الامن السيبراني وتداعياته على الامن القومي المصري

م.م. أحمد طلال احمد حسن
جامعة كركوك / كلية القانون والعلوم السياسية

Cyber security and its repercussions on Egyptian national security

M. M. Ahmed Talal Ahmed Hassan
University of Kirkuk / Faculty of Law and Political Science

المستخلص: هدفت الدراسة الى معرفة ابعاد الامن السيبراني ومنها البعد الاجتماعي والاقتصادي والصحي والعسكري والبعد السياسي والغذائي للجريمة السيبرانية وتحليل هذه التحديات والتهديدات التي يواجها الامن القومي المصري , وعلى مدى تأثير الجريمة السيبرانية على بروز صراع قومي مصري والاستراتيجية التي وضعتها مصر في مواجهة هذه الهجمات السيبرانية والحد من الجريمة المفتعلة اذ استخدمت الدراسة المنهج التحليلي والوصفي لوصف هذه الجريمة والحد منها ووضع استراتيجية لحماية البنية التحتية للدولة .**الكلمات المفتاحية :** الامن السيراني , الابعاد، الاستراتيجيات للحد من الجريمة , التكنولوجيا ، الامن القومي .

Abstract: The study aimed to know the dimensions of cyber security, including the social, economic, healthy, and military dimensions, and the political and nutrition dimensions of cybercrime, and to analyze these challenges and threats facing Egyptian national security and the extent of the impact of cybercrime on the emergence of an Egyptian national conflict, and the strategy that Egypt has developed to confront these cyber attacks and reduce crime. It is contrived, as the study used the analytical and descriptive approach to describe this crime, reduce it, and establish basics for protecting the state's infrastructure. **Keywords:**

Cybersecurity, Dimensions, Strategies to Reduce Crime, Technology, National Security.

المقدمة

بعد التقدم التكنولوجي المستمر في العالم تعتمد المجتمعات الحديثة بشكل مستمر على التكنولوجيا والاتصالات والمعلومات المترابطة بالشبكة العالمية حيث هذه الاعتماد التزايد ترافقه مخاطر عديدة والمحتملة التي تهدد بل اساس الشبكات وامن المعلومات والمجتمع المعلوماتي والافراد وحتى الامن القومي للدولة اذ ان هذه التهديدات او هذه المخاطر تودي الى خلق عدم استقرار بين افراد المجتمع داخل حدود الدولة وعدم استقرار لدي جميع مؤسسات الدولة ان كانت هذه المؤسسات امنية او خدمية ، لقد بات اليوم الامن السيبراني يشكل جزاء اساسي من سياسة الامن الوطني ، اذ بات معلوم لدي صاحب القرار ان يصنف الامن السيبراني او الدفاع السيبراني كأولوية في سياسه الدولة الدفاعية الوطنية حيث حتم على الدول في العالم على اختلاف سياستها الاقتصادية والاجتماعية والتعاون البيئي من اجل البحث عن استراتيجيات فعاله لتصدي لمثل هذه النوع من التهديدات التي تعمل على تحطيم البنية التحتية الإلكترونية للدولة ومنظومتها الامنية والاقتصادية والعسكرية وتعطيل مصالحها المادية والمعنوية وبالخصوص ما ستملت الرقمنه التكنولوجيا معظم قطاعات سيادة الدول اذ تقوم هذه الدراسة على معرفة حاله جمهورية مصر العربية من خلال الاستراتيجيات المتخذة لحماية امنها السيبراني وحماية انظمتها المعلوماتية وشبكات الاتصال ووضع اسس قانونية لحد من التهديدات والجرائم التي تقع فيها ان كانت على المستوى المحلي او على المستوى الدولي لحماية مجتمعها وافرادها ومؤسساتها المالية والاقتصادية من هذه الجرائم .

اهمية الدراسة : تكتسب اهمية البحث من خلال الاهتمام المتزايد بالمخاطر التي تعرض له نظام المعلومات الإلكترونية والبيانات والهيئات والمؤسسات المختلفة اذ يمكن ان تنشأ هذه التهديدات في اي مكان واي وقت وتسبب اضرار جسيمة في لحظة وهذه الاضرار تزايد مع

ارتباط تكنولوجيا والمعلومات والشبكات مع البنية التحتية للدولة اذ يجب ان يعمل المجتمع بالقضاء على هذه التهديدات المتكررة .

هدف الدراسة : هدفت الدراسة الى بيان دور الامن القومي المصري في مواجهة التهديدات الداخلية والخارجية التي تطال الامن القومي المصري وزعزعة الاستقرار المجتمعي من خلال وضع خطط استراتيجية محكمة فعاله للتخلص من هذة التهديدات .

مشكلة الدراسة : تتمحور اشكاليه الدراسة حول تساؤل رئيسي مفاده ما هو دور الامن القومي المصري في مواجهة الهجمات السيرانية بالإضافة الى وجود مجموعة من التساؤلات الفرعية وهي كلاتي

١. هل هناك منظومة معلوماتية على قدر كبير من الجودة لمواجهة هذه الهجمات السيبرانية

٢. ماهي الاجراءات التي اتخذتها الامن القومي المصري في مواجهة المخاطر والتهديدات

٣. الدور التشريعي في مواجهة مخاطر الامن السيبراني .

فرضية الدراسة : تنطلق فرضية البحث من ان كلما زادت قدرة الدولة على حماية امنها الفضائي وحماية انظمتها المعلوماتية وبياناتها وتوظيف هذه التكنولوجيا في مجالاتها ان كانت الامنية او الخدمية زادت قوتها واستقرار امنها الداخلي وعلى العكس كلما كانت الدولة ضعيفة من الناحية الامنية والتكنولوجيا اصحبت دولة محترقة وعدم استقرار امنها وبروز الجرائم وفتح المجال امام المستفيدين والمتنفذين من هذه الجرائم على التخريب واستغلال الوضع بكافة انواع الجرائم في الدولة .

منهجية الدراسة : فرضت طبيعة الدراسة على المنهج التحليلي والوصفي ورسم الاستراتيجيات المستقبلية لتحقيق الامن القومي المصري وجعل النظام صعب اختراقه .

هيكلية الدراسة : تقسمت الدراسة الى مبحثين بالإضافة الى مقدمة وخاتمة وقد تناول المبحث الاول الاطار النظري للأمن السيبراني ، اما المبحث الثاني فقد تناول أثر الحرب السيبرانية على الامن القومي المصري .

المبحث الاول : الاطار النظري للأمن السيبراني

يعيش العالم اليوم في عصر الرقمنه بفضل التطور الهائل في تكنولوجيا المعلوماتية والاتصالات بسبب الترابط والتشابك بين شبكات الاتصال التي ادت الى ظهور بيئة جديدة للتفاعل بين الافراد والمجتمعات والدول وهو ما اصطلح عليه بالفضاء السيبراني الذي ادى الى سوء الاستخدام هذا التكنولوجيا بين الدول التي ادت الى ضهور مخاطر وتهديدات تتعرض لها الدول في امنها وادى الى بروز الامن السيبراني كركيزة اساسية في بناء الامن القومي للدول .

