الفضاء السيبراني: تشكيل ساحة المعركة في القرن الحادي والعشرين

Cyberspace: Formation of the battlefield in the twenty-first century

طالب الدكتوراه/ علاء الدين فرحات [1,2]

[1] المدرسة الوطنية العليا للعلوم السياسية، (الجزائر)

[2] المؤلف المراسل: alaferhat@gmail.com

تاريخ الاستلام: 2019/03/03 تاريخ القبول للنشر: 2019/09/23 تاريخ النشر: 2019/12/28

مراجعة المقال: اللغة العربية: د./ العزوزي حرزولي (جامعة الوادي) اللغة الإنجليزية: أ./ سارة الناصر (الاردن)

ملخّص:

يمكن النظر إلى هذه الدراسة في عمومها كقراءة في مقاربة تحولات الحرب، وبشكل خاص كمقاربة متعددة المداخل لإشكالية العلاقة بين الحرب والفضاء السيبراني، حيث ستعالج إمكانية شن الحرب السيبرانية في الواقع وستتطرق في إطار ذلك إلى بعض أهم القراءات التي تعاملت مع الموضوع.

كما ستتوقف عند إحدى أهم الإشكاليات المؤسسة لهذه الدراسة وهي الصراع السيبراني باعتباره الشكل الأكثر تطورا للحرب الحديثة، الأمر الذي تجلى على أرض الواقع وهبط من الفضاء النظري الذي رسم سيناريوهاته وتأثيراته المحتملة طوال سنوات مضت، تستند هذه المادة إلى تحليل شامل للعلاقة بين هذا النمط من الحروب والنمط التقليدي، فالحروب السيبرانية قد تتحول إلى سبب مباشر لاندلاع الصراعات العسكرية التقليدية.

تخلص الدراسة لمدى عمق الخطر الاستراتيجي الذي يترتب عن حروب الفضاء الالكتروني، الأمر الذي دفع الأمن السيبراني لشغل صدارة أولويات الأمن القومي الدولي.

الكلمات المفتاحية: الفضاء السيبراني؛ الحرب السيبرانية؛ الجيش السيبراني؛ الردع السيبراني.

Abstract:

This study can be considered as a new reading in the alteration of war, by using a multifaceted approach to understanding the relationship between war and cyberspace. It questions the extent to which the launching of cyber warfare in reality is possible.

In fact, cyber war is the most sophisticated form of modern warfare, which has recently appeared in the real world, leaving the theoretical realm which has shaped it since the last few years.

The importance of this paper lies in the determination of the potential link between this new form of wars and the traditional ones (ancient wars)

The study concludes that these new wars have deepened the strategic threat, and prioritized cyber security in the international security agendas.

Keys words: *Cyberspace; cyber war; cyber army; cyber deterence.*

مقدّمة:

خلال العقد الأخير شهد المجتمع الدولي بروز مجال جديد وبيئة جديدة مؤثرة في حركة التفاعلات والتحولات البنيوية في العلاقات الدولية تضاف إلى البيئات الأربع السابقة (الأرض، الجو، البحر، الفضاء الخارجي) أطلق على هذا البعد الفضاء السيبراني، والذي أصبح جزءًا أصيلاً من عمل الدول ومن بنيتها التحتية.

وتستخدم العديد من الدول القدرات التي يوفرها هذا الفضاء لاعتبارات في مقدمتها الأمن والقوة العسكرية، نظرا لان زيادة الاعتماد على الفضاء الإلكتروني مرئية في جميع القطاعات العامة والخاصة وكذا العمليات الحكومية، فضلا عن الاتصالات بين المجموعات والأفراد، صَاحَب هذا صعود القوة الإلكترونية في الشؤون الدولية، الأمر الذي جعل الدول تُدخل الفضاء الإلكتروني ضمن حساباتها الإستراتيجية وأمنها القومي خاصة في ظل تنامي التهديدات الإلكترونية Cyber threats من حيث النطاق والجدية التي ولدتها الثورة في نظم المعلوماتية وما لها من علاقة وطيدة بين الأمن والتكنولوجيا، ما جعل أغلب البنى التحتية للدول مربوطة آليا بقاعدة معلومات شكلت البيئة الرقمية التحتية، وبما أن لكل عصر نوعه الخاص من الحروب – وفق كلاوزفيتز –كنتيجة لعددٍ من التغيرات الجذرية في البيئة الدولية، تزايدت الدراسات حول اعتبار الفضاء الإلكتروني وسيط ومصدر لأدوات جديدة للصراع الدولي المتعدد الأطراف، وظهر بعد جديد في الصراعات الدولية سمي بـ "صراع الفضاء الإلكتروني"، وساهمت هذه المتغيرات في بروز عديد الاتجاهات التي تدارست الفضاء السيبراني كساحة جديدة للصراع ذو الطابع الالكتروني في القرن الحادي والعشرين.

ومما سبق فإن مَشْكَلة «Problématisation» هذا الموضوع من هذه الزاوية يمكننا من فهم تطور مفهوم الحرب الذي تولّد جراء التزاوج بين الفكر الاستراتيجي وثورة تكنولوجيات المعلومات والاتصالات، وبالتحليل هذه الدراسة ستُبيّن الاتجاهات البحثية التي تعتبر أو تناقض كون الفضاء السيبراني كساحة للمعركة في هذا القرن، ووفق هذا تأتي دراستنا حاملة الإشكال التالي:

الإشكالية: هل سيكون الفضاء السيبراني التحول التكتيكي القادم في طبيعة الحرب في القرن الحادي والعشرين؟

تسعى هذه الدراسة إلى تسليط الضوء على هذا المجال (الفضاء السيبراني) ومحاولة استكشاف وتحديد معالم الحروب التي تدار فيه.

اعتمدت الدراسة على المنهج الوصفي التحليلي وفق هذا المنهج سندرس وبالتحليل تحولات الحرب من طابعها التقليدي إلى السيبراني، كون الفضاء السيبراني ساحة تدار فيها تلك الحروب، ومن خلال هذا التحليل واستقراء الوقائع الجزئية (المنهج الاستقرائي) وترتيبها داخل نسق ينتهي إلى آليات للتنفيذ من شأنها أن تسهم في تقديم الحلول الملائمة للمشكلة محل الدراسة.

كما تعتمد الدراسة أيضا على المنهج التاريخي للضرورة البحثية، والمنهج المقارن لضرورة المقارنة بن أنماط الفعل ورد الفعل لدول متعددة من خلال إبراز حجم التأثير والتأثر من دولة لأخرى في أوروبا.

كما سنقارب الدراسة وفق طروحات النظرية الواقعية التي أخذت من القوة بعدا أساسيا في منظارها الابستيمولوجي، وكذا طروحات الأمن الموسع بناء على تطور التهديدات وضرورة بناء منظار أمني جديد تتخطى حيثياته مفهوم الامن التقليدي غير القابل للتعامل مع الحقائق الجديدة للبيئة الأمنية.

1- الفضاء السيبراني: تأصيل مفاهيمي

بالرجوع الى عام 1982، وهو تاريخ ظهور هذا المصطلح، صاغ كاتب الخيال العلمي ويليام جيبسون William Gibdon تصورا غريبا: "هلوسة جماعية يشترك فيها مليارات المشغلين يوميا، في كل دولة.. كتمثيل للبيانات المستخلصة من بنوك المعلومات في جميع اجهزة الكمبيوتر في العالم"

ولتسمية هذه الفكرة، جمع جيبسون كلمة "السبرنطيقا" Cybernetics (التي تعني علم التحكم الآلي) مع كلمة "الفضاء" Space، وسك منهما مصطلح "الفضاء السيبراني" Cyberspace الذي أصبح حقيقة مع انتشار شبكة الإنترنت على نطاق العالم[1].

فالفضاء السيبراني (Cyberspace) إذن مصطلح حديث، ظهر نتيجة لثورة تكنولوجيا المعلومات. ويشمل جميع الحواسيب والمعلومات التي بداخلها والأنظمة والبرامج والشبكات المفتوحة لاستعمال الجمهور العام أو تلك الشبكات التي صممت لاستعمال فئة محددة من المستعملين ومنفصلة عن شبكة الإنترنت العامة[2]، فـ "الفضاء السيبراني" هو العالم المادي والمفاهيمي الذي توجد فيه جميع هذه الأنظمة[3].

فيما عرّفت الوكالة الفرنسية لأمن أنظمة الإعلام Agence Nationale de Sécurité des Systèmes d'information (والتي تعد وكالة قطاعية للدولة مكلفة بالدفاع السيبراني الفرنسي) الفضاء السيبراني على أنه "فضاء التواصل المشكل من خلال الربط البيني لمعدات المعالجة الآلية للمعطيات الرقمية".

