رسالة ماجستير بعنوان:

التهديدات السيبرانية وتداعياتها على الأمن القومي (دراسة حالة ليبيا 2011-2024)

إعداد :أسراء الأحول

منشورات البرنامج الوطني لتطوير المجلات العلمية

دولة ليبيا

وزارة التعليـم العالـي والبحـث العلمـي

الأكـاديميـة الليبية للدراسـات العليـا

مدرسة الدراسات الاستراتيجية والدولية

قسم الدّراسات الإقليمية والدّولية

التهديدات السيبرانية وتداعياتها على الأمن القومي (دراسة حالة ليبيا 2011-2024)

إعداد الباحثة:

أسراء علي أبوعجيلة الأحول

رقم القيد:21981065

إشراف :

أ . د منصور فرج الشكري

دراسة مقدّمة استكمالاً لمتطلبات الحصول على درجة الإجازة العالية "الماجستير"

في الدراسات الإقليمية والدولية

الفصل الدراسي: ربيع - 2025م

وزارة التعليم العالي والبحث العلمي
الأكاديمية الليبية للدراسات العليا
مدرسة الدراسات الاستراتيجية والدولية
قسم :الدراسات الإقليمية والدولية
شعبة :الدراسات الأمريكية

(قرار المناقشة النهائي)
(التجليد)

لجنة المناقشة للطالبة/ إسراء أبوعجيلة الأحول
للحصول على درجة الإجازة العالية في الدراسات الإقليمية والدولية

قامت اللجنة المشكلة بقرار السيد وكيل الأكاديمية للشؤون العلمية رقم (32) الصادر بتاريخ 2025/02/25م بمناقشة الرسالة المقدمة من الطالبة / إسراء أبوعجيلة الأحول رقم القيد: 21981065 ، لنيل درجة الإجازة العالية (الماجستير) في قسم الدراسات الإقليمية والدولية. وعنوانها:

((التهديدات السيرانية وتداعياتها على الأمن القومي "دراسة حالة ليبيا 2011-2024"))

وبعد مناقشة الرسالة علنيًا على تمام الساعة الحادية عشر صباحا يوم الثلاثاء الموافق8//2025/04 م، بالأكاديمية وتقويم مستوى الرسالة العلمي والمنهج الذي اتبعته الطالبة في بحثها قررت اللجنة ما يلي: قبول الرسالة ومنح الطالبة / إسراء أبوعجيلة الأحول . درجة الإجازة العالية (الماجستير) في قسم الدراسات الإقليمية والدولية .

أعضاء لجنة المناقشة :		التوقيع	التاريخ
1. أ. د. منصور فرج الشكري	"مشرف"		2025/4/22
2 .أ. د. سليمان ساسى الشحومي	"ممتحن خارجي – متقاعد "		2025/4/28
3. .د. وجدى محمد بقبق	" ممتحن داخلي – الاكاديمية الليبية "		2025/4/28

بعتمد

د. محمد عاشور عيواز
وكيل الأكاديمية للشؤون العلمية

التوقيع:

التاريخ:

أ.د.عارف أحمد الير
عميد مدرسة الدراسات الإستراتيجية والدولية

﴿يَرْفَعِ اللَّـهُ الَّذِينَ آمَنُوا مِنكُمْ وَالَّذِينَ أُوتُوا الْعِلْمَ دَرَجَاتٍ
وَاللَّـهُ خَبِيرٌ بِمَا تَعْمَلُونَ﴾

سورة المجادلة {الآية- 11}

الإهداء

الحمد لله رب العالمين، والصلاة والسلام على سيدنا محمد وعلى آله وصحبه أجمعين.
ما سلكنا البدايات إلا بتيسيره، وما بلغنا النهيات إلا بتوفيقة، وما حققنا الغايات إلا بفضله ..
فالحمد لله.. حباً وشكراً وامتناناً.. الحمد لله على البدء والختام.

في أعماق هذه الرسالة، تكمن قصص حياة، وأحلام تحولت إلى واقع، وعلاقات نُسجت بخيوط من الطموح والإصرار.
فكل حرف فيها.. يحمل في طياته جزءاً من روحي.. وكل سطر يعكس ساعات من التمعن والتفكر
هذا العمل ليس مجرد دراسة أكاديمية، بل هو شهادة على شغفي بالمعرفة، وعلى حبي للتنقيب في أعماق القضايا.

أهدي هذه الرسالة إلى روح والدي الحبيب، الذي كان رمزاً للتضحية والعطاء.. رحل عنا جسداً ولكنه ترك في قلوبنا إرثاً من القيم والمبادئ.. التي ستظل حية في كل خطوة أخطوها.
وإلى أخي الشهيد الذي ضحى بحياته في سبيل الوطن، أكرس هذه الصفحات التي تحمل بصمات حبه وعزيمته وشجاعته، رحمكم الله وأسكنكم فسيح جناته.

إلى والدتي العظيمة، وحبيبة قلبي الأولى ..التي تضئ ظلمات الحياة، والتي تبقى مصدراً للقوة والإلهام..
فهي التي علمتني أن الصمود في وجه الصعاب هو السبيل الوحيد للنجاح..
إليكي أهدي حبي وقلمي ورسالتي وجهدي .

إلى جدتي النبع الذي ارتويت منه حروف هذه الرسالة.. التي كانت دائما تزرع في نفسي الأمل والإصرار.

إلى أخواني الأعزاء: إيمان، وإبتهال، ومحمد، وأحمد، ونوري، ومودة، ومالك، أنتم الأوتار التي تعزف لحن حياتي.. وأشكركم جميعاً على الدعم والحب الذي منحتموني إياه.. أنتم السبب في كل ما وصلت إلية، وملاذي في كل زمان ومكان.

إلى أرواح شهداء مدينة العجيلات الذين رسموا بدمائهم طريق الحرية، وإلى كل من حمل راية النضال من أجل وطننا الحبيب" **ليبيا** " .

إلى أميرة السلام، المرأه الحديدية ونموذج للمرأة القوية عائشة معمر القدافي، التي ألهمتني منذ قراءتي لكلماتها عام 2011 وبعثت فيّ الشغف الذي أوصلني لما أنا عليه اليوم.

أهدي هذا العمل إلى كل من دعمني، ووقف بجانبي في الأوقات الصعبة، إلى كل من شجعني ولو بكلمة طيبة أو دعاء صادق.. أنتم النور الذي أضاء طريقي، والأمل الذي دفعني للاستمرار.
إلى كل من جعل من هذا الإنجاز ممكنًا، أهديكم هذا العمل بكل امتنان.

وأخيراً، إلى نفسي الطموحة التي لم تتخل عن أحلامها رغم كل شيء.. التي كانت اهلاً للمصاعب..
ها أنا اختم كل ما مررت به بفخر وعزيمة.

الباحثة: أسراء

الشكر والعرفان

من صفحات التاريخ، استلهمت الشغف وعبر ضفاف المعرفة، بنيت هذا العمل الذي أعتز به.
أوجه خالص الشكر لكل من غرس في قلبي حب المعرفة، وإلى من شجعني على مواصلة السير نحو النجاح.
إلى من كان لهم الفضل في توجيهي ودعمي، أرفع قلمي وأهدي كلماتي إلى البروفيسور منصور الشكري، الذي أضاء لي دروب المعرفة بحكمته وإلهامه.

إلى رئيس الأكاديمية الليبية للدراسات العليا الدكتور رمضان المدني وعميد مدرسة الدراسات الاستراتيجية والدولية الدكتور العارف التير، وكل أعضاء هيئة التدريس في قسم الدراسات الإقليمية والدولية وبالأخص الدكتور كمال الشكري، أقدم لكم خالص الشكر على كل ما بذلتموه من جهد في سبيل تعزيز مسيرتنا الأكاديمية.. إن تفانيكم وإخلاصكم كانا مصدر إلهام لنا جميعاً.

ولا يسعني إلا أن أخص بالشكر صديقتي ورفيقة دربي، الباحثة مودة البكوش، التي كانت دائمًا إلى جانبي، تقدم لي الدعم والتشجيع، إن صداقتنا هي مصدر قوة لي، وأقدر كل لحظة قضيناها معًا في سبيل تحقيق أهدافنا، والشكر لكل زملائي وأصدقائي بالأكاديمية الليبية للدراسات العليا.

كما أوجه جزيل الشكر لكل الأشخاص الذين قابلتهم من مختلف المؤسسات في الدولة، لقد كانت تجاربكم الغنية ومساهماتكم الفعالة جزءًا لا يتجزأ من رحلتي.

وأخص بالشكر المؤسسة الليبية للتقنية، شركة اليمامة، شركة الجذور الليبية، شركة الاتحاد الدولي للخدمات المالية والإلكترونية، شركة عبور للتقنية، شركة الدليل الرقمي، شركة البركة للتأمين، شركة العنكبوت الليبي، الذين كان لهم دور بارز في تقديم الدعم والمساندة، إن التزامهم بتطوير المجتمع ودعم البحث العلمي يستحق كل التقدير والاحترام.

أشكر كل من ساهم في بناء مجتمع يسعى نحو المعرفة والتقدم ، ولكل من يؤمن بأهمية التعليم.

الباحثة

فهرس المحتويات

الفصل الثاني: التهديدات السيبرانية للأمن القومي : التداعيات وسبل المواجهة

قائمة الجداول

قائمة الأشكال

قائمة الاختصارات

الإختصار	الإسم
(CSIRTs)	Computer Security Incident Response Teams فرق الاستجابة لحوادث الأمن الحاسوبي
(CIRTs)	Computer Incident Response Teams فرق الاستجابة للحوادث الحاسوبية
(ICT)	Information and Communications Technology أمن المعلومات والاتصالات
(GOAT)	Global Online Assessment Tool أداة تقييم بناء القدرات
(NCAF)	National Cybersecurity Assessment Framework إطار تقييم القدرات الوطنية
(SCADA)	Supervisory Control and Data Acquisition أنظمة التحكم الإشرافي واكتساب البيانات
(OASIS CTI TC)	OASIS Cyber Threat Intelligence Technical Committee اللجنة الفنية لاستخبارات التهديدات السيبرانية
(ASPI)	Australian Strategic Policy Institute المعهد الأسترالي للسياسات الاستراتيجية
(NISSA)	National Information Security and Safety Authority الهيئة العامة لأمن وسلامة المعلومات
(LPTIC)	Telecommunication and Information Technology ،Libyan Post Company الشركة الليبية للبريد والاتصالات وتقنية المعلومات القابضة
(NIST)	National Institute of Standards and Technology المعهد القومي الأمريكي للمعايير القياسية والتكنولوجية
(CRI)	Cyber Readiness Index الرقم القياسي للتأهب السيبراني
(GCSCC)	Global Cyber Security Capacity Centre المركز العالمي لقدرات الأمن السيبراني
(CIS)	Critical Infrastructure Security البنى التحتية الحرجة
(Clls)	Critical Information Infrastructure البنى التحتية للمعلومات الحرجة
(HIPAA)	Health Insurance Portability and Accountability Act القانون الصحي المحمي للتأمين المحمي
(ITU)	International Telecommunication Union الاتحاد الدولي للاتصالات
(NII)	National Information Infrastructure البنية التحتية الوطنية للمعلومات
(NISS)	National Information Security Strategy الاستراتيجية الوطنية لأمن المعلومات
(NCA)	National Cybersecurity Authority الهيئة الوطنية للأمن السيبراني في السعودية
(IEC)	International Electrotechnical Commission اللجنة الكهرتقنية الدولية
(MitM)	Man-in-the-Middle رجل في الوسيط
(GCI)	Global Cybersecurity Index

	مؤشر الأمن السيبراني العالمي
(FBI)	Federal Bureau of Investigation مكتب التحقيقات الفدرالي الأمريكي
(CCDCOE)	Cooperative Cyber Defence Centre of Excellence مركز التميز في الدفاع السيبراني التعاوني
(WEF)	World Economic Forum منتدى الاقتصاد العالمي
(SOC)	Security Operations Center مراكز متخصصة لرصد الشبكات السيبرانية
(ISMS)	Information Security Management System معيار إدارة أمان المعلومات
(GDPR)	General Data Protection Regulation لائحة حماية البيانات العامة
(MCIT)	Ministry of Communications and Information Technology وزارة الاتصالات وتقنية المعلومات
(NPS)	Naval Postgraduate School كلية الدراسات العليا البحرية الأمريكية
(DDoS)	Distributed Denial of Service هجمات الحرمان من الخدمة
(WEF)	World economic forum المنتدى الاقتصادي العالمي
(FIRST)	Forum of Incident Response and Security Teams منتدى فرق الاستجابة للحوادث وأمن البيانات
(CERT/CC)	Computer Emergency Response Team Coordination Center مركز تنسيق الاستجابة لطوارئ الحاسب الآلي
(ICANN)	Internet Corporation for Assigned Names and Numbers مؤسسة الإنترنت للأسماء والأرقام المخصصة
(CMM)	Cybersecurity Maturity Model نضج القدرات السيبرانية
(NPS)	Naval Postgraduate School كلية الدراسات العليا البحرية الأمريكية
(DDoS)	Distributed denial-of-Service Attacks هجمات الحرمان الخدمة
(CIS)	Center for internet securty مركز أمن الإنترنت
(LITC)	Libya international Telecom Company شركة الاتصالات الدولية الليبية

المـلـخـص

هدفت هذه الدراسة إلى تعريف وتحليل المفاهيم الأساسية المتعلقة بمفهوم التهديدات السيبرانية وتحليل أنواعها وأدواتها، والتعرف على الجهود الدولية المبذولة للتعامل مع هذه التهديدات، ومدى استفادة ليبيا منها، والتعرف على الأليات والسياسات والتشريعات التي يمكن تفعيلها من قبل صناع القرار في الدولة، لتحقيق الأمن السيبراني الليبي، وإرشاد الحكومة الليبية نحو تعزيز التعاون الإقليمي والدولي في مجال الأمن السيبراني، كما سعت إلى اقتراح إطار عمل شامل لاستراتيجية وطنية للأمن السيبراني في ليبيا، قادرة على مواجهة هذه التحديات المتصاعدة.

استندت الدراسة إلى منهجية بحثية متكاملة، باستخدام المنهج الوصفي التحليلي، ومنهج دراسة الحالة، وأيضا المنهج الاستقرائي، وشملت تحليلًا معمقًا للبيانات باستخدمت أدوات جمع البيانات كالمقابلات، مع عينة الدراسة وهم المدراء في مجال الأمن السيبراني وأمن المعلومات والاتصالات في المؤسسات الحكومية والخاصة في ليبيا، ولتحليل البيانات التي جمعت تم استخدام تحليل MaxqudA، وقد خلصت الدراسة إلى مجموعة من النتائج أهمها، أن الأمن السيبراني ليس مجرد تحدٍ تقني، بل هو قضية تتطلب تعاونًا متعدد الأوجه بين الحكومات والقطاع الخاص والمجتمع المدني، و أنه على الرغم من الجهود المبذولة، لا يوجد إطار دولي شامل يعالج التهديدات السيبرانية، فالتحليلات تشير إلى أن التأثيرات الناتجة عن التهديدات السيبرانية تختلف بناءً على الهدف المحدد وقد كشفت النتائج غياب استراتيجية وطنية شاملة لمعالجة هذه المشكلة، علاوة على ذلك، توصلت النتائج إلى أن تحسين الأمن السيبراني يعد جزءًا أساسيًا من تعزيز الاستقرار الوطني والتنمية الاقتصادية والاجتماعية في ليبيا، بناءً على هذه النتائج، اقترحت الدراسة مجموعة من التوصيات أبرزها دعوة الحكومة الليبية إلى تنفيذ مقترح الأستراتيجية الوطنية للأمن السيبراني.

Cyber Threats and Their Repercussions on National Security

(A Case Study of Libya 2011-2024)

By

Asraa Ali Aboujaylah Alahwal

Supervisor

Prof. Mansour F. Alshoukry

Abstract

The aim of this study was to define and analyze the fundamental concepts related to the notion of cyber threats، analyzing their types and tools، identifying the international efforts made to address these threats، assess Libya's utilization of them، recognize the mechanisms، policies، and legislations that can be activated by decision-makers in the country to achieve Libyan cybersecurity، guide the Libyan government towards enhancing regional and international cooperation in the field of cybersecurity، It also sought to propose a comprehensive framework for a national cybersecurity strategy in Libya capable of confronting these escalating challenges.

The study was conducted by using an integrated research methodology، employing descriptive-analytical، case study، and inductive approaches. It included an in-depth analysis of data using data collection tools such as interviews with experts in the field of cybersecurity، information security، and communications in governmental and private institutions in Libya. Data analysis was conducted by using MaxqudA analysis. The study revealed a number of key findings، including that the cybersecurity is not merely a technical challenge but rather an issue that necessitates multidimensional cooperation between governments، the private sector، and civil society. Despite efforts، there is a lack of a the remarkable comprehensive international framework addressing cyber threats.

The results indicated variations in the impacts of cybersecurity threats depending on the specific target. Furthermore، the study highlighted the absence of a comprehensive national strategy to address this issue. Additionally، the results emphasized that enhancing cybersecurity is an essential component of strengthening national stability، economic development، and social progress in Libya. Based on these findings، the study proposed several recommendations، notably urging the Libyan government to implement the proposed national cybersecurity strategy.

مـقدّمـــة

في عالم اليوم، باتت التقنية الرقمية تدخل جميع مناحي الحياة، بتحول الفضاء الإلكتروني إلى ساحة جديدة للصراع والتنافس، بين الدول والفاعلين في المجتمع الدولي، ونظرا لكونه مجالاً افتراضيًا، على عكس المجالات التقليدية المتعارف عليها (البرية، والبحرية، والجوية)، فقد جعل هذا التطور الخطير الصراعات والحروب لا تخوضها الدول بالدبابات والطائرات فحسب، بل امتدت إلى أبعاد جديدة، تمثلت في ظهور تهديدات سيبرانية معقدة تستهدف البنى التحتية الحيوية، والاقتصادات الوطنية، حتى الديمقراطيات وأنظمة الحكم، لم تتوقف عند كونها مجرد تحديات تقنية، بل تطورت لتشكل تهديداً وجودياً للأمن القومي للدول.

أدت هذه التطورات إلى ظهور تحديات جديدة تتعلق بالتهديدات السيبرانية، التي تشكل بأنواعها وآثارها المتزايدة، تهديداً وجوديًا للعديد من الدول، في هذا العصر الرقمي، ولا نستثنى ليبيا من هذه الحقيقة الواقعة، فهي تتعرض لتهديدات متكررة تستهدف بنيتها التحتية الحيوية ومؤسساتها الحكومية والقطاع الخاص وقلب أنظمة المعلومات لديها، مما استدعى الحاجة إلى دراسة تأثيراتها. لذا فإنَّ هذه الدراسة تسلط الضوء على هذه التهديدات وتداعياتها على الأمن القومي في ليبيا، خلال الفترة من 2011 إلى 2024م، حيث تتعرض ليبيا إلى تهديدات سيبرانية خطيرة، معرضة البلاد لمخاطر جسيمة تؤثر على استقرارها وأمنها؛ فليبيا كغيرها من الدول تواجه تحديات سيبرانية كثيرة تودي هذه التهديدات إلى خسائر اقتصادية فادحة، وإلى تعطيل الخدمات الأساسية وتقويض الثقة في المؤسسات الحكومية.

فقد شهدت ليبيا تغيرات جذرية في الهيكل السياسي منذ بدء احداث عام 2011م، وهو ما شكل وضعا أمنيًا هشًا، ووضع تحديات أمام الحكومات الليبية، وأسهمت النزاعات السياسية والاجتماعية في تفاقم الوضع الأمني، مما جعل البلاد هدفًا للعديد من التهديدات السيبرانية. من هنا، تبرز أهمية اختيار هذه الدراسة، نظرًا لتزايد التهديدات السيبرانية وتطور أساليبها، مما يجعل من الضروري فهم هذه التهديدات وتداعياتها بشكل عميق، كما أن هذا الموضوع يكتسب أهمية خاصة في ظل التغيرات الجيوسياسية المتسارعة، حيث تستخدم الدول والفواعل غير الدولية التهديدات السيبرانية كأداة لتحقيق أهدافها، مما يستدعي ضرورة البحث عن حلول فعالة لتعزيز الأمن السيبراني في ليبيا.

لذلك فقد أصبح الأمن السيبراني، في عالم اليوم، أكثر من كونه مسألة مرتبطة بأمن المعلومات والتقنيات وشبكات الحاسوب، بحكم علاقاتها المباشرة بالمجال السياسي والأمني والاقتصادي والاجتماعي والثقافي، وحيث أنَّ معظم مؤسسات الدولة باتت تعتمد على أنظمة الاتصالات والمعلومات، فقد أصبح تحقيق الأمن السيبراني من أهم مجالات الأمن في القرن الحادي والعشرين، وعلى هذا النحو يمكن اعتبار التحديات على المستوى السيبراني أعلى تحديات الأمن القومي، خاصة مع كثرة الهجمات والاختراقات الإلكترونية.

1. إشكالية الدراسة

تتعرض معظم الدول لتهديدات خطيرة، وجديدة، لها علاقة مباشرة بتطور التقنيات الرقمية، وتقنية المعلومات؛ فيما يُعرف بالتهديدات السيبرانية، التي باتت تهدد مختلف مؤسسات الدول، وتنذر بعرقلتها أو تدميرها، تتزايد هذه التهديدات بسرعة ملحوظة، مما يجعل مواجهتها والتنبؤ بتطوراتها، أمرًا معقدًا ومكلفا، بسبب تعددها وتنوعها وآثارها المدمرة على الأمن القومي، من هذا المنطلق سيتم طرح الإشكالية التالية:

س1. ما مدى تداعيات التهديدات السيبرانية على الأمن القوي للدول؟ وإلى أي مدى يمكن أن تكون هذه التهديدات خطيرة على ليبيا؟

وقد تم تجزئية الإشكالية المذكورة إلى مجموعة من الأسئلة الفرعية وهي:

- ما الأنواع الرئيسية للتهديدات السيبرانية؟ وما الأدوات المستخدمة في تنفيذها؟
- ما التداعيات المترتبة على الأمن القومي للدول التي تعرضت لتهديدات سيبرانية، وكيف يمكن أن تستفيد ليبيا من تجارب تلك الدول؟
- ما هي التهديدات السيبرانية التي تتعرض لها ليبيا ؟ و ما هي الاستراتيجيات والسياسات التي تعتمدها في مواجهة هذه التهديدات ؟

2. أهمية الدراسة

تتمثل أهمية الدراسة في جانبين، علمي وعملي:

الأهمية العلمية:

- الإسهام في الدفع نحو توجهات جديدة لصانعي القرار في الدولة؛ لاتخاذ سياسات وإجراءات وقائية لحماية البنية التحتية الرقمية من التهديدات السيبرانية.
- المشاركة في زيادة المعرفة العلمية التي ستمكن بدورها من توفير رؤى جديدة وملاحظات قيمة تعزز المعرفة في هذا المجال، تكون إضافة علمية، يستفيد منها الطلاب، والمهتمون، والأكاديميون.
- الإسهام في إثراء المكتبة العربية، والليبية خاصة بمرجع جديد، إذ يعتبر هذا الموضوع من الدراسات الحديثة.

الأهمية العملية :

- تكمن هذه الدراسة في أنها تعمل على توجيه الاهتمام نحو أهمية الأمن السيبراني؛ لتساعد على بناء خبرات ومهارات في المجال الأكاديمي والمهني، والقدرة على التحليل والبحث في الدراسات السيبرانية مستقبلاً.
- تسليط الضوء على التحديات التي تواجه ليبيا للتعامل مع التهديدات السيبرانية، وتقديم حلول عملية؛ لتعزيز الأمن السيبراني ، وتحسين السياسات، والإجراءات، والمبادرات في هذا المجال.
- فهم مدى خطورة التهديدات السيبرانية التي يمكن ان تؤدي إلى تعطيل البنية التحتية الحيوية، والخدمات الحكومية، والتعرف على السبل الصحيحة لمواجهتها.

3. أهداف الدراسة

تتمثل أهداف هذه الدراسة في النقاط التالية:

- تحليل طبيعة التهديدات السيبرانية التي واجهت ليبيا في الفترة الممتدة من 2011 إلى 2024م، وتقييم تداعيات هذه التهديدات على مختلف جوانب الأمن القومي الليبي.
- تعريف وتحليل المفاهيم الأساسية المتعلقة بمفهوم التهديدات السيبرانية.
- إقتراح توصيات عملية وواقعية لتعزيز أمن ليبيا الإلكتروني في مواجهة التهديدات السيبرانية.
- التعرف على الجهود المبذولة للتصدي للتهديدات السيبرانية العالمية وخاصة في ليبيا.
- الإسهام في تقديم مقترح حول إمكانية تحقيق استراتيجية وطنية للأمن السيبراني؛ للحفاظ على الأمن القومي الليبي، و الاستقرار الجيوسيبراني
- التعرف على الأليات والسياسات والتشريعات التي يمكن تفعيلها من قبل صناع القرار في الدولة؛ لتجسيد الأمن السيبراني الليبي .
- إرشاد الحكومة الليبية نحو تعزيز التعاون الإقليمي والدولي في مجال الأمن السيبراني.

4. فرضية الدراسة

تنطلق هذه الدراسة من فرضية أساسية مفادها أن:

التهديدات السيبرانية تمثل خطراً حقيقيا على الأمن القومي الذي يمثل الأساس لاستقرار الدولة وذلك من خلال استهدافها البنية التحتية الحيوية للدولة، فكلما اعتمدت الدولة على استراتيجية وطنية فعالة للأمن السيبراني، زادت إمكانية تقليل المخاطر الناتجة عن هذه التهديدات؛ بينما تكون النتائج كارثية كلما تباطأت الدولة في اتخاذ الإجراءات الضرورية للتصدي لتلك التهديدات.

5. مبررات اختيار الدراسة

قامت هذه الدراسة على مجوعة من المبررات منها:

- قلة الوعي بمخاطر الفضاء الإلكتروني حيث أنه لا يدرك العديد من الليبيين أهمية الأمن السيبراني، مما يجعلهم أكثر عرضة للاختراقات والتهديدات وأكثر تذمراً من الإنفاق علية.
- قلة الدراسات والأبحاث حول الأمن السيبراني في دولة ليبيا.
- الحاجة إلى تقييم شامل لطبيعة التهديدات السيبرانية، حيث إنه لم يتم نشر أي تقييم شامل لطبيعة هذه التهديدات من قبل الحكومة، وستساعد هذه الرسالة على فهم أفضل للتهديدات السيبرانية التي تواجهها دولة ليبيا.
- توافق الدراسة مع رؤية دولة ليبيا 2030، حيث إن دولة ليبيا تسعى إلى تحقيق هذه الرؤية، التي من أهدافها بناء مجتمع رقمي آمن.
- الاهتمام الشخصي بالموضوع، فالباحثة مهتمة بمجال الأمن السيبراني، وترغب بالمساهمة في تعزيزه بدولة ليبيا.

6. مناهج الدراسة

نظراً لطبيعة هذه الدراسة فإنها تعتمد المنهج الوصفي التحليلي؛ حيث تم توظيفه لتحليل ودراسة ماهية التهديدات السيبرانية ، وطبيعتها، وكيفية استخدامها أداة من أدوات التأثير على الأمن القومي وذلك بتفكيك الظاهرة إلى عواملها الأولية، وفي إطار التكامل المنهجي وللتحكم أكثر في متغيرات الدراسة تم الاستعانة بمنهج دراسة الحالة؛ للتعمق في الحالة الليبية وتوضيح مدى تداعيات التهديدات السيبرانية على أمنها القومي، وتمت الاستعانة أيضا بالمنهج الاستقرائي الذي يقوم على تقديم رؤية مستقبلية لوضع مقترح استراتيجية وطنية للأمن السيبراني في ليبيا؛ للتصدي للتهديدات السيبرانية وطرق الحماية منها.

7. أدوات جمع البيانات

تستخدم هذه الدراسة منهجية (كيفية) نوعية، حيث تم تجميع البيانات من مصادر عديدة كالتقارير والدوريات الأكاديمية، والكتب، والمؤتمرات والوثائق الحكومية، والإحصائيات والرسوم البيانية والدراسات السابقة، وتم الاستعانة بأداة سكوبوت(Schobot) للذكاء الاصطناعي لتنظيم وترتيب المحتوى العلمي الموثق والمترجم من المراجع، مما يعكس منهجية علمية دقيقة في معالجة البيانات، بالإضافة إلى ذلك تم أيضا استخدام مجموعة من الأدوات نظرا لطبيعة الدراسة وأهدافها، وتتمثل هذه الأدوات في الآتي:

أولاً: المقابلات المفتوحة(شبه المقننة) :

تم إجراء المقابلات الشخصية مع عينة الدراسة وهم مدراء إدارات أمن المعلومات والاتصالات والأمن السيبراني في ليبيا، وتم الحصول على النتائج باستخدام برامج تحليل البيانات النوعية (MaxQudA) لتوجيه الدراسة نحو فهم أفضل لمواقف وآراء المدراء حول تحليل الوضع الراهن لمخاطر التهديدات السيبرانية في ليبيا، وتحليل الاتجاهات والتحديات التي تواجههم، واستخلاص الأنماط والاتجاهات الرئيسية من مقابلاتهم للمساعدة في تقديم تحليلات موضوعية وعميقة تدعم الدراسة وتضيف قيمة للمجال، وشملت خمسة وثلاثون مقابلة وتم تقسيم المقابلات إلى مجموعتين المجموعة الأولى تحتوي على خمسة عشر سؤالاً موجهة للمؤسسات الحكومية أما المجموعة الثانية فهي تحتوي على ثمانية عشر سؤالاً موجهة للشركات الخاصة، سيتم عرضها في الملاحق، واستغرقت عملية اجراء المقابلات خمسة أشهر بداية من شهر 5 إلى 9 عام 2024م، وسيتم توضيح الجهات التي تم إجراء مقابلات معهم وذلك على النحو التالي:

1. **المؤسسات الحكومية:** منها الهيئة العامة للاتصالات والمعلوماتية، والهيئة العامة لأمن وسلامة المعلومات، والمفوضية الوطنية العليا للانتخابات، وديوان المحاسبة، وهيئة الرقابة الإدارية، ووزارة الخارجية والتعاون الدولي، ووزارة الداخلية، ووزارة الاقتصاد والتجارة، ووزارة التخطيط، ووزارة الحكم المحلي، ووزارة الصحة، ووزارة العدل، ووزارة المالية، ووزارة المواصلات، ووزارة التعليم العالي والبحث العلمي، ووزارة الشؤون الاجتماعية، ومصرف ليبيا المركزي، وشركة ليبيا للتأمين.

2. **شركات الاتصالات:** شركة المدار الجديد، والشركة الليبية للبريد والاتصالات وتقنية المعلومات القابضة(LPYIC)، وشركة ليبيانا للهاتف المحمول (Libyana) وشركة الاتصالات الدولية الليبية(LITC)، وشركة بريد ليبيا.
3. **القطاعات النفطية:** المؤسسة الوطنية للنفط، وشركة الواحة للنفط.
4. **الشركات الخاصة:** شركة الجذور الليبية لأمن المعلومات، والمؤسسة الليبية للتقنية، وشركة الاتحاد الدولي للخدمات المالية والإلكترونية، وشركة البركة للتأمين، وشركة الدليل الرقمي، وشركة العنكبوت الليبي، وشركة اليمامة، وشركة عبور لحلول أمن المعلومات.

ثانياً: اداة تحليل (PESTLE) :

هي أداة استراتيجية تستخدم لتقييم العوامل الخارجية، التي تؤثر على البيئة التنظيمية؛ حيث تعتبر هذه العوامل مهمة لفهم السياق الذي تعمل فيه الدولة، ولتوجية اتخاد القرارات الاستراتيجية، سيتم تطبيقها في وضع إطار مقترح لتطوير استراتيجية الأمن السيبراني في ليبيا من خلال الخطوات الآتية:

1. تحديد العوامل السياسية (Political): وذلك بتحليل الوضع السياسي والأمني وتقييم كيفية تأثيرها على البنية التحتية السيبرانية وتقنية المعلومات.
2. تحليل العوامل الاقتصادية (Economic): من خلال تحليل الوضع الاقتصادي والأثار المترتبة عليه؛ لتطبيق مقترح استراتيجية الأمن السيبراني في ليبيا، وتقييم تأثيرها على الاقتصاد المحلي.
3. تحليل العوامل الاجتماعية (Social): بدراسة عادات وثقافة المستخدمين، وكيفية تأثيرها على أمن المعلومات والسلوك السيبراني في ليبيا.
4. تحليل العوامل التقنية (Technological): وذلك بتقدير التكنولوجيا المستخدمة في مجال الأمن السيبراني في ليبيا، وكيفية تطورها وتأثيرها على مقترح الاستراتيجية .
5. تحليل العوامل القانونية (Legal): من خلال دراسة التشريعات واللوائح المتعلقة بالأمن السيبراني في ليبيا، وضبط الاستراتيجية وفقًا لهذه التشريعات.
6. تحليل العوامل البيئية (Environmental): من خلال تحديد التهديدات البيئية، والتغيرات في التكنولوجيا التي يجب مراقبتها.

وبعد إجراء هذه التحليلات المهمة، تم تحديد الفرص والتحديات، وضبط التوصيات لوضع مقترح الاستراتيجية الوطنية للأمن السيبراني.

خطوات تطبيق التحليل:

1. جمع البيانات والمعلومات من مصادر موثوقة حول كل عامل من العوامل المذكورة أعلاه.
2. تحليل البيانات لتحديد نقاط القوة والضعف والفرص والتهديدات المرتبطة بكل عامل.
3. تحليل النتائج وكتابة التوصيات التي تأخذ في الاعتبار جميع العوامل وتحقيق التوازن بينها لضمان تعزيز الأمن سيبراني في ليبيا.

ثالثاً: أداة التحليل الاستراتيجي (SWOT Analysis)

أداة التحليل الاستراتيجي SWOT Analysis تُعتبر واحدة من أفضل الأساليب التحليلية لتطوير الاستراتيجيات (سواء كانت قصيرة الأمد أو طويلة الأمد)، بهدف تحقيق الأهداف المنشودة، تعتمد هذه الأداة على تحليل الوضع الداخلي والخارجي للمنظمة من خلال النظر لأربعة جوانب رئيسية وهي نقاط القوة، ونقاط الضعف، والفرص، والتهديدات.

تم استخدام أداة SWOT Analysis في هذه الدراسة لتحليل الوضع القائم للأمن السيبراني في ليبيا من أجل وضع مقترح استراتيجية وطنية للأمن السيبراني، من خلال دراسة التفاعل بين العوامل الداخلية (نقاط القوة ونقاط الضعف)، والعوامل الخارجية (الفرص والتهديدات)، لتحديد الأسس والتوجهات الاستراتيجية التي ستضع الأمن السيبراني في الموقع المثالي لمواجهة التحديات السيبرانية.

خطوات تطبيق التحليل:

1. تحديد نقاط القوة (Strengthns): اكتشاف الجوانب الإيجابية لوضع الأمن السيبراني في ليبيا.
2. تحديد نقاط الضعف (Weaknesses): تحديد المجالات السلبية التي تحتاج إلى تطوير وتحسين لنجاح مقترح الاستراتيجية.
3. تحديد الفرص (Opportunities):اكتشاف الفرص الخارجية التي يمكن استغلالها لتحسين الأمن السيبراني .
4. تحديد التهديدات (Threats): تحديد التحديات الخارجية التي تشكل تهديداً لنجاح مقترح الاستراتيجية.
5. تقييم النتائج: تقييم العوامل الداخلية والخارجية، وتحليل كيفية تأثيرها على نجاح مقترح استراتيجية الأمن السيبراني في ليبيا.
6. وضع الاستراتيجيات: تحديد الإجراءات والتوصيات اللازمة بناءً على نتائج التحليل.

8. حدود الدراسة

في السعي لفهم طبيعة التهديدات السيبرانية وتأثيرها على الأمن القومي الليبي، ترسى الدراسة الحالية حدودها ضمن إطار زمني ومكاني وموضوعي محدد؛ لتحقيق الأهداف بدقة وفعالية.

الحدود الزمنية: تم تحديد الفترة الزمنية في الدراسة من سنة 2011 إلى 2024م نظرًا للأحداث المهمة التي شهدتها ليبيا خلال هذه الفترة، يعود اختيارهذه الفترة إلى تغيرات النظام والتوجهات السياسية والاجتماعية مما أدى إلى تصاعد التهديدات السيبرانية وتأثيرها على استقرار البلاد وأمنها القومي.

الحدود المكانية: سيتم تناول هذه الدراسة للتركيز على دولة ليبيا على أنها حالة دراسية محددة، وما قد يهدد الأمن القومي بها في الفضاء الإلكتروني.

الحدود الموضوعية: تركز الدراسة على فهم طبيعة التهديدات السيبرانية وتأثيرها على الأمن القومي ويتضمن التحليل تأثير التطورات التكنولوجية، والاضطرابات السياسية على الأمن السيبراني في ليبيا.

9. الدراسات السابقة

مع محدودية الدراسات والأبحاث العربية في مجال التهديدات السيبرانية وتداعياتها على الأمن القومي، استعانت الباحثة بعدة دراسات ذات العلاقة للتعمق في هذا الموضوع.

أولاً: الدراسات العربية :

1. **دراسة الدام محمد، "الأمن السيبراني" رسالة ماجستير منشورة، جامعة الشهيد حمه لخضر في الجزائر 2022م.** هدفت هذه الدراسة إلى تبيان مفهوم الأمن السيبراني وتحديد الجرائم السيبرانية التي تعتمد على تكنولوجيات المعلومات والاتصالات بمختلف تطبيقاتها، بالإضافة إلى تحديد بعض المفاهيم المتعلقة بالجرائم السيبرانية بعد تشخيص واقعها ورصد أبعادها ، كما سعت إلى معرفة كيفية تعامل الدول، وخاصة الجزائر، معها مع إبراز اهتمام المشرع الجزائري ومدى توفيره للإطار القانوني المناسب لمواكبة المتغيرات المتسارعة للثورة الرقمية، وتأهيل الموارد البشرية المتخصصة في هذا المجال.

واعتمدت الدراسة على المنهج الوصفي والمنهج التحليلي، وتوصلت الدراسة إلى مجموعة من النتائج أبرزها، تطور الأمن السيبراني يسير بالتوازي مع تطور أساليب وأشكال الجريمة السيبرانية، مما يستدعي تعزيز التدابير لمواجهة المخاطر ودعم البنية التحتية للدول والقطاع الخاص، وأن الأمن السيبراني أصبح جزءًا أساسيًا من أي سياسة أمنية وطنية، حيث يصنفه صناع القرار على أنه أولوية في سياساتهم الدفاعية، وأوضحت الدراسة أيضا أن الجرائم السيبرانية لها تأثير سلبي كبير على الحريات الفردية وحرمة الحياة الخاصة عند استخدام تكنولوجيا الإعلام والاتصال بشكل مخالف للقوانين والتشريعات، كما ذكرت محاولات المشرع الجزائري جاهداً مواكبة التطور المستمر للجرائم السيبرانية من خلال سن مجموعة من القوانين العامة والخاصة لحماية الحريات الفردية وحرمة الحياة الخاصة، وحماية المجتمعات من التهديدات والانتهاكات في الفضاء السيبراني.

تختلف هذه الدراسة عن الدراسة الحالية، في أنها تناولت الجرائم السيبرانية وآليات مكافحتها على الصعيد الدولي والجزائري بالتحديد، ووفقًا لبعض القوانين المحلية والمؤسسات المختصة بالأمن السيبراني في الجزائر، أما أوجه التشابه، فجاءت في التعريف النظري لمفهوم الجرائم السيبرانية التي تعتبر من أنواع التهديدات السيبرانية، وكذلك في تحليل مفهوم الأمن السيبراني من خلال نشأته وأبعاده، وأيضًا في ذكر بعض الجهود الدولية لمكافحة الجرائم السيبرانية على المستويين الإقليمي والدولي.

2. **دراسة نور الموصلي، "الهجمات السيبرانية في ضوء القانون الدولي الإنساني"،رسالة ماجستير منشورة، الجامعة الافتراضية السورية (سوريا) 2021.** هدفت هذه الدراسة إلى تقديم فهم شامل للهجمات السيبرانية وتوضيح معايير تحديد الأهداف العسكرية المشروعة أثناء هذه الهجمات، وأوضحت الدراسة أن استخدام الفضاء السيبراني في العمليات العسكرية، أحدث تحولًا جذريًا في قوانين النزاع

المسلح، واعتمدت الدراسة على المنهج الوصفي التحليلي، وخلصت إلى أن هناك جهودًا دولية لتنظيم الأنشطة السيبرانية، مثل اتفاقية بودابست، ودليل تالين، وقرارات الأمم المتحدة، كما أبرزت الدراسة الميزة النسبية للهجمات السيبرانية من حيث انخفاض تكاليفها وسهولة تنفيذها، وأشارت إلى أن الفضاء الإلكتروني أصبح مجالًا دوليًا جديدًا يمثل امتدادًا لنشاط الإنسان المدني والعسكري.

تأتي أوجه الاختلاف بين الدراسة الحالية ودراسة الباحثة في أن هذه الدراسة تتناول الهجمات السيبرانية والجهود الدولية من الجانب القانوني لتنظيمها، وهو ما يختلف عن الدراسة الحالية التي تركز على التهديدات السيبرانية للأمن القومي، وبخاصة في ليبيا على الإطار التنظيمي، ومع ذلك، تتفق الدراستان في النهج الإجرائي والنظري لتناول الموضوع السيبراني، وتسليط الضوء على بعض النماذج السيبرانية.

3. **دراسة أكرم رياض، "السياسات الدولية لمكافحة الإرهاب الإلكتروني السيبراني"، رسالة ماجستير منشورة، جامعة العربي بن مهيدي أم البواقي، كلية الحقوق والعلوم السياسية، الجزائر، 2021م.** تناولت هذه الدراسة تأثير الفضاء السيبراني على انتشار القوى بين مختلف الفاعلين، مما أتاح للفواعل من غير الدول، مساحة متزايدة للتأثير في التفاعلات الدولية، وأدى إلى تراجع سيادة الدولة المطلقة على إقليمها، واعتمدت الدراسة على المنهج الوصفي التحليلي والمنهج القانوني، وتوصلت إلى ضرورة بناء البنية التحتية العسكرية بتكليف عدد كبير من الأفراد العسكريين بمهمة مراقبة الواقع الافتراضي وضمانه، كما أوصت بدمج المؤسسات الأمنية للدولة مع بعض القطاعات الجديدة لتحقيق تبادل الخبرات والمعلومات، والاستفادة من المعلومات التي تمتلكها الأجهزة الأمنية المختلفة ضمن هيكل أمني مكرس للنشاط السيبراني، وأكدت الدراسة على أهمية تكوين نخب وطنية مختصة في مجال الأمن السيبراني، وإجراء مؤتمرات علمية يشارك فيها مختلف المختصين العالميين للاستفادة من خبراتهم، كما دعت إلى إقامة محتوى بديل لتوعية جميع فئات المجتمع ضد الأفكار الإرهابية الفوضوية الهدامة، وضرورة التعاون الإقليمي والعالمي في مجال الأمن السيبراني من خلال تبادل المعلومات والخبرات في ظل مبدأ المعاملة بالمثل، وأشارت إلى أهمية بناء استراتيجية مكافحة الإرهاب من خلال إيجاد تعاون وتوافق بين المعالجات الدولية والداخلية للإرهاب السيبراني.

تتفق دراسة أكرم مع الدراسة الحالية في تناول الإرهاب السيبراني، كونه من أهم أنواع التهديدات التي تم ذكرها في هذه الدراسة، وكذلك في تسليط الضوء على الجهود الدولية المبذولة لمواجهة هذا الإرهاب، ومع ذلك، تختلف الدراستان في أن دراسة أكرم ركزت على السياسات الدولية لمكافحة الإرهاب السيبراني بشكل عام، دون التركيز على دولة محددة، بينما تناولت الدراسة الحالية تداعيات التهديدات السيبرانية على الأمن القومي من خلال دراسة نماذج لدول محددة مع التركيز على دراسة حالة ليبيا.

4. **دراسة صلاح عبد الواحد، حروب الفضاء الإلكتروني؛ دراسة في مفهومها وخصائصها وسبل مواجهتها، رسالة ماجستير منشورة، جامعة الشرق الأوسط، كلية الآداب والعلوم، قسم العلوم السياسية،2021.** هدفت الدراسة إلى التعرف على ماهية حروب الفضاء الالكتروني، والتعرف على

الخصائص التي تتميز بها حروب الفضاء الالكتروني، والتعرف على السبل والإمكانيات المتاحة لمواجهتها، اعتمدت الدراسة على المنهج التاريخي والمنهج الوصفي التحليلي والمنهج المقارن والمنهج القانوني بالإضافة إلى منهج تحليل النظم.

توصلت الدراسة إلى مجموعة من الاستنتاجات أبرزها تزايد عدد الهجمات السيبرانية خلال العقدين الأخرين حتى باتت إحدى أهم الوسائل والتكتيكات المعتمدة بين الأطراف المتصارعة حول العالم، هناك تنوع في الأدوات والوسائل وأشكال الهجمات السيبرانية، وأيضا توصلت الدراسة إلى إن الهجمات السيبرانية عززت من مستويات وفرص الحرب اللامتماثلة، وذلك مع تمكن دول متفاوتة القوة، وحتى تنظيمات من غير الدول من شن الهجمات ضد الدول ذات القوة العسكرية والاقتصادية الأكبر، وأيضا إن التحدي الأكبر الذي يواجه التنظيم القانوني للهجمات في الفضاء الإلكتروني هو عدم وجود إدارة دولية على صعيد المفاوضات أو على صعيد قرار مجلس الأمن الدولي، واقترحت الدراسة مجموعة من التوصيات، ضرورة تطوير استراتيجيات جديدة في الدول العربية تتلاءم مع التحديات الأمنية المستجدة للعصر الرقمي بما يحمله من تغيرات في حسابات القوى والردع، وتطوير قدرات الدول العربية على إنتاج وتطوير أسلحة الكترونية تمكنها من تحقيق أهدافها في الفضاء الإلكتروني وأيضا تطوير برامج حماية الكترونية لمواجهة الهجمات الالكترونية، وإعادة النظر في القواعد القانونية الدولية التي تنظم هذا النوع من الحروب وضرورة بلورة توافق دولي بهذا الخصوص.

تتمثل أوجة الاختلاف بين دراسة صلاح والدراسة الحالية في إن دراسة صلاح ركزت بشكل أساسي على مفهوم حروب الفضاء الالكتروني وخصائصها وسبل مواجهتها، مع التركيز على الجوانب التقنية والقانونية الدولية، أما الدراسة الحالية تناولت التهديدات السيبرانية بشكل أوسع ولم تقتصر على الحرب السيبرانية وتناولت الجهود الدولية في مكافحة هذه التهديدات التي تتمثل في الاتفاقيات الدولية والإقليمية والمؤتمرات والاستراتيجيات والمعايير، أما أوجه التشابه فكلتا الدراستين تناول الحرب السيبرانية بوصفها تحدياً خطيراً يواجه الدول، وتم دراسة نماذج لهذة الحروب، وسلطت كلتا الدراستين الضوء على أهمية التعاون الدولي في مجال مكافحة هذه الحروب.

5. **دراسة فريدة طاجين، تأثير القوة السيبرانية على الاستراتيجيات الأمنية للدول الكبرى (دراسة حالة – الصين)، رسالة ماجستير منشورة، جامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية قسم العلوم السياسية(2018).** هدفت هذه الدراسة إلى التعرف على القوة السيبرانية من الناحية النظرية، والبحث عن الآثار التي خلفتها هذه القوة في الدول الكبرى، وبالتحديد في استراتيجياتها الأمنية، وذلك بالاستعانة بمناهج البحث العلمي التي تتمثل في، المنهج التاريخي والمنهج الاستنباطي ومنهج دراسة الحالة، وتوصلت الدراسة إلى مجموعة من النتائج، أبرزها أن الفضاء الإلكتروني يعد ساحة جديدة للصراع بشكله التقليدي لكنه ذا طابع سيبراني، وأنَّ كافة المؤشرات تؤكد على أن القوة الصينية في صعود مستمر، وأن التفوق الصيني السيبراني من الممكن أن يضاعف من قوتها.

وأوجه التوافق بين دراسة الباحثة وهذه الدراسة، هي التعرف على المفاهيم المرتبطة بالفضاء الإلكتروني من الناحية النظرية، وتناولت للفواعل الرئيسية التي تمتلك القوة السيبرانية في هذا الفضاء، ومع ذلك تختلف الدراستان في أن، دراسة طاجين ركزت على الاستراتيجية الأمنية الدولية والوطنية المتعلقة بالصين وبعض الدول الكبرى فقط من ناحية الاستراتيجيات، بينما ركزت الدراسة الحالية على مخاطر التهديدات السيبرانية على هذه الدول، وكذلك جهودها في مكافحة هذه التهديدات من خلال الاتفاقيات والمؤتمرات والاستراتيجيات مع تحديد حالة ليبيا.

6. **دراسة سليم دحماني، "أثر التهديدات السيبرانية على الأمن القومي: الولايات المتحدة نموذجًا (2001-2017)"، رسالة ماجستير منشورة، جامعة محمد بوضياف – المسيلة، كلية الحقوق والعلوم السياسية. قسم العلوم السياسية2017**. هدفت هذه الدراسة إلى إبراز وتوضيح المفاهيم الجديدة في الفضاء السيبراني، وتسليط الضوء على إسهامات الدول وجهودها، وخاصة الولايات المتحدة الأمريكية، في مواجهة التهديدات السيبرانية، واعتمدت الدراسة على مجموعة من المناهج العلمية، منها المنهج الوصفي، ودراسة الحالة، ومنهج تحليل المضمون، وخلصت الدراسة إلى أنه على الرغم من أن الولايات المتحدة تعد أقوى دولة سيبرانية، فإنها تواجه تهديدات سيبرانية حالية ومستقبلية، ومنافسات شديدة في الفضاء الإلكتروني، خاصة بين الصين وروسيا، مما قد يهدد أمنها القومي ودورها في الأمن العالمي، كما أن الولايات المتحدة تعمل من خلال وكالات وهيئات مختلفة على مواجهة تحديات الأمن السيبراني لضمان فضاء الكتروني آمن يساعد على التقدم والنمو.

تتفق دراسة دحماني مع الدراسة الحالية في تناول مدى مخاطر التهديدات السيبرانية على الأمن القومي للدول، وضرورة وجود رؤية استراتيجية للحماية، ومع ذلك، تختلف الدراستان في أن دراسة دحماني ركزت على حالة الولايات المتحدة التي تمتلك إمكانيات سيبرانية متقدمة لتقليل مخاطر هذه التهديدات، بينما ركزت الدراسة الحالية على التهديدات السيبرانية للأمن القومي الليبي، الذي يعاني من محدودية الإمكانيات بالإضافة إلى ذلك، ركزت الدراسة الحالية على حالات ونماذج للتهديدات السيبرانية، وكذلك جهود عدة دول في مكافحة هذه التهديدات من خلال جوانب مختلفة.

ثانياً: الدراسات الأجنبية:

1. **Study Mohamed Ben Naseir، National Cybersecurity Capacity Framework for Countries in a Transitional Phase (Using Spring Land as a Case Study) A thesis submitted in partial fulfillment of the requirements of Bournemouth University for the degree of Doctor of Philosophy،2021.**

هدفت الدراسة إلى التحقيق في أحدث أطر الأمن السيبراني وأطر بناء القدرات، مع التركيز على التحديات والعناصر الأساسية لإطار بناء القدرات السيبرانية الناجح والأساليب الممكنة لدمجها بطريقة أفضل وأكثر فعالية لتوجيه إطار بناء القدرات السيبرانية في ليبيا، وأيضا هدفت إلى تحليل العمليات الأمنية للدولة الليبية

باستخدام نهج نوعي يسمى الإدارة التفاعلية (CCMM)، وتحليل تأثير المخاطر بناءً على نموذج نضج القدرات السيبرانية لليبيا، كما سعت إلى تقييم مستوى النضج الحالي لقدرات الأمن السيبراني في أرض الربيع، التي وصفها الباحث في دراسته بأنها ليبيا، وقد اعتمدت الدراسة المنهج الاستقرائي والاستنباطي وقد توصلت الدراسة إلى مجموعة من النتائج، وهي أنَّه يجب وضع استراتيجية وطنية للأمن السيبراني بمشاركة أصحاب المصلحة المتعددين، وبناء عقيدة الدفاع السيبراني بتطوير قدرات الدفاع السيبراني لمواجهة التهديدات السيبرانية في مجالات السياسة والتجسس والأنشطة العسكرية، أيضا ينبغي تطوير برنامج وطني للتوعية يستهدف جميع شرائح المجتمع لتعزيز الوعي بالأمن السيبراني وتبني سلوكيات آمنة على الإنترنت، ويجب تعزيز قدرات الاستجابة الوطنية للحوادث من خلال إنشاء فرق الاستجابة لحوادث أمن الحاسوب الوطنية (CSIRT)، وضمان الموارد الكافية، وتحديد العمليات والمسؤوليات بوضوح، ويجب إنشاء إطار وطني لتعليم الأمن السيبراني وتطوير القوى العاملة في مجال الأمن السيبراني، وهو يعد جزءًا أساسيًا من استراتيجية بناء القدرات الوطنية.

تتمثل أوجه الاختلاف والتشابه بين الدراسة الحالية ودراسة الباحث في أن الدراسة الحالية تركز على إطار بناء القدرات الوطنية للأمن السيبراني للدول في مرحلة انتقالية، مستخدمةً أرض الربيع على أنها دراسة حالة وهي ليبيا، بينما تركز دراسة الباحثة على وضع مقترح لتطوير استراتيجية الأمن السيبراني في ليبيا، وتأتي أوجه التشابه في اختيار حالة ليبيا لكلتا الدراستين، مع التركيز على طبيعة التهديدات السيبرانية التي تواجه ليبيا وطرق حمايتها، بالإضافة إلى التطرق للتدابير الليبية في مكافحة الهجمات السيبرانية وتعزيز دور ليبيا في مجال الأمن السيبراني.

2. **Study Adel Azzam Alhait ،Cyber Hacking: Building a Harmonised Criminal Legal Framework for Addressing Cyber Hacking in the Arab Convention on Combating Information Technology Offences: A Comparative Study Between Jordanian & Saudi Cyber Laws A thesis in partial fulfilment of the requirements of Anglia Ruskin University for the degree of Doctor of Philosophy2021، .**

هدفت الدراسة إلى توفير إطار قانوني أكثر صرامة، سواء على المستوى المحلي أو الدولي، استعان الباحث بالمنهج الاستقرائي والمنهج المقارن والمنهج التاريخي، وتوصلت الدراسة إلى مجموعة من التوصيات، أهمها يجب تعديل المادة السادسة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ومراجعتها، ويجب مراجعة الاتفاقية لدمج بعض القواعد الواردة في اتفاقية بودابست وقوانين الإجراءات الجنائية في ولايات قضائية مختارة، مثل الولايات المتحدة والمملكة المتحدة وفرنسا وألمانيا، وأيضا يجب أن تتناول الاتفاقية مجرد الوصول غير المصرح به إلى نظام كمبيوتر، أو الوصول غير المصرح به الذي يسهل ارتكاب جرائم أخرى، بالإضافة إلى أنه يجب أن تعاقب الاتفاقية على البقاء غير المصرح به في نظام كمبيوتر، على الصعيد

التشريعي المحلي وضع دليل يشرح أساليب التعامل مع الأدلة الرقمية مثل المبادئ التوجيهية الفيدرالية الأمريكية لتفتيش ومصادرة أجهزة الكمبيوتر لمساعدة المدعين العامين العرب لأغراض التدريب وإنفاذ القانون، بالنسبة للهيئات التشريعية العربية، يجب أن تلزم جميع الشركات التجارية بتبني تدابير أمنية كافية لمنع الوصول غير المصرح به من الخارج والداخل إلى أنظمتها، ويجب على النواب العامين الالتزام بالقواعد المعمول بها في مجال تبادل المعلومات والمساعدة القضائية الدولية بموجب أحكام الاتفاقية العربية، وهناك حاجة إلى تعزيز التعاون بين وكالات التحقيق الجنائي بشأن جرائم القرصنة، وتبادل المعلومات وتتبع البيانات المتعلقة بالجرائم الإلكترونية والمجرمين المرتبطين بها على المستويين الإقليمي والدولي من خلال التفاصيل التي يوفرها الإنتربول، لتوحيد مفاهيم مكافحة القرصنة الإلكترونية وتبادل الخبرات، من الضروري تشجيع المؤتمرات والندوات والمناقشات الدورية حول التحقيق الجنائي في الجرائم المعلوماتية.

تتمثل أوجه التشابه بين الدراستين في أنَّ كلتاهما تتناولان الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، ولكن تختلفان في المنهج وفي التحليل، حيث قامت الدراسة الحالية بتحليل الاتفاقية من منظور قانوني، ووضعت بعض المقترحات لتحسينها بينما ركزت دراسة الباحثة على الاتفاقية على أنها من الجهود الدولية لمكافحة التهديدات السيبرانية، مما يبرز اختلافاً جوهرياً في الأهداف والمنهجية وأيضا الدراسة الحالية تسعى إلى تعزيز الإطار القانوني وتقديم توصيات محددة لتعديل الاتفاقية، في حين أن دراسة الباحثة تركز على التعاون الدولي وتبادل المعلومات في إطار الاتفاقية لمواجهة التهديدات السيبرانية.

10.صعوبات الدراسة

1. ندرة الوثائق والتقارير الرسمية المنشورة للعامة من قبل الحكومة الليبية التي تحلل الوضع في مجال الأمن السيبراني وتوضخ التهديدات السيبرانية التي تتعرض لها ليبيا.
2. صعوبة إجراء المقابلات الشخصية مع عينة الدراسة في المؤسسات الليبية الحكومية والخاصة، لا بل إن بعضهم رفض المشاركة في إجراء المقابلة.
3. قلة الدراسات السابقة المتاحة حول تحليل مخاطر التهديدات السيبرانية في الشأن الليبي.
4. صعوبة التعاون من بعض الجهات المعنية بموضوع الدراسة، بسب نقص الوعي بأهمية البحث العلمي في مجال الأمن السيبراني.

11.مفاهيم ومصطلحات الدراسة

1. **الفضاء الإلكتروني(Cyberspace) :**

إجرائيًا: يُمثل البيئة التي تحدث فيها كل الاستجابات، والتفاعلات، والأنشطة الرقمية.

2. **الأمن السيبراني (Cyber Security) :**

إجرائيًا: حماية أجهزة الحاسب الآلي وشبكاتها وبرامجها من أي دخول غير مرخص به ، أو اتلاف أو تغيير أو إساءة، وبعبارة أخرى، الأمن السيبراني هو حالة الحماية والأمان ضد التهديدات السيبرانية، أو ضد استخدام البيانات الرقمية، أو الشروع في ذلك.

3. **الأمن القومي (National security)** :

إجرائيا: قدرة الدولة على حماية مواردها وأراضيها ومصالحها، والدفاع عنها من أي تهديد أو هجوم محتمل، سواء كان من الداخل أو الخارج، باستخدام أدوات تقنية للحفاظ على كيانها في الفضاء الإلكتروني.

4. استراتيجية الأمن السيبراني(Cybersecurity strategy) :

إجرائيا : هي مجموعة من الأهداف، الخطط، والسياسات، والإجراءات التي تسعى الدولة إلى تحقيقها لحماية الفضاء الإلكتروني.

5. **التهديدات السيبرانية (Cyber threats) :**

إجرائيا: هي أي خطر، أو هجوم، أو عنف يحدث في الفضاء الإلكتروني، ويستهدف تخريب الأجهزة، والحواسيب، والشبكات الإلكترونية، ويمكن أن تنفذ هذه التهديدات من قبل دول أو فواعل غير دولية، بهدف إلحاق الأذى أو الضرر بالبنية المعلوماتية، والأنظمة المستهدفة، ويمكن أن تكون لها دوافع اقتصادية، أو سياسية، أو عسكرية، أو أيديولوجية، وذلك من خلال استخدام أدوات وتقنيات رقمية.

6. **التداعيات(Consequences)**:

إجرائيا: هي النتائج المحتملة، أو الآثار المترتبة عن تهديد معين، أو مجموعة من التهديدات.

7. الهجمات السيبرانية (Cyber attacks):

إجرائياً: هي أي عمل عدواني يستهدف أنظمة المعلومات والشبكات الرقمية بهدف إلحاق الضرر بها أو اختراقها أو تعطيلها.

12.تقسيمات الدراسة

تم تقسيم هذه الدراسة إلى ثلاثة فصول، وكل فصل إلى ثلاثة مباحث وسيتم تناولها على النحو الآتي:

الفصل الأول : التهديدات السيبرانية والأمن القومي : طبيعة المفهوم.

المبحث الأول : التهديدات السيبرانية : الخصائص، المصادر والأهداف.

المبحث التأني: تحليل أدوات التهديدات السيبرانية وأنواعها .

المبحث الثالث : مفهوم الأمن القومي وعناصره.

الفصل التأني : التهديدات السيبرانية للأمن القومي: التداعيات وسبل المواجهة

المبحث الأول : الأمن السيبراني ودوره في حماية الأمن القومي .

المبحث الثاني: دراسة حالات ونماذج للتهديدات السيبرانية.

المبحث الثالث : الجهود الدولية لمواجهة التهديدات السيبرانية.

الفصل الثالث : تداعيات التهديدات السيبراني للأمن القومي الليبي وطرق التصدي.

المبحث الأول : تحليل التهديدات السيبرانية التي تواجه ليبيا.

المبحث الثاني: تقييم الجهود الليبية لمكافحة التهديدات السيبرانية

المبحث الثالث: مقترح إطار عام لاستراتيجية وطنية للأمن السيبراني في ليبيا.

الفصل الأول

التهديدات السيبرانية والأمن القومي : طبيعة المفهوم

1.1. تمهـيد

أصبحت التهديدات السيبرانية من أخطر التحديات التي تؤثر على أمن المعلومات للدول، مما يعني المساس بشكل مباشر بالأمن القومي للدولة، وفي هذا السياق يمكن أن تمثل تهديدًا مباشرًا للوطن والمواطن والقيادات السياسية والأنظمة العسكرية في جميع أنحاء العالم، سواء خلال فترات السلم أو الحروب، ونظرا لأن الأمن القومي يعد من أبرز الأولويات لدى الدول، فإن الفهم الدقيق لطبيعة وتأثيرات هذه التهديدات السيبرانية يصبح أمرًا ضروريًا وحيويًا.

يتناول هذا الفصل ثلاثة مباحث، في المبحث الأول سيتم تعريف التهديدات السيبرانية، وتوضيح خصائصها الفريدة التي تميزها عن غيرها من أنواع التهديدات التقليدية، كما سيتم تناول المصادر المختلفة لهذه التهديدات، بما في ذلك الفاعلين الدوليين، والجماعات الإجرامية، والأفراد، وستساعد هذه الدراسة في فهم كيفية ظهور هذه التهديدات وتطورها في سياق بيئة رقمية متغيرة، و التركيز على الأهداف الاستراتيجية التي تسعى إليها، سواء كانت اقتصادية، أو سياسية، أو اجتماعية وسيسهم هذا التحليل في تقديم رؤية شاملة حول كيفية تأثير هذه التهديدات على الأمن القومي.

أما في المبحث الثاني، فسيتم تحليل أبرز الأدوات المستخدمة في تنفيذ التهديدات السيبرانية، وسنقوم بتحليل كيفية استخدام الأدوات المتاحة في تنفيذ هذه التهديدات من قبل المهاجمين لتحقيق أهدافهم، كما سيتم تصنيف الأنواع المختلفة لهذه التهديدات ، وسنعتمد على نهج متعدد التخصصات، يجمع بين المنظورات التقنية، والفنية، والسياسية؛ لتحليل طبيعة التهديدات السيبرانية وفهمها بشكل أعمق، وأيضا سيتم مناقشة النظريات التي تفسر مفهوم التهديدات السيبيرانية، وسنعرض في المبحث الثالث مفهوم الأمن القومي من زوايا مختلفة، مع التركيز على العناصر الأساسية التي تشكله، كالأمن العسكري، السياسي، والاقتصادي، والاجتماعي، والتقني وسيتم مناقشة الإطار النظري لمدرسة كوبنهاغن لتحليل مفهوم الأمن القومي وتطوره.

يهدف هذا الفصل إلى تقديم إطار فهم شامل وعميق حول التهديدات السيبرانية، والأمن القومي كما يُمهد الطريق للدراسات المستقبلية التي تستكشف سبل التعامل مع التهديدات السيبرانية في سياق حماية الأمن القومي.

2.1. التهديدات السيبرانية: الخصائص، المصادر والأهداف

قبل ما يزيد عن الخمسين عاماً، كان مفهوم الفضاء الإلكتروني والتهديدات السيبرانية ذا طابع استثنائي في نظر عدد قليل من الأكاديميين والمفكرين، وحتى الآن ليست هناك معايير واضحة لتحديد ما إذا كان الهجوم الإلكتروني يمثل جريمة أو عمل إرهابي، أو أن استخدامًا للقوة السيبرانية من قبل دولة ما، يعادل هجومًا مسلحًا، ولم تتم صياغة مواثيق دولية ملزمة قانونيًا على نحو صريح لتنظيم العلاقات بين الدول في الفضاء الإلكتروني، وذلك لأن التهديدات السيبرانية أصبحت قادرة على التأثير في الأصول السيبرانية الوطنية على مستوى الحدود، والمستوى الوطني، والمؤسسي، والإقليمي، والدولي، وفي المستويات الحرجة للبنية التحتية (Li and Liu: 2021:3) .

وبناءً على ذلك، فأن التهديدات السيبرانية تشكل مخاوف أمنية وطنية واقتصادية؛ وذلك نظرًا للتقدم السريع في تكنولوجيا المعلومات والاتصالات، وزيادة الاعتماد عليها، التي تدعم المزيد من جوانب المجتمع والحياة الحديثة(Schreier: 2015: 91) . يُعَدّ الخطر الناتج عن التهديد السيبراني أحد الأنماط الأكثر خطورة للنزاع، فهو يختلف إلى حد بعيد عن أساليب الصراع التقليدية، إذ يحمل القدرة على تجاوز رقابة الدولة ، وقَد يؤدي هجومه إلى وقوع أضرار جسيمة على جوانب حماية الدولة على المستويين الأمني والاقتصادي، بالإضافة إلى الحاجة للحصول على معلومات تشكل تهديدًا للأمن القومي (رياض:2021: 30). ويمكن أن يكون تأثير الهجوم على نطاق واسع أو محدود، وقد يكون الغرض من الهجوم تحقيق أهداف اقتصادية، أو سياسية، أو اجتماعية، أو نفسية، مما يعيق التحقيق في الإحصائيات الدقيقة والموثوقة للهجمات الرقمية؛ وذلك نظرًا لتعددها وتنوعها(Kenny: 2015: 4) .

1.2.1. مفهوم التهديدات السيبرانية :

لا يوجد تعريف عالمي موحد للتهديدات السيبرانية؛ وذلك لتباين الآراء والمعايير بين الجهات المعرفة، ويمكن أن يتباين هذا المفهوم وفقًا لمصالح وسياسات كل دولة، لذا يتعين علينا استكشاف وتحليل التعريفات المُقدمة لهذا المفهوم بعد تجزئته، من أجل فهمه وتحليله بشكل أعمق، وسيتم تقسيم مفهوم التهديدات السيبرانية إلى "التهديد" و"السيبرانية."

1.1.2.1. التهديد في اللغة: اشتقت كلمة "تهديد" من الفعل "هدد"، و يُقصد بها محاولة إلحاق الضرر والأذى، وكل ما يمكن أن يُعيق عملية بناء الأمن، أو يُؤدي إلى تقليل الشعور به (ياسمين والحسين: 2021: 163).

وقد عرَّف معجم أكسفورد (Oxford Dictionary) التهديد(threat) على أنه "محاولة شخص أو شيء لإلحاق الأذى بحياة الآخرين" (Oxford Basic English Dictionary: 2012: 404).

بينما وُصف في معجم وِبستر (Webster Dictionary) على أنه "تعبير عن نية لإلحاق الضرر أو التدمير، أو العقوبة، أو الترهيب، أو الانتقام" ،وفي اللغة الفرنسية يُشير مصطلح التهديد حسب معجم Petit) (Robertإلى الطريقة التي يوحي بها الرعب على وجه شخص ما، وذلك بنية جعله يَخشى الإيذاء الذي كانت النية وراءه (بالة: 2019).

2.1.2.1. التهديد اصطلاحاً: عرفه باري بوزان (Barry Buzan) بأنه يشكل خطراً على مؤسسات الدولة من خلال استخدام الإيديولوجيا، أو عناصر القوة لدولة ضد دولة أخرى، و يمكن أن يكون إقليم الدولة معرضاً لضرر أو غزو أو احتلال، وقد يأتي التهديد من الداخل أو الخارج (دحماني: 2017: 20).

أما تيري ديبيل (Terry L. Debel) فيرى أن التهديد هو عمل نشط وفعال تقوم به دولة معينة ؛ للتأثير في تصرفات دولة أخرى، ويشترط نجاحه توفر عدة عوامل أبرزها المصداقية ، والجدية ، والقدرات التي تتناسب مع التهديد، ويتضمّن التهديد ثلاث خصائص أساسية وهي الخطورة، واحتمالية حدوثه، بالإضافة إلى الزمن المُلائم لحدوثه (عادل: 2017).

3.1.2.1 .تعريف السيبرانية (Cyber) لغة واصطلاحاً :

أولاً: السيبرانية (Cyber) في اللغة:

عرفها معجم أكسفورد:(Oxford Dictionary) بأنها: "وصف لأي شيء مرتبط بثقافة الحواسيب، أو تقنية المعلومات، أو الواقع الافتراضي"(الصحفي:2020: 7).

ويشير معجم المورد (Almawrid) إلى أن السيبرانية "مشتقة من الضبط الأوتوماتي لعملية ما، باستخدام الحواسيب، وتعني علم الضبط، ومصدرها(Cybernetics)" (البعلكي:2004:307) .

وفي معجم المعاني تعرّف السيبرانية بأنها: تخيلي أو افتراضي(الموصلي: 2021:9.).

أما في معجم المصطلحات العسكرية الأمريكية (Dictionary of Military terms) فتعرف السيبرانية بأنها: فعل يستخدم عبر شبكات إلكترونية بهدف السيطرة، أو تعطيل برامج إلكترونية أخرى (مهدي:2020:149).

أما في معاجم اللغة العربية فلا يوجد مصطلح مرادف لكلمة "Cyber" ، وقد واجه المختصون العرب تحديًا كبيرا في إيجاد مصطلح مقارب لها، إلا أن اتفاقية مجلس أوروبا (Convention on Cybercrime) ترجمتها إلى اللغة العربية بأنها الاتفاقية المتعلقة بالجريمة الإلكترونية، و بناء على هذه الاتفاقية قد تم ترجمة كلمة سايبر باللغة العربية على أنها إلكتروني (الفتلاوي: 2016: 215-216).

وتعرف الباحثة كلمة السيبرانية إجرائياً بأنها البيئة الرقمية التي تضم الشبكات والأنظمة المعلوماتية، ويتم استخدامها لوصف الفضاء الافتراضي الذي يتضمن هذه الشبكات، والتقنيات المتصلة بها.

ثانياً: السيبرانية (Cyber) اصطلاحاً :

يرجع أصل كلمة السيبرانية حسب عدد من المؤرخين، إلى عالم الرياضيات الأمريكي نوربرت وينر(Norbert Wiener)1894-1964 الذي استخدمها للتعبير عن التحكم الآلي، من خلال مؤلفه الشهير (Cybernetics or control and communication in the animal and the machine)بمعنى السبرنتيقية، أو التحكم والتواصل عند الحيوان والآلة، حيث أشار فيه إلى أن السبرنتيقية تعنى التحكم والتواصل عند الحيوان، والآلة، والإنسان، وبعد الحرب العالمية الثانية، تم استبدال مصطلح الآلة بالحاسوب وقد اشتقت كلمة السيبرانية من كلمة السبرنتيقية (العمري: 2020: 16).

وعلاوة على ذلك، فقد انتشر استخدام هذا المصطلح بشكل كبير بعد صدور رواية الخيال العلمي نيورومانسر،(Neuromancer) التي كتبها ويليام جيبسون (William Gibson) عام 1984م، وقد تناولت هذه الرواية الفضاء الإلكتروني وأعمال التخريب فيه(خليل: 2023: 267-268) .

وتشير السيبرانية إلى أنها لفظة يونانية الأصل، مشتقة من كلمة (kybernetes) ، التي تعني الشخص الذي يدير دفة السفينة، وتُستخدم هذه الكلمة مجازًا لوصف المتحكم (قرة: 2019) هذا المصطلح استخدم لاحقاً للإشارة إلى التحكم والقيادة في الانظمة.

فالسيبرانية تُستخدم لوصف أي شيء مرتبط بثقافة الحواسيب، أو تقنية المعلومات، أو الواقع الافتراضي، و هي متأصلة في العديد من المصطلحات الشائعة في مجال تكنولوجيا المعلومات والاتصالات، كالفضاء الإلكتروني، والخيال العلمي (مهدي:2020: 148).

4.1.2.1. تعريف التهديدات السيبرانية :

عرفها معجم اكسفورد (Oxford Dictionary) بأنها: إمكانية حدوث محاولات خبيثة لتعطيل أو تدمير شبكة أو نظام حاسوب (setrfanescu and Papol:2020:178). ويعد هذا التعريف دقيقا، ويصف الجانب التقني والنتائج المحتملة للتهديدات السيبرانية، وهذا يعني أن هناك جهة ما تستخدم الإنترنت أو طرق أخرى للوصول إلى البيانات، أو الأنظمة، أو الشبكات التي تستخدمها الدولة أو المؤسسة أو الفرد، وتحاول إلحاق الضرر بها أو منعها من العمل بشكل صحيح.

وتُعرّف التهديدات السيبرانية أيضا بأنها أي ظرف أو حدث يمكن أن يؤثر سلبًا على العمليات التنظيمية، والمؤسسات، والأفراد، والمنظمات، أو حتى الدول من خلال نظام المعلومات، أو من خلال الوصول غير المصرح به، أو التلاعب، أو حجب الخدمة(Johnson and others: 2016:2) .

ويتضح من خلال هذين التعريفين أن معجم أكسفورد ركز في تعريفه بشكل رئيسي على النواحي التقنية والتهديدات الفعلية المحتملة، بينما قدم التعريف الثاني رؤية واسعة وشاملة للتهديدات السيبرانية وتأثيراتها على المستوى الاجتماعي، والاقتصادي، والسياسي.

وقد عرف معجم مصطلحات الأمن المعلوماتي التهديدات السيبرانية بأنها هجوم عبر الفضاء الإلكتروني، يهدف إلى السيطرة على المواقع الإلكترونية أو البنى المحمية إلكترونيًا؛ لتعطيلها، أو تدميرها، أو إلحاق الضرر بها (الفتلاوي: 2016: 216). وهذا التعريف يوضح الغرض من التهديدات السيبرانية، ويحدد نوعها على أنها هجمات الكترونية.

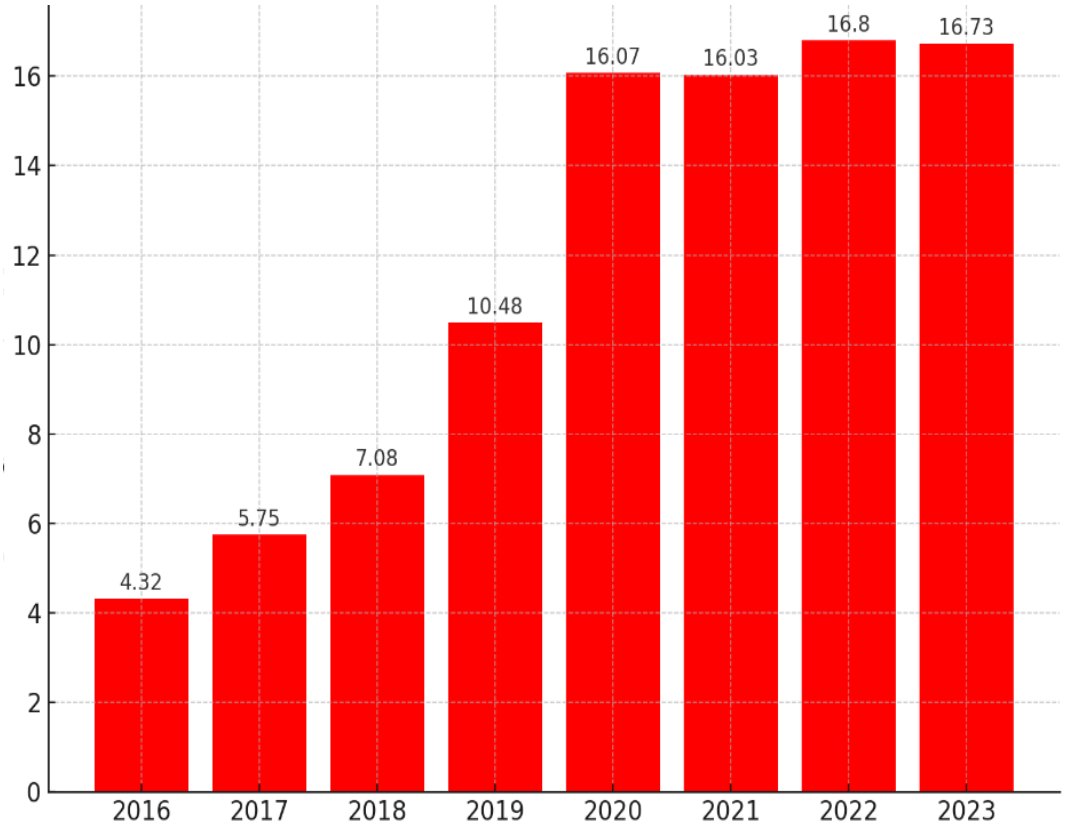
وعُرفت التهديدات السيبرانية أيضا بأنها "الهجمات والمخاطر التي تُنفّذ باستخدام شبكات الإنترنت، وأجهزة الحاسب الآلي، بهدف إلحاق الضرر بالدولة المستهدفة، حيث تتباين هذه التهديدات وتتفاوت من دولةٍ لأخرى نتيجة للتطوّر والتقدّم التقني (جعفري: 2022: 247). وهذا التعريف يركز على الأدوات المستخدمة في تنفيذ التهديدات السيبرانية، والتنوع في مستوى التحكّم بهذه الأدوات بين الدول، ويُظهر ذلك من خلال أن الدول قد تواجه تهديدات سيبرانية متباينة استنادًا إلى مستوى تطوّرها التقني، وقدرتها في مجالها السيبراني.

وتعرف المتحدثة باسم مجلس الأمن القومي في البيت الأبيض حينها كاتلين هايدن (Katlin Hayden)، التهديدات السيبرانية بأنها هجمات تشتمل على مجموعة واسعة من الأنشطة الضارة التي يمكن أن تحدث عبر الفضاء الإلكتروني، وقد أشارت إلى أن هذه التهديدات تتضمن التجسس، وسرقة الملكية الفكرية، وهجمات الحرمان من الخدمة(DDoS) بالإضافة إلى البرمجيات الخبيثة المدمرة (yusuf:2013:132).

وهذا التعريف يعكس تنوع الأشكال والأنواع المختلفة للتهديدات السيبرانية، حيث تستغل هذه التهديدات نقاط الضعف أو الثغرات الموجودة في الفضاء الإلكتروني.

وتعرف التهديدات السيبرانية أيضا بأنها برامج ضارة تنشأ في الفضاء الإلكتروني؛ لاستهداف الميكروكمبيوترات، والهواتف الذكية، والأجهزة اللوحية، والشبكات المتصلة بالإنترنت، ويمكن أن يكون الجاني وراء هذه التهديدات شخصًا، أو دولة، أو مجموعة من القراصنة، أو منظمة لها أهداف جيوسياسية (بوقرص:2022:65). من خلال هذا التعريف يتضح لنا أنه يقدّم نظرة شاملة على التهديدات السيبرانية، وذلك من خلال التركيز على الأدوات المستخدمة، والجهات الفاعلة، كما أنه يسلط الضوء على الأبعاد الجيوسياسية لهذه التهديدات، مما يعكس تعقيد وتأثير الهجمات السيبرانية في العصر الحديث.

كل التعاريف التي تم ذكرها قد تجسدت في الواقع على شكل هجمات سيبرانية، سيتم توضيح عدد هذه الهجمات كما هو موضح في الشكل رقم(1) للهجمات السيبرانية المسجلة في جميع أنحاء العالم من عام 2016 إلى 2023م تهدف هذه الاحصائيات لتقديم نظره عامة على مشهد التهديد .



الشكل رقم(1)عدد الهجمات السيبرانيةالمسجلة في جميع أنحاء العالم2016-2023، المصدر:(STATISTA2024)

يوضح الرسم البياني عدد الهجمات السيبرانية على مستوى العالم، حيث بلغت هذه الهجمات عام 2016 4.32 مليون هجوم واستمر العدد في الارتفاع بشكل ملحوظ حتى عام 2023 ما يقرب من 17 مليون هجوم، ومن المتوقع أن يستمر العدد في الارتفاع خلال السنوات القادمة.

وفقاً لتقرير صادر عن المنتدى الاقتصادي العالمي حول تحليل المخاطر العالمية لعام 2024م، تحتل الهجمات السيبرانية المرتبة الخامسة بنسبة 39% من بين أكثر المخاطر العالمية شيوعاً (World economic forum:2024).

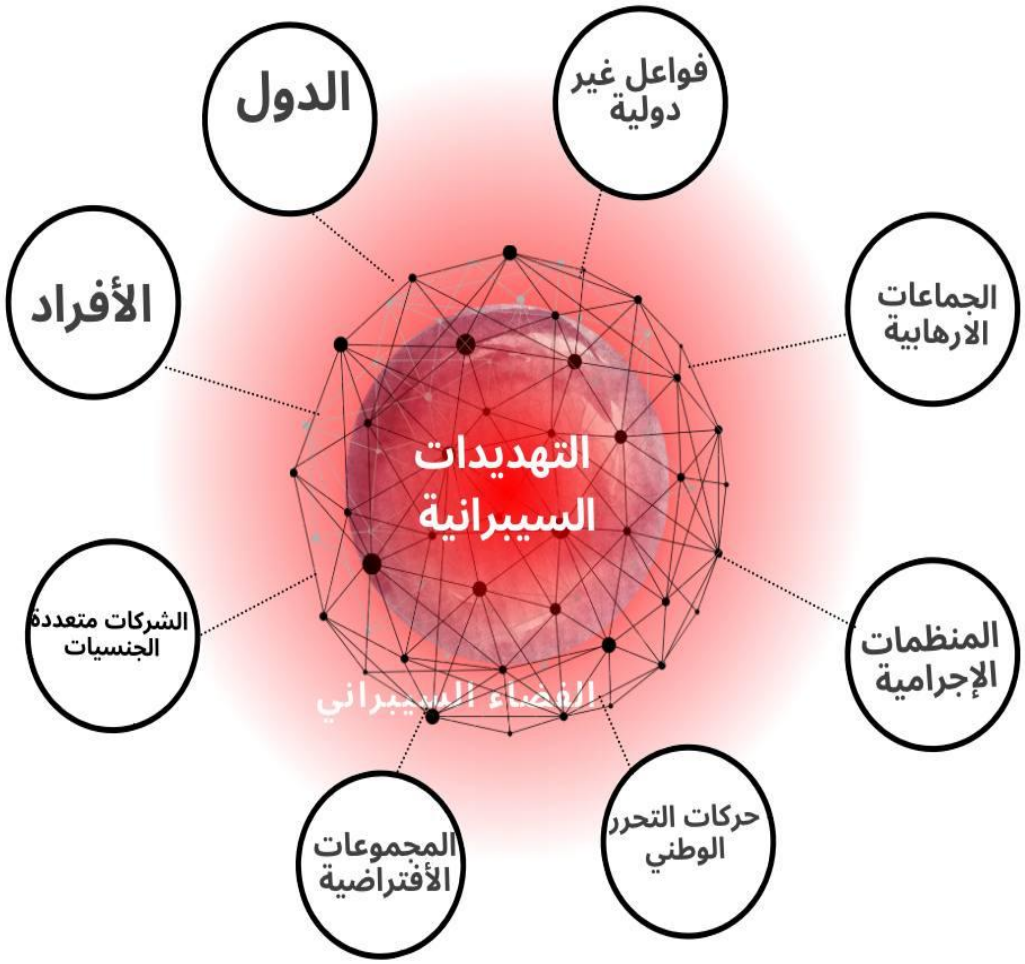
2.2.1. خصائص التهديدات السيبرانية :

تتميز التهديدات السيبرانية بخصائص فريدة تميزها عن غيرها من التهديدات التقليدية، وذلك لأنها تُنفذ عبر شبكات الحاسوب والإنترنت في الفضاء الإلكتروني ومن أبرز هذه الخصائص:

1. السرعة الفائقة في التدمير: يمكن للتهديدات السيبرانية أن تلحق أضرارًا جسيمة بالأمن القومي للدول في وقت قصير قد لا يتجاوز الساعة ، وفي بعض الحالات يمكن أن يحدث الضرر في دقائق معدودة، و يمكن أن تحدث الأضرار قبل أن تدرك الضحية أنها مستهدفة، مما قد لا يتيح لها فرصة للدفاع عن نفسها. (عبدالصادق: 2015).
2. صعوبة تحديد هوية المهاجمين السيبرانيين: تتيح التقنيات المتطورة في الشبكات المعلوماتية إمكانية إخفاء هوية منفذي الهجمات السيبرانية، مما يجعل عملية تحديد هويتهم تعتمد غالبًا على التخمينات، ومحاولة الربط بين الأحداث دون وجود أدلة قاطعة (خليل: 2023: 288).
3. انتقائية التهديدات السيبرانية والتحكم في تداعياتها: يمكن أن تكون انتقائية ويتم التحكم في تداعياتها، فعلى سبيل المثال، يمكن للهجوم السيبراني أن يستهدف اقتصاد دولة كاملة دون تدمير البنية التحتية الأساسية الحرجة، أو يمكن استخدامه لاستهداف البنية التحتية للدولة و اقتصادها معاً (السدخان: 2021: 224).
4. تعقد التهديدات السيبرانية: تُعد هذه التهديدات معقدة للغاية، حيث لا يمكن تحديد نقطة بداية لها ، ولا يمكن معرفة نهايتها، ولا توجد لها حدود جغرافية واضحة بين الدول، حيث تشترك الدول الصغيرة والكبيرة في الفضاء الإلكتروني (عبد الواحد:2021: 44).
5. تنوع دوافعها: فالتهديدات السيبرانية لا تنشأ نتيجة الخلافات السياسية فحسب، بل يمكن أن تنشأ نتيجة للتطور الاقتصادي، أو بهدف سرقة المعلومات الاستراتيجية؛ لفهم نوايا الخصوم، أو لسرقة تصميمات الأسلحة العسكرية، والتقنيات التكنولوجية الحديثة، بالإضافة إلى أنها قد تكون مدفوعة بأسباب أيديولوجية وغيرها(خليفة: 2019: 115).
6. عدم التقيد بالنطاق الجغرافي: عند تنفيذها ليس من الضروري أن يكون المهاجم في نفس الموقع أو المكان، أو أن يكون مراقبًا بشكل مباشر، فمن الممكن أن يكون الهجوم موجهًا من دولة أو قارة أخرى، وهذا ما يجعله غير خاضع لنطاق إقليمي محدد (العمري: 2020: 77).
7. لا تحدث في ساحات المعارك التقليدية: أي أن لا تتطلب ساحات معارك تقليدية، بل يتم تنفيذها عبر الفضاء الإلكتروني؛ للسيطرة على الأهداف بسرعة أو تعطيلها دون الحاجة إلى التغلب على الدفاعات التقليدية للدول (جواد: 2016: 131).
8. صعوبة الحصول على الأدلة الرقمية: تتميز بسرية هوية منفذيها، حيث إنها لا تترك أثرا واضحا عند تنفيذها، ولا تخضع لأي قيود إقليمية أو زمنية، ويمكن أن تسبب أضرارًا فورية لعدد لا يحصى من الضحايا (الأمم المتحدة: 2019: 48) كما أن الحصول على الأدلة الرقمية في هذه الحالات يعد أمرًا صعبًا، إذ أنه من الممكن التخلص منها وإزالتها بسهولة (العمري: 2020: 5).

3.2.1. مصادر التهديدات السيبرانية :

تتنوع المصادر الفاعلة للتهديدات السيبرانية لتشمل مجموعة من الفواعل التي تمتلك القوة في الفضاء السيبراني كما هو موضح في الشكل رقم(2)، ويمكن تصنيف هذه الجهات إلى، أفراد ودول وفواعل من غير الدول، وسيتم توضيح ذلك على النحو الآتي:



الشكل رقم (2) مصادر التهديدات السيبرانية، المصدر: من إعداد الباحثة.

1.3.2.1. الدول :

تعد الدول فاعلاً محورياً في الفضاء الإلكتروني، وذلك نظرًا لامتلاكها الإمكانيات المادية، والبشرية، والقانونية اللازمة لعملها (صفاء ومهدي:2020: 150). وتُعد الفئة الأولى الأكثر أهمية بين فواعل القوة السيبرانية، حيث تستغل الفضاء الإلكتروني لتحقيق مصالحها وأهدافها على المستويات الإقليمية، والدولية ،كما أنها تمتلك القدرة على تنفيذ هجمات إلكترونية وممارسة السلطة ضمن حدودها، ولكي تتمكن الدول من ممارسة نفوذها داخليًا وخارجيًا عبر الفضاء الإلكتروني، يجب أن تتوفر لديها مجموعة من العناصر المتنوعة، من بنية تحتية سيبرانية متطورة، وبنية مؤسسية وتشريعية قوية، واستراتيجية واضحة تحدد الأهداف والمبادئ (طالة: 2020: 60).

