انعكاسات البعد العسكري للفضاء السيبراني على الجغرافيا السياسية للدولة

الدكتور سالم صابر

كلية العلوم السياسية والعلاقات الدولية،

جامعة الجزائر 3

الملخص

في أعقاب التطور التقني الذي جسده الاتصال بالإنترنت، في منتصف التسعينيات، وصف الأكاديميون والمفكرون الظاهرة بأنها إشارة رسمية لإلغاء الفضاء الجغرافي. في الوقت الحاضر يمكننا أن نؤكد أن ظهور الإنترنت كان بمثابة سيف ذو حدين في تطور طبيعة العلاقات الدولية، من خلال كونها قوة دافعة لمزيد من التكامل الاقتصادي العالمي والعولمة والتقدم الحديث، وأيضًا مصدر عدم يقين يفرز تهديدات أمنية جديدة ومعضلة تواجهها الدول التي تخلق ساحة معركة دولية فوضوية ، بدون هيئة حاكمة أو قوة شرطة.

الكلمات المفتاحية : الفضاء السيبراني، الأمن السيبراني، الهجمات السيبرانية، الردع السيبراني، البعد العسكري للفضاء السيبراني، الجغرافيا السياسية، السيادة، القوة، الإنترنت، العالم الافتراضي، البيانات والمعلومات، الذكاء الاصطناعي، تكنولوجيا المعلومات، التحولات الجيوسياسية.

Abstract

In the wake of the technical development embodied by the internet outreach, in the mid-nineties, scholars and thinkers, described the phenomenon as the formal signal introducing the abolishment of geography and space, In nowadays, we can affirm that the advent of the internet played a double-edged sword in the evolution of the nature of international relations, by being a driving force of a greater worldwide economic integration, globalization and modern progress, and also a source of uncertainty creating a new security threats and dilemma faced by the nations creating an anarchic international battlefield, with no governing body or police force.

Keywords: cyberspace, cyber security, cyber attacks, cyber deterrence, the military dimension of cyberspace, geopolitics, sovereignty, power, the Internet, virtual world, data and information, artificial intelligence, information technology, geopolitical shifts.

المقدمة

مع تطور مجال التقنيات وتزايد اعتماد الدول على الاتصالات والشبكات الإلكترونية في إدارة وتوجيه مختلف البنى والمفاصل الحيوية لمؤسسات الدولة، المدنية منها والعسكرية، بدأ في الظهور بشكل متزايد خطر جديد، تمثل في إمكانية لجوء بعض الفواعل إلى إلحاق الضرر والأذى بل وحتى تخريب الدول عن طريق الفضاء السيبراني، الذي أصبح يمثل مصدرا رئيسيا للمخاطر التي تهدد الدول، بعد أن تطورت استخداماته لتشمل المجال العسكري، ما جعله أكبر تأثيرًا على أمنها وسلامة أراضيها، في ظل عدم وجود اتفاق واضح بين الفضاء السيبراني واستخداماته المشروعة، أضف إلى ذلك إلى ذلك أن تزايد حدة الصراعات الجيوسياسية، بسبب انتشار التجسس الإلكتروني والجريمة السيبرانية، ساعد على خلق بيئة دولية مضطربة وغير مستقرة، تطلبت تغييرا في تحديد أدوات قوة الدولة، لتصبح أكثر فعالية في مواجهة التهديدات الجديدة من حروب الجيلين الرابع والخامس، والتي أصبحت تؤثر في الجغرافيا السياسية للدولة، بتحديد عوامل قوتها وسلوكها السياسي ضمن بيئة تفاعلية، تنعكس على مقوماتها وأوضاعها الداخلية وعلاقاتها الخارجية. وعليه، سنحاول في هذا المقال طرح والإجابة على الإشكالية التالية:

إلى أي مدى ينعكس البعد العسكري للفضاء السيبراني على الجغرافيا السياسية للدولة؟

المحور الأول: مدخل مفاهيمي

أولا: الفضاء السيبراني

أفرز التطور المتسارع لتكنولوجيا المعلومات والاتصالات وتقنيات الذكاء الاصطناعي تحولا كبيرا في مفاهيم: الأمن - القوة - السيادة، تبعه دخول العالم في مرحلة جديدة يلعب فيها الفضاء السيبراني دورا محوريا في بناء القدرات العسكرية للدولة، بحيث أصبح أمنها مرتبط بمدى قدرتها وتحكمها في الفضاء السيبراني، باعتباره مجال افتراضي من صنع الانسان، يرتكز على الكمبيوتر والإلكترونيات وشبكات الإنترنت وكَم هائل من البيانات والمعلومات والأجهزة، بوصفه الذراع الرابع للجيوش الحديثة، والبعد الخامس للحرب[1]، معبرا بذلك عن العلاقة بين مركب الإنترنت من جهة والجغرافيا – السياسة – الاقتصاد - المجتمع، من جهة أخرى.

ثانيا: الأمن السيبراني

تم التطرق إلى مفهوم الأمن السيبراني بمنظورات مختلفة ومتعددة، تهدف في مجملها إلى التأكيد على: «مجموعة الآليات والإجراءات المتبعة، التي تشمل وضع وتنفيذ التدابير المضادة المطلوبة في مجال الدفاع ضد الهجمات السيبرانية ومخرجاتها».

في هذا السياق، يعرفه «إدوارد أمورس» (Amorso Edward) بأنه: «وسائل وآليات من شأنها الحد من خطر الهجوم على البرمجيات - أجهزة الحاسوب – شبكة المعلومات، أي تلك

الميكانيزمات المستخدمة في مواجهة القرصنة وكشف الفيروسات والتصدي لها، وتوفير الاتصالات المشفرة والآمنة»[2].

