الفضاء السيبراني وابعاده الجيوبولتيكية العراق نموذجا

م.م. ايات جبار فاضل عبد الله
جامعة المستنصرية \ كلية التربية \قسم الجغرافية
ayat.jabbar@uomustansiriyah.edu.iq

المستخلص

تعد الجغرافية من العلوم المتجددة والمتطورة باستمرار ، إذ تخضع الظواهر الجغرافية لتغيّرات زمنية متواصلة متأثرة بمجموعة من العوامل الطبيعية والبشرية. وقد انعكست هذه السمة على فروع الجغرافيا كافة، ولا سيّما الجغرافيا السياسية والمفاهيم المرتبطة بها مثل السيادة والحدود، التي شهدت تحولات جوهرية نتيجة التقدّم التكنولوجي المتسارع الذي يشهده العالم المعاصر. فقد أسهمت الثورة الرقمية في إعادة تشكيل طبيعة السيادة، إذ أصبحت بيانات الدول ومعلوماتها عرضة للاختراق، ولم تعد قدرة كل دولة مؤكدة في الحفاظ على اتصالاتها وقيادتها وسيطرتها وقدراتها الحاسوبية في مواجهة التهديدات الجديدة المنبثقة من الفضاء الإلكتروني، مثل الهجمات الإرهابية والعصابات الإجرامية المنظمة.

وتأتي هذه التحوّلات في سياقٍ أوسع يشهد تغيرًا جوهريًا في مفاهيم المكان والحدود والسلطة؛ إذ فرض الفضاء السيبراني نفسه بوصفه حدودًا غير مرئية للدولة، تمتد خارج الإطار الجغرافي التقليدي، وتؤثر بصورة مباشرة في مكانتها وأمنها القومي. فالمساحة الافتراضية التي يشغلها الإنترنت أصبحت تمثل امتدادًا مكملاً للحدود المادية، كما غدت قادرة على تهديد سيادة الدول ومصالحها الوطنية نظرًا لطابعها العابر للحدود ولإمكانية نقل المعلومات خارج نطاق السيطرة التقليدية

ومن هذا المنطلق، يسلّط البحث الضوء مفهوم الفضاء السيبراني وخصائصه القدرات السيبرانية وتأثيرها في طبيعة الصراعات والتهديدات الأمنية وأنماط الحروب السيبرانية في العالم و العراق نموذجا التحديات التي تواجه الأمن السيبراني في العراق و فرص تعزيز الأمن السيبراني في العراق

الكلمات المفتاحية : الفضاء ، السيبراني ، وابعاده الجيوبولتيكية، العراق نموذجا

Abstract

Geography is regarded as one of the ever-evolving sciences, as geographical phenomena are continuously subject to temporal changes influenced by various natural and human factors. This dynamic nature has been reflected across all branches of geography, particularly political geography and its related concepts such as sovereignty and borders, which have undergone profound transformations due to the rapid technological advancements of the contemporary

world. The digital revolution has significantly reshaped the nature of sovereignty, as state data and information have become increasingly exposed to cyber intrusions. Consequently, many states can no longer fully guarantee the protection of their communications, command systems, control mechanisms, and computing capabilities against emerging threats originating from cyberspace, such as cyberterrorism and organized cybercrime.

These transformations are part of a broader shift in the understanding of space, boundaries, and authority, as cyberspace has established itself as an invisible frontier of the state that extends beyond traditional geographical borders, directly influencing its standing and national security. The virtual dimension created by the Internet has become a vital extension of physical boundaries, capable of undermining state sovereignty and national interests due to its transnational nature and the ability to transfer information beyond traditional control frameworks.

From this perspective, the study seeks to explore the concept of cyberspace, its key characteristics, and cyber capabilities, while analyzing their impact on the nature of conflicts, security threats, and cyber warfare patterns globally — with Iraq as a case study. Furthermore, it examines the challenges confronting cybersecurity in Iraq and highlights the opportunities available to strengthen and enhance its cyber resilience

Keywords: Cyberspace, Cyber Dimensions, Geopolitical Aspects, Iraq as a Case Study.

المقدمة :

يشهد العالم اليوم مرحلة غير مسبوقة من التحول الرقمي السريع، حيث أصبح الأمن السيبراني محوراً أساسياً في منظومة الأمن القومي للدول. ومع اتساع نطاق التفاعل عبر الفضاء الإلكتروني، برز هذا المجال كأحد أشكال الحدود الجديدة التي لم تعد تُقاس بالمكان المادي، بل تمتد إلى فضاءات غير مرئية تتجاوز الجغرافيا

التقليدية. وقد ترك هذا الواقع المتغيّر أثره العميق في الجغرافيا السياسية، التي أخذت تعيد النظر في مفاهيمها الكلاسيكية، وعلى رأسها السيادة والحدود، في ضوء التحولات التكنولوجية المتسارعة التي أحدثتها الثورة المعلوماتية وثورة الاتصالات.

لقد أدّى هذا التقدّم إلى تآكل بعض أوجه السيادة التقليدية للدولة، إذ باتت بياناتها ومعلوماتها الحيوية عرضة للاختراق، وأصبحت قدرتها على حماية شبكاتها وأنظمتها الإلكترونية موضع اختبار دائم أمام موجات متصاعدة من الهجمات السيبرانية. فالمجال الافتراضي الذي يتيحه الإنترنت تجاوز الإطار الجغرافي المألوف، وأصبح يشكّل فضاءً عالمياً تتداخل فيه المصالح وتتقاطع فيه التهديدات، مما جعل من الصعب على الدول الإحاطة الكاملة بحركة المعلومات داخل حدودها أو السيطرة عليها خارجياً.