وبناءً على هذا، يمكننا القول بأن الدول تشكل أخطر مصدر للتهديدات السيبرانية وتُعد الأكثر تأثيرًا في الفضاء الإلكتروني، وتتنوع هذه التهديدات من نشر للمعلومات المضللة، وجمع المعلومات الاستخباراتية،

وشن هجمات صغيرة وكبيرة على البنى التحتية الحيوية، على سبيل المثال لا الحصر في نهاية عام 2008م، نجحت حوالي 140 دولة في تطوير ترسانة من الأسلحة السيبرانية (Lord:2011:31).

2.3.2.1.الفواعل من غير الدول :

يعرفها *بريان هوكينغ (Brian Hocking)، ومايكل سميث (Michael Smith)*بأنهم جماعات أو منظمات تتمتع باستقلالية تمنحها حرية السعي لتحقيق أهدافها، و بقدرة على تمثيل أتباعها، ومؤيديها، وكذلك القدرة على إحداث تأثير ملموس في قضايا معينة، مقارنة بتأثير فاعلين آخرين في نفس القضايا (صفاء ومهدي: 2020: 155).

وتشن هذه الفواعل هجمات إلكترونية تهدف إلى قطع الخدمة، أو تعطيل الأنظمة على الرغم من أنها لا تمتلك نفس القدرات التي تتمتع بها الحكومات الكبرى، وتستهدف هذه الفواعل شبكات الجريمة المنظمة، ومهاجمة الأفراد والشركات على حد سواء، ويميل هؤلاء المهاجمون إلى تجنب الاشتباك المباشر مع الكيانات الحكومية وعملياتها في الفضاء الإلكتروني (Lord: 2011:32) . ويمكننا تقسيم هذه الفواعل إلى مجموعة من فئات رئيسية تتمثل في الآتي:

- المنظمات الإجرامية: تعتمد هذه المنظمات بشكل كبير على شبكة الإنترنت ووسائل التكنولوجيا الحديثة لتعبئة الرأي العام، والضغط على الحكومات، وذلك من خلال تنظيم الحملات الاجتماعية، وتعبئة المجتمع المدني لتغيير سياسات معينة (محمود وآخرون: 2023). وتقوم هذه المنظمات بعمليات القرصنة السيبرانية، وسرقة المعلومات، واختراق الحسابات البنكية، وتحويل الأموال، كما أنه توجد سوق سوداء على الإنترنت المظلم (Dark internet) (دحماني: 2018: 26). حيث تركز هذه المنظمات بشكل أساسي على الربح المالي، ويستغلون أدوات كبرامج الفدية، ورسائل التصيد الاحتيالي عبر البريد الإلكتروني لسرقة المعلومات، والوصول إلى بطاقات الائتمان وغيرها، حيث تقدر تكلفة هذه الجرائم السيبرانية بمليارات الدولارات سنويًا (Cunningha :2015:15) .

- الشركات متعددة الجنسيات: تمتلك بعض شركات التكنولوجيا موارد تفوق قدرة بعض الدول، ولا ينقصها سوى شرعية ممارسة القوة التي ما زالت حكراً على هذه الدول، فخوادم شركات مثل جوجل (Google) ومايكروسوفت (Microsoft) ، وآبل (Apple) ، وميتا (Metaverse) ،تسمح لها بامتلاك قواعد بيانات عملاقة، من خلالها تستكشف وتستغل الأسواق، وتؤثر في اقتصاديات الدول وثقافة المجتمعات وتوجهاتها (عبدالجواد: 2020: 400). ومن خلال وسائل التواصل الاجتماعي العالمية التابعة لهذه الشركات مثل فيسبوك ،وتويتر، واتساب، التي أصبحت تملك دوراً أساسياً في النظام العالمي بفضل ما تمتلكه من بيانات وقدرات، تمتلك هذه المنصات كمية هائلة من المعلومات، مما يمنحها قدرات من خلال هذه المعلومات، تستطيع اختراق البيانات، وتوجيه المجتمعات، وتشكيل الرأي العام العالمي (جمال الدين: 2023: 201).

- الجماعات الإرهابية: تُعد هذه الجماعات من أبرز الفواعل غير الدولية، و خاصة بعد أحداث 11 سبتمبر، وتستغل هذه الجماعات الفضاء الإلكتروني في عمليات التجنيد والتعبئة والدعاية، وجمع الأموال، كما تسعى إلى جمع المعلومات حول الأهداف العسكرية، وتعلم كيفية التعامل مع الأسلحة السيبرانية، وتدريب المجندين

الجدد عن بُعد (طالة: 2020: 61). ودوافعهم وراء ذلك ليست مالية فحسب، بل لديهم قضية معينة يدافعون عنها، وعادة ما يقومون بإرسال رسائل تهديد، أو تدمير للبيانات المخزنة وغيرها في نظم المعلومات الحكومية المستهدفة(طاجين: 2018: 23).

- المجموعات الافتراضية: هي مجموعات من الأشخاص يتواصلون ويتفاعلون عبر الإنترنت، أو عبر وسائل التواصل الرقمية، دون أن يكونوا مقيدين بزمان أو مكان محددين، وتشكل هذه المجموعات شبكات اجتماعية تستند إلى اهتمامات أو أهداف أو قيم مشتركة بين أعضائها (عبد الجواد: 2020: 400-401).

- حركات التحرر الوطني: تُعد هذه الحركات من أبرز الجهات الفاعلة غير الحكومية على الساحة الدولية، حيث تنشط في الفضاء الإلكتروني لإطلاق هجماتها، وذلك بهدف تحقيق أهداف سياسية، ومن بين هذه الحركات، حركة حماس، وحزب الله، وعلى الرغم من أن هذه الحركات تضم عدداً كبيراً من الأفراد، إلا أنه قد يقوم فرد واحد بشن هجمات سيبرانية ضد الأعداء عبر الإنترنت، وذلك دفاعاً عن قضية الحركة التابع لها (رياض:2022: 31).

3.3.2.1. الأفراد :

هم مستخدمو الإنترنت، والشبكات، والأجهزة الإلكترونية، وغالبا ما يمتلكون القدرة على استخدامها للحصول على المعلومات والخدمات، ويمكن أن يكونوا مستخدمين أو مستهلكين أو منشئين للفضاء الإلكتروني، وهذا يجعلهم فاعلين مؤثرين، فقد يكونون مواطنين اعتياديين، أو نشطاء في القرصنة، أو محتالين سيبرانيين، أو من المجرمين الإلكترونيين المنظمين، أو عملاء التجسس السيبراني، أو المرتزقة السيبرانيين، أو الميليشيات السيبرانية (Sigholm:2016:1622) .

ولفهم الدور الكبير الذي تلعبه مصادر التهديدات السيبرانية في العصر الحديث، يجب النظر في العوامل المتعددة التي تسهم في تنامي هذه التهديدات، وتأثيرها على البنية التحتية العالمية، و يمكن تلخيص هذه العوامل كما يلي:

أولاً: الاعتماد المتزايد على الفضاء الإلكتروني: كلما زاد ارتباط دول العالم بالفضاء الإلكتروني، زادت المخاطر والهجمات التي تهدد البنية التحتية للمعلومات على مستوى العالم (كلاع: 2022: 299).

ثانياً: تراجع دور الدولة التقليدي في ظل العولمة وانسحابها من العديد من القطاعات الاستراتيجية لصالح القطاع الخاص: وهذا أدى إلى تعاظم دور الشركات الأجنبية والمتعددة الجنسيات، خاصة في مجال التكنولوجيا، ولاسيما مع تفوقها في القدرات التقنية على الحكومات لتصبح لاعباً رئيسياً في الفضاء الإلكتروني (كلاع: 2022: 299).

ثالثاً: سهولة استخدام ممارسة الحروب السيبرانية: يمكن لبعض الكيانات، أو الدول استخدام التهديدات السيبرانية ضد أعدائها، دون الحاجة إلى الدخول إلى أراضيها، مع اعتماد الدول على الأنظمة الإلكترونية في غالبية منشآتها الحيوية يجعلها عرضة لهجمات مزدوجة، سيبرانية وبريّة (مركز نورس للدراسات: 2019: 7-8).

رابعاً: التكلفة المنخفضة: تعد التهديدات السيبرانية أقل تكلفة من نظيراتها التقليدية، وقد لا تكلف قيمة دبابة واحدة، و تتطلب بعض الأسلحة السيبرانية الحديثة مهارات بشرية فقط، دون التقيد بقيود الوقت أو الظروف السياسية (كلاع: 2022: 299).

خامساً: استعراض للقوة من خلال التهديدات السيبرانية: حيث أصبحت هذه التهديدات وسيلة لإظهار قوة الدول وتفوقها التقني، مما أدى إلى تبني الدول لاستراتيجيات سيبرانية جزءاً من قواتها القومية، ومجالا للتوظيف في ساحات الفضاء الإلكتروني، فقد صارت هذه الاستراتيجيات عنصرًا من عناصر القوة القومية للدول (مركز نورس للدراسات: 2019: 7-8). بالإضافة إلى أن هذه التهديدات قد تنشأ من كيانات داخلية أو خارجية، أو من مزيج بينهما، وسيتم التركيز هنا على التصنيف الثنائي لمصادر التهديدات لتحديدها بدقة (Mouna and Aissab:2014:94)على النحو الآتي:

- **التهديدات الداخلية**: تشير هذه التهديدات إلى المخاطر التي تنشأ داخل المنظمة أو الدولة نفسها، سواء كانت عن قصد، أو عن غير قصد، وهذه التهديدات يمكن أن تكون من قبل الموظفين الحاليين أو السابقين، أو المتعاقدين، أو أي شخص لديه القدرة على الوصول إلى الأنظمة الحساسة داخل هذه المنظمة.

- **التهديدات الخارجية**: قد تنشأ هذه التهديدات من أفراد، أو منظمات تعمل خارج المنظمة، وليس لديهم حق الوصول المصرح به إلى أنظمة الكمبيوتر، أو الشبكات الخاصة بالمنظمة، ويمكن أن تحدث التهديدات الخارجية أيضا عبر شبكات الاتصال (السلكية واللاسلكية)، أو الاختراق المادي أو شبكة التعاون.

وبناء على ما سبق، يمكن تلخيص التهديد الداخلي بأنه تهديد يشمل سوء السلوك من قبل الموظفين الداخليين، وذلك من خلال سرقة البيانات، أو الإفصاح غير المشروع عن المعلومات الحساسة، وعدم المرونة في تطبيق السياسات الأمنية الداخلية من قبلهم، وهذا يفتح ثغرات أمنية داخلية وهجمات نشطة من الداخل، حيث يقوم الموظفون العاملون بالشركة بعمليات تخريبية داخلها، أما التهديد الخارجي فيشمل هجمات القرصنة الإلكترونية، من قبل مجموعة من القراصنة أو الهاكرز الخارجية، بالأضافة إلى هجمات الاحتيال الإلكتروني، كالبريد الإلكتروني الاحتيالي، والتصيد الاحتيالي ،والبرمجيات الخبيثة، والفيروسات التي يتم نشرها عبر الإنترنت للاختراق والتجسس.

4.2.1.أهداف التهديدات السيبرانية :

تختلف أهداف التهديدات السيبرانية باختلاف الجهات الفاعلة والمنافسين، حيث تُعد هذه الجهات الأكثر إثارة للجدل في النظام الدولي، فقد تكون الجهات الفاعلة من غير الدول أهدافًا فقط، وليست جهات مبادرة، وهذا يعني أنها تستهدف مجموعة متنوعة من الأهداف، ولا تقتصر على الأهداف العسكرية فحسب، فيمكن أن تكون الأهداف ثقافية، كطمس هوية الدولة، أو اقتصادية، كتدمير أجهزة المعلومات لمجموعة من المؤسسات المالية، خاصةً مع تحول معظم قطاعات الدولة إلى الرقمنة، بالأضافة إلى أنه من الممكن أن تستهدف المواقع الرسمية وأنظمة الشبكات الحكومية، بقصد تحقيق أهداف سياسية، كزعزعة الاستقرار، أو التأثير على السياسات الحكومية لاسيما تتضمن هذه الأهداف مهاجمة الأنظمة العسكرية والبنى التحتية

الحيوية، بهدف إضعاف القدرات الدفاعية للدولة، و يمكن أن يكون التأثير المقصود للهجوم السيبراني مرتبطًا بهدف الهجوم في سياق التهديدات السيبرانية، حيث تستهدف البنى التحتية للدولة وسيتم تناول هذه الأهداف كما يلي:

1. اختراق قواعد البيانات: يعد اختراق قواعد البيانات من أخطر أهداف التهديدات السيبرانية، حيث يتضمن حذف أو تعديل المعلومات المخزنة أو الاستيلاء عليها، كأسماء المستخدمين، وأرقامهم السرية، وعناوين الاتصال الخاصة بهم، واستخدامها لأغراض غير مشروعة أو بيعها لجهات مستفيدة سواء كانت اقتصادية، أو تجارية، أو سياسية، أو أمنية (عبد الجواد: 2020: 410). إن اختراق الأجهزة والشبكات الخاصة بالدولة، أو الجهة المستهدفة، وتغيير البيانات الموجودة عليها، قد لا يُكتشف إلا بعد مرور فترة من الزمن، مما قد يؤدي إلى اتخاذ قرارات مهمة بناءً على معلومات خاطئة، وتتراوح حدة هذه الهجمات بين تشويه المواقع بتغيير المحتوى الوارد عليها، وتصل إلى ذروتها عند استهداف قواعد البيانات الخاصة بالأسلحة وأنظمة القيادة والتحكم (عبدالعزيز: 2017).
2. استهداف البنية التحتية الحيوية: تُعد البنية التحتية من أهم الأهداف الاستراتيجية لأية دولة، حيث يجب حمايتها وتأمينها من الهجمات الإلكترونية التي تستهدفها، سواء كانت مدنية، أو عسكرية، إذ تؤدي هذه الهجمات إلى شل الأنظمة وتدميرها، مما يؤثر على تدفق المعلومات، ويُربك عمل البنية التحتية الحيوية، مما ينتج عنها تعطيل العديد من مرافق الحياة وسيادة الفوضى في البلاد(كلاع: 2022: 300). ويزداد خطورته عندما يتعلق بالبنية التحتية الحرجة كقطاعات الطاقة، والكهرباء، والنقل، والاتصالات، والسدود، والخزانات، والطاقة الشمسية، والمفاعلات النووية، حيث يؤدي تهديدها إلى خسائر كبيرة في الأرواح والأموال (البيديري: 2021: 102). بالأضافة إلى أن تشكل أنظمة التحكم الإشرافي واكتساب البيانات (SCADA) ثغرة فريدة من نوعها فإن تعطيل محطة طاقة كهربائية من خلال مهاجمة هذا النظام الخاص بها، يمكن أن يخلف تأثيرات لاحقة كبيرة (Theohary:2015:9)، على سبيل المثال لا الحصر تعرض أوكرانيا في يونيو 2017م، لهجمة إلكترونية، شملت محطات الطاقة، والمؤسسات المالية، وأحد أكبر مطاراتها من خلال هذا النظام (خليفة: 2017: 57).
3. استهداف الشبكات الحكومية: تُعد من الأهداف الرئيسية للهجمات السيبرانية، التي تنفذها الدول القومية، أو الكيانات، وتهدف هذه الهجمات إلى استخراج البيانات للحصول على ميزة استخباراتية، أو زرع شفرات خبيثة يمكن تنشيطها في أوقات الأزمات لتعطيل العمليات أو منعها فمثلا، في عام 2008م، تعرض البنتاغون لاختراق كبير عندما تم إدخال محرك أقراص محمول مصاب ببرنامج خبيث يُدعى (Agent.btz)في جهاز كمبيوتر، متصل بشبكات وزارة الدفاع السرية، وقد أدى اكتشاف هذا البرنامج إلى عملية تنظيف واسعة النطاق، عُرفت باسم (Buckshot Yankee) وعلى الرغم من ارتباط الحادث بالتجسس وسرقة المعلومات الحساسة، فأنه من المحتمل أن تكون البرامج الضارة قد احتوت على وظائف خفية أكثر خطورة، كتعطيل الاتصالات، أو نشر معلومات مضللةTheohary and Maness (:2015:5).

4. التجسس الصناعي: يُعد القطاع الصناعي من الركائز الأساسية للتنمية الاقتصادية، وغالبًا ما يكون محورًا للنزاع بين الدول، وتلجأ الدول إلى التجسس الإلكتروني للحصول على معلومات حول الأدوات والركائز الأساسية التي تدعمه، ومن أبرز الأمثلة على ذلك، تعرض ألمانيا عام 2010م لعمليات تجسس صناعي من قبل روسيا والصين، نتيجة للمنافسة الاقتصادية بين هذه الدول (إبراهيم: 2022).
5. استهداف الهوية الوطنية الاجتماعية، وذلك بهدف تضليل أو تخويف الأفراد والشخصيات البارزة، والاحتيال عليهم، فمثلا، في عام 2014م، تعرضت كوريا الجنوبية لاختراق كبير استهدف البيانات الشخصية الهامة، كأرقام التعريف، والعناوين، وأرقام بطاقات الائتمان، مما أدى إلى سرقة بيانات حوالي 20 مليون مستخدم، أي ما يعادل 40٪ من سكان البلاد(Seiss and others:2015:18).
6. جمع المعلومات الاقتصادية: من خلال اختراق قواعد البيانات المالية والمصرفية، وقواعد البيانات للشركات والبنوك، فهذه الهجمات تستهدف الحصول على معلومات حساسة قد تؤثر على الأمن القومي للدولة، كما تشمل التجسس على المسؤولين الماليين، ووزراء المالية، ورؤساء الشركات الكبرى (خليفة:57:2017).
7. إثارة الفتن داخل الدولة على المستوى السياسي: تهدف التهديدات السيبرانية إلى شحن الشعب ضد السلطة الحاكمة، ويتم ذلك من خلال نشر خطابات الكراهية عبر منصات التواصل الاجتماعي، مما يؤدي إلى زعزعة الاستقرار السياسي والاجتماعي، فهذه الاستراتيجية لعبت دورًا كبيرًا في ثورات الربيع العربي عام 2011م، حيث أسهمت في سقوط أنظمة حكم بعض من الدول العربية (إبراهيم:2022)وفقًا لتقرير نشره موقع ستاتيستا (Statista) في عام 2024م، تم تصنيف الدول الأكثر استهدافًا سياسيًا من التهديدات السيبرانية خلال الفترة من عام 2000 إلى 2023، جاءت الدول غير المعروفة في المرتبة الأولى بنسبة 44.81%، تلتها الصين في المرتبة الثانية بنسبة 11.87%، ثم روسيا في المرتبة الثالثة بنسبة 11.58%، وأيضا إيران في المرتبة الرابعة بنسبة 5.27% من إجمالي الدول المستهدفة عالميًا(Statista:2024).
8. تعطيل قطاعي التجارة والخدمات: يُعد القطاعين من الركائز الأساسية لتلبية احتياجات السكان في الدول، فالتهديدات على هذه القطاعات يمكن أن تؤدي إلى شلل اقتصادي، وهذا قد يعوق تقديم الخدمات، ويزيد من تذمر السكان، ومن جودة الخدمات المقدمة، ويتم ذلك غالبًا من خلال قرصنة المواقع الإلكترونية، وهذه الهجمات تُكبد الدول خسائر مالية ضخمة تصل إلى مليارات الدولارات سنويًا (إبراهيم:2022) وقد تم استخدام الإرهاب السيبراني لتخريب منظمات القطاع الصناعي الخاص مثل PayPal وMasterCard وVisa حتى الشركات الكبرى في مجال التكنولوجيا لم تعد محصنة، لضحايا التهديدات السيبرانية مثل شركة قوقل Google وسوني Sony (Seissa and others:2015: 182).
9. استهداف الأنظمة العسكرية: عادةً ما تستهدف الأهداف العسكرية غير المدنية المرتبطة بشبكات المعلومات، من خلال السرقة، أو التلاعب بالمعلومات والبيانات العسكرية (عبد الجواد: 2020: 431). تشمل هذه الهجمات قيام قراصنة محترفين، أو جيوش نظامية إلكترونية بشن هجمات للسيطرة على نظم

القيادة والتحكم عن بعد، مما يؤدي إلى إخراج بعض منظومات الأسلحة عن سيطرة القيادة المركزية، وإعادة توجيهها نحو أهداف داخلية أو ضد دول صديقة، و يمكن أيضًا السيطرة على الطائرات من دون طيار، والغواصات النووية في أعماق البحار، أو الأقمار الصناعية العسكرية في الفضاء الخارجي، وإخراجها عن سيطرة الدولة المالكة لهذه الأسلحة والمعدات، وتزداد خطورة هذه الهجمات مع التطور التكنولوجي، واعتماد اللوجستيات ونظم القيادة والتحكم، وتحديد الأهداف وإصابتها على برامج الكمبيوتر، وشبكات الاتصالات (خليفة:2017: 57). كما تشمل التدخل في سلامة البيانات العسكرية الداخلية لدول أخرى، ومحاولات الإرباك والتشويش على أجهزتها، وسرقة تصميمات الأسلحة العسكرية والتقنيات التكنولوجية الحديثة ، فمثلا قيام قراصنة صينيين بشن هجمات على شركة (لوكهيد مارتن) الأمريكية، وسرقة معلومات عن تكنولوجيا تصنيع المقاتلة (أف 35)، التي استخدمتها الصين لاحقًا في تصميم وتصنيع مقاتلة (تي 20) الصينية (كلاع: 2022: 202).

وبهذا يمكن القول بأن التهديدات السيبرانية تستهدف مختلف المصالح والأهداف في مختلف المجالات والقطاعات ويمكن أن تصنف أهدافها إلى أربعة أهداف رئيسية بناء على ما تم ذكره أعلاه وتتلخص في الآتي:

1. الهدف الأول: الجانب المادي ويتعلق بالحصول على مكاسب أو موارد مادية من أموال، و معلومات.
2. الهدف الثاني: يتمثل في الاهداف الاقتصادية، وهي تلك التي تلحق الضرر بالاقتصاد، أو الاستفادة منه.
3. الهدف الثالث: الأهداف السياسية والعسكرية وهي التي تتعلق بالتأثير على السياسة، أو الحكم، أو في مسار العلاقات الدولية.
4. الهدف الرابع: الأهداف الاجتماعية التي تتعلق بالتأثير على الثقافة، أو النظام الاجتماعي.

5.2.1. الأطر النظرية المفسرة لموضوع السيبرانية :

تشمل مجموعة من المفاهيم، والقواعد، والنماذج، والأساليب التي تهدف إلى شرح وتحليل مختلف جوانب السيبرانية، و تتناول هذه الأطر المبادئ الأساسية من حيث التطور التاريخي، و التحديات الحالية، والتوقعات المستقبلية، وتستند هذه الأطر إلى نظريات علمية تساعد في فهم طبيعة السيبرانية على أنها علم مستقل، أو أنها جزء من علوم أخرى، و بناءً على ما سبق يتم تبني وسائل الدفاع والحماية من التهديدات السيبرانية من خلال تحليل نظرية الردع، وذلك على النحو التالي:

1.5.2.1.نظرية الردع السيبراني :

الردع هو حالة ذهنية تعكس تأثير دولة على دولة أخرى، حيث تختار الدولة المتأثرة عدم القيام بأفعال تتعارض مع مصالح الدولة المؤثرة، على الرغم من تجنب الدول الرادعة اتخاذ إجراءات معينة، لأنها تدرك أو تخشى أن تؤدي هذه الإجراءات إلى عواقب لا تُحتمل ، مما يؤثر سلبا على قرارات الدول(77:2015 :

Schreier)ويُعرَّف الردع السيبراني بأنه منع الأعمال الضارة التي تستهدف الأصول الوطنية في الفضاء الإلكتروني، والأصول الداعمة للعمليات الفضائية، ويستند على ثلاث ركائز أساسية تشكل عماد استراتيجية الدفاع السيبراني هي مصداقية الدفاع، والقدرة على الانتقام، والرغبة في الانتقام (قرة: 2019).

ويمكن توضيحها على النحو الآتي:

1. الركيزة الأولى مصداقية الدفاع: يتطلب الدفاع عن أنظمة المعلومات وردع أي محاولة لاختراقها توفر أنظمة نسخ احتياطية، وهذا يعني أن أي هجوم ناجح على هذه الأنظمة لا يمكن أن يؤدي إلى تدميرها كلياً، أو فقدان المعلومات التي تحتويها بشكل كامل، وعلى الرغم من ارتفاع تكلفة هذا الحل، فأنه يُعد الحل العملي الأكثر فعالية (البهي:2017).
2. الركيزة الثانية القدرة على الانتقام: يجب أن يتكبد المهاجم ضررًا يفوق ما وقع على المدافع من أضرار، وهذا يتطلب القدرة على الانتقام وتنفيذ هجمة سيبرانية أو أكثر ضد المهاجم الأصلي بعد التعرف عليه، وهذا أمر صعب تحقيقه (البهي: 2017).
3. الركيزة الثالثة الرغبة في الانتقام: يجب على المدافع أو من تعرض للهجوم أن يعلن عن رغبته في الانتقام من المهاجم، فامتلاك القدرة على الانتقام وحدها لا تكفي لردع المهاجم (البهي: 2017).

قد ظهرت نظرية الردع في العشرينيات والثلاثينيات من القرن الماضي، عندما اعتُبرت الطائرات القاذفة غير قابلة للإيقاف بوسائل الدفاع التقليدية لذلك، اعتقد الاستراتيجيون أن الهجمات واسعة النطاق على المدن يمكن منعها فقط إذا خشي الطرف الآخر من الهجمات المضادة ذات الحجم المماثل أو الأكبر، وبناءً على ذلك، أصبحت فكرة الردع تعتمد على التهديد بالانتقام لضمان عدم وقوع الهجوم الأولي، وكان *برنارد برودي* من أوائل من لاحظوا أن الهدف الرئيسي للمؤسسة العسكرية هو تجنب الحروب، حيث افترض *جيريمي بنثام* أن الأفراد العقلانيين يقومون بحسابات التكلفة والعائد قبل اتخاذ أي إجراء ومع ذلك، أثارت الشكوك حول نموذج الفاعل العقلاني بسبب التفكير الجماعي والسياسة البيروقراطية (Bendiek and Metzger:2015:555-556) .

وقد ازداد الاهتمام بنظرية الردع بعد الحرب العالمية الثانية ومع ظهور الأسلحة النووية، ومع ظهور السايبر، أصبحت مصطلحات الأمن والحرب والردع شائعة، واستكشف العلماء أوجه التشابه والاختلاف بين الردع النووي والسيبراني، مما أدى إلى تغيير التفكير الاستراتيجي في الأمن الحديث، وأصبحت القدرة على ردع التهديدات السيبرانية جزءًا أساسيًا من الاستراتيجيات الوطنية للأمن السيبراني، ومشابهة لجوانب الردع النووي(Samuel and Sharma :2019).

أما أصول الردع السيبراني فترجع إلى عملية عاصفة الصحراء عام 1991، حيث اكتسبت فكرة الثورة في الشؤون العسكرية شعبية كبيرة خلال المراحل الأولى من العملية التي شنتها الولايات المتحدة الإمريكية، التي عرفت بحرب المعلومات وهذا أدى إلى تشكيل أولى أدبيات الردع السيبراني في الحروب الحديثة (فرحات:272:2021). وفي عام 1994 صاغ البروفيسور جيمس دير ديريان مصطلح الردع السيبراني في

مجلة وايرد، مفكرًا في التأثير الرادع الذي قد تخلفه تقنيات الشبكات على ساحة المعركة المادية(will:2010:103).

وقد تناول العديد من الباحثين مدى إمكانية تطبيق نظرية الردع في الفضاء الإلكتروني، حيث تشكل النتائج المتعلقة بالملاءمة والقيود نقطة انطلاق أساسية لتوصيات صنع السياسات، وتتناول الانتقادات الموجهة للردع الكلاسيكي في هذا المجال الجديد نسبيًا، وتوضح كيف يختلف الردع السيبراني عن الردع التقليدي؟ بينما تتساءل الدراسات حول فعالية القدرات السيبرانية الهجومية في ردع الخصوم؟ وما إذا كان من الواجب أن يكون الانتقام التقليدي مطروحًا لضمان نجاح الردع؟ لاسيما أن فعالية الردع السيبراني تتطلب وجود مخطط شامل للقدرات الهجومية والدفاعية السيبرانية، مدعومًا بإطار قانوني دولي قوي (Bendiek and Metzger: 2015).

من خلال ما سبق يتضح لنا أن، نظرية الردع السيبراني من خلال تحديد الأهداف المحتملة في المجال السيبراني، والأساليب المستخدمة، ومستوى العمليات اللازمة للتعامل مع التهديدات بطرق هجومية ودفاعية، توضح الجدل الحاصل حول فعالية نظام الردع في العمليات السيبرانية؛ حيث يرى بعض الباحثين أنه يمكن تحقيق الردع في الفضاء الإلكتروني، بينما يرى آخرون بأن الردع غير ممكن بسبب صعوبة تحديد مصدر الهجمات وسرعة تدميرها، مما يعوق فعالية الردع ولتحقيق المصداقية، التي تعتبر عنصرا أساسيا في نظرية الردع، إذ يجب أن تكون القدرات معروفة وعلنية، وهذا الأمر يكاد أن يكون مستحيلًا في التكتيكات السيبرانية؛ لأن الكشف عن القدرات يجعلها عرضة للرقابة-46 :Valeriano and Maness: 2015) 47).

ويتضح لنا من خلال ما سبق أن عملية تحقيق الردع في الفضاء الإلكتروني تواجه صعوبات عديدة، وذلك لتعقيد البيئة التي يعمل فيها الإنترنت، يمكن توضيح هذه الصعوبات على النحو التالي:

1. صعوبة معرفة مصدر الهجمات (الطرف المعتدي) :كالهجمات الروسية على إستونيا عام م2007، والهجمات الأمريكية الصهيونية على المفاعل النووي الإيراني عام 2010م، لم يتم تبنيهما صراحة من قبل الدول المعتدية، بل أنكر بعضها القيام بها (خليل: 2023).
2. صعوبة وضع الخصم في تهديد حقيقي: أن الدول التي تتعرض لهجمات إلكترونية هي التي تستطيع ان تقدر مدى فداحة هذه الهجمات، والخسائر المترتبة عليها، ومن ثم فقد تقوم دولة بشن هجوم الكتروني انتقامي على دولة أخرى بهدف تحقيق الردع بالانتقام، لكن هذا الهجوم في تقدير الدولة المعتدى عليها غير مؤثر، وفي هذه الحالة يفشل تحقيق الردع (خليل:2023).
3. صعوبة منع الهجمات الصفرية في الفضاء الإلكتروني: يتم اختراع وتطوير فيروسات لم يتم الكشف عنها مسبقاً، فبعضها يصيب المكون المادي، وبعضها يصيب الجانب البرامجي، والبعض الآخر غير محدود ويركز على المعلومات، بهدف السرقة والتضليل، أو التدمير. كما أن هذه الفيروسات تستغل الثغرات الحديثة التي تظهر في الأنظمة، قبل ان يتم تحديثها ومعالجتها، وتستغلها بعض الفواعل لشن هجمة الكترونية قبل أن يتم اكتشافها، ومعالجتها من قبل الاجهزة المختصة (خليفة:2019: 164-165).

4. القيود القانونية في ميثاق الأمم المتحدة تجعل الردع في الفضاء الإلكتروني غير فعال: هذه القيود تتعلق بالجوانب القانونية والسياسية أكثر من الجوانب العسكرية، ووفقًا للمادة 51 من الميثاق، يجب على الدولة إبلاغ مجلس الأمن بأية تدابير هجومية تتخذها الدولة في حالة الدفاع عن النفس (خليفة:2019: 164-165).

وتؤكد نظرية الردع أن، مجرد امتلاك القدرة على الانتقام والتواصل الفعال لا يكفي؛ بل يجب أن يقتنع الطرف المهدد بأن التهديد بالانتقام، أو الضربة الاستباقية شي حقيقي، ويعد هذا الشرط هو الأصعب تحقيقًا على المستوى الوطني، وقد كان من غير المرجح أن تضحي الدول بالكثير لمنع انتشار أدوات وتقنيات الهجوم الإلكتروني. على الرغم من أنها تسبب أضرارًا مالية هائلة، وأن قادة العالم يزدادون قلقًا من التجسس السيبراني، وأن البنى التحتية الحيوية المتصلة بالإنترنت أصبحت الآن في خطر، بناء على هذه الأسباب فإن أي هجوم إلكتروني مستقبلي قد يغير هذا التصور إذا تسبب في تأثيرات كبيرة (Geers:2011: 113-120) وتتمثل المشكلة الرئيسية في الردع السيبراني، في كوننا ما زلنا في مرحلة مبكرة جدًا من العصر الإلكتروني، مما يجعل من الصعب تحديد مقدار الضرر الذي يمكن أن تتسبب فيه الدول، أو الجهات الفاعلة الأخرى من خلال الهجمات الإلكترونية، بالإضافة إلى أننا لا يمكن أن نعرف مدى فعالية قدرات المهاجمين في رد الانتقام، كما أن هناك الكثير من السرية حول قدرات الهجوم السيبراني الحالية على البقاء وذلك لغرض الانتقام (Schreier :2015: 80) .

كما أنه لا يوجد إجماع حول كيفية التعامل مع التفاعلات السيبرانية، لذا ينبغي على علماء العلاقات الدولية والأمن المساهمة في التقييم النظري للسيبرانية، وتطوير المفاهيم اللازمة لتحليلها، وقد أعرب العلماء عن شكوكهم حول أهمية الدراسات السيبرانية، مشيرين إلى عقبتين رئيسيتين تحولان دون ذلك (kello:20913:8-10) وهما :

الأولى: تتعلق بنقص الحالات المتاحة لاقتراح الادعاءات النظرية، واختبارها، وتنقيحها بشأن الظواهر الإلكترونية.

الثانية: تتعلق بمشكلة أكثر جوهرية في الدراسات السيبرانية، حيث يزعمون أن خصائص الظاهرة السيبرانية غير معروفة بشكل كافٍ .

وقد تساءل المنظرون عن كيفية منع التهديدات السيبرانية، أو الدفاع عنها في المستقبل، فأدرجوا الردع كأحد الأساليب الممكنة، ومن المهم الإشارة إلى أن الدول القومية تبنت استراتيجيتين أساسيتين لنظرية الردع التي وضعها *لورانس وفريدمان* (Samuel and sharma:2019:16) هي:

1. الردع عن طريق الإنكار وهو استراتيجية تهدف إلى منع الخصم من الحصول على التكنولوجيا، ويمكن ضبط الهجمات الإلكترونية في أوقات محددة مسبقًا، ولكن من الصعب حتى على الخبراء إزالة أدوات الهجوم كلها من الشبكات، وتهدف هذه الاستراتيجية إلى إقناع المهاجمين بأن فرص نجاحهم ضعيفة، وأن تكلفة الهجوم ستكون أعلى من الفوائد المتوقعة،

2. الردع عن طريق العقاب الذي يشير إلى استخدام التهديد بالانتقام لمنع العدوان، فإذا فشل الردع بالإنكار، فإن الدولة "س" تستخدم التكنولوجيا لتهديد الدولة "ص" والهدف هو، منع العدوان، ويعتمد هذا الردع على الخوف من رد قوي، وقد يؤدي حجم الانتقام إلى إلحاق ضرر أكبر مما يمكن للخصم تحمله(cheria and munish: 2019:16).

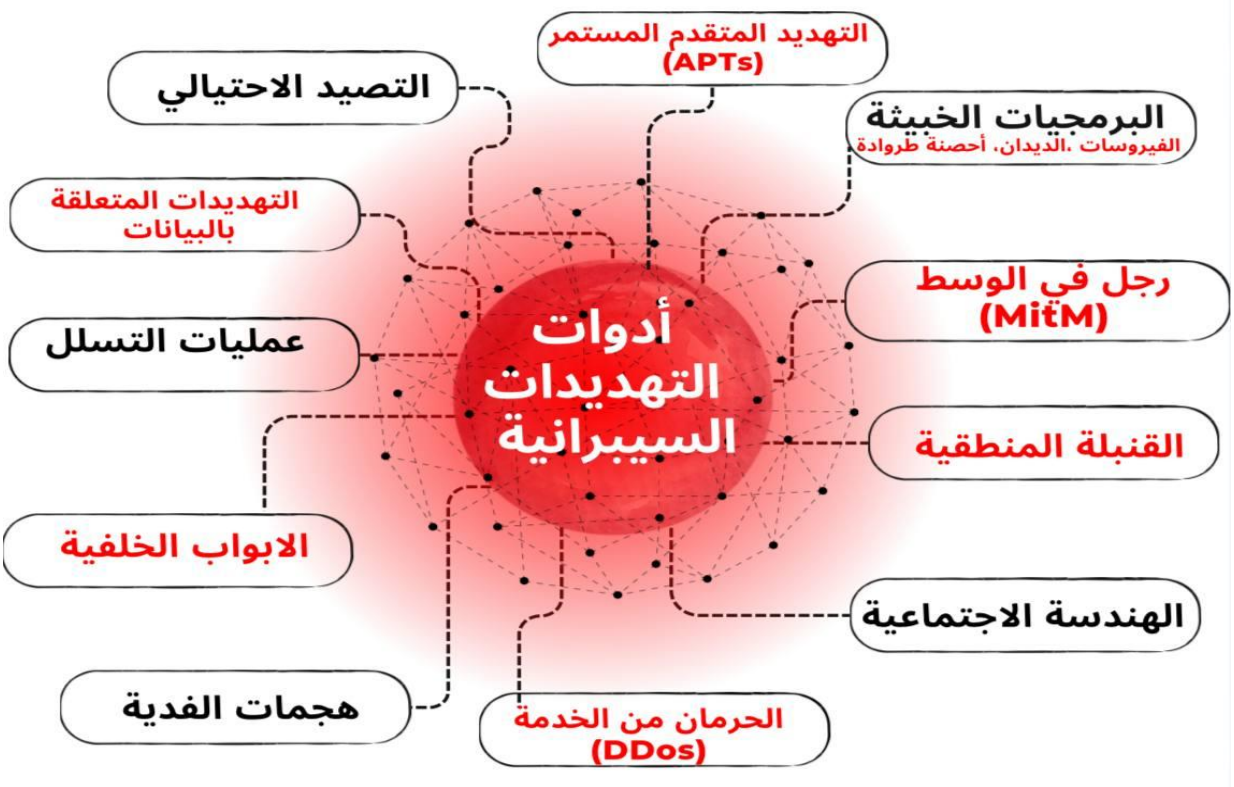
وبذلك فإن نماذج الردع المعروفة في الحروب التقليدية، وغير التقليدية (النووية، البيولوجية، والكيميائية) تفشل في هذه الحروب، فهي غير ممكنة في العالم المعلوماتي، إذ يتعذر إظهار القوة الإلكترونية المهاجمة لردع العدو عن الهجوم، فالردع بالانتقام، أو العقاب لا ينطبق على هذه الحروب؛ لأنه من الصعب أن يكون بمكان، بل ومن المستحيل في كثير من الأحيان تحديد مصدر الهجمات الإلكترونية، وحتى إذا ما تم تتبع مصدر الهجمات الإلكترونية، وتبيّن أنها تعود إلى دول محددة أو فاعلين غير حكوميين، فإنه في هذه الحالة لن يكون لديهم قواعد، أو فضاءات مادية يمكن الرد عليها من خلال استهدافها، كما أن بعض الهجمات قد تتطلب أشهراً لرصدها، مما يلغي فعالية الردع بالانتقام (عبد الواحد:2021: 43).

باختصار، يمكن القول بأن تطبيق نظرية الردع على مستوى دولة كاملة هو عملية معقدة ومتعددة الأبعاد، تتطلب توافر عدة عناصر وشروط، ومن أهم هذه العناصر القدرة على تحديد وتتبع مصدر التهديد السيبراني، ويعتبر من أكبر التحديات التي تواجه الردع السيبراني؛ بأنه يؤثر على المصداقية والفعالية والشرعية للرد، كما تتطلب القدرة على إلحاق ضرر مقبول ومتناسب بالخصم في حالة الهجوم، بالإضافة إلى القدرة على إظهار هذه القوة بطريقة مقنعة وواضحة للخصم، وذلك باستخدام عدة أساليب من بينها التصريحات الرسمية، و التجارب العسكرية، والتسريبات الإعلامية، والمفاوضات السرية، كما يجب أن تكون هناك قدرة على التواصل مع الخصم بطريقة فعالة ومنطقية؛ لإيصال رسالة التهديد، أو التحذير، أو المطالبة، وذلك عبر قنوات كالدبلوماسية، أو الاستخبارات، أو المنظمات الدولية، أو المجتمعات المدنية، لتصبح فكرة الردع ضرورية في الفضاء الإلكتروني، وجزء من الاستراتيجية الأمنية السيبرانية لأي دولة.

3.1. تحليل أدوات التهديدات السيبرانية وأنواعها:

1.3.1. أدوات التهديدات السيبرانية :

أدوات التهديدات السيبرانية التي تعرف أيضا بالسلاح السيبراني متنوعة بشكل كبير ولا يمكن تحديد الكثير منها وتصنيفها في دراسة واحدة نظراً لتعددها، لذلك سنركز في هذا المبحث على أبرز أدوات التهديدات وأكثرها شيوعاً في استهداف الدول، وسنقوم بتحليل هذه الأدوات بطريقة علمية لفهم أسلوبها وتأثيرها، كما هو موضح في الشكل رقم (3) الآتي :



الشكل رقم(3) يوضح مصادر التهديد السيبراني، المصدر: إعداد الباحثة

1.1.3.1.هجمات الحرمان من الخدمة(Distributed Denial of Service attacks) :

تُعد هذه الهجمات من أخطر أشكال الهجمات الإلكترونية، حيث يقوم المهاجمون بإطلاق هجمات ضخمة على الضحية تؤدي إلى إغراقها بالآلاف من الرسائل والطلبات، بانقطاع الخدمة ووقفها، سواء كان ذلك لموقع من مواقع الإنترنت، أو لخدمة إلكترونية خاصة أو حكومية (خليفة:2017: 42).

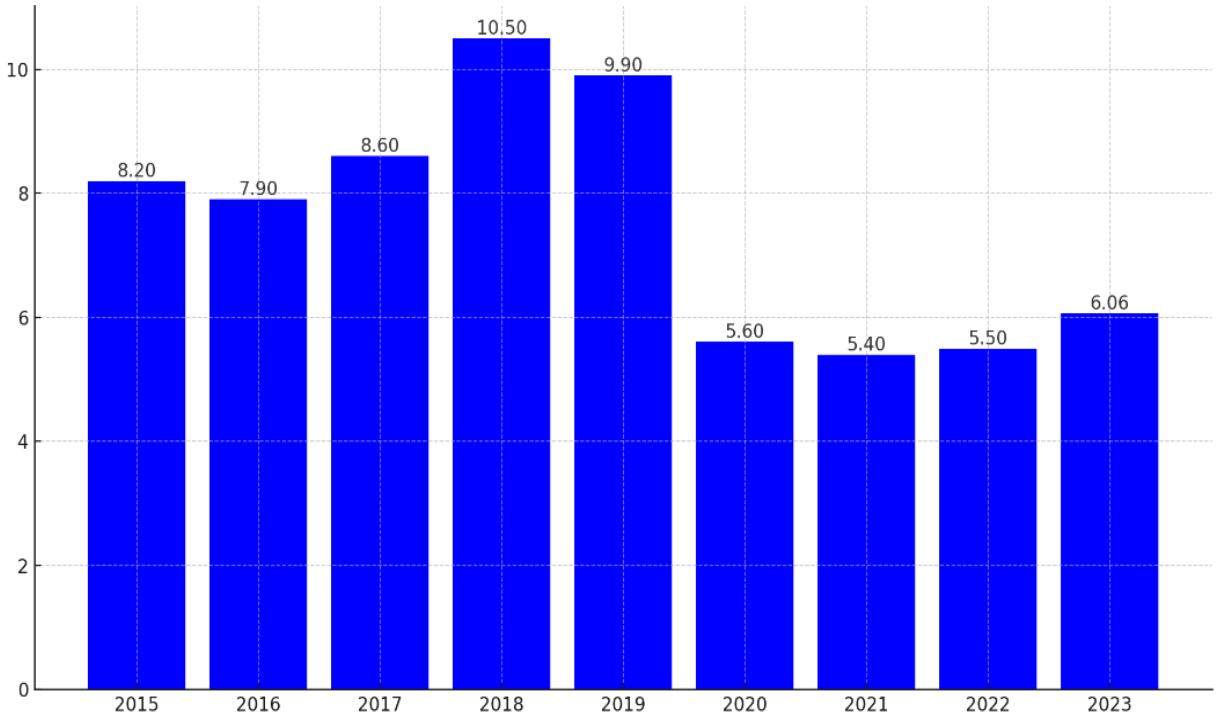
وتتسبب هذه الهجمات في العديد من الآثار السلبية، كالخسائر المالية للدولة المستهدفة، واهتزاز ثقة المواطنين في قدرة الأنظمة المعلوماتية للدولة على مواجهة تلك الهجمات، كما تؤدي إلى فقدان قدرة قطاعات الدولة على التواصل فيما بينها، مما يمكن للدولة المعتدية استغلال هذه الحالة؛ لنشر حملات عدائية، وإثارة الاضطرابات والفوضى؛ لتحقيق أهدافها (عبد العزيز: 2017: 4). تتميز هجمات DDoS بثلاث خصائص هي استغلال نقاط الضعف في البرامج، أو نظام التشغيل الخاص بالهدف، التي لا يمكن إصلاحها بسهولة، أيضا كل حزمة فردية هي طلب مشروع، ولكن معدل الحزم وحجمها الإجمالي يعطيان للهجوم تأثيره المدمر وأخيراً يتم قياس خطورة الهجوم من حيث مدته (Theohary and Rollins:2015:4) .

ويُعد رفض الخدمة ذا قيمة عسكرية كبيرة ووسيلة لتعطيل أنظمة الكمبيوتر الخاصة بالخصم، ويمكن أن تشمل الأهداف المحتملة شبكات القيادة والتحكم، وخوادم الملفات التي تحمل خطط المهام، وخوادم الويب التي تحمل اعتراضات اتصالات العدو(Janczewski and Colarik:2008:94) . فعلى سبيل المثال لا الحصر، عام 2014م، قامت كل من البي بي سي، ونيويورك تايمز، وغيرهما من المؤسسات الإخبارية الكبرى، بالترويج لهجوم رفض الخدمة، لكونه أكبر هجوم إلكتروني على الإطلاق (2015:12

Valeriano and Maness:). وتشير التقديرات إلى أن هجمات رفض الخدمة ضد، Yahoo و CNN و eBay، ومواقع التجارة الإلكترونية الأخرى، إلا أنها تسببت في خسائر تقدر بأكثر من مليار دولار، كما إنها تزعزع ثقة رجال الأعمال والأفراد في التجارة الإلكترونية(Denning:2000:3) .

2.1.3.1.البرمجيات الضارة، او الخبيثة (Types malwares) :

تعرف بأنها أي رمز برمجي مصمم للوصول غير مصرح به إلى أنظمة الكمبيوتر الخاصة، أو تعطيل عملياتها، أو حذف البيانات الحساسة، أو عرض إعلانات غير مرغوب فيها (Seissa and others:2015:181). إذ تعود فكرة فيروس، أو دودة الكمبيوتر إلى عام 1949م، عندما اقترح عالم الرياضيات جون فون نيومان(John Von Neumann) مفهوم التشغيل الآلي الذاتي، على الرغم من أن هذه البرمجيات الضارة قد ظلت في مرحلة تجريبية حتى أوائل التسعينيات(Geers:2011:22) الا أنها استمرت في الازدياد ويوضح الشكل رقم(4) تزايد هجمات البرمجيات الخبيثة على مستوى العالم من عام 2015 إلى 2023م.



الشكل رقم (4)عدد البرمجيات الخبيثة على مستوى العالم2015-2023م، المصدر (statista:2024)

يوضح الرسم البياني عدد هجمات البرمجيات الخبيثة في عام 2015م بلغ عددها 8.20 مليار هجوم وارتفع العدد عام 2018م بزيادة 10.50 مليار هجوم بزيادة قدرها 20% مقارنة بالسنوات الماضية، واستمر العدد في الانخفاض حتى عام 2021م بنسبة 5.40 مليار هجوم ووصل عدد الهجمات عام 2023م إلى 6.06 مليار هجوم على مستوى العالم. وسيتم توضيح هذه الأنواع على النحو التالي:

1. **الفيروسات(Viruses)** : يعرفها المركز القومي للحاسب الآلي في الولايات المتحدة الأمريكية بأنه برنامج مهاجم يصيب أنظمة الحواسيب بأسلوب يماثل إلى حد كبير أسلوب الفيروسات الحيوية التي تصيب الإنسان، حيث ينتشر عن طريق إدخال نفسه في الخلايا الحية ، ويقوم بالتجول في أنظمة الحاسب

الآلي، وعندما يجد أحد الأنظمة ينتج نسخة من نفسه لتدخل فيه، فيقوم البرنامج المصاب فيما بعد بتنفيذ أوامر هذا الفيروس (العيسي وعناب: 2018: 7).

يعود أول تصور لفيروس المعلوماتي إلى الدكتور فريد كوهن (Fred Cohen) الذي قدمه في محاضرة بجامعة كاليفورنيا، حول أمن الحاسب الآلي عام 1983م، حيث وضح بأن هذه الفيروسات تتميز بقدرتها على الاختفاء، والانتشار، والاختراق (الموصلي: 2021: 17). وتُعد هذه الفيروسات برمجيات خبيثة بطبيعتها، حيث تؤثر سلبًا على الحواسيب بشكل مباشر، وعلى غير الحواسيب بشكل غير مباشر، فعندما يقوم الفيروس بحذف ملفات مهمة من الجهة المستهدفة، يتعدى تأثيره الحاسوب ليشمل عدة أوجه من حذف، أو تعطيل ملفات وبرامج، أو زراعة برمجيات خبيثة أخرى تجسسيه، أو حتى تعطيل الجهاز كله (البيديري: 2021: 101). فعلى سبيل المثال عام 1990م استغرق فيروس (Nimda) 22 دقيقة فقط ليصبح الفيروس الأول في العالم (Janczewski and Colarik: 2008:28). ولا بد من الإشارة إلى أن عدد الفيروسات كبير جدًا، ولا يمكن تغطيته، ولكن سيتم التركيز على الفيروسات الأشهر التي سيتم ذكرها أثناء الدراسة، ومن أبرز هذه الفيروسات:

- فيروس دوكو (Duqo) الذي تم اكتشافه في سبتمبر عام 2011م، بواسطة معمل التشفير والأمن الالكتروني التابع لجامعة بودابست للاقتصاد والتكنولوجيا، وتتمثل الوظيفة الرئيسية لهذا الفيروس في التجسس على نظام التحكم الصناعي، وجمع المعلومات الاستخباراتية والاستراتيجية (خليفة: 201 : 120 - 121).
- فيروس فلام (Flame) تم اكتشافه عام 2012م، بواسطة فريق الاستجابة والطوارئ الإيراني، فضلا عن شركة كاسبر كي لاب، وقد أوضحت هذه الجهات أنه أكثر فيروس معقد تم العثور علية، حيث اصدرت الامم المتحدة تحذيرا اعتبرته الفيروس الأكثر خطورة الذي استهدف دول الشرق الاوسط بالأساس وتم العثور عليه في اكثر من 1000 جهاز في مؤسسات حكومية وتعليمية (خليفة : 2019 : 122).
- فيروس شمعون (Shamoon)تم اكتشافه في عام 2012م يمكن أن يكون هذا الفيروس مرتبطا بكلية سامي شمعون للهندسة، وهي أكبر كلية هندسة وأكثرها شهرة في الكيان الصهيوني ، يركز هذا الفيروس على قطاع الطاقة، وقد تم تصميمه لتدمير البيانات (Rid:2013: 63-64).
- فيروس نوت بيتا (Note Betty) تم اطلاق هذا الفيروس عام 2017م للشركات التجارية العالمية المتصلة بالشبكات، بواسطة آلية لتحديث البرامج لاحد برامج المحاسبة شائعة الاستعمال ، وفي غضون دقائق معدودة أصاب البرنامج الخبيث عشرات الآلاف من الأنظمة المتصلة بالأنترنت ، في اكثر من 65 دولة (عبد الجواد:2020:385-386).

2. **الديدان(Worms) :** هي نوع من البرامج الضارة التي لا تحتاج إلى ملف، أو برنامج آخر لتكرار نفسها، بل تكون مكتفية بذاتها (Janczewski and Colarik: 2008:2) . وصُممت هذه الديدان للقيام بأعمال تخريبية، كقطع الاتصال بالشبكة، أو سرقة البيانات الخاصة بالمستخدمين أثناء تصفحهم الإنترنت، و تمتاز هذه الديدان بسرعة انتشارها وصعوبة التخلص منها، وذلك لقدرتها الفائقة على التلون

والتناسخ والمراوغة، وغالبًا ما تُستخدم في حروب المعلومات، حيث تستهدف الشبكات المالية التي تعتمد على الحاسوب كشبكات البنوك، ومن أبرز هذه الديدان، دودة ستاكسنت (2009-2020). ويعتبرها بعضهم أول سلاح إلكتروني، وقد يكون لها تأثير تدميري دائم (theohary and rollins:2015:1) ويرى بعضهم أن وصولها نقطة تحول في عالم الأمن، ويعدها أخرون أنها أكثر البرامج الضارة تطورا على الإطلاق (Schreier:2015:87). وبصورة عامة يقوم "ستاكسنت" بمهاجمة أنظمة التحكم الصناعي المستخدمة على نطاق واسع في المنشآت المهمة مثل خطوط نقل النفط ومحطات توليد الكهرباء والمفاعلات النووية وغيرها من المنشآت الاستراتيجية الحسّاسة، وتقوم بالانتقال بين الأجهزة عبر أجهزة USB، مستغلةً إحدى نقاط الضعف في برنامج التشغيل (خليفة:2019: 121).

3. **أحصنة طروادة (Trojan Horse) :** يُعرّف حصان طروادة بأنه جزء متخصص من التعليمات البرمجية تم تصميمه لغرض مهاجمة نظام كمبيوتر معين، بطريقة تسمح للمهاجم بالوصول غير المصرح به والشامل إلى نظام كمبيوتر الضحية (Janczewski and Colarik:2008:155).

استمدت هذه البرامج تسميتها من حصان طروادة في التاريخ اليوناني (السدخان:2020: 206)، حيث تتسلل هذه البرامج إلى النظام المستهدف متخفيةً كبرنامج اعتيادية، وتتواجد عادةً داخل برامج كبيرة وشائعة الاستخدام (خليفة: 2019: 117).تتعدد طرق إرسال هذا النوع من البرامج وزراعته، ويعد استخدام البريد الإلكتروني من أبرز هذه الطرق، حيث يقوم المخترق بإرسال رسالة بريد إلكتروني إلى الضحية، مرفقة بملف يحتوي على حصان طروادة، و لعدم وعي الضحية بمحتوى الرسالة، يقوم بفتحها وتحميل الملف المرفق، معتقدًا أنه برنامج مفيد ويكتشف الضحية لاحقًا أن البرنامج لا يعمل، فيظن أنه معطل فيهمله في هذه الأثناء، وبهذا يكون حصان طروادة قد استقر في نظام الحاسب الآلي وبدأ في تنفيذ مهامه التجسسيه، حتى إذا قام الضحية بحذف البرنامج بعد ذلك، فإن ذلك لا يجدي نفعًا، حيث يكفي ملف حصان طروادة أن يعمل مرة واحدة فقط ليقوم بمهامه (الورفلي:2023: 132).

3.1.3.1. الأبواب الخلفية (Backdoors) :

هي برامج تُضاف بطريقة غير مرخصة إلى برمجيات أخرى؛ بهدف السماح بالوصول غير المصرح به إلى الشبكات، أو الأنظمة الحاسوبية (علي :2011: 246) وتُستخدم بشكل مقصود لأغراض عدة؛ كالتجسس، والمراقبة، أو جمع المعلومات (محمد:2022:455). وتلجأ بعض الشركات إلى هذه الأساليب لتمكين الدخول المباشر إلى أجهزة المستخدمين لإصلاح مشكلات فنية أو لجمع بيانات حول كيفية عمل الأجهزة، كما تسعى بعض المنظمات والمؤسسات الأمنية لاستخدامها في تحقيق أهداف معينة(خليفة:2019:105). أن الأنظمة والبرامج التي تُنتجها الولايات المتحدة الأمريكية غالبًا ما تحتوي على أبواب خلفية، ما يسمح لهيئات حرب المعلومات بالتنقل بحرية داخل أنظمة الدول عند الضرورة (طاجين: 2018: 26).

4.1.3.1. القنبلة المنطقية (Logic Bombs) :

تُعرف القنابل المنطقية بأنها شفرات برمجية تُدرج عمدًا في الأنظمة البرمجية بهدف تنفيذ وظائف ضارة عند توافر شروط معينة (عبد الواحد: 2021: 43). تُزرع هذه البرمجيات داخل النظام أو البرنامج أثناء تطويره، مما يعني أن المستهلك يحصل على البرنامج أو الجهاز مصابًا بالسلاح السيبراني منذ البداية، تُصمم هذه البرمجيات لتبدأ العمل عند حدوث أمر معين، أو تحت ظروف محددة، مما يمكن العدو في النهاية من السيطرة الكاملة على الجهاز، أو تدميره (خليفة: 2019: 117). كان أول هجوم إلكتروني شُنَّ عام 1982م، عندما تسببت قنبلة منطقية مزعومة في انفجار خط أنابيب نفط سوفيتي، خلال الحرب الباردة (Kello:2013:19). وفي عام1988م، تعرض الجيش الأمريكي لهجوم قنبلة منطقية أدى إلى حذف كميات كبيرة من البيانات. لاحقًا، أعاد الجيش تلك البيانات بعد إنفاق أكثر من 2.5 مليون دولار للتحقيق في المشكلة وإصلاح أنظمته (Awati and Fitzgibbons:2000) .

5.1.3.1. عمليات التسلل الدقيقة (Precision Infiltrations) :

في هذا النوع من الهجمات السيبرانية، يقوم المهاجم بمحو جميع البيانات داخل النظام، أو الشبكة الإلكترونية التابعة لدولة أخرى، فقد يتكرر الهجوم بهدف إفساد، أو تعطيل الملفات، أو التقاط المعلومات المتدفقة عبر الإنترنت، وتُعد هذه الأسلحة متطورة للغاية، وتستهدف العدو بشكل خاص، وذلك لفداحة تأثيرها، خاصة إذا كانت تستهدف البنى التحتية للدول (علي : 2017: 7).

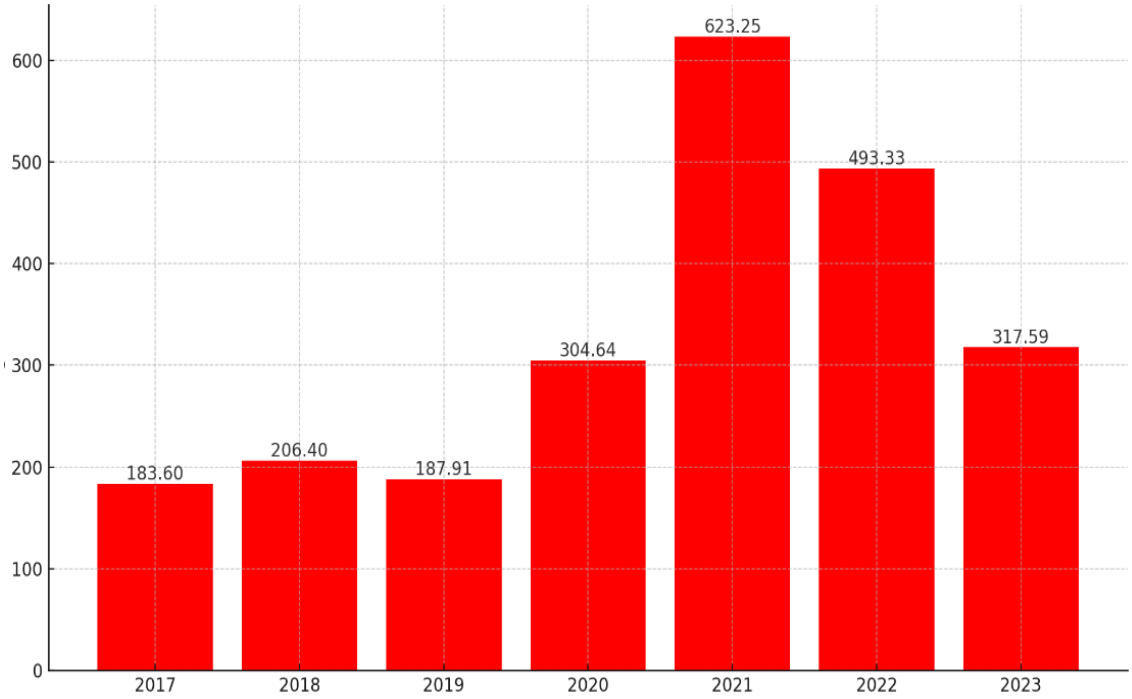
6.1.3.1. التصيد الاحتيالي (Phishing attacks) :

يعتمد التصيد الاحتيالي على (الهندسة الاجتماعية)، لتحفيز الضحية على فتح رابط يحتوي على برمجية خبيثة، وذلك عبر رسائل تتناول موضوعات تهم الضحية، أو تستخدم أسماء مألوفة لهم، وبمجرد فتح الرسالة تبدأ عملية القرصنة، فعلى سبيل المثال يعد البريد الإلكتروني والرسائل الشخصية وتطبيقات التواصل الاجتماعي من أكثر المنصات عرضة لهذه الهجمات (خليفة: 2017: 42). ويهدف هذا النوع من الهجمات إلى الحصول على معلومات شخصية تحت ستار شركة أو منظمة موثوقة، ووفقًا لدراسة نادي خبراء المعلومات، والأمن الرقمي الفرنسي، تعرضت 80% من الشركات الفرنسية لعمليات احتيال في عام 2018م، حيث أُرسلت آلاف الرسائل النصية القصيرة تعد المستلمين بتذاكر سفر مجانية على خطوط الطيران الفرنسية بمناسبة الذكرى السنوية الـ85 (بوقرص:2022: 69-70).

7.1.3.1. هجمات الفدية (Ransomware) :

تشمل هجمات الفدية تشفير البيانات على النظام المستهدف، مع مطالبة المستخدم بدفع فدية لاستعادة الوصول إلى بياناته، وتتفاوت هذه الهجمات من كونها مجرد إزعاج بسيط إلى حوادث خطيرة تهدد الشركات والمؤسسات الحكومية، والأفراد بشكل كبير، و معظم متغيرات برامج الفدية الحالية تقوم بتشفير الملفات، بينما قد تسمح بعض المتغيرات الأخرى بالملفات، أو تمنع الوصول إلى النظام بطرق مختلفة (السدخان: 2020: 207). فعلى سبيل المثال لا الحصر شنت يوم 12 مايو 2017م، مجموعة من القراصنة المجهولين، هجومًا باستخدام برمجية خبيثة تُعرف باسم أريد البكاء(WannaCry) ، مما أدى إلى إصابة أكثر من

200،000 ضحية في أكثر من 150 دولة خلال أول 48 ساعة فقط من الهجوم، مما جعل هذا اليوم يُعرف باليوم الأسود (خليفة:2017: 43). ومن بين الآثار الأخرى إمكانية استخدام البرامج الضارة التابعة للدولة، لتحقيق مكاسب مالية، أي أنه يمكن لمجرمي الإنترنت، أو المتسللين الأقل خبرة استخدام هذه البرمجيات، للحصول على فدية كبيرة من منشآت عدة، كالمصانع، أو محطات معالجة المياه، أو مرافق الطاقة، وقد ظهرت متغيرات أخرى من برامج الفدية الضارة مثل نوت بتيا (NotPetya) الذي انتشر من أوكرانيا (شوارتز: 2017).يوضح الشكل رقم (5) العدد السنوي لمحاولات برامج الفدية على مستوى العالم من عام 2017م إلى 2023م بملايين الهجمات.



المصدر (statista:2024) الشكل رقم(5) العدد السنوي لمحاولات برامج الفدية على مستوى العالم

يوضح الرسم البياني في عام 2017م اكتشفت المؤسسات في جميع أنحاء العالم بان عدد محاولات هجمات الفدية وصلت 183.60 مليون محاولة وبشكل عام ارتفع العدد حتى عام 2021م وصل 623.25 مليون محاولة، وانخفض هذا الرقم بشكل كبير إلى عام 2023م حوالي 317.59 مليون هجوم فدية .

8.1.3.1. التهديدات المتعلقة بالبيانات :

تُعد من أخطر الجرائم التي تهدد مستخدمي الإنترنت والخدمات الإلكترونية، حيث يمكن أن تتعرض البيانات للسرقة بهدف انتحال الشخصية، والاستيلاء على الممتلكات، مما يشكل خطرًا كبيرًا على مصالح المستخدمين، والخدمات الإلكترونية، والمؤسسات الحكومية (البابلي: 2021: 35). وتشمل هذه التهديدات سرقة المعلومات السرية سواء كانت اقتصادية كتجارة الشركات، أو استراتيجية، أو عسكرية بين الدول، كما تتضمن التعدي على الملكية الفكرية وقرصنة المعلومات، كسرقة البرامج الحاسوبية، وتوزيع المواد المكتوبة أو المصورة دون إذن المالك الشرعي، وقد أدى انتشار الإنترنت إلى تسهيل هذه العمليات وذلك لسهولة

النشر والتوزيع عبر الشبكة (العيسي وعناب: 2018: 7). وهذا قد يؤدي إلى تدمير المعلومات كلها (دحماني:33:2017). ومن الأمثلة على سرقة المعلومات العسكرية، الهجوم الذي استهدف حواسيب الجيش الأمريكي عام 2008م، باستخدام وصلة (USB) متصلة بكمبيوتر محمول في قاعدة عسكرية بالشرق الأوسط (جعفري: 2022: 249)، كما يمكن أن تتعرض البيانات المهمة للتعديل دون أن يكتشف الضحية ذلك، مما يؤدي إلى نتائج كارثية، خاصة إذا كانت تتعلق بخطط عسكرية أو مواعيد أو خرائط سرية (الشمري: 2021: 149).

في عام 2023م كانت 97% من الجهات الفاعلة تقوم باختراق البيانات لدوافع مالية، وبلغت التكلفة العالمية المتوسطة لاختراق لبيانات في عام 2024 حوالي 4.88 مليون دولار على مستوى العالم وهو ما يمثل زيادة بنسبة 10% عن العام الماضي (Varonis:2024).

9.1.3.1. هجمات رجل في الوسيط (Man in the middle Attacks) :

تُعرف بأنها بهجمات التنصت، وتحدث عندما يقوم المهاجمون بإدخال أنفسهم في معاملة ثنائية الأطراف، وبمجرد أن يتمكن المهاجمون من اعتراض حركة مرور البيانات، يصبح بإمكانهم تصفية البيانات وسرقتها (فرحاتي وقنيش: 610:2022). وهذا النوع من الهجمات يتضمن اعتراض المحادثات الجارية، أو نقل البيانات السرية بين طرفين (حمود: 2021). ويتم استخدامها في المجال العسكري؛ لإرباك العدو (السدخان:2020: 206).

10.1.3.1. التهديد المستمر المتقدم (Advanced Persistent Threat) :

هو نوع من الهجمات التي تُنفذ عادةً من قبل مجموعة قراصنة ترعاهم الدولة، أو عصابات الجريمة المنظمة، ويحدث هذا الهجوم عندما يستخدم مهاجم غير مصرح له تقنيات متقدمة للوصول إلى نظام أو شبكة وتُعتبر هجمات (APT) أكثر إثارة للقلق من الهجمات التقليدية، لتعقيدها العالي واستخدامها لتقنيات متطورة في البرمجيات الخبيثة، بالإضافة إلى استهدافها لشبكات أو خوادم معينة ؛ لجمع معلومات ذات قيمة، أو لإلحاق الضرر بأهداف محددة (Theohary:2019:7).

وقد تم استخدام مصطلح التهديد المستمر المتقدم لوصف أنشطة التجسس السيبراني التي تقوم بها الدول القومية، ومع هذا فإن المنظمات التي قد تكون أو لا تكون برعاية الدولة قد تستخدم أيضًا تقنيات التهديد المستمر المتقدم؛ وذلك للحصول على ميزة عسكرية تنافسية (schreier:2015:31). وفي عام 2013م، نشرت شركة الأمن الأميركية مانديانت تقريراً استخباراتياً من 60 صفحة، عن عملية صينية حددتها الشركة باسم(APT1)، والتي يزعم أنها سرقت مئات التيرابايت من البيانات من 141 منظمة على الأقل، عبر 20 صناعة في جميع أنحاء العالم منذ عام 2006م، وخلص تحليل مانديانت إلى أن (APT1) من المرجح أن تكون برعاية الحكومة، ويعتقد أنها تابع للمكتب الثاني لدائرة الأركان العامة لجيش التحرير الشعبي، وهي واحدة من أكثر الجهات الفاعلة إضراراً في الصين.(Theohary and Harrington: 2015:11)

11.1.3.1. الهندسة الاجتماعية (Social Engineering) :

تُعرف الهندسة الاجتماعية في سياق الأمن السيبراني بأنها عملية التلاعب بالأفراد لدفعهم إلى تنفيذ إجراءات، أو الكشف عن معلومات حساسة تفيد المهاجم، ويتم تحقيق ذلك عادةً من خلال بناء الثقة مع الضحية، ثم تحويل حالته النفسية إلى وضع يجعله أكثر عرضة لتعليمات المهاجم، فقد يتصل المهاجم بموظف في مؤسسة ويدعي أنه فني مكتب مساعدة، ويطلب من المستخدم الكشف عن معلومات كلمة المرور لغرض الصيانة، وقد تحدث هجمات الهندسة الاجتماعية عبر العديد من الوسائط حيث إنها لا تقتصر على المكالمات الهاتفية المقنعة فحسب (Janczewski and Colarik: 2008:191).وهي عملية إقناع الأفراد بتنفيذ رغبات معينة، وهذا المصطلح يُستخدم لوصف التقنيات والأساليب التي يلجأ إليها الأشخاص للحصول على معلومات حساسة بشكل غير مباشر، وبدون الوصول القانوني إلى تلك المعلومات (182: 2008 Janczewski and Colarik:).

عندما ننظر إلى استخدام أدوات التهديدات السيبرانية، نجد أنها تتميز بقدرتها الفتاكة على تعطيل أنظمة معينة وتدميرها، خاصة عند استهداف الأمن القومي لدولة ما، تختلف هذه الأدوات في أساليبها وتقنياتها، مما يجعلها أكثر فتكاً وصعوبة في اكتشافها وصدها، تتمثل أهمية دراسة هذه الأدوات في تحديد كيفية التصدي لها وتعزيز الجهود لحماية البنى التحتية والمعلومات الحيوية للدولة، فهذه الادوات وغيرها تؤثر بشكل كبير على الأمن القومي، حيث يُعتبر الفضاء الإلكتروني فضاءً واسعًا ومرنًا، وقد أخذت التهديدات السيبرانية بُعدًا إلكترونيًا مرتبطًا ارتباطًا وثيقًا بالتطور التكنولوجي الذي شهده العالم في السنوات الأخيرة.

2.3.1.أنواع التهديدات السيبرانية :

مع تطور الفضاء السيبراني وظهور دور الفواعل غير الدولية في النظام الدولي، برزت أنواع جديدة من التهديدات التي تعتمد على الإنترنت والتكنولوجيا الحديثة، ووفقًا لعالم السياسة جوزيف ناي(joseph Nye)، يمكن تصنيف المخاطر التي تهدد الأمن القومي إلى أربعة أنواع رئيسية وهي التجسس السيبراني، والجريمة السيبرانية، والحرب السيبرانية، والإرهاب السيبراني، تُعد الحرب والإرهاب التهديدين الأكثر تدميرًا في الفضاء السيبراني، بينما قد تكون تهديدات التجسس والجريمة أقل تدميرًا مقارنة بالحرب السيبرانية (van:2023: 15). ويمكن تُصنّيَف أنواع التهديدات السيبرانية إلى عدة مستويات، وذلك بناءً على طبيعتها وتأثيرها في المستوى الأول نجد القرصنة الإلكترونية، أو التخريب الإلكتروني، وفي المستويين الثاني والثالث، تبرز الجريمة العابرة للحدود والتجسس السيبراني، أما في المستوى الرابع فيأتي الإرهاب السيبراني، وفي المستوى الأخير، الذي يعد الأخطر، نجد الحرب السيبرانية وسيتم توضيح هذه الأنواع كما هو موضح في الشكل رقم (6)الآتي:

الشكل رقم (6) أنواع التهديدات السيبراني المصدر: إعداد الباحثة

1.2.3.1.القرصنة الإلكترونية (Cyber Conflict) :

يعرف فرنكلاين كرامر (Franklin Kramer) القرصنة الإلكترونية بأنها تلاعب بالمعلومات الرقمية، لتعزيز أيديولوجية سياسية، وغالبًا ما يستهدف المخترقون صناع القرار بشكل مباشر؛ للتعبير عن عدم رضاهم عن السياسات المختلفة (Kramers and others :2009: 538) .

وتُعد القرصنة من أقوى الأسلحة السيبرانية في الفضاء الرقمي وأشملها، حيث تعتمد هذه الأداة التقنية على تجنيد أفراد ذوي الكفاءة العالية للتعامل مع الحاسوب، ويُعرفون بالهاكرز، ويتمتع هؤلاء الأفراد بقدرة فائقة على اختراق مختلف وسائل الاتصالات، والنظم التكنولوجية، بما في ذلك الحواسيب والهواتف والموجات وغيرها، مما يجعلهم قادرين على تنفيذ عمليات معقدة في الصراع السيبراني (خالد ومحمد: 20:2020) .

ويسعى المخترقون، من خلال هذه الهجمات، إلى التأثير على آراء الجمهور، من خلال تشويه سمعة الجهات المستهدفة، أو التدخل في العمليات الديمقراطية، كما أنهم يحاولون التأثير على سلوك، السياسيين أو قرارات المسؤولين، أو إخضاعهم للابتزاز والتهديد، وتتضمن القرصنة السيبرانية عمليات تعديل، أو تغيير محتوى معين أو تخريبه؛ لخدمة مصالح جهة محددة ومن أمثلة ذلك، قرصنة المواقع الإلكترونية، أو تعطيل الخوادم من خلال إغراقها بالبيانات (علي: 2017: ص 240). حيث يتمكن قراصنة الحاسوب من الوصول إلى المعلومات السرية والشخصية، واختراق الخصوصية بسهولة، ويرجع السبب في هذا إلى التطور الكبير الحاصل في مجال الحاسب الآلي والشبكات المعلوماتية، وما صاحبه من تقدم في الجرائم المعلوماتية، وطرق ارتكابها، بالإضافة إلى أن مرتكبي هذه الجرائم ليسوا مستخدمين اعتياديين، بل يمتلكون خبرة فائقة في مجال الحاسوب (عبد الجواد:2020: 409).

وتتضمن القرصنة الإلكترونية عدة أنواع من الفاعلين، كالهاكرز، والكراكرز، ويُعرف الهاكرز بأنهم مبرمجون محترفون قادرون على التعامل مع مشكلات الكمبيوتر وتقديم حلول برمجية تطوعية، ويستخدمون تقنيات وبرامج لاختراق الأنظمة والوصول إلى معلومات سرية (الشمري: 2021: 148) وغالبًا ما يسعون لتحقيق أهداف ربحية، أو سياسية، أو أيديولوجية (طاجين، 2018، ص 23). على سبيل المثال مجموعة أنونيموس، تُعد من أبرز القراصنة السياسيين، حيث تضم عددًا كبيرًا من القراصنة المنتشرين حول العالم، ويعتمد هؤلاء القراصنة على مهاراتهم للوصول بطرق غير قانونية إلى معلومات مخترقة، ويجعلونها متاحة للجمهور (مهدي: 2020: 157). وتتراوح أنشطة هذه المجموعات من هجمات رفض الخدمة التي تسبب إزعاجًا وتشويهًا لمواقع الويب، إلى تعطيل العمليات التجارية الحكومية والخاصة (Theohary and Rollins:2015:3).

القرصنة الإلكترونية عملية تشمل نسخ البرمجيات غير المصرح بها، أو إعادة إنتاجها، أو استخدامها، أو تصنيع نسخ منها بطرق غير شرعية، أو نشر وتوزيع المنتج البرمجي، أو استغلاله ماديًا، أو تقليده، أو محاكاته، مما يخل بحقوق الدول والمؤسسات، دون الحصول على إذن أو تفويض (عبدالجواد: 2020: 408). ومن أبرز هؤلاء القراصنة (باتريوت) وتتمثل دوافعهم الرئيسية في مساعدة، الدولة أو دعمها، في صراع أو حرب مستمرة في العالم الحقيقي، من خلال تنفيذ العديد من الإجراءات التخريبية الموجهة في الفضاء الإلكتروني نحو عدو الدولة (Sigholm:2016:16).

وتُعد ظاهرة ويكيليكس (Wikileaks)، التي ظهرت عام 2007م، من أبرز الأمثلة على الجماعات الاحتجاجية المنتشرة في الفضاء الإلكتروني، وتهدف هذه الجماعة إلى تحقيق أهداف سياسية من خلال توزيع المعلومات السرية، وتشويه المواقع، وتوليد احتجاجات حول القضايا السياسية، وتمثل هذه الظاهرة نمطًا جديدًا من الفاعلين السياسيين، الذين يعتمدون على إخفاء الهوية، والقيادة غير المركزية، والانخراط الفردي دون عضوية دائمة، وتنفيذ هجمات افتراضية ضد أهداف مادية، بهدف تشجيع التغيير السياسي (علي :2017: 8). وقد نجحت ويكيليكس في نشر ملايين الوثائق السرية، المتعلقة بالحكومة الأمريكية وقنصلياتها، وقد أدى هذا إلى خلق مشاكل دبلوماسية بين الولايات المتحدة وحلفائها (طالة: 2020: 57).

2.2.3.1.التجسس السيبراني(Cyber Espionage) :

يُستخدم التجسس السيبراني لجمع المعلومات، وغالبا ما تكون دوافع استخدامه مالية، ويمكن أن تكون له تأثيرات استراتيجية خطيرة تهدد قطاعات واسعة، قد تكون عسكرية، أو سياسية، أو صناعية، أو تقنية (دحماني:63:2017). كما أنه من الممكن أن تكون أعمال التجسس السيبراني أكثر انتشارا من أعمال الحرب السيبرانية (schreier:2015:9). والتجسس السيبراني هم أفراد يسرقون معلومات سرية، أو مملوكة، تستخدمها الحكومات، أو الشركات الخاصة، لاكتساب ميزة تنافسية استراتيجية، أو أمنية، أو مالية، أو سياسية، وغالبًا ما يعمل هؤلاء الأفراد بناءً على طلب من الكيانات الحكومية الأجنبية ويتلقون التوجيه منها) (theohary and rollins:2015:2. ومن بين النماذج الأولى للتجسس السيبراني، حادثة (متاهة ضوء القمر)، وهو اسم أُطلق على عملية تجسس إلكتروني سرية للغاية، اكتُشفت في عام 1999م وقد اكتشف سلاح

الجو الأمريكي هذا الاختراق بالصدفة، مما دفعه لتنبيه مكتب التحقيقات الفيدرالي (FBI) واستدعى المحققون الفيدراليون وكالة الأمن القومي الأمريكية (NSA) ناسا، وكشف التحقيق عن نمط من التسلل إلى أجهزة الكمبيوتر في الإدارة الوطنية للملاحة الجوية، ووزارة الطاقة، والجامعات، والمعامل البحثية، حيث بدأت هذه التسللات في مارس 1998م، وقد تم خلالها نسخ خرائط للمنشآت العسكرية، وتصميمات الأجهزة وغيرها من المعلومات الحساسة (Rid:2013:9).

وتتعدد مجالات التجسس الإلكتروني بتنوع أنشطته فمثلا، في المجال التجاري تركز العمليات على كشف الأسرار التسويقية والتجارية، أما في المجال الصناعي والتقني، فتهدف إلى كشف نتائج الأبحاث والتطورات والبيانات المتعلقة بعمليات الإنتاج، وأسرار تصميم المنتجات، وخاصة تصميمات الشرائح الصغيرة من أشباه الموصلات، وفي المجالات العسكرية والاستخباراتية والنووية، تُكثف الجهود لاختراق الأنظمة الأمنية، والعسكرية، والاستخباراتية، والنووية، وذلك للوصول إلى أدق تفاصيل البيانات والمعلومات المتعلقة بهذه المجالات، مما يؤثر بشكل كبير على أمن الدول والحكومات واستمراريتها (الورفلي: 2023: 132).

ويعتبر التجسس السيبراني من الأساليب التي تعتمد عليها التنظيمات الإجرامية والإرهابية، لجمع معلومات حساسة عن المؤسسات والقطاعات الحكومية، والعسكرية، والسياسية، والاقتصادية، وتهدف هذه المعلومات إلى الإضرار بالمجتمع ومصالحه، ويتم التجسس السيبراني عبر اختراق المواقع والصفحات الإلكترونية على الإنترنت، بهدف التجسس، أو التنصت على البيانات والمعلومات النصية، أو الصوتية، أو المرئية التي تهم الجهة المستفيدة من التجسس، كما يمكن أن يتم التجسس من خلال إرسال رسائل بريد إلكتروني، تحتوي على ملفات برمجية وقادرة على إرسال المعلومات المتوفرة على جهاز المستخدم بشكل آلي، سواء كانت نصية، أو صوتية، أو مرئية (عبد الجواد: 2020: 416-418). فعلى سبيل المثال اكتشفت مجموعة بحث كندية تُعرف باسم (Information Warfare Monitor) ، عام2009م، شبكة تجسس إلكترونية تُدعى (Ghost Net)، حيث تضمنت هذه الشبكة أكثر من 1000 جهاز كمبيوتر مخترق في 103 دول، استهدفت معلومات دبلوماسية وسياسية واقتصادية وعسكرية (Geers :2011 :21).

يعرف التجسس السيبراني بأنه استخدام إجراءات استخباراتية خطيرة، وهجومية للتفاعل في الفضاء الإلكتروني(Valeriano and Maness:2015:67). ويهدف إلى إحداث خسائر اقتصادية، أو سرقة الابتكارات والأبحاث والمفاوضات السرية وغيرها... (عبد العزيز: 5:2017). ويُعرف أيضا بأنه، عملية تقوم بها دولة أو جهاز تابع لها، أو وكيل عنها، للوصول إلى البيانات السرية التي لا تتاح للجمهور، والبيانات المحفوظة على أنظمة تكنولوجيا المعلومات، أو شبكات الكمبيوتر في منطقة تخضع لولاية دولة أخرى ونسخها، ويتم تنفيذ هذه العمليات بسرية تامة، وباستخدام ذرائع مزيفة، أو كاذبة، دون الحصول على تراخيص، أو موافقة من مالكي أو مشغلي هذه الأنظمة، أو شبكات الحاسوب المستهدفة، أو الدولة الإقليمية (ولي: 2022: 90). ويمكن تعريفه بأنه، استخدام مجموعة من الأساليب لاختراق الأنظمة الإلكترونية، بهدف سرقة معلومات قد تكون ذات أهمية وخطورة كبيرة للطرف المستهدف، والمستفيد من هذه المعلومات (عبد

الجواد: 2020: 416) ويمكن التنبية إلى أنه توجد ثلاث تناقضات تحد من نطاق التجسس السيبراني (Rid:2013: 82-84). نلخصها في الآتي:

1- الخطر: على الرغم من أن التجسس السيبراني لا يُعد عملاً حربياً، ولا يُصنف على أنه سلاح أو هجوم مسلح، فأنه قد يمثل تهديداً كبيراً للاقتصادات الأكثر تطوراً في العالم.

2- الأهمية: قد يكون التجسس السيبراني الشكل الأكثر أهمية للهجمات السيبرانية، على الرغم من أنه قد لا يُحدث تغيراً جذرياً في قواعد اللعبة بالنسبة لوكالات الاستخبارت.

3- التطبيع: عندما تتعامل وكالة استخبارات بجدية مع العمليات السيبرانية، فإنها تدعم هذه العمليات بمصادر بشرية ومخبرين ذوي خبرة، وعملاء متخصصين، مما يؤدي إلى نقل مفهوم التجسس السيبراني تدريجياً من العالم السيبراني إلى الأساليب التقليدية لوكالات الاستخبارات.

ونستنتج بأن التجسس السيبراني يبرز تحديًا آخر يواجه الردع السيبراني، وهو غياب الثقة، لوجود نقص في القوانين والأعراف الدولية التي تحدد السلوك المقبول وغير المقبول في الفضاء الإلكتروني، وهذا الوضع يجعل من الصعب على الدول أن تكون مطمئنة لكونها لن تتعرض لهجمات سيبرانية إذا امتنعت عن استهداف الآخرين.

3.2.3.1. الإرهاب السيبراني (Cyber Terrorism) :

يُعتبر هذا النوع من الإرهاب تطورًا حديثًا لمفهوم الإرهاب التقليدي، حيث يشمل استخدام تكنولوجيا المعلومات والاتصالات من قبل الجماعات الإرهابية لتحقيق أهدافها، وقد ظهر هذا المصطلح عام 1996م، وقد اكتسب شهرة واسعة بعد تبنيه من قبل القوات المسلحة الأمريكية (Janczewski and Colarik 2008: 14) وازدادت أهمية هذا المفهوم بعد أحداث 11 سبتمبر، حيث لوحظت زيادة في الهجمات الإرهابية عبر الإنترنت.(DCAF: 2015:1).

ويمثل الإرهاب السيبراني تهديدًا واضحًا للأمن القومي للدول، حيث يتم استخدام التقنيات الذكية لتنفيذ هجمات إرهابية عبر الفضاء الإلكتروني، أو استخدام الروبوتات والطائرات من دون طيار، وأحيانا الطابعات ثلاثية الأبعاد لتصنيع الأسلحة (محمد: 2022: 456). وتتجلى خطورة هذا النوع من الإرهاب في حجم التهديدات التي يفرضها على الأمن القومي (لطفي: 1:2022). وفي هذا السياق، يحذر مسؤولو المخابرات الأمريكية؛ كمدير وكالة المخابرات المركزية السابق جيمس وولزي(James Woolsey)، من أن الجماعات الإرهابية ستتمكن من امتلاك أسلحة إلكترونية ذات أهمية استراتيجية في المستقبل القريب(Geers:2011:98) .

وغالبًا ما يرتبط الإرهاب السيبراني بتنفيذ هجمات، لتحقيق أهداف سياسية واجتماعية فمثلا في عام 1998م، قامت جماعة إرهابية مسلحة بإغراق السفارات السريلانكية بـ 800 رسالة بريد إلكتروني يوميًا و لمدة أسبوعين، وقد كانت هذه الرسائل تحتوي على عبارة نحن نمور الإنترنت السوداء، ونقوم بذلك لتعطيل اتصالالتكم(Janczewski and Colarik: 2008:3). وقد وصفت وكالات الاستخبارات السريلانكية، أنذاك، هذا الهجوم بأنه أول هجوم معروف من قبل الإرهابيين ضد أنظمة الكمبيوتر في دولة ما . (Denning:2000:5)

هذا وقد بدأ استخدام مصطلح الإرهاب السيبراني في ثمانينيات القرن العشرين، حيث أشار باري كولن (Barry Collon)في دراسته إلى صعوبة تعريف هذه المفهوم (لطفي: 2022: 10). ومع ذلك قدم تعريفًا أوليًا للإرهاب السيبراني، لكونه هجومًا إلكترونيًا يهدف إلى تهديد الحكومات أو العدوان؛ لتحقيق أهداف سياسية، أو دينية، أو أيديولوجية، ويجب أن يكون للهجوم تأثير مدمر ومخرب يعادل الأفعال المادية للإرهاب (محمد:2022: 456). ويعتمد هذا التعريف على استخدام أنظمة تكنولوجيا المعلومات، أو الاتصالات لمهاجمة، أو تخريب، أو تعطيل، أو اختراق، أو سرقة، أو تزوير، أو تلاعب بالمعلومات، أو البرامج، أو الأجهزة، أو الشبكات، و يسعى هذا الهجوم إلى تغيير حالة معينة، أو إحداث تأثير محدد على المستوى السياسي، أو الديني، أو الأيديولوجي، ويستند إلى فكرة أن الإرهاب السيبراني يجب أن يكون مكافئًا للأفعال المادية للإرهاب، وأن يحقق نفس المستوى من العنف، والتخويف، والتأثير.

ويعرفه حلف شمال الأطلسي (الناتو) بأنه، هجوم إلكتروني يستغل شبكات الكمبيوتر، أو الاتصالات، لإحداث دمار كافٍ، ولنشر الخوف، أو ترهيب المجتمع، وذلك بهدف تحقيق غاية أيديولوجية Seissa and ohers:2015:181). ويمكن القول، أن تعريف حلف الناتو للإرهاب السيبراني يركز على استخدام التقنية الحديثة لتحقيق أهداف إرهابية تقليدية، مع التركيز على التأثير النفسي والاجتماعي للهجمات.

ويعرف جيمس لويس(James Lewiss)، الباحث والخبير في مجال الأمن السيبراني والسياسة التكنولوجية، الإرهاب السيبراني بأنه، استخدام أدوات شبكة الكمبيوتر لتدمير البنى التحتية الوطنية الحيوية أو تعطيلها كالطاقة، والنقل، والعمليات الحكومية، أو بهدف ترهيب الحكومة والمدنيين (Lewis:2002:1). ويلخص هذا التعريف استخدام الإنترنت لتدمير المصادر الحيوية، أو التأثير على الحكومة، أو المجتمع بدافع إرهابي.

كل تعريف من التعريفات السابقة للإرهاب السيبراني، يسعى إلى توضيح ماهيته، ومميزاته، ومخاطرة، مستخدمًا مصطلحات ومفاهيم مختلفة، تعكس وجهة نظر وخلفية الكاتب، أو المؤسسة التي صاغته، ولا يوجد تعريف موحد، أو مقبول بشكل عام للإرهاب السيبراني، ويمكننا تعريف الإرهاب السيبراني إجرائيا على أنه، استخدام التقنية الحديثة للتهديد، أو العنف بطريقة غير قانونية، من قبل فواعل متعددين، بهدف استهداف أنظمة المعلومات والبنية التحتية، لأغراض سياسية أو أيديولوجية، ويميز بعض الباحثين بين نوعين من الإرهاب السيبراني وهما :

النوع الأول: الإرهاب السيبراني الخالص (Pure Cyber Terrorism) ويتضمن هجمات مباشرة على البنية التحتية للضحية، لتحقيق أهداف متنوعة، يركز على التلاعب وإفساد وظائف أنظمة المعلومات، وتدمير الأصول الافتراضية والمادية، باستخدام فيروسات الكمبيوتر، والديدان، وأحصنة طروادة، والهجمات الفدية (العمري: 2020: 79-80).