وعليه، فالأمن السيبراني هو: جملة العمليات والمهام الوقائية والتوجيهية المخصصة لحماية الأفراد والأنظمة والحفاظ على سلامة البنى التحتية للدولة، وتجنب تعرضها للهجمات والاختراقات مهما كان نوعها – توقيتها ومصدرها.

ثالثا: الردع السيبراني

يعرف الردع السيبراني على أنه «منع الأعمال الضارة ضد الأصول الوطنية في الفضاء السيبراني والأصول التي تدعم العمليات الفضائية»[3]، أي توفير الحماية التأمينية اللازمة لأمن المعلومات .

يقوم الردع السيبراني على ثلاث ركائز، تعتبر أساس الاستراتيجيات الدفاعية السيبرانية والمتمثلة في[4]:

- **مصداقية الدفاع:** يتطلب الدفاع عن أنظمة المعلومات وردع أي محاولة لإختراقها توفر أنظمة نسخ احتياطية (BACKUP SYSTEMS)، ما يعني أن أي هجوم عليها لن يؤدي إلى التدمير التام لها أو الفقدان الكلي لمحتوياتها.

- **القدرة على الانتقام:** ضرورة تكبد المهاجم ضررا يفوق ما وقع على المدافع من أضرار، ما يتطلب تنفيذ هجمة سيبرانية أو أكثر ضد المهاجم الأصلي، في الاتجاه المعاكس وبنفس الشدة، طبعا بعد التعرف عليه.

- **الرغبة في الانتقام وتنفيذه:** على المدافع أن يعلن عن رغبته في الانتقام وينفذها ضد المهاجم، ذلك لأن امتلاك القدرة على الانتقام لا تكفي بمفردها على ردعه.

رابعا: الجغرافيا السياسية

أكد «نابليون بونابارت» أن الجغرافيا تتحكم وتدير سياسة الأمم، من خلال قدرة الدولة على رسم وتوجيه سياستها وتحديد مركز ثقلها الإقليمي والدولي، مع تحديد نوعية ومدى البدائل المتاحة لها عند توجيه وبلورة استراتيجيتها الأمنية والدفاعية[5].

بالمقابل تؤكد أغلب الدراسات أن الفضاء السيبراني أصبح مجالا جديدا للجغرافيا السياسية، إذ تجاوز هذا الأخير المساحة الجغرافية التقليدية القائمة على العوامل الطبيعية ليشمل أمن حدود المعلومات[6] .

خامسا: البعد العسكري

توجه الدول عادة سياساتها تجاه محيطها الإقليمي والدولي استنادا إلى قوتها النسبية في النظام العالمي، مما يجعل من القوة العسكرية ضرورة لازمة لسلوك الدولة، فكلما امتلكت قوة عسكرية متنوعة ورادعة استطاعت تحقيق أهدافها الاستراتيجية بشكل أفضل، لذلك فإن الدول تسعى إلى تحديث وتنويع قدراتها العسكرية باستمرار[7].

إلا أن هناك من يرى أن تحولات العصر وتطوراته مع بروز الفضاء السيبراني، قد حدت من فاعلية الأداة العسكرية التقليدية، لصالح الأدوات التكنولوجية والمعلوماتية، إذ لم تعد نتائجها مضمونة، ولا تحقق الأهداف المرجوة للدولة نظراً لارتفاع تكاليفها ووقوفها كحجر عثرة في وجه تحقيق التنمية الشاملة[8]، مقابل تأثير متعاظم للفضاء السيبراني في تحقيق الأهداف العسكرية للدولة بفاعلية أكبر وتكلفة أقل.

المحور الثاني: أدوات وفواعل الفضاء السيبراني

أولا: أدوات الفضاء السيبراني

لاستيعاب الفضاء السيبراني وتوظيفه بما يحقق أهداف وأمن الدولة، وجب امتلاك والتحكم في مجموعة من الأدوات أهمها[9]:

- **بنية تحتية سيبرانية:** لتكون البنية التحتية السيبرانية فعالة وقادرة على تحقيق أهداف الدولة، يجب أن تشمل على آخر ما توصلت إليه التكنولوجيا الحديثة من خدمات البنية التحتية السيبرانية وأجهزة الكمبيوتر، وبرامج المكافحة والفيروسات والبرمجيات، وأنظمة أمن المعلومات ...الخ.

- **بنية مؤسساتية:** تتكون من جهاز أو مجموعة من الأجهزة سواء كانت مدنية أو عسكرية، تتولى إدارة وتسيير الفضاء السيبراني، بما يتماشى ويحقق الأهداف الأمنية والإستراتيجية للدولة.

- **آليات تشريعية قانونية** : تحدد بداية ونهاية استخدام الفضاء السيبراني، وضوابطه المشروعة.

- **الأدوات الرقابية والتقيمية :** تعمل على إجراء تقييم دوري لتفاعلات الفضاء السيبراني، بما يسمح بتحديد التهديدات والمخاطر المحتملة على أمن الدولة، وبما يتيح الاستفادة من المزايا التي يوفرها هذا الأخير[10]، وإدراج برامج تعليمية وتحسيسية حول مزايا ومخاطر الفضاء السيبراني.

