ISSN: 2663-5798 || Arab Journal for Scientific Publishing

الإصدار الثامن – العدد السابع والسبعون
تاريخ الإصدار: 2 – آذار – 2025م
www.ajsp.net

"القوة السّيبرانيّة أداة للتأثير والسيطرة في الفضاء السيبراني والعلاقات الدّوليّة"

(بحث مكمل لمناقشة رسالة دكتوراه)

إعداد الباحث:

محمد محمود زيتون

ISSN: 2663-5798 || Arab Journal for Scientific Publishing

الإصدار الثامن – العدد السابع والسبعون
تاريخ الإصدار: 2 – آذار – 2025م
www.ajsp.net

الملخص:

تتناول هذه الدّراسة مفهوم القوّة السّيبرانيّة كأداة حديثة للتأثير والسيطرة في الفضاء السيبراني والعلاقات الدّوليّة، وتطرقت الى فهم القوة السّيبرانيّة ومكوناتها ومصادرها، وكيفيّة توظيفها في العلاقات الدّوليّة، وناقشت أدوات القوة السّيبرانيّة الصلبة والنّاعمة المتمثلة بالقدرات السّيبرانيّة والعمليات السّيبرانيّة، واستخدامها من الدول أو الفاعلين غير الدّوليين في الفضاء السيبراني في تحقيق أهداف سياسيّة، اقتصاديّة، وعسكريّة، لإحداث تأثير استراتيجي على العلاقات الدّوليّة، وذلك جعلها تطرح تحديات جديدة للسيادة التقليدية بعد تداخل الفضاء السيبراني مع الحدود الماديّة للدول، ما يستدعي إعادة التفكير في المفاهيم التّقليديّة للسيادة والردع والحروب.

الكلمات المفتاحية: الفضاء السّيبراني؛ سيطرة؛ تأثير ؛ قوّة ؛علاقات دوليّة.

المقدمة:

أسهم التّطور التكنولوجي والشّبكي الى تشكيل ديناميكيّات جديدة من التّفاعلات الدّوليّة في الفضاء السيبراني، أدّت الى خلق مظاهر سيبرانيّة ومصالح رقميّة تتأثر وتؤثّر في العالم الرقميّ، ونتيجة لهذه التغيرات والمظاهر السياسيّة برز فاعلين جدد في العلاقات الدّوليّة من غير الدول، تنافس الدول القوميّة على التأثير في مجالات التّعاون والصّراع في مجال أُزيلت فيه حواجز الزمان والمكان. إنّ ارتباط الفضاء السيبرانيّ بموارد القوّة التقليديّة للدول ووسائلها، سمح لها بمزامنة خدمات بنيتها التحتيّة ومصالحها الحيويّة الى فضاء الشبكة العالميّة كأصول رقميّة. ونظرًا لما يوفره هذا الفضاء من فرص متعددة بدأت الدّول ببناء القدرات الرّقميّة وأنظمة الدّفاع السّيبراني والهجومي، وتعزيز المهارات، والالتزام بالمعايير وأفضل ممارسات الحماية الدّوليّة بهدف تعظيم قوّتها وحماية مصالحها وضمان بقائها في العالم الرّقمي. حيث ساعدت هذه القدرات في بلورة مفهوم "القوة السّيبرانيّة" الذي يجمع بين عناصر مبتكرة في البيئة السيبرانيّة، وعناصر ماديّة في مجالات الدّول يمكّنها من ممارسة التأثير في الفضاء السّيبراني والعلاقات الدّوليّة، من خلال توظيف قدراتها في امتلاك البيانات الضخمة والقدرات السّيبرانيّة، وشن العمليات السّيبرانيّة لتحقيق أهداف قوميّة وسياسيّة واقتصاديّة، مثل الضغط السياسي والتأثير على الرأي العام، وتقويض العمل الرقمي الخدماتي.

فإذًا، لم يعد مفهوم القوة يُختزل في التّحكم في الموارد بقدر ما أصبح يتعلق بالتّحكم في النتائج، ولم يعد قياس القوة مقتصرًا على حساب الموارد، بل أصبح مرتبطًا بمدى القدرة على توظيفها بفاعليّة لتحقيق الأهداف المرجوة. كما أشار جوزيف ناي عند حديثه عن القوة، إذ يرى أن قياس القوة ينبغي أن يرتبط بفعاليتها في تحقيق الأهداف، وليس فقط بما تملكه الدولة من أدوات.

أهمية الموضوع: تكمن أهمية هذا البحث في تسليط الضوء على دور الفضاء السّيبراني في تشكيل القوة السّيبرانيّة، واستعراض تطورها كأداة مبتكرة للتأثير والسيطرة، أضف إلى كونها إحدى الوسائل الحديثة في الصراعات الدّوليّة.

أهداف البحث: تهدف الدراسة إلى تحقيق عدة أهداف، أبرزها تسليط الضوء على أهمية الفضاء السّيبراني في تعزيز القوة السّيبرانيّة، إلى جانب تعريف مفهوم القوة السّيبرانيّة وتحديد نطاقها ومكوناتها، وتوضيح كيفية تأثيرها في الفضاء السيبراني والعلاقات الدولية.

إشكالية البحث: أصبحت القوة السّيبرانيّة ظاهرة متنامية في النّظام الدّولي المعاصر، خاصة بعدما أصبح الفضاء السيبراني ميدانًا جديدًا للصراع والتنافس، وهنا تبرز إشكاليّة تحديد مجال القوّة السّيبرانيّة، ونطاق تأثيرها على السّيادة والعلاقات الدّوليّة والديناميكيات الاخرى. فكيف تُعرَّف القوة السّيبرانيّة في سياق التحولات التكنولوجية الراهنة؟ وكيف أصبحت القوة السّيبرانيّة أداة مركزية للتأثير والسيطرة؟

منهجية البحث: سأتناول في هذا البحث المنهج الوصفي والتحليلي لتوصيف التحولات التي طرأت على القوة السّيبرانيّة، وتحليل أساليبها واستخدامها كمنهج جديد في الدّيناميكيات الدّوليّة في التأثير والسيطرة في الفضاء السيبراني.

تصميم البحث:

المبحث الأول: الإطار النّظري للقوّة السّيبرانيّة

المطلب الأول: مفهوم وخصائص القوّة السّيبرانيّة

المطلب الثاني: أدوات وأساليب القوّة السّيبرانيّة

المبحث الثاني: تأثيرات القوّة السّيبرانيّة على العلاقات الدّوليّة في الفضاء السيبراني

المطلب الأول: توظيف القوّة السّيبرانيّة في العلاقات الدّوليّة

المطلب الثاني: تأثير القوة السّيبرانيّة على العلاقات الدّوليّة

المبحث الأول: الإطار النظري للقوة السّيبرانيّة

تُعَدّ القوّة أداة أساسية في تفسير طبيعة العلاقات بين الدول وناظم مهم في العلاقات الدّوليّة، وتعبّر عن مدى قدرة الدّول أو الفاعلين الجدد في تحقيق مصالحهم، القوة السّيبرانيّة تُشبه القوة التّقليديّة في تعريفها، إذ تُعَرَّف أنها القدرة على التأثير في سلوك الآخرين لتحقيق الأهداف، سواء من خلال الإقناع، أو الترغيب، أو الإكراه. واتخذت أشكالًا متعددة، منها القوة الصلبة التي تعتمد على الوسائل العسكريّة والاقتصاديّة لفرض السيطرة وتحقيق المصالح، والقوّة النّاعمة ترتكز على الجذب والإقناع من خلال التأثير على الثقافة، والقيم، في حين أنّ القوّة الذكيّة هي دمج بين الصلبة، والنّاعمة وتسخيرها في تحقيق أقصى فعاليّة في تحقيق الأهداف. واستخدامها ونطاقها يعتمد على الأساليب والأهداف التي نريد تحقيقها. وكذلك اتخذت القوّة السّيبرانيّة المفهوم التقليدي للقوة، وأصبح لديها قوة صلبة متمثلة بالأدوات السّيبرانيّة المادية والافتراضيّة المتمثلة بالعمليات السّيبرانيّة، والناعمة المتمثلة بالأدوات المناسبة والعمليات السّيبرانيّة البسيطة لنشر القيم الثقافية عبر الجذب والتأثير على الرأي العام، وسنبين ذلك في سياق البحث.

سأحاول توسيع كل ذلك في مطلبين أستعرض في الأول مفهوم وخصائص القوة السّيبرانيّة، بينما سأحلل في الثاني أدوات القوة السّيبرانيّة وأساليبها.

المطلب الأول: مفهوم وخصائص القوة السّيبرانيّة

في الفضاء السيبراني، برزت القوة السّيبرانيّة كقوّة جانبيّة لتعظيم قوّة الدّول الشّاملة تتميز بخصائص فريدة وأنماط تجعلها متميزة عن القوة التقليدية، تُستَخدَم فيها التقنيات السّيبرانيّة للتأثير على الدول والمجتمعات والأفراد. ما جعلها أداة مهمة للهيمنة والسّيطرة في الفضاء السيبراني والعلاقات الدّوليّة. ووسيلة لتحقيق التعاون والاستقرار أو النزاعات والصراعات بين الدول، وتؤثر بشكل مباشر على الأمن القومي والسيادة.

1.مفهوم القوة السّيبرانيّة وميزاتها: تُعرّف القوة السّيبرانيّة **(Cyber Power)** عن أستاذ العلاقات الدّوليّة جوزيف ناي Joseph Nye، "أنّها القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المُرتبطة بالفضاء السّيبراني لإيجاد مزايا للدّولة، والتأثير في الأحداث المتعلّقة بالبيانات التّشغيليّة الأخرى من خلال أدوات سيبرانيّة" [1].

