلاح روسيا ضد الخصوم. مركز صنع السياسات للدراسات الدولية الإستراتيجية. 2018/06/19.

.2019/05/26http://www.making policies.org.

6.عمرو عبد العاطي. إستراتيجية أمريكية هجومية ضد التهديدات السيبرانية المركز المصري للفكر والدراسات الإستراتيجية.

.2019/05/23. http:www. Ecsstudies.com.2018/10/31

7.عبد الغفار عفيفي الدويك فجوة القوة السيبرانية والحاجة إلى مبلدرة أممية ، الحياة، 2018/02/12.

.2019/05/25 .http://www.qlhqyqt.com.

8.عمرو صبحي. تكتيك الدرع والسيف في استخدام القوة السيبرانية. المركز العربي للبحوث والدراسات.2018/04/26.

http://www.qcrrseg.org/40716. 02/06/2019 .

الملخص:

عرفت العلاقات الدولية تطورا بارزا من حيث الفواعل والمواضيع و الأدوات المستخدمة في ادارة تفاعلاتها، وفي ظل هذه القفزة النوعية التي تزامنت مع ثورة تكنولوجية ورقمية مذهلة اقتحمت شتى أنماط الحياة لإنسانية والتفاعلات الدولية ظهر نوع جديد من التهديدات التي أصبحت تواجه الدولة القومية والمتمثلة في الصراعات الإلكترونية.

فتبلورت ظاهرة الحروب الإلكترونية بوصفها شكلا جديدا من أشكال التفاعلات الدولية، وصورة جديدة من صور الحروب ما أدى الى ظهور القوة الإلكترونية كشكل جديد من أشكال القوة فسعت الدول الكبرى وعلى رأسها الولايات المتحدة الأمريكية وروسيا الاتحادية للاستفادة من الميزات التي يوفرها الفضاء الإلكتروني، وبالتالي تم نقل ذلك الصراع الأزلي الى جدران الفضاء الافتراضي وكانت حادثة التدخل الروسي في الانتخابات الرئاسية الأمريكية الأخيرة 2016 أوضح صورة للحروب الإلكترونية وتجسيدا واقعيا لهّذا النوع من الحروب.

Abstract:

International relations have witnessed a remarkable development in terms of the actors, topics and tools used to manage their interactions With this qualitative leap that coincided with a spectacular technological and digital revolution that has penetrated the various lifestyles of humanity and international interactions, a new type of threats has come to face the nation-state of electronic conflicts

The phenomenon of cyber warfare crystallized as a new form of international interaction, and a new form of warfare, which led to the emergence of cyber power as a new form of power expanded the major countries, led by the United States of America and the Russian Federation to take advantage of the advantages provided by cyber-lobes, and therefore was transferred The timeless conflict to the walls of virtual space The Russian intervention in the last US presidential election 2016 was the clearest image of cyber warfare and a realistic embodiment of this kind of war.