يمكن القول أن هذا التعريف جاء مركزا على الجانب التقني للفضاء السيبراني، إذ يولي الاعتبار إلى "التجهيزات" و"الأتمتة"، وأن البعد الفضائي ناتج عن الربط البيني العالمي، في حين أن البناء نجده يتمخض عن عاملين: أحدهما تقني(ربط بيني) وثانيهما (جغرافي)، مما يجعل هذا التعريف مشمول بمأخذ عدم استيعابه من عموم الجمهور[4].

وفق هذا فالفضاء السيبرنيتي هو وطن جديد لا ينتمي إلى الجغرافيا ولا إلى التاريخ، وهو وطن دون حدود، ودون ذاكرة، ودون تراث، إنه الـ "وطن الذي تبنيه شبكات الاتصال المعلوماتية الإلكترونية، الفضاء السيبرنيتي (Cyberspace) نسبة إلى"السيبرنيتيك" وهو العلم الذي يدرس طرق سيلان المعلومات ومراقبتها عند الكائنات الحية وداخل الأجهزة الآلية والمنظومات الاجتماعية والاقتصادية[5].

فالعالم أصبح يعتمد أكثر فأكثر على الفضاء الإلكتروني لاسيما في البنى التحتية المعلوماتية العسكرية والمصرفية والحكومية إضافة إلى المؤسسات والشركات العامة والخاصة[6]. واليوم، أصبح من المستحيل تقريبا سبر أغوار مركزية الفضاء السبراني بالنسبة إلى نمط الحياة في العالم. فجميع مجالات الأنشطة اليوم – بدءا من التجارة، إلى الاتصالات إلى البنية التحتية الحساسة التي تغذي حضارتنا

الحديثة وتحميها – تعتمد على التشغيل المأمون والآمن لهذه الشبكة المعولمة[7]. كما تجدر الإشارة الى أنه ومن عام 2000 إلى 2010 ، زاد استخدام الإنترنت العالمي من 360 مليون إلى أكثر من 2 مليار شخص[8].

وعليه يمكننا القول إن الفضاء السيبراني يعتبر مجالاً حيوياً وجيوستراتيجياً يُخاض فيه العديد من الحروب والهجمات الرقمية، وهو مجال مركّب يشمل عدداً من العناصر هي: أجهزة الكمبيوتر، أنظمة الشبكات والبرمجيات، حوسبة المعلومات، نقل وتخزين البيانات[9]، ومستخدمو كل هذه العناصر وعليه فمسألة تحديد مفهوم (الفضاء السيبراني)، هي مسألة نسبية تتوقف على طبيعة إدراك وفهم كل دولة لأمنها القومي.

2- نشأة الهجمات السيبرانية:

ترتبط الهجمات السيبرانية مباشرة بحدثين مهمين:

الأول باستحداث أجهزة الكمبيوتر في منتصف الخمسينيات من القرن المنصرم كأداة لمعالجة وحفظ المعلومات رقميا، وقد تطورت بصورة جذرية في العقود اللاحقة، حتى أصبح جهاز الكمبيوتر، أساسا في عمل الكثير من المؤسسات الخاصة والعامة، فضلا عن الحياة اليومية للأفراد.

أما الحدث الثاني فهو بظهور الشبكة العنكبوتية والذي أحدث انقلابا مثيرا في حياة البشرية من خلال التواصل ونقل المعلومات بسرعة فائقة عن طريق سيل البيانات المرسلة عبر الأثير.

وفي سياق متصل، يصف البعض أن الثورة المعلوماتية الحالية هي بمثابة الجيل الثالث للثورات التقنية التي غيرت في أسلوب الحياة وإمكانيات البشرية، وبعبارة أخرى الثورتان الزراعية والصناعية وأخيرا الثورة المعلوماتية.

هذا وقد سارعت الدول في وتيرة استخدام الكمبيوتر لتحقيق قفزات نوعية في المجال الأمني والعسكري، وذلك في مطلع التسعينيات من القرن المنصرم حتى أطلق البعض عليها مصطلح الحرب السيبرانية الباردة(Cyber Cold War) أو سباق التسلح السيبراني (Cyber Arms Race).

وفي بادئ الأمر لم يكن للهجمات السيبرانية صدى على المستوى الدولي، إذ نشأت أولا على هيئة جرائم طالت المؤسسات المالية والمصرفية، فضلا عن الشركات المتخصصة ببرمجة نظم الاتصالات[10]. هذا وقد تعددت التهديدات عبر الانترنت من التهديد بالقتل لشخصيات سياسية إلى التهديد بتفجيرات في مراكز سياسية ثم بإطلاق فيروسات لإتلاف الأنظمة المعلوماتية في العالم[11].

كما يمكن أن تتخذ الجهات المهاجمة في الفضاء الإلكتروني أشكالًا عديدة بما في ذلك الأفراد أو الكارتلات الإجرامية أو الإرهابيين أو الدول القومية. في الوقت الذي يتخذ فيه المهاجمون أشكالاً كثيرة، فإنهم يسعون جميعاً إلى استغلال نقاط الضعف الناتجة عن تصميم أو تنفيذ البرامج والأجهزة والشبكات والبروتوكولات لتحقيق مجموعة واسعة من التأثيرات السياسية أو الاقتصادية. كما يزيد اعتمادنا على الفضاء الإلكتروني كذلك من نطاق الضرر الذي يمكن أن تفرضه الجهات الفاعلة الخبيثة[12].

في بداية الثمانينيات ارتبطت الهجمات السيبرانية بعمليات اقتحام نظم الحاسوب عن بعد، ونشر الفيروسات عبر شبكات الكمبيوتر الأمر الذي سبب تدمير الملفات والبرامج، حينها شاع اصطلاح (الهاكر) المعبر عن مقتحمي النظم، وبقي الحديث دائما عن دوافع هذه الهجمات محصورا في اختراق أمن المعلومات وإظهار التفوق التقني لمرتكبي تلك الأفعال، لكن بتزايد خطورة هذه الممارسات أصبح من الضروري إعادة تصنيف الفاعلين وتحديد طوائفهم ولا سيما بعد تحول تلك الهجمات من مجرد مغامرة إلى أفعال ممنهجة تستهدف التجسس والاستيلاء على البيانات الاقتصادية، الاجتماعية، السياسية والعسكرية.

فيما شهدت فترة التسعينات تطورا هائلا في مجال الهجمات السيبرانية وتغيرا في نطاقها ومفهومها، بفعل ما أحدثته شبكة الانترنت من تسهيل لعمليات دخول الأنظمة واقتحام شبكات المعلومات حينما أصبحت مواقع الانترنت أكثر عرضة للهجمات التي ظهرت بسببها أنماط جديدة من الهجمات؛ مثل تعطيل النظام التقني ومنعه من القيام بعمله المعتاد الذي يتسبب بانقطاع النظام عن الخدمة لساعات، فنتج عنه خسائر مالية كبيرة قدرت بالملايين، وقد توسعت جرائم نشر الفيروسات عبر الانترنت؛ لما تسهله من وصول الى ملايين المستخدمين في الوقت نفسه، ليفتح الباب على مصراعيه لمختلف الأفعال غير السوية المتطورة بتطور التقنية، وقد سجّلت عبر هذه المراحل مجموعة من القضايا، منها: قضية (موريس الشهرية) سنة 1988 حينما نشر فيروس الكتروني عرف بـ: (دودة موريس) عبر آلاف الكمبيوترات، وفي عام 1990 شهدت الأجهزة هجوما عرف باسم (IP-SPOOFING) أدى إلى إيقاف عمل أجهزة أصلية وأخر ى وهمية، لتبرز قضية (الجحيم العالمي) التي اختص بها مكتب التحقيقات الفدرالية مكنتها من اختراق موقع البيت الأبيض، ومن ثم تلتها الكثير من الحوادث كحادثة شركة أوميغا، وفيروس مليسا، وغيرها من الهجمات السيبرانية.

أما في مرحلة ما بعد التسعينيات وبداية الألفية فقد تطورت هذه الهجمات بنحو أوسع، وتم استخدام المعلومات في الإرهاب المنظم ومن طرف الدول أيضا، من خلال ضرب البنى التحتية للدول الأخرى سواء أكانت مرافق عامة أم خدمات البنى العسكرية والاقتصادية، وغيرها[13].

في سنة 2003 أصدر دان فرنون وهو أحد أعضاء جهاز المخابرات الأمريكي كتابا بعنوان: الثلج الأسود التهديد الخفي للارهاب المعلوماتي Black Ice : the Invisible Threat of Cyber Terrorism عرض فيه يشكل مثير نوع المخاطر التي يمكن أن تهدد العالم في المستقبل القريب، نتيجة اختراق أنظمة المعلومات المتوافرة لدى الحكومات والمؤسسات المالية والشركات الاقتصادية الكبرى، واستخدامها في تدمير البنية التحتية الالكترونية التي تعتمد عليها الدول[14].