ويضيف ماكس فيبر Max Weber عن استخدام القوّة السّيبرانيّة وخصائصها، ومدى نطاقها في الفضاء، يقول: يجب أن نعرف إذا كان للفاعل له علاقة اجتماعيّة أو أن ينفذ إرادته، للتركيز على فاعلين معينين، ولا يمكننا أن نقول إن الفاعل "يمتلك القوة" دون تحديد القوة " لفعل ماذا"[2]. يجب تحديد الفاعل من خلال "من " وأين" هو من ذلك بعلاقة القوة (نطاق القوة) و(مجال القوة) وهذا ما ينطبق على الفضاء السّيبراني. لأن القوة السّيبرانيّة كما عرفها ناي " هي القدرة على الحصول على النتائج المفضلة من خلال استخدام موارد المعلومات المترابطة إلكترونيًا في المجال السيبراني، وهي أيضًا القدرة على استخدام الفضاء السيبراني لخلق مزايا، والتأثير على الأحداث في بيئات تشغيليّة أخرى وعبر أدوات القوة المختلفة، وذلك لتحقيق نتائج مرغوبة في مجالات أخرى خارج الفضاء السيبراني من خلال استخدام الأدوات والتقنيات السّيبرانيّة في العمليات السّيبرانيّة[3].

ولكن في الواقع القوة السّيبرانيّة ما زالت تشهد تحولات، وتغيرات لم تصل الى مرحلة النّضج النهائي، فهي ما زالت في طور التكتل والنمو، وغير منتظمة، بسبب ما نشهده من تغيرات متسارعة في المجال الرقمي خاصة بعدما أصبحت قوة للتنافس الدّولي في الفضاء السيبراني. وبالعودة الى نشأتها، كانت في البداية تعرف بالقوة الرّقميّة ترتكز على قوة الإنترنت، ثم تحولت الى قوة مصادر المعلومات عندما بدأت وزارة الدفاع الأمريكيّة في العام 1969 اتصالًا بشبكة من أجهزة الكمبيوتر،[4] وفي العام 1972، أُنشئت رموز تبادل البيانات لتشكل شبكة إنترنت لتبادل حزم المعلومات (TCP/IP)، ثم في العام 1983 استُحدِث نظام أسماء النّطاقات لعناوين الإنترنت(DNS)، وترافق معه أولى فيروسات الكمبيوتر، ثم بدأت شبكة الويب العالمية في الظهور العام 1989 مثل جوجل، وموسوعة ويكيبيديا في العام 2001، وبدأت معها الشركات الكبرى رقمنة مشاريعها على الانترنت مثل –amazon , Ebay– في سلاسل التوريد العالميّة. وبشكل مماثل ظهرت الحوسبة السّحابيّة –cloud computing–لاستضافة الخوادم والخدمات وتخزين البيانات، وهكذا كان ميلاد القوة السّيبرانيّة تتحول، وتتطور إلى أن أصبحت قوّة جديده في استعمار البيانات، والسّيطرة عليها وقدرة حجبها عن العديد من الدول، وبدأت مؤشرات الهيمنة والسيطرة عندما أعلن الليبراليون أنّ "المعلومات يجب أن تكون مجانيّة"، ودول أخرى ترى أنّها حصرية لها، وبعد انتشار العمليات السّيبرانيّة أصبحت احدى الأدوات الناشئة في الفضاء السيبراني وإحدى مصادر القوة السّيبرانيّة لتصبح قوة تأثير وتأثّر.

2.الفرق بين القوة التقليدية والقوة السّيبرانيّة: القوة التقليديّة هي القوة الفعليّة المدركة للدولة التي يشعر بها المجتمع الإقليمي والدولي، وتعتمد على الأساليب التقليديّة الماديّة مثل الجيوش والأسلحة بما فيها الاقتصاد او لغة الاكراه، وتستخدم في الدّفاع والهجوم أو الردع في تحقيق الأهداف السياسيّة والاقتصاديّة ومصالح الدول. بينما القوّة السّيبرانيّة هي القوّة التي تعتمد على التكنولوجيا الرّقميّة بما فيها امتلاك المنصات، والمعلومات والأدوات السّيبرانيّة التي تمكّن الدول من شن عمليات سيبرانيّة تستهدف الشبكات وأنظمة الحاسوب،

1- Joseph S.(Nye), **Cyber Power**, may 2010, p4.

2- Jack Nagel, The Descriptive Analysis of Power, (New Haven, Yale University Press, 1975), p. 14.

3- Joseph S. Nye, Jr, The Future of Power in the 21st Century, Public Affairs Press, 2011, p. 12-1.

4- The Advanced Research Projects Agency Network (ARPANET) was the first wide-area packet-switched network with distributed control and one of the first computer networks to implement the TCP/IP protocol suite

وبسبب كلفتها المنخفضة وسهولة امتلاكها وصعوبة تعقّبها أصبحت أداة جذابة تُوظَّف في استراتيجيات الحروب الهجينة، والدفاع عن الأمن الرّقمي، ومهاجمة البنية التحتية، والتّجسس السيبراني، وتدمير أو تعطيل الأنظمة المعلوماتية للعدو عبر الشبكة العالمية.

على الرّغم من ضبابيّة المشهد السيبراني، وترسانات الأسلحة التقليديّة لم تعد المعيار الأساسي لقياس القوة بعد الثورة الرّقميّة، إلّا إنّ تكاملها مع القوة الوطنيّة أصبحت القوة السّيبرانيّة قوّة جانبيّة تساهم في تعظيم النفوذ، والقدرات الاقتصاديّة والدّفاعيّة والعسكريّة والأمنيّة العالمية في المجال الرقمي، إلّا أنّ اختلافها في المفهوم والوسائل والمجال الزمني والمكاني والهدف والتأثيرات. بدأت الدول والكيانات الأخرى تنظر اليها بأنّها وسيلة سهلة في تحقيق أهدافها بعيدًا من صدام الجيوش وإراقة الدّماء وبسبب الخصائص التي تتميز بها عن القوة التقليدية كما يبين الجدول (1).

جدول (1) مقارنة بين القوة التقليدية والقوة السّيبرانيّة

الخاصية	التكلفة	سهولة التنفيذ	صعوبة التعقب	نطاق التأثيرات	قياسها	تأسيسها
القوة التقليدية	عالية	صعبة	سهلة	نطاق جغرافي	مدركة	صعب
القوة السّيبرانيّة	بسيطة	سهلة	صعبة	عابرة للحدود	غامض	سهل

3. **سمات القوّة السّيبرانيّة:** إن المجال السّيبراني يختلف عن المجالات التّقليديّة الأخرى إذ إنّه المجال الوحيد من صنع البشر، ويخضع لتغيرات تكنولوجية ويتكيّف معها أسرع من المجالات الأخرى لقابلية أدواته على التعاطي مع هذا الفضاء. لذلك يقول أحد المراقبين: إنّ جغرافية الفضاء السيبراني أكثر قابلية للتغيير من المجالات الأخرى، إذ من الصعب تحريك الجبال والمحيطات، ولكن من السّهل تشغيل وإيقاف أجزاء بنى تحتية من الفضاء السيبراني بنقرة زر واحدة، ونقل المعلومات والبيانات عبر العالم بأقل تكلفة، وأسرع من نقل أدوات القوة التقليديّة (طائرات، دبابات، جنود، صواريخ) عبر السفن الكبيرة لمسافات طويلة [5]. وفي حين تظل السيطرة على المضائق بعيدة من متناول الجهات غير الحكوميّة في الدول المستقرة أو الفاعلة، وبالمثل، في حين أن هناك العديد من الجهات الفاعلة واللادولاتيّة قادرة أن تتحكم وتسيطر في الفضاء السيبراني وتنفذ عمليات سيبرانيّة دون علم حكوماتها [6]. فإنّ العوائق التي تحول من دون الدخول إلى المجال السيبراني منخفضة إذ يمكن للكيانات اللادولاتية، والدول الصغيرة والافراد أن تؤدي أدوارًا مؤثرة بمستويات منخفضة من التكلفة على عكس المجالات الاخرى.

على الرّغم من إنّ الدولة هي من يحتكر استخدام مجالات القوة التقليدية، ولكن يعتمد سلوك القوة السّيبرانيّة على مجموعة من الموارد والتقنيات والبنية التّحتية والشّبكات والبرمجيات والمهارات البشرية. وإنّ تنفيذ العلميات السّيبرانيّة خارج عن سيطرة الدولة، لذلك باتت القوة السّيبرانيّة أداة مهمّة في العلاقات الدّوليّة، وتؤدي دورًا بديلًا عن القوة التقليديّة في تحقيق الأهداف السياسيّة والعسكريّة والاقتصاديّة من دون اللجوء إلى القوة الصلبة بسبب الخصائص التي تتميز بها وأهمها:

[5]- Gregory J. Rattray, "An Environmental Approach to Understanding Cyber power," in Kramer, cited, 253-274, esp. 256.

-**السرعة(Speed)** : تميز القوة السّيبرانيّة المتمثلة بالعمليات السّيبرانيّة بسرعة الرد مقارنة بالحروب التقليدية أو الدبلوماسية. يمكن تنفيذ هجوم سيبراني في لحظات بقياس سرعة الانترنت، ما يتيح للدول استجابة سريعة لتغيرات المواقف أو التّهديدات، ما يعزز من فعالية القوة السّيبرانيّة في الأزمات.

-**الاسناد (attribute)** : هو القدرة على تنفيذ العمليات السّيبرانيّة من دون كشف هوية المهاجم أو اسنادها لجهة مسؤولة، ما يسمح للدول باستخدامها بشكل غير معلن، ويزيد من فرص الإنكار أو إخفاء المسؤولية.

