الثورة الرقمية في المجال العسكري وتداعياتها على الحروب الحديثة (الحرب السيبرانية نموذجا)

The digital revolution in the military and its implications for modern wars (cyber warfare as a model)

معيزي ليندة [1]*، دهقاني أيوب[2]،

[1] كلية الحقوق، جامعة تيسمسيلت (الجزائر)،

مخبر الأمن القومي الجزائري- رهانات وتحديات- جامعة الجيلالي بونعامة خميس مليانة (الجزائر)،

lynda.maizi@cuniv-tissemsilt.dz

[2] كلية الحقوق، جامعة تيسمسيلت (الجزائر)،

dehegani.ayoub@cuniv-tissemsilt.dz

تاريخ الإرسال: 2022/03/03 تاريخ القبول: 2022/04/15 تاريخ النشر: 2022/06/01

****

ملخص:

تهدف هذه الدراسة إلى عرض مضامين الثورة الرقمية وتطبيقاتها التكنولوجية على المجال العسكري، كما تناقش الآثار السلبية لهذا الاستخدام من ضمنها ظهور أشكال جديدة للحرب والقتال والتي مسرحها الفضاء السيبراني وتكون في مقابل ذلك أكثر تأثيرا وأقل جهدا، هذا ما دفع بالقادة العسكريين إلى تطوير استراتيجياته متجاوبا مع العصر الرقمي.وخلصت الدراسة بتداعيات التحديث العسكري الذي فرضته التغيرات التكنولوجية على الساحة الدولية الأمر الذي ساهم في التحولات السريعة التي طرأت على مستوى أجيال الحروب وأنماط خوضها.

الكلمات المفتاحية:

الثورة الرقمية، الإستراتيجية العسكرية، أنماط الحروب، الحرب السيبرانية، تكنولوجيا الأسلحة.

Abstract:

This study aims to present the contents of the digital revolution and its technological applications to the military sphere, it also discusses the negative effects of this use, including the emergence of new forms of war and combat that are being released by cyberspace and in turn are more influential and less demanding,the study concluded that the military modernization imposed by technological changes in the international arena has increased the intensity of wars.

***المؤلف المراسل**

مقدمة:

تعد الحرب ظاهرة اجتماعية وسياسية معقدة ومتعددة الجوانب، وهناك من يرى أنها استمرار للسياسة بوسائل أخرى،لذا اعتمدت الدول والكيانات الاجتماعية على العمل المسلح لتحقيق غاياتها ومصالحها الوطنية خاصة عندما يتعلق الأمر بالجوانب الإستراتيجية، وبذلك كانت الحرب ومازالت واحدة من أهم الأدوات الأساسية لتفاعلات العلاقات الدولية.

وبعد نهاية الحرب الباردة تغير الوضع الدولي وأصبح أكثر مرونة وأسرع من حيث الحركية والتغيرات السياسية، الاقتصادية، التكنولوجية والعلمية كما أصبح يتميز بالتطور الهائل في كم المعلومات وتعددها واختلاف مصادرها وأصبح ما يعرف بعصر المعلومات.

بحيث أدى الانتشار الواسع للتكنولوجيا الرقمية إلى التغيير في طبيعة المجتمعات والاقتصاديات وامتد هذا التغيير إلى المجال العسكري حيث وصفه البعض بأنه ثورة في الشؤون العسكرية، إذ أن نشأة الحروب السيبرانية مرتبط بشكل أساسي بالتطور التقني المتسارع وزيادة الاعتماد على شبكة الحواسيب والانترنت وتشعبها في أوساط المجتمع أدى إلى زيادة احتمالات الاعتداء، وانتقلت تداعيات هذا التطور التكنولوجي إلى ميدان النزاعات والحروب حيث تحولت العديد من وسائل السيطرة والتحكم والعمليات الحربية ومعظم النظم التي تتحكم بالمنشآت المدنية الهامة إلى الحاسب الآلي ، كما انتقل جانب المواجهات الحربية إلى الفضاء السيبراني و أصبح هذا الفضاء ساحة للقتال منفصلة عن الساحة التقليدية للحرب والنزاع ،وباتت الحروب اليوم تجرى في الفضاء السيبراني وتظهر نتائجها بصورة مادية في الواقع هذا ما دفع بالدول المتقدمة إلى التحديث العسكري بما يتناسب مع متغيرات البيئة الإستراتيجية للحرب في العصر الرقمي.

إشكالية الدراسة:

على ضوء ما تم طرحه يهدف هذا المقال الذي يندرج ضمن الدراسات الإستراتيجية إلى الإجابة على الإشكالية التالية: كيف أثرت الثورة الرقمية في الشؤون العسكرية على نمط الحروب الحديثة وأساليب خوضها؟.

فرضية الدراسة:

كلما زاد توظيف التكنولوجيا المعلوماتية في الميدان العسكري كلما أدى ذلك إلى التغيير في المنطق الاستراتيجي للحرب وانتقالها من نمط المواجهة الصلبة إلى النمط السيبراني .

أهمية الدراسة:

تكمن أهمية الدراسة في معرفة أهم التطورات الحاصلة في المجال العسكري والتي ساهمت في تغيير المنظور التقليدي للإستراتيجية العسكرية والحروب وطريقة خوضها بإدخال المجال الخامس لهذه المواجهة وهو (الفضاء السيبراني) الذي أصبح العالم يعتمد عليه أكثر فأكثر لاسيما في البنى التحتية المعلوماتية العسكرية وأصبح هناك ما يعرف بالحروب الالكترونية التي مسرحها الفضاء السيبراني.

تقسيمات الدراسة: مسار الدراسة سيكون من خلال ثلاث محاور هي:

- الثورة الرقمية في الشؤون العسكرية: دراسة في المفهوم والتوظيف في الشأن العسكري.
- الفضاء السيبراني وتغير مضامين الحرب.
- نماذج للحروب السيبرانية وتداعياتها على السياسة الدولية.

المبحث الأول

الثورة الرقمية في الشؤون العسكرية: دراسة في المفهوم والتوظيف في الشأن العسكري

يهدف هذا المحور إلى تحديد مفهوم الثورة الرقمية والدافع لاستخدام التقنيات الرقمية والمعلوماتية في القطاع العسكري.