المطلب الاول : مفهوم الامن السيبراني: تعد مهمة الضبط للمفاهيم والمصطلحات تحدياً يواجهة الباحثين والدارسين في العديد من التخصصات والمجالات وهذا ما يطرقة من اشكاليات تجعل من الصعب الاتفاق على تعريف واضح وشامل وموحد بين جميع اعظاء المجتمع العلمي ، اذ يعد الامن السيبراني واحداً من هذا المفاهيم المعقدة التي تقوم بها العديد من التعاريف المختلفة ، اذ يعد الامن السيبراني لغويا مكون من لفضين (الامن و السيبراني) اذ يعد الامن هو نقيض الخوف اي بمعنى السلام والامن مصدر الفعل أمن امنأ وامنا وامنه اي طمئنينة النفس وسكون القلب وزوال الخوف ويقال (امن من الشر اي اسلم منه) اذ يعرفة قاموس بنغوين للعلاقات الدولية بأنة بمصطلح يشير الى غياب ما يهدد القيم النادرة وبالرغم من ان مصطلح الامن القومي شاع بعد الحرب العالمية الثانية الا ان جذورة تعود الى القرنالسابع عشر وخاصة بعد معاهدة وستفاليا عام ١٦٤٨ التي اسست الدول القومية ، اذ شكلت حقبة الحرب الباردة الاطار والمناخ الذي من خلاله تحركت به محاولات صياغة مقاربات نظرية وصولاً الى استخدام منعى استراتيجية الامن القومي وسادت هذا المصطلحات ابان الحرب الباردة مثل الاحتواء والردع والتوازن والتعايش السلمي عناوين بارزة في هذا المقاربات الهدف هو تحقيق

الامن والسلم وتجنب الحرب المدمرة التي شهدتها في النصف الاول من القرن العشرين [١]، وبالرغم من ان هناك اتفاق على ان الفرد هو جوهر مفهوم الامن وهو الوحيد او الوحدة الاساسية للتحليل اذ ان هناك اختلاف حول التهديد او اعطاء تعريف جامح بين الباحثين في مجال الدراسات الامنية ومن بينهم [٢].

لوريد المسودرنيي اذ يعرف ان الامن السبراني في جوهرة هو محاوله لبناء مجتمع عالمي اذ تكون فيه سلامه الفرد في صميم الاولوية الدولية اذ تقدم المواقف الدولية لحقوق الانسان وسيادة القانون وينسجم في شبكة متماسكة تحمي الفرد

ويذهب (بول هينكر) بتعريفة الذي قال ان الامن الانساني هو التركيز على الافراد والمجتمعات بدل من الدولة كونه غير كاف لضمان بقاء الافراد فالامن الانساني يركز على مصادر التهديد التقليدية والعسكرية وغير العسكرية معأ فامن الافراد هو تحقيق الامن على المستوى العالمي

اما(جورج ماكلين) برى ان الامن الانساني في معناة الشامل يعنى تحويل الانتباه من الامن القومي الى امن الافراد فان الامن يعد حماية للافراد لن يتحقق من خلال حماية الدولة كوحدة اساسيسة ولكن من خلال التركيز على رفاهية الافراد ونوعية الحياة [٣].

ويعرف الامن السبيراني بانه توظيف التقنيات العلمية والعمليات والتدابير الازمة لضمان امن الشبكات والبرامج والاجهزة وحماية البيانات من الهجمات الاكترونية اذ يمثل العرض الاساسسي منه في تقليل المخاطر الاكترونية التي قد تتعرض لها الانظمة والشبكات وحمايتها من الاستقلال الغير شرعي والغير مصرح به[٤].

---

[١] فارس محمد عمدات و ابراهيم الحماحمه ، الامن السيبراني المفهوم والتحديات ، دار الخليج للنشر والتوزيع ، عمان ، الاردن ، العبدلي ،٢٠٢٢ ، ص ص ١٣,١٤.

[٢] راضية خماسمية ونور الهدى رويبع ، البعد الانساني للدبلوماسية الجزائرية ٢٠١٧/٢٠١١ ، جامعة العربي التبسي ، تبسة ، كلية الحقوق والعلوم السياسية ، رساله ماجستير غير منشورة ،٢٠١٨ ،ص ص ١٥ ،١٦.

[٣] راضية خماسميه و نور الهدى رويبع ، مصدر سبق ذكرة ،ص ١٧.

[٤] عبدالله دغش العجمي ، المشكلات العلمية والقانونية للجرائم الإلكترونية دراسة مقاربة ، جامعة الشرق الاوسط ، عمان ، رساله غير منشورة ، ٢٠١٤ ،ص ١١.

المطلب الثاني : ابعاد الامن السيبراني: للأمن السيبراني مجموعة من الابعاد متداخلة ومترابطة مع بعضها البعض وان كل بعد من هذا الابعاد يختلف من دولة الى اخرى :

١ . **البعد العسكري** : تميز القوة السيبرانية في قدراتها على دمج كل الوحدات العسكرية بعضها البعض عبر الشبكات العسكرية في الفضاء الاكتروني بما يسمح بسهولة تبادل المعلومات وتدفقها وسرعة اعطاء الاوامر العسكرية وقدرتها على اصابه الاهداف عن بعد وتدميرها وتحول هذا الميزة الى نقطة ضعف ان لم تكن هذه الشبكات الاكترونية المستخدمة في هذا مؤمنة جيداً من اي تدخل واختراق خارجي قد يسبب في شن هجمات الكترونية مضادة على شبكات القوات المسلحة واجهزتها الاستخبارتية ومن ثم تدمير قواعد البيانات العسكرية وتعطيل قدرتها وقدرة الدولة على النشر السريع لقدراتها وقوتها او قطع انظمةة الاتصال بين وحدتها العسكرية وتعطيل شبكة الكومبيوتر كما يتمكن من شل انظمة الدفاع الجوي او التوجية الاكتروني للخصم فظلأ عن امكانية فقدان السيطرة على الوحدات بالقيادة والتوجيه بالاضافة الى فقدان العدو قدرته على التحكم او الاتصال بالأقمار الصناعية [١].

٢ . **البعد الاقتصادي** : اصبحت التكنولوجية جاذبة لقطاعات المجتمع كافة جماعات وافراد والاعتماد عليه بصورة اساسية على التكنولوجية الرقمية في تخزين البيانات والمعلومات بالاضافة الى استخدام الحاسبة الالية في تطوير الصناعات وتحريك الاقتصاديات واصبحت العمولات المالية والاقتصادية محسوبة وباتت شبكات البنوك والبورصات وشركات الكترونية مما اصبحت شبكة الانترنيت هي اساس المعاملات المالية وباتت تشكل محور مهم ما اثار الحديث عن اهمية تحقيق الامن السيبراني في المجال الاقتصادي[٢].

[١] سعد بوه الشيخ محفوظ الحبيب ، ابعاد الامن السي براني ، الجيش والوطني الموريتاني ، الاثنين ٢٠٢٤/٥/١٣ MP١٠:٢٥ متاح على الرابط : https://armee.mr/node/3066

[٢] محمد ابو حمور ، الابعاد الاقتصادية للأمن السي براني ، الرأي ، ٢٠٢٤/٤/٣٠ ، ٤:٤٤ pm ، متاح على الرابط : https://alrai.com/article/10833703/

٣ . **البعد الاجتماعي** : يمكن تعريفة بانه هو اطمئنان الانسان على نفسة وماله واهله ودينة وسائر حقوقه وعدم خوفه او تهديده حاليا او مستقبلا في داخل بلدة او خارجه[١] اذ يعد البعد الاجتماعي عنصرأ مهم في التحقيق والحفاظ على الامن الرقمي اذ يتحقق الامن السيبراني بحماية الانظمة الاكترونية والشبكات من اي تهديدات الاكترونية واختراقات وذلك يتعدى الى ان يصل ليشمل العوامل الاجتماعية والبشرية اذ يوئيد هذا البعد في الامن السيبراني بعدت جوانب اي على سبيل المثال يلعب الوعي والتثقيفي السيبراني دورأ حاسمأ في تعزيز الامن السيبراني ووتحصين الافراد والمجتمع ضد الشبكات الاجرامية النشطة في هذه الفضاء وتمارس الابتزاز وتجارة الممنوعات والمخدرات والاستقلال الجنسي والتجارة بالبشر والهجرة الغير شرعية والافكار المتطرفة وجنى تجارة الاعظاء البشرية ويساعد بتعزيز الوعي المستخدمين بالمخاطرة السيبرانية المتمله وكيفية التعامل معها وتجنب التصرفات الخاطئة والوقوف في وجة التهديدات هنا بشكل افضل [٢].

