السنة: السابعة المجلد: 07 العدد:02 ص ص:172- 190
ISSN 2543-375X EISSN2676-1645

الحروب السيبرانية: المخاطر واستراتيجيات تحقيق الأمن السيبراني الدولي والداخلي.

Cyber wars - risks and strategies for achieving international and internal cyber security

ربيعي حسين*، جامعة الأخوة منتوري – قسنطينة1
hocine.rebiai@umc.edu.dz
وسمر محمود ، جامعة الأخوة منتوري – قسنطينة1
mahmoudouasmer04@gmail.com

تاريخ الإستلام : 2022/01/05 تاريخ القبول : 2022/02/28

الملخص : تهدف هذه الدراسة إلى تحديد مفهوم الحرب السيبرانية كأحدث شكل من أشكال الحروب القائمة بين الدول داخل الفضاء السيبراني، هذا الأخير الذي أصبح مصدر تهديد فعلي لأمن الدول والمجتمعات بصفة مشتركة ومنفردة، من خلال إتاحته لكل الأعمال العدائية ذات الطابع الإلكتروني ضد أي كان دون تمييز، بالإضافة إلى التطرق إلى الجهود الدولية التي تسعى إلى إرساء قواعد تحقق وتحافظ على الأمن السيبراني العالمي باعتباره إرثا مشتركا، كما تسلط الضوء على تجربة الجزائر في مجال خوضها لهذه الحرب في ظل تنامي التهديدات الدولية والإقليمية الموجهة ضدها في هذا المجال.

الكلمات المفتاحية: الحرب السيبرانية، الفضاء السيبراني، الأمن السيبراني، الهجمات الإلكترونية، التجسس الإلكتروني.

Abstract: This study aims to define the concept of cyber warfare as the latest form of inter-state warfare within cyberspace. This latter has become a source of threat to the states' security as well as societies, jointly and individually. This is due to its accessibility for all types of electronic hostilities against everyone with no discrimination. In addition to that, it is

* المؤلف المراسل

necessary to consider the international efforts being seeked to set up rules in order to achieve and preserve global cybersecurity that is considered as a common heritage. Moreover, this study sheds light on the Algerian experience in fighting this war in the light of the growing regional and international threats against it in this scope.

Keywords: Cyber wars - cyberspace – cyber security - cyber attacks - cyber espionage.

مقدمة :

تشهد ساحة الصراع الدولي بين فواعل الدول تحولا بارزا وذلك بالموازاة مع التطور الملفت في مجال تكنولوجيا التحكم في المعلومات ونظم الإتصالات، التي أصبحت من أساسيات حوكمة المجتمعات والدول، فقد أصبحت الإستراتيجيات العسكرية للدول تعتمد على التخطيط وتنفيذ الهجمات الإلكترونية ضد الدول الصديقة والمعادية على حد سواء بهدف إضعافها والسيطرة على فضائها السيبراني، وتحقيق الأهداف المسطرة من وراء ذلك في إطار ما يعرف بحروب الجيل الجديد، التي تعتبر بمثابة وسائل تحقيق الدمار وتحطيم الأمم بأقل تكلفة بعيدا عن التدخل والعمل العسكري التقليدي، من خلال إستهداف الأنظمة المعلوماتية العسكرية الهجومية والدفاعية بالإضافة إلى أنظمة التحكم الرئيسية للدولة ضمن شتى المجالات بالنظر إلى أثرها على المصالح العامة والخاصة على حد سواء، ولعل أن أبرز مثال على ذلك هوما عانته أوكرانيا نهاية سنة 2016 من إنقطاع في شبكة الكهرباء وحالة الشلل التامة المترتبة على ذلك بعد أن شنت عليها روسيا هجوما إلكترونيا استهدف نظام التحكم في محطات توليد الكهرباء، وكذلك إيران مؤخرا بتاريخ 26 أكتوبر 2021 بعد توقف كل محطات توزيع الوقود بفعل هجوم سيبرآني يرجح انه من إسرائيل يهدف إلى تأجيج مشاعر الإيرانيين ضد النظام .

ويشهد العالم حربا سيبرانية معلنة بين الولايات المتحدة الأمريكية من جهة والصين وروسيا وإيران، غير أن جانبها الخفي يظل أكبر من الظاهر للعيان، فهي ساحة مفتوحة دون قيد أو الخضوع لإذن قيادة عليا، وتعتبر الجزائر في قلب

هذا النوع من الحروب من خلال الحملات الهجومية التي تشنها ضدها الكيانات المعادية في صورة المغرب وإسرائيل بهدف إضعاف الدولة ومحاربة دورها الاستراتيجي في المنطقة، وهوما برز بشكل واضح في الآونة الأخيرة من خلال استغلال شبكات التواصل الاجتماعي لترويج الأخبار الكاذبة الشائعات والتحريض على المساس بمؤسسات الدولة بهدف إرباكها من الداخل والخارج، وقد ساعدهم في ذلك وسائل ومنصات التواصل الاجتماعي التي تعتبر الفضاء الأمثل لنشر الأفكار الهدامة للبنية والوحدة الوطنية والمرجعيات الدينية والثقافية والفكرية .

إن هذا التحول في نمط التهديد وصفة العدو وطبيعة قواعد الاشتباك، من التقليدي إلى السيبراني فرض تحولات جذرية على عديد المفاهيم التي تحكم قواعد الحرب ووسائلها وأثارها وآليات تنظيمها وتعزيز استقرار الأمن الدولي والداخلي للدول وهوما يدفعنا إلى معالجة ذلك من خلال طرح الإشكالية التالية : ما هو واقع الحروب السيبرانية بين فواعل الدول، وما هي الحلول المقترحة لتعزيز الأمن السيبراني دوليا وداخليا ؟ وفي سبيل الإجابة عن هذا التساؤل تضمنت هذه المساهمة البحثية العناصر التالية :

ـأولا : الفضاء السيبراني – ساحة القتال الجديدة .

