التهديدات السيبرانية وانعكاساتها على الأمن القومي الليبي
(التأسيس وآليات التحصين المعرفي)

د. سليمة مصباح حامد
عضو هيئة تدريس/ جامعة سرت
salimamosbahhamed@gmail.com

الملخص:

نخلص مماسبق انه في ظل التطورات الحاصلة في مجال التكنولوجيا أصبحت قضية الأمن السيبراني من التحديات الكبرى على الصعيدين الإقليمي والعالمي ، لا سيما مع تزايد التهديدات السيبرانية الجديدة التي تصيب أمن معلومات الدول ، الأمر الذى يؤدي إلى انهيار أمنها الوطني وبالتالي انهيار الدولة تماماً ؛ وليبيا من بين الدول التي تتعرض إلى التهديدات السيبرانية لهذا أصبحت تهتم بالأمن السيبراني بشكل كبير ، وذلك بوضع مجموعة من الآليات والاستراتيجيات المحلية والدولية مبنية على التعاون مع الدول الإقليمية والعالمية للتصدي لهذه التهديدات والحد من انتشارها عن طريق إنشاء مراكز تعنى بمكافحة التجسس وحماية أمن المعلومات.

الكلمات المفتاحية: الأمن السيبراني، التهديدات السيبرانية ، الأمن القومي الليبي.

Summary:

We conclude from the above that in light of the developments taking place in the field of technology , the issue of cyber security has become one of the major challenges at the regional and global levels , Especially with the increase in cyber threats , which are considered new threats to countries' information security , Which leads to the collapse and penetration of its national security , and thus the complete collapse of the state , Libya is among the countries exposed to cyber threats , so it has become greatly concerned with cyber security , This is done by developing a set of local and international mechanisms to limit the spread of this phenomenon. It is also trying to develop strategies based on cooperation with many regional and global countries to address these threats by establishing centers concerned with combating espionage and protecting information security.

Keywords: cyber security, cyber threats , Libyan national security.

1- مقدمة:

إن مفهوم الأمن من المنظور التقليدي جسد فكرة حماية الدولة من التهديدات الداخلية الخارجية وذلك بالوسائل العسكرية فقط إلا أن هذه النظرة السائدة لفترة طويلة بدأت تتغير مع ظهور تهديدات وتحديات جديدة كالنزاعات الداخلية و التلوث البيئي والفقر والجريمة الإلكترونية والتهديدات السيبرانية وهذا ما جعل بعض المفكرين يبحثون في تطوير مجالات الأمن فقاموا بتوسيع قطاعات الأمن لتشمل قطاعات أخرى كالقطاع العسكري والسياسي و المجتمعي و البيئي بالإضافة إلى قطاع أخر وهو موضوع بحثنا والذى يركز على الجانب الإلكتروني" الأمن السيبراني" والذى أصبح في عالمنا المعاصر أكثر من كونه مسألة مرتبطة بأمن المعلومات والتقنيات بحكم علاقته المباشرة بالمجال السياسي ، والأمني ، والاقتصادي ، والاجتماعي ، والثقافي ، تعتمد عليه معظم إن لم تكن جميع المؤسسات الحيوية ، وتعاطياً مع الاختلاف والتنوع في طبيعة التهديدات الأمنية تبرز لنا التهديدات السيبرانية لتأخذ بعدا إقليمياً ودولياً خاصة بعد اتجاه العديد من دول العالم إلى الاعتماد على التكنولوجيا الإلكترونية في إدارة وتسيير منشآتها الحيوية ومؤسساتها ، بشكل جعل تدخلها ضمن حساباتها الاستراتيجية وأمنها القومي ، لكن بالرغم من المميزات التي تقدمها هذه الأخيرة إلا أن هذه الدول أصبحت عرضة لتحديات واختراقات عدة ،لاسيما تلك الهجمات الإلكترونية التي تستهدف البنية التحتية و تهدد أمنها ، الأمر الذي جعل هذه الدول تعيد قراءة العديد من حساباتها وتحاول تكييف استراتيجياتها وفقا للتغيرات الحاصلة حتى تستطيع الحفاظ على أمنها القومي وايضاً ادراج مسألة الأمن السيبراني كأحد أولويات أمنها الوطني لنشر دعائم الأمن السيبرانى.

وفي هذا السياق فإن دراسة التهديدات السيبرانية يقودنا إلى دراسة أحد الدول، وهذه الدولة هي ليبيا، التي يتعرض أمنها الوطني لهذه التهديدات، والتي ترجمت في شكل جرائم إلكترونية لم تفرق بين الأشخاص والمؤسسات والدول كما أخذت منحا تصاعدياً في الآونة الأخيرة، وهو ما ينبأ بخطورة الوضع مما جعل مؤسسات ليبيا العامة والخاصة أكثر عرضة لهذه الهجمات السيبرانية، وفرض تحديات أثرت بشكل مباشر في منظومة أمنه الوطني وتركت آثار سلبية على الأمن القومي الليبي.

ومن هذا المنطلق فإن السلطات الليبية تحاول تجاوز هذه التهديدات؛ وذلك باتخاذ الإجراءات والاحتياطات الأمنية اللازمة على الصعيدين المحلى والدولي مع وضع حلول لمواجهة هذه التهديدات الذي تترصد بأمنها الوطني لتفادي هذه الجرائم الإلكترونية المهددة لها، وذلك عن طريق وضع قوانين وتشريعات خاصة بالاستخدامات الإلكترونية الحديثة، كما تسعى جاهدة للتعاون مع بقية دول العالم

في مجال الحماية السيبرانية. عليه سوف نسلط الضوء في هذا البحث على التهديدات السيبرانية وانعكاساتها على الأمن القومي الليبي مع تبيان مفهوم الأمن السيبرانى، واهدافه، وخصائصه، ومرتكزاته، وعلاقته بالأمن القومى، والمخاطر والتهديدات السيبرانية للأمن القومي، وجهود وآليات مواجهة ليبيا للتهديدات السيبرانية وسبل الحماية منها.

2-أهمية البحث :

تكمن أهمية البحث في كونه من المواضيع المعاصرة والمطروحة حالياً على الساحة العربية والعالمية تلقى الضوء على اهم واخطر ساحات الصراع الدولي في الوقت الحالي وهو الفضاء السيرانى ، تحتل صدارة اهتمامات الباحثين والمختصين بالشأن الأمني والسياسي اذ أصبحت من أهم قضايا الأمن القومي لأية دولة وان اي تعرض للهجمات الإلكترونية سوف يؤثر مباشرةً بأمنها القومي ، وفيما يتعلق بليبيا؛ زادت أهمية الأمن السيبراني بحكم الاستخدام الواسع للفضاء السيبراني وتصاعد التهديدات السيبرانية وتأثيرها وانعكاساتها على الأمن القومي الليبي.

3-أهداف البحث:

ما تشكله التهديدات السيبرانية على دول العالم الثالث في ظل انتشار التكنولوجيا الحديثة وعدم وعي الأفراد بمخاطرها وتأثيرها جعلنا نتجه بالبحث إلى ضرورة التعرف على انعكاسات التهديدات السيبرانية على الأمن القومي الليبي ، فمتغير التهديد يأتي متضاد مع تحقيق الأمن وغياب أحدهما يؤدي إلى تحقيق الآخر ، ونظراً لما تشهده ليبيا من أحداث متتالية تأتي أهداف البحث للتعرف على مفهوم الأمن السبراني وتأثيراته المختلفة على البيئة الداخلية الليبية خاصة بعد انتشار الإعلام الموازي والشبكات المختلفة التي أصبحت منبر لمن لا منبر له وما يشكله تأثيرها على أمن المجتمع ، وفيما ما يلى توضيح هذه الأهداف:

أ-إثارة انتباه واهتمام الباحثين لهذا الموضوع للخوض فيه وتحديد مخاطرة وآليات ليبيا لمكافحته.

ب-تقديم رؤية علمية حول التهديدات السيبرانية وانعكاساتها على الأمن القومي الليبي وآليات المواجهة والجهود الليبية وسبل الحماية منها مع القيام بتحليلها تحليلياً موضوعياً.

4-فرضية البحث:

للإجابة عن التساؤلات التي يتم طرحها يقترح الباحث الفرضيات التالية:

أ- الفرضية المركزية: كلما زادت مخاطر التهديدات السيبرانية على الأمن الوطني الليبي كلما أدى ذلك إلى ضعف المنظومة الأمنية الليبية مما يستوجب إعادة ضبط استراتيجية المواجهة.

ب-الفرضيات الفرعية:

1- تعتبر الاختراقات السيبرانية في ليبيا بمثابة تهديد للأمن القومي الليبي بالنظر لإمكانية المساس بالبنية التحتية الإلكترونية للدولة ومنظومتها الاستراتيجية.

2-إن التعاون والتنسيق بين الدول في الفضاء السيبراني يؤدي حتماً إلى التقليل من التهديدات للأمن القومي.

3-ان الجرائم التي يفعلها الأمن السيبرانى في تدمير السياسة الأمنية في ليبيا سوف تؤدى بالضرورة إلى الإضرار بالوضع العام في ليبيا وعدم استقراره.