٤ . **البعد السياسي** : يعد البعد السياسي من اهم الابعاد في الامن السيبراني اذ هناك العديد من الامثلة التي توكد على اهمية هذا البعد مثل على ماجرى من تسريب وثائق حساسه مختلفة التي سببت مشاكل جسيمة على المستوى الداخلي والخارجي وتؤثر بصفه حريصه على العلاقات بين الدول مثل ماحدث بالخليج بين قطر ودول الخليج الاخرى عام ٢٠١٧ اذ كانت الشرارة هي عملية اختراق تعرضت لها وكالة الانباء القطرية في ٢٣ مايو ايار ٢٠١٧ كمالا يمكن ان ينكر دور الشبكات التواصل الاجتماعية في المشهد السياسي فهى تستخدم في التظاهرات والحملات الانتخابية والحركات والاحتجاجات الاكترونية كما لايمكن ان ينكر دور الشبكات في قيام ثورات الربيع العربية اواخر ٢٠١٠ بالاضافة تستغل العديد من الحكومات هذه المنصات لترويج سياساتها ولانغفل عن استخدام الجماعات الارهابية لتلك المواقع لتجنيد اعضاء

[١] سلوى احمد ميدان و قحطان ياسين عطية ، الامن السيبراني واثرة على السيادة ، جامعه كركوك ، مجلة كلية القانون والعلوم السياسية ، المجلد ١٢ ، العدد ٤٤، الجزء ١ ، ٢٠٢٣ ، ص ٢٦.
[٢] سعد بو الشيخ مخفوظ الحبيب ، مصدر سبق ذكرة .

جدد وجمع المال لعملياتها والترويج لافكارها التخريبية وتعد هذه المنصات وسيله للتواصل بين الافراد والجماعات والتهديدات والمخاطرة التي تنطوي عليها شبكة الانترنيت [١].

٥ . **البعد الغذائي** : اختلفت الاراء حول مفهوم الامن الغذائي ومن اهم ماتعرف به هذا المفهوم من قبل الامم المتحدة على انه ضمان حصول كل الافراد وفي كل الاوقات على كفايتهم من الغذاء الذي يجمع بين النوعية الجدية والسلامة لكي يعيش الناس حياة كريمة وصحية اذ لاياتي ذلك الا بعملية توفير الامدادات الغذائية المستمرة وتكون متاحة مادياً واقتصادياً لجميع اذ يعد الامن الغذائي قدرة المجتمع لتوفير الغذاء لجميع افراد الشعب [٢]. الا ان التعريف الاكثر تداولا هو قدرة المجتمع على توفير احتياجات التغذية الاساسية لافراد الشعب وبضمان الحد الادنى من تلك الاحتياجات بانتظام اذ تزداد اهمية الامن الغذائي بتحقيق الامن القومي اذ تكاد تحتكر الدول الكبرى معظم فائض الانتاج الزراعي والغذائي وتقوم بستخدامة كسلاح لخدمة اهدافها واغراضها متى ما شاءت [٣]. اذ يوكد ذلك ماقيل من قبل الرئيس السابق للولايات المتحدة الامريكية (فورد) بان الترسانة الامريكية تضم سلاحاً سياسياً ذوفاعلية خاصة انه الغذاء وبذلك ان الولايات المتحدة الامريكية ليست بحاجة الى استخدام اسلحتها الحربية في المستقبل طالما اصبح الغذاء اكبر سلاح اذ تعد قضية الامن الغذائي من ابرز القضايا التي يواجهها العالم في الحاظر والمستقبل على الصعيد الاقتصادي والسياسي فعندما لايتم توفير الغذاء بالقدر الكافي والنوعية المناسبة تكون امام حالة فقدان للامن الغذائي وهذه الحاله تظهر بشكلها الموقت ثم تتلاشى وقد تتحول الى حالة دائمة كما هو الحال في الكثير من بلدان العالم في وقتنا الحالي وتعتبر قضية الامن الغذائي قضية استراتيجية اساسية وبالوقت نفسة قضية اقتصادية بحته [٤].

---

[١] سعد بوه الشيخ محفوظ الحبيب ، مصدر سبق ذكره .

[٢] اسماء حمزة علي ، الامن السيبراني ومستقبل الصراع الدولي في القرن الحادي والعشرين (ايران واسرائيل) انموذجاً ،جامعة كركوك ، كلية القانون والعلوم السياسية ، رساله ماجستير غير منشورة ، ٢٠٢٢ ، ص ١٠.

[٣] صالح الامين الارباح ، الامن الغذائي ابعادة ومحدداته وسبل تحقيقه ، الهيئية القومية للبحث العلمي ، ١٩٩٦ ، ص ١٣ .

[٤] ابراهيم حربي ابراهيم ، سياسة الامن الغذائي في العراق التحديات والحلول ، الجامعة التقنية الوسطى ، المعهد التكنولوجي ، بغداد , العدد ٢٧ ، ٢٠١٦ ، ص ٢٠٣.

٦ . **البعد الصحي** : تعد حماية الافراد في المجتمع من المخاطر التي تهدد صحتهم وحياتهم اذ ان هناك ترابط بين الامن الصحي والبيئي والغذائي يوثر بشكل كبير على الامن الصحي لان الغذاء له دور كبير في تدهور صحة الانسان وكذلك الحال بالتلوث البيئي [١].

٧ . **البعد القانوني** : تتمثل المخاطر القانونية بشكل اساسي بغياب الإطارين التشريعي والتنظيمي المناسبين للتعامل مع الاعمال القانونية وغير القانونية منها والتي يتم بالفضاء السيبراني اذ يتطلب النشاط الاقتصادي والتجاري وغيرها تحديا كبيرا واضحا للواجبات والحقوق فان مستخدمو هذه التقنية عبر الفضاء السيبراني بحاجة الى اطار قانوني يؤمن حماية استخداماتهم ففي حاله غياب الاطار التشريعي توثر الجرائم السي برانية على عمليات معلوماتية تخص حقوق الانسان الدولية وتدفع على العنف وتؤدى الى اضرار اقتصادية خطيرة فضمان ادارة مخاطر الامن السيبراني على النحو ممنهج تهدف الى حماية الاصول المعلوماتية والتقنية وفقاً للسياسات والاجراءات التنظيمية والمتطلبات التشريعية ومن هذه المنطلق تتمثل المخاطر القانونية في غياب الامن القانوني وحتى في نقض الاحكام والقوانين وتنازع الانظمة القانونية فمبدى الى ارتفاع نسبة المخاطر مع انعدام ملاحقة فاعله وصيغة الاعمال الاجرامية التنظيمية والمتطلبات التشريعية ومن هذا المنطلق تتمثل المخاطرة القانونية في غياب الامن القانوني وحتى في نقض الاحكام والقوانين وتنازع الانظمة القانونية مبتدئ الى ارتفاع نسبة المخاطر مع انعدام ملاحقة فاعلة وصيغة الاعمال ا الاجرامية والاعتداء السيبراني العابر الحدود وللأنظمة القانونية بحيث تطل الي مواطن في اي مكان على الارض وتطل امن الدولة واستقرارها اذ تعد هذه المخاطرة التي تعرض لها الافراد والدولة مخاطرة هائلة وغير مفيدة بالأطر القانونية الجارية التي لا تستوعب العصر السيبراني بالعذر الكافي وهذه على البلدان ان تتسارع في حماية انظمتها وتسوية قوانين صارمه اتجاه منفذي اي هجمة على اي فرد او اي دوله [٢] .

