الحرب السيبرانية: الخلفية_ المستويات _الآثار المستقبلية

Cyber War: Background_Levels_Future Effects

بوالطمين لخضر *
جامعة سطيف 2-الجزائر
le_vert26@hotmail.com

تاريخ الارسال:2022/02/16 تاريخ القبول:2022/06/02 تاريخ النشر:2022/06/15

ملخص:

في ضوء التطور التكنولوجي المتسارع، وتنامي دور الفاعلين من دول ودون دول في المجال السيبراني زادت التهديدات الإلكترونية بصورة شملت، ليس فقط المواقع والخدمات الإلكترونية المدنية، ولكن أيضاً البيانات والمنشآت العسكرية، بالإضافة إلى البنية التحتية العسكرية الحرجة كالمفاعلات النووية، وهو تطور يفرض تحديات وأعباء كبرى على الأمن القومي للدول، بحيث يضعها على حافة حرب ذات نمط جديد في مفهومه، أبعاده ومستوياته...

فلقد أدّى تحول الفضاء الإلكتروني إلى أكبر ساحة للتفاعلات الدولية لبروز العديد من الأنماط التوظيفية السلبية له، سواءً على صعيد الاستخدامات ذات الطبيعة المدنية أو العسكرية، الأمر الذي جعل هذا الفضاء مجالا للصراعات المختلفة، سواءً للفاعلين من الدول أو غير الدول بغية إحداث أكبر قدر من النفوذ والتأثير السيبراني.

كلمات مفتاحية:الحرب السيبرانية. التهديد السيبراني. الأمن السيبراني. الصراع السيبراني. مستقبل الأمن الدولي.

Abstract:

Because of the accelerating technological development, and the growing role of actors from states and non-states in the cyber field, electronic threats have increased in a way that includes, not only civilian electronic sites and services, but also military data and facilities, in addition to sensitive military infrastructure such as nuclear reactors, a development that poses major challenges and burdens. on the national security of countries, That puts it In a confrontationof new kind of war with a new style in its concept, dimensions and levels...

The transformation of cyberspace into the largest arena for international interactions has led to the emergence of many negative employment patterns for it, whether in terms of civilian or military uses, which has made this space a field for various conflicts, whether for state or non-state actors in order to achieve the greatest influence. and cyber influence.

Keywords: Cyber War. Cyber Threat. Cyber Security. cyber Conflict. The Future of International Security.

*المؤلف المرسل

مقدمة:

مع تحوّل الفضاء الالكتروني إلى ساحة للتفاعلات العالمية، تبلورت ظاهرة الحروب السيبرانية التي اتسمت بخصائص مختلفة عن نظيراتها التقليدية، من حيث طبيعة الأنشطة العدائية، والفواعل، والتأثيرات في بنية الأمن العالمي. وعبّرت تلك الحرب عن نمطين من القوة في عملية توظيف التفاعلات في الفضاء الإلكتروني: الناعمة والصلبة ، ممّا يعكس تنامي القدرات والتهديدات المتصاعدة لأمن البنية التحتية الكونية للمعلومات. بحيث لم تعُد الخطط والاستراتيجيات التقليدية ذات جدوى إزاء طبيعة التهديدات التي تحملها الحرب السيبرانية، فضلاً عن تغيّر طبيعة الفواعل وأهدافهم القتالية وأدواتهم الحربية في هذا الفضاء، إضافة إلى التحوّل الشامل في ميدان الحرب وأطرافها.

الإشكالية:

تعالج هذه المقالة مجموعة من التساؤلات المتعلقة أساساً بمفهوم الحرب السيبرانية وتحديد مستوياتها وفحص الآثار التي يمكن أن تُحدثها على مستقبل الأمن العالمي من خلال طرح الإشكالية التالية: **ما هو مفهوم ومستويات الحرب السيبرانية، وما الدافع وراء تصاعد التهديدات السيبرانية وكيف تنعكس على الأمن العالمي؟**

الفرضية:

أدى التحول في طبيعة الحرب السيبرانية إلى إحداث آثار جوهرية في فهم وإدراك آليات المواجهة والتصدي للتهديدات المرافقة للظاهرة السيبرانية.

أهداف الدراسة:

تهدف هذه المقالة إلى تقديم دراسة تحليلية لمفهوم الحرب السيبرانية والإحاطة بمستوياتها لفهم طبيعتها ومقارنة أهم الفروقات التي تميّزها عن الحرب التقليدية، من حيث طبيعة الفواعل وأهدافهم ومجال تفاعلهم. كما ترمي المقالة إلى تحديد أهم التغيّرات الملموسة أو المتوقّعة التي تحدثها الحرب السيبرانية على الأمن العالمي.

منهج الدراسة:

تحقيقاً للغاية البحثية تمّ توظيف مقاربة منهجية متنوعة، فالمنهج التحليلي وضّح أهم التحولات التي عرفها سياق بناء مفهوم الحرب السيبرانية، كما ساهم في إبراز أهم العوامل المؤدية إلى تصاعد التهديدات السيبرانية، والمنهج المقارن أبرز مستويات الحرب السيبرانية وحدد العلاقة بينها، أما منهج دراسة الحالة فكان أساس المقالة باعتباره يعتمد على مفهوم الحرب السيبرانية كحالة للدراسة.

هيكلية الدراسة:

يتم تناول موضع الحرب السيبرانية: الخلفية _ المستويات_ الآثار المستقبلية ، من خلال استعراض العناصر التالية:

1. مفهوم الحرب السيبرانية

2. ظهور الحرب السيبرانية
3. عوامل تصاعد التهديدات السيبرانية
4. مستويات الحروب السيبرانية
5. مستقبل الحروب السيبرانية
6. انعكاسات الحروب السيبرانية على مستقبل الاستقرار الدولي

أولا: مفهوم الحرب السيبرانية

ينصرف معنى الحرب السيبرانية إلى توظيف التطبيقات العسكرية في بعدها الإلكتروني، حيث تعني قيام دولة أو فواعل من غير الدول بشن هجوم إلكتروني في إطار متبادل، أو من قبل طرف واحد. وبرغم شيوع مسمّى الحرب الإلكترونية، فإنه يُعدّ مصطلحاً قديما كان بالأساس مقصورا على رصد حالات التشويش على أنظمة الاتصال والرادار وأجهزة الإنذار، بينما يكشف الواقع الراهن في الفضاء الإلكتروني عن دخول شبكات الاتصال والمعلومات إلى بنية ومجال الاستخدامات العسكرية[1].

