مجلّة نصف سنوية محكّمة تصدر عن قسم الدراسات السياسية والاستراتيجية في بيت الحكمة ـ بغداد
رقم إيداع مجلة دراسات سياسية وأستراتيجية في دار الكتب والوثائق ٦٧٨ لسنة ٢٠٠٩
رقم الإيداع الدولي ISSN 2223-9464
Info@baytalhikma.iq

تداعيات الحروب السيبراني على الامن والسلم الدولي نماذج مختارة

الباحث محمد صالح فرحان *

المقدمة

أدت المتغيرات التي أحدثتها الثورة المعلوماتية والتكنولوجية الى التحول من مفهوم الحرب في العلاقات الدولية بمدلوله التقليدي الى مفهوم الحرب الإلكترونية اذ أصبح الصراع الإلكتروني اليوم أحد اوجه الصراع الذي يهدد الأمن الدولي، عن طريق سعي الكثير من الدول للدخول في مجال الفضاء السيبراني اذ تناولت الكثير من الدول هذا المجال كميدان للصراعات الدولية، ولقد كانت للتطورات الحاصلة في حقل التكنولوجيا الرقمية أثراً واضحاً على مفهوم استخدامات القوة في الصراع الدولي لاسيما في مجال الحروب الالكترونية، اذ تحول مفهوم الحروب والتهديدات من المفهوم التقليدي الى مستوى الحروب والتهديدات الألكترونية عن طريق استخدام القوة والقدرات الالكترونية، والذي بدوره ادى الى التنافس والصراع الذي يشهده العالم اليوم لاسيما الصراع الحاصل ما بين الولايات المتحدة الأمريكية والصين، اذ يسعى الأثنين الى استهداف قدرات أحداهما الاخر عن طريق السباق التكنولوجي الذي تشهده كلتا الدولتين، كذلك الصراع الحالي بين كل من روسيا الاتحادية واوكرانيا الذي يمثل احدث صورة للحرب السيبرانية في القرن الحادي والعشرين.

اهمية البحث: يكتسب الموضوع اهميته من تسارع التطورات التكنولوجية على كافة الأصعدة وفي مختلف المجالات مما ادى الى تسارع الدول في مواكبة التطورات التكنولوجية والتي بدورها ادت الى التحول في سلوك الحرب من التقليدي الى السيبراني المتضمن كل وسائل التكنلوجيا الحديثة وتوظيفها لتحقيق لغايات التي تسعى الدول الى تحقيقها عن طرق الفضاء السيبراني، لذا برزت اهمية البحث عن طريق تحليل الحروب السيبرانية وبيان نماذج من تلك الحروب.

Medm٠٨٢٦٥@gmail.com

Semi-annual Quarterly journal issued byPolitical and Strategic Studies In Bayt Al-Hikma Baghdad
No.of deposit at Political and Strategic Studies(678)2009
ISSN.2223-9464
Info@baytalhikma.iq

اشكالية البحث: تكمن مشكلة البحث في تساؤل محوري مفاده في ضل التطورات التكنولوجية المتسارعة برز نوع من الحروب الحديثة والي يطلق عليه الحروب السيبرانية، ماذا تعني وكيف اثرت في الدول الكبرى لتصبح انموذج لها.**وعن طريق هذا التساؤل تنطرح عدة تساؤلات فرعية كالاتي:**

ماذا يقصد بالحرب السيبرانية؟

ماهي طبيعة واليات الحرب السيبرانية؟

ماهي تداعيات الحروب السيبرانية الى الأمن والسلم الدولي؟

ما طبيعة الحرب السيبرانية بين القوى الكبرى؟

فرضية البحث: ينطلق البحث من فرضية مفادها شهد العالم تغيرات جوهرية في ظل التطورات التكنولوجية الحديثة، اثرت في جميع المجالات وعلى كافة الاصعدة ومن ضمنها الحروب التي تحولت من الحروب التقليدية الى الحروب السيبرانية لمواكبة تلك التطورات والتي ادت الى تسارع الدول الكبرى في النظام الدولي على امتلاك مقوماتها حتى اصبحت نماذج لتلك الحروب والذي يبرهن لنا الصورة التي نشهدها اليوم للعالم عن الحروب والصراعات السيبرانية.

منهجية البحث: تم الاعتماد الى المنهج التحليلي ومن ثم المنهج الاستقرائي في تحليل نماذج الحرب وكذلك المنهج التاريخ في تتبع تطور الحرب السيبرانية.

هيكلية البحث: تم تقسيم البحث الى مقدمة وثلاث مباحث في المبحث الاول نتطرق الى مفهوم الحرب السيبرانية والياتها، اما جاء في المبحث الثاني تاثيرها على الامن والسلم الدوليتن، وتناولنا في المبحث الثالث النماذج المختارة للبحث ومن ثم الخاتمة.

المبحث الاول: مفهوم الحرب السيبرانية

خلال هذا المبحث نحاول بيان المقصود بالحرب السيبرانية بشكل واضح يمكننا من تمييزها عن غيرها من المفاهيم المرتبطة بالاستخدام غير المشروع للفضاء السيبراني، ثم نبين الآليات التي تدار بها، وذلك على النحو التالي:

المطلب الأول: تعريف الحرب السيبرانية:

يعد منع استخدام القوة في العلاقات الدولية من المبادئ الرئيسة الراسخة في القانون الدولي، والتي تشكل التزاماً أساسياً يقع على عاتق كل الدول، تمكنت من إرسائه بعدما أنهكتها الحروب والصراعات، وكلفتها أرواحاً وأموالاً باهظة. ولقد حرص ميثاق الأمم المتحدة على إقرار هذا المبدأ بنصه في الفقرة (٤) من مادته (٢) على أن « يمتنع أعضاء الهيئة جميعاً في علاقاتهم الدولية عن التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأي دولة أو على وجه آخر لا يتفق ومقاصد الأمم المتحدة. « كما أكدته العديد من الإعلانات والمواثيق الدولية العالمية منها والإقليمية وحتى في تلك الأحوال التي تجيز فيها أحكام القانون الدولي اللجوء إلى القوة يكون ذلك بشروط وضوابط وفي حالات محددة[1].

مجلّة نصف سنوية محكّمة تصدر عن قسم الدراسات السياسية والاستراتيجية في بيت الحكمة - بغداد
رقم إيداع مجلة دراسات سياسية وأستراتيجية في دار الكتب والوثائق ٦٧٨ لسنة ٢٠٠٩
رقم الإيداع الدولي ISSN 2223-9464
Info@baytalhikma.iq

وعلى الرغم من استقرار تحريم استخدام القوة كقاعدة قانونية دولية آمرة، إلا أن ذلك لم يمنع نشوب حروب ونزاعات مسلحة، دفعت الدول لتطوير قدراتها العسكرية وتنويع أسلحتها لتجنب تعرضها لأي اعتداء، وكان للتطور العلمي والتكنولوجي الهائل الذي تحقق أثر كبير في استحداث أسلحة، وفي اكتشاف طرق وأساليب تشن وتدار عن طريقها الحروب . وبعد تسخير الفضاء السيبراني في المجال العسكري تطبيقاً للاستفادة من هذه التطورات، والتي مكنت من إدارة العمليات والهجمات أثناء النزاعات بوسائل وآليات تعتمد على تقنيات مغايرة تماماً لوسائل الحرب التقليدية، حتى أصبحت الحرب السيبرانية من سمات الحروب المعاصرة . والفضاء السيبراني هو « مجال مادي وغير مادي يشمل مجموعة من العناصر وهي: أجهزة الكمبيوتر، وأنظمة الشبكات والبرمجيات، وحوسبة المعلومات، ونقل وتخزين البيانات ومستخدمو كل هذه العناصر[٢].

ونظراً لأن الفضاء السيبراني مجال مفتوح تصعب السيطرة عليه، تزايدت المخاطر التي تنتج عن استعماله، وتنوعت التهديدات المرتبطة به من جرائم إلكترونية، وهجمات سيبرانية مرورا بالتجسس السيبراني، والإرهاب الإلكتروني، والقرصنة السيبرانية، بل أصبح هذا الفضاء أيضا ساحة جديدة للحرب ، توصف العمليات العسكرية التي تدار فيه بالحرب السيبرانية، كما هو شأن الحرب البرية والبحرية والجوية، وهو ما دفع الباحثين والخبراء في القانون الدولي، والدول والمنظمات الدولية إلى الاهتمام بهذا النوع المتطور للحروب، ومحاولة ضبطها وفقا لأحكام القانون الدولي.

وبداية تجدر الإشارة إلى أن مصطلح الحرب السيبرانية له مدلول محدد يختلف عن مصطلح الهجوم السيبراني أو الهجمات السيبرانية التي تشنها دولة ضد الأنظمة الإلكترونية لدولة أخرى، اذ يقصد بالهجوم السيبراني تلك الإجراءات التي تتخذها الدولة من أجل الهجوم على نظم المعلومات للعدو لهدف التأثير والإضرار فيها والدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة [٣].

