الإصدار 16 // ابريل 2024
العدد الثالث
مجلة رسالة الحقوق ISSN-2032-2075

الضمانات القانونية الدولية للأمن السيبراني.

International legal safeguards for cyber security.

بحث مقدم من قبل
الدكتور أدريس عبد الله فيصل
دكتوراه في القانون العام
جامعة كربلاء / كلية العلوم الطبية التطبيقية

الخلاصة.
يشكل الامن السيبراني القاعدة الأساسية التي تعمل على ضمانتها وصيانتها جميع الدول على حد سواء حيث تسعى الى تامين المتطلبات الأساسية التي يتم من خلالها ضمان امنها بصورة مستمرة فضلا عن قيام الدول بتحديد الوسائل والتدابير والاليات التي تسهم في مواجهة التهديدات والاعتداءات والتحديات السيبرانية ، ولكون الامن السيبراني يمثل النطاق الذي يسعى الى تحقيقه المجتمع الدولي في العصر الحديث . ومما لا شك فيه ان العالم يشهد العديد من التحولات العميقة نتيجة النمو المتسارع في الشبكات الإلكترونية والتي ادت الى ظهور اشكال جديدة من العلاقات والنشاطات المختلفة وقد احدثت التكنولوجيا الحديثة للمعلومات والاتصالات ثورة شاملة في جميع نواحي الحياة الاقتصادية والاجتماعية والسياسية والثقافية وفي مقابل ذلك تزايدت المخاطر السيبرانية كلما تزايدت هيمنة تكنولوجيا الاتصالات والمعلومات على الحياه العامة فاصبحنا امام تحديات حقيقيه عن طريق شبكة الانترنت بمختلف اشكاله ، وعلى هذا الاساس تطور مفهوم الامن السيبراني في ظل تطور تكنولوجيا المعلومات حيث يمكن اعتبار تحديد الامن السيبراني اعلى تحديات الامن الوطني والدولي باعتبار التهديدات السيبرانية عابرة للحدود الوطنية مما يتطلب التعاون الدولي لمكافحه الهجمات السيبرانية وهذا يتأتى من خلال ابرام المعاهدات الدولية الإقليمية والعالمية فضلا عن تشريع القوانين الوطنية التي تواكب التشريعات الدولية للتصدي للاعتداءات السيبرانية وتؤمن الامن السيبراني الوطني والدولي . وقد تعرضنا في هذا البحث الى بيان التعريف بالأمن السيبراني بالمطلب الاول بينما تناولنا في المطلب الثاني التدابير القانونية للأمن السيبراني
الكلمات المفتاحية : الضمانات القانونية ، الدولية ، الامن السيبراني ، الهجمات السيبرانية ، الابعاد القانونية ، الامن السيبراني الوطني ، الامن السيبراني الدولي .

Abstract.
Cybersecurity constitutes the basic rule that all countries work to guarantee and maintain alike, as they seek to secure the basic requirements through which their security is continuously ensured, in addition to the countries defining the means, measures and mechanisms that contribute to confronting cyber threats, attacks and challenges, and because cyber security represents The scope that the international community seeks to achieve in the modern era.There is no doubt that the world is witnessing many profound transformations as a result of the rapid growth in electronic networks, which led to the emergence of new forms of relationships and various activities. Modern information and communication technology has brought about a comprehensive revolution in all aspects of economic, social, political and cultural life. The dominance of information and communication technology over public life has increased, so we are facing real challenges through the Internet in its various forms. On this basis, the concept of cyber security has evolved in light of the development of information technology. Defining cyber security can be considered the highest challenge to national and international security, given that cyber threats are transnational, which requires International cooperation to combat cyber-attacks, and this comes through the conclusion of international, regional and global treaties, as well as the enactment of national laws that keep pace with international legislation to address cyber-attacks and secure national and international cyber security.In this research, we have presented a definition of cybersecurity in the first requirement, while we have dealt in the second requirement with legal measures for cybersecurity.
Keywords: legal guarantees, international, cyber security, cyber-attacks, legal dimensions, national cyber security, international cyber security.

المقدمة .

اولاً / موضوع البحث .

ان التطور المتسارع في تكنولوجيا المعلومات والاتصالات ادى الى اعتماد دول العالم على شبكات الكمبيوتر والانترنت بالأبعاد الأمنية والسياسية والاقتصادية والاجتماعية والقانونية لكن هذا التطور لم يكن خاليا من المخاطر وذلك لإمكانية اختراق الشبكات المعلوماتية من قبل الدول الاخرى والجهات غير الحكومية والافراد والمجاميع الإرهابية بالاستفادة من ثغرات برامج شبكات الاتصال وصعوبة كشف الهوية ، مما يسبب اضرار بالبنى التحتية المعلوماتية والحيوية وقطع انظمه الاتصالات مثل تحطيم الطائرات وتعطيل شبكات الطاقة الكهربائية وغيرها من البنى التحتية التي تعتمد في عملها على شبكات الانترنت والاتصالات الإلكترونية ، وهذا يحصل عندما تتعرض هذه المنظومة المعلوماتية الإلكترونية للاعتداءات والتهديدات وبالتالي اصبح بإمكان اي فرد بقليل من الخبرات التقنية الحاق الاضرار بالفضاء السيبراني التابع لأي دولة فضلا عن امكانيه المهاجمين السيبرانيين من الهجوم على الشبكات المعلوماتية لأي دوله دون انذار مسبق والاضرار بالمنظومة الإلكترونية لتلك الدول بسرعة بالغة وعلى هذا الاساس تبنى المجتمع الدولي الاهتمام بإيجاد الاليات والتدابير والاطر القانونية على المستوى الوطني والدولي لتحقيق الامن السيبراني لمكافحة الهجمات السيبرانية ومن خلال التعاون الدولي في اطار المنظمات الدولية للتصدي للتهديدات السيبرانية كون هذه التهديدات السيبرانية عابرة للحدود الوطنية بوصفها جرائم دولية ، وهذا يتحقق من خلال برام الاتفاقيات الدولية والتشريعات الوطنية التي باتت الزاما وضرورة ان تواكب التطورات التكنولوجية المتسارعة .

ثانياً / اهميه البحث .

تبرز اهمية البحث من تزايد التهديدات والتحديات السيبرانية التي تواجه الامن السيبراني فضلا عن أن هذه الهجمات السيبرانية شغلت حيزا واسعاً من الاهتمام الوطني والدولي خصوصاً في ظل التطورات التكنولوجية المتسارعة في عالم الاتصالات الإلكترونية . وتكمن اهمية موضوع البحث في ندرة الابحاث والدراسات التي تناولت هذا الموضوع .

ثالثاً / اشكالية البحث.

ان التطورات التي أحدثتها وسائل الاتصالات الإلكترونية في مجمل الحياة الإنسانية ودخولها بشكل سريع في المجالات كافة مما جعلها سمه اساسية من سمات العصر الحديث ولا سيما في ظل تزايد مخاطر الاعتداءات والتهديدات السيبرانية حيث امتدت في معظم دول العالم ومنها العراق لتطال مختلف القطاعات السياسية والاقتصادية والعسكرية والأمنية والثقافية والاجتماعية مهددةً بذلك الامن الوطني والدولي بصورة عامة .

وعلى هذا الاساس يمكن طرح الإشكالية الأتية :

1. ما هو الامن السيبراني وما تأثيره على الامن الوطني والامن الدولي .
2. ما هي الابعاد القانونية للأمن السيبراني .
3. ما هي الاليات الدولية للأمن السيبراني ومكافحه الجرائم السيبرانية المعلوماتية
4. ما هي الابعاد القانونية في التشريع العراقي للأمن السيبراني ومكافحه الجرائم السيبرانية المعلوماتية .

رابعاً / فرضية البحث .

ان البحث في الضمانات القانونية الدولية للأمن السيبراني ينطلق من فرضية مفادها ان كلما تمكنت الدول من زياده مستوى الامن السيبراني كلما اسهم ذلك في حماية امنها الوطني وبالتالي الامن الدولي وكلما ارتفعت حجم الاعتداءات والهجمات السيبرانية كلما زادت تهديدات على الامن الوطني والامن الدولي .

خامساً / منهجية البحث.

ان طبيعة هذا البحث تستلزم الاستعانة بأكثر من منهج منها المنهج الوصفي والتحليلي لكون موضوع البحث من الموضوعات الحديثة مما يتطلب وصف وتحليل وتأثير الامن السيبراني على الامن الوطني والدولي.

سادساً / هيكلية البحث .

لغرض الإحاطةبموضوع البحث فقدتضمن مقدمةمع مطلبين وخاتمةوكلاتي:المطلب الاول:التعريف بالأمن السيبراني.

الفرع الاول : تعريف الامن السيبراني لغة واصطلاحا
الفرع الثاني : نطاق الامن السيبراني وجرائم المعلوماتية
المطلب الثاني : الاليات القانونية للأمن السيبراني
الفرع الاول : الاليات القانونية للأمن السيبراني في التشريع العراقي .
الفرع الثاني : الاليات القانونية الدولية للأمن السيبراني .
الخاتمة
اولاً : النتائج
ثانياً : المقترحات

المطلب الاول/ التعريف بالأمن السيبراني.

