تأثير الفضاء الافتراضي على الأمن القومي
The influence of cyberspace on national security

عبد الكريم باسماعيل*
جامعة قاصدي مرباح ورقلة (الجزائر)
مخبر تحولات سياسية اجتماعية اقتصادية في التجربة الجزائرية
abdelkrim.basmail@yahoo.com

تاريخ الاستلام: 2021/05/21 تاريخ القبول للنشر: 2021/07/20 تاريخ النشر: 2022/01/01

ملخص

تعاني الدول الحديثة من معضلة حماية سيادتها وتأمين حدودها من التدخل الخارجي، في هذا الإطار يعتبر الفضاء الافتراضي أحد أهم العوامل المؤثرة في بناء منظومة الأمن بالنسبة للدولة؛ لما يشكله من مجال مفتوح لتصاعد التهديدات الأمنية وانعدام الاستقرار. حيث يهدف الهجوم عبر الفضاء الإلكتروني إلى السيطرة على بنى مؤمنة إلكترونيا بغرض تعطيلها. يهدف هذا البحث إلى فحص مضمون الفضاء السيبراني، وكيفية توظيفه لأغراض تهديد الأمن القومي للدول، وما هي مصادر وأنواع وأبعاد هذا التهديد. نتساءل عن كيفية حماية الدول لحدودها سواء كان ذلك بالجيوش الإلكترونية أو الأطر القانونية، وعلاقة ذلك كله

* المؤلف المراسل

بتحولات النسق الدولي ومستقبل مفهوم السيادة.

- الكلمات المفتاحية: الفضاء الافتراضي، السيبرانية، الأمن القومي، السيادة، الدولة القومية.

Abstract:

Modern countries suffer from the dilemma of protecting their sovereignty and securing their borders from external interference. In this context, the Cyberspace is considered one of the most important factors affecting the building of the security system for the state, as it is an open field for the escalation of security threats and instability. An attack through cyberspace aims to take control of cyber-secured structures in order to disable them.

This research aims to examine the content of cyberspace and how to use it for the purposes of threatening the national security of states. We ask about how countries protect their borders, whether by electronic armies or legal frameworks, and how relates to the changes in international system and sovereignty.

key words: Cyberspace; cybernetics; national security; sovereignty; national state;

مقدّمة:

تعاني الدول الحديثة من معضلة حماية سيادتها وتأمين حدودها، في هذا الإطار يعتبر الفضاء الافتراضي (السيبيراني) أحد أهم العوامل المؤثرة في بناء منظومة الأمن بالنسبة للدولة؛ لما يشكله من مجال مفتوح لتزايد التهديدات وانعدام الاستقرار. من ثم أضحت إشكالية الحفاظ على الأمن القومي للدولة موضوعا غاية في الأهمية في مجال الدراسات الأمنية والإستراتيجية على حد سواء من جهة لتعدد مصادر التهديد الإلكتروني، ومن جهة أخرى عدم قدرة الدول على استيعاب التغيير الحاصل في مجال التهديدات السيبرانية وعدم قدرتها على الحد من خطورتها، ما يؤثر فعليا في كيفية حماية حدودها وأمنها الوطني، هذا ما

يشكل مأزقا بالنسبة لمفهوم السيادة.

في هذا الصدد نجد مجموعة من الدراسات التي تناولت الموضوع من زوايا مختلفة، على سبيل المثال نجد مقالا بعنوان: متطلبات تحقيق الأمن السيبيراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، البحث صادر عن مجلة كلية التربية بجامعة المنصورة، العدد 111 جويلية 2020، وقد تطرق البحث في مضمونه إلى مضمون الأمن السيبيراني وعلاقته بحفظ المعلومات الإدارية. ونجد كذلك مقالا بعنوان: النزاع السيبراني والقانون الدولي الإنساني الصادر عن المجلة الدولية للصليب الأحمر، العدد 94 صيف 2021، والذي تطرق فيه الكاتب هربرت لين إلى سلوكات الفاعلين في الفضاء السيبيراني ومدى خضوعهم للقانون الدولي. ونجد كذلك مقالا بعنوان: الأبعاد العسكرية للقوة السيبيرانية في الأمن القومي للدول دراسة حالة إسرائيل، الصادر عن المركز الديمقراطي في برلين عام 2016، ويتطرق إلى دور القوة العسكرية الافتراضية ودورها في حماية الأمن القومي الإسرائيلي. أما دراستنا فتهتم بدراسة دور الفضاء السيبيراني وتأثير ذلك على الأمن القومي، وفي هذا الإطار نطرح الإشكالية التالية: **إلى أي مدى يؤثر الفضاء الافتراضي على الأمن القومي للدولة؟ وما هي انعكاسات ذلك على السيادة؟** ولتحليل هذه الإشكالية نقوم بتحديد عناصر البحث التالية:

المبحث الأول: الإطار المفهومي

المبحث الثاني: مصادر التهديدات السيبرانية.

المبحث الثالث: انعكاسات التهديدات على الأمن القومي.

- خاتمة:

أما الفرضية فتم بناؤها على النحو التالي: كلما اجتهدت الدولة في حماية مجالها الافتراضي، كلما كان ذلك حاسما في حماية أمنها القومي، وحماية سيادتها.

بينما تحتاج الدراسة إلى المنهج الوصفي والمنهج المقارن؛ كونهما من المناهج الأساسية للدراسات الاستكشافية.

المبحث الأول: الإطار المفهومي

يعتبر ضبط المفهوم من أهم المفاتيح التي يجب التحكم فيها في البحث العلمي، ذلك أن تحديد المفهوم يسمح بفحص وتحديد طبيعة الإشكالية المراد تحليلها، ومن ثم سنقوم بتحديد مفهومي الفضاء الافتراضي وكذا الأمن القومي.