يواجه المجتمع الدولي نوعا جديدا من الحروب تستعمل فيه طرق مستحدثه في القتال بعيدا عن ارض المعركة التقليدية من بينها الحروب السيبرانية، التي جاءت كنتيجة منطقية لتطور وانتشار الأنظمة المعلوماتية والشبكات، وبروز معطيات حيوية كالفضاء السيبراني والأمن السيبراني واحتلالهما لمكانة بالغة الأهمية في مسار حياة الدول، لما يشكلانه من دور أساسي في مجال الحفاظ على أمنها واستقرارها.

ـ1 فضاء القوة السيبرانية ـ التعريف .

تشمل فضاءات الفكر الإستراتيجي في مجال امن الدول على خمسة 05 عناصر هي، فضاء القوة البرية/الجوية/البحرية/الفضائية وفضاء القوة

السيبرانية، فإذا كانت الفضاءات الأربع الأولى ذات أهمية مطلقة في مجال الحروب التقليدية فإن فضاء القوة السيبرانية هوبيئة جديدة تستخدمها أطراف الحرب بغرض إضعاف العدو. (بوبرطخ، 2020، صفحة 24)

ويعرف بأنه " مجال أوبيئة إفتراضية تتكون من تفاعل عناصر مادية وأخرى غير مادية تتيح التواصل بين كل أجزاء العالم من خلال شبكات الكترونية مترابطة، وتسمح بتداول قدر غير محدود من المعلومات المختلفة، ويتمثل الجزء المادي في البنية التحتية الإلكترونية في شبكة الإنترنت والحاسبات المتصلة به، والعنصر غير المادي في الوسط الافتراضي الذي يتم من خلاله تداول المعلومات. (عسكر محمد، 2021، صفحة 262).

2- خصائص الفضاء السيبراني

يذهب الكثير إلى تشبيه الفضاء السيبراني إلى حد بعيد بالمحيط، فهو بطبيعته مجال إلكتروني يمتاز بالتجانس والمرونة، ولا تحده أي نوع من الحدود، فهو ذلك الفضاء الذي يسمح لأي كان من الولوج إليه دون قيود والتنقل بين حدوده ونطاقه وبلوغ أقصى حدوده في أقصر مدة زمنية معينة، ومن بين أهم خصائصه ثراءه من حيث المعلومات المخزنة عليه او المتداولة عبره. (léoutre, 2021, p. 137)

يعتمد الفضاء السيبراني كمجال افتراضي على نظم الحواسيب وشبكات الاتصال ومخزون هائل من البيانات بحيث يسمح بالاتصال بالشبكات دون تقييد بالحدود الجغرافية، ومن ابرز خصائصه انه أصبح مكمنا للتهديدات الإجرامية اللامتناهية من هجمات إلكترونية، وملاذا للمتطرفين والإرهابيين، ومجالا حيويا لتنفيذ سياسات التجسس الإلكتروني وإلحاق الضرر بالغير في صورة الحروب السيبرانية، وذلك راجع أساسا إلى غياب سلطة عليا تتحكم فيه وآليات تسمح بحصر مجال الخطر الناتج عنه سواء من الناحية القانونية او المؤسساتية الآلية . (شلوش، 2015، صفحة 190).

3ـ أهمية الفضاء السيبراني .

يعتبر الفضاء السيبراني أحد المقومات الأساسية في مجال تسير الدول الحديثة، فهومجال حيوي لا يمكن الإستغناء عنه من حيث المزايا التي يوفرها، إلا أن أهميته في المجال العسكري تعتبر إستراتيجية بإعتباره الفضاء الخامس في الشؤون الإستراتيجية، وذلك نظرا لتطور أدوات القتال الشبكي والإستخدام المتزايد لمفاهيم ثورة المعلومات في الحروب الحديثة، وتبرز أهميته من خلال إدارة العمليات الهجومية والدفاعية بواسطة الأنظمة المعلوماتية ضد شبكات العدو، وكذلك إدارة العمليات القيادية التي تجمع بين الهجمات الإلكترونية والتقليدية ضد أنظمة العدو للقيادة بهدف تعطيلها. (بوبرطخ، الصفحات 24 -25).

ثانيا : الحرب السيبرانية ـ مفهومها وأبعادها .

لقد أفرزت العولمة مجموعة من التطورات وتحديدا على الصعيد التكنولوجي، فتم الدمج بين الفضاء السيبراني والأساليب المستخدمة في مجال الصراعات الدولية، فأصبحت بذلك حرب المعلومات عمليات عسكرية تدور في ميدان تكنولوجي رفيع المستوى في صورة حرب سيبرانية بين القيادات الصديقة والمعادية. (غريب، 2018، صفحة 113)

1ـ تعريفها

تعني الحرب الإلكترونية الأفعال التي تقوم بها الدول القومية لاختراق الأنظمة والشبكات المعلوماتية للدول الأخرى بغاية إحداث الضرر والتخريب ويعرفها هيرش (herch)بأنها اختراق للشبكات الأجنبية من اجل تخريب أو تفكيك تلك الشبكات وجعلها غير قابلة للعمل . (بوبرطخ، صفحة 25)

وتعرف كذلك بأنها : كل فعل فردي أو جماعي مخطط له يهدف إلى المساس بوحدة وسلامة النظام المعلوماتي لمؤسسة أو منظمة أو دولة معينة، بإستخدام كل أو جزء من شبكة الإتصالات سواء الإنترنت أو أنواع من الشبكات الإتصالية الرقمية .(Lehu, 2018, p. 42) ، بحيث تؤدي إلى حدوث أضرار توازي ما قد ينجم عن إستخدام القوة العسكرية المسلحة وقد صنفتها وزارة

الدفاع الأمريكية إلى ثلاث 03 أصناف : حرب سيبرانية هجومية وأخرى دفاعية وإستخباراتية. (عسكر محمد، صفحة 275)

-2 طبيعتها ودوافعها.