-**الاستخدام من بعد(Remote Capability)** : يمكن تنفيذ العمليات السّيبرانيّة الدّفاعيّة والهجوميّة من بعد، من أي مكان في العالم من خلال استخدام جهاز كومبيوتر وإنترنت وشن عمليات على الخصوم دون الحاجة إلى وجود عسكري او تحريك مدافع او أن تتشظى في الهواء أصداء مدويّة [7].

-**القدرة على التوسع(Scalability)** : بسبب الترابط الشّبكي في العالم، يمكن استخدام العمليات السّيبرانيّة ضد دولة أو مجموعة ويمكن أن ينتشر الفيروس الى دول أخرى مثل ما حصل أثناء هجوم الفدية الخبيث، ويمكن تكييفها لتشمل الأنظمة الصّغيرة أو الكبيرة تتناسب مع مستوى التّهديد أو الهدف.

-**التّأثير العابر للحدود(Cross-border Impact)** : المجال السّيبراني لا يفهم الحدود الجغرافيّة، فيمكن للقوة السّيبرانيّة بشقيها الناعم والصلب أن تتخطى الحدود الشبكيّة للدول، وسيادتها ليشمل أيّ هدف في أي مكان، ما يعزز من فاعليتها في سياق العلاقات الدّوليّة، وتؤثر على عدة دول أو كيانات في وقت واحد، نتيجة للطبيعة العالميّة للإنترنت والشّبكات، ما يزيد من تعقيد الردود الدّوليّة ويدفع نحو التّوسع في التّعاون الأمني السيبراني بين الدول.

-**التّكلفة المنخفضة (Low Cost)**: إنّ هذه السمة شجّعت المنظمات والأفراد للانخراط في التأثير السّيبراني عالميًا، فالمقارنة مع العمليات العسكريّة التقليديّة، يمكن تنفيذ عمليات سيبرانية بتكلفة أقل بكثير. لا يتطلب الأمر معدات باهظة أو موارد بشريّة ضخمة. وهذه السّمة تجعل القوة السّيبرانيّة أكثر جاذبية للدول والكيانات اللادولاتية للانخراط بامتلاك هذه القوة واستخدامها.

-**التّأثير النّفسي(Psychological Impact)** : قدرتها على التأثير النّفسي من خلال العمليات السّيبرانيّة الهجوميّة، أو استخدامها في التّجنيد والتّرهيب ما يثير حالة من الفزع، وتضر بثقة الأنظمة الحكوميّة أو الاقتصاديّة كأداة لتقويض الاستقرار الداخلي في الدول المستهدفة من خلال التأثير على الرأي العام، وعلى معنويات الأفراد والمجتمعات.

-**السيطرة المركزية (Central control)**: وهنا نقصد بالسيطرة الرقمية واستعمار البيانات او الاستحواذ على السحابة والتحكم في تدفق البيانات، بحيث يمكن لمايكروسوفت او شركة امازون أو غوغل أن تقيّد الوصول الى معلومات عن جهة او موضوع معيّن، تستطيع شركة (Facebook) أو منصة (X) العرب من التسجيل او المشاركة وارزها منع الرئيس الأمريكي ترامب من المشاركة في منصة إكس، ومتجر (Apple) لديه العديد من التطبيقات المجانية في أمريكا ولكنها في الشرق الأوسط غير متاحة أو لا يمكن شرائها. ولذلك عمدت روسيا والصين الى توطين أنظمة كومبيوتر خاصة بها.

المطلب الثاني: أدوات وأساليب القوة السّيبرانيّة

تأثرت القوة السّيبرانيّة بالمفاهيم والدّراسات التي تمخضت عن مفهوم القوة التقليديّة، فقدّم الأكاديميون والباحثين في مجال القوة نقلًا عن توماس هوبز هانز مارغينثو Hobbes Hans Margenthau ، أمثال أستاذ القوة جوزف ناي وجون ميرشايمر Joseph

[7] Cyber Power - An Emerging Factor in National and International Security https://www.cirsd.org/en/horizons/horizons--autumn-2016--issue-no-8/cyber-power-an-emerging-factor-in-national-and-international-security

Nye and John Mearsheimer وغيرهم بتوظيف القوّة السّيبرانيّة في العلاقات الدّوليّة، وأفضت هذه التحقيقات الى تحديد أدوات وأساليب القوة السّيبرانيّة من عدة عناصر: التقنية، والسياسيّة، والاقتصاديّة، والرّمزيّة وعادة ما تُصنَّف في القوّة الصّلبة والنّاعمة.

1.أدوات القوة السّيبرانيّة: القوة النّاعمة والصلبة هي إحدى مكونات القوة السّيبرانيّة والتي تستخدم من خلالهما الأدوات التقنية الدّفاعيّة؛ والهجوميّة والاستباقيّة السّيبرانيّة، للتأثير على البنى التحتية للدول؛ والاقتصاد والسياسة والثقافة لتحقيق الأمن، أو التأثير من خلال حرمان الوصول الرقمي، أو تقييد العمليات الرّقميّة والتأثير على الرأي العام أو توجيه البيانات أو تعطيل الخدمات، وسأفصّل ذلك في ثلاثة أنماط للقوة في المجال السيبراني وهي من ثلاثة جوانب للقوة العلائقيّة مقارنة بالعمليات السّيبرانيّة، ويشير الجدول العمليات السّيبرانيّة الهجومية أو استخدام أدوات القوة السّيبرانيّة هي القوة الصّلبة، وقد تكون قوّة ناعمة في استخدامات أخرى، إذ يمكن استخدام أدوات المعلومات لإنتاج القوة النّاعمة في الفضاء السيبراني من خلال تقيد الأجندة أو الجذب أو الإقناع:[8]

أوجه القوة السّيبرانيّة	القوة الصلبة	القوة الناعمة
الوجه الأول: (أ) يجبر (ب) على القيام بشيءٍ لم يكن (ب) ليقوم به في البداية	–هجمات رفض الخدمة –تنصيب البرامج الضارة –اعتقال المدونين –تعطيل أنظمة SCADA	–حملة المعلوماتية لتغير أولويات واهداف المتسللين –تجنيد أعضاء المنظمات الإرهابية
الوجه الثاني: التحكم في القائمة: قدرة (أ) يمنع خيارات (ب)، من خلال استبعاد استراتيجيات(ب)	–استخدام جدران الحماية (firewalls) و(Filters) –الضغط على الشركات لاستبعاد بعض الأفكار	مزودو خدمات الإنترنت (ISP's) –محركات البحث يقومون بالمراقبة الذاتية –معايير وممارسات ICANN بشأن أسماء النطاقات –استخدام معايير وافضل الممارسات على البرمجيات المقبولة
قدرة الفاعل (أ) على إعادة جدولة أولويات الفاعل (ب)	تهديدات بمعاقبة المدونين الذين ينشرون مواد خاضعة للرقابة	–استخدام المعلومات لتغير المحتوى (نشر القومية)، تطوير معايير اشمئزازيه ضد (المواد الاباحية للمراهقين)

أ–القوة الناعمة السّيبرانيّة (Soft Cyber Power): وهي تشير إلى استخدام القدرات السّيبرانيّة للتأثير على الدّول والشّعوب الأخرى، وإقناعها في تشكيل تفضيلاتها وسلوكياتها من دون اللجوء إلى الإكراه أو العمليات السّيبرانيّة الهجوميّة، كما يبّن الجدول والتي تنطوي على التأثير الثقافي والدّبلوماسي والمعلوماتي، ولكنها تستفيد من التقنيات الرّقميّة والإنترنت في تحقيق اهدافها. ووسائل القوة السّيبرانيّة الناعمة المهمّة:

- **عمليات المعلومات والتأثير:** من خلال حملات وسائل التواصل الاجتماعي لنشر المعلومات، وتشكيل الرأي العام والترويج لأفكار محددة عبر إنتاج المحتوى الرقمي وتوزيعه (مقاطع الفيديو والمقالات) لتعزيز قيم الدولة وثقافتها وسياساتها، أو لتعزيز

[8] Nye, Joseph S. "Deterrence and Dissuasion in Cyberspace." International Security, vol. 41, no. 3, Winter 2016, pp. 44--71.

استخدام الدّبلوماسيّة الرّقميّة للانخراط في الحوار عبر الإنترنت والتّبادلات الثقافية لتعزيز التفاهم المتبادل وتحسين العلاقات الدّوليّة.

- **الدبلوماسية السّيبرانيّة:** وذلك من خلال التّعاون الدولي لبناء التّحالفات، والشّراكات من خلال الاتفاقيات والمبادرات المتعلقة بالأمن السّيبراني، وتعيين سفراء للدول مع الشّركات الكبرى في سليكون فالي، ورقمنة عمل السّفراء في القنصليات والوزرات على المواقع وتطبيقات التواصل الاجتماعي باللغات العالميّة. والمشاركة في وضع القواعد وبناء القدرات والمعايير الدّوليّة لسلوك الدولة المسؤول في الفضاء السيبراني في حماية سلاسل الإمداد ومواجهة الهجمات السّيبرانيّة[9].
- **التأثير الاقتصادي الرقمي:** من خلال صادرات التكنولوجيا والخدمات الرّقميّة لتعزيز الروابط الاقتصاديّة، والنّفوذ الذي يعزز مفهوم الدّبلوماسيّة التقنية بهدف التقدم التكنولوجي، والابتكارات لتعزيز حسن النية والتعاون، على سبيل المثال الصين تستخدم مشاريع البنية التحتيّة الرّقميّة مثل طريق الحرير الرقمي، لتوسيع نفوذها وبناء علاقات إلكترونية مع الدول الأخرى[10].
- **التعليم والتدريب السيبراني:** من المكونات المهمّة التي تساعد في انتشار القوة السّيبرانيّة الناعمة لأنها لغة التدريب الرقمي، وذلك من خلال المبادرات التعليميّة، وتقديم المنح الدراسية وبرامج التدريب والتبادل لبناء الخبرات السّيبرانيّة، وتعزيز حسن النية والتي تعزيز برامج التبادل الثقافي التي تركز على الثقافة الرّقميّة والوعي السيبراني. الاتحاد الأوروبي يدافع عن معايير قوية لحماية البيانات ويعزز الحقوق الرّقمية من خلال مبادرات مثل اللائحة العامة لحماية البيانات (GDPR). كوريا الجنوبيّة تستخدم صادراتها الثقافية، مثل موسيقى البوب الكورية والدراما الكورية، جنبًا إلى جنب مع المنصات الرقمية، لتعزيز نفوذها العالمي[11].

