# رسم السياسة العامة للدولة العراقية في الأمن و الردع السيبراني: دراسة في دستور ٢٠٠٥

Drawing up the general policy of the Iraqi state in security and cyber deterrence


ا.م.د سنان طالب شهيد

تدريسي كلية القانون
جامعة الكوفة
البريد الالكتروني:
٠٧٧٢٥٩٨٧٧٢١



الكلمات الافتتاحية :
رسم السياسة ,العامة للدولة العراقية , الأمن , الردع السيبراني
**Keywords :**
Drawing , general policy , Iraqi state , security , cyber deterrence



Abstract: Security is one of the most important pillars of living in society. Life cannot be imagined without it, and the meaning of security is not limited; Not only legal, psychological and intellectual security, but also extends to technical security. In recent years, humanity has witnessed the emergence of a new dawn. It is the dawn of the "information society", which was called cyberspace, and this space has become, with the passage of time, one of the most important requirements of humanity. As it was the result of cyberspace; The emergence of many changes in the activity of the government and individuals, so e-governments appeared, distance education, e-commerce, and other emerging activities that relied directly on the Internet, computers, smart tablets, and others. In the midst of these changes, the term "cybersecurity" appeared as a wall and a method of defense for cyberspace, as serious problems arose as a result of relying on cyberspace. information space is at risk..


## المقدمة

**يعد الأمن من أهم ركائز العيش في المجتمع؛ فلا يمكن تصور قيام الحياة بدونه، ولا يقتصر مدلول الأمن؛ على الأمن القانوني، و الأمن النفسي و الفكري فقط، بل يمتد ليشمل الأمن التقني، فلقد شهدت البشرية في السنوات الأخيرة بزوغ لفجر جديد؛ وهو فجر "المجتمع المعلوماتي" الذي أطلق علية إسم الفضاء الإلكتروني، هذا الفضاء الذي أضحى مع مرور**

الوقت من أهم متطلبات الإنسانية. كما كان من نتيجة الفضاء الإلكتروني: ظهور العديد من التغييرات على نشاط الحكومة والأفراد، فظهرت الحكومات الإلكترونية، التعليم عن بعد، التجارة الإلكترونية، وغيرها من أنشطة مستجدة اعتمدت بصورة مباشرة على الإنترنت و الحواسيب و الاجهزة الذكية اللوحية و غيرها. وفي خضم تلك التغيرات ظهر مصطلح "الأمن السيبراني"، كحائط صد وطريقة دفاع عن الفضاء السيبراني، إذ قد ظهرت مشكلات خطيرة نتيجة الاعتماد على الفضاء الإلكتروني لم تقف تلك المشكلات عند حد الأفراد والإساءة إليهم، بل تعدت ذلك إلى محاولة و اقتحام مواقع الحكومات الإلكترونية وتعريض "الفضاء المعلوماتي" العائد لها للخطر. إذ أصبح الأمن المعلوماتي في وقتنا الحالي في الدولة؛ قوة لابد من امتلاكها, وأنّ مستوى حماية النظام المعلوماتي فيها متوقف على قوة أمنها السيبراني أو ضعفهُ, إذّ من خلاله يمكن التصدي لأي هجوم إلكتروني أو تجسس إلكتروني على منظومة الدولة و مواطنيها؛ من هنا نتبين إن الحاجة إلى الأمن المعلوماتي و ضمان الردع السيبراني؛ لا تقل عن الحاجة إلى الفضاء الإلكتروني نفسه، فتحقيق الثقة في الفضاء الإلكتروني يعد من أهم أساسيات تسخير تقنيات المعلومات والاتصالات، ولو نظرنا إلى تشابك الفضاء المعلوماتي من شبكات تواصل اجتماعي وسرعة تداول المعلومات وسرعة الوصول للمعلومات – سواء معلومات اقتصادية أو عسكرية – بين الدول والأفراد والشركات؛ سيظهر لنا بجلاء خصوصية منازعات الفضاء المعلوماتي والحاجة لضمان الأمن المعلوماتي. ولقد أثبت لنا الواقع العملي للدول أنها تتسابق فيما بينها من أجل حماية فضائها المعلوماتي من هجمات الآخرين، و ذلك لما ينتج عن هذه الهجمات من اختراق المعلومات الاقتصادية التي يترتب على إفشائها إنهيار الاقتصاد القومي. ومن المعروف أن الدساتير تتميز بقالب جامد فهي لا تقبل التغيير بسهولة، ومعظم دساتير الدول العربية تم وضعها في نهايات القرن الماضي أو مع بدايات القرن الحالي، وفي هذا الوقت لم يكن موضوع الأمن السيبراني قد أخذ مكانته في الفكر القانوني أو لفت أنتباه المشرعين في تلك الدول، فصدرت معظم الدساتير ولم تعر هذا الموضوع القدر الكافي من الاهتمام، فهي وإن تحدثت عن حقوق الإنسان الرقمية أو حرية الاتصالات الإلكترونية؛ إلا أنها قواعد لا تكفي لحماية هذا النوع من الأمن. فعلى الرغم من المخاطر التي تتمثل في الهجمات الإلكترونية، فإن البنية الدستورية والقانونية غير مكتملة ولا تزال المسؤولية المدنية الناجمة عن مثل هذه الهجمات غير واضحة وتثير قضايا قانونية معقدة، خاصة بسبب تنوع عمليات إعادة تنظيم المسؤولية القابلة للتطبيق، وبالتالي قد يكون هناك ما يبرر اتخاذ إجراء تشريعي بشأن هذه المسألة في وقت ما في المستقبل. أولا-أهمية البحث : تكمن أهمية الدراسة في أنها محاولة لوضع إطار قاعدي لمفهوم الردع السيبراني من الناحية الدستورية؛ على اعتبار أنّ الأمن السيبراني من خلال الردع، يعد أحد صور حقوق الإنسان الحديثة، فضلا عن معرفة الوضع القائم في العراق، فتظهر اهمية الدراسة متى علمنا أنها محالة لتحدي الأمن المعلوماتي كفكرة أساسية مرتبطة بقيام الدولة العراقية، ومحاولة إعطاء وصف قانوني لمبدأ سياسي هام وخصوصًا في ظل أنتشاره في الآونة الأخيرة. ومن الضروري دراسة الموضوع من الوجهة الدستورية و

ذلك من أجل الكشف عن مواطن القوة والضعف التي تعتري هذه المسألة، فعدم توافر الأمن المعلوماتي يترتب عليه أضرار خطيرة؛ وذلك لما للأمن السيبراني من أثر بالغ على الحقوق والحريات العامة. والأطر القانونية والسياسية والاقتصادية والاجتماعية للدولة وللأفراد والمؤسسات على حد سواء، ولا يمكن بناء دولة قوية حصينة؛ إلا بتوفير الأمن الذي يضمن حمايتها من التحديات الإلكترونية كافة، لضمان الردع الإلكتروني المنشود.

ثانيا-نطاق الدراسة: يتحدد نطاق هذه الدراسة بموضوع الأطر الدستورية المعتمدة في رسم السياسة العامة للدولة العراقية لتحقيق الأمن السيبراني، وهو ما يستوجب تناول هذا الموضوع من منظور الدستور وكيفية التعامل مع متطلبات هذا الأمن المهم من خلال ما جاء في الدستور العراقي والتشريعات المنظمة لتكنولوجيا المعلومات. و موضوع الدارسة يتحدد في تفحص الوضع القائم في العراق بالنسبة لقضية الأمن السيبراني من خلال ما جاء به الدستور العراقي وما جاءت به التشريعات المنظمة للتقنيات الإلكترونية محاولة استخلاص إطار قاعدي لفكرة الردع السيبراني، فمما لاشك فيه أن قضية هذا الأمن تعد من حقوق الإنسان، وصفة تتمتع بها النظم السياسية والقانونية في الدول المتقدمة، كما و إنه يعد أحد مرتكزات بناء الدولة القوية.

ثالثا-إشكالية الدراسة: تظل قضية الأمن السيبراني أحد المحددات الرئيسية في صياغة وتشكيل النظم القانونية وخاصة في بعديها السياسي و الاجتماعي، وهي معيار تقاس به درجة تقدم الأمم؛ ورقيها ومقدرتها على تحقيق أهدافها ووجودها ومكانتها الدولية، فمصطلح أمن السايبر ليس شكل من أشكال ترف القانوني بل هو مضمون مفاهيمي، ومن أهم هذه المضامين الإطار الدستوري والقانوني له.

تساؤلا الدراسة/ سيقوم الباحث من خلال هذه الدارسة الإجابة على تساؤلات تتمثل فيما يلي:

السؤال الرئيسي: إلى أي مدى توفر نصوص الدستور العراقي البنية أو الإطار القاعدي لرسم سياسة عامة لتحقيق ولحماية الأمن و تهيئة الردع الفعال في مجال الفضاء المعلوماتي، بالشكل الذي يمتنع فيه بصورة أو بأخرى من اللجوء إلى قواعد أخرى؟

الأسئلة الفرعية : ومن هذا التساؤل الرئيس تنبع تساؤلات عدة فرعية :

١- ما هو مدلول كلمة الأمن و الردع السيبراني و الهجمات السيبرانية ؟.
٢- هل يتوافر في الدستور العراقي أساس قاعدي لحماية الأمن السيبراني لتحقيق الردع؟.
٣- ما هي الاستراتيجية العراقية لرسم السياسة العامة للأمن و الردع السيبراني؟.
٤- من هو المختص برسم السياسات العامة لمواجهة حالات الهجمات السيبرانية و تحقيق الردع ؟.
٥- ماهي المراحل التي وصلت لها هكذا سياسات إنْ كانت موجودة فعلا، و ما تم تنفيذه منها و كيف تمت ترجمته على أرض الواقع؟.

رابعا-منهج الدراسة:

يعتمد الباحث في أطروحته على المنهج التحليلي والمنهج الاستنباطي :

المنهج التحليلي: حيث نتعرض لتحليل نصوص الدستور العراقي المرتبطة بقضية الأمن السيبراني، وطبيعة العلاقة بينها وبين القوانين والاتفاقيات الدولية ومن ثم تحليلها وإبداء الرأي المناسب بشأنها.

المنهج الاستنباطي: والذى يعتمد على محاولة استنباط الحلول من الفقه و القضاء وذلك بعد تحليل أحكام القضاء وأراء الفقهاء

سادسا-هيكلية الدراسة:

المبحث الأول: التعريف بالأمن و الردع السيبرانيين و تمييزهما عما يشتبه معهما من مصطلحات.

المطلب الأول/ التعريف بالأمن و الردع السيبرانيين.

المطلب الثاني/ تمييز الردع السيبراني عن ما يشتبه به:

المبحث الثاني/مجالات الردع السيبراني و الاساس الدستوري لتحقيقه في العراق

المطلب الأول/ مجالات الردع السيبراني

المطلب الثاني/ الأساس الدستوري لتحقيق الردع السيبراني في العراق و مدى كفايته

المبحث الثالث/ السلطة المختصة برسم سياسة الأمن و وضع استراتيجية تحقيق الردع السيبراني في العراق

المبحث الأول :التعريف بالأمن و الردع السيبرانيين و ما يشتبه معهما من مصطلحات:

يشهد العصر الحالي ثورة معلوماتية: قدمت للبشرية الكثير من الايجابيات بل غيَّرت الطريقة التي تسير بها الدولة في اعمالها, إذ أثرت في اعمال المؤسسات الحكومية وتركيب المجتمع، إلا أنّ مع هذه الإيجابيات تترافق مخاطر أمنية حقيقية، تمثلت بما خلفته من إساءات في استخدامها من قبل بعض الهواة والمجرمين الذين ساهموا في عولمة الجريمة في الفضاء (المعلوماتي) السيبراني، ومن ثم ولدت هذه الثورة المعلوماتية، تهديدات ظهرت لها صور وأنماط عدة، والتي يعد من أخطرها الهجمات السيبرانية و أفعال التجسس الالكتروني، إذ يُعدان من الأساليب والوسائل الخطيرة في الزمن سواء على مستوى المؤسسات الحكومية أم أفراد المجتمع؛ وتطال مجالات عدة في الحياة. وعلى ذلك يشمل مصطلح الأمن السيبراني أمن المعلومات على أجهزة وشبكات الحاسب الآلي سواء للأفراد أم الشركات أم الحكومات، بما في ذلك العمليات والآليات التي يتم من خلالها حماية معدات الحاسب الآلي والمعلومات والخدمات من أي تدخل غير مقصود أو غير مصرح به أو تغيير أو إتلاف قد يحدث[1] و للفائدة العلمية سيتناول الباحث هنا التعريف بالأمن و الردع السيبراني من خلال المطلبين الآتيين:

المطلب الأول :التعريف بالأمن و الردع السيبراني: يتضح من مصطلح الأمن السيبراني، بأن ميدانه هو الفضاء السايبر، و يقصد "بالفضاء السيبراني": ( المجال الرقمي و الالكتروني الممتد عبر مختلف خطوط الاتصالات المعدنية والضوئية و الهوائية و قنواتها في شبكة الانترنت؛ فهو الحيز المادي و غير المادي الذي يتكون أو ينشأ من جزء أو من مجموع الحواسيب،

شبكات، معلومات محوسبة، برامج و مضامين، معطيات مرور و رقابة، و الذين يستخدمون كل ذلك).[٢] من التعريف المتقدم يمكن استخلاص مجموعة عناصر للفضاء السيبراني[٣]، يعتبرها البعض فريدة من نوعها في الحروب و النزاعات المسلحة، إذ تمكن الدولة بجهازها العسكري أو حتى الافراد من توجيه هجمات من نوع مختلف مؤثرة و بسرعة قصوى ضد أعداء موجودين على مساحات بعيدة جدا من دون تعرض المهاجم للخطر وقت شن الهجمات. كون إنَّ الهجمات التي توجه عبر الفضاء السايبر تتصف بالصمت و قلة التكلفة اذا ما قورنت بالهجمة العسكرية المادية، كما تمتاز ب سرعة الاداء و قوة التأثير، و تعذر معرفة هوية المهاجم و خلفيته الايدولوجية و غيرها في معظم الحالات، لهذه الاسباب و غيرها عدت الهجمات السيبرانية ضد الأمن المعلوماتي للدولة هجمات غاية في الخطورة و التأثير.[٤] و لهذا فعملية الردع المعلوماتي، أصبحت ركيزة أساسية في كل الدول والشركات؛ بل امتدت لتصبح كذلك في المنظمات والمؤسسات كافة، وذلك بهدف مواجهة الحروب الإلكترونية التي باتت تميز حروب العصر الحديث؛ فضلا عن مواجهة المخاطر السيبرانية الأخرى.

و فيما يلي توضيح لأهم المصطلحات الخاصة بهذا المطلب، و على وفق الفروع الاتية:

الفرع الأول: مدلول كلمة الأمن السيبراني و الردع : إنَّ توضيح معنى و مفهوم الردع السايبر يستلزم توضيح مفهوم الامن السايبر كذلك، و مدلول كلمة "الأمن السيبراني" يشير إلى معطيات عدة، تنطلق من الحفاظ على الحكومات الإلكترونية و التركيز على استقرار النظام، وصولاً إلى حماية القيم الجوهرية لمجتمع ما، لكن وبغض النظر عن تقارب أو اختلاف النظرات الفلسفية والسياسية حول الموضوع، فإن الراسخ هو الخشية التي تبديها معظم الدول حالياً، من تعرض أمنها القومي للخطر نتيجة الاشكال المختلفة للجرائم الإليكترونية.[٥] لا سيما و أن تقنيات المعلومات والاتصالات قد رفعت منسوب الخطر، عبر إتاحتها مصادر جديدة متشعبة ومتعددة، مقابل انخفاض نسبة المخاطر وامكانات الانكشاف في جانب الجهة المعتدية[٦]، ربما هذا ما يفسر التنسيق المتزايد بين إدارات الأمن والاقتصاد، فضلا عن الترابط الذي يراه قادة العالم بين الأمن المعلوماتي والاقتصاد والأمن القومي[٧] . كلمة "الأمن السيبراني" هي كلمة لاتينية في الأصل؛ مشتقة من (Cyber security) ومعناها الأمن المعلوماتي، وعلى ذلك يقصد بالأمن السيبراني "الأمن المعلوماتي"، ف هو – أمن الفضاء المعلوماتي أو الأمن المعلوماتي – هو عبارة عن مجموع الوسائل التقنية والإدارية التي يتم استخدامها لمنع الاستخدام غيرالمصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتأمين حماية وسرية وخصوصية البيانات الشخصية ولحماية المواطنين [٨] . يقدح مما تقدم، بأنَّ "الأمن المعلوماتي" إذن هو: أمن الشبكات والأنظمة المعلوماتية والبيانات والأجهزة المتصلة بالإنترنت، فهو المجال الذي يتعلق بإجراءات ومعايير الحماية، المفروض الالتزام بها حيال التهديدات ومنع القيام بالتعديات أو حتى الحد من آثارها في أقسى وأسوأ الأحوال [٩] . كما عرفه آخر انطلاقا من أهدافه بأنه: النشاط الذي يهدف إلى حماية الموارد البشرية والمالية المرتبطة بتقنيات

الاتصالات والمعلومات، ويضمن إمكانات الحد من الخسائر والأضرار، التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ما كان عليه، بأسرع وقت ممكن، بحيث لا تتوقف عجلة الإنتاج، وبحيث لا تتحول الأضرار إلى خسائر جسيمة (١٠) . و إذا أردنا تعريفه تعريفا يظهر "الجانب الاجرائي" ف هو: أمن المعلومات على أجهزة وشبكات الحاسب الآلي، والعمليات والآليات التي يتم من خلالها حماية معدات الحاسب الآلي والمعلومات والخدمات من أي تدخل غير مقصود أو غير مصرح به أو تغيير أو اختلاف قد يحدث، حيث يتم استخدام مجموعة من الوسائل التقنية والتنظيمية والإدارية لمنع الاستخدام غير المصرح به، ومنع سوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها.(١١) و من المعلوم اليوم أنَّ الامن المعلوماتي، قد وصل الى جميع المسائل الاقتصادية والاجتماعية والسياسية، والانسانية، وهو ما ينسجم تماما مع التعريف المعطى له، بأنه قدرة الدولة على حماية مصالحها وشعبها، في مختلف مجالات حياته اليومية، ومسيرته نحو التقدم بأمان، من "جهة اولى"، ومن كونه يرتبط ارتباطا وثيقا بسلامة مصادر الثروة الحديثة، ويعني بها الباحث: "البيانات والمعلومات"، والقدرة على الاتصال والتواصل، و أيضا الانتاج، والابداع، والقدرة على المنافسة، من "الجهة الثانية". ورد له تعريف كذلك في التقرير الصادر عن الاتحاد الدولي للاتصالات حول" اتجاهات الإصلاح في الاتصالات للعام ٢٠١٠ – ٢٠١١ إذ قيل عنه بأنه: " مجموعة الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصال والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية و اتخاذ جميع التدابير اللازمة لحماية الموطنين والمستهلكين من المخاطر في الفضاء السيبراني" (١٢). يظهر مما ذكر آنفا، مدى الارتباط الوثيق بين مفهوم كلمة الأمن عمومًا بموضوع أمن المعلومات، ففي الغالب يكون الهدف من وراء الهجمات السيبرانية و عمليات التعدي، و اختراق الشبكات للدول أو الأفراد: هو بثها أو الاطلاع عليها والمتاجرة بها، أو تشويهها واستغلالها (١٣). و يرى الباحث إنَّ مفهوم "الأمن السيبراني" يتحقق من خلال حماية أجهزة الحاسوب وأنظمتها والخوادم والأجهزة المحمولة والأنظمة الإلكترونية والشبكات والبيانات من الهجمات الضارة ومن سرقة أو تلف برامجها أو بيانتها الإلكترونية، سواء كانت هذه الحواسيب خاصة بالدولة و مؤسساتها؛ أو كانت خاصة بالأفراد العاديين. اما بعد أن اتضح معنى الامن المعلوماتي، فإن الردع السيبراني يقتضي توضيح مفهوم الردع بشكل عام أولا. ف الجنرال :أندريه بوفر" عرَّف الردع بالقول إنه: "منع دولة معادية من اتخاذ قرار باستخدام أسلحتها _أو بصورة أعم_ منعها من العمل أو الرد إزاء موقف معين باتخاذ مجموعة من التدابير و الاجراءات التي تشكل تهديدا كافيا حيالها، و النتيجة التي يراد الحصول عليها بواسطة التهديد، هي سيكولوجية نفسية".(١٤)

لهذا فإنَّ الردع السيبراني سيعني: " منع الاعمال الضارة ضد الأصول الوطنية في الفضاء السايبر"(١٥)، و يرى اتجاه فقهي أن نظرية الردع عندما ظهرت و استعملت بمفهومها