تختلف الحروب السيبرانية من حيث طبيعتها لان الصراع داخل الفضاء السيبراني غير مضمون النتائج المتوقعة والمسطرة، فهي حروب تهدد وتستهدف النظام والأمن العام بصفة مباشرة من خلال محاولات شل وتعطيل الأنظمة المعلوماتية المتعلقة بالمسائل الحيوية للدولة المستهدف، كما انها ديناميكية ودائمة لأنها خفية فالدول في ظلها وقيادتها العسكرية إما في حالة هجوم اودفاع دائم. (غريب، صفحة 113)

كما أنها تتسم من حيث طبيعتها العملياتية :

-عدم وضوح الخطوة الفاصلة بين الحرب والسياسة وبين المقاتلين والمدنين.

-غياب التسلسل الهرمي للقيادات كما أنها لا تستند إلى قيادة وطنية.

-تستهدف جمع المعلومات الإستخباراتية والمتعلقة بالبنية الإستراتيجية.

-تستهدف تفكيك البنية النفسية والانسجام داخل مجتمع العدو. (بوبرطخ، صفحة 25)

أما من حيث دوافعها فيمكن ذكر إلى جانب واقع تزايد ارتباط العالم بالفضاء الرقمي وتراجع دور الدول في الرقابة والتحكم في الفضاء السيبراني وقلة تكلفة الحروب السيبرانية:

-ظهور قواعد البيانات Big Data حيث أدى الاعتماد على الأنظمة المعلوماتية في مجال اتخاذ القرارات العسكرية منها خصوصا وتسيرها إلى توفير كم هائل من المعلومات التي تستخدم في مجال تسيير المعارك وتنمية الكفاءات القتالية، وهوما جعل منها هدفا لمختلف الهجمات الإلكترونية بغرض الاستيلاء عليها .

-طغيان الطابع الهجومي على الدفاعي بحيث تميل الكفة في مجال الحروب السيبرانية للهجمات الإلكترونية أكثر من الأحزمة الدفاعية وهوما جعل الكل إما عنصرا مهاجما او مدافعا بشكل إجباري في ظل عدما اعتراف الهجمات الإلكترونية بالحدود لا المكانية ولا الزمانية. (Danet, 2013, pp. 130-131)

-ثالثا : الأمن السيبراني في مواجهة الحروب السيبرانية.

إنتقل العالم بعد الحرب الباردة من مرحلة التعامل مع القضايا الأمنية من مفهوم العدو إلى مفهوم التهديد دون إقصاء كلي لمفهوم الأعداء، هذا الإنتقال إنعكس على مفهوم الأمن الذي أصبح أكثر تعقيدا، بفعل الأولوية المعطاة لأحدهما على حساب الأخر، فخلال الحرب الباردة سيطرت فكرة القوة والنظرة الواقعية على العلاقات الدولية فطغت صفة العدو على الخطر والتهديد وارتكزت على القوة العسكرية، لكن في ظل التطور التكنولوجي الحاصل وتنامي التهديدات السيبرانية غير المادية أصبح الأن من الصعب مواجهة هذه التهديدات عن طريق القوة العسكرية .(حموم، 2011، صفحة 73)

-1الأمن السيبراني – المفهوم.

يعرف الأمن السيبراني على انه عبارة عن مجموعة من الوسائل التقنية والتنظيمية والإدارية التي يتم إستخدامها لمنع الإستخدام غير المصرح به وسوء الإستغلال وإستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات، وتعزيز الحماية وسرية وخصوصية البيانات الشخصية وإتخاذ جميع التدابير اللازمة لحماية مستخدمي الفضاء السيبراني، وهو جزء لا يتجزأ من التكتيكات الحديثة للحروب بإعتباره المجال الخامس للحروب الحديثة بعد البر والبحر والجووالفضاء .(عطية، 2019، صفحة 104)

وتتصل فكرة الأمن السيبراني بشكل وثيق بما أصبح يعرف بالقوة السيبرانية، أي قدرة الدول في السيطرة والتأثير داخل وعبر الفضاء السيبراني لدعم المجالات الأخرى للسلطة، وتعتمد في تحقيقها على قدرة الدولة على تطوير

موارد العمل في الفضاء السيبراني وهوما يختلف عن العمل في الفضاء البري او الجو او البحري، فبدل الطائرات والسفن والأسلحة تحتاج الدولة إلى مقومات رقمية كالحواسيب والأنظمة الشبكات والاتصالات وبنية تحتية قوية وعناصر ذات قدرات عالية تشارك في ذلك.(شرايطية، 2020، صفحة 400).

-2 مرتكزات وعناصر الأمن السيبراني .

يرتكز الأمن السيبراني على مرتكزين أساسين هما :

-التقنية : تلعب تكنولوجيا المعلومات دورا كبيرا في تحقيق الأمن السيبراني فهي ما يؤمن المعلومات المخزنة والمتداولة .

-التشريع : يلعب التشريع دور العنصر الذي يستجيب لمتطلبات البيئة الرقمية في مجال التنظيم ووضع الآليات القانونية الكفيلة لضمان الحماية الملائمة للفضاء السيبراني .

