مجلة البحوث المالية والتجارية
المجلد (٢٤) – العدد الأول – يناير ٢٠٢٣

"الجيوسيبرانية العالمية والتحولات في أبعاد وخصائص القوة"

"آليات التوظيف في الاستراتيجية الروسية والصينية"

"Global Geo- Cyber space and shifts in the dimensions and characteristics of power, the mechanisms of the application in the Russian and Chinese strategy"

د. ايهاب محمد أبو المجد محمود عياد.

مدرس العلوم السياسية

تاريخ الإرسال	2023-01-4
تاريخ القبول	2023-1-21
رابط المجلة:	https://jsst.journals.ekb.eg/

الملخص

تهدف الدراسة إلى الإجابة على الإشكالية الرئيسية والتى مفادها: إلي أي مدي كان للبيئة الرقمية البديلة للتفاعلات الدولية "الجيوسيبرانية" أثرها على التحول في القوة الروسية والصينية؟، وإلى أى مدى كان للوجود الروسي والصيني في الفضاء الجيوبولوتيكي أثره على آليات التوظيف في الاستراتيجية الروسية والصينية؟. من خلال ثلاثة محاور جاء الأول بعنوان: أبعاد العلاقة بين الجيوسيبرانية والتحولات في خصائص وأبعاد القوة في ظل بيئة عالمية متغيرة؛ ليؤكد فرضية، أن القوة تتغير بتغير التكنولوجيا وتطورها، مما يؤثر على الفضاء الجيوبوليتيكي للدولة، وجاء المحور الثانى بعنوان: الجيوسيبرانية وآليات التوظيف في الاستراتيجية الروسية؛ ليؤكد أن السيبرانية الهجومية تلعب دوراً هاماً وكبيراً في عقيدة الجيش الروسي التقليدي، ثم تناول المحور الثالث الجيوسيبرانية وآليات التوظيف في الاستراتيجية الصينية، ليؤكد أن هناك اختلاف في توظيف القوة السيبرانية الصينية عن توظيف القوة الروسية، وتمثلت التوصيات من الناحية القيمية فى: العمل على تفعيل الدور القانوني على المستوي الدولي، ومن الناحية البنيوي: العمل على رسم هيكل للأمن السيبراني يتمتع بنوع من المرونة.

الكلمات المفتاحية: الجيوسيبرانية الروسية – الجيوسيبرانية الصينية – الفضاء الإلكتروني – التهديدات السيبرانية – الهجوم السيبراني.

Abstract

The study aims to answer the main problematic issue, to what extent did the substituted digital environment for international interactions (Geo-Cyber) have an impact on the shift in Russian and Chinese power? In addition, to what extent did the Russian and Chinese presence in the geopolitical space have an impact on the mechanisms of application in the Russian and Chinese strategy?. Through three axes, the first came under the title: Dimensions of the relationship between Geo-Cyber and shifts in the characteristics and dimensions of power in a changing global environment, to confirm the hypothesis, that power changes with the change and development of technology, which affects the geopolitical space of the state, and the second axis came under the title: Geo-Cyber and application mechanisms in the Russian strategy to confirm that offensive cyber plays an essential and major role in the doctrine of the traditional Russian army. Then, the third axis dealt with Geo-Cyber and the application mechanisms in the Chinese strategy, to confirm that there is a difference in applicating Chinese cyber force to employing Russian power, and the recommendations from the value point of view came up with: working to activate the legal role at the international level, and from a structural point of view: work on drawing up a structure for cybersecurity that enjoys a kind of flexibility.

Keywords: Russian Geo-Cyber – Chinese Geo-Cyber – Cyber – Cyber Threats – Cyber Attack.

أولاً: مقدمة الدراسة:

ظلت الصراعات التقليدية، والقوة العسكرية تحددان لفترة طويلة طبيعة الصراعات على المستوى الدولي، فلم تكن القوة العسكرية هي القوة الحاكمة؛ بل كانت أبرز مظاهر القوة خلال تلك الفترة، إلا أنه إبان الحرب الباردة بدأت القوة الاقتصادية تتعاظم لتحكم العلاقات الدولية، ثم شهد مفهوم القوة مجموعة من التغيرات التي سعت بدورها لمواكبة التطورات الحادثة فى مجال العلاقات الدولية، والذي أمكن معه التفرقة بين مستويين للتغير الذي طرأ على مصطلح القوة، المستوي الأول: وهو معني بتلك الفواعل التي تمتلك القوة وعلى وجه الخصوص مع امتلاك فاعليين غير الدول بعض المصادر الخاصة بالقوة والتأثير. والمستوي الثاني: معني بالعناصر التي تتكون منها القوة، والأشكال المتعددة التي تمتلكها القوة (لبني مهدي، ٢٠٢٠، ص ١٤٥)، (Daniel Kuehl, 2009). والتي تمثلت في العامل العلمي، والتكنولوجي وثورة المعلومات والاتصالات، ولقد أدي اتساع تأثيرات هذه العوامل في السياسات الدولية خلال الفترة الماضية إلى زيادة القدرة التصارعية بين القوى المتضاربة في مضامير العلاقات السياسية الدولية؛ حيث أحدث الصراع والتنافر الاستراتيجي بين القوي الدولية نوع جديد من الصراع والتصاعد الاستراتيجي أدي إلى ظهور جيل جديد من أدوات القوة والصراع والاشتباك أحدثت نوع جديد من التحديات التي تواجه الهياكل الأساسية الحيوية للدول (علي فتحي، ٢٠١٩، ص٣).

كما كان للثورة المعلوماتية والاتصالات انعكاساتهما على تجميع المصالح التي تتميز بالقومية للدول، بالبنية الحيوية التحتية لها، ومع التحول الحادث في "الفضاء السيبراني" والذي جعله ساحة للعديد من التفاعلات الدولية ظهرت؛ العديد من الأشكال التي توظفه في العديد من الاستخدامات التي تتميز بالطابع المدني أو العسكري؛ الأمر الذي جعل من الفضاء مجالاً للنزاعات المتنوعة، يمكن من خلاله قياس القوة، وبات واضحاً؛ أن من يمتلك "الآليات التوظيفية" للقوة السيبرانية" يكون قادر على تحقيق الأهداف المرجوه، ويؤثر فى آداء الفواعل المُستخدمه لهذه القوة، كما أربك الإنترنت الثقافات التقليدية والسياسات العامة، وساعد "الفضاء السيبرانى" على زيادة الدور النسبى للقوة فى أبعادها العسكرية والاقتصادية والسياسية، فواقع الثورة العلمية المعرفية المعتمدة على التقنية، وثورة المعلومات والاتصالات والطفرة الرقمية ألقي بظلاله على مفهوم القوة، كما أسس العلاقة بين الواقع الافتراضي، والواقع الحركي للنظام الدولي، ودفع العديد من الفواعل من الدول وغير الدول ممن يمتلكون القوة للتوجه نحو "الاستقطاب السيبرانى"؛ مما جعل من "القوة السيبرانية" سلاحاً ذا حدين يمكن استخدامها للمصالح القومية أو لهلاك الدول،

فطبيعة الأسلحة المتطورة للقوة السيبرانية مثل الفيروسات وغيرها، والتى تصيب الحواسيب المرتبطة بشبكات الإنترنت لها آثار تدميرية تسبب خسائر اقتصادية هائلة عند شن إحدى الفواعل الدولية هجوماً سيبرانياً على بنى تحتية حيوية لدولة ما، مما يبرز أهمية الاستراتيجيات الدفاعية والردع السيبراني للدول.

ثانياً: أهداف الدراسة:

تهدف الدراسة إلى:

١- تحليل العلاقة بين الجيوسيبرانية والتحولات في خصائص وأبعاد القوة وآليات التوظيف.
٢- دراسة وتحليل تصاعد القدرات الجيوسيبرانية الروسية وآليات التوظيف.
٣- دراسة وتحليل تصاعد القدرات الجيوسيبرانية الصينية وآليات التوظيف.

ثالثاً: أهمية الدراسة:

تتمثل أهمية الدراسة في أن بروز التكنولوجيا وهيمنتها، وسيطرتها على الساحة الدولية، وقدرتها على التحكم في قوة وسلوك الدول، قد ساعد على انتقال الصراع عبر الفضاء الإلكتروني، وحفز الدول إلى التسارع في وضع استراتيجيات تختص بآليات توظيف القوة والأمن السيبراني، ومع هذا الاتساع فى تأثير العامل العلمى والتكنولوجى؛ لم يكن من المقبول أن تصبح قوة الدولة العسكرية هى العنصر المتحكم فى مسار البيئة الدولية فقط أو حتى داخل الأنظمة السياسية ذاتها؛ بل استلزم الأمر إجراء مجموعة من التغيرات على مصطلح القوة ليتناسب مع المتغيرات في النظام العالمي الجديد كالإنترنت وانتشار المعلومة، والتى كان لظهورهما تأثير كبير على إحداث تغيرات كبيرة فى المعتقدات ذات الطابع السياسي، واتجاهات الفواعل سواء كانت دولاً أو غير ذلك، فلم تظل القوة مقتصرة فقط على الفواعل الدولاتية، وإنما نشأت فواعل لها طابع جديد تمكنت من إعطاء مصطلح القوة بعداً جديداً غير البعد المادي، يتعدي البعد المعنوي والجيوسيبراني. ومن هذا المنطلق تأتى أهمية الدراسة من منطلق بعدين: البعد الأول: الأهمية الوجودية لأي دولة فى الفضاء الجيوبوليتيكي من منطلق أن استخدام "الفضاء السيبراني" كأحد أنماط امتلاك القوة من خلال إحداث تأثير في عمل المصادر المعلوماتية، والأنظمة المعنية بالاتصالات من خلال "التهديد السيبراني"، قد يؤدي إلي إرباك عمل البنية التحتية الحيوية؛ لذا ظهرت مسارات ومحفزات الجيوسيبرانية والتي احتضنت مجمل التفاعلات الإلكترونية بين القوي الدولية الفاعله. كما يتمثل البعد الثاني في: أن "الفضاء السيبراني" هو مجال عالمي داخل بيئة المعلومات تم تشكيلة من

خلال استغلال المعلومات، وأنه قد يستخدم البعض التطور التقني الرقمي في خلق المشاكل الجيوسياسية والجيواقتصادية، كما أن "الهجمات السيبرانية" قد تساهم في تعطيل برامج نووية أو اختراق الأجهزة الأمنية للدول العظمي.

وتعود أهمية الدراسة إلى اعتبارين: (موضوعي، وشخصي):

الاعتبار الأول: الناحية الموضوعية، وتتمثل في: الأهمية العلمية، والأهمية العملية، كما يلي:

١- الأهمية العلمية تتمثل في:

تقديم زاوية جديدة في تحليل أثر التطور في مجال الاتصالات والتكنولوجيا مما أدي إلى ظهور محفزات التطور الجيوسيبراني مما أثر على التحول في خصائص وأبعاد القوة الروسية والصينية وآليات توظيفها.

٢- الأهمية العملية تتمثل فى:

التوصل إلى حلول للتحديات والتهديدات الناجمة عن التحول في خصائص القوة والثورة السيبرانية والتطور الجيوسيبراني.

الاعتبار الشخصى، ويتمثل فى:

محاولة الباحث استكمال البحث فى مجال العلاقات الدولية والاستراتيجية باعتباره جزءًا لا يتجزأ من العلوم السياسية، بما يحدثه ذلك من التراكم العلمي الإيجابي لدي الباحث .

رابعاً: تساؤلات الدراسة:

تقوم الدراسة على فرضية رئيسية مفادها: أن القوة تتغير بتغير التكنولوجيا وتطورها، مما يؤثر على الفضاء الجيوبوليتيكي للدولة، ومن هذا المنطلق تطرح الدراسة اشكالية رئيسية تتمثل في:

(إلي أي مدي كان للبيئة الرقمية البديلة للتفاعلات الدولية "الجيوسيبرانية" أثرها على التحول في القوة الروسية والصينية؟ وإلى أي مدي كان للوجود الروسي والصيني في الفضاء الجيوبولوتيكي أثره على آليات التوظيف في الاستراتيجية الروسية والصينية؟).

وفى إطار الإشكالية الرئيسية، يمكن الإجابة على التساؤلات الفرعية التالية:

١- ماهية أبعاد العلاقة بين الجيوسيبرانية والتحولات في خصائص وأبعاد القوة؟.

٢- ما هي آليات توظيف الجيوسيبرانية في الاستراتيجية الروسية؟.

٣- ما هي آليات توظيف الجيوسيبرانية في الاستراتيجية الصينية؟.