المطلب الأول: تعريف الثورة الرقمية أو المعلوماتية

هي مصطلح يستخدم لوصف مختلف ظواهر التغير التي يمكن ملاحظتها في عالم اليوم ،وهي نتاج التقدم في تكنولوجيا المعلومات والاتصالات السلكية واللاسلكية المحوسبة[1] والتطورات المستمرة في مجالات متعددة مثل الذكاء الاصطناعي ورقمنة المعلومات والتصنيع (مثل الطباعة ثلاثية الأبعاد) والواقع الافتراضي والتعليم الآلي و Blockchain والروبوتات والحوسبة الكمومية والبيولوجيا التركيبية كما هو الشأن في الثورة الصناعية.[2]

وتعتمد التكنولوجيا الرقمية الحالية على جميع الوسائل التقليدية إلا أنها أكثر ارتباطا بالانترنت.

ويعرفها إسماعيل صبري مقلد على أنها "ذلك الكم الهائل من المعرفة الذي أمكن السيطرة عليه بواسطة تكنولوجيا المعلومات وثورة الاتصال المتمثلة في تكنولوجيا الاتصال الحديثة ،وقوامها الأقمار الصناعية والألياف البصرية وثورة الحواسيب الالكترونية التي توغلت جميع مناحي الحياة" [3].

وينظر الكثير إلى المعلومات على أنها السمة المميزة للعالم الحديث بحيث تمت صياغة عصرنا الحالي بأنه "عصر المعلومات "والمجتمع الحالي هو" مجتمع المعلومات".

أما الثورة الرقمية في الشؤون العسكرية: هي مصطلح نشأ في السبعينات والثمانينات من القرن الماضي في الكتابات السوفيتية تحت اسم "الثورة الفنية العسكرية" لكنه سرعان ما تطور إلى مصطلح أكثر شمولية وهو الثورة في الشؤون العسكرية **RMA**.[4]

وهناك تعريفات واسعة ومتنوعة لهذا المصطلح نذكر من بينها:

هي " تغيير رئيسي في طبيعة الحرب نتيجة للتقدم المبتكر في تكنولوجيا العسكرية إلى جانب التغيرات الدراماتيكية في العقيدة العسكرية والمفاهيم العملياتية والتنظيمية بشكل يغير من سلوك العمليات العسكرية وسيرها".

ويعرفها معظم المحللين بأنها الزيادة في القدرة والفعالية العسكرية الناشئة عن التغير الداعم والمتبادل في تكنولوجيا الأنظمة وأساليب التشغيل والمنظمات العسكرية.

ويعرفها أندرو مارشال**AndroMarchal** بأنها "تغيرات أساسية بعيدة المدى في كيفية تخطيط الجيوش المتقدمة لإجراء عمليات عسكرية أو ملاحقتها فعليا".

---

[1]Norman c. Davis, " an information-based revolution in military affaires ",strategic revieu,vol.24,No.01, winter1996.p79.

[2]Raport prepared by the Word in 2050 initiative," the digital révolution and sustainable development: opportunities and challenges ". International institute for applied systèmes analysis (IIASA). Luxemburg. Austria ,2019. P19.

[3]إسماعيل صبري مقلد،" مخاطر تسببها الفجوة الرقمية: ثورة المعلومات وحروب المستقبل المحتملة"، مجلة استراتيجيا آفاق المستقبل، العدد15، يوليو/أغسطس/سبتمبر2012، ص40.

[4]Metz,s and kievit.j,"Strategy and the revolution in military affairs ",from theory to policy .strategic studies institute ,1995.p.10

ويؤكد هاندليHandley أنRMA ينطوي على نقلة نوعية في طبيعة وسلوك العمليات العسكرية ."[1]

المطلب الثاني: دور الثورة الرقمية في تطور الميدان العسكري:

أصبح العالم اليوم يتصف بالتطور السريع والمستمر نتيجة التدفق الهائل للمعلومات وما يصاحب ذلك من تطور في مجال الحاسوب وأنظمة الشبكات،وأضحت بذلك المعلومات تشكل حجر الأساس لمختلف مجالات الحياة لاسيما في المجال العسكري الذي بات يعتمد اعتمادا كليا على أجهزة الحاسوب وأنظمة المعلومات والشبكات في العمليات العسكرية الحديثة هذا ما أدى الى تحولات عميقة في تسيير القوات من خلال الربط الشبكي للمعلومات التشغيلية وجعل انتقالها متاح لكل مقاتل.[2]

وهناك علاقة معقدة بين المجتمع العسكري والتقنية ويعود ذلك الى التطورات التي حدثت في الستينات من القرن الماضي بحيث مثل الميدان العسكري السوق الرئيسي لتكنولوجيا المعلومات[3].

ولعل من أبرز التطورات التكنولوجية في الميدان العسكري ما يلي:

1.**الطابعة الثلاثية الأبعاد :additive manufacturing**التي تحولت من مجرد هواية إلى صناعة تنتج مجموعة لامتناهية من المنتجات شكلت تحول كبير للتصنيع، ولعل قائمة العشر الأوائل الحديثة تشمل: المعادن مثل الفولاذ المقاوم للصدأ والبرونز والذهب والألمنيوم والسراميك والأنابيب النووية إضافة إلى مجموعة أخرى من المواد.

وتشير التطورات التكنولوجية الحديثة الى أن الصناعة قادرة على زيادة سرعة هذه الطباعة بهدف زيادة الإنتاج، وقد كشفت شركة الطباعة الالكترونية في يناير 2015عن طابعة جديدة تطبع طائرات بدون طيار تشغيلية كاملة مع الالكترونيات والمحرك.

2.**النانو تكنولوجي :Nanotechnology**الذي شهد تقدما سريعا في مجالات عدة خاصة فيما يتعلق اولا بالأمن القومي وهو الطاقة النووية، ففي 2002 أنتجت المتفجرات النووية تبلغ ضعف قوة المتفجرات التقليدية وهذا ما يؤدي الى الزيادة في القدرة التدميرية.