وتشير العديد من التقارير إلى تزايد أعداد الهجمات الالكترونية التي تقوم بها مجموعات أو حكومات تتدرج في الاستهداف من أبسط المستويات إلى أكثرها تعقيدا وخطورة.

ففي ديسمبر من العام 2009 أوردت الحكومة الكورية الجنوبية تقريرا عن تعرضها لهجوم نفذه قراصنة شماليين بهدف سرقة خطط دفاعية سرية تتضمن معلومات عن شكل التحرك الكوري الجنوبي والأمريكي في حالة حصول حرب في شبه الجزيرة الكورية.

وفي جويلية 2010، أعلنت ألمانيا أنها واجهت عمليات تجسس شديدة التعقيد لكل من الصين وروسيا كانت تستهدف القطاعات والبنى التحتية الحساسة في البلاد ومن بينها شبكة الكهرباء التي تغذي الدولة.

ويجمع الخبراء على أن الهجوم الالكتروني الذي استهدف استونيا العام 2007، يكاد يكون الهجوم الالكتروني الأول الذي يتم على هذا المستوى ويستخدم لتعطيل المواقع الالكترونية الحكومية والتجارية والمصرفية والإعلامية مسببا خسائر بعشرات الملايين من الدولارات إضافة إلى شلل البلاد، وعلى الرغم من أن الشكوك كانت تحوم حول موسكو على اعتبار أن الهجوم جاء بعد فترة قصيرة من خلاف إستوني-روسي كبير، إلا أن أحدا لم يستطع أن يحدد هوية الفاعل الحقيقي أو مصدر الهجوم الذي تم، وهي من المصاعب والمشاكل التي ترتبط بحروب الانترنت إلى الآن[15].

وفي دراسة بعنوان " لقد بدأ سباق التسلح السيبراني" قام بها كيفين كولمان Kevin Coleman الباحث في معهد Technolytics يقول فيها: أن الصراع بين استونيا وروسيا كان مجرد قمة جبل الجليد في الحرب السيبرانية. واصفا الصراع الذي وقع في أفريل وماي من عام 2007. بـ :حرب إلكترونية في ذروتها تم إطلاق أكثر من 4 ملايين معاملة وهمية في الثانية ضربت الأهداف المرجوة منها[16].

وإلى يومنا هذه تبقى عملية Stuxnet الضّربة الإلكترونية الأمريكية لأجهزة الطّرد النّووية الإيرانية من خلال جرثومة أو دودة افتراضية في أوائل عام 2011 سميت بـStuxnet والعمليات التي استهدفت جورجيا في حربها مع روسيا هي الأكثر تعقيدًا في سياق حروب السايبر. وبالطبع أتى رد إيران سريعًا من خلال استهداف مصالح أمريكية وصهيونية كاستهداف شركة أرامكو في الخليج[17].

في عام 2014 أجرت كوريا الشمالية هجومًا إلكترونيًا ضد شركة Sony Pictures Entertainment، مما جعل الآلاف من أجهزة كمبيوتر سوني غير صالحة للعمل، وتم اختراق المعلومات التجارية السرية للشركة. بالإضافة إلى الطبيعة المدمرة للهجمات، سرقت كوريا الشمالية نسخًا رقمية لعدد من الأفلام التي لم يتم إطلاقها، بالإضافة إلى آلاف المستندات التي تحتوي على بيانات حساسة تتعلق بالشخصيات الشهيرة وموظفي شركة Sony. رافقت كوريا الشمالية هجماتها الإلكترونية بالإكراه والتخويف والتهديد.

كان هجوم كوريا الشمالية على سوني واحدًا من أكثر الهجمات الإلكترونية تدميراً على أي كيان أمريكي حتى الآن. أدى هذا الهجوم إلى مزيد من النقاش حول طبيعة التهديد السيبراني والحاجة إلى تحسين الأمن السيبراني[18].

هذا وقد كانت سنة 2017 بمثابة دعوة للاستيقاظ المقلق لوقائع الصراع السيبراني. خاصة وأن البلدان والمجرمين على حد سواء قد أظهروا أكبر قدر من الاستعداد لإطلاق العنان للفوضى لعملياتهم

على الإنترنت[19]، بهذا أصبح الفضاء السيبراني مجالا للصراع والتنافس يستخدمه الفاعلون من الدول ومن غير الدول للتعبئة والحشد والتنظيم والدعاية[20].

3- الحرب السيبرانية: الانتقال من فضاء حقل المعركة إلى الفضاء السايبيري:

عرفت الحرب، كما هو حال باقي الأمور الإنسانية تحولات وتغيرات كانت في بعض الأحيان قوية لدرجة يمكن اعتبارها منعطفات أو منعرجات، تغير لم يطل فقط استراتيجياتها وتكتيكاتها، وإنما طال شكل الحرب وأسلحتها[21]، جراء ثورة المعلومات والابتكارات التنظيمية، التغيير حدث أيضا في طبيعة الصراع وأنواع الهياكل والعقائد والاستراتيجيات العسكرية التي ستكون ضرورية في هذه الحرب.

1- تحولات الحرب:

أدى التصنيع إلى حرب الاستنزاف من قبل الجيوش الضخمة (الحرب العالمية الأولى على سبيل المثال). ومن ثَمَّ المكننة التي أدت إلى مناورات تغلب عليها الدبابات (على سبيل المثال الحرب العالمية الثانية). في حين تشير ثورة المعلومات إلى ظهور الحرب السيبرانية، حيث من يعرف أكثر، يمكنه أن يشتت ضباب الحرب .

تشير الحرب السيبرانية إلى أنها ستنمو أكثر بشكل مساعد للإستراتيجية العسكرية الشاملة. وبهذا المعنى، فإن ثورة المعلومات قد تنطوي على تأثيرات شاملة تستلزم إجراء تعديلات جوهرية على التنظيم العسكري ووضع القوة. قد تكون الحرب السيبرانية في القرن الحادي والعشرين بمثابة الحرب الخاطفة في القرن العشرين.

في حين أن الحرب الإلكترونية تشير إلى الصراع المرتبط بالمعرفة على المستوى العسكري، تنطبق الحرب المعلوماتية على الصراعات المجتمعية التي غالباً ما ترتبط بالنزاعات المنخفضة الكثافة من قبل جهات غير تابعة للدولة، مثل الإرهابيين أو كارتلات المخدرات أو مؤيدي أسلحة الدمار الشامل في السوق السوداء. ويعني كلا المفهومين أن الصراعات المستقبلية ستخاض أكثر في "الشبكات" أكثر من "التسلسلات الهرمية"، وأن أي شخص يتقن العمل على تشكيل-إعادة تشكيل الشبكة سيكتسب مزايا رئيسية[22]. لأنه وفي معادلة التهديدات الأمنية الجديدة يكون الطرف المستهدف قابلا للعطب بشكل بالغ الحساسية؛[23] بسبب الانتشار الواسع لمصالحه في هذا الفضاء.

لن نتوقف طويلا أمام مسألة التعريفات، وإنما سنستخدم التعريف الذي طرحه ريتشارد كلارك وهو الآن التعريف المعتمد في المعاهدات الدولية في هذا الشأن، حيث يعتبر ريتشارد حرب الفضاء الالكتروني على أنها تعني: اختراق شبكة أو حاسوب دولة أخرى اختراقا غير مصرح به بواسطة حكومة ما، أو نيابة عنها، أو دعما لها، أو أي نشاط آخر يؤثر على نظام حاسوبي بغرض إضافة أو تغيير أو تزييف البيانات، أو التسبب في تعطيل جهاز حاسوب أو إتلافه، أو تعطيل أو إتلاف جهاز متصل بشبكة أو الأشياء التي يتحكم فيها نظام الحاسوب[24].

في ضوء هذا التعريف الإنترنت أصبحت أحدث ساحة معركة في العالم، والشاهد على هذا تلك المناوشات التي اندلعت بين الولايات المتحدة والصين والتي دارت رحاها على الإنترنت. وقعت هذه

المناوشات الإلكترونية في صيف عام 2007، هددت الصين بتكثيفها إلى حرب سيبرانية كاملة. فيما قلل بعض قادة الأمن السيبراني الأمريكي من خطورة الأمر، في حين أعرب الخبراء الدوليون عن قلقهم بشأن التبادل عبر الإنترنت.

وقد أكدت هذه الأحداث على ضعف نظم المعلومات والتحكم في الولايات المتحدة في الهجمات السيبرانية. فحذر تقرير صدر في جويلية 2007 أمام الكونغرس الأمريكي من أن جمهورية الصين الشعبية تخلق هجمات على شبكة الإنترنت يمكن أن تسبب "اضطرابات وفوضى" من حجم أسلحة الدمار الشامل. وأفادت وزارة الأمن الداخلي أن الهجمات ضد الولايات المتحدة ارتفعت بما يقرب من 900٪ بين عامي 2005 و2007. وذكرت مصادر أخرى أن وزارة الدفاع الأمريكية تواجه حوالي3 ملايين هجوم على الشبكات والأنظمة يوميًا، بعد هذه الحادثة كرست إدارة بوش الابن 6 مليارات دولار لتطوير دفاعات للبنية التحتية المعلوماتية الحكومية[25].