خامساً: الدراسات السابقة:

لقد كان هناك حرص من الباحث على ألا يكون موضوع الدراسة نوعاً من التكرار، غير أنه – بطبيعة الحال – هنالك استفادة في هذه الدراسة من الدراسات السابقة بما يمكن تسميته بـ "التراكم العلمي"، نتيجة للإسهامات التي قام بها عدد كبير من الباحثين الذين تصدوا لدراسة موضوعات الجيوسيبرانية أو لأحد ظواهرها، وبالتالي فإن الدراسة ما لم تكن تتم على هذا النحو إلا بعد قراءة الدراسات السابقة، والتي يمكن توضيحها فيما يلي:

- **دراسات تتعلق بـ "القوة السيبرانية"، والظواهر المرتبطة بها ويمكن إيجازها فيما يلي: دراسة "إيهاب خليفة،٢٠١٤"، دراسة "يحيى بن مفرح الزهراني"، ٢٠١٦، Michael Connell & Sarah, 2017، دراسة "خالد حنفي علي، ٢٠١٧"، دراسة "عادل عبد الصادق، ٢٠١٧"، دراسة "بسمة يونس محمد الرفادي"، ٢٠١٨، دراسة "إسماعيل زروقة،٢٠١٩"، دراسة "رغده البهي، وآخرون،٢٠٢٠"، وكان من أوجه الاستفادة من هذه الدراسات في الدراسة الحالية، أنها كشفت عن تأثير الفضاء الإلكتروني في الأشكال التقليدية للقوة، وظهور أشكال جديدة من الأسلحة الغير تقليدية، وتوصلت الدراسة إلى نتيجة مفادها أن أشكال القوة تتغير بتغير التكنولوجيا وتطورها، كما أوضحت مفهوم "الحرب السيبرانية"، والمصطلحات والمفاهيم الخاصة بها، وسلطت الضوء على إشكالية تداخل الصراعات السيبرانية والتقليدية، وتوصلت بعض الدراسات إلى أن هناك ثمة علاقة ارتباطية بين طبيعة الصراعات وأشكالها.**
- **ودراسات تتعلق بالجيوسيبرانية، ويمكن إيجازها فيما يلي: دراسة "زياد علي فتحي،٢٠١٩"، دراسة "علي زياد العلي، ٢٠١٩"، وكان من أوجه الاستفادة منهما في الدراسة الحالية، طرح مفهوماً جديداً، وشكلاً جديداً وهو القوة الإلكترونية، وتوصلت الدراسة أيضاً إلى النتيجة السابقة أن أشكال القوة تتغير بتغير التكنولوجيا وتطورها، كما تم تناول بعض المفاهيم الخاصة "بالجيوسيبرانية" وتناولت بعض الظواهر المتعلقة بالمفهوم بما يخدم الدراسة الحالية.**

سادساً: الإطار المنهجي للدراسة:

من أجل تحقيق التكامل المنهجي، والموضوعية والدقة، حتي نصل إلى النتائج المرجوه؛ استخدمت الدراسة الإطار المنهجي المتكامل، وهو ما توصي به الدراسات الحديثة، فقد اهتمت الدراسة بظاهرة (الجيوسيبرانية)، فاستخدمت أكثر من منهج؛ حيث استخدمت منهج المصلحة الوطنية ومنهج دراسة الحالة، كما أمكن الاستفادة من المنهج الوصفي الذي يهتم بدراسة الظواهر:

الطبيعية، والاجتماعية، والدراسات الوصفية والسياسية، ودراسة كيفية توضيح خصائص الظاهرة ومدي ارتباطها بالظواهر الأخري.

سابعاً: أقسام الدراسة:

ولما كانت هذه الدراسة تسعى للإجابة على إشكالية رئيسية مفادها: (إلي أي مدي كان للبيئة الرقمية البديلة للتفاعلات الدولية "الجيوسيبرانية" أثرها على التحول في القوة الروسية والصينية؟ وإلى أي مدي كان للوجود الروسي والصيني في الفضاء الجيوبولوتيكي أثره على آليات التوظيف في الاستراتيجية الروسية والصينية؟). وعلى ضوء الإشكالية الرئيسية للدراسة والمدي الزمني والمقتضيات الخاصة بها، تشتمل الدراسة بخلاف مقدمتها العامة: على ثلاثة من المحاور الرئيسية، ويلحق بها خاتمة حول نتائج الدراسة، وأهم التوصيات. وتتمثل أقسام الدراسة في: المحور الأول ويحمل عنوان: "أبعاد العلاقة بين الجيوسيبرانية وخصائص القوة في ظل بيئة عالمية متغيرة"، وتناول المحور الثاني: الجيوسيبرانية وآليات التوظيف في الاستراتيجية الروسية، ثم المحور الثالث: الجيوسيبرانية وآليات التوظيف في الاستراتيجية الصينية على نحو ما هو مبين بالدراسة.

المحور الأول: أبعاد العلاقة بين الجيوسيبرانية والتحولات في أبعاد وخصائص القوة في ظل بيئة عالمية متغيرة.

أولاً: التطور الجيوسيبراني ودلالات المفهوم:

تتبلور العقيدة الجيوسيبرانية لأي دولة في مفهوم الأنشطة الفضائية المعلوماتية لقواتها العسكرية لتوضح الإطار المهم الذي تعنيه المعلومة في إطار الدولة الاستراتيجي، ولقد تبنت وثيقة وزارة الدفاع الروسية تعريف "فضاء المعلومات" بأنه "إطار العمل المتصل بتكوين المعلومة واستخدامها ونقلها"، هذا بالإضافة إلى ما يطلق عليه عقيدة "جيراسيموف"، وتتشكل هذه العقيد من مجموعة من المعتقدات فيما يخص الأدوات الغير تقليدية، والتي يتم استخدامها في الحروب الراهنه، والتي يأتي من ضمنها العديد من الأدوات المختلفة المتمثلة في المعلومات، سواء كان ذلك عن طريق الفضاء الإلكتروني أو الإعلامي، واستغلال نقاط ضعف الخصوم، والحرص على عدم مواجهة الخصم بصورة علنية حتى ينتهي الصراع (سلام الوافي، ٢٠١٧)، وسوف يتم تناول شرح الوثيقة في المحور الثاني من الدراسة.

ومن ثم فيعرف "الفضاء الجيوسيبراني" بأنه العلاقة بين الشبكة المعلوماتية والموقع الجغرافي والديمغرافيا، واقتصاد وسياسة الدولة، والسياسه الخارجية الخاصة بها. كما يعرف "الاستقرار الجيوسيبراني" على أنه القدرة التي تتمتع بها الدول في الحصول على أعلى مكاسب من الشبكة المعلوماتية لتحقق بذلك العديد من الفوائد الاقتصادية والسياسية والديمغرافية مع عدم القيام بأي نشاط قد يسبب الدمار والمعاناة (تغريد حسن، ٢٠١٩، ص٢٤١). ولقد عنيت الجغرافيا السياسية بدراسة تنافس القوة والتأثير على الإقليم، على مستويات مختلفة من التحليل؛ حيث يلاحظ اهتمامها بديناميات أي نزاع على هذا الإقليم، والدفاع عن مصالحها داخل الحيز الجغرافي الخاص به، وعلى الوجه الآخر هناك الجغرافيا السياسية في الفضاء الإلكتروني "الجيوسيبرانية"؛ الذي يتكون بدوره من أربع طبقات، تأتي على رأسها الطبقة المادية، وهي شبكة عالمية من الكابلات ومحطة التبديل، ومركز تخزين البيانات، وهناك أيضًا طبقات منطقية وبيانات اجتماعية، وتأخذ جميع الطبقات الأربع الطابع "السياسي والجيوسياسي" (Carlos Exk, 2017, p339).

كما تقسم الجغرافيا السياسية "للفضاء الإلكتروني" إلى قسمين هما: "الجغرافيا الكلاسيكية"، و"الجغرافيا التقليدية"، وتنظر الجغرافيا الكلاسيكية سبل صياغة الجغرافيا السياسية، وهذا يوضح أن للفضاء هو الآخر جغرافيا مسؤولة عن تقرير البنية المادية لشبكة الإنترنت، فعلى سبيل المثال نجد أن ٨٠% من حركة الإنترنت في العالم تمر عبر الولايات المتحدة الأمريكية، وساهم ذلك في إعطاء الولايات المتحدة الأمريكية ميزة لمراقبة حركة الإنترنت العالمية. ويمكن القول بأن ذلك قد يشكل سلوك حكومات الدول الأخرى؛ حيث ستبدأ في التفكير في كيفية تغيير الوضع لذلك، فعلى سبيل المثال فإن العنصر الرقمي لمبادرة الحزام والطريق الصينية المقترحة في أوروبا مكنت الأوروبيون من تجنب مثل هذه المراقبة الأمريكية (Christian Agrum, 2020, p217).

وفي ضوء ما سبق– يلاحظ أن "الفضاء الإلكتروني" يتشكل بمساحة غير مرتبطة بحدود جغرافية؛ حيث أن الموقع والموضع هنا لم يكن له دور استراتيجي في معركة "الفضاء الإلكتروني" فلا يؤثر في قيام الحروب الإلكترونية أو الهجمات السيبرانية، بمعني أنها تجري فيها عمليات تبادل غير مقيدة بين مواطني جميع الدول، وبسرعة فورية تلغي أي فكرة عن البعد والمسافة بين الدول، مما يجعلها بعيدة كل البعد عن نظرية " ماكندر وماهان وسبايكمان" (Christian Agrum, op.cit, p220-221). وبعد أن فسر التطور التقني على أنه فضاء سياسي من نوع جديد "افتراضي" تتعارض فيه مصالح مختلف الفاعلين السياسيين والدول المختلفة، ومراكز القوى السياسية بعد ظهورها تقريبًا، تحول الفضاء الإلكتروني إلى ساحة المعركة الخامسة، بعد "البر والبحر والجو والفضاء" لمختلف القوى السياسية والعسكرية ومازالت كذلك على هذا النحو (ضحي

كاظم، ٢٠٢١، ص١٩٢-١٩٣، Daniel Venter, 2017, p175-177). كما أصبح الإنترنت إحدى وسائل الاتصال السياسي والدبلوماسي في العلاقات الدولية المعاصرة، ووسيلة اتصال فاقت جميع وسائط النقل المتطورة والسريعة، وبالرغم من استخداماته في الأغراض التجارية والاقتصادية بكل جوانبها، أصبح أحد أبرز وسائط العصر الحديث في الحروب أو ما تسمى "حروب الجيل الرابع" ومنها التدخل بشكل مباشر أو الاعتداء على خصوصيات الدول وتعطيل برامجها النووية أو كشف المخططات السياسية للدول، ويمكن القول بأن العالم اليوم يواجه العديد من المشاكل على الصعيد الجيو سياسي والجيو اقتصادي، سيما وأن الهجمات السيبرانية انتشرت بشكل كبير في الآونة الأخيرة مما يستدعي الحد منها، وحماية شبكات المعلومات عن طريق "الأمن السيبراني" (Myriam Kimner, Jean-paul Bente, 2012, p21-23).

ثانياً: أثر السيبرانية على تطور القوة في العلاقات الدولية:

١- إشكالية العلاقة التأثيرية للسيبرانية بمفهوم القوة:

تمثل قوة الدولة أحد مقوماتها لكي تحقق المصالح التي تسعى إليها؛ بل تعد أيضاً وسيلتها وآداتها التي عن طريقها تستطيع الدولة أن تحتل المكانة والهيبة في منظومة السياسة الدولية التي تتحرك داخل إطار المنظومة الدولية. وتبدي أغلب الدول الاهتمام الكبير فيما يخص توزيع القوة بين بعضها البعض، كما تسعى بشكل كبير من خلال تطوير نفسها لتحقق المكانه المرجوه في المنظومة الدولية كأحد الفواعل الرئيسية، وتحديث قدراتها عن طريق إعداد الاستراتيجيات الاقتصادية والأمنية والسياسية لكي تضمن البقاء والاستقلال بين القوي الدولية، وذلك لأن امتلاك القوة يعد أحد المحاور التي يتم الارتكاز عليها في تحديد مسار السياسة الدولية؛ لأنها أحد أهم الآليات والأدوات التي يتم استخدامها من قبل العديد من الدول بهدف تحقيق المصالح الخاصة بها، والوصول إلى الأهداف والغايات. ومن هذا المنطلق، فإنه عندما تتحقق المصلحة القومية للدول، يتطلب ذلك امتلاك الدولة قدراً كبيراً من القوة تستطيع من خلالها أن تحقق غاياتها التي سعت إلى إدراكها وتحقيقها؛ لذلك أصبحت الثنائية المعروفة بالقوة والمصلحة، الوسيلة والهدف، ومن ثم لا يمكن أن تحقق مصلحة بدون قوة، ولا يمكن أن يتم تحقيق القوة للدولة دون أن تمتلك الموارد التي تأتي بهذه القوة؛ حيث ترتبط قوة الدولة بمواردها من خلال روابط شديدة، فمن المصلحة لأي دولة أن تزيد من قدرتها على حماية كياناتها وتحافظ على وحدتها وأمنها وسلامة أراضيها، وأن تحقق الأهداف التي تسعي إليها، ولن يتحقق هذا إلا عندما تمتلك الدولة القوة التي

تمثل آداتها المثالية في تحقيق هذه الأهداف، والمصالح، والغايات (عبد الله عطوي، ٢٠٠١، ص١٤٣).

