أمننة الفضاء السيبراني في السياسة الخارجية اليابانية: التحالف السيبراني مع الولايات المتحدة الامريكية_ دراسة حالة

م.د علي غسان سامي
الجامعة العراقية–رئاسة الجامعة–قسم شؤون الطلبة والتسجيل العام

المستخلص

شهد الفضاء السيبراني في العقود الأخيرة تحولاً جذرياً في بنيته ووظائفه، إذ لم يُعد مجرد ساحة للتفاعل الرقمي والتبادل المعلوماتي، بل أصبح ميداناً استراتيجياً للصراع والمنافسة بين الدول، الأمر الذي أدى إلى "أمننته" وجعله جزء لا يتجزأ من الحسابات الأمنية والسياسات الخارجية، وفي هذا السياق، برزت اليابان بوصفها دولة فاعلة تسعى إلى تعزيز أمنها السيبراني عبر تبنّي سياسات متقدمة، أهمها تعزيز شراكتها مع الولايات المتحدة الأمريكية عبر ما يُعرف بالتحالف السيبراني.

إذ يُركّز هذا البحث على دراسة أبعاد أمننة الفضاء السيبراني ضمن السياسة الخارجية اليابانية، وتحليل التحالف الياباني–الأمريكي في المجال السيبراني بوصفه إحدى أهم أدوات مواجهة التهديدات العابرة للحدود، لا سيما في ظل تصاعد التحديات القادمة من قوى كبرى مثل الصين وكوريا الشمالية. إذ يعتمد البحث على المنهج التحليلي–الوصفي ومنهج دراسة الحالة، ويستعرض الوثائق الرسمية، والمواقف السياسية، والمبادرات الثنائية ذات الصلة.

وفي هذا الإطار تهدف هذه الدراسة إلى توضيح كيف تحوّل الأمن السيبراني من مسألة تقنية إلى أولوية استراتيجية في السياسة الخارجية اليابانية، وتبيان كيف تُوظف اليابان تحالفاتها الأمنية، ولا سيما مع الولايات المتحدة الامريكية، لحماية مصالحها في الفضاء الرقمي.

الكلمات المفتاحية: أمننة الفضاء السيبراني، السياسة الخارجية اليابانية، التحالف السيبراني، الأمن السيبراني، العلاقات اليابانية الأمريكية.

Securitization of Cyberspace in Japanese Foreign Policy: The Cyber Alliance with the United States A Case Study

Dr. Ali Ghassan Sami- Al-Iraqi a University

Abstract

In recent decades, cyberspace has undergone a profound transformation from a domain of digital communication to a strategic arena of conflict and interstate competition. This shift has led to the securitization of cyberspace, making it a critical component of national security and foreign policy strategies. In this context, Japan has emerged as an active player aiming to bolster its cyber security capabilities, most notably through its alliance with U.S.

This study explores the securitization of cyberspace within Japan's foreign policy framework, focusing on the Japan–U.S. cyber alliance as a case study. The research analyzes how Japan has positioned cybersecurity as a central pillar in its international relations, particularly as threats from state and non-state actors, such as China and North Korea, continue to escalate.

Keywords: Securitization of Cyberspace, Japanese Foreign Policy, Cyber Alliance, Cybersecurity, Japan–US Relations.

المقدمة

لقد شهد العالم في العقود الاخيرة تحولاً جذرياً في مفهوم الامن القومي، إذ لم يعد مقتصراً على الدفاع التقليدي عن الحدود البرية والبحرية والجوية، بل أمتد ليشمل بعداً جديداً وأكثر تعقيداً يتمثل في الفضاء السيبراني، إذ أضحت التهديدات السيبرانية تُمثل تحدياً وجودياً للدول؛ مما دفع العديد منها إلى إعادة صياغة سياستها الخارجية والامنية لمسايرة هذا التهديد المتنامي، وفي هذا السياق برزت اليابان بوصفها دولة متقدمة لا سيما على الصعيد التكنولوجي تواجه تحديات سيبرانية متزايدة دفعتها بالمحصلة إلى تبني نهج أمننة الفضاء السيبراني بوصفها جزء لا يتجزأ من سياستها الخارجية.

إذ تأتي الشراكة السيبرانية بين اليابان والولايات المتحدة الامريكية في صدارة التوجه، إذ تسعى اليابان من خلالها إلى تعزيز قدراتها الدفاعية الرقمية، ناهيك عن ردع الهجمات السيبرانية المحتملة، وضمان الامن القومي في بيئة دولية تتسم بالتحول السريع والتنافس الجيوسياسي لا سيما في مجالات التي تمس جانب التكنولوجيا والمعلومات، إذ تُعد هذه العلاقة تحالفاً استراتيجياً يعكس حالة التقاطع بين الامن السيبراني والمصالح الجيوسياسية في منطقة الهندوباسيفيك في ظل تصاعد التهديدات من قوى دولية فاعلة مثل الصين وكوريا الشمالية.

إذ تهدف هذه الدراسة إلى تحليل كيف تم توظيف الأمنة السيبرانية في السياسة الخارجية اليابانية؟، وما هي الابعاد الاستراتيجية لهذا التحالف مع الولايات المتحدة الامريكية، فضلاً عن تسليط الضوء على السياق الدولي والاقليمي الذي فرض هذا التحول، واختبار مدى نجاحه في تعزيز أمن اليابان السيبراني.

وفي ظل الاعتماد المتزايد على البنية التحتية الرقمية في القطاعات الحيوية من الطاقة والنقل وصولاً إلى المصارف والدفاع باتت الهجمات السيبرانية تُمثل خطراً مباشراً على استقرار الدول ووظائفها الحيوية، وقد أدركت اليابان ان التصدي لهذه التهديدات لا يمكن

ان يتم ضمن أطار أمني داخلي فحسب، بل يستوجب بناء شراكات دولية قوية لا سيما مع قوى تكنولوجية مثل الولايات المتحدة الامريكية، التي تربطها بها علاقات استراتيجية تاريخية منذُ نهاية الحرب العالمية الثانية.

وقد جاء هذا التوجه نحو أمننة الفضاء السيبراني- أي تحويل قضايا الانترنيت والتكنولوجيا إلى قضايا أمن قومي بوصفها جزء من عملية اعادة تعريف الاولويات الامنية في السياسة الخارجية اليابانية وهو ما انعكس في مجموعة من الوثائق الاستراتيجية اليابانية مثل استراتيجية الامن القومي واستراتيجية الدفاع السيبراني، فضلاً عن الخطط المشتركة مع الولايات المتحدة الامريكية لتعزيز التعاون في مجال تبادل المعلومات الاستخبارية والتدريبات المشتركة، ناهيك عن الاستجابة للهجمات السيبرانية المحتملة.

