جامعة محمد بوضياف المسيلة

كلية الحقوق والعلوم السياسية **فرع:** علاقات دولية

قسم العلوم السياسية والعلاقات الدولية **تخصص:** علاقات دولية

مذكرة مكملة لنيل شهادة الماستر الأكاديمي تخصص علاقات دولية بعنوان:

التهديدات الإلكترونية و الأمن القومي.

إعداد الطالب:

عجيل فطيمة الزهرة

إشراف الأستاذ:

عرجون شوقي

أعضاء لجنة المناقشة:

الأستاذ: غربي عزوز	**رئيسا**
الأستاذ: عرجون شوقي	**مشرفا ومقررا**
الأستاذ: عاشور سليم	**مناقشا**

السنةالجامعية:2018 / 2019

اهداء

أسال الله سبحانه وتعالى أن يجعل هذا العمل المتواضع في ميزان الحسنات،يوم لا ينفع مال ولا بنون إلا من أتى الله بقلب سليم.أهدي هذا العمل المتواضع إلى:

وطني الحبيب...محبة وصدقا ووفاء...ربي اجعل هذا البلد آمنا.

إلى من حملتني في بطنها وهنا على وهن، ولازالت تحملني برعايتها وحنانها، إلى من أهدتني حياتها وسهرت الليالي من أجل راحتي، إلى من الجنة تحت أقدامها، إلى رمز الصمود والصبر والعطاء بغير حساب، إلى من بسهرها ودعائها تفتح الأبواب في وجهي، إلى أعز ما أملك في الدنيا، إلى معلمتي في الحياة :أمي الغالية.

إلى عوني ومنبع راحتي، إلى من صنع حاضري وكان لي السند المتين، إلى من ناضل من أجلي لأرتاح وهيأ لي أسباب النجاح، والذي سعى جاهدا على تربيتي وتعليمي، إلى الشمعة التي أنارت دربي :أبي الغالي.

إلى القلب الرفيق الطيب، إلى توأم روحي :أختي الحبيبة ، كما أتقدم بالإهداء لزوجها عيساوي عبد الوهاب.

باقة امتنان إلى إخوتي: عبد الحميد، فاتح ،محمد وفاق...محبة وصدقا ووفاء وتقديرا.

إلى من رسما البسمة في بيتنا، إلى كتاكيت العائلة :أكرم، زياد.

إلى من لا يقاس رحيله بأي وجع، إلى قرتي عيني إلى أخي الذي لم تلده لي أمي، إلى روح أخي الغالي :ياسر حمزة غفر الله لك عدد ما هزني الحنين لك إلى جنات الخلد يا أخي، وانس وحشتك وأسكنك فسيح جناته.

إلى أعمامي عمتي، أخوالي وخالاتي، زوجاتهم وأزواجهم، أبنائهم وبناتهم، إلى كل من تجمعني بهم صلة الرحم و القرابة، كل باسمه.

بعدد قطرات الماء في البحر أهدي هذا العمل المتواضع إلى حبيباتي :آية،لميس،أمينة، رندة،سهام،غدير، منار، نور، ملاك، أميرة، بلقيس، مروة ودعاء.

إلى الكتاكيت :نعمة، أمير، محمود.

كما لا يفوتني أن أخص إهدائي بذكر الجدين العزيزين، والجدتين الحنونتين.

إلى روح فقيدتي جدتي حبيبتي، اللهم أنزل على قبرها رحمة واسعة، وأنس وحشتها، وأسكنها فسيح جنتك.

إلى من أضاء دربي وأنار قلبي إلى الدكتور الذي كان كالنور لعيني عرجون شوقي صدقا وشكرا وعرفانا وتقديرا، الذي تحملني ولم يضجر من تساؤلاتي ولم يبخل بتوجيهاته، حفظه الله ورعاه..

إلى من عشت معهم أجمل اللحظات، فإستوت أسماؤهم على عرش قلبي صديقاتي :نسيمة، حفصة، فضيلة، سمية بوعوينة، سمبة، ابتسام، هدى، آسية طرشون، حميدة، حياة، آسية، سليمة، حسناء، سلمى، منيرة، مريم، إيمان وابتسام، سمية، عبلة، صبرينة، إكرام، سعيدة، كهينة، ريان، أمل، خولة، هدى، إيمان، ابتسام، ياسمين، زهرة،ريمة، وفاء، سمية، أسماء، ماجدة، صافية، بسمة، أنيسة،ظريفة، خنساء، ساندي، وفاء، بثينة، مروة، سمية، سمية قامبل، سلمى، حورية. وإلى صديقتي: سامية فلتان.

إلى أصدقائي زملائي في الدراسة :محمد مقيرش، شمس الدين، عبد القادر صخر، كريم، الأزهر، فيصل، حكيم، يوسف، وليد، بلال رحمه الله، أمين، صلاح الدين، عبد الرؤوف، بوزيد، وليد، صالح، عمر،زكريا، هشام، بلال ، محفوظ ، وأخص بالذكر الشخص الذي كان رفيقا وموجها وبسمة في حياتي عيسى.

وإلى كل الرفقاء زميلات وزملاء قسم العلوم السياسية.

إلى كل من ساعدني وساهم في مساندتي وتشجيعي ونصحي ولو بكلمة طيبة شكرا وتقديرا وإحتراما وعرفانا.

وإلى أولئك الذين خذلناهم وخاذلونا شكرا وإمتنانا لكم لقد علمتمونا.

فطيمة الزهرة عجيل

شكر وعرفان

الحمد والشكر والثناء لله لا نحصي عليه ثناء، الحمد لله الذي أنعم علينا بنعمة العقل وأرشدني إلى طريق العلم وجعل من الصعب هينا، الحمد لك حتى ترضى، والحمد لك إذا رضيت، والحمد لك بعد الرضا، والصلاة والسلام على النبي المطهر صاحب الوجه الأنور والجبين الأزهر،أن أمدني بتوفيق لإتمام هذا العمل المتواضع الذي أهدي ثمرته إلى:

إلى كل من كانت إشراقتهم مضيئة، إلى ينابيع الحكمة، إلى شعلة المعرفة أينما حلوا وارتحلوا، أسطر كلمات شكر وتقدير وعرفان إلى من قيل فيهم من علمني حرفا صرت له عبدا، إلى كل معلم مخلص أمين، إلى جميع الأساتذة الذين ساهموا في تكويننا طيلة مشوارنا الدراسي.

كما يطيب لي أن أتقدم بعظيم الشكر والتقدير والعرفان إلى الأستاذ المشرف الدكتور شوقي عرجون، الذي أكن له فائق التقدير والاحترام وأتمنى له دوام الصحة والعافية ومزيد التألق و النجاح، على ما قدمه لي من دعمه في انجاز هذه الدراسة بتوجهاته ونصائحه القيمة وإفادته لي بالمعرفة.

كما أتقدم بخالص الشكر و التقدير إلى أعضاء لجنة المناقشة الدكتور غربي عزوز والدكتور عاشور سليم على تكرمهم بمناقشة المذكرة.

كذلك الشكر مفعم بالاحترام والتقدير والعرفان للهيئة التدريسية بقسم العلوم السياسية والعلاقات الدولية، وخاصة الأستاذ حسام الدين بوعيسي، الأستاذ نور الدين دومي، الأستاذ كمال شطاب، والأستاذ نور الدين فلاك.

إلى عمال مصلحة شؤون الطلبة وأخص بالذكر حليمة، وإلى عمال المكتبة.

إلى الدكتور سعيد كليوات، صدقا وعرفانا وتقديرا واحتراما.

إلى الأستاذة فوزية شرقي، صدقا ومحبة وعرفانا.

إلى رفيقة دربي ورمز الوفاء والإخلاص إلى من شاركتني هذا الجهد، صديقتي وأختي العزيزة والغالية نسيمة نوي.

إلى من أوصاني الله تعالى ببرهما ومصاحبتهما في الدنيا معروفا :والدي الحبيبين أطال الله في عمرها وأقول لهما :ربي ارحمهما كما ربياني صغيرة.

إلى كل من ملأ قلبي ولم يسعه قلمي، إلى قارئ الأسطر وكل من أعرفهم...والحمد لله ربي العالمين.

فطيمة الزهرة عجيل

خطة الدراسة:

مقدمة:

الفصل الأول: الإطار النظري والمفاهيمي للدراسة.

المبحث الأول: تطور مفهوم الأمن القومي.

المطلب الأول: مفهوم الأمن القومي.

المطلب الثاني: أهم الاتجاهات في الدراسات الأمنية.

المطلب الثالث: مهددات الأمن القومي.

المبحث الثاني: مفهوم التهديدات الإلكترونية.

المطلب الأول: تعريف التهديدات الإلكترونية ومضمونها.

المطلب الثاني: أنواع التهديدات الإلكترونية ومستوياتها.

المطلب الثالث: الجهود المبذولة لمحاربة التهديدات الإلكترونية.

الفصل الثاني: الثورة الإلكترونية والأمن القومي

المبحث الأول: المخاطر الإلكترونية على المجتمع والسيادة

المطلب الأول: أثر مواقع التواصل الاجتماعي على الأمن المجتمعي.

المطلب الثاني: التهديدات الإلكترونية وقضايا السيادة.

المطلب الثالث: علاقة الأمن الإلكتروني بالأمن القومي.

المبحث الثاني: نماذج عن التهديدات الإلكترونية.

المطلب الأول: الجريمة الإلكترونية في التشريع الجزائري.

المطلب الثاني: الإرهاب الإلكتروني في الولايات المتحدة الأمريكية.

المطلب الثالث: القرصنة الإلكترونية في روسيا.

المطلب الرابع: الشباب العربي الإسلامي و الحرب الإلكترونية على الاحتلال الإسرائيلي.

الخاتمة.

مقدمة

مقدمة

إن التحولات المتسارعة في عالم مابعد الحرب الباردة أفرزت جملة من التفاعلات المستحدثة على الصعيد الدولي، وكان مفهوم الأمن القومي أهم المفاهيم التي تأثرت بهذه التفاعلات والقوى الجديدة على الساحة الدولية...؛ فالثورة الالكترونية التي شهدها العالم ألقت بضلالها على الدول بشكل لافت وأصبح تحدي تحقيق الأمن القومي تحديا كبيرا بالنسبة للدول بشكل متفاوت، حيث أصبح معيار التحكم في الإلكترونيات حاسما في تحقيق الأمن القومي بأبعاده الجديدة.

كما ودخلت تكنولوجيا الاتصالات والمعلومات الحياة الانسانية بقوة لتكتب بداية لعصرنا الحالي بلغة إلكترونية ومحوسبة، حيث أحدثت هذه الوسائل طفرة علمية غير مسبوقة، وهذه الطفرة أوجدت فوارق كبيرة بين الأمم، لتظهر التقنيات بمختلف مجالاتها، بل وأضافت مجالات جديدة في الحياة البشرية؛ فأحدثت ثورة معلوماتية ضخمةفي جميع القطاعات الاقتصادية؛ الاجتماعية؛ السياسية؛ الثقافية والأمنية التي كان لها وقع كبير على سلوكيات المجتمع وهويته، وانتشار آليات تجمع بين المجموعات البشرية المتمثلة في مواقع التواصل الاجتماعي والتي أحدثت تغيرات كبيرة في الكثير من المقومات الاجتماعية.

وفي المقابل، كلما ازدادت هيمنة وسائل تكنولوجيا الاتصالات والمعلومات كلما زادت المخاطر الإلكترونية التي تهدد أمن الدول و تؤثر عليه وعلى هذا الأساس يمكن اعتبار الأمن الإلكتروني أعلى تحديات الأمن القومي، فقد أسقطت تكنولوجيا الاتصالات والمعلومات مفهوم الحدود الجغرافية، السياسية، والثقافية بين الدولفأصبحت مشكلة عابرة للحدود؛ ما يضع سيادة الدول على المحك خاصة مع اختراق المواقع الحكومية الرسمية والتجسس الإلكتروني على الدول وشن الحروب الإلكترونية عليها.

هذا ما يفرض عليها التعامل مع قضايا التهديدات الالكترونية التي تمس الأمن القومي للدول بمرونة تامة، لأن مستقبل تكنولوجيا الإتصالات في تطور مستمر مما أدى إلى زيادة التهديدات الإلكترونية وتحول شبكة الأنترنت غلى ساحة كبيرة تكثر فيها المخاوف والتهديدات والهجمات، وهذه الهجمات تستطيع أن تدمر البنية التحتية لأي عدو يواجهها، مستخدمة لذلك شكلا من أشكالها والمتمثلة في القرصنة الإلكترونية، التجسس الإلكتروني، الجريمة الإلكترونية، الإرهاب الإلكتروني، الحرب الإلكترونية.

وهذه المنظومة المعلوماتية والتقنية و الهجمات الحاسوبية باتت تؤرق الكثير من دول العالم، وهي وسائل أصبحت تزداد مؤخرا وبشكل قوي مما يدفع بهذه الدول إلى وضع إستراتيجيات لمواجهتها والقضاء عليها.