ولمواجهة هذا التهديد، حاولت أميركا وحلفاؤها توسيع نطاق عملياتهم الدفاعية الخاصة للحيلولة دون القرصنة الحكومية وإحباطها. التي استهدفت أنظمتها بنجاح من قبل بكين وطهران في الماضي، فبدأت بتعزيز إستراتيجيتها السيبرانية، مع خطط تطوير أسلحة سيبرانية يمكن استخدامها داخل وخارج ساحة المعركة.

تحت هذه الظروف خزان تفكير خاص يسمى TASC (مؤسسة العلوم التحليلية) يقوم بالعمل على عقيدة المعلومات في مجال الدفاع ضد أمريكا، والى هذا الحد الكثير من المناقشات العقائدية لا زالت تركز على تفاصيل الحرب الالكترونية- تدمير وتعطيل رادار معاد، وتلويث حاسباته بواسطة فيروسات، واستخدام رسائل أخرى لخداعه.

إنها تحدد قيادة وسيطرة الحرب باستخدام مدمج لأمن المعلومات، الخداع العسكري، العمليات النفسية والحرب الالكترونية والتدمير الفيزيائي، المدعم بالمخابرات لحرمات المعلومات وتحط من قدر أو تدمير قدرات القيادة والسيطرة لتنفيذ ضربة قاضية قبل بداية العدوان التقليدي[26].

وترجع أهمية الحروب السيبرانية إلى طبيعة الفضاء الالكتروني وخصائصه وما يترتب عليه من أثار أدت إلى بروز التهديدات التي تختلف جوهريا عن التهديدات التقليدية، إذ يتسم الفضاء السيبراني بغياب الحواجز المكانية والزمانية. فالمسافات الطبيعية ما بين الدول عادة ما تؤدي إلى وجود حواجز متعلقة بالوقت والأبعاد الجغرافية، والتي تقيد من العمليات العسكرية التي قد تقوم بها إحدى الدول ضد دولة أو دول أخرى، سواء في البر أم البحر. هذه الحواجز المادية والزمنية تمكن الطرف المتعرض للهجوم من التحضير للدفاع أو القيام بأعمال وقاية.

كما أن هذه الهجمات التقليدية عادة ما تسبقها تدابير يمكن ملاحظتها، كتجهيز الجيوش، تحضير نظام التسليح، أو حتى الإعلان بشكل مباشر عن النية في الهجوم. ومن ثم تتمكن الأطراف المتعرضة للهجوم من اتخاذ التدابير اللازمة لصد الهجوم أو تجنب الخسائر. وعلى العكس من ذلك، تغيب الحواجز

الجغرافية والزمنية كلية في الفضاء الالكتروني، ومن ثم تكون الحروب الالكترونية غير مقيدة بالحدود الجغرافية إلى جانب عدم قدرة الهدف على كشف الهجوم قبل وقوعه أو حتى الاستعداد له[27].

أصبحت الجيوش العسكرية في أنحاء العالم كافة تهتم بحرب المعلومات ودورها في حروب المستقبل، ووضع عدد من دول العالم إستراتيجية تهدف إلى تحقيق الأمن الالكتروني ضمن خططها الأمنية والدفاعية للمحافظة على مصالحها الاقتصادية، السياسية، العسكرية، وظهرت مناورات يتم إجراؤها للتدريب على مثل هذا النوع الجديد من الصراع وكيف يمكن مواجهته والاستعداد له. ففي الصين هناك تدريب ميداني للجيش الصيني يستخدم تقنيات متطورة، ويمكن توقع استخدامها الفضاء الالكتروني لمهاجمة أعدائها في حالة أي قتال ينشب في المستقبل.

وظهر الارتباط بين تكنولوجيا الاتصال والمعلومات والحرب بجميع أنواعها في شكل تطوير للفكر النمطي في شن الحرب ووسائلها فيما يطلق عليه الثورة في الشؤون العسكرية وحروب المستقبل. (28)

2- أسباب انتشار الحرب السيبرانية:

دفعت عدة عوامل إلى تصاعد توظيف عدد متزايد من الدول أو حتى الفواعل المسلحة من دون الدول للحرب السيبرانية في تفاعلاتها العدائية، وهو ما يمكن إجماله في العناصر التالية:

- ضعف بنية الشبكات المعلوماتية وقابليتها للاختراق:

حيث إن شبكات المعلومات مصمّمة بشكل مفتوح دون حواجز أمنية عليها، رغبة في دخول المستخدمين، ويمكن للدول أو المنظمات الإرهابية استغلال الثغرات المتواجدة في الأنظمة والشبكات المعلوماتية بهدف التسلل إلى البنى المعلوماتية التحتية لأي دولة اخرى وتخريبها[29]، إذن فالبيئة التي ترتكب فيها الحرب السيبرانية تعمل أيضًا على تفسير انتشار الظاهرة[30].

- دعم العمليات العسكرية التقليدية:

الحرب السيبرانية يمكن توظيفها إلى جانب "العمل العسكري الحركي" من أجل زيادة تداعيات العمليات العسكرية على الخصم، فقد حذر وزير الدفاع الأمريكي الأسبق ليون إدوارد بانيتا Leon Edward Panetta عام 2012 من مخاطر التهديدات السيبرانية، واعتبر أن السيناريو الكارثي بالنسبة لواشنطن، هو قيام دولة بشن حرب سيبرانية تستهدف البنية التحتية الحرجة[31] في الولايات المتحدة بالتزامن مع قيامها بشن ضربة عسكرية ضدها[32]، بهذا فالهجمات السيبرانية غير الحركية قد يكون لها عواقب حقيقية على القوات في ساحة المعركة[33]، فالترابط بينها و بين الهجمات العسكرية الحركية في تزايد، على سبيل المثال: استهداف المنشآت السيبرانية عسكرياً باستخدام صاروخ أو طائرة، فضلا عن إمكانية شن هجمات سيبرانية ضد الأسلحة الحركية مثل منظومات الصواريخ مثلا، Kinetic Weapons وهو ما قد يؤدي إلى تطور المواجهات بين الدول إلى مواجهات عسكرية شاملة غير محسوبة العواقب.

- زيادة اعتماد الدول على الفضاء السيبراني:

فقد عمدت الدّول إلى توظيف الفضاء السيبراني في العديد من الاستخدامات المدنية والعسكرية على حد سواء. وتقوم الدول المتقدمة، مثل الولايات المتحدة، بربط الأنظمة المسؤولة عن توجيه وإدارة

البنية التحتية الحيوية بالشبكات الإلكترونية، وهو ما يزيد من احتمالية اختراقها، في ضوء صعوبة تأمين الدّولة بصورة كاملة من التهديدات السيبرانية، وذلك على الرغم من إنفاق الدّول مليارات الدولارات لتأمين هذه المنشآت.

وعلى الجانب الآخر، شرعت الدول في الاعتماد على منصات الذكاء الاصطناعي في أنظمتها التسليحية، وهو ما اتضح في توسع الجيوش في الاعتماد على "الأنظمة القتالية ذاتية التشغيل" Lethal Autonomous Weapons systems كالدرونز والدبابات الموجهة عن بعد. ويحذر العديد من الخبراء من إمكانية اختراق هذه المنظومات التسليحية، والسيطرة عليها سواء من جانب الدول المعادية أو الفواعل المسلحة من دون الدول، وتوجيهها لتنفيذ ضربات عسكرية ضد الدولة المالكة لها، أو حتى استهداف المدنيين.

- سهولة الحصول على الأسلحة السيبرانية:

حيث يمكن العثور على السلاح السيبراني بسهولة من خلال "الإنترنت المظلم "، كما Dark Web أن تكلفة الحرب السيبرانية منخفضة مقارنة بغيرها من وسائل القتال التقليدية. فشن الحرب السيبرانية لا يحتاج إلى قدرات دولة، بل إلى مجموعة صغيرة من الأفراد، بل وفي بعض الأحيان فرد واحد، إذا ما امتلك الخبرات المناسبة لذلك.

- غموض هوية الطرف القائم بالهجوم:

إذ أن عدم القدرة على تحديد هوية منفذ الهجوم السيبراني قد يغري الدول إلى التوسع في استخدامها في دفاعاتها العدائية، وهو ما قد يدفع الدول المتضررة إلى توجيه عمليات انتقامية ضد الدولة التي تشتبه في أنها استهدفتها، وهو ما قد يؤدي إلى تصعيد حدة المواجهات بين الدولتين، وانتقالها من المجال السيبراني إلى مجالات الحرب الأخرى (البر والبحر والجو والفضاء)[34].

