مجلة كلية الآداب بقنا (دورية أكاديمية علمية محكمة)

الجيوبوليتيكا في زمن الفضاء السيبراني: بين الكلاسيكية والنقدية
رؤية معاصرة فى الجغرافية السياسية

د. عيسى السيد عيسى دسوقي

مدرس الجغرافيا السياسية

كلية الدراسات الآسيوية العليا – جامعة الزقازيق

د. حسن قطب حسن قطب

أستاذ الجغرافيا السياسية المساعد

كلية الآداب – جامعة أسيوط

DOI: 10.21608/qarts.2025.356882.2163

مجلة كلية الآداب بقنا – جامعة جنوب الوادي – المجلد (٣٤) العدد (٦٧) أبريل ٢٠٢٥

الترقيم الدولي الموحد للنسخة المطبوعة ISSN: 1110-614X

الترقيم الدولي الموحد للنسخة الإلكترونية ISSN: 1110-709X

موقع المجلة الإلكتروني: https://qarts.journals.ekb.eg

الجيوبوليتيكا في زمن الفضاء السيبراني: بين الكلاسيكية والنقدية رؤية معاصرة فى الجغرافية السياسية

الملخص:

يتناول البحث أثر الفضاء السيبراني على التحولات الجيوبوليتيكية المعاصرة، ودوره في إعادة تشكيل ديناميات القوة العالمية في عصر الرقمنة. ويستعرض موجز للتغيرات الدولية التي أعقبت الحرب الباردة، وكيفية تعامل الجيوبوليتيكا مع العولمة، وتعدد التدفقات التي تسهم في تشكيل الفضاء السيبراني. كما يناقش التحديات التي أفرزتها الثورة التقنية والمعلوماتية على المفاهيم التقليدية للسيادة والصراعات الدولية، متتبعًا تذبذب الفكر الجيوبوليتيكي بين المدرسة الكلاسيكية والنقدية.

كما يتناول البحث التداخل بين البنى التحتية المادية والمنطقية للفضاء السيبراني، وتأثير هذا التداخل على الأمن القومي. ويستعرض أمثلة عملية من الهجمات السيبرانية الكبرى، موضحاً من خلال هذه الأمثلة كيف تُعيد التكنولوجيا الرقمية تشكيل الجغرافيا السياسية للعالم، مما يُبرز الدور المتزايد للفضاء السيبراني كأداة استراتيجية في العلاقات الدولية.

تفتح الدراسة آفاقاً جديدة لفهم الصراعات في الفضاء السيبراني من منظور جيوبوليتيكي معاصر، وتعزز الحاجة إلى استراتيجيات دولية متكاملة للتعامل مع التحديات الناشئة عن هذا المجال. كما تسلط الضوء على أهمية تحقيق التوازن بين الأمن والحرية وحقوق الأفراد، مع دمج الفضاء السيبراني كعنصر أساسي في التحليل الجيوسياسي لفهم التحولات المعقدة التي يشهدها العالم. وتتناول الدراسة تداخل الأبعاد

المادية والافتراضية في تشكيل السياسات الدولية، بما يضمن تحقيق السيادة وتعزيز الأمن في مواجهة التحديات الرقمية المتزايدة.

خلص البحث إلى ضرورة تطوير نموذج تحليلي يجمع بين المنظورين الكلاسيكي والنقدي، لمعالجة التوترات القائمة بين الأبعاد المادية وغير المادية للقوة في الفضاء السيبراني، ويأخذ هذا النموذج بعين الاعتبار التحديات القانونية والأخلاقية والسياسية التي يفرضها هذا المجال الديناميكي.

الكلمات المفتاحية: الجيوبوليتيكا، الفضاء السيبراني، العولمة، الأمن السيبراني، السيادة الوطنية.

مقدمة:

أفضت التطورات السياسية والاقتصادية خلال العقود الثلاثة الماضية (١٩٩٥ – ٢٠٢٥م)، إلى تنظيم اجتماعي وسياسي جديد على جميع المستويات، تمثّل في الفضاء السيبراني. ولمواكبة هذه التحولات البارزة، كان على الجغرافيا السياسية إعادة التفكير وتوسيع مفاهيمها التقليدية. فتجاوزت الجغرافيا الأنجلو أمريكية مناهجها الراديكالية التي كانت تعد مسلّمات لفترة طويلة، وطورت مسارين مفاهيميَّين، كلاهما لا يزال وثيق الصلة بالجغرافيا السياسية المعاصرة (Reuber, 2000, p. 39):

- **الأول مسار عملي:** يتضمن زيادة الوعي بالمكان والتنوع الإقليمي والاختلافات، وما إلى ذلك في سياق الصراعات المتعلقة بالفضاء.
- **الآخر مسار بنائي:** يفكك الخطابات والسرديات والخرائط الجغرافية باعتبارها تمثيلات أو أدوات استراتيجية، يستخدمها السياسيون في السياسة الدولية وكذلك في الصراعات على المستوى المحلي والإقليمي.

هذان الجانبان لا يُعتبران نموذجين متنافسين، بل نهجين متكاملين يهدفان لفهم "العمليات التي تؤدي إلى التوزيع غير المتكافئ للسلطة على سطح الأرض"، ويتفاعلان بشكل متكامل في مشاريع البحث المختلفة.

ومع ظهور الفضاء السيبراني حدث تحوّل جذري في الجغرافيا السياسية. فقد غيّرت الثورة الرقمية طريقة تفاعل الأفراد والمجتمعات، وأساليب ممارسة القوى السياسية على المستوى العالمي. فأضاف الفضاء السيبراني بُعدًا جديدًا إلى الأبعاد التقليدية للجيوبوليتيكا، حيث أصبح الفضاء الافتراضي ساحة تتداخل فيها القوى السياسية والعسكرية والاقتصادية والثقافية، مما يفرض تحديات وفرصًا غير مسبوقة.

فلم تعد الجيوبوليتيكا تعني بالسيطرة على الأراضي فحسب، بل امتدت إلى السيطرة الرمزية والواقعية على الفضاء الرقمي. أصبح الإنترنت والشبكات الاجتماعية والأدوات الرقمية اليوم ساحات جديدة للصراعات الجيوبوليتيكية، حيث تُدار عبرها الحروب السيبرانية، وتُستخدم المعلومات كأداة للهيمنة والتأثير، وتتزايد الأنشطة الاقتصادية عبر الفضاء الرقمي، الذي بات عنصرًا أساسيًا في الديناميكيات الجيوبوليتيكية الحديثة، حيث تحولت الدول إلى "فضاءات سيبرانية" مفتوحة للتنافس والتفاعلات الدولية.

ومن هذا المنطلق، تتجلى الحاجة لدراسة هذه الظاهرة من خلال منظور جيوبوليتيكي جديد، يتجاوز الحدود التقليدية ويعترف بالأبعاد الرقمية. يهدف هذا المنظور إلى تحليل كيفية تأثير الفضاء السيبراني على القوة السياسية والعلاقات الدولية والسيادة الوطنية، بالإضافة إلى استكشاف دوره في صياغة السياسات الداخلية والخارجية للدول في عصر المعلومات الرقمية.

فرضيات الدراسة:

تتضمن فرضيات الدراسة مجموعة من الأسس والمبادئ التي تحدد إطار الدراسة وتحليلها. وفيما يلي عرض لهذه الفرضيات على النحو التالي:

- لم تسهم العولمة في تسريع حركة الأشخاص والمعلومات والسلع فحسب، لكنها أيضًا عززت انسيابية انتقال المخاطر عبر الحدود، ما أوجد تحديات جديدة تتعلق بالأمن، والبيئة، والمخاطر الاقتصادية والاجتماعية.
- على الرغم من نجاح الجيوبوليتيكا النقدية في تحليل وتفكيك الخطابات الجيوبوليتيكية نظرياً، إلا أنها لم تقدم بدائل عملية قوية في تعزيز السلام الدولي،

أو المساهمة بفعالية في تشكيل السياسات الدولية، أو معالجة القضايا الجغرافية الحرجة.

- على الرغم من الانتقادات الأكاديمية للجيوبوليتيكا الكلاسيكية، إلا أن أفكارها لا تزال تُستخدم على نطاق واسع في صياغة الاستراتيجيات الجيوسياسية المعاصرة، ومنها سياسات السيطرة على الفضاء السيبراني.
- أن الفصل بين "العالم الافتراضي" و"العالم الحقيقي" ليس مطلقًا؛ حيث يظل الموقع الجغرافي والمكان عاملين حاسمين في تشكيل تفاعلات الفضاء السيبراني، كما يتجلى بوضوح في توزيع مراكز البيانات والبنية التحتية للإنترنت، فهي متجذرة في الواقع الجغرافي. ومن ناحية أخرى، فإن التفاعلات في الفضاء السيبراني تؤثر بشكل كبير على هذا الواقع المادي، وذلك في سياقات متعددة تشمل الجوانب السياسية والعسكرية والاقتصادية والاجتماعية والثقافية.
- يفرض الفضاء السيبراني تحديات جديدة على مفهوم السيادة والهوية الوطنية، بسبب طبيعة الشبكات الرقمية العابرة للحدود الجغرافية، حيث يصعب على الدولة أحياناً فرض احترام قوانينها وأنظمتها، حتى على أراضيها من قبل مواطنيها، ولا سيما عندما تُوفَّر الخدمة المستخدمة من قِبَل شركات أجنبية عملاقة.
- الفضاء السيبراني أصبح جزءًا لا يتجزأ من الاستراتيجيات العسكرية الحديثة، حيث يشكل ساحة جديدة للتفاعلات والصراعات الجيوبوليتيكية، بجانب الفضاءات الجغرافية التقليدية (الأرض، والبحر، والجو، والفضاء الخارجي).
- يُعيد التقدم التكنولوجي تشكيل موازين القوى العالمية، من خلال تمكين بعض الدول من التفوق على الأخرى.

أهداف الدراسة:

تسعى الدراسة إلى تحقيق مجموعة من الأهداف المرتبطة بفهم الفضاء السيبراني وعلاقته بالجيوبوليتيكا، وذلك من خلال:

- استكشاف المخاطر الأمنية التي أوجدتها العولمة، خاصة في ظل توسع الفضاء السيبراني وتأثيره على الاستقرار القومي والدولي.
- تحليل أسس الجيوبوليتيكا النقدية، وتقييم قدرتها على تقديم تفسير أكثر شمولاً للتغيرات الدولية التي أعقبت الحرب الباردة مقارنة بالجيوبوليتيكا الكلاسيكية.
- تحليل تأثير مفهوم الفضاء السيبراني على النظريات الجغرافية التقليدية، مثل تلاشي الحدود وفقدان المسافات في ظل العولمة، وكيف يمكن تطوير مقاربات جديدة لفهم هذه الظواهر في الدراسات الجغرافية.
- دراسة السمات الجغرافية لهندسة الفضاء السيبراني، وتحليل دور الجهات الفاعلة ـ بما في ذلك الدول ذات السيادة ـ في تشكيل معالم الفضاء السيبراني.
- استعراض الأنشطة السيبرانية التي تشكل تهديدًا للسيادة الوطنية، مثل الهجمات الإلكترونية، والجرائم العابرة للحدود، والتأثيرات السلبية على الأمن الوطني.
- استكشاف كيف أصبح الفضاء السيبراني مجالًا للنفوذ الجيوبوليتيكي، وتقييم تأثيراته على العلاقات الدولية والأمن القومي.
- تحليل كيف أصبحت الحرب السيبرانية جزءًا لا يتجزأ من الاستراتيجيات العسكرية الحديثة، مع تسليط الضوء على بعض النظريات العسكرية حول العمليات السيبرانية الحاسمة.

- تقييم المخاطر المتزايدة المرتبطة بعسكرة الفضاء السيبراني وتأثيرها على الاستقرار العالمي، مع التركيز على الصراعات بين الدول في المجال السيبراني.

الدراسات السابقة:

تناولت دارسات عديدة الفضاء السيبراني من زوايا متعددة، من بينها ما ركّز على التحديات الجغرافية في ظل الفضاء السيبراني، مثل دراسة Sidaway (١٩٩٤)، الذي أشار إلى أن الفضاء السيبراني يُعيد تشكيل الجغرافيا السياسية دون إلغاء أهمية مفاهيم الدولة والحدود، لكنه يجعلها أكثر تعقيداً بفعل التدفقات العالمية.

كما ركزت دراسات مثل دراسة Robine and Salamatian (٢٠١٤)، ودراسة Gao وآخرين (٢٠١٩) على تعقيدات تمثيل الفضاء السيبراني جغرافياً. فهو يجمع بين البنى التحتية المادية (كالكابلات ومراكز البيانات) والتفاعلات الافتراضية، مما يتطلب أدوات تحليلية جديدة تربط الجغرافيا التقليدية بالمجال الرقمي. كما تُبرز دراسة Grandin(٢٠٢٣) تحديات إنتاج خرائط سيبرانية شاملة، نظراً للتداخل بين العناصر المادية وغير المادية.

وتعرضت دارسات أخرى للعلاقة بين الأمن السيبراني والجغرافيا السياسية، مثل دراسة تغريد المشهدي (٢٠١٩) وضحى لعيبي (٢٠٢١)، مؤكدين أن الأمن السيبراني لم يعد مجرد قضية تقنية، بل أصبح عنصراً استراتيجياً في الفضاء الجغرافي الدولي. يتجلى ذلك في التنافس بين القوى الكبرى مثل الولايات المتحدة والصين وروسيا، حيث تُستخدم القدرات السيبرانية كأدوات لتعزيز السيادة الرقمية ومواجهة التهديدات، سواء عبر هجمات على البنى التحتية (مثل إيران) أو التدخل في العمليات السياسية (مثل الانتخابات الأمريكية).

كما تطرقت دراسات أخرى إلى تحولات القوة الجيوسيبرانية، مثل دراسة عياد (٢٠٢٣) التي تناولت كيف أسهم الفضاء الجيوسيبراني في إعادة صياغة مفهوم القوة، خاصة في استراتيجيات روسيا والصين. فالقدرات السيبرانية أصبحت أداة لتوسيع النفوذ الدولي، سواء عبر الهجمات السيبرانية أو بناء بنى تحتية رقمية مستقلة. وأضافت دراسة حشاني و حكيمي (٢٠٢٤) بُعداً دبلوماسياً، حيث سلطت الضوء على "الدبلوماسية السيبرانية" كأداة جديدة للحوكمة والتنافس في الفضاء السيبراني، مما يعكس الحاجة إلى إطار دولي لتنظيم هذا المجال.

وانطلاقاً من الدراسات السابقة، تناول الباحثان في دراستهما التحولات الجيوبوليتيكية التي فرضها الفضاء السيبراني على العلاقات الدولية، خاصة في ظل العولمة والثورة الرقمية. وقد ناقشا كيف أعادت التكنولوجيا تشكيل مفاهيم تقليدية مثل السيادة والمكان والصراع، حيث أصبح الفضاء الرقمي ساحة جديدة للمنافسة بين الدول والجهات الفاعلة غير الحكومية. وتسعى الدراسة إلى تطوير نموذج تحليلي يجمع بين المنظورين الكلاسيكي والنقدي لفهم هذه التحولات، مع التركيز على البنية التحتية السيبرانية، والهجمات الرقمية الكبرى، وتفاعل القوى العالمية داخل هذا الفضاء. وتخلص إلى ضرورة بناء استراتيجيات دولية متكاملة، قادرة على التعامل مع التحديات المتزايدة التي تواجه مفاهيم السيادة والأمن والحرية، وذلك في ظل تراجع تأثير الحدود الجغرافية التقليدية، وبروز الفضاءات الافتراضية كساحات مؤثرة وفاعلة في صياغة السياسات العالمية وصراعات القوى الدولية.

منهجية الدراسة:

اعتمدت الدراسة على منهجية متكاملة تأخذ بعين الاعتبار الطبيعة متعددة الأبعاد للموضوع. وفيما يلي مقترح لمنهجية الدراسة:

المنهج التحليلي: والذي يعتمد أولاً على الوصف وجمع المعلومات والبيانات المتعلقة بالفضاء السيبراني، مع التركيز على التغيرات التي طرأت على المفاهيم الكلاسيكية والنقدية للجيوبوليتيكا. ويعتمد أيضاً على تحليل العلاقات بين القوى العالمية في السياق السيبراني، وكيفية تأثير التطورات التكنولوجية على توازن القوى التقليدي.

المدخل التاريخي: ويعني بدراسة تطور مفهوم الجيوبوليتيكا من الكلاسيكية إلى النقدية، وتطور مفهوم الفضاء السيبراني. كما يتناول تحليل الأحداث التاريخية التي تبرز العلاقة بين التكنولوجيا والصراعات الجيوبوليتيكية، مثل الهجمات السيبرانية الكبرى والتنافس الرقمي بين الدول.

المدخل البنيوي: تحليل بنية القوة في الفضاء السيبراني، بما في ذلك الفاعلين الرئيسيين (الدول، الشركات الكبرى، الفاعلون غير الحكوميين).

مدخل دراسة الحالة: اختيار حالات واقعية مثل الهجمات السيبرانية الكبرى، والصراعات الرقمية بين الدول، لتحليل تأثير الفضاء السيبراني في الواقع الجيوبوليتيكي، مع دراسة التنافس السيبراني بين القوى الدولية مثل الولايات المتحدة والصين وروسيا كنماذج.

يعالج البحث أربعة محاور رئيسة حول الفضاء السيبراني: النظام العالمي الجديد والجيوبوليتيكا، الجغرافيا السياسية للفضاء السيبراني، أثر الفضاء السيبراني على سيادة الدول، وتحليل الفضاء السيبراني من منظور الصراع الدولي.

المبحث الأول: النظام العالمي الجديد والجيوبوليتيكا

أيقظت نهاية الحرب الباردة ـ لفترة وجيزة ـ الأمل القديم في بناء مجتمع عالمي جديد يتسم بالديمقراطية، يكون أكثر حرية، وأقل عنفًا مقارنة بالعصور السابقة. وبدلاً من ذلك، شهد "النظام العالمي الجديد" تصاعد حدة النزاعات المسلحة، حيث اندلعت الحروب في البوسنة وكوسوفو والشيشان، وشهدت درجة حرجة من العنف كان يُعتقد أنه انتهى بعد الحرب العالمية الثانية. وكان لهذه الصراعات الجديدة بالتأكيد بعد جيوبوليتيكي محدد وواضح.

وشهدت مجتمعات ما بعد الحداثة ـ في الوقت ذاته ـ تحولات اجتماعية واقتصادية وسياسية بعيدة المدى على المستويين المحلي والإقليمي، وقد أسفرت التداعيات الاجتماعية والبيئية للحداثة عن التحول نحو ما يُعرف بـ"مجتمع المخاطر"، مما تسبب في عودة الشعور بعدم اليقين إلى المجتمع؛ بحيث أصبح القلق المتزايد بشأن التهديدات جزءًا من الحياة اليومية. ورغم توثيق الجوانب الإيجابية للعولمة، مثل تعزيز التنقل وتسريع حركة الأشخاص والمعلومات والسلع والخدمات، إلا أن هذه الديناميكيات ذاتها ساهمت في تسهيل انتشار المخاطر عبر الدول والقارات. حتى الدول المزدهرة كان عليها أن تواجه تطورات ومخاطر عديدة، منها: الأزمات المؤسسية والمالية، والمشكلات البيئية، وتحديات التحرر الاقتصادي، وزيادة مظاهر عدم المساواة الاجتماعية، وتقسيم السكان ـ وفق نمط الحياة ـ إلى مجتمع يحتفي بالتمييزات الطفيفة في الذوق والإهتمام (Mythen, 2015, pp. 44-45).

فأصبحت حالة ما بعد الحداثة جزءًا من اقتران الزمان والمكان، وهي المرحلة التي أطلق عليها "ديفيد هارفي David Harvey" عام ١٩٨٩ "ضغط المكان والزمان"، والتي باتت بمثابة آلية وسيطة بين القوى الهيكلية الأساسية للرأسمالية

والأشكال الثقافية الناتجة عن التحولات الفكرية في مختلف المجالات (Woodward & John, 2008, p. 132).

لم تترك هذه التطورات التنظيم المكاني للمجتمع بلا تغيير؛ لقد أدت في بعض الأحيان إلى تغييرات حادة في التوازن التقليدي للقوة "الجيوبوليتيكية" على جميع المستويات، حتى باتت النظريات التي تم تطويرها في ظل الظروف الجيوبوليتيكية شبه المستقرة لـ "النظام العالمي القديم" غير مناسبة لفهم هذه التغييرات. فعلى الصعيد الدولي، أصبح من المستحيل شرح ما يحدث في العالم بنفس البساطة التي كانت ممكنة في زمن المواجهة بين الأيديولوجيتين العظمتين، كما واجهت الأولوية التقليدية للدولة القومية تحديًا من قبل الشبكات والمؤسسات المعولمة، وكذلك من قبل النظم الإقليمية وخصوصيتها (Sidaway, 1994, p. 490).

في ظل هذه التطورات، نشأت مناقشات موضوعية في علم الاجتماع والعلاقات الدولية والجغرافيا؛ حول تشكيل "خطاب العولمة" المتباين. وبدا للوهلة الأولى على الأقل، أن عوالم الجغرافيا السياسية والدول "ذات السيادة" المحددة إقليمياً، تتعرض للتقويض بسبب حجم ووتيرة التدفقات في النظام العالمي المعاصر (Walker, 1992, 5). وللتعامل بشكل مناسب مع هذا "التنظيم الاجتماعي والسياسي الجديد"، كان على الجيوبوليتيكا إعادة التفكير وتوسيع مفاهيمها التقليدية.

اكتسبت الجيوبوليتيكا بحلول تسعينيات القرن العشرين طابعًا متعدد التخصصات بامتياز، حيث أسهمت نظرية النظم العالمية، والأساليب الكمية، إلى جانب الكتابات ما بعد البنيوية حول السياسة العالمية، في إعادة تشكيل الأطر الفكرية لهذا المجال (Dodds, 2001, p. 470)؛ ومن ثم ركزت الجيوبوليتيكا على دراسة الآثار العميقة للتغيرات الأيديولوجية والسياسية والعسكرية والاستراتيجية، بالإضافة إلى الاقتصادية

والاجتماعية والثقافية والديمغرافية والإثنوغرافية، مع دراسة تأثير هذه التغيرات في حركة التحولات وسرعتها ضمن سياق الكيانات المادية والبشرية.

وبدأت مجموعة من الأكاديميين أمثال "كلاوس دودز Klaus Dodds" و "جون أغنيو John Agnew" و "جيروید تواتيل Gearo´id O´ Tuathail" و "سيمون دالبي Simon Dalby" وآخرين، في إعادة فحص الأدبيات الجيوبوليتيكية القديمة، والتي كانت من المحرمات منذ عام ١٩٤٥، بسبب تواطؤ هتلر المزعوم مع علماء الجيوبوليتيكا. وفي عملية إعادة التقييم هذه، حاولت المجموعة الأكاديمية دحض بعض الافتراضات الضمنية المتأصلة في الجيوبوليتيكا التقليدية (١٨٩٩-١٩٤٥). كما قاد عملهم إلى تحقيق معمق في أعمال بعض رواد الفكر الجيوبوليتيكي التقليدي، بدءًا من "ماهان Mahan" و "ماكيندر Mackinder"، وصولاً إلى المدرسة الألمانية المثيرة للجدل في الجيوبوليتيكا، ورائدها الصوري "كارل هوشوفر Karl Haushofer".

سعت هذه المجموعة التي لا يزال "دودز" أحد أعضائها البارزين، إلى تطوير نموذجها الخاص المتمثل في الجيوبوليتيكا النقدية. ومن اللافت للنظر أن ظهور هذا الاتجاه تزامن مع تطور النظريات النقدية في العلاقات الدولية، بدءًا من أواخر الثمانينيات، وهو ما برز بشكل خاص في أعمال باحثين أمثال "ريتشارد أشلي Richard Ashley"، و "جيمس دير ديريان James Der Derian"، و "مايكل شابيرو Michael Shapiro"، و "روب ووكر RobWalker" (Power & Campbell, 2010, p. 243).