ثانيا: فواعل الفضاء السيبراني

يحدد «جوزيف ناي» ستة أنواع من الفواعل الدولية وغير الدولاتية ضمن الفضاء السيبراني[11]:

1. **الدولة:** يضع القرن الحادي والعشرين الدول المتقدمة في المجال التكنولوجي والمعلوماتي ضمن دائرة الفواعل الأكثر تأثيرا في بنية النظام الدولي، ليصبح العالم الرقمي عنوان للوحدات الدولية الفاعلة، بما يضفي على القوة بعدا جديدا يتحدد عن طريق امتلاك أسلحة رقمية قادرة على شن وصد الهجمات السيبرانية بكل أنواعها.

2. **الفواعل غير الدولاتية:** وتشمل هذه الفواعل ما يلي:

- **الشركات المعلوماتية:** تلعب كبرى الشركات المعلوماتية مثل ميكروسوفت -جوجل -آبل، دورا كبيرا ليس فقط في توفير الخدمات الإلكترونية الأساسية، بل السيطرة والتحكم في الفضاء السيبراني وتوجيهه، وهي الوظيفة التي يفترض أن تؤديها الدول. ففي مؤتمر باريس للسلام في نوفمبر 2018 وقعت هذه الأخيرة مع 50 حكومة إتفاقية جديدة للأمن السيبراني بدون حكومات: الولايات المتحدة الأمريكية -الصين -روسيا؛

- **الشركات المتعددة الجنسيات:** هي ذات بعد عالمي، تعتبر المفتاح الأول للعولمة التي شهدها العالم بشكل واضح في بداية القرن الواحد والعشرين، توصف بالشركات العملاقة، ولا تنقصها سوى شرعية ممارسة القوة التي ما زالت حكراً على الدولة. فهي تمتلك قواعد بيانات ضخمة تستكشف من خلالها وتستغل الأسواق وتؤثر في اقتصاديات الدول وفي ثقافة المجتمعات وتوجهها؛

- **القراصنة السيبرانيون (الهاكرز –الكراكرز):** مجموعة من الأشخاص يوظفون قدراتهم البرمجية عالية المستوى لتحقيق مكاسب شخصية أو مالية أو سياسية غير مشروعة، عن طريق اختراق أجهزة الكمبيوتر وشبكات المعلومات؛

هنا تجدر الإشارة إلى أن القراصنة السيبرانيون عادة ما يشكلون منظمات إجرامية ذات مستوى عالى من الانضباط والتنظيم.

- **الجماعات الإرهابية:** علاوة على استخدام الجماعات الإرهابية للفضاء السيبراني لأغراض التخويف والإرغام ونشر الرعب لأسباب سياسية أو دينية أو إيديولوجية، فإنها تستغل هذا الفضاء في عمليات التجنيد ونشر الأخبار الكاذبة وإشاعتها، بالإضافة إلى اختراق المواقع المدنية والعسكرية الحساسة للدولة وتوظيفها لتحقيق أجنداتها الإرهابية؛

- **الأفراد:** ارتبطت ظاهرة الفاعل الفرد بما يمتلكه هذا الأخير من جملة الامكانيات المادية وغير المادية مثل: المال- الإعلام- الأفكار- المعلومات، وتوظيفها ضمن أهداف خاصة، بهدف التأثير في سلوك الوحدات الفاعلة على المستوى الدولي، بما يخدم ويحقق مصالحه، فعلى سبيل المثال استطاع «روبرت مردوخ» (Rupert Murdoch) تحقيق نفوذ وتأثير في السياسة الدولية بما يمتلكه من مؤسسات إعلامية وإخبارية فاقت 800 مؤسسة في أكثر من 55 بلد[12].

المحور الثالث: الحرب السيبرانية

بداية، تجب الإشارة إلى أن هناك اختلاف كبير بين الحرب السيبرانية (Cyber war) والحرب الإلكترونية (Electronic war)، كون الأولى تعني تعني مجموعة من الإجراءات والمنظومات الإلكترونية التي تستخدم من أجل الاستطلاع، والتشويش على أسلحة العدو. في حين تعتمد الحرب السيبرانية على مجموعة من الوسائل والأدوات، حيث لا تحتاج إلى منصات لإطلاقها مقارنة مع الأسلحة التقليدية، وإنما تتطلب مهارات لإستخدامها ومواقع لإطلاقها على شبكات المعلومات. هذه الحرب هي عبارة عن هجمات يشنها الفواعل في الفضاء الإفتراضي من أجل اختراق الشبكات وإلحاق الضرر بالعدو أو المنافس.

إذن، فالحرب السيبرانية هي جزء فرعي من حرب المعلومات التي تنطوي على استخدام ساحة المعارك وإدارة تكنولوجيا المعلومات والاتصالات، السعي لتحقيق ميزة تنافسية على الخصم.

كما يعرفها (رؤساء الأركان المشتركة JOINT CHIEFS OF STAFF) وزارة الدفاع الأمريكية بأنها التوظيف المتكامل للحرب المعلوماتية، وأنشطة شبكات الحاسوب، والحرب النفسية، والخداع العسكري، وأمن العمليات، بالتنسيق مع قدرات داعمة، وما يتصل بها مع إمكانية التأثير أو الإخلال بقدرات العدو.