5-اشكالية البحث:

تزايدت مخاطر التهديدات السيبرانية في العصر الرقمي وتباينت أثارها وانعكاساتها على العالم عامة وليبيا خاصة حيث مست هذه التهديدات ليبيا لتطال عبرها مختلف القطاعات الاقتصادية، والعسكرية ، والسياسية ، كما أصبحت تهدد أمنها الوطني بشكل دائم ومستمر بالرغم من الدور الذي تلعبه نظم الحماية في الحد منها ، ومما تقدم يمكن طرح تساؤل رئيسي:

ماهي انعكاسات التهديدات السيبرانية على الأمن الوطني الليبي؟

ويتفرع عن هذا التساؤل تساؤلات فرعية:

أ- ما مفهوم الأمن السيبرانى؟ وما أهدافه وخصائصه ومرتكزاته؟ أي ماهي أبرز المضامين لدراسة الأمن والتهديدات السيبرانية؟

ب- ماهي علاقة الأمن السيبراني بالأمن القومي؟

ج- ما ابرز التهديدات السيبرانية للأمن القومي الليبي؟ وما آليات المواجهة والجهود الليبية وسبل الحماية من التهديدات السيبرانية؟

6-مناهج واقترابات البحث:

من أجل معالجة الموضوع نستخدم في هذا البحث منهجين:

أ-مناهج البحث:

1- المنهج الوصفي التحليلي: يتم من خلاله تحديد خصائص وأبعاد الظاهرة المدروسة ووصفها وصفاً موضوعياً من خلال جمع الحقائق والبيانات و تحليل المعطيات التي يتم وصفها ويتم استخدامها في هذا البحث من خلال تفصيل و تفسير ظاهرة التهديدات السيبرانية و الأمن السيبرانى وتحديد اهميته ومرتكزاته و طبيعة العلاقة بين الأمن السيبراني والأمن القومي وذلك من خلال جمع البيانات الوصفية

حول التهديدات السيبرانية والأمن السيبراني ومن ثم تحليل المعلومات المتحصل عليها بما يخدم البحث أي تحليل التهديدات السيبرانية وانعكاساتها على الأمن القومي الليبي.

2-منهج دراسة الحالة: يقوم منهج دراسة الحالة بدراسة الظاهرة بشكل معمق وذلك بجمع بيانات ومعلومات شاملة ومفصلة عنها بهدف الوصول إلى فهم أعمق للظاهرة المدروسة وكشف الحقائق والمعلومات التفصيلية الدقيقة عنها ، يتم استخدامه في هذا البحث من خلال الاعتماد على ليبيا كحالة تستحق البحث لإسقاط انعكاسات التهديدات السيبرانية على الأمن القومي الليبي.

ب-إقترابات البحث: يمكن تناول موضوع البحث وفقاً للمقترب التالي:

1- الاقتراب الوظيفي يبرز هذا المقترب الوظيفة الوقائية التي تتبناها الدولة الليبية في مواجهة التهديدات السيبرانية والحد من تأثيرها على الأمن القومي الليبي.

المحور الأول: مقاربة مفاهيمية للأمن السيبراني (المفهوم والأهداف والمرتكزات)

أولاً: مفهوم الأمن السيبرانى:

تناول العديد من الباحثين مفهوم الأمن السبراني نوضحه فيما يلي:

1-معنى كلمة سيبرانى: تطلق كلمة "سيبراني" على كل ما يتعلق بالشبكات الإلكترونية الحاسوبية وشبكة الإنترنت ، والفضاء السيبراني يعني الفضاء الإلكتروني(Cyberspace) وهو كل ما يتعلق بشبكات الحاسوب ، والإنترنت ، والتطبيقات المختلفة كالوتسآب ، والفيس بوك وغيرها وكل الخدمات التي تقوم بتنفيذها كتحويل الأموال والشراء عبر الأنترنت وغيرها من الخدمات على مستوى العالم [1].

2-الأمن السيبرانى:

أ- الأمن السيبرانى لغوياً: مكون من لفظين " الأمن" و"السيبراني"، والأمن:هو نقيض الخوف أي بمعنى السلامة ، وهو مصدر الفعل أَمِن أَمناً وأَماناً وأَمنةً أي اطمئنان النفس وسكون القلب وزوال الخوف ، ويقال :أَمِن من الشر أي سلم منه قل تعالى في كتابه العزيز " وَا ذْ قَالَ إبراهيم رَب اجْعلْ هَذَا بَلَداً آمِناً وَارْزقْ أَهْلَه مِنَ الثَّمَرَاتِ " ، اما السيبراني كلمة السسبرانية مأخوذة من كلمة (سيبر) وتعني صفة أي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي ، كذلك هي كلمة يونانية الأصل مشتقة من الكلمة Cybernetics والتي تعنى الشخص الذي يدير دفة السفينة تستخدم مجازاً

(1) د. منى عبدالله السمحان، متطلبات تحقيق الأمن السيبرانى لأنظمة المعلومات الإدارية بجامعة الملك سعود مجلة كلية التربية، جامعة المنصورة، كلية التربية، العدد 111، يوليو 2020، ص9.

للمتحكم ومعناها أمن الفضاء المعلوماتي[1] والسيبراني من أكثر المصطلحات تردداً في معجم الأمن الدولي يعرفه المعجم الفرنسي Le Petit Larousse بأنه" العلم الذي يدرس آليات الاتصال والتحكم في الآلات والكائنات الحية " أما معجمOxford الإنجليزي فيعرفه على أنه "دراسة فاعلية العمل البشري بمقارنتها بفاعلية الآلات الحاسبة تتصل بالحواسيب وتكنولوجيا المعلومات والواقع الافتراضي" في حين يعرفه قاموس مصطلحات الأمن المعلوماتي بأنه" هجوم الفضاء الإلكتروني للسيطرة على المواقع إلكترونية وتعطيلها أو تدميرها [2].

ب- الأمن السيبراني اصطلاحاً: تعددت التعاريف التي تناولت مصطلح السيبرانية والتي اشتركت في مضمون واحد وهو" استهداف المواقع إلكترونية من خلال الوسائل الإلكترونية "وهنا عرف " ريتشارد كمرر " Richard A Kemmerr الأمن السيبراني بانه " عبارة عن وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القراصنة" [3] ايضاً إدوارد أمو رسو Amoroso Edward) عرفه بأنه " وسائل من شأنها الحد من خطر الهجمات الضارة على البرمجيات أو أجهزة الحاسوب أو الشبكات من خلال استخدام أدوات كشف الاختراقات ووقف أنشطة الفيروسات ومنع الدخول غير المسموح به وتأكيد الهويات وتمكين الإتصالات المشفرة [4] كذلك عرفه NIST على أنه" حماية الأصول المعلوماتية من خلال معالجة التهديدات التي تتعرض لها المعلومات التي تتم معالجتها "[5] ايضاً (LEWIS J. A) قام بتوسيع الأمن السيبراني لكي يعبر عن القدرة عن حماية بيانات الدولة وشبكاتها من الاختراق ، كذلك عرف الكاتبان Neittaanmäki Pekka ، Lehto Martti الأمن السيبراني بأنه "مجموعة من الإجراءات المتخذة في مجال الدفاع ضد الهجمات السيبرانية ونتائجها التي تشمل تنفيذ التدابير المضادة المطلوبة" [6] ايضاً الاتحاد الدولي للاتصالات عرف الأمن السيبراني على أنه (مجموعة الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام والاستغلال غير المشروع

(1) المرجع السابق، ص9.

(2).Dictionnaire français Le petit Larousse, (France, Edition, 2001), p104

(3) Dan Craiyen and others, "Defining cybrescurity", Technology innovation management review, Montreal, Canada, (october 2014).p14.

(4) ايهاب خليفة، الأمن السيبراني: الماهية والإشكاليات، رؤى مصرية، اكتوبر، 2019، ص5.

(5)د. راشد محمد المري، الأمن السيبراني وحماية الأنظمة الإلكترونية، دراسة تحليلية تأصيلية، مجلة الدراسات القانونية والاقتصادية، القاهرة، اكاديمية سعد العبدالله للعلوم الأمنية،، المجلد 9، العدد 1، مارس 2023، ص965.

(6) نهى على أمير، الأمن السيبراني في استراتيجية الأمن القومي الروسي، مجلة آفاق اسيوية، مصر، الهيئة العامة للاستعلامات، المجلد7، العدد 11،مارس 2023، ص173.

واستعادة المعلومات الإلكترونية ونظم الاتصالات وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات ، وتعزيز حماية وسرية وخصوصية البيانات الشخصية للمواطنين ، واتخاذ التدابير لحماية المواطنين من الهجمات السيبرانية [1] كذلك يعرف الأمن السيبراني بأنه " مجموعة السياسات والحمايات الأمنية ومناهج إدارة المخاطر الأمنية والتكنولوجيات التي يمكن استعمالها لحماية البيئة السيبرانية والمؤسسات والمستخدمين "، هذا كما قدمت وزارة الدفاع الأمريكية تعريفاً للأمن السيبراني بأنه "الإجراءات اللازمة لحماية المعلومات والاتصالات من الجرائم والهجمات والتخريب والتجسس" ، ايضاً المعهد الوطني للمعايير والتقنية في الولايات المتحدة عرف الأمن السيبراني بأنه " العمليات والآليات التي يتم من خلالها حماية معدات الحاسب الألى والمعلومات والاتصالات والخدمات والدفاع عنها ضد الضرر أو الإستخدام أو التعديل من أي تدخل غير مصرح به " [2] في حين اعتبر الإعلان الأوروبي الأمن السيبراني بأنه " قدرة النظام المعلوماتي على مقاومة محاولات الإختراق التي تستهدف البيانات " ، كذلك الوكالة الفرنسية لأمن أنظمة الإعلام ANSSI عرفته بأنه" فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية ويشمل شبكة الإنترنت و الشبكات العالمية والخاصة [3] ايضاً يراه البعض الآخر بانه" فن ضمان وجود واستمرارية مجتمع المعلومات وضمان حماية المعلومات والبنية التحتية في الفضاء الإلكتروني"[4]

مما سبق نعرف الأمن السيبراني بانه " المجال الجديد للحروب الحديثة بعد البر والبحر والجو والفضاء يمثل جميع شبكات الحاسب الآلي الموجودة حول العالم؛ ويشمل الأجهزة الإلكترونية المرتبطة من خلال شبكة الألياف البصرية واللاسلكية والفضاء السيبراني.

