مجلة جامعة الانبار للعلوم القانونية والسياسية

اسم المقال: أمننة الفضاء السيبراني: دراسة نقدية للدراسات الأمنية السيبرانية
اسم الكاتب: أ.د. أنور محمد فرج محمود، م. فرهاد جلال مصطفى سعيد
رابط ثابت: https://political-encyclopedia.org/index.php/library/9740
تاريخ الاسترداد: 2026/11/01 12:13 +03

الموسوعة السياسيّة هي مبادرة أكاديمية غير هادفة للربح، تساعد الباحثين والطلاب على الوصول واستخدام وبناء مجموعات أوسع من المحتوى العلمي العربي في مجال علم السياسة واستخدامها في الأرشيف الرقمي الموثوق به لإغناء المحتوى العربي على الإنترنت.
لمزيد من المعلومات حول الموسوعة السياسيّة - Encyclopedia Political، يرجى التواصل على info@political-encyclopedia.org

استخدامكم لأرشيف مكتبة الموسوعة السياسيّة - Encyclopedia Political يعني موافقتك على شروط وأحكام الاستخدام المتاحة على الموقع https://political-encyclopedia.org/terms-of-use

تم الحصول على هذا المقال من موقع مجلة جامعة الانبار للعلوم القانونية والسياسية ورفده في مكتبة الموسوعة السياسيّة مستوفياً شروط حقوق الملكية الفكريّة ومتطلبات رخصة المشاع الإبداعي التي ينضوي المقال تحتها.

Journal of Anbar University for Law and Political Sciences
مجلة جامعة الانبار للعلوم القانونية والسياسية
P. ISSN: 2706-5804 E.ISSN: 2075-2024
Volume 15- Issue 2- September. 2025
المجلد ١٥- العدد ٢ – ايلول ٢٠٢٥

The Securitization of Cyberspace: A Critical Study of Cybersecurity Studies

[1] Dr. Anwar Mohammed Faraj[2] Farhad Jalal Mustaffa
College of Political Science - University of Sulaimani

Abstract:

The emergence of cyberspace has created a new challenge for security. This means that security studies need to be updated to include the concept of cybersecurity, which is the output of the securitization of cyberspace. Our research contributes to existing debates about cyber security studies in three main ways. First, this research argues that despite scientific efforts over the past two decades, security studies regarding cybersecurity remains nascent to the extent that they need to be updated, broaden, and even challenging their previous perspectives and understandings. The research contributes to these scientific efforts by identifying the challenges facing this task. Second, the research criticizes the cyber security literature, especially the Hyper securitization of cyber threats and policies. Finally, the research critically analyzes the literature on the concept of cyber security and argues that they have failed to provide an appropriate view of this new concept, which is the gap that the paper finally tries to fill by presenting a new concept of cyber security consistent with the essence of the concept of security.

1: Email:
Anwar.faraj@univsul.edu.iq
2: Email:
Farhad.mustaffa@univsul.edu.iq

DOI
https://doi.org/10.37651/aujlps.2024.154169.1367

Submitted: 1/10/2024
Accepted: 10/10/2024
Published: 1/9/2025

Keywords:
Cybersecurity
security studies
securitization
cyberspace
Hypersecuritization.

©Authors, 2024, College of Law University of Anbar. This is an open-access article under the CC BY 4.0 license (http://creativecommons.org/licenses/by/4.0/).

أمننة الفضاء السيبراني: دراسة نقدية للدراسات الأمنية السيبرانية

[١] أ.د.أنور محمد فرج محمود [٢] م.فرهاد جلال مصطفى سعيد
[١] كلية العلوم السياسية - جامعة السليمانية

الملخص:

لقد خلق ظهور الفضاء السيبراني تحديًا جديدًا للأمن، وهذا يعني أن الدراسات الأمنية بحاجة إلى التحديث لتشمل مفهوم الأمن السيبراني كمخرج لأمننة الفضاء السيبراني. يساهم بحثنا هذا في المناقشات القائمة حول دراسات الأمن السيبراني بثلاث طرق رئيسة. أولاً، يجادل هذا البحث أنه على الرغم من الجهود العلمية على مدى العقدين الماضيين، فإن الدراسات الأمنية المتعلقة بالأمن السيبراني لا تزال ناشئة إلى الحد الذي تحتاج إلى التحديث والتوسيع وحتى تحدي وجهات نظرها السابقة. ويساهم البحث هنا من خلال تحديد التحديات التي تواجه هذه المهمة. ثانيًا، ينتقد البحث أدبيات الأمن السيبراني، وخاصة من ناحية الإفراط في أمننة التهديدات والسياسات السيبرانية. ثالثاً وأخيرًا، يحلل البحث بشكل نقدي الأدبيات حول مفهوم الأمن السيبراني ويجادل بأنها فشلت في تقديم وجهة نظر مناسبة لهذا المفهوم الجديد، وهي الفجوة التي تحاول الدراسة سدها من خلال تقديم مفهوم جديد للأمن السيبراني متسق مع جوهر مفهوم الأمن ذاته.

الكلمات المفتاحية: الأمن السيبراني؛ الدراسات الأمنية؛ الأمننة؛ الفضاء السيبراني؛ الأمننة المفرطة.

المقدمة

لقد خلق ظهور الفضاء السيبراني وسطاً جديداً للتفاعلات الدولية بين الجهات الفاعلة المختلفة من دول وغير الدول، ونشأ معه تحديًا جديدًا للأمن، وذلك كمخرج لأمننة الفضاء السيبراني. وهذا يعني أن الدراسات الأمنية بحاجة إلى التحديث إستجابةً للتطورات الناشئة المتعلقة بقضية الأمن، وأبرزها الأمن السيبراني.

يعد الأمن السيبراني بعدًا أساسيًا في العالم المعاصر، وهذا لا يجعل التعامل معه مشكلة عملية فقط بل وايضاً مشكلة تحليلية صعبة. ومن هذا المنطلق، تتجه دراسة الأمن السيبراني إلى إحتلال مكانة بارزة في الدراسات الأمنية المعاصرة.

وعلى الرغم من الإستخدام الواسع نسبياً في الوقت الراهن لمصطلح "الأمن السيبراني" من قبل الممارسين والتقنيين والسياسيين، ومع ذلك، يبدو أن هناك القليل جدًا من الفهم لما ينطوي عليه المصطلح حقًا، وخاصة من الناحية البحثية حيث لم يَحسِم الباحثون جدلهم بعدُ بشأن ماهية الأمن السيبراني، وهذا يدل على أن الموضوع يستحق اهتماماً أكبر.

أولاً: أهمية البحث:

تبرز أهمية البحث من ناحيتين:

أهمية موضوع البحث؛ وذلك ليس لكونه موضوعاً جديداً نسبياً فقط، وإنما أيضاً لثقل تأثيره في السياسات الدولية الراهنة. فبسبب تطور سيبرنة العلاقات الدولية وبسبب الأهمية المتزايدة للفضاء السيبراني للسياسة الدولية المعاصرة والأنشطة الاقتصادية والاجتماعية العالمية، هناك حاجة عميقة لعلماء السياسة والباحثين في العلاقات الدولية لتحديد ووصف وشرح هذه التطورات والآفاق والتحديات الناشئة نظريا وتجريبيا بطريقة دقيقة. ويكتسي البعد الأمني في العلاقات السيبرانية الدولية أهمية بالغة من هذه المهمة وذلك لأن أمننة الفضاء السيبراني أي اضفاء الطابع الأمني على الفضاء السيبراني أحد أبرز ملامح التفاعلات العالمية اليوم.

أهمية ذاتية للبحث أي المساهمة العلمية للبحث؛ وتتجسد تلك على وجه الخصوص في الجهد الذي بذل، قدر المستطاع، من أجل الكشف عن القصور في بعض من الآراء و التصورات الواردة في أدبيات الدراسات الأمنية السيبرانية وإنتقادها، كما تتجسد في التقدم بتعريف خاص بالبحث لمفهوم الأمن السيبراني.

ثانياً: إشكالية البحث:

يتطور التكنولوجيا بإستمرار ويتطور بالتوازي معها تهديدات جديدة، فمع تطور تكنولوجيا المعلومات والإتصالات وظهور الفضاء السيبراني، تطورت تهديدات سيبرانية والتي بدورها اثارت موضوع الأمن السيبراني. ومن هنا تتبلور إشكالية البحث و التي تتمثل في التساؤل الرئيسي : كيف إنعكست عملية أمننة الفضاء السيبراني في الدراسات الأمنية؟

إلى جانب التساؤل الرئيسي اعلاه، ثمة تساؤلات فرعية مقترنة بجوهر موضوع البحث، منها: كيف يتم بناء العلاقة بين الفضاء السيبراني والعلاقات الدولية؟ ماهي مواطن النقص في أدبيات الدراسات السيبرانية؟

ثالثاً: فرضية البحث:

الفرضية الأساسية التي حاول البحث التثبت من صحتها تنطلق من فكرة مفادها "إن إضفاء الطابع الأمني على الفضاء السيبراني بالكيفية التي تجسدته الدراسات الأمنية افضت إلى اتسام هذه الدراسات بالمبالغة والإفراط في تصور التهديدات السيبرانية"

رابعاً: مناهج البحث:

يستخدم هذا البحث منهجين:

١. المنهج الوصفي التحليلي: لبيان المقصود بالأمن السيبراني.

٢. المنهج النقدي: للوقوف على المبالغة والإفراط في أمننة التهديدات السيبرانية

خامساً: هيكل البحث:

يتضمن البحث مقدمة عامة، ثلاثة مطالب، وخاتمة عامة.

يتناول المطلب الأول، الفضاء السيبراني والعلاقات الدولية، والذي سينصرف الى معالجة كيفية تجسير العلاقة بين الإثنين. أما المطلب الثاني الذي يحمل عنوان: الأمن السيبراني في الدراسات الأمنية : أمننة الفضاء السيبراني، فهو يتناول، من خلال فرعين مستقليين، ضرورة تجديد وتطور الدراسات الأمنية سبيلاً لمجاراة التطورات التكنولوجية المعاصرة وظهور الفضاء السيبراني وعواقبه أمنياً كنتيجة لأمننة هذا الفضاء. ويذهب المطلب الثالث والأخير الى الحديث عن ماهية الأمن السيبراني، ويتم فيه عرض وإنتقاد

مفاهيم مطروحة للأمن السيبراني وينتهي بإقتراح تعريف جديد للمفهوم.

I. المطلب الأول

الفضاء السيبراني والعلاقات الدولية

أن وجود علاقة بين العلم والأمن أمر لاشك فيه، وتأريخياً كانت الحاجة إلى زيادة القدرة العسكرية دافعاً مهماً للإستثمار في العلم والتكنولوجيا(١). ولايزال هذا الدافع قائماً إلى يومنا هذا.

ومن المعلوم أن العلم متجدد بطبعه، سواءً كان إجتماعياً أو طبيعياً، ولهذا مخرجات على قضية الأمن، وتأثيرات بأشكال مباشرة أو غير مباشرة في أنماط التفاعلات بين الدول وغيرها من الفاعلين. في السابق أدى التقدم العلمي والتكنولوجي في وسائل الملاحة البحرية، والطائرات، والأقمار الصناعية والصواريخ المرسلة إلى الفضاء الخارجي، إلى تحولات كبيرة ليس في بعدها الجغرافي فحسب، بل أيضاً في توازنات القوة الدولية وبنية النظام السياسي الدولي. ومن المتوقع أن يفضي التقدم التكنولوجي السيبراني اليوم بدوره إلى مخرجات مهمة في العلاقات الدولية.