يعد الامن السيبراني في وقتنا الحاضر اهم عناصر الامن في الدول المتطورة ولا سيما في ظل التحول الكبير نحو السيبرانية في جوانب الحياة كافة وتكون فكرة الامن السيبراني على تحقيق البنية التحتية المعلوماتية والتي تشمل المنشآت الهامة ونظم المعلومات الهامة وخاصة نظم ادارة الحكومات الإلكترونية والتي تدار بها هيئات الدول الحيوية . وعلى هذا الاساس قامت العديد من الدول بإعداد المؤسسات التي تختص بحمايه الامن السيبراني واصبح الامن السيبراني جل اهتمام غالبية الدول المتحضرة وسخرت له كافة الامكانيات بحيث اصبح من معايير تطور وامكانياتها يتعلق بالجاهزية السبرانية لمواجهة التهديدات الإلكترونية . وجدير بالإشارة ان الاتحاد الدولي للاتصالات يقدم سنويا مؤشرا يتم ترتيب الدول حسب الجاهزية السيبرانية . ان شبكه المعلومات الإلكترونية اصبحت جزء لا يتجزأ من الحياة اليومية في المؤسسات الحكومية والأهلية وامتدت حتى للاستخدامات الشخصية التي تستخدم المعلومات الرقمية ومع زياده هذه المعلومات وتوسعها واصبحت حماية هذه المعلومات الإلكترونية ضرورية واكثر حيوية من خلال تأثيرها الفعال والمباشر على الامن الوطني والدولي في الوقت نفسه ، حيث ان التدابير المستمرة في حماية شبكات وبيانات الهيئات والافراد من الاستخدام غير المصرح به او اي اختراق يلحق الشبكة المعلوماتية يعد من اولويات حماية الامن الوطني . لقد اصبح من الضروري دراسة الامن السيبراني بالنظر للتطور التكنولوجي والرقمي الذي يعيشه العالم حيث لا يمكن باي حال ان نغفل هذا التسارع في التطور التكنولوجي ولكن في جانب اخر هذا التطور الرقمي يمكن ان يجعل اكثر الدول والشركات والمؤسسات مهددة بالاختراق والقرصنة الإلكترونية وهذا يجعل من اهم اسباب دراسة الامن السيبراني الذي يتولى حماية الأنظمة الإلكترونية وكافة الشبكات والبيانات الرقمية. وعموما فان الامن في الفضاء السيبراني يشمل مختلف اصول وقواعد وانظمة ضبط الاتصال وانتقال المعلومات وحفظها وتخزينها كما يضمن امن المواقع الإلكترونية وعمليات استثمارها فضلا من امن الاتصال وبالتالي فان الامن السيبراني يشمل جميع التدابير والاليات والاجراءات والتقنيات التي تستخدم لحماية سلامة وامن الشبكات والبرامج الإلكترونية من الهدم او العبث او الوصول غير المرخص والمصرح به كما يشمل حمايه البيانات والأجهزة المتعلقة بها . ولغرض التعرف اكثر على مفهوم الامن السيبراني سنقوم بتقسيم هذا المطلب الى فرعين سنخصص الفرع الاول الى تعريف الامن السيبراني لغة واصطلاحا بينما سيكون الفرع الثاني مخصص لبيان نطاق الامن السيبراني .

الفرع الاول/ تعريف الامن السيبراني لغةً واصطلاحاً.

لغرض التعرف على المقصود بالأمن السيبراني لابد من التعرف على هذا المصطلح من الناحية اللغوية والاصطلاحية وكالاتي

اولاً : الامن السيبراني من الناحية اللغوية .

ان كلمه الامن وردت في مصادر اللغة العربية بمعنى ضد الخوف بمعنى الطمأنينة اي أطمأن ولم يخف بمعنى امن[1] ، وقد ورد في هذا القران الكريم في مواضيع عديدة وهو ضد الخوف كقوله تعالى " الذي اطعمهم من جوع وامنهم من خوف "[2] ، وقوله تعالى " ادخلوها بسلام آمنين "[3] ، وكلمه " آمن " بمعنى أمناً وأماناً وامانة اي اطمئن ولم يخف خير امن البلد الذي أطمأن فيه اهله كما ورد في المعجم الوسيط[4] . اما يخص كلمه سايبر " cyber " فمن خلال المصادر اللغوية تبين بأن اصلها يوناني وتعود الى مصطلح " kybemeles " ويقصد بها القيادة او التحكم عن بعد[5] .وجدير بالذكر ان كلمة سايبر " cyber " وردت في قاموس المورد بمعنى علم الضبط ومصدرها " cybeme liec " اي ربط الاشياء عن بعد والسيطرة عليها[6] ، حيث ورد لفظها في قاموس المورد بمعنى تخيلي او افتراضي وجاء استخدامها لوصف الفضاء في الشبكات المحوسبة واشتقت صفة السيبراني منها " cybeme liec " ، وتعني علم التحكم الاوتوماتيكي او علم الضبط . لكن من الناحية الفنية التطبيقية يقصد بالسبراني ترابط حواسيب مع انظمة أوتوماتيكية والنظم السيبرانية المركزية . ان التعبير عن السيبرانية يمكن ملاحظته من خلال عالم اجهزه الكمبيوتر والانترنت ومن ثم فان تكنولوجيا المعلومات والاتصالات الإلكترونية والامر المفترض ممكن وعيه وليس لمسه اذن فهو مفهومي وليس مادي اي انه العالم الافتراضي الذي عرف حديثاً من خلال عالم الانترنت وفيه قامت المواقع الإلكترونية وهذه تقوم على اساس عالم قائم افتراضياً غير ملموس فعليا وهو يمثل العالم الالكتروني او السيبراني الذي نبتغيه بفضل الأجهزة في عالم الانترنت والكمبيوتر[7] .

ومما تقدم فالأمن هو نقيض الخوف او بمعنى السلامة والامن مصدر الفعل امنا واماننا وتعني زوال الخوف وكلمه سيبراني تعني تقنيه المعلومات والواقع الافتراضي وتعني الشخص الذي له القدرة على التحكم والسيطرة وبالتالي فان الامن السيبراني يعني جميع الاجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع اشكالها الإلكترونية والمادية من الهجمات ومختلف الجرائم والحوادث واعمال التخريب والتجسس .

ثانياً : الامن السيبراني من الناحية الاصطلاحية .

ان مفهوم الامن السيبراني مفهوماً واسعاً يتضمن جميع عمليات الدخول والخروج والبقاء والتصرف والتعرف في مكان ما ، ولذلك فأن في الفضاء السبراني يشمل مختلف قواعد واصول ضبط الاتصال هو انتقال المعلومات وحفظها وتخزينها ويتضمن امن المواقع والأنظمة الإلكترونية . فالأمن السيبراني وفق التعريف الوارد في التقرير الصادر عن الاتحاد الدولي للاتصالات بخصوص اتجاهات الاصطلاح في الاتصالات لعام " 2010 - 2011 " يمثل مجموعه من المهمات مثل تجميع وسائل وسياسات واجراءات امنية ومبادئ توجيهيه ومقاربات لإدارة المخاطر والتدريبات وممارسات فضلى وتقنيات يمكن

استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين[8] ويمكن تعريف الامن السيبراني بانه عبارة عن مجموعة من الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع استخدام غير المصرح به وسوء الاستخدام واستعادة المعلومات الإلكترونية ونظم المعلومات والاتصالات التي تتضمنها لضمان توافر واستمرارية نشاط نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية وذلك لاتخاذ الاجراءات اللازمة لحماية الافراد والمستخدمين من حوادث ومخاطر في الفضاء السيبراني . وعلى هذا الاساس فان الامن السيبراني يعد سلاح امني استراتيجي بيد الحكومات والافراد ولا سيما ان الحرب السيبرانيه اصبحت جزء لا يتجزأ من التقنيات الحديثة للنزاعات والتهديدات والهجمات بين الدول[9] وقد عرف الامن السبراني حسب الاعلان الاوروبي على انه قدرة النظام المعلوماتي على مقاومة محاولات الاختراق التي تستهدف البيانات الإلكترونية وجدير بالإشارة ان وزارة الدفاع الأمريكية اعطت تعريف لمصطلح الامن السيبراني على انه جميع الاجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع اشكالها المادية والإلكترونية من مختلف الجرائم والهجمات والتخريب والتجسس والحوادث وعرفه استاذ الاتصالات في جامعه كاليفورنيا " ريتشارد كمرر " على انه عبارة عن وسائل دفاعية من شانها ان تكشف وتحبط المحاولات التي يقوم بها القراصنة[10] ، وانطلاقاً من مهام الامن السيبراني يمكن تعريفه على انه النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات ويضمن امكانيه الحد من الاضرار والخسائر التي تترتب في حالة تحقق التهديدات والمخاطر ويسمح باعادة الوضع الى ما كان عليه بأسرع وقت ممكن تكون البيانات الواردة فيه محميه من اي دافع من التلف والاستخدام غير المرخص به[11] ، وعرف الامن السيبراني من الناحية الاصطلاحية العملية على انه فن ضمان وجود واستمرارية مجتمع المعلومات للامة وضمان حماية فضاء الانترنت والمعلومات المتعلقة به والبنى التحتية الحيوية .

كما عرف الامن السيبراني على انه مجموعة من الادوات والسياسات والمفاهيم الأمنية والضمانات الأمنية والمبادئ التوجيهية من المخاطر المحدقة بالمعلومات ومعالجتها والتدابير والتدريب من اجل افضل الممارسات والوسائل لحماية البيئة الإلكترونية ويمثل الامن السيبراني القدرة والإمكانية على الحماية والدفاع عن استخدام الفضاء الالكتروني من الهجمات السبرانية[12]

مما تقدم خلصنا الى ان الامن السيبراني يمثل مزيج من التحديات التقنية والسياسية والاجتماعية والثقافية علما بان صلاحية الامن السيبراني تعتمد على خلق قدرات وطنية لإدارة مخاطر حاسوب الالي والعمل على انشاء ثقافه وطنية للأمن السيبراني وعلى ردع التهديدات والجرائم والسيبرانية الإلكترونية فضلا عن العمل على تطوير استراتيجية وطنية للأمن السيبراني وحماية البنية التحتية للمعلومات الإلكترونية الحساسة .

ويمكن تعريف الامن السيبراني من الناحية القانونية على انه الضمانات التشريعية والقواعد والتدابير والاليات النظامية للحماية من مخاطر الجرائم الإلكترونية السيبرانية وهذا يتجسد من خلال وجود تشريعات لمكافحة التهديدات الإلكترونية السيبرانية التي تمس البيئة الإلكترونية للدولة مؤسسات وافراد .

الفرع الثاني/ نطاق الامن السيبراني .

تعد العلاقة بين القانون والتكنولوجيا الحديثة علاقة تبادلية فالتطورات التكنولوجية المتعاقبة والمختلفة تفترض مواكبة التشريعات القانونية لها من خلال انشاء أُطر تشريعية للأعمال القانونية وغير القانونية منها .

وجدير بالإشارة ان الجريمة السيبرانية عموما تفتقر حاليا للأطر القانونية الصارمة للتعامل معها ولعل هذا يرجع لأسباب عديده منها طبيعة الجريمة الإلكترونية ذاتها وصعوبة تحديد هوية مرتكب تلك الجرائم فضلا عن مرونة التعريفات المرتبطة بتكنولوجيا المعلومات الى جانب كون الجرائم السيبرانية غير مقيدة بحدود الدول اي عابرة للحدود الدولية الامر الذي يقتضي تفعيل التعاون الدولي المشترك لمكافحتها والتصدي لها[13]

ونستعرض ادناه النطاق الوطني والدولي للأمن السيبراني كالاتي :

اولاً : النطاق الوطني للأمن السيبراني.

