المجلد الثالث
العدد السادس
سبتمبر 2025

مجلة جامعة درنة للعلوم الإنسانية والاجتماعية
DERNA UNIVERSITY JOURNAL OF HUMANITIES AND SOCIAL SCIENCES
Available online at https://dujhss.uod.edu.ly/
P-ISSN: 2959-6475 E-ISSN: 2959-6483 Impact Factor: 0.82

أثر التهديدات السيبرانية على الأمن القومي في ليبيا

أ.الوليد عبد المجيد عصمان
محاضر مساعد، العلوم السياسية، كلية الاقتصاد والعلوم السياسية، جامعة الزيتونة، ليبيا.
Alwaos308@gmail.com

https://www.doi.org/10.58987/dujhss.v3i6.18

تاريخ الاستلام: 2025/05/28 ؛ **تاريخ القبول:** 2025/07/31 ؛ **تاريخ النشر:** 2025/09/01

المستخلص

أصبح الأمن السيبراني سلاحاً استراتيجي بيد الدول والأفراد، ومع تزايد التهديدات والهجمات السيبرانية على مختلف المؤسسات داخل الدولة الواحدة، سعت هذه الدول وبكل جدية لوضع خطط واستراتيجيات للتصدي لمثل هذه التهديدات، وبما أنَّ ليبيا من ضمن أعضاء المجتمع الدولي، والتي تعرضت مؤسساتها المختلفة للعديد من الهجمات السيبرانية، سعت هده الدراسة إلي توضيح الأمن السيبراني وأهميته، وذلك من خلال تعريفه وتوضيح أهدافه وابعاده، والتطرق إلي التهديدات السيبرانية التي تعرضت لها الدولة الليبية في مختلف مؤسساتها والتي أثرت سلباً عليها، كالهجمات السيبرانية التي تعرض لها مصرف ليبيا المركزي، والمؤسسة الوطنية للنفط، كما رمت الدراسة إلي التعرف على أهم الخطط والآليات التي إتخادتها الدولة الليبية للتصدي لمثل هده التهديدات، ومن بين هده الخطط التي قامت بها الدولة الليبية، وضع القوانين المتعلقة بالأمن السيبرني، وإنشاء المراكز والهيئات المختصة بشأن السيبراني ، فضلاً على نشر ثقافة الوعي بين الموطنين على أهمية هذا الموضوع، وأعتمد الباحث في هده الدراسة على المنهج الوصفي التحليلي لجمع المعلومات والبيانات وتحليلها وتفسيرها وصولاً إلى تعميمات حول الموضوع، وخلصت الدراسة إلى أن الأمن السيبراني أصبح من أهم أولويات الدولة الليبية، نظرا لدوره المحوري في الواقع المعاصر. كما أكدت على أن للهجمات السيبرانية تأثيرا سلبيا مباشرا على مؤسسات الدولة في ليبيا، مما تسبب في خسائر مادية فادحة انعكست بدورها على الأمن القومي للبلاد واستقراره، وعليه فإن هذه النتائج تؤكد الحاجة الملحة إلى استمرار الجهود المبذولة في تعزيز الأمن السيبراني في ليبيا، لضمان حماية مؤسساتها وبنيتها التحتية الحيوية من التهديدات المتزايدة .

الكلمات الافتتاحية: التهديدات السيبرانية ، الأمن السيبراني ، الأمن القومي.

Abstract:

Cyber security has become a strategic weapon in the hands of states and individuals, and with the increasing threats and cyber-attacks on various institutions within the same country, these countries have sought and seriously to develop plans and strategies to address such threats, and since Libya is among the members of the international community, whose various institutions were subjected to many cyber-attacks, this study sought to clarify cybersecurity and its importance, through its definition and clarification Its goals and its elaboration, and touched on the cyber threats that the Libyan state was exposed to in its various institutions, which affected it negatively, such as the cyber-attacks that the Central Bank of Libya and the National Oil Corporation, and the study also threw to identify the most important plans and mechanisms that the Libyan state had to address such threats, and among these plans made by the Libyan state, setting laws related to security security Centers and specialized bodies regarding cyberspace, as well as spreading a culture of awareness among citizens on the importance of this

المجلد الثالث
العدد السادس
سبتمبر 2025

مجلة جامعة درنة للعلوم الإنسانية والاجتماعية
DERNA UNIVERSITY JOURNAL OF HUMANITIES AND SOCIAL SCIENCES
Available online at https://dujhss.uod.edu.ly/
P-ISSN: 2959-6475 E-ISSN: 2959-6483 Impact Factor: 0.82

topic, and the researcher in this study relied on the descriptive, analytical approach to collecting information and data, analyzing and interpreting it to generalizations on the subject, and the study concluded that cybersecurity has become one of the most important priorities of the Libyan state, given its pivotal role in the contemporary reality. She also stressed that cyber attacks have a direct negative impact on state institutions in Libya, which caused fatal material losses that in turn reflected on the country's national security and stability, and therefore these results confirm the urgent need for the continued efforts to enhance cybersecurity in Libya, to ensure the protection of its institutions and vital in Fra structure from the increasing threats .

Keywords: Cyber Threats, Cybersecurity, National Security.

(1_1): المقدمة:

يشهد العالم في السنوات والعقود الأخيرة تطورا سريعا وهائلاً في مختلف تكنولوجيا الإعلام والاتصال بجميع أشكالها ومجالاتها، مما جعل الأفراد داخل المجتمع الواحد لا يمكن أن يعيشوا من دون هذه التكنولوجيا أو يستغنوا عن خدماتها، وذلك نتيجة لفهمها السريع والاستخدام السهل لها. ومن ناحية أخرى أصبحت هذه التكنولوجيا، وخاصة في وقتنا الراهن، تشكل خطرا جسيما على أمن الأفراد والمجتمعات والأمن القومي للدول، نتيجة الاستخدام غير الأمثل والفهم الخاطئ لتكنولوجيا الإعلام والاتصال، وهو ما يشهده العالم في الآونة الأخيرة جراء التصاعد المستمر لمختلف التهديدات السيبرانية في مختلف المجالات، ما جعل الدول والحكومات تعيد النظر في سياساتها الأمنية والدفاعية ليس بمفهومها القديم أو التقليدي وإنما بطرق حديثة وجديدة تتماشى مع هذه التكنولوجيا، وكل هذا كان بهدف تعزيز أمنها القومي، فهناك بعض الدول اتجهت لتكوين هيئات، ومنها من ارتقى إلى أن وصل لتكوين ما يشبه الوزارات لمواجهة التهديدات السيبرانية التي تواجه هذه الدول (craiyen، 2014:15).

وبهذا ، فإن الأمن السيبراني يعتبر واحدا من أهم التحديات التي تواجه العالم في الوقت الحالي، ولا تختلف ليبيا عن غيرها من دول العالم في هذا الصدد، إذ تشهد البلاد زيادة ملحوظة في التهديدات السيبرانية التي تتزايد تصاعديا مع التقدم التكنولوجي واعتماد الأفراد والمؤسسات على الإنترنت في مختلف جوانب حياتهم. وعليه، فإن ليبيا، كغيرها من الدول، ومن أجل حماية أمنها المحلي والقومي، اتجهت إلى إصدار العديد من القرارات المهمة والصادرة عن الجهات الرسمية في الدولة الليبية لإنشاء وتنظيم نشاط مزاولة خدمات الأمن السيبراني لمواجهة هذه التهديدات، والذي يحتاج إلى تحليل دقيق لتقييم مدى توافقه مع الوضع الراهن للأمن السيبراني في البلاد. وبالنظر إلى مفهوم الأمن السيبراني، فإننا نجد أنه مفهوم يتطور بسرعة وقد يتطلب خدمات جديدة بمرور الوقت، ولذلك يمكن القول إن ليبيا، كغيرها من الدول، اتخذت العديد من القرارات

المجلد الثالث
العدد السادس
سبتمبر 2025

مجلة جامعة درنة للعلوم الإنسانية والاجتماعية
DERNA UNIVERSITY JOURNAL OF HUMANITIES AND SOCIAL SCIENCES
Available online at https://dujhss.uod.edu.ly/
P-ISSN: 2959-6475 E-ISSN: 2959-6483 Impact Factor: 0.82

لمواجهة هذه التهديدات، وهي تمثل خطوة إيجابية نحو تنظيم نشاط خدمات الأمن السيبراني في ليبيا، ولكن هذا الأمر يتطلب دائما التعديل والتطوير لمواكبة تطور مفهوم التهديدات السيبرانية.