من هنا تثار تساؤلات عن التجديد الذي يحتاجه حقل العلاقات الدولية في ضوء متغيرات يشهدها العالم. وبالطبع السؤال عن ضرورة التجديد في فرع الدراسات الأمنية بحيث يستوعب قضايا ومتغيرات جديدة أو متجددة. وربما قول (إدوارد أ. كولودزيج' Edward A. Kolodziej) هنا دقيق جداً بأنه "من الصعب على المراقبين والباحثين المتمرسين، وخاصة على الجمهور المستنير، مواكبة الأحداث السريعة التغير، ولا سيما تلك التي تؤثر على الأمن"(٢).

أدرك الباحثون منذ عقود ضرورة سد الفجوة بين الخبرة التكنولوجية وخبرة العلوم الاجتماعية(٣)، من ضمنها العلوم السياسية. فمع بروز ثورة تكنولوجيا المعلومات والإتصالات، حدثت طفرة في أهمية التكنولوجيا والعلم في الحياة السياسية، ومعها بدأت دراسات في تسعينيات القرن العشرين تتناول قضايا التكنولوجيا والسياسة، وعلى وجه الخصوص في ظل تيار أطلق عليه (دراسات العلم والتكنولوجيا' Science and Technology Studies) (STS)(٤) والذي ركز في مشاريعه البحثية على التعاون بين

---

(١). إيان أنطوني، *مقدمة: الأمن الدولي، والتسلح، ونزع السلاح، في: معهد ستوكهلم لأبحاث السلام الدولي (سيبري)، التسلح ونزع السلاح والأمن الدولي (الكتاب السنوي ٢٠١٤)*، تر: عمر سعيد الأيوبي و أمين سعيد الأيوبي، (بيروت: مركز دراسات الوحدة العربية، ٢٠١٤)، ٤٢.

(2). Edward A. Kolodziej, *Security and International Relations*, (Cambridge: Cambridge University press, 2005), 11.

(3). Johan Eriksson and Giampiero Giacomello, Cyberspace in Space: Fragmentation; Vulnerability; and Uncertainty, in: Myriam Dunn Cavelty and Andreas Wenger (eds.), *Cyber Security Politics Socio-Technological Transformations and Political Fragmentation*, (London & New York: Routledge, 2022), 105.

(٤). سوزي رشاد، "التهديدات الأمنية الهجين في العلاقات الدولية: السيبرانية والذكاء الأصطناعي نموذجاً"، *مجلة وادي النيل للدراسات والبحوث الإنسانية والإجتماعية والتربوية*، ٣٣، (كانون الأول ٢٠٢٢)، ٦٦٤. و

المجالات المتنوعة من العلوم من ضمنها البحث عن تأثير العلم والتكنولوجيا على مختلف التخصصات بما فيها تخصص العلوم السياسية، والعلاقات الدولية.

لعل من أهم المشاريع البحثية في هذا الإطار هو المشروع البحثي متعدد التخصصات تحت العنوان (استكشافات في العلاقات الدولية السيبرانية' Explorations in Cyber International Relations) الذي يقوم به تعاونياً (معهد ماساتشوستس للتكنولوجيا' Massachusetts Institute of Technology) و(جامعة هارفارد' Harvard University) والمعروف إختصاراً بـ (MIT-Harvard ECIR) بموجب منحة من (مبادرة مينيرفا' Minerva Initiative) بوزارة الدفاع الأمريكية. يساهم في المشروع مجموعة من الباحثين المختصيين في العلوم السياسية، العلوم الحاسوب والهندسة، الأعمال والإدرة، علوم التكنولوجيا، الحكومة والقانون. ومن أبرز الباحثين المشاركين بالمشروع الباحثة (نازلي شكري' Nazli Choucri)[١]، والتي يتم تحت إشرافها انجاز المشروع[٢]. يحاول المشروع استكشاف جوانب مختلفة من العلاقات الدولية السيبرانية، بما فيها آثار الظاهرة السيبرانية على القوة، السياسة، الصراع والحرب[٣].

وعلى العموم ظهرت مفاهيم تعبر عن الدمج بين التكنولوجيا والأمن، على سبيل المثال فقط وليس الحصر اخترع الأكاديمي الفرنسي في مجال الإعلام والإتصال (أرمان ماتلار' Armand Mattelart) مصطلح (نموذج تكنو-أمني' Tenchnosecurity Paradigm) في كتابه (المراقبة الشاملة: أصل النظام الأمني) المنشور سنة ٢٠١٠[٤]. كما صاغ (جوتا ويبر' Jutta Weber) و(كاترين م. كامبف' Katrin M. Kampf) مفهوم (ثقافة التكنو-الأمني' Technosecurity Culture)[٥].

هكذا ظهرت محاولات لسد الفجوة بين دراسات العلم والتكنولوجيا وأدبيات العلاقات الدولية، إلا أن الأمر بحاجة إلى جهد أكثر وعلى وجه الخصوص ضمن حقل العلاقات الدولية وفرع الدراسات الأمنية.

كذلك: Tanja Bogusz, "Fieldwork in the Anthropocene: on the Possibilities of Analogical Thinking between Nature and Society", *Since & Technology Studies*, 36:2, (September 2023), 5.

(١). استاذة العلوم السياسية بمعهد ماساتشوستس للتكنولوجيا في الولايات المتحدة الأمريكية وهي مصرية الأصل.

(٢). انطلق المشروع في عام ٢٠٠٩ ومنذ ذلك الحين انجزت ١٧٦ عملاً منشوراً من مواقع الكترونية وأوراق عمل وبحوث ومقالات وكتب وتقارير وغيرها. للمزيد من المعلومات حول المشروع يمكن الرجوع للموقع الإلكتروني الخاص به على الرابط: https://ecir.mit.edu

(3). Nazli Choucri (Preparator), Explorations in Cyber International Relations: A Research Collaboration of MIT and Harvard University, (Cambridge and Mass: MIT Press, 2015).

(٤). أرمان ماتلار، *المراقبة الشاملة: أصل النظام الأمني*، تر: ريمون شاهين، (بيروت: شركة المطبوعات للتوزيع والنشر، ٢٠١٣)، ١٨٩ وما بعدها. ويشرح الكتاب تنامي الأمن واجهزته وأساليب المراقبة والملاحقة عن طريق التكنولوجيا.

(5). Jutta Weber and Katrin M. Kampf, "Technosecurity Cultures: Introduction", *Science as Culture*, 29:1 (March 2020): 1-10.

يقترح الكاتب هنا فهم العلاقة الحالية بين التكنولوجيا والأمن باعتبارها ثقافة تكنوأمنية تتشكل بشكل عميق من خلال تأثير تقنيات المراقبة وتحديد الهوية عالية التقنية. يمكن الرجوع إلى الصفحة رقم ٤ من المرجع المذكور أعلاه.

ففي عام ٢٠١٤ أشار الباحثان (جان فريدريك كريمر ‘ Jan-Frederik Kremer) و (بنديكت مولر ‘ Benedikt Muller) أنه على الرغم من الإنتشار المتزايد للفضاء السيبراني وآثاره الواضحة على السياسة الدولية والنشاط الاقتصادي العالمي والعلاقات الاجتماعية عبر الوطنية، إلا أنه لا تزال هناك نقطة غائمة في البحث فيما يتعلق بمعالجة هذه الآثار نظريًا وتجريبيًا في إطار شامل وواسع[١]. بالطبع الباحثان مطلعان على وجود عدد كبير من المقالات والكتب حول القضايا المتعلقة بأمن الفضاء السيبراني ولكن يؤكدان على إنها لم تكن بمستوى الآثار المترتبة على عملية (سيبرنة العلاقات الدولية‘ cyberization of international relations)[٢].

و في عام ٢٠٢٣ يسجل البعض نفس الملاحظة أو التقيم السابق بوجود نقص ملحوظ في التحليلات البحثية في الأدبيات الموجودة حول الأمن السيبراني، والذي يرجع جزئيًا إلى التطور السريع للتكنولوجيا السيبرانية التي بدأت العديد من العمليات، والتي لم تظهر آثارها جميعها على الفور، كما أن تأثيرها على الحياة السياسية أو الاقتصادية أو الاجتماعية ليس مفهومًا تمامًا[٣].

عليه فمنذ قرابة عقدين من الزمن بدأ الإهتمام التحليلي بالأمن السيبراني، وطوال تلك المدة يظهر الباحثون بإستمرار ويقرون بوجود فجوة بحثية حول الموضوع ويحاولون سدها، ولكن تظهر بعدها فجوة أُخرى ويأتي آخرين وهم على نفس المنوال. وهكذا تظل الحاجة لتحديد ووصف وشرح هذه التطورات والآفاق والتحديات الناشئة نظريا وتجريبيا بصورة أعمق مستمرة لعلماء السياسة والباحثين في العلاقات الدولية.

ويرجع ذلك برأينا للحقائق الآتية:

أولاً: لم تكتشف بعد كل الأبعاد المخفية للظاهرة السيبرانية ذاتها، بل لاتزال في طور التغيير والتطور والتحول، مما يعني تغيُّر آثارها وعواقبها وتبعاتها على الدوام.

ثانياً: عدم توصل الفاعلين الدولين، وعلى وجه الخصوص الدول وأكثر تحديداً الدول الكبرى، إلى إتفاق بل وتفاهم مشترك حول كيفية التعامل مع الفضاء السيبراني في قضايا كثيرة وفي مقدمتها كيفية إدارة الفضاء السيبراني، والسيادة السيبرانية، والهجمات السيبرانية والرد عليها وغيرها.

ثالثاً: على المستوى النظري، لم تصل الجهود العلمية لحد الآن إلى نشوء مفاهيم عامة وطروحات نظرية وفرضيات علمية قابلة للإختبار والتعميم في إطار نظرية أو مدرسة فكرية خاصة بالأمن السيبراني على غرار المدارس الفكرية الأخرى ضمن فرع الدراسات

(1). Jan-Frederik Kremer and Benedikt Müller (eds.), *Cyberspace and International Relations: Theory, Prospects and Challenges*, (Heidelberg: Springer, 2014), xi.

(٢). تشير سيبرنة العلاقات الدولية إلى الاختراق المستمر لجميع مجالات نشاط العلاقات الدولية المختلفة من خلال وسائل مختلفة للفضاء السيبراني من جهة، والاعتماد المتزايد للفاعلون في العلاقات الدولية على البنية التحتية والأدوات والوسائل التي يوفرها الفضاء السيبراني من جهة أخرى. يمكن مراجعة Ibid .

(3). Marek Górka, “Conceptualising Securitisation in the Field of Cyber Security Policy”, *Journal of Modern Science*, 53(4) (December 2023): 265.

الأمنية[١]. فكل ما موجود بهذا الشأن هي بحوث في إطار الدراسات الأمنية السيبرانية وهي محدودة من حيث إرتباطها بتعقيدات الفضاء السيبراني. والنتيجة هي ميل للتركيز على الأحداث العنيفة، كالهجوم السيبراني الروسي على استونيا في ٢٠٠٧، و الهجوم السيبراني على إيران عن طريق دودة ستوكسنت Stuxnet في ٢٠١٠ مع غياب أو ندرة دراسات الحالة المقارنة.

انطلاقاً من الوقائع المعطاة، المطلوب هو التركيز على التقدم نحو تطوير أُسس نظرية تجاوز وصف الأحداث الغامضة أحياناً والناقصة لأدلة كافية، لأن الفجوة الحالية في البحوث والدراسات تمنع التقدم الفكري للعلاقات الدولية. فالحوادث السيبرانية تحدث بتواتر مستمر، وفي المقابل، هناك عجز نظري أو غير كافي لتفسيرها وتحليل تأثيرها على السياسات الأمنية الوطنية والدولية. وربما من المفيد في هذا المسار ان يتم توسيع آفاق البحث نحو المزيد من الإهتمام بالطابع غير الحكومي/الرسمي في السياسات الوطنية والعالمية في المجال السيبراني وذلك لتنامي دور الفاعلون غير الحكوميين وعلى وجه الخصوص الشركات العملاقة في هذا المجال.