وفي ضوء ذلك، غدا الفضاء السيبراني بمثابة حدٍّ جديدٍ من حدود الدولة غير المرئية، وعنصراً محورياً في حماية أمنها القومي وترسيخ مكانتها الدولية في عصرٍ باتت تُقاس فيه القوة بقدراتها الإلكترونية بقدر ما تُقاس بإمكاناتها العسكرية أو الاقتصادية. وتكمن أهمية هذا البحث في تناوله هذه الظاهرة من منظور جغرافي سياسي حديث، يسعى إلى تحليل التحوّلات التي نقلت مفهوم الحدود من صورته المادية المرئية — البرية والبحرية والجوية — إلى صورته الرقمية غير المرئية التي يمثلها الفضاء الإلكتروني، باعتباره مجالاً استراتيجياً جديداً

للصراع والتنافس الجيوبولتيكي في العالم المعاصر.

مشكلة البحث :

بكيفية تمكين الدول من حماية سيادتها الوطنية في ظل التهديدات السيبرانية المتصاعدة، التي باتت تستهدف البنى التحتية الحيوية والأنظمة الرقمية لمؤسساتها الحكومية والاقتصادية. إذ تُثير هذه التحديات إشكاليات معقدة تتعلق بقدرة الدولة على صون فضائها الرقمي وضمان أمن معلوماتها وبياناتها الحساسة، في مواجهة أشكال متطورة من الهجمات الإلكترونية وعمليات التجسس السيبراني التي تتخطى الحدود الجغرافية التقليدية وتُضعف مظاهر السيادة في عالمٍ يتزايد فيه الاعتماد على التكنولوجيا الرقمية.

فرضية البحث :

هدف حماية الأمن السيبراني إلى حفظ سيادة الدولة والسيطرة على الفضاء الرقمي، تعزيز ثقة المواطنين، تأمين الاقتصاد الوطني، حماية المؤسسات الحكومية، وضمان التعاون الدولي والإقليمي في تبادل المعلومات بما يحفظ مصالح الدول .

هدف البحث:

تحليل تأثير التهديدات السيبرانية على مفهوم الحدود السياسية للدولة، وتقييم آثارها على السيادة الوطنية، التوازنات الدولية، والاستقرار الإقليمي.

منهجية البحث :

اعتمد البحث على التحليلي والوصفي للوصول الى النتائج التي يتوخاها البحث

هيكلية البحث:

الاطار النظري: مشكلة البحث، فرضية البحث، هدف البحث،منهجية البحث، هيكلية البحث، الاستنتاجات والتوصيات

الفصل الأول: مفهوم الفضاء السيبراني، خصائص الفضاء السيبراني، القدرات السيبرانية وتأثيرها في طبيعة الصراعات والتهديدات الأمنية، أنماط الحروب السيبرانية في العالم

الفصل الثاني : العراق نموذجا ، التحديات التي تواجه الأمن السيبراني في العراق ، فرص تعزيز الأمن السيبراني في العراق

الفصل الأول : أولا: مفهوم الفضاء السيبراني

الفضاء السيبراني هو بيئة رقمية افتراضية غير ملموسة، تتميز بتفاعلات معقدة بين عناصرها المادية وغير المادية، وتشمل أجهزة الكمبيوتر، الشبكات، البرمجيات، البيانات، ومعطيات التحكم والنقل، إلى جانب مستخدميها. يمثل هذا الفضاء امتدادًا للعالم المادي، حيث تتشابك فيه العمليات الرقمية مع الواقع المادي بشكل متبادل، فتتأثر الدول والمؤسسات والمجتمعات بالأنشطة الإلكترونية وتؤثر فيها في الوقت ذاته.

يمكن النظر إلى الفضاء السيبراني على أنه حدود جديدة للدولة، تتجاوز الحواجز الجغرافية والسياسية التقليدية، إذ يسمح بتحقيق الاتصال والتفاعل الإلكتروني بين الأفراد والكيانات على نطاق عالمي. كما أنه يشكل بيئة لمحاكاة الظواهر الواقعية من خلال التفاعلات البعيدة، وتعد هذه المحاكاة وسيلة لتعزيز القدرات البشرية والتقنية، سواء في المجالات المدنية أو العسكرية أو حتى في نشاطات الجماعات غير الحكومية.

وصفت بعض الدراسات الفضاء السيبراني بأنه البعد الخامس للحرب أو "الذراع الرابعة للجيوش الحديثة"، إلى جانب القوات البرية والبحرية والجوية، حيث يشهد الإنترنت معارك حقيقية تشمل الهجمات، التجسس، واختراق البنى التحتية الحيوية، ما أحدث نمطًا جديدًا من الصراعات غير التقليدية وأعاد تشكيل مفاهيم القوة والسيادة.

كما يُنظر إليه من زاوية اجتماعية وثقافية على أنه حيزمكاني ينشأ عن دمج التكنولوجيات الرقمية والإنترنت ضمن شبكة مترابطة، تتيح إنتاج وتبادل البيانات النصية والسمعية والبصرية، بما يحكمه السياق الاجتماعي والثقافي للمستخدمين. ويؤكد هذا البعد على أن السيطرة على الفضاء السيبراني وحمايته لا يمكن أن تتحقق إلا عبر امتلاك أدوات المعرفة الرقمية والتقنيات الحديثة، بما يضمن حماية المعلومات وتأمين التواصل الرقمي. (كلاع، ٢٠٢٢، صفحة ٢٩٤)

وقد تطورت تعريفات الفضاء السيبراني عبر الزمن، بدءًا من التعريفات التقنية البحتة التي تركز على الأجهزة والبرمجيات، وصولًا إلى التعريفات متعددة التخصصات التي تربطه بالأبعاد السياسية والأمنية والاجتماعية. ووفقًا لتعريف وزارة الدفاع الأمريكية، فهو "مجال يستخدم الإلكترونيات وتكنولوجيا المعلومات والطيف الكهرومغناطيسي لتخزين البيانات ومعالجتها وتبادلها عبر الشبكات والبنية التحتية المرتبطة بها

باختصار، يمكن القول إن الفضاء السيبراني أصبح عنصرًا محوريًا في العلاقات الدولية والأمن القومي والصراعات الحديثة، إذ يجمع بين القدرات التقنية والتحليلية والبعد الاجتماعي والسياسي، ويستمر في تشكيل تهديدات وفرص جديدة للدول والمؤسسات على حد سواء. (الجميلي، ٢٠٢٤، صفحة ١١٢)

ثانيا:خصائص الفضاء السيبراني

الفضاء السيبراني هو بيئة رقمية افتراضية أُنشئت بواسطة الإنسان، تعتمد بشكل أساسي على شبكات الإنترنت وأنظمة الحاسوب، وتضم كمًا هائلًا من البيانات والمعلومات والأجهزة المترابطة. يُنظر إليه اليوم كأداة استراتيجية حديثة يمكن أن تكون بمثابة الذراع الفاعل للجيوش، ويعتبره بعض الخبراء البُعد الأكثر تأثيرًا في الحروب المعاصرة، مما جعله عاملًا مهمًا في صياغة التوازنات الدولية.

