الحروب السيبرانية : تحول في أساليب القتال وثبات في المبادئ والأهداف

Cyber wars : a shift in fighting methods and stability in principles and goals

حنان دريسي*، كلية العلوم السياسية والعلاقات الدولية، جامعة الجزائر3

hanane.drissi@yahoo.com

تاريخ إرسال المقال: 2022/02/08 تاريخ قبول المقال: 2022/04/24 تاريخ نشر المقال: 2022/05/12

الملخص:

تركز هذه الدراسة على مفهوم الحرب السيبرانية و التي ساعدت على تطورها مجموعة من العوامل و التحولات التكنولوجية التي شهدها العالم في السنوات الماضية، و تسعى الى ابراز الابعاد الاستراتيجية و الواقعية لهذه الحرب، التي تختلف مع الحروب التقليدية في اساليب القتال و تتفق معها في المبادئ و الاهداف.

كما تسعى الدراسة الى بيان مدى تأثير الحروب السيبرانية على العلاقات الدولية عامة و الأمن القومي للدول على وجه الخصوص.حيث تحمل الحروب السيبرانية في طياتها العديد من مواطن الهشاشة و قابلية شديدة للعطب ما يشكل تهديدا حقيقيا للأمن القومي للدول.

الكلمات المفتاحية : الحرب السيبرانية–الفضاء السيبراني–الأمن القومي–العلاقات الدولية.

Abstract:

This study focuses on the concept of cyber war whose development has been promoted by a group of factors and tecnological transformations that the world has witnessed in thepast years, and seeks to highlight the strategic and realistic dimensions of this war wich differ with traditional wars in fighting methods and agree with them in principles and objectives.

The study also seeks to show the extent of the inpact of cyber wars on international relations in general and the national security of countries in particular,where cyber wars carry with it many vulnerabilities and high vulnerability wich poses a real threat to the national security of countries.

Key words : cyber war-cyber space-national security-international relations

.

*المؤلف المرسل

المقدمة:

تعتبر الحرب ظاهرة اجتماعية رافقت البشرية على مرّ العصور، بحيث يرى العديد من علماء الإجتماع أنها حتمية لا بد من حدوثها، و تراها بعض نظريات العلاقات الدولية حالة طبيعية نظرا لإختلاف إرادات و توجهات الأفراد أو الدول أو الكيانات المشكلة للنظام العالمي، و في بعض الأحيان تتقاطع هذه الإرادات ليحدث الصدام أو الحروب، فأخذت هذه الأخيرة في التطور مواكبة للتطور التقني و التكنولوجي الذي تشهده البشرية، و عرفت في كل جيل من أجيالها أساليب و تقنيات جديدة في القتال و استراتيجيات تزاوج بين التراكمات و الخبرات السابقة و التطور التقني الذي تشهده المرحلة التي تندلع فيها.

و في مجال التكنولوجيا و المعلومات و الرقمنة عرف العالم موجة جديدة من الحداثة نتيجة للثورة المعلوماتية الهائلة حتى أصبح العصر الحالي يسمى بعصر المعلومات أو الموجة الثالثة للتطور البشري– حسب ألفن توفلر– و قد رافق هذه الطفرة ظهور جيل جديد من الحروب يعتمد على المعلومة و التقنية و التفوق التكنولوجي. و لكن بالرغم من التغير في أساليب القتال، إلا أن حروب عصر المعلومات أو ما يسمى بالحروب السيبرانية لا زالت تحتفظ بالمبادئ و الأهداف التقليدية للحرب.

الحروب السيبرانية يمكن ان تكون الفيصل و عامل حاسم في العديد من الصراعات التي سيشهدها العالم بين مختلف وحدات النظام الدولي المتنافسة، لكن بالرغم من الميزة التي تمنحها الحروب السيبرانية للطرف الذي يتحكم فيها، إلا أنها في نفس الوقت تحمل في طياتها العديد من مواطن الهشاشة مما يضعها تحت طائل الاختراق الإلكتروني و الهجمات السيبرانية ما يشكل تهديدا مباشرا لأمنها القومي.

المشكلة البحثية : الهدف من خلال هذه الدراسة هو الإجابة على المشكلة البحثية التالية : فيما تختلف الحروب السيبرانية عن الحروب التقليدية و كيف تؤثر على الأمن القومي للدول؟.

فرضيات الدراسة :

1. كلما زاد اعتماد الدول على التكنولوجيات الحديثة و الرقمنة في تسيير شؤونها، زادت لديها القابلية للإختراق الإلكتروني.

2. تعكس الحروب السيبرانية رهانات التنافس الدولي.

منهج الدراسة :

اعتمدنا في هذه الدراسة على المنهج الوصفي التحليلي بهدف تحديد العلاقة التأثيرية بين متغيرات الدراسة.

1.ثورة المعلومات في الشؤون العسكرية :

ساهمت ثورة المعلومات في تحسين الحياة البشرية و نقلها إلى العصرنة و الرقمنة، كما ساهمت الإكتشافات التكنولوجية الناتجة عنها في إعطاء بعد عسكري لهذه الثورة. حيث أصبحت المعرفة توظف في إنتاج الدمار من خلال ابتكار الأسلحة الشد فتكا و الأكثر تطورا لضمان الفعالية في الضربة، و عليه فقد

جاءت الثورة المعلوماتية في الشؤون العسكرية لتغير من أساليب القتال و تطوره بما يتماشى و الإكتشافات التكنولوجية المتوصل إليها في عصر المعلومات.