II. المطلب الثاني

الأمن السيبراني في الدراسات الأمنية : أمننة الفضاء السيبراني

يرمي هذا المطلب إلى الحديث عن ماتوصل إليه الدراسات الأمنية ومكانة الأمن السيبراني فيه. ويحاول المطلب الإجابة عن التساؤل: مالذي يمكن أن تخبرنا أدبيات الدراسات الأمنية حول الأمن السيبراني؟ ويتم ذلك خلال فرعين مستقليين.

II.أ. الفرع الأول

الدراسات الأمنية: التقليدية والتوسعية

على الرغم من أن التفكير بمسألة الأمن وتناولها تعود إلى زمن بعيد، إلا أن تطور دراستها ضمن فرع علمي في إطار حقل العلاقات الدولية بدأت بعد الحرب العالمية الثانية وأكثر تحديداً في خمسينيات القرن العشرين تحت تسمية **(الدراسات الأمنية)** والتي تميزت بدراسة التهديدات واستخدام القوة العسكرية و ضبطها[٢]. مرت الدراسات الأمنية منذ ذلك الحين بموجات ومراحل تطور متنوعة يتنازع فيها على مفهوم الأمن، مرجع الأمن، القيم المهددة، طبيعة التهديدات، مصادر التهديد، وكذلك السياسات الأمنية.

وبهذا الصدد يتم التميز بصورة عامة بين اتجاهين مختلفين: **اتجاه التقليدي** و**اتجاه الحديث** (التوسعي).

ينتمي **الإتجاه التقليدي** إلى النظرية الواقعية وهيمن على الدراسات الأمنية إبان الحرب الباردة وينظر إلى الدولة بوصفها أقوى فاعل بالنظام الدولي، و للأمن أولوية مطلقة

(١) . كمدارس: كوبنهاجن، و باريس، وأبريستويث في الدراسات الأمنية.

(2). Ali Muhammad and Sugeng Riyanto, "International Security Studies: Origins, Development, and Contending Approaches", *Austral: Brazilian Journal of Strategy & International Relations*, 10:20 (December 2021): 230.

بالنسبة للدولة[١]. كما ارتبط الأمن في المنظور التقليدي بكيفية استعمال الدولة لقوتها العسكرية[٢]، من أجل حماية القيم والمصالح الحيوية للدولة[٣]، وفي مواجهة التهديدات الخارجية[٤].

هكذا درجت تقليدياً تحاليل الأمن على التركيز على البعد العسكري دون الحاجة لتوسيع مفهوم الأمن. وقد يلاحظ تناول بعض التقليديين تطور تكنولوجيا المعلومات، ولكن فقط فيما يتعلق بالتعزيز التكنولوجي للقدرات العسكرية، وبالتالى فإن تكنولوجيا المعلومات، بالنسبة لمعظم التقليديين، هي مجرد إضافة جديدة لابأس بها[٥].

يدعي الإتجاه الحديث، الذي يمثل مزيجًا من الليبراليين والمنظرين النقديين، أن مفهوم الأمن يجب أن يتسع (أفقياً Horizontally) و(عمودياً Vertically) ليشمل تهديدات وتحديات جديدة، سياسية، ثقافية، إجتماعية إقتصادية وبيئية[٦]. فضلاً عن إضافة جهات فاعلة أخرى من غير الدول كأطراف معنية بالأمن، ولا سيما المنظمات الدولية، والجماعات الإثنية، والمنظمات الإرهابية، والشركات الخاصة، والأفراد.

ومن المثير للدهشة، نادراً ما تناول الإتجاه التوسعي ثورة المعلومات وتأثيرها على الأمن، إذ تغطي مفاهيمه الأمنية الموسعة عادةً القضايا الاقتصادية والبيئية والسياسية والثقافية[٧].

انطلاقاً من هذه المعطيات، لم يحظ الأمن السيبراني قبل عقدين من الزمن بالإهتمام الكافي لا في عالم السياسة كقضية دولية، مثلما أشار اليه (جوزيف ناي Joseph S. Nye)[٨] ولافي الجانب النظري في حقل العلاقات الدولية كما أكد عليه (إريكسون Eriksson)

---

(١). محمد عبدالقادر حاتم، *العولمة: مالها وماعليها*، (القاهرة: الهيئة المصرية العامة للكتاب، ٢٠٠٥)، ١٩٢.

(٢). فرهاد جلال مصطفى، *الأمن ومستقبل السياسة الدولية*، (السليمانية: أكاديمية التوعية وتأهيل الكوادر، ٢٠١٠)، ٣٤.

(٣). عبدالرحمن احمد الدوري، "الامن القومي العربي: المفهوم- التحديات- المواجهة"، *مجلة الدفاع*، ٤ (١٩٨٨): ص١٤١-١٤٢.

(٤). فاضل البراك، *استراتيجية الامن الداخلي*، (بغداد: دار الحرية للطباعة، ١٩٨١)، ٨٢. و مازن اسماعيل الرمضاني، "الامن القومي العربي و الصراع الدولي"، *مجلة العلوم السياسية*، ٢ (١٩٨٨): ٦٣.

(5). David J. Lonsdale, "Information Power: Strategy, Geopolitics, and the Fifth Dimension", *Journal of Strategic Studies*, 22(2–3) (1999): 143.

(6). Nils Petter Gleditch, "Environmental Change, Security, and Conflict", in: Chester A. Crocker, Fen Oster and Pamela Aall (eds.), *Turbulent Peace: The Challenges of Managing International Conflict*, (Washington DC: United States Inst of Peace Pr., 2001), 53-54.

(7). Johan Eriksson and Giampiero Giacomello, "Closing the Gap between International Relations Theory and Studies of Digital-age Security", in: Johan Eriksson and Giampiero Giacomello (eds.), *International Relations and Security in the Digital Age*, (London and New York: Routledge, 2007), 11.

(8). Joseph S. Nye, "How Will New Cybersecurity Norms Develop," *Project Syndicate*, March 8, 2018, https://www.project-syndicate.org/commentary/origin-of-new-cybersecurity-norms-by-joseph-s--nye-2018-03?barrier=accesspay (accessed June 25, 2022).

و(جياكوميلو، Giacomello) في عام ٢٠٠٧[١].

لكن اليوم لم تعد هذه الملاحظة صحيحة، لأن الأبحاث التي تطبق الأدوات النظرية في العلاقات الدولية وطروحات الدراسات الأمنية على جوانب مختلفة من الظاهرة السيبرانية لم تعد نادرة. وذلك نتيجة توسع انتشار الظاهرة على الدوام وتجرياتها والتزايد المستمر لتأثيراتها المتنوعة والمتباينة. فمن المعروف أن التغييرات في البحث مرتبطة بالتغييرات في الظاهرة التجريبية، حيث يمكن لهذه التغييرات أن تسير في كلا الاتجاهين: غالبًا ما تؤثر ظاهرة البحث على اتجاهات البحث، ولكن البحث يسلط الضوء أيضًا على جوانب الظاهرة التي مرت دون أن يلاحظها أحد من قبل. ولذلك نلاحظ وجود نقاشات بين عالم السياسة والأوساط الأكاديمة حتى بدرجة أكبر منها بين الباحثين الأكاديمين أنفسهم حول ما إذا كانت السيبرانية تغير قواعد اللعبة بالنسبة للبيئة الأمنية الدولية[٢].

من هنا نحن مدعُوين لإلقاء نظرة على ولوج الأمن السيبراني إلى الدراسات الأمنية وتبدأ ذلك اولاً وقبل كل شيء بأمننة الفضاء السيبراني.

II.ب. الفرع الثاني

الدراسات الأمنية السيبرانية: نحو أمننة الفضاء السيبراني

إن (**الأمننة**، Securitization) مفهوم قدمته مدرسة كوبنهاجن في الدراسات الأمنية في منتصف تسعينيات القرن الماضي وارتبط بشكل كبير بالتفاعلات في العلاقات الدولية إلى جانب الإضطرابات الداخلية للدول. كما أصبحت الأمننة نظرية يستخدمها الباحثون في وجه الأساليب التقليدية للدراسات الأمنية بشكل أساسي.

لقد تم تطوير نظرية الأمننة استجابة للحاجة إلى توسيع الدراسات الأمنية بعد الحرب الباردة، وهي تقدم طريقة لدراسة الأمن باعتباره نتاجًا لخطابات وممارسات اجتماعية وسياسية معينة. إذن الفكرة من وراء الأمننة هي إعطاء القضية وزناً كافياً لكسب موافقة الجمهور، وهو ما يمكن السلطة من استخدام أي وسيلة تراها مناسبة. بمعنى آخر، تجمع الأمننة بين سياسة تصميم التهديد وسياسة إدارة التهديد[٣].

اصبحت الأمننة لدى البعض بمثابة (**النموذج المثالي**، Ideal Type)[٤] يلجأ اليه الباحثون للتحليل في القضايا الأمنية[٥]. وتعني الأمننة النظر إلى قضية الأمن بوصفها بناء

(1). Eriksson and Giacomello, Closing the Gap …, 236.

(2). Michael C. Horowitz, "Do Emerging Military Technologies Matter for International Politics," *Annual Review of Political Science*, 23, (May 2020): 392.

(3). Thierry Balzacq, "A Theory of Securitization: Origins, Core Assumptions, and and Variants," in: Thierry Balzacq (ed.), *Securitization Theory: How Security Problems Emerge and Dissolve*, (London and New York: Routledge, 2011) 3.

(٤). بالدلالة التي صاغها عالم الإجتماع الألماني ماكس فيبر.

(5). Lance Caldwell, "Cybersecurity as a Human Right: A Reformulation of the Theoretical Framework of Securitization Theory," (PhD Dissertation, Northcentral University/School of Business, 2021), 30-31.

إجتماعي يمكن تأسيسه خلال (فعل خطابي' Act of speech) [١]. يمكن فعلًا خطابيًا محددًا أن ينجح في ظل ظروف معينة، وتحديدًا في المواقف التي يستخدم فيها الفاعل الأمني خطاب التهديد الوجودي وبالتالي يكون له آثار سياسية كبيرة[٢].

عليه، وبالنسبة إلى قضية الأمن في الفضاء السيبراني فإن الأدبيات الأكاديمية حول السيبرانية، على النقيض من التوجهات الواقعية للأدبيات السياسية، هي في الغالب بنائية. تركز هذه الأدبيات في الغالب على كيفية تسهيل الفضاء السيبراني لانتشار الأفكار التحويلية التي يمكن أن تؤدي إلى تغييرات في الهوية والتصورات التي تهدد بتعطيل النظام الاجتماعي القائم. كما تتناول هذه الأدبيات الطريقة التي يتم بها تفسير هذه العملية على أنها تهديد للأمن القومي. ومن هنا تاتي دور نظرية الأمننة لإضفاء الطابع الأمني للفضاء السيبراني.

هناك من ينظر إلى أمننة الفضاء السيبراني كـ"عملية تحويل أمن الفضاء السيبراني إلى شأن أمني وطني"[٣]. وهذا مايتجلى في تصورات وخطابات رسمية للدول حول التهديدات السيبرانية وانعكاسها في إستراتيجياتها القومية وسياساتها الداخلية والخارجية تجاهها.

سوف يقوم الفاعلون بإضفاء الطابع الأمني على المشاكل وفقًا لتصوراتهم أو أجنداتهم. على سبيل المثال، في حين قد تؤكد إحدى الدول أن هناك تهديدًا وجوديًا يفرضه هجوم الحرمان من الخدمة على بنيتها التحتية المصرفية الهشة، قد تسلط دولة أخرى الضوء على قضايا مختلفة جوهريًا. قد يدرج البعض التهديدات من مواقع الويب التي تنتقد الأنظمة الحكومية لتكون جزءًا من أمن الفضاء السيبراني[٤].