ثانياً: أهداف الأمن السيبرانى:

يهدف الأمن السيبرانى الى ما يلي:

(1)صالح مهدى هادى الشمري، زيد محمد على اسماعيل، الأمن السيبرانى كمرتكز جديد في الاستراتيجية العراقية، مجلة قضايا سياسية، جامعة النهرين، كلية العلوم السياسية، المجلد 12، العدد 62، 2020، ص277

(2) مصطفى ابراهيم سلمان الشمري، الأمن السيبرانى واثره في الأمن الوطني العراقي، مجلة العلوم القانونية والسياسية،جامعة ديالى، كلية القانون والعلوم السياسية،المجلد العاشر، العدد الأول،2021،ص ص155 . 156

(3) د. راشد محمد المري، مرجع سبق ذكره، ص965.

(4) صالح بن على بن عبد الرحمن الربيعة، الأمن الرقمي وحماية المستخدم من مخاطر الأنترنت متاح على الرابط: 4 . https://www.google.com/url?sa=2019

1-حماية أنظمة التقنيات وما تحويه من بيانات بكل خصوصية وسرية من الإختراقات من خلال إتباع التدابير اللازمة لحماية المواطنين من المخاطر.

2-التصدي لهجمات امن المعلومات التي تستهدف الأجهزة الحكومية والحد من التجسس والتخريب الإلكتروني في أنظمة الحاسب الآلي ومقاومة البرمجيات الخبيثة لما تستهدفه من أضرار للمستخدمين مع توفير بيئة أمنة موثوقة للتعامل في مجتمع المعلومات.

3-تدريب الأفراد على آليات لمواجهة التحديات الخاصة باختراق أجهزتهم التقنية

4-استكشاف نقاط الضعف في الأنظمة وتقديم الحلول لتعزيز الأمن الرقمي للهيئات الحكومية [1].

ثالثاً: خصائص الأمن السيبرانى:

يتميز الأمن السيبرانى بخصائص أهمها ما يلي:

1-الاكتشاف والتعقب: أي اكتشاف الجرائم الإلكترونية وتعقب أثرها للتغلب عليها.

2-السرعة وغياب الدليل :إن استخدام وسائل تقنية حديثة من قبل المخترقين جعل من الصعب إثبات هذه الجرائم لذلك أتى الأمن السيبراني بتقنيات عالية الحداثة تفوق خبرة المخترقين.

3-(السرية): أي أن الأفراد المصرح لهم فقط يمكنهم تلقي أو تغيير أو إدارة المعلومات.

4-السلامة: الحفاظ على سلامة البيانات والمعلومات وحمايتها من الهجمات التخريبية أو السرقة [2].

رابعاً: عناصر ومرتكزات الأمن السيبرانى:

1- القوة السيبرانية (Cyber Power):يعد استاذ العلاقات الدولية(Nye. S Joseph) من اهم مفكري القوة السيبرانية والتي تعرف " بانها القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء الإلكتروني "، أدت الى دخول مجال جديد للتفاعلات الدولية وبروز تهديدات والتأثير على استراتيجيات الأمن القومي للدولة، تركز على وجود نظام متماسك فيه تناغم بين القدرات التكنولوجية، والاقتصادية، والعسكرية، والإدارية، وغيره من العوامل التي تساهم في دعم امكانيات الدولة من خلال السيطرة على الفضاء الإلكتروني فضلا" عن ان تكلفة الحصول على القوة اصبحت مرهونة بالتطور التكنولوجي الذى مكن من ادراج فواعل جديدة ، ومما زاد من حالة الانكشاف الأمني للدولة الاعتماد على البرامج الحكومية الإلكترونية التي

(1) د. منى عبدالله السمحان، مرجع سبق ذكره، ص12.

(2) نشوة اسماعيل زقوت واخرون، مدى وعى أعضاء هيئة التدريس بالجامعات الليبية بأهمية الأمن السيبرانى ، المؤتمر العلمي الأول لتقنية المعلومات، الزاوية، جامعة الزاوية، كلية تقنية المعلومات، 21 .22، 2022، ص ص5 . 6.

اصبحت عرضة للاختراق والهجوم وهو ما جعل المعضلة الأمنية تبرز من جديد لتكون امام معضلة امنية سيبرانية[1].

2-الفضاء السيبرانى (Cyber Space: هو بيئة تفاعلية حديثة مكونة من مجموعة من الأجهزة الرقمية وانظمة شبكات الاتصالات والبرمجيات والحاسب والأنترنت ، يتوقف فيه مفهوم الامن السيبرانى على مواجهة المخاطر الكامنة في هذا الفضاء السيبرانى والذى يعد نقطة الانطلاق لصياغة الاستراتيجية السيبرانية كما يستخدم كوسيلة للصراع داخل الدولة في دعم طرفي النزاع بغير قتال مما يسهل عملية الاختراق الخارجي من خلال شبكات الاتصال [2].

3- الدفاع السبرانى: (Cyber Defense): يقصد به الدفاع الإلكتروني لمجموعة القدرات النظامية للقوات المسلحة للحماية من الهجمات السيبرانية" عرفته العقيدة الفرنسية بانه" مجموعة الوسائل الفنية وغير الفنية التي تسمح للدولة بالدفاع في الفضاء الإلكتروني عن نظم المعلومات السرية والمهمة" بينما ترى الإستراتيجية النمساوية انه " يشير الى التدابير اللازمة للدفاع عن الفضاء الإلكتروني بالوسائل المناسبة" ، ايضاً البرلمان الأوروبي يرى انه" عملية تطبيق الإجراءات الأمنية من أجل الحماية من الهجمات السيبرانية" ، هذا ويمكن أن تنتقل المعلومات السيبرانية عبر الفضاء الإلكتروني لجذب مواطنين في دولة أخرى أو إلحاق الضرر بالأهداف المادية في دولة أخرى.

4-الردع السيبرانى: نتيجة لطبيعة الفضاء الإلكتروني فانه من الصعوبة منع الهجمات السيبرانية نتيجة للهجمات الحديثة أو الفيروسات والأسلحة السيبرانية المتطورة فضلا" عن صعوبة تعقب مصدر الهجمة، ولذا فان تحقيق الردع التقليدي قد لا يثبت نجاحاً فعلياً الأمر الذى يدفع الى البحث عن تعريف غير تقليدي للردع يتحقق من خلال خطط واستراتيجيات للتعامل مع الهجمات السيبرانية تشمل التخفيف من حدتها وعدم التأثير على البنية التحتية والخدمات التي تشكل ركيزة للأمن القومي[3].

5-الهجوم السيبرانى: هو من الأفعال التي تقوض القدرات والوظائف لشبكات الحاسوب من أجل هدف قومي أو سياسي تمكن المهاجم من خرق الأنظمة والعبث بها ، له القدرة على إغلاق انظمة

(1) ماجد صدام سالم، الأمن السيبرانى العراقي واثره في قوة الدولة، مجلة العلوم التربوية والإنسانية، العراق، جامعة ميسان، كلية التربية الاساسية، قسم الجغرافيا، العدد 18، ديسمبر 2022 ، ص71.

(2) المرجع السابق، ص ص71 . 72.

(3) نهى على امير، مرجع سبق ذكره، ص174.

الدفاع الجوية والشبكات الكهربائية التي تهدد الأمن القومي ، كما انه هجوم يشنه المهاجمون بمساعدة أجهزة الكمبيوتر أو الشبكات المخترقة يمكن أن يؤثر على النظام ويسرق البيانات[1].

المحور الثاني: العلاقة بين الأمن السيبراني والأمن القومي:

أولاً- مفهوم الأمن القومي: إن الأمن القومي ضروري للدولة يساوي كيان الدولة وأساس بقائها يتسم بالعمومية لتأثره بحقائق متنوعة نابعة من العوامل الداخلية والخارجية ، تعددت مفاهيمه هناك من يرى إن الأمن القومي " ما تقوم به الدولة للحفاظ على سلامتها ضد الأخطار الخارجية والداخلية التي تؤدي بها إلى الوقوع تحت سيطرة أجنبية نتيجة ضغوط خارجية او انهيار داخلي " ، ايضاً عرفه الكاتب السياسي الأمريكي(والتَّر ليبمان) بأنه قيمة قد تزيد أو تنقص وذلك حسب قدرة الأمة على ردع أي هجوم أو هزيمته " ، كذلك عرف(فرانك تراغر) و(فرانك سيموني) الأمن القومي بأنه " ذلك الجزء من السياسة الحكومية الذي يهدف إلى خلق الظروف القومية والدولية اللازمة لحماية وتوسيع القيم الوطنية الحيوية ضد الخصوم الحاليين أو المحتملين"[2].

ثانياً- العلاقة بين الأمن السيبراني والأمن القومي: في عصر الثورة التقنية والمعلوماتية وجب الوقوف على حدود التفاعل الرقمي بين أمن المعلومات الإلكترونية والأمن القومي للدول ، فمع انصهار الحدود الجغرافية وتقلص المسافات بين الدول بفعل الثورة الإلكترونية أحدثت هذه التغييرات العديد من التأثيرات على الأمن القومي نتيجة البيئة التكنولوجية التي أتاحت للدول إمكانية الولوج في فضاء إلكتروني يحوي العديد من عناصرها القومية والأمنية والإقتصادية والسياسية والإجتماعية ' ومن هنا أصبحت العلاقة بين الأمن القومي والتكنولوجيا علاقة متزايدة اذ إن ارتباط الأمن السيبراني بالتحول الرقمي يعتمد على أُطر وآليات حكومية و تشريعية متقدمة داعمة للرقمية والبنية التحتية المتقدمة كما أن الأمن السيبراني والإلكتروني جزء لا يتجزأ من الأمن القومي خاصة مع تنامي حجم التهديدات وعلاقة البعد الإلكتروني بعمل المنشآت الحيوية سواء كانت مدنية أو عسكرية[3] إضافة الى ان الأمن القومي لأي دولة له محاوره الرئيسية والمتمثلة في المحاور العسكرية ، السياسية ، الجغرافية ، الإجتماعية ، الإقتصادية والأمنية وأخيراً التقنية وهو المحور الذي يهم الدول اليوم نظراً لإستنادها على منظومة تقنية

(1) ماجد صدام سالم، مرجع سبق ذكره ، ص72.