عرّف «قاموس أوكسفورد الإنكليزي» الحرب السيبرانية بأنّها: «استخدام تقنيات الحاسوب لتخريب نشاطات دولة أو منظمة، وبخاصة الهجومات المحضّرة على منظومات المعلومات الخاصة، وذلك لغايات استراتيجية أو عسكرية». أمّا موقع تكوبيديا Techopedia فقد عرّفها بأنّها: «كل هجوم افتراضي يجري بدوافع سياسية على أجهزة العدو الإلكترونية وشبكات الإنترنت وأنظمة المعلومات الخاصة به، لتعطيل منظوماته المالية وأنظمته الإدارية، وذلك من خلال سرقة قواعد معلوماته السرّية أو تعديلها لتقويض شبكات الاتصالات والمواقع ونظام الخدمات»[2].

مع تمدد الأعمال العدائية الإلكترونية إلى البنية التحتية المعلوماتية للدول لتحقيق أغراض متداخلة (سياسية، واقتصادية، وإجرامية، وغيرها)، حمل مفهوم الحرب الإلكترونية أبعادا جديدة، وصار البعض يفضل مصطلح الحرب السيبرانية، كتعبير عن ذلك التوجه الجديد، وإن ظل مفهوم الحرب ذاته محل جدل، خاصة أن هناك مسميات عديدة تطلق على تلك الأنشطة العدائية الإلكترونية، منها مثلا، الهجمات الإلكترونية والإرهاب الإلكتروني، وغيرهما.

فوفقاً للمفهوم التقليدي للحرب، فإنها تنطوي 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 العابرة للحدود الدولية، إضافة إلى اعتمادها على أسلحة إلكترونية جديدة تلاءم طبيعة السياق التكنولوجي لعصر المعلومات، حيث يتم توجيهها ضد المنشآت الحيوية، أو صبّها عن طريق برامج أو عملاء لأجهزة الاستخبارات.

ومن ذلك، بدا أن الأعمال العدائية في الفضاء الإلكتروني _إن لم يتم وصفها بالحرب_ يتم اعتبارها عملاً عدائياً، ولا يحمل هذا الأمر تقييما أخلاقيا لها بقدر ما هو تعبير عن طبيعة الهجمات الإلكترونية الفنية وطرق

حدوثها[3]. فتلك الهجمات تعتمد على التشويش والترويع، وبث الخوف، ومجهولية المصدر، أو حتى الحجم الفعلي للخسائر، أو الكيفية التي تمت بها.

وتتضمن الحرب السيبرية عمليات التخريب والتجسس:

– **التخريب Sabotage**: قد تتعرض حواسيب الأنظمة العسكرية والمالية لخطر التخريب بهدف تعطيل عملياتها الطبيعية وتجهيزاتها.

– **التجسس Espionnage**: تستخدم طرق غير شرعية لتعطيل عمل الشبكات العنكبوتية وحواسيبها، وأنظمتها بهدف سرقة معلومات سرّية من مؤسسات الخصم أو الأفراد ونقلها إلى الصديق السياسي، أو العسكري أو المالي.

الحرب السيبرانية هي حرب بكل ما للكلمة من معنى، ويعرّفها الدكتور بول روزنفياغ، أستاذ القانون في جامعة جورج واشنطن، في بحث له عن قانونية هذه الحرب نُشر في العام 2012 بأنّها: «حربٌ ذكية أقوى من أي هجوم بري أو جوي، وأكثر ذكاءً وأقل تكلفة، فهي لا تحتاج إلى معدات حربية ولا جنود، لكنّها تحتاج إلى قدرات علمية عالية». وهو يعتبر أنّ «حرب السايبر هي تطوّر طبيعي في مفهوم الحروب، نقلتها إلى جيل جديد يعتمد على التحكّم والسيطرة عن بعد» .وأشار روزنفياغ إلى «أنّ لحرب السايبر تأثيرًا عالميًا مدمرًا، إذ قد تؤدي إلى تدمير بنية تحتية لدولة ما، بما في ذلك سدودها المائية ومفاعلاتها النووية»[4].

وهناك من يرى أنّ مضمون الحرب الإلكترونية يتعلق بالتطبيقات العسكرية للفضاء السيبراني، حيث تعني – في أحد تعريفاتها – قيام دولة أو فواعل من غير الدول بشنّ هجوم إلكتروني في إطار متبادل، أو من قبل طرف واحد.

أيضا، تدخل تلك الأعمال العدائية في إطار الحرب غير المتكافئة، كون الطرف الذي يتمتع بقوة هجومية، ويبادر باستخدامها هو الأقوى، بغض النظر عن حجم قدراته العسكرية التقليدية، الأمر الذي يؤثر في أسس نظريات الردع الاستراتيجي، فضلاً أن عدم القدرة على التمييز بين استهداف المنشآت المدنية أو العسكرية في هجمات الحرب الإلكترونية يُصعّب من فرض حماية دولية.

ثانيا: ظهور الحرب السيبرانية

تعود بداية الحروب السيبرانية إلى حقبة الحرب الباردة، حيث كان مورتون كابلان يعتبرها إحدى مخرجات شذوذ الصراع بيم الكتلتين ورفعهما مستوى السباق إلى مجالات غير مسبوقة، حيث كان الجواسيس السوفييت والأمريكان يعترضون بشكل دوري ومنتظم على اتصالات بعضهما البعض من إشارات راديوية واتصالات هاتفية بهدف تحصيل معلومات عن نوايا وقدرات الطرف الآخر قصد الحصول على أسبقية وأفضلية في أي حرب متوقع اندلاعها بينهما.