وعليه، يساعد هذا التمييز في تحديد مدى السبل التي قد تغير بها الثورة المعلوماتية والرقمية طابع القوة والحرب، وكذلك سياقها وميدانها وأدواتها، حيث يتضمن مفهوم الحرب السيبرانية شكلين من عمليات شبكة الحاسوب[13]:

- **الهجوم السيبراني**: يستهدف قدرات شبكة معلومات العدو، مثل سرقة المعلومات من أجهزة التخزين، أو الهجوم على العمليات التي تقوم بجمع وتحليل ونشر المعلومات وتدميرها، فقد أعلن المنتدى الاقتصادي العالمي سنة 2020 أن الهجمات السيبرانية تشكل خامس الأخطار العالمية، إلى جانب أسلحة الدمار الشامل وقضايا التغير المناخي.

- **الدفاع السيبراني** : هو عبارة عن آلية للدفاع عبر شبكة المعلومات، يرتكز على منع وكشف وتوفير الاستجابات في الوقت المناسب للهجمات أو التهديدات، بما يوفر حماية كبيرة للبنية التحتية المعلوماتية للدولة[14]، حيث تساعد حلول الدفاع السيبراني المؤسسات العسكرية على حماية الأنظمة والبرامج العسكرية من كافة أشكال الاختراقات الممكنة.

ولتحقيق أهداف الحرب السيبرانية يجب توفر ثلاثة عوامل أساسية[15]:

أ- **الفضاء السيبراني:** كما سبق تعريفه، هو المجال الخامس للحرب، إذ يشير إلى البيئة التي تجتمع فيها شبكات الحاسوب وترتبط مع بعضها البعض: أجهزة الحاسوب- أنظمة تكنولوجيا المعلومات- البنى التحتية للاتصالات.

ب- القوة السيبرانية: تمثل القدرة على الحصول على النتائج المرجوة، من خلال استخدام موارد المعلومات المترابطة إلكترونيا في المجال السيبراني، وهي مجموع التأثيرات الاستراتيجية الناتجة عن العمليات الرقمية في الفضاء السيبراني.

ج- الاستراتيجية السيبرانية: هي تطوير وتوظيف القدرات التكنولوجية اللازمة للعمل ضمن الفضاء السيبراني، بحيث تكون متكاملة مع المجالات العملياتية الأخرى، لتحقيق أو دعم تحقيق الأهداف عبر عناصر القوة الوطنية.

هذا وتعتمد الاستراتيجية السيبرانية على مزيج منظم من الغايات والوسائل، لتحقيق أهداف الأمن العسكري والسياسي والاقتصادي، من خلال الاعتماد على القدرات السيبرانية وتوفير الموارد والتكاليف الضرورية لمواجهة التهديدات.

وعليه تتمثل المساهمة الرئيسية للاستراتيجية الوطنية للفضاء السيبراني، في توضيح صريح لكيفية تحقيق جميع الاستراتيجيات الأخرى، لاسيما استراتيجية الدفاع الوطني في مواجهة الحروب السيبرانية بأنواعها الثلاثة[16]:

- **الحرب السيبرانية الباردة منخفضة الشدة:** هي النمط الأكثر شيوعا ضمن تفاعلات البيئة العالمية يمكن وصفها -بحرب الكل ضد الكل- في شكل دائرة صراع عدائي وغير سلمي، حيث يتم استخدام الفضاء السيبراني كأداة للتأثير- التنافس - الصراع – النفوذ- الهيمنة، بين مختلف الفواعل الدولاتية وغير الدولاتية، في كافة مناحي الحياة العامة والخاصة، تستعمل فيها كافة أسلحة الفضاء السيبراني الناعمة، كالتجسس الإلكتروني– سرقة المعلومات والبيانات – اختراق شبكات الحاسوب – الحرب النفسية – الحرب الاعلامية...الخ[17].

هذا النمط من الحروب يعبر عن:

• التنافس والصراع خاصة بين الدول الكبرى في المجال الاستخباراتي: الولايات المتحدة الأمريكية – الصين – روسيا.

• الصراعات التقليدية: ذات الأبعاد السياسية – الاجتماعية - الدينية ، كالصراع الهندي الباكستاني[18].

• التجسس الاقتصادي: سرقة الأسرار التجارية بهدف تحقيق ميزة تنافسية أو منفعة تجارية أو إلحاق الضرر بالمنافس، كفضيحة استيلاء شركة «أوبر UBER» الأمريكية للتكنولوجية على الأسرار التجارية الخاصة بشركة «وايمو WAYMO» الأمريكية للسيارات ذاتية القيادة.

- **الحرب السيبرانية متوسطة الشدة:** يعتمد هذا النمط من الحروب على توظيف الفضاء السيبراني على نطاق واسع من خلال شل شبكات الاتصالات للنظم العسكرية والمدنية، حيث يستمد هذا النمط شدته من قوة أطرافه وقد يمهد للعمل العسكري. ومن بين الأمثلة على ذلك استخدام هذا النوع بشكل واضح في الحرب بين روسيا وجورجيا عام 2008.

- **الحرب السيبرانية الساخنة مرتفعة الشدة:** حيث يعبر هذا النمط عن نشوء حروب في الفضاء السيبراني، منفردة وغير متوازية مع العمليات العسكرية التقليدية .

يقوم هذا النوع من الحروب المستقبلية على سيطرة البعد التكنولوجي في إدارة جميع العمليات العسكرية، حيث يتم حصرا استخدام الأسلحة الإلكترونية كتقنيات الذكاء الاصطناعي والطائرات دون طيار وإدارتها عن بعد، إلى حد الوصول إلى استعمال جميع القدرات الهجومية والدفاعية السيبرانية، من أجل إلحاق الضرر أو التصدي للعدو[19].