إذ يُعد التحالف السيبراني بين اليابان والولايات المتحدة نموذجاً معبراً عن كيفية تحول الفضاء السيبراني إلى ساحة تنافس وصراع دولي، إذ يتداخل عبرها الامن مع السياسة والاقتصاد والتكنولوجيا، كما يمثل هذا التحالف استجابة عملية للتهديدات المتزايدة بين الفاعلين ممن يستخدمون الفضاء السيبراني كسلاح لتحقيق أهداف سياسية أو عسكرية وحتى أحياناً تخريبية.

ومن هنا تسعى هذه الدراسة إلى استكشاف دوافع أمننة الفضاء السيبراني في السياسة الخارجية اليابانية، فضلاً عن تحليل أبعاد التعاون السيبراني مع الولايات المتحدة الامريكية بوصفها دراسة حالة؛ وذلك لفهم كيف تُعاد صياغة التحالفات التقليدية في ضوء تهديدات وصفت بكونها غير تقليدية، وكيف توظف الدول التكنولوجيا بوصفها أداة للردع والسيطرة والنفوذ في ضوء النظام الدولي المعاصر.

أولاً: أهمية البحث: تنبع أهمية هذا البحث من كونه يتناول أحد أبرز التحولات في مفاهيم الامن والسياسة الخارجية المعاصرة، والمتمثل في أمننة الفضاء السيبراني بوصفه

مجالاً جديداً للصراع والتعاون بين الدول، إذ تكمن الاهمية في كون البحث يساهم في تطوير فهم أعمق لنظرية الأمنة ضمن أطار مدرسة كوبنهاغن من خلال تطبيقها على الحالة اليابانية في الفضاء السيبراني، وهو مجال لا يزال بحاجة إلى المزيد من الدراسة في الادبيات الغربية، فضلاً عن ان البحث يسلط الضوء على السياسات العملية التي اعتمدتها اليابان لتحصين فضائها السيبراني؛ مما يشكل نموذجاً لدول أخرى تواجه تحديات سيبرانية متماثلة، والاهم من ذلك ان هذه الدراسة تكشف عن دور التحالفات السيبرانية لا سيما بين اليابان والولايات المتحدة في إعادة تشكيل توازنات القوة الاقليمية والدولية في ظل تصاعد التهديدات غير التقليدية.

ثانياً: اشكالية البحث: تتمثل اشكالية البحث في السؤال الرئيس الآتي: كيف تم توظيف أمننة الفضاء السيبراني في السياسة الخارجية اليابانية وما الدور الذي يلعبه التحالف السيبراني مع الولايات المتحدة الامريكية؟، وينبثق من هذا السؤال سؤالين فرعيين يشكلان محور هذه الدراسة وهما:

- ما الابعاد الامنية للفضاء السيبراني في الاستراتيجية الوطنية اليابانية؟
- ما أبعاد التحالف السيبراني الامريكي الياباني وانعكاساته على السياسة الخارجية اليابانية؟

ثالثاً: فرضية البحث: يستند البحث على افتراض مفادهُ إن أمننة الفضاء السيبراني قد أصبحت أداة مركزية في السياسة الخارجية اليابانية وقد تم توظيفها من خلال تعزيز التحالف السيبراني مع الولايات المتحدة الامريكية؛ بهدف مواجهة التهديدات السيبرانية المتنامية، وضمان الردع الرقمي، ودعم المكانة الدولية لليابان في ضوء بيئة أمنية معقدة.

رابعاً: منهجية البحث: إذ تعتمد هذه الدراسة على المنهج التحليلي الوصفي مدعوماً بمنهج دراسة الحالة، عبر تحليل أبعاد الامننة السيبرانية في السياسة الخارجية اليابانية،

فضلاً عن وصف طبيعة التهديدات السيبرانية التي تواجه اليابان وتقييم استجابتها المؤسسية لها، ناهيك عن تحليل التحالف السيبراني الياباني الامريكي كدراسة حالة سبيلاً لرصد تطوره وأهدافه وانعكاساته على الامن الاقليمي والدولي.

خامساً: هيكلية البحث: تنتظم هذه الدراسة في مبحثين فضلاً عن المقدمة والخاتمة والاستنتاجات، إذ يُعالج المبحث الاول الابعاد الامنية للفضاء السيبراني في الاستراتيجية الوطنية اليابانية، في حين يذهب المبحث الثاني في البحث عن أبعاد التعاون السيبراني الياباني–الامريكي.

المبحث الاول

الابعاد الامنية للفضاء السيبراني في الاستراتيجية الوطنية اليابانية

تعتمد الاستراتيجية الوطنية اليابانية على منظومة متكاملة تجمع بين الحماية، الردع، التعاون الدولي، التطوير التقني، والتوعية القانونية لضمان أمن الفضاء السيبراني، فضلاً عن حماية المصالح الوطنية في عالم رقمي متغير، لذا يُقسم هذا المبحث الذي حمل عنوان الابعاد الامنية للفضاء السيبراني في الاستراتيجية الوطنية اليابانية إلى مطلبين، الاول يبحث في مفهوم الامننة وتطبيقه على الفضاء السيبراني، في حين يعالج الثاني: تطور ادماج الفضاء السيبراني في العقيدة الامنية اليابانية، وكما في التفصيل الآتي:

المطلب الاول: مفهوم الامننة وتطبيقه على الفضاء السيبراني:

إذ تُشير الامننة في اللغة العربية في انها مصدر من الفعل أمَّن أي جعل الشيء آمناً مثل أمن البلد: أي أطمأن به أهله " رَبِّ اجْعَلْ هَذَا بَلَدًا آمِنًا" سورة البقرة:١٢٦ وهي تدل على إضفاء صفة الأمن أو الحماية على شيء ما أو في سياق ما من حيث البُنية، وبطبيعة الحال الأمننة على وزن فعللة: وهي صيغة تدل على تحويل حالة أو صفة إلى أخرى، أي تحويل شيء ما إلى قضية أمنية[١]، أما من الناحية الاصطلاحية الأمننة(Securitization) تُعرّف على أنها: عملية خطابية يتم عبرها تقديم قضية معينة

بوصفها خطر أمني وجودي يهدد الكيان المرجعي إن كان دولة، مجتمع، قيم، وأفراد، بهدف تبرير اتخاذ إجراءات استثنائية تتجاوز ما هو معتاد في السياسة العادية[٢] .

ولقد طورت "مدرسة كوبنهاغن" للأمن، وعلى رأسها الباحث باري بوزان مفهوم الامننة Securitization، إذ يُشير هذا المفهوم إلى عملية تحويل قضية معينة من موضوع عادي إلى موضوع أمني يُنظر إليه على أنه تهديد وجودي، مما يبرر اتخاذ إجراءات استثنائية لمواجهته، حتى وإن كانت خارج الإطار الديمقراطي أو القانوني المعتاد[3]. كما موضح في الجدول الآتي:-

جدول ١ (عناصر الأمننة وفق منظور مدرسة كوبنهاغن)

العنصر	الوصف
فاعل الامننة	الجهة التي تُصدر خطاب الأمن (مثل الدولة، السياسيين، الإعلام)
الكيان المرجعي	من يُراد حمايته (الدولة، المجتمع، الأفراد، القيم)
التهديد الوجودي	ما يُعرض الكيان للخطر أو الفناء (كالهجوم السيبراني، الإرهاب)
الجمهور/المتلقي	من يُفترض أن يقتنع بأن التهديد حقيقي ويقبل الإجراءات
مستوى القبول	لا تتحقق الأمننة إلا إذا أقنع الخطاب الجمهور بالتهديد

الجدول من إعداد الباحث استنادا إلى:

Jonathan Bright, Securitization, Terror and Control: towards a theory of the breaking point, Cambridge University, 2012, pp3-8.