أما المجال الثاني: وهو المواد النانوية والتي من المحتمل أن تكون لها أثار كبيرة في زيادة نطاق المركبات التي تعمل بالطاقة الكهربائية، كما أن العديد من الشركات توظف المواد النانوية على البطاريات لزيادة سعتها التخزينية.

3.**القدرات الفضائية وشبه الفضائية :Space and space-like capabilities** أن توافر المراقبة المستمر في الفضاء يعمل على توفير المعلومات اللازمة لتوظيف هذه التقنيات الجديدة في الفضاء فمثلا شركة جوجل سكاي بوكس للتصوير بالأقمار الصناعية **Google skybox imaging**تهدف الى تسويق خدمات توفر صور عالية الدقة ، كما تعمل شركات أخرى على أنظمة يمكنها تكرار وظائف الاتصالات والمراقبة التي توفرها الأقمار الصناعية باستخدام الأنظمة التي تعمل في

---

[1]Metz,s and kievit.j. op.cit .p.v.

[2]عبد الرحمن حسن الشهري،"تطور العقائد والاستراتيجيات العسكرية "،(الرياض:بدون دار نشر، 2003)،ص357

[3]François Levieux, « la défense et les technologies de l'information et de la communication », Annales Des Mines, Novembre 2005.p68.

الغلاف الجوي للأرض مثل مشروع جوجل لوون**project Google loon**، وتسعى هذه الشركة لتقديم خدمات انترنت بأقل تكلفة لمعظم أنحاء الكرة الجنوبية من خلال نشر مجموعة البالونات التي تنقل الإشارات إلى الأرض[1].

4.الذكاء الاصطناعي :Artificial Intelligenceتتضمن الأسلحة الذكية اليوم مجموعة من الأسلحة الموجهة والدقيقة [2]والتي تتمثل في تطبيق القوة الذكية بإطلاق ذخائر دقيقة التوجيه (تحقيق الوعي بساحة المعركة)، عن طريق طائرات المراقبة والمركبات الجوية بدون طيار والأقمار الصناعية[3] وصواريخ الرؤوس الحربية الفردية وصاروخ كروز و توماهوك التابع للبحرية البريطانية الموجه بنظام تحديد الموقع (GPS)الذي يمكن أن يصيب هدف بحجم غرفة صغيرة على بعد ألف ميل، ولقد أدت الأسلحة الذكية إلى زيادة القوة التدميرية بشكل كبير جدا عما كانت عليه بالأمس[4].

وبهذا يتضح أن للتطور التكنولوجي دور حاسم في الحرب الحديثة من خلال تطوير الذخائر الموجهة بدقة والتي استخدمت لأول مرة في حرب الفيتنام وقد ازدادت دقتها بشكل كبير منذ حرب الخليج.

المبحث الثاني

الفضاء السيبراني وتغير مضامين الحرب

يتناول هذا المحور تأثير التطور التكنولوجي في المجال العسكري على طبيعة الحروب وطريقة سيرها والانتقال بذلك من المفهوم التقليدي للحرب لدى كلاوزوفيتش الذي يركز على قاعدة القتال في المجال المادي الى مفهوم صان تزو الذي يركز على قاعدة المعرفة وتقليل من العنصر البشري والقتال في الفضاء السيبراني.

المطلب الأول: مفهوم الفضاء والحرب السيبرانية:

أ)- مفهوم الفضاء السيبراني:cyber space يشير الفضاء السيبراني إلى شبكات الاتصال الالكتروني والواقع الافتراضي وشبكات الانترنت وعدد هائل من البيانات، وهناك من وصفه بأنه الذراع الرابع للجيوش[5] .

وقد تطور هذا المصطلح من التحكم الآلي الى الفضاء السيبراني ، وتعددت التعاريف الموجهة إليه ونجد من بينها: تعريف إدارة السلامة العامة الكندية "بأنه العالم الإلكتروني الذي تم إنشاؤه بواسطة شبكة تكنولوجيا المعلومات المترابطة ،والمعلومات متاحة على هذه الشبكات ويتم مشاركتها على نطاق واسع حيث يرتبط الناس عن طريق تبادل الأفكار والخدمات والصداقة ، والفضاء الكتروني ليس ثابتا وإنما هو نظام بيئي ديناميكي متطور ومتعدد المستويات البنية التحتية

[1]T. X. Hammes, « Technologies Converge and Power Diffuses ...The Evolution of Small, Smart, and Cheap Weapons, policyanaysis, no.786, ,27 January 2016. p.p3-5.

[2]carlo al bertocuoco,"the revolution in military affairs: theoretical utility and historical evidence», researchpaper, no.142.april 2010p.p16.17.

[3]Elinorc.sloan ,"the revolution in military affairs implication for canada and nato", Canadian Military Journal, autum,2000.p03

[4]Op.cit . p.07

[5]عباس بدران،" الحروب الالكترونية: الاشتباك في عالم متغير"،(بيروت: مركز دراسات الحكومة الالكترونية، 2010)، ص 4

المادية والبرمجيات واللوائح والأفكار والابتكارات التي يتأثر بها العدد المتزايد من المساهمين الذين يمثلون المجموعة المتنوعة من المقاصد البشرية" [1].

وعرفه الاتحاد الدولي للاتصالات بأنه" المجال المادي وغير المادي الذي يتكون من العناصر التالية: أجهزة الكمبيوتر، الشبكات، البرمجيات، حوسبة المعلومات، المحتوى، معطيات النقل والتحكم وكل مستعملي هذه العناصر" [2].

وبذلك فان الفضاء الالكتروني هو فضاء افتراضي يستخدم الطيف الالكتروني والكهرومغناطيسي لتخزين المعلومات وتبادلها من خلال أنظمة الشبكية والهياكل المادية ذات الصلة، وهو بيئة افتراضية غير ملموسة حيث يتبادل أكثر من 7.2 مليار شخص المعلومات والاتصالات مما يوفر مكانا مشترك للتبادل الأفكار والآراء والخدمات والصدقات دون أي قيد مادي او سياسي[3].