غير أن العالم لم يشهد إلى حد الساعة هذا النوع من الحروب، وإن كانت احتمالات حدوثها واردة في المستقبل، مع تطور القدرات التكنولوجيه واتساع الاعتماد بين الدول والفواعل من غير الدول على قدرات الفضاء السيبراني.

استنتاجا مما سبق، فالحرب السيبرانية بأنواعها الثلاثة تتمحور، حول ما يوفره الفضاء السيبراني من قدرات وإمكانيات تكنولوجية هائلة وغير محدودة، تستعمل بغرض تحقيق أهداف سياسية أو اقتصادية أو عسكرية ترتبط بمصالح الفواعل وأوزانها ضمن تفاعلات البيئة العالمية، وهو ما يؤكد أن المعلومات أصبحت هي السلاح والهدف باعتبارها أحد أهم المصادر، وأحد أهم عناصر القوة، ما جعل المؤسسات العسكرية تنظر إليها باعتبارها كفاءة عسكرية أساسية[20].

المحور الرابع: القدرات العسكرية بين الجغرافيا السياسية والفضاء السيبراني

يعيش العالم العديد من الأزمات والصراعات، منها ما هو تقليدي متعلق بأسباب وعوامل جغرافية وتاريخية دينية أو حضارية تستعمل فيها العديد من الوسائل والأدوات العسكرية، والتي قد تصل إلى حد المواجهة العسكرية المباشرة، ومنها ما هو حديث يرتكز على استخدام الفضاء السيبراني من أجل تحقيق أهداف مرتبطة أساسا بقوة الدولة ومكانتها على المستويين الإقليمي والدولي، وهو ما فرض على الدول إعادة التفكير في مفهوم الأمن، لدرجة تمكن الدول من أن تصبح في مأمن من المخاطر التي تتعرض لها سواء في سلامة أراضيها أو استقلالها السياسي أو حماية البنى التحتية لمنشآتها الحيوية، من كافة أوجه الاستخدام غير المشروع لتكنولوجيا الاتصال والمعلومات.

كما أثر الفضاء السيبراني خاصة في بعده العسكري، على الجغرافيا السياسية للدولة، إذ أصبحت القدرات السيبرانية العسكرية التي تمتلكها الجيوش، مؤشرا هاما لقوة الدولة، بعدما تم دمج عمليات الفضاء الإلكتروني في هياكل القوة المرتبطة بالقدرات العسكرية في مجالات استراتيجية الخطط الحربية ومجال الأقمار الصناعية العسكرية، والمجالات المتعلقة بتدريبات الدفاع، إلى حد الوصول إلى دمج القدرات السيبرانية في جميع المستويات والمراحل العملياتية التي تقوم بها القوات المسلحة لمواجهة التهديدات المحتملة.

هنا يمكن القول، أن مفهوم الأمن الوطني قد تطور بشكل واضح تجاه التهديدات السيبرانية الجديدة، واتسع مجاله ليمتد من الجانب العسكري إلى جوانب أخرى. وأن الأجهزة الأمنية للدولة أصبحت تعمل في جزء كبير منها ضمن فضاء مفتوح، يعرضها للعديد من الأخطار تحت دوافع مختلفة، فمن الممكن أن يتم مهاجمتها سواء من الداخل أو من الخارج عن طريق الهاكرز، أو عن طريق أجهزة الاستخبارات في بلدان معادية عبر تنفيذ هجمات إلكترونية بهدف اختراق النظام الأمني المعلوماتي للدولة[21].

نتيجة لذلك، فإن المجال العسكري السيبراني يأتي في مقدمة المجالات التي تشهد نقلة نوعية كبيرة في مجال تعزيز القدرات والاستراتيجيات العسكرية على المستويين التخطيطي والعملياتي، حيث أنه يلعب دورا يفوق بكثير كونه سلاحا في حد ذاته. فعلى المستوى التخطيطي يلعب الفضاء السيبراني دورا في تعظيم القدرات العسكرية، عن طريق التنبؤ والإدراك اللحظي للتهديدات، وسرعة الاستجابة في اتخاذ القرار، أما على المستوى الاستراتيجي المرتبط بصنع القرار العسكري، فتمكن أنظمة القيادة المعززة بتكنولوجيات الذكاء الاصطناعي من تجنب العديد من أوجه القصور المصاحبة لعمليات اتخاذ القرارات الاستراتيجية التقليدية.

من جهة أخرى وبما أن مفهوم الحرب السيبرانية يعني قيام دولة أو فواعل من غير الدول بشن هجوم سيبراني في إطار متبادل أو من طرف واحد، فهو يختلف كثيرا عن مفهوم الحرب التقليدية التي تتطلب استخدام جيوش نظامية ويسبقها إعلان واضح لحالة الحرب وميدان قتال محدد. بينما تبدو هجمات الفضاء السيبراني غير محددة المجال وغامضة الأهداف كونها تتحرك عبر شبكات المعلومات والاتصالات المتجاوزة للحدود الجغرافية للدولة، فضلا عن اعتمادها على أسلحة إلكترونية جديدة تعكس طبيعة سباق التسلح السيبراني[22]، حيث يؤكد المختصون في الدراسات الأمنية على مصطلح «سباق التسلح السيبراني» لوصف التطورات الجيوسياسية والتفاعل الاستراتيجي للدول ضمن الفضاء السيبراني، وفق مقاربة «المعضلة الأمنية»، أين تسعى الدول لتعظيم قدراتها العسكرية لحماية نفسها من أي تهديد، ما يشكل تهديدا مباشراً لأمن الدول الأخرى، يفرز بدوره إجراءات استجابة مضادة تخلق حلقات ردود فعل متعارضة، في شكل سباق تسلح عالمي[23].

