أثر سياسات الأمن السيبراني على الأمن القومي الأمريكي: قراءة في التجربة وفي إمكانية التطبيق على الحالة الجزائرية

Cybersecurity Policies and U.S. National Security: An Examination of Experience and Potential Applicability to the Algerian Context

ط/د بن جدو أسماء*

جامعة أمحمد بوقرة بومرداس(الجزائر)

a.bendjeddou@univ-boumerdes.dz

د. سلاف بوصبع

جامعة أمحمد بوقرة بومرداس(الجزائر)

s.bousbaa@univ-boumerdes.dz

تاريخ الارسال: 2024/09/11 تاريخ القبول: 2024/12/21 تاريخ النشر: 2024/12/22

ملخص:

*حاولنا في هذه الدراسة تحديد العلاقة بين الأمن السيبراني والأمن القومي بالتركيز على التجربة الأمريكية مع إمكانية تطبيقها على الحالة الجزائرية، فتمثلت إشكالية الدراسة في: **كيف أثرت سياسات الأمن السيبراني على الأمن القومي الأمريكي وكيف يمكن إسقاط التجربة الأمريكية على الحالة الجزائرية؟***

تقوم التجربة الأمريكية على ثلاث سياسات للأمن السيبراني مبنية على أطر قانونية ومؤسساتية، تطوير الصناعات التقنية المحلية، الإندماج في النسق الدولي للأمن السيبراني، وهي سياسات يمكن للجزائر إعتمادها كمقاربة لتقوية أمنها السيبراني نظرا لتشابهها مع الحالة الأمريكية في عنصر التهديدات السيبرانية التي عرفتها مؤخرا.

الكلمات المفتاحية: *الأمن السيبراني؛ الأمن القومي؛ السياسات؛ التهديدات السيبرانية؛ الإصلاحات.*

تصنيف جال: *O2؛ O21؛ O210.*

***Abstract**:*

*This study explores the relationship between cybersecurity and national security by focusing on the American experience and its potential application to the Algerian context. The central research question is **How Have Cybersecurity Policies Affected U.S. National Security, and How Can the American Experience Be Applied to the Algerian Context?***

Three cybersecurity strategies form the foundation of the American model: establishing legal and institutional frameworks, advancing domestic technology industries, and integrating into the global cybersecurity ecosystem. Through these strategies, America has achieved the top position globally on the Global Cybersecurity Index (GCI). Our findings indicate that key aspects of the American experience could be effectively applied to the Algerian context.

***Key words:** Cybersecurity; National Security; Policies; Cyber Threats; Reforms.*

JEL classification: O2 ; O21 ; O210.

* المؤلف المرسل: ط/د. بن جدو أسماء

مقدمة:

إن التطور الذي عرفه في أواخر القرن العشرين بعد ظهور الإنترنت والثورة التي شهدتها "تكنولوجيات الإتصال COMMUNICATION TECHNOLOGIES" و"مواقع التواصل الاجتماعي SOCIAL MEDIA"، فرضَ بيئة موازية للبيئة الطبيعية تسمى بـ"بالبيئة الرقمية"، المتكون من عناصر إفتراضية تتنقل فيها "البيانات DATA" و"المعلومات INFORMATION"، ولأن البيانات والمعلومات تعتبر عصب السياسة والإقتصاد، أصبح من الضروري البحث عن طرق متنوعة لتحصيلها من البيئة الرقمية، ونظرا لعامل التنافس الذي يحكم العلاقات بين الدول، ظهر نوع آخر من الحروب يكتسح البيئة الرقمية يعرف بـ "الحروب السيبرانية" (CYBER WARS)، وهي نوع من التنافس بين تنظيمات رسمية أو غير رسمية لإمتلاك أحدث المعلومات وتوظيفها في مجالات التنافس ضمن مساحات إفتراضية.

هذا الوضع من حالة اللإستقرار الذي خلقه التنافس في "الفضاء السيبراني CYBER SPACE"، دفع حكومات الدول إلى البحث عن مقاربات لحماية أمنها، الذي أصبحت التهديدات المرتبطة به تذهب إلى حد التأثير على "أمنها القومي NATIONAL SECURITY"، وفي ظل تزايد الهجمات السيبرانية بعد أحداث 11 سبتمبر 2001، تزايد الهاجس الأمني كثيرا من تكرارها، ومع تفاقم ظاهرة الإرهاب الدولي والجريمة المنظمة العابرة للحدود، تحول الاهتمام بالفضاء السيبراني إلى أكثر من ضرورة حتمية، تتطلب سن سياسات وقائية آنية وإستشرافية للحد من تفاقم "التهديدات السيبرانية CYBER THREATS".

إستحوذت الدول الغربية على جل الاهتمام بتجارب الأمن السيبراني نظرا لكونها الأكثرُ تضرراً، ومنه تجسد الإهتمام من خلال تبني عدة سياسات تحمي من خلالها أمنها القومي، إذ لم تصبح تلك التهديدات موجهة نحو قواعد البيانات العسكرية فقط وفق ما هو متصور، بل تعدتها إلى ضرب قواعد بيانات أخرى خاصة بالتعليم والصحة والإقتصاد وغير ذلك، بغية شل مختلف القطاعات وتعطيلها عن أداء وظيفتها، لخلق حالة من عدم الاستقرار في النظم السياسية.

مع تفاقم كل هذه العوامل، ليست الجزائر بمعزل عن ما هو حاصل في البيئة السيبرانية، ما يفرض عليها هي الأخرى تبني سياسات في مجال الأمن السيبراني حماية لأمنها القومي، ونظرا لكونها مستجدةً في هذا المجال فلم يبرز إهتمامها به إلا في العشرية الماضية، نظرا لموجة التحول الرقمي التي تعرفها مختلف القطاعات الحيوية فيها، يستوجب عليها البحث عن مقاربات وسياسات تحمي بها قواعد معلوماتها، في ظل التهديدات الإقليمية التي تحيط بها من منطقة الساحل الإفريقي خاصة.

ومنه يأتي إختيارنا لهذه الدراسة لعدة "**أسباب ذاتية**"، تتعلق بميول الباحثين للدراسات من هذا النوع نظرا لحداثتها، ومع ظهور مفاهيم أخرى في الفضاء السيبراني كـ"الذكاء الإصطناعي ARTIFICIAL INTELLIGENCE" و"التشفير ENCRYPTION"، و"السرية CONFIDENTIALITY"، و"المصادقة AUTHENTICATION"، و"أنظمة كشف ومنع التسلل IDPS"، و"إدارة الثغرات VULNERABILITY MANAGEMENT"...دفعنا هذا إلى محاولة دراسة عناصر هذه المفاهيم ونقلها للعربية بغية الإستفادة منها. أما "**الأسباب الموضوعية**" التي دفعتنا إلى إختيار هذه الدراسة، فتتعلق بما يمكن أن توفره من معلومات

حديثة تخص تجارب بعض الدول الغربية في مجال الأمن السيبراني، وأهميتها بالنسبة للأمن القومي خاصة تجربة الولايات المتحدة الأمريكية، ثم محاولة ربطها بتجربة الجزائر المستجدة في مجال الأمن السيبراني والإستفادة من بعض جوانبها في سياساتها.

بناءً على ما سبق تكون إشكالية دراستنا كالآتي:

"***كيف أثرت سياسات الأمن السيبراني على الأمن القومي الأمريكي وكيف يمكن إسقاط التجربة الأمريكية على الحالة الجزائرية*** ؟".

تتمخض عن الإشكالية جملة من التساؤلات الفرعية:

* ماذا نقصد بالأمن السيبراني والأمن القومي؟
* ما هي السياسات المعتمدة في الولايات المتحدة في مجال الأمن السيبراني؟
* كيف تتعامل الولايات المتحدة مع التهديدات السيبرانية؟
* ما هي مؤشرات تحقيق الأمن السيبراني والأمن القومي في ظل التجربة الأمريكية؟
* كيف يمكن تطبيق نتائج التجربة الأمريكية على الحالة الجزائرية؟

وقد قمنا بصياغة جملة من الفرضيات التي تحاول الإجابة عن الإشكالية المطروحة، تتمثل في:

- توفر أطر قانونية ومؤسساتية تنظم الفضاء السيبراني، أثر بشكل كبير على تعزيز مقاربتي الأمن السيبراني والقومي في الولايات المتحدة.
- أثرت سياسات البحث والتطوير على بناء نماذج فعالة للتجربة الأمريكية ضمن مجال الأمن السيبراني والأمن القومي.
- المشاركة في السياسات الدولية للأمن السيبراني، سمح بتبادل المعلومات الاستخباراتية وتنسيق الدفاعات والاستجابة للتهديدات السيبرانية العالمية في ظل التجربة الأمريكية.
- ما توفره الحالة الأمريكية من تجارب، يمكن تطبيقه على الحالة الجزائرية نظرا للتهديدات السيبرانية التي أصبحت تعانيها.