التقليدي، فإنها اليوم تستخدم في مجال السايبر لأنها أصبحت ضرورة لا غنى عنها، لذا تم الحديث عن الردع السيبراني؛ إذ بدونه ستكون البيانات المفتوحة عرضة لأشكال بدائية و أخرى خطيرة من الاستغلال و الاعتداء عليها من قبل كل من تسول له نفسه، فتسرق البيانات و تنتهك حقوق الملكية الفكرية، و تعطل الاعمال التجارية و حتى الرسمية مما يصيب نظم التشغيل كافة بالشلل التام.[١٦] إنَّ تحقيق أمن المعلومات يتم وفق معنى حماية بيانات الأجهزة المتصلة بالحاسب الآلي؛ من الاختراق أو الوصول إلى تلك البيانات المخزنة داخل ذاكرة الحاسوب، إلا أن معالجة موضوع الأمن بل وتحقيق الأمان الالكتروني يتطلب في البداية معرفة التهديدات والمخاطر التي من الممكن أنْ يتعرض لها النظام[١٧]؛ فالخطرالذي يهدد أمن الشبكات وأمن المعلومات يأخذ صورتين الأولى وهي تهديد البنية التحتية وما عليها من نقاط دخول وخروج وتخزين، و اعتراض للمعلومات، والثانية وهي عمليات التخريب والتدمير والتعطيل التي تطالها وتطال الأموال، والأشخاص من خلالها [١٨]. وتتميز الشبكة العالمية للمعلومات – الإنترنت – بمجموعة مواصفات تقنية وفنية خاصة، ينتج عنها مخاطر ذات صفات خاصة، من أهم تلك الصفات إن الشبكات المتصلة بها معرضة للمخاطر ذاتها، وبذلك يمكن تصور تعرض نظام المعلومات للدولة أو الأفراد أو الشركات لاعتداء، مما يجعله يتوقف عن تأدية الخدمات التي كان يقدمها، أو يفشي أسرار تلك المؤسسات والأفراد، سواء أكانت تلك الأسرار شخصية أو صناعية أو مهنية، أو بما يؤدي إلى تلف البيانات الحساسة، أو بث معلومات مغلوطة [١٩]. وعلى ذلك نجد أنَّ أول خطوات تحقيق الأمن المعلوماتي، هو موضوع مراقبة هذه التكنولوجيا، لا سيما في الجانب الفني المتمثل في الاتصالات، ومراقبة حركة انتقال المعلومات؛ وذلك بما يضمن إزالة العوائق أمام الوصول إليها، وانسيابها، ويمنع التنصت عليها سواء من جانب الطرف المنافس أو من قبل الطرف الذي يسعى إلى الاعتداء[٢٠]. وتهدف عملية حماية المعلومات إلى جعل المعتدين يحجمون عن خطتهم، أو إلى منعهم من تحقيقها، أو إلى ضمان حد مقبول من الأخطار، و هذا هو معنى الردع السايبر و وظيفته؛ ويكون ذلك عبر وضع خطة أمن تتلاءم والمحيط التقني والبشري التنظيمي والقانوني. وقد ذهب جانب من الفقه إلى أنَّ الأمن بصورة شاملة، ومضمونه يعد أمرًا بعيد المنال فلكل نظام معلوماتي نقاط ضعف وثغرات خاصة به، جعلت البعض يعتبرون قوة أي نظام إنما تقاس بقوة أضعف نقطة فيه. و مما لا شك فيه أنَّ اهتمامات الأمن، تختلف باختلاف المواد والموارد المعرضة للتهديد، فمواقع الشركات التجارية الخاصة أو مواقع الأفراد تختلف عن المواقع الحكومية، وهذه الأخيرة تختلف عن المواقع المالية، والعقارية، كما تختلف عن مواقع التسلية والترفيه، مما يتعين تحقيق "الردع المعلوماتي" لحمايتها كلها [٢١]. هذا كله يفسر الاسباب وراء سعي الدول الحديثة لتعزيز قدراتها التقنية من اجل أمن شبكاتها الالكترونية، لتحسين مستوى دفاعها عنها بما يحقق الردع المعلوماتي، و تأمين العمليات التي تتم على الشبكة المعلوماتية الخاصة بالدولة، و عادة يتم اللجوء لمجموعة من الوسائل التقنية مثل " الجدران النارية"، تشفير البيانات، مكافحة الفايروسات التي

مصدرها الشبكة العنكبوتية، علاج الثغرات الأمنية، و تطوير التكنولوجيا اللازمة لتقليل التوقيع الكهرومغناطيسي.[٢٢]

الفرع الثاني: ارتباط الأمن و الردع السيبراني بالأمن العام: ما تقدم من معنى حول أمن الشبكات المعلوماتية دفع معظم الدول من لديها امكانيات إلى تأسيس قيادة سيبرانية لها لتعزيز قدراتها القتالية في ما يضمن لها الردع السيبراني، ف الولايات المتحدة اسست( يو اس سايبركوم)، و التي يقودها رئيس وكالة الأمن القومي الأمريكية، و ضمت القيادة السيبرانية الجديدة الفروع التي كانت تتبع القوات البحرية و الجوية، بريطانيا انشأت كذلك " القوات المشتركة للجماعة السيبرانية، و التي بدورها تشرف على ثلاث مؤسسات تعمل في مجال الأمن السيبراني، إذ يدخل ضمن عملها الاستفادة من خبرات المتخصصين في مجال الفضاء المعلوماتي و السيطرة الأمنية، و كذلك فعلت ألمانيا و هولندا و غيرها.[٢٣] فماذا يعني الامن العام و ما علاقة الامن و الردع السيبراني به؟

حماية الأمن العام تعد من الوظائف الأساسية للدولة في كل النظم الدستورية الحديثة، و حتى قديما كانت فكرة الدولة الحارسة التي تأخذ على عاتقها حماية الامن الداخلي و الخارجي هي السائدة، إذ يجب على الدولة في كل وقت أنْ تدافع عن نفسها و ترد أي إعتداء خارجي يهددها و يقع على أراضيها، و بالتالي هي مسؤولة بأجهزتها ذات العلاقة عن تحقيق و نشر الأمن و الامان في اقليمها الأرضي و الجوي و المائي، و مسؤولة عن بث الطمأنينة في نفوس رعاياها كافة، لكي تثبت دعائم الاستقرار و تتجنب شبح الاضطرابات و الفوضى التي ستنجم فعلا إذا ما إختل و اضطرب أمنها العام، و كانت الدولة و لا تزال تعتمد في تحقيق هذه الأمور كلها على جهازها التنفيذي، و على وزاراتها ذات الاختصاص الامني البحت.[٢٤] المعنى المتقدم دفع جانب من الفقه الدستوري إلى تعريف الأمن العام بالقول هو: ( اطمئنان الإنسان على نفسه و ماله من خطر الاعتداءات التي يمكن أنْ تقع عليه، و يتحقق ذلك ب اتخاذ الإجراءات اللازمة لمنع أي فعل من شأنه إلحاق ضرر بالغير، سواء كان ذلك بفعل الإنسان كمنع الجرائم التي تقع على الاشخاص أو الأموال، درء الفتن و الاضطرابات، أو أي خطر يمكن أنْ يتأتى من الأشياء، كهدم المنازل الآيلة للسقوط، أو بسبب أخطار الطبيعة كمجابهة أخطار الفيضانات و الزلازل و الحرائق و غير ذلك).[٢٥] و يتضح مدى السعة في المعنى المعطى للأمن العام في التعريف المتقدم، و مع ذلك فهو لم يحط بكل الامور التي يمكن أنْ تنشأ عنها مخاطر جدية تطال أمن مواطني الدولة. يعني أنَّ الأمن العام يعرف بمعنيين، المعنى الواسع: و يشمل المؤسسات الأمنية في الداخل و الخارج كافة، و على وجه التحديد أجهزة الشرطة و الحرس الوطني و الجيش و جهاز الامن الوطني و جهاز المخابرات و غيرها من المؤسسات الامنية من التي تختص بمكافحة الجريمة( عادية و سياسية) و محاربة المعتدين، أما المعنى الضيق له ف يقف عند مؤسسات الأمن التابعة لوزارة الداخلية المخصصة لحفظ الأمن الداخلي فقط. و يعبر هذا المفهوم عن التركيز في التمييز بين كل من الامن العام الداخلي" أمن المجتمع، أمن الدولة، الوقاية من الجريمة" و تحقيق الاطمئنان لأفراد المجتمع كافة و هي مهمة تقع على عاتق وزارة الداخلية كما وضح اعلاه، و بين الامن العام الخارجي الذي يعبر عن أمن حدود الوطن و ترابه و الدفاع

عنه في مواجهة الغزاة، و هي مهمة تقع على عاتق الجيش و المؤسسة العسكرية بكاملها و التي تتبع وزارة الدفاع (٢٦). عليه ف مفهوم الأمن و الردع السيبراني؛ يرتبط بمفهوم الأمن العام بشكل وثيق؛ فالتقنيات التي وسعت الآفاق وأثرت الثقافة، وسمحت للثقافة المحلية بالامتداد إلى المجال العالمي، باتت تهدد الهوية الوطنية والقومية مع تأثر الأجيال الصاعدة بما يصلها وبما تصل إليه عبر الإنترنت.(٢٧)، إذ تبدو الهوية وكأنها خاضعة لعملية إعادة تشكيل، من خلال تكنولوجيا المعلومات، إذ حرص الغالبية العظمى من الناس، على استخدامها في تكوين مجتمعهم الخاص الافتراضي، وتفكيرهم وبيئتهم المميزة(٢٨). فالأمن السيبراني فضاء معلوماتي يستحضر فيه الأفراد قيمهم ومصالحهم واهتماماتهم المختلفة، "و إن كان بشكل افتراضي" ؛ التي يمكن أن تؤثر وتتأثر بالأخرين، فبتنا نلاحظ على سبيل المثال أن بعض مجموعات المصالح الخاصة، تهدد بالحلول كبديل لهوية يندمج تحت مظلتها، مجموعات أكبر من الناس(٢٩). إنَّ العلاقة بين الردع السيبراني، وبين الأمن العام، علاقة قوية تزداد متى زاد نقل المحتوى المعلوماتي والعسكري والأمني والفكري والسياسي والاجتماعي والاقتصادي والخدمي والعلمي والبحثي إلى الفضاء السايبر، خاصة مع تسارع الدول في تبني الحكومات الإلكترونية والمدن الذكية واتساع نطاق وعدد مستخدمي خدمة الانترنت في العالم، مما أدى إلى أن تكون قواعد البيانات الوطنية معرضة للكشف من جهات خارجية، إضافة إلى حملات الدعاية والمعلومات المضللة ونشر الشائعات أو الدعوة لأعمال تحريضية أو دعم المعارضة أو الأقليات داخل الدولة، مما يؤثر سلبًا على مفهوم سيادة الدولة مما ينتج عنه خللا في قدرة الدولة في الحفاظ على أمنها الداخلي.(٣٠) وقد أعلن المسؤول السابق عن الأمن الوطني الأميركي أن الإنترنت قد رفع مستوى الأخطار التي يتعرض لها النظام بشكل غير مسبوق. وذلك في إشارة واضحة إلى التهديدات الجديدة التي تستهدف الأمن القومي الأمريكي والتي يمكن أن تتخذ أشكالاً غير متوقعة وتطاول مجالات أساسية وحيوية(٣١).

المطلب الثاني : تمييز الردع السيبراني عن ما يشتبه به: نسمع كثيرا في الأخبار و التقارير السياسية بمصطلح "نظرية الردع"؛ و يقصد بها أهل السياسية: بأنها إحدى نظريات إدارة الصراع التي تستند أساساً على الأدوات العسكرية بالدرجة الأساس، لذلك كثيراً ما يقرن البعض مصطلح "الاستراتيجية" بمصطلح "الردع"). عليه فقد بات مصطلح «إستراتيجية الردع» من المصطلحات شائعة الاستخدام سواء في مجال التخطيط العسكري أو العلاقات الدولية. و لكن هل يتشابه الردع السيبراني مع الردع العسكري التقليدي؟ و هل يوجد فعلا ردع سياسي أو اقتصادي و بالتالي يختلف عن الردع السيبراني؟ هذا ما سأعمد لتوضيحه في الاتي:

الفرع الأول : تمييز الردع العسكري النووي عن الردع السيبراني: منذ ٢٠٠ عام تقريبا؛ كانت الدول و لا تزال تستخدم التهديدات العسكرية؛ المباشرة وغير المباشرة كوسيلة من أجل ردع الأزمات والحروب الدولية، و بات الحديث عن هذه الموضوع الشغل الشاغل لعدد كبير من الكتاب و الباحثين في المجال السياسي و الأمني، إذ ركزت الأبحاث في الغالب على نظرية (الردع العقلاني) لتحليل الظروف التي يُحتمل أنْ ينجح فيها الردع التقليدي أوقد يفشل.

و ظهرت نظريات بديلة تحدت "نظرية الردع العقلاني" وركزت على النظرية التنظيمية وعلم النفس المعرفي كبديل لتفسير اللجوء للردع. و الذي يمكن هنا تعريفه: بأنه استخدام تهديدات أحد الأطراف من أجل إقناع طرف آخر بالامتناع عن الشروع في بعض الإجراءات. و يعد التهديد بمثابة رادع إلى الحد الذي يقنع به المعني بعدم تنفيذ الإجراء المزعوم؛ بسبب التكاليف والخسائر التي سيتكبدها هذا الطرف.[٣٢] ففي مجال الأمن الدولي، تشير سياسة الردع عمومًا إلى تهديدات الانتقام العسكري التي يوجهها قادة إحدى الدول، إلى قادة دولة أخرى، في محاولة لمنع الدولة الأخرى من اللجوء إلى التهديد باستخدام القوة العسكرية في مواجهة دولتها لأهداف سياسية. يشير نجاح الردع من الناحية العسكرية إلى منع قادة الدول من إصدار تهديدات أو إجراءات عسكرية تصعد التعاون الدبلوماسي والعسكري في أوقات السلم إلى أزمة أو مواجهة عسكرية تهدد بالصراع المسلح وربما الحرب. غير أن منع أزمات الحروب ليس هو الهدف الوحيد للردع. فضلا عن ذلك، يجب أن تكون الدول المدافعة قادرة على مقاومة المطالب السياسية والعسكرية للدولة المهاجمة المحتملة. إذا اجتُنب النزاع المسلح بسعر تنازلات دبلوماسية إلى الحد الأقصى لمطالب الدولة المهاجمة المحتملة تحت تهديد الحرب، فلا يمكن القول بأن الردع قد نجح. علاوة على ذلك، يجادل البعض مثل جينتلسون بأن مجموعتين رئيستين من عوامل الردع الناجح هما المهمان: (١) إستراتيجية الدولة المدافعة التي توازن أولًا بين الإكراه ذي المصداقية والدبلوماسية الماهرة بما يتسق مع المعايير الثلاثة المتمثلة في التناسب والمعاملة بالمثل والمصداقية القسرية، وتقلل ثانيةً القيود الدولية والمحلية، و (٢) مدى ضعف الدولة المهاجمة مثلما تتشكل من ظروفها السياسية والاقتصادية الداخلية.[٣٣] إذن مفهوم "نظرية الردع النووي"، أن الأسلحة النووية تهدف إلى ردع الدول الأخرى عن مهاجمة أسلحتها النووية، من خلال الوعد بالانتقام وربما التدمير المتبادل (M.A.D.)؛ يمكن أيضًا تطبيق الردع النووي على هجوم القوات التقليدية، إذا كان عنيفا و قويا، على سبيل المثال ما كان يحصل من تهديد باستخدام مبدأ (الانتقام الشامل) بإطلاق أسلحة نووية أمريكية ردًا على الهجمات السوفيتية و بالعكس. ف الردع النووي الناجح يتطلب، أنْ يحافظ أي بلد على قدرته على الرد، إما عن طريق الرد قبل تدمير أسلحته أو عن طريق ضمان قدرته على القيام بالضربة الثانية، و كثيرا ما نسمع الدول النووية تتحدث عن ضرورة امتلاكها ل "الثالوث نووي" كمتطلب ضروري للردع النووي، مثلما في حالة الأسلحة النووية التي تملكها الولايات المتحدة ، روسيا، جمهورية الصين الشعبية، والهند.[٣٤] من مجمل القول يبين مدى الاختلاف بين الردع النووي و الردع المعلوماتي، و مرد هذا الاختلاف إلى عدد من العوامل، أولها إنّه لم يحدث حتى الآن صراع عسكري حاد في الفضاء السايبر، و ذلك على الرغم من التطور الواضح ل قدرات الدول في هذا المجال، و ثانيهما: أنّ الردع في المجال النووي استند إلى افتراض أساسي وهو " العقلانية" لدى قادة الدول ذات القدرات النووية العسكرية، ومن ثم فإنهم لم يقدموا على استخدام السلاح النووي مع محافظتهم على الردع، في حين يضم الفضاء المعلوماتي فواعل مسلحة من دون الدولة و الذين لا يتسمون بالضرورة بالعقلانية. و ثالثها هو تراجع الخوف من التهديد برد عسكري

مقابل على أي تجاوز عسكري، نظرا لصعوبة التيقن من هوية الطرف الذي قام بشن الهجوم الالكتروني العدائي، إلا بعد فترة طويلة نسبيا، وهو أمر يظل قويا بطبيعة الحال في مجال الردع النووي، إذ يخاف الفاعل الدولي نتيجة علمه بتعرضه المباشر و السريع للرد و العقاب.

و يظهر رابع هذه الاختلافات في وجود صعوبة في تحديد العناصر المادية لقوة الخصم، و التي سيتم استهدافها في حال التعرض لهجوم سيبراني، و أخيرا فإن المصداقية في إنفاذ التهديد تتراجع نظرا لغياب قواعد اشتباك واضحة، و صعوبة التعرف على القدرات الالكترونية المعلوماتية للخصوم بدقة، و بناء على ما تقدم كله فإنَّ هذه العوامل ستدفع إلى تطبيق الدول للردع عبر تدابير المنع في الفضاء السايبر، و ذلك من خلال آليات مختلفة و متداخلة، لعلنا نوفق إذا قلنا أن من أبرزها عدم منح الاستثمارات الاجنبية في البنية التحتية المعلوماتية المهمة للدولة، مع تطوير برمجيات وطنية فعالة، و اخيرا التدريب المتواصل للأفراد ليكونوا على أتم الجاهزية لتشغيل المنظومات الوطنية و صيانتها، و التصدي للتهديدات السيبرانية و وأدها أو الرد المباشر الملائم عليها، و لا يجب أنْ ننسى دور التشريعات ذات العلاقة اقليميا و وطنيا.(٣٥)

الفرع الثاني: تمييز الردع السيبراني عن الهجمات السيبرانية: الفضاء السيبراني: هو الميدان الرئيس للهجمات السيبرانية التي تشنها جيوش خاصة تم تدريبها و تجهيزها لهذا الغرض، و لا مناص من القول إنَّ هذه الجيوش يمكنها أنْ تقاتل في ميادين القتال التقليدية، فضلا عن ميدان فضاء السايبر، و الاخير هو نفسه ميدان تحقيق الردع السيبراني المعلوماتي، مما يعني إن الاثنين يشتركان، في وحدة الميدان الخاص وهو " الفضاء السايبر"، و آليات المهاجم السيبراني و أدواته تتشابه مع أدوات المدافع السايبر، لكن ليس بالضرورة أنْ تتماثل معها، في وقت السلم نلاحظ أنَّ المهمة الوحيدة للجيوش السيبرانية تتلخص في تقديم الدعم المعلوماتي و اللوجستي لجيوش الميادين الاخرى التقليدية، فيقومون بالتجسس الكترونيا على العدو عبر اختراق شبكاته للاطلاع على أسراره و سرقة تصميماته العسكرية للأسلحة المتقدمة المخزنة الكترونيا، فضلا عن الخطط الاستراتيجية و الاقتصادية؛ و نوع التسليح الذي لديه و مناطق توزيعه و نشره، ناهيك عن معرفة أهم الأهداف التي يسعى إلى تدميرها اذا ما اندلعت مواجهة مسلحة مباشرة، و عديد القوات و اعدادهم و تجهيزاتهم، كل هذا يتم من خلال شن عديد من الهجمات الالكترونية التي يُعدُ لها مسبقا بشكل جيد، و في وقت الحرب؛ تحدد لهم دولهم مهام مزدوجة في كل من الهجوم و الدفاع معا؛ فضلا عن تقديم الدعم المباشر للقوات المسلحة المقاتلة في ميادينها الخاصة، فيقومون ب هجمات الكترونية لتعطيل نظم التحكم و السيطرة لدى العدو، تعطيل أنظمة دفاعه الجوي و منصات إطلاق الصواريخ، و حتى ما بات يعرف ب مراكز السيطرة على "الاسلحة ذاتية التشغيل"، و عمليات أخرى مثل الخداع الالكتروني و التشويش الرقمي على مختلف أجهزة العدو و معداته التقنية، و بالوقت عينه توضع على عاتقهم مسؤولية الدفاع "الردع"، من خلال تأمين الاتصالات بين الوحدات العسكرية الصديقة المقاتلة، ومنع أي محاولة لأختراق أجهزتها و معداتها و مواقع بياناتها، أو حتى

التجسس عليها.[٣٦] يعرف البروفسور فويرتس (Fruertes)، استاذ قسم الكيمياء (جامعة تكساس)، الهجمة "السيبرانية" بأنّها: "هجوم عَبرَ الإنترنت يقوم عَلَى التسلل إلى مواقع الإلكترونية غَيْر مرخص الدخول إلَيْها بهدف تعطيل البيانات المتوفرة أو إتلافها أو الاستحواذ عليها، ووصفها بأنّها سلسلة هجمات إلكترونية تقوم بها دولة ضَدّ دولة أخرى".[٣٧] ورأى فيها: ((مايكل شميت)) بأنّها "إجراءات تتخذها الدولة، بهدف الهجوم عَلَى نظم مَعَلومات للدولة المعادية والتَأثير بها"[٣٨]. و هذه التعاريف تبين الجانب الهجومي لهذه الهجمات فقط و ليس الدفاعي. و الباحث يعرِّف الهجمات السيبرانية بالقول: (أنّها عمليات تقنية معقدة، يتولى القيام بها جيوش الكترونية مختصة، تَتمثل بالدخول المباشر إلى النِظَام المعَلوماتي دُون وجه حق، مرادها تعطيل النِظَام المعلوماتي لدولة أخرى عدوه أم غير عدوه، أو إتلاف هذا النظام، او الاستحواذ على البيانات؛ باستعمال برامج وفايروسات عدة، وقَدّ يصاحب مَعَهُ تعطيل الأجهزة الإلكترونية أو أجْهِزَة الذكاء الاصطناعي). من التعريف المتقدم؛ نستخلص أنَّ للهجمات السيبرانية خَصَائص عدة؛ ومنها :

١-إنها هجمات متطورة حديثة؛ تتصل بالثورة المعَلوماتية، وهي صورة مَن صور الجرائم الإلكترونية، ولا تحتاج إلى كلفات عالية فكلفتها متدنية، إذ كَلّ مَا تحتاجه هو أجْهِزَة إلكترونية متطورة، قيَّاساً للهجمات المسلحة التي تحتاج إلى أسلِحة مادية وجَيْش منظم خاصّ في الدولة.[٣٩]

٢-إنَّها هجمات تحدث بدون حدود زمنية ومكانية، فهي تحدث سَوَاء بالحرب أو في وقت السلم، فهي هجمات غَيْر محدودة النطاق، أيّ عابرة للحدود، مَعَ صعوبة تحديد موقع مرتكب الهجمة بسُهولة؛ لأنّها لا تتَرك أَثراً عَلَى شخصية مرتكبها.[٤٠]

٣- إنّها هجمات رفيعة المستوى، لأنّها أوسع مَجَالاً ونَتَائجها أكبر، فالأضرار التي تَصَاحَبَها، تَتمثل بالأضرار المَعَنوية المادية مَعَاً، إذ يصاحب الهجمات السيبرانية إتلاف البيانات وتعطيل النظام، وكذلكَ إتلاف وتعطيل أجْهِزَة الحواسيب المختلفة؛ وهذه أضرار مادية ومَعَنوية في الوَقْت نفسه.[٤١]

إنَّ اتصال مَفْهُوم الرَدَعَ السيبراني بمَفْهُوم الأمَن السيبراني، وبالتَعريف الدَقيق لهذا النوع من الأمَن الذي يتعلق كما اتضح ب" أمَن المعَلومات وأمَن تكنولوجيا المعلومات؛ لذا وجدنا البعض يعرِّفه بأنهُ: " "القُدَرَة عَلَى إحباط الهجمات"[٤٢]. و لذلك تختلف الهجمة السيبرانية عن الردع السيبراني من حيث المدلول و المفهوم كذلك، لكنهما يتشابهان في أنّ كليهما يدخل ضمَن مَفْهُوم الفضاء السايبر، وهما قائمان و يحدثان سَوَاء في زمَن السلم أم الحرب، لاسيما مع التطور التقني الحديث الذي باتت تشهده عديد من الدول.