المبحث الثاني : الحرب السيبرانية و الامن القومي المصري

---

[١] ساعد حمزة علي ، الامن السي براني ومستقبل الصراع الدولي ،

[٢] اسلام فوزي ، الامن السيبراني والابعاد الاجتماعية والقانونية تحليل سوسيولوجي ، جامعة دمنهور ، مصر ، كلية الاداب ، قسم علم الاجتماع ، المجلة الاجتماعية القومية ، المجلد السادس والخمسون ، العدد الثاني ، ٢٠١٩ ، ص ص ١١٣ ، ١١٤.

ان المحافظة على الاراضي المصرية وفرض سيادة الدولة والقانون على ربوعها وبيان حالة الاستقرار المجتمعي الداعم للتقدم والنهضة وضمان بقاء المؤسسات وتطويرها تعد ثروه من ثروات البلد البشرية وان صيانه لكيان الدولة بكل ما بها من مقدرات ومن ثم تصبح حماية المجتمع وقيمته الاجتماعية ومؤسساته وحدود الوطن الجغرافية مسئوليه النظام السياسي للدولة اذ ان هذا الامر يأتي في مقدمة الامن القومي المصري

المطلب الاول : اثر الحرب السيبرانية على الامن القومي المصري

تعد الحروب السيبرانيه حروب افتراضية التحليل غير ملموسة تحاكي الواقع على نحو شبه تام ، اذ تنحصر بمواجهات الكترونية عبر برامج تقنية ولديها جنود تتمثل ببرامج التخريب المحسوبة اذ يستخدمون حلقات من لوحات المفاتيح ونقرات المبرمجين اذ يرى البعض ان هذه الحروب تتقابل مع الحروب التقليدية بأحداثها وبث الارهاب والرعب لدي الاخرين عبر هذه الشبكات مستهدفين الدول والافراد والمؤسسات والجماعات وتكبدهم خسارة اقتصادية لدخالهم حاله من الازمات النفسية والاجتماعية نتيجة تعرضهم لما يعرف بالإرهاب الصامت [١]. ان عالم اليوم اكثر ترابط مما مضى وذلك الترابط ادى الى تزايد المخاطر على الدول والافراد ومنها مخاطر السرقة والاحتيال والاساءة وتزايد اعتماد الاشخاص على التكنولوجية حول العالم اذ اصبحوا اكثر عرضة لتمثل هذه الهجمات الإلكترونية مثل الاختراق للأمن بالشركات والتهديد الاحتيالي والابتزاز والنصب عبر الوسائل منها وسائل التواصل الاجتماعي اذ يلاحظ ان الفضاء السي براني والبنية التحتية الاساسية لها عرضه واسعه للهجمات والمخاطر الناجمة عن التهديدات والمخاطر المادية الإلكترونية اذ تستقبل الجهات الفاعلة الكرتونية والدول القومية نقاط ضعف لدى خصومها لسرقة البيانات والمعلومات والاموال وتطوير القدرات على التعطيل وتدمير قدرة الدولة الخصم [٢]. اذ يعد الفضاء الإلكتروني من احد اهم الاشكال الجديدة لمفهوم القوة والتغيير بما يمكن من المتنفذ فيها من استخدام علاقته الدولية بطريقة تضمن مصالحها وامنها القومي

[١] فرج يحيى زعاترة ، التهديدات السيبرانية على الامن القومي الامريكي ، العربي للنشر والتوزيع ،لبنان ، بيروت ، ٢٠٢٣ ص ٢٠ .

[٢] حسين باسم عبد الامير ، تحديات الامن السيبراني ، مركز الدراسات الاستراتيجية ، جامعة كربلاء ، ٢٠١٨ ، متاح على الرابط : https://kerbalacss.uokerbala.edu.iq/wp/blog/2018/05/17/

وبهذا يصبح احد الفاعليين الرئيسين في مجتمع الدول الصراعية [١]. اذ ان تطور الامن القومي افرز تحديات والعاد جديدة لهذا المفهوم حيث افرزت التحديات العديد من التهديدات واحد من اهم التهديدات هو التهديد الإلكتروني وواحد من اهم التحديات اذ اصبح التهديد الإلكتروني يوثر بقوة على الامن القومي للدولة في الوقت الراهن على الاقل اذ اصبحت السياسات الامنية للدول تضمن التركيز على مفاهيم امنية جديدة منها الحرب الإلكترونية والجريمة السي برانية وجرائم الانترنيت والقرصنة واختراق الاجهزة القومية الحسابية للمؤسسات العسكرية وتهديد القيم الاخلاقية وتهديد ازمة عدم الثقة للجيل والمجتمع [٢]. وعلى المستوى الوطني ان بعض او معظم الحكومات تعترف بضرورة توزيع الموارد واصلاح الاستراتيجيات بالأمن الوطني من خلال وضع برامج على زيادة التمويل والبحث عن الموارد التكتيكية والدبلوماسية التي تعزز امنها السيبراني على المستوى الداخلي اما على المستوى الدولي فيغير الحوار العالمي والتعاون الضروري نظريا لكون المعايير القانونية الدولية غير مجهزة لتعامل مع التهديدات بابتكار التطبيقات الذكية مع المسح البارومتري لا حداث التقنيات والبرمجة السي برانية لتحليل الحالات الطارئة المتعلقة بالأنترنيت والتي تهدد الانظمة بالطاقة الذكية كاستراتيجية هجومية على مستوى الشبكات

اذا اثرت الحرب السي برانية على الامن القومي المصري على عدة اشكال منها

_ زيادة معدل الجرائم السيبرانية

_ التجسس والقرصنة السيبرانية

_الارهاب السيبراني

_الحرب السيبرانية

[١] صفاء حسين علي ، الحرب الاكترونية في المدرك الاستراتيجي الامريكي ، جامعة كركوك ، كلية القانون والعلوم السياسية ، دراسات دولية ، العدد ٨٢ ، ٢٣٢.

[٢] سمير باي ، التهديدات الامنية السيبرانية دراسة في انعكاسات الحرب الاكترونية على الامن القومي للدول واستراتيجية المقاومة ، جامعة الجزائر ، مجلة الدراسات والبحوث الانسانية ، مجلد ٨ ، العدد ٢، ٢٠٢٣ ،ص ١٩٨.