إعتمدنا في التحليل على المنهج الوصفي الذي يقوم بوصف الظاهرة وصفا علميا دقيقا يكون نوعيا (كيفيا)، يحدد لنا نوع الظاهرة وخصائصها وعلاقتها بباقي الظواهر، أما الوصف الكمي فيعطيها بعدا رقميا بالإعتماد على جملة من المؤشرات تشير إلى مدى التأثير الذي أحدثه المتغير (أ) على المتغير (ب) (عمار بوحوش، 2007، صفحة 138). وعند الحديث عن الأمن السيبراني والأمن القومي في التجربة الأمريكية، نجد أن المنهج الوصفي يقوم بوصف خصائص المفهومين، ثم يأتي الوصف الكمي ليعطي المؤشرات والمعايير والإنجازات في صورة رقمية تتضمن إحصائيات وأرقام، لمدى الأثر الذي حققته سياسات الأمن السيبراني على الأمن القومي ضمن الحالة الأمريكية.

نعتمد كذلك في دراستنا على "المنهج المقارن"، الذي يمكن إعتباره مجموعة خطوات يسلكها الباحث في المقارنة بين متغيرين أو أكثر، وتقوم المقارنة على تحديد أوجه التشابه والإختلاف بينهما، بشرط أن لا تختلف الظواهر تماما وأن لا تتشابه تماما، ثم يتم تطبيق نتائج المقارنة على حالة ما (شلبي، 1997، صفحة

71). وجاء إعتمادنا على هذا المنهج عند المقارنة بين الحالتين الأمريكية والجزائرية في مجال الأمن السيبراني والأمن القومي، لإستخلاص أوجه التشابه والإختلاف بينهما، ثم تحديد إمكانية تطبيق نتائج دراسة الحالة الأمريكية على الحالة الجزائرية.

نسعى من خلال هذه الدراسة إلى تحقيق مجموعة من الأهداف، تتلخص في محاولة الباحثين وضع تصور علمي للعلاقة بين الأمن السيبراني والأمن القومي، في ظل محدودية إعتماد معظم الدول العربية على مقاربات الأمن السيبراني في حماية أمنها القومي، ومنه يمكن أن يفيد بحثنا في إستنباط إستراتيجيات الأمن السيبراني في التجربة الأمريكية، وتطبيق نتائجها على الحالة الجزائرية التي تعتبر تجربتها حديثة، ومنه المساعدة على سن سياسات جديدة تتماشى والتهديدات السيبرانية التي عرفتها الجزائر مؤخراً.

بناء على كل ما سبق قمنا بتقسيم الخطة البحثية إلى:

1. تأصيل مفاهيمي لمصطلح الأمن السيبراني والأمن القومي.
2. سياسات ومؤسسات الأمن السيبراني في الولايات المتحدة الأمريكية.
3. الإندماج الأمريكي في النسق الدولي للأمن السيبراني والأمن القومي.
4. إمكانية تطبيق سياسات الأمن السيبراني الأمريكية على الحالة الجزائرية.

بما أن كل دراسة لها خلفيات نظرية تستند عليها وتشير إلى جوهرها أو منظورها من عدة باحثين، نستهل تحلينا بالإشارة إلى بعض الجوانب النظرية حول الأمن السيبراني والأمن القومي كما وردت في بعض الأدبيات والمراجع العربية والأجنبية.

1. تأصيل مفاهيمي لمصطلح الأمن السيبراني والأمن القومي

لا بد من إبراز مدى تقاطع مفهوم الأمن السيبراني والقومي ومدى إنسجامهما معا، للتعرف على أهم المتغيرات التي حولت النظرة إلى الأمن القومي من مجرد توظيف للقوة المادية العسكرية، إلى قوة ضمن مجال آخر هو المجال الرقمي، وكيف إنتقلت الحروب من مجرد كونها حروبا تجري في مجالات مادية ملموسة، إلى حروب إفتراضية تسمى بـ"حروب الجيل الرابع Fourth Generation Warfare أو GW4".

من ناحية ما هو أشمل، يعتبر مفهوم "الأمن القومي NATIONAL SECURITY" سباقاً في الظهور على "الأمن السيبراني CYBER SECURITY"، ومنه يمكن إعتبار الأمن القومي أشمل من الأمن السيبراني. برز الاهتمام بمصطلح "الأمن القومي" في خضم القرن 16، بعد أن إرتبط المفهوم مع مفهوم الدولة القومية ضمن معاهدة "واستفاليا" سنة 1648، وزاد الاهتمام به أكثر من الناحية الآكاديمية والعلمية في خضم الحرب الباردة، من طرف الجامعات ومخابر ومراكز البحث الأمريكية خاصة، إلى حد الوصول إلى إصدار الكونغرس الأمريكي "قانون الأمن القومي NATIONAL SECURITY LAW " سنة 1947، حيث تم التركيز عليه من الناحية المؤسساتية والتنظيمية (فرج عصام بن جليل، 2021، صفحة 127).

عرفته الأمانة العامة لجامعة الدول العربية بأنه: "**قدرة الأمة على الدفاع عن أمنها وحقوقها وصياغة إستقلالها وسيادة أراضيها وتنمية قدراتها في مختلف المجالات، مستندة في ذلك إلى القدرة العسكرية والدبلوماسية...**" (محمد، 2022، صفحة 451).

ويعني الأمن القومي الحماية ضد التهديدات أو التهديدات المحتملة الآتية من خارج الدولة أو حتى من داخلها...فهو محصلة المصالح القومية الحيوية للدولة عبر أبعاد عسكرية وسياسية وإقتصادية وإجتماعية وثقافية (عتيقة، 2023، صفحة 209).

الأمن السيبراني نعني به الإجراءات الواجب إتخاذها من الأجهزة الأمنية للحفاظ على سرية المعلومات الإلكترونية، ومنع الإختراقات الفيروسية من أجل ضمان وصول المعلومات الحاسوبية إلى الجهات المختصة في الوقت المناسب، وضمان عدم وقوعها في أيدي غير حليفة للدولة... (كلاع، 2022، صفحة 298).

الأمن السيبراني هو حماية الأجهزة الرقمية وقنوات الاتصال الخاصة بها للحفاظ على استقرارها واعتماديتها وخلوها من الخطر أو التهديد. عادةً ما يجب أن يكون مستوى الحماية المطلوب كافيًا لمنع الوصول غير المصرح به، أو التدخل الذي يمكن أن يؤدي إلى أضرار شخصية، مهنية، تنظيمية، مالية أو سياسية، كما أن الأمن السيبراني يتعلق بحماية ما هو أكثر من أجهزة الكمبيوتر، فهو يتجاوز مجرد حماية كل التكنولوجيا في الحقيقة، الأمن السيبراني يتعلق بحماية الأشخاص الذين يعتمدون بشكل مباشر أو غير مباشر على أي شيء إلكتروني (MEEUWISSE, 2015, p. 24).

يتعلق الأمن السيبراني بالفضاء السيبراني، الفضاء السيبراني يشير إلى مساحة تفاعلية تتألف من الشبكات الرقمية التي تجمع وتخزن وتتعامل مع المعلومات لتسهيل أشكال مختلفة من الاتصال، لذلك يشمل الفضاء السيبراني الإنترنت ومجموعة الأنظمة التي تدعم خدمات الإنترنت وبنيته التحتية والمشاركين فيه، تعمل خصائص الفضاء السيبراني التي نوقشت أعلاه معًا لخلق تهديدات بنفس الطريقة التي تخلق بها فرصًا متعددة، مع استمرار نمو عالم الأعمال تصبح التهديدات أكثر تعقيدًا وتزداد تكاليف الإصلاح بشكل أكبر، الأمن السيبراني يتعلق بحماية توافر المعلومات ونزاهتها وسريتها (walker, 2019, p. 13).

في عالم اليوم "المتصِل"، تسهم برامج الدفاع السيبراني في مصلحة كل مستخدم، يمكن أن يؤدي الهجوم من خلال دفاع سيبراني مخترق إلى مجموعة متنوعة من العواقب، من سرقة المعلومات الشخصية إلى الابتزاز المالي أو فقدان البيانات القيمة مثل الصور العائلية، كل ذلك يعتمد على البنى التحتية الحيوية، مثل محطات الطاقة والمستشفيات وشركات الخدمات المالية (STEVEN, 2019, p. 13).

لقد صاحب التطور السريع في التكنولوجيا السيبرانية تحديات أمنية خطيرة، تعددت أحداث الأمن السيبراني من تسرب البيانات إلى انهيار الشبكات بتواتر أعلى من السنوات الماضية، ومن أشهر هذه الأحداث "حدث سنودن SNOWDEN EVENT"*، الذي أوضح للعالم أن الأمن السيبراني له تأثير مباشر على الأمن القومي، اجتذب الأمن السيبراني اهتمامًا كبيرًا في كل من المجتمع الأكاديمي والصناعي، خاصة "تقنيات الحوسبة السحابية TECHNIQUES OF CLOUD COMPUTING"*، و"إنترنت الأشياء

* "**حدث سنودن**" يشير إلى الكشف الذي قام به "إدوارد سنودن Edward Snowden"، وهو متعاقد سابق مع وكالة الأمن القومي الأمريكية (NSA)، في عام 2013 كشفت تسريبات سنودن عن مدى الرقابة العالمية التي تقوم بها وكالة الأمن القومي والوكالات الاستخباراتية الأخرى.

* **تقنيات الحوسبة السحابية** تشير إلى مجموعة من الأساليب والأدوات التي تستخدم لتوفير وتوزيع الموارد الحوسبية والخدمات عبر الإنترنت، تساعد هذه التقنيات في تحسين كفاءة الأداء وتخزين البيانات وتوفير الوصول إلى التطبيقات والخدمات من أي مكان.