ب)-مفهوم الحرب السيبرانية:cyberwarfare ليس هناك إجماع محدد ودقيق لمفهوم الحرب السيبرانية بحيث عرفت وزارة الدفاع الأمريكية الحرب السيبرانية على أنها " توظيف القدرات الالكترونية ويكون الغرض الأساسي هو تحقيق أهداف أو آثار عسكرية في الفضاء السيبراني أو من خلاله"[4].

كما حاول عدد من الباحثين تقديم تعريف يحيط بهذا المفهوم وقد عرفها كل من ريشارد كلارك وروبرت كناكي على أنها " أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف إلحاق الضرر بها وتدميرها " [5].

وهناك من عرفها على أنها "صراع يستخدم معاملات أو هجمات معادية وغير مشروعة على أجهزة الكمبيوتر والشبكات لمحاولة تعطيل الاتصالات وأجزاء أخرى من البنية التحتية كآلية لتسبب في خسارة اقتصادية أو تعطيل الدفاعات" [6].

و الحرب الإلكترونية هي جزء من عمليات المعلومات المستخدمة على مستويات ومراحل مختلفة من الصراع سواء من الناحية التكتيكية أو الإستراتيجية أو العملياتية للتأثير سلبًا على المعلومات وأنظمة عملها[7].

---

[1]Dan Craigen and Nadia Diakun-Thibault and Randy Purse," Defining Cybersecurity, Technology Innovation Management Review", (Ottawa: Technology Innovation Management, October 2014), p.p. 13 – 14.

[2]إسماعيل زروقة،"الفضاءالسيبراني والتحول في مفاهيم القوة والصراع "،مجلة العلوم القانونية والسياسية، المجلد 1، العدد 01،أفريل 2019.ص1018.

[3]مصطفى إبراهيم سلمان الشمنري،"الأمن السيبراني وأثره في الأمن الوطني العراقي "، مجلة العلوم القانونية والسياسية، كلية القانون والعلوم السياسية –جامعة ديالي، المجلد 10. العدد .01 2021،ص.152.

[4]Schreier Fred, « On Cyberwarfare », Dcaf Horizon Working Paper No07 ,2015,20p16.

[5]المجال الخامس.. الحروب الالكترونية في القرن ال21، مركز الجزيرة للدراسات، على الرابط http://studies.aljazeera.net/ar/issues/2010/20117212274346868.html

[6]SchreierFred, op.cit,p16.

[7]عادل عبد الصادق، "الحروب السيبرانية: تصاعد القدرات والتحديات للأمن العالمي"، المركز العربي لأبحاث الفضاء الالكتروني، (2017/03/12). على الرابط http://www.accronline.com/article_detail.aspx?id=28395

وتستهدف قدرات الحرب السيبرانية شبكات الكمبيوتر والاتصالات السلكية واللاسلكية والمعالجات ووحدات التحكم المدمجة في المعدات والأنظمة والبنية التحتية[1].

المطلب الثاني: طبيعة الفواعل في الحرب السيبرانية.

يمكن تصنيف طبيعة الفاعلين في الحرب السيبرانية إلى ما يلي:

1)- الدول والحكومات: يتم تنفيذ الهجوم الالكتروني من قبل الجهات الحكومية لأغراض متعددة سواء كانت أمنية أو سياسية او أيديولوجية أو غيرها ويمكن للحكومات هنا استغلال الجهات الفاعلة غير الحكومية سواء كانت أفراد او جماعات للقيام بهذه الهجمات ضد دول معادية، أو تقوم بعض أجهزتها بذلك وهنا تصبح مخاطر كبيرة لان بعض الدول تمتلك تقنيات وقدرات تكنولوجية فائدة الدقة.

وفي هذا السياق يرى جوزيف ناي أن هناك أربعة تهديدات تشكل خطر على الأمن القومي للدول وتكون محل اهتمام الحكومات في الحروب السيبرانية وهي: التجسس الاقتصادي، الجريمة الكترونية، الحرب الكترونية والإرهاب الالكتروني.

2)-الفاعلون غير الدول: من الأمثلة على ذلك ما يلي:

أ) -الشركات المتعددة الجنسيات: التي تتوفر على موارد مالية ضخمة ولها فروع في مختلف دول العالم هذا ما يتيح لها السيطرة على التعليمات البرمجية الخاصة، كما يوفر لها موارد أكبر في العديد من الحكومات لذا يمكن لهذه الشركات أن تلعب دورا في صراعات الفضاء الالكتروني نتيجة انخفاض تكلفة الاستثمار وصعوبة تحديد الهوية مما يجعلها تتعاون مع الحكومات أحيانا وتعمل ضدها أحيانا أخرى.

ب) - الجماعات الإرهابية: يحاول هذا الفاعل استخدام الأدوات الكترونية في الفضاء السيبراني لتدشين عمليات مسلحة في الواقع بالإضافة الى استخدام هذه الجماعات لمواقع التواصل الاجتماعي كوسيلة لتجنيد أتباع جدد لنشر ثقافتهم ومعتقداتهم بدلا من الحصول على الدعم المادي[2].

ج) -المنظمات الإجرامية: تقوم بعمليات القرصنة الالكترونية من خلال سرقة المعلومات واختراق الحسابات البنكية وتحويل الأموال بحيث توجد سوق سوداء على الانترنت لبيع معلومات مرتبطة بكلمات المرور الشخصية والحسابات البنكية وغيرها، وتكفل هذه الجرائم السيبرانية مليارات الدولارات سنويا.

د)- الأفراد: أصبح الفرد فاعل مؤثر في العلاقات الدولية بفضل الفضاء السيبراني ولعل من ابرز مجموعات القرصنة في الفضاء الكتروني هي مجموعة انونيموس**anonymous** التي تأسست سنة 2003، وهي المنتشرة عبر العالم وذات الثقل الكبير فيما يسمى بالحرب الالكترونية وقد كانت هذه المجموعة مسؤولة عن تسريب العديد من رسائل البريد الكتروني المتعلقة بالشخصيات الحكومية

---

[1]Saalbach, Klaus-Peter, "Cyber war Methods and Practice ". Germany: Osnabrueck,2019. P.09

[2]سماح عبد الصبور،"الصراع السيبراني.. طبيعة المفهوم وملامح الفاعلين"، مجلة السياسة الدولية، العدد 208 المجلد 52،افريل 2017 ص 7-8.

