الاصطفاف الدولي في الفضاء السيبراني: الابعاد الاستراتيجية والتحديات المستقبلية

International Alignment in Cyberspace: Strategic Dimensions and Future Challenges

م.م. سيف نايف عبد العباس
جامعة بغداد– مركز الدراسات الاستراتيجية والدولية
saif.n@cis.uobaghdad.edu.iq

م.م. دعاء ضياء ابراهيم
جامعة النهرين– كلية الهندسة
doaadheyaa79@gmail.com

تاريخ استلام البحث: ٢٠٢٥/٥/٨ **تاريخ قبول النشر: ٢٠٢٥/٨/١٠**

الملخص:

ان التطور السريع الذي احدثته تكنولوجيا المعلومات، خاصةً في الشبكات ادى الى تحول كبير في مفهوم القوة، وترتب عليه دخول العالم في مرحلة جديدة تلعب فيها هجمات الفضاء السيبراني دوراً اساسياً، واصبح التفوق والتسابق والسيطرة على هذا الفضاء اهم اهداف الاصطفاف الدولي، وعليه فان هذه الدراسة تناولت مفهوم الاصطفاف الدولي كنمط من انماط التحالفات السياسية والاقتصادية والعسكرية، كما حاولنا في هذه الدراسة توضيح العلاقة بين الفضاء السيبراني والاصطفاف الدولي والتركيز على التحديات ومستقبل الاصطفاف الدولي في هذا المجال.

الكلمات الافتتاحية: الاصطفاف الدولي، التعاون والشراكة، القدرات الرقمية، الأمن السيبراني، التنافس الرقمي.

Abstract:

The rapid development of information technology, particularly in networks, has led to a major shift in the concept of power. This has led the world to enter a new phase in which cyberspace attacks play a fundamental role. Superiority, competition, and control of this space have become the most important goals of international alignment. Accordingly, this study examines the concept of international alignment as a model of political, economic, and military alliances. We also attempt to clarify the relationship between cyberspace and international alignment, focusing on the challenges and future of international alignment in this area.

Keywords: International Alignment, Collaboration and Partnership, Digital Capabilities, Cybersecurity, and Digital Competition.

المقدمة

في عصر الثورة الرقمية والتكنولوجيا المتسارعة، أصبح الفضاء السيبراني أحد أهم المجالات الاستراتيجية التي تحدد مسارات القوة والنفوذ في القرن الحادي والعشرين. ومع تنامي الاعتماد على التكنولوجيا في جميع جوانب الحياة من الاقتصاد إلى الدفاع، ومن الخدمات العامة إلى العلاقات الدولية تحول الفضاء السيبراني إلى ساحة جديدة للتنافس والصراع بين الدول والكيانات غير الحكومية. هذا التنافس لم يعد محصورًا في الحدود الجغرافية التقليدية، بل امتد ليشمل الهجمات الإلكترونية، التجسس الرقمي، والحرب المعلوماتية، ما ادى إلى اعادة رسم خريطة القوة العالمية.

على الصعيد الآخر، برز مفهوم الاصطفاف الدولي كنمط من أنماط التحالفات السياسية والاقتصادية والعسكرية التي تتشكل بناءً على المصالح المشتركة أو التهديدات المشتركة. وفي ظل التغيرات الجيوسياسية الأخيرة، مثل الحرب في أوكرانيا، وتصاعد التوتر بين الولايات المتحدة والصين، وبروز القوى الناشئة مثل الهند والبرازيل وجنوب إفريقيا، يشهد العالم إعادة تشكيل للكتل الدولية، مما ينعكس بشكل مباشر على كيفية إدارة الدول لمسائل الأمن السيبراني والتعاون الرقمي.

وبالتالي، فإن العلاقة بين الفضاء السيبراني والاصطفاف الدولي علاقة وثيقة ومتداخلة؛ إذ باتت الدول تستخدم الفضاء الإلكتروني كأداة ضغط سياسي، ووسيلة للتأثير في الرأي العام العالمي، وأحيانًا كسلاح فعّال في الصراعات الحديثة. كما أصبح التعاون أو الخلاف بين الكتل الدولية يمتد إلى الفضاء السيبراني، سواء في مجال وضع المعايير الأخلاقية لاستخدام التكنولوجيا، أو في تأمين البنية التحتية الرقمية، أو حتى في تطوير سياسات مواجهة للهجمات الإلكترونية العابرة للحدود. وبالتالي، فإن فهم ديناميكيات الفضاء السيبراني والاصطفاف الدولي فيه يصبح ضروريًا لفهم التحديات الأمنية والقانونية والسياسية في القرن الحادي والعشرين.

أهمية البحث: ان تزايد الاعتماد على الفضاء السيبراني في الحياة اليومية (الاقتصاد، السياسة، الأمن، التواصل)، وتصاعد التهديدات السيبرانية العابرة للحدود (الهجمات، القرصنة، الحرب الإلكترونية)، مما ادى الى الحاجة لتنسيق دولي لضمان أمن واستقرار الفضاء السيبراني، ومن هنا تبرز أهمية هذا البحث كونه يسلط الضوء على أحد أكثر التحديات تعقيداً وتأثيرا في العصر الحديث.

هدف البحث: يهدف البحث الى تحليل أشكال الاصطفاف الدولي في الفضاء السيبراني، ودراسة التحالفات القائمة والتحديات التي تواجهها، واستشراف مستقبل التعاون أو التنافس الدولي في هذا المجال.

اشكالية البحث: هل يمكن تحقيق اتفاق دولي شامل حول استخدامات الفضاء السيبراني؟ وكيف تتعامل الدول مع التحديات القانونية والأخلاقية في استخدام الفضاء السيبراني؟ وما هي أبرز أشكال الاصطفاف الدولي في الفضاء السيبراني؟

فرضية البحث: يعد الفضاء السيبراني ساحة جديدة للتنافس الدولي، وتسعى الدول من خلاله إلى تعزيز نفوذها الجيوسياسي، بالتالي فان هناك حاجة ملحة إلى تعاون دولي مدعوم بإطار قانوني واضح لضمان الاستقرار والأمن في الفضاء السيبراني.