ويعرف أيضاً بأنه استخدام أنشطة متعمدة لتغيير أو إفساد أو خداع أو إضعاف أو تدمير أنظمة الحاسوب، أو شبكات الحاسوب للخصم أو المعلومات، والبرامج المدرجة في هذه الأنظمة، أو الشبكات أو ترسل من خلالها. [٤] أما الحرب السيبرانية فلم تتضمن المواثيق الدولية سواء تلك التي شكلت قواعد القانون الدولي الأساسية، أو تلك المتعلقة بالقانون الدولي الإنساني على تعريف للعمليات السيبرانية، أو الحرب السيبرانية، أو القتال السيبراني، مما جعل الفقه الدولي يجتهد في محاولة للوقوف على معنى واضح لها، وهو ما أدى إلى تعدد وتنوع التعريفات بتعدد وكثرة الدراسات التي تناولتها، فيعرفها البعض بأنها « أساليب الحرب ووسائلها التي تعتمد على تكنولوجيا المعلومات وتستخدم في سياق نزاع مسلح، أو هي الهجمات والعمليات التي ترتكب ضد أو بواسطة شبكات الحواسيب وأنظمة البيانات بين الدول أو الجماعات المسلحة المنظمة في سياق نزاع مسلح، أو سياسات الردع المتبادل.[٥]

Semi-annual Quarterly journal issued byPolitical and Strategic Studies In Bayt Al-Hikma Baghdad
No.of deposit at Political and Strategic Studies(678)2009
ISSN.2223-9464
Info@baytalhikma.iq

وعرفها دليل «تالين» المتعلق بتطبيقات القانون الدولي في مجالات الصراع والحروب بأنها « كل العمليات السيبرانية سواء كانت دفاعية أو هجومية، والتي يعتقد أنها قد تسبب إصابات أو وفيات للبشر ، أو تلف وضرر للأشياء المادية »[٦].

ومما سبق يتضح أن مفهوم الهجوم السيبراني أوسع من مفهوم الحرب السيبرانية فالهجوم السيبراني قد يقع في أي وقت وقد يكون شرارة البدء للحرب أو إعلاناً لها، لكنه إذا وقع أثناء النزاع المسلح يوصف بأنه حرب سيبرانية، باعتباره جزء من حرب قائمة. ولهذا التمييز إذا ما أخذنا به أهمية كبيرة في البحث عن طبيعة الحروب السيبرانية في إطار قواعد القانون الدولي، فهو من ناحية يوجب التطرق إلى تكييف الحرب السيبرانية وفقا لمبدأ حظر استخدام القوة في العلاقات الدولية، ومن ناحية أخرى سيمكننا من المطالبة بتطبيق قواعد القانون الدولي الإنساني كونها القواعد الواجبة التطبيق عند وقوع الحرب.

المطلب الثاني: طبيعة وآليات الحرب السيبرانية

تتميز الحرب السيبرانية عن الحرب التقليدية، في أن المفهوم التقليدي للحرب، ينطوي على استخدام الجيوش النظامية ويسبقها إعلان واضح لحالة الحرب وميدان قتال محدد، بينما تبدو هجمات الفضاء الإلكتروني غير محددة المجال وغامضة الأهداف، كونها تتحرك عبر شبكات المعلومات والاتصالات المتعدية للحدود الدولية، إضافة إلى اعتمادها على ما يمكن وصفه بأسلحة إلكترونية جديدة تلاءم طبيعة السباق الإلكتروني لعصر المعلومات، حيث يتم توجيهها ضد المنشئات الحيوية أو دسها عن طريق عملاء لأجهزة الاستخبارات، وعليه فإن أحد معايير التمييز بين الحرب السيبرانية والحرب التقليدية يمكن أن يكون بالاستناد إلى طبيعة السلاح المستخدم[٧].

ومن أمثلة استخدام العمليات السيبرانية أثناء النزاعات التجسس، وتحديد الأهداف، والعمليات المعلوماتية الرامية إلى التأثير على معنويات العدو وإرادته إزاء القتال، وقطع نظم اتصالات العدو أو تضليلها أو التشويش عليها ابتغاء إعاقة تنسيق القوات، والعمليات السيبرانية الرامية إلى دعم العمليات الحركية كتعطيل محطات الرادار العسكرية للعدو لدعم الضربات الجوية، ومفهوم الحرب السيبرانية لا يستهدف القدرات والأنظمة العسكرية وحسب، ولكنه ايضا يستهدف البنية التحتية الحيوية للمجتمع، وتشمل الأسلحة السيبرانية الفيروسات والديدان الحاسوبية وعمليات جمع البيانات السيبرانية، وأجهزة تشويش اتصالات البيانات اللاسلكية، وبرمجيات الحاسوبية المزيفة المشبوهة وأسلحة النبض الكهرمغناطيسي، وأدوات استطلاعات الحاسوب والشبكات والقنابل الزمنية الطروادية المدمجة[٨].

ويرى البعض أنه يمكن تحديد ثلاثة مستويات رئيسة للحرب السيبرانية أو الهجمات السيبرانية

المستوى الأول: ويتمثل في تلك العمليات المصاحبة للحروب التقليدية كمهاجمة نظام الدفاع الجوي، والذي يؤدي إلى خسائر إستراتيجية واسعة النطاق نتيجة لأهمية الدفاع الجوي بالنسبة للدول.

مجلّة نصف سنوية محكّمة تصدر عن قسم الدراسات السياسية والاستراتيجية في بيت الحكمة - بغداد
رقم إيداع مجلة دراسات سياسية وأستراتيجية في دار الكتب والوثائق ٦٧٨ لسنة ٢٠٠٩
رقم الإيداع الدولي ISSN 2223-9464
Info@baytalhikma.iq

المستوى الثاني: فيتمثل في الحرب الإلكترونية المحدودة، والتي تتعرض فيها البنية التحتية والأهداف المدنية للهجمات السيبرانية.

المستوى الثالث: يتمثل في الحرب الإلكترونية غير المحدودة والتي يسعى من خلالها القائم بالهجوم إلى تعظيم الآثار التدميرية للبنية التحتية، حيث يؤثر سلباً في البناء الاجتماعي للدولة ، كمهاجمة أسواق المال، وخدمات الطوارئ، والأنظمة الإلكترونية الخاصة بمولدات الطاقة، وغيرها من الأهداف التي يترتب عليها آثار تدميرية واسعة النطاق، ويكون الهدف من هذا النوع من الحروب هو توسيع نطاق الخسائر المادية قدر الإمكان [٩].

لقد أضحى استخدام العمليات السيبرانية أثناء النزاع المسلح سمة واقعية من سمات النزاعات المسلحة، ويرى البعض أن أول مرة نفذت فيها الهجمات السيبرانية، كانت في حرب كوسوفو عام ١٩٩٩، من خلال استهداف سلاح الجو التابع لحلف شمال الأطلسي «الناتو الشبكات الهاتف في يوغسلافيا السابقة.

وأقرت بعض الدول علناً بأنها أجرت عمليات سيبرانية في نزاعات مسلحة جارية. فقد كشفت الولايات المتحدة، والمملكة المتحدة، وأستراليا على وجه الخصوص أنها لجأت إلى العمليات السيبرانية في نزاعها ضد تنظيم الدولة الإسلامية، ونشرت تقارير تشير إلى أن إسرائيل استخدمت عمليات سيبرانية ضد حماس، وأثرت العمليات السيبرانية على بلدان أخرى مشاركة في نزاعات مسلحة، مثل جورجيا في عام ٢٠٠٨ وأوكرانيا في الفترة بين ٢٠١٥ - ٢٠١٧[١٠].

وأكدت التقارير الاستخبارية الأمريكية في عام ٢٠٠٩، بقيام بعض من المجموعات المسلحة في أثناء احتلال العراق باختراق مواقع الكترونية كانت تستقبل بيانات غاية في الأهمية تنقلها الطائرات بدون طيار لتحديد تحركات هذه المجموعات، ما ساعد الأخيرة في مراقبة التحركات العسكرية الأمريكية لموجهة ضدهم [١١].

وفي النزاع الروسي الأوكراني بدأت الهجمات الألكترونية الروسية في وقت مبكر من عام٢٠١٤ بهدف تدمير البنية التحتية والبيانات او اتلافها، وحاولت القيام بذلك مرة اخرى في عام ٢٠٢٢، بقصد خلق لفوضى والتغلب على الدفاعات الأوكرانية وسعت روسيا الى تعطيل الخدمات وتثبيت برامج ضارة مدمرة على الشبكات الاوكرانية مستهدفة مواقع الحكومة الاوكرانية ومقدمي خدمات الطاقة والاتصالات والمؤسسات المالية ووسلئل الاعلام[١٢].