في هذا الصدد، أجري مسح تقييمي لمعهد الأمم المتحدة لبحوث نزع السلاح عام 2012 للمعلومات المتاحة للجمهور مس 193 عضوا في الأمم المتحدة جاءت نتائجه كالتالي:

- 144 دولة لديها برامج وطنية للأمن السيبراني؛
- 47 دولة برامجها السيبرانية مرتبطة بشكل أساسي بقواتها المسلحة؛
- 12 من أصل 15 دولة من أكبر المُنْفِقين العسكريين لديهم أو يطورون وحدات مخصصة للحرب السيبرانية؛
- 10 دول تمتلك أو تطور قدرات عسكرية سيبرانية هجومية، منها الولايات المتحدة الأمريكية - المملكة المتحدة - الصين – روسيا – فرنسا – إيران وكوريا الشمالية.

نتيجة لذلك، من المتوقع أن يرتفع استخدام القدرات العسكرية السيبرانية خاصة الهجومية منها، ضمن القدرات العسكرية الاجمالية للدول بنسبة تصل إلى 39 % بحلول عام 2027، بسبب ارتفاع ميزانيات سباق التسلح السيبراني في جميع أنحاء العالم[24].

استنادا إلى ما سبق، لا يمكن الإنكار أن البعد العسكري للفضاء السيبراني، قد أحدث تغييرات عميقة في المفاهيم المرتبطة بالجغرافيا السياسية للدولة، فمفهوم الحدود قد تغير كليا. فالدولة تواجه تحديات أمنية كي تضمن وتؤكد الحفاظ على حدودها واتصالاتها وقيادتها وسيطرتها وقدرتها الحاسوبية ضد التهديدات الجديدة عبر الإنترنت التي تواجه العالم برمته، كالهجمات الإرهابية السيبرانية وعصابات الجريمة المنظمة. فشساعة المساحة الافتراضية التي تشغلها الإنترنت، تضع سيادة الدولة ومصالحها موضع تهديد مباشر ومستمر، فمنذ نهاية الحرب الباردة كانت هناك العديد من الحجج، التي تشير إلى أنه بسبب ترابط الانسانية عبر الإنترنت، فإن مفهوم الدولة ومفاهيم الجغرافيا السياسية قد تم تجاوزها، كظاهرة موازية لعولمة السلع والأفكار المادية، فضلاً عن أن العولمة قد أثرت في الأمن الوطني للدولة بطرق مختلفة، وهذا ما دفع الدول إلى التسابق نحو التسلح العسكري السيبراني، وتطوير واقتناء أحدث الأنظمة الإلكترونية، لتوظيفها ضمن ترسانتها العسكرية سواء الدفاعية منها أو الهجومية، ما وضع بدوره الجغرافيا السياسية للدولة في موضع مباشر لمواجهة التهديدات المتعلقة بالأمن السيبراني وذلك لعدة أسباب أهمها[25]:

- أن البنى التحتية للإنترنت من الأقمار الصناعية إلى الموجهات والكوابل توضع في نقاط جغرافية محددة (معظمها تم وضعها من قبل شركات خاصة) ويؤخذ بوضعها اعتبارات الجغرافية السياسية للدولة؛

- تحدث عملية التبادل السيبراني في مناطق توجد فيها توترات جيوسياسية؛

- الاستخدام السيبراني له بعد جيوسياسي كون أدواته افتراضية، وتأثيره يحدث في الواقع؛

- أن الفضاء السيبراني يعمل كمساحة افتراضية للعديد من الجهات الفاعلة، لاستغلال استراتيجيتهم الجيوسياسية المتأصلة في العالم المادي الواقعي[26].

بناء عليه، يمكن القول أن الاستخدام المتزايد للفضاء السيبراني من أجل تحقيق أهداف جيوسياسية، أدى إلى ظهور مقاربة جديدة في المجال العسكري عرفت بالجيوسيبرانية كإطار للنشاط المتصل بفضاء المعلومات واستخداماتها العسكرية، فلم يعد ممكنا فصل القدرات العسكرية التقليدية عن مثيلاتها السيبرانية في عملية واضحة للاعتماد المتبادل، كما لم يعد هناك إمكانية لفصل الفضاء السيبراني عن التفاعلات الجيوسياسية التي تحدث على أرض الواقع.

الخاتمة

أَدْخَلتْ التطورات التكنولوجية للمعلومات الجغرافيا السياسية للدولة في حقبة جديدة،

مما فرض على الدول تغيير كيفية تعاملها مع الفواعل الأخرى وتحديد مصالحها الوطنية وأولوياتها الاستراتيجية بما يتماشى مع ما يفرضه الفضاء السيبراني من معطيات مرتبطة بالأساس بأمن الدولة وسيادتها.

فالتطورات التكنولوجية والمعلوماتية الحديثة أدت إلى ثورة في مجال الأسلحة، وفي استراتيجيات شن الحروب المسلحة، حيث أصبح الاتجاه العام يشير إلى زيادة الاعتماد على الفضاء السيبراني في شكل سباق تسلح سيبراني عسكري، قد يؤدي لأي سبب كان إلى مواجهة عسكرية تقليدية وغير تقليدية في العالم الواقعي.