تتطرق المراجع العلمية إلى كون عالم الرياضيات "نوربرت وينر" Norbert Wiener أول من استعمل مصطلح "سيبرانية" cybernetic عام 1948، أثناء دراسته لموضوع القيادة والسيطرة والاتصال في عالم الحيوان، وحقل الهندسة الميكانيكية. ويعرف قاموس المصطلحات العسكرية الأمريكية السبرانية بأنها: "أي فعل يستخدم عن طريق الشبكات الإلكترونية لأغراض السيطرة أو تعطيل برامج إلكترونية أخرى".[1] ويعرف الفضاء السيبيراني على أنه: "فضاء مكون من ثلاثة طبقات: الطبقة الأولى تقنية وتكنولوجية ومادية وطبيعية، تمثل البنية التحتية للمواد. والطبقة الثانية تشمل التطبيقات البرمجية. أما الثالثة فهي معرفية"[2]. وعرف قاموس مصطلحات الأمن المعلوماتي الهجوم السبراني بأنه: "هجوم عبر الفضاء الإلكتروني يهدف إلى السيطرة على مواقع إلكترونية أو بنى مؤمنة إلكترونيا بغرض تعطيلها أو تدميرها إلكترونيا"[3]. ومن هذا المنطلق بدأ الاستخدام السياسي والعسكري للسبرانية من خلال مصطلحات الحرب السيبرانية أو الهجمات السبرانية. حيث عرفه المختص في القانون الدولي الإنساني "فيورتس" fuertes: "هجوم عبر الإنترنت للدخول إلى مواقع إلكترونية غير مرخص الدخول إليها، بهدف إتلاف أو تعطيل أو الاستحواذ على البيانات الموجودة فيها، وهي عبارة عن هجمات إلكترونية تقوم بها دولة ضد أخرى"[4]. ويمكن أن يستخدم مفهوم الحرب الإلكترونية كمرادف للحرب السبرانية، ويعرفه "ريتشارك كلارك" Richard A. Clarke و"روبرت كناكي" Robert knake بأنها: "أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها"[5].

أما الأمن القومي فيكمن تحديده من خلال مفهوم الأمن أولا، إذ يعرف الأمن بأنه: "أن تكون سليما من الأذى"[6]. حيث ينطوي هذا المدلول على الطابع الحسي للأمن. ويشاطر هذا الطرح قاموس أكسفورد، حيث يعرف الأمن بأنه: " الحالة التي تشعر من خلالها بالسلامة وعدم الخوف[7]. كما يعرفه "ارنولد ولفرز" Arnold Wolfers بأنه: "الأمن، بالمعنى الموضوعي، يقيس غياب التهديدات إلى القيم الأساسية المكتسبة، أو بمعنى شخصي، غياب الخوف من أن هذه القيم الأساسية يمكن أن يكون موضوعا لهجوم[8]. في حين يعتقد بوزان أن الأمن متعلق أساسا ب: "السعي وراء التحرر من كل تهديد"[9].

يعود الاستخدام الأول للأمن القومي إلى القرن السابع عشر تحديدا في الفترة التي تلي انعقاد مؤتمر وست وفاليا 1648 الذي أسس للخصائص المعاصرة للدولة القومية[10]. ومادام الأمن الواقعي متعلقا أساسا بالدولة فهذا يعني أن بوزان يقترح أن تتحرر الدولة من كل عوامل الخوف والتهديد ومسبباتها. في هذا الإطار يرى بوزان بأن الدولة هي مصدر السلطة العليا وبالتالي هي المعنية بتحقيق الأمن في إطار (مبدأ اخدم نفسك)[11]. تقوم الدولة بمهمة حماية مصالحها وقيمها من تهديدات الدول الأخرى، ويؤكد "كين بوث" Ken Booth أنه: "لا يمكن تحقيق الأمن المستمر إلا إذا امتنعنا من حرمان الآخرين منه، ويتحقق ذلك إذا نظرنا للأمن أنه عملية تحرر[12].

أما الأمن القومي فقد عرفه "والتر ليبمان" Walter Lippmann قائلا: "إن الأمة تبقى في وضع آمن إلى الحد الذي لا تكون فيه عرضة لخطر التضحية بالقيم الأساسية إذا كانت ترغب تفادي الدخول في الحرب، وتبقى قادرة، لو تعرضت للتحدي، على صون هذه القيم عن طريق انتصارها في حرب كهذه[13]، هذا يعني أن ليبمان يقدر أن الأمن القومي للدولة يتعلق أساسا في قدرتها خوض الحرب لضمان حماية مصالحها وقيمها الأساسية. أما باري بوزان يعتبر من أبرز الذين أسسوا لمفهوم أوسع للأمن القومي بحيث يأخذ بعين الاعتبار الجوانب السياسية والاجتماعية والاقتصادية والبيئية. كما عرفت دائرة المعارف البريطانية الأمن القومي بأنه: "حماية الأمة من خطر القهر على يد قوة أجنبية[14] أما "هانز

مورقانثو" Hans Morgenthau فيرى أن الأمن القومي ينصرف إلى: "المساهمة في وحدة الإقليم الوطني ومؤسساته[15].