(1_2): مشكلة الدراسة

تدور مشكلة الدراسة حول مجموعة التهديدات السيبرانية التي تعرضت لها مؤسسات الدولة في ليبيا، والتي كان لها أثر كبير في خسائر هده المؤسسات، سواء كانت على المستوى السياسي أو على المستوى الاقتصادي، فقد تعرضت المؤسسات في ليبيا للعديد من الهجمات السيبرانية ومن بين هده المؤسسات "مصرف ليبيا المركزي"، حيث تعرضت منظومة بيع العملات الأجنبية " الدولار" لعدة هجمات سيبرانية، أثرت سلباً على سير عملها، كما تعرضت بعض شركات المؤسسة الوطنية للنفط والتي تعتبر عمود الاقتصاد للدولة الليبية إلي العديد من التهديدات السيبرانية، وتسببت هده الهجمات في خسارة لبعض إيرادات المؤسسة الوطنية للنفط، وكل هذا انعكس سلباً على الأمن داخل ليبيا، والتي ينعكس بدوره على الأمن القومي للدولة بشكل عام، ومن هذا المنطلق فإن السلطات الليبية سعت وبكل جدية تجاوز هذه التهديدات بالرغم من الوضع السياسي الغير مستقر، وذلك باتخاذ الإجراءات والاحتياطات الأمنية اللازمة على الصعيدين المحلى والدولي مع وضع حلول لمواجهة هذه التهديدات الذي تترصد بأمنها الوطني لتفادي هذه الهجمات الإلكترونية المهددة لها، وذلك عن طريق وضع قوانين وتشريعات خاصة بالاستخدامات الإلكترونية الحديثة، كما تسعى جاهدة للتعاون مع بقية دول العالم في عقد اتفاقيات في هذا الشأن.

ومن هنا تأتي مشكلة الدراسة والتي تتمثل في السؤال البحثي التالي: **ما هو أثر التهديدات السيبرانية على الأمن القومي في ليبيا ؟**

ويتفرع من السؤال الرئيسي مجموعة من الأسئلة الفرعية:

1_ ماهية الأمن السيبراني وأهدافه وابعاده ؟

2_ ما هي اهم التهديدات السيبرانية وعلاقتها بالأمن القومي في ليبيا؟

3_ ما هي أهم جهود الدولة الليبية لمواجهة التهديدات السيبرانية ؟.

(1_3): أهداف الدراسة:

يسعى الباحث في هذه الدراسة إلى تحقيق الأهداف التالية:

1_ التعرف على ماهية الأمن السيبراني وأهدافه وابعاده .

2_ تحديد اهم التهديدات السيبرانية وعلاقتها بالأمن القومي في ليبيا.

3_ إبراز أهم جهود الدولة الليبية لمواجهة التهديدات السيبرانية .

المجلد الثالث
العدد السادس
سبتمبر 2025

مجلة جامعة درنة للعلوم الإنسانية والاجتماعية
DERNA UNIVERSITY JOURNAL OF HUMANITIES AND SOCIAL SCIENCES
Available online at https://dujhss.uod.edu.ly/
P-ISSN: 2959-6475 E-ISSN: 2959-6483 Impact Factor: 0.82

(1_4): أهمية الدراسة:

تتبع أهمية الدراسة في كونها تعالج أحدى أهم القضايا التي أحدثت الكثير من الجدل بين الباحثين، ويمكن بيان أهمية الموضوع من خلال:

1_ تكمن أهمية الدراسة في كونها تتزامن مع المستجدات المعاصرة التي تشهدها الساحة الليبية.

2_ تحتل دراسة الأمن السيبراني مكانة كبيرة في مجال العلوم السياسية، وخاصة الوقت الراهن.

3_ توضيح مدى أثر التهديدات السيبرانية على مؤسسات الدولة بصفة عامة، وتأثيرها على المؤسسات في ليبيا بصفة خاصة.

4_ تكمن أهمية الدراسة كونها تقدم مجموعة من الحلول والمقترحات، التي إتخادتها الدولة الليبية في مواجهة التهديدات السيبرانية، وتوضيح مجموعة الاتفاقيات التي وقعتها ليبيا مع غيرها من الدول في هذا المجال.

(1_5): مفاهيم ومصطلحات الدراسة.

هناك عدة مفاهيم ومصطلحات يستوجب على الباحث توضيحها وهى كما يلي:

_ التهديدات السيبرانية: "هي أي نوع من التهديدات التي تستهدف الأنظمة الحاسوبية أو الأجهزة المتصلة بالإنترنت بهدف تعطيلها أو سرقتها أو إلحاق الضرر بالبنية التحتية المعلوماتية".(كمال، 2022: 17)

_ الأمن السيبراني: " هو مجموعة التدابير والتقنيات والممارسات التي تستخدم لحماية الأنظمة الحاسوبية والشبكات والبرمجيات والبيانات من الهجمات السيبرانية أو الأضرار أو الوصول غير المصرح به".(العمري، 2020: 28)

_ الأمن القومي:" يقصد به حماية الدولة ومصالحها الحيوية من التهديدات الداخلية والخارجية، بما في ذلك التهديدات العسكرية والسياسية والاقتصادية والاجتماعية، ويهدف إلى ضمان سيادة الدولة واستقرارها وحماية مواطنيها وممتلكاتهم".(قبلان،2023: 43)

(1_6): الدراسات السابقة.

1- دراسة (لامية، 2020) بعنوان(التهديدات والجرائم السيبرانية: تأثيرها على الأمن القومي للدول واستراتيجيات مكافحتها)

تناولت هذه الدراسة مفهوم التهديدات والجرائم السيبرانية، وأبرز التحديات التي تواجه الدول في هذا المجال، كما هدفت هده الدراسة إلى تقديم مجموعة من الحلول والاستراتيجيات التي ينبغي أن تتخذها الدول لمواجهة التهديدات السيبرانية وتعزيز أمنها القومي، وتوصلت الدراسة إلي أن كلما كانت للدولة استراتيجيات حديثة

المجلد الثالث
العدد السادس
سبتمبر 2025

مجلة جامعة درنة للعلوم الإنسانية والاجتماعية
DERNA UNIVERSITY JOURNAL OF HUMANITIES AND SOCIAL SCIENCES
Available online at https://dujhss.uod.edu.ly/
P-ISSN: 2959-6475 E-ISSN: 2959-6483 Impact Factor: 0.82

ومتنوعة في هذا المجال، كان من الصعب خرق مؤسستها والتأثير فيها، كما وضحت الدراسة مفهوم الأمن السيبراني توضيحاً دقيقاً وموسعاً، وأن الأمن السيبراني أصبح شيئاً مهماً لجميع الدول من أجل حماية مؤسساتها، وأوصت الدراسة بالعديد من التوصيات أهمها، مواكبة الدولة الوطنية للتطورات الحاصة في مجال الأمن السيبراني وتثقيف مواطنيها بهذا الشئ.

2- دراسة (عبد الرحمان،2020) بعنوان (الحرب السيبرانية: التحديات والاستراتيجيات)

هدفت هذه الدراسة إلي توضيح مفهوم الحرب السيبرانية وأبرز التحديات التي تواجهها الدول في هذا المجال. كما عرضت هده الدراسة مجموعة من الاستراتيجيات لمواجهة التهديدات السيبرانية وتعزيز الأمن القومي، واستعرضت ايضاً أهم أنواع الهجمات السيبرانية وطرق التصدي لها باستخدام التقنيات الحديثة، وتوصلت الدراسة إلي مجموعة من النتائج أهمها ، التحديات والمخاطر التي تواجه الدولة من جراء هذا الخطر وكيف تؤثر عليها، ووضع العديد من الاستراتيجيات لمواجهة هذا التهديدات، كما أوصت الدراسة بإقامة العديد من المراكز المهتمة بشأن السبيراني، وعقد العديد من المؤتمرات التي تناقش هذا الخطر والتهديد.

3_ دراسة (السحاتي، 2023) بعنوان(الأمن السيبراني ودوره في حماية الأمن القومي)

تناولت هذه الدراسة دور الأمن السيبراني في حماية الأمن القومي للدول، وأبرز التحديات التي تواجهها في ظل التطورات السريعة في وسائل الاتصال، كما ناقشت الحلول لمعالجة هذه التحديات، واستعرضت أبرز الهجمات السيبرانية التي تعرضت لها بعض الدول وتأثيرها على أمنها القومي، وتوصلت الدراسة إلي مجموعة من النتائج، حيث أوضحت دور الأمن السيبراني وأهميته للدولة الوطنية وحماية أمنها القومي، كما توصلت الدراسة إلي تعزيز والاهتمام بالأمن السيبراني، فكلما كانت الدولة مهتمة بهذا الجانب، كان أمنها القومي قويا ويصعب تهديده.