جادل " ألفن توفلر" في تحليله للثورة في الشؤون العسكرية أن التطور في الاقتصاد المدني يصاحبه تطور في الاقتصاد العسكري و يمثل أساسا في التقليل من التضخيم في الآلات و التقليل من الخسائر أيضا، من خلال الدقة في إصابة الهدف أي أن الأسلحة أصبحت مبنية على المعلومات لا على الحجم[1].

أشارت الكثير من الدراسات و التحاليل العسكرية في علم الإستراتيجية الى أن ثورة المعلومات في الشؤون العسكرية هي أمريكية بامتياز كنتيجة للتطور غير المسبوق في جمع و معالجة و توزيع المعلومات بين الوحدات القتالية بواسطة تكنولوجيا المعلومات المتقدمة، و أكثر تجلياتها وضوحا شبكة الأنترنت التي تتدفق عبرها المعلومات بحجم غير مسبوق في مجال الاتصالات، ليس للجيش الأمريكي فقط و إنما أيضا للقوات الحليفة و المؤسسات العالمية و المجتمعات عبر العالم. لاشك في أن كل ثورة كانت استجابة أو رد فعل لتحديات قاسية واجهت القوات المسلحة فوق أرض المعركة، و حالت دون ربحها لحرب أو قلصت من الفعالية القتالية للقوات المسلحة[2].

وتعود أصول الثورة في الشؤون العسكرية إلى إسهامات الفكر العسكري السوفياتي لمرحلة الحرب الباردة و التي كانت تشير آنذاك إلى التطور التكنولوجي العسكري الذي وصل إليه المعسكر الغربي بقيادة الولايات المتحدة الأمريكية، مما يحتم على المعسكر الشرقي بقيادة الإتحاد السوفياتي مجاراة هذا التطور. كما ساهم المذهب الماركسي – اللينيني من خلال فكرة التغيير الثوري في ترسيخ دعائم الثورة في الشؤون العسكرية من خلال أعمال المنظرين السوفيت و تحليلهم للتقنيات العسكرية في الحرب العالمية الأولى و الثانية، و قد لاحظوا أن الحرب الخاطفة الألمانية Blitz Kreig أثبتت إمكانية حدوث تغييرات جذرية في كيفية القيام بالحرب التي تحولت من الطابع الستاتيكي الجامد في الحرب العالمية الأولى إلى الطابع الديناميكي السريع القائم على المناورة و سرعة تحريك الجيوش في الحرب العالمية الثانية[3].

انَّ الاستعمال الفعلي لمصلح " الثورة في الشؤون العسكرية " كانت في أوائل التسعينات في الدوائر العسكرية الأمريكية، بحيث كان يشير إلى التحول الجذري في طبيعة الحرب الحديثة و الذي تجسد فعليا في حرب الخليج الثانية التي اعتبرها العديد من الاستراتيجيين على أنها بداية حقبة جديدة في المجال العسكري، حيث أوضح "ألفن توفلر" أن الثورة في الشؤون العسكرية هي ان تضع المعرفة في قلب القوة و أن توظف أقوى ما وصلت إليه التكنولوجيا في قلب المعركة و هو الجديد الذي جاءت به عاصفة الصحراء 1991 كالضربة الدقيقة بعيدة المدى و التكامل بين صنوف القوات البرية و البحرية و الجوية و إصابة مراكز الثقل الإستراتيجي للعدو بصفة مباشرة.

2.حرب المعلومات :

أدى السعي إلى اكتساب المعلومة إلى جعل هذه الأخيرة مصدرا للصراع الذي تجلى في حروب المعلومات و التي تركز أساسا على تدمير النظم المعلوماتية للعدو، مما يؤدي إلى إصابته بالعطب، و في نفس الوقت الحماية الذاتية من العمليات المماثلة، و إنجر عن هذه الحروب تهديدات تتمثل في إمكانية اختراق الأمن القومي للدول نظرا لارتباط منظوماتها الأمنية و قواعد بيانات مؤسساتها السياسية و الإقتصادية بتكنولوجيات الحاسوب و الشبكات الإفتراضية التي صارت مسرحا للهجمات و الجرائم الإلكترونية المسببة لخسائر كبيرة التكاليف.

تُعرف حرب المعلومات (Information Warfare) على أنها تخريب المعلومات أو تدميرها أو سرقتها أو تحريفها، أو إساءة استخدامها أو المنع من الوصول إليها، أو تقليل موثوقيتها، أو استخدامها ضد أصحابها و حماية الذات و القوات الصديقة من عمليات مماثلة[4].

إن الهدف الأساسي وراء حرب المعلومات يكمن في تعجيز العدو و إصابته بالشلل الإستراتيجي أي "القابلية للعطب" عن طريق تدمير نظم الحاسوب و شبكات الاتصال و قواعد البيانات الخاصة به و بنيته الأساسية و مؤسساته الإستراتيجية و ذلك باستخدام فيروسات و ديدان الحاسوب (Worms)، و برامج التجسس و القنابل المثبتة في مواقع محددة، و في نفس الوقت حماية الذات و القوات الصديقة من العمليات المماثلة الصادرة عن العدو و بواسطة منظومات الدفاع الإلكترونية و برامج المنع و الوقاية[5].

و على غرار الحروب التقليدية، فإن لحرب المعلومات أبعادا هجومية و دفاعية تتمثل في :

1.1عمليات هجومية (Offensive Operations):

الهدف منها مهاجمة نظم المعلومات الطرف العدو سواء لأسباب عسكرية أو سياسية أو إقتصادية أو لمجرد الإثارة و إظهار القدرات و شن حرب نفسية على الخصم.