وبقدر تعلق مفهوم الامننة وتطبيقه على مجال الامن السيبراني، إذ تُعرف الامننة في مجال الامن السيبراني في انها عملية تصوير قضايا الفضاء السيبراني مثل القرصنة، الهجمات السيبرانية، التجسس الرقمي، واختراق الخصوصية كتهديدات وجودية للأمن

القومي أو السيادة الوطنية أو حتى الأفراد، مما يبرر اتخاذ إجراءات استثنائية مثل تشديد الرقابة، إصدار قوانين صارمة، أو حتى شن هجمات سيبرانية مضادة، وتُعرف كذلك في انها عملية خطابية–سياسية يتم عبرها تصوير قضايا تتعلق بالفضاء السيبراني مثل الهجمات الإلكترونية، اختراق البيانات، التجسس الرقمي، التلاعب بالمعلومات كـ"تهديدات وجودية" تستدعي ردود فعل استثنائية من الدول أو الفاعلين السياسيين والأمنيين، تتجاوز آليات السياسة العادية وتبرر تبنّي إجراءات أمنية غير اعتيادية [4].

إذ لم يُعد الفضاء السيبراني(Cyberspace) مجالًا تقنياً فقط، بل أصبح ساحة جديدة للصراعات، وبالتالي فإن تحول قضاياه إلى تهديدات أمنية هو تطبيق صريح للأمننة، إذ تحدث الامننة في المجال السيبراني عبر عنصر الخطاب أي الجهات السياسية أو الأمنية التي تقدم قضية سيبرانية (مثل هجوم إلكتروني) كـ تهديد وجودي، فضلاً عن الهدف أي حماية السيادة الرقمية، البنية التحتية الحرجة، البيانات الشخصية، أو الديمقراطية، ناهيك عن عنصر النتيجة التي يتم تبريرها عبر: تشريع قوانين رقابة إلكترونية. ، إنشاء وكالات للأمن السيبراني، فضلاً عن شن هجمات سيبرانية مضادة، وفرض قيود على حرية الإنترنت[٥]. لذا في الجدول الآتي يوضح بعض الحالات والجانب التطبيقي لها من منظور الامننة.

جدول ٢(نماذج تحديد الامننة)

الحالة	شكل الامننة
اتهام الصين وروسيا بشن هجمات على أنظمة أمريكية	تحويل الصراع السيبراني إلى تهديد جيوسياسي
فرض رقابة على الإنترنت في دول مثل إيران أو الصين	الأمننة لتبرير السيطرة السياسية
سن قوانين مكافحة "الإرهاب الإلكتروني"	الأمننة لتوسيع سلطة الدولة

الجدول من إعداد الباحث استناداً إلى:

هبة جمال الدين، الامن السيبراني والتحول في النظام الدولي، مجلة كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، المجلد ٢٤، العدد١ ٢٠٢٣، ص ص ٢١٦-٢٢٠.

لذا الامننة السيبرانية تحوي على عدد من المزايا لعل أهمها: تعزيز الحماية الوطنية، زيادة الوعي الامني الرقمي، دعم القدرات الدفاعية الالكترونية، ودفع الشركات لتأمين بياناتها، لكنها مع ذلك لا تخلو من السلبيات أبرزها: تبرير القمع الرقمي، تقليص الحريات الرقمية، عسكرة الفضاء السيبراني، فضلاً عن فرض سيطرة مركزية على الانترنت(٦).

ولا شك ان الامننة في الفضاء السيبراني تملك من الخصوصية ما يميزها عن مجالات الامن التقليدي سواء العسكري أو الاقتصادي من حيث الطبيعة (غير مادي، افتراضي، لا حدود جغرافية له)،ومن حيث الجهات الفاعلة ليست فقط الدول، بل تشمل: أفراد، شركات، ومجموعات الهاكرز، وحتى على صعيد شكل التهديد، إذ لا يتطلب عنفاً مادياً – يمكن أن يكون اختراقاً بسيطاً لكن ذا أثر ضخم(٧).

أما على صعيد مستويات الامننة السيبرانية تتمثل في الآتي(٨):

<u>أولاً: على المستوى الوطني:</u>

- تصوير القرصنة على المؤسسات الحكومية بوصفها عمل عدائي أو حربي.
- تحويل شركات التكنولوجيا إلى جهات أمنية شريكة في الدفاع الوطني مثل Google أو Microsoft.

<u>ثانياً: على المستوى المجتمعي:</u>

- تصوير الأمن الرقمي بوصفه جزء من الهوية الوطنية أو السيادة الثقافية.
- اعتبار تطبيقات أجنبية مثلTikTok تهديداً لقيم المجتمع أو أداة تجسس.

ثالثاً: على المستوى الفردي:

دفع المواطنين لقبول رقابة الدولة على الإنترنت بهدف حمايتهم من الجرائم الإلكترونية أو الإرهاب السيبراني.

لذا فيما يلي بعض الأمثلة والتطبيقات العملية لنموذج الامننة السيبرانية كما في الجدول الاتي:

جدول ٣ (أمننة السيبرانية وفق منظور بعض القوى الفاعلة على المستوى الدولي)

الدولة (الجهة)	نموذج الامننة السيبرانية
الولايات المتحدة الامريكية	الهجمات على الانتخابات ٢٠١٦ أمننت قضية "مصداقية الديمقراطية"، وتمخض عنها فرض عقوبات وتجريم تدخلات خارجية
جمهورية الصين الشعبية	تستخدم خطاب "الأمن السيبراني القومي" لفرض رقابة صارمة على الإنترنت وتعزيز "السيادة الرقمية"
روسيا الاتحادية	تطرح فكرة "الفضاء السيبراني السيادي"، وتبرر عزل الإنترنت الروسي عن الشبكة العالمية
الاتحاد الاوروبي	يركز على الأمننة الناعمة عبر تشريعات مثل GDPRلحماية البيانات بوصفها جزء من "حقوق الإنسان الرقمية"

الجدول من إعداد الباحث استنادا إلى:

١- Vladimir Tsakanyan, The role of cybersecurity in world politics, Russia, 2017, pp342-345.