ساهم "كلاوس دودز" منذ البداية في إثراء هذا النقاش، حيث ركّز بشكل خاص على الربط بين تحليل السياسة الخارجية والجيوبوليتيكا النقدية. علاوة على ذلك، فهو معروف أيضًا باهتمامه المستمر بالأطر الفكرية والمفاهيمية الجيوسياسية، وأبحاثه

المتميزة حول السياسة الدولية في أنتاركتيكا والمحيط الجنوبي. كما قدّم إسهامات رائدة من خلال دراساته الأصلية والمحفّزة حول بريطانيا وإمبراطورية جنوب المحيط الأطلسي.

ويتم إعادة تصور الجيوبوليتيكا ـ وفق هذا النهج ـ كعملية استطرادية، لا تقتصر على موضوعات بعينها أو مجموعة صغيرة من العلماء والباحثين، فيبدأ التفكير الجيوبوليتيكي من مستوى بسيط ثم يسود الممارسة اليومية للسياسة الدولية. باختصار، فالجيوبوليتيكا النقدية تُعنى بدراسة كيفية إضفاء الطابع المكاني على السياسة الدولية من قبل القوى الرئيسية والدول المهيمنة. أو كما يوضح كلاوس دودز، تستكشف الجيوبوليتيكا النقدية الافتراضات والتفاهمات الجغرافية التي تقوم عليها صنع السياسة الخارجية ونظريات السياسة العالمية. وبخلاف الجيوبوليتيكا التقليدية، تركّز الجيوبوليتيكا النقدية على تفسير كيفية دخول العلامات والتسميات الجغرافية في الخطاب الشعبي والرسمي، بدلاً من افتراض علاقة سببية قوية بين الجغرافيا الطبيعية وسلوك الدولة (Dodds, 2007, p. 79).

كما أشار بول روبر Paul Reuber"، فإن "الجيوبوليتيكا النقدية تسعى إلى تفكيك الكيفية التي تفكر بها النخب السياسية تجاه الأماكن والمواقع الجغرافية وتوظفها كأدوات للسلطة". وتهدف هذه العملية إلى إزالة الطابع الأسطوري عن تلك التخيلات أو التصورات الجغرافية، وكشف أبعاد السلطة الرمزية الكامنة وراءها. ومن خلال هذا النهج، تصبح الجغرافيا السياسية قادرة على إظهار كيفية استغلال مفاهيم مثل (الهوية المكانية والوطن والعرق .... إلخ) لتحقيق مصالح جيوبوليتيكية محددة. يكشف هذا المنظور عن كيفية بناء التصورات الجيوبوليتيكية وتوظيفها للتلاعب بالمشاعر الجماهيرية، سواء في سياق المظاهرات أو الحروب الدموية أو التطهير العرقي والإبادة

الجماعية. ويتجلى هذا المنظور بشكل أكثر كثافة خلال الصراعات العسكرية، حيث تتكاثر التمثيلات الجيوبوليتيكية بشكل لافت كالفطر، كما حدث في تغطية أحداث حرب الخليج والبوسنة وكوسوفو والشيشان (Reuber, 2000, p. 39).

ومن أمثلة توظيف التمثيلات الجيوبوليتيكية في الصراعات العنيفة، الحرب الأهلية في نيجيريا، حيث يمكن ملاحظة كيف يُوظَّف الاستغلال الاستراتيجي للاختلافات الإثنوغرافية الدقيقة بين السكان، بالتوازي مع تعزيز خطاب الهوية الإقليمية، في تشكيل ما يُعرف بـ"جغرافية العنف" الجديدة. وقد أصبحت هذه الظاهرة واقعًا عالميًا بارزًا منذ نهاية الحرب الباردة، حيث يُعاد تشكيل الصراعات على أسس عرقية وإقليمية تخدم أجندات سياسية وجيوبوليتيكية معقدة.

ولا تقتصر التمثيلات الجيوبوليتيكية على الصراعات العنيفة فقط، بل تتجلى أيضًا في النزاعات المتعلقة بالفضاء على مختلف المستويات، وفي الصراعات حول حدود المجتمعات أو التخطيط الإقليمي لاستخدام الأراضي، حيث تُعد "التخيلات الجغرافية الاستراتيجية" أدوات تفسيرية تُستخدم بشكل واعٍ من قبل السياسيين، كاستراتيجيات لتحقيق مصالحهم الخاصة. يستفيد هؤلاء السياسيون من نماذج التخطيط الجغرافي، مثل نموذج كريستالر Christaller للمكان المركزي، ومن البيانات الجغرافية، لتقديم تفسيرات أحادية الجانب تتماشى مع أهدافهم. حتى الهوية العرقية والإقليمية يمكن استغلالها كأدوات خطابية فعالة في صراعات استخدام الأراضي (Reuber, 2000, p. 39).

وقد انخرط رواد الجيوبوليتيكا النقدية بفاعلية في هذا الاتجاه، حيث ركزوا على تحليل وتفكيك الأطر الخطابية والسياساتية التي تُستغل لتبرير النزاعات وإعادة تشكيل الهويات الجغرافية. وقد ذكر "جيروید تواتيل Gearóid Ó Tuathail": أن

الجيوبوليتيكا النقدية تعد ادعاءً يفترض أنه يمكن للمرء أن يتجاوز الجيوبوليتيكا التقليدية التي تتسم بالتوجهات البغيضة، ساعيةً إلى استعادة الحقيقة بعيدًا عن الفوارق الفئوية والأيديولوجية والعقائدية والإمبريالية. ويرى أنها ليست سوى نقطة انطلاق نحو شكل جديد من الجيوبوليتيكا، يُؤمل أن يكون أقل عبئًا بالنزعات القومية والشوفينية العالمية، وأكثر التزامًا بمبادئ العدالة العالمية والتحليل النقدي الذاتي (Jones & Sage, 2010, p. 316).

تناول هؤلاء الرواد طيفًا واسعًا من الأدبيات التي باتت تعكس الجيوبوليتيكا المعاصرة. وتشمل هذه الأدبيات قضايا مثل الفصل العنصري العالمي، والعلاقات بين الشمال والجنوب، والجيوبوليتيكا الشعبية التي تتناول تمثيل العالم من خلال وسائل الإعلام كالأفلام والرسوم المتحركة والموسيقى. كما تشمل عولمة الخطر، مع التركيز بشكل أساسي على أسلحة الدمار الشامل، وعولمة القضايا البيئية، بدءًا من مؤتمر ستوكهولم وصولًا إلى ريو وما بعدها. بالإضافة إلى ذلك، استعرضوا موضوعات مثل عولمة النزعة الإنسانية، وعولمة المعارضة، وعولمة الإرهاب، فضلاً عن العالم غير المتكافئ، والفضاء السيبراني. وشملت الأدبيات أيضاً قضايا الطاقة، بما في ذلك التدافع العالمي على احتياطيات النفط والغاز المتناقصة، خاصة نتيجة للنمو الاقتصادي في الصين والهند. إلى جانب ذلك، تناولت الأدبيات التحديات الديموغرافية في القرن الحادي والعشرين، مما يبرز الطابع المتداخل لهذه الموضوعات في سياق الجيوبوليتيكا الحديثة (Dodds, 2007, pp. 80-81).

وبالتالي فإن السؤال الأكاديمي يطرح نفسه، حول ما إذا كان نموذج الجيوبوليتيكا النقدية هو الأداة الوحيدة المتاحة، لتحقيق فهم أفضل للتطورات الجيوبوليتيكية التي نراها في السياسة العالمية المعاصرة؟

ألقى الجغرافي الأمريكي "نيل سميث Neil Smith" محاضرة بعنوان "ما بعد الجيوبوليتيكا؟"، خلال إحدى جلسات مؤتمر نظمته جمعية الجغرافيين الأمريكيين (AAG) عام ٢٠٠٧، والذي تناول "اتجاهات جديدة في الجيوبوليتيكا النقدية"، وأعلن فيها أن مفهوم الجيوبوليتيكا النقدية يحمل تسمية مضللة، معتبرًا أنه يعادل مفهوم "الرأسمالية النقدية"، نظرًا لارتباطه الوثيق بالمشاريع التي تقودها الدولة لتحقيق السيطرة المكانية وتعزيز النزعات الإمبريالية (Jones & Sage, 2010, p. 315).

وقد أشار "فيرجيني مامدوح Virginie Mamadouh" خلال المؤتمر نفسه، إلى أن "النقد" في سياق الجيوبوليتيكا النقدية كان غالبًا ما يقتصر على تفكيك الخطابات، دون أن يرتقي إلى مستوى إحداث تغيير فعلي يجعل العالم مكانًا أفضل. وأضاف أن الجيوبوليتيكا النقدية كانت في كثير من الأحيان أقل انخراطًا في التعامل مع القضايا الحيوية في العلاقات الدولية أو المناطق الجغرافية الحرجة، إذ ركّزت بشكل أكبر على النهج البنائي بدلاً من السعي إلى تغيير العالم. وتساءل ساخراً: هل يمكن أن يُطلق على ذلك ضوء فوكو[*]؟ (Jones & Sage, 2010, p. 320).

يبدو أن مشكلة الجيوبوليتيكا النقدية هنا تتعلق بغياب تأثير ملموس لها على المناقشات السياسية، ففي الوقت الذي يسعى الجيوبوليتيكيون الفاعلون، سواء كانوا مسؤولين حكوميين أو رجال أعمال أو نشطاء، إلى إيجاد تفسيرات مستنيرة وجديدة لفهم العالم المتغير من حولنا، تبدو الجيوبوليتيكا النقدية غير قادرة على تقديم الإلهام أو تقديم رؤى وقرائن تساعد في تشكيل تصورات جديدة، أو توليد تمثيلات مبتكرة، أو

[*] ميشال فوكو (بالفرنسية: Michel Foucault) (١٩٢٦– ١٩٨٤)، فيلسوف فرنسي بارز، اهتم بشكل خاص بدراسة كيفية استخدام الفلسفة كأداة لتسليط الضوء على أنماط الهيمنة والسلطة في المجتمعات. كان من أبرز اهتماماته تحليل العلاقة بين المعرفة والسلطة، ودراسة كيفية تشكيل الخطابات التي تساهم في تعزيز السيطرة الاجتماعية والسياسية.

تحفيز الناس في عالم يزداد عولمة. قد يعتقد بعض الجغرافيين أن هذا النقص في التأثير المجتمعي ليس بالضرورة مشكلة كبيرة، إذ يمكن تعويضه من خلال تعزيز الروابط مع حركات النضال القومية والمؤسسات الدولية، وأكاديميًا من خلال التركيز على تقديم دراسات متنوعة حول مناطق الأزمات وتحليل ديناميكياتها (Jones & Sage, 2010, pp. 320-321).

لكن، على الرغم من الادعاءات بشأن أهمية الجيوبوليتيكا النقدية، لم تنحسر القومية الخبيثة، ولا الشعبوية العنيفة، ولا النزعات العسكرية المتصاعدة في ظل العولمة. بل، وبشكل مأساوي، ظل العنف الجماعي المدعوم من الدولة ظاهرة بارزة خلال العقود الماضية، كما يتضح من المجازر التي وقعت في يوغوسلافيا السابقة والشيشان ورواندا، وغيرها من عمليات التطهير العرقي والإبادة الجماعية. وتجلى ذلك أيضًا في إخفاق الأمم المتحدة في حماية السكان البوسنيين في "سريبرينيتشا Srebrenica" من الهجمات التي شنتها القوات الصربية.

وكان ذلك في الوقت الذي ركز فيه علماء الجيوبوليتيكا النقدية ـ على مدى العقود الثلاثة الماضية ـ بشكل أكبر على تفكيك التمثيلات والعمليات الجيوبوليتيكية بدلاً من السعي إلى تخيل أو اقتراح استراتيجيات بديلة. ونتيجة لذلك، لم يقترن نضج الجيوبوليتيكا النقدية داخل المجال الأكاديمي للجغرافيا بالمشاركة الفعّالة في عمليات السياسة الدولية، أو تعزيز السلام العالمي، أو معالجة قضايا التنمية الجغرافية غير المتكافئة، وما يرتبط بها من تعزيز العدالة الاجتماعية المكانية (Bachmann & Moisio, 2020, pp. 252-253).

فأظهرت الجيوبوليتيكا النقدية، ولأسباب قد تكون مفهومة، إحجامًا ملحوظًا عن الانخراط في قضايا الشؤون العسكرية والاستراتيجية. ومن المفارقات أن الانتقادات

الراسخة التي قدمتها تجاه الرؤى الجيوبوليتيكية التقليدية، مثل تلك الخاصة بكتابات "هالفورد ماكيندر"، لم تُستبدل بدراسات تسلط الضوء على كيفية تأثير الجيوبوليتيكا في الحياة اليومية. ومن ثم كانت الجيوبوليتيكا النقدية ـ كما يرى كلاوس دودز ـ مخيبة للآمال للغاية، حيث أولت اهتمامًا كبيرًا بتحليل الرموز (مثل الشعارات أو الخطابات الرسمية)، والتواريخ (الأحداث التاريخية المؤثرة)، والجغرافيات الوطنية (مثل الحدود والمناطق التي تُحدد هوية الدولة). ولكن، على الرغم من هذا التركيز، لم تُظهر أو توضح كيف تؤثر هذه العوامل بشكل مباشر في حياة الناس اليومية، أو كيف تُستخدم هذه الرموز والجغرافيات لفرض سياسات تُحول الحياة اليومية إلى وسيلة لتعزيز سيطرة الدولة، أي تأميمها (Dodds, 2001, pp. 472- 474).

دفع ذلك "فريزر ماكدونالد Fraser MacDonald" إلى القول: "هناك خطر على جيلي ـ أولئك الذين نشأوا مع انتقادات جون أغنيو وسيمون دالبي وجيروويد تواتايل ـ أن يفكروا في الجيوبوليتيكا النقدية على أنها تغلبت على سلفها الكلاسيكي، سيكون هذا خطأ. على الرغم من كل الشراء الفكري والسياسي غير المشكوك فيه للمجموعة الجيوبوليتيكية النقدية ضمن الجغرافيا الأكاديمية، إلا أنها لم تشكل تحديًا خطيرًا للطرق التي يتم من خلالها تصور وممارسة الجيوبوليتيكا بشكل عام على الصعيد العالمي" (Jones & Sage, 2010, p. 318).

ويضيف: "أقول هذا بصفتي شخصًا يعمل ضمن الإطار الجيوبوليتيكي النقدي ولدي تأثير عميق لهذا العمل السابق. للأسف، الجيوبوليتيكا الكلاسيكية لا تزال مزدهرة. على سبيل المثال، سياسة الإدارة الأمريكية الحالية بشأن "التفوق الفضائي" ـ

كما كتبت في مكان آخر ـ فإن الدافع لفرض السيطرة على الفضاء المداري(*) هو حالة كتابية في تطبيق الفكر الماكنديري. ألقِ نظرة أيضًا على عمل "الجيواستراتيجيين" الحاليين مثل "كولن س. جراي Colin S. Gray" والعديد من أنصار المذاهب العسكرية الجديدة: يبدو أن الإرث الفكري للمفكرين الجيوبوليتيكيين الكلاسيكيين، الذين اعتقدنا أننا تجاوزنا أفكارهم، لا يزال يشكل مصدرًا مهمًا للعديد من الكتاب والجيواستراتيجيين" (Jones & Sage, 2010, p. 318).

المبحث الثاني: الجغرافية السياسية للفضاء السيبراني

تطورت شبكة الويب العالمية (WWW) منذ إطلاقها في عام ١٩٩١، من شبكة نصوص تشعبية، يستخدمها عدد قليل من المحترفين، إلى وسيط يستخدمه ملايين الأشخاص حول العالم يوميًا. ومنذ ذلك الحين، دخل مصطلح "الفضاء السيبراني" في المناقشات بين كافة الدوائر، ويعني حرفيًا "الفضاء القابل للملاحة"، ويتألف من جميع المساحات التي تم فتحها بواسطة تكنولوجيا الاتصالات الحديثة، بما في ذلك التلفزيون والهواتف (Gibbs, Kim & Ki, 2016, p. 1). ويعرّف "كوهل Kuehl" الفضاء السيبراني بأنه "مجال عالمي يقع ضمن بيئة المعلومات، يتميز بطابعه الفريد في الاعتماد على الإلكترونيات والطيف الكهرومغناطيسي، لإنشاء المعلومات وتخزينها وتعديلها وتبادلها واستغلالها عبر شبكات مترابطة، مدعومة بتقنيات المعلومات والاتصالات" (Robinsona, Jonesb & Janickea, 2015, p. 6).

(*) يشير مصطلح "الفضاء المداري" إلى المساحات المحيطة بالأرض التي تُستخدم لتحديد مسارات الأقمار الصناعية والمركبات الفضائية. هذه المدارات تختلف في الارتفاع والمسافة عن سطح الأرض.

ويشير مصطلح "الفضاء السيبراني" ـ في التعريف الأكثر شيوعًا ـ إلى المساحات التي تغطيها شبكة الإنترنت. وتعد شبكة الويب العالمية (WWW) واحدة من أبرز التطبيقات المستندة إلى الإنترنت. ومن التقنيات الأخرى التي تتجلى ضمن هذا الفضاء: تقنيات الوسائط الاجتماعية، ومجموعات أخبار لوحة الإعلانات، والدردشة عبر الإنترنت (IRC)، والأبراج المحصنة متعددة المستخدمين (MUDs) (Gibbs et al., 2016, p. 1).

وقد دخل مصطلح "الفضاء السيبراني" إلى النقاشات الجغرافية، بعد أكثر من ست سنوات من النشر الأول لرواية "ويليام جيبسون[*] William Gibson" الشهيرة "نيورومانسر Neuromancer". في هذه الرواية، قدم جيبسون وصفًا مبتكرًا لمصطلح "الفضاء السيبراني"، واصفًا إياه بأنه "هلوسة توافقية يعاني منها المليارات من البشر يوميًا"؛ حيث تتحلل الأجساد، ويتلاشى المكان والزمان في تدفق مستمر للمعلومات. من هذا المنطلق، بات يُنظر إلى الفضاء السيبراني بوصفه عالمًا من الروابط والنصوص التشعبية، عالمًا افتراضيًا منفصلًا عن العالم الحقيقي غير المتصل. لهذا، ومنذ منتصف التسعينيات، أعرب معظم الجغرافيين عن أسفهم لاستمرار هذه الرؤية لما يُعرف بـ"عالم ما بعد الحداثة". فقد انتقدوا تلاشي المادية والجنس البشري، وفقدان الإنتماء إلى المكان كعنصر جوهري من عناصر الهويات الشخصية والقومية، بالإضافة إلى انهيار الحدود الجغرافية وتلاشي المسافات (Wissmann & Palis, 2017, pp. 2 -3).

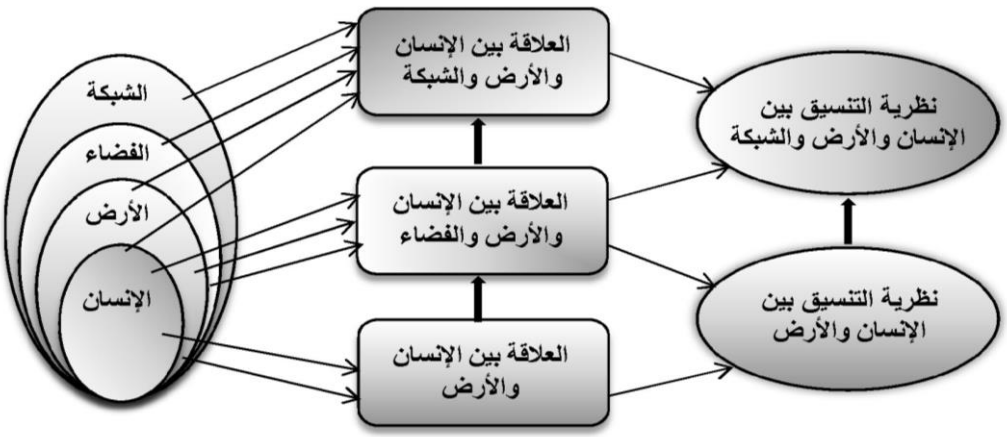
[*] ويليام جيبسون، كاتب متخصص في أدب الخيال العلمي، يُعرف بشكل خاص بإسهاماته البارزة في نوع أدبي يُطلق عليه اسم "الشر الإلكتروني Cyberpunk".

وعلى ذلك، تحول الفضاء السيبراني إلى ساحة رئيسية لجولة جديدة من المنافسة الجيوبوليتيكية، مما أدى إلى بروز الجغرافيا السياسية للفضاء السيبراني كمنظور تحليلي حديث. وقد تضافرت عدة عوامل لإضفاء الطابع الجغرافي على هذا الفضاء، من أبرزها: السمات الجغرافية لهندسة الفضاء السيبراني، ودور الجهات الفاعلة الرئيسية فيه، بالإضافة إلى القوة المتزايدة للدول ذات السيادة التي تسعى لتعزيز نفوذها في هذا المجال.

وفي هذا الإطار، يمكن تمييز ستة جوانب رئيسية تعكس منطق الجغرافيا السياسية للفضاء السيبراني: ١. التفكير الجيوبوليتيكي تجاه خطاب وسياسة الأمن السيبراني ٢. التداخل بين حدود الفضاء السيبراني والفضاء الجيوبوليتيكي ٣. مفهوم سيادة الفضاء السيبراني يردد صدى النظريات الكلاسيكية في الجغرافيا السياسية ٤. التشابه بين المنافسة والصراع على السيادة في الفضاء السيبراني والفضاء الجيوبوليتيكي ٥. اتجاه عسكرة الفضاء السيبراني يزيد من مخاطر الصراعات الجيوبوليتيكية ٦. الدمج التدريجي لقضايا الفضاء السيبراني في البنية الجيوبوليتيكية التقليدية.

يمثل الفضاء السيبراني بُعدًا مكانيًا جديدًا يضم أنشطة تجمع بين البشر والبيانات، وقد أصبح عنصرًا أساسيًا للأمن القومي لكل دولة. إن الفهم العلمي للفضاء السيبراني يُعد ضروريًا لتحليل أساليب إدارته وحوادثه وضمان أمنه. بناءً على ذلك، أصبح الفضاء السيبراني مجالاً جديداً للبحث الجغرافي في عصر المعلومات. وعلى خلفية المنافسة الدولية المحتدمة على الفضاء السيبراني، كانت هناك حاجة ملحة لتعزيز البحث بين مجالات الجغرافيا والأمن السيبراني، مما أدى إلى ابتكارات نظرية ومنهجية أوجدت فرعاً جديدًا من الجغرافيا يُعرف بـ "جغرافية الفضاء السيبراني Cyber Geography". يوسع هذا الفرع البحث الجغرافي ليشمل دراسة المساحات الافتراضية

بجانب المساحات الواقعية، وينطوي أساسه النظري حول تطور مجال الجغرافيا من دراسة العلاقة التقليدية بين الإنسان والأرض (شكل "١")، إلى دراسة العلاقة بين الإنسان والأرض والشبكة (Gao, Guo, Jiang, Wang, Fang, & Hao, 2019, p. 1949).



Source:-
Gao, C., Guo, Q., Jiang, D., Wang, Z., Fang, C., & Hao, M. (2019). Theoretical basis and technical methods of cyberspace geography. Journal of Geographical Sciences, 29(12), p. 1956.

شكل (١) إطار تطوري لتحول العلاقة بين الإنسان والأرض إلى العلاقة بين الإنسان والأرض والشبكة

تتضمن الأساليب الفنية لجغرافية الفضاء السيبراني (CG)، جمع ودمج البيانات حول عناصر الفضاء السيبراني، والتمثيل المرئي لهذا الفضاء، وتعزيز الوعي بالذكاء السيبراني الظرفي والسلوكي. كما تشتمل على رسم وبناء علاقات بين خرائط الفضاء السيبراني والفضاء الحقيقي، وإعادة تعريف المفاهيم الجغرافية التقليدية مثل المسافة والمساحات بما يتناسب مع الفضاء السيبراني، وإنشاء لغة ونماذج ومنهجيات لتمثيل الفضاء السيبراني بشكل مرئي، ورسم خرائطه، ودراسة المبادئ التي تتحكم في تطور هياكله وسلوكياته (Gao et al., 2019, p. 1949).