1.2 عمليات دفاعية (Defensive operations):

و تشمل جميع الوسائل المعلوماتية الوقائية المتوفرة للحد و التقليل من أعمال التخريب التي قد تتعرض لها نظم المعلومات، و تتضمن وسائل الدفاع أربع مجالات هي[6]:

- المنع و الوقاية: أي حماية نظم المعلومات منذ البداية قبل التعرض للهجوم.
- التحذير و التنبيه: أي التنبؤ بحدوث الهجوم قبل وقوعه من خلال تفعيل أنظمة الإنذار المبكر.
- كشف الإختراقات و التعامل معها قبل وقوعها.

و تستمد حروب المعلومات تأثيرها و فعاليتها من العديد من الخصائص، فهي حروب ذات طابع أكثر شمولا و تستهدف جميع نظم المعلومات المتصلة بتكنولوجيا الحاسوب و الرقمنة و البرمجيات عبر العالم، إضافة إلى الفجوات و المخاطر المرافقة لها، بحيث تحمل هذه الحروب أشكالا جديدة من التهديدات أهمها إمكانية التعرض للإختراق و إصابة البنى التحتية و مؤسسات الدولة المرتبطة بتكنولوجيات الحاسوب و

الشبكات و هو ما ينجر عنه قابلية شديدة للعطب،و تهديدا حقيقيا للأمن القومي للدول. بالإضافة إلى البعد النفسي و السيكولوجي من خلال إرباك العدو و جعله في حالة من التوتر و الشلل غير قادر على المواجهة من جراء الأعطاب التي تمس مراكز ثقله الإستراتيجي.

3.الفضاء السيبراني : ساحة جديدة للصراع الإفتراضي

يعتبر الفضاء السيبراني(Cyberspace) مجالا جديدا للحروب التقليدية (البر، البحر و الجو)، بحيث يختلف في الخاصة البنيوية (كونه افتراضا) و فواعله و التفاعلات الجارية فيه عن سابقيه. غير أن مخرجاته و تأثيراته تنعكس على الواقع مباشرة، و لا تختلف عن تلك التي نجدها في الحروب التقليدية، حتى و إن اختلف معها في الأساليب و الكيفيات، إلا أن لديه ثبات في المبادئ و الأهداف من حيث إكراه العدو و تدمير إراداته على القتال و المواجهة المباشرة.

يقوم القضاء السيبراني كميدان افتراضي على المعلومات و الرقمنة و تكنولوجيات الحاسوب و الاتصال، و قد تشكل نتيجة التطور التكنولوجي و التقني و الثورة المعلوماتية التي نقلت البشرية من المجتمع الصناعي إلى المجتمع المعلوماتي، فهو مجال افتراضي يحتضن مجموعة من التفاعلات التعاونية و الصراعية الهادفة لتحقيق مصالح معينة للفواعل فيه.

يشير المعنى اللغوي لمصطلح الفضاء السيبراني إلى الفضاء القابل للملاحة، و هو مشتق عن الكلمة اليونانية Navigate و التي تعني التنقل، أما المصدر الأصلي للمصطلح فهو Neuromancer و الذي أطلقه "وليام جيبسون" سنة 1984 و يشير إلى مساحة رقمية قابلة للملاحة و التنقل عن طريق أجهزة الكمبيوتر المتصلة بالشبكات. فهو يعني حركية التنقل و الاتصال ضمن بيئة إلكترونية[6].

تعرفه وزارة الدفاع الأمريكية على أنه : "البيئة الإفتراضية التي يتم فيها نقل المعلومات الرقمية عبر شبكات الحاسوب"، و أبرز هذا التعريف الجانب الوظيفي للفضاء السيبراني كونه مجالا لتبادل المعلومات ذات الطابع الرقمي عن طريق وسائط شبكية و مادية (الحاسوب)[7].

كما عرفته وزارة الدفاع اليابانية على أنه تلك المساحة الإفتراضية التي تتضمن شبكات الأنترنت التي يتم فيها تبادل تكنولوجيا المعلومات، فهو البنية التحتية الأساسية التي تحتضن عمليات مختلفة في جميع المجالات في البر و البحر و الجو و الفضاء، و مجالاً يتم فيه القيام بمختلف الأنشطة على غرار الجريمة و التجسس و البيع و الشراء و مختلف أنواع المعاملات، و تشكل هذا المجال نتيجة للنمو و التطور في تكنولوجيا المعلومات و الاتصالات على غرار الحواسيب و الهواتف المحمولة حتى أصبح الفضاء السيبراني جزءا لا يتجزأ من الحياة البشرية[8].

لقد أدى تضاعف عدد المستخدمين و تعدد الفواعل ضمن الفضاء السيبراني إلى تعدد المصالح و الأهداف و تقاطعها، و هو ما صاحبته العديد من التجاوزات التي ترتقي في أغلب الأحيان إلى درجة التهديد، بحيث أدرجت بعض الدول الرائدة في مجال تكنولوجيات الاتصال و الحواسيب أمن الفضاء

السيبراني ضمن أولويات استراتيجياتها الدفاعية نظرا لما تتعرض له من هجمات إلكترونية تمس بأمنها القومي بصفة مباشرة، و بالتالي فإن التطور الرقمي الذي بلغته هذه الدول بات يشكل في نفس الوقت و بالموازاة مع الميزات التي تمنحها هذه التكنولوجيا المتقدمة مصدرا للتهديد الأمني الذي يمس الأشخاص ليصل إلى الدول نظرا لاتصال و ترابط بُناها التحتية و مؤسساتها الحساسة بشبكات الأنترنت القابلة للإختراق.