المبحث الثاني: تداعيات الحروب السيبراني على الأمن والسلم الدوليين

أدى التطور التكنولوجي، كانتشار الإنترنت والحواسيب والأجهزة النقالة، وتوافر الحزمة العريضة للإنترنت عبر الأجهزة النقالة وتدني كلفتها، إلى ارتفاع أعداد مستخدمي الإنترنت وتزايد اعتماد الدول على هذه التكنولوجيات في التنمية الاقتصادية والاجتماعية . إلا أن الانفتاح الذي يميز شبكة الإنترنت، والفضاء السيبراني

Semi-annual Quarterly journal issued byPolitical and Strategic Studies In Bayt Al-Hikma Baghdad
No.of deposit at Political and Strategic Studies(678)2009
ISSN.2223-9464
Info@baytalhikma.iq

عموماً، جعلها عرضة للتعديات والأنشطة الغير سلمية، فأصبح المستخدمين للفضاء السيبراني من الدول وغير الدول عرضة للانتهاكات والتهديد لمنظومتها الإلكترونية، إذ لا يمكن لأي حكومة ، أو إدارة سواء أكانت من العالم الثالث، او في الدول الأكثر تقدماً، أن تنأى بنفسها عن الخطر الذي يتمثل باختراق الشبكات، وتهديد أمنها ومصالحها.

مارسَ الفضاء السيبراني (الإلكتروني)، ومنذ ظهوره، دوراً اساسياً في تعظيم القوة أو الاستحواذ على عناصرها الاساسية في العلاقات الدولية، اذ أصبح التفوق في ذلك المجال عنصراً حيوياً في تنفيذ عمليات ذات فاعلية على الأرض، والبحر، والجو والفضاء، واعتماد القدرة والتفوق في الفضاء الإلكتروني على نظم التحكم والسيطرة التكنولوجية. أدى ذلك إلى تغيير ليس في مفهوم الأمن القومي للدولة فحسب، بل لمفهوم القوة الوطنية للدولة ايضاً، إذ بات بالإمكان تعريفها على أنها مجموعة الوسائل، والطاقات والإمكانيات المادية وغير المادية المنظورة وغير المنظورة التي تمتلكها الدولة، ويستخدمها صانع القرار في فعل مؤثر يحقق مصالح الدولة، وتؤثر في سلوك الوحدات السياسية الأخرى[١٣].

ينظر ذوي الاختصاص إلى الحرب الإلكترونية على أنها حرب العصر الحقيقية، مسارها الرئيس الشبكات الرقمية والإلكترونية، كذلك الوسائل التكنولوجية الأخرى، والأدوات الإعلامية، وكل ما يتعلق بعالم المعلوماتية والحداثة والغاية الرئيسية لهذه الحرب هي الأضرار النفسية والمعنوية بالدرجة الأولى، ثم تتبعها الأضرار المادية، وهي حرب ناعمة صامتة مظلمة بعيدة عن الوسائل الحربية الخشنة، لكنها لا تمانع في امتطاء الترسانات المسلحة والعسكرية الضخمة باعتبار أن الغاية الرئيسة والنواة الأولى من ابتكار الاقمار الصناعية، والفضاء الإلكتروني كانت عسكرية بامتياز كما تم ذكره انفاً[١٤].

ويعتبر آخرون أن الحرب الإلكترونية هي امتداداً للحروب التقليدية والمادية، بحيث يتألف جندها من المدنيين والعسكريين في آن واحد . كما أنها حرب أدمغة بالدرجة الأولى، كونها تستهدف في المقام الأول تدمير البنية العلمية والمعلوماتية للهدف، وتأخذ أشكالاً عدة؛ كشكل الاتصالات بين الجيوش وقياداتها، وإضعاف شبكات النقل والإمدادات اللوجستية، وضرب المعلومات الاقتصادية، وإحراج الساسة، والعبث بالمحتوى التقني والرقمي وغيرها[١٥].

إذن الحرب السيبرانية هي حرب تتخذ من الفضاء الإلكتروني ساحة وميدان لتفاعلاتها وقضاياها ومصالحها، وتستمد هذه القضايا والمصالح من الفضاء العام التقليدي . وعلى وفق ذلك، ومنذ اجتياح الإنترنيت العالم وما تبعه من مخلفات واسعة، أصبح هاجساً للدول الكبرى، وهذا يعزى لارتباطه بمستقبل الاستقرار العالمي، إذ صار له رده فعل خطيرة على النظام العالمي، لذلك يشهد العالم الآن تسابق في فهم التحركات الاساسية للنظام الإلكتروني والآثار المترتبة منه. ومن ثم، بدأت الولايات المتحدة وروسا، والصين، وإيران، وغيرها من الدول المتطورة بتشكيل خلايا غير معلنه ضمن تشكيلاتها العسكرية والأمنية مهمتها القيام بهجوم أو صد هجوم إلكتروني على بنيتها

مجلّة نصف سنوية محكّمة تصدر عن قسم الدراسات السياسية والاستراتيجية في بيت الحكمة - بغداد
رقم إيداع مجلة دراسات سياسية وأستراتيجية في دار الكتب والوثائق ٦٧٨ لسنة ٢٠٠٩
رقم الإيداع الدولي ISSN 2223-9464
Info@baytalhikma.iq

حـرب حقيقية قد تقـع عبر توظيـف المعلومات والاتصـالات في ادية للدولة أو سـرقة معلومات مخابراتية[١٦].

وعند التمعن في ما يشـهده النظام العالمي بشـكل عام، والأمن والسلم الدوليين بشكل خاص، لتضح وبشـكل جلي أن العالم منقسم إلى كتلتين كبيرتين في اطار التحالفات الاسـتراتيجية؛ الأول - بقيادة الولايـات المتحدة وبريطانيا واسـرائيل، والثاني بقيادة روسـيا والصين وإيران، هـذا الوضع هو اشـبه بالوضع الذي سبق الحرب العالمية الأولى والثانيـة، والتـي كان الفضـاء العـام التقليـدي ميدانهما الرئيس، لكن هذه المرة وبفعل العصرنة سـيكون الميـدان الرئيس هو الفضاء السـيبراني (الإلكتروني) ويمكن تقسـيم الحرب الإلكترونية إلـى ثلاث مجالات أولهمـا - الدفاع الإلكتروني، الذي يعني بالدفاع عن انظمة وأجهزة ومعلومات الدولـة والجيـش والمجتمـع، وثانيهمـا الهجوم الإلكترونـي، وهـو المجال المختـص بالعمليات الإلكترونيـة، والتـي تهـدف للتشـويش علـى مصادر المعلومات وتدميرها وحرمان العدو من استخدامها لمصلحتهم، واخيراً - التجسس الرقمي على امكانيات وقدرات الفاعلين الآخرين.

وعليه، فقد أصبح الفضاء الإلكتروني ساحة جديدة للصراع بشكله التقليدي ولكنه ذو طابع إلكتروني يعكس النزاعات التي تخوضها الدول أو الفاعلين مـن غير الـدول على خلفيـات دينيـة أو عرقية أو إيديولوجيـة أو اقتصادية أو سياسـية، ويتمدد الصـراع الإلكترونـي بداخل شـبكات الاتصال والمعلومـات متجـاوزا الحدود التقليدية وسـيادة الـدول، ويؤثر ذلك في امتداد مجاله وتداعياته أو آثاره، ويخلق حالة من عدم الثقة بين الدول.

ونظرا لارتباط الشبكات المحلية للدول بالشبكات العالمية للانترنت، وبمـا ان هناك ضعف وثغرة في انظمـة التشـغيل الالكترونية، يصبـح انتقال الصراعات الى حروب سيبرانية بين الدول قائما، وخيـر دليل على ذلك هي الاختراقات الألكترونية المتبادلة بين الدول والفاعلين الدوليين في الاونة الاخيرة.

فضـلاً عن ذلـك، الاختراق الذي اصاب شـركة (SONY) الامريكيـة عام ٢٠١٤، وكان الهدف من ذلـك منع إطـلاق فيلـم "The Interview" من إنتاج الشـركة، وهو فيلم كوميدي يدور حول مؤامرة لاغتيال الزعيم الكوري الشمالي كيم جونغ أون، إذ اتهمت بذلك كوريا الشمالية. كذلك الاتهام الموجـه إلى الصيـن، الذي مفـاده هجوم صيني الإلكتروني على مؤسسـات الـدول الاقتصادية، وبخاصة الامريكية، وسـرقة الاسـرار التجارية وتوظيفهـا لصالح صناعاتها الخاصة، مما احدث نوع من الحساسية الدولية .

ايضاً ما حصل لقطر من هجوم سـيبراني، حيث شـنت الـدول الرباعيـة السـعودية والإمـارات والبحرين ومصر في بداية حصارها لقطر هجوماً سيبرانياً لفقت به خطاباً مفبركاً لأمير البلاد الشيخ تميم بن حمد آل ثاني استعملته تبريراً لإجراءاتها العدائية[١٧].