سهولة الوصول إلى الفضاء السيبراني وانخفاض تكاليف استخدامه زاد من إمكانيته على التأثير في المجالات السياسية والاقتصادية والعسكرية. فالجهة التي تمتلك وسائل السيطرة على هذا الفضاء تستطيع توجيه سلوك الآخرين بما يخدم أهدافها بشكل أكثر فعالية.

ما يميز الفضاء السيبراني عن الفضاء التقليدي هو طبيعته الافتراضية وخصائصه الفريدة، إذ أصبح ساحة جديدة للصراعات، حيث تتخذ الحروب السيبرانية أشكالاً مشابهة للحروب التقليدية، لكنها تجري ضمن شبكات الاتصال والمعلومات، متجاوزة الحدود الجغرافية والسيادية للدول. ومع أن الحروب الواقعية تستخدم جميع أنواع الأسلحة المتاحة، إلا أن الفضاء السيبراني أصبح أحد الميادين الرئيسية التي تُوظف فيها هذه الأسلحة بطرق مبتكرة.

بالتالي، يمكن تلخيص الخصائص الأساسية للفضاء السيبراني والحروب المرتبطة به في عدة نقاط تحدد طبيعته الاستراتيجية وتأثيره على الصعيد الدولي (جيجان و فاضل، ٢٠٢٤، صفحة ٣٣١)

١- الحرية : يوفر الفضاء السيبراني مساحة واسعة للتواصل وبناء شبكات افتراضية دون رقابة صارمة، مما يتيح للأفراد والجماعات التأثير في القضايا السياسية والاجتماعية، ويُمكّن الجماعات الإرهابية من التخطيط والتنسيق بسهولة، متجاوزة الحدود الجغرافية والقيود التقليدية، مع إمكانية استهداف أهداف مدنية وعسكرية على حد سواء.

٢- الطابع الاخياري للمشاركة :المشاركة في الفضاء السيبراني اختيارية بالكامل، ما يجعله مجالًا مفتوحًا للصراعات بين الدول والجماعات، ويتيح تنفيذ الأهداف بدقة وكفاءة منخفضة التكلفة مقارنة بالحروب التقليدية.

٣- تعقيد اليات الردع: اختلاف الدول في تعريف الأمن السيبراني يزيد تعقيد الردع، فبينما تركز الولايات المتحدة على الشبكات والتقنيات، ترى روسيا والصين أن المعلومات نفسها جزء من الأمن. هذا التباين يجعل من الصعب صياغة استراتيجيات موحدة للردع، رغم وجود اتفاقيات دولية مثل اتفاقية الجريمة السيبرانية ٢٠٠١، التي لم تنضم إليها بعض القوى الكبرى.

٤- إخفاء الهوية: الهجمات السيبرانية غالبًا ما تكون مجهولة المصدر، ما يصعب تحديد الجهة المهاجمة أو مساءلتها قانونيًا. برامج مثل "ستاكس نت" تُظهر كيف يمكن للجهات المهاجمة إخفاء آثارها تمامًا، مما يجعل التفريق بين هجمات الدول والجماعات الإجرامية تحديًا مستمرًا (خلف، ٢٠٢٣، الصفحات ٣١٨-٣٢٠)

ثالثا: الأبعاد الجيوبوليتيكية للأمن السيبراني

يُعدّ الأمن السيبراني في الوقت الحاضر امتداداً طبيعياً للفكر الجيوبوليتيكي المعاصر، إذ غدت السيطرة على تدفق المعلومات وإدارتها من أهم أدوات النفوذ والقوة في العلاقات الدولية. ويمكن تحديد أبرز أبعاده على النحو الآتي:

١-البعد الجغرافي – التقني: يتعلق بالبنية التحتية للاتصالات وشبكات الربط الدولي عبر الكابلات البحرية والأقمار الصناعية، وهي التي تحدد موقع الدولة ومكانتها ضمن "الخريطة الرقمية العالمية

٢-البعد السياسي – الأمني: أصبح الفضاء السيبراني ميداناً جديداً للصراع بين الدول، تُستخدم فيه الهجمات الإلكترونية وسيلةً للضغط والتأثير وتحقيق المكاسب الجيوسياسية عد الفضاء السيبراني ساحة جديدة للصراعات بين الدول، لكن القوانين الدولية ما زالت عاجزة عن مواكبة طبيعته المعقدة. فالهجوم السيبراني يُعتبر "عملاً مسلحًا" فقط إذا تسبب بأضرار مادية أو بشرية كبيرة، مثل تعطيل منشآت حيوية. كما يواجه تطبيق مبادئ القانون الدولي الإنساني مثل التناسب والتمييز صعوبة، لأن الشبكات المدنية والعسكرية غالبًا مترابطة، مما يجعل تجنب الأضرار الجانبية أمرًا معقدًا وتبرز مشكلة المساءلة في صعوبة تحديد الجهة المسؤولة عن الهجوم، إذ يستخدم المهاجمون وسطاء وتقنيات إخفاء الهوية. وقد حاول دليل تالين ٢.٠ وضع مبادئ لتحميل الدول المسؤولية عن الهجمات التي تنفذها أو تدعمها، لكنه يبقى غير ملزم قانونيًا. لذا، يعتمد التعامل مع هذه القضايا على التعاون الدولي في التحقيقات، ورفع الشكاوى إلى الأمم المتحدة أو محكمة العدل الدولية عند توفر الأدلة الكافية