1. أهمية الدراسة:

إن الاهتمام بموضوع التهديدات الإلكترونية هو حتمية تاريخية عايشتها الدول واهتمت بها اضطراريا لكون المسألة فرضت نفسها في ظل طغاء المتغيرات الإلكترونية على الساحة الدولية في مزاياها ومساوئها.

لذلك تتدرج أهمية الدراسة في أهمية علمية وأهمية عملية:

- **الأهمية العلمية:**

يندرج موضوع الدراسة ضمن الدراسات الأمنية والإستراتيجية التي برزت كحقل مركزي وأساسي في حقل العلاقات الدولية، بالإضافة إلى تطور مفهوم الأمن القومي ليتوسع ويشمل جميع القطاعات السياسية والاجتماعية والاقتصادية والثقافية والأمنية.

- **الأهمية العملية:**

تكمن أهمية الموضوع في تزايد التهديدات الالكترونية في الفضاء الالكتروني الذي يتوسع يوما بعد يوم وهذا نتيجة للمخاطر السلبية التي تشكلها هذه التهديدات على الأمن القومي للدول.

2. أهداف الدراسة:

تسعى هذه الدراسة إلى تحقيق جملة من الأهداف تتمثل في:

- إبراز وتوضيح المفاهيم المتعددة لمتغيرات الدراسة.
- توضيح العلاقة بين الأمن الإلكتروني والأمن القومي.
- إبراز أثر التهديدات الإلكترونية على الأمن القومي في نماذج مختلفة (الجزائر؛ الولايات المتحدة الأمريكية؛ روسيا؛ إسرائيل).

3. مبررات اختيار الدارسة:

- **مبررات الذاتية:**

اهتمامات الباحث الشخصية بالتطورات التكنولوجية، إضافة إلى تنوير القارئ العادي والباحث على حد سواء بالخطورة الخفية التي تحملها التكنولوجيا إذا استعملت دون أخذ احتياطات أمنية صارمة.

- **مبررات موضوعية:**

تسعى الدراسة لتقديم تصور تحليلي للتهديدات الإلكترونية وانعكاساتها على الأمن القومي للدول من خلال الآليات والجهود والسياسات التي تنتهجها الدول في مواجهة هذه التهديدات.

4. إشكالية الدراسة:

في عصرنا الحالي، تزداد أشكال التهديدات الإلكترونية وتتنوع مخاطرها، وفي المقابل تزداد آثار وانعكاسات هذه المخاطر و التهديدات لتشمل جميع القطاعات السياسية، العسكرية، الثقافية، الاقتصادية، الاجتماعية، الأمنية، مهددة بذلك الأمن القومي للدول.

وانطلاقا مما تقدم؛ يمكن تحديد معالم إشكالية الدراسة، وذلك عن طريق صياغتها على النحو التالي:

كيف تؤثر التهديدات الإلكترونية على الأمن القومي للدول؟

وبهدف معالجة هذه المشكلة البحثية قمنا بصياغة الأسئلة الفرعية التالي:

- كيف تطور مفهوم الأمن القومي؟
- ما هي أبرز المخاطر الإلكترونية التي قد تؤثر على الأمن القومي للدول؟
- ما هي النماذج الواقعية التي توضح الجانب الإلكتروني للتهديدات الأمنية؟

5. فرضيات الدراسة:

في نفس السياق الفكري السابق لإشكالية الدراسة؛ تم تصميم وصياغة الفرضيات على النحو التالي:

- هنالك علاقة متبادلة التأثير بين تطور مفهوم الأمن القومي والتطور الإلكتروني والتكنولوجي الذي حدث في العالم.
- أصبحت التهديدات الإلكترونية تحديا كبيرا بالنسبة للدول.
- أفرز التطور الإلكتروني جملة من المخاطر على الأمن القومي في معظم الدول.
- تمظهرت التهديدات الإلكترونية للأمن القومي بشكل أساسي وواضح في الاختراق النسبي لسيادة الدول.

- العديد من التجارب أثبتت أن الاستخدامات الإلكترونية المتطورة وتطبيقاتها قد تستعمل كسلاح لضرب أمن الدول والشركات.
- هناك استجابة واسعة من طرف الدول لمواجهة التهديدات الإلكترونية الجديدة لحماية أمنها القومي سواء من خلال التشريع أو من خلال التعاون الدولي.

6. حدود الدراسة:

- **الإطار الزماني:**

بما أن دراستنا هته مرتبطة بمتغيرين هما التهديدات الإلكترونية والأمن القومي فإن الإطار الزماني للدراسة يعود إلى نشأة هذين المفهومين وبما أن مفهوم الأمن القومي قديم قدم نشوء الدول فإن المتغير الثاني هو المرجعية الزمنية للدراسة وتعود الفترة الزمنية لظهور التهديدات الإلكترونية مع بداية الثورة الإلكترونية وتطور الشبكة العنكبوتية.

إذن يمكن تحديد الفترة الزمنية للدراسة منذ بداية الثورة الإلكترونية إلى غاية سنة 2019 سنة اتمام هته الدراسة.

- **الإطار المكاني:**

بما أنه كل دول العالم انخرطت في عالم الإلكترونيات، وأن ظاهرة العولمة فرضت على الدول توظيف التكنولوجيات الحديثة والإلكترونيات في شتى مجالات الحياة والمجتمع والإدارة والسياسة ؛ لذلك فإن المجال المكاني يشمل جميع دول العالم مع التركيز على الدول الأكثر تطورا في مجال الإلكترونيات ونذكر منها: الولايات المتحدة الأمريكية؛ روسيا؛ إسرائيل كما وسنخصص جانبا لدراسة الظاهرة في الجزائر.

7. الإطار النظري للدراسة:

النظرية الواقعية الجديدة ستكون هي الإطار النظري الأساسي لهذه الدراسة بحكم أنها أكثرها ملائمة وإسقاطا لموضوع دراستنا وأنها أكثر النظريات اهتمام بالأمن القومي وارتباطاته الخارجية وتنطلق النظرية من:

تفسير العلاقات الدولية من وجهة نظر بنيوية مناسبة للنظام الدولي خاصة توزيع القوى، فالواقعية الجديدة لها نظرة سوداوية للعلاقات الدولية انطلاقا من افتراض أن الحرب والنزاع ظاهرتان قابلتان للتجنب بسبب فوضوية النظام الدولي وعدم وجود سلطة دولية عليا فوق الدولة.

من ناحية أخرى افترض الواقعيون الدفاعيين طبعا في إطار الواقعية الجديدة، أن الدول ليس لديها مصلحة حقيقية تذكر في الغزو العسكري، على خلاف الواقعيين الهجوميين الذين يركزون على تشجيع نماذج معينة من سلوك الدول في النظام الدولي.

ومن ناحية مفهوم الصراع فالواقعية الجديدة افترضت أن الدولة يجب أن تتعامل مع أسوأ الاحتمالات، وأن تبني قراراتها بناءا على تقييم الاحتمالات بالنظر إلى التهديدات الأمنية. وفي سبيل تفسيرها لمفهوم صناعة القرار تطرح الواقعية الجديدة فكرة نظرية التوقع فهي ترى أن الفاعلين يعطون وزنا معتبرا أكثر للخسارة أكثر منه للربح .

وبالتالي فان الواقعيون الجدد يركزون على إقامة التحالفات المتوازنة والقوة الدفاعية الرادعة التي تتحقق الأمن للدول.[1]

8. الإطار المنهجي للدراسة:

- **المنهج المقارن:** هو أحد المناهج البحثية التي تبحث في أسباب حدوث بعض الظواهر عن طريق إجراء مقارنات بظواهر أخرى مشابهة وذلك بهدف التعرف على العوامل المسببة لحدوث هذه الظاهرة والتعمق في فهم أسبابها.
- أما استخداماته فهي:

❖ في مقارنة درجات التأثير المتباينة للتهديدات الإلكترونية على أمن الدول بين دولة وأخرى.

❖ الاختلافات بين الدول الأكثر استخداما للإلكترونيات وتكنولوجياتها والدول الأقل استخداما لها، وهذه المقارنة هي من خلال مستويات التهديد المختلفة وسياسات المواجهة وأنواع التشريع القانوني والجزائي.

[1]James E. Dougherty & Robert L Pfaltzgraff., **Contending Theories of International Relations: A Comprehensive Survey**, New York: Longman, Fifth Edition, 2001 , P 82.

❖ مقارنة درجات التهديدات الإلكترونية للأمن القومي والمفاهيم المختلفة من القرصنة إلى التجسس الالكتروني إلى الجريمة الالكترونيةإلى الإرهاب الإلكتروني إلى الحرب الإلكترونية.

- **المنهج الوصفي:** يقوم منهج على أساس وصف الظاهرة محل الدراسة، وتتبع جزئياتها وتفاصيلها والتعبير عنها كما وكيفا، ويهتم بوصفها وصفا دقيقا ويعبّر عنها كيفيا بوصفها وبيان خصائصها، وكميا بإعطائها وصفا رقميا من خلال أرقام وجداول توضح مقدار هذه الظاهرة أو حجمها أو درجة ارتباطها مع الظواهر الأخرى.[1]
- **المنهج التاريخي:**واسترجاع للماضي، وهو منهج علمي مرتبط بمختلف العلوم الأخرى، حيث يساعد الباحث الاجتماعي خصوصا عند دراسته للتغيرات التي تطرأ على البنى الاجتماعية وتطور النظم الاجتماعية في التعرف على ماضي الظاهرة وتحليلها وتفسيرها علميا، في ضوء الزمان والمكان الذي حدثت فيه، ومدى ارتباطها بظواهر أخرى ومدى تأثيرها في الظاهرة الحالية محل الدراسة ومن ثم الوصول إلى تعميمات.
- أما أهم استخداماته هي:

❖ في التطور التاريخي وتتبع أهم مراحل تطور الأمن القومي للدول وكذا التهديدات الإلكترونية المختلفة.

❖ في التطور التاريخي لسياسات الدول في مكافحة الجرائم الإلكترونية ومتابعتها.

9. أدبيات الدراسة :

1. كتاب **ذياب البداينة الأمن وحرب المعلومات، ط01، عمان: دار الشروق للنشر والتوزيع، 2006.**

يتناول هذا الكتاب الأمن والمجتمع المعلوماتي، وحرب المعلومات حيث تناول مواضيع الأمن وخصائص المجتمع المعلوماتي، وعمليات حرب المعلومات الهجومية، والدفاعية، وأمثلة

[1]عمار بوحوش، ومحمد محمود ذنيبات، **مناهج البحث العلمي**،الجزائر: ديوان المطبوعات الجامعية، 1997، ص،120.

وتطبيقات لحرب المعلومات، كما تطرق إلى مهددات الأمن ومعززاته في المجتمع، وبالتالي فهم أساليب حرب المعلومات الهجومية والدفاعية والثنائية (الهجوم والدفاع).

2. كتاب بعنوان **إيهاب خليفة بعنوان القوة الإلكترونية : كيف يمكن أن تدير الدول شؤونها في عصر الأنترنت؟ " الولايات المتحدة الأمريكية نموذجا، مصر: العربي للنشر والتوزيع، دون سنة النشر**. حيثيتناول الكتاب استخدام القوة الإلكترونية في إدارة التفاعلات الدولية مع الولايات المتحدة الأمريكية ، حيث ربط الكاتب مفهوم القوة الإلكترونية كنطاق تشغيلي محكم الاستخدام للإلكترونيات لاستكشاف المعلومات عبر أنظمة مترابطة ببعضها البعض وبنية تحليلية لها.

3. دراسة الباحث **وليد غسان سعيد جلعود، "دور الحرب الإلكترونية: في الصراع العربي الإسرائيلي، (رسالة ماجستير منشورة)، فلسطين، 2013**. حيث تهدف هذه الدراسة إلى ما يلي:

- معرفة ما هو مفهوم أمن المعلومات وعلاقته بالأمن القومي.
- التعرف على مفهوم الحرب الإلكترونية، وطبيعة عملها، وأنواعها، والقطاعات التي تستهدفها.
- .تناول الدور الذي لعبته الحرب الإلكترونية في الصراع العربي الإسلامي، والآثار التي خلفتها حرب الفضاء الإلكتروني على إسرائيل (اقتصادياً، نفسياً، سياسياً وأمنياً).

4. دراسة بعنوان:" **أثر التهديدات السيبرانية على الأمن القومي للدول: الولايات المتحدة الأمريكية –أنموذجا–"، من إعداد سليم دحماني، 2017-2018، جامعة المسيلة.**

حيث تتناول هذه المذكرة ابراز وتوضيح المفاهيم الجديدة في الفضاء الإلكتروني،وإبراز أشكال هذه التهديدات، كما توضح العلاقة بين الأمن القومي و الأمن الإلكتروني، مبرزة في الأخير إسهامات وجهود الدول وخاصة الولايات المتحدة الأمريكية في مواجهة هذه التهديدات الالكترونية.