تشكل المخاطر القانونية الشكل الرئيسي لغياب الاطارين التشريعي والتنظيمي للتعامل مع نتائج الاعمال القانونية وغير القانونية منها والتي تتم في الفضاء السيبراني حيث يتطلب النشاط الاجتماعي والاقتصادي وغيرها من الأنشطة تحديد واضحا للحقوق والالتزامات فالمستخدمين لهذه التقنيات مؤسسات حكومية وغير حكومية منظمات وافراد عبر الفضاء السيبراني بحاجة ضرورية الى اطار يكفل ويضمن حماية استخدامهم[14] فعند غياب الاطر القانونية والتشريعية تؤثر الجرائم الإلكترونية السيبرانية على عمليات معلوماتية تتعلق بحقوق الانسان الدولية وتدفع على العنف وتسبب ضرراً اقتصادياً خطيراً حيث ان ضمان ادارة مخاطر الامن السيبراني وفق منهج يهدف الى حماية الاصول المعلوماتية والتكنولوجية طبقا للسياسات والتدابير التنظيمية والمتطلبات والاطر والاليات القانونية . وعلى هذا الاساس فان المخاطر القانونية تتمثل في غياب الامن القانوني وتنازع الأنظمة القانونية وهذا يؤدي الى ارتفاع منسوب المخاطر ومع انعدام ملاحقة فاعلة تتناسب وطبيعة الاعمال والجرائم والتهديدات والاعتداءات السيبرانية العابرة للحدود ولأنظمه القانونية حتى تطال الى فرد في اي بقعة من الارض بما يطال الدول واستقرارها وامنها[15] ، حيث تعتبر المخاطر التي يتعرض لها الافراد والدول مخاطر هائلة وغير مقيدة بالأطر القانونية والتي قد لا تستوعب التقدم السيبراني والقدر الكافي وبالتالي فانه هنالك حاجة ضرورية وعاجلة الى الخطوات السريعة التي تقيم بها الدول القيادات السيبرانية وتوسع قدراتها وامكانياتها

العسكرية لتتضمن النزاع والتهديدات السيبرانية بحيث تتوازن مع القوانين والتشريعات الوطنية [16] وفي هذا الاطار يتطلب ان ترتقي القوانين الوطنية بحيث تتمكن في مكافحة الجرائم السيبرانية وتامين الامن السيبراني والحد من ظاهره القرصنة الإلكترونية عن طريق تشريع القوانين الصارمة لمواجهتها ضمن النطاق الوطني .

ثانياً : النطاق الدولي للأمن السيبراني.

بالنظر لطبيعة مجتمع الفضاء السيبراني العابر للحدود الدولية يقر قطاع تنميه الاتصالات بأهمية التعاون الدولي من اجل تعزيز المواقف الدولية في استخدام التكنولوجية المعلوماتية الحديثة وامن استخدامها . وعلى هذا الاساس يعترف قطاع تنمية تكنولوجيا الاتصالات بالحاجة الضرورية لدعم الدول لوضع وانشاء اليات محددة لتنفيذ متطلباتها الوطنية الخاصة بالأمن السيبراني من اجل افساح المجال امام تبادل افضل الممارسات في الاطار الدولي[17] وبالإمكان ان تصدر التهديدات في الهجمات السيبرانية من اي مكان مما يجعل هذه الهجمات دولية وتتطلب التعاون الدولي في تدابير التحقيق والاحكام الإجرائية والموضوعية لمعالجتها وفق اطار ملائم فضلاً عن ذلك من المعترف به بشكل واسع . ان التعاون الدولي يشكل احد المتطلبات الأساسية لتامين الامن السيبراني على المستوى الدولي . والجدير بالذكر انه خلال عامين 2003 و 2005 اتفقت الدول في القمة العالمية لمجتمع المعلومات " wsis " على ضرورة انشاء ادوات تتسم بالكفاءة والفعالية على المستوى الوطني والعالمي للارتقاء بالتعاون الدولي بخصوص الامن السيبراني[18] وعلى هذا الاساس يستلزم ان يكون التعاون وفق الاطار الدولي بدافع الرغبة المشتركة في السلام فضلاً عن المصلحة الفردية لكل دولة ، وجدير بالذكر ان المؤتمر الاقليمي للأمن السيبراني والذي اقره المركز العربي الاقليمي " ITU – ARCC " التابع للاتحاد الدولي للاتصال لتوحيد التعاون في المنطقة العربية وتعزيز دور الاتحاد الدولي للاتصالات بتأسيس الثقة والامن في ظل تقنية المعلومات والاتصالات في المنطقة العربية والشرق الاوسط وفي الاطار الاوربي اكدت الاتفاقية الاوربية لمكافحة الجريمة السيبرانية الى ابرام ما تعتبره اعمالا غير مشروعة تضمنت الجرائم ضد سرية الأنظمة والمعلومات وسلامتها فضلا عن الجرائم المتعلقة بالأجهزة الإلكترونية والجرائم المتعلقة بالمحتوى والجرائم المتعلقة بالملكية الفكرية[19] لقد اتجهت معظم الدول المتقدمة الى اقرار برامج واليات وتدابير وقائية ودفاعية ضد الهجمات السيبرانية بحيث خصصت بعض الدول ومنها الولايات المتحدة الأمريكية واستراليا وانكلترا [20] مبالغ هائلة لمعالجة قضايا الامن السيبراني ، وحقيقة الامر هذا يؤكد حرص هذه الدول على الاهتمام بقضية الامن السيبراني على المستوى الدولي فالعلاقات الدولية مهددة في اي وقت نتيجة التهديدات والاعتداءات والاختراقات على الشبكة المعلوماتية العالمية. والجدير بالإشارة الى ان الإدارة الأمريكية لم تتأخر في استحداث قيادة عسكرية دفاعية خاصة بأمن الفضاء السيبراني فقد اقترح الاتحاد الدولي للاتصالات عملية كاملة لإنشاء خطة وطنية للأمن السيبراني وتنفيذها " ICEGOV1 " وبالتالي فان هذه العملية تتطلب استراتيجية كاملة وشاملة تشمل استعراضا اولياً وواسعا لمدى تطابقها مع الممارسات الوطنية[21] وفي ظل التهديدات والمخاطر التي يتعرض لها الامن السيبراني على المستوى الدولي يمكن الاستناد على نتائج المبادرة الافريقية والتي ورد فيها على ان " ضرورة مساعدة الدول الاعضاء على وضع وتنفيذ سياسات واستراتيجيات ومعايير واليات لتحسين ام نظم وشبكات المعلومات وحماية البيانات والاشخاص وضمان الثقة الرقمية وحماية البنيه التحتية لتكنلوجيا المعلومات والاتصالات وبناء الثقة في استعمال تكنولوجيا المعلومات والاتصالات وتطبيقاتها "[22] ويتضح من المبادرة اعلاه مساعدة الدول الاعضاء على تقييم وتكييف الاطر التنظيمية والتشريعية على اساس الاستخدام الامثل للتقرير الصادر عن الاتحاد الدولي بشان " CGI " فضلاً عن التشجيع على وضع اساس عالمي للتعاون على المستوى الوطني والاقليمي لغرض ترسيخ ثقافة دولية عالمية للأمن السيبراني واعتماد تدابير واليات مؤسسية وتنظيمية لحماية الخصوصية والبيانات الشخصية فضلاً عن وضع استراتيجية لتحسين امن الشبكة المعلوماتية الإلكترونية ومكافحة التهديدات السيبرانية على الصعيد الوطني والدولي . ومن الأهمية بمكان القول ان برنامج الامن السبراني العالمي لعام 2007 يعد اطار للتعاون الدولي يسعى الى تعزيز الامن والثقة في مجتمع المعلومات ، حيث اكد هذا البرنامج على تحقيق عدة اهداف لعل من اهمها التدابير القانونية ، والتدابير الاجرائية والتقنية والهياكل التنظيمية ، بناء القدرات ، التعاون الدولي[23] مما تقدم فأن النطاق والاطار الدولي للأمن السيبراني يدعو الى مكافحة التهديدات السيبرانية وتحليل الاثار المترتبة على الجريمة السيبرانية والنزاع السيبراني فضلاً عن وضع اليات وطنية دولية لمواجهة تلك الاعتداءات على الامن السيبراني كونها عابر للحدود الدولية .

المطلب الثاني/ الاليات القانونية للأمن السيبراني.

ان وجود الخطر الارهابي والجرائم الإرهابية في العديد من مناطق العالم يتطلب وجود اليات قانونية لمكافحة هذه المخاطر على المستويات كافة الوطنية والدولية وان مكافحة الارهاب يواجه الصعوبات الكثيرة وهذا الامر بالنسبة للإرهاب التقليدي فكيف يكون الامر بالنسبة للفضاء السيبراني حيث الانتشار الواسع للجرائم الإلكترونية على الشبكة المعلوماتية من حيث سهولة ارتكاب الجرائم السيبرانية مما يدعو الى بدل المزيد من الجهود بمواجهة تلك التهديدات وعلى هذا الاساس لابد من تطبيق التدابير والاجراءات والوسائل في علاج الارهاب الالكتروني ولكي تكون المواجهة الأمنية للتهديدات السيبرانية مجديه وفعالة مما يتطلب ان تكون المواجهة قانونية مستندة على قواعد قانونية ولهذا حرصت الدول على تأمين قانون للمواجهة الأمنية القانونية للجرائم السيبرانية عبر الانضمام الى الاتفاقيات الدولية واصدار التشريعات الوطنية الخاصة بتدابير الامن السيبراني . وفي هذا الاطار سنتناول الاليات القانونية الوطنية للأمن السيبراني في التشريع العراقي في الفرع الاول بينما نتطرق الى الاليات القانونية الدولية للأمن السيبراني في الفرع الثاني .

الفرع الاول/ الاليات القانونية للأمن السيبراني في التشريع العراقي.