ويُعد الفضاء السيبراني مفهومًا أوسع وأكثر شمولاً من الإنترنت، حيث تمثل مساحة الإنترنت في الواقع جزءًا فرعيًا من الفضاء السيبراني، ومن الممكن أن يكون هناك العديد من الفضاءات الإلكترونية البديلة، التي تم تحديدها وإنشاؤها من خلال أساليب مختلفة للتوصيل البيني. بمعني آخر، فالفضاء السيبراني هو جميع الاتصالات أو الأجهزة التي لديها واجه اتصال وتتصل مع بعضها البعض، دون الحاجة إلى أن تكون مرتبطة مباشرة بشبكة الإنترنت. ومن أمثلة ذلك، الأجهزة الكهربائية الذكية، والأجهزة اللاسلكية، والهواتف المحمولة، وأجهزة الألعاب الإلكترونية، حيث تمتلك هذه الأجهزة القدرة على التواصل فيما بينها دون الاعتماد على الإنترنت كوسيط (Clark, 2010, pp. 1-2).

ويتجاوز الفضاء السيبراني البعد المكاني المادي، حيث تنشأ المجتمعات الافتراضية فيه حول مفاهيم قد لا يكون لها نظير في عالم الواقع. وتقدم البرمجيات مفتوحة المصدر التي طورتها مجتمعات المستخدمين حول العالم مثالاً ملموسًا على ذلك. وبالتالي، فإن الجغرافيا السياسية للفضاء السيبراني تشكل البيئة التي تنفذ فيها الجهات الحكومية وغير الحكومية العمليات السيبرانية. كما تستكشف كيف تشكل تجربة الإنترنت (الحالة الجيوسياسية)، والمساحات التي تحدث فيها التفاعلات (المجالات الجيوسياسية)، والثقافات الجيوسياسية المختلفة، سلوك واستراتيجيات هذه الجهات الفاعلة في الفضاء السيبراني.

ويرى "إلكسندر جراندين Alexander Grandin" أن الفضاء السيبراني يتكون من ثلاث طبقات (جدول "١" وشكل "٢")، وهي الطبقة المادية (الطبقة الجغرافية)، والطبقة المنطقية، وطبقة الشخصية السيبرانية (Grandin, 2023, p. 210). وهم على النحو المفصل:-

الجدول (١): مكونات الفضاء السيبراني

المستوى / المكونات	المستوى المادي	المستوى المنطقي	المستوى المعرفي
العقد	معدات الشبكات، البلدان، المدن	عنوان IP، الشبكة، التطبيقات، خدمات الشبكة	الهوية، رقم الهوية، عنوان البريد الإلكتروني
الحواف	علاقات الاتصال بين العقد	الاتصالات المنطقية مثل VPN، التبديل، نظير إلى نظير التطبيقات	التفاعلات بين العقد
الجهات	الأجهزة والموارد التي تشكل البنية التحتية للشبكة	خدمات التطبيق	وسائل الإعلام والأشخاص الذين يستخدمون كيانات المستوى المادي بمساعدة خدمات المستوى المنطقي

Source:-

Grandin, A. (2023). Cyberspace geography and cyber terrain: Challenges in producing a universal map of cyberspace. Proceedings of the 22nd European Conference on Cyber Warfare and Security (ECCWS), 22(1), p. 211.

الطبقة المادية: وهي أساس الفضاء السيبراني؛ حيث تتكون من أجهزة تكنولوجيا المعلومات والبنية التحتية للشبكة، بما في ذلك أجهزة وبرامج ومستودعات التخزين والنقل ومعالجة المعلومات داخل الفضاء السيبراني. لتشمل مستودعات البيانات، والكابلات التي تنقل البيانات، والاتصالات فيما بينها، وجدران الحماية. وقد تتم الاتصالات عبر الأسلاك أو الألياف، أو عبر الإرسال اللاسلكي، أو عن طريق النقل المادي لأجهزة الحوسبة، والتخزين من مكان إلى آخر. ولعل الطبقة المادية هي

الأسهل فهماً؛ لأنها ملموسة، كما أن ماديتها تمنحها إحساساً ثابتاً بالموقع الجغرافي، ومن ثم تخضع بالتالي لقيود الجغرافيا السياسية.

المصدر:-

الشكل من عمل الباحثَين إعتماداً على بيانات الجدول (١)

شكل (٢) مكونات الفضاء السيبراني

الطبقة المنطقية: وهي الجهاز العصبي المركزي للفضاء السيبراني، وتتكوّن من الاتصالات المنطقية التي تربط بين عُقد الشبكة، ويُقصد بالعُقد الأجهزة المتصلة بشبكة الكمبيوتر، وتوجد هذه العُقَد في مواقع جغرافية متعددة. وهذه الطبقة مسؤولة عن توجيه حزم البيانات إلى وجهاتها النهائية في المقام الأول، عبر أنظمة أسماء النطاقات (DNS)، وبروتوكولات الإنترنت، والمتصفحات، ومواقع الويب، والبرامج، وكلها تعتمد على كابلات الألياف الضوئية ومكونات الطبقة المادية المذكورة أعلاه. تتميز هذه الطبقة بطبيعتها الافتراضية، مما يجعل التحكم فيها والتعامل معها مرهونًا بالقدرة على إدارة الفضاء السيبراني والسيطرة عليه.

طبقة الشخصية السيبرانية: وتعني الهويات الافتراضية المشتقة من مستوى الشبكة المنطقية، مثل عناوين البريد الإلكتروني، وأرقام الهواتف، والعناوين الشخصية لأجهزة الحاسوب، وحسابات مستخدمي تكنولوجيا المعلومات. لذلك تمثل هذه الطبقة الشخصيات البشرية الحقيقية التي تعمل ضمن الفضاء السيبراني. وتجدر الإشارة إلى أن الفرد الواحد يمكن أن يمتلك أكثر من هوية سيبرانية، من خلال امتلاكه عدة حسابات بريد إلكتروني أو استخدامه لأجهزة حاسوب متعددة.

وتجدر الإشارة أيضاً، أن الناس ليسوا مجرد مستخدمين سلبيين للفضاء السيبراني، بل إنهم يحددون ويشكلون شخصيته من خلال الطرق التي يختارون استخدامها. والناس وشخصياتهم، التي قد تختلف من منطقة إلى أخرى، تشكل جزءاً مهماً من شخصية الفضاء السيبراني. فإذا ساهم الناس في ويكيبيديا فإن ويكيبيديا موجودة، وإذا غرد الناس فإن تويتر موجود. لذا يتعين علينا أن ندرك أن الناس يشكلون عنصراً مهماً من عناصر الفضاء السيبراني، تماماً كما يتعين علينا أن ندرك أهمية الأسلاك والبروتوكولات (Clark, 2010, p. 4).

تُعد جميع هذه الطبقات أساسية لفهم الفضاء السيبراني. فعلى سبيل المثال، إذا أراد شخص ما دراسة أمن الفضاء السيبراني، فلا يمكنه التركيز على طبقة واحدة فقط. ذلك لأن الهجمات قد تستهدف جميع الطبقات، بدءًا من تدمير المكونات المادية، ومرورًا بالمساس بالعناصر المنطقية، ووصولًا إلى إفساد المعلومات أو التأثير على الأفراد. لذا، فإن الدفاع الفعّال يجب أن يعتمد على استيعاب شامل لجميع هذه الطبقات وتكاملها.

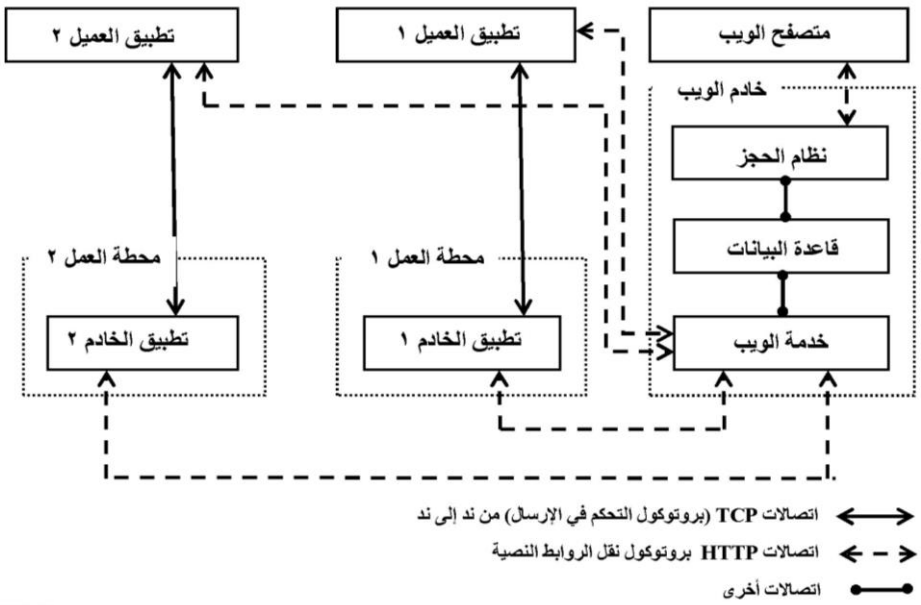
ويثير وضع الشبكة في المشهد المادي العديد من التساؤلات الجيوبوليتيكية التقليدية، من حيث التخطيط المكاني ومستوى الحماية المتوفرة. هذا البعد المتعلق

بالموقع الفعلي للمعدات، مثل الكابلات والخوادم ومراكز البيانات ونقاط التبادل ومراكز عمليات الشبكة وغيرها، يقودنا إلى الاعتقاد بأن الإنترنت وحركة المرور التي تمر عبره، يمكن التعامل معها مثل غيرها من البنى التحتية للشبكات الأخرى، مثل خطوط أنابيب النفط أو شبكات النقل التي تسهل تدفق البضائع. وبالتالي، فإن تبني منظور جيوبوليتيكي لقضايا الإنترنت وبنيته التحتية يُضيف بُعدًا جديدًا للتحليل الجغرافي والجيوبوليتيكي للفضاء السيبراني، مما يعزز فهم العلاقة بين الموقع الفعلي للبنية التحتية وتأثيرها على ديناميكيات القوة والصراعات الدولية (Robine & Salamatian, 2014, p. 124).

وكما أن فهم الجغرافيا يتطلب أحيانًا الإلمام بعلوم مثل الجيولوجيا أو العلوم السياسية أو علم النبات، فإن فهم الجغرافيا السيبرانية بشكل كامل يستلزم أولاً امتلاك معرفة أساسية بالبنية التقنية للإنترنت.

يعد الإنترنت نظام عالمي يربط شبكات الكمبيوتر ببعضها البعض باستخدام مجموعة بروتوكولات (TCP/IP)، تعرف ببروتوكولات الإنترنت، مما يتيح ربط مليارات الأجهزة حول العالم. ويُعرف بأنه شبكة من الشبكات، تتكون من ملايين الشبكات الخاصة والعامة والأكاديمية والتجارية والحكومية، التي تعمل على نطاقات محلية وعالمية، وتعتمد على تقنيات متعددة من الشبكات الإلكترونية السلكية واللاسلكية والألياف البصرية. ويحمل الإنترنت نطاقًا واسعًا من الموارد والخدمات، بما في ذلك مستندات وتطبيقات النص التشعبي المتصلة عبر شبكة الويب العالمية (WWW)، بالإضافة إلى خدمات البريد الإلكتروني، والاتصال الهاتفي، وشبكات نظير إلى نظير لمشاركة الملفات (Pursel, 2025, p. 10).

يعتبر "التعاون" الكلمة المحورية في هذا التعريف. وتُحدد طبيعة هذا التعاون من خلال بروتوكولات الاتصال، التي توفر إطارًا ولغة مشتركة تعتمدها الجهات الفاعلة طوعًا للتواصل مع بعضها البعض. عادةً ما تكون هذه الأشكال من التعاون متداخلة، حيث يعتمد كل مستوى منها على الأسس التي يضعها مستوى التعاون الأدنى. على سبيل المثال، يعتمد التعاون بين المتصفح والخادم على التعاون بين أجهزة التوجيه التي تربط العميل بالخادم (شكل "٣"). وفي المقابل، يعتمد هذا التعاون على نشر روابط الاتصالات، ومعدات الشبكات التي تربط بين المشغلين. هذا التداخل بين مستويات التعاون المختلفة، والذي يُشكّل البنية الطبقية للإنترنت، يُعد من العوامل الرئيسية التي ساهمت في تطورها السريع وانتشارها العالمي (Robine & Salamatian, 2014, p. 126).



Source:-
Callaghan, M. J., Harkin, J., McColgan, E., McGinnity, T. M., & Maguire, L. P. (2007). Client–server architecture for collaborative remote experimentation. *Journal of Network and Computer Applications, 30*(4), p. 1299.

شكل (٣) نموذج بيئة إلكترونية مماثلة توضح التعاون بين مكونات الشبكة

تتنوع الشبكات واستخداماتها في مختلف المجالات، ويبرز فرق جوهري بين نوعين رئيسيين من الشبكات: شبكات المعلومات التي تنقل البيانات والمعلومات (مثل الإنترنت والشبكات الاجتماعية، وما إلى ذلك)، وشبكات النقل التي تحمل المنتجات أو السلع المادية (مثل شبكات الطرق، والشبكات التجارية، وخطوط الأنابيب). وفي حين أن بعض الشبكات تقتصر على فئة واحدة فقط، هناك شبكات تجمع بين الفئتين معًا. على سبيل المثال، تعتمد شبكة توزيع الكهرباء على شبكة معلومات تتحكم في تدفق الطاقة. وفي بعض الحالات، إذا تعرضت شبكة المعلومات الداعمة للتدمير، فقد يؤدي ذلك إلى شلل شبكة النقل المرتبطة بها.

يتطلب فهم شكل شبكة النقل ونموها إدراك دور شبكات المعلومات الأساسية التي أسهمت في تشكيلها. وتُعرف شبكة المعلومات بأنها بنية تستخدم لمعالجة البيانات، ودعم عمليات الاتصال، ونقل أشكال وأنواع مختلفة من المعلومات على نطاق واسع، بالإضافة إلى تمكين الوصول عن بُعد إلى الشبكة، وتقديم خدمات مثل البريد الإلكتروني، ولوحات الإعلانات الإلكترونية، ومجموعات الأخبار. تتألف هذه الشبكات من الجهات الفاعلة الفردية الموزعة على الفضاء، والتي تتعاون لتبادل المعلومات. ولا يحدد هذا التعريف طبيعة المساحة التي يتواجد فيها الفاعلون، أو طبيعة تعاونهم، أو نوعية المعلومات المتبادلة (Salihović & Džubur, 2021, p. 59).

ونظراً لانتشار شبكة الإنترنت في جميع أنحاء العالم الواقعي، يمكن تبنّي منظور جيوسياسي لتحليل الآثار الناتجة عن التوزيع المكاني للبنى التحتية التي تجعل الإنترنت ممكنًا. وتشمل هذه البنى التحتية الخوادم، والتي يمكن أن تكون خوادم فردية منخفضة السعة، أو على العكس من ذلك، قد تكون مراكز بيانات تحتوي على عشرات الآلاف من الخوادم. ونظرًا لأن هذه الخوادم ومعدات الاتصال يجب أن تكون موجودة

في مكان ما في العالم المادي، فإن الإنترنت يظل عرضة لفقد أحد عناصر المعالجة أو الاتصال، سواء بسبب حادث تقني، أو هجوم إلكتروني، أو فقدان السيطرة على المنطقة التي تحتضن أجزاء من هذه البنى التحتية (Robine & Salamatian, 2014, p. 127).

وقد أظهرت التحديات الأمنية المتزايدة، مثل التنصت واعتراض البيانات، أنها لا تؤدي فقط إلى فقدان الخصوصية وتكبّد خسائر مالية وانقطاع كبير في الخدمات، بل يمكن أن تهدد أيضًا أمن واستقرار الدول. ولذلك، يعد تأمين الشبكات أمرًا بالغ الأهمية، خاصة للتطبيقات التي تتطلب مستوى عالٍ من الأمان، مثل مجالات الدفاع، والتمويل، والكيانات الحكومية والخاصة (Sharma, Bhatia & Prakash, 2022, p.1). وتزداد حدة المشكلة بشكل ملحوظ عندما تعتمد الدول بشكل كامل على تكنولوجيا المعلومات والاتصالات (ICT) والإنترنت، حيث تصبح بنيتها التحتية أهدافًا عالية القيمة وأكثر عرضة للهجمات.

المبحث الثالث: سيادة الدول في ظل الفضاء السبيراني

تستند سيادة الدول، في مفهومها التقليدي، على ركيزتين أساسيتين: الحيز المادي والإقليمي. وبالتالي، يتم تعريف السيادة فيما يتعلق بمفهوم الحدود الوطنية في ثلاثة أبعاد هي: الأرض والجو والبحر؛ حيث تهدف الدولة إلى فرض القانون الوطني والسلطة الوطنية. لذلك، تبدو السيادة كمفهوم مطلق حيث لا يمكن لسلطة أو قوة خارجية منافسة الحكومة الوطنية في أراضيها. وتكتسب الأنشطة التي يتم إجراؤها عبر شبكة الإنترنت البعد العابر للحدود، حيث يمكن أن يتأثر الناس من مختلف البلدان بهذه الأنشطة، ويمتد هذا التأثير إلى سيادة الدول واستقرارها أيضاً.

تشير الطبيعة الافتراضية للفضاء السيبراني إلى إزالة الطابع المادي (كل شيء بلا أوراق)، وإزالة الطابع الزمني (اتصال فوري)، وإضفاء الطابع الإقليمي والدولي (كسر الحدود الجغرافية والمسافات) للأنشطة عبر الإنترنت والتفاعلات، بل وإضفاء الطابع الفردي على المستخدم من خلال السماح له بالاستمتاع بالتحرر الكامل من سيطرة الدولة أو الحكومة، ولمصالحه الخاصة الأسبقية على مصالح الدولة أو المجتمع معاً، ويمكن تفسير ذلك على أنه انتهاك لسيادة الدولة. ويؤدي التأثير المشترك الناتج عن عملية المحاكاة الافتراضية إلى فكرة الوجود في كل مكان. وبالتالي، يمكن التعرف على تأثير الفضاء السيبراني على السيادة من خلال البعدين الزماني والمكاني معاً (Adams & Albakajai, 2016, pp. 256-257).

يعد تسريع الوقت سمة مهمة للفضاء السيبراني، مما يجعل القوانين الوطنية غير قادرة على مواكبة ذلك حتى الآن مع التطورات التكنولوجية، وهذا يخلق حالة من عدم اليقين القانوني لدى المواطن، ويقود مفهوم السيادة إلى الهاوية. وبالنسبة للمكانية، هي سمة أخرى للفضاء السيبراني، تشكل تحديًا كبيرًا لمفهوم الإقليمية في القانون التقليدي، فالدولة تستمد سيادتها من قدرتها على ممارسة الهيمنة والسيطرة على أراضيها، من خلال فرض سلطتها التشريعية الخاصة، وهذه السيادة عادة ماتكون مفوضة من قبل الأفراد إلى سلطة الدولة رأساً. لكن السيادة في ظل الفضاء السيبراني على النقيض من ذلك، تكون أفقية؛ حيث توجد كيانات ذات سيادة بجانب بعضها البعض، تنازع سلطة الدولة سيادتها (Adams & Albakajai, 2016, p. 260).

شرح "غرابوسكي Grabosky" طبيعة الجرائم الإلكترونية والجرائم العابرة للحدود، حيث أوجز ثلاثة أنشطة نموذجية قد تقوض سيادة الدولة، وهي: الجرائم التقليدية المرتكبة بأجهزة الكمبيوتر (مثل المواد الإباحية الرقمية للأطفال أو القرصنة أو

سرقة الملكية الفكرية والتزوير)؛ الهجمات على شبكات الحاسب من خلال البرامج الضارة مثل الفيروسات وغيرها؛ والإرهاب السيبراني وقدرته في خلق حالة فوضى ما بعد الحداثة، بالإضافة إلى القضايا الجنائية التقليدية مثل الاتجار بالمخدرات على سبيل المثال (Grabosky, 2004, p.146).

تتحمل الدولة عبئاً اقتصادياً أكبر في مواجهة خطورة هذه الأنشطة؛ حيث تنفق الدولة قدرًا كبيرًا من المال في تأمين وحماية أنظمة شبكتها من التهديدات المتوقعة، والتي يمكن أن تعبر حدود وأراضي الدولة على الرغم من جميع الاحتياطات التي تتخذها الدولة لحماية سيادتها. فالفضاء السيبراني بخصائصه (إزالة الطابع المادي، إزالة الطابع الزمني، وإزالة الحدود الإقليمية)، هذه الخصائص تجعل القوانين الوطنية غير قادرة على مواكبة التطورات التكنولوجية، والتي تتطور من المستوى الأكثر سطحية إلى المستوى الأكثر تعقيدًا، من دولة إلى دولة أخرى.

كان لدى مصممي ومطوري تكنولوجيا الإنترنت رغبة سياسية في تلبية رغبات الرأسماليين في الولايات المتحدة الأمريكية. وكانت الرغبة الأساسية هي الحد من سيادة الحكومات على أراضيها، من خلال جعل الشبكة مفتوحة على نطاق واسع، والاتصال بالعالم كله دون هوية جنسية أو عقدة قيادة مركزية. وفي وقت لاحق، لعبت الطبيعة الافتراضية للإنترنت دورًا مهمًا في تحقيق تلك الرغبة، والتقليل من دور الحكومات فيما يتعلق بالسيطرة على أنشطة وتفاعلات الفضاء السيبراني (Albakajai, Adams & 2016, p. 257).

وكان الفضاء السيبراني ـ حتى وقت قريب ـ (كما يرى شكري وكلارك) إلى حد كبير مستوى منخفض في تصنيف المخاطر السياسية، وهو المصطلح الذي يستخدمه علماء السياسة للإشارة إلى خلفية الظروف والقرارات والعمليات الروتينية. ولكن على

مدى العقدين الماضيين، بدأ الفضاء السيبراني، وفي جوهره شبكة الإنترنت، في تشكيل مجال السياسة العليا، واعتبارات الأمن القومي، والمؤسسات الأساسية، وأنظمة اتخاذ القرار التي تشكل أهمية بالغة للحكومات الوطنية. لقد احتكرت هذه الحكومات لفترة طويلة السياسة العليا، وتحاول بدورها السيطرة على مستقبل الفضاء السيبراني، ولكن بنجاح محدود للغاية في أفضل الأحوال (Choucri & Clark, 2013, p. 21).

يؤكد "بيرتاند دي لا شابيل Bertrand De La Chapelle"، المؤسس المشارك والمدير التنفيذي لشبكة سياسات الإنترنت والولاية القضائية، على المدى الذي أصبحت فيه ممارسة السيادة أكثر تعقيدًا بالنسبة للدول. ذلك لأن غالبًا ما تكون الأنشطة في الفضاء السيبراني عابرة للحدود، ويصعب أحيانًا على الدولة فرض احترام قوانينها وأنظمتها على أراضيها أو حتى مواطنيها، ولاسيما عندما يتم توفير الخدمة المستخدمة من قبل شركات أجنبية عملاقة، فتصبح حدود الولاية القضائية أكثر مرونة وتداخلا في الفضاء السيبراني. وهذه الولاية تشكل في كثير من الأحيان تنافس على السلطة وليس تعريفًا قانونيًا توافقيًا، وهذا يمثل على الفور تحدياً للنموذج الويستفالي(*) لسيادة الدولة بموجب القانون الدولي" (Chapelle & Fehlinger, 2016, p. 2).