في المجالات كلها باتت أهمّية القوة السّيبرانيّة الناعمة تزداد في العصر الرقمي، فتسعى الدول إلى بناء النفوذ وتحقيق الأهداف الاستراتيجيّة من دون اللجوء إلى الصراع المباشر. فهو يستفيد من الطبيعة المترابطة للعالم الرقمي لتشكيل التّصورات وتعزيز التعاون على نطاق عالمي.

ب–القوة السّيبرانيّة الصلبة (Hard Cyber Power): القوة السّيبرانيّة الصلبة هي امتداد للقوة السّيبرانيّة، التي تُستخدم فيها القدرات السّيبرانيّة لممارسة القوّة القسرية، وهي تنطوي على عمليات سيبرانية هجوميّة ودفاعيّة تدمر وتعطل أنظمة معلومات الخصم والبنية التحتيّة، وتحقق الأهداف العسكرية الاستراتيجيّة، وأهم وسائلها:

- **القوة الهجوميّة السّيبرانيّة (Cyber Offensive Power):** وهي متمثلة العمليات السّيبرانيّة الهجوميّة التي تهدف إلى تعطيل أو إضعاف أو تدمير أنظمة أو شبكات معلومات الخصم، مثل هجمات DDoS (رفض الخدمة الموزعة) التي تغرق شبكة الخصم بحركة المرور تجعلها غير قابلة للاستخدام، او استخدام البرامج الضارة وإدخال برامج ضارة لتلف البيانات أو سرقتها أو تدميرها) مثل برنامج Stuxne الذي استهدف أجهزة الطرد المركزي النووية الإيرانيّة، أو هجمات برامج الفديّة حيث تمّ تشفير بيانات المستخدمين وقيّد الوصول اليها مقابل الدّفع بعملة(bitcoin) مقابل رفع التشفير عنها، بالإضافة الى التجسس السيبراني لسرقة المعلومات الحساسة، أو الملكية الفكرية أو أسرار الدولة للحصول على ميزة استراتيجيّة، وعمليات التهديدات

[9] Nye, Joseph S. "Deterrence and Dissuasion in Cyberspace." International Security, vol. 41, no. 3, Winter 2016, pp. 44--71.

[10] Kalathil, Shanthi, and Taylor C. Boas , Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule, Carnegie Endowment for International Peace, 2003.p.135.

[11] Carr, Madeline,US Power and the Internet in International Relations: The Irony of the Information Age, Palgrave Macmillan, 2016,p.p.15-30.

المستمرة المتقدمة (APTs) يمكن أن تبقى في الشبكة لمدة طويلة غير مكتشفة أثناء جمع المعلومات الاستخباريّة، والعمليات النفسيّة السّيبرانيّة التي تهدف إلى نشر المعلومات المضللة، أو التلاعب بالرأي العام، وخلق الارتباك والذعر بين سكان الخصم[12].

- **القوة الدّفاعيّة السّيبرانيّة (Cyber Defensive Power):** وهنا نعني بها الأمن السّيبراني أو سياسات الأمن السّيبراني الدّفاعيّة التي تشمل العمليات السّيبرانيّة الدّفاعيّة وهي تدابير وإجراءات ومعايير دوليّة تعرف بأفضل الممارسات لحماية البنية التّحتيّة الحيويّة للدولة والشّبكات العسكريّة وأنظمة المعلومات من الهجمات السّيبرانيّة، وأهم هذه الأدوات: أنظمة كشف التّسلل، وجدران الحماية، التشفير، والاستجابة للحوادث. وهدفها للتخفيف من حدّة الحوادث السيبرانية.
- **القوة السّيبرانيّة الاقتصادية (Cyber Economic Power):** وهي المتمثلة بالعمليات السّيبرانيّة الهجومية على الاقتصاد الرقمي أو المؤسسات المالية، أو من خلال العقوبات الاقتصاديّة التي تفرضها الدّول لمواجهة العمليات السّيبرانيّة.

وعادة العمليات الدّفاعيّة والهجومية منوطة بالدول الكبرى التي لديها قوة عسكرية سيبرانية على مستوى عال، كالناتو والولايات المتحدة " القيادة السّيبرانيّة الأمريكية"(USCYBERCOM) [13]. وروسيا تُعرف بعملياتها السّيبرانيّة المتقدمة التي تشمل التدخل في الانتخابات الأجنبيّة، والتّجسس الإلكتروني، وتنفيذ هجمات تخريبيّة تستهدف البنية التحتية الحيوية. أمّا الصين، فهي تنخرط في عمليات تجسس سيبراني واسع لجمع المعلومات الاستخباريّة، والتكنولوجيّة إلى جانب تطوير قدرات هجوميّة متقدمة في المجال السيبراني. من جهة أخرى، يتمتع الكيان الصهيوني بقدرات سيبرانية عالية، تُنسب في الغالب إلى الوحدة العسكرية 8200 التي تشارك في عمليات دفاعيّة وهجوميّة، إضافةً إلى امتلاك أداة التجسس العالميّة "بيغاسوس" التي تُعد واحدة من أكثر أدوات التجسس تطورًا على مستوى العالم.

2.القوة الذكية في الفضاء السيبراني:(Cyber Smart Power) : تأسيسًا على ما جاء في فهم القوة الناعمة والصلبة، وإتماما الى تعريف القوة الذكية التقليديّة الذي يقول، إنّها سياسة تهدف إلى استخدام استراتيجي للدّبلوماسيّة في الاقناع والخضوع للخصم من دون مقاومة بتسخير كل الأدوات من القوّة الصّلبة المتمثّلة في زيادة القوّة العسكريّة والاقتصاديّة والقوّة النّاعمة المتمثّلة باستثمار القيم[14]. يمكن أن نستنتج مفهوم القوة الذّكيّة السّيبرانيّة (Cyber Smart Power) أنّها مزيج من القوة الصلبة، والقوة الناعمة في المجال السيبراني يحقق للدول أهدافًا استراتيجيّة في المجال السيبراني. على سبيل المثال، يمكن لدولة ما استخدام الهجمات السّيبرانيّة (قوة صلبة) لتعطيل أنظمة الخصم، وفي الوقت نفسه تُستخدم وسائل الإعلام الرّقميّة والمنصّات الاجتماعيّة للتأثير على الرأي العام العالمي (قوة ناعمة).

المبحث الثاني: تأثيرات القوة السّيبرانيّة على العلاقات الدّوليّة في الفضاء السيبراني

القوة السّيبرانيّة لم تعد تشير على نمو الدول رقميًّا، بل أصبحت قوّة مؤثرة في الفضاء السيبراني قادرة على تغيير ديناميكيات القوة التقليديّة، وتوسيع مجالات الصراع والتّعاون، وتغيير موازين القوى وتوسيع ونطاق السياسة الخارجية، لذلك سنبين تأثير القوة

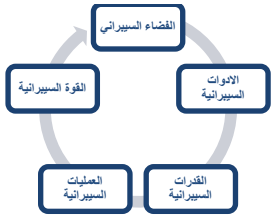
[12] Healey, Jason (ed.), A Fierce Domain: Conflict in Cyberspace, 1986 to 2012, Cyber Conflict Studies Association, - 2013, P.153.
[13] Clarke, Richard A., and Robert K. Knake, Cyber War: The Next Threat to National Security and What to Do About It, - Ecco, 2010,
[14] – ليلى نقولا، العلاقات الدولية .. من تأثير القوة الى قوة التأثير، الأرز للنشر، لبنان ، 2021، ص211.

السّيبرانيّة على الفضاء السيبراني، والعلاقات الدّوليّة من خلال مطلبين، سأبيّن في الأول توظيف القوة السّيبرانيّة في العلاقات الدّوليّة، بينما في الثاني سأحاول أن نظهّر تأثير القوة في العلاقات الدّوليّة على السياسة والاقتصاد والسّيادة السّيبرانيّة.

المطلب الأول: توظيف القوة السّيبرانيّة في العلاقات الدّوليّة

بات من المؤكد أن القوة السّيبرانيّة تؤثر بشكل كبير في العلاقات الدّوليّة، وأصبحت أحد المفاهيم الحديثة في العلاقات الدّوليّة، نتيجة لتوسع الفضاء السّيبراني وزيادة أهميته في حياة الدول والمجتمعات، وتؤثر بشكل كبير على كيفيّة تفاعل الدّول وتنافسها في العصر الرّقمي، وهو ما دفع المفكرين مثل جوزيف ناي Joseph Nye إلى الربط بين القوة وفاعليتها في تحقيق الأهداف، وتتيح تحقيق مزايا وتأثيرات في مختلف المجالات عبر استغلال الموارد الرّقميّة.