وعلى الرغم من أنها كانت تدور في نطاق محدود نوعاً ما، فإن أول موقعة سيبرانية حدثت بين الولايات المتحدة والاتحاد السوفييتي كانت في 1982 أحدثت آثارا بارزة تمثلت في تخريب خط الأنابيب السوفييتي العابر

لسيبيريا، حيث كانت هناك عملية ضخمة لجهاز المخابرات السوفييتي**KGB** ، تسمى (**Line X**) صُممت لتساعد الاتحاد السوفييتي، والذي كان متأخراً إلى حد كبير في مجال تصميم التكنولوجيا والإلكترونيات الدقيقة على تخطي هذه الفجوة عن طريق سرقة تكنولوجيا المعلومات لكل الأنشطة من الغرب[5].

حيث قامت المخابرات السوفييتية بتدريب جيش من العلماء على التسلل إلى الشركات والوكالات لسرقة المخططات والرسوم للمشروعات والإنشاءات والمعلومات السرية للأبحاث.

وتسربت معلومات إلى وكالة المخابرات المركزية الأمريكية، والتي بدلاً من أن تشن حملات ومداهمات ضد هؤلاء العلماء العملاء، قررت القيام بما هو أبعد من ذلك، ونصبت فخاخاً لتنفيذ عملية تجسس مضادة، أي أنها بدلاً من إلقاء القبض عليهم تركتهم يواصلون العمل، ولكن مع إمدادهم بمعلومات مغلوطة، وسمحت لهم بالولوج إلى مخططات لمنشآت يمكنهم بناءها، من بينها مخططات لبناء خطوط أنابيب للنفط والغاز الطبيعي.

وحصل الجواسيس السوفييت على وثائق تتضمن مخططات الإنشاء، ولكنها كانت تتضمن خطأ بسيطاً في الشفرة لم يُمكن ملاحظته. واستخدم السوفييت المخططات بالفعل لبناء العمود الفقري لخطوط نقل الغاز الطبيعي والنفط القادمة من سيبيريا. ولكن بعد فترة قصيرة تسبب الخطأ المتعمد في الشفرة في حدوث انفجار لخط الأنابيب يعادل ثلث حجم انفجار القنبلة النووية في هيروشيما.

ثالثاً: عوامل تصاعد التهديدات السيبرانية

تبلورت مصالح قومية للدول في الفضاء الإلكتروني بتزايد الاعتماد على ربط البنى التحتية لها بذلك الفضاء في بيئة عمل تشابكية واحدة، تعرف بالبنية التحتية القومية للمعلومات(**NII**) مثل قطاعات الطاقة، والاتصالات، والنقل، والخدمات...وغيرها. وبالتالي فأي تهديد محتمل أو هجوم على إحدى تلك المصالح أو كلها للدولة قد يشكل مدعاة لحدوث عدم توازن استراتيجي، وهو ما يكشف عن نمط جديد من التهديدات للأمن القومي للدول[6]. ساعد على تنامي مثل هذه التهديدات الإلكترونية لمصالح الدول، ومن ثم إمكانية بروز حروب سيبرانية، سياق تاريخي حامل لعدة عوامل أساسية مُحفِّزة ، منها:

1- تزايد ارتباط العالم بالفضاء الإلكتروني، الأمر الذي اتسع معه خطر تعرض البنية التحتية الكونية للمعلومات لهجمات إلكترونية، فضلا عن استخدامه من قبل الفاعلين من غير الدول، خاصة الجماعات الإرهابية لتحقيق أهدافها التي تنال من الأمن القومي للدول.

2- تراجع دور الدولة في ظل العولمة وانسحابها من بعض القطاعات الاستراتيجية لمصلحة القطاع الخاص. في الوقت عينه، تصاعدت أدوار الشركات متعددة الجنسيات، خاصة العاملة في مجال التكنولوجيا كفاعل مؤثر في الفضاء الإلكتروني، لاسيما مع امتلاكها قدرات تقنية تفوق الحكومات.

3- نشوء نمط جديد من الضرر على خلفية الهجمات الإلكترونية يمكن أن تسببه دولة لأخرى، 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 سمات مدنية وعسكرية متداخلة، خاصة أن الثورة التكنولوجية الحديثة تمخضت عنها ثورة أخرى في المجالات العسكرية، وتطور تقنيات الحرب[7] .

4- قلة تكلفة الحروب السيبرانية مقارنة بنظيراتها التقليدية، فقد يتم شن هجوم إلكتروني بما يعادل تكلفة دبابة واحدة، من خلال أسلحة إلكترونية جديدة ومهارات بشرية، علاوة على أن هذا الهجوم قد يتم في أي وقت، سواء أكان وقت سلم أم حرب أم أزمة، ولا يتطلب تنفيذه سوى وقت محدود.

5- تحوّل الحروب السيبرانية 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 ظهر ما يسمي الاستراتيجية السيبرانية للدول، والتي تشير إلى القدرة على التنمية، وتوظيف القدرات للتشغيل في الفضاء الإلكتروني، وذلك بالاندماج والتنسيق مع المجالات العملياتية الأخرى لتحقيق أو دعم إنجاز الأهداف، عبر عناصر القوة القومية.

7- أدّى 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 من غير الدول في الحرب السيبرانية. 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 السيبرانية، مقارنة بممارسة القوة الناعمة على الفضاء الإلكتروني لنشر الأفكار المتطرفة، فإن هناك مؤشرات على احتمال تطوير تلك الجماعات لقدراتها الهجومية مستقبلا.

رابعاً: مستويات الحروب السيبرانية

إن سعي الدول لحيازة القوة السيبرانية، علاوة على تغير طبيعة الصراعات الدولية، يشكلان بدورهما مدخلاً تفسيرياً لنشوب الأنشطة العدائية الإلكترونية مما يعكس معضلة تشابك تفاعلات الفضاء الإلكتروني. ففيما يرتبط الأمن السيبراني، سواء للدول أو العالم، ارتباطا وثيقا بهذه الحروب فإن مستويات الحروب السيبرانية تتمايز وفق درجة الانخراط فيها بالنسبة للأطراف المتورطة فيها، ويمكن تفصيل ذلك على النحو التالي:

1. <u>الأمن السيبراني:</u>

تزايدت العلاقة بين الأمن والتكنولوجيا، خاصة مع إمكانية تعرض المصالح الاستراتيجية للدول إلى أخطار وتهديدات، الأمر الذي حوّل الفضاء الإلكتروني لوسيط ومصدر لأدوات جديدة للصراع الدولي. وفرضت

تلك التطورات إعادة التفكير في مفهوم الأمن القومي للدولة، الذي يعتني بحماية قيم المجتمع الأساسية وإبعاد مصادر التهديد عنها وغياب الخوف من خطر تعرض هذه القيم للهجوم[8].