٢- Official Journal of the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/

لذا يتضح مما تقدم ان الأمننة ليست فقط إجراءً سياسياً، بل هي عملية لغوية–اجتماعية–سياسية معقدة تُعيد تشكيل طريقة فهمنا للتهديدات، وفي الفضاء السيبراني، أصبح هذا المفهوم ذا أهمية في فهم التوتر بين الأمن الرقمي والحريات الرقمية، لا سيما في ظل تصاعد التهديدات العابرة للحدود.

المطلب الثاني: تطور ادماج الفضاء السيبراني في العقيدة الامنية اليابانية

في عقد التسعينيات من القرن الماضي وبداية الألفية للقرن الحالي، كان الاهتمام بالفضاء السيبراني في اليابان محدوداً ومتمحوراً حول حماية المعلومات الحكومية والبنية التحتية الحيوية من الهجمات الإلكترونية، إذ كانت السياسات الأولية تركز على تطوير الدفاع الإلكتروني وحماية الشبكات الحكومية، مع تعاون محدود بين القطاعات العسكرية والمدنية. لكن في عام ٢٠١٤ أنشأت اليابان مركز الأمن السيبراني الوطني (NISC) لتعزيز التنسيق بين الوكالات المختلفة، وتم على أثرها إدراج الأمن السيبراني بشكل واضح في الاستراتيجية الوطنية للأمن، مع التركيز على بناء القدرات الدفاعية والردع، فضلاً عن تطوير نظام رصد وتحليل الهجمات الإلكترونية الحكومية[٩].

فمع تصاعد التهديدات السيبرانية من دول مثل الصين وكوريا الشمالية، بدأت اليابان تعزز من قدرة قوات الدفاع الذاتية على العمل في الفضاء السيبراني، ففي تحديثات استراتيجيات الدفاع الوطني لا سيما في عامي ٢٠١٨ و٢٠٢١ تم توضيح أن الفضاء السيبراني أصبح ساحة حيوية مثل البر والبحر والجو والفضاء، إذ تم على أثرها تطوير وحدات متخصصة في الفضاء السيبراني داخل قوات الدفاع الذاتية اليابانية، وتعزيز التعاون الاستخباراتي مع الحلفاء لا سيما الولايات المتحدة الامريكية، إذ لم تعد اليابان تركز فقط على الدفاع، بل بدأت تستكشف إمكانات الردع والهجوم السيبراني، مع تطوير تقنيات متقدمة لمواجهة الهجمات قبل وقوعها، لا سيما مع عَدّ الهجمات الإلكترونية تهديداً مباشراً للأمن القومي، ما يستوجب رد فعل سريع وفعال، والاهم من ذلك إنشاء

وحدات مختصة داخل الجيش الياباني للرد على الهجمات السيبرانية، والعمل على صياغة قواعد قانونية واضحة تسمح باستخدام القوة في الفضاء السيبراني ضمن إطار القانون الدولي[10] .

عملت كذلك اليابان في الدخول في المنتديات الدولية مثل مجموعة العشرين ومنظمة الأمن والتعاون في أوروبا (OSCE) لتعزيز قواعد السلوك في الفضاء السيبراني، ناهيك عن اتفاقيات تعاون مع دول الجوار لمواجهة تهديدات القرصنة والهجمات الإلكترونية[11] لذا تسعى اليابان بشكل مستمر لتطوير جهودها في وضع استراتيجيات شاملة تشمل الأمن السيبراني الصناعي، وتأمين البنى التحتية الحيوية، وضمان أمن المعلومات في المجالات الحيوية مثل الطاقة والنقل، فمع تطور الذكاء الاصطناعي وإنترنت الأشياء، أصبح هناك تركيز على تحديث العقيدة الأمنية لمواجهة تهديدات أكثر تعقيداً ومتعددة الأوجه في الفضاء السيبراني، وهذا يعطي مؤشر إلى سعي اليابان الجاد في أن تصبح قوة "سيبرانية" رائدة، وهي رؤية تعززت خلال إدارة رئيس الوزراء الاسبق شينزو آبي، والتي أدركت الأهمية الأمنية الحيوية للتهديدات السيبرانية المتزايدة. إذ لم تعزز اليابان فقط أطرها السياسية المحلية وقدراتها الدفاعية السيبرانية، بل تنسق أيضاً استراتيجياتها مع الولايات المتحدة (حليفها الرئيسي)، لمواجهة التهديدات السيبرانية، خصوصاً من الصين، إذ يشير التركيز المتزايد على الأمن السيبراني إلى تحول مهم في موقف اليابان الأمني، معترفاً بالدور الأساسي للأمن السيبراني في الدفاع والاستراتيجية. مع مبادرات تهدف إلى دمج العمليات عبر المجالات المختلفة، حيث تعمل اليابان على رفع قدراتها السيبرانية، مما يغير قدراتها الدفاعية على الأرض والبحر والجو والفضاء الخارجي، مسجلة تحولاً في استراتيجيتها الأمنية الوطنية والإقليمية[١٢]، وكما مبين في الجدول الآتي:

جدول ٤ (مراحل تكامل الفضاء السيبراني ضمن العقيدة الدفاعية اليابانية)

المرحلة	المدة الزمنية	النقاط الرئيسة
المرحلة الاولى (مجابهة التهديدات التقليدية)	قبل عام ٢٠١٠	الفضاء السيبراني كان غير مدمج في العقيدة الأمنية اليابانية، إذ كان التركيز على التهديدات الأمنية التقليدية فقط.
المرحلة الثانية (مأسسة الامن السيبراني)	٢٠١٠-٢٠١٥	تصاعد الهجمات السيبرانية العالمية، ادى الى تأسيس وكالة الأمن السيبراني الوطني الياباني (NISC) عام ٢٠١٤.
المرحلة الثالثة (إدراج الفضاء السيبراني)	٢٠١٥-٢٠٢٠	إدراج الفضاء السيبراني بوصفه ساحة دفاعية إلى جانب المجالات التقليدية، فضلاً عن تطوير قدرات الدفاع والهجوم السيبراني.
المرحلة الرابعة (التعاون الدولي)	بعد عام ٢٠٢٠	تعزيز التعاون مع الولايات المتحدة الامريكية وحلفاء آخرين لا سيما في مشاركة المعلومات والتدريبات المشتركة.
المرحلة الخامسة (التحديثات المستقبلية)	المستقبل	الاستثمار في الذكاء الاصطناعي وأمن البنية التحتية الحيوية، فضلاً عن بناء نظام دفاعي سيبراني متكامل.

الجدول من إعداد الباحث استناداً إلى:

Pratnashree Basu, From reactive to proactive: Japan's advances in cybersecurity and cyber defense strategies, ORF Observer Researcher foundation, India, 2024,

لا شك انه يبقى هناك تساؤل مهم ضمن ثنايا هذه الدراسة الا وهو ما هي أبعاد التحالف السيبراني الامريكي _ الياباني، وما انعكاساته على السياسة الخارجية اليابانية؟ وهذا بطبيعة الحال سيتم معالجته في المبحث التالي.

