DOI: https://doi.org/10.25130/tjfps.v3i25.360

TJFPS
ISSUE 25

IRAQI Academic Scientific Journals
العراقية المجلات الاكاديمية العلمية
ISSN: 2663-9203 (Electronic)
ISSN: 2312-6639 (print)

Contents lists available at:
http://tjfps.tu.edu.iq/index.php/poiltic
Tikrit Journal For Political Science

Tikrit Journal For Political Science
SINCE 2014

العقيدة الاستراتيجية وإدراك التهديدات السيبرانية

"Strategic Doctrine and Cyber Threats Realization"

Dr. Muammar Muneim Sahi Al-Ammar [a]
Al-Nahrain University/College of political science

م.د . معمر منعم صاحي العمار [a] *
جامعة النهرين /كلية العلوم السياسية

Article info.

Article history:
- Received 15 .7. 2021
- Accepted 23.9. 2021
- Available online 30\9\2021

Keywords:
-Strategic Doctrine
-Cyber security
-Strategic studies

©2021. THIS IS AN OPEN ACCESS ARTICLE UNDER THE CC BY LICENSE
http://creativecommons.org/licenses/by/4.0/

Abstract: Cyber security is considered one of the most important points of exposure and weakness that embarrasses the national strategy of the state, as it has become a new and widely threatening entrance, and its practice pollutes the faith and its pillars. As long as it does not exceed as an information technology management, a positive management represented by protection and security, and a negative management in terms of war, attack and crimes, and in our study we will explain The course of strategic doctrine and its awareness of cyber threats.

Strategic doctrine for states and organizations relies on recognizing and effectively addressing cyber threats. Cyber threats have increased over the past two decades with technological advancements and growing reliance on digital systems. These threats include attacks on critical infrastructure, data theft, cyber espionage, and cyber-terrorism. Recognizing these threats requires developing defensive strategies based on international cooperation, information sharing, and advancing cybersecurity technologies. Additionally, states must enhance national capabilities by training experts, raising security awareness among individuals and institutions, and updating legislation to include cybercrimes. These efforts contribute to creating a safer digital environment, thereby enhancing national security and stability and ensuring the continuity of essential services and operations.

*Corresponding Author: Dr. Muammar Muneim Sahi Al-Ammar,E-Mail: Muamiq89@gmail.com
Tel: xxx, Affiliation: Al-Nahrain University/College of political science

معلومات البحث :

تواريخ البحث:

الاستلام: 15 \7\2021
القبول: 23\9\2021
النشر :30\9\2021

الخلاصة : يعد الأمن السيبراني واحداً من اهم نقاط الانكشاف والضعف التي تصيب حرجاً للاستراتيجية القومية للدولة كونها اصبحت مدخلاً جديداً ومهدداً واسعاً وممارستها تلوث العقيدة واركانها . ما دامت لا تتعدى بوصفها إدارة تقنية للمعلومات، إدارة إيجابية تتمثل بالحماية والأمن، وسلبية حيث الحرب والهجوم والجرائم، وفي محض دراستنا سنوضح مجريات العقيدة الاستراتيجية وادراكها للتهديدات السيبرانية .

تعتمد العقيدة الاستراتيجية للدول والمنظمات على إدراكها للتهديدات السيبرانية والتعامل معها بفعالية. تزايدت التهديدات السيبرانية في العقدين الأخيرين مع التقدم التكنولوجي والاعتماد المتزايد على الأنظمة الرقمية. تشمل هذه التهديدات الهجمات على البنى التحتية الحيوية، سرقة البيانات، التجسس السيبراني، والهجمات الإرهابية. إدراك هذه التهديدات يتطلب تطوير استراتيجيات دفاعية تعتمد على التعاون الدولي، وتبادل المعلومات، وتطوير تكنولوجيا الحماية السيبرانية. بالإضافة إلى ذلك، يتعين على الدول تعزيز القدرات الوطنية من خلال تدريب الخبراء، وتعزيز الوعي الأمني بين الأفراد والمؤسسات، وتحديث التشريعات لتشمل الجرائم السيبرانية. تساهم هذه الجهود في بناء بيئة رقمية أكثر أمانًا، مما يعزز الاستقرار والأمن الوطني ويضمن استمرارية الأعمال والخدمات الأساسية.

الكلمات المفتاحية:

– العقيدة الاستراتيجية

–الامن السيبراني

–الدراسات الاستراتيجية

المقدمة:

شكلت العقيدة الاستراتيجية موضوعاً للبحث والدراسة وما تزال، ولعل هذه الأهمية التي يتمتع بها هذا الموضوع في علم الاستراتيجية اليوم على صعيد العالم لم تتأتى من فراغ، إذ ان العقيدة الاستراتيجية تدخل في صناعتها متغيرات عدة، لعل احدها نظام المعتقدات والمبادئ التي يؤمن بها صناع الإستراتيجية والتي تهيئ لهم وعلى اختلاف مراكزهم تصور وتفسير خاص للأحداث، والذي يختلف من صانع قرار إلى آخر بالضرورة والتي قد تكون (أي هذه العقيدة) اقتصادية أو دينية أو سياسية، الخ.. ، ونتيجة لحركة التغيير الدولية التي اصابت العالم ودخول التكنولوجيا والعولمة ومروراً بالاحداث الدولية خصوصاً احداث 11 / ايلول /2001 وما تلاها من تغييرات اصبح التهديد الذي يواجه الاستراتيجية العليا هو وجود نقاط انكشاف وضعف تؤثر على منظومة القيم الاستراتيجية (كالسيبرانية) فقد اصبح التهديد السيبراني او الحروب السيبرانية باعتبارها حروب لا تناظرية، ذات تكلفة متدنية تعطي للمهاجم أفضلية واضحة، نظراً لما تتميز به من سرعة ومرونة ومبادأة، مما اسس اولاً عدم اشتغال لنظم الردع التقليدية وثانياً تعدد المستويات من حيث الشدة، فهناك المنخفضة والمتوسطة والخشنة ، ومرتفعة الشدة الموازية للأعمال العسكرية التقليدية لدرجة ان البعض من المحللين والمراقبين، بدأ مقتنع بأن تلك الحرب بكل ما تضمه من أدوات متعددة، ستكون سلاحاً حاسماً في النزاعات بين الدول في المستقبل.

اهمية البحث :تأتي اهمية البحث على المستوى الفكري والنظري والتطبيقي حول ادراك العقيدة الاستراتيجية لتهديدات السيبرانية كونها اسلوب خفي في بيئة عالمية متغيرة ، و أن توضيح واثبات الدور الذي تلعبه العقيدة الاستراتيجية التي يؤمن بها صناع الإستراتيجية في بناء الإستراتيجية العالمية من خلال توفير تفسير مسبق للأحداث نابع عن صورة مسبقة وإيمان مسبق بخط سير الأحداث ، فضلاً عن ذلك، فإن هذا النمط من التهديدات، استراتيجياً، سيوجد مخاطر وتحديات شتى، وبالتالي وجود سباق تسلح من نوع جديد كونه يمثل احد اهم الأسلحة المرشحة للاستخدام العالمي و تغيير نمط الردع من المنظومة التقليدية والنووية الى ردع سيبراني خفي متمثل بالتكنولوجيا والحوسبة الرقمية .

اشكالية البحث :تناول هذا البحث إشكالية دور العقيدة الاستراتيجية تجاه التهديدات السيبرانية بوصفها متغير داخل في عملية صنع الإستراتيجية والكيفية التي يؤثر بها من خلال : **كيف يتم ذلك؟، وما هي صور الإفصاح عن مظاهر ذلك الإدراك؟، ما هو أثر العقيدة الاستراتيجية في زيادة مناعة الدولة الأمنية؟.**

فرضية البحث :تنطلق فرضية البحث من رؤية مفادها أن صناع الإستراتيجية وفي تعاطيهم واحتوائهم لقضية التهديدات السيبرانية لما تمتلكه هذه التهديدات من انتقاليه في الحركة والتأثير ساعدت على الايمان برسخ العقيدة الاستراتيجية كونها تستحضر مقتربات تأهيل لإدراك تلك التهديدات وتصويب سبل مكافحتها، معرفياً ومؤسساتياً.

منهجية البحث :اعتمدت الدراسة، على منهج الاستنباط لكل المعطيات المؤلفة لفكرتها وعلى وفق النسغين الصاعد والنازل حيث موضوع العقيدة الاستراتيجية ، وذلك لتحقيق إدراك مقنع لما يتوجب تبنيه من افتراضات وتم اعتماد المنهج التحليلي الأقرب إلى المنهج الاستنباطي، طالما وجد به نوعاً من التوازن في إدراك، حيث عالج الباحث عبر (المنهج التحليلي) مستويات التفكير التي يرتكز اليها صانعي القرار الاستراتيجي من خلال دراسة العقيدة الاستراتيجية وعملية ادراك التهديدات ضمن حركة التغيير الدولية عن طريق نموذج تحليلي التي تبين التطور الحاصل في انماط الحروب و الردع وتغيير المفاهيم والمكنونات الفكرية والعملياتية كالحرب السيبرانية .

هيكلية البحث :يتكون البحث من مقدمة ومبحثين وخاتمة تبين الاستنتاجات والتوصيات الفعلية في موضوع العقيدة الاستراتيجية وادراكها للتهديدات السيبرانية حيث تناول المبحث الاول :مدخل حول موضوع العقدية الاستراتيجية من خلالها نحاول وضع الافكار الاولية ورسم الاطر النظرية لموضوع العقيدة الاستراتيجية ، اما المبحث الثاني فتناول السيبرانية في علم الاستراتيجية من حيث المنطلق الفكري والعملياتي وصولاً الى تغيير نمط الردع عن طريق الحروب السيبرانية .

المبحث الاول : مدخل حول موضوع العقيدة الاستراتيجية :

سنبين في هذا المبحث حول الرؤى والافكار في موضوع العقيدة الاستراتيجية وما تمثله من تحقيق اداء مرتبط في صياغة الاهداف الاستراتيجية تبعاً لما يواجهه صانع القرار الاستراتيجي في موضوع القضية او الحدث او الازمة بما يضمن تحقيق الاداء الاستراتيجي في ظل حركة التغيير الدولية صعوداً ونزولاً.

المطلب الاول : افكار اولية :لا جدال في ما تمثله العقيدة الاستراتيجية من أهمية في بناء الدولة وتفسير سلوكياتها، كونها تمثل المرتكز الأساس المولّد للرؤى والأفكار، بل والمحور الذي تستند عليه كل المواقف سواءاً في صياغة حيثياتها أو إخراج إحداثياتها، والمرتكز الأساس المسّوغ لاتجاهات الأداء الذاتية لصنّاع القرار الاستراتيجي، طالما عدّت العقيدة الضابط المحّدد لنوعية تصرفاتهم وهم يواجهون البيئة المحيطة بهم بكل معطياتها وصفاتها وتهديداتها[1].

وإذ يخضع البعض العقيدة الاستراتيجية بتجلياتها التاريخية لمسارات التفكير الاستراتيجي لدولة ما، مادامت تلك المسارات ناتجة عن تلاقح اتجاهات معرفية متعددة وقدرات ذهنية خلافية، تلاقح هادف إلى بناء نموذج محدد/خاص للتصور الواعي الذي يعزز حقائق الوجود، إدارة للأزمات ومجابهة التهديدات والتحديات على مختلف أنماطها[2]، لتغدو الأهداف مساوية للغايات في تلك العقيدة تبعاً لما أسماه البعض بـ(حدسيات المعالجة) الناتجة أساساً عن حساسية المنفعة من السياسات المنفذة لها، وضعاً ومآلاً[3]. الأمر الذي يعلي من القيمة الذاتية للمواقف اللاحقة، لاتصالها الجوهري بالإدراك المتحقق لدى صنّاع القرار الاستراتيجي لاسيما لما تمر به الدولة من متغيرات وتحديات[4].

فإن البعض الآخر، رأى أن العقيدة الاستراتيجية، وهي المكونة بطريقة جدلية، تتجلى في تكوينها طبيعة الصورة التي تنسجها الدولة/الأمة لذاتها، ذلك التجلي ناتج أساساً مما تضمه تلك العقيدة من قدرات إدراكية تساعد صنّاع القرار على اكتشاف ما هو موجود في البيئة الاستراتيجية لا ما تضمه فحسب، لتتحرك

---

(1) عبد الرحمن حسن الشهري، تطور العقائد والاستراتيجيات العسكرية، الطبعة الأولى، مكتبة الملك فهد الوطنية، الرياض، 2003، ص58-61.

(2) عبد المنعم سعيد، إدارة الأزمات والصراعات الدولية، مجلة المنار، العدد 20، باريس، 1986، ص63.

(3) جوانيتا إلياس وبيتر ستش، أساسيات العلاقات الدولية، ترجمة: محي الدين حميدي، إدارة الفرقد، دمشق، 2016، ص18-21.

(4) مهند علي عمران، أثر القوة والقدرة وحرية العمل في الاستراتيجية الشاملة للدولة، رسالة ماجستير غير منشورة، كلية العلوم السياسية، جامعة النهرين، 2003، ص132-134.

حياله سواءً كان ذلك فرصة أم تهديداً[5]. لذا لا غرابة أن يماثل دعاة هذه النظرة، السياسيون وهم يبحثون في قدرات النظام السياسي، لاسيما قدرته التحويلية، نظراً لتماثل الغاية المنشئة لتلك القدرات مع أجناس اختصاصاتها واهتماماتها والخاصة بتحقيق الاستجابة المدركة التي تقتضيها طبيعة الظروف التي يمر بها النظام السياسي[6].

ومهما يكن من أمر، فإن وجهتي النظر أعلاه، وإن اختلف دعاتهما في تحديد مكانة الإدراك في مواجهة متغيرات البيئة المحيطة بالدولة، فإنهما ركزا على حقيقة مهمة للغاية، مفادها إن العقيدة الاستراتيجية تمثل الموجه الأوحد لإدراك ما يمر على الدولة من تهديدات وتحديد كيفية التعامل معها، ذلك الإدراك الذي يعدّ المقترب الأكثر تأثيراً في التحكم بسلوك الدولة رداً/وأداً للتهديدات لاسيما السيبرانية منها[7].

فغالباً ما يغط صنّاع القرار الاستراتيجي في أوهام مفرطة تجعلهم غير قادرين على رؤية مخاطر الواقع، تهديدات وتحديات، أزمات وصراعات، على حقيقتها، ليزيدها تهاونهم في ذلك، استعاراً وسخونة، مع حيرة طاغية في العثور على نمط إدارة ذات جدوى سوى الإدارة بالمخاطر على حد قول (رينولد نيبور) في كتابه سخرية التاريخ الأمريكي الصادر عام 1952[8]. الأمر الذي غالباً ما يفقدهم فرصة ما أسماه البعض بـ(صنع اللحظة التاريخية) التي تستجمع عندها كل المرتكزات العقائدية، لتقدم الدولة، ومن خلفها الشعب، ذاتها كنموذج حي قادر على إدارة الذات، لا كمكون متصارع مع ذاته[9].

وقد تصادفنا ونحن نهّم بقراءة فصول التاريخ السياسي الدولي، انتباهة في غاية الأهمية، غالباً ما تعبر عن نفسها بصيغة تساؤل منطقي، هل بالإمكان قراءة ما حلّ بالنظام السياسي الدولي وما تتعرض له

---

[5] سيوم براون، وهم التحكم: القوة والسياسة الخارجية في القرن الحادي والعشرين، ترجمة: فاضل جتكر، شركة الحوار الثقافي، بيروت، 33-34.

[6] Bert Chapman, Researching National Security and Intelligence Policy, Washington, DC. CQ Press, 2004, p.p.73-75.

[7] Divya Srikanth, Non-Traditional Security Threats in the 21st Century: A review, International Journal of Development and Conflict, No.2, 2014, p.p.63-66.

[8] From: Prabh Karam, National Security, Imperative and Challenges, New Delhi, Tata Mc Graw, 2008, p.p.16-17.

[9] برتران بديع، زمن المذلولين، باثولوجيا العلاقات الدولية، ترجمة: ماجد جيور، المركز العربي للأبحاث والدراسات، بيروت، 2015، ص58.

الدولة (وحدته وشخصه القانوني الأساس)، من دفق المتغيرات التقنية (الثورة المعلوماتية/التكنولوجية)؟[10]، طالما بدت تلك المتغيرات تمثل روافع لفهم الاستراتيجية، صياغة وعقائد، لاسيما وأن صنّاع القرار (سلطة ومنظومات ومنظمات داخلية/دولية)، انكبّوا على التماس فاعلية تلك المتغيرات في تفسير أداء سياساتهم الداخلية والخارجية، تبعاً لما تقدمه من وسائل إدارة وتوجيه وتحكم، ضرورات وإغراءات، ومنها (التحكم الآلي، أو السيبرانية، التي لم يزل الأداء فيها أو مواجهة مخاطرها قائم على أساس الافتراق بين الاستراتيجية كنظام والسياسة كمنظومة[11].

الأمر الذي يفسر لنا حيويتها في التبادل السلوكي بين الاضداد على المستوى الاستراتيجي (نموذج الإرهاب)، والنظام السياسي ومعارضيه على المستوى السياسي (نموذج الاحتجاجات)، وهو ما يجعل صنّاع القرار بحاجة إلى من يحذّرهم من تدافع ضغوط المعطيات السيبرانية حيث التحول والارتداد، وكذلك الانفعالية في استشارة الانتباه للتهديد الواضح أو الخفي، بما يحقق الحاجة للارتكان للعقيدة الاستراتيجية المؤسسّة للبعد الإدراكي والذي يستوعب التهديد أو يحصر استمراره أو استدامته لدى صنّاع القرار، بدلاً من وقوعهم في الاعتقاد المطلق بالتهديد أو ما يسمى بـ(هوام المؤامرة)[12]، المفضي دوماً إلى التركيز (تركيز صنّاع القرار) على العائد الأقصى للمجابهة دون تفعيل المخيلة الايجابية المتجاوزة للانشغال بالتهديد لاسيما الملامس للأمن القومي حيث تواتر الأزمات واستدامة التحديات مثل الاختراقات، واختلال موازين القوى، والجرائم السيبرانية، وتبدل منحنيات الردع، وظهور فواعل من غير الدول، فضلاً عن الاعتداءات السيبرانية (الإلكترونية) في ظل سطوة ما يسمى بـ(الفضاء السيبراني)[13].

---

[10] عن حيثيات ذلك التساؤل ومنطقيته في ظل هيمنة النظام الويستفالي على العلاقات الدولية وحركية قواها، ينظر: هنري كيسنجر، النظام العالمي: تأملات حول طلائع الأمم ومسار التاريخ، ترجمة: فاضل جتكر، الطبعة الأولى، دار الكتاب العربي، بيروت، 2015، ص148 وما بعدها.

[11] عبد الكريم محمود برم، التقنية في الحرب، البعد الإلكتروني، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، 2010، ص36–42. وكذلك ينظر: علاء أبو عامر، العلاقات الدولية: الظاهرة والعلم... الدبلوماسية والاستراتيجية، دار الشروق للنشر والتوزيع، عمان، 2004، ص94 وما بعدها.

[12] عن مضمون هذا المصطلح، ينظر: منعم صاحي العمار، جوف المحنة، اقتفاء أثر الذات العراقية، دار ومكتبة الغفران للطباعة، بغداد، 2016، ص8–9.

[13] عما يعنيه الفضاء السيبراني وما يتضمنه من خطط ومدركات، ينظر:

Peter Long, Hays, Struggling Towards Space Doctrine: U.S Military Space Plans, Programs, and Perspectives during the Cold war, Boston, 1994, p.p.32-41.

وإزاء ذلك، بدت العقيدة الاستراتيجية بمضامينها المتجددة وكأنها مستوعباً لحوافز تترى من أجل إدراك التهديدات السيبرانية ومعادلة زخمها بالتصدي لها ولانعكاساتها، مما يوفر قدرات متجددة تعطي للأداء الاستراتيجي مرونة تتجاوز طبيعة المؤثرات التقنية، وكذلك الحدود الجغرافية لتأثيرها المرصود والمتوقع[14].