(*) في عام ١٦٤٤ شاركت الدول المتحاربة لوضع حد للقتال وايجاد الحلول لاشاعة الاستقرار، وحضر المؤتمر ممثلين عن السويد وفرنسا وملوك النمسا والدنمارك واسبانيا والامراء الالمان فضلا عن ممثلي البابا. ان المؤتمر الذي انتهى بعقد معاهدة وستفاليا عام ١٦٤٨م قد وضع الاسس الجديدة للعلاقات بين الدول؛ حيث اعترف المؤتمر بالحرية الدينية، وساعد على انتشار فكرة التسامح الديني التي اصبحت احدى اسس الدساتير الاوربية لاحقا، كما تم الاعتراف برسم الحدود بين الدول وإحترام المصالح القومية وسيادة الدول على أرضها، كما شكلت الاتفاقية بداية للاعراف الدبلوماسية التي أُقرت كقوانين واعراف تلتزم بها الدول.

لقد خلق الفضاء السيبراني مرحلة جديدة في ديناميكيات القوة والحرية، حيث أتاح للأفراد أدوات ومنصات تمكنهم من تجاوز القيود التقليدية لنشر المعلومات والتأثير على الرأي العام، مما أعاد تشكيل العلاقة بين السلطة والمؤسسات والجمهور، خاصة فيما يتعلق بحرية التعبير ونشر المعلومات الحساسة. فقبل عشرين عاماً، كان نشر الفيديوهات أو الوثائق يتطلب الوصول إلى منصات إعلامية رئيسية، مثل محطات التلفزيون والقنوات الإخبارية، هذه الوسائل كانت تحت سيطرة مؤسسات قوية تخضع لقيود سياسية واجتماعية ومؤسسية تحدد ما يُنشر وما لا يُنشر. أما في ظل الفضاء الإلكتروني والمنصات الإعلامية الحديثة، فقد وفّرت أدوات جديدة تجاوزت هذه القيود، فأتاح سُبلًا مبتكرة لتعبئة الرأي العام وانتقاد السياسات أو الإجراءات العسكرية، مثل قواعد الاشتباك. هذه التغييرات منحت الأفراد قوة لم تكن متاحة لهم من قبل، مما أدى إلى إعادة تعريف العلاقة بين السلطة والجمهور (Benkler, 2011, p. 722).

ولفهم كيفية تأثير النشاط السيبراني على سيادة الدول، من المفيد رؤيتها على أرض الواقع، عبر سلسلة من الأمثلة الواقعية التي حدثت في السنوات القليلة الماضي، وذلك من خلال العرض التالي:

١- تسريبات ويكيليكس Wikileaks:

تصنف ويكيليكس نفسها على أنها منظمة إعلامية غير ربحية متعددة الجنسيات، وقد أسسها "جوليان أسانج[*] Julian Assange" في عام ٢٠٠٦.

[*] هو محرر وناشر وناشط أسترالي أسس موقع ويكيليكس في عام ٢٠٠٦. وقد لفت انتباه العالم في عام ٢٠١٠ بعد أن نشر موقع ويكيليكس سلسلة من التسريبات واللقطات من غارة جوية أمريكية في بغداد، وسجلات عسكرية أمريكية من حربها في أفغانستان والعراق وبرقيات دبلوماسية أمريكية. نشأ أسانج في أستراليا؛ حيث استقرت عائلته في ملبورن في منتصف مراهقته. انخرط

تتخصص ويكيليكس في تحليل ونشر مجموعات كبيرة من البيانات من المواد الرسمية الخاضعة للرقابة أو المقيدة، والتي تتعلق بالحرب والتجسس والفساد. وقد نشرت حتى الآن أكثر من عشرة ملايين وثيقة، إلى جانب التحليلات المرتبطة بها.

تطور موقع ويكيليكس ـ في غضون حوالي خمس سنوات ـ من كونه وسيطًا غير مباشر يمكّن النشطاء من نشر الوثائق دون الكشف عن هويتهم، إلى جهة فاعلة نشطة تتولى اختيار المواد أو حذفها، وتتواصل مباشرة مع وسائل الإعلام الرئيسية لزيادة النشر والوصول إلى جمهور أوسع. وفي نوفمبر ٢٠٠٧، حقق موقع ويكيليكس أول سبق كبير بنشره دليل العمليات العسكرية في خليج غوانتانامو، بعنوان: إجراءات التشغيل القياسية لمعسكر دلتا، والذي كشف عن العمليات اليومية والإجراءات التفصيلية في مركز الاحتجاز الخاضع للسيطرة الأمريكية في جزيرة كوبا. بحلول عام ٢٠٠٨، اكتسب موقع ويكيليكس شهرة عالمية واحترامًا واسعًا داخل مجتمع القرصنة، مما أدى إلى زيادة عدد المبلغين عن المخالفات عبر الموقع، بهدف الكشف عن وثائق حساسة. ومن بين أبرز الوثائق المنشورة: الملفات التي تدين البنك السويسري "جوليوس بار Julius Baer" فيما يتعلق بالتهرب الضريبي وغسيل الأموال، وكتيبات السيانتولوجيا السرية(*). كما تضمنت التسريبات رسائل البريد الإلكتروني الخاصة بالنائبة الأمريكية "سارة بالين Sarah Palin" منذ أن كانت حاكمة ولاية ألاسكا، وقائمة

في مجتمع القراصنة وأدين بتهمة القرصنة في عام ١٩٩٦. حصل على جوائز متعددة في مجال النشر والصحافة.

(*) هي مجموعة من المعتقدات والممارسات الدينية التي وضعها كاتب الخيال العلمي الأميركي "رون هوبارد Ron Hubbard"، الذي عاش في الفترة من عام ١٩١١ حتى ١٩٨٦. تستند السينتولوجيا إلى فلسفة علمانية تأسست عام ١٩٥٤ من قبل هوبارد، ثم أعاد صياغتها باعتبارها "فلسفة دينية تطبيقية".

عضوية الحزب الوطني البريطاني الفاشي (BNP)، وسجلات الحرب في أفغانستان والعراق (يوليو/نوفمبر ٢٠١٠)، والتي كشفت عن وحشية الحرب وسخرية السياسة الواقعية. بالإضافة إلى ذلك، تسريب البرقيات الدبلوماسية الأميركية، وكلها صادرة عن نفس المصدر، وتسببت في حالة من الفوضى الدولية.

وكان أبرز ما تم تسريبه، نشر ما سمي بفيديوهات "القتل العمد" في أبريل عام ٢٠١٠، وهي فيديوهات مسربة من الجيش الأمريكي، تُظهر هجومًا شنته مروحية هجومية أمريكية من طراز أباتشي، حيث أُطلق النار على مجموعة من الأشخاص في أحد شوارع بغداد في ١٢ يوليو ٢٠٠٧، وأسفر الهجوم عن مقتل أكثر من ٢٣ شخصًا، من بينهم اثنان من الصحفيين العاملين لدى وكالة رويترز. وشكل هذا الفيديو دليلاً مرئيًا صارخًا على إساءة استخدام القوة العسكرية من قبل الدولة، وكان أحد أبرز الأحداث في تاريخ ويكيليكس، وأثار الكثير من الجدل. لقد دفعت التسريبات إلى "نقد جذري للقوة العسكرية والجيوبوليتيكية الأميركية في الخطاب الشعبي السائد (وخاصة في الولايات المتحدة)"، فلم تقتصر تأثيرات التسريب على كشف انتهاكات الحرب الإنسانية فقط، بل زعزعت أيضًا أسطورة القوة الأمريكية الخيّرة، وأثارت تساؤلات جوهرية حول فكرة "حياد التكنولوجيا" ودورها المفترض في خدمة التنمية البشرية (Christensen, 2014, pp. 2593 - 2596).

رسّخ موقع ويكيليكس بذلك هويته كعلامة تجارية قوية وغير تقليدية، تُعرف بقدرتها على نشر الوثائق السرية والمعلومات الحساسة باستخدام تقنيات متقدمة. ولذا، أصبح الموقع منبرًا حيويًا للناشطين والصحفيين، وأداة فعّالة لكشف الحقائق التي قد تبقى مخفية عن العامة.

تكشف قضية ويكيليكس عند التعامل معها على مستوى الجهات الفاعلة عن مجموعة متنوعة من الروابط القوية والضعيفة والكامنة. وهي النقطة التي سبق الإشارة إليها فيما يتعلق بديناميكيات الشبكة التي تديرها ويكيليكس، وكيف تعتمد على أنماط مختلفة من الروابط لتعزيز وجودها وزيادة تأثيرها. يمكن تحليل هذه الديناميكيات وفقًا لنظرية الشبكات الاجتماعية، حيث يلعب كل نوع من الروابط دورًا مختلفًا في نجاح المنظمة وتحقيق أهدافها. وذلك على النحو التالي :-

الروابط القوية: وتتمثل في العلاقات الوثيقة التي تجمع بين الأعضاء الأساسيين في المنظمة، مثل جوليان أسانج، والصحفيين الذين يتولون مهام تحليل الوثائق ونشرها. تُبنى هذه الروابط على مستويات عالية من الثقة، وهي ضرورية للحفاظ على سرية العمليات وضمان تنسيق الجهود بفعالية. **الروابط الضعيفة:** وتمثل العلاقات مع المتطوعين والمساهمين من خارج الدائرة الأساسية للمنظمة، وهؤلاء غالبًا ما يقدمون دعمًا في جوانب محددة مثل الترجمة أو الترويج، دون أن يكون لهم ارتباط مباشر بالإدارة. وهذه الروابط تكون أقل التزامًا لكنها تتيح الوصول إلى موارد وخبرات جديدة. **الروابط الكامنة:** وتشير إلى الاتصالات غير المباشرة أو غير الظاهرة مع مجموعات من الهاكرز المجهولين، مثل مجموعة "أنونيموس Anonymous". ويعتمد ويكيليكس على المزج بين هذه الروابط لضمان المرونة العالية في العمل؛ فالروابط القوية تحافظ على استقرار وسرية العمليات، بينما تسهم الروابط الضعيفة والكامنة في توسيع نطاق العمل وتعزيز الابتكار. هذا المزيج يجعل المنظمة نموذجًا فريدًا في كيفية بناء الشبكات الفعالة، خاصة في بيئات عالية المخاطر مثل تسريب المعلومات الحساسة (Cammaerts, 2013, pp. 422-424).

لذلك، تعرض موقع ويكيليكس لضغوط هائلة من الحكومات والشركات الكبرى في محاولة لتعطيل نشاطه، فبجانب استهداف مصادر تمويله، تم استهداف كل من الاستضافة المادية للمحتوى الفعلي، وكذلك الارتباط بين عنوان IP وأسماء النطاق الخاصة بـ الموقع. فبعد أربعة أيام من نشر البرقيات الدبلوماسية الأمريكية في ٢ ديسمبر ٢٠١٠، حث السيناتور الأمريكي جو ليبرمان الشركات الأمريكية، على قطع روابطها مع ويكيليكس ومؤسسه جوليان أسانج. وذكر شركة أمازون Amazon Web Services على وجه الخصوص، التي استجابت بإنهاء عقدها لاستضافة محتوى ويكيليكس، مشيرة إلى أن الموقع انتهك شروط الخدمة المتعلقة بحقوق الملكية والتحكم في المحتوى. وفي اليوم نفسه، أوقفت شركة EveryDNS مزود اسم النطاق لويكيليكس، وزعموا أن أسماء نطاق الموقع تتعرض لهجمات متواصلة من نوع هجمات رفض الخدمة الموزعة (DDOS)، مما يعرض مستخدمي خدماتهم الآخرى للخطر. وردًا على ذلك، نفّذت ويكيليكس سلسلة من استراتيجيات المقاومة الشبكية لمواجهة هذه الضغوط، فلجأت إلى نقل استضافة محتواها إلى مزود الخدمة الفرنسي OVH، ومزود الخدمة السويسري DNS، كما استضاف العديد من المدافعين نسخًا منها في جميع أنحاء العالم، مما أكد بشكل قاطع استحالة حجب المعلومات بشكل كامل (Cammaerts, 2013, p. 429).

ويخلص "بنكلر Benkler" إلى أن ويكيليكس تمثل مثالاً حياً لقدرة المجتمعات الشبكية على تحدي الهياكل التقليدية للسلطة، مثل الحكومات أو الشركات الكبرى، من خلال تمكين الأفراد والجماعات الصغيرة من التأثير والمشاركة (Benkler, 2011, p. 750). وهو أمر يبرز كيف أن التكنولوجيا والشبكات قد أعادت تشكيل آليات السلطة التقليدية، مما أدى إلى خلق فرص جديدة للحرية وتوسيع نطاقها.

٢- وسائل التواصل الاجتماعي وثورات الربيع العربي:

شهدت المنطقة العربية منذ أواخر عام ٢٠١٠ ما اصطلح على تسميته بـ ثورات الربيع العربي، في كل من تونس ومصر، وفي وقت لاحق دول عربية أخرى (اليمن وسوريا وليبيا)، وكانت انتفاضات غيرت المسار الطبيعي للسياسة في المنطقة العربية، من خلال الاستخدام المكثف لشبكات التواصل الاجتماعي، مثل فيسبوك وتويتر، كأدوات للتعبئة والتنظيم ونشر المعلومات. ساعدت هذه المنصات على كسر القيود التي فرضتها الأنظمة على وسائل الإعلام التقليدية، مما أتاح للناس إمكانية التعبير عن آرائهم ونقل الأخبار والتنسيق في الوقت المناسب. في البداية حاولت الحكومات قمع الاحتجاجات من خلال قطع الإنترنت وتعطيل الاتصالات في محاولة للحد من قدرة النشطاء على التنظيم والتواصل؛ إلا أن الظاهرة لم تعد مجرد دعوات افتراضية للاحتجاج، بل حدث سيبراني موجه من الخارج ومترجم على أرض الواقع (في الشارع العربي). مما أثبت أن قوة الشبكات الاجتماعية تتعدى كونها أدوات تقنية. كما أدى الربط بين العالم الافتراضي والواقع إلى تغيير عميق في طبيعة السلطة والمقاومة، حيث أصبحت الحكومات مجبرة على التعامل مع تحدٍ جديد، لا يمكن احتواؤه بسهولة داخل الحدود الجغرافية التقليدية.

ويمكن استخلاص بعض الاستنتاجات النهائية حول الفضاء السيبراني وعلاقته بثورات الربيع العربي، وهي: أن الطبقات الدنيا من بنية الإنترنت أكثر قابلية للتنظيم من قِبَل الدولة، لأنها أكثر "مادية" يمكن التحكم فيها من قبل مؤسسات الدولة وما يتبعها، على الرغم من أن بعض عناصر البنية التحتية وخاصة الكابلات البحرية تُديرها جهات فاعلة متعددة الجنسيات. أما التحدي الأكبر في التنظيم يكمن في الطبقات العليا، مثل طبقة المعلومات، لأنها تحتوي على جهات فاعلة أصغر حجمًا

يمكنها الإفلات من السيطرة الحكومية بسهولة أكبر. هذا الأمر يجعل إدارة الأنشطة السيبرانية أكثر تعقيدًا، ولاسيما أن هناك العديد من الجهات الفاعلة غير الحكومية التي تنشط في الطبقات العليا، مما يعكس اهتمامها بالمعلومات والناس أكثر من اهتمامها بالبنية التحتية المادية. وهذه الجهات غير الحكومية تظهر مرونة وسرعة في التعامل مع القضايا السيبرانية، مما يجعلها منافسة للمؤسسات الحكومية في مجال الرقابة والحوكمة، ضمن السياق المعقد للعلاقات الدولية السيبرانية (Choucri & Clark, 2013, p. 26).

تتسم تكنولوجيا المعلومات في "الربيع العربي" بتشابه ملفت مع مصطلح "موقف خطابي مثالي"، الذي ظهر في الفلسفة المبكرة للفيلسوف الألماني المعاصر "يورغن هابرماس Jürgen Habermas"، وقد طوّره في إطار نظريته عن الفعل التواصلي. ويُعتبر هذا المفهوم جزءًا من رؤية هابرماس لكيفية بناء الحقيقة والمعرفة، من خلال الحوار العقلاني والتواصل الحر غير المقيد. إن خط تفكير هابرماس ـ والذي تطور قبل عقود من انتشار الإنترنت بين عامة الناس ـ يرى أن الاتصالات غير المقيدة هي الركيزة الأساسية لتحقيق الإجماع الاجتماعي. وكان هدفه الأساسي هو تصور فضاء (ساحة افتراضية) يمكن فيه تحقيق حوار حر وعقلاني وديمقراطي، يتيح للجميع المشاركة بغض النظر عن الوضع الاجتماعي أو الاقتصادي أو الثقافي. إن مصطلح "موقف خطابي مثالي" يعمل كمقياس واقعي لتحليل السياقات الاجتماعية، التي يتعرض فيها التواصل للتشوية بفعل العقبات السياسية أو الاقتصادية أو الثقافية. ووفق هذا المنظور المثالي، لا تعتبر الحقيقة كيانًا متعالياً أو منفصلاً عن الواقع كما في الفلسفة الأفلاطونية، بل هي نتاج تفاعل اجتماعي يحدث في سياق الممارسات الإنسانية اليومية (Fekete & Warf, 2013, p. 213).

إن الفضاء السيبراني يجسد رؤية هابرماس بشكل أكثر قوة ووضوحًا، مقارنة بأي ظاهرة اجتماعية أخرى اليوم. لقد أتاحت منصات مثل البريد الإلكتروني ويوتيوب وتويتر وفيسبوك، والتقنيات ذات الصلة مثل الهواتف المحمولة، تمكينًا غير مسبوق لمواطني الدول العربية. وساهمت هذه الأدوات في تسهيل المناقشات الصاخبة وغير المقيدة، ما أدى إلى نتائج سياسية عميقة، مع عواقب بعيدة المدى، بات يستشعرها الجميع الآن.

٣- النزاع المتكرر حول حماية حرية التعبير بين الدول والشركات العالمية الفاعلة:

يعد النزاع المتكرر بين فرنسا وشركة تويتر الأمريكية بشأن حماية حرية التعبير أحد الأمثلة البارزة في هذا السياق؛ حيث تخضع شركة تويتر لقيود في فرنسا بطرق غير مقبولة في القانون الأمريكي. وكان من بين هذه النزاعات ما شهده عام ٢٠١٢ من نزاع بين الطرفين؛ عندما أثيرت ضجة كبيرة بسبب تعليقات معادية للسامية، نُشرت على تويتر باللغة الفرنسية ضمن مسابقة "نكتة مثيرة للغثيان"، تحت هاشتاغ (#UnBonJuif -#AGoodJew)، وتعني "اليهودي الصالح". هذا الموقف تحول إلى اختبار قوة بين القضاء الفرنسي والشركة الأمريكية. ورغم أن فرنسا تطبق قوانين صارمة ضد العنصرية ومعاداة السامية، إلا أنها واجهت صعوبة في التحرك ضد الرسائل العنصرية على شبكات التواصل الاجتماعي، واستغرق الأمر عشرة أشهر من الجدل الإجرائي، قبل أن يوافق تويتر على تسليم المحاكم الفرنسية البيانات اللازمة لتحديد هوية بعض المستخدمين المتورطين في هذه القضية (Crace, 2013).

٤- ازدياد عمليات القرصنة والاحتيال المالي وتفاقم الأزمات المالية الدولية:

اكتسبت شركات الإنترنت العملاقة GAFA (جوجل، وأمازون، وفيسبوك، وأبل) قوة اقتصادية كبيرة، بحيث أصبحت قادرة على ممارسة سلطتها الخاصة وعدم الخضوع

بسهولة للنظام القانوني للدولة. لهذا باتت السيادة الاقتصادية والمالية للدول على المحك أيضاً، حيث تعمل الشبكات على تسريع تداول السلع والتدفقات المالية بشكل كبير، مما يزيد من مخاطر وحجم التجسس الاقتصادي، وسرقة الملكية الفكرية والصناعية، بل وحتى الأسرار التجارية، علاوة على تسهيل التهرب الضريبي وانتشار الأزمات المالية الدولية.

ورغم أن بعض هذه التهديدات ليست ظاهرة جديدة، إلا أنها تنتشر في الفضاء السيبراني بوتيرة سريعة وبقوة غير مسبوقة وعلى نطاق واسع. ويتّأتّى ذلك، سواء كان الأمر يتعلق بكميات المعلومات المسروقة من قبل القراصنة، أو زيادة هجمات برامج الفدية(*)، أو خروقات البيانات، أو الاحتيال المالي، أو التجسس الإلكتروني.

يمكن تفسير ذلك، شهدت هجمات برامج الفدية ـ على سبيل المثال ـ تصاعدًا كبيرًا، حيث يعتمد المتسللون على تشفير البيانات والمطالبة بفدية لإعادتها، مستهدفين الأفراد والمؤسسات، بما في ذلك البنية التحتية الحيوية؛ حيث ارتفعت هجمات برامج الفدية بأكثر من ١٥٠٪ في السنوات القليلة الماضية، مع الإبلاغ عن آلاف الهجمات سنويًا. ففي عام ٢٠٢٢، سجل باحثو التهديدات في معامل SonicWall(**) أكثر من ٤٩٣.٣ مليون محاولة هجوم ببرامج الفدية في جميع أنحاء العالم (جدول "٢" – شكل

(*) برامج الفدية هي عائلة من البرامج الضارة التي تستخدم تقنيات الأمان مثل التشفير لاختطاف ملفات المستخدم والموارد المرتبطة بها، ثم تطلب العملة المشفرة في مقابل البيانات المقفلة. تدخل بعض برامج الفدية إلى النظام باستخدام الهندسة الاجتماعية والإعلانات الضارة والرسائل غير المرغوب فيها والتنزيلات العشوائية، بينما تحاول برامج أخرى اكتشاف نقاط الضعف لاستغلالها، باستخدام المنافذ المفتوحة أو استغلال الباب الخلفي للدخول.

(**) تعمل SonicWall في مجال الأمن السيبراني؛ حيث تقدم خدماتها وبرامج الحماية للشركات والحكومات والشركات الصغيرة والمتوسطة في جميع أنحاء العالم، من خلال الحماية السلسة التي توقف الهجمات السيبرانية الأكثر مراوغة.

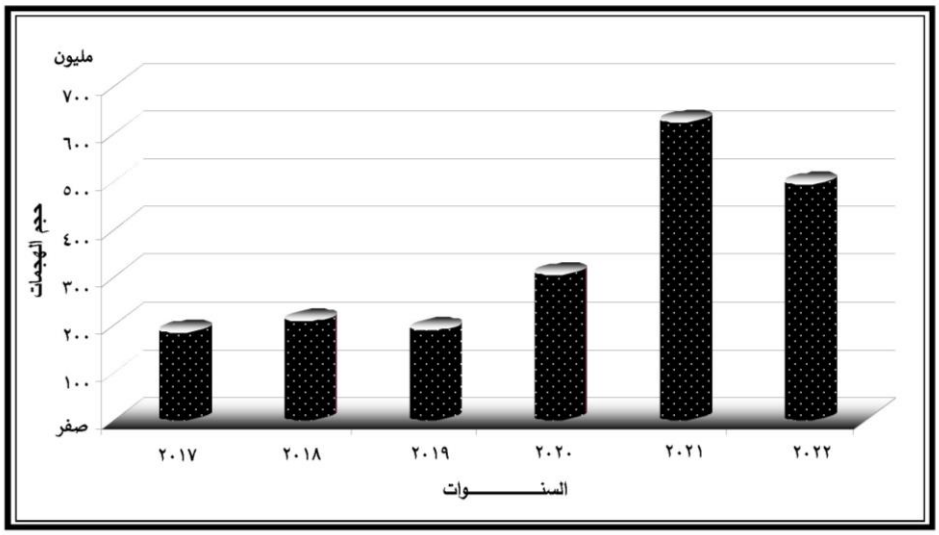
"٤"). ورغم انخفاض عدد الهجمات بنسبة٢١٪ مقارنة بعام ٢٠٢١، الذي سجل حوالي ٦٢٣.٣ مليون محاولة هجوم، إلا أن عام ٢٠٢٢ كان لا يزال ثاني أعلى عام على الإطلاق في عدد هجمات برامج الفدية عالمياً. وهو أقرب كثيرًا إلى حجم الهجمات الهائل الذي شهده العالم في عام ٢٠٢١ مقارنة بالأعوام السابقة، متجاوزًا عام ٢٠١٧ بأكثر من ١٥٥٪، وعام ٢٠١٨ بأكثر من ١٢٧٪، وعام ٢٠١٩ بأكثر من ١٥٠٪، وعام ٢٠٢٠ بأكثر من ٥٤٪.