النوع الثاني: الإرهاب السيبراني الهجين (Hybrid Cyber Terrorism) حيث يستخدم الإرهابيون الفضاء الإلكتروني في أنشطة متعددة كالدعاية، والحرب النفسية، والتخطيط لهجمات إرهابية فعلية، و تجنيد أعضاء جدد، وجمع الأموال والتبرعات (البهمي: 2019).

4.2.3.1. الحرب السيبرانية(Cyber War) :

ظهرت الحرب السيبرانية بشكل فعلي على الساحة الأمنية والمعلوماتية في منتصف العقد الأول من القرن الحالي، مما أحدث تحولًا نوعيًا في مفهوم الحروب التقليدية من حيث الوسائل والأهداف والنتائج (عبد العزيز: 2017: 3) وتشير التحليلات الحالية إلى أن حرب القرن الحادي والعشرين ستكون معتمدة على المعلومات بقدر اعتمادها على الأسلحة النارية، وستكون هذه الحرب مشابهة لـ(الحرب الخاطفة) التي وقعت في القرن العشرين، حيث سيكون الهدف العسكري الرئيسي هو تحويل ميزان التحكم في المعلومات لصالح الفرد، خاصة إذا لم يكن ميزان القوى التقليدية كذلك (Geers:2011:25-26).

وفي هذا السياق، اقترح رئيس قسم الحرب السيبرانية الصينية، *داي كوينجمن* عام 2003م، بأن تستعد الصين لحرب سيبرانية تتضمن سلسلة من الهجمات الإلكترونية، مما يستدعي الإعداد والتنسيق في العمليات العسكرية؛ لصد الهجمات السيبرانية المضادة (الفتلاوي: 2016: 620). أما الرئيس الأمريكي السابق *(باراك أوباما)* فقد قال "من الواضح الآن أن الحرب السيبرانية هي أحد أخطر التهديدات الاقتصادية، وأخطر تحديات الأمن القومي التي نوجهها كأمة" (Andress and Winterfeld:2011:240).

وتُعد الحرب السيبرانية الميدان الرابع من ميادين الحروب، حيث تتسم بكونها صراعات خفية تقتحم الأنظمة الإلكترونية، وتسبق العمليات العسكرية التقليدية (لطفي: 2022: 12). ويعكس هذا الأمر عمق الخطر الاستراتيجي لهذه الحرب، مما دفع معظم دول العالم إلى وضع الأمن المعلوماتي والسيبراني في مقدمة أولويات الأمن القومي (عبد العزيز: 2017: 2).

وفي عام 1993م، تناولت مقالة نشرتها كلية الدراسات العليا البحرية الأمريكية (NPS) الجوانب التاريخية للحرب السيبرانية، حيث جادل مؤلفوها بأن، ثورة المعلومات لن تغير كيفية خوض الحروب فقط، بل ستؤثر أيضًا على أسباب خوضها (Geers :2011:25). وتشمل الحرب السيبرانية، التجسس على الدول، وسرقة الأسرار التجارية والعسكرية، بالإضافة إلى مهاجمة أجهزة الكمبيوتر المسؤولة عن تشغيل البنية التحتية الحيوية، وأنظمة الأسلحة، واختراق المعلومات الأمنية والاقتصادية الحساسة، كما تستهدف مرافق الخدمات الحيوية، أو تلك المتعلقة بالأمن القومي للدول التي تُعتبر معادية (يونيبات:2022:1). ولأن هذه الحرب تُعد حربًا غير تقليدية وغير متكافئة، فمن المرجح أن تستثمر الدول الأضعف فيها وسيلة لتعويض ذلك الضعف في القوة العسكرية التقليدية، حيث أنه من الأسهل الحصول على سلاح سيبراني، مقارنةً بالحصول على دبابة أو بندقية (Geers:2011: 98).

وتختلف الأسلحة السيبرانية المستخدمة في هذه الحرب عن الأسلحة التقليدية، حيث لا تنتهي صلاحيتها بمجرد استخدامها، ويمكن أن يكون لها عمر غير محدود، كما أنه من الممكن تطوير الأساليب المستخدمة في هجوم إلكتروني واحد، مما يجعل هذه الأسلحة أكثر خطورة من الأسلحة التقليدية (Valeriano and Maness:2015:61).ففي منتصف التسعينات من القرن الماضي، أوضحت دراسة أجرتها مؤسسة راند (Rand Corporation)أن تكاليف تطوير الأسلحة السيبرانية اللازمة لإجراء الحرب السيبرانية متواضعة للغاية، مما يجعلها في متناول معظم الدول، وفي تقرير وضعته (Spy-Ops) في عام 2007م، تبين أن حوالي 140 دولة لديها برامج نشطة لتطوير الأسلحة السيبرانية وتشغيلها (فرحات: 2022: 682-683).

ظهرت فكرة الحرب السيبرانية أول مرة عام 1997م، عندما كتب (جون أركيلا John Arquilla)، و(ديفيد رونفيلدت David Ronfeldt) ، مقالًا بعنوان الحرب السيبرانية قادمة (Cyber War is Coming) وعرَّفها الكاتبان بأنها، تنفيذ العمليات العسكرية والاستعداد لها، وفقًا للمبادئ المعلوماتية، من خلال تعطيل، أو تدمير نظم المعلومات، والاتصالات على نطاق واسع، كما أنهما وسعا مفهوم الحرب السيبرانية ليشمل أبعادًا غير مادية، كتدمير العقيدة العسكرية للعدو، والتي تشكل الأساس الذي يعتمد عليه في تحديد هويته، وخططه، وتصرفاته، وأهدافه، والتحديات التي يوجهها (خليفة: 2019: 146-147).

ويعرِّف ريتشارد كلارك (Richard Clarke) وروبرت كناك(Robert Knaack) في كتابهما Cyber War: The Next Threat to National Security and What to Do About It (2010) الحرب السيبرانية بأنها الإجراءات التي تقوم بها دولة ما، لاختراق أجهزة الكمبيوتر، أو الشبكات الخاصة بدولة أخرى، وذلك بهدف إلحاق أضرار جسيمة بها، أو تعطيلها (Abdyraeva:2020:16). ويستند هذا التعريف إلى فكرة أن الحرب هي صراع القوة بين الدول، وأن الإنترنت يمثل ساحة جديدة لهذا الصراع.

وعُرِفت في دراسة لمركز أبحاث الكونجرس في الولايات المتحدة الأمريكية عام 2015 بأنها، إجراء من دولة ضد دولة أخرى، يتمثل في القيام بهجوم مسلح، أو استخدام للقوة في الفضاء الإلكتروني (Theohar and Rollins: 2015: 1) . وهذا التعريف يحاول تطبيق مفهوم الحرب التقليدية، التي تستخدم القوة، أو التهديد بها بين الدول، في المجال السيبراني، الذي يشمل الحواسيب والشبكات والمعلومات.

تتفق جميع التعريفات التي ذكرت أعلاه أن الحرب السيبرانية هي استخدام للأجهزة الحاسوبية، أو الوسائل الرقمية، لإلحاق ضرر بدولة أخرى، أو بمصالحها، وهذا يعني أن الحرب السيبرانية تشمل عناصر عديدة كالفضاء السيبراني، والسلاح السيبراني، والضرر، والفاعل، و الغاية، والنتيجة، وبهذا سيتم تعريف الحرب السيبرانية إجرائيا بانها نزاع رقمي يحدث في الفضاء الالكتروني بين دولتين، او كيانين متعارضين، أو أكثر، لتحقيق أهداف سياسية، او اخضاع العدو لإرادة الدولة المستهدفة، وفي هذا الإطار تنقسم الحرب السيبرانية إلى ثلاثة أنماط مختلفة كل منه حسب درجة الشدة والخطورة وهي على النحو التالي :

1. النمط الأول الحرب السيبرانية الباردة منخفضة الشدة: يعبر هذا النمط عن نزاع مستمر بين الأطراف المتنازعة، قد يكون ذو طبيعة طويلة المدى ودائمة النشاط العدائي، أو غير السلمي، ويتميز هذا النزاع بعمق جذوره وتشابكه، وله جوانب متعددة كالثقافية، والاقتصادية، والاجتماعية وغالبًا ما يتم اللجوء إلى القوة الناعمة في هذه الحروب السيبرانية، كشن الحروب النفسية، والاختراقات المتنوعة، والتجسس، وسرقة المعلومات، والتنافس بين الشركات التكنولوجية العالمية، وأجهزة الاستخبارات الدولية (موسى:204:2020) ويظهر هذا النمط في الصراعات السياسية ذات الأبعاد الاجتماعية والدينية الممتدة، كالنزاع العربي – الصهيوني، أو النزاع الهندي - الباكستاني، وكهجوم فيروس واناكراي في عام 2017م، الذي اتهمت كوريا الشمالية بتنفيذه (عبد الصادق:2019).
2. النمط الثاني: الحرب السيبرانية متوسطة الشدة: يتميز هذا النمط بتحول الصراع عبر الفضاء الإلكتروني إلى ساحة موازية للحرب التقليدية الدائرة على الأرض، ويعكس هذا النمط حدة الصراع بين الأطراف

المتنازعة، وقد يمهد لعمل عسكري، ويشتمل هذا النمط على عدة أنشطة منها اختراق المواقع الإلكترونية وتخريبها، وشن حرب نفسية ضد الخصوم (عبدالصادق: 2019). أما تاريخيًا، فقد استُخدمت الحروب السيبرانية متوسطة الشدة في هجمات حلف الناتو على يوغوسلافيا في عام 1999م، حيث استهدفت الهجمات الإلكترونية تعطيل شبكات الاتصالات للخصوم، وقد برزت هذه الحروب خلال النزاع بين حزب الله والكيان الصهيوني عام 2006م، وأيضًا في الحرب بين روسيا وجورجيا عام 2008م (علي : 2017: 43).

3. النمط الثالث الحرب السيبرانية الساخنة، أو مرتفعة الشدة: يعبر هذا النوع من الأنماط على نشوب حروب في الفضاء الإلكتروني، تكون منفردة وغير متوازية مع الأعمال العسكرية التقليدية، ويتميز هذا النمط بسيطرة البعد التقني على إدارة العمليات الحربية، حيث تُستخدم الأسلحة الإلكترونية فقط ضد منشآت العدو، ويشتمل هذا النمط على اللجوء إلى الروبوتات الآلية، والطائرات دون طيار، التي تُدار عن بعد، بالإضافة إلى تطوير القدرات في مجالي الدفاع والهجوم الإلكتروني، والاستحواذ على القوة الإلكترونية (عبد الصادق: 2019).

5.2.3.1. الجريمة السيبرانية (Cyber Crime) :

في ظل التطور التقني السريع الذي يشهده العالم، ظهرت جرائم تقنية حديثة بجانب الجرائم التقليدية، واعتمدت هذه الجرائم على تقنيات متقدمة، مما حول الجريمة من شكلها التقليدي إلى أبعاد جديدة، ومع تزايد التطور التكنولوجي، ارتفعت نسبة هذه الجرائم، ولم تقتصر على المجالين العسكري والسياسي، بل امتدت لتشمل المجالات الاقتصادية والتجارية والثقافية أيضًا (العيشي وعناب: 2018: 11).

وقد شهدت الجريمة السيبرانية تطورًا ملحوظًا منذ ظهورها في الإحصائيات لأول مرة، بين عامي 1971م و1990م، حيث كانت نادرة جدًا، تنحصر بين جريمة واحدة إلى ثلاث جرائم سنويًا، وكانت أبرز هذه الجرائم وقعت سنة 1988م، وفي تسعينات القرن الماضي، شهدت معدلات الجريمة السيبرانية ارتفاعًا كبيرًا، وكان من أبرزها حادثة عام 1994م، حيث تمكن طالب أمريكي يبلغ من العمر ستة عشر عامًا من اختراق أجهزة الكمبيوتر في معهد أبحاث الطاقة الكورية، ووكالة ناسا، ووكالات حكومية أخرى، ومنذ ذلك الحين، استمرت الجريمة السيبرانية في التصاعد، وأصبحت تهديدًا حقيقيًا لأمن المعلومات، ومصدر خطر على الأمن القومي للدول (مجمع البحوث والدراسات: 2016: 7-10). ومن الجذير بالذكر أن التكاليف العالمية للجرائم السيبرانية ضخمة جدا، حيث إنها قد تصل إلى حوالي تريليون دولار أمريكي سنويًا (Schreier: 2015:9) .

ومع تزايد وتيرة الجرائم السيبرانية وتنوع أساليبها، فإنها، لا شك تسببت في خسائر مادية جسيمة، ليس فقط على مستوى الأفراد، بل أيضا على مستوى المنظمات والمؤسسات والبنى التحتية للدول، مما يؤثر سلبا على الأمن القومي. فمثلا، بلغت قيمة الخسائر الناتجة عن هذه الجرائم، عام 2011م حوالي 388 مليار دولار أمريكي (ناصر:2022: 111). ومع استمرار التطور التقني، أصبحت الجرائم السيبرانية أكثر تعقيدًا، مستفيدة من تقنيات أخرى كإنترنت الأشياء، والحوسبة الحسابية، والذكاء الاصطناعي، والشبكة المظلمة، وغيرها من التقنيات (لطفي :2022 : 4).

كما شهدت الجرائم السيبرانية تنوعًا في تسمياتها، حيث بدأت بمصطلح إساءة استخدام الكمبيوتر، ثم تطورت لتصبح احتيال الكمبيوتر، والجريمة المعلوماتية، والجريمة المرتبطة بالكمبيوتر، وجرائم التقنية العالية، وصولًا إلى جرائم القراصنة (الهاكرز) وجرائم الإنترنت، وأستقر على مصطلح الجرائم السيبرانية (عطية الله :2020: 9). ويعتبرها الباحث الفرنسي كولين روز (COLIN ROSE) ، الجريمة السيبرانية ثالث أكبر تهديد يواجه القوى العظمى، بعد الأسلحة الكيميائية والبيولوجية والنووية (بوقرص: 2022:65).

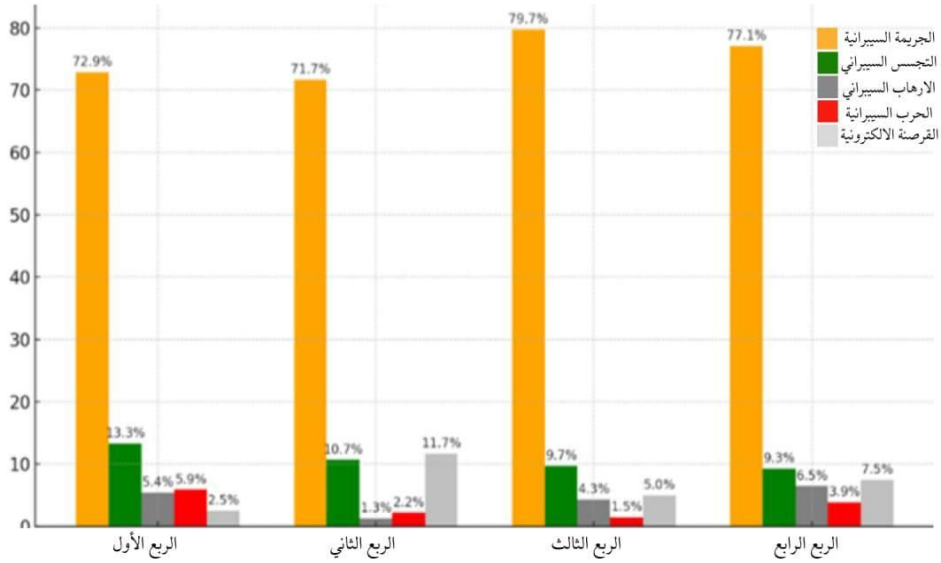
تُعرف الجريمة السيبرانية بأنها، جريمة تشمل جميع الأنشطة الإجرامية التي تُنفذ باستخدام أنظمة الكمبيوتر، عبر شبكات الاتصالات السلكية واللاسلكية (كريم: 2011: 141) ويُبرز استخدام مصطلح (جميع) في هذا السياق شمولية المفهوم، مما يعني أن أي فعل إجرامي يتم من خلال نظام الكمبيوتر عبر شبكة الاتصالات، يُصنف بأنه جريمة سيبرانية.

وفي التشريعات الليبية، وفقًا للقانون رقم 5 لعام 2022م، بشأن مكافحة الجرائم الإلكترونية، الصادر عن البرلمان الليبي، تُعرف الجريمة الإلكترونية في المادة الأولى بأنها، كل فعل يُرتكب باستخدام أنظمة الحاسب الآلي، أو شبكة المعلومات الدولية، أو غيرها من وسائل تقنية المعلومات (مجلس النواب الليبي: 2022).

وتُعرّف منظمة الإسكوا الجريمة السيبرانية، بأنها نشاط إجرامي، يُستخدم فيه الحواسيب والإنترنت للاعتداء، سواء كان الاعتداء بشكل مباشر، أو غير مباشر، وتشمل هذه الجرائم سرقة الأموال من المصارف أو البطاقات المصرفية، أو انتحال الهوية، أو التعدي على الملكية الفكرية، وتختلف دوافع مرتكبي هذه الجرائم، فقد تكون بدافع الربح المادي، أو الشهرة، أو الأهداف السياسية، كمهاجمة المواقع الإلكترونية لدولة معادية (عبد الصادق:2015: 67-68). هذا التعريف يحدد ماهية الجريمة السيبرانية، وكيفية ارتكابها، والفئات والدوافع والأهداف التي تشملها، وبالتالي يمكننا تصنيف أهم أنواع الجرائم السيبرانية، وذلك على النحو التالي:

1. **الجرائم ضد الأفراد**: تتضمن هذه الجرائم سرقة الهوية، كسرقة البريد الإلكتروني، أو الاشتراك في مواقع الإنترنت، وانتحال شخصية أخرى بطرق غير شرعية عبر الإنترنت (العمري:2020: 44-45).
2. **الجرائم ضد الملكية**: تشمل هذه الجرائم نقل البرمجيات الضارة إلى بعض البرامج والتطبيقات، بهدف تدمير الأجهزة الحكومية، والمصارف، والممتلكات الشخصية (العمري :2020 : 44 - 45).
3. **الجرائم ضد الحكومات:** تتجسد هذه الجرائم في مهاجمة المواقع الرسمية، وأنظمة الشبكات الحكومية، سواء على المستوى المحلي، أو الدولي، وتشمل هذه الجرائم الهجمات الإرهابية على شبكة الإنترنت، بهدف تدمير البنى التحتية، ومهاجمة شبكات الكمبيوتر، وغالبًا ما تكون دوافعها سياسية (القطروني: 2018: 96).

ولتوضيح أنواع التهديدات السيبرانية التي تم ذكرها ه سيتم عرض النسب المئوية لها، وسيتم إجراء مقارنة بين عام 2023م كما موضح في الشكل(6) وعام 2024م كما هو موضح في الشكل رقم(7) على النحو التالي:



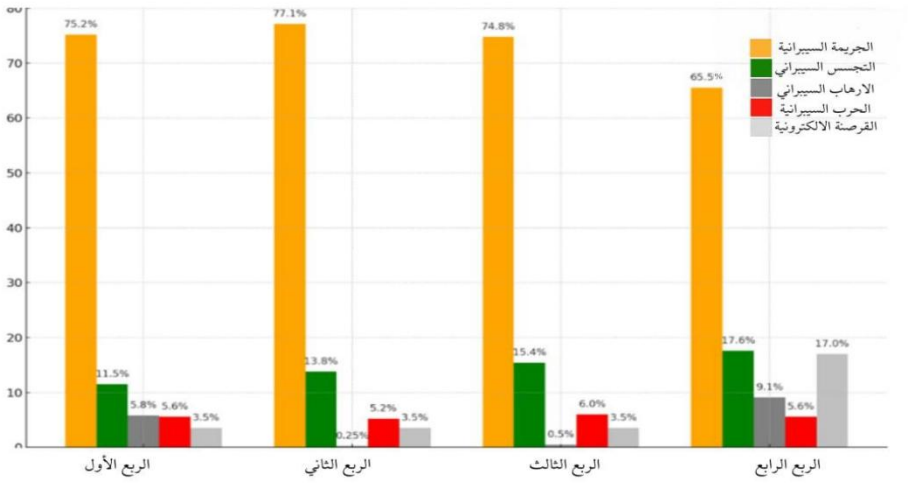
الشكل(6)النسب المئوية لأنواع التهديدات السيبرانية عام 2023م، المصدر(Hackmageddon:2024)

هذا الرسم البياني يعرض أنواع التهديدات السيبرانية لعام 2023 التي تشمل الجريمة السيبرانية (باللون البرتقالي)، والتجسس السيبراني (باللون الأخضر)، والإرهاب السيبراني (باللون الرمادي) والحرب السيبرانية (باللون الأحمر) والقرصنة الإلكترونية (باللون الفضي)، كل نوع من التهديدات يظهر بأربعة أعمدة، يمثل كل عمود نسبة انتشار هذا النوع في ربع من الأرباع السنوية.

تمثل نسبته المئوية في الأرباع الأربعة، في عام 2023 في الجريمة السيبرانية النسبة الأكبر من التهديدات على مدار الأرباع الأربعة، أعلى نسبة كانت في الربع الثالث (79.7%)، وأقل نسبة في الربع الثاني (71.7%)، أما التجسس السيبراني تتراوح نسبته بين 13.3% في الربع الأول و9.3% في الربع الرابع يُظهر انخفاضًا تدريجيًا على مدار العام، أما الإرهاب السيبراني شهد الربع الأول أعلى نسبة (5.4%)، بينما كانت النسبة الأدنى في الربع الثاني (1.3%)، لا سيما إلى الحرب السيبرانية تذبذبت النسبة بين 5.9% في الربع الأول و1.5% في الربع الثالث، أيضا القرصنة الإلكترونية كانت نسبتها متقلبة، حيث ارتفعت بشكل ملحوظ في الربع الثاني (11.7%)، بينما انخفضت إلى أدنى مستوياتها في الربع الأول (2.5%).

في عام 2024م يوضح الشكل رقم (7) الجريمة السيبرانية أعلى نسبة بين كل التهديدات، مما يشير إلى أنها الأكثر انتشارًا وتأثيرًا، النسب تتناقص بمرور الوقت خلال العام يأتي الربع الأول بنسبة 75.2%، الربع الثاني 77.1% (أعلى نقطة خلال العام)، الربع الثالث بنسبة 74.8%، أما الربع الرابع65.5% (انخفاض ملحوظ)، أما التجسس السيبراني يُظهر تزايدًا ثابتًا ومستمرًا طوال العام الربع الأول11.5%، الربع الثاني13.8%، الربع الثالث 15.4%، وأيضا الربع الرابع: 17.6%، هذا النوع يعكس تركيزًا متزايدًا من الجهات الفاعلة على جمع المعلومات الحساسة مع مرور الوقت، وهو مؤشر على تطور تقنيات التجسس أو اهتمام أكبر بالبيانات السرية، وأيضا الإرهاب السيبراني يأتي الربع الأول بنسبة 5.8% والربع الثاني

0.25% (انخفاض حاد جدًا) والربع الثالث0.5% أما الربع الرابع 9.1% (أعلى نقطة)، والحرب السيبرانية بقيت نسبتها ثابتة نسبيًا على مدار العام يأتي الربع الأول 5.6%، الربع الثاني 5.2%، أما الربع الثالث 6.0%، والربع الرابع 5.6%، وأيضا القرصنة الإلكترونية تُظهر تزايدًا كبيرًا في الربع الرابع مقارنة بالأرباع السابقة الربع الأول3.5%، الربع الثاني: 3.5%، الربع الثالث: 3.5% والربع الرابع: 17.0% (قفزة كبيرة جدًا).



الشكل(7)النسب المئوية لأنواع التهديدات السيبرانية عام 2024، المصدر(Hackmageddon:2024)

وتستنتج الباحثة بأنَّ القرصنة والجرائم الإلكترونية تتسبب في خسائر اقتصادية فادحة للشركات والحكومات، وتقوض الثقة في البنية التحتية الرقمية، وتؤدي إلى سرقة البيانات الحساسة، وتعطيل الخدمات الأساسية، وتشويه السمعة، أما التجسس السيبراني فيهدف إلى سرقة المعلومات الحساسة، مثل الأسرار التجارية والمعلومات العسكرية والاستخباراتية، ويمكن أن يؤدي إلى تفوق منافس اقتصادي، أو اتخاذ قرارات سياسية خاطئة، أو حتى شن هجمات سيبرانية، كذلك الإرهاب السيبراني يستخدم التقنيات الحديثة لتنفيذ أعمال إرهابية، مثل تعطيل البنية التحتية الحيوية (الكهرباء والمياه والاتصالات وغيرها)، ونشر الدعاية، وتخويف السكان، وأخيراً، الحرب السيبرانية هي استخدام القدرات السيبرانية ضد أهداف عسكرية، أو مدنية لدولة أخرى يمكن أن تشمل تعطيل أنظمة القيادة والسيطرة، وتدمير البنية التحتية الحيوية، والتأثير على الرأي العام وأيضا استهداف الأمن القومي لدولة ما.

بشكل عام تشكل أنواع التهديدات السيبرانية تهديداً وجودياً للأمن القومي للدول؛ فهي لا تهدد فقط الأمن الاقتصادي والاجتماعي، بل تهدد أيضاً السيادة الوطنية والاستقرار السياسي.

4.1. مفهوم الأمن القومي وعناصره

شهد مفهوم الأمن القومي تطورا كبيرا؛ إذ لم يعد يقتصر على الناحية العسكرية، ولم تعد وحدها صوراً التهديد ولا هي وحدها مصدره ويمكننا القول بأن، الأمن القومي بمفهومه المعاصر، هو مفهوم متعدد الجوانب

والأبعاد وكذلك يمتاز باتساع نطاق المصالح السياسية والاقتصادية والعسكرية للدول وتشابكها وتعارضها، والتطور العلمي والتقني، في كافة المجالات الحيوية (ياكرة يى: 2011:44).

كذلك فإنَّ الامن القومي ذو صلة بالمجتمع بكافة مصالحه، وهو ظاهرة حركية متطورة، وليس حالة سكونيه جامدة، يتفاعل مع المرحلة الزمنية ومع أمن الوحدات السياسية والإقليمية الأخرى، والوضع الدولي وتوازن القوى فيه، كما أن التهديد العسكري الخارجي لم يعد هو الخطر الوحيد على الأمن القومي، فهناك عدة أشكال من التهديدات العسكرية والاقتصادية والتقنية ومنها الخارجي ومنها الداخلي (عابد:2017:36-37). تم في الآونة الأخيرة انتقاد مفهوم الأمن القومي، لكونه غير دقيق في مفهومه، وقد كان *ريتشارد أولمان* من أوائل العلماء الذين انتقدوا التركيز الحصري على التهديدات العسكرية في التفكير التقليدي للأمن القومي، حيث يؤكد أن تعريف الأمن القومي من الناحية العسكرية فقط ينقل صورة زائفة عن الواقع لعدة أسباب، من أبرزها أنه يجعل الدولة تركز على التهديدات العسكرية، وتتجاهل التهديدات الأخرى غير العسكرية، وقد تكون الأخطر، ما يقلل من أمنها الكلي، وتكون التهديدات الناشئة من خارج الدولة أكثر خطورة على أمنها من التي تنشا داخلها (الامير:2021:81).

ثم توسع مفهوم الأمن القومي، فلم يعد يقتصر على الجانب العسكري فقط، فالتطورات العلمية والتقنية أضافت عناصر جديدة لهذا المفهوم، وتعتبر التهديدات السيبرانية من أخطر التحديات الاقتصادية والأمنية التي تواجهها الدول، مما يجعلها أولوية قصوى في استراتيجيات الأمن القومي، حيث تتطلب خططًا متقدمة لحماية البنية التحتية الحيوية والمعلومات الحساسة(Yusuf:2013:131). وإذا كان الأمن القومي يُعني غياب التهديد لقيم المجتمع الأساسية وغياب الخوف من خطر تعرض هذه القيم للهجوم، فإن الفضاء الالكتروني قد فرض إعادة التفكير في مفهوم الأمن، الذي يتعلق بتلك الدرجة التي تمكن الدولة من أن تصبح في مأمن من خطر التعرض لهجوم عسكري، أو إرهابي، وإجراءات الحماية ضد تعرض المنشآت الحيوية للبنية التحتية للأعمال العدائية من خلال الاستخدام السيئ لتكنولوجيا الاتصال والمعلومات (نوره:2018:197).

1.4.1. مفهوم الأمن القومي :

1.4.1 .1. تعريف الأمن لغة واصطلاحاً:

الأمن في اللغة: من أمن، يأمن ، آمناً، فهو آمن ، وأمن أمناً، وأماناً، اطمأن ولم يخف، فهو آمن وأمين ، فالأمن يعني الاستقرار والاطمئنان، ونقول (أمن منه)، أي سلم منه، فهو نقيض الخوف، والأمانة ضد الخيانة (جعفري: 2022: 243) وقد تناولت معظم المصادر اللغوية مفهوم الأمن بمعانٍ متقاربة جدًا، فجاء في معجم المورد أن كلمة (أمن) تعني السلام والطمأنينة، وتشير أيضًا إلى حماية أي تدابير تتخذ للوقاية من التجسس والتخريب (البعلبكي :1044).

الأمن إصطلاحاً: عرفه جوزيف ناي بأنه، غياب التهديد بالحرمان الشديد من الرفاهية الاقتصادية، مما يشير إلى أن القوة الاقتصادية هي الركيزة الأساسية لأمن الدولة، دون النظر إلى المقومات الأخرى (عبد العال:2018). وعرفه باري بوزان بأنه، العمل على التحرر من التهديد، فيركز في تعريفه على مفهوم التحرر من أي تهديدات قد تواجه الدولة، أو الأفراد (توفيق:48:2018). والتعريف العام للأمن يشير إلى وجود تهديدات (حقيقية أو متخيلة)، تواجهها الدول والأفراد والنظام، والتي تؤثر على العلاقات بين الدول والبيئة السياسية المحلية(Valeriano and maness:2015:37).

1.4.1 .2. تعريف القومي لغة واصطلاحاً :

القومي لغة: هو اسم منسوب إلى قوم، ويعني الشخص الذي يؤمن بوجوب معاونته لقومه ومساعدتهم على جلب المنفعة ودفع المضرة (الحلبي:2020: 137). وعُرّف في معجم المورد، بأنه خاص بأمة أو شعب (البعلبكي:2014:59).

القومي اصطلاحاً، يُعبر عن مفردة قوم، أو أمة، أو جماعة، يربطهم العرق والدين ومقومات مادية ومعنوية في إطار الوحدة السياسية للدولة (حمد:31:2016). ويُعرَّف أيضاً بأنه، الشعور بالانتماء إلى مجموعة بشرية معينة، ترتبط فيما بينها بروابط مشتركة، قد تكون ناجمة عن وحدة الأصل العرقي، أو اللغة، أو الثقافة، أو التاريخ، أو المصالح المشتركة، فتشعر بأن لها هوية خاصة تميزها عن أقوام أخرى مختلفة عنها في كل، أو في بعض هذه السمات (محمد :451:2022).

1.4.1. 3 .تعريف الأمن القومي :

مفهوم الأمن القومي مفهوم حديث نسبيًا في ميدان العلوم السياسية، وقد تطور بشكل كبير منذ ظهوره، فهو ليس ثابتًا، بل متغيراً يعتمد على العديد من العوامل، كالنظام الدولي، والظروف السياسية، والعسكرية، والتقنية، والاقتصادية لكل دولة، فمثلا، الأمن القومي الأمريكي يختلف بشكل كبير عن الأمن القومي العربي؛ بسبب الفروقات في القدرات العسكرية، والتقنية، والسياسية بين الأمتين، فبينما تركز الولايات المتحدة على حماية مصالحها العالمية من خلال قدراتها العسكرية، والتقنية المتقدمة، نرى أنَّ الدول العربية تركز على حماية حدودها واستقرارها الداخلي في ظل التحديات الإقليمية، والمحلية، وسوف يتم تحديد مفهوم الأمن القومي على النحو الآتي:

تُعرفه الموسوعة السياسية بأنه يشير إلى الإجراءات التي تتخذها الدول للحفاظ على سلامتها ضد الأخطار الخارجية والداخلية، التي قد تؤدي إلى الوقوع تحت سيطرة أجنبية، نتيجة ضغوط خارجية أو انهيار داخلي (دحماني: 20:2017). هذا التعريف يركز على الجانب الدفاعي للأمن، أي قدرة الدولة على صون سلامتها وسيادتها من أي تهديد، أو تدخل خارجي، أو داخلي.

وعرفه الدكتور علاء الدين هلال بأنه تأمين كيان الدولة ضد الأخطار التي تهددها داخليًا وخارجيًا، وتأمين مصالحها، وتهيئة الظروف المناسبة لتحقيق أهدافها وغاياتها القومية (جعفري:2022: 245). هذا التعريف يأخذ في الاعتبار جميع الجوانب والأبعاد والتحديات التي تواجه الدولة وشعبها في مجالات مختلفة، ووفقًا

لهذا التعريف، يتضح لنا أن الأمن القومي يتمثل في تأمين كيان الدولة، من التهديدات المادية، والمعنوية، والثقافية، والبيئية، بالإضافة إلى تأمين مصالحها، وتهيئة الظروف المناسبة لتحقيق أهدافها وغاياتها القومية. وعرف أيضا بأنه يشير إلى أن هناك تهديدات غير تقليدية وظواهر جديدة، تهدد الأمن القومي، وهي تهديدات ذات طابع عالمي، ولا تقتصر على دولة معينة، وهذه التهديدات متشابكة، بحيث يمكن أن يؤدي أحدها إلى تفاقم الآخر، ولا يمكن التعامل معها بشكل نهائي وفقًا لنظريات الأمن التقليدية، حتى إنه يُعتبر الأمن السيبراني أحد عناصر الأمن القومي غير التقليدي، حيث يمكن لأحد مستخدمي الفضاء الإلكتروني أن يتسبب في خسائر كبيرة للطرف الآخر (محمد:2022:451). وفقًا لهذا التعريف، يتضح أنَّ الأمن القومي لا يقتصر على التهديدات التقليدية التي تستهدف الدولة من الخارج فحسب، بل يشمل أيضًا التهديدات السيبرانية التي تستهدف المجتمع والبنية التحتية، والثقافة، والبيئة من الداخل أو الخارج.

2.4.1.عناصر الأمن القومي :

يُعد مفهوم الأمن القومي من المفاهيم الجدلية، التي يصعب تحديدها بدقة، وذلك بسبب عناصره المختلفة والمتعددة، و يمكن تحديد هذه العناصر على النحو الآتي:

1.2.4.1.الأمن العسكري:

تتحقق مطالب الأمن والدفاع من خلال بناء قوة عسكرية قادرة على تلبية احتياجات التوازن الاستراتيجي العسكري، والردع الدفاعي، على المستوى الإقليمي لحماية الدولة من العدوان الخارجي، وذلك من خلال الاحتفاظ بالقوة العسكرية، في حالة استعداد قتالي دائم وكفاءة قتالية عالية للدفاع عن حدود الدولة وعمقها، فالقوة العسكرية هي الأداة الرئيسية في تأييد السياسة الخارجية للدولة، وصياغة دورها القيادي على المستوى الإقليمي والدولي (إبراهيم:2022).

فهذا الأمن يركز على دور ومهام القوات المسلحة للدولة، من خلال حمايتها ضد أي نشاط مسلح خارجي يهدد حدودها، وأرضها، أما دورها الخارجي فيكون في أن تكون قوة يدركها العالم الخارجي، ويقتنع بأنها قادرة على الحفاظ على مصالحها، وتحقيقها في حالة الاضطرار لاستخدام القوة، أو العمل كقوة رادعة للقوى المعادية، دون أن تقوم باستخدام القوة، الأمر الذي يلقي بمسئولية تحقيق الأمن القومي على عاتق الجيوش وأجهزة المخابرات التابعة للدولة.

2.2.4.1.الأمن السياسي:

يسعى البعد السياسي للأمن القومي إلى حماية النظام السياسي للدولة، وضمان الأمن والنظام العام، بالإضافة إلى حماية المؤسسات الحكومية التي تسهم في تعزيز العلاقة بين المواطن والدولة (عطية: 2020). ويتمثل هذا البعد للحفاظ على الكيان السياسي للدولة، ويتضمن شقين هما الشق الأول هو البعد الداخلي الذي يتعلق بتماسك الجبهة الداخلية، والسلم الاجتماعي، والوحدة الوطنية، أما الشق الثاني فهو البعد الخارجي الذي يتناول الأطماع الخارجية في موارد الدولة ومقدراتها، ومدى توافق تلك الدول مع الدولة المعنية سياسياً،

واقتصادياً، واجتماعياً، وذلك وفقاً لمجموعة من المبادئ الاستراتيجية، التي تحدد أولويات المصالح الأمنية وأسبقياتها (محمد: 2022: 453)

3.2.4.1.الأمن الاقتصادي:

يتمثل هذا الأمن في حماية موارد الدولة واقتصادها، وتطويرهما لتلبية متطلبات المعيشة للمواطنين، ويُعد البعد الاقتصادي ذا أهمية كبيرة، لارتباطه بتوفير احتياجات الدولة الاقتصادية، وقدرتها على التعامل مع الدول الأخرى (عطية: 2020).

كما يسعى هذا الأمن إلى توفير المناخ المناسب لتلبية احتياجات الشعب، وتوفير سبل التقدم والرفاهية له، ويُعتبر الأمن القومي الاستراتيجية العليا الوطنية التي تهتم بتنمية واستخدام كافة موارد الدولة لتحقيق أهدافها السياسية، لذلك فإن النمو الاقتصادي والتقدم التكنولوجي هما السبيل لتحقيق المصالح الأمنية للدولة، وبناء قوة الردع الاستراتيجية، وتنمية التبادل التجاري، وتصدير العمالة، وغيرها من المؤشرات المهمة التي تدل على اندماج الجانب الاقتصادي بالأمن القومي (أسامة: 2020).

4.2.4.1.الأمن الاجتماعي:

يهدف إلى توفير الأمن للمواطنين، بما يعزز شعورهم بالانتماء والولاء للمجتمع، و يتحقق ذلك من خلال إقامة العدالة الاجتماعية، وتقريب الفوارق بين الطبقات، مما يساهم في حماية الأمن القومي من المخاطر، وذلك بتحقيق العدالة، ويتم تعزيز الوحدة الوطنية، والتفاف الشعب حول القيادة السياسية، وعلى النقيض فإن الظلم الاجتماعي يؤدي إلى تهديد داخلي حقيقي للأمن القومي، و يصعب السيطرة عليه خاصة في ظل تفاقم مشاكلات البطالة، والصحة، والتعليم (أبراهيم:2022). ويحتل الأمن الاجتماعي في الوقت الحاضر أهمية بالغة، حيث كان الاهتمام بهذا البعد متدنياً في السابق، خاصة في الدول النامية، وتثبت الثورات الشعبية التي شهدها الوطن العربي منذ مطلع عام 2011م، أهمية تأثير البعد الاجتماعي على الأمن القومي، وأنه يساوي في أهميته الأبعاد الأخرى للأمن القومي لأي دولة في العالم، ويُعد إهمال هذا البعد من أخطر مصادر التهديد للأمن القومي (منصور: 2011: 56) .

5.2.4.1.الأمن التقني (المعلوماتي):

يُعد من أهم عناصر الأمن القومي، حيث أصبحت التقنية جزءًا أساسيًا من حياتنا، حيث يمكن أن تؤثر على الأمن القومي للدولة من خلال تهديد البنية التحتية الحيوية، بسرقة البيانات الحساسة، ونشر المعلومات المضللة، وغيرها من الوسائل المؤثرة، مما يجعلها هدفًا للتهديدات والمخاطر التي يمكن أن تؤثر سلبا على الأمن القومي للدولة وتعد الولايات المتحدة أولى الدول التي استفادت من الثورة الصناعية الرابعة، أو ما يُعرف بثورة المعلومات، مما جعلها رائدة في مجالات التقنية المعقدة، كالمجالات العسكرية، والاتصالات، والفضاء، والعقول الإلكترونية وغيرها (حامد: 2016: 53-54).ويمكننا أن نستنتج إن البعد المعلوماتي يشير إلى قدرة الدولة على حماية مصادرها وقنواتها والبنية التحتية للمعلومات من أية تهديدات، أو تدخلات، أو

تضليل، أو تخريب من قبل الجهات المعادية، كما يشير إلى قدرة الدولة على استخدام المعلومات والاتصالات أدوات لتحقيق مصالحها وأهدافها السياسية، والاقتصادية، والاجتماعية، والثقافية.

وانطلاقًا من المفهوم النظري للأمن القومي، مع الأخذ بعين الاعتبار المستويات العملية كإطار استراتيجي، ومع تنوع المدارس التي تحلل هذا المفهوم، تبرز مدرسة كوبنهاغن إطاراً مهماً للدراسة، نظرًا لقدرتها على معالجة القضايا الأمنية الجديدة، كالتهديدات السيبرانية، لذا تسعى الباحثة إلى تسليط الضوء على هذه المدرسة، لفهم كيفية تعاملها مع هذه التحديات الحديثة.

3.4.1.مدرسة كوبنهاغن لتحليل مفهوم الأمن القومي :

تُعد مدرسة كوبنهاغن من أبرز المدارس الفكرية التي أسهمت في توسيع مفهوم الأمن، مستندةً إلى أعمال باري بوزان (Barry buzan) في كتابه (الناس الدول والخوف): مشكلة الأمن القومي في العلاقات الدولية، الذي صدر عام1991م، حيث تُركز هذه المدرسة على أنه ليس للأمن مفهوم ثابتا، بل هو بناء اجتماعي يتشكل من خلال الممارسات والتفاعلات بين الفاعلين، مما يجعل الأمن حركيا ومتغيراً، ويتجاوز مفهوم الأمن الأطر التقليدية التي تركز على الحروب بين الدول (توفيق: 2018: 47). تمثل فكرة الأمننة جوهر نظرية مدرسة كوبنهاغن، حيث يُنظر إلى الأمن على أنه عملية ترتبط بفكرة البقاء، وفقاً لبوزان، ويتعلق هذا البقاء بالأخطار الوجودية التي قد تواجه الأفراد والدول، ومع تغير مفهوم الأمن تظل قيمة البقاء ثابتة كمحور رئيسي يدور حوله (خليفة:2020: 53).

وينطلق منظور (كوبنهاغن) للأمن من تعريف (باري بوزان) للأمن بأنه جهد لتحرير الذات من التهديدات، ويشير (بوزان) إلى أن الأمن في سياق النظام الدولي يعني كفاءة الدول والمجتمعات في الحفاظ على استقلالها وترسيخ تماسكها الوظيفي أمام القوى التي تراها معادية، ويعد الحد الأدنى للأمن هو البقاء، ويتضمن أيضًا اهتمامًا معقولًا بشروط حماية هذا الوجود (توفيق: 2019: 48). ولا يعني بوزان بالتحرر من التهديد القدرة على الانفلات منه، أو تحييده تمامًا في تحليله للبنية الفوضوية للنظام الدولي، ويشير إلى أن الأمن في ظل هذه الفوضى يمكن أن يكون نسبيًا فقط، وليس مطلقًا، أما بالنسبة لمفهوم الأمن القومي، فيراه بوزان كمفهوم محافظ يتعلق بقدرة الدول بالحفاظ على هويتها المستقلة، ووحدتها الوظيفية (توفيق: 2019: 48).

1.3.4.1 نظرية الأمننة :

ظهر مفهوم الأمننة في منتصف التسعينيات من القرن الماضي، وقد ارتبط بشكل وثيق بالتفاعلات في العلاقات الدولية، وما تخلقه من مخاطر وتهديدات، وهذا يمثل تحولًا حاسمًا في الدراسات الأمنية (خليفة:2020: 52). وتسعى نظرية الأمننة إلى توسيع نطاق الدراسات الأمنية لتشمل أكثر من مجرد التحليل الضيق الذي يركز على التهديدات العسكرية، واستخدام القوة، بينما حاول بعض العلماء الحفاظ على إطار ضيق للدراسات الأمنية، كدراسة التهديدات، واستخدام القوة العسكرية، وتعكس نظرية الأمننة رؤية أكثر شمولية، وتشير إلى أن القضايا تصبح مسائل أمنية، ليس بسبب وجود تهديدات وجودية يمكن قياسها بشكل موضوعي، بل لأن الجهات الفاعلة الرئيسية تقوم بتقديم هذه القضايا وتأسيسها على أنها تهديدات (Kerttunen and Tikk: 2020.). وتُعد نظرية الأمننة من أبرز النظريات في حقل الدراسات الأمنية

المعاصرة، وتتميز هذه النظرية بالابتكار والجدل في آن واحد، وقد نشأت هذه النظرية عام1955م، للكاتب أولي وايفر (OLE Waever) من خلال مقاله (الأمننة واللا أمننة) (securitization and desecuritisation) ويرى (وايفر) أن التحدي الرئيسي في توسيع الأحتياجات الأمنية يكمن في الانتقال من التركيز التقليدي على أمن الدولة إلى أمن الأفراد، ويتعلق الأمر بمعرفة متى يجب أن نتوقف عن اعتبار أمن الأفراد مسألة ذات أبعاد متعددة ومعقدة (قاسي:2019: 1509). وقد سعى وايفر للإجابة عن سؤال محوري هو ما الذي يجعل قضية معينة تُعد مشكلة أمنية؟ فقد أجاب عنه من الناحية النظرية، حيث اعتبر أن المشاكل الأمنية هي، تلك التطورات التي تهدد سيادة الدولة، أو استقلالها، بشكل سريع وملحوظ، وهذا يستدعي استجابة قصوى، وحشد جميع الموارد المتاحة عمليًا، فإن اعتبار بعض القضايا مشكلات أمنية يتيح للنخب السياسية (أمننة) تلك القضايا للتحكم فيها (قاسي:2019: 1509) ولذا يمكن القول بأن الأمن هو فعل خطابي، حيث لا يرتبط بمسألة ملموسة في الواقع، بل يتحدد من خلال التصريحات والقرارات السياسية.

ويرى باري بوزان، الذي أسهم في تطوير هذه النظرية، بأنها عملية تحويل المشكلات إلى قضايا أمنية، حيث تُقدّم كتهديد وجودي، ويتطلب إجراءات عاجلة تشمل الفواعل الرئيسية في هذه العملية وهي، الحكومات، والقادة، وصناع السياسات، ووفقًا لبوزان يُفهم الأمن على أنه فعل كلامي، حيث تُعد المشكلة الأمنية تهديدًا لبقاء الدولة، مما يستدعي اتخاذ تدابير استثنائية، ويمكن التعامل مع المشكلة بسرعة وفقًا لقواعد صنع السياسات الأمنية (قاسمي وبلغيث: 2020: 34).

وقد اقترح باري بوزان دراسة الأمن من خلال ثلاث وجهات نظر وهي، الفرد، والدولة، والنظام الدولي، مشيرًا إلى أن أمن الفرد والنظام الدولي يعتمدان على أمن الدولة، وبناءً على ذلك، قدم ثلاثة مستويات لدراسة الأمن: وهي الدولة (المهددة بالسيادة والقوة)، المجموعة (المهددة بالهوية)، والفرد (المهدد بالبقاء والرفاه). كما يرى بوزان أن الدولة تتكون من ثلاثة مكونات رئيسية وهي فكرة الدولة الوطنية، والقاعدة الفيزيائية (الشعب والموارد والتكنولوجيا)، والمظهر المؤسساتي (النظام السياسي والإداري)، وهذا يسهل تصور التهديدات لهذه المكونات (توفيق:2019:49-50). و يبرز جوهر نظرية الأمننة، أن سياسات الأمن القومي ليست ثابتة ولا مفروضة مسبقًا، بل هي نتيجة لتصميم استراتيجي من قبل الفاعلين الرئيسيين في السياسة، حيث يقوم هؤلاء الفاعلون بتصوير واقع دولي معين، على أنه تهديد يستدعي اتخاذ إجراءات عاجلة (رياض : 17:2021). طبقًا لكلام (باري بوزان) لا توجد أسباب عديدة لتعقيد العلاقة بين مفهوم الأمن القومي والتهديد السيبراني، ويرجع ذلك جزئيًا إلى تأخر نظري في فهم مفهوم الأمن القومي، ويُظهر التعدد النظري نفسه من خلال نظرية الأمننة (Buzan:1983: 6-10) التي تتمثل في النقاط التالية:

1. يعد مفهوم الأمن القومي معقدًا ومركبًا إلى درجة تجعل من الصعب فهمه بوضوح، مما أدى إلى انحياز الباحثين نحو مفاهيم أكثر مرونة، وبالتالي، يُعتبر هذا المفهوم مثيرًا للجدل والتناقض.

2. نظرا للتشابك بين مفهوم الأمن القومي ومفهوم القوة، خاصة بعد ظهور المدرسة الواقعية، التي نشرت فكرة التنافس من أجل القوة في العلاقات الدولية، يُدرك الأمن على أنه مُشتق من القوة، ويُعتبر وسيلة لتعزيزها.

3. ظهور تيار من المثاليين يُعارض المدرسة الواقعية، ويعرض هدفًا بديلًا للأمن القومي، وهذا الهدف هو السلام.

4. تفوق الدراسات الاستراتيجية في مجال الأمن القومي، واهتمامها بالجوانب العسكرية للأمن، وتكريسها لخدمة المتطلبات الدفاعية، والحفاظ على الوضع القائم، مما أدى إلى تقليل النظرة التحليلية والبعد النظري لهذا المفهوم.

5. دور السياسيين في تعزيز غموض مفهوم الأمن القومي، لتوفير مساحة أوسع للتلاعب به، سواء لأغراض داخلية، أو بسبب الصراعات الخارجية.

يتضح مما سبق أنَّ نظرية الامننة هي نظرية تحليلية تستخدم في دراسة العلاقات الدولية، وتهدف إلى فهم كيفية تحويل بعض القضايا أو الظواهر إلى قضايا أمنية، تستوجب تدخلات استثنائية أو عاجلة من قبل السلطات، ووفقًا لهذه النظرية، فإن الأمن ليس حالة موضوعية يمكن قياسها بمؤشرات محددة، بل هو عملية إنشائية تعتمد على التفسير، والتأطير، والتبرير من قبل الفاعلين المعنيين في الدولة، لذا فإن الأمن لا يتعلق فقط بالتهديدات المادية، أو العسكرية، بل يشمل أي شيء يُعتبر خطرًا او تهديدا، ويمكن تطبيق نظرية الأمننة لفهم كيفية تحويل بعض الأحداث، أو الظواهر في الفضاء الإلكتروني، إلى قضايا أمنية تستدعي ردود فعل من قبل الدول، أو المجتمعات، فمثلا يمكن اعتبار هجوم برامج ضارة على شبكة كهرباء لدولة ما، على أنه حادث سيبراني اعتيادي، أو على أنه تهديد أمني خطير يستوجب اتخاذ إجراءات عسكرية، أو سياسية، وبناء على نظرية الأمننة فإن هذا التصور يعتمد على كيفية تقديم وتبرير هذا الحادث من قبل الفاعلين المختلفين، كالحكومة، أو وسائل الإعلام، أو المجتمع، لذا فإن نظرية الأمننة تساعد في دراسة دور الخطاب والسرد في صناعة وإدارة الأزمات الأمنية.

تتمثل خلاصة هذا الفصل في ان التهديدات السيبرانية باتت تشكل تحديا كبير للأمن القومي للدول، وأنه وعلى الرغم من تعدد تعريفات التهديدات السيبرانية، فأنه لا يوجد تعريف عالمي موحد، وتتميز هذه التهديدات بخصائصها المتغيرة باستمرار وباستخدامها أدوات متنوعة لا يمكن حصرها، وتتخذ التهديدات السيبرانية أنواعاً متعددة، وبالإضافة إلى ذلك يتطور مفهوم الأمن القومي بمرور الزمن ليواكب التطورات التكنولوجية، ويتسع ليشمل الأبعاد التقليدية والحديثة التي باتت تشكل تهديداً حقيقياً في حال استهدافها لاستقرار الدول وسيادتها.

الفصل الثاني

التهديدات السيبرانية للأمن القومي: التداعيات وسبل المواجهة

1.2. تمـهـيد

تشكل التهديدات السيبرانية في عصر المعلومات والتكنولوجيا المتقدمة تحديًا كبيرًا للأمن القومي للدول، الأمر الذي يقود إلى الاعتماد المتزايد على الأنظمة الرقمية في جميع مجالات الحياة، وهذا يفتح المجال أمام مخاطر جديدة تهدد البنية التحتية الحيوية، والأمن الاقتصادي، والاجتماعي لذا، فإن دراسة الأمن السيبراني ودوره في حماية الأمن القومي يعد ذا أهمية متزايدة.

يتناول هذا الفصل ثلاثة محاور رئيسية، ففي المبحث الأول، سنستعرض التطور التاريخي للأمن السيبراني بدءًا من بدايات الإنترنت في السبعينيات وصولا للقرن الحادي والعشرون، وسنبدأ أولا بتعريف الأمن السيبراني كحقل يتعامل مع حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية، وسنقوم بتحليل أبعاده المختلفة، كما سنناقش العلاقة الوثيقة بين الأمن السيبراني والأمن القومي.

أما في المبحث الثاني، فسنعرض دراسة لحالات ونماذج للتهديدات السيبرانية التي تعرضت لها دول مختلفة، مع بيان مدى تأثيرها على الأمن القومي، وسنستعرض أيضا أمثلة حقيقية لهجمات سيبرانية بارزة، وبيان أثرها على البنية التحتية والخدمات الحيوية، مما يعكس الفجوات الموجودة في الاستجابة لهذه التهديدات .

وسيتم في المبحث الثالث توضيح الجهود الدولية المبذولة لمواجهة التهديدات السيبرانية، وبيان التعاون بين الدول والمنظمات الدولية، والإقليمية، وسنناقش المبادرات المشتركة، والمعايير الدولية، وأهمية تبادل المعلومات والخبرات في بناء استراتيجيات فعالة لمكافحة هذه التهديدات.

من خلال هذا الفصل تهدف الدراسة إلى تقديم رؤية شاملة حول أهمية الأمن السيبراني للدولة من أجل الحفاظ على الأمن القومي، وكيفية وضع استراتيجيات التعامل مع التهديدات السيبرانية، مما يسهم في تعزيز الفهم الأكاديمي والعملي لهذا المجال الحيوي.

2.2. الأمن السيبراني ودوره في حماية الأمن القومي

يظهر بشكل أساسي مدى ارتباط شبكة الإنترنت مع الحياة الاقتصادية والاجتماعية، فقد أصبحت هدفًا لهجمات سيبرانية متكررة وخطيرة، تواجهها الحكومات والشركات والأفراد، لذلك فقد أصبح الأمن السيبراني أمرًا ذا أهمية بالغة لأسلوب حياتنا، حيث صارت حياتنا مرتبطًة بالإنترنت؛ سواء كان بالتواصل، أو التفاعل، أو الاعتماد، شاملا الدفاع الوطني والبنية الأساسية الحيوية كالطاقة؛ والنقل، والخدمات الصحية وغيرها؛ فكلما زاد اعتمادانا على الإنترنت وشبكات الكمبيوتر، زاد شعورنا بالأضرار التي قد نتعرض لها في حال تعرضنا للتهديدات السيبرانية، وهذا يعد واحدًا من أهم الأسباب التي تجعلنا بحاجة ماسة إلى تعزيز الأمن السيبراني (Cunningham: 2015:9).

يعرّف الاتحاد الدولي للاتصالات الأمن السيراني بأنه، مجموعة الأدوات والسياسات والمفاهيم الأمنية، والضمانات الأمنية، والمبادئ التوجيهية، ونهج إدارة المخاطر والإجراءات والتدريب، وأفضل الممارسات، وسبل الضمان والتقنيات التي يمكن استخدامها في حماية البيئة السيبرانية (الاتحاد الدولي للاتصالات: 2010). وتعد وكالة الأمن الرقمي الأوروبي، أول من اصدرت تشريعا في هذا المجال، وعرَّفته بأنه قدرة

نظام المعلومات على مقاومة محاولات الاختراق، أو الحوادث غير المتوقعة، التي تستهدف البيانات المتداولة، او المخزنة، وفق إطار توافقي (مجلي أوروبا: 2001). ويعرفه جيميس لويس James Lewisعلى أنه حماية شبكات الحاسوب والمعلومات من الاختراق، أو التدمير، أو البرامج الضارة (Lewis: 2017:1).

1.2.2.مراحل تطور الأمن السيبراني :

1.1.2.2. حقبة السبعينيات :

يعود ظهور مصطلح (الأمن السيبراني)، إلى سبعينيات القرن الماضي، تزامنًا مع تزايد الاعتماد على أجهزة الكمبيوتر وشبكات الاتصال المختلفة، عندما كانت التهديدات السيبرانية بسيطة نسبيًا، حيث اقتصرتْ على محاولات سرقة البيانات، أو التجسس على الوثائق، ولكن سرعان ما تطوّرتْ أساليب التهديد مع ازدياد تطور التقنية، ممّا دفعَ خبراء الكمبيوتر إلى ابتكار حلولٍ لمواجهتها، وكان من أوائل هذه الحلول برنامج (Creeper) الذي صمّمه *روبرت توماس* عام 1970م، وكان قادرًا على الانتقال عبر شبكة (Tenex) لمكافحة الملفات الضارة، بعد ذلك ظهور برنامج (Reaper) الذي ابتكره *راي توملينسون* عام 1971م، وهو أول برنامج مضاد للفيروسات، حيث كانت وظيفته مطاردة البرامج الضارة وحذفها (Madnick and Madnick:2024: 204-225).

كما شهدتْ هذه الحقبة بدايات ظهور مفهوم (الأمن السيبراني) بشكلٍ واضح، وذلك مع ازدياد اعتماد المؤسسات والأفراد على أجهزة الكمبيوتر، ممّا جعلها أكثر عرضةً للاختراق والهجمات الإلكترونية، ومن أبرز التطورات في تلك الفترة ازدياد جرائم الإنترنت وتطورها، ممّا دفعَ إلى اتّخاذ خطواتٍ جادة لحماية البيانات والأنظمة، وتنامي الوعي بأهمية الأمن السيبراني، وبدء الشركات والمؤسسات بتخصيص ميزانياتٍ لحماية أنظمتها، وأيضا ظهور برامج مكافحة الفيروسات بشكلٍ فعّال لمواجهة التهديدات المتزايدة (Middleton : 2017).

2.1.2.2.حقبة الثمانينيات :

تميّزتْ هذه الحقبة بثورةٍ في مجال الأمن السيبراني، عندما ظهر عام 1988م، فيروس (Morris)، الذي أدّى إلى خسائر فادحة في أنظمة الكمبيوتر في العديد من البلدان، وقد حفّز هذا الفيروس عمليات البحث في مجال مكافحة الفيروسات، التي كان من أبرزها تصميم العديد من برامج مكافحة الفيروسات المتقدمة، وتأسيس شركاتٍ متخصصة في مجال الأمن السيبراني؛ سعت جميعها إلى تقديم حلولٍ شاملة لحماية البيانات والأنظمة، كما ازداد الوعي بأهمية التشفير لحماية البيانات من الاختراق غير المُصرح به (Tarhan:2022).

3.1.2.2.حقبة التسعينيات :

شهدتْ هذه الحقبة ازديادًا هائلاً في اعتمادها على الإنترنت، ممّا أدّى إلى ظهور تهديداتٍ جديدةٍ ومتطورة، فمع ازدياد عدد مستخدمي الإنترنت، ازدادتْ أيضًا كمية البيانات الشخصية والمالية الحساسة المتاحة على

الشبكة، ممّا جعلها هدفًا مغريًا للمُخترقين (Tarhan:2022). وفي عام 1990م، شهد العالم هجوما عرف باسم (Spoofing)، أدى إلى إيقاف عمل أجهزة أصلية، مبرزا قضية (الجحيم العالمي)، التي زادت من مخاوف توسع الهجمات السيبرانية ثم تلتها الكثير من الحوادث الخطيرة، كحادثة شركة أوميغا، وفيروس مليسا، وغيرها (علاء الدين:2019: 92).

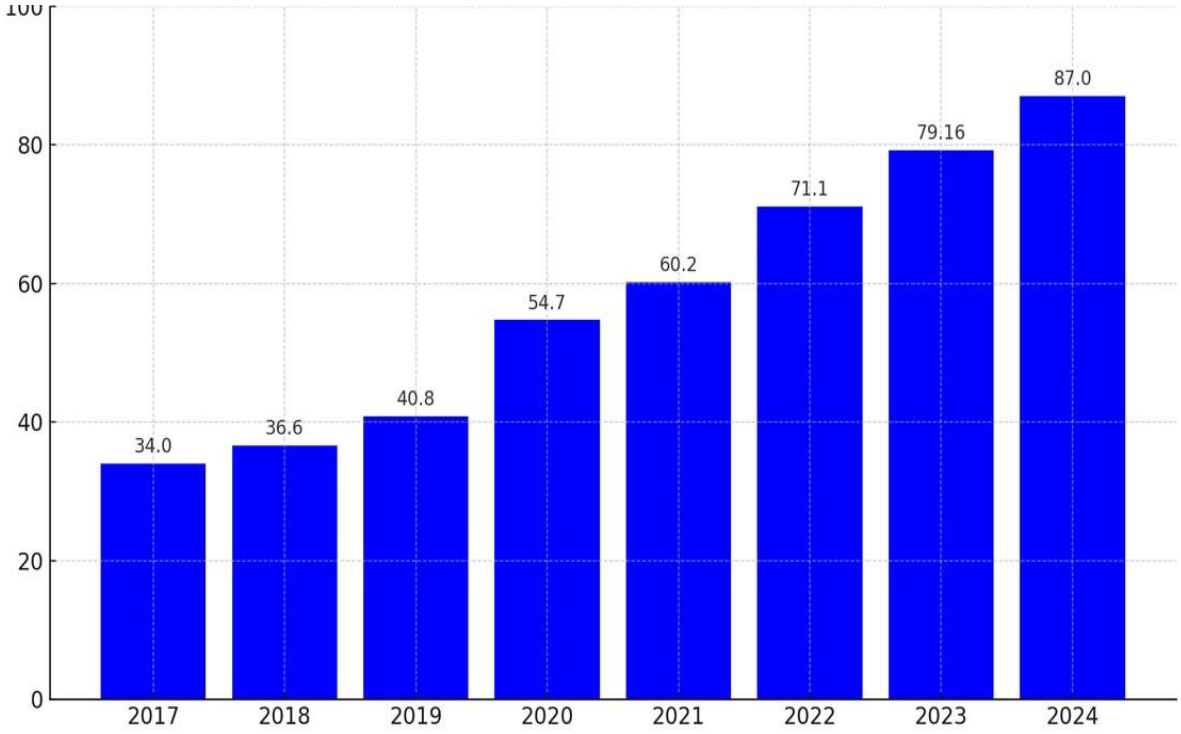
ورغم هذه الهجمات، أصبح الإنترنت أسرع وأقوى ثورة تكنولوجية في تاريخ البشرية، ففي غضون خمسة عشر عامًا، ارتفع عدد مستخدمي الإنترنت من 16 مليون مستخدم في عام 1995 إلى أكثر من 1.7 مليار، أواخر عام 2010م (Shrivastava:2013:8). وبعد التطورات والاختراعات الحديثة، وصل عدد مستخدمي الانترنت في العالم عام 2024م، إلى حوالي 5.52 مليار، وفقاً لبعض التقديرات، ومن المتوقع أن يستمر هذا الاتجاه الصاعد في السنوات القادمة(statista:2024).

وواكب هذا التطور والتوسع في استخدام الانترنت، ظهور أنواعٌ جديدةٌ من الفيروسات وبرامج التجسس وبرامج الاختراق، ممّا أدّى إلى مضاعفة الجهود لمكافحتها، وزاد انتشار جدران الحماية، وتمّ تطويرها لحماية أجهزة الكمبيوتر والشبكات من الهجمات الخارجية، ونمت صناعة الأمن السيبراني، وظهرتْ شركاتٌ متخصصةٌ في تقديم الحلول الأمنيةٍ الشاملة للمؤسسات والأفراد (Akeem:2019:37). منها على سبيل المثال لا الحصر، تأسيس شركة "مايكروسوفت" عام 1995م، لقسم الأمن الخاص بها (Microsoft Security:2011).

4.1.2.2.القرن الحادي والعشرون :

تميزت بداية القرن بظهور تطوّرات هائلة في مجال الأمن السيبراني، تزامنا مع تزايد تعقيد التهديدات السيبرانية، حيث ارتفعت وتيرتها على نطاق واسع، وشملت مؤسسات حكوميةً وشركات كبيرة، وظهرت جرائم إلكترونية وجماعات إجرامية منظمة، تهدف إلى سرقة البيانات والمعلومات الحساسة، من أجل الابتزاز، أو البيع في السوق السوداء، وبهذا ازدادت أهمية الأمن السيبراني لحماية الأمن القومي للدول، حيثُ أصبحت هذه التهديدات تُستخدم أداة للحرب والتجسس (Radhi and others:2013).

وقد تحول الأمن السيبراني من مجال تقني إلى قطاع اقتصادي ضخم يسجل أعلى نمواً بأربع مرات من الاقتصاد العالمي، حيث بات بحد ذاته سوقاً تجاوز قيمته 2 تريليون دولار في العام الواحد(المنتدي الدولي للأمن السيبراني:2024). وارتفع الإنفاق على الأمن السيبراني في جميع أنحاء العالم من 2017م إلى 2024م كما هو موضح في الشكل رقم(8) .



الشكل رقم(8)الإنفاق على الأمن السيبراني في جميع أنحاء العالم، المصدر(statista:2024)

يوضح الرسم البياني نسبة الإنفاق على صناعة الأمن السيبراني في جميع أنحاء العالم حيث سجل عام 2017م 34 مليار دولار، واستمر الإنفاق في الارتفاع حتى وصل 60.2 عام 2021م وزاد بشكل ملحوظ حتى وصل 87 مليار دولار عام 2024م.

5.1.2.2.الأمن السيبراني في المستقبل :

مع استمرار التطور التقني، تصبح التهديدات السيبرانية أكثر تعقيدًا وخطورة، ويواجه خبراء الأمن السيبراني تحديات هائلة في مقاومة هذه التطورات، ومن أبرز اتجاهاته في المستقبل هي التقنيات الحديثة التالية:

1. **الذكاء الاصطناعي**: إن العواقب المترتبة على الهجمات السيبرانية كبيرة، ويتعين على الدول معالجة المخاوف المتعلقة بأخلاقيات الذكاء الاصطناعي المضادة لها، والتهديدات المحتملة التي تشكلها الأنظمة السيبرانية المستقلة، من خلال تطوير القواعد اللازمة للاستخدام المناسب للذكاء الاصطناعي في العمليات السيبرانية (Petar:2024:35).
2. **الحوسبة السحابية**: تُصبحُ الحوسبة السحابية هدفًا مغريًا للمُخترقين، ممّا يتطلّبُ من مزودي الخدمات السحابية اتّخاذ تدابير أمنيةٍ مشدّدة (Bell:2024).
3. **تقنية (البلوك تشين)**: تُعَد نظامًا لسجلات موزعة، ويسمح بإجراء معاملات آمنة وشفافة دون سلطة مركزية، ورغم ارتباطها بالعملات المشفرة مثل البيتكوين، فإن تطبيقها أوسع بكثير من الأموال الرقمية، ولتقنية (البلوك تشين) تطبيقات عديدة، وتتمتع هذه التقنية بمقاومة شديدة للتلاعب والاختراق، بفضل تصميمها اللامركزي، وإجراءاتها التشفيرية. ومع تزايد التهديدات السيبرانية،

فإن نشر تقنية (البلوك تشين) في البنية التحتية الحرجة وأنظمة الاتصالات، يمكن أن يحسن الأمن السيبراني من خلال الحفاظ على سلامة البيانات وخفض خطر الهجمات السيبرانية التي تعطل الاتصالات الدبلوماسية(Petar and Redanliev:2024:39).

4. **المدن الذكية**: في هذه المدن يتم ضمان الأمن السيبراني، من خلال تحديد الأصول الحرجة وإعطائها الأولوية للأمن القائم على السلوك الذي يضع معيارًا للتشغيل الطبيعي للأصول الحرجة، والتأكد باستمرار من أن جميع أجزاء المدينة تلتزم بالمعيار المذكور، واستبدال المكونات بسرعة في حالة الاختراق، أو الفشل، والتجزئة الآمنة للأصول الحرجة في شبكة المدينة (CITIESand and THREATS:2016:1).

2.2.2. أبعاد الأمن السيبراني :

يشمل الأمن السيبراني جميع القطاعات الاقتصادية والاجتماعية والسياسية والعسكرية، ويحمل امتدادات وأبعاداً استراتيجية، فأن أي خلل في أحد هذه القطاعات، قد يؤدي إلى عواقب وخيمة، حيث أن الفضاء الإلكتروني يتسم بالسرعة في التخطيط والتنفيذ، ويتطلب وجود قوة وأسلحة سيبرانية رادعة، تكون في مستوى قوة الهجوم الإلكتروني، وسيتم توضيح هذه الأبعاد على النحو التالي:

أولا: المجال السياسي :

الأمن السيبراني للقطاع السياسي يتمثل في حماية نظام الدولة وكيانها، وسيادتها على حدودها ومواردها، التي تعني حقها وواجبها في السعي إلى تحقيق رفاه شعبها في وقت تؤثر موازين القوة داخل المجتمع نفسه أمنها وسيادتها (قاسمي وبلغيث 2020:27:). وفي ظل الفضاء الإلكتروني أصبح بإمكان المواطن أن يتحول إلى لاعب أساسي، من خلال قدرته على الاطلاع على خلفيات القرارات السياسية، عبر الكم الهائل من المعلومات، التي تبثها الإنترنت، ومن خلال التسريبات المتعلقة بالوثائق الحساسة مثلا، والتي تثير مشكلات كبيرة للحكومات، كما تلعب شبكات التواصل الاجتماعي دورا بارزا في تنظيم الدعايات السياسية، والانتخابات، وتنظيم التظاهرات الافتراضية، وافتعال الاحتجاجات الإلكترونية...إلخ (Marina : 2019 : 468) . ومن أبرز الامثلة على ذلك، ما شهدته بعض الدول العربية، ومنها ليبيا، من احتجاجات عام 2011م، استخدمت فيها وسائل التواصل الاجتماعي لتعبئة الناس وتنسيق الاحتجاجات، أدت إلى سقوط بعض الأنظمة الحاكمة (Palmieri: 2021) . ويعد الأمن السيبراني للقطاع السياسي، ذو أهمية بالغة، فالسياسة تلعب دورًا كبيرًا في صنع السياسات والتشريعات التي تؤثر على كيفية تعزيز الأمن السيبراني، على المستوى الوطني والدولي، بالإضافة إلى أن السياسة تلعب دورًا حيويًا في تحديد كيفية التعاون بين الدول، والمؤسسات الدولية، لمواجهة التهديدات المشتركة.

ثانياً: المجال العسكري :

كانت البدايات الأولى للإنترنت في القطاع العسكري، من خلال التعاون مع المؤسسات العلمية والأكاديمية، تمثلت في إجراء أبحاث علمية تخدم القدرات العسكرية وتطورها، والإنجازات العلمية التي تسهم في تفوق بلد على آخر (لامية:2020:356) وتكمن الميزة النسبية للقوة السيبرانية في قدرتها على ربط الوحدات

العسكرية بعضها ببعض عبر الشبكات العسكرية في الفضاء الإلكتروني، مما يسمح بسهولة تبادل المعلومات وتدفقها، وسرعة أتخاد القرارات العسكرية، وتحقيق الأهداف عن بعد، فعدم استغلال هذه التقنية والتسلح بها، أو تأمينها بشكل جيد قد يؤدي إلى شن هجمات إلكترونية مضادة على شبكات القوات العسكرية، معرضا إياها لتدمير قواعد البيانات وملحقا بها مخاطر كبيرة (Kostyuk:2024).

ومما يدل على أهمية للأمن السيبراني في القطاع العسكري، ارتفاع نسب انفاق دول عليه، حيث بلغ الانفاق العسكري على حرب الفضاء الالكتروني 127 مليون دولار سنويا، من اجمالي الانفاق العسكري الذي بلغ اربعين مليار دولار في روسيا، والتي تحتل المركز الرابع عالمياً في مجال تطوير قدرات الأسلحة الالكترونية، بينما تأتي الصين في المركز التأني وتبلغ قيمة انفاقها 55 مليار دولار(العمري2020:36).

هذا يعني أنَ الأمن السيبراني زاد من التزامات الدول نحو أمنها القومي، ومن الأمثلة التي يمكن الاستدلال بها لتوضيح الأبعاد العسكرية للأمن السيبراني وخطورة الهجمات السيبرانية، ما حصل في جورجيا واستونيا وإيران، من الهجمات والاختراقات، وما حصل بين روسيا وجورجيا، أو عندما انقطع اتصال الانترنت في استونيا، الذي أثر على الدولة والموطنين، وكذلك التشويش على الإدارات الحكومية (جبور:2016:28).

ثالثاً: المجال الاقتصادي :

يرتبط الأمن السيبراني ارتباطا وثيقا بالاقتصاد، فقد أصبح الفضاء الإلكتروني داعما لقطاعات المجتمع كافة، وباتت المعرفة محرك الانتاج والنمو الاقتصادي، كما أيقن الجميع أن مبدأ التركيز على المعلومات والتقنية، يعد عامل من العوامل الأساسية للنهوض بالاقتصاد، وهو ما يبرر تزايد الاستثمارا في المعرفة، ودخل العالم عصر الاقتصاد الرقمي (لامية:2020: 357). وبالتالي فإن استخدام الكمبيوتر وشبكات الإنترنت في تطوير وتحريك الاقتصاد، ومعالجة كل المعاملات الإقتصادية والمالية، زاد من أهمية وضرورة توفير الأمن السيبراني، لضمان حماية هذه المعلومات (بارة: 2017: 160) .

هذا وقد أصبحت هذه المجالات مرتبطة ببعضها، عبر شبكات الكمبيوتر (سلمان وجاسم:2023: 636). وانطلاقا من أنَّ الأمن السيبراني يعني القدرة على التحكم في الوصول إلى أنظمة الشبكات والمعلومات التي تحتوي عليها، كما أنه يعني القدرة على الحفاظ على سرية تلك المعلومات وسلامتها، وضمان حماية أنظمة الكمبيوتر من التداخل عبر الإنترنت، فإنَّ لانعدام الأمن السيبراني تأثير على الاقتصاد كله، فهو ينطوي على أبعاد أمنية وطنية ودولية (قوادرة وكحلوش:2021:211). وبهذا يمكن أن يسهم الأمن السيبراني في استخدام أدوات تحليل التكلفة لاتخاذ القرارات في سياق إدارة المخاطر، التي تهدف إلى تحديد حجم الاستثمار في الأمن السيبراني حسب التكلفة المتوقعة (Uddin and others:2020:215). لقد أصبحت جرائم الإنترنت من الأعمال التجارية، حيث يتجاوز حجم الاحتيال، عبر الإنترنت وسرقة الهوية، وانتهاكات الملكية الفكرية، وأعمال الفدية والتصيد، ما يُقدر بتريليون دولار سنويًا وهناك دول أصبحت عرضة للتهديدات السيبرانية التي أثرت على مصالحها الاقتصادية، حيث تم تعطيل بعض المصانع، وتأخير أعمال الشركات والمؤسسات المالية، فقد شهدت المملكة المتحدة وألمانيا والهند وأستراليا العديد من الهجمات الإلكترونية الخطيرة، التي استهدفت الخدمات الحكومية خلال السنوات الـــ 10 الماضية، ومن أبرزها الاعتداءات على

الوكالات الحكومية، والإدارات الدفاعية، وشركات التقنية المتقدمة في الدولة، وأدت إلى خسائر اقتصادية تجاوزت المليون دولار(Marina:2019:480).

وعلى سبيل المثال لا الحصر، يمكننا الاستشهاد بهجوم (WannaCary)، الذي استهدف أكثر من 200 ألف شركة في جميع أنحاء العالم عام 2017م، وأدى إلى خسائر اقتصادية تقدر بمليارات الدولارات (Algarni: 763 : 2021). وهجوم (SolarWinds)، عام 2020م، الذي استهدف الحكومة الأمريكية، وشركات القطاع الخاص، وأدى إلى سرقة بيانات حساسة، وإلحاق الضرر بالبنية التحتية الرقمية للولايات المتحدة (Huddleston: 2021: 760).

رابعاً: المجال الاجتماعي :

يفوق عدد مستخدمي الانترنت 5.52 مليار شخص في العالم عام 2024م، منهم ما يزيد على 5 مليار يستخدمون وسائل التواصل الاجتماعي (Statista:2024). حيث تساهم شبكات التواصل الاجتماعي بشكل مباشر في فتح المجال للأفراد، للتعبير عن تطلعاتهم السياسية وطموحاتهم الاجتماعية بأشكالها المختلفة، كما أنَّ مشاركة جميع شرائح المجتمع ومكوناته تشكل فرصة لتطوير المجتمع، من خلال الاطلاع على الأفكار والمعلومات، كما أن انفتاح المجتمعات على بعضها، يمنح الفرص لتبادل الخبرات والأفكار وتوسيع آفاق للتعاون والتكامل (قاسمي وبلغيث :2010: 28). وتعتبر الشبكة الدولية للمعلومات مجالاً مفتوح لجميع الأفراد، حيث يمكن لجميع المتعاملين السيبرانين أن يستفيدوا من البنية التحتية والخدمات المتاحة من دون تحمل أية مخاطر أمنية، وهنا يجب التنويه إلى ضرورة التحسيس بأخلاقيات الأمن السيبراني (Henschke:2022).

وقد جاء في تقرير الاتحاد الدولي للاتصالات لعام 2010م، بشأن الإبعاد الاجتماعية للأمن السيبراني أن، الثورة الرقمية غيرت كيفية التعامل التجاري، وعمل الحكومات، وقد أدت العولمة والتقدم التقني إلى إضعاف البنيه التحتية، وبالتالي جعلها هدفًا محتملاً لهجمات إرهابية، حيث تُواجه البلدان مخاطرا حقيقية، حيث يمكن أن تُستغل مواطن الضعف التي تعاني منها أنظمة المعلومات الدقيقة، لشن هجمات تؤدي إلى تعطيل البينة التحتية والموارد الأساسية من أجل تهديد الأمن القومي (الاتحاد الدولي للإتصالات:2010).

ومع تزايد أعداد المستخدمين للتقنية، ارتفعت معدلات الجريمة السيبرانية، وظهرت مجموعة من البرامج السلبية الإلكترونية، الهادفة إلى التنمر، والاحتيال، والابتزاز الإلكترونى، وغيرها من الممارسات التي تتسببت في العديد من المشكلات الاجتماعية (حسن 2018: 17). وفي هذا السياق يأتي التشديد من قبل المنظمات والهيئات الدولية على نشر ثقافة الأمن في الفضاء الإلكتروني، وضرورة تعاون المجتمع، بكل مكوناته، على تحقيقه وضمانه، فلا شك أنَّ المخاطر السيبرانية ستطال الجميع عند وقوعها، لذا فلابد من بناء مجتمع مسؤول، ومدرك لمخاطر الفضاء الإلكتروني، وقادر على التعامل مع قواعد السلامة، وإدراك العواقب القانونية التي يمكن ان تترتب عن بعض التصرفات في هذا الفضاء(جبور: 2016:29).

ومن ابرز الأمثلة على ذلك هجوم تنظيم الدولة الإسلامية(داعش) الذي شنه عبر تويتر عام 2015م، وتمثل في بنشر تغريدات مزيفة على الموقع ، تُهدد بشنّ هجمات إرهابية على الولايات المتحدة الأمريكية، مما أدى

إلى اندلاع حالة من الخوف والذعر بين المواطنين الأمريكيين (Magdy: 2015). ولهذا يعد تعزيز الثقافة الرقمية الإيجابية أمرًا ضروريًا لحماية الأمن القومي للدول، من مخاطر التهديدات السيبرانية.

خامساً : المجال القانوني :

يترتب على النشاط الفردي والمؤسساتي والحكومي في الفضاء الإلكتروني التزامات قانونية، وهو ما يستدعى مواكبة التطورات التي رافقت ظهور مجتمع المعلومات، وما ظهر خلالها من أليات وأساليب وممارسات، عند استخدام شبكة المعلومات؛ كإنشاء المدونات والتجمعات على الإنترنت، حيث ترتب على ذلك الحق في حماية حقوق ملكية البرامج المعلوماتية، والإبلاغ عن المخالفات والجرائم السيبرانية، وإلى ظهور ترسانة قانونية تتوافق مع التغيرات الحاصلة (لامية:357:2020-354).

وتمثلت المخاطر القانونية، فى غياب القوانين المنظمة، وفي تناقض القوانين، وتنازع الأنظمة القانونية، مما أدى إلى ارتفاع معدل المخاطر، وضعف آليات الملاحقة القانونية الفاعلة، التي تتلاءم مع طبيعة الأعمال والجرائم والاعتداءات السيبرانية العابرة للحدود، وللأنظمة القانونية، حيث تطول أي مواطن في جميع الدول، وتعد المخاطر التى يتعرض لها الأفراد والدول هائلة وغير مقيدة بالأطر القانونية السائدة، التى ما زالت لا تستوعب العصر السيبرانى بالقدر الكافى، وهناك حاجة عاجلة إلى خطط وسياسات سريعة تُقيم بها القيادات السياسية والسيبرانية، هذه المخاطر، وتوسع قدراتها العسكرية لتشمل النزاع السيبرانى، ويجب أن تتوازن بحيث لا تتعارض مع القوانين والتشريعات (المطيري 2022: 969).

ويمكن استنتاج بأنه المعالجات القانونية لمخاطر الأمن السيبراني تُعد أمر ذو أهمية بالغة، فهي تلعب دورًا حيويًا في تحديد الأطر القانونية، التي تُنظم استخدام وحماية البيانات الرقمية، بالإضافة إلى أنه يساهم في توفير الحماية القانونية للأفراد والمؤسسات ضد التهديدات السيبرانية، وضمان تطبيق العدالة الرقمية، لذلك، فإن تطوير القوانين والتشريعات والامتثال لها، يُعد عنصر أساسي لضمان الأمن السيبراني وحماية البيانات الحساسة.

3.2.2 العلاقة بين الأمن السيبراني والأمن القومي :

تزداد العلاقة بين المفهومين، بازدياد عمليات نقل البيانات والمعلومات، في مختلف المجالات، إلى الفضاء الإلكتروني، خاصة مع ظهور الحكومات الالكترونية، والمدن الذكية في العديد من الدول، واتساع نطاق مستخدمي الانترنت في العالم، والثورة الكبرى في انترنت الاشياء، فقد أصبحت قواعد البيانات القومية في حالة انكشاف، وهو ما دفع الدول إلى ادخال الأمن السيبراني ضمن استراتيجية الأمن القومي (عبد الجواد:435:2020:).

فتهديدات الأمن السيبراني تمثل أحد أخطر التحديات التي تواجهنا، وذلك فيما يتصل بالأمن القومي، والسلامة العامة، ومختلف مناحي الحيالة، خاصة وأن التقنيات ذاتها، تعمل على تمكين أولئك الذين يسعون إلى التعطيل والتدمير، فحياتنا اليومية وسلامتنا العامة تعتمدان على شبكات الطاقة والكهرباء والمواصلات... وغيرها،

وهي نقاط ضعف، قد يستغلها الخصوم المحتملين لتعطيلها على نطاق واسع، إذا، فحماية البنية التحتية الرقمية هي أولوية للأمن القومي (McKenzie :2017 :1) .

هذا وقد تبلورت المصالح القومية للدول في الفضاء الإلكتروني، نتيجةً لزيادة الاعتماد على ربط بنيتها التحتية به، في بيئة تشابكية واحدة تُعرف بالبنية التحتية الوطنية للمعلومات (NII)، وتتضمن قطاعات حيوية كقطاع الطاقة، والاتصالات، والنقل، والخدمات الحكومية والمالية، والتجارة الإلكترونية وغيرها (فرحات:2019:102). وأصبح الأمن القومي ذا صلة وثيقة بتقنية المعلومات والاتصال الخاص بأية دولة، وذلك بحكم قدرتة على التأثير في أي مجتمع، فقد اختصرت وسائل التواصل الاجتماعي الوقت والمسافة، وحققت تأثيرا فعالا لدى معظم الدول (الشمري: 2021:161-162).

وهكذا، أصبح الأمن السيبراني جزاء لا يتجزأ من الأمن القومي، خاصة مع تنامي حجم التهديدات، وارتباط الأمن الإلكتروني بعمل المنشآت الحيوية، ومع اعتمادنا على شبكات الكمبيوتر أساسا للقوة العسكرية والاقتصادية، فإن أمننا الوطني والاقتصادي قد يصبح معرضاً للخطر :Finnemore and Hollis) (426 :2016 إن الدول التي تهتم بالأمن السيبراني تتمتع بقدرة الحفاظ على قوات عسكرية وقدرات اقتصادية أقوى داخل النظام الدولي، فهي أكثر حرصا على تأمين الفضاء الإلكتروني، بنفس المستوى الذي تتعامل به مع التهديدات الأكثر تقليدية، لأنها تدرك أن الخصوم المحتملين قد يعرضون بنيتها التحتية الحيوية للخطر في الفضاء الإلكتروني (Hare: 218:2010) . إذا، فالأمن السيبراني يرتبط بالأمن القومي بشكل وثيق، والتقنيات التي وسعت الأفكار وأثرت على الثقافة، وسمحت للثقافة المحلية بالامتداد إلى المجال العالمي، باتت تهدد الهوية الوطنية والقومية، ومع تأثر الأجيال الصاعدة بما يصلها وبما تصل اليه عبر شبكة الانترنت، أصبحت الهوية كأنها خاضعة لعملية إعادة تشكيل من خلال تكنولوجيا المعلومات (جبور:2016: 27).

إنَّ الأمن السيبراني يهدف إلى مقاومة المخاطر السيبرانية، التي تهدد الدول، وبالتالي تحريرها من الخطر، او الأضرار الناجمة عن إساءة استخدام تقنية المعلومات والاتصالات، بحماية الاجهزة والشبكات والبرامج والبيانات من الهجوم، او الضرر. ونتيجة لأهمية الأمن السيبراني، فقد جعلته العديد من الدول على راس أولوياتها، خاصة بعد التهديدات التي بدات تظهر تجلياتها بين الدول الكبرى (عبد الجواد : 2020: 437-438). ويمكننا الاستنتاج أن الأمن السيبراني ليس مسألة تقنية فقط، بل هو جزء أساسي من استراتيجية الأمن القومي لأي دولة، لكونه يلعب دوراً حيوياً في حماية الأمن القومي للدول حيث يسهم في تأمين البنية التحتية الحيوية والحفاظ على السيادة الوطنية، والتصدي للتهديدات السيبرانية بكل أشكالها وأنواعها.

3.2.حالات ونماذج للتهديدات السيبرانية

سيتم في هذا المبحث تقديم تحليل علمي لحالات ونماذج متعلقة بالتهديدات السيبرانية التي تعرضت لها دول مختلفة وكيفية تأثيرها على أمنها وسيتم التركيز على حالات دراسية بارزة مثل التهديدات التي تعرضت لها إستونيا عام 2007، وأيضا التحديات السيبرانية التي واجهتها جورجيا خلال الحرب الروسية الجورجية عام 2008، بالإضافة إلى تلك التهديدات التي واجهتها السعودية عام 2012 وسيتم استعراض نماذج

للتهديدات السيبرانية بين دول كبرى مثل روسيا وأوكرانيا، وبين الصين والولايات المتحدة الأمريكية، وبين إيران والولايات المتحدة الأمريكية ، وأيضًا الصراعات بين روسيا والولايات المتحدة الأمريكية.

إن الغرض من دراسة هذه النمادج والحالات هو زيادة مستوى المعرفة بأهمية الأمن السيبراني ومعرفة اخطر الحوادث للتهديدات السيبرانية في العالم التي غيرت افاق كل العالم السيبراني حيث تبرز هذه الحالات والنماذج التصاعد السريع للهجمات السيبرانية بين الدول، وتسلط الضوء على كيفية تأثيرها على السياسات الخارجية والقرارات الاستراتيجية للدول المتورطة كما توفر هذه النماذج فهمًا عميقًا لعملية تحليل التهديدات السيبرانية، وسيتم مناقشة مدى تأثير التهديدات على النحو الآتي :

1.3.2. التهديدات السيبرانية على إستونيا :

تُعد استونيا من الدول المتقدمة في مجال تكنولوجيا الاتصال والمعلومات، حيث شهد ذلك القطاع نمواً سريعاً بين عامي 2000م و 2007م، عندما أصبح 25% من السكان يستطيعون الدخول إلى الانترنت والتمتع بالعديد من الخدمات الحكومية، وغيرها من الخدمات التي تعتمد على الفضاء الإلكتروني (الموصلي:2021:70). وقد بدأت الحرب السيبرانية في العاصمة تالين بالقرب من هلسنكي يوم الجمعة 27 ابريل 2007م، واستمرت لمدة ثلاثة اسابيع (Shrivastava:2013:13). وفي صباح الثامن والعشرين من شهر إبريل 2007م، حاصرت موجات من هجمات الحرمان من الخدمة، مواقع إلكترونية في إستونيا وعلى مدى اسبوعين متتاليين، استهدف المهاجمون قطاعات حيوية، فأغلقوا الوصول إلى الإنترنت لمئات من صفحات الويب الرئيسية التابعة للحكومة والمصارف ووسائل الإعلام (Theohary and Harrington:2015:12) وتسبب الهجوم في عرقلة وصول المواطنين إلى بعض المواقع مثل، موقع الحزب السياسي الذي ينتمى إليه رئيس الوزراء (البهى: 6:2017) ولم يعد المواطنون قادرين على إجراء معاملاتهم المصرفية الإلكترونية التي يتم 97% منها عبر الانترنت، أو التواصل مع بعضهم بالبريد الإلكترونى لأيام عديدة، وتم تعطيل البنية التحتية للاقتصاد الرقمي الإستوني (خليفة: 2018: 11). وكان هذا الهجوم قد بدأ على خلفية قرار الحكومة الإستونية نقل تمثال يخلد تضحيات جنود روس في الحرب العالمية الثانية إلى مكان آخر (شفيث: 2028: 139).