كيف يتم ذلك؟، وما هي صور الإفصاح عن مظاهر ذلك الإدراك؟، ما هو أثر العقيدة الاستراتيجية في زيادة مناعة الدولة الأمنية؟، هذا ما سنعمد على مناقشته في المفردات الآتية:

المطلب الثاني : ماهية العقيدة الاستراتيجية

نال مفهوم العقيدة الاستراتيجية اهتماماً كبيراً من لدن الباحثين في علميّ السياسة والاستراتيجية معاً. والسر في ذلك يكمن فيما تؤديه العقيدة من أدوار/مهام. فهي المرجعية المفّسرة للرؤى والأفعال والمبرّرة لديمومتها أو تجاهلها تارة. وهي المرجعية الضابطة للمتغيرات المتوالدة في البيئة، أو المعنية على صياغة القرارات السياسية والاستراتيجية تارة أخرى[15]. لذا ليس من السهولة بمكان اختزالها بدلالات مفاهيمية مجردة أو مقارنتها بمعطياتها الفرعية كالدين والإيديولوجيا السياسية والثقافة الاستراتيجية[16].

ومثلما تشّكل العقيدة مرتكزاً أساسياً في ذات الفرد، تمثل الدليل (المرجعية) الذي تحتكم إليه الدولة في تشكيل رؤاها ومواقفها وسلوكياتها، فضلاً عن القناعات المشكّلة لدى صناع القرار فيها، لذا لا مساومة حول مكانتها، في أية استراتيجية مفترضة، كونها/ الأخيرة تعدّ جزءً من العقيدة طالما التزمت بمهامها حيث الإرشاد والتوجيه والتحكم، لتتحمل العقيدة مهمة التسويق للأهداف والغايات معاً[17].

والعقيدة، اصطلاحاً، مفردة من أصل لاتيني، وتعني النظرية العلمية والفلسفية. مصدرها في اللغة الإنكليزية (Doctrine)، والذي يعني المذهب أو العقيدة[18]، ويماثل هذا التفسير/ الإحالة اللغوية/ ما ورد في اللغة العربية، من كونها مفردة مشتقة من فعل عقد، وهو ما عقد عليه القلب والضمير وما يدين به الإنسان

---

(14) Matt, Hidek, Military Doctrine and Integrated Intelligence in the City, San Fransico, 2007, p.p.11-13.

(15) سعد أبو رية، البيئة النفسية وأثرها في عملية صنع القرار في سياسة الأردن الخارجية، المنظمة العربية للعلوم الإدارية، عمان، 1983، ص13-14.

(16) مفيد نجم، النظام الدولي الجديد وغياب الاستراتيجية والمعايير، مجلة الفكر السياسي، العددان 4-5، اتحاد الكتاب العرب، دمشق، 1999، ص208 وما بعدها.

(17) فضلاً عن تحديد الوسائل الموصلة لها، للمزيد ينظر: هنري كيسنجر، العقيدة الاستراتيجية الأمريكية ودبلوماسية الولايات المتحدة، ترجمة: حازم طالب مشتاق، دار واسط، بغداد، 1987، ص45-46.

(18) فؤاد أفرام البستاني، منجد الطلاب، الطبعة الأولى، مطبعة دار الشروق، بيروت، 1986، ص488-489.

واعتقد، وجمعها عقائد، وأصلها مأخوذ من العقد والربط والشد بقوة أيضاً[19]، وغالباً ما ينحصر إدراك العقيدة واستحضارها بالعقل، لتغدو رديفة الحكمة بكل ما يترشح عنها من رؤى وتوجيهات ودلالات بناء ذات نسغ يقيني لا يتطرق الشك إليه، عندما تكون مولّدة للمواقف لاسيما المبدئية منها[20].

والعقيدة، كمفهوم، تعني مجموعة التعاليم والقيم السامية والمبادئ السياسية والعسكرية والاقتصادية والاجتماعية والعلمية، فضلاً عن المعنوية التي تنبع أو تولد من حضارة الشعب بعد أن ترسخت في وجدانه وضميره، كمنظومة فكرية متكاملة ترتكز على ملاحظة وتفسير الوقائع بقصد توجيه سلوك وعمل قواه ومكوناته، مكونة لهما ذاكرة تاريخية تتضمن المبادئ المبررة والمسوقة لوجودهما وإدارتهما، بما يعين النظم السياسية، المنشئة من قبلهما كإنجاز حضاري وتاريخي، على الاهتداء إلى تبني السياسات الحكومية/الرسمية فيما يتعلق بالشؤون السياسية والعسكرية والاقتصادية، بل والتدابير الاستراتيجية كوعاء شامل لما يسميه البعض بـ(إدارة المصير)[21].

وإزاء ما تقدم، بدت العقيدة، مفهوماً شاملاً وواسعاً، يترآى للدارس والباحث تنوعه نظرياً وأسلوبياً، نظراً لاستطالاته العلمية وفروعه المتعددة كالعقيدة السياسية أو العسكرية...الخ والأهم العقيدة الاستراتيجية[22]. والسر في ذلك إن مفهوم العقيدة يمثل كلاً شاملاً، يأخذ قيمته من ارتباطاته الفلسفية المكونة له حسب نظرية (جشطلت)... النظرية الكلية في الفلسفة، المعّززة بافتراضاتها الحوافز المعنوية لترجمتها واقعياً كنهج أداء مقصود ومعترف به، يصبح فيما بعد وبتراكم انجازاته نموذجاً تعنون به الشعوب والدول، بما يتجاوز الخلط الشائع بينها وبين الإيديولوجيا بعدّهما محتويان فكريان[23].

---

[19] محمد بن مكرم بن منظور، لسان العرب، الجزء الثالث، الطبعة الثانية، دار أحياء التراث العربي، بيروت، 1999، ص196.

[20] فيما يرى البعض، إن ترسخها كمنهج فيقع في الضمير. للمزيد ينظر: منعم صاحي العمار، العقيدة العسكرية العراقية الجديدة: دراسة في نظم تشكيلها، مجلة قضايا سياسية، العددان 23–24، كلية العلوم السياسية، جامعة النهرين، بغداد، 2011، ص3.

[21] عن مجمل تلك المتطلبات والغايات، ينظر الدراسة القيمة الآتية:

HQ Integrated Defence Staff, Understanding Military Doctrine A primer, Directorate of Doctrine Training and Doctrine Divison, Military of Defence, New Delhi, 2018, p.p.3-6.

[22] علاء عبد الحفيظ محمد، النسق السياسي والعقيدي لرجب طيب أردوغان، مجلة رؤية استراتيجية، العدد 3، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، 2013، ص5–6.

[23] عن التعاريف الخاصة بالمعطيين، ينظر: غراهام إيفانز وجيفري نونيهام، قاموس بنغوين للعلاقات الدولية، الطبعة الأولى، مركز الخليج للأبحاث، دبي، 2003، ص321و ص322.

ولا توجد عقيدة استراتيجية جاهزة، بل تتعمد الدول، ورغم قناعة نخب المجتمعية بكونها متغير رمزي، بصياغتها عبر تعبئة جميع قدراتها وإمكاناتها وتوجيهها في خدمة الاستراتيجية العليا للدولة، وإن خضعت لاتجاهات متعددة بقصد معلمتها (Remark) وتأشير أو تحديد مضامينها[24]. فثمة اتجاه يراها بدلالة الإيديولوجية المختزنة بالتفكير الاستراتيجي المؤطر لحركة صانع القرار ونتاجه الموقفي حتى تبدو بنى إدراكية تتوفر عليها الدولة كأساس معرفي وفكري لها وقع كبير في تحديد صانع القرار لخياراته، وهو يسعى لبناء ذاته (قوى وقدرات وحرية عمل)[25]، كما ولها أثر كبير في معلّمة شروط المواجهة للتهديدات، الانتقالية منها أو المستديمة لاسيما تلك التي تتدخل المتغيرات الدولية في بلورتها كتهديدات ذات وقع (أخطار/آثار) استراتيجي شامل، كما في التهديدات السيبرانية[26].

فيما برز اتجاه آخر، رأى دعاته، وهم مأخوذون بضرورة صياغة نص معقول يصلح أن يكون مرجعية حكم للاستراتيجية المراد صياغتها أو تنفيذها على المدى البعيد، إن العقيدة الاستراتيجية هي منظومة فكر وشعور وأداء متجدد يجمعهما اطار شرعي (الهوية/باعتبارها نسق عقيدي) من القيم والمصالح والغايات، الذي يلزم الدولة نظاماً ومؤسسات، الاستنجاد به في صياغتها لأفعالها الاستراتيجية الحاملة لما تسعى إليه من أهداف. عندها تبدو العقيدة الاستراتيجية، النموذج التاريخي الخاص بتسويق الذات، توكيداً لوجودها وتبريراً لسلوكياتها، أو معالجة لما يتعرض له من تهديدات[27]. ومن هنا التمست العقيدة العسكرية مكنون غرضيتها حيث التوجيه والسيطرة والاندفاع، كعملية متكاملة لعنونة الفعل حيال ما يستهدفه منه كأغراض

---

[24] يرد البعض ذلك إلى تدخل القيادة التاريخي في صياغة العقائد. للمزيد ينظر: محمود شيت خطاب، بين العقيدة والقيادة، الطبعة الأولى، دار القلم للطباعة والنشر، دمشق، 1998، ص33 وما بعدها.

[25] لاسيما على الصعيد الخارجي، ينظر: محمد السيد سليم، التحليل السياسي الناصري، دراسة في العقائد والسياسة الخارجية، الطبعة الثانية، مركز دراسات الوحدة العربية، بيروت، 1978، ص27 وما بعدها.

[26] هنا تتدخل الكفاءة والذكاء في بلورة تلك المعلّمة/التحديد بصورة أكبر من رصد التهديدات التقليدية. للمقارنة أنظر الدراسة القيمة بـ: جان بيريه، الذكاء والقيم المعنوية في الحرب، ترجمة: أكرم ديري والمقدم الهيثم الأيوبي، المؤسسة العربية للدراسات والنشر، بيروت، 1981، ص25 وما بعدها.

[27] وسام صالح عبد الحسين، المتغير العقيدي وأثره في انتشار القوة، الجمهورية الإسلامية الإيرانية إنموذجاً، اطروحة دكتوراه غير منشورة، كلية العلوم السياسية، جامعة بغداد، بغداد، 2020، ص9-10.

(أهداف وغايات)، دون التغافل عن المجال المطلوب الذي غالباً ما يستغله القادة في تبرير ابتكارهم وفاعليتهم بل وكفايتهم القيادية أستلهاماً من المكنون التاريخي والإيديولوجي لما يؤمنون به من عقيدة[28].

وهكذا تبدو العقيدة الاستراتيجية منتجة، تجدد ذاتها بذاتها، طالما بدت مستودع الحيوية التي تمتلكها الشعوب والدول. لذا لا غرو أن ينظر لها البعض كمتغير (المتغير العقيدي)، بكل ما يضمه من مقدمات وشروط تفعيل لما تحويه من منظومات متكاملة من العقائد لها مواقفها من المتغيرات البيئية، التي غالباً ما تمثل مقتربات ضامنة لما يسميه البعض بـ(الاستجابة المخطط لها)، خاصة عندما تكون قواعد الأداء محددة بأسلوب ثابت وضامن للمصالح[29].

فإذا ضمنت الدولة صلادة عقيدتها الاستراتيجية، غلب على سلوكياتها (أفعالها) ومواقفها صفة التأثير والانطلاق نحو تعزيز القدرات المستهدفة أساساً، اختزالاً للزمن ودرءاً لأي تأثير أو ضغوط. أما إذا تهاوت الدولة في ذلك، نراها وقد أخضعت نفسها عمداً لهاجس الانسحاق أمام التهديدات التي تولدها البيئتين الداخلية والخارجية وفواعلهما[30]. وهكذا يبدو وجود العقيدة الاستراتيجية أو استحضارها، أمراً حاسماً في مكانة الدولة ودورها بل ووظيفتها ووظيفة نظامها السياسي، سواء على صعد التكيف مع المتغيرات بأنماطها المختلفة (الإيجابي أو السلبي/الإذعاني)، أو على صعيد قيادة التغيير خاصة عندما تبدو العقيدة الاستراتيجية وكأنها عقيدة أدائية للمشاريع التاريخية – الحضارية[31]، كما هو الحال مع (العثمنة الجديدة، وأم القرى، أمركة العالم (السلام الأمريكي)، والسلام الروماني..الخ).

والأهم، كما يرى الكثير من المفكرين الاستراتيجيين، إن العقيدة الاستراتيجية بمقاصدها وانساق الإفصاح عما يجب فعله حيال ما تتعرض له الدولة من تهديدات وتحديات ومشاغل، والأهم ما تطمح إليه من أهداف، تشكل بتواترها مدارات فعل تداؤبية مستمرة، تساهم في بلورة وصياغة نموذج إدراك لما يتوجب

---

[28] للمزيد حول ذلك الالتمساس وتحفز القادة لاستغلاله، ينظر: أندريه بوفر، مدخل إلى الاستراتيجية العسكرية، ترجمة: أكرم ديري والهيثم الأيوبي، الطبعة الأولى، دار الطليعة، بيروت، 1970، ص32 وما بعدها.

[29] عن الاستجابة المخطط لها، كنمط أداء خاضع لرؤية وسطوة العقيدة الاستراتيجية، ينظر: معمر منعم العمار، الدولة واستراتيجية إدارة التغيير، مكتبة السنهوري القانونية، بغداد، 2019، ص248 وما بعدها.

[30] Robert M. Grant, Contemporary Strategy Analysis, New Jersey, John Wiley and Sons Ltd, 2010, p.p.9-11.

[31] أهدافاً وخططاً، للمزيد ينظر: عامر مصباح، نظريات التحليل الاستراتيجي والأمني للعلاقات الدولية، الطبعة الأولى، دار الكتاب الحديث، القاهرة، 2011، ص119 وما بعدها.

فعله أو صياغته من المواقف، لتغدو سلوكيات صناع القرار وكأنها قرارات ناتجة من وحي العقيدة[32]. ولهذا غالباً ما يدعو الجميع، لاسيما في زمن الأزمات والتحديات، إلى اكتساب القدرة (من مصادرها المضمومة والمضمونة) للاستدلال على ما تضمه العقيدة الاستراتيجية والاحتكام لها، باعتبارها عنصراً فاعلاً في منظومة القرار الداخلية للدولة صنعاً واتخاذاً وتنفيذاً، مما يجعلها (العقيدة) ضامنة ليس للأهداف التي ترنو لها الدولة، بل والوسائل التي تتوسل بها لتحقيق تلك الأهداف، تبعاً لما أسماه البعض بـ(التناظر الوسائلي) من جهة أو التماثل الغرضي من جهة أخرى[33].

ونظراً لضخامة المتغيرات الدولية والإقليمية، وحاجة فواعلها إلى نُهج مبدئية كأساس لإدارتها وحيازة العوائد الإيجابية منها لا الابتلاء بكلفها فحسب، أخذت الكثير من الدراسات، مأخوذة بالطبيعة الديناميكية للنظام الدولي، والتعدد/التنوع الكبير في القوى الفاعلة فيه، حساب أثر العقيدة الاستراتيجية من مناظير/عدسات مختلفة، بدءاً من الإدراك كعنصر محاكاة للعقيدة الاستراتيجية وتوأم صناعتها، مروراً بالاستجابة وصناعتها وتسويقها، كحاضنة كشف وتعبير عن تلك العقيدة لاسيما عندما تكون قرارات القادة على وفق مبادئها وما تضمه من تصورات، وانتهاءاً بكونها النموذج المعياري للأفعال الاستراتيجية، الصانعة والمبررة لها (تدفقاً وتوظيفاً واستثماراً)[34].

وإزاء ذلك، لا غرابة أن تبدو مضامين الهداية (الإرشاد) التي تؤسسها العقيدة الاستراتيجية لأفعال الدولة، وكأنها دعوات محققة/حوافز عملية لاستحضار مضامين فكرية أساسية، تتولى القيادات استثمارها/توظيفها أو استدعائها لتغدو وكأنها معطيات واجبة الإحلال، سواءً لبناء القوة الشاملة للدولة (القدرة) أو تكتيل عناصرها لمواجهة التهديدات (الداخلية أو الخارجية) لاسيما السيبرانية منها، عبر صياغة مجموعة فروض عنها واختبار مصداقيتها وصولاً إلى اختبار (البدائل السلوكية) التي تمكّن الدولة ليس لمواجهة التهديدات بل وإيقاف استنزاف وتقليص قدراتها[35]. وهكذا تبدو التهديدات بمناظير الضد وكأنها

---

[32] وصح هذا الكلام حتى مع سياسات التوازن أو بناء التكتلات لاسيما بعد نزاعات الهيمنة الإقليمية أو الدولية، للمزيد ينظر: هاري. آر ياغر، الاستراتيجية ومحترفوا الأمن القومي، التفكير الاستراتيجي وصياغة الاستراتيجية في القرن الحادي والعشرين، الطبعة الأولى، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، 2011، ص17 وما بعدها.

[33] Brian Manthe, United States Military Doctrine and the Conduct of Couaterin- surgency Operation: Fixing the Discannect, From: http://handle.dtic.mil/100-2/APA393508,2001

[34] ويستوي هذا الأمر، عند أي مستوى من مستويات القوة. للمزيد ينظر: جوزيف ناي، مستقبل القوة، ترجمة: أحمد عبد الحميد نافع، المركز القومي للترجمة، القاهرة، 2015، ص28 وما بعدها.

[35] Christopher, P. Twomey, The Military Lens: Doctrine Differences, Misperception, and Deterrence Failure in Sino- American Relations, Massachusetts Institute of Technology, 2005, p.p.21-27.

متغير مؤثر ومنتج لعملية البناء والتأثير الاستراتيجي، عندها لا مراء في القول إن العقيدة الاستراتيجية تجدد نفسها بنفسها كما أسلفنا.

من جانب آخر، تتولى العقيدة العسكرية الإفصاح عن العقيدة الاستراتيجية، عندما تأخذ الأولى على عاتقها تعظيم فائض القوة وتحديد أساليب تعريفه، بل وتعبئة وتوظيف أدوات القوة الوطنية بطريقة متزامنة ومتكاملة لتحقيق أهداف الأمة/الدولة[36]. حتى إذا ما نجحت في ذلك، بدت رافعة للعقيدة الاستراتيجية وعنصر كشف لها، لاسيما وهي التي توفر الدعم الأقصى للاستراتيجية/ السياسية التي تتبناها الدولة في السلم والحرب، دون أن تنال من شمولية العقيدة الاستراتيجية وسموها بل وقدرتها على تحقيق التأثير بين الأهداف والوسائل[37]، أو بين الأهداف والموارد والتي غالباً ما تأخذ بأسباب نجاحها، توسلاً بقدراتها المستهدفة أو بالمتغيرات الدافعة لمضامينها، لاسيما التقنية منها، والتي لم تعد متغيراً ثانوياً كما كان سابقاً، بل غدت عنصر مولد لقابلية التحكم والمحدد الأساس لتخصيص الموارد اللازمة لضبط الأداء الاستراتيجي العام بمسارات متوازية، لطالما بدت العقيدة بذاتها ليست منتجاً نهائياً، كما هي دوماً قيد العمل، صياغة ومراجعة[38].

الأمر الذي يحيلنا إلى أمر في غاية الأهمية حيث دور السياسة (إدارة أمة/شعب/قيادات/مؤسسات) في تأهيل العقيدة الاستراتيجية لكي تكون صنو الإرادة العامة، لا أداة ذاتية محفزة لإرادة القادة فحسب[39]. ولم يكن هذا الأمر ليتحقق لولا تدخل التقنية في تأهيل الشعوب للاستدلال على العقيدة واستحضارها في مواجهة التهديدات التي يتعرض لها الأمن والمصالح الوطنية، خاصة عندما تتجاوز فروض تحقيقهما حركة

---

[36] ليزلي جيلب، قواعد القوة، كيف يمكن للتفكير البديهي انقاذ السياسة الخارجية الأمريكية، ترجمة: كمال السيد، الطبعة الأولى، مطابع الأهرام التجارية، القاهرة، 2013، ص152 وما بعدها.

[37] اندريه بوفر، مدخل إلى الاستراتيجية العسكرية، ترجمة: أكرم ديري وهيثم الأيوبي، الطبعة الثالثة، دار الطليعة للطباعة والنشر، بيروت، 1987، ص19 وما بعدها.