منهجية البحث: تم الاعتماد على المنهج التاريخي للتعرف على مفهوم الفضاء السيبراني ومراحل تطوره التاريخي، والمنهج التحليلي لتحليل الأطر القانونية والسياسية الحالية المتعلقة بالفضاء السيبراني.

هيكلية البحث: تناول البحث ثلاث مباحث تطرق المبحث الاول الى توضيح مفهوم الفضاء السيبراني والاصطفاف الدولي، والمبحث الثاني ركز على اشكال الاصطفاف الدولي في الفضاء السيبراني، اما المحث الاخير فقد تناول مستقبل الاصطفاف الدولي في الفضاء السيبراني.

المحور الأول: الفضاء السيبراني والاصطفاف الدولي – المفهوم والتطور

الفضاء السيبراني والاصطفاف الدولي موضوعان مترابطان بشكل متزايد في القرن الحادي والعشرين، حيث أصبحت التكنولوجيا الرقمية عاملاً محورياً في العلاقات الدولية، وتحديدًا في سياق الأمن القومي، والتنافس الجيوسياسي، والتعاون الدولي.

اولاً: تعريف الفضاء السيبراني ومراحل تطوره: ان الفضاء السيبراني مصطلح حديث ظهر نتيجة لثورة تكنولوجيا المعلومات ويشمل جميع الحواسيب والمعلومات التي بداخلها والأنظمة والبرامج والشبكات المفتوحة لاستعمال الجمهور العام أو تلك الشبكات التي صممت لاستعمال فئة محددة من المستعملين ومنفصلة عن شبكة الإنترنت العامة [١]. ويتميز الفضاء السيبراني بقدرته على تجاوز الحدود الجغرافية والزمنية مما يجعله وسيلة رئيسية للتواصل بين الناس ولتنفيذ العديد من الأنشطة التجارية والتعليمية والترفيهية، كما أنه يشكل منصة لظهور تقنيات حديثة مثل الذكاء الاصطناعي وإنترنت الأشياء، التي تعزز من تداخل حياتنا اليومية مع العالم الرقمي [٢]، ومما سبق يمكن توضيح ما يلي:

أ. التعريف: هو بيئة تفاعلية حديثة، تشمل عناصر مادية وغير مادية، ومكون من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين، سواء كانوا مشغلين أو مستعملين، اضافة الى ذلك فان مسألة تحديد مفهوم الفضاء السيبراني تتوقف على طبيعة ادراك الدول والهيئات الرؤية الاستراتيجية والقدرة على استغلال المزايا المتاحة، ومواجهة المخاطر الكاملة في هذا الفضاء [٣]، بالتالي فان الفضاء السيبراني ليس مجرد منصة ابتكار وتطوير بل يمثل تحدياً كبيراً يتعلق بأمن العلوات وخصوصية الافراد [٤]، لذلك فقد أصبح ساحة استراتيجية للصراع والتعاون بين الدول، ويؤثر بشكل مباشر على الاصطفافات الدولية، حيث تتحول القوة الرقمية إلى معيار جديد من معايير القوة الوطنية.

ب. مراحل تطور الفضاء السيبراني: ان تطور الفضاء السيبراني هو مسار تاريخي طويل يعكس التقدم التكنولوجي في مجالات الحوسبة، والاتصالات، وشبكات الإنترنت. يمكن تقسيم هذا التطور إلى عدة مراحل رئيسية:

١. **بدايات الاتصالات الرقمية (قبل الثمانينات):** ظهر مفهوم الشبكات الحاسوبية مع مشروع ARPANET الذي أطلقته وكالة DARPA الأمريكية عام ١٩٦٩، وهو أساس الإنترنت الحديث، وكانت هذه المرحلة تتعلق بإنشاء بنية تحتية لنقل البيانات بين المؤسسات العلمية والعسكرية، بالتالي لم يكن هناك فضاء سيبراني حقيقي، بل كانت عمليات تبادل بيانات محدودة بين المؤسسات البحثية.

٢. انتشار الإنترنت (١٩٨٠–١٩٩٥): في عام ١٨٨٣ تم اعتماد بروتوكول TCP/IP كمعيار رسمي في ARPANET، مما سهل الربط بين الشبكات المختلفة، وفي عام ١٩٩٨ قدم تيم بيرنرز–لي (Tim Berners-Lee) فكرة الويب العالمي (World Wide Web) وفي ١٩٩١ تم إتاحة الويب العالمي للعامة، مما أدى إلى تسريع انتشار الإنترنت (٥).

٣. تحول الفضاء السيبراني من مجرد شبكة اتصال إلى بيئة اجتماعية واقتصادية وسياسية من خلال ظهور مواقع مثل (Amazon) عام ١٩٩٤ و(eBay) عام ١٩٩٥ وبدأت المؤسسات باستخدام تحليل

البيانات لفهم المستخدمين في الفضاء السيبراني وظهور وسائل التواصل الاجتماعي حيث أطلق عام ٢٠٠٤ (Facebook) وعام ٢٠٠٦ (Twitter) (٦).

٤. **العصر الرقمي والفضاء السيبراني الحديث (٢٠١٠ –حتى الآن):** تطور خدمات الحوسبة حيث أصبح الفضاء السيبراني جزءاً أساسياً من الأمن القومي، الاقتصاد، السياسة، وحتى الحياة اليومية. بالتالي ادى هذا الى زيادة الهجمات السيبرانية، لهذا ظهرت خطوط حمراء في تفاعلات الدولية في الفضاء السيبراني خاصة بعملية الردع السيبرانية (٧).