4.التهديدات الأمنية ضمن الفضاء السيبراني :

في ظل تنامي دور النشطاء و الفاعلين في الفضاء السيبراني تعددت أنواع التهديدات الأمنية التي تمس بأمن الأفراد و الدول، و التي يمكن تحديدها فيما يلي :

1.4الجريمة الإلكترونية (Cyber crime):

تعددت تعريفات الجريمة الإلكترونية نذكر منها: " الجرائم التي تلعب فيها بيانات الكمبيوتر و البرامج المعلوماتية دورا هاماً، أو هي فعل إجرامي يستخدم الحاسب الآلي في ارتكابه كأداة رئيسية[9]".

و جاء في توصيات الأمم المتحدة العاشر لمنع الجريمة و معاقبة المجرمين المنعقدة في فينا سنة 2000 م تعريف الجريمة الإلكترونية كما يلي: " هي أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوبي، و الجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية"[10].

و تأخذ الجريمة الإلكترونية في الفضاء السيبراني منحًا تصاعدياً، حيث أفادت إحصائيات مقدمة من قبل مؤسسة Herjavec Group الكندية المختصة بشؤون الأمن السيبراني بأنها ستكلف العالم ما يقارب 6 ترليون دولار سنويا بحلول العام 2021، و هذا راجع بالدرجة الأولى إلى ارتفاع عدد المستخدمين و مرتادي الشبكات الإلكترونية و مستعملي الحواسيب، حيث من المتوقع أن يصل عدد المستخدمين إلى 6 مليار بحلول العام 2022 و أكثر من 7.5 مليار بحلول العام 2030 [11]، و هذا مؤشر على الإرتفاع المتزايد لنسبة الجريمة الإلكترونية عبر العالم الذي يقابله زيادة الإنفاق العالمي على قطاع تكنولوجيا المعلومات.

كما تتنوع الجريمة الإلكترونية ما بين الجرائم ذات الصلة بالحاسوب المركزة على استغلال الثغرات الإلكترونية للأنظمة المعلوماتية بهدف السرقة أو إتلاف المعلومات أو التجسس عليها دون ترخيص أو علم صاحبها. كما يمكن أن تكون الجريمة الإلكترونية في شكل غسيل أموال أو مختلف الجرائم الاقتصادية التي يرتكبها القراصنة Hackers المتمرسون في تقنيات الاتصال و الحاسوب و التي تشمل مختلف أنواع السرقات و الإبتزاز و التلاعب و التخريب باستخدام هويات زائفة لتفادي المتابعة القضائية بهدف الحصول على الأموال[12].

2.4 الإرهاب السيبراني Cyber Terririsme:

إنّ الإرهاب السيبراني أو الإلكتروني كمفهوم مستحدث يكتنفه الكثير من الغموض، و ذلك أنه يعتمد على تقنية أنظمة المعلومات من حيث وسيلة ارتكابه و من حيث دور الفاعل فيه و طبيعة سلوكه، فضلا عن أن نتائجه تطول أمن المعلومات و تقنية أنظمة المعلومات بالإضافة إلى ما يتسبب به من أضرار واسعة الإنتشار و عظيمة الأثر على المجتمعات و الأفراد.

إنّ أول استخدام لمصطلح "الإرهاب السيبراني" ظهر خلال فترة الثمانينيات في دراسة لـ Berry Collin التي خلص فيها الى صعوبة تعريف الظاهرة بدقة و أيضا الأساليب و الحلول المطلوبة لمواجهته، و تحديد دور الأنترنت في العمل الإرهابي، و خلال فترة التسعينيات صدر تقرير عن الأكاديمية الأمريكية للعلوم عن أمن الكمبيوتر جاء فيه: " نحن بصدد مخاطر متزايدة بسبب اعتماد الولايات المتحدة الأمريكية على أجهزة الكمبيوتر، حيث غدا بإمكان الإرهابيين إحداث تدمير أكبر بالإعتماد على لوحة المفاتيح أكثر من استخدام القنبلة، و قد يتسبب ذلك في بيرل هاربر الكتروني جديد"[13].

يعتبر التعريف الذي قدمه "دورثي دايينج Dorthy Dayang " من أشمل تعاريف الإرهاب السيبراني حيث قال: "إنه إلتقاء و تزاوج الإرهاب مع الفضاء السيبراني، و هو يعني التهديدات غير القانونية ضد الحاسبات الآلية أو الشبكات الإلكترونية و المعلومات المخزنة، و ذلك لإخافة الحكومات أو إجبارها أو حتى الناس على اتخاذ مواقف معينة لتعزيز أهداف سياسية أو إجتماعية، و هو عنف ضد الأفراد أو الممتلكات و يسبب أذى لدرجة كافية لخلق الخوف، و إنعكاساته يمكن أن تسبب خسائر مادية أو إقتصادية و قد تصل إلى بشرية إذا استهدفت العمليات الإرهابية شبكات الصناعة النووية و المصانع الكيميائية"[14].

و تعرّفه وكالة المخابرات المركزية الأمريكية بأنه: "أي هجوم تحضيري ذي دوافع سياسية موجهة ضد نظم معلومات الكمبيوتر و برامجه و البيانات و المعلومات و التي تنتج عن عنف ضد الأهداف المدنية عن طريق جماعات دون قومية أو عملاء سريين"[15].

3.4 التجسس الإلكتروني:

يصنف التجسس الإلكتروني على أنه شكل من أشكال الإرهاب المعلوماتي و هو محاولة الوصول إلى معلومات يخفيها الطرف المستهدف، بحيث يستهدف المتسللون الحصول على معلومات سرية أو غيرها من المعلومات التي قد تكون مربحة أو مفيدة للهاكر، و هي عملية مستمرة تتم عبر مدة زمنية معينة و بدون انقطاع ، تهدف إلى الحصول على معلومات سرّية، و يمكن أن ينجم عنها عمليات إرهابية أو كوارث اقتصادية. و يأخذ التجسس الإلكتروني عدة أشكال و هي كلها أعمال غير شرعية مثل: التصنُت، المعلومات المضللة، الإختراق دون اتصال...