تفضل الولايات المتحدة وغيرها من الديمقراطيات الليبرالية شبكات الاتصال المفتوحة، وعرض الأفكار، وتنظر إلى الفضاء السيبراني -مع بعض الاستثناءات- في المقام الأول كمورد مشترك بين القطاعين العام والخاص. من ناحية أخرى، تركز الصين وروسيا ومعظم الدول الاستبدادية وغير الديمقراطية بشكل أكبر على "أمن المعلومات"، والذي يطابق بشكل عام أمن النظام. تميل هذه الدول إلى فرض ضوابط إقليمية على الفضاء السيبراني، وترى أن التهديدات الأساسية تأتي من دول أخرى ومن الحركات المنظمة المناهضة للنظام. وهم يميلون أيضاً إلى رؤية اختلال التوازن المنحاز نحو مصالح الولايات المتحدة وحلفائها في ترتيبات إدارة الفضاء السيبراني القائمة، وهو ما أدى تقليدياً إلى التوتر في شبكة الإنترنت

---

(١). محمد مسعد العربي، "نظرية الأمننة وتصاعد الجدل حول التوسع في مفهوم الأمن،" *مجلة اتجاهات الأحداث* ٨ (مارس ٢٠١٥):٤.

(2). Barry Buzan, Ole Wæver and Jaap de Wilde, *Security: A New Framework for Analysis*, (Boulder: Lynne Rienner,1998), 24-25.

(٣). فنسنت بولانان، "الأمن الإلكتروني وصناعة الأسلحة،" في: معهد ستوكهلم لأبحاث السلام الدولي (سيبري)، *التسلح ونزع السلاح والأمن الدولي (الكتاب السنوي ٢٠١٣)*، (بيروت: مركز دراسات الوحدة العربية، ٢٠١٣)، ٣٠١؛ Marek Górka, Conceptualising Securitisation in the Field of …, op. cit., 269.

(4). Forrest Hare, "Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security," in: Christian Czosseck and Kenneth Geers (eds.), *The Virtual Battlefield: Perspectives on Cyber Warfare*, (Amsterdam: IOS Press, 2009), 3:90.

الدولية ومنتديات الإدارة الأخرى[١]. فمثلاً ترى روسيا أن تقويض الأنظمة الاقتصادية والاجتماعية للدولة والتلاعب النفسي بالسكان بغرض زعزعة استقرار المجتمع هي إحدى مكونات أمن المعلومات الدولي[٢].

ومع ذلك، فإن مثل هذا التقسيم لايعطينا الصورة النهائية للنظر إلى الفضاء السيبراني من قبل الحكومات. على سبيل المثال، فمع ميل الصين إلى المراقبة الإقليمية- أي المحلية- على خدمات الإنترنيت[٣]، تعتمد في الوقت ذاته على شبكة الإنترنت المفتوحة لأسباب اقتصادية واجتماعية، ويجب عليها أن تسير بشكل يضمن من ناحية سيطرة الدولة ومن ناحية أخرى دون تنفير شعوبها، أو تخويف استثمارات القطاع الخاص، أو تأجيج عدم الاستقرار الدولي[٤]. على نحو مماثل، بذلت الولايات المتحدة الأمريكية وحلفاؤها في قلب الديمقراطية الليبرالية جهوداً هائلة لإجبار الشركات الوطنية على التواطؤ حول الضوابط على المعلومات، وأثبتت قدرتها على تعطيل الشبكات وتخريبها وحظرها عندما يعتبرون أن اعتبارات أمنية وطنية أو مؤسسية تبرر ذلك[٥].

هذه المعطيات صحيحة ايضاً للدول الأخرى، مع مراعاة التباين في الدرجة، حيث يؤكد الباحث البولندي (**ماريك جوركا**' Marek Górka) أنه في جميع أنحاء العالم، تفرض الدول سيطرتها على الفضاء السيبراني للتأكد من أن المحتوى الموجود فيه يناسب مصالحها الداخلية والخارجية[٦]. وبعبارة أخرى، على الرغم من اختلاف خطابها وفلسفاتها السياسية الأساسية، فإن معظم الحكومات تتحرك في نفس الاتجاه العام وهو زيادة سيطرة الدولة على الفضاء السيبراني داخل الحدود الإقليمية الوطنية. لذلك تعد تنقية أو تصفية محتوى الإنترنيت إحدى السمات الأساسية لأمننة الفضاء السيبراني والتي يتوسع على الدوام على الصعيد العالمي، بغض النظر عن اختلاف مبررات تنفيذ التصفية من بلد إلى آخر، كما يختلف المحتوى المستهدف للحجب[٧].

لم يتوقف التدخل الحكومي في الفضاء السيبراني عند تصفية الإنترنت، بل أظهرت

---

(1). Ronald Deibert, Cyber-Security, in: Myriam Dunn Cavelty and Thierry Balzacq (eds.), *Routledge Handbook of Security Studies*, 2nd ed., (London and New York: Routledge, 2017), 318.; Karen A. Mingst and Ivan M. Arreguin-Toft, *Essentials of International Relations*, 7th ed., (New York and London: W. W. Norton & Company, 2017), 428.

(2). Forrest Hare, Borders in Cyberspace …, Op. cit., 90.

(٣) باتريك هـ أونيل، *مباديء علم السياسة المقارن*، تر: باسل جبيلي، (دمشق: دار الفرقد للطباعة والنشر والتوزيع، ٢٠١٢)، ص٧٠.

(4) . Ronald Deibert, Cyber-Security, Op. cit., 318.

(5). Ibid.

(6). Marek Górka, Conceptualising Securitisation in …, Op. cit., 270.

(٧). يبرر بعض الدول تصفية الإنترنت للتحكم في الوصول إلى المحتوى الذي ينتهك حقوق الطبع والنشر، أو يتعلق بالاستغلال الجنسي للأطفال، أو يشجع على الكراهية والعنف. وتقوم بلدان أخرى بتصفية الوصول إلى المحتوى المتعلق بحقوق الأقليات والحركات الدينية والمعارضة السياسية وجماعات حقوق الإنسان. وعلى سبيل المثال فقط وليس الحصر، رداً على مقطع فيديو مثير للجدل اعتبر تشهيراً بالإسلام، قامت باكستان لعدة سنوات بحظر الوصول إلى الإنترنت على منصة يوتيوب بالكامل، فضلاً عن المحتوى السياسي والمتعلق بحقوق الإنسان والمتعلق بالأمن. تقوم تايلاند بتصفية أي محتوى يعتبر مسيئًا أو مهينًا للعائلة المالكة بموجب قوانين. ولمعلومات أكثر يمكن الرجوع لطفاً الى:

Ronald Deibert, Cyber-Security, Op. cit., 319.

الحكومات استعداداً أكبر لاستخدام نطاق أوسع من الوسائل، بما في ذلك التكتيكات السرية والهجومية، لتشكيل الفضاء السيبراني بما يخدم مصالحها الاستراتيجية. على سبيل المثال، كان هناك عدد متزايد من الحوادث التي قامت فيها الدول بتعطيل شبكات الاتصالات أو التلاعب بها لأغراض سياسية، بما في ذلك ما يتعلق بالانتخابات والمظاهرات العامة[١]. فقد قطعت كل من مصر وليبيا كل سبل الوصول إلى الإنترنت لفترات وجيزة خلال ما يسمى بالربيع العربي. ولجأت جمهورية ايران الإسلامية أثناء عدد من المظاهرات الإحتجاجية إلى إغلاق تطبيقي (واتساب) و(إنستغرام) لإعتبارات أمنية[٢].

هناك أمثلة كثيرة من اللجوء إلى هذه الأساليب لمنع الوصول إلى الخدمات أو مواقع الويب وهي لا تقتصر فقط على الأنظمة غير الديمقراطية. فمع الابتكارات في مجال مراقبة ورصد الحياة اليومية أصبحت الدولة دولة أمنية من هذه الناحية.

هناك نقطة أخرى في عملية الأمننة في الفضاء السيبراني، وهي حساسة جداً برأينا و تتعلق بتقدير التهديدات. إن تصور التهديدات بحاجة إلى دقة بالغة، لأنه سيكون مدخلاً لتطوير سياسات أمنية. ففي حالة المبالغة في تقدير التهديدات، قد نجد مبالغة مماثلة في السياسات المصنوعة لمواجهتها. يطلق (لين هانسن' Lene Hansen) و(هيلين نسنباوم' Helen Nissenbaum) على هذه الحالة تسمية (الأمننة المفرطة' Hypersecuritization)[٣].

حسب جوزيف ناي، فمنذ عام ٢٠١٣، تم وصف الفضاء السيبراني بأنه أكبر خطر يواجه الولايات المتحدة[٤]. وفي خطاب أمام الكونجرس في ٢٠١٥، أعلن مدير المخابرات الوطنية الأمريكية (جيمس كلابر' James Clapper) أن "الهجمات السيبرانية تشكل تهديدًا للأمن القومي أكبر من المتطرفين السنة، والطموحات النووية لإيران وكوريا الشمالية، والعملاء الروس والصينيين الذين يحاولون اختراق مجتمع الأمن القومي في الولايات المتحدة"[٥].

إننا نرى بأنه سيكون من المضلل، إن لم يكن خطيراً، المبالغة في تقدير التهديدات، وسيكون من غير الحكمة أيضًا أن نسير في الاتجاه المعاكس، من خلال التقليل من شأن الفرص التي يخلقها الفضاء السيبراني لهجمات سيبرانية لفاعلين المختلفة ضد بعضهم البعض. ولكن يمكن احتواء مثل هذا الصراع احياناً داخل الفضاء السيبراني. على سبيل المثال لاحظ (روبيرت ريدرون' Robert Reardon) و(نازلي شكري' Nazli Choucri) أن معظم الهجمات المستمرة والمتزايدة في الفضاء السيبراني هي من نوع التجسس، وهو نشاط لا

(1). Ibid.

(٢). إرم نيوز، اعتبرتهما تهديدا أمنيا: "إيران تحظر واتساب وإنستغرام نهائيا"، الموقع الإلكتروني لإريم نيوز- تأريخ النشر وزيارة الموقع ٢٢ تشرين الأول ٢٠٢٢، متوفر على الرابط: https://www.eremnews.com/news/world/ctxgbaixx2

(3). Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly* 53 (4) (December 2009), 1155.

(4). Joseph S. Nye, *How Will New Cybersecurity Norms Develop,* Op. cit.

(5). James R. Clapper, *Statement for the Record Worldwide Threat Assessment of the US Intelligence Community*, (N.P.: Office of the Director of National Intelligence 2015), 1-4.

يعتبر تقليديًا هجومًا على الإطلاق، على الأقل ليس في سياق قوانين الحرب المقبولة دوليًا[١]. حتى مع إرتفاع عدد الحوادث السيبرانية من هذا النوع إلا أن تأثيرها وخطورتها تظل ثابتا وعلى مستوى منخفض نسبيا .

مع ذلك قد يؤدي بعض الهجمات السيبرانية إلى التصعيد في العالم المادي، أو إلحاق أضرار اقتصادية أو مادية، ذلك أن الهجمات الاستراتيجية واسعة النطاق عبر الفضاء السيبراني ضد البنية التحتية الحيوية تشكل تهديداً خطيراً للأمن القومي[٢].

فضلاً عن ذلك، أن الأمر لايتوقف عند الدول فقط، لأن الفاعلين في الفضاء السيبراني متعددة[٣]، وبالتالي ينبغي توقع خطابات مختلفة من قبل جهات فاعلة مختلفة لديها وجهات نظر معينة حول الأمن السيبراني ونماذج مختلفة من التفكير حول التهديدات السيبرانية. على سبيل المثال، قد يكون الفاعلون ذات الخلفية التقنية أكثرعرضة لتصوير مشاكل الأمن السيبراني على أنها حوادث ناجمة عن التعقيد الداخلي للأنظمة الشبكية، وبالتالي تنطوي على إجراءات من شأنها نزع تسييس القضايا الأمنية[٤]. وقد تكون عملية الأمننة في الفضاء السيبراني جماعياً Collective Securitization أي بناء تصور جماعي من قبل مجموعة من الدول أو كتلة دولية للتهديدات السيبرانية التي تواجههم. وهذا المفهوم لاحظه (جورج كريستو' George Christou) في الأتحاد الأوروبي عند البحث عن التصورات المشتركة للتهديدات السيبرانية وكذلك التشريعات الجماعية فيما تخص القضايا الرئيسية في الأمن السيبراني دون استبعاد سياسات وطنية مستقلة في بعض الأحيان[٥].