ثانياً: تعريف الاصطفاف الدولي ومظاهره: ان مصطلح الاصطفاف الدولي يستخدم لوصف توزيع الدول او التحالفات في العلاقات الدولية حيث تجمعهم مصالح مشتركة او خصومات مشتركة، بالتالي هو أحد انماط التفاعلات الاساسية التي تجري في البيئة الدولية.

أ. **تعريف الاصطفاف الدولي:** هو ظاهرة تشير إلى تشكيل تحالفات ومحوريات بين الدول على أساس المصالح المشتركة، أو التهديدات المتقاربة، أو الرؤى الموحدة فيما يتعلق باستخدام الإنترنت والفضاء الرقمي، هذا الاصطفاف يعكس بشكل كبير الواقع الجيوسياسي في العالم المادي، لكن له خصوصيته التي تنبع من طبيعة الفضاء السيبراني كمجال غير ملموس، سريع التغير، وذو طبيعة عابرة للحدود [٨].

ب. **مظاهر الاصطفاف الدولي:** للاصطفاف الدولي مظاهر كثيرة أسهمت في تعزيز فكرة الاصطفاف والتعاون الدولي في الفضاء السيبراني من خلال تشكيل التحالفات الدولية في المجال الرقمي، ويعد التعاون الدولي أحد اهم ادوات المواجهة للأخطار السيبرانية خاصة تلك العابرة للحدود فهذا الامر يستدعي تنسيق دولي لتحقيق الحد الأدنى من تدابير الامن وتبادل المعلومات وتدوين قواعد السلوك من خلال التدابير الاتية [٩]:

١. الاتفاقيات الثنائية ومتعددة الأطراف: وفقاً لمؤشر الامن السيبراني العالمي للعام ٢٠٢٠، فأن هناك ٩٠ دولة فقط لديها اتفاقيات ثنائية في مجال التعاون السيبراني من بينها ١٠ دول عربية.

٢. المشاركة في الأنشطة الدولية: مشاركة ١٤٠ دولة في أنشطة دولية مثل مؤتمرات الامن السيبراني.

٣. الشراكة بين القطاع العام والقطاع الخاص: انخراط ٨٦ دولة في شراكة بين القطاع العام والقطاع الخاص سواء كان ذلك على المستوى المحلي او الدولي.

المحور الثاني: اشكال الاصطفاف الدولي في الفضاء السيبراني

ان أشكال الاصطفاف الدولي في الفضاء السيبراني يكون في عدة صور، منها: تشكيل تحالفات وتكتلات سيبرانية بين الدول، وسباق التسلح السيبراني، ونشوب صراعات سيبرانية، بالإضافة إلى ظهور جهات فاعلة من غير الدول في هذا المجال [١٠]، والهدف الاساسي من تشكيل هذه التحالفات او التكتلات لتعزيز القدرات الدفاعية والهجومية في الفضاء السيبراني، وتبادل الخبرات والمعلومات، ومواجهة التهديدات المشتركة [١١].

اولاً: نداء باريس (٢٠١٨) لتعزيز الأمن السيبراني والمبادئ الديمقراطية: هي مبادرة أطلقتها فرنسا في عام ٢٠١٨، وتهدف إلى تعزيز الأمن والاستقرار في الفضاء السيبراني من خلال التعاون

الدولي وتطبيق مجموعة من المبادئ المشتركة، يقترح النداء رؤية لتنظيم الفضاء السيبراني والمبادئ الرئيسية المرتبطة به، لا سيما منع فشل الأمن والامتناع عن استخدام بعض الممارسات التي قد تضر باستقرار الفضاء السيبراني [١٢].

أ. اهداف النداء: يهدف الى تعزيز التعاون الدولي من خلال جمع الدول والمنظمات والشركات الخاصة والمجتمع المدني معًا للعمل على تحقيق الأمن السيبراني، اضافة الى مواجهة التهديدات السيبرانية، والتأكيد على اهمية القانون الدولي وحقوق الانسان في الفضاء السيبراني، تبني معايير وممارسات جيدة في مجال الامن السيبراني، فضلاً عن اشراك الجهات الفاعلة الخاصة في تعزيز الامن السيبراني [١٣].

ب. المبادئ: يضع نداء باريس عدة مبادئ وإرشادات توجيهية مهمة في مسألة الأمن الإلكتروني العالمي، ومسؤوليات الجهات الفاعلة الرئيسة في القطاع الخاص وجهودها في تحسين الثقة والأمن والاستقرار في الفضاء الإلكتروني، ومشجعاً المبادرات الرامية إلى تعزيز أمن العمليات والمنتجات الرقمية على امتداد سلاسل التوريد، ومن أبرز هذه المبادئ [١٤]:

١. حماية الافراد والبنية التحتية ومنع الانشطة الالكترونية الضارة والتعافي منها.

٢. التعاون لبناء الثقة والأمن على جميع الجهات الفاعلة التعاون مع بعضها البعض لتبادل المعلومات، وتطوير القدرات، وتعزيز الثقة في الفضاء السيبراني.

٣. دعم القدرات السيبرانية على الدول الاستثمار في بناء قدرات الأمن السيبراني، وتدريب الموارد البشرية، وتطوير التكنولوجيا اللازمة لمواجهة التهديدات السيبرانية.

٤. مكافحة الجريمة السيبرانية من خلال تقديم مرتكبي الجرائم إلى العدالة.

٥. دعم حقوق الإنسان في الفضاء السيبراني، بما في ذلك حرية التعبير والخصوصية.

٦. تشجيع الحوار والتعاون وبناء وتعاون دولي لتعزيز الأمن السيبراني والاستقرار.