_ تدمير البنية التحتية للدولة

اذ كشفت لجنة الاتصالات والتكنولوجية على وضع دراسة جديدة عن قانون الجريمة الإلكترونية في مصر وبدل العمل لاكن ترتكب للأسف عشرات الجرائم الإلكترونية يوميا منها سرقات وتزوير ونصب وابتزاز الفتيات وغيرها من الجرائم الاخرى اذ ذكر احمد بدوي رئيس اللجنة ان كل يوم تلو الاخر تزداد الجريمة الإلكترونية في مصر وزادت بشكل اكبر في المناطق الريفية في مختلف محافظات الدولة ولفت انتباه الاباء والامهات بضرورة مراقبة ابناءهم من خطر استخدام وسائل التواصل الاجتماعية حيث ذكرت اللجنة عن كشف شهري في سبتمبر واكتوبر تقديم ما يقارب ١٠٨٣ بلاغ عن جريمة الكترونية اذ تمكنت وزارة الداخلية من ضبط والقاء القبض على البعض من مرتكبي الجريمة والمتهمين بهذا الجرم اذ في اواخر شهر اكتوبر اي بل ١٠ ايام الاخيرة وقعت ٣٦٥ جريمة الكترونية وان اغلبهن نصب واحتيال وتركيب صور للفتيات وبيع الادوية المنتهى الصلاحية للاستخدام الادمي عبر الانترنيت الى جانب التجارة بالأثار المزورة عبر صفحات الانترنيت [١]. اذ اكدت مصادر الادارة العامة للمعلومات والوثائق بوزارة الداخلية المصرية على ان البعض استغل ما اتيح له العلم والتقدم التكنولوجي الحديث استغالا نسبأ وبدأ بارتكاب اعمال او انفعال ترقي المستوى الجريمة واصبحت تشكل هاجسا وتحديا للأجهزة الامنية وباتت واضحة بان التهديد القادم شديد الخطورة في ظل هذه الظروف الدولية والاقليمية المتشابكة اذ جرى الاعداد منذ اكثر من سنتين على تأسيس وحدة مباحث جديدة تكون معينة بعملية وصد ومتابعة وضبط جميع هذا الجرائم المستخدمة بجميع اشكالها واساليبها والتي تكون الكمبيوتر بها العنصر في ارتكابها خاصة بعد ان بداءات هذه الجرائم تأخذ اشكال وابعاد دولية جديدة وبشكل خاص وسريع ومن اهم الجرائم التي استحدث في مصر هي استخدام بطاقات الائتمان المملوكة لغير شخص او يتم السرقة بها من خلال استخدامها في شراء السلع والخدمات من الخارج وجرائم الشبكات واختراقها والدخول الى اجهزة الحاسوب وسرقه المعلومات التي لها سرية خاصه للبعض من الاشخاص او الشركات والمؤسسات كما نشرها

[١] دراسة برلمانية عن الجرائم الاكترونية ، اليوم السابع ، مصر ، الثلاثاء ٢٣/يوليو / ٢٠٢٤ / ٢:٣٠ ، متاح على الرابط. http://yaum7.com/story/20/9/11/5/4486999

مقاطع تسئ لا شخاص اخرين او تسئ لشكل ومظهر الدولة والهاكرز واطلاق الفايروسات بالكمبيوتر التابع للمؤسسات والافراد وجرائم الغش الصناعي والسطو وتجارة السلاح والمخدرات وغسيل الاموال والآداب وجرائم مجتوى الانترنيت والمواقع الاباحية والمعادية سواء دينيا وسياسيا [١]. ففي عام ٢٠٢٣ قام فريق البحث والتحليل العالمي في الشرق الاوسط وافريقيا وتركيا المتمثل بشركة (كاسبرسكي) المتخصصة في خدمة الامن السي براني عن الكشف نحو ١٣ مليون هجمة سيبرانية على مصر خلال الربع الاول من العام وتركزت هذه الهجمات على الحسابات المصرفية وبيانات العملاء في القطاعات المصرفية المصرية بنسبة ١٨٦% خلال الربع الاول من العام مقارنة بنفس هذه الفترة عام ٢٠٢٢ ويغأ لهده ايضا فان وجود زيادة في الهجمات القرصنة التي تستهدف نظم المعلومات في قطاع التجزئة المصرفي في مصر وزيادة الهجمات التصييد الاحتيالي عبر البريد الإلكتروني والرسائل النصية وتعرض مايقارب ٧٥ الف مستخدم في مصر خلال الربع الاول عام ٢٠٢٣ تهجمات التصييد الاحتيالي وتعرض المؤسسات الحكومية المصرية شخصيا الى فرق قرصنة بهدف التجسس وسرقة بيانات العملاء [٢].

المطلب الثاني :الاستراتيجية المصرية في مواجهة الحرب السيبرانية

بالجهود المبذولة لدعم الامن القومي وتنمية المجتمع المصري ووفق المادة رقم ٣١ من دستور جمهورية مصر العربية التي نصت على ان امن الفضاء المعلوماتي هو الجزء الاساسي من الاقتصاد والامن القومي اذ تلتزم الدولة اتخاذ التدابير اللازمة لمحافظه عليها وعلى النحو الذي ينظمه القانون ومع تزايد التهديد والتحدي المستقبلي في المجال السي براني والمجتمع الرقمي ورصد ومحاربة المخاطر والتهديدات المتزايدة وانطلاق من اهداف دعت الي انشاءها المجلس الأعلى لتأمين البنية التحتية للاتصالات والمعلومات (المجلس الاعلى للأمن السي براني) اذ تم اعداد وثيقة تتضمن عدد من البرامج التي تدعم الاهداف الاستراتيجية للأمن السي براني كما

---

[١] محمد صادق اسماعيل ، الجريمة الاكترونية في مصر واساليب مكافحتها ، المرجع الكتروني للمعلومات ، ٢٠٢٤/٢/٢٥ ، ٣:٣٠ mp، متاح على الرابط : https://mail.almerja.com/reading.php?idm=223857

[٢] رغد البهي ، التجربة المصرية في مكافحة الارهاب السيبراني رؤية تحليلة ، مركز الاهرام للدراسات السياسية والاستراتيجية ،٢٠٢٣/١٢/٢٢، متاح على الرابط :http://acpss.ahram.org.egl/News/2/074.aspx .

تبين توزيع الادوار بين الجهات الحكومية والقطاع الخاص ومؤسسات الاعمال والمجتمع المدني نحو اقتصاد رقمي متكامل يعمل على تحقيق طموحات المواطنين في التنمية الاجتماعية واقتصادية شامله ويحمي مصالحهم ويحافظ على مصالح الدولة ويسهم في نجاحها وازدهارها ورخائها [١].

ان الاهمية الاستراتيجية للأمن السيبراني المصري تتجلى في نقطتين اساسيتين هما :

_ التصدي للحوادث من حيث عددها ومصدرها

_صناعه فرص جديدة للسوق المصري عبر بناء وانشاء كوادر بشرية متطورة وتطوير صناعتها الوطنية التي تسهم في زيادة اجمالي النتائج وتتجلى الى قوة الامن السي براني بي زيادة اعداد الطلاب واعضاء هيئة التدريس بالجامعات التكنولوجية ونحو البنية التحتية للاتصالات وتكنولوجيا المعلومات مما يجذب خدمات الامن السيبراني اذ تعمل مصر على تطوير استراتيجيتها الوطنية لعام ٢٠٢٣ على تجارب الدول الرائدة في ادارة الامن والخبراء الاكاديميين والشركات العاملة في هذه المجال وتكنولوجيا المعلومات وتطوير الابحاث في مجال الامن السي براني ووضع برامج استراتيجية حديثة [٢]. اذ وضعت الحكومة المصرية نصوص قانونية ذات صله بمختلف التهديدات السي برانية بشكل عام والارهاب بشكل خاص اذ هي نصوص يمكن الوقوف على ابرزها بما نصت المادة ٣١ من الدستور المصري ووفقا على التعديلات التي ادخلت علية في ٢٣ ابريل ٢٠١٩ ونصت بما يلي :

أولا : قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ اذ نصت على مادتين (المادة ٢٠ والمادة ٢١)

المادة ٢٠ : يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتي ألف جنيه ، أو بإحدى هاتين العقوبتين ، كل من دخل عمدا ، أو دخل بخطأ غير

[١] نجوان احمد عاصم عبد الجواد ، الجريمة السيبرانية وتاثيرها على الامن القومي المصري دراسة سوسيو تحليلة ، جامعة الفيوم ، مجله كلية الاداب ، مجلد ٥ ، عدد ١ ، ٢٠٢٣ ، ص ٢٠١١٧

[٢] الضوي احمد ، استراتيجية الامن السيبراني المصري : حصن الوطن من الاحداث حروب العصر الحالي ،بوابه الاهرام ، متاح على الرابط : https://gate.ahram.arg.eg/.