وقد يكون الفاعل فرداً، حيث الفضاء السيبراني هو فضاء يوجد فيه قلق من أن الفرد يمكن أن يصبح مشكلة أمن قومي كما يقول (مارك لاسي' Mark Lacy) و(دانيال برنس' Daniel Prince[٦]، وربما يكون (جوليان أسانج' Julian Paul Assange) خير دليل على ذلك[٧].

---

(1). Robert Reardon and Nazli Choucri, *The Role of Cyberspace in International Relations: A View of the Literature*, (Massachusetts: Massachusetts Institute of Technology, 2012), 22.

(2). Richard Clarke, "War from Cyberspace," National Interest 104 (2009), 31-36.

(٣) يقسم جوزف ناي الفاعلين في الفضاء السيبراني إلى نوعين هما الدول وغير الدول ويشمل الأخير الشركات عابرة الجنسية، المنظمات الإجرامية، الجماعات الإرهابية، والأفراد.

(4). Liu Yangyue, The Conceptual Underpinning of Cyber Security Studies, in: Nazli Choucri and Chrisma Jackson, *Perspectives on Cybersecurity: A Collaborative Study*, (Massachusetts: Massachusetts Institute of Technology, 2015), 25-26.

(5). George Christou, The Collective Securitisation of Cyberspace in the European European Union, *West European Politics* 42 (2), (2018): 278-279.

(6). Mark Lacy and Daniel Prince, Securitization and the Global Politics of Cybersecurity, *Global Discourse* 8 (1), (February 2018):101.

(٧). هو صحفي وناشط ومبرمج أسترالي، أسس موقع ويكيليكس ورأس تحريره. كان أسانج هاكر عندما كان كان مراهقا، ثم مبرمج كمبيوتر قبل أن يصبح معروفاً لعمله مع ويكيليكس. أصبحت ويكيليكس معروفة عالمياً في عام ٢٠١٠ عندما بدأ في نشر وثائق عسكرية ودبلوماسية عن الولايات المتحدة. ورد وثائق سلاح الجو الأميركي أن العسكريين الذين يجرون اتصالات مع ويكيليكس أو «مؤيدي ويكيليكس» معرضون لخطر اتهامه بـ"التواصل مع العدو". اعتقلت الشرطة البريطانية أسانج داخل السفارة الإكوادورية يوم ١١ أبريل عام ٢٠١٩، وفي ٢٥ يونيو ٢٠٢٤ أطلق سراحه بموجب صفقة مع القضاء الأمريكي.

كما يمكن توظيف أو استخدام جماعات الإنترنت الإجرامية كقوة وكيلة، أو إنخراط قوات غير نظامية رسمية في التجسس أو مهاجمة المعارضين بناءً على طلب الحكومة، مع توفير درجة من الإنكار المعقول(١).

علاوة على ذلك بإمكاننا أن نلاحظ بأن الكثير من البحوث يركز على الجماعات الإرهابية كفاعل أمني في الفضاء السيبراني. يستخدم الفضاء السيبراني من قبل الجماعات الإرهابية إضافةً إلى الهجمات السيبرانية على البنية التحتية للدول، للإتصال، التدريب والتخطيط والتنفيذ للعمليات، الأعلام والدعاية ونشر الأفكار، والتجنيد(٢). ويذهب (جاريت براخمان' Jarret Brachman) إلى حد القول بأن التهديد الذي يشكله الإرهابيون السيبرانيون أكبر من خطر الهجوم على البنية التحتية الحيوية(٣). ولكن يبدو تقدير التهديدات الإرهابية هي الأخرى تعرض للمبالغة في كثير من الأحيان. وهذا ما أشار اليه (براندو فاليرانو' Brando Valeriano) و (رايان مانيس' Rayan C. Maness) في تقدير التهديد الإرهابي من قبل الولايات المتحدة الأمريكية(٤)، وتطرقت إليه أيضاً الباحثة (ماورا كونواي' Maura Conway) التي جادل بأن معظم الأنشطة التي يشير إليها كأعمال إرهابية لا تنطوي على أعمال عنف ضد غير المقاتلين، بل إنها غالبًا ما تكون أنشطة قانونية(٥).

عليه نظرًا لوجود خطابات متعددة وصور تهديد متنافسة بل متصارعة أحيانا للأمن السيبراني، سيكون من الصعب إلى حد ما التوصل إلى مفهوم دقيق مقبول لدى جميع الفاعلين السيبرانيين المعنيين.

يرى الباحث اليوم هناك إشكالية في ترسيم حدود الدراسات الأمنية. أين نرسم الخط في دراسة الأمن؟ ما الذي يجب تضمينه أو استبعاده؟ إذا تم اتخاذ فهم واسع وشامل للأمن كنقطة انطلاق، فسيكون ذلك بمثابة القول بأن كل قيمة ومصالح إنسانية تقريبًا، إذا رأى الطرف المتضرر أنها مهددة، هي مسألة أمنية. وعلى العكس من ذلك، إذا تم تبني مفهوم أضيق للأمن، يتم تحديده فقط بالقوة والتهديدات القسرية، فقد نستبعد الجهات الفاعلة والعوامل التي تؤثر بشكل متباين على الأمن.

أدت التفاعلات في الفضاء السيبراني إلى تغيير ميزان القوى بين مختلف الفاعلين، بما في ذلك سلطات الدولة التقليدية، ومكنت الفاعلين الأضعف من التأثير أو حتى تهديد الفاعلين

---

(1). Clement Guitton, *Inside the Enemy's Computer: Identifying Cyber Attackers*, (Oxford and New York: Oxford University Press, 2017), 68.

(٢). محمد زهير عبدالكريم، "الإرهاب السيبراني: أزمة عالمية،" *قضايا سياسية* ٦٤، (شباط ٢٠٢١): ٢٨٤-٢٨٨.

(3). Jarret Brachman, "Watching the Watchers," *Foreign Policy*, October 12, 2010, 2010, available at the link: https://foreignpolicy.com/2010/10/12/watching-the-watchers/

(4). Brando Valeriano and Rayan C. Maness, International Relations Theory and Cyber Security: Threat, conflict and Ethics in an Emergent Domain, in: Chris Brown and Robyn Eckersley (eds.), *The Oxford Handbook of International Political Theory*, (Oxford: Oxford University Press, 2018), 259.

(5). Maura Conway, "What Is Cyberterrorism," *Current History* 101, (December 2002): 436-442.

الأقوى. هذا النوع من التحول ليس له سابقة تذكر في السياسة الدولية. وبالتالي نشهد تحولا قويا محتملا في طبيعة اللعبة. قد يؤدي التأثير المتزايد للكيانات غير الحكومية إلى تحولات كبيرة قد تصل إلى تقويض السيادة كمبدأ محدد للنظام الدولي.

III. المطلب الثالث

نحو تعريف بديل للأمن السيبراني

يتناول هذا المطلب إشكالية التعريف بمفهوم الأمن السيبراني، ومن ثم تقديم رؤية نقدية حول بعض التعاريف الموجودة، وبعده الذهاب إلى تقديم تعريف بديل للأمن السيبراني.

III.أ. الفرع الأول

مفهوم الأمن السيبراني: إشكالية التعريف

يعد مفهوم الأمن واحداً من المفاهيم الخلافية الغامضة والمثيرة للجدل، اذ يتبادر إلى الذهن معانٍ وقيم مختلفة حول الأمن لدى الدارسين وصانعي القرار. ويكمن سبب ذلك في السمات التي يتسم بها الأمن ذاته كالنسبية والنفسية والعمومية أو المطاطية.

فللأمن مفهوم نسبي لأن ضمانه المطلق لايمكن تحقيقه(١). وهو مسألة احساس وشعور وإدراك، أي موقف ذاتي تقديري نفسي أكثر مما هو موضوعي(٢).

ويعود عمومية مصطلح الأمن إلى أنه اصطلاح واسع الانتشار ubiquitous(٣) ومطاط يستخدم في الكثير من المجالات والمواقف وعلى أصعدة متباينة ومستويات مختلفة ابتداء بما يتعلق بأمن الأفراد وانتهاء بما يتعلق بالأمن العالمي، وبالتالي فإن التداخل والتشابك فيما بين الأصعدة المتابينة من جانب والمستويات المختلفة من جانب ثان وثالثاً بين الأصعدة والمستويات كلها تزيد من تعقيد المفهوم واشكاليته(٤).

مفاد ما تقدم أن الأمن مفهوم إشكالي معقد إلى حد دفع البعض إلى أن يصفه بأنه (اشمئزازي' ad nauseam) وتأريخياً فشلت محاولات اخضاعه للنقاش(٥)، اذ يتميز بعدم قدرة النقاشات على تحديد معناه واستخداماته، بل وأكثر من ذلك أن مصطلح الأمن يتحدى أى سعي وراء تقديم تعريف مقنع له(٦).

---

(١). نجدت صبري ئاكره يى، *الإطار القانوني للأمن القومي*، (أربيل: مطبعة زانكو، ٢٠٠٤)،١٧.

(٢). عبدالقادر محمد فهمي، "في مفهوم الأمن القومي والأمن القومي العربي"، *مجلة الأمن القومي*، ٣، (١٩٨٨): ٧٣.؛ سعد ياسين الناصري، "محددات مفهوم الامن القومي العربي،" *بيت الحكمة*، ٥، (شتاء ٢٠٠٠-٢٠٠١): ٥١. ؛ وكذلك:

Ali bin Faiz Al-Jahni, *Terrorism: Concept and Reality*, tr. Zubair Ahmad, (Riyadh: Naif Arab Academy for Security Sciences, 2002), 38.

(٣). عمر احمد قدور، *شكل الدولة واثره في تنظيم مرفق الامن*، (القاهرة: مكتبة مدبولي، ١٩٩٤)، ٦٣.

Ali bin Faiz Al-Jahni, *Terrorism: Concept and Reality*, Op., cit., 38.؛

(٤).. مصطفى علوي، "الأمن الإقليمي بين الأمن الوطني والأمن العالمي،" *المركز الدولي للدراسات المستقبلية والإستراتيجية*، ٤، (٢٠٠٥): ٨-١٠.

(5). Michael Sheehan, *International Security: An Analytical Survey*, (Boulder: Lynne Rienner Publishers, 2005), 1-2.

(6). Martin Shaw, *Global Society and International Relations: Sociological Concepts and Political Perspectives*, (Cambridge: polity press, 1994), 31.

والآن التساؤل هو: ماذا عن مفهوم الأمن السيبراني؟

السؤال المطروح أعلاه هو موضوع نقاش وكتابة لا نهاية لها. تمت مناقشة هذا المصطلح كثيراً، مما يسبب ارتباكاً كبيراً ويطرح أسئلة أكثر من الإجابات. فالمفهوم يزداد غموضاً وتعقيداً عند البحث عن الأمن السيبراني بحيث لايسمح بتعريف مباشر وسريع، وإنما خاضع لمناقشات سياسية واكاديمية، ومرد ذلك عدة أسباب، من بينها:

١. أن الأمن السيبراني مصطلح جديد نسبيًا[١].
٢. اختلاف التصورات طبقاً لتعدد الفاعلين والطبيعة المجهولة لهم ولدوافعهم في الفضاء السيبراني[٢].
٣. غياب الاتفاق على مفردات مشتركة بسبب السرعة في الإنتشار[٣].
٤. بالتوازي مع التقدم الرقمي في جوانب الاقتصاد والمجتمع والسياسة (أكثر من أي وقت مضى)، تتوسع مخاوف الأمن السيبراني لتشمل مجالات سياسية إضافية[٤].
٥. الخلط بين مصطلحي الأمن السيبراني والأمن المعلوماتي[٥].
٦. التطور المستمر في معنى المصطلح عبر الزمن، فمنذ وقت ليس ببعيد، كان الأمن السيبراني يمثل قضية تناقش في المقام الأول في دوائر الخبراء باعتبارها مشكلة فنية أو مشكلة تتعلق بإدارة المخاطر، أما الآن فقد أصبحت قضية أمن قومي يتم التعامل معها في

(1). Rossouw von Solms and Johan van Niekerk, "From Information Security to Cyber Security," *Computers & Security* 38, (2013): 99.