٣-البعد الاقتصادي – التنموي: يعتمد الاقتصاد الرقمي المعاصر على أمن البيانات والمعاملات الإلكترونية، وأي خلل في منظومة الحماية السيبرانية يشكل تهديداً مباشراً للاستقرار والنمو الاقتصادي وان هجمات السيبرانية تمثل تهديدًا كبيرًا للعراق، فهي تتسبب بخسائر مالية مباشرة وغير مباشرة تؤثر على الثقة والاستثمار، حيث تشمل التكاليف توقف العمل ودفع الفدية وفقدان السمعة والعملاء. قد تخسر الشركات الكبيرة ملايين الدولارات، بينما تصل خسائر الشركات الصغيرة لعشرات الآلاف. وتعاني القطاعات الحيوية مثل التجارة الإلكترونية والنفط والصناعة من ضعف الجاهزية أمام هذه التهديدات

٤. البعد الاجتماعي – الثقافي: أعدّ الفضاء السيبراني في العراق أحد أبرز مظاهر التحول الاجتماعي والثقافي في العصر الرقمي، إذ أسهم في توسيع العلاقات والتواصل، ونشر الوعي المدني والسياسي، وتعزيز حرية التعبير، كما ساعد على تطوير التعليم الإلكتروني والإبداع الرقمي. وفي المقابل، أدى إلى تحديات اجتماعية وأمنية مثل ضعف الخصوصية، والابتزاز الإلكتروني، وتبدّل القيم الاجتماعية. ومن ثمّ، تبرز الحاجة إلى تعزيز الوعي الرقمي وسنّ تشريعات سيبرانية فعّالة لحماية المستخدمين وضمان توظيف الفضاء السيبراني في خدمة التنمية والتطور الثقافي في العراق (الزهراني، ٢٠١٩، صفحة ٧٤٠)

رابعا:القدرات السيبرانية وتأثيرها في طبيعة الصراعات والتهديدات الأمنية

أحدث الفضاء السيبراني تحولاً جذرياً في مفهوم الصراع الأمني، إذ ألغى الحواجز التقليدية للزمان والمكان، وخلق بيئة افتراضية جديدة للتفاعلات الداخلية والدولية. ومع هذا التحول، ظهرت أنماط غير تقليدية من الصراعات تعتمد على أدوات رقمية وأساليب هجومية غير مألوفة، ما جعل القدرات السيبرانية أحد أبرز عناصر القوة الحديثة.

برز اهتمام الدول والفاعلين من غير الدول بالفضاء السيبراني باعتباره ساحة استراتيجية لتحقيق النفوذ والهيمنة، لعدة أسباب رئيسية:

١. فضاء صراع منخفض التكلفة: يتميز الفضاء السيبراني بكونه ساحة افتراضية تتجاوز حدود الصراعات التقليدية، حيث يمكن تحقيق أهداف استراتيجية عبر وسائل رقمية بتكاليف محدودة مقارنة بالحروب العسكرية، مع دقة عالية في استهداف الخصوم.

٢. تصاعد الاعتماد على التكنولوجيا: أصبحت البنى التحتية الحيوية للدول، مثل شبكات الطاقة والمياه والاتصالات والمصارف، مترابطة بشكل وثيق مع الأنظمة الرقمية، مما جعلها عرضة للهجمات السيبرانية التي يمكن أن تشل مؤسسات الدولة الحيوية وتؤثر في أمنها الاقتصادي والاجتماعي.

٣. تلاشي الحدود الجغرافية: أدى الاستخدام الواسع للتكنولوجيا من قبل الأفراد والجماعات والدول إلى توسع الفضاء السيبراني بحيث تجاوز الحدود السياسية، فبات التأثير متبادلاً بين الداخل والخارج، وشمل شبكات التواصل الاجتماعي، والهواتف الذكية، والمنصات المالية والتجارية.

لقد أصبح الفضاء السيبراني اليوم عنصراً فاعلاً في صياغة ديناميات العلاقات الدولية، إذ لم يقتصر دوره على إحداث تحولات في البنى التحتية للدول، بل امتد ليؤثر في طبيعة النظام الدولي ذاته، من خلال إعادة تشكيل مفاهيم القوة والسيادة والأمن. ومع تزايد التطور التكنولوجي، تعاظمت المخاطر الأمنية الرقمية، مما جعل أمن الفضاء السيبراني قضية مركزية على الأجندة الأمنية العالمية (ربيع، ٢٠٢١، الصفحات ٤١٥٧–٤١٧٩)

خامسا:أنماط الحروب السيبرانية في العالم

١–الحرب الباردة الإلكترونية والصراع منخفض الحدة

يُعَدّ هذا النمط من الصراعات أحد أبرز سمات البيئة الرقمية الحديثة، إذ يجسد شكلاً مستمرًا وطويل الأمد من المواجهة ذات الطابع غير العسكري المباشر، حيث تتخذ الصراعات فيه أشكالاً غير تقليدية تركز على المجالات الثقافية والاقتصادية والاجتماعية والفكرية. ويتميز هذا النوع من الحروب بطابعها المعقّد والمتداخل، إذ تدور رحاها في فضاء مفتوح لا يعرف حدودًا زمنية أو مكانية واضحة، مما يجعلها صراعًا دائمًا يتجدد بتغير أدواته وأساليبه.

تُعرف هذه الظاهرة اصطلاحًا بـ"الحرب الباردة الإلكترونية"، وهي تقوم على استخدام أدوات غير عنيفة في تحقيق الأهداف الاستراتيجية، مثل التجسس الإلكتروني، والاختراقات الشبكية، وحروب المعلومات، وحملات التأثير النفسي، وحرب الأفكار، دون الحاجة إلى اللجوء إلى القوة المسلحة أو شن هجمات إلكترونية شاملة.