5.الحرب السيبرانية و التحول في أساليب القتال :

يقتضي شرح مفهوم الحرب السيبرانية التطرق له من جوانبه المختلفة، و بالتالي صعوبة رصد تعريف جامع له نظرا لتداخل الإختصاصات و تعدد المقاربات، و عليه وجب التطرق لمجموعة من التعاريف بمختلف مضامينها و الربط بينها لتكوين رؤية واضحة عن المفهوم.

- تعرّف وزارة الدفاع الأمريكية (DOD) الحرب الإلكترونية بأنها: "نوع من أنواع القتال الذي يستهدف النصر من خلال إخضاع الخصم و النيل من إرادته و هزيمته دون أن ينجر عن ذلك سفك للدماء في المجال السيبراني[16]".
- تعرّف الحرب السيبرانية كذلك على أنها عمليات عسكرية ضمن الفضاء السيبراني تحمل طابعاً معلوماتياً و يمكن أن تتخذ ثلاثة أشكال أساسية:
  - ✓ جمع المعلومات الإستخبارية من بيانات العدو و شبكاته حول خططه و كيفية انتشاره و ما ينوي القيام به و التوجهات العامة له.
  - ✓ مهاجمة أنظمة كمبيوتر العدو و بياناته الحساسة خاصة تلك المرتبطة بالمؤسسات و البنى التحتية أو ضرب مراكز الإتصال عنده و جعله عاجزا ممّا يؤدي إلى إضعاف قياداته السياسية و العسكرية.
  - ✓ الدفاع و حماية البيانات الإلكترونية و الشبكات الخاصة بالدولة و الوقوف دون التعرض لها و إتلافها[17].
- و يرى بعض القانونيين أن ديناميكيات عمل الحروب الإلكترونية تتقارب من ناحية قانونية مع إشاعة الرعب و الإرهاب، لذلك يمكن تعريف الحروب الإلكترونية استنادا لهذه النظرة القانونية بأنها: " نظام قائم على الرعب المنتشر في الشبكة العنكبوتية (الأنترنت)، و التي تهدف إلى تنفيذ العديد من الأعمال لترويع أمن الأفراد و الجماعات و المؤسسات و الدول، و إرهاقهم اقتصاديا و إدخالهم في أزمات نفسية و إجتماعية ناتجة عما يعرف بالإرهاب الصامت[18]".
- يعرِّف حلف الناتو (NATO) الحرب الإلكترونية بأنها : "ذلك القسم العسكري الذي يستخدم إلكترونيات تهتم بالإجراءات التي تتخذ لمنع أو تقليل استخدام العدو لطاقته الكهرومغناطيسية المنبعثة الفعالة و الإجراءات التي تتخذ لحماية طاقتنا الكهرومغناطيسية المنبثقة الفعالة [19]".

تحتوي الحرب الإلكترونية على العديد من مصطلحات و مفاهيم الحرب التقليدية على غرار الهجوم و الدفاع و الردع و كذا الأهداف السياسية كإخضاع العدو و إجباره على الإستسلام و جعله غير قادر على تأدية مهامه، لنستنتج أن الحرب الإلكترونية ما هي إلا إسقاطات عن الحرب التقليدية في الفضاء السيبراني و تطبيقا لما تطرق إليه القادة العسكريين و المنظرين الإستراتيجيين في الحروب، بحيث اعتبر القائد الإستراتيجي الصيني "سن تزو" أن جوهر الحرب هو كسب المعلومة و أن من يكسبها يكسب الميدان، و أن

القائد الحقيقي هو الذي يربح المعارك و الحروب دون سفك للدماء و استنزاف قواته، و هي الميزات التي توفرها الحروب الإلكترونية ذات الطابع المعلوماتي و التي لا تستهدف الإشتباك و التدمير بقدر ما تستهدف الفوز بالحرب دون خوضها من خلال ضرب مراكز الثقل الإستراتيجي لديه لإصابته بالشلل و العطب الإستراتيجي، بحيث يمكن لهجوم إلكتروني على أنظمة الإتصال و الشبكات المالية و الكهربائية المرتبطة بأجهزة الحاسوب و الإتصال و شبكات الأنترنت أن يوقف جُلَّ الوظائف الحيوية للدولة و تصبح عاجزة عن تأدية مهامها.

تجسدت الحرب السيبرانية في العديد من الهجمات الإلكترونية التي تعرضت لها دول مثل الهجمات التي تعرضت لها كل من إستونيا في سنة 2007 و جورجيا سنة 2008، بالإضافة إلى الهجمات التي مست كل من الولايات المتحدة الأمريكية سنة 2009 و التي استهدفت مواقع الوزارة الخارجية و وكالة الأمن القومي (NSA) و البيت البيض، و في عام 2012 تم تدمير 35 ألف جهاز كمبيوتر لشركة أرامكو السعودية للنفط لتخريب صادرات النفط نحو الولايات المتحدة الأمريكية.

بالإضافة إلى الهجوم الإلكتروني على إيران العام 2010 بواسطة فيروس (ستكسنت/Stuxnet) حيث أكدت إيران أن العديد من وحداتها الصناعية تعرضت لهجوم إلكتروني بعد إصابتها بفيروس "ستكنست" و يعد هذا الفيروس وفقا للعديد من التقارير واحدا من أعقد الأدوات التي تمّ استخدامها إلى حد الآن.