عمدى وبقى بدون وجه حق ، أو تجاوز حدود الحق المخول له من حيث الزمان أو مستوى الدخول أو اخترق موقعا او بريدا إلكترونيا أو حسابا خاصا أو نظاما معلوماتيا يدار بمعرفه أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة ، أو مملوكا لها ، أو يخصها. فإذا كان الدخول بقصد الاعتراض أو الحصول بدون وجه حق على بيانات أو معلومات حكومية ، تكون العقوبة السجن ، والغرامة التي لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه. وفى جميع الأحوال، إذا ترتب على أي من الأفعال السابقة إتلاف تلك البيانات أو المعلومات أو ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي أو البريد الإلكتروني ، أو تدميرها أو تشويهها أو تغييرها أو تغيير تصاميمها أو نسخها أو تسجيلها أو تعديل مسارها أو إعادة نشرها ، أو إلغاؤها كليا أو جزئيا ، بأي وسيلة كانت ، تكون العقوبة السجن ، والغرامة التي لا تقل عن مليون جنيه ولا تجاوز خمسة ملايين جنيه[١].

المادة ٢١ : يعاقب بالحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه ، أو بإحدى هاتين العقوبتين ، كل من تسبب متعمدا في إيقاف شبكة معلوماتية عن العمل أو تعطيلها أو الحد من كفاءة عملها أو التشويش عليها أو إعاقتها أو اعتراض عملها أو أجرى بدون وجه حق معالجة الكترونية للبيانات الخاصة بها ويعاقب كل من تسبب بخطئه في ذلك بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتي الف جنيه ، أو بإحدى هاتين العقوبتين. فإذا وقعت الجريمة على شبكة معلوماتية تخص الدولة أو أحد الأشخاص الاعتبارية العامة او تمتلكها او تدار بمعرفتها تكون العقوبة السجن المشدد ، وبغرامة لا تقل عن خمسمائة ألف جنيه ول اتجاوز مليون جنيه[٢].

ثانيا : قانون رقم ٩٤ لسنة ٢٠١٥ الذي نصت مواده (١ و ٣ و ١٥ و٢٩ و ٤٦) ما يلي

---

[١] رئيس الجمهورية ، قانون رقم ١٧٥ لسنه ٢٠١٨ ، في شأن مكافحة جرائم تقنية المعلومات ، الجريدة الرسمية العدد ٣٢ مكرر ، (ج) في ١٤ اغسطس ٢٠١٨ ص ١٦.

[٢] رئيس الجمهورية ، مصدر سبق ذكرة ، ص ١٧.

المادة ١ : في تطبيق أحكام هذا القانون ، يقصد بالكلمات والعبارات التالية المعنى المبين قرين كل منهما الجهاز :الجهاز القومي لتنظيم الاتصالات.

الوزير المختص : الوزير المعنى بشئون الاتصالات وتكنولوجيا المعلومات .

البيانات والمعلومات الإلكترونية : كل ما يمكن إنشاؤه أو تخزينه أو معالجته أو تخليقه أو نقله أو مشاركته أو نسخه ، بواسطة تقنية المعلومات ، كالأرقام والأكواد والشفرات والحروف والرموز والإشارات والصور والأصوات ، وما في حكمها .

بيانات شخصية : أي بيانات متعلقة بشخص طبيعي محدد أو يمكن تحديده ، بشكل مباشر أو غير مباشر عن طريق الربط بينها وبين بيانات أخرى .

بيانات حكومية : بيانات متعلقة بالدولة أو إحدى سلطاتها ، أو أجهزتها أو وحداتها ، أو الهيئات العامة ، أو الهيئات المستقلة أو الأجهزة الرقابية ، أو غيرها من الأشخاص الاعتبارية العامة وما في حكمها ، والمتاحة على الشبكة المعلوماتية أو على أي نظام معلوماتي أو على حاسب أو ما في حكمها .

المعالجة الإلكترونية : أي عملية إلكترونية أو تقنية تتم كليا أو جزئيا لكتابة أو تجميع أو تسجيل أو حفظ أو تخزين أو دمج أو عرض أو إرسال أو استقبال أو تداول أو نشر أو محو أو تغييرا تعديل أو استرجاع أو استنباط البيانات والمعلومات الإلكترونية ، وذلك باستخدام أي وسيط من الوسائط أو الحاسبات أو الأجهزة الأخرى الإلكترونية أو المغناطيسية أو الضوئية أو ما يستحدث من تقنيات أو وسائط أخرى.

تقنية المعلومات: أي وسيلة أو مجموعة وسائل مترابطة وغير مترابطة تستخدم لتخزين واسترجاع وترتيب وتنظيم ومعالجة وتطوير وتبادل المعلومات أو البيانات ، ويشمل ذلك كل ما يرتبط بالوسيلة أو الوسائل المستخدمة سلكياً أو لاسلكياً.

مقدم الخدمة: أي شخص طبيعي أو اعتباري يزود المستخدمين بخدمات تقنيات المعلومات والاتصالات ، ويشمل ذلك من يقوم بمعالجة أو تخزين المعلومات بذاته أومن ينوب عنه في أي من تلك الخدمات أو تقنية المعلومات.

المستخدم: كل شخص طبيعي أو اعتباري ، يستعمل خدمات تقنية المعلومات ، أو يستفيد منها بأي صورة كانت .

البرنامج المعلوماتي: مجموعة الأوامر والتعليمات المعبر عنها بأي لغة أو رمز أو إشارة والتى تتخذ أي شكل من الأشكال ، ويمكن استخدامها بطريق مباشر أو غير مباشر في حاسب آلي لأداء وظيفة أو تحقيق نتيجة ، سواء كانت هذه الا وامر والتعليمات في شكلها الأصلي أو في أي شكل آخر تظهر فيه من خلال حاسب ألي، أو نظام معلوماتي.

النظام المعلوماتي: مجموعة برامج وأدوات معدة لغرض إدارة ومعالج البيانات والمعلومات ، أو تقديم خدمة معلوماتية .

شبكة معلوماتية: مجموعة من الأجهزة أو نظم المعلومات تكون مرتبطة معا ، ويمكنها تبادل المعلومات والاتصالات فيما بينها ، ومنها الشبكات الخاصة والعامة وشبكات المعلومات الدولية ، والتطبيقات المستخدمة عليها.

الموقع: مجال أو مكان افتراضي له عنوان محدد على شبكة معلوماتية ، يهدف إلى إتاحة البيانات والمعلومات للعامة أو الخاصة .

مدير الموقع: كل شخص مسئول عن تنظيم أو إدارة أو متابعة أو الحفاظ على موقع أو أكثر على الشبكة المعلوماتية ، بما في ذلك حقوق الوصول لمختلف المستخدمين على ذلك الموقع أو تصميمه أو توليد وتنظيم صفحاته أو محتواه أو المسؤول عنه.

الحساب الخاص: مجموعة من المعلومات الخاصة بشخص طبيعي أو اعتباري ، تخول له دون غيره الحق فى الدخول على الخدمات المتاحة أو استخدامها من خلال موقع أو نظام معلوماتي.