إن هذا النمط من الصراعات يُعبّر عن مرحلة جديدة من المواجهات بين الدول والفاعلين غير الدوليين، حيث تُدار المعارك بأساليب رقمية وإعلامية تهدف إلى تقويض الخصم من الداخل، وإضعاف استقراره السياسي والاجتماعي دون تكاليف مادية كبيرة. وتُعد هذه الحروب امتدادًا للصراعات التقليدية ذات الجذور التاريخية، مثل النزاع العربي–الإسرائيلي، والتوتر بين الهند وباكستان، أو بين الكوريتين، لكنها في صيغتها الحديثة اتخذت طابعًا إلكترونيًا يقوم على السيطرة على المعلومة، وتوجيه الرأي العام، وزعزعة الثقة بالمؤسسات

٢– الحرب الإلكترونية متوسطة الحدة

يُعدّ هذا النمط من الصراعات السيبرانية مرحلة وسطى بين الحرب الباردة الرقمية والهجوم الإلكتروني الشامل، إذ يمثّل مستوى من التصعيد يتجاوز العمليات الرمزية أو التجسسية، دون أن يبلغ حدّ المواجهة العسكرية الكاملة. وتدور أحداث هذا النوع من الحروب داخل الفضاء الإلكتروني بالتوازي مع النزاعات التقليدية، حيث يُستخدم كجبهة مساندة أو تمهيدية للعمل العسكري الميداني

تعتمد هذه الحروب على اختراق الشبكات الإلكترونية، وتعطيل أنظمة الاتصالات، واستهداف البنى التحتية الرقمية الحساسة، وشن حملات نفسية رقمية تهدف إلى إرباك الخصم وشلّ قدراته التنظيمية. وتمتاز الحرب

الإلكترونية متوسطة الشدة بانخفاض تكلفتها مقارنة بالحروب التقليدية، إذ يمكن تنفيذ عمليات مؤثرة عبر الإنترنت بتكلفة ضئيلة لا تتجاوز جزءًا بسيطًا من نفقات آلة الحرب الميدانية، فضلاً عن سرعتها العالية في التنفيذ والانتشار

لقد أثبت التاريخ الحديث أنّ هذا النمط من الحروب أصبح جزءًا لا يتجزأ من النزاعات المعاصرة، حيث جرى توظيفه إلى جانب العمليات العسكرية في عدد من المواجهات، من أبرزها حرب الناتو ضد يوغسلافيا عام ١٩٩٩، والنزاع الروسي–الجورجي عام ٢٠٠٨، والحروب المتكررة بين إسرائيل وحزب الله (٢٠٠٦)، وكذلك بين إسرائيل وحركة حماس (٢٠٠٩ و٢٠١٢). ففي هذه الحالات، لم يقتصر الصراع على الميدان العسكري، بل امتد إلى الفضاء الرقمي لتعطيل شبكات القيادة والسيطرة، وبثّ الدعاية، والتأثير في المعنويات

وبذلك، تمثّل الحرب الإلكترونية متوسطة الشدة أحد أشكال الحروب المركّبة الحديثة التي توظّف التكنولوجيا كسلاح داعم للهيمنة والسيطرة، وتعيد تعريف مفاهيم الردع والسيادة في العصر الرقمي

٣–الحرب الإلكترونية "الساخنة" والصراع مرتفع الشدة

يمثل هذا النمط المرحلة الأكثر تطورًا في مسار الحروب السيبرانية، إذ يدمج القدرات التكنولوجية المتقدمة بالعمليات العسكرية، ليشكّل ساحة صراع مكتملة الأركان تُدار فيها المواجهة عبر أدوات رقمية خالصة أو داعمة للعمل العسكري التقليدي. ورغم أن العالم لم يشهد بعد حربًا إلكترونية خالصة تُدار بمعزل عن القتال الميداني، فإن الاتجاهات الحالية تشير إلى إمكانية تحقق ذلك في المستقبل القريب مع تصاعد الاعتماد على الأنظمة الذكية في إدارة الصراعات.

تقوم هذه الحروب على استخدام الأسلحة الرقمية والهجمات السيبرانية الهجومية التي تستهدف البنية التحتية الحيوية للخصم، بما في ذلك شبكات الاتصالات والطاقة والمياه والمصارف والأنظمة العسكرية. وتُعدّ الطائرات المسيّرة والروبوتات القتالية ومنظومات الذكاء الاصطناعي أدوات رئيسة في هذا النمط من الصراع، إذ تُدار العمليات عن بُعد بدقة عالية وبكلفة أقل مقارنة بالحروب التقليدية.

ويُنظر إلى هذا النمط بوصفه تمهيدًا لحروب المستقبل، التي تعتمد على تحقيق الهيمنة الإلكترونية قبل أو أثناء النزاع، عبر ضرب الأنظمة التقنية الحساسة وشلّ مراكز القيادة والتحكم. ويُستخدم الفضاء السيبراني في هذا السياق لإجراء محاكاة وتدريبات متقدمة على توجيه الضربات الاستباقية وتعطيل قدرات العدو التقنية.

ومن أبرز الأمثلة التاريخية التي تجسّد هذا النمط، الهجوم بفيروس "ستاكس نت" عام ٢٠١٠، الذي استُخدم لتعطيل البرنامج النووي الإيراني في عملية مشتركة بين الولايات المتحدة وإسرائيل، ما كشف عن انتقال الصراع من المجال الافتراضي إلى واقع يمكنه إحداث تأثيرات مادية ملموسة، وبيّن أن السيطرة على الفضاء الإلكتروني قد تُصبح في المستقبل ركيزة أساسية لتفوق الدول في ميادين الحرب (عبد الصادق، ٢٠١١، صفحة ١٧)

الفصل الثاني :

أولا: العراق نموذجا

يعد العراق من الدول التي تواجه تحديات كبيرة في مجال الفضاء السيبراني، لاسيما على الصعيد الأمني، حيث يفاقم ضعف البنية التحتية وعدم الاستقرار العام من صعوبة التعامل مع هذه المخاطر. ومع الانتقال السريع للمجتمع من الواقع المادي إلى الفضاء الافتراضي، وجد العراق نفسه منخرطًا في هذا العالم الديناميكي دون مرحلة انتقالية مدروسة، ما كشف عن محدودية قدراته في التعامل مع التهديدات الرقمية.