ثانياً: التعاون بين روسيا والصين في مجال السيبرانتميديا (الإنترنت السيادي): بعد أن أصبح الفضاء السيبراني مجالا فريدا للتهديدات السيبرانية ويؤثر على سيادة ومصالح الدول واستقرار العلاقات الدولية، فلا بد من بناء استراتيجية للأمن السيبراني موحدة على صعيد دولي توحد الجهود والتعاون بين الدول من أجل إرساء فضاء سيبراني آمن، مما يعزز الثقة بين الدول، ويدعم التجارة الدولية، ويحمي البنية التحتية لأنشاء نظام عالمي يعتمد على التعاون في مواجهة التهديدات المشتركة بدلاً من التنافس[١٥].

وبذلك يعد التعاون الروسي الصيني ركيزة أساسية لضمان الاستقرار الاقتصادي والتنموي لكلا البلدين، كما يتوقع أن يشهد العام الجديد تركيزًا متزايدًا على التعاون في مجال الأمن السيبراني والذكاء الاصطناعي، في ظل تزايد التهديدات الرقمية، وتعاظم أهمية التكنولوجيا في تحديد ملامح المستقبل الاقتصادي والجيوسياسي[١٦].اضافة الى ذلك فان جهود روسيا للحصول على مساعدة الصين في تعزيز الذكاء الاصطناعي تعد محاولة لتحدي ريادة أمريكا في هذا المجال، وتعاونها مع الصين باعتباره خطوة ضرورية نحو اكتساب المهارات والمعرفة والتكنولوجيا المتعلقة بالذكاء الاصطناعي [١٧]، ومن ابرز اهداف التعاون:

١. مكافحة التجسس تسعى روسيا والصين إلى حماية بياناتهما من عمليات التجسس التي تقوم بها الولايات المتحدة وحلفاؤها، والعمل على تطوير قدراتهما في مجال الأمن السيبراني لمواجهة هذه التهديدات.

٢. إعادة تشكيل الإنترنت للحد من الهيمنة الغربية والسيطرة على الفضاء السيبراني [١٨].

٣. التنسيق في مجلس الأمن تستخدم روسيا والصين حق النقض (الفيتو) في مجلس الأمن الدولي بشكل متزامن للدفاع عن مصالحهما المشتركة في مواجهة القرارات الغربية.

٤. تحقيق الامن السيبراني ومواجهة التهديدات حيث قامت روسيا بتأسيس فضاء إلكتروني خاص بها مستقل عن شبكة الانترنت الحالية بهدف التخلص من الهيمنة وعمليات التجسس الالكتروني الامريكية، اضافة الى انها اعتمدت استراتيجية خاصة بالحرب الإلكترونية الهجومية من خلال استخدام الأسلحة الإلكترونية الهجومية باعتبار انها قوة مضافة في الحرب، وبذلك طبقت كل من روسيا والصين نموذج "السيادة الإلكترونية" بدلاً من حرية الفضاء السيبراني بهدف حماية امنهم القومي. ما يجعل هاتان الدولتان لهما تأثير دولي في هذا السياق هو السلطة التي تمتلكها للتحكم في بيانات الإنترنت الخاصة بالمواطنين ومراقبتها من أجل فرض القوانين الوطنية التي تنظم الخطاب العام ووسائل الإعلام، بالإضافة إلى القدرة على تنظيم النشاط السياسي [١٩].

٥. نبادل الخبرات والمعلومات حيث وقعت روسيا والصين عدة اتفاقيات ثنائية للتعاون في مجال التكنولوجيا وحوكمة الإنترنت، ففي عام ٢٠١٥، اتفق كل منهما على التعاون داخل منظمة شنغهاي للتعاون لحماية حقوق الدولة في تحديد وتنفيذ السياسات العامة المتعلقة بالاتصالات والمعلومات، بما في ذلك الإنترنت. وفي عام ٢٠١٦، أكد البيان المشترك للبلدين على مبدأ احترام السيادة الوطنية في مجال المعلومات وضمان تنظيم فعال لـ "مساحة المعلومات"، تم تعزيز التعاون من خلال معاهدة ثنائية في عام ٢٠١٩ تركز على حوكمة الإنترنت وإدارة المحتوى عبر الويب، بالإضافة إلى ذلك، دعم كل من البلدين مجموعات العمل التابعة للأمم المتحدة التي تشجع على مبادئ السيادة الإلكترونية في مناقشات حوكمة الإنترنت، وعارضوا مبادرات الأمم المتحدة في هذا الإطار المرتكزة على حقوق الإنسان بدعم من الولايات المتحدة وحلفاؤها (٢٠).

ثالثاً: تحالف العيون الخمس: لكي تبقى الولايات المتحدة الامريكية في مكانتها المهيمنة على النظام الدولي قامت بأنشاء تحالف العيون الخمس ويعني (Eyes Five The) ويكتب اختصاراً (FVEY) وهو تحالف استخباراتي يضم أستراليا وكندا ونيوزيلندا والمملكة المتحدة والولايات المتحدة، ويضم تحالف منظمة العيون الخمس المؤسسات الاستخبارية الآتية: وكالة الأمن القومي الأميركية، والقيادة العامة لاتصالات حكومة المملكة المتحدة، ومؤسسة أمن الاتصالات الكندية، والمديرية الأسترالية للإشارات، ومكتب أمن اتصالات الحكومة النيوزيلندية، فيكون مهمة هذا التحالف (جمع المعلومات التي تتحرك في منظومات الاتصال المختلفة، والاستحواذ على الاتصالات، والوثائق والمعدات، وتحليل حركة الاتصالات، وتحليل الشفرات والرموز، وفك الشفرات والترجمة، والحصول على المعلومات الخاصة بالمؤسسات العاملة في مجالات الاتصالات، والأساليب، والتطبيقات والمعدات) [٢١].