المبحث الثاني

أبعاد التعاون السيبراني الياباني–الامريكي

إنَّ التعاون السيبراني الياباني–الامريكي ليس مجرد شراكة فنية، بل هو تحالف استراتيجي متعدد الأبعاد يشمل الأمن، التكنولوجيا، الاقتصاد، السياسة، والقانون. يمثل استجابة مشتركة لعالم تزداد فيه التهديدات الرقمية تعقيداً، ويعكس رغبة البلدين في قيادة النظام السيبراني العالمي القائم على القيم الديمقراطية والانفتاح، لذا يُقسم هذا المبحث الذي حمل عنوان أبعاد التعاون السيبراني الياباني–الامريكي الى مطلبين، يُعالج الاول منها التحالف السيبراني في إطار الشراكة الامنية اليابانية–الامريكية، في حين الثاني يذهب في البحث عن انعكاسات هذا التحالف على السياسة الخارجية اليابانية.

المطلب الاول: التحالف السيبراني في إطار الشراكة الامنية اليابانية–الامريكية

أضحى الفضاء السيبراني ساحة مركزية لصراعات القوى العظمى، فالصين وروسيا وكوريا الشمالية طورت قدرات هجومية سيبرانية؛ مما أدى إلى تزايد القلق لدى كل من اليابان والولايات المتحدة، فالهجمات المتكررة على البُنية التحتية اليابانية، ومنها تسرب بيانات من مؤسسات حكومية، فضلاً عن الهجمات القرصنة الالكترونية بين الحين والاخر من كوريا الشمالية والتي استهدفت شبكات مصرفية في اليابان، على اثر ذلك توسع التحالف الياباني–الأمريكي، فالتحالف الأمني التقليدي بين الولايات المتحدة واليابان كان مبنياً على الردع العسكري التقليدي، لا سيما في ظل التهديد النووي من كوريا الشمالية. ومع التطورات الأخيرة، أصبح من الضروري توسيع هذا الردع ليشمل

الفضاء السيبراني، بحيث يُنظر إلى الهجمات السيبرانية بنفس خطورة الهجمات العسكرية[13].

فالعلاقات السيبرانية كانت في بداياتها غير رسمية ومحدودة، وتركزت على تبادل المعلومات بشأن التهديدات الإلكترونية، في سياق الشراكة الأمنية الأوسع التي بدأت منذُ معاهدة الأمن المشترك لعام 1960، فمع تصاعد هجمات القرصنة على الشركات اليابانية والبُنية التحتية، بدأ النقاش حول تعزيز التعاون السيبراني، وفي عام 2013 بدأ الاعتراف الرسمي بالفضاء السيبراني بوصفه جزء من المجالات الأمنية المشتركة، حين أعلنت وزارة الدفاع اليابانية لأول مرة إدراج الأمن السيبراني ضمن أولويات الدفاع الوطني، وفي أبريل من عام 2015، خلال مراجعة المبادئ التوجيهية للتعاون الدفاعي بين البلدين، تم إدراج الأمن السيبراني بوصفه أحد مجالات التعاون الأمني الثنائي، جنباً إلى جنب مع الدفاع الفضائي والصاروخي، وفي عام ٢٠١٨، تم إطلاق الحوار السيبراني الثنائي(Japan–U.S. Cyber Dialogue) لتنسيق السياسات وتبادل الخبرات بين المسؤولين من وزارتي الخارجية والدفاع، وبعدها وتحديداً في عامي ٢٠٢١–٢٠٢٢، ومع تصاعد التوترات مع الصين وكوريا الشمالية، بدأ التركيز على تحويل التعاون من الدفاع فقط إلى الردع السيبراني والهجمات الوقائية[14].

ومن ثم بدأ التحالف يدخل في نقطة تحول جديدة وتحديداً في يناير من عام ٢٠٢٣، عبر اجتماع ٢+٢ (وزيري الخارجية والدفاع من كلا البلدين)، إذ تم تأكيد على أن الهجوم السيبراني واسع النطاق يمكن أن يفعّل المادة الخامسة من معاهدة الأمن المشترك، إذ ان هذا الحدث يمثل نقطة الانطلاق الفعلية لما يُمكن تسميته بـ"التحالف السيبراني الرسمي" (كما مبين في الجدول ٥)، إذ تم ضم الفضاء السيبراني إلى نطاق الدفاع المشترك الصريح،ناهيك عن تطوير قوات سيبرانية مشتركة لتبادل الخبرات وشن عمليات دفاع نشطةActive Cyber Defense ، ومحاكاة الحرب السيبرانية ضمن

تدريبات مثل Keen Edge و Cyber Storm، والاهم من ذلك دمج الذكاء الاصطناعي والتحليل السلوكي في أنظمة الدفاع، وأن أي هجوم سيبراني واسع النطاق على البُنية التحتية اليابانية يُعتبر هجوماً على الولايات المتحدة أيضاً، ويستدعي رداً مشتركاً[15].

جدول ٥ (تطور التحالف السيبراني الياباني–الامريكي)

السنة	الحدث الرئيسي	الحالة
٢٠٠٠–٢٠١٠	بداية التعاون الفني والاستخباراتي المحدود	ركز التعاون على تبادل محدود للمعلومات حول التهديدات السيبرانية، دون إطار رسمي.
٢٠١١	الهجمات السيبرانية على مؤسسات يابانية (بعد زلزال فوكوشيما)	شكلت حافزًا لإعادة تقييم الأمن السيبراني الوطني.
٢٠١٣	إعلان اليابان إدراج الأمن السيبراني في استراتيجيتها الدفاعية	بداية رسمية للاعتراف بالتهديدات السيبرانية بوصفها قضية أمن قومي.
٢٠١٤	تأسيس مركز التنسيق السيبراني الوطني في اليابان(NISC)	جاء بدعم فني واستشاري أمريكي.
٢٠١٥	تحديث المبادئ التوجيهية للتعاون الدفاعي بين البلدين	تم إدراج الأمن السيبراني بوصفه مجال تعاون أمني رسمي ضمن المعاهدة الأمنية.
٢٠١٧	أول حوار سيبراني ثنائي (Cyber Dialogue)	تأسيس إطار سياسي وفني لتنسيق الجهود السيبرانية.
٢٠١٨	انطلاق تدريبات سيبرانية مشتركة	تدريب على الدفاع ضد

	بين قوات الدفاع الذاتي والقيادة السيبرانية الأمريكية	هجمات البنية التحتية.
٢٠٢١	التركيز على الردع السيبراني في المحادثات الأمنية	توسيع نطاق الشراكة ليشمل قدرات هجومية ردعية.
٢٠٢٣	تأكيد أن الهجمات السيبرانية الواسعة تُفعل المادة الخامسة من معاهدة الدفاع	نقطة التحول الحاسمة: التحالف السيبراني يدخل في نطاق الدفاع الجماعي الصريح.
٢٠٢٤	إطلاق مبادرة مشتركة للذكاء الاصطناعي والسيبراني (AI-Cyber Task Force)	تهدف إلى تطوير قدرات مبكرة على كشف الهجمات وتحييدها.