(2) مصطفى ابراهيم سلمان الشمري،مرجع سبق ذكره، ص ص 161 . 162.

(3) د.عادل عبد الصادق،" الحروب السيبرانية :تصاعد القدرات والتحديات للأمن العالمي، تقرير استراتيجي، المركز العربي لأبحاث الفضاء الإلكتروني، 12مارس، 2017 ، ص 2.

وإلكترونية عالية الدقة وغزيرة التكنولوجيا تعتمد على صناعة المعلومات والبحث العلمي والمعلوماتي في جميع الجوانب ، وبهذا يمكن الإشارة إلى أن الأمن القومي المعلوماتي هو عبارة عن" مدى جاهزية الدول لحماية مخزونها الإلكتروني من المعلومات وعدم الوصول إليها بأية طريقة تقنية أو تقليدية"[1].

لقد شكل هذا التعاون المعلوماتي القومي بين دول العالم هاجس الخوف من الطرف الآخر ومدى امتلاكه للأسلحة التكنولوجية والمعلوماتية المدمرة والتي لم تعد حكرا على القطاعات العسكرية للدول فحسب بل أصبحت سلاحاً تتقن استخدامه غالبية مستخدمي الحواسيب ووسائل الاتصال الحديثة وفي صورة زادت من تفاعل المعلومات الإلكترونية والأمن القومي بحيث رفعت من وتيرة الخوف الذي تعاني منه شعوب العالم المعاصر [2] وبهذا أدخلت ثورة المعلومات دول العالم في هاجس أمني قوي فقد قامت بوضع مدخرتها القومية على شكل معلومات رقمية عبر فضاء مذاب الخصوصية وضعيف الأمن لبعض دول العالم مما زاد من الفجوة المعلوماتية القومية بين الدول[3] ايضاً العلاقة بين الأمن السيبراني والأمن القومي تزداد كلما نقل المحتوى المعلوماتي والعسكري والأمني والفكري والسياسي والاجتماعي والاقتصادي وغيرهما الى الفضاء السيبراني خاصة مع سرعة تبنى الحكومات الإلكترونات الذكية في العديد من دول العالم واتساع نطاق مستخدمي الانترنت أي إن اهتمام الدول بالأمن السيبراني لم يقتصر على البعد التقني وحسب بل تجاوزه الى الأبعاد الثقافية والاجتماعية والاقتصادية والعسكرية وهو ما عمل على دعم حقيقة ان الاستخدام غير السلمى للفضاء الإلكتروني يؤثر على الرخاء الاقتصادي والإستقرار الإجتماعي لجميع الدول التي اصبحت تعتمد على البنية التحتية الكونية للمعلومات ، إضافة إلى أن تصاعد دور الفاعلين من غير الدول في العلاقات الدولية قد اثر بدوره على سيادة الدول وبخاصة مع بروز دور الشركات التكنولوجية العابرة للحدود الدولية وبروز اخطار القرصنة والجرائم السيبرانية والجماعات الارهابية ، ايضاً قواعد البيانات القومية اصبحت في حال انكشاف خارجي إضافة إلى حملات الدعاية والمعلومات المضللة ونشر الشائعات أو الدعوة لأعمال تحريضية أو دعم المعارضة أو الأقليات الأمر الذى يسهم في تلاشى سيادة الدولة ويشكك

(1) وليد غسان سعيد جلمود،" دور الحرب الإلكترونية في الصراع العربي الإسرائيلي"، أطروحة ماجستير في التخطيط والتنمية السياسية، فلسطين، جامعة نابلس، كلية الدراسات العليا،،2013 ، ص53 .

(2) المرجع السابق، ص 54.

(3) بكوش الروميساء، انعكاس التهديدات السيبرانية على الأمن الوطني الجزائري ، مذكرة مقدمة لنيل شهادة الماستر في العلوم السياسية، تبسة، جامعة العربي التبسي، كلية الحقوق والعلوم السياسية، 2018 . 2019، ص9.

في قدرتها على الحفاظ على امنها القومي [1] كذلك نرى إن المصالح الاستراتيجية ذات الطبيعة الإلكترونية تعرضت إلى أخطار إلكترونية تهدد بتحول الفضاء الإلكتروني إلى وسيط ومصدر لأدوات الصراع وتغذية للتوترات الدولية[2] وهنا تزداد الخطورة كلما زاد اعتماد الدولة على تقنية المعلومات وارتباطها بالفضاء السيبراني ذلك إن الهجمات السيبرانية يمكن لها أن تقوض الأمن الوطني فأية فجوة تقنية ستؤدي إلى خسائر كبيرة للدولة في مؤسساتها الرسمية ولمواطنيها بل انه يعرض هيبة الدولة وسمعتها الدولية إلى الخطر ، إذ لا تقف هذه الخسائر عند الجانب المادي فحسب بل ستؤثر مباشرة ايضاً على الجانب المعنوي و تلحق ضررًا في نفسية المواطنين وقادتهم كونه يولد قناعة عامة بضعف قدرة الدولة على حماية المواطنين ومؤسساتها والدليل على ذلك إن وسائل التواصل الاجتماعي من فيسبوك وتويتر والفايبر والتيليجرام والواتساب والسكايب واليوتيوب وغيرها اختصرت الوقت والمسافة وأخذت تحظى بتأثير فعال ومتنامي لدى معظم شعوب العالم ، ويبرز في هذا الخصوص الحراك الشعبي والاحتجاجات الجماهيرية التي اخذت تنتظم على شكل مظاهرات وشكلت مصدر قلق للأنظمة الحاكمة إذ ان لها دور في توجيه الرأي العام وتعبئة الشارع ، وخير مثال على ذلك ما تعرضت له الدول العربية منذ العام 2011التي تأثرت بالربيع العربي[3].

وبذلك نرى ان هذه التطورات فرضت علينا إعادة التفكير في مفهوم الأمن القومي الذي يعنى بحماية قيم المجتمع وإبعاد مصادر التهديد عنها وغياب الخوف من خطر تعرض تلك القيم للهجوم الأمر الذي يوفر أمن الفضاء الإلكتروني حال تحقيق إجراءات الحماية ضد التعرض للأعمال العدائية وللاستخدام السيئ لتكنولوجيا الاتصال والمعلومات "[4] ومن هنا نستنتج أن الأمن السيبراني والأمن القومي يتشابكان من ناحية الهدف حيث يسعى كل منهما إلى حماية البنى التحتية والحدود من كل الاختراقات التكنولوجية والتخوف من زعزعة أمن الدولة. وعليه أصبح الأمن السيبراني وثيق الصلة بالأمن القومي وقضية أمنية وطنية.

(1) ماجد صدام سالم، مرجع سبق ذكره، ص80.

(2) د.عادل عبد الصادق،" المجلس الأعلى للأمن السيبراني خطوة في دعم استراتيجية الأمن القومي"، الرابط:
www.aceronline.com/article-detal.Aspxd=20284 /.2019/03

(3) مصطفى ابراهيم سلمان الشمري، مرجع سبق ذكره، ص ص 161 . 162.

(4) علي عباس مراد،" الأمن والأمن القومي، مقاربات نظرية " الجزائر، ابن النديم للنشر، 2017 ، ص12 .

المحور الثالث: الأمن القومي الليبي في ظل تحديات وتهديدات الأمن السيبراني:

أولاً: التهديدات السيبرانية: هي "أي فعل ضار يحاول الوصول إلى شبكات الحاسوب بدون ترخيص أو إذن من أصحابها" ، تنطوي على التأثير سلباً على العمليات التنظيمية أو الأفراد من خلال نظام معلومات عن طريق الدخول غير المصرح به أو التدمير"[1] واهم التهديدات السيبرانية ما يلي:

1- الإرهاب السيبراني: هو الهجوم غير المشروع أو التهديد بالهجوم المنظم من الجماعات الإرهابية باستخدام الوسائل الإلكترونية على البنى التحتية وانظمة المعلومات والشبكات واجهزة الكمبيوتر ذو دوافع سياسية أو دينية أو عقائدية ، يهدف الى التخريب وتدمير البنية التحتية يتجلى في العديد من الطرق كإختراق أنظمة الكمبيوتر ونشر الفيروسات أو تعطيل نظام إلكتروني [2] استطاعت من خلاله الجماعاتُ الإرهابية التواصل مع بعضها بعضاً لجمع المعلومات الاستخباراتية حول أهدافها ، من انواعه هجوم الفدية وهو نوع من البرمجيات الضارة إذا اصابت جهاز كمبيوتر أو شبكة يحجب الفيروس الوصول إلى النظام أو يقوم بتشفير البيانات لذلك يطلب المجرمون الإلكترونيون مبلغ فدية من ضحاياهم مقابل فك التشفير وهنا تشير التقارير الدولية إلى أن فيروس الفدية تسبب في خسائر مالية تفوق المليارات خلال العام الواحد ، ايضاً من انواعه التنظيم الإرهابي "داعش" والذى له خلايا كل خلية لها آلاف المواقع الإلكترونية وآلاف الصفحات على موقع التواصل الاجتماعي [3] .

2-الحروب السيبرانية: هي هجمات معتمدة على أسلحة إلكترونية تناسب طبيعة المهام التي تقوم لأجلها" ، تستخدم لحملات التخريب وتعطيل الإنترنت وصولاً إلى الحرب الفعلية باستخدام الوسائل الإلكترونية تم اعتمادها كالحروب التقليدية تستهدف المقدرات والأنظمة العسكرية والبنية التحتية للمجتمع بما في ذلك شبكات المراقبة والذكية تتمخض عن عواقب تهدد الحياة [4].