الجدول (٢)

حجم هجمات الفدية العالمية في الفترة ما بين عامي (٢٠١٧ . ٢٠٢٢م) بالمليون دولار

العام	٢٠١٧	٢٠١٨	٢٠١٩	٢٠٢٠	٢٠٢١	٢٠٢٢
القيمة	١٨٣.٦	٢٠٦.٤	١٨٨	٣٠٤.٥	٦٢٣.٣	٤٩٣.٣

Source:- SonicWall. (2023). *Cyber threat report: Charting cybercrime's shifting frontlines*. SonicWall.



المصدر: الشكل من عمل الباحثين اعتمادًا علي الجدول رقم (٢)

شكل رقم (٤) حجم هجمات الفدية العالمية في الفترة ما بين عامي (٢٠١٧ . ٢٠٢٢م) بالمليون دولار

وقد قامت شركة RiskRecon ـ على مدى ثماني سنوات من يناير ٢٠١٦ إلى ديسمبر ٢٠٢٣ ـ بفهرسة وتحليل ١٤٥٤ حدثًا مدمرًا من أحداث برامج الفدية. وقد تجاوز تأثير العديد من هذه الحوادث نطاق الحدث نفسه، مما أبرز التداعيات الواسعة لهذه الهجمات على المؤسسات والأفراد. شملت هذه التداعيات؛ شللاً في آليات توصيل خدمات الطاقة والمرافق، وإغلاق العديد من المدارس والجامعات، وتعطيل قدرات المستشفيات، وتوقف إنتاج الغذاء، إلى جانب الإضرار بـ ٦٤ قطاعًا فرعيًا مختلفًا من قطاعات الصناعة. كما تأثرت سلاسل التوريد بشكل كبير نتيجة لهذه الهجمات. ومع انتهاء عام ٢٠٢٣، توسعت قائمة الضحايا لتشمل الكازينوهات والفنادق وإدارات الإطفاء والشرطة المحلية والزراعة، وحتى خطوط الرحلات البحرية والجوية، بالإضافة إلى العيادات الصحية لم تنجو من هذه الهجمات. ما ألحق أضرارًا بآلاف المؤسسات والمنظمات، متجاوزًا حدود الضحايا المباشرين (RiskRecon's leadership Team, 2024, pp. 3-5).

ومن أهم وأشهر الهجمات السيبرانية التي حدثت خلال العقدين الماضي والحالي ما يلي:

أ. الهجوم على شركة أرامكو السعودية أغسطس ٢٠١٢:

أصيبت شبكة الكمبيوتر التابعة لشركة أرامكو السعودية بفيروس قادر على التكاثر ذاتيًا في ١٥ أغسطس ٢٠١٢، فأصاب ما يصل إلى ثلاثين ألف جهاز كمبيوتر يعمل بنظام التشغيل ويندوز. وعلى الرغم من مواردها الهائلة باعتبارها شركة النفط والغاز الوطنية في المملكة العربية السعودية، فقد استغرقت أرامكو، وفقًا للتقارير، ما يقرب من أسبوعين للتعافي من الضرر. وكان من المثير للقلق أن يتم تنفيذ هجوم بهذا الحجم ضد شركة بالغة الأهمية لأسواق الطاقة العالمية. وقد أطلق على الفيروس

اسم "شمعون Shamoon"، وتسبب في تعطيل كبير لأكبر منتج للنفط في العالم، حيث عمد إلى الحذف العشوائي للبيانات من محركات الأقراص الصلبة لأجهزة الكمبيوتر. ورغم أن هذا الهجوم لم يسفر عن تسرب نفطي أو انفجار أو أي خلل كبير آخر في عمليات أرامكو، إلا أنه أثر بشكل ملحوظ على الأنشطة التجارية للشركة، ومن المرجح أن بعض بيانات الحفر والإنتاج قد فُقدت (Bronk & Tikk-Ringas, 2013, pp. 81-82).

وقع هذا الحادث بعد سنوات من التحذيرات المتكررة بشأن مخاطر الهجمات الإلكترونية على البنية التحتية الحيوية. وعلى مدى عقود، كانت حماية العمليات البترولية في المملكة العربية السعودية من الهجمات المادية تشكل أولوية قصوى لكل من الرياض وواشنطن. وذلك لأن أي تعطيل جزئي لمرافق الإنتاج في منطقة مثل المنطقة الشرقية من المملكة، قد يؤدي إلى تأثيرات فورية على إمدادات النفط وأسعاره، مما ينعكس بشكل غير مباشر على الاقتصاد العالمي. ورغم أن فيروس شمعون لم يتسبب في أضرار مادية لمرافق إنتاج أرامكو، إلا أنه أثر على تقييم المخاطر المتعلقة بالبنية التحتية الحيوية على مستوى العالم. وكان الحادث ذا خطورة كافية دفعت وزير الدفاع الأميركي آنذاك "ليون بانيتا Leon Panetta" إلى وصف الفيروس بأنه "متطور للغاية" ويثير "قلقاً هائلاً"، وذلك في كلمته أمام قادة الأعمال في نيويورك. كما أشار بانيتا إلى أن "هناك عدداً قليلاً من البلدان في العالم لديها القدرة في تطوير مثل هذه الفيروسات" (Reuters, 2012). وساعدت تعليقاته في تحفيز التكهنات بأن الهجوم نفذته إيران.

ب. هجمات الفدية WannaCry في عام ٢٠١٧:

يعد أحد أكبر وأقدم هجمات برامج الفدية حول العالم، ويسلط الضوء على التهديد السيبراني المتنامي، والذي يبدو وكأنه كامن في الخلفية ويتطور تدريجياً في المكان والزمان بطريقة غير خطية(*)، مع تلقيه مستويات متفاوتة من الاهتمام حتى تحين لحظة الهجوم. ففي ١٢ مايو ٢٠١٧، تفاجأ عدد كبير من المستخدمين عند تشغيل أجهزة الكمبيوتر الخاصة بهم، ليجدوا هذه الرسالة على شاشاتهم: "آه، لقد تم تشفير ملفاتك!" "Oops, your files have been encrypted!". كانت الرسالة مصحوبة بموعد نهائي محدد بثلاثة أيام، كان على المستخدم أن يدفع فدية قدرها ٣٠٠ دولار أمريكي بعملة البيتكوين المشفرة لفك تشفير ملفاته. وحذرت الرسالة من أنه إذا لم يتم الدفع خلال المهلة المحددة، فإن قيمة الفدية ستتضاعف. وفي حال تجاوز الموعد النهائي الممتد لسبعة أيام دون دفع، فسيتم حذف الملفات المشفرة بشكل نهائي (Prevezianou, 2021, p.38).

لقد وقع هؤلاء المستخدمون ضحية لفيروس الفدية "Cryptoworm"، المعروف الآن باسم WannaCry، وهو برنامج خبيث مكّن المتسللين من تشفير بيانات المستخدمين. حيث أطلق المهاجمون دودة التشفير WannaCry Ransomware، والتي اخترقت الأنظمة الضعيفة عن بُعد عبر الإنترنت، ونسخت نفسها للانتشار من جهاز كمبيوتر مصاب إلى آخر. انتشر الفيروس بمعدل ١٠.٠٠٠ جهاز في الساعة، مما أدى إلى إصابة أكثر من ٢٣٠ ألف جهاز كمبيوتر يعمل بنظام Windows، في ١٥٠ دولة حول العالم في غضون يوم واحد (Prevezianou, 2021, p.40).

(*) فإن الأزمات السيبرانية ليس لها بداية أو نهاية واضحة، وقد تستمر في الغليان لفترة طويلة بعد انتهاء "المرحلة الساخنة" من "الأزمة".

كان انتشار الفيروس غير مسبوق، حيث تأثر العديد من المستخدمين الأفراد والمنظمات حول العالم بالهجوم، بما في ذلك مشغلو البنية التحتية الحيوية، والشركات المصنعة، ومقدمو الخدمات. وقد تم ضبط أنظمتهم بحيث تتوقف عن العمل ـ ما لم يدفعوا الفدية، وحتى في حالة الإستجابة للتهديد، لم يكن بوسع أحد أن يضمن إمكانية استعادة الأنظمة بعد دفع الفدية. ومن أبرز الأمثلة على المنظمات التي تأثرت بهذا الهجوم (BBC News, 2017):

- هيئة الخدمات الصحية الوطنية البريطانية.
- وزارة الصحة والخدمات الإنسانية الأمريكية.
- وزارة الداخلية الروسية، والعديد من البنوك، وميجافون MegaFon.
- ثاني أكبر شركة لتشغيل الهواتف المحمولة في روسيا.
- السكك الحديدية الألمانية.
- شركة الهاتف الإسبانية تليفونيكا Telefonica، وشركة الطاقة إيبردرولا Iberdrola.
- ومقدم الخدمات العامة جاز ناتشرال Gas Natural.
- شركة تصنيع السيارات الفرنسية رينو Renault.
- الجامعات الصينية.
- ٦٠٠ شركة يابانية.
- المستشفيات الإندونيسية.
- شرطة ولاية أندرا براديش Andhra Pradesh في الهند.
- شركة الشحن المتعددة الجنسيات FedEx .

تسبب هذا العطل في خسائر اقتصادية كبيرة، قُدِّرَت بنحو ٨ مليارات دولار أميركي، وفقًا لتقرير صادر عن شركة "لويدز أوف لندن Lloyd's of London" للتأمين، بالتعاون مع شركة نمذجة المخاطر "ساينس Cyence". ولم يقتصر التأثير على الجانب الاقتصادي فحسب؛ بل كان الهجوم بمثابة جرس إنذار عالمي، حيث أظهر كيف يمكن لأزمة خفية في الفضاء الإلكتروني أن تُحدث تداعيات كبيرة في "العالم الحقيقي" (Barlyn, 2017).

ج. الهجوم السيبراني على خط أنابيب كولنيل(*) Colonial Pipeline للنفط:

يعد هذا الهجوم أكبر الهجمات السيبرانية التي استهدفت البنية التحتية للطاقة في الولايات المتحدة. ففي صباح ٧ مايو ٢٠٢١، تعرضت شركة أنابيب كولنيل لهجوم بواسطة مجموعة القرصنة "دارك سايد DarkSide"، التي تمكنت من اختراق أنظمة المعلومات الخاصة بالشركة. وطالب المبتزون بـ ٧٥ بيتكوين (بقيمة حوالي ٤.٤ مليون دولار في ذلك الوقت) مقابل أداة فك التشفير اللازمة لفتح قفل البيانات، مما اضطر الشركة إلى إيقاف خط الأنابيب بالكامل كإجراء احترازي لحماية باقي النظام. تسبب الإغلاق على الفور في توقف إمدادات نقل الوقود، مما أثر على حوالي ٤٥٪ من إمدادات الوقود في الساحل الشرقي الأمريكي (١٣ ولاية وعاصمة البلاد ـ شكل "٥") (Gawazah, Rondla, & Abalhareth, 2024, pp. 2-5).

(*) تأسست شركة Colonial Pipeline في عام ١٩٦٢، وكانت شركة خاصة، ولعبت دورًا حاسمًا في البنية التحتية للطاقة الوطنية في الولايات المتحدة الأمريكية؛ حيث قامت الشركة بتشغيل أكبر نظام لخطوط أنابيب المنتجات البترولية المكررة في الولايات المتحدة، والتي يبلغ طولها ٥٥٠٠ ميل من هيوستن إلى ميناء نيويورك. وتقوم الشركة بتسليم أكثر من ١٠٠ مليون جالون من الوقود يوميًا للعملاء في جميع أنحاء الـ١٤ ولاية، وتخدم ٢٨ مصفاة ونحو ٥٠ منشأة عسكرية ومطارات رئيسية.

تفاقمت الأزمة على مدار الأيام التالية للهجوم؛ حيث نفذت كميات الوقود في محطات عديدة، واصطفت الطوابير الطويلة أمام المحطات، وارتفعت أسعار الوقود، وأعادت شركات الطيران توجيه الرحلات، وأعلنت حكومة الولايات المتحدة حالة طوارئ إقليمية للحفاظ على تدفق الوقود. ومع بقاء أحد أهم خطوط الأنابيب في العالم خارج نطاق العمل، كشف الهجوم عن نقاط ضعف في البنية التحتية المتقادمة للطاقة في أمريكا، فرغم أن كولنيل اضطرت إلى دفع الفدية للحصول على أداة فك التشفير، إلا أن الأداة كانت بطيئة في استعادة النظام، لذا اعتمدت الشركة على النسخ الاحتياطية لإعادة تشغيل العمليات تدريجيًا (Gawazah et al., 2024, pp. 2-5).

Source:
Gawazah, L., Rondla, A., & Abalhareth, M. S. (2024). *To pay or not to pay: The US Colonial Pipeline ransomware attack*. Thunderbird School of Global Management, Arizona State University, p. 9. https://www.researchgate.net/publication/383206534_To_Pay_or_Not_to_Pay-_The_US_Colonial_Pipeline_Ransomware_Attack.

شكل (٥) خط أنابيب كولنيل في شرق الولايات المتحدة الأمريكية

أعلن الرئيس السابق جو بايدن ـ استجابة لهذا الحدث ـ حالة الطوارئ لرفع القيود على نقل الوقود من الولايات غير المتضررة عن طريق البر، بهدف التخفيف من حدة نقص الإمدادات. كما وقع أمرًا تنفيذيًا يهدف إلى تعزيز الأمن السيبراني في البلاد. وعلى صعيد آخر، دعا روسيا إلى تحمل مسؤوليتها تجاه الأنشطة التي تقوم بها مثل هذه المجموعات السيبرانية، والتي تتخذ من أراضيها قاعدة لتنفيذ هجماتها (The White House, 2021).

هذا، وقد استند الباحثان في مناقشة أثر الفضاء السبيراني على أمن وسيادة الدول إلى مجموعة من الأمثلة الحديثة، مثل تسريبات ويكيليكس، ومخاطر عمليات القرصنة الإلكترونية على استقرار النظام المالي العالمي، ودور وسائل التواصل الاجتماعي في زعزعة استقرار الدول. ومع ذلك، فإن هذه الأمثلة ليست استثناءً، حيث تعج وسائل الإعلام بأخبار مماثلة عن الحروب الافتراضية والهجمات السيبرانية، التي أصبحت محور اهتمام متزايد من قبل المشرعين والمنظمين على مستوى العالم.

تزداد تحديات الفضاء السيبراني تعقيدًا بسبب صعوبة تحديد وإثبات مصدر الهجوم، وعدم القدرة على توقعه أو منعه أو إيقافه، فضلاً عن الالتباس بشأن قضايا السيادة والاختصاصات القضائية. يضاف إلى ذلك التطور السريع للتكنولوجيا، وإعادة التشكيل المستمر للشبكات، وإمكانية تطوير أسلحة سيبرانية تجريبية، مع صعوبة إجراء تجارب ميدانية لها وعدم اليقين بشأن آثارها. كما أن الاستراتيجيات التي تعتمدها الدول لحماية سيادتها وتعزيز قوتها في الفضاء السيبراني تؤدي إلى تداعيات جيوسياسية جديدة، تثير بدورها مزيدًا من التحديات والتهديدات. كل ذلك يشير إلى وجود درجة كبيرة من عدم اليقين بشأن المخاطر المحتملة للكوارث السيبرانية، وما قد تحمله

الأحداث المستقبلية في هذا المجال، مما يجعلها أكثر غموضًا مقارنةً بأي تهديدات أخرى.

وتعزز الطبيعة اللامحدودة للفضاء السيبراني الشعور بعدم الارتياح، مما دفع العديد من الحكومات إلى تبني سياسات وإجراءات تضمن الحفاظ على سيادتها وحماية مصالحها داخل هذا الفضاء اللامحدود. وتتأتّى المصداقية في تحقيق هذه الإجراءات على أرض الواقع من عدة حقائق، أهمها: أن السيادة الجغرافية تظل مفهومًا أساسيًا حتى في الفضاء السيبراني. كما أن هذا الفضاء، رغم طبيعته الإفتراضية، هو في النهاية نتاج ابتكار بشري، يتطلب بنية تحتية ملموسة تخص كيانات قانونية أو مادية، مثل الشركات أو الحكومات. وبالتالي، تصبح حماية هذه البنية التحتية جزءًا أساسيًا من حماية السيادة الوطنية للدولة داخل حدودها الجغرافية.

ويسهم تقدم التقنيات وتطوير السياسات الوطنية في تمكين الدول من فرض سيطرتها على الإنترنت وحماية مصالحها الوطنية، وإن كان ذلك يتطلب توازنًا دقيقًا بين متطلبات الأمن وحماية الحريات وحقوق الأفراد. ويعتبر جدار الحماية الصيني مثالًا بارزًا على قدرة دولة على ممارسة سيادتها السيبرانية. يعتمد هذا النظام على مجموعة من التقنيات التي تُستخدم لتقييد الوصول إلى المحتوى وفقًا للسياسات المحلية. ورغم وجود تحديات تواجهه، مثل استخدام الشبكات الافتراضية الخاصة (VPN)للالتفاف عليه، إلا أنه أثبت فعالية نسبية في التحكم بتدفق المعلومات داخل حدود الدولة (Midson, 2014, p.80).

المبحث الرابع: تحليل الفضاء السيبراني من منظور الصراع الدولي

يعتمد عالم اليوم بشكل أساسي على الفضاء السيبراني لتحقيق الأهداف الاقتصادية والاجتماعية والأمنية، مما يجعل حماية الأمن السيبراني وضمان حرية استخدامه يمثل أولوية قصوى للعديد من الدول. ومع ذلك، تواجه الدول في سبيل تحقيق هذه الأهداف العديد من التهديدات، جراء الأنشطة التي تُضعف أو تُعطل قدرتها على الاستفادة من الفضاء السيبراني، وتلجأ بعضها إلى تنفيذ عمليات عسكرية في هذا المجال لمواجهة هذه التحديات. وهنا تسهم الجيوبوليتيكا في فهم الصراعات التي تحدث في الفضاء السيبراني، فهي تعني في مفهومها التقليدي دراسة التنافس على السلطة والنفوذ داخل مناطق محددة، عبر مستويات متعددة، وتركز على ديناميكيات الصراع، وتمثيلات الأطراف المتنازعة، واستراتيجياتهم للسيطرة على المنطقة أو الاستحواذ عليها، وكذلك الدفاع عن مصالحهم ضمن النطاق الجغرافي المعني. وعند تطبيق هذا المنظور على الفضاء السيبراني، يفتح آفاقًا جديدة لفهم طبيعة الصراعات في العالم الرقمي، وربطها بالإطار المفاهيمي للجيوبوليتيكا، فكما كان الحال منذ العصور القديمة، ستظل العوامل الجيوبوليتيكية تؤثر وتوجه الشؤون العالمية في عصر الرقمنة، ولن تؤدي التقنيات الناشئة إلا إلى رفع الرهانات بين الدول.

وتبرز أهمية الجيوبوليتيكا في الفضاء السيبراني، وتزداد هذه الأهمية بشكل ملحوظ مع التقدم السريع في التقنيات المعتمدة على البيانات، مثل الذكاء الاصطناعي (AI). ويعود ذلك إلى ثلاثة أسباب رئيسية، وهي:-

أولًا: تمتلك الدول سلطة مباشرة على البنية التحتية للإنترنت ومقدمي الخدمات داخل حدودها. فالإنترنت، المدعوم بالكابلات البحرية العابرة للقارات، وأجهزة التوجيه الشبكية، ومراكز البيانات المتزايدة، يتمتع ببصمة مادية ضخمة تمنح الدول أدوات قوية في

عصر المعلومات. فعلى سبيل المثال، مرور معظم حركة الإنترنت عبر الولايات المتحدة يمنحها ميزة استراتيجية ميدانية.

ثانيًا: بات العالمان المادي والرقمي يتداخلان بشكل متزايد، حيث أصبحت التقنيات الرقمية الحديثة عنصرًا أساسيًا في معظم البنى التحتية للقرن الحادي والعشرين. وتشمل هذه الشبكات أنظمة حيوية مثل شبكات الكهرباء، ومراكز التحكم الصناعية، وشبكات مراقبة المدن، بالإضافة إلى أنظمة تحديد الهوية الوطنية والرعاية الصحية، مما يعكس التداخل العميق بين العالمين وأهمية التقنيات الرقمية في دعم وتشغيل هذه الأنظمة. ومن ثم لم يعد الفضاء السيبراني مجرد فضاء افتراضي للتبادل الرقمي كما كان يُعتقد في الماضي، بل تحول إلى قوة ذات تأثير ملموس في العالم الواقعي. هذا يعني أن الدول التي تملك القدرة على تطوير التقنيات السيبرانية المتقدمة ستتمكن من توسيع نفوذها الجيوبوليتيكي في العالم المادي.

ثالثًا: أدت كثافة الأنشطة الإلكترونية إلى جعل الفضاء السيبراني موقعًا استراتيجيًا بالغ الأهمية، حيث يمكن اعتباره مكافئًا للمساحات الجغرافية التقليدية مثل الأرض والبحر والجو والفضاء، مما يعكس الأهمية المتزايدة للفضاء السيبراني في تخطيط وتنفيذ الاستراتيجيات العسكرية الحديثة (Adams & Albakajai, 2016, 257). وبذلك، أصبح هذا الفضاء ساحة جديدة للصراعات الجيوبوليتيكية التقليدية.

وتتجلى بوضوح معالم خطوط التصدع الجيوسياسية الراهنة؛ حيث أدى الفضاء السيبراني إلى ظهور فرص وتحديات استراتيجية جديدة، وساهمت التغطية الإعلامية المتزايدة لمصطلح الحرب السيبرانية، في رفع مستوى الوعي العام بأن الفضاء السيبراني قد تحول إلى ساحة صراع حديثة. وأصبحت الحكومات تدرك بشكل متزايد، أهمية اتخاذ إجراءات حاسمة لمواجهة التهديدات الناشئة عن الفضاء السيبراني.

لذلك، نظرت الصين وروسيا ودول أخرى غير غربية ـ على مدى العقدين الماضيين ـ إلى الإنترنت كأداة للنفوذ الغربي، مما دفعها إلى معارضة هذا الواقع واستغلال الفضاء السيبراني لتعزيز مصالحها وأولوياتها الوطنية. ووفقًا لبحث حديث صادر عن المعهد الأسترالي للسياسة الاستراتيجية ASPI، يشارك عمالقة التكنولوجيا الصينيين في إنشاء أكثر من ٧٠ مدينة ذكية عبر أوروبا وأمريكا الجنوبية وأفريقيا، بالإضافة إلى ٥٢ مبادرة في مجال تقنية الجيل الخامس G5[*] في ٣٤ دولة. ونظرًا لأن الشركات الصينية ملزمة قانونًا بالتعاون مع وكالة الاستخبارات والأمن الصينية، فإن بصمتها العالمية تتيح للصين فرصًا واسعة للمراقبة والتجسس، مما يمنحها نفوذًا غير مسبوق للتدخل والضغط على الدول المستقبلة في حال توتر العلاقات (Mansted, 2019).

تؤكد العقيدة العسكرية الصينية على أهمية السيطرة على المعلومات في المراحل المبكرة من أي صراع، مشددة على ضرورة تحقيق النصر في ظل ما يُعرف بـ "الظروف المعلوماتية". ووفقًا لطبعة عام ٢٠٠١ من علم الاستراتيجية العسكرية، وهو بيان مؤثر صادر عن جيش التحرير الشعبي الصيني، يمكن للضربات الدقيقة في بداية الحرب أن "تشل العدو بضربة واحدة". وتُبرز النسخ المحدثة من هذه الاستراتيجية أهمية "القمع والتدمير الفعال" لأنظمة معلومات العدو، مع تعزيز "القدرة على حماية المعلومات". ويبدو أن الصين تعتقد أنها لا تستطيع تحقيق النصر إذا لم "تستولي على

[*] تمثل تقنيات الجيل الخامس الإطار الذي ستتكشف من خلاله الثورة الصناعية القادمة، فقد تم بناء هذه البنية الأساسية الجديدة لتلبية المتطلبات التقنية اللازمة لتطوير تقنيات متقدمة مثل الروبوتات عالية الدقة، والذكاء الاصطناعي، والمركبات ذاتية القيادة، إلى جانب الأجهزة التي تشكل إنترنت الأشياء.