في الحقيقة انصرفت أعمال الأكاديميين إلى تحديد اتجاهين رئيسين في دراسة الأمن القومي، أما الاتجاه الأول يعتقد بأن الأمن القومي هو عبارة عن قيمة استراتيجية تتعلق أساسا بشؤون الاستقلال والسيادة، ومصالح الدول وقيمها الوطنية، فوفقا لهذا الاتجاه فإن الأمن القومي هو :" تصور إستراتيجي ينبع من متطلبات حماية المصالح الحيوية الأساسية لأي شعب، ويقدم الإجابات النابعة من التصورات المستمدة من التاريخ والجغرافيا لكل المعضلات التي تواجه الوجود الحي لأي أمة من الأمم[16]، بينما يقدر دعاة الاتجاه الثاني أن الأمن القومي ينحصر في المفهوم الواقعي القائم على أساس مركزية الدولة واضطلاعها بمهمة حماية أمنها القومي وفقا لمتطلبات الوضع إن كان يقتضي توظيف القوة العسكرية أو توظيف وسائل أخرى، وفي هذا الإطار يدخل أمن الفرد والجماعة ضمن متطلبات حماية أمن الدولة. وللأمن القومي أبعاد متعددة هي[17]:

-البعد السياسي: حيث يدخل الأمن في سلامة أراضي الدولة وسيادتها ونظامها السياسي وبقاء أركانها. الذي يعتبر من الهداف الحياتية القريبة المدى.

-البعد العسكري: وذلك بتنظيم والحفاظ على الشؤون العسكرية للدولة وحماية كافة أفرع القوات المسلحة من الاختراق، وتنظيمها وتدريبها ورفع الروح المعنوية باستمرار. ما يمكن الجيش من القيام بمهامه الأساسية التي أنشأ من أجلها وهي الدفاع عن حدود البلاد المادية والافتراضية.

البعد الاقتصادي: يعني التمكن من تحقيق مستوى متطور من ضمان الحاجيات الأساسية للشعب، سواء كان ذلك بمجهود السلطة التي تبني إمكانياتها الاقتصادية وقواعدها التكنولوجية وكذا تستغل كل امكاناتها الفلاحية والتصنيعية والخدمات لتطوير الأمن الاقتصادي أو عبر عمليات الاعتماد المتبادل مع مجمعات اقتصادية أخرى.

-البعد الاجتماعي: يهدف إلى حماية الشعور بالانتماء وزيادة الولاء للعيش في مجتمع معين، وكذا حماية المجتمع من أشكال الاغتراب والاستيلاب الاجتماعي وتعزيز الشعور الوطني، ومنه البحث عن مجتمع متماسك وبعيد عن أشكال التردي والجريمة.

-البعد الثقافي: أي القدرة على تأمين الأنساق الفكرية والعمل على عدم اختراق الكيان الثقافي من القيم والعادات الدخيلة.

-البعد البيئي: والذي يعني حماية الجغرافيا من مخاطر التلوث التي يمكن أن تحدث تهديدا خطيرا على الإيكولوجيا وكذا الحفاظ على بعض الموارد الطبيعية.

ووفقا للاتجاه الثاني نجد العديد من التهديدات للأمن القومي منها مصادر التهديد السيبيرانية.

المبحث الثاني: مصادر التهديدات السيبيرانية.

يمكن أن يدخل في التهديدات السيبرانية العديد من أشكال التهديد يمكن حصرها على النحو التالي:

أ/ شبكة الإنترنت كمصدر للتهديد:

يعتبر الكمبيوتر والإنترنت أحد أهم مصادر التهديد التي يوفرها الفضاء الافتراضي، وذلك لقدراتها الإنسيابية في اختراق الحدود وبدون أي مقاومة لدى الدول الضعيفة. حيث يمكن للدول المتحكمة في برامج المعلوماتية ذات التقنية العالية اختراق شبكات الويب بشكل يسمح بالاطلاع على أسرار المؤسسات والدوائر السيادية في الدولة المراد اختراقها، ويمكن كذلك تعطيلها، ما يجعل الدولة المستهدفة في حرج تقني وفي فراغ أمني[18]. ومن ثم أصبح موضوع تأمين الشبكات العنكبوتية أمرا غاية في الأهمية؛ من أجل حماية مؤسسات وسيادة الدولة. حيث أضحى ممكنا جدا إرسال فيروسات تقوم بتحطيم الشبكة الأمنية لدولة معينة؛ ليسهل بذلك احتلالها أو الحصول على معلومات سرية وسيادية منها. من أجل

ISSN: 1112-4938, EISSN: 2600-6456

الهجوم على بعض الدول وابتزازها وتدمير مؤسساتها يتم تطوير عدة برامج خبيثة وفيروسات، يتم إرسالها عن طريق الإنترنت وشبكات الكمبيوتر، ويمكن تحديدها: بالفيروسات، والديدان، والخدع والكلام الكاذب، والأحصنة الطروادية، ورسائل الاصطياد الخادعة، وبرامج التجسس، وبرامج الإعلانات، وصفحات فقاعية أو انبثاقيه، وبرنامج تسجيل نقرات لوحة المفاتيح. حيث يتم إرسال هذه البرامج الخبيثة عن طريق وسائط التخزين وكذا البريد الإلكتروني، أو تحميل برامج من الإنترنت أو الدخول إلى المواقع غير الآمنة[19] ويساعد على نجاح كل هذا وجود مؤسسات دولية و قراصنة جيدون يؤدون المهمة بكفاءة عالية[20].

ب/ الوسائل التكنولوجية كمصدر للتهديد:

في الحقيقة يمكن اعتبار وسائط الاتصال الحديثة أجهزة بارعة في نقل المعلومات إلى الخارج فبفضل التقنية الرقمية والذكاء الإلكتروني ومختلف التطبيقات أصبح بإمكان القوى الخارجية معرفة معطيات دقيقة عن الدول والمؤسسات والأفراد المراد التجسس عليهم، في هذا الإطار نجد العديد من الأجهزة الإلكترونية التي أضحت ذات استعمال يومي لدى فئات واسعة من الشعب، يمكن أن تكون مصدرا لتهديد أمن الفرد والمجتمع والدولة معا. فالوسائل الإلكترونية الذكية كالهواتف وشاشات التلفزيون وساعات اليد كلها تحمل تطبيقات يمكن أن تساهم في تحديد الموقع، وكذا كاميرات يمكن أن تفتح بشكل غير ظاهر داخل البيوت للاطلاع على الحياة الخاصة للأفراد من غير علمهم. كما يمكن أن تلعب الهواتف الذكية أدوارا مهمة بحكم قدرتها على تصوير مختلف المواقع التي تتواجد أو تنعدم فيها التغطية والتي يمكن أن تساهم في مد الأطراف المعادية بمعلومات سرية عن مواقع حساسة يمكن أن تهدد سلامة الأمن القومي للدولة، وهذا ما يطلق عليه بالقرصنة الإلكترونية[21] القائمة على التدمير الإلكتروني والتجسس والاختراق للمواقع الحكومية وغير الحكومية، والتحكم في تغيير بعض قواعد البيانات.