[38] وهذا ما تحقق، بعد أن أثبتت العقائد الاستراتيجية استيعابها للسيبرانية، رؤية وأفعال واستراتيجيات. للمزيد ينظر:
Joseph S. Nye, Cyber Power, Center for Science and International Affairs, Harrard, Kennedy School, 2010, p.p.13-17.

[39] وهذا ما تحقق جلياً في رد الأمريكان على أحداث 11 أيلول 2001، عندما بدت إرادة القادة هي صنو إرادة الشعب الأمريكي في مكافحة الإرهاب (القاعدة).. للمزيد ينظر:
R.S. Mcnamara and J. G. Blight, Wilson's Ghost, Reducing the Risk of Conflict, Killing and Cata Stropke in the Century, New York, Public a Hairs, 2001, p.p. 50-52.

صناع القرار وإدراكهم للمواقف، إلى فاعلية الأداء التي تحتاج إلى تحكم احتمالي فائق القدرة بين العقيدة وصفاتها المحدودة[40].

لهذا لا غرابة أن تبدو السيبرانية، أداة توجيه لسلوك الدولة، تارة مكملة للعقيدة الاستراتيجية، وتارة أخرى وسيلة من وسائل احتوائها[41]. ومن هذه التوليفة، نستكشف سر الخطورة التي تؤسسها التهديدات السيبرانية، ومن ملامحها تقطيع/قطع الاتصال والتواصل بين القابليات والتصورات، الأحكام والآمال، وبما يجعل العقيدة الاستراتيجية وحتى العسكرية، مجرد أفكار يلتمسها القادة وقت تذكرها، وكأنها أمر ثانوي/ترفي[42]. وهذا ما سنعمد على مناقشته لاحقاً.

المبحث الثاني : السيبرانية في علم الاستراتيجية (المنطلقات والتطبيقات) :

سنبين في هذا المبحث مطلبين رئيسين الاول: هو الاصول الفكرية والنظرية لمفهوم السيبرانية والقدرة على استخدام الفضاء السيبراني لخلق مزايا التأثير في الأحداث في جميع البيئات وعبر أدوات القوة والاتصال بالمعلومات الالكترونية مع توضيح انواع التهديدات التي يحتويها ، اما المطلب الثاني: فسنبين التغيير الذي اصاب نمط الردع ضمن نموذج عملياتي حول الحرب السيبرانية وتكوين ضغوطاً هائلة على العقيدة الاستراتيجية باتجاه استيعابها أو التكييف معها، كمرجع ثابت وتحديد للأولويات، وترسيخاً لمعيارية قياس الأداء الاستراتيجي.

المطلب الاول :ماهية الارتباط بين السيبرانية بعلم الاستراتيجية :

لا جدال في أن الاستراتيجية، مهما تعددت التعاريف المحّققة في ما تعنيه، فهي كمعطى، تمثل بناءً إدراكياً قصده الأول (الإرشاد والتوجيه والتحكم)، وكل ما يدخل ضمنها فهو عبارة عن محتوى ومضمون لسيرورة جديدة سرعان ما يظهر بصورة إدراك عيني لما يحفل به الواقع من أحداث... ووقائع، أفعال وأزمات،

---

[40] وهذا الأمر كان له دور كبير في تفوق الاستراتيجية الأمريكية الشاملة، حتى قبل بداية القرن الحادي والعشرين. للمزيد ينظر: بروس دبير كويتز، سوقيات الحرب، استعداد أمريكا لحرب الحاسوب، دراسات استراتيجية، مركز الدراسات الدولية، جامعة بغداد، 1997، ص2 وما بعدها.

[41] كما حصل مع تهديدات تنظيم القاعدة الإرهابي. للمزيد ينظر: صباح عبد الصبور عبد الحي، استخدام القوة الإلكترونية في التفاعلات الدولية، تنظيم القاعدة انموذجاً، نشرة دراسات استراتيجية، المعهد المصري للدراسات السياسية والاستراتيجية، اسطنبول، 2016، ص22–23.

[42] توماس كوبلاند، ثورة المعلومات والأمن القومي، دراسات عالمية، العدد 46، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، 2003، ص88 وما بعدها.

أهداف ومطامح[43]. وتلك الصفة هي من جعلت الاستراتيجية علماً قائماً بذاته لا ينال الشك منه من جراء تدافع موجات التغيير الاستراتيجية. بل هي من خلّصت الاستراتيجية، كعلم من تدافع النماذج التجريدية التي تأتي بها التمثلات العقلية التي تخزن في الذهن على شكل رسيمات، لصالح تحقيق نوع من الديناميكية في صناعة فرضياته وتحليل متغيراته ومراقبة ما تخلص إليه تدابيره وأفعاله من نتائج[44].

إلا أن تلك الصفة، وإن جعلت من علم الاستراتيجية، علماً تركيبياً كعلم السياسة، تبعاً لوحدة المورد لهما حيث (الفلسفة)، إلا أنها رسخت بذات الوقت، قدرة علم الاستراتيجية على استيعاب كل ما يحقق في اشتراطات وجود الدولة، ومنها التحكم، الذي غالباً ما يأتي كحقل متخصص مليء بالتدابير العملياتية التي تهتم تالياً بالرقابة والتوجيه، طالما الاتجاه موجه دوماً لصناعة الأهداف[45]. الأمر الذي يجعل من علم الاستراتيجية ذا مفعول ارتجاعي مهمته خلق اختصاصات جديدة لم تألفها بطون تطوره سابقاً، ومنها البحث في السيبرانية[46].

وهكذا برز لنا اهتماماً علمياً أبان الحرب العالمية الثانية، أطلق عليه بـ(التحكم الآلي) أو (القيادة الأوتوماتيكية)، هدف دعاته ومروجيه (إعادة النظر بفكرة التنظيم الذاتي للفعل الاستراتيجي)، طمعاً في خلق تأسيسات منطقية وشاملة لما يرصف من أهداف، ليبدو ذلك الاهتمام مشروع المستقبل الذي صادف اهتماماً بالغاً من الانثروبولوجيين والمناطقة، وحتى علماء النفس، طالما استهدف ذلك الاهتمام التأثير في إعادة

---

(43) تصلح هذه المقاربة أيضاً، لإدراك تطورات العلاقات الدولية، ومكانة الحروب في ذلك. للمزيد ينظر:
Cyntha Weber, International Relations Theory: a Critical Inteoduction, 3rd, London, Routledge, 2010, p.p.31-41.

(44) لاسيما الحروب. وللمزيد عن ذلك ينظر: روبرت غيلين، الحرب والتغيير في السياسة العالمية، ترجمة: عمر سعيد الأيوبي، الطبعة الأولى، دار الكتاب العربي، بيروت، 2009، ص58 وما بعدها.

(45) غسان مدحت، مدخل إلى الفكر الاستراتيجي، دار الراية للنشر والتوزيع، عمان، 2013، ص20-22.

(46) إيهاب خليفة، القوة الالكترونية، كيف يمكن أن تدير الدول شؤونها في عصر الانترنت، الولايات المتحدة الأمريكية انموذجاً، الطبعة الأولى، العربي للنشر والتوزيع، القاهرة، 2017، ص62 وما بعدها.

معمار الوقائع[47]. لذا لا غرابة أن تكون السيبرانية (التحكم الآلي) هي الحاضنة لما نطلق عليه بالإزاحة الوقائعية للخصوم، والتي وجدت لها مكاناً في علم الاستراتيجية الأعم حيث الحرب[48].

اولاً : السيبرانية كأطار فكري ومفاهيمي :

السيبرانية كمصطلح تعني كل ما يتعلق بالجهد/النتاج الالكتروني من حواسيب وشبكات الانترنت، المعبر عنه بـ(الفضاء السيبراني)، وهو فضاء افتراضي ووهمي، تجريدي وتخيلي بل وتجريبي يخضع للنمذجة، ولكنه ديناميكي تبعاً لما يضمه من تفاعلات الكترونية في فضاء أقل ما يقال عنه أنه معقد ومتغير، تبعاً لملامسة فاعليه للقوة النسبية بأنماطها المختلفة لاسيما في عصر العولمة[49].

وعلى الرغم من وجود الفكرة/المرجعية للسيبرانية حيث التفاعلية في صلب فكرة النظام التي جاء بها علماء السياسة والعلاقات الدولية، إلا أن حوافز تلك الفكرة واستطالاتها لم تخضع لنظام مغلق كما عند (ديفيد آستن)، ولا يستدعي ثباتها تغذية عكسية محددة، لطالما بدت قوى التفاعل فيها قائمة على أساس التواصل الديناميكي/التخيلي وإن كان بدلالات الاختراق[50].

الأمر الذي يجعلنا نقرّ ونعترف بأن السيبرانية ومدلولاتها ليست بجديدة، ولكن الجديد فيها أنها أخضعت لمعطيات ومتبنيات جديدة في القيادة ولوازم ممارستها للمكنّة التي ستتولى عبر تفكيك رموزها وضبطها، توليفها على وفق قيم جديدة لتغدو قوة مضافة، حتى وإن خالفت تلك القيم، ما تستند عليه العقيدة الاستراتيجية. تلك التوليفة التي تُرى بوضوح في تحولات الأداء الاستراتيجي وإن لم تتجاوز منطق الحوسبة/الحوكمة[51]. وهذا ما يجعلها رهن الدوافع لممارستها والغايات التي أجازت تفعيلها، فإن تطابقت

---

[47] جان فرانسوا دورتيه، معجم العلوم الإنسانية، ترجمة: جورج كتورة، الطبعة الأولى، المؤسسة الجامعية للدراسات والنشر والتوزيع، بيروت، 2009، ص207.

[48] Michael Olender, Keeping Pace wkth Cyber Power, Defense and War Fare, Journal of International and Global Studies, No.2, Center for International and Global Studies, Duke University, North Carolina, 2015, p.p.58-59.

[49] عادل عبد الصادق، الفضاء الإلكتروني وتهديدات جديدة للأمن القومي، مجلة السياسة الدولية، العدد 180، مؤسسة الأهرام، القاهرة، 2010، ص104 وما بعدها.

[50] رضوان بروسي، من الدولة الفيبرية إلى الحوكمة كمنظور دولتي جديد، رؤية نقدية، المجلة العربية للعلوم السياسية، العدد 1، مركز دراسات الوحدة العربية، بيروت، ربيع 2013، ص62-63.

[51] هذا ما خلصت إليه معظم المؤسسات/الأوساط الرسمية وغير الرسمية الأمريكية وهي تحلّل اشتراطات قدرتها السيبرانية المستقبلية ومكانتها في خططها الاستراتيجية الشاملة. للمزيد ينظر: ويليام مارسيلينو وميجان ل. سميث وآخرون، رصد

الغايات مع ما تستهدفه الدولة، كان عائد السيبرانية رعاية للدولة وتحقيقاً لذاتها، وإن افترقاً مضموناً وتحقيقاً كانت السيبرانية مؤسسة لعقد أمنية كأداء، تستنزف قدرات الدولة وإمكانياتها، ولهذا عدّ الاتصال والتواصل شرط لازم لكي تتجاوز الدولة ما أسماه علماء الاجتماع بـ(العزلات المدينية) والتي هي صورة من صور إهمال التفاعلية بين الدولة وأندادها[52]. وهذا ما تسوغه السيبرانية وتتجاوزه لصالح زيادة فاعلية الدولة، وإن اقترن ذلك بطفح (العصبية – الدولنة)، أو نرجسية مكوناتها/مجتمعها (الإعجاب بالذات)، تلك الفاعلية التي يعبر عنها، تخصيصاً، بالقوة السيبرانية، التي تنص على كونها، القدرة على استخدام الفضاء السيبراني لخلق مزايا التأثير في الأحداث في جميع البيئات وعبر أدوات القوة، أو هي مجموعة الموارد التي تتعلق بالتحكم والاتصال بالمعلومات الالكترونية والمعلومات المستندة إلى الكومبيوتر والبنية التحتية والشبكات والبرمجيات والمهارات البشرية[53].

ويشير تاريخ العلوم، إن أول اهتمام بهذا الحقل، جاء بعد دراسة العالم الأمريكي واستاذ الميكانيك في معهد (ماساشوتز) للتكنولوجيا (MIT)(نوبرت فينر) (1894–1964)، الذي يعد أول من استخدم كلمة (Cybernetics) (التحكم الآلي) ليشير إلى آلية (فن) القيادة الأوتوماتيكية في أربعينات القرن المنصرم المعتمدة على التحكم والتواصل بين الكائن الحي (الإنسان أو الحيوان) مع الآلة (التي تحولت إلى الحاسوب)[54].

والحق إن (فينر) وهو يؤلف كتابه (السبرنتقية) الصادر عام 1948، لم يدر بخلده إن فكرية ستكون فاتحة لتخصصات علمية تلقي بضلالها على علم الاستراتيجية حيث أثر العلوم المعرفية والرياضيات والذكاء الاصطناعي...الخ، تلك الفكرة التي تلاقاها أساتذة المعهد وطوروها أمثال (فارن ماكولوش، ولورفينغ فون برتالونفي، وجاك.ف.فورستر) وهم علماء الكترونيات، واتخذوا من المنهج النسقي القائم على أساس ثلاثية جديدة حيث (التفاعل، الكلية، المفعول الرجعي)، مرجعية تفسير لمعطيات الأمن....[55]، التي بدت بحاجة

وسائل التواصل الاجتماعي عبر التحليلات لوسائل الدفاع الأمريكية، وسائل التواصل الاجتماعي في المستقبل دعماً لعمليات المعلومات، مؤسسة راند، كاليفورنيا، 2017، ص19 وما بعدها.

[52] جان فرانسوا دورتيه، مصدر سبق ذكره، ص349. وكذلك: بيتر بي سيل، الكون الرقمي: الثورة العالمية في الاتصالات، ترجمة: ضياء وارد، مؤسسة هنداوي سي آي سي، المملكة المتحدة، 2017، ص45 وما بعدها.

[53] John. J. B Sheldon, Deciphering Cyber Power, Strategic Purpose in Peace and war, air University, Strategiy Studies Quartery, 2011, p.p. 91–92.

[54] جان فرانسوا دورتيه، مصدر سبق ذكره، ص207.

[55] نقلاً عن: أميل خوري، صراعات الجيل الخامس، شركة المطبوعات للتوزيع والنشر، بيروت، 2016، ص14–15.

إلى تأطير وصياغة مقتربات إدارة لها مع تنوع ما يتعرض له من تهديدات ومخاطر، ذلك التأطير الذي شكل فيما بعد نظام معلوماتي قائم بذاته[56].

وقد أحدثت هذه الفكرة بكل ما صادفته من اهتمام، هزة معرفية لدى الكثير من علماء الاستراتيجية، وكذلك المهتمين بتاريخية ذلك العلم لاسيما من اللسانيين وعلى رأسهم (نعوم تشومسكي)، الذي عدّ علم الاستراتيجية، في سياق انتقاده لأساتذة معهد (ماساشوتز)، من العلوم التوليدية، لاسيما التي وأن قواعده التركيبية هي قواعد إنتاجية لما يسمى بـ(النموذج البنائي) بالأساس، وأي مخالفة لذلك سيفقد ذرائعيته، كنوع من التعبيرية عن نماذج الفكر بالتصرف، وبعد تعمقه في شروط (السيبرانية) وأطوار تكونها وتطورها، وحفاظها كتقنية على حدود المسافات العينية بين الحقائق والمواقف، جعله يغير رأيه، مسوقاً لها[57]، طالما اعتمدت حقائق مركزية، تأخذ بمهمة توليد الممارسات عبر اختبار التمثلات من جهة، وتختص عبر جزيئات المعرفة وسلمية وسلاسة بالانتقال من الإدراك إلى الوعي، عبر استخلاص منتظمات أوتوماتيكية تتعاطى مع الواقع لا تقف خلفه على حد قول (Gideon Rachman)، أو عبر استحداث معيارية مقننة تضبط ارتجالية ممارسة (فن) القيادة من خلال الموازنة بين الحتمية والحرية[58]، تلم المقاربة التي ابتليت بها السياسة قبل الاستراتيجية كما يقول (رونالد دانروثر) والتي كانت السيبرانية سبباً في فك إشكاليتها عبر تبني معايير قياس، جزء منها لقياس التطور الموازي بين النوايا والإمكانات والقدرة على الفعل، والجزء الآخر محصور في فهم التحليل التزامني للأفكار/الحقائق[59]، ذلك الفهم الذي يرد له فضل اكتشاف ما يعنيه (العمق الاستراتيجي)، والذي مع الأسف، أول من أدركه الإرهابيون، كميدان لتمثيل حركي متعدد ومتنوع المديات[60]. ولهذا لا يخطئ من يرى أثر السيبرانية بعدستين أحدهما لأمة بأثرها المطور لعلم الاستراتيجية، والأخرى المعرفة بأثرها المؤسس لارتباطات فكرية وعملية لذلك العلم سواء أكانت واقعية أم مستقبلية. وهذا ما

---

[56] هذه المقاربة تم التعمق باشتراطاتها تحت مسمى (الأمن السيبراني). للمزيد ينظر:

Kenneth J. Knapp, Cyber Security and Global Information Assurance, Thereat Analysis and Response Solions, 2019, from, online, http://epdf.pub/cyber-security and global-information-sols-9733.htm

[57] نقلاً عن:

Christian Whiton, Smart Power: Between Diplomacy and War, Washington. D.C. Potomac Book-INC, University of Nebraska Press, 2013, p.p.71-78.

[58] Gideon Rachman, Zero-Sum World, Power and Prosperity After the Grash, Atlantic Books, London, 2010, p.p.31-33.

[59] Roland Dannreuther and John Peterson, Security Strategy and Transtlantic Relations, Routledge, New York, 2006, p.26.

[60] غادة نصار، الإرهاب والجريمة الإلكترونية، العربي للنشر والتوزيع، القاهرة، 2017، ص23.

تبدى في البحث المعمق في فرضيات ونظريات الردع السيبراني والأمن السيبراني على حدٍ سواء لماثل الأثنين في الحاجة الماسة للتوافق بين الوسائل والأهداف من جهة، والتركيز على بناء استراتيجيات دفاعية وهجومية في آن معاً[61].

وتلخيصاً لما تقدم، نجد أن السيبرانية ومهما قيل بصددها، هي مفيدة للغاية في حساب ما أسماه البعض بـ(الأفعال المتعاكسة) أو (التفاعلات)، التي تؤسس بتواترها مقدمة واضحة لحقيقة، المواجهة بين خصوم موصوفين، إثباتاً للذات لا بحث عنها أو رسماً لها. وهكذا بدت السيبرانية تتوضح أكثر فأكثر في الاستراتيجية لا في السياسة، لاسيما في الأمن ودالة/وسيلة تحقيقه الحرب[62].

وإذ يرى البعض بتلك المقاربة، ترسيخاً لما يمتاز به علم الاستراتيجية ودراسته من تعقيد موصوف، نظراً لصعوبة فك الاشتباك بين منظوماته ونمذجة انتظاماتها الحركية، لتؤسس السيبرانية تالياً نوع من التنظيم القسري بأطر عقلية، نظراً لقدرتها على إعادة توصيف الوقائع برؤى متعددة، تولد بتواترها ظواهر جديدة حسبها البعض تطوراً ملفتاً لعلم الاستراتيجية ودلالة إثبات على كفاءة القيادة العملياتية للسيبرانية[63].

ورأى (كينيث. ج. ناب)، إن السيبرانية، وإن أنبئتنا بمسيرة فكرية جديدة، فإنها وكجزء من مهمتها الأساس، سعت أدبياتها ودعاتها إلى ترسيخ هدفها الأساس، حيث تذويب المعارف المتفرقة في نظام افتراضي الأبعاد، له القدرة على لملمة الفوضى عن بعد، وإن كان ذلك من دون تمييز بين الذات والنوع[64].

وهذا ما انعكس جلياً، أثراً ودوراً، في ما تلقاه علم الاستخبارات من دفعة قوية لتطور، حتى أصبحت ممكناته عند تكتلها، نمط مستقل من أنماط القوة[65]. والسر في ذلك، إن السيبرانية ساهمت مساهمة كبيرة في تأهيل (الاستخبارات) وجعلها أداة لاستيعاب التحول الذي يشهده الواقع، لا ملاحقة مقارباته السلوكية[66]. لذا

---

[61] عبد الكريم محمود برم، مصدر سبق ذكره، ص48.