التعليق على الدراسات السابقة:

هناك العديد من الدراسات التي تناولت التهديدات السيبرانية والأمن السيبراني وقد تم استعراض جملة من الدراسات السابقة والتي تناولت موضوع هده التهديدات في المجتمع الدولي، إلا إن بعض هده الدراسات شابها بعض النقص حول الوقوف على الخطط والاستراتيجيات التي اتخذتها بعض الدول لمواجهة هده التهديدات والتصدي لها، وان ما يميز هده الدراسة عن سابق الدراسات التي تناولت هذا الموضوع، كون هده الدراسة أوضحت بشكل دقيق مدي أهمية موضوع التهديدات السيبرانية التي تتعرض إليها الدول بشكل عام والدولة الليبية بشكل خاص، وعليه فإن هده الدراسة سعت إلي توضيح التعريف بالأمن السيبراني بشكل أكبر وأوسع، وركزت على مجموعة الخطط والاستراتيجيات التي اتخذتها بعض الدول لمواجهة التهديدات السيبرانية

المجلد الثالث
العدد السادس
سبتمبر 2025

مجلة جامعة درنة للعلوم الإنسانية والاجتماعية
DERNA UNIVERSITY JOURNAL OF HUMANITIES AND SOCIAL SCIENCES
Available online at https://dujhss.uod.edu.ly/
P-ISSN: 2959-6475 E-ISSN: 2959-6483 Impact Factor: 0.82

ومن بينها ليبيا، كذلك سعي الدولة الليبية لمواجهة التهديدات السيبرانية والحفاظ علي أمنها القومي، والخطط والاستراتيجيات التي وضعتها الدولة الليبية لتصدى لمثل هذه التهديدات.

(1_7): منهجية الدراسة:

سيعتمد الباحث في هذه الدراسة على المنهج الوصفي التحليلي لجمع المعلومات والبيانات وتحليلها وتفسيرها وصولًا إلى تعميمات حول الموضوع. كما استعان الباحث بمنهج دراسة الحالة لتحليل أبرز التحديات التي تواجه الأمن السيبراني في ليبيا والتركيز عليها.

(1_8): تقسيم الدراسة:

قام الباحث بتقسيم الدراسة إلى ثلاثة محاور رئيسة وخاتمة، وجاءت المحاور كالتالي:

1. المحور الأول: الأمن السيبراني (المفهوم، الأهداف، الأبعاد).
2. المحور الثاني: التهديدات السيبرانية وتداعيها على الأمن القومي في ليبيا.
3. المحور الثالث: جهود الدولة الليبية في مواجهة التهديدات السيبرانية.

المحور الأول: الأمن السيبراني (المفهوم، الأهداف، الأبعاد):

مع التوسع المتسارع في استخدام التكنولوجيا الرقمية في مختلف جوانب الحياة اليومية، أصبحت التهديدات السيبرانية تمثل خطرا متزايدا على الأمن القومي للدول، وتشير التهديدات السيبرانية إلى محاولات غير المشروعة للوصول إلى الأنظمة الحاسوبية والشبكات والبيانات، بهدف السرقة أو التخريب أو التلاعب، وتعتمد هذه التهديدات على تقنيات وتكتيكات متنوعة، مثل البرمجيات الخبيثة، والهجمات المنسقة على الشبكات، وصولًا إلى استهداف البنية التحتية الحيوية كشبكات المياه والكهرباء والمرافق العامة (ال مواش، 2017: 17).

وترجع بدايات ظهور مفهوم الأمن السيبراني بشكله الحالي إلى العام*1983* م، إذ تمكّن معهد ماساتشوستس للتقنية *(MIT)* من تطوير نظام وطريقة اتصالات قائمة على مبدأ التشفير، وبالتالي اتخذ الخبراء هذا النظام ركيزة ومبدأ أساسياً لتطوير وسائل حديثة في مجال الأمن السيبراني وحماية العالم الرقمي من أشكال التهديد المختلفة.

الأمن السيبراني: "هو ممارسة حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية، حيث تسعى هذه الهجمات عادة إلى الوصول للمعلومات الحساسة، أو القيام بتغييرها أو إتلافها، أو ابتزاز بدفع الأموال من المستخدمين عبر برامج الفدية، أو تعطيل العمليات التجارية الاعتيادية، وبذلك فأن الأمن السيبراني يعمل على حماية المؤسسة وموظفيها وأصولها من التهديدات المخاطر الإلكترونية". (بارة،2017: 258)

المجلد الثالث
العدد السادس
سبتمبر 2025

مجلة جامعة درنة للعلوم الإنسانية والاجتماعية
DERNA UNIVERSITY JOURNAL OF HUMANITIES AND SOCIAL SCIENCES
Available online at https://dujhss.uod.edu.ly/
P-ISSN: 2959-6475 E-ISSN: 2959-6483 Impact Factor: 0.82

ومع تزايد شيوع وكثرة الهجمات السيبرانية وتطورها، وتزايد تعقيد شبكات الشركات الإلكترونية، تبرز الحاجة إلى مجموعة متنوعة من حلول الأمن السيبراني للتخفيف من مخاطرها السيبرانية، حيث تمثل الهجمات السيبرانية في وقتنا الحاضر مصدر قلق كبير لجميع دول المجتمع الدولي. (شلوش، 2108: 11)، وعند الاشارة الي مصطلح الهجمات السيبرانية وتفسيرها ، نجد أن هذه الهجمات يمكن وصفها بأنها عبارة عن: تصرف واقعي، يدور في عالم افتراضي قائم على استخدم بيانات رقمية، ووسائل اتصال تعمل إلكترونياً، ومن ثم تطور هذا المفهوم، حيث أصبح واسعاً يقوم على تحقيق أهداف عسكرية أو أمنية ملموسة ومباشرة، جراء اختراق مواقع إلكترونية حساسة، عادة ما تقوم بوظائف تصنف بأنها ذات أولوية ، كأنظمة حماية محطات الطاقة النووية، أو الكهربائية، أو المطارات، ووسائل النقل الأخرى، لذا وجب على الدول تطوير أمنها السيبراني لمواجهة مثل هذه التهديدات.(منصور، 2019: 99)

أنواع برامج حماية الأمن السيبراني.

يسعى الأمن السيبراني إلي حماية أجهزة الكمبيوتر والشبكات وتطبيقات البرامج والأنظمة الهامة والبيانات من التهديدات الرقمية المحتملة، وتتحمل المؤسسات مسؤولية تأمين البيانات للحفاظ على ثقة العملاء والامتثال للمتطلبات التنظيمية، فهي تعتمد تدابير وأدوات الأمن السيبراني من أجل حماية البيانات الحساسة من الوصول غير المصرح به، وكذلك منع أي انقطاع للعمليات التجارية بسبب نشاط الشبكة غير المرغوب فيه، و تطبق المؤسسات الأمن السيبراني من خلال تبسيط الدفاع الرقمي بين الأفراد والعمليات والتقنيات، وهناك العديد من البرامج التي تعتمدها هده المؤسسات لحماية بيناتها الشخصية . (كمال، 2022، 63)

- جدران الحماية المتقدمة.
- أنظمة كشف و الاختراق.
- أنظمة إدارة كلمات المرور.
- برامج مكافحة الفيروسات.
- برامج مكافحة البرمجيات الخبيثة.
- برامج الكشف عن التهديدات.
- أنظمة منع التسلل.
- برامج الحماية من التصيد الاحتيالي.

المجلد الثالث
العدد السادس
سبتمبر 2025

مجلة جامعة درنة للعلوم الإنسانية والاجتماعية
DERNA UNIVERSITY JOURNAL OF HUMANITIES AND SOCIAL SCIENCES
Available online at https://dujhss.uod.edu.ly/
P-ISSN: 2959-6475 E-ISSN: 2959-6483 Impact Factor: 0.82

ثانيا: الأهداف الأساسية للأمن السيبراني.

يعتبر الأمن السيبراني عنصرا أساسياً لحماية البيانات والأنظمة من الهجمات الإلكترونية، مع ضمان سرية البيانات وسلامتها، وتوفيرها عند الحاجة إليها من خلال تقنيات مثل التشفير والمصادقة والحفظ، كما يهدف الأمن السيبراني إلى حماية المؤسسات من تهديدات البرامج الضارة والقرصنة، ويعزز استمرارية الأعمال والامتثال للوائح الأمنية، كما يعتبر اليوم أداة حيوية لمنع الهجمات الإلكترونية وضمان الثقة بين الشركات والعملاء. (Thomas، March2014)

وتتعدد أهداف الأمن السيبراني، الذي يعد الإجراء الأحسن والأقوى لحماية الأنظمة والشبكات والبرامج من الهجمات الرقمية الخبيثة، حيث يلجأ الأفراد والمؤسسات إلى هذه الممارسات للحفاظ على المعلومات الحساسة ومراكز البيانات والأنظمة المحوسبة الأخرى من المخترقين والذين يقومون بتغييرها أو حذفها أو تدميرها أو ابتزاز أصحابها بها. (السمحان، 2020: 12)

وهناك أهداف أخرى لممارسة الأمن السيبراني، نستعرض منها الآتي.