تقوم الدول بالتجسس كآلية لاختراق أنظمة معادية سواء بزرع جواسيس أو عن طريق توظيف الفضاء الافتراضي، الذي يسمح من خلال استعمال الشبكات والأجهزة الإلكترونية إلى تحقيق نتائج مثمرة تسمح بالحصول على معلومات تؤدي حتما إلى السيطرة السيبرانية. ومنه، فإن التجسس هو القدرة على الدخول غير المشروع على شبكات الخصم دون أن يصاحب ذلك تخريب أو تدمير للبيانات أو المعلومات التي قد تشمل خططا عسكرية هجومية أو دفاعية أو أسرارا حربية، أو معلومات سياسية أو استخباراتية ومعرفة دور شبكات الحاسب الآلي[22]. وللتجسس أنواع[23]:

1-التجسس العسكري: حيث تعمد الجيوش العالمية إلى توظيف شبكات الهاتف والاتصالات واختراق المكالمات عن طريق التنصت وكسر شيفرة البرقيات اللاسلكية والرسائل السلكية الحساسة، وتعتبر الحرب العالمية الأولى منطلقا لهذا الفعل حين أقدمت بريطانيا على الولوج إلى شبكات الاتصال الألمانية وأمكنها من فك شفرة ما يعرف ببرقية زيرمان — هي برقية دبلوماسية من الإمبراطورية الألمانية إلى المكسيك، أرسلت عام 1917 فيها اقتراح لشن الحرب على الولايات المتحدة حيث اعترضتها المخابرات البريطانية، وفكّت شفرتها، وهي السبب الرئيس في دخول الولايات المتحدة الأمريكية الحرب العالمية الأولى.

2-التجسس الصناعي والتجاري: كالتجسس على الشركات والمؤسسات ذات الطابق التكنولوجي والاقتصادي ومعرفة أسرارها وطرق إدارتها وخططها الاستراتيجية.

إن التجسس يؤرق بشدة دور الحكومات، ويزيد من دورها في تأمين مصادر المعلومات، أي تحقيق الأمن المعلوماتي الذي يمكن اعتباره هو تلك الرؤى والسياسات والإجراءات التي تصمم وتنفذ على مستويات مختلفة، فردية، مؤسسية ومجتمعية وتستهدف تحقيق عناصر الحماية والصيانة المختلفة التي تضمن أن تحقق للمعلومات السرية أو الموثقة أن لا تكتشف ولا تخترق من قبل أشخاص غير مخول لهم ذلك[24]، و يمكن كذلك من خلال التجسس القيام بعمليات تخريبية كتعطيل الخدمات وإتلاف المعلومات وأصولها ومختلف قواعد

ISSN: 1112-4938, EISSN: 2600-6456

البيانات[25]. وهناك من يصنف التهديدات الإلكترونية على النحو التالي:

1-القرصنة والتخريب الإلكتروني: حيث يتم هذا العمل عن طريق القيام بتعديل أو تخريب أو إلغاء المحتوى كقرصنة المواقع الإلكترونية أو بتعطيل الحواسيب.

2-الجريمة والتجسس الإلكتروني: غالبا ما يستهدفان الشركات والمؤسسات العمومية والهيئات الحكومية.

3-الإرهاب الإلكتروني: ويستخدم هذا المصطلح لوصف الهجمات التي تقوم بها فواعل غير حكومية ضد الأجهزة والشبكات والمعلومات ما يؤدي إلى ضرر مادي وخراب في الممتلكات العامة والخاصة.

4-الحرب الإلكترونية: حيث تهدف إلى التأثير على الإرادة السياسية لصانع القرار في المجال الإلكتروني أو على مستوى العمل العسكري أو المدني.[26]

المبحث الثالث: انعكاسات التهديدات السيبرانية على الأمن القومي:

يمكن استخدام الفضاء الافتراضي كمنطلق للتهديدات الإلكترونية من أطراف داخل الدولة أو خارجها. فالصراعات الطائفية والمجتمعية والحرب النفسية التي تشن على جماعة معينة تجد الكثير ممن يحركها من خلال الوسائط الإلكترونية، وهو ما يسهل عادة الاختراق الخارجي، ويجعل من ضعف القوة السيبرانية وانكشاف الأمن القومي أمرا ممكن الحدوث.