ولقد تعددت المفاهيم المعنية بالقوة في العلاقات السياسية الدولية من حيث شكلها وقدرتها ومدي تأثيرها والكيفية التي يتم من خلالها الاستعمال والممارسة، ويرجع السبب في ذلك كون كل صراع يمثل القوة التي يحاول الإنسان من خلالها أن يخضع الطبيعة من حوله عن طريق استخدام القوة، أما على مستوي العلوم السياسية فهناك ثلاث اتجاهات لدراسة مفهوم القوة وتفسيراتها والتي قد ركزت على مفاهيم أخرى بخلاف القوة والتي يتم توضيحها على النحو التالي (لايدر جوليان، ١٩٨١، ص٩١-٩٣):

- الاتجاه الأول: عرف القوة بأنها القدرة في التأثير على الآخرين أي بمعنى المقدرة على جعل الغير يتصرف بطريقة تزيد من مصالح صاحب القوة.
- الاتجاه الثاني: عرف القوة بأنها مشاركة الأطراف الفاعله في عملية صنع القرارات الهامة التي تمس المجتمع.
- الاتجاه الثالث: عرف القوة بأنها محاولة للجمع بين الاتجاهين السابقين؛ حيث عرف القوة على أنها السيطرة، والتحكم بصورة مباشرة أو غير مباشرة لشخص محدد أو مجموعة محدده في القضايا السياسية، أو هي العملية التي يتم من خلالها توزيع المهام وما يترتب عليه من مقدرة في التقرير أو التأثير في المواقف ناحية الاتجاه الذي يرغبه الذي يمتلك القوة.

والمتمعن في ممارسة القوة في العلاقات الدولية، يلاحظ أنها تطورت بشكل كبير، إبان ظهور "القوة السيبرانية"، ويرجع السبب في ذلك للتطور الذي أصاب المعلومات والاتصالات؛ إذ أصبحت المعلومات والاتصالات هدفاً لطالما سعت الدول للحصول عليها، كون القوة هي المحدد الرئيس للأداء الاستراتيجي للدولة، وترسم أبعاد دورها في الوقت الحالى والمستقبلي.

ويعد "وليام جيبسون **William Gibson**" أول من أستخدم كلمة "**cyber**" مقترنة بكلمة "**space**" ليظهر مصطلح "الفضاء السيبراني **cyber space**" في كتابة الكلاسيكي عام ١٩٨٤. وقد جاء استخدام "الفضاء السيبراني" كنموذج لاستخدام القوة من خلال تأثيرها على آداء المصادر المعلوماتية والأنظمة الخاصة بالاتصالات من خلال "الهجوم السيبراني" بما يؤدي ذلك إلى إرباك عمل البنية التحتية الحيوية (عادل عبد الصادق، ٢٠٠٩، ص٣٧-٣٨).

ولقد اشتق مفهوم "السيبرانية **Cybernetic**" من مصطلح إغريقي "**kyber netes**" ويعني الحاكم أو قائد الدفة أو الطيار، ويفيدنا هذا الاشتقاق في التوضيح أن كلمة "سيبرانية" تحتوي على

آليات التعقيب التي تتيح وظائف القيادة والتحكم في ظل أنظمة مغلقة. ومصطلح سيبرانية مشتق من كلمة "سيبر" وهي صفة لأي شيء مرتبط بثقافة الحاسوب أو التقنية المعلوماتية أو الواقع الافتراضي. كما أن جذور الكلمة الإنجليزية "cyber" متأصل في العديد من العبارات الشائع استخدامها في مجال التكنولوجيا المعلوماتية ومجال الاتصالات مثل: "الفضاء السيبراني cyber space" و"الخيال العلمي السيبراني cyber punk" (بيتر سيل، ٢٠١٧، ص٢٠-٢١)؛ حيث تعرف "السيبرانية" وفقاً لمصطلحات "الأمن المعلوماتي" بأنها هجوم من خلال "الفضاء الإلكتروني" يهدف إلى السيطرة على مواقع إلكترونية أو بنى محمية إلكترونياً بهدف تعطيلها أو تدميرها أو الإضرار بها (أحمد الفتلاوي، ٢٠١٦، ص٦١٢-٦١٣). كما يشير قاموس "المورد" إلى "السيبرانية" بأنها علم الضبط، ومصدرها "cybernetics" وهو مصدر يتطابق مع المفهوم السابق، والذي يعني "الهجمات السيبرانية"، أي ضبط الأشياء عن بعد والسيطرة عليها (منير البعلبكي، ٢٠٠٤، ص٢٤٣-٢٤٤). فيما عرف قاموس المصطلحات العسكرية الأمريكية "السيبرانية" بأنها أي فعل يستخدم عن طريق شبكات إلكترونية بهدف السيطرة أو التعطيل لبرامج إلكترونية أخري (أحمد الفتلاوي، مرجع سابق، ص٦١٤).

وهناك العديد من التعريفات "للفضاء السيبراني"، فنجد أن الاتحاد الدولي للاتصالات ووكالة الأمم المتحدة التي تخصصت في مجال التكنولوجيا والمعلومات والاتصالات تعرفه بأنه "حيز مادي وغير مادي ينشأ أو يتكون من أحد العناصر أو جميعها والتي تتمثل في: الحواسيب والشبكات، والأجهزة الممكنة، والمعلومات المحوسبة، والبرامج والمضامين والمعطيات للمرور، والرقابة وجميع المستخدمون لكل ذلك، والفضاء السيبراني هو مجال عالمي داخل بيئة المعلومات تم تشكيله من خلال استخدام الإلكترونيات واستغلال المعلومات عبر الشبكات المترابطة والمرتبطة باستخدام تكنولوجيا المعلومات والاتصالات. ويمكن تعريفه على أنه امتداد للوسائط الرقمية عبر خطوط نقل مختلفة معدنية وألياف بصرية ولاسلكية وقنواتها على شبكات الإنترنت؛ إذ يعد "الفضاء السيبراني" التعبير التكنولوجي الفائق السرعة للمعلومات، كما تعرفه الوكالة الفرنسية للأمن وأنظمة الإعلام "ANSSI" وهي الوكالة الحكومية المكلفة بالدفاع السيبراني الفرنسي بأنه "فضاء التواصل المشكل عن طريق الربط العالمي لمعدات المعالجة الآلية للمعطيات الرقمية" (Daniel Kuehl, op.cit).

وبعد استعراض ما سبق – وبعد أن أصبح "الفضاء السيبراني" ميداناً للحروب الحديثة فإن تركيبة الفواعل فيه قد اختلفت عما كانت عليه من قبل، فيلاحظ أنها قد تأخذ أحد الشكلين التاليين أو الاثنين معاً، فقد تأخذ الفواعل الدولية شكل الدولة؛ حيث تعتبر في هذه الحالة أحد الفواعل

المحورية التي تُسَير "الفضاء السيبراني" انطلاقاً من الإمكانيات المادية والبشرية والبنيوية والقانونية التي تمتلكها. وعلى الوجه الآخر قد تأخذ شكل الفواعل من غير الدول، وهنا يأتي دور الأفراد والمجموعات والمؤسسات الغير حكومية والشركات اللذين يمكنهم التحكم في التوجهات الخاصة بالدول وفق سياسات معينة (Deibert Palfrey and other, 2011).

وهنا يمكن القول بأن عملية التأثير والتأثر تنتقل من وإلى "الفضاء السيبراني" من خلال المسارات الخاصة بالقوة أو الاتجاهات التي تسيطر على النظام الدولي العام فيلاحظ أن هذه المسارات قد تأخذ الأشكال التالية (Deibert Palfrey and other, op.cit):

أ- المسار الأول: يتعلق بعملية الانتقال للأحداث من أرض الواقع إلى "الفضاء السيبراني".

ب- المسار الثاني: يتعلق بالانتقال وبتحديد "الفضاء السيبراني" لمصادر التهديدات إلى أرض الواقع من خلال الاستجابة.

ج- المسار الثالث: يتعلق بالدور الذي يقوم به "الفضاء السيبراني" كأحد الوسائل التي يتم الإعلام من خلالها وتستخدم على اعتبارها نشاط موازٍ للحوادث على الأرض.

د- المسار الرابع: فيتعلق بما يتم نشره عبر "الفضاء السيبراني" مثل: إطلاق الفيروسات أو القرصنة أو سرقة المعلومات كما سيتم توضيحه من خلال المحور الثاني.

وخلاصة القول فإن "الفضاء السيبراني" اقترن بمفاهيم مختلفة منها انعدام الجغرافية وظهور "جغرافيا الإبحار المعلوماتي" في اتجاهات شتى، وهذا ما جعل من ظاهرة "الفضاء السيبراني" أهم خصائص عصر المعلومات والاتصالات وبدون منازع؛ حيث تجمع التكنولوجيا الخاصة بالمعلومات والاتصال بين التكنولوجيا المعلوماتية، والتي تمثل مجموعة من وسائل مستخدمة لإنتاج واستغلال وتوزيع المعلومات بكافة اشكالها. وهي التي تمثل البنية التحتية التي من خلالها تتم عملية التواصل الاجتماعي وتأمين الانتقال الآمن للرسائل من المرسل إلى المتلقي.

٢- القوة السيبرانية:

لقد انتجت الثورة المعلوماتية شكلاً جديداً من أشكال القوة أطلق عليها "القوة السيبرانية"، ويرجع السبب في ذلك للتقدم التكنولوجي السريع الذي حدث في أجهزة الكومبيوتر والاتصالات والبرمجيات بحلول القرن الحادي والعشرين. ويعرف مصطلح "القوة السيبرانية cyber power" على أنها "القدرة على استخدام "الفضاء السيبراني" للحصول على العديد من المزايا والتأثير في الأحداث على مستوي جميع البيئات من خلال أدوات القوة". ولقد قام "جوزيف ناي" بتحديد مفهوم "القوة السيبرانية" بهدف فهم العمل الذي تقوم به شبكة المعلومات في تكوين القدرة الخاصة

بالأطراف الدولية، والتي يعد من أهم أشكالها الدول الناشئة والأطراف الدولية لتحقيق أهدافها. ويمكن تعريف "القوة السيبرانية" على أنها مجموعة الموارد التي تتعلق بالتحكم والاتصال بالمعلومات الإلكترونية والمعلومات المستندة إلى الكومبيوتر والبنية التحتية والشبكات والبرمجيات والمهارات البشرية، أو هي امكانية الحصول على النتائج المطلوبه عن طريق الاستخدام الأمثل للموارد المعلوماتية التي تتمتع بالترابط الإلكتروني في "الفضاء السيبراني" للتعرف على مزايا الدولة وقدرتها في التأثير على المجريات المتعلقة بالبيئة التشغيلية للدول الأخري، وذلك عبر الأدوات الإلكترونية. وانها مجموعة موارد تتعلق بالتحكم والسيطرة على الأجهزة الحاسوبية والمعلوماتية والبنية التحتية المعلوماتية والشبكات الإلكترونية والمهارات البشرية المدربة للتعامل مع هذه الأدوات (Joseph Nye, 2010, p3-10).

ويمثل الجدول (١) الأبعاد المادية والافتراضية للقوة السيبرانية على النحو التالي(Joseph Nye, 2010, p5-6):

	الفضاء السيبراني الداخلي	الفضاء السيبراني الخارجي
أدوات المعلومات	القوة *الصلبة*: هجمات رفض الخدمة وإدخال البرامج الضاره. القوة الناعمة: وضع القواعد والمعايير.	القوة الصلبة: إحداث هجوم على أنظمة SCADA. القوة الناعمة: القيام بحملة دبلوماسية عامة للتأثير على الرأي العام بالأدوات المادية.
الأدوات المادية	القوة الصلبة: الضوابط الحكومية على الشركات. القوة الناعمة: بنية تحتية لمساعدة رواد التواصل الاجتماعي.	القوة الصلبة: موجهات قطع الخدمة والكابلات. القوة الناعمة: كشف أفعال مقدمي خدمات الإنترنت.