بناء على كل ما سبق، يتبين أن الجغرافيا السياسية للدولة لها أهمية خاصة في مواجهة التهديدات المتعلقة بالأمن السيبراني وأثره في قوة الدولة من خلال ظهور شكل جديد للقوة وهو القوة الافتراضية والتي تعرف بالقدرة على الحصول على النتائج المرجوة، من خلال مصادر المعلومات المرتبطة إلكترونيا بالميدان المعلوماتي، وهو ما بات يعرف بالجيوسيبرانية.

ومنه يمكن القول إن الأمن السيبراني هو بُعد جديد ضمن أبعاد الأمن الوطني للدولة، أحدث تغييرات جوهرية في مفاهيم العلاقات الدولية كالتسلح -الأمن -القوة -التهديد، حيث حتّم على فواعل المجتمع الدولي الإنتقال من عالم مادي إلى عالم افتراضي في غاية التعقيد والتشابك، وبالتالي أصبح مفهوم الأمن السيبراني ضرورة حتمية في عالم اليوم، خاصة في ظل ارتباط كافة التفاعلات الدولية بالجانب الرقمي والتكنولوجي، الأمر الذي يستدعي من الدول ضرورة إيجاد ميكانيزمات ووسائل فعالة لمواجهة المخاطر والتهديدات السيبرانية التي تتميز بالسرعة والغموض والدقة، ومن ثمة تحقيق الأمن السيبراني والحفاظ على وجود الدولة وأمنها الوطني.

كنتيجة لكل ما سبق، أصبحت الجغرافيا السياسية بعيدة كل البعد عن الإطار المادي الجغرافي الأصلي المخصص لها، ليستحوذ الفضاء السيبراني على أهم الأسلحة العسكرية من جهة وأبرز نقاط الضعف الجيوسياسية للدول من جهة أخرى، مقلصا المسافة بين التهديدات السيبرانية والتهديدات المادية■

الهوامش

1. علي زياد علي، الصراع والأمن الجيوسيبراني في الساحة الدولية: دراسة في استراتيجيات الاشتباك الرقمي، (عمان: دار أمجد للنشر والتوزيع، 2020)، ص 121.
2. إيفانز غراهام، نوينهام جيفري، قاموس بنغوين للعلاقات الدولية. تر: مركز الخليج للأبحاث، (الإمارات العربية المتحدة: مركز الخليج للأبحاث 2004)، ص369.
3. الإستراتيجية الوطنية للأمن السيبراني 2018 - 2023 : وزارة الاتصالات وتكنولوجيا المعلومات.
4. Putten, Frans-Paul Van Der, Minke Meijnders & Jan Rood, Deterrence as a Security Concept against Non-traditional Threads, Clingendal Monitor, 2015, pp 1-64.

5. مكرديس روي، تومبسون كينت، مرجع سابق، ص 189.

6. علي رياد علي، مرجع سابق، ص 129.

7. Ivo H. Daalder and James M. Lindsay, America Unbound: The BushRevolution, in Foreign Policy, Washington, D.C., Brookings Institution Press, 2003, p 29 .

8. مكرديس وتومبسون، مرجع سابق، ص ص 39-41.

9. Daniel Venter, (2017), "A Future and Strategic Study - Changes in Cybersecurity: Factors Constraints, and Variables," Naples, p 186.

10. Ravikumar Ramachandrani, considered cybersecurity and its crucial role in the global economy, Cambridge, London, 2018, p 44.

11. Joseph S. Nye, Cyber Power, (Cambridge: Harvard Kennedy School. Belfer Center for Science and (International Affairs، 2010) , p 216.

12. Lehto Martti , Neittaanmäk Pekka. Cyber Security: Analytics, Technology and Automation. Switzerland: Springer International Publishing, 2015, p 19.

13. Brandon Valeriano and Manes Ryan., Cyber War versus Cyber Realities: Cyber Conflict in the International System, New York, Oxford, (2015), p 59.

14. Ibid , p70.

15. منى الأشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، بيروت ،2017، ص 66.

16. عبد الصادق عادل، الإرهاب الإلكتروني القوة في العلاقات الدولية: نمط جديد وتحديات مختلفة، (القاهرة: مركز الدراسات السياسية والاستراتيجية بالأهرام، 2009)، ص ص 93-97.

17. عبد الغفار عفيفي الدويك، «معضلة تعريف الإرهاب في الفكر والممارسة الدوليين»، مجلة السياسة الدولية، العدد 210، أكتوبر، 2017، ص 17.

18. المرجع نفسه، ص 19.

19. Robert McMillan. "Was Stuxnet Built to Attack Iran's Nuclear Program?", PC World, 21 September 2014. Available at: https://www.pcworld.com/article/205827/was_stuxnet_built_to_attack_irans_nuclear_program.html

20. سلوان جابر هاشم، حالة الضرورة العسكرية في القانون الدولي الانساني، لبنان: المؤسسة الحديثة للكتاب، ط 9، 2013)، ص 59.

21. نسرين الشحات الصباحي، الأبعاد العسكرية للقوة السيبرانية على الأمن القومي للدول دراسة حالة «إسرائيل» منذ عام 2010، المركز الديمقراطي العربي، 29 أفريل 2016.

22. Robert Mandel, Global Security Upheaval: Armed Non-State Groups Usurping State Stability, Functions, (California: Stanford University Press, 2013), p 11.

23. John Arquilla, (August 4, 2015), Deterrence After Stuxnet, Communications of the ACM , Available at: https://goo.gl/wR99ff.

24. Carmen-Cri 1 Solène Baudouin-Naneix, 3 September 2019, Cyber Weapons: The New 'Arms Race', European Army Interoperability Centre.