تُظهر هذه الحالة الحاجة الماسة لتعزيز القدرات التقنية والقوانين المنظمة، وتطوير الموارد البشرية والإدارية، لتتمكن الدولة من مواجهة المخاطر السيبرانية بفاعلية. ومن ثم، يصبح من الضروري وضع استراتيجيات شاملة تعزز الأمن السيبراني وتحمي المعلومات الوطنية من الهجمات والتهديدات المستقبلية. (خرسان، ٢٠٢٣، صفحة ٢٣)

ثانيا:: البعد الجيوبوليتيكي للأمن السيبراني في العراق

مع تزايد إدراك الحكومات لأهمية تبنّي نهج شامل لمواجهة الهجمات السيبرانية، اتجهت الدول إلى وضع سياسات وإجراءات تعزز الأمن السيبراني بوصفه جزءاً أساسياً من منظومة الأمن الوطني. ونظراً لكون الفضاء السيبراني يضم نشاطات الأفراد والمؤسسات على حد سواء، فقد أصبح من الضروري سنّ تشريعات قانونية تنظم التعاملات الإلكترونية وتحميها من الجرائم السيبرانية، مع مراعاة مواكبة التطورات التكنولوجية الحديثة، مثل الذكاء الاصطناعي. ولهذا أصدرت العديد من الدول قوانين خاصة بأمن المعلومات وتجريم الأفعال الإلكترونية الإجرامية

وتُعنى استراتيجية الأمن السيبراني بجميع التدابير المتعلقة بسرية المعلومات والبيانات ومعالجتها وتخزينها وتداولها عبر الوسائل الإلكترونية، بما يضمن حمايتها من التهديدات الداخلية والخارجية. ومن أبرز أولويات هذه الاستراتيجية ما يأتي:

١-حماية خصوصية الأفراد والحفاظ على بياناتهم

٢-تأمين الخدمات الرقمية المقدَّمة للمواطنين

٣-تعزيز مرونة استخدام الأنظمة والخدمات في مواجهة التهديدات السيبرانية

٤-حماية البنى التحتية الحيوية للجهات الحكومية

٥-تنسيق الاستجابة السريعة عند وقوع الهجمات السيبرانية

٦-ضمان استمرارية تقديم الخدمات أثناء الأزمات وبعدها

وقد أطلقت العراق استراتيجية الأمن السيبراني (٢٠٢٢–٢٠٢٥) انطلاقاً من مبدأ أساسي يتمثل في حماية أمن الدولة ووجودها في الفضاء الرقمي، وتأمين بنيتها التحتية للمعلومات، وبناء مجتمع إلكتروني موثوق وآمن. وتقوم هذه الاستراتيجية على مجموعة من الإجراءات الرامية إلى حماية الفضاء السيبراني العراقي والدفاع عنه

وكشفت تقارير لشركات أمنية متخصصة عام ٢٠١٤م عن اندلاع حرب سيبرانية في العراق، استخدمت فيها وسائل التواصل الاجتماعي لأغراض دعائية وتحشيد جماهيري لصالح الجماعات الإرهابية، إضافة إلى تنفيذ عمليات تجسس إلكتروني من خلال قراصنة يقومون بإرسال رسائل وبرامج خبيثة لاختراق الأجهزة وسرقة البيانات أو مراقبة الأفراد عبر الكاميرا والميكروفون. وتُعد هذه الهجمات مثالاً على امتداد الحروب السيبرانية إلى الميادين المدنية والعسكرية على حد سواء.

وقد دفع هذا الواقع العديد من الدول، ومن بينها العراق، إلى تشكيل هيئات وطنية للأمن السيبراني تتولى إعداد وتنفيذ الاستراتيجية الوطنية، ووضع السياسات والحوكمة والإرشادات الخاصة بالأمن السيبراني، إلى جانب إدارة المخاطر، والاستجابة للحوادث، ووضع معايير التشفير الوطنية، ورفع مستوى الوعي المجتمعي في هذا المجال

وتشير مجمل التفاعلات الجيوبوليتيكية للأمن السيبراني في العراق إلى وجود خيارين رئيسين أمام الدولة

الخيار الأول: المضي في تطوير قدراتها التقنية الوطنية في مجال الأمن السيبراني بشكل مستقل أو من خلال التحالفات الإقليمية والدولية، بما يحقق توازناً أمنياً رقمياً

الخيار الثاني: الاعتماد على الدول الأقوى تقنياً في مواجهة التهديدات السيبرانية، وما يترتب عليه من تبعية أمنية في المجال الرقمي

وبذلك يمكن القول إن العراق يتجه نحو بناء منظومة تعاون إقليمي ودولي لمواجهة التهديدات السيبرانية، عبر تحالفات تشكل نواة لأمن سيبراني مشترك، يعزز قدراته الوطنية ويحافظ على استقراره وأمنه المعلوماتي في بيئة دولية متشابكة ومتغيرة

وفي هذا السياق، سعت الجهات المعنية إلى وضع تدابير وإجراءات عملية لمعالجة الفجوة في الأمن السيبراني والتقليل من مواطن الضعف الأساسية فيه. وقد تولى الفريق المختص بهذه المهمة تشكيل عدد من الفرق الفرعية تعمل بصورة مستقلة ومنسقة في الوقت ذاته، لضمان تحقيق أهداف الاستراتيجية الوطنية للأمن السيبراني العراقية بكفاءة وضمن إطارٍ زمني محدد

واعتمد هذا التنظيم على ثمانية محاور رئيسة تتماشى مع المعايير العالمية المعتمدة من قبل الاتحاد الدولي للاتصالات، وتهدف جميعها إلى الارتقاء بمكانة العراق في المؤشر العالمي للأمن السيبراني، وهي على