ونظـراً، للإضـرار الخطيـرة التـي قد تسـببها الحـرب الإلكترونية على كل مـن الامن القومي والعسـكري، والاقتصـادي والاجتماعي، ويهدد البنيـة التحتيـة والحرجة للدول، وأسـواق المال

Semi-annual Quarterly journal issued byPolitical and Strategic Studies In Bayt Al-Hikma Baghdad
No.of deposit at Political and Strategic Studies(678)2009
ISSN.2223-9464
Info@baytalhikma.iq

والقطاعات المصرفية، والسلم الدولي والمنشآت النووية، والمؤسسات الصحية وقطاعات النقل بكل انواعها البرية والبحرية والجوية، ورفاه الشعوب. وغياب الاطارين التشريعي والتنظيمي الحاكم للفضاء السيبراني. اتجهت معظم الدول المتقدمة، الى اقرار سياسات وقائية ودفاعية ضد الهجمات السيبرانية، وخصصت الدول الكبرى مثل الولايات المتحدة الاميركية، واستراليا، والمملكة المتحدة واسرائيل مبالغ طائلة، لإنشاء هيئات وأقسام تهتم بذلك ، ومعالجة مسائل الامن السيبراني، واستقرار الفضاء السيبراني. وليست هذه الحقيقة، سوى مؤشر، الى مدى الاهتمام الذي توليه هذه الدول، لارساء الثقة والاستقرار، كما السلامة والأمن في هذا الفضاء . فاقتصاد العالم، كما حياتنا اليومية متصلان اتصالا وثيقا بالفضاء السيبراني، والخدمات الحيوية، كما الامن والدفاع، والعلاقات الدولية، مهددة في كل لحظة، نتيجة الاختراقات والاعتداءات على الشبكة العالمية للمعلومات، وعلى الانظمة المعلوماتية، وقواعد المعلومات، ولم تتأخر الادارة الاميركية، عن استحداث قيادة عسكرية جديدة مختصة بأمن الفضاء السيبراني. وتتولى مروحة من النشاطات العسكرية، تشمل الى الحماية، والقيام بمناورات سيبرانية، سواء لتحديد مدى فاعلية الحماية، أو مدى القدرة على الرد أو للتعرف الى مكامن الضعف والتدريب على آليات الرد، ويتم ذلك في اطار استراتيجية اعدتها وزارة الدفاع في العام ٢٠١١ حول كيفية العمل في الفضاء السيبراني[١٨].

وعليه، فقد انتقل الاهتمام الذي كان مخصصاً للتجهيزات والتطويرات العسكرية التقليدية للدول إلى الاهتمام لإيجاد الوسائل الملائمة لطبيعة الخطر السيبراني والكفيلة بتداركه وردعه. هذا الامر ينذر بسباق للتسلح، وعسكرة الفضاء السيبراني، مما سيكون له الأثر في زعزعة الأمن والسلم الدوليين في المستقبل المنظور.

ثانيا: تداعيات الحروب السيبرانية على أمن الدول واستقرارها في الفضاء السيبراني

يعُد الإرهاب الإلكتروني تهديد حقيقي لأمن واستقرار الدول في مجالها السيبراني لاسيما بعد توجه معظم دول العالم نحو ما يعرف بالإدارات الإلكترونية، فقد تبلورت مصالح قومية للدول في الفضاء الإلكتروني إثر تزايد الاعتماد على ربط البني التحتية لها بذلك الفضاء في بيئة عمل تشابكية واحدة تعرف بـ «البنية التحتية القومية للمعلومات» (NII) مثل : قطاعات الطاقة، والاتصالات، والنقل والخدمات الحكومية والمالية والتجارة الإلكترونية وحتى مؤسسات الدولة الحيوية والحساسة كالمؤسسة العسكرية باتت تمتلك مواقع إلكترونية ما قد يجعلها عرض لهجوم ارهابي عن طريق اختراقها بهدف نشر الرعب وتحقيق أهدافها السياسية. ومن ثم، فأي تهديد محتمل أو هجوم على إحدى تلك المصالح أو كلها للدولة قد يشكل خطر يؤدي إلى حدوث عدم توازن استراتيجي وهو ما يكشف عن نمط جديد من التهديدات للأمن القومي للدول[١٩]، عن طريق ذلك سنحاول فهم أبرز التداعيات التي يخلفها الإرهاب السيبراني على أمن الدولة لاسيما في الفضاء السيبراني باعتبار أن هذا الأخير أصبح يعد فضاء من الفضاءات الأساسية

مجلّة نصف سنوية محكّمة تصدر عن قسم الدراسات السياسية والاستراتيجية في بيت الحكمة - بغداد
رقم إيداع مجلة دراسات سياسية وأستراتيجية في دار الكتب والوثائق ٦٧٨ لسنة ٢٠٠٩
رقم الإيداع الدولي ISSN 2223-9464
Info@baytalhikma.iq

التي تحدث فيها الحروب وهي كالاتي:.

التهديد السياسي : تعمل المنظمات الإرهابية على إلحاق الشلل بأنظمة القيادة أو قطع شبكات الاتصال بين الوحدات والقيادات المركزية أو تعطيل أنظمة الدفاع الجوي، أو إخراج الصواريخ عن مسارها.

كما تهدد شخصيات سياسية بارزة في المجتمع بالقتل، أو بالقيام بتفجير منشآت وطنية، أو بنشر فيروسات من أجل إلحاق الضرر والدمار بالشبكات المعلوماتية والأنظمة الإلكترونية ، إضافة لاختراق البريد الإلكتروني لرؤساء الدول وكبار الشخصيات السياسية وهتك أسرارهم والاطلاع على معلوماتهم وبياناتهم والتجسس عليها لمعرفة مراسلاتهم ومخاطباتهم والاستفادة منها في عملياتهم الإرهابية، فمثلا: في عام ٢٠١٠ ظهر ما عُرف باسم «إعصار ويكيليكس» إذ تم استغلال شبكة الإنترنت العالمية في تسريب وثائق تحوي معلومات سرية للغاية متداولة بين الإدارة الأمريكية وقنصلياتها الخارجية بدول العالم(٢٠).

التهديد الأمني: ويكون هذا من خلال:

عمل الجماعات الإرهابية على التسلل الإلكتروني إلى الأنظمة الأمنية في دولة ما وشلها لصالحها، وفك الشفرات السرية للتحكم بتشغيل منصات إطلاق الصواريخ الاستراتيجية والأسلحة الفتاكة.

تعطيل مراكز القيادة والسيطرة العسكرية على وسائل الاتصال للجيوش بهدف عزلها عن قواتها، والنفاذ إلى النظم العسكرية واستخدامها لتوجيه الجنود إلى نقطة غير آمنة قبل قصفها أو تفجيرها.

فضلا شن عمليات إرهابية على المواقع الحيوية، أو التحكم في خطوط الملاحة الجوية والبرية والبحرية، فمثلا في يناير ٢٠٠٨ تم قطع الكابل البحري الذي يربط أوروبا بالشرق الأوسط والكابل القريب من ساحل دبي وخليج عمان، مما أدى إلى خسائر بقطاع الاتصالات والتعاملات الإلكترونية أو شل محطات إمداد الطاقة والماء، حيث تشير مصادر كلية الحربية الأميركية إلى أن ضرب مولدات الطاقة الكهربائية العراقية أدى بشكل غير مباشر إلى موت ما بين ٧٠ إلى ٩٠ ألف مواطن عراقي كنتيجة مباشرة لعدم توفر الطاقة الكهربائية .

فضلا عن ذلك نجد أن تهديد الإرهاب السيبراني لا يتوقف عند هذا الحد، حيث يمكننا وجود تأثيرات سلبية أخرى تؤثر على الأمن السيبراني للدول، والتي تتمثل في(٢١):

تؤدي الهجمات الإرهابية الإلكترونية إلى الحرمان من الخدمة من خلال إبطاء أو منع المستخدمين الشرعيين من الوصول إلى النظام معين، بعد وضع البرمجيات الخبيثة.

يمكن أن تؤدي الهجمات على أنظمة التحكم الصناعية إلى تدمير أو تعطيل المعدات التي تسيطر عليها، مثل المولدات والمضخات وأجهزة الطرد المركزي.

من المسلم به على نطاق واسع ان الهجمات الالكترونية يمكن ان تكون مكلفة بالنسبة للافراد

Semi-annual Quarterly journal issued byPolitical and Strategic Studies In Bayt Al-Hikma Baghdad
No.of deposit at Political and Strategic Studies(678)2009
ISSN.2223-9464
Info@baytalhikma.iq

والمنظمـات، يمكن ان يكون مـن الصعب قياس الاثـار الاقتصادية وتختلف تقديـرات تلك الاثار اختلافا كبيرا.

المبحث الثالث: نماذج الحروب السيبرانية

المطلب الاول: الحرب السيبرانية- الامريكية _ الصينية

القـوة السـيبرانية هـي قـدرة الدولـة الوطنيـة علـى السـيطرة والتأثيـر داخـل وعبـر الفضاء الالكتروني، بما يدعم عناصر القوة الأخرى التي تشـكل في مجموعها القدرات الشاملة لأي دولة، لتحقيـق القوة السـيبرانية تحتاج الـدول لتطوير مـوارد للعمـل في البيئة السـيبرانية الحواسـيب المتطورة المرتبطة بالشبكات السلكية واللاسلكية والبرامج المتطورة للعمل، والأشخاص المدربون على هـذه النوعية الخاصة من الأعمـال القتالية الجديدة(العقول). ومن هنا سـوف نوضح قوة كل من الولايات المتحدة الامريكية والصين كالاتي:

اولاً: مقومات قوة الصين السيبرانية

تعتمد القوة السيبرانية الصينية على عدة مرتكزات منها: [٢٢]

١- امتـلاك البنيـة التحتية للمعلومـات: اذ يجب أن تمتلـك الدولة البنية التحتيـة اللازمة لصناعة الانترنـت، سـواء كانـت شـركات عملاقـة أو كبار المطوريـن، على غرار الولايـات المتحدة التـي تمتلـك شـركات كبرى مثـل أبـل وبي أم ومايكروسوفت وانتل وجوجل وغيرها

٢- قدرات سوق الانترنت: بمعنى عدد مستخدمي الانترنت داخل الدولة (كماً ونوعاً) ونشـر ثقافة الانترنـت وتغلغلهـا، ومدى قدرتهـا على تغيير سـلوكيات عامة فـي المجتمع وعبـر القطاعات المختلفة (الصحة ، التعليم الخدمات... الخ).