كما هاجمت مواقع حكومية أمريكية وبريطانية وحتى إسرائيلية [1]، أيضا قضية الويكيليكس **wikileaks** الذي تمكن من نشر الملايين من الوثائق الخفية للإدارة الأمريكية وقنصليتها مما أدى إلى خلق العديد من المشاكل الدبلوماسية بين الولايات المتحدة الأمريكية والدول الصديقة[2].

المبحث الثالث

نماذج الحروب السيبرانية وتداعياتها على السياسة الدولية

أصبحت الحرب السيبرانية نموذجا تسعى إليه العديد من الدول لكونها غير مكلفة مقارنة بالوسائل التقليدية كما أنها تلحق أضرار جسيمة بالخصوم وتتسم بصعوبة تحديد مصدر الهجوم مما يسمح بتجنب الدول لتبعات القانونية والعسكرية.

المطلب الأول:النماذج التطبيقية للحروب السيبرانية

كانت أولى الهجمات السيبرانية هو الهجوم الذي نفذته الولايات المتحدة الأمريكية عام 1982 ضد منظومة التحكم في أنبوب النفط **(chelyabinsk)**التابعة للاتحاد السوفياتي، والذي نتج عنه انفجار كبير أدى إلى خسائر بالغة، في حين يرى آخرون أن أول مرة ينفذ فيها الهجوم السيبراني أثناء حرب كوسوفو عام 1999 وذلك من خلال استهداف سلاح الجو التابع لحلف الناتو لشبكات الهاتف في يوغسلافيا سابقا [3].

وبالنظر الى أحدث الهجمات السيبرانية نجد انه في أواخر عام 2016 اكتشفت شركة أمن تكنولوجيا المعلومات **(crowdstrike)**هجوما سيبرانيا على مدافع اوكرانية من نوع هاوتزر، بحيث تم زرع برنامج **x-agent** الخبيث في حزمة **android**ويدعم هذا التطبيق أسلحة مدفعية هاوتزر**D-30** لمعالجة بيانات الاستهداف في وقت قصير وساهم في خسارة 80%من أسلحة الهاوتزر المدفعية.[4]كما تعرضت أوكرانيا لهجوم من قبل روسيا في 27 يونيو 2017 بسبب الخلاف المستمر حول شبه جزيرة القرم وبعض المناطق الشرقية والجنوبية للبلاد ، حيث بدأت الهجمات الروسية على المواقع الالكترونية للمنظمات والمؤسسات الأوكرانية باستخدام إصدارات "بيتا" من البرامج الضارة وأدى الهجوم إلى اختراق أنظمة المعلومات وإغلاق أجهزة الكمبيوتر والمطالبة بتقديم فدية بالنقود الالكترونية "بيتكوين"، وبعد ذلك أوضحت السلطات الأوكرانية أن هدف الفدية هو التستر على الهجوم والغرض الأساسي من الهجمات هو تعطيل أعمال الشركات الحكومية والخاصة وزعزعة الأمن والاستقرار في أوكرانيا [5].

---

[1]إيهاب خليفة. **القوة الالكترونية وأبعاد النحول في خصائص القوة،** (مصر: مكتبة الإسكندرية ،2014)، ص40.41.

[2]إسماعيل زروقة، مرجع سابق، ص 1020.

[3]أحمد عبيس نعمة الفتلاوي، "الهجمات السيبرانية : مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر" ، مجلة المحقق الحلي للعلوم القانونية والسياسية ، كلية القانون ،جامعة بابل ، العدد الرابع ، المجلد .8 ديسمبر 2016ص.626

[4]Saalbach, Klaus-Peter.op.cit.p49

[5]صلاح حيدر عبد الواحد،"حروب الفضاء الالكتروني، دراسة في مفهومها وخصائصها وسبل مواجهتها "،(رسالة ماجستير غير منشورة،جامعة الشرق الأوسط، قسم العلوم السياسية، كلية الآداب والعلوم، تموز2021)، ص29.

كما تعرضت روسيا في المقابل لهجمات سيبرانية حيث أعلن نائب مدير المركز التنسيقي الروسي لمواجهة حوادث الحاسوب" نيقولاي موراشوف" أن هناك هجوما سيبراني قوي وقع ضد روسيا من الخارج يوم الانتخابات الرئاسية في مارس 2018، وعبر "موراشوف" أن المركز بدء في رصد الهجمات السيبرانية ابتداء من جوان2017 و بلغت هذه الهجمات ذروتها يوم "الخط المباشر" مع الرئيس فلاديمير بوتين يوم 15 جوان 2017 ،وتجددت في 18 مارس 2018 يوم الانتخابات واستهدفت تعطيل عمل مراقبة نتائج الاقتراع عبر الفيديو بهدف تشويه نتائج التصويت[1].

وفي مايو 2017 تعرضت بريطانيا لهجوم سيبراني عرف بهجوم "واناكراي" الذي نسبته المملكة المتحدة الى كوريا الشمالية، والذي تسبب في خسائر كبيرة متمثلة في توقف الأنشطة التجارية والاقتصادية وخدمات حكومية في مناطق مختلفة من العالم من بينها الصحة العامة في بريطانيا إذ أن الهجوم استهدف أجهزة الكمبيوتر المرتبطة بالنظام الصحي الالكتروني مما أدى إلى تعطيل في السجلات الصحية وتوقف بعض المؤسسات الصحة عن العمل[2].

وفي مايو 2018استهدف برنامج الفدية **(Wannacry)**ثغرات أمنية في نظام التشغيل مايكروسوفت ويندوز **Microsoft Windous** مما أدى إلى إصابة الملايين من أجهزة الكمبيوتر في دول مختلفة من العالم ،كما أدى هذا الهجوم العالمي إلى تعطيل عمليات التصنيع والنقل والاتصالات وأصاب نحو 81 منظمة للخدمات الصحية مما أثر بشكل سلبي على الصحة العامة[3].