تعتبر حماية وضمان خصوصية البيانات الحساسة والمهمة هي الهدف الأساسي للأمن السيبراني سواء كانت معلومات شخصية للمستخدم، أو أسرارا تجارية، أو وثائق حكومية، فإن حماية البيانات من الوصول غير المصرح به أمر بالغ الأهمية، ومنها تتفرع العديد من الأهداف الأخرى منها حماية النظام الإلكتروني لأي مؤسسة والمحافظة عليها وإتاحة الوصول الصحيح الآمن إليها كذلك يسعى الأمن السيبراني للدفاع ضد أي تهديدات الكترونية أو سيبرانية ، وحوكمة الأمن السيبراني تسعى دائماً إلي تعزيز الوعي لدى منسوبي أي مؤسسة واستمرارية الأعمال والتعافي من الحوادث السيبرانية.(السمحان، 2020: 13)

كذلك من الأهداف التي يقوم بها الأمن السيبراني تدريب الموظفين داخل المؤسسة والتوعية الأمنية، والهدف منها تعزيز ثقافة الوعي الأمني والتأكد من أن جميع الموظفين على دراية جيدة بأفضل ممارسات الأمن السيبراني، ويتم ذلك بتوفير تدريب إلزامي في مجال الأمن السيبراني لجميع الموظفين وإجراء تمارين محاكاة ربع سنوية للاختراق الاحتيالي وتحسين قدرة الموظفين على التعرف على أنواع هذه الاختراقات. (سالم، 2022: 72)

وأخيرا يجب القول أن العديد من أهداف الأمن السيبراني تستند إلى أفضل الممارسات الراسخة، وهي مشتركة بين جميع أنواع المؤسسات، إلا أنها قد تختلف باختلاف حجم المؤسسة، حيث تختلف أولويات وتحديات المؤسسات الصغيرة عن المؤسسات الكبيرة. ومن المؤكد أن أهداف الأمن السيبراني المحددة ستختلف لتلبية مختلف الميزانيات والموارد، فالمؤسسات الصغيرة والمتوسطة تبدأ بأهداف أساسية للأمن السيبراني، وتطبيق

المجلد الثالث
العدد السادس
سبتمبر 2025

مجلة جامعة درنة للعلوم الإنسانية والاجتماعية
DERNA UNIVERSITY JOURNAL OF HUMANITIES AND SOCIAL SCIENCES
Available online at https://dujhss.uod.edu.ly/
P-ISSN: 2959-6475 E-ISSN: 2959-6483 Impact Factor: 0.82

تدابير أساسية للأمن السيبراني، مثل جدران الحماية، وبرامج مكافحة الفيروسات، وسياسات كلمات المرور الآمنة، ويتمثل اهتمامها الرئيس في تحديد مستوى أساسي من الحماية، وقد تحدد قيود الميزانية أهداف الأمن السيبراني للمؤسسات الصغيرة والمتوسطة. وقد تشمل هذه الأهداف تعظيم الاستفادة من الموارد المحدودة، والاستفادة من حلول أمنية فعالة وبأسعار معقولة، وبهذا فإن المؤسسات الصغيرة والمتوسطة تعطي الأولوية لبرامج التوعية والتدريب على الأمن السيبراني لضمان اطلاع الموظفين جيدا على التهديدات المحتملة وأفضل الممارسات وإيجاد أنسب وأفضل الحلول لهذه التهديدات.

ثالثا : أبعاد الأمن السيبراني.

يطال الأمن السيبراني جميع النواحي المختلفة للدولة سواء أكانت سياسية أو اقتصادية أو اجتماعية أو حتى إنسانية، فعند الرجوع الى بعض التعريفات للأمن السيبراني نجد أنها تتكلم عن مدى قدرة الدولة على حماية الشعب في مختلف المجالات، مما يضمن له التقدم والازدهار هذا من ناحية، ومن ناحية أخري يضمن له عملية الاتصال والتواصل بأمان وهو المحور الاساسي الذى يقوده للإبداع والقدرة على المنافسة.

ومن هذا المنطلق سوف نتطرق للحديث عن أبعاد الأمن السيبراني، والتي تنقسم الى العديد من الأبعاد ومنها.

1- البعد السياسي.

يتمثل البعد السياسي للأمن السيبراني بشكل أساسي في قدرة الدولة على حماية نظامها السياسي والحفاظ عليه، والحفاظ على أمنها الاقتصادي وديمومته، والدفاع عن كيان الدولة من أي خطر أو تهديد، سواء أكان من الداخل أو من خارج الدولة (السمحان، 2023: 15).

عليه، فإن البعد السياسي للأمن السيبراني ينطلق من منطلق حماية نظام الدولة السياسي وكيانها المستقل، حيث يمكن في بعض الأحيان أن تستخدم بعض الجهات المعادية للدولة آليات وتقنيات في بث معلومات وبيانات قد يحدث من خلالها زعزعة لاستقرار أمن هذه الدولة وحكوماتها، حيث تصل بسرعة فائقة إلى أكبر شرائح من المواطنين وتتسع في أكثر من رقعة جغرافية بغض النظر عن صحة البيانات والمعلومات التي يتم نشرها. وهنا يأتي دور الدولة في حماية والحفاظ على أمنها القومي والمحافظة على نظامها السياسي (جبور، 2016: 29).

المجلد الثالث
العدد السادس
سبتمبر 2025

مجلة جامعة درنة للعلوم الإنسانية والاجتماعية
DERNA UNIVERSITY JOURNAL OF HUMANITIES AND SOCIAL SCIENCES
Available online at https://dujhss.uod.edu.ly/
P-ISSN: 2959-6475 E-ISSN: 2959-6483 Impact Factor: 0.82

2- البعد الاقتصادي.

هناك ارتباط وثيق بين الأمن السيبراني من جهة والحفاظ على المصالح الاقتصادية للدولة من جهة أخرى، إذ يرتبط الاقتصاد بالمعرفة بشكل كبير. تعتمد معظم الدول في تعزيز اقتصادها وازدهاره على إنتاج وتداول المعرفة والمعلومات، مما يبرز الدور الحيوي للأمن السيبراني في حماية الاقتصاد من السرقة والاعتداء على الملكية الفكرية.

لذا، توجد علاقة قوية بين الأمن السيبراني والاقتصاد والمعرفة والمعلومات، خاصة مع تزايد الاعتماد على البيانات وتكنولوجيا المعلومات والاتصالات في التنمية الاقتصادية، ودخول العالم عصر النقود الإلكترونية والخدمات المالية الرقمية. وقد طورت معظم الدول تشريعات لحماية أموالها من الجرائم الاقتصادية العابرة للحدود مثل غسيل الأموال والسرقة والتهرب الضريبية وغيرها. (مختار، 2015: 6).

3_ البعد القانوني.

يشير البعد القانوني للأمن السيبراني إلى مجموعة القوانين والتشريعات التي تنظم وتحمي المعلومات والبيانات الرقمية من التهديدات والاختراقات الإلكترونية، ويهدف هذا البعد إلى توفير إطار قانوني يحمي الأفراد والمؤسسات من الاعتداءات السيبرانية، ويعاقب مرتكبي الهجمات الإلكترونية، كما تختلف التشريعات من دولة لأخرى، وتشمل قوانين حماية البيانات: مكافحة الجرائم السيبرانية، تنظيم الاتصالات الإلكترونية، حقوق الملكية الفكرية، والخصوصية الإلكترونية، وغيرها من التشريعات ذات الصلة، وتسهم هذه التشريعات في تحديد الأنشطة غير المشروعة على الإنترنت، وتحديد الجرائم السيبرانية وعقوباتها، كما تحمي حقوق الأفراد والشركات فيما يخص الخصوصية والملكية الفكرية والمعلومات الحساسة، ومن خلال إطار قانوني قوي، يتم تعزيز الأمن الاجتماعي وتوفير بيئة آمنة للمستخدمين وضمان حماية خصوصياتهم وبياناتهم الشخصية (العوادي، 2016: 9).

4_البعد العسكري.

يقصد بالبعد العسكري للأمن السيبراني ذلك الجانب المرتبط بالجوانب العسكرية والدفاعية، حيث يهدف إلى حماية البنية التحتية السيبرانية للقوات المسلحة والأنظمة العسكرية من الهجمات السيبرانية، وتأمين المعلومات الحساسة والمهمة للأمن القومي.