المحور الثالث: التحديات والآثار المترتبة عن للاصطفاف السيبراني على الساحة الدولية

أصبح الفضاء السيبراني ساحة استراتيجية ومحورية للتعاون والشراكة من جهة والصراع والتنافس من جهة أخرى، هذا الامر الذي أدى الى تشكيل تحالفات دولية تعكس تباين المصالح والاولويات بينها، اذ أدى التنافس الرقمي العالمي الى اتجاه العلاقات الدولية نحو مرحلة هجينة يعاد بها تشكيل موازين القوى في الفضاء السيبراني، وبهذه التحولات المتسارعة يتوجب علينا الإجابة عن عدد من التساؤلات التي يعد أهمها عن ماهية ملامح مستقبل الاصطفاف الدولي في الفضاء السيبراني؟

اولاً: مستقبل الاصطفاف الدولي: ان التهديدات السيبرانية اليوم تعتبر أحد أبرز التحديات الجيوسياسية التي تواجه الأمم، فتزداد أهمية القدرات السيبرانية والسيادة الرقمية كأحد العناصر المؤثرة في العلاقات الدولية مما سيعطي احتمالية تعزيز التعاون الدولي لمواجهة التهديدات السيبرانية، لذا فمستقبل هذا الاصطفاف يتجه نحو مرحلة ذات تعقيد كبير بسبب التداخلات ذات الاعتبارات الأمنية والتكنولوجية والاقتصادية والسيادية، هذا سيعيد رسم خارطة التحالفات الدولية وفقاً لمعايير جديدة ليست بالضرورة ان تكون جغرافية او أيديولوجية بل رقمية ومعلوماتية.

١. **تكثيف الجهود الدولية للتصدي للهجمات السيبرانية:** تشهد الساحة الدولية اليوم سعياً كبير تقوم به الدول والمنظمات لمواجهة التهديدات السيبرانية، اذ تتباين دور هذه الجهود من حيث الأدوار فيمكن ان تكون في تبادل الخبرات والمعلومات إضافة الى وضع الخطط والاستراتيجيات لمكافحة الجرائم السيبرانية وزيادة الدعم الدولي للتصدي لها، فعلى الرغم من غياب وجود سلطة عليا تنظم التفاعلات في الفضاء السيبراني، الا ان هناك جهود كبيرة تسعى الى ضبط التفاعلات وسلوك الدول والفواعل من غير الدول في الفضاء السيبراني في اطار التنظيمات الدولية القائمة والتي اسفر عنها اتفاقيات على الصعيد الدولي والإقليمي والثنائي، منها من تم وضعه في صياغة الخطط والاستراتيجيات الوطنية ومنها ما يقدم للدعم التقني والفني، ومنها ما هو متعلق في تدريب القوى البشرية، ومنها ما أسهم من خلاله في تفعيل آليات الحساب والعقاب كالمنظمة الدولية للشرطة الجنائية "الإنتربول، ومنهاما قامت به منظمة الأمم المتحدة من جهود متعددة لمأسسة وتنظيم التصدي للتهديدات السيبرانية ووضع قواعد موضوعية واجرائية وعقد المؤتمرات والقمم الدولية [٢٢].

٢. **تشكيل التكتلات السيبرانية المتعددة:** تسعى العديد من الدول الى تكثيف جهودها في اعلان تكتلات سيبرانية لمواجهة التهديدات، لتعزيز تبادل المعلومات وتطوير بنى تحتية مشتركة لمراقبة الحوادث والاستجابة لها، مستفيدةً من الخبرات المتراكمة والمراكز الوطنية للأمن السيبراني [٢٣].

٣. **الاستثمار في البنى التحتية السيبرانية:** تعمل الدول اليوم على بناء بنية تحتية قوية للأمن السيبراني، من خلال انشاء المراكز الوطنية للأمن السيبراني التي يكون من اعمالها رصد وتحليل التهديدات وتقديم الاستجابة الفورية للحوادث السيبرانية، فضلاً عن تحديث الأنظمة التكنولوجية لضمان حماية البيانات الحساسة، اذاً أصبحت دول تدرك تماماً بأن تطوير القدرات السيبرانية والاستثمار في بنيتها التحتية ضرورة أساسية في الحفاظ على امنها القومي، خاصة ونحن نشهد اليوم صراعاً دولياً يتجه بالأساس نحو

المغالبة والتنافس وتعزيز النفوذ في الساحة التكنولوجية التي غيرت شكل الحروب التقليدية وادواتها التي اثرت في ديناميكية العلاقات الدولية [٢٤].

ثانيا: التحديات التي تواجه الاصطفافات الدولية: أن التهديدات السيبرانية التي افرزت تحديات امنية معقدة امام الدول دفعتهم لتشكيل اصطفافات دولية في الفضاء السيبراني لتوفير بيئة تعاونية في مواجهة الاخطار الرقمية، الان ان هذه الاصطفافات تواجه تحديات تكمن في كونها امراً جوهرياً لتقدير طبيعة النظام السيبراني الدولي المشكل، والتنبؤ بمستقبل الامن السيبراني الدولي خاصة في ظل اعتماد الدول على الأدوات السيبرانية ضمن استراتيجيتها الهجومية او الدفاعية، وعلى الرغم من الحاجة الملحة للتعاون الدولي، فإن العديد من التحديات تجعل تنسيق الأمن السيبراني العالمي صعباً، وتتعدد التحديات التي تواجه الاصطفاف الدولي لتشمل ما يأتي [٢٥]:

١. **انعدام الشفافية:** قيام الدول غالباً إضفاء الطابع السري لاستراتيجياتها وقدراتها السيبرانية وهذا يمكن أن يعيق الشفافية المحدودة لفهم التدابير التي تتخذها الدول في استجابتها لمواجهات التهديدات السيبرانية مما سيؤدي الى تحليلات غير كاملة او متحيزة.

٢. **اختلاف وجهات النظر الوطنية:** عادة ما تكون وجهات نظر الدول متباينة في شؤون امنها السيبراني بناءً على سياقها الجيوسياسي وقيمها الثقافية وتجاربها التاريخية، مما ستعقد هذه الاختلافات الجهود المبذولة لوضع معايير واتفاقيات دولية يكون شأنها زيادة التعاون بين الدول لمواجهة التهديدات السيبرانية.