تقاطع القوة السّيبرانيّة في الفضاء السيبراني: يبيّن الرّسم البياني إنّ القوة السّيبرانيّة تتقاطع في أدوات بيئة الفضاء السيبراني، وكلها تحقق بعضها ولا يمكن لقيام أي منها من دون الأخرى، ولكن العمليات السّيبرانيّة تحقق الصراع، والأدوات السّيبرانيّة تحقق التنافس، والقدرات تحقق التعاون، ثم كلّها تحقق القوة السّيبرانيّة، وتكاملها يحقق الفضاء السيبراني أي البيئة التي تحدث فيها هذه الأنشطة.



بسبب هذه التفاعلات تكمن أهمية القوة السّيبرانيّة في العلاقات الدّوليّة، أداة لتحقيق التفوق من دون اللجوء إلى القوة العسكريّة التقليديّة، وحاجة أساسية لحماية الأمن القومي وركيزة جديدة في قواعد الردع السّيبراني. إلى تأثيرها على السياسات الداخليّة، وسلوك الدول الأخرى في العلاقات الدّوليّة في الفضاء السيبراني، وتسهم في تعظيم النفوذ والقدرات الاقتصادية والدّفاعيّة والعسكريّة، والأمنية العالميّة وحتى الصراع الدولي اتّجه نحو المنافسة وتعزيز النفوذ في مجال التكنولوجيا، والابتكار الذي غيّر من شكل الصراعات والحروب وأدواتها، وساهم في إعادة التّفكير في حركيّة وديناميكيّة العلاقات الدّوليّة، لأنّ القوة السّيبرانيّة وعناصرها أزاحت العديد من عناصر القوة التقليديّة من مكانها. فامتلاك الدول الأموال والثروات والقدرات العسكريّة والجغرافيا الشاسعة وكثرة السكان، لم يعد كافيًا لبلورة دورها كقوة فاعلة، ومؤثرة في السياسات العالميّة التي تتحكم في الفضاء السيبراني. بل أصبحت ساحة للتغلب على القوى العظمى بديلًا عن القوة التقليديّة العسكرية، في ظل العسكرة المتزايدة للفضاء السيبراني، وغياب الإنذار المبكر في الصراعات السّيبرانيّة ما يشكل ضبابيّة للوقوف على القوة السّيبرانيّة الواقعيّة لكل دولة وفاعل دولي بالنظام العالمي، لأنّ القوة السّيبرانيّة استندت على إحدى مرتكزاتها العمليات السّيبرانيّة ميزة التنكر، وعدم الوضوح الذي يغلب عليها السرية وعدم المكاشفة، ما خلق نقصًا في البيانات المتاحة حول قدرتها مثل عدد العسكريين العاملين في الفضاء السيبراني، أو عدد الأشخاص داخل المخابرات المختصين سيبرانيا، بالإضافة الى نوعية القدرات ومفاعليها وقدرتها على الوصول الى أي مكان في ساحة النشاطات.

لذلك أصبحت القوة السّيبرانيّة عاملًا مؤثرًا بشكل كبير في تشكيل العلاقات الدّوليّة المعاصرة، وتأثيرها يعد جزءًا من التطور الأوسع في طبيعة القوة في النّظام الدّولي. فهي تجمع بين القوة الصلبة من خلال الهجمات السّيبرانيّة والقوة الناعمة من خلال التأثير على الأفكار والقيم عبر الإنترنت، ما يجعلها عاملًا أساسيًّا في تشكيل ديناميكيات السياسة الدّوليّة الحديثة في سياق العلاقات الدّوليّة، وفي أفق

ومجالات جديده تتحكم بها القوة السّيبرانيّة أدت إلى إحداث تحولات جوهرية في مفهوم القوة وديناميكيات الصّراع بين الدّول على الشكل الآتي:

–**تغيير ديناميكيات القوة التقليديّة:** من مبادئ المدرسة الواقعيّة أن الدول هي أبرز الفاعلين في السياسة الدّوليّة، لكن ظهور أنماط جديدة من القوة أدّت إلى بروز فاعلين جدد في الفضاء السيبراني يهددون ديناميكيات القوة التقليدية، ما أدى إلى إعادة ترتيب منظومة الفاعلين في العلاقات الدّوليّة. إذ لم تعد الدّول وحدها هي اللاعب الرئيس، بل ظهرت كيانات جديدة من غير الدّول قادرة على التأثير دوليًا مثل الأفراد والمنظمات والجماعات الإرهابيّة السّيبرانيّة تنافس الدول وتزعزع أمنها واستقرارها في البيئة الدّوليّة. وبعض الدول تستخدمها في لإخفاء أفعالها وتمويل أنظمتها. وفاقًا لجوزيف ناي Joseph Nye، أصبحت القوة السّيبرانيّة قادرة على خلق تأثيرات في مجالي القوة الناعمة والصلبة. فيمكن استخدامها في الدبلوماسيّة العامة عبر الإنترنت، كما يمكن توظيفها لإلحاق أضرار مادية بأهداف في دول أخرى.

–**توسيع مجالات الصراع والتّعاون:** خلق الفضاء السيبراني مساحات جديدة للتفاعلات الدّوليّة، سواء في مجال التعاون أو الصراعات. فتتمثل الصراعات السّيبرانيّة بالعمليات السّيبرانيّة التي تستهدف بنى تحتية حيوية تؤدي إلى تصعيد التوترات بين الدول، أو تؤثر على الرأي العام خلال الحملات الانتخابيّة مما تعدُّه الدّول تدخلًا في شؤونها الداخليّة ولا سيما بين روسيا، والولايات المتحدة والذي يؤدي بدوره الى تآكل الثقة بين الدّول وتتبادل العقوبات أو تصريحات عالية النبرة وربما ردود عسكرية تقليديّة. وفي المقابل أصبحت قضايا مثل الأمن السيبراني والجريمة السّيبرانيّة محور نقاشات دبلوماسيّة مهمة أسست تحالفات دوليّة، مثل جهود الأمم المتحدة ومبادرات مثل "اتفاقيّة بودابست" والعيون الخمس والناتو لمكافحة التهديدات السّيبرانيّة.

–**توازن القوى (Balance of power):** أدى تصاعد القوة السّيبرانيّة المتنامي الى خلل في توازن القوى في العالم الرّقمي والعلاقات الدولية، بعدما أتاحت القوة السّيبرانيّة للدول الصغيرة، والمتوسطة فرصة تحدي الدّول التقليديّة الكبرى في السّاحة الدّوليّة، مثل كوريا الشّماليّة وإيران، تستخدم القوة السّيبرانيّة لمواجهة دول أكبر وأكثر قوة سياسيًا وعسكريًا، ما غيّر طبيعة الصراعات والمنافسة بين الدول. وفي التأثير السياسي والدبلوماسي، استخدمت روسيا والصين قدراتها السّيبرانيّة لتعزيز نفوذها الدولي عبر التأثير على القرارات السياسيّة للدول الأخرى، مثل التدخلات السّيبرانيّة في الانتخابات الأمريكية 2016. بالإضافة الى التأثير العسكري ومحاولة إضعاف القدرات الدّفاعيّة للخصوم من خلال شن عمليات سيبرانيّة، تهدف إلى تعطيل البنية التّحتيّة العسكريّة والأنظمة الدّفاعيّة للخصوم، على سبيل المثال الهجوم على منشأة "نطنز" النّووية الإيرانيّة باستخدام فيروس "Stuxnet". والتأثير الاقتصادي أو التّجسس الصناعي والاقتصادي، حيث تسعى الدول لاختراق أنظمة الدّول الأخرى للحصول على أسرار صناعية وتقنية، ما يمنحها ميزة تنافسية، مما ساهم في ظهور "عصر القوة النّسبيّة"، لأنّ القوة العسكريّة التقليديّة غير كافية وحدها لتأمين البنية التحتيّة الرقمية للدول، فأثّر على توازنات النّظام الدولي. وهذا يؤثر على تشكيل التحالفات الاستراتيجيّة بين الدول، إذ تتحالف بعضها لمواجهة التّهديدات السّيبرانيّة المتزايدة، بينما تعتمد أخرى على تطوير قدراتها السّيبرانيّة لتحقيق الردع[15].

–**تمدد السياسة الخارجيّة:** بفضل انخراط القوة السّيبرانيّة في العلاقات الدّوليّة، وسّع نطاق الأدوات الدّبلوماسيّة أصبحت القوة السّيبرانيّة أداة دبلوماسيّة جديدة تستخدمها الدول لتحقيق أهدافها الخارجيّة. فهي تتيح للدول ممارسة الضغط والتأثير على الدول الأخرى بطرق غير

[15] – أنماط "الحرب السيبرانية" وتداعياتها علي الأمن العالمي، متوافر على الموقع الالكتروني ، https://www.siyassa.org.eg/News/12072.aspx، تاريخ الزيارة 24-8-2024.

تقليديّة، وبتكلفة أقل مقارنة بالوسائل التقليدية. ما دفع الدول بتطوير وحدات خاصة مسؤولة عن الحرب الإلكترونيّة، والاستخباراتيّة الى تعزيز القدرات الاستخباراتيّة من خلال استخدام أدوات القوة السّيبرانيّة في جمع المعلومات الاستخباراتيّة أكثر فعالية، تؤثر على صنع القرار في السياسة الخارجية وعلى العلاقات الدّوليّة والتأثير على الرأي العام.