أما عناصره فتشمل على :

-السرية والموثوقية التي يقصد بها التأكد من عدم الكشف عن المعلومات .

-التكامل وسلامة المحتوى من التلاعب.

-الإستمرارية والتي يقصد بها ضمان تقديم الخدمة دون انقطاع .(قصعة، 2020، صفحة 380)

-3 أبعاد الأمن السيبراني.

-البعد العسكري : تكمن الميزة الأساسية للقوة السيبرانية في قدرتها على ربط الوحدات العسكرية ببعضها البعض عبر الشبكات العسكرية في الفضاء السيبراني، بما يسمح بإتخاذ القرارات والقدرة على تحديد الأهداف وتدميرها .

-البعد الإقتصادي : يرتبط الأمن السيبراني بالإقتصاد إرتباطا وثيقا فإعتماد إقتصاد المعرفة يتصل وثيقا بتقنيات المعلوماتية.

-البعد الإجتماعي: يرتبط الأمن السيبراني بالخصوص بشبكات التواصل الإجتماعي التي تسمح وتتيح جمع المعلومات المتعلقة بالأفراد بالخصوص بما اصبح يعرف " الهندسة الإجتماعية" من خلال معرفة تطلعاتهم السياسية والإجتماعية وإستغلالها لتحقيق تطلعاتهم.

-البعد القانوني: وهي العلاقة المتجلية في الطبيعة التبادلية بين التطور التكنولوجي وتطور النظام القانوني والتشريعي.(عطية، صفحة 107)

-رابعا : الحروب السيبرانية –الأمن القومي والفواعل .

أصبح الفضاء السيبراني لا يختلف عن الفضاءات الأخرى الجوية والبرية والبحرية والفضائية فيما يتعلق بمبادئ الحرب وخصائص القوة، بحيث أصبحت العقيدة العسكرية هي السارية ضمن نطاقه، والتي ترتكز على اللامركزية في التنفيذ والمركزية في السيطرة. (السعبري، 2020، صفحة 423).

ـ1 تحديد مفهوم الأمن القومي وأبعاده.

يشهد الفضاء السيبراني محاولات سيطرة واسعة على المؤسسات الحيوية للدولة عن طريق إستخدام أسلحة معلوماتية ضد المنشآت المدنية والعسكرية وأنظمة الدولة ومؤسساتها، بهدف تعطيل عملها بشكل يمثل تهديدا مباشرا بأمنها القومي، من خلال تدمير بنيتها التحتية المعلوماتية العسكرية والمدنية والإقتصادية والسياسية، فتشل عن القدرة على صنع القرار والسيطرة والهجوم على الأنظمة الدفاعية للدولة المهاجمة . (شلوش، صفحة 199).

فالأمن القومي حسب تعريف " كرنبرج" هو: ذلك الجزء من سياسة الحكومة الذي يستهدف خلق الظروف المواتية لحماية القيم الحيوية، ويعرفه " كسينجر" بأنه : أي تصرفات سعى المجتمع عن طريقها إلى حفظ حقه في البقاء " ويتميز الأمن القومي بمفهومه المعقد والمركز لأنه يتقاطع مع مفهوم القوة والسلام، كما انه يعبر عن الإتجاهات الإستراتيجية المتعلقة بالجوانب العسكرية.

تتعلق أبعاد الأمن القومي بمجموعة من السياسات المتخذة لضمان سلامة الإقليم والدفاع عن مكتسبات الأمة في مواجهة الأعداء سواء من الداخل أوالخارج، وقد إتسع مفهومه ليشمل الأبعاد السياسية والإجتماعية والإقتصادية بعد ان ثبت أنها تشكل مصدر تهديد للأمن القومي إلى جانب الأبعاد العسكرية. (محمدي، 2019، صفحة 70).

وقد تزايدت العلاقة بين الأمن القومي والتكنولوجيا الحديثة خاصة مع إمكانية تعرض المصالح الإستراتيجية للدول إلى أخطار وتهديدات من خلال الفضاء السيبراني،وهوما دفع إلى التفكير في صياغة حديثة لمفهوم الأمن القومي، فقد أصبح توفير الأمن القومي الإلكتروني مرهونا بوجود إجراءات الحماية ضد الأعمال العدائية، وهوما جعله يمتد إلى خارج إقليم الدولة ليشمل الأمن الجماعي العالمي.(صالحي، 2021، صفحة 381).

- 2 الفواعل في الحروب السيبرانية

يمكن تقسيم الفواعل في الفضاء السيبراني ومن يمتلكون القدرة على شن الهجمات الإلكترونية إلى:

-الدول : تعتبر الدول الفاعل الأكثر قوة في مجال الفضاء السيبراني ومن يملك القدرة الأكبر على شن الحروب السيبرانية، فحسب إحصائيات سنة 2018 فإنه تمكنت أكثر من 180 دولة من امتلاك ترسانة أسلحة إلكترونية هجومية ودفاعية، وهومؤشر على زيادة معدلات ونشاط الهجمات الإلكترونية مستقبلا.

- الجماعات الإفتراضية : وهم شبكات تتكون من مجموعة من الأفراد يتشاركون نفس الأفكار والرغبات النشاط ويهدفون إلى تحقيق غاية اواهداف مشتركة، كمجموعة " أنونيموس"، وأكثر ما تؤثر هذه المجموعات إذا ما كانت متصلة بالجماعات الإرهابية على شاكلة تنظيم الدولة الإسلامية في الشام والعراق الذي فرض نفسه في وقت ما كفاعل مؤثر على الأمن الدولي عبر الفضاء السيبراني.(عطية، صفحة 107).