(INTERNET OF THINGS (IOT"*، و"البيانات الضخمة BIG DATA"، التي تجعل الأنظمة الشبكية الموزعة أكثر تعقيدًا وقوة وسهولة في الاستخدام (Kuan-Ching Li , 2019, p. 11).

في الوقت نفسه أصبح الأمن السيبراني جزءًا من الأمن القومي، فقد قامت الدول بإنشاء وحدات عسكرية مختصة في الهجمات السيبرانية، وأصبحت أجهزة إستخباراتها تستغل العمليات في الفضاء السيبراني، بما يتجاوز جمع المعلومات الاستخباراتية السياسية والعسكرية التقليدية، وقد توقعت "إدارة الاستخبارات الوطنية الأمريكية US Office of Director of National Intelligence" أن: "الزيادة في إستخدام الدول للعمليات السيبرانية كأداة من أدوات القوة القومية، بما في ذلك الاستخدام المتزايد من قبل الجيوش حول العالم، يرفع احتمالية زيادة الأنشطة السيبرانية التدميرية والمُعطِّلة"، ومع سعي الدول للقيام بعمليات سيبرانية أكثر عدوانية، فإنها من المرجح أن تؤثر على السكان المدنيين وتزيد من جرأة الدول الأخرى التي تسعى لتحقيق نتائج مشابهة، ومن هنا يتلازم تحقيق الأمن القومي مع قدرات الدولة في مجال الأمن السيبراني كمحدد من محددات الأمن القومي (Derek S. Reveron, 2024, p. 296) .

2. سياسات ومؤسسات الأمن السيبراني في الولايات المتحدة الأمريكية

لقد كان للتقدم في تكنولوجيا المعلومات والاتصالات تأثير هائل على المجتمعات الحديثة، ونتيجة لذلك قام عدد متزايد من الحكومات بتطوير سياسات وطنية للأمن السيبراني.

1.2 تهديدات الأمن السيبراني في الولايات المتحدة الأمريكية:

إنطلق الاهتمام بتطوير سياسة الأمن السيبراني في الولايات المتحدة بشكل خاص مع نهايات القرن 20 وبدايات القرن 21، هذه الإجراءات السياسية أثرت بشكل مباشر على الأمن القومي الأمريكي في مجالات الأمن الداخلي والدفاع والسياسة الخارجية، تشمل هذه الإجراءات الوثائق الاستراتيجية، والمبادرات التنظيمية، والإجراءات الإضافية التي نشأت من الحكومة الفيدرالية الأمريكية، معظمها من البيت الأبيض، وعلى الرغم من مناقشة سياسة الأمن السيبراني الأمريكية من قبل صناع السياسة منذ الستينيات على الأقل، فإن سياسة الأمن السيبراني الأمريكية انطلقت وأصبحت أولوية للأمن القومي خلال سنوات الرئيس الأمريكي عن الحزب الديمقراطي سابقا "باراك أوباما BARACK OBAMA"، عندما قررت الإدارة الانتقال من التدابير العشوائية والقطاعية إلى نهج أكثر تنظيماً وشمولية (Lilli, 2020, p. 01) .

كان أول هجوم إرهابي كبير على الأراضي الأمريكية منذ تفجير قنبلة TNT في وول ستريت عام 1920، الذي أسفر عن مقتل 35 شخصًا بهدف إسقاط أطول برج في المدينة وسط سحابة من غاز السيانيد، لو كان الهجوم قد تم كما هو مخطط له، لكان عشرات الآلاف من الأمريكيين قد لقوا حتفهم من التفجير، توفي ستة أشخاص وأصيب أكثر من ألف، وُجدت تفاصيل الهجوم لاحقًا على الكمبيوتر المحمول للإرهابي،

* **إنترنت الأشياء (IOT)** يشير إلى شبكة من الأجهزة والأشياء المادية التي تتصل ببعضها البعض عبر الإنترنت وتبادل البيانات والمعلومات. تتيح هذه التقنية للأشياء اليومية أن تكون "ذكية" وموصولة، مما يعزز الأتمتة والفعالية في مختلف التطبيقات، ونعطي مثالا عن ذلك الأجهزة والمستشعرات، المنازل الذكية، المدن الذكية...

وهو أول حالة معروفة لإرهابي يستخدم حاسوبًا شخصيًا لمتابعة الخطط والمعلومات، وقد كانت قلة من الأمريكيين يدركون الحجم الحقيقي للتدمير، على الرغم من أن بعد عامين كان الشخص الرئيسي المسؤول عن العملية، رجل دخل إلى الولايات المتحدة بجواز سفر عراقي تحت اسم "رمزي يوسف"، مشاركًا في مؤامرة تفجيرية أخرى في يناير 1995، أين خطط وشركاؤه لتفجير 11 طائرة تجارية أمريكية في يوم واحد، كان من المقرر أن تصنع القنابل من متفجرات سائلة مصممة لتجاوز أجهزة الكشف عن المعادن في المطارات. (others, 2012, pp. 212-213).

تعرضت وزارة الدفاع الأمريكية "PENTAGON" كذلك إلى هجمات سيبرانية ضد القوات الجوية الأمريكية في مارس 1994، إستهدفت شبكة الكمبيوتر في مختبرات "روما"، وهي منشأة تابعة للقوات الجوية في "نيويورك"، وتم تتبع الهجوم في النهاية إلى إثنين من الهاكرز الشباب " KUJI AND DATASTREAM COWBOY"، الذين كانوا من "المملكة المتحدة"، ولكنهم كانوا يستخدمون نقاط وصول مختلفة لاختراق منشآت أخرى للقوات الجوية ومنظمة حلف شمال الأطلسي (NATO) (others, 2012, p. 213).

في منتصف عام 1994، نجحت عصابة إجرامية روسية منظمة في تحويل 10 ملايين دولار من "سيتي بنك" إلى حسابات مصرفية مختلفة حول العالم، والمعروفة بـ"مغامرة سيتي بنك Citibank Caper"، كانت هذه الحادثة جزءاً من الأسباب التي دفعت إلى عقد جلسات الاستماع حول "الأمن في الفضاء الإلكتروني" في الكونغرس الأمريكي برئاسة السيناتور "سام نون Sam Nunn".

خلال صيف وخريف عام 2009، أرسل قراصنة مرتبطون بالحكومة الصينية رسائل بريد إلكتروني ورسائل فورية خبيثة إلى أهداف في جميع أنحاء العالم والولايات المتحدة، فيما يعرف بـ: "عملية أوروراOPERATION AURORA"، عندما فتح المستهدَفون الرسائل ونقروا على الرابط داخلها، قادهم متصفحهم إلى موقع ويب مستضاف في "تايوان"، كان هذا الموقع يحتوي على استغلال برمجي قام المتصفح بتحميله وتنفيذه تلقائيًا. هذه طريقة لتوصيل الشيفرة الخبيثة التي يسميها الباحثون بـ"التحميل التلقائي"، استفاد الاستغلال من ثغرة غير مصححة في متصفح "إنترنت إكسبلورر INTERNET EXPLORER"، الذي كان المتصفح المهيمن تلك الفترة، قامت الشيفرة الخبيثة بتحميل المزيد من الشيفرات الخبيثة من الموقع التايواني، متنكرة في "صورة IMAGE" لتجنب إثارة الشكوك، بعد أن تم تثبيت الشيفرة الخبيثة الإضافية على الكمبيوتر المستهدف، تواصلت مع خوادم التحكم والسيطرة التابعة للقراصنة، والتي كانت أيضًا موجودة في "تايوان"، للحصول على مزيد من التعليمات في هذه المرحلة، بعد نقرة واحدة فقط على الرابط الخطأ من المستخدم، أصبح القراصنة الصينيون في الداخل (Buchanan, 2020, p. 66).

كان لدى المخترقون ثلاثة أهداف على الأقل لعملية "أورورا"، الأول كان التجسس على المعارضين الصينيين باستخدام التكنولوجيا الأمريكية (Drummond, 2010). كان هدفهم الثاني هو تقويض ميزة الإستخبارات الأمريكية على الأرض بشكل كبير، لمعرفة الأهداف في الصين التي كانت الولايات المتحدة تراقبها من خلال أنظمة جوجل (Carlin, 2018, p. 180). الدافع الثالث وراء العملية الصينية ضد شركات التكنولوجيا الأمريكية كان رغبتهم في الوصول إلى أسرار تلك الشركات، بدءًا من شيفرة المصدر الخاصة بها،

فالشيفرة تعد شكلًا ثمينًا من أشكال الملكية الفكرية، وغالبًا ما تكون محط اهتمام كبير من قبل الحكومات الأجنبية، وكانت شيفرة المصدر للشركات التي استهدفتها عملية "أوروورا" ذات قيمة هائلة لمنافسيهم الصينيين الذين يحاولون اكتساب ميزة في السوق العالمية (Buchanan, 2020, p. 67).