–**تحوّل في ديناميكيات الحروب:** مع بروز القوة السّيبرانيّة كعامل مؤثر في العلاقات الدّوليّة تغيّرت معها بعض المفاهيم التقليديّة كالرّدع والسّيطرة والحروب. في المجال التقليدي، يعتمد الردع على إظهار القوة العسكريّة علنًا، بينما في المجال السّيبرانيّة القوة السّيبرانيّة غير مادية ولا يُشعر بها إقليميًّا أو دوليًّا، فالدّول الصغيرة وغير الفاعلة سياسيًّا واقتصاديًّا تتبنى نهج خدماتي رقمي عالمي على سبيل المثال الفليبين، وعمان لديها صناعات سيبرانيّة وتقنيّة ولكنها غير قادرة على مواجهة الصين لا سيبرانيا ولا عسكريًّا. فميزة الإنكار والغموض في المجال السيبراني أضعف فعاليّة الردع التقليدي، لذلك بدأت الدول تتجه الى الرّدع السيبراني وبناء القدرات السّيبرانيّة لقياس قدرة الأعداء سيبرانيًّا لردعها اقتصاديًّا وسياسيًّا. وتقليديًّا كانت الدّول تسيطر على الدول الأخرى بالتّفوق العسكري، أو الاحتلال المادي بينما في مجال أُذيبت فيه الحواجز الجغرافيّة تسعى الدول إلى السيطرة على تدفق المعلومات من خلال مراقبة الإنترنت، والبنية التّحتيّة الرقميّة لضمان عدم استخدام هذه الشبكات ضد مصالحها وضد سيادتها[16].

وأدى ظهور العمليات السّيبرانيّة الهجوميّة، والدّفاعيّة إلى صراعات تدور في الفضاء الرقمي بهدف تحقيق أهداف سياسيّة أو عسكرية من دون استخدام القوات التقليدية، على سبيل المثال، الهجوم السيبراني الروسي على إستونيا العام 2007، بصور غير متكافئة فمنحت القوة السّيبرانيّة الدول الصغيرة، والجماعات اللادولاتيّة قدرة على مواجهة دول أقوى، ما يجعل الحروب أكثر تعقيدًا وأقلّ ارتباطًا بالتفوق التقليدي وخاصة إنّها بدأت تستخدم في الحرب الهجينة، وتؤثر على الشبكات المدنية في مراكز الرعية الصحية وخدمات الكهرباء والماء[17].

بعد هذه التحولات لا شك إنّ القوة السّيبرانيّة تشكل عاملًا مهما في تشكيل موازين القوى العالمية وأنماط التفاعل بين الدول والفاعلين من غير الدول. وساهمت في تغيير جذري في طبيعة العلاقات الدّوليّة وآليات إدارة الصراعات وتحقيق المصالح على الساحة العالمية، وعاملًا في تشكيل السياسات الخارجية للدول، إذ توفر أدوات جديدة للتأثير والضغط والدفاع في الساحة الدّوليّة. ومع تزايد أهمية الفضاء السيبراني، من المتوقع أن يزداد تأثير هذه القوّة على العلاقات الدّوليّة في المستقبل.

المطلب الثاني: تأثير القوة السّيبرانيّة على العلاقات الدّوليّة

بعدما أصبحت القوة السّيبرانيّة عاملا مهما في العلاقات الدّوليّة وتعكس قدرة الكيانات على استخدام الفضاء السيبراني لتحقيق أهداف سياسيّة أو اقتصاديّة أو عسكريّة أو اجتماعيّة، وتؤثر بشكل كبير على ميزان القوى والحروب والصراعات كما أشرنا في المطلب السابق. ويتجلى تأثيرها من خلال مجموعة متنوعة من الأنشطة السّيبرانيّة، مثل العمليات السّيبرانيّة، والتّجسس، بالإضافة إلى التأثير على الرأي العام وصنع القرار سياسيًّا واقتصاديًّا وعسكريًّا واجتماعيًّا. لكن بسبب حدود البحث سأتناول الآثار السياسيّة بين روسيا وأمريكا والاقتصاديّة على مستوى الجرائم السّيبرانيّة.

16 –محمد زيتون، نحو إستراتيجية فعّالة للأمن السيبراني في لبنان، رسالة ماجستير غير منشورة، الجامعة اللبنانية –كلية فؤاد شهاب، 2022.

17 – نفس المصدر

1. القوة السّيبرانيّة كأداة تحقيق أهداف سياسية ودبلوماسية:

– **وسيلة لممارسة الضغط:** استخدام القوة السّيبرانيّة في التفاوض، أو ممارسة الضغط في المفاوضات الدبلوماسية لتحقيق أهداف سياسية، فيمكن من خلالها التأثير على الطرف الآخر من خلال استخدام عمليات سيبرانية هجوميّة لتعطيل البنية التحتية، أو إلحاق الضرر بالأنظمة الحيوية لدولة بهدف خلق بيئة ضاغطة على الحكومات، أو المفاوضين للاستجابة لمطالب الطرف المهاجم. على سبيل المثال الهجوم الروسي على استونيا.

–**استخدام العمليات السّيبرانيّة كقوة سيبرانية ناعمة:** القوّة الناعمة تتعلق باستخدام الجاذبيّة والإقناع لتحقيق الأهداف من دون استخدام القوة الصلبة، ويمكن أن تُستخدم بشكل غير مباشر كجزء من القوة السّيبرانيّة الناعمة من خلال التأثيرات التي تحدثها على الأفراد، الحكومات، أو الرأي العام فتدفعها لاتخاذ قرارات معيّنة بالتهديد عن كشف الفساد، أو المعلومات المضللة التي تؤدي إلى تعزيز صورة الفاعل السيبراني كقوة مصلحة للعدالة أو الحرية.

2.التأثير على الاستقرار السياسي:

–**التأثير على نتائج الانتخابات:** كان التدخل الروسي في الانتخابات الرئاسيّة الأمريكيّة 2016 عندما دعمت هيلاري كلينتون Hillary Clinton الاحتجاجات التي تلت الانتخابات الرّوسيّة في مارس 2012، ما أدى إلى احتجاجات ومعارضة داخليّة وقمع من السلطات الروسية. رأت روسيا في دعم كلينتونClinton لهذه الاحتجاجات محاولة لزعزعة الاستقرار السياسي في البلاد. في 2015، كُشِف استخدام كلينتونClinton لبريد إلكتروني خاص بدلًا من البريد الرسمي. استغلت روسيا هذه القضية وانتقمت من كلينتون Clinton عبر قرصنة، رسائلها الإلكترونيّة ونشرها للتشكيك في نزاهة الانتخابات الأمريكيّة، والتأثير على نتائجها لصالح دونالد ترامب Donald Trump . وكان التّدخل الروسي من خلال أنشطة متنوعة تهدف إلى التأثير على نتائج الانتخابات وتوجيه الرأي العام الأمريكي، وقد أثار جدلًا واسعًا وأدى إلى تحقيقات موسعة داخل الولايات المتحدة. ومن العمليات الرّوسيّة المهمّة:

– **حملات التضليل عبر وسائل التواصل الاجتماعي** (Phishing& impersonation attack): استخدمت روسيا وسائل التواصل الاجتماعي لنشر معلومات مضللة، ومحتويات مثيرة للانقسام بهدف زعزعة الثقة في العملية الديمقراطية الأمريكيّة، عملت مجموعات مثل "وكالة أبحاث الإنترنت (IRA) "الرّوسيّة على إنشاء حسابات مزيفة تهدف إلى التأثير على النّاخبين، ونشر الأخبار الكاذبة المؤيدة والمعادية وركزت هذه الحسابات على إثارة التوترات العرقيّة والدّينيّة، ودعم دونالد ترامبDonald Trump والهجوم على هيلاري كلينتونHillary Clinton .

– **اختراق وتسريب البيانات** (SQL Injection Attack) اخترق قراصنة روس شبكات الحزب الديمقراطي، بما في ذلك اللجنة الوطنية الديمقراطيّة (DNC) وحملة هيلاري كلينتونHillary Clinton الرّئاسيّة. ثم قاموا بتسريب هذه المعلومات عبر منصات مثل "ويكيليكس"، ما أضر بصورة الحزب الديمقراطي والمرشحة هيلاري كلينتونHillary Clinton .

– **الهجمات السّيبرانيّة على البنية التحتية الانتخابيّة:** حاولت جهات روسية اختراق أنظمة التصويت في بعض الولايات الأمريكيّة. فقد استخدم ضباط المخابرات العسكرية الروسية أيضًا رسائل بريد إلكتروني ضارّة، للوصول إلى شبكة كمبيوتر لجنة الحملة الانتخابية الديمقراطية في الكونجرس، قام المتسللون بتثبيت برامج ضارة سمحت لهم بالوصول إلى المزيد من أجهزة الكمبيوتر، وسرقة آلاف رسائل

البريد الإلكتروني والوثائق المتعلقة بالانتخابات. هذه المحاولات أثارت قلقًا كبيرًا بشأن سلامة أنظمة التصويت وشفافيّة العمليّة الانتخابيّة[18].

-**الأهداف الرّوسيّة من التدخل:** إضعاف الثقة في الديمقراطيّة الأمريكيّة، وتقويض النّظام الديمقراطي الأمريكي وإظهاره بمظهر غير مستقر. دعم مرشح مفضل (دونالد ترامب Donald Trump) بالاعتقاد أنّ ترامبTrump يمكن أن يتبنى سياسات أكثر مرونة تجاه روسيا. والتأثير على السياسة الخارجيّة الأمريكيّة خصوصًا في ما يتعلق بالعلاقات بين البلدين وتخفيف العقوبات المفروضة على موسكو بعد ضمها شبه جزيرة القرم في2014 [19].