أظهر التطور الحاصل في التحكم، والسيطرة على الحواسيب والأجهزة الإلكترونية إلى بروز مصطلح جديد يطلق عليه القوة الإلكترونية. وتتضح خطورة القوة الإلكترونية من خلال التأثير في مستويات الأمن لدى الوحدات الدولية، وهو ما جعل معضلة التحكم في الفضاء الافتراضي تدخل في صلب القضايا الاستراتيجية للأمن القومي؛ من أجل الاستحواذ على مصادر القوة داخل الفضاء الإلكتروني، ومنه صار الفضاء الافتراضي

يدخل ضمن محددات القوة وأبعادها من حيث طبيعتها وأنماط استخدامها وحتى طبيعة الفاعلين[27]

يعتبر جوزيف ناي القوة الإلكترونية مفهوما مركزيا يدل على قدرة الشبكات الافتراضية على لعب دور مؤثر في التحكم في إرادات الوحدات الدولية، إذ يقدر أنها عبارة عن نظام متماسك ناتج من التناغم بين الوسائل التكنولوجية، والسكان، والاقتصاد، والصناعة، والقدرات العسكرية، ومختلف موارد الدولة، ومدى قدرة هذا المركب المتجانس من الاختراق والسيطرة على قدرات الآخرين، والتحكم في إراداتهم من خلال المجال الإلكتروني[28]. وحسب جوزيف ناي فإن فهناك ثلاثة أنواع من الفاعلين الذين يمتلكون القوة السيبيرانية، وهم[29]:

1-الدولة: حيث تمتلك القدرة على تنفيذ هجمات إلكترونية على غيرها.

2-الفاعلون من غير الدول: هي لا تمتلك نفس إمكانية الدول، ولكنها تمتلك الأسس التنظيمية التي تتمتع بها، وتسمح لها بالقيام بعمليات مؤثرة تجاه البنية الإلكترونية للدولة ذات السيادة.

3-الأفراد: حيث يمتلكون المعرفة التكنولوجية والقدرة على توظيفها رغم الصعوبة البالغة في ملاحقتهم والكشف عن هويتهم.

وبما أن المفهوم الكلاسيكي للقوة يعني قدرة الفاعل (أ) على التأثير على سلوكيات الفاعل (ب) ودفعه للقيام بأعمال معينة، فإن تحولات القوة تقتضي دخول الفضاء الافتراضي إلى التأثير بعمق في سيادة الدول، وبفواعل غير سيادية في غالب الأحيان[30]. وبهذا باتت القوة السيبرانية دعامة مهمة لمضمون القوة الناعمة بالنسبة للدولة القومية حيث أضحى الفضاء الإلكتروني مسرحا لشنّ هجمات تخريبية ترتبط بنشر المعلومات المضللة، والحرب النفسية، والتأثير في توجهات الرأي العام، والنشاط السري والاستخباراتي. كما ازداد الإنفاق لحماية الحدود الافتراضية، وحماية شبكاتها الإلكترونية من خطر التهديدات، وتحول العمل من بناء شبكات إلكترونية ذات طابع دفاعي إلى بناء تطوير

بنى وهياكل إلكترونية من أجل شن هجمات على أطراف معادية[31].

وحماية الأمن القومي من التهديدات السيبرانية تقوم الدول الكبرى ببناء استراتيجيات مركبة لحماية فعالة لأمنها القومي. حيث قامت العديد من الدول على تشكيل وحدات للحرب الإلكترونية ضمن الأفرع الرئيسية للقوات المسلحة، ومنها الولايات المتحدة التي قامت بتشكيل قيادة عسكرية للفضاء الإلكتروني، وخصصت ميزانية ضخمة لمواجهة التهديدات الإلكترونية، وعملت على تطوير أسلحة إلكترونية، منها: فيروسات قادرة على تخريب البنية الإلكترونية للعدو[32]، وبهذا تعرف القيادة الاستراتيجية الأمريكية الهجمات السيبرانية بأنها: "تطويع عمليات نظام الكمبيوتر بهدف منع الخصوم من الاستخدام الفعال لها، فضلا عن التسلل إلى أنظمة المعلومات وشبكات الاتصال بهدف جمع وحيازة وتحليل البيانات التي تحتويها"[33]. ولفعالية أكبر تركز الولايات المتحدة على ما يلي[34]:

-الخبرة النفسية والتسويقية في تطبيق مبادئ النفوذ.

-الخبرة في المجالات الجغرافية والثقافية واللغوية وغيرها حيث سيتم تطبيق المبادئ.

-الخبرة الفنية والإدارية في استخدام القدرات والتكتيكات السيبرانية.

وجاء في استراتيجية الأمن القومي للولايات المتحدة عام 2017 ما يلي: "تنظر العديد من البلدان الآن إلى القدرات السيبرانية كأدوات لإسقاط النفوذ، ويستخدم البعض الأدوات السيبرانية لحماية وتوسيع أنظمتها الاستبدادية. أصبحت الهجمات الإلكترونية سمة رئيسية للصراع الحديث. ستقوم الولايات المتحدة بالردع والدفاع، وعند الضرورة، هزيمة الجهات الخبيثة التي تستخدم قدرات الفضاء الإلكتروني ضد الولايات المتحدة. عندما تأتي الفرصة لاتخاذ إجراءات ضد الجهات الخبيثة في الفضاء الإلكتروني، فإن الولايات المتحدة سوف تكون على علم بالمخاطر، ولكن لن تتجنب المخاطرة، عند النظر في خياراتنا"[35].

كما أسست مجموعة من الدول وحدات للدفاع الإلكتروني على غرار ما قامت به روسيا

والصين وبريطانيا واليابان، وإيران التي أسست مقرا للدفاع الإلكتروني في اكتوبر 2011 وأضحت من الدول التي تمتلك منظومة دفاع إلكتروني متطورة لمواجهة التهديدات وحماية منظومة الأمن القومي خاصة البرنامج النووي. وأسست ألمانيا جيشا إلكترونيا الذي سيعمل جنبا إلى جنب مع باقي أفرع القوات المسلحة الجوية والبحرية والبرية، وستكون مهمة جنود الجيش الإلكتروني الألماني حماية الشبكات الإلكترونية وأنظمة الأسلحة التابعة للجيش الألماني، وستكون قادرة أيضا على شنّ هجمات[36] وسيبلغ قوام هذا الجيش الإلكتروني نحو 13 ألف جندي وموظف مدني، وسيصبح هذا السلاح الجديد في الجيش الألماني بكامل طاقته اعتبارا من عام 2021. وعين الجنرال لودفيغ لاينهوز كأول مشرف على السلاح الإلكتروني، حيث يعتبر خبيرا في الحرب الإلكترونية.