زمام المبادرة في ساحة المعركة وتسيطر عليها، وشل وتدمير نظام العمليات لدى الخصم، وإضعاف إرادته في مواصلة الحرب" (Rovner, 2021).

تعتبر الولايات المتحدة توسّع تقنيات الجيل الخامس الصينية ليس مجرد تحدٍ اقتصادي، بل أيضًا تهديدًا جيوسياسيًا يمسّ مكانتها العالمية. هذا التوسع يُنظر إليه على أنه تحدٍ مباشر للتفوق التاريخي الذي لطالما تمتعت به الولايات المتحدة في مجال الابتكار التكنولوجي.

وتُعرِّف العقيدة العسكرية المشتركة للولايات المتحدة عمليات الفضاء السيبراني، على أنها "الاستخدام الموجّه للقدرات السيبرانية، بما في ذلك الشبكات وأجهزة الحاسوب والبرمجيات والبيانات، بهدف تحقيق أهداف محددة داخل الفضاء السيبراني أو من خلاله، لدعم العمليات العسكرية، وتعزيز الأمن القومي، وتحقيق الأهداف الاستراتيجية" (Mueller, Jensen, Valeriano, Maness, & Macias, 2023, p. 2). انطلاقًا من هذه الرؤية، أعلن الرئيس الأمريكي الأسبق باراك أوباما: "أن البنية التحتية الرقمية تُعد أحد المكونات الأساسية للاستراتيجية الوطنية"، وقام في ٢٣ يونيو ٢٠٠٩ بتأسيس قيادة العمليات السيبرانية (Cybercom)، وهي وحدة متخصصة داخل البنتاغون، تُكلّف بتنفيذ ما يُعرف بـ "عمليات الطيف الكامل" Perform Full Spectrum Operations في مجال الفضاء السيبراني. إضافةً إلى ذلك، كشفت وثائق مُسرّبة من وكالة الأمن القومي الأمريكية عن جهود مكثّفة يبذلها المسؤولون الأمنيون لتعزيز القدرات السيبرانية الهجومية، بما يضمن قدرة الولايات المتحدة على التصدي للتحديات المستقبلية وتحقيق التفوق في هذا المجال الحيوي (Robinsona et al., 2015, p.2).

من جانبها، سعت روسيا إلى دمج عمليات الفضاء السيبراني مع الهجمات التقليدية، رغم أن النتائج كانت متباينة في حالات مثل جورجيا وأوكرانيا، إلا أن العمليات السيبرانية – من وجهة نظر الاستراتيجيين الروس – تهدف إلى إرباك العدو وإضعافه قبل اندلاع الصراع، ومن ثم تحييد أنظمة القيادة والسيطرة التابعة له خلال العمليات العسكرية (Rovner, 2021).

وفي المملكة المتحدة، دقّ المسؤولون الحكوميون ناقوس الخطر بشأن ضعف الاستعداد لمواجهة الحروب السيبرانية، مما دفع إلى إطلاق استثمارات جديدة لتعزيز الدفاع، مثل برنامج الأمن السيبراني الوطني. من جهته، عمل حلف شمال الأطلسي (الناتو) على زيادة الوعي بالقوانين المطبقة على الصراعات السيبرانية، وذلك من خلال إصدار دليل "تالين Tallinn"، الذي يُقدم إرشادات للدول حول كيفية التحرك بشكل قانوني في هذا المجال المستجد (Robinsona et al., 2015, p.2).

وعلى الرغم من الاستثمار الكبير في تكنولوجيا الجيل الخامس في العديد من الدول الأعضاء، فإن الاتحاد الأوروبي يكافح من أجل إيجاد مكان له في هذه البيئة المتغيرة، لإن السباق نحو الجيل الخامس يوفر للاتحاد الأوروبي فرصة ممتازة لتعزيز سيادته التكنولوجية، من خلال استراتيجية مشتركة تجاه شركات الاتصالات الأجنبية وسياسة متماسكة للأمن السيبراني (Mariani, & Bertolini, 2019, P. 1).

تعكس هذه التطورات حجم القلق العالمي المتزايد بشأن الحرب السيبرانية، وتؤكد الحاجة المُلحّة لتعزيز الاستعدادات الدفاعية والهجومية في مواجهة هذا النوع من التهديدات، الذي يعيد تشكيل ديناميكيات الأمن الدولي. فبالنسبة للكثيرين، تُعد العمليات السيبرانية أداة لتحقيق ميزة حاسمة وخلق مسار سريع نحو النصر. وكما أشار

"جوش روفنر[*] Joshua Rovner"، فإن هذه العمليات تمثل لصنّاع السياسات والمخططين "وسيلة منخفضة التكلفة لتحقيق انتصارات سريعة وحاسمة" (Rovner, 2021).

وتُعد نظرية الحرب السيبرانية مشروعًا قيد التطوير، إلا أن ملامحها الأساسية بدأت تتبلور خلال الحقبة الأخيرة. وتتمحور الفرضية الرئيسية في هذه النظرية، حول أن الفضاء السيبراني سيصبح وسيلة فعّالة لتحقيق الأهداف الجيوبوليتيكية في المستقبل، من خلال زعزعة استقرار الدول المعادية. فالنظرية في جوهرها تعني باستغلال نقاط الضعف الكامنة في هذه الدول، حيث تهدف الهجمات السيبرانية في نهاية المطاف إلى دفع الخصم نحو حالة من "الانتروبيا"، عبر إحداث صدمة نظامية في الهياكل المؤسسية للخصم (Kallberg, 2016, p. 123).

تم توسيع هذه الفكرة بشكل أوضح في نظرية "جان كالبرج Jan Kallberg" حول العمليات السيبرانية الحاسمة. يرى كالبرج، الباحث السابق في معهد الجيش السيبراني في ويست بوينت، أن "النتيجة السيبرانية الحاسمة يمكن تحقيقها عبر الهجمات السيبرانية، سواء من خلال إضعاف القدرات العسكرية للخصم أو زعزعة استقرار المجتمع المستهدف". تعتمد هذه الاستراتيجية على استغلال "الانتروبيا الخاملة[**] Dormant Entropy" الكامنة في الدول التي تعاني من ضعف مؤسساتها، مما يؤدي إلى إضعاف قدرتها على التصدي للهجمات السيبرانية أو مواجهة

(*) الأستاذ المساعد في كلية الخدمة الدولية بالجامعة الأمريكية، وعمل باحثًا مقيمًا في وكالة الأمن القومي وقيادة الأمن السيبراني الأمريكية في عامي (٢٠١٨-٢٠١٩).

(**) أصل المصطلح مأخوذ عن اليونانية، ويُستخدم في الفيزياء والمجالات المرتبطة بها، للإشارة إلى حالة من الاعتلاج أو القصور الحراري. ومعناها تحول أو تلاشى النظام كله، ليتحوَّل إلى كتلة من المادة الخاملة التي لا حراك فيها.

التهديدات الداخلية بفعالية. إن الصراع السيبراني على المستوى الاستراتيجي لن يكون له جدوى أو تأثير حقيقي، إذا لم تُسفر الهجمات السيبرانية عن نتائج ملموسة تؤثر على المجتمع المستهدف بشكل مباشر (Kallberg, 2016, p. 123).

يُعد استهداف البنية المؤسسية لدولة معادية ـ في نظرية الحرب السيبرانية الاستراتيجية ـ وسيلة فعّالة لزعزعة استقرارها، مما يمهد الطريق لإخضاعها للإرادة الأجنبية. وتعتمد هذه الاستراتيجية على هجمات سيبرانية ممنهجة ومتعمدة، تستغل عنصر المفاجأة وسرعة التنفيذ، مما يجعلها تسبق قدرة القيادات على إدراك المشهد الاستراتيجي أو اتخاذ إجراءات مضادة. ومن ثم تتسبب في إحداث صدمة للمجتمع المستهدف، بحيث يدفع المجتمع إلى تخطي نقطة الانهيار الحاسمة أو عتبة الإنتروبيا، ويحول دون تمكين النظام الحاكم من تطوير تدابير دفاعية أو تشكيل قيادة سيبرانية دفاعية متماسكة (Sharma, 2010, pp. 63-68).

يكمن الهدف من هذه الاستراتيجية، هو تعزيز شعور المواطنين بعدم كفاءة النظام في حماية مؤسساته، وتحميله مسؤولية انهيار البنية المجتمعية، مما يشكل تحديًا غير مباشر للسلطة ويزيد احتمالات الفوضى الداخلية. وقد يؤدي ذلك إلى تداعيات خطيرة مثل اندلاع حرب أهلية، أو انهيار النظام، أو تغييرات عنيفة في بنيته.

إن هذه الاستراتيجية في الحقيقة هي نفسها التي استخدمتها دول الحلفاء والمحور في الحرب العالمية الثانية (١٩٣٩–١٩٤٥)، كان القصف الاستراتيجي وسيلة أساسية استهدفت البنية التحتية الخدمية والصناعية والسياسية للعدو، بدلاً من الأهداف العسكرية البحتة. وشمل القصف استهداف السكك الحديدية والموانئ والمدن والمناطق السكنية، وغالبًا المدنيين، بهدف إرهابهم وتعطيل الحياة اليومية. وبلغت الغارات الجوية ذروتها بالقصف الأمريكي الناري والذري لهيروشيما وناجازاكي.

يشير "كولن إس جراي Colin S. Gray" ـ أستاذ السياسة الدولية والدراسات الاستراتيجية في جامعة "ريدينغ Reading" بإنجلترا ـ إلى أن القوة السيبرانية تُعد في الأساس أداة تمكين للعمليات العسكرية المشتركة. ورغم أن طبيعة القوة السيبرانية تحمل خصوصياتها، إلا أن تعاملها ضمن سياق استراتيجي يجعلها امتدادًا لمفاهيم القوة التقليدية. كما يؤكد جراي أن الفضاء السيبراني، بكل أبعاده التكنولوجية والنفسية والسياسية والعسكرية، يخضع لإطار النظرية العامة للاستراتيجية، مما يعزز من أهميته كعنصر رئيسي ضمن الفكر الاستراتيجي الحديث (Gray, 2013, p. 12).

ويبدو أن الفضاء السيبراني يحمل العديد من التحديات التي أصبحت واقعًا مفروضًا. ففي عالم تآكل فيه مبدأ النظام الويستفالي في ترسيخ سيادة الدولة على أراضيها، وتراجعت فيه هيمنة فكر "كلاوزفيتز(*) Clausewitz" في الاستراتيجية العسكرية، تبرز تحديات جديدة يفرضها الصراع السيبراني، أخطرها أنه لا يمكن تحديد هوية الخصم بدقة مما يعقد عملية تقييم قدراته، بالإضافة إلى أن الأهداف ليست ثابتة، بل تتغير باستمرار مما يحد من إمكانيات المناورة التقليدية، كما أن غياب معايير واضحة لقياس فعالية العمليات، يجعل من الصعب على الدول تقييم التأثير الحقيقي لها ضمن الأطر الزمنية القصيرة. علاوة على ذلك، تؤدي سرعة التنفيذ في العمليات السيبرانية إلى خلق معارك تُدار غالبًا بواسطة أنظمة آلية وليس البشر. كل هذه العوامل تجعل التفكير العسكري التقليدي غير ملائم في الفضاء السيبراني، وإذا تم الاعتماد عليه لصياغة استراتيجية سيبرانية، فمن المرجح أن يقود إلى افتراضات خاطئة

(*) نسبة إلى "كارل فون كلاوزفيتز Carl von Clausewitz"، وهو جنرال ومؤرخ حربي ألماني. تركت كتاباته حول الفلسفة والتكتيك والإستراتيجية أثرا عميقاً في المجال العسكري في البلدان الغربية. تدرس أفكاره في العديد من الأكاديميات العسكرية، ويعتبر من أكبر المفكرين العسكريين شهرة وتأثيراً على مر التاريخ.

ويقلل من فعالية العمليات الهجومية كأداة جيوبوليتيكية (Kallberg, 2016, p. 125).

إن استخدام الأسلحة الإلكترونية لإحداث الضرر بات حقيقة لا يمكن إنكارها. وكجزء من تصنيفها، تُعد الأسلحة الإلكترونية أكثر انتشارًا وتدخلاً مقارنة بأنواع الأسلحة الأخرى التي يمكن تصنيفها بيئيًا. ومع ذلك، تشترك الأسلحة الإلكترونية في التطبيق التكتيكي كأداة للسياسة والاستراتيجية، جنبًا إلى جنب مع القوة البرية والبحرية والجوية والفضائية. ورغم التحدي الذي تواجهه هذه التصنيفات الجغرافية بسبب الطبيعة المتداخلة والمشتركة للعمليات العسكرية الحديثة، فإن هذا التشابك لا يلغي أهمية التمييز بين المجالات الخمسة للحرب (الأرض، البحر، الجو، الفضاء، والفضاء السيبراني)، ولا يُبطلها. في نهاية المطاف، تخضع جميع الأسلحة والجهود الاستراتيجية، بغض النظر عن المجال الجغرافي الذي تنتمي إليه، لإطار موحد من النظرية العامة للاستراتيجية. وتتماشى هذه القراءة مع الفهم الكلاوزفيتزي للاستراتيجية، باعتبارها "توجيه واستخدام القوة، أو التهديد باستخدامها، لتحقيق أهداف السياسة كما تحددها السياسة"، مما يعكس الأصول التقليدية للاستراتيجية وتطبيقاتها الحديثة (Gray, 2013, p. 12).

لذلك، أصبحت الدول والمجتمعات غير الحكومية والشركات والمؤسسات الأكاديمية والأفراد، تشارك بشكل غير مسبوق في العمليات السيبرانية لتعزيز مصالحها الاستراتيجية، إلى حد لم يكن من الممكن تصوره من قبل. وفي الوقت ذاته، زاد الاعتماد العسكري على أنظمة الكمبيوتر والشبكات بشكل كبير، مما أدى إلى ظهور المجال الخامس للمعركة، وهو الفضاء السيبراني، ليضاف إلى المجالات التقليدية المعترف بها: البر، والبحر، والجو، والفضاء الخارجي.

أدى هذا التطور إلى تغيّر جذري في مشهد الحروب، وظهور عقائد عسكرية جديدة مثل الحرب المتمحورة حول الشبكات، فضلاً عن أشكال الصراع غير التقليدية، بما في ذلك الحرب الهجينة، والحرب المعلوماتية، والحرب غير المتكافئة. ويؤكد "إلكسندر كوسينكوف Alexander Kosenkov" بشكل خاص على ظهور الصراع السيبراني وتصاعده، والذي يُعرَّف على أنه استخدام استراتيجي للقدرات السيبرانية، لتحقيق أهداف داخل الفضاء السيبراني أو من خلاله، مما يجعله تهديداً عالمياً محورياً ومتزايداً (Kosenkov, 2016, P.1). وفي هذا السياق، تسعى الدول إلى تطوير ونشر أدوات جديدة للسيطرة على الساحة السيبرانية، وفي كثير من الحالات تطمح بوضوح إلى أن تصبح اللاعب الرئيسي فيه. ونتيجة لذلك، أصبحت الاستعدادات للحرب السيبرانية جزءاً مهماً من بناء الجيوش في عدد غير قليل من البلدان.

ومن ثم أصبحت أهمية الفضاء السيبراني وفعالية استراتيجيات الردع السيبراني ذات أولوية قصوى، حيث تؤدي دورًا محوريًا في تشكيل الجغرافيا السياسية للعالم المعاصر. ولفهم كيفية تأثير النشاط السيبراني على الدوافع الجيوبوليتيكية والصراع العالمي، من المفيد رؤيتها على أرض الواقع، من خلال سلسلة من الأمثلة الواقعية التي شهدتها السنوات القليلة الماضية، وتوضح كيف أصبح الفضاء السيبراني أداة أساسية لتحقيق الأهداف العسكرية. كما توضحها أمثلة عديدة من الهجمات الإلكترونية. وذلك من خلال العرض التالي:

أ. الهجوم على البرنامج النووي الإيراني بفيروس "ستوكسنت Stuxnet" الخبيث:

لعبت الولايات المتحدة في عام ٢٠١٠ دوراً رئيسياً فيما وصفه العديد من الخبراء بأنه الخطوة الأولى في "الحرب السيبرانية". وكان هذا بمثابة تجربة أو محاولة

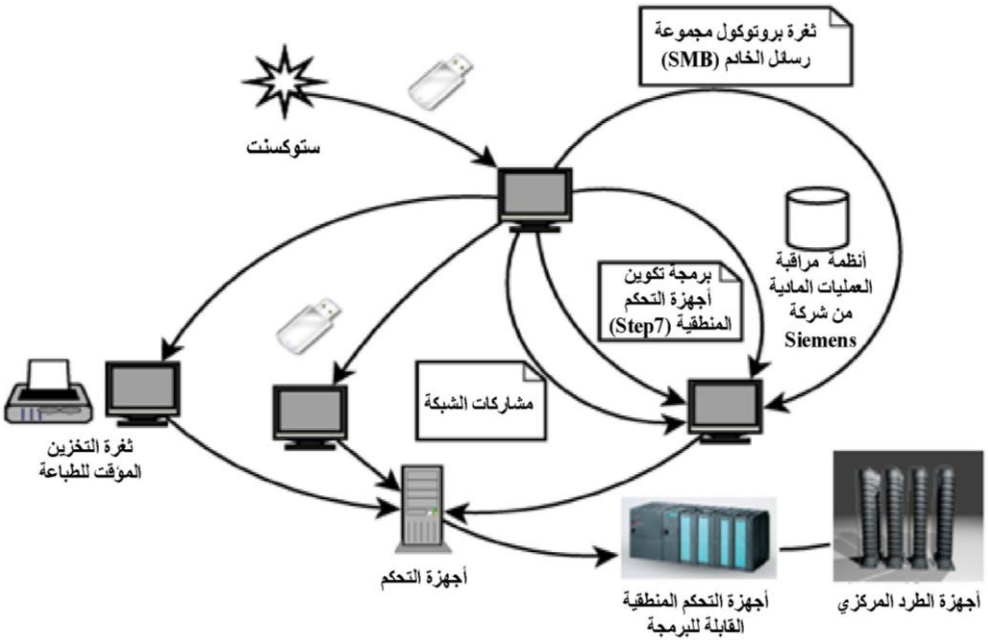
لاستكشاف "الطريق الثالث" الذي يقع بين الدبلوماسية القسرية والهجوم العسكري التقليدي (Douzet, 2014, p.12).

حيث تم اكتشاف دودة "ستوكسنت Stuxnet" على أحد أجهزة كمبيوترات البرنامج النووي الإيراني، مما أثار دهشة خبراء الأمن السيبراني بفضل تطورها، واستخدامها لأربع ثغرات أمنية غير معروفة سابقًا. وعلى عكس البرمجيات الخبيثة التقليدية، لم يكن الهدف من "ستوكسنت" التجسس، بل التخريب المباشر لأجهزة الطرد المركزي المستخدمة في منشآت الطاقة النووية الإيرانية في "نطنز Natanz". تشير التقارير إلى أن الولايات المتحدة، بدعم من إسرائيل، طورت "ستوكسنت" لتعطيل أو تأخير البرنامج النووي الإيراني. ويُعتقد أن الدودة تم زرعها في شبكة محطة الطاقة باستخدام محرك أقراص USB مخترق، وهي تقنية سمحت للفيروس بالوصول إلى شبكة كانت معزولة عن الشبكات الأخرى، ما جعل الهجوم السيبراني ممكنًا في ظل هذه الظروف الأمنية المشددة؛ حيث أثرت على المنشآت النووية الإيرانية آنذاك (Baezner & Robin, 2017, p.4).

قام "ستوكسنت" بمهاجمة جميع طبقات البنية الأساسية المستهدفة، بدءًا من نظام التشغيل Windows، مرورًا ببرامج Siemens التي تتحكم في أجهزة التحكم المنطقية القابلة للبرمجة، وصولًا إلى البرامج المدمجة داخل تلك الأجهزة (شكل "٦"). وقد عمل "ستوكسنت" على تغيير برمجة أجهزة التحكم المنطقية القابلة للبرمجة، مما تسبب في دوران أجهزة الطرد المركزي بطريقة غير منتظمة، ما أدى إلى تلفها أو تدميرها أثناء العملية. وأثناء حدوث ذلك، كانت أجهزة التحكم المنطقية تزود الكمبيوتر المركزي بمعلومات خاطئة، تفيد بأن كل شيء يعمل بشكل طبيعي، مما صعّب اكتشاف

المشكلة أو تشخيصها إلا بعد فوات الأوان (Mueller & Yadegari, 2012, p.10).

رفضت إيران إصدار أي تفاصيل دقيقة حول آثار الهجوم آنذاك لدواعي أمنية، إلا أن التقديرات الحالية تشير إلى أن دودة "ستوكسنت" تسببت في تدمير ٩٨٤ جهاز طرد مركزي لتخصيب اليورانيوم، مما أدى إلى انخفاض كفاءة عملية التخصيب بنحو ٣٠٪ على أقل تقدير (Holloway, 2015). وقد دفع هذا الهجوم السيبراني إلى إحداث تغييرات جذرية في السياسات والاستراتيجيات السيبرانية للدول (Baezner & Robin, 2017, p.5).



Source:
Mueller, P., & Yadegari, B. (2012). *The Stuxnet worm*. University of Arizona. P. 4. https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/topic9-final/report.pdf

شكل (٦) ثغرات وصول ستوكسنت إلى أجهزة التحكم المنطقية القابلة للبرمجة المستهدفة

ب. عملية تفخيخ أجهزة اتصالات حزب الله اللبناني:

شهد لبنان في يوم الثلاثاء ١٧ سبتمبر ٢٠٢٤ انفجارًا واسع النطاق، استهدف قُبيل الساعة الثالثة والنصف عصرًا، آلاف أجهزة النداء pager وأجهزة الاتصال اللاسلكي التي يستخدمها مقاتلو حزب الله. بدأت أجهزة النداء في إطلاق صافرات الإنذار، ما بدا في البداية كرسالة عادية من قيادة الحزب، ولكن بعد ثوانٍ قليلة، انفجرت الأجهزة بشكل متزامن، متسببة في سقوط عدد كبير من القتلى والجرحى في مختلف أنحاء البلاد. وفي اليوم التالي، وقع هجوم ثانٍ استهدف أجهزة الاتصال اللاسلكي، مما زاد من حجم الكارثة. وأسفرت الهجمات المنسقة عن مقتل ٣٧ شخصًا وإصابة الآلاف، من بينهم أطفال، وفقًا لبيان صادر عن وزارة الصحة اللبنانية (Miller, Brown, Morris, Rubin, & Swaine, 2024).

وذكرت وكالة رويترز: أن قيادة حزب الله كانت قد وضعت خطة حرب في فبراير ٢٠٢٤، تهدف إلى معالجة الثغرات في بنيتها التحتية الاستخباراتية. تضمنت الخطة التحول إلى استخدام أجهزة تناظرية مثل الهواتف الأرضية وأجهزة النداء اللاسلكية، في محاولة لتجنب عمليات المراقبة المتطورة التي تنفذها إسرائيل، تلك العمليات التي أسفرت عن مقتل حوالي ١٧٠ شخصًا من كبار قادة الجماعة في غارات مستهدفة. وكجزء من هذه الخطة، استورد حزب الله نحو ٥ آلاف جهاز استدعاء "بيبجر pagers" طراز (AR-924)، من إنتاج شركة "جولد أبولو Gold Apollo" التايوانية. يتميز هذا الجهاز بقدرته على استقبال وعرض الرسائل النصية لاسلكياً، لكنه غير قادر على إجراء مكالمات هاتفية. ووفقاً لعدة مصادر، أُدخلت هذه الأجهزة إلى لبنان في وقت سابق من عام ٢٠٢٤ (Bassam & Gebeily, 2024).