كما أن للبعد العسكري للأمن السيبراني تأثيرا واضحا على الجغرافيا السياسية للدولة، إذ أصبحت القدرات السيبرانية العسكرية مؤشرا مهما لقوة الدولة؛ لذلك تم دمج عمليات الفضاء الإلكتروني في هياكل القوة

المجلد الثالث
العدد السادس
سبتمبر 2025

مجلة جامعة درنة للعلوم الإنسانية والاجتماعية
DERNA UNIVERSITY JOURNAL OF HUMANITIES AND SOCIAL SCIENCES
Available online at https://dujhss.uod.edu.ly/
P-ISSN: 2959-6475 E-ISSN: 2959-6483 Impact Factor: 0.82

العسكرية، خاصة في الخطط الحربية، والأقمار الصناعية العسكرية، وتدريبات الدفاع، حتى أصبح دمج القدرات السيبرانية جزءا أساسيا من جميع المستويات للقوات المسلحة لمواجهة التهديدات المحتملة، ضمن السياسات الموضوعة لحماية أمن الدولة ونظامها السياسي القائم (العمري، 2020: 35).

المحور الثاني : التهديدات السيبرانية وتداعيها على الأمن القومي في ليبيا.

أصبح الأمن السيبراني أحد أهم التحديات التي تواجه جميع دول العالم في الوقت الحالي، ولا تختلف ليبيا عن غيرها في هذا الصدد، إذ تشهد ليبيا، كغيرها من الدول، زيادة ملحوظة في التهديدات السيبرانية التي تتزايد بسرعة مع التقدم التكنولوجي، وبالاعتماد المتزايد من قبل الأفراد والمؤسسات على الإنترنت والتكنولوجيا في مختلف جوانب حياتهم؛ فإنه يمكن القول إن التكنولوجيا التي وفرت لنا كل شيء نريده، هي نفسها التي قد تسلب منا كل شيء لدينا، وفي ظل عصر الذكاء الاصطناعي ومع تزايد اعتماد الدول على شبكات الإنترنت المتطورة، وبسبب ربط البنية التحتية بهذا النمط، برز الفضاء السيبراني ليشكل تهديداً للأمن القومي للدول، حيث تعتبر ليبيا جزءاً من هذا العالم الرقمي، مما يجعل أفرادها ومؤسساتها عرضة للتهديدات السيبرانية بجميع أشكالها (أبو مهارة، 2024: 1).

وتعتبر ليبيا من بين الدول التي يتعرض أمنها الوطني للتهديدات السيبرانية، والتي تمثلت في شكل جرائم إلكترونية لم تفرق بين الأشخاص والمؤسسات والدول، كما أخذت شكلاً تصاعدياً في الآونة الأخيرة، وهو ما ينبئ بخطورة الوضع، مما جعل مؤسسات ليبيا العامة والخاصة أكثر عرضة لهذه الهجمات، وفرض تحديات أثرت بشكل مباشر على منظومة أمنها الوطني وتركت آثاراً سلبية على الأمن القومي الليبي ،وعلى هذا الأساس، فإن السلطات الليبية تحاول تجاوز هذه التهديدات، وذلك باتخاذ الإجراءات والاحتياطات الأمنية اللازمة على الصعيدين المحلي والدولي، مع وضع حلول لمواجهة هذه التهديدات التي تترصد بأمنها الوطني لتفادي هذه الجرائم الإلكترونية التي تهدد أمنها الوطني والقومي، وذلك عن طريق وضع قوانين وتشريعات خاصة بالاستخدامات الإلكترونية الحديثة، كما تسعى جاهدة للتعاون مع بقية دول العالم (مانيطه، 2017: 4).

- أمثلة لبعض التهديدات السيبرانية التي تعرضت لها الدولة الليبية وكيف أثرت على أمنها القومي والوطني .

ففي ظل هشاشة الوضع الأمني والانقسام السياسي الحاصل في ليبيا، خاصة بعد عام 2011، تعرضت الدولة الليبية خلال السنوات السابقة للعديد من الاختراقات والهجمات السيبرانية، حيث استهدفت هذه الهجمات العديد من المرافق والمؤسسات العامة، منها السيادية ذات الطابع الخاص والقومي، وكان لها أثر

المجلد الثالث
العدد السادس
سبتمبر 2025

مجلة جامعة درنة للعلوم الإنسانية والاجتماعية
DERNA UNIVERSITY JOURNAL OF HUMANITIES AND SOCIAL SCIENCES
Available online at https://dujhss.uod.edu.ly/
P-ISSN: 2959-6475 E-ISSN: 2959-6483 Impact Factor: 0.82

سلبي على الدولة الليبية بشكل عام، وعلى أمنها القومي بشكل خاص، وبالتالي، فإن أي هجوم على مؤسسات الدولة ينعكس بشكل مباشر على أمنها القومي، وهناك العديد من الهجمات السيبرانية التي تعرضت لها المؤسسات داخل الدولة الليبية، خاصة في السنوات الأخيرة الماضية، ومن هذه المؤسسات التي تعرضت للهجمات السيبرانية (صحيفة المرصد، 2023).

1: مصرف ليبيا المركزي.

يرتبط الهجوم السيبراني الذي تعرض له مصرف ليبيا المركزي بمصالح بعض الجهات الرامية إلى عرقلة الحجز للأغراض الشخصية التي أطلقها المصرف، وهي من ضمن سياسات المصرف الاقتصادية التي تهدف إلى حجز قيمة مالية بالعملة الأجنبية مقابل الدينار الليبي، وذلك لتخفيف العبء على المواطن الليبي وحل أزمة السيولة في المصارف التجارية الليبية .(المرصد، 2024).

و يعاني مصرف ليبيا المركزي في الفترة الأخيرة من العديد من الهجمات الإلكترونية المتنوعة، حيث تعرضت منصة حجز العملة الأجنبية للأفراد بتاريخ 3 أبريل 2024 إلى هجوم سيبراني من نوع حجب الخدمة (DDoS)، مما أدى إلى حجب الخدمة عن مستخدمي هذه المنصة، بدوره تصدى فريق تقني تابع للمصرف للهجوم عبر منع الوصول للمنظومة لأي عنوان شبكي مسجل خارج ليبيا، ولم تنته الهجمات الإلكترونية على منصات مصرف ليبيا المركزي عند هذا الحد، إذ أشار المصرف إلى تعرض الموقع الإلكتروني الرسمي له لهجوم آخر من نفس النوع، متحدثاً عن عملية تصد له ومعالجة أي اختراقات مستقبلية مشابهة.(وكالة الأنباء الليبية،2024)

و تأتي هذه الهجمات الإلكترونية في وقت أطلق فيه مصرف ليبيا المركزي، منذ الثاني من فبراير 2024، منصة حجز العملة الأجنبية للأفراد، بعدما أعلن مجموعة ضوابط لشراء النقد الأجنبي للأغراض الشخصية، ومن بين ضوابط "المركزي الليبي" المعلنة تحديد مبلغ قدره أربعة آلاف دولار أو ما يعادله من العملات الأخرى كحد أقصى لما يباع للشخص الواحد ، ومن خلال جميع المصارف العاملة في ليبيا، ومنحت الضوابط المصارف صلاحية البت في طلبات بيع النقد الأجنبي للأغراض الشخصية عن طريق الرقم الوطني لكل مواطن ليبي يبلغ من العمر 18 سنة فما فوق، بعد استيفاء جميع الأوراق والمتطلبات المطلوبة (وكالة الأنباء الليبية، 2024).

وعليه، فإن إعلان المصرف المركزي الليبي عن هذه الإجراءات المالية، فضلاً عن فرض ضريبة على سعر صرف العملات الأجنبية في وقت سابق، كانت من بين الأسباب التي تكثفت معها الهجمات الإلكترونية على موقع المصرف، وفق بعض المراقبين.

المجلد الثالث
العدد السادس
سبتمبر 2025

مجلة جامعة درنة للعلوم الإنسانية والاجتماعية
DERNA UNIVERSITY JOURNAL OF HUMANITIES AND SOCIAL SCIENCES
Available online at https://dujhss.uod.edu.ly/
P-ISSN: 2959-6475 E-ISSN: 2959-6483 Impact Factor: 0.82

2: شركة ليبيا للاتصالات والتقنية :

كذلك من بين التهديدات السيبرانية، الهجوم الذي تعرضت له شركة ليبيا للاتصالات والتقنية، حيث أعلنت الشركة، في يوم الأربعاء الموافق 12 يوليو سنة 2023، عن تعرض مركز البيانات التابع لها لهجوم حجب الخدمة شمل كافة مشغلاتها، وأشارت إلى أن الهجوم استمر لعدة أيام، مما أثر بشكل كبير على خدمات الشبكة.