٣-الدبلوماسـية الرقميـة وقـدرات السياسـة الخارجيـة: اذ تحتـاج القوة السـيبرانية لإمتلاك دبلوماسية قوية قادرة على التفاوض والدفاع عن مصالح الدولة بهذا الاتجاه، والتفاوض مع الدول الأخرى التي تمتلك شـبكات منافسـة، ودراسـة فرص التعاون واحتمـالات الصراع او التصادم وكيفيـة إدارة الأزمات ذات الصلـة بهذا القطاع الجديد.

٤-القوة العسكرية السـيبرانية: إذ يجب أن تمتلك الدولـة القـدرة علـى الدفاع عـن البنيـة التحتية لتكتولوجيا المعلومات مـن أي تهديدات محتملة، عبر تطوير الاسـتراتيجيات والتكتيكات الدفاعية بهذا الخصوص، كما يجب أن تمتلك الدولة قدرات الهجـوم والـردع للخصـوم المحتملين، خاصة مـع عمليـات التجسـس والاختـراق والقرصنة الالكترونية.

٥-وضع القوة السـيبرانية كمصلحة وطنية عليا: لا يكفي أن تمتلـك الدولة جانب من البنية التحتية السيبرانية حتى يكون لديها قوة سيبرانية حقيقية، بـل يجـب أن يكون لـدى الدولة الدافـع والرغبة الحقيقيـة في اسـتخدام تلك القوة مـن أجل تحقيق المصالـح العليـا للدولة في المجـالات المختلفة(الاقتصادية والسياسية والأمنية والعسكرية).

٦- قدرات البحـث والتطوير، ومدى قدرة الدولة

مجلّة نصف سنوية محكّمة تصدر عن قسم الدراسات السياسية والاستراتيجية في بيت الحكمة ـ بغداد
رقم إيداع مجلة دراسات سياسية وأستراتيجية في دار الكتب والوثائق ٦٧٨ لسنة ٢٠٠٩
رقم الإيداع الدولي ISSN 2223-9464
Info@baytalhikma.iq

على إجراء البحوث وتطوير المعلومات وتعزيز الابتكار وتطبيق البحوث.

٧- القوة السيبرانية والقطاع الاقتصادي للأمن القومي. تعتبر هذه الركيزة من أهم ما يميز التجربة الصينية، حيث أكد الرئيس الصيني شي جي بينغ أن تطوير أعمال الشبكات ينبغي أن يطبق التنمية المتمركزة حول الإنسان، وينبغي تسخيرها لخدمة قضايا هامة مثل الفقر والبطالة وغيرها (التجارة الالكترونية، والأسواق الرقمية)، حيث تعتبر الصين حالياً هي أكبر سوق رقمي في العالم في مجال التجارة الالكترونية.

في عام ٢٠١٥ أطلقت الصين أكبر عملية إعادة تنظيم على مستوى القوات المسلحة(جيش التحرير الشعبي) حيث شملت الإصلاحات جميع صنوف وفروع الجيش البرية والبحرية والجوية، وكان من ضمن الاصلاحات المهمة استحداث فرع جديد يسمى « قوات الدعم الاستراتيجي» من بين مهامها الأساسية هي تأمين الفضاء الكهرومغناطيسي والفضاء الالكتروني، والتحكم في العمليات السيبرانية إدارتها إلى مستويات عليا، بما يضمن تحقيق السيادة السيبرانية عبر قوة سيبرانية فعالة(٢٣).

كما عملت الصين على ترسيخ أُسس استراتيجية الأمن الإلكتروني في العلوم والأدبيات العسكرية الصينية، مثل: المبادئ التوجيهية للاستراتيجية العسكرية The Military Strategic Guidelines ، وعلم الاستراتيجية العسكرية The Science of Military Strategy، فضلاً عن المبادرات الحكومية، مثل مبادرة ''المهام التاريخية الجديدة'' لـ''هو جين تاو'' Hu Jintao's New Historic Missions، والأوراق البيضاء للدفاع الوطني The National Defence White Papers. ومن خلال هذه العلوم والأدبيات العسكرية، بحث العسكريون في استراتيجيات تُمكنهم من استغلال المجال الإلكتروني في مختلف السيناريوهات الهجومية والدفاعية.(٢٤)

ثانياً: القوة السيبرانية الامريكية

تعُد الولايات المتحدة من الدول الرائدة في المجال السيبراني، إذ طوّرت قدرات متقدمة مكّنتها من قيادة هذا القطاع لسنوات طويلة، قبل أن تبرز الصين كمنافس قوي، لاسيما عبر تطوير تقنيات شبكات الجيل الخامس (٥G) وتقديم بدائل للتكنولوجيا الأمريكية، الأمر الذي أثار قلق واشنطن. اذ أصدرت الولايات المتحدة عام ٢٠١٨ استراتيجية الأمن السيبراني في عهد الرئيس (دونالد ترامب)Donald Trump، والتي تبنّت نهجاً أكثر تشدداً مقارنة بسياسات إدارة Barack Obam(بارك اوباما). وقد سمحت الاستراتيجية بتوسيع نطاق العمليات السيبرانية الهجومية، وأكدت أن أي هجوم سيبراني قد يُواجَه بردّ هجومي أو دفاعي، ليس بالضرورة في الفضاء السيبراني وحده، بل قد يمتد إلى المجال المادي باستخدام القدرات العسكرية التقليدية، كما تبنّت مبدأ '' الهجوم الدفاعي'' القائم على التحرك الاستباقي، واختراق شبكات الخصوم، وتعزيز جمع المعلومات الاستخباراتية استعداداً للصراعات المستقبلية، ومن أبرز المشروعات المرتبطة بهذا التوجه مشروع الحوسبة السحابية

Semi-annual Quarterly journal issued byPolitical and Strategic Studies In Bayt Al-Hikma Baghdad
No.of deposit at Political and Strategic Studies(678)2009
ISSN.2223-9464
Info@baytalhikma.iq

التابـع لـوزارة الدفـاع الأمريكيـة، المعـروف رسـمياً باسـم (Joint Enterprise Defense Infrastructure) (JEDI)، والذي قُدّرت قيمته بنحـو ١٠ مليارات دولار. يهدف المشـروع إلى إنشـاء بنية تحتية سـحابية موحّدة لتخزين وإدارة البيانـات الضخمة داخـل البنتاغـون، بما يعزز كفاءة نظم المعلومات العسـكرية ويسـتبدل آلاف الشـبكات المتفرقة بنظام أكثر تكامـلاً. ويُعد هذا المشروع ركناً أساسياً في تطوير القدرات القتالية الأمريكية، لا سيما في ظل بيئة تكنولوجية معقدة تتسم بتسـارع تطورات الجيل الخامس والتحول الرقمي العسكري.(٢٥)

ونتيجـة للمتغيرات التي أحدثتها ثورة المعلومات والتكنولوجيـا، ظهر ما يعرف بحرب المعلومات الإسـتراتيجية والتـي عرفهـا البعـض على انها «اعمـال تقوم بها دول تحاول من خلالها اختراق أجهزة الكمبيوتر والشـبكات التابعة لدولة اخرى بهدف تحقيق أضرار بالغة او تعطيلها او سـرقة المعلومات»(٢٦). ترى الولايات المتحدة الامريكية ان أكبـر وأكثـر التهديدات التـي يواجهها الأمن القومي الأمريكي في القرن الحادي والعشـرين هـي قضية الأمن الألكترونـي، وهذه التهديدات متأتيـة من الصين، اذ تعمل الأخيرة على سـرقة معلومات التجارة الامريكية ومعلومات وأسـرار عسـكرية، مع توجيـه هجمـات الكترونية تعمل على تعطيل المنظومة الالكترونية لشبكات الدفاع والأسـتخبارات الامريكية، لذلـك تُعد قضية أمن الانترنت من أبرز القضايا المؤثرة في العلاقات بيـن(الصيـن والولايـات المتحـدة الامريكية) ولاسـيما عام ٢٠١٣ اذ أتهمت الولايات المتحدة الأمريكية الصين بالقيام بإعمال تجسـس لسـرقة معلومات عسكرية وتجارية سرية، وقامت شركة مانديانـت الأمريكيـة للأمـن الألكترونـي بتقديم تقريـر إتهمت فيه الجيش الصيني بشـن هجمات الكترونية واسعة النطاق على مؤسسات امريكية، أن الاتهامـات المتبادلـة بين(الصيـن والولايات المتحـدة الامريكيـة) تدلـل على وجـود تنافس دولـي على ما يعرف بالذكاء الاصطناعي والقوة الألكترونية وبالتالي إسـتخدام هذه الإمكانيات في تنفيذ هجماتها وإحتمالات توجه الدولة المستهدفة الى إستخدامات التطور التكنولوجي والحصول عليهـا، وهـذا مـا اكدتـه ريفا جوجـون كبيرة المحللين بمعهد سـترانفورد الأمريكي للدراسات الأمنية والإسـتراتيجية بقولهـا " أن التنافس بين اقطاب العالم ودوله الصغيرة على أمتلاك أحدث برمجيـات الـذكاء الإصطناعي سـيؤدي الى صراعات جديدة بسـبب تخوف الأطراف الدولية من بعضها" وبالتالي أن تقنية الذكاء الاصطناعي والحصـول عليها أصبح تحديـاً للدول الكبرى، إسـتناداً لمـا تقدم، فأن الامـن الالكتروني يُعد من أهم المتغيـرات الجديدة المؤثرة في العلاقات (الامريكية – الصينية)، بسبب أن إمتلاك القوة التقنيـة والمعرفية هي قوة إضافيـة لعناصر قوة الدولة الشاملة في القرن الحادي والعشرين، وهذا يعني التأثيـر الأقليمي والدولي للصين وهو الذي لا ترغب الولايات المتحدة به في سـياق رغبتها المستمرة بالسيطرة والهيمنة على النظام الدولي. (٢٧)