البريد الاليكتروني: وسيلة لتبادل رسائل إلكترونية على عنوان محدد ، بين أكثر من شخص طبيعي أو اعتباري ، عبر شبكة معلوماتية ، أو غيرها من وسائل الربط الإلكترونية من خلال أجهزة الحاسب الآلي وما في حكمها.

الاعتراض: مشاهدة البيانات أو المعلومات أو الحصول عليها ، بغرض التنصت أو التعطيل أو التخزين أو النسخ أو التسجيل أو تغيير المحتوى أو إساءة الاستخدام أو تعديل المسار أو إعادة التوجيه ، وذلك لأسباب غير مشروعة ودون وجه حق.

الاختراق: الدخول غير المرخص به ، أو المخال لأحكام الترخيص ، أو الدخول بأي طريقة غير مشروعة إلى نظام معلوماتي أو حاسب آلى أو شبكة معلوماتية وما في حكمها.

المحتوي: أي بيانات تؤدي بذاتها أو مجتمعه مع بيانات أو معلومات أخرى إلى تكوين معلومة أو تحديد توجه أو اتجاه أو تصور أو معني أو إشارة إلى بيانات أخرى .

الدليل الرقمي: أي معلومات إلكترونية لها قوة أو قيمة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية وما في حكمها ، ويمكن تجميعها وتحليلها باستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة .

الخبرة: كل عمل يتصل بتقديم الاستشارات أو الفحص أو المراجعة أو التقييم أو التحليل في مجالات تقنية المعلومات.

حركة الاتصال (بيانات المرور): بيانات ينتجها نظام معلوماتي تبين مصدر إلا تصال وجهته والوجهة المرسل منها والمرسل إليها ، والطريق الذي سلكه وساعته وتاريخه وحجمه ومدته ونوع الخدمة .

الحاسب: كل جهاز أو معدة تقنية تكون قادرة على التخزين وأداء عمليات منطقية أو حسابية ، وتستخدم لتسجيل بيانات أو معلومات أو تخزينها أو تحويلها أو تخليقها أو استرجاعها أو ترتيبها أو معالجتها أو تطويرها أو تبادلها أو تحليلها أو للاتصالات.

دعامة إلكترونية: أي وسيط مادى لحفظ وتداول البيانات والمعلومات الإلكترونية ، ومنها الأقراص المدمجة و الأقراص الضوئية و الذاكرة الإلكترونية أو ما في حكمها.

الأمن القومي: كل ما يتصل باستقلال واستقرار وأمن الوطن ووحدة وسلامة أرضيه ، وما يتعلق بشئون رئاسة الجمهورية ومجلس الدفاع الوطني ومجلس الأمن القومي ، ووزارة الدفاع والإ نتاج الحربى ، ووزارة الداخلية ، والمخابرات العامة ، وهيئة الرقابة الإدارية ، والأجهزة التابعة لتلك الجهات . جهات الأمن القومي: رئاسة الجمهورية ، ووزارة الدفاع ، ووزارة الداخلية ، والمخابرات العامة ، وهيئة الرقابة الإدارية التزامات وواجبات مقدم الخدمة [١]

المادة ٣ : مع عدم الإخلال بأحكام الباب الأول من الكتاب الأول من قانون العقوبات ، تسري أحكام هذا القانون على كل من ارتكب خارج جمهورية مصر العربية من غير المصريين جريمة من الجرائم المنصوص عليها من هذا القانون ، متي كان الفعل معاقبا عليه في الدولة التي وقع فيها تحت أي وصف قانوني ، وذلك في أي من الأحوال الاتية :

١- إذا ارتكبت الجريمة على متن أيه وسيله من وسائل النقل الجوي أو البري أو المائي ، وكانت مسجله لدي جمهورية مصر العربية أو تحمل علمها.

٢- إذا كان المجني عليهم أو أحدهم مصرياً.

٣- إذا تم الاعداد للجريمة أو التخطيط أو التوجيه أو الاشراف عليها أو تمويلها في جمهورية مصر العربية.

٤- إذا ارتكبت الجريمة بواسطة جماعة إجرامية منظمة ، تمارس أنشطة إجرامية في أكثر من دولة من بينها جمهورية مصر العربية .

---

(١) رئيس الجمهورية ، قانون مكافحة الارهاب ، الجريدة الرسمية ، جمهورية مصر العربية ،العدد٣٣ في ١٥ اغسطس ٢٠١٥ ، الباب الاول الاحكام الموضوعة ،ص ٥ص٦.

٥- إذا كان من شأن الجريمة إلحاق ضرر بأي من موطني جمهورية مصر العربية أو المقيمين فيها ، أو بأمنها أو بأي من مصالحها ، في الداخل أو الخارج.

٦- إذا وجد مرتكب الجريمة في جمهورية مصر العربية ، بعد ارتكابها ولم يتم تسليمة[١].

المادة ١٥ : يعاقب بالحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه ، أو بإحدى هاتين العقوبتين ، كل من دخل إلى موقع أو حساب خاص أو نظام معلوماتي مستخدما حقا مخولا له ، فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول[٢].

المادة ٢٩ : يعاقب بالسجن المشدد مدة لا تقل عن خمس سنين، كل من أنشأ أو استخدم موقعاً على شبكات الاتصالات أو شبكة المعلومات الدولية أو غيرها، بغرض الترويج للأفكار أو المعتقدات الداعية إلى ارتكاب أعمال إرهابية، أو لبث ما يهدف إلى تضليل السلطات الأمنية، أو التأثير على سير العدالة في شأن أية جريمة إرهابية، أو لتبادل الرسائل وإصدار التكليفات بين الجماعات الإرهابية أو المنتمين إليها، أو المعلومات المتعلقة بأعمال أو تحركات الإرهابيين أو الجماعات الإرهابية في الداخل والخارج. ويُعاقب بالسجن المشدد مدة لا تقل عن عشر سنين، كل من دخل بغير حق أو بطريقة غير مشروعة موقعاً إلكترونياً تابعاً لأية جهة حكومية، بقصد الحصول على البيانات أو المعلومات الموجودة عليها أو الاطلاع عليها أو تغييرها أو محوها أو إتلافها أو تزوير محتواها الموجود بها، وذلك كله بغرض ارتكاب جريمة من الجرائم المشار إليها بالفقرة الأولى من هذه المادة أو الإعداد لها[٣].

المادة ٤٦ : للنيابة العامة أو سلطة التحقيق المختصة، بحسب الأحوال، في جريمة إرهابية أن تأذن بأمر مسبب لمدة لا تزيد على ثلاثين يوماً، بمراقبة وتسجيل المحادثات والرسائل التي ترد على وسائل الاتصال السلكية واللاسلكية وغيرها من وسائل الاتصال الحديثة، وتسجيل وتصوير

(١) رئيس الجمهورية ، قانون مكافحة الارهاب رقم ٩٤ لسنة ٢٠١٥ ، منشورات قانونية ،٣ مارس ٢٠٢٠ متاح على الرابط : https://manshurat.org/node/14679.
(٢) رئيس الجمهورية ، مصدر سبق ذكرة ص ١٦.
(٣) رئيس الجمهورية ، مصدر سبق ذكرة ص ١٧.

ما يجري في الأماكن الخاصة أو عبر شبكات الاتصال أو المعلومات أو المواقع الإلكترونية وما يدون فيها، وضبط المكاتبات والرسائل العادية أو الإلكترونية والمطبوعات والطرود والبرقيات بجميع أنواعها. ويجوز تجديد الأمر المشار إليه في الفقرة الأولى من هذه المادة مدة أو مدداً أخرى مماثلة[١].