كما أوضحت الشركة في منشور لها عبر صفحتها الرسمية بموقع التواصل الاجتماعي، أن الهجوم الذي بلغ حجمه أكثر من 50 جيجابايت، أدى إلى تذبذب خدمات مركز البيانات، وأوضحت أن شركتي ليبيا للاتصالات والتقنية والاتصالات الدولية تعاونتا مع فريق الأمن السيبراني للشركة القابضة للاتصالات للتصدي لهذا الهجوم والسيطرة عليه. وأكدت الشركة القابضة للاتصالات أن الهجمات السيبرانية التي تعرضت لها قواعد بيانات شركة «ليبيانا للهاتف المحمول» لم ينتج عنها تسريب أي بيانات خاصة بالمشتركين، وأن البيانات التي تم الهجوم عليها تخص المنظومة الداخلية الخاصة بالموظفين داخل الشركة، عليه أكدت الشركة الليبية للاصالات والتقنية أن هذه الهجمة لا علاقة لها بسجل المكالمات أو بعمليات اختراق حسابات مواقع التواصل الاجتماعي الخاصة بالمشتركين، حيث تعرضت عدة شركات وبنوك عالمية لنفس الهجمة السيبرانية وفي نفس التوقيت (الموقع الرسمي لشركة ليبيا للاتصالات والتقنية، 2023). ومن أجل حماية بيانات المواطنين الليبيين، قامت الشركة القابضة للاتصالات والتقنية بإنشاء فريق خاص بالأمن السيبراني للتصدي لمثل هذه الهجمات وجعل فضاء الإنترنت أكثر أماناً، حيث تعتبر معركة الأمن السيبراني مستمرة في كل العالم. عليه، صرحت الشركة بأنها تقوم بعمل يومي مستمر لحماية الشبكات ضد الهجمات والتهديدات السيبرانية.

3: المؤسسة الوطنية للنفط.

كذلك تعرضت المؤسسة الوطنية للنفط في ليبيا، لعدة هجمات سيبرانية متكرره ومختلفة ، حيث تعرضت شركة مليتة للنفط والغاز في مايو 2024، وطالبو منفذو هذا الهجوم وهم مجموعة تدعى RansomHub بفدية مقابل عدم نشر بيانات سرقوها من الشركة، كما تمكنت شركة "زلاف" في نفس العام من التصدي لهجوم تصيد احتيالي، بالإضافة إلى ذلك كانت هناك الكثير من التقارير والأخبار التي تفيد عن هجوم إرهابي في عام 2018 على مقر المؤسسة في طرابلس، وفي نفس العام سنة 2018، وقع هجوم إرهابي على مقر المؤسسة الوطنية للنفط في طرابلس. (المرصد، 2024)

هذه الحوادث تظهر حجم المخاطر السيبرانية والإرهابية التي تواجهها المؤسسة الوطنية للنفط في ليبيا وتأثيرها المباشر على الأمن القومي والاقتصاد الوطني، كما تعرضت بعض الشركات الأخرى التابعة

المجلد الثالث
العدد السادس
سبتمبر 2025

مجلة جامعة درنة للعلوم الإنسانية والاجتماعية
DERNA UNIVERSITY JOURNAL OF HUMANITIES AND SOCIAL SCIENCES
Available online at https://dujhss.uod.edu.ly/
P-ISSN: 2959-6475 E-ISSN: 2959-6483 Impact Factor: 0.82

للمؤسسة الوطنية للنفط لبعض التهديدات والهجمات السيبرانية، والتي أثرت فيها بشكل مباشر، مما خلفت العديد من الخسائر لهده الشركات، ونذكر منها :

هجوم شركة "مليتة" (مايو 2024):

تعرضت شركة مليتة للنفط والغاز لهجوم سيبراني من مجموعة RansomHub، حيث سرقوا 1 تيرابايت من البيانات المالية والإنتاجية والمراسلات السرية، وطالبوا بفدية قدرها 50 مليون دولار مقابل عدم نشرها، وأكدت شركة "إيني" الإيطالية أن الهجوم لم يؤثر على أنشطة الإنتاج أو العمليات التشغيلية، ويجري حالياً استعادة أنظمة تكنولوجيا المعلومات المتضررة تدريجياً، فالمشكلة بقيت محصورة في أنظمة مليتة، ولم تتأثر بها أقسام أو وحدات شركة إيني الأخرى.(المرصد، 2024)

هجوم شركة " زلاف " (مايو 2024):

في مايو 2024، تمكن فريق الأمن السيبراني في شركة "زلاف" من التصدي لهجوم تصيد احتيالي استهدف أنظمتهم، واتخذوا إجراءات احترازية عاجلة لضمان عدم تأثر الأنظمة، في المؤسسة الوطنية للنفط حيث أشادت بهذه الجهود وأكدت أهمية الأمن السيبراني لحماية البيانات الحساسة المتعلقة بالإنتاج والتسويق والعقود، ما يجعلها هدفاً للمهاجمين السيبرانيين، كما شددت المؤسسة على أهمية حماية الأنظمة لضمان استمرار عمليات الإنتاج والتوزيع، خاصة وأن القطاع النفطي هو حجر الزاوية في الاقتصاد الليبي. (المرصد، 2024)

وأخيراً يمكن القول إنَّ ليبيا كغيرها من الدول تشهد تحولاً رقميا سريعا، مما يجعل الأمن السيبراني ضرورة أساسية لحماية الأنظمة والبيانات من الهجمات الإلكترونية، فهناك حاجة ملحة لتوعية المسؤولين بأهمية الأمن السيبراني، وسن قوانين جديدة وتحديث التشريعات لمواكبة التهديدات الحديث، فجعل الأمن السيبراني أولوية وطنية ضروري لضمان نجاح التحول الرقمي واستقرار المؤسسات الوطنية في ليبيا.

المحور الثالث : جهود الدولة الليبية لمواجهة التهديدات السيبرانية .

تعتبر التهديدات السيبرانية من أكثر المخاطر التي تواجهها الدول في الوقت الراهن، حيث يمكن لهذه التهديدات أن تستهدف البنية التحتية الحساسة، وتؤدي إلى خسائر اقتصادية كبيرة، وتؤثر على الأمن العام والأمن القومي للدولة، وكما أشرنا سابقاً، فإن التهديدات السيبرانية تتضمن مجموعة واسعة من الأنشطة الضارة مثل الهجمات على الشبكات الحكومية والعسكرية، وسرقة البيانات الحساسة، والتجسس الإلكتروني وهجمات الفدية، وتعطيل الخدمات الحيوية. ومع تزايد تطور الأدوات والتقنيات المستخدمة في تنفيذ هذه

المجلد الثالث
العدد السادس
سبتمبر 2025

مجلة جامعة درنة للعلوم الإنسانية والاجتماعية
DERNA UNIVERSITY JOURNAL OF HUMANITIES AND SOCIAL SCIENCES
Available online at https://dujhss.uod.edu.ly/
P-ISSN: 2959-6475 E-ISSN: 2959-6483 Impact Factor: 0.82

الهجمات، يصبح من الضروري على الدول فهم وتحليل مظاهر هذه التهديدات، وتأثيرها على الأمن القومي والجهات الفاعلة فيها. (عبد الصادق، 2016: 2)

وتختلف الهجمات السيبرانية عن بقية التهديدات التقليدية الأخرى التي تؤثر على الأمن القومي للدول، حيث عرفت الهجمات السيبرانية بأنها وسيلة قتالية من خلال استخدامها بذاتها للتسلل إلى أنظمة إلكترونية معدة لحماية أو لتنظيم سير عمل منشآت حيوية، كمحطات توليد الطاقة النووية، أو السدود، أو وسائل النقل كالمطارات؛ بهدف تطويعها والسيطرة عليها، لتدمير ذاتها بذاتها من خلال تغذيتها بمعلومات غير صحيحة لأجهزة التحكم الإلكترونية (شلوش2018: 7).

وبذلك فقد تنوعت الجهود الدولية في مكافحة الجريمة السيبرانية، حيث تم اتخاذ العديد من الآليات والإجراءات للحد والتقليل منها، إلا أنه ومن الناحية الواقعية فإن هذه الجهود تبقى غير كافية مقارنة بالتقدم التكنولوجي الذي تشهده الدول على مستوى السيبرانية والاستعمال الكبير للكمبيوتر والإنترنت، وفي ظل هذه التحديات، سعت العديد من دول العالم ومن بينها ليبيا لوضع العديد من الاستراتيجيات الفعالة للأمن السيبراني، بحيث تكون مرنة وقابلة للتكييف بشكل كاف لتتسنى لها مواكبة التقدم التكنولوجي السريع وتحديات الأمن المرتبطة بها والاستجابة لها، وكل هذا يصب في حماية أمنها القومي والمحافظة عليه، كما سعت هذه الدول لاتخاذ إجراءات لتحديد مصدر الهجمات وهوياتها، وإنشاء أجهزة تابعة للدولة من أجل التصدي للهجمات السيبرانية المجهولة الهوية والاشتباكات الدولية التي تهدد الأمن القومي لها (عبد الرحمن، 2021: 43).