وما يَفْرُقُهما بَعَض النقَاط، منها :

إنَّ الرَدَعَ السيبراني؛ في الأصل هو بمثابة الانتقَامَ العيني ضَدّ استعمال الهجمات الالكترونية ضَدّ الدولة، أما الهجمات السيبرانية فتكون هجوما ضَدّ دولة ما، إذ يصف (مارتين ليبيكي) في كتابه "رَدَعَ الانترنت والحرب السيبرانية"، أنّ الرَدَعَ السيبراني له صورتان، الأولى أنّ يكون (رَدَعَ سيبراني سِلْبي)، ويَعْنِي هو صورة عدم الرد عَلَى الهجوم

السيبراني والاكتفاء بتحسين وتَطْوِير وَسائِل الأمَن المعَلوماتي للدولة, مثل بناء شبكات مرنة تقلل مَن الهجوم.

أمّا الصورة الثانية فتتمثل ب (الرَدَعَ السيبراني المنشط). ومَعَناه: ذلك الرَدَعَ الذي يأخذ صورة هجمة سيبرانية مُنْتَقِمَةٌ كرَدّ عَلَى هجمة أخرى سَبَقتها مَن دولة أجنبية, ومما تَقَدم يتضح القَوْل, أنّ الرَدَعَ السيبراني قَدّ يتحول إلى هجمات سيبرانية ايضا, إذا كانت كرد فعل عَلَى هجمة اليكترونية سَبَقتها ضَدّهم, ولذلك أطلق عليها التسمية اعلاه؛ تَحْتَ معنى الرَدَعَ عَن طَرِيق المعاقبة بذات الفعل.[٤٣] و لا يتفق الباحث مع الصورة الثانية التي تحدث عنها الكاتب اعلاه, و ذلك لكونها تتمثل في الواقع بعمل انتقامي مجرم مماثل؛ ترد به دولة على هجمات سيبرانية طالتها نتيجة اعتداء مجرم أصلا, و ليس هذا هو المعنى الذي يقصد الباحث أنْ يوصله عن مفهوم و معنى الردع, إذ ما نتحدث عنه بعيد كل البعد عن الاعمال الانتقامية التي يتوجه العالم أجمع إلى حضرها و تجريمها, بل ما نتحدث عنه هو: (مجموعة الاستراتيجيات و الاجراءات العملية التي تتخذها الدولة في حدود صلاحياتها المخولة لها؛ لتجعل من أصولها الالكترونية و بياناتها؛ و جميع أصول و بيانات مواطنيها؛ محصنة ضد كل أنواع الهجمات الخبيثة التي قد تتعرض لها من أي مصدر كان داخلي أو خارجي, مما يحقق الأمن السايبراني المطلوب, من دون التورط أو الدخول في أعمال مجرمة بمقتضى القانون الدولي أو حتى الداخلي).

المبحث الثاني: مجالات الردع السيبراني و الاساس الدستوري لتحقيقه في العراق و مدى كفايته: لقد تم إثبات كيف ارتبط مفهوم الأمن, بكيفية استخدام الدولة لقوتها لإدارة الأخطار التي تُهدد وحدتها و استقلالها و استقرارها السياسيّ في مواجهة مواطنيها, و كذلك في مواجهة الدول الأجنبية, وعليه فإنَّ الأمن هو: ما تقوم عليه الدولة من قيم وأهداف وظيفية, و الإجراءات المُتعلّقة بتأمين وجودها وسلامة كيانها و استمرارها و استقرارها كافة, وتلبية احتياجاتها وضمان مصالحها الحيويَّة وحمايتها من "التداخلات الخارجيَّة" مع مراعاة التطورات الإقليميَّة والدوليَّة. وهو ما سيتم الحديث عنه في المطلب الاول, و الثاني سيخصص لبيان الاساس الدستوري لتحقيق الردع و مدى كفايته:

المطلب الأول: مجالات الردع السيبراني: علما أن ل الردع السيبراني مجالات تتعدد لتشمل المسائل الاقتصادية والعسكرية و الاجتماعية والسياسية, ف "الأمن المعلوماتي" يعبر عن قدرة الدولة على حماية مصالحها و مصالح شعبها في جميع المسائل التي تستخدم فيها التكنولوجيا؛ والتي باتت تستخدم في مجالات الحياة كلها, و في الفروع الآتية توضيح لها:

الفرع الأول: المجال العسكري :اتجهت أغلب الدول إلى الأخذ بالمفهوم الواسع (للأمن العام), وكذلك فعل الفقه أمثال الفقيه روبرت ماكنمار "Robert Mcnamara" ، إذ عرَّف "الأمن القوميّ" [٤٤]، بكونه لا يعني تراكم السلاح, بالرغم من أنَّ ذلك قد يكون جزءًا منه, وليس هو القوة العسكريَّة؛ بالرغم من أنَّه قد يشتمل عليها, وليس النشاط العسكريّ التقليديّ بالرغم من أنَّه قد يحتوي عليه, إنَّ الأمن: هو التنميَّة؛ وبدون التنميَّة لا يمكن الحديث عن الأمن.[٤٥] و المجال العسكري بات يعد هو "المجال الخصب" للهجمات

السيبرانية. ففي الغالب يكون الهدف من اختراق الفضاء الإلكتروني للدول هو الحصول على المعلومات العسكرية، والقيام ببثها للأعداء(٤٦). ولذا يمكن القول إنّ الهجمات السيبرانية و الهجمات المسلحة هي أعمال عدوانية, ومرتكبها يعد مسؤولاً, وكلاهما يعدان انتهاكاً لحقوق الدولة أو الأفراد, ويسببان أضراراً كبيرة, إلا أنهما يختلفان بنسبة الضرر وطبيعته, فالهجمات السيبرانية إن حدثت فهي تحدث في الفضاء السيبراني, الذي يتميز بغياب الحدود والحواجز المكانية والزمانية؛ وكذلك الأبعاد الجغرافية, أما الهجمات المسلحة, فهي تتقيد بزمن وحواجز مادية و لأبعاد الجغرافية, وأنّ الهجمات المعلوماتية لا تحتاج الى عدّة كثيرة, أو تكاليف عالية في شراء أسلحة وإنشاء جيش بأعداد كبيرة, خلافاً للهجمات المسلحة التي تحتاج إلى تدابير كثيرة للهجوم وصد الهجوم.(٤٧) لا يخفى على أحد مدى خطورة اختراق الأنظمة العسكرية عن طريق الفضاء الإلكتروني من ضرر يهدد السلم والأمن ليس الداخلي فحسب، و إنّما الدولي كذلك. فقد وقع صراع مسلح بين روسيا وجورجيا بسبب الهجمات و الاختراقات الإلكترونية.(٤٨) كذلك تعرضت إيران لاختراق أنظمة المنشآت النووية وتم التلاعب بها، ويمكن إيراد الاختراق الذي حصل في البرازيل، والمملكة المتحدة للبنية التحتية للطاقة، حيث انقطع التيار الكهربائي، ما طال بآثاره السلبية ملايين الأشخاص، والمؤسسات والمصالح (٤٩). ويرى الباحث ضرورة وجود أطر قانونية في حماية الأمن السيبراني و تحقيق الردع الذي من خلالها يمكن حماية المواقع العسكرية؛ ولذلك يجب أنْ يكون هناك قانون صريح في حماية المنشآت العسكرية التي تعد ذات اهمية كبيرة في الدولة. وقد نص الدستور العراقي في المادة ٩ / أولا / د على: " يقوم جهاز المخابرات الوطني العراقي بجمع المعلومات وتقويم التهديدات الموجهة للأمن الوطني وتقديم المشورة للحكومة العراقية ..... و يعمل وفقا للقانون..... "(٥٠). فمن هنا يتضح أنَ المشرع الدستوري العراقي قد كلف جهاز المخابرات الوطني،(٥١) بمهمة حماية المعلومات العسكرية من الغزو و الاختراق في الفضاء السايبر، إذ أسند إلى هذا الجهاز مهمة جمع المعلومات وتقويم التهديدات التي تواجه الأمن الوطني بغض النظر عن مصدر تلك التهديدات سواء أكانت تهديدات سيبرانية أم غيرها، خارجية أو داخلية. وبهذا النص يكون المشرع الدستوري العراقي قد وضع "بنية تشريعية أساسية" تصلح لإصدار تشريعات عدة؛ لتكون عاملا مهما في حماية الأسرار و المعلومات العسكرية لدولة العراق؛ من الاختراق بسبب الهجمات الإلكترونية، و يبقى التساؤل قائما، هل تم اصدار تشريع فعلا؟ سيما و ان المادة ٨٤ من دستور ٢٠٠٥ نصت على ( أولا- ينظم بقانون عمل الأجهزة الأمنية و جهاز المخابرات الوطني، و تحدد واجباتها و صلاحياتها، و تعمل وفقا لمبادئ حقوق الإنسان، و تخضع لرقابة مجلس النواب. ثانيا- يرتبط جهاز المخابرات الوطني بمجلس الوزراء). و على الرغم من أهمية و جسامة الدور الذي يضطلع به جهاز المخابرات الوطني، و برغم النصوص الدستورية المتقدمة؛ التي أرست الأساس الدستوري اللازم لأنشاء هذا الجهاز على أسس قانونية كافية، لكن قانونه مع ذلك لم يصدر، وحاول مجلس النواب منذ العام ٢٠١٥، إنجاز تشريع قانون جهاز المخابرات الوطني، كون أنَ الدستور قد خصه بهذا الأمر، إلا أنَ "الصراعات التحاصصية" داخل أروقة هذا المجلس من جهة؛ والموانع القانونية

الدستورية من الجهة الثانية حالت دون أنْ يبصر هذا القانون المهم النور إلى يومنا هذا!. فالأحزاب السياسية ذات التوجهات الاسلامية و الحاكمة حاليا في العراق، ترغب بشدة في أنْ تحصل على جهاز يكون (فوق القانون)؛ غير محكوم بالموانع الدستورية مثل المادة (٤٠) بحيث تستطيع استخدامه للتجسس على المواطنين اولا وعلى خصومها السياسيين ثانيا، وقد انهى المجلس القراءتين الاولى والثانية لمشروع القانون بداية العام ٢٠١٥ وفي نهايته، وبقي التصويت النهائي الذي ما زال قيد التعثر.[٥٢] كما أنهى المجلس ذاته القراءة الاولى لمشروع قانون جهاز الامن الوطني العراقي والمقدم من لجنة الامن والدفاع لاستحداث جهاز للأمن الوطني العراقي؛ يتولى استخدام الوسائل الاستخبارية والامنية بطرق علمية وفنية ومنهجية واضحة؛ للمحافظة على الدولة من التهديدات التي ترمي الى النيل من كيان الدولة وأمن المجتمع واستقراره وتنميته ومصالحه الاساسية الاخرى بالتعاون مع اجهزة الدولة المعنية الاخرى. إذ أنَّ جهاز المخابرات الوطني؛ ليس هو الجهة الوحيدة التي ستتولى حفظ الأمن العام في العراق؛ ومن أجل وضع إطار قانوني للأنشطة الاستخبارية والامنية بما يكفل احترام حقوق الافراد، تم قراءة و مناقشة كل المشروعات أعلاه داخل مجلس النواب، و مع هذا لم يصدر أي قانون، علما إنَّ هذه الاجهزة قائمة موجودة و تعمل، و لكن بجهل الأساس التشريعي لوجودها و عملها، و لا نعلم ماذا ينتظر مجلس نوابنا الموقر كي يولي هذه المشروعات الاهتمام المطلوب.

الفرع الثاني: المجال الاقتصادي :من أهم المجالات التي تسعى الدولة إلى الاهتمام بها و تطويرها؛ هو المجال الاقتصادي، قاصدة تحقيق التنمية المطلوبة فيه، لما في ذلك من خير لها و لمواطنيها على السواء، إنَّ دراسة التنمية الاقتصادية هي من الدراسات الحديثة نسبياً التي اهتم بها علم الاقتصاد بعد بداية القرن العشرين خاصة في الدول النامية، ووجدت من المفيد أولاً أنْ أعرض أهم تعريف لهذا النوع من التنمية وأشملها، لما تضمنه من عناصر مهمة في التنمية وشروط العمل و الاستمرار بها وهو: (عملية يتم فيها زيادة الدخل الحقيقي زيادة تراكمية وسريعة ومستمرة عبر مدة من الزمن، بحيث تكون هذه الزيادة أكبر من معدل نمو السكان، مع توفير الخدمات الإنتاجية والاجتماعية وحماية الموارد المتجددة من التلوث والحفاظ على الموارد الغير متجددة من النضوب)[٥٣]. ف بعد أنْ كانت العلاقات القانونية تقع اغلبها في العالم المادي؛ و بوسائل تقليدية ورقية، أضحى اليوم يتقاسم تكوينها، نشأتها، و آثارها العالم المادي و العالم الافتراضي؛ الذي من أهم سماته سيادة الوسائل الالكترونية و على رأسها و في مقدمتها "الفاكس" و الانترنت, بل إنَّ حصة الوسائل الالكترونية و خاصة "الانترنت" من هذه العلاقات هي الأكثر في الوقت الحاضر و في حالة ازدياد في المستقبل، من هنا يتضح أنَّ المجال الاقتصادي؛ هو من المجالات التي يهدف "الردع السيبراني" إلى ضمان حمايتها، فمن دون شك يرتبط الأمن الالكتروني؛ ارتباطا وثيقا بالاقتصاد الوطني للدولة، ولقد ظهر في الآونة الأخير مصطلح اقتصاديات المعرفة والذي يعبر عن التوسع في استخدام تكنولوجيا الاتصالات والمعلومات في مجال الاقتصاد [٥٤]. فقد تم التوسع في استخدام البيانات، والمعلومات المتداولة والمخزنة والمستخدمة من أجل تعزيز التنمية الاقتصادية لبلدان كثيرة؛ وذلك عبر إفادتها من فرص الاستخدام التي

تقدمها الشركات الدولية، والشركات الكبرى التي تبحث عن إدارة كلفة إنتاجها بأفضل الشروط. إلا أنَّ هذا الواقع يطرح مسائل مختلفة سواء منها ما يتعلق بحماية مقدم الخدمة والعمل، أو بحماية المستهلك على الإنترنت.

ف العالم في الآونة الأخيرة يشهد عصر المال الإلكتروني؛ وهو من نتاج بيئة تقنية بعد إطلاق خدمات المحفظة الإلكترونية. فقد تتزايد استثمارات المصارف والمؤسسات المالية في مجال المال الرقمي كما تنافس الشركات على إصدار تطبيقات الإلكترونية التي تسمح بتقديم خدمات مصرفية أمنة، فيتم حفظ المال في المحفظة الإلكترونية واستخدامها كرصيد افتراضي، وقد وضعت بعض الدول تشريعات خاصة للتعامل بالمال الإلكتروني.[٥٥] وغني عن القول ما يمكن أنْ يثيره هذا الأمر من صعوبات وما يتطلب من تشريعات للحد من بعض الجرائم الاقتصادية والمالية الخطرة، والعابرة للحدود، مثل جريمة غسيل الأموال، والتهرب الضريبي [٥٦] . الفقه ربط بدوره بين قدرة الدولة على توفير الردع السيبراني، وبين النمو الاقتصادي، إذ أنَّ الأمن المعلوماتي، هو ما يضمن تقديم خدمات محمية بمقتضى تقنيات الاتصال الحديثة والإقبال عليها بما يؤدي إلى تطوير الأسس الاقتصادية، ولعل الدليل الأوضح على هذه القيمة؛ هو استهداف هذه المعلومات، منذ القديم، سواء من خلال عمليات التجسس الصناعي والعسكري التقليدية، أو من خلال الاعتداء على الملكية الفكرية [٥٧].

عند تصفح نصوص دستور العراق لعام ٢٠٠٥ لوحظ النص على : " تكفل الدولة اصلاح الاقتصاد العراقي وفق اسس اقتصادية حديثة وبما يضمن استثمار كامل موارده وتنويع مصادره وتشجيع القطاع الخاص وتنميته " [٥٨]؛ كما نص في مادة أخرى على:" تنظم بقانون الاحكام الخاصة بحفظ املاك الدولة وإدارتها وشروط التصرف فيها والحدود التي لا يجوز فيها النزول عن شيء من هذه الاموال " [٥٩]. و ما تقدم يوضح ما سعى له المشرع العراقي في سبيل وضع البنية التحتية القانونية اللازمة؛ لحماية المجال الاقتصادي من الأخطار المعلوماتية، فألزم الدولة بحماية الاقتصاد ووضع أسس اقتصادية حديثة بما فيها الأمن و الردع السيبراني، كما ألزمها بإصدار القوانين اللازمة لحفظ وإدارة أملاك الدولة، بحيث يشمل ذلك القوانين التي تنظم المعاملات الإلكترونية في المجال الاقتصادي.

الفرع الثالث: المجال السياسي :المنطقة العربية شهدت في السنوات الأخيرة تحولات سياسية جذرية؛ كان سببها الأول تكنولوجيا الاتصال الحديثة، ففي مصر قامت ثورة يناير ٢٠١١، والتي أطاحت بحكم أستمر أكثر من ثلاثين عاما، و قامت هذه الثورة عن طريق الدعوات على وسائل الاتصال الحديثة بل و أستمرت تكنولوجيا الاتصال المحرك الرئيسي والأسلوب الذي تدار به الثورة. أرتبط مفهوم الأمن بكيفية استخدام الدولة لقوتها لإدارة الأخطار التي تُهدد وحدتها؛ و استقرارها السياسيّ داخليا، و في مواجهة الدول الأخرى خارجيا، وعليه فإنَّ الأمن هو ما تقوم عليه الدولة من قيم وأهداف وظيفية الإجراءات المُتعلّقة بتأمين وجودها، سلامة كيانها، استمرارها، و استقرارها كافة، وتلبية احتياجاتها وضمان مصالحها الحيويَّة وحمايتها من التداخلات الخارجيَّة؛ مع مراعاة التطورات الإقليميَّة والدوليَّة، لذا فإنَّ مفهوم الأمن مفهوم واسع، وبما أنَّ تهديد أمن الدول

يعد من أهداف التدخل السياسي، فلا بدَّ من تقسيم الأمن إلى الأمن القوميّ أو أمن الدولة، وإلى "أمن إنساني" أي: أمن الأشخاص الذين يعيشون داخل الدولة؛ و لكل منهما مفهومة الخاص به.[١٠] لذا تظهر الأبعاد السياسية للأمن السيبراني؛ بشكل أساسي في حق الدولة في حماية أمنها السياسي وكيانها ومصالحها العليا بوصفها أحد أشخاص المجتمع الدولي، وهو ما يعني حقها وواجبها في السعي إلى تحقيق الرفاهية لشعبها، وفي زمن انتشرت التكنولوجيا وتغيرت موازين القوى داخل المجتمع نفسه، فأصبح بالإمكان أن يتحول المواطن إلى لاعب أساسي يتحكم في العملية السياسية، كما أصبح بإمكانه الاطلاع على خلفيات ومبررات القرارات السياسية التي تتخذها حكومته عبر الكم الهائل من المعلومات التي يمكنه الوصول إليها أو التي يمكن أنْ تنتشر على شبكة الإنترنت وكافة الأجهزة المتعاملة معه[١١]. ولا يتوانى العاملون في الشأن السياسي عن الإفادة مما تقدمه هذه التقنيات للوصول إلى أكبر شريحة ممكنة من المواطنين والترويج لسياساتهم في العالم، وغني عن البيان مدى التأثير الذي يتركه هذا الأمر بغض النظر عن صحة السياسات والمبادئ والمواقف التي يروج لها فقد استخدم أوباما مثلاً الشبكات الاجتماعية بشكل كثيف خلال حملته الانتخابية، كما تركت التسريبات لآلاف الوثائق الدبلوماسية السرية عبر الويكيليكس أثرًا سلبياً على العلاقات بين الدول وعلى مصداقيتها [١٢]. الباحث يرى :أنَّ على المختصين بتوفير الأمن السيبراني وضع الأدوات والسياسات والمفاهيم الأمنية وضمانات الأمان والمبادئ التوجيهية وأساليب إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات والضمان والتقنيات التي يمكن استخدامها لحماية البيئة الإلكترونية والتنظيم والمستخدمين. يكون في مقدمتها نظم حماية متقدمة لرصد و منع الاختراقات، أي نظم تمكن من مراقبة و كشف كل محاولات الاختراق الرقمية، فضلا عن القدرة على منع و إيقاف هكذا اختراقات فيما لو تم رصد حدوثها، لكل الحوادث المشبوهة و المحتملة، و هذه لا تتحقق مالم تتهيأ كل الأرضيات اللازمة من تشريعية و تنظيمية و تقنية و تدريبية اعدادية على وفق أكثر التقنيات المتطورة، و هذا بالتأكيد جهد دولة بأكملها؛ لا جهازا واحدا أو وزارة أو مؤسسة بعينها من دون الأخريات.