جدول من إعداد الباحث استناداً إلى:

١- Ministry of defense, Japan, Annual White Paper, 2024, Op.cit, p25.

٢- Jeffrey W. Hornung, Japan Lead, National Security Research Division; Senior Political Scientist, The U.S.–Japan Alliance: Realizing a Free and Open Indo-Pacific, USA, RAND, 2024, pp7-15.

ولا شك ان لهذا التحالف بعد استخباراتي وتقني عبر تبادل قواعد بيانات التهديدات Threat Intelligence Sharing، ودمج النظم اليابانية في شبكة المراقبة الأمريكية لحركة البرمجيات الخبيثة عالمياً، فضلاً عن إنشاء "غرف عمليات سيبرانية مشتركة" لرصد الأنشطة المشبوهة في الوقت الفعلي، وسيساهم هذا التحالف في إسناد البعد

الاقتصادي والخاص عبر دعم شركات التكنولوجيا اليابانية لتبني معايير الأمن الأمريكية (NIST Standards)، فضلاً عن الدخول في شراكات مع شركات مثل Hitachi وNTTو Fujitsu لتعزيز دفاعات سلاسل التوريد، والتصدي للهجمات على أنظمة التحكم الصناعي(ICS) ومحطات الطاقة[١٦] .

لكن في العموم هناك تحديات تعيق تطوير التحالف السيبراني أبرزها: قوانين الخصوصية اليابانية إذ لا تزال تقيّد تبادل البيانات مع جهات أجنبية، وبطبيعة الحال البيروقراطية في اليابان تُبطئ الاستجابة للهجمات السيبرانية مقارنة بالنموذج الأمريكي الأكثر مرونة، فضلاً عن نقص المهندسين المتخصصين في الأمن السيبراني في اليابان، ناهيك عن ان الولايات المتحدة تمتلك قاعدة تدريب سيبراني أوسع مثلNSA Cyber School ، بينما لا تزال اليابان تعتمد على تدريب محدود ضمن وزارة الداخلية[١٧] .

ومع ذلك يعمل كلا الطرفين على تخطي العقبات والتوجه نحو ردع سيبراني استباقي، عبر تطوير قدرة هجومية منسقة للردع دون إطلاق نار (cyber preemption) ، واعتماد مفهوم التدمير الرقمي المتبادل الذي يفترض أن الهجوم على دولة قد يؤدي إلى شلل واسع النطاق، والعمل على إدامة الحوار ووضع آلية ثلاثية مع كوريا الجنوبية تحت مظلة "شراكة المحيط الهادئ السيبرانية، فضلاً عن تعزيز الربط السيبراني مع أستراليا والهند ضمن إطار الرباعية (Quad) لاحتواء النفوذ السيبراني الصيني في منطقة الهندو باسيفيك، والعمل على التعاون في استخدام الذكاء الاصطناعي للكشف عن التهديدات قبل وقوعها، ودعم شبكات الجيل الخامس (5G) الآمنة، لا سيما في ظل التحديات المتعلقة بـHuaweiوتأمين البنية التحتية اللاسلكية[١٨].

لذا يُدرك جزء كبير من الرأي العام الياباني، خاصة في المدن الكبرى وبين الشباب، أهمية الأمن السيبراني ويدعم التعاون مع الولايات المتحدة، فاستطلاعات رأي أجراها معهد NHK في عام ٢٠٢٣ تُشير إلى إن أكثر من ٦٥٪ من اليابانيين يؤيدون تعزيز

الدفاع السيبراني، ونحو ٥٢٪ يؤيدون التعاون مع الولايات المتحدة حتى في الجوانب الهجومية السيبرانية، لكن بلا شك هناك قلق واسع لدى النخب الأكاديمية ووسائل الإعلام بشأن: انتهاك الخصوصية وتوسيع نطاق المراقبة، والخوف من تورط اليابان في عمليات سيبرانية هجومية تقودها الولايات المتحدة، فضلاً عن المخاوف التقليدية المتعلقة بـ(الانجرار إلى صراعات أمريكية)، وهو امتداد للنقاش الأوسع حول المادة التاسعة من الدستور الياباني والتي تُقيّد العمل العسكري الهجومي[١٩].

وعلى الصعيد السياسي فإن الحزب الليبرالي الديمقراطي (الحاكم) يدعم بشدة التحالف السيبراني، ويرى فيه ركيزة للأمن القومي الحديث، في حين الحزب الديموقراطي الدستوري وبعض أحزاب المعارضة تُعبّر عن تحفظات، وتطالب برقابة مدنية ومزيد من الشفافية في عمليات تبادل المعلومات[٢٠] .

المطلب الثاني: انعكاسات التحالف السيبراني الياباني-الامريكي على السياسة الخارجية اليابانية

بلا شك هناك تحول في العقيدة الأمنية اليابانية، إذ أصبح الأمن السيبراني جزءً لا يتجزأ من مفهوم الدفاع الشامل؛ مما أدى إلى: رفع مستوى اليقظة ضد الهجمات غير التقليدية، وإعداد قوات دفاع ذات قدرات سيبرانية هجومية محتملة، رغم القيود الدستورية، إذ أصبحت اليابان ولأول مرة تناقش الردع الاستباقي السيبراني بما يشمل قدرات الردع الثانية(Second-Strike Capability) ، والتوجه نحو تغيير تفسير المادة التاسعة من الدستور لإدراج الهجمات السيبرانية ضمن التهديدات التي تبرر الرد الجماعي[٢١].

ومن الناحية التقنية والاستخبارية، تتعاون اليابان مع الولايات المتحدة في تتبع وتحليل الهجمات السيبرانية المتقدمة، إذ بدأت اليابان في استثمار مبالغ ضخمة في تطوير البنية التحتية للذكاء الاصطناعي لتعزيز استقلالها السيبراني، فضلاً عن إنشاء وكالة الأمن السيبراني الوطني(NISC) ، وتؤكد اليابان دعمها المستمر للمبادئ الليبرالية في الإنترنت

وذلك عبر الانفتاح، الشفافية، وحرية الوصول، إذ تتعاون مع الولايات المتحدة وأوروبا في إنشاء أطر دولية لمساءلة الجهات الفاعلة في الهجمات السيبرانية، والاهم من ذلك ان التحالف السيبراني شجع اليابان على توسيع شراكاتها مع دول أخرى مثل أستراليا، الهند، والمملكة المتحدة(٢٢) .