ونتيجة لشدة تعقيد هذه الهجمات، وما أحدثته من شلل كامل في كافة أجهزة الدولة، استعانت استونيا بحلف شمال الأطلسي لمواجهتها، ووجهت استونيا الاتهامات للحكومة الروسية، بأنها تقف وراء ما تعرضت له من هجمات، بعد أن اكتشفت ان انظمة التحكم التي شنتها موجودة في روسيا، وعلى الرغم من انكار روسيا لصلتها بالهجوم، فأنها اعترفت أنه من الممكن ان يكون قد شن من داخل روسيا من قبل منظمات إجرامية غاضبة من القرار الإستوني بنقل التمثال هذا وقد انقسمت الهجمات الالكترونية التي تعرضت لها استونيا في 2007م (شفيق: 2018: 141) إلى مرحلتين هي:

المرحلة الأولى: مرحلة الرد المباشر من 27-29 ابريل 2007م، حيث بدأت الهجمات باستهداف المواقع الالكترونية الحكومية والإعلامية التي بثت أخبار عن العمل في استونيا، كموقع رئيس الوزراء، ورئيس

والبرلمان والوزارات ومؤسسات الدولة الأخرى كالشرطة، وتم اختراق عديد من المواقع الأخرى، التي كان من بينها موقع حزب الاصلاح الذي قام المهاجمون من خلاله بنشر اعتذار رسمي مزور باللغة الروسية عن نقل التمثال الذي يبدو وكأنه صادر من رئيس الوزراء الإستونى، ولكن اتسمت هذه الهجمات في هذه المرحلة ببساطتها، إذ كانت أشبه بالاحتجاج الشعبي.

المرحلة الثانية: مرحلة التعقيد من 30 إبريل إلى 18 مايو 2007م، شهدت تلك الفترة هجمات أكثر تعقيداً وتنظيماً، تم فيها استخدام البوتنتس Botnets وهجمات الحرمان من الخدمة الموزعة، والتي اتسع نطاق استهدافها لتهاجم اكبر المصارف الموجودة في إستونيا، حيث فاق عدد طلبات الدخول الى هذه المواقع ٤٠٠ ضعف المستوى الطبيعي، كما استهدفت أيضاً البنية التحتية القومية للإنترنت، وخط الطوارئ القومي للحيلولة دون تلقى الشكاوى من المواطنين، وقد كان لهذا الهجوم الذي تعرضت له استونيا آثارا قصيرة المدى وطويلة المدى، سواء على المواطنين، أو الأجهزة الحكومية، أو المصارف؛ فمن جهة ترتب على الهجوم تعطيل كامل لكافة الخدمات التي تقدمها الحكومة للمواطنين فترة طويلة نسبيا(لوماس: 2015: 77-79).

وكانت الأهداف الرئيسية لهذا الهجوم في المقام الأول خوادم المؤسسات المسؤولة عن البنية التحتية للإنترنت الإستونية وتليها الأهداف الحكومية والسياسية مثل البرلمان والرئيس والوزارات والهيئات الحكومية، وأيضا الخدمات التي كان يقدمها القطاع الخاص (الخدمات المصرفية الإلكترونية، ووكالات الأنباء، وغيرها) وأخيرا، الأهداف الشخصية والعشوائية (Shrivastava:2013:14) ويلاحظ هنا أن، الأثر كان معنوياً أكثر منه مادياً، إذ لم ينتج عن الهجوم أية أثار تدميرية، فقد انتهت آثار الهجوم فور السيطرة عليه، ولم تمتد الى فترة أبعد، في حين أن ما نتج عن هذا الهجوم هو توجيه انتباه استونيا وغيرها من الدول إلى خطورة التهديدات الالكترونية، وكيف أنه بإمكانها شل حركة الدولة تماماً حتى وان كان لفترة محدودة (شفيق: 2018: 143).

أثبت هذا الهجوم أنَّ موقف الردع السيبراني لإستونيا قابل للجدل، كما توقع المنظرون ولكن ليس بالدرجة التي توقعوها، على الرغم من أن جهود الأسناد أظهرت عدم فعالية، بسبب انتهاك روسيا لاتفاقياتها القانونية الدائمة مع إستونيا، فأنه ذلك أدى إلى رفض روسيا احترام الاتفاقيات، مما منح إستونيا فرصة تحميل روسيا المسؤولية عن الهجوم ولكن، حتى لو قامت استونيا بتحميل المسؤولية إلى روسيا، فإن عدم توازن القوى بين البلدين سيترك لاستونيا خيارات قليلة للانتقام، لذا سعت إستونيا إلى استعادة التوازن في علاقتها مع روسيا من خلال التواصل مع حلفائها في حلف شمال الأطلسي لإضافة الدفاع السيبراني إلى ميثاق الناتو، بغية تحقيق مشاركة مشتركة في الدفاع السيبراني (will: 2010:114).

2.3.2.التهديدات السيبرانية على جورجيا :

يأتي التهديد السيبراني على جورجيا، في إطار زمني وسياق صراع مسلح أوسع نطاقاً اندلع يوم الجمعة 8 أغسطس 2008م، واستمر حتى يوم الخميس 28 أغسطس 2008م، وبلغت المدة الإجمالية لهذا الهجوم 3 أسابيع (Shrivastava:2013:16). خلال الحرب بين روسيا وجورجيا، أدت الهجمات الالكترونية المتزامنة مع العمليات البرية والجوية الروسية إلى، شلل الانترنت الجورجي، وتم ذلك من خلال إغراق

خوادم النظام بسيل، لا يمكن السيطرة عليه من حركة الويب، وقد ضغطت الهجمات على المواقع الحكومية والمصرفية والاعلامية (van:2023:17) . وقد اتخذ هذا الهجوم محورين رئيسين هما:

أولا: اختراق بعض المواقع الالكترونية فقد تم مهاجمة مواقع إلكترونية سياسية، حكومية، من بينها موقع رئيس الجمهورية ووزارة الخارجية، ثم ظهرت على الموقع صورة الزعيم النازي ادولف هتلر بجانب صور لرئيس الجمهورية، وغيره من الحكام الديكتاتوريين.

تانياً: هجمات الحرمان من الخدمة حيث تم مهاجمة المواقع الخدمية مثل، موقع وزارة التربية والتعليم، وموقع البرلمان والرئاسة، وأكبر مصرف تجاري في جورجيا، كما تمت مهاجمة مواقع الأخبار ووسائل الاعلام، التى شملت أكبر مواقع أخبار في جورجيا، وشبكات إخبارية من بينها ،BBC CBC، لدرجة أنَّ وزارة الشؤون الخارجية الجورجية، وضعت لنفسها بريدا الكترونيا مجانيا على موقع البحث الالكترونى جوجل Google، واستبدلت الموقع الالكترونى، الذى توقف فجأة، بمدونة الكترونية مجانية من جوجل ايضاً (عبد الصادق : 2009: 216). وياتي هذا الهجوم الروسى رداً على إرسال الحكومة الجورجية الموالية للغرب قوات ضد الحكومة الانفصالية المدعومة من موسكو في جورجيا، وكانت الأهداف الرئيسية لهذا الهجوم هي؛ المواقع الحكومية مثل المواقع الرسمية لرئيس جمهورية جورجيا، وبرلمان جمهورية جورجيا، وبوابة أخبار جورجيا، ومواقع الأخبار والإعلام ومنتديات النقاش على الإنترنت المؤسسات المالية (17-2013:16 Shrivastava).

3.3.2 التهديدات السيبرانية على المملكة العربية السعودية :

تعرضت السعودية لعدد من الهجمات السيبرانية، التي استهدفت في البداية شركة أرامكو المملوكة للدولة، فقد ظهرت صور لعلم امريكي محترق، على شاشة الحواسيب العاملة في مكاتب الشركة، كنتيجة لهجمات مجهولة المصدر، وقد سببت هذه الهجمات أضرارا كبيرة على البنية التحتية، وعطلت نشاط الشركة لمدة شهر فيما يشار إليه بأكبر اختراق في التاريخ (Arab News :2016) . ويعود تاريخ هذا الهجوم إلى 15 أغسطس 2012م، عنما استهدف فيروس شمعون الخبيث الشركة، أدى إلى تدمير البيانات على ثلاثة أرباع أجهزة الكمبيوتر التجارية المملوكة للشركة، ولتقليل المخاطر، تم فصل شبكات الأعمال عن أنظمة التحكم التشغيلية، مما يعني أن الضرر لم يؤثر على إنتاج النفط بشكل، انَّ القراصنة الذين أطلقوا على أنفسهم اسم "سيف العدالة القاطع"، أعلنوا عن مسؤوليتهم عن الهجوم، ولكن خبراء الأمن السيبراني، الذين أرسلوا إلى الشركة للتحقيق، اكتشفوا شفرة تشبه فيروس "فليم"، الذي سبق أن استُخدِم في هجوم على محطة النفط الإيرانية في جزيرة خرج، وكان الاستنتاج أن إيران سعت إلى الرد على هذا الهجوم (Schwindt and Marcinek:2019:25).

ترك شمعون العمليات التجارية للشركة في حالة يرثى لها؛ فقد فقدت أرامكو السعودية قدرتها على سداد المدفوعات، وإدارة الإمدادات وتتبع الشحنات، وتوقف توزيع النفط محليًا مدة سبعة عشر يومًا، مما أدى إلى نقص الغاز وانتهى الأمر بالشركة إلى توزيعه مجانًا لفترة قصيرة وإلى استبدال أجهزة الكمبيوتر الخاصة

بها، واستخدمت أرامكو طائرات خاصة لنقل الموظفين إلى مصانعها في جنوب شرق آسيا مع أوامر بشراء كل محرك أقراص ثابت متاح، مما أدى إلى ارتفاع الأسعار العالمية للنفط، واستغرق المعالجات خمسة أشهر لإعادة العمليات التجارية إلى العمل (Finnemore and Hollis:2016:430). وأوضح تقرير صادر عن المجلس الاستشاري للأمن السعودي في عام 2016م، أن الهجوم على شركة أرامكو السعودية كلفها تغيير 50 ألف قرص صلب لأجهزتها الحاسوبية، ولم تستطع استخدام الإنترنت لمدة خمسة أشهر تقريبا، وهذا يعد زمنًا قياسيًا في الإصلاح؛ خاصة إذا ما أخذنا في الاعتبار إمكانات أرامكو المالية والتقنية (السمحان:2020:5-6).

لاحقا، استثمرت المملكة العربية السعودية بكثافة في الأمن السيبراني، من خلال إنشاء الهيئة الوطنية للأمن السيبراني (NCA) ، وتطوير الاستراتيجية الوطنية لأمن المعلومات(NISS) ثم أصدرت الهيئة الوطنية للأمن الإلكتروني لوائح وإرشادات جديدة لتحسين ممارسات الأمن السيبراني في القطاعين الحكومي والخاص، مع التركيز على رفع مستوى الوعي العام حول تهديدات الأمن السيبراني وأفضل الممارسات (IBM X-Force :2023).

4.3.2. التهديدات السيبرانية بين الولايات المتحدة الأمريكية- والصين :

تعود التهديدات السيبرانية بين البلدين إلى أبريل 2001م، حيث حدث توتر في العلاقات الأمريكية الصينية عندما أرسلت الولايات المتحدة الامريكية طائرة تجسس على الساحل الجنوبي للصين، وهو ما ردت عليه الصين بإرسال طائرة حربية اصطدمت مع الطائرة الأمريكية فأسقطتها، وأضطر طاقم الطائرة الأمريكية إلى الهبوط على الأراضي الصينية، ليتم احتجازهم، وفي ظل هذا التوتر، تعرضت المواقع السيبرانية الخاصة بالجيش الأمريكي إلى هجمات الحرمان من الخدمة من قبل عدة جماعات صينية (Eliot :2015).

ولعل من اخطر ما تعانيه الولايات المتحدة الأمريكية في مجال التهديدات السيبرانية ذات البعد العسكري هو تعرضها المستمر لسرقة البيانات والمعلومات العسكرية، أو التلاعب بها، والسيطرة على نظم الدفاع الجوي والطيران، لاسيما أن المؤسسات العسكرية الأمريكية وإدارة الأقمار الصناعية والصناعات الحربية والغواصات النووية ونظم الدفاع الجوي والطيران كلها مرتبطة بأنظمة الكترونية حديثة(Chasdi:2017) وقد اظهرت دراسة تم نشرها عام 2018م، أقرها مجلس المستشارين الاقتصاديين للبيت الأبيض أن، الاقتصاد الامريكي يخسر سنويا بين 57 و109 مليار دولار، بسبب الهجمات السيبرانية على قطاع الخدمات المالية وشبكات الطاقة، وذكرت صحيفة (نيويورك تايمز) ان الحكومة الأمريكية تتهم الصين بمحاولة سرقة معلومات عن ابحاث بخصوص لقاح كوفير-19(كورونا)، واستغلال وقت الوباء لعمل هجمات على البنية التحتية والمؤسسات المالية الأمريكية، ويؤكد تقرير صادر من مجلس السياسة الخارجية الأمريكية أنَّ، أجهزة الاستخبارات الصينية تعمل على استغلال الأشخاص ذوي الاصول الصينية داخل الشركات الأمريكية، من اجل سرقة المعلومات الاقتصادية من خلال البريد الالكتروني، على سبيل المثال لقد تم خلال عام 2014م،

الحكم في سبع قضايا تجسس اقتصادي ذات صلة بالصين (طة:2023:19-198 9). وقام قراصنة صينيون، بسرقة معلومات عسكرية أمريكية، تتعلق بمنظومات مضادة للصواريخ، من طراز (PAC-3) ونظام (THAAD)، مما مكن الحكومة الصينية من استخدام هذه المعلومات لتطوير تقنياتها العسكرية، ووفقا لتقرير لشبكة فوكس نيوز، فان الصين نجحت في تصنيع طائراتها المقاتلة من الجيل الخامس عن طريقة التجسس السيبراني، من خلال قيامها بنسخ التقنية العسكرية الأمريكية المتطورة، وتعود محاولات الصين للتحول إلى قوة سيبرانية عظمى، إلى عام 2014م، حيث قدَّم الرئيس الصيني (*شي جين بينغ*) مفهوم "القوة السيبرانية العظمى(كلاع: 2023: 227). ثم بدأت الصين في الاهتمام بوضع استراتيجية سيبرانية عام 2016م، خلال المؤتمر العاشر للحزب الشيوعي الصيني، حيث أكدت السلطات العليا على أهمية المجال السيبراني، وتم دعم هذه الاستراتيجية من خلال أول قانون صيني للأمن السيبراني الصادر في 2017م (Jinghua :2019). الذي حدد تسع مهام أساسية، مع التركيز على السيادة وتقوية الدفاع الإلكتروني، وعملت اللجنة المركزية للحزب على تطويره، وفي الوقت نفسه حوكمته، وقامت أيضاً بترتيب القضايا ذات الصلة بالإعلام والقوة السيبرانية في جميع المجالات، مما يتيح للصين فرصة بناء وتطوير استراتيجية سيبرانية قادرة على المنافسة في الساحة الدولية (الجاني والشمري:2012:17). إنّ التطورات التي حققتها الصين والقدرة التي اكتسبتها في تطوير قدرات الهجمات السيبرانية، وبناء المؤسسات ذات الصلة، والقدرة على توظيف أدواتها السيبرانية في العمليات العسكرية، جعل مؤشر القوة السيبرانية الوطني لعام 2022م، الصادر عن مركز بيلفر للعلوم والشؤون الدولية، التابع لجامعة هارفادر، يصنف الصين على أنها ثاني أكبر قوة سيبرانية شمولاً بعد الولايات المتحدة (Baidya:2022).

وتتوافق هذه التقديرات، إلى حد كبير، مع ما استعرضه المعهد الدولي للدراسات الاستراتيجية (IISS) في تقريره الصادر في يوليو 2021م، ووضع ترتيباً للقوى السيبرانية الكبرى في العالم، معتمداً على سبعة معايير هي الاستراتيجية والعقيدة، والإدارة والقيادة والسيطرة، وقدرات الاستخبارات السيبرانية، والاعتمادية على الفضاء السيبراني، والأمن السيبراني، والريادة العالمية في الفضاء السيبراني، والقدرات السيبرانية الهجومية (IISS:2021).

في مايو عام 2014م، وجهت الولايات المتحدة الأمريكية الاتهامات إلى خمسة ضباط عسكريين صينيين قاموا باختراق أجهزة الكمبيوتر، والتجسس الاقتصادي، وجرائم أخرى ضد ستة أهداف في صناعات الطاقة النووية والمعادن والطاقة الشمسية في الولايات المتحدة، وتمثل هذه التهم أول اتهامات توجه إلى جهة فاعلة تابعة للدولة الصينية بهذا النوع من الاختراق (Theohary and Harrington:2015:34). كما ادانت المحكمة العليا الأمريكية في نفس العام ضباطا في الجيش الصيني، بارتكاب جرائم في مجال الشفرة وسرقة معلومات سرية ذات طبيعة تجارية، وتضمنت لائحة الاتهام قيامهم باختراق 6 اجهزة كمبيوتر لشركات امريكية، كذلك اتهمت وزارة العدل الأمريكية، عام 2017م، ثلاثة موظفين صنيين من شركة تقنية المعلومات، باختراق شركات أمريكية تعمل داخل الولايات المتحدة، منها سيمنتس(Siemens)، وموودي أناليتكس(Mmoodysa Analytics) (الموصلي:2021: 69).

وتشير بعض الأدلة إلى أنَّ الصين كانت وراء هجوم سولار ويندز خلال عام 2020م، ويُعدّ هذا الهجوم أحد أخطر الهجمات السيبرانية في التاريخ، حيث استهدف برامج شركة سولار ويندز الأمريكية، مما أدى إلى اختراق أنظمة حكومية وشركات في الولايات المتحدة وحلفائها، وتُشير الأدلة إلى تورط جهات قراصنة صينية في هذا الهجوم (Tran:2021).

كما أتهمت الصين في هجوم مايكروسوفت الذي تم خلال عام 2021م، والذي استهدف خوادم البريد الإلكتروني لشركة مايكروسوفت، وأثر على ملايين المستخدمين حول العالم، وتُشير التحقيقات إلى تورط جماعة صينية مدعومة من الحكومة في هذا الهجوم (Pitney and others:2022:3).

تم رصد هجمات سيبرانية على البنية التحتية الحيوية في كلتا الدولتين، بما في ذلك محطات الطاقة وشبكات النقل(Lehto:2022:9). وفي عام 2023م،، تعرضت عشرات الكيانات ذات البنية التحتية الحيوية لهجمات إلكترونية ضخمة، بما في ذلك شركة مياه في هاواي وميناء رئيسي على الساحل الغربي، وشبكة الكهرباء في ولاية تكساس (ناكاشيما ومين: 2023). وفي مايو من العام نفسه، نشرت مايكروسوفت تقريرًا زعمت فيه أنها وجدت مجموعة القرصنة الصينية (فولت تايفون) تعرض البنية التحتية الحيوية للخطر في الولايات المتحدة، وسردت عددًا من القطاعات الأخرى، بما في ذلك شركات الاتصالات (Megi:2024).

في مايو 2023م، كما اتّهمت وزارة الخارجية الأمريكية، في مايو 2023م، الصين بشنّ هجمات سيبرانية طويلة المدى ضدّ البنية التحتية الحيوية للولايات المتحدة، في المقابل، اتهمت الصين الولايات المتحدة بشنّ هجمات سيبرانية ضدّها منذ فترة طويلة (McAndrew:2023:540). وفي عام 2024م، أكد العديد من المسؤولين الأمريكيين، رفيعي المستوى، أن الصين اخترقت البنية التحتية الحيوية للولايات المتحدة، في شهادتهم أمام لجنة مجلس النواب المختارة للمنافسة الاستراتيجية بين الولايات المتحدة والحزب الشيوعي الصيني، وقد تمكنت فرق CISA من اكتشاف واستئصال الاختراقات الصينية للبنية التحتية الحيوية عبر قطاعات متعددة، بما في ذلك الطيران والطاقة والمياه والاتصالات (Megi:2024).

5.3.2. التهديدات السيبرانية بين الولايات المتحدة الأمريكية- وإيران :

تُعد الولايات المتحدة الامريكية في المستوى الأول في المجال السيبراني؛ إذ انَّها قادرة على تنفيذ مهام معقدة للغاية من التهديدات السيبرانية السرية، باستخدام برامج ضارة ضمن الأهداف الموجهة لديها Schulze and kerscher:2020:8). وإذ تعود بداية التهديدات السيبرانية للولايات المتحدة الأمريكية ضد إيران الى حملة سرية تدعى (عملية الألعاب الأولمبية) التي انطلقت عام 2006م، تحت إدارة الرئيس الأمريكي الأسبق *جورج دبليو بوش*(Andrew:2021)، الذي أراد اخراج البرنامج النووي الإيراني عن مساره، او إبطائه، ومع ذلك لم يرغب في شن غارات جوية على منشاة تخصيب اليورانيوم الايراني، وبدلاً من ذلك سعى إلى خيار الهجوم السيبراني لاستهداف انظمة التحكم في الحاسب الآلي، في منشاة نطنز باستخدام فيروس ستوكسنت (Stuxnet) الذي تم تطويره بمشاركة الكيان الصهيوني، من أجل استهداف أنظمة الحاسب الآلي للحكومة الإيرانية وقدرات إيران النووية (الموصلي:71:2021). وفي عام2010م، اعترف

المسؤولون الإيرانيون، أنّ أجهزة الكمبيوتر في محطة بوشهر النوويّة قد أصيبت بفايروس له تأثير بالغ، أدى الى توقف تخصيب اليورانيوم في محطة نطنز النووية بالكامل، جراء الفيروس المعروف باسم (ستوكسنت) الذي اتهمت ايران الولايات المتحدة الأمريكية بالوقوف وراءه(baezner:2017: 9). وأكد نائب مدير الوكالة الدولية للطاقة الذرية السابق (أولي هينونن)، انَّ الفيروس الالكتروني المعروف باسم (ستوكسنت) قد ولّد مشاكلات تقنية أثرت على البرنامج النووي الإيراني مما أدى ألى إيقاف الآلاف من أجهزة الطرد المركزي الخاصة بتخصيب اليورانيوم، وأظهر بحث أجرته شركات الأمن المعلوماتي أنَّ (60%) من الأجهزة المصابة بفايروس (ستوكسنت) توجد في ايران، لذا جاء في تقرير للوكالة الدولية للطاقة الذرية، نُشر في سبتمبر 2010م، أن إيران فصلت (160) جهاز طرد مركزي عن شبكة التحكم، حيث كان أول سلاح سيبراني حقيقي تم تصنيعه بهدف التسبب في ضرر حقيقي، وتشير التقديرات إلى أن ستوكسنت دمر ما يقرب من خمس أجهزة الطرد المركزي النووي الإيراني (Manikyam and Romala:2021:5).

إن الفيروس (ستوكسنت) غيّر برمجة أجهزة التحكم المنطقي القابلة للبرمجة، ممّا أسفر عن دوران أجهزة الطرد المركزي سرعة كبيرة جدّاً لمدة طويلة أدى الى تلف المعدات الحساسة في الهجوم، التي دخلها خلال مدة (13) يوماً في سجل بيانات أجهزة الطرد المركزي، وبعد تلك المدة بدأ التعرف على أجهزة الطرد المركزي مؤدّياً الى اهتزازها مسببة ارتفاع درجة الحرارة المؤدية في النهاية إلى تعطل المعدات الحساسة(Iran’s cyber attacks capabilities:2020). إن التأثير الإجمالي الذي خلفه ستوكسنت على البرنامج النووي الإيراني غير واضح، فقد اعترفت إيران منذ ذلك الحين بالهجوم، ولكنها تؤكد أن ستوكسنت لم يغير المعدل الذي تمكنت به من زيادة مخزونها من اليورانيوم المخصب Theohary and) Harrington:2015:1). كما إنَّ إيران كانت هدفا للبرنامج الاكثر تقدما المتمثل في (Falme، Duqu، stuxnet). ويقال إنها اختارت الرد بالمثل عن طريق هجمات الكترونية قامت بها جماعات غير حكومية مثل، (عز الدين القسام) و(الجيش السيبراني الإيراني)، ويُعتقد أن المجموعة الأخيرة مرتبطة بالجيش الإيراني، وفي مارس 2012م، صدر مرسوم بإنشاء المجلس الأعلى للفضاء الإلكتروني المكلف بتنسيق الحرب السيبرانية الوطنية وأمن المعلومات، وكانت إيران قد اعلنت خلال عام2011م، انها تخطط لإنشاء قيادة الكترونية للقوات المسلحة للدفاع ضد الهجمات الالكترونية للقوات المسلحة للدفاع ضد الهجمات الالكترونية، يتم تنسيق القدرات السيبرانية الإيرانية داخل الجيش، من قبل منظمة الدفاع السلبي (cristin:2014:6). لذا اولت العقيدة الامنية الإيرانية اهتماما اكبر بالأمن السيبراني، وبات يدخل ضمن نطاق استراتيجية الأمن القومي الإيراني، التي بنيت على ركزيتين هما حماية الأمن القومي الايراني عن طريق إقامة بنية تحتية علمية وتكنولوجية واستخبارية، تعتمد على استراتيجية وقائية في اثناء الدفاع، واستراتيجية استباقية في اثناء الهجوم، وتطوير عدد من المفاهيم القتالية الخاصة بها، وذلك عن طريق تشكيل شبكة معقدة من الجيوش الالكترونية القادرة على شن هجمات سيبرانية، إلى جانب تفعيل قدرتها الاستخبارية في نشر المعلومات المضللة (صالحي:2021:380).

وفي الحقيقة فإنَّ المجال السيبراني، بين الولايات المتحدة الأمريكية وإيران، لم يتوقف منذ سنوات؛ ففي عام 2011م، اعلنت القيادة المركزية الأمريكية ان إيران نجحت في السيطرة سيبرانياً على طائرة استطلاع، دون طيار امريكية فوق مياه مضيق هرمز وارغمتها على النزول (طه: 3023 :202). وفي 25 أبريل 2011م، اكتشفت وكالة الدفاع السيبرانية الايرانية فيروس (النجوم)، الذي تم تصميمه للتسلل إلى منشآتها النووية، وإلحاق الضرر بها، وفي 23 أبريل 2012م، اجبرت الهجمات السيبرانية ايران على ايقاف العديد من محطات تكرير النفط، وانتشر فيروس (المسحة)، عبر وزارة النفط الإيرانية، وشركة النفط الوطنية الإيرانية (Springe:2017) وفي 9 مايو 2012م، أقرّت إيران بأن فيروس (flame)، القادر على سرقة البيانات، اصاب اجهزة الكمبيوتر الحكومية (CNA:2014:5).

في 19 مايو 2012م، قال مسؤولون غربيون لصحيفة واشنطن بوست، إنَّ الولايات المتحدة الأمريكية والكيان الصهيوني، نشرا فيروس فليم(flame) لجمع معلومات استخبارية عن شبكات الكمبيوتر الإيرانية من أجل الاستعداد لحملة حرب سيبرانية (Springer:2017). وفي سبتمبر 2018م، سمحت أدارة دونالد ترامب، لوكالة المخابرات المركزية الأمريكية، بشن هجمات سيبرانية واسعة ضد البنية التحتية الحيوية الأيرانية، ومن ثم قامت في أبريل 2019م، باختراق سيبراني لمراكز البيانات الإيراني وترك العلم الامريكي على شاشات الكمبيوتر الايرانية، الى جانب رسالة بعدم التدخل في الانتخابات الامريكية، وفي يونيو 2019م، اكتشفت طهران شبكة تجسس سيبرانية تديرها وكالة المخابرات المركزية الامريكية وفككتها (Baezner:2019). وفي سبتمبر من نفس العام، شنت الولايات المتحدة الأمريكية هجوماً سيبرانياً على إيران، ردّاً على هجوم بطائرة دون طيار على منشآت سعودية، وقال مسؤولون أمريكيون إنَّ هذه الهجمة استهدفت قدرة أيران على نشر الدعاية، ومنعت الولايات المتحدة الأمريكية، في 25 يناير 2020م، إيران من الوصول إلى (Fars Newscom) وهو عنوان الويب لوكالة انباء فارس التابعة للحرس الثوري الإيراني(Hashemzadegan:2023). وفي14 فبراير 2020م، ألقى رئيس منظمة الدفاع المدني الإيرانية باللوم على الولايات المتحدة الأمريكية في هجوم سيبراني بفيروس (DDOS) الذي ادى الى انقطاع الخدمة لساعات (Almanna:2023). وفي 15 أكتوبر 2020م، أكدت إيران أنَّ هجومين سيبرانيين استهدفا اهدافا حكومية خلال الفترة من 12 إلى 13 اكتوبر، وقالت هيئة الموانئ الإيرانية إنَّها احبطت هجوماً سيبرانياً على الانظمة الالكترونية للوكالة، وقامت وكالات عدة بتعليق الخدمات مؤقتاً وأجرت اختبارات فنية بعد الابلاغ عن الهجمات (Andrew:2021).

6.3.2. التهديدات السيبرانية بين الولايات المتحدة الأمريكية- وروسيا :

بدأت التهديدات السيبرانية بين البلدين منذ عام 1996م، بهجوم من نوع (Moonlight Maze)، وهي واحدة من أولى حملات التجسس السيبراني الي ترعاها موسكو، والتي تضمنت سرقة كمية هائلة من المعلومات السرية من العديد من الوكالات الحكومية بما في ذلك وزارة الطاقة ووكالة ناسا ووزارة الدفاع الأمريكية. وفي إطار ضمها لشبه جزيرة القرم عام2014م، استخدمت روسيا العمليات السيبرانية لاستهداف

إمدادات الطاقة في كييف، كذلك لجأت لهذه العمليات باستخدام مزيج من الدعاية لاستقطاب المجتمعات للتأثير في الانتخابات الرئاسية الأمريكية عام 2016(van :2023:27) .

تُعد الولايات المتحدة، الدولة الأكثر تفوقا في مجال امتلاك القدرات السيبرانية والعسكرية منها، ولديها قيادة سيبرانية موحدة، وتعتمد القيادة السيبرانية الأمريكية على خمسة مكونات أساسية هي القيادة السيبرانية للجيش، وقيادة الأسطول السيبراني، والقيادة الإلكترونية للقوات الجوية، والقيادة الإلكترونية لقوات مشاة البحرية وخفر السواحل، إضافة إلى وحدات الحرس الوطني، ويبلغ عدد الفرق السيبرانية في هذه القيادة نحو 133 فريقا تضطلع بمهمات مختلفة في مجال حماية الأمن السيبراني(Izycki: 2022). وتقدر ميزانية القدرات السيبرانية وتكنولوجيا المعلومات للجيش الأمريكي لعام 2023 ما مقداره 16.6 مليار دولار يخصص الجزء الأكبر منها والذي يساوي 9.8 مليار دولار تقريبا للقيادة التكنولوجية لشبكة الجيش الأمريكي (Swallow: 2023: 20).

أثناء فترة الانتخابات الأمريكية لعام 2016، تم اتهام روسيا باستخدام الاختراق السيبراني وسيلة للتأثير في نتائج تلك الانتخابات، لصالح الرئيس "دونالد ترامب " ورغم أنه لم يتم الحسم بعد في ذلك الاتهام، لكن التهديدات السيبرانية اشتعلت من جديد بسبب تعرض العديد من الوزارات والهيئات ومؤسسات أمريكية حساسة عام 2020م، لهجمات سيبرانية تم استهداف من خلالها، المكتب الذي يدير الأسلحة النووية، التابع لوزارة الطاقة الأمريكية وأيضا وزارتا التجارة والخزانة ولم يقتصر تأثيرها فقط على الإدارة الأمريكية بل امتد ليشمل الشعب الأمريكي كافة نفدت الهجوم مجموعة هاكرز تدعمهم روسيا، وفق تصريح لوزير خارجية الولايات المتحدة الأميركية السابق مايك بومبيو (Mike Pompeo) رغم النفي الرسمي الروسي لتورطها في هذه الهجمات(Hansel:2023:189) .

- وفي عام 2019م، تعرضت روسيا لهجوم إلكتروني أصاب شبكتها الكهربائية، وذكرت صحيفة نيويورك تايمز أن متسللين أمريكيين قاموا بوضع برامج ضارة قادرة على تعطيل الشبكة الكهربائية الروسية، مما أدى إلى تخصيص مبالغ كبيرة لهذه الأعمال وهي المبالغ الي كانت مخُصصة في الأساس لمكافحة الإرهاب والحروب الأمريكية، ولطالما اتهمت الولايات المتحدة نظيرتها روسيا، بتنفيذ الأخرة هجمات على مرافق أمريكية حيوية، فيما تعي واشنطن أن قدرة روسيا على إجراء هجمات إلكترونية مدمرة في الوطن ربما تظل مرتفعة للغاية(Hansel:2023:190).

- وفي 19 ديسمبر من عام 2020م، اتهم وزير الخارجية الامريكي السابق (مايك بومبيو) روسيا بالوقوف وراء شن اسوء هجوم تجسس سيبراني على الحكومة الامريكية، واعلنت الولايات المتحدة عن تعرضها لهجمات سيبرانية وقرصنة معلوماتية ضخمة استهدفت مؤسسات امريكية حساسة من بينها المكتب الحكومي، الذي يدير الاسلحة النووية التابع لوزارة الطاقة الامريكية (طه:2023:202).

- كما تتهم واشنطن موسكو، باختراق شركة "SolarWinds" في أواخر عام 2020م، حيث تقول الولايات المتحدة إن مجرمي الإنترنت المدعومين من روسيا تمكنوا من الوصول إلى 10 وكالات حكومية أمريكية، بما في ذلك وزارة الأمن الداخلي ووزارة التجارة(Mahoney:2021:69).

- وفي عام 2021م، قالت الولايات المتحدة إن مجرمي الإنترنت المتمركزين في روسيا تسببوا في هجوم إلكتروني من أكثر الهجمات الإلكترونية تدمراً، حيث كانت شركة كولونيال بايبلاين ضحية لهجوم برمجيات الفدية في مايو 2021 ، مما أدى إلى إغلاق العمليات وتسبب في انقطاعات واسعة النطاق في جميع أنحاء البلاد(Eshov and Ismailova :2022:140) وفي نفس العام كشفت شبكة (بالو التو) الامنية بان قراصنة يشتبه بانهم أجانب تمكنوا من اختراق تسع منظمات حساسة في قطاعات الدفاع والطاقة والتكنلوجيا في الولايات المتحدة الأمريكية، وبينت الشبكة الامنية انه بمساعدة من وكالة الأمن القومي الأمريكي وهيئة الأبحاث الأمنية السيبرانية تم الكشف عن اختراق القراصنة الذين كانوا يهدفون الى سرقة معلومات حساسة من شركات متعاقدة مع وزارة الدفاع الامريكية (Mahoney:2021:81).

- وفي اكتوبر2022 اتهم الرئيس الروسي فلاديمر الحكومة الأمريكية وحلفاءها شن حملة منسقة من الهجمات الإلكترنية ضد روسيا، وفي 20 ابريل من عام 2023م، تعرضت مطارات الولايات المتحدة الامريكية الى عطل غامض في انظمة القيادة والحاسوب، مما افضى إلى تأخير رحلات الطيران في جميع انحاء الولايات المتحدة، وعلى الرغم من نفي الرئيس الأمريكي جون بايدن تعرض المطارات لهجوم سيبراني، لاسيما ان الولايات المتحدة سبق ان تعرضت في منتصف عام 2022م، الى هجوم سيبراني أفضى الى تعطل عدة مواقع الكترونية لمطارات امريكية تبنت مسؤوليته مجموعة من القراصنة الروس(Janson:2023). ومنذ اندلاع الحرب الروسية - الاوكرانية، ازدادت التحذيرات الدولية من نشوء حرب سيبرانية بين روسيا من جهة، والولايات المتحدة وأوربا من الجهة الأخرى، لاسيما ان هذه التهديدات السيبرانية تعد واحدة من سيناريوهات الحرب الحديثة(Dorn:2023).

إن استمرار التهديد السيبراني بين الولايات المتحدة الأمريكية، وروسيا، قد يؤدي إلى تصاعده والانتقال به من الصراع على السيادة والهيمنة في الفضاء الإلكتروني، إلى ميدان الفضاء الخارجي، خاصة في ظل التداخل والتكامل بين المجالين؛ فروسيا تدرك جيدا أن القدرة الفضائية المتفوقة لأمريكا هي، نقطة ضعفها، حيث تعتمد القوات الأمريكية في مناطق الحرب على كوكبة من 31 قمرا صناعيا، لتحديد المواقع العسكرية المستهدفة وتحديد أماكن الأفراد، وهو ما جعل روسيا تطور وتختبر نظام الصواريخ المضادة للأقمار الصناعية (ASATS)، والتي تم تصميمها خصيصا لضرب الأقمار الصناعية للعدو، فالتفوق في ميدان الفضاء الخارجي معناه التفوق في الفضاء الإلكتروني (Sokolsky and Rumer:2020) .لا سيما وأن الصراع بين الولايات المتحدة الأمريكية وروسيا قائم من أجل تعزيز القيادة والسيطرة، وقد ينتقل من الصراع الناعم المقتصر على المجال المعلوماتي، إلى الصراع الصلب من خلال الاستحواذ على القوة السيبرانية ذات الطابع التدميري، وبناء القدرات في مجال شن الهجمات السيبرانية المنظمة، والتحول من تبني السياسات الدفاعية إلى أخري هجومية، لذلك تسعى كل من روسيا والولايات المتحدة الأمريكية، إلى إيجاد الدعم لسياساتهما السيبرانية عبر تكتلات دولية وإقليمية تضمن لهما المساندة والضغط على الطرف الآخر من خلال سلاح العقوبات(Lawrence and others:2021).

من الواضح أن هناك توازنا بين واشنطن وموسكو في مجال الردع السيبراني، على الرغم من الاختلاف في القدرات فكلا البلدين يعتبر الآخر عدوًا قويًا، وعلى الرغم من التشابه في استراتيجيات الاستهداف الإلكتروني بينهما، فأنهما سارتا في مسارات مختلفة في تطوير القدرات والسياسات الخاصة بالحرب السيبرانية، ويرجع ذلك جزئيًا إلى التفسيرات المختلفة للأحداث العالمية، وكمية الموارد المتاحة هذا الاختلاف خلق فجوة في استخدام العمليات الإلكترونية، ورغم فشل الولايات المتحدة في مواكبة القدرات الجديدة في مجال العمليات الإلكترونية، خاصة داخل جيشها، فأن روسيا نجحت في استخدام العمليات الإلكترونية ضد الخصوم المحتملين من خلال تعزيز قدراتها العسكرية الإلكترونية وتوسيع مبادرات التجنيد، وتطوير البرمجيات الضارة (Luigi:2016:98).

7.3.2. التهديدات السيبرانية بين روسيا – وأوكرانيا :

منذ أحداث أوكرانيا عام 2014م، التي شهدت الإطاحة بالرئيس فيكتور يانوكوفيتش، شهدت أوكرانيا عددًا متزايدًا من الهجمات الإلكترونية وخاصة في قطاع الطاقة والكهرباء التي تتمثل في التخريب وتقويض شرعية الحكومة المستهدفة من خلال عجزها الواضح عن توفير الوظائف والخدمات الأساسية (Danyk and Maliarchuk :2020:2) وفي نفس العام أتهمت روسيا بتنسيق الانشطة العسكرية والسيبرانية في الصراع الأوكراني، استولى المتمردون المسلحون من روسيا على شبة جزيرة القرم قبل هجوم الحرمان من الخدمة (DDoS) (Manikyam and Romala2021:3232).

في هذا السياق اقترح الباحث (جريس بي مولر، وآخرون) في دراسة نشرت في مركز الدراسات الاستراتيجية والدولية، في يوليو 2023م، بعنوان دور العمليات السيبرانية في الحرب الروسية الأوكرانية وتقييم طبيعتها، وكيف تحولت هذه العمليات إلى أداة للقتال والإكراه، وما إذا كان دورها داعماً أم حاسماً في اندلاع الحروب الكبرى (Mueller and others:2023). وتستند العمليات السيبرانية الروسية على أهداف استراتيجية تتجلى في التعطيل (التسبب في حوادث منخفضة التكلفة ومنخفضة التأثير)، والتجسس قصير المدى (الوصول إلى التأثير الفوري)، والتجسس طويل المدى (الاستفادة من المعلومات) في إطار العمليات المستقبلية، وكذلك التدهور (السعي إلى التدمير المادي والإعاقة) (Wille :2022:20).

تم تسجيل 30 حادثة سيبرانية ثنائية بين روسيا وأوكرانيا، بين عامي 2000 و2020م، من بينها 93% قامت بها روسيا، وتركزت غالبية هجمات موسكو، (57%) على جهات فاعلة خاصة وغير حكومية، كما استهدفت 11% فقط أهدافاً عسكرية حكومية داخل أوكرانيا لأغراض التعطيل، أو التجسس بدلاً من إضعاف الشبكات الحكومية المهمة، واتسمت غالبية العمليات السيبرانية الروسية بمحاولات التصيد الاحتيالي وحملات حجب الخدمة الموزعة وجهود الدعاية، أو التخريب وسيلة لمضايقة أوكرانيا أكثر، إذ تستهدف روسيا جراء توظيفها النسبي للحرب السيبرانية عدة أهداف؛ منها الحرب النفسية والخداع الاستراتيجي والإخلال بمعادلة الدعم الغربي لأوكرانيا، وتقويض الثقة في النظام الأوكراني و حرب السرديات وتآكل الثقة (Lin:2022:40).

فقد شهد العام الأول لحرب أوكرانيا 47 هجوماً سيبرانياً روسياً، بهدف جمع البيانات مباشرة من مصادر الحكومة الأوكرانية، وتزايدت العمليات السيبرانية من حيث التكرار، لكن ليس الخطورة في المراحل الأولى من الحرب خلال 2022م، مقارنة بإحصائيات ما قبل الحرب، ومع ذلك، لا تزال العمليات السيبرانية أداة قسرية ضعيفة بالنسبة لموسكو على الرغم من استخدامها المتكرر، إذ زادت العمليات السيبرانية بنسبة 75% لكن هناك انخفاض في متوسط خطورة الهجوم بعد الغزو الروسي واسع النطاق لأوكرانيا (Lewis:2022).

وبالنظر إلى أسلوب التهديدات السيبرانية الروسية، فإن الأهداف المفضلة لها ظلت أنشطة التشكيل التخريبية وحملات التجسس خلال الأشهر الأولى من حرب أوكرانيا سنة 2022م، إذ شكلت حوادث التعطيل 57.4%، من إجمالي الحوادث، يليها التجسس (21.3%)، وتركزت معظم الهجمات السيبرانية الروسية على استهداف جهات فاعلة من القطاع الخاص غير الحكومي بنسبة 59.6%، تليها الجهات الحكومية والمحلية بنحو 31.9%، وأربعة حوادث فقط، أي نسبة 8.5% لاستهداف الجهات العسكرية الحكومية، وهو ما يتوافق مع أهداف روسيا بين عامي 2000 و2020 إذ تركّزت نسبة 57% من العمليات السيبرانية في استهداف جهات فاعلة خاصة غير حكومية، و32% جهات فاعلة حكومية غير عسكرية، و11% جهات عسكرية حكومية ويدل ذلك على أنَّ الجهود السيبرانية التي تبذلها روسيا كانت ذات تأثير محدود في الجهود العسكرية الروسية في أوكرانيا (Zedelashvili and Giorgadze: 2020:29).

واتضحت مؤشرات استخدام روسيا العمليات السيبرانية لمهاجمة مواقع أوكرانية وتعطيل القيادة والسيطرة منذ بداية الحرب من خلال نشر روسيا برامج ضارة عطلت نظام الأقمار الاصطناعية وأدت إلى انقطاع أكثر من 30 ألف اتصال بالإنترنت في جميع أنحاء أوروبا، إلى جانب أنه منذ بداية الحرب وردت تقارير عن اكتشاف برامج ضارة في البنية التحتية الحيوية في البلدان التي تدعم أوكرانيا بمساعدة عسكرية أجنبية، فعلى سبيل المثال تم اكتشاف برامج ضارة روسية في البنية التحتية الحيوية المرتبطة بتوليد وتوفير الكهرباء في الولايات المتحدة الأمريكية منذ بداية الحرب في أوكرانيا (Lewis:2022:16) .

بعد دراسة الحالات والنماذج للتهديدات السيبرانية التي واجهت دولاً مختلفة مثل إستونيا، السعودية، وجورجيا، بالإضافة إلى الهجمات بين الدول الكبرى مثل روسيا وأوكرانيا، الصين والولايات المتحدة الأمريكية، وإيران، فإن العالم بأسره سعى إلى تعاون دولي مشترك وجهود منسقة لمكافحة التهديدات السيبرانية وضمان استقرار الأمن السيبراني على مستوى العالم، وهذا ما سوف نوضحه في المبحث التالي.

4.2. الجهود الدولية في مواجهة التهديدات السيبرانية

هناك جهوداً دولية تستهدف ضبط التفاعلات وسلوك الوحدات الدولية الفاعلة في الفضاء الإلكتروني ضمن إطار التنظيمات الدولية القائمة، وتلك الجهود قد أسفرت عن اتفاقيات دولية على الصعيد العالمي والإقليمي، سواء ثنائية بين الوحدات الدولية، أو متعددة الأطراف (جمال الدين:206:2023). وتتمثل الجهود المبذولة من قبل الدول والمنظمات الدولية في تركيزها على قواعد القانون الدولي، والتي يمكن أن تسهم في احتواء التهديدات السيبرانية والحدّ منها، بمنع الأعمال العدائية التي تشمل استخدام القوة، وإقرار معايير

وتدابير لبناء الثقة وتطبيقها على المستوى الدولي وتشمل هذه الجهود المنظمات العالمية والإقليمية التي تلعب دورًا بارزًا في صياغة سياسات الأمن والدفاع السيبراني (الشادلي:2023: 1257) وسيتم توضيحها على النحو التالي:

1.4.2.الاتفاقيات الدولية :

1.4.2. 1. الاتفاقية المتعلقة بالجريمة الإلكترونية (بودابست) :

تُعد بودابست بشأن الجرائم الإلكترونية أول اتفاقية ملزمة وقعت عليها 26 دولة أوروبية عام 2001، وبالرغم من إن هذه الاتفاقية أوروبية المنشأ، فإن عضويتها مفتوحة لجميع الدول التي تريد الانضمام إليها(المجلس الاوروبي:2001). وفي عام 2014 انضمت إليها دول أخرى مثل الولايات المتحدة الأمريكية، وكندا واليابان، جنوب أفريقيا وبعض الدول العربية وهي المغرب والجزائر وتونس واصبحت 79 دولة طرف في هذه الاتفاقية(Chang:2020:20-22).

وفي عام 2016م، أصدرت لجنةُ اتفاقية الجرائم السيبرانية مذكرة توجيهية تتعلَّق بجوانب الإرهاب السيبراني بموجب اتفاقية بودابست، تعلن فيها أن "الجرائم الموضوعية في الاتفاقية قد تكون أيضًا أعمالا إرهابية على النحو المحدد في القانون المعمول به" وجاءت هذه المذكرة الإضافية بموجب الاتفاقية لتسلط المذكرة الضوء على أن هذه الإتفاقية ليست معاهدة مختصة بالإرهاب، إلا أنه يمكن القول بإن الجرائم الموضوعية في الإتفاقية يمكن أن تنفذ على أنها أعمال إرهابية، لتسهيل الإرهاب ولدعم الإرهاب، وتعد الاتفاقية الأوربية بمثابة دعوة موجهه إلى دول العالم للتفاعل مع الجرائم المستحدثة وتعكس الاتفاقية الجهد الواسع والمميز للاتحاد الأوروبي ولجان الخبراء فيهما لوضع حد لمسائل الجرائم السيبرانية وأغراضها منذ اكثر من ثلاثة وعشرين عاماً (Nguye and Golman:2021:255) .

تتكون الاتفاقية من مقدمة وأربعة فصول، فبعد أن استعرضت المقدمة أهداف الاتفاقية ومنطلقاتها ومرجعياتها السابقة وما تقوم عليه من جهود ارشادية وتوجيهية وتدابير اقليمية ودولية، جاء الفصل الأول لتغطية المصطلحات في مادة (1) وتضمن الفصل الثاني الذي جاء تحت عنوان الإجراءات المتعين اتخاذها على المستوى الوطني، ثلاثة أقسام: الأول، ويضم المواد من 132 يعالج النصوص الموضوعية لجرائم الكمبيوتر والقسم الثاني ويضم المواد من 21-14 تتعلق بالقواعد الإجرائية والقسم الثالث ويضم المادة 22 وتعلق بالاختصاص، أما الفصل الثالث من الاتفاقية والذي جاء تحت عنوان التعاون الدولي تضمن قسمين، الأول تحت عنوان المبادئ العامة ويضم المواد من 22-3 والقسم الثاني تتعلق بالنصوص الخاصة ويضم المواد من 29-35، أما الفصل الخامس فيتضمن الاحكام الختامية ويضم المواد من 36-48 (مجلس أوروبا:2001).

أكدت الاتفاقية في مقدمتها على أهمية ما أنجز من جهود في مجال الإجرام السيبراني من طرف الأمم المتحدة، إضافة الى منظمة التعاون الاقتصادي والتنمية، إلى جانب الاتحاد الأوربي ومجموعة الدول الصناعية، كما نجد أن الاتفاقية قد ركزت على ثلاثة عناصر أساسية، انطلاقا من التدابير التشريعية التي تضمنت (نصوص) (التجريم) في الفصل الأول، إضافة إلى الفصل الثاني الذي تناول التدابير التشريعية الإجرائية التي تتخذ

لإجراء تحقيقات أكثر فعالية خاصة فيما يتعلق بجرائم الكمبيوتر، وصولا الى الفصل الثالث الذي يبين أهمية التعاون الدولي والإقليمي في مجال مكافحة الجرائم السيبرانية(مجلس أوروبا:2001). ومن أهم أهداف الاتفاقية هي :

1. توحيد عناصر القانون الجزائي المحلي مع الأحكام المتعلقة بالجرائم الإلكترونية.
2. توفير الإجراءات القانونية اللازمة للبحث والتحري عن الجرائم المرتكبة إلكترونيا.
3. جمع المعلومات عن البيانات وعن إمكان وجود الاختراق أو التدخل في محتواها
4. تضمنت المبادئ العامة المتعلقة بالتعاون الدولي في تسليم المجرمين والمساعدة الدولية، وتبادل المعلومات بصورة آلية، وتفعيل الولاية القضائية على أي جريمة.

ومن أهم الأسباب التي أدت إلى إبرام الاتفاقية، الحاجة إلى اتخاذ تدابير تشريعية لمكافحة الجريمة السبرانية ومخاطرها المدمرة على الدول، خاصة في ظل شيوع التهديات السيبرانية، وفي ظل التوسع الكبير لأنظمة الحوسبة المفتوحة، ونقل وتدفق المعلومات، إضافة إلى التشديد على أهمية مكافحة كافة الأنشطة التي تستهدف أمن المعلومات ونظم الكمبيوتر، وتوفير قواعد ملائمة للتحري والتحقيق والضبط والتفتيش والمحاكمة مع التركيز على اهمية التعاون المحلي والاقليمي والدولي مع وجوب اقامة التوازن بين متطلبات تنفيذ القانون وبين وجوب احترام الحقوق الاساسية والسيادة فأن مشروع الاتفاقية قد ركز على عناصر أساسية ثلاثة هي:

- أهمية التدابير التشريعية الموضوعية (نصوص التجريم)
- أهمية التدابير التشريعية الإجرائية (النصوص الإجرائية).
- أهمية تدابير التعاون الدولي والإقليمي في مجال مكافحة الجرائم.

لا سيما أنَّ البنود الرئيسية لاتفاقية بودابست تغطي مجموعة واسعة من الجرائم الإلكترونية (مجلس أوروبا:2001) بما في ذلك :

- الاختراق غير المشروع لنظام حاسوبي: الدخول غير المصرح به إلى نظام حاسوبي.
- التدخل غير المصرح به في نظام حاسوبي: تعطيل البيانات الموجودة في نظام حاسوبي أو تغيير أو تدمير.
- الاعتراض غير المشروع: اعتراض البيانات التي يتم نقلها عبر شبكة حاسوبية.
- التدخل غير المشروع في الأجهزة: التدخل في عمل الأجهزة المتصلة بشبكة حاسوبية.
- صنع وتوزيع برامج ضارة: إنتاج أو توزيع برامج مصممة للتسبب في الضرر لأنظمة الحاسوب.
- الاحتيال الإلكتروني: استخدام وسائل إلكترونية لخداع الآخرين والحصول على أموالهم.
- تشويه السمعة الإلكترونية: نشر معلومات كاذبة أو مسيئة عن الغير عبر الإنترنت

ويمكننا أن تستنتج أن، اتفاقية بودابست بشأن الجريمة الإلكترونية تُعد حجر الزاوية في الجهود الدولية لمكافحة الجرائم الإلكترونية، فهي توفر إطارًا قانونيًا متكاملًا للتعاون الدولي في هذا المجال، وتحدد مجموعة واسعة من الجرائم الإلكترونية والعقوبات المقررة على مرتكبيها، في سياق دراسة حالة ليبيا والتي شهدت تصاعدًا ملحوظًا في التهديدات السيبرانية. وتكتسب هذه اتفاقية بودابست أهمية خاصة من حيث امكانية ربط هذه الاتفاقية بواقع ليبيا ، وما هي الدروس المستفادة التي يمكن أن تقدمها هذه الاتفاقية لدعم جهود ليبيا في مواجهة التحديات السيبرانية؟ وهذا يقودنا إلى التساؤل ما هي علاقة اتفاقية بودابست بالتهديدات السيبرانية التي تتعرض لها ليبيا؟ حيث تشترك ليبيا مع العديد من الدول الأخرى في مواجهة تحديات مشابهة في مجال الأمن السيبراني.

إن أهمية انضمام ليبيا لاتفاقية بودابست، يوفر الإطار القانوني اللازم لبناء نظام وطني لمكافحة الجرائم السيبرانية، لتعزز التعاون الدولي بين ليبيا والدول الأخرى الأعضاء في الاتفاقية، مما سيساعد على تبادل المعلومات والخبرات وتنسيق الجهود لمكافحة الجرائم العابرة للحدود، ويمكن أن تلعب دورًا حاسمًا في دعم جهود ليبيا في هذا المجال من خلال تبني أحكام الاتفاقية وبناء نظام وطني متكامل لمكافحة الجرائم السيبرانية، يمكن ليبيا من أن تحمي نفسها من التهديدات السيبرانية وتعزز أمنها القومي.

2.1.4.2. دليل تالين(Tallinn Manual) :

يشكل دليل دالين بإصداريه؛ الأول عام 2013م، والثاني عام2017م، أول محاولة دولية للبحث في مجال التكييف القانوني للهجمات السيبرانية، حيث أكدت قواعده على، أن بعض أحكام القانون الدولي المعاصر يمكن تطبيقها في مجال الفضاء الإلكتروني، أو اعتبارها نقطة انطلاق مناسبه لكيفية التعامل مع هذا التطور التقني، لقد ساهم هذا الدليل بشكل فعال في النقاش بين الدول، حول المواضيع المثيرة للتحديات وكيفية تفسير القانون الدولي عامة والقانون الدولي الإنساني خاصة، وكيفية تطبيقه على أنشطة الدول، والأطراف من غير الدول، في الفضاء الإلكتروني (Pratama and Bamatraf:2021:1) .

يحتوي دليل تالين على 95 قاعدة، تمثل تحدياته الرئيسية في ضمان توجيه الهجمات ضد الاهداف العسكرية فقط، ويجيب دليل تالين عن أهم النقاط الحساسة ذات الصلة بالحروب والهجمات السيبرانية كمفهوم نظام النزاع المسلح في إطار الحرب السيبرانية، ومفهوم الجيوش السيبرانية، وكيفية إدارة الحروب السيبرانية، من خلال قواعد الاشتباك السيبراني، إضافة إلى إمكانية مراعاة القانون الدولي الانساني المعروفة كمبدأ للتمييز ومدى شرعية استهداف المقاتل السيبراني بالوسائل العسكرية كاطائرات العسكرية دون طيار (قاسمي وبلغيث:47:2020).

ويُعد دليل تالين، وثيقة قانونية دولية بالغة الأهمية، رغم طابعها غير الملزم، فهو يمثل محاولة جادة لتحديد الإطار القانوني الدولي للعمليات العسكرية السيبرانية ويعتبر مرجعًا أساسيًا للباحثين وصانعي السياسات، على حد سواء، وتتمثل أهداف هذا الدليل في تحديد الثغرات القانونية الموجودة في القانون الدولي الحالي فيما يتعلق بالعمليات العسكرية السيبرانية، وتقديم تفسير أولي للقواعد القانونية الدولية القابلة للتطبيق على

العمليات العسكرية السيبرانية، وتشجيع الحوار بين الدول والمختصين القانونيين حول القضايا القانونية الناشئة عن العمليات العسكرية السيبرانية، وأيضا توجيه صانعي السياسات العسكرية والقانونية في اتخاذ قرارات بشأن العمليات العسكرية السيبرانية (Hykkönen:2024) .

وأهم بنود دليل تالين تلك التي تتضمن مجموعة واسعة من القضايا القانونية المرتبطة بالعمليات العسكرية السيبرانية، ويقدم الدليل تعريفات للعمليات السيبرانية المختلفة، ويحدد العناصر الأساسية التي تميز الهجوم السيبراني عن الأنشطة السلمية (Hykkönen:2024) كما موضح على النحو الآتي:

- يناقش الدليل تطبيق مبادئ القانون الدولي الإنساني على الهجمات السيبرانية، بما في ذلك مبدأ التمييز ومبدأ التناسب.
- يبحث الدليل في مسؤولية الدول عن الأنشطة السيبرانية التي تقوم بها، سواء كانت مباشرة أو غير مباشرة.
- يستكشف الدليل إمكانية تطبيق قوانين الجرائم الدولية على الأفعال السيبرانية التي تشكل جرائم حرب أو جرائم ضد الإنسانية أو إبادة جماعية.

ويمكن الاستنتاج بأن على الرغم من أهمية دليل تالين، إلا أنه يواجه بعض التحديات والحدود وهي :

- ليس لدليل تالين قوة قانونية ملزمة للدول، مما يعني أن الدول ليست ملزمة بتطبيق أحكامه.
- يتطور مجال التكنولوجيا بسرعة كبيرة، مما يجعل من الصعب على أي وثيقة قانونية أن تبقى محدثة.
- توجد اختلافات في التفسير بين الدول والمختصين القانونيين حول بعض أحكام الدليل.

1.4.2. 3. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات :

إن تزايد مخاطر الجرائم المرتكبة بواسطة تقنية المعلومات، أصبح يشكل هاجسًا كبيرًا للدول عامة، والعربية خاصة، مما دفع هذه الدول للاستعجال في إبرام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات التي تم توقيعها في مدينة القاهرة في جمهورية مصر في 12/21/ 2010م، ووافق عليها مجلسا وزراء الداخلية والعدل العرب في اجتماعهما المنعقد بمقر الامانة العامة لجامعة الدول العربية، وسرت هذه الاتفاقية بعد مضي ثلاثين يوما من تاريخ ايداع وثائقها تم التصديق عليها من سبعة عشر دولة عربية بموجب الفقرة 3 من الأحكام الختامية للاتفاقية، ولكن لم تصادق عليها الا ست دول هي الاردن، الامارات العربية المتحدة، السودان، فلسطين، قطر ودولة الكويت عام 2013م (الاتفاقية العربية لمكافحة جرائم تقنية المعلومات : 2010).

ومن أهداف الاتفاقية تعزيز التعاون بين الدول العربية في مجال جرائم تقنية للمعلومات، ودعم التعاون بين الدول العربية لتدارك الأخطار الناجمة عن هذه الجرائم، إضافة إلى الحفاظ على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها في الفضاء الإلكتروني (الاتفاقية العربية لمكافحة جرائم تقنية المعلومات سنه 2010م). وتنص الاتفاقية على جملة الأفعال التي تعتبر جرائم تقنية المعلومات، حيث خصت في المادة 16

منها على الأفعال الخاصة بالجرائم المنظمة التي ترتكب بواسطة الانترنت مثل جريمة الإتجار بالأشخاص، كنوع من جرائم تقنية المعلومات، بينما خصصت الاتفاقية الفصل الثالث لتناول الأحكام الإجرائية (شرف الدين:2018:94). وتُعد الاتفاقية العربية فرصة قيمة لليبيا لتعزيز الجهود في مكافحة جرائم تقنية المعلومات من خلال التوعية وتطوير القدرات والتعاون الإقليمي، ويمكن لليبيا تعزيز أمنها السيبراني وحماية بنيتها التحتية الرقمية بفضل تعزيز التشريعات واعتماد إجراءات أمنية متقدمة، يمكن لليبيا تعزيز استعدادها للتصدي للتهديدات السيبرانية وضمان سلامة البيانات والمعلومات الحيوية للحكومة والشعب الليبي.

4.1.4.2. اتفاقية أمن الفضاء الالكتروني وحماية البيانات ذات الطابع الشخصي (مالابو) :

اتفاقية مالابو حول الأمن السيبراني وحماية البيانات الشخصية، هي مبادرة رائدة من الاتحاد الأفريقي تهدف إلى وضع إطار قانوني موحد لمواجهة التحديات المتزايدة التي يشكلها الفضاء الإلكتروني على القارة الأفريقية، تم اعتماد هذه الاتفاقية عام 2014م، خلال القمة الـ22 للاتحاد الأفريقي في مالايو، عاصمة غينيا الاستوائية (Lungu:2022:66) . تتكون الاتفاقية من 38 مادة، وجاء في المادة 23 بأنَّه يجب بناء إطار تأمين الفضاء الالكتروني الوطني، والتي تتمثل في السياسة الوطنية والاستراتيجية، وجاء في المادة 25 التدابير القانونية والمادة 26 النظام الوطني لتأمين الفضاء الالكتروني، أما المادة 28 فقد أشارت إلى التعاون الدولي، الذي تلتزم فيه الدول الأطراف بضمان ان التدابير التشريعية المعتمدة لمكافحة الجريمة الالكترونية سوف تعزز امكانية المواءمة الاقليمية، وأيضا تلتزم الدول الاطراف التي ليس لديها اتفاقيات المساعدة المتبادلة في مجال الجريمة الالكترونية، وتلتزم الدول الاطراف بالاستفادة من وسائل التعاون الدولي القائمة بهدف الاستجابة للتهديدات السيبرانية، وتشير إلى أنها تهدف إلى محاولة تحديد الأهداف والتوجهات الرئيسية لمجتمع المعلومات في إفريقيا وتعزيز التشريعات والأنظمة الحالية الخاصة بتكنولوجيا المعلومات والاتصالات للدول الأعضاء والمجموعات الاقتصادية الإقليمية، وتعني بأن الاتفاقية تهدف إلى تنظيم مجال تكنولوجي متطور بشكل خاص، وسعيا إلى الاستجابة للتطلعات الملحة للعديد من الأطراف الفاعلة التي غالباً ما تتعارض مصالحها وتحدد هذه الاتفاقية قواعد الأمن الضرورية لإنشاء فضاء رقمي موثوق به للمعاملات الإلكترونية، وحماية البيانات ذات الطابع الشخصي ومكافحة الجريمة الإلكترونية (الاتحاد الأفريقي:2014). تهدف اتفاقية مالايو إلى تحقيق مجموعة من الأهداف الاستراتيجية،(Ajufo:2023:47) أبرزها:

- وضع إطار قانوني موحد ومتسق لمواجهة الجرائم الإلكترونية، وحماية البيانات الشخصية في جميع أنحاء القارة الأفريقية.
- تعزيز التعاون بين الدول الأفريقية في مجال الأمن السيبراني، وتبادل المعلومات والخبرات.
- حماية البنية التحتية الحيوية للدول الأفريقية من الهجمات السيبرانية التي تهدد الأمن والاستقرار.
- حماية حقوق الأفراد في خصوصية بياناتهم الشخصية من الانتهاكات والاختراقات.
- دعم التنمية الاقتصادية في أفريقيا من خلال توفير بيئة آمنة وموثوقة للتجارة الإلكترونية والخدمات الرقمية.

على الرغم من أهمية اتفاقية مالايو، فأنه عملية التصديق عليها وتنفيذها واجهت بعض التحديات، حيث لم توقع جميع الدول الأفريقية على الاتفاقية حتى إعداد هذه الرسالة ومع ذلك، هناك عدد متزايد من الدول الأفريقية يعمل على دمج أحكام الاتفاقية في تشريعاتها الوطنية حيث تمثل اتفاقية مالابو خطوة مهمة في جهود القارة الأفريقية لمواجهة التحديات المتزايدة التي يشكلها الفضاء الإلكتروني فهي توفر إطارًا قانونيًا متينًا للتعاون الإقليمي في هذا المجال، وتسهم في حماية المصالح الاقتصادية والاجتماعية للدول الأفريقية (Nimigan:2019:1010). تواجه اتفاقية مالابو بعض التحديات في تنفيذها (Akintayo:2024:608) منها:

- وجود اختلافات كبيرة بين الدول الأفريقية في مستوى التطور التكنولوجي والبنية التحتية، مما يجعل من الصعب تطبيق الاتفاقية بشكل موحد.
- تعاني العديد من الدول الأفريقية من نقص في الخبرات والكفاءات اللازمة لتنفيذ الاتفاقية.
- تتطور التقنية بسرعة كبيرة، مما يتطلب تحديث الاتفاقية بشكل دوري لمواكبة هذه التطورات.

اتفاقية مالابو هي وثيقة بالغة الأهمية لتعزيز الأمن السيبراني في إفريقية ومع ذلك، فإن نجاح هذه الاتفاقية يتطلب تضافر الجهود الوطنية والإقليمية، وتوفير الموارد اللازمة لتنفيذها(Awosusi:2022:93) . كما إنَّ اتفاقية مالابو تعتبر مهمة لمواجهة التهديدات السيبرانية في ليبيا بالنظر إلى تأثيرها المحتمل، يمكن أن تسهم الاتفاقية في تعزيز الأمن السيبراني في ليبيا عبر عدة طرق منها تعزيز الوعي بأهمية الأمن السيبراني من خلال تبني أفكار ومفاهيم الاتفاقية، وتعزيز التعاون الإقليمي توفر الاتفاقية إطارًا للتعاون وتبادل المعلومات بين دول أفريقية، مما يعزز التعاون الإقليمي ويسهم في مواجهة التهديدات السيبرانية بشكل مشترك، وتحسين قدرات الدولة في مجال الأمن السيبراني وحماية البيانات الشخصية من خلال تطوير استراتيجيات فعالة وتقديم التدريب والتأهيل للكوادر العاملة في هذا المجال.

5.1.4.2. اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية :

تم إعلان هذه الاتفاقية في 27 نوفمبر 2024م، وتتكون من 68 مادة، حتى تاريخ هذه الدراسة، لم يتم التصديق على الاتفاقية، سيتم فتح باب التوقيع عليها في مدينة هانوي بفيتنام عام 2025، ثم في مقر الأمم المتحدة في نيويورك حتى 31 ديسمبر 2026م، ستدخل الاتفاقية حيز التنفيذ بعد 90 يوماً من تصديق 40 دولة عليها، تهدف اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية إلى تعزيز التدابير الرامية إلى منع ومكافحة الجريمة السيبرانية بكفاءة وفعالية أكبر، وتشجيع التعاون الدولي في هذا المجال، كما تدعم توفير المساعدة التقنية وبناء القدرات، خاصة للدول النامية(الأمم المتحدة، 2024).

تحث الاتفاقية جميع الدول ومنظمات التكامل الاقتصادي الإقليمية على التوقيع والتصديق عليها في أقرب وقت ممكن لضمان التعجيل ببدء تنفيذها، كما تؤكد على أن مسؤولية منع الجريمة السيبرانية ومكافحتها تقع على عاتق جميع الدول، التي يجب أن تتعاون فيما بينها بدعم من المنظمات الدولية والإقليمية المعنية، وكذلك المنظمات غير الحكومية ومنظمات المجتمع المدني والمؤسسات الأكاديمية وكيانات القطاع الخاص، لا تُلزم

الاتفاقية الدول الأطراف بأن تستنسخ حرفياً في قوانينها الداخلية نفس المصطلحات المعرفة في المادة 2، شريطة أن تشمل تلك القوانين هذه المفاهيم بما يتسق مع مبادئ الاتفاقية ومقاصدها، وأن توفر إطاراً مكافئاً لتنفيذها وفقاً للمادة 17، لا يُعتبر الفعل جريمة إلا إذا كانت الجريمة الأصلية مجرمة وفقاً للمواد 7 و16 من الاتفاقية (الأمم المتحدة، 2024).

يمكن لليبيا الاستفادة من اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية بعدة طرق لتعزيز أمنها السيبراني وحماية بنيتها التحتية الرقمية، ستتيح الاتفاقية لليبيا فرصة التعاون مع دول أخرى في مجال مكافحة الجريمة السيبرانية، ستوفر الاتفاقية الدعم الفني والتدريب لبناء القدرات الوطنية في مجال الأمن السيبراني، ستساعد الاتفاقية ليبيا على تحديث قوانينها وتشريعاتها لتتوافق مع المعايير الدولية، مما يعزز من قدرتها على مكافحة الجرائم السيبرانية بفعالية، من خلال الالتزام بالاتفاقية، يمكن لليبيا تعزيز ثقة المواطنين والشركات في الفضاء الرقمي، مما يشجع على استخدام التكنولوجيا بشكل آمن وفعال.

2.4.2. المؤتمرات الدولية والإقليمية :

تلعب المؤتمرات الدولية والإقليمية دوراً حيوياً في مكافحة التهديدات السيبرانية، من خلال توفير منصات لتبادل المعلومات وتحديد الاستراتيجيات، وتعزز هذه المؤتمرات التعاون الدولي والقدرات الوطنية في مواجهة التحديات السيبرانية المتنامية، لاسيما أنه عدد المؤتمرات الدولية والإقليمية التي تناولت موضوع الأمن السيبراني لا يمكن حصره ومع ذلك، سأسلط الضوء على بعض من أبرز هذه المؤتمرات التي لعبت دوراً بارزاً في تعزيز التعاون الدولي وتحسين الوعي بأهمية الأمن السيبراني، ما يلي:

1.2.4.2.المؤتمر الثاني للمتخصصين في أمن وسلامة الفضاءالإلكتروني المنعقد في مقر المركز العربي للبحوث القضائية والقانونية بيروت 25-27 /2014/8م وكان من اهم التوصيات التي اقرها المؤتمر هي متابعة دراسة مسودة مشروع الاتفاقية العربية لحماية أمن وسلامة الفضاء بعد مراجعتها من المؤتمر على ضوء الملاحظات الواردة من الدول العربية الاعضاء والتأكيد على ضرورة ايجاد آلية لتفعيل التعاون العربي وتبادل الخبرات والزيارات ووضع الخطط لتفعيل التدريب وضرورة دعوة الدول العربية لانشاء هيئة مركزية وطنية مختصة بحماية امن وسلامة الفضاء السيبراني والتأكيد على دعوة الدول العربية إلى استكمال الأطر التشريعية والبنى التحتية تمهيدا لتشكيل هيئات، او لجان المصادقة والتوقيع الإلكتروني والاستفادة من التجارب العربية في هذا المجال وأخيراً أنشاء مراكز الاستجابة لطواري الحاسوب في الدول العربية (الاشقر:2016:174-173).

2.2.4.2.مؤتمر قمة الأمن السيبراني مينابولس مينيسوتا الولايات المتحدة 22-21 اكتوبر عام 2014م شارك فيه ممثلون من القطاع العام والخاص لمناقشة التدابير المضادة للتهديدات السيبرانية وتعزيز امن القطاع العام والخاص في مواجهة الجريمة الإلكترونية وقياس مدى تامين برامج الحاسب الالي ضد الهجمات السيبرانية(العمري:2020:117).

3.2.4.2.المؤتمر الثالث عشر للأمم المتحدة لمنع الجريمة والعدالة الجنائية المنعقد في الدوحة بقطر في الفترة الممتدة بين 12 و 19 أبريل عام 2015م، ومن أهم التوصيات التي أقرها المؤتمر في مجال مكافحة الجريمة السيبرانية وهي يجب استحداث أدوات وبرامج من أجل تسهيل مكافحة الجريمة السيبرانية ومنعها، حيث أن هذا النوع من الجرائم يتطلب من الدول أن تنمي قدرتها في جانب تدابير المنع والتحري المضادة وبناء قدرات أجهزة إنفاذ القانون ونظم العدالة الجنائية في مجال التحري عن الجرائم السيبرانية والتحقق فيها، وعمليات الاستدلال الجنائي الرقمية، وكيفية التعامل مع الأدلة الإلكترونية وأيضا بأن تنظر الدول في وضع اتفاقية بشأن الجريمة السيبرانية ضمن سياق المؤتمر والتأكيد على أهمية إشراك القطاع الخاص في مجال مكافحة الجريمة السيبرانية ويتعين على المحققين والجهات المختصة في مجال المكافحة لهذا النوع من الجرائم أن يعتمدوا استراتيجيات جديدة كأن يعملوا على تدعيم الشركات مع فرق بحث أكاديمية في مجالات متنوعة (المؤتمر الثالث عشر للأمم المتحدة:2015).

4.2.4.2. المؤتمر الإقليمي الثامن للأمن السيبراني يومي 27 - 28 اكتوبر 2019م، بسلطنة عمان تحت شعار ثورة الأمن السيبراني مع مشاهدة ملامح تطبيقات الثورة الصناعية الرابعة من خلال مجموعة التقنيات المكونة لها من ذكاء اصطناعي، وشبكة الجيل الخامس، والصناعات الروبوتية والطباعة ثلاثية الأبعاد والتحول الرقمي للأعمال وتناول، المؤتمر التطور التقني الصناعية الرابعة ومناقشة أفضل الممارسات لتحديد سياسة الأمن السيبراني الوطنية والتنظيمية، ومن أهم أهدافه الاطلاع على افضل الممارسات من كبار الخبراء في مجال الامن السيبراني (بلعسل وعمروش:2021:174).

5.2.4.2.مبادرة عمل وارسو عقد ممثلو أكثر من 40 دولة مجموعة عمل معنية بأمن الفضاء الإلكتروني في يومي 7 إلى 8 ديسمبر عام 2019م في كوريا الجنوبية لمناقشة استراتيجيات الردع والهجمات الالكترونية بشكل افضل (العمري:2020:117).

6.2.4.2.المؤتمر الاول للأمن السيبراني المنعقد في المملكة الاردنية الهاشمية بشهر أغسطس عام 2019م، والذي يتضن احدث أنواع التقنية في مجال الامن والجرائم الالكترونية والادلة الجنائية الرقمية، بمشاركة نخبة من الخبراء على المستوى الدولي وكبريات الشركات العالمية المتخصصة، وسعى المؤتمر إلى تقديم مجموعة من الأهداف أبرزها التعريف بقانون الأمن السيبراني الأردني 2019 وقانون الجرائم الالكترونية وتعزيز الأمن السيبراني ونشر الوعي بالمفاهيم الخاصة بالأمن السيبراني على مستوى الافراد المؤسسات(العمري:2020:125-126).

7.2.4.2.المؤتمر الدولي الثالث لأمن المعلومات والأمن السيبراني، القاهرة، 3-4 يونيو 2024م في إطار مساعي وجهود المنظمة العربية لتكنولوجيات الاتصال والمعلومات لتعزيز العمل العربي المشترك والتعاون الاقليمي والعالمي، وشهد هذا المؤتمر مشاركة مجموعة من الوزارات والهيئات والشركات العربية والدولية إضافة لأكثر من 20 وزارة وهيئة ومؤسسة حكومية مصرية (المؤتمر الدولي الثالث لأمن لمعلومات والامن السيبراني:2024).

ويمكننا استنتاج أن المؤتمرات الإقليمية والدولية تعتبر منصات حيوية لتبادل المعرفة والخبرات في مجال الأمن السيبراني وتلعب هذه المؤتمرات دورًا أساسيًا في تعزيز التعاون بين الدول والمنظمات، حيث تجمع خبراء وصناع قرار من مختلف أنحاء العالم لمناقشة التحديات التي تواجه الدول في هذا المجال، كم تسهم المؤتمرات في تعزيز الوعي حول قضايا الأمن السيبراني، وتوفير فرص للتدريب والتطوير المهني، وتسهيل تبادل المعلومات حول أحدث التقنيات والأساليب المتبعة في مواجهة التهديدات السيبرانية، كما تساهم في بناء شراكات استراتيجية بين القطاعين العام والخاص، مما يعزز من قدرة الدول على التصدي للهجمات السيبرانية، علاوة على ذلك، توفر هذه الفعاليات منصة لتطوير السياسات والاستراتيجيات المتعلقة بالأمن السيبراني، مما يساعد في تحسين استجابة الدول للتهديدات المتزايدة من خلال النقاشات وورش العمل والتوصيات، حيث يتمكن المشاركون من التعرف على أفضل الممارسات العالمية وتطبيقها في سياقاتهم المحلية، وتمثل المؤتمرات الدولية والإقليمية عنصرًا أساسيًا في تعزيز الأمن السيبراني على المستوى العالمي، حيث تسهم في بناء مجتمع متعاون وقادر على مواجهة التهديدات السيبرانية.

3.4.2 جهود المنظمات والشركات الإقليمية والدولية :

تلعب المنظمات والشركات دوراً حيوياً في تعزيز الأمن السيبراني على مستوى العالم وذلك من خلال مجموعة واسعة من الأنشطة والجهود المشتركة التي تتمثل في وضع الإطارات القانونية والمعايير التقنية وتسهيل التعاون الدولي، وتقديم الدعم التقني في مجال الأمن السيبراني، وسيتم تناول على سبيل المثال لا الحصر مجموعة من المنظمات والشركات الدولية مع التركيز على الجهود الأكثر اهمية والتي تعتبر مهمة في تعزيز الامن السيبراني وهي :

1.3.4.2. الأمم المتحدة: اهتمت الأمم المتحدة بالبناء المؤسسي، فقامت بإنشاء بعض الكيانات مثل، الشراكة التعددية ضد التهديدات السيبرانية IMPACT عام 2009 أول منظمة تدعمها الأمم المتحدة للتحالف لدعم الأمن السيبراني (جمال الدين:207:2023). ولعبت الامم المتحدة دورا بناءً في الدبلوماسية السيبرانية حيث انشات فريقياً من الخبراء الاكاديميين لتحقيق التعاون الدولي في دراسة قضايا الأمن السيبراني وتقديم توصيات بشأن التدابير الرامية إلى تقليل التهديدات والمخاطر السيبرانية وزيادة الاستقرار وفي عام 2013 نادى فريق الخبراء الأكاديمين من خلال الجهود الدبلوماسية بأن مبدا السيادة الوطنية ينطبق على الفضاء الإلكتروني بدرجة انطباقه على الارض نفسها كما تم الاتفاق على قائمة مطولة من قواعد واجراءات بناء الثقة في الفضاء الإلكتروني (الشادلي:1258:2023).

ولعبت القرارات الصادرة عن الأمم المتحدة حول الأمن السيبراني دورا في جذب انتباه الدول الاعضاء إلى اهمية التحديات السيبرانية، كذلك اصدرت قرارا حول ضرورة نشر ثقافة الأمن السيبراني، وضرورة زيادة الوعي والمسؤولية لدى الدول بما يضمن التعاون في الوقت المناسب، لمنع الحوادث السيبرانية، وقد بدا اهتمام الدول بالتعاون واضحا من خلال مشاركتها في اعمال الجمعية العامة للأمم المتحدة التي ضمت 192 دولة التي واصدرت عدداً من القرارات التي يمكن اعتبارها قاعدة لانطلاق الجهود في مكافحة التهديدات السيبرانية (الاشقر:106:2016).

وبذلت الأمم المتحدة جهدا كبيرا في مجال مكافحة التهديدات السيبرانية، من خلال الجمعية العامة، ومجلس الامن، ومكتب مكافحة الارهاب، ودعت دول العالم إلى ضرورة الالتفات إلى هذا الخطر الجديد على الامن الداخلي للدول وكذلك على أمن العلاقات بين الدول لكونه خطرا امنيا لا يختلف في تهديده عن التهديدات الامنية التقليدية التي واجهت الدول وكانت المرة الأولى التي يتخذ فيها قرار سياسي على المستوى الدولي لترجمة الجهود الدولية إلى مراحل عملية(عبدالصادق:2015). وتم تشكيل هذه المجموعة من أربعة فرق للخبراء الحكوميين، لمعالجة الأخطار القائمة والمحتملة في الفضاء الإلكتروني وتدابير التعاون الممكنة للتصدي لها، وفي سياق سبل الحفاظ على استعمال الفضاء الخارجي لأغراض سلمية، تم الاتفاق في تقرير لجنة استخدام الفضاء الخارجي في الأغراض السلمية في دورتها الثانية والستين للجمعية العامة 2019، على أَنَّ لها دوراً أساسيًا عليها أن تلعبه في تعزيز الشفافية، وبناء الثقة بين الدول وكذلك في ضمان الحفاظ على استخدام الفضاء الخارجي في الأغراض السلمية، وذلك من خلال أعمالها في المجالات العلمية والتقنية والقانونية ومن خلال سعيها إلى تشجيع الحوار، وتبادل المعلومات على الصعيد الدولي بشأن مختلف المواضيع المتعلقة باستكشاف الفضاء الخارجي واستخدامه (الجمعية العامة للأمم المتحدة :2019).

وقامت الأمم المتحدة بتأسيس الاتحاد الدولي للاتصالات (ITU) عام 1865م، في باريس ،ويعد هذا الاتحاد ثاني أقدم منظمة دولية قائمة حتى الآن، يظم الاتحاد الدولي للاتصالات 193 دولة، بالإضافة إلى العديد من الشركات والمؤسسات المتخصصة في مجال الاتصالات، هذه العضوية الواسعة تجعل الاتحاد منصة عالمية للتعاون وتنسيق الاتصالات والأمن السيبراني، ويعترف الاتحاد الدولي للاتصالات بأهمية هذه القضية وقد وضع مؤشر الأمن السيبراني هو أداة قيمة لقياس مستوى الأمن السيبراني في الدول المختلفة ويعتمد هذا المؤشر على مجموعة من المؤشرات الفرعية التي تغطي جوانب مختلفة من الأمن السيبراني (International Telecommunication Union:2024) وتأتي أهمية المؤشر كالآتي:

- يساعد في تحديد نقاط الضعف والقوة في نظام الأمن السيبراني للدولة.
- يوفر معلومات أساسية لصناع القرار لوضع سياسات فعالة لتعزيز الأمن السيبراني.
- يسمح للدول بمقارنة أدائها في مجال الأمن السيبراني مع الدول الأخرى.
- يشجع الدول على اتخاذ الإجراءات اللازمة لتحسين مستوى أمنها السيبراني.

ويقدم مؤشر الأمن السيبراني العالمي (GCI) لمحة عامة عن مستوى تطورات الأمن السيبراني في دول العالم بالتركيز على التدابير القانونية، التدابير التقنية، التدابير التنظيمية، بناء القدرات والتعاون الدولي، (International Telecommunication Union :2024).

نشر الاتحاد الدولي للاتصالات (ITU) دليلاً لتطوير استراتيجية وطنية للأمن السيبراني بالشراكة مع أكثر من اثنين وعشرين شريكا من المنظمات الحكومية الدولية والقطاع الخاص والاوساط الأكايمية وتم اصدار نسختين؛ الطبعة الاولى 2017م، والطبعة الثانية 2021م، ويهدف الدليل إلى تعزيز الأمن السيبراني ودعم القادة وواضعي السياسات، على الصعيد الوطني، في مجال اعداد استجابات دفاعية واستباقية للمخاطر السيبرانية في شكل استراتيجية وطنية للأمن السيبراني، وفي التفكير الاستراتيجي بالأمن السيبراني والتأهب

السيبراني والاستجابة والصمود وبناء الثقه، والأمن في استعمال تكنولوجيا المعلومات والاتصالات وفقًا للاتحاد الدولي للاتصالات فإن الدليل مبني على خمس ركائز استراتيجية، يجب تنفيذ الركائز الثلاث الأولى، أي الإطار القانوني والتدابير الفنية والهياكل التنظيمية على المستويين الوطني والإقليمي ولكن على المستوى الدولي تبدو الركيزتان الأخيرتان، مثل بناء القدرات والتعاون الدولي، متقاطعتين في جميع المجالات(دليل لوضع استراتيجية الامن السيبراني:2017).

2.3.4.2. جامعة الدول العربية: صدر عن جامعة الدول العربية قرار استرشدي لمكافحة الجريمة تقنية المعلومات وما في حكمها عام 2004م، ونظرا للتطور السريع في مجال الفضاء الإلكتروني، سعت الدول العربية إلى تقنين وتجريم الأعمال غير المشروعة المرتكبة من خلال استخدام هذا الفضاء بالتوقيع على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010م، من أجل تعزيز التعاون بين الدول العربية لمكافحة الجرائم السيبرانية والحفاظ على امنها وسلامة مجتمعاتها ودعا المجلس الدول العربية المصدقة على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إلى التعاون لمنع الارهابيين من استغلال تكنولوجيا المعلومات والإتصالات والإنترنت وأكد المجلس على أهمية تعزيز التعاون مع المنظمات والوكالات الدولية المتخصصة للحصول على المساعدات المطلوبة في بناء القدرات اللازمة (عبد الجواد:2020: 499-500) ورحب مجلس وزراء الخارجية العرب في دورته 160 بقرار المجلس الاقتصادي والاجتماعي بجامعة الدول العربية انشاء مجلس وزراء الأمن السيبراني العرب بناء على مقترح من المملكة العربية السعودية، ويهدف المجلس إلى تنمية التعاون وتوثيقة وتنسيق الجهود بين الدول العربية في جميع الجوانب المتعلقة بموضوعات الأمن السيبراني، ويأتي انشاء المجلس استشعاراً من الدول العربية بأهمية التنسيق والتعاون الإقليمي العربي في الأمن السيبراني (الشرق الاوسط:2024) وخلال إفتتاح أعمال الدورة 51 تم إطلاق الرؤية العربية للأمن السيبراني الواقع - التحديات الفرص بالتعاون مع المنظمة العربية لتقنية الاتصال والمعلومات، وقامت جامعة الدول العربية بنشر الاستراتيجية العربية للأمن السيبراني 2023-2027م. هدفت الاستراتيجية إلى تحقيق تطور نمو موحد ومتناغم داخل المنطقة العربية لمستوى النضج لحماية الفضاء الإلكتروني من التهديدات السيبرانية التي تتطور بشكل مستمر وسريع، كما حدثت الاستراتيجية التحديات التي تواجه الحكومات العربية عند العمل على تأمين فضاءها الإلكتروني، والطريقة المثلى للتعامل معها، والغاية الرئيسية من الاستراتيجية هو توفير التوجيه والتأطير بشان الامن السيبراني، وتقديم أفضل الممارسات التي تشكل الركيزة الأساسية لغالبية البلدان العربية في هذا المجال (الاستراتيجية العربية للأمن السيبراني:2023).

3.3.4.2 منظمة حلف شمال الاطلسي(الناتو): دفع عجز حلف الناتو في مواجهة الهجمات السيبرانية على إستونيا عام 2007م، وعلى جورجيا عام 2008م، إلى تكوين وحدة دفاع للأمن السيبراني مقرها تالين عاصمة استونيا وعمل على تطوير المفهوم الاستراتيجي للحلف حتى اصبح الفضاء الإلكتروني منطقة لعمليات الحلف وأيضا نفد الناتو السياسة الخاصة به في مجال الدفاع السيبراني في 2008م، من أجل حماية مواردها (عبدالجواد:2020:501). وجزء من هذه السياسة أنشاء حلف شمال الاطلسي هيئة معنية بإدارة الدفاع السيبراني وفريقاً للاستجابة للحوادث الحاسوبية يكفل إرسال فرق الدعم السريع إلى البلدان الأعضاء

ومركزاً للتميز من أجل الدفاع السيبراني التعاوني، ويضم هذا المركز خبراء في مجال الامن السيبراني(جمال الدين:2023:207) .

ومن بين الجهود الأخرى التي قام بها الحلف هو إنشاء مركز التميز للدفاع السيبراني التعاوني وهو منشأة بحثية وتدريبية معتمدة من الحلف في مجال الأمن السيبراني تعمل على تعزيز التعاون وتبادل المعلومات بين الدول الأعضاء ومن بين الجهود الأكاديمية مركز القدرات العالمية للأمن السيبراني (GCSCC) في جامعة أكسفورد، ويقوم المركز لبناء القدرات في مجال الأمن السيبراني ويدعو إلى زيادة النطاق العالمي و بناء القدرات في هذا مجال ، وقد طور نهجًا هو الأول من نوعه لتقييم نضج القدرات في مجال الأمن السيبراني، عبر خمسة أبعاد لتمكين الدول من تقييم نفسها وقياسها والتخطيط بشكل أفضل للاستثمارات وخطط الأمن السيبراني الوطنية، وتحديد أولويات تنمية القدرات (Redanliev:2024:28).