المطلب الثاني :الأساس الدستوري لتحقيق الردع السيبراني في العراق و مدى كفايته: نص دستورنا الحالي لعام ٢٠٠٥، على أنْ: "يحترم العراق الاتفاقيات الدولية" أي يحترم التزاماته الدولية كافة الناشئة عن مختلف الاتفاقيات الدولية، فهي تعلو على القواعد الداخلية كلها بما في ذلك الدساتير، إذ قال المشرع الدستوري العراقي:"يرعى العراق مبدأ حسن الجوار، ويلتزم بعدم التدخل في الشؤون الداخلية للدول الاخرى، ويسعى لحل النزاعات بالوسائل السلمية، ويقيم علاقاته على اساس المصالح المشتركة والتعامل بالمثل، ويحترم التزاماته الدولية " [١٣] . فمن المعروف في علم القانون إنَّ أي تشريع داخلي لابد أنْ يكون متفق مع قواعد القانون الدولي، وإذا خالف القانون الدولي حينئذ لا يعترف له بشرعية ما؛ وكذلك الحال في تحديد الأطر الدستورية لتحقيق الردع السيبراني، فيجب أن تكون القوانين المنظمة لهذا لردع؛ متماشية مع ما صدق عليه العراق من اتفاقيات أو

معاهدات دولية. وفي المجال العملي نجد أنَّ العراق قد وقع على عدة اتفاقيات تهدف إلى تنظيم التعاون مع دول الجوار لتنظيم مسألة الأمن المعلوماتي. ونتناول في هذا المطلب بحث مسألة الأساس الدستوري الردع السيبراني في العراق و مدى كفايته في فرعين على النحو التالي :

الفرع الأول :الاساس الدستوري للردع السيبراني في العراق: إنَ المتأمل لدستور العراق، و على الرغم من صدوره عام ٢٠٠٥ في وقت كانت الدول العربية حديثة عهد بموضوع الأمن السيبراني، وبالرغم من أنه لم يتناول هذه القضية بصورة مباشرة؛ إلا أنه من الممكن البحث عن إطار قاعدي أو بنية تحتية تصلح كإطار عام لرسم السياسة العراقية للردع السيبراني. فقد نص الدستور العراقي في المادة ٧ / ثانياً على أنْ :" تلتزم الدولة محاربة الارهاب بجميع اشكاله، وتعمل على حماية اراضيهامن أن تكون مقراً أو ممراً أو ساحة لنشاطه "(١٤). فمن هذه المادة يمكن القول بأن الدستور العراقي ألزم الدولة بمحاربة الإرهاب بجميع أشكاله بما في ذلك الإرهاب الإلكتروني، ولا يقتصر الامر على ذلك، بل إنه رفض و نهى من أنْ تكون أرض العراق مقر للجماعات التي تقوم بأعمال الهجمات الإلكترونية بوصفه نوعا من الإرهاب الدولي. في المادة ١٥ أكد المشرع الدستوري على حق الحياة المهم للشخص و صيانته ليس هو فحسب بل كل ما يتعلق به؛ إذ قال: " لكل فرد الحق في الحياة والأمن والحرية، و لا يجوز الحرمان من هذه الحقوق أو تقييدها إلا وفقاً للقانون، وبناءً على قرار صادر من جهة قضائية مختصة "(١٥). فالدستور العراقي كفل الحق في الحياة الأمنة لكل مواطن عراقي، والأمن السيبراني يعد حق من حقوق الإنسان – كما سبق – ف بالتالي يدخل ضمن طائفة الحقوق المحمية، مما يدل على أنَ الأمن السيبراني جزء من حياة الإنسان وحقوقه. ولم يغب عن المشرع الدستوري الحديث عن حماية خصوصية المواطن، ف خصص له المادة ١٧/ أولاً فنص على أن: " لكل فرد الحق في الخصوصية الشخصية بما لا يتنافى مع حقوق الاخرين والآداب العامة "(١٦). يمثل الحق في الأمن السيبراني الصورة المثلى للحق في الخصوصية فأجهزة الأشخاص الإلكترونية ومواقعهم الإلكترونية محمية بكلمات السر لما لها من خصوصية، وهي بالتالي تخضع لحماية الدستور والذي كفل الحق في الخصوصية. و في المادة (٤٠ ) لم ينسى المشرع الدستوري التأكيد على أن " حرية الاتصالات والمراسلات البريدية والبرقية والهاتفية والالكترونية وغيرها مكفولة، ولا يجوز مراقبتها أو التنصت عليها، أو الكشف عنها، الا لضرورة قانونية وأمنية، وبقرار قضائي " (١٧). و من المادة أعلاه يتضح أنها تعد أساسا قاعدي؛ وبنيه تحتية دستورية للحق في الأمن السيبراني. فقد جاءت بصورة مباشرة لتنص على الحق في الأمن المعلوماتي لضمان الردع السيبراني، بصراحة نصها على حماية حرية الاتصالات والمراسلات الإلكترونية. كما منعت هذه المادة مجرد مراقبة أو التصنت على الاتصالات الالكترونية؛ و بصورة أولى منعت الهجمات الإلكترونية، فضلا عن منعها التعرض لحرية الاتصالات الإلكترونية.

الفرع الثاني: الأمن السيبراني وحقوق الإنسان الرقمية: عززت الدساتير فكرة حقوق الإنسان، فعلى سبيل المثال نجد الدستور العراقي قد أفرد الباب الثاني منه للحقوق والحريات، وقد وضع بنية تحتية لتنظيم الحقوق الرقمية، إذ قد عدَ الأمن السيبراني من

ضمن حقوق الإنسان، بل إنّه أدخل الحقوق الرقمية من ضمن طائفة الحريات التي كفلها للمواطن العراقي، أخذ المشرع الدستوري العراقي بالتأسيس لحقوق الانسان بشكل عام؛ و لحقوقه الرقمية بشكل خاص على أسس عالمية متقدمة تراعي كافة متطلبات توفير الحماية لهذه الحقوق من نصوص قانونية و مؤسسات تسهر على متابعة احترامها، ف وفقا لمبادئ باريس عمل قانون إدارة الدولة للمرحلة الانتقالية للنص على هذه الحقوق و مؤسسات حمايتها، ف جاء فيه: " تؤسّس الحكومة العراقية الانتقالية هيئة وطنية لحقوق الإنسان لغرض تنفيذ التعهّدات الخاصّة بالحقوق الموضحة في هذا القانون. وللنظر في شكاوى متعلّقة بانتهاكات حقوق الإنسان. تُؤسَّس هذه الهيئة وفقاً لمبادئ باريس الصادرة عن الأمم المتحدة والخاصّة بمسؤوليات المؤسّسات الوطنية. وتضمّ هذه الهيئات مكتباً للتحقيق في الشكاوى. ولهذا المكتب صلاحية التحقيق بمبادرة منه أو بشكوى ترفع في أيّ ادّعاءٍ بأنّ تصرفات السلطات الحكومية تجري بغير وجه حقٍّ وخلافاً للقانون).[١٨] و على الرغم من إنّ الهيئة المذكورة لم يتم تشكيلها لقصر مدة نفاذ القانون المذكور، إلاّ إن النص اعلاه قد جاء متوائما بالفعل مع ما ورد في مبادئ باريس، و يعبر عن ايفاء دولة العراق لما تعهد به من صيانة لحقوق الانسان، و الامتثال لها و الايمان بجدواها و ضرورتها للمرحلة الراهنة، و قد أضفى هذا النص على المفوضية العليا لحقوق الانسان التي أنشئت لاحقا؛ خاصية الاستقلال عن كل سلطات الدولة الأخرى، وهو ما يجسد مبادئ باريس التي أوجبت هذا الأمر في انشاء المؤسسات الوطنية ذات الطابع المستقل، إذ أن هذا الشرط يضمن استقلالية هذه المؤسسة في عملها و الحد من امكانية خضوعها للضغوطات، مما يسهل عليها أداء مهامها في مجال الحقوق الإنسانية كافة، بما في ذلك الرقمية منها. أما عند صدور دستور ٢٠٠٥، أكد المشرع الدستوري فيه على ذات نهج المشرع في الدستور السابق من صيانة حقوق الانسان و تشكيل المؤسسات ذات العلاقة بحمايتها و متابعة احترام السلطات لها، فنص في الفصل الخاص بالهيئات المستقلة على : ( تعد المفوضية العليا لحقوق الانسان ..... هيئات مستقلة تخضع لرقابة مجلس النواب، و تنضم أعمالها بقانون)[١٩]. و يلحظ اخضاع المشرع الدستوري مفوضية حقوق الانسان لرقابة مجلس النواب من دون ان يكون ذلك ماسا باستقلالها، إذ أن الرقابة هنا ستقتصر على تقديم التقارير السنوية الخاصة بحقوق الانسان و مناقشتها امام المجلس المذكور، و تلقي الشكاوى من المواطنين ممن تضررت حقوقهم جراء أعمال السلطات.[٧٠] و في موضع آخر نصَ على أنَّ: " حرية الاتصالات والمراسلات البريدية والبرقية والهاتفية والالكترونية وغيرها مكفولة، ولا يجوز مراقبتها أو التنصت عليها أو الكشف عنها الا لضرورة قانونية وأمنية، وبقرار قضائي " (٧١). فقد كفل الدستور العراقي الحرية الرقمية وحماها من الهجمات السيبرانية، حقوق الإنسان الرقمية هي حقوق الإنسان التي تسمح للفرد بالوصول إلى الإعلام الرقمي واستخدامه وإنشائه ونشره أو الوصول إلى أجهزة الحاسوب وغيرها من الأجهزة الإلكترونية أو شبكات الاتصال واستخدامها (٧٢). ويعد من أبرز الضوابط القانونية في مجال الردع السيبراني، ضمان بعض الحقوق في هذا مجال الحقوق الرقمية كالحق في النفاذ إلى الشبكة العالمية للمعلومات، وأيضاً توسعت

بعض المفاهيم لتشمل أساليب الممارسة الجديدة باستخدام تقنيات المعلومات والاتصالات، كالحق في إنشاء المدونات السيبرانية، الحق في إنشاء التجمعات على الإنترنت، و الحق في حماية ملكية البرامج المعلوماتية(٧٣).

وتتميز حقوق الإنسان بالطابع العالمي، وقد عقدت عدة مؤتمرات عالمية لتقنين الحقوق الرقمية، فقد جاءت القمة العالمية لمجتمع المعلومات التي عقدت في تونس في دورتها الثانية ٢٠٠٥ لتؤكد على الطابع العالمي لجميع حقوق الإنسان والحريات(٧٤). وصدر في مايو ٢٠١١ تقرير تضمن توصيات المقرر الخاص للأمم المتحدة والتي قدمها إلى مجلس حقوق الإنسان في الجمعية العامة للأمم المتحدة، ذكر هذا التقرير أن شبكة الإنترنت هي واحدة من أقوى أدوات القرن التي تمكن من زيادة الشفافية ومن سرعة الحصول على المعلومات، وتسهيل مشاركة المواطنين في بناء مجتمع ديموقراطي، واستناداً إلى وقائع من المظاهرات الأخيرة في جميع بلدان الشرق الأوسط وشمال أفريقيا، أدت شبكة الإنترنت دوراً رئيسياً في تعبئة السكان، للدعوة للتظاهر من أجل العدالة، المساواة، المساءلة، واحترام أفضل لحقوق الإنسان.(٧٥) وبالتالي يعد الفضاء السايبر، ذا دور فعال في ممارسة حقوق الإنسان، وأن أي مخاطر في هذا الفضاء تؤثر على تلك الحقوق لاسيما في الصحة البشرية والسلامة والرفاهية، ولذلك نادى البعض بضرورة إنشاء وحدات خاصة لمكافحة الجريمة المعلوماتية بواسطة الحاسب والإنترنت، وذلك أسوة بجهات البحث الجنائي الدولية "الإنتربول" لإثبات الجريمة السيبرانية وتحديد أدلتها وفاعليها، كما تهدف إلى إيجاد صيغة ملائمة للتعاون الدولي لمكافحة هذه الجرائم الخاصة بالحاسب وشبكة المعلومات الدولية ويكون من عملها تبادل الخبرات والمعلومات حول هذا النوع من الجرائم ومرتكبها وسبل مكافحتها (٧٦). إنَّ كل عملية إرهاب سيبراني؛ وكل خطوة من الحرب على الإرهاب، ينتج عنها تقلص في الحريات الشخصية؛ حيث زيادة سطوة الجانب الأمني ورجاله على الجانب القانوني؛ ولا يختلف في ذلك كون تلك الحكومات ديمقراطية أو ديكتاتورية، فالانتهاك قد شمل الجميع (٧٧).

المطلب الثاني: الإطار القاعدي لتجسيد استراتيجية الأمن و الردع السيبراني في الدستور العراقي: استراتيجية العراق في الأمن و الردع السيراني، هي سياسة و تدابير الاستعداد الوطني، تحتوي على إجراءات متماسكة لضمان أمن و حماية الوجود العراقي في الفضاء السايبر؛ فضلا عن حماية البنية التحتية المعلوماتية، و بناء و رعاية مجتمع إنترنت موثوق به، في العادة تتألف استرتيجية الأمن المعلوماتي من استراتيجيات عدة، قصيرة، متوسطة، و طويلة الأمد، لتغطي جميع الأولويات الوطنية، و تعالج كل مسائل التعرض الوطني لكافة المخاطر السيبرانية، إذ ثبت من الواقع العملي وجود تهديدات سيبرانية فعلية مصدرها من كافة أنحاء العالم و التي تضر بالمصالح الوطنية للدولة و أفرادها.(٧٨) هذه الاستراتيجية تحوي على مبادرات مختلفة في المجالات المركز عليها، لاسيما الاطار التشريعي و التنظيمي، وضع الآليات الوطنية لتسهيل تنفيذ الحكومة الالكترونية الفعالة؛ فضلا عن الاطار تكنولوجي متقدم لتوفير ثقافة سيبرانية، مما يضمن معه تحقق الوعي بالأمن السيبراني و تهديداته؛ للوصول للردع المطلوب في فضاء المعلومات الرحب.

بناء القدرات العلمية، في البحث و التطوير المستمر للتقنيات المطلوبة للأمن المعلوماتي، بغية الوصول إلى مرحلة الاعتماد على القدرات الذاتية في توفير مختلف الخدمات الإلكترونية، بما في ذلك البرمجيات المطلوبة التي سيعدها مهندسون وطنيون يتم اعدادهم خصيصا لهذا الغرض، على أنْ لا يتم نسيان ضرورة تطوير آليات التعاون الدولي و الإقليمي؛[٧٩] في هذا الموضوع فائق الأهمية، وهنا لابد من طرح التساؤل الآتي: لماذا يجب على الحكومة أنْ تعد الفضاء الالكتروني من أهم أولوياتها؟ بما أنه من الثابت أن لكل دولة ثلاث مجالات مهمة هي الأرض و الماء و الجو، الجواب هو أنَّ الفضاء السايبر هو المجال الرابع الواعد لكل دولة، لما له من تأثير فعال و واضح في قيادة المهام الوطنية الحرجة مثل التنمية الاقتصادية الوطنية، التجارة، المعاملات، التفاعلات الاجتماعية، العمليات الحكومية، الواقع الصحي الطبي، و أخيرا الأمن القومي و الدفاع الداخلي. قطعا فإنَ توفير الأمن للبنية التحتية المعلوماتية الحيوية، في نظام معلومات الدولة و في ضل الوضع الراهن؛ هو تحد وطني ضخم، إذ يحتاج الأمن الوطني إلى إطار متماسك من الردع السيبراني، لتوفير نهج شامل إزاء المشهد الأمني الحالي و المستقبلي، لأنَّ أمن الدولة و التضاريس و الاقتصاد يسير بخطى سريعة؛ و يتجهان نحو تضاريس رقمية متحركة متنقلة و بسرعة، فالجهات الفاعلة "حكومية و غير حكومية" التي تتورط في الهجمات السيبرانية مجهزة تجهيزا كافيا بأحدث الأدوات و التقنيات الالكترونية؛ مما يمكنها من التسبب في أضرار ذات أبعاد لم يسبق لها مثيل؛ و من شأن إدراج الأمن السيبراني في مجال الاهتمام بالفضاء الإلكتروني، أنْ يساعد البلد على الاستعداد و الاستجابة لهذه التهديدات المستحدثة بما يحقق الردع المطلوب.[٨٠] يُعد (الأمن الإنسانيّ)[٨١]، من المفاهيم الحديثة للأمن بصورة عامَّة؛ إذ يتمحور حول التهديدات التقليديَّة للدولة ومنها النزاعات المُسلَّحة، حينما يجدُ الفرد نفسه في وسط صراعات لا دخل و لا ذنبَ له بها، ومع ذلك يكون هو الضحية الأكبر بكل ما للكلمة من معنى، ولكن في دراستنا للأمن الرقميّ ستتناول الأمن الإنسانيّ من ناحية مختلفة، وهي هل يحقق زعزعة الأمن الإنسانيّ هدفًا من أهداف الهجوم الرقميّ؟ هذا ما يفسر كون قضية الأمن السيبراني؛ أصبحت من أهم استراتيجيات الأمن القومي للعديد من الدول ومنها العراق، وذلك من أجل الاستحواذ على مصادر القوة اللازمة داخل الفضاء السيبراني، في محاولة لمنع تعرض بنيتها التحتية للخطر الذي قد يحدث جراء قطع خدمة الإنترنت، أو ضرب مواقعها أو توقف رسائل البث الإذاعي أو التلفزيوني، أو توقف موجات الراديو أو سقوط شبكات المحمول أو البث الفضائي، وأصبح لها تأثير عميق على المجتمع والاقتصاد على النطاق الدولي (٨٢). ونتج عن ذلك أنَّ قضية الردع السيبراني قد فرضت نفسها كبعد جديد ضمن أبعاد الأمن الدولي، وترتب عليه إحداث تغييرات جوهرية في مفاهيم العلاقات الدولية كطبيعة الصراعات والتهديدات بين الدول، مما حتم على المجتمع الدولي الانتقال من عالم مادي إلى عالم افتراضي في غاية التعقيد والتشابك (٨٣). ومع تأخر الدساتير في تقنين قضية الأمن و الردع المعلوماتي؛ بل تأخرها عن تقنيات الحقوق الرقمية للإنسان، كان لابد من البحث عن إطار لتحقيق الردع السيبراني في القانون الدولي بوصفة من أهم المصادر المكتوبة للدستور.

إن الهدف الأساسي من إثارة موضوع للأمن السيبراني هو الكشف عن قدرة الدولة على مقاومة المخاطر السيبرانية التي تهدد الدول، وبالتالي التحرر من الخطر أو الأضرار الناجمة عن إساءة استخدام تكنولوجيا المعلومات والاتصالات، مما يتطلب حماية المجتمع المعلوماتي داخل حدود الدولة، وفي الآونة الأخيرة ظهرت تهديدات عديدة للأمن السيبراني حتى وصل الحد بالفقهاء بإطلاق مسمى "الحرب السيبرانية".[٨٤] فظهرت قضية الأمن السيبراني على الساحة الدولية وثار التساؤل عن أسلوب التعامل مع الأسلحة التي تستخدم الذكاء الاصطناعي والمستخدمة في عمليات التجسس و اختراق شبكات الدول، فظهر خلاف حول مدى إمكانية إخضاع تلك الأسلحة لقيود حظر استخدام القوة في العلاقات الدولية ولاتفاقيات الحد من التسلح أي باعتبارها أسلحة تقليدية (٨٥).

يعد مبدأ حظر استخدام القوة أو التهديد بها في العلاقات الدولية من المبادئ الأساسية التي نص عليها ميثاق الأمم المتحدة في المادة ٢ الفقرة ٤ منه والتي نصت على أن: "يمتنع أعضاء الهيئة جميعا في علاقاتهم الدولية عن التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو على أي وجه آخر لا يتفق ومقاصد الأمم المتحدة".

و عند تأمل ميثاق الأمم المتحدة نجد أنَّ نصوصه لم تحدد مدلول كلمة "القوة"، وهو ما أثار خلافا فقهيا حول مدى اعتبار "الهجمات السيبرانية" تدخل تحت مفهوم القوة من عدمه، و انقسم إلى اتجاهين:

الاتجاه الأول: ذهب إلى أن لفظ القوة الوارد في المادة( ٢/ ف / ٤) من ميثاق الأمم المتحدة يجب تفسيره تفسيراً ضيقاً، من ثم فإنه لا يعتد بغير القوة المسلحة ولا يدخل ضمن تعريف القوة الأشكال المختلفة من القوة، وبالتالي لا تدخل ضمن هذا الحظر والدليل على ذلك ما جاء في ديباجة الميثاق بمنع استخدام القوة المسلحة إلا للأغراض العسكرية(٨٦).

الاتجاه الثاني: يرى أنصار هذا الاتجاه أنَ الضغوط الاقتصادية وكافة الأعمال الانتقامية سواء منها ما اتخذ شكل القوة المسلحة أو غيرها من الأعمال المشابهة تدخل في نطاق مدلول كلمة القوة التي حظرها الميثاق، حيث أن الميثاق قد أوضح أن القوة هي كل عمل ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة والتي تتفق مع مقاصد الأمم المتحدة وليست القوة المسلحة وحدها (٨٧).