تشير معلومات موثوقة إلى أن جهاز الموساد الإسرائيلي قام بتعديل هذه الأجهزة "على مستوى الإنتاج"، حيث زُرعت شريحة داخلية تحتوي على مادة متفجرة تُفعَّل عبر شفرة خاصة. وأفاد مصدر لرويترز بأن هذه المادة المتفجرة صُممت بحيث يصعب اكتشافها، حتى باستخدام أحدث أجهزة المسح أو الكشف. وأوضحت عدة مصادر أن المؤامرة استغرقت عدة أشهر من التخطيط والتنفيذ، مما يعكس درجة عالية من التعقيد في العملية (Bassam & Gebeily, 2024).

ويبدو أن التلاعب بأجهزة الاتصالات عبر جهود استخباراتية مكثفة، يشير إلى أن الهجوم لم يكن الهدف الوحيد للعملية، فمن المحتمل أن تكون الاستخبارات قد جمعت معلومات دقيقة عن تنظيم حزب الله، وعملياته اليومية خلال الأشهر التي سبقت التفجير بواسطة ذات الأجهزة. ووصف "ليور تابانسكي Lior Tabansky"، الخبير في مجال التكنولوجيا والأمن في مركز "بلافاتنيك Blavatnik" للأبحاث السيبرانية متعددة التخصصات، العملية بأنها مزيج من الهجوم السيبراني والهجوم التقليدي. وأوضح أن بطاريات الليثيوم رغم إمكانية انفجارها، لا تمتلك القوة الكافية لإحداث هذا المستوى من الدمار، كما أن ارتفاع حرارة البطارية قبل انفجارها يمنح المستخدم فرصة لملاحظة وجود أي خلل إن وجد، وهذا يعزز فرضية وجود شريحة متفجرة مصممة خصيصًا لهذا الغرض. وأضاف تابانسكي: "مثل هذا الهجوم يتطلب عملية استخباراتية سرية طويلة المدى، لفهم سلسلة إمداد حزب الله، ثم إيجاد الثغرات لاختراق الأجهزة" (Roussi, 2024).

لذلك، وصف خبراء الاستخبارات العملية بأنها لا مثيل لها في تاريخ التجسس من حيث نطاقها وعدد ضحاياها، وهي أحد أكثر الاختراقات نجاحاً وابتكاراً من قبل جهاز استخبارات في التاريخ الحديث (Dou & Vynck, 2024). وأضافوا: "أن مثل

هذه الهجمات تُنفذ عادةً كمقدمة لعمليات عسكرية أوسع، بهدف نشر الفوضى وتهيئة المسرح للتحركات العسكرية اللاحقة" (Miller et al., 2024). من جانبه، قال "روب موغا Rob Muggah"، مدير مجموعة "سيك ديف SecDev" الاستشارية في مجال المخاطر السيبرانية: "إن هذا الهجوم غير المسبوق، قوّض ثقة حزب الله في أنظمة اتصالاته الإلكترونية وسلاسل التوريد الخارجية، كما أضعف بشكل كبير قدرة التنظيم على التواصل الفعال، مما يمثل ضربة استراتيجية لعملياته" (Roussi, 2024).

أقنعت العملية القادة الإسرائيليين بإمكانية دفع حزب الله إلى حافة الانهيار، وتعريضه للتفكيك المنهجي باستخدام الضربات الجوية، وفي النهاية، الغزو البري. فأقدمت على اغتيال حسن نصر الله الزعيم المخضرم للحزب في ٢٧ سبتمبر ٢٠٢٤، أي بعد أسبوع واحد فقط من عملية التفجير. وكان اغتياله تتويجاً لسلسلة سريعة من الضربات التي استهدفت نصف مجلس قيادة حزب الله، ودمرت قيادته العسكرية العليا، وقدرته الصاروخية، بما في ذلك خطوط إمداده (Nakhoul, Hafezi, & Lubell, 2024). على إثر ذلك، تصاعدت وتيرة الصراع بشدة، فشنت إسرائيل حملة جوية مكثفة وغزوًا بريًا لجنوب لبنان؛ ليصل عدد القتلى إلى ٣٨٠٠ شخص، وأُجبر مليون شخص على الفرار من منازلهم وفقاً للسلطات اللبنانية، إلى أن تم سريان اتفاق وقف إطلاق النار بين الجانبين في ٢٧ نوفمبر ٢٠٢٤ (BBC News, 2024).

وتسلط عملية تفخيخ أجهزة اتصالات حزب الله الضوء على مخاطر العبث المادي بالأجهزة الإلكترونية المستخدمة يوميًا، وإمكانية استغلالها في حروب "سيبرانية" مستقبلية؛ حيث تصبح أجهزة بسيطة مثل: الساعات والنظارات والسماعات الذكية وأجهزة تنظيم ضربات القلب عرضة للتلاعب، إذا حصل المهاجمون على إمكانية الوصول إلى سلاسل التوريد العالمية، حيث يمكن تحويل الأجهزة غير الضارة إلى

أسلحة مدمرة، كما أثبتتها هذه التفجيرات في لبنان. وتثير هذه التطورات تساؤلات حول كفاءة الإجراءات التنظيمية والتفتيشية على الأجهزة الإلكترونية خلال دورة تصنيعها وتسويقها، بدءٍ من تصنيع المكونات إلى التجميع النهائي والشحن أو التوريد. الأمر الذي يجعل تعزيز الرقابة على مراحل التصنيع والتوريد أمرًا ضروريًا، للحد من تهديدات التعديلات الخبيثة.

ج. الحرب الروسية ـ الأوكرانية:

يعكس تاريخ العمليات السيبرانية الروسية، كم الوسائل السيبرانية التي يستخدمها الكرملين للانخراط في منافسة طويلة الأمد مع المنافسين. ففي تمهيد لحملتها العسكرية ضد أوكرانيا، لجأت موسكو إلى العمليات السيبرانية لتدمير البنية التحتية الحيوية لأوكرانيا. مثل استهدفت إمدادات الطاقة في كييف في ديسمبر ٢٠١٥، بواسطة برنامج BlackEnergy الخبيث، والذي أدى إلى حرمان منطقة أوكرانية يبلغ عدد سكانها حوالي ١.٥ مليون شخص من الكهرباء. شهد هذا البرنامج الخبيث تطورًا ملحوظًا، حيث انتقل من كونه مجرد أداة بسيطة لتنفيذ هجمات رفض الخدمة (DoS)، إلى أن أصبح تهديدًا مستمرًا متقدمًا (APT) يتمتع بقدرات أكثر تطورًا. وقد اتسعت دائرة الاستهداف لتشمل العديد من البنوك، ومؤسسات النقل، والخدمات العامة، مما يعكس قدرته على التسلل إلى البنى التحتية الحيوية وإحداث أضرار واسعة النطاق (Pollard, 2024, pp.3-13).

ويأتي هجوم برنامج NotPetya الخبيث بمثابة نقطة تحول في الحرب السيبرانية. وقد نسبت الحكومة الأمريكية الهجوم إلى روسيا في البيان التالي الصادر عن السكرتير الصحفي للبيت الأبيض:

"شن الجيش الروسي في يونيو ٢٠١٧ الهجوم الإلكتروني الأكثر تدميراً وتكلفة في التاريخ. وانتشر الهجوم الذي أطلق عليه اسم "NotPetya" بسرعة في جميع أنحاء العالم، مما تسبب في أضرار بمليارات الدولارات في جميع أنحاء أوروبا وآسيا والأمريكيتين وأستراليا. ورغم أنه كان جزءًا من جهود الكرملين المستمرة لزعزعة استقرار أوكرانيا، إلا أنه كان له عواقب عالمية بعيدة المدى، أدى إلى تعطيل البنية التحتية الحيوية في هذه المناطق" (Krasznay, 2020, p. 491). وأظهر الهجوم كيف يمكن لحدث سيبراني واحد أن يتجاوز الحدود الجغرافية، متسببًا في تأثيرات امتدت إلى دول متعددة. مما يبرز الطبيعة العابرة للحدود للهجمات السيبرانية، وقدرتها على إحداث اضطرابات واسعة النطاق على المستويين الإقليمي والعالمي.

اعتمدت موسكو، في سياق الحرب الروسية الأوكرانية الدائرة منذ ٢٤ فبراير ٢٠٢٢، على استغلال عمليات الاختراق للشبكات الأوكرانية لتحقيق نصر حاسم، متجاوزة بذلك أهداف ساحة المعركة التقليدية، ومستهدفة تقويض الثقة في الحكومة الأوكرانية. استندت هذه الرؤية إلى نظرية كالبرج، التي تركز على الدول الضعيفة، حيث ترى أن "الهجمات السيبرانية يمكن أن تثير شعورًا لدى المواطنين بعدم سيطرة دولتهم، وإلقاء اللوم عليها لفشلها في حماية البنية المجتمعية". وعكست هذه الرؤية الطموحات الروسية تجاه أوكرانيا، إذ اعتقدت موسكو أن شن حرب خاطفة سيكون كافيًا لزعزعة استقرار الحكومة، مما يؤدي إلى انهيار شامل يمكّنها من فرض سيطرتها على البلاد. ويتماشى هذا المنطق مع أفكار منظري القوة الجوية في فترة ما بين الحربين العالميتين، الذين اعتقدوا أن قصف المدن سيجبر السكان على الضغط على حكوماتهم للاستسلام.

لذا، يرى المحللان في حلف شمال الأطلسي، "ديفيد كاتلر David Cattler ودانيال بلاكDaniel Black "، أن العمليات السيبرانية تمثل "أكبر نجاح عسكري حققته روسيا حتى الآن في الحرب على أوكرانيا" (Mueller et al., 2023, p. 4). وذلك لسببين واضحين:

أولاً، هناك دلائل تشير إلى أن روسيا تعمل على تعطيل القيادة والسيطرة الأوكرانية منذ بداية الحرب. فقبل ساعات من بدء الغزو البري، نشرت روسيا برامج ضارة استهدفت نظام الأقمار الصناعية Viasat، مما أدى إلى انقطاع مؤقت لأكثر من ٣٠ ألف اتصال بالإنترنت في جميع أنحاء أوروبا، بما في ذلك التأثير على ٥٨٠٠ توربين رياح في ألمانية، وغيرها في مختلف أنحاء الاتحاد الأوروبي (O'Neill, 2022). وأفادت قيادة شركة "سبيس إكس[*] SpaceX"، أن شبكة "ستارلينك Starlink" التابعة لها نجحت في التصدي لعدة هجمات إلكترونية نفذتها روسيا. يذكر أن الشبكة قد تم نشرها في أوكرانيا بعد وقت قصير من بدء الغزو الروسي في فبراير ٢٠٢٢، لتوفير وسيلة اتصال داخل البلاد، في ظل تضرر البنية التحتية المحلية للإنترنت بسبب الصراع المستمر. كما استُخدمت الشبكة لأغراض عسكرية في مواقع أخرى، حيث دعمت القوات الأوكرانية في استهداف الدبابات والمواقع الروسية باستخدام اتصالات الطائرات بدون طيار (Browne, 2022).

كما أفادت التقارير بوجود محاولات روسية لاختراق وكالة "دلتا" الأوكرانية عبر برمجيات خبيثة، بهدف سرقة البيانات. تُعد هذه الوكالة جزءًا من الاستخبارات

[*] شركة تقنيات استكشاف الفضاء، هي شركة خاصة أمريكيَّة تعمل على تصنيع الطيران والنقل الفضائي، أسسها إيلون ماسك في ٢٠٠٢، وأطلقت العديد من الأقمار الصناعيّة لخدمة الإنترنت ومنها شبكة ستارلنك.

العسكرية الأوكرانية، وتضطلع بدور حيوي في جمع المعلومات عن العدو، والتنسيق بين قوات الدفاع، وتعزيز الوعي بالموقف الميداني. وقد اكتسبت الوكالة سمعة كأداة ذات قيمة كبيرة في ترسانة أوكرانيا، مما يجعلها هدفًا رئيسيًا لهجمات القراصنة الروس. ووفقًا لمركز الاستجابة للطوارئ في أوكرانيا، استخدم المهاجمون حسابات بريد إلكتروني مخترقة لموظفين في وزارة الدفاع، بالإضافة إلى تطبيقات مراسلة، لإرسال رسائل خادعة للمستلمين تدعوهم إلى تحديث الشهادات في نظام "دلتا". تضمنت هذه الرسائل مستندات تحتوي على روابط لملفات أرشيفية مستضافة على نطاق مزيف يحاكي "دلتا." وقد صُممت هذه الملفات لنشر نوعين من البرامج الضارة على الأجهزة المستهدفة؛ الأول يُعرف باسم FateGrab، ويعمل على جمع رسائل البريد الإلكتروني، وقواعد البيانات، والبرمجيات النصية، والمستندات. أما الثاني فهو StealDeal، ويُستخدم لجمع بيانات متصفح الإنترنت ومعلومات أخرى من النظام المصاب (Kovacs, 2022).

ثانيًا، منذ بداية الحرب، وردت تقارير عن اكتشاف برامج ضارة استهدفت البنية التحتية الحيوية، في الدول التي تدعم أوكرانيا بالمساعدات العسكرية. ففي الولايات المتحدة، تم الكشف عن برامج روسية خبيثة، استهدفت تعطيل نحو اثني عشر موقعًا لتوليد الكهرباء ومحطات الغاز الطبيعي المسال. ولو لم يتم اكتشافها في الوقت المناسب، لكان من المحتمل أن تُستخدم للتسبب في انقطاع التيار الكهربائي وتعطيل الإمدادات. وكانت الولايات المتحدة قد أعلنت عن اكتشاف هذه البرامج الضارة الخطيرة في أبريل ٢٠٢٢، بعد ثلاثة أسابيع فقط من تحذير الرئيس السابق "جو بايدن Joe Biden"، من احتمال قيام روسيا بهجمات إلكترونية ضد الولايات المتحدة، داعيًا مجموعات البنية التحتية الحيوية إلى تعزيز جهودها الأمنية لمواجهة هذه التهديدات (Miller, 2023).

وقد أصدر المركز الوطني للأمن السيبراني(NCSC)، الذراع الأمني للمعلومات التابع لمقر الاتصالات الحكومية في المملكة المتحدة، تحذيرًا بشأن جهات تهديد روسية مرتبطة بالدولة، تستهدف تنفيذ هجمات تخريبية ومدمرة ضد البنية التحتية الحيوية في الدول الغربية. وأوضح المركز أن هذه الجهات تركز على شن هجمات حجب الخدمة الموزعة (DDoS)، وتشويه المواقع الإلكترونية، ونشر المعلومات المضللة. كما حذر من أن "بعض الجهات أبدت رغبتها في تحقيق تأثير أكثر تدميرًا وإرباكًا على البنية التحتية الوطنية الحيوية في الغرب، بما في ذلك المملكة المتحدة. ويرى المركز أن هذه المجموعات ستركز جهودها على استهداف أنظمة البنية التحتية الحيوية، التي تفتقر إلى الحماية الكافية لإحداث اضطرابات كبيرة. وتشمل هذه الجهات الفاعلة مجموعات مدعومة من الحكومة الروسية، بالإضافة إلى متسللين متعاطفين مع روسيا (Arghire, 2023).

يُعد التركيز على تخريب البنية التحتية الحيوية عنصرًا محوريًا في النظرية العسكرية الروسية، والتي تُعرف باسم "العملية الاستراتيجية لتدمير الأهداف ذات الأهمية الحرجة (SODCIT)"، هي عملية مصممة لإلحاق الضرر بالخصم (التحالف)، مما يدفعه إلى التخلي عن التصعيد، أو استمرار النزاع تحت ظروف تُعد مواتية لروسيا. تستهدف العملية منشآت وأهداف بالغة الأهمية، سواء كانت من النواحي العسكرية أو الاقتصادية أو السياسية أو الإدارية. كما قد تمتد لتشمل عناصر تنتمي إلى "نظام قيادة الدولة والجيش والشرطة"، مما يجعلها استراتيجية شاملة لإضعاف قدرة الخصم على المقاومة أو الرد (Kofman, Fink, Gorenburg, Chesnut, Edmonds, & Waller, 2021, p. 68).

وتكشف عملية تقييم موازين القوى بين الجانبين، أن موسكو رغم وضوح رؤيتها فيما يخص الحرب السيبرانية، إلا أنها أخفقت في تقليص الدعم الغربي أو إضعاف القدرات العسكرية الأوكرانية بالقدر المتوقع. يبدو أن التفسير الوحيد لهذا الفشل يكمن في أن موسكو وجدت نفسها تواجه ليس فقط أوكرانيا، بل أيضًا شبكة عالمية متكاملة من خبراء الأمن السيبراني من القطاعين العام والخاص، مما حدَّ بشكل كبير من قدرتها على تحقيق أهدافها في الفضاء السيبراني.

إذ شهدت السنوات الماضية جهودًا غير معلنة لتنسيق سياسات الأمن السيبراني بين أوكرانيا والولايات المتحدة، مع إشراك القطاع الخاص بشكل فعّال. وشارك مهندسو الاستراتيجية السيبرانية الأوكرانية في مبادرات متنوعة نظمتها وزارة الخارجية الأمريكية، ومكتب التحقيقات الفيدرالي (FBI)، والوكالة الأمريكية للتنمية الدولية، ووزارة الطاقة الأمريكية (USAID)، ووكالة الأمن السيبراني، وأمن البنية التحتية (CISA)، ووزارة الأمن الداخلي، ووزارة العدل. كما شمل ذلك اجتماعات مع مدير الأبحاث في لجنة "السايبر سبيس سولاريوم Cyberspace Solarium" الأمريكية، قبل عام من اندلاع الصراع. وتمتلك هذه الوكالات برامج تدعم تطوير شبكات أوكرانيا، وتعزيز مبادرات إصلاح الأمن السيبراني، والبنية التحتية الرقمية، بالإضافة إلى ضمان استمرار وصول أوكرانيا إلى الإنترنت وتقوية دفاعاتها السيبرانية (U.S. Department of State, 2022).

وتوازي هذه الجهود مبادرات مشابهة من الاتحاد الأوروبي، حيث قام بتنشيط فريق الاستجابة السيبرانية السريعة، لدعم أوكرانيا في التصدي للهجمات الإلكترونية الروسية. كما اتخذ حلف شمال الأطلسي خطوة بارزة بقبول أوكرانيا كمشارك في مركز التميز الدفاعي السيبراني التعاوني. وفي الوقت نفسه، تجاوزت الجهود الأمريكية حدود

الدفاع السيبراني التقليدي، حيث تم وضع هذه الجهود موضع التنفيذ، فنجحت في إزالة البرامج الروسية الضارة سرًا من شبكات الكمبيوتر حول العالم، مع نشرها لقوات إلكترونية لدعم دفاعات الشركاء. لكن، لا يزال غير واضح حتى الآن، ما إذا كانت هذه الأنشطة قد شملت أيضًا تنفيذ عمليات هجومية لتعطيل القدرات السيبرانية الروسية أم لا (Mueller et al., 2023, p. 10).

لكن من الجدير بالذكر أن أوكرانيا أصبحت رهينة للصراعات الحزبية في الغرب، حيث بات دعمها موضوعًا للنقاش المتزايد داخل كل من الاتحاد الأوروبي والولايات المتحدة. ويعتمد استمرار الدعم الغربي لأوكرانيا بشكل أساسي على قدرة الدول الغربية على الحفاظ على وحدتها. وقد شهدت هذه الوحدة تراجعًا بحلول أواخر عام ٢٠٢٣، حيث انخفضت المساعدات الجديدة المقدمة من الحلفاء بنسبة تقارب ٩٠٪ بين أغسطس وأكتوبر ٢٠٢٣، مقارنة بالفترة نفسها من عام ٢٠٢٢. ومع تذبذب مستوى المساعدات الاقتصادية والعسكرية التي يقدمها الغرب لأوكرانيا، قد تتمكن روسيا من تحقيق تفوق عسكري ملموس عليها في الفترة المقبلة. ويأمل الكرملين في استغلال هذه الانقسامات الحزبية لتقويض الدعم الغربي لأوكرانيا بشكل أكبر، من خلال أدوات تشمل الاعتماد على تقليص صادرات الغاز، والاستثمارات، والأوليغارشيين(*)، وحملات التضليل، والاستخبارات، والجواسيس، فضلاً عن دعم الأحزاب الشعبوية (Snegovaya, 2024, pp. 6-9).

(*) حكم الأقلية أو الأوليغاركية أو الأوليغارشية، بالإنجليزية: Oligarchy، هي شكل من أشكال الحكم، بحيث تكون السلطة السياسية محصورة بيد فئة صغيرة من المجتمع، تتميز بالمال أو النسب أو السلطة العسكرية.

ويُرجَّح أن يزداد الموقف الروسي تعنتًا في أوكرانيا عقب تراجع نفوذه في الشرق الأوسط، وذلك مع انهيار نظام الرئيس السوري بشار الأسد خلال أيام معدودة. ففي ظل انشغال موسكو بحربها الشاملة ضد أوكرانيا، عجزت عن منع سقوط أبرز حلفائها في المنطقة في ٨ ديسمبر ٢٠٢٤. ومع لجوء الأسد إلى روسيا، أصبحت القواعد العسكرية الروسية في سوريا تواجه مصيرًا غامضًا، كما تعرضت هيبة الكرملين لضربة قاسية على الساحة الدولية.

قد يدفع هذا التطور عواصم الدول الحليفة لموسكو إلى إعادة تقييم مدى موثوقية الدعم الروسي، مما يُضعف ثقة الحلفاء المحتملين في ضمانات موسكو الأمنية. كما أن فقدان روسيا لقاعدة طرطوس البحرية، من شأنه أن يضعف موقفها في البحر المتوسط بشكل كبير، وقد يقلل من قدرتها على التهديد الكامن في مواجهة أوروبا. إضافة إلى ذلك، أصبحت الطموحات الروسية في أفريقيا موضع تساؤل. فقد لعبت قاعدة حميميم الجوية دورًا رئيسيًا في العمليات اللوجستية العالمية لموسكو، حيث ساهمت في نقل القوات والمعدات الثقيلة إلى القارة الأفريقية. ومع فقدان هذه القاعدة، ستحتاج روسيا إلى إعادة هيكلة طرق الدعم اللوجستي بشكل عاجل، وهو ما يتطلب موارد مالية وزمنية وجهودًا كبيرة (Kozhanov, 2024).

ويعتقد بعض المحللين أن انهيار نظام الأسد قد يعقد موقف أوكرانيا في أي محادثات سلام مستقبلية مع روسيا، فمن المرجح أن يدفع سقوط الأسد موسكو، إلى إعادة توجيه جزء من قواتها ومعداتها العسكرية من سوريا لتعزيز جبهتها في أوكرانيا. هذا التحول يمكن أن يعزز القوة القتالية الروسية على الأراضي الأوكرانية. وفي الوقت نفسه، قد يشكل هذا التطور حافزًا قويًا للمعارضين للحرب الروسية في أوكرانيا، مما

يزيد من زخم الدعم الدولي لكييف، ويُعزز الاعتقاد بأن هزيمة روسيا أمر ممكن التحقيق (Sukhov, 2024).

الخاتمة:

يتضح من العرض السابق أن التطورات التي شهدها العالم خلال الثلاثة عقود الماضية، قد أعادت الجيوبوليتيكا إلى صدارة الاهتمام العالمي؛ حيث ساهمت هذه التطورات في تعميق الانقسامات على الساحة العالمية، في ظل استقطاب سياسي متزايد، وهياكل سلطة متشعبة، تعيق التوصل إلى توافق حول القضايا الدولية الأساسية.