وضعت منظمة حلف شمال الأطلسي (الناتو)، عن طريق مركز التميز في الدفاع السيبراني التعاوني، مبادئ توجيهية لاستراتيجية الأمن السيبراني الوطنية عام 2013م، هدفت هذه الارشادات إلى مساعدة مخططي السياسات الوطنية في صياغة وتحسين وتنفيذ وتقييم استراتيجياتهم الوطنية للأمن السيبراني من أجل تحقيق أعلى مستوى من الحماية ضد التهديدات السيبرانية سريعة التطور وتتخدد هذه الإرشادات نهجا شاملاً للأمن السيبراني حيث تصل إلى مجموعة واسعة من الجهات الفاعلة والجوانب ذات الصلة من أجل دعم تطوير استراتيجيو وطنية للأمن السيبراني من شأنها أن تعود بالنفع على الحماية الشاملة لأنظمة الاتصالات والمعلومات الوطنية والأمن الوطني، وتحتوي المبادئ على الأبعاد الثلاثة لاستراتيجية الأمن السيبراني الوطنية وهي نهج الحكومة ككل (الحكومية)، ونهج النظام بأكمله لتحسين التنسيق الدولي والوطني (الدولي)، ونهج الأمة بأكملها للتعاون مع الجهات الفاعلة غير الحكومية (CCDCOE:2013).

4.3.4.2. الاتحاد الأوروبي: أنشأت وكالة الاتحاد الأوروبي لأمن الشبكات والمعلومات (ENISA) دليلاً عمليًا حول وضع وتصميم استراتيجيات الأمن السيبراني الوطنية (NCSS) 2012م، وتم تطويره عام 2016م، لدعم الدول الأعضاء في الاتحاد الاوروبي ومنطقة رابطة التجارة الحرة الاوروبية، والهدف من هذا الدليل هو تطوير دعم الدول الاعضاء في الاتحاد الاوروبي في جهودها لتطوير وتحديث استراتيجياتها الوطنية للأمن السيبراني كما يوفر رؤى مفيدة لإصحاب المصلحة المشاركين في دورة حياة الاستراتيجية منهم القطاع الخاص والمجتمع المدني، والجمهور المستهدف من هذا الدليل هم المسؤولون العموميون وصناعو السياسات على الصمود السيبراني (ENISA: 2016).

5.3.4.2. شركة ميكروسوفت: وضعت الشركة دليلاً لإعداد استراتيجية وطنية للامن السيبراني عام 2013م، وتعتقد الشركة ان كل دولة يجب ان يكون لديها استراتيجية وطنية للأمن السيبراني وان الاستراتيجية أمر بالغ الاهمية لإدارة المخاطر السيبرانية على المستوى الوطني وتطوير التشريعات او اللوائح المناسبة لدعم هدة الجهود، والهدف من هذه الدليل هو وضع توصيات لصناع القرار من اجل تطوير استراتيجية الامن الوطني (Mirosoft:2013) .

6.3.4.2. منظمة الدول الأمريكية: أنشأت منظمة الدول الأمريكية، بالشراكة مع بعض المؤسسات، دليل استراتيجية الأمن السيبراني الوطنية عام 2022م، وكان الهدف من هذه الاستراتيجية هو معالجة تحديات التهديدات السيبرانية من خلال تقديم معلومات حول النهج الممكن اتباعه لصناع السياسات الذين يعملون على تطوير أنظمة الامن السيبراني في الأمريكتين وقد قدم في هدا الدليل اوصاف النهج والاعتبارات المختلفة والمحتملة، التي تم توضيحها من خلال امثلة من بعض الدول الاعضاء في منظمة الدول الأمريكية وغيرها من الدول ذات الصلة عالمياً، لتطوير نظام الامن السيبراني، ومعالجة تهديدات الامن السيبراني وفي حين ان صناع السياسات في الامريكتين هم الجمهور الأساسي لهذا الدليل من أجل ان تكون هذة الوتيثة مفيدة لاي جهة تعمل في بناء قدرات الأمن السيبراني من خلال تقديم امثلة عملية للممارسات الجيدة (Secretary general of the organization of American states:2022).

ونستنتج بأن المنظمات الدولية والإقليمية لعبت دوراً محورياً في تعزيز الأمن السيبراني على الصعيد العالمي وتسعى هذه المنظمات إلى توحيد الجهود الدولية لمواجهة التهديدات المتزايدة في الفضاء الإلكتروني وذلك من خلال وضع المعايير الدولية، تسهيل التعاون بين الدول وبناء القدرات الوطنية، كما تشجع على تبادل أفضل الممارسات، الا أن التحديات المستقبلية تتطلب تضافر جهود أكبر، فالتعاون الدولي هو السبيل الوحيد لمواجهة التهديدات السيبرانية المتطورة باستمرار.

4.4.2. معايير الأمن السيبراني :

هناك العديد من المعايير الدولية التي تساهم في تعزيز الأمن السيبراني من أبرزها :

1. المعيار الذي نشرته المنظمة الدولية للمقاييس (ISO) وأيضا المعهد الوطني للمعايير والتكنولوجيا والتوحيد القياسي واللجنة الكهرتقنية الدولية (IEC) ISO/IEC 27001 هذا المعيار هو الأكثر شهرة لإدارة أمن المعلومات (ISMS) حيث يحدد متطلبات نظام إدارة أمن المعلومات ويشمل تقييم مخاطر أمن المعلومات ومعالجتها https://www.iso.org/standard/27001 .
2. إطار عمل الأمن السيبراني من المعهد الوطني للمعايير والتكنولوجيا NIST Cybersecurity Framework (NIST) يوفر إرشادات لتحسين إدارة مخاطر الأمن السيبرانيhttps://www.nist.gov/cyberframework
3. اللائحة العامة لحماية البيانات في الاتحاد الأوروبي General Data Protection Regulation(GDPR). https://gdpr-info.eu/
4. قانون قابلية التأمين الصحي والمساءلة في الولايات المتحدة يحدد معايير لحماية المعلومات الصحية المحمية، Health Insurance Portability and Accountability Act (HIPAA) https://www.cdc.gov/phlp/php/resources/health-insurance-portability-and-accountability-act

5. مجموعة من الضوابط الأمنية التي وضعها مركز أمن الإنترنت CIS Controls: (CIS) توفر إرشادات عملية لتحسين الأمن السيبراني وتقليل المخاطر. https://www.cisecurity.org/controls
6. دليل شامل حول التعامل مع الحوادث FIRST(Forum of Incident Response and Security Teams) التابعة للاتحاد الأوروبي والذي يقدم نصائح وتوصيات عملية لدعم جهود الاستجابة للحوادث، ويوفر إرشادات ومعايير للتعامل مع الحوادث الأمنية والاستجابة لها بشكل فعال.https://www.pcisecuritystandards.org / .
7. اللجنة الفنية لاستخبارات التهديدات السيبرانية OASIS CTI (Cyber Threat Intelligence Technical Committee تعمل على التطوير المستمر لمعايير STIX و TAXII تهدف إلى تطوير مجموعة من التمثيلات والبروتوكولات المعلوماتية، و تعمل على تطوير وتحديث المعايير لضمان توافقها مع أحدث التهديدات والتحديات السيبرانية.-https://www.oasis-open.org/committees/cti/charter.php.
8. ـ دليل الاستجابة للحوادث التابع لمركز تنسيق الاستجابة لطوارئ الحاسب الآلي (CERT/CC): والجهة المنفذة لدليل هي فرق الاستجابة للحوادث السيبرانية (CSIRTs) التي تتبع إرشادات CERT/CC يوفر إرشادات مفصلة حول كيفية الاستجابة للحوادث السيبرانية والتعامل معها يتضمن هذا الدليل خطوات وإرشادات مفصلة حول كيفية اكتشاف الحوادث، تقييمها، احتوائها، والقضاء عليها، واستعادة الأنظمة المتضررة، كما يشمل الدليل أيضًا أفضل الممارسات لتوثيق الحوادث وتحليلها لمنع تكرارها في المستقبل https://cert.gov.sa/ar/about-us/services /.
9. سلسلة الاتحاد الدولي للاتصالات X.1500 تشمل معايير وإرشادات لتعزيز الأمن السيبراني على مستوى الاتصالات والجهة المنفذة لهذه المعايير هي قطاع توحيد مقاييس الاتصالات (ITU-T)، الذي يعمل على تطوير وتحديث هذه التوصيات بالتعاون مع الدول الأعضاء وأعضاء القطاع الخاص والأكاديميين https://www.itu.int/ar/history/Pages/AnnualReports.aspx .
10. مؤسسة الإنترنت للأسماء والأرقام المخصصة ICANN وهي منظمة غير ربحية مسؤولة عن تنسيق نظام أسماء النطاقات (DNS) وضمان استقراره بالتعاون مع مختلف الجهات الفاعلة في مجال الإنترنت لضمان تنفيذ خطة الاستجابة بشكل فعال .https://www.icann.org/cybersecurityincidentlog
11. أدوات القدرات السيبرانية القائمة على الصعيد الوطني، Global Open Access Tool، تُعتبر أدوات مهمة لتقييم وتحسين القدرات السيبرانية على مستوى الدول (المنتدى العالمي للأمن السيبراني (2020:) ومع ذلك، لا تُعتبر هذه الأدوات بالضرورة معايير دولية رسمية مثل ISO أو NIST، لكنها تُستخدم على نطاق واسع على أنها أدوات مرجعية لتقييم القدرات السيبرانية الوطنية وتعزيزها (المنتدى العالمي للخبرات السيبراني:2020). والتي تتمثل على النحو الآتي:

- أداة تقييم بناء القدرات (GOAT) أداة وضعها البنك الدولي لدعم البلدان النامية لمكافحة الجريمة السيبرانية في تحديد المجالات ذات الأولوية لتوزيع الموارد بشكل فعال في مجال بناء القدرات.
- الرقم القياسي للتأهب السيبراني 2.0 (CRI): أداة من معهد بوتوماك لدراسة السياسات العامة لتقييم التزام البلدان ونضجها في تأمين البنية التحتية الرقمية.
- نموذج لتقييم نضج القدرات السيبرانية للدول، (CMM) الصادر عن المركز العالمي لقدرات الأمن السيبراني (GCSMM)، جامعة أكسفورد وشركائها، يعمل هذا النموذج على قياس قدرة الأمن السيبراني للبلد، قامت ليبيا بعمل هذا النموذج سنة 2023م.
- إطار وضع الاستراتيجيات السيبرانية وتنفيذها (CSDI): نموذج من شركة MITRE لتطوير الاستراتيجيات السيبرانية الوطنية وتنفيذها.
- إطار تقييم القدرات الوطنية (NCAF)، أداة من وكالة الاتحاد الأوروبي للأمن السيبراني (ENISA) لدعم الدول الأعضاء في قياس مستوى نضج قدراتها السيبرانية.
- (NCSI)الرقم القياسي الوطني للأن السيبراني الصادر عن أكاديمية الحوكمة الإلكترونية(eGA) وهو رقم قياسي عالمي يقيس تأهب البلدان لمنع التهديدات السيبرانية وإدارة الحوادث السيبرانية.

5.4.2. الاستراتيجيات الوطنية للأمن السيبراني(NISS) :

من الواضح أن وتيرة تطوّر التهديدات السيبرانية أصبحت تسير بشكل متوازي مع التطورات التي تشهدها تكنولوجيا الاتصال والمعلومات، أصبحت التهديدات الحديثة معقدة جدا، بمعنى أنها تؤدي إلى أضرار جسيمة، وتؤثر على نطاق واسع للدول بما في ذلك الأمن القومي لها، وقد أجبر هذا التطور الدول عبر العالم على تحسين برامج الأمن السيبراني الخاصة بها، من خلال تطوير الاستراتيجيات الوطنية للأمن السيبراني، وفقًا لمؤشر الاتحاد الدولي للاتصالات، نجد أن 127 دولة خلال السنوات السابقة قد طورت استراتيجيات وطنية للأمن السيبراني من أجل التعامل مع التهديدات السيبرانية بطريقة عملية وأكثر تنظيما (International Telecommunication Union :2024). وقد تم اختيار استراتيجيات خمس دول وهي الدول الاولى دوليًا وإقليمًا وعربياً ورياديا حسب مؤشر الاتحاد الدولي للاتصالات عام 2024م.

1.5.4.2.الاستراتيجية الوطنية لأمن المعلومات للمملكة العربية السعودية :

تم اصدار هذه الاستراتيجية عام 2011م وتسعى الاستراتيجية الوطنية لأمن المعلومات إلى تحقيق مجموعة من الأهداف وهي تمكين استخدام المعلومات ومشاركتها بحرية وأمان، زيادة أمن وسلامة المعلومات عبر الإنترنت، تطوير المرونة في نظم المعلومات وزيادة الوعي والتثقيف بالمخاطر الأمنية ومسؤولية حماية المعلومات وأيضا إنشاء مجموعة من المبادئ التوجيهية الوطنية لإدارة أمن المعلومات، وإدارة المخاطر، واستمرارية الأعمال وتتكون الاستراتيجية الوطنية لأمن المعلومات من ثلاثة عناصر رئيسية (National Information Security Strategy for the Kingdom of Saudi Arabia NISS:2011).

- الناس: تقترح هذه الاستراتيجية من بين مجموعات أخرى من الأشخاص الاستفادة من النساء والشباب السعوديين عنصر أساسياً لنجاح انتشار تنظيم الدولة الإسلامية.
- العمليات: من خلال الاستفادة من بعض النقاط الرئيسية هنا والاستفادة من القوانين الحالية في المملكة، فإن المملكة العربية السعودية في وضع جيد لتنفيذ جهاز الأمن والمخابرات الوطني.
- التكنولوجيا: ستكون التكنولوجيا متاحة دائمًا والمفتاح هو استخدام الأدوات المناسبة في الوقت المناسب،.

تُعد الاستراتيجية الوطنية لأمن المعلومات وثيقة مهمة ستساعد المملكة العربية السعودية على حماية المعلومات والأنظمة الحيوية من التهديدات السيبرانية، وهذا يمكن المملكة العربية السعودية ضمان مستقبل آمن ومزدهر للجميع.

2.5.4.2.استراتيجية الأمن السيبراني لإستونيا :

استراتيجية الأمن السيبراني الإستونية من بين الاستراتيجيات الأولى من نوعها على مستوى العالم ، وكانت استراتيجية الأمن السيبراني لعام 2008م، أول وثيقة استراتيجية وطنية لإستونيا اعترفت بالطبيعة المتعددة التخصصات للأمن السيبراني والحاجة إلى عمل منسق في المنطقة، وتم تاسيسها بعد الهجمات السيبرانية التي وقعت عام 2007 ضد إستونيا، وبدأ يُنظر إلى الأمن السيبراني على أنه جزء أساسي من الأمن القومي.(Cyber security Strategy Republic of Estonia:2019-2022). وتعد استراتيجية الأمن السيبراني هذه هي الوثيقة الوطنية الثالثة لاستراتيجية الأمن السيبراني في إستونيا وتحدد الرؤية والأهداف ومجالات العمل ذات الأولوية على المدى الطويل والأدوار والمهام للمجال، باعتبارها الأساس لتخطيط الأنشطة وتخصيص الموارد، وتستند الاستراتيجية إلى الدروس المستفادة خلال الفترتين الاستراتيجيتين السابقتين (2008-2013 و2014-2017) إنها تشمل جميع أصحاب المصلحة المساهمين في إستونيا القطاع العام (المدني والدفاعي)، ومقدمي الخدمات الأساسية، ورجال الأعمال القطاعيين، والأوساط الأكاديمية وتهدف هذه الوثيقة إلى الاتفاق على وتهيئة الظروف لتنفيذ سياسة قطاعية ومنهجية وشاملة، وقد تم إعداد استراتيجية الأمن السيبراني في عملية متماسكة مع المتطلبات الرقمية لإستونيا لعام 2020م(Cyber security Strategy Republic of Estonia:2019-2022).

لقد تم التخطيط للأهداف والمؤشرات الرئيسية لاستراتيجية الأمن السيبراني على مدى أربع سنوات، مع إجراء مراجعة مؤقتة في نهاية الأجندة الرقمية الحالية في عام 2020. وتمثلت الرؤية في مجتمع إستوني آمن ومزدهر في بيئة رقمية موثوقة، وتمثلث الأهداف للاستراتيجية في تعزيز قدرة الدولة على الصمود في مواجهة التهديدات السيبرانية وزيادة الوعي بالأمن السيبراني وتحسين الثقافة الأمنية ، بناء اقتصاد رقمي آمن وموثوق، تعزيز التعاون الدولي في مجال الأمن السيبراني ، (Republic of Estonia:2019-2022 Cyber security Strategy) وتمثل المبادئ الأساسية للاستراتيجية على النحو الآتي:

- أن يكون الأمن السيبراني في صميم جميع القرارات المتعلقة بتكنولوجيا المعلومات والاتصالات.
- يجب أن يتقاسم جميع أصحاب المصلحة المسؤولية عن الأمن السيبراني.

- أن تستند جهود الأمن السيبراني إلى تقييم المخاطر واتخاذ قرارات مستنيرة.
- تعزيز التعاون الدولي في مجال الأمن السيبراني.
- تشجيع الابتكار في مجال الأمن السيبراني.
- أن يتم ضمان الأمن السيبراني مع احترام حقوق الإنسان والحريات الأساسية.

3.5.4.2.استراتيجية الأمن السيبراني للولايات المتحدة الامريكية :

تُعد استراتيجية الأمن السيبراني للولايات المتحدة وثيقة حكومية تم إصدارها عام 2003م وتحدد الأهداف والخطط لحماية البلاد من التهديدات الإلكترونية وتُغطي هذه الاستراتيجية مجموعة واسعة من الموضوعات بما في ذلك حماية البنية التحتية الحيوية، ومكافحة الجرائم الإلكترونية وحماية الخصوصية المدنية وتعزيز الابتكار في مجال الأمن السيبراني والتعاون الدولي، بالإضافة إلى ذلك، تهدف استراتيجية الأمن السيبراني للولايات المتحدة إلى تحقيق الأهداف(The national strategy to secure cyberspace:2003) الأتية:

- تقليل مخاطر الهجمات الإلكترونية وحماية البيانات والأنظمة الحساسة.
- تُساعد بيئة الإنترنت الآمنة على تعزيز الابتكار، والنمو الاقتصادي.
- تُؤكد الاستراتيجية على أهمية حماية الخصوصية، وحريات التعبير.
- التعاون مع الدول الأخرى لمواجهة التهديدات الإلكترونية العالمية.

تعد الاستراتيجية الوطنية للولايات المتحدة الأمريكية مسارا منظماً وطموحاً لتعزيز الدفاعات السيبرانية في البلاد وتشير الى التزام الولايات المتحدة بتحسين قدراتها في مجال الامن السيبراني، وتوكد الاستراتيجية على الاستثمار في البحث والتطوير في مجال الأمن السيبراني، الذي يدعم سعي الامة الى ايجاد حلول متطورة لمكافحة التهديدات السيبرانية وتوكد الاستراتيجية على اهمية زيادة تبادل المعلومات حول التهديدات السيبرانية وتحسين التعاون بين القاطعين العام والخاص لانشاء نظام بيئي اكثر شمولا للدفاع السيبراني، وتهدف الاستراتيجية إلى سد فجوة مهارات الأمن السيبراني من خلال إعطاء الألولوية لتطوير وتدريب خبراء الامن السيبراني، وضمان قوة عاملة مدربة، ذات معرفة قادرة على الدفاع بكفاءة ضد الهجمات السيبرانية، وتوكد الاستراتيجية على تعزيز مرونة البنية التحتية الحيوية من خلال حماية الأنظمة والشبكات المهمة من الاضطرابات السيبرانية المحتملة، وتستند هذه الاستراتيجية على ركائز أساسية هي المرونة، الكشف، الاستجابة، التخفيف (Redanliev:-2024:14-15).وتتضمن استراتيجية الأمن السيبراني للولايات المتحدة الأمريكية عددًا من المبادرات الرئيسية منها إنشاء وكالة جديدة للأمن السيبراني تكون مسؤولة عن التنسيق بين الجهود الفيدرالية للأمن السيبراني، تحسين مشاركة المعلومات بين القطاعين العام والخاص، تعزيز البحث والتطوير في مجال الأمن السيبراني، رفع مستوى الوعي العام بالأمن السيبراني(The national strategy to secure cyberspace:2003). وتتضمن خطة العمل على

المدى القريب للولايات المتحدة 10 عناصر رئيسية The national strategy to secure) cyberspace:2003)، منها:

- تعيين مسؤول سياسة الأمن السيبراني في البيت الأبيض لتنسيق جهود الأمن السيبراني الوطنية، وتأسيس مديرية قوية داخل مجلس الأمن القومي لدعم مسؤول سياسة الأمن السيبراني، وضمان التنسيق الفعال بين الوكالات الحكومية المختلفة المعنية بالأمن السيبراني.
- تحديث الاستراتيجية الوطنية للأمن السيبراني لضمان مواكبتها للمخاطر والتهديدات المتطورة، والتأكد من تضمين الاستراتيجية تقييمًا مستمرًا لعمليات المركز الوطني للبنية التحتية للمعلومات والاتصالات (CNCI)والاستفادة من نجاحاته.
- تعيين مسؤول الخصوصية، والحريات المدنية داخل مديرية الأمن السيبراني في مجلس الأمن القومي، وضمان مراعاة الخصوصية والحريات المدنية في جميع سياسات، وممارسات الأمن السيبراني.
- تحسين التنسيق بين الوكالات وإنشاء آليات مشتركة بين الوكالات لتحليل القضايا المتعلقة بالأمن السيبراني بشكل تعاوني، وصياغة توجيهات سياسية موحدة، تحدد الأدوار والمسؤوليات، وتوضح سلطات كل وكالة فيما يتعلق بالأمن السيبراني.
- رفع مستوى الوعي العام، وإطلاق حملة وطنية للتوعية والتثقيف العام لتعزيز ممارسات الأمن السيبراني الجيدة بين الأفراد والمؤسسات، توفير معلومات وموارد تعليمية حول كيفية حماية أنفسهم من التهديدات السيبرانية.
- تطوير مواقف حكومية أمريكية موحدة بشأن قضايا الأمن السيبراني الدولي.
- تعزيز الشراكات الدولية لمعالجة التحديات المشتركة المتعلقة بالأمن السيبراني.
- بناء مبادرات دولية تتناول مجموعة واسعة من القضايا والسياسات والفرص المتعلقة بالأمن السيبراني.

4.5.4.2.الاستراتيجية الوطنية للأمن السيبراني للمملكة المتحدة :

نشرت المملكة المتحدة عام 2022م، الاستراتيجية الوطنية للأمن السيبراني لتلك السنة، وهي خطة لتحقيق أهداف محددة بحلول عام 2030م. تهدف الاستراتيجية إلى ضمان أن تظل المملكة المتحدة "قوة إلكترونية رائدة ومسؤولة وديمقراطية(National cyber strategy UK:2022)

تتمثل رؤية المملكة المتحدة لعام 2030م، في أن تكون قوة سيبرانية رائدة ومسؤولة وديمقراطية، تسعى المملكة المتحدة إلى استخدام قدراتها السيبرانية لخلق مجتمع أكثر أمانًا وازدهارًا واستدامة، وتعزيز مكانتها كقوة عالمية وتبني استراتيجية المملكة المتحدة للأمن السيبراني على التقدم المحرز في السنوات الماضية، تشمل هذه الاستراتيجية نهجًا شاملًا يُشرك جميع قطاعات المجتمع، وتُركز الاستراتيجية بشكل كبير على التعاون الدولي وسيلة لمعالجة التحديات المشتركة في الفضاء الإلكتروني، وتوكد الاستراتيجية على أهمية حماية الحريات المدنية والقيم الديمقراطية في الفضاء الإلكتروني، وتقدم الاستراتيجية خطة طموحة للاستثمار في البحث والتطوير في مجال الأمن السيبراني (Montasari:2023:15) . بشكل عام، تُقدم رؤية

المملكة المتحدة للعصر الرقمي رؤية متوازنة ومتفائلة لمستقبل التكنولوجيا، تُدرك المملكة المتحدة التحديات، لكنها تؤمن أيضًا بإمكانيات التكنولوجيا الرقمية لتحقيق عالم أفضل.

وتهدف الاستراتيجية الوطنية للملكة المتحدة إلى تحقيق أربعة أهداف رئيسية(National cyber strategy UK:20022) هي على النحو الآتي:

- جعل المملكة المتحدة أكثر أمانًا ومرونة وذلك من خلال التصدي للتهديدات والمخاطر المتطورة بشكل أفضل، واستخدام القدرات السيبرانية لحماية المواطنين.
- خلق اقتصاد رقمي مبتكر ومزدهر، وذلك من خلال توفير فرص متساوية للجميع في جميع أنحاء البلاد.
- أن تصبح قوة عظمى في مجال العلوم والتكنولوجيا، وذلك من خلال الاستفادة من التقنيات التحويلية لخلق مجتمع أكثر خضرة وصحة.
- أن تصبح شريكًا عالميًا أكثر تأثيرًا، وذلك من خلال المساعدة في تشكيل مستقبل الإنترنت المفتوح والمستقر.

لتحقيق هذه الأهداف، حددت الاستراتيجية خمس ركائز رئيسية تُشكل أساسًا استراتيجيًا قويًا لتعزيز الأمن السيبراني للمملكة المتحدة خلال العقد القادم من خلال التركيز على هذه المجالات الرئيسية، يمكن للمملكة المتحدة أن تبني مملكة رقمية أكثر أمانًا وازدهارًا، وتعزز مكانتها وتكون رائدة عالمية في مجال الأمن السيبراني (Pleta and Latvys:2020:806) تتمثل هذه الركائز في:

1. تعزيز النظام السيبراني للمملكة المتحدة: وذلك من خلال الاستثمار في الأشخاص والمهارات وتعزيز الشراكة بين الحكومة والأوساط الأكاديمية والصناعية.
2. بناء المملكة المتحدة الرقمية المرنة والمزدهرة وذلك من خلال تقليل المخاطر السيبرانية، وتحسين الأمن عبر الإنترنت للمواطنين.
3. أخذ زمام المبادرة في التقنيات الحيوية للقوة السيبرانية، وذلك من خلال بناء قدرات صناعية وتطوير أطر لتأمين التقنيات المستقبلية.
4. تعزيز القيادة العالمية للمملكة المتحدة وتأثيرها من خلال العمل مع الشركاء الدوليين لتطوير نظام دولي أكثر أمانًا وازدهارًا وانفتاحًا.
5. اكتشاف الخصوم أو ردعهم من خلال تحسين استخدام أدوات المملكة المتحدة السيبرانية لتعزيز الأمن الوطني.

5.5.4.2.استراتيجية موريشيوس للأمن السيبراني :

اعتمدت دولة موريشيوس استراتيجية وطنية للأمن السيبراني خلال 2007م – 2011م، كإصدار أول، وثم الإصدار الثاني خلال 2011-2014م، واخر نسخة كانت خلال 2014-2019م، تسعى استراتيجية موريشيوس للأمن السيبراني إلى تحقيق الأهداف التالية: (National cyber security strategy Republic of mauritius:2014).

- تأمين الفضاء الإلكتروني لدى الدولة، وإنشاء خط دفاع أمامي ضد الجرائم الالكترونية
- تعزيز قدرة موريشيوس على الصمود في مواجهة التهديدات السيبرانية والقدرة على الدفاع ضد مجموعة كاملة من التهديدات.
- تطوير نموذج تعاوني فعال بين السلطات ومجتمع الأعمال، بهدف تعزيز الأمن السيبراني الوطني.
- تحسين الخبرة السيبرانية، والوعي الشامل بالأمن السيبراني للمجتمع على جميع المستويات.

وتعتبر استراتيجية الأمن السيبراني أمرًا حيويًا لحماية موريشيوس في العصر الرقمي من خلال اتخاذ إجراءات وقائية قوية، يمكن لموريشيوس حماية اقتصادها وبنيتها التحتية وأمنها القومي Familoni and . (Shoetan:2024:855).

وبهاذ يمكننا القول بأن استراتيجيات الأمن السيبراني للدول المذكورة أعلاه تتباين فيما بينها، إلا أنها تتفق في جوهرها على أهمية بناء قدرات وطنية قوية، وتبني شراكات دولية، والاستثمار في التكنولوجيا الحديثة ودعم البحث والتطوير والتعاون بين القطاع العام والخاص وتعزيز البنية التحتية وتبني تشريعات حديثة لحماية البيانات والخصوصية، يمكن لليبيا الاستفادة من هذه التجارب من خلال تكييفها مع سياقها المحلي، مع التركيز على بناء نظام بيئي رقمي آمن ومرن من خلال تبني نهج شامل ومتكامل للأمن السيبراني، يمكن لليبيا حماية بنيتها التحتية الحيوية، وتعزيز مكانتها في الاقتصاد الرقمي العالمي.

نخلص إلى أنَّ الأمن السيبراني يزداد أهمية في حماية الأمن القومي، من خلال حماية الأنظمة والشبكات والبيانات، من التهديدات السيبرانية، كما تزداد العلاقة بين الأمن السيبراني والأمن القومي بتوسع ساحات الفضاء الإلكتروني، وهو ما عزز الجهود الدولية الطامحة إلى تقنين وتنظيم أساليب وطرائق العمل في هذا الفضاء ، التي تمثلت في الاتفاقيات والمؤتمرات الدولية، ويزداد دور المنظمات والشركات في وضع اسس لاستراتيجية الأمن السيبراني للدول، وبالتالي الوضع الراهن في ليبيا، يتطلب فهمًا شاملاً للتحديات والفرص التي تواجهها هذه البلاد في هذا المجال الحيوي وهو ما سوف يتم تناوله في الفصل التالي.

الفصل الثالث

تداعيات التهديدات السيبرانية للأمن القومي الليبي وطرق التصدي

1.3. تمـــهيد

لا شك أن التهديدات السيبرانية أصبحت من أبرز التحديات التي تواجه الدول، حيث تتخطى تأثيراتها الحدود الجغرافية، لتشكل تهديدًا مباشرًا للأمن القومي، وليبيا كغيرها من الدول، تجد نفسها عرضة لهذه التهديدات التي تستهدف بنيتها التحتية الرقمية ومؤسساتها الحيوية وتتنوع هذه التهديدات بين الهجمات الإلكترونية التي تهدف إلى سرقة المعلومات والتجسس الإلكتروني، وصولًا إلى الهجمات التخريبية التي تستهدف تعطيل الخدمات الحيوية.

يستعرض هذا الفصل ثلاثة مباحث رئيسية، في المبحث الأول، سيتم التركيز على تحليل وتحديد التهديدات السيبرانية التي تستهدف ليبيا، و سيتم اجراء دراسة للأنماط الهجومية المستخدمة، وللجهات التي تقف وراء هذه التهديدات، بهدف بناء فهم عميق حول السياق السيبراني الذي تنشأ فيه هذه التهديدات، أما المبحث الثاني يسلط الضوء على الجهود التي بذلتها الجهات الليبية في مراجعة وتقييم التهديدات السيبرانية الموجهة للبلاد من خلال استعراض التدابير والاجراءات المتخذة في هذا المجال.

أما المبحث الثالث، فيدور حول مقترح لتطوير استراتيجية وطنية للأمن السيبراني في ليبيا وسيكون هذا المبحث أساسيًا في وضع خطة شاملة تهدف لتوجيه الجهود نحو تحقيق الأهداف الاستراتيجية المحددة بشكل واضح ومنظم، وضمان الحماية الكاملة للأنظمة الحيوية والبنية التحتية الحيوية للدولة، وسيتم استعراض الخبرات والدروس المستفادة من البلدان الأخرى التي نجحت في بناء استراتيجيات فعالة للأمن السيبراني، مما يسهم في تحديد التوجهات التي يجب أخذها في الاعتبار أثناء تصميم الإطار الاستراتيجي المحلي.

2.3. تحليل التهديدات السيبرانية التي تواجه ليبيا

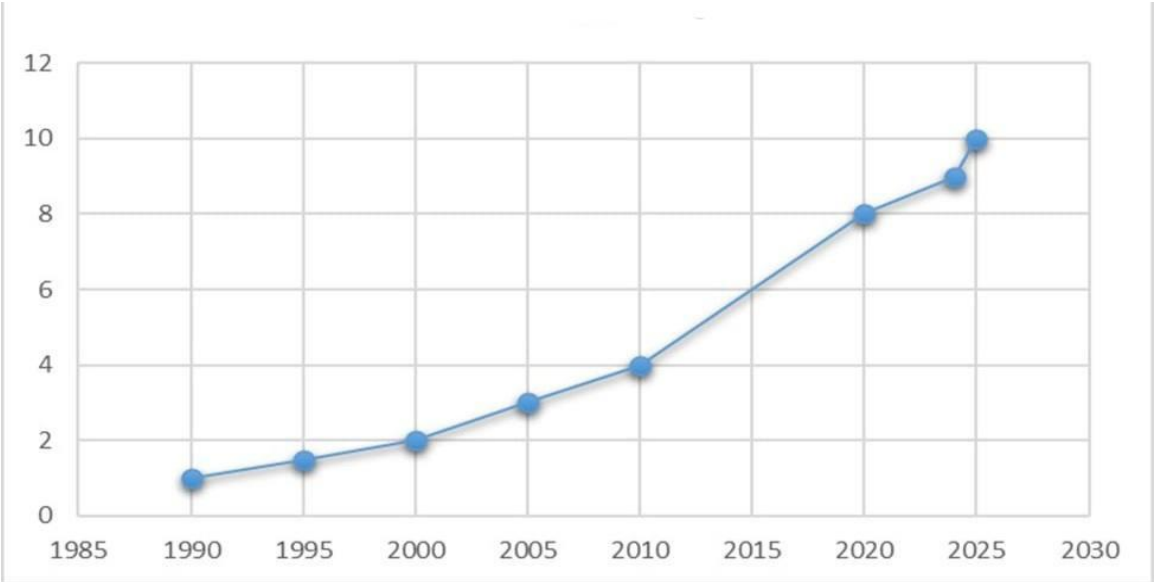
تُعد التهديدات السيبرانية من القضايا الملحة التي تواجه الدول في العصر الرقمي، حيث أصبح الفضاء الإلكتروني ساحة جديدة للصراعات والتحديات، وفي هذا السياق، تبرز ليبيا دولة ذات أهمية استراتيجية، لا سيما في ظل التغيرات السياسية والاجتماعية التي شهدتها على مر السنوات الأخيرة منذ بداية أحداث عام 2011م، ومع تطور الإنترنت في البلاد، ظهرت مجموعة من التهديدات السيبرانية التي تستهدف مؤسسات الدولة والمواطنين على حد سواء، تجدر الإشارة إلى أن هذه الدراسة لا تهدف إلى حصر جميع التهديدات السيبرانية التي تواجه ليبيا، وذلك لعدة أسباب:

أولاً. تفتقر الحكومة الليبية إلى نشر إحصائيات موثوقة ومعلنة حول هذه التهديدات، مما يجعل من الصعب الحصول على صورة شاملة ودقيقة عن الوضع الراهن.

ثانياً. فإن المعلومات المتاحة مستمدة بشكل رئيسي من مقابلات شخصية مع خبراء في مجال الأمن السيبراني، بالإضافة إلى إحصائيات ومراجع من شركات عالمية، وبعض الدراسات المنشورة والتي تظل محدودة نوعًا ما.

1.2.3.تطور الإنترنت في ليبيا :

في أوائل التسعينيات، من القرن الماضي، بدأت ليبيا في استخدام الإنترنت بشكل محدود جدًا كما هو موضح في الشكل رقم (9)، كان استخدامه مقتصرًا على الجهات الحكومية والمؤسسات الأكاديمية الكبرى، في هذه الفترة لم يكن هناك وصول واسع النطاق للإنترنت للأفراد، وكان الهدف الرئيسي من الاتصال مرتبطًا بالتواصل بين الجهات الرسمية وبعض الجامعات، رغم ذلك، شهدت هذه الفترة بداية الوعي بأهمية الإنترنت أداة للاتصال وتبادل المعلومات (الرمحي: 2022).



الشكل رقم (9) يوضح تطور الإنترنت في ليبيا،المصدر: من إعداد الباحثة.

وفي عام 1995م، سجلت ليبيا أدنى معدل لانتشار تقنية المعلومات في القطاع غير الحكومي في شمال أفريقيا، وكان ذلك نتيجة للعقوبات التجارية التي فرضتها الأمم المتحدة على ليبيا، عام 1992م، فقد كانت البيانات في تلك الفترة محدودة (Ali and others:2011:2) وفي نهاية عام 1997م كان تعداد مستخدمي الانترنت في ليبيا لا يتجاوز المئة نسمة أغلبهم في المؤسسات الاقتصادية والسياسية في الدولة (أكاكوس للدراسات الاستراتيجية:2004: 4-5). وعلى الرغم من البداية البطيئة لليبيا، إلا أن السنوات التالية عكست زيادة كبيرة في الوصول إلى الإنترنت، وأفادت المنظمة العربية لحقوق الإنسان أن عدد مستخدمي الإنترنت في ليبيا خلال نهاية التسعينات حتى بداية الالفية قد ارتفع قليلاً (الشبكة العربية لحقوق الإنسان: 2004).

وفي عام 2001م، وصل عدد مستخدمي الانترنت إلى 300 ألف، بمجرد توسيع الخدمة للجمهور، ثم تضاعف العدد بحلول منتصف عام 2003م، ليصل إلى نحو 850 ألف (Ali and others:2011:3). وكان الدافع وراء انتشار الانترنت هو القرار السياسي للدولة الذي اتخذه الرئيس الراحل معمر القذافي، في خطابه في عيد ثورة الفاتح عام 2000م، في مدينة بنغازي، عندما أقترح الانترنت سوق عمل للشباب الليبي (أكاكوس للدراسات الاستراتيجية:2004: 6).

بحلول عام 2004م، زاد عدد الليبيين الذين لديهم إمكانية الوصول إلى الإنترنت بشكل كبير، وأصبح الاتصال بالإنترنت متاحًا لأول مرة للمواطنين الليبيين، بشكل أكثر مرونة (Reilton:2013: 20). وفي 2005م، بدأ

الإنترنت يكتسب حضورًا أوسع في ليبيا، وإن كان بوتيرة بطيئة شهدت هذه المرحلة تأسيس الشركة الليبية للبريد والاتصالات وتقنية المعلومات (القابضة) لتطوير قطاع الاتصالات وتوسيع نطاق استخدام الإنترنت، وتم إنشاء بوابات إلكترونية حكومية محدودة لخدمة القطاعات الحيوية، مثل التعليم والصحة ورغم ذلك، ظل الوصول إلى الإنترنت مكلفًا بالنسبة للأفراد، مما حدّ من انتشاره على نطاق واسع (طالة: 2020). وفي عام 2005م، وصل عدد مستخدمي الإنترنت بسرعة إلى مليون مستخدم، وهي زيادة كبيرة مقارنة بعام 1998م، حيث لم يتمكن سوى عدد قليل من الأفراد من الوصول إلى الإنترنت (Ali and others:2011:3). ومع تطوير قدرة شبكة الاتصالات على استيعاب الاتصالات المتطورة وحركة تقنية المعلومات انتشر الانترنت انتشارا واسعا في ليبيا ليصل تعداد الاستخدام حسب بعض الآراء إلى حوالي سدس عدد السكان (أكاكوس للدراسات الاستراتيجية :2004: 4-5).

وبدأت خدمات الإنترنت تتوسع بشكل ملحوظ، ففي عام 2006م، بدأ توفير الإنترنت عبر تقنيةADSL ، مما أتاح للأفراد الحصول على خدمات إنترنت أسرع وأكثر استقرارًا، وفي عام 2008م، دخلت ليبيا عصر الإنترنت اللاسلكي، مع إطلاق خدمات WiMax ، التي سهلت الوصول إلى الإنترنت في المناطق النائية، وتم إنشاء العديد من المقاهي الإلكترونية(Cyber Cafes) والتي أصبحت مركزًا رئيسيًا للوصول إلى الإنترنت للشباب والمجتمع بشكل عام (طالة: 2020). في هذه الفترة، ازداد الوعي باستخدام الإنترنت، وظهرت مواقع إخبارية ومنتديات محلية لتعزيز التواصل ونقل المعلومات (باي، 2023).

بحلول 2009 – 2010م، كان هناك أكثر من 350 ألف مستخدم للإنترنت، ووصلت نسبته إلى 5.5% من إجمالي السكان، وارتفع العدد من خلال زيادة عدد مستخدمي وسائل التواصل الاجتماعي في بداية أحداث 2011م، وبلغ معدل انتشار الفيسبوك في ليبيا 2.8%، وبالمثل، وصل موقع تويتر إلى أقل من 1% من السكان الليبيين (Reilton:2013: 20) وحسب منصة سلايد شير الامريكية، وخلال العشر السنوات الماضية بعد 2011م، ارتفع عدد مستخدمي الانترنت من 877 الف مستخدم الى 3.7 مليون مستخدم بما يمثل 49.6% من عدد السكان (Slideshare:2020).

في عام 2022م، بلغ مستخدمو الانترنت حوالي 3.47 مليون شخصا، وخلال هذه السنة بلغ معدل انتشاره 49.6% من اجمالي السكان، وتشير تحليلات شركة ديتربرتل إلى أن عدد مستخدمو الانترنت زاد بمقدار 320 الف بين عامي 2021 و 2022م، وخلال هذه السنة بلغ مستخدمي وسائل التواصل الاجتماعي ما يعادل 91.4 في المئة من اجمال السكان وبعد سنة زاد عدد مستخدمي الانترنت، وسجل عام 2023م، وصل العدد إلى 3.14% بمعدل انتشار 45.9%. وبلغ عدد مستخدمي وسائل التواصل الاجتماعي 5.65% من إجمالي السكان، وبلغ عدد مستخدمي الانترنت في ليبيا 6.13 مليون مستخدم للإنترنت مع بداية سنة 2024م، كما بلغ مستخدمو وسائل التواصل الاجتماعي في نفس العام، ما يعادل 85.2% من إجمالي السكان (Datareportal:2024).

بمجرد الانفجار السريع لاستخدام الإنترنت في ليبيا على مدى السنوات الماضية، انتشر تأثير وسائل التواصل الاجتماعي بسرعة أكبر كما يتصور، مالكوم جلادويل (Malcolm Gladwell)، ليصبح أداة للتغيير

السياسي(Ali and others:2011:4). أصبحت سياسات الحكومة الليبية آنذاك تركز على رصد أدوات الحماية لمعالجة الكابوس الرقمي، بمراقبة الانترنت ومواقع التواصل والمراسلات الالكترونية، حيث كان الهدف تأمين دوائر المعلومات والحد من الانتقادات (حامد: 2023). كما أنَّ الحكومة الليبية سيطرت على البنية التحتية للاتصالات، وهو ما مكنه من التحكم فيه، لكن هذه السياسة تركزت على الرقابة لضمان الأمن مع تضمن أي تدابير وقائية لمواجهة الهجمات الالكترونية القادمة من الخارج (طالة: 2020).

وقد تم انشاء الجيش الليبي الإلكتروني، في مجموعة صغيرة من PGEAs الذين تم تجميعهم قبل أحداث 2011، على الرغم من أن التاريخ الدقيق لإنشائه غير مؤكد، كما ورد أن بعض هؤلاء الأفراد كانوا نشطين في تشجيع المعتصم معمر القذافي بصفته مستشار للأمن الوطني أنداك في سياق الجهود المبذولة للرد على العمليات الإعلامية التي قامت بها الجماعات المنفية، وبعد ذلك تطورت هذه المجموعة من PGEAsإلى جيش ليبي إلكتروني أكثر رسمية، وذلك بناءً على طلب محمد القذافي المدير العام لشركة البريد والاتصالات وتم شراء المعدات، وتخصيص المباني، واكتسبت ليبيا هيكلًا سيبرانيا رسميًا، على الرغم من أن التسلسل الهرمي التنظيمي الدقيق لا يزال غير واضح(Reilton:2013:130-131).

2.2.3.بداية التهديدات السيبرانية بعد أحداث عام 2011 :

بعد انهيار الدولة الليبية، بدأت ليبيا تتعرض للتهديدات سيبرانية مع اشتداد الاحداث الأمنية والسياسية، مما ادى إلى ظهور تحدي جديد واجه الأمن القومي الليبي (طالة: 2020). كانت ليبيا في حالة من الفوضى السياسية والأمنية، وواجهت حملات سيبرانية مكثفة ومتعددة المصادر، التي سعت جميعها لاستغلال الفوضى في البلاد، لأغراض سياسية واقتصادية، وحتى تدميرية (Deszca and others:2019) .

خلال أحداث 2011م، لعب الإنترنت دورًا محوريًا في تنسيق الاحتجاجات ونقل الأخبار، وتم إنشاء صفحات على مواقع التواصل الاجتماعي مثل، تطبيق فيسبوك وتويتر لتنظيم المظاهرات وأظهرت هذه الفترة أهمية الإنترنت وسيلة للتعبير الحر، ونقل الأخبار في ظل غياب وسائل الإعلام التقليدية المستقلة (باي: 2023). استخدمت القوات غير الموالية للحكومة الليبية، الإنترنت على نطاق واسع، بما في ذلك المعارك، وتحديد الأهداف لحلف شمال الأطلسي، وتنسيق الخدمات اللوجستية واستخدم الليبيون أدوات التواصل لبث تدفق متزايد التعقيد من الصور والأخبار والمعلومات إلى الجمهور عبر الإنترنت، وتم تضخيم تأثير هذه الأنشطة من خلال اعتماد وسائل الإعلام التقليدية المكثف على المصادر عبر الإنترنت (Reilton:2013: 17).

بعد ذلك شهدت ليبيا تحولًا كبيرًا في قطاع الإنترنت من بداية بسيطة ومحدودة إلى أداة حيوية تُستخدم في جميع جوانب الحياة رغم التقدم الملحوظ في بعض الفترات، ومع ذلك فما تزال ليبيا بحاجة إلى تعزيز البنية التحتية الرقمية وتطوير سياسات فعالة لدعم الاستخدام الآمن والشامل للإنترنت (رجب: 2017). كان الدور المركزي للإنترنت في أحداث عام 2011م، هو أنَّها ربطت الليبيين أفراد ومجموعات، ليس فقط بالويب، ولكن أيضًا بالشبكات العابرة للحدود الوطنية، لليبيين المغتربين غير الواليين لنظام الرئيس معمر القدافي ووفرت العمود الفقري الرئيسي للأحداث، حيث قامت بتنسيق كل شيء بدءًا من المساعدات الخارجية حتى

الأسلحة (Reilton:2013: 18). وهكذا فقد لعب الإنترنت دورا رئيسيا في انتصار الجماعات غير الموالية لنظام القدافي، وساهمت في تقدم قواتهم، وفي سقوط النظام، وفي تحول تاريخي هائل في ليبيا.

وقد كشف الانقلاب الرقمي الذي نتج عنه تغييرات جذرية عن بداية تهديدات سيبرانية موجهة ضد ليبيا، ورغم عدم إصدار الحكومة الليبية تقارير رسمية منشورة يمكن الاستعانة بها في هذه الدراسة، الا أننا استطعنا، من خلال الاستعانة بالشركات العالمية، والدراسات الأجنبية والعربية، بالإضافة إلى المقابلات الشخصية مع مدراء أمن المعلومات والأمن السيبراني في المؤسسات الحكومية والخاصة، للوصول إلى معلومات ملموسة تسلط الضوء على طبيعة الوضع السيبراني في ليبيا، وفهم التهديدات السيبرانية التي تواجه البلاد.

فليبيا، شأنها شأن، أية دولة في هذا العالم، تتعرض لتهديدات مستمرة، وأحيانًا تكون ساحقة، يستخدم فيها المهاجمون مجموعة واسعة من ناقلات البرامج الخبيثة، لاختراق الوكالات الحكومية والمنظمات الخاصة، وكذلك الشخصيات المؤثرة والسياسية، ومع تصاعد التهديدات السيبرانية في سياق الأحداث السياسية بعد عام 2011م، أصبحت ليبيا تتعرض لتهديدات، تستهدف التخريب نتيجة لأحداث الفوضى السياسية والأمنية، تركزت هذه التهديدات في مجالات عديدة مثل، المصارف، والمؤسسات السيادية والنفطية، وشركات الاتصالات وغيرها(Railton: 2013) . إنَّ ما يميز التدخل السيبراني الخارجي الموجه ضد ليبيا، أنَّه تم تنفيذه، برعاية دول ومجموعات تسعى إلى تغيير التوازن السياسي في البلاد، لصالح مصالحها، وقد كانت هذه التهديدات معقدة ومتطورة للغاية، استخدمت فيها تقنيات حديثة؛ مثل الهجمات ضد الشبكات والأنظمة الحكومية للحصول على معلومات مصنفة، أو تعطيل الخدمات داخل المؤسسات العامة (شعيتير:2023). ففي عام 2020م، تم تسجيل 43 حادثة اختراق سيبراني لمواقع في ليبيا، منها 7 مواقع حكومية سيادي،ة تضمنت هذه الحوادث تغيير صفحات رئيسية، أو تسريب بيانات حساسة. (الرمحي:2022).

كما استغل المهاجمون الوضع السياسي والأمني الهش، في ليبيا، لتنفيذ تهديدات سيبرانية بهدف نشر الفوضى، وتجنيد الأفراد عبر الإنترنت، والتأثير على الرأي العام الليبي. فعلى سبيل المثال، استخدمت هذه الجماعات وسائل التواصل الاجتماعي لنشر الدعاية واستهداف الشباب الليبي، وأدت إلى تعزيز حالة عدم الاستقرار وزيادة التهديدات الأمنية (Railton:2013). كما تعاني البنية التحتية الرقمية في ليبيا، من وجود خدمات وقواعد بيانات مكشوفة بشكل علني على الإنترنت، ما يجعلها عرضة لتهديدات سيبرانية خطيرة (باي: 2023). وتأتي التحديات المرتبطة بسهولة الوصول للبيانات، وبوجود خدمات مكشوفة، يعني أن أي مهاجم يمكنه استغلالها للحصول على بيانات حساسة، دون الحاجة إلى تقنيات معقدة، لتنفيذ هجمات حجب الخدمة، وتعطيل الأنظمة المستهدفة (Deszca and others:2019). هذه الخدمات والقواعد المكشوفة، تعرض المؤسسات لخطر الهجوم وسرقة البيانات الحساسة، مثل معلومات العملاء أو البيانات المالية، مما يضر بسمعة المؤسسات وأمنها التشغيلي(سمير: 2023).

أشار رئيس الهيئة العامة لأمن وسلامة المعلومات أثناء مقابلتي معه، إلى أن البنية التحتية الرقمية في ليبيا، تُعتبر بيئة ناشئة مقارنةً بالدول الأخرى، وقد شهدت هذه البنية تحولًا ملحوظًا خلال فترة انتشار فايروس

كوفيد 19، حيث زاد الطلب على تقديم الخدمات إلكترونيًا في الربع الأول من عام 2020م، وأوضح أن هذا التحول الرقمي كان مدفوعًا بضرورة الاستجابة لتحديات الجائحة، مما دفع العديد من المؤسسات إلى التركيز على تعزيز قدراتها الرقمية، ومع ذلك، فإن هذا التوجه أدى إلى تسارع وتيرة التهديدات السيبرانية، نتيجة للزيادة الكبيرة في الاعتماد على الخدمات الإلكترونية(رئيس الهيئة العامة لأمن وسلامة المعلومات، مقابلة خاصة:2024).

على الصعيد التقني، يُعتبر ضعف البنية التحتية أحد التحديات الرئيسية التي تواجه جهود تعزيز الأمن السيبراني في ليبيا، حيث تعاني شبكات الاتصالات والأنظمة التقنية من نقص واضح في الحماية والتحديث المستمر، مما يجعلها عرضة للاختراقات والاستغلال من قبل القراصنة، بالإضافة إلى ذلك، يُعزى غياب مراكز متخصصة لرصد الشبكات السيبرانية (SOC) في المؤسسات الحكومية إلى صعوبة رصد الهجمات الإلكترونية، والاستجابة لها بشكل فوري، (رجب: 2017). وتشمل الاختراقات مجموعة متنوعة من الأهداف، مثل سرقة البيانات، واختراق المواقع الحكومية، وتنفيذ هجمات حجب الخدمة الموزعة (DDoS)، التي تهدف إلى تعطيل الخدمات الحيوية، في ظل غياب وسائل حماية فعالة، وتواجه المؤسسات الليبية تحديات كبيرة في التعافي من هذه الهجمات، مما يؤدي إلى تكبد خسائر مادية ومعنوية جسيمة (القطروني: 2018). يشير تقرير لشركة مايكروسوفت لسنة 2015م، أن ليبيا كانت تعاني من أعلى نسبة من أجهزة الكمبيوتر غير المحمية، مما يعكس ضعف مستوى الأمان لدى المستخدمين والمؤسسات، هذا الافتقار إلى الحماية يزيد من فرص تعرض الأنظمة للهجمات السيبرانية، مما يجعلها أهدافًا سهلة للمهاجمين (Microsoft 2016): ويشير تقرير لشركة كاسبرسكي لاب، الذي يسلط الضوء على الهجمات الضارة، إلى أن ليبيا احتلت المركز الثالث عالميًا في نسبة المستخدمين الذين تعرضوا لهجمات حصان طروادة، وتعتبر هجمات حصان طروادة من بين أخطر أنواع البرمجيات الخبيثة (Kaspersky : 2017). ولذلك فقد تم تصنيف ليبيا كواحدة من أهم عشرة مصادر لمضيفي التصيد الاحتيالي وخوادم السيطرة والتحكم في إفريقيا، خلال سنة 2016م، وقد أشار قرصان ينتمي إلى مجموعة تُعرف باسم "فراشة الربيع" إلى أن مجموعته كانت قادرة، في فترة زمنية قصيرة، على السيطرة على أكثر من 99% من المواقع الرسمية الحكومية. بالإضافة إلى ذلك، أعلن القراصنة أنهم تمكنوا من الوصول إلى أنظمة مصرف ليبيا المركزي والسجل المدني، مما أثر بشكل كبير على الخدمات اليومية المقدمة للمواطنين في هذه المؤسسات (observer Libya:2016).

ووفقًا لشركة كاسبرسكي تشير الإحصاءات المتعلقة بليبيا في الربع الثالث من سنة 2018م، إلى أن حوالي 0.04٪ من مستخدمي كاسبرسكي في ليبيا كانوا ضحية لهجمات أحصنة طروادة المستهدفة لخدمات الهواتف الذكية العاملة بنظام الأندرويد. كما أظهرت البيانات أن 0.11٪ من المستخدمين تعرضوا لهجمات فيروسات الفدية، و1.2٪ واجهوا هجمات من قبل أحصنة طروادة وبرمجيات خبيثة أخرى تستهدف هذه الهجمات بشكل خاص المؤسسات المصرفية ونقاط البيع، علاوة على ذلك، تم تسجيل أنَّ 20.3٪ من المستخدمين تعرضوا لهجمات متنوعة على الويب، بينما اكتشف 38.6٪ منهم وجود برمجيات خبيثة على أجهزتهم بعد

تفعيل أنظمة الحماية من الفيروسات، هذه الإحصاءات تسلط الضوء على الحاجة الملحة لتعزيز الأمن السيبراني في ليبيا لمواجهة التهديدات المتزايدة وحماية المعلومات الحساسة (Kaspersky:2024).

وفي عام 2018م، واجهت المؤسسات الليبية للنفط عدة هجمات إلكترونية متنوعة، بما في ذلك البرمجيات الخبيثة، والتصيد، والبريد المزعج، وهجمات تخمين كلمات السر، وغيرها من الهجمات (شركة الجذور الليبية، 2018: 2). هذا وتحتل ليبيا المركز 43 عالميا، مصدر لشبكات الاختراق (Botnets)، حيث يتراوح عدد الأجهزة المخترقة في البلاد بين 9367 عنوان شبكة يتم التحكم بها عن بُعد بشكل أسبوعي عبر مراكز التحكم (شركة الجذور الليبية: 2020: 12). كما يتم تسجيل تسريب لـ 15،700 عنوان بريد إلكتروني يحتوي على بيانات حساسة، مثل كلمات المرور وأرقام الهواتف (الرمحي: 2022). وهناك سيناريو آخر محتمل، يتمثل في استخدام العديد من المؤسسات والموظفين في ليبيا لخدمات البريد الإلكتروني العامة مثل Yahoo وGmail لأغراض شخصية وعملية، مما يؤدي إلى خلط المستندات والبيانات الخاصة مع بيانات العمل وفي نفس الوقت، يقوم المستخدمون، أو الموظفون بالتسجيل في عدة منتديات ومواقع باستخدام نفس البريد الإلكتروني، وأحيانًا كلمة المرور نفسها، وعند اختراق أحد هذه المواقع، أو المنتديات، يتم نشر قواعد البيانات الخاصة بها، مما يتيح الوصول إلى المؤسسات التي يعمل بها هؤلاء المستخدمون من خلال البيانات المسربة (شركة الجذور الليبية :8:2020).

وأظهرت نتائج المقابلات التي أجرتها الباحثة مع عينة الدراسة، أن الوضع الراهن للتهديدات السيبرانية في ليبيا يُعتبر معقدًا وخطيرًا، نتيجة لتفاعل مجموعة من العوامل؛ منها عدم الاستقرار الأمني، والبيئة السياسية المضطربة، والقدرات التقنية المحدودة، وتتضمن هذه التهديدات مجموعة متنوعة مثل الهجمات على البنية التحتية الحيوية، وسرقة البيانات الشخصية والحساسة، والهجمات المستهدفة ضد المؤسسات الحكومية والخاصة، وتشير المعطيات إلى أن هذه التهديدات تتكرر بشكل يومي، حيث تفتقر الكثير منها إلى الوعي الكافي بالمخاطر والتهديدات المحتملة، هذا النقص في المعرفة والاستعداد، يؤدي إلى ردود فعل بطيئة وغير فعالة عند حدوث الهجمات، كما أن العديد من الهجمات التي تُنفذ ضد هذه المؤسسات لا يتم الإبلاغ عنها، مما يساهم في زيادة المخاطر، حيث تظل الأضرار غير مرئية وغير موثقة، تعكس هذه الحالة من التأخر في الاستجابة للتهديدات السيبرانية، نقصًا في البنية التحتية الأمنية والتخطيط الاستراتيجي لمواجهة المخاطر، عندما تتعامل المؤسسات مع الحوادث بعد وقوعها، فإنها غالبًا ما تفقد القدرة على تقليل الأضرار المحتملة، مما يؤدي إلى تبعات مالية وتشغيلية سلبية، فليبيا تعاني من حالة حرجة من عدم الجاهزية لمواجهة المخاطر والهجمات السيبرانية التي تستهدفها.

تُظهر الإحصائيات المتعلقة بالتهديدات السيبرانية في ليبيا أن الوضع الأمني الرقمي يتطلب اهتمامًا كبيرًا، وفقًا لكاسبرسكي، تعرض حوالي 10٪ من مستخدميها في ليبيا لهجمات تصيد إلكتروني، حيث تم انتحال صفة مؤسسات وشركات رسمية لاستهداف عملائها عبر روابط ومواقع مزيفة، هذه الروابط تطلب من العملاء إدخال معلوماتهم الشخصية وبياناتهم الحساسة، مثل كلمات المرور، تحت ذريعة الفوز بجوائز وهمية، مما يؤدي إلى سرقة تلك المعلومات. (شركة الجذور الليبية: 9:2018). تشير البيانات من

(Kaspersky Securelist)إلى انتشار ملحوظ للبرمجيات الخبيثة في ليبيا، مما يشكل تهديدًا كبيرًا للبنية التحتية الرقمية. كما تعرضت مؤسسات حكومية وخاصة لهجمات سيبرانية موجهة (Targeted Attacks) تهدف إلى سرقة المعلومات الحساسة، أو تعطيل الخدمات، وهو ما يؤكد على الحاجة الملحة لتعزيز الدفاعات السيبرانية (الرمحي: 2022) بالإضافة إلى ذلك، تنتشر البرمجيات الإعلانية (Adware) التي تؤثر سلبًا على تجربة المستخدم وتعرض الأجهزة لمخاطر أمنية إضافية (شعيتير: 2023).

وفي عام 2020م، شهدت ليبيا زيادة ملحوظة في عدد حالات الاختراق المعلنة، حيث تم تسجيل حوالي 43 حالة ادعاء اختراق وفقًا لموقع Zone-H، ما يثير الانتباه أن عددًا من هذه الاختراقات كان نتيجة لتهديدات داخلية، مما يشير إلى وجود مشاكل في الأمان الداخلي للمؤسسات من بين هذه الحالات، كانت هناك سبع اختراقات تستهدف مواقع حكومية، والتي قد تتراوح تأثيراتها بين مجرد تغيير الصفحة الرئيسية للموقع لإثبات عملية الاختراق، إلى تسريب بيانات حساسة أو الدخول غير المصرح به إلى الأنظمة (شركة الجذور الليبية: 2020 :4-12).

وفي نفس العام واجهت المؤسسات في ليبيا مجموعة من التهديدات السيبرانية، التي أثرت بشكل كبير على عملها وأمنها، ومن أبرز هذه الحوادث ما تعرضت له مؤسسة مصرفية وشركة اتصالات، لعملية اختراق استهدفت تطبيقات الهواتف المحمولة الخاصة بخدمات العملاء، وأيضا تم اختراق موقع تابع لوزارة سيادية، حيث تم تصنيفه كمصدر للرسائل المزعجة (Spam) وقد عكس هذا الاختراق التهديدات التي تواجه المواقع الحكومية وكيف يمكن أن تتعرض لهجمات ضارة، بالإضافة إلى ذلك، شهدت أربع مؤسسات مصرفية محاولات لاختلاس مبالغ مالية من موظف مخول داخل المؤسسة (شركة الجذور الليبية :2020 :12). وكشفت نتائج المقابلات التي أجرتها الباحثة عن مشهد معقد من التهديدات السيبرانية التي تستهدف ليبيا، حيث تتنوع الجهات الفاعلة التي تسعى لتحقيق أهداف مختلفة، ومن أبرز الجهات الفاعلة المحتملة، دول أجنبية وعربية مثل روسيا والصين، الولايات المتحدة ، إندونيسيا، مصر، الهند، بالإضافة إلى جماعات مسلحة وميليشيات محلية، تسعى للحصول على معلومات حساسة قد تساعدها على تعزيز نفوذها أو تقويض الحكومة المركزية وتمثل عصابات الإنترنت والمجموعات الإجرامية تهديدًا متزايدًا، حيث تسعى لتحقيق مكاسب مالية من خلال هجمات الفدية، أو سرقة البيانات، وتستخدم هذه الفواعل تقنيات متقدمة لاقتحام الأنظمة واستغلال الثغرات الأمنية لتحقيق أهدافها المالية.

بالنظر إلى الدوافع وراء التهديدات التي تواجه ليبيا، نجد أنها متنوعة وتشمل دوافع سياسية تسعى إلى تعطيل استقرار النظام، أو فرض تنازلات عليه، بالإضافة إلى دوافع اقتصادية تهدف للاستحواذ على الأموال، أو المعلومات السرية، ودوافع اجتماعية تهدف إلى خلق الفوضى، أو زعزعة الثقة بين الشعب ومؤسسات الدولة (طالة: 2020). ومن المهم أن ندرك أن بعض الهجمات قد تكون مُحركة بدوافع مالية، بينما قد تكون غيرها محركة برغبة في إثارة الفوضى، ويمكن أن تكون هناك دوافع أكثر سرية، ويمكن أن تشمل الجهات المُنفذة المحتملة مجموعات قرصنة، أو أفراد في منظمات إجرامية منظمة تسعى لتحقيق مكاسب عبر الإنترنت، أو قراصنة يُدعمون من قبل دولة، أو جواسيس صناعيين وغيرها (Ali and others:2011:48) .

وفي عام 2020م، تم الإبلاغ عن تسريب خطير لقواعد بيانات تتعلق بأحد المواقع التي كانت تقدم خدمات للمواطنين من خلال مؤسسة حكومية، يحتوي هذا التسريب على معلومات حساسة تشمل عناوين البريد الإلكتروني، كلمات المرور، أرقام الهواتف، وبيانات شخصية أخرى، يُظهر التسريب أعدادًا كبيرة ومتنوعة من عناوين البريد الإلكتروني، مما يزيد من خطر اختراق حسابات المستخدمين على منصات التواصل الاجتماعي وحسابات الشركات والمؤسسات، وبلغ إجمالي عدد عناوين البريد الإلكتروني المسربة 15،700 عنوان (شركة الجذور الليبية: 2020: 15).

وكشفت نتائج المقابلات التي أجرتها الباحثة، أنه في 2020م، تم توثيق هجوم سيبراني على شركة الاتصالات الليبية (LTT)، مما أدى إلى توقف خدمات الإنترنت في أجزاء متعددة من البلاد، بالإضافة إلى ذلك تم في يونيو 2023م، اختراق موقع وزارة الداخلية الليبية مما أدى إلى تسريب بيانات حساسة لموظفي الوزارة، وفي مارس 2024م، تعرضت شركة الكهرباء الليبية لهجوم سيبراني أدى إلى انقطاع التيار الكهربائي عن مناطق واسعة في طرابلس لمدة 12 ساعة.

تواجه ليبيا مجموعة متنوعة من التهديدات السيبرانية التي تؤثر بشكل كبير على بنيتها التحتية المعلوماتية تشمل هذه التهديدات هجمات على شبكات الاتصالات، وسرقة البيانات، والتجسس الإلكتروني، مما يسعى إلى تقويض القدرة السيادية للبلاد ومصالحها الحيوية (رجب: 2017). تزداد تعقيدات الأمن السيبراني بسبب الجرائم السيبرانية العابرة للحدود، حيث يمكن تنفيذ الهجمات من مواقع بعيدة باستخدام تقنيات متطورة يصعب تتبعها (القطروني: 2018). على سبيل المثال، تعرضت وزارة الحكم المحلي في ليبيا لهجوم فدية في عام 2022م، حيث أدى هذا الهجوم إلى تعطيل الأنظمة داخل الوزارة وتشفير بعض البيانات، مما أثر سلبًا على سير العمل والعمليات الإدارية (مدير التحول الرقمي بوزارة الحكم المحلي، مقابلة خاصة:2024).

تواجه وزارة الخارجية والتعاون الدولي، هي الأخرى تهديدات بشكل متكرر تستند بشكل كبير على أخطاء مستخدمين عاديين داخل المؤسسة؛ فبدلاً من هجمات من قراصنة (هاكرز)، تبرز حالات تصيد احتيالية عبر البريد الإلكتروني، تهدف إلى الوصول إلى أنظمة المعلومات وسرقة البيانات، بالإضافة إلى حالات ابتزاز وتشويه سمعة الأفراد داخل الوزارة، كما شملت التهديدات البارزة اختراقات لشخص ذو أهمية في الوزارة لم يدكر أسمة (مدير إدارة تقنية المعلومات بوزارة الخارجية والتعاون الدولي: مقابلة خاصة: 2024).

من أبرز الجرايم السيبرانية، التي تستهدف المواطنين في ليبيا، التي تم الإبلاغ عنها من معظم المدن، شملت جرائم الاحتيال، الابتزاز الإلكتروني، الاختراق، التشهير، المضايقة، قضايا انتحال الشخصية، طلب البيانات، تشويه السمعة، والنصب ووفقًا لإحصائيات السنوات 2022، 2023، والربع الأول من 2024، ارتفع عدد هذه الجرائم بشكل ملحوظ؛ ففي سنة 2022م، وصل العدد إلى 257 جريمة، بينما وصلت في 2023م، إلى 425 جريمة، وفي الربع الأول من 2024م، وصل عدد الجرائم التي تتعلق بقضايا التشهير إلى 139 جريمة، يُذكر أن هذه الأرقام تمثل الجرائم التي تم الإبلاغ عنها فقط. ويتبين أن الجهات المسؤولة عن هذه الجرائم عادة ما تكون داخلية من داخل الدولة الليبية، وتترتب عن هذه الجرائم تأثيرات اجتماعية

خطيرة تعتمد على نوع الجريمة المُرتكبة (مدير إدارة الجرائم الإلكترونية بجهاز المباحث الجنائية التابع لوزارة الداخلية، مقابلة خاصة: 2024).

في نوفمبر 2021م، تعرضت المفوضية العليا للانتخابات لهجوم من قبل قراصنة مجهولين استهدفوا الصفحة الرسمية الموثقة للمفوضية، ونشروا أخبارًا كاذبة، كان هذا الحادث الثاني من نوعه من حيث هجوم الفدية خلال 2022م، ولقد أثر بشكل كبير على سير عملية الانتخابات، تم استخدام هذا الهجوم لعرقلة والتشويش على سير العملية الانتخابية بشكل خاص، وقد تم التعامل مع هذا الهجوم بفعالية وسرعة، وتم حل المشكلة دون وقوع أية خسائر، وكان واضحا أنَّ الهدف الرئيسي من هذه الهجمات كان الاستفزاز والتشويش على العمليات في مفوضية الانتخابات، بهدف التأثير على سير العمل وزرع الشك والريبة في أعمالها (مدير إدارة نظم المعلومات بالمفوضية الوطنية العليا للانتخابات، مقابلة خاصة: 2024). كما تعرضت احدى المؤسسات في ليبيا لهجوم ادى الى خسائر تقدر بملايين الدنانير، والسبب يعود عدم وجود خطط لإدارة السجلات أو التعافي من الكوارث في هذه المؤسسة (Ben Nzsir:2022:164).

ويواجه القطاع المصرفي في ليبيا، كما هو الحال في باقي دول العالم، تهديدات سيبرانية متزايدة، نظرًا لأهميته كمزود للخدمات المالية الأساسية للاقتصاد، ونظرًا لكون ليبيا من الدول النامية، تواجه تحديات في التكنولوجيا مقارنة بالدول المتقدمة، وقد أشار مدير إدارة تقنية المعلومات في مصرف ليبيا المركزي إلى أن أحد أبرز التهديدات التي واجهت المصرف عام 2014م، هو الهجوم الداخلي الذي استهدف نظام 5000 دولار، حيث كان المهاجم يتلاعب بقيمة المعاملات المالية، وقد تم كشفه وتحويله إلى الجهات القضائية. كما تعرض المصرف المركزي لتهديد سيبراني بنهاية ديسمبر 2022م، لهجوم حجب الخدمة DDOS لعدة أيام، وأشار المدير إلى أن التهديدات السيبرانية لم تقتصر على المصرف المركزي فقط، بل طالت المؤسسات الحكومية الأخرى، وبعض شركات الاتصالات الليبية، وقال: إنَّ المصرف تعرض للعديد من الهجمات مثل، احصنة طرواده والديدان والهندسة الاجتماعية والتصيد الاحتيالي، وتمت هذه الهجمات نتيجة لعدم وجود أجهزة حماية كافية، نتيجة للتأثير السلبي لهجمات سنة 2022م، وقد تم بشراء أنظمة حماية جديدة لتعزيز الأمن السيبراني داخل المصرف (مدير إدارة تقنية المعلومات في مصرف ليبيا المركزي، مقابلة خاصة:2024).

وتعرض المصرف المركزي لهجوم سيبراني حجب الخدمة آخر في عام 2023م، استهدفت منصة حجز العملة الأجنبية للأفراد بهجوم يهدف للوصول للمنظومة، وأعلن المصرف أن المنصة تعمل بشكل طبيعي بعد توقف الهجوم، ولكن أبلغ عن استمرار تعرض موقعه الإلكتروني الرسمي لنفس نوع الهجوم، وتم التصدي له والعمل على معالجة أي اختراقات مستقبلية مشابهة (عبدالله:2024).

وتوصلت نتائج المقابلات أن الهجمات على البنية التحتية الحيوية، مثل شبكات الكهرباء والمياه، تُعد من التهديدات الخطيرة التي واجهت ليبيا عام 2022م، فقد تعرضت شبكة الكهرباء الوطنية لهجوم سيبراني أدى إلى انقطاع التيار الكهربائي عن 15% من المناطق لمدة 24 ساعة، كما تواجه المصارف الليبية هجمات سيبرانية متزايدة، تهدف إلى سرقة البيانات، أو تعطيل الأنظمة المصرفية، ووفقًا لتقرير صادر عن مصرف

ليبيا المركزي في 2023م، تم تسجيل خمس محاولات اختراق كبرى لأنظمة المصارف، مما أدى إلى خسائر مالية مباشرة تُقدر بنحو مليوني دولار .

وتُظهر الإحصائيات التي نشرتها بيزنس إنسايدر في يوليو 2023م، أن ليبيا تواجه تحديات كبيرة في مجال الأمن السيبراني، حيث تحتل المرتبة الأولى في إفريقيا من حيث التعرض للتهديدات السيبرانية، ومرتبة 90 على المستوى العالمي(باي: 2023) وتشير البيانات إلى أن 49% من الهجمات تأتي من الولايات المتحدة الأمريكية، وهو ما يثير تساؤلات حول استخدام القراصنة لشبكات VPN لإخفاء مواقعهم الحقيقية (شعيتير: 2023). أما بالنسبة لمصادر الهجمات الأخرى، فإن النسب المئوية تشير إلى فرنسا بنسبة (12%) وألمانيا بنسبة (11%) وكندا وسنغافورة وأوكرانيا بنسبة (6%) لكل منها، وهو ما يعكس تنوع مصادر التهديدات (الرمحي:2022)

وفي أغسطس عام 2023م نفذ هجوم كبير استهدفت بالأساس قطاع الاتصالات، استهدفت حجب الخدمة، حيث بلغ عددها أكثر من 4400 هجمة من بين الشركات التي تعرضت لهذه الهجمات كانت شركة ليبيا للاتصالات والتقنية، والجيل الجديد، وشركة المدار، أثرت على عدة خدمات وتطبيقات، بما في ذلك خدمات المشتركين، من بين الشركات المتأثرة بشدة، شركة ليبيانا للهاتف المحمول، التي تعرضت لهجوم آخ، وقد تم وصف هذه الهجمات بأنها منسقة من خارج الشركات المستهدفة وأدت إلى انقطاع مؤقت للخدمة، انتشرت شائعات واسعة على شبكات التواصل الاجتماعي عن احتمالية تعرض بيانات العملاء للاختراق، ولكن شركة القابضة للاتصالات نفت أي تسريب لبيانات المشتركين وأكدت أن الهجوم كان يستهدف بيانات الموظفين (سالم: 2024).

ويُشير رئيس مجلس إدارة المؤسسة الليبية، للتقنية أمين صالح، في حديث لـ"اندبندنت عربية"، إلى أن القفزات السريعة التي حدثت في الحوكمة والخدمات الإلكترونية من قبل الحكومة الليبية، أدت إلى وجود نقاط ضعف واضطراب في طريقة عمل بعض الأنظمة التابعة للدولة والهيئات الحكومية، هذا الوضع جعل من السهل على المهاجمين تنفيذ عمليات الاختراق، ويُؤكد أيضا، على أن الفيروسات التي استهدفت المؤسسات الليبية هي فيروسات فدية وهجمات لحجب الخدمة، وقد حدث ذلك فعليًا في حالات مثل مصرف ليبيا المركزي وشركات الاتصالات الأخرى (اندبندنت عربية :2024).

أما وزارة المواصلات، فقد تعرضت لهجوم حصان طروادة عام 2013م. وفي عام 2022م، تعرضت الوزارة لهجوم عام، وصفه المدير بالكارثي، استخدم فيه رجل في الوسيط، هجوم الفدية وأدى إلى توقف الأجهزة مدة يومين كاملين، كما تعرضت الشبكة لهجوم التصيد الاحتيالي، من قبل قرصان مراهق (هاكر 17 سنة) ولم يحدد جنسيته، وتعرض أيضا ايميل وزير المواصلات لهجوم الفدية وقال إنَّ المهاجم طلب فدية؛ قائلا بانه يملك بيانات مهمة في الايميل، ولكن لم يتم دفع الفدية (مدير إدارة الموقع الإلكتروني بوزارة المواصلات، مقابلة خاصة:2024).

بدأت محاولات التهديدات السيبرانية التي استهدفت وزارة العدل، عام 2022م، تركز على الشبكات الداخلية، ومن أبرز التهديدات التي حدثت في السنوات الأخيرة، كانت تلك التي استهدفت مزود خدمة شركة ليبيا

للاتصالات والتقنية، المستضيف الرسمي لمعظم أجهزة وزارة العدل، فقد تمكن القراصنة من اختراق بيانات الشركة وسرقة بيانات الوزارة، وعلى الرغم من أنَّه تم معالجة الأمر في أقل من يوم، إلا أنَّ الهجمات استمرت بشكل شبه يومي على الوزارة (مدير ادارة الشؤون الفنية والشبكات و رئيس قسم السلامة والمعلوماتية بوزارة العدل، مقابلة خاصة :2024).

في 16 ديسمبر 2022م، أعلنت الشركة الليبية للبريد والاتصالات وتقنية المعلومات القابضة، وهي الشركة الرئيسية في قطاع الاتصالات في ليبيا، عن نجاح مهندسو شركة (LTT) في رصد هجمات سيبرانية استهدفت مركز استضافة البيانات، حيث تمكن المهندسون من الحد من تأثير الهجمات، ولم تتأثر إلا بعض المواقع بشكل محدود، ومن دون إلحاق أضرار بالزبائن. وأشارت الشركة إلى أن هجمات حجب الخدمة (DDoS)ليست جديدة، لكنها ازدادت حدة وتنوعًا مؤخرًا، واستمرت 10 ساعات(عين ليبيا: 2022).

وتعرضت شركة المدار الجديد للعديد من الهجمات، وكان أبرزها هجوم حجب الخدمة في شهر أكتوبر 2023م، كان له آثار كبيرة على مدى فترة طويلة(مدير إدارة تقنية المعلومات بشركة المدار: مقابلة خاصة.2024). كما واجهت شركة ليبيانا العديد من التهديدات خلال السنوات الماضية، وكان أبرزها هجمات الفدية، التي طالب أصحابها دفع أموال للمهاجمين لفك تشفير البيانات، أو لمنع تسريب بيانات الموظفين (رئيس قسم الأمن السيبراني بشركة ليبيانا للهاتف المحمول، مقابلة خاصة:2024). كما تعرضت الشركة للاختراق من قبل مجموعة من القراصنة، استهدفوا بيانات تتعلق بالمستندات المالية والمحاسبية، والمعلومات الشخصية، وبيانات جوازات السفر، وقواعد البيانات، وتقارير المدققين، والمعلومات الاستراتيجية، وبيانات التسويق، ووثائق عدم الإفصاح، وسجل المراسلات والمحادثات مع إدارة الشركة، وأوضح موقع هاكمانك بأن القراصنة تمكنوا من اختراق موقع شركة ليبيانا عبر استغلال نقاط ضعف في نظام الحماية الخاص بها، ومع ذلك، نفت شركة ليبيانا للهاتف المحمول تعرض بياناتها للاختراق، مؤكدة أن منظومتها تعمل بشكل طبيعي، كما نفت الشركة القابضة للاتصالات تسرب أي بيانات خاصة بالمشتركين في شركة ليبيانا، موضحة أن البيانات التي تعرضت للهجوم تتعلق بالمنظومة الداخلية للموظفين داخل الشركة، مشيرة إلى أن عدة شركات ومصارف عالمية تعرضت لهجمات سيبرانية مشابهة، وأوضحت الشركة أن معركة الأمن السيبراني مستمرة على مستوى العالم، وأنها تعمل يوميًا لحماية الشبكات ضد الهجمات العنيفة على ليبيا (بوابة الوسط: 2023).

في 21 أغسطس 2023م، أعلنت الشركة القابضة للاتصالات أن شركات الاتصالات الكبرى التابعة لها، والتي تعمل تحت شركة البريد الليبي للاتصالات وتقنية المعلومات(LPTIC) ، تواجه هجمات إلكترونية تهدف إلى تعطيل خدماتها، وفي بيان نُشر على (Facebook) أكدت الشركة أن هذه الهجمات تسببت في عدم استقرار العديد من الخدمات والتطبيقات، وأضافت أنَّ محاولات اختراق أنظمة شركاتها مستمرة، وأصبحت أكثر تنظيمًا، حيث بلغت التهديدات ضد ليبيا 114 جيجابايت، ووقع ما يقرب من 4400 هجوم خلال الربع الثالث من عام 2023م (libya review:2023) .

كما أوضح مدير التحول الرقمي بوزارة التعليم العالي والبحث العلمي، أن العصر الرقمي يمثل سيفًا ذو حدين؛ فمن ناحية، يوفر فرصًا غير مسبوقة للنمو والازدهار، ومن ناحية أخرى، يعرضنا لمجموعة واسعة من التهديدات السيبرانية، مثل انتهاكات البيانات، وهجمات الفدية، والاحتيال الإلكتروني، وهجمات حجب الخدمة، وهي هجمات يمكن أن تؤدي إلى خسائر مالية كبيرة، وتلف البيانات، وفقدان الثقة في الخدمات، وفي 12 يوليو 2023م، تعرض مركز التوثيق والمعلومات بوزارة التعليم العالي والبحث العلمي لهجمات حجب الخدمة (DDoS) من نوعين: هجمات البروتوكول (Protocol attacks) وهجمات طبقة التطبيقات (Application layer attacks). بدأت الهجمات باستهداف الخوادم المستضيفة، ثم امتدت لتشمل معظم الخدمات وخوادم مركز البيانات(مدير التحول الرقمي بوزارة التعليم العالي والبحث العلمي، مقابلة خاصة:2024) .

وهناك أيضاً، حملات تجسس متطورة تستهدف ليبيا، حيث كشفت شركة Check Point في شهر أغسطس 2023م، عن سلسلة من هجمات التجسس المستهدفة تستخدم تقنية الباب الخلفي الجديدة المسماة بـ "Stealth Soldier"التي تسمح للمشغلين بالتجسس على أجهزة الضحايا مثل الهواتف الذكية وأجهزة الكمبيوتر، واستخراج البيانات وتنصيب برامج ضارة لشن هجمات التصيد الاحتيالي، هذه الهجمات تبدو موجهة نحو مواقع تابعة لوزارة الخارجية الليبية بهدف التجسس، وهذا يشير إلى خطورة التهديدات السيبرانية التي تواجهها الحكومة الليبية (checkpoint:2023) ومن جانبها، أكدت شركة مايكروسوفت في تقرير حديث أن نظام الكمبيوتر في ليبيا يواجه أعلى نسبة إصابة بالبرامج الضارة مقارنة بالأنظمة الأخرى على مستوى العالم (Benqdara and other:2020:12) وفقًا لإحصائيات موقع كاسبرسكي لعام 2023، تم منع 437 مليون هجومًا برمجيًا خبيثًا على مستوى العالم. أما بالنسبة لليبيا، فتُظهر البيانات من موقع Securelist أن ليبيا تواجه تهديدات سيبرانية متعددة، بما في ذلك البرمجيات الخبيثة والهجمات المستهدفة (Deszca and others:2019).

في أغسطس 2023، تعرضت ليبيا لسلسلة من هجمات حجب الخدمة الموزعة (DDoS) التي استهدفت 161 عنواناً IP، شملت هذه الهجمات البنية التحتية الحكومية الرئيسية، والتعليم، والخدمات المالية، وصناعة الطاقة، وشركات الاتصالات مثل LTT وليبيانا، وقطاعات أخرى مهمة، استمرت الهجمات من 1 أغسطس حتى 26 أغسطس، واستهدفت وزارة التخطيط (planning.gov.ly)، والموقع الرسمي لوزارة العدل(aladel.gov.ly)، وجامعة الزاوية(zu.edu.ly)،ومصرف اليقين،ومعهد النفط الليبي (Ipilibya.com)، وشبكة التصويت الليبية (libyavotes.ly) خلال الجولة الثانية من انتخابات رئاسة المجلس الوطني الأعلى للدولة في 6 أغسطس، مثلت هذه الهجمات 5.8% من إجمالي عناوين IP العامة في ليبيا، والتي تبلغ 434،258 عنوانًا (NSFOCUS:2023).

خلال 20 عام من 2004 حتى 2024 تم تسريب أكثر من مليون ومئة ألف حساب في ليبيا تقريباً وهناك 1.139 مليون حساب مخترق وتم تسريبهم على الإنترنت، وخلال الربع الأول من عام 2024م تم تسريب

21584 حساب وفي الربع الثاني 4870 حساي وفي الربع الثالث تم تسريب 14505 حساب ، تقريبا عدد التسريبات لكل مئة حساب هو 17 حساب مخترق(شركة الجذور الليبية:2024).

وأصدر تقرير تقني عن موقع Business Insider الأمريكي يسلط الضوء على القلق المتزايد من انتهاكات الأمن السيبراني التي تهدد الشركات في إفريقيا، ووفقًا للتقرير، فإن ليبيا هي الأكثر تعرضًا لتهديدات الأمن السيبراني، حيث تحتل المرتبة 90 عالميًا، مما يجعلها عرضة للهجمات (Libya Review:2023).

في 1 مايو 2024م، تعرضت شركة مليته للنفط والغاز، إحدى أكبر الشركات المشغلة في ليبيا، لهجوم إلكتروني، وفقًا لموقع Hackmanac المتخصص في قضايا الأمن السيبراني، تسبب قراصنة روس في تعطيل قراءات ضغط الغاز وأجهزة استشعار خطوط الأنابيب، وقاموا بتشفير جميع بيانات المصنع، طالب المهاجم بفدية قدرها 50 مليون دولار مقابل عدم نشر 1 تيرابايت من بيانات الشركة، والتي تشمل المستندات المالية والمصرفية، وبيانات جوازات السفر والتأمين للموظفين والعملاء، بالإضافة إلى التقارير والتنبؤات الجيولوجية وتفاصيل إنتاج النفط في مناطق مختلفة والمراسلات السرية (Hackmanac:2024). وهكذا تمتلك ليبيا عددًا كبيرًا من أنظمة الشبكات المخترقة والتقنية القديمة، مما يجعلها عرضة للاستغلال من قبل الجهات الحكومية ومجموعات القرصنة، وهذه التهديدات المنسقة جيدًا، مثل تلك التي تستهدف مصافي النفط الليبية، لا تؤثر فقط على إنتاج النفط، بل قد تؤثر أيضًا على سوق النفط العالمية (Ali and others:2011:55). وفي هذا الصدد، قال مدير إدارة أمن المعلومات بالمؤسسة الوطنية للنفط، إن التهديدات السيبرانية التي تواجهها المؤسسة تتنوع بشكل كبير، حيث أن معظم هذه التهديدات تأتي عبر البريد الإلكتروني، ويرجع ذلك إلى إهمال الموظفين وعدم وعيهم الكافي بأهمية الأمن السيبراني، مما يزيد من احتمالية التعرض للاختراقات، وأشار إلى حادثة تعرضت لها إحدى الشركات النفطية التابعة للمؤسسة، حيث أستُغل (فلاش ميموري)، تم جلبه من مصدر غير موثوق، مما أدى إلى هجوم من قبل قراصنة الإنترنت، وذكر المدير أن أكبر هجوم تعرضت له المؤسسة كان في شهر مارس 2024م، حيث تعرضنا لتهديدات مستمرة شملت مجموعة متنوعة من الهجمات، مثل هجمات الحرمان من الخدمة (DDoS)، وهجمات الفدية، وهجمات التصيد الاحتيالي، بالإضافة إلى الابتزاز الإلكتروني، وقد أوضح المدير أن هذه الهجمات تؤثر بشكل كبير على الشبكة، مما يؤدي إلى تلف الأجهزة، وتسريب البيانات، والتعدي على صلاحيات المؤسسة (مدير إدارة أمن المعلومات بالمؤسسة الوطنية للنفط، مقابلة خاصة:2024). كما أشار السيد مدير إدارة أمن المعلومات بشركة الواحة للنفط إلى أنَّ التهديدات السيبرانية التي واجهتها الشركة، أصبحت متكررة ومتعددة الأبعاد، وتهدف إلى اختراق الأنظمة الداخلية وسرقة البيانات لأغراض تجارية ومالية، وقد أكد أن الشركة تتعرض لهذه الهجمات بشكل يومي، سواء كانت بسيطة، أو ذات تأثير كبير(مدير إدارة أمن المعلومات بشركة الواحة للنفط، مقابلة خاصة:2024).

بحسب موقع Zone-h في عام 2024 تم اختراق 19 موقع إلكتروني للمؤسسات الليبية و 11 موقع حكومي إمتداده .gov.ly قد نتج عنه تسريب بيانات حساسه ودخول غير مسموح به للموقع وقد كان التأثير مجرد تغير الصفحة الرئيسية للموقع، وهناك إدعاءات على تسريب بيانات شركة نفطية في ليبيا وإمكانية الوصول

لأنظمة البريد الإلكتروني للعديد من المؤسسات الليبية معرضه للبيع في الإنترنت المظلم، وأيضا بيانات جواز سفر للآلاف من المواطنين الليبين وقواعد بيانات لمصرف حكومي وجامعة ليبية لم يتم ذكر أسماهم معرضه بياتهم للبيع في الأنترنت المظلم(شركة الجذور الليبية: 2024).

نستنتج مما سبق، أنَّ ليبيا تواجه تهديدات سيبرانية متكررة تستهدف قواعد البيانات الحساسة والمؤسسات الحكومية، مما يهدد الأمن القومي ويضعف الثقة في البنية التحتية الرقمية، هذه التهديدات المستمرة تؤثر على الخدمات، حيث تتسبب في توقفها وتعرض أغلب الوزارات الليبية لهجمات من قراصنة داخليين وخارجيين، تتنوع هذه التهديدات بين العشوائية والموجهة، وتشمل مجموعة من الأدوات الأكثر استخدماً، مما يعطل الخدمات الحكومية ويؤدي إلى خسائر مالية كبيرة، تؤثر أيضا بشكل كبير على نظم المعلومات، مما يعوق الأداء الحكومي ويؤثر على تقديم الخدمات الحيوية للمواطنين وسيتم توضيح في الشكل رقم (10)خمس تهديدات أكثر شيوعاً في ليبيا بناء على نتائج المقابلات التي أجرتها الباحثة.

الشكل رقم (10) أنواع التهديدات الأكثر استهدافا على ليبيا، المصدر: من إعداد الباحثة.

يظهر الرسم التوضيحي أن الأدوات الأكثر استخداماً في ليبيا موضحة باللون الأحمر الفاتح، بينما يوضح التدرج إلى اللون الأحمر الداكن التهديدات السيبرانية الأقل شيوعاً، ومن خلال تحليل النتائج، يتبين أن القطاعات الأكثر عرضة للتهديدات السيبرانية تشمل قطاع الاتصالات، بسبب إمكانية استغلاله لتعطيل عمليات واسعة النطاق، وقطاع النفط والغاز، حيث تمثل الهجمات عليه خطراً كبيراً على الاقتصاد الوطني، كما تتعرض الخدمات المالية، بما في ذلك المصارف الليبية، لهجمات تشير إلى هشاشة البنية الأمنية في هذا القطاع، بالإضافة إلى البنية التحتية الحيوية الأخرى مثل الكهرباء والمياه والمؤسسات الحكومية، وبما أنَّ هذه القطاعات تعتمد بشكل كبير على التقنية الرقمية والبيانات الحساسة، فهي أهداف سهلة للتهديدات السيبرانية، ويؤدي استهدافها إلى تأثيرات كبيرة على الصعيدين الاقتصادي والسياسي، وهذا ما لزم وضع إجراءات واليات لمواجهة هذه التهديدات وهو ما سوف نتناوله في المبحث التالي.