(2). Forrest Hare, Borders in Cyberspace …, Op. cit., 90.

(3). Tim Stevens, *Cyber Security and the Politics of Time*, (Cambridge: Cambridge University Press, 2016), 3.

(4). Myriam Dunn Cavelty and Florian J. Egloff, "The Politics of Cybersecurity: Balancing Different Roles of the State," *St Antony's International Review* 15 (1), (2019): 38.

(٥) على الرغم من التداخل والتشابك بين المصطلحين، ولكن لابد من الإنتباه إلى التمييز بينهما، فهناك من يرى من جانب ان الأمن المعلوماتي أشمل وأعم من الأمن السيبراني، إذ أن الأول يشمل حماية المعلومات الرقمية وغير الرقمية، بينما الثاني يهتم فقط بحماية البيانات الرقمية. ومن جانب آخر أن الأمن السيبراني يشمل بعض الأمور التي لاتندرج تحت أمن المعلومات، كحماية البنى التحتية مثل شبكات الماء والكهرباء، والمعدات الطبية وغيرها التي أصبحت تعتمد على شبكات الإنترنيت. يمكن النظر لطفاً: منصور عبدالحكيم، *الحرب السيبرانية*، (الجيزة: دار الفاروق للإستثمارات الثقافية، ٢٠٢٢)، ٥.؛ ويضيف البعض أيضاً بأن الأمن السيبراني يتجاوز حدود أمن المعلومات التقليدي ليشمل ليس فقط حماية موارد المعلومات، ولكن أيضًا حماية الأصول الأخرى، بما في ذلك الشخص نفسه. في أمن المعلومات، عادة ما تتعلق الإشارة إلى العامل البشري بدور البشر في عملية الأمن. أما في مجال الأمن السيبراني، هذا العامل له بعد إضافي، وهو البشر كأهداف محتملة للهجمات السيبرانية أو حتى المشاركة دون علم في هجوم سيبراني. ولهذا البعد الإضافي آثار أخلاقية على المجتمع ككل، حيث يمكن اعتبار حماية بعض الفئات الضعيفة، مثل الأطفال، مسؤولية مجتمعية. يمكن الرجوع لطفاً الى: Rossouw von Solms and Johan van Niekerk, "From Information Security to Cyber Security," … Op. cit., 97.

أعلى الدوائر الحكومية[١].

من هنا نأتي بمثال فقط في هذا السياق، إذ يعترف (بروس شناير' Bruce Schneier) -المستشار في مجال التشفير- في العام ٢٠٠٠ بخطأ آرائه حول الأمن في المجال الرقمي في كتاب له نشر طبعته الأولى عام ١٩٩٣ تحت العنوان (التشفير التطبيقي' Applied Cryptography). وصف في الكتاب (مدينة فاضلة رياضياتية) بحيث من شأن الخوارزميات أن تحافظ على أعمق الأسرار آمنة لآلاف السنين، وإجراء التفاعلات الإلكترونية بسلامة وأمان. في رؤيته، أن التشفير بمثابة المعادل التكنولوجي العظيم؛ ويمكن لأي شخص يمتلك جهاز كمبيوتر رخيص الثمن أن يتمتع بنفس مستوى الأمان الذي تتمتع به أكبر حكومة. وفي الطبعة الثانية من نفس الكتاب، التي نشرت بعد ذلك بعامين، ذهب إلى حد الأعتقاد بأن لا يكفي أن نحمي أنفسنا بالقوانين، نحن بحاجة إلى حماية أنفسنا بالرياضيات. ولكن في سنة ٢٠٠٠، أي بعد سبع سنوات من الطبعة الأولى للكتاب، نشر كتاب آخر جزئياً لتصحيح آرائه السابقة الخاطئة مثلما يقول نفسه. في الكتاب الجديد المعنون (أسرار وأكاذيب: الأمن الرقمي في عالم شبكي' Secrets and Lies: Digital Security in a Networked World) يرى أن التشفير لايضمن الأمن، لأن التشفير يتعلق بالرياضيات وهي تتضمن الأرقام والمعادلات والمنطق، أما الأمن فيتعلق بالناس، والعلاقات بين الناس، وكيفية ارتباط الناس بالآلات. وبالتالي فهو استنتج بأن نقاط الضعف موجودة في الأجهزة، والبرمجيات، والشبكات، والأشخاص. ولخص بأن"الأمن هو عملية، وليس منتج"، وفي النهاية "من يعتقد بأن التكنولوجيا يمكنها حل المشكلات الأمنية، فأنه لا يفهم المشكلات ولا يفهم التكنولوجيا"[٢].

إذن إن الشعور بالأمن في الفضاء السيبراني له بعد زلق أو مراوغ[٣]، وبالتالي التعريفات البسيطة والثابتة ليست مناسبة تمامًا للتعامل مع السياقات المتغيرة باستمرار[٤]. وفي هذا السياق يضع (مادلين كار' Madeline Carr) و(فيجا ليسنيوسكا' Feja Lesniewska) الأمن السيبراني ضمن (المشكلات الشريرة' Wicked Problems)[٥] لأن

(1). Myriam Dunn Cavelty and Florian J. Egloff, "The Politics of Cybersecurity…" Op. cit., 38.

(2). Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World,* (Indiana: John Wiley & Sons, Inc, 2000), xxiii-xxiv.

(3). Stamatia Sofiou, Ethics in Cyberspace: Cyber-Security, in: Nicholas J. Daras (ed.), *Cyber-Security and Information Warfare*, (New York: Nova Science Publishers, 2019), 333.

(4). Myriam Dunn Cavelty and Andreas Wenger, Cyber Security between Socio-technological Uncertainty and Political Fragmentation, in: Myriam Dunn Cavelty and Andreas Wenger (eds.), Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation, (London & New York: Routledge, 2022), 1.

(٥). تشير المشكلات الشريرة إلى تلك المشكلات المعقدة والمترابطة والمعتمدة على بعضها البعض والمقاومة للحلول. وهذا يعني أنه بدلاً من "حلها"، لابد من العمل على "ترويضها". يمكن النظر لطفاً: Madeline Carr and Feja Lesniewska, "Internet of Things, Cybersecurity and

لأن الأمن السيبراني ذو طبيعة عابرة للحدود، ويحدث على مستويات متعددة عبر القطاعات، وبين المؤسسات، وسيؤثر على جميع الجهات الفاعلة، العامة والخاصة، بطرق معقدة ومترابطة وغالبًا ما تكون مسيسة للغاية[١].

عليه غالبًا ما يكون الأمن السيبراني مرنًا من حيث التعريف، ونظراً لاهتماماته بكل شيء تقريباً يتصل رقمياً وإلكترونياً، سواء كان ذلك الأشخاص أو الشركات أو الحكومات أو الجيوش أو وكالات الاستخبارات أو الآلات أو الخوارزميات، فإن الأمن السيبراني يؤثر على العالم بطرق عديدة لا يمكن استيعابها بسهولة في التعريفات[٢].

كل ماسبق أعلاه لايعني أن نترك مهمة تعريف الأمن السيبراني وأن لا نبذل جهود لتبني مفهوم معين له، إذ أن مهمة التعريف بمفهوم موضوع الدراسة من الضرورات والمهام البحثية الأساسية التي لايمكن الإستغناء عنها الباحث في مشروعه البحثي.

III.ب. الفرع الثاني

تعريف بديل للأمن السيبراني

ومن خلال تفحص الكثير من الأدبيات المعنية بالموضوع، يمكن ملاحظة اتجاهين فيما يخص مفهوم الأمن السيبراني: اتجاه يتعامل مع الأمن السيبراني على نطاق أوسع- اي الأهتمام بكل شيء يحدث في الفضاء السيبراني-، واتجاه آخر يتركز على الجوانب السياسية للقضية، ومن ضمنها البعد الدولي لسياسات الأمن السيبراني[٣]، وذلك نظراً لكون الأمن السيبراني من القضايا الأمنية العابرة للوطنية[٤].

كما يمكن تسجيل ملاحظة أُخرى وهي مهمة، فالغالبية العظمى لمفاهيم الأمن السيبراني يعبر عن مفهوم (السياسات الأمنية السيبرانية) وليس الأمن السيبراني ذاته. بعبارة أُخرى التعاريف تنطلق من السياسات أو الإجراءات والتدابير الأمنية المتبعة من قبل الفاعلين، وفي مقدمتهم الدول، في الفضاء السيبراني. وقد يكون سبب ذلك، حسب رأينا، أن البحوث المعنية بالموضوع كانت تبحث وتعالج المشاكل و الحالات الإمبريقية التي وقعت في الفضاء السيبراني وما آثارها أمنياً، من تسلل وخراب وهجمات سيبرانية، وكذلك كيفية مواجهتها والرد عليها، وبالإيجاز كيفية الحماية في الفضاء السيبراني. وكل هذه تعبر عن السياسات و التدابير الأمنية السيبرانية.

وفي هذا السياق، الأمن السيبراني هو "الجهد المبذول لحماية المعلومات والاتصالات

Governing Wicked Problems: Learning from Climate Change Governance," *International Relations* 34 (3), (2020): 398.

(1). Ibid, 392.

(2). Tim Stevens, *Cyber security and the politics of time*, …, Op. cit., 23.

(3). Andreas Wenger and Myriam Dunn Cavelty, in: Myriam Dunn Cavelty and Andreas Wenger (eds.), *Cyber Security Politics*: … Op. cit., 261-262.

(4). Raju G.C. Thomas, "What Is Third World Security," *Annual Review of Political Science* 6, (June 2003): 216-217.

والتكنولوجيا من الضرر الناجم إما عن طريق الخطأ أو عن قصد"[١]. وأيضاً يحدد الأمن السيبراني "التدابير الفنية والتنظيمية التي يتم اتخاذها لتقليل المخاطر التي تتعرض لها البنى التحتية الرقمية للبلد"[٢]. ويتعلق الأمن السيبراني بـ"الحفاظ على سلامة المساحة التي يوفرها الكمبيوتر والإنترنت لمختلف مستخدمي التكنولوجيا"[٣]. كما يتم تعريفه كـ "مسألة تتعلق بسيادة الدولة والأمن القومي والتراث الثقافي للأمم وحماية البنية التحتية الحيوية والأنظمة والشبكات والسلع والقيم"[٤]. وأنه "النشاط أو العملية أو القدرة أو الإمكانية أو الحالة التي يتم بموجبها حماية نظم المعلومات والإتصالات والمعلومات الواردة فيها من و/أو الدفاع عنها ضد الضرر أو الاستخدام أو التعديل غير المصرح به أو الإستغلال"[٥]. ويقصد به أيضاً "مجموعة الأنظمة التقنية الحديثة التي تستخدمها الدول لحماية الشبكات وأجهزة الحاسوب الآلي وكل ما هو موجود على الشبكة الدولية للمعلومات"[٦].