٣. **التوترات الجيوسياسية:** يمكن للاعتبارات السياسية والتوترات الجيوسياسية ان تعيق إنشاء آليات تعاونية، مما يحد من فعالية الجهود الدولية للتصدي للتهديدات السيبرانية.

٤. **التحديات القانونية والتنظيمية:** تتباين الأطر القانونية والتنظيمية للأمن السيبراني بشكل ملحوظ بين الدول وهذا سيشكل عائق أمام تحقيق التعاون الدولي الفعال في هذا المجال، فالتحديات الرئيسة تكمن في ضرورة مواءمة هذه الأطر على الرغم من الفروقات الجوهرية في التقاليد القانونية وتباين مقاربات الخصوصية، واختلاف أولويات الأمن القومي بين الدول.

٥. **التفاوتات في الموارد:** تشهد الدول تفاوت في الموارد والقدرات المتاحة لمواجهة تهديدات الأمن السيبراني، حيث تواجه البلدان النامية والفقيرة اقتصادياً صعوبات كبيرة في تبني وتنفيذ تدابير سيبرانية ذات قدرة فعالة، مما سيؤدي هذا التفاوت في اتساع الفجوة السيبرانية على المستوى العالمي، وهذا قد ينعكس سلباً على جهود تحقيق التعاون الدولي في الأمن السيبراني.

٦. **الاعتبارات الأخلاقية:** يطرح استخدام القدرات السيبرانية الهجومية مجموعة من القضايا الأخلاقية المعقدة، من بينها مسألة التناسب واحتمال وقوع أضرار جانبية والمخاطر المرتبطة بعسكرة الفضاء السيبراني، وغالباً لا تحظى الاعتبارات الاخلاقية اهتماماً كافياً ضمن استجابات الدول أو في إطار الاتفاقيات والمعايير الدولية المنظمة للسلوك في الفضاء السيبراني.

الخاتمة

يعتبر الفضاء السيبراني اليوم ساحة استراتيجية ناشئة تشهد تصاعداً كبيراً في التنافس بين الفواعل الدولية، حيث تجاوز الأمن السيبراني طابعه التقني الضيق ليصبح مكون أساسي في تشكيل السياسات الخارجية والتحالفات الدولية، لذا أن الاصطفاف الدولي في الفضاء السيبراني يمثل امتداد لتفاعلات القوة التقليدية، مما جعل الدول تسعى إلى بناء تحالفات تقنية وأمنية بهدف تعزيز قدراتها الدفاعية والهجومية في بيئة رقمية متسارعة التغير، فضلاً عن بروز تحديات متعددة تعيق تحقيق تنسيق فعال بين الدول، من أبرزها التفاوت في الأطر القانونية والتنظيمية، واختلال موازين القدرات التقنية، بالإضافة إلى تنامي الاعتبارات الأخلاقية المتعلقة باستخدام القدرات السيبرانية الهجومية كل هذه العوامل تسهم في تعقيد مشهد الاصطفاف السيبراني، لذا فإن مستقبل الاصطفاف الدولي في الفضاء السيبراني يظل رهيناً بقدرة المجتمع الدولي على تحقيق توازن دقيق بين ضرورات الأمن السيبراني، واحترام مبادئ السيادة الوطنية، وضمان حماية الحقوق والحريات الفردية، ويتطلب ذلك تبني مقاربات تعاونية، وتفعيل آليات الحوكمة متعددة الأطراف، فضلاً عن بلورة رؤى استراتيجية مشتركة تستجيب للتحولات المتسارعة في الفضاء السيبراني.

التوصيات

١. الحاجة الى قواعد مشتركة ووضع أطر قانونية وسياسية دولية لضبط استخدام الفضاء السيبراني خصوصاً في المجالات العسكرية والاقتصادية.

٢. تعزيز الجهود لمواكبة التطور السريع في اساليب مخاطر وهجمات سيبرانية من خلال الحفاظ على السيادة الوطنية والعمل الجماعي لمواجهة التحديات السيبرانية، خاصة ان الامن السيبراني لم يعد خياراً بل أصبح شرطاً اساسياً لاستقرار الدول وحمايتها في عصر رقمي متسارع.

٣. دعم قدرات الدول النامية في مجال الأمن السيبراني من خلال مبادرات تقنية وتمويلية تهدف إلى تقليص الفجوة الرقمية وضمان شمولية الحماية السيبرانية.

٤. تأسيس معايير أخلاقية دولية تنظم استخدام القدرات السيبرانية الهجومية، وتراعي مبادئ التناسب والتمييز والحد من الأضرار الجانبية.

الهوامش:

(١) محمود محارب، "إسرائيل والحرب الالكترونية، قراءة في كتاب حرب في الفضاء الالكتروني: اتجاهات وتأثيرات على إسرائيل"، سلسلة مراجعة كتب صادرة عن المركز العربي للأبحاث ودراسة السياسات، ٢٠١١، ص١.

(٢) سيناء علي محمود، "التحديات الامنية للدول في الفضاء السيبراني"، مجلة قضايا سياسية، العدد ٨٠، (٢٠٢٥)، ص ٣١٥.

(٣) حازم محمد خليل، "استغلال الفضاء السيبراني في الحروب غير التقليدية: دراسة في الوكالة السيبرانية والإرهاب السيبراني"، المجلة العلمية لكلية الدراسات الاقتصادية والعلوم السياسية بالجامعة الإسكندرية، المجلد الثامن، العدد ٥، (٢٠٢٣)، ص٢٧١.

(٤) حمدون توريه، الفضاء السيبراني وتهديد الحرب السيبرانية البحث عن السلام السيبراني، الاتحاد الدولي للاتصالات، ٢٠١١، ص٩.