وبات توافر أمن الفضاء الإلكتروني يتحقق حال وجود إجراءات الحماية ضد التعرض للأعمال العدائية، والاستخدام السيئ لتكنولوجيا الاتصال والمعلومات[9]. وعنى ذلك الأمن الإلكتروني بعملية وضع المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين بها عبر الاتصالات، ولضمان أصالة وصحة هذه الاتصالات.

بيد أن طبيعة ذلك الفضاء كساحة عالمية عابرة لحدود الدول، جعل الأمن السيبراني يمتد من داخل الدولة إلى النظام الدولي ليشكل نوعا من الأمن الجماعي العالمي، خاصة مع وجود مخاطر تهدد جميع الفاعلين في مجتمع المعلومات العالمي.

لهذا أصبحت هناك مصلحة قومية، وكذلك دولية في الحفاظ على أمن الفضاء الإلكتروني على أساس أن الأخير صار جزءا من الأمن العالمي. ودعم ذلك الطبيعة المتغيرة للتفاعلات الإلكترونية، خاصة مع تطور القدرات البشرية على إنتاج تقنيات جديدة، فضلا عن تصاعد مخاطر التهديدات الإلكترونية على البنية التحتية الكونية للمعلومات[10].

ولم يقتصر الاهتمام بالأمن السيبراني على البعد التقني فحسب، بل تجاوزه إلى أبعاد أخرى ذات طبيعة ثقافية واجتماعية واقتصادية وعسكرية وغيرها، خاصة أن الاستخدام غير السلمي للفضاء الإلكتروني يؤثر في الرخاء الاقتصادي والاستقرار الاجتماعي لجميع الدول التي أصبحت تعتمد بنيتها التحتية على الفضاء الإلكتروني.

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

2. القوة السيبرانية:

لعب الفضاء الإلكتروني دورا أساسيا في تعظيم القوة أو الاستحواذ على عناصرها الأساسية في العلاقات الدولية، حيث أصبح التفوق في ذلك المجال عنصرا حيويا في تنفيذ عمليات ذات فاعلية في الأرض والبحر والجو والفضاء، واعتماد القدرة القتالية في الفضاء الإلكتروني على نظم التحكم والسيطرة التكنولوجية [11].

وأدّى ذلك الأمر إلى تغيير في مفهوم القوة الوطنية للدولة، فبات بالإمكان تعريفها بأنها: مجموعة الوسائل والطاقات والإمكانيات المادية وغير المادية، المنظورة وغير المنظورة التي بحوزة الدولة، ويستخدمها صانع القرار في فعل مؤثر يحقق مصالح الدولة، وتؤثر في سلوك الوحدات السياسية الأخرى[12].

وفي غمار هذا التحول، برزت القوة السيبرانية التي عرّفها جوزيف ناي بأنها:مجموعة الموارد المتعلقة بالتحكم في والسيطرة على أجهزة الحاسبات والمعلومات، والشبكات الإلكترونية، والبنية التحتية المعلوماتية، والمهارات البشرية المدربة للتعامل مع هذه الوسائل.

ترتكز عناصر تلك القوة على وجود نظام متماسك يعظم القوة الناتجة عن التناغم بين القدرات التكنولوجية والسكانية والاقتصادية والصناعية والقوة العسكرية وإرادة الدولة وغيرها، بما يسهم في دعم إمكانات الدول على ممارسة الإكراه أو الإقناع أو ممارسة التأثير السياسي في أعمال الدول الأخرى بغرض الوصول للأهداف الوطنية، من خلال قدرات التحكم، والسيطرة على الفضاء الإلكتروني[13].

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

3. الصراع السيبراني:

تعرضت ظاهرة الصراع إلى تغيرات مع بروز الفضاء الإلكتروني، كمجال تنشأ فيه نزاعات بين الفاعلين المختلفين، خاصة مع الاعتماد الكثيف على تكنولوجيا الاتصال والمعلومات. وهنا، برز الصراع السيبراني كحالة من التعارض في المصالح والقيم بين الفاعلين، سواء أكانوا دولاً أم غير دول في الفضاء الإلكتروني.
وبرغم الآثار المدمرة لهذا النمط من الصراعات، فلا يرافقه دماء، وقد يتضمن التجسس والتسلل إلى مواقع الخصوم الإلكترونية، وقرصنتها، دون أنقاض، أو غبار. كما أن أطرافه يتسمون بعدم الوضوح، وتنطوي كذلك تداعياته على مخاطر عدة على أمن الدول، سواء عن طريق التخريب، أو استخدام أسلحة الفضاء الإلكتروني المتعددة[14].

ومع انتشار الفضاء الإلكتروني، وسهولة الدخول إليه، اتسعت دائرة الصراعات السيبرانية، وزاد عدد المهاجمين، وباتت هناك حالة من الكر والفر في الهجمات الإلكترونية لتعبر عن الصراع الممتد[15]. ولهذا صار الصراع بين الفاعلين المختلفين حول امتلاك أدوات الحماية والدفاع، وتطوير القدرات الهجومية الإلكترونية يستهدف حيازة القوة والتفوق والهيمنة، وتعزيز التنافس حول السيطرة، والابتكار والتحكم في المعلومات، وتعظيم القدرات القادرة على زيادة النفوذ والتأثير في المستويين المحلي والدولي.