لذا ان انعكاسات التحالف السيبراني الياباني–الأمريكي على توجهات السياسة الخارجية اليابانية تتجاوز المجال الأمني البحت، وتشير إلى تحولات استراتيجية أعمق في طبيعة الدور الياباني إقليمياً ودولياً. وكما في التفصيل الآتي(٢٣):-

أولاً: التحول من سياسة الحذر إلى الفاعلية الدولية: لعقود طويلة، اتبعت اليابان سياسة خارجية تتسم بالحذر والانكفاء النسبي عن الملفات الأمنية المعقدة انسجاماً مع دستورها السلمي لا سيما (المادة ٩)، لكن التحالف السيبراني يعكس توجهاً نحو سياسة خارجية أكثر جرأة، عبر: لعب دور فاعل في تشكيل قواعد الحوكمة السيبرانية الدولية، والانخراط في مبادرات أمنية خارج الحدود تحت غطاء الأمن السيبراني، فضلاً عن تعزيز حضور اليابان في المحافل الدولية بوصفها قوة مسؤولة في مواجهة التهديدات العابرة للحدود.

ثانياً: تعزيز التحالفات الثنائية والمتعددة الأطراف: إذ كان في السابق التركيز على العلاقات الثنائية لا سيما مع الولايات المتحدة تصب في الإطار التقليدي، لكن دفع التحالف السيبراني الياباني إلى إعادة صياغة توجهاتها عبر: توسيع شبكة التحالفات الإقليمية مثل الهند، أستراليا، كوريا الجنوبية عبر شراكات سيبرانية، والانخراط في أطر متعددة الأطراف مثل تحالف QUAD والشراكة من أجل الأمن السيبراني في المحيطين الهندي والهادئ، ناهيك عن تعزيز دبلوماسية الأمن السيبراني بوصفها وسيلة لتوسيع النفوذ الناعم.

ثالثاً: إعادة تعريف مفهوم الردع والدفاع: إذ لم تعد اليابان تتجه نحو الدفاع عن النفس في حالات التهديد العسكري التقليدي فقط، بل باتت اليابان ترى في الفضاء السيبراني

مجالاً رئيساً للردع، مما أدى إلى: اعتماد مبدأ الدفاع السيبراني الاستباقي (Pre-emptive Cyber Defense)، واعتبار الهجمات السيبرانية تهديداً سيادياً قد يُبرر استخدام القوة في الرد، فضلاً عن تقارب أكبر مع العقيدة الأمريكية في هذا المجال؛ مما ينعكس على الخطاب الدبلوماسي الياباني.

رابعاً: تغيير أولويات السياسة الخارجية نحو الأمن التكنولوجي: إذ تزايد التركيز على التقنيات الحساسة مثل الذكاء الاصطناعي، شبكات الجيل الخامس، الحوسبة الكمومية بوصف كل ذلك أدوات جيوسياسية، إذ أصبحت اليابان تعتمد الحيطة التكنولوجية بوصفها جزء من سياستها الخارجية، ومن مظاهره: فرض قيود على التعاون التكنولوجي مع الصين، ودعم حلفاء يشتركون في مبادئ سلاسل الإمداد الآمنة، فضلاً عن تقديم الدعم الفني السيبراني لدول نامية ضمن استراتيجية تعزيز النفوذ.

خامساً: تعقيد العلاقات مع القوى الإقليمية المنافسة لا سيما الصين وكوريا الشمالية: إذ إن التحالف يُفسر في الصين وكوريا الشمالية بأنه جزء من استراتيجية تطويق؛ مما أدى إلى: توتر متزايد في الخطاب الدبلوماسي المتبادل، واتهام اليابان بأنها تتخلى عن "الحياد الاستراتيجي" في الأمن الإقليمي، فضلاً عن مزيد من الضغوط على اليابان لموازنة تحالفها مع الولايات المتحدة بعلاقات مستقرة مع جيرانها[٢٤].

لذا يتضح مما سبق ان التحالف السيبراني مع الولايات المتحدة أحدث تحولاً بنيوياً في توجهات السياسة الخارجية اليابانية، يتمثل في: الخروج من إطار الحياد الأمني التقليدي، وتبني أدوار أكثر فاعلية ومسؤولية على الصعيد العالمي، فضلاً عن الدمج بين الأدوات الدبلوماسية والأمنية والتكنولوجية في إدارة العلاقات الدولية، وهذا التحول لا يزال قيد التشكيل، لكنه يشير إلى أن اليابان لم تعد فقط قوة اقتصادية، بل باتت تسعى بوضوح لأن تكون فاعلاً مركزياً في الأمن السيبراني العالمي.

الخاتمة والاستنتاجات

إن أمننة الفضاء السيبراني أصبحت ضرورة استراتيجية لا غنى عنها في السياسات الخارجية للدول المتقدمة، لا سيما في ظل التطور السريع للتكنولوجيا الرقمية، وتزايد التهديدات السيبرانية التي لم تعد تقتصر على الفاعلين من الدول، بل تشمل جهات غير حكومية، وجماعات منظمة، وحتى أفراداً يمتلكون قدرات تخريبية عالية.

في هذا السياق، اتخذت اليابان خطوات واضحة لتأطير الفضاء السيبراني بوصفه أحد ركائز أمنها القومي، وجاء ذلك بشكل جلي في سياستها الخارجية، لا سيما في ضوء تعزيز التحالف الاستراتيجي مع الولايات المتحدة الأمريكية، إذ انتقلت اليابان من موقف دفاعي تقليدي إلى تبنّي توجه أكثر شمولاً وتفاعلاً مع البيئة الدولية المتغيرة، مدفوعة بعوامل داخلية منها ضعف البُنية التحتية السيبرانية، وزيادة الهجمات، ومنها عوامل خارجية تتمثل في تصاعد التوترات مع الصين وكوريا الشمالية، وتنامي تهديدات الحرب السيبرانية.

إذ تبيّن الدراسة أن الأمننة السيبرانية اليابانية ليست مجرد استجابة لتحديات أمنية تقنية، بل إنها تمثل توجهاً أعمق نحو إعادة صياغة دور اليابان في النظام الدولي، وتوسيع أدوات سياستها الخارجية، بما يتماشى مع المبادئ الليبرالية والالتزامات الأمنية الجماعية ضمن التحالفات القائمة، وعلى رأسها التحالف مع الولايات المتحدة الامريكية.

لذا توصلت هذه الدراسة إلى جملة من الاستنتاجات لعل أبرزها تكمن في التفصيل الآتي:

١. **تزايد الاهتمام بالأمننة السيبرانية في السياسة اليابانية:** إذ عززت اليابان من خطابها ومؤسساتها لمواجهة التهديدات السيبرانية، فصارت تدرج الأمن السيبراني في وثائق الأمن القومي، وتوسّع من صلاحيات المؤسسات الأمنية المختصة.

٢. **التحالف مع الولايات المتحدة بوصفها دعامة أساسية:** إذ لا يقتصر التحالف السيبراني على المشاركة في المعلومات، بل يشمل كذلك تدريبات مشتركة، ومواءمة تشريعية، وتبادل تقني، ما يدل على عمق الترابط بين الأمنين القومي والسيبراني لكلا البلدين.