في القضية رقم Case 8:14-cr-00131-CAS Document 86، يبدو أنه وفي سنة 2012 رصد "جهاز الاستخبارات الإشارية SIGNALS INTELLIGENCE APPARATUS"، التابع لوكالة الأمن القومي الأمريكية (NSA)، سلسلة من الرسائل الإلكترونية بين ثلاثة مواطنين صينيين، كان اثنان منهم قراصنة عسكريون في الصين، أما الثالث فكان رجل أعمال في أواخر الأربعينيات من عمره يدعى "سو بين SU BIN"، الذي كان يشرف على مكتب شركة الطيران "لود-تيك LODE-TECH" في كولومبيا البريطانية بكندا، كانت أعمال "لود-تيك" تتعلق بتتبع تطورات تكنولوجيا الطيران العالمية لعملائها، وكانت مهمة "سو بين" تتبع تطورات الطيران العسكري الأمريكي لصالح الصين، استخدم معرفته بالصناعة والطيران والإنجليزية لتوجيه القراصنة الصينيين نحو الأهداف الأكثر قيمة (Buchanan, 2020, p. 73).

يبدو أن وكالة الأمن القومي (NSA) قد زودت مكتب التحقيقات الفيدرالي (FBI) برسائل "SU BIN" الإلكترونية (Graff, 2018). وجد مكتب التحقيقات الفيدرالي أن "SU BIN"ونظراءه العسكريين كانوا يتجسسون على تطورات الطائرات في الولايات المتحدة لسنوات، بدءًا من عام 2009 (justice, 2016). كانت طريقة عملهم بسيطة، كان "سو بين" يحدد الشركات التي تعمل على مشاريع طائرات مهمة، ثم يُبلغ القراصنة الصينيون الذين يستخدمون "التصيد الاحتيالي SPEAR-PHISHING" للوصول إلى رسائل البريد الإلكتروني للمديرين التنفيذيين وقواعد الشركات، لكي ينسخ القراصنة قوائم كبيرة من الملفات من داخل شبكات الشركات المخترقة، ويقوم "SU BIN" بدراسة هذه القوائم بعناية لتحديد الملفات المهمة، وباستخدام هذه التقنية وصل القراصنة إلى كميات هائلة من المعلومات (Buchanan, 2020, p. 73).

الهجمات السيبرانية التي تعرضت لها الولايات المتحدة متنوعة، ما دفعها إلى البحث عن إستراتيجيات قانونية وتقنية ومؤسساتية تقيها من هذه الهجمات التي أضرت بقواعد بياناتها المالية والدفاعية.

2.2 سياسات الحماية من الهجمات السيبرانية في الولايات المتحدة الأمريكية:

بعد بضعة أيام فقط من توليه الرئاسة، أمر أوباما بإجراء مراجعة شاملة بين الوكالات لأمن الفضاء السيبراني الأمريكي، والتي تم إصدارها في نهاية ماي 2009، وجد المراجعون أن هيكل البنية التحتية الرقمية ليست آمنة، كما أوصى التقرير أن الحكومة الفيدرالية ليست منظمة بشكل فعال لمعالجة هذه المشكلة المتزايدة، وقد إعترف تقرير مراجعة الأمن السيبراني (CPR) CYBERSPACE POLICY REVIEW" بالحاجة إلى صياغة رؤية شاملة لأمن الفضاء السيبراني، كما دعت الوثيقة بشكل علني إلى أن تكون قيادة السياسة السيبرانية مرتكزة داخل البيت الأبيض، وأخيرًا قدمت (CPR) إرشادات عملية تمثلت في خطة عمل قصيرة الأجل ومتوسطة الأجل للفضاء السيبراني (Lilli, 2020, p. 08).

الوثيقة الثانية هي "إستراتيجية الأمن القومي NATIONAL SECURITY STRATEGY" التي أصدرها البيت الأبيض في ماي 2010، وقد حددت التهديدات السيبرانية كواحدة من أخطر التحديات التي تواجه

الأمن القومي والسلامة العامة والاقتصاد في الولايات المتحدة، كما رفعت (NSS 2010) البنية التحتية الرقمية الأمريكية إلى مكانة "أصل استراتيجي قومي STRATEGIC NATIONAL ASSET"، وجعلت حمايتها أولوية للأمن القومي، والأهم من ذلك أن NSS 2010 وفرت الشرعية السياسية والسلطة لجهود الأمن السيبراني للإدارة الجديدة (justice, office of justice programme, 2010).

في عام 2011، أصدرت وزارة الأمن الداخلي HOMELAND SECURITY DEPARTMENT" الرؤية الأساسية لخطة عمل واضحة، تتبناها مؤسسة الأمن الداخلي (department, 2011, p. 06)استنادًا إلى استراتيجية الأمن القومي للرئيس لعام 2010، حددت الخطة الأساسية مهمة حماية وتأمين الفضاء السيبراني كواحدة من المجالات الأساسية الخمس لوزارة الأمن الداخلي، إلى جانب منع الإرهاب، تأمين الحدود، إنفاذ قوانين الهجرة، وضمان القدرة على التكيف مع الكوارث، كما وصفت الوثيقة منطقتين رئيسيتين للعمل، المنطقة الأولى تتعلق بحماية البنية التحتية الحيوية للمعلومات، من خلال إجراءات تهدف إلى تقليل التعرض للمخاطر السيبرانية، وضمان الاستجابة والأولوية وسرعة التعافي من أضرار الهجمات، مع زيادة الحفاظ على الوعي المشترك بالمواقف وزيادة المرونة (Lilli, 2020, p. 08).

كانت المنطقة الثانية تتعلق ببناء نظام بيئي سيبراني أقوى من خلال تمكين الأفراد والمنظمات من العمل بأمان، وإنشاء واستخدام بروتوكولات ومنتجات وخدمات وتكوينات وهياكل سيبرانية أكثر موثوقية، وبناء مجتمعات تعاونية، مع إرساء عمليات شفافة تماشيًا مع مستندات أخرى من إدارة أوباما، دمجت الخطة الأساسية حماية الخصوصية والحريات المدنية في أنشطة الأمن السيبراني لوزارة الأمن الداخلي، كان استخدام وزارة الأمن الداخلي لمصطلحي "مؤسسة الأمن الداخلي HOMELAND SECURITY ENTERPRISE" و"النظام البيئي السيبراني CYBER ECOSYSTEM"، اعترافًا بأن هدف تحسين الأمن السيبراني الوطني، يتجاوز قدرة أي وكالة منفردة وأيضًا قدرة الحكومة الفيدرالية بأكملها، كما أشارت إلى ذلك وزيرة الأمن الداخلي السابقة، "جانيت نابوليتانو JANET NAPOLITANO"، بقولها: "**التهديدات السيبرانية الناشئة تتطلب مشاركة المجتمع بأسره، من الحكومة و إنفاذ القانون إلى القطاع الخاص وأعضاء الجمهور بشكل خاص**" (department, 2011, p. 03).

في 12 فبراير 2013، أصدر الرئيس أوباما مرسوما رئاسيا والآخر تنفيذيا، الأول هو " PRESIDENTIAL POLICY DIRECTIVE 21 (PPD21)" إضافة إلى "الأمر التنفيذي (EO13636) EXECUTIVE ORDER"، اللذان قدما وصفًا تفصيليًا للجهود الواسعة للإدارة في حماية البنية التحتية القومية الحيوية، كان الهدف العام هو تعزيز الأمن والمرونة للبنية التحتية القومية، مع تشجيع الابتكار التكنولوجي والاقتصادي وتعزيز الخصوصية، كما قام المرسومان بتوضيح الأدوار والمسؤوليات المناطة بالحكومة الفيدرالية، مع إعادة التأكيد على الحاجة إلى وحدة وطنية في الجهود لمواجهة مجموعة واسعة من التهديدات السيبرانية، اعترفت PPD-21 و EO13636 بدور وزارة الأمن الداخلي كمنسق رئيسي (house, 2013, pp. 02-03).

في إطار الشراكة بين القطاعين الحكومي والخاص، وجدت مكتب محاسبة الحكومة الأمريكية GOVERNMENT ACCOUNTING OFFICE (GAO)" أنه من سنة 2006 إلى 2012، زاد عدد الحوادث

السيبرانية المبلغ عنها ضد الأنظمة الداعمة للبنية التحتية الحيوية، والعمليات الفيدرالية بنسبة 782% (Office, 2013, p. 02)، لذلك ليس من المستغرب أن قانون PPD-20 الذي صدر قبل PPD21، يخول للحكومة الأمريكية استخدام "عمليات تأثير السيبرانية الدفاعية DEFENSIVE CYBER EFFECT OPERATIONS (DCEO)" نيابة عن الكيانات في القطاع الخاص، عندما يتطلب الأمر حماية ضد الأنشطة السيبرانية الخبيثة، على الرغم من أنها مملوكة أو خاضعة لسيطرة القطاع الخاص، فإن البنية التحتية الحيوية تعتبر محمية بموجب السيادة الإقليمية للولايات المتحدة.

أدى استمرار سرقة الملكية الفكرية والأسرار العسكرية الأمريكية من الصين إلى تنبؤات بتراجع الولايات المتحدة عسكريًا واقتصاديًا، وظهور الصين كقوة عالمية (Melnitzky, 2012, pp. 537-570). تتمثل الأهمية التي توليها الولايات المتحدة لحماية بنيتها التحتية الحيوية في قانون PPD-20 من خلال تبني سياسات "العمل الاستباقي ANTICIPATORY ACTION" و"التهديدات الوشيكة IMMINENT THREATS"، تقترح هاتان العبارتان بقوة أن تدمج سياسات الأمن السيبراني الأمريكية، الدفاع السيبراني النشط مع الخيارات الدبلوماسية والمعلوماتية والعسكرية والاقتصادية والمالية وإنفاذ القانون، يشير تحديد هذه الخيارات الإضافية إلى أن الرد السيبراني ليس متاحًا فقط كخيار مستقل، بل أيضًا بالتزامن مع خيارات أخرى، مما يدمج استراتيجية الدفاع السيبراني النشط ضمن مجموعة التدابير الدفاعية المتاحة للولايات المتحدة (Zeadally, 2014, pp. 296-297).