3-قرصنة البرمجيات (السرقة الالكترونية): هي العملية التي يقوم بها شخص أو عدة أشخاص متمكنين في برامج الحاسوب يستطيعون اختراق حاسوب معين والتعرف على محتوياته ومن خلالها يتم إختراق الأجهزة المرتبطة معها، تشمل سرقة البرمجيات النسخ الإلكتروني غير القانوني للبرامج الأصلية للشركات

(1) بكوش الروميساء، مرجع سبق ذكره ، ص 26.

(2) المرجع السابق، ص16.

(3) الهيئة العامة للاستعلامات، مصر والأمن السيبراني، مصر، 11 يونيو 2023
https://www.sis.gov.eg/Story/258293/%D9%85%D8%B5%D8%B1-%D9%88%D8%A7%D9%84%D8%A3%D9%85%D9%86-% D9%89?lang=ar

(4) المرجع السابق.

والمؤسسات أو تنزيل غير القانوني من الإنترنت دون إذن مسبق منها، يستخدم فيها المجرم الرسائل الإلكترونية أو الدخول لغرف الدردشة الموجود بها الشخص ويقوم بمضايقته[1].

4- التجسس السيبراني: يتم باستخدام وسائل التكنولوجيا والهجمات السيبرانية المتطورة يحصل فيه على معلومات سرية بطرق غير مشروعة يوقع خسائر كبيرة بالطرف الاخر عسكرية أو اقتصادية من خلال اختراق البيئة المعلوماتية والإتصالاتية وذلك بالتلاعب بالبيانات وسرقة المعلومات او مسحها من أجهزة الحاسب الإلكتروني أو سرقة النطاق الترددي بغية الوصول غير المصرح للإنترنت[2] تشمل انتهاك الخصوصية والانتحال والاحتيال للاستيلاء على الأموال من خلال البريد الإلكتروني والسطو على أرقام البطاقات الائتمانية والاختلاس وتزوير الوثائق والمستندات المالية والابتزاز وتشويه السمعة في المواقع الإلكترونية ونشر رسائل الكراهية[3].

5-نشر الفيروسات التقنية في البيئات المعلوماتية: هي برامج إلكترونية مدمرة يقوم الأفراد بنشرها تتسبب في تلف البيانات الموجودة في جهاز الضحية والتحكم بجهازه وانتحال شخصيته[4].

6-الأقمار الصناعية :هدفها السيطرة على أكبر قدر ممكن من المعلومات وذلك عبر التقاط ملايين الصور للهدف وإرسالها للقاعدة المعلوماتية الموجودة على الأرض.

7-أسلحة النانو التكنولوجية: تسلط هذه التكنولوجيات على الأجزاء المادية للأجهزة الحاسوبية وتتسلل إلى أنظمة التشغيل وتفرغ ما بحوزتها من أنظمة تدميرية لهدم البناء المعلوماتي.

8-الطائرات الإلكترونية دون طيار: دخلت هذه الطائرات الحرب الإلكترونية كما انها تحوي العديد من التأثيرات السلبية على جسم الإنسان ناتجة عن الموجات التي تطلقها والأصوات الصادرة عنها.

9-الخداع الإلكتروني: يشتمل هذا السلاح الرقمي على عدة وسائل: أهمها التقليد الصوتي، التشويش الإلكتروني، الخداع ونشر الشائعات، انتحال الشخصيات افتراضياً، الابتزاز الإلكتروني [5].

ثانياً: انعكاسات التهديدات السيبرانية على الأمن القومي الليبي:

---

(1) يوسف إسماعيل يوسف مانيطه، نظرة عامة عن الجريمة الإلكترونية في الفضاء السيبراني المجلة الليبية العالمية، جامعة بنغازى، المرج، كلية التربية ، العدد32، 30 نوفمبر 2017، ص ص 4 .5.

(2) ماجد صدام سالم، مرجع سبق ذكره، ص ص 78 . 79.

(3) د .عبدالسلام محمد المايل، الجريمة الإلكترونية في الفضاء الإلكتروني المفهوم – الأسباب، سبلُ المكافحة مع التعرض لحالة ليبيا، مجلة آفاق للبحوث والدراسات السياسية، المركز الجامعي، العدد 4، يوليو 2019 ص250.

(4) يوسف إسماعيل يوسف مانيطه، مرجع سبق ذكره، ص 4.

(5) بكوش الروميساء، مرجع سبق ذكره، ص ص32 . 33.

1-تهديد القيم والأخلاق الاجتماعية: تترك التهديدات السيبرانية غير المشروعة تأثير سلبي على أخلاقيات المجتمع اذ تؤدى الى ارتفاع نسبة الممارسات الإجرامية كالإباحية، والترويج للإتجار بالممنوعات، والدعارة، والإرهاب والتجنيد لقضايا تمس الأمن والسلم الدوليين لتهديد القيم والاخلاق [1] ايضاً برز الابتزاز الإلكتروني خصوصا على النساء بإعتباره أخطر التهديدات سواء كان أخلاقي أو مالي مما أدى الى كثرة عمليات الإنتحار كما لم تغب الإباحية الإلكترونية عن قائمة التهديدات الخاصة بالأطفال [2].

2-تصدير لأزمة عدم الثقة بين الأفراد: إن الهجمات السيبرانية تحدث آثاراً مدمرة على استقرار المجتمع متمثلة في تصدير أزمة عدم الثقة بين الأفراد وتوجيه الرأي العام ضد الدولة نتيجة للمعلومات المغلوطة والأفكار الهدامة التي تهدد استقرار الوطن والأمن القومي اذ انها تصل بسرعة فائقة إلى أكبر شرائح من المواطنين بغض النظر عن صحتها كما تدعو إلى نشر الفوضى والعنف والتطرف وتهديد الأمن القومي [3].

3-الأفكار الهدامة التي تحملها التهديدات السيبرانية والتي تهدد الوطن ووحدته وتزعزع استقراره كالإرهاب السيبراني وذلك من خلال اختراقها لقواعد بيانات الحكومة لاستخدام معلومات حساسة [4] مثال على ذلك تعرض شركة ليبيانا للهاتف المحمول للهجمات السيبرانية في قواعد بياناتها إلا أن هذه المحاولة باءت بالفشل [5].

4-تعطيل واتلاف البنية التحتية والأنظمة الحيوية الإقتصادية والأمنية والعسكرية والسياسية لليبيا كأنظمة الكهرباء والطب والنقل والبنوك والمؤسسات النفطية وغيرها من القطاعات التي تعد ركائز

---

(1) الهيئة العامة للإستعلامات، مصر والأمن السيبراني، مرجع سبق ذكره.

(2) تصريح لأخبار ليبيا 24 " مستشار بالأمن القومي فيصل بوالرايقة"، المجلس مدرك لأهمية مواجهة التهديدات السيبرانية المحدقة بليبيا، أخبار ليبيا 24، 24 يناير 2023 على الرابط

https://akhbarlibya24.net/2023/01/24/%D9%85%D8%B3%D8%AA%D8%B4%D8%A7%%D9%85%D8%AF%D8%B1%D9%83-%D9%84%D8%A3%D9%87%D9%85

(3) على الفيتوري، تتابع أعمال مؤتمر ليبيا الدولي للأمن السيبراني تحت شعار ''الأمن القومي والتهديدات السيبرانية في عالم متغير''، الموقف الليبي، بنغازي، يناير 2023

https://libyanstand.net/2023/01/30/%D8%A7%D9%84%D9%85%D9%88%D9%82%D9-D9%85%D8%A4%D8%AA%D9%85%D8%B1-%D9%84%D9%8A%D8%A8

(4) يوسف إسماعيل يوسف مانيطه، مرجع سبق ذكره، ص6.

(5) مستشار الأمن القومي الليبي إبراهيم بوشناف (أرشيفية)،مجلس الأمن القومي يشكل غرفة طوارئ لمتابعة تداعيات الهجوم السيبراني على إحدى شركات الاتصالات،جريدة بوابة الوسط ، القاهرة، 13 مايو 2023

https://alwasat.ly/news/libya/398554

أساسية للدولة[1] اذ تقوم التهديدات السيبرانية بالإختراق والتجسس على جميع المؤسسات الحيوية في الدولة مما يهدد أمنها ويعطل قوتها الأمر الذى يضر بالأمن القومي الليبي [2].