وفي ضوء الجدول (١) يلاحظ أنه يمكن استخدام أدوات المعلومات لإنتاج القوة الناعمة في "الفضاء السيبراني" من خلال الجذب أو الإقناع. فعلى سبيل المثال، فإن جذب مجتمع البرمجيات مفتوحة المصدر من المبرمجين للالتزام بمعيار جديد هو مثال على القوة الناعمة المستهدفة داخل الفضاء الإلكتروني. كما يمكن أن تنتج الموارد السيبرانية أيضًا قوة صلبة داخل الفضاء السيبراني.

على سبيل المثال، يمكن للدول أو الجهات الفاعلة غير الحكومية تنظيم هجوم رفض الخدمة الموزع باستخدام "شبكات الروبوت" لمئات الآلاف أو العديد من أجهزة الكمبيوتر الخاصة بشركة أو دولة وتمنعها من العمل وهذا ما سيتم الكشف عنه في المحور الثاني من الدراسة (Martin Libicki, (2009، (william Owens and Other, 2009).

كما يمكن أيضاً أن تنتقل المعلومات السيبرانية أيضاً عبر "الفضاء الإلكتروني" لخلق قوة ناعمة من خلال جذب المواطنين في بلد آخر. ومن الأمثلة على ذلك حملة الدبلوماسية العامة عبر الإنترنت. وعلى الوجه الآخر يمكن للمعلومات السيبرانية أن تصبح أيضاً مصدراً للقوة الصلبة بحيث تلحق الضرر بالأهداف المادية في بلد آخر. ومن أمثلة ذلك، ما تمتلكه العديد من الصناعات والمرافق الحديثة من عمليات يتم التحكم فيها بواسطة أجهزة كمبيوتر مرتبطة بأنظمة "SCADA" للتحكم الإشرافي والحصول على البيانات، ويمكن توجيه البرامج الضارة التي يتم إدخالها في هذه الأنظمة لإغلاق عملية قد يكون لها تأثيرات جيوسيبرانية. فمثلاً إذا قام أحد الفواعل من الأفراد أو الحكومات بإغلاق مصدر توفير الكهرباء في مكان ما، فقد يكون الدمار الذي يلحق به أكثر تكلفة مما لو تم استخدام أسلحة في ذلك (Ronald Deibert and Other, 2010, p25-27).

وخلاصة القول في شأن "القوة السيبرانية" أن مفهوم القوة لا يزال يمثل أحد المرتكزات الأساسية في تفسير وتحليل الظواهر السياسية بدءاً من مفهومها العسكري مروراً بمفهومها الاقتصادي وصولاً لمفهومها السيبراني، مهما كان نوع القوة وطبيعتها وترتيبها حسب الأدوار القائمة التي تضطلع بها وتوزيعها بين القوى، ولا تكمن "القوة السيبرانية" في وجود عناصرها فحسب وإنما في عملية استثمارها، وتوظيفها توظيفاً فعلياً، وعلى وجه الخصوص في الجانب السياسي، ووفقاً للمفهوم الجديد لم تعد القوة عادية وفقاً للطريقة التقليدية التي تحدثت عنها المدرسة الواقعية، فمما لا شك فيه أن الطبيعة القائمة عليها العلاقات الدولية هي التي تحدد في المقام الأول الكيفية التي تستخدم بها الدولة قوتها للدفاع عن أهدافها ومصالحها، أي: أن هناك علاقة تناسب بين القوة المستخدمة، وطبيعة العلاقات الدولية المتبادلة، وقد اتسع مفهوم القوة؛ ليتضمن عناصر أخرى غير القنوات القتالية مثل امتلاك الدولة لعناصر مثل: الموارد الطبيعية والمساحة والموقع الجغرافي والاستقرار السياسي والتطور العسكري والنمو الاقتصادي، وأن السيبرانية مجال آخر لاستعراض القوة، وممارسة النفوذ وتحقيق التفوق والتنافس الدولي، ونستنتج مما سبق: أن القوة السيبرانية باتت واقع مساند للقوة التقليدية، ولم يقف الأمر عند هذا الحد؛ بل أصبحت داعمة لها في العديد من العمليات العسكرية والأنشطة السياسية الاقتصادية والدبلوماسية للدول، كما أصبحت أيضاً إحدى عوامل مضاعفة قوة الدول وفاعليتها. كما وفرت لها مجالا حركياً

تستطيع من خلاله تجاوز الحدود الجغرافية للوصول لأهداف قد يصعب وصولها عن طريق القوة التقليدية وهذا ما يرسخه مفهوم الجيوسيبرانية.

المحور الثاني: الجيوسيبرانية وآليات التوظيف في الاستراتيجية الروسية.

لقد تعددت استخدامات "القوة السيبرانية" في الاستراتيجية الروسية، واختلفت الآلية التي تدير بها روسيا حروبها السيبرانية، وذلك وفقاً لطبيعة الظروف الدولية المحيطة بها؛ حيث استخدمت روسيا تلك القوة من خلال العديد من الأنماط والتي سيتم تناولها من خلال هذا المحور. وبالنظر للاستراتيجية السيبرانية الروسية يلاحظ أن هدفها الرئيسى لا يكمن فقط في قدرتها على مقاومة التهديدات التي تواجهها سواء كانت متعمدة أو غير متعمدة ومدي استجابتها لمواجهة تلك المخاطر؛ بل إن عقيدتها الجيوسيبرانية تنطلق من تبنى موقفاً اندفاعياً أكثر حزماً من منطلق رغبتها في استهداف أنظمة البنية التحتية الحيوية، والسلوك والعمليات الاستخباراتية في "الفضاء السيبراني" للدول المعادية لها، وعلى وجه الخصوص الدول الغربية، وخير مثال على ذلك استهداف "الفضاء السيبراني" الأوروأطلسي؛ حيث استهدفت العقيدة الروسية مصالح دول حلف الشمال الأطلسي، والذي يمثل بوابة من بوابات الحرب للمنظومة الغربية حيال روسيا، كما ارتبط التصاعد في الصراع بين الدول الأوروأطلسية تقودها أمريكا والجانب الروسي، بالاستدعاء المتزايد للحرب المعلوماتية كأحد الركائز المهمة التي تؤثر في مسار الصراع، وفي زروة التنافس على قيادة النظام تشكل توجه استراتيجي مغاير لدي روسيا له جذورة التاريخية في فترة الصعود السوفيتية، هذا التوجه يري أن الانتصار في الصراع مع الغرب لن يتحقق بالاعتماد القاصر على الأدوات العسكرية التقليدية، ولكن الأمر يتطلب أدوات الحرب الحديثة، وغيرها من الأدوات وهو ما أطلق عليه رئيس هيئة الأركان العامة الروسية "فاليري جيراسيموف" نهجاً مختلفاً لتحقيق الأهداف السياسية والعسكرية الروسية من خلال الطرق غير المباشرة، وغير المتماثلة (على فتحي، مرجع سابق، ص٤).

أولاً: العقيدة الجيوسيبرانية في الاستراتيجية الروسية.

لقد تبلورت العقيدة "الجيوسيبرانية" الروسية من خلال الوثيقة الخاصة بوزارة الدفاع الروسية والتي تحمل عنوان "مفهوم الأنشطة الفضائية" المعلوماتية للقوات الروسية المسلحة" لتوضح الإطار المهم الذي تقوم به المعلومات في صياغة الإطار الاستراتيجي الروسي، وتبنت الوثيقة – كما سبق وأن تم توضيحه من قبل– تعريف "الفضاء المعلوماتي" على أنه هو ذلك المجال الخاص

بالأنشطة المتصلة بتكوين المعلومات واستخدامها ونقلها، بالإضافة إلى ما يطلق عليها عقيدة "جيراسيموف"، والتي تحتوي على عدد من الأفكار التي تخص الوسائل الغير تقليدية في الحروب الحالية؛ حيث تزايد اللجوء إليها في روسيا خلال الفترة السابقة، مع السعى الحثيث لروسيا كى تستعيد الإرث التقليدي كقوة مؤثرة في النظام الدولي، ما يستلزمه ذلك من توظيف أدوات الحرب السيبرانية، وفي هذا السياق، اعتمدت روسيا على عقيدة أمن المعلومات في الاتحاد الروسي، وأكدت الوثيقة على البعد العسكري لمسالة المعلومات كأساس لأمن الدولة، وتحدد أسلحة المعلومات باعتبارها إحدى الأدوات لتحقيق الأهداف السياسية، وتتمثل مفردات هذه العقيدة في (على فتحي، مرجع سابق، ص٥-٦):

١- تقويض القدرة على المواجهة: فالعديد من عمليات الحرب المعلوماتية التي تقوم بها روسيا وعلى وجه الخصوص المتعلقة بـ"القرصنة الإلكترونية" تهدف في المقام الأول إلى إضعاف امكانيات خصوم روسيا، وتقليل القدرة على المواجهة، وهو ما بدا واضحاً في الحرب الروسية الجورجية عام ٢٠٠٨م؛ حيث أن "التهديدات السيبرانية" التي قامت بها روسيا في الدولة الجورجية في نفس وقت دخول القوات الروسية أدت إلى تعطيل الاستجابة الجورجية للغزو الروسي لها؛ حيث أضعفت عمليات القرصنة التي قامت بها روسيا قنوات تواصل الحكومة مع المواطنين، وإيقاف المعاملات المالية، وعرقلة انتقال المعلومات حول ما يحدث في مناطق الحرب إلى العالم الخارجي.

٢- توظيف المعلومات ضد القوي المناهضة: ويتضح ذلك من خلال ما قامت به روسيا من توظيف المعلومات ضد القوي المناهضة لها مثلما حدث في جورجيا وأوكرانيا، بأن ما حدث كان نتاجاً للتدخلات الأمريكية، وفي الوقت ذاته تشييد صور إيجابية لحلفائها. كما استحضرت روسيا هذا النموذج أيضاً خلال الانتخابات التي حدثت في الدول الغربية خلال الفترة الأخيرة؛ حيث ساندت تكتلات على حساب تكتلات أخري وهذا ما سيتم التطرق له فيما بعد.

٢- مواجهة العقوبات الغربية: وهذا ما يمكن ملاحظته عقب التدخل الروسي في أوكرانيا عام ٢٠١٤، بعد استفتاء مارس ٢٠١٤م، وضم شبه جزيرة القرم، وتزايد العزلة الأوروبية المفروضة على روسيا، وفي عام ٢٠٢٢م أيضاً عقب تدخلها في أوكرانيا والتي تضمنت عدداً من العقوبات التجارية والاقتصادية.

ثانياً: تصاعد القدرات الجيوسيبرانية وآليات التوظيف في الاستراتيجية الروسية.

تمثل الدولة الروسية ثقل عالمي في المجال السيبراني ويرجع السبب في ذلك لتفوقها في مجال المعلومات والاتصالات؛ حيث تحتل وكالة "زيكوريون الاستشارية" للاستشارات الأمنية والتي يقع المقر الخاص بها في موسكو المرتبة الأولي في تحليل المعلومات، والخدمات الخاصة بالقرصنة كواحدة من خمس جيوش سيبرانية في العالم"؛ ولقد قامت روسيا بزيادة تمويلها لقدرات الإنترنت الدفاعية بعد العديد من سلاسل الهجمات الأمريكية، والإسرائيلية الإلكترونية على مواقع نووية إيرانية في عام ٢٠١٠م؛ بحيث تقدر حجم القوى السيبرانية الروسية، وعلى وجه الخصوص الموجهة نحو منطقة الأوروأطلسية ما بين ٢٠٠٠ إلى ١٠٠٠ عامل، كما تمثل النفقات الخاصة بوزارة الدفاع الروسية حوالي ٥٠٠ مليون دولار سنوياً على هذه الترتيبات الإلكترونية، ومن ثم يمكن القول بأن مجالات القوة والتفوق الروسي تندرج نحو التأثير الكبير للدعاية الإلكترونية الروسية فضلاً عن عمق التأثير للحرب الإلكترونية العسكرية لاعتبارات تتعلق بتفوق روسيا في منظومات التشويش والتضليل العسكري، فضلا عن القوة الردعية الروسية في خلق الفيروسات ومنع الاختراقات المضادة، كذلك الإمكانات العالية في مجال الاختراق الإلكتروني (Andy Greenberg, 2017).