[62] نورة شلوش، القرصنة الإلكترونية في الفضاء السيبراني، التهديد المتصاعد من الدول، مجلة مركز بابل للدراسات الإنسانية، العدد 2، بابل، 2018، ص205-207.

[63] Michael Olender, op. cit. p.67-69.

[64] Kenneth, J. Knapp, op. cit.

[65] منعم العمار، من يدين لمن؟، مكانة الاستخبارات في الاستراتيجية الأمريكية الشاملة، الطبعة الأولى، مكتبة الغفران للخدمات الطباعية، بغداد، 2012، ص23.

[66] مارك بيردسول، مستقبل الاستخبارات في القرن الحادي والعشرين، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، 2014، ص19-21.

لا غرابة أن تتغلغل السيبرانية إلى إدارة التحديات والسلوكيات وترسم خرائط الأداء، لا الاكتفاء بتقديم تسهيلات افتراضية أو تكنيكية لصناع القرار أو القادة، نظراً لقدرة معطياتها على التمييز بين خصوصية الحوادث وخصوصية الاستراتيجيات (الخطط) المرصوفة لمعالجة التهديدات. وهذا ما تلمسناه مع بداية القرن الحادي والعشرين، لاسيما عندما بدت خواتيم الاستراتيجيات واضحة المراسي. فالإرهاب، بدا مكشوفاً بعتبات انطلاقه ومآلات أفعاله، كذلك تهديدات الأمن... التي لم تعد ذات صلة بـ(الوظيفة البنيوية) للاستراتيجية، بل بدت جزءاً من حركية مقومات الدولة التي تتولاها أطراف متعددة من بينها السياسة والعسكر وحتى التقنين لترتيب مظاهر متوالدة وجديدة[67]، طالما بدت السيبرانية تعد جزءً من الثورة المعلوماتية أو ما يسميه البعض بـ(انترنت الأشياء).

مقابل كل ما تقدم، برز لنا تيار واسع ومقنع بطروحاته، يعد السيبرانية، حرجاً للاستراتيجية... وممارستها تلويثاً للعقيدة، ما دامت لا تتعدى بوصفها إدارة تقنية للمعلومات، إدارة إيجابية تتمثل بالحماية والأمن، وسلبية حيث الحرب والهجوم والجرائم، ولا يستاهل وجودها للمبادلة مع العقيدة الاستراتيجية، بل هي وسيلة مستحدثة، سيتراكم الغبار عليها في العقود اللاحقة لتصبح جزءً من الماضي، حالها في ذلك حال تكتيكات الحرب السابقة[68].

وبقراءة محققة لحجج هذا التيار، تصادفنا مقاربة في غاية الأهمية، مفادها، إن السيبرانية بقدر ما أعطت في تشكيلها لقوائمها، نظم متعددة في البناء الكلي للأداء الاستراتيجي/السياسي عموماً، فإنها بتواتر قيمها وتطوراتها وتعدد الأقطاب الملتمسة لها، فرضت على صناع القرار أن يكونوا أكثر قدرة على ما أسماه (الكسندر جورج) بـ(الانتباه التلقائي)، طالما بدت جزء من معطيات النظام الدولي التي يستدعي التعامل معها بنوع من المرونة والالتزام والاحتكام للتعاقب في الوقائع، بدلاً من اندفاعهم نحو المعتقدات الوسائلية على حساب مثيلتها الفلسفية في ظل ما أسماه (جاك ليفي) بالتناقض في فهم الواقع المؤسس لحقائق الانحراف المعياري في معالجة المعلومات التي تأتي بها قوانين السيبرانية (التحكم) ليغدو صناع القرار فاقدي الثقة بالنفس أو لديهم تعسفاً في الافصاح (النرجسية)، وفي كلا الحالتين، تبدو السيبرانية مصدر أغواء وتمرد لهم[69].

---

[67] بيرت تشايمان، العقيدة العسكرية – دليل مرجعي، ترجمة: طلعت الشايب، الطبعة الأولى، المركز القومي للترجمة، القاهرة، 2015، ص182 وما بعدها.

[68] ديفيد جي. بيتز وتيم ستيفنز، الفضاء السيبراني، نحو استراتيجية للقوة السيبرانية، دلفي للأمن السيبراني والدراسات الاستراتيجية، لندن، 2006، ص15.

[69] جان فرانسوا دورتيه، مصدر سبق ذكره، ص348.

من جانب آخر، جاء الحث للاهتمام بالسيبرانية لاسيما في العقد الثاني من القرن الحادي والعشرين، معززاً بإرادة الحفاظ على الإلهام في التخطيط والأداء الاستراتيجيين لفضح انحرافات لعبة الأمم التي أديرت فصولها بعد انتهاء الحرب الباردة بانحرافات دوغمائية واضحة، وهو ما جعل الدول تنازع أمرها في الاستدلال على الدرب الأسلم لتجاوزها ما يسمى بـ(الوهم الوضعي) الذي بدأت تعاني منه لاسيما بعد تصاعد حدة الإرهاب كجزء من تواتر التحديات التي وإن كانت صغيرة[70]، فإن تأثيرها غالباً ما يمس الأمن في الصميم تبعاً لانتشار (نظرية الآثار–أثر الفرشة) تداعياته (تداعيات الإرهاب) وملامستها للغايات الاستراتيجية التي تحرص الدولة على حيازتها عبر الأداء الحاذق الذي يهدف إلى التحرر من القيود، لتأتي السيبرانية لتزيد ذلك الأداء والقائمين عليه وهماً[71].

فالعقل التواصلي لحد هذه اللحظة، وإن خلق تطوراً أساسياً من أجل التفكر بقراءة التحديات وما يؤسسه من نقاش، إلا أنه يزيد من حدة الانشغال بما أسماه البعض بـ(الشمولية المجردة) والتي تركز على الكلية في قراءة التهديد لا على علاجه، لأن استيعاب التهديد وعلاجه والقيام بأفعال أخرى... ليس من السيبرانية بشيء. فالأخيرة تصنع دوماً الاضطراب وتجعل الحيلة التي يتلقاها من الآخر، مجرد زرع لصور الاضطراب في المدرك لصالح الغموض الموقفي الذي يخشى أصحابه البوح به تبعاً لغموضه وتمدد تداعياته[72]. وهكذا صنعت السيبرانية لذاتها مكانة عبر ما تقدمه من تهديدات تلامس الأمن، كمعطى شامل يوازي ببناءه الفضاء السيبراني، لا عبر ما تقدمه من ممكنات تفعيل تقليدية للأداء[73]. وهذا ما سنراه في تحقيقنا في مضمون الأمن السيبراني وما يتعرض له من تهديدات حققت أثراً مركباً، في صياغة العقيدة الاستراتيجية من جهة، وفي تغيير نمطي الردع والحرب معاً. الأمر الذي يجعل تلك العقيدة أمام محنة تجديد ذاتها. وهذا ما سنناقشه تباعاً.

---

[70] أميل خوري، مصدر سبق ذكره، ص9.

[71] محمد قيراط، استراتيجية وطنية للأمن السيبراني، موقع الشرق للإدارة الإلكترونية، 2008، شبكة المعلومات الدولية، على الرابط:

http://al-sharq.com

[72] جوزيف ناي، كيف يتم تطوير معايير جديدة للأمن السيبراني، شبكة النبأ للمعلوماتية، 2018، على الرابط:

http://annabaa.org

[73] يرد البعض سر ذلك النجاح إلى معطيات متعددة جاءت بها الثورة المعرفية. للمزيد ينظر:

Marcos Degant, Spies and Policy Makers, Intelligence in the Information Age, Intelligence and National Security, No.4, 2016, p.p.511-513.

ثانياً : مهددات الأمن السيبراني :

لقد حققت موجات التغيير الدولية المتوالية التي شهدها النظام الدولي، بوابات مراجعة إدراكية لمستدعيات الأمن وغاياته، تلك البوابات التي بقدر ما حكمت الافتراضات الدولية السائدة، نظرياً وعملياً، فإنها أنضجت صور ما يفصح عنه الأمن من رؤى وأفكار وعتبات أداء ساهمت في تحليل وتصويب الكثير من الرؤى السائدة في حقلي العلاقات الدولية والاستراتيجية[74].

وقد كان من نتائج ذلك النضج، أن أخذت ظاهرة الأمن مداها، لتغدو العنصر الأكثر تأثيراً في شكل العلاقات الدولية ومن ثم هيكلية النظام الدولي، لاسيما بعد تعدد فواعله وتنوع وتمدد غاياتها. إذ لم يعد سلوك الدولة وحدها، المتحكم في توصيف حالة الأمن من عدمها، بناء أو اختلالاً، بل بدت الفواعل من غير الدول تبحث عن أداء أدوار مؤثرة في صياغة الأمن، ليغدو الأخير بتدابيره وكأنه استراتيجية قائمة بذاتها لا حاملاً لاستراتيجية الدولة فحسب[75].

وقد سهلت المقاربة أعلاه، من تدخل العقيدة الاستراتيجية في صياغة الأمن المستهدف، متخذة من القدرة مصدراً لها لشرعنة أهدافه وتسويقها، الأمر الذي جعل الإدراك به يتقدم على مختلف متطلبات العقيدة ومستدعياتها كمرجعية منظمة لمصادر القوة وسياساتها[76]. والسر في ذلك يكمن بأن الأمن لم يعد رهيناً أو حصيلة لمصادر القوة، بل حصيلة للقدرات المملوكة، حتى إذا ما صادفت تلك القدرات منظومات توظيف موحدة لمجابهة ما تتعرض له من تهديدات، بدت الهوة الحاصلة في المدركات الأمنية منحسرة وغير ذات بال، لاسيما غير المنظورة من تلك التهديدات[77]، والتي ساهمت ثورة الاتصال والمعلوماتية في تواترها، مثل

---

[74] منعم صاحي العمار، الأمن الدولي وبوابات الإدراك العشرة، مجلة قضايا سياسية، العدد 59، 2019، ص46-47.

[75] عن تلك الرؤى ينظر: موسى الزعبي، الجيوسياسية والعلاقات الدولية، أبحاث في الجيوسياسية وفي الشؤون والعلاقات الدولية المتنوعة، وزارة الثقافة، دمشق، ص168 وما بعدها.

[76] يربط البعض ذلك بالتحفز العالمي مع نهاية الحرب الباردة لشرعنة الحروب التي تخوضها القوى الدولية والإقليمية، رغم الهيمنة الأمريكية حينئذ، طالما بدت تلك الحروب تدار بمكنونات القدرة لا القوة فحسب. للمزيد ينظر: جيمس لي دي، الحروب في العالم: الاتجاهات العالمية ومستقبل الشرق الأوسط، الطبعة الأولى، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، 1998، ص35 وما بعدها.

[77] وهذا ما حصل بالضبط بعد أحداث 11 أيلول عام 2001، وسعي المحافظين الجدد لجعل نشر الديمقراطية في الخارج شاغلاً من شواغل الأمن القومي الأمريكي لاسيما إبان فترتي رئاسة (بوش الأبن). للمزيد ينظر: توني سميث، حلف مع الشيطان، سعي واشنطن لسيادة العالم وخيانة الوعد الأمريكي، ترجمة: هشام عبد الله، المؤسسة العربية للدراسات والنشر، بيروت، 2010، ص104.

الهجمات السيبرانية (الالكترونية) والإرهاب السيبراني، والجرائم السيبرانية (كالتجسس والاحتيال والسرقة) وصولاً إلى الحرب السيبرانية... متخذة من البرمجيات الخبيثة أسلحة لها، التي استدعت مجابهتها تبني منظومات أمن متخصصة، أطلق عليها (الأمن السيبراني)[78]، الذي يتخذ من الفضاء السيبراني مجالاً له، وليغدو بعداً جديداً ضمن أجندة حقل الدراسات الأمنية، بعداً يسهم بمجابهة التهديدات اللامتماثلة أو اللاتناظرية العابرة للحدود والتي لا تعترف بالسيادة الوطنية أو فكرة الدولة القومية، رغم إقرار مدارسه ونظرياته المنشئة بمهمة الدفاع والبحث عن التدابير المضادة لتلك التهديدات[79]. الأمر الذي ينبئ بضرورة التحفز لمجابهة مخاطر تآكل الردع التقليدي، بل والتحفز لإعادة التفكير فيما نقصده بـ(الأمن القومي للدولة)[80].

والأمن السيبراني، كما عرفته وزارة الدفاع الأمريكية (البنتاغون)، هو (جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والالكترونية عن مختلف الجرائم: الهجمات، التخريب، والحوادث (القرصنة وغيرها)[81]، ليغدو فيما يشمله أوسع من أمن المعلومات الذي تختص معطياته وموجبات تحقيقه، منع وصول المعلومات الأمنية إلى أيدي أشخاص غير مخولين بها عبر الاتصالات[82].

ولم يكن الأمن السيبراني ليصادف وصفه الحالي، دون تاريخ طويل من التخمينات حول دور التكنولوجيا الرقمية في الدراسات الأمنية، ذلك التاريخ الذي جاءت به ابتداءاً مدرسة (كوبنهاكن) التي تجاوزت رؤاها النظرة الضيقة المتمركزة حول الدولة لصالح تبني مشروع (الأمننة) دون إهمال الاختبارات النظرية والأخلاقية بشأن المخاوف المتعلقة بالأمن السيبراني[83]. ذلك المشروع بقدر ما يؤسس تحرراً من المخاطر

---

[78] سين إس كوستجان، الأمن السيبراني، منهج رجعي عام، مركز جورج كاتليت مارشال الأوروبي للدراسات الأمنية، بروكسل، 2012، ص17 وما بعدها.

[79] جوزيف ناي، الردع في الفضاء الإلكتروني، المركز العربي لأبحاث الفضاء الإلكتروني، الدوحة، 2019، ص18 وما بعدها.

[80] عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، سلسلة أوراق، العدد 3، وحدة الدراسات المستقبلية، الإسكندرية، مصر، 2016، ص62-63.

[81] الموسوعة السياسية، الأمن السيبراني، شبكة المعلومات الدولية، على الرابط:

http://political-encyclopedia.org

[82] إيهاب خليفة، القوة الإلكترونية: كيف يمكن أن تدير الدولة شؤونها في عصر الانترنت، الولايات المتحدة إنموذجاً، العربي للنشر والتوزيع، القاهرة، 2017، ص35 وما بعدها.

[83] عن رؤى هذه المدرسة، ينظر: الموسوعة الجزائرية للدراسات السياسية والاستراتيجية، التصور الأمني لمدرسة كوبنهاكن، دراسات أمنية، حزيران 2019، شبكة المعلومات الدولية، على الرابط:

والأضرار الناتجة عن إساءة استخدام تكنولوجيا المعلومات والاتصالات أو قصدية استخدامها في الهجوم، فإنه يؤسس التفاتة مهمة لبداية حرب جديدة في الحروب الألكترونية (السيبرانية)، بكل ما تضمه من فواعل وأبعاد ودرجات عالية من التغيير والترابط وسرعة التفاعل بين فصولها ووقائعها، خاصة في ظل تعدد الفواعل غير الدول (الشركات التكنولوجية العابرة للحدود، شبكات الجريمة، القرصنة الالكترونية، الجماعات الإرهابية) والتي يفرض وجودها تحديات كبيرة للأمن السيبراني العالمي، من أهمها[84]: ارتباك مدركات الدفاع، وتعدد اتجاهات التصدي بل واختلاف التنسيق بين الأطراف المعنية بالدفاع، فضلاً عن تواتر تهديدات جديدة نشأت بسبب الديناميكيات التكنولوجية التي غيرت قواعد ونظم الاشتباك، مستحدثة معايير ونظم إجرائية لإدارتها على مختلف الصعد/الأبعاد، والتي أشار إليها دليل الأمن السيبراني العالمي (GCI–global Cyber Sscurity) الذي يقيس مستوى التزام الدول المختلفة بالأمن السيبراني عبر خمسة ركائز أساسية (القانون، التقنية، التنظيم، بناء القدرات، التعاون)[85]، عدت لاحقاً أدوات تسهم في تهيئة الحلول الأمنية في الفضاء السيبراني، علاوة على استدامة واستقامة البيانات ومعالجة الخدمات، بما يوفر الجهود لوقايتها من أي تلاعب أو تعديلات عارضة، أو تهديدات قادمة من عبر الحدود، والتي غالباً ما تكون ذا قدرة تخريبية عالية وانتشار سريع ومديات تأثير جيو–سياسية واسعة[86]. الأمر الذي يستلزم التصدي لها، قدرات دفاعية غير محدودة، لاسيما إذا ما جاءت عن فواعل/جهات معروفة بامتلاكها لمهارات تنفيذ/أداء عالية يصعب على المدافع، إدارة الصراع بمفرده من دون مساعدة/تحالف من/مع الآخرين[87].

ولم يكتف الأمن السيبراني بالتدابير الخاصة بحفظ أمن المعلومات، بل وتحاول بناه وأدواته ترجمة السياسات العامة إلى تدابير تنفيذية تساهم بدرجة أو بأخرى في الحد من العديد من المشكلات الأمنية، كتلك

---

http://www.politics-dz-com

[84] عباس بدران، الحروب الإلكترونية: الاشتباك في عالم المعلومات، مركز دراسات الحكومة الإلكترونية، بيروت، 2010، ص51–63.

[85] علم الدين بانقا، مخاطر الهجمات الإلكترونية (السيبرانية) وآثارها الاقتصادية، دراسة حالة مجلس التعاون الخليجي، سلسلة دراسات تنموية، العدد 63، المعهد العربي للتخطيط، الكويت، 2019، ص32.

[86] عن تلك الحلول، وأهمية النظرة إليها كرزمة وليس فرادى، ينظر: أوس مجيد غالب العوادي، الأمن المعلوماتي السيبراني، مركز البيان للدراسات والتخطيط، بغداد، 2016، ص7 وما بعدها.

[87] نسرين الصباحي، الحروب السيبرانية وتحديات الأمن العالمي، المركز العربي للبحوث والدراسات، شبكة المعلومات الدولية، على الرابط:

http://www.acrseg.org/40594

الحاصلة في الخدمات العامة وخدمات نظم المعلومات ودورها في تأهيل الأداء الحكومي في مفاصله/أبعاده المهمة مثل العسكرية والسياسية والاقتصادية والاجتماعية، فضلاً عن القانونية[88]، من خلال ردع:

1. الجريمة السيبرانية (الالكترونية)

على الرغم من قدم هذه الجرائم وتعدد أنماطها، والاعتراف بعدم قانونية (تجريم) ما تضمه من أفعال، وجدارة مرتكبيها لتلقي العقاب، ظل اطار فعلها حبيس الحواسيب وأنظمة المعلومات، مثلما ظلت أهدافها واضحة حيث التربح، القرصنة، التخريب بهدف تحميل الخصوم خسائر باهظة وبأقل الكلف[89].

وإزاء ذلك لا غرو من عدّ تلك الجرائم أشكال سلوك قصدية غير مشروعة وضارة بالمجتمع ترتكب باستخدام الحاسب الآلي[90]، أو هي مجموعة الأفعال الضارة وغير القانونية (طالما تتحدى السرية والنزاهة) والتي تتم عبر معدات/أجهزة الكترونية أو شبكة الانترنت تبث عبرها محتوياتها، بقصد لحاق الأضرار في نظم تكنولوجيا المعلومات والاتصالات والبيانات التي تحويها من أجل تحقيق مكاسب مادية أو خدمية (سرقة المعلومات واختراق الحسابات البنكية وتحويل أصولها)، أو أهداف استراتيجية أو سياسية والأهم عسكرية حيث: التجسس لسرقة المعلومات الأمنية أو جرائم التضليل التي تقوم بها المجاميع الإرهابية لإحداث الفوضى وعدم الاستقرار عبر الشائعات أو الأخبار المفبركة[91].

---

[88] عشور عبد الكريم، دور الحكم الإلكتروني في مكافحة الفساد الإداري، الولايات المتحدة الأمريكية انموذجاً، مجلة المفكر، العدد 11، جامعة محمد خيضر–بسكرة، الجزائر، 2019، ص466 وما بعدها. وعن علاقة ذلك وأثره على الدبلوماسية الإلكترونية، ينظر: فرانز ستيفن وغرين أوستن، روسيا والولايات المتحدة: الدبلوماسية الإلكترونية الطريق لفتح الأبواب، ترجمة: طارق ذنون، اكاديميون للنشر والتوزيع، عمان، 2015، ص59 وما بعدها.