وقد أحصى معهد الأبحاث الأمريكي simon-wiesenthal قرابة 1500 موقع يروج للعنف والتطرف سنة 1999، وأغلقت الوم ألأمريكية على سبيل المثال سنة 2005 أكثر من 6000 موقع يشكل مصدر للفكر المتطرف .(موسى، 2009، صفحة 227).

-الأفراد: أضحى الفرد داخل الفضاء السيبراني صاحب قدرة وتاثير في مجال إحداث التغيير فقد بلغ عدد الأفراد المتصلين بشبكة الأنترنت سنة 2021 - 4,9 مليار نسمة، فقدرتهم على التحكم في آليات تسيير الشبكات والمنظومات الإلكترونية قد تفوق قدرات هيئات متخصصة بذاتها، كما ان ظهور وسائل التواصل الإجتماعي(يستخدم أكثر من 3,9 مليار نسمة حول العالم منصات التواصل الإجتماعي) مكن الأفراد من ممارسة حريتهم وإبداء أرائهم بل والمشاركة في تهديد من وسلامة المجتمعات المعادية .(عطية، صفحة 107).

3- التجسس الإلكتروني أبرز أسلحة الحروب السيبرانية.

يعتبر التجسس الإلكتروني من أهم المستويات التمهيدية للعمليات الحربية السيبرانية، ويعرف بأنه وسيلة للإعتراض غير المصرح به لأنظمة الاتصالات والشبكات والبيانات من أجل الحصول على البيانات والمعلومات والتلاعب بها، فالتجسس الإلكتروني أولى أشكال التهديد التي تمس بالأمن القومي الوطني، وتهدد مصالح الدولة والأفراد.(رقولي، 2019، صفحة 74).

وقد عرفه المُؤلف الخاص بحلف الناتوبعنوان : Peace Time Regime For State Activities In Cyberspace بانه : قيام دولة أو جهاز تابع لها او وكيل عنها بالإطلاع على أو نسخ البيانات السرية غير المتاحة للجمهور اوالمحفوظة على أنظمة تكنولوجيا المعلومات أو شبكات الإتصال الموجودة في إقليم أو منطقة خاضعة لولاية دولة أخرى، بواسطة عمليات سرية وبذرائع مزيفة أو كاذبة ودون ترخيص او موافقة من مالكي او مستخدمي هذه الأنظمة. (عسكر محمد، صفحة 277)، وقد إهتز المجتمع الدولي عقب إكتشاف

فضيحة التجسس المعروفة بإسم قضية " برنامج بيغاسوس" التي تورط فيها النظام الصهيوني والمغربي.

ويهدف التجسس عموما عبر الفضاء السيبراني إلى :

-إختراق النظام المعلوماتي بهدف نقل المعلومات اوالبرامج كليا اوجزئيا.

-اختراق النظام المعلوماتي للمؤسسات الهامة بهدف الاطلاع على الأسرار .

-اختراق النظام المعلوماتي بهدف تدمير ثروته المعلوماتية جزئيا أوكليا.(الدسوقي عطية، 2009، صفحة 315).

ـخامسا : الآليات الدولية والإقليمية لتجسيد البرنامج العالمي للأمن السيبراني.

ـ1 دور الإتحاد الدولي للإتصالات التابع لوكالة الأمم المتحدة المتخصصة.

الاتحاد الدولي للاتصالات هووكالة الأمم المتحدة المتخصصة في مجال تكنولوجيا المعلومات والاتصالات (ICT).يتمثل الدور الأساسي للاتحاد، استناداً إلى توجيهات القمة العالمية لمجتمع المعلومات (WSIS)، في بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات (ICT)، ويشتمل برنامجه على تنفيذ خمس ركائز أو مجالات عمل هي: التدابير القانونية؛ والتدابير التقنية والإجرائية؛ والهياكل التنظيمية؛ وبناء القدرات؛ والتعاون الدولي، وهو مصمم من أجل التعاون والكفاءة بين أصحاب المصلحة المتعددين، من خلال تشجيع التعاون مع جميع الشركاء ذوي الصلة وفيما بينهم، وقد حظي الإطار الذي توفره الركائز الخمس للبرنامج بالتقدير على نطاق واسع من جانب أعضاء الاتحاد ولا يزال يوفّر إطاراً واسعاً للتعاون الدولي بشأن الأمن السيبراني، فاعتباراً من2019، وقّع أكثر من 125 بلداً و/ أوصدق على اتفاقيات أو إعلانات أو مبادئ توجيهية أو اتفاقات مختلفة بشأن الأمن السيبراني والجريمة السيبرانية مثل اتفاقية مجلس أوروبا بشأن الجريمة السيبرانية لعام 2001 التي صادقت عليها 65 دولة إلى غاية مارس 2020

والبروتوكول الإضافي الثاني للاتفاقية بشأن الأمن السيبراني الذي بدأت المفاوضات بشأنه في 2017.

كما تم نشر دليل تالين 02 - سنة 2017، الذي يشير إلى أن تغطية القانون الدولي الذي يحكم الحرب السيبرانية تنطبق أيضاً على الأنظمة القانونية في وقت السلم..(الوثيقة رقم A65/C20 المتضمنة تقرير الأمين العام للإتحاد الدولي للإتصالات بخصوص المبادئ التوجيهية لتنفيذ البرنامج العالمي للأمن السيبراني، 2020)

ـ2 جهود الأمم المتحدة في بلورة أسس فضاء سيبراني آمن.