5. مقال **عبد الله الحربي سليمان بعنوان:" مفهوم الأمن: مستوياته وصيغه وتهديداته (دراسة نظرية في المفاهيم والأطر)، المجلة العربية للعلوم السياسية، العدد 19، 2008.**

تناول المقال مفهوم الأمن القومي، أبعاده ومستوياته، كما تطرق أيضا إلى التحدياتوالتهديدات التي تواجهه باختلاف درجاتها وأبعادها وتوقيتها، مبرزا أيضا تصنيفات التهديدات الأمنية ومستخدما لذلك معايير عديدة ومتنوعة.

10. مصطلحات الدراسة:

- **الأمن القومي:** يعرف بأنه قدرة الدّولة على تَأمين استمرار أساس قوّتها الدّاخلية والخارجية، والعسكريّة والاقتصاديّة في مُختلف مناحي الحياة لمواجهة الأخطار التي تهدّدها من الدّاخل والخارج، وفي حالة الحرب والسِّلم على حدٍّ سواء.[1]
- **التهديدات الإلكترونية:**الهجوم القائم على مهاجمة الحاسوب، وأن التهديد به يهدف إلى الترويع أو إجبار الحكومات أو المجتمعات لتحقيق أهداف سياسية أو دينية أو عقائدية، وينبغي أن يكون الهجوم مدمراً وتخريبياً لتوليد الخوف بحيث يكون مشابه للأفعال المادية للإرهاب.
- **الأمن الإلكتروني:** تعزيز الحماية الناجمة عن تدابير الحد من مخاطر التكنولوجيا الرقمية بسبب استخدامها المتزايد للأغراض غير القانونية، كما يرتكز على العمليات القائمة على ضمان سرية وسلامة المعلومات والبيانات من كل الهجمات الالكترونية. [2]

[1] مراد علي عباس ، **الأمن والأمن القومي**، مقاربة نظرية، الجزائر: ابن النديم للنشر والتوزيع، 2017، ص 15.

[2]DOROTHY E. DENNING, **Cyber terrorism, Global Dialogue**, Autumn, 2000,p01.

11. صعوبات الدراسة:

- ضيق الوقت حيث أن الطالبة مقيدة بفترة زمنية محددة لإنجاز هذه الدراسة.
- طبيعة الموضوع نفسه من حيث الحيز الزمني والجغرافي الكبير الذي يحاول تغطيته خاصة أنه موضوع حديث الدراسة ومتشعب جدا.

12. تقسيم الدراسة:

قصد الإلمام بمتطلبات الدراسة، تم إدراج مضامينها وعرض محتوياتها في فصلين على النحو التالي:

الفصل الأول يخص بعرض الجوانب المفاهيمية والنظرية للمتغيرين: **التهديدات الإلكترونية** و**الأمن القومي**، والذي يحتوي عل مبحثين: ويتضمن **الأول** مفهوم الأمن القومي: نشأته، تعريفه، خصائصه، محدداته، مستوياته أبعاده، ثم تم تناول **أهم الاتجاهات في الدراسات الأمنية**، ثم تطرقنا إلى **مهددات الأمن** القومي، أما **الثاني** فيتضمن **مفهوم التهديدات الالكترونية**،ا ثم تم تناول **أنواعها** و**مستوياتها**، ثم تطرقنا إلى **الجهود الوطنية والدولية المبذولة لمحاربتها والقضاء عليها**.

الفصل الثاني فتم التطرق فيه إلى **الثورة الإلكترونية والأمن القومي**، والذي قسم إلى مبحثين **الأول** تناول **المخاطر الإلكترونية على المجتمع والسيادة**، يلي ذلك **مفموم مواقع التواصل الاجتماعي**، خصائصها، نماذج عنها، وأثرها على الأمن المجتمعي، كما وقد تناول **التهديدات الإلكترونية وقضايا السيادة**، ثم تطرق إلى **أثر الأمن الإلكتروني على الأمن القومي**، أما **الثاني** فقد **أبرز نماذج عن أنواع مختلفة من التهديدات الإلكترونية** مثل الجريمة الإلكترونية في الجزائر، الإرهاب الإلكتروني في الولايات المتحدة الأمريكية، القرصنة الإلكترونية في روسيا، والشباب العربي الإسلامي والحرب الإلكترونية على إسرائيل.

وسنختم هذه الدراسة بخاتمة عامة، نستعرض فيها أبرز النتائج المتوصل إليها، بالإضافة إلى جملة من التوصيات.

الفصل الأول
الإطار المفاهيمي والنظري للدراسة

تمهيد:

يحتل موضوع الأمن القومي أهمية كبيرة في سياسات الدول،التي تسعى من خلاله إلى الحفاظ على مقومات المجتمع من التهديدات والمخاطر التي تواجهه خصوصا الحديثة منها والمتمثلة في التهديدات الإلكترونية على اختلاف اشكالها.

وعليه فقد تناول هذا الفصل تأصيل مفاهيمي نظري لمفهوم الأمن القومي، وكذلك تعريف التهديدات الإلكترونية، وأنواعها، والجهود الوطنية و الدولية لواجهتها.

وفي هذا الإطار يقسم الفصل إلى مبحثين كالتالي:

المبحث الأول: تطور مفهوم الأمن القومي.

المبحث الثاني: مفهوم التهديدات الإلكترونية.

المبحث الأول: تطور مفهوم الأمن القومي:

سنقوم في هذا المبحث باستعراض أهم التعريفات التي ذكرها الباحثون فيما يتعلق بمفهوم الأمن القومي، وبوادر ظهوره.

المطلب الأول: مفهوم الأمن القومي:

سنقوم في هذا المطلب بدراسة بوادر ظهور الأمن القومي وأهم سماته وكذلك ارتباطه بالمصلحة القومية.

أولا: بوادر ظهور مفهوم الأمن القومي:

كان قيام الدراسات المهتمة بالأمن القومي متوافقاً مع ظروف عالمية سياسية وعسكرية جديدة أعقبت الحرب العالمية الثانية والتوازنات والتكتلات والمحاور التي نتجت عن الحرب بين القوى الدولية، بالإضافة إلى الانتشار الكثيف للأسلحة والتطور النوعي الذي شهدته هذه الأخيرة، والذي أدى إلى تعديلات في النظام الدفاعي العالمي وثوابته التقليدية ، وفرض رؤية جديدة للأمن، وتحديداً جديداً للمجال الأمني للدول.[1]

وقد تضمن المفهوم في نشأته الغربية الأمريكية أهدافا سياسية، حيث برز كمحور للسياسات الخارجية للدول الكبرى في فترة الحرب الباردة والاستقطاب الدولي.

وعلى الرغم من أن مصطلح الأمن القومي قد شاع بعد الحرب العالمية الثانية، إلا أن جذوره تعود إلى القرن السابع عشر، وخاصة بعد معاهدة واستفاليا عام 1648 التي أسست لولادة الدولة القومية أو الدولة **الأمة Nation – State** وشكلت حقبة الحرب الباردة الإطار والمناخ اللذين تحركت فيهما محاولات صياغة مقاربات نظرية وأطر مؤسساتية وصولاً إلى استخدام تعبير "إستراتيجية الأمن القومي".[2]

---

[1] عبدالله بلقزيز ، **الأمن القومي العربي**، القاهرة: الهيئة المصرية العامة للكتاب،1989، ص 15.

[2] محمد علاء عبد الحفيظ ، " تعريف مفهوم الأمن القومي وتحديد أبعاده"، **المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات**، تم التصفح يوم 26-12-2018، على الساعة 17:35، على الرابط الإلكتروني:
https://www.europarabct.com/%D9%85%D9%81%D9%87%D9%88%D9%85-%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D9%82%D9%88%D9%85%D9%8A-%D9%88%D8%AA%D8%AD%D8%AF%D9%8A%D8%AF-%D8%A3%D8%A8%D8%B9%D8%A7%D8%AF%D9%87/

وسادت مصطلحات الحرب الباردة مثل الاحتواء والردع والتوازن والتعايش السلمي كعناوين بارزة في هذه المقاربات، بهدف تحقيق الأمن والسلم وتجنب الحروب المدمرة التي شهدها النصف الأول من القرن العشرين.

نشأت تبعاً لذلك مؤسسات أكاديمية مهتمة بمسائل الأمن القومي: مصادره، مقوماته، إجراءات ضمان حمايته، من معاهد ومراكز بحث تنتمي إلى جامعات ومؤسسات علمية وإعلامية ومجلات متخصصة وإدارات مؤسسات مرتبطة بالقرار السياسي الرسمي.

ويشكل مجلس الأمن القومي في الولايات المتحدة الأمريكية النموذج الأول والأمثل لهذه المؤسسات، حيث جسّد هذا المجلس التعريف الذي طرحه **والتر ليبمان walter lippmann** عن الأمن القومي بأنه: (قدرة الدولة على تحقيق أمنها بحيث لا تضطر إلى التضحية بمصالحها المشروعة لتفادي الحرب، والقدرة على حماية تلك المصالح إذا ما اضطرت عن طريق الحرب).

وقد بدأ التشكيل التنظيمي المؤسسي لمصطلح الأمن القومي بصدور قانون الأمن القومي لعام 1947 عن الكونجرس الأمريكي، أما بقية دول العالم فقد وضعت عنواناً آخر هو "الدراسات الإستراتيجية" على الأدبيات التي عالجته بوصفها اجتهادات في التخطيط السياسي النشط حول المستقبل، بدلاً من اجتهادات تعني ضمنياً محاولة لصياغة أجوبة أو ردود فعل بقصد حماية السيادة. وكأي مصطلح أو مفهوم، فإن مفهوم الأمن القومي لا يمكن التوصل إلى تحديد دقيق له خارج نطاق المكان والزمان الذي يتحرك من خلاله، وهو يخضع دائماً للتعديل والتطوير انسجاماً مع المتغيرات والعوامل التي تؤثر في بروزه إلى مسرح التداول.

وهكذا أصبح الأمن القومي فرعاً جديداً في العلوم السياسية، حيث امتلك ثقافة وتوفرت له المادة والهدف العلمي (تحقيق الأمن) وإمكانية الخضوع لمناهج بحث علمية، بالإضافة إلى كونه حلقة وصل بين علوم عديدة، فالأمن القومي ظاهرة مركبة متعددة الأبعاد تربط في دراستها بين علوم الاجتماع والاقتصاد والعلاقات الدولية ونظم الحكم وغيرها، كما تتطلب الاستفادة من المناهج المختلفة وقدراً أكبر من التكامل المنهجي.[1]

[1] محمد علاء عبد الحفيظ ، **مرجع سابق الذكر**.

لقد مر مفهوم الأمن القومي بمرحلتين مهمتين نتيجة التطورات العالمية:

❖ **المرحلة الأولي:**

كان ينظر إليه بالنظرة العسكرية الضيقة وهي صد هجوم عسكري معادٍ وحماية الحدود من الغزوات الخارجية والمحافظة على الاستقلال الوطني.

❖ **المرحلة الثانية :**

صار على الدولة أن تؤمن مواطنيها سياسيا واقتصاديا واجتماعيا وثقافيا ضد أخطار متعددة فرضتها طبيعة الانفتاح الواسع على العصر الحديث.

وفي ظل انتهاء عصر العزلة، وذيوع فكر العولمة تراجعت سيادة الدولة وتناقصت استقلالية القرار الوطني لصالح قوي إقليمية أو دولية، فهناك قرارات أصبحت تصدر بالمشاركة بين السلطة الوطنية وغيرها من السلطات الخارجية مثل المنظمات الدولية، ولم تعد القرارات الاقتصادية حكرًا للمسئولين في الدولة وإنما أصبحت مشاعا، بالإضافة إلى تأثرها بالمؤسسات الخارجية كالبنك الدولي ومنظمة التجارة العالمية وغيرهما، مما يعد انتقاصا من السيادة ومن الأمن القومي.

وهكذا أصبحت مساحة التدخل الأجنبي في كثير من شؤون الدولة في ظل العولمة، أكبر من أي عصر مضى، واتخذت صورا متغيرة، كما سمحت بأدوار متعددة لبعض التيارات الاجتماعية والأفكار الجديدة ومنظمات المجتمع المدني المختلفة، كما أن ظاهرة العنف والإرهاب التي برزت خلال العقدين الأخيرين أدت إلى تغيير مفاهيم الأمن القومي للدول.[1]

ثانيا: تعريف الأمن القومي:

تجدر الإشارة بداية إلى أن مسألة ضبط تعريف للأمن لا يعد أمرا هينا، وذلك لأنه شأن كثير من المفاهيم غير المتفق عليها بصورة عامة، كما أنه يفتقر لضبط معرفي، شأنه شأن كثير من المصطلحات المتداولة التي يصعب تحديد تعريف لها بشكل قاطع .