[89] أمير فرج يوسف، الجرائم المعلوماتية على شبكة الانترنت، دار المطبوعات الجامعية، الإسكندرية، 2008، ص18 وما بعدها.

[90] ليلى الجنابي، فعالية القوانين الوطنية والدولية في مكافحة الجرائم السيبرانية، الحوار المتمدن، العدد 4634 في 2017/9/8، شبكة المعلومات الدولية، على الرابط:

http://www.ahewar.org

[91] اسراء جبريل رشاد مرعي، الجرائم الإلكترونية، الأهداف والأسباب وطرق المعالجة، المركز الديمقراطي العربي للدراسات الاستراتيجية والاقتصادية، برلين، 2016، شبكة المعلومات الدولية، على الرابط:

http://democraticac.de/?p=35426

وتبعاً لفداحة الأضرار التي تسببها تلك الجرائم، والتي تعد من أخطر التهديدات السيبرانية[92]، أخذت بعض الدول بالتحالف فيما بينها للتصدي لهذه الجرائم، ففي عام 1946 تم توقيع اتفاقية (بارسا) بين كل من (استراليا ونيوزلندا وكندا والمملكة المتحدة والولايات المتحدة الأمريكية)، لتتطور فيما بعد إلى تحالف (خمس عيون)، لم ينفرط عقده إلا عام 2017 عندما رفعت الولايات المتحدة الأمريكية الخصوصية الدولية عن حرية المعلومات بسبب عدم التزام دول التحالف بقانون حرية المعلومات، ورفعت دعوى قضائية ضد حلفائها الأربعة[93].

كما وتوجد هناك اتفاقية مجلس أوروبا الخاصة بالتصدي للجرائم السيبرانية الموقعة في تشرين الأول/أكتوبر عام 2001، والتي دخلت حيز التنفيذ في تموز/يوليو عام 2004. كما هناك دليل برلين، وهو عبارة عن صك قانوني دولي عدّه مجموعة من خبراء القانون الدولي بدعوة من حلف الناتو عام 2013 على أثر تداعيات الهجوم السيبراني الروسي على أستونيا عام 2007، متضمنة التهديد بتدمير أهداف عسكرية وبنى تحتية مدنية[94]. كما عمدت الكثير من الدول لاسيما الولايات المتحدة الأمريكية إلى مراقبة حدوث تلك الجرائم عبر وسائل الاتصال الاجتماعي، كما حصل مع جريمة قتل الشرطي الأمريكي (جورج فلويد) أيام حكم الرئيس (دونالد ترامب)[*].

---

[92] زادت خطورة تلك الجرائم بعد ظهور الإرهاب كتحدٍ عالمي، للمزيد ينظر: ناجي ملاعب، الأمن السيبراني، تعريف الجرائم السيبرانية وتطورها، موقع الأمن والدفاع العربي، شبكة المعلومات الدولية، على الرابط:

http://sdarabia.com

[93] Joe Carter, What you Should Know about the (five eyes) Intelligence Community Providence, Journal of christnty and American Foreign Policy, on line, http://www.providence Nag.com

[94] سليم دحماني، أثر التهديدات السيبرانية على الأمن القومي، الولايات المتحدة الأمريكية انموذجاً 2001-2017، رسالة ماجستير غير منشورة، كلية الحقوق والعلوم السياسية، جامعة محمد ضياف، الجزائر، 2018، ص55 وما بعدها.

[*] جورج فلويد، مواطن أمريكي من أصل أفريقي توفي في 25 أيار 2020 في مدينة مينابوس مينيسوتا في الولايات المتحدة الأمريكية، بعد تثبيته في الأرض من قبل شرطة المدينة لغرض اعتقاله. تلك الطريقة التي أثارت احتجاجات غير مسبوقة أردفت بأعمال شغب وحرق وتدمير. للمزيد ينظر: ياسر محجوب الحسين، مقتل فلويد وفرص إعادة انتخاب ترامب، قناة العربي 21، 10/ حزيران/2020، شبكة المعلومات الدولية، على الرابط:

http://arabi21.com/story/2177452/%09

2. الإرهاب السيبراني (الإلكتروني).

وهو جريمة من جرائم الإرهاب، يستغل مرتكبوها من الأفراد والجماعات الفضاء السيبراني للقيام بعمليات التجنيد والتعبئة والدعاية وجمع الأموال والمتطوعين، فضلاً عن جمع المعلومات حول الأهداف العسكرية (مخازن أسلحة، تجمعات الأفراد، مراكز تدريب، منشآت البنية التحتية للدولة، بقصد إنتاج عنف أو تدمير أو بث الخوف، فضلاً عن تحقيق أجندة سياسية أو اجتماعية أو فكرية معينة[95]، أو هو كل هجوم مخطط له بدافع سياسي ضد المعلومات وأنظمة الحاسوب الآلي وبرامجه وبياناته، مما يؤدي إلى العنف ضد أهداف غير حربية من قبل مجموعات وطنية فرعية أو عملاء[96].

ونظراً لخطورة الجريمة، سميّ فاعلوها بـ(الجماعات/التنظيمات العنفية) التي لا تنتمي لأجهزة الدولة الرسمية، مثل الحركات الراديكالية والجماعات والأصولية التي تأخذ على عاتقها تهديد الحكومات أو العدوان عليها سعياً لأهداف سياسية أو دينية أو إيديولولوجية، بكل ما يؤسسه تحقيق تلك الأهداف من آثار مدمرة تعد مكافئة للآثار المادية وغير المادية التي تخلفها الأفعال الإرهابية[97].

وإذ يرى البعض إن مصطلح (الإرهاب السيبراني)، جاء من الالتقاء بين الفضاء السيبراني والإرهاب، دالاً على وجود خرق قانوني (فردي أو جماعي) ناتج عن هذا الالتقاء، مستهدفاً إثارة الأضرار الخطيرة في النظام العام عن طريق وسائل الاتصال وأنظمة المعلومات[98]، لاسيما في ظل غياب الرقابة على تلك الوسائل/الأنظمة، وصعوبة الإثبات/الدليل المادي على ما ترتكبه تلك الجماعات المنبثة عبر العالم/عابرة للقارات) من جرائم إرهابية التي غالباً ما تكون سهلة لا تتطلب سوى المعرفة لاختراق الحواجز الالكترونية فقط[99]، كما حصل بأحداث 11 أيلول/سبتمبر عام 2001 والنتاجات العلمية لدراعش الإرهابي بعد عام 2014، مثل (صليل الصوارم)، و(فجر البشاير) وغيرها والتي اتخذت من (غوغل) منصة عرض لها[100].

---

[95] عادل عبد الصادق، الإرهاب الإلكتروني، القوة في العلاقات الدولية، نمط جديد وتحديات، مركز الأهرام للدراسات السياسية والاستراتيجية، القاهرة، 2019، ص107.

[96] أوشينا جيروم أورجي، ردع الإرهاب السيبراني في مجتمع المعلومات العالمي، قضية المسؤولية الجماعية للدول، مراجعة الدفاع عن الإرهاب، العدد 1، 2004، ص31.

[97] Mitko Bogdnoski & Drage Petreski, Cyber Terrorism – Global Security Threat, International Scientific defense, Security and Peace Journal, No.3, 2014, p.p.54-60.

[98] بهاء عدنان السعيري وعماد عبد خضير الزرفي، انتقال التهديدات من الواقع إلى العالم الافتراضي، مجلة جامعة بابل للعلوم الإنسانية، العدد 4، بابل، 2019، ص88 وما بعدها.

[99] عن جدلية تلك العلاقة ومظاهر اثبات صلادتها، ينظر:

ومنذ عام 2007، بدأت الدول وبالتعاون مع بعضها البعض، للتصدي لجرائم الإرهاب السيبراني، كما حصل مع التعاون المصري – الأمريكي للقبض على الجماعات التي ارتكبت جرائم الإرهاب السيبراني على البنوك (Wels Fargs, AOL) الأمريكية كجزء من التعاون الأمريكي – الشرق أوسطي[101]، والجهد الأمريكي الخاص لملاحقة الجماعات الإرهابية في جورجيا لاستغلال مواقع القمار الافتراضية على الانترنت للإضرار بالاقتصاد العالمي، بعد أن تسللت إلى الأنظمة الخاصة بالمعلومات تحت مسميات متعددة. وبذات الطريقة لم يزل الإرهابيون يتسللون لمنظومات المعلومات بقصد انتهاك الأمن القومي للدولة، مستغلة ما توفره شبكات الانترنت من خدمات عبر العناوين الالكترونية وما يسمى بـ(غرف الدردشة)، الدعاية، نشر الأفكار، والأهم تجنيد عناصر جديدة وجمع التبرعات وربما وضع الخطط[102].

المطلب الثاني :الأمن السيبراني وتغير نمط الردع... (الحرب السيبرانية إنموذجاً)

ومما يزيد من خطورة التهديدات السيبرانية، التغيير الذي رتبه الفضاء السيبراني على أنماط وأساليب الردع وجدواه حيال تلك التهديدات بكل ما تفرزه من آثار مضاعفة لاسيما في الاطار العسكري، نظراً لما تبدو عليه القدرات العسكرية من أوضاع تخضع بكامل بنائها لخاصية البحث عن الميزة النسبية مادية أم معنوية[103]. وهذا ما يفسر لنا مناوبة الأفعال الإرهابية بين الأهداف المدنية والأهداف العسكرية، إخواءً لتلك القدرات من تأثيرها وترسيخاً لمظاهر الحرب (النفسية السيبرانية)، الأمر الذي يجعل المستهدف غير قادر تحت هول الصدمة والمباغتة، الرد عليها لهلامية الفاعل من جهة، ولصعوبة إعادة مصداقية الدفاع لا القدرة على الانتقام فحسب[104]. وهو ما جعل الكثير من الدراسات الأمنية، تبشر بضرورة تبني نمط/مستوى جديد

Abrahan Wagner Intelligence for Counter?. Terrorism: Technology and Methods, Journal of Policing, Intelligence and Counter Terrorism, No.3, 2011, p.p.51-56.

[100] حسنين توفيق إبراهيم، التنظيمات الجهادية الإرهابية وشبكات التواصل الاجتماعي، داعش انموذجاً، كراسات استراتيجية، العدد 268، مركز الأهرام للدراسات السياسية والاستراتيجية، القاهرة، 2016، ص24 وما بعدها.

[101] حميد حمد السعدون، استخدام الفضاء السيبراني وتأثيره في العلاقات الدولية، الشرق الأوسط انموذجاً، مجلة دراسات دولية، العدد 59، جامعة بغداد، 2018، ص10 وما بعدها.

[102] شريف درويش اللبان، تكنولوجيا المعلومات والعلاقات الاجتماعية/دراسة في أخلاقيات العصر الإلكتروني: الاتجاهات الحديثة في المكتبات والمعلومات، العدد 13، المكتبة الأكاديمية، القاهرة، 2000، ص16–19.

[103] للمزيد عن هذه التغييرات، ينظر:

Adam Lowther, ed, Deterrence: Vising Powers, Rogne Regime, and Terrorism in the Twenty-First Century, New York, 2012, p.p.91-93.

[104] عبد الغفار الديواني، القرن السيبراني، الردع الإلكتروني بين المنع والانتقام، نظرية الردع في القرن السيبراني، المعهد الألماني للشؤون الأمنية والدولية، برلين، العدد 15، ص13–16. وكذلك: عبد الباسط محمد أبو ناموس، الحرب النفسية التي

من التفكير يتجاوز النظرة الضيقة المتمركزة حول الدولة والتي تجعل من الأمن، كمعطى/مفهوم تقليدي، إلى ما يسميه البعض بـ(الهندسة الاستباقية) للقدرات وتفعيل سبل توظيفها واستخدامها في الفضاء الافتراضي القائم على أساس التفوق التكنولوجي[105]، ذلك التفعيل الذي يبدو للوهلة الأولى صورة من صور التهديدات، إلا أنه ما يلبث أن يكشف عن نفسه كأسلوب جديد للردع، حسبه البعض مستودعاً لتدشين سباق تسلح سيبراني[106].

ذلك الأسلوب الذي يعتمد على التداوبية (الاستمرار المقصود) في طرح أطر أداء/تعامل جديدة لتوزيع وانتشار القوة بين أكثر من فاعل، بما يؤسس دروب بناء وتصريف لعلاقات القوة خارج اطار المدرك[107]، أو كما يصفه (ديموند سيجل) بأنه سلوك مركب لمجموعة من الفاعلين السيبرانيين، يجمعهم عنوان واحد يمارسون عبر وظيفة الردع عبر استراتيجية (التماثل الغرضي)، ليؤسسوا تالياً عصراً جديداً من الجيوبوليتيك في الفضاء لا في الأرض، رغم انتهاكهم لحدود السيادة واشتراطاتها[108]. وقد كان لطبيعة الفضاء السيبراني وتشكله التفاعلي المتواصل بين مجموعة من الأنظمة والبرمجيات والأجهزة الرقمية، فضلاً عن المستخدمين (مشتغلين وزبائن)، ليغدو ذراعاً رابعة للجيوش الحديثة، أثر كبير في ما لاح التهديدات السيبرانية من تطور أكبر من تطور قدرة المجابهين (القدرة العالمية) على التعامل معها. كما وله أثر كبير في توسيع مساحات ومديات وأنماط ما يسمى بـ(الصراع السيبراني)، من دون وجود لضمانات أمنية لاحتواء مخاطره[109].

استخدمتها المقاومة الفلسطينية في مواجهة العدوان الإسرائيلي على غزة عام 2014، رسالة ماجستير غير منشورة، أكاديمية الإدارة والسياسات للدراسات العليا، فلسطين، 2015، ص33 وما بعدها.

[105] بن ضيف الله بلقاسم، القوة الذكية في الفكر الاستراتيجي الأمريكي المعاصر، مجلة المستقبل العربي، العدد 483، مركز دراسات الوحدة العربية، بيروت، 2019، ص9 وما بعدها.

[106] خالد حنفي علي، إشكاليات تداخل الصراعات السيبرانية والتقليدية، مجلة السياسة الدولية، العدد 208، مركز الأهرام، القاهرة، 2017، ص3 وما بعدها.

[107] Charles. L. Glaser, Deterrence of Cyber Attacks and U.S. National Security Report G.W. CSPRI, June, 2011, p.p.4-6.

[108] نقلاً عن:

James J. Wirtz (eds), Complex Deterrence Strategy in the Global Age, United States, The University of Chicago Press, 2004, p.p. 8-10.

[109] .....، الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية، رقم الوثيقة E/ESCVA/TDD/2015/1، الأمان في الفضاء، 2016، شبكة المعلومات الدولية، على الرابط:

Unescwa.org

وعلى الرغم من الاتفاق العلمي والعملياتي على تعرض ظاهرة الصراع مع بروز ظاهرة الفضاء السيبراني إلى تغييرات هائلة تعدت بتأثيرها مضمونها[110]، حيث لم يعد الصراع السيبراني حالة من التعارض في المصالح والقيم بين الفاعلين فحسب، بل وبسبب طبيعة ونمط الصراع الذي يخوضه الفاعلون دون غبار أو انقاض أو حتى دماء، بدت حالته متراوحة بين صراع سيبراني ذو طبيعة سياسية وإن اتخذ أشكالاً عسكرية ودفاعية، وبين صراع سيبراني ذو طبيعة ناعمة عن طريق شن حرب نفسية وإعلامية، أو صراع سيبراني ذو طبيعة تكنولوجية، الهدف منها سرقة الأسرار العلمية وبراءات الاختراع[111]، فإن تلك التغييرات لاحت أيضاً، القصد من الصراع، حيث زيادة التأثير والنفوذ على المستويين المحلي والدولي، لزيادة القدرة التدميرية للأسلحة المستخدمة فيه، لنكون أمام استراتيجية ردع جديدة، استراتيجية الردع السيبرانية، والتي من مهامها التحقق ليس من مصداقية الفعل وتوافر الوسائل، بل وعقلانية القرارات المسّوقة للمصالح القومية، ما دامت تمثل ممارسة افتراضية في فضاء مفتوح[112].وبقدر ما فرضت التهديدات آنفاً، فضلاً عن التغييرات التي نالت نمط الردع، ضغوطاً هائلة على العقيدة الاستراتيجية باتجاه استيعابها أو التكييف معها، مراجعة للثوابت وتحديداً للأولويات، وترسيخاً لمعيارية قياس الأداء الاستراتيجي، كما أفصحت عن ذلك ما أسماه البعض بـ(الاستراتيجية الوطنية للأمن السيبراني) والتي تم تحديد هدفها الأساس، حيث تشييد بيئة آمنة[113]، بدت الوظائف المستحدثة للأمن في الفضاء السيبراني تتوالى متخذة من وظائف العقيدة الاستراتيجية وما تسّوقه من أهداف، مهام محددة بغية تحديد ورسم مشاهد المرونة والإحراج في المواقف المتوقعة، كما حصل ذلك مع العقيدة السيبرانية القومية الأمريكية المعدة من قبل إدارة (بوش الأبن)، والتي سميت فيما بعد بـ(استراتيجية الطريق إلى الأمام)[114].

---

[110] سامر مؤيد عبد اللطيف، الحرب في الفضاء الرقمي: رؤية مستقبلية، مجلة رسالة الحقوق، العدد 2، مركز الدراسات القانونية والدستورية، جامعة كربلاء، 2015، ص87 وما بعدها.

[111] عبد المالك تكركارت، المعلومات وإدارة الحرب النفسية (دراسة وصفية مع حالات وتطبيقات في الحرب الاستعلامية الإعلامية)، رسالة ماجستير غير منشورة، قسم علوم الإعلام والاتصال، كلية العلوم السياسية والإعلام، جامعة الجزائر، 2004، ص25-29.

[112] أحمد زكي عثمان، تأثيرات القدرات السيبرانية في الصراعات الإقليمية، ملحق مجلة السياسة الدولية، اتجاهات نظرية، العدد 208، مركز الأهرام، القاهرة، 2017، ص21 وما بعدها.

[113] ريتشارد كلارك وروبرت نيك، حرب الفضاء الإلكتروني، التهديد التالي للأمن القومي وكيفية التعامل معه، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، 2012، ص13 وما بعدها.

[114] Wyatt Hoffman, Is Cyber Strategy Possible?, The Washington Quarterly, No.1, 2018, p.135.

وإزاء ذلك بدت العقيدة الاستراتيجية أمام محنة مضافة تمثلت بتسويغ التوجه نحو بناء (سياسات دفاعية) تغلب عليها الصفة الإجرائية المستمرة، تعزيزاً للقدرات، ومراجعة لهياكل الردع، بكل ما تحتاجه تلك السياسات من توجيهات سياسية/إدارية لا استراتيجية شاملة فحسب، لتتزاوج المهام الهجومية والدفاعية معاً[115]، كملمح تطور جديد فرض على الجميع الإقرار بحتمية المشاركة بين الاستراتيجية والسياسة، تبعاً لتداخل وتمازج مخاطر ما تفرزه البيئتين الداخلية والخارجية على الأمن القومي للدولة كذلك[116].

وقد أسست التطورات أعلاه، فتحاً استراتيجياً جديداً تمثل ببروز نمط جديد للحرب يدعى بـ(الحرب السيبرانية) نظراً لارتياد المتنافسون والمتصارعون للفضاء السيبراني، ميداناً لمقابلاتهم ومعاركهم، مروجين لما يسمى بـ(الحرب الافتراضية) بدلاً من الحروب التدميرية[117]، تلك الحرب التي عدّت تقدماً عملياتياً غير مسبوق، دفاعياً لصد الهجمات السيبرانية المعادية أو إبطال الصواريخ المعادية وتعطيها، وهجومياً معتمداً على السيطرة والضبط، بما يؤسس لمجال واسع لتدخل التكنولوجيا في صياغة قيم التفاعل والأداء الاستراتيجي، ليبرز لنا نمط جديد من الحروب، سميت بـ(الحروب السيبرانية أو حروب المجال الخامس) والتي تعني (استخدام أجهزة الكمبيوتر والانترنت لإجراء الحرب في الفضاء السيبراني) أو (التنفيذ أو الاستعداد لتنفيذ العمليات العسكرية، وفقاً للمبادئ المعلوماتية، من خلال تعطيل أو تدمير نظم المعلومات والاتصال على مستوى واسع النطاق)[118]، بكل ما تعنيه من تدمير للعقيدة العسكرية للعدو وحرمانه من ميزان المعرفة، لاسيما بعد التطور الكبير الذي لاح أدوات الحرب، لتغدو الأخيرة من دون نار أو دخان أو قصف، بل هي عنف من خلال الاختراق لـ(سيادة ونظم المعلومات) والقرصنة ونشر الفايروسات التي يصعب اكتشافها مادام استخدامها يتم بسرية تامة وغير محسوسة، فضلاً عن التجسس للحصول على

---

[115] هذا ما حصل فعلاً في مكافحة إرهاب داعش. للمزيد ينظر: مصطفى تاهمي، البعد المعلوماتي في الحروب اللاتماثلية، دراسة التنظيمات الإرهابية (داعش انموذجاً)، رسالة ماجستير غير منشورة، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجزائر، 2017، ص21 وما بعدها.