ان مكافحة الجرائم الإرهابية السبرانية يتم من خلال التدخل القانوني والتشريعي بتجريم ما تقوم به المجاميع والمنظمات الإرهابية بأعمالها التجسسية والجرمية والتخريبية كافة فضلا عن تشديد العقوبات على تلك الاعمال بمكافحة الارهاب السيبراني تشريعياً يتم بمواكبة التطور الحاصل في مجال الجرائم السيبرانية والمواجهة القانونية الكافية للتعامل مع هذه الجرائم ومن الضرورة بمكان ايجاد قواعد قانونية غير تقليدية للتصدي ومعالجة الجرائم السيبرانية[24] ومن خلال مراجعة موقف المشرع العراقي ومدى مواجهته ومكافحته للجرائم المعلوماتية السيبرانية لغرض مواكبة التطور الحاصل بخصوص الجرائم السيبرانية، نجد ان خلو الساحة العراقية الوطنية من قانون خاص بمكافحة الجرائم الإلكترونية السيبرانية وهذا جعلنا ندعو مجلس النواب الى الاسراع في تشريع هذا القانون لما له من حاجة ضرورية حالية في ظل تزايد الجرائم المعلوماتية السيبرانية [25] فضلا عن ان الجرائم السيبرانية تعد جرائم حديثة العهد ومتطورة في اسلوب ارتكابها وغير مألوفة في التشريعات العراقية وتحتاج الى توعية قانونية بمخاطر هذه الجرائم والتوعية الإعلامية ولا سيما بعد الاجتياح الهائل للثورة المعلوماتية وخطورتها وبالتالي من الضروري الاسراع بتشريع قانون مكافحة الجرائم المعلوماتية الإلكترونية السيبرانية شريطة عدم مساسه بالحقوق والحريات الشخصية ويكون متوافقا مع الدستور العراقي لعام 2005 وندرج ادناه اهم التشريعات الوطنية العراقية التي يمكن الرجوع اليها في ظل غياب قانون خاص بمكافحة الجرائم السيبرانية .

اولا : دستور جمهورية العراق لعام 2005 .

تناولنا في البداية الاحكام القانونية في دستور جمهورية العراق لعام 2005 بوصفه القانون الاعلى في العراق ويسمو على جميع القوانين ويكون ملزما في انحائه كافة وبدون استثناء ولا يجوز سن قانون يتعارض معه ويعد باطلا كل نص يحد في دساتير الاقاليم او اي نص قانوني اخر يتعارض معه[26] ، حيث يعد دستور جمهوريه العراق لعام 2005 من الدساتير التي نصت بشكل صريح على خطر الارهاب بصورة عامة حيث جاء بنص المادة " 7 " على انه " 1 - يحضر كل كيان او نهج يتبنى العنصرية او الارهاب او التكفير او التطهير الطائفي او يعرض او يهدد او يمجد او يروج له او يبرر له وبخاصه البعث الصدامي في العراق ورموز وتحت اي مسمى ولا يجوز ان يكون ذلك ضمن التعددية السياسية وينظم ذلك بقانون. 2 - تلتزم الدولة بمحاربة الارهاب بجميع اشكاله وتعمل على حماية اراضيها من ان تكون مقرا او ممر او ساحة لنشاطه "[27] وفي السياق نفسها نصت المادة " 3/21 " على انه " لا يمنح حق اللجوء السياسي الى المتهم بارتكاب جرائم دولية او ارهابية او كل من الحق ضررا بالعراق "[28] وجاء بالمادة " 73 " على انه " يتولى رئيس الجمهورية صلاحيات اصدار العفو بتوصية من رئيس مجلس الوزراء باستثناء ما يتعلق بالحق الخاص والمحكومين بأرتكاب الجرائم الدولية والارهاب والفساد المالي والاداري "[29] ومما تقدم نستشف ان دستور جمهورية العراق لعام 2005 النافذ قد اكد بشكل على مكافحة الجرائم الإرهابية بشكل عام والتي تتضمن في محتواها جميع الجرائم الإرهابية سواء كانت جرائم ارهابيه تقليدية او جرائم ارهابية الكترونية سيبرانية .

ثانياً : قانون العقوبات العراقي المرقم " 111 " لسنه 1969 المعدل .

يتضمن قانون العقوبات العراق المرقم "111 " لسنه 1969 المعدل القواعد القانونية العامة التي يتم الرجوع اليها في حالة عدم وجود قانون خاص والجدير بالإشارة الى ان هذا القانون يعد جرائم الاعتداء على وسائل الاتصالات السلكية واللاسلكية من الجرائم ذات الخطر العام التي تضر بالمصلحة العامة حيث نصت المادة " 361 " من هذا القانون على انه " يعاقب بالسجن مدة لا تزيد على سبع سنوات او بالحبس من عطل عمدا وسيلة من وسائل الاتصال السلكية او اللاسلكية المخصصة لمنفعة عامة او قطع او اتلف شيئاً من اسلاكها او اجهزتها او حال عمداً دون اصلاحها وتكون العقوبة السجن اذا ارتكبت الجريمة باستعمال مواد مفرقعة او متفجرة واذا ارتكبت في وقت حرب او فتنه او هياج "[30] وجدير بالذكر ان المادة " 403 " من قانون العقوبات العراقي رقم " 111 " لسنه 1969 المعدل قد اكدت على الحبس وبالغرامة لكل من صنع او استورد او اصدر او حاز او احرز او نقل بقصد الاستغلال او التوزيع كتابا او مطبوعات اذا كانت مخلة بالحياء او الآداب العامة لكن هذه المادة تم تعديلها بقرار مجلس قياده الثورة المنحل للمرقم " 266 " لسنه 2002 وهي الاكثر ملائمه للتكييف مع الواقع حيث جاء فيها على انه " يعاقب بالحبس مدة لا تقل عن ستة اشهر وبغرامة لا تقل عن " 500,000 " خمسمائة الف دينار ولا تزيد عن " 2000,000,00" مليوني دينار او بإحدى هاتين العقوبتين كل من صنع بقصد الاستغلال او التوزيع كتابا او مطبوعات او كتابات اخرى او رسوما او صور او افلاما او رموز او غير ذلك من الاشياء اذا كانت مخلة بالآداب العامة "[31] يتضح لنا مما سبق وطبقا لقانون العقوبات العراقي رقم "111 " لسنه 1969 بان المشرع العراقي قد عاقب على الافعال المضرة بالمصلحة العامة او الواقعة على الاشخاص او الاموال عمدا بصرف النظر عن الوسيلة التي تستخدم في ارتكابها ومن ثم فان استخدام الوسائل التكنولوجية الحديثة الإلكترونية في الجرائم الإرهابية والتزوير والتعدي على حقوق الملكية المعنوية والسب والقذف والابتزاز الالكتروني والاعمال المنافية للأخلاق والآداب العامة تمثل تهديدات سيبرانية عند استخدام الوسائل الإلكترونية وبالتالي شمولها بقانون العقوبات حسب نوع كل جريمة في حالة عدم وجود قانون خاص يجرمها وبالأحرى عند غياب قانون الجرائم المعلوماتية الإلكترونية .

ثالثاً : قانون مكافحة الارهاب العراقي المرقم " 13 " لسنة 2005 .

لقد شرع هذا القانون الخاص بالجرائم الإرهابية لتزايد العمليات الإرهابية وتهديد حياة المواطنين في العراق مما جعل الحاجة الضرورية لتشريعه وفق قانون خاص لمكافحه الارهاب والتصدي للجرائم الإرهابية التي تستخدم شتى الوسائل

التقليدية او الإلكترونية لتنفيذ جرائمها وقد عرف هذا القانون الارهاب في مادته الاولى على انه " كل فعل اجرامي يقوم به فرد او جماعة منظمة تستهدف فردا او مجموعة او افراد او جماعة او مؤسسات رسمية او غير رسمية او وقع الاضرار في الممتلكات العامة او الخاصة بغية الاخلال بالوضع الامني او الاستقرار والوحدة الوطنية او ادخال الرعب والخوف والفزع بين الناس واثارة الفوضى تحقيقاً لغايات ارهابية "[32] مما تقدم فان هذا القانون لم يشر بصورة صريحة الى الجرائم الإرهابية الإلكترونية لكن الاصل العام ان المنظمات الإرهابية تستخدم كافه الوسائل التكنولوجية في تنفيذ غاياتها الإجرامية والتي تهدد الامن والوحدة الوطنية بشتى الوسائل فهذا القانون يسري عليها . وجدير بالإشارة الى ان المادة " 4 " من قانون مكافحه الارهاب المرقم " 13 " لسنه 2005 قد اشارت الى ايقاع عقوبة الاعدام كل من ارتكب بصفته فاعلاً اصلياً او شريك عملاً من الاعمال الإرهابية ويعاقب المحرض والمخطط والممول وكل من مكن الارهابيين من القيام بالجرائم الواردة في هذا القانون بعقوبة الفاعل الاصلي ويعاقب بالسجن المؤبد من اخفا عن عمد اي عمل ارهابي او اوى شخص ارهابي بهدف التستر[33] ويتضح لنا من المادة اعلاه ان هذا القانون قد شدد العقوبة على الاعمال الإرهابية بصورة عامة قد تصل الى السجن المؤبد او الاعدام حسب خطورتها بغض النظر عن الوسائل المستخدمة لارتكابها سواء كانت وسائل تقليدية او الكترونية .

رابعاً : مشروع قانون مكافحة جرائم تقنية المعلومات لسنه 2018

ان قانون الجريمة المعلوماتية او الإلكترونية لم يرى النور لحد الان ولم يتم اقراره لكن لأهمية تشريع هذا القانون بعد مناقشته وتعديله اذا تطلب ذلك ومن ثم اصداره ونشره في جريدة الوقائع العراقية ومن خلال مرورنا على مشروع هذا القانون ولأهميته القانونية في الامن السيبراني ارتأينا ان نشير الى اهم ما ورد فيه من اجل الاحاطة بالتدابير الوطنية للأمن السيبراني سواء تم اقراره او لم يتم اقراره ، حيث ان ضرورة البحث تتطلب الاطلاع عليه ولعل اهم ما تضمنه مشروع هذا القانون .

1. يهدف هذا القانون الى توفير الحماية القانونية للاستخدام المشروع للأجهزة الإلكترونية والشبكة المعلوماتية وتحقيق الامن المعلوماتي وتوفير اقصى الدرجات الممكنة من الحماية لشبكات المعلومات واجهزه الكمبيوتر من التهديدات والاعتداءات وسوء الاستخدام والهجوم الالكتروني ومعاقبه مرتكبي الجرائم المعلوماتية وحفظ الاستخدام القانوني المشروع للحاسبات والشبكات المعلوماتية فضلا عن حماية المصلحة العامة والاخلاق والآداب العامة وحماية الاقتصاد الوطني[34] .