3.3. تقييم الجهود الليبية في مكافحة التهديدات السيبرانية

خلال العقد الأول من القرن الحالي، ومع زيادة التوجه نحو الرقمنة، برزت الحاجة إلى حماية الفضاء الإلكتروني الليبي، حيث تُعد البنية التحتية الرقمية مكونًا أساسيًا للأمن القومي، هذا التطور ألقى الضوء على أهمية بناء منظومة سيبرانية قوية قادرة على مكافحة التهديدات السيبرانية في ليبيا، وحيث أنَّ الأمن السيبراني أصبح أولوية وطنية، وجب على الحكومة الليبية إدراك الأهمية الحاسمة لإنشاء إطار للأمن السيبراني لحماية أنظمة المعلومات والبنية التحتية الرقمية ومن أبرز هذه الجهود ما يأتي :

1.3.3 جهود المؤسسات الحكومية :

1. تم إنشاء الهيئة العامة لأمن وسلامة المعلومات (NISSA) بموجب القرار رقم (28) لسنة 2013م، الصادر عن مجلس رئاسة وزراء بالحكومة الليبية المؤقتة بتاريخ 22 يناير 2013م، تتمثل مهمتها في تعزيز واستدامة الاستخدام الآمن لتكنولوجيا المعلومات والاتصالات ومنع المخاطر المرتبطة بها واكتشافها والاستجابة لها بفعالية، قامت الهيئة العامة لأمن وسلامة المعلومات بصياغة الاستراتيجية الوطنية للأمن السيبراني الخاصة بليبيا سنة 2022م، وتم اعتمادها رسمياً من طرف مدير الهيئة في أوائل عام 2023م، تتمثل الرؤية التي تنص عليها الاستراتيجية الوطنية للأمن السيبراني في توفير بيئة آمنة للتحول الرقمي وبناء القدرات اللازمة لمواجهة المخاطر المرتبطة به وتمكين الأفراد والمؤسسات من الاستفادة من الفضاء السيبراني بشكل آمن، يشمل نطاق الاستراتيجية الوطنية للأمن السيبراني، كل ما له علاقة بحماية وضمان مصالح الوطن والشعب، وحددت الاستراتيجية خمسة أهداف استراتيجية وتسعة مجالات تنفيذ(الهيئة العامة لأمن وسلامة المعلومات:2023)، تتمثل الأهداف الاستراتيجية الخمسة في:

- تعزيز وتطوير الإطار القانوني والتشريعي وضمان تعزيز الإدارة الجيدة للفضاء السيبراني.
- بناء القدرات البشرية والمادية اللازمة لحماية وتأمين الفضاء السيبراني والتحول الرقمي.
- تعزيز أمن ومصداقية المعاملات الإلكترونية.
- تشجيع التعاون مع الجهات الداخلية والخارجية ومع الأفراد والمؤسسات من أجل توطين صناعة الأمن السيبراني.
- دعم التوجه نحو التحول الرقمي من خلال نشر ثقافة الأمن السيبراني في المجتمع.

قال رئيس الهيئة العامة لأمن وسلامة المعلومات ومدير مكتب التعاون الدولي التابع لها، إن الهيئة تساهم على المستويين المحلي والدولي في تعزيز الأمن السيبراني من خلال مجموعة من الجهود(مدير إدارة الهيئة العامة لأمن وسلامة المعلومات ومدير مكتب التعاون الدولي التابع لها، مقابلة خاصة:2024).

- عام 2019م، أصدرت الهيئة أول دليل للسياسات الوطنية لأمن وسلامة المعلومات، الذي يتضمن سياسات حماية البيانات، الاستخدام المقبول، المستخدم، مكافحة الفيروسات، أمان الشبكة، الطرف الثالث، النسخ الاحتياطي للبيانات، والأمان المادي.

- في 2021م، أصدرت الهيئة الإصدار الثاني من السياسات الوطنية، والتي تشمل سياسات تصنيف المعلومات، حماية البيانات، الاحتفاظ بالسجلات وإتلافها، نشر البيانات، الاستخدام المقبول، كلمة السر،

اســتعمال البريد، الحماية من البرمجيات الخبيثة، التوعية والتدريب، الجدار الناري، التشــفير، التعامل مع الحوادث، النسخ الاحتياطي، وخصوصية بيانات العملاء.

- تم إنشاء الفريق تحت مظلة الهيئة بدعم من الاتحاد الدولي للاتصالات، وهو مسؤول عن منع التهديدات السيبرانية وكشفها والتخفيف من حدتها على المستوى الوطني.

- قامت الهيئة بتجهيز مختبر الطب الشــرعي الرقمي الجديد بالكامل وبدأت في إجراء الاختبارات المعملية.

- نظمت الهيئة ورش عمل للمتخصصين الفنيين لعرض سيناريوهات فعلية تحاكي الهجمات السيبرانية في وزارة المالية والجهات التابعة لها، وأجرت العديد من اختبارات الاختراق وتقييمات الضــعف لوكالات متعددة، بالإضافة إلى عقد العديد من الندوات وورش العمل التوعوية في أغلب المؤسسات.

- شــاركت الهيئة في الحدث الرابع لسلسلة ابتكارات الأمن السيبراني CSIS في تونس في سبتمبر 2022.

- شاركت في بعض ورش العمل والتدريبات السيبرانية الدولية، والعديد من المؤتمرات الدولية في تونس وقطر ، وكذلك مؤتمر تقييم الفضاء الإلكتروني في عمان، والاجتماعات السنوية لمنظمة التعاون الإسلامي.

- شاركت في فعاليات الأسبوع الإقليمي للأمن السيبراني 2022م، والذي شمل الاجتماع العام العاشر والمؤتمر السنوي الرابع عشر لـــOIC-CERT ، والقمة الإقليمية العاشرة للأمن السيبراني في مسقط، سلطنة عمان.

- عملت الهيئة على إعداد برامج تعليمية للأمن الســيبراني بالتعاون مع وزارة التعليم العالي ووزارة التعليم الفني، وأعدت إطار الترخيص لشركات الأمن السيبراني بالتعاون مع وزارة التجارة.

- تم توقيع مذكرات تفاهم واتفاقيات عدم الإفشاء مع معاملات للخدمات المالية (المفتاح الوطني) في أبريل 2022، ووزارة المالية في يونيو 2022.

- شــاركت الهيئة في منتدى إطلاق الرؤية الاســتراتيجية العربية للأمن السيبراني في تونس في أكتوبر 2021، تحت رعاية جامعة الدول العربية.

- تتعاون الهيئة مع منظمات دولية مثل الاتحاد الدولي للاتصــالات لتحسين القدرات الوطنية، وتمثل ليبيا في المؤتمرات والمنتديات الدولية المتعلقة بالأمن السيبراني، مما يسهم في نقل الخبرات وتطبيقها محليًا.

- أطلقت الهيئة العديد من المبادرات، منها ورش العمل والندوات التثقيفية، التي ســاهمت في تدريب أكثر من 500 مختص في الأمن الســيبراني بين عامي 2018 و2022 واســتمر التدريب لكل المؤســســات في الدولة حتى 2024.

2. أعلن مصرف ليبيا المركزي في 22 يونيو 2021م، عن مشروع "سايبر ليبيا"، وهو مبادرة تهدف إلى تكوين بنية تشريعية للمعاملات الإلكترونية، مما يؤسس لتحول رقمي يفتح المجال للاستثمار في المجال

السـيبراني. تهدف رؤية هذه المبادرة إلى تطوير الصـناعة المصـرفية في ليبيا من خلال الاسـتفادة من تكنولوجيا الاتصـالات وتقنية المعلومات، على المسـتوى الدولي، تعتبر لجنة الأمم المتحدة (الإسـكوا) الشريك الاستراتيجي لهذا المشروع، بالتعاون مع عدد من الخبراء الدوليين، وتأتي مبررات اختيار هذه المبادرة على ثلاث أسـس رئيسـية هناك مبادرات من عدة مؤسـسـات بخصـوص قانون المعاملات الإلكترونية وقانون الجرائم الإلكترونية، يقود مصـرف ليبيا المركزي مشـروعًا مهمًا وهو مشـروع الدفوعات الوطني، الذي يهدف إلى طرح منتجات جديدة في سـوق المدفوعات الليبي مثل التجارة الإلكترونية، يعتبر مصرف ليبيا المركزي المستشار الاقتصادي للدولة الليبية، ويسعى لتطوير وتنويع الأنشطة الاقتصادية من خلال التحول الرقمي، الذي يُعد محركه الأساسي هو التشريعات السيبرانية ودورها في دعم التحول الرقمي(مدير إدارة تقنية المعلومات بمصـرف ليبيا المركزي، مقابلة خاصة:2024)

3. أصـدر وزير العدل السـابق بالحكومة الليبية المؤقتة، مبروك قريرة، القرار رقم 26 لعام 2016 بشـأن إنشـاء إدارة أبحاث ودراسـات مكافحة الجريمة الإلكترونية، وذكر رئيس مركز الخبرة القضـائية والبحوث، عمر الحجازي، أن إنشـاء هذه الإدارة جاء بناء على طلب من مركز الخبرة القضـائية والبحوث، وقد وافق وزير العدل على ذلك، تتمتع إدارة الأبحاث ومكافحة الجريمة الإلكترونية بالاستقلالية الفنية، وتتبع إداريًا وماليًا لمركز الخبرة القضائية والبحوث، تأسست الإدارة العامة لمكافحة الجريمة الإلكترونية وأمن المعلومات بقرار من وزير العدل في الحكومة الليبية المؤقتة بتاريخ 21 فبراير 2016، وهي الإدارة الفنية الأولى من نوعها المتخصصة في مكافحة جرائم الإنترنت والإرهاب الإلكتروني، يأتي إنشاء هذه الإدارة في ظل انتشار الجريمة السيبرانية بأشكالها المختلفة، التي أصبحت تشكل تهديدًا واضحًا لأمن الدولة والمجتمع (القطروني:2018:98).
4. قام جهاز المباحث الجنائية التابع لوزارة الداخلية بسلسلة من الإجراءات القانونية والإدارية والتقنية للحد والوقاية من التهديدات السـيبرانية(مدير إدارة جهاز المباحث الجنائية بوزارة الداخلية، مقابلة خاصة:2024)، من بين الإجراءات:

- تم وضـع مقترح مشـروع الاسـتراتيجية الوطنية لمكافحة الجرائم الإلكترونية في ليبيا، بقرار من مكتب الوزير الداخلية المفوض رقم 3193/6.1 بتاريخ 26-04-2020م، حيث اكتمل 80% منه وتوقفت عملية تنفيذها بعد ذلك.
- شـاركت مندوبين عن جهاز المباحث الجنائية في ورش عمل ومؤتمرات دولية ومحلية وإقليمية تتعلق بالأمن السيبراني.
- تم تعيين مندوب لوزارة الداخلية في مجلس وزراء الداخلية العرب، وتم الموافقة على اقتراح إنشـاء مكتب للأمن السيبراني والجريمة الإلكترونية في الجزائر يتبع مجلس وزراء الداخلية العرب.

- عُقدت ورش عمل تتعلق بالأمن السـيبراني، بما في ذلك ورشــة عمل نظمها جهاز المباحث الجنائية في جامعة طرابلس حول الأمن السـيبراني خلال عام 2016م، وأفضـت إلى توصـيات، كونها أول ورشــة عمل تُنظم في هذا المجال.
- تم توقيع مذكرة تفاهم مع الهيئة الوطنية لأمن وسـلامة المعلومات لمراقبة الشـبكة من التهديدات وتعزيز التعاون وتبادل الخبرات.
- نُفذت دورات تدريبية تقنية تخصـصـية بدعم من الجانب الأوروبي لأفراد وضـباط وزارة الداخلية لدعم البنية التحتية التقنية.
- شُكلت لجان من الوزارة لإقامة فعاليات شهر التوعية بالأمن السيبراني خلال شهر أكتوبر من كل عام.
- تم تضـــمين مواضـــيع الأمن الســـيبراني ضـــمن برامج الإعلام الأمني لتوعية الناس بمجالات الأمن السيبراني من خلال برامج الإعلام المرئي الأمني.
- وُضـعت حقائب تدريبية تخصصية لتنفيذها بالتعاون مع الجانب الأوروبي والأمم المتحدة لتأهيل الضباط والأفراد تقنيًا في مجال الأمن السيبراني.
- تم تخصـيص الميزانيات اللازمة لدعم خطة التحول الرقمي والابتعاد عن الورق وضـمان سـرية الوثائق وحمايتها من الهجمات.
- تُتبع بعض الجرائم الســـيبرانيـة التي أثرت في البنيـة التحتيـة الرقميـة في ليبيـا، وتم إعداد تقارير وتبادل المعلومات مع الدول المجاورة، كما تم التعامل مع فيروس وان كاراي الذي أثر على أجهزة الحواســيب بنظام ويندوز خلال عام 2018م.
- عُقدت اتفاقيـات تعـاون مع أجهزة إنفـاذ القـانون الـدولية مثل الانتربول وافريبول من خلال قســم جرائم السيبرانية.

أكدت نتائج المقابلات التي أجرتها الباحثة أن اســتراتيجية الأمن الســيبراني الوطني في ليبيا، لا تزال قيد التطوير، مما يعرقل تنفيذها بشـكل كامل، وتظهر تحديات تنفيذ هذه الاسـتراتيجية نتيجة نقص البنية التحتية التقنية المتقدمة ونقص الكوادر المتخصـصـة في هذا المجال، بالإضـافة إلى ذلك، هناك تباين واضـح في فهم وتنفيذ سياسات الهيئة الوطنية لأمن وسلامة المعلومات(NISSA) ، مما يوحي بالحاجة إلى إجراءات أكثر وضوحًا وتنسيقًا في هذا الصدد.

على صـعيد البنية التحتية الرقمية، تعمل الحكومة على تحسـينها من خلال تحديث الأنظمة واعتماد التقنيات المتقدمة مثل التشـفير والجدران النارية وغيرها من وسـائل الحماية ورغم وجود هذه الجهود، إلا أنها تواجه تحديات بسـبب ضـعف الاسـتثمار في هذا القطاع علاوةً على ذلك، تبدي المؤسـسـات تفاوتًا بين القطاعات، حيث يظهر عدم وجود سجلات محددة للحوادث السيبرانية الخطيرة، مما يعيق القدرة على التخطيط لتعزيز القدرات والاســتعداد لمواجهـة هذه التحـديـات، يُلاحظ أن ليبيـا تواجـه تحـديـات كبيرة نتيجة لنطاق الحماية الضعيف وعدم وجود قائمة وطنية بالبنية الأساسية الحرجة، ومن المؤسف أن الأمان المادي للبنية الأساسية

يعتبر عامل سلبي يؤثر على الجدوى والفعالية، هناك نقص واضح في عمليات كشف وحماية القطاعات المختلفة، باستثناء قطاع الاتصالات الذي يتولى اهتمامًا خاصًا.

أما بشأن القطاع المصرفي، يُلاحظ اهتمامًا خاصًا بتنفيذ المعايير الدولية للأمن السيبراني، ولكن لا تزال برامج التوعية بالأمن السيبراني تعاني من قلة التوسع وعدم الشمولية، ويُسلط التحليل الضوء على دور المواطن الليبي في تعزيز الأمن السيبراني من خلال اتباع الممارسات السليمة ونشر الوعي بأهمية حماية المعلومات الشخصية.

2.3.3. الإطار القانوني لحماية الفضاء الإلكتروني :

في السنوات الأخيرة، بدأت ليبيا تُدرك أهمية تحديث تشريعاتها القانونية لمواكبة التطورات المتسارعة في مجال الأمن السيبراني ومن بين الجهود التي بذلتها الدولة لتحسين الإطار القانوني:

1. أصدر مجلس النواب القرار رقم 5 لسنة 2022م، الذي يركز على مكافحة الجرائم الإلكترونية والذي يضم في طياته 52 مادة مع أهميتها الكبيرة، تتضمن المادة الأولى تعريفًا شاملاً لمجموعة من المفاهيم المرتبطة بالجريمة الإلكترونية، بينما تناولت المادة الثانية أهداف القانون التي تركز على تعزيز العدالة والأمن المعلوماتي، وحماية النظام العام والآداب العامة، وحفظ الحقوق المترتبة على الاستخدام الشرعي لتقنيات الحوسبة الحديثة، يسعى القانون أيضًا إلى تعزيز الثقة العامة في صحة المعاملات الإلكترونية، ويحظر بشدة الأنشطة المرتبطة بالاحتيال عبر الإنترنت، مثل سرقة الهوية الإلكترونية واستخدامها في أنشطة غير قانونية، كما يجرم القانون التلاعب بالبيانات الإلكترونية أو التزوير، خاصة إذا كانت هذه البيانات تتعلق بالمؤسسات الحكومية أو تحتوي على معلومات حساسة، وأخيراً يهدف هذا القانون إلى تعزيز الأمن السيبراني وحماية المعلومات الرقمية في المجتمع، وتحقيق تنظيم وإدارة فعالة للأنشطة الإلكترونية (مجلس النواب الليبي:2023).
2. صدر القانون رقم 6 لسنة 2022م، بشأن المعاملات الإلكترونية، الصادر عن مجلس النواب الليبي، يتضمن تسعة فصول، الفصل الأول يتناول الأحكام العامة، حيث تحتوي المادة الأولى على 21 تعريفًا، أما المادة الثانية تحدد هدف القانون، وهو تنظيم وحماية المعاملات الإلكترونية وتعزيز الثقة العامة في صحتها وسلامتها، تنص المادة الثالثة على أن أحكام هذا القانون تسري على السجلات أو التوقيعات الإلكترونية والوسائل الإلكترونية، وكذلك على التصرفات والمعاملات التي تتم بين الأشخاص الذين اتفقوا على إجراء معاملاتهم بطرق إلكترونية، يمكن استنتاج موافقة الشخص على ذلك من سلوكه مع مراعاة حكم المادة الرابعة، يجب أن يكون قبول الحكومة للتعامل الإلكتروني صريحًا، ولا يعد قبولها التعامل بوسائل إلكترونية في معاملة معينة قبولًا للتعامل بهذه الوسائل في معاملات أخرى، المادة السابعة تنص على أن الجهات الحكومية، إذا قررت استخدام الوسائل الإلكترونية وفقًا للمادة السادسة، يجب أن تحدد الشروط والمواصفات اللازمة لذلك يجوز لمجلس الوزراء استثناء بعض الجهات من حكم هذه المادة لاعتبارات متعلقة بالأمن القوم (مجلس النواب الليبي :2022).

3. قرار رقم 150 لسنة 2024 الصادر عن وزارة الاقتصاد والتجارة في ليبيا، ويهدف هذا القرار إلى وضع إطار تنظيمي لمزاولة خدمات الأمن السيبراني. يتألف القرار من خمسة مواد ويستند إلى سوابق قانونية متنوعة، حيث يحدد التعريفات ومتطلبات الحصول على تراخيص ممارسة النشاط، بالإضافة إلى المعايير التشغيلية لمقدمي خدمات الأمن السيبراني(ديوان وزارة الاقتصاد والتجارة:2024).

يؤكد القرار على أهمية تنظيم خدمات الأمن السيبراني من خلال ضرورة وجود تراخيص ممارسة صالحة لتقديم الخدمات، مع التأكيد على أهمية تجديد التراخيص التجارية، هذا من شأنه أن يسهل ضمان توافق عمليات الأمن السيبراني مع المعايير الوطنية والمتطلبات القانونية، يعكس هذا القرار السعي نحو تعزيز الأمان السيبراني ورفع مستوى الحماية في البيئة الرقمية، ويساهم في خلق بيئة إلكترونية آمنة وموثوقة.

4. القرار رقم 37 لسنة 2024م، الصادر عن الهيئة العامة لأمن وسلامة المعلومات بشأن اعتماد ضوابط استخدام حسابات الجهات الحكومية على منصات التواصل الاجتماعي في ليبيا، يتكون هذا القرار من ثلاثة مواد، وتهدف الضوابط المعتمدة إلى وضع إطار يضمن الاستخدام الآمن والمسؤول لحسابات الجهات الحكومية في منصات التواصل الاجتماعي(المجمع القانوني الليبي:2024).

تأتي هذه الضوابط في سبيل حماية البيانات والمعلومات، وتقليل التهديدات السيبرانية المرتبطة باستخدام حسابات الجهات الحكومية بطريقة آمنة، يهدف ذلك إلى الحد من مخاطر جرائم اختراق حسابات التواصل الاجتماعي الخاصة بالمؤسسات، والحد من انتحال الشخصيات أو سوء استغلالها، تطبق هذه الضوابط على جميع الجهات الحكومية في ليبيا، سواء كانت وزارات أو هيئات أو مؤسسات أخرى والتي تمتلك حسابات رسمية على منصات التواصل الاجتماعي، تعكس هذه التدابير المتخذة رغبة في تعزيز الأمان السيبراني والحماية الشاملة للمعلومات والبيانات الحكومية في البيئة الرقمية.

وتوصلت نتائج المقابلات التي أجرتها الباحثة أن الحكومة الليبية تبدي جهودًا في إطار التشريعات لتحسين قوانين الأمن السيبراني ومع ذلك أن هذه التشريعات لا تلبي المعايير الحديثة المطلوبة لحماية البنية التحتية الرقمية، وليست على مستوى التطورات السريعة في مجال التهديدات السيبرانية.

أشارت نتائج المقابلات إلى ضرورة مراجعة وتحديث هذه القوانين، نظرًا لوجود أخطاء فنية وعقوبات قد تكون تعسفية وغير منطقية، مما يجعلها غير كافية لمواجهة التحديات الأمنية بشكل فعال، بالإضافة إلى ذلك، يظهر أن التشريعات السيبرانية في ليبيا لا تشمل كافة جوانب الأمن السيبراني الضرورية كحماية البيانات الشخصية ومكافحة الجرائم الإلكترونية، و أيضا أن النظام القانوني في ليبيا يعاني من نقص في هيئة تنظيمية مركزية للإشراف على تنفيذ هذه التشريعات، مما يؤثر على التنسيق بين الجهات الحكومية في مجال الأمن السيبراني، كما تظهر دراسة الحاجة الملحة لزيادة العدد من المدعين العامين أو القضاة المتخصصين في الجرائم السيبرانية.

بصورة عامة، تشير البيانات إلى نقص في التعاون بين أجهزة إنفاذ القانون والقطاع الخاص في مجال الأمن السيبراني، وتفتقر الشركات إلى آليات رسمية للإبلاغ عن الجرائم السيبرانية، ويركز العمل على التعامل مع الجرائم الإلكترونية ضمن القوانين الجنائية العامة، مما يعقد العملية في مجال محاسبة الجناة،

ومع ذلك هناك جهود من بعض الجهات الحكومية، مثل مصـــرف ليبيا المركزي، لفرض تدابير أمنية في القطاع المصـــرفي عبر دليل حوكمة تقنية المعلومات ومع ذلك، يظل هذا الإجراء محدودًا في ظل غياب تشريعات واضحة تغطي جميع القطاعات.

3.3.3. التعاون الإقليمي والدولي في مجال الأمن السيبراني :

سعت ليبيا إلى التعاون مع المنظمات الدولية والدول الأخرى لتبادل الخبرات وبناء القدرات في مجال الأمن السـيبراني، وعلى الرغم من التحديات، تسـعى لتعزيز وجودها في المبادرات الدولية المتعلقة بالأمن السيبراني، من أبرز هذه المبادرات "مبادرة الأمن السيبراني الإفريقي" التي تشرف عليها مفوضية الاتحاد الإفريقي، وتهدف إلى تعزيز تبادل المعلومات والخبرات بين الدول الأعضـاء (مسيكة، 2022). كما وقّعت ليبيا اتفاقيات تعاون مع عدة دول لتعزيز قدراتها في مجال الأمن السـيبراني، منها اتفاقية مع الوكالة الدولية للأمن السـيبراني في فرنسـا عام 2019م، وأخرى في تونس عام 2021م، أسـهمت هذه الاتفاقيات في نقل الخبرات وتبادل المعلومات حول التهديدات السيبرانية المشتركة (حامد: 2023). كما سعت ليبيا الانضـمام إلى اتفاقية الاتحاد الإفريقي بشـأن أمن الفضـاء الإلكتروني وحماية البيانات ذات الطابع الشـخصـي بصـفة مراقب، وأجلت الانضـمام حتى يتم اعتماد منظومة تشـريعية ليبية حول الفضـاء السـيبراني وحماية البيانات الشخصية (الهيئة العامة للاتصالات والمعلوماتية: 2022).

تعد ليبيا من بين الدول الموقعة على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2001م، لكنها لم تصـــادق عليها بعد حتى تاريخ هذه الدراســـة، وهي حاليًا ليســـت من بين الدول الموقعة على أي اتفاقيات إقليمية أو دولية أخرى متعلقة بالأمن السيبراني، مثل اتفاقية بودابست التي تعد عدة بلدان أخرى في المنطقة عضوة فيها أو لديها صفة المراقب. تبذل ليبيا جهودًا لتحسين تعاونها الدولي في مجال الأمن السيبراني في عام 2022م، أطلقت الحكومة مشـروع "تحالف الأمن السـيبراني في شـمال إفريقيا"، بهدف تعزيز التعاون الإقليمي لمواجهة التهديدات السـيبرانية المشـتركة، شـمل هذا المشـروع عقد اجتماعات دورية بين الدول الأعضاء، مما أدى إلى تطوير خطة إقليمية للتصدي للتهديدات السيبرانية العابرة للحدود (رجب: 2017).

بالإضـافة إلى ذلك، تسـعى ليبيا إلى تعزيز شـراكاتها مع القطاع الخاص، فقد أبرمت اتفاقيات مع شـركات تقنية عالمية مثل Microsoft وCisco وغيرها من الشـركات لتطوير حلول تقنية لتحسـين حماية الأنظمة الرقمية الوطنية وبحسـب البيانات الرسـمية، سـاهمت هذه الشـراكات في تقليل عدد التهديدات السـيبرانية المستهدفة للمؤسسات الحكومية بنسبة 15% بين عامي 2021 و2023م (مسيكة، 2022). كما تعمل ليبيا على تحسين تمثيلها في المحافل الدولية، حيث شاركت في أكثر من 25 مؤتمرًا دوليًا حول الأمن السيبراني منذ عام 2019، أسهمت هذه المشاركات في تبادل الخبرات وبناء شبكات تعاون مع دول ومنظمات دولية، مما عزز قدرات ليبيا في مواجهة التهديدات الرقمية (Railton:2013).

أكدت نتائج المقابلات التي أجرتها الباحثة أن التعاون الدولي والإقليمي يعد عنصـرًا أسـاسـيًا في جهود ليبيا لمواجهة التحديات السـيبرانية المتزايدة، تعتمد ليبيا على الشـراكة مع منظمات ودول مثل الاتحاد الأوروبي

والأمم المتحدة للحصـــول على دعم فني وتقني، مما يســـهم في تدريب الكوادر الوطنية وتبادل المعلومات حول التهديدات السيبرانية. ومع ذلك، تؤثر الانقسامات السياسية الداخلية على قدرة الحكومة على الاستفادة الكاملة من هذا التعاون، ويشير الوضع الحالي للتعاون الدولي في ليبيا إلى أنه لا يزال في مراحله الأولى، حيث يعتمد بشـــكل أســـاســـي على مشـــاركة الخبرات والمعرفة من خلال المؤتمرات الدولية والمكتبات المعرفية. هناك حاجة إلى المزيد من الجهود لتوســـيع هذا التعاون وتفعيله بشـــكل أكثر فعالية، بما في ذلك تحسين السياسات المحلية وتطوير القوانين المتعلقة بالأمن السيبراني وتدريب الكوادر المحلية، من ناحية أخرى، لا يزال التعاون بين القطاعين العام والخاص ضعيفًا، مما يؤثر على سرعة استجابة ليبيا للتحديات السيبرانية. تواجه الاستثمارات الحالية في مجال الأمن السيبراني تحديات كبيرة تعكس الوضع الاقتصادي والسياســي الســائد في البلاد، على الرغم من وجود بعض الاستثمارات من قبل الحكومة والمؤســســات الخاصة، إلا أنها تبقى محدودة وغير كافية للتصدي للتهديدات السيبرانية المتزايدة .

تتركز الاستثمارات الخاصة في الأمن السيبراني بشكل أكبر في الشركات الكبرى، خصوصًا في قطاعات مثل البنوك والنفط والاتصالات، بينما تظل المؤسسات الصغيرة والمتوسطة أقل استثمارًا في هذا المجال، تتفاوت هذه الاستثمارات حسب الحجم والقدرة المالية للمؤسسات، مما يستدعي تعزيز هذه الاستثمارات لتتناسب مع التحديات الحالية، بالرغم من وجود بعض المبادرات من قبل المؤسسات الحكومية، إلا أنها لا تزال محدودة ولا تصل إلى المواطنيين العام بشكل كافٍ.

4.3.3. سياسات التوعية المجتمعية بالأمن السيبراني :

تُعد التوعية المجتمعية بالأمن الســـيبراني إحدى الركائز الأســـاســـية لتعزيز الحماية الرقمية في ليبيا تســـعى الدولة من خلال حملات وطنية إلى تعريف المواطنين بخطورة الجرائم الســـيبرانية وأهمية حماية البيانات الشـــخصـــية، اســـتهدفت هذه الحملات مختلف شـــرائح المجتمع، بما في ذلك المدارس والجامعات والمؤسسات الحكومية(Railton:2013). وقد تضمنت جهود التوعية تنظيم أكثر من 30 ورشة عمل منذ عام 2019 بالتعاون مع شـــركات تقنية محلية ودولية. شـــملت هذه الورش مواضـــيع متنوعة مثل حماية الحسابات الشخصية، التعامل مع البرمجيات الخبيثة، والتعرف على المخاطر السيبرانية. بالإضافة إلى ذلك، تعاونت الدولة مع شركات الاتصالات مثل "ليبيا تيليكوم" لتوفير منصات تعليمية تُعزز من سلوكيات الأمان الإلكتروني، مما أدى إلى تدريب أكثر من 10،000 مستخدم منذ عام 2020. تم إدراج مفاهيم الأمن الســـيبراني في بعض المناهج التقنية لتأهيل الجيل القادم للتعامل مع التحديات الرقمية (القطروني: 2018). من خلال التدريب والتطوير، تم إطلاق مبادرات وطنية لتعزيز الوعي بالأمن الســـيبراني بين المواطنين وفي المؤســـســـات الحكومية (باي: 2023). ومن الجوانب الإيجابية، أن القطاع الخاص في ليبيا يظهر اهتمامًا متزايدًا بالأمن الســـيبراني، حيث أطلقت بعض الشـــركات مبادرات للتوعية. ومع ذلك، تبقى هذه الجهود محدودة وغير منظمة، حيث لا يوجد إطار عمل موحد يشـــرف على تنفيذ هذه المبادرات ويضـــمن تكاملها مع الجهود الوطنية (Deszca and others:2019).

أكدت نتائج المقابلات التي أجرتها الباحثة أن الوزارات الليبية تسعى إلى تعزيز التوعية بالأمن السيبراني بين الموظفين والمستخدمين من خلال مجموعة من التدابير الوقائية التي تشمل برامج تدريبية متنوعة، رغم محدوديتها تشمل هذه التدابير تنفيذ برامج توعية تهدف إلى رفع الوعي بالمخاطر المتعلقة بالتهديدات السيبرانية، وتتضمن ورش عمل، ومواد توعوية إلكترونية مثل الصور والفيديوهات والمقالات المكتوبة، بالإضافة إلى الملصقات التوعوية، كما تستخدم بعض المؤسسات الحكومية مثل مصرف ليبيا المركزي والمؤسسة الوطنية للنفط رسائل البريد الإلكتروني الرسمية لتوزيع نصائح وتوجيهات تتعلق بالأمن السيبراني، إلى جانب إجراء تقييمات واستبيانات سنوية لقياس مدى فهم الموظفين لهذه المواضيع.

علاوة على ذلك، تعتمد بعض الوزارات على التدابير الموجهة مباشرة نحو تدريب الموظفين باستخدام تقنيات مؤمنة وبرامج مراقبة الأنظمة، يتم تنفيذ هذه التدابير غالبًا عبر عطاءات أو مناقصات خاصة بالتدريب، وتتم معظم البرامج التدريبية بشكل شخصي، حيث لا تتوفر بعد منصات توعية آلية معتمدة على نطاق واسع، تركز هذه البرامج على تنمية مهارات الأمان السيبراني لدى الموظفين، لكنها ليست منتشرة أو شاملة في كافة المؤسسات الليبية، ولا توجد مناهج دراسية أو وثائق رسمية تحتوي على الأولويات الوطنية للتثقيف بشأن الأمن السيبراني بعد، رغم أن التثقيف بهذه المسألة مدرج في أولويات تنفيذ الاستراتيجية الوطنية للأمن السيبراني التي صادره عن الهيئة العامة لأمن وسلامة المعلومات، علاوة على ذلك، لم يتم وضع ميزانية وطنية تركز على التثقيف بمسألة الأمن السيبراني حتى الآن، إذ تتعاون المدارس والجامعات والقطاعات فيما بينها وبين الهيئة العامة لأمن وسلامة المعلومات بصورة مؤقتة لتوفير الموارد اللازمة لتقديم دورات تثقيفية في مجال الأمن السيبراني، وتساهم بعض الجامعات الليبية مثل جامعة طرابلس، التي أنشأت تخصص الأمن السيبراني في كلية تقنية المعلومات بدرجة الماجستير، في تطوير القدرات المحلية من خلال إدراج برامج دراسية وتدريب الكوادر في مجال الأمن السيبراني، بالإضافة إلى ذلك، تقوم بعض المراكز المتخصصة بإنشاء شراكات مع شركات دولية لتوفير حلول متقدمة للأمن السيبراني، لكن لا توجد حتى الآن أدلة على قيام جامعات أو مؤسسات تعليمية أخرى عامة مماثلة بتوفير درجات علمية كاملة في مجالات متصلة بالأمن السيبراني.

فيما يتعلق بمستوى الوعي الحالي بالأمن السيبراني واستخدام ممارسات آمنة في هذا المجال،يمكن القول أن المؤسسات التي تنتمي إلى قطاعي النفط والاتصالات والقطاع المصرفي تأخذ المساعدة من الحكومة بشكل منتظم لحماية بياناتها. بالتالي، هناك بعض الوعي بقضايا الأمن السيبراني والحاجة إلى اتباع ممارسات آمنة ضمن هذه القطاعات التي تعتبر حيوية في ليبيا، وينظر إليها على أنها أكثر نضجًا مقارنة بغيرها من حيث الوعي بالأمن السيبراني والممارسة في هذا المجال.

5.3.3. المؤتمرات المحلية :

قامت المؤسسات الحكومية والشركات الخاصة في ليبيا بتنظيم العديد من المؤتمرات على المستويين المحلي والدولي بهدف تبادل المعرفة وتعزيز التعاون في مختلف المجالات، نظرًا لتنوع وكثرة هذه

المؤتمرات، سنركز في هذه الدراسة على بعض المؤتمرات التي تم الإعلان عنها عبر منصات التواصل الاجتماعي والمتوفرة منها، سيتم ذكر بعض الأمثلة على النحو التالي:

- مؤتمر ليبيا الدولي للإنترنت الآمن (الدورة الأولى)، أقيم في 24 مايو 2022م، بمدينة بنغازي، ليبيا. هدف المؤتمر إلى التعرف على الواقع الراهن لدولة ليبيا ومعرفة التحديات التي تواجهها في الفضاء السيبراني وتحديد خطط الارتقاء بها نحو المستقبل للوصول إلى إنترنت آمن. تضمنت الأهداف تعزيز دور المجتمع الليبي والمنظمات الحكومية وغير الحكومية والجهات المعنية عبر التعاون وبذل الجهود المطلوبة للوصول إلى فضاء سيبراني آمن، وتبني الخطط الموضوعية والعلمية، وخلق مجالات للتعاون بين الوزارات والمؤسسات الحكومية والقطاع الخاص لنشر التوعية على المخاطر السيبرانية، والاستعداد لمواجهة المخاطر والتهديدات السيبرانية المختلفة التي قد تتعرض لها منظومة معلومات الدولة، واعتماد الممارسات الأفضل لمواجهة الحوادث الأمنية المحتملة، وتسليط الضوء على النقص والقصور في التشريعات الداخلية والدولية، واقتراح عناصر النهوض بمنظومة قانونية أكثر فاعلية مع البيئة الإلكترونية.
- مؤتمر ليبيا الدولي للأمن السيبراني: أقيم في 21 يناير 2023م، بمدينة بنغازي، ونظمه مجلس الأمن القومي تحت شعار "الأمن القومي والتهديدات السيبرانية في عالم متغير"، شاركت في المؤتمر دول عربية مثل مصر، الأردن، تونس، العراق، الجزائر، المغرب، سوريا، والسودان،، تضمنت توصيات المؤتمر ضرورة توظيف تطبيقات الذكاء الاصطناعي في الدفاع السيبراني عن المجتمع والمنظومات الوطنية المعلوماتية، إضافة إلى تدشين برامج تدريبية لمجلس الأمن القومي الليبي لبناء القدرات الشبابية في مجال الأمن السيبراني. كما شدد المؤتمر على أهمية دور مؤسسات التنشئة الاجتماعية والدينية في حماية الأطفال والمراهقين والمرأة من المخاطر السيبرانية، وتبني تشريعات وقوانين للحماية الفكرية عبر الإنترنت، وتفعيل قوانين حماية البيانات الشخصية، دعا المؤتمر إلى ضرورة مواجهة تصاعد الابتزاز السيبراني، وبناء استراتيجية وطنية للأمن السيبراني بإشراف مجلس الأمن القومي الليبي على غرار الدول العربية، وإعداد خطة للتحول الرقمي لجميع المؤسسات والقطاعات، وإنشاء بنية تحتية للتحولات الرقمية، وفتح مسارات أكاديمية للتخصص النوعي في مجال الأمن السيبراني، وتعزيز الشراكة في مجال الأمن السيبراني بين القطاعين العام والخاص، والتعاون مع الجهات الإقليمية والدولية المعنية بأمن الفضاء السيبراني، أوصى المشاركون العرب بدراسة انضمام ليبيا إلى الاتفاقيات العربية والدولية المعنية بالحماية الإلكترونية، والمشاركة في المؤتمرات والندوات وورش العمل الدولية للاستفادة من التجارب والخبرات المختلفة، والاستعانة بالاتفاقيات الدولية المرتبطة بتشريعات الفضاء السيبراني وضمان تناسقها مع نظيراتها الوطنية(مؤتمر ليبيا الدولي للأمن السيبراني:2023).
- مؤتمر ليبيا الدولي للمخاطر السيبرانية 2023م،، عُقد مؤتمر ليبيا الدولي للمخاطر السيبرانية في دورته الأولى بمدينة طرابلس يومي 30 و31 يناير 2023 تحت شعار "نحو بيئة رقمية آمنة". هدف المؤتمر إلى الارتقاء بالمؤسسات الوطنية من خلال تأهيلها وفق المعايير الدولية لمواجهة الأخطار السيبرانية.

شـــاركت في المؤتمر دول مثل الولايات المتحدة، فرنســـا، البحرين، ودول عربية أخرى (مؤتمر ليبيا الدولي للمخاطر السيبرانية: 2023).

- مؤتمر ليبيا الدولي لمكافحة الإرهاب الســـيبراني 2023م، انطلق مؤتمر ليبيا الدولي الأول لمكافحة الإرهاب الســـيبراني في مدينة بنغازي يوم 9 فبراير 2023 تحت شـــعار "ليبيا تتحدى الإرهاب" هدف المؤتمر إلى التعرف على التحديات الحالية والمســـتقبلية التي تواجه ليبيا في مجال الإرهاب الســـيبراني ووضـــع الخطط الأمنية والعملية المثلى لمواجهتها، شـــملت توصـــيات المؤتمرتطوير الكفاءات الأمنية الوطنية لخبراء مكافحة الإرهاب، وضـــع خطط توعية وتدريب وتأهيل للمهنيين والشـــباب، فتح قنوات تعاون أكاديمية وعلمية مع القطاع الأمني العربي والدولي، تأسيس مرصد عربي متخصص في مكافحة التطرف والإرهـاب الســـيبراني وأخيراً دعم القيـادة العـامـة للقوات المســـلحـة في برنـامج التحول الرقمي(مؤتمر ليبيا الدولي لمكافحة الإرهاب السيبراني: 2023).

اسـتنادًا إلى الجهود التي بذلتها الحكومة الليبية في تعزيز المؤسـسـات الحكومية، بالإضـافة إلى الإجراءات المتعددة التي ربما لم تتناولها الدراســـة، يمكن القول إن ليبيا قد حققت تقدمًا ملحوظًا في مؤشـــر الأمن السـيبراني وفقًا للاتحاد الدولي للاتصـالات (ITU) يتجلى هذا التقدم من خلال التحسـينات المسـتمرة التي سجلتها البلاد منذ أول إصدار للمؤشر عام 2015 وحتى آخر تحديث له في عام 2024، يعكس هذا التطور التزام الحكومة الليبية بتعزيز البنية التحتية الرقمية وتطوير السـياسـات اللازمة لحماية المعلومات والبيانات الحسـاسـة، فيما يلي مقارنة بين تصنيفات ليبيا في مؤشر الأمن السيبراني العالمي (GCI) بين عامي 2015 و2024م:

- عام 2015م، سـجلت ليبيا فعالميًا في مؤشـر الأمن السـيبراني العالمي(GCI) نسـبة التأهب السـيبراني وجاءت المرتبة 19 عالميا من أصـل 29 درجة على مسـتوى العالم، وحسـب الترتيب الإقليمي سـجلت مرتبة 18 إقليميا، وهو أول إصـدار لهذا المؤشـر، (الرقم القياسـي العالمي للأمن السـيبراني وسـمات السلامة السيبرانية:286:2015-288).قد صنف هذا المؤشر بناء على هذه الإجراءات :

- التدابير القانونيـة: لم تكن هنـاك تشـــريعـات محـددة تتعلق بـالجرائم الإلكترونيـة أو متطلبـات تنظيميـة وامتثالية محددة للأمن السيبراني.
- التدابير الفنية: طلبت ليبيا المساعدة من الاتحاد الدولي للاتصالات لإنشاء فريق

وطني للاســـتجابـة للطوارئ الحاســـوبيـة(CERT) ، الذي بدأ عمله في فبراير 2013 تحت مظلة الهيئة الوطنية لأمن المعلومات والسلامة.(NISSA)

- المعايير: لم تكن هناك أطر وطنية معترف بها رسميًا لتنفيذ معايير الأمن السيبراني المعترف بها دوليًا، ولا شهادات أو اعتمادات للوكالات الوطنية والمتخصصين في القطاع العام.
- التدابير التنظيمية: لم تكن هناك استراتيجية وطنية معترف بها رسميًا للأمن السيبراني أو خارطة طريق وطنية لحوكمة الأمن السيبراني.

- بناء القدرات: لم يكن هناك برامج أو مشاريع بحث وتطوير معترف بها رسميًا لمعايير الأمن السيبراني، باستثناء بعض الجهود من الهيئة العامة لأمن وسلامة المعلومات لتنفيذ برنامج وطني لرفع الوعي وتعزيز البرنامج التعليمي للأمن السيبراني.
- التعاون الدولي: اعترفت ليبيا بشراكاتها مع منظمات دولية مثل غرفة التجارة الوطنية الأمريكية العربية وشركة Alcatel-Lucent، وشاركت في برامج مثل ITU-IMPACT 2012 وAfrica-CERT وOIC-CERT وSANS و EC-Council

- عام 2017م، حصلت ليبيا على المرتبة 104 عالميًا في مؤشر الاتحاد الدولي للاتصالات (ITU) لقياس جاهزية الدول في التعامل مع التهديدات السيبرانية، مما يضعها ضمن الدول ذات الأداء المنخفض في الأمن السيبراني مقارنة بمتوسط الترتيب العالمي، أما بالنسبة للجهود المبذولة تضمنت إنشاء فريق استجابة للطوارئ، تنفيذ بعض التدابير التنظيمية، إطلاق حملات توعية عامة، تقديم دورات تدريبية مهنية، وبناء القدرات، كما شاركت ليبيا في بعض المبادرات الدولية غير المحددة(Global cybersecurty index:2017:2017:31).
- عام 2018م، استمرت ليبيا في الأداء المنخفض، حيث جاءت في المرتبة 117 عالميًا من بين 194 دولة، والمرتبة 16 إقليميًا، أما لجهود المبذولة استندت هذه المرتبة إلى المعلومات المقدمة من الحكومة الليبية، والتي تضمنت الإجراءات المذكورة أعلاه (Global cybersecurty index:2018:58).
- عام 2020م، تحصلت ليبيا على المرتبة 113 من أصل 149 دولة ممثلة عربيًا ودوليًا، والمرتبة 14 من أصل 22 دولة عربية، أشار تقرير مؤشر الأمن السيبراني العالمي إلى أن التدابير التقنية والتعاونية كانت مجالات قوة، بينما كانت التدابير القانونية والتنظيمية مجالات تحتاج إلى نمو(الرقم القياسي العالمي للأمن السيبراني::2020) :29 كم موضح في الشكل رقم (11) .

الدرجة الإجمالية	التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	التدابير التعاونية
28,78	3,73	8,54	3,13	5,34	8,04

الشكل رقم (11)، الرقم القياسي العالمي للأمن السيبراني لعام 2020 ، المصدر مؤشر الاتحاد الدولي للاتصالات 2020

تُظهر الدرجات الموضحة في الشكل بالنسبة للتدابير القانونية بدرجة (3.73) وهذا تعكس ضعف التشريعات والقوانين المتعلقة بالأمن السيبراني، بينما تشير التدابير التنظيمية (3.13) إلى غياب أو ضعف السياسات

التنظيمية اللازمة، على الرغم من الأداء العام الضعيف، فإن التدابير التقنية (8.54) تُظهر محاولات لتطوير البنية التحتية الرقمية، في حين أن بناء القدرات (5.34) يعكس قلة البرامج التدريبية والتوعوية أخيرًا، تُعتبر التدابير التعاونية (8.04) مقبولة نسبيًا، حيث يسهم التعاون مع الدول الأخرى والمنظمات الدولية في تعزيز قدرات ليبيا للتعامل مع التهديدات السيبرانية.

وتأتي الدرجة الإجمالية:(28.78) المنخفضة تؤكد على الحاجة الماسة إلى وضع استراتيجية شاملة لتحسين جميع الجوانب المتعلقة بالأمن السيبراني وبهذا يمكن القول بأن ليبيا بحاجة إلى وضع خطة تتضمن تحسين التشريعات، وتعزيز البنية التحتية، ورفع مستوى التدريب، وتوسيع التعاون الدولي.

- عام 2024م، وفقًا لمؤشر الأمن السيبراني العالمي لعام 2024، يتم تقسيم الدول العربية إلى خمس فئات تعكس مدى تقدمها في الأمن السيبراني، حسب المؤشر تقع ليبيا ضمن الفئة "T3(Evolving)" من الدول التي أحرزت بعض التقدم لكنها لا تزال في مرحلة التطوير، ويشير هذا التصنيف إلى أن ليبيا نجحت في وضع بعض الأسس في مجال الأمن السيبراني، مثل وجود إجراءات تقنية أو تعاون دولي محدود، ويعكس تقدمًا نسبيًا لكنه يشير أيضًا إلى وجود فجوات تحتاج إلى معالجة لتحسين أدائها والوصول إلى الفئات الأعلى، ويشمل خمسة محاور رئيسية مع بيان نقاط القوة ومجالات التحسين، بالنسبة للتدابير القانونية الدرجة 20/16.75 تُظهر ليبيا أداءً جيدًا نسبيًا في هذا المحور، حيث لديها بعض التشريعات المتعلقة بالأمن السيبراني، اما التدابير التقنية الدرجة 20/11.2 وتُظهر الدرجة أن ليبيا لديها أسس تقنية لكنها بحاجة إلى تحسينات كبيرة في هذا المجال مثل تعزيز البنية التحتية التقنية وزيادة الاعتماد على أنظمة متطورة بالإضافة إلى التدابير التنظيمية الدرجة 20/14، يُظهر هذا المحور أن ليبيا لديها بعض الهياكل التنظيمية لكنها بحاجة إلى هيئات أكثر تخصصًا وقوة لإدارة الأمن السيبراني بفعالية، أما تطوير القدرات الدرجة 20/15.75 يعد هذا أحد المحاور التي تُظهر فيها ليبيا أداءً قويًا نسبيًا، ما يدل على الجهود المبذولة في بناء قدرات الأفراد والمؤسسات، أخيراً التدابير التعاوني الدرجة 20/10.39 تُعد التدابير التعاونية من أضعف المجالات في ليبيا، مما يشير إلى الحاجة لتعزيز التعاون مع الدول الأخرى والمنظمات الدولية(Global cybersecurity index: 2024).

تشير مناطق القوة في ليبيا، مثل التدابير التقنية وتطوير القدرات، إلى أن البلاد تمتلك أساسيات قوية في البنية التحتية والتدريب، لكنها تحتاج إلى تعزيز هذه الجوانب للوصول إلى مستويات أعلى. أما بالنسبة لمناطق النمو المحتمل، مثل التدابير القانونية والتنظيمية والتعاونية، فإنها تُظهر الحاجة إلى تحسين السياسات والقوانين وتوسيع نطاق التعاون الدولي والمحلي، من هذا المنطلق، يمكن القول أن ليبيا تحقق تقدمًا في بعض المجالات مثل "تطوير القدرات" و"التدابير التقنية"، لكنها تواجه تحديات كبيرة في مجالات التعاون والتنظيم. تحسين هذه الجوانب سيعزز من موقع ليبيا في التصنيف العالمي ويزيد من قدرتها على مواجهة التهديدات السيبرانية.

نستنتج بأن ليبيا حققت تقدمًا ملحوظًا في مجال الأمن السيبراني بين عام 2015م إلى 2024م، مما يعكس جهودها المستمرة لتعزيز الأمان السيبراني لمواجهة التهديدات الرقمية ومع ذلك، لا تزال ليبيا في مرحلة التطوير وتحتاج إلى جهود إضافية للارتقاء بمستوى قدراتها وتعزيز أدائها في هذا المجال .

4.3.إطار بناء مقترح استراتيجية وطنية للأمن السيبراني في ليبيا

يُعد الفضاء الإلكتروني نقطة الانطلاقة لصياغة الاستراتيجية السيبرانية، فمن خلال الطريقة التي يوضع بها الفضاء، تنبع وجهات النظر التي تعتمدها في المجال المادي وغير المادي الذي يتكون وينتج عن عناصر هي أجهزة الكمبيوتر، الشبكات، البرمجيات، حوسبة المعلومات، المحتوى، ومستخدمي كل هذه العناصر (الاتحاد الدولي للاتصالات:2011). وانطلاقا من هذه الاعتبارات حول طبيعة الفضاء الإلكتروني نحن بحاجة إلى استراتيجية وطنية تحمي هذا الفضاء، ويمكن النظر إلى الاستراتيجيات السيبرانية التي صيغت في السنوات الأخيرة بوصفها استراتيجيات متطورة اذ انها تمثل الجيل الجديد من الاستراتيجيات التي يمكن اعتبارها الامتداد الطبيعي للوثائق التي نشرت على مدار عشرين سنة الماضية، ومن الممكن أن تكون الاستراتيجية السيبرانية وطنية، دولية، إقليمية وامنية ودفاعية متخصصة في مكافحة الجريمة السيبرانية والهجومية كما يمكن أن ترتبط بالاعتداء والقوة والحرب السيبرانية والصراع السيبراني فضلا عن انها تعد وقائية ونشطة واستباقية وعمومية وشاملة وقد تعمل على تحديد وسائل، أو طرق الكشف عن الهجمات، أو الردع، أو الرد على الهجمات السيبرانية (هينروتين وأخرون:2019:70). وتشترك أنجح الاستراتيجيات الوطنية في ثلاث خصائص مهمة هي:

أولا، يتم إدراجها في وثائق حية تم تطويرها وتنفيذها بالشراكة مع أصحاب المصلحة الرئيسيين من القطاعين العام والخاص.

ثانيا، تستند إلى مبادئ واضحة المعالم تعكس القيم المجتمعية والتقاليد والمبادئ القانونية.

ثالثا، تستند الاستراتيجيات إلى نهج إدارة المخاطر حيث تتفق الحكومات والشركاء من القطاع الخاص على المخاطر التي يجب إدارتها أو تخفيفها، وحتى تلك التي يجب قبولها (Microsoft developing a national strategy for cybersecurty:2013).

في ليبيا قامت الهيئة العامة لأمن وسلامة المعلومات بإعداد الاستراتيجية تنفيذا لاختصاصاتها المحددة في قرارها الذي قضي في مادته الرابعة باختصاص الهيئة بالقيام بأعداد الاستراتيجيات والسياسات المتعلقة بأمن وسلامة المعلومات والاتصالات، رغم أنها نقطة البداية وأول استراتيجية وطنية في ليبيا الا أنها واجهت تحديات كبيرة في التنفيذ، لكونها تفتقر إلى فعالية التنفيذ نتيجة لغياب خطة عمل شاملة ومحددة مما أدى إلى ضعف فعاليتها، لذلك يتطلب الوضع الحالي تحليلًا دقيقًا للاستراتيجية القديمة وتقديم اقتراحات لتطويرها من خلال إضافة خطة عمل شاملة وإجراءات دقيقة ومواعيد محدده واضحة لضمان تحقيق أهداف الأمن السيبراني وتعزيز توافقها مع المعايير الدولية المعترف بها وتكون ليبيا دولة رائدة في مجال الأمن السيبراني.

تسعى هذه الدراسة لتقديم مقترح لوضع إطار بناء استراتيجية وطنية شاملة للأمن السيبراني أن من شأنها أن تؤسس منظومة وطنية متكاملة للأمن السيبراني تكون متسقة مع أبرز الممارسات الدولية المتميزة في هذا المجال ،وأن تبني منهجا شاملاً يمكن جميع الجهات من رفع مستوى امنها السيبراني وحماية شبكاتها وأنظمتها وبياناتها الإلكترونية وأن تسهم في تطوير مبادئ الأمن السيبراني وتعزيز إدراك المؤسسات والأفراد لمسؤولياتهم الوطنية تجاهه ومن شأنها كذلك أن تحقق مستوى عالياً من النضج والمهنية في الممارسات وفق مسؤولية كل جهة من أمنها السيبراني وأيضا تسهم في حماية الأمن القومي الليبي وتأسيس قدرات للدافع عن ثروات ليبيا وعرقلة أنشطة الجهات الفاعلة الخبيثة والاستثمار في منظومة رقمية أكثر أماناً، حيث اشتمل إعداد مقترح إطار بناء الاستراتيجية على المراجع والخطوات الأساسية التالية:

1. الرجوع إلى تجارب الدول الرائدة حسب مؤشر الأمن السيبراني الصادر عن الاتحاد الدولي للاتصالات سنة 2024، الذي يقيس التزام الدول بالأمن السيبراني، تم اختيار الدول الأهم على المستويات الإقليمية والدولية والعربية والريادية، حيث تمت دراسة تجارب الولايات المتحدة والمملكة المتحدة، والمملكة العربية السعودية، وإستونيا وموريشيوس.
2. دليل صنع السياسات (2020) الذي يركز على إشراك أصحاب المصلحة في استراتيجيات الأمن السيبراني الوطنية، الصادر عن الشركاء العالميون الرقميون.
3. دليل تطوير استراتيجية وطنية للأمن السيبراني الصادر عن شركة مايكروسوفت (Microsoft) في عام 2013.
4. المبادئ التوجيهية لاستراتيجية الأمن السيبراني الوطنية، منظمة حلف شمال الاطلسي (الناتو) الصادر عن مركز التميز الفاعي السيبراني التعاوني التباع لحلف شال الاطلسي ، 2013.
5. دليل استراتيجيات الأمن السيبراني الوطنية الصادر عن منظمة الدول الأمريكية(2022)
6. دليل الممارسات الجيدة لتطوير استراتيجية الأمن السيبراني الوطنية الصادر عن مجلس الاتحاد الأوروبي لوكالة الشبكات والمعلومات (ENISA) في نوفمبر 2016.
7. الاستراتيجية العربية للأمن السيبراني (2023-2027) الصادرة عن جامعة الدول العربية والمنظمة العربية لتكنولوجيا الاتصالات والمعلومات في 24 يناير 2024.
8. دليل إعداد الاستراتيجيات الوطنية للأمن السيبراني، بمشاركة أكثر من أثني عشر شريكًا في الإصدارين الأول والثاني، وشملت هذه المشاركة المنظمات الحكومية، والدولية، والخاصة، بالإضافة إلى الأكاديميين والجمعيات المدنية التي تمثل بعض الجهات البارزة في هذا الجهد الاتحاد الدولي للاتصالات، والبنك الدولي، وأمانة الكومنولث، ومركز التميز التعاوني للدفاع السيبراني التابع لحلف شمال الأطلسي، بالإضافة إلى جهات أخرى، تم تنفيذ هذا العمل خلال فتريين عام 2018 و عام 2021.
9. الاستراتيجية الصادرة عن الهيئة العامة لأمن وسلامة المعلومات الصادرة سنة 2023. وأيضا تم الاستعانة ببعض الوثائق الوطنية.

10. من خلال توظيف أدوات تحليلية متقدمة مثل SWOT وPESTEL، بالإضافة إلى استخدام أسلوب المقابلات الشخصية مع الكوادر القيادية في مجالي إدارة أمن المعلومات والأمن السيبراني في المؤسسات العامة والخاصة في ليبيا، وبدراسة أبرز الهجمات والتهديدات والمخاطر السيبرانية العالمية والإقليمية والمحلية ومدى تأثيرها.

يهدف هذا المقترح إلى التصدي للمخاطر المتعلقة بالتهديدات السيبرانية، وتعزيز الثقه في بيئة الإنترنت، وزيادة الوعي بأمن السيبراني لدى افراد المجتمع، مع مشاركة وتمكين الليبيين من تأمين أجزاء الفضاء الإلكتروني الذي يمتلكونه، أو يعملون فيه، أو يسيطرون عليه، أو حتى يتفاعلون معه، كما يُعتبر تأمين هذا الفضاء يُعد تحديًا استراتيجيًا معقدًا يتطلب تنسيقًا وتركيزًا من مجتمعنا بأسره.

إن دعم تنفيذ هذه الاستراتيجية على أرض الواقع وتمويلها من السلطة التنفيذية سيكون عاملًا معززًا لجهود ليبيا في المحافظة على منظومة الأمن والأمان وتعزيزها، بالإضافة إلى رفع مستوى الأمن السيبراني. يهدف مقترح الاستراتيجية إلى أن يكون إطارًا وطنيًا لدعم الجهود الحكومية وتطوير البنية التحتية التي تضمن النهوض بدولتنا على مدى خمس سنوات(2025-2029) وتشمل أهدافاً محددة وخطة عمل مفصلة ومؤشرات أداء لقياس التقدم، يستند مقترح الاستراتيجية إلى أفضل الممارسات لتعزيز أمن الفضاء السيبراني لليبيا و أيضًا إلى تحويل ليبيا إلى واحدة من الدول الرائدة في الأمن السيبراني خلال السنوات القادمة، بطموح شعبها وقادتها.

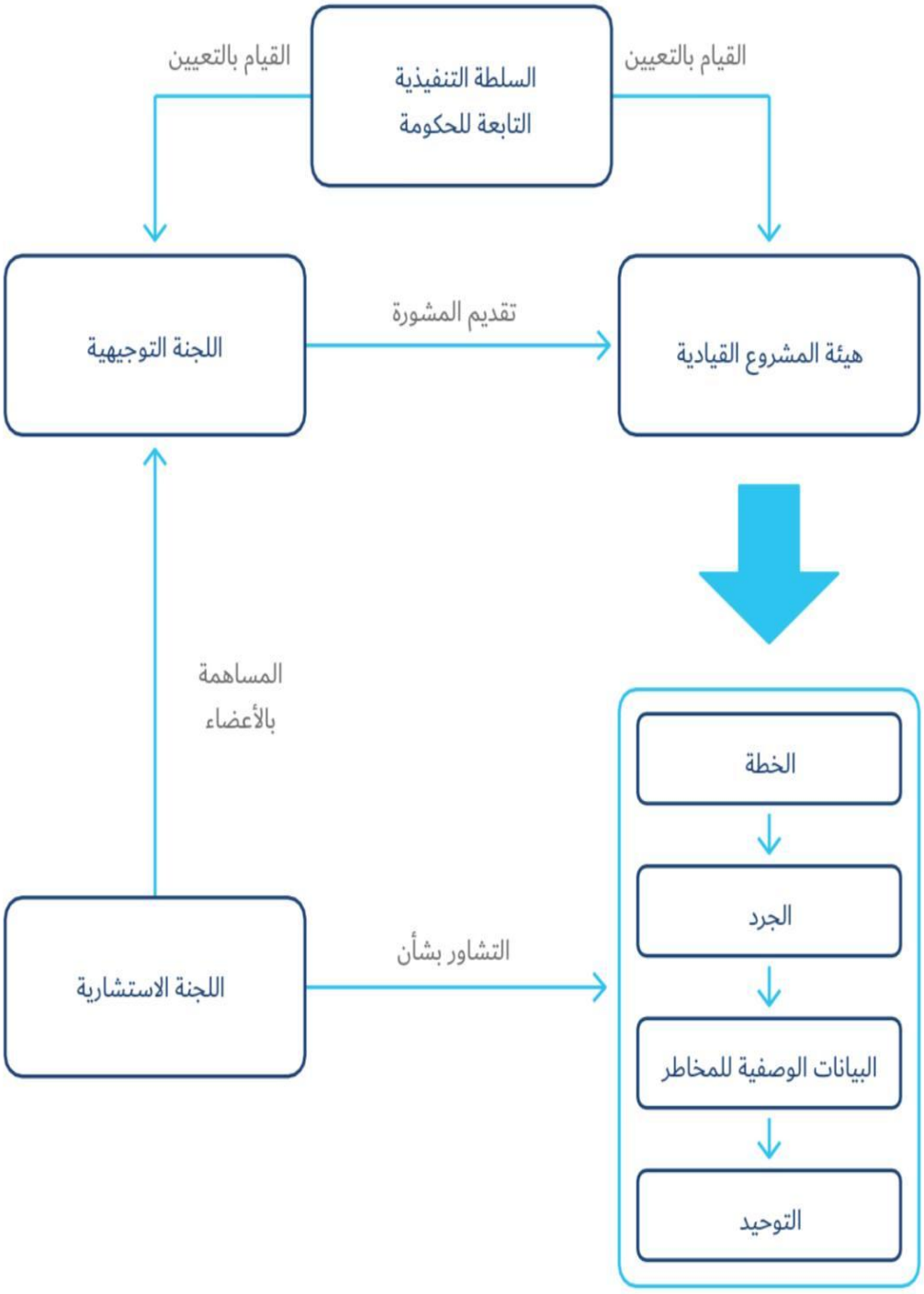
1.4.3. مراحل بناء الاستراتيجية :

1.1.4.3. المرحلة الأولى الاستهلال :

1. تحديد الجهة المسؤولة عن تنفيذ مقترح الاستراتيجية :

في المرحلة الأولى من تنفيذ مقترح الاستراتيجية، يجب تحديد الجهة المسؤولة عن التنفيذ، يُوصى بأن تقوم السلطة التنفيذية بتشكيل لجنة توجيهية متخصصة تحت إشراف مجلس رئاسة الوزراء والمجلس الرئاسي كما موضح في الشكل رقم(12)، تتولى إنشاء مجلس وطني للأمن السيبراني (هيئة المشروع القيادية) ينبغي أن يتمتع هذا المجلس بصلاحيات سيادية مستقلة، وأن تكون رئاسة هذا المجس من ثلاث مؤسسات حكومية هي وزارة الدفاع، ووزارة الداخلية، مجلس الأمن القومي، يجب أن يتم اختيار رئيس المجلس ونائبه من قبل السلطة التشريعية وان يكون مجلس الأمن السيبراني تحت قيادة المجلس الرئاسي(تابع له)، ليكون مسؤول عن تقييم وتنفيذ مقترح الاستراتيجية الوطنية للأمن السيبراني، لكون الأمن السيبراني هو خط الدفاع الأول عن الأمن القومي الليبي.

يجب أن تشارك الهيئة العامة لأمن وسلامة المعلومات في إعداد هذه الاستراتيجية، وأن تُكلف بمهام محددة تُحال إليها من قبل رئيس المجلس الوطني للأمن السيبراني، كما يجب أن يشارك جميع أصحاب المصلحة في الدولة الليبية في تقييم مقترح الاستراتيجية كما هو موضح في الشكل رقم (13)،



الشكل رقم(12) دورة حياة مقترح الاستراتيجية، المصدر: دليل إعداد الاستراتيجيات الوطنية للأمن السيبراني(2021)

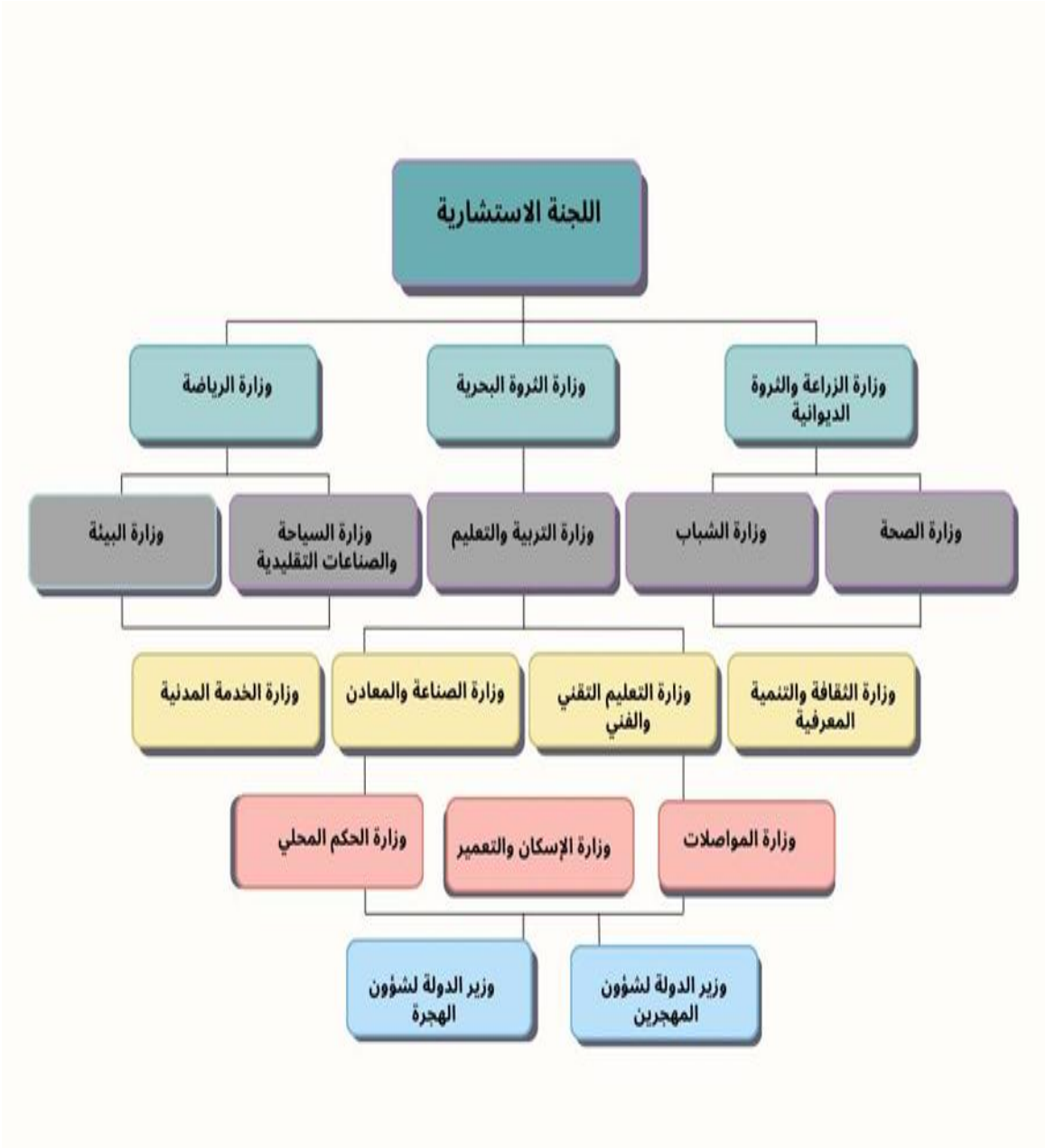
حيث تُحدد أدوارهم ومسؤولياتهم وحقوقهم في اتخاذ القرارات وكيفية تعاونهم خلال فترة تقييم الاستراتيجية من جانبها، يجب على السلطة التنفيذية ضمان التمويل اللازم لكامل دورة الاستراتيجية، ويجب على المجلس الوطني للأمن السيبراني الحفاظ على الاتصال المستمر مع اللجنة التوجيهية لضمان الاستفادة من جميع المعارف والخبرات المتاحة.

المصدر من إعداد الباحثة الشكل (13) أصحاب المصلحة

2. إنشاء لجنة استشارية

ستقوم السلطة التنفيذية بإنشاء لجنة استشارية للعمل بالتعاون مع المجلس الوطني لتقييم مقترح الاستراتيجية، حيث ستضم جميع المؤسسات الحكومية التي لم تشارك في المرحلة الأولى كما هو موضح في الشكل

رقم(14)، سيتم تحديد وتأكيد تفويض ومهام الكيانات المسؤولة عن المشاريع والمبادرات في مجال الأمن السيبراني، وسيتم شرح كيفية تفاعلها ومساهمتها في اللجنة الاستشارية استنادًا إلى خبراتهم ومهاراتهم في هذا المجال، سيتم توزيع الأدوار والمسؤوليات على جميع أعضاء اللجنة، بدءًا من رئيس اللجنة ونائب الرئيس ومنسقي الفرق الفرعية التي تركز على جوانب مختلفة من الاستراتيجية، يتعين تمكينهم لتقديم التوجيه للمجلس الوطني، ويمكن أن يتحقق ذلك من خلال مجموعة متنوعة من الالتزامات، بما في ذلك الاستشارات عبر الإنترنت أو ورش العمل لإقرار الصلاحيات ويتوقع أن تستعمل التعقيبات والتعليقات الناتجة عن هذه العملية لوضع اللمسات النهائية للاستراتيجية.



الشكل رقم(14) اللجنة الاستشارية المصدر من إعداد الباحثة

يجب على أعضاء اللجنة الالتزام بالشفافية والشمولية في عملية التوجيه، وعلى كل عضو تحمل المسؤولية المسندة له من أجل تحقيق الأهداف المرجوة.

3. تخطيط وضع الاستراتيجية

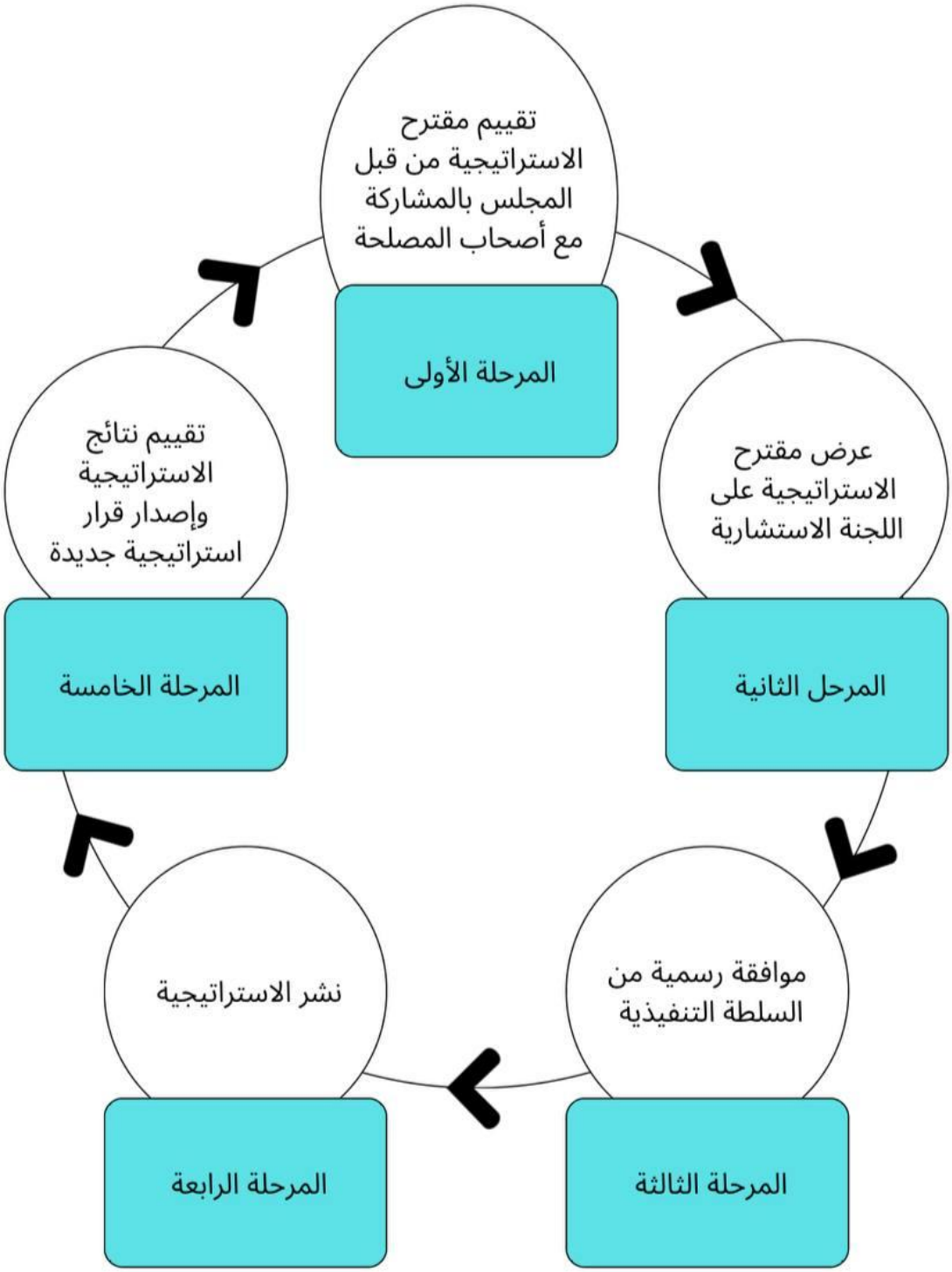
يجب على المجلس، في مرحلة الاستهلال، تقديم مقترح الاستراتيجية إلى اللجنة التوجيهية لمراجعته، وبعد الموافقة عليه، يتم إحالته إلى السلطة التشريعية للمصادقة عليه، ومن ثم تنفيذه وفقًا لذلك كما هو موضح في الشكل رقم(15)، فيما بعد، يتوجب على المجلس مُراقبة التقدم المحرز في تنفيذ الاستراتيجية بانتظام وفق جدول زمني متفق عليه طوال دورة حياة الاستراتيجية، تتضمن حصيلة نشاط المراقبة تقريرًا يُشير، على سبيل المثال، إلى أي انحرافات عن الجداول الزمنية المتفق عليها وأسباب أي تأخير، يتعين على كل من أصحاب المصلحة المشاركة في مراقبة الاستراتيجية بمشاركة فعّالة، مما سيضمن تحملهم المسؤولية المحددة لتحقيق الأهداف المطلوبة. كما سيسهل هذا النهج تحديد التحديات المحتملة المبكرة يتعلق بتنفيذ الاستراتيجية، وستتيح للحكومة إما تصويب الوضع أو تعديل خططها وفقًا للتجارب المكتسبة أثناء التنفيذ.

بالإضافة إلى ذلك، من الأهمية بمكان إجراء تقييم دوري للنتائج ومقارنتها بالأهداف الأصلية لفهم مدى تحقيق أهداف الاستراتيجية واستعداد لأي تعديلات ضرورية، ينبغي تجميع التقييمات ذات الصلة في تقرير يُعرض للمجلس الوطني، يحتوي على توصيات لتحديث خطة العمل وضمان سريانها والتكيف مع التحديات المتغيرة. في النهاية ، يجب أن تشكل التقارير خلال دورة حياة الاستراتيجية أساسًا لاستعراض شامل لاستراتيجية الأمن السيبراني الوطنية وفقًا للجدول الزمني المحدد خلال مرحلة التأسيس، ينبغي ألا يقتصر الاستعراض الشامل على التقدم المحقق والتغييرات في البيئة الخارجية، بل ينبغي أيضًا إعادة تقييم أولويات الحكومة وأهدافها. .

2.1.4.3. المرحلة الثانية: الجرد والتحليل

سيتم في المرحلة الثانية، وهي مرحلة الجرد والتحليل، تقييم المشهد الوطني للأمن السيبراني في ليبيا وستتضمن هذه العملية دراسة شاملة على مستوى الدولة باستخدام منهجية إعداد الاستراتيجية التي تتضمن الأدوات التالية:

- **أداة تحليل بيستل (PESTLE)** هي أحد الأدوات التي تسهم في تحديد ودراسة المتغيرات الخارجية التي تؤثر على الدولة سواء صورة إيجابية أو سلبية، بهدف جمع وتوفير البيانات اللازمة لاتخاذ القرارات الاستراتيجية عند تنفيذ الخطة الاستراتيجية لتحقيق الأهداف المرجوة، ويأتي تحليل PESTLE اختصارا لستة عوامل رئيسية وهي العوامل السياسية والاقتصادية والاجتماعية والتكنولوجية والبيئية والقانونية كما موضح في الجدول رقم(1)، وهي تساعد على فهم السياق الخارجي الذي يمكن أن يؤثر على استراتيجية الأمن السيبراني في ليبيا.



الشكل رقم (15) مراحل تنفيذ الاستراتيجية الوطنية للأمن السيبراني، المصدر من إعداد الباحثة

جدول رقم (1) تحليل بيستل(PESTLE)

عوامل تحليل بيستل	العوامل المؤثرة	الأمثلة	تقييم التأثير
العوامل السياسية Political Factors	عدم الاستقرار السياسي والأمني.	ليبيا تعاني من عدم استقرار سياسي وأمني منذ ثورة 2011، مما أدى إلى صعوبة في تنفيذ السياسات الوطنية بشكل فعال و قد أدى ذلك إلى انقسام السلطة في البلاد، وسبب في ضعف التعاون بين الأطراف المعنية، وأثر سلبًا على ثقة المجتمع الدولي في القدرة والجدية في ليبيا على حماية بياناتها وتعزيز الأمن السيبراني .مما يجعل من الصعب وضع استراتيجية سيبرانية موحدة وفعالة دون وحدة الرؤية والتنفيذ.	سلبي قوي، حيث يؤدي إلى بيئة غير مستقرة تزيد من التهديدات السيبرانية.
	التزام بالتعاون الدولي.	يلزم تعاون ليبيا مع الجهات الدولية في مجال مكافحة الجرائم السيبرانية بالانضمام للمنظمات الدولية وإمكانية الاستفادة من الخبرات الدولية والتعاون مع منظمات مثل الاتحاد الدولي للاتصالات.	إيجابي، حيث يمكن أن يؤدي إلى تبادل المعلومات والخبرات وتقليل التهديدات.
	إرادة سياسية بناءة.	وجود إرادة سياسية قوية لتعزيز الأمن السيبراني وحماية البنية التحتية الرقمية في البلاد.	إيجابي، حيث يمكن أن يؤدي إلى تحسين البنية التحتية للأمن السيبراني.
	تعزيز الشرعية السياسية.	. من خلال إجراء الانتخابات الديمقراطية، يتم تعزيز الشرعية السياسية للحكومة المنتخبة، مما يسهل تطبيق السياسات والإجراءات اللازمة لتعزيز الأمن السيبراني.	إيجابي، حيث يمكن أن يعزز من الالتزام بالسياسات الأمنية.
	التقسيمات السياسية. الداخلية.	الانقسامات السياسية الداخلية بين الشرق والغرب والجنوب أدي إلى صعوبة في توحيد الجهود الوطنية لمكافحة التهديدات السيبرانية على سبيل المثال، في الغرب الليبي، توجد القوات التي تدعمها حكومة الوحدة الوطنية برئاسة عبد الحميد الدبيبة، بينما في الشرق الليبي، تنافس هذه الحكومة الفصائل المسلحة المنضوية تحت قيادة خليفة حفتر هذا التقسيم قد أدى إلى تشتت الجهود الأمنية وصعوبة تحقيق وحدة في وضع استراتيجية أمن سيبراني موحدة للبلاد.	سلبي، حيث يمكن أن يؤدي إلى ضعف التنسيق بين الجهات المختلفة.
	التدخل الخارجي.	.يشهد الصراع الليبي تدخلات خارجية تزيد من التوترات، حيث	سلبي قوي، حيث يمكن أن يؤدي إلى زيادة الهجمات السيبرانية.
	فقدان الثقة في المؤسسات.	تشهد ليبيا تدخلات من دول مختلفة مثل تركيا وروسيا والإمارات العربية المتحدة ومصر وغيرها، حيث تقدم هذه الدول الدعم لأطراف محددة داخل البلاد على سبيل المثال، تقدم تركيا الدعم لحكومة الوحدة الوطنية في طرابلس، بينما تقدم دول أخرى مثل روسيا الدعم للفصائل المسلحة في شرق ليبيا بقيادة خليفة حفتر، وأيضا الدعم العسكري والمالي الذي تقدمه بعض الدول للجماعات المسلحة يزيد من قدرتها على تنفيذ هجمات سيبرانية ضد الحكومة والمؤسسات الوطنية هذه التدخلات الأجنبية تزيد من التوترات السياسية وتعقد	سلبي، حيث يمكن أن يؤدي إلى ضعف في تنفيذ السياسات.

		المشهد الليبي، مما يجعل عملية وضع استراتيجية امن سيبراني فعالة اكثر صعوبة وتحديًا وقد تعيق الجهود المبذولة في هذا الصدد	
	السياسات الأمنية الوطنية.	تعاني ليبيا من فقدان الثقة في المؤسسات الرسمية، مما يؤثر على القدرة على وضع وتنفيذ استراتيجيات الأمن السيبراني مثال على ذلك، عدم القدرة على توحيد الجهود بين المؤسسات السيادية و الحكومة والمجتمع المدني والقطاع الخاص، لاسيما ان كل جهة تخدم داخل نطاقها الداخلي.	إيجابي، حيث يمكن أن يعزز من الحماية السيبرانية.
	مستوى قوة الحكومة المركزية.	توجد السياسات الصادرة عن الهيئة العامة لأمن وسلامة المعلومات ولكن عدم تنفيذ هذه السياسات يؤدي إلى خسائر اقتصادية هائلة ويؤثر سلبًا على سمعة الدولة على المستوى الدولي، ويزيد من تعرض المؤسسات الحكومية في ليبيا لخطر الاختراقات السيبرانية والهجمات الإلكترونية، وعدم حماية البيانات الحكومية والمؤسسات الحيوية يؤثر على السيادة الوطنية ويمكن أن يصل إلى الحياة اليومية للمواطنين، ويؤدي إلى تعرض بياناتهم الشخصية والمالية للخطر، ويكون له تأثير كبير على الدولة ومواطنيها، وقد يؤدي إلى تبعات خطيرة على الأمن الاقتصادي والوطني.	سلبي، حيث يمكن أن يؤدي إلى بيئة غير محمية.
	مستوى الفساد وعدم الشفافية.	منذ سقوط نظام الرئيس الراحل معمر القذافي، ظهرت هشاشة الهياكل الحكومية في ليبيا، وعدم قدة الحكومات المتعاقبة في توفير الخدمات الأساسية بشكل مناسب للمواطنين والمؤسسات الحكومية وتعزيز الأمن السيبراني .	سلبي قوي، حيث يمكن أن يؤدي إلى ضعف في الحماية السيبرانية.
	نفوذ الجماعات المسلحة.	انتشار مستوى الفساد وعدم الشفافية في مؤسسات الدولة الليبية يؤدي إلى استنزاف الموارد العامة وتفشي ظاهرة الرشوة والإهمال والمحاصصة، وعدم توفير الخدمات الضرورية يؤدي إلى فقدان الثقة في هذه المؤسسات، ويعيق جهود مكافحة التهديدات السيبرانية ويضعف من فعالية الاستراتيجيات الأمنية.	سلبي قوي، حيث يمكن أن يؤدي إلى زيادة الهجمات السيبرانية.
العوامل الاقتصادية Economic Factors	الاستفادة من الثروات الطبيعية.	يمكن استخدام الثروات الطبيعية في ليبيا - مثل النفط والغاز - كمورد اقتصادي لتعزيز الاستثمار في تكنولوجيا المعلومات وتعزيز أمن البنية التحتية السيبرانية.	إيجابي، حيث يمكن ان يوفر التمويل اللازم لتطوير البنية التحتية السيبرانية.
	استخدام التكنولوجيا لحماية الموارد الطبيعية.	يمكن توظيف التكنولوجيا المتقدمة، مثل أنظمة المراقبة الذكية وتحليل البيانات، لحماية الموارد الطبيعية الهامة في ليبيا من التهديدات السيبرانية	إيجابي، حيث يمكن ان يعزز من القدرات السيبرانية ويقلل من التهديدات.
	الاستثمارات في البنية التحتية الرقمية.	زيادة الاستثمارات في البنية التحتية الرقمية يمكن أن تعزز من قدرات الأمن السيبراني وتوفر موارد مالية وتقنية لتطوير الحلول الأمنية.	إيجابي قوي، حيث يمكن ان يعزز من القدرات السيبرانية ويحسن من الحماية.
	نقص التمويل والموارد للمؤسسات الحكومية.	قد يكون نقص الميزانية والموارد المخصصة للأمن السيبراني عاملاً رئيسياً يعيق تعزيز الأمن السيبراني.	سلبي، حيث يمكن ان يعيق تنفيذ استراتيجيات الامن السيبراني.

	معدلات البطالة .	ارتفاع معدلات البطالة، خاصة بين الشباب، يؤدي إلى زيادة الفقر وعدم الاستقرار الاقتصادي، مما يؤثر على القدرة على الاستثمار في الأمن السيبراني وقلة الموارد المتاحة لتعزيزه.	سلبي، حيث يمكن ان يؤدي إلى زيادة الجرائم السيبرانية بسبب نقص الفرص الاقتصادية.
	معدلات النمو الاقتصادي.	الوضع الاقتصادي في ليبيا مازال يواجه تحديات كبيرة ولا يمكن تحديد مدى ارتفاع النمو الاقتصادي بدقة في الوقت الحالي.	متنوع، حيث يمكن ان يؤثر على الاستثمارات في الامن السيبراني.
	التضخم وارتفاع الأسعار.	التضخم وارتفاع الأسعار يؤثران على القوة الشرائية للأفراد والمؤسسات، مما يحد من القدرة على الاستثمار في التكنولوجيا والأمن السيبراني	سلبي، حيث يمكن ان يقلل من القدرة الشرائية ويؤثر على تمويل الأمن السيبراني.
	اسعار الصرف وأسعار الفائدة.	نقص قيمة الدينار مقابل النقد الاجنبي مما يؤثر على شراء التقنيات الحديثة والمتطورة بسبب سعرها المرتفع.	متنوع، حيث يمكن ان يؤثر على تكلفة الاستثمارات في التكنولوجيا.
	الدخل المتاح لموظفين الأمن السيبراني	الأفراد الموظفون في المؤسسات الحكومية ذوي الدخل المنخفض لا يستمرون في العمل لكونه القطاع الخاص مرتباته مرتفعة جداً مما يؤثر على الموظفين الحكومين .	سلبي، حيث يمكن ان يقلل من القدرة على الاستثمار في الامن السيبراني.
	التعاون بين القطاعين العام والخاص.	يمكن تعزيز الكفاءات التقنية من خلال التعاون المستمر مع الشركات الخاصة والمؤسسات الحكومية لتبادل المعرفة والخبرات في مجال الأمن السيبراني	إيجابي، حيث يمكن ان يعزز من تبادل المعلومات والموارد.
	التكلفة الاقتصادية للهجمات السيبرانية	الهجمات السيبرانية تؤدي إلى خسائر مالية كبيرة للشركات والحكومات ، مما يجعل الاستثمار في الأمن السيراني ضرورة اقتصادية.	سلبي، تكاليف استعادة الانظمة يمكن ان تكون باهظة .
العوامل الاجتماعية Social Factors	تعزيز التعليم والتدريب.	يوجد نقص في برامج تعليمية وتدريبية في مجال الامن السيبراني لتحسين الوعي وزيادة الكفاءات في المجتمع.	إيجابي قوي، حيث يمكن ان يقلل من الهجمات السيبرانية ويزيد من الكفاءات المحلية.
	توظيف الخبرات المحلية.	الاعتماد على الخبرات المحلية وتوظيف الكفاءات التقنية الموجودة في ليبيا يعزيز من القدرات الأمنية وتطوير الحلول المحلية.	إيجابي، حيث يمكن ان يعزز من القدرات المحلية ويقلل من الاعتماد على الخبرات الخارجية.
	التوعية والتعليم.	نقص البرامج التدريبية والتاهيلية في مجال الامن السيبراني يؤدي إلى قلة عدد الخبراء والمتخصصين في هذا المجال مما يعقد عملية تطبيق استراتيجيات أمن سيبراني فعالة و غياب الكفاءات الفنية يمكن أن يترك الأنظمة الرقمية عرضة للهجمات والانتهاكات.	إيجابي، حيث يمكن ان يزيد من الالتزام بالسياسات الامنية.
	الشباب المهتمين بالتكنولوجيا	وجود نسبة كبيرة من الشباب المهتمين بالتكنولوجيا يمكن ان يكون دافعًا قويًا لتطوير حلول مبتكرة في مجال الأمن السيبراني.	إيجابي، حيث يمكن ان يعزز من الابتكار في مجال الامن السيبراني.
	قلة الاستثمار في التدريب .	نقص الاستثمار في برامج التدريب والتأهيل في مجال الأمن السيبراني يؤدي إلى قلة عدد الخبراء والمتخصصين في هذا المجال، مما يضعف من قدرة الدولة على مواجهة التهديدات السيبرانية بفعالية.	سلبي، حيث يمكن ان يؤدي إلى ضعف في الحماية السيبرانية.
	تداول البيانات الشخصية بشكل غير آمن.	قد يكون تبادل البيانات الشخصية عبر الإنترنت دون الحماية الكافية عاملاً يسهم في تعريض الأفراد لخطر الاختراقات السيبرانية .	سلبي، حيث يمكن ان يؤدي إلى زيادة الهجمات السيبرانية.