ويمكن القول بأن تعريف (الأتحاد الدولي للإتصالات) للأمن السيبراني هو الآخر يأتي في هذا النطاق، بأن الأمن سيبراني هو "مجموع الأدوات والسياسات والمفاهيم الأمنية والضمانات والمباديء ومناهج إدارة المخاطر والإجراءات والتدريبات وأفضل الممارسات والضمانات التكنولوجية، التي يمكن استخدامها لحماية البيئة السيبرانية والمستخدم والمؤسسة بصورة عامة"[٧].

فضلاً عن ملاحظاتنا السابقة حول هذه التعاريف، نرى إنها تركز على البعد الدفاعي في السياسات والتدابير الأمنية السيبرانية، وكأن الأمن السيبراني يضمن عن طريق الدفاع فقط، وهذا برأينا نقص كبير في فهم السياسات الأمنية بشكل عام، لأن الأمن كقيمة يتم ضمانها أيضاً عن طريق السياسات الهجومية جنباً الى جنب السياسات الدفاعية، وعلى وجه الخصوص بما يتضمن الهجوم من مسائل الردع، والهجمات الإستباقية والوقائية، وهي كلها مهمة لتوفير الأمن.

مع ذلك، قد نجد تعاريف، ولو قليلة جداً، للأمن السيبراني تأخذ ببعدي الدفاعي

---

(1). Amos N. Guiora, *Cybersecurity: Geopolitics, law, and policy*, (London and New York: Routledge, 2017), 17-18.

(2). Reto Inversini, Cyber Peace: And How It Can Be Achieved, in: Markus Christen, Bert Gordijn and Michele Loi (eds.), *The Ethics of Cybersecurity*, (Switzerland: Springer Open, 2020), 267.

(3). George Thomas Kurian (ed. in Chief), *The Encyclopedia of Political Science*, (Washington DC: CQ Press, 2011), Cybersecurity, 372.

(4). Solange Ghernaouti, *Cyber Power: Crime, Conflict and Security in Cyberspace*, (Lausanne: EPFL Press, 2013) 6.

(٥). سين إس. كوستيجان ومايكل إيه هينيسي (تح.)، *الأمن السيبراني: منهج مرجعي عام*، (دب.: أكاديمية الدفاع الكندية، ٢٠١٦)، ١٧.

(٦). نانيس عبدالرزاق فهمي، "مستقبل الأمن السيبراني في عصر الميتافيرس،" *آفاق مستقبلية (اصدارة سنوية)*، (القاهرة: مركز المعلومات ودعم اتخاذ القرار برئاسة مجلس الوزراء (٣)، (كانون الأول ٢٠٢٣)، ٣٠٥.

(٧). نقلاً عن: إيهاب خليفة، "تهديدات الأمن الإقليمي العربي في الميدان الخامس: نحو إستراتيجية للحماية،" للحماية،" *أوراق السياسات الأمنية*، جامعة نايف العربية للعلوم الأمنية، ٢٠٢١، ٤.

والهجومي في السياسات الأمنية السيبرانية، ومنها تعريف (ستاماتيا صوفيو، Stamatia Sofiou) الذي يرى أن "الأمن السيبراني يغطي الاستخدام الدفاعي والعدواني لأنظمة الويب للمعلومات..."[١].

إضافة الى ما سبق نجد تعاريف أُخرى للأمن السيبراني وهي قريبة إلى القوة السيبرانية أكثر من قربها للأمن السيبراني. من هذه التعاريف، تعريف (**كيرياكي أثاناسولي**، Kyriaki Athanassouli) للأمن السيبراني بـ "القدرة على التحكم في الوصول إلى أنظمة الشبكات والمعلومات التي تحتوي عليها" و"القدرة على الحفاظ على سرية وسلامة وتوافر الفضاء السيبراني، وضمان حماية أنظمة الكمبيوتر والبيانات من التدخل عبر الإنترنت" [٢].

من أجل تجاوز ملاحظاتنا السابقة حول مفهوم الأمن السيبراني، لابد من بذل جهد إضافي أكثر للوصول الى مفهوم دقيق نسبياً. ويبدأ هذا بالذهاب الى الباحثين الرواد في دراسة الأمن السيبراني.

يقدم (تيم ستيفنز، Tim Stevens)، وهو من الباحثين البارزين في المجال، تعريفاً واسعاً للأمن السيبراني كونه "وسيلة ليس فقط لحماية المجتمع والدفاع عنه والبنى التحتية المعلوماتية الأساسية الخاصة به ولكن أيضًا وسيلة لملاحقة السياسات الوطنية والدولية من خلال وسائل تكنولوجيا المعلومات"[٣]. وهذا يسلط الضوء على الخصائص الأنطولوجية والعملية للأمن السيبراني. وهو يدرك أن الأمن السيبراني ليس مجرد أمر دفاعي، كما يتبين من خلال التدخل والمشاركة النشطة العابرة للحدود الوطنية[٤].

والأمن السيبراني، كما عرفه اثنان من كبار الباحثين في هذا المجال (ميريام دان كافيلتي، Myriam Dunn Cavelty) و(مانويل سوتر، Manuel Suter)، هو "غياب التهديد سواء عبر تكنولوجيات وشبكات المعلومات والاتصالات أو عليها"[٥]. الأمن السيبراني هو الأمن الذي يتمتع به المرء في الفضاء السيبراني ومنه، ولذلك، لم يعد الأمن السيبراني يتعلق فقط بـ "أمن الفضاء السيبراني"، بل أصبح أيضًا "الأمن عبر الفضاء السيبراني".

ننضم بدورنا إلى هذا التعريف الأخير للأمن السيبراني وذلك لكونه أدق وأوضح من غيرها من التعاريف. فغياب التهديد هو مايدور عنه جوهر أي تعريف للأمن[٦]. وبالتالي الأمن السيبراني، حسب رأينا، بكل بساطة هو"غياب التهديد السيبراني سواء كان ذلك التهديد

(1). Stamatia Sofiou, Ethics in Cyberspace, … Op. cit., 333.

(2). Kyriaki Athanassouli, Economic Implications of the Rise of Information Warfare, in: Nicholas J. Daras (ed.), *Cyber-Security and Information Warfare*, … Op. cit., 45.

(3). Tim Stevens, *Cyber security and the politics of time*, …, Op. cit., 11.

(4). Tim Stevens, "Global Cybersecurity: New Directions in Theory and Methods," Methods," *Politics and Governance* 6(2), (June 2018): 1–4.

(5). Myriam Dunn Cavelty and Manuel Suter, The Art of CIIP Strategy: Taking Stock of Content and Processes, in: Javier Lopez, Robert Setola and Stephen D. Wolthusen (eds.), *Critical Information Infrastructure Protection: Information Infrastructure Models، Analysis, and Defense*, (Berlin: Springer Verlag, 2012), 19.

(٦). فرهاد جلال مصطفى، الأمن ومستقبل السياسة الدولية، مرجع سابق، ٣٠-٣١.

على البنية التحتية للفضاء السيبراني، أي تكنولوجيا المعلومات والإتصالات، أو عبر الفضاء السيبراني، أي العمليات السيبرانية ايأ كانت طبيعتها سياسية، عسكرية، جاسوسية، اقتصادية وغيرها، وأياً يكون وراءها دول أو فاعلون من غير الدول، وأينما يكون مصدرها، داخلية أو خارجية".

إذن فلم يعد مفهوم الأمن حسب الاتجاهين: التقليدي والتوسعي قادراً على ضم المتغيرات الدالة على العمليات السيبرانية. وهذا ما جعل القائمين على المنظومات الأمنية يرتدون إلى النظريات والدراسات الأكاديمية وتصميم سياسات معنية بها. فلا مناص للباحث من الاعتراف والاقرار بالدرجة العالية من التعقيد التي يتميز بها مفهوم الأمن السيبراني ومدى الاشكالية التي تنبثق من اختلاف الباحثين والمختصين وحتى صناع القرار حول المفهوم. وما يمكن القول بشأنه هو الإفترض بأن ثورة المعلومات والإتصالات تجعل الأمن شاغلاً متزايد الأهمية في جميع قطاعات المجتمع، والتخصصات العلمية المتنوعة، وكذلك لدى الباحثين والقائمين بالسياسات المعنية.

الخاتمة

أفرزت التفاعلات السيبرانية الدولية ضرورة التعاون بين دارسي تكنولوجيا المعلومات والإتصالات من جهة والعلاقات الدولية من جهة أُخرى من أجل فهم عواقب ظهور الفضاء السيبراني على قضية الأمن. فلم يعد الأمر يتعلق بالأمن التقني فقط، بل يتجاوز ذلك لبناء تصور أكثر شمولاً لماهية الأمن في الفضاء السيبراني عبر عملية الأمننة لهذا الفضاء، يتلاقى فيها جهات متنوعة من دول وغير الدول، وعلى أصعدة مختلفة وطنية، دولية وعالمية، وفي مجالات شتى تكنولوجية، إجتماعية، إقتصادية، ثقافية، عسكرية وقبل كل ذلك سياسية- لأن الأعتقاد المركزي لهذا البحث في النهاية هو أن الأمن السيبراني سياسي بالنسبة لنا.

وعلى الرغم من توجه فرع الدراسات الأمنية منذ فترة نحو التركيز على الأمن السيبراني، إلا إن انتاجه العلمي التحليلي لحد الآن لم يصل لمستوى حجم الموضوع من ناحية، ومن ناحية أُخرى يفتقد سمة الدقة في بنائه لتصور التهديات السيبرانية والسياسات السيبرانية آزاءها والتي تتسم بالمبالغة فيها الى جانب تعميمات غير دقيقة.

فضلاً عما سبق، أن مفهوم الأمن السيبراني نفسه هو الآخر تعرض لتعاريف غير دقيقة وذلك تارةً للتوسع غير اللازم في تعريفه، وتارةً أُخرى لدمجه بمفاهيم أُخرى ذات علاقة بها كمفهوم السياسات السيبرانية أو القوة السيبرانية. فالتعريف المناسب لمفوم الأمن السيبراني، بالنسبة لهذا البحث، هو التعريف الذي ينطلق من جوهر مفهوم الأمن ألا وهو إقترانه بغياب التهديد. عليه، الأمن السيبراني هو غياب التهديد السيبراني سواء كان ذلك التهديد على البنية التحتية للفضاء السيبراني، أي تكنولوجيا المعلومات والإتصالات، أو عبر الفضاء السيبراني، أي العمليات السيبرانية ايأ كانت طبيعتها سياسية، عسكرية، جاسوسية، اقتصادية وغيرها، وأياً يكون وراءها دول أو فاعلون من غير الدول، وأينما يكون مصدرها، داخلية أو خارجية

قائمة المراجع

أولاً: الكتب:

١. أنطوني، إيان. مقدمة: الأمن الدولي، والتسلح، ونزع السلاح. في: معهد ستوكهلم لأبحاث السلام الدولي (سيبري). *التسلح ونزع السلاح والأمن الدولي*. تر: عمر سعيد الأيوبي و أمين سعيد الأيوبي. بيروت: مركز دراسات الوحدة العربية. ٢٠١٤.

٢. أونيل، باتريك ه. *مباديء علم السياسة المقارن*. تر: باسل جبيلي. دمشق: دار الفرقد للطباعة والنشر والتوزيع. ٢٠١٢.

٣. البراك، فاضل. *استراتيجية الامن الداخلي*. بغداد: دار الحرية للطباعة. ١٩٨١.

٤. بولانان، فنسنت. الأمن الإلكتروني وصناعة الأسلحة. في: معهد ستوكهلم لأبحاث السلام الدولي (سيبري). *التسلح ونزع السلاح والأمن الدولي*. بيروت: مركز دراسات الوحدة العربية. ٢٠١٣.

٥. حاتم، محمد عبدالقادر. *العولمة: مالها وماعليها*. القاهرة: الهيئة المصرية العامة للكتاب. ٢٠٠٥.

٦. عبدالحكيم، منصور. *الحرب السيبرانية*. الجيزة: دار الفاروق للإستثمارات الثقافية. ٢٠٢٢.