2. فيما يتعلق بالعقوبة المقترحة على مرتكب الجريمة السيبرانية فقد نصت عليها المادة " 2 / 2 " حيث جاء فيها " يسري هذا القانون على اي من الجرائم المنصوص عليها فيه اذا ارتكبت كليا او جزئيا داخل العراق او خارجه او امتد اثرها داخل العراق وسواء كان الفاعل اصليا او شريكا او محرضا على ان تكون تلك الجرائم معاقب عليها خارج العراق مع مراعاة المبادئ العامة الواردة في قانون العقوبات العراقي "[35] ، وقد نصت المادة " 34 / 1 " على انه " 1 - يعاقب بالسجن المؤبد وبغرامه لا تقل " 25000000 " خمسة وعشرون مليون دينار ولا تزيد عن " 50,000,000 " خمسون مليون دينار كل من استخدم عمدا اجهزة الحاسوب وشبكة المعلومات لارتكاب احد الافعال الأتية : أ - المساس باستقلال البلاد ووحدتها وسلامتها او مصالحها الاقتصادية والعسكرية والأمنية العليا . ب - الاشتراك او التفاوض او الترويج او التعاقد مع جهة معادية باي شكل من الاشكال بقصد زعزعة الامن والنظام العام وتعريض البلاد للخطر . ج - أتلف او اعيب او أعاق اجهزة او انظمة او برامج او شبكة المعلومات العائدة للجهات الأمنية او العسكرية او الاستخبارات بقصد المساس بأمن الدولة الداخلي او الخارجي او تعريضها للخطر. 2 - يعاقب بالعقوبة المنصوص عليها في البند / 1 من هذه المادة كل من استخدم عمدا اجهزة الحاسوب وبرامج وانظمة او شبكة المعلومات التابعة للجهات الأمنية او العسكرية او الاستخباراتية بقصد الاضرار بها او النسخ منها او بقصد ارسال محتواها لجهة معادية او الاستفادة منه لتنفيذ جرائم ضد امن الدولة الداخلي او الخارجي او تسهيل اخفاء معالم تلك الجرائم او تعطيلها "[36] ، لكن هذا المشروع لم يصدر لحد الان لوجود اختلافات على تشريعه بين الكتل السياسية في مجلس النواب ونأمل ان يتم اقراره وتشريعه بأسرع وقت ممكن بعد التصويت عليه بشكل نهائي لمواكبة التطورات التكنولوجية المتسارعة في العالم فضلا عن استخدامه في مكافحة الجرائم السيبرانية التي باتت منتشرة في العراق مما يتطلب ارساء تدابير قانونية للتصدي لهذه الجرائم الإلكترونية السيبرانية التي تهدد امن واستقرار المجتمع العراقي . مما سبق فقد تطرقنا لاهم التشريعات الوطنية العراقية التي تضمنت التدابير القانونية لمكافحة الجريمة السيبرانية والامن السيبراني سواء نصت على ذلك بصورة صريحة او ضمنية وبالتالي يبقى القصور التشريعي قائماً ما لم يتم تشريع قانون مكافحة الجرائم السبرانية والمعلوماتية .

الفرع الثاني/ الاليات القانونية الدولية للأمن السيبراني.

تعد الجرائم السيبرانية نوع جديد من انماط الجريمة وما يتميز به من خاصية عابرة للحدود الدولية وهذا أدى الى شروع المجتمع الدولي للتعاون من أجل مكافحة ومواجهة تلك الجرائم ، وعلى هذا الأساس سعت الدول لاتخاذ تدابير مشتركة لمواجهة هذا النوع من الجرائم المعلوماتية من خلال ابرام الاتفاقيات والمواثيق الدولية للتصدي لتلك الجرائم فضلاً عن العمل على مكافحتها سواء كانت اتفاقية اقليمية أو عالمية أو اتفاقيات ثنائية لتسليم المجرمين الذين يرتكبون الجرائم السيبرانية ويهددون الأمن الوطني والدولي وفي هذا الإطار سنتطرق الى اتفاقية جامعة الدول العربية للأمن السيبراني واتفاقية بودابست لمكافحة الجرائم السيبرانية .

اولاً :- الآليات القانونية للأمن السيبراني في الاتفاقية العربية

لقد تضمنت الاتفاقية العربية لمكافحة جرائم المعلوماتية التي تعد اساساً قانونياً للأمن السيبراني نصوص قانونية تناولت فيه التعاون القضائي والقانوني بين الدول العربية وجدير بالذكر أن هذه الاتفاقية وقعها مجلس وزراء الداخلية والعدل العربي في القاهرة بتاريخ " ٢١/ ١٢/ ٢٠١٠ " وجاءت تتويجاً للجهود الحثيثة التي تقوم بها جامعة الدول العربية لتدعيم وتعزيز الاجراءات والتدابير الأمنية للأمن السيبراني لمكافحة الجرائم المعلوماتية الالكترونية في ظل الاسس النظامية والبيئة القانونية[37] . والتزاماً من الدول العربية بضرورة الحاجة الى تبني سياسة جنائية مشتركة تهدف الى حماية المجتمع العربي ضد جرائم تقنية المعلومات وتطبيقاً للمبادئ الدينية والاخلاقية السامية ولاسيما احكام الشريعة الاسلامية وكذلك التراث الانساني للأمة العربية التي تستنكر كل اشكال الجرائم ومع مراعاة النظام العام لكل دولة فضلاً عن التزام الدول العربية بالمعاهدات والمواثيق العربية والدولية المتعلقة بحقوق الانسان ذات الصلة من ضمانها واحترامها وحمايتها[38] .

وقد صادقت جمهورية العراق على هذه الاتفاقية بموجب القانون المرقم "٣١" لسنة ٢٠١٣ والمنشور في جريدة الوقائع العراقية في العدد " ٤٢٩٢" في ٣٠ / ايلول / ٢٠١٣ [39] .

لقد اوردت هذه الاتفاقية بوصفها اتفاقية دولية ذات نطاق اقليمي عدد من المبادئ والاسس القانونية سنتناولها على النحو الآتي :-

1- المبادئ العامة المتعلقة بالتعاون الدولي

وهذه الاسس العامة تضمنت عدد من المبادئ ولعل من أهمها :

أ- مبدأ التعاون الدولي العربي الى اقصى حد ممكن وهذا نجده من خلال ما اوردته المادة "٣٢" حيث جاء فيها " أ – على جميع الدول الاطراف تبادل المساعدة فيما بينها بأقصى مدى ممكن لغاية التحقيق والاجراءات "[40] .

ونلاحظ من ذلك ان الاتفاقية تهدف الى تعزيز المساعدة والتعاون بين الدول العربية والحفاظ على امنها وسلامتها فمبدأ التعاون الدولي خاص بالدول العربية كنطاق اقليمي وهذا يشمل جميع قواعد التعاون الدولي الواردة في الاتفاقية

ب- مبدأ شمول التعاون على جرائم خارج اطار الاتفاقية هذا المبدأ يقضي بتوسيع نطاق الاتفاقية حيث شملت الجرائم التقليدية بالإضافة على الجرائم السيبرانية في مسائل التعاون بمعنى لجميع الادلة الالكترونية في الجرائم كافة وعلى هذا الاساس يمكن تفصيل نصوص الاتفاقية بصرف النظر اذا كانت الجريمة المرتكبة سرقة او قتل ومن ضمن ادلة الجريمة عنصراً سيبرانياً مثل الاتصالات الدولية تحتوي على تهديد او ابتزاز.

ج- مبدأ التعاون الفعال في القضايا الجنائية :

لقد نصت المادة " ٣١ / ٢" على ان " ان الجرائم المنصوصة في الفقرة "١" من هذه المادة تعتبر جرائم قابلة لتسليم المجرمين قائمة بين الدول الاطراف "[41] .

د- مبدأ كفاية الأدلة وازدواجية التجريم.

يتعلق هذا المبدأ في تسليم المجرمين شريطة ان تكون الجرائم المرتكبة يعاقب عليها قانون الدول الاطراف المعنية بسلب الحرية لفترة ادناه سنة او بعقوبة أشد فضلاً عن ابداء المساعدة المتبادلة حيثما يسمح للدولة الطرف المطلوب منها المساعدة المتبادلة شريطة ازدواجية التجريم[42] .

2- الاحكام القانونية للتعاون العربي الاقليمي.

في ظل اجراءات تسليم المجرمين فإن الاتفاقية تتيح لمكافحة الجرائم المعلوماتية الالتكرونية للدول الاطراف ان تستعمل هذه الاتفاقية اساساً قانونياً لقبول تسليم المجرمين وهذا ما اوردته المادة "٣١/ ١- أ" على انه " هذه المادة تنطبق على تبادل المجرمين بين الدول الاطراف على الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية بشرط ان تكون تلك الجرائم يعاقب عليها في قوانين الدول الاطراف ...." . وقد اوردت الفقرة "٣" من المادة ذاتها على انه " اذا قامت دولة طرف ما بجعل تسليم المجرمين مشروط بوجود معاهدة وقامت باستلام طلب لتسليم المجرمين من دولة طرف اخرى ليس لديها معاهدة تسليم فيمكن اعتبار هذه الاتفاقية كأساس قانوني لتسليم المجرمين فيما يتعلق بالجرائم المذكورة في الفقرة "١" من هذه المادة "[43] . ان المادة اعلاه قد نصت بشكل واضح وصريح عن اعتبار هذه الاتفاقية كأساي قانوني يعتمد به في حالة وجود معاهدة مشتركة لتسليم المجرمين بين الدول الاطراف او بين طرف وآخر.أما في مجال المساعدة المتبادلة فقد اكدت الاتفاقية في مادتها " ٣٢ / ١،٢" على انه " ١- على جميع الدول الاطراف تبادل المساعدة فيما بينها بأقصى مدى ممكن لغايات التحقيقات أو الاجراءات المتعلقة بجرائم معلومات وتقنية المعلومات أو لجميع الادلة الالكترونية في الجرائم

2- تلزم كل دولة طرف بتبني الاجراءات الضرورية من اجل تطبيق الالتزامات الواردة في المواد ٣٤ – ٤٢"[44] ، من الاتفاقية والتي تتعلق بالمساعدة المتبادلة حيث عدت هذه الاتفاقية أساس قانوني يعتمد عليه بين الدول الأطراف في تدابير تسليم المجرمين سواء في الجرائم التقليدية او السيبرانية فالمعنى ورد بشكل عام.ومما سبق فإن الاتفاقية العربية للأمن السيبراني والمتعلقة بمكافحة جرائم تقنية المعلومات اهتمت بعدد من الجرائم ومنها جريمة الدخول غير المشروع للأنظمة الالكترونية والاعتراض غير المشروع لبعض البيانات الالكترونية والاعتداء عليها واساءة استخدام وسائل تقنية المعلومات وجرائم التزوير والاحتيال الالكتروني والجرائم المتعلقة بانتهاك الحقوق الملكية الفكرية .وجدير بالذكر ان هذه الاتفاقية اكدت على ضرورة ان تلتزم كل دولة طرف وتتبنى في قانونها الوطني التشريعات والتدابير القانونية لمكافحة الجرائم المعلوماتية تحقيقاً للأمن السيبراني الوطني .