ركزت العديد من الجهود المبكرة للحكومة الأمريكية في الفضاء السيبراني على العناصر الإجرامية، في عام 2008 تم تشكيل "قوة المهام المشتركة للتحقيقات الوطنية السيبرانية NATIONAL CYBER INVESTIGATIVE JOINT TASK FORCE" كمركز متعدد الوكالات، يهدف إلى متابعة أولئك الذين ينتهكون قوانين الأمن السيبراني الأمريكية، يتيح عملهم لوزارة العدل تقديم لوائح اتهام ضد الأفراد المتهمين بانتهاك قوانين القرصنة أو التجسس، وفي وقت مبكر من عام 2010، اعترف مسؤولوا وزارة الدفاع بأن أنظمتهم كانت تتعرض لمحاولات استكشاف من قبل مستخدمين مجهولين، حوالي 250,000 مرة في الساعة، أي ما يعادل 6 ملايين مرة في اليوم (Derek S. Reveron, 2024, p. 164).

إستراتيجية الأمن السيبراني الوطنية لعام 2018 أكدت أن الأمن الاقتصادي مرتبط جوهريًا بالأمن القومي، لذا فإن التعاون الوثيق بين القطاعين العام والخاص هو حجر الزاوية في الاستراتيجية السيبرانية الأمريكية (House, 2018, p. 165). وفي نفس العام، أنشأ الكونغرس "وكالة الأمن السيبراني والبنية التحتية CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA)"، تحت إشراف "وزارة الأمن الداخلي DEPARTMENT OF HOMELAND SECURITY (DHS)"، نشأت CISA من صلب "مديرية الحماية والبرامج الوطنية NATIONAL PROTECTION AND PROGRAMS DIRECTORATE" في وزارة الأمن الداخلي، وتعمل اليوم بوظيفة تنسيقية هامة داخل الحكومة الوطنية وبين الحكومة والقطاع الخاص، يساعد القرب بين وزارة الأمن الداخلي (DHS) ووكالة الأمن القومي (NSA) على ترقية تطبيقات الفضاء الإلكتروني بين المستوى العسكري والمدني، لتعزيز التعاون بين القطاعين العام والخاص، ويوضح الجدول

الموالي ما قامت به الحكومة الأمريكية تدريجياً، بإنشاء هيئات سيبرانية جديدة تظهر على اليسار، والتي غالبًا ما تأثرت بالحوادث السيبرانية الموضحة على اليمين (Derek S. Reveron, 2024, p. 165).

جدول رقم (01) يوضح بعض الهيئات التي نشأت بموجب السياسة الأمريكية للأمن السيبراني والحوادث المرتبطة بها

تسمية الهيئات	الإنشاء	الحوادث المرتبطة
مكتب الفضاء السيبراني والسياسات الرقمية Bureau of Cyberspace and Digital Policy (DOS)	2022	الهجوم السيبراني على شركة "Colonial Pipeline" المتخصصة في نقل البنزين والديزل ووقود الطائرات
مديرية الأمن السيبراني National Cyber Director (NCD)	2021	
وكالة الأمن السيبراني وأمن البنية التحتية Cybersecurity and Infrastructure Security Agency Created	2018	هجوم SolarWinds Supply Chain المختصة في برامج إدارة ومراقبة تكنولوجيا المعلومات
القيادة السيبرانية الأمريكية العليا US Cyber Command Elevated	2017	التدخل الروسي في الانتخابات الرئاسية 2016
المعهد الوطني للمعايير والتقنية National Institute of Standards and Technology (NIST)	2014	هجومات كوريا الشمالية على شركة " SONEY PICTURES ENTERTAINMENT" إختراق الصين مكتب إدارة شؤون الموظفين Office of Personnel Management (OPM)
منسق الأمن السيبراني الدولي (وزارة الخارجية) International Cyber Coordinator (DOS)	2012	فيروس "Shamoon" or "W32.Shadow,"، إستهدف شركة "آرامكو Aramco" السعودية للنفط
القيادة السيبرانية الأمريكية (وزارة الدفاع) US Cyber Command (DOD)	2010	حادثة "فيروس Stuxnet" برنامج حاسوبي مصمم خصيصًا لاستهداف أنظمة التحكم الصناعية
نائب وكيل وزارة الأمن الداخلي للأمن السيبراني Deputy Undersecretary for Cyber (DHS)		

المصدر: من إعداد الباحثتان بالإعتماد على (Derek S. Reveron, 2024, p. 165)

تعتمد الهيئات الموضحة في الجدول على العديد من المؤسسات الخاصة المتخصصة في صناعة التكنولوجيات والبرامج عن طريق البحث والتطوير، كالدور الذي تتولاه "**وكالة مشاريع البحوث المتطورة الدفاعية Defense Advanced Research Projects Agency (DARPA)**"، قادت (DARPA) العديد من المبادرات في مجال الأمن السيبراني لإنشاء أنظمة مستقلة قادرة على اكتشاف وتصحيح الثغرات البرمجية في الوقت الفعلي دونما أي تدخل بشري، إضافة إلى بحوثها في مجال ربط الأمن السيبراني بالذكاء الإصطناعي الذي عرفته السنوات الأخيرة.

بدأت القيادة السيبرانية الأمريكية في عام 2019 بالإعلان عن أنها ستتبع استراتيجية "الانخراط المستمر PERSISTENT ENGAGEMENT"، كتحول كبير في التفكير ضمن حلول جديدة للأمن السيبراني،

لأن "الانخراط المستمر" ومفهومه الشقيق "الدفاع للأمام DEFENDING FORWARD" يعنيان أن القيادة السيبرانية ستسعى لإقامة وجود خارجي بدعوة من الحكومات الصديقة، للمساعدة في التصدي للهجمات قبل أن تصل إلى السواحل الأمريكية (Derek S. Reveron, 2024, p. 166).

ووفقاً لرئيس القيادة السيبرانية الأمريكية الجنرال "بول ناكاسوني PAUL M. NAKASONE" سنة 2019، ستتنازع القوى في الفضاء السيبراني لإلحاق الضرر بالمصالح الأمريكية، قوى متأتية من ممارسات الصين وروسيا وإيران وكوريا الشمالية...التي توظف حاليا ميليشيات سيبرانية للإضرار بالمصالح الأمريكية، ستقوض هذه الهجمات البنية التحتية والموارد الأخرى، ولا يمكن الانتظار حتى تؤثر الهجمات السيبرانية على "الشبكات العسكرية MILITARY NETWORKS"، الدفاع عن الشبكات العسكرية يتطلب تنفيذ عمليات خارجها، لذلك وجب على العقيدة الأمريكية السيبرانية بناء خطة سيبرانية تقوم على المراقبة الاستباقية والمتابعة ومواجهة عمليات الخصم، وفرض تكاليف في المنافسة اليومية لتعطيل وهزيمة الحملات السيبرانية الخبيثة الجارية، وردع الحملات المستقبلية وتعزيز المعايير الدولية السلوكية المواتية باستخدام جميع أدوات القوة القومية (Nakasone, 2019, pp. 02-03)

3. الإندماج الأمريكي في النسق الدولي للأمن السيبراني والأمن القومي

على المستوى الدولي ولأن البيئة السيبرانية تنقسم هي الأخرى إلى بيئة داخلية وخارجية، تشترط أن يكون الاهتمام بهما في نفس المستوى، إنخرطت الولايات المتحدة في النسق الدولي للأمن السيبراني والأمن القومي، من منطلق فرضية أن أمن البيئة السيبرانية الخارجية من أمن البيئة الداخلية.

1.3 نداء باريس للثقة والأمن في الفضاء السيبراني

The Paris Call For Trust And Security in Cyberspace (2018):

تم إطلاق نداء باريس في 12 نوفمبر 2018 خلال منتدى باريس للسلام، ويهدف إلى تعزيز المبادرات المتعلقة بالقضايا الناشئة، التي لم يتم تنظيمها بشكل كافٍ بعد، من خلال العمل مع مجموعة متنوعة من الجهات الفاعلة، بما في ذلك الدول والشركات والجمعيات المهنية ومنظمات المجتمع المدني، يقترح النداء رؤية لتنظيم الفضاء السيبراني والمبادئ الرئيسية المرتبطة به، لا سيما منع فشل الأمن والامتناع عن استخدام بعض الممارسات التي قد تضر باستقرار الفضاء السيبراني (Affairs، 2018).