وبما أن المتنازعين يلجأون في الصراعات التقليدية إلى استخدام شتى أنواع أسلحة التدمير الممكنة، فقد انتقلت جبهات القتال بشكل مواز إلى ساحة الفضاء الإلكتروني[16]. وكان لهذا التغيير دور في إعادة التفكير في حركية وديناميكية الصراع، بل وبروز ما يعرف بعصر القوة النسبية، التي تعني أن القوة العسكرية قد لا تكفي وحدها لتأمين البنية التحتية للدول، الأمر الذي يخلف آثارا استراتيجية هائلة على مستوى تركيبة وتوازنات النظام

الدولي. ولقد أسهم عاملان رئيسيان في انتشار رقعة الصراع في الفضاء الإلكتروني، وبالتالي إفساح المجال لنشوء الحروب السيبرانية، وهما:

1- تغيّر منظور الحرب جذريا، حيث انتقلت من نسق الحروب بين الدول إلى وسط الشعوب فكان الغرض من الحرب قديما هو تدمير الخصم، إما باحتلال أرضه أو الاستيلاء على موارده. أما الحروب الجديدة فقد استهدفت بالأساس التحكم في إرادة وخيارات المجتمعات. ومن ثم، بدا للشعوب أهمية محورية في هذا النمط الجديد من الحروب، سواء تعلق الأمر بالسكان المستهدفين في أرضية المواجهة أو بالرأي العام في الدولة التي تشن الحرب أو بالرأي العام على الصعيدين الإقليمي والدولي.

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

2- بروز الصراعات ذات الأبعاد المحلية_الدولية، حيث ساعد اشتعال الصراعات الداخلية في مرحلة ما بعد الحرب الباردة، وكذلك طبيعة السياق الدولي للفضاء الإلكتروني، في توفير بيئة مناسبة لدمج الفئات والقوى المهمّشة في السياسة الدولية، وخلق شبكة تحالفات مؤيدة أو معارضة ذات نطاق دولي عريض، إما على أساس قيم حقوقية، أو انتماءات عرقية أو دينية.

إذ 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. هنا تختلف أهداف الحروب الإلكترونية وفقا لطبيعة أهداف الصراعات السيبرانية، وذلك على النحو الآتي:

1- صراع سيبراني ذو طبيعة سياسية، حيث 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[17].

2- صراع سيبراني ذو طبيعة ناعمة، أي الصراع 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.

3- صراع سيبراني على التقدم التكنولوجي، حيث يأخذ هذا النمط من الصراعات السيبرانية طابعا تنافسيا حول الاستحواذ على سباق التقدم التكنولوجي، وسرقة الأسرار الاقتصادية والعلمية. وقد يمتد إلى محاولة للسيطرة على الإنترنت وأسماء النطاقات وعناوين المواقع والتحكم بالمعلومات والعمل على اختراق الأمن القومي

للدول بدون استخدام طائرات أو متفجرات أو حتى انتهاك حدود الدول، كهجمات قراصنة الكمبيوتر، وتدمير المواقع والتجسس، بما قد يكون له من تأثيرات مدمرة في الاقتصاد والبنية التحتية بذات قوة التفجير التقليدي.

4- صراع سيبراني 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 دعم قدرة الأجهزة الأمنية للدول أو حتى الجماعات المختلفة، على تشكيل شبكة عالمية من العملاء بدون تورط مباشر، بالإضافة إلى رخص التكلفة وسهولة الاتصال وصعوبة الرقابة التقليدية على التفاعلات الإلكترونية، ومثّل ذلك عنصرا جذابا لاستخدام الأسلحة الإلكترونية وتوظيفها لتحقيق أهداف سياسية وعسكرية.

خامساً: مستقبل الحروب السيبرانية

ذكر تقرير أعده مارك بوميرلو وظهر في إصدار خاص من دورية **Cyber Defense Review**، وهي دورية علمية يصدرها معهد الجيش السيبراني الأمريكي في ويست بوينت، أن الجنرال ستيفن فوغارتي، قائد القيادة الإلكترونية للجيش الأمريكي **ARCYBER**، قدّم خارطة طريق من ثلاث مراحل تنفذها القيادة السيبرانية للجيش الأمريكي على مدى عشر سنوات انتهت المرحلة الأولى منها منتصف العام الماضي (2021)[18]، وتهدف هذه الخطة إلى تحديد ملامح الأسس التي ستقوم عليها الأهداف الأمريكية المتعلقة بالتحضير للأنماط الجديدة من الحرب السيبرانية.

1- المرحلة الأولى: تأمل القيادة في تحقيق الإنشاءات الأولية للبرامج والتشكيلات الجديدة، والتي تمّ بالفعل تنفيذ العديد منها لبعض الوقت. يتمثل الجهد الرئيسي في نقل مقر القيادة من فورت بيلفوار في فيرجينيا، إلى فورت جوردون في جورجيا، بهدف تمكين القوات السيبرانية العملياتية والمؤسسية للجيش الأمريكي من العمل بتآزر غير مسبوق من خلال منصة عرض طاقة معلوماتية واحدة.

تعد كتيبة دعم الحرب الإلكترونية 915 أحد الكيانات الجديدة نسبياً حيث تتكون الكتيبة، التي تم إنشاؤها في عام 2019، من 12 فريقاً تدعم فرق الألوية القتالية أو غيرها من التشكيلات التكتيكية. تساعد **فرق التحليق في أفاق بعيدة**، كما يسميها بعض المسؤولين، في التخطيط للعمليات الإلكترونية التكتيكية للقادة في مسرح العمليات وتنفيذ المهام من جانب واحد بالتنسيق مع القوات في ميدان القتال.

لاحظ المسؤولون سابقاً أن هذا التشكيل من المرجح أن يتطور على مر السنين: بينما تجري القوة عمليات وتدريبات، فربما تحتاج إلى إعادة النظر في هيكلها وقدراتها. كما ستخضع القيادة، بحسب فوغارتي لعملية إعادة تنظيم لزيادة عدد فرق دعم عمليات المعلومات الميدانية المتاحة، وتوسيع نطاق الوصول إلى الخلف وقدرات وسائل التواصل الاجتماعي لتشمل كل من قوات العمليات التقليدية والخاصة[19].