ثانياً :- اتفاقية بودابست للأمن السيبراني ومكافحة جرائم المعلوماتية لعام ٢٠٠١

بعد أن تطرقنا الى الاتفاقية العربية للأمن السيبراني لمكافحة جرائم المعلوماتية كاتفاقية اقليمية لحماية المواطن العربي بوصفه المتضرر من الجرائم المعلوماتية الالكترونية العابرة للحدود الوطنية الدولية سوف تستعرض اتفاقية بودابست الدولية للأمن السيبراني لمكافحة الجريمة الالكترونية . جدير بالذكر ان هذه الاتفاقية تم عقدها من قبل مجلس اوربا في مدينة بودابست بتاريخ " ٢٣/ ١١/ ٢٠٠١" ودخلت حيز النفاذ في ١/ ٧ / ٢٠٠٤ وتعد الصك الدولي الاول الذي اتجه لتجريم جميع اشكال الجرائم المعلوماتية الالكترونية[45] .

لقد تعددت الاسس القانونية المشتركة في اتفاقية بودابست لمكافحة الجرائم السيبرانية فضلاً عن انها تضمنت عدد من المبادئ والاحكام المتعلقة بالتعاون الدولي للتصدي للجرائم السيبرانية وعلى النحو الآتي :-

1- المبادئ العامة المتعلقة بالتعاون الدولي

تتضمن هذه الاسس أ - مبدأ التعاون الدولي الى أقصى حد ممكن حيث يفرض التزاماً على الاطراف بالتعاون الدولي على نطاق واسع فضلاً عن العمل على تذليل العقبات التي تعوق التدفق السريع للمعلومات والادلة الالكترونية[46] ، واكدت المادة "٢٣" من هذه الاتفاقية على توفير التعاون " على اوسع نطاق ممكن " مبدأ شمول التعاون على جرائم خارج نطاق الاتفاقية حيث تمنح هذه الاتفاقية اسس وقواعد قانونية وأحكام أوسع من نطاق الاتفاقية ذاتها . حيث تتضمن الجرائم كافة المرتبطة بنظم وبيانات الكترونية معلوماتية بمعنى تشمل جميع اشكال الجرائم السيبرانية الواردة في الاتفاقية فضلاً عن الجرائم التقليدية حيث ورد في نص المادة "٢٣" على انه " الاغراض اجراء التحقيقات والمتابعات التي تتعلق بالجرائم الجنائية ذات الصلة بنظم وبيانات الكمبيوتر أو من اجل جمع ادلة بشأن جريمة جنائية في شكل الكتروني "[47] . ج - وتتضمن الاسس العامة مبدأ التعاون الفعال في المسائل الجنائية وفقاً لهذا المبدأ تطبق الاتفاقية ولا تلغي الاتفاقيات الدولية ذات الصلة بالتعاون الدولي او تسليم المجرمين فضلاً عن تطبيق الترتيبات المتفق عليها على اساس التشريع الموحد أو المتبادل أو القوانين وأحكامها المتعلقة بالتعاون الدولي فمثلاً يمكن الاستناد الى الاتفاقية الاوربية المتعلقة بالمساعدة المتبادلة في المسائل الجنائية فضلاً عن الترتيبات التي تستند الى تشريعات موحدة او متبادلة كنظام التعاون الذي وضعته دول الشمال الاوربي[48] .

وجدير بالذكر ان الشروط الوارد ذكرها في القواعد القانونية للاتفاقات المتعلقة بالتعاون لا تبطل شروط الوثائق الدولية المتعلقة بالتعاون بالنص على ان التعاون في المادة "٣٢" يتم من خلال تطبيق الصكوك الدولية ذات الصلة والمتعلقة بالتعاون الدولي الفعال وبالترتيبات المتفق عليها بمقتضى التشريعات الموحدة ذات العلاقة بالتعامل بالمثل والتشريعات الوطنية[49] د- مبدأ كفاية الادلة وازدواجية التجريم هذا المبدأ يتطلب اعداد طلبات المساعدة والتعاون القانونية ووجود وتوافر أدلة اثبات كافية لتقديمها وهذه الادلة مستندة جزئياً في التشريعات القانونية الصادرة عن الدولة متلقية الطلب فضلاً عن ازدواجية التجريم الذي يقتفي ان يكون فعل الشخص مجرم في الدول التي تبتغي التعاون الدولي وهذا المبدأ اوردته المادة "٢٤" من الاتفاقية بالنص " ... شريطة ان يعاقب على هذه الجرائم بموجب قوانين كلا الطرفين المعنيين "[50] .

2- الاحكام القانونية للتعاون الدولي للأمن السيبراني هذه الاسس القانونية تتعلق بعدة مبادئ اساسية ولعل من اهمها أ– في اطار تسليم المجرمين وهذا نجده في المادة "٢٤" من اتفاقية بودابست التي تعد اساس قانوني للتعاون الدولي في مجال تسليم المجرمين حيث جاء فيها على انه " أ – تنطبق هذه المادة على تسليم المجرمين بين الدول الاطراف بالنسبة للجرائم المنصوص عليها في المواد "٢" الى "١١" من هذه الاتفاقية أو وجوب التسليم في حال ارتكاب الجرائم آنفة الذكر وفي كل اتفاق مبرم أو يمكن ان يجرم في المستقبل ج – طلب التسليم ممكن من دولة طرف في الاتفاقية صادر من دولة اخرى لا ترتبط معها بمعاهدة لتسليم المجرمين حيث يجوز لتلك الدولة الطرف اعتبار هذه الاتفاقية بمثابة الأساس القانوني لعملية التسليم "[51] . أوضحت هذه المادة اجراءات وآليات تسليم المجرمين سواء المجرمين للأجرام التقليدية أو الجرائم السيبرانية وبالإمكان الاستناد على هذه الاتفاقية بين اطرافها حتى في حالة وجود اتفاقية ثنائية لتسليم المجرمين بين طرف وآخر في هذه الاتفاقية . ب- في اطار المساعدة المتبادلة هذا المبدأ أوجد قواعد قانونية مشتركة للتعاون الدولي هي ذاتها المبادئ العامة ذات العلاقة بالتعاون الدولي وتفرض التعاون الدولي في اطار المساعدة المتبادلة[52] . وقد على المساعدة المتبادلة في هذه الاتفاقية بين أطرافها المادة "٢٥" حيث جاء فيها " توفر الدول الاعضاء المساعدة المتبادلة بعضها البعض على أوسع نطاق ممكن " [53] . وفي حالة تعذر وجود اتفاق دولي واجب التطبيق بشأن المساعدة المتبادلة على أساس وجود تشريع موحد متعلق بمبدأ المعاملة بالمثل بين اطرافه بينت الاتفاقية تعيين سلطة مركزية تكون مسؤولة على ارساء طلبات المساعدة والرد عليها.مما تقدم فإن اتفاقية بودابست الدولية للأمن السيبراني لمكافحة الجرائم المعلوماتية اوجدت العديد من الالتزامات على عاتق الدول الاطراف فيها ولاسيما فيما يتعلق بالتعاون الدولي لمكافحة الجرائم الالكترونية المعلوماتية ومن أهم تلك الالتزامات كما اشرنا سلفاً ادراج الالتزامات الدولية في التشريعات الوطنية والالتزامات بتسليم المجرمين وملاحقتهم بين الدول الاطراف باعتبار ان الجريمة السيبرانية جريمة عابرة للحدود فضلاً عن الالتزامات الدولية ذات الصلة بالتعاون الدولي ويمكن القول بأن اتفاقية بودابست للأمن السيبراني لعام ٢٠٠١ تتطلب اعادة النظر في احكامها لمضي فترة طويلة على تشريعاتها وظهور مستجدات جديدة في عالم الانترنت والتكنلوجيا مما يتطلب مواجهة تشريعية في النطاق الدولي العالمي لتكون هذه الاتفاقية مواكبة للتطورات الحاصلة في عالم الاتصالات وترتقي بمستوى خطورة الجرائم السيبراني ونرى بالإمكان الشروع بإبرام اتفاقية دولية عالمية متعددة الاطراف برعاية الامم المتحدة تتضمن الاطر الموضوعية والاجرائية وآليات واجراءات للتعاون الدولي للتصدي للجرائم السيبرانية.

الخاتمة.

من خلال ما تطرقنا له في البحث توصلنا الى جملة من النتائج والمقترحات نود الإشارة الى البعض منها :

اولاً / النتائج.

1- يعد الأمن السيبراني الالكتروني ذو أهمية كبيرة في حماية الأمن الوطني للدولة فهو يهدد أمن الدولة كلياً اذا ما تعرضت انظمتها المعلوماتية الالكترونية للاختراق وبالتالي يكلف الدولة الكثير من الخسائر الاقتصادية والاجتماعية والسياسية فضلاً عن الأمنية .

2- لوحظ عدم وجود تشريعات وطنية صريحة تتعلق بالأمن السيبراني وفي ظل القانون العراقي لا يوجد قانون خاص بالأمن السيبراني وجرائم المعلوماتية وهنالك اشارات ضمنية في بعض القوانين الوطنية.

3- لاحظنا وجود هيئات وطنية متخصصة في مسائل الأمن السيبراني تضطلع بمكافحة التهديدات السيبرانية والجرائم الالكترونية في البعض من دول العالم .

4- لوحظ استغلال المجاميع الارهابية التي ظهرت في عدد من دول العالم والعراق خصوصاً القضاء السيبراني والتكنلوجيا الحديثة من أجل تحقيق اهدافها في الدعاية والاعلان عن افكارها الارهابية المتطرفة فضلاً عن استغلال هذه الشبكة المعلوماتية في أعمال الابتزاز والقرصنة الالكترونية حيث تقوم المجاميع الارهابية بشأن هجماتها الإلكترونية المعلوماتية لانتهاك وتدمير المواقع والنظم المعلوماتية عن الحاق الضرر بالبنية التحتية المعلوماتية.

5- على المستوى الاقليمي والدولي فإن هنالك جهود دولية تسعى الى عقد اتفاقيات ومؤتمرات للحفاظ على الأمن السيبراني ومنها الاتفاقية العربية للأمن السيبراني ومكافحة الجرائم المعلوماتية لعام ٢٠١٠ واتفاقية بودابست للأمن السيبراني ومكافحة الجرائم المعلوماتية السيبرانية لعام ٢٠٠١ .