ويمكن أن تلجأ أقطاب دولية أخرى إلى ما يسمى بالتحالفات السيبرانية، حيث يشير هذا المفهوم إلى: "النمط الرسمي النابع عن الاتفاق الصريح بين الجهات الفاعلة الدولية، والذي ينتج عنه التزامات متبادلة لتدعيم موقف الأطراف في المجال السيبراني"[37].

تنبري الدول في حماية حدودها الإلكترونية وأمنها المعلوماتي إلى القيام بعدة خطوات، منها تأمين العنصر البشري من خلال عمليات التحري عن الأفراد العاملين، ومدى إخلاصهم وولائهم للمؤسسات والدول التي يشتغلون بها، وعدم إغرائهم من طرف جهات خارجية، مهما كانت طبيعتها أو حجمها. كما يمكن إبرام تشريعات قانونية مع الدول، خاصة التي تمتلك وزنا في مجال النشاط الإلكتروني، سواء أكان ذلك بطريقة ثنائية أو متعددة الأطراف؛ من أجل منع الاعتداء أو تبادل الخبرات والحماية المتبادلة[38]، وأما على الصعيد التكنولوجي يمكن أن يكون للتحالف السيبراني الأنماط التالية:

1-الأحلاف التقليدية: حيث يعد نموذج حلف الناتو الأبرز، لقد تم تشكيل وحدة الدفاع الإلكتروني بعد الفشل في حماية الهجوم على إستونيا وجورجيا، ومن ثم تمّ تطوير مفهوم إستراتيجي جديد للحلف، وذلك من خلال تطوير القدرات الدفاعية الإلكترونية بما يشمل مساندة الحلفاء الذين يتعرضون لهجمات إلكترونية، وأن أية هجمات إلكترونية

على دولة معينة تعني أن الهجوم وقع على جميع الأعضاء[39].

2-التحالف بين الدولة وشركات داخلية: ومثال ذلك التحالف القائم بين وزارتي الدفاع والأمن الداخلي في الولايات المتحدة مع شركات صناعية خاصة لبناء شراكة تحقق الأمن السيبراني.

3-التحالف بين شركات تكنولوجية خاصة: بحيث يقوم هذا النمط على توحيد الجهود بين شركات خاصة من أجل بناء شراكة إلكترونية؛ من أجل الدفاع الإلكتروني كما حصل في بلجيكيا بين القطاعات الأكاديمية والمؤسسات الخاصة. أو التحالف في أمريكا بين شركات مكافي ومايكروسوفت وسيمانتك.

4-التحالف بين منظمات دولية وشركات التكنولوجيا: مثلا ما هو حاصل بين منظمة حلف الناتو وأعضاء آخرين من غير الدولة القومية، وفي مناطق خارج حدود الحلف كمنطقة الشرق الأوسط[40].

ساهم ظهور مفهوم الحكومة الإلكترونية في إضفاء الجانب الافتراضي على الحياة السياسية، حيث أضحت أنشطة الدولة الرسمية وغير الرسمية تدار بطريقة إلكترونية. حيت تساعد تكنولوجيا الإعلام والاتصال على تسهيل تبادل المعلومات وتوصيل القرارات والأوامر، والحصول على النتائج بطريقة أسرع. وأحد أهم المجالات التي تأثرت بدور المجال الافتراضي في العمل الحكومي نجد الدبلوماسية، والتي تعنى بطرق وآليات وعمليات التفاوض والاتصال والتمثيل، حيث برز مصطلح الدبلوماسية السيبرانية الذي يدل على القيام بالوظيفة الدبلوماسية إلكترونيا وعن بعد.

تعرف الدبلوماسية السيبرانية بأنها: "وسيلة تحقيق أهداف الدبلوماسية العامة عن طريق استخدام أنظمة الاتصال الحديثة...وما تتضمنه من مواقع التواصل الاجتماعي، ومواقع الإنترنت، وذلك بواسطة التفاعل بين المواطنين والمسؤولين..."[41]. حيث كانت الولايات المتحدة من المبادرين للاهتمام بهذا المجال، وأسست لذلك مكتب (E-

Diplomacy) التابع لوزارة الخارجية عام 2003 ومكتب إدارة المعلومات الذي تتمثل مهمته أساسا في مساعدة الدبلوماسيين على التواصل الإلكتروني، وكذا المساعدة على تنفيذ السياسة الخارجية الأمريكية، كما قامت المملكة المتحدة في نوفمبر 2009 بإنشاء مكتب الشؤون الخارجية والكومنولث من خلال إنشاء "مجموعة الدبلوماسية الرقمية" وتمثلت مهمتها في تحفيز استخدام تقنيات الإعلام الجديدة في الدبلوماسية[42].

خاتمة:

تنبري حماية الأمن بالنسبة للدولة القومية إلى الحفاظ على السيادة في المجتمع الدولي، حيث أضحى مفهوم السيادة الذي أقره بودان في تآكل مستمر في ظل الاستعمال المتزايد للفضاء الإلكتروني في إدارة الشؤون الدولية سواء ذات الطابع الهجومي أو الدفاعي في ميدان السلم أو الحرب.