	قضايا الخصوصية والثقة.	قد تكون قضايا الخصوصية ونقص الثقة في حماية البيانات الشخصية عاملاً مهمًا في زيادة التهديدات السيبرانية على سبيل المثال، إذا لم يتم التعامل بشكل صحيح مع بيانات المواطنين وعدم ضمان خصوصيتها، فقد يزيد ذلك من احتمالية تعرض هذه البيانات للاختراقات.	سلبي، حيث يمكن ان يؤثر على قبول السياسات الامنية.
	التوزيع غير المتساوي للتكنولوجيا	قد يكون التوزيع غير المتساوي للتكنولوجيا والوصول إليها بين الطبقات الاجتماعية مشكلة تزيد من فجوة الأمن السيبراني على سبيل المثال، إذا كان هناك فجوة بين الذين يمتلكون تكنولوجيا متقدمة والذين لا يمتلكونها، فقد تتعرض الفئات الأكثر فقرًا للتهديدات السيبرانية بشكل أكبر.	سلبي، حيث يمكن ان يؤدي إلى فجوات في الحماية السيبرانية.
	ثقافة السلامة السيبرانية.	قد يكون نقص الوعي والتثقيف بشأن مفاهيم السلامة السيبرانية عاملا رئيسيا في زيادة الضعف الأمني فعدم التعرف على أساسيات الحماية السيبرانية وكيفية التصرف في حالة وقوع هجوم سيبراني يجعل الأفراد أكثر عرضة للتهديدات.	إيجابي، حيث يمكن ان يقلل من الهجمات السيبرانية.
	نقص الجلسات الحوارية.	تعتبر الجلسات الحوارية وورش العمل حول الامن السيبراني اداة فعالة لتوعية المجتمع بمخاطر الإنترنت ووسائل الوقاية لذا يجب تنظيم مثل هذه الفعاليات لتوعية الناس بأهمية حماية بياناتهم وأمانهم السيبراني.	سلبي، حيث يمكن ان يؤدي إلى ضعف في التنسيق.
	التعداد والنمو السُكاني وديموغرافية السُكان.	عدد سكان ليبيا يسمح بتعزيز الأمن السيبراني نسبيا في وقت قصير.	إيجابي، حيث يمكن ان يزيد من الابتكار في مجال الامن السيبراني.
	مستويات التعليم.	عدم وجود مناهج تعليمية متخصصة في الامن السيبراني لكل المراحل الدراسيةيزيد من مخاطر التعرض للهجمات السيبرانية.	سلبي، حيث يمكن ان يؤدي إلى تفاوت في الوعي الامني.
	تعزيز ثقافة المشاركة.	تشجيع المشاركة المجتمعية في إيجاد السياسات والحلول لمشكلات الامن السيبراني يعزز من التأثير الإيجابي للاستراتيجية.	إيجابي، حيث يمكن ان يعزز من الالتزام بالسياسات الامنية.
العوامل التكنولوجية Technological Factors	تحسين البنية التحتية الرقمية.	المساهمة في تحسين البنية التحتية التكنولوجية وتطويرها، يسهل تنفيذ استراتيجية امن سيبراني فعالة.	إيجابي قوي، حيث يمكن ان يعزز من القدرات السيبرانية ويحسن من الحماية.
	التحول الرقمي.	يسهم التحول الرقمي في تعزيز الابتكار من خلال تطوير تقنيات جديدة وإيجاد حلول إبداعية للتحديات المختلفة.	إيجابي، حيث يمكن ان يعزز من الكفاءة ويقلل من التهديدات السيبرانية.
	ضعف البنية التحتية التكنولوجيه.	تواجه ليبيا تحديدً في البنية التحتية التكنولوجية وهذا يعيق تقديم خدمات الإنترنت بشكل موثوق وآمن، مما يزيد من مخاطر التعرض للهجمات السيبرانية .	سلبي، حيث يمكن ان يزيد من التهديدات السيبرانية.
	الاستثمار في البحث والتطوير.	تعزيز الاستثمار في البحث والتطوير في مجال الامن السيبراني بتطوير تقنيات وحلول جديدة تلبي احتياجات البلد يسهم في تعزيز الأمن السيبراني.	إيجابي، حيث يمكن ان يعزز من الابتكار في مجال الامن السيبراني.
	الافتقار إلى تقنيات المتقدمة.	استخدام تقنيات وانظمة قديمة وغير محدثة ونقص التقنيات المتقدمة في مجال الامن السيبراني يجعل من الصعب على ليبيا مواكبة التهديدات السيبرانية المتطورة هذا النقص يمكن أن يؤدي إلى ثغرات أمنية يمكن استغلالها من قبل المهاجمين.	سلبي، حيث يمكن ان يعيق من تطوير القدرات السيبرانية.
	تبني المعايير الدولية.	تتبنى بعض المؤسسات في ليبيا معايير دولية مثل ISO 27001 لتعزيز نظم إدارة امن المعلومات، مما يسهم في تحسين مستوى الأمان السيبراني وضمان حماية البيانات بشكل أفضل.	إيجابي، حيث يمكن ان يعزز من الحماية السيبرانية.
	الاستثمارات في التكنولوجيا	عندما تكون هناك استثمارات متزايدة في قطاع التكنولوجيا والمعلومات، مما يعزز من القدرة على تطوير وتنفيذ استراتيجيات الأمن السيبراني المتقدمة.	إيجابي، حيث يمكن ان يعزز من القدرات السيبرانية
	تشجيع الإبداع والابتكار.	دعم الابتكار والتكنولوجيا الحديثة في مجال الامن السيبراني لتحسين القدرات والتصدي للتهديدات.	إيجابي، حيث يمكن ان يؤدي إلى حلول جديدة. ومبتكرة في الأمن السيبراني.

	استخدام التكنولوجيا الذكية.	يمكن اعتماد تكنولوجيا الحوسبة السحابية وتطبيقات الذكاء الاصطناعي وغيرها من التقنيات الحديثة لرصد ومراقبة الأنظمة السيبرانية على نطاق واسع.	إيجابي، حيث يمكن ان يعزز من الكفاءة ويقلل من التهديدات السيبرانية.
	الكوادر الشابة المهتمة بالتكنولوجيا	وجود نسبة كبيرة من الشباب المهتمين بالتكنولوجيا يوفر قاعدة قوية من المواهب التي يمكن تدريبها وتطويرها للعمل في مجال الأمن السيبراني.	إيجابي، حيث يمكن ان يعزز من الابتكار في مجال الامن السيبراني.
العوامل البيئية Environmental Factors	التكيف مع التغيرات المناخية	تطوير استراتيجيات للتكيف مع التغيرات المناخية يمكن ان يشمل تحسين البنية التحتية الرقمية لتكون أكثر مقاومة للكوارث الطبيعية، مما يعزز من الأمن السيبراني.	إيجابي، حيث يمكن ان يعزز من استدامة البنية التحتية.
	قلة تاثير الاوضاع الطبيعية	ندرة الكوارث الطبيعية مثل الفيضانات او الزلازل والتي يمكن ان تلحق اضرارا بالبنية التحتية التكنولوجية .	إيجابي، حيث يقلل من المخاطر.
	نقص الاستراتيجيات الوقائية.	يوجد نقص في تطوير استراتيجيات الوقاية والاستجابة السريعة للهجمات السيبرانية المحتملة.	سلبي، حيث يزيد من المخاطر.
	الاستدامة البيئية.	تبني ممارسات مستدامة في تطوير البنية التحتية الرقمية يمكن ان يسهم في تقليل المخاطر البيئية المرتبطة بالتكنولوجيا.	إيجابي، حيث يعزز من استدامة البنية التحتية.
العوامل القانونية Legal Factors	القوانين السيبرانية.	وجود قوانين مثل قانون مكافحة الجرائم الإلكترونية رقم (5 لسنة 2022) وقانون تنظيم المعاملات الإلكترونية رقم (6 لسنة 2022) تعتبر وجود هذه القوانين خطوة إيجابية نحو بناء بيئة رقمية آمنة وموثوقة في ليبيا، وتعزيز الثقة في استخدام التكنولوجيا علاوة على ذلك، من خلال تفعيل هذه القوانين وتطبيقها بشكل فعال، يمكن تعزيز الوضع القانوني للأمن السيبراني وحماية البيانات والمعاملات الإلكترونية في البلاد.	إيجابي، حيث يعزز من الحماية القانونية.
	غياب التوجيهات القانونية	غياب التوجيهات القانونية الواضحة يترك المؤسسات والافراد دون إرشادات محددة حول كيفية التعامل مع التهديدات السيبرانية، مما يزيد من مخاطر التعرض للهجمات في هذا الصدد من دون إطار قانوني قوي، قد يكون من الصعب تحديد المسؤوليات وتنظيم الإجراءات الضرورية.	سلبي، حيث يزيد من الفجوات القانونية.
	ضعف الحماية القانونية.	ضعف الحماية القانونية للافراد والمؤسسات يجعل من الصعب محاسبة المهاجمين السيبرانيين، مما يشجع على زيادة الجرائم السيبرانية	سلبي، حيث يزيد من المخاطر.
	عدم توفير الإطار التنظيمي للأمن السيبراني.	عدم وجود إطار تنظيمي شامل للامن السيبراني يؤدي إلى تشتت الجهود وعدم التنسيق بين الجهات المختلفة، مما يضعف من فعالية الاستجابة للتهديدات السيبرانية.	سلبي، حيث يعيق من تطبيق السياسات.
	التباين بين القوانين الجنائية والمدنية.	قد يكون هناك تباين في التطبيق القانوني بين الانظمة الجنائية والمدنية في التعامل مع حالات انتهاكات الأمن السيبراني، مما يؤثر على عمليات التحقيق والمحاكمة.	سلبي، حيث يعيق من تنفيذ القوانين.
	الرقابة والتنظيم.	وجود الرقابة والتنظيم في مجال الامن السيبراني يحمي ويراقب الانشطة السيبرانية غير القانونية ويتم اتخاذ الإجراءات اللازمة ضدها.	إيجابي، حيث يعزز من الحماية.
	تناقضات القوانين الدولية	تناقضات القوانين الدولية المتعلقة بالامن السيبراني بشان امور مثل الخصوصية وحرية الإنترنت يمكن أن تعيق التعاون الدولي وتبادل المعلومات أكثر تعقيدًا.	سلبي، حيث يعيق من التعاون الدولي.
	تاخر التشريعات التقنية	تاخر التشريعات التقنية في مواكبة التطورات السريعة في مجال التكنولوجيا يؤدي إلى ثغرات قانونية يمكن استغلالها من قبل المهاجمين	سلبي، حيث يعيق من التقدم.
	نقص التنسيق بين الأجهزة القضائية.	قد تواجه الاجهزة القضائية صعوبة في التعاون والتنسيق لمكافحة الجرائم السيبرانية بسبب فجوات في التعاون القانوني والتقني.	سلبي، حيث يعيق من تنفيذ القوانين

- نتائج تحليل بيستل تتمثل في صياغة الفرضيات التي تمثل الخطوة الأولى لوضع أهداف الاستراتيجية وهي كالاتي:
- إذا تم تعزيز الشرعية السياسية، فإن ذلك سيزيد من الالتزام بالسياسات الأمنية.
- التعاون مع الدول والمنظمات الدولية سيعزز من قدرات ليبيا في مواجهة التهديدات السيبرانية، وتبادل المعلومات والخبرات.
- إن عدم الاستقرار السياسي يخلق فجوات في الحماية السيبرانية ويزيد من فرص الهجمات.
- تعزيز الشفافية والثقة ومكافحة الفساد سيزيد من فعالية تنفيذ الاستراتيجيات الأمنية، ويقلل من الثغرات الأمنية.
- وضع استراتيجيات لمواجهة التدخلات الخارجية سيعزز من سيادة ليبيا، وحمايتها من التهديدات السيبرانية.
- إن وضع سياسات أمنية والالتزام بها سيقلل من التهديدات السيبرانية.
- إن تحسين التنسيق بين الجهات المختلفة سيعزز من فعالية تعزيز الامن السيبراني.
- إذا تم توفير التمويل والموارد الكافية للمؤسسات الحكومية، فإن ذلك سيعزز من تنفيذ استراتيجيات الأمن السيبراني.
- إذا تم استغلال الثروات الطبيعية بشكل فعال، فإن ذلك سيوفر التمويل اللازم لتطوير البنية التحتية السيبرانية.
- إذا تم استخدام التكنولوجيا لحماية الموارد الطبيعية، فإن ذلك سيعزز من القدرات السيبرانية ويقلل من التهديدات.
- إذا تم زيادة الاستثمارات في البنية التحتية الرقمية، فإن ذلك سيعزز من القدرات السيبرانية ويحسن من الحماية.
- إذا تم تقليل معدلات البطالة، فإن ذلك سيقلل من الجرائم السيبرانية الناتجة عن نقص الفرص الاقتصادية.
- إذا تم تعزيز التعاون بين القطاعين العام والخاص، فإن ذلك سيؤدي إلى تحسين تبادل المعلومات والموارد وتقليل التهديدات السيبرانية.
- إذا تم تعزيز التعليم والتدريب في مجال الأمن السيبراني، فإن ذلك سيزيد من الوعي الأمني ويقلل من الهجمات السيبرانية.
- إذا تم توظيف الخبرات المحلية، فإن ذلك سيعزز من القدرات المحلية، ويقلل من الاعتماد على الخبرات الخارجية.
- إذا تم نشر التوعية والتعليم بأهمية الأمن السيبراني، فإن ذلك سيزيد من الالتزام بالسياسات الأمنية.
- إذا تم تشجيع الشباب على استخدام التكنولوجيا بشكل آمن، فإن ذلك سيعزز من الابتكار في مجال الأمن السيبراني.
- إذا تم زيادة الاستثمار في التدريب، فإن ذلك سيعزز من الكفاءات السيبرانية ويقلل من المخاطر.
- إذا تم تبني التحول الرقمي، فإن ذلك سيزيد من الكفاءة والانتاجية ومواكبة التطورات العالمية.
- إذا تم زيادة الاستثمارات في البحث والتطوير، فإن ذلك سيؤدي إلى حلول جديدة ومبتكرة في الأمن السيبراني.
- إذا تم تبني التقنيات المتقدمة، فإن ذلك سيعزز من القدرات السيبرانية.
- إذا تم تبني المعايير الدولية، فإن ذلك سيعزز من الحماية السيبرانية.

- إذا تم تطوير استراتيجيات وقائية فعالة، فإن ذلك سيقلل من المخاطر البيئية.
- إذا تم تطوير القوانين السيبرانية وتحديثها، فإن ذلك سيعزز من الحماية القانونية.
- إذا تم توفير التوجيهات القانونية اللازمة، فإن ذلك سيقلل من الفجوات القانونية.
- إذا تم توفير إطار تنظيمي فعال، فإن ذلك سيساعد على الحد من الجرائم السيبرانية.
- إذا تم تعزيز الرقابة والتنظيم، فإن ذلك سيقلل من المخاطر.

بشكل عام بعد إجراء تحليل بيستل (PESTEL) الشامل تم تحديد العديد من التأثيرات الإيجابية والسلبية التي تؤثر على استراتيجية الأمن السيبراني في ليبيا حيث إن هذا التحليل يوفر رؤية واضحة وشاملة للبيئة الخارجية التي تعمل فيها الاستراتيجية، ويشير إلى ضرورة اتخاذ إجراءات شاملة وتكاملية لدعم الأمن السيبراني في ليبيا وحماية المعلومات في المجتمع، مما يسهم في تعزيز الاستقرار والتنمية في البلاد، وتساعد هذه النتائج على تحديد الفرص والتهديدات المحتملة بناءً على النتائج المستخلصة من تحليل بيستل، سيتم الانتقال إلى الخطوة التالية وهي إجراء تحليل سوات (**SWOT**) هذا التحليل سيساعد في تحديد نقاط القوة والضعف الداخلية، بالإضافة إلى الفرص والتهديدات الخارجية، علماً أن الهدف من تحليل سوات هو تطوير استراتيجيات فعالة تعزز من نقاط القوة وتستغل الفرص، بينما تعمل على تقليل نقاط الضعف ومواجهة التهديدات وبذلك يمكن القول بأنه من خلاله سيتم تحديد الإجراءات والتدابير اللازمة لتحقيق الأهداف، وضمان استدامة الأمن السيبراني في مواجهة التحديات المستقبلية.

- **ثانياً: أداة التحليل سوات SWOT**

يعد تحليل سوات بمثابة إطار لجمع وتنظيم واستخدام البيانات المتحصل عليها من تحليل الموقف استناداً إلى ظروف كل من البيئة الداخلية والبيئة الخارجية وهو اختصار لأربع كلمات نقاط القوة ونقاط الضعف، الفرص والتهديديات وسيتم دراسة الأداة لتحليل الوضع الراهن لوضع مقترح استراتيجية وطنية للأمن السيبراني في ليبيا كم موضح في الجدول رقم (2) .

بعد الانتهاء من مرحلة تحليل سوات (**SWOT**)الخطوة التالية هي اقتراح التوصيات التي تسهم في تطوير مقترح الاستراتيجيات الوطنية للأمن السيبراني في ليبيا :

- الشباب المتعلم والمهتم بالتكنولوجيا: إنشاء برامج تدريبية وتوظيفية للشباب في مجال الأمن السيبراني.
- تطبيق السياسات الوطنية: تعزيز تنفيذ السياسات الوطنية وتحديثها بانتظام لمواكبة التهديدات الجديدة.
- التشريعات والقوانين: تطبيق القوانين الحالية بفعالية وتطوير تشريعات جديدة حسب الحاجة.
- إعادة بناء البنية التحتية: الاستثمار في إعادة بناء البنية التحتية المتضررة بسبب النزاعات.
- الانضمام إلى الاتفاقيات الدولية: الاستفادة من الدعم الدولي لتحسين البنية التحتية التكنولوجية والأمنية.
- الاستثمار في التعليم والتدريب: رفع مستوى الكوادر الوطنية في مجال الأمن السيبراني.

الجدول رقم (2)تحيل سوات **SWOT**

البيئة الداخلية	
نقاط القوة (Strengths)	**نقاط الضعف**(Weaknesses)
توفر الهيئة العامة لأمن وسلامة المعلومات إطارًا تنظيميًا وإرشاديًا، مما يسهل وضع السياسات والمعايير الأمنية.	ضعف البنية التحتية التكنولوجية وعدم تحديثها بشكل دوري.
توفر قوة عمل شابة ومتعلمة يمكن أن تسهم في تطوير حلول أمنية مبتكرة.	انخفاض الوعي المجتمعي بأهمية الأمن السيبراني ووسائل الحماية المتاحة.
توفر إطار قانوني يحمي الأفراد والمؤسسات من الجرائم الإلكترونية مثل قانون مكافحة الجرائم الإلكترونية رقم (5 لسنة 2022) وقانون تنظيم المعاملات الإلكترونية رقم (6 لسنة 2022).	نقص التمويل والاستثمار في تعزيز الحماية السيبرانية للمؤسسات الحكومية.
توفر الورش الوطنية لتوعية بالأمن السيبراني تسهم هذه الورش في رفع مستوى الوعي والمعرفة حول المخاطر السيبرانية.	تأخر في تنفيذ التشريعات والسياسات المتعلقة بالأمن السيبراني.
وجد مؤسسات تعليمية وأكاديمية خاصة تدعم تطوير مهارات الأمن السيبراني.	محدودية قدرات الدفاع السيبراني المتاحة
مع الإيرادات العالية من قطاع النفط والغاز، يمكن استثمار جزء من هذه الأموال في مشاريع الأمن السيبراني لتعزيز البنية التحتية الرقمية.	نقص التدريب المستمر للكوادر العاملة في مجال الأمن السيبراني داخل المؤسسات الحكومية.
اهتمام القطاع الخاص بتطوير حلول أمنية سيبرانية يعكس رغبة القطاع الخاص في المشاركة في تعزيز الأمن السيبراني..	زيادة التهديدات الناتجة عن هجمات سيبرانية متطورة.
التوجه نحو التحول الرقمي يوفر فرصة لتعزيز الأمن السيبراني من خلال تحديث الأنظمة والبنية التحتية.	قلة وجود مركز بيانات وآليات فعالة للكشف المبكر عن التهديدات السيبرانية في بعض المؤسسات الحكومية
الفريق الوطني للاستجابة لطوارئ الكمبيوتر (Libya-CERT) التابع للهيئة.	نقص التعاون والتنسيق بين الجهات المعنية بالأمن السيبراني، وقلة تبادل المعلومات والخبرات بين الجهات الحكومية.
تقارب وجهات النظر في تعزيز الأمن السيبراني في البلاد.	غياب استراتيجية موحدة لحماية البيانات والمعلومات.

	ضعف النظام القضائي وعدم فعاليته في مكافحة الجرائم السيبرانية، مما يحد من قدرة الدولة على تطبيق القانون.
	نقص وجود إدارة مختصة بالأمن السيبراني في المؤسسات الحكومية.
	قلة الخبراء والكفاءات المتخصصة في مجال الأمن السيبراني.
	انخفاض نسبة تطبيق السياسات الوطنية الصادرة عن الهيئة العامة لأمن وسلامة المعلومات
البيئة الخارجية	
الفرص المحتملة (Opportunities)	**التهديدات**(Threats)
وجود فرص في الاستفادة من اتفاقيات دولية ومبادرات لتحسين البنية التكنولوجية والأمنية.	التهديدات السيبرانية المتزايدة الخطيرة التي تستهدف البنية التحتية الحيوية.
امكانية التدريب والتعليم للكوادر الوطنية قابلة للتطوير لرفع مستوى الأمن السيبراني.	صعوبة مواكبة التطورات السريعة في مجال الأمن السيبراني بسبب التطور السريع للتكنولوجيا.
تشجيع الابتكار المحلي وتطوير حلول لمواجهة التحديات السيبرانية.	عدم الاستقرار السياسي والأمني يمكن أن يؤثر سلبًا على جهود تعزيز الأمن السيبراني.
الاستفادة من التعداد السكاني القليل لتعزيز الأمن السيبراني بشكل سريع.	التقسيمات السياسية الداخلية تؤدي إلى ضعف التنسيق بين الجهات المختلفة.
تعزيز التعاون بين القطاعين العام والخاص لتحسين الخدمات السيبرانية.	فقدان الثقة في المؤسسات يمكن أن يؤدي إلى ضعف التعاون بين المواطنين والحكومة في مجال الأمن السيبراني.
القدرة على اســتثمار تحســين البنية التحتية الرقمية لتعزيز قدرة ليبيا على مواجهة التهديدات السيبرانية.	ضعف الحكومة المركزية والفساد وعدم الشفافية يمكن أن يؤدي إلى ضعف تنفيذ السياسات الأمنية.
تعزيز مستوى الأمان السيبراني من خلال تبني المعايير الدولية والممارسات العالمية.	نفوذ الجماعات المسلحة واستمرار النزاعات يشكل تهديدًا كبيرًا للأمن السيبراني.
تعزيز قدرات ليبيا في مجال الأمن السيبراني من خلال الاستثمار في التكنولوجيا.	التدخل الخارجي وتأثير الدول الأجنبية في الشؤون الداخلية وزيادة التوترات يمكن أن يزيد من التهديدات السيبرانية.

تحسين كفاءة الأنظمة الرقمية الأمنية من خلال استخدام التكنولوجيا الذكية والاستثمار فيها.	غياب التوجيهات القانونية وضعف الحماية القانونية السيبرانية ونقص التنسيق بين الأجهزة القضائية يمكن أن يعيق تنفيذ القوانين السيبرانية بفعالية.
تكوين قاعدة قوية من الشباب المهتمين بالتكنولوجيا لتطوير قطاع الأمن السيبراني.	التباين بين القوانين الجنائية والمدنية وتناقضات القوانين الدولية في مجال الحماية السيبرانية.
زيادة القدرة على تمويل مشاريع الأمن السيبراني من خلال ارتفاع معدلات النمو الاقتصادي.	الاعتماد الكبير على التكنولوجيا الأجنبية بدلاً من تطوير حلول محلية وغياب استراتيجيات وقائية فعالة يزيد من تعرض البنية التحتية السيبرانية للمخاطر.
تطوير إطار قانوني شامل يحمي الأمان السيبراني ويعزز الحماية القانونية.	ضعف البنية التحتية التكنولوجية والاعتماد على التقنيات القديمة قد يحد من قدرة ليبيا على مواجهة التهديدات السيبرانية بفعالية.
تنظيم حملات توعية وبرامج تعليمية لجميع الفئات العمرية لرفع الوعي بأهمية الأمن السيبراني.	معدلات البطالة يزيد من التحديات الاقتصادية وتؤثر على القدرة على الاستثمار في الأمن السيبراني.
تعزيز الأمن السيبراني من خلال التعاون مع المنظمات الدولية واستفادة من الخبرات الدولية والدعم السياسي.	التضخم وارتفاع الأسعار يؤثر على القدرة الشرائية ويزيد من التحديات التكنولوجية.
تيسير تطبيق السياسات والإجراءات الضرورية لتعزيز الأمن السيبراني عبر تعزيز الشرعية السياسية.	تداول البيانات الشخصية بشكل غير آمن يزيد من مخاطر الاختراقات السيبرانية.

- دعم المشاريع والمبادرات الحكومية: الاستفادة من تزايد الاهتمام الحكومي بالأمن السيبراني.
- تشجيع الابتكار المحلي: دعم المشاريع المحلية لتطوير حلول سيبرانية مبتكرة.
- تبني التقنيات الحديثة: استخدام التقنيات الحديثة لتحسين البنية التحتية وتطوير الاقتصاد الرقمي.
- الشراكة بين القطاعين العام والخاص: تعزيز التعاون بين القطاعين لتحسين الخدمات التكنولوجية والأمنية
- التوجه نحو التحول الرقمي: تعزيز الأمن السيبراني من خلال تحديث الأنظمة والبنية التحتية.
- الاستفادة من التطورات السريعة في التكنولوجيا: تبني أحدث التقنيات لتعزيز الأمن السيبراني.
- الاستثمار في تحسين البنية التحتية الرقمية: تعزيز قدرة ليبيا على مواجهة التهديدات السيبرانية بفعالية.
- استخدام التكنولوجيا الذكية: تحسين كفاءة الأنظمة الرقمية الأمنية وفعاليتها.
- الاهتمام بالكوادر الشابة: تكوين قاعدة قوية لتطوير قطاع الأمن السيبراني.
- زيادة الوعي المجتمعي: تنظيم حملات توعية لتعزيز فهم المجتمع لأهمية الأمن السيبراني.
- زيادة التمويل والاستثمار: تخصيص موارد مالية أكبر لمشاريع الأمن السيبراني.
- تسريع تطبيق التشريعات: وضع آليات لتسريع تنفيذ التشريعات والسياسات.
- وضع خطة للتعامل مع التهديدات: تطوير خطة شاملة للتعامل مع هجمات القرصنة الإلكترونية.
- التدريب المستمر: تنظيم دورات تدريبية مستمرة للكوادر العاملة في مجال الأمن السيبراني.
- تحسين آليات الكشف المبكر: تطوير أنظمة للكشف المبكر عن التهديدات السيبرانية.
- تعزيز التوجيه السياسي: وضع استراتيجية شاملة للأمن السيبراني بدعم من القيادة السياسية.
- تعزيز التعاون والتنسيق: تحسين التنسيق بين الجهات المعنية بالأمن السيبراني.
- التعامل مع التقلبات السياسية والاقتصادية: وضع خطط للتعامل مع تأثير التقلبات على البنية التحتية الرقمية.
- حماية البيانات والمعلومات: تطوير استراتيجية موحدة لحماية البيانات والمعلومات.
- تبادل المعلومات والخبرات: تعزيز تبادل المعلومات والخبرات بين الجهات الحكومية والقطاع الخاص.
- تحسين النظام القضائي: تعزيز فعالية النظام القضائي في مكافحة الجرائم السيبرانية.
- تعزيز الدفاع السيبراني: تطوير القدرات لمواجهة التهديدات المتزايدة.
- مواكبة التطورات السريعة: الاستثمار في البحث والتطوير لمواكبة التطورات السريعة في مجال الأمن السيبراني.
- تحسين التنسيق بين الجهات المختلفة: تعزيز التعاون بين الجهات الحكومية والقطاع الخاص.
- بناء الثقة في المؤسسات: تعزيز الشفافية والمساءلة لبناء الثقة بين المواطنين والحكومة.
- تعزيز الحكومة المركزية: دعم الحكومة المركزية لتنفيذ السياسات الأمنية بفعالية.

- التعامل مع نفوذ الجماعات المسلحة: وضع خطط للتعامل مع تهديدات الجماعات المسلحة.
- التصدي للتدخل الخارجي: تعزيز السيادة الوطنية وتقليل تأثير التدخلات الخارجية.
- تطوير الكفاءات المتخصصة: تنظيم برامج تدريبية لتطوير الكفاءات المتخصصة في مجال الأمن السيبراني.
- توحيد القوانين الجنائية والمدنية: وضع إطار قانوني موحد يتماشى مع القوانين الدولية.
- تشجيع تطوير حلول محلية: تقليل الاعتماد على التكنولوجيا الأجنبية وتعزيز الابتكار المحلي

يتطلب تعزيز الأمن السيبراني في ليبيا تكامل الجهود على مختلف الأصعدة، بدءًا من تحديث البنية التحتية، وصولاً إلى رفع الوعي العام وتفعيل الشراكات من خلال تنفيذ هذه التوصيات، يمكن تحسين مستوى الأمان وتقليل المخاطر المرتبطة بالتهديدات السيبرانية.

3.1.4.3. المرحلة الثالثة :مراحل بناء مقترح الاستراتيجية الوطنية للأمن السيبراني :

1. الاطار المرجعي لتطوير الاستراتيجية :

لتوفير مرجع عملي شامل للجوانب المختلفة للأمن السيبراني على المستوى الوطني، تم بناء إطار مرجعي للأمن السيبراني خاص بالدولة الليبية، هذا الإطار مبني على أفضل الممارسات المحلية والعالمية، ويأخذ في الاعتبار أحدث المستجدات والتحديات التي تواجه الأمن السيبراني، يُعد هذا الإطار نموذجًا متقدمًا يغطي مختلف جوانب الأمن السيبراني على مستوى الدول، ويحتوي على ستة محاور رئيسية، من خلال هذا الإطار نضع أسس رؤيتنا الاستراتيجية للأمن السيبراني في ليبيا، ونؤكد على النقاط التالية، كما هو موضح في الشكل رقم(16).

1. سيادة وطنية غير قابلة للتفاوض: أمننا السيبراني هو امتداد لسيادتنا الوطنية، وجزء لا يتجزأ من وحدتنا واستقلالنا الوطني.
2. تنمية الكوادر البشرية وكفاءتها: سيكون من الركائز رفع مستوى الوعي وبناء القدرات الوطنية في مجال الأمن السيبراني، لضمان استجابة تكنولوجية فعالة وظهور جيل جديد من المختصين الليبيين.
3. استثمار استباقي وتحديث مستمر: سيكون من الاولويات الاستثمار في البحث والتطوير لمواجهة التحديات القائمة والمستجدات في مجال الأمن السيبراني بشكل استباقي، وضمان استمرارية تطوير أدواتنا وخططنا.
4. منظومة متكاملة مع المعايير الدولية: تتطلع الدولة الليبية إلى بناء استراتيجية تتوافق مع أفضل الممارسات العالمية وتجارب الدول المتقدمة، مع الحفاظ على خصوصيتنا ومتطلباتنا الوطنية وأن تكون ليبيا دولة رائدة في مجال الأمن السيبراني.
5. أمن شامل وتعاون مؤسسي: نرمي إلى تعزيز التكاتف والتعاون بين جميع الجهات الحكومية، الخاصة، ومنظمات المجتمع المدني، لتكريس نهج موحد يضمن عمقاً استراتيجياً في خطتنا للأمن السيبراني.
6. إطار تعاون دولي: السعي لتأسيس شراكات فعّالة ومستدامة مع الهيئات والمنظمات الدولية لتبادل الخبرات والمعرفة، وتعزيز قدراتنا في التصدي للتهديدات السيبرانية.

الشكل رقم (16)أساسيات الاطار المرجعي لتطوير مقترح الاستراتيجية الوطنية للأمن السيبراني، المصدر من إعداد الباحثة

من خلال هذه الأركان الراسخة، نطمح إلى صياغة استراتيجية وطنية للأمن السيبراني وتنفيذها تتضمن معيارًا يحتذى به في الحماية الالكترونية، وتبشر بمستقبل تقني مزدهر لليبيا تترسخ فيه الثقة الرقمية والريادة السيبرانية.

2. الرؤية :

تعكس هذه الاستراتيجية الطموح الاستراتيجي بأن تصبح ليبيا بحلول عام 2029 دولة رائدة في مجال الأمن السيبراني، من خلال إنشاء بيئة رقمية آمنة وموثوقة تحمي البيانات والخصوصية، وتدعم الابتكار والنمو الاقتصادي، مع تعزيز القدرة على التصدي للتهديدات السيبرانية بكفاءة وفعالية وحماية الأمن القومي الليبي، وستكون هذه الرؤية شاملة للفضاء السيبراني تلبي اجتياحات الدولة الليبية واولوياتها وتطلعاتها والتأكيد على حماية الانظمة التقنية والتشغيلية والبنى التحتية الحساسة ومواجهة الاضرار والتعافي منها في الوقت المناسب، وتتضمن الرؤية التي تسعى الدراسة إلي الوصول اليها:

" فضاء سيبراني ليبي آمن - موثوق ومستدام، يحمي المصالح الوطنية ويعزز التنمية والنمو ويواجه التهديدات السيبرانية".

3. الرسالة :

بناء بيئة رقمية قوية، تحمي سيادتنا الوطنية ومواردنا الحيوية وتعزز مكانتنا في الفضاء السيبراني، تكون الخدمات الرقمية موثوقة ومتاحة للجميع، مبنية بقدرات وطنية متخصصة تنظمها تشريعات متكاملة وحديثة.

4. المبادي الأساسية :

أظهرت دراسة الوضع الراهن والتجارب الدولية أهمية وجود مبادئ اساسية تساهم في بناء استراتيجية فعالة وشاملة وقد تم تحديد مجموعة من المبادئ التالية:

- **السيادة الوطنية**:حماية البنية التحتية الرقمية الليبية من التدخلات الخارجية، وضمان السيطرة الكاملة على القرارات المتعلقة بالأمن السيبراني.
- **الشفافية والنزاهة :**الانفتاح ومشاركة المعلومات والبيانات مع كل الاطراف المعنية، واتخاد القرارات بكل أمانة وموضوعية.

- **حماية الخصوصية**: التأكيد على أهمية حماية خصوصية الأفراد والمؤسسات وضمان أن تكون البيانات محمية بشكل صارم.
- **الشراكة والتعاون**:بناء شراكات قوية مع القطاع الخاص، والمجتمع المدني، والمنظمات الدولية لتبادل الخبرات والمعرفة وتعزيز التعاون.
- **الابتكاروالتطوير**:دعم وتشجيع الأبتكارواستخدام التكنولوجيا الحديثة لتعزيز الأمن السيبراني وتطوير حلول مبتكرة لمواجهة التهديدات المتطورة.
- **الاستدامة والمرونة**:ضمان استمرارية الجهود والسياسات والتشريعات على المدى الطويل والقدرة على التكيف بسرعة مع التهديدات الجديدة والتغيرات في البيئة السيبرانية.

5. أهداف الاستراتيجية :

لتحقيق فضاء سيبراني ليبي آمن وموثوق يعزز النمو والتنمية، تسعى الاستراتيجية الوطنية للأمن السيبراني إلى تحقيق الأهداف الرئيسية التالية:

الهدف الأول: تأسيس البنية التحتية الرقمية :

أن يتم حماية البنى التحتية الحرجة (CIS) والبنى التحتية للمعلومات الحرجة (Clls) من منظور إدارة المخاطر، و يجب أن يوجه تقييم مفصل للمخاطر عملية تحديد البنى التحتية الوطنية الحرجة (Cls) والبنى التحتية للمعلومات الحرجة والخدمات الأساسية التي قد يؤدي تعطيلها إلى تأثيرات خطيرة على الصحة أو السلامة أو الأمن أو الرفاهية الاقتصادية للمواطنين، أو على الأداء الفعال للحكومة والاقتصاد. علاوة على ذلك، ينبغي اعتماد نهج قائم على المخاطر في تحديد وترتيب أولويات تنفيذ البرامج والسياسات المصممة لحماية البنى التحتية الحرجة والبنى التحتية للمعلومات الحرجة ولتسهيل التعاون مع القطاع الخاص، يمكن النظر في نهج إدارة المخاطر المستند إلى المعايير الدولية.

ينبغي أن تصف الاستراتيجية على مستوى عالٍ بنية الإدارة والأدوار والمسؤوليات لمختلف أصحاب المصلحة في حماية البنى التحتية الحرجة والبنى التحتية للمعلومات الحرجة وفقاً لمبدأ القيادة الواضحة وتخصيص الموارد، يتطلب أي برنامج فعال وكفء لحماية البنى التحتية الحرجة أن يكون لدى أصحاب المصلحة أدوار ومسؤوليات محددة بوضوح، وأن تنشأ آلية تنسيق لإدارة القضايا الجارية.

غالباً ما لا تملك الحكومة أو تتحكم بالبنى التحتية الحرجة والبنى التحتية للمعلومات الحرجة، وتتجاوز جهود حماية هذه البنى التحتية قدرات وولاية أي وكالة حكومية منفردة. لذا، فإن تعيين منسق عام لأمن البنى التحتية الحرجة (السيبراني) من خلال لجنة مشتركة بين الوكالات يمكن أن يعزز بشكل كبير الجهود المبذولة لحماية هذه البنى التحتية.

ينبغي أن يشمل نموذج الحوكمة الخاص بحماية البنى التحتية الحرجة والبنى التحتية للمعلومات الحرجة تحديد الهيئات الحكومية المسؤولة عن قطاعات محددة، ومسؤوليات ومساءلة مشغلي هذه البنى التحتية، بالإضافة إلى قنوات الاتصال وآليات التعاون بين الوكالات العامة والخاصة لضمان تشغيل الخدمات والبنى التحتية الحرجة وتعافيها، هناك العديد من المرجعيات الدولية التي يمكن الاستعانة بها، مثل إطار NIST للأمن السيبراني، الذي يركز على خمسة محاور متوازية:

تحديد الأصول الرقمية والمخاطر المرتبطة بها، الحماية والتأمين، اكتشاف الهجمات والحوادث السيبرانية، التعافي منها، وتطوير طريقة لتحديد البنية التحتية الحرجة.الهدف الثاني: أنشاء مراكز استجابة للحوادث السيبرانية.

الهدف الثاني: إنشاء مراكز استجابة للحوادث السيبرانية :

إن المراكز الوطنية للاستجابة للحوادث السيبرانية هي خط الدفاع الأول ووحدات الكشف المبكر عن التهديدات السيبرانية، تلعب هذه المراكز دورًا حيويًا في تحديد مصادر الهجمات وأهدافها، وتحليل أساليب عملها والثغرات المستهدفة، يتطلب ذلك بناء قدرات وطنية مناسبة للتصدي للحوادث السيبرانية، من خلال إنشاء فرق الاستجابة للطوارئ الحاسوبية (CERTs) أو فرق الاستجابة لحوادث الأمن الحاسوبي (CSIRTs) أو فرق الاستجابة للحوادث الحاسوبية (CIRTs)على المستوى الوطني.

يجب أن توفر هذه الفرق مجموعة من الوظائف الاستباقية والتفاعلية، بالإضافة إلى الخدمات الوقائية والتعليمية، مما يعزز قدرة ليبيا على الاستجابة السريعة والتعافي من التهديدات السيبرانية، وتحسين قدرتها على الصمود أمام هذه التهديدات، كما يجب أن تتعاون هذه الفرق وتتواصل مع نظرائها الدوليين، ينبغي وضع خطة طوارئ لإدارة الأزمات المتعلقة بالأمن السيبراني، تكون جزءًا من خطة الطوارئ الوطنية الشاملة، وتشمل آليات للتعافي من الكوارث، كما يجب إنشاء مراكز مشابهة تعمل على مستوى المؤسسات أو الوزارات، حيث تختلف متطلبات وأولويات التهديدات من قطاع لآخر، يمكن اتباع أحد الأطر العالمية للأمن السيبراني، مثل إصدارات الاتحاد الدولي للاتصالات المتعلقة بهذه المراكز، والمركز الأوروبي للأمن السيبراني (ENISA)، والمعهد القومي للمعايير القياسية والتكنولوجية بالولايات المتحدة الأمريكية.

الهدف الثالث: وضع إطار قانوني شامل للأمن السيبراني :

ينبغي وضع إطار قانوني محلي يحدد بوضوح الأنشطة السيبرانية المحظورة بهدف الحد من الجرائم السيبرانية، يمكن تحقيق ذلك من خلال تعديل قانون الجرائم الإلكترونية رقم (5) الصادر عام 2022م وسن قوانين جديدة، يجب تشجيع استحداث عملية لمراقبة تنفيذ ومراجعة التشريعات وآليات الحوكمة، واستبانة الثغرات وتداخل السلطات، وتحديد المجالات التي تتطلب التحديث وترتيب أولوياتها.

ينبغي أيضًا بناء إطار يحمي الحقوق الأساسية في الإجراءات القانونية الواجبة في حالة التحقيقات الجنائية والادعاء، وكذلك حقوق حماية البيانات، بما في ذلك حماية خصوصية البيانات الشخصية، يمكن تحقيق ذلك من خلال وضع إطار لحماية البيانات والخصوصية، ووضع آليات امتثال محلية لمنع ومكافحة وتخفيف الأعمال التي تهدد سرية وسلامة وتوفر أنظمة تكنولوجيا المعلومات والاتصالات والبنى التحتية.

كما ينبغي تشجيع تطوير القدرات على إنفاذ القانون السيبراني، بما في ذلك التدريب والتعليم لأصحاب المصلحة المعنيين بمكافحة الجريمة السيبرانية، مثل الشرطة والقضاة والمدعين العامين والمحامين وموظفي إنفاذ القانون والمحققين الجنائيين، يجب أن تتلقى هذه الأجهزة تدريبات متخصصة على الجرائم السيبرانية وكشفها وردعها والتحقيق فيها ومقاضاة مرتكبيها، التحقيق الرقمي والاعتراض المشروع للاتصالات واستخدام الأدلة الرقمية، وتطوير المعرفة بشأن التهديدات والثغرات الناشئة المتعلقة بهذه الجرائم، وإقامة تعاون مع المؤسسات الأكاديمية والبحثية والتطويرية الرائدة في مجال تقنيات الطب الشرعي الرقمي، يجب التعاون مع أصحاب المصلحة في القطاعين العام والخاص من أجل

التصدي للقضايا المتعلقة بالجرائم الإلكترونية والاستجابة لها بسرعة، ينبغي أيضًا التعاون مع هيئات إنفاذ القانون الدولية مثل الإنتربول واليوروبول للتصدي للجرائم السيبرانية.

أخيرًا، ينبغي تحديد كيان لإنفاذ القانون يتحمل المسؤولية الأساسية عن قضايا الأمن السيبراني، وضمان حصول هذا الكيان على التدريب والموارد الكافية للمساعدة في الشراكة مع الضحايا والكيانات ذات الصلة لتعزيز تبادل المعلومات حول التهديدات الجديدة والمبتكرة.

الهدف الرابع: تعزيز الشفافية والمساءلة في الأمن السيبراني :

يجب بناء بيئة رقمية يثق بها المواطنون والمؤسسات الحكومية، حيث تُحمى حقوق المستخدمين ومصالحهم لضمان أمن البيانات والأنظمة، هذا ضروري لاستغلال الإمكانات الكاملة للفرص الاجتماعية والسياسية والاقتصادية التي توفرها تكنولوجيا المعلومات والاتصالات، يجب تقديم خدمات حيوية آمنة تعتممها تكنولوجيا المعلومات ويستخدمها المواطنون، مما يعزز الثقة في استخدام الفضاء السيبراني.

الهدف الخامس: الشراكة بين القطاعين العام والخاص :

أن تكون الشراكة بين القطاعين العام والخاص أداة فعالة لتجميع الخبرات والموارد، حيث تحدد نطاقاً وأهدافاً مشتركة وتستخدم أدواراً ومنهجيات عمل محددة لتحقيق الأهداف المشتركة، فينبغي أن يقوم المجلس على إقامة شراكات رسمية بين القطاعين لتعزيز أمن البنى التحتية، حيث تعتبر هذه الشراكات حجر الزاوية في حماية البنى التحتية الحرجة وإدارة المخاطر الأمنية على المديين القصير والطويل .

تعد هذه الشراكات ضرورية لتعزيز الثقة بين القطاعين، وتتطلب إنشاء شراكات مستدامة وفهم واضح لأهداف الشراكة من قبل جميع أصحاب المصلحة، يمكن أن تشمل الخطوط الأساسية المشتركة للأمن السيبراني إنشاء هياكل تنسيق فعالة، وعمليات تبادل المعلومات والبروتوكولات، وبناء الثقة، وتحديد وتبادل الأفكار وأفضل الممارسات لتحسين الأمن السيبراني، كما ينبغي البحث عن فرص لإنشاء روابط دولية من الشراكات بين القطاعين العام والخاص.

الهدف السادس: إنشاء برامج تدريبية متخصصة :

يجب وضع برامج تدريبية متخصصة في الأمن السيبراني، تشمل خطط تنمية المهارات للخبراء وغير الخبراء في جميع القطاعات، ينبغي توفير التدريب التنفيذي والتشغيلي، والتدريب الداخلي والمهني، بالإضافة إلى الشهادات الوطنية والدولية علاوة على ذلك، يجب تطوير مسارات مهنية متخصصة في الأمن السيبراني، ويجب إقامة هذه البرامج بالشراكة مع الأوساط الأكاديمية، والقطاع الخاص، والمجتمع المدني، من الضروري اعتماد نهج متوازن بين الجنسين لتحفيز وتشجيع مشاركة المرأة في جميع الجهود الرامية إلى تنمية المهارات والتدريب، مما يساهم في معالجة الفجوة بين الجنسين بين خبراء الأمن السيبراني ويضمن الشمولية في المستقبل.

الهدف السابع: تعزيز الوعي المجتمعي بالأمن السيبراني :

يجب تنسيق حملات توعية وأنشطة على المستوى الوطني من خلال تأسيس سلطة مختصة تركز على نشر المعلومات حول مخاطر وتهديدات الأمن السيبراني وأفضل الممارسات للتصدي لها، ينبغي أن تشمل هذه البرامج التوعوية جميع فئات المجتمع الليبي، بما في ذلك الأشخاص ذوي الإعاقة الرقمية، وبرامج تعليمية تركز على المستهلك، ومبادرات توعية تستهدف المديرين التنفيذيين في مختلف قطاعات القطاعين العام والخاص .

يجب تعزيز وتشجيع العلاقات بين الأوساط الأكاديمية وصناعة الأمن السيبراني، ووضع مناهج تعليمية في جميع مراحل نظام التعليم لتعزيز مهارات الأمن السيبراني والتوعية به، ينبغي دمج دورات الأمن السيبراني في برامج علوم الحاسوب وتكنولوجيا المعلومات في التعليم المتوسط والجامعات والدراسات العليا، لتعزيز الوعي وزيادة الاهتمام بفرص العمل في هذا المجال.

ينبغي للحكومة النظر في وضع خطط حوافز مثل المنح الدراسية لتدريس الأمن السيبراني في أفضل الجامعات الدولية والعربية، لبناء أجيال رقمية متمكنة في هذا المجال، يجب تحديد يوم وطني للأمن السيبراني يحتفل به جميع الليبيين، بهدف إشراك المواطنين والشركاء من القطاعين العام والخاص من خلال الفعاليات والمبادرات، يمكن اعتماد نماذج وأطر عالمية شهيرة، مثل نموذج المبادرة الوطنية لتعليم الأمن السيبراني (NICE) الذي طوره المعهد القومي الأمريكي للمعايير القياسية والتكنولوجية(NIST) ، والإطار السعودي لكوادر الأمن السيبراني (سيوف).

الهدف الثامن: تعزيز البحث والتطوير في مجال الأمن السيبراني والتكنولوجيا الحديثة :

يجب تطوير الابتكار في مجال الأمن السيبراني والتكنولوجيا الحديثة من خلال تمويل الأبحاث وإنشاء مراكز بحثية متخصصة تدعم الأبحاث والمشاريع المبتكرة في هذا المجال بالإضافة إلى ذلك، ينبغي تشجيع الشركات الناشئة عبر حاضنات الأعمال ومراكز الريادة والابتكار، وتقديم الحوافز المالية والشهادات المهنية، يجب تحفيز الابتكار من خلال تنظيم مسابقات وجوائز، وعقد منتديات ومؤتمرات دولية، وإطلاق مبادرات في مجال الأمن السيبراني، بما في ذلك استخدام الذكاء الاصطناعي والتعلم الآلي لتحسين الكشف عن التهديدات السيبرانية والاستجابة لها.

ينبغي تعزيز بيئة تحفيز البحوث الأساسية والتطبيقية في مجال الأمن السيبراني عبر القطاعات المختلفة لضمان دعم الجهود الوطنية في هذا المجال. يجب وضع برامج بحث وتطوير تركز على الأمن السيبراني في مراكز البحوث العامة، مع نشر فعال للنتائج الجديدة والتقنيات الأساسية والأساليب والعمليات والأدوات.

كما يجب على الحكومة السعي لإقامة علاقات مع المجتمع الدولي للبحوث في المجالات العلمية المتعلقة بالأمن السيبراني، مثل علوم الحاسوب والهندسة بفروعها المختلفة، والرياضيات التطبيقية، وعلم التحفيز، بالإضافة إلى المجالات غير التقنية مثل العلوم الاجتماعية والسياسية، وإدارة الأعمال، والقانون

الهدف التاسع: تعزيز التعاون الدولي والإقليمي :

ينبغي الالتزام بالتعاون الدولي في مجال الأمن السيبراني، والاعتراف بالمسائل السيبرانية على أنها عنصر متأصل في السياسة الخارجية للدولة الليبية، من المهم تشجيع تنمية الكفاءات والمهارات التي تركز على المسائل السيبرانية (الدبلوماسية السيبرانية) لاستكمال الأساليب والعمليات الدبلوماسية التقليدية .

يجب تحديد مجالات تركيز الحكومة للأهداف طويلة الأجل للتعاون الدولي بوضوح، بما في ذلك مشاركة أصحاب المصلحة من القطاعين العام والخاص على الصعيدين الإقليمي والعالمي، قد تشمل هذه المجالات دعم وضع قواعد الأمن السيبراني في ليبيا، وتدابير بناء الثقة، والالتزام ببناء قدرات الأمن السيبراني، والانضمام إلى المعاهدات الإقليمية والدولية القائمة والاتفاقيات الثنائية أو متعددة الأطراف.

ينبغي تحديد آليات التعاون مع المنتديات الدولية للمشاركة بفعالية في المسائل السيبرانية، يمكن أن تشمل هذه الآليات منظمات إقليمية أو عالمية، ومناقشات حكومية دولية، وتحالفات في القطاعين العام والخاص، وكذلك آليات التعاون التقليدية التي تشمل مسائل الأمن السيبراني.

يجب تحديد إطار للانضمام إلى مبادرات الأمن السيبراني الإقليمية والدولية القائمة أو بناء مبادرات جديدة، وتعزيز التنسيق للاستفادة من أفضل الممارسات القائمة، كما ينبغي تشجيع المشاركة في التدريبات الإقليمية والدولية كوسيلة لدعم التعاون مع الشركاء الاستراتيجيين، والمساهمة في تماسك وتقارب نهج الأمن السيبراني.

ويجب التعامل مع الأمن السيبراني كقضية دولية تتطلب التعاون الدولي وتبادل المعلومات والقدرات، ينبغي تبني معايير فعالة للأمن السيبراني، وتحديد المبادئ الخاصة بهذه المعايير، وتعيين سلطة وقائد واضح لتنسيق وتطوير هذه المعايير، وإنشاء عملية للتواصل بشأن المواقف في المحافل الدولية القائمة.

لقد طورت العديد من دول العالم معايير وضوابط قياسية ملزمة لتحقيق حد أدنى من أهداف الأمن السيبراني، لتأمين المنظومات التكنولوجية في المؤسسات، من أشهر هذه النماذج في الولايات المتحدة هي معايير معالجة المعلومات الفيدرالية (FIPS)، والمعايير المشتركة (CC)، وضوابط الأمن والخصوصية لنظم المعلومات (NIST 800-53 r5). كما توجد نماذج عالمية لا ترتبط بدولة معينة، يمكن استخدامها كمرجعيات عامة، مثل ضوابط CIS (CIS Controls) والمعيار الدولي للأمن (ISO 27001).

كل هدف من هذه الأهداف يُشكل ركيزة أساسية في إطار بناء استراتيجية الأمن السيبراني الوطنية، ويُمثل خطوة مهمة نحو الوصول إلى نظام أمن سيبراني شامل ومتكامل يحمي مصالح ليبيا الوطنية في الفضاء السيبراني.

4.1.4.3. المرحلة الرابعة التنفيذ :

تهدف الخطة التنفيذية إلى تحقيق أثر وطني ملموس على المدى البعيد، بالإضافة إلى مكاسب سريعة على المدى القصير، سيتم تحديد الأطر الوطنية والمبادرات التي ستساعد في تحقيق الأهداف الاستراتيجية، وتحديد الموارد المطلوبة (مالية، بشرية، تكنولوجية)، مع وضع جدول زمني للتنفيذ وتحديد مؤشرات الأداء. سيظهر أثر التنفيذ من خلال الإسهام في النمو، وتقليل المخاطر، وتعزيز الثقة، مع تطور تنفيذ الاستراتيجية، والتزام الجهات الوطنية بالأدوار والمسؤوليات، والأطر والمعايير المناطة بها، ستظهر المخرجات الوطنية تحسناً كبيراً على المدى البعيد.

أولاً: الأطر الوطنية :

سيتم وضع الأطر الوطنية لتحقيق أهداف الاستراتيجية وبناء منظومة متكاملة للأمن السيبراني، حيث تضم ستة مسارات وطنية متوازنة ومتكاملة، وسيتم تنفيذها من خلال 58 مبادرة وطنية.

1. **المسار الأول: برنامج وطني لتوعية الجهات الوطنية وتمكينها :**

تعزيز برنامج توعية وطني شامل لتمكين جميع الليبيين والكيانات الوطنية من تأمين الأجزاء الخاصة بهم من الفضاء الإلكتروني، وتقديم خدمات أساسية للجهات الوطنية لرفع مستوى الأمن السيبراني لديها.

2. **المسار الثاني: نظام وطني للاستجابة لأمن الفضاء السيبراني :**

إنشاء هيكل يجمع بين القطاعين العام والخاص للتصدي للحوادث السيبرانية على المستوى الوطني وإدارة المخاطر بشكل فعال.

3. **المسار الثالث: برنامج وطني للحد من التهديدات السيبرانية ونقاط الضعف :**

تعزيز قدرات أجهزة إنفاذ القانون في منع وتحليل هجمات الفضاء الإلكتروني وتقليل تقييم نقاط الضعف الوطنية.

4. **المسار الرابع: الأمن الوطني والتعاون الدولي :**

تعزيز مكافحة التجسس السيبراني وتحسين قدرات الهجوم والاستجابة، والالتزام بالتعاون الدولي لتسهيل الحوار والشراكات بين المنظمات الدولية، وتعزيز إنشاء شبكات المراقبة والإنذار الوطنية والدولية لكشف ومنع الهجمات السيبرانية عند ظهورها.

5. **المسار الخامس: إدارة مخاطر الأمن السيبراني وتبادل المعلومات :**

- يشمل إدارة المخاطر السيبرانية وتحديد الأصول الوطنية، ووضع الخطط والسياسات والمعايير والإجراءات لمواجهة التهديدات، وآليات المراقبة والمتابعة للتأكد من التزام الجهات المعنية بذلك، بالإضافة إلى حوكمة تبادل المعلومات السيبرانية لضمان فعالية الاستجابة للحوادث.

ثانياً: المبادرات والمشاريع المقترحة لمقترح الاستراتيجية :

1. برنامج وطني للتوعية وتدريب الجهات الوطنية وتمكينها

- تطوير منصة شاملة تتيح الوصول إلى أبحاث الأمن السيبراني للجميع.
- تنظيم هاكاثونات سنوية لتعزيز الابتكار وتطوير مهارات الشباب في مجال الأمن السيبراني.
- إنشاء حاضنات تكنولوجية لدعم وتمويل المشاريع البحثية في الأمن السيبراني.
- إقامة مسابقات سنوية للابتكار التكنولوجي والأفكار الإبداعية في الأمن السيبراني.
- تقديم منح دراسية مدعومة من الدولة لتعزيز الكفاءات والخبرات السيبرانية.
- تأسيس مركز وطني للبحث في الأمن السيبراني لدعم الأبحاث والابتكارات.
- إنشاء منصات إلكترونية توعوية تقدم المعلومات والنصائح الهامة في مجال الأمن السيبراني.
- تشجيع الابتكار وريادة الأعمال في مجال الأمن السيبراني من خلال دعم المشاريع الشبابية.
- تقديم برامج تدريبية متقدمة لتأهيل المحترفين في مجال الأمن السيبراني.
- إقامة مركز وطني لتنظيم ندوات توعية دورية للمجتمع المحلي بخطورة التهديدات السيبرانية.
- إنشاء منصة لجميع البحوث رفيعة المستوى بمشاركة كل أصحاب المصلحة.
- دعم مشاريع ذات العائد المرتفع للبحث والتطوير من خلال إنشاء برامج أو صناديق بحثية.
- إنشاء تجمع للخبراء في مختلف التخصصات لتنفيذ حلول للمشاكل المتعددة والأبعاد المعقدة.

- إعداد إرشادات منهجية لتقديم برامج تدريبية متخصصة في الأمن السيبراني عبر الإنترنت.
- تأسيس مركز لتنظيم مؤتمرات محلية للأمن السيبراني لخلق اندماج بين الدوائر الأكاديمية.
- إنشاء سجل وطني يضم خبراء الأمن السيبراني المعتمدين ذوي المهارات التدريبية.
- إنشاء منصات إلكترونية ووضع سياسات للتوعية تقدم المعلومات والنصائح.
- إنشاء برامج تدريبية لتأهيل العاطلين عن العمل في مجال الأمن السيبراني وتوظيفهم في مشاريع وطنية.
- إعداد برامج تعليمية لتعريف الأطفال والشباب بأساسيات الأمن السيبراني.
- مبادرات لحماية الطفل في الفضاء السيبراني.
- مبادرة تمكين المرأة في مجال الأمن السيبراني

2. نظام وطني للاستجابة لأمن الفضاء السيبراني

- تطوير تقنيات لرصد وتحليل التهديدات باستخدام الذكاء الاصطناعي.
- إنشاء فرق متخصصة للاستجابة الفورية للحوادث السيبرانية.
- تطوير منصة لتبادل المعلومات بين القطاعين العام والخاص حول التهديدات السيبرانية.
- إعداد إطار عمل دوري لتقييم المخاطر وتقديم توصيات لتحسين الأمان.
- إعداد مسح للفرق الوطنية والقطاعية مثلCSIRT ، CERT، وCIRT
- إنشاء قاعدة بيانات للخبرات المحلية وتوظيفهم في مشاريع وطنية.
- تحسين التنسيق بين الجهات المختلفة من خلال إنشاء لجان تنسيق لتعزيز التعاون.

3. **إدارة مخاطر الأمن السيبراني وتبادل مشاركة المعلومات**

- وضع أطر عمل مشتركة لتعزيز الابتكار في الشركات الناشئة في مجال الأمن السيبراني.
- إنشاء فريق عمل داخل رئاسة مجلس الوزراء لمعالجة القضايا الخاصة بالمخاطر السيادية.
- إصدار توجيهات قانونية واضحة للشركات والمؤسسات بشأن الامتثال لمتطلبات الأمن السيبراني.
- إطلاق برامج إصلاح وتحديث للبنية التحتية التكنولوجية الضعيفة.
- إطلاق صندوق استثماري لدعم مشاريع تطوير البنية التحتية.
- إنشاء شراكات مع شركات محلية وعالمية لتبني وتطوير التقنيات المتقدمة في مجال الأمن السيبراني.
- تقديم حوافز ضريبية للشركات التي تسهم في تمويل مشاريع الأمن السيبراني الحكومية.
- إنشاء مركز أبحاث لتحليل البرمجيات الخبيثة والهجمات المعقدة والمركبة.
- دعم 30 شركة ناشئة في مجال التكنولوجيا والأمن السيبراني خلال السنوات الخمس القادمة.
- تدريب 5000 متخصص في الأمن السيبراني خلال الثلاث سنوات القادمة.

- إنشاء 10 شراكات جديدة بين القطاعين العام والخاص في مجال الأمن السيبراني كل سنة.
- نشر تقارير سنوية عن حالة الأمن السيبراني في ليبيا.

4. **الأمن القومي والتعاون الدولي في مجال الأمن السيبراني**

- وضع خطة لاعتماد المعايير ونشرها وتصميم وتنفيذ آليات الإشراف عليها.
- تأسيس لجنة وطنية لتنسيق المشاركة في المبادرات والبرامج الدولية.
- إنشاء لجنة لتبادل الخبرات والتكنولوجيا مع الدول والمنظمات الدولية.
- توقيع اتفاقيات تعاون مع الدول لتبادل المعلومات والخبرات.
- تطوير برامج لحماية البيانات الحكومية والمعلومات الرسمية خلال العامين المقبلين.
- إنشاء لجنة لمراقبة تطبيق المعايير الدولية.

5. **برنامج وطني للحد من التهديدات السيبرانية ونقاط الضعف**

- إنشاء وحدات وطنية متخصصة في مكافحة جرائم السيبرانية وحماية البيانات الشخصية.
- إنشاء مركز عمليات أمنية (SOC) متقدم يخدم كل أنحاء الدولة لرصد التهديدات السيبرانية وتحليلها.
- تأسيس مركز بيانات مملوك للدولة لضمان سيادة البيانات وحمايتها.
- تشكيل لجنة قانونية تعمل على معالجة الفجوات في التشريعات القديمة المتعلقة بالأمن السيبراني.
- تقديم منهجية موحدة لتحديد وقياس مستويات النضج للأمن السيبراني.
- إنشاء مراكز بحثية متخصصة في تطوير حلول الأمن السيبراني وتقديم دعم مالي لها.
- تطوير نظام لمتابعة وتقييم أداء الأمن السيبراني في المؤسسات الحكومية.
- وضع خطط تدقيق ومتابعة لقياس مدى امتثال المؤسسات لمتطلبات الأمن السيبراني.
- إنشاء مراكز تدريب ومعامل للتدريب على اختبارات الاختراقات وإدارة الثغرات.
- تأسيس وحدات أمن سيبراني متخصصة داخل كل مؤسسة حكومية.
- تنفيذ نظام شامل لإدارة الهوية والوصول لضمان أن الأفراد المناسبين لديهم حق الوصول إلى الموارد المناسبة.

ثالثاً: تخصيص الموارد البشرية والمالية للتنفيذ :

بعد تحديد المبادرات ذات الأولوية، يتعين على المجلس الوطني للأمن السيبراني تحديد المراكز أو اللجان الحكومية المسؤولة عن تنفيذ كل مبادرة، يجب أن يكون لكل مركز أو لجنة مسؤولية واضحة عن تنفيذ المبادرة المحددة له، كما يجب على المجلس الوطني للأمن السيبراني التواصل مع هذه المراكز، أو اللجان لتحديد الموارد المطلوبة، بما في ذلك الموارد البشرية والتكنولوجية والمالية، وتوفيرها وتأمينها لهم.

لا ينبغي النظر إلى الأهداف والمهمات في إطار الاستراتيجية على أنها تتطلب تخصيصاً للموارد مرة واحدة فقط، بل يجب مراجعة متطلبات الموارد بصفة دورية بناءً على نسبة التقدم والعراقيل الكبيرة في تنفيذ البرامج والمهمات والأهداف المدرجة ضمن الاستراتيجية.

رابعاً: مؤشرات قياس الاداء الرئيسية :

لقياس كفاءة الاستراتيجية الوطنية في تحقيق أهدافها على مدار خمس سنوات، تم تصميم عدد من مؤشرات الأداء الرئيسية؛ لقياس مستوى التقدم لكل الأهداف، كما تم تحديد خط أساس ومستهدف سنوي لكل مؤشر؛ كما موضح في الجدول رقم(3).

5.1.4.3 المرحلة الخامسة المراقبة والتقييم :

يجب على المجلس الوطني للأمن السيبراني تحديد لجنة تكون مسؤولة عن مراقبة وتقييم التقدم المحرز في تنفيذ الاستراتيجية وكفاءتها، بالتعاون مع جميع أصحاب المصلحة، يتعين على هذه اللجنة وضع جدول زمني يمتد لخمس سنوات يغطي دورة الاستراتيجية بأكملها، وإجراء تقييم دوري للنتائج ومقارنتها بالأهداف المحددة لضمان تحقيق أهداف الاستراتيجية، من الضروري أن تقوم هذه اللجنة بتقييم بيئة المخاطر الأوسع بانتظام لفهم ما إذا كانت هناك متغيرات خارجية تؤثر على نواتج الاستراتيجية، ويجب تجميع التقييم مع التوصيات المرتبطة به ورفعها إلى المجلس الوطني للأمن السيبراني، يتعين أن تشمل هذه التوصيات وسائل لتحديث خطة العمل وضمان أنها معاصرة ومستجيبة للتغيرات، بالإضافة إلى تقييم الأولويات والأهداف الخاصة بالحكومة، وأيضا يجب وضع آلية لتقييم التقدم بشكل دوري (ربع سنوي أو نصف سنوي) وتعديل الاستراتيجية حسب الحاجة بناءً على النتائج والبيانات المجمعة، ومن المهم التأكد من أن جميع المعنيين (الحكومة، القطاع الخاص، المجتمع المدني) على علم بالتقدم المحرز والتحديات التي تواجهها الاستراتيجية.

في ختام هذا الفصل، نجد أن التهديدات السيبرانية تشكل تحديًا كبيرًا للأمن القومي في ليبيا، مما يستدعي استجابة شاملة وفعالة تدمج بين التحليل الدقيق لتلك التهديدات، من خلال فهم طبيعة التهديدات السيبرانية، يمكن لليبيا بناء تحليل عميق للسياق الذي تنشأ فيه تلك التهديدات، وهذا يساهم في تعزيز القدرة على مواجهتها بفعالية، كما أن مراجعة الجهود التي بذلتها الجهات الليبية في مجال مكافحة التهديدات السيبرانية تبرز أهمية التعاون بين الجهات المختلفة واتخاذ الإجراءات الوقائية الملائمة ومع ذلك، يظل تطوير استراتيجية شاملة للأمن السيبراني ضروريًا لضمان حماية الأنظمة الحيوية والبنية التحتية الحيوية للدولة.

يمكن الاستفادة من التجارب الناجحة في بناء استراتيجيات فعالة للأمن السيبراني أن توفر رؤى قيمة لتوجيه الجهود المحلية نحو تعزيز الأمن السيبراني، ومن خلال تطبيق مقترح إطار الاستراتيجية الوطنية، يمكن لليبيا تعزيز قدراتها في مجال الأمن السيبراني وضمان استدامة وحماية أمنها القومي في مواجهة التحديات الناشئة.

جدول رقم (3) مؤشرات قياس الاداء الرئيسية

الهدف	مؤشرات الآداء	الموارد المطلوبة	الوقت المتوقع
الأول	نسبة الأنظمة التي تم تحديثها لتتوافق مع معايير الأمان الحديثة. عدد نقاط الضعف التي تم اكتشافها ومعالجتها. شمولية القطاعات الحيوية التي تم تحديدهم.	استثمارات في تحديث الأجهزة والبرمجيات. فرق تقنية متخصصة في إدارة البنية التحتية. أدوات لرصد الأداء والأمان.	2028-2025
الثاني	عدد الحوادث السيبرانية التي تم التعامل معها بنجاح. عدد فرق الاستجابة للحوادث الأمنية الحاسوبية القطاعية والوطنية التي تم إنشاؤها نسبة الحوادث التي تم حلها ضمن الإطار الزمني المحدد.	فرق متخصصة في الاستجابة للحوادث. أدوات وتقنيات متقدمة لرصد الحوادث وتحليلها. تدريب مستمر للفرق على أحدث التهديدات والتقنيات.	2027-2025
الثالث	عدد القوانين واللوائح التي تم إصدارها. نسبة الامتثال للقوانين الجديدة. عدد الحالات القانونية التي تم التعامل معها بنجاح.	فرق قانونية متخصصة. استشارات قانونية. ميزانية لدعم تطوير الإطار القانوني.	2026-2025
الرابع	عدد التقارير الدورية التي تم نشرها. نسبة الشكاوى التي تم التعامل معها بشفافية. مستوى رضا الجمهور عن الشفافية والمساءلة.	فرق متخصصة في الشفافية والمساءلة. أدوات لرصد الأداء والإبلاغ. ميزانية لدعم مبادرات الشفافية.	2029-2025
الخامس	عدد الشراكات والمبادرات المشتركة بين القطاعين. عدد ورش العمل والندوات المشتركة. نسبة المشاريع المشتركة التي تم تنفيذها بنجاح.	منصات للتواصل والتعاون. فرق متخصصة في إدارة الشراكات. ميزانية لدعم المبادرات المشتركة.	2029-2025
السادس	عدد البرامج التدريبية التي تم تطويرها وتنفيذها. نسبة المشاركين الذين أكملوا البرامج بنجاح. مستوى رضا المشاركين عن البرامج التدريبية.	خبراء في تطوير المناهج التدريبية. منصات تعليمية وتدريبية. ميزانية لدعم البرامج التدريبية.	2027-2025
السابع	عدد حملات التوعية التي تم تنفيذها. نسبة الجمهور المستهدف الذي تم الوصول إليه. عدد فعاليات التوعية العامة(المؤتمرات وورش العمل).	فرق متخصصة في التوعية والتدريب. مواد تعليمية وتوعوية. ميزانية لدعم حملات التوعية.	2029-2025
الثامن	عدد الأبحاث والدراسات التي تم نشرها. عدد براءات الاختراع المسجلة. نسبة التمويل المخصص للبحث والتطوير.	فرق بحثية متخصصة. مختبرات وأدوات بحثية. ميزانية لدعم البحث والتطوير	2029-2025
التاسع	عدد الاتفاقيات الدولية التي تم توقيعها. عدد المشاريع والمبادرات المشتركة مع الدول الأخرى. نسبة المشاركة في المؤتمرات والفعاليات الدولية.	فرق متخصصة في العلاقات الدولية. منصات للتواصل والتعاون الدولي. ميزانية لدعم التعاون الدولي	2029-2025

الخاتمة

تحول الفضاء السيبراني إلى ساحة صراع جديدة، حيث تتجلى التحديات الأمنية بأشكال متعددة ومتجددة، وقد كشفت هذه الدراسة عن عمق هذه التحديات وتأثيرها المباشر على الأمن القومي للدول، لا سيما في دول مثل ليبيا، فالتطور المتسارع للتقنيات الرقمية، وما يرافقه من زيادة في الهجمات السيبرانية المعقدة، قد خلق بيئة محفوفة بالمخاطر تتطلب استجابات سريعة وحلولاً مبتكرة.

تم تحليل طبيعة التهديدات السيبرانية المتنوعة، التي تواجه الدول، وبخاصة ليبيا، بما في ذلك التي تستهدف البنية التحتية الحيوية والبيانات الحساسة، وقد أظهرت هذه الدراسة أن التهديدات تأتي من مصادر متعددة، بما في ذلك الجهات الفاعلة غير الحكومية، والهجمات المدعومة من دول، مما يعكس تعقيد البيئة الأمنية الرقمية، وقد تم تقييم الجهود المحلية المبذولة لتعزيز الأمن السيبراني مثل الاتفاقيات والمبادرات الإيجابية وأيضا جهود المنظمات الدولية والمحلية، وكما تم تسليط الضوء على استراتيجيات وطنية لبعض الدول الرائدة في هذا المجال.

الأمن السيبراني لم يعد مجرد مسألة تقنية تتعلق بحماية الأنظمة والشبكات، بل أصبح مكونًا جوهريًا، ضمن استراتيجيات الحفاظ على الأمن القومي للدول. وقد كشفت التطورات التي حدثت في ليبيا، منذ سنة 2011م، عن تزايد التهديدات السيبرانية من حيث العدد والتعقيد، ما شكل خطرًا كبيرًا على استقرار القطاعات الحيوية، بما في ذلك المؤسسات الحكومية، القطاع المصرفي، البنية التحتية للطاقة، وقطاع الاتصالات. سلطت هذه التهديدات الضوء على ضعف البنية التحتية الرقمية في ليبيا، نتيجة لتقادم الأنظمة وغياب تقنيات الحماية المتطورة، بالإضافة إلى نقص التشريعات المحلية التي تنظم وتحمي الفضاء السيبراني.

ختامًا، يتضح أن الأمن السيبراني يتطلب تكامل الجهود الدولية، وإن التصدي للتهديدات السيبرانية ليس مجرد مسؤولية تقنية، بل هو مسؤولية وطنية تتطلب وعيًا جماعيًا وتعاونًا مستدامًا، ومن خلال تنفيذ التوصيات المطروحة في هذه الدراسة، يمكن لليبيا أن تبني نظامًا قويًا للأمن السيبراني، يساهم في حماية مصالحها الوطنية وضمان استقرارها في عالم رقمي متزايد.

تأمل الباحثة أن تكون هذه الدراسة نقطة انطلاق للجهود المستقبلية التي ينبغي على الباحثين وصناع القرار أن يبدلوها لتعزيز الأمن السيبراني في ليبيا والحفاظ على الأمن القومي والاستقرار، لقد حاولنا التوجه نحو فهم أعمق لهذه التحديات، والآن يأتي دور الحكومة الليبية في تطبيق الخطط والإجراءات اللازمة لحماية الدولة ومواطنيها من أي تهديدات سيبرانية مستقبلية.

النتائج :

- إن أدوات التهديدات السيبرانية شاملة لا تقتصر على البرمجيات الخبيثة، الاختراقات الإلكترونية، التصيد الاحتيالي، والهجمات بالحرمان من الخدمة.
- أن التأثيرات الناتجة عن التهديدات السيبرانية تختلف بناءً على الهدف المستهدف.
- على الرغم من الجهود المبذولة، فأنه لا يوجد إطار دولي شامل يحكم التهديدات السيبرانية هذا يؤكد على ضرورة تعزيز التعاون الدولي وتبادل المعلومات لمكافحة التهديدات السيبرانية بشكل أفضل وتحقيق الأمن السيبراني.
- أصبح الأمن السيبراني ضرورة لا غنى عنها في العصر الحديث، حيث أصبح يشمل مجموعة واسعة من الجهود والسياسات والتقنيات التي تهدف لحماية الأنظمة الرقمية والمعلومات من التهديدات السيبرانية ويجب على كل دولة الالتزام بها .
- أن جهود الحكومة الليبية في مجال الأمن السيبراني لا يزال غير كافي، وهناك حاجة ملحة لتعزيز القدرات وتطوير استراتيجيات فعالة.
- إن التهديدات السيبرانية تشكل تحديًا تقنيًا وسياسيًا، يتطلب تبادل معلومات وتعاون دولي لضمان مواجهتها بنجاح.
- أهمية تحسين الوعي والتدريب في مجال الأمن السيبراني بين المؤسسات والفرق العاملة في هذا المجال لرفع مستوى الاستعداد والحماية.
- هناك نقصًا في الوعي العام حول الأمن السيبراني بين الأفراد والمؤسسات في ليبيا، بالإضافة إلى نقص في برامج التدريب المتخصصة، مما يزيد من تعرض البلاد للهجمات.
- الحاجة الملحة لتطوير استراتيجية وطنية شاملة للأمن السيبراني في ليبيا تتضمن جميع القطاعات وتحدد المسؤوليات بوضوح.
- أن التعاون الدولي في مجال تبادل المعلومات والخبرات يمكن أن يعزز من قدرة ليبيا على مواجهة التهديدات السيبرانية، ويجب أن يكون جزءًا من الاستراتيجية الوطنية.
- ضرورة الاستثمار في تطوير البنية التحتية للأمن السيبراني في ليبيا، بما في ذلك إنشاء مراكز وطنية متخصصة لمراقبة وتحليل التهديدات.
- أهمية وجود آليات استجابة سريعة وفعالة للتعامل مع الحوادث السيبرانية في ليبيا، بما في ذلك خطط الطوارئ والتدريب المنتظم.
- ضرورة مراجعة وتحديث السياسات والإجراءات المتعلقة بالأمن السيبراني بشكل دوري لضمان فعاليتها في مواجهة التحديات المستمرة.

- الزيادة الملحوظة في عدد التهديدات السيبرانية التي تستهدف المؤسسات الحكومية والخاصة في ليبيا، خاصة منذ عام 2011، مما يعكس ضعف البنية التحتية للأمن السيبراني.
- إن الأوضاع السياسية غير المستقرة في البلاد تؤثر سلبًا على تطوير السياسات الأمنية، حيث يتم تحويل الموارد والاهتمام إلى قضايا أخرى.
- هناك مبادرات محلية تسعى لتعزيز الوعي بالأمن السيبراني وتطوير المهارات، لكن هذه المبادرات تحتاج إلى دعم أكبر من الحكومة والمجتمع الدولي.
- على الرغم من التحديات السياسية التي تواجه البلاد، فإنها تمكنت من إحراز تقدم ملحوظ في مؤشر الأمن السيبراني خلال السنوات الأخيرة.
- ليبيا تواجه تحديات كبيرة في مجال الأمن السيبراني نتيجة لمجموعة متنوعة من التهديدات، من بين تلك التهديدات البارزة هجمات الفدية، هجمات حجب الخدمة، كما تشمل التهديدات الأخرى مثل أحصنة طروادة والبرمجيات الخبيثة التي تستخدم للتسلل إلى الأنظمة والشبكات بغرض الإضرار بها.
- أدت الهجمات الإلكترونية إلى إعادة تقييم استراتيجيات الأمن القومي، حيث أصبحت الدول الكبرى تدرك أن التهديدات السيبرانية يمكن أن تؤثر على البنية التحتية الحيوية والأمن الداخلي.
- تسببت الهجمات السيبرانية في خسائر اقتصادية كبيرة، حيث تكبدت الشركات والدول تكاليف باهظة نتيجة تعطيل الأنظمة، وسرقة البيانات، وعمليات الفدية.
- دفعت التهديدات السيبرانية الدول الكبرى إلى تعزيز التعاون الدولي لمواجهة هذه المخاطر، مما أدى إلى إنشاء تحالفات جديدة وتطوير معايير مشتركة للأمن السيبراني.

التوصيات :

- أن تقوم الحكومة الليبية بتنفيذ مقترح الاستراتيجية الوطنية للأمن السيبراني .
- إنشاء مركز وطني للأمن السيبراني يكون مسؤول عن تنسيق جهود الأمن السيبراني على مستوى الدولة.
- على الحكومة الليبية تعزيز التعاون مع الدول الأخرى ومنظمات الأمن السيبراني الدولية والانضمام إلى المبادرات والاتفاقيات الإقليمية والدولية .
- وضع معايير وممارسات أمنية إلزامية للمؤسسات الحكومية والخاصة.
- تعزيز التنسيق بين الوزارات والهيئات الحكومية لضمان تبادل المعلومات حول التهديدات السيبرانية والاستجابة لها بشكل متكامل.
- على الحكومة الليبية توجيه المزيد من الموارد المالية نحو تطوير البنية التحتية الرقمية وشراء أنظمة أمان متقدمة.
- الاستفادة من الخبرات الدولية في مجال الأمن السيبراني من خلال التعاون المستمر وتبني أفضل الممارسات العالمية.
- على الحكومة الليبية الاستمرار في تحديث التشريعات والسياسات الخاصة بالأمن السيبراني لمواكبة التطورات التقنية والتهديدات الجديدة.

المصادر والمراجع

أولاً المصادر:

1. البعلكي. منير. (2004). المورد الحديث قاموس انجليزي – عربي. دار العلم للملايين. لبنان. بيروت.
2. الحكومة الليبية المؤقتة، ديوان رئاسة الوزراء، قرار مجلس الوزراء رقم (28) لسنة 2013 م بإنشاء الهيئة الوطنية لأمن وسلامة المعلومات.
3. الاتحاد الإفريقي، اتفاقية الاتحاد الإفريقي (مالابو) بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي، https://2u.pw/2A67PB
4. الاتحاد الدولي للاتصالات وأخرون، دليل لوضح استراتيجية وطنية للأمن السيبراني(التزام استراتيجي بالأمن السيبراني).2018. http://creativecommons.org
5. المنتدى العالمي للأمن السيبراني (2020). نظرة عامة على أدوات تقييم القدرات السيبرانية القائمة على الصعيد الوطني(GOAT)
6. الاتحاد الدولي للاتصالات واخرون، العمل الاستراتيجي في مجال الأمن السيبراني، دليل إعداد الاستراتيجيات الوطنية للأمن السيبراني. الطبعة الثانية.2021.-https://creativecommons.org/licenses/by-nc/3.0/igo/U.
7. الاستراتيجية الوطنية للأمن السيبراني، الهيئة الوطنية الليبية للأمن وسلامة المعلوماتعلى شبكة الأنترنت : https://2u.pw/9UJMVF
8. الأمم المتحدة، الجمعية العامة . اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية. 2024.
9. الهيئة الوطنية الأمن وسلامة المعلومات. (2021). السياسات الوطنية لأمن وسلامة المعلومات (2.0 الإصدار الثاني ، تاريخ الزيارة 2024/4/4، https://www.nissa.gov.ly
10. الهيئة الوطنية الأمن وسلامة المعلومات. (2019). السياسات الوطنية لأمن وسلامة المعلومات الإصدار الأول . https://www.nissa.gov.ly
11. جامعة الدول العربية. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات،2010 www.arablegalent.org.
12. جامعة الدول العربية والمنظمة العربية للتكنولوجيات الاتصال والمعلومات.الرؤية العربية للأمن السيبراني الواقع-التحديات – الفرص،2021.
13. جامعة الدول العربية والمنظمة العربية للتكنولوجيات الاتصال والمعلومات، الاستراتيجية العربية للأمن السيبراني 2023-2027.
14. مجموعة المعاهدات الأوروبية رقم 185، الاتفاقية المتعلقة بالجريمة الالكترونية (بودابست) 2001 https://2u.pw/LXPNcj
15. المجلس الأوروبي. المذكرة التفسيرية لاتفاقية بودابست 2001 النسخة المترجمة بالعربية، https://rm.coe.int/budapest
16. مجلس النواب الليبي، قانون رقم 5 لسنة 2022م بشأن مكافحة الجرائم الإلكترونية.

17. مجلس النواب الليبي، قانون رقم(6) لسنة 2022م بشأن المعاملات الالكترونية
18. قاموس أكسفورد المصور. إنجليزي – عربي. Parnwell، E. C. Oxford English Arabic picture dictionary
19. ديوان وزارة الاقتصاد والتجارة بحكومة الوحدة الوطنية، (2024). قرار رقم 150 لسنة 2024. https://www.economy.gov.ly/report/2024 .

ثانيا: المراجع (العربية) :

أ. الكتب :

1- ئاكرة يى نجدت(2011)، الإطار القانوني للأمن القومي دراسة تحليله(ط1)**.** دار دجلة. الأردن. عمان..
2- الحلبي، هشام (2020). حروب الجيل الرابع والأمن القومي فهم التغير في شكل الحرب (ط1). أبوظبي: مركز الإمارات للدراسات والبحوث الاستراتيجية.
3- حمد، ثائر خليل (2016). الأمن القومي الأمريكي والتغيير في المنطقة العربية (ط1). عمان: دار الحامد للنشر والتوزيع.
4- خليفة، إيهاب (2020). مجتمع ما بعد المعلومات تأثير الثورة الصناعية الرابعة على الأمن القومي (ط1). المستقبل للأبحاث والدراسات المتقدمة. القاهرة: العربي للنشر والتوزيع.
5- خليفة، إيهاب، (2021). الحرب السيبرانية الاستعداد لقيادة المعارك العسكرية في الميدان الخامس (ط1). المستقبل للأبحاث والدراسات المتقدمة . القاهرة: العربي للنشر والتوزيع.
6- خليفة، إيهاب (2017). القوة الإلكترونية كيف يمكن أن تدير الدول شؤونها في عصر الانترنت" الولايات المتحدة الأمريكية أنموذجاً (ط1). القاهرة: العربي للنشر والتوزيع.
7- رجب، إيمان (2017). الأمن القومي العربي: تحول خريطة التهديدات والاستراتيجية المقترحة للمواجهة. معهد البحوث والدراسات العربية. القاهرة https://acpss.ahram.org.eg/News/16590.aspx
8- العمري، محمد محمود (2020). مدخل إلى الأمن السيبراني. الأردن، عمان: دار زهران للنشر والتوزيع.
9- الكعبي، سليمان محمد (2018). موسوعة استشراف المستقبل (ط1). الإمارات العربية المتحدة: دار قنديل للطباعة والنشر والتوزيع.
10-منصور، شادي عبد الوهاب (2019). حروب الجيل الخامس أساليب "التفجير من الداخل" على الساحة الدولية (ط1). المستقبل للأبحاث والدراسات المتقدمة. القاهرة: العربي للنشر والتوزيع.
11-نوران، شفيق (2018). أثر التهديدات الالكترونية على العلاقات الدولية: دراسة في أبعاد الأمن الالكتروني(ط1). القاهرة: المكتب العربي للمعارف.

ب. الرسائل العلمية (رسائل الماجستير والأطروحات) :

1. الموصلي، نور أمين (2021). **الهجمات السيبرانية في ضوء القانون الدولي الإنساني**. رسالة ماجستير، الجامعة الافتراضية السورية، سوريا.
2. دحماتي، سليم (2017). ***أثر التهديدات "السيبرانية" على الأمن القومي للولايات المتحدة - أنموذجاً – (2001-2017)***. رسالة ماجستير، جامعة محمد بوضياف، المسيلة، كلية الحقوق والعلوم السياسية قسم العلوم السياسية، الجزائر.
3. رياض، أكرم (2021). ***السياسات الدولية لمكافحة الإرهاب الإلكتروني السيبراني***. رسالة ماجستير، جامعة العربي بن مهيدي أم البواقي، كلية الحقوق والعلوم السياسية، الجزائر.
4. طاجين، فريدة (2018). ***تأثير القوة السيبرانية على الاستراتيجيات الأمنية للدول الكبرى دراسة حالة الصين.*** رسالة ماجستير، جامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية قسم العلوم السياسية، الجزائر.
5. محمد ،الدام (2022). **الأمن السيبراني**. رسالة ماجستير، جامعة الشهيد حمه لخضر، الوادي كلية الحقوق والعلوم السياسية، قسم الحقوق، الجزائر.
6. عبد الواحد، صلاح حيدر(2021)، **حروب الفضاء الإلكتروني؛ دراسة في مفهومها وخصائصها وسبل مواهتها**. رسالة ماجستير، جامعة الشرق الأوسط، قسم العلوم السياسية،كلية الآداب والعلوم، عمان، الأردن.

ت. المواقع الالكترونية :

1. أبو السعود، أحمد (2017). الإرهاب الالكتروني. الموسوعة السياسية. تاريخ الزيارة: 2023/6/28. على شبكة الأنترنت https://2u.pw/NGuiL5 .
2. إبراهيم، محمد عاطف (2022). الفضاء الالكتروني وأثره على الأمن القومي للدول: الحروب الالكترونية نموذجاً. المركز الديمقراطي العربي، تاريخ الزيارة 2023/8/3 على شبكة الانترنت .htts://democraticac.ed/?p=81775
3. المنتدى الدولي للأمن السيبراني ، تاريخ الزيارة 2024/2/18 على سبكة الانترنت /Https://gcforum.org/ar،
4. المجمع القانون الليبي (2024). قرار رقم 37 لسنة 2024م بشأن اعتماد ضوابط استخدام حسابات الجهات الحكومية على منصات التواصل الاجتماعي. تاريخ الزيارة 2024/9/12 على شبكة الأنترنت . /https://www.lawlibya.ly/decision
5. البيديري، عبد الواحد (2021). استراتيجية الأمن السيبراني: دراسة حالة المغرب. المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، تاريخ الزيارة 2023/8/25 على شبكة الانترنت . https://democratiicac>de/?p=74973
6. البهي، رغدة(2019) الإرهاب السيبراني المفهوم والسمات والأنماط، المركز المصري للفكر والدراسات الاستراتيجية، تاريخ الزيارة: 14\5\2023، على شبكة الأنترنت https://ecss.com.eg/7141/ ، .
7. بالة، صباح(2019). التهديدات الأمنية. الموسوعة السياسية، تاريخ الزيارة: 9/9/ 2023 على شبكة الأنترنت .political-encyclopedia.org//: https

8. الدورة الثالثة للجنة الفنية المتخصصة للاتصال وتكنولوجيا المعلومات والاتصالات(2019)، تاريخ الزيارة2024/5/6 ، على شبكة الأنترنت https://au.int/sites/default/

9. الرمحي، مرعى على(2022). الحرب السيبرانية ومتطلبات الأمن القومي الجديدة. المركز الديمقراطي العربي، تاريخ الزيارة 2024/9/22 على شبكة الأنترنت https://democraticac.de/?p=83629

10. حمود، رؤى(2024). ابرز انواع الهجمات السيبرانية حتى عام 2021 . مجموعة ريناد المجد لتقنية المعلومات، تاريخ الزيارة 2023/9/4، على شبكة الأنترنت https://www.rmg-sa.com

11. سرحات، شوبو اوجلو (2019). تزايد استخدام الأسلحة السيبرانية في الصراعات الدولية. تاريخ الزيارة 2024/5/15 على شبكة الانترنت https://futureuae.com/ .