[116] لم يزل علم الحرب وتقليديته وفق هذه المقاربة حاضراً. للمزيد ينظر: منير شفيق، علم الحرب، المؤسسة العربية للدراسات والنشر، بيروت، 1975، ص27 وما بعدها.

[117] سعاد محمود أبو ليلة، دور القوة: ديناميكيات الانتقال من الصلبة إلى الناعمة إلى الافتراضية، ملحق مجلة السياسة الدولية، اتجاهات نظرية، العدد 188، مركز الأهرام، القاهرة، 2012، ص13-15.

[118] نسرين الصباحي، الحروب السيبرانية وتحديات الأمن العالمي، المركز العربي للبحوث والدراسات، شبكة المعلومات الدولية، على الرابط:

http://www.acrseg.org/40594

معلومات استخبارية لتحييد العملاء[119]، كما حصل مع هجوم (روسيا) على (جورجيا) عام 2008، وقبل ذلك هجوم (روسيا) على (أستونيا) عام 2007، وهجوم الولايات المتحدة الأمريكية عام 2018 بناءً على الأمر التنفيذي الذي أصدره (دونالد ترامب) على أنظمة إيران وحواسيبها، تمهيداً لإحداث شلل تام لأنظمة الدفاع[120].

ونظراً لأهمية ما تقدم، وتبعاً لتغير شكل الحرب، لصالح الحرب السيبرانية، عمدت دول بعينها إلى تأسيس وحدات الكترونية على شبكات الانترنت، مثل الولايات المتحدة الأمريكية، وروسيا الاتحادية، والصين، وكوريا الجنوبية، وكوريا الشمالية،...الخ، وآخرها (إسرائيل) عندما أنشئت الوحدة (8200) للحماية تتكون من مئات بل آلاف القراصنة المحترفين[121].

ومع كثرة المسّوقين للقيمة الاستراتيجية والعملياتية لهذا النمط من الحروب باعتبارها حروب لا تناظرية، ذات تكلفة متدنية تعطي للمهاجم أفضلية واضحة، نظراً لما تتميز به من سرعة ومرونة ومبادأة، دون اشتغال لنظم الردع التقليدية (إلغاء مفعول الردع بالانتقام) نظراً لعدم القدرة على تحديد مصدرها)[122]، فضلاً عن تعدد مستوياتها من حيث الشدة، فهناك المنخفضة (الناعمة) والمتوسطة الشدة، ومرتفعة الشدة الموازية للأعمال العسكرية التقليدية[123]، بدا البعض الآخر من المحللين والمراقبين، مقتنع بأن تلك الحرب بكل ما تضمه من أدوات متعددة، ستكون سلاحاً حاسماً في النزاعات بين الدول في المستقبل، خاصة بعد الدروس التي استفادت منها الدول من الجيل الرابع من الحروب، وكيف أسس التوظيف السياسي للإرهاب مقدمات ابتكارية للاستفادة من الحرب النفسية والرأي العام أو ما يسميه البعض بـ(استراتيجية القدم الخفية) أي (وضع الدولة باستمرار تحت ضغط الشائعة وفضح أخطاء أجهزتها الأمنية وغير الأمنية)[124]. كما وأن

---

[119] عادل عبد الصادق، الإرهاب الإلكتروني: القوة في العلاقات الدولية، مصدر سبق ذكره، ص155.

[120] مارك بيردسول، مصدر سبق ذكره، ص50. وكذلك: يحيى سعيد قاعود وعلا عامر الجعب، وثيقة الأمن القومي الأمريكي 2017، قراءة تحليلية في استراتيجية دونالد ترامب، قراءات استراتيجية، العدد 20، القاهرة، 2018، ص18-20.

[121] عن بدايات هذا الإدراك، ينظر:

Efraim Inbar, Israel's National Security, Issues and Challenges Since the yom Kippur, London, Routledge, 2008, p.p.12-16.

[122] Richard A. Clarke and Robert Knake, Cuber War, The next Threat to National Security and What to Do about it, Harpercollins e-books, New York, 2010, p.p. 31-42.

[123] عن أنواع هذه الحروب، ينظر: نضال ناجي بدوي بريوش، الصراع السيبراني مع العدو الصهيوني، أكاديمية دراسات اللاجئين، رام الله، 2019، ص14 وما بعدها.

[124] إيهاب خليفة، حروب مواقع التواصل الاجتماعي، العربي للنشر والتوزيع، القاهرة، 2016، ص75 وما بعدها.

تزايد الارتباط العالمي في الفضاء السيبراني، وتراجع دور الدولة مقابل العولمة والانسحاب من بعض القطاعات الاستراتيجية لمصلحة القطاع الخاص (شركات التكنولوجيا الفاعلة في الفضاء السيبراني)، فضلاً عن نشوء نمط جديد من الصراعات الدولية التي لا تحتاج إلى الدخول المادي لأراضي الخصم، جعل من تلك الحرب، النمط الأكثر تأثيراً في تقويض قدرة الخصم على الضبط والتحكم، خاصة عندما تداخلت مهامها، مع مهام الاستخبارات[125].

ورغم منطقية ما تقدم من رأي، إلا أن الحرب السيبرانية ولأسباب شتى، لم تزل لدى الكثيرين غير مفهومة، وذات مدلولات إعلامية أكثر منها واقعية، بل مازالت عند الكثيرين بحاجة إلى فهم/معرفة مقدماتها[126]، في ظل استمرار احتكار الدولة في استخدام القوات المسلحة، مع ظهور التنظيمات الإرهابية بما فيها قيامها بالهجمات الالكترونية كما هو الحال مع استخدام إيران الأنظمة الالكترونية لشركة نفط ارامكو السعودية[127].

فضلاً عن ذلك، فإن التعويل على هذا النمط من الحروب، استراتيجياً، سيعرض العالم لمخاطر وتحديات شتى، فبالإضافة إلى انتشار مخاطر السيبرانية بعد عسكرة الفضاء السيبراني واندماجه ضمن الأمن القومي للدول، والحاجة المكلفة لتحديث الأنشطة الدفاعية (سباق تسلح من نوع جديد) يبقى الخطر الأهم هو معضلة الدول في تحديد ماهية الأسلحة المرشحة للاستخدام في تلك الحرب، وإمكانية تدخل العالم في الحد من انتشارها بعد أن يغدو أثرها أمضى من تأثير أسلحة الدمار الشامل[128].

---

[125] Jonathan Pinkus, Intelligence and Public Diplomacy: The Changing Tide, Journal of Strategic Security, No.1, 2014, p.p.12-16.

[126] سيف نصرت الهرمزي، رصف المقاربات لمنظورات الفاعل الرقمي والانكشاف الاستراتيجي في ظل الفضاء السيبراني، مجلة آداب الفراهيدي، العدد 37، 2019، ص436.

[127] غريب حكيم، الإرهاب السيبراني والأمن الدولي، التهديدات العالمية الجديدة وأساليب المواجهة، المجلة الجزائرية للدراسات السياسية، العدد 2، الجزائر، 2018، ص106 وما بعدها.

[128] وقد تنبهت الولايات المتحدة الأمريكية، لذلك حتى أخذت تربي مقاتليها السيبرانيين على استخدام الأسلحة الجديدة. للمزيد ينظر: .....، كيف تربي أمريكا مقاتليها السيبرانيين، وكيف يبدأ الهجوم السيبراني على العالم، مقالات استراتيجية، قسم الترجمة، مركز الكاشف للمتابعة والدراسات الاستراتيجية، آذار 2012، ص6-11.

الخاتمة

لقد تبين لنا فيما سبق، إن السيبرانية بما احتوت عليه من مضامين وما احتوت عليه من مرجعيات تسويق، كانت جزءاً من التحوط الاستراتيجي لمعالجة المحتمل والمقبل من الانكشاف الاستراتيجي، لتتحول تالياً إلى ميدان أداء للحروب التي لم تقيّم إلا بكونها تدابير لوأد تهديدات مقبلة أريد منها اثبات الفواعل من غير الدول لمكانتها كندٍ للدولة. لتغدو (السيبرانية) نمطاً من أنماط المواجهة لقدر الدولة في اثبات وجودها. وتلك حقيقة ظلت راسخة سلّم بها الجميع، بكل ما حملته من تقديرات لاستفزاز وجود الدولة واستقرارها من جهة، وللنظام الدولي وتوازن قواه من جهة أخرى. وتلقفاً للمقاربة أعلاه، اتخمت أدبيات السياسة الدولية، وحتى الاستراتيجية بالعديد من الرؤى المحققة لتصاعد الاهتمام بـ((السيبرانية حيث الحوسبة، الاتصال والتواصل، التحكم)) كميدان من ميادين (الإزاحة الكلية) لوجود الفواعل العامة سواء كأنداد أو أعداء، رغم اقتناع الجميع ببعد المسافة في القدرات وتفاوتها نظراً لتعدد مسارب تراكمها وتوظيفها على حدٍ سواء. الأمر الذي جعل الدارسين للسيبرانية، مختلفين في قراءتها، كمعطى مؤثر رغم وضوح أهدافها حيث تسريع فواعلها لتآكل القدرات لدى خصومهم. وهذا ما جعلها (السيبرانية) كاشفة ومولدة للتحديات، أكثر مما هي محققة في مواجهتها لاسيما في ظل ديناميكية تبادل المواقف في فضاء متسع لا قدر لفواعلها تغطية ذلك، ما لم يحزم فواعلها أمرهم في امتلاك المبادأة، لتعود السيبرانية فاقدة التحكم بذاتها، لتلتمسه من العقيدة الاستراتيجية بكل ما تضمه من اشتراطات، وإن سدر فاعلوها بغيّهم وامتنعوا عن العودة مكتفين بمخيالهم، عندها ستكون الاستراتيجية بمجملها كعلم وفن، في جرح مقيم، وما عليهم سوى اللجوء إلى السياسة لتبرير أفعالهم، دون تبرير صلادة المواقف أو تأثير ما تحصده من أهداف لاسيما في ظل التطور التقني الذي لا يعترف بالتفوق الدائم أو السطوة المشهودة.

وإزاء ذلك بدت السيبرانية ميدان إشعال لا ميدان فعل، لا لأنها ليست كل شيء، بل لأنها عدت مراراً فخاً لاستفزاز الدولة التي يجب عليها معرفة حدود ولوجها في هذا المضمار، من دون تجاهلها ضمن اطار كلي شامل لاسيما في حيازة القدرات، لتؤسس أية قراءة لها إشكالية تعقيد واضحة وإذا ما أضيفت إلى سمة التعقيد التي تتميز بها البيئة الدولية، نكون قطعاً أمام (معضلة) غير معلومة الحدود لا لعلم الاستراتيجية، بل للعقيدة الاستراتيجية، طالما ظلت الدولة، كبنية، أكبر من كل ما تتضمنه. وربما هذا هو السر الذي يجعل العقيدة الاستراتيجية حساسة بمضامينها حيال الأمن/كمعطى، وما يتعرض له من تهديدات انتقالية أو مستديمة، ما لم يعثر حاملو تلك العقيدة على مقتربات تأهيل لإدراك تلك التهديدات، معرفياً ومؤسساتياً وسياسياً كي لا يقعوا في ما يسمى بـ(معضلة الاستجابة)، التي تبدو فيها التقنية ووسائلها غير ذات جدوى

دون حوامل فكرية تحدد مسار/اتجاه الفعل ومآله لا كيفيته فحسب. وهذا ما حصل في مكافحة الإرهاب لاسيما إرهاب داعش، والذي لم يندحر إلا بعد تدخل العقيدة الاستراتيجية في تصويب سبل مكافحته. وتلك هي العبرة التي ينبغي الاستفادة منها دون اهمال ما تؤسسه السيبرانية من مقدمات فعل وتخطيط لأهداف بعينها، كونها لم تزل عند حدود الوسيلة فحسب. لذا لا بد لنا من أخذ الحيطة والحذر ونحن نباشر بإعداد مسودة العقيدة الاستراتيجية للدولة، وكذلك العقيدة العسكرية، وأن نقرأ الواقع ومتطلباته كما نقرأ المستقبل واشتراطاته التي لا نميل إلى رأي قاطع حاسم. فكل الأبواب مفتوحة على العلوم الابتكارية والوسائل التناظرية، ولربما ستغدو السيبرانية بعد عقد من الزمان جزءاً من إرث الحرب التقليدية.

وحسماً لجدال قد يطول، بسبب مبهرات العلم والتقنية، أدعو، عراقياً، إلى تأسيس (مديرية النظم والأبحاث السيبرانية) تكون مقدمة لتأسيس صنف خاص لانجازاتها، بعد عدّها أسلحة تكتيكية واجبة الاستخدام ولو كردع أولاً.

In conclusion

as we have discussed earlier, cyber warfare, with its contents and marketing references, has been a strategic containment strategy to address potential and future strategic vulnerabilities. It has evolved into a field of operation for wars, which are now perceived as measures to deter future threats, irrespective of their origin. This has elevated cyber warfare to a mode of confrontation, demonstrating a state's capabilities and resilience on one hand, and the international system's balance of power on the other.

In line with this approach, international politics and even strategy literature have seen numerous insights into the increasing significance of cyber warfare, encompassing computing, communication, and control as part of the total shift in the state's role, whether as allies or adversaries. Despite the recognition of disparities in capabilities due to the diverse accumulation and employment of these capabilities, cyber warfare remains a revealing and generative field of challenges, often exceeding its effectiveness in confronting them, especially in the context of the dynamic exchange of positions in a vast space, unless its actors are restrained by their initiative.

At that point, cyber warfare becomes uncontrollable in itself, seeking guidance from strategic doctrine with all its requirements. If its actors avoid returning to

doctrine, relying solely on their imagination, strategy as a whole will be wounded, and they will resort to politics to justify their actions, without justifying the rigidity of their positions or the impact of their objectives. This is particularly challenging in light of technological advancements that do not acknowledge permanent superiority or established dominance.

Consequently, cyber warfare appears to be a field of ignition rather than action, not because it lacks importance but because it repeatedly poses a strategic challenge that states must recognize within a comprehensive framework, especially when they possess capabilities. Any analysis of cyber warfare should consider its inherent complexity, coupled with the international environment's complexity. This could lead to an "unknown boundary" dilemma not just for strategy but for strategic doctrine, as long as the state, as an entity, remains greater than its components.

This underscores the importance of addressing threats both in terms of awareness and institutional readiness. We should learn from the lessons of counterterrorism, especially in countering groups like ISIS, which were defeated only after strategic doctrine corrected the course of action. Cyber warfare offers similar challenges, as it is not limited to a means but involves specific objectives. Thus, we must exercise caution while preparing the state's strategic doctrine and military doctrine, reading the present and its requirements just as we read the future and its uncertain demands. All doors are open to innovative sciences and analogical means. In a decade or so, cyber warfare might become a part of the legacy of traditional warfare.

In conclusion, to resolve the ongoing debate sparked by the marvels of science and technology, I propose the establishment of a 'Directorate of Cyber Systems and Research' in Iraq. This would serve as a precursor to creating a dedicated category for its achievements, even if initially intended as tactical weapons of first resort.

قائمة المصادر :

اولاً : القواميس والمعاجم

1. غراهام إيفانز وجيفري نونيهام، قاموس بنغوين للعلاقات الدولية، الطبعة الأولى ، مركز الخليج للأبحاث ، دبي، 2003.
2. محمد بن مكرم بن منظور، لسان العرب، الجزء الثالث، الطبعة الثانية ، دار أحياء التراث العربي ، بيروت ،1999 .

ثانياً :الكتب :

1. أمير فرج يوسف، الجرائم المعلوماتية على شبكة الانترنت، دار المطبوعات الجامعية، الإسكندرية، 2008.
2. أميل خوري، صراعات الجيل الخامس، شركة المطبوعات للتوزيع والنشر، بيروت، 2016.
3. أندريه بوفر، مدخل إلى الاستراتيجية العسكرية، ترجمة: أكرم ديري والهيثم الأيوبي، الطبعة الأولى، دار الطليعة، بيروت، 1970.
4. اندريه بوفر، مدخل إلى الاستراتيجية العسكرية، ترجمة: أكرم ديري وهيثم الأيوبي، الطبعة الثالثة، دار الطليعة للطباعة والنشر، بيروت، 1987.
5. أوس مجيد غالب العوادي، الأمن المعلوماتي السيبراني، مركز البيان للدراسات والتخطيط، بغداد، 2016.
6. إيهاب خليفة، القوة الإلكترونية: كيف يمكن أن تدير الدولة شؤونها في عصر الانترنت، الولايات المتحدة إنموذجاً، العربي للنشر والتوزيع، القاهرة، 2017.
7. إيهاب خليفة، القوة الالكترونية، كيف يمكن أن تدير الدول شؤونها في عصر الانترنت، الولايات المتحدة الأمريكية انموذجاً، الطبعة الأولى، العربي للنشر والتوزيع، القاهرة، 2017.
8. إيهاب خليفة، حروب مواقع التواصل الاجتماعي، العربي للنشر والتوزيع، القاهرة، 2016.
9. برتران بديع، زمن المذلولين، باثولوجيا العلاقات الدولية، ترجمة: ماجد جيور، المركز العربي للأبحاث والدراسات، بيروت، 2015.
10. بيتر بي سيل، الكون الرقمي: الثورة العالمية في الاتصالات، ترجمة: ضياء وارد، مؤسسة هنداوي سي آي سي، المملكة المتحدة، 2017.

11. بيرت تشايمان، العقيدة العسكرية – دليل مرجعي، ترجمة: طلعت الشايب، الطبعة الأولى، المركز القومي للترجمة، القاهرة، 2015.
12. توني سميث، حلف مع الشيطان، سعي واشنطن لسيادة العالم وخيانة الوعد الأمريكي، ترجمة: هشام عبد الله، المؤسسة العربية للدراسات والنشر، بيروت، 2010.
13. جان بيريه، الذكاء والقيم المعنوية في الحرب، ترجمة: أكرم ديري والمقدم الهيثم الأيوبي، المؤسسة العربية للدراسات والنشر، بيروت، 1981
14. جان فرانسوا دورتيه، معجم العلوم الإنسانية، ترجمة: جورج كتورة، الطبعة الأولى، المؤسسة الجامعية للدراسات والنشر والتوزيع، بيروت، 2009.
15. جوانيتا إلياس وبيتر ستش، أساسيات العلاقات الدولية، ترجمة: محي الدين حميدي، إدارة الفرقد، دمشق، 2016.
16. جوزيف ناي، الردع في الفضاء الإلكتروني، المركز العربي لأبحاث الفضاء الإلكتروني، الدوحة، 2019.
17. جوزيف ناي، مستقبل القوة، ترجمة: أحمد عبد الحميد نافع، المركز القومي للترجمة، القاهرة، 2015.
18. جيمس لي دي، الحروب في العالم: الاتجاهات العالمية ومستقبل الشرق الأوسط، الطبعة الأولى، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، 1998.
19. ديبر كويتز، سوقيات الحرب، استعداد أمريكا لحرب الحاسوب، دراسات استراتيجية، مركز الدراسات الدولية، جامعة بغداد، 1997.
20. ديفيد جي. بيتز وتيم ستيفنز، الفضاء السيبراني، نحو استراتيجية للقوة السيبرانية، دلفي للأمن السيبراني والدراسات الاستراتيجية، لندن، 2006.
21. روبرت غيلين، الحرب والتغيير في السياسة العالمية، ترجمة: عمر سعيد الأيوبي، الطبعة الأولى، دار الكتاب العربي، بيروت، 2009.
22. ريتشارد كلارك وروبرت نيك، حرب الفضاء الإلكتروني، التهديد التالي للأمن القومي وكيفية التعامل معه، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، 2012.
23. سعد أبو رية، البيئة النفسية وأثرها في عملية صنع القرار في سياسة الأردن الخارجية، المنظمة العربية للعلوم الإدارية، عمان، 1983.