حيث أكدت ليبيا أن مسؤولية التأمين من الأخطار السيبرانية مسؤولية مشتركة بين جميع أبناء الوطن الواحد، ومساهمة جميع أصحاب المصلحة في تنفيذ الخطط السيبرانية التنموية والأمنية، وضمن الخطط المستقبلية، أكدت ليبيا على أهمية دور مؤسسات التنشئة الاجتماعية والدينية لحماية الأطفال والمراهقين والمرأة من المخاطر السيبرانية (مانيطه، 2017: 5) ايضاً قامت ليبيا بمكافحة الإرهاب والتهديدات السيبرانية في مجال الأمن القومي وتوحيد الجهود لمواجهة تحديات الأمن السيبراني، وتوفير الحماية اللازمة للبيانات والمعلوماتية الحساسة ، إضافة إلى تعزيز دور مجلس الأمن القومي الليبي والجهات ذات العلاقة في مجال الأمن السيبراني ، وتعزيز الجاهزية والإستعداد المواجهة المخاطر السيبرانية ، هذا كما انتقلت ليبيا إلى المبادرات والتعاون الإقليمي والدولي مع بقية الدول الصديقة لإيجاد حلول لهذه التهديدات.(شعيتير، 2023)

عليه فقد سعت الدولة الليبية كغيرها من الدول لتصدي للتهديدات والجرائم السيبرانية، وحماية أمنها القومي، وفي هذا الشأن وضعت الدولة الليبية العديد من الخطط، وأنشات العديد من الاجهزة لتصدي لهده التهديدات التي تشكل خطر على أمنها القومي بشكل مباشر، ومن الخطط التي وضعتها الدولة الليبية لمواجهة

المجلد الثالث
العدد السادس
سبتمبر 2025

مجلة جامعة درنة للعلوم الإنسانية والاجتماعية
DERNA UNIVERSITY JOURNAL OF HUMANITIES AND SOCIAL SCIENCES
Available online at https://dujhss.uod.edu.ly/
P-ISSN: 2959-6475 E-ISSN: 2959-6483 Impact Factor: 0.82

التهديدات السيبرانية، قامت ليبيا بإنشاء العديد من المراكز التي تعنى بالتأمين السيبراني وتهديداته، ومن بين هذه المراكز المعهد الوطني للأدلة الجنائية، وعلم الإجرام للأمن الوطني، ومركز الوقاية من جرائم الإعلام الآلي، والجرائم المعلوماتية للأمن الوطني، والهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، بالإضافة إلى المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني، ومنظمة رصد الجرائم في ليبيا ، والجمعية الليبية للإنترنت الآمن.(الفيتوري،2023)

هذا كما اعتمدت الحكومة الليبية الأول من يونيو في كل عام يوماً وطنيا لتقنية المعلومات، وأنشئت لجنة وطنية للتحول الرقمي، إضافة للهيئة الوطنية لأمن وسلامة المعلومات، كذلك اهتمت ليبيا بالتحول الرقمي تحت شعار ليبيا دولة رقمية سنة 2023، كذلك قامت الدولة الليبية بدعم وتأسيس المواقع العلمية والمراكز المهنية والأكاديميات العلمية لتعزيز دور مجلس الأمن القومي الليبي نحو التحول الرقمي، إضافة إلى وضع خطة لتأهيل الكوادر الأمنية بالدولة الليبية في مجال إدارة الحالات الطارئة، والتعامل مع مخاطر الهجمات السيبرانية، أيضاً قامت ليبيا بنشر الوعي الأمني حول الأمن السيبراني وخطورته لدى المجتمع الليبي، وتطوير العمل الأمني في العصر الرقمي للأجهزة الأمنية الوطنية وعصر سرعة انتقال المعلومة ودعم الاستراتيجيات الوطنية في مجالات الأمن القومي الليبي.(شعيتير،2023)

وصدر بتاريخ 31 مارس 2024 عن وزارة الاقتصاد والتجارة في ليبيا قرار بتنظيم نشاط مزاولة خدمات الأمن السيبراني، والذي يحتاج إلى تحليل دقيق لتقييم مدى توافقه مع الوضع الراهن للأمن السيبراني في البلاد، وبعد دراسة القرار رقم (150) لسنة 2024م الصادر عن وزير الاقتصاد والتجارة بشأن تنظيم نشاط خدمات الأمن السيبراني، يظهر أن هناك توازناً مهماً بين الضرورة لتنظيم هذا النشاط، وبين التحديات والتهديدات التي قد تواجهه الشركات والأفراد في هذا المجال داخل الدولة .(أبومهارة، 2024)

أما بالنسبة لتشريعات التي وعتها الدولة الليبية لمواجهة التهديدات السيبرانية للأمن القومي الليبي، قامت ليبيا بسن العديد من التشريعات والقوانين الرادعة للحد من التهديدات السيبرانية ، منها القانون رقم 3 لسنة 2014 الصادر عن مجلس النواب، والذي نص على مكافحة الإرهاب والجرائم الإلكترونية وذلك في مادته (2) والمادة (15) والمادة (17) ،أيضاً النص على تحريم الاعتداء على المال المعلوماتي المعنوي من قبل المشرع الليبي لمكافحة الجرائم الإلكترونية، سواء بالسرقة أو الإتلاف أو غيرهما، (1) كذلك قانون مكافحة الجرائم الإلكترونية" والذي أقره مجلس النواب الليبي في جلسته المنعقدة في 26 أكتوبر 2021 ؛ إذ أعلن المستشار الإعلامي لرئيس مجلس النواب الليبي " إن قانون مكافحة الجرائم الإلكترونية يعنى بالجرائم الإلكترونية التي تمس الدولة ولكنه، لا يتعارض رغم ذلك مع حرية التعبير، وتابع أن القانون يعنى بأي جرم

المجلد الثالث
العدد السادس
سبتمبر 2025

مجلة جامعة درنة للعلوم الإنسانية والاجتماعية
DERNA UNIVERSITY JOURNAL OF HUMANITIES AND SOCIAL SCIENCES
Available online at https://dujhss.uod.edu.ly/
P-ISSN: 2959-6475 E-ISSN: 2959-6483 Impact Factor: 0.82

أو استخدام خاطئ للأدوات الإلكترونية تسبب المشاكل للدولة، (قانون مكافحة الجرائم الالكترونية الصادر عن مجلس النواب الليبي، 2021).

وسن أيضا القانون رقم (5) السنة 2022 والذي أصدره مجلس النواب الليبي في 27 سبتمبر 2022، بشأن مكافحة الجرائم الإلكترونية ؛ اذ نصَّ في مادته الثانية على تحقيق العدالة والأمن المعلوماتي، وحماية النظام العام والآداب العامة والاقتصاد الوطني وحفظ الحقوق، كذلك نصَّ القانون على تمكين الهيئة الوطنية لأمن وسلامة المعلومات من فرض رقابة شاملة على كافة البيانات والمعلومات المنشورة على شبكة الإنترنت، وعلى جميع الأنظمة الإلكترونية والتقنية، كما طالب بالعمل على حماية خصوصية المواطنين وحماية بياناتهما ،أيضاً نصَّ القانون في مادته رقم (4) على أن يكون استخدام شبكة المعلومات الدولية، ووسائل التقنية الحديثة مشروعة ما لم يترتب عليه مخالفة للنظام العام ، أو الآداب العامة، كذلك نصت المادة (5) من نفس القانون على أن المواقع الإلكترونية وأنظمة المعلومات الرقمية ملك لأصحابها، لا يجوز الدخول إليها أو إلغائها أو حذفها أو إتلافها وتعطيلها أو تعديلها أو نقل أو نسخ بياناتها، أما المادة (7) من القانون فقد سمحت بتمكين الهيئة الوطنية لأمن وسلامة المعلومات بحجب كل ما ينشر النعرات ،أو الأفكار التي من شأنها زعزعة أمن المجتمع واستقراره ، والمساس بسلمه الاجتماعي.(الجريدة الرسمية قانون رقم 5 الصادر عن مجلس النواب الليبي، 2022).

الخاتمة والنتائج.