4- تسليح الفضاء الالكتروني:

في الأول من تشرين الأول/ أكتوبر 2009 تولى أحد جنرالات الجيش ترأس هيئة عسكرية جديدة بالولايات المتحدة تعرف بقيادة حرب الفضاء الالكتروني، مهمتها استخدام تقنيات المعلومات والانترنت كسلاح للحرب. وجدير بالذكر أن هناك قيادات مماثلة في كل من روسيا والصين وعشرات الدول الأخرى، حيث تقوم هذه المؤسسات العسكرية والاستخباراتية بتجهيز ساحة حرب الفضاء الالكتروني بما يطلق عليه "القنابل المنطقية logic bombs" و"ثغرات التسلل trapdoors"، ووضع متفجرات افتراضية في الدول الأخرى في وقت السلم. ونظرا للطبيعة الفريدة لحرب الفضاء الالكتروني، فإنها قد تشجع على المبادرة إلى شن الهجوم(35)، وأكثر الأهداف المحتملة التي قد تتعرض لها هي الأهداف ذات الطبيعة الحيوية عن طريق استخدام عديد البرامج/الأسلحة سنأتي على شرحها في هذه الجزئية:

1- الأسلحة السيبرانية وتغير معنى العنف:

يرى كلاوزفيتز أن كل عصر يخوض الخروب بأساليبه الخاصة، وهذا ما يفسر لنا أن لكل زمن من أزمنة الحرب سماته المميزة له(36)، فالحروب السيبرانية صراع يستخدم معاملات أو هجمات معادية غير

قانونية على الحواسيب والشبكات في محاولة لتعطيل الاتصالات وغيرها من البنى التحتية كآلية لإلحاق الضرر الاقتصادي، والسياسي وكذا العسكري، ويتعاون خبراء التكنولوجيا والإستراتيجيون العسكريون والمخططون المدنيون على تصميم استراتيجيات الحرب السيبرانية لعرقلة عمليات الدفاع الهجومية والدفاعية والدفاع عنها. حددت مدرسة الدراسات العليا البحرية The Naval Postgraduate School ثلاثة مستويات من القدرات السيبرانية الهجومية.

- **بسيطة غير منظمة:**

القدرة على إجراء الاختراقات الأساسية ضد الأنظمة الفردية باستخدام أدوات تم إنشاؤها بواسطة شخص آخر.

- **هيكلية متقدمة:**

القدرة على شن هجمات أكثر تطوراً ضد أنظمة متعددة وربما لتعديل أو إنشاء أدوات أساسية.

- **مركبة منسقة:**

القدرة على شن هجمات منسقة قادرة على إحداث تعطيل شامل ضد العديد من أنظمة الدفاع.

باستخدام مزيج من المستويات المذكورة أعلاه، تظهر خطط الحرب السيبرانية وتزيد من الحاجة إلى مجموعة واسعة من الأسلحة السيبرانية(37) CYBER WEAPONS التي يتم توظيفها عبر الفضاء الالكتروني، وهي عبارة عن تطوير وسائل لتعطيل الكمبيوترات الأساسية الداعمة للبنية التحتية الوطنية(38)، وتشمل الأسلحة السيبرانية المستخدمة من أجل تحقيق الأهداف الجيوسياسية مجموعة كبيرة من الأدوات مثل تلك المتعلقة بالمراقبة، والتجسس، والتضليل، أو الهجمات المدمرة. ويمكن تقسيم الهجمات السيبرانية إلى نوعين:

- الاختراقات التي تستهدف جمع المعلومات (التجسس الرقمي).
- الهجمات على الأنظمة الأجنبية لإيقاف شبكات الخصوم أو إتلافها، مثل الهيئات الحكومية والأهداف الرمزية والبنية التحتية الحيوية.[39]

2- التغير في مفهوم القوة: ظهور مفهوم القوة السيبرانية Cyber power:

في الفترات السابقة، كان تقدير موارد قوة الدولة أسهل. فكان من بين الاختبارات التقليدية لقوة عظمى في السياسة الدولية قوتها في الحرب، ولكن مع مرور القرون وتطور التقنيات، تغيرت مصادر وأشكال ومفاهيم القوة في الحرب كثيرا، وتوزيع القوة في عالم المعلومات المعاصر يختلف كثيرا بالنسبة لقضايا مختلفة[40]، ففي الحروب الهجينة Hybrid Warfare تعتمد الدول على أشكال مختلفة من القوة، والتي تتمثل في الأسلحة العسكرية التقليدية، مثل الأسلحة المضادة للأقمار الصناعية، وصواريخ كروز والصواريخ الباليستية العابرة للقارات، بالإضافة إلى القدرات اللامتماثلة مثل توظيف الجماعات الإرهابية والحرب السيبرانية[41].

يقول "ولتر رستون Walter Wriston": "إنَّ ثورة المعلومات قد غيرت عالمنا، بحيث أصبح العلم والتكنولوجيا، المحركان بشكل واضح للتاريخ والعلاقات الدولية، وأيضاً ما يسمَّى بسلطة الدولة". وهو ما

جعل بعض الدول تسعى في المُضيّ قدماً لاستغلال القوة السيرانية في مضاعفة قوتها في النظام الدولي، خاصةً أنَّ القوة السيبرانية تتميز بقلة تكلفتها، واعتمادها على مهارات العقل البشري، مقارنة بتكاليف باهظة للقوة التقليدية الأخرى[42].

لقد دار النقاش، ولا يزال، حول طبيعة القوة في المجال السيبراني، أهي قوة صلبة، أم ناعمة، أم ذكية، من دون أن يتم التوصل إلى توصيف دقيق لهذه الطبيعة، هذا فضلا عن الخلاف القائم حول تعريف القوة بحد ذاتها[43]. ويتوسع النقاش ليشمل كذلك التباين في وجهات النظر حول عديد النقاط نبرز أهمها في:

- التحول في مفهوم القوة العسكرية:

أحدث هذا التطور تحولاً كبيًرا في مفهوم القوة ترتب عليه دخول المجتمع الدولي في مرحلة جديدة تلعب فيها هجمات الفضاء الإلكتروني دورًا أساسيًّا سواء في تعظيم القوة أو الاستحواذ على عناصرها الأساسية، وأصبح التفوق في مجال الفضاء الإلكتروني عنصرًا حيويًّا في تنفيذ عمليات ذات فاعلية في الأرض وفي البحر والجو والفضاء. واعتماد القدرة القتالية في الفضاء الإلكتروني على نظم التحكم والسيطرة.

- صعود القوة الإلكترونية في الشئون الدولية:

دخل المجال الإلكتروني ضمن المحددات الجديدة للقوة من حيث طبيعتها وأنماط استخدامها وطبيعة الفاعلين، وإنعكاس ذلك على قدرات الدول وعلاقاتها الخارجية، وتعلقت الخصائص الجديدة للقوة "بأنها مجموعة الوسائل والطاقات والإمكانيات المادية وغير المادية، المنظورة وغير المنظورة التي بحوزة الدولة، يستخدمها صانع القرار في فعل مؤثر يحقق مصالح الدولة، وتؤثر في سلوك الوحدات السياسية الأخرى."

- تعريف جديد لمفهوم القوة في العلاقات الدولية:

ويعرف "جوزيف ناي" مفهوم القوة الإلكترونية بأنها تشير إلى "مجموعة الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات والشبكات الإلكترونية والبنية التحتية المعلوماتية والمهارات البشرية المدربة للتعامل مع هذه الوسائل."

- عناصر القوة الإلكترونية:

و ترتكز على وجود نظام متماسك يعظم من القوة الناتجة عن التناغم بين القدرات التكنولوجية والسكان والاقتصاد والصناعة والقوة العسكرية وإرادة الدولة وغيرها من العوامل التي تسهم في دعم إمكانيات الدولة على ممارسة الإكراه، أو الإقناع أو ممارسة التأثير السياسي على أعمال الدول الأخرى، أو على الحكام في العالم بغرض الوصول للأهداف الوطنية من خلال قدرات التحكم والسيطرة على الفضاء الإلكتروني...

- تصاعد دور القوة الناعمة:

إلى جانب إمكانية استخدام الحروب السيبراية لشن هجمات تخريبية ضد الخصم فهناك أيضا قدرات في مجال استخدام القوة الناعمة عبر نشر المعلومات المضللة والحرب النفسية والتأثير في توجهات الرأي العام ، والنشاط السري والاستخباراتي[44].