وفي هذا السياق يقول المفكر **فافردي فوجلاس Vavardy Fouglas**: "أن الأمن هو شيء مختلف عن اليقين والضمان والثقة، لكن يبدو لي أنه يقترب أكثر من الثقة."[2]

---

[1] عبد الحفيظ زكي، **(الأمن القومي قراءة في المفهوم والأبعاد، مجلة المعهد المصري للدراسات السياسية والإستراتيجية) ،** 9فيفري2016، ص 02.

[2] حنان بن عبد الرزاق، **تأثير المأزق الأمني الإثني على الاستقرار الداخلي للدولة –دراسة للنموذج الإسباني منذ 1936،** (أطروحة دكتوراه منشورة)، بسكرة، 2016–2017، ص 13–14.

وقد أرجع جل الدارسين غموض موضوع الأمن إلى سببين:

❖ **الأول:** الإجماع بين الباحثين في مجال الدراسات الأمنية ونظرية العلاقات الدولية على أن مفهومّ الأمن معقد وواسع من حيث محتواه المعرفي، أبعاده وكذا أشكال تحقيقه.

❖ **الثاني:** الجدل الذي أثاره مصطلح الأمن في محاولة لتوسيع مجال الدراسات الأمنية خاصة بعدّ اعتماد وحدات مرجعية – غير الدولة – لموضوع الأمن ما أثر على مسألة التنظير في العلاقات الدولية[1].

1. التعريف اللغوي للأمن:

أما في اللغة العربية فقد تعددت تعاريف الأمن ، فمنه قول ابن فارس: **الهمزة والميم والنون،** أصلان متقابلان: أحدهما الأمانة التي هي ضد الخيانة ومعناها سكون القلب،والآخر التصديق.[2]

بالنسبة **للمعجم العربي (مختار الصحاح)** فإن كلمة أمن من باب: فهم وسلم، أصلها " الأمن" بهمزتين الثانية لينت للتخفيف والأمن ضد الخوف ، و الأمنة الذي يثق بكل أحد ، والإيمان أي التصديق ومنه؛**قوله تعالى:**"**إِذْ يُغَشِّيكُمُ النُّعَاسَ أَمَنَةً مِّنْهُ وَيُنَزِّلُ عَلَيْكُم مِّنَ السَّمَاءِ مَاءً لِّيُطَهِّرَكُم بِهِ وَيُذْهِبَ عَنكُمْ رِجْزَ الشَّيْطَانِ وَلِيَرْبِطَ عَلَىٰ قُلُوبِكُمْ وَيُثَبِّتَ بِهِ الْأَقْدَامَ**" **سورة الأنفال الآية 11،** وفي قوله؛ **عز وجل :**"**وهذا البلد الأمين**" **سورة التين الآية 03.**

في القرآن الكريم وردت كلمة "الأمن "وحدها خمس مرات بهذه الصيغة وسبع مرات بهذه الصيغة "آمنين"، وبدا الأمن كنقيض للخوف في ثلاث مواضع وهي؛**قال الله تعالى:**" **وَإِذَا جَاءَهُمْ أَمْرٌ مِّنَ الْأَمْنِ أَوِ الْخَوْفِ أَذَاعُوا بِهِ ۖ وَلَوْ رَدُّوهُ إِلَى الرَّسُولِ وَإِلَىٰ أُولِي الْأَمْرِ مِنْهُمْ لَعَلِمَهُ الَّذِينَ يَسْتَنبِطُونَهُ مِنْهُمْ ۗ وَلَوْلَا فَضْلُ اللَّهِ عَلَيْكُمْ وَرَحْمَتُهُ لَاتَّبَعْتُمُ الشَّيْطَانَ إِلَّا قَلِيلً**". **سورة النساء الآية 83.**

وفي قوله تعالى:" **وَعَدَ اللَّهُ الَّذِينَ آمَنُوا مِنكُمْ وَعَمِلُوا الصَّالِحَاتِ لَيَسْتَخْلِفَنَّهُمْ فِي الْأَرْضِ كَمَا اسْتَخْلَفَ الَّذِينَ مِن قَبْلِهِمْ وَلَيُمَكِّنَنَّ لَهُمْ دِينَهُمُ الَّذِي ارْتَضَىٰ لَهُمْ وَلَيُبَدِّلَنَّهُم مِّن بَعْدِ خَوْفِهِمْ أَمْنًا ۚ يَعْبُدُونَنِي لَا يُشْرِكُونَ بِي شَيْئًا ۚ وَمَن كَفَرَ بَعْدَ ذَٰلِكَ فَأُولَٰئِكَ هُمُ الْفَاسِقُونَ**". **سورة النور الآية 55.**

---

[1] محمد بن أبي بكر عبد القادر الرازي، **قاموس مفتاح الصحاح**، القاهرة: مطبعة البابي الحلبي، 1990، ص 38.

[2] أشرف علام، **مشروع قناة البحرين والأمن العربي**، القاهرة: مجموعة النيل العربية، 2002، ص 68.

وهذا تأكيد لحقيقة أن الأمن يعني: السكون والطمأنينة في ظاهره و باطنه والتخلص من مظاهر الخوف والقلق بكافة أشكاله.[1]

2. **التعريف اللغوي للقومية:(Nationalisme)** هي شعور أبناء الأمة الواحدة بأن ثمة رابطة تجمعهم وتميزهم عن الأمم الأخرى، وقد تكون هذه الرابطة عرقية أو لغوية أو ثقافية أو حضارية أو تاريخية أو اقتصادية أو سياسية، يمكن تبسيط المفهوم كـ : "جماعة من الناس تربطهم وحدة اللغة والثقافة والمصالح المشتركة"، أما الدولة القومية فهي منطقة جغرافية تتميز بأنها تستمد شرعيتها السياسية من تمثيلها لأمة مستقلة ذات سيادة، أي أنها توافق الكيان الجيوسياسي مع الكيان الثقافي والإثني.[2]

3. تعريف الأمن القومي:

يُعرّف الأمن القومي بأنه قدرة الدولة على تَأمين استمرار أساس قوتها الداخلية والخارجية، والعسكرية والاقتصادية في مُختلف مناحي الحياة لمواجهة الأخطار التي تهددها من الداخل والخارج، وفي حالة الحرب والسِّلم على حدٍّ سواء.

ويعرفه **هنري كيسنجر Henry kissinger** بأنه يعني: "أية تصرفات يسعى المجتمع – عن طريقها – إلى حفظ حقه في البقاء".

أما **روبرت ماكنمارا Robert Mcnamara** فيرى أن: "الأمن هو التنمية، وبدون تنمية لا يمكن أن يوجد أمن، والدول التي لا تنمو في الواقع، لا يمكن ببساطة أن تظل آمنة".

كما عرف **الأمن القومي** بأنه: " ذلك الجزء من سياسة الحكومة الذي يستهدف خلق الظروف المواتية لحماية القيم الحيوية."[3]

كما عبر عدد من المهتمين في علم الاجتماع عن رؤيتهم لمفهوم الأمن القومي عندما قالوا: "بأنه قدرة الدولة على حماية كيانها الداخلي من التهديدات الخارجية بغض النظر عن تلك

---

[1] محمد بن أبي بكر الرازي، **مرجع سابق الذكر**، ص 38.

[2] " تعريف القومية"، تم التصفح الموقع يوم 15-12-2018، على الساعة: 11:05، على الرابط الإلكتروني: https://weziwezi.com/%D8%AA%D8%B9%D8%B1%D9%8A%D9%81-%D8%A7%D9%84%D9%82%D9%88%D9%85%D9%8A%D8%A9/

[3] طارق عب العال عالي، " مفهوم الأمن القومي... بين الحقيقة والخيال"، تم التصفح يوم 12-12-2018، على الساعة: 15:20، على الرابط الإلكتروني: https://www.almasryalyoum.com/news/details/1217546

التهديدات–، فيما وضع عدد من المختصين بالشؤون السياسية والمنية تعريفاتهم لهذا المفهوم والتي من أبرزها:

هو مفهوم جوهري عسكري ينبع من خصائص الأوضاع الدفاعية للإقليم القومي، يتحول في صياغة تنظيرية بحيث يصير قواعد للسلوك الجماعي والقيادي بدلالة سياسية وبجزاء لا يختصر على العامل الداخلي.[1]

القدرة على توفير الحماية والاستقرار للعمل الوطني والقومي في جميع المجالات في الدولة ضد كل أنواع التهديدات الداخلية والخارجية سواء إقليمية أو عالمية.[2]

هو جملة المبادئ والقيم النظرية والأهداف الوظيفية والسياسات العملية المتعلقة بتأمين وجود الدولة، وسلامة أركانها ومقومات استمرارها واستقرارها، وتلبية احتياجاتها وحماية من الأخطار القائمة مع مراعاة المتغيرات الداخلية والإقليمية والدولية.[3]

تشير هذه التصورات إلى أن الأمن القومي هو مفهوم نظري يؤسس لوظائف وسياسات معينة، ويحدد طبيعتها وتوجيهاتها، كما أن المبادئ النظرية لمفهوم الأمن القومي، وما نجم عنها من وظائف وسياسات عملية، إنما هي أسس تصاغ نظريا وتنفذ إجرائيا بالاستناد إلى قيم الدولة وظروفها واحتياجاتها ومصالحها وأهدافها، ومن ثم كانت مبادئ الأمن القومي وثوابته هي جوهر السياسة العليا للدولة ومحورها، هذه المبادئ تعني تأمين كيان الدولة من أجل تحقيق الاستقرار، أي أن الدولة تواجه مشكلات شتى لبعض مصادرها داخل الدولة وبعضها مصدره الوحدات الدولية الخارجية.[4]

---

[1] ربيع حامد، **نظرية الأمن القومي العربي**، القاهرة: دار الموقف العربي، 1984، ص 43.

[2] خالد بن سلطان بن عبد العزيز ، **مقابل من الصحراء حقائق وذكريات ورؤيا مستقبلية لقائد القوات المشتركة ومسرح العمليات**، بيروت: دار الساقي للنشر والتوزيع، 1996، ص 66.

[3] مراد علي عباس، **مشكلات الأمن القومي: نموذج تحليل مقترح**، أبوظبي: مركز الإمارات للدراسات الإستراتيجية 2005، ص12.

[4] علي بن جمعة بن جمعة، **الأمن العربي في عالم متغير**، القاهرة: مكتبة مدبولي، 2010، ص27.

ثالثا: الارتباط بين الأمن القومي والمصلحة الوطنية:

تُستخدم المصلحة القومية كأداة تحليلية لوصف وشرح وتقويم مصادر السياسة الخارجية للدولة ومدى كفاءتها ويتم توظيفها كأداة للعمل السياسي في تبرير أو استنكار أو اقتراح سياسة ما، وغالباً ما يتم الربط بين المصلحة القومية والقوة، والنظر إلى المصلحة القومية على أنها هي التي تقرر السياسة الخارجية، وذلك أن تلك السياسة يتم رسمهابهدف تعزيز المصالح القومية وليس فقط مصالح كل فرد على حدة.

إن المصلحة القومية هي الأوضاع التي ترى الدولة في وجودها واستمرارها ما يحقق أهدافها، وهي تتضمن الحفاظ على قيم الدولة وصيانة استقلالها وكيانها وحرياتها في علاقاتها الخارجية ودعم هيمنتها الاقتصادية وغالباً ما تستخدم الدولة هذا المفهوم في محاولتها للتأثير على البيئة الدولية لصالحها.[1]

وإذا انتقلنا إلى التعرف على العلاقة بين الأمن القومي والمصلحة القومية، نجد أن هناك اتجاهاً يستخدم كلا المفهومين كمرادف للآخر؛ وهناك اتجاه آخر يرى وجود علاقة تأثير متبادل بين المفهومين، فنظرية الأمن القومي لدولة ما تعكس مصلحتها القومية، وكذلك فإن تحديد المصلحة القومية للدولة ينطلق من مفهوم واضح لأمنها وما يمكن أن يشكل خطراً أو تهديداً للأمن القومي.

وهنالك عدة عوامل تؤثر على الأمن القومي والمصلحة القومية مع بعضهما داخلية بالقوى السياسية المحلية والبناء الهرمي للقيم السياسية والشخصية والقومية التي تدور حول تغيرات النظام الدولي والتوازن الإقليمي.[2]

---

[1] Keith Krause and Michael William, (ed.), **Critical Security Studies : Concepts and Cases**, Mineapolis: University of Minnesota Press, 1987,p34.

[2] آدم محمد أحمد عبد الله، **العلاقات السودانية المصرية من منظور الأمن القومي والمصالح الإستراتيجية**، الخرطوم: شركة مطابع السودان، 2005، ص30.