وفي 14 مايو 2019 تعرضت السعودية لانفجار أصاب محطتين للنفط بسبب هجمات مباشرة بواسطة طائرات مسيرة انفجارية تابعة للحوثيين، كما سجلت سنة 2019 عدة غارات بطائرات مسيرة على قاعدة حميميم متسببة في إصابة طائرات الميغ الروسية وأجهزة الرادار في المطار بعدة قذائف صاروخية. [4]

وفي جوان 2019 قامت الولايات المتحدة الأمريكية بشن هجمات الكترونية على شبكة الطاقة الروسية بحيث تم وضع برامج ضارة تستهدف تعطيل الشبكة الكهربائية الروسية حسب ما ذكرته صحيفة نيويورك تايمز[5].

وفي فيفري 2019 صرح مسؤول في وحدة الدفاع الالكتروني التابعة للجيش الإسرائيلي لوكالة بلومبرغ الأمريكية بأن الجيش الإسرائيلي كشف عن محاولة إيرانية لاختراق نظام الإنذار الصاروخي الإسرائيلي ، وبحسب شركة الأمن الالكتروني **Fireeys** أن الهجمات قد تعود إلى عام 2017 ، وأوضح رئيس الوزراء بنيامين نينياهو أن إسرائيل تعاملت مع هذه التهديدات بإنشاء

---

[1] روسيا اليوم، أقوى هجمات سيبرانية استهدفت روسيا،العربية، (2019/01/31)، على الرابط https ://www.arabic.com

[2]"لندن: بيونغ مسؤولة عن هجوم "واناكراي" الالكتروني"، العربية، (2017/12/27)، على الرابط https ://www.alarabiya.net

[3]أميرة عبد العظيم محمد عبد الجواد، "المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام "، مجلة الشريعة والقانون، العدد. 35، الجزء. 3 ،2020 ص. 385.

[4]سركان بالكان، ترجمة مركز الخطابي للدراسات،"إستراتيجية داعش في استخدام الطائرات المسيرة "، نوفمبر 2019. ص03.

[5]Kate Sullivan, " New York Times: US ramping up cyber-attacks on Russia", CNN, (17/06/2019). At : https://www.nytimes.com/.

المزيد من التحصينات لمنع المخترقين من الوصول إلى أنظمة التحكم مع وضع أنظمة لمراقبة مختلف النشاطات البرمجية على الشبكة [1].

وتعرضت الولايات المتحدة الأمريكية في ديسمبر 2020 لهجمات سيبرانية واسعة النطاق استهدفت وكلات حكومية وكيانات البنية التحتية الحيوية وشركات القطاع الخاص ، وأوضحت وكالة الأمن السيبراني وامن البنية التحتية المكلفة بحماية الشبكات الأمريكية أن المتسللين تمكنوا من اختراق شبكات الحاسوب، وبعدها أصدرت وكالة الأمن القومي "إن المخترقين قد وجدوا طرقا للتزوير بيانات الكمبيوتر للوصول إلى اكبر عدد من الشبكات وسرقة البيانات "، وخلص بذلك المسؤولون الحكوميين وخبراء الأمن السيبراني إلى أن روسيا هي المسؤولة عن هذا الاختراق نظرا للمهارات الكبيرة التي ينطوي عليها هذا الهجوم[2].

وفي مايو 2021 تم اختراق البرنامج الخاص بشركة **salar winds** من قبل قراصنة روسيين تسبب الهجوم في تعريض تسعة وكالات أمريكية وعشرات المنظمات الخاصة للخطر كما تم شن هجوم الكتروني على الولايات المتحدة الأمريكية تسبب في غلق أكبر أنابيب نقل الغاز[3].

وفي جويلية 2021 أوردت تقارير إعلامية عالمية أن الجزائر تعرضت لعمليات تجسس باستعمال برنامج بيغاسوس ، كما صرحت الخارجية الجزائرية بقيام سلطات بعض الدول متهمة على وجه الخصوص المغرب باستخدام هذا البرنامج ضد مسؤولين ومواطنين جزائريين بهدف تسليمها لدول أجنبية بحيث يؤدي جمعها إلى الإضرار بمصالح الدفاع الوطني ، كما أوضحت صحيفة **le monde** وموقع (تي اس آه) الناطق بالفرنسية أن تحقيق منظمتي فوربيدنستوريو والعفو الدولية أظهر أن الآلاف من أرقام الهواتف الجزائرية يعود بعضها إلى مسؤولين سياسيين وعسكرين كبار وحدد على أنها أهداف محتملة لبرنامج بيغاسوس الذي طورته شركة (اس أو) الإسرائيلية عام 2019 هذا ما أثار سخط واسع في الجزائر خاصة على مواقع التواصل الاجتماعي واعتبرته الخارجية الجزائرية ممارسة غير قانونية و انتهاكا للمبادئ والأسس التي تحكم العلاقات الدولية.[4]

المطلب الثاني: تداعيات ومخاطر الحروب السيبرانية على السياسة الدولية

أدى اتساع نطاق الفضاء الالكتروني الى تنامي العديد من التهديدات الالكترونية بين الدول ومن ثم إمكانية بروز الحروب السيبرانية وما تخلفه من مخاطر على السياسة الدولية ولعل من أبرز التداعيات والمخاطر ما يلي:

---

[1] جواداه آري غروس،" إيران حاولت اختراق نظام الإنذار الصاروخي الإسرائيلي "، تايمز أوف إسرائيل، (2019/02/25)، على الرابط http://ar.timesofisrael.com

[2] Dustin Volz and Robert Mc Millan ," Hack suggests New Scope Sophistication for cyberattacks ", wall street journal ,(17/12/2020) .At :https://www.wsj.com .

[3] "اكبر الهجمات الالكترونية منذ بداية 2021" ،العربية،(10/05/ 2021)،على الرابط : https:// www.alarabiya .net

[4] " الجزائر تعلن فتح تحقيق حول عمليات تجسس تعرضت لها باستخدام برنامج بيغاسوس" فرانس24، (2021/07/23)، على الرابط :https//www.france24.com

-مخاطر استخدام الفضاء الالكتروني من قبل الفاعلين من غير الدول خاصة الجماعات الإرهابية لتحقيق مصالح وأهداف تتعارض مع الأمن القومي للدول.