ثانيا: الحرب السيبرانية الروسية –الاوكرانية

السـيبرانية منـذ بدايـة التصعيـد الروسـي ضد

مجلّة نصف سنوية محكّمة تصدر عن قسم الدراسات السياسية والاستراتيجية في بيت الحكمة - بغداد
رقم إيداع مجلة دراسات سياسية وأستراتيجية في دار الكتب والوثائق ٦٧٨ لسنة ٢٠٠٩
رقم الإيداع الدولي ISSN 2223-9464
Info@baytalhikma.iq

أوكرانيا في أوائل هذا العام، توجهت أنظار المراقبين جميعا نحو الهجمات السيبرانية المحتملة التي يمكن أن تقوم بها روسيا ضد الأهداف المدنية والعسكرية في أوكرانيا. وقد كان هناك اعتقاد شائع بأن روسيا ربما ستستبق هجومها العسكري بهجمات سيبرانية موسعة ضد أوكرانيا؛ نظرًا للخبرات التي راكمتها عبر سنوات في هذا المضمار وقد كانت أوكرانيا أحد أبرز الأهداف للهجمات السيبرانية في السنوات القليلة الماضية. ومن هذه الهجمات على سبيل المثال عمليات التدخل والتلاعب بالانتخابات الرئاسية الأوكرانية لعام ٢٠١٤، التي أضرت بالنظام الانتخابي المركزي، وشوهت نزاهة العملية الانتخابية والهجوم الواسع الذي أصاب شبكة الكهرباء الأوكرانية عام ٢٠١٥، مما أدى إلى انقطاع التيار الكهربائي في عموم البلاد؛ وهجمات NotPetya التي غدت واحدة من أكثر الهجمات السيبرانية الضارة تكلفة، حيث أصابت عام ٢٠١٧ الشبكات الخدمية التابعة للقطاعات المصرفية والحكومية الأوكرانية وعطلت الوصول إليها، وتسربت بعد ذلك لتصيب بعض الشبكات في كل من إيطاليا وبولندا وروسيا والمملكة المتحدة والولايات المتحدة وأستراليا. وقد قدرت تكلفة هذه الهجمات حينها بعشرة مليارات دولار. وبالمجمل، فقد أكدت وحدة الاستخبارات الأمنية المعروفة بـ SBU التابعة لوكالة المخابرات الأوكرانية أنها حيدت أكثر من ٢٢٠٠ هجوم سيبراني على أوكرانيا العام الماضي وحده.

لم تعترف روسيا على الصعيد الرسمي بارتكاب أي من هذه الهجمات، وهي بذلك تؤكد على واحدة من أبرز خصائص حروب الشبكات السيبرانية، وهي غياب الإسناد أو الاعتراف من جانب، والمجهولية من جانب آخر وهي بذلك تعمل على جعل الانتقام من الطرف الآخر أكثر صعوبة، فالرد والانتقام يحتاجان إلى معرفة الفاعل على وجه التحديد.

أما في الحرب الحالية التي بدأتها روسيا على أوكرانيا في ٢٤ فبراير/ شباط ٢٠٢٢، فقد لجأت روسيا إلى تفعيل الجبهة السيبرانية جنبا إلى جنب الجبهة الميدانية للحرب، وفق مصادر رسمية أوكرانية وغربية وذلك من خلال شن مجموعة من الهجمات السيبرانية التي أصابت الشبكات الإلكترونية الأوكرانية سواء الرسمية منها أو المدنية وقد جاءت هذه الهجمات واسعة ومركزة، وهو ما ينفي فرضية تقاعس روسيا عن استخدام الاستراتيجية السيبرانية في حربها الدائرة مع أوكرانيا. أما تقييم نتائج هذه الهجمات فهو أمر آخر، حيث يرى العديد من المراقبين أن هذه الهجمات لم تسفر عن نتائج ملموسة من شأنها أن تسهم إما في دعم العمليات العسكرية الروسية على الأرض، أو في إخراج الشبكات الإلكترونية الأوكرانية من الخدمة، ومن ثم إرباك الحكومة الأوكرانية وحرمانها من حرية التصرف والقيام بهجمات مضادة.[٢٨]

وقد يعود السبب في عدم فاعلية الهجمات الروسية على أوكرانيا التي شئت في هذه الفترة التي يغطيها التقرير إلى عدة أسباب أبرزها[٢٩]:

أولا: عدم رغبة روسيا في القيام بهجمات

Semi-annual Quarterly journal issued byPolitical and Strategic Studies In Bayt Al-Hikma Baghdad
No.of deposit at Political and Strategic Studies(678)2009
ISSN.2223-9464
Info@baytalhikma.iq

سـيبرانية فتاكة تحـدث ضررًا كبيرًا بالشـبكات الأوكرانية على أساس حسابات مسبقة لدى القيادة الروسـية حول سـهولة احتلال العاصمة كييف، ومن ثم تنصيب حكومة موالية لموسـكو سـتكون بحاجة لهذه الشبكات للتحكم والسيطرة على البلاد بعد إسـقاط حكومة الرئيس الأوكراني فولوديمبر زيلينسكي.

ثانيا: عدم رغبة روسيا في توسيع دائرة الهجمات السـيبرانية، خشـية من حدوث هجمـات مضادة من طرف حلف الناتو على الشـبكات الروسـية، خصوصا تلك المتعلقة بالسيطرة والتحكم، والتي تعـد حيوية فـي المجهـود الحربـي. وقد صرح مسؤول في حلف الناتو نهاية شهر فبراير/ شباط، أي في الأيام الأولى للحرب، أن هجومًا سـيبرانيا علـى دولـة عضو فـي حلف شـمال الأطلسـي قـد يـؤدي إلى تفعيـل المـادة ٥، أي بنـد الدفاع الجماعي، وذلك وسـط مخـاوف من قيادة الحلف من انتشار الفوضى في الفضاء الإلكتروني حول الغزو الروسي لأوكرانيا إلى مناطق أخرى تابعة للحلف.

ثالثـا: قد تكون أوكرانيـا نجحت إلى حد كبير في تعزيز دفاعاتها السيبرانية، وهو ما انعكس إيجابا على اسـتراتيجية الردع السـيبرانية، الأمر الذي حـرم الهجمات الروسـية من إمعـان الضرر في شـبكاتها الإلكترونية. وسوف تحظى استراتيجية الـردع السـيبرانية لأوكرانيـا بمزيد من تسـليط الضوء لاحقا.

الخاتمة

خلاصـة القـول ان الصراعـات السـيبرانية تعد من أهم المتغيرات المؤثـرة في العلاقات الدولية الحديثة اذ شـهدت هذه العلاقات ومنذ بداية القرن الحادي والعشـرون صراعـاً واضحاً عن طريق دخول الدول الكبرى والمتقدمة الفضاء الألكتروني ورغبـة كل منهما في امتلاك القوة التقنية الرقمية والتكنولوجية والمعرفية، اذ ترى كل من الولايات المتحـدة الأمريكيـة والصين وروسـيا الاتحادية ان القـوة التكنولوجيـة والمعلوماتيـة هـي قـوة إضافية هامة تضـاف لعناصر القوة التي تمتلكها الدول، لاسـيما وأن الصين تحاول بكل ما أوتيت مـن قوة للعمل مـن أجل تفردها فـي امتلاك قوة سيبرانية تستند على أسـاليب حديثة في العمليات السـيبرانية الدفاعية والهجوميـة اكثر تطوراً من تلك التـي تمتلكها الولايات المتحدة الأمريكية من أجـل بناء منظومـة الكترونية تضمـن لها حماية مسـتمرة مـن التهديـدات السـيبرانية وفي نفس الوقـت تضمن امتلاكها القدرة على وسـائل ردع الكترونية فاعلة وذلك عن طريق دخولها الفضاء الالكتروني، وهذا ما لا ترضها الولايات المتحدة الأمريكية التي تعـد الدولة الأكثر قدرة في مجال الفضاء السـيبراني، أذ تسـعى الولايات المتحدة الامريكيـة دائما لكبح جماح الصيـن ومنعها من امتلاكهـا وسـائل تكنولوجية فاعلـة تجعلها اكثر قدرة على مواجهتها، من هنا شـهدت الصراعات السـيبرانية مابين الولايات المتحدة الأمريكية من جهة وروسيا الاتحادية واوكرانيا من جهة اخرى تطـورا في اسـاليب الهجمـات السـيبرانية وفي الوقت نفسـه تطوراً في اسـاليب الحماية من تلك الهجمات.