2.3 المنتدى العالمي لبناء القدرات في الفضاء السيبراني The Global Forum on Cyber Expertise:

يعزز المنتدى (GFCE) الذي تأسس سنة 2015، التعاون الدولي في بناء القدرات السيبرانية من خلال ربط الاحتياجات والموارد والخبرات، ومن خلال إتاحة المعرفة العملية. يركز المنتدى حاليًا على ثلاثة مجالات تضم تنسيق المشاريع والمبادرات الإقليمية والعالمية لبناء القدرات السيبرانية، تبادل المعرفة والخبرات، وتلبية الاحتياجات الفردية لبناء القدرات السيبرانية، ومن خلال عروض الدعم، يحسن المنتدى الكفاءة على المستوى العالمي في تقديم برامج بناء القدرات، وتم إضافة تركيز جديد في النصف الثاني من عام 2020، وهو جمع وتحديد أولويات الفجوات البحثية (كما حددتها مجموعات العمل التابعة للمنتدى)، لتضمينها في جدول أبحاث بناء القدرات السيبرانية العالمية (Expertise, 2015) .

3.3 الإتفاقيات مع حلف الشمال الأطلسي (NATO):

اعترف الناتو بالفضاء السيبراني كأحد مجالات العمليات في عام 2016 إلى جانب المجالات التقليدية الأخرى كالجو والبر والبحر، يتيح هذا الاعتراف لقادة الناتو العسكريين حماية المهام والعمليات بشكل أفضل من التهديدات السيبرانية، بما في ذلك الاعتماد على القدرات السيبرانية الوطنية للحلفاء، يحتفظ الحلفاء بالملكية الكاملة لهذه القدرات، تمامًا كما يمتلك الحلفاء الدبابات والسفن والطائرات، وكما هو الحال في جميع المجالات الأخرى، فإن إجراءات الناتو في الفضاء السيبراني تكون دفاعية ومتناسبة ووفقًا للقانون الدولي، يتفق الحلفاء على أن الجميع سيستفيدون من فضاء سيبراني يستند إلى القواعد ويكون قابلًا للتنبؤ به، مفتوحًا، حراً وآمنًا. (NATO, 2016).

4.3 الحوار السيبراني الأمريكي الأوروبي THE U.S.-EU CYBER DIALOGUE:

شمل الحوار السيبراني الأمريكي الأوروبي التاسع سنة 2023 تبادلات حول الدفاع السيبراني، وحدد المزيد من الإجراءات لتعزيز التعاون والتصدي للأنشطة الإلكترونية الخبيثة، تسعى الولايات المتحدة والاتحاد الأوروبي إلى تعاون إقليمي أوسع مع الدول في أمريكا اللاتينية ومنطقة المحيطين الهندي والهادئ وإفريقيا، لتعزيز سلوك الدول المسؤول من خلال العمل الدبلوماسي والمشاركة، ولتعزيز الأمن السيبراني والمرونة لمواجهة هذه التحديات، تبادلت الولايات المتحدة والاتحاد الأوروبي، التحديثات بشأن عدة أولويات رئيسية تم تحديدها في البيان المشترك الصادر في يناير 2023، من وزير الأمن الداخلي "أليخاندرو مايوركاس ALEJANDRO MAYORKAS" والمفوض الأوروبي للسوق الداخلية "تييري بريتون THIERRY BRETON"، شملت هذه الأولويات أمن المنتجات الرقمية والمعايير السيبرانية ذات الصلة، مرونة البنية التحتية الحيوية وتأثير فرص التقنيات الناشئة، والتعاون بين الوكالات السيبرانية (states, 2023).

قررت الولايات المتحدة والاتحاد الأوروبي أيضًا تعميق تعاونهما بشكل أكبر لمواجهة تحديات الأمن السيبراني المتعلقة بالتقنيات الناشئة، مع التركيز بشكل خاص على "الذكاء الاصطناعي INTELLIGENCE ARTIFICIAL" و"التشفير CRYPTOGRAPHY"، ويهدف التعاون بين الولايات المتحدة والاتحاد الأوروبي إلى تعزيز الاستخدام الآمن للذكاء الاصطناعي في البنية التحتية الحيوية، كما ناقش المشاركون في الحوار الإلكتروني الأنشطة المشتركة المحتملة في الانتقال نحو التشفير (states, 2023).

5.3 التعاون السيبراني الأمريكي الياباني THE U.S.-JAPAN CYBERSECURITY COOPERATION:

عُقد الحوار الإلكتروني التاسع بين اليابان والولايات المتحدة في واشنطن العاصمة في 26 يونيو 2024، وبناءً على ضرورة مواصلة الجهود الحكومية الشاملة من قبل كل من "اليابان" و"الولايات المتحدة"، ناقش المشاركون مجموعة واسعة من القضايا المتعلقة بالتعاون الياباني الأمريكي في مجال الأمن السيبراني، بما في ذلك السياسات السيبرانية المحلية، والتعاون السيبراني الثنائي في العمليات، والتعاون الدولي والإقليمي وبناء القدرات.

قاد السيد "ناوكي كوماتاجاي KUMAGAI Naoki"، السفير الياباني المكلف بسياسات الأمن السيبراني، ونائب المدير العام لمكتب السياسات الخارجية، وفدًا مشتركًا يمثل الوزارات والوكالات المعنية،

مثل وزارة الخارجية و"المركز الوطني للاستعداد للحوادث والاستراتيجية للأمن السيبراني NATIONAL CENTER OF INCIDENT READINESS AND STRATEGY FOR CYBERSECURITY، و"وكالة الاستخبارات الأمنية العامة PUBLIC SECURITY INTELLIGENCE AGENCY"...ووزارة الدفاع. أما من الجانب الأمريكي قادت السيدة "ليسيل فرانز LIESYL FRANZ"، نائبة مساعد وزير الخارجية في مكتب الفضاء الإلكتروني والسياسات الرقمية بوزارة الخارجية، الوفد الأمريكي المشترك (japan, 2024) .

6.3 الإتفاقية السيبرانية الأمريكية الأسترالية The U.S.-Australia Cyber Agreement:

في إطار جهود وزارة الدفاع الأمريكية وتعزيز الشراكات في الفضاء الإلكتروني، أطلقت الولايات المتحدة وأستراليا أول اتفاقية من نوعها لتطوير مجال تدريب افتراضي مشترك على الفضاء الإلكتروني، وقعت الدولتان مؤخرًا ترتيب مشروع القدرات التدريبية السيبرانية في 3 نوفمبر 2020، وهي اتفاقية دولية ثنائية تمكن قيادة الفضاء الإلكتروني الأمريكية (USCYBERCOM) من دمج ملاحظات قوات الدفاع الأسترالية، ضمن ما يسمى بـ "بيئة التدريب السيبراني المستمرة THE PERSISTENT CYBER TRAINING ENVIRONMENT (PCTE)"، التي هي منصة تدريب على المهام الدفاعية الواقعية عبر حدود الشبكات، واستخدامها وتطويرها المشترك سيجعلها تتطور باستمرار ويعزز الجاهزية في الإجراءات السيبرانية، وفق ما أشارت "إليزابيث ويلسون Elizabeth Wilson"، نائبة مساعد وزير الجيش لصادرات الدفاع والتعاون، فبيئة التدريب السيبراني المستمرة (PCTE) هي جزء من إطار العمل الشامل للحرب السيبرانية المشتركة، وهو إطار شامل يساعد في تطوير القدرات عبر الخدمات لنظام وظيفي قابل للتكيف (defence, 2020).

4. إمكانية تطبيق سياسات الأمن السيبراني الأمريكية على الحالة الجزائرية

بعد عرض مختلف الجوانب الأساسية في سياسات الأمن السيبراني الأمريكية وأثرها على الأمن القومي، نأتي إلى الحالة الجزائرية لنرى إن كانت تتمتع بالبيئة المناسبة والمتطلبات الضرورية لبناء سياسات سيبرانية، تتماشى والتهديدات المستجدة في البيئة السيبرانية للجزائر.

1.4 حالات التهديدات السيبرانية التي عرفتها الجزائر:

مؤخراً شهدت الجزائر تناميا ملحوظا في الهجمات السيبرانية، خاصة بعد سياسات التحول الرقمي التي أُعلن عنها منذ مشروع الجزائر الإلكترونية "E-Algeria 2013"، ما دفعها إلى التفكير في سن سياسات سيبرانية حديثة، إضافة إلى تأسيس نظام مؤسساتي ذو طابع أمني تابع لوزارة الدفاع الوطني، وقد تعددت حالات الهجمات هذه لتستهدف قطاعات عدة:

- في فيفري 2023 صرحت وكالة الأنباء الجزائرية عن أن موقعها تعرض إلى هجوم سيبراني (زهار، 2023).
- في مارس 2022، أعلنت وزارة العدل عن أن حسابها على تويتر أيضا تعرض للقرصنة (الأنباء، 2022).
- بتاريخ ماي 2023 تم تسجيل حوالي 30 مليون تهديد سيبراني على الجزائر (micro, 2022).
- تقرير من منظمة الشرطة الجنائية الدولية"INTERPOL" والشرطة الإفريقية "AFRIPOL" صدر في مارس 2023، يفيد بأن الجزائر والدول الإفريقية عامة أصبحت تشهد تناميا لموجات من الهجمات السيبرانية، تستهدف قواعد بيانات القطاعات الحيوية فيها (INTERPOL, 2023).

-تقرير صادر عن منظمة الأمم المتحدة، بعنوان: "E-GOVERNMENT SURVEY" سنة 2022، يفيد أن الجزائر تحتل المرتبة 112 عالميا في مجال تطور الحكومة الإلكترونية (Affairs D. o., 2022, p. 213).