ثالثاً: آليات المواجهة والجهود الليبية وسبل الحماية من المخاطر والتهديدات السيبرانية:

1-الجهود الليبية والوسائل لمواجهة التهديدات السيبرانية للأمن القومي الليبي:

أهم هذه الجهود الرقابة الأسرية والمجتمعية والحرص على تحديث أنظمة الحماية والإمتناع عن تنزيل أي ملف من مصادر غير معروفة وعدم الإفصاح عن كلمة السر ، ايضاً أعلن مجلس الأمن القومي الليبي عن تشكيل غرفة طوارئ لمتابعة تداعيات الهجوم السيبراني وإنشاء فريق خاص بالأمن السيبراني للتصدي لمثل هذه الهجمات كما حصل ذلك في تشكيل غرفة طوارئ لمتابعة تداعيات الهجوم السيبرانى على إحدى شركات الإتصالات الليبية في 13 مايو 2023 وقال المجلس في بيان له " إن الغرفة تلقت منذ الساعات الأولى صباح السبت 13 مايو 2023 تعليمات من مستشار الأمن القومي المستشار إبراهيم بوشناف بحضور أعضائها وعدد من خبراء الأمن السيبراني لمناقشة تداعيات الهجوم السيبراني حسب التقارير الأمنية الواردة للمجلس وتحققت الغرفة من بعض المعلومات الواردة بشأن الموضوع فيما عملت الجهات المختصة على رفع جدار الحماية للشبكة من خلال استراتيجية وضعتها مختلف الجهات المعنية بالتعاون مع مجلس الأمن القومي وفق البيان وأكدت الغرفة أن التنبؤ بالمخاطر قبل حدوثها وآليات الاستجابة للطوارئ ضمن أولويات مجلس الأمن القومي الذي يعمل على إعداد تقريره السيبراني بشأن تقييم المخاطر والتعافي منها إضافة إلى تحديد أوجه الضعف ومعالجتها وحماية بيانات المواطنين الليبيين" وقالت: نقوم بعمل يومي مستمر لحماية الشبكات ضد الهجمات العنيفة على بلدنا الحبيب إلى ذلك قررت رئاسة هيئة الرقابة الإدارية اتخاذ الإجراءات اللازمة للتّأكد والتّحقق ممّا يُتداول عبر وسائل الإعلام مِن اختراق قواعد البيانات المالية والمحاسبية وغيرها لشركة ليبيانا ونص قرار رئاسة الهيئة على مراجعة نظام الحماية الرقمية الشاملة للشركة واتخاذ كل الإجراءات القانونية حيال ما تسفر عنه نتائج المتابعة وفقا لأحكام قانون إنشاء

(1) تصريح لأخبار ليبيا 24 " مستشار بالأمن القومى فيصل بوالرايقة "، المجلس مدرك لأهمية مواجهة التهديدات السيبرانية المحدقة بليبيا، مرجع سبق ذكره.

(2) د.م، النظام القانوني للأمن الوطني الالكتروني في ظل الثورة الرقمية"، الرابط:
www.univ-chlef.dz/fdsp/pdf/je- 2019/02/ 28

الهيئة رقم (20 لسنة 2013) وتعديله ولائحته التنفيذية [1] ايضاً قامت ليبيا بإنشاء العديد من المراكز التي تعنى بالتأمين السيبراني وتهديداته ومن بينها المعهد الوطني للأدلة الجنائية وعلم الإجرام للأمن الوطني ومختص في الجرائم الإلكترونية ومركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للأمن الوطني والهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بالإضافة إلى المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني ومنظمة رصد الجرائم في ليبيا والجمعية الليبية للإنترنت الآمن في 2021[2] هذا كما اعتمدت الحكومة الليبية الأول من يونيو في كل عام يوما وطنيا لتقنية المعلومات وأنشئت لجنة وطنية للتحول الرقمي إضافة للهيئة الوطنية لأمن وسلامة المعلومات كذلك اهتمت ليبيا بالتحول الرقمي تحت شعار ليبيا دولة رقمية 2023 وإطلاق مشروع سايبر ليبيا [3] كذلك قامت ليبيا بدعم وتأسيس المواقع العلمية والمراكز المهنية والأكاديميات العلمية لتعزيز دور مجلس الأمن القومي الليبي نحو التحول الرقمي إضافة إلى وضع خطة لتأهيل الكوادر الأمنية بالدولة الليبية في مجال إدارة الحالات الطارئة والتعامل مع مخاطر الهجمات السيبرانية ، ايضاً قامت ليبيا بنشر الوعي الأمني حول الأمن السيبراني وخطورته لدى المجتمع الليبي وتطوير العمل الأمني في العصر الرقمي للأجهزة الأمنية الوطنية وعصر سرعة انتقال المعلومة ودعم الاستراتيجيات الوطنية في مجالات الأمن القومي الليبي ضمن خططه المستقبلية ' كذلك اكدت ليبيا على أهمية دور مؤسسات التنشئة الإجتماعية والدينية لحماية الأطفال والمراهقين والمرأة من المخاطر السيبرانية ، ايضاً قامت ليبيا بمكافحة الإرهاب والتهديدات السيبرانية في مجال الأمن القومي و توحيد الجهود لمواجهة تحديات الأمن السيبراني وتوفير الحماية اللازمة للبيانات والمعلوماتية الحساسة ، إضافة إلى تعزيز دور مجلس الأمن القومي الليبي والجهات ذات العلاقة في مجال الأمن السيبراني وتعزيز الجاهزية والإستعداد لمواجهة المخاطر والتهديدات السيبرانية ، هذا كما انتقلت ليبيا إلى المبادرات والتعاون الإقليمي والدولي مع بقية الدول الصديقة لإيجاد حلول لهذه التهديدات السيبرانية مع فتح باب التعاون مع المراكز الدولية والعربية والمحلية ضمن خطة مجلس الأمن القومي الليبي في دعم عملية التطوير ورفع الأداء العلمي والمهني وضرورة إضافة الأمن السيبراني والأمن القومي إلى قائمة الأولويات القومية لاستراتيجية الدولة

(1) مستشار الأمن القومي الليبي إبراهيم بوشناف (أرشيفية)،مجلس الأمن القومي يشكل غرفة طوارئ لمتابعة تداعيات الهجوم السيبراني على إحدى شركات الاتصالات،مرجع سبق ذكره.

(2) على الفيتوري، مرجع سبق ذكره.

(3) جازية شعيتير، السيبرانية على قائمة أولويات الأمن القومي، جريدة بوابة الوسط،،2 فبراير 2023
https://alwasat.ly/news/opinions/387415?author=1

ومواجهة حملات التضليل والتخريب وتداول الأنباء الكاذبة والتحريض على ارتكاب أفعال محظورة قانوناً[1] ايضاً تبنت ليبيا الاستراتيجية الوطنية للأمن السيبراني وايجاد تدابير واجراءات استراتيجية متماسكة لضمان أمن الوجود الليبي وحمايته في الفضاء السيبراني وحماية البنية التحتية الحيوية للمعلومات ، كذلك قامت ليبيا بنشر الوعي السيبراني بين طلاب المدارس والقيام ببعض الورش بتوعية الإخصائيات الاجتماعيات في المدارس عن الاستخدام الآمن للإنترنت وطرح فكرة الحاجة لحماية البيانات الشخصية والمؤسسية في البيئة الرقمية وضرورة تعزيز مشاركة جميع أفراد المجتمع ورفع وعيهم بأي نشاطات إلكترونية مشبوهة وتمكينهم من استخدام منجزات التكنولوجيا الرقمية في بيئة أقل تهديدا مع الاهتمام بالجانب الاقتصادي التنموي حول التنمية الرقمية والاستثمار لدى الشباب وإعادة تأهيلهم سيبرانياً ، ايضاً أكدت ليبيا إن مسؤولية التأمين من الأخطار السيبرانية مسؤولية مشتركة ويوجب مساهمة مختلف أصحاب المصلحة في تنفيذ الخطط السيبرانية التنموية والأمنية وذلك من خلال استهدافهم بالحوار المفتوح والمستمر بشأن قضايا السياسات العامة العالمية المتصلة بالأنترنت[2].

2-التشريعات الليبية لمواجهة التهديدات السيبرانية للأمن القومي الليبي:

قامت ليبيا بسن العديد من التشريعات والقوانين الرادعة للحد من التهديدات السيبرانية ، منها القانون رقم 3 لسنة 2014 الصادر عن مجلس النواب والذى نص على مكافحة الإرهاب والجرائم الإلكترونية وذلك في مادته (2) والمادة (15) والمادة (17) ، ايضاً النص على تجريم الإعتداء على المال المعلوماتي المعنوي من قبل المشرع الليبي لمكافحة الجرائم الإلكترونية سواء بالسرقة أو الإتلاف أو غيرهما[3] كذلك قانون "مكافحة الجرائم الإلكترونية" والذى أقره مجلس النواب الليبي في جلسته المنعقدة في 26 أكتوبر 2021 إذ اعلن المستشار الإعلامي لرئيس مجلس النواب الليبي " إنّ قانون مكافحة الجرائم الإلكترونية يُعنَى بالجرائم الإلكترونية التي تمس الدولة ولكنه لا يتعارض رغم ذلك مع حرية التعبير وتابع أنّ القانون يعنى بأي جرم أو استخدام خاطئ للأدوات الإلكترونية يسبب مشاكل

(1) على الفيتورى، مرجع سبق ذكره

(2) جازية شعيتير، مرجع سبق ذكره.

(3) د .عبدالسلام محمد المايل، مرجع سبق ذكره، ص ص 252. 253.

للدولة أو للشخص وإن من أمثلة تلك الجرائم التزوير أو نشر الإشاعات" [1] ايضاً قانون رقم (5) لسنة 2022 والذى اصدره مجلس النواب الليبي في 27 سبتمبر 2022 بشأن مكافحة الجرائم الإلكترونية اذ نص في مادته الثانية على تحقيق العدالة والأمن المعلوماتي وحماية النظام العام والآداب العامة والاقتصاد الوطني وحفظ الحقوق[2] كذلك نص القانون على تمكين الهيئة الوطنية لأمن وسلامة المعلومات من فرض رقابة شاملة على كافة البيانات والمعلومات المنشورة على شبكة الإنترنت وعلى جميع الأنظمة الإلكترونية والتقنية كما طالب بالعمل على حماية خصوصية المواطنين وحماية بياناتهما ، ايضاً نص القانون في مادته 4 على أن يكون "استخدام شبكة المعلومات الدولية ووسائل التقنية الحديثة مشروعة ما لم يترتب عليه مخالفة للنظام العام أو الآداب العامة" [3] كذلك نصت المادة 5 من القانون على ان المواقع الإلكترونية وأنظمة المعلومات الرقمية ملك لأصحابها لا يجوز الدخول إليها أو إلغاؤها أو حذفها أو إتلافها وتعطيلها أو تعديلها أو نقل أو نسخ بياناتها اما المادة 7 من القانون فقد سمحت بتمكين الهيئة الوطنية لأمن وسلامة المعلومات بحجب كل ما ينشر النعرات أو الأفكار التي من شأنها زعزعة أمن المجتمع واستقراره والمساس بسلمه الاجتماعي ، ايضاً فرضت المادة 8 حجب المواقع أو الصفحات الإلكترونية التي تعرض مواد "مخلة بالآداب العامة" ، كذلك نص القانون على انه يعاقب بالحبس وبغرامة لا تقل عن 1 ،000 ألف دينار ولا تزيد على 3 ،000 ثلاثة آلاف دينار كل من ضايق غيره على شبكة المعلومات الدولية أو بأي وسيلة إلكترونية أخرى بقصد إشباع رغبته الجنسية ، ايضاً نصت المادة 22 من القانون كل من استخدم شبكة المعلومات الدولية أو أي نظام إلكتروني آخر لغرض استغلال القصر أو المعاقين نفسياً أو عقلياً في أعمال إباحية في حين نصت المادة 23 من القانون على ان يعاقب بالسجن مدة لا تقل عن خمس سنوات وبغرامة