ومن وجهة نظر الباحث؛ إن العبرة بما تحدثه الهجمات السيبرانية من أضرار جسيمة، ومن ثم يمكن أنْ تشمل كلمة القوة كافة الضغوط السياسية والاقتصادية، فضلا عن استخدام كافة أشكال القوة الأخرى كهجمات الفضاء السيبراني [٨٨]؛ من القوى المحظور استخدامها في العلاقات الدولية، ويعد ذلك التطور الطبيعي لمفهوم القوة تماشياً مع المستحدثات العالمية في مجال الاتصالات والتكنولوجيا وأثرها على سيادة الدول.[٨٩]

المبحث الثالث: السلطة المختصة برسم سياسة الأمن و تحقيق الردع السيبراني في العراق: سياسة الأمن من أهم مفردات السياسة العامة لكل دولة، و تضعها في مقدمة أولويات عقيدتها الأمنية و الردعية، هذا ما جعل السياسة العَامّة، تعد مَن الركائز الأسَاس التي يقاس بِها نَجَاح الدولة أو فشلها, لَذا تَسْعَى الحكومات فِي مُختَلَف النظم

إلى رسم سيَاسَة عَامّة متطورة وكفؤة؛ لتعالج بها مشاكَلّ المجتمع كافة, السياسة العَامّة سيتضح بأنها نشاط تقوم به الحكومة, أي هي نشاط حكومي بحت؛ ولهذا كلما نسمع أو يتم ذكر مصطلح " سياسية عامة"، لابد أنْ ينصرف الذهن إلى ذلك النشاط الحكومي الفني الذي تتخذه في سبيل ترجمة برنامجها الحكومي و تجسيده على أرض الواقع بما يضمن بأنْ يعود على الدولة و مواطنيها بالنفع العام, و تحقيق الرخاء و الرفاهية المنشودين لمواطنيها كافة. و في هذا المبحث سيحاول الباحث الاجابة عن هل استغلت السلطة التنفيذية في العراق صلاحياتها الدستورية لمعالجة مشكلة تعزيز الأمَن السيبراني؟ أم لمّ تقم بذلك؟ ومما لا شك فيه أنَّ تشريعات الأمن السيبراني حديثة النشأة على الساحة القانونية [٩٠]، لذلك أهتم العراق به كثيرًا بسبب المخاطر المحيطة بها وقد وضعت أطر قانونية في ظل الدستور تعمل على توفير الأمن السيبراني للعراق بحكومته و أفراده ومؤسساته, إذ تهدف الاستراتيجية العراقية إلى حماية الدولة من تهديدات حوادث الهجمات السيبرانية؛ وبناء قدرات وطنية تضمن مواجهة التهديدات التي تعترض أنظمة المعلومات والبنية التحتية الخاصة بها كل ذلك لتحقيق الردع المنشود في هذا المجال. ولهذا سأقسم المبحث على مطلبين؛ الأول أخَصِّصُه لدراسة السلطة التنفيذية بوصفها مختصة برسم سياسة الأمن في العراق بكافة تفاصيله, و الثاني لدراسة أنواع اختصاصات السلطة التنفيذية:

المطلب الأول: السلطة المختصة برسم السياسة العامة للأمن و الردع السيبراني في العراق: عدت السلطة التنفيذية في الأنظمة البرلمانية الحَجَر الأسَاس في إدارة شؤون الدولة, إذ تمنح لهَا العَديد مَن الاختصاصات في مَجَالات متعددة, تستطيع بوساطتها أنّ تَتَصَدَّى لمخَاطِرُ الأمن الأَلكتروني كافة؛ التي تعد مَن أخطر التهديدات السيبرانية. وعَلَى المستوى التَشْرِيعي يحق لهَا أنْ تقترح مشاريع القوانين الخاصّة في حماية الأمَن السيبراني, ولهَا أنّ تقترح تعديل النَصّوص الدستورية التي تتعلق بحماية الاتصالات أو البيانات, ولهَا في المَجَال السيَاسيّ أنّ تعقد المعاهدات والاتفاقيات أو تنظم إلَيْهَا خاصّة في مَجَال حماية الأمَن السيبراني للدولة, أما مَن حَيْث اختصاصاتها ذات الطابع الإداري والتنفيذي, فلهَا الأثر في مداولة الأفكار اقتراح مشروعات القوانين وغَيْرها في جَلَسَات مجلس الوزراء, ولهَا أنّ تصدر قرارات أو تعليمات أو أنْظمَة تَطْبِيقا للقوانين بما يحقق الصالح العَام, يفترض في النظام السياسي العمل على حفظ ذاته من خلال مؤسسات يبنيها, وقواعد يقررها وممارسات يلتزم بها وعلاقات يدخل فيها ووظائف يؤديها؛ تتمثل وظائف المدخلات وفقاً للمدخل الوظيفي في كل من التنشئة السياسية والاتصال السياسي وتجميع المصالح والتعبير عنها, بينما تتمثل وظائف المخرجات في صنع القواعد القانونية وتنفيذها والتقاضي بموجبها.[٩١] وقد تشترك النظم السياسية كافة في مجموعة من الوظائف وفقاً للتحليل الوظيفي بالمدخلات وتضم: بلورة المصالح وتجميعها, و المخرجات وتضم: صنع القانون وتطبيق أحكامه؛ بينما كيفية أداء الوظائف قد يختلف من نظام إلى آخر, وهذا يعني أنَّ الوظائف هي نفسها ولكن أدوات إنجازها تختلف. تعرف السياسة العَامّة بأنّها" كَلّ تصرف أو قرار تقوم به الحكومة أو مَن يمثلهَا للتدخل

بشؤون المجتمع وحَلّ المشاكَلّ التي تواجهها داخليا أو خَارِجِيّا ". بينما عرفها :توماس داي" بأنها: "كَلّ مَا تقرر الحكومة عمله أو عدم عمله"[٩٢]؛ ف السياسة العامة بحق هي "العلاقة بين الوحدة الحكومية و بيئتها". و بهذا ندلل على الاصل الحكومي للسياسة العامة، رغم أن التعريف المتقدم و بسبب من سعته قد يجعل أغلب الدارسين غير متأكدين من حقيقة المعنى وقد لا يسعفهم كثيرا للفهم، الأمر هذا دفع بجانب فقهي آخر لطرح تعريف جديد بأسلوب أكثر بساطة ليساعد على الفهم، ف قالوا: "هي تقرير أو أختبار حكومي للفعل أو عدم الفعل". وهذا التعريف يفصح عن السياسات العامة الايجابية و السلبية على حد سواء؛ كما قد ينصرف إلى أعمال لا يبدو أنها تدخل ضمن أطار السياسة العامة، كتعيين شخص أو منح شهادة.[٩٣] يبدو ان السياسة العامة هي آليات و برامج تطورها الأجهزة الحكومية من خلال مسؤولياتها، علما توجد قوى أخرى غير حكومية(غير رسمية) قد تساهم هي الأخرى أو تؤثر بأي شكل كان في رسم و تطوير بعض السياسات العامة، و تستمد خصوصيتها من كونها متخذة من قبل السلطات المخولة من جانب النظام السياسي القائم و الحاكم.

وهنا لابد من تحديد بعض المفاهيم للسياسة العامة على وفق التعريفات السابقة:

١- إنها تشمل الأعمال الموجهة نحو أهداف مقصودة، و يخرج منها التصرفات العشوائية و العفوية التي تصدر من بعض المسؤولين، فالسياسات العامة في الأنظمة السياسية لا تتضمن أشياء تحدث توا و صدفة، بل أمور تدرس بعناية.

٢- إنها تشمل البرامج و الاعمال المنسقة التي تصدر عن القادة الحكوميين، و ليست القرارات المنفصلة المنقطعة، فهي تشمل ما تشتمل عليه المراسيم التشريعية و القرارات التنفيذية لها.

٣- إنها تشمل على جميع القرارات الفعلية المنظمة و الضابطة للتجارة أو لمعالجة التضخم أو لمعالجة مشكلة السكن، و لا تشمل ما تنوي الحكومة أن تفعله أو تعد لفعله الا على نحو محدود، ذلك أن الوعود و الأماني الحكومية ليست من السياسة العامة في شيء.

٤- كما قد تكون السياسة العامة إيجابية، فهي ممكن أن تكون سلبية في صياغتها كذلك، فهي قد تأمر بالتصرف باتجاه معين؛ وقد تنهى فقط عن القيام بتصرفات غير مرغوبة، أو قد يعد سكوتها أو عدم التزامها بالتصرف إزاء ظواهر معينة بمثابة توجه.[٩٤]

و لقد عرفنا أن السياسة العامة إنما هي مجموعة من الاستراتيجيات الحكومية الرئيسة، و من ضمنها استراتيجية الأمن العام؛ و من ثم ف الحكومة هي المعنية برسم و وضع السياسة العامة و الاستراتيجيات المتعلقة بها[٩٥]، المنطق يفرض أنْ تكون سياسة الأمن الوطني من ضمن سياسات الحكومة الأصيلة، وهي تأخذ على عاتقها مهمة وضعها و تنفيذها، لذا فعملية وضع سياسة للأمن الوطني تمر بالخطوات الآتية: ١-رسم سياسة للأمن الوطني، يكون الأمن المعلوماتي من أهم مفرداتها، ٢-وضع آليات تنفيذ هذه

السياسة و تحديد الأجهزة المختصة بهذا التنفيذ. ف بالنسبة للنقطة الأولى، ستكون عملية رسم سياسة الأمن الوطني هي العملية المحورية، و التي تبدأ بها السلطة المختصة بهدف الوصول إلى اتفاق على تعريف المشكلة الأمنية و معرفة وجوه حلها كافة، و ما هي أسس المفاضلة التي ستعتمد في ترتيب أولويات معالجة المشكلات، كتمهيد للبديل الذي سيقترح إقراره في شكل سياسة عامة، وفي هذا كما عرفنا ستشترك جهات حكومية و غير حكومية. و بناء على تلك الاختيارات يقوم المشرع بتشريع القوانين، و في العراق تتشارك السلطتين التشريعية و التنفيذية في هذه المهمة، ف الثانية تضع مشروع التشريع و الثانية تناقشه و تقره بسنه، لتمثل بعد ذلك أسسا تستند عليها السلطة التنفيذية في تنفيذ سياسة الأمن الوطني، و لها في ذلك و بطبيعة الحال أن تضع الأنظمة التفصيلية التنفيذية لوضع هذه التشريعات موضع التنفيذ، أما عن النقطة الثانية، فتبقى مسألة اتخاذ القرار السياسي المتعلق بالأمن الوطني هو نهاية لعملية صنع السياسة الأمنية، و البداية العملية للتنفيذ لكل التشريعات و الانظمة الموضوعة سلفا، و القرار السياسي هذا يمثل التجسيد المادي لنتيجة التفاعل و الصراع السياسي بين الأطراف المعنية في إطار النظام السياسي القائم، ف السلطة التنفيذية بمجرد صدور القانون المطلوب و اكتمال ولادته التشريعية، تصبح هي المسؤول الأصيل عن تنفيذ محتواه الذي جاء تجسيدا للسياسة التي رسمت سلفا في مجال الأمن . و لسنا بصدد ترف علمي لما نقول ان التنفيذ هو ترجمة للأهداف التشريعية و السياسية كافة، فهوي برامج و نشاطات و اجراءات و خطوات عمل مستقلة مهنية متخصصة متكاملة بين اجهزة مختصة يعمل بها موظفين بمختلف الوحدات التنظيمية المكونة للإدارة الأمنية.[٩٦] إنَّ إستراتيجية الأمن السيبراني الوطني بشكل عام، هي: "كافة التدابير المتعلقة بسرية المعلومات والبيانات التي يتم معالجتها وتخزينها وإبلاغها عن طريق وسائل إلكترونية أو مشاة، وحمايتها والنظم المرتبطة بها من التهديدات الخارجية أو الداخلية". تمثل عملية بناء بنية تشريعية الخطوة الأولى لتحقيق الأمن السيبراني، إذ ستعمل تلك البنية على الحماية من أشكال المخاطر السيبرانية كافة؛ من خلال تعزيز سلامة البنية التحتية الحيوية للمعلومات التي تعتمد عليها القطاعات الحساسة، وكذلك تأمين الشبكات والخدمات التي توفر الاحتياجات اليومية للمستعملين من خلال تجريم التعدي على الامن السيبراني. ويقصد بالإطار التشريعي: إطار يرسم حدود القوانين والأنظمة المنبثقة عنها؛ التي قرر المجتمع أن يعمل في ظلها و التي وضعتها السلطة المختصة في الدولة؛ في صورة مكتوبة بوصفها قواعد ملزمة لتنظيم العلاقات في المجتمع طبقا للإجراءات المقررة لذلك، بمعنى أن التشريع الأمني كمصدر من مصادر القانون يقصد به عملية سن القواعد القانونية ذات العلاقة بحفظ الأمن، و إخراجها بألفاظ و إجراءات معينة بواسطة سلطة مختصة بذلك؛ لضمان تحقيق أهدافها.[٩٧] و تؤثر التشريعات الوطنية على أدوار السلطات الامنية من حيث نجاعة أو عدم نجاعة ما يتخذ من تدابير أمنية لضمان حماية أمن الفضاء المعلوماتي، لذلك ستحتاج الأجهزة التابعة للسلطات هذه إلى التفكير ليس فقط في نطاق سلطاتها التشريعية؛ ولكن أيضاً

في الأحكام القانونية التي ستؤثر في قدرتها على إعلام وتوعية المواطنين وتحقيق المشاركة الشعبية في عملها الهادف لضمان أمنهم السيبراني، و يمكن أجهزة الأمن المعنية من تحقيق الردع المطلوب في مواجهة الهجمات في الفضاء السايبر. و بالرغم من أن دستور العراق لعام ٢٠٠٥، قد وضع البنية التحتية لضمان و حماية الحقوق الرقمية وضرورة توفير الأمن والسلم الرقمي للعراق؛ لا يختلف العراق عن غيره من دول العالم، إذ يعد من الدول التي تواجه تحدي الفضاء السيبراني في مختلف مجالاته سالفة الذكر، ويزداد الأمر سوءًا حيث حالة الضعف التي يعيشها، كما تمثل مشكلة عدم الاستقرار العام دورًا كبير في التهديد السيبراني؛ فضلاً عن ضعف امكاناته المطلوبة للتكيف مع تلك التحديات التي يفرضها الفضاء السيبراني. ومع ظهور عملية الانتقال السريع للمجتمعات من الفضاء الحقيقي إلى الفضاء الافتراضي، وجد العراق نفسه يدخل إلى هذا الفضاء الواسع دون إرادة منه، ودون إعداد بنية تشريعية ملائمة، فلم يمر بمرحلة انتقالية، فالبنى المادية والبشرية في العراق لا تزال غير قادرة على التفاعل الايجابي مع تحديات للفضاء السيبراني، وعند البحث في الامكانيات العراقية في مجال الامن السيبراني سوف نجد بأنّ العراق بحاجة إلى الكثير من الجهد المعرفي والاداري والقانوني والتقني، حتى يصبح قادرًا على حماية أمنه من التهديدات السيبرانية المتنوعة و المتطورة (٩٨). فالوضع في العراق مازال يحتاج إلى مزيد من الجهد والعمل لبناء إطار قاعدي لتحقيق الردع السيبراني ، حيث نجد أن العراق وعلى الرغم من التحسن الذي حدث في موقعه في مؤشر عام2018 حيث شغل ( ١٠٧ ) عالمياً و ( ١٣) عربيا، إلا أنه تراجع نحو ( ٢٢) نقطة في مؤشر العام 2020 ليكون ( ١٢٩ ) عالمياً من أصل ( ١٨٤ ) دولة و ( ١٧) عربياً بدرجة ( ١٧.٢٠ ) (٩٩). ربما هذا يفسر حاجة العراق فعلا لضمان الأمن المعلوماتي، وإنْ كانت هناك عوامل عدة قد أدت إلى تلك الضرورة ، حيث لا يزال قانون جرائم المعلوماتية لم يصوت عليه بالرغم من القراءة الاولى له، وتبدل نسخه لعدة مرات بطريقة تثير المخاوف على الحريات العامة (١٠٠). فالتطور التكنولوجي الذي شهده العراق في مجال الاتصالات وتكنولوجيا المعلومات منذ عام ٢٠١٣ والذي واكب ضعف الإمكانيات الأمنية الإلكترونية في البنية التحتية الوطنية، وعدم وجود تشريع يضبط عملية الأمن السيبراني، كل ذلك نتج عنه أن أصبح العراق منكشفاً استراتيجيا لكثير من جماعات الإرهاب السيبراني؛ ومن السهل القيام ب اختراقه والتجسس على المعلومات الخاصة بالمؤسسات والأفراد، بل ويظهر الخطر الأكبر إذا تمكنت تلك الجماعات الإرهابية من استخدام العراق كساحة لشن الهجمات الإلكترونية؛ لضرب أمن معلومات أي دولة كانت واختراقه، فضلاً عن استراق أي معلومة واستخدامها لأغراض المساومة، وتنفيذ عمليات إرهابي، وهذا ما حذر منه الدستور في المادة ٧ / ثانياً التي أكدت على أنْ: " تلتزم الدولة محاربة الارهاب بجميع اشكاله، وتعمل على حماية اراضيها من أنْ تكون مقراً أو ممراً أو ساحة لنشاطه " (١٠١). إنّ الغاية من وضع استراتيجية عراقية لضمان الأمن و تحقيق الردع السيبراني؛ تكمن في وضع الاحكام والضوابط والمعايير القانونية، والتي تمثل الركيزة والمرجع الاساس للجهات المعنية لضمان حماية الأمن السيبراني الوطني(١٠٢) . وتقوم الاستراتيجية على وجود مراكز تعنى بأمن المعلومات العراقي وإدارة الحوادث

السيبرانية ومعالجتها والسيطرة على جرائم المعلوماتية وهو أمرًا هامًا جداً وضروري، لأن العراق كما قلنا يتعرض و لا يزال للعديد من الهجمات الإرهابية السيبرانية (١٠٣). يمثل موضوع الحفاظ على بيئة آمنة للأنشطة على الإنترنت أمر ضروري، إذ يعمل على تعزيز الثقة الرقمية مما ينتج عنه اقتصاد مزدهر عبر الإنترنت، فيجب أنْ يطمئن الأفراد على إتمام تعاملاتهم في سلام، و أنَ معلوماتهم الشخصية محمية بشكل كاف، ويعد تعزيز الوعي والتشجيع على تبادل المعلومات بين الجهات الحكومية والشركات والمؤسسات من أهم الوسائل الفعالة في تحسين الأمن السيبراني:. ومن أهم مقتضيات الاستراتيجية العراقية لتحقيق الأمن السيبراني وضع الإطار القانوني التنظيمي لتعزيز سلامة الفضاء الإلكتروني، ويكون ذلك عن طريق تشريع قوانين تعمل على مكافحة الجريمة الإلكترونية(١٠٤)،وحق تّقديم مشروعات القوانين أصبح اليوم من صلاحية السلطة التنفيذية بطرفيها (مجلس الوزراء ورئيس الجمهورية) على وفق المادة ٦٠ أولا من الدستور، لأنَّ مشروع القانون يقَدم بهيكَلّية تختلف عَن هيكَلّية مقترح القانون بسبب من أهميته و الغايات المتوخاة من ورائه، فالأول يقَدم مصاغاً ومبوباً ويذكر فيه المواد متسلسلة، بينما مقترح القانون لا يقَدم إلّا بشكَلّ فكرة، و البرلمان هو الذي يعده، وأنّ مقترح القانون في بادئ الأمر يقدم إلى لجان مختصة تقوم بتّقديم تَقْرير مفصل عنهُ، بينما مشروع القانون معفى مَن هذه الآلية.

فمشروع القانون يمر بمراحل عدة، تبدأ مَن قيام الوزارة المعَنية أو رئيس الجِهَة غَيْر المرتبطة بوزارة بإعداد مسودة المشروع، ولكَوْن الحديث عَن الأمن الإلكتروني والردع السيبراني، بما يضمن حماية البنى التحتية للحكومة، فمَن البَديهيّ أنّ تختص بهذا الأمر وزارة الدَاخلِيّة وَفْقاَ لقانونها، وكذَلكَ يقع ضمن اختصاص وزارة الدفاع، إذ أنّ هاتيْن الوزارتين تختصان بحِفْظ الأمَن الوَطنيّ في عموم العراق داخليا و خارجيا.(١٠٥) العمل على بناء منظومة فعالة للأمن السيبراني على المستوى الوطني وتطويرها وتنظيمها لحماية العراق من تهديدات الفضاء السيبراني ومواجهتها بكفاء وفاعلية بما يضمن استدامة العمل والحفاظ على الأمن الوطني وسلامة الأشخاص والممتلكات والمعلومات، ومن ضمن ما نقترحه في هذا الصدد إنشاء مجلس وطني للأمن السيبراني، يترك لوزارتي الداخلية و الدفاع اختصاص إعداد مشروع القانون الخاص به (١٠٦).

المطلب الثاني : الأبعاد الجديدة في استراتيجية الأمن الوطني العراقي لتحقيق الردع السيبراني: في ظلّ التطور المعلوماتيّ، أصبح التدخل بشؤون الدول لا يتمّ بالصورة التقليديَّة؛ إذ بات يأخذ شكل الهجمات الإلكترونيَّة التي تتمّ بواسطة استخدام أجهزة الكومبيوتر أو الشبكات أو الأنظمة التي من خلالها يتمّ تدمير البيانات أو تعطيل الشبكات أو اختراق الأنظمة. و ما يؤدي إليه ذلك من فك و معرفة الأسرار والمعلومات الخاصة بالدولة، وبالتالي يمكن أنْ يؤدي استخدامها إلى التأثير في القرار داخل الدولة، أيّ فيما يتعلق بالنطاق المحفوظ للدولة، وعليه نصل إلى سؤال مهم وهو ما مدى انطباق مفهوم الأمن الرقميّ على التدخل في شؤون الدول في ظلّ المتغيرات في الفضاء المعلوماتي؟

**الفرع الأول:** انضمام العراق ل الاتفاقية العربية لمكافحة جرائم تقنية المعلومات (١٠٧) :صدق العراق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بالقانون رقم ٣١ لسنة ٢٠١٣. وذلك في محاولة منه لوضع استراتيجية للأمن و الردع السيبراني (١٠٨). وجاء في الأسباب الموجبة للتصديق من أجل تعزيز التعاون بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات حفاظًا على أمن الدول العربية ومصالحها وسلامته ولفرض مصادقة جمهورية العراق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات شرع هذا القانون " (١٠٩) . وذلك يكون المشرع العراقي قد أخذ خطوة إيجابية نحو وضع استراتيجية فعالة لتحقيق الأمن السيبراني . ظهرت معالم هذه الخطة بالتصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، فمما لا شك فيه إن انضمام العراق لتلك الاتفاقية يجعلها نافذة كقانون من قوانينه، خصوصا بعد التصديق عليها. وتضمن الاتفاقية العربية حفظ سيادة الدولة، ضد هجمات **الإرهاب السيبراني**:[١١٠] حيث تلتزم كل دولة طرف وفقًا لنظمها الأساسية أو لمبادئها الدستورية بتنفيذ الالتزامات الناشئة عن تلك الاتفاقية على نحو يتقف مع مبدأي المساواة في السيادة وعدم التدخل في الشؤون الداخلية.

الفرع الثاني: مشروع قانون مكافحة الجرائم الإلكترونية العراقي لعَامّ ٢٠١٩: إنّ وجود تشريع يعمل على توفير الأمن السيبراني و حماية الدولة من تهديدات حوادث الأمن السيبراني ورفع مستوى الأمن الوطني العام والشامل للمؤسسات والأفراد وتطوير قدراتهم على ردع ومراقبة وانذار واستجابة حوادث الأمن السيبراني والتخفيف من الاضرار الناجمة عنها. كما يعمل التشريع على خلق بيئة آمنة تكون جاذبة للاستثمارات؛ ومحفزة الاقتصاد الوطني خاصة في ظل تسارع التطور في أنظمة المعلومات و البنية التحتية وتنامي حجم الخدمات الحكومية، وكذا مراقبة الفضاء السيبراني الوطني ورصده وتوثيق حوادث الأمن السيبراني. وإيمانًا من المشرع العراقي بوجوب تحقيق هذه الأهداف في الاستراتيجية الجديدة لتحقيق الأمن السيبراني قام بمحاولة لإصدار قانون مكافحة الجرائم الإلكترونية، وقد نص مشروع القانون على أن الهدف هو حماية الافراد المجتمع من الجريمة الإلكترونية، ومكافحة الجريمة الإلكترونية التي تشكل تهديدًا لأمن الدولة وسلامتها، والعمل على زيادة الوعي العام بمخاطر الجريمة الإلكترونية، وتطوير قدرات العاملين على إنفاذ القانون وتقديم الدعم التقني للسلطة لمواكبة أخر التطورات الحاصلة مجال الجرائم الإلكترونية (١١١). حتى وإن كان المشرع العراقي لم يوفق في إصدار قانون جرائم مكافحة المعلومات الإلكترونية أي أنه سعى لتوفير الأمن السيبراني في إطار من الشرعية الدستورية، رغم عدم اكتمال جهوده و تتويجها بتشريع.