إن ما كشفت عنه الأحداث التي شهدها العالم مؤخراً، يؤكد أن خطر التصعيد لابد وأن يؤخذ على محمل الجد، لأن هذه الأحداث تثبت أنه لا يوجد ما يضمن، أن الصراع الذي يبدأ في الفضاء السيبراني سوف يستمر هناك. فضلاً عن ذلك فإن الآثار الجانبية للأسلحة السيبرانية غير معروفة على نحو كاف. وتظل مسألة الثقة في الفضاء السيبراني شائكة، وهذا يتفق مع المثل القائل بأن "لا يوجد أصدقاء في الفضاء السيبراني" (Douzet, 2014, p.16).

وقد أظهرت الهجمات السيبرانية التي تعرضت لها إستونيا وجورجيا وأوكرانيا ولبنان وإيران والولايات المتحدة، فضلاً عن فضايح التجسس والتسريبات العديدة، أن هناك صعوبة متزايدة في الحفاظ على النظام والأمن في الفضاء السيبراني. فعلى الرغم من الاستعدادات المتقدمة التي تتخذها بعض الدول تحسبًا لحروب سيبرانية محتملة، سواء في مواجهة خصوم دوليين أو لمواجهة هجمات ينفذها فاعلون غير حكوميين، إلا أن الفضاء السيبراني لا يزال يعاني من فراغ تشريعي واضح على المستوى الدولي، في ظل غياب إطار قانوني دولي موحد ينظّم هذا المجال الحيوي.

يأتي ذلك رغم انعقاد المؤتمر العالمي للاتصالات الدولية بشكل دوري كل أربع سنوات، كان آخرها في دبي خلال الفترة من ٢٠ نوفمبر إلى ١٥ ديسمبر ٢٠٢٣، برعاية الاتحاد الدولي للاتصالات (ITU). ويظل هذا المؤتمر، الذي يُعنى بمراجعة اللوائح الدولية للاتصالات باعتبارها معاهدة دولية ملزمة، مخصصًا لتعزيز التعاون الدولي وتيسير تقديم خدمات الاتصالات والإنترنت، بدلاً من معالجة القضايا التشريعية للفضاء السيبراني بشكل مباشر.

لذلك تظل الحدود القضائية ضعيفة في الفضاء السيبراني، في الوقت الذي تمتلك الجهات الفاعلة التي تسعى للتأثير على طبيعة هذا الفضاء أدوات متنوعة، ودرجات متفاوتة من الوصول إلى نقاط التحكم الرئيسية فيه، في مقابل محدودية إمكانيات بعض الدول الأخرى. وفي هذا السياق، يمكن وصف ما نشهده بأنه "صراع غير متكافئ" حول تحديد معالم المستقبل (Choucri & Clark, 2013, p. 30).

في هذا السياق، أصبحت الجيوبوليتيكا في عصر الفضاء السيبراني حقلًا دراسيًا حيويًا ومهمًا لفهم ديناميكيات القوة والتأثير في العالم الرقمي. فقد أسهمت التطورات التكنولوجية والعولمة في تحويل الفضاء السيبراني إلى ساحة تنافس جديدة بين الفاعلين الدوليين وغير الدوليين، مما أدى إلى إعادة صياغة مفهوم السيادة، وأهمية البنية التحتية الرقمية، وتعاظم التحديات المرتبطة بالأمن السيبراني.

ورغم أن الجيوبوليتيكا النقدية قدمت أدوات تحليلية لتفكيك الخطابات الجيوبوليتيكية السائدة، إلا أنها لم تستطع دائمًا تقديم بدائل عملية لاستيعاب التغيرات الجديدة، وهو ما يظهر الحاجة إلى تطوير نموذج يجمع بين الكلاسيكية والنقدية. هذا النموذج يجب أن يعالج التوترات بين الأبعاد المادية وغير المادية للقوة في الفضاء السيبراني، مع الأخذ في الاعتبار التحديات القانونية والأخلاقية والسياسية المرتبطة به.

إن هذه الدراسة تفتح آفاقًا جديدة لفهم الصراعات في الفضاء السيبراني من منظور جيوبوليتيكي معاصر، وتعزز الحاجة إلى استراتيجيات دولية متكاملة للتعامل مع التحديات الناشئة عن هذا المجال، مع الحفاظ على التوازن بين الأمن والحرية وحقوق الأفراد.

تناولت الدراسة مجموعة من الفرضيات التي تسلط الضوء على العلاقة المتبادلة بين الفضاء السيبراني والعوامل الجيوبوليتيكية والاجتماعية والسياسية، مع التركيز على تأثيرات العولمة والتطور التكنولوجي على الأمن والسيادة الوطنية. وبعد تحليل شامل، يمكن التأكيد على النقاط التالية:

برهنت الدراسة على صحة الفرضية الأولى، فلم تسهم العولمة فقط في تسريع حركة الأشخاص والمعلومات والسلع، بل عززت أيضًا انتقال المخاطر عبر الحدود، مما أوجد تحديات جديدة تتعلق بالأمن والبيئة والمخاطر الاقتصادية والاجتماعية. وقد تم تناول هذه القضايا عبر أمثلة تطبيقية تبرز أهمية التعاون الدولي في مواجهتها.

كما أثبتت الدراسة صدق الفرضية الثانية؛ فعلى الرغم من نجاح الجيوبوليتيكا النقدية في تحليل وتفكيك الخطابات الجيوبوليتيكية نظرياً، إلا أنها لم تتمكن من تقديم بدائل عملية قوية تعزز السلام الدولي أو تساهم بفعالية في تشكيل السياسات الدولية، وهو ما يدعو إلى ضرورة تطوير أطر عملية مستمدة من النقد الجيوبوليتيكي.

برهنت الدراسة أيضاً على صدق الفرضية الثالثة: فعلى الرغم من الانتقادات الأكاديمية للجيوبوليتيكا الكلاسيكية، إلا أن أفكارها لا تزال تُستخدم على نطاق واسع في صياغة الاستراتيجيات الجيوسياسية، لا سيما في سياسات السيطرة على الفضاء السيبراني، وهو ما يعكس التداخل المستمر بين النظريات القديمة والمتغيرات الحديثة.

برهنت الدراسة على أن الفصل بين العالم الافتراضي والعالم الحقيقي ليس مطلقًا، حيث يظل الموقع الجغرافي والمكان عاملين حاسمين في تشكيل تفاعلات الفضاء السيبراني، كما يتضح من توزيع مراكز البيانات والبنية التحتية للإنترنت. وفي الوقت ذاته، تؤثر التفاعلات في الفضاء السيبراني بشكل كبير على الواقع المادي، خاصة في السياقات السياسية والعسكرية والاقتصادية.

كما أثبتت الدراسة قدرة الفضاء السيبراني على فرض تحديات جديدة أمام مفهوم السيادة الوطنية والهوية، حيث تُصَعِب طبيعة الشبكات الرقمية العابرة للحدود على الدول فرض قوانينها داخل حدودها، لا سيما في ظل هيمنة الشركات الأجنبية العملاقة على تقديم الخدمات الرقمية.

أظهرت الدراسة أن الفضاء السيبراني أصبح جزءًا لا يتجزأ من الاستراتيجيات العسكرية الحديثة، حيث يشكل ساحة جديدة للتفاعلات والصراعات بجانب الفضاءات التقليدية (الأرض، البحر، الجو، والفضاء الخارجي).

تُؤكد الدراسة أن التقدم التكنولوجي قد أعاد تشكيل موازين القوى العالمية، حيث أتاح لبعض الدول التفوق على غيرها بفضل ريادتها التكنولوجية. وهذا يعكس أهمية تعميق الفهم للعلاقة المتداخلة بين التكنولوجيا والسياسة الدولية.

من كل ما سبق توصي الدراسة بما يلي:

١. ضرورة الجمع بين الأطر الكلاسيكية والنقدية لتطوير فهم أعمق لديناميكيات الفضاء السيبراني.

٢. تعزيز التشريعات الوطنية والدولية المتعلقة بالأمن السيبراني، بما يضمن الحد من استغلال الفضاء السيبراني في أعمال تهدد الأمن القومي.

٣. تعزيز التعاون الدولي في مجال الأمن السيبراني لمواجهة التهديدات المتزايدة، من خلال تبادل المعلومات والخبرات بين الدول والمؤسسات.

٤. تطوير استراتيجيات وطنية شاملة للأمن السيبراني، تشمل حماية البنية التحتية الحيوية، وتأمين الفضاء السيبراني ضد التهديدات المحتملة.

٥. الاستثمار في بناء القدرات التقنية والبشرية، من خلال تدريب الكوادر الوطنية وتأهيلها للتعامل مع التحديات السيبرانية.

٦. دعم البحث العلمي والابتكار في مجال الأمن السيبراني، لتطوير حلول تقنية مستدامة تسهم في التصدي للهجمات المتطورة.

٧. توعية المجتمعات بمخاطر التهديدات السيبرانية وتعزيز ثقافة الاستخدام الآمن للتكنولوجيا الرقمية.

المراجع العربية والأجنبية

أولاً: المراجع العربية

١- السدخان، ضحى لعيبي كاظم. (٢٠٢١). البعد الجيو سياسي للأمن السيبراني. *مجلة العلوم الإنسانية*، ٥ (١).

٢- المشهدى، تغريد معين حسن. (٢٠١٩). الأثر العسكري للأمن السيبراني في الجغرافيا السياسية للدولة. *مجلة البحوث الجغرافية*، (٣٠).

٣- حشاني، فاطمة الزهراء؛ وحكيمي، توفيق. (٢٠٢٤). الدبلوماسية السيبرانية وجيوسياسية الفضاء السيبراني: بين مساعي الحوكمة وحسابات التنافس. *مجلة الباحث للدراسات الأكاديمية*، ١١ (٢).

٤- عياد، إيهاب محمد أبو المجد محمود. (٢٠٢٣). الجيوسيبرانية العالمية والتحولات في أبعاد وخصائص القوة: آليات التوظيف في الاستراتيجية الروسية والصينية. *مجلة البحوث المالية والتجارية*، ٢٤ (١).

ثانياً: المراجع الأجنبية

A – Books:

1. Prevezianou, M. F. (2021). WannaCry as a creeping crisis. In A. Boin, M. Ekengren, & M. Rhinard (Eds.), Understanding the creeping crisis. Palgrave Macmillan & Springer Nature
2. Snegovaya, M. (2024). Putin's efforts to divide the West. In C. Cohen & A. Kisling (Eds.), *Global forecast 2024: Conflict zones*. Center for Strategic and International Studies.
3. Mythen, G. (2015). The problem of governance in the risk society: Envisaging strategies, managing not-knowing. In U.

Fra.Paleo (Ed.), *Risk governance: The articulation of hazard, politics and ecology*. Springer.

4. Gray, C. S. (2013). *Making strategic sense of cyber power: Why the sky is not falling*. Strategic Studies Institute; U.S. Army War College Press.
5. Woodward, K., & Jones, J. P., III. (2008). The condition of postmodernity (1989): David Harvey. In P. Hubbard, R. Kitchin, & G. Valentine (Eds.), *Key texts in human geography*. SAGE Publications.
6. Midson, D. (2014). Geography, territory and sovereignty in cyber warfare. In H. Nasu & R. McLaughlin (Eds.), *New technologies and the law of armed conflict*. T.M.C. Asser Press.
7. Krasznay, C. (2020). Case study: The NotPetya campaign. In K. Norbert & A. Koltay (Eds.), *Sustainable security and social environment studies*. Ludovika University Publishing House.
8. Walker, R. B. J. (1992). *Inside/outside: International relations as political theory*. Cambridge University Press.
9. Wissmann, T., & Palis, J. (Eds.). (2017). Geographies of media. Springer

B – Periodicals:

1. Adams, J., & Albakajai, M. (2016). Cyberspace: A new threat to the sovereignty of the state. *Management Studies*, 4(6).

2. Bachmann, V., & Moisio, S. (2020). Towards a constructive critical geopolitics: Inspirations from the Frankfurt School of Critical Theory. *Environment and Planning C: Politics and Space*, 38(2).

3. Benkler, Y. (2011). Networks of power, degrees of freedom. *International Journal of Communication*, 5.

4. Bronk, C., & Tikk-Ringas, E. (2013). The cyber attack on Saudi Aramco. *Survival: Global Politics and Strategy*, 55(2).

5. Cammaerts, B. (2013). Networked resistance: The case of WikiLeaks. *Journal of Computer-Mediated Communication*, 18.

6. Chapelle, B. D., & Fehlinger, P. (2016). Jurisdiction on the internet: From legal arms race to transnational cooperation. (*Paper Series*: No. 28). Global Commission on Internet Governance.

7. Choucri, N., & Clark, D. D. (2013). Who controls cyberspace? *Bulletin of the Atomic Scientists*, 69(5).

8. Christensen, C. (2014). WikiLeaks and the afterlife of collateral murder. *International Journal of Communication, 8*.

9. Gao, C., Guo, Q., Jiang, D., Wang, Z., Fang, C., & Hao, M. (2019). Theoretical basis and technical methods of cyberspace geography. *Journal of Geographical Sciences, 29*(12).

10. Clark, D. D. (2010). *Characterizing cyberspace: Past, present and future* (ECIR Working Paper No. 2010-3). MIT Political Science Department.

11. Dodds, K. (2001). Political geography III: Critical geopolitics after ten years. *Progress in Human Geography, 25*(3).

12. Dodds, K. (2007). [Review of the book *Global geopolitics: A critical introduction*]. *Journal of International Relations and Development, 10*(1).

13. Douzet, F. (2014). Understanding cyberspace with geopolitics. *Hérodote, 152-153*(1-2).

14. Fekete, E., & Warf, B. (2013). Information technology and the "Arab Spring." *The Arab World Geographer, 16*(2).

15. Gibbs, J. L., Kim, H., & Ki, S. (2016). Investigating the role of control and support mechanisms in members' sense of virtual community. *Communication Research*, *46*(1).

16. Grabosky, P. (2004). The global dimension of cybercrime. *Global Crime*, *6*(1).

17. Grandin, A. (2023). Cyberspace geography and cyber terrain: Challenges in producing a universal map of cyberspace. Proceedings of the 22nd European Conference on Cyber Warfare and Security (ECCWS), 22(1).

18. Jones, L., & Sage, D. (2010). New directions in critical geopolitics: An introduction. *GeoJournal*, *75*.

19. Kallberg, J. (2016). Strategic cyberwar theory: A foundation for designing decisive strategic cyber operations. *The Cyber Defense Review*, *1*(1).

20. Kosenkov, A. (2016). Cyber conflicts as a new global threat. *Future Internet*, *8*(3).

21. Mariani, L., & Bertolini, M. (2019). *The US–China 5G contest: Options for Europe* (Papers 19). Istituto Affari Internazionali.

22. Callaghan, M. J., Harkin, J., McColgan, E., McGinnity, T. M., & Maguire, L. P. (2007). Client–server architecture for collaborative remote experimentation. *Journal of Network and Computer Applications*, *30*(4).

23. Power, M., & Campbell, D. (2010). The state of critical geopolitics. *Political Geography*, *29*(5).

24. Reuber, P. (2000). Conflict studies and critical geopolitics: Theoretical concepts and recent research in political geography. *GeoJournal*, *50*.

25. RiskRecon's Leadership Team. (2024). *The 2024 state of ransomware: Five lessons for TPRM professionals*. RiskRecon.

26. Robine, J., & Salamatian, K. (2014). Envisioning cyber-geography? *Hérodote, 152–153*(1–2).

27. Robinsona, M., Jonesb, K., & Janickea, H. (2015). Cyber warfare: Issues and challenges. *Journal of Computers and Security, 49*.

28. Pollard, M. (2024). A case study of Russian cyber-attacks on the Ukrainian power grid: Implications and best practices for the United States. *Pepperdine Policy Review, 16*, Article 1.

29. Salihović, N., & Džubur, A. H. (2021). Information networks: Concept, classification and application. *Science, Engineering and Technology Journal, 1*(2).

30. Sharma, A. (2010). Cyber wars: A paradigm shift from means to ends. *Strategic Analysis, 34*(1).

31. Sharma, P., Bhatia, V., & Prakash, S. (2022). Efficient ordering policy for secret key assignment in quantum key distribution-secured optical networks. *Optical Fiber Technology, 68*.

32. Sidaway, J. D. (1994). Political geography in the time of cyberspaces: New agendas? *Geoforum, 25*(4).

33. *SonicWall. (2023).* Cyber threat report: Charting cybercrime's shifting frontlines. *SonicWall.*

C - Researches:

1. Baezner, M., & Robin, P. (2017). *Hotspot analysis: Stuxnet*. Center for Security Studies, Swiss Federal Institute of Technology.

2. Kofman, M., Fink, A., Gorenburg, D., Chesnut, M., Edmonds, J., & Waller, J. (2021). *Russian military strategy: Core tenets and operational concept*. Center for Naval Analyses.
3. Mueller, G. B., Jensen, B., Valeriano, B., Maness, R. C., & Macias, J. M. (2023). *Cyber operations during the Russo-Ukrainian War: From strange patterns to alternative futures*. Center for Strategic and International Studies.

D- Electronic Sources:

1. Arghire, I. (2023). Cyberwarfare: UK warns of Russian hackers targeting critical infrastructure. *SecurityWeek*. https://www.securityweek.com/uk-warns-of-russian-hackers-targeting-critical-infrastructure/.

2. Barlyn, S. (2017). Global cyber attack could spur $53 billion in losses: Lloyd's of London. *Reuters*. https://www.reuters.com/article/us-cyber-lloyds-report/global-cyber-attack-could-spur-53-billion-in-losses-lloyds-of-london-idUSKBN1A20AB.

3. Bassam, L., & Gebeily, M. (2024). Israel planted explosives in Hezbollah's Taiwan-made pagers, say sources. *Reuters*. https://www.reuters.com/world/middle-east/israel-planted-explosives-hezbollahs-taiwan-made-pagers-say-sources-2024-09-18/.

4. BBC News. (2017, May 15). Ransomware cyber-attack: Who has been hardest hit? https://www.bbc.com/news/world-39919249.

5. BBC News. (2024). Israel-Hezbollah conflict in maps: Ceasefire in effect in Lebanon. *BBC News*. https://www.bbc.com/news/articles/c9vp7dg3ml1o/.

6. Browne, E. (2022). Elon Musk says Starlink has resisted hacking attempts from Russia 'so far'. *Newsweek*.

https://www.newsweek.com/elon-musk-starlink-resisted-hacking-attempts-russia-1705495/.

7. Crace, J. (2013). Twitter gives data to French authorities after spate of antisemitic tweets. *The Guardian*. https://www.theguardian.com/technology/2013/jul/12/twitter-data-french-antisemitic-tweets.

8. Dou, E., & Vynck, G. D. (2024). Pagers attack brings to life long-feared supply chain threat. *The Washington Post*. https://www.washingtonpost.com/technology/2024/09/19/hezbollah-pager-attack-supply-chain/.

9. Gawazah, L., Rondla, A., & Abalhareth, M. S. (2024). *To pay or not to pay: The US Colonial Pipeline ransomware attack*. Thunderbird School of Global Management, Arizona State University.https://www.researchgate.net/publication/383206534_To_Pay_or_Not_to_Pay_The_US_Colonial_Pipeline_Ransomware_Attack.

10. Holloway, M. (2015). *Stuxnet worm attack on Iranian nuclear facilities*. Stanford University. http://large.stanford.edu/courses/2015/ph241/holloway1/.

11. Kovacs, E. (2022). Cyberwarfare: Ukraine's Delta military intelligence program targeted by hackers. *SecurityWeek*. https://www.securityweek.com/ukraines-delta-military-intelligence-program-targeted-hackers/.

12. Kozhanov, N. (2024). Russia has lost prestige after the fall of Assad. It has also been freed of a difficult partner. *Chatham House*. https://www.chathamhouse.org/2024/12/russia-has-lost-prestige-after-fall-assad-it-has-also-been-freed-difficult-partner/.

13. Mansted, K. (2019). The revenge of geography in cyberspace. *The Strategy Bridge*. https://thestrategybridge.org/the-bridge/2019/6/4/the-revenge-of-geography-in-cyberspace.

14. Miller, G., Brown, C., Morris, L., Rubin, S., & Swaine, J. (2024). Exploding pagers leave clues to Israeli 'red button' plot, officials say. *The Washington Post*. https://www.washingtonpost.com/world/2024/09/21/israel-lebanon-hezbollah-exploding-pagers/

15. Miller, M. (2023). Cybersecurity: Russian-linked malware was close to putting U.S. electric, gas facilities 'offline' last year. *Politico*. https://www.politico.com/news/2023/02/14/russia-malware-electric-gas-facilities-00082675/.

16. Mueller, P., & Yadegari, B. (2012). *The Stuxnet worm*. University of Arizona. https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/topic9-final/report.pdf.

17. Nakhoul, S., Hafezi, P., & Lubell, M. (2024). Nasrallah's killing reveals depth of Israel's penetration of Hezbollah. *Reuters*. https://www.reuters.com/world/middle-east/nasrallahs-killing-reveals-depth-israels-penetration-hezbollah-2024-09-28/.

18. O'Neill, P. H. (2022). Russia hacked an American satellite company one hour before the Ukraine invasion: The attack on Viasat showcases cyber's emerging role in modern warfare. *MIT Technology Review*. https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/.

19. Pursel, B. (2005). *Information, people, and technology*. Pressbooks. https://psu.pb.unizin.org/ist110/.

20. Roussi, A. (2024). How did Israel blow up Hezbollah pagers? *Politico*. https://www.politico.eu/article/israel-pagers-hezbollah-lebanon-health-ministry/.

21. Reuters. (2012, October 12). Shamoon virus most destructive yet for private sector, Panetta says. *Reuters*.

https://www.reuters.com/article/technology/shamoon-virus-most-destructive-yet-for-private-sector-panetta-says-idUSBRE89B04Y/.

22. Rovner, J. (2021). Warfighting in cyberspace. *War on the Rocks*. https://warontherocks.com/2021/03/warfighting-in-cyberspace/.

23. Sukhov, O. (2024). What does Assad's downfall mean for Russia and Ukraine? *Kyiv Independent*. https://kyivindependent.com/assads-downfall-shows-kremlin-is-not-invincible-undermines-trust-in-russian-led-alliances/.

24. The White House. (2021). *Remarks by President Biden on the Colonial Pipeline incident*. https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/05/13/remarks-by-president-biden-on-the-colonial-pipeline-incident/.

25. U.S. Department of State. (2022). U.S. support for connectivity and cybersecurity in Ukraine [Fact sheet]. https://www.state.gov/u-s-support-for-connectivity-and-cybersecurity-in-ukraine/.

Geopolitics in the Time of Cyberspaces: Between Classicism and Criticism Contemporary Vision in Political Geography

Abstract:

The research study the impact of cyberspace on contemporary geopolitical transformations, and its role in reshaping global power dynamics in the digital age. The research presents a summary of the international changes that followed the Cold War, how geopolitics deals with globalization, and the multiplicity of flows that contribute to shaping cyberspace. It also discusses the challenges that the technological and information revolution has posed to traditional concepts of sovereignty and international conflicts, tracing the oscillation of geopolitical thought between the classical and critical schools.

The research also addresses the overlap between the physical and logical infrastructures of cyberspace, and the impact of this overlap on national security. It reviews real-life cases of major cyber attacks, explaining through these examples how digital technology is reshaping the world's geopolitics, highlighting the growing role of cyberspace as a strategic tool in international relations.

The study opens new horizons for understanding conflicts in cyberspace from a contemporary geopolitical perspective, and reinforces the need for integrated international strategies to deal

with the challenges arising from this field. It also highlights the importance of achieving a balance between security, freedom, and individual rights, while integrating cyberspace as a fundamental element in geopolitical analysis to understand the complex transformations the world is witnessing. The study addresses the overlap of physical and virtual dimensions in shaping international policies, ensuring sovereignty and enhancing security in the face of increasing digital challenges.

The research concludes that it is necessary to develop an analytical model that combines classical and critical perspectives to address the tensions between the material and immaterial dimensions of power in cyberspace. This model takes into account the legal, ethical and political challenges posed by this dynamic field.

Keywords: Geopolitics ,Cyberspace ,Globalization ,Cybersecurity , National Sovereignty