رابعا: خصائص الأمن القومي:

إن ملاحظة الأمن القومي وقيمه النظرية العامة والثابتة يمكن أن تساعد على تحديد خصائص هذا المفهوم وتطبيقاته التي يمكن تلخيصها فيما يلي:

1. التركيب:

حيث أن الأمن القومي مركب من اجتماع وتفاعل القيم النظرية والسياسات العملية، وناتج عن محصلة انجازاتها وهو ذو بعدين داخلي يتعلق بالدولة وخصائصها واحتياجاتها للوحدات الجديدة في النظام الدولي ومطالبها الأمنية الخاصة التي قد لا تماثل المطالب الأمنية للدولة لكنها لا تقل عنها أهمية وتأثيرا.

2. الشمول:

حيث أن الأمن القومي مفهوم شامل تجمع في إطاره ركنية النظري والعلمي وأوجه الحياة الانسانية كلها ونشاطاتها كلها ما يجعل من هذا المفهوم مصدرا لإنتاج المفاهيم التطبيقية والنوعية المتخصصة للأمن القومي في الحقول النشاطية المختلفة للحياة الإنسانية مثل الأمن العسكري، والاقتصادي؛ والسياسي...والتي تبقى في النهاية مفاهيم فرعية تطبيقية تابعة للمفهوم الكلي للأمن القومي التي نتجت عنه وتطورت في إطاره مثلما يشمل عناصر الكيان الاجتماعي والسياسي للدولة التي تمس في الدائرة المجتمعية كل الأفراد والجماعات والمؤسسات آنية ومستقبلية.[1]

3. الثبات:

حيث أن الأمن القومي مفهوم ثابت ودائم سواء على المستوى القيم النظرية العامة والأساسية أو على المستوى الضروري والأهمية، إذ تبقى القيم والسياسات والرهانات مشروطة بتحقيقه واستمراره فليس من الممكن تحقيقه إذا اختلت أحد القيم لأنه يبقى في النهاية شرط كل الشروط ورهان كل رهانات.

[1] حامد ربيع، (**نظرية الأمن القومي : حول عمليات التأصيل الفكري لمنهجية تقنين مبادئ الأمن القومي والواقع العربي، دوريات آفاق عربية**،) عدد03، بغداد، 1984، ص 17-28.

4. التنوع:

حيث أن الثبات والديمومة مفهوم الأمن القومي على مستوى القيم النظرية العامة لا يمنع تعدده وتنوعه على مستوى الصياغة المفاهيمية أو السياسات التطبيقية الخاصة؛ ليس بالنسبة للدول كلها فحسب بل وحتى بالنسبة للدولة ذاتها إذا اختلفت الظروف والأوقات.[1]

خامسا : محددات الأمن القومي: [2]

1. مجموعة محددات البيئة الداخلية:

وهي المحددات المؤثرة في تكوين مفهوم الأمن القومي وتطبيقاته ويكون مصدرها البيئة الداخلية للدولة وخصائصها الذاتية وتشمل المحددات الداخلية:

أ. **النظام القيمي الاجتماعي:** حيث أن لكل مجتمع وهو المادة البشرية للدولة وركنها الحي أنظمته القيمة التي تؤمن بها وتثق بصوابها فيعتمدها ويعتمد عليها في تحديد معاييره الفكرية والسلوكية وينظم حياته على أساسها فرديا وجماعيا داخليا وخارجيا ومن ثم فإن نشاطهم بشكل أو بآخر.

ب. **التجارب والخبرات السابقة:** حيث أن لكل مجتمع تجاربه التاريخية المكتسبة وخبراته المتراكمة التي تنعكس على جوانب حياته وأنشطتها كلها وبتطور أشكال التنظيم السياسي للمجتمع الإنساني فقد أصبح التجارب والخبرات التاريخية انعكاساتها على مفاهيم الأنظمة السياسية ونشاطاتها.

ت. **القدرات المتاحة:** يشمل مفهوم القدرات المتاحة إطارا واسعا يحتشد فيه كم ونوع متعدد من الامكانيات والموارد المادية والمعنوية والبشرية والتقنية أو الجغرافية والاقتصادية والسياسة المجتمعية.

ث. **طبيعة النظام السياسي:** حيث أن الدولة وإن تعددت أركانها وتنوعت تتجسد عمليا في النظام السياسي الذي يحكمها ويعبر عليها ويحدد خصائصها، حيث يعد الأمن المصدر الأساسي لكل كائن وكيانه فإنه يكون في صورته السياسية.

ج. **طبيعة البيئة المجتمعية:** حيث يتحدد جانب من مفاهيم الأمن القومي وسياساته أيضا بتأثير القوى السياسية والاجتماعية الناشطة في إطار الدولة وقدرتها على دفع النظام

[1] عبد المنعم المشاط، **نظرية الأمن القومي العربي**، القاهرة: دار الموقف العربي، 1989، ص 64-72.

[2] مراد علي عباس، **الأمن والأمن القومي مقاربة نظرية**، الجزائر: ابن نديم للنشر والتوزيع، 2017، ص48-55.

السياسي إلى تبني وجهات نظر جديدة في هذا الشأن أو عجزها عن ذلك، فإذا وجدت بعض الاختلافات بين الطرف المجتمعي أو السياسي أو أخر في هذا الخصوص ستكون اختلافات تكتيكية حول التفاصيل الاجرائية ولا تمس الثوابت الأساسية العامة لأمن في أيه دولة.

2. مجموعة محددات البيئة الخارجية:

وهي المحددات المؤثرة في مفهوم الأمن وتطبيقه ويكون مصدرها البيئة الخارجية للدولة وخصائصها الاقليمية أو الدولية أو العالمية أو كلها معا، فبقدر ماتنتمي أيضا إلى بيئات خارجية إقليمية أو دولية وتتأثر أيضا بمكوناتها وخصائصها وتفاعلاتها.

وتتفاعل الدولة في إطار البيئات الخارجية مع وحدات تمتلك بعضها أركان الدولة وخصائصها، وفي كل الأحوال فقد فرضت شروط الاعتماد المتبادل في عالمنا المعاصر وتفرض حداثته مع الوحدات الأخرى ومفاهيمها وسياساتها الأمنية، وإن كانت البيئة الخارجية تفرض على وحدتها بعض القيود أحيانا فإنها توفر لها أحيانا الفرص وهو مايشمل بتأثيره أيضا مفاهيم للأمن وسياساتها لتحقيقه.[1]

سادسا: مستويات وأبعاد الأمن القومي:

1. مستويات الأمن القومي:

توسع نطاق الأمن الذي يركز على البقاء الوطني وحماية الدولة (الحدود ،الشعب)،إضافة إلى أمن القيم ضد العدوان الخارجي، حيث برزت سيطرة الدولة على قضايا الأمنأما في مرحلة ما بعد الحرب الباردة فإن الانقسامية العرقية أو الطائفية التي عرفتها كثير من المجتمعات قد أدت إلى ظهور مستوى أمني داخل المجتمع الواحد، أو ما يسمى بالأمن الوطني.

ومع انتهاء الاستقطاب الدولي الثنائي أصبح الأمن الإقليمي وكذا الدولي أكثر ظهورا وتأثيرا وبأبعاد جديدة ، و هو ما يشير إلى تعدد مستويات الأمن التي يمكن حصرها في:

- **أمن الفرد:**

يقصد بأمن الفرد توفر الحاجات الأساسية اللازمة لقيام هذا الأخير بوظائفه الحيوية والاجتماعية كعضو في المجتمع ، أما حاجاته الأساسية فمنها ما هو فيزيولوجي ومنها ما هو معنوي ، في المقابل يرتبط أمن الفرد بحمايته من أي أخطار تهدد حياته حيث يمارس المجتمع

[1] **المرجع نفسه** ، ص57 .

نوعا من الضبط الخارجي الرسمي وغير الرسمي كما يوزع آليات ضبط للفرد في حد ذاتهُ ، تشمل ذلك المجتمعّ لإشباع الحاجات بالطرق المقبولة اجتماعيا.[1]

وضمن هذا السياق تشير المادة (03) من الإعلان العالمي لحقوق الإنسان: "أن لكل فرد الحق في الحياة والحرية وسلامة شخصه، وكذا الحصول على الخدمات العامة في مقدمتها: التعليم والصحة".

- **الأمن القومي:**

بدأ الاستخدام الرسمي لمصطلح الأمن القومي مع نهاية الحرب العالمية الثانية بالضبط عام 1947، عندما أنشأت الولايات المتحدة الأمريكية هيئة رسمية سميت بـ: مجلس الأمن الوطني الأمريكي الذي أُسندت إليه كافة الأمور والأحداث ، أما من حيث التعريف فإن الأمن الوطنيّ وتيشير: "إلى قدرة الدولة في المحافظة على أراضيها ومواردها الطبيعية ونظمها المختلفةالاقتصادية، الاجتماعية و السياسية.[2]

في حين يرى **آرنست ماي Ernest May** أن: "استخدام مصطلح الأمن القومي جاء كرد فعل لحماية السيادة الوطنية، وهذا ضمن المذهب السياسي الذي تطور خاصة بعد الحرب العالمية الثانية، وعليه يعتبر الأمن الوطني المستوى الأساسي للأمن الذي تسعى الدول لتحقيقه داخليا أو وخارجيا."[3]

- **الأمن الإقليمي:**

يعتبر تحليل الأمن على هذا المستوى من أبرز الإسهامات التي قدمها **باري بوزان،** حيث يشير إلى أن: "الإقليم هو مستوىّ ترتبط فيه الدول أو وحدات أخرى بما فيه الكفاية مباشرة مع بعضها البعض ، بحيث أن أوضاعها الأمنية لا يمكن النظر إليها بمعزل عن بعضها البعض".

ومن هذا المنطلق ينحصر تحقيق أمن الأمن الإقليمي حول أمن مجموعة من الدول المرتبطة بعضها البعض.

---

[1] ذياب موسى البداينة، **الأمن الوطني في عصر العولمة**، الرياض: مؤسسات شباب الجامعة، 2009، ص 64.

[2] ذياب موسى البداينة، **المرجع نفسه**، ص24.

[3] K.Jholsti**, international politics ATromane work for analaysis**, U.S.E : hall international, 1995, p38.

و في هذا السياق، استخدم **بـوزان Buzan** مصطلحا يرى أنه الأكثر دقة وهو: " مجموعة من الدول ترتبط اهتماماتها الأمنية الأساسية مع بعضها الإقليمي "بشكل وثيق لدرجة أن أوضاعها الأمنية الوطنية لا يمكن بحثها واقعيا بمعزل عن بعضها البعض".[1]

- **الأمن العالمي:**

في سياق هذا المستوى تتولى الأمم المتحدة كهيئة دولية مسؤولية استتباب الأمن والحفاظ عليه على المستوى العالمي، ذلك أن هذا المفهوم يرتبطّ الأمن الجماعيمن قبل بعض المحللين،[2] بالتزام كل الأطراف بأخاذ تدابير جماعية لمواجهة أي عمل عدواني من جانب أي دولة ضدّ دولة اخرى أيضا أن ترتيبات – آليات يستند عليها–لا يرتبط بوجودّ ومن جوهر هذا المفهوم له خصم أو تحالف مسبق.[3]

بالإضافة إلى ذلك، يرى كل من **تشـارلز Charles وكليفـورد كوبشـان clifford Kupchan** في إطار تناولهما لمعنى الأمن الجماعي: " أن الدول توافق على التقيد ببعض المعايير والقواعد بغية المحافظة على الاستقرار وأنها عند الظروف تتكاتف لوقف العدوان.[4]

- **الأمن الإنساني:**

يرتبط هذا الأمن بجانبين رئيسيين هما:

- الأول : السلامة من التهديدات المزمنة : مثل الجوع ، المرض و الاضطهاد.
- الثاني: الحماية من الإختلالات المفاجئة والمؤلمة في أنماط الحياة اليومية للبشر، على جميع المستويات والأماكن.

وقد أشار وزير الخارجية الكندي **إكسووشـي ليـود Axwochy Lyod** إلى أن الأمن الإنساني هو: "أمن ضد الحرمان الاقتصادي نوعية مقبولة من الحياة وضمان لحقوق الإنسان الأساسية، أو هو حماية الأفراد من التهديدات المصاحبة وغير المصاحبة بالعنف؛ فهو يتعلق بوضع يتميز بانتفاء المساس بالحقوق الأساسية للأشخاص بأمنهم وحياتهم".[5]

---

[1] Balzacq thierry , **(Que'est ce que la sécurité national,revue international et strategique),**n52 ,4-2003.p37.

[2] W.Ziegtez David,**war peace and international politics**,Boston:SME, 1984,p98.

[3] Barry buzan, **people state and fear,** second edition, london : wheatshzaf books, 1983, p5

[4] جون بيليس، ستيف سميث، **عولمة السياسة العالمية**، ترجمة: مركز الخليج للأبحاث: 2004، ص 431.

[5] Charles philippe David**, la guerre et la paix, paris**, presse de science politique, 2000, p95.