ولقد استغلت روسيا في نزاعاتها الأخيرة أسلوب "الهجمات السيبرانية"، في غزوها لجورجيا في عام ٢٠٠٨، والقِرم في عام ٢٠١٤، ومنذ ذلك الوقت، أصبحت أوكرانيا "ساحة تدريبية" للعمليات السيبرانية للحرب الروسية، وفق ما أوضحته "لورين زابيريك"، العاملة في مجال أمن الحاسوب خلال الصراعات الدولية بكلية "هارفارد كينيدي" بولاية ماساتشوستس الأمريكية، كما أضافت "زابيريك" أنه في عامي ٢٠١٥، ٢٠١٦م، عطَّلت "الهجمات السيبرانية" التي نسبت لروسيا الشبكات الخاصة بالطاقة الأوكرانية لعدة ساعات (Elizabeth Gibney, 2022). ويوضح الجدول (٣،٢) أهم الهجمات السيبرانية المنسوبة لروسيا على النحو التالي (محمد جلال، وآخرون، ٢٠٢٠، ص١٩٨-٢٠٢)، (أحمد حمدي، ٢٠١٩)، (Bidemun, 2000, p39)، (Liaropoulos Andrew, 2018, p545):

١- أهم التهديدات السيبرانية خلال الفترة من ٢٠٠٧ وحتى ٢٠١٤ جدول (٢):

الفترة	الهجمات السيبرانية	الوصف	ملاحظات
٢٠٠٧	الهجوم السيبراني لأستونيا بعد الخلاف مع روسيا.	استهدف شبكات الاتصال وأنظمة البنوك والمصارف والهواتف المحمولة.	
٢٠٠٨	الهجوم السيبراني ضد جورجيا بعد الصراع على أوسيتيا الجنوبية.	استهداف خدمات الإنترنت وتوقف الاتصالات الداخلية.	تقرير مركز التعاون المشترك ضد الهجمات الإلكترونية CCDCOE
٢٠٠٩	الهجوم السيبراني على قرغيزستان لإلغاء القاعدة العسكرية الأمريكية.	استهداف اثنين من مزودي خدمة الإنترنت في قرغيزستان من قبل قراصنة روس من خلال شن هجمات DDOS.	
٢٠١٣	الهجوم السيبراني على مواقع التواصل الاجتماعي بأوكرانيا.	استهداف وسائل الاعلام والتلاعب بالمعلومات للتأثير على الرأي العام ونشر معلومات غير صحيحة مستخدمة وسائل التواصل الاجتماعي لمنع انضمام أوكرانيا للاتحاد الأوروبي.	
٢٠١٤	الهجوم السيبراني لقطع الخدمة والاختراق والتلاعب في البيانات على موقع الانتخابات الأوكرانية.	استهداف موزع الخدمة الرئيسي للمواقع الإلكترونية التابع للحكومة، وتعطيل النظام الإلكتروني لجمع نتائج الانتخابات واختراق الحواسيب المسجل عليها البيانات.	

وبعد استعراض أهم الهجمات السيبرانية المنسوبة لروسيا خلال الفترة من ٢٠٠٧ وحتى ٢٠١٤م، يلاحظ أن الدوافع من هذه الهجمات قد تكون دوافع عسكرية أو اقتصادية أو سياسية فعلى سبيل المثال يلاحظ أن الهجوم السيبراني الذي استهدف أستونيا عام ٢٠٠٧م، كانت دوافعه تحمل الطابع العسكري؛ حيث أدت هذه الهجمات إلى إحداث نوع من الشلل الكامل في كامل أجهزة الدولة، واستعانت "إستونيا" بحلف شمال الأطلنطي لمواجهتها، وأشارت أصابع الاتهام إلى الحكومة الروسية التى أنكرت صلتها بالهجوم في بادئ الأمر، لكنها أقرت بعد ذلك أنه من الجائز أن يكون قد تم الهجوم من داخل الأراضي الروسية من قبل فواعل إجرامية لم يعجبها القرار الإستوني بنقل تمثال يخلد ضحايا جنود روس في الحرب العالمية الثانية (إيهاب خليفة، ٢٠١٨، ص١٩-٢١). أيضاً الهجوم السيبراني ضد جورجيا من أجل أوسيتيا الجنوبية عام ٢٠٠٨م والذي استهدف خدمات الإنترنت وتوقف الاتصالات الداخلية، وكذلك الهجوم السيبراني على قرغيزستان في ٢٠٠٩م والذي جاء بهدف إزالة القاعد الأمريكية وهو ما دفع روسيا لمنح قرغيزستان قروضاً ومساعدات

مالية بقيمة ٢ مليار دولار. وكذلك الهجوم السيبراني على أوكرانيا ٢٠١٣-٢٠١٤ على مواقع التواصل الاجتماعي والذي جاء لمنع انضمام أوكرانيا للاتحاد الأوروبي.

٢- أهم التهديدات السيبرانية خلال الفترة من ٢٠١٥ وحتى ٢٠٢٢ جدول (٣):

لقد جاءت أغلب الهجمات السيبرانية خلال هذه الفترة تحمل الطابع السياسي والاقتصادي؛ حيث مثلت الحرب الروسية على ألمانيا في عام ٢٠١٥م الطابع السياسي والذي تمثل في التسريبات الخاصة بالبرلمان الألماني. وكذلك الهجوم السيبراني الروسي على الانتخابات الأمريكية عام ٢٠١٦م والذي استهدفت أنظمة الانتخابات الأمريكية لفوز "دونالد ترامب" في الانتخابات وذلك وفقاً لتقرير مكتب التحقيق الفيدرالي الأمريكي. أما الهجوم السيبراني الروسي على المطارات الأمريكية في عام ٢٠٢٢م جاء يحمل الطابع الاقتصادي.

السنة	الهجمات السيبرانية	الوصف	ملاحظات
٢٠١٥	الحرب السيبرانية الروسية على ألمانيا.	تسريب وثائق سرية رسمية تخص البرلمان الألماني.	
٢٠١٦	الهجوم السيبراني الروسي للانتخابات الأمريكية.	استهداف أنظمة الانتخابات الأمريكية لفوز "دونالد ترامب".	التقرير التحليلي المشترك الصادر عن مكتب التحقيق الفيدرالي الأمريكي.
٢٠١٧	الهجوم السيبراني لأقراد روس والذي عرف بـ "Zero Day".	استهداف أجهزة الأندرويد، واستغلال الثغرات الأمنية لأنظمة مايكروسوفت.	تقرير صادر عن "كاسبر سكي لاب".
٢٠١٩	الهجوم السيبراني الذي استهدف أفراد في أوروبا.	تم الاستهداف من قبل قراصنة تابعة للحكومة الروسية.	
٢٠١٩	الهجوم السيبراني على اللجنة الوطنية الديمقراطية الأمريكية.	استهداف اللجنة الوطنية الديمقراطية الأمريكية من قبل متسللين روس في الفترة التي تلت انتخابات التجديد النصفي.	تقرير اللجنة الوطنية الديمقراطية الأمريكية.
٢٠٢٢	هجمات سيبرانية تستهدف المواقع الإلكترونية لمطارات أميركية وتعطلها.	استهداف مطار دي موين الدولي في ولاية أيوا، ومطار لوس أنجلوس الدولي، ومطار شيكاغو أوهير الدولي، ومطار هارتسفيلد جاكسون أتلانتا الدولي. كما تعرض موقع "فلاي لاكس" FlyLAX الإلكتروني لتعطيل جزئي، قبل أن يستعيد نشاطه لاحقا.	نقلاً عن شبكة "إيه بي سي" ABC الأميركية بأن الهجمات من داخل روسيا.

وبعد استعراض أهم الهجمات السيبرانية الروسية يمكن القول بأن روسيا في استراتيجيتها الجيوسيبرانية تختلف اختلافاً كلياً عن نقيضتها من الدول الأخري وعلى وجه الخصوص الغربية فيما يخص العقيدة السيبرانية وسبل توجه أدوات هذه العقيدة نحو العمق التأثيري، والموجه للمصالح الروسية؛ كما أن لها رؤية "للحرب السيبرانية" مختلفة عن نظيراتها من دول "المنظومة الغربية"، فروسيا لديها أكثر الطرق الاستراتيجية لدمج منظومات الجيل الخامس، والتي تشمل "الحرب الدعائية الإلكترونية" و"منظومة الحرب الإلكترونية" بالإضافة إلى منظومة "الحرب السيبرانية، وبالتالي تمتلك من السطوة والتأثير ما يأهلها من ممارسة السطوة الإلكترونية والتأثير الإلكتروني" في العمق الاستراتيجي لأي دولة من خلال تنظيم وسائل التدخل والنفوذ في العمق، وفي داخل الحلفاء الاستراتيجيين للولايات المتحدة الأمريكية؛ إذ أمكن القول بأن التوجهات السيبرانية الروسية تختلف تماماً عن نقيضتها الغربية؛ حيث ينظر منظرو الفكر السيبراني على أن التوجه والانغماس السيبراني ينبع من العقيدة الجيوسيبرانية الروسية، والتي تتمثل في كيفية استخدام قدرات الاتصال للإنترنت وتنظيم الوسائل الإلكترونية من أجل تدعيم الجهد الحربي الإلكتروني، ومن هنا يلاحظ أن الاستراتيجية الجيوسيبرانية الروسية تبني على مجموعة من المعتقدات التي تتمثل في (David Batashvil, 2017):

١- يعتقد الروس بأن روسيا مقفلة جيواستراتيجياً لذلك فهي في صراع مع القوى الداخلية والخارجية التي تسعى إلى الاضرار بأمنها من خلال مجال المعلومات والإنترنت، والتدفق الحر للمعلومات التي يولدها، والتي تمثل على حد سواء تهديداً وفرصاً في نفس الوقت.

٢- لا يستخدم المنظرون العسكريون الروس عموما مصطلحات حروب الإنترنت أو الحرب الإلكترونية، بدلاً من ذلك، فإنهم يستخدمون مصطلح "العمليات السيبرانية" في نطاق أوسع يتمثل في إطار حروب المعلومات، وهو مفهوم شامل يشمل أمن الحواسيب وعمليات الشبكة، والحرب الإلكترونية، والعمليات النفسية، والاستخبارات الإلكترونية.

٣- أن السيبرانية الهجومية تلعب دوراً هاماً وكبيراً في عقيدة الجيش الروسي التقليدي، وربما فإنها تلعب دوراً في الرؤي المستقبلية في الاستراتيجية الروسية والتي سميت بـ "إطار الردع"، وهذا ما تم ملاحظته خلال الحرب الروسية – الأوكرانية الأخيرة في عام ٢٠٢٢م وما قامت به روسيا من استخدام التكنولوجيا المتطورة في حروبها السيبرانية مع أوكرانيا، وعلى الرغم من أن الجيش الروسي كان بطيئا في احتضان السيبرانية لأسباب هيكلية وعقائدية على حد سواء؛ إلا أن الدراسات الغربية تؤكد أن روسيا في صدد تعزيز القدرات السيبرانية الهجومية وكذلك

القدرات السيبرانية الدفاعية، من أجل تعضيد القوة التقليدية خصوصاً في الجناح الشرقي لأوروبا من أجل ممارسة النفوذ واسترجاع استراتيجية الذات الروسية المفتقدة.

المحور الثالث: الجيوسيبرانية وآليات التوظيف في الاستراتيجية الصينية.

لم تحذوا الصين حذو روسيا في آليات توظيف "القوة السيبرانية" في استراتيجيتها؛ حيث اختلفت الآلية التي تدير بها الصين "حروبها السيبرانية"، فطبيعة الظروف الدولية المحيطة بها جعلتها تقوم بتوظيف "القوة السيبرانية" بالطريقة التي تتناسب وهذه الظروف؛ حيث استخدمت الصين تلك القوة من خلال العديد من الأنماط فاستخدمت القوة الناعمة في استراتيجيتها الشاملة والتي تمثلت في "مباردة الحزام والطريق"، واستخدمت القوة الصلبة مثلما فعلت روسيا في حروبها السيبرانية، وبالنظر للاستراتيجية السيبرانية الصينية يلاحظ أن هدفها الرئيسى هي الأخري، لا يكمن في القوة الناعمة فقط؛ بل في قدرتها على مقاومة التهديدات التي تواجهها سواء كانت متعمدة أو غير متعمدة، ومدي استجابتها لمواجهة تلك المخاطر ؛ ويلاحظ أن عقيدتها الجيوسيبرانية هي الأخري في استخدام القوة الصلبة تنطلق من تبنى موقفاً اندفاعياً أكثر حزماً من منطلق رغبتها في استهداف أنظمة البنية التحتية الحيوية، والسلوك والعمليات الاستخباراتية هي الأخري في الفضاء السيبراني للدول المعادية لها، وعلى وجه الخصوص الدول الغربية، وخير مثال على ذلك استهداف الفضاء السيبراني الأمريكي والعديد من الدول الأخري. وفي ضوء ذلك يتم تناول الجيوسيبرانية وآليات التوظيف في الاستراتيجية الصينية على النحو التالي:

أولاً: العقيدة الجيوسيبرانية في الاستراتيجية الصينية.