(1) قانون مكافحة الجرائم الإلكترونية الليبي الجديد: تشريع القمع، مجلس النواب الليبي يقر مشروع قانون مكافحة الجرائم الالكترونية بعد اقرار مشروع قانون المعاملات الألكترونية، مجلس النواب الليبي، 26 اكتوبر 2021
https://smex.org/ar/%D9%85%D9%83%D8%A7%D9%81%D8%AD%D8%A9-%D8%A7%D9%84%D8%AC%D8%B1%D8%A7%D8%A6%D9%85-D9%8A%D8%A9-%D9%84%D9%8A%D8%A8%D9%8A%D8%A7/

(2) المرصد ، ليبيا: ممارسة الحقوق الدستورية في ظل قانون مكافحة الجرائم الإلكترونية، صحيفة المرصد، 30 /8/ 2023، https://adalaforall.org/%D9%84%D9%8A%D8%A8%D9%8A -%D8%A7- -9- /%D9%81%D9%8A-%D8%B8%D9%84-%D9%82%D8%A7

(3) ورقة تلخيصية: قانون مكافحة الجرائم الالكترونية الجديد يفاقم ظاهرة الافلات من العقاب، تونس , 16 نوفمبر 2022.
https://lcw.ngo/%D9%88%D8%B1%D9%82%D8%A9-%D8%AA%D9%84%D8%AE%D9%8A%D8%B5%D9%8A%D8%A9- -%D8%A7%D9%84%D8%AC%D8%B1%D8%A7%D8%A6%D9%85-%D8%A7

لا تقل عن 10 ،000 عشرة آلاف دينار ولا تزيد على 100 ،000 مائة ألف دينار كل من قام بإتلاف أدلة قضائية معلوماتية أو بإخفائها أو التعديل فيها أو محوها أو العبث بها بأي شكل من الأشكال ، كذلك نضت المادة 37 من القانون على أن يعاقب بالسجن مدة لا تقل عن خمس سنوات وبغرامة لا تقل عن 10 ،000 عشرة آلاف دينار ولا تزيد على 100 ،000 مئة ألف دينار كل من بث إشاعة أو نشر بيانات أو معلومات تهدد الأمن والسلامة العامة في الدولة أو أي دولة أخرى من خلال شبكة المعلومات الدولية أو استعمال أي وسيلة إلكترونية أخرى[1] ايضاً جرمت المادتين 9 و39 من القانون رقم (5) لعام 2022 حيازة وسائل التشفير واستعمالها معرضة بذلك ضحايا التعذيب والمعاملة السيئة والمهينة وجميع أشكال الجرائم الأخرى التي من شأنها الإضرار بالحق في الحياة والحق في الحرية والحق في التمتع بالحماية من خطر المراقبة والتقييد والملاحقة وهنا يقيد نص التشريع استعمال كافة المنصات الإلكترونية ومواقع الإنترنت بفرض معايير غير واقعية على مستخدميها تتمثل في الحصول على تراخيص أو تصاريح من قبل الهيئة الوطنية لأمن وسلامة المعلومات للحصول على وسائل التشفير [2] كذلك نصت المادة 46 على ان يعاقب بالسجن كل من أنشأ موقع أو نشر معلومات على شبكة المعلومات الدولية أو إحدى الوسائل الإلكترونية لجماعة إرهابية تحت مسميات تمويهية لتسهيل الإتصالات بقيادتها ، أو أعضائها ، أو ترويج أفكارها ، أو تمويلها ، أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرة ، أو أية أدوات تستخدم في أعمال محظورة ‘ايضاً نصت المادة 47 على ان يعاقب بالحبس مدة لا تقل عن سنة كل من تصنت لصالح نفسه أو لصالح غيره على الاتصالات التي تجري عبر شبكة المعلومات الدولية وتكون العقوبة السجن إذا كان التصنت بقصد الحصول على أسرار حكومية أمنية أو عسكرية أو مصرفية على انه إذا نشر الأسرار المذكورة بالفقرة السابقة عبر شبكة المعلومات الدولية أو أي وسيلة إلكترونية أخرى أو مكن شخص أو جهة أخرى من الحصول عليها تكون العقوبة السجن المؤبد[3] اضافة الى ذلك استجابت السلطة التشريعية ممثلة في مجلس النواب الليبي للتطور السيبراني وقامت بالتدخل التشريعي لتنظيم وحماية

(1) الجريدة الرسمية، قانون رقم 5 لسنة 2022 بشأن مكافحة الجرائم الإلكترونية، مجلس النواب ،العدد 1،السنة الأولى سبتمبر27، 2022

https://lawsociety.ly/legislation/%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%B1%D9%82%D9%85-5-%D9%84%D8%B3%D9%86%D8%A9-2022-%D8%A7%D9%84%D8%AC%D8%B1%D8%A7%D8%A6%D9%85-%D8%A7

(2) ورقة تلخيصيه: قانون مكافحة الجرائم الالكترونية الجديد يفاقم ظاهرة الافلات من العقاب، مرجع سبق ذكره.

(3)الجريدة الرسمية، قانون رقم 5 لسنة 2022 بشأن مكافحة الجرائم الإلكترونية، مرجع سبق ذكره

المعاملات الإلكترونية بالقانون رقم 6 لسنة 2022 بشأن مكافحة الجرائم الإلكترونية ، ايضاً تبنت ليبيا تشريعات وقوانين للحماية الفكرية عبر الأنترنت وتفعيل قوانين حماية البيانات الشخصية البيانات والخصوصية من التهكير وصنوف التهديدات السيبرانية كافة [1]

النتائج:

تم في هذا البحث التوصل إلى النتائج التالية:

1-إن الأمن السيبرانى الليبي جزء من الأمن القومي لليبيا وأهم عوامل قوتها وفاعليتها وفى تحقيق الأمن السيبراني الليبي استقرار ليبيا وتحقيق امنها القومي وفى ضعفه تهديد امنها القومي.

2-نقص الخبرة لدى العاملين في قطاع أمن المعلومات والقصور التنفيذي للقوانين الليبية وفى الحماية الجنائية للنظم والمعلومات الإلكترونية ومكافحة السلوك الإجرامي الإلكتروني مما يؤثر على الأمن القومي على الرغم من الجهود المبذولة التشريعية والأمنية.

3- تنامى الإستغلال السيئ والمنحرف للشبكات الإلكترونية يترك آثار تدميرية على الأمن القومي الليبي إذ ان الاختراق والتجسس الإلكتروني للبنية التحتية يمكن من الوصول الى معلومات حساسة وسرية حول الحكومات والشركات والمؤسسات مما يهدد الأمن القومي بالإضافة إلى قيام التهديدات بنشر الأفكار المتطرفة التي تؤثر على الأمن القومي.

4-غياب الأمن وعدم الإستقرار في ليبيا جعل ليبيا دولة ذات استراتيجية منكشفة إزاء الدول مما جسد فرصة لاختراق وتهديد امنها المعلوماتي ومن ثم تهديد امنها القومي.

التوصيات:

بعد هذه المقاربة التحليلية للوقوف على الأمن السيبرانى والجرائم السيبرانية وانعكاساتهم على الأمن القومي الليبي، وبناء على النتائج السابقة تم التوصل لجُملة من التوصيات:

1-العمل على الحد من الجريمة السيبرانية وضرورة تدخل المشرع القانوني لمواجهتها وتفعيل القوانين والنصوص والأجهزة الخاصة بالجرائم السبرانية وتدريب وتأهيل وحدات عسكرية وأمنية وكوادر متخصصة فنياً لمتابعة هذه الجرائم.

2-إنشاء هيئة وطنية ومركز عربي للأمن السيبرانى وغرفة استراتيجية للأمن السيبراني يشرف عليها مجلس الأمن القومي الليبي ومراكز للسلامة المعلوماتية ولطوارئ الإتصالات تتعاون فيما بينها وفق آلية واضحة وفعالة تتولى مراقبة المواقع الإلكترونية لحجب المواقع التي تهدد أمن واستقرار المجتمع.

(1) جازية شعيتير، مرجع سبق ذكره.

3-ضرورة وضع خطط استراتيجية وسياسة أمنية هادفة لنشر الوعي للأمن السيبراني ولمخاطر الجريمة السيبرانية من خلال التنسيق بين الوزارات والهيئات ومؤسسات المجتمع المدني مع عقد الندوات والدورات التدريبية والمؤتمرات والملتقيات وورش العمل الخاصة بالتوعية في مجال الأمن السيبراني والتهديدات السيبرانية و تجريم صور الجريمة السيبرانية وإحالتها إلى قضاء متخصص في الجرئم السيبرانية وبناء منظومة قانونية وقضائية تتعلق بالجرائم السيبرانية.