٣. **بروز الفضاء السيبراني بوصفه مجال صراعي جديد في شرق آسيا:** إذ تمثل التهديدات القادمة من الصين وكوريا الشمالية دافعاً رئيساً وراء أمننة الفضاء السيبراني؛ مما جعل اليابان تنظر إلى هذا المجال بوصفه بعد استراتيجي حيوي في توازن القوى الإقليمي.

٤. **التحدي القانوني والمؤسسي في الداخل الياباني:** فعلى الرغم من تقدم اليابان في المجال السيبراني، إلا أن البُنية القانونية لا تزال بحاجة إلى تحديث لمواكبة تطور التهديدات، لا سيما فيما يتعلق بالهجمات الاستباقية، والردع، والمسؤولية الدولية.

٥. **دور الفاعلين غير الحكوميين:** إذ أظهرت الدراسة أن الشركات الكبرى والقطاع الخاص الياباني يلعبان دوراً محورياً في بناء القدرة الدفاعية السيبرانية، الأمر الذي يتطلب تنسيقاً أعلى بين الدولة والقطاع الخاص.

٦. **إعادة تعريف "السيادة الرقمية":** إذ إن أمننة الفضاء السيبراني دفعت اليابان لإعادة تعريف مفهوم السيادة الرقمية بما يشمل حماية البيانات، وتعزيز السيطرة على الشبكات الوطنية، ومواجهة الاختراقات الممنهجة.

التوصيات الختامية

١. **تعزيز القدرات الوطنية عبر بناء هيكل سيبراني موحد:** ينبغي على اليابان أن تواصل جهودها في توحيد المؤسسات السيبرانية، وتحديد مسؤوليات واضحة بين الجهات المدنية والعسكرية، بما يضمن الاستجابة الفعالة للهجمات.

٢. **تبني استراتيجية هجينة تجمع بين الردع والدبلوماسية السيبرانية:** إذ ينبغي أن تجمع السياسة اليابانية بين الإجراءات الدفاعية والتحركات الدبلوماسية في الفضاء السيبراني، بما في ذلك التعاون مع الأمم المتحدة والمؤسسات الدولية لوضع معايير عالمية للسلوك السيبراني المسؤول.

٣. **تطوير إطار قانوني مرن يتماشى مع المعايير الدولية:** ضرورة تحديث القوانين الوطنية لتعزيز القدرة على التصدي للهجمات السيبرانية، مع الحفاظ على حقوق الإنسان وحماية الخصوصية الرقمية.

٤. **الاستثمار في البحث والتطوير والتدريب السيبراني:** فمن أجل ضمان مستقبل آمن، ضرورة الاستثمار في تطوير الكوادر البشرية، وتشجيع الابتكار في الأمن السيبراني، ودعم الشركات الناشئة المتخصصة في هذا المجال.

٥. **تعزيز التوعية المجتمعية والثقافة السيبرانية:** فمن الضروري نشر الوعي العام بالأمن السيبراني، وتضمينه في المناهج التعليمية، وتعزيز المسؤولية الفردية والمؤسسية تجاه الأمن الرقمي.

الهوامش والمراجع

(١) أحمد مختار عمر، معجم اللغة العربية المعاصرة، المجلد ١، القاهرة، عالم الكتب للنشر والتوزيع والطباعة، ٢٠٠٨، ص ص١٢٢-١٢٣.

(2) Barry Buzan & Ole Wæver & Jaap de Wilde, SECURITY A New Framework for Analysis, London, 1998, p23.

(3) Barry Buzan & Ole Wæver & Jaap de Wilde, Op.cit, pp23-24.

(4) محمد مسيكة، الفضاء السيبراني وتحديات الامن القومي للدول، مجلة العلوم القانونية والاجتماعية، الجزائر، جامعة زيان عاشور بالجلفة، المجلد٧، العدد٤، ٢٠٢٢، ص٤٥٨.

(٥) هبة جمال الدين، الامن السيبراني والتحول في النظام الدولي، مجلة كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، المجلد ٢٤، العدد١، ٢٠٢٣، ص١٩١.

(٦) عمر محمود مهدي ومحمد نوح، الهجمات السيبرانية وأثرها على تغير مفهوم السيادة لحدود الدولة، مجلة مداد الآداب، الجامعة العراقية، مجلة ١٤، ص ص١٠١٤-١٠٢٥.

(٧) محمد أكرم محسن، السيبرانية الماهية-الخصائص-الفواعل-الابعاد الاستراتيجية، مجلة حمورابي للدراسات، جامعة الموصل، العدد٤٣، ٢٠٢٢، ص ص٣٩٧-٣٩٩.

(٨) هبة جمال الدين، مصدر سبق ذكره، ص ص١٩٥-١٩٨.

(9) Ministry of Foreign Affairs, Japan, Diplomatic bluebook, 2024, pp212-213.

(10) Ministry of defense, Japan, Annual White Paper, 2024, pp191-193.

(11) Ibid, pp194-196.

(12) Pratnashree Basu, From reactive to proactive: Japan's advances in cybersecurity and cyber defense strategies,

(13) John A. Davis & Palo Alto Networks, The U.S.-Japan Alliance and Deterrence in Cyberspace, The US-Japan.

(14) Mina Pollmann, Japan's Ever-Evolving Signpost for Its Desired Regional Order, The U.S.–Japan Alliance

(15) Ministry of defense, Japan, Annual White Paper, 2024, Op.cit, pp339-340.

(16) Ministry of Foreign Affairs, Japan, Diplomatic bluebook, 2024, Op.cit, pp111-112.

(17) Keiichi Hori, Japan's Growing Cyber Security Talent Gap and Its Impacts, Japan, Nihon cyber defense

(18) Keiko Kono, A Japanese Perspective on Deterrence in Cyberspace Gray Zone Contingencies and the Role of the Japan-U.S. Alliance, The US-Japan Alliance & Deterring Gray Zone Coercion in the maritime Cyber & Space Domains, USA, Santa Monica, Rand, 2017, pp70-71.

(19) Mihoko Matsubara, Japan's Cybersecurity Resilience Efforts in Collaboration with the United States, U.S.-JAPAN TECHNOLOGY AND ECONOMIC SECURITY ACHIEVING RESILIENCE IN AN ERA OF DISRUPTION, 2025, pp51-54.

(20) Ministry of Foreign Affairs, Japan, Diplomatic bluebook, 2024, Op.cit, pp105-111.

٢١) رملي مخلوف، فلسفة الادارة اليابانية الحديثة واستراتيجية مواجهة التهديدات الالكترونية، مجلة الاقتصاد والتنمية، الجزائر، ص ص٤٤-٤٥.

(22) Hiroyuki Suzuki, The Strategic Role of Japan's Development Finance under the New Dimension of Digital Infrastructure,

(23) Mina Pollmann, Op.cit, pp16-23.

(24) Guilio Pugliese & Alessio Palalano, Diplomatic & Security Practice under Abe Shinzo: The case for realpolitik Japan