وأورد أن العنصر الأخير من المرحلة الأولى، وفقاً لما وصفه فوغارتي يشتمل على إنشاء كتيبة إشارات هجومية جديدة للعمليات السيبرانية، وهو ما حصلت **ARCYBER** على الموافقة بشأنه، والتي بدأت مهامها في

فورت جوردون في ديسمبر 2021 وتقدم الدعم لقوات الجيش الأمريكي الإلكترونية. ونظراً لأنها كيان جديد، فإنه لا تتوفر سوى معلومات قليلة عنها، لكن وفقاً لما تطرق إليه فوغارتي فإنها من المتوقع أن تعكس المهمة التي كانت تؤديها قوات الحرس الوطني سابقاً باسم **Task Force Echo** . تنفذ قوة المهمة الوطنية السيبرانية عمليات إلكترونية هجومية تحت ستار الدفاع عن الأمة من الجهات الفاعلة السيبرانية الخبيثة.

2- المرحلة الثانية: ووفقاً لخارطة الطريق، فإن المرحلة، التي ستتم بين 2021 و2027، هي المكان الذي ستجرب فيه القوة وتبتكر، حيث ستشهد هذه المرحلة توظيف القدرات والوحدات الجديدة التي تم إنشاؤها في المرحلة الأولى. وكتب فوغارتي قائلاً :بينما يكتسب قادة الجيش مجموعات وممثلين متزايدين يدمجون قدرات المعلومات في عمليات مستدامة، فإن **ARCYBER**، بالاشتراك مع (قيادة التدريب والعقيدة) وقيادة مستقبل الجيش**AFC** ، سيكون بمثابة جامع المعرفة الرئيسي للجيش من أجل القتال الحربي الناشئ في القرن الحادي والعشرين في بيئة المعلومات[20]. وستنشئ **ARCYBER** مركزاً لعمليات حرب المعلومات في فورت جوردون وسيوفر المركز لـ**ARCYBER** قدرة غير مسبوقة في الوقت الحقيقي لاستشعار وفهم بيئة المعلومات العالمية مع الاتصال بجميع أوامر مكونات خدمة الجيش.

وأضاف فوغارتي: ستسمح هذه الميزة الفريدة لـ **ARCYBER** باستشعار وفهم واتخاذ القرار والاستجابة لظروف العنصر المعلوماتي العالمي الناشئ، مما يوفر خيارات للقيادة العليا للجيش والقادة الإقليميين والجيش المشترك بسرعة لا مثيل لها، مما يتيح ميزة اتخاذ القرار الاستراتيجي.

يهدف إنشاء هذا المركز الجديد إلى الاستفادة بشكل مباشر من دعم **ARCYBER** للقيادة السيبرانية من خلال مقر القوة المشتركة وأوامر المقاتلين التي تدير العمليات السيبرانية من أجلها. وسيكون من الأمور الحاسمة لنجاح مركز العمليات الجديد توافر لواء استخبارات عسكري متخصص، وهو الذي أشار فوغارتي إلى أنه سيركز فور تزويده بالموارد اللازمة، على بيئة المعلومات لتشمل الفضاء السيبراني والطيف الكهرومغناطيسي.

كما ذكر فوغارتي أنه مع تطور حرب المعلومات، يمكن أن تتحول مهام الفرق الإلكترونية الهجومية التي ينفذها **ARCYBER** للقيادة الإلكترونية من خلال لواء المخابرات العسكرية 780 نحو تشكيل بيئة المعلومات. سيطوّر الجيش الأمريكي أيضاً قواته التكتيكية من خلال توسيع الأنشطة الإلكترونية والكهرومغناطيسية الحالية(**CEMA**)، داخل أقسام الأركان لتشمل عمليات المعلومات والعمليات النفسية وموظفي الشؤون العامة وتعمل هذه الخلية على إعلام وتخطيط العمليات للقائد في القيادة داخل بيئة **CEMA**، وعلى نفس المنوال سيعمل الجيش على تحسين مكونات الاحتياط[21].

وأشار فوغارتي إلى أن العديد من القدرات المعلوماتية المتوافقة مع دعم القوات التقليدية تكمن في عناصر قوات الاحتياط، ووصف فوغارتي أيضاً قدراً لا بأس به من التجارب التي ستحدث في المرحلة الثانية مما سيساعد هذا على التطوير المستمر للقوات والقدرات لدعم العمليات متعددة المجالات. ستشمل هذه التجربة:

• فرقة العمل متعددة المجالات، وتحديداً **ARCYBER** ، تساعد في تدريب وإعداد كتيبة الاستخبارات والمعلومات والحرب الإلكترونية والحرب الإلكترونية والفضاء.

• قيادة معلومات لمسرح العمليات، وهي مفهوم قيادة مستقبلية للجيش الأمريكي لقيادة من الرتب الشابة، تزود قادة مسرح العمليات بقدرات التأثير التي سيتم اختبارها خلال تقييمات القتال الحربي المشترك وتدريبات الدفاع.

• ستجري فرقة عمل حرب المعلومات في أفغانستان، التي قادها مجتمع العمليات الخاصة بالجيش الأمريكي، عمليات دعم المعلومات العسكرية وجمع وسائل التواصل الاجتماعي وتحليلات البيانات وتكنولوجيا الإعلان الرقمي المتطورة لرسائل التأثير على الرأي العام.

3- المرحلة الثالثة: ستبدأ المرحلة الثالثة اعتباراً من عام 2028 وما بعده، وستركز على القدرات متعددة المجالات. عند هذه النقطة أضاف فوغارتي أنه مهما كانت القيادة السيبرانية للجيش الأمريكي، يجب أن تكون قادرة على النجاح في المعلومات والحرب غير التقليدية وإجراء عمليات استخباراتية واستطلاع مضاد للخصم وإظهار قدرة على الردع ذات مصداقية.

وشرح فوغارتي قائلاً: كجزء من القوة المشتركة يجب أن يتقن الجيش إجراءات المنافسة الأساسية من خلال ما يسميه عمليات متعددة المجالات **(MDO)** ، ليصبح قادراً على تنفيذها في كل مهمة حاسمة. وستلعب **ARCYBER** دوراً داعماً أساسياً، حيث يطور الجيش بشكل أفضل قدرته على إجراء مشاركة نشطة من خلال التوظيف المتقارب لقدرات المناورة والمعلومات التي تركز على تحقيق التأثيرات والسلوكيات المعرفية المرغوبة في خصوم الولايات المتحدة[22].