6- يتضح في اطار الأمن السيبراني بأن نطاقها الواسع يتضمن معاني ودلالات من بينها الحماية والمكافحة كما يقوم بترسيخ معايير قانونية واجتماعية من بينها مواجهة العنف والتمسك بالقيم والاخلاق ومواجهة الجريمة السيبرانية فضلاً عن تفعيل العقاب التشريعي في الحماية.

7- من الملاحظ ان التشريعات الدولية والدراسات الفقهية لم تتفق على تعريف موحد للجرائم السيبرانية حيث تغيير وتطور المفاهيم الخاصة لها طبقاً لتطور تكنلوجيا المعلوماتية الالكترونية مما يجعل المفاهيم القانونية تكتسب صفة عدم الوضوح وهذا يؤثر على قصور التشريعات في استيعاب الانشطة الاجرامية المعلوماتية .

8- بالرغم من كون الجرائم السيبرانية والأمن السيبراني يعد مفهوماً حديثاً وبتطور بسرعة فائقة وعند وجود الفراغ التشريعي يمكن الرجوع الى قرارات محكمة العدل الدولية مثل قرارها بشأن مشروعية التهديد بالأسلحة النووية أو استخدامها وقرارها في قضية الانشطة العسكرية وشبه العسكرية ضد نيكاراغوا وقضية الابادة الجماعية في يوغسلافيا فضلاً عن الاستناد الى قرار المحكمة الجنائية الدولية الخاصة بيوغسلافيا السابقة .

9- ان الصلة بين القانون والتكنلوجيا الحديثة المتطورة تعد علاقة متبادلة فالتطورات الالكترونية تفترض مواكبة التشريعات القانونية لها سواء على المستوى المحلي للدولة أو على المستوى الدولي وبالتالي فإن الانشطة السيبرانية تفتقد الى الاطر القانونية الصارمة للتعامل معها والتشريعات الدولية المعاصرة وان كانت تنطبق على الجهات السيبرانية لكنها لا تغطي كل اشكال وتهديدات الجرائم السيبرانية .

10- لاحظنا ان آليات وضع تنظيم شامل للأمن السيبراني والجرائم السيبرانية تتسم بصعوبات كثيرة لأن المصالح الدولية للقوى العظمى تعرقل ذلك كما حدث بالعقوبات التي واجهت المجتمع الدولي عند ابرام الاتفاقية المتعلقة بالأسلحة النووية والخلافات حول تقييدها أو حظر استخدامها كلياً.

ثانياً / المقترحات.

1- ترسيخ بنية تحتية الكترونية متطورة في مجال البرامجيات وتوفير المتطلبات كافة في اطار التعاون المعلوماتي بين هيئات الدولة للحفاظ على سرية البيانات والمعلومات للتصدي للهجمات والتهديدات السيبرانية .

2- ندعو الى تشريع قوانين للأمن السيبراني ومكافحة الجرائم السيبرانية وخاصة بالنسبة الدول التي تفتقر الى وجود تلك التشريعات ومنها العراق حيث ندعو الى الاسراع في تشريع قانون الأمن السيبراني ولمكافحة جرائم المعلوماتية لمواكبة التطورات المتسارعة الحاصلة في عالم الانترنت والاتصالات والتصدي للاستخدام غير المشروع لتلك التقنيات الالكترونية

3- ضرورة انشاء هيئة وطنية تعنى بالأمن السيبراني تأخذ على عاتقها مسؤولية تعزيز الامن السيبراني من مخاطر الفضاء السيبراني الالكتروني الذي يهدد الأمن الوطني للدول .

4- من الضروري الترويج لثقافة وطنية لتنمية الوعي للأمن السيبراني على الصعيد الشخصي والمجتمعي وفي المجالات كافة وخاصة الذين يستخدمون الشبكات الالكترونية المعلوماتية عليهم فهم قضايا الأمن السيبراني بأن يتخذوا التدابير اللازمة لحماية شبكاتهم وفق الاطر القانونية وحماية سرية المعلومات الشخصية من خلال قيام الدولة بتلك الإجراءات الضرورية .

5- من الضروري حجب المواقع الالكترونية المشبوهة التي تسعى الى نشر الافكار المتطرفة والكراهية والابتزاز وأعمال القرصنة الالكترونية والارهابية .

6- ندعو الى تفعيل التدابير الوقائية والاحترازية الذي يسبق وقوع الجرائم السيبرانية من خلال تعزيز دور الهيئات التوعوية وفي المستويات كافة لغرض التوعية بخطورة هذه الجرائم الالكترونية على الاسرة والمجتمع بصورة عامة .
7- ندعو المجتمع الدولي الى تكثيف التعاون الدولي الفعال من خلال ابرام اتفاقيات ثنائية واقليمية ودولية للأمن السيبراني ومكافحة الجرائم السيبرانية الالكترونية كون تلك الجرائم عابرة للحدود الوطنية فضلاً عن ابرام معاهدات تسليم المجرمين سواء فيما يتعلق بالجرائم التقليدية أو الالكترونية ولا سيما بين الدول التي لا توجد معاهدات بينهم تخص تسليم المجرمين المطلوبين للعدالة.
8- من الضروري جدا اعادة النظر بالاتفاقيات الدولية الاقليمية والدولية العالمية مثل الاتفاقية العربية للأمن السيبراني واتفاقية بودابست للأمن السيبراني والعمل على تعديلها وتحديثها وتضمينها جزاءات صارمة لتواكب التطورات المتسارعة في الجرائم السيبرانية .
9- ندعو الى ضرورة تطوير التشريعات القانونية العقابية الحالية بجانبها الموضوعي والاجرائي لمراعاة تطور الحاصل في المجال المعلوماتي والالكتروني السيبراني مع مراعاة ضرورة التوازن بين متطلبات الامن السيبراني وحقوق الانسان المشروعة .
10- من الضروري ان تكون هنالك مواءمة وتطابق وتنسيق بين التشريعات الوطنية والتشريعات الدولية في الاتفاقيات الدولية والإقليمية لتحقيق التعاون في مجال الامن السيبراني الوطني والدولي وبالتالي الحفاظ على الامن والسلم الدوليين.
11- من الضروري تنفيذ برامج شامله للأمن السيبراني من قبل الدول وتحديثها على اساس افضل للممارسات التكنولوجية الحديثة والمعايير الدولية فضلا عن استخدام الأجهزة الإلكترونية الحديثة لحمايه الخصوصية الشخصية.
12- ندعو الى التعاون الامني بين القطاعات الحكومية والقطاع الخاص ومعالجه المعوقات لإنشاء اطار تشريعي قانوني يرسخ هذا التعاون ويضمن التوازن بين مصلحه الدولة والقطاع الخاص وبما يراعي حقوق الانسان وحرياته الأساسية المشروعة وبما يحقق المصلحة العليا للدولة والامن الوطني.

الهوامش.

(1) محمد بن ابي بكر الرازي، مختار الصحاح دار الكتب العربية ، بيروت ، 1981 ص 26 2
(2) سورة قريش الآية / ٤
(3) سورة الحجر، الآية / ٤٦
(4) شعبان عبد المعطي عطية واخرون ، المعجم الوسيط ، ط٤ ، مكتب الشروق الدولية (مجمع اللغة العربية) ، القاهرة ، 2004 ، ص 28/
(5) د. احمد عبيس نعمه الفتلاوي ، الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية،العدد/٤/ المجلد/8 كلية القانون ،جامعة بابل ،2016 ، ص614.
(6) منير البعلبكي ، المورد قاموس انجليزي - عربي ، ط١ ، دار الملايين ، بيروت 2004، ص ٢٣٤
(7) محمود بري ، السيبرانية عالم القدرة على التواصل والتحكم والسيطرة ، ط ١ ، المركز الاسلامي للدراسات الاستراتيجية ، بيروت ،2019 ، ص 17- 18
(8) ابن مرزوق عنترة والكرم محمد ، البعد الالكتروني للسياسة الأمنية الجزائرية في مكافحة الارهاب ، حملة العلوم الإنسانية والاجتماعية ، العدد 38 / الجزائر، 2018، ص ٣٤
(9) منى الاشقرجبور،الامن السيبراني التحديات ومستلزمات المواجهة،بحث مقدم للمركزالعربي للبحوث القانونية و القضائية،جامعةالدول العربيةاللقاءالسنوي للمختصين في امن وسلامةالقضاء السيبراني ، بيروت٢٧–٢٨/آب/٢٠١٢،ص٣
(10) خالد حسن احمد لطفي ، الارهاب الالكتروني افة العصر الحديث والاليات القانونية للمواجهة ، ط ١ دار الفكر الجامعي ، الإسكندرية ، 2018، ص 174
(11) يوسف بو غزارة ، الامن السيبراني الاستراتيجية الجزائرية للأمن والدفاع في القضاء السيبراني ، مجلة الدراسات الافريقية وحوض النيل ، العدد / ٣ ، المجلد الاول ، المركز الديمقراطي العربي ، 2018 ، ص 107
(12) بارة سمير ، الدفاع الوطني والسياسات الوطنية للأمن السيبراني ، ط ٢ ، الملتقى الدولي حول سياسات الدفاع الوطني بين الالتزامات السياسية والتحديات الإقليمية ، كلية الحقوق والعلوم السياسية الجزائر ، 2017، ص 427
(13) حمزة صيوان عطيه الفتلاوي ، الامن السيبراني والحروب السيبرانية ، مجلة خيمة العراق ، وزاره الدفاع العراقية ، العدد / 357 السنة الثالثة / اذار/ ٢٠١٥ ، ص٢
(14) مجموعة باحثين ، دليل الامن السيبراني للبلدان النامية ، الاتحاد الدولي للاتصالات ، سويسرا ، 2006 ص 18
(15) منى الاشقر جبور ، مصدر سابق ، ص ٤
(16) حمدون توريه ، البحث عن السلام السيبراني ، الاتحاد الدولي للاتصالات ، فريق الرصد الدائم لامن المعلومات ، الاتحاد العالمي للعلماء ، صقليه 2011 ، ص٦
(17) المصدر نفسه / ص ٥

([18]) تقرير ITUالوثيقة RPM – ARB10 / 14 –A قطاع تنمية الاتصالات ، الاجتماع الاقليمي التحضيري للمؤتمر العالمي لتنمية الاتصالات ، ٢٠١٠ ، لمنطقة الدول العربية ، دمشق ، الجمهورية العربية السورية ، ٢٠١٠
([19]) القمة العالمية لمجتمع المعلومات ، برنامج عمل تونس بشان مجتمع المعلومات ، الفقرة / ٤٠ ، القمة العربية لمجتمع المعلومات ، 18 تشرين الثاني / 2005 منشور على الموقع الالكتروني WWW .it4 . int / WsiS / dOcs2 / tunis / off / Grev . html . تاريخ الزيارة ٢٠ / ٧ / ٢٠٢٣