3- العمليات العسكرية في الفضاء السيبراني:

وفقا لـ هربرت ريموند ماكماستر H. R. McMaster مستشار الأمن القومي في البيت الأبيض و جاري كوهن Gary Cohn مدير المجلس الاقتصادي الوطني فإن العالم ليس "مجتمعًا دوليًا"، بل معتركًا تنخرط فيه الدول والجهات غير الحكومية الفاعلة والشركات، وتتنافس فيه؛ بحثًا عن التفوق على غيرها " وتابَعَا بِقَوْلِهما: "بدلًا من إنكار هذه الطبيعة الأساسية للشؤون الدولية، فإننا نعتنقها". وباستبدال كلمة "العالَم" بكلمة "الفضاء السيبراني"، يتضح توجُّه الدول الكبرى نحو مناصرة الهيمنة على الفضاء السيبراني من خلال عسكرة هذا الفضاء[45]، هذا وتختلف العمليات ذات الطابع العسكري في الفضاء السيبراني حسب قوة الدولة وتوجهاتها، ويمكن تصنيف العمليات العسكرية في الفضاء السيبراني في أربع فئات منفصلة ذات أربعة أهداف:

- عمليات جمع المعلومات الاستخباراتية:

وتهدف إلى جمع المعلومات من بيانات العدو الالكترونية.

- عمليات تستهدف المعنويات:

بهدف إلحاق الضرر بالروح المعنوية وإرادة القتال لدى شعب العدو من خلال الدعاية والتضليل المعلوماتي، وغير ذلك من تقنيات حرب المعلومات.

- عمليات هجومية:

وتستهدف إلحاق الضرر ببيانات العدو وشبكاته الالكترونية أو تعطيلها، و/أو إلحاق المزيد من الضرر المادي بأفراد العدو أو عتاده، على سبيل المثال إضعاف دفاعات العدو الالكترونية (مثل شبكات الدفاع الجوي).

- عمليات دفاعية:

هدفها حماية البيانات الالكترونية والشبكات الخاصة بالدولة والحيلولة دون إلحاق الضرر بالشعب والممتلكات[46].

تجدر الإشارة إلى أن التأثير الأولي للعمليات العسكرية في الفضاء السيبراني على شبكات العدو بشكل مؤقت، والمنطق العسكري يدعوا إلى هجوم مكمل بالآلات للاستفادة من ارتباك العدو وشلله. فبدون هجوم لتدمير أو الاستيلاء على ما تم إيقاع الفوضى فيه، سيقوم العدو بكل بساطة بإصلاح موقفه والعودة إلى الهجوم، وبالتالي فإن المعركة الالكترونية تعزز الاتجاه إلى الهجوم، وميزة عنصر المفاجأة. وللأسف فإن هذا الأسلوب من شأنه فقط أن يعزز فرص تصعيد الأزمات إلى حروب وأن يجعل من فرضية كبح الحروب أكثر صعوبة[47].

5- إعادة صياغة مفهوم المنافسة العسكرية:

أشار دونالد رامسفيلد Donald Rumsfeld، وزير الدفاع الأمريكي السابق، إلى أن"التحدي الذي يواجهنا في هذا القرن الجديد تحدّ صعب، انه يتمثل في الدفاع عن أمتنا ضد المجهول، غير المؤكد وغير المنظور وغير المتوقع" . لقد أصبحت هذه اللغة علامة بارزة في عصر المخاطر.

يضيف رامسفيلد: "يتعين علينا التخلي عن طرائق التفكير والتخطيط المريحة، أن نُقْدم على المخاطر ونجرب أشياء جديدة". إن الحرب تتطور بشكل يواكب هذا التحدي، وتتم إعادة معايرة الإقدام على المخاطر على أدق نحو ممكن، فقواعد الحرب اليوم تختلف عن تلك التي عهدناها خلال الحرب الباردة[48]، هذه التطورات أحدثت طفرة إبستيمولوجية Epistemological Mutation في الدراسات العسكرية وأدت بالباحثين لإعادة صياغة مفهوم جديد للمنافسة العسكرية، مفهوم يتماشى وضرورات العصر، فالحروب في القرن الحادي والعشرين الأسلحة فيها متاحة بسهولة، كما تشهد انطماس الخطوط الفاصلة بين التكنولوجيا العسكرية والتكنولوجيا المدنية، وتصاعد عدد النزاعات المرتبطة بالمال والسلع والأفكار أكثر من ارتباطها بالأراضي كما كان في السابق، الأمر الذي مهد الطريق للمنافسة المفرطة في مجال الحرب والأمن. وكحال الأحزاب السياسية الرئيسية، أو المؤسسات الصناعية والمصرفية العملاقة، تواجه المؤسسات العسكرية الكبرى منافسين جددا لم تعد توقفهم حواجز الدخول التقليدية.

وفي هذا المشهد المبعثر تظل المؤسسة العسكرية التقليدية مهمة ومؤثرة، فهي تملك مزايا الموارد العامة والقدرة على جعل نفسها الأولوية القصوى في الميزانيات الحكومية، كما أن السيادة الوطنية تعطيها الثقل المعنوي الذي يجتذب المجندين ويسوّغ الاستثمار والإنفاق، والشرعية السياسية للدخول في تحالفات. إن لديها تقليدا يعزز مكانتها غير أنها فقدت تفرّدها وطابعها الاحتكاري. وهناك نوعان حاسمان من الاحتكار – أحدهما فلسفي والآخر عملي – قد تلاشيا وكشفا عن نقاط ضعف المؤسسة العسكرية التقليدية، الاحتكار الأول هو احتكار الدولة الفلسفي للاستخدام المشروع للقوة. والاحتكار الثاني هو احتكار عملي يتمتع به الجيش بسبب التنافس الجيوسياسي بين الدول ذات السيادة والحاجة إلى تكنولوجيا أكثر تطورا للفوز في هذا التنافس.

إن صعود الجهات الفاعلة من غير الدول وانتشار التكنولوجيا الخطر والسريع إلى ساحات تتجاوز عالم المتخصصين قد حطّما ركائز تلك الميزة. واليوم تحاول الجيوش الوطنية أن تتكيف – بسرعات ونتائج مختلفة – مع طيف كامل من الحروب التي أصبحت فيها الأسلحة رقمية بقدر ماهي مادية، والأساليب نفسية بقدر ما هي قسرية، والمقاتلون مدنيين ومبعثرين بقدر ما هم رسميون ونظاميون.

كما أن النزاعات التنافسية المفرطة لا تعني بالضرورة حروبا أكثر أو أسوأ من ذي قبل، سواء قيست بالخسائر في الأرواح أو فقدان المنافع الاقتصادية، كما أنها لا تشير، بأي حال، إلى نهاية الجيوش الوطنية، ولكنها تضع ما يمكن أن يُتَوقّع من الجيش الوطني تحقيقه من منظور جديد[49].

6- من التوازن الاستراتيجي العسكري إلى التوازن الاستراتيجي المعلوماتي:

كانت الحكومات بطيئة في التكيف مع كون الفضاء السيبراني ساحة معركة، ومن الواضح أن قراصنة الحاسوب ومهاجمي الإنترنت يتمتعون بمجال حركة واسع من حيث الفرص المتاحة لهم لتعطيل الوظائف الحكومية الحرجة. ولا شك في أن الوقت يمثل عاملا جوهريا في هذا الصدد: "إن البقاء في وضع متقدم مقارنة بقراصنة الانترنت أمر مهم في ضوء تغيير السرعة المربك في عالم الانترنت"، على حد قول عاموس يادلين Amos Yadlin رئيس شعبة الاستخبارات بالجيش الإسرائيلي سابقا: "إن الاستجابة للتغيير تتطلب بضعة أشهر على الأكثر، مقارنة بالسنوات التي كانت متوافرة للطيارين".

ويشير المفكر العسكري أركويلا إلى أن التأخير في إجراء التعديلات اللازمة للبقاء على قيد الحياة في مسرح الحرب الجديد المبعثر ليس بالضرورة خطأ العقول العسكرية. وكتب أركويلا في عام 2010 " لكن كبار القادة سوف يميلون إلى الاستسلام لقدر نابع من اعتقادهم أن قادة الكونغرس وقادة القطاع الصناعي سوف يحبطون أي محاولة لإحداث أي تغيير جذري"[50].

إن الانعكاس للتحول من النظريات الخاصمة بالتدمير الشامل يجعل الرجل العسكري اليوم يكرر أقوال سان تزو Sun Tzu الشهيرة: "إن تحقيق مائة انتصار في مائة معركة ليس ذروة المهارة، إن هزيمة العدو بدون قتال هو قمة المهارة" ومع ذلك فإن هذه التكنولوجيا غير الفتاكة مبعثرة وغير مدمجة وخارج إطار المعرفة العسكرية التي تركز أساسا على قتل العدو. إن المطلوب، إعادة تفكير كاملة في الحرب[51].

من كل ما سبق ندرك أن ما سيتحقق من تحولات بعيدة المدى بفعل الثورة المعلوماتية المعرفية من شأنه أن ينقل قريبا علاقات توازن القوى من مرحلة التوازن الاستراتيجي العسكري إلى مرحلة التوازن الاستراتيجي المعلوماتي.

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، 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[52].