سادساً: انعكاسات الحروب السيبرانية على مستقبل الاستقرار الدولي

أدى اتساع علاقة الدول بالفضاء الإلكتروني، وما خلّفته من حروب سيبرانية إلى جملة من المخاطر والتداعيات على تفاعلات السياسة الدولية، يمكن طرح أبرزها على النحو الآتي:

1- تصاعد المخاطر الإلكترونية: خاصة مع قابلية المنشآت الحيوية (مدنية وعسكرية) في الدول للهجوم الإلكتروني عليها عبر وسيط وحامل للخدمات، أو شل عمل أنظمتها المعلوماتية، الأمر الذي يؤثر في وظائف تلك المنشآت. وبالتالي، فإن التحكم في تنفيذ هذا الهجوم يُعدّ أداة سيطرة استراتيجية بالغة الأهمية، سواء في زمن السلم أو الحرب[23].

2- تعزيز القوة وانتشارها: فمن جهة، عزز الفضاء الإلكتروني القوة المؤسسية في السياسة الدولية، وهي تعني أن يكون لها دور في قوة الفاعلين، وتحقيق أهدافهم وقيمهم في ظل التنافس مع الآخرين، والإسهام في تشكل الفعل الاجتماعي في ظل المعرفة والمحددات المتاحة، والتي تؤثر في تشكيل السياسة العالمية[24]. ومن جهة أخرى، عمل الفضاء الإلكتروني على إعادة تشكيل قدرة الأطراف المؤثرة، مثل الولايات المتحدة.

فبعدما كانت الأخيرة تملك ما يشبه الاحتكار لمصادر القوة، بعد انتهاء الحرب الباردة، برزت عملية انتشار القوة بين أطراف متعددة، سواء أكانت دولا أم من غير الدول [25].

3- عسكرة الفضاء الإلكتروني، وذلك 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 لدي الأجهزة المعنية بالدفاع والأمن في الدول، وتزايد الاستثمار في مجال تطوير أدوات الحرب السيبرانية داخل الجيوش الحديثة[26].

4- إدماج الفضاء الإلكتروني ضمن الأمن القومي للدول، وذلك عبر تحديث الجيوش، وتدشين 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[27].

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 القرار 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 القادر على شل القوة، والتشويش على المعلومة[28].

6- تحديث القدرات الدفاعية والهجومية، حيث سعت الدول إلى تحديث النشاط الدفاعي لمواجهة مخاطر الحرب السيبرانية، 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[29]. وهنا، يتعلق التوجه الأخطر بنقل تلك القدرات من الدفاع إلى الهجوم عن طريق استخدام تلك الهجمات في إطار إدارة الصراع والتوتر مع دول أخرى.

الخاتمة:

تبقى مشكلة دخول العالم سباق التسلح السيبراني في تحديد ماهية تلك الأسلحة التي يمتلكها الآخرون، حيث لا يملك المجتمع الدولي قدرة سريعة على التدخل لاحتوائها، ولا يوجد مجال لتفعيل التفتيش كآلية مراقبة، مثل حالة الأسلحة النووية.

وإن كانت عملية بناء القدرات العسكرية في مجال الأسلحة الإلكترونية تنطوي على عناصر أساسية، منها أولا السعي إلى امتلاك التكنولوجيا، وأنظمة الحماية، وتطوير قدرات هجومية تعمل على تحقيق التفوق التقني، وثانيا تطوير القدرات الهجومية، إما عبر بناء القدرات الذاتية، أو بالاستعانة بالأفراد والشركات المتخصصة، وتطوير القدرة على اختبار مدى الجاهزية لمواجهة الهجمات الإلكترونية، وثالثا العمل على توفير الميزانيات

المخصصة لتطوير القدرات الهجومية والدفاعية، وخاصة مع قلة تكلفتها، مقارنة بحجم ما ينفق على الجيوش التقليدية.

وتتمثل متطلبات توافر الأمن الإلكتروني الدولي في التأكد من سلامة الدفاعات الإلكترونية، وعدم تعرضها لأي خلل فني طارئ، وألا تعالج هذه المسألة منفصلة عن غيرها، وإنما ضمن ترسانة شاملة للدفاع تشكل إطاراً رادعاً لأي حرب استباقية.

وختاماً يمكن إيجاز أهم نتائج هذه الدراسة في النقاط التالية:

1. الحرب السيبرانية هي تطوّر طبيعي في مفهوم الحروب نقلتها إلى جيل جديد يعتمد على التحكّم والسيطرة عن بعد بحيث أن صار لها تأثيرًا عالميًا مدمرًا، إذ قد تؤدي إلى تدمير بنية تحتية لدولة ما، بما في ذلك سدودها المائية ومفاعلاتها النووية ومراكزها الحيوية.

2. الحرب السيبرانية تُصنّف من الأعمال العدائية في إطار الحرب غير المتكافئة، كون الطرف الذي يتمتع بقوة هجومية، ويبادر باستخدامها هو الأقوى، بغض النظر عن حجم قدراته العسكرية التقليدية، الأمر الذي يؤثر في أسس نظريات الردع الاستراتيجي ويفرض مراجعة نظرية وتطبيقية للفكر والخطط الاستراتيجية القائمة منذ نهاية الحرب العالمية الثانية على الأقل.

3. تزايد ارتباط العالم بالفضاء الإلكتروني أدى إلى اتساع خطر تعرض البنية التحتية الكونية للمعلومات لهجمات إلكترونية، فضلا عن استخدامه من قبل الفاعلين من غير الدول، خاصة الجماعات الإرهابية لتحقيق أهدافها التي تنال من الأمن القومي للدول، وكل هذا بفعل تراجع دور الدولة في ظل العولمة وانسحابها من بعض القطاعات الاستراتيجية لمصلحة القطاع الخاص، وفي ذات الوقت، تصاعدت أدوار الشركات متعددة الجنسيات، خاصة العاملة في مجال التكنولوجيا كفاعل مؤثر في الفضاء الإلكتروني، لاسيما مع امتلاكها قدرات تقنية تفوق الحكومات.