مجلّة نصف سنوية محكّمة تصدر عن قسم الدراسات السياسية والاستراتيجية في بيت الحكمة - بغداد
رقم إيداع مجلة دراسات سياسية وأستراتيجية في دار الكتب والوثائق ٦٧٨ لسنة ٢٠٠٩
رقم الإيداع الدولي ISSN 2223-9464
Info@baytalhikma.iq

الاستنتاجات

توصلت الدراسة الى عدة استنتاجات كالاتي:

ان المتغيرات التكنولوجية حولت الحرب التقليدية الى حرب الكترونية عبر الفضاء السيبراني.

تحولت القدرات الدولية التقليدية للقوة الى قدرات الكترونية رقمية.

حقق التطور العلمي والتكنولوجي اثر كبير في استحداث أسلحة الحرب والتي مكنت من ادارة العمليات والهجمات اثناء النزاعات بوسائل وآليات تعتمد على تقنيات مغايرة تماما لوسائل الحرب التقليدية.

ان الحرب الإلكترونية حرب العصر الحقيقية، مسارها الرئيس الشبكات الرقمية والإلكترونية، كذلك الوسائل التكنولوجية الأخرى.

اصبح التنافس الدولي بين القوى الكبرى على امتلاك القوة السيبرانية كونها تمثل سمة العصر في بدأ وحسم النزاعات الدولية.

اصبحت الحروب السيبرانية من اخطر التحديات الامنية في العصر الرقمي اذ تستهدف البنية التحتية الحيوية والانظمة المعلوماتية للدول، اذ بامكانها احداث اضرار سياسية واقتصادية وامنية كبيرة دون استخدام القوة العسكرية المباشرة.

قائمة المراجع

اولا: الكتب

منى الاشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية_ مجلس وزراء العدل العرب، لبنان، ٢٠١٦.

ثانيا: الدوريات

هربرت لين « النزاع السيبراني والقانون الدولي الإنساني مختارات من المجلة الدولية للصليب الأحمر، مجلد ٩٤ (٨٨٦) صيف ٢٠١٢.

نورية السعدي المقريف، الحرب السيبرانية في ضوء احكام القانون الدولي العام، مجلة ابحاث قانونية، كلية القانون - جامعة سرت، ليبيا، م٩، العدد(٢)، ٢٠٢٢.

لور انجيرلو تيلمان ، القانون الدولي الانساني وحماية المدنيين من اثار العليات السيبرانية اثناء النزاعات المسلحة، المجلة الدولية للصليب الاحمر، م(١٠٢)، العدد(٩١٣)، ٢٠٢٠.

عباس بدران، الحرب الالكترونية: الاشتباك في عالم المعلومات، مركز دراسات الحكومة الالكترونية، لبنان، ٢٠١٠.

نبيل عودة، العمليات السيبرانية في الحرب الروسية الأكرانية طبيعتها وانماطها، مركز الشرق للابحاث الاستراتيجية، ٢٠٢٢.

عادل عبد الصادق، انماط الحروب السيبرانية وتداعياتها على الامن العالمي، مجلة السياسة الدولية_ ملحق اتجاهات نظرية، العدد(٢٠٨)، مصر، ٢٠١٧.

حكيم غريب و صبرينة مزياني، تهديد الارهاب في الفضاء السيبراني نحو رسم مقاربة معرفية للتهديد الناشئ، مجلة الدراسات الاستراتيجية

Semi-annual Quarterly journal issued byPolitical and Strategic Studies In Bayt Al-Hikma Baghdad
No.of deposit at Political and Strategic Studies(678)2009
ISSN.2223-9464
Info@baytalhikma.iq

والعسكرية، المركز الديمقراطي العربي، برلين، العدد(٧)، ٢٠٢٠.

امير حسين واخرون، مبدأ منع التهديد باستعمال القوة في العلاقات الدولية في اطار ميثاق الامم المتحدة، المؤسسة العربية للعلوم ونشر الابحاث، مجلة العلوم الاقتصادية والادارية والقانونية، م(٣)، العدد (٩)، الولايات المتحدة الامريكية، ٢٠١٩.

انعام عبد الرضا سلطان، توظيف الحروب السيبرانية في تطوير مفهوم القوة للدول الكبرى، مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين، العدد(٧٣)، العراق، ٢٠٢٣.

ثالثا: الانترنت

درويش سعيد الحروب السيبرانية وأثرها على حقوق الإنسان، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية ، عبر شبكة المعلومات الدولية الانترنت، متاح على الرابط الاتي:

https://www.asjp.cerist.dz/en/٨٣٢٠٥/٥/٥٤/٣٢/downArticle

طلال ياسين عدي محمد عناب، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الزرقاء للبحوث والدراسات الإنسانية، المجلد ١٩ العدد الأول ، ٢٠١٩، عبر شبكة المعلومات الدولية الانترنت، متاح على الرابط الاتي:.https://doi ٠٠٥٤٧٨٨/١٠,١٢٨١٦/org

هالة أحمد الرشيدي هل من حرب سيبرانية بين الولايات المتحدة وروسيا منشور في جريدة الأهرام، العدد (٤٨٩٧٢) م١٤٥ بتاريخ ٤ يناير ٢٠٢١ ، عبر شبكة المعلومات الدولية الانترنت، متاح على الرابط الاتي:

https://gate.ahram.org.eg/daily/٧٩٢٣٥٢/٤/٢٠٣٦٢٠/News

يحيى الحياوي، حرب المعلومات ، بحث منشور عبر موقع الكاتب يحيى الحياوي، تاريخ النشر١٣-١٢-٢٠١٠، تاريخ الدخول ٢٠٢٥/٣/١٣ عبر شبكة المعلومات الدولية الانترنت، متاح على الرابط الاتي:

/https://www.elyahyaoui.org

عبد الجليل المرهون، عصر الردع الألكتروني، تقرير منشور في موقع قناة الجزيرة بتاريخ ٢٦-١٠-٢٠١٢، عبر شبكة المعلومات الدولية الانترنت، متاح على الرابط الاتي:https:// ١٦٨٤/studies.aljazeera.net/ar/profile

عادل عبد الصادق، انماط الحروب السيبرانية وتداعياتها على الامن العالمي، مجلة السياسة الدولية- ملحق اتجاهات نظرية، مركز الاهرام للدراسات السياسية والاستراتيجية، مصر، ٢٠١٧، عبر شبكة المعلومات الدولية الانترنت، متاح عبر الرابط الاتي:

https://www.siyassa.org.eg/aspx.١٢٠٧٢/News

علي موسى الكناني، الامن السيبراني في العلاقات الامريكية_ الصينية، جريدة الزمان

العربيــة، تاريــخ النشــر ٢١-٤-٢٠٢٠، تاريــخ الدخول الــى الموقع ١٢-٤-٢٠٢٥، عبر شــبكة المعلومــات الدولية الانترنــت، متاح عبر الرابط الاتي:

A٧٪https://www.azzaman.com/٪D٨-٨٦٪D٩٪٨٥٪D٩٪A٣٪D٨٪٨٤٪D٩٪D٨٪B١٪D٨٪ ٪A٧٪D٨٪

رابعا: المصادر الاجنبية

Steve Winterfeld & Jason Andress, The basics of cyber warfare, Understanding the fundamentals of cyber warfare in theory and practice, Syngress, USA , ٢٠١٣,p.١٦.

Jayadeva Ranade, Major structural reforms in PLA: brief lnitial assessment, Vivekananda international foundation, New Delhi Jan ١٣,٢٠١٦, Available at the link: https://www.vifindia.org/article/٢٠١٦/january/١٣/major-structural-reforms-in-pla-brief-initial-assessment?

الهوامش

١- امير حسين واخرون، مبدأ منع التهديد باستعمال القوة في العلاقات الدولية في اطار ميثاق الامم المتحدة، المؤسسة العربية للعلوم ونشر الابحاث، مجلة العلوم الاقتصادية والادارية والقانونية، م(٣)، العدد (٩)، الولايات المتحدة الامريكية، ٢٠١٩، ص١٥٠.

٢- نورية السعدي المقريف، الحرب السيبرانية في ضوء احكام القانون الدولي العام، مجلة ابحاث قانونية، كلية القانون - جامعة سرت، ليبيا، م٩، العدد(٢)، ٢٠٢٢، ص ٥.