و هناك من يرى بأن وكالتي الإستخبارات الأمريكية و الإسرائيلية استطاعتا تصميم هذا الفيروس و الذي عمل على اختراق و تعطيل المنشآت النووية الإيرانية، حيث هناك العديد من الخبراء من يعتقد بأن هدف الفيروس هو مفاعل بوشهر، كما أن هناك يرى بأن إسرائيل قامت لوحدها بشن هذا الهجوم حيث كان دقيقا إلى درجة تحديد عدد أجهزة الطرد المركزي و إختراقها بمهارة فائقة.

يعتبر البعض بأن نجاح هذا الهجوم انتقل بالعالم إلى مرحلة توظيف الهجمات السيبرانية في تحقيق أضرار مادية معتبرة، و هو ما يجعل هذا النوع من الأسلحة المتطورة يمكن أن تكون أمراً شائعا في المستقبل.

6.خصائص و أنواع الحروب السيبرانية :

على الرغم من أن الحروب السيبرانية تتقاطع مع الحروب التقليدية في المبادئ و الأهداف إلا أنها تكتسي طابعا خاصا بها من حيث أساليب القتال و المواجهة ، هذه الخصائص يمكن إجمالها في النقاط التالية:

- فعلى عكس الحروب التقليدية التي كانت تدور في ميادين و مسارح عمليات محددة للقتال، فإن الحروب السيبرانية تعتمد الفضاء السيبراني ميدانا للصراع مزيحة بذلك الحدود الجغرافية، حيث أدت عولمة تكنولوجيات الاتصال إلى جعل العالم قرية صغيرة يسهل التفاعل ضمنها، و هو ما أضفى على الحرب السيبرانية طابعا شاملاً.

- يتم الهجوم في الفضاء السيبراني عن طريق أدوات و أسلحة خاصة بالحرب السيبرانية يطلق عليها بأدوات العدوان Assaut Tools و تختلف هذه الأدوات باختلاف الهدف من الهجوم، إذ يمكن أن تقوم بتغيير الخصائص التقنية للجهاز المستهدف إذا كان ذو طبيعة مادية Hard Ware، أو من خلال التلاعب بالبرمجيات بإدخال تعديلات عليها أو إتلافها، إذا كان الهدف ذو طبيعة معلوماتية أو برمجية Logicial Target أي Soft ware .
- لا تنحصر أهداف الحروب السيبرانية في المواقع العسكرية فحسب، فهناك جهود متزايدة لإستهداف البُنى التحتية المدنية و الحساسة في البلدان المستهدفة، و هو أمر أصبح واقعيا في ظل القدرة على استهداف شبكات الكهرباء و الطاقة و شبكات النقل و النظام المالي و المنشآت الحساسة النفطية أو المائية أو الصناعية بواسطة فيروس يمكنه إحداث أضرار مادية حقيقية تؤدي إلى إنفجارات أو دمار هائل[20].
- يتمتع المهاجم في الحروب السيبرانية بأفضلية واضحة و كبيرة على المدافع، فهذه الحروب تميز بالسرعة و المرونة و المراوغة، و في بيئة مماثلة يتمتع بها المهاجم بأفضلية من الصعب جدا على عقلية التحصن لوحدها أن تنجح، فالتحصين بهذا المعنى سيجعل من هذا الطرف عرضة لمزيد من محاولات الإختراق و بالتالي المزيد من الضغط[21].
- الحرب السيبرانية هي حرب رقمية و تقنية جدٌّ متطورة، حيث جسدت قمة التطور الذي بلغته ثورة المعلومات و بوابتها الحاسبة الإلكترونية التي شكلت بدورها الأداة المحورية لهذا النوع من الحروب و الميدان الرئيس لها، فكانت نتيجة لذلك عرضة للتطور المستمر و التنوع و الإبتكار في تقنياتها و وسائلها لإرتباطها الرأسي بقمتي الهرم التقني للحضارة الإنسانية و المصالح الحيوية للدول[22].

7.الأطروحات النظرية للحرب السيبرانية :

هناك إختلاف كبير بين الأكاديميين و المفكرين حول مصطلح "الحرب السيبرانية" و ما إذا كانت العمليات الإلكترونية التي تحدث على مستوى الفضاء السيبراني تصل إلى درجة "الحرب" أم أنها تبقى مجرد "هجمات إلكترونية" لكونها لم تستوف شروط الحرب التقليدية، حيث ظهر هناك فريقين الأول يؤيد فكرة الحرب السيبرانية بينما الثاني يجادل و يعارض أن العمليات الإلكترونية في الفضاء السيبراني تصل إلى درجة وصفها بالحرب.

يكمن الإختلاف الجوهري بين الفريقين في طبيعة الهجمات الإلكترونية و الآثار و المخاطر الناتجة عنها ، بحيث يرى الفريق المعارض لمصطلح "الحرب السيبرانية" أن هناك مبالغة في تقييم المخاطر و عدم تطابق كلي مع نظرة "كلاوزفيتز" للحرب، خاصة من حيث درجة الخسائر و التأثير المادي للهجمة الإلكترونية الذي لا يمكن أن يعادل في حِدَّته أو يصل إلى درجة الدمار الناجم عن هجمة عسكرية تقليدية أو نووية، و يقتصر فقط على تخريب أنظمة المعلومات دون وجود دمار مادي ملحوظ.

أما الفريق المؤيد للحرب السيبرانية يعادل بأن لهذه الأخيرة خصوصيتها، فهي ذات طبيعة معلوماتية و قد لا تنطبق بالضرورة معاييرها مع الحرب التقليدية نظراً للإختلاف البنيوي لميدان المعركة و أسلحة المواجهة، و يتمسك الفريق المعارض لفكرة الحرب السيبرانية بعناصر الحرب التقليدية لكلاوزفيتز في موقفهم من النقاش، و قد استندوا على المعايير التالية[23]:

1) أن تكون للحرب خلفية سياسية.
2) أن يكون الهدف من الحرب هو إنهاك العدو و القضاء عليه من خلال الإشتباك و إنتاج المقدار المناسب من العنف و الدمار.
3) أن تتسم الحرب بالعنف.