النحو
الآتي
١-الحكومة الفاعلة: تفعيل منظومة الحكومة الإلكترونية بما يحقق سهولة الخدمات ويُعزّز راحة المواطنين
٢-الإطار التشريعي والتنظيمي: تطوير القدرات القانونية والتشريعية للجهات الوطنية المعنية بإنفاذ القوانين السيبرانية
٣-الإطار التكنولوجي للأمن السيبراني: تحديد المتطلبات الفنية اللازمة لضمان السيطرة والحماية الفعالة على الفضاء السيبراني العراقي
٤-تعزيز ثقافة الأمن السيبراني وبناء القدرات: وضع آليات لنشر الوعي والمعرفة بالأمن السيبراني على المستوى الوطني وتطوير مهارات الكوادر المتخصصة
٥-تطوير الاعتماد على الذات: دعم البحث العلمي وتأسيس مجتمع وطني متخصص في دراسات وتطبيقات الأمن السيبراني
٦-الامتثال والتنفيذ: إعداد أطر ومعايير وطنية لتقييم وإدارة مخاطر الأمن السيبراني وضمان الالتزام بها
٧-الجاهزية لحماية الأمن السيبراني: إنشاء آليات فعّالة للإبلاغ والاستجابة السريعة للحوادث والاختراقات السيبرانية
٨-التعاون الدولي: تعزيز التواصل مع الاتحاد الدولي للاتصالات وبناء شراكات مع فرق الاستجابة الإلكترونية الدولية من أجل تبادل الخبرات والتنسيق المشترك
وبذلك تسعى هذه الجهود إلى تحقيق منظومة أمن سيبراني وطنية متكاملة تسهم في حماية البنية الرقمية للعراق وتدعم موقعه ضمن النظام السيبراني العالمي

يعدُّ مؤشر الأمن السيبراني العالمي أداة معيارية موثوقة تقيس مستوى التزام الدول بمعايير الأمن الرقمي عبر العالم، ويهدف إلى رفع الوعي بأهمية الأمن السيبراني وأبعاده المتعددة. يغطي الأمن السيبراني نطاقًا واسعًا من التطبيقات والقطاعات، لذا يُستخدم المؤشر لتصنيف البلدان من حيث جاهزيتها وقدرتها على مواجهة الهجمات الإلكترونية. يقيس المؤشر مستوى التنمية والمشاركة الوطنية عبر خمسة ركائز رئيسية: الإجراءات القانونية، والإجراءات التقنية، والإجراءات التنظيمية، وبناء القدرات، والتعاون الدولي؛ ثم تُجمَع هذه المؤشرات في نتيجة إجمالية تعكس نجاح الدولة في مواجهة التحديات السيبرانية
ومن أولويات التصدي لهذه التهديدات تعزيز الوعي بالمخاطر السيبرانية، وتشجيع استخدام أجهزة وتقنيات وخدمات موثوقة عالميًا، واتخاذ تدابير وطنية متسقة داخل إطار دولي مشترك. كما يتطلب ذلك الاستعداد

الدائم للتعامل مع جرائم المعلوماتية عبر عقود الاتفاقيات والبروتوكولات الدولية، ووضع استراتيجيات وطنية واضحة تُعلي مصلحة الأمن الوطني والدولي وتدفع نحو تكامل أمني عالمي

وتعتمد قدرة الدولة على حماية بنيتها التحتية الحيوية من الهجمات السيبرانية بصورة أساسية على توافر قوة عاملة مُتعلمة ومتخصّصة وماهرة في إدارة الشبكات والأنظمة. وينشأ ذلك من نظام تعليمي قادر على بناء هيكل مؤسسي يواكب التطورات السريعة في المجال، ويجهِّز كوادر ذات كفاءة لاكتشاف الهجمات والتعامل معها ومعالجتها. يمكن الاستفادة من الأدبيات الدولية والتجارب والارشادات الاستراتيجية في تطوير هذه الطاقات الوطنية.

لذلك تَحمَل المؤسسات التعليمية دورًا محوريًا في تزويد الطلاب بالمعارف والمهارات المناسبة؛ ومن هنا تظهر الحاجة الملحّة لوضع استراتيجية وطنية لتعليم الأمن السيبراني. كما يمكن للحكومة والأوساط الأكاديمية التعاون لمعالجة المتطلبات التعليمية، وتعزيز مبادرات تدريب المعلمين، وتطوير برامج أكاديمية متخصصة. ينبغي أيضًا غرس الوعي الأمني لدى الطلبة عبر المقررات الجامعية، وإنشاء مكتبات ومراكز متخصصة، وتعزيز عقد المؤتمرات وورش العمل لرفع الخبرات الوطنية

تلجأ بعض الحكومات كذلك إلى توظيف مجموعات من القراصنة المدنيين من القطاع الخاص —سواء كانوا مختصين تقنيًا قانونيًا أو قراصنة سابقين أعيد تأهيلهم— للاستعانة بمهاراتهم في حالات الحاجة، كما قد تستعين دولٌ بوكالات وخبراء خارجيين للعمل بالنيابة عنها. هذه الممارسات تعكس تحول استراتيجيات الرد إلى منهجية أكثر استباقية في حرب المعلومات

ومقابل ذلك، ظهر سوق لشركات متخصصة تقدم خدمات هجومية أو برمجيات متقدمة تُستخدم كـ«أسلحة إلكترونية» للدفاع أو لشن هجمات مدفوعة. ومع اتساع رقعة الصراع السيبراني، يتطلع فاعلون متنوّعون— من جماعات الجريمة المنظمة إلى «جيوش إلكترونية» وجماعات إرهابية—إلى توسيع قدراتهم الهجومية لتحقيق تأثيرات بعيدة المدى، سواء بسرقة أموال أو معلومات أو تعطيل خصوم

وبالنظر إلى المستقبل، يمكن تَخيُّل ثلاثة سيناريوهات محتملة لمسار الأمن السيبراني العالمي