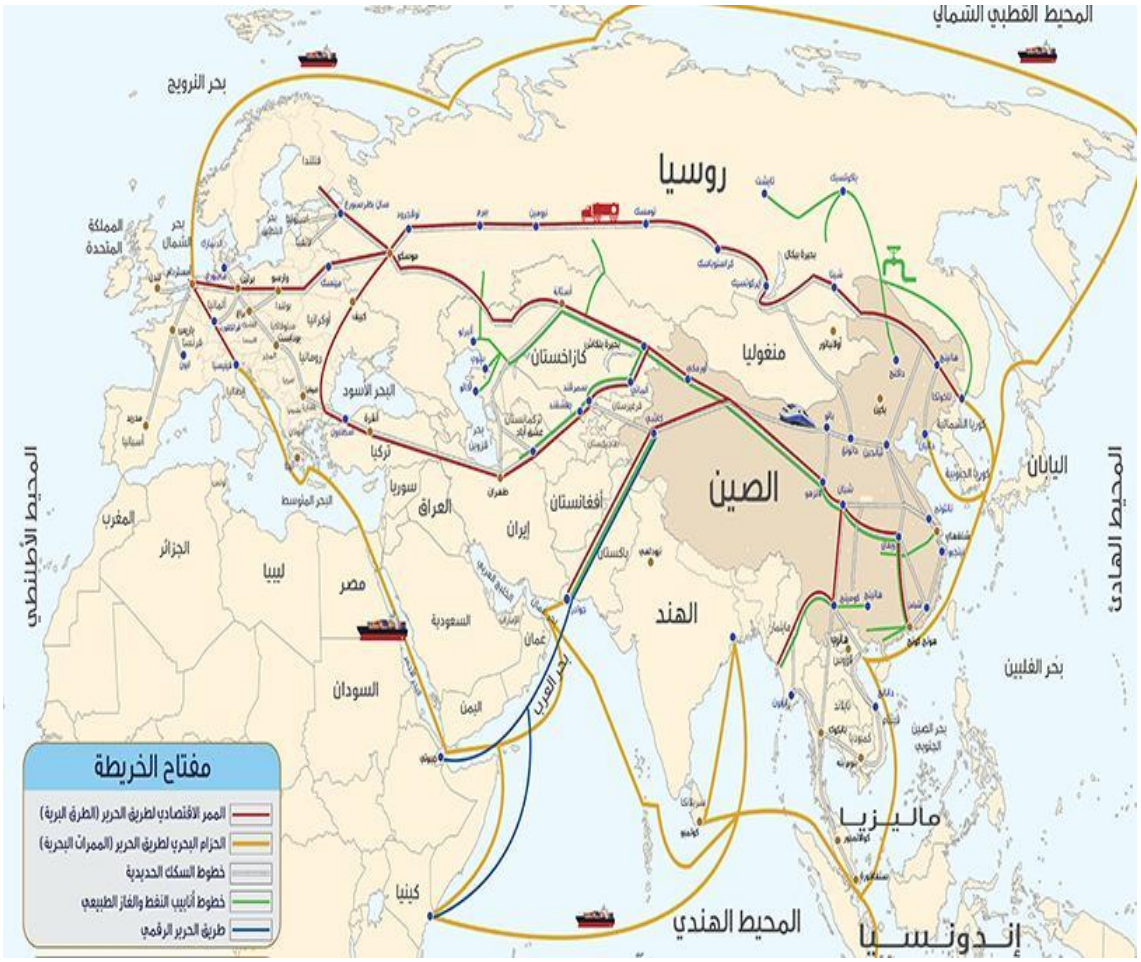
لقد عكست استراتيجية الصين الشاملة في الحزام الجيوبوليتيكي الصيني، رؤية الصين الاستراتيجية لوجودها في هذا الفضاء الجيوبوليتيكي، وذلك بهدف الترسيخ للمصالح الاستراتيجية الصينية، عن طريق ضخ الاستثمارات في بنيها التحتية؛ حيث تغلغلت الصين بمجموعة من الاتفاقيات ذات البعدالاستراتيجي مع أكثر من ٢٠ دولة في آسيا وأفريقيا وأوروبا، والتي استطاعت من خلالها تعزيز المصالح الخاصة بها بمجموعة استثمارات بمليارات الدولارات، ارتكزت على مجموعة من المشاريع الخاصة بالطرق الاستراتيجية للنقل والمواصلات، والموانئ الاستراتيجية، وخطوط السكك الحديد، والتي انصب مجمل تركيزها على التأجير والاستثمار في الموانئ البحرية المهمة. لتكون الغطاء الاقتصادي الاستثماري لانتشارها العسكري في المستقبل القريب (على العلى، ٢٠١٩).

ومن هذا المنطلق تحركت بشيئ من الحزر بهدف منع احتواء نفوذها الاستراتيجي، كما حدث مع الاتحاد السوفيتي من قبل؛ حيث تمكنت من التوجه خارجياً من خلال مجموعة من الاتفاقيات الاستراتيجية الملزمة مع مجموعة من الدول الهامة، لتأمين المصالح الحيوية التي تتركز حول ضمان تصريف المنتجات الاقتصادية الخاصة بها، وترسيخ وجودها الأمني التكتيكي، وبالتالي تأمين الاحتياجات الخاصة بها من صادراتها من الطاقة، والنفط والغاز وعلى وجه الخصوص أنها تمثل ثاني أكبر دولة في العالم تستهلك الغاز المسال بعد اليابان؛ حيث اندفعت لتعزيز الاستثمارات الخاصة بها في مجال الطاقة بالعديد من الشراكات مع الشركات التي تعمل في مجال النفط في العديد من البلدان من أسيا وأفريقيا؛ حيث استطاعت الصين توسيع مجال اندماجها الجيواستراتيجي وتأمين المصالح الداخلية والخارجية لها بمجموعة من المحالفات الأمنية والاقتصادية (على العلى، مرجع سابق).

ثانياً: تصاعد القدرات الجيوسيبرانية وآليات التوظيف في الاستراتيجية الصينية.

١- القدرات الجيوسيبرانية الصينية في استراتيجية الحزام والطريق "القوة الناعمة".

لقد أعلن الرئيس الصيني "شي جين بينغ" في عام ٢٠١٣م، خلال الزيارات التي قام بها إلى أندونيسيا وكازاخستان، عن الاستراتيجية الصينية الشاملة في الحزام الجيوبوليتيكي للصين، والتي تشمل القارة الأسيوية والأفريقية وبعض من القارة الأوروبية؛ حيث أطلق عليها "طريق الحرير الجديد" أو مبادرة "الحزام والطريق". وتنقسم هذه المبادرة إلى طريقين: "الطريق البحري" وبدايته من "فوتشو الصينية مروراً بأندونيسيا وفيتنام وبنجلاديش وسيريلانكا والهند وجزر المالديف وعلى طول الساحل الأفريقي بشرق أفريقيا، متجهاً إلى البحر الأحمر، ويمر بقناة السويس إلى البحر المتوسط متجهاً لأوروبا"، و"الطريق البري" الذي يضم ستة من الممرات الاقتصادية البرية هي: ممر الصين وباكستان الاقتصادي، وممر بنجلاديش والصين والهند وميانمار الاقتصادي، وممر الصين وشبه جزيرة الهند الصينية الاقتصادي، وممر الصين وآسيا الوسطى وغرب آسيا، والجسر القاري الأوراسي الجديد (على العلى، مرجع سابق). وتوضح خريطة (١) الدول التي تمر بها مبادرة "الحزام والطريق" الصينية.



ويمثل "طريق الحرير" شبكة من طرق تجارية، ومسارات تربط الصين بجيرانها وبالقارة القديمة، التي تواجدت في القرن الثاني قبل الميلاد. وشملت مبادرة "الحزام والطريق" خطوط بحرية يتم من خلالها ربط موانئ رئيسية في دول تربطها مع الصين علاقات تجارية تشمل تبادل البضائع المختلفة مثل: المعادن الثمينة والحرير، والورق، والتوابل والبارود. ويمكن القول بأن قيمة هذه الطرق تراجعت بعد أن أدخل الأوروبيين التحسينات الكثيرة على الأنظمة الخاصة بالنقل البحري، وبعد أن تعاظم الدور الذي تقوم به قناة السويس في التبادل التجاري الدولي (الخليج، ٢٠٢٢).

كما تهدف المبادرة إلى إعادة إحياء هذا طريق الحرير القديم كي تربط مدن الصين بوجهات روسيا وآسيا وأوروبا التجارية. كما ستسعى إلى ضم مجموعة من الطرق البحرية للطريق الجديد بهدف تأسيس تعاون منتج مع الدول التي تقع في أوقيانوسيا وجنوب شرق آسيا وأفريقيا وآسيا وطريق بحر الشمال الروسي. وعلى الرغم من أن الاستراتيجية كان من الممكن تنفيذها من خلال ربط شبكات السكك الحديدية بين الصين وكازاخستان في ١٩٩٠م، إلا أنه في عام ٢٠٠٨م، شهد المشروع نقطة تحول هامة عندما وصل أول قطار للصين قادما من ألمانيا. وقد بلغ عدد الدول

الموقعة على وثائق للتعاون في هذا المشروع حتى الآن ١٢٦ دولة و٢٩ منظمة عالمية؛ حيث ستقوم كازاخستان بإنفاق ٩ مليارات دولار لتحسين شبكة السكك الحديدية والطرق. وكما وقعت إيطاليا من جانبها، على مجموعة من الاتفاقيات بقيمة ٨ مليارات دولار بهدف تطوير الموانئ الخاصة بتصدير المواد الغذائية والمنتجات إلى الصين. مع عمل خط للسكة الحديدية جديد من جاكرتا الإندونيسية حتي عاصمة مقاطعة جاوة "باندونغ" كي يقليص فترة الرحلة من ٣ ساعات إلى ٤٠ دقيقة. وفي باكستان فسيتم تحديثها للسماح بشحن ونقل البضائع إلى أفريقيا وغرب آسيا بالقطار والموانئ الواقعة في جوادار وكراتشي (على العلى، مرجع سابق).

ومن أجل تعزيز الاستراتيجية الشاملة، عمدت الصين على وضع استراتيجية "الحزام والطريق" ذات الطابع السيبراني المعزز؛ حيث أشارت العديد من التقارير الغربية أن الدولة الصينية استطاعت أن توسع المصالح الأمنية المعززة الخاصة بها في عدد من الدول التي تربطها بالصين اتفاقيات استثمارية واقتصادية في الدائرة الاستراتيجية لمبادرة "حزام وحد طريق واحد"، فمن المعروف لدى العديد من الدول أن الصين تمتلك قوة سيبرانية فوق المتوسطة، بالمقارنة بالمستوى الغربي، وبحكم افتقارها تكنولوجيا أشباه الموصلات أو "علم الرقائق"، وعلى الرغم من ذلك تمكنت الصين من ممارسة "الهجوم السيبراني"، والحصول على التكنولوجيا من بعض مشاريع الغرب الاستراتيجية، مثل مشروع "لوكهيد مارتون" والمعني بتطوير الجيل الخامس من الطائرات الأمريكية؛ حيث استخدمت الهجمات السيبرانية على بعض أذرع صناعة هذه الطائرات، كما أنها استطاعت أن تمتلك القدرة على بناء الجدار الناري الإلكتروني للفضاء الإلكتروني الخاص بها؛ بهدف ممارسة السيطرة المعلوماتية، كما عملت على إطلاق المشروع الخاص بالسيادة الرقمية والذي يعمل على منع الألاف من الصفحات الإلكترونية التي أرتأت أنها تهدد أمنها القومي (على العلى، مرجع سابق).

وخلاصة القول في هذا الشأن أن الصين مارست التطلعات الجيوسيبرانية وعلى وجه الخصوص مع البلدان التي رأت أنها تمثل تهديداً سيبرانياً لها؛ إذ زودت الصين العديد من الدول وعلى وجه الخصوص منطقة الشرق الأوسط وآسيا الوسطى وأفريقيا، بالبنية التحتية الرقمية والبرامج الإلكترونية لكي تتمكن من ممارسة سلطتها أو سيادتها السيبرانية في مجال التفاعلات السيبرانية.

٢- القدرات الجيوسيبرانية الصينية وآليات التوظيف "القوة الصلبه".