يركز الفريق المعارض لفكرة الحرب السيبرانية على العنصر الثالث (العنف)، بحيث يجادل Thomas Rid في كتابه "الحرب الإلكترونية لن تحدث" أنَّ العنف لم يتجسد في جميع الهجمات الإلكترونية التي عرفها العالم بما في ذلك الهجمات على إستونيا، و لم يشهد العالم لحد الآن منذ ظهور الحاسوب و الأنترنت هجوما إلكترونيا فتاكاً و مُدمِّراً.

8.تأثير الحروب السيبرانية على العلاقات الدولية :

يظهر العلاقة الموجودة بين الحرب السيبرانية و الأمن القومي للدول من خلال:

1) إمكانية الاستعمال العدواني للفضاء الإلكتروني لأغراض عسكرية أو مآرب سياسية.
2) المخلفات المترتبة عن الهجمات الإلكترونية و التي تمس بصفة مباشرة الأمن القومي للدول.

نقصد بالأمن القومي قدرة الدولة على التحرر من جميع التهديدات و الأخطار التي تمس مصادر قوتها الداخلية أو الخارجية أو منظومتها القيمية، و مع توسع مفهوم الأمن أخذ أبعادا أخرى غير البُعد العسكري حسبما كان سائداً في المفهوم الضيِّق و التقليدي للمصطلح، حيث أصبح يشمل إلى جانب البُعد العسكري مجالات أخرى مثل: السياسية، الاقتصادية، الاجتماعية، الثقافية، البيئية.....

لقد أفرز الارتباط الكبير بتكنولوجيات الحاسوب و الأنترنت تهديدا حقيقيا للأمن القومي للدول، خاصة ما تعلق منه بالاستعمال الغير السلمي للفضاء السيبراني، فقد يمثل هجوماً إلكترونياً على المنظومات المعلوماتية للمؤسسات السيادية للدول كالوزارات أو منشآتها الحيوية كالبنوك و أنظمة المواصلات اعتماداً صارخا على سيادة هذه الدول و الولوج إلى المنظومات المعلوماتية للمؤسسات الحساسة أو شبكة البنى التحتية المرتبطة بالفضاء السيبراني يؤشر على جملة من الهشاشات و الثغرات التي أفرزت قابلية شديدة للعطب.

عموما، تؤثر الحروب السيبرانية على الأمن القومي للدول من خلال:

1. **تصاعد المخاطر الإلكترونية:** خاصة مع قابلية المنشآت الحيوية (مدنية و عسكرية) في الدول للهجوم الإلكتروني عليها عبر وسيط و حامل للخدمات أو شلل أنظمتها المعلوماتية ما يؤدي إلى بروز جملة من الهشاشات التي أفرزت قابلية شديدة للعطب.
2. **عسكرة الفضاء السيبراني:** إنّ التوظيف العسكري للفضاء السيبراني يمكن أن يعرض المصالح الإستراتيجية إلى أخطار إلكترونية جسيمة كتلك التي تكبدها المفاعل النووي الإيراني "ناتانز" من جراء الهجمة الإلكترونية "STUXNET" أو الهجمات الإلكترونية الروسية على إستونيا، أو تسريبات "ويكيليكس" التي مست الجهاز الأمني الإستخباراتي الأمريكي، و هو ما أدخل أمن الفضاء السيبراني ضمن أجندات و أولويات الأمن القومي للدول.

و سعيًا لدرء مخاطره على الدول، ظهر في هذا الإطار اتجاهات مثل التطور في مجال سياسات الدفاع و الأمن السيبراني، تصاعد القدرات في سباق التسلح السيبراني، تبني الدول لسياسات دفاعية سيبرانية، خاصة زيادة حجم الإنفاق على الأمن السيبراني في العديد من الدول مثل: الولايات المتحدة الأمريكية التي خصصت حوالي 19 مليار دولار للأمن السيبراني خلال عام 2017.

3. **إدماج الأمن السيبراني ضمن أجندات الأمن القومي للدول:** و ذلك من خلال تحديث الجيوش و تدشين وحدات متخصصة في الحروب الإلكترونية، و إقامة هيئات وطنية للأمن و الدفاع الإلكتروني و القيام بالتدريب، و إجراء المناورات لتعزيز الدفاعات الإلكترونية، و العمل على تعزيز التعاون الدولي في مجالات تأمين الفضاء السيبراني.

لقد أصبح الدفاع السيبراني لا يقل أهمية عن الدفاع العسكري التقليدي خاصة إذا علمنا أنّ الحرب الإلكترونية تترجم الصراعات الواقعية بين مختلف الفواعل الدولية، و عليه عكفت الدول على تطوير قدراتها الإلكترونية من خلال صياغة استراتيجيات سيبرانية تترجم تصور الدول لمصالحها و توجهاتها في هذا الفضاء، حيث تعمل الجيوش الإلكترونية على جعل هذه الإستراتيجيات قابلة للتحقيق على غرار روسيا، الصين و الولايات المتحدة الأمريكية.

4. **توتر العلاقات الدبلوماسية:** حيث يؤدي الهجمات الإلكترونية إلى توتير العلاقات الدبلوماسية بين الدول مثل: التوتر الذي حدث بين الولايات المتحدة الأمريكية و روسيا خلال الإنتخابات الرئاسية الأمريكية.