12. شعيتير، جازية (2023). السيبرانية على قائمة أولويات الأمن القومي. بوابة الوسط، تاريج الزيارة 2024/8/11 على شبكة الأنترنت .https://alwasat.ly/news/opinions/

13. صالح، محمد (2022). الفضاء الالكتروني وأثره على الأمن القومي للدول: الحرب الالكترونية نموذجاً. المركز الديمقراطي العربي، تاريخ الزيارة 2023/12/6 على شبكة الانترنت htpps://democraticac.de/ .

14. عبد الجواد، يارا(2021) تطور استراتيجية الدفاع للناتو بين الأمن التقليدي والأمن السيبراني.مركز الحضارة للدراسات والبحوث. تاريخ الزيارة: 2023/2/4.على شبكة الأنترنت https://2u.pw/ZugaL1 .

15. عبد الرحمان، أسامة (2020). الأمن القومي. الموسوعة السياسية، تاريخ الزيارة 2023/8/22 على شبكة الأنترنت .https://political-encyclopedia.org

16. عبد الصادق، عادل(2015). الأمم المتحدة ودعم الاستخدام السلمي للفضاء الإلكتروني. المركز العربي لأبحاث الفضاء الالكتروني، تاريخ الزيارة 2023/6/26، على شبكة الأنترنت https://accronline.com .

17. عبد الصادق، عادل(2019) الهجمات السيبرانية: أنماط وتحديات جديدة للأمن السيبراني ، تاريخ الزيارة 2023/8/17 ، على شبكة الأنترنت https://worldpolicyhub.com .

18. عبد العال، أحمد أمين(2018)، الأمن القومي العربي بين النظرية والتطبيق، المركز الديمقراطي العربي، تاريخ الزيارة: 17/ 6/ 2023 ، على شبكة الأنترنت https://democraticac.de/?p=56363

19. عبد العزيز، سارة (2017). الحرب السيبرانية التداعيات المحتملة لتصاعد الهجمات الالكترونية على الساحة الدولية. تاريخ الزيارة 2024/4/12 على شبكة الانترنت https://futureuae.com

20. عين ليبيا.(2022) القابضة للاتصالات تُعلن إحباط هجمات سيبرانية، تاريخ الزيارة 2024/7/16 ، على شبكة الأنترنت.https://www.eanlibya.com/

21. فرجان، عطية (2022). مفهوم الأمن القومي: التطور والأبعاد. المعهد المصري للدراسات، تاريخ الزيارة 2023/8/23 على شبكة الانترنت https://eipss-eg-org/ .

22. فايروس ضرب برنامج ايران النووي(2010). عربيbbc new ، تاريخ الزيارة 2023/9/18على شبكة الأنترنت/https://www.bbc.com

23. قره، فارس(2019) الأمن السيبراني. الموسوعة السياسية، تاريخ الزيارة: 2023/2/19. على شبكة الأنترنت https://2u.pw/abM5dV
24. ليبيا الأكثر عرضة لتهديدات الأمن السيبراني في أفريقيا Review Libya review/ – Libya(2023) ، تاريخ الزيارة 2024/6/10 على شبكة الأنترنت https://lywitness.com
25. موقع اتحاد الدولي للإتصالات، تاريخ الزيارة 2024/3/2 على شبكة الأنترنت،https://www.itu.int/ar .
26. وزارة الدفاع الأمريكية، تاريخ الزيارة 2023-2/7/19 ، على شبكة الأنترنت https://www.defense.gov/News
27. وقائع الحرب السيبرانية "الخفية " بين الولايات المتحدة وإيران(2021). الحرة. ترجمات – واشنطن، تاريخ الزيارة 2023/9/18 على شبكة الأنترنتhttps://2u.pw/xXB7MHYu

ث. الدوريات :

1. البابلي، عمار ياسر زهير (2021). التحديات الأمنية المعاصرة للهجمات السيبرانية. مجلة الفكر الشرطي، المجلد 30 العدد3، ص ص 19-83، الإمارات العربية المتحدة
2. البهي، رغدة (2017). الردع السيبرانى: المفهوم والإشكاليات والمتطلبات، مفاهيم استراتيجية. مصر، القاهرة: المركز العربي لأبحاث الفضاء الالكتروني.
3. السدخان، ضحي لعيبي (2021). البعد الجيو سياسي للأمن السيبراني. مجلة العلوم الإنسانية، المركز الجامعي علي كافي تندوف، المجلد 5، العدد 1، الجزائر.
4. الشادلي، ناجي محمد (يوليو 2023). الجوانب القانونية للحرب السيبرانية دراسة في إطار القانون الدولي الإنساني. مجلة روح القوانين، كلية الحقوق، العدد 103، الجزء التاني.
5. الشمري، سهام حسن علي (2020). تمظهرات الأمن السيبراني والممارسة الإعلامية وعلاقتها بصناعة الحرب النفسية الافتراضية (رؤية نقدية علائقية). جامعة بغداد مركز الدراسات الاستراتيجية والدولية، العدد 83، صص139-164.
6. الجنابي، حازم موسى والشمري، عبد الكريم عطية (2021). مطارحات هيمنة الاستراتيجية الأمريكية السيبرانية. مجلة تكريت للعلوم السياسية، العدد 24، ص ص 3-37، العراق.
7. الشمري، مصطفي ابراهيم (2021). الأمن السيبراني وأثره في الأمن الوطني العراقي. مجلة العلوم القانونية والسياسية، المجلد العاشر، العدد الأول، العراق
8. الفتلاوي، أحمد (2016). الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر. مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد الرابع، السنة الثامنة.
9. القطروني، سالم حسين (2018). الأمن الوطني الإلكتروني في ليبيا: استجابة أمنية متأخرة لواقع سياسي مغاير. مجلة شؤون دبلوماسية، الجامعة البريطانية الليبية،معهد الدراسات الدبلوماسية العددان 2 و3، ص ص 90-113، ليبيا.

10. الشمري، سهام حسن علي (2020). تمظهرات الأمن السيبراني والممارسة الإعلامية وعلاقتها بصناعة الحرب النفسية الافتراضية (رؤية نقدية علائقية). مجلة دراسات دولية، العدد 83، ص ص 139-164.
11. الشمري، عبد الكريم زهير عطية، والجنابي، حازم موسى (2021). مطارحات هيمنة الاستراتيجية الأميركية السيبرانية. مجلة تكريت للعلوم السياسية، جامعة تكريت، العدد24 ، ص ص 3-37، العراق.
12. الشمري، مصطفي ابراهيم (2021). الأمن السيبراني وأثره في الأمن الوطني العراقي. مجلة العلوم القانونية والسياسية، كلية القانون والعلوم السياسية، جماعة ديالي، المجلد العاشر، العدد الأول.
13. الفتلاوي، أحمد (2016). الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر. مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد الرابع، السنة الثامنة.
14. المطيري، خالد عبد لله (2022). دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي. مجلة البحوث الفقهية والقانونية، العدد 38.
15. إيهاب، خليفة (2017). اليوم الأسود: أساليب الاستعداد لتطور الهجمات السيبرانية، المستقبل للأبحاث والدراسات المتقدمة، العدد 21، أبوظبي.
16. العيسى، طلال ياسين، وعناب، عدي محمد (2018). المسؤولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر. جامعة عجلون الوطنية، الأردن.
17. باي، سمير(2023). التهديدات الأمنية السيبرانية: دراسة في انعكاسات الحرب الإلكترونية على الأمن القومي للدول وإستراتيجيات المقاومة. مجلة الرسالة للدراسات والبحوث الإنسانية.المجلد 8العدد 2.ص ص 189-200.
18. بارة، سميرة (2017). الأمن السسيبراني في الجزائر. المجلة الجزائرية للأمن الإنساني، جامعة قاصدي مرباح ورقلة، المجلد 7 ، العدد 2، ص ص 10-31، الجزائر.
19. بلعسل، ياسمين، وعمروش الحسين (2021). التهديدات الالكترونية والأمن السيبراني في الوطن العربي. مجلة نوميروس الأكاديمية، المجلد 2، العدد 2، ص ص 161-180.
20. بن تغري، موسى (2020). الحرب السيبرانية والقانون الدولي الإنساني. مجلة الاجتهاد القضائي، المجلد 12، عدد خاص (العدد التسلسلي 22)، جامعة يحي فارس، المدينة، الجزائر.
21. بن عربية، رياض (2022). التهديدات اللاتماثلية في الفضاء السيبراني: حروب الجيل الرابع نموذجاً. دفاتر البحوث العلمية، المجلد 10، العدد 1، المدرسة الوطنية العليا للصحافة وعلوم الإعلام، الجزائر.
22. بن عزوز، حاتم، ومنامي حليمة (2022). الأمن السيبراني والجريمة الإلكترونية في الدول ما بعد الحداثية: الولايات المتحدة – نموذجاً. مجلة الرسالة للدراسات الإعلامية، المجلد 06، العدد 02، جامعة العربي التبسي تبسة.
23. بنت عطية الله، روان (2020). الجرائم السيبرانية. المجلة الالكترونية الشاملة متعددة التخصصات، العدد 24.
24. بنت نبي ياسمين، بلعسل، وعمروش، الحسين (2021). التهديدات الإلكترونية والأمن السيبراني في الوطن العربي. مجلة نوميروس الأكاديمية، المجلد الثاني، العدد الأول، جامعة الدكتور يحي فارس المدية، كلية الحقوق، الجزائر.
25. بهلول، خلفان، توجهات كبرى تصمم مستقبل العالم في 2024. مؤسسة دبي للمستقبل، العدد 10.

26. البهى، رغدة (2017). الردع السيبراني: المفهوم والإشكاليات والمتطلبات. مجلة الدراسات الإعلامية، المركز الديمقراطي العربي، العدد الأول، جامعة القاهرة، مصر.
27. بوقرص، ساعد (2022). الأمن السيبراني: مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات واستراتيجيات خاصة. مجلة الأبحاث في الحماية الاجتماعية، المجلد 3، العدد 1، جامعة العلوم والتكنولوجيا هواري بومدين.
28. تغريد، صفاء وخميس، مهدي لبنى (2020). أثر السيبرانية في تطوير القوة. مجلة حمورابي، العدد 33-34، السنة الثامنة، الجزائر.
29. جعفري، عبد الله (2022). التهديدات السيبرانية وتأثيرها على الأمن القومي الجزائري. المجلة الإفريقية للدراسات القانونية والسياسية، جامعة أحمد دراية، المجلد 06، العدد02، الجزائر.
30. جمال الدين، هبة (2023). الأمن السيبراني والتحول في النظام الدولي، المجلد24 ، العدد1.
31. حسين، الورفلي عبير علي (2023). جرائم التجسس الإلكتروني للمعلومات الشخصية في إطار اتفاقية بودابست بشأن الجريمة الالكترونية. مجلة أبحاث بكلية الآداب جامعة سرت، المجلد 15، العدد 01.
32. حامد، سليمة مصباح (2023). التهديدات السيبرانية وانعكاساتها على الأمن القومي الليبي(التأسيس وآليات التحصين المعرفي) المؤتمر العلمي السنوي الرابع، كلية الاقتصاد والتجارة، جامعة سرت.
33. خليفة ايهاب، (2017). تنامي التهديدات السيبرانية للمؤسسات العسكرية. اتجاهات الأحداث، العدد 2.
34. خليل، حازم محمد، (2023). استغلال الفضاء السيبراني في الحروب الغير تقليدية: دراسة في الوكالة السيبرانية والارهاب السيبراني. المجلة العملية لكلية الدراسات الاقتصادية والعلوم السياسية، ، جامعة الإسكندرية، المجلد 8، العدد 15.
35. زروقة، إسماعيل (2019). الفضاء السيبراني والتحول في مفاهيم القوة والصراع. مجلة العلوم القانونية والسياسية، المجلد10 العدد 01، ص ص1016-1032.
36. زهير، عبد الكريم محمد (2022). الإرهاب السيبراني: أزمة مالية جديدة. قضايا سياسية، كلية العلوم السياسية، جامعة الموصل، العدد 64.
37. سلمان، حنان وجاسم، ابتسام (2023). القوة السيبرانية وأثرها على القوة الاقتصادية – الصين نموذجاً. مجلة مركز دراسات الكوفة، جامعة الكوفة، المجلد70، العدد 01.
38. شرف الدين، وردة (2018). الأحكام الإجرائية لمكافحة جريمة الاتجار بالبشر المرتبكة بواسطة تقنية المعلومات، دراسة ضمن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات سنه 2010. مجلة الاجتهاد القضائي، جامعة محمد خضير، العدد 16، العدد 16، الجزائر .
39. طالة، لامية (2020). التهديدات والجرائم السيبرانية: تأثيرها على الأمن القومي للدول واستراتيجيات مكافحتها. معالم للدراسات القانونية والسياسية، 4المجلد (2).ص ص 56–69.
40. شلوش، نوره (2018). القرصنة الالكترونية في الفضاء السيبراني التهديد المتصاعد لأمن الدول. مجلة مركز بابل للدراسات الإنسانية، المجلد 8، العدد2.

41. شنوف، زينب (2020). الحرب السيبرانية في العصر الرقمي: حروب ما بعد كلاوزفيتش. المجلة الجزائرية للأمن والتنمية، المجلد 9، العدد 2، المدرسة الوطنية العليا للعلوم السياسية، الجزائر.
42. صالحي، نصيرة (2021). القوة الذكية، التنافس العالمي على قوة الفضاء الالكتروني والقدرات السيبرانية. دفاتر السياسة والقانون، المجلد 13، العدد 1.
43. طالة، لامية (2020). التهديدات والجرائم السيبرانية: تأثيرها على الأمن القومي للدول واستراتيجيات مكافحتها. مجلة معالم للدراسات القانونية والسياسية، المجلد 4، العدد 2.
44. طه، جاسم (2023). التهديدات السيبرانية وانعكاسها على الأمن القومي الأمريكي. المجلات الأكاديمية العلمية، جامعة الموصل، كلية العلوم السياسية، العدد 2(32)، ص ص 2023، العراق.
45. طوالبية، محمد (2019). أيديولوجية الفضاء الرقمي: دراسة في الخلفيات المرجعية. الأكاديمية للدراسات الاجتماعية والإنسانية، العدد21، الجزائر.
46. عبد الجواد، أميرة وعبد العظيم، محمد (2020). المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام. مجلة الشريعة والقانون، العدد 35، الجزء الثالث ، مصر.
47. عبد الكريم، محمد زهير (2021). الإرهاب السيبراي: أزمة عالمية جديدة. قضايا سياسية، كلية العلوم السياسية، جامعة الموصل، العدد 64.
48. عبد الوهاب، علي محمد (2021). الإرهاب الالكتروني. مجلة مركز بحوث الشرطة، العدد 39.
49. علاء الدين، فرحات (2019). الفضاء السيبراني: تشكيل ساحة المعركة في القرن الحادي والعشرين. مجلة العلوم القانونية والسياسية، المدرسة الوطنية العليا للعلوم السياسية، المجلد 10، العدد 3، الجزائر.
50. علاء الدين، فرحات (2021). من الردع النووي إلي الردع السيبراني: دراسة لمدى تحقيق مبدأ الردع في الفضاء السيبراني. مجلة المفكر، المدرسة الوطنية العليا للعلوم السياسية، المجلد 16، العدد 01.
51. علاء الدين، فرحات (2022). الحرب السيبرانية ومستقبل الأمن العالمي. مجلة الناقد للدراسات السياسية، المدرسة الوطنية العليا للعلوم السياسية، المجلد 6، العدد ، 2الجزائر.
52. علي، خالد حنفى (2017). الصراع السيبراني التنازع العالمي على قوة الفضاء الالكتروني. ملحق مجلة السياسة الدولية، عدد أبريل.
53. علي، صفاء حسين (2020). الحرب الالكترونية في المدرك الاستراتيجي الأمريكي. جامعة بغداد، مركز الدراسات الاستراتيجية والدولية، العدد 82، ص ص 193-235 ، العراق.
54. علي، ولي بيداء (2022). التجسس السيبراني على المحفوظات الدبلوماسية. كلية القانون جامعة القادسية، العدد 1 المجلد 13.
55. غريب، حكيم (2018). الارهاب السيبراني والأمن الدولي: التهديدات العالمية الجديدة وأساليب المواجهة. المجلة الجزائرية للدرسات السياسية، المجلد 05-العدد02.
56. فرحاتي، لويزة، قنيش، مختار (2022). التهديدات السيبرانية الناجمة عن تقنيات الثورة الصناعية الرابعة، مجلة اقتصاديات الأعمال والتجارة، المجلد 7، العدد 1.

57. فريحة، كريم (2011). الجريمة الإلكترونية. جامعة عنابة، العدد 110، الجزائر.
58. فرحات، علاء الدين (2019). الفضاء السيبراني تشكيل ساحة المعركة في القرن الحادي والعشرين، المجلد 10، العدد 3،ص ص 88-107.
59. قاسمي، شعيب، وبلغيث، فؤاد (2020). الاستراتيجيات الدولية في مكافحة الجريمة السيبرانية دراسة حالة الجزائر، جامعة العربي التبسي، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية، الجزائر.
60. قاسيمي، صافية (2016). الفضاء السيبراني والاغوار الإلكترونية: إشكالية خلق فضاء عمومي افتراضي حسب المنظور.العدد 7 ، الجزائر.
61. كلاع، شريفة (2022). الأمن السيبراني وتحديات الجوسسة والاختراقات الالكترونية للدول عبر الفضاء السيبراني. مجلة الحقوق والعلوم الإنسانية، جامعة الجزائر، المجلد 15، العدد 01 ، الجزائر.
62. لامية، طالة (2020). الإرهاب السيبراني والأمن القومي: قراءة في تحولات الاستراتيجية الدفاعية. كلية علوم الإعلام والاتصال، جامعة الجزائر 3، الجزائر.
63. لطفي، وفاء (2022). الجهود الدولية في مجال مكافحة جرائم الإرهاب السيبراني: التجربة الماليزية نموذجاً، مدرسة العلوم السياسية، كلية الاقتصاد والإدارة، مصر.
64. محمد، ناصر (2022). أشكال انتهاك الفضاء السيبراني ووسائلها وآثارها. مجلة الندوة للدراسات القانونية، العدد الأربعون، السعودية.
65. مسيكة، محمد (2022). الفضاء السيبراني وتحديات الأمن القومي للدول. مجلة العلوم القانونية والاجتماعية، ، جامعة طاهري محمد، العدد الرابع، الجزائر.
66. مشوش، مراد (2019). الجهود الدولية لمكافحة الإجرام السيبراني. مجلة الواحات للبحوث والدراسات، جامعة غرداية، المجلد 12، العدد 2 ، ص ص 703-726.
67. موسى، جواد انمار (2016). حرب الفضاء الالكتروني المفهوم – الأدوات والتطبيقات. مجلة العلوم القانونية والسياسية، المجلد الخامس، العدد الثاني، كاية اليرموك الجامعة.
68. مركز نورس للدراسات (2019). الحرب السيبرانية "الالكترونية" نقلة نوعية في الاستراتيجيات العسكرية وأثر ملحوظ على العلاقات الدولية.
69. هبه، جمال الدين (يناير 2023). الامن السيبراني والتحول في النظام الدولي. معهد التخطيط القومي، المجلد الرابع والعشرين، العدد الأول،.
70. وفاء، لطفي (2022). الجهود الدولية في مجال مكافحة جرائم الإرهاب السيبراني: التجربة الماليزية نموذجاً. كلية الاقتصاد والإدارة، جامعة 6 أكتوبر، المجلد الثالث والعشرون، العدد الأول.

ج. المؤتمرات :

1. المؤتمر الثالث عشر للأمم المتحدة لمنع الجريمة والعدالة الجنائية المنعقد في الدوحة بقطر في الفترة الممتدة بين 12 و 19 أفريل 2015.

2. المؤتمر الثاني عشر للأمم المتحدة حول منع الجريمة والعدالة والجنائية المتعقد في سلفادور البرازيلية في الفترة الممتدة 12 و 19 ابريل 2010، تاريخ الزيارة 2023/12/12 على شبكة الأنترنت https://www.unodc.org/.
3. المؤتمر الدولي الثالث لأمن المعلومات والأمن السيبراني، القاهرة، 3-4 يونيو 2024، http://www.aicto.org/ar/.
4. مؤتمر ليبيا لمكافحة الإرهاب السيبراني، الأكاديمية العسكرية للعلوم الامنية والاستراتيجية،2023.
5. مؤتمر ليبيا الدولي للمخاطر السيبرانية ، 2023.
6. مؤتمر ليبيا الدولي للأمن السيبراني في بنغازي، 2023. https://akhbarlibya24.net/

ح. التقارير

1. أكاكوس للدراسات الاستراتيجية (2004). تقرير عن الانترنت في ليبيا ، على شبكة الأنترنت https://www.reallibya.org 2024/8/8
2. إندبندنت عربية(2024). تقرير إندبندنت عربية (https://www.independentarabia.com/report/2024
3. الاتحاد الدولي للاتصالات (2020). الرقم القياسي العالمي لأمن السيبراني. على شبكة الأنترنت https://www.itu.int/ar/
4. الاتحاد الدولي للاتصالات(2015). الرقم القياسي العالمي للأمن السيبراني وسمات السلامة السيبرانية. على شبكة الأنترنت https://www.itu.int/ar/
5. الاجتماع الإقليمي التحضيري للمؤتمر العالمي لتنمية الاتصالات 2010 لمنطقة الدول العربية (17-19 يناير 2010). دمشق، الجمهورية العربية السورية.
6. الأشقر، جبور منى (2016). السيبرانية هاجس العصر. دراسات وأبحاث جامعة الدول العربية.
7. الأمم المتحدة، مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، 2019.
8. تقرير الاتحاد الدولي للاتصالات (ITU) (2010). الوثيقة : RPM-ARB10/14-A قطاع تنمية الاتصالات.
9. سالم، محمد (2024). الهجمات السيبرانية تتكثف ضد المؤسسات الاقتصادية والسياسية الليبية منذ سنتين من ورائها.
10. شركة الجذور الليبية (2018). إحصائيات أمن المعلومات في ليبيا .
11. شركة الجذور الليبية(2020). احصائيات امن المعلومات في ليبيا سنة 31 ديسمبر 2020 .
12. شركة الجذور الليبية(2024). مؤشر المخاطر والتهديدات السيبرانية عن ليبيا سنة 2024.
13. مكتب الأمم المتحدة المعنى بالمخدرات والجريمة، الأمم المتحدة، دراسة شاملة عن الجريمة السيبرانية، نيويورك 2013.
14. نوران، شفيق (2014). أثر التهديدات الالكترونية على العلاقات الدولية دراسة في أبعاد الأمن الالكتروني.
15. عبد الله ، وليد(2024). الهجمات السيبرانية المتكررة تقلق المؤسسات المالية في ليبيا.

خ. المقابلات الشخصية :

1. إبراهيم سالم نجم، مدير إدارة تقنية وأمن المعلومات بالمؤسسة الوطنية للنفط أجريت المقابلة بمقر المؤسسة بمدينة طرابلس بتاريخ 2024/8/20 الساعة 10:00 صباحاً.
2. أبو بكر رمضان حدود، مدير التحول الرقمي بوزارة الحكم المحلي أجريت المقابلة بمقر الوزارة بمدينة طرابلس بتاريخ 2024/9/9 الساعة 11:00 صباحاً.
3. أحمد القنصل، رئيس قسم أمن المعلومات بالهيئة العامة لأمن وسلامة المعلومات، أجريت المقابلة بمدينة طرابلس بتاريخ 2024/8/27 الساعة 12:00 صباحاً.
4. أحمد خليفة أبو زنقرة، مدير إدارة تقنية المعلومات بشركة المدار الجديد، أجريت المقابلة بمقر الشركة بمدينة طرابلس بتاريخ 2024/8/13 الساعة 9:50 صباحاً.
5. أم السعد المهدي هندر، مدير إدارة تقنية المعلومات بشركة ليبيا للتأمين أجريت المقابلة بمقر الشركة بمدينة طرابلس بتاريخ 2024/7/25 الساعة 11:50 صباحاً.
6. أمير مصطفى بن يزيد، رئيس قسم الشبكات والدعم الفني بشركة بريد ليبيا، أجريت المقابلة بمقر البريد بمدينة طرابلس بتاريخ 2024/8/8.
7. أمين صالح، مدير المؤسسة الليبية للتقنية، أجريت المقابلة بمقر المؤسسة بمدينة طرابلس بتاريخ 2024/7/18 الساعة 11:00 صباحاً.
8. إيهاب الرفاعي، رئيس قسم الأمن السيبراني بشركة الليبية للبريد والاتصالات وتقنية المعلومات القابضة، أجريت المقابلة بمقر الشركة بمدينة طرابلس بتاريخ: 2024/8/9 الساعة 10:00 صباحاً.
9. خليفة الرياني، مدير إدارة الأمن السيبراني بشركة ليبيا للاتصالات والتقنية، أجريت المقابلة بمقر الشركة بمدينة طرابلس بتاريخ 2024/7/22 الساعة 11:00 صباحاً.
10. رفيق المزوغي العجمي، مدير مكتب التحول الرقمي بالهيئة العامة لأمن وسلامة المعلومات أجريت المقابلة بمقر الهيئة بمدينة طرابلس بتاريخ: 2024/7/23 الساعة 9:30 صباحاً.
11. زكريا الحسن الباروني، المدير العام بشركة البركة للتامين أجريت المقابلة بمقر الشركة بمدينة طرابلس بتاريخ2024/7/27 الساعة 12 صباحاً.
12. زياد خليل، المدير العام لشركة الجذور الليبية لأمن المعلومات، أجريت المقابلة أونلاين بتاريخ: 2024/7/25 الساعة 11:30 صباحاً.
13. سالم مفتاح السيوي، مدير إدارة أمن المعلومات بمصرف ليبيا المركزي، أجريت المقابلة بمقر المصرف بمدينة طرابلس بتاريخ: 2024/1/25 الساعة 9:39 صباحاً.
14. صلاح التبيني، رئيس الهيئة العامة لأمن وسلامة المعلوماتـ أجريت المقابلة بمقر الهيئة يوم 2024/2/4 الساعة 9:30 صباحاً.

15. صلاح الدين مصطفى بن سليمان، مدير إدارة مكافحة جرائم تقنية المعلومات والمستشار بشير فرج برنوص، جهاز المباحث الجنائية بوزارة الداخلية، أجريت المقابلة بمقر الوزارة بمدينة طرابلس بتاريخ: /2024/8/18 الساعة 11:00 صباحاً.
16. ضو علي زين العابدين، المدير العام لشركة الدليل الرقمي، أجريت المقابلة أونلاين بتاريخ: 2024/5/26 الساعة 6:00 مساءً.
17. طه محمد العيان، مهندس شبكات في مكتب التوثيق والمعلومات بوزارة المالية، أجريت المقابلة بمنى التوثيق في مدينة طرابلس بتاريخ: 2024/8/18 الساعة 12:00 صباحاً.
18. عادل جمعة التوفي مدير مكتب الخبراء، الهيئة العامة للاتصالات والمعلوماتية، أجريت المقابلة في مقر الهيئة بمدينة طرابلس بتاريخ: 2024/5/15 الساعة 10:30 صباحاً.
19. عبد الرحيم أبو بكر بلال، مدير إدارة الشؤون الفنية والشبكات والمهندس حسام عبد الكافي الطشاني رئيس قسم السلامة والمعلوماتية بمركز التوثيق والمعلومات بوزارة العدل، أجريت المقابلة بمدينة طرابلس بمقر المركز بتاريخ: 2024/8/8 الساعة 9:00 صباحاً.
20. عبد السلام عبد الله الحفيظ، مراقب البنية التحية بمكتب إدارة تقنية المعلومات والاتصالات بشركة الواحة للنفط، أجريت المقابلة بمقر الشركة بمدينة طرابلس بتاريخ: 2024/8/20 الساعة 10:20 صباحاً.
21. عبد الله أبو بكر الغول، مدير مكتب تقنية المعلومات الصحية بوزارة الصحة، أجريت المقابلة بمقر الوزارة بتاريخ: 2024/7/29 الساعة 12:30 صباحاً.
22. على عامر الطويل، مدير إدارة أمن المعلومات بشركة عبور لحلول الدفع الالكتروني، أجريت المقابلة أونلاين بتاريخ: 3 مارس 2024 الساعة 7 مساءً.
23. عماد صالح عاشور، مدير مكتب الإعلام وتقنية المعلومات بوزارة الاقتصاد والتجارة أجريت المقابلة بمدينة طرابلس بمقر الوزارة بتاريخ: 19 سبتمبر 2024 الساعة 11:00 صباحاً.
24. فرج أبو شعالة، مدير إدارة المعلومات والتوثيق والدعم الفني بوزارة التخطيط، أجريت المقابلة بمقر الوزارة بمدية طرابلس بتاريخ: 2024/8/22 صباحاً.
25. مؤمن التاجوري، مدير إدارة أمن المعلومات بشركة الاتحاد الدولي للخدمات المالية والالكترونية أجريت المقابلة بمقر الشركة بمدينة طرابلس بتاريخ: 2024/2/26 الساعة 12:00 صباحاً.
26. محمد جلال القريتلي، كبير مهندسي أمن الشبكات، شركة اليمامة لتقنية المعلومات ونظم الاتصالات، أجريت المقابلة اونلاين بتاريخ: 11/9/ 2024الساعة 5 مساءً.
27. محمد سيدي أحمد حمادي، مدير التحوب الرقمي بمركز التوثيق والمعلومات بوزارة التعليم العالي والبحث العلمي أجريت المقابلة بمقر الوزارة بمدينة طرابلس بتاريخ: 2024/8/6 الساعة 1 صباحاً.
28. محمد علي أبولسين، رئيس قسم البرمجة والتطبيقات بمكتب إدارة أمن المعلومات بديوان المحاسبة أجريت المقابلة بمقر الديوان بمدينة طرابلس بتاريخ: 2024/8/7 الساعة 10:00 صباحاً.

29. محمد ميلاد، المدير العام لشركة العنكبوت الليبي، أجريت المقابلة بمقر الشركة بمدينة طرابلس بتاريخ: 2024/9/10 الساعة 10:00 صباحاً.
30. محمود أبوغفة، مدير مكتب تقنية المعلومات بوزارة الخارجية والتعاون الدولي، أجريت المقابلة بمدينة طرابلس بتاريخ: 2024/5/21 الساعة 9:55 صباحاً.
31. محمود الهادي عبدو، مدير إدارة نظم المعلومات بالمفوضية الوطنية العليا للانتخابات، أجريت المقابلة في مقر المفوضية بمدينة طرابلس بتاريخ: 2024/8/19 الساعة 10:57 صباحاً.
32. مهندسين مكتب منحة الزوجة والأبناء بوزارة الشؤون الاجتماعية أجريت المقابلة بمقر الوزارة بمدينة طرابلس بتاريخ: 2024/8/4 الساعة 11:30 صباحاً.
33. هاني رضمان تربح، رئيس لجنة متابعة موقع الوزارة بوزارة المواصلات، أجريت المقابلة بمقر الوزارة طرابلس بتاريخ: 2024/8/7 الساعة 12:00 صباحاً.
34. وديع محمد الزنتوتي، مدير مكتب التوثيق وتقنية المعلومات ومهندسين التابعين للمكتب بهيئة الرقابة الإدارية أجريت المقابلة بمقر الهيئة بمدينة طرابلس بتاريخ: 2024/2/27 الساعة 11:00 صباحاً.
35. يونس أبو زيد أحمد، رئيس قسم أمن المعلومات والأمن السيبراني والمهندس علي عبد السلام خالد رئيس قسم المخاطر بالشركة الدولية للاتصالات أجريت المقابلة بمقر الشركة بمدينة طرابلس بتاريخ: 2024/9/2 الساعة 10 صباحاً.

ثانياً- المراجع الأجنبية (Foreign References):

1-Sources :

1. ENISA، NCSS good practice Guide ، desiging and implementing national cyber security strategies، 2016.
2. HM government. National cyber strategy 2022 pioneering a cyber future with the whole of the UK.
3. Ministry of communications and information technology. developing national information security strategy for the kingdom of Saudi Arabia.2011.
4. Ministry of economic Affairs and communications. Cybersecurty strategy republic of Estonia،2019-2022.
5. Microosoft، developing a national strategy for cybersecurity. foundations for ،secueity، and innovation، 2013.
6. Nato cooperative cyber defence centre of excellence،national cyber security strategy guidelines. Tallinn 2013.

7. Organization of American states(OAS) and global partners digital. national cybersecurity strategies: lessons learned and reflections from the Americas and other regions.2022

8. Republic of Mauritius. National cyber security strategy 2012-2019.

9. Global partners، involving stakeholders in national cybersecurity strategies: A Guide for policymakers.2020.

10. The white house Washington.the national strategy to secure cyberspace .2003.

2- Book :

1. Barry، Buzan (1983). People، States and Fear. London: Wheatsheaf Books، LTD.
2. Geers، Kenneth (2011). *Strategic cyber security*. Estonia: CCD COE PUBLICATION.
3. Goodman، will (2010). cyber deterrence tougher in theory than in practice (p103). Strategic studies quarterly.
4. Joseph، S. NYE (2010). cyber power. Harvard kennedy school: belfer center for science and international affairs.
5. Le Nguyen، C.، & Golman، W. (2021). Computer law & security Review، 40، 105521. Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries:'Law on the books' vs 'law in action'.
6. Marina، Magakia (2019) ، Cyber Security and Threat Policy: The United States' Efforts to Secure the Information Age. New York: Routledge.
7. Springer، P. J. (Ed.). (2017). Encyclopedia of cyber warfare. Bloomsbury Publishing USA.
8. Thomas، rid (2013). cyber war will not take place**.** America: oxford university press.
9. Tikk، eneken and mika، kerttunen(2020). Routledge handbook of international cybersecurity**.** Routledge 2 Park Square: Milton Park، Abingdon.

3.Journals :

1. Almanna، A. (2023). Cybercrime. **In Legal Translation between English and Arabic** (pp. 197-212). Cham: Springer International Publishing.

2. Benqdara، S.، Sultan، A.، & Elfergani، A. (2020a). Assessment of Security Issues in Banking Sector of Libya. **International Journal of Computer Applications**، 176(13).
3. Awosusi، O. E. (2022). The Imperative of Cyber Diplomacy and Cybersecurity in Africa: A New Means to a'Borderless' Regional End?. **Journal of African Foreign Affairs**، 9(3).
4. Bell، C (2024). Cloud computing. In MicroPython for the Internet of Things: A Beginner's Guide to Programming with Python on Microcontrollers (pp. 413-424). **Berkeley، CA: A press.**
5. Balbaa، M. E.، Eshov، M. P.، & Ismailova، N. (2022، December). The Impacts of Russian Ukrainian War on the Global Economy in the frame of digital banking networks and cyber attacks. **In Proceedings of the 6th International Conference on Future Networks & Distributed Systems** (pp. 137-146).
6. Danowitz، A.K.، Y. Nassef and S.E. Goodman. 1995. Cyberspace in the Sahara، Computing across North Africa. International Perspectives Communications of the ACM Vol. 38، No. 12.
7. Epps، Geoff van. common ground U.S and nato engahment with Russia in the studies institutes، **partnership for peace consortium of defense academies and security studies instituters،source connections** Vol 12 No 4 fall2023 pp 15-50.
8. Familoni، B. T.، & Shoetan، P. O. (2024). Cybersecurity in the financial sector: a comparative analysis of the USA and Nigeria. **Computer Science & IT Research Journal**، 5(4)، 850-877.
9. Finnemore، M.، & Hollis، D. B. (2016). Constructing norms for global cybersecurity. American .**Journal of International Law**، 110(3)، 425-479.
10. Guchua، A.، Zedelashvili، T.، & Giorgadze، G. (2022). Geopolitics of the Russia-Ukraine War and Russian cyber attacks on Ukraine-Georgia and expected threats. **Ukrainian Policymaker**، *10*(1)، 26-36.

11. Hashemzadegan، A.، & Sabooripour، M. (2023). Silencing a Nation: How the United States Restricts and Censors Iranians on the Internet. **Journal of Intercultural Communication Research**، *52*(1)، 99-124.

12. Hare، F. (2010). The cyber threat to national security: Why can't We agree?. In: Conference on cyber conflict proceedings (Vol. 15). Tallinn، Estonia: CCD COE Publications.

13. Hansel، M. (2023). Great power narratives on the challenges of cyber norm building. **Policy Design and Practice**، 6(2)، 182-197.

14. Kostyuk، N.، & Gartzke، E. (2024). Fighting in cyberspace: Internet access and the substitutability of cyber and military operations. **Journal of Conflict Resolution**، *68*(1)، 80 Ifeanyi-Ajufo، N. (2023). Cyber governance in Africa: at the crossroads of politics، sovereignty and cooperation. **Policy Design and Practice**، 6(2)، 146

15. Lin، H. (2022). Russian cyber operations in the invasion of Ukraine. **The Cyber Defense Review**، *7*(4)، 31-46.

16. Lord، K. M.، & Sharp، T. (Eds.). (2011). America's Cyber Future: Security and Prosperity in the Information Age (Vol. 1). **Washington، DC: Center for a New American Security.**

17. Madnick، B.، Huang، K.، & Madnick، S. (2024). The evolution of global cybersecurity norms in the digital age: A longitudinal study of the cybersecurity norm development process**. Information Security Journal: A Global Perspective**، 33(3)، 204-225.

18. Manikyam، K. S.، & Romala، D. V. (2021). A Critical Study On Major Issues And Implications Of Cyber Warfare. **Turkish Online Journal of Qualitative Inquiry**، 12 p32-35.

19. Nimigan، S. (2019). The Malabo Protocol، the ICC، and the idea of 'regional complementarity'. **Journal of International Criminal Justice**، 17(5)، 1005-1029.

20. Nir Kshetri (2019) .Cybercrime and Cybersecurity in Africa، **Journal of Global Information Technology Management**، 22:2، 77-81.

21. Pitney، A. M.، Penrod، S.، Foraker، M.، & Bhunia، S. (2022، July). A systematic review of 2021 microsoft exchange data breach exploiting multiple vulnerabilities**. In the international conference on smart and sustainable technologies** (SpliTech) (pp. 1-6).
22. Pratama، B.، & Bamatraf، M. (2021، April). Tallinn manual: Cyber warfare in Indonesian regulation. In IOP Conference Series: Earth and Environmental Science. **IOP Publishing**. (Vol. 729، No. 1، p. 012033).
23. Sabillon، R.، Cavaller، V.، & Cano، J. (2016). National cyber security strategies: global trends in cyberspace. **International Journal of Computer Science and Software Engineering**، 5(5)، 67.
24. Shawe، R.، & McAndrew، I. R. (2023). Increasing threats to United States of America infrastructure based on cyber-attacks. **Journal of Software Engineering and Applications**، 16(10)، 530-547.
25. strategies in Africa. In Cybersecurity capabilities in developing nations and its impact on global security. **). IGI Global**. (pp. 1-19
26. Sungkur، R. K.، & Maharaj، M. S. (2021). Design and implementation of a SMART Learning environment for the Upskilling of Cybersecurity professionals in Mauritius. **Education and Information Technologies**، *26*(3)، 3175-3201.
27. Swallow، R. C. (2023). Considering the cost of cyber warfare: advancing cyber warfare analytics to better assess tradeoffs in system destruction warfare. **The Journal of Defense Modeling and Simulation**، 20(1)، 3-37.
28. Tvaronaviciene، M.، Pleta، T.، Della Casa، S.، & Latvys، J. (2020). Cyber security management of critical energy infrastructure in national cybersecurity strategies: Cases of USA، UK، France، Estonia and Lithuania. **Insights into regional development**، *2*(4)، 802-813.
29. Van epps Geoff،common ground U.S and nato engahment with Russia in the studies institutes،published by: partnership for peace consortium ofdefense **academies and security studies instituters**،**source connections** Vol 12 No 4 fall2023 pp 15-50،17.

30. Yusuf، idown (2013). bobade،CYBER THREATS AND NATIONAL SECURITY IN NIGERIA: CHALLENGES AND OPTIONS، **ndc journal.**

4.Reports :

1. Altaher Ben Naseir، M. (n.d.). National Cybersecurity Capacity Building Framework for counties in a Transitional Phase (Using Spring Land as a case study).
2. Abdyraeva cholpon(2020). the use of cyberspace in the context of hybrid warfare،Austrian institute for international affairs.
3. Ben Naseir، M. (2024). Cybersecurity Challenges in Libya: An In-Depth Analysis of DDoS Attacks.
4. Benqdara salima،sultan almabruk، elfergani awad (2020). assessment of security issues in banking sector of Libya، international journal of computer applications.
5. Brandon valeeriano، ryan C. maness ،(2015). cyber war versus cyber realities: cyber conflict in the international system ،America: oxford university press .
6. Change، L. Y. (2020). The Palgrave Handbook of International Cybercrime and Cyberdeviance، (327-343). Legislative frameworks against cybercrime: The Budapest convention and Asia.
7. Cirstina cristina ، cyber defence in the EU preparing for cyber warfare?، European parliamentary research service ، October 2014
8. Council of Europe. (2022.). *Libya*. Octopus Project. Retrieved from
9. CSFI. (2011). Project Cyber Dawn – Libya.
10. Annegret، Bendiek' And Tobias (2015). Metzger، Deterrence theory in the cyber-century. Lessons from a state-of-the-art literature review، Lecture Notes in Informatics (LNI)، Gesellschaft für Informatik، Bonn
11. Chasdi، R. J. (2017). Corporate security crossroads: responding to terrorism، cyberthreats، and other hazards in the global business environment. Bloomsbury Publishing USA..
12. Cirlig Carmen; cristina، (2014). cyber defence in the EU preparing for cyber warfare،european parliamentary research service، members research service.
13. Cunningham، T. (2015). A cyber-threat intelligence program–how to develop one and why it matte.

14. Cunningham، T. (2015). A cyber-threat intelligence program–how to develop one and why it matters
15. Cirlig، carmen cristina.(2014) cyber defence in the EU preparing for cyber warfare،european parliamentary research service، members research service.
16. Chat Le Nguyen.(2021) Wilfred Golman Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: ،Law on the books،vs 'law in action'' computer law & security review .
17. Dcaf and BSF (2013). cybersecurty :issues،actors and challenges،
18. Dorn، T. M. (2023). US critical infrastructure: Its Importance and Vulnerabilities to Cyber and Unmanned Systems. Page Publishing Inc.
19. Deloitte. (2021). *Cybersecurity in Libya*.
20. Deszca، G.، Ingols، C.، & Cawsey، T. F. (2019). Organizational change: An action-oriented toolkit (2nd ed.). SAGE Publications.
21. Digital Ecosystem Country Assessment (DECA). (2022). In Libya Country Snapshot.
22. DOROTHY E. DENNING،(2013)" Cyber terrorism"، Global Dialogue، Autumn، 2000.
23. Eliot، L.(2015). Politics of Cyberspace: Balancing Virtual Attacks and Real-World Responses. CISD Yearbook of Global Studies.
24. Grace B. Mueller.، Benjamin Jensen.، Brandon Valeriano.، Ryan C. Maness & Jose M. Macias. (2023). Cyber Operations during the Russo-Ukrainian War: From Strange Patterns to Alternative Futures، Center for Strategic and International Studies.
25. Gharssalla، M. O. A. (2018). Exploring the use and the role of the Internet in Libya: A study of Tripoli University and Azzaway University students .In Liverpool University.
26. Global Cyber Security Capacity Centre. (2023). Cyber Maturity in Libya 2023: Final Report.
27. Goldsmith، J. (Ed.). (2022). The United States' Defend Forward Cyber Strategy: A Comprehensive Legal Assessment. Oxford University Press.
28. Gray، C. F.، & Larson، E. W. (2020). Project management: The managerial process (8th ed.). McGraw-Hill Education.

29. Hill Richard ، dealing with cyber security threats: international cooperation،ITU،and WCIT،international conference on cyber conflict،Nato ccd coe publications،Tallinn،2015.
30. House of Representatives of Libya. (2022). Law No. 6 of 2022 on Electronic Transactions.
31. Henschke، A. (2022).Cybersecurity، Critical Infrastructure، and Ethics .Cybersecurity، Critical Infrastructure، and Ethics.
32. International telecommunication Union. Global cybersecurty index 2024 5th edition.
33. ……. Global cybersecurty index (GCI) 2018.
34. ……. Global cybersecurty index(GCI)2017.
35. Iran's cyber attacks capabilities، king Feisal center for researchand Islamic studies، special report، January، 2020.
36. Izycki، E. (2022). Nation-State cyber offensive capabilities: An in-depth look into a multipolar dimension. Editora Dialética.
37. Information Security Statistics in Libya. (2018). In Report Sections (pp. 1–9).
38. James Lewis (2022). Cyber war and Ukraine. Center for Strategic and International Studies (CSIS).
39. …….. (2002) .assessing the risks of cyber terrorism ،cyber war and other cyber threats: center for strategic and international studies .
40. …….(2006). Cybersecurity and Critical Infrastructure Protection، Center for Strategic and International Studies.
41. Janson، M. (2023). Enhancing Cyberspace Monitoring in the United States Aviation Industry: A Multi-Layered Approach for Addressing Emerging Threats.
42. Jean-Sun Luigi(2016). Cyberguerre، nouveau visage de la guerre، Revue Stratégique (N° 112)، Institut de Stratégie Comparée، Paris.
43. Jonas Kjellen، (September 2018). "Russian Electronic Warfare: The role of Electronic Warfare in the Russian Armed Forces.

44. Kenney Michael (2015). cyber terrorism in a post–stuxnet world‹foreign policy research institute by Elsevier.
45. Kloppenborg‹ T. J.‹ Anantatmula‹ V.‹ & Wells‹ K. (2019). Project management: A systems approach to planning‹ scheduling‹ and controlling (13th ed.). Wiley.
46. Kello‹ Lucas (2013). The meaning of the cyber revolution. vol .38‹ no 2 ‹pp7-40. international security: Harved college and massachuseths institute of technology.
47. Lungu‹ S. (2022). Appraising the Regime of Cooperation Under the Malabo Protocol. In National Accountability for International Crimes in Africa (pp. 65-89). Cham: Springer International Publishing.
48. Lebogang‹ V.‹ Tabona‹ O.‹ & Maupong‹ T. (2022). Evaluating cybersecurity.
49. Li yuchong and liu qinghui(2021). acomprehensive review study of cyber attacks and syber security emerging trends and vrecent developments.
50. Libya Observer. (2023). LPTIC says cyber attack against Libyan communication companies not over.
51. ……. (2023). *Mellitah denies cyber attack on gas complex*. Libya Observer.
52. Mckenzie‹ T. M (2017). Is Cyber Deterrence Possible‹. Air University Press ‹Air Force Research Institute‹ Maxwell Air Force Base‹ Alabama.
53. mattias schulze‹ joseph kerscher‹Paul bochtler. (2020) cyber escalation:the conflict dyad USA /Iran as a test case‹ working paper‹swp‹ german institute for internationaland security affairs‹December.
54. McKenzie‹ T. M. (2017). Is Cyber Deterrence Possible‹. Air University Press‹Air Force Research Institute‹Maxwell Air Force Base‹ Alabama.
55. Megi Benia‹China's (2024). Cyber Operations Against the United States Critical Infrastructure.
56. Middleton‹ B. (2017). A history of cyber security attacks: 1980 to present. Auerbach Publications.
57. Michael Connell.(2014)deterring Iran; use of offensive cyber: a casestudy‹ report C N A‹ Analysis and solutions‹ Washington.
58. National Information Security & Safety Authority. (2021). National Information Security & Safety Authority (NISSA) Policy Manual Version 2.0. Tripoli‹ Libya: NISSA.

59. …….. (2023). Resolution No. 5: National Cybersecurity Strategy.

60. Naseir، M. A. B. (2021). National cybersecurity capacity building framework for counties in a transitional phase (Doctoral dissertation، Bournemouth University.

61. Organization of the Islamic Cooperation - Computer Emergency Response Team. (2023). OIC-CERT Annual Report 2023. CyberSecurity Malaysia.

62. Petar redanliev (2024) ، cyber diplomacy defining the opportunities for cybersecurtity and risks form artificial intelligence ،Iot، blockchains، and quantum computing journal of cyber security technology

63. Railton، John، (2013). "Revolutionary Risks: Cyber Technology and Threats in the 2011 Libyan Revolution" CIWAG Case Studies.

64. Rosenzweig paul، national security threats in cyberspace، halo corporation .2009

65. Scott-Railton، J. (2013). Revolutionary Risks: Cyber Technology and Threats in the 2011 Libyan Revolution. Center on Irregular Warfare and Armed Groups، U.S. Naval War College.

66. Security Week. (2023). Small botnet launches record-breaking 26 million RPS DDoS attack. SecurityWeek.

67. Shrivastava، R. (2013). International Law and Cyber-Warfare.

68. Radhi، M. A. H.، Hussien، N. M.، Mohialden، Y. M.، & Radhi، M. A. H. (2023). Reviewing organized cybercrime: a global perspective on cyber security.

69. Schreier fred، on cyberwarfare ، dcaf horizon ، 2015.

70. Schwindt، K.، Hodgson، Q. E.، Marcinek، K.، & Ma، L. (2019). Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace.

71. Stevenson، W. J. (2021).Operations management (14th ed.). McGraw-Hill Education.

72. The Record. (2023). Cloudflare says it stopped largest HTTPS DDoS attack on record last week.

73. Tarhan، K. (2022). Historical development of cyber security studies: a literature review and its place in security studies.

74. Theohary، C. A.، & Harrington، A. I. (2015). Cyber operations in dod policy and plans: Issues for congress (Vol. 5). Washington، DC: Congressional Research Service.

75. Shrivastava، R. (2013). International Law and Cyber-Warfare.

76. Sigholm، johan (2016). non state actors in cyberspace operations، Swedish national defence college.

77. Sokolsky، R.، & Rumer، E. (2020). US-Russian relations in 2030. Carnegie Endowment for International Peace.

78. Springer، P. J. (Ed.). (2017). Encyclopedia of cyber warfare. Bloomsbury Publishing USA.

79. Samuel، cherian ; sharma ، munish. 2019. India is strategic options in: a changing cyberspace. avantika printers private limited.

80. Scott-Railton، J. (2013). Revolutionary Risks: Cyber Technology and Threats in the 2011 Libyan Revolution. U.S. Naval War College Digital Commons. Available at: US Naval War College.

81. WEF (2021). Principles for board governance of cyber risk. Geneva.

82. WilGoodman .(2010).cyber deterrence tougher in theory than in practice،strategic studies quarterly .

83. Willett، M. (2023). The cyber dimension of the Russia–Ukraine War.

84. Theohary، C. A.، & Harrington، A. I. (2015). Cyber operations in dod policy and plans: Issues for congress (Vol. 5). Washington، DC: Congressional Research Service

85. Thomas rid (، 2013)cyber war will not take place ، America: oxford university press .

86. Yuriy Danyk & Tamara Maliarchuk (2020): Hybrid war and cyber-attacks: creating legal and operational dilemmas، Global Change، Peace & Security.

87. Zabierek، L.، Lawrence، C.، Neumann، M.، Sharikov، P.، Yefimova-Trilling، N.، & Saradzhyan، S. (2021). US-Russian Contention in Cyberspace. Are “Rules of the Road” Necessary or Possible.

5.WEBSITES :

1. Awati، Rahul. 2000.Fitzgibbons Laura،threats and vulnerabilities، Accessed on 20\5\2023. accessible at :https://2u.pw/htZRKO.
2. Andrew Hanna، the invisibleU.S. – Iran cyber war، Theiran primer، united states instituteof peace ، 29/july/2021، international information network accessed on 2/4/2023،https://www.iranprimer.usip
3. Arab News (2016)، Cybercrime hit 6.5m in Kingdom last year، 11 August 2016. accessed on 2/6/2024 www.arabnews.com/node/967966/saudi-arabia-
4. Baram، Marcus. 2011. Libya‘s Billions Invested in U.S. Private Equity. Big Banks. Huffington Post Online accessed on 2024/5/21http://www.huffingtonpost.com/
5. .https://www.academia.edu.
6. Catherine A Theohary and John W. Rollins، "Cyberwarfare and Cyberterrorism: In Brid"، Congressional Research Service Report، no. /R43955،March 27،2015. accessed on 2023/7/21 on www.crs.gov .
7. Biswarup، Baidya. May 5، 2023. Cyberwarfare: Growing Chinese Cyber Threats and Implications for India، Accessed: 12/7/2024 https://urlz.fr/q0Vf ، See Also: National Cyber Power Index 2022، Belfer Center for Science and International Afiairs، Accessed12/7/2024. https://urlz.fr/mMqt
8. Country Facts ، Accessed on 20/2/2023. https://2u.pw/gsHba4
9. Hlatshwayo، M. A(2023) . CYBERSECURITY IN THE DIGITAL SPACE accessed on.https://www.academia.edu.
10. CSFI. (2011). Project Cyber Dawn: Libya. Retrieved from accessed on 28/8/2024 https://www.csfi.us
11. CSIS، Significant cyber incidents ، 2/2/2023 accessed on 29/5/2024. https://2u.pw/HNcs3P
12. Cyber Capabilities and National Power: A Net Assessment، IISS، 28th June 2021، Accessed: 12/7/2024. https://urlz.fr/q0U7

13. Cyber security statistics. 2024. Accessed 2024/11/5، hptts://www.nu.edu/blog/cybersecurty-statistics.
14. Cyber security varonis،2024، Accessed 2024/8/19، hptts://www.varonis.com/blog/.
15. Check point research reports ، 2024، Accessed 2024/9/23، hptts://blog.checkpoint.com.
16. Check Point. (2023). accessed on 22/8/2024 [Check Point 2023 Cyber Security. Report] (https://www.checkpoint.com/research/2023-cyber-security-report.
17. David Dorman،2017 The Digital China "Plan" is New، but "Digital China" is Not، Digital china wins the future، accessed on 27/2/2023(، https://urlz.fr/q0Xw.
18. Datareportal. (2024). [Datareportal] accessed on 1/11/2024 (https://www.datareportal.com.
19. European Union Agency for Cybersecurity (ENISA). (2024). ENISA Threat Landscape 2024: July 2023 to June 2024. European Union accessed on 21/2/2024. Available at: ENISA Website(ENISA20Landscape%202024
20. Janczewski، lech j and Colarik Andrew M. 2008.cyber warfare and cyber terrorism IN: information science reference (an imprint of IGI global)، America
21. Hackmanac. (2024). [Hackmanac 2024 Report] accessed on 2/10/2024 (https://www.hackmanac.com/report/2024.
22. Ivanov Anton، Orkhan Mamedov. The Return of Mamba Ransomware Secure list - Information about Viruses، Hackers and Spam. N.p.، 09 Aug. 2017. Web. 13. accessed on 2024/2/21 Sept.2017.https://securelist.com/thereturn-ofmamba-ransomware/79403
23. Kaspersky. (2024). [Kaspersky 2024 Report] accessed on 25/9/2024 (https://www.kaspersky.com/report/2024).
24. Kaspersky. (2017). [Kaspersky 2017 Report] accessed on 2/9/2024 (https://www.kaspersky.com/report/2017).
25. Kaspersky company،2024، Accessed 2024/9/23،https://me-en.kaspersky.com.
26. Look at:-WEF(2021). These are the top cybersecurity challenges of 2021. accessed on 21 /3/2024 https://www.weforum.org/agenda.

27. MATT، HERBERT.(8 oct 2019). Libya's war becomes a tech battleground. Accessed on : 21/2/2023. https://2u.pw/cnD8YM .
28. Mohamed، Ahmed. (December 17، 2022). Libyan Telecom thwarts cyber-attacks ، - 20:43، Accessed on 21/2/2023. https://2u.pw/FGfAEA
29. National Information Security & Safety Authority (NISSA). (2021). National CyberSecurity Strategy، Libya. NISSA. accessed on 21/7/2024 Available at: NISSA Website(National_CyberSecurity.
30. NSFOCUS. (2023). accessed on 21/7/2024 (https://www.nsfocus.com/report/2023.
31. SMART CITIES AND CYBER THREATS،Nicolas Reys، Control risks group limited 2016 accessed on 2024/1/21. www.controlrisks.com
32. Scott-Railton، J. (2013a). Revolutionary Risks: Cyber Technology and Threats in the 2011 Libyan Revolution. CIWAG Case Studies. accessed on 21/8/2024 https://digital-commons.usnwc.edu/ciwag-case-studies/14
33. Schwartz، M. (2017) Ukraine power supplier hit by Wannacry lookalike. Bank Info Security. We- blog. Available from: accessed on 6\4\2023. https://2u.pw/G3D6kD
34. SafaAlharathy، LPTIC says cyber attack against Libyan communication companies is not over، 21/08/2023.LPTIC says cyber attack against Libyan communication companies is not over .
35. Stefanescu، D.C.، Papoi، A. New threats to the national security of states – *cyber threat. Scientific Journal of Silesian University of Technology*. Series Transport. 2020، 107، 177-182. ISSN: 0209-3324. DOI: accessed on 2023/8/21 https://doi.org/10.20858/sjsutst.2020.107.13
36. Stewart، Scott. 2011. Will Libya Again Become The Arsenal Of Terrorism? Stafor. 8 10، 2024). accessed on 2024/8/12http://www.defenceweb.co.za/ .
37. The Peninsula. 2011. Clashes as Libya Braces for Day of Anger. (February 17، 2011). http://www.thepeninsulaqatar.com/middle-east/142870-clashes-as-libya-braces-for-day-of-anger.html (accessed April 11، 2011).
38. TechnoLibya. 2010. LTT to Double ADSL and Add Extra 5gigs on Libyamax (October 7، 2010). http://www.technolibya.com/communications/ltt-to-double-adsl-and-add-extra-5gigs-on- libyamax.html (accessed 2 7، 2024).

39. The Arabic Network for Human Rights Organization. 2004. The Internet in an Arab World: A New Space for Repression? Libya، the Internet in a Conflict Zone. accessed on 21/8/2024 http://www.anhri.net/en/reports/net2004/libya.shtml.

40. Tran، C. (2021). The SolarWinds attack and its lessons. E-International Relations. accessed on 21/9/2023 https://www. e-ir. info/2021/06/17/the-solarwinds-attack-and-its-lessons.

41. TechnoLibya. (2010). Vodafone and Almadar Aljadid Sign Strategic Partnership. accessed April 10، 2011. http://www.technolibya.com .

42. TechnoLibya. 2010. LTT to Double ADSL and Add Extra 5gigs on Libyamax . accessed April 8، 2010.

43. Look at:-WEF(2021). These are the top cybersecurity challenges of 2021. accessed on 2024/3/ 21https://www.weforum.org/agenda.

44. Theohary Catherine A**.** AND ROLLINS john ، cyberwarfare and cyberterrorism : in brief ، congressional research service ، march 27 2015. accessed on 2023/8/28 www.crs.gov.

45. SlideShare. (2024). [SlideShare] accessed on) 2024/8/21https://www.slideshare.net.

46. accessed on 2024/6/2 www.arabnews.com/node/967966/saudi-arabia-

47. Stewart، Scott. (March 10، 2011). Will Libya Again Become The Arsenal Of Terrorism? Stafor. accessed April 10. 2024

48. Lyu Jinghua. (April 01،2019). What Are China's Cyber Capabilities and Intentions?، Carnegie Endowment for International Peace، Accessed، 2024/7/12. https://urlz.fr/q0Y7

49. 2023. https://2u.pw/cnD8YM .

50. TechoLibya. 2010. HP to Expand In Libyan Market. (November 22، 2010). (accessed 26 8، 2024. http://www.technolibya.com/**.**

ثالثاً: اللغة الروسية :

1. Еремян А.، Еремян Л. Международно-правовые вопросы кибероборонь. accessed on 2/12/2023 – Московский журнал международногоправа.

المـــــلاحـــــق

الملحق الأول : مقابلة الشركات الخاصة

الموضوع: دعوة لإجراء مقابلة شخصية من أجل الحصول على الإجازة العالية الماجستير *بعنوان* "التهديدات السيبرانية وتداعياتها على الأمن القومي دراسة حالة ليبيا 2011-2024"

السيد /

مع فائق التحية والاحترام ،،،

أتقدم إليكم بوافر الشـــكر والتقدير لدوركم البارز في مجال الأمن الســـيبراني في دولة ليبيا، إدراكًا لما تمتلكونه من خبرة قيمة في هذا المجال، أدعوكم بكل احترام للموافقة على إجراء المقابلة، وأنا على ثقة بأن تجاوبكم سيوفر دعامة قوية لفهم الواقع وسيقدم لنا دليلاً قيماً في سعينا لتعزيز الأمن السيبراني.

المقابلة المقررة إجراؤها معكم، والتي تتضـمن الأسـئلة المدرجة في الأسـفل، تشـكل جزءاً أسـاسـياً من الدراسـة، إذ ستسهم إجاباتكم في تقديم نظرة شاملة حول السياق الحاضر للأمن السيبراني في ليبيا على النحو الاتي:

- تقييم الإطار الحالي وتحديد النقاط العرضة للخطر وتمييز الأصول الرقمية الحرجة.
- تقييم مدى تأثير الهجمات السيبرانية على الأمن القومي.
- فهم التحديات والمخاطر السيبرانية.
- استشراف الآفاق المستقبلية لسياسات الأمن السيبراني.
- معرفة موقف ليبيا من الممارسات الدولية والأهداف الاستراتيجية للأمن السيبراني.
- تحديد سبل تطوير الوعي السيبراني بين المواطنين والمؤسسات.
- إثراء المشـــهد الليبي بمعطيات قد تســـهم في صـــياغة الحلول والتوصـــيات من أجل وضـــع استراتيجية وطنية متكاملة للأمن السيبراني.
- توجيه الدراسة نحو استراتيجيات عملية مدروسة تسهم في تعزيز منظومة الأمن السيبراني.

وأنتم أكثر من يدرك أن الأمن السيبراني هو ليس فقط تحدي للمؤسسات والجهات الحكومية بل هو شأن وطني يهم كل فرد ويؤثر بشكل مباشر على الأمن القومي.

أخيراً، أؤكد لكم الحفاظ التام على خصـوصـية وسـرية المعلومات المقدمة وسـيتم واسـتخدامها بما يخدم أهداف البحث العلمي فقط، وإلى جانب ذلك سـأكون ممتنة لتوجيهكم وملاحظاتكم التي سـتسـاهم بشـكل مباشر في إثراء الدراسة.

شكراً لكم مقدماً على دعمكم وتعاونكم، وأتطلع إلى تحديد موعد يناسبكم لإجراء هذه المقابلة.

مع خالص احترامي وتقديري لشخصكم ومكانتكم المهنية.

الاسم: **العمر:**

الوظيفة: **سنوات الخبرة:**

التخصص: **أسم الجامعة :**

المؤسسة المنتمي إليها: **دولة التخرج:**

التاريخ: **التوقيع:**

1. كيف تقيمون الوضـــع الحالي للتهديدات الســـيبرانية في ليبيا؟ هل يمكنك تقديم أمثلة على التحديات السيبرانية البارزة التي واجهت البلاد وكيف تم التعامل معها؟
2. ما هي أبرز التهديدات السيبرانية التي تواجهها المؤسسات المختلفة في ليبيا وما هي درجة تأثيرها على الأمن القومي؟ وهل تعتقد أن هناك دول أو جهات فاعلة معروفة تشـــن هجمات سيبرانية ضد ليبيا ؟
3. ما هي القطاعات الحيوية الأكثر عرضـــة للمخاطر الســـيبرانية؟ وهل قامت الحكومة الليبية باتخاذ تدابير أمنية كافية لمواجهتها ؟ وإذا لم تكن كافية، فما الأســـباب وكيف يمكن تعزيز جهود الحماية؟
4. ما هي الاستراتيجيات والسياسات التي تعتمدها الحكومة الليبية للتصدي للتهديدات السيبرانية وتعزيز الأمن السيبراني في البلاد وحماية البنية التحتية الرقمية ؟
5. ما هي الشراكات المحلية والدولية التي تساهم في تعزيز القدرات السيبرانية في ليبيا وتبادل المعلومات والتجارب؟
6. هل يوجد تشريعات سيبرانية فعالة موجودة في ليبيا؟ وإذا كان الأمر كذلك، ما هو دورها في تعزيز الحماية السيبرانية؟
7. ما هي الســـياســـات والتشـــريعات التي تنصـــحون للحكومة الليبية اعتمادها لتعزيز الحماية السيبرانية في ليبيا؟
8. كيف تتعامل الجهات المعنية في ليبيا مع اكتشـاف الاختراقات السـيبرانية ومعالجتها وتحقيق أمن البيانات والمعلومات الحساسة في الحالات القانونية؟
9. مـا هي التدابير الوقائية التي تتخذها الوزارات الليبية لتعزيز التوعية بالأمن الســـيبراني بين الموظفين والمستخدمين وزيادة مستوى الجاهزية السيبرانية؟

10.كيف ترون أهمية التعاون الدولي في مجال الأمن السـيبراني، وهل لديكم جهود تبذلونها لتعزيز التعاون مع الدول الأخرى في هذا المجال؟

11.ما هو دور المواطن الليبي في الحفاظ على الأمن السيبراني، وما هي الرسائل التي توجهونها للمواطنين لزيادة وعيهم بالمخاطر السيبرانية وكيف يمكنهم حماية أنفسهم ؟

12.هل يوجد لديكم دراسـات سـابقة أو تقارير تتعلق بالتهديدات السـيبرانية التي واجهها الأمن القومي الليبي يمكن الاستفادة منها في مجال الدراسة؟

13. ما مستوى الوعي العام والاستعداد في مواجهة التهديدات السيبرانية في ليبيا؟

14.ما هي القوانين والسياسات الحالية المتعلقة بالأمن السيبراني في ليبيا وما مدى فعاليتها؟

15.كيف تقيم التعاون بين القطاعات العامة والخاصة في مجال الأمن السيبراني؟

16.ما مستوى الاستثمارات الحالية في مجال الأمن السيبراني وما هي الاحتياجات المالية المقدرة لتعزيزه؟

17.ما هي الإجراءات التي اتخذتها الحكومة الليبية لتعزيز الأمن السـيبراني في البلاد، وما هي النصائح التي تقدمونها في هذا الصدد؟

18.في حال توليتم منصـب رئيس هيئة الأمن السـيبراني في ليبيا، ما هو النهج الذي تخططون لتبنيه لحماية الفضـاء الالكتروني، وما الأولويات التي تضـعونها في مقدمة أهدافكم لتحقيق بيئة سيبرانية آمنه؟

الملحق الثاني: مقابلة المؤسسات الحكومية

الموضوع: دعوة لإجراء مقابلة شخصية من أجل الحصول على الإجازة العالية الماجستير بعنوان

"التهديدات السيبرانية وتداعياتها على الأمن القومي دراسة حالة ليبيا 2011-2024"

السيد /

مع فائق التحية والاحترام ،،،

أتقدم إليكم بوافر الشكر والتقدير لدوركم البارز في مجال الأمن السيبراني في دولة ليبيا، إدراكًا لما تمتلكونه من خبرة قيمة في هذا المجال، أدعوكم بكل احترام للموافقة على إجراء المقابلة، وأنا على ثقة بأن تجاوبكم سيوفر دعامة قوية لفهم الواقع وسيقدم لنا دليلاً قيماً في سعينا لتعزيز الأمن السيبراني.

المقابلة المقررة إجراؤها معكم، والتي تتضمن الأسئلة المدرجة في الأسفل، تشكل جزءاً أساسياً من الدراسة، إذ ستسهم إجاباتكم في تقديم نظرة شاملة حول السياق الحاضر للأمن السيبراني في ليبيا على النحو الاتي:

- تقييم الإطار الحالي وتحديد النقاط العرضة للخطروتمييز الأصول الرقمية الحرجة.
- تقييم مدى تأثير الهجمات السيبرانية على الأمن القومي.
- فهم التحديات والمخاطر السيبرانية.
- استشراف الآفاق المستقبلية لسياسات الأمن السيبراني.
- معرفة موقف ليبيا من الممارسات الدولية والأهداف الاستراتيجية للأمن السيبراني.
- تحديد سبل تطوير الوعي السيبراني بين المواطنين والمؤسسات.
- إثراء المشهد الليبي بمعطيات قد تسهم في صياغة الحلول والتوصيات من أجل وضع استراتيجية وطنية متكاملة للأمن السيبراني.
- توجيه الدراسة نحو استراتيجيات عملية مدروسة تسهم في تعزيز منظومة الأمن السيبراني.

وأنتم أكثر من يدرك أن الأمن السيبراني هو ليس فقط تحدي للمؤسسات والجهات الحكومية بل هو شأن وطني يهم كل فرد ويؤثر بشكل مباشر على الأمن القومي.

أخيراً، أؤكد لكم الحفاظ التام على خصوصية وسرية المعلومات المقدمة وسيتم واستخدامها بما يخدم أهداف البحث العلمي فقط، وإلى جانب ذلك سأكون ممتنة لتوجيهكم وملاحظاتكم التي ستساهم بشكل مباشر في إثراء الدراسة.

شكراً لكم مقدماً على دعمكم وتعاونكم، وأتطلع إلى تحديد موعد يناسبكم لإجراء هذه المقابلة.

مع خالص احترامي وتقديري لشخصكم ومكانتكم المهنية.

الاسم: **العمر:**

الوظيفة: **سنوات الخبرة:**

التخصص: **أسم الجامعة:**

المؤسسة المنتمي إليها: **دولة التخرج:**

التاريخ: **التوقيع:**

1. ما هي التهديدات السيبرانية التي تتعرض لها (المؤسسة) من عام 2011 حتى 2024 ؟ وما مدى تأثيرها؟وما هي الجهات الدولية أو الإقليمية أو الداخلية التي تقف وراء هذه التهديدات؟
2. ما هي أبرز الهجمات السيبرانية التي شهدتها (المؤسسة) في السنوات الأخيرة؟ هل كان الهجوم عملا تخريبا؟ وما هو التخريب بشكل عام؟ وما هو الغرض منه؟
3. بالنظر إلى التهديدات السيبرانية الحالية التي تواجه (المؤسسة) التي تديرها، هل تعتبر الإجراءات الحالية كافية؟ وما هي التحديات الرئيسية التي تواجهها في تعزيز الأمان السيبراني؟ وإذا كانت هناك، فما هي وكيف يمكن التعامل معها؟
4. هل تقوم (المؤسسة) بحماية بياناتها ومعلوماتها الحساسة من الهجمات السيبرانية وفق المعايير الدولية ؟ وكيف يتم تقييم فعالية الإجراءات والتدابير السيبرانية المعتمدة؟ وما هي الخطوات المتبعة للتحسين المستمر للأمن السيبراني؟
5. ما هي السياسات والإجراءات والاستراتيجيات التي تتبعها (المؤسسة) لضمان أمن البنية التحتية السيبرانية؟
6. هل يوجد لديكم دراسات سابقة أو تقارير تتعلق بالتهديدات السيبرانية التي واجهها الأمن القومي الليبي يمكن الاستفادة منها في مجال الدراسة؟
7. هل قامت (المؤسسة) بتقديم برامج توعية مثل ورش العمل أو ندوات في مجال الأمن السيبراني على المستوى المحلي والدولي؟ واذا كان كذلك ماهي ؟

8. هل شـاركت (المؤسـسـة) في مؤتمرات محلية ودولية سـابقاً؟ ما هي الموضـوعات التي تم تناولها؟ وكيف استفادت منها ؟
9. هل هناك أي اسـتثمارات تتم في تدريب وتأهيل الكوادر العاملة في مجال الأمن السـيبراني؟ وما هي الخطوات التي تتخذها (المؤسـسـة) لتطوير قدرات هذه الكوادر لمواجهة التهديدات السيبرانية المستقبلية؟
10. هل يوجد تشـريعات سيبرانية فعالة داخل (المؤسسـة)؟ وإذا كان الأمر كذلك، ما هي وما هو دورها في تعزيز الحماية السيبرانية؟
11. هل هناك تعاون دولي يجري لمكافحة التهديدات السـيبرانية داخل(المؤسـسـة)؟ وما هو نوع هذا التعاون؟
12. ما هي الشـراكات المحلية والدولية التي تسـعى (المؤسـسـة) إلى بنائها لتعزيز القدرات السيبرانية؟ وهل يتم تبادل المعلومات والتجارب بين الأطراف المعنية؟
13. ما هي التحديات والصعوبات التي تواجه تطبيق استراتيجية وطنية للأمن السيبراني في ليبيا؟
14. ما هي الدروس المستفادة من الهجمات السـيبرانية السـابقة؟ وما هي التوصـيات والمقترحات التي يمكن تقديمها للحكومة الليبية لتحسـين الاسـتجابة للتهديدات السـيبرانية ولتعزيز الأمن السيبراني في البلاد؟
15. في حال توليتم منصـب رئيس هيئة الأمن السـيبراني في ليبيا، ما هو النهج الذي تخططون لتبنيه لحماية الفضـاء الالكتروني، وما الأولويات التي تضـعونها في مقدمة أهدافكم لتحقيق بيئة سيبرانية آمنه؟

الملحق الثالث: الاستراتيجية الوطنية للأمن السيبراني في ليبيا

لم يعد التحول الرقمي ترفاً تسعى لتحقيقه الدول ليسهل عليها أعمالها ومعاملاتها، بل أصبح أمراً محتوماً لا مفر منه تفرضه طبيعة الحياة العصرية واعتمادنا المتزايد بشكل متسارع على تقنيات الاتصالات والمعلوماتية. إذ لم يعد هناك قطاع أو صناعة يمكنها الاستغناء عما تُيسِّره لها التقنية من إمكانيات والعمل في معزل عنها. ناهيك عما توفره التقنية من حلول للكثير من المشاكل التي تواجهه بلادنا كالمركزية والبيروقراطية وما يشكله اتساع الرقعة الجغرافية من تحديات.

إلا أن عملية التحول الرقمي، وبطبيعة الحال، تنطوي على عدد من التحديات والمخاطر التي يجب أن يُسعى لمعالجتها والاستعداد للتعامل مع تبعاتها والحد من آثارها السلبية. وهو الأمر الذي نسعى إلى تحقيقه عبر تَبنِّي تقنيات وآليات الأمن السيبراني. كما أنه ومن خلال تنسيق وتوحيد جهود مؤسسات الدولة المختلفة في كل القطاعات عبر استراتيجية وطنية للأمن السيبراني يمكننا النجاح في تأمين وحماية هذا المجال الحيوي والحساس، وكذلك الحد من أي تهديدات أو مخاطر قد تُعرقل قدرتنا على تسخير التقنية لخدمة بلادنا.

1. توطئة

1.1. التحديات

1.1.1. الأمن الوطني

كما هو متوقع، ومثله مثل كل تقنية جديدة يبتكرها الإنسان، يتم استغلال الفضاء السيبراني من قبل الحكومات المختلفة كسلاح ضد خصومها ومجال لفرض سيطرتها وتحقيق مصالحها. إذ أمسى الفضاء السيبراني ثغراً جديداً يحتاج من يرابط عنده ويذود عنه. فهناك العديد من البنى الحيوية الحساسة التي تعتمد في عملها على تقنيات المعلوماتية والاتصالات مثل معامل ومركبات إنتاج النفط والغاز ومحطات الطاقة الكهربائية ومنظومات إمداد المياه. وكذلك ما تشكله شبكات الاتصالات الوطنية بمختلف أنواعها بحد ذاتها من بنية تحتية حيوية وحساسة لا غنى عنها للعديد من الأنشطة الاقتصادية للمجتمع مثل ربط المصارف وفروعها والمؤسسات الحكومية ومكاتبها في كل المدن. كما أن الكثير من الدول أحالت الفضاء السيبراني إلى مسرح جديد لبسط نفوذها بوسائل القوة الناعمة، وتستغل إمكانات وسائط التواصل الاجتماعي للتأثير في المجتمعات بما يخدم أهدافها.

2.1.1. صعوبات التنظيم

تشكل طبيعة الفضاء السيبراني الخاصة تحدياً عند محاولة الاعتماد على التشريعات التقليدية في تنظيمه، فبالرغم من أن التعاملات في الفضاء السيبراني قد تشبه شكلياً مثيلاتها في الحياة الواقعية، إلا أنها تختلف اختلافاً جوهرياً في تفاصيلها من الناحية العملية. فمثلاً، وكما نعلم جميعاً، قد يتشارك البريد الإلكتروني ومثيله العادي في الاسم والغرض، المتمثل في تيسير التواصل بين أكثر من طرف، إلا أن هذا التشابه يقف عند هذا الحد ليس أكثر، فالبريد الإلكتروني يختلف اختلافاً تاماً عن نظيره العادي من كل النواحي الأخرى، مثل طريقة العمل والحفظ والنقل والتخزين. وبالتالي فإننا سنحتاج تنظيماً وحوكمة مختلفة اختلافاً كلياً لكل منهما، والأمر سيان في كل ما يتعلق بتنظيم شؤون الفضاء السيبراني الأخرى. كما تضيف حقيقة تشارك دول العالم جميعاً لهذا الفضاء فيما بينها، ودون وجود حدود واضحة لمجال سلطة كل منها، المزيد من التعقيدات والعقبات لمساعي تنظيم وضبط الجرائم السيبرانية.

2.1.1. نقص القدرات

لا يمكن أن تلقى مسئولية الأمن السيبراني، مثله مثل أي نوع آخر من الأمن، على عاتق طرف غريب أو أجنبي، إذ حتى المؤسسات لا يمكنها أن تثق ثقة تامة في أن يقوم طرف آخر غير موظفيها بالقيام بهذه المهمة. ومع حداثة العهد بهذا المجال، تعاني صناعة الأمن السيبراني من شح حاد في الكوادر المتخصصة والخبيرة، والأمر لا يقتصر على بلادنا فحسب، بل هو نقص تعاني منه كل دول العالم. كما أن تسارع وتيرة تطور وتعقيد التهديدات والمخاطر السيبرانية يجعل من الضروري تبنّي مقاربات مختلفة وجديدة كلياً لأساليب وإجراءات الحماية والتأمين للأصول والبنى التحتية.

2.1.1. موثوقية المعاملات

بسبب اختلاف المعاملات الإلكترونية عن مثيلاتها في الحياة الواقعية في طريقة عملها اختلافاً جوهرياً، فبالتالي ستشكل طرق التحقق من سلامة وأمان هذه المعاملات تحدياً في حد ذاتها، كما ستتغير طرق المصادقة على صحة المعاملات والتحقق من هوية أطرافها وامتلاكهم صلاحية إجراءها تغيراً كلياً، الأمر الذي يحتم ضرورة تغيير وتحديث التشريعات المنظمة لها.

2.1.1. ثقافة الأمن السيبراني

لا جرم أن سهولة التواصل وتلاشي الحدود بين الدول والمجتمعات له الكثير من المزايا والفوائد، إلا أنه وفي نفس الوقت سيُسهِّل على من يريد أن يصل بضرره إلى أي طرف أو شريحة ما في المجتمع أن يفعل ذلك وبيسر لم يكن ببالغه لولا هذا المجال المفتوح المتمثل في الفضاء السيبراني. وهو الأمر الذي لم يَخْفى عن المجرمين والمخربين والمتطرفين، مما حدا بهم إلى نقل أنشطتهم إلى هذا الفضاء الرحب. ولم يقتصر الأمر على الأفراد بل أن كل الحكومات حول العالم تعمل على تطوير قدراتها السيبرانية في المجالات الدفاعية والأمنية والاستخباراتية، فيما يعرف بالحرب السيبرانية. كما اتجهت بعض الدول المتقدمة إلى تطوير أساليب وآليات تمكنها من استغلال وسائل التواصل الاجتماعي للتأثير والتغيير في المجتمعات بُغْية تحقيق أهدافها وتلبية مصالحها على حساب الدول التي تكون ضحية مثل هذه الممارسات.

2. الرؤيــة

توفير بيئة آمنة للتحول الرقمي وبناء القدرات
اللازمة لمجابهة المخاطر المصاحبة له،
وتمكين الأفراد والمؤسسات من النجاح في
الاستفادة من الفضاء السيبراني بأمان.

3. نطاق الاستراتيجيـة

4. أهداف الإستراتيجية

1.4. تعزيز وتطوير الإطار القانوني والتشريعي وضمان ترسيخ الحوكمة الرشيدة للفضاء السيبراني.

2.4. بناء ورفع القدرات البشرية والمادية الضرورية لحماية وتأمين الفضاء السيبراني والتحول الرقمي.

3.4. تعزيز موثوقية وأمان واعتمادية المعاملات الإلكترونية.

4.4. تشجيع التعاون مع الداخل والخرج، أفراداً ومؤسسات، سعياً لتوطين صناعة الأمن السيبراني.

5.4. دعم التوجه نحو التحول الرقمي عبر نشر ثقافة الأمن السيبراني في المجتمع.

5. مجالات تنفيذ الإستراتيجية

1.5. برنامج لتهيئة الأطر العامة والبيئة القانونية والتشريعية للفضاء السيبراني.

يتم خلاله العمل على سد الفراغ التشريعي في كل ما يتعلق بتأمين الفضاء السيبراني ومكافحة الجرائم السيبرانية وحماية الخصوصية وتأمين الهوية الرقمية والمعاملات الإلكترونية وحقوق الإنسان. بحيث يتم التواصل بين كل المؤسسات الوطنية الحكومية والأهلية ذات العلاقة للتشاور والعمل على إصدار القوانين المنظمة لشؤون الفضاء السيبراني واللوائح التنفيذية الخاصة بها، وخاصة التشريعات المنظمة للمعاملات الإلكترونية والجرائم السيبرانية ومكافحة الإرهاب.

2.5. برنامج لإنشاء وتطوير آليات متكاملة لحماية أمن الفضاء السيبراني وتأمين البنى التحتية الحيوية للاتصالات وتقنية المعلومات.

يعمل من خلال هذا البرنامج على توجيه المؤسسات الوطنية لإنشاء أجسام تُعنَى بمسائل الأمن السيبراني وبالأخص المؤسسات المسؤولة عن البنى الحيوية التي يجب أن تكوِّن أيضاً فرقاً خاصة للاستجابة لحوادث الأمن السيبراني (CSIRT)، وتكون مهمة الفريق الوطني (LibyaCERT) أن ينسق بين جهود كل هذه الفرق وأن يُشكِّل نقطة التواصل الرئيسية بينها ومع مثيلاتها حول العالم. ونظراً لأنه لا يمكن حماية ما لا يمكن رؤيته، فإن هذا البرنامج يستهدف إقامة مراكز عمليات أمن سيبراني تُعنى بمراقبة الأنظمة والشبكات (cSOC) بشكل مستمر للكشف عن أي مخاطر قد تُهدد هذه البنى الحيوية وكذلك تبنِّي كل الآليات الكفيلة بتوقع ومنع أي تهديدات مستقبلية محتملة الحدوث. ولتكوين صورة شاملة وموحدة لوضع الفضاء السيبراني، يتم العمل على إنشاء غرفة مركزية لعمليات الأمن السيبراني على مستوى الوطن ككل.

3.5. برنامج تجهيز البيئة الوطنية لتقنيات التشفير والتوقيع الرقمي والمصادقة على المعاملات الإلكترونية.

التحول الرقمي يعني أن تُصبح المعاملات كلها رقمية وهو الأمر الذي لن يتحقق دون أن تكون مُؤمنة عبر آلية تضمن سرية وسلامة هذه المعاملات وكذلك هوية من يقوم بها، وليتم ذلك يجب العمل على إنشاء معمارية المفتاح العام والتي تُشكل حجر الأساس الذي لا غنى عنه لرقمنة المعاملات. كما يتم أيضاً العمل على ترسيخ مفهوم الهوية الرقمية التي من شأنها تيسير وتأمين المعاملات الإلكترونية.

4.5. برنامج بناء القدرات البشرية والخبرات الوطنية في مجال الأمن السيبراني بمختلف القطاعات.

إن مسؤولية أمن الوطن مهمة منوطة بأهله دون غيرهم، والأمن السيبراني ليس استثناءً. لذا يهدف هذا البرنامج إلى بناء كوادر تقنية وطنية متخصصة بهذا النوع المهم من الأمن. وكذلك العمل على تطوير خبرات محلية متقدمة على كل الأصعدة العلمية والعملية وفي كل القطاعات يمكنها سد العجز الحالي والمستقبلي في كوادر الأمن السيبراني. كما يجب العمل على توفير التدريب والتطوير المستمر لمواكبة الطبيعة المتغيرة والمتطورة بشكل سريع لتهديدات ومخاطر الفضاء السيبراني. وهو ما يوجب الاستفادة من خبرات من سبقنا في هذا المجال عبر التواصل والتعاون معهم والاستفادة من تجاربهم بالمشاركة في المناشط الدولية المختلفة ذات العلاقة.

5.5. برنامج لدعم البحث العلمي وتعزيز روح المبادرة والابتكار وتوطين صناعة الأمن السيبراني

التهديدات والمخاطر السيبرانية دائمة التغير والتطور وبشكل متسارع، لذا يهدف هذا البرنامج إلى توفير الدعم والتشجيع لأنشطة البحث العلمي في المؤسسات الوطنية. كما يتم من خلاله العمل على تأطير المبادرات البحثية الفردية وتشجيعها وتقديم الدعم لها لما عرف عنها من قدرة متميزة غير تقليدية في كشف الكثير من التهديدات السيبرانية التي لم تتمكن المؤسسات البحثية الاعتيادية من اكتشافها. ويسعى البرنامج إلى دعم القطاع الخاص الوطني وتحفيزه لتطوير صناعة أمن سيبراني محلية تشكل رافداً وداعماً للقطاع الأهلي والحكومي.

6.5. البرنامـج الوطني لتعزيز ثقافة الأمن السيبراني للمجتمع لتحقيق الاستفادة الأفضل من التقنية.

يتم عبر هذا البرنامج بذل كل الجهود الرامية لرفع مستوى وعي المجتمع بالمخاطر والتهديدات في الفضاء السيبراني وكيف يمكن للجميع أن يستفيد مما تقدمه التقنية من فوائد دون أن يتعرضوا لما ينطوي عليه ذلك من أخطار. كما يشمل هذا البرنامج إطلاق حملات تستهدف كل شرائح المجتمع وكل الفئات العمرية وخاصة الأطفال بشكل مباشر أو عبر توعية من يحيط بهم كأولياء الأمور والمعلمين. ويجب أن تنشر ثقافة الأمن السيبراني عبر كل وسائل إيصال المعرفة المختلفة كالمناهج الدراسية والدورات المتخصصة والتلفزيون والإذاعة ومواقع التواصل الاجتماعي والمطبوعات المختلفة على سبيل المثال لا الحصر. كما يجب العمل على حماية المجتمع من مخاطر استغلال الفضاء السيبراني في نشر التطرف والترويج للأنشطة الغير قانونية.

7.5. برنامج لتأهيل وضمان التزام المؤسسات الوطنية بمعايير وضوابط وسياسات الأمن السيبراني المحلية والدولية.

يستهدف هذا البرنامج أن تلتزم المؤسسات الوطنية منذ لحظة تأسيسها وأثناء عملها بأن تجعل متطلبات الأمن السيبراني أساساً لأي من أنشطتها الحالية والمستقبلية وجزءاً محورياً لمنظومة الحوكمة لديها. يتم بناء آليات تنظيمية واضحة تضمن قيام المؤسسات العاملة في البلاد بالالتزام بما يصدر عن الجهات المنظمة لقطاع الأمن السيبراني من ضوابط وسياسات. كما يتم دعم وتشجيع المؤسسات الوطنية للعمل نحو الالتزام بالمعايير الدولية ذات العلاقة.

8.5. برنامج لتعزيز الشراكات والتعاون الدولي والإقليمي والمحلي لتأمين الفضاء السيبراني.

تضطرنا حقيقة أن الفضاء السيبراني هو مجال تشترك فيه كل دول العالم وليس مقيداً بالحدود الجغرافية التقليدية، أن نولي أهمية كبرى للتعاون والتواصل مع محيطنا الإقليمي والعالمي لكي نتمكن من تأمين هذا المجال الحيوي بالشكل الصحيح. فعادة ما يكون مصدر العديد من التهديدات والمخاطر يقع في أماكن خارج نطاق سلطة الدولة المتأثرة بنتائج تلك التهديدات. كما يتوجب أن يتم تعزيز الشراكات بين المؤسسات الوطنية المختلفة وفي كل القطاعات لكي يمكنها تبادل المعلومات والخبرات، وتوضع آلية خاصة لتبادل المعلومات حول الحوادث السيبرانية تستهدف الحد من خطر انتشار الاختراقات التي تكون قد تعرضت له إحدى المؤسسات من أن يصل ضرره لمؤسسة أخرى.

9.5. برنامج رفع جاهزية البنى التحتية لتقنية المعلومات والاتصالات للمؤسسات الوطنية لمواجهة الطوارئ والتعافي منها وضمان استمرارية الأعمال.

من أهم مميزات التحول الرقمي هو ما يقدمه من تيسير وتسهيل لأعمال وإجراءات المؤسسات والأفراد، إلا أنه في حالة لم يتم تأهيل البنى التحتية الحيوية لتقنيات الاتصالات والمعلوماتية بحيث يكون لها القدرة على التعامل مع أي تغير في الأعباء التشغيلية وأن تكون لها المرونة الكافية للتعافي بسلاسة من أي طوارئ قد تواجهها، فقد يصبح التحول الرقمي عائقاً يعرقل عمل الدولة ونقمة بدل أن يكون نعمة تُيسِّر وتسهل على المواطنين إجراءاتهم ومعاملاتهم. عليه يتوجب إلزام المؤسسات الوطنية ضمن سعيها نحو التحول الرقمي بضرورة تلبية متطلبات رفع جاهزية بُناها التحتية لمواجهة الطوارئ والتعافي منها، وكذلك تزويدها بما تتطلبه معايير استمرارية الأعمال من موارد.