3.تأثير القوة السّيبرانيّة على الاقتصادي العالمي: أدّت الرقمنة الاقتصاديّة دورًا متزايد في التفاعلات الدّوليّة، أتاح للشركات المتوسطة والصغيرة الوصول إلى أسواق عالمية جديدة، يزيد من حجم التبادل التجاري بين الدول ويعزز التدفقات التّجاريّة والتعاون في مجال الابتكار والتّطوير التكنولوجي، واستغلت بعض الدول والمنظمات القوة السّيبرانيّة المتمثلة بالعمليات السّيبرانيّة، وشن عمليات ذات تأثيرات عميقة على الاستقرار الاقتصادي العالمي على الشكل الآتي:

-**الأضرار الاقتصاديّة:** استهدفت العمليات السّيبرانيّة الهجوميّة الاقتصاد الدّولي والمحلي والعديد من المرافق الحيويّة والبنية التحتيّة الحيويّة، للشّركات، والحكومات، والبنوك، ما يؤدي إلى تأثيرات واسعة على الاقتصاد والمجتمع ناتجة عن عمليات وجرائم سيبرانيّة. وفقًا لشركة ماكافي ومركز الدراسات الاستراتيجية والدّوليّة، فإنّ الجرائم السّيبرانيّة مسؤولة عن خسارة حوالى واحد في المائة من الناتج المحلي الإجمالي العالمي كل عام، وقد تصل تكلفة الجرائم السّيبرانيّة إلى 600 مليار دولار في الولايات المتحدة كما موضحة حسب المنطقة في الجدول أدناه[20].

المنطقة (البنك الدولي)	الناتج المحلي للمنطقة تريليونات الدولارات	تكلفة الجرائم السّيبرانيّة مليارات الدولارات	خسائر الجرائم السّيبرانيّة بالنسبة إلى الناتج المحلي
أمريكا الشمالية	20.2	175 – 140	%0.87–0.69
أوروبا وآسيا الوسطى	20.3	180 – 160	%0.89–0.79
شرق آسيا والمحيط الهادئ	22.5	200 – 120	%0.89–0.53
جنوب آسيا	2.9	15 – 7	%0.52–0.24
أمريكا اللاتينية والبحر الكاريبي	5.3	30 – 15	%0.57–0.28

[18] Hacking the Democratic National Committee, Available on internet , https://time.com/5565991/russia-influence-2016--election/ , visited 19-10-2024.
[19] The Perfect Weapon: How Russian Cyberpower Invaded the U.S ,Available on internet , -https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html , visited 19-10-2024.
[20] Economic impact of cybercrime , available on internet, https://www.helpnetsecurity.com/2018/02/23/economic-impact--of-cybercrime/, visited 23-2024.

جنوب الصحراء الكبرى أفريقيا	1.5	3 – 1	%0.20–0.07
الشرق الأوسط (MENA)	3.1	5 – 2	%0.16–0.06
العالم	$75.8	$608–$455	%0.80–0.59

ويضيف نائب الرئيس الأول في مركز الدراسات الاستراتيجيّة، والدّوليّة (جيمس لويسJames Lewis)، حسب أبحاث وتحقيقات المركز أن روسيا هي الرائدة في مجال الجرائم السّيبرانيّة، وتأتي كوريا الشّمالية في المرتبة الثانية، فتقوم هذه الدول سرقة العملات المشفرة لتمويل أنظمتها ومساندتها على البقاء بسبب العقوبات، وتشهد العديد من الدول تصاعدًا في نسبة الجرائم السّيبرانيّة خاصة في الدّول النامية ذات النية التحتيّة الهشة، وتشهد عمليات تجارية كثقة بما في ذلك البرازيل والهند وفيتنام[21].

تكلف الجرائم الإلكترونية الشركات ما يقرب من 600 مليار دولار، أو 0.8 في المائة من الناتج المحلي الإجمالي العالمي، وهو ما يزيد عن دراسة أجريت العام 2014 والتي قدرت الخسائر العالميّة بنحو 445 مليار دولار عن تقرير من شركة ماكافي، بالشراكة مع مركز الدراسات الاستراتيجية والدّوليّة (CSIS). وتتضمن تكاليف الجرائم الإلكترونية إتلاف وتدمير البيانات، سرقة الأموال، فقدان الإنتاجيّة، سرقة الملكية الفكرية، سرقة البيانات الشّخصيّة والماليّة، الاختلاس، التّعطيل بعد الهجوم لسير العمل الطبيعي، التحقيق الجنائي، تكلفة التعافي بعد الهجوم الإلكتروني، الضرر الذي يلحق بالسمعة، التكاليف القانونية، الغرامات التنظيمية المحتملة، فقدان الثقة، ومدفوعات الفدية[22].

– **استهداف أسواق مالية عالمية ومنشآت حيوية:** تطور العمليات السّيبرانيّة الهجومية والجرائم بشكل لافت، أصبحت تستهدف أسواق مالية عالمية ومنشآت حيوية خسائر تكبد الاقتصاد العالمي بشلل يستغرق أيامًا للتعافي، ويلاحظ إنّ خلال العام 2022 ارتفعت الهجمات السيبرانية بمختلف أشكالها بنسبة 38 بالمئة على المستوى العالمي، و وفق بيانات ستاتيستا سجلت خسائر بقيمة 8.4 تريليون دولار أميركي، مقابل 5.99 تريليون دولار في العام 2021. الولايات المتحدة من أكثر الدول تعرضًا لهذا النمط من الهجمات. من المتوقع أن تتجاوز التكلفة العالمية للجرائم الإلكترونية 8 تريليون دولار في العام 2022. ومن المتوقع أن يتجاوز الرقم 11 تريليون دولار في العام 2023. وتتوقع الإحصائيّات أن تكلف الجرائم الإلكترونيّة الاقتصاد العالمي أكثر من 20 تريليون دولار أمريكي بحلول العام 2026، بزيادة قدرها 1.5 مرة مقارنة بالأرقام في العام 2022.[23] أستعرض أبرز أنواع العمليات السّيبرانيّة (الجرائم السّيبرانيّة) الذي تؤثر على الاقتصاد:

أبرز الهجمات أثرا على الاقتصاد العالمي				
#	السنة	أبرز الهجمات	الخسائر المالية $	الخسائر التقنية	الدول المستهدفة
1	2013	yahoo attack	350 مليون	3 مليارات حساب مستخدم	عالميا

[21] Same reference.-
[22] Cybercrime To Cost The World $9.5 Trillion USD Annually In 2024, available on site, https://www.esentire.com/web-native-pages/cybercrime-to-cost-the-world-9-5-trillion-usd-annually-in-2024
[23] إنفوغراف: 8.2 تريليون دولار خسائر الهجمات السيبرانية بنهاية 2023، https://rb.gy/xnbkco متوافر على الموقع الالكتروني

2	2014	Sony attack	35 مليون	تدمير محتويات الخوادم	الولايات المتحدة
3	2015–2016	Bangladesh swift attack	81 مليون	أنظمة SWIFT	بنغلادش
4	2017	attack NotPetya	10 مليارات	49000 جهاز كمبيوتر وتدمير 1000 تطبيق	60 دولة
5	2017	WannaCry	4 مليارات	230 ألف كمبيوتر	150 دولة
6	2019–2020	solarwinds attack	171 مليون	عدة سيرفرات تخزين	الولايات المتحدة
7	2021	Exchange attack	10 مليارات	250 ألف خادم (Servers)	عالميا

4.السيادة السّيبرانيّة بين فكّي المهينة والسيطرة: إن اختلاف وجهات النظر حول الفضاء السيبراني جعل مفهوم السيادة أكثر تعقيدًا، فالولايات المتحدة والمملكة المتحدة يريدان فضاء سيبرانيًّا فوضويًّا يعكس الواقع الدّولي مع دور أساسي للقطاع الخاص، ومن دون حاجة تدخّل الحكومات في حوكمة الانترنت وغدارة التدفقات الرقميّة، وأن تكون تدفّقات البيانات بالمفهوم الليبرالي، وروسيا والصين يريدان فضاءً سياديًّا منظمًا له دور أساسي للدولة والتدخل الحكومي لإدارته، ما جعل السيادة السّيبرانيّة محورًا للجدال تجزئها المصالح، تتراوح بين التّشريعات المحليّة والدّوليّة والأنظمة الحاكمة، والحوكمة وسياسات الأمن السيبراني والعمليات السّيبرانيّة، وتتمثل في ثلاثة تناقضات:

– **السيادة السّيبرانيّة وروح الإنترنت:** السيادة السّيبرانيّة تشير إلى مبدأ أنّ الدول لها الحق في التحكم في الفضاء السيبراني داخل حدودها وخارجها، بما في ذلك إدارة الإنترنت وتنظيمه، والسّيطرة على البيانات والمعلومات التي تنتقل عبر شبكاتها[24]، ما يؤدي إلى تجزئة الإنترنت إلى أجزاء مختلفة تخضع لقوانين وسياسات مختلفة، تعيق حرية التّعبير والتعاون العالمي، ويحرم العديد من الوصول إلى المعلومات والانترنت.

– **السيادة السّيبرانيّة وحقوق الإنسان الرقميّة:** يعكس هذا التناقض بين مبدأ وحق حرية التعبير على الإنترنت والسّيادة[25]، حيث يشهد الانترنت تفاوتًا كبيرًا في التعامل بين الدول الديمقراطيّة والأنظمة القمعيّة، فالدول ذات الأنظمة القمعيّة تستخدم تقنيات التّجسس الرّقمي لمراقبة نشاطات المواطنين عبر الإنترنت، بما في ذلك المراقبة على وسائل التواصل الاجتماعي والمنتديات، وتتدخل باسم السيادة السّيبرانيّة لسن القوانين وفرضها على الإنترنت، لمراقبة المحتوى وتقييد حريّة التعبير وحجب المواقع، ومعاقبة الأفراد الذين يعبرون عن آرائهم بحرية، وتعتقل النشطاء والصحفيين بسبب منشوراتهم على الإنترنت. وأبرز الأمثلة البارزة جدار الحماية العظيم في الصين –

[24] Hao Yeli, A Three-Perspective Theory of Cyber Sovereignty, PRISM Volume 7, No 2,P.3.-
[25] Hao Yeli, ibid, P.3.-

Great Firewall of China–لتنظيم الوصول الى الشبكة المحلية ومراقبة المحتوى، وتبرر الصين هذه التدخلات بحماية الأمن الوطني ومنع الجرائم السّيبرانيّة وتنظيم البيانات [26].