24. سين إس كوستجان، الأمن السيبراني، منهج رجعي عام، مركز جورج كاتليت مارشال الأوروبي للدراسات الأمنية، بروكسل، 2012.
25. سيوم براون، وهم التحكم: القوة والسياسة الخارجية في القرن الحادي والعشرين، ترجمة: فاضل جتكر، شركة الحوار الثقافي، بيروت.
26. صباح عبد الصبور عبد الحي، استخدام القوة الإلكترونية في التفاعلات الدولية، تنظيم القاعدة انموذجاً، نشرة دراسات استراتيجية، المعهد المصري للدراسات السياسية والاستراتيجية، اسطنبول، 2016.
27. عادل عبد الصادق، الإرهاب الإلكتروني، القوة في العلاقات الدولية، نمط جديد وتحديات، مركز الأهرام للدراسات السياسية والاستراتيجية، القاهرة، 2019.
28. عامر مصباح، نظريات التحليل الاستراتيجي والأمني للعلاقات الدولية، الطبعة الأولى، دار الكتاب الحديث، القاهرة، 2011.
29. عباس بدران، الحروب الإلكترونية: الاشتباك في عالم المعلومات، مركز دراسات الحكومة الإلكترونية، بيروت، 2010.
30. عبد الرحمن حسن الشهري، تطور العقائد والاستراتيجيات العسكرية، الطبعة الأولى، مكتبة الملك فهد الوطنية، الرياض، 2003.
31. عبد الكريم محمود برم، التقنية في الحرب، البعد الإلكتروني، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، 2010.
32. عبد المنعم سعيد، إدارة الأزمات والصراعات الدولية، مجلة المنار، العدد 20، باريس، 1986.
33. علاء أبو عامر، العلاقات الدولية: الظاهرة والعلم... الدبلوماسية والاستراتيجية، دار الشروق للنشر والتوزيع، عمان، 2004.
34. غادة نصار، الإرهاب والجريمة الإلكترونية، العربي للنشر والتوزيع، القاهرة، 2017.
35. غسان مدحت، مدخل إلى الفكر الاستراتيجي، دار الراية للنشر والتوزيع، عمان، 2013.
36. فرانز ستيفن وغرين أوستن، روسيا والولايات المتحدة: الدبلوماسية الإلكترونية الطريق لفتح الأبواب، ترجمة: طارق ذنون، اكاديميون للنشر والتوزيع، عمان، 2015.
37. فؤاد أفرام البستاني، منجد الطلاب، الطبعة الأولى، مطبعة دار الشروق، بيروت، 1986.

38. ليزلي جيلب، قواعد القوة، كيف يمكن للتفكير البديهي انقاذ السياسة الخارجية الأمريكية، ترجمة: كمال السيد، الطبعة الأولى، مطابع الأهرام التجارية، القاهرة، 2013.
39. مارك بيردسول، مستقبل الاستخبارات في القرن الحادي والعشرين، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، 2014.
40. محمد السيد سليم، التحليل السياسي الناصري، دراسة في العقائد والسياسة الخارجية، الطبعة الثانية، مركز دراسات الوحدة العربية، بيروت، 1978.
41. محمود شيت خطاب، بين العقيدة والقيادة، الطبعة الأولى، دار القلم للطباعة والنشر، دمشق، 1998.
42. معمر منعم العمار، الدولة واستراتيجية إدارة التغيير، مكتبة السنهوري القانونية، بغداد، 2019.
43. منعم العمار، من يدين لمن؟، مكانة الاستخبارات في الاستراتيجية الأمريكية الشاملة، الطبعة الأولى، مكتبة الغفران للخدمات الطباعية، بغداد، 2012.
44. منعم صاحي العمار، جوف المحنة، اقتفاء أثر الذات العراقية، دار ومكتبة الغفران للطباعة، بغداد، 2016.
45. منير شفيق، علم الحرب، المؤسسة العربية للدراسات والنشر، بيروت، 1975.
46. موسى الزعبي، الجيوسياسية والعلاقات الدولية، أبحاث في الجيوسياسية وفي الشؤون والعلاقات الدولية المتنوعة، وزارة الثقافة، دمشق.
47. هاري. آر ياغر، الاستراتيجية ومحترفوا الأمن القومي، التفكير الاستراتيجي وصياغة الاستراتيجية في القرن الحادي والعشرين، الطبعة الأولى، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، 2011.
48. هنري كيسنجر، العقيدة الاستراتيجية الأمريكية ودبلوماسية الولايات المتحدة، ترجمة: حازم طالب مشتاق، دار واسط، بغداد، 1987.
49. هنري كيسنجر، النظام العالمي: تأملات حول طلائع الأمم ومسار التاريخ، ترجمة: فاضل جتكر، الطبعة الأولى، دار الكتاب العربي، بيروت، 2015.
50. ويليام مارسيلينو وميجان ل. سميث وآخرون، رصد وسائل التواصل الاجتماعي عبر التحليلات لوسائل الدفاع الأمريكية، وسائل التواصل الاجتماعي في المستقبل دعماً لعمليات المعلومات، مؤسسة راند، كاليفورنيا، 2017.

البحوث والدراسات :

1. أحمد زكي عثمان، تأثيرات القدرات السيبرانية في الصراعات الإقليمية، ملحق مجلة السياسة الدولية، اتجاهات نظرية، العدد 208، مركز الأهرام، القاهرة، 2017.
2. أوشينا جيروم أورجي، ردع الإرهاب السيبراني في مجتمع المعلومات العالمي، قضية المسؤولية الجماعية للدول، مراجعة الدفاع عن الإرهاب، العدد 1، 2004.
3. بن ضيف الله بلقاسم، القوة الذكية في الفكر الاستراتيجي الأمريكي المعاصر، مجلة المستقبل العربي، العدد 483، مركز دراسات الوحدة العربية، بيروت، 2019.
4. بهاء عدنان السعيري وعماد عبد خضير الزرفي، انتقال التهديدات من الواقع إلى العالم الافتراضي، مجلة جامعة بابل للعلوم الإنسانية، العدد 4، بابل، 2019.
5. توماس كوبلاند، ثورة المعلومات والأمن القومي، دراسات عالمية، العدد 46، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، 2003.
6. حسنين توفيق إبراهيم، التنظيمات الجهادية الإرهابية وشبكات التواصل الاجتماعي، داعش انموذجاً، كراسات استراتيجية، العدد 268، مركز الأهرام للدراسات السياسية والاستراتيجية، القاهرة، 2016.
7. حميد حمد السعدون، استخدام الفضاء السيبراني وتأثيره في العلاقات الدولية، الشرق الأوسط انموذجاً، مجلة دراسات دولية، العدد 59، جامعة بغداد، 2018.
8. خالد حنفي علي، إشكاليات تداخل الصراعات السيبرانية والتقليدية، مجلة السياسة الدولية، العدد 208، مركز الأهرام، القاهرة، 2017.
9. رضوان بروسي، من الدولة الفيبرية إلى الحوكمة كمنظور دولتي جديد، رؤية نقدية، المجلة العربية للعلوم السياسية، العدد 1، مركز دراسات الوحدة العربية، بيروت، ربيع 2013.
10. سامر مؤيد عبد اللطيف، الحرب في الفضاء الرقمي: رؤية مستقبلية، مجلة رسالة الحقوق، العدد 2، مركز الدراسات القانونية والدستورية، جامعة كربلاء، 2015.
11. سعاد محمود أبو ليلة، دور القوة: ديناميكيات الانتقال من الصلبة إلى الناعمة إلى الافتراضية، ملحق مجلة السياسة الدولية، اتجاهات نظرية، العدد 188، مركز الأهرام، القاهرة، 2012
12. سيف نصرت الهرمزي، رصف المقاربات لمنظورات الفاعل الرقمي والانكشاف الاستراتيجي في ظل الفضاء السيبراني، مجلة آداب الفراهيدي، العدد 37، 2019.

13. شريف درويش اللبان، تكنولوجيا المعلومات والعلاقات الاجتماعية/دراسة في أخلاقيات العصر الإلكتروني: الاتجاهات الحديثة في المكتبات والمعلومات، العدد 13، المكتبة الأكاديمية، القاهرة، 2000.
14. عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، سلسلة أوراق، العدد 3، وحدة الدراسات المستقبلية، الإسكندرية، مصر، 2016.
15. عادل عبد الصادق، الفضاء الإلكتروني وتهديدات جديدة للأمن القومي، مجلة السياسة الدولية، العدد 180، مؤسسة الأهرام، القاهرة، 2010.
16. عبد الغفار الديواني، القرن السيبراني، الردع الإلكتروني بين المنع والانتقام، نظرية الردع في القرن السيبراني، المعهد الألماني للشؤون الأمنية والدولية، برلين، العدد 15.
17. عشور عبد الكريم، دور الحكم الإلكتروني في مكافحة الفساد الإداري، الولايات المتحدة الأمريكية انموذجاً، مجلة المفكر، العدد 11، جامعة محمد خيضر –بسكرة، الجزائر، 2019.
18. علاء عبد الحفيظ محمد، النسق السياسي والعقيدي لرجب طيب أردوغان، مجلة رؤية استراتيجية، العدد 3، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، 2013.
19. علم الدين بانقا، مخاطر الهجمات الإلكترونية (السيبرانية) وآثارها الاقتصادية، دراسة حالة مجلس التعاون الخليجي، سلسلة دراسات تنموية، العدد 63، المعهد العربي للتخطيط، الكويت، 2019.
20. غريب حكيم، الإرهاب السيبراني والأمن الدولي، التهديدات العالمية الجديدة وأساليب المواجهة، المجلة الجزائرية للدراسات السياسية، العدد 2، الجزائر، 2018.
21. كيف تربي أمريكا مقاتليها السيبرانيين، وكيف يبدأ الهجوم السيبراني على العالم، مقالات استراتيجية، قسم الترجمة، مركز الكاشف للمتابعة والدراسات الاستراتيجية، آذار 2012.
22. مفيد نجم، النظام الدولي الجديد وغياب الاستراتيجية والمعايير، مجلة الفكر السياسي، العددان 4–5، اتحاد الكتاب العرب، دمشق، 1999.
23. منعم صاحي العمار، الأمن الدولي وبوابات الإدراك العشرة، مجلة قضايا سياسية، العدد 59، 2019.
24. منعم صاحي العمار، العقيدة العسكرية العراقية الجديدة: دراسة في نظم تشكيلها، مجلة قضايا سياسية، العددان 23–24، كلية العلوم السياسية، جامعة النهرين، بغداد، 2011.

25. نضال ناجي بدوي بريوش، الصراع السيبراني مع العدو الصهيوني، أكاديمية دراسات اللاجئين، رام الله، 2019.
26. نورة شلوش، القرصنة الإلكترونية في الفضاء السيبراني، التهديد المتصاعد من الدول، مجلة مركز بابل للدراسات الإنسانية، العدد 2، بابل، 2018.
27. يحيى سعيد قاعود وعلا عامر الجعب، وثيقة الأمن القومي الأمريكي 2017، قراءة تحليلية في استراتيجية دونالد ترامب، قراءات استراتيجية، العدد 20، القاهرة، 2018.

الرسائل والاطاريح:

1. سليم دحماني، أثر التهديدات السيبرانية على الأمن القومي، الولايات المتحدة الأمريكية انموذجاً 2001–2017، رسالة ماجستير غير منشورة، كلية الحقوق والعلوم السياسية، جامعة محمد ضياف، الجزائر، 2018.
2. عبد الباسط محمد أبو ناموس، الحرب النفسية التي استخدمتها المقاومة الفلسطينية في مواجهة العدوان الإسرائيلي على غزة عام 2014، رسالة ماجستير غير منشورة، أكاديمية الإدارة والسياسات للدراسات العليا، فلسطين، 2015.
3. عبد المالك تكركارت، المعلومات وإدارة الحرب النفسية (دراسة وصفية مع حالات وتطبيقات في الحرب الاستعلامية الإعلامية)، رسالة ماجستير غير منشورة، قسم علوم الإعلام والاتصال، كلية العلوم السياسية والإعلام، جامعة الجزائر، 2004.
4. مصطفى تاهمي، البعد المعلوماتي في الحروب اللاتماثلية، دراسة التنظيمات الإرهابية (داعش انموذجاً)، رسالة ماجستير غير منشورة، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجزائر، 2017.
5. مهند علي عمران، أثر القوة والقدرة وحرية العمل في الاستراتيجية الشاملة للدولة، رسالة ماجستير غير منشورة، كلية العلوم السياسية، جامعة النهرين، 2003.
6. وسام صالح عبد الحسين، المتغير العقيدي وأثره في انتشار القوة، الجمهورية الإسلامية الإيرانية إنموذجاً، اطروحة دكتوراه غير منشورة، كلية العلوم السياسية، جامعة بغداد، بغداد، 2020.

الانترنيت :

1. محمد قيراط، استراتيجية وطنية للأمن السيبراني، موقع الشرق للإدارة الإلكترونية، 2008، شبكة المعلومات الدولية، على الرابط:

http://al-sharq.com

2. جوزيف ناي، كيف يتم تطوير معايير جديدة للأمن السيبراني، شبكة النبأ للمعلوماتية، 2018، على الرابط:

http://annabaa.org

3. الموسوعة السياسية، الأمن السيبراني، شبكة المعلومات الدولية، على الرابط:

http://political-encyclopedia.org

4. الموسوعة الجزائرية للدراسات السياسية والاستراتيجية، التصور الأمني لمدرسة كوبنهاكن، دراسات أمنية، حزيران 2019، شبكة المعلومات الدولية، على الرابط:

http://www.politics-dz-com

5. نسرين الصباحي، الحروب السيبرانية وتحديات الأمن العالمي، المركز العربي للبحوث والدراسات، شبكة المعلومات الدولية، على الرابط:

http://www.acrseg.org/40594

6. ليلى الجنابي، فعالية القوانين الوطنية والدولية في مكافحة الجرائم السيبرانية، الحوار المتمدن، العدد 4634 في 2017/9/8، شبكة المعلومات الدولية، على الرابط:

http://www.ahewar.org

7. اسراء جبريل رشاد مرعي، الجرائم الإلكترونية، الأهداف والأسباب وطرق المعالجة، المركز الديمقراطي العربي للدراسات الاستراتيجية والاقتصادية، برلين، 2016، شبكة المعلومات الدولية، على الرابط:

http://democraticac.de/?p=3542 6

8. ناجي ملاعب، الأمن السيبراني، تعريف الجرائم السيبرانية وتطورها، موقع الأمن والدفاع العربي، شبكة المعلومات الدولية، على الرابط:

http://sdarabia.com

9. ياسر محجوب الحسين، مقتل فلويد وفرص إعادة انتخاب ترامب، قناة العربي 21، 10/ حزيران/2020، شبكة المعلومات الدولية، على الرابط:

http://arabi21.com/story/2177452/%09

10. نسرين الصباحي، الحروب السيبرانية وتحديات الأمن العالمي، المركز العربي للبحوث والدراسات، شبكة المعلومات الدولية، على الرابط:

http://www.acrseg.org/40594

11. الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية، رقم الوثيقة E/ESCVA/TDD/2015/1، الأمان في الفضاء، 2016، شبكة المعلومات الدولية، على الرابط: Unescwa.org

English resources :

1. Abrahan Wagner Intelligence for Counter?. Terrorism: Technology and Methods, Journal of Policing, Intelligence and Counter Terrorism, No.3, 2011.
2. Adam Lowther, ed, Deterrence: Vising Powers, Rogne Regime, and Terrorism in the Twenty-First Century, New York, 2012.
3. Bert Chapman, Researching National Security and Intelligence Policy, Washington, DC. CQ Press, 2004.
4. Charles. L. Glaser, Deterrence of Cyber Attacks and U.S. National Security Report G.W. CSPRI, June, 2011.
5. Christian Whiton, Smart Power: Between Diplomacy and War, Washington. D.C. Potomac Book-INC, University of Nebraska Press, 2013.
6. Christopher, P. Twomey, The Military Lens: Doctrine Differences, Misperception, and Deterrence Failure in Sino- American Relations, Massachusetts Institute of Technology, 2005.
7. Cyntha Weber, International Relations Theory: a Critical Inteoduction, 3rd, London, Routledge, 2010.
8. Divya Srikanth, Non-Traditional Security Threats in the 21st Century: A review, International Journal of Development and Conflict, No.2, 2014.
9. Efraim Inbar, Israel's National Security, Issues and Challenges Since the yom Kippur, London, Routledge, 2008.

10. Gideon Rachman, Zero-Sum World, Power and Prosperity After the Grash, Atlantic Books, London, 2010.
11. HQ Integrated Defence Staff, Understanding Military Doctrine A primer, Directorate of Doctrine Training and Doctrine Divison, Military of Defence, New Delhi, 2018.
12. James J. Wirtz (eds), Complex Deterrence Strategy in the Global Age, United States, The University of Chicago Press, 2004.
13. John. J. B Sheldon, Deciphering Cyber Power, Strategic Purpose in Peace and war, air University, Strategiy Studies Quartery, 2011.
14. Jonathan Pinkus, Intelligence and Public Diplomacy: The Changing Tide, Journal of Strategic Security, No.1, 2014.
15. Joseph S. Nye, Cyber Power, Center for Science and International Affairs, Harrard, Kennedy School, 2010.
16. Marcos Degant, Spies and Policy Makers, Intelligence in the Information Age, Intelligence and National Security, No.4, 2016.
17. Matt, Hidek, Military Doctrine and Integrated Intelligence in the City, San Fransico, 2007.
18. Michael Olender, Keeping Pace wkth Cyber Power, Defense and War Fare, Journal of International and Global Studies, No.2, Center for International and Global Studies, Duke University, North Carolina, 2015.
19. Mitko Bogdnoski & Drage Petreski, Cyber Terrorism – Global Security Threat, International Scientific defense, Security and Peace Journal, No.3, 2014.
20. Peter Long, Hays, Struggling Towards Space Doctrine: U.S Military Space Plans, Programs, and Perspectives during the Cold war, Boston, 1994.

21. Prabh Karam, National Security, Imperative and Challenges, New Delhi, Tata Mc Graw, 2008 .

22. R.S. Mcnamara and J. G. Blight, Wilson's Ghost, Reducing the Risk of Conflict, Killing and Cata Stropke in the Century, New York, Public a Hairs, 2001.

23. Richard A. Clarke and Robert Knake, Cuber War, The next Threat to National Security and What to Do about it, Harpercollins e-books, New York, 2010.

24. Robert M. Grant, Contemporary Strategy Analysis, New Jersey, John Wiley and Sons Ltd, 2010.

25. Roland Dannreuther and John Peterson, Security Strategy and Transtlantic Relations, Routledge, New York, 2006.

26. Wyatt Hoffman, Is Cyber Strategy Possible?, The Washington Quarterly, No.1, 2018.

27. Brian Manthe, United States Military Doctrine and the Conduct of Couaterin- surgency Operation: Fixing the Discannect, From: http://handle.dtic.mil/100-2/APA393508,2001

28. Kenneth J. Knapp, Cyber Security and Global Information Assurance, Thereat Analysis and Response Solions, 2019, from, online, http://epdf.pub/cyber-security and global-information-sols-9733.html

Source list:

First: dictionaries and glossaries

1. Graham Evans and Geoffrey Nunniham, Penguin Dictionary of International Relations, First Edition, Gulf Research Center, Dubai, 2003.
2. Muhammad bin Makram bin Manzoor, Lisan Al Arab, Part Three, Second Edition, Dar Revival of Arab Heritage, Beirut, 1999.