مع تزايد الاعتماد الكلي على التكنولوجيا في جميع مجالات الحياة، سواء أكانت سياسية أو اقتصادية أو عسكرية، أصبحت التهديدات السيبرانية تمثل خطرا متناميا على الأمن القومي للدول. وتعتبر ليبيا من بين هذه الدول التي مسها خطر التهديدات السيبرانية، وأثر بشكل مباشر على أمنها القومي؛ بل وتعدى هذا الخطر إلى أبعد من ذلك، حيث كما أوضحنا في دراستنا هذه كيف أثرت الهجمات السيبرانية على المؤسسات داخل الدولة في ليبيا، وحجم الخسائر التي تعرضت لها هذه المؤسسات، فالهجمات السيبرانية أصبحت ليست مجرد اعتداءات تقنية؛ بل هي تهديدات ذات آثار عميقة تمتد إلى جوانب اقتصادية، واجتماعية وسياسية، كما أوضحنا. ومن خلال تحليل أنماط التهديدات السيبرانية وأهدافها، أصبح من الواضح أن هذه التهديدات تتطلب استراتيجيات متعددة الأبعاد للتصدي لها، وبات من الضروري على ليبيا تطوير أمنها السيبراني للتصدي لهذه التهديدات، وإيجاد استراتيجيات وحلول لمثل هذه المشاكل.

ويمكن تحديد أبرز النتائج التي توصلت إليها الدراسة في النقاط التالية:

المجلد الثالث
العدد السادس
سبتمبر 2025

مجلة جامعة درنة للعلوم الإنسانية والاجتماعية
DERNA UNIVERSITY JOURNAL OF HUMANITIES AND SOCIAL SCIENCES
Available online at https://dujhss.uod.edu.ly/
P-ISSN: 2959-6475 E-ISSN: 2959-6483 Impact Factor: 0.82

1_ خلصت الدراسة على التشديد بأهمية الأمن السيبراني واعتباره عنصراً مهماً للدولة، لمواجهة التهديدات السيبرانية التي تعتبر مصدر تهديد مباشر للأمن القومي للدولة، لدى وجب على الدولة تعريف مواطنيها بأهمية الأمن السيبراني .

2_ أوضحت الدراسة التهديدات التي تعرضت لها الدولة الليبية، ومنها الهجوم السيبراني التي تعرض له مصرف ليبيا المركزي، والشركة الليبية للاتصالات والتقنية، كذلك المؤسسة الوطنية للنفط.

3_ كانت لهده الهجمات تداعيات كبيرة على الدولة الليبية سواء كانت من الناحية السياسية أو الاقتصادية أو من الناحية الاجتماعية، حيث أترت سلبا على عمل مؤسسات الدولة وتعرضها لخسائر كبيرة.

4_ امتدت تداعيات التهديدات السيبرانية التي تعرضت لها الدولة الليبية، لتشمل أيضاً التأتير على الأفراد عن طريق توجيه الرأي العام ، وهذا بدوره يؤثر على استقرار الأمن في ليبيا، وبتالي ينعكس سلباً على أمنها القومي.

5_كما أوضحت الدراسة الجهود التي قامت بها ليبيا في مواجهة التهديدات السيبرانية، سواء كانت عن طريق سن القوانين الخاصة بالأمن السيبراني ، أو عن طريق عقد الاتفاقيات التي عقدتها الدولة الليبية مع غيرها من الدول لمواجهة هده التهديدات ، كذلك عن طريق تثقيف المواطنين بأهمية الأمن السيبراني ، وذلك عن طريق عقد الندوات والمؤتمرات المتعلقة بالأمن السيبراني.

التوصيات.

1_ يجب نشر الوعي داخل المجتمع الليبي بمفهوم الأمن السيبراني، وذلك من خلال التوعية بين مستعملي شبكات الإنترنيت، لاتخاذ التدابير اللازمة للحد من الخطر والتهديدات السيبرانية.

2_ تنظيم مؤتمرات علمية وندوات دولية بمشاركة ليبيا، حول خطر التهديدات السيبرانية وطرق التصدي لها.

3_ زيادة إصدار قوانين خاصة بالأمن السيبراني من مجلس النواب الليبي، يوضح في هده القوانين صور الجرائم السيبرانية والعقوبة المترتبة لفاعليها أو المشاركة في مثل هده الأعمال التي تؤثر على الأمن القومي الليبي.

4_ وضع خطط واستراتيجيات محكمة للتصدي لمثل هده التهديدات، والانضمام إلى اتفاقيات عربية ودولية، وذلك من أجل المواجهة المشتركة لهذه التهديدات.

المجلد الثالث
العدد السادس
سبتمبر 2025

مجلة جامعة درنة للعلوم الإنسانية والاجتماعية
DERNA UNIVERSITY JOURNAL OF HUMANITIES AND SOCIAL SCIENCES
Available online at https://dujhss.uod.edu.ly/
P-ISSN: 2959-6475 E-ISSN: 2959-6483 Impact Factor: 0.82

المراجع

اولا : المراجع باللغة العربية.

(أ) _ الكتب

1. آل مواش، ضرغام جابر، 2017، جريمة التجسس المعلوماتي: دراسة مقارنة، ط1، المركز العربي للنشروالتوزيع، القاهرة.
2. العمري، محمد محمود، 2020، مدخل إلى الأمن السيبراني، ط1، دار زهران للنشر والتوزيع، الاردن.
3. العوادي، أوس غالب،2106، الأمن المعلوماتي السيبراني، مركز البيان للدراسات والتخطيط، لبنان.
4. جبور، منى الأشقر، 2018، البيانات الشخصية والقوانين العربية الهم الأمني وحقوق الأفراد، ط1، المركز العربي للبحوث القانونية والقضائية، لبنان.
5. كمال، محمد مصطفي، 2022،الإرهاب السيبراني، ط1، دار كليم للطباعة والنشر والتوزيع، مصر.
6. قبلان، مروان،2023، الأمن القومي العربي وتحديات الأمن الإقليمي، ط1، المركز العربي للأبحاث ودراسة السياسات، لبنان.
7. منصور، شادي عبد الوهاب، 2019، حروب الجيل الخامس، ط1، دار العربي للنشر والتوزيع، الاردن.

(ب) _ الدوريات العلمية والمجلات والصحف.

1. السمحان، منى عبدالله، 2020، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية جامعة المنصورة، العدد 111، مصر، ص 4_27.
2. الفيتوري، علي، تتابع أعمال مؤتمر ليبيا الدولي للأمن السيبراني تحت شعار "الأمن القومي والتهديدات السيبرانية في عالم متغير"، الموقف الليبي، بنغازي، يناير 2023.
3. المرصد، ليبيا، 2023، ممارسة الحقوق الدستورية في ظل قانون مكافحة الجرائم الإلكترونية، صحيفة المرصد الليبية ، تم النشر 30_8_2023.
4. باره، سمير،2017، الأمن السيبراني في الجزائر: دراسة في الدوافع والتحديات، المجلة الجزائرية للأمن الإنساني، المجلد 2، العدد 2، الجزائر، ص243-268.

المجلد الثالث
العدد السادس
سبتمبر 2025

مجلة جامعة درنة للعلوم الإنسانية والاجتماعية
DERNA UNIVERSITY JOURNAL OF HUMANITIES AND SOCIAL SCIENCES
Available online at https://dujhss.uod.edu.ly/
P-ISSN: 2959-6475 E-ISSN: 2959-6483 Impact Factor: 0.82

5. سالم، ماجد صدام،2022، الأمن السيبراني العراقي وأثره على قوة الدولة، مجلة العلوم الأساسية قسم الجغرافيا، العدد18، العراق، ص70_90.
6. شلوش، نورة، 2018، القرصنة الإلكترونية في الفضاء السيبراني "التهديد المتصاعد لأمن الدول"، مجلة مركز بابل للدراسات الإنسانية، المجلد8، العدد 2، العراق، ص9_37.
7. شعيتير، جازية،2023، السيبرانية على قائمة أولويات الأمن القومي، جريدة بوابة الوسط، 2فيبراير 2023،طرابلس_ ليبيا .
8. عبد الصادق، عادل، *2016*،أسلحة الفضاء الإلكتروني في ضوء القانون الدولي، مجلة مكتبة جامعة الإسكندرية، العدد*23*، ص *60*_88.
9. قانون مكافحة الجرائم الإلكترونية الليبي الجديد، مجلس النواب الليبي يقر قانون مكافحة الجرائم الإلكترونية بعد إقرار مشروع قانون المعاملات الإلكترونية، مجلس النواب الليبي،26 أكتوبر 2012.
10. مختار، محمد،2015 ،هل يمكن للدولة أن تتجنب مخاطر الهجمات السيبرانية، مجلة إتجاهات الأحداث، العدد6، أبوظبي، ص3_32.
11. ما نيطه، يوسف أسماعيل،2017، نظرة عامة على الجريمة الإلكترونية في الفضاء السيبراني، المجلة الليبية العالمية،العدد32، ليبيا، ص4_9.

ثانيا: المراجع باللغة الأجنبية.

1. *Craiyen , dan, October 2014, "Defining cybersecurity", Technology innovation management review, Montreal, Canada .*
2. *Craigen,D, Diakun-Thibault, N., & Purse, R. (2014, October).Defining cybersecurity. Technology Innovation Management Review, 4(10), 13–21. https://doi.org/10.22215/timreview/835*