- بإمكان أي دولة أن تشن هجوما الكترونيا على دولة أخرى دون الدخول فعليا إلى أراضيها لان الاعتماد المتزايد للدول على الأنظمة الالكترونية في كافة منشأتها الحيوية يجعل هذه الأخيرة عرضة لهجوم مزدوج، حيث تتداخل خصائصها المدنية والعسكرية خاصة وان الثورة التكنولوجية الحديثة أدت إلى ثورة أخرى في المجال العسكري ساهمت بدورها في تطوير طرق خوض الحروب.

- تصاعد المخاطر والتهديدات في الفضاء الالكتروني أدى إلى ظهور المنافسة بين الشركات العاملة في مجال الأمن السيبرانيل تعزيز سوق الإنفاق العالمي في تأمين البنية التحتية السيبرانية للدول بالإضافة إلى ظهور لاعبين آخرين من شبكات الجريمة المنظمة والإرهاب الالكتروني وغيرهم[1].

- تراجع النزاعات بين الدول وتزايد النزاعات الداخلية التي تقوم بين الدولة والفواعل المسلحة غير الحكومية مع إمكانية تدخل دول أخرى في هذه الصراعات الداخلية مساندة لأطراف التحالف.

- تصعيد التعاون بين الجهات المسلحة غير الحكومية وجهات الجريمة المنظمة العابرة للحدود الدولية وأن كانت أهدافها مختلفة تماما إلا أن المصالح المشتركة تدفعهم إلى التعاون، وأدى ذلك إلى زيادة الفوضى الأمنية ووجود مناطق خارجة عن سيطرة أجهزة الدولة.

- سيطرت الفواعل الأخرى من غير الدول على المواد والتقنيات المزدوجة الاستخدام والتي تستعمل لأغراض تجارية وقابلة لإعادة التوظيف واستعمالها لأعمال إرهابية مثل تحميل الدرونز بالمتفجرات آو استخدام الطابعة ثلاثية الأبعاد في تصنيع الأسلحة المتفجرة.[2]

- سعي الدول إلى تحديث قدراتها الدفاعية والهجومية لمواجهة مخاطر الحروب السيبرانية من خلال الاستثمار في البنية التحتية المعلوماتية وتأمينها، وتحديث قدراتها العسكرية لاستعدادها لمثل هذه الحرب عن طريق المشاركة الدولية في حماية البنية المعلوماتية والاستثمار في رفع القدرات البشرية داخل الأجهزة الوطنية المعنية، وهنا يصبح الخطر أكبر من خلال محاولة نقل القدرات من الدفاع الى الهجوم عن طريق استخدام تلك الهجمات في إطار إدارة الصراع مع الدول الأخرى[3].

وبهذا أصبحت حروب اليوم حروبا هجينة يلعب فيها التطور التقني والفضاء السيبراني دورا حاسما كما أن الحرب السيبرانية تتسم بالتطور السريع والمنافسة الشديدة والتعاون بين شركات البرمجيات الكبرى وشركات تصنيع السلاح وما ينجم عن ذلك من فرص للتكامل بين الجانبين.

---

[1] محمد صخري،"الحرب السيبرانية وتداعياتها على الأمن العالمي "، الموسوعة الجزائرية لدراسات السياسية والإستراتيجية،(27-06-2019)، على الرابط https://www.politics-dz.com

[2] شادي عبد الوهاب ،"حروب الجيل الخامس : التحولات الرئيسية في المواجهات العنيفة غير التقليدية في العالم "، مجلة دراسات المستقبل ، العدد01 ،نوفمبر 2017 ،ص. 06.

[3] عادل عبد الصادق،" أنماط الحرب السيبرانية وتداعياتها على الأمن القومي "، مجلة السياسة الدولية، العدد 208، افريل2017، المجلد 52،ص .35.

خاتمة:

ومما سبق يتضح أن الثورة الرقمية في المجال العسكري أثرت بشكل كبير في طبيعة الحرب وطريقة خوضها، إذ أدخلت التقنيات الحديثة في مجال تكنولوجيا المعلومات تغيرات جذرية في العمليات والتكتيكات العسكرية، وقد أثر التقدم التكنولوجي الهائل في بنية الثورات العسكرية على مستوى تنظيم القوات المسلحة والتحول في المذهب وأساليب القتال.

والثورة الرقمية أحدثت طفرة حقيقة في الحروب بحيث ابتكرت أساليب جديدة تختلف عن سابقتها ، واستناد على ذلك نجد أن مختلف التطورات الكبيرة في صناعة تكنولوجيا المعلومات ساهمت في ظهور الأنظمة والأسلحة الذكية التي سرعان ما أصبحت ضمن أساليب القتال الجديدة إذ عملت هذه الأسلحة الذكية على تقليل المدة الزمنية بين وقت تحديد الهدف ووقت المهاجمة ، كما انعكست على عقيدة استعمال الجيوش من خلال تطبيقات وبرامج الذكاء الاصطناعي إذ قامت بتطوير أسلحة صغيرة وذكية وفي نفس الوقت لديها القدرة على تقديم نتائج مرضية أثناء استعمالها في المواجهات الحربية كالطائرات بدون طيار التي أثبتت نجاحها كسلاح فعال في الحرب المعاصرة.

وعليه يمكن القول أن تطبيق تكنولوجيا الرقمية في القطاع العسكري نتج عنه تطور كبير في إستراتيجية شن الحروب وزيادة الفعالية القتالية عن طريق رقمنة ساحة المعركة، لكن بالمقابل ذلك خلقت أشكال جديدة للحرب ولعل أهمها الحرب السيبرانية التي تتدخل فيها فواعل أخرى غير الدول كما ان الرد على الهجوم الرقمي في حالة وقوعه قد تكون نتائجه كارثية.

قائمة المصادر والمراجع

أولا: باللغة العربية.

أ)- الكتب:

1)- عبد الرحمن حسن الشهري،"تطور العقائد والاستراتيجيات العسكرية "،(الرياض :بدون دار نشر، 2003).

2)-عباس بدران،" الحروب الالكترونية: الاشتباك في عالم متغير"، (بيروت: مركز دراسات الحكومة الالكترونية، 2010).