وهكذا الى مدى أوسع بكثير فإن التبني النظري للموضوع مؤسس على عمل عالمين في مؤسسة راند RAND في سانتامونيكا بكاليفورنيا Californie -Santa Monica هما دافيه رونفلت David Ronfeldt، وجون اركيلا John Arquilla، ففي نظرية عامة إبتدائية عما يسمونه حرب التحكم الآلي أو الحرب السيبرانية CYBER WAR يلمحون إلى مسائل إستراتيجية عريضة، أنها تعني التحول إلى توازن المعلومات والمعرفة لصالح القوى الصديقة خاصة إذا لم يكن التوازن في القوات غير متزن.

ومع ذلك فإن أشياء محددة قد تكون واضحة، إن أي إستراتيجية عسكرية عليها أن تقوم بأربع وظائف هامة على الأقل بخصوص المعرفة. فيجب عليها أن تحصل على (وتعالج وتوزع وتحمي) المعلومات، وهذا مفتاح لغالبية الانتصارات العسكرية للغد، إضافة إلى أن البرامج SOFTWARE تغير التوازن

العسكري في العالم، خاصة أن نظم التسليح يتم حملها بواسطة ما يطلق عليه المنصة PLATFORMS[53] التي تعتمد بالدرجة الأولى على منظومة معلومات جد متطورة.

الصراع السيبراني العالمي يشتد وقد يصل إلى نزاع بين الدول، فدول مثل روسيا وكوريا الشمالية وإيران تستخدم الهجمات الإلكترونية لزيادة مجال نفوذهم[54]، في حين شرعت الولايات المتحدة الأمريكية والصين في مباحثات ثنائية رسمية بخصوص الفضاء السيبراني في عام 2013، إلا أن الصين أوقفت هذه المباحثات في 2014، بعد إدانة الولايات المتحدة لخمسة ضباط بجيش التحرير الشعبي لتجسسهم الإلكتروني على أهداف تابعة للولايات المتحدة، رغم التخلي عن نهج مجموعة العمل الثنائية المختصة بالفضاء الإلكتروني (Cyber Working Group)، جرت بالفعل مباحثات بشأن الفضاء الالكتروني في الحوار الاستراتيجي والاقتصادي الثنائي صيف 2015، وتصدر الاتفاق المبدئي للمضي قدما في القضية قائمة النتائج التي عقدت بين تشي جين بينغ Xi Jinping وباراك أوباما Barack Obama في واشنطن في سبتمبر 2015. رغم ذلك، تبقى أسئلة جوهرية حول العلاقة بين الدولتين فيما يخص الفضاء السيبراني، ففي غياب مجموعة معايير وإجراءات تفصيلية كاملة لضبط الأنشطة المثيرة للقلق وقواعد رأسية خاصة به، ستستمر المشكلة في تشكيل خطر كبير على العلاقة الثنائية وعى السلام والاستقرار الإقليميين وعلى النظام العالمي أيضا[55].

يقول ديفيد كين David Keen في كتابه حرب بلا نهاية: وظائف خفية للحرب على الإرهاب "في ظل هذه الظروف تصبح محاولة تطبيق النموذج العسكري القديم أشبه بمحاولة دق الماء بمطرقة، أو قتل فيروس برصاصة"[56]، لهذا وجب مراعاة هذا التطور على مستوى التهديدات وخلق توازن استراتيجي في الفضاء السيبراني بآليات حديثة تتماشى والأسلحة السيبرانية التي تملكه الدول الأخرى وتسعى لتطويرها.

الخاتمة:

من خلال البحث في الفضاء السيبراني كساحة للمعركة في القرن الحادي والعشرين خلصت الدراسة إلى أنه ومثل عديد الظواهر؛ غيرت تكنولوجيا المعلومات والاتصالات ظاهرة الحرب أيضا، وبفعل هذه التطورات برز البعد الالكتروني كأحد مصادر الصراع، وبات الفضاء الالكتروني من أبرز مساحاته. وعليه، بدا الفضاء السيبراني وبأوجه مختلفة ساحة جديدة للصراع، حيث يمكن تبادل الهجمات وتنفيذ الأعمال العدائية متفاوتة الشدة بين الخصوم أسوة بباقي المجالات: البحر، البر، الجو، والفضاء الخارجي.

هذا وقد توصلت الدراسة إلى عدد من الاستنتاجات التي نلخص أبرزها كما يأتي:

الاستنتاجات:

في المجال السيبراني، توارت الحروب التقليدية كثيرا وراء الحروب التي تعتمد على التقنية حيث يقدم الفضاء السيبراني لصانعي السياسات مجالا رحبا حول كيفية التفكير في قضية أمنية مستحدثة.

الفضاء السيبراني اخرج للعلن العديد من التهديدات ووضع السعي التقليدي نحو القوة موضع تشكيك.

تمثل الحروب السيبرانية مدخلًا جديدًا على نطاق الصراع الذي يمتد عبر أشكال اقتصادية وسياسية واجتماعية وعسكرية "للحرب".

قد تثير الحرب السيبرانية قضايا واسعة تتعلق بالتنظيم والعقيدة العسكريين، بالإضافة إلى الإستراتيجية والتكتيكات وتصميم الأسلحة. قد تكون قابلة للتطبيق في النزاعات المنخفضة والعالية الشدة، في البيئات التقليدية وغير التقليدية، ولأغراض دفاعية أو هجومية.

إن قوة المؤسسات العسكرية التقليدية وبفعل التغيير الفعلي في مشهد الأمن الدولي سوف تكون أقل مما كانت عليه في الماضي.

أصبحت الجيوش العسكرية في أنحاء العالم كافة تهتم بحرب المعلومات ودورها في حروب المستقبل، ووضع عدد من دول العالم إستراتيجية تهدف إلى تحقيق الأمن الالكتروني ضمن خططها الأمنية والدفاعية للمحافظة على مصالحها الاقتصادية، السياسية، العسكرية.

إن الهجمات مثل تلك التي عطلت الخدمات المصرفية عبر الإنترنت في استونيا والمواقع الإلكترونية الحكومية في جورجيا ، وكذلك دودة Stuxnet التي أغلقت برنامج إيران النووي بشكل مؤقت، هي أمثلة حية لما يمكن تحقيقه في هذا المجال الاستراتيجي الجديد.

التحولات التي شهدتها الحرب في ظل الثورة في الشؤون العسكرية مع تلك التي كانت في الأجيال السابقة للحرب، شكلت مخاطر تصاعدية خطيرة، لأن الاستخدام المتزايد للأسلحة السيبرانية يذكي التوترات التي قد تؤدي إلى إشعال صراعات تقليدية جديدة، والتي بدورها يمكن أن تعرض الاستقرار الدولي للخطر.

المعركة الالكترونية تعزز الاتجاه إلى الهجوم. وللأسف؛ فإن هذا الأسلوب من شأنه فقط أن يعزز فرص تصعيد الأزمات إلى حروب وأن يجعل من فرضية كبح الحروب أكثر صعوبة.

تكاليف دخولها المنخفضة نسبياً وفرص النجاح العالية تجعل الأسلحة السيبرانية وسيلة اختيارية للجهات الفاعلة الحكومية وغير الحكومية لتأكيد سلطتها، وإظهار قوتها، وإثبات قدراتها في الفضاء السيبراني.

من كل ما سبق ندرك أن ما سيتحقق من تحولات بعيدة المدى بفعل الثورة المعلوماتية المعرفية من شأنه أن ينقل قريبا علاقات توازن القوى من مرحلة التوازن الاستراتيجي العسكري إلى مرحلة التوازن الاستراتيجي المعلوماتي.

الهوامش:

(1) بيتر سينجر، دروس الحروب الماضية والاتجاهات التكنولوجية المستقبلية، الحروب المستقبلية في القرن الحادي والعشرين، ط 1، مركز الإمارات للدراسات والبحوث الإستراتيجية، 2014، ص 83.

(2) محمود محارب، إسرائيل والحرب الالكترونية، قراءة في كتاب حرب في الفضاء الالكتروني: اتجاهات وتأثيرات على إسرائيل، سلسلة مراجعة كتب صادرة عن المركز العربي للأبحاث ودراسة السياسات، 2011، ص 1.

(3) حمدون توريه، الفضاء السيبراني وتهديد الحرب السيبرانية، البحث عن السلام السيبراني، الاتحاد الدولي للاتصالات، جانفي 2011، ص ص 9-12.

(4) بلفرد لطفي أمين، الفضاء السيبراني: هندسة وفواعل، المجلة الجزائرية للدراسات السياسية، 5، جوان 2016، ص ص 145-.155

(5) كلثوم زينب، مبدأ التواصل مرجعية الأدب الرقمي بين التكنولوجي والفكر الفلسفي، مجلة مقاليد، العدد 3، ديسمبر2012، 161-176.