١–أن يتحوّل الفضاء الإلكتروني إلى بيئة أكثر مرونة ومناعة، ما يجعل شن هجمات واسعة النطاق أمراً صعباً للغاية

٢–أن تتفوّق تقنيات الدفاع والحلول المعلوماتية لصالح المدافعين، فتقل قدرة المهاجمين على الإضرار

٣–أن يتفاقم انعدام المساءلة، فيزداد نشاط المهاجمين السيبرانيين ويعملون بحرية تامة بعيداً عن العقاب

هذه السيناريوهات تُظهر أن مستقبل الأمن السيبراني سيعتمد بدرجة كبيرة على موازين القوة التقنية، وكفاءة التعليم والتدريب، وفعالية الأطر التشريعية والتنظيمية، ومدى التعاون الدولي في مواجهة تهديدات تتجاوز الحدود الوطنية

(صليبي، ٢٠٢٤، الصفحات ٥١٦-٥٢٠)

الاستناجات

١-تشير السيبرانية إلى كل ما يتعلق باستخدام الحاسوب والتقنيات الرقمية المتصلة بشبكة الإنترنت العالمية، وما ينشأ عنها من أنشطة وتفاعلات في الفضاء الإلكتروني.

٢-أما الهجمات السيبرانية فهي تمثل عمليات اختراق أو اعتداء على الحدود غير المرئية للدولة في فضائها الإلكتروني، يقوم بها طرف خارجي أو داخلي بهدف الوصول غير المشروع إلى المعلومات أو الوثائق الحساسة، سواء كانت ذات طبيعة أمنية أو مالية أو مصرفية أو إعلامية بمختلف أشكالها

٣-على الرغم من تعرّض العديد من الدول لهجمات سيبرانية متكررة، إلا أنها غالبًا ما تمتنع عن الإعلان الرسمي عنها، وذلك حفاظًا على هيبتها وسيادتها، وتجنبًا لإظهارها بمظهر الدولة الضعيفة أو العاجزة عن حماية فضائها الإلكتروني

٤-مع التطور المتسارع في تقنيات المعلومات والاتصالات، أنشأت معظم الدول وحدات وأجهزة متخصصة لمواجهة الهجمات السيبرانية، وتعزيز قدراتها على الردع والدفاع، بهدف حماية أنظمتها الرقمية من الاختراق، سواء كانت تلك الأنظمة إعلامية أو مالية أو أمنية أو عسكرية.

٥-ويُنظر اليوم إلى الأمن السيبراني بوصفه شكلاً من أشكال الحدود السيادية للدولة، لما يمثله من خط دفاع استراتيجي يحافظ على خصوصيتها ويحمي أمنها القومي من التهديدات الرقمية

التوصيات

١-تنفيذ برامج توعوية شاملة تستهدف المجتمع لرفع الوعي بأهمية الأمن السيبراني، وتثقيف الأفراد حول سبل حماية بياناتهم ومعلوماتهم الشخصية على الإنترنت

٢-تعزيز حماية البنية التحتية الحيوية عبر تطوير أنظمة الأمان الرقمية، وتبني آليات فعّالة للمراقبة والتقييم المستمر للأداء السيبراني

٣-ضرورة تحديث التشريعات والقوانين بصورة منتظمة لمواكبة التطور المتسارع في مجال التكنولوجيا والتصدي لأشكال الهجمات السيبرانية المستجدة

٤-على الجهات المعنية رفع كفاءتها في مجال التحقيقات الإلكترونية من خلال تأهيل كوادر متخصصة، واستخدام أدوات وتقنيات متقدمة لتحديد مصادر التهديد وملاحقة مرتكبي الجرائم السيبرانية

المصادر :

١–اسراء شريف جيجان، و صفا عباس فاضل. (٢٠٢٤). تأثير الفضاء السيبراني على الحروب الحديثة . *مجلة دراسات تربوية ، العدد(٦٥) ، وزارة التربية العراقية* ، ٣٣١.

٢-باسم علي خرسان. (٢٠٢٣). الامن في الفضاء السيبراني :دراسة في التهديدات واستراتيجية المواجهة . *مجلة كلية التراث الجامعة ، المجلد(١) ، العدد(٣٦)*، ٢٣.

٣-رعد خضير صليبي. (٢٠٢٤). تعزيز الامن السيبراني في العراق : التحديات والفرص . *مجلة دراسات دولية ، العدد٩٩* .

٤-شريفة كلاع. (٢٠٢٢). الامن السيبراني وتحديات الجوسسة والاختراقات الالكترونية للدولة عبر الفضاء السيبراني. *مجلة الحقوق والعلوم الانسانية ، جامعة زيان عشور الجلفة*، ٢٩٤.

٥-شيخة حسين الزهراني. (٢٠١٩). التعاون الدولي في مواجهة الهجوم السيبراني. *مجلة جامعة الشارقة للعلوم القانونية ، كلية القانون، جامعة الشارقة ، المجلد (١٧)، العدد(١)*.

٦-صدام مرير حمد الجميلي. (٢٠٢٤). الحروب الهجينة واثرها في مستقبل الصراع العالمي . *مجلة تكريت للعلوم السياسية ، المجلد (١) ، العدد(٣٤)*،.

٧-عادل عبد الصادق. (٢٠١١). *انماط الحرب السيبرانية وتداعيتاتها على الامن العالمي السياسية الدولية*. قاهرة.

٨-كريم زيدان خلف. (٢٠٢٣). تأثير الفضاء السيبراني على مبدأ سيادة احكام القانون في اطار القانون الدستوري . *مجلة كلية القانون للعلوم القانونية والسياسية ، المجلد(١٣)، العدد(٥٠)*،

٩-محمد صلاح عبد ربيع. (٢٠٢١). الهجمات السيبرانية بين مشروعيتها كوسيلة للدفاع الشرعي وادانتها كاعتداء غير مشروع . *مجلة الدراسات القانونية والاقتصادية ، العدد(٢)*.