يعتبر قرار الجمعية العامة للأمم المتحدة الصادر في 27 ديسمبر2019 :بشان مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، أحدث قرارات الجمعية العامة لإنشاء لجنة خبراء حكومية دولية مخصصة مفتوحة العضوية تُمثَّل فيها جميع الأقاليم، لوضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية. آخذة بعين الاعتبار كامل الصكوك والجهود العالمية المبذولة حالياً لمكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، بما في ذلك على وجه الخصوص، عمل فريق الخبراء الحكومي الدولي المفتوح العضوية المعني بإجراء دراسة شاملة عن الجريمة السيبرانية وقد اعتمدت الجمعية العامة القرار بأغلبية 79صوتاً مؤيداً مقابل 60 صوتاً معارضاً مع امتناع 30 دولة عن التصويت.(الوثيقة رقم A65/C20 المتضمنة تقرير الأمين العام للإتحاد الدولي للإتصالات بخصوص المبادئ التوجيهية لتنفيذ البرنامج العالمي للأمن السيبراني)

ـ3 دور المركز العربي الإقليمي للأمن السيبراني(ITU-ARCC) ـ نموذجا.

تم تأسيس المركز العربي الإقليمي للأمن السيبراني (ITU-ARCC) من قبل الاتحاد الدولي للاتصالات (ITU) وسلطنة عمان في ديسمبر 2012 ممثلة في وزارة التقنية والاتصالات، مع رؤية لإنشاء بيئة أكثر أمناً وتعاوناً في مجال الأمن السيبراني في المنطقة العربية وتعزيز دور الاتحاد الدولي للاتصالات في بناء الثقة

والأمن في استخدام تكنولوجيا المعلومات والاتصالات في المنطقة. تماشياً مع أهداف الأجندة العالمية الأمن السيبراني للاتحاد الدولي ومن مهامه:

- تكوين مركز موحد للدول الأعضاء للإدارة وتنفيذ أهداف البرنامج العالمي للأمن السيبراني.

- الإشراف على تنفيذ البرنامج العام للأمن السيبراني للاتحاد الدولي للاتصالات في جميع أنحاء المنطقة العربية.

- العمل على وضع الأطر والخطط في مجال الأمن السيبراني من خلال إجراء الدراسات الإقليمية ورفع مستوى الوعي والخبرات في الأمن السيبراني في قطاع البني التحتية للمعلومات (https://arcc.om/, 29/12/2021).

ـ سادسا : الجزائر في مواجهة الحروب السيبرانية

تشهد الجزائر شكلا جديدا من الصراع والتحدي الأمني، تدور وقائعه ضمن الفضاء السيبراني تستهدف أساسا الأمن القومي والوحدة الوطنية بالذات من قبل عديد الفواعل الدولية في صورة دول أو منظمات او أفراد، ولعل ان معدلات التهديدات السيبرانية في تصاعد مستمر وآخذ في الزيادة من حيث خطورتها ودرجة تهديدها خصوصا من قبل التحالف المغربي الإسرائيلي الذي يصنف كالخطر الأول على امن البلاد وإستقرارها وبذلك فقد صرح السيد رئيس الجمهورية عبد المجيد تبون بتاريخ: 2021/11/08 بمناسبة ترؤسه ندوة رؤساء البعثات الدبلوماسية والقنصلية الجزائرية بالخارج بأنه :" إن قراءتنا للسياق الدولي الذي تتفاعل معه دبلوماسيتنا لن يكتمل دون التعرض للتهديدات التي تثقل كاهل الجزائر بشكل مباشر وتهدف إلى إضعافها من الداخل مستعملة في ذلك ما يعرف بحرب الجيل الرابع، التي تتم ممارستها ضد بلادنا في إطار مخطط واسع يستهدف إفريقيا والشرق الأوسط". وقد أكد التقرير السنوي لسنة 2020 لمخبر الأمن السيبراني KASPERSKY ان الجزائر تحتل المركز الثاني من حيث العتاد الإلكتروني المستهدف بواسطة هجمات إلكترونية .

1 -الإستراتيجية الوطنية لتحقيق الأمن السيبراني

على غرار دول العالم لم تعد الجزائر بمنأى عن التهديدات السيبرانية التي لا تعترف بالحدود الجغرافية او القانونية، لذا فهي تعمل على تعزيز إستراتيجيتها الوطنية السيبرانية في إطار تجسيد مشروع حوكمة الانترنت ومجتمع معلوماتي منفتح وآمن في نفس الوقت، وتستند الآليات العملية لتنفيذ هذه الإستراتيجية عموما على دور الجيش الشعبي الوطني لما يملكه من قدرات ومؤهلات متقدمة في هذا المجال وقد اتخاذ هذا النهج منذ نوفمبر 2015 أين تم إستحداث مصلحة الدفاع السيبراني ومراقبة الأنظمة لأركان الجيش الشعبي الوطني التي جاءت تأكيدا على عزم القيادة العليا على إرساء بيئة سيبرانية أمنة ومستدامة ومحصنة من المخاطر والتهديدات، والتي تعمل على المستوى العسكري على تعزيز القدرات الدفاعية السيبرانية وتامين منظومة الأسلحة والإعلام والإتصال العسكرية، كما تسهر على التنسيق مع الهيئات الوطنية ذات الصلة على إعداد سياسة وطنية خاصة بتامين المنشاة الحساسة في المجال السيبراني .

وفي نفس السياق تم سنة 2016 إستحداث المرجعية الوطنية الموحدة لأمن الإعلام الآلي المكيفة والتي كان الهدف منها تعميم الترتيبات بشان حماية وتامين الأنظمة المعلوماتية على مستوى هياكل ومؤسسات الدولة وتحسيس وتوعية مستخدمي شبكة الأنترنت بالمخاطر الناتجة عنها .