(6) علي حسين باكير، المجال الخامس.. الحروب الإلكترونية في القرن الـ21، مركز الجزيرة للدراسات، تم تصفح المقال يوم 14-02-2017. https://goo.gl/2fC3WM

(7) بيتر سينجر، مرجع سابق، ص 83.

(8) Department of Defense Strategy for Operating in Cyberspace, July 2011, p 1. Book online , available from https://goo.gl/ksfKzW

(9) محمود عزت، الفضاء السيبراني وتحديات الأمن المعلوماتي العربي، مقال من موقع المجلة العربية، تم تصفح الموقع يوم 16-04-2018. https://goo.gl/CK54yS

(10) أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، المجلد8، عدد4 ، 2016، ص 610-688.

(11) أمير فرج يوسف، مكافحة الإرهاب الالكتروني: الإرهاب الرقمي في ظل اتفاقية دول مجلس التعاون الخليجي، دار الكتب والدراسات العربية، 2016، ص 253.

(12) The National Strategy to Secure Cyberspace, February2003, p 28. Book inline, available from https://goo.gl/dSvVfM

(13) مجيد غالب العداوي، الأمن المعلوماتي السيبراني، مركز البيان للدراسات والتخطيط، (أوت 2016)، ص ص 4-5.

(14) حسنين المحمدي بوادي، إرهاب الانترنت الخطر القادم،ط1 ، دار الفكر الجامعي، 2002، ص 111.

(15) فيصل محمد عبد الغفار، الحروب الالكترونية، الجنادرية للنشر والتوزيع، 2015 ، ص ص 11– 13.

(16) Kevin Coleman, The Cyber Arms Race Has Begun , JAN 28.2008, accessed 2018-06-06, available from https://goo.gl/xKcvK4 .

(17) د.ذ.ك، حرب المعلومات في سياق الحروب اللامتماثلة، مقال من موقع باب الواد، تم تصفح الموقع يوم 10-05-2018. https://goo.gl/DMSzWn.

(18) Department of Defense Cyber Stratigy, Department of Defense, April 2015, p 2. Book online, available from https://goo.gl/g4hpuA.

(19) Justin Ling, "2018 will be the year of cyberwar", MACLEANS, December ,2017, accessed avril 26 , 2018, Available from :https://goo.gl/28iSfz.

(20) شيرين فهمي، مراجعة كتاب الإرهاب الالكتروني: القوة في العلاقات الدولية، مجلة النهضة، م. 11، ع.4 (أكتوبر 2010)، ص ص 196-203.

(21)زهير اليعكوبي، الحرب مقاربة فلسفية سياسية، ط 1(الجزائر: منشورات ضفاف، 2016)، ص 161.

(22)John Arquilla & David Ronfeldt , Cyberwar is coming!, Comparative Strategy, Volume 12, Issue 2,1993, pp 141-165.

(23) عامر مصباح، نظريات التحليل الاستراتيجي والأمني للعلاقات الدولية، ط1، دار الكتاب الحديث، 2010، ص 22.

(24) ريتشارد إيه كلارك، روبرت كيه كنيك، حرب الفضاء الالكتروني الخطر القادم على الأمن القومي وسبل المواجهة، ط 1، مركز الإمارات للدراسات والبحوث الإستراتيجية، 2012، ص 267.

(25) Kevin Coleman, op.cite.

(26) الفين توفلر، مرجع سابق، ص 188.

(27) نوران شفيق، أثر التهديدات الالكترونية على العلاقات الدولية دراسة في أبعاد الأمن الالكتروني، ط1، المكتب العربي للمعارف،2016، ص 8.

(28) عادل صادق، استخدام الإرهاب الالكتروني في الصراع الدولي، ط 1، دار الكتاب الحديث، 2015، ص 100.

(29) مصطفى يوسف كافي ،ماهر عودة الشمايلة، الإعلام والإرهاب الالكتروني، ط1، دار الإعصار العلمي للنشر والتوزيع، 2015، ص 151.

(30) Edward Mercer, Causes of Cyber Crime, it still works web cite, accessed avril 26 , 2018, available from https://goo.gl/JY3tYj.

(31) تعرف البنية التحتية الحرجة في قانون الولايات المتحدة الأمريكية الوطنية بأنها "تلك الأنظمة والأصول، سواء المادية أو الافتراضية الحيوية للغاية بالنسبة للولايات المتحدة ، فعجز أو تدمير هذه النظم والأصول سيكون له تأثير موهن على الأمن الاقتصادي الوطني، الصحة العامة الوطنية أو السلامة، أو أي مجموعة من هذه القضايا " انظر:

United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism, USA PATRIOT ACT, 2001, pp. 107-56. Available from: https://goo.gl/1s2HDU

(32) سرحات شوبوأوجلو، تزايد استخدام الأسلحة السيبرانية في الصراعات الدولية، اتجاهات الأحداث، نوفمبر 2017، ص 59.

(33) Todd South, New cyber weapons are here and no one is prepared, experts say, Army Times, 25-01-2019. available from https://goo.gl/pJVVfk.

(34) سرحات شوبوأوجلو، مرجع سابق، ص 59.

(35) ريتشارد إيه كلارك، روبرت كيه كنيك، مرجع سابق، ص ص 8-9.

(36) كريستوفر كوكر، الحرب في عصر المخاطر، ط 1، مركز الإمارات للبحوث والدراسات الإستراتيجية، 2011، ص 9.

(37) Kevin Coleman, The Cyber Arms Race Has Begun, op.cit.

(38) عادل صادق، مرجع سابق ، ص ص99-102

(39) عادل رفيق، الجيوبوليتكس السيبرانية والاستقرار في الشرق الأوسط، المعهد المصري للدراسات، تم تصفح الموقع يوم 27-04-2018 https://goo.gl/Fzq8jW

(40) جوزيف ناي، القوة الناعمة وسيلة للنجاح في السياسة الدولية،تر محمد توفيق البجرمي، ط1، العبيكان للنشر، 2007، ص ص 22-23.

(41) David J.Betz and Tim Stevans, cyberspace and the state: Toward a Strategy for Cyber power, New York : Routledfe , 2011, p 75 book online, available from https://goo.gl/u6wYx4.

(42) عمرو صبحي، تكتيك الدِرع والسيف في استخدام القوة السيبرانية، مقال من موقع المركز العربي للبحوث والدراسات، تم تصفح الموقع يوم 26-04-2018 https://goo.gl/Z8KQ7Y

(43) أنديرا عراجي، القوة في الفضاء السيبراني: فصل عصري من التحدي والاستجابة، رسالة لنيل دبلوم الدراسات العليا في العلوم السياسية والإدارية بكلية الحقوق والعلوم السياسية والإدارية بالجامعة اللبنانية، 2015-2016 ، ص 2.

(44) عادل عبد الصادق، خطر الحروب السيبرانية عبر الفضاء الالكتروني، مقال في موقع لغة العصر، تم تصفح الموقع يوم 12-05-2018 https://goo.gl/e3Nm3q

(45) Steven Aftergood, Cybersecurity: The cold war online, nature international journal of science, accessed 12-11-2018, available from: https://goo.gl/Xc73sw

(46) جون باسيت، حرب الفضاء الالكتروني: التسلح وأساليب الدفاع الجديدة، الحروب المستقبلية في القرن الـ 21، ط 1، مركز الإمارات للدراسات والبحوث الإستراتيجية، 2014)، ص 57.

(47) عبد الكريم محمود برم، مرجع سابق، ص 451

(48) كريستوفر كوكر، مرجع سابق، ص 10.

(49) موسى نعيم، نهاية عصر القوة من قاعات اجتماعات مجالس الإدارة إلى ساحات الحرب والكنائس إلى الدول لماذا لم يعد تولي المسؤولية كما كان في السابق؟، ط1، مركز الإمارات للدراسات والبحوث الإستراتيجية، 2016، ص ص 183- 184.

(50) موسى نعيم، المرجع نفسه، ص ص 186-187.

(51) ايدين و هايدي توفلر، مرجع سابق، ص 183.

(52) عادل عبد الصادق، أنماط الحرب السيبرانية وتداعياتها علي الأمن العالمي، ملحق اتجاهات نظرية، مجلة السياسة الدولية، تم تصفح الموقع يوم 10-05-2018. http://www.siyassa.org.eg/News/12072.aspx

(53) ألفين توفلر، مرجع سابق، ص ص 187-189.

(54) Craig cohen and Melissa G .Dalton, Global Forecast 2016, Center of Strategic and International Studies, 2015, pp 148.

(55) سكوت وارين هارولد وآخرون، التوصل إلى اتفاق مع الصين بشأن الفضاء الالكتروني، تقارير مؤسسة راند، 2016، ص ص 8-9.

(56) ديفيد كين، حرب بلا نهاية ؟ وظائف خفية للحرب على الإرهاب، تر معين إمام، العبيكان للنشر، ط1،2008، ص 12.