**الخاتمة:** تأسيسا على ما سبق، فقد ظهر من خلال دراستنا لموضوع أسس رسم السياسة العامة للدولة العراقية لتحقيق الردع السيبراني، أنّ الأمن السيبراني مرتبط بالفضاء المعلوماتي وهو غير مرئي، وبحاجة إلى تقنيات إلكترونية عالية من اجل حمايته

من الهجمات الإلكترونية التي تستهدف كشف البيانات والمعلومات الاقتصادية والعسكرية والسياسية للدول والمؤسسات والأفراد، و فيما يلي أبرز النتائج و أهم التوصيات التي يمكن أن نتوجه بها في هذا المقام.

أولا_ النتائج:

١- إتضح أنَّ المشرع العراقي لم يقم بإصدار أي تشريع لتوفير الأمن السيبراني ولحماية الفضاء المعلوماتي العراقي، بما في ذلك قانون مكافحة جرائم المعلوماتية، فضلا عن إنَّ المشرع العادي العراقي لم يولي الحقوق الرقمية؛ أي اهتمام تشريعي يستحق الذكر، بالرغم من تقنين العديد والعديد من حقوق الإنسان في الدستور وفي القوانين، إلا أن حداثة نشأة الحقوق الرقمية حالت دون تقنينها، مما نتج عنه عدم توفير غطاء تشريعي كاف لحماية الأمن المعلوماتي و تحقيق الردع السيبراني.

٢- إن حماية الأمن المعلوماتي ما هي إلا حماية للأمن العام الوطني للعراق، وهو من صميم اختصاص السلطة التنفيذية، لاسيما وزاراتها الأمنية و المتخصصة الأخرى، وهذه كلها تحتاج لأرضية تشريعية رصينة، عليه سيكون إصدار قانون لحماية الأمن المعلوماتي؛ ضرورة لكي يكون جزء من متطلبات الأمن الوطني العراقي، و ضمان قدرة الدولة في تحقيق الردع السيبراني المطلوب.

٣- العراق بلد ضعيف البنية التحتية في المجال السيبراني المعلوماتي، و تعرض و لا يزال للعديد من الهجمات الالكترونية الخبيثة، التي كانت تستهدف تدمير القدرات المعلوماتية للدولة و مؤسساتها و قدرات مواطنيها كذلك، و امام هكذا حقيقة لا يمكن الحديث عن أمن سيبراني أو حتى أمن إنساني لمواطني الدولة، مالم تتخذ خطوات جدية عاجلة في سبيل الوصول لهذه الغاية المهمة، ف المنفذ لا يمكنه العمل بمعزل عن القوانين و الاتفاقيات التي يحتاجها، لكي يؤطر عمله بالإطار الشرعي، و ليتخذ خطوات ليس في مجال التنفيذ الأمني و حسب، بل حتى في المجال التوعوي المكمل له.

ثانيا_ التوصيات:

١- يوصي الباحث المشرع العراقي ممثلا بمجلس النواب بوجوب الإسراع في إصدار قانون لحماية الأمن و الردع السيبراني، مستندًا على الأسس الدستورية العديدة التي تمت الاشارة لها خلال البحث، و ضرورة مراعاة ان لا تتخذ نصوصه ذريعة لتقييد غير مقبول للحقوق و الحريات الرقمية.

٢- يوصي الباحث المشرع العادي العراقي بوجوب تقنين الحقوق الرقمية للمواطن، سيما و إنَّ دستور عام ٢٠٠٥ قد خص مجلس النواب بسلطة تعديله مع ضرورة اجراء الاستفتاء

الدستوري عليه، لتكون من ضمن طائفة الحقوق والحريات في دستورنا، و العمل بعد ذلك على سن التشريعات العادية التي ستحوي الأطر التفصيلية الخاصة بحمايتها.

٣- نوصي المشرع العراقي بوجوب اعتماد تفسير موسع لكلمة القوة عند إصدار قانون حماية الأمن و الردع السيبراني، مع مراعاة أنْ لا يتضمن مفهوم الردع المعلوماتي، أي استخدام لقوة مادية من جانب الدولة، مالم يكن ذلك ضرورة قصوى ملجئه بسبب من شدة الهجمات السيبرانية و حجمها، على أنْ يكون القرار في هذا الصدد من صلاحية المجلس الوطني للأمن السيبراني الذي اقترحنا تشكيله في متن البحث، و بأجماع من أعضاءه.

٤- اللجوء الى القواعد الدستورية والوطنية في تشكيل الحكومة العراقية والابتعاد عن مبدأ المحاصصة الطائفية والحزبية، كيما نضمن وصول وزراء مهنيين و مختصين( تكنوقراط)، ليعملوا على تطبيق هذا المبدأ في كل مفاصل و مؤسسات الدولة الأخرى، و بالأخص هنا الوزرات و الأجهزة الأمنية كافة.

قائمة المصادر/

أولا/ الكتب العربية:

١- د.أحمد يوسف كيطان، استراتيجية الأمن الوطني السيبراني للصين "قراءة في قانون الأمن السيبراني الصيني"، مركز النهرين للدراسات الاستراتيجية، ٢٠١٨.

٢- د. إسماعيل بدوي، اختصاصات السلطة التنفيذية في الدولة الاسلامية و النظم الدستورية المعاصرة، دار النهضة العربية، القاهرة، ١٩٩٣.

٣- أندريه بوفر، الردع و الاستراتيجية، ترجمة أكرم ديري، دار الطليعة للطباعة و النشر، بيروت، ١٩٧٠.

٤- إيهاب خليفة، القوة الالكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الانترنيت، دار العربي، ٢٠١٧.

٥- د. إيهاب خليفة، الحرب السيبرانية: الاستعداد لقيادة المعارك في الميدان الخامس، سلسلة كتب المستقبل، الطبعة الاولى، العربي للنشر و التوزيع، القاهرة، ٢٠٢١.

٦- د.جيمس جيفرسون، صنع السياسات العامة، ترجمة د. عامر الكبيسي، دار المسيرة للنشر و التوزيع و الطباعة، عمان، الاردن،١٩٩٨.

٧- د. حسنين المحمدي بوادي، الإرهاب الدولي بين التجريم والمكافحة، دار الفكر العربي، ٢٠٠٦.

٨- د. سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، الطبعة الرابعة، دار النهضة العربية، القاهرة، ٢٠١٧.

٩- د. سوسن العساف، استراتيجية الردع: العقيدة الأمريكية الجديدة و الاستقرار الدولي، الطبعة الأولى، الشبكة العربية للأبحاث و النشر، ٢٠٠٨.

١٠-د. شادي عبد الوهاب منصور، حروب الجيل الخامس: اساليب "التفجير من الداخل" على الساحة الدولية، سلسلة كتب المستقبل، الطبعة الأولى، العربي للنشر و التوزيع، القاهرة، ٢٠١٩.

١١-عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الإسكندرية، 2010 .

١٢-د. عبد السلام هابس السويفان، إدارة مرفق الأمن بالوسائل الالكترونية "دراسة تطبيقية"، دار الجامعة الجديدة، الاسكندرية، ٢٠١٢.

١٣-عبد الفتاح بيومي حجازي، النظام القانوني لحماية الحكومة الإلكترونية، الكتاب الثاني، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى ، ٢٠٠٣ .

١٤-د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والإنترنت، دار . الكتب القانونية ، ٢٠٠٧ .

١٥-د. عبد الفتاح باغي، السياسة العامة: النظرية والتطبيق، جامعة الإمارات العربية المتحدة، الطبعة الأولى، ٢٠٠٩.

١٦-د. علي الطوالبة، التفتيش الجنائي على نظم الحاسوب والإنترنت، الطبعة الاولى، عالم الكتب الحديث، الاردن، ٢٠١٥.

١٧-علي جبار الحسيناوي، جرائم الحاسوب و الأنترنت، دار اليازوري العلمية للنشر و التوزيع، عمّان، ٢٠٠٩.

١٨-علي محمد كاظم الموسوي، المشاركة المباشرة في الهجمات السيبرانية، الطبعة الأولى، شركة المؤسسة الحديثة للكتاب، بيروت، لبنان، ٢٠١٩.

١٩-د. علي محمد بدير و د. عصام عبد الوهاب البرزنجي و د. مهدي ياسين السلامي، مبادئ و احكام القانون الإداري، بيروت، ٢٠١٢.

٢٠-د. محمد أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمان، الطبعة 3، ٢٠٢٠ .

٢١-د. محمد أمين الرومي، جرائم الكمبيوتر والأنترنت، دار المطبوعات الجامعية، الإسكندرية، ٢٠١٣.

٢٢-محمد أمين البشري، التحقيق في الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، مركز الدراسات والبحوث، الرياض، ٢٠١٤.
٢٣-د. منى الأشقر جبور، الأمن السيبراني ( التحديات ومستلزمات المواجهة )، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، بيروت، ٢٠١٢.
٢٤-نائلة عادل قورة ، جرائم الحاسب الاقتصادية ( دراسة نظرية وتطبيقية )، دار النهضة العربية، القاهرة ، ٢٠١٤ .
٢٥-د . نبيل أحمد حلمي، القانون الدولي وفقاً لقواعد القانون الدولي العام، دار النهضة العربية، القاهرة، ١٩٩٩.
٢٦-د . هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، ١٩٩٢.
٢٧-د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة ،٢٠٠٩.
٢٨-د. وصال نجيب العزاوي، مبادئ السياسة العامة، دار أسامة للنشر والتوزيع، عمان، الأردن، ٢٠٠٣.

ثانيا/الرسائل العلمية:
١- بوشعرة أمنية و موساى سهام، الإطار القانوني للجريمة الإلكترونية، رسالة ماجستير، كلية الحقوق و العلوم السياسية، جامعة عبد الرحمان ميرة، الجزائر، ٢٠١٨ .
٢- حنين جميل أبو حسين، الإطار القانوني لخدمات الأمن السيبراني " دراسة مقارنة "، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، الأردن، ٢٠٢١.
٣- زينب رياض جبر، التجسس الرقمي في ضوء قواعد القانون الدولي، أطروحة دكتوراه، كلية القانون، جامعة كربلاء، ٢٠٢١.
٤- سليمان العنزي، وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٣.
٥- صالح هادي منسي, تشارك السلطة التنفيذية مع البرلمان بالتشريع في النظام البرلماني (دراسة مقارنة), رسالة ماجستير, معهد العلمين للدراسات العليا, العراق, ٢٠١٦.
٦- عادل عبد الصادق، أثر الإرهاب الإلكتروني على مبدأ استخدام القوة في العلاقات الدولية، رسالة ماجستير، كلية العلوم السياسيَّة، جامعة القاهرة ، ٢٠٠٩.
٧- عبدالله السحبياني، كفاءة الإجراءات الإدارية في المحافظة على أمن المعلومات، رسالة ماجستير، الرياض، جامعة نايف العربية للعلوم الأمنية، ٢٠١١.

٨- عبد الله داغش العجمي، المشكلات العلمية والقانونية للجرائم الإلكترونية "دراسة مقارنة"، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، الأردن، ٢٠١٤.
٩- د. عبد السلام هابس السويفان، إدارة مرفق الأمن بالوسائل الالكترونية "دراسة تطبيقية"، دار الجامعة الجديدة، الاسكندرية، ٢٠١٢.
١٠-د. علي الطوالبة، التفتيش الجنائي على نظم الحاسوب والإنترنت، رسالة دكتوراه، جامعة عمان العربية، منشورة، الطبعة الأولى، عالم الكتب الحديث ، ٢٠١٥ .
١١- علي زايد محمد الشهري، الإطار القانوني للحد من الجرائم الإلكترونية لتعزيز الأمن السيبراني في المملكة العربية السعودية، رسالة دكتوراه، جامعة نايف العربية للعلوم الأمنية، كلية العلوم الاستراتيجية، ٢٠١٩.
١٢-علي زياد العلي، التحديات غير المرئية للأمن الوطني العراقي، مركز البيان للدراسات والتخطيط، بغداد، الترويج لثقافة وطنية للأمن السيبراني، رسالة على الانترنت، على الرابط
www.itu.int/dms_pub/itu-d/opd/stg/D-STG-SG01.22-2010-MSWAdocx
١٣-فارس رشيد البياتي، التنمية الاقتصادية سياسيا في الوطن العربين أطروحة دكتوراه، كلية الإدارة و الاقتصاد، الاكاديمية العربية المفتوحة في الدنمارك، عمّان، ٢٠٠٨.
١٤-محمد كاظم محمود، مجلس الوزراء في العراق ولبنان: دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق، الجامعة الإسلامية اللبنانية، بيروت، ٢٠١٩.
١٥-هدير مشرع حسين، اختصاص السلطات الاتحادية في وضع سياسة الأمن الوطني و تنفيذها: دراسة مقارنة، رسالة ماجستير، معهد العلمين للدراسات العليا، ٢٠٢٠.
١٦-وميض عبد المهدي، اختصاص وزارة الداخلية في حفظ الامَن العام وفقاً لقانون رقم (٢٠) لسنة ٢٠١٦(دراسة مقارنة)، رسالة ماجستير ، معهد العلمين للدراسات العليا، العراق، ٢٠٢١.

ثالثا/ البحوث و الدوريات و المقالات:
١- د. أحمد عبيس الفتلاوي و أزهر عبد الأمير الفتلاوي، المسؤولية الناشئة عن استخدام وسائل القتال الفتاكة في نشر الأوبئة: الهجمات السيبرانية في مواجهة جائحة كورونا نموذجا، بحث منشور، مجلة الحقوق، كلية الحقوق، الجامعة المستنصرية، المجلد ١، العدد ٤١، ٢٠٢١.
٢- د. أحمد علي عبود، آليات رسم السياسة العامة في دستور جمهورية العراق لسنة ٢٠٠٥، بحث منشور، مجلة جامعة أهل البيت عليهم السلام، العدد ٢٩، ٢٠٢١.

٣- الهام ناصر، نظرية الردع، مقال منشور على الانترنت على موقع الموسوعة السياسية، الرابط www.political-encyclopedia.org/dictionary/

٤- د. أميرة عبد العظيم محمد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي، مجلة الشريعة والقانون، تصدر عن كلية الشريعة والقانون، جامعة الأزهر، مصر، العدد ٣٥، ج ٣، ٢٠٢٠

٥- د. أميرة محمد سيد أحمد، استراتيجيات مكافحة الجرائم الإلكترونية في العصر المعلوماتي تعزيزا لرؤية مصر ٢٠٣٠: دراسة استشرافية، بحث منشور، مجلة البحوث الإعلامية، كلية الاعلام، جامعة الأزهر، العدد ٥٨ ، الجزء الرابع، يوليو، ٢٠٢١.

٦- د. باسم علي خريسان، الأمن السيبراني في العراق – قراءة في مؤشر الأمن السيبراني العالمي في ٢٠٢٠، بحث منشور على الانترنت، ٢٠٢١، و على الموقع الإلكتروني لمركز البيان للدراسات و التخطيط، على الرابط www.bayancenter.org

٧- حسن بن أحمد الشهري، قانون دولي موحد لمكافحة الجرائم الإلكترونية، بحث منشور، المجلة العربية للدراسات الأمنية والتدريب، جامعة نايف للعلوم الأمنية، العدد47 ، العدد 53، رجب 1434 هـ .

٨- خولة محي الدين يوسف، الأمن الإنساني وأبعاده في القانون الدولي، بحث منشور، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد ٢٨، العدد الثاني، ٢٠١٢.

٩- رغد البهي، الردع السيبراني: المفهوم و الاشكاليات و المتطلبات، بحث منشور، مجلة العلوم السياسية و القانون، العدد الاول، المركز الديمقراطي العربي، برلين، ٢٠١٧.

١٠-سعد السعيدي، مشروع قانون جهاز المخابرات العراقي، مقال على الانترنت و على الرابط
www.tellskuf.com/index.php/mq/63145-de68.html .

١١-د. صلاح مهدي هادي ود. زيد محمد علي أسماعيل، الأمن السيبراني كمرتكز جديد في الاستراتيجية العراقية، بحث منشور، مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين، العدد ٦٢، السنة ١٢ ، ٢٠٢٠.

١٢-د. عبد الله ذياب محمود، جريمة الاختراق الواقعة على البيانات و المواقع الحكومية، بحث منشور، مجلة المنارة للدراسات القانونية و الإدارية" عدد خاص حول الثورة الرقمية و إشكالاتها"، أبريل-نيسان، دار القلم للطباعة، الرباط، ٢٠٢٠.

١٣-عبدالله السحبياني، كفاءة الإجراءات الإدارية في المحافظة على أمن المعلومات، رسالة ماجستير، الرياض، جامعة نايف العربية للعلوم الأمنية، ٢٠١١.

١٤-علي زياد فتحي، العمليات السيبرانية الأوروأطلسية و مهددات الجيوسيبرانية الروسية: رؤية في الاشتباك السيبراني الأورو- روسي، بحث منشور، مجلة حمورابي للدراسات، مركز حمورابي للبحوث و الدراسات الاستراتيجية، العدد ٣٠، السنة السابعة، بغداد، ٢٠١٩.

١٥-علي زياد العلي، التحديات غير المرئية للأمن الوطني العراقي، مقال منشور، مركز البيان للدراسات والتخطيط، بغداد، نشر ٢٠١٨/٦/٢٦،الشبكة الدولية للمعلومات (الانترنت ) على الموقع www.bayancenter.org.

١٦-محمد زهير عبد الكريم، الإرهاب السيبراني: أزمة عالمية جديدة، بحث منشور، مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين، العدد ٦٤، ٢٠٢١.

١٧-د. مصدق عادل طالب و حسين فياض نايف، الأساس الدستوري و القانوني للمؤسسات الوطنية لحقوق الانسان في العراق و مدى موائمتها مع المعايير الدولية، بحث منشور، مجلة العلوم القانونية، كلية القانون، جامعة بغداد، مجلد ٣٦، العدد ٣، ٢٠٢١.

١٨-د. نوري حمد خاطري، حماية المصنفات والمعلومات ذات العلاقة بالحاسوب بقانون حماية حقوق المؤلف، بحث منشور، مجلة المنارة، جامعة آل البيت، العدد (٤)، كانون ثاني، ٢٠١٢.

١٩-أ. نوفل عبد الله و أ. محمد عزت، جريمة إنشاء مواقع أو نشر معلومات مخلة بالآداب العامة بوسائل تقنية المعلومات، بحث منشور، مجلة الرافدين للحقوق، كلية الحقوق، جامعة الموصل، المجلد ١٢، العدد ٤٤، ٢٠١٠.

٢٠-نورة شلوش، القرصنة الإلكترونية في الفضاء السيبراني: التهديد المتصاعد لأمن الدول، بحث منشور، مجلة مركز بابل للدراسات الإنسانية، مركز بابل للدراسات الانسانية، جامعة بابل، المجلد٨، العدد٢٠١٨،٢.

٢١-ياسمين عبد اللطيف زرد، الولايات المتحدة بحاجة لوكالة مركزية للأمن السيبراني، مقال منشور على الانترنت على موقع مجلة الشروق الالكترونية، على الرابط https://www.shorouknews.com/columns/view.aspx

رابعا- الدساتير و القوانين:

١- الدستور العراقي لعام ٢٠٠٥.
٢- قانون أدارة الدولة للمرحلة الانتقالية العراقي لعام ٢٠٠٤.
٣- قانون التوقيع الالكتروني و المعاملات الالكترونية العراقي رقم ٧٨ لسنة ٢٠١٢.
٤- قانون وزارة الداخلية رقم (٢٠) لسنة٢٠١٦.
٥- مشروع قانون مكافحة الجرائم الإلكترونية العراقي لعَامّ ٢٠١٩.

٦- قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨/ الوقائع المصرية، العدد ٣٢ مكرر ٢٠١٨.

**خامسا- الوثائق /**

١- وثيقة استراتيجية الأمن السيبراني العراقي، إعداد مستشارية الأمن الوطني/ اللجنة الفنية العليا لأمن الاتصالات و المعلومات، على الانترنت و على الرابط www. nsa.gov.iq

٢- دليل الأمن السيبراني للدول النامية، الاتحاد الدولي للاتصالات، ٢٠١٠.

**سادسا- المصادر باللغة الأجنبية:**

1- Christophe Haynes, Stuart Casey-Maslen, Thomas Robert, The definition of an" attack" under the law of armed conflict, articles of war, Nov 3, 2020.

2- Bruno Gruselle- Bruno Tertrais- Alain Esterle, Cyber Dissuasion, Recherches & Documents, FONDATION RECONNUE D'UTILITÉ Publique, Paris, N° 03/2012.

3- Evelyn Jacque, Regulating Cyber Security; What civil liability in case of cyber-attacks,2020.

4- James A. Green, Cyber Warfare ;Multi-Disciplinary and Analysis, 2016.

5- Kyung Shick, Claire Lee ,The Present and Future of Cybercrime, Cyber terrorism, and Cyber security, International Journal of Cyber security Intelligence & Cybercrime 2000, Vol. 1, No .1 ,2018.

6- Kamal Ahmad Khan, Use of Force and Human Rights under International Law ،Athens Institute for Education and Research, Conference Paper Series BLE, 2017- 2205.

7- Kenneth gears , The Challenge of cyber-attack deterrence , computer law &security report, vol.303, 2010.

8- Kevin Pollpeter, Chinese writing on cyberwarfare and coercion, in; Jon R. Lindsay, Oxford University press, 2015.

9- Marco Roslyn, Cyber operations and the computer science, Vol.10, No.1, 2018.

10- Mehdi Kadivar, Cyber – Attack Attributes, Technology Innovation Management Review, October, 2014.

11- Michael schmitt, computer network attack and the use of force in international law, thought son normative, framework approved for public release, distribution unlimited,1998.