3)-إيهاب خليفة. القوة الالكترونية وأبعاد النحول في خصائص القوة، (مصر: مكتبة الإسكندرية ،2014).

4)-سركان بالكان، ترجمة مركز الخطابي للدراسات،"إستراتيجية داعش في استخدام الطائرات المسيرة "، نوفمبر 2019.

ب)- المقالات العلمية:

1)- إسماعيل صبري مقلد،" مخاطر تسببها الفجوة الرقمية: ثورة المعلومات وحروب المستقبل المحتملة"، مجلة استراتيجيا آفاق المستقبل، العدد15، يوليو/أغسطس/سبتمبر2012.

2)-إسماعيل زروقة "الفضاء السيبراني والتحول في مفاهيم القوة والصراع " ، مجلة العلوم القانونية والسياسية ، المجلد 1، العدد 01 ،أفريل 2019.

3)-مصطفى إبراهيم سلمان الشمنري "الأمن السيبراني وأثره في الأمن الوطني العراقي " مجلة العلوم القانونية والسياسية، كلية القانون والعلوم السياسية - جامعة ديالي المجلد 10 العدد 01. 2021.
4)-أميرة عبد العظيم محمد عبد الجواد "المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام «، مجلة الشريعة والقانون العدد 35 الجزء 3 ،2020.
5) -شادي عبد الوهاب «حروب الجيل الخامس: التحولات الرئيسية في المواجهات العنيفة غير التقليدية في العالم "، مجلة دراسات المستقبل ، العدد01 ،نوفمبر 2017 ،ص07.
6)-أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر ، مجلة المحقق الحلي للعلوم القانونية والسياسية ، كلية القانون ،جامعة بابل ، العدد الرابع ، المجلد 8 ديسمبر 2016.
7) -سماح عبد الصبور،"الصراع السيبراني.. طبيعة المفهوم وملامح الفاعلين"،مجلة السياسة الدولية العدد 208 المجلد 52،افريل2017.
8)- عادل عبد الصادق،" أنماط الحرب السيبرانية وتداعياتها على الأمن القومي "، مجلة السياسة الدولية، العدد 208، افريل2017، المجلد **52.**

ج)- مذكرات الماجستير:

صلاح حيدر عبد الواحد،"حروب الفضاء الالكتروني، دراسة في مفهومها وخصائصها وسبل مواجهتها " ،(مذكرة ماجستير غير منشورة، جامعة الشرق الأوسط ،قسم العلوم السياسية، كلية الآداب والعلوم ،تموز 2021).

د)- المواقع الالكترونية:

1)- المجال الخامس.. الحروب الالكترونية في القرن ال21، مركز الجزيرة للدراسات، على الرابط
http://studies.aljazeera.net/ar/issues/2010/20117212274346868.html
2)- عادل عبد الصادق، "الحروب السيبرانية: تصاعد القدرات والتحديات للأمن العالمي"، المركز العربي لأبحاث الفضاء الالكتروني، (2017/03/12). على الرابط
http://www.accronline.com/article_detail.aspx?id=28395
3)-روسيا اليوم، أقوى هجمات سيبرانية استهدفت روسيا،العربية، (2019/01/31)، على الرابط
https ://www.arabic.com
4)-لندن : بيونغ مسؤولة عن هجوم "واناكراي" الالكتروني" ،العربية،(2017/12/27)،على الرابط
https ://www.alarabiya.net
5)- جواداه آري غروس،" إيران حاولت اختراق نظام الإنذار الصاروخي الإسرائيلي "، تايمز أوف إسرائيل، (2019/02/25)، على الرابط
http://ar.timesofisrael.com
6)-"أكبر الهجمات الالكترونية منذ بداية 2021"العربية، (2021 /05/10)، على الرابط:
https:// www.alarabiya .net

7)-الجزائر تعلن فتح تحقيق حول عمليات تجسس تعرضت لها باستخدام برنامج بيغاسوس" فرانس24، (2021/07/23)، على الرابط:https//www.france24.com
8)-محمد صخري، "الحرب السيبرانية وتداعياتها على الأمن العالمي "، الموسوعة الجزائرية لدراسات السياسية والإستراتيجية، (2019-06-27)، على الرابط https://www.politics-dz.com

ثانيا: باللغة الأجنبية:

أ)- الكتب:

1)- Raportprepared by the Word in 2050 initiative," the digital révolution and sustainable développement : opportunities and challenges ". International institute for applied systèmes analysis (IIASA). Luxemburg. Austria ,2019.
2)- Metz,s and kievit.j,"Strategy and the revolution in military affairs ",from theory to policy .strategic studies institute ,1995.
3)-Saalbach, Klaus-Peter, "Cyber war Methods and Practice ". Germany : Osnabrueck,2019.

ب)- المقالات العلمية:

1)-Norman c. Davis, " an information-based revolution in military affaires ", strategic revieu,vol.24,No.01, winter1996.
2)- François Levieux, « la défense et les technologies de l'information et de la communication », Annales Des Mines, Novembre 2005.
3)- T. X. Hammes, « Technologies Converge and Power Diffuses ...The Evolution of Small, Smart, and Cheap Weapons, policyanaysis, no.786, ,27 January 2016.
4)-carlo al bertocuoco,"the revolution in military affairs: theoretical utility and historical evidence», researchpaper, no.142.april 2010.
5)-Elinorc.sloan ,"the revolution in military affairs implication for canada and nato", Canadian Military Journal, autum,2000.
6)-Dan Craigen and Nadia Diakun-Thibault and Randy Purse," Defining Cybersecurity, Technology Innovation Management Review", (Ottawa: Technology Innovation Management, October 2014).
7)-Schreier Fred, « On Cyberwarfare », Dcaf Horizon Working Paper No07.

ج)- المواقع الالكترونية:

1)-Kate Sullivan, " New York Times: US ramping up cyber-attacks on Russia", CNN, (17/06/2019). At: https://www.nytimes.com .
2)- Dustin Volz and Robert Mc Millan, " Hack suggests New Scope Sophistication for cyberattacks ", wall street journal, (17/12/2020). At: https://www.wsj.com