– **السيادة السّيبرانيّة وأصحاب المصالح:** إنّ السيادة السّيبرانيّة تثير جدلًا حول نمط إدارة الإنترنت[27]، الحكومات ترى أنّ لها الحقّ السيادي في تنظيم الفضاء السيبراني لحماية الأمن الوطني والمصالح الاقتصاديّة، وأصحاب المصلحة المتعددين من مختلف الجهات الفاعلة كالقطاع الخاص، والمنظمات الدّوليّة، والمؤسسات الدولية المصنّعة للتقنيّة السيبرانيّة مثل(IEEE)، والمؤسسات التي تضع الممارسات والمعايير(Cobit 5,NIST, ISO) تطمح الى توزيع السلطة وكيفيّة إدارة الفضاء السيبراني، والمشاركة في اتخاذ القرارات الجماعيّة لتعزيز الشفافيّة، والمساءلة ومراعاة المصالح العالمية والمحلية على حد سواء.

تعتبر هذه التناقضات إحدى التحديات التي تعكس تنافس الولايات المتحدة، والصين وروسيا الأيديولوجي والاستراتيجي حول كيفيّة إدارة الفضاء السيبراني والهيمنة عليه. روسيا والصين تؤيدان "السيادة السّيبرانيّة" من وجهة نظر السيطرة الكاملة على البنية التحتية الرقمية، ومحتوى الإنترنت داخل حدودهما الوطنية وخارجها. وترى بأن حوكمة الإنترنت خارج سيطرتها ورقابتها سيكون أداة للسيطرة على سيادة بياناتها ويهدد استقرارها الداخلي وأمنها القومي، ويُستخدم كوسيلة للتدخل الخارجي في شؤونهما الدّاخليّة من خلال القوة السّيبرانيّة كالدعاية السياسيّة، التّجسس السيبراني، أو دعم الحركات المعارضة. بيدا أنّ الولايات المتحدة وحلفائها تدافع عن نموذج الإنترنت المفتوح، وتشجّع التدفق الحر للمعلومات وتقنيات البيانات الضخمة، والتعلم الآلي من دون قيود من الحكومات، وذلك وفقاً للقيم الليبرالية التي تدعم حرية التعبير والأسواق الحرة.

الخاتمة: ناقشت هذه الدراسة القوة السّيبرانيّة كأداة جديدة للتأثير، والسيطرة في الفضاء السيبراني والعلاقات الدّوليّة، وتناولت فيها، مفهوم القوة السّيبرانيّة والتحولات التي طرأت عليها، بالإضافة الى فهم عناصرها وأنماطها، وآثارها على العلاقات الدّوليّة وسيادة الدول، والاقتصاد والأسواق المالية. وأجابت على إشكاليّة، كيف تُعرَّف القوة السّيبرانيّة في سياق التحولات التكنولوجية الراهنة؟ وكيف أصبحت القوة السّيبرانيّة أداة مركزية للتأثير والسيطرة. أثبتت الدراسة إنّ القوّة السّيبرانيّة مفهومٌ ناشئ يؤدي دورًا مؤثرا في العلاقات الدّوليّة وتشكيلاتها، وأصبحت قوّة جانبية تؤثر على مفهوم القوّة التقليدية والسيادة السّيبرانيّة والوسائل القتالية. وساهمت العمليات السّيبرانيّة في تعظيم القوّة السّيبرانيّة، وأضافت عليها مكونات جديدة قوّة ناعمة وصلبة تتضمن الأنشطّة السّيبرانيّة، والهجمات السّيبرانيّة وقدرات أخرى. ومن خلال القدرات السّيبرانيّة يمكن للدول التأثير على الامن القومي، الاقتصاد وحتى السياسة الداخلية للدول الأخرى ما جعلها أداة رئيسة في السياسة الدّوليّة تخلق تحديات، وفرص جديدة في النظام الدولي.

الاستنتاجات:

- القوة السّيبرانيّة تسهم في تحدي المفهوم التقليدي للسيادة الوطنية وأدّت الى إعادة تشكيل مفهوم السيادة الرّقميّة.
- تستخدم الدول القوة السّيبرانيّة لتعزيز تأثيرها في العلاقات الدّوليّة من خلال أدوات مثل العمليات السّيبرانيّة، التجسس الرقمي، ونشر المعلومات المضللة لتحقيق أهداف سياسيّة واقتصاديّة.

---

[26] Baidu and CloudFlare Boost Users Over China's Great Firewall, available on internet - https://www.benton.org/headlines/baidu-and-cloudflare-boost-users-over-chinas-great-firewall, visited 13-7-2024.

[27] Hao Yeli, Ibid.,. P.3.

- ساهمت القوة السّيبرانيّة في تصاعد العمليات، والحروب السّيبرانيّة كبديل للنزاعات التقليديّة، وأصبحت أداة جذابة لدى بعض الدول، نظرًا لتكلفتها المنخفضة مقارنة بالحروب التّقليديّة.
- تصاعد أهمية القوة السّيبرانيّة دفع الدول إلى تطوير دبلوماسيّة سيبرانية نشطة للتفاوض، بناء التحالفات، وتخفيف التصعيد السيبراني.
- الفضاء السيبراني والقوة السّيبرانيّة فتح المجال أمام كيانات لادولاتية كلاعبة مؤثرة تعقّد المشهد الدولي مثل الشركات الكبرى والقراصنة.
- أثبتت القوة السّيبرانيّة أنها تؤثر على الاقتصاد العالمي من خلال استهداف البنى التحتية الاقتصاديّة للدول والمؤسسات المالية يؤدي إلى خسائر اقتصادية ضخمة بين الدّول والشّركات الكبرى.

المراجع:

نقولا، ل .(2021) .العلاقات الدّوليّة .. من تأثير القوة إلى قوة التأثير .الأرز، لبنان.

زيتون، م .(2022) .نحو إستراتيجية فعّالة للأمن السيبراني في لبنان (رسالة ماجستير غير منشورة). الجامعة اللبنانية، كلية فؤاد شهاب.

متاح على موقع .(n.d.) .أنماط "الحرب السيبرانيّة" وتداعياتها على الأمن العالمي سياسة: https://www.siyassa.org.eg/News/12072.aspx.

Carr, M. (2016). US power and the internet in international relations: The irony of the information age (pp. 15-30). Palgrave Macmillan.

Clarke, R. A., & Knake, R. K. (2010). Cyber war: The next threat to national security and what to do about it. Ecco.

Cyber power - An emerging factor in national and international security. (2016). Retrieved from https://www.cirsd.org/en/horizons/horizons-autumn-2016--issue-no-8/cyber-power-an-emerging-factor-in-national-and-international-security

Rattray, G. J. (2016). An environmental approach to understanding cyber power. In Kramer (Ed.), Cyber power: An emerging factor in national and international security (pp. 253-274).

Yeli, H. (2017). A three-perspective theory of cyber sovereignty. PRISM, 7(2), 3.

Healey, J. (Ed.). (2013). A fierce domain: Conflict in cyberspace, 1986 to 2012 (p. 153). Cyber Conflict Studies Association.

Nagel, J. (1975). The descriptive analysis of power (p. 14). Yale University Press.

Nye, J. S., Jr. (2011). The future of power in the 21st century (p. 121). Public Affairs Press.

Nye, J. S. (2010). Cyber power (p. 4).

Kalathil, S., & Boas, T. C. (2003). The impact of the internet on authoritarian rule (p. 135). Carnegie Endowment for International Peace.

Nye, J. S. (2016). Deterrence and dissuasion in cyberspace. International Security, 41(3), 44-71.

Baidu and CloudFlare boost users over China's Great Firewall. (n.d.). Retrieved from https://www.benton.org/headlines/baidu-and-cloudflare-boost-users-over-chinas-great-firewall

Cybercrime to cost the world $9.5 trillion USD annually in 2024. (n.d.). Retrieved from https://www.esentire.com/web-native-pages/cybercrime-to-cost-the-world-9-5-trillion-usd-annually-in-2024

Economic impact of cybercrime. (2018). Retrieved from https://www.helpnetsecurity.com/2018/02/23/economic-impact-of-cybercrime/

Hacking the Democratic National Committee. (2019). Retrieved from https://time.com/5565991/russia-influence-2016-election/

The perfect weapon: How Russian cyberpower invaded the U.S. (2016). Retrieved from https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.

"Cyber power is a tool for influence and control in cyberspace and international relations"

Researcher:

Mohammad Zeitoun

Abstract:

This study addresses the concept of cyber power as a modern tool for influence and control in cyberspace and international relations. It explores the understanding of cyber power, its components, and sources, as well as how it is employed in international relations. The study also discusses the tools of cyber power, both hard and soft, represented by cyber capabilities and operations, and their use by states or non-state actors in cyberspace to achieve political, economic, and military objectives, creating a strategic impact on international relations. This has introduced new challenges to traditional sovereignty, as the integration of cyberspace with the physical boundaries of states necessitates rethinking traditional concepts of sovereignty, deterrence, and warfare.

Keywords: Cyberspace; Control; Influence; power; International relations.