12- Myriam A. Dunn, The Internet and the Changing Face of International Relations and Security", Volume number.7, Issue number.1, ProCon. Ltd., Bulgaria, Sofia, 2001.

13- Nicola Lucchi, Access to Network Services and Protection of Constitutional Rights: Recognizing the Essential Role of Internet Access for the Freedom of Expression, Cardozo Journal of International and Comparative Law, Vol.19, No.3, 2011.

14- P.K. Huth, Deterrence and international conflict: Empirical findings and theoretical debates, Annual Review of political science, second part, 1999.

15- Richard Stiennon, A short history of cyber warfare, Cyber Warfare: A multidisciplinary analysis, Oxon; Routledge, 1st edition, 2015.

16- Samuel Dominion, Stability, internet management and disinformation, EEuromesco Policy Study, European Institute for the Mediterranean, No. 22, 2021.

17- Steven l. kwast, timothy m. McKenzie, Is Cyber Deterrence possible?, Air force research Institute, Papers air, University Press, 2017.

18- Tim Jordan, Cyber power: The Culture and Politics of Cyberspace.Rout ledge .and the Internet.

19- Thomas R. Dye, Understanding public policy, Englewood Cliffs, N. Prentice-Hall, 2nd ed., 1975.

20- Wayne M. Alder, Data Breaches: Statutory and Civil Liability, and How to Prevent and

**الهوامش**

(١) د. هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، بدون سنة نشر، ص ٥

٢ () ينظر عن هذا التعريف للأستاذ( كريستوفر دي لوكا) أورده: علي محمد كاظم الموسوي، المشاركة المباشرة في الهجمات السيبرانية، الطبعة الأولى، شركة المؤسسة الحديثة للكتاب، بيروت، لبنان، ٢٠١٩، ص ١٩.

٣ ) see Département fédéral de la défense, de la protection de la population et des sports (DDPS, CONCEPTION GÉNÉRAL Cyber, Centre des médias numériques de l'armée (MNA), 86.084 d, 2022, p.9

٤ ()و تكون أكثر خطورة لو ارتكبت من أشخاص حكوميين مصرح لهم بالدخول للمواقع الحكومية الالكترونية بوصفهم عاملين على هذه المواقع و صيانتها من العبث، ف يأتي فعلا ينتهك أمن المعلومات المحفوظة فيها، و تزداد الخطورة عندما يحوز هكذا أشخاص معلومات عن أمن الدولة نتيجة لهذا الانتهاك، ينظر د. عبد الله ذياب محمود، جريمة الاختراق الواقعة على البيانات و المواقع الحكومية، بحث منشور، مجلة المنارة للدراسات القانونية و الإدارية" عدد خاص حول الثورة الرقمية و إشكالاتها"، أبريل-نيسان، دار القلم للطباعة، الرباط، ٢٠٢٠، ص ١٧٢.

٥ () فالجريمة الالكترونية أو السيبرانية" هي: ( شكل من أشكال الجرائم المرتبطة بالحاسوب الآلي، و تستخدم تكنولوجيا الشبكة المعلوماتية الدولية، و تغطي كل الجرائم المرتكبة في الفضاء السايبر، وهي سلوكيات غير اخلاقية و غير مشروعة كونها غير مرخص لها، تتجسد بالسطو على معلومات و بيانات و معطيات و القيام بمعالجتها على نحو يجعل صاحبها غير قادر على استرجاعها و الافادة منها)، ينظر علي محمد كاظم، مصدر سابق، ص٣٠، و هي بذلك تكون على نوعين: الأول هو الجرائم الموجهة ضد جهاز الحاسوب الآلي أو أنظمة تقنية المعلومات و الاتصالات الأخرى بقصد تعطيلها أو اتلافها، أما الثاني، فيشمل الجرائم التي يكون فيها الحاسوب وسيلة ارتكاب جرائم الاحتيال الالكتروني و سرقة الهويات و بطاقات الائتمان، و الارصدة المالية و التزوير و الاختلاس و سرقة حقوق الملكية الفكرية و السلوك المنحرف و جرائم الاستغلال الجنسي للأطفال، ينظر عنها الجريمة الالكترونية في المجتمع الخليجي و كيفية مواجهتها، اعداد/ مجمع البحوث و الدراسات في أكاديمية السلطان قابوس لعلوم الشرطة، الأمانة العامة لمجلس التعاون الخليجي، ٢٠١٦، ص ٩.

٦ Kyung Shick , Claire Lee ,The Present and Future of Cybercrime, Cyber terrorism, and Cyber security, International Journal of Cyber security Intelligence & Cybercrime, Vol. 1, No .1 ,2018, pp 1-4.

وراجع كذلك د. نائلة عادل قورة، جرائم الحاسب الاقتصادية ( دراسة نظرية وتطبيقية )، دار النهضة العربية، القاهرة، ٢٠١٤ ، ص ٣٢

(٧) د. اميرة محمد، استراتيجية مكافحة الجرائم الإلكترونية في العصر المعلوماتي، بحث منشور، مجلة البحوث الإعلامية، العدد ٥٨، الجزء الرابع، يوليو ٢٠٢١، ص ١٧٩٥

(٨)د. منى الأشقر جبور، الأمن السيبراني ( التحديات ومستلزمات المواجهة )، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، بيروت، ٢٠١٢ ، ص ٢

(٩) حنين جميل أبو حسين، الإطار القانوني لخدمات الأمن السيبراني" دراسة مقارنة "، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط ، الأردن ، ٢٠٢١ ، ص ١٨

(١٠) د. سعيد عبد اللطيف حسن ، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، دار النهضة العربية، القاهرة، الطبعة الرابعة ، ٢٠١٧ ، ص ٤١٤.

١١( ) ينظر سليمان العنزي، وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٣، ص٢٣

(١٢) دليل الأمن السيبراني للدول النامية، الاتحاد الدولي للاتصالات، ٢٠١٠، ص ٤٢١.

(١٣) بوشعرة أمنية و موساى سهام، الإطار القانوني للجريمة الإلكترونية، رسالة ماجستير، كلية الحقوق و العلوم السياسية، جامعة عبد الرحمان ميرة، الجزائر، ٢٠١٨، ص ٢٢

(١٤) ينظر أندريه بوفر، الردع و الاستراتيجية، ترجمة أكرم ديري، دار الطليعة للطباعة و النشر، بيروت، ١٩٧٠، ص ٣١.

[15] See Bruno Gruselle- Bruno Tertrais- Alain Esterle, Cyber Dissuasion, Recherches & Documents, FONDATION RECONNUE D'UTILITÉ Publique, Paris, N° 03/2012, p.63-64.

[16] () ينظر عنهم رغد البهي، الردع السيبراني: المفهوم و الاشكاليات و المتطلبات، بحث منشور، مجلة العلوم السياسية و القانون، العدد الاول، المركز الديمقراطي العربي، برلين، ٢٠١٧، ص ٥١.

[17] () فالتجسس الالكتروني، الذي تتعرض له الدولة بكثرة هذه الأيام؛ هو من صور "الهجمات الالكترونية" التي تتم عبر فضاء السايبر. ويتمثلان في صورة الدخول غير المصرح به للنظام المعلوماتي، ويهددان الأمن السيبراني للدولة، و يستوجبان نشاطا من الدولة في سبيل تحقيق الردع السيبراني المطلوب، ينظر

Marco Roslyn, Cyber operations and the computer science, Vol.10, No.1, 2018, p.373.

(١٨) علي جبار صالح الحسيناوي، جرائم الحاسوب و الإنترنت، دار اليازوري العلمية للنشر و التوزيع، عمان، ٢٠١١، ص٣٧.

(١٩) د. محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، ٢٠١٣، ص ٧
وتختلف المعلومة عن أدوات التكنولوجيا، حيث أن المعلومة هي ما ينتج عن معالج البيانات والمعطيات بشكل معين، تستخدم فيه التكنولوجيا سواء للتجميع أو للوصول، أو للتخزين، والمعالجة، للمزيد ينظر حسن بن أحمد الشهري، قانون دولي موحد لمكافحة الجرائم الإلكترونية، بحث منشور في المجلة العربية للدراسات الأمنية والتدريب، تصدر عن جامعة نايف للعلوم الأمنية، العدد47 ، العدد 53 ، رجب 1434 هـ

(٢٠)عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامعة الجديدة، الإسكندرية، ٢٠١٠، ص ٣٤.

[21] Wayne M. Alder . Data Breaches: Statutory and Civil Liability, and How to Prevent and Defend a Claim.2018 . P. 114.

[22] Kevin Pollpeter, Chinese writing on cyberwarfare and coercion, in; Jon R. Lindsay, Oxford University press, 2015. P.145.

[23] Richard Stiennon, A short history of cyber warfare, Cyber Warfare: A multidisciplinary analysis, Oxon; Routledge, 1st edition, 2015, p.24-26.

[24] () ينظر د. إسماعيل بدوي، اختصاصات السلطة التنفيذية في الدولة الاسلامية و النظم الدستورية المعاصرة، دار النهضة العربية، القاهرة، ١٩٩٣، ص ٣١٢.

[25] () ينظر د. علي محمد بدير و د. عصام عبد الوهاب البرزنجي و د. مهدي ياسين السلامي، مبادئ و احكام القانون الإداري، بيروت، ٢٠١٢، ص ٢١٦.

(٢٦) ينظر د. عبد السلام هابس السويفان، إدارة مرفق الأمن بالوسائل الالكترونية "دراسة تطبيقية"، دار الجامعة الجديدة، الاسكندرية، ٢٠١٢، ص ٥٤٨.

(٢٧) ينظر علي زايد محمد الشهري، الاطار القانوني للحد من الجرائم الالكترونية لتعزيز الأمن السيبراني في المملكة العربية السعودية، اطروحة دكتوراه، كلية العلوم الاستراتيجية، جامعة نايف العربية للعلوم الأمنية، ٢٠١٩، ص ٢٣١.

[28] EVELYNE JACQUE, Regulating Cyber Security- What civil liability in case of cyber-attacks,2020. p. 231.

[29] () عبد الفتاح بيومي حجازي، النظام القانوني لحماية الحكومة الإلكترونية، الكتاب الثاني، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، ٢٠٠٣ ، ص ٣٥.

[30] () د. إيهاب خليفة، القوة الالكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الانترنيت، دار العربي، ٢٠١٧، ص٥.

(٣١)أعلن الرئيس الأميركي بارك أوباما، أن ضمان "أمن" الأمن السيبراني، يأتي في مقدمة اهتماماته معتبرًا التهديد الآتي من الأمن المعلوماتي، من أخطر المسائل التي تطرح على المستوى الاقتصادي و مستوى الأمن القومي، ربما يكون هذا تفسير لتعيينه ووقتها مسؤولا عن تأمين الأمن السيبراني، يكون على اتصال وتنسيق دائمين معه، ويكون عضواً في الأمن القومي، وفي المجلس الاقتصادي الوطني، ينظر ياسمين عبد اللطيف زرد، الولايات المتحدة بحاجة لوكالة مركزية للأمن السيبراني، مقال منشور على الانترنت على موقع مجلة الشروق الالكترونية، على الرابط https://www.shorouknews.com/columns/view.aspx ، الزيارة في ٥-١٢-٢٠٢٢.

٣٢ ) see P.K. Huth, Deterrence and international conflict: Empirical findings and theoretical debates, Annual Review of political science, second part, 1999, p.p. 25- 36.

٣٣ () ينظر د. سوسن العساف، إستراتيجية الردع: العقيدة الأمريكية الجديدة و الاستقرار الدولي، الطبعة الأولى، الشبكة العربية للأبحاث و النشر، ٢٠٠٨، ص ٢٦٢.

٣٤ () ينظر الهام ناصر، نظرية الردع، مقال منشور على الانترنت و على موقع الموسوعة السياسية على الرابط www.political-encyclopedia.org/dictionary/ الزيارة في ٢٠-١٢- ٢٠٢٢.

٣٥ () ينظر تفصيلا د. شادي عبد الوهاب منصور، حروب الجيل الخامس: اساليب "التقجير من الداخل" على الساحة الدولية، سلسلة كتب المستقبل، الطبعة الأولى، العربي للنشر و التوزيع، القاهرة، ٢٠١٩، ص١٨٥- ١٨٨.

٣٦ () ينظر د. إيهاب خليفة، الحرب السيبرانية: الاستعداد لقيادة المعارك في الميدان الخامس، سلسلة كتب المستقبل، الطبعة الاولى، العربي للنشر و التوزيع، القاهرة، ٢٠٢١، ص ١٠-١١.

٣٧ ) مشار للتعريف لدى د. أحمد عبيس الفتلاوي و أزهر عبد الأمير الفتلاوي، المسؤولية الناشئة عن استخدام وسائل القتال الفتاكة في نشر الأوبئة: الهجمات السيبرانية في مواجهة جائحة كورونا نموذجا، بحث منشور، مجلة الحقوق، كلية الحقوق، الجامعة المستنصرية، المجلد ١، العدد ٤١، ٢٠٢١، ص ٣١.

٣٨ ) Michael schmitt, computer network attack and the use of force in international law, thought son normative, framework approved for public release, distribution unlimited,1998, pp-4-8.

٣٩ () ينظر: نور امير الموصلية، الهجمات السيبرانية في ضوء القانون الدولي الإنساني، رسالة ماجستير، كلية القانون، الجامعة الافتراضية السورية، ٢٠٢١، ص ١٩.

٤٠ ) James A. Green, Cyber Warfare ;Multi-Disciplinary and Analysis, 2016 , P.61.

٤١ ) Mehdi Kadivar, Cyber – Attack Attributes, Technology Innovation Management Review, October, 2014,P.26.

٤٢ ) Steven l. kwast, timothy m. McKenzie, Is Cyber Deterrence possible?, Air force research Institute, Papers air, University Press, 2017,p.14.

٤٣ )Kenneth gears , The Challenge of cyber-attack deterrence , computer law &security report, vol.303, 2010, p.301.

٤٤ () البعض يشير لمصطلح الأمن القومي كمرادف لمصطلح الأمن الوطني أو الأمن العام، و يؤكد أن بعد معاهدة وستاليا عام ١٦٤٨ م بات الفقه يسمي هذا النوع من الأمن ب" الأمن الوستالي"، كون إنّ هذه المعاهدة هي التي أسست إلى ظهور الدولة القومية الحديثة القائمة على الرابطة الوطنية" الجنسية بين أبناء الأمة الواحدة داخل كل دولة، ينظر زينب رياض جبر، التجسس الرقمي في ضوء قواعد القانون الدولي، أطروحة دكتوراه، كلية القانون، جامعة كربلاء، ٢٠٢١، ص ٣٢.

٤٥ () ينظر عادل عبد الصادق، أثر الإرهاب الإلكتروني على مبدأ استخدام القوة في العلاقات الدولية، رسالة ماجستير، كلية العلوم السياسيَّة، جامعة القاهرة، ٢٠٠٩، ص ٢٩.

(٤٦) د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، ٢٠٠٧، ص ٢٩

[٤٧] ) Christophe Haynes, Stuart Casey-Maslen, Thomas Robert, The definition of an" attack" under the law of armed conflict, articles of war, Nov 3, 2020, pp. 3-9.

[٤٨]( ) شهدت جورجيا في عام ٢٠٠٨ اعتداء مسلحا من قبل جارها الكبيرة و القوية "روسيا"، و ترافق مع هذا الاعتداء العديد من الهجمات السيبرانية، التي اتفق عليها عدد من المحللين بأنّ مصدرها كان روسيا نفسها، و قد كانت خطرة جدا، حتى و إنْ كان ضررها الفعلي في حده الأدنى، ينظر: نورة شلوش، القرصنة الإلكترونية في الفضاء السيبراني: التهديد المتصاعد لأمن الدول، بحث منشور، مجلة مركز بابل للدراسات الإنسانية، مركز بابل للدراسات الانسانية، جامعة بابل، المجلد٨، العدد٢،٢٠١٨، ص، ١٩٥- ١٩٦، و رغد البهي، مصدر سابق، ص ٥٤.

[٤٩] حنين جميل أبو حسين، مصدر سابق، ص ٣٤

[٥٠] ينظر المادة ٩ من دستور العراق لعام ٢٠٠٥.

[٥١] ( تم إعادة تأسيس جهاز المخابرات الوطني العراقي بعد سقوط النظام البائد في عام ٢٠٠٣، لا سيما بعد إشارة الدستور لهذا الجهاز و دوره في حماية الأمن العام الوطني على وفق المادة ٩ اعلاه منه؛ و جعله تحت السيطرة المدنية وأخضعه لرقابة مجلس النواب العراقي، مع ارتباط هذا الجهاز بمجلس الوزراء؛ و جري بالذكر أن المادة ٨٤ من الدستور اشترطت أنْ يتم تنظيم عمل هذا الجهاز بقانون تحدد بموجبه صلاحياته و واجباته، و الغريب أنه لم يصدر هذا القانون لحد الآن، مما يدفعنا لوضع أكثر من مؤشر على هذا الأمر، و من البديهي التساؤل عن كيفية عمل هذا الجهاز طوال هذه المدة بدون التشريع المطلوب؟ ينظر عما ورد اعلاه وميض عبد المهدي، اختصاص وزارة الداخلية في حفظ الامَن العام وفقاً لقانون رقم (٢٠) لسنة ٢٠١٦(دراسة مقارنة)، رسالة ماجستير، معهد العلمين، العراق، ٢٠٢١، ص ١٥.

[٥٢] ( ينظر لمعلومات مفصلة، سعد السعيدي، مشروع قانون جهاز المخابرات العراقي، مقالة على الانترنت و على موقع تللسقف و على الرابط
www.tellskuf.com/index.php/mq/63145-de68.html ، الزيارة في شهر ١١/ ٢٠٢٢.

[٥٣] ( نقلا عن فارس رشيد البياتي، التنمية الاقتصادية سياسيا في الوطن العربين أطروحة دكتوراه، كلية الإدارة و الاقتصاد، الاكاديمية العربية المفتوحة في الدنمارك، عمّان، ٢٠٠٨، ص ٦٣.

[٥٤] الترويج لثقافة وطنية للأمن السيبراني، الشبكة الدولية للمعلومات ( الانترنت) على الموقع:
www.itu.int/dms_pub/itu-d/opd/stg/D-STG-SG01.22-2010-MSWAdocx

[٥٥] ( العراق سن قانونا خاصا بالمعاملات الالكترونية و بآليات إبرامها و إجرائها أسماه (( قانون التوقيع الالكتروني و المعاملات الالكترونية رقم ٧٨ لسنة ٢٠١٢))، وقد جاء في أسبابه الموجبة أن صدوره جاء انسجاما مع التطور الحاصل في مجال تكنولوجيا المعلومات و الاتصالات و انشطة الانترنت، و توفير الأسس و الأطر القانونية للمعاملات الالكترونية من خلال وسائل الاتصالات الحديثة، و تشجيع صناعة الانترنت..... و تطويع النظام القانوني التقليدي بما ينسجم مع نظم تقنية المعلومات الحديثة؛ لابد من الذكر أن سن هذا القانون قد جاء ترجمة كذلك لقانون تصديق العراق على اتفاقية تنظيم أحكام التوقيع الالكتروني في مجال المعاملات الالكترونية في البلاد العربية رقم ١٠١ لسنة ٢٠١٢، و التي ابرمت ووقع عليها العراق في القاهرة عام ٢٠٠٨، و يحمد للمشرع العراقي هذا التوجه في صدد تشريع هذا القانون، رغم تأخره في التصديق على الاتفاقية المذكورة و سن القانون اللازم لوضعها موضع التنفيذ في الداخل العراقي.
ينظر متن القانون اعلاه، مجموعة القوانين العراقية، اعداد المهندس صفاء الزبيدي، الطبعة الاولى، بغداد، ٢٠٢٠، ص٣.

[٥٦] عبدالله السحبياني، كفاءة الإجراءات الإدارية في المحافظة على أمن المعلومات، رسالة ماجستير، الرياض، جامعة نايف العربية للعلوم الأمنية ، ٢٠١١ ، ص ١٢٤

[٥٧] حنين جميل أبو حسين، المصدر السابق ، ص ٣٩

[٥٨] راجع المادة ٢٥ من دستور العراق ٢٠٠٥.