لقد استطاعت الصين وضع الاستراتيجية الاستثنائية للتطلع والتوجه الجيواستراتيجي، والذي جعلها تجني مردوداً سياسياً واقتصادياً وأمنياً، حتى وصل إلى العائد الرقمي المعزز في بعد وعمق استراتيجي اصطدم مع المصالح الخاصة بالقوى الدولية الفاعلة، وأدى إلى تكوين فضاء من الصراعات في الإطار الجيواستراتيجي، والجيوسيبراني، وستتعمق هذه الصراعات مع الاستمرار في التغلغل الصيني على هذا النحو في الأجل القريب والمتوسط والبعيد. ولذلك لم تتخلي الصين عن قوتها السيبرانية الصلبة والتي مارستها في السابق، وما تزال تمارسها حتى الآن وفي ضوء ذلك نستعرض أهم التهديدات الجيوسيبرانية الصينية خارج نطاقها السيبراني على النحو التالي (أ ف ب، ٢٠٢٢)، (إينيه سوريد، ٢٠٢٢)، (أحمد حمدي، مرجع سابق)، (Gandhi, Robin,) :2011

١- أهم التهديدات السيبرانية خلال الفترة من ١٩٩٩ وحتى ٢٠١٨ جدول (٤):

الفترة	الهجمات السيبرانية	الوصف	ملاحظات
١٩٩٩	الهجوم السيبراني من مجموعة قراصنة صينيون على الولايات المتحدة.	استهدف مواقع إلكترونية رسمية للولايات المتحدة الأمريكية وبالأخص موقع تخص البيت الأبيض.	
١٩٩٩	الهجوم السيبراني ضد ضد تايوان.	استهداف واختراق موقع تابعة للحكومة التايوانية.	
٢٠٠١	الحرب السيبرانية ضد الولايات المتحدة الأمريكية.	استهداف طائرات استطلاع أمريكية وتحطيمها.	
٢٠٠١	الحرب السيبرانية ضد اليابان.	استهداف مواقع وخدمات الإنترنت في اليابان.	
٢٠١٨	الهجوم السيبراني على الولايات المتحدة.	استهداف والحصول على معلومات تخص عقود بحرية وأمور تتعلق بصيانة السفن وخطط الصواريخ.	حسب إفادة مسؤلين أمريكان.

٢- أهم التهديدات السيبرانية خلال الفترة من ٢٠١٩ وحتى ٢٠٢٢ جدول (٥):

الفترة	الهجمات السيبرانية	الوصف	ملاحظات
٢٠١٩	الهجوم السيبراني على ٢٧ جامعة أمريكية من قبل قراصنة صينيون.	استهداف ٢٧ جامعة أمريكية واختراقها من قبل راصنة صينيون ومحاولة الحصول على الابحاث التي تخص التقنيات البحرية.	
٢٠١٩	الهجوم السيبراني على شركة إيرباص الفضائية الأوروبية من قبل قراصنة صينيون.	استهداف شركة إيرباص الفضائية الأوروبية والحصول على معلومات شخصية تخص الموظفين.	
٢٠٢١	الهجوم السيبراني الصيني على البرلمان النرويجي.	استهداف نظام البريد الإلكتروني لبرلمان النرويج حيث نفذ الهجوم من الصين.	
٢٠٢٢	الهجوم السيبراني من قبل قراصنة صينيون على ٦ ولايات أمريكية.	استهداف ٦ ولايات أمريكية من خلال استغلال نقاط ضعف في برامج إلكترونية من قبل جزء من المجموعة الصينية "أفنسد برسيستنت تريد 4 "APT41" وهذا ما نفته الصين.	

وفي ضوء ما سبق يمكن القول بأن آليات توظيف القوة السيبرانية الصينية قد اختلفت عن توظيف القوة الروسية؛ حيث سعت الاستراتيجية الشاملة الصينية لاستخدام القوة الناعمة في مبادرة "حزام واحد طريق واحد"، والقوة الصلبة في الهجمات السيبرانية واستهداف البني التحتية للدول المعادية لها.

خاتمة الدراسة:

ويمكن تناول الخاتمة فى النقاط التالية، للإجابة على التساؤل الرئيسي للدراسة وتساؤلاتها الفرعية على النحو التالى:

أولاً: النتائج:

لقد توصلت الدراسة إلى مجموعة من النتائج من واقع الإشكالية الرئيسية والتى تم طرحها لتحقيق أهداف الدراسة وهى: (إلي أي مدي كان للبيئة الرقمية البديلة للتفاعلات الدولية "الجيوسيبرانية" أثرها على التحول في القوة الروسية والصينية؟ وإلى أى مدى كان للوجود الروسي والصيني في الفضاء الجيوبولوتيكي أثره على آليات التوظيف في الاستراتيجية الروسية والصينية؟).

وخلاصة القول فى ضوء ما تم عرضه من واقع الدراسة وتحليل "الجيوسيبرانية والتحولات في خصائص وأبعاد القوة وآليات توظيفها في الاستراتيجية الروسية والصينية"، بدا واضحاً أهمية التكنولوجيا والهيمنة والسيطرة التي تمارسها على الساحة الدولية، ومدي القدرة على التحكم في قوة وسلوك الدول، مما ساعد على انتقال الصراع عبر الفضاء الإلكتروني، وأعطي حافزاً للدول لكي تتسارع في صياغة استراتيجيات تختص بآليات توظيف القوة والأمن السيبراني، وفي ظل هذا الاتساع فى تأثير العامل العلمي والتكنولوجي؛ لم يعد من المقبول أن تكون القوة العسكرية هى العنصر الذي يتحكم في مسار العلاقات الدولية، مما جعل هناك حاجه لإحداث تغيرات على مفهوم القوة حتى تتواكب مع متغيرات النظام الحديث كالإنترنت وانتشار المعلومة، مما يعطي مصطلح القوة بعداً آخر لا يحتوي على البعد المادى فقط؛ وإنما يمتد ليشمل الأبعاد المعنوية والجيوسيبرانية. وقد بدا ذلك واضحاً من خلال تحليل نتائج الدراسة؛ حيث جاءت كالتالي:

استعرض المحور الأول ... أبعاد العلاقة بين الجيوسيبرانية والتحولات في خصائص وأبعاد القوة في ظل بيئة عالمية متغيرة وكانت النتائج كالتالي:

- أن القوة في العلاقات الدولية تطورت إبان ظهور القوة السيبرانية بفعل التطور الذي أصاب المعلومات والاتصالات مما جعلها هدف تسعي الدول للوصول إليه.
- أن عملية التأثر والتأثير تنتقل من وإلى الفضاء السيبراني عبر مسارات القوة أو الاتجاهات التي سيطرت على الإطار العام الدولي.

- اقتران "الفضاء السيبراني" بمفاهيم مختلفة منها انعدام الجغرافية وظهور ما يطلق عليه جغرافيا الإبحار المعلوماتي.
- تعد ظاهرة "الفضاء السيبراني" أهم خصائص عصر المعلومات والاتصالات بدون منازع.
- أن مفهوم القوة لا يزال يمثل أحد المرتكزات الأساسية لتفسير وتحليل الظواهر السياسية.
- أن القوة السيبرانية باتت واقع مساند للقوة التقليدية.
- أن الجيوسيبرانية قد وفرت مجالاً حركياً تستطيع القوة السيبرانية من خلاله تجاوز الحدود الجغرافية للوصول لأهداف قد يصعب الوصول إليها عبر القوة التقليدية.
- أن التقدم التكنولوجي جعل العالم يدخل في مضمار سباق تسلح جديد، من نوع أخر وهو سباق تسلح الفضاء الخارجي الباهظ الثمن، وهي جزء من مسرح الحروب تستخدم نفس اساليب الحرب القديمة بالتدمير والخداع، والتسلل مع اختلاف طريقة التنفيذ.
- على الرغم من التكاليف الباهظة التي قدمتها التكنولوجيا في مجال تقدم تقنيات أشكال الأسلحة، إلا أنها وفرت من امكانية انتقال الصراع المستقبلي نحو الفضاء، وبهذا دخل نمط جديد من الحروب اللادموية الغير مكلفة مادياً وهي "الحروب السيبرانية".

وفي المحور الثاني ... الجيوسيبرانية وآليات التوظيف في الاستراتيجية الروسية، كانت النتائج كالتالي:

- أن العقيدة الجيوسيبرانية الروسية تنطلق من تبنى موقفاً دفاعياً من منطلق رغبتها في استهداف أنظمة البنية التحتية الحيوية في الفضاء السيبراني للدول المعادية لها.
- أن الدوافع من هذه الهجمات السيبرانية الروسية قد تكون دوافع عسكرية أو اقتصادية أو سياسية.
- استغلال روسيا سلاح الهجمات السيبرانية في نزاعاتها الأخيرة مع أوكرانيا والدول الغربية ٢٠٢٢م.
- اختلاف الاستراتيجية الجيوسيبرانية الروسية عن نقيضتها من الدول الأخري وعلى وجه الخصوص الغربية.
- اختلاف الرؤية الروسية "للحرب السيبرانية" اختلافاً كلياً عن نظيراتها من دول "المنظومة الغربية"، ويرجع السبب في ذلك لامتلاك روسيا العديد من الطرق الاستراتيجية لدمج منظومات الجيل الخامس والتي بدورها تشمل الحرب الدعائية الإلكترونية، ومنظومة الحرب الإلكترونية بالإضافة إلى منظومة الحرب السيبرانية، ومن ثم تمتلك بذلك السطوة والتأثير التي تمكنها من

ممارسة السطوة الإلكترونية والتأثير الإلكترونية في العمق الاستراتيجي لأي دولة من خلال تنظيم وسائل التدخل والنفوذ في العمق.

- اعتقاد الروس بأن روسيا مقفلة جيواستراتيجياً جعلها في صراع مع القوى الداخلية والخارجية التي تسعى إلى الاضرار بأمنها من خلال مجال المعلومات والإنترنت، والتدفق الحر للمعلومات التي يولدها، والتي تمثل على حد سواء تهديداً وفرصاً في نفس الوقت.
- عدم استخدام المنظرون العسكريون الروس مصطلحات حروب الإنترنت أو الحرب الإلكترونية، ويستخدمون بدلا منها مصطلح العمليات السيبرانية.
- أن السيبرانية الهجومية تلعب دوراً هاماً وكبيراً في عقيدة الجيش الروسي التقليدي، وربما تلعب دوراً في الرؤي المستقبلية في الاستراتيجية الروسية والتي سميت بـ "إطار الردع"، وهذا ما تم ملاحظته خلال الحرب الروسية – الأوكرانية الأخيرة في عام ٢٠٢٢م. وما قامت به روسيا من استخدام التكنولوجيا المتطورة في حروبها السيبرانية مع أوكرانيا، وعلى الرغم من أن الجيش الروسي كان بطيئا في احتضان السيبرانية لأسباب هيكلية وعقائدية على حد سواء؛ إلا أن الدراسات الغربية تؤكد أن روسيا في صدد تعزيز القدرات السيبرانية الهجومية وكذلك القدرات السيبرانية الدفاعية.

وفي المحور الثالث ... الجيوسيبرانية وآليات التوظيف في الاستراتيجية الصينية، كانت النتائج كالتالي:

- أن تطلعات الصين الجيوسيبرانية جعلتها تزود مجموعة من الدول وعلى وجه الخصوص في منطقة آسيا الوسطى والشرق الأوسط وأفريقيا، بالبنية التحتية الرقمية والبرامج الإلكترونية التي تستطيع من خلالها ممارسة سلطتها أو سيادتها السيبرانية في مجال التفاعلات السيبرانية للدول.
- عكست الاستراتيجية الصينية الشاملة في حزامها الجيوبوليتيكي، الرؤية الصينية بعيدة المدي لوجودها في الفضاء الجيوبوليتيكي الواسع، وذلك بهدف تحقيق المصالح الاستراتيجية للصين، من خلال الاستثمار في البنية التحتية.
- أن هناك اختلاف في توظيف القوة السيبرانية الصينية عن توظيف القوة الروسية؛ حيث سعت الاستراتيجية الشاملة الصينية لاستخدام القوة الناعمة في مبادرة "حزام واحد طريق واحد"، والقوة الصلبة في الهجمات السيبرانية واستهداف البني التحتية للدول المعادية لها. بينما ركزت روسيا في القوة الصلبة فقط.