Tim Jordan, Cyberpower: an introduction to the politics of cyberspace, op cit. p 20_21.

(٦) ايهاب خليفة، "الدائرة المغلقة: لماذا تتجه الدول لتأسيس شبكات إنترنت وطنية"، مركز المستقبل للأبحاث والدراسات المتقدمة، العدد ٧، (٢٠١٥)، ص ٦٠_ ٦٤.

(٧) رغد البهي، "الردع السيبراني: المفهوم والإشكاليات والمتطلبات"، مجلة العلوم السياسية والقانونية، العدد الأول، (٢٠١٧)، ص٥١_٥٣.

(٨) سايل سعيد، "التعاون الاوروبي المتوسطي في ضوء الازمة الاقتصادية العالمية (٢٠٠٧-2011)"، رسالة ماجستير غير منشورة، كلية الحقوق والعلوم السياسية (جامعة مولود معمري، ٢٠١١)، ص٢٠.

(٩) رانيا سليمان سعد الدين، "رؤية امنية في مؤشر الامن السيبراني العالمي لعام ٢٠٢٠"، ورقة بحثية مقدمة الى جامعة نايف العربية، ٢٠٢٣، ص٩_١٠.

(١٠) خالد وليد محمود، "الفضاء السيبراني وتحولات القوة في العلاقات الدولية"، المركز العربي للأبحاث والدراسات، قطر، ٢٠٢٥، ص٣.

(١١) ناجي محمد أسامة، "الجوانب القانونية للحرب السيبرانية، دراسة في إطار القانون الدولي"، مجلة روح القوانين، العدد ١٠٣، (٢٠٢٣)، ص٣٠.

Affairs, M. f. (2018). Paris Call for Trust and Security in Cyberspace. Retrieved, pp 1.

(١٣) "فرنسا وضمان أمن الفضاء الإلكتروني"، موقع وزارة أوروبا والشؤون الخارجية، تاريخ الدخول: ٢٠٢٥/٥/٤، على الرابط: https://www.diplomatie.gouv.fr/

(14) The 9 principles", Paris Call website. Entry on 4/5/2024, on the link; https://pariscall.international/en/principles

(١٥) محمد محمود زيتون، العمليات السيبرانية وتأثيرها على تحولات السيادة في الفضاء السيبراني، المجلة العربية للنشر العالمي، الاصدار الثامن، العدد: ٧٧، (٢٠٢٥)، ص١٧٢.

(١٦) ديمتري بريجع، أولويات التعاون الروسي الصيني في عام ٢٠٢٥، مركز الدراسات العربية الأوراسية، ٢٧ يناير ٢٠٢٥، تاريخ الدخول: ٢٠٢٥/٥/٥، على الرابط: https://eurasiaar.org/

(١٧) "امن دولي . ما هي أهداف روسيا من التعاون مع الصين في مجال الذكاء الاصطناعي"، المركز الاوروبي لدراسات مكافحة الارهاب والاستخبارات، ١١ يناير ٢٠٢٥، تاريخ الدخول: ٢٠٢٥/٥/٥، على الرابط: https://www.europarabct.com/

(١٨) عائشة إبراهيم الحوسني، "آفاق العلاقات الصينية–الروسية في ضوء زيارة فلاديمير بوتين للصين"، ترينذز للبحوث والاستشارات، ابو ظبي، ٤ يونيو ٢٠٢٤، تاريخ الدخول: ٢٠٢٥/٥/٥، على الرابط: https://trendsresearch.org/ar/insight/

(١٩) سهيلة محمد احمد، صفاء عبد الباسط، "البعد السيبراني في السياسة الخارجية: روسيا والصين نموذجاً، مركز العرب للأبحاث والدراسات، ٢ أكتوبر ٢٠٢٤، تاريخ الدخول: ٢٠٢٥/٥/٨، على الرابط: https://alarab2030.com/

(٢٠) خالد وليد محمود، "المغالبة والتنافس في القدرات السيبرانية الأمريكية الصينية"، مجلة شؤون استراتيجية، العدد ١٨، يونيو ٢٠٢٤، ص ١٩٣_ ١٩٤.

(٢١) عبد الله عبد الأمير، "منظمة العيون الخمسة"، مركز البيان للدراسات والتخطيط، ٢٠١٩، تاريخ الدخول: ٢٠٢٥/٥/١٥، على الرابط: https://www.bayancenter.org/2019/09/5429/

(٢٢) هبة جمال الدين، "الامن السيبراني والتحول في النظام الدولي"، مجلة كلية الاقتصاد والعلوم السياسية، المجلد ٢٤، العدد ١، (٢٠٢٣) ص ٢٠٦_٢٠٧.

(٢٣) احمد فتحي، " مستقبل الصراعات السيبرانية في الشرق الأوسط: التداخل بين الجيوسياسية والامن"، مركز آتون للدراسات، ٣٠ أبريل، ٢٠٢٥، تاريخ الدخول: ٢٠٢٥/٥/١٥، على الرابط: https://www.atoonra.com/

(٢٤) خالد وليد محمود، "المغالبة والتنافس في القدرات السيبرانية الامريكية الصينية"، مجلة شؤون استراتيجية، العدد ١٨، ٢٠٢٤، ص١٨٠.

(25) Michael Leung, "Cyber security Challenges in International Relations: State Responses and Global Cooperation", International Journal of Open Access Publishing and Exploration International Journal of Publishing and Exploration Volume 3, Issue 2, (2015), p 16_17.

قائمة المصادر

١) محمود محارب، "إسرائيل والحرب الالكترونية، قراءة في كتاب حرب في الفضاء الالكتروني: اتجاهات وتأثيرات على إسرائيل"، سلسلة مراجعة كتب صادرة عن المركز العربي للأبحاث ودراسة السياسات، ٢٠١١.