- قضية التجسس التي قادها "المغرب" ضد "الجزائر" سنة 2021 بإستخدام برنامج "بيغاسوس PEGASUS"، الشيء نفسه الذي تكرر مع عدة دول أوروبية كانت إسبانيا أكثرها تضررا.

كل هذه الهجمات في البيئة السيبرانية للجزائر، تجعلها تتشابه مع نفس الحالة الأمريكية -وإن كانت أكثر وزنا من الحالة الجزائرية- وهذا ما دفع المشرع الجزائري إلى تبني سياسات ضمن أطر قانونية ومؤسساتية في مجال الأمن السيبراني بإشراف وزارة الدفاع.

من بين السياسات التي تبنتها الجزائر في مجال الأمن السيبراني نجد سياسات قانونية وأخرى مؤسساتية تنتظم في الجدول الموالي.

جدول رقم (02) يوضح أهم سياسات الأمن السيبراني القانونية والمؤسساتية في الجزائر

السياسات القانونية	السياسات المؤسساتية
قانون العقوبات رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-156 في المادة 394 مكرر 7 المعنون بـ: "المساس بأنظمة المعالجة الآلية للمعطيات"	مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني تم إنشاؤه سنة 2008
القانون رقم 09-04 الصادر في 5 أوت 2009 في المادة 04 من الفصل الثاني المعنون بـ "مراقبة الاتصالات الالكترونية"	المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني أنشأ سنة 2004
القانون رقم 18-05 المؤرخ في 10 ماي 2018 والذي وضع الضوابط العامة المتعلقة بالتجارة الالكترونية والتي تحدد واجبات ومسؤوليات وحقوق المورد والمستهلك الالكتروني وكذا طريقة الدفع الالكتروني	المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني تم إنشاؤها سنة 2011
القانون رقم 15-04 المؤرخ في 1 فيفري سنة 2015 والمتعلق بالتوقيع والتصديق الالكترونيين حيث يحدد كيفية إجراء هذه العملية وشروط تأمينها وكذا السلطة المسؤولة	الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها أنشئت سنة 2009
القانون رقم 18-04 المؤرخ في 10 ماي 2018 والذي نص في مادته 10 على الأمن السيبراني من خلال تجنيد كل الأدوات والسياسات والآليات الأمنية لضمان سرية البيانات المخزنة أو المعالجة أو المرسلة	المنظومة الوطنية لأمن الأنظمة المعلوماتية ووكالة أمن الأنظمة المعلوماتية أنشأت سنة 2020

المصدر: من إعداد الباحثتان بالإعتماد على مجموعة من الأطر القانونية

يظهر مدى تأثر سياسات الأمن السيبراني بالتجربة الأمريكية في مجال تنظيمه، إذ يظهر إنتظام السياسة السيبرانية في الجزائر عبر مستويين قانوني ومؤسساتي، مثل ما هو عليه الحال في السياسة السيبرانية الأمريكية، غير أن التجربة الأمريكية في الحقيقة ترتكز على عنصر مهم وهو دعم المؤسسات

الناشئة في مجال تكنولوجيات الإتصال والتقنيات، إضافة إلى دعم نشاطات البحث وإستقطاب الأدمغة المختصة، الشيء الذي يندر الإعتماد عليه في الجزائر.

في ظل سياسة التحول الرقمي التي بادرت بها مختلف القطاعات الحيوية في الجزائر، لابد من طرح سؤال يخص مدى أمن الأنظمة المعلوماتية، خاصة وأن الجزائر تتميز بضعف الإستثمار في الحلول التكنولوجية، الأمر الذي لا يترك مجالا للشك، بزيادة إحتمالية تعرض قواعد معلومات الدولة إلى هجومات سيبرانية للتخريب أو الجوسسة، ومع مواقف الجزائر في المنظومة الدولية التي يظهر في نظر معظم فواعلها أنها تسير بعكس مسار هذه المنظومة، فإحتمالية تعرض الجزائر لهجمات سيبرانية تستهدف قطاعات الدفاع والأمن غير مستبعدة، لذلك فتوجه الجزائر في السياسة السيبرانية يجب أن يكون بالإعتماد على القدرات المحلية وليس الأجنبية، مثل ما إعتمدت عليه السياسة الصينية كذلك في مجال الأمن السيبراني، عن طريق إنشاء مؤسسات ناشئة مختصة.

تنقص التجربة الجزائرية -عكس ما هو متوفر في التجربة الأمريكية كذلك- ضعف إنخراط الأولى في المبادرات الدولية للأمن السيبراني، فحضور الجزائر ضمن هذا النسق قد يعزز من خبراتها، التنسيق مع الدول الحليفة في المنطقة، يعطي للجزائر هامش للتنبؤ بالهجمات قبل حدوثها ويعزز من حضورها، ويمكن في هذا الصدد التركيز على مبادرات المؤتمرات الدولية التي تنعقد سنويا، والتي نذكر منها مؤتمرات الأمن السيبراني الروسية، كـ "أيام الاختراق الإيجابي POSITIVE HACK DAYS – PHD"، "روسكريبتو (RUSCRYPTO)، "إنفوسيكيوريتي روسيا INFOSECURITY RUSSIA"، إضافة إلى مؤتمرات الأمن السيبراني الصينية كـ "أسبوع الأمن السيبراني في الصين CHINA CYBERSECURITY WEEK"، "قمة الأمن السيبراني CYBER SECURITY SUMMIT (CHINA)"، و"مؤتمر أمن الإنترنت في الصين CHINA INTERNET SECURITY CONFERENCE (ISC)".

خاتمة:

حاولنا من خلال هذه الدراسة تسليط النظر على سياسات الأمن السيبراني الأمريكية وأثرها على الأمن القومي، حيث تمثلت إشكاليتنا: " **بناء على تجربة الولايات المتحدة الأمريكية، كيف أثرت سياسات الأمن السيبر اني الأمريكية على أمنها القومي في ظل التهديدات الإقليمية والدولية؟**.

توصلت الدراسة إلى جملة من النتائج:

1. قامت السياسات السيبرانية الأمريكية على مجموعة من الأطر القانونية المنظمة لعمل المؤسسات المشرفة على التنفيذ، كالبيت الأبيض ووكالة الأمن الداخلي ووكالة الأمن القومي ووزارة الدفاع ووكالة الأمن السيبراني والبنية التحتية ، إضافة إلى مديرية الحماية والبرامج الوطنية وغيرها...فحقيقة وجود هذه الأطر يسهل من عمليات الإشراف والتنفيذ وتنسيق السياسات.

2. تقوم سياسات الأمن السيبراني الأمريكية على دعم جهود البحث والتطوير الذي تشرف عليه مختلف الوكالات الحكومية أو الخاصة، كـ"وكالة مشاريع البحوث المتطورة الدفاعية (DARPA)، ومنه تعتمد السياسة الأمريكية في مجال الأمن السيبراني على الصناعات التقنية المحلية.

3. تنخرط الولايات المتحدة مع مختلف حلفائها تحت إشراف وزارة الخارجية الأمريكية ووزارة الدفاع، ضمن النسق الدولي للأمن السيبراني، الذي يسمح بتنسيق جهود التصدي للهجمات السيبرانية، إضافة إلى جهود البحث والتطوير، ناهيك عن تنسيق ضربات سيبرانية إستباقية في حال التنبؤ بوجود تهديد من أي كيانات رسمية أو غير رسمية، تنشط لزعزعة الأمن القومي الأمريكي في شقه السيبراني.

4. تحتل الولايات المتحدة المرتبة الأولى عالميا في مجال الأمن السيبراني، بناء على "مؤشر الأمن السيبراني العالمي GLOBAL CYBERSECURITY INDEX" لسنة 2024 (Cywreck, 2024).

5. تتشابه الحالة الأمريكية مع الحالة الجزائرية فيما يتعلق بالأمن السيبراني، بحكم ما تعرضت إليه الجزائر مؤخرا من هجمات إستهدفت بعض مواقعها الرسمية، فنفس الهجمات التي أصابت الولايات المتحدة الأمريكية في بداية تجربتها، ودفعتها إلى تبني سياسات الأمن السيبراني كمقاربة لحماية الأمن القومي، تتعرض لها الجزائر اليوم، ومع التحول الرقمي الذي يشهده قطاع الدفاع والخدمات، أصبح البحث عن سبل لحماية الأمن السيبراني أكثر من ضرورة في الجزائر.

ومنه فإن الفرضيات المطروحة في هذه الدراسة والتي تعتبر حلولا مؤقتة للإشكالية المطروحة، هي فرضيات صحيحة بحكم ما توصلنا إليه من نتائج.

بناء على هذه النتائج نقدم جملة من الإقتراحات لتطوير سياسات الأمن السيبراني في الجزائر بناء على الحالة الأمريكية:

1. إنشاء وزارة مختصة في الأمن السيبراني تشرف على جهود تطوير السياسات من هذا النوع وتمويلها وتنفيذها، إضافة إلى لجنة مختصة في الأمن السيبراني كذلك على مستوى البرلمان بغرفتيه.

2. دعم جهود الصناعات التقنية المحلية في مجال تكنولوجيات الإتصال، مع التخلي التدريجي عن إستيراد مثل هذه التقنيات، لأن التجارب أثبتت أن الدول التي تعتمد على إستيراد الحلول التكنولوجية، تبقى تحت رحمة الدول المصدرة لها، فالأنسب هو دعم الصناعات المحلية عن طريق تشجيع جهود البحث في مراكز ومخابر البحث المختصة.