وأمام تصاعد حجم التهديدات المتصلة بالهجمات الإلكترونية التي تستهدفنا عموما أولى المخطط العام للحكومة المصادق عليه بتاريخ 06 فيفري 2020 خلال الإجتماع الإستثنائي لمجلس الوزراء أهمية بالغة لتعزيز قدرات الجيش الشعبي الوطني في مجال الدفاع السيبراني على وجه الخصوص، وفي ذات الإطار فقد تم بتاريخ 20 جانفي 2020 وبناء على صدور مرسوم رئاسي وضع منظومة وطنية لأمن الأنظمة المعلوماتية موضوعة لدى وزارة الدفاع الوطني تشمل المجلس الوطني لأمن الأنظمة المعلوماتية بالإضافة إلى وكالة أمن الأنظمة المعلوماتية تعمل كل منهما على دراسة وإعداد الإستراتيجية الوطنية مجال

الأمن السيبراني مع التنسيق والعمل على تنفيذ الإستراتيجية الوطنية في نفس المجال.

كما تم في إطار تجديد آليات تنفيذ هذه الإستراتيجية وبتاريخ 18 جويلية 2020 وفق ما نشر في الجريدة الرسمية رقم : 40 لنفس السنة وبموجب مرسوم رئاسي إعادة هيكلة وتنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وهي سلطة إدارية مستقلة موضوعة تحت تصرف رئيس الجمهورية تعكف على اقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المعلوماتية، وفي سياق متصل تم شهر أوت 2021 استحداث قطب جزائي متخصص جديد مكلف بمتابعة الجرائم السيبرانية ومكافحتها، وهي الجهود التي تعكس الاهتمام الذي توليه الجزائر من خلال قيادتها السياسية والعسكرية لتامين الفضاء السيبراني داخليا وخارجيا من كل أنواع التهديدات.(جنادي، 2020، صفحة 31).

2 -قراءة في إستراتيجية الجيش الشعبي الوطني في مجال الدفاع السيبراني

تتمحور استراتيجية الدفاع السيبراني للجيش الشعبي الوطني حول تعزيز وتحيين الإطار القانوني المتعلق باستعمال تكنولوجيات الإعلام والاتصال وتامين المنظومات المعلوماتية والاتصالية، وتقوم أساسا على سبعة 07 محاور هي :

-جانب وظيفي وتنظيمي يهدف إلى تنفيذ أعمال الدفاع السيبراني بشكل موجه ضمن سلسلة وظيفية وتنظيمية مكرسة لضمان تجانس الأعمال

-جانب قانوني يهدف من خلاله على تحين وتعزيز الإطار القانوني لضمان أمن المنظومة المعلوماتية بشكل دائم ومستمر

- جانب الموارد البشرية يسمح بتوفير مورد بشري ذو كفاءة عالية في مجال النشاطات العملياتية والتسيير في مجال الدفاع السيبراني

-جانب تقني يعمل من خلاله على رفع القدرات التقنية للحماية واليقظة وضمان القدرة على الرد السريع على الهجمات السيبرانية

-جانب الوقاية والتحسيس لمستخدمي الجيش والقطاعات الأخرى بخطر استخدامات تكنولوجيا الإعلام والاتصال .

-جانب التعاون في مجال الدفاع السيبراني إلى جانب جيوش الدول الصديقة والشريكة من أجل ضمان نقل واكتساب الخبرات وتطويرها.

- جانب البحث والتطوير الذي تعتبر جانبا حاسما في إستراتيجية الدفاع السيبراني من خلال القدرة على تشخيص المشكلات وإيجاد الحلول لها. (بوكبشة، 2017، صفحة 35)

ويسهر الجيش الشعبي الوطني على تنظيم وبشكل دوري منذ سنة 2017 الملتقى المتعلق بالأمن والدفاع السيبراني أخره الذي أنعقد بين تاريخ 23 و24 ماي 2022 تحت عنوان" الأمن السيبراني والدفاع رهانات وتحديات" وكذلك الملتقى المنظم يوم 30 نوفمبر 2021 بعنوان " السيادة الرقمية في مواجهة قوة غافام " من قبل المعهد العسكري للوثائق والتقويم والاستقبالية بالتنسيق مع مصلحة الدفاع السيبراني ومراقبة امن الأنظمة لدائرة الاستعمال والتحضير لأركان الجيش الشعبي الوطني.

- الخاتمة

يتضح من خلال ما سبق التعرض له بان الحروب السيبرانية قد خرجت من فصول التصورات المستقبلية إلى الواقع والتطبيق، فقد أضحى الفضاء الرقمي ساحة قتال اشتباك ما بين الدول، وهي في منحى تصاعدي مستمر من حيث تطور أساليبها وتهديداتها، كما يتأكد بشكل واضح مدى خطورتها وتأثيرها على الأمن الجماعي والفردي للدول من خلال زيادة ارتباط هذه الأخيرة بالأنشطة المعلوماتية، فكلما زاد منحى التطور التكنولوجي في هذا الجانب زادت معه حدة وشراسة الهجمات السيبرانية، كما ان أغلب الدول قد ركبت رحال هذه الحرب بصفتها عنصرا مهاجما مسيطرا او مدافعا حفاظا على أمنها السيبراني، خصوصا في ظل بطئ الحركات التشريعية الدولية منها خصوصا في الحد من خطورة هذه الحروب، وفشل المجتمع الدولي في تأطير وتنظيم

إستخدامات الفضاء السيبراني بشكل سلمي، ويمكن حصر أهم النتائج المتوصل إليها في النقاط التالية :

-أن الفضاء السيبراني هو أحد العناصر الإستراتيجية التي تعتمد في مجال تحقيق الأمن القومي نظرا لحجم التهديدات التي يحتويها .