السيادة المطلقة لم تعد تجد لها مكانا في ظل عولمة وسائل الاتصال، وانتشار المعلومات، وصعوبة التحكم في تدفقها بعد توصيلها بشبكة الإنترنت، وتوسيع توظيف المجال الإلكتروني، وتحولت المفاهيم من إشكالية ضبط الحدود الجغرافية وتحضير ترسانات عسكرية لذلك، إلى إشكالية ضبط الحدود الافتراضية وتحضير ترسانات قانونية وإلكترونية لذلك. ومع إنشاء فروع في القوات المسلحة مهمتها التحكم والسيطرة والدفاع الإلكتروني أصبح الحديث عن الهجوم والحرب الإلكترونية أمرا واقعا وملموسا، ومن نافلة القول أن الدول التي لا تمتلك دفاعات وتحصينات إلكترونية هي حتما دول مستباحة افتراضيا، ومحل تدخل سيبراني من دول أكثر تحكما وسيطرة في هذا المجال. حيث يتطور هذا المجال باستمرار، وتعاني منه حتى الدول المتقدمة تكنولوجيا، وما حدث من تدخل روسي في أوكرانيا عام 2008، وكذا ما قيل عن اختراق روسيا للانتخابات الرئاسية الأمريكية عام 2016، وكذا الاختراق الإماراتي لوكالة الأنباء القطرية عام 2017، وما نتج عنه من حصار خليجي لقطر، كل هذا يؤكد أن الحروب والتدخلات الإلكترونية هي تهديد حقيقي للأمن القومي، ولا تقل خطورتها عن التدخل العسكري التقليدي.

بهذا يمكن القول أن الفضاء الافتراضي أدى إلى مزيد من تسهيل الحياة ومساعدة السلطة في إدارة الحياة العامة من خلال تعميق آليات الحكومة الإلكترونية، إلا أن ذات الفضاء أدى إلى تقليص دور الحدود السيادية، وزاد من التغلغل والنفوذ الجيوسياسي للوحدات الدولية عن طريق عمليات تدمير البنية التحتية الإلكترونية للدولة والتدخل في عمليات صنع القرار. ومنه، فإن أي توسيع في العمل الإلكتروني للدولة يصاحبه تقلص في الحدود السيادية إن لم يكن للدولة القومية أي استعدادات ودفاعات عن حدودها الافتراضية.

الهوامش:

1- "الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر،" أحمد عبيس الفتلاوي، مجلة المحقق الحلي للعلوم القانونية والسياسية،4، (2016)، جامعة بابل، ص.ص، 610 . 688.

2- حرب وإستراتيجية نهوج ومفاهيم، هنروتين جوزيف، وأوليفييه شميت، وتايات ستيفان،(2019)، ترجمة: أيمن منير، الكويت: عالم المعرفة المجلس الوطني للثقافة والفنون والآداب، ص.71.

3- "الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر،" أحمد عبيس الفتلاوي، ص.ص، 610. 688.

4- "الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر،" أحمد عبيس الفتلاوي، ص.ص، 610. 688.

5 علي حسن باكير، "المجال الخامس.. الحروب الإلكترونية في القرن الـ21،" (مركز الجزيرة للدراسات)، متاح على الرابط التالي:

https://studies.aljazeera.net/ar/issues/2010/20117212274346868.html

تم الاطلاع عليه في 2016/07/07

6- المفاهيم الأساسية في العلاقات الدولية، مارتين غريتيفيتش وتيري أوكلاهان (2002) ط.1. دبي: مركز الخليج للأبحاث، ص.78.

7-Oxford word power dictionary. P. 641.

8-**Théories des relations internationale**, Dario Battistella, (2009) paris : presses de sciences po ,3ed, p. 508.

9-**Théories des relations internationale**, Dario Battistella, p. 508.

10- "الأمن القومي والأمن الإنساني دراسة في المفاهيم،" عادل عبد الحمزة ثجيل، مجلة العلوم السياسية. مركز الدراسات الإستراتيجية والدولية جامعة بغداد. (2016) العدد 51، ص.ص، 325. 375 .

11- "معضلة الأمن اليمني الخليجي دراسة في المسبّبات والانعكاسات والمآلات، "أحمد محمد أبو وزيد. المستقبل العربي. بيروت: مركز دراسات الوحدة العربية. 414 (أوت 2013)، ص.ص، 71. 93 .

12- "مفهوم الأمن: مستوياته وصيغه وتهديداته (دراسة نظرية في المفاهيم والأطر)،" سليمان عبد الله الحربي، المجلة العربية للعلوم السياسية، ع. 19 (صيف 2008)، ص. ص، 9. 30.

13-- "مفهوم الأمن: مستوياته وصيغه وتهديداته (دراسة نظرية في المفاهيم والأطر)،" سليمان عبد الله الحربي، ص.ص، 9. 30.

14- "الأمن القومي والأمن الإنساني دراسة في المفاهيم"، عادل عبد الحمزة ثجيل، ص.ص، 325. 375.

15- "الأمن القومي والأمن الإنساني دراسة في المفاهيم"، عادل عبد الحمزة ثجيل، ص.ص، 325. 375.

16- مفهوم الأمن: مستوياته وصيغه وتهديداته (دراسة نظرية في المفاهيم والأطر)،" سليمان عبد الله الحربي، ص.ص، 9. 30.

17- "الأمن القومي والأمن الإنساني دراسة في المفاهيم"، عادل عبد الحمزة ثجيل، ص.ص، 325. 375.

18- "أمن الشبكات والإنترنت"، منى الأشقر جبور وعزيز ملحم بربر، حلقة علمية الإنترنت والإرهاب جامعة عين شمس بالتعاون مع جامعة نايف العربية للعلوم الأمنية القاهرة، ص.3.

19- أمن المعلومات بلغة ميسرة، خالد بن سليمان غثبر ومحمد عبد الله القحطاني، ط.1. الرياض: مكتبة الملك فهد الوطنية، ص. 58.

20- "cyber threats to national security. Anca DINICU, Specific features and actors involved," (buletin ştinţific), Nr. 2 (38) 2014, p.p. 109. 113.

21- القرصنة الإلكترونية أسلحة الحرب الحديثة، بشرى حسين الحمداني، ط.1. عمان: دار أسامة للنشر والتوزيع، ص.12.