4. قلّة تكلفة الحروب السيبرانية مقارنة بنظيراتها التقليدية، تُغري بشن هجوم إلكتروني من خلال أسلحة إلكترونية جديدة ومهارات بشرية، علاوة على أن هذا الهجوم قد يتم في أي وقت، سواء أكان وقت سلم أم حرب أم أزمة، ولا يتطلب تنفيذه سوى وقت محدود ومن أطراف أقل ضعفاً أو إمكانيات.

5. من أجل الاستعداد لحروب المستقبل تبني العديد من الدول استراتيجية حرب المعلومات بحسبانها حربا للمستقبل، والتي يتم خوضها بهدف التشتيت، وإثارة الاضطرابات في عملية صناعة القرار 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 القادر على شل القوة والتشويش على المعلومة.

6. أهمية تحديث القدرات الدفاعية والهجومية، حيث سعت الدول إلى تحديث النشاط الدفاعي لمواجهة مخاطر الحرب السيبرانية، 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.

الهوامش:

[1] عادل عبد الصادق، حروب المستقبل.. الهجوم الإلكتروني على برنامج إيران النووي، مجلة السياسة الدولية، مؤسسة الأهرام، أفريل 2011.

[2] محمد علّام فرغلي، العنف الرقمي... أحدث صيحات الحروب الجديدة، قانون الرحب، مجلة الإنساني، العدد 59، 24 جوان 2018.

[3] عادل عبد الصادق، الإرهاب الإلكتروني: القوة في العلاقات الدولية .. نمط جديد وتحديات مختلفة، القاهرة: مركز الدراسات السياسية والإستراتيجية، ط1، 2009، ص 58.

[4] يحي اليحياوي، الإنترنت كفضاء للحروب الافتراضية القادمة، مركز الجزيرة للدراسات، سلسلة تقارير، 22 جانفي 2014، تاريخ التصفح من الموقع 2022/01/29 : https://studies.aljazeera.net/en/node/1975

[5] الحرب السيبرانية: نتائج ملموسة لمعارك غير مرئية، من الموقع: https://www.aljundi.ae

[6] Richard K. Betts, Conflict after the Cold War: Arguments on Causes of War and Peace, 2nd ed. (New York: Longman, 2002), p 552

7 Jennie M. Williamson, Information Operations: Computer Network Attack in the 21st Century, Strategy Research Project (Pennsylvania: U.S. Army War College. Carlisle Barracks, 2002) p 18.

[8] مصطفي علوي، مفهوم الأمن في مرحلة ما بعد الحرب الباردة، في أبحاث المؤتمر الذي عقده مركز الدراسات الآسيوية 4-5 ماي 2002: قضايا الأمن في آسيا، تحرير: هدي ميتكيس، والسيد صدقي عابدين (القاهرة: كلية الاقتصاد والعلوم السياسية، مركز الدراسات الآسيوية، 2004 ص14.

[9] Martin C. Libicki, Conquest in Cyberspace: National Security and Information Warfare (New York: Cambridge University Press, 2007): p 05.

10 Morgane Fouch, Robert Macrae and Jon Danielson, Could a Cyber Attack Cause a Financial Crisis ، World Economic Forum (13 June 2016), online e-article ,https://www.weforum.org/agenda/06/2016/could-a-cyber-attack-cause-a-financial-crisis

11 Arsenio T. Gumahad, Cyber Troops and Net War: The Profession of Arms in the Information Age (Alabama: Air University. Air War College, 1996): p 156.

[12] جوزيف س. ناي الابن، المنازعات الدولية: مقدمة للنظرية والتاريخ، ترجمة: أحمد أمين الجمل، ومجدي كامل، القاهرة: الجمعية المصرية لنشر المعرفة والثقافة العالمية، 1997، ص82.

[13] عادل عبد الصادق، الفضاء الإلكتروني والتحول في سياسات أجهزة الاستخبارات الدولية، كراسات استراتيجية، العدد 247، 2013، ص12.

14 Myriam Dunn, The Cyberspace Dimension in Armed Conflict: Approaching a Complex Issue with Assistance of the Morphological Method , Information and Security: An International Journal7 (2001): 145-158, online e-article ,http://procon.bg/system/files/07.08_Dunn.pdf

15 Jennie M. Williamson. Information Operation s, Op.Cit, P-22.

[16] عادل عبد الصادق، هل يمثل الإرهاب الإلكتروني شكلا جديدا من أشكال الصراع الدولي؟ ملف الأهرام الاستراتيجي، العدد 156، ديسمبر 2007.

17 Dunn, Information Age Conflicts: Op.Cit, P .5

[18] الحرب السيبرانية: نتائج ملموسة لمعارك غير مرئية، مرجع سابق.

[19] سو غوردون، إيريك روزنباخ، أمريكا تصفّي حساباتها السيبرانية وتعيد النظر فيها: سبل إصلاح استراتيجية فاشلة في مواجهة الحرب الرقمية، اندبندنت عربية مترجم عن **مترجم عن فورين أفيرز (مجلة الشؤون الخارجية) جانفي_ فيفري 2021**، تاريخ التصفح 2021/12/21 من الموقع: https://www.independentarabia.com/node/286926

[20] نفس المرجع.

[21] الحرب السيبرانية: نتائج ملموسة لمعارك غير مرئية، مرجع سابق.

[22] سو غوردون، إيريك روزنباخ، مرجع سابق.

[23] عادل عبد الصادق، الفضاء الإلكتروني والعلاقات الدولية: دراسة في النظرية والتطبيق، القاهرة: المكتبة الأكاديمية، 2016، ص 22.

[24] David Held et al., Global Transformations: Politics, Economics, and Culture (California: Stanford University Press, 1999 .p123.

[25] Joseph S. Nye. The Future of Power) New York :Public Affairs, 2011 .p 43.

[26] Ibid. p 46.

[27] Ibid. p 59.

[28] E. Nakashima. "U.S. Accelerating Cyber weapon Research", The Washington Post, online e-article, https://www.washingtonpost.com/world/national-security/us-accelerating-cyberweapon-research/13/03/2012/gIQAMRGVLS_story.html

[29] عادل عبد الصادق، القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني، مجلة السياسة الدولية، العدد 188، أفريل 2012.