الخاتمة : تعد التهديدات السيبرانية وما تنتج عنها من الحروب الإلكترونية المهددة للأمن الدولي بصفه عامه والامن القومي بصفه خاصة ، وبعد التطور الكبير الذي يشهده النظام المعلوماتي والاتصالات التي جعلت هذه الصورة وحركة العولمة العالم عبارة عن قرية صغيرة ، وبالنظر ما تشكله هذه التهديدات من صعوبة وعرقلة في تطوير الدول وازدهارها بمحيطها الاقليمي فقد ادت الى تنامي الجهود الدولية وتكثيف العمل والتعاون والتنسيق في مجالات عديدة منها البرمجة والصناعات الإلكترونية التي من خلالها يمكن وضع استراتيجيات للتصدي لهذه المخاطر التي تهدد المجتمع والانظمة السياسية ،

اذ نستنتج منها ان كلما كانت التهديدات السيبرانية والهجمات الإلكترونية شديدة ومعقدة ومتشابكة كلما اثرت على امن الدول واستقرارها بمختلف المجالات ان كانت سياسية واقتصادية واجتماعية وعسكرية التي يتطلب من الدول مقاومة هذه الحروب والهجمات والتقليل من تداعياتها وتسخير كافة الطاقات والجهود المادية والتكنولوجيا واستخدام الوسائل الحديثة والمتطورة والطاقات البشرية التي تشمل الخبراء والتقنيين في مجالات البرمجة والحوسبة والحروب الهجينة بالغة التطور والتعقيد .

قائمة المصادر :

١ . فارس محمد عمدات و ابراهيم الحماحمه ، الامن السيبراني المفهوم والتحديات ، دار الخليج للنشر والتوزيع ، عمان ، الاردن ، العبدلي ،٢٠٢٢.

[١] رئيس الجمهورية مصدر سبق ذكرة ، ص ٢١.

٢ . راضية خماسمية ونور الهدى رويبع ، البعد الانساني للدبلوماسية الجزائرية ٢٠١١/٢٠١٧ ، جامعة العربي التبسي ، تبسة ، كلية الحقوق والعلوم السياسية ، رساله ماجستير غير منشورة ، ٢٠١٨ .

٣ . عبدالله دغش العجمي ، المشكلات العلمية والقانونية للجرائم الإلكترونية دراسة مقارنة ، جامعة الشرق الاوسط ، عمان ، رساله غير منشورة ، ٢٠١٤.

٤ . سعد بوه الشيخ محفوظ الحبيب ، ابعاد الامن السي براني ، الجيش والوطني الموريتاني ، الاثنين ١٣/٥/٢٠٢٤ ١٠:٢٥MP متاح على الرابط : https://armee.mr/node/3066

٥ . محمد ابو حمور ، الابعاد الاقتصادية للأمن السي براني ، الرأي ، ٣٠/٤/٢٠٢٤ ، ٤:٤٤ pm ، متاح على الرابط : https://alrai.com/article/10833703/

٦ . اسماء حمزة علي ، الامن السيبراني ومستقبل الصراع الدولي في القرن الحادي والعشرين (ايران واسرائيل) انموذجاً ،جامعة كركوك ، كلية القانون والعلوم السياسية ، رساله ماجستير غير منشورة ، ٢٠٢٢ .

٧ . صالح الامين الارباح ، الامن الغذائي ابعادة ومحدداته وسبل تحقيقه ، الهيئية القومية للبحث العلمي ، ١٩٩٦ .

٨ . ابراهيم حربي ابراهيم ، سياسة الامن الغذائي في العراق التحديات والحلول ، الجامعة التقنية الوسطى ، المعهد التكنولوجي ، بغداد , العدد ٢٧ ، ٢٠١٦.

٩ . اسلام فوزي ، الامن السيبراني والابعاد الاجتماعية والقانونية تحليل سوسيولوجي ، جامعة دمنهور ، مصر ، كلية الاداب ، قسم علم الاجتماع ، المجلة الاجتماعية القومية ، المجلد السادس والخمسون ، العدد الثاني ، ٢٠١٩.

١٠ . فرج يحيى زعاترة ، التهديدات السيبرانية على الامن القومي الامريكي ، العربي للنشر والتوزيع ،لبنان ، بيروت ، ٢٠٢٣ .

١١ . سلوى احمد ميدان و قحطان ياسين عطية ، الامن السيبراني واثرة على السيادة ، جامعه كركوك ، مجلة كلية القانون والعلوم السياسية ، المجلد ١٢ ، العدد ٤٤، الجزء ١ ، ٢٠٢٣.

١٢ . حسين باسم عبد الامير ، تحديات الامن السيبراني ، مركز الدراسات الاستراتيجية ، جامعة كربلاء ، ٢٠١٨ ، متاح على الرابط : /https://kerbalacss.uokerbala.edu.iq/wp/blog/2018/05/17

١٣ . صفاء حسين علي ، الحرب الاكترونية في المدرك الاستراتيجي الامريكي ، جامعة كركوك ، كلية القانون والعلوم السياسية ، دراسات دولية ، العدد ٨٢ .

١٤ . سمير باي ، التهديدات الامنية السيبرانية دراسة في انعكاسات الحرب الاكترونية على الامن القومي للدول واستراتيجية المقاومة ، جامعة الجزائر ، مجلة الدراسات والبحوث الانسانية ، مجلد ٨ ، العدد ٢، ٢٠٢٣ .

١٥ . دراسة برلمانية عن الجرائم الاكترونية ، اليوم السابع ، مصر ، الثلاثاء ٢٣/يوليو / ٢٠٢٤ / ٢:٣٠ ، متاح على الرابط. http://yaum7.com/story/20/9/11/5/4486999

١٦ . محمد صادق اسماعيل ، الجريمة الاكترونية في مصر واساليب مكافحتها ، المرجع الكتروني للمعلومات ، ٢٠٢٤/٢/٢٥ ، ٣:٣٠ mp، متاح على الرابط : https://mail.almerja.com/reading.php?idm=223857

١٧ . رغد البهي ، التجربة المصرية في مكافحة الارهاب السيبراني رؤية تحليلة ، مركز الاهرام للدراسات السياسية والاستراتيجية ،٢٠٢٣/١٢/٢٢، متاح على الرابط : .http://acpss.ahram.org.egl/News/2/074.aspx

١٨ . نجوان احمد عاصم عبد الجواد ، الجريمة السيبرانية وتاثيرها على الامن القومي المصري دراسة سوسيو تحليلة ، جامعة الفيوم ، مجله كلية الاداب ، مجلد ٥ ، عدد ١ ، ٢٠٢٣ .

١٩ . الضوي احمد ، استراتيجية الامن السيبراني المصري : حصن الوطن من الاحداث حروب العصر الحالي ، ببوابه الاهرام ، متاح على الرابط : https://gate.ahram.arg.eg/.

٢٠ . رئيس الجمهورية ، قانون رقم ١٧٥ لسنه ٢٠١٨ ، في شأن مكافحة جرائم تقنية المعلومات ، الجريدة الرسمية العدد ٣٢ مكرر ، (ج) في ١٤ اغسطس ٢٠١٨.

٢١ . رئيس الجمهورية ، قانون مكافحة الارهاب ، الجريدة الرسمية ، جمهورية مصر العربية ،العدد٣٣ في ١٥ اغسطس ٢٠١٥ ، الباب الاول الاحكام الموضوعة .

٢٢ . رئيس الجمهورية ، قانون مكافحة الارهاب رقم ٩٤ لسنة ٢٠١٥ ، منشورات قانونية ،٣ مارس ٢٠٢٠ متاح على الرابط : https://manshurat.org/node/14679.