2. أبعاد الأمن القومي:

- **البعد العسكري:**

تتحقق مطالب الدفاع والأمن والهيبة الإقليمية من خلال بناء قوة عسكرية قادرة على تلبية احتياجات التوازن الاستراتيجي العسكري والردع الدفاعي على المستوى الإقليمي لحماية الدولة من العدوان الخارجي، عبر الاحتفاظ بهذه القوة في حالة استعداد قتالي دائم وكفاءة قتالية عالية للدفاع عن حدود الدولة وعمقها.

والقوة العسكرية هي الأداة الرئيسية في تأييد السياسة الخارجية للدولة وصياغة دورها القيادي وبخاصة على المستوى الإقليمي، ويمتد البعد العسكري إلى إعداد الدولة والشعب للدفاع ودعم المجهود الحربي في زمن الصراع المسلح ولتحقيق مطالب الردع في فترات السلم.[1]

- **البعد السياسي:**

ويتمثل في الحفاظ على الكيان السياسي للدولة وهو ذو شقين داخلي وخارجي. يتعلق البعد الداخلي بتماسك الجبهة الداخلية وبالسلام الاجتماعي والوحدة الوطنية. أما البعد الخارجي فيتصل بتقدير أطماع الدول العظمى والكبرى والقوى الاقليمية في أراضي الدولة ومواردها، ومدى تطابق أو تعارض مصالحها مع الدولة سياسيا واقتصاديا واجتماعيا، وتحكمه مجموعة من المبادئ الاستراتيجية التي تحدد أولويات المصالح الأمنية وأسبقياتها.[2]

- **البعد الاقتصادي:**

ويرمي إلى توفير المناخ المناسب للوفاء باحتياجات الشعب وتوفير سبل التقدم والرفاهية له. فمجال الأمن القومي هو الإستراتيجية العليا الوطنية التي تهتم بتنمية واستخدام كافة موارد الدولة لتحقيق أهدافها السياسية، كذلك فالنمو الاقتصادي والتقدم التكنولوجي هما الوسيلتان الرئيسيتان والحاسمتان لتحقيق المصالح الأمنية للدولة وبناء قوة الردع الإستراتيجية وتنمية التبادل التجاري وتصدير العمالة والنقل الأفقي للتكنولوجيا وتوطينها وبخاصة التكنولوجيا العالية والحيوية.[3]

---

[1] عبد المعطي زكي، مفهوم الأمن قراءة في المفهوم والأبعاد، **مرجع سابق الذكر**، ص 05.

[2] **المرجع نفسه**، ص ص03.

[3] **المرجع نفسه**، ص 04.

- **البعد الاجتماعي:**

ويرمي إلى توفير الأمن للمواطنين بالقدر الذي يزيد من تنمية الشعور بالانتماء والولاء فبغير إقامة عدالة اجتماعية من خلال الحرص على تقريب الفوارق بين الطبقات وتطوير الخدمات يتعرض الأمن القومي للخطر.

ويرتبط هذا البعد كذلك بتعزيز الوحدة الوطنية كمطلب رئيسي لسلامة الكتلة الحيوية للدولة ودعم الإرادة القومية وإجماع شعبها على مصالح وأهداف الأمن القومي والتفافه حول قيادته السياسية، ويؤدي الظلم الاجتماعي لطبقات معينة أو تزايد نسبة المواطنين تحت خط الفقر إلى تهديد داخلي حقيقي للأمن القومي تصعب السيطرة عليه، وبخاصة في ظل تفاقم مشاكل البطالة والإسكان والصحة والتعليم والتأمينات الاجتماعية.[1]

- **البعد الثقافي:**

ويقوم على حماية الفكر والمعتقدات ويحافظ على العادات والتقاليد والقيم، وهو الذي يعزز ويؤمّن انطلاق مصادر القوة الوطنية في كافة الميادين في مواجهة التهديدات الخارجية والتحديات الداخلية، ويوسع قاعدة الشعور بالحرية والكرامة وبأمن الوطن والمواطن، وبالقدرة على تحقيق درجة رفاهية مناسبة للمواطنين وتحسين أوضاعهم المالية بصورة مستمرة.

إن الدور الثقافي بالغ الأهمية في تحصين الوطن من الأطروحات الثقافية للعولمة وصراع الحضارات، إذا أخذناه بالمفهوم الشامل متضمنا الفكر والثقافة والتعليم والإعلام والفنون والأدب. فالأمن القومي يعني "تمكين الشعب من ممارسة منظومة القيم الخاصة به على أرضه المستقلة"

وأمام التعدد في الأبعاد، يمكن القول أن الهدف الرئيسي للأمن القومي هو التركيز على قيمة الإنسان، فالقاعدة الشعبية العريضة هي ركيزة الأمن. ورغم أن القوة العسكرية مهمة ومطلوبة لكن هناك أيضا القوة الاقتصادية ونصيب الفرد من الدخل القومي، ودرجة نمو المجتمع، والمنظومة السياسية والاجتماعية السائدة التي تتيح لكل قوى الشعب التعبير عن نفسها، ومستوى التنمية، والمعادلة بين مستوى المعيشة ونفقات الدفاع، وتحديد المصالح الحيوية في الداخل والخارج، وأيضا تحديد الدوائر الحيوية وأولويتها.[2]

---

[1] فكتور ربلة، أحمد حمودة، **التربية السكانية في الوطن العربي: واقعها واتجاهات تطويرها**، عمان: ورقة عمل للنشر والتوزيع، 1990، ص 112.

[2] عبد المعطي زكي، **مرجع سابق الذكر**، ص 05.

المطلب الثاني : أهم الاتجاهات في الدراسات الأمنية:

يحتل موضوع الأمن أهمية كبرى في الدراسات الدولية باعتباره يشكل محور بحث أساسي في كتابات واهتمامات دارسي العلاقات الدولية، ويمكن حصر هذه الأهمية في مستويين الأول أكاديمي والثاني تطبيقي أما على المستوى الأكاديمي فتتجلى هذه الأهمية من خلال مركزية موضوع الأمن كبرنامج بحثي في الأطر والمقتربات النظرية الكلاسيكية والمعاصرة للعلاقات الدولية، إضافة إلى كونه نقطة ارتكاز منهجية للانطلاق في دراسة المنظورات الأمثل لتفسير التحولات الدولية المتعاقبة، فالأمن هو إحدى تركيبات وعمليات السياسة العالمية التي تشكل محوراً لمناظرة ضمنية بين شتى الاتجاهات النظرية الكبرى في العلاقات الدولية.

بينما على المستوى التطبيقي تتجلى هذه الأهمية من خلال مدى إدراك الدول لبيئتها الأمنية داخليا وخارجيا وانعكاس ذلك على صياغة منظوماتها الأمنية بشكل توافقي أو تعارضي استنادا إلى مقوماتها وإمكانياتها الداخلية وارتباطا بتموقعها في النظام الدول..[1]

ولذلك وتلازما مع اختلاف الجوانب التي تركز عليها كل نظرية ودراسة في تعريفها للأمن سنحاول رصد أهمها من خلال اتجاهين عامين تقليدي ومعاصر:

أولا: الاتجاه التقليدي للأمن القومي:

تمت الصياغة المفاهيمية للأمن استنادا إلى طبيعة البيئة الدولية ومتغيراتها لقد كانت مسألة الأمن دافعا طبيعيا يوجه سلوك الأفراد والمجتمعات منذ فجر البشرية بغية توفير السلم والاستقرار كبديل لحالة الخوف والضرر، وهذا ما مثل مبررا أساسيا لانضمام الأفراد إلى تكتلات اجتماعية أكبر نتيجة للحاجة الأمنية الملحة، وهذا ما يعكس بداية التأصيل السوسيولوجي لكرونولوجيا الانتقال من الأمن الخاص إلى الأمن الجماعي أي بروز بذور تشكل الجانب الهيكلي في تحديد مفهوم الأمن ومعناه.[2]

ولذلك كان لزاما أن يفهم الأمن من داخل الوحدة أو على أقصى تقدير من حدود تماسها المباشر مع الوحدات الأخرى، فاندرج الأمن كموضوع للسياسة العليا التي تصيغ التوجه الوطني

[1] خالد معمري، **التنظير في الدراسات الأمنية لفترة ما بعد الحرب الباردة: دراسة في الخطاب الأمني الأمريكي بعد 11 سبتمبر**،(رسالة ماجستير منشورة)، باتنة، 2007-2008، ص 18.

[2] جون بيليس وستيف سميث، **مرجع سابق الذكر**، ص 121.

والقومي للدولة، بتسخير الإمكانيات والموارد لرسم الإستراتيجيات المناسبة لتحقيق أمنها القومي.[1]

إذن فالأمن في صورته التقليدية كان مرادفا لوجود عدوٍ خارجي تستدعي ضرورة البقاء هزمه أو منعه من بسط نفوذه بواسطة الأداة العسكرية للدولة.

وعموما فتحديد مفهوم الأمن وفقا لهذا الاتجاه يعني حماية مصالح الدولة الوطنية من التهديدات الخارجية باستخدام القوة العسكرية لقطع دابر مصادر التهديد الخارجية، وضمان استمرار تحقيق تلك المصالح، وهذا لايتحقق إلا بزيادة الإمكانات العسكرية التي تجعل الدول تنظر بعين الرضا إلى ما تتوفر عليه من قوة واقتدار يجعلانها آمنة فيما يتعلق بعدم تهديد مصالحها.[2]

لذلك يفهم كيف يتم الربط ضمن هذا الاتجاه بين متغيري الأمن والقوة العسكرية باعتبار أن الوسيلة العسكرية هي الأداة الرئيسية لتحقيق الأمن الخاص بالدول وعدم الفصل بينهما هو إعمالٌ للسيادة القومية وحماية للدولة من التهديدات الخارجية، حيث أن استخدام القوة العسكرية دائما ما يكون مرتبطا بوجود تفكير عدواني على كيان الدولة، الأمر الذي يدفع بـ **فرانك تريجر Trager France** إلى القول إن جوهر العملية الأمنية هو حماية القيم القومية الحيوية **Values Care** وعلى العموم يعرف عبد الوهاب الكيالي الأمن بمنظوره التقليدي على أساس أنه تأمين سلامة الدولة من أخطار داخلية وخارجية قد تؤديها إلى الوقوع تحت سيطرة أجنبية نتيجة ضغوط خارجية أو انهيار داخلي.[3]

[1] عبد المجيد صادق، **أمن الدواة والنظام القانوني للفضاء الخارجي**، القاهرة: جامعة القاهرة، 1976، ص07.

[2] تامر كامل، **دراسة في الأمن الخارجي العراقي وإستراتيجية تحقيقه**، العراق: وزارة الثقافة والإعلام، 1979، ص 131.

[3] عبد الوهاب الكيالي، **مرجع سابق الذكر**، ص 131.

ثانيا:الاتجاه المعاصر للأمن القومي:

يرى **جون بيرتون Burton John** أن الأمن قد تغير تعريفه مع الثورة المعلوماتية ولم يعد يعرف بأعداد القوات التي يمكن نشرها في اللحظة المناسبة، بل بالقدرة على الحصول أو منع الحصول على مصادر المعلومات المهمة.[1]

لذلك ارتبط الاتجاه المعاصر في تحديد مفهوم الأمن أساسا بطبيعة التطورات والتغيرات التي مست شكل وجوهر النظام الدولي والإفرازات التي نتجت عنها، ومن الناحية النظرية يمكن استيعاب مضامين هذا الاتجاه من خلال الاقتراب إلى العناصر التالية ، التي تشكل دلالات جوهرية في الدراسات الأمنية[2] :

أ. صورة التحولات الدولية المباشرة (السياسية، الاقتصادية، الاجتماعية)

ب. التحديات والرهانات التي فرضتها هذه التحولات اقتصاديا، قيميا وأمنيا

ت. التطورات الرئيسية لمفهوم الأمن.

لقد أدت التحولات التي شهدها النظام الدولي لما بعد الحرب الباردة إلى تزايد حالة التشابك والترابط بين وحدات التفاعل الأساسية في العلاقات الدولية من خلال تبلور ظاهرة الاعتماد المتبادل . ومن أهم هذه التحولات، نجد :

1. اتساع هيكل النظام الدولي إلى جميع الدول والمناطق بدون استثناء إلى جانب المنظمات الدولية والإقليمية، ومرد ذلك حصول العديد من الشعوب التي خضعت للاستعمار على استقلالها السياسي .

2. تقلص الفوارق النسبية بين المناطق الهامشية والمناطق الاستراتيجية من حيث التأثير في مجمل إستراتيجيات الدول بفعل التقدم في وسائل الاتصال والمواصلات، إن تشابكية المشهد الدولي هذه قد أسهمت –بشكل كبير– في بلورة تحديات جديدة شكّلت مداخل إضافية مسرعة لضرورة إيجاد مفهوم أوسع للأمن يتناسب وحجم التحول المتسارع من جهة، ويتكيف مع الرهانات الجديدة التي فرضتها البيئة الدولية من جهة أخرى.[3]

---

[1] محمود حيدر، **(السيادة الدولية في تحولات العولمة: الدولة المغلولة، مجلة شؤون الأوسط)**، العدد100، 2004، ص48.