25. Stuart H. STARR., Towards an Evolving Theory of Cyber power, a Center for Technology and National Security Policy (CTNSP) National Defense University (NDU), Cryptology and Information Security Series, Volume 3: The Virtual Battlefield: Perspectives on Cyber Warfare, 2009 , p 81.

26. WANG Limao, M. Changes in driving forces of geopolitical evolution and the new trends in geopolitics studies[J]. Geographical Research, 2016 , p 197.

قائمة المراجع

أولا: باللغة العربية

1) أحمد عبيس نعمة الفتالوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، جامعة بابل- كلية القانون، العدد الرابع، السنة الثامنة، 2016.

2) إيفانز غراهام، نوينهام جيفري. قاموس بنغوين للعلاقات الدولية. تر: مركز الخليج للأبحاث. الإمارات العربية المتحدة: مركز الخليج للأبحاث 2004.

3) سلوان جابر هاشم، حالة الضرورة العسكرية في القانون الدولي الانساني، ط9 ،المؤسسة الحديثة للكتاب، لبنان، 2013.

4) عبد الصادق عادل، الإرهاب الإلكتروني القوة في العلقات الدولية: نمط جديد وتحديات مختلفة، مركز الدراسات السياسية والاستراتيجية بالأهرام، القاهرة، 2009.

5) عبد الغفار عفيفي الدويك، «معضلة تعريف الإرهاب في الفكر والممارسة الدوليين»، مجلة السياسة الدولية، العدد 210، أكتوبر 2017.

6) علي زياد علي، الصراع والأمن الجيوسيبراني في الساحة الدولية: دراسة في استراتيجيات الاشتباك الرقمي، (عمان: دار أمجد للنشر والتوزيع، 2020).

7) الاستراتيجية الوطنية للأمن السيبراني 2018-2023 .وزارة الاتصالات و تكنولوجيا المعلومات، الأردن.

8) منى الأشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية و القضائية، بيروت ،2017.

9) نسرين الشحات الصباحي، الأبعاد العسكرية للقوة السيبرانية على الأمن القومي للدول دراسة حالة «إسرائيل» منذ عام 2010، المركز الديمقراطي العربي، 29 افريل 2016.

10) أليكس مينتس وكاري دي روين، فهم صنع القرار في السياسة الخارجية ، ترجمة محمد ولد المنى (الإمارات: مركز الإمارات للدراسات والبحوث الإستراتيجية ، 1999) .

ثانيا : باللغة الاجنبية

1) Brandon Valeriano and Manes Ryan., (2015), Cyber War versus Cyber Realities: Cyber Conflict in the

2) Daniel Venter, 2017, "A Future and Strategic Study - Changes in Cybersecurity: Factors Constraints, and Variables," Naples.

3) Frank Trager and Philip Kronenberg , National Security and American Society , Kansas : Kansas University Press , 1973 .

4) International System, New York, Oxford.

5) Iulian F. Popa, cyber geopolitics and sovereignty. an introductory overview ,Conference Paper, Conference: 5th International scientific conference „National and International Security", At Armed Forces Academy of Genera.

6) Ivo H. Daalder and James M. Lindsay, America Unbound: The BushRevolution , in Foreign Policy, Washington, D.C., Brookings Institution Press, 2003 p29 .

7) Joseph S. Nye، Cyber Power (Cambridge: Harvard Kennedy School. Belfer Center for Science and (International Affairs، 2010)

8) Lehto Martti , Neittaanmäk Pekka .Cyber Security: Analytics, Technology and Automation. Switzerland : Springer International Publishing, 2015.

9) Myriam Dunn, "The Cyberspace Dimension in Armed Conflict: Approaching a Complex Issue with Assistance of the Morphological Method", Information and Security: An International Journal, vol. 7, 2001.

10) Putten, Frans-Paul Van Der, Minke Meijnders & Jan Rood, Deterrence as a Security Concept against Non-traditional Threads, Clingendal Monitor, 2015.

11) Ravikumar Ramachandrani, 2018, considered cybersecurity and its crucial role in the global economy, Cambridge, London, 2018.

12) Robert Mandel, Global Security Upheaval: Armed Non-State Groups Usurping State Stability ,Functions,(California: Stanford University Press, 2013).

13) Robert Mandel, Global Security Upheaval: Armed Non-State Groups Usurping State Stability ,Functions,(California: Stanford University Press, 2013) .

14) Schreier, Fred (2015). On Cyber Warfare. 1st edition. DCAF. Switzerland: Geneva

15) Stuart H. STARR., Towards an Evolving Theory of Cyber power, a Center for Technology and National Security Policy (CTNSP) National Defense University (NDU), Cryptology and Information Security Series, Volume 3: The Virtual Battlefield: Perspectives on Cyber Warfare, 2009.

16) WANG Limao, M. Changes in driving forces of geopolitical evolution and the new trends in geopolitics studies[J]. Geographical Research, 2016.

17) Carmen-Cri 1 Solène Baudouin-Naneix, 3 September 2019, Cyber Weapons: The New 'Arms Race', European Army Interoperability Centre.

ثالثا : الوابوغرافيا

1) Robert McMillan. "Was Stuxnet Built to Attack Iran's Nuclear Program?", PC World, 21 September 2014. Available at: https://www.pcworld.com/article/205827/was_stuxnet_built_to_attack_irans_nuclear_program.html

2) Schreier, Fred (2015). On Cyber Warfare. 1st edition. DCAF. Switzerland: Geneva https://statesassembly.gov.je/assemblyreports/2017/r.1242017.pdf. p.2-3.