3. تشجيع الإستثمار في الحلول التكنولوجية وتسويقها محليا بإنشاء مؤسسات ناشئة "STARTUP" متخصصة في الحلول التقنية، كالأقمار الصناعية والبرامج والتطبيقات والموصلات وأشباه الموصلات.

4. الإنخراط في المبادرات الدولية للأمن السيبراني وتنسيق الجهود مع حلفاء الجزائر كروسيا والصين، بغية الإستفادة من خبراتهم، خاصة وأنها تحتل المراتب الأولى بعد الولايات المتحدة في مجال الأمن السيبراني، بناء على "مؤشر الأمن السيبراني العالمي GLOBAL CYBERSECURITY INDEX" لسنة 2024.

5. إنشاء عبر كل النواحي العسكرية الست لجان دفاعية مختصة في الأمن السيبراني وأمن الأنظمة المعلوماتية، خصوصا من ناحية الدول التي تعرف حالة عدم إستقرار أمني.

6. التوسيع في إنشاء مدارس عليا للذكاء الإصطناعي وفتح تخصصات في مجال الصناعات الإلكترونية عبر مختلف جامعات الوطن.

قائمة المراجع:

أولا: المراجع باللغة العربية:

1. الكتب:

1.1 محمد محمود الذنيبات عمار بوحوش. (2007). **مناهج البحث العلمي وطرق إعداد البحوث** (الإصدار 04). الجزائر، العاصمة، الجزائر: الديوان الوطني للمطبوعات الجامعية.

2.1 محمد شلبي. (1997). **المنهجية في التحليل السياسي-المفاهيم، المناهج، الإقترابات، الأدوات** (الإصدار 01). العاصمة، الجزائر: الديوان الوطني للمطبوعات الجامعية.

2. المقالات:

1.2 عتيقة,ك ,2023 .جويلية .**تداعيات الإرهاب السيبراني على الأمن القومي الجزائري** .المجلة الجزائرية للأمن والتنمية ,المجلد 12 ، العدد 03.

2.2 فرج عصام بن جليل, ي. و ,2021 .أوت .**أثر التحديات الداخلية والخارجية على الأمن القومي العربي: الواقع و آفاق المستقبل** .مجلة علوم الإنسان والمجتمع ,المجلد 10 ، العدد 03.

3.2 كلاع, ش ,2022) .مارس .**الأمن السيبراني وتحديات الجوسسة والإختراقات الإلكترونية للدول عبر الفضاء السيبراني** .مجلة الحقوق والعلوم الإنسانية ,المجلد 15 ، العدد 01 .

4.2 مسيكة محمد. (12 ,2022). **الفضاء السيبراني وتحديات الأمن القومي للدول**. مجلة العلوم القانونية والإجتماعية، المجلد 07، العدد 04.

3. المواقع الإلكترونية:

1.3 حسان حويشة. (2023). **إحباط قرابة 30 مليون تهديد سيبراني ضد الجزائر**. موقع الشروق نيوز. تم الاسترداد من https://n9.cl/zanlxn

2.3 حسان زهار. (2023). **الحرب السيبرانية تتصاعد ضد الجزائر**. الإخبارية. تم الاسترداد من https://n9.cl/e8qtgh/

3.3 موقع وكالة الأنباء. (2022). **فتح تحقيق في واقعة اختراق حساب "تويتر" لوزارة العدل**. وكالة الأنباء الجزائرية. تم الاسترداد من: https://www.aps.dz/ar/algerie/122757

ثانيا: المراجع باللغات الأجنبية

I. BOOKS:

1. Buchanan, B. (2020). **THE HACKER AND THE STATE Cyber Attacks and the New Normal of Geopolitics** (1 ed.). Massachusetts, united states of america: harvard university press.

2. Carlin, J. P. (2018). ***Dawn of the Code War: America's Battle against Russia, China, and the Rising Global Cyber Threat*** *(1 ed.). new york, united states of america: PublicAffairs.*

3. Derek S. Reveron, J. (2024). ***Security in the cyber space: An Introduction to Policy and technology*** *(01 ed.). cambridge, united kingdom: cambridge university press.*

4. Kuan-Ching Li , X. W. (2019). ***Advances in Cyber Security: Principles, Techniques, and Applications*** *(01 ed.). Singapore: Springer Nature Singapore Pte Ltd.*

5. MEEUWISSE, R. (2015). ***Cybersecurity for Beginners*** *(01 ed.). North Carolina, United states of america: Lulu Publishing Services rev.*

6. Others, J. L. (2012). ***Cyber Security Policy guidebook*** *(01 ed.). New Jersey, united states of america: Published by John Wiley & Sons, Inc.*

7. STEVEN, M. (2019). ***CYBER SECURITY Ultimate Beginners Guide to Learn the Basics and Effective Methods of Cyber Security (An Essential Guide to Ethical Hacking for Beginners****). Maryland , united states of america: Independently Published.*

8. Walker, b. (2019). ***Cyber Security: Comprehensive Beginners Guide to Learn the Basics and Effective Methods of Cyber Security****. australia: Independently Published.*

II. ARTICLES:

1. *Melnitzky, A. (2012, Cardozo Journal of International & Comparative Law).* ***Defending America against Chinese cyber espionage through the use of active defenses****. Cardozo Journal of International & Comparative Law, 20(02).*

2. *Zeadally, A. F. (2014, january).* ***US Policy on Active Cyber Defense****. Journal of Homeland Security and Emergency Management, 11(02).*

III. WEBSITES:

1. Affairs, D. o. (2022). ***E-GOVERNMENT SURVEY****. NEW YORK: UNITED NATIONS. Retrieved 08 25, 2024, from https://n9.cl/2wnfn*

2. Affairs, M. f. (2018). ***Paris Call for Trust and Security in Cyberspace****. Retrieved 08 24, 2018, from https://n9.cl/pcaj6*

3. Cywreck, B. (2024, 03 04). ***Top 10 Cybersecurity Powerhouses: Ranking the Global Defenders in 2024****. Retrieved 08 28, 2024, from https://n9.cl/7posi*

4. Defence, u. M. (2020). ***US and Australia sign first-ever cyber agreement to develop virtual training range****. U.S. Cyber Command. Retrieved from https://n9.cl/mdmbmk*

5. Department, h. s. (2011, november). ***Blueprint for a Secure Cyber Future; cyber security strategy for the homeland security entreprise****. Retrieved from https://n9.cl/7ne9x*

6. Drummond, D. (2010, 01 12). ***A New Approach to China****. Retrieved from Google Official Blog: https://googleblog.blogspot.com/2010/01/new-approach-to-china.html*

7. Expertise, T. G. (2015). ***GFCE****. Retrieved 08 24, 2024, from https://thegfce.org/about-gfce/*

8. Graff, G. (2018, 10 11). ***How the US Forced China to Quit Stealing—Using a spy****. Retrieved from wired: https://n9.cl/8cktj*

9. house, w. (2013, february 12). ***Presidential Policy Directive/PPD-21****, Subject: Critical Infrastructure Security and Resilience. Retrieved from national securiy archive: file:///C:/Users/User/Desktop/Document-86.pdf*

*10. House, W. (2018). **National Cyber Strategy. whashington dc: seal of the president of the united states**. Retrieved from file:///C:/Users/User/Desktop/National-Cyber-Strategy%202018.pdf*

*11. INTERPOL. (2023). **AFRICAN CYBERTHREAT ASSESSMENT REPORT CYBERTHREAT TRENDS**. france: The African Cybercrime Operations Desk. Retrieved from file:///C:/Users/User/Desktop/2023_03%20CYBER_African%20Cyberthreat%20Assessment%20Report%202022_EN.pdf*

*12. Japan, M. o. (2024). **The 9th Japan-US Cyber Dialogue**. Retrieved from https://n9.cl/bzo2y*

*13. justice, u. d. (2010, may). **office of justice programme**. Retrieved from https://n9.cl/0ljdh*

*14. Justice, u. d. (2016, july 13). **office of public affaire**. Retrieved from department of justice: file:///C:/Users/User/Desktop/sentencing_response_to_su_bin.pdf*

*15. Lilli, E. (2020, jun 11). **President Obama and US cyber security policy**. journal of cyber policy, 01.doi: file:///C:/Users/User/Desktop/23738871.2020.1778759.pdf*

16. Micro, T. (2022). Trend Micro Blocked over 29.7 Million Threats in Algeria: Reveals Annual Cybersecurity Report. Retrieved 08 25, 2024, from https://n9.cl/hmou3

*17. Nakasone, P. M. (2019). **Statement Of General Paul M. Nakasone**, Commander, United States Cyber Command Before The Senate Committee On Armed Services. February 14, 2019. Unclassified. National Security Achieve. Retrieved from file:///C:/Users/User/Desktop/Nakasone_02-14-19.pdf*

*18. NATO. (2016). NATO Cyber Defence. Belgium: **Public Diplomacy Division (PDD)** – Press & Media Section. Retrieved from file:///C:/Users/User/Desktop/NATO%20cyber%20defence.pdf*

*19. States, u. d. (2023). **joint Statement on the United States-European Union 9th Cyber Dialogue in Brussels**. Brussels: Office of the Spokesperson. Retrieved from: https://n9.cl/ppy73*