٢) سيناء علي محمود، "التحديات الامنية للدول في الفضاء السيبراني"، مجلة قضايا سياسية، العدد ٨٠، ٢٠٢٥.

٣) حازم محمد خليل، "استغلال الفضاء السيبراني في الحروب غير التقليدية: دراسة في الوكالة السيبرانية والإرهاب السيبراني"، المجلة العلمية لكلية الدراسات الاقتصادية والعلوم السياسية بالجامعة الإسكندرية، المجلد الثامن، العدد ٥، (٢٠٢٣).

٤) حمدون توريه، الفضاء السيبراني وتهديد الحرب السيبرانية البحث عن السلام السيبراني، الاتحاد الدولي للاتصالات، ٢٠١١.

5) Tim Jordan, Cyberpower: an introduction to the politics of cyberspace, op cit. p 20-21.

٦) ايهاب خليفة، "الدائرة المغلقة: لماذا تتجه الدول لتأسيس شبكات إنترنت وطنية"، مركز المستقبل للأبحاث والدراسات المتقدمة، العدد ٧، (٢٠١٥).

٧) رغد البهي، "الردع السيبراني: المفهوم والإشكاليات والمتطلبات"، مجلة العلوم السياسية والقانونية، العدد الأول، (٢٠١٧).

٨) سايل سعيد، "التعاون الاوروبي المتوسطي في ضوء الازمة الاقتصادية العالمية (٢٠٠٧-٢٠١١)"، رسالة ماجستير غير منشورة، كلية الحقوق والعلوم السياسية (جامعة مولود معمري، ٢٠١١).

٩) رانيا سليمان سعد الدين، "رؤية امنية في مؤشر الامن السيبراني العالمي لعام ٢٠٢٠"، ورقة بحثية مقدمة الى جامعة نايف العربية، ٢٠٢٣.

١٠) خالد وليد محمود، "الفضاء السيبراني وتحولات القوة في العلاقات الدولية"، المركز العربي للأبحاث والدراسات، قطر، ٢٠٢٥.

١١) ناجي محمد أسامة، "الجوانب القانونية للحرب السيبرانية، دراسة في إطار القانون الدولي"، مجلة روح القوانين، العدد ١٠٣، (٢٠٢٣).

12) Affairs, M. f. (2018). Paris Call for Trust and Security in Cyberspace. Retrieved, pp.

١٣) "فرنسا وضمان أمن الفضاء الإلكتروني"، موقع وزارة أوروبا والشؤون الخارجية، تاريخ الدخول: ٤/٥/٢٠٢٥، على الرابط: https://www.diplomatie.gouv.fr/

14) The 9 principles", Paris Call website. Entry on 4/5/2024, on the link; https://pariscall.international/en/principles

١٥) محمد محمود زيتون، العمليات السيبرانية وتأثيرها على تحولات السيادة في الفضاء السيبراني، المجلة العربية للنشر العالمي، الاصدار الثامن، العدد: ٧٧، (٢٠٢٥).

١٦) ديمتري بريجع، أولويات التعاون الروسي الصيني في عام ٢٠٢٥، مركز الدراسات العربية الاوراسية، ٢٧ يناير ٢٠٢٥، تاريخ الدخول: ٢٠٢٥/٥/٥، على الرابط: https://eurasiaar.org/

١٧) "امن دولي . ما هي أهداف روسيا من التعاون مع الصين في مجال الذكاء الاصطناعي"، المركز الاوروبي لدراسات مكافحة الارهاب والاستخبارات، ١١ يناير ٢٠٢٥، تاريخ الدخول: ٢٠٢٥/٥/٥، على الرابط: https://www.europarabct.com/

١٨) عائشة إبراهيم الحوسني، "آفاق العلاقات الصينية–الروسية في ضوء زيارة فلاديمير بوتين للصين"، ترينذز للبحوث والاستشارات، ابو ظبي، ٤ يونيو ٢٠٢٤، تاريخ الدخول: ٢٠٢٥/٥/٥، على الرابط: https://trendsresearch.org/ar/insight/

١٩) سهيلة محمد احمد، صفاء عبد الباسط، "البعد السيبراني في السياسة الخارجية: روسيا والصين نموذجاً، مركز العرب للأبحاث والدراسات، ٢ أكتوبر ٢٠٢٤، تاريخ الدخول: ٢٠٢٥/٥/٨، على الرابط: https://alarab2030.com/

٢٠) خالد وليد محمود، "المغالبة والتنافس في القدرات السيبرانية الأمريكية الصينية"، مجلة شؤون استراتيجية، العدد ١٨، يونيو ٢٠٢٤.

٢١) عبد الله عبد الأمير، "منظمة العيون الخمسة"، مركز البيان للدراسات والتخطيط، ٢٠١٩، تاريخ الدخول: ٢٠٢٥/٥/١٥، على الرابط: https://www.bayancenter.org/2019/09/5429/

٢٢) هبة جمال الدين، "الامن السيبراني والتحول في النظام الدولي"، مجلة كلية الاقتصاد والعلوم السياسية، المجلد ٢٤، العدد ١، (٢٠٢٣).

٢٣) احمد فتحي، "مستقبل الصراعات السيبرانية في الشرق الأوسط: التداخل بين الجيوسياسية والامن"، مركز آتون للدراسات، ٣٠ أبريل، ٢٠٢٥، تاريخ الدخول: ٢٠٢٥/٥/١٥، على الرابط: https://www.atoonra.com/

٢٤) خالد وليد محمود، "المغالبة والتنافس في القدرات السيبرانية الامريكية الصينية"، مجلة شؤون استراتيجية، العدد ١٨، ٢٠٢٤.

25) Michael Leung, “Cyber security Challenges in International Relations: State Responses and Global Cooperation”, International Journal of Open Access Publishing and Exploration International Journal of Publishing and Exploration Volume 3, Issue 2, (2015).