ثانياً: توصيات الدراسة:

وفى هذا الإطار فقد اقترحت الدراسة مجموعة من التوصيات تمثلت في:

١- على المستوي القيمي:

- **العمل على تفعيل الدور القانوني على المستوي الدولي، وصياغة آليات وقواعد تتناسب مع هذا النوع من الحروب الجديدة، آخذة في الاعتبار التطور الحاصل في المجال التكنولوجي، والعمل على تكثيف الجهود الدولية لسن هذه القوانين لمواجهة الحرب الحديثة التي فرضت نفسها على الساحة الدولية.**
- **العمل على صياغة استراتيجية خاصة بمنظومة الأمن السيبراني، واتخاذ التدابير اللازمة للحد من الهجمات والاختراقات المدمرة، للحيلولة دون قيام حرب سيبرانية عالمية شاملة كما هو ظاهر الآن في الحرب الروسية الأوكرانية. مع زيادة فاعلية جوانب الأمن السيبراني ورفع أنظمة حماية الشبكات عن طريق وضع البرامج الخاصة بحماية الأنظمة، والمعلومات وشبكات البنى التحتية من الهجمات السيبرانية.**
- **خلق بيئة سيبرانية آمنة في الدول التي تعاني من الاختراقات السيبرانية بجهود دولية؛ لتمكن الأفراد والمؤسسات من تحقيق طموحاتهم التكنولوجية في ظل التقدم الرقمي الهائل.**

٢- على المستوي البنيوي:

- **تخصيص جزء من ميزانيات الدول لإشاء برامج توعية لمواجهة وتجنب الهجمات السيبرانية.**
- **العمل على رفع مستوى الأمن الرقمي للمدن الرقمية.**
- **العمل على رسم هيكل للأمن السيبراني يتمتع بنوع من المرونة لاسيما بالجوانب التجارية والاقتصادية.**

المراجع العربية:

أ ف ب. (٢٠٢٢). *استهداف ٦ ولايات أمريكية بهجوم سيبراني صيني*". (موقع أندبندنت عربية. نشر بتاريخ ٢٠٢٢/٣/٩). تاريخ زيارة الموقع: ٢٠٢٢/١١/١٢م. موقع: https://www.independentarabia.com/node/310091/الأخبار/استهداف-٦-ولايات-أميركية-بهجوم-سيبراني-صيني.

أحمد حمدي. (٢٠١٩). *تعرف على أبرز الهجمات السيبرانية لعامي (٢٠١٨-٢٠١٩)*". (مقال منشور بجريدة ماكس الإلكترونية بتاريخ ٢٠١٩/١١/٣). تاريخ الزيارة: ٢٠٢٢/١١/١٠. موقع: https:Jawalmak.com//eam.

أحمد عبيس الفتلاوي. (٢٠١٦). "*الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناتجة عنها في ضوء التنظيم الدولي المعاصر*". (العراق. مجلة المحقق للعلوم القانونية والسياسية. المجلد٨. العدد٤).

إسماعيل زروقة. (٢٠١٩). "*الفضاء السيبرانى والتحول فى مفاهيم القوة والصراع*". (الجزائر. مجلة العلوم القانونية والسياسية. المجلد ١٠. العدد١).

إينه إريكسن سوريد. (٢٠٢١). "*النرويج تتهم الصين بتنفيذ هجوم سيبراني على برلمانها*". (موقع روسيا اليوم العربية نقلاً عن وكالة رويترز نشر بتاريخ ٢٠٢١/٧/١٩). تاريخ الزيارة: ٢٠٢٢/١١/١٠. موقع: https://arabic.rt.com/world/1253353-النرويج-تتهم-الصين-بتنفيذ-هجوم-سيبراني-على-برلمانها

إيهاب خليفة. (٢٠١٤). "*القوة الإلكترونية وأبعاد التحول فى خصائص القوة*". (الإسكندرية. مكتبة الإسكندرية. وحدة الدراسات المستقبلية).

إيهاب خليفة. (٢٠١٨). "*الحرب السيبرانية مراجعة العقيدة العسكرية استعداد للمعركة القادمة*". (القاهرة. الأهرام للدراسات السياسية والاستراتيجية. مجلة السياسة الدولية. العدد ٢١١).

بسمة يونس محمد الرفادى. (٢٠١٨). "*الحروب السيبرانية وأثرها فى النظام الدولى*". (ليبيا. جامعة بنغازى. مجلة العلوم والدراسات الإنسانية. العدد٤٩).

بيتر في سيل. (٢٠١٧). "*الكون الرقمي: الثورة العالمية في الاتصالات*". ترجمة: ضياء وارد. (المملكة المتحدة. مؤسسة هنداوي سي.أي.سي).

تغريد معين حسن. (٢٠١٩). "*الأثر العسكري للأمن السيبراني في الجغرافيا السياسية للدولة*". (مجلة البحوث الجغرافية. العدد٣٠). موقع: https://search.emarefa.net/detail/BIM-948225

خالد حنفى على. (٢٠١٧). "*الصراع السيبرانى: التنازع العالمى على قوة الفضاء الإلكترونى*". (القاهرة. مركز الأهرام للدراسات السياسية والاستراتيجية. مجلة السياسة الدولية. ملحق اتجاهات نظرية. العدد٢٠٨).

رغده البهى، وآخرون. (٢٠٢٠). *"التطورات التكنولوجية: اختراقات سيبرانية – وفرص ذكاء اصطناعى"*– فى خالد حنفى. *"توقعات: استشراف مصرى لأبرز قضايا الإقليم العربى والعالم"* – (المركز المصرى للفكر والدراسات الاستراتيجية).

زياد على فتحى. (٢٠١٩). *"رؤية استراتيجية: العمليات السيبرانية الأوروأطلسية ومهددات الجيوسيبرانية الروسية "رؤية في الاشتباك السيبراني الأورو– روسي"*. (العراق. مجلة حمورابي. العدد ٣٠).

سلام الوافي. (٢٠١٧). *"الحرب الإلكترونية مظهر من مظاهر عرض القوة بين روسيا وأمريكا"* . (مركز الوقت للتحليل والأخبار. شبكة المعلومات الدولية). تاريخ زيارة الموقع: ٢٠٢٢/١٠/١. موقع: https://www.alwaght.com/ar//News/8293.

صحيفة الخليج. (٢٠٢٢). *"تعرف إلى طريق الحرير الجديد"* . (موقع صحيفة الخليج. نشر بتاريخ ٢٠٢٢/٣/١٤). تاريخ الدخول: ٢٠٢٢/١١/١٠م. موقع: https://www.alkhaleej.ae/2022-03-14/تعرف-إلى-طريق-الحرير-الجديد/قراءات-في-كتب/ثقافة

ضحي كاظم. (٢٠٢١). *"البعد الجيوسياسي للأمن السيبراني"* . (الجزائر. مجلة العلوم الإنسانية. المركز الجامعي على كافي. المجلد ٥. العدد١).

عادل عبد الصادق. (٢٠٠٩). *"الإرهاب الإلكتروني: القوة في العلاقات الدولية نمط جديد وتحديات مختلفة"* . (القاهرة. مركز الأهرام للدراسات السياسية والاستراتيجية).

عادل عبد الصادق. (٢٠١٧). *"الحروب السيبرانية: تصاعد القدرات والتحديات للأمن العالمي"* . (مجلة قضايا استراتيجية. المركز العربى لأبحاث الفضاء الالكترونى).

عبد الله عطوي. (٢٠٠١). *"جغرافيا السكان"* . ط١. (بيروت. دار النهضة العربية).

على زياد العلى. (٢٠١٩). *"الجيوسيبرانية في استراتيجية طريق واحد حزام واحد الصينية"* . (شبكة النبأ المعلوماتية). تاريخ الزيارة: ٢٠٢٢/٧/٢٧. موقع: https://annabaa.org/arabic/print/18538.

على زياد فتحى. (٢٠١٩). *"العمليات السيبرانية الأوروأطلسية ومهددات الجيوسيبرانية الروسية: رؤية فى الاشتباك السيبرانى الأورو – روسى"*. (العراق. مجلة حمورابى. العدد ٣٠).

لايدر جوليان. (١٩٨١). *"حول طبيعة الحرب"* . ط١. (دمشق. مركز الدراسات العسكرية).

لبنى خميس مهدى، وآخرون. (٢٠٢٠). *"أثر السيبرانية فى تطور القوة"* . (العراق. مجلة حمورابى. العدد ٣٣–٣٤).

مايكل كوفمان، كاتيا ميجاشيفا. (٢٠١٧). *"عبر من عمليات روسيا في شبه جزيرة القرم وشرق أوكرانيا"* . (كاليفورنيا. مؤسسة راندا).

محمد منذر جلال، وآخرون. (٢٠٢٠). *الأمن السيبراني وسياسات المواجهة الدولية"*. (ألمانيا. المركز العربي الديمقراطي. مجلة الدراسات الاستراتيجية والعسكرية. المجلد٢. العدد٩).

منير البعلبكي. (٢٠٠٤). *المورد"* . (بيروت. دار العلم للملايين).

يحيى بن مفرح الزهرانى. (٢٠١٧). *الأبعاد الاستراتيجية والقانونية للحرب السيبرانية* . (الجزائر. جامعة الشهيد حمه لخضر الوادى. مجلة البحوث والدراسات. العدد٢٣).

المراجع الأجنبية:

Greenberg. A. (2017). ***How An Entire Nation Became Russia›s Test Lab for Cyberwa.*** **(Center wired‹ Article published on the World Wide Web on the following). (Accessed November 11, 2022). Link https://www.wired.com/story/ russian-hackers-attack-ukraine.**

Agrum. C. (2010). ***Words for Understanding Cyber Security: Enjoying a Calm Internet.*** **(Editions).**

Andrew. L. (2018). ***Fower and security in cybersface: implications for the west phhalian state system*****. (Center for wuropean and North American Affaris).**

Batashvil. D. (2017). ***Russia's cyber war: past, present.*** **(Euobserver center. Article published on the World Wide Web on the following). (accessed November 11, 2022), link https://euobserver.com/opinion/136909**

Connell. M & Sarah. (2017). ***Russia›s Approach to Cyber Warfare.*** **(Ealcleardefense. Vogler). Article published on the World Wide Web on the following link https://www.realcleardefense. Com/articles/2017/05/09/russias_ approach_to_cyber_warfare_ 111338.html.**

Exk. C. (2017). ***The World Evolves*****. (Copenhagen, translation: Raffi Adorard).**

Gibney. E. (2022). ***Where is Russia's cyberwarfare? Researchers deconstruct its strategy*****. (Nature magazine on March 21). (Accessed November 11, 2022). Link https://www.scientificamerican.com/article/where-is-russias-cyberwar-researchers-decipher-its-strategy/.**

John. O. & Toal. G. (2015). ***Mistrust about Political Motives in Contested Ukraine*****. (Washington Post, February 13). (Accessed November 11, 2022). https://www.washingtonpost.com/blogs/monkey-cage/wp/2015/02/13/ mistrust-about-political-motives-in-contested-ukraine/.**

Jolanta. D. (2014). ***The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study*****. (Warsaw. Poland: Centre for Eastern Studies. Point of View Number 42, May), (accessed November 11, 2022). http://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_infor mation_ warfare.pdf.**

Joseph S. Nye, Jr. (2010). ***Cyber Power,*** **(Cambridge, Belfer Center for Science and International Affairs, Harvard Kennedy School).**

Kenneth W. Dam. William A. Owens & Herbert S. Lin, eds. (2009). ***Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities,*** **(Washington, D.C.: National Academies Press).**

Kimner. M. & Paul Bente. J (2012). ***Cyber Security for Economic Actors: Legal and Legal Risks and Responses*****. (Hermes Scientific Publications, coll. "Cybercrime and Cybercrime", 13 December).**

Kuehl. Daniel T. (2009). ***From cyber space to cyber power: defining the problem in cyber power and national security*****. (Washington. D.C: national Defence up). Joseph S. Nye. Jr. (2011).** ***The future of power*****. Bulletin of the American Academy.**

Libicki. Martin C. (2009). ***Cyberdeterrence and Cyberwarfare*****. (RAND: Santa Monica).**

Palfrey, J. G., Rohozinski. Zittrain, J. In addition, Deibert, R. J., R. (Eds.), (2011). ***Access Contested Security, Identity and Resistance in Asian Cyberspace*****. (MIT Press).**

Robin. G. (2011). ***Dimensions of cyber-Attacks*****. (Technology and society Magazine. vol 11. spring).**

Rohozinski. R. & Ronald J. Deibert. (2010). ***Risking Security: Policies and Paradoxes of Cyberspace Security*****. (International Political Sociology 4, 1)**

Scottw**. B. (2000).** ***Difining and deterring Cyber war fare*****. (USA, strategy Research project).**

Stephen. E. (2016). ***Putin's RIA Novosti Revamp Prompts Propaganda Fears*****. (BBC Monitoring. December 9). (Accessed November 11, 2022). Link http://www.bbc.com/news/world-europe-25309139.**

Venter. D. (2017). ***A Future and Strategic Study - Changes in Cybersecurity: Factors Constraints, and Variables*****. (Naples).**