([20]) convention – 23 XL – 2001
([21]) cyber security M. &A : Decoding Deals in the price water house cookipers , GlobaL Cyber secuity industry (Nov , 2011) p.76:
([22]) تقرير ITU , الوثيقة (RpM – ARB 10 / 14 – A ، 2010 مصدر سابق ، ص ٣
([23]) ٢٣ – تقرير ITU، ٢٠١٧ ، مصدر سابق ، ص ١٦٧
([24]) تقرير، ITU ٢٠١٠ ، مصدر سابق ، ص ١٠٢
([25]) محمود صالح العادلي ، الفراغ التشريعي في مجال مكافحة الجرائم الإلكترونية ، 2009 ، ص ٣ ، بحث منشور على شبكه الانترنت الدولية على الموقع htt p // www تاريخ الزيارة ٢٢ / ٧ / ٢٠٢٣
([26]) ينظر المادة / ١٣ من دستور جمهورية العراق لعام 2005
([27]) ينظر نص المادة (٧) من دستور جمهورية العراق لعام 2005
([28]) ينظر نص المادة (3/21) من دستور جمهورية العراق لعام 2005
([29]) ينظر نص المادة (73) من دستور جمهورية العراق العام 2005
([30]) ينظر نص المادة (361) من قانون العقوبات العراقي المرقم (111) لسنة 1969 المعدل
([31]) ينظر المادة (اولا) من قرار مجلس قياده الثورة المنحل رقم(266) لعام ٢٠٠٢ في جريدة الوقائع العراقية رقم 3963 في 2002/12/30
([32]) ينظر المادة / 1 من قانون مكافحة الارهاب العراقي رقم 13 لسنه 2005
([33]) ينظر نص المادة / 4 من قانون مكافحة الارهاب العراقي رقم 13 لسنه 2005
([34]) ينظر المادة (٢/ ١) من مشروع قانون جرائم المعلومات لسنة 2018
([35]) ينظر المادة (٢ / ٢) من مشروع قانون جرائم المعلومات لسنه 2018
([36]) ينظر المادة (34) من المشروع قانون جرائم المعلومات لسنه 2018
([37]) د . محمد حمد عمر الغباش الجرائم المعلوماتية عابرة الحدود(دراسة مقارنة) أطروحة الدكتوراه في كلية الحقوق / جامعة القاهرة ، 2013 ، ص 65
([38]) ينظر ديباجة الاتفاقية العربية لمكافحة الجرائم المعلوماتية لعام 2010
([39]) نصت المادة / ١ من القانون المرقم (31) لسنة 2013 المنشور في جريدة الوقائع العراقية العدد (4292) في 30 / ايلول / 2013 على انه (تصدق جمهورية العراق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الموقعة في القاهرة بتاريخ (٢١ / ١٢ / ٢٠١٠)
([40]) ينظر نص المادة (32) من الاتفاقية العربية لمكافحة جرائم المعلوماتية لسنه 2010
([41]) ينظر نص المادة (2/31) من الاتفاقية العربية لمكافحة جرائم المعلوماتية لسنه 2010
([42]) ينظر نص المادة (٣٢ / ٢) من الاتفاقية العربية لمكافحة جرائم المعلوماتية لسنة ٢٠١٠
([43]) ينظر نص المادة (3/31) من الاتفاقية العربية لمكافحة جرائم المعلوماتية لسنه 2010
([44]) ينظر نص المادة (32 / 2 ،1) من الاتفاقية العربية لمكافحة جرائم المعلوماتية لسنة ٢٠١٠
([45]) د . رامي حتومي القاهي مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية ، ط١ ، دار النهضة العربية، القاهرة ، 2011 ، ص 147
([46]) د . أيمن عبد الحفيظ ، حدود مشروعية دور اجهزة الشرطة في مواجهة الجرائم المعلوماتية ، مركز ابحاث الشرطة بأكاديمية مبارك ، العدد / ٢٥ / 2004 ص 389
([47]) ينظر نص المادة(23) من اتفاقية بودابست للأمن السيبراني
([48]) د . علاء الدين شحاته ، التعاون الدولي لمكافحة الجريمة ، الاترال للنشر والتوزيع ، القاهرة ، 2000 ، ص 31
([49]) ينظر المادة (32) من اتفاقية بودابست للأمن السيبراني لعام 2001
([50]) ينظر المادة (24) من اتفاقية بودابست للأمن السيبراني لعام 2001
([51]) ينظر الفقرات (1 ، 2 ، 3) من المادة (24) من اتفاقية بودابست للأمن السيبراني
([52]) ينظر التقرير التشريعي لاتفاقية الجريمة السيبرانية
([53]) ينظر نص المادة (25) من اتفاقية بودابست للأمن السيبراني

المصادر.
القران الكريم.
اولا / الكتب .
1- شعبان عبد المعطي عطيه واخرون ، المعجم الوسيط ، ط ٤ ، مكتب الشروق الدولية ، القاهرة ، 2004
2- منير البعلبكي ، المورد قاموس انجليزي - عربي ، ط ١ ، دار الملايين ، بيروت ، 2004
3- محمود بري، السيبرانية عالم القدرةعلى التواصل والتحكم والسيطرة،ط١،المركزالاسلامي للدراسات الاستراتيجية، بيروت2019
4- خالد حسن احمد لطفي ، الارهاب الالكتروني ، افة العصر الحديث والاليات القانونية للمواجهة ، ط ١ ، دار الفكر الجامعي ، الإسكندرية ، 2018
5- مجموعة باحثين ، دليل الامن السيبراني للبلدان النامية ، الاتحاد الدولي للاتصالات سويسرا ، 2006
6- حمدون توريه ، البحث عن السلام السيبراني ، الاتحاد الدولي للاتصالات ، فريق الرصد الدائم لأمن المعلومات ، الاتحاد العالمي للعلماء ، صقليه ، ٢٠١١
7- د. رامي متولي القاضي ، مكافحه الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات 2011 والمواثيق الدولية ، ط ١ ، دار النهضة العربية القاهرة
8- علاء الدين شحاته ، التعاون الدولي لمكافحه الجريمة ، ايتراك للنشر والتوزيع ، القاهرة ، 2000
9- د . هلالي عبد الله احمد ، جرائم المعلوماتية العابرة للحدود ، دار النهضة العربية ، القاهرة 2007
ثانيا / الأطاريح والرسائل والمؤتمرات والمجلات.
1- محمد حمد عمر الغياش،الجرائم المعلوماتيةعابره الحدود"دراسة مقارنه" اطروحة دكتوراه في كلية الحقوق،جامعة القاهرة2013
2- د. احمد عبيس نعمة الفتلاوي ، الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية ، العدد / ٤ / المجلد / ٨/ كلية القانون جامعه بابل 2016
3- ابن مرزوق عنترة والكرم محمد ، البعد الالكتروني للسياسة الأمنية الجزائرية في مكافحه الارهاب ، مجلة العلوم الإنسانية والاجتماعية ، العدد/ 38 الجزائر ، 2018
4- منى الاشقر جبور ، الامن السيبراني التحديات ومستلزمات المواجهة ، بحث مقدم للمركز العربي للبحوث القانونية والقضائية ، جامعة الدول العربية ، اللقاء السنوي للمختصين في امن وسلامه القضاء السيبراني ، بيروت ، آب / 2012
5- يوسف بوغزارة ، الامن السيبراني الاستراتيجية الجزائرية للأمن والدفاع في القضاء السيبراني ، مجلة الدراسات الأفريقية وحوض النيل ، العدد / ٣ ، المجلد الاول ، المركز الديمقراطي العربي ، 2018
6- باره سمير الدفاع الوطني والسياسات الوطنية للأمن السيبراني ، ط ٢ ، الملتقى الدولي حول سياسات الدفاع الوطني بين الالتزامات السيادية والتحديات الإقليمية ، كلية الحقوق والعلوم السياسية ، الجزائر ، 2017
7- حمزة صيوان عطيه الفتلاوي ، الامن السيبراني والحروب السيبرانية ، مجلة خيمه العراق ، وزارة الدفاع العراقية ، العدد / 357 ، السنة / ٣ / اذار ، 2015
8- قطاع تنمية الاتصالات الاجتماع الاقليم التحضيري للمؤتمر العالمي لتنمية الاتصالات لمنطقة الدول العربية دمشق ، 2010
9- د. ايمن عبد الحفيظ ، حدود مشروعية دور اجهزة الشرطة في مواجهة الجرائم المعلوماتية ، مركز ابحاث الشرطة بأكاديمية مبارك ، العدد / 25/ ٢٠٠٤
ثالثاً / المصادر الاجنبية.
1 - Cuber security M&A : Decoding Deals the pricewater house coopers , Global cyber security industry , 2011
2 - Convention on cybercrime – Budupest . 23 XL – 2001
رابعاً / المصادر الالكترونية.
1- محمود صالح العادلي ، الفراغ التشريعي في مجال مكافحة الجرائم الالكترونية ، ٢٠٠٩ ، ص٣ ، بحث منشور على شبكة الانترنيت الدوليةcom . Shaimeatalla . http // www
2- القمه العالمية لمجتمع المعلومات ، برنامج عمل تونس بشان المجتمع المعلومات ، الفقرة / 40 / القمة العربية لمجتمع المعلومات ، 18 / تشرين الثاني / 2005
3- منشور على الموقع الالكتروني
4- WWW .itu .int / wsis / does2 / tunis / off/ Grev .html.
خامساً / القوانين والتشريعات الوطنية .
1- دستور جمهورية العراق لعام 2005
2- قانون العقوبات العراقي رقم "111 " لسنة 1969 المعدل
3- قرار مجلس قيادة الثورة المنحل رقم " 266" لعام 2002
4- 2002 قانون مكافحة الارهاب العراقي رقم " 13 " لسنة 2005
5- مشروع قانون جرائم المعلوماتية العراقي لعام 2018
6- القانون المرقم "31 " لسنة 2013 قانون مصادقة جمهورية العراق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات .
سادساً / الاتفاقيات والتقارير الدولية.
1. تقرير ITU . الوثيقة RPM – ARB10 / 14 , 2010
2. الاتفاقية العربية للأمن السيبراني ومكافحه جرائم المعلوماتية لعام 2010
3. اتفاقية بودابست الدولية للأمن السيبراني ومكافحة الجرائم المعلوماتية لعام ٢٠١٠