[2] إسماعيل صبري مقلد، **العلاقات السياسية الدولية: دراسة في الأصول والنظريات**، الكويت: منشورات ذات السلال، 1985، ص 46-48.

[3] وليد عبد الحي، **(تأثير التكنولوجيا على العلاقات الدولية، المجلة الجزائرية للعلاقات الدولية)**،العدد04، ص 25.

المطلب الثالث: مهددات الأمن القومي:

أولا : مفهوم التهديدات الأمنية:

1.تعريف التهديدات الأمنية:

اشتقت كلمة "تهديد" من الناحية اللغوية من لفظ "هدد"، ويقصد به محاولة إلحاق الضرر والأذى بشيء معين قصد الإخلال بالأمن.[1]

ويشار إليه في اللغة الانجليزية**"Threat"**وبالألمانية**"Drohung"**أو **"Budrohung"** وبالفرنسية**"Menace"**، ويُعبر التهديد عن وجود نية لإيذاء أو معاقبة أو إلحاق ضرر من خلال عمل عدائي على شخص معين.[2]

ولقد ورد في قاموس "أكسفورد Oxford "على أن التهديد هو: "محاولة شخص أو شيء الإضرار بحياة الآخرين".[3]

ويرى **تيري ديبيل Terry L. Debel** على أن التهديد: "عمل نشط وفعال تقوم به دولة معينة للتأثير في سلوك دولة أخرى، ويشترط نجاحه توفر عدة عوامل أبرزها المصداقية والجدية والقدرات التي تتناسب مع التهديد، وهناك ثلاث سمات يتميز بها التهديد، وهي: درجة الخطورة ومدى احتمالية وقوع التهديد وعنصر التوقيت.[4]

ويعتبر الباحث **يان إيشلر Jan Eichler** أن التهديد يعبر عن إرادة إلحاق الضرر بفاعل (الفرد/جماعة/دولة...)، ويشترط فيه توفر العناصر التالية:

- ❖ أن يسبب حالة من الهلع والخوف.
- ❖ توفر القدرة على الاستهداف سواء استهداف الدولة مباشرةً أو مواطنيها أو الدول المجاورة للدولة، وهنا يكون للتهديد تأثير جيوسياسي، فمثلاً: الفوضى الأمنية والتهديدات الأمنية الموجودة بدول الجوار الجزائرية خاصة ليبيا تجعل الجزائر في حالة من الخوف والترصد والتأهب لمواجهة تهديدات محتملة قد تأتي منها.

---

[1] لندة عكروم، **تأثير التهديدات الأمنية بين شمال و جنوب المتوسط،عمان:** دار ابن بطوطة للنشر والتوزيع، 2013، ص30.

[2] Hans Gunter Brauch, **Coping with Global Environmental Change, Disasters and Security** , USA: Springer Verlag Berlin Heidelberg, 2011, p 62.

[3] عادل جارش،(**مُقاربة معرفية حول التهديدات الأمنية الجديدة"، مجلة العلوم السياسية والقانون)** ،العدد الأول 2017، ص 252.

[4] تيري ديبيل، **إستراتيجية الشؤون الخارجية...منطق الحكم الأمريكي**، ترجمة: وليد شحادة ، بيروت: دار الكتاب العربية مؤسسة محمد بن آل راشد آل مكتوم، 2009، ص ص 258-261.

❖ درجة الخطورة، أي طبيعة الخطورة (محتملة، فعلية، كامنة)، فكلما كان التهديد خطير كلما تطلب ذلك رد فوري فعال من الطرف المهدد.[1]

2.التهديدات الأمنية ومفاهيم مشابهة:

1.2التحدي(Challenge)

اشتقت كلمة "تحدي" من الناحية اللغوية من اللفظ "تحدى"، حيث يُقال في اللغة العربية فلان تحدى فلان حول شيء معين أي طالب مباراته في هذا الشيء، ويقابل لفظ التحدي في اللغة الإنجليزية كلمة **(Challenge)** ، وفي الألمانية **(Herausforderung)** وبالفرنسية**(Défi)**.

وتشير القواميس الانجليزية البريطانية إلى عدة معاني للتحدي، فهو يعبر على شيء صعب يجب اختباره ويحتاج إلى القوة والمهارة، وهو أيضاً دعوة للمنافسة والمواجهة كأن يقترح شخص مبارزة آخر وما إلى ذلك.[2]

ومن الناحية العلمية؛ فإن المتفق عليه أن مُفردة "التحدي" يقصد بها مجموعة معقدة من المشاكل والظروف التي ننتجها في الواقع والمستقبل بإرادتنا ورغباتنا الواعية وغير الواعية،[3] فلقد عرفها "سليمان عبد الله الحربي" بأنها: "المشاكل والصعوبات أو المخاطر التي تواجه الدولة وتحد وتعوق من تقدمها وتشكل حجر عثرة أمام تحقيق أمنها واستقرارها ومصالحها الحيوية الذاتية المشتركة ويصعب تجنبها أو تجاهلها"، فعلى سبيل المثال تعتبر كل من معضلة البطالة ومشاكل الانفجار الديمغرافي تحدياً بالنسبة للدولة.[4]

والتحدي شيء صعب يتم فيه اختبار قدرة الدولة على إدارة شؤونها ومنافسة الآخرين سواء تعلقت هذه التحديات بالمشاكل الداخلية أو الخارجية.[5]

---

[1]Jan Eichler, **(Comment apprécier les menaces et les risques du monde contemporain?, Défense nationale et sécurité collectiveà),** vol.62, n°11, Novembre2006, p.161.

[2]Hans Gunter Brauch ,**Op,cit**, p 62

[3]أمين المشافية، وسعد شاكر شبلي،**التحديات الأمنية للسياسة الخارجية الأمريكية في الشرق الأوسط في مرحلة ما بعد الحرب الباردة**،عمان: دار ومكتبة حامد للنشر والتوزيع، 2012، ص16.

[4]سليمان عبد الله الحربي، **(مفهوم الأمن: مستوياته وصيغه وتهديداته "دراسة نظرية في المفاهيم و الأطر"،المجلة العربية للعلوم السياسية،)** العدد 19،صيف 2008، ص28.

[5]فوزي حسن الزبيدي، **(منهجية تقييم مخاطر الأمن القومي"، مجلة رؤى إستراتيجية)،** العدد11،جويلية 2015، ص22.

2-2 الخطر (Risk)

عرف قاموس" Le Petite Robert الخطر" على أنه كل فعل مهدد يُحتمل وقوعه وإمكانية التنبؤ به تتأرجح بين الزيادة والنقصان، وهو مرتبط بمدى قدرة المجتمع ومناعته حيال مواجهته.[1]

ويعتبره الكثير من المفكرين والمختصين على أنه خاصية تدل على شيء يلحق ضرر معنوي أو مادي، فعندما نقول عن شيء خطر بمعنى أنه يحمل ضرر معنوي أو مادي يُحتمل وقوعه، وقد يؤدي إلى الخسارة أو الدمار أو الإصابة، ويشمل الخطر ثلاث عناصر أساسية تتمثل في:

- المصدر المنتج للخطر.
- الوسيلة الناقلة للخطر بحيث قد تكون ميكانيكية أو كيميائية أو إشعاعية.
- البيئة الناقلة للخطر التي قد تكون مائية أو حضرية أو هوائية.[2]

3.الظاهرة الأمنية المتعدية لحدود الدولة القومية:

لم يعد إطار الظاهرة الأمنية المعاصرة بأبعادها المختلفة محددًا بنطاق الحدود الإقليمية للدولة، بل تعدى هذا الإطار الحدود ليشمل دول الجوار الجغرافي المباشر ، ويمتد إلى الإطار الاقليمي والدولي وأساليب التعامل الممكنة والمتاحة تتأثر هي الأخرى بالعديد من المتغيرات الآتية من الخارج والتي يصعب تجاهل تأثيرها، وفي هذا الإطار يمكننا القول بأن هناك تداخلا واضحا بين العوامل الداخلية والخارجية (إقليمية – دولية) المؤثرة على الأوضاع الأمنية في جميع دول العالم في الوقت المعاصر، لوضع السياسات الأمنية لأية دولة في العالم اليوم لابد وأن يأخذ في الاعتبار هذه الأمور ، سواء من حيث مصادر التهديد ونوعيته وكثافته وأساليب التعامل معه.

ويزيد من تعقد الظاهرة الأمنية المتعدية للحدود أن بعض مصادر التهديد قد تكون خارج نطاق سيطرة السلطات السياسية في الأطراف الدولية المعنية ، وبعضها يكون نتيجة الصراعات الداخلية الحادة في بعض الدول والتي قد تصل إلى الحروب الأهلية، وما يترتب عليها من آثار

---

[1]Le Petite Robert**, Dictionnaire Alphabétique et Analogique de la Langue Française** , Paris: Editionfirmindidol, , 1979, P 1720.

[2]قاسم حجاج، **(التدخل الإنساني للجيش الوطني الشعبي في مواجهة الكوارث الطبيعية، مجلة السياسة والقانون)**، العدد الرابع عشر، ورقلة، جانفي 2016، ص07.

كنزوح أعداد كبيرة من البشر واختراقهم حدود الدول المجاورة هربًا مما قد يتعرضون له من مخاطر نتيجة الأوضاع الداخلية في بلادهم ،آما ان بعض مصادر التهديد المتعدية للحدود قد تتمثل في منظمات الجريمة دولية النشاط المافيا وتجارة المخدرات والسلاح وعصابات القرصنة.[1]

4.ظهور نوعية جديدة من التهديدات الأمنية التي لم تكن معروفة من قبل:

وأبرزها التهديدات الأمنية لنظم المعلومات وإمكانية ممارسة أعمال القرصنة المعلوماتية بأبعادها المختلفة ،فمع ازدياد الاعتماد على نظم المعلومات والحاسب الآلي في تسيير الأعمال فإن إمكانية اختراق هذه المنظومة من شأنه أن يخلق تهديدات أمنية خطيرة والتأثير على حركة الطيران والمعاملات من خلال ميكانزمات التجارة الالكترونية وأعمال البنوك وغيرها من المؤسسات التي تستخدم الأساليب الآلية الحديثة في المعاملات ،هذا بالإضافة إلى إمكانية اختراق منظومات المعلومات الأمنية للأجهزة المختلفة فضلاً عن امكانية منظومات الاتصال والتحكم المستخدمة لإدارة العمليات.

وثمة نوعية جديدة من التهديدات ناتجة عن اتساع نطاق التدخل الخارجي في الشؤون الداخلية للدولة لاعتبارات عديدة تخضع في الغالب لمعايير مزدوجة وغير قابلة للقياس والتحديد الموضوعي[2].

ثانيا: تصنيفات التهديدات الأمنية:

هناك عدة معايير مستعملة لتصنيف التهديدات الأمنية من قبل الدارسين والباحثين، حيث تعددت المعايير المستعملة لتصنيف التهديدات الأمنية، إذ يركز بعض الباحثين على معيار المجال في تصنيفهم للتهديدات، ومنهم من يستخدم المعيار الجغرافي، ومنهم من يحبذ استخدام تصنيفات معاصرة تركز على معيار التماثل والتأثير.

[1] قاسم حجاج، **مرجع سابق الذكر**، ص ص 32.

[2] محمد سعد أبو عامود، (**المفهوم العام للأمن، مجلة مركز الإعلام الأمني**)، مصر،جامعة حلوان، ص 65.