Secondly: books:

1. Amir Farag Youssef, Information Crimes on the Internet, University Press, Alexandria, 2008.
2. Emile Khoury, Fifth Generation Conflicts, Publications Company for Distribution and Publishing, Beirut, 2016.
3. Andre Buffer, An Introduction to Military Strategy, translated by: Akram Dairy and Al-Haytham Al-Ayyubi, first edition, Dar Al-Tali`ah, Beirut, 1970.
4. Andre Buffer, An Introduction to Military Strategy, translated by: Akram Dairy and Haitham Al-Ayoubi, third edition, Dar Al-Talee'ah for Printing and Publishing, Beirut, 1987.
5. Aws Majid Ghaleb Al-Awadi, Cyber Information Security, Al-Bayan Center for Studies and Planning, Baghdad, 2016.
6. Ihab Khalifa, Electronic Power: How can the state manage its affairs in the era of the Internet, the United States as a model, Al-Araby for Publishing and Distribution, Cairo, 2017.
7. Ihab Khalifa, Electronic Power, How Countries Can Manage Their Affairs in the Age of the Internet, The United States of America as a Model, First Edition, Al Arabi for Publishing and Distribution, Cairo, 2017.
8. Ihab Khalifa, Social Media Wars, Al-Araby for Publishing and Distribution, Cairo, 2016.
9. Bertrand Badie, The Time of the Humiliated, Pathology of International Relations, translated by: Majed Jewer, Arab Center for Research and Studies, Beirut, 2015.
10. Peter B. Sell, The Digital Universe: The Global Revolution in Communications, translated by: Zia Ward, Hindawi CIC, UK, 2017.
11. Bert Chaiman, Military Doctrine - A Reference Guide, Translated by: Talaat Al-Shayeb, First Edition, National Center for Translation, Cairo, 2015.
12. Tony Smith, Pact with the Devil, Washington's Quest for World Sovereignty and Betrayal of the American Promise, Translated by: Hisham Abdullah, Arab Institute for Studies and Publishing, Beirut, 2010.
13. Jean Perrier, Intelligence and Moral Values in War, translated by: Akram Dairy and Lieutenant Colonel Al-Haytham Al-Ayoubi, Arab Institute for Studies and Publishing, Beirut, 1981
14. Jean-François Dortier, Dictionary of Human Sciences, translated by: Georges Ktoura, first edition, University Foundation for Studies, Publishing and Distribution, Beirut, 2009.
15. Juanita Elias and Peter Sche, Fundamentals of International Relations, translated by: Mohieddin Hamidi, Al-Farqad Administration, Damascus, 2016.
16. Joseph Nye, Deterrence in Cyberspace, Arab Center for Cyberspace Research, Doha, 2019.

17. Joseph Nye, The Future of Power, translated by: Ahmed Abdel Hamid Nafie, The National Center for Translation, Cairo, 2015.
18. James Lee Dee, Wars in the World: Global Trends and the Future of the Middle East, first edition, Emirates Center for Strategic Studies and Research, Abu Dhabi, 1998.
19. Debre Koetz, War Logistics, America's Preparation for Computer War, Strategic Studies, Center for International Studies, University of Baghdad, 1997.
20. David J. Betz and Tim Stephens, Cyberspace: Towards a Strategy for Cyber Power, Delphi Cyber Security and Strategic Studies, London, 2006.
21. Robert Guillen, War and Change in World Politics, translated by: Omar Saeed Al-Ayoubi, first edition, Dar Al-Kitab Al-Arabi, Beirut, 2009.
22. Richard Clarke and Robert Nick, Cyberwar, The Next Threat to National Security and How to Deal with It, Emirates Center for Strategic Studies and Research, Abu Dhabi, 2012.
23. Saad Abu Rayya, The Psychological Environment and its Impact on the Decision-Making Process in Jordan's Foreign Policy, Arab Organization for Administrative Sciences, Amman, 1983.
24. Sean S. Kostejan, Cybersecurity, a general reactionary approach, Georges Catlett-Marshall European Center for Security Studies, Brussels, 2012.
25. Seyoum Brown, The Illusion of Control: Power and Foreign Policy in the Twenty-First Century.
26. Sabah Abdel-Sabour Abdel-Hay, The Use of Electronic Power in International Interactions, Al-Qaeda as a Model, Strategic Studies Bulletin, Egyptian Institute for Political and Strategic Studies, Istanbul, 2016.
27. Adel Abdel Sadiq, Electronic Terrorism, Power in International Relations, New Pattern and Challenges, Al-Ahram Center for Political and Strategic Studies, Cairo, 2019.
28. Amer Mesbah, Theories of Strategic and Security Analysis of International Relations, first edition, Dar Al-Kitab Al-Hadith, Cairo, 2011.
29. Abbas Badran, Electronic Wars: Conflict in the Information World, Center for Electronic Government Studies, Beirut, 2010.
30. Abd al-Rahman Hassan al-Shehri, The Development of Military Doctrines and Strategies, First Edition, King Fahd National Library, Riyadh, 2003.
31. Abdul Karim Mahmoud Barm, Technology in War, The Electronic Dimension, Emirates Center for Strategic Studies and Research, Abu Dhabi, 2010.
32. Abdel Moneim Saeed, Management of International Crises and Conflicts, Al-Manar Magazine, No. 20, Paris, 1986.
33. Alaa Abu Amer, International Relations: Phenomenon and Science... Diplomacy and Strategy, Dar Al-Shorouk for Publishing and Distribution, Amman, 2004.
34. Ghada Nassar, Terrorism and Cybercrime, Al-Araby for Publishing and Distribution, Cairo, 2017.
35. Ghassan Medhat, Introduction to Strategic Thought, Dar Al-Raya for Publishing and Distribution, Amman, 2013.

36. Franz Stephen and Green Austin, Russia and the United States: Electronic Diplomacy, the Way to Open Doors, translated by: Tariq Thanoun, Academics for Publishing and Distribution, Amman, 2015.
37. Fouad Afram Al-Bustani, Munjid Al-Talaba, first edition, Dar Al-Shorouk Press, Beirut, 1986.
38. Leslie Gelb, The Rules of Power, How Intuitive Thinking Can Save American Foreign Policy, translated by: Kamal El-Sayed, first edition, Al-Ahram Commercial Press, Cairo, 2013.
39. Mark Birdsall, The Future of Intelligence in the Twenty-First Century, Emirates Center for Strategic Studies and Research, Abu Dhabi, 2014.
40. Muhammad al-Sayyid Salim, Nasserite Political Analysis, A Study in Beliefs and Foreign Policy, second edition, Center for Arab Unity Studies, Beirut, 1978.
41. Mahmoud Chit Khattab, Between Faith and Leadership, first edition, Dar Al-Qalam for Printing and Publishing, Damascus, 1998.
42. Muammar Moneim Al-Ammar, The State and Change Management Strategy, Al-Sanhouri Law Library, Baghdad, 2019.
43. Munem al-Ammar, Who owes to whom?, The place of intelligence in the comprehensive American strategy, first edition, Al-Ghufran Bookshop for Printing Services, Baghdad, 2012.
44. Munim Sahi al-Ammar, Jawf al-Mahna, Tracing the Traces of the Iraqi Self, Al-Ghufran Publishing House and Library, Baghdad, 2016.
45. Mounir Shafik, The Science of War, Arab Foundation for Studies and Publishing, Beirut, 1975.
46. Musa Al-Zoubi, Geopolitics and International Relations, research in geopolitics and various international affairs and relations, Ministry of Culture, Damascus.
47. Harry. R. Yager, Strategy and National Security Professionals, Strategic Thinking and Strategy Formulation in the Twenty-First Century, First Edition, Emirates Center for Strategic Studies and Research, Abu Dhabi, 2011.
48. Henry Kissinger, American Strategic Doctrine and US Diplomacy, translated by: Hazem Talib Mushtaq, Dar Wasit, Baghdad, 1987.
49. Henry Kissinger, The World Order: Reflections on the Vanguards of Nations and the Course of History, translated by: Fadel Jetker, first edition, Dar Al-Kitab Al-Arabi, Beirut, 2015.
50. William Marcelino and Megan L. Smith et al., Social Media Monitoring through Analytics for US Defense, Social Media in the Future in Support of Information Operations, RAND Corporation, California, 2017.

Research and studies:

1. Ahmed Zaki Othman, Effects of Cyber Capabilities in Regional Conflicts, Supplement to the Journal of International Politics, Theoretical Directions, Issue 208, Al-Ahram Center, Cairo, 2017.
2. Oceana Jerome Orji, Deterring Cyberterrorism in the Global Information Society, The Case for the Collective Responsibility of States, Defense of Terrorism Review, Issue 1, 2004.

3. Ben Daifallah Belkacem, Smart Power in Contemporary American Strategic Thought, Arab Future Magazine, Issue 483, Center for Arab Unity Studies, Beirut, 2019.
4. Bahaa Adnan Al-Sairi and Imad Abdul Khudair Al-Zarfi, Threats Transition from Reality to the Virtual World, Babylon University Journal for Human Sciences, Issue 4, Babel, 2019.
5. Thomas Copeland, The Information Revolution and National Security, International Studies, Issue 46, Emirates Center for Strategic Studies and Research, Abu Dhabi, 2003.
6. Hassanein Tawfiq Ibrahim, Terrorist Jihadi Organizations and Social Media Networks, ISIS as a Model, Strategic Brochures, No. 268, Al-Ahram Center for Political and Strategic Studies, Cairo, 2016.
7. Hamid Hamad Al-Saadoun, The use of cyberspace and its impact on international relations, the Middle East as a model, Journal of International Studies, No. 59, University of Baghdad, 2018.
8. Khaled Hanafi Ali, Problems of Overlapping Cyber and Traditional Conflicts, International Politics Journal, No. 208, Al-Ahram Center, Cairo, 2017.
9. Radwan Brosi, From the Weberian State to Governance as a New State Perspective, A Critical View, Arab Journal of Political Science, Issue 1, Center for Arab Unity Studies, Beirut, Spring 2013.
10. Samer Moayyed Abdel Latif, War in the Digital Space: A Future Vision, Risala Al-Huqoq Magazine, Issue 2, Center for Legal and Constitutional Studies, University of Karbala, 2015.
11. Souad Mahmoud Abu Laila, The Role of Power: Dynamics of the Transition from Hard to Soft to Virtual, International Politics Journal Supplement, Theoretical Directions, Issue 188, Al-Ahram Center, Cairo, 2012
12. Saif Nusrat Al-Harmuzi, Coordination of Approaches to the Perspectives of the Digital Actor and Strategic Exposure in Light of Cyberspace, Adab Al-Farahidi Magazine, Issue 37, 2019.
13. Sherif Darwish Al-Labban, Information Technology and Social Relations/A Study in the Ethics of the Electronic Age: Modern Trends in Libraries and Information, No. 13, Academic Library, Cairo, 2000.
14. Adel Abdel-Sadiq, Cyber Weapons in Light of International Humanitarian Law, Paper Series, No. 3, Future Studies Unit, Alexandria, Egypt, 2016.
15. Adel Abdel Sadiq, Cyberspace and New Threats to National Security, International Politics Journal, No. 180, Al-Ahram Foundation, Cairo, 2010.
16. Abdul Ghaffar Al-Diwani, The Cyber Century, Electronic Deterrence between Prevention and Retaliation, The Theory of Deterrence in the Cyber Century, German Institute for Security and International Affairs, Berlin, No. 15.
17. Ashour Abdel-Karim, The Role of Electronic Governance in Combating Administrative Corruption, USA as a Model, Al-Mufaker Magazine, Issue 11, Mohamed Kheidar University-Biskra, Algeria, 2019.

18. Alaa Abdel Hafeez Muhammad, The Political and Doctrinal Formation of Recep Tayyip Erdogan, Strategic Vision Journal, Issue 3, Emirates Center for Strategic Studies and Research, Abu Dhabi, 2013.
19. Alamuddin Banga, The Risks of Electronic (Cyber) Attacks and Their Economic Impacts, Case Study of the Gulf Cooperation Council, Development Studies Series, Issue 63, Arab Planning Institute, Kuwait, 2019.
20. Gharib Hakim, Cyberterrorism and International Security, New Global Threats and Methods of Confrontation, Algerian Journal of Political Studies, No. 2, Algeria, 2018.
21. How America educates its cyber fighters, and how the cyber attack begins on the world, strategic articles, translation department, Al-Kashif Center for Follow-up and Strategic Studies, March 2012.
22. Mufid Najm, The New International Order and the Absence of Strategy and Standards, Journal of Political Thought, Issues 4-5, Arab Writers Union, Damascus, 1999.
23. Munem Sahi al-Ammar, International Security and the Ten Gates of Perception, Journal of Political Issues, Issue 59, 2019.
24. Munim Sahi al-Ammar, The New Iraqi Military Doctrine: A Study of Its Forming Systems, Journal of Political Issues, Issues 23-24, College of Political Science, Al-Nahrain University, Baghdad, 2011.
25. Nidal Naji Badawi Brioche, The Cyber Conflict with the Zionist Enemy, Refugee Studies Academy, Ramallah, 2019.
26. Noura Shaloush, Electronic piracy in cyberspace, the escalating threat from states, Babylon Center for Humanitarian Studies Journal, Issue 2, Babel, 2018.
27. Yahya Saeed Qaoud and Ola Amer Al-Ja'b, American National Security Document 2017, Analytical Reading in Donald Trump's Strategy, Strategic Readings, Issue 20, Cairo, 2018.

Letters and treatises:

1. Salim Dahmani, The Impact of Cyber Threats on National Security, USA as a Model 2001-2017, Unpublished Master Thesis, Faculty of Law and Political Science, Mohamed Diaf University, Algeria, 2018.
2. Abd al-Basit Muhammad Abu Namous, The psychological war used by the Palestinian resistance in the face of the Israeli aggression on Gaza in 2014, an unpublished master's thesis, The Academy of Management and Politics for Graduate Studies, Palestine, 2015.
3. Abdelmalek Tuckerkart, Information and Psychological Warfare Management (a descriptive study with cases and applications in media information warfare), unpublished master's thesis, Department of Media and Communication Sciences, Faculty of Political Science and Information, University of Algiers, 2004.
4. Mustafa Tahmi, The Informational Dimension in Asymmetric Wars, Studying Terrorist Organizations (ISIS as a Model), Unpublished Master's Thesis, Faculty of Law and Political Science, Zayan Ashour University, Algeria, 2017.

5. Muhannad Ali Omran, The Impact of Power, Ability, and Freedom of Action on the Comprehensive Strategy of the State, unpublished master's thesis, College of Political Science, Al-Nahrain University, 2003.
6. Wissam Salih Abd Al-Hussein, The Doctrinal Variable and its Impact on the Spread of Power, The Islamic Republic of Iran as a Model, Unpublished PhD Thesis, College of Political Science, University of Baghdad, Baghdad, 2020.

the internet:

1. Muhammad Qirat, A National Strategy for Cybersecurity, Al-Sharq Electronic Administration website, 2008, International Information Network, at the link:
http://al-sharq.com
2. Joseph Nye, How are new standards for cybersecurity developed, Al-Nabaa Informatics Network, 2018, at the link:
http://annabaa.org
3. The Political Encyclopedia, Cyber Security, International Information Network, at the link:
http://political-encyclopedia.org
4. Algerian Encyclopedia of Political and Strategic Studies, Copenhagen School's Security Perception, Security Studies, June 2019, International Information Network, at the link:
http://www.politics-dz-com
5. Nisreen Al-Sabahi, Cyber Wars and Global Security Challenges, Arab Center for Research and Studies, International Information Network, at the link:
http://www.acrseg.org/40594
6. Laila Al-Janabi, The Effectiveness of National and International Laws in Combating Cybercrimes, Al-Hiwar Al-Mutamaddin, Issue No. 4634 dated 9/8/2017, International Information Network, at the link:
http://www.ahewar.org
7. Israa Jibril Rashad Marai, Cybercrimes, Goals, Causes and Methods of Treatment, Arab Democratic Center for Strategic and Economic Studies, Berlin, 2016, International Information Network, at the link:
http://democraticac.de/?p=35426
8. Naji Malaeb, Cybersecurity, definition and development of cybercrime, Arab Security and Defense website, International Information Network, at the link:
http://sdarabia.com
9. Yasser Mahjoub Al-Hussein, the killing of Floyd and the chances of Trump's re-election, Al-Araby 21 channel, June 10, 2020, the International Information Network, at the link:
http://arabi21.com/story/2177452/%09
10. Nisreen Al-Sabahi, Cyber Wars and Challenges of Global Security, Arab Center for Research and Studies, International Information Network, at the link:
http://www.acrseg.org/40594
11. Safety in Cyberspace and Combating Cybercrime in the Arab Region, Document No. E/ESCVA/TDD/2015/1, Safety in Space, 2016, International Information Network, at the link:

Unescwa.org

English resources :

29. Abrahan Wagner Intelligence for Counter?. Terrorism: Technology and Methods, Journal of Policing, Intelligence and Counter Terrorism, No.3, 2011.
30. Adam Lowther, ed, Deterrence: Vising Powers, Rogne Regime, and Terrorism in the Twenty-First Century, New York, 2012.
31. Bert Chapman, Researching National Security and Intelligence Policy, Washington, DC. CQ Press, 2004.
32. Charles. L. Glaser, Deterrence of Cyber Attacks and U.S. National Security Report G.W. CSPRI, June, 2011.
33. Christian Whiton, Smart Power: Between Diplomacy and War, Washington. D.C. Potomac Book-INC, University of Nebraska Press, 2013.
34. Christopher, P. Twomey, The Military Lens: Doctrine Differences, Misperception, and Deterrence Failure in Sino- American Relations, Massachusetts Institute of Technology, 2005.
35. Cyntha Weber, International Relations Theory: a Critical Inteoduction, 3rd, London, Routledge, 2010.
36. Divya Srikanth, Non-Traditional Security Threats in the 21st Century: A review, International Journal of Development and Conflict, No.2, 2014.
37. Efraim Inbar, Israel's National Security, Issues and Challenges Since the yom Kippur, London, Routledge, 2008.
38. Gideon Rachman, Zero-Sum World, Power and Prosperity After the Grash, Atlantic Books, London, 2010.
39. HQ Integrated Defence Staff, Understanding Military Doctrine A primer, Directorate of Doctrine Training and Doctrine Divison, Military of Defence, New Delhi, 2018.
40. James J. Wirtz (eds), Complex Deterrence Strategy in the Global Age, United States, The University of Chicago Press, 2004.
41. John. J. B Sheldon, Deciphering Cyber Power, Strategic Purpose in Peace and war, air University, Strategiy Studies Quartery, 2011.
42. Jonathan Pinkus, Intelligence and Public Diplomacy: The Changing Tide, Journal of Strategic Security, No.1, 2014.
43. Joseph S. Nye, Cyber Power, Center for Science and International Affairs, Harrard, Kennedy School, 2010.
44. Marcos Degant, Spies and Policy Makers, Intelligence in the Information Age, Intelligence and National Security, No.4, 2016.
45. Matt, Hidek, Military Doctrine and Integrated Intelligence in the City, San Fransico, 2007.

46. Michael Olender, Keeping Pace wkth Cyber Power, Defense and War Fare, Journal of International and Global Studies, No.2, Center for International and Global Studies, Duke University, North Carolina, 2015.
47. Mitko Bogdnoski & Drage Petreski, Cyber Terrorism – Global Security Threat, International Scientific defense, Security and Peace Journal, No.3, 2014.
48. Peter Long, Hays, Struggling Towards Space Doctrine: U.S Military Space Plans, Programs, and Perspectives during the Cold war, Boston, 1994.
49. Prabh Karam, National Security, Imperative and Challenges, New Delhi, Tata Mc Graw, 2008 .
50. R.S. Mcnamara and J. G. Blight, Wilson's Ghost, Reducing the Risk of Conflict, Killing and Cata Stropke in the Century, New York, Public a Hairs, 2001.
51. Richard A. Clarke and Robert Knake, Cuber War, The next Threat to National Security and What to Do about it, Harpercollins e-books, New York, 2010.
52. Robert M. Grant, Contemporary Strategy Analysis, New Jersey, John Wiley and Sons Ltd, 2010.
53. Roland Dannreuther and John Peterson, Security Strategy and Transtlantic Relations, Routledge, New York, 2006.
54. Wyatt Hoffman, Is Cyber Strategy Possible?, The Washington Quarterly, No.1, 2018.
55. Brian Manthe, United States Military Doctrine and the Conduct of Couaterin- surgency Operation: Fixing the Discannect, From:
http://handle.dtic.mil/100-2/APA393508,2001
56. Kenneth J. Knapp, Cyber Security and Global Information Assurance, Thereat Analysis and Response Solions, 2019, from, online,
http://epdf.pub/cyber-security and global-information-sols-9733.html