٧. قدور، عمر احمد. *شكل الدولة واثره في تنظيم مرفق الامن*. القاهرة: مكتبة مدبولي. ١٩٩٤.

٨. ماتلار، أرمان. *المراقبة الشاملة: أصل النظام الأمني*. تر: ريمون شاهين. بيروت: شركة المطبوعات للتوزيع والنشر. ٢٠١٣.

٩. مصطفى، فرهاد جلال. *الأمن ومستقبل السياسة الدولية*. السليمانية: أكاديمية التوعية وتأهيل الكوادر. ٢٠١٠.

١٠. ئاكرەيى، نجدت صبري. *الإطار القانوني للأمن القومي*. أربيل: مطبعة زانكو. ٢٠٠٤.

ثانياً: المجلات العلمية:

١- الدوري، عبدالرحمن احمد. "الامن القومي العربي: المفهوم- التحديات- المواجهة." *مجلة الدفاع*، ٤ (١٩٨٨): ١٤١-١٤٢.

٢- الرمضاني، مازن اسماعيل. "الامن القومي العربي و الصراع الدولي." *مجلة العلوم السياسية*، ٢ (١٩٨٨): ٦٣.

٣- العربي، محمد مسعد. "نظرية الأمننة وتصاعد الجدل حول التوسع في مفهوم الأمن." *مجلة اتجاهات الأحداث*، ٨ (مارس ٢٠١٥):٤.

٤- الناصري، سعد ياسين. "محددات مفهوم الامن القومي العربي." *بيت الحكمة* ، ٥، (شتاء ٢٠٠٠-٢٠٠١): ٥١.
٥- رشاد، سوزي. "التهديدات الأمنية الهجين في العلاقات الدولية: السيبرانية والذكاء الأصطناعي نموذجاً." *مجلة وادي النيل للدراسات والبحوث الإنسانية والإجتماعية والتربوية*، ٣٣، (كانون الأول ٢٠٢٢)، ٦٦٣-٧٠٠.
٦- عبدالكريم، محمد زهير. "الإرهاب السيبراني: أزمة عالمية." *قضايا سياسية*، ٦٤، (شباط ٢٠٢١): ٢٧٧-٢٩٤.
٧- فهمي، عبدالقادر محمد. "في مفهوم الأمن القومي والأمن القومي العربي." *مجلة الأمن القومي*، ٣ (١٩٨٨): ٧٣.

ثالثاً: دراسات وأوراق علمية:

١- علوي، مصطفى. "الأمن الإقليمي بين الأمن الوطني والأمن العالمي." المركز الدولي للدراسات المستقبلية والإستراتيجية ٤، (٢٠٠٥): ٨-١٠.
٢- كوستيجان، سين إس. وهينيسي مايكل إيه. *الأمن السيبراني: منهج مرجعي عام*، (دب.: أكاديمية الدفاع الكندية، ٢٠١٦)، ١٧.
٣- نانيس عبدالرزاق فهمي، "مستقبل الأمن السيبراني في عصر الميتافيرس،" *آفاق مستقبلية (اصدارة سنوية)*، (القاهرة: مركز المعلومات ودعم اتخاذ القرار برئاسة مجلس الوزراء (٣)، (كانون الأول ٢٠٢٣)، ٣٠٥.
٤- إيهاب خليفة، "تهديدات الأمن الإقليمي العربي في الميدان الخامس: نحو إستراتيجية للحماية،" *أوراق السياسات الأمنية*، جامعة نايف العربية للعلوم الأمنية، ٢٠٢١، ٤.

رابعاً: المصادر باللغة الانكليزية

1- Kurian, George Thomas (ed. in Chief). *The Encyclopedia of Political Science*. Washington DC: CQ Press. 2011.
2- Al-Jahni, Ali bin Faiz. *Terrorism: Concept and Reality*. tr. Zubair Ahmad. Riyadh: Naif Arab Academy for Security Sciences. 2002.
3- Athanassouli, Kyriaki. Economic Implications of the Rise of Information Warfare Edited by Daras, Nicholas J. *Cyber-Security and Information Warfare*. New York: Nova Science Publishers. 2019.
4- Balzacq, Thierry. *Securitization Theory: How Security Problems Emerge and Dissolve*. London and New York: Routledge. 2011.
5- Brown, Chris and Eckersley, Robyn. (eds.) *The Oxford Handbook of International Political Theory*. Oxford: Oxford University Press. 2018.

6- Buzan, Barry, Wæver, Ole and Wilde, Jaap de. *Security: A New Framework for Analysis*. Boulder: Lynne Rienner. 1998.
7- Cavelty, Myriam Dunn and Balzacq, Thierry. (eds.) *Routledge Handbook of Security Studies*. 2nd ed. London and New York: Routledge. 2017.
8- Cavelty, Myriam Dunn and Wenger, Andreas. (eds.) Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation. London & New York: Routledge. 2022.
9- Christen, Markus, Gordijn, Bert and Loi, Michele. (eds.) *The Ethics of Cybersecurity*. Switzerland: Springer Open. 2020.
10- Clapper, James R. *Statement for the Record Worldwide Threat Assessment of the US Intelligence Community*. N.P.: Office of the Director of National Intelligence. 2015.
11- Crocker, Chester A., Oster, Fen and Aall, Pamela. *Turbulent Peace: The Challenges of Managing International Conflict*. Washington DC: United States Inst of Peace Pr. 2001.
12- Czosseck, Christian and Geers, Kenneth. *The Virtual Battlefield: Perspectives on Cyber Warfare*. Amsterdam: IOS Press. 2009.
13- Daras, Nicholas J. (ed.) *Cyber-Security and Information Warfare*. New York: Nova Science Publishers. 2019.
14- Eriksson, Johan and Giacomello, Giampiero. *International Relations and Security in the Digital Age*. London and New York: Routledge. 2007.
15- Ghernaouti, Solange. *Cyber Power: Crime, Conflict and Security in Cyberspace*. Lausanne: EPFL Press. 2013.
16- Guiora, Amos N. *Cybersecurity: Geopolitics, law, and policy*. London and New York: Routledge 2017.
17- Guitton, Clement. *Inside the Enemy's Computer: Identifying Cyber Attackers*. Oxford and New York: Oxford University Press. 2017.
18- Kolodziej, Edward A. *Security and International Relations*. Cambridge: Cambridge University press. 2005.
19- Kremer, Jan-Frederik and Müller, Benedikt. (eds.) *Cyberspace and International Relations: Theory, Prospects and Challenges*.

Heidelberg: Springer. 2014.

20- Lopez, Javier, Setola, Robert and Wolthusen, Stephen D. (eds.) *Critical Information Infrastructure Protection: Information Infrastructure Models، Analysis, and Defense*. Berlin: Springer Verlag. 2012.

21- Mingst, Karen A. and Arreguin-Toft, Ivan M. *Essentials of International Relations*. 7th ed. New York and London: W. W. Norton & Company. 2017.

22- Shaw, Martin. *Global Society and International Relations: Sociological Concepts and Political Perspectives*. Cambridge: polity press. 1994.

23- Sheehan, Michael. *International Security: An Analytical Survey*. Boulder: Lynne Rienner Publishers. 2005.

24- Schneier, Bruce. *Secrets and Lies: Digital Security in a Networked World.* Indiana: John Wiley & Sons, Inc. 2000.

25- Stevens, Tim. *Cyber Security and the Politics of Time*. Cambridge: Cambridge University Press. 2016.

26- Bogusz, Tanja. "Fieldwork in the Anthropocene: on the Possibilities of Analogical Thinking between Nature and Society." *Since & Technology Studies* 36:2 (September 2023): 3-25.

27- Carr, Madeline and Lesniewska, Feja. "Internet of Things, Cybersecurity and Governing Wicked Problems: Learning from Climate Change Governance." *International Relations* 34:3 (2020): 391-412.

28- Cavelty, Myriam Dunn and Egloff, Florian J. "The Politics of Cybersecurity: Balancing Different Roles of the State." *St Antony's International Review* 15:1 (2019): 37-57.

29- Christou, George. "The Collective Securitisation of Cyberspace in the European Union." *West European Politics* 42 (2) (2018): 278-301.

30- Clarke, Richard. "War from Cyberspace." National Interest 104 (November/December 2009): 31-36.

31- Conway, Maura. "What Is Cyberterrorism." *Current History* 101 (December 2002): 436-442.
32- Górka, Marek. "Conceptualising Securitisation in the Field of Cyber Security Policy." *Journal of Modern Science* 53:4 (December 2023): 263-290.
33- Hansen, Lene and Nissenbaum, Helen, "Digital Disaster, Cyber Security, and the Copenhagen School." *International Studies Quarterly* 53 (4) (December 2009): 1155-1175.
34- Horowitz, Michael C. "Do Emerging Military Technologies Matter for International Politics." *Annual Review of Political Science* 23 (May 2020): 385-400.
35- Lacy, Mark and Prince, Daniel. "Securitization and the Global Politics of Cybersecurity." *Global Discourse* 8 (1) (February 2018):100-115.
36- Lonsdale, David J. "Information Power: Strategy, Geopolitics, and the Fifth Dimension." *Journal of Strategic Studies* 22(2–3) (1999): 137-157.
37- Muhammad, Ali and Riyanto, Sugeng. "International Security Studies: Origins, Development, and Contending Approaches." *Austral: Brazilian Journal of Strategy & International Relations* 10:20 (December 2021): 230-249
38- Solms, Rossouw von and Niekerk, Johan van. "From Information Security to Cyber Security." *Computers & Security* 38 (2013): 97-102.
39- Stevens, Tim. "Global Cybersecurity: New Directions in Theory and Methods." *Politics and Governance* 6:2 (June 2018): 1–4.
40- Thomas, Raju G.C. "What Is Third World Security." *Annual Review of Political Science* 6 (June 2003): 205-232.
41- Weber, Jutta and Kampf, Katrin M. "Technosecurity Cultures: Introduction." *Science as Culture* 29:1 (March 2020): 1-10.
42- Caldwell, Lance. "Cybersecurity as a Human Right: A Reformulation of the Theoretical Framework of Securitization Theory." PhD Dissertation. Northcentral University/School of

Business. 2021.

43- Nazli Choucri (Preparator), Explorations in Cyber International Relations: A Research Collaboration of MIT and Harvard University, (Cambridge and Mass: MIT Press, 2015).
44- Reardon, Robert and Choucri, Nazli, *The Role of Cyberspace in International Relations: A View of the Literature*. Massachusetts: Massachusetts Institute of Technology. 2012: 36p.
45- Yangyue, Liu. "The Conceptual Underpinning of Cyber Security Studies". Edited by Choucri, Nazli and Jackson, Chrisma. *Perspectives on Cybersecurity: A Collaborative Study*. Massachusetts: Massachusetts Institute of Technology. 2015: 16-35.

سادساً: مصادر إلكترونية:

١- إرم نيوز. "اعتبرتهما تهديدا أمنيا: إيران تحظر واتساب وإنستغرام نهائيا." الموقع الإلكتروني لإريم نيوز- تأريخ النشر ٢٢ تشرين الأول ٢٠٢٢. متوفر على الرابط:
2- https://www.eremnews.com/ news/world/ctxgbaixx2 (زيارة الموقع ٢٢ تشرين الأول ٢٠٢٢)

3- Brachman, Jarret. "Watching the Watchers." Foreign Policy, October 12, 2010. available at the link:
4- https://foreignpolicy.com/2010/10/12/watching-the-watchers/ (accessed July 12, 2021).

5- Nye, Joseph S., "How Will New Cybersecurity Norms Develop." Project Syndicate, March 8, 2018. available at the link
6- https://www.project-syndicate.org/commentary/origin-of-new-cybersecurity-norms-by-joseph-s--nye-2018-03?barrier=accesspay (accessed June 25, 2022).