خـــاتمة :

أصبحت الحروب السيبرانية في عصر المعلومات وسيلة للصدام و المواجهة و فرض الإرادات السياسية و العسكرية، و أصبح الفضاء السيبراني ميدانا لهذه المواجهة. و على الرغم من التطور التقني و الطابع المعلوماتي و الإلكتروني الذي يكتسبه هذا النوع من الحروب و خصوصياته من حيث أساليب المواجهة، إلا أنه يحتفظ بالمبادئ و الأهداف و الخلفيات السياسية للحرب التقليدية. و لذلك يتوجب على

الدول و الأفراد الحذر عند استخدام البيانات و المعلومات في الفضاء السيبراني لتجنب الوقوع في مخاطر التصيُّد الشبكي و الهاكرز و الجماعات الإرهابية.

و لذلك تخلص الدراسة إلى النتائج التالية:

1. تشكل الثغرات المرافقة لتكنولوجيا الحاسوب و الأنترنت هاجسا أمنيا كبيراً للدول المعتمدة بشكل كبير على الرقمنة، حيث يمكن إصابتها بالشلل الوظيفي و القابلية الشديدة للعطب ما يعني فقدان مؤسسات الدولة قدرتها على تأدية وظائفها.
2. أصبحت الحروب السيبرانية تتصدر أولويات الأمن القومي للدول خاصة الدول الكبرى و في مقدمتها الولايات المتحدة الأمريكية.
3. مع إزدياد حدّة الهجمات الإلكترونية عبر العالم، وجد المجتمع الدولي نفسه أمام ضرورة إيجاد ضوابط قانونية للتقليص من حدة الهجمات الإلكترونية و منع الإنزلاق نحو حرب واقعية من خلال العمل الجماعي المشترك الذي لا يزال محتشماً و بطيئا لم يرقى إلى مستوى تطلعات الدول و الشعوب، بالنظر إلى إختلاف وُجهات النظر الدولية بشأن التشريعات القانونية الخاصة بالأمن السيبراني و صعوبة الجمع بين المعرفة التقنية و القواعد القانونية.

الهوامـش :

1) ألفن و هايدي توفلر، الحرب و ضد الحرب، ترجمة محمد عبد الحليم أبو غزالة ، (بيروت: دار المعارف،2000)، ص.114.
2) عامر مصباح، تطور علم الإستراتيجية، (القاهرة: دار الكتاب الحديث، 2017)، ص.395.
3) Mickeal.j.Thompson : "Revolution in military affairs :accurat description of change or intellectual constructs ?"in : www.artsites.uottawa.ca/strata/doc/strata3_082-108.pdf.p.16 (22/08/2018)
4) ذياب موسى البداينة، الإرهاب المعلوماتي (التعريف- المفهوم- المجالات – النتائج)حلقة علمية حول الأنترنت و الإرهاب، جامعة نايف العربية للعلوم الأمنية، الرياض: السعودية،2008،ص.07.
5) صفات أمين سلامة، "أسلحة حروب المستقبل بين الخيال و الواقع"، مجلة الدراسات الإستراتيجية، مركز الإمارات للدراسات و البحوث الإستراتيجية، ع 112 (2005)، ص.16.
6) Mladen Milicevic,cyber space and globalization,(California : Loyala Marynout university), p.13.
7) Jason Andress and Steve Winterfeld, cyber warfare techniques,Tacties and Tools, for security practitioners,(USA, Syngress imprint of Elsivier, 2011),p.02.
8) Minstry of defeuse, japan,toward stable and effective use of cyber space,september,2012,p.2-3
9) سليمة ذياب و بلال بوترعة، الجريمة الإلكترونية: الأسس و المفاهيم، مجلة تطوير العلوم الإجتماعية، العدد 01، 2020.ص ص. 7-20.

10) المرجع نفسه.
11) أوس مجيد غالب العوادي، "الأمن المعلوماتي السيبراني"، سلسلة إصدارات مركز البيان للدراسات و التخطيط، عدد 1، (أوت 2016)، ص.10.
12) المرجع نفسه، ص.12.
13) عادل صادق،استخدام الإرهاب الإلكتروني في الصراع الدولي، دار الحديث، القاهرة، 2015، ص.104.
14) ذياب موسى البداينة، مرجع سابق، ص.12.
15) رافعي ربيع، الإرهاب الدولي و علاقته بالجريمة المنظمة: الإرهاب الإلكتروني نموذجا، مجلة القانون و العلوم السياسية، المجلد 07، العدد 01، 2021، ص ص .70-78.
16) Jeffery Carr, Inside cyber warfare, (USA :O'Reilly media, IMC.,1005Gravenstein Highway North sebastopol, december 2009, Firstedition), p.02.
17) جون باسيت، الحروب المستقبلية في القرن الحادي و العشرين (أبو ظبي: مركز الإمارات للدراسات و البحوث الإستراتيجية، 2014)ص.57.
18) عياد سامي، استخدام تكنولوجيا المعلومات في مكافحة الإرهاب (القاهرة: دار الفكر الجامعي، 2007).
19) غريب حكيم، شرقي صبرينة، تداعيات الحرب الإلكترونية على العلاقات الدولية: دراسة في الهجوم الإلكتروني على إيران (فيروس ستكنست)، مجلة دفاتر السياسة و القانون، المجلد 12، العدد 02، 2020، ص ص.92-107.
20) عبد الغفار فيصل محمد، الحرب الإلكترونية، عمان: الجنادرية للنشر و التوزيع، 2016.ص.12.
21) المرجع نفسه، ص.11.
22) غريب حكيم، شرقي صبرينة، مرجع سابق، ص ص.92-107.
23) نوران شفيق، اثر التهديدات الإلكترونية على العلاقات الدولية (القاهرة: المكتب العربي للمعارف، 2016)، ص.177.