(٥٩) راجع المادة ٢٧ / ثانيًا من الدستور اعلاه لعام ٢٠٠٥.
٦٠ () ينظر زينب رياض جبر، مصدر سابق، ص ٣١.
(٦١)محمد أمين البشري، التحقيق في الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، مركز الدراسات والبحوث، الرياض، ٢٠١٤ ، ص ٢٢
(٦٢) د. علي الطوالبة، التفتيش الجنائي على نظم الحاسوب والإنترنت، الطبعة الاولى، عالم الكتب الحديث، الاردن، ٢٠١٥، ص ٥٦
(٦٣) ينظر المادة ٨ من دستور العراق لعام ٢٠٠٥.
(٦٤) ينظر: المادة ٧ من دستور عام ٢٠٠٥.
(٦٥) راجع المادة ١٥ من الدستور العراقي ٢٠٠٥
(٦٦) راجع المادة ١٧ من الدستور العراقي ٢٠٠٥
(٦٧) راجع المادة ٤٠ من الدستور العراقي ٢٠٠٥
٦٨ () ينظر نص المادة ٥٠ من قانون ادارة الدولة للمرحلة الانتقالية، منشور على الانترنت على موقع مجلس القضاء الاعلى، على الرابط
www.sjc.iq/view.78/الزيارة في كانون الثاني ٢٠٢٢.
٦٩ () تنظر المادة ١٠٢ من دستور عام ٢٠٠٥ بخصوص الهيئات المستقلة.
٧٠ () ينظر د. مصدق عادل طالب و حسين فياض نايف، الأساس الدستوري و القانوني للمؤسسات الوطنية لحقوق الانسان في العراق و مدى موائمتها مع المعايير الدولية، بحث منشور، مجلة العلوم القانونية، كلية القانون، جامعة بغداد، مجلد ٣٦، العدد ٣، ٢٠٢١، ص ٦٨٨- ٦٨٩.
(٧١) راجع المادة ٤٠ من الدستور العراقي ٢٠٠٥
(٧٢) د . أميرة عبد العظيم محمد، المصدر السابق، ص ٤٦٠
٧٣ **) N. Lucchi, "Access to Network Services and Protection of Constitutional Rights: Recognizing the Essential Role of Internet Access for the Freedom of Expression", Journal of International and Comparative Law (JICL), Vol. 19, No. 3, 2011, p.214.**
(٧٤) تم عقد القمة بناء على قرار اتخذته الجمعية العامة للأمم في ديسمبر ٢٠٠١ وعقد مؤخرا منتدى القمة العالمية لمجتمع المعلومات ٢٠٢٠ لتعزيز التحول الرقمي والشراكات العالمية لتحقيق أهداف التنمية المستدامة ويمثل هذا المؤتمر أكبر تجمع سنوي في العالم لمجتمع "تكنولوجيا المعلومات والاتصالات من أجل التنمية" وأثبت منتدى القمة العالمية لمجتمع المعلومات، الذي شارك في تنظيمه الاتحاد الدولي للاتصالات واليونسكو وبرنامج الأمم المتحدة الإنمائي و الأونكتاد، بالتعاون الوثيق مع جميع المشاركين في خط العمل للقمة العالمية لمجتمع المعلومات، أنه آلية فعالة لتنسيق أنشطة التنفيذ بين أصحاب المصلحة المتعددين، وتبادل المعلومات، وإنشاء أصناف من المعرفة وتبادل أفضل الممارسات وتواصل تقديم المساعدة في تطوير الشراكات بين أصحاب المصلحة المتعددين والقطاعين العام والخاص للنهوض بأهداف التنمية.
سيوفر هذا المنتدى فرصًا منظمة للتواصل والتعلم والمشاركة في مناقشات أصحاب المصلحة المتعددين والمشاورات حول تنفيذ القمة العالمية لمجتمع المعلومات .سيتم بناء جدول أعمال وبرنامج المنتدى على أساس التقديمات التي وردت خلال عملية المشاورة المفتوحة. راجع في ذلك د. أميرة عبد العظيم، مصدر سابق، ص هامش ٤٦٢ و ٤٦٣
٧٥ () و في العام نفسه أي في ٢٠١١ أبرمت الدول العربية ،الاتفاقية العربية لمكافحة جرائم تقنية المعَلومات هذه الاتفاقية فِي تاريخ (٢٠١١/١٢/٢١)، و وقعت عليها دول عربية عدة منها العراق و صادق عليها، جاء في ديباجتها: " إنَ الدول العربية الموقعة، رغبة منها في تعزيز التعاون فيما بينها لمكافحة جرائم تقنية المعلومات التي تَهدد أمنها ومصالحها وسلامة مجتمعاتها، واقتناعاً منها بضرورة الحاجة إلى تبني سياسة جنائية مشتركة تَهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات، وأخذاً بالمبادئ الدينية والأخلاقية السامية، ولا سيما أحكام الشريعة الإسلامية، وكذلك بالتراث الإنساني للأمة العربية التي تنبذ كل أشكال الجرائم، ومع مراعاة النظام العام لكل دولة، وإلتزاماً بالمعاهدات

والمواثيق العربية والدولية، المتعلقة بحقوق الإنسان ذات الصلة من حيث ضمانها واحترامها وحمايتها، **المادة الأولى**: الهدف من الاتفاقية: هدف هذه الاتفاقية الى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، لدرء أخطار هذه الجرائم حفاظا على أمن الدول العربية، ومصالحها وسلامة مجتمعاتها وأفرادها) ، المادة الثالثة: مجالات التطبيق: تنطبق هذه الاتفاقية ما لم ينص على خلاف ذلك، على جرائم تقنية المعلومات بهدف منعها والتحقيق فيها وملاحقة مرتكبيها، وذلك في الحالات الآتية:

١- ارتكبت في أكثر من دولة
٢- ارتكبت في دولة وتم الإعداد أو التخطيط لها أو توجيهها أو الإشراف عليها في دولة أو دول أخرى.
٣- ارتكبت في دولة وضلعت في ارتكابها جماعة إجرامية منظمة تمارس أنشطة في أكثر من دولة.
٤- ارتكبت في دولة وكانت لها آثار شديدة في دولة أو دول أخرى.

و في الحقيقة يحسب للدول العربية تنبهها للمخاطر السيبرانية كافة في مثل هذا الوقت و إبرامها لهذه الاتفاقية التي أملت من وراءها أن تكون الدول على مستوى عال من الجدية، لغرض وضع أحكامها موضع التنفيذ، ليس فقط بالمصادقة عليها، بل مع إصدار التشريعات الوطنية اللازمة لدمجها مع قوانينها الداخلية، لكي يكتمل إطار الحماية و الردع المطلوب بالثالوث الخاص به –لو صح التعبير- وهو " الاتفاقية الدولية الخاصة، أحكام الدستور ذات العلاقة، التشريع الداخلي الخاص بدمج الاتفاقية مع القانون الداخلي"، ينظر نص الاتفاقية على الانترنت، على الرابط /www.ar.wikisource.org/wiki/الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

(٧٦) ينظر د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، اتحاد مكتبات الجامعات المصرية، مصر،٢٠٠٩ ، ص ٤٧

(٧٧) د. حسنين المحمدي بوادي، الإرهاب الدولي بين التجريم والمكافحة، دار الفكر العربي، القاهرة ، ٢٠٠٦ ، ص ٥٤

٧٨ () و من أبرز هذه التهديدات كما تعرفنا عليها: الارهاب الالكتروني، الهجمات الالكترونية متنوعة الصور متعددة الغايات، التجسس الالكتروني الذي صار ديدن حكومات و ليس الأفراد و الشركات الأمنية فقط، و أخطرها إساءة و استغلال الاطفال جنسيا عبر الانترنت.

٧٩ () في هذا النوع من التعاون سيكون من المحتم ان تشترك عدة مؤسسات دستورية و حكومية في سبيل تحققه بفعالية، منها مجلس النواب العراقي لأغراض الموافقة على ما يبرم من اتفاقيات و بروتوكولات خاصة بالأمن السايبر، كذلك وزارات الخارجية و الداخلية و تكنولوجيا المعلومات و التخطيط و المالية، فضلا عن مؤسسات وزارة الدفاع ذات التخصص المباشر بالأمن العسكري المعلوماتي، ينظر للتفصيل وثيقة استراتيجية الأمن السيبراني العراقي، إعداد مستشارية الأمن الوطني/ اللجنة الفنية العليا لأمن الاتصالات و المعلومات، على الانترنت و على الرابط www. nsa.gov.iq ، ص٢ من الوثيقة، الزيارة في ٣٠-٢١-٢٠٢٢.

٨٠ ) **Samuel Dominion, Stability, internet management, and disinformation, Euromesco Policy Study, European Institute for the Mediterranean, No. 22, 2021, pp.34- 35.**

٨١ () يعرف الأمن الإنساني بأنه "ضمان أمن الأفراد من مخاطر متنوعة على رأسها الأمراض والإرهاب والفقر والمخدرات ووجود نظام عالمي غير عادل، وذلك عن طريق تحقيق التنمية وإصلاح المؤسسات الدولية وعلى رأسها الأمم المتحدة والمنظمات الاقتصادية العالمية، كصندوق النقد الدولي والبنك الدولي للتعمير والتنمية، وذلك عبر شراكة حقيقية بين دول العالم كلّها" ينظر: خولة محي الدين يوسف، الأمن الإنساني وأبعاده في القانون الدولي، بحث منشور، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد ٢٨، العدد الثاني، ٢٠١٢، ص٥٢٦.

٨٢ ) Tim Jordan, Cyber power: The Culture and Politics of Cyberspace, Rout ledge and the Internet, 2000, pp.160-200.

(٨٣) صلاح مهدي هادي و زيد محمد علي، الأمن السيبراني كمرتكز جديد في الاستراتيجية العراقية، بحث منشور، مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين، العدد ٦٢، السنة ١٢ ، ٢٠٢٠، ص ٢٧٦

[٨٤] () د. أميرة عبد العظيم محمد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي، بحث منشور، مجلة الشريعة والقانون، كلية الشريعة والقانون، جامعة الأزهر، مصر، العدد ٣٥، المجلد ٣، ٢٠٢٠، ص ٤٣٨.

[٨٥] ) Myriam A. Dunn, The Internet and the Changing Face of International Relations and Security, Volume number: 7, Bulgaria, Sofia, ProCon Ltd., Issue number: 1, 2001.

[٨٦] ) Kamal Ahmad Khan, Use of Force and Human Rights under International Law, Athens Institute for Education and Research, Conference Paper Series BLE, 2017, p. 2205

(٨٧) د .نبيل أحمد حلمي، القانون الدولي وفقاً لقواعد القانون الدولي العام، دار النهضة العربية، القاهرة، ١٩٩٩، ص ١٢٠ – ٢٠٠

[٨٨] () اليوم أصبحت أدوات ممارسة القوة في العلاقات الدولية متعددة، على وفق قدرات و امكانيات و رغبات القوى المشاركة فيها، و لفترة طويلة كانت القوة العسكرية من أهم هذه الأدوات؛ كما قد تكون القوة الاقتصادية و الحصار الاقتصادي عاملا رئيسا للسيطرة على الخصم و ممارسة القوة عليه.

إلا أن ما يقصده الباحث بالقوة هنا ليس أي مما ذكر من أدوات القوة، بل ما يقصده هو ضرورة امتلاك الدولة للقوة السيبرانية، من خلال وسائل الاتصال و التكنلوجيا الحديثة و الإنترانت التي هي اليوم عاملا حاسما في أي صراع قد ينشب بين أي دولتين، إذ يتميز العصر الراهن بظاهرة الثورة الصناعية للمعلومات و التكنولوجيا التي أزاحت الكثير من عناصر القوة و أدواتها التقليدية عن مواقعها التي تربعت عليها لفترة طويلة، وهو ما عرض المفهوم التقليدي للقوة إلى انتقادات عديدة، و أفصح عن محتوى جديد للقوة، لا يعتمد على قدرات عسكرية من معدات و عتاد و قوات بشرية مدربة بصنوف مختلفة، فهذه لم تعد كافية لأي دولة لتتبلور كقوة ذات تأثير و فاعلية، ما دعا الى ضرورة وجود شكل جديد هو القوة السيبرانية التي يتصاعد دورها يوما بعد على المستويين العالمي و الدولي.

فمن ناحية ادت الى توزيع و انتشار القوة بين عدد اكبر من الفاعلين، ما جعل قدرة الدولة على السيطرة على هذا الميدان موضع شك مقارنة بالمجالات الاخرى، و من ناحية أخرى جعلت القوة السيبرانية، بعض الفاعلين الاصغر في الساحة العالمية لديهم قدرة اكبر على ممارسة كل من القوة الصلبة و الناعمة عبر الفضاء السيبراني، وهو ما عنى تغيرا واضحا في علاقات القوى في السياسات الدولية.

ف القوة السيبرانية هي: القدرة على الحصول على النتائج المرجوة، من خلال استخدام مصادر المعلومات المتداولة و المرتبطة بالفضاء السيبراني، أي إنها القدرة على استخدام الفضاء السيبراني لخلق مزايا فاعلة و للتأثير في الاحداث المتعلقة بالبيئات الواقعية الأخرى، و ذلك كله يكون عبر أدوات إلكترونية يحسن استخدامها من قبل مختصين.

[٨٩] () يذكر أن مسؤولين عسكريين أميركان أبدوا قلقهم و مخاوفهم من تعرض بلدهم لهجمات سيبرانية متكررة، طالت المنشئات الحساسة و البنى التحتية المختلفة و الاعلام و مؤسساته، كان مصدر أغلبها على حد زعمهم الصين، وهذا المر بالذات و ماتعرضت له دول غربية عدة من أمر مماثل، جعل حلف الشمال الأطلسي بدوله كافة يؤكد أنّ الحرب الألكترونية أصبحت سلاحا جديدا، و أثره كأثر الاسلحة التقليدية الأخرى على الدولة؛ إن لم يكن أشد من ذلك، وهو الأمر الذي دفعهم إلى تبني ما بات يعرف ب "عقيدة التالين الاستراتيجة(استراتيجية تالين) المكونة من ٢٨٢ صفحة"، تضمنت رؤى و اساليب و تكتيكات جلها تعلق بالحرب الالكترونية المستحدثة و خطط مواجهتها، و من أبرز ما جاء فيها الاعتراف بالحق للدولة المعتدى عليها و التي ترعضت لهجوم الكتروني مؤذي، بأن تشن هي ذاتها هجوما الكترونيا مقابلا على دولة مصدر الهجوم الأول، و الأخطر أن عقيدة تالين ضمنت الحق للدولة المعتدى عليها في مثل هكذا هجوم بأمكانية استخدام القوة العسكرية المادية الحقيقية، في حال أدى الهجوم الالكتروني عليها، إلى إيقاع خسائر بشرية في الأرواح، أي من مواطنيها.

و واضح مكمن الخطورة في ما انتهت اليه هذه العقيدة، و أيا ما كانت مبرراتها، ف لابد من التذكير أن القانون الدولي الانساني يحظر الأعمال الانتقامية، لأنها جرائم بالأصل يرد بها على جرائم مماثلة، كما إنّ الهجوم العسكري او

الالكتروني في مثل هذه الحالة ليس هو المعنى الذي يقصد الباحث توضيحه للقارئ فيما يخص ضرورة امتلاك كل دولة لمقومات الردع السيبراني، وهو ما اقتضى التنويه هنا، اتساقا مع ما تقدم من معنى للردع السيبراني.
للمزيد عن عقيدة تالين و ما قررته دول الناتو فيها، ينظر علي زياد فتحي، العمليات السيبرانية الأوروأطلسية و مهددات الجيوسيبرانية الروسية: رؤية في الاشتباك السيبراني الأورو- روسي، بحث منشور، مجلة حمورابي للدراسات، مركز حمورابي للبحوث و الدراسات الاستراتيجية، العدد ٣٠، السنة السابعة، بغداد، ٢٠١٩، ص ٨-١٠.

[٩٠] () لقدّ اعتمدَ "مجلس وزراء العدل العرب"، قانون الإمارات لمكافحة جرائم تقنية المعلومات لسنة ٢٠٠٤م في دورته التاسعة عشر، عَلَى حين اعتمدَهُ بَعْدها "مجلس وزراء الدَاخليّة العرب"، في دورته الحادي والعشرون. ف الامارات كانت السباقة في الدعوة لتبني هكذا قانون، و سباقة في الدعوة لتبني اتفاقية عربية لمكافحة جرائم المعلوماتية، من هنا جاء طلب الأمانة العَامّة لجامعَة الدول العربية أنّ يتم تعميم قانون الإمارات في مكافحة جرائم تقنية المعلوماتية عَلَى وزارات الدَاخليّة للدول العربية، ومعَ ذَلكَ لمّ تعره أغلبيّة الدول الاهتمام الكافي ومنها العراق، كما نجد أن المشرع الأردني نظمَ الأمن السيبراني عام ٢٠١٩، أما المشرع المصري فقد نظمه بقانون الجرائم الإلكترونية بالقانون رقم ١٧٥ لسنة ٢٠١٨، ينظر قراري مجلس وزراء العدل و الداخلية العرب في الدورة التاسعة عشرة و الحادية و العشرون برقم ٤١٧/ ٢١ لعام ٢٠٠٤، مشار له لدى أ. نوفل عبد الله و أ. محمد عزت، جريمة إنشاء مواقع أو نشر معلومات مخلة بالآداب العامة بوسائل تقنية المعلومات، بحث منشور، مجلة الرافدين للحقوق، كلية الحقوق، جامعة الموصل، المجلد ١٢، العدد ٤٤، ٢٠١٠، ص ٣٠٧.

[٩١] () ينظر د. وصال نجيب العزاوي، مبادئ السياسة العامة، دار أسامة للنشر والتوزيع، عمان، الأردن، ٢٠٠٣، ص ٢٤.

[٩٢] () ينظر د. عبد الفتاح باغي، السياسة العامة: النظرية والتطبيق، جامعة الإمارات العربية المتحدة، الطبعة الأولى، ٢٠٠٩، ص٢٥.

[٩٣] ) Thomas R. Dye, Understanding public policy, Englewood Cliffs, N.Prentice-Hall, 2nd ed., 1975,p.p. 1-3.

[٩٤] () للمزيد ينظر د.جيمس جيفرسون، صنع السياسات العامة، ترجمة د. عامر الكبيسي، دار المسيرة للنشر و التوزيع و الطباعة، عمان، الاردن، ١٩٩٨، ص١٥- ١٦.

[٩٥] () الأعم الأغلب من الكتاب و الباحثين يقرون بأرتباط مفهوم السياسة العامة بما تعده الحكومة و تخططه و تضمنه مناهجا الوزاري أو برنامجها الحكومي، للتدليل ينظر د. أحمد علي عبود، آليات رسم السياسة العامة في دستور جمهورية العراق لسنة ٢٠٠٥، بحث منشور، مجلة جامعة أهل البيت عليه السلام، العدد ٢٩، ٢٠٢١، ص ٢١٢.

[٩٦] () للمزيد من التفصيل ينظر هدير مشرع حسين، اختصاص السلطات الاتحادية في وضع سياسة الأمن الوطني و تنفيذها: دراسة مقارنة، رسالة ماجستير، معهد العلمين للدراسات العليا، ٢٠٢٠، ص ١٦- ى١٩.

[٩٧] () ينظر وثيقة استراتيجية الأمن السيبراني العراقي، إعداد مستشارية الأمن الوطني/ اللجنة الفنية العليا لأمن الاتصالات و المعلومات، مصدر سابق، ص ٦.

(٩٨) عبد الله داغش العجمي، المشكلات العلمية والقانونية للجرائم الإلكترونية" دراسة مقارنة"، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، الأردن، ٢٠١٤، ص ٨٨

(٩٩) راجع د. باسم على خريسان، الأمن السيبراني في العراق – قراءة في مؤشر الأمن السيبراني العالمي ٢٠٢٠ ، بحث منشور، و على موقع مركز البيان للدراسات والتخطيط على الانترنت، ٢٠٢١، على الرابط http://www.bayancenter.org. الزيارة في ٢٠-١٠- ٢٠٢٢، ص٩ من البحث.

(١٠٠) صلاح محمد مهدي و زيد محمد علي، الأمن السيبراني كمرتكز جديد في الاستراتيجية العراقية، مصدر سابق، ص ٢٩١ و د . باسم على خريسان، المصدر السابق، ص ١٠.

(١٠١) علي زياد العلي، التحديات غير المرئية للأمن الوطني العراقي، مقال منشور، مركز البيان للدراسات والتخطيط، بغداد، نشر ٢٠١٨/٦/٢٦،الشبكة الدولية للمعلومات (الانترنت ) على الموقع www.bayancenter.org تم الاطلاع على المصدر يوم ٢٩ / ١١ / ٢٠٢١.

(١٠٢) صلاح محمد مهدي و زيد محمد علي، الأمن السيبراني كمرتكز جديد في الاستراتيجية العراقية، مرجع سابق، ص ٢٧٨

(١٠٣) د. صلاح مهدى هادى ود. زيد محمد على أسماعيل، الأمن .....، ذات المصدر أعلاه، ص ٢٧٩.

(١٠٤) د. حنين جميل أبو حسين ، الإطار القانوني لخدمات الأمن السيبراني ، مصدر سابق ، ص ٥٠

١٠٥ () ينظر محمد كاظم محمود, مجلس الوزراء في العراق ولبنان (دراسة مقارنة), أطروحة دكتوراه, كلية الحقوق, الجامعة الإسلامية اللبنانية, بيروت, ٢٠١٩, ص، ٢٨٤، و ينظر صالح هادي منسي, تشارك السلطة التنفيذية مع البرلمان بالتشريع في النظام البرلماني (دراسة مقارنة), رسالة ماجستير, معهد العلمين للدراسات العليا, العراق, ٢٠١٦, ص ٨٣، و المادة (٢) مَن قانون وزارة الداخلية رقم (٢٠) لسنة٢٠١٦ الَّتي نصت (اولاً: تنفيذ سياسة الامَن الوطني للدولة في حفظ الامَن الداخلي والمساهمة في وضع ورسم تلك السياسة), الوقائع العراقية, رقم العدد ٤٤١٤, تاريخ العدد٢٩-٨-٢٠١٦, ص٣، و كذلك القسم الرابع مَن امر (٦٧) سلطة الائتلاف لسنة ٢٠٠٤, الذي جاء فيه (... ٣- تكون مهمة وزارة الدفاع هي تأمين وحماية وضمان أمن الحدود العراقية والدفاع عن العراق), الوقائع العراقية, رقم العدد ٣٩٨٣ لعام ٢٠٠٤, ص١٤.

(١٠٦) د. محمد أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمان، ط3 ، ٢٠٢٠ ، ص354

(١٠٧) قامت الدول العربية و بوساطة جامعة الدول، بوضع الاتفاقية العربية لمكافحة جرائم تقنية المعلومات عام ٢٠١٠

(١٠٨) راجع الوقائع العراقية، العدد ٤٢٩٢، ٣٠ أيلول ٢٠١٣

(١٠٩) مجلة الوقائع العراقية، المصدر السابق، ص ١

١١٠ () بات شبح "الإرهاب السيبراني" يطل علينا في الأفق بوصفه أزمة عالمية جديدة، الامر الذي جعل هذا الفضاء المعلوماتي، مجالاً للأعمال والهجمات والجرائم الالكترونية الارهابية من جانب افراد، جماعات، أوْ مؤسسات؛ وأصبحت هذه المجاميع، تضع سيناريوهات اجرامية عدة؛ يقوم بها الإرهابيون باستهداف البنى التحتية للدول، وأنظمة معلوماتها، وقواعدها العسكرية، والبنى الاقتصادية والتجارية من خلال هجمات سايبرانية، تفوق اثارها و من دون مبالغة، تلك التي قد تنتج عن الإرهاب التقليدي، هذا فضلاً عن إستغلال "الفضاء السايبر" من قبل الجماعات الإرهابية التي تبنت النهج الأرهابي علنا، تستخدمه في خدمة اغراضها المختلفة ذات الصلة بنشاطاتها، هذا الواقع و غيره من الحقائق، هي ما باتت تدفع حكومات الدول اليوم، لضرورة تبني سياسات و استراتيجيات ببرانية واعدة لدفع المخاطر هذه كلها، و توقي حدوثها عليها و على مواطنيها، و هذا هو بالفعل ما قصده الباحث من وراء مفهوم الردع السيبراني؛ للمزيد ينظر: محمد زهير عبد الكريم، الإرهاب السيبراني: أزمة عالمية جديدة، بحث منشور، مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين، العدد ٦٤، ٢٠٢١، ص ٢٧٧ و ص ٢٨٢- ٢٨٤.

(١١١) راجع مشروع قانون مكافحة الجرائم الإلكترونية العراقي، والذي رفضه مجلس النواب العراقي ولم يصدر حتى الآن، ٢٠١٩.