22- "الأمن السيبيرني، هل يمكن أن تتجنب الدول مخاطر الهجمات الإلكترونية؟" محمد المختار، مفاهيم المستقبل، ملحق شهري يصدر مع دورية اتجاهات الأحداث، 6، 2015، ص.ص،5. 7.

23- جرائم نظم المعلومات، حسن طاهر داوود. ط.1. الرياض: أكاديمية نايف للعلوم الأمنية، ص.59.

24- "الأمن المعلوماتي والجرائم الإلكترونية أدوات جديدة للصراع"، جمال محمد غيطاس مركز الجزيرة للدراسات، متاح على الرابط الإلكتروني التالي:

https://studies.aljazeera.net/ar/issues/2012/02/2012229132228652960.html

تم الاطلاع عليه في 07/07/ 2020

25- "الأمن السيبيراني، هل يمكن أن تتجنب الدول مخاطر الهجمات الإلكترونية؟" محمد المختار، ص.ص،5. 7.

26- علي حسن باكير، "المجال الخامس.. الحروب الإلكترونية في القرن الـ21"، (مركز الجزيرة للدراسات)، متاح على الرابط التالي:

https://studies.aljazeera.net/ar/issues/2010/20117212274346868.html

تم الاطلاع عليه في 2016/07/07

27- "القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الالكتروني، (المركز العربي

لأبحاث الفضاء الإلكتروني)، عادل عبد الصادق. متاح على الرابط التالي:
https://drive.google.com/file/d/0B7Xzn6q9WBfsYkVMZXhOSnZ0NFU/view
تم الاطلاع عليه في 2020/02/05.

28- "القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الالكتروني، (المركز العربي لأبحاث الفضاء الإلكتروني)، عادل عبد الصادق. متاح على الموقع التالي:
https://drive.google.com/file/d/0B7Xzn6q9WBfsYkVMZXhOSnZ0NFU/view
تم الاطلاع عليه في 2020/02/05.

29- "القوة السيبرانية نمط جديد لممارسة التأثيرات غير التقليدية في العلاقات الدولية"، إيهاب خليفة، اتجاهات الاحداث 6، (جانفي 2016) ملحق مفاهيم المستقبل. مركز المستقبل للأبحاث والدراسات المتقدمة. ص.ص.2. 4.

30- "القوة السيبرانية نمط جديد لممارسة التأثيرات غير التقليدية في العلاقات الدولية"، إيهاب خليفة، ص.ص.2. 4.

31- "أنماط الحرب السيبرانية وتداعياتها علي الأمن العالمي"، عادل عبد الصادق، متاح على الرابط التالي:
: http://alimbaratur.com/?p=2850
تم الاطلاع عليه في 13 /06/ 2020.

33-"الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر،" أحمد عبيس الفتلاوي، ص.ص، 610. 688.

34-Franklin D. Kramer and Larry Wentz, "Cyber Influence and International Security" (Center for Technology and National Security Policy National Defense University) available in: https://ndupress.ndu.edu/Portals/68/Documents/defensehorizon/DH-061.pdf?ver=2016-11-15-092816-993 site visited on 03/25th/2020.

35 -*U.S. national Security strategy, 2017, available in:* https://www.government.se/4aa5de/contentassets/0e04164d7eed462aa511ab03c890372e/national-security-strategy.pdf site visited on 12/12th/2020.

36- " ألمانيا تطلق جيشها الإلكتروني وتحدد مهامه بدقة"(2017). متاح على الرابط

ISSN: 1112-4938, EISSN: 2600-6456

الإلكتروني التالي:
https://www.dw.com/ar/%D8%A3%D9%84%D9%85%D8%A7%D9%86%D9%8A%D8%A7-%D8%AA%D8%B7%D9%84%D9%82-%D8%AC%D9%8A%D8%B4%D9%87%D8%A7-%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A-%D9%88%D8%AA%D8%AD%D8%AF%D8%AF-%D9%85%D9%87%D8%A7%D9%85%D9%87-%D8%A8%D8%AF%D9%82%D8%A9/a-38314944

تاريخ التصفح 18/ 02/ 2021.

37- التحالفات السيبرانية طريق محتمل لمواجهة تهديدات الفضاء الإلكتروني"، دعاء الجهيني، اتجاهات الأحداث 6، (جانفي 2016) ملحق مفاهيم المستقبل. مركز المستقبل للأبحاث والدراسات المتقدمة. ص.ص،11. 13.

38- "الأمن المعلوماتي للحكومة الإلكترونية وإرهاب القرصنة"، فتيحة ليتيم ونادية ليتيم، مجلة المفكر، العدد 12 (مارس 2015) كلية الحقوق والعلوم السياسية جامعة محمد خيضر بسكرة. ص.ص، 237. 253 .

39- "القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني، عادل عبد الصدق (المركز العربي لأبحاث الفضاء الإلكتروني)، متاح على الموقع التالي:
https://drive.google.com/file/d/0B7Xzn6q9WBfsYkVMZXhOSnZ0NFU/view
تاريخ التصفح: 20/01/2021

40- التحالفات السيبرانية طريق محتمل لمواجهة تهديدات الفضاء الإلكتروني"، دعاء الجهيني، ص.ص،11. 13

41- الدبلوماسية السيبرانية بعد غير تقليدي في العلاقات غير الرسمية بين الدول، سارة يحي، اتجاهات الأحداث 6، (جانفي 2016) ملحق مفاهيم المستقبل. مركز المستقبل للأبحاث والدراسات المتقدمة. ص.ص،8. 10

42- الدبلوماسية السيبرانية بعد غير تقليدي في العلاقات غير الرسمية بين الدول، سارة يحي، ص.ص،8. 10