4- التأكيد على دور التنشئة الإجتماعية في الأسرة والمدرسة والمسجد والجامعة في مكافحة الجرائم الإلكترونية والتشجيع على البحث والدراسة في مجال الأمن السيبراني والجريمة السيبرانية وإدراج مجال الفضاء السيبراني ضمن مناهج التعليم في ليبيا وتدشين برامج تدريبية لمجلس الأمن القومى الليبي لبناء القدرات الشبابية في مجال الأمن السبرانى وتوظيف تطبيقات الذكاء الأصطناعى في الدفاع السبرانى عن المجتمع وترقية البحث العلمي في قضايا الأمن السيبراني من خلال تأِسيس مراكز وأكاديميات متخصصة في هذا الميدان و بناء مؤسسات أمنية سيبرانية مثل الشرطة السيبرانية والمخابرات السيبرانية والجيش السيبراني واستيعاب النوابغ في مجال الأمن السيبراني من أجل استقطابهم وتمكينهم من توجيه مواهبهم لخدمة الأمن القومي الليبي.

5-الإنضمام إلى اتفاقيات التعاون العربية والدولية في مجال حماية البيانات والمعلومات ومكافحة الجرائم السيبرانية.

6-التأكيد على دور وسائل الإعلام في معالجة هذه الجرائم وتعزيز آليات الوقاية منها.

المراجع المستعملة في البحث:

أولاً: المراجع العربية:

1-ايهاب خليفة، الأمن السيبرانى: الماهية والإشكاليات، رؤى مصرية، اكتوبر، 2019.

2-بكوش الروميساء، انعكاس التهديدات السيبرانية على الأمن الوطني الجزائري، مذكرة مقدمة لنيل شهادة الماستر في العلوم السياسية، تبسة، جامعة العربي التبسي، كلية الحقوق والعلوم السياسية 2019.-2018،

3-د. راشد محمد المري، الأمن السيبرانى وحماية الأنظمة الإلكترونية، دراسة تحليلية تأصيلية، مجلة الدراسات القانونية والاقتصادية، القاهرة، اكاديمية سعد العبدالله للعلوم الأمنية، المجلد 9، العدد 1 ، مارس 2023 ،

4-صالح مهدى هادى الشمري، زيد محمد على اسماعيل، الأمن السيبرانى كمرتكز جديد في الإستراتيجية العراقية، مجلة قضايا سياسية، جامعة النهرين، كلية العلوم السياسية، العدد 62، السنة 12، 2020.

5-د. عادل عبد الصادق،" الحروب السيبرانية :تصاعد القدرات والتحديات للأمن العالمي، تقرير استراتيجى، المركز العربي لأبحاث الفضاء الإلكتروني، 12مارس، 2017

6-د. عبدالسلام محمد المائل، الجريمة الإلكترونية في الفضاء الإلكتروني المفهوم – الأسباب، سبلُ المكافحة مع التعرض لحالة ليبيا، مجلة آفاق للبحوث والدراسات السياسية، المركز الجامعي، العدد 4، يوليو 2019

7- علي عباس مراد ، الأمن والأمن القومي ، مقاربات نظرية ، الجزائر ، ابن النديم للنشر ،2017 .

8-ماجد صدام سالم ، الأمن السيبرانى العراقي واثره في قوة الدولة ، مجلة العلوم التربوية والإنسانية ، العراق ، جامعة ميسان ، كلية التربية الأساسية ، العدد 18 ديسمبر 2022 .

9-مصطفى ابراهيم سلمان الشمري ، الأمن السيبرانى واثره في الأمن الوطني العراقي ، مجلة العلوم القانونية والسياسية ،جامعة ديالى ، كلية القانون والعلوم السياسية ،المجلد العاشر ، العدد الأول ، 2021.

10-د. منى عبدالله السمحان، متطلبات تحقيق الأمن السيبرانى لأنظمة المعلومات الإدارية بجامعة الملك سعود مجلة كلية التربية، جامعة المنصورة، كلية التربية ، العدد 111 ، يوليو .2020

11- نشوة اسماعيل زقوت واخرون ، مدى وعى أعضاء هيئة التدريس بالجامعات الليبية بأهمية الأمن السيبرانى ، المؤتمر العلمي الأول لتقنية المعلومات ، جامعة الزاوية ، كلية تقنية المعلومات ، 21 .22 ، 2022.

12-نهى على أمير، الأمن السيبرانى في استراتيجية الأمن القومي الروسي، مجلة آفاق اسيوية ، مصر ، الهيئة العامة للاستعلامات ، المجلد7 ، العدد 11 ،مارس 2023

13- وليد غسان سعيد جلمود ،" دور الحرب الإلكترونية في الصراع العربي الإسرائيلي" ، أطروحة ماجستير في التخطيط والتنمية السياسية فلسطين ، جامعة نابلس ، كلية الدراسات العليا ،2013 .

14-يوسف إسماعيل يوسف ما نيطه، نظرة عامة عن الجريمة الإلكترونية في الفضاء السيبراني المجلة الليبية العالمية، المرج، جامعة بنغازي، كلية التربية، العدد 32، 30 نوفمبر 2017.

ثانياً: شبكة المعلومات الدولية (الأنترنت):

1- الجريدة الرسمية ، قانون رقم 5 لسنة 2022 بشأن مكافحة الجرائم الإلكترونية ، مجلس النواب ،العدد 1 ،السنة الأولى ، 27سبتمبر ، 2022
https://lawsociety.ly/legislation/%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%B1%D9%82%D9%85-5-%D9%84%D8%B3%D9%86%D8%A9-2022-%D8%A7%D9%84%D8%AC%D8%B1%D8%A7%D8%A6%D9%85-%D8%A7
2- المرصد ، ليبيا: ممارسة الحقوق الدستورية في ظل قانون مكافحة الجرائم الإلكترونية ، صحيفة المرصد ، 30 /8 / 2023 ،
https://adalaforall.org/%D9%84%D9%8A%D8%A8%D9%8A%D8%A7--9-%D9%81%D9%8A-%D8%B8%D9%84- %D9%82%D8%A7/
3- الهيئة العامة للاستعلامات ، مصر والأمن السيبراني ، مصر ، 11 يونيو 2023
https://www.sis.gov.eg/Story/258293/%D9%85%D8%B5%D8%B1-%D9%88%D8%A7%D9%84%D8%A3%D9%85%D9%86-% D9%89?lang=ar
4- تصريح لأخبار ليبيا 24 " مستشار بالأمن القومى فيصل بوالرايقة" ، المجلس مدرك لأهمية مواجهة التهديدات السيبرانية المحدقة بليبيا ، أخبار ليبيا 24 ، 24 يناير2023 على الرابط
https://akhbarlibya24.net/2023/01/24/%D9%85%D8%B3%D8%AA%D8%B4%D8%A7% %D9%85%D8%AF%D8%B1%D9%83-%D9%84%D8%A3%D9%87%D9%85
5- جازية شعيتير ، السيبرانية على قائمة أولويات الأمن القومي ، جريدة بوابة الوسط ، 2، فبراير 2023 https://alwasat.ly/news/opinions/387415?author=1
6- د.م ، النظام القانوني للأمن الوطني الإلكتروني في ظل الثورة الرقمية" ، الرابط 2019/02/ 28 www.univ-chlef.dz/fdsp/pdf/je-
7- صالح بن علي بن عبد الرحمن الربيعة ، الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت .متاح على الرابط 2019-04- https://www.google.com/url?sa،
8- د. عادل عبد الصادق ،" المجلس الأعلى للأمن السيبراني خطوة في دعم استراتيجية الأمن القومي" ، الرابط/2019/03 : www.aceronline.com/article-detal.Aspxd=20284 .
9- علي الفيتورى ، تتابع أعمال مؤتمر ليبيا الدولي للأمن السيبراني تحت شعار ‘‘الأمن القومي والتهديدات السيبرانية في عالم متغير’’ ، الموقف الليبي ، بنغازي ، يناير 2023
https://libyanstand.net/2023/01/30/%D8%A7%D9%84%D9%85%D9%88%D9%82%D9-D9%85%D8%A4%D8%AA%D9%85%D8%B1-%D9%84%D9%8A%D8%A8
10- قانون مكافحة الجرائم الإلكترونية الليبي الجديد: تشريع القمع ، مجلس النواب الليبي يقر مشروع قانون مكافحة الجرائم الإلكترونية بعد اقرار مشروع قانون المعاملات الألكترونية ، مجلس النواب الليبي ، 26 اكتوبر 2021

https://smex.org/ar/%D9%85%D9%83%D8%A7%D9%81%D8%AD%D8%A9-%D8%A7%D9%84%D8%AC%D8%B1%D8%A7%D8%A6%D9%85-D9%8A%D8%A9-%D9%84%D9%8A%D8%A8%D9%8A%D8%A7/

11-مستشار الأمن القومي الليبي إبراهيم بوشناف. (أرشيفية)، مجلس الأمن القومي يشكل غرفة طوارئ لمتابعة تداعيات الهجوم السيبراني على إحدى شركات الاتصالات، جريدة بوابة الوسط، القاهرة ، 13 مايو 2023 ، https://alwasat.ly/news/libya/398554

12-ورقة تلخيصية: قانون مكافحة الجرائم الإلكترونية الجديد يفاقم ظاهرة الافلات من العقاب، تونس ، 16 نوفمبر 2022.

https://lcw.ngo/%D9%88%D8%B1%D9%82%D8%A9-%D8%AA%D9%84%D8%AE%D9%8A%D8%B5%D9%8A%D8%A9- -%D8%A7%D9%84%D8%AC%D8%B1%D8%A7%D8%A6%D9%85-%D8%A7

ثالثاً: المراجع الأجنبية:

1- Dictionnaire français Le petit Larousse , (France , Edition , 2001) ,

2- Dan Craiyen and others, "Defining cybrescurity", Technology innovation management review, Montreal, Canada, (october 2014).