-أن الحروب السيبرانية في مراحلها الأولى وصورها البسيطة، فما يمكن أن تأول إليه من حدة وخطورة مستقبلا متعلق بدرجة التطور التي ستئول إليها النظم المعلوماتية.

-تطابق موازين القوى الدولية على واقع الحروب السيبرانية فغالبية الدول العظمى أصبحت هي المسيطرة في مجال الأمن السيبراني العالمي، عكس الدول النامية والضعيفة التي لا نجد لها أثرا في هذا المجال.

-تعتبر الجهود الدولية المبذولة من قبل الاتحاد الدولي للاتصالات ولمختلف الوكالات الإقليمية الأخرى، جهودا بسيطة بالنظر إلى عدم اعتراف الدول المسيطرة في مجال الحروب السيبرانية بأي قيود وضوابط وعملها على تطوير منظومتها الحربية السيبرانية الهجومية والدفاعية، واضعة الأمن الدولي والفردي للدول المستهدفة كأخر اهتماماتها .

-تعتبر الجزائر من الدول التي تبذل جهودا معتبرة للحاق ومواكبة النسق التقني والقانوني في مجال بناء استراتيجية أمنية سيبرانية فعالة مقارنة بدول الجوار في ظل تنامي التهديدات وزيادة حدتها .

ـ قائمة المراجع

ـ باللغة العربية
-الكتب :
الدسوقي عطية,طارق إبراهيم .(2009) الامن المعلوماتي-النظام القانوني للحماية المعلوماتية. مصر .دار الجامعة الجديدة للنشر .
موسى مصطفى محمد .(2009).الإرهاب الإلكتروني.الطبعة 01 مصر.دار الكتب والوثائق القومية المصرية.
-المقالات:
بوبرطخ نسيم. (2020). الفضاء السيبراني مسرح الصراعات الجيوسياسية المعاصرة. مجلة الجيش .العدد 685.

بوكبشة محمد (2017) - الدفاع والأمن السيبراني أولوية قصوى .مجلة الجيش. العدد 651.
جنادي إسماعيل(2020). الدفاع السيبراني من أهم تحديات الجيش الشعبي الوطني .مجلة الجيش العدد 685.
حموم فريدة .(2011) .الأمن الإنساني بين جدلية أمن الإنسان وامن الدولة .مجلة الحكمة. المجلد 03.العدد 06.
رقولي كريم ونويوة لخضر. (2019). الأمن السيبراني المتوسطي بين الواقع والرهانات الأمنية. مجلة طبنة للدراسات العلمية الأكاديمية. المجلد 02.العدد02.
السعبري بهاء عدنان. (2020). العناصر التقنية للتهديد الإكتروني.مجلة مركز دراسات الكوفة. العدد 57.
شرايطية سميرة. (2020). السيادة السيبرانية في الصين بين متطلبات القوة وضروريات الأمن القومي. المجلة الجزائرية للامن والتنمية، المجلد 09.العدد 16.
شلوش نورة. (2015) القرصنة الإلكترونية في الفضاء السيبراني التهديد المتصاعد لأمن الدول . مجلة مركز بابل للدراسات الأساسية.المجلد 08. العدد02.
صالحي نصيرة(2021) القوة الذكية التنافس العالمي على قوة الفضاء الإلكتروني والقدرات السيبرانية .دفاتر السياسة والقانون المجلد 13 .العدد01.
عادل محمد عسكر محمد. (2021). وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم- دراسة على ضوء دليل تالين بشان القانون الدولي المطبق على العمليات السيبرانية . مجلة البحوث القانونية والإقتصادية.المجلد 33.العدد01.
عطية إدريس. (2019). مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري. مجلة مصداقية . المجلد 01 – العدد01.
غريب حكيم. (2018). الإرهاب السيبراني والأمن الدولي التهديدات العالمية الجديدة وأساليب المواجهة. المجلة الجزائرية للدراسات السياسية، المجلد 05. العدد02.
قصعة سعاد. (2020). تحديات الأمن المعلوماتي في مواجهة الجرائم الإلكترونية في ظل الإعلام الجديد. مجلة المعيار. المجلد 24.العدد 50.
محمدي صليحة وشفيعة حداد. (2019). الإرهاب الإلكتروني والأمن القومي للدول نمط جديد وتهديدات مختلفة. المجلة الجزائرية للأمن والتنمية، المجلد 08.العدد15.
-الوثائق:
الوثيقة رقم A65/C20 المتضمنة تقرير الأمين العام للإتحاد الدولي للإتصالات بخصوص المبادئ التوجيهية لتنفيذ البرنامج العالمي للأمن السيبراني.(2020). متوفرة على شبكة الأنترنت على الرابط : https://bit.ly/3zmNVuX تم الإطلاع بتاريخ : 2021/12/29.
مواقع إلكترونية:
موقع المركز العربي للامن السيبراني : https://bit.ly/3pQdcLa تم التصفح بتاريخ (2021/12/28).
-باللغة الفرنسية .
-المقالات:
Danet didier. (2013). la strategie millitaire a l'heure des NTIC et du BIGDATA quelle hypothese structurante. revue internationale dinteligence economique .numero 05.
Lehu jean marc (2018). cyberattaque : la gestion du risque est elle encore possible. la revue des siences de gestion .numero 291/292.
Léoutre pierre marie (2021). l'appropriation du cyberespace pour la politque. Revue de la scurité globale. numero25.