٣- هربرت لين « النزاع السيبراني والقانون الدولي الإنساني مختارات من المجلة الدولية للصليب الأحمر، مجلد ٩٤ (٨٨٦) صيف ٢٠١٢ ص.

٤- منى الاشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية_ مجلس وزراء العدل العرب، لبنان، ٢٠١٦، ص٦٦.

٥- درويش سعيد الحروب السيبرانية وأثرها على حقوق الإنسان، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية ، ص ١٨١، عبر شبكة المعلومات الدولية الانترنت، متاح على الرابط:

https://www.asjp.cerist.dz/en/٨٣٢٠٥/٥/٥٤/٣٢/downArticle

٦- طلال ياسين عدي محمد عناب، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الزرقاء للبحوث والدراسات الإنسانية، المجلد ١٩ العدد الأول ، ٢٠١٩، ص ٨٥، عبر شبكة المعلومات الدولية الانترنت، متاح على الرابط الاتي:

Semi-annual Quarterly journal issued byPolitical and Strategic Studies In Bayt Al-Hikma Baghdad
No.of deposit at Political and Strategic Studies(678)2009
ISSN.2223-9464
Info@baytalhikma.iq

https://doi.org/10.12816/0047880.

٧- عادل عبد الصادق، انماط الحروب السيبرانية وتداعياتها على الامن العالمي، مجلة السياسة الدولية- ملحق اتجاهات نظرية، مركز الاهرام للدراسات السياسية والاستراتيجية، مصر، ٢٠١٧، عبر شبكة المعلومات الدولية الانترنت، متاح عبر الرابط الاتي:

https://www.siyassa.org.eg/News/١٢٠٧٢.aspx

٨- نورية السعدي المقريف، مصدر سبق ذكره، ص٧.

٩- درويش سعيد، مصدر سبق ذكره، ص١٨٤.

١٠- لور انجيرلو تيلمان ، القانون الدولي الانساني وحماية المدنيين من اثار العليات السيبرانية اثناء النزاعات المسلحة، المجلة الدولية للصليب الاحمر، م(١٠٢)، العدد(٩١٣)، ٢٠٢٠، ص٢٩١.

١١- هالة أحمد الرشيدي هل من حرب سيبرانية بين الولايات المتحدة وروسيا منشور في جريدة الأهرام، العدد (٤٨٩٧٢) م١٤٥ بتاريخ ٤ يناير ٢٠٢١ ، عبر شبكة المعلومات الدولية الانترنت، متاح على الرابط الاتي:

https://gate.ahram.org.eg/daily/News/٢٠٣٦٢٠/٤/٧٩٢٣٥٢

١٢- المصدر السابق نفسه.

١٣- عادل عبد الصادق، انماط الحروب السيبرانية وتداعياتها على الامن العالمي، مجلة السياسة الدولية_ ملحق اتجاهات نظرية، العدد(٢٠٨)، مصر، ٢٠١٧، ص٣٣.

١٤- يحيى الحياوي، حرب المعلومات ، بحث منشور عبر موقع الكاتب يحيى الحياوي، تاريخ النشر١٣-١٢-٢٠١٠، عبر شبكة المعلومات الدولية الانترنت، متاح على الرابط الاتي:

https://www.elyahyaoui.org/

١٥- انعام عبد الرضا سلطان، توظيف الحروب السيبرانية في تطوير مفهوم القوة للدول الكبرى، مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين، العدد(٧٣)، العراق، ٢٠٢٣، ص٤٢٩.

١٦- عبد الجليل المرهون، عصر الردع الألكتروني، تقرير منشور في موق قناة الجزيرة بتاريخ ٢٦-١٠-٢٠١٢، عبر شبكة المعلومات الدولية الانترنت، متاح على الرابط الاتي:https://studies.aljazeera.net/ar/profile/١٦٨٤

١٧- المصدر السابق نفسه.

١٨- عباس بدران، الحرب الالكترونية: الاشتباك في عالم المعلومات، مركز دراسات الحكومة الالكترونية، لبنان، ٢٠١٠، ص٤.

١٩- منى الاشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، مصدر سبق ذكره، ص٨٦.

٢٠- حكيم غريب و صبرينة مزياني، تهديد الارهاب في الفضاء السيبراني نحو رسم

مجلّة نصف سنوية محكّمة تصدر عن قسم الدراسات السياسية والاستراتيجية في بيت الحكمة - بغداد
رقم إيداع مجلة دراسات سياسية وأستراتيجية في دار الكتب والوثائق ٦٧٨ لسنة ٢٠٠٩
رقم الإيداع الدولي ISSN 2223-9464
Info@baytalhikma.iq

مقاربة معرفية للتهديد الناشئ، مجلة الدراسات الاستراتيجية والعسكرية، المركز الديمقراطي العربي، برلين، العدد(٧)، ٢٠٢٠، ص ٤٢.

٢١- المصدر السابق نفسه، ص ٤٣.

٢٢- اكرم حسان فرحات، حوائط الردع.. الجدار السيبراني الصيني في مواجهة مشروع العقل الامريكي، تاريخ النشر ٢-٣-٢٠٢١، تاريخ الدخول الى الموقع ١٢-١٢-٢٠٢٥، عبر شبكة المعلومات الدولية الانترنت، متاح عبر الرابط الاتي:

https://tahreersr.com/reports/%D%٨AD%D%٨٨%٩D%٨A%٧D%٨A%٦D٨%B%-٧D%٨A%٧D%٨٤%٩D%٨B

23-Jayadeva Ranade, Major structural reforms in PLA: brief lnitial assessment, Vivekananda international foundation, New Delhi Jan 13,2016, Available at the link: https://www.vifindia.org/article/2016/january/13/major-structural-reforms-in-pla-brief-initial-assessment?

٢٤- المصدر السابق نفسه.

٢٥- اكرم حسان فرحات، مصدر سبق ذكره.

26- Steve Winterfeld & Jason Andress, The basics of cyber warfare, Understanding the fundamentals of cyber warfare in theory and practice, Syngress, USA , 2013,p.16.

٢٧- علي موسى الكناني، الامن السيبراني في العلاقات الامريكية _ الصينية، جريدة الزمان العربية، تاريخ النشر ٢١-٤-٢٠٢٠، تاريخ الدخول الى الموقع ١٧-١٢-٢٠٢٥، عبر شبكة المعلومات الدولية الانترنت، متاح عبر الرابط الاتي:

https://www.azzaman.com/%D%٨A٧%D%٨٤%٩D%٨A%٣D%٨٥%٩D-٨٦%٩%D%٨A%٧ %D%٨B%١D٨

٢٨- نبيل عودة، العمليات السيبرانية في الحرب الروسية الأكرانية طبيعتها وانماطها، مركز الشرق للابحاث الاستراتيجية، ٢٠٢٢، ص١٠.

29- المصدر السابق نفسه، ص11.

الملخص

تناول البحث موضوع تداعيات الحروب السيبرانية على الامن والسلم الدولي وفقا لنماذج مختارة وذلك لبيان تاثير الحروب السيبرانية في البيئة الدولية، وتحليل التغيرات والتحولات في طبيعة الحروب واستخدامات القوة، ولتحقيق اهداف البحث تم الاعتماد على المنهج التاريخي لمقتضيات مفاهيمية فضلا عن المنهج التحليلي لتحليل التداعيات على الامن والسلم الدولي ومن ثم تم الاعتماد على المنهج الاستقرائي في اختيار نماذج لدراسة الحالة، وتكمن مشكلة البحث في التطور التكنولوجي المتسارع الذي افرز لنا ومن الممكن ان يفرز نماذج حروب جديدة، والتاثير

Semi-annual Quarterly journal issued byPolitical and Strategic Studies In Bayt Al-Hikma Baghdad
No.of deposit at Political and Strategic Studies(678)2009
ISSN.2223-9464
Info@baytalhikma.iq

الـذي يحـدث للـدول على اثـر ذلـك، وخلصت الدراســة الى ان التطورات التكنولوجية انعكست على مفهوم القوى الكبـرى في النظام الدولي في خـوض الحـروب وتصاعـد التنافس فيمـا بينها لامتلاك مقومات القوة والقدرة السيبرانية.

الكلمـات المفتاحيـة: الحـروب السـيبرانية، التداعيات الامنية، الامن والسلم الدولي، الولايات المتحـدة الامريكيـة، الصين، روسـيا الاتحادية، اوكرانيا.

Abstract

The research addressed the issue of the repercussions of cyber warfare on international security and peace, according to selected models, in order to demonstrate the impact of cyber warfare on the international environment, and to analyze the changes and transformations in the nature of warfare and the uses of power. To achieve the research objectives, the historical method was adopted for conceptual requirements, as well as the analytical method to analyze the repercussions on international security and peace. Then, the inductive method was adopted in selecting case study models. The research problem lies in the rapid technological development that has produced and may produce new models of warfare, and the impact that occurs on states as a result. The study concluded that technological developments have been reflected in the concept of major powers in the international system in waging wars and the escalation of competition between them to possess the elements of power and cyber capability.

Keywords: Cyber warfare, security implications, international peace and security, United States of America, China, Russian Federation, Ukraine