1. من حيث المجال: يحبذ الكثير من الباحثين تصنيف التهديدات الأمنية حسب معيار المجال، بحيث يتضمن هذا التصنيف مايلي:

- **التهديدات السياسية:** تتضمن غياب نظام سياسي يتميز بالقبول العام الداخلي والخارجي متماسك ومتجاوب مع تطلعات الشعب، إضافة إلى غياب شبه تام لمؤشرات الديمقراطية والحكم الرشيد.
- **التهديدات الاقتصاديّة:** تتمثل فيعدم وجود توزيع عادل للثروة، وضعف في الناتج القومي والدخل الفردي وتأثر الدولة بإفرازات العولمة الاقتصادية والأزمات المالية والعقوبات الاقتصادية.
- **التهديدات الاجتماعية والثقافية:** تتجلَّى في اتساع دائرة الفقر والجوع والأمية والبطالة والأوبئة والهجرة والتزايد الديمغرافي الذي لا يتماشى ولا يتوافق مع نسبة النمو الاقتصادي، وزيادة التفكك الاجتماعي وتدني مستوى الخدمات الاجتماعية مما يؤدي إلى تدهور حالة البشر، إضافةً إلى الاختراق الثقافي لهوية المجتمعات والدول نتيجة لتطور مسارات العولمة التي ارتبطت ارتباطاً عضوياً بتطور وسائل الاتصال والتكنولوجيا.
- **التهديدات البيئية:** وتتضمن كل تهديد يمس الحيز (المحيط) الذي نعيش فيه سواء كان يابسة أو ماء أو هواء، وتشمل هذه التهديدات التلوث، الاحتباس الحراري وتآكل طبقة الأوزون، وظاهرة الانقراض الحيواني والنباتي، وتلوث التربة بسبب سوء استخدام الأسمدة والمبيدات، وتلوث الهواء والمياه العذبة والجوفية ومياه البحار والمحيطات والاستهلاك المفرط لمصادر الطاقة غير المتجدِّدة **(نفط، فحم حجري، غاز طبيعي وصخري).**[1]

2. حسب درجة الخطورة:

يرى المفكر العربي سليمان عبد الله الحربي في مقال له بالمجلة العربية للعلوم السياسية موسوم بما يلي مفهوم الأمن: مستوياته وصيغه وتهديداته (دراسة نظرية في المفاهيم والأطر)، أنه يمكن تصنيف التهديدات الأمنية من حيث درجة الخطورة إلى:

- **التهديدات فعلية:** وهي ما يعرض الدولة لخطر داهم نتيجة الاستخدام الفعلي والجاد للقوة العسكرية.

[1] إلياس أية جودة، **الأمن البشري وسيادة الدول**، بيروت: مجد المؤسسات الجامعية للدراسات والنشر والتوزيع، 2008، ص 29-34.

- **التهديدات المحتملة:** تُرصد هذه التهديدات من خلال مجموعة من الأسباب الحقيقية التي تؤكد تعرض الدولة لمجموعة من التهديدات دون وصولها إلى مرحلة استخدام القوة العسكرية.
- **التهديدات الكامنة:** تتميز بأنها غير مرئية(كامنة)، كوجود أسباب خلاف بين دولتين أو أكثر دون وجود أي مظاهر مرئية على السطح.
- **التهديدات المتصورة:** وهي التهديدات التي يُحتمل ظهورها مستقبلاً.[1]

3. حسب درجة التماثل:

يرى بعض الباحثين أنه يمكن تصنيف التهديدات الأمنية حسب درجة تشابه الفواعل **(Actors)**إلى:

أ. **التهديدات التماثلية:** يطلق على النمط التقليدي للتهديدات الذي تتميز بالطابع البيني والعسكري وتتشابه في الفواعل من حيث الخصائص كالتهديد العسكري الذي يكون بين دولة "أ" ودولة "ب"، مثل: التهديدات المتبادلة بين كوريا الشمالية وكوريا الجنوبية باستخدام القوة بينهما.

ب. **التهديدات اللاتماثلية:** هي تلك التهديدات التي تُبنى على فكرة الغموض وعدم إمكانية تحديد ماهية العدو، إذ تكون بين أطراف غير متكافئة من حيث القوة، ويشمل هذا النوع من التهديدات الجريمة الاقتصادية والمتاجرة بالأسلحة والإرهاب العابر للحدود، والجريمة المنظمة والنزاعات الداخلية، وما يصحبها من انتهاكات واسعة لحقوق الإنسان، والإبادة الجماعية التي تجد لها مكاناً مثالياً في الدول الفاشلة**(Failed States)** ، ولقد برزت نتيجة للتغير المهم في هيكلة المخاطر الأمنية من النمط التماثلي إلى "النمط اللاتماثلي" تزامناً مع التحولات والتغيرات الحاصلة في النظام العالمي.[2]

وتجدر الإشارة إلى أن هناك مجموعة من العناصر التي تساهم في تحديد التهديد الأمني، ويمكن من خلالها تحليل أي تهديد أمني لا بد من التطرق لها على النحو التالي:

- **طبيعة التهديد:** ما هو تصنيف هذا التهديد؟ و ما هي أبرز أبعاده؟

---

[1] سليمان عبد الله حربي، مفهوم الأمن ومستوياته وصيغه وتهديداته(دراسة نظرية في المفاهيم والأطر)، **مرجع سابق الذكر**، ص 29.

[2] شهرزاد أدمام، **(الطبيعة اللاتماثلية للتهديدات الأمنية الجديدة، مجلة الندوة للدراسات القانونية)**، العدد01، 2013، ص01.

- **مكان التهديد:** ما هو النطاق الجغرافي لهذا التهديد؟ وما هي امتداداته؟
- **زمان التهديد:** ما هي تأثيراته الأنية والمستقبلية؟
- **درجة التهديد:** ما قوة هذا التهديد؟ وما هي خطورته؟
- **تعبئة الموارد:** ما هي الإجراءات والتدابير المناسبة المادية والبشرية والمعنوية لمواجهة هذا التهديد ومحاولة الحد من تأثيره وأبعاده.[1]

الجدول رقم (01): جدول يُبين أبرز أوجه الاختلاق بين التهديدات التماثلية والتهديدات اللاتماثلية

نوع التهديد/مؤشر الاختلاف	التهديدات التماثلية	**التهديدات اللاتماثلية**
من حيث مضمون كل مفهوم	هي التهديدات التقليدية التي تحمل بُعد عسكري تحاول فيها دولة تهديد دولة أخرى بغرض تحقيق أهدافها.	تهديدات تكون بين فواعل غير متناظرة كحرب دولة ضد جماعة إرهابيه وتُعبر عن النمط الجديد من التهديدات السائدة بكثرة منذ أحداث الحادي عشر من سبتمبر 2001.
من حيث المصدر	الدولة	فاعل من غير الدولة: جماعات الإرهابية، وجماعات تمرد، عصابات جريمة منظمة...، وغيرها.
من حيث الخصائص	يكون العدو واضح ويمكن تحديده بسهولة واستهدافه، وعادة ما تكون بين أطرف متشابهة كتهديد دولة لدولة ويتشابهان في العديد من النقاط.	تُبنى على فكرة الغموض وعدم إمكانية تحديد ماهية العدو، وتكون بين أطراف غير متكافئة تختلف من حيث القوى التنظيم وامتلاك الوسائل والأساليب

[1] سليمان عبد الله حربي، **مرجع سابق الذكر**، ص 29-30.

المبحث الثاني: مفهوم التهديدات الإلكترونية:

مع التطور الهائل الذي شهدته تكنولوجيا الاتصالات و المعلومات، و التي أحدثت ثورة معلوماتية مست جميع المجالات:(الاقتصادية، السياسية، العسكرية، الاجتماعية و الأمنية) والتي أظهرت مجموعة من المخاطر و التهديدات الإلكترونية تعددت أنواعها وفي المقابل زادت آثارها وانعكاساتها.

المطلب الأول: تعريف التهديدات الإلكترونية ومضمونها:

تختلف التهديدات الإلكترونية من حيث أشكالها ومصادرها ودرجة خطورتها وتتراوح ما بين تهديدات بسيطة ومتوسطة ومعقدة، فالتهديدات البسيطة **simple threats** تتمثل في تلك الهجمات التي يستطيع أي فرد يمتلك قدرات تحليلية وتقنية بدائية القيام بها، تشير القدرات التحليلية إلى القدرة على تحديد الهدف المراد مهاجمته وتحليل نقاط الضعف الموجودة فيه والتي يمكن مهاجمتها، أما القدرات التقنية فتشير إلى امتلاك الآليات الإلكترونية من برامج وشبكات للقيام بالهجوم.[1]

التهديدات الإلكترونية إذن هي مجموعة الاختراقات الموجهة لشبكات الحاسب الآلي لسرقة أو تغيير معلومات أو تدمير النظام الإلكتروني أو استخدام الشفرات الخبيثة والتي تنتقل من حاسب آلي إلى حاسب آلي آخر وتقوم بتعطيل الوظائف التي تقوم بها تلك الأجهزة أو إيقاف عمل الشبكات.[2]

يرى العديد من الباحثين على أنها شكل جديد من أشكال التهديدات التقليدية التي تعتمد على استخدام تكنولوجيا المعلومات لإيذاء الآخرين وبناءا عليه عرفوها من خلال استخدام الوسائل التكنولوجية أو من خلال تطبيق معايير التهديدات التقليدية.

---

[1] نوران شفيق، آثار الهجمات الإلكترونية وخطورتها، تم التصفح يوم 12-07-2018، على الرابط الإلكتروني:
https://www.europarabct.com/%D8%A2%D8%AB%D8%A7%D8%B1-%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9-%D9%88%D8%AE%D8%B7%D9%88%D8%B1%D8%AA%D9%87%D8%A7%D8%8C%D9%86/

[2] نوران شفيق، **أثر التهديدات الإلكترونية على العلاقات الدولية: دراسة في أبعاد الأمن الالكترونية**، القاهرة: المكتب العربي للمعارف، 2018، ص56.

كما يعرف أيضا على أنه فعل يقوض من قدرات وظائف شبكة الكومبيوتر لغرض قومي أو سياسي، من خلال استغلال نقطة ضعف ما تمكن المهاجم من التلاعب بالنظام.[1]

يعد **بيلزي Beelze** أول من أطلق مصطلح التهديدات الإلكترونية ومن أوائل الباحثين الذين اهتموا بدراستها ويعرفها بأنها استخدام تكنولوجيا المعلومات والاتصالات مثل رسائل البريد الإلكتروني والهاتف المحمول والرسائل النصية ومواقع الأنترنت بهدف الأذية.

كما تعرف التهديدات الإلكترونية على أنها: العدوان باستخدام الوسائل التكنولوجية من خلال برامج الدردشة وتشمل بعض السلوكيات مثل الشتائم والسخرية ونشر المعلومات الشخصية والسرية وهذه التهديدات تصل إلى حد القتل.

نخلص من خلال التعريفات السابقة أن التهديدات الإلكترونية تنسب إلى الوسائل المستخدمة وبعض السلوكيات لتعريف التهديدات الإلكترونية مثل التكرار والتعمد.[2]

يتضح من خلال ما سبق أن هنالك تنوعا في استخدام الوسائل التكنولوجية والسلوكيات التي تتم في التهديدات الإلكترونية بالإضافة إلى وجود جدل كبير حول معايير التهديدات الإلكترونية ومن هنا نعتمد

التعريف الإجرائي: التهديدات الإلكترونية هي استخدام الوسائل الالكترونية بشكل عشوائي ومتكرر للسخرية والتهديد، وانتحال الشخصيات وإفشاء الأسرار والاستعباد وذلك عن طريق تطبيقات الأنترنت والهاتف المحمول على اختلافها.

- **الفرق بين التهديدات الإلكترونية والتهديدات التقليدية:**

إن التهديدات الإلكترونية إحدى أشكال التهديدات التقليدية والتي لها بعض الخصائص التي تستمدها من اعتمادها على وسائل تكنولوجية والجدير بالذكر أن هذه التهديدات تنقسم إلى تهديدات مباشرة وأخرى غير مباشرة حيث أنه من الصعب إدراج التهديدات الإلكترونية ضمن التهديدات المباشرة أو غير المباشرة حيث يجب أن تكون لها فئة خاصة نظرا للتفاصيل التي تحتويها في تصنيفها.

---

[1] نورة شلوش، **(القرصنة الإلكترونية في الفضاء السيبراني: التهديد المتصاعد لأمن الدولة، مجلة مركز بابل)**، المجلد 08، العدد 02، 2018، ص 191.

[2] سلوى حلمي علي يوسف، **(واقع البلطجة الإلكترونية بين طلاب جامعة بني سويف وإمكانية التغلب عليها، مجلة العلوم التربوية)**، العدد04، 2017، ص60-61.

وعليه فإنه يمكن ارجاع الاختلاف إلى طبيعة الوسائل المستخدمة وطبيعة العالم الذي تنشط فيه وما تفرضه من ديناميات للتعامل بين أفراده ويمكن إجمال الاختلافات في:

- ❖ الاستمرار: يمكن للتهديدات الإلكترونية أن تستمر على مدار 24 ساعة طوال أيام الاسبوع.
- ❖ الإعتماد على الأجهزة الالكترونية للضغط على الاخرين.
- ❖ امكانية عدم الكشف عن هوية المهدد.
- ❖ الجمهور أو الشهود حيث أن جمهور التهديدات واسع غير محدود.
- ❖ حيث أن التهديدات الإلكترونية واسعة جدا وذات خطورة كبيرة لأنها تتبع الضحية عبر الإنترنت كما أنها أكثر تدميرا وفتكا.[1]

المطلب الثاني: أنواع التهديدات الالكترونية ومستوياتها.

- **أنواع التهديدات الالكترونية.**

أولا: القرصنة الإلكترونية:

إن مفهوم القرصنة الإلكترونية يشير الى إستخدام وسائل الاتصال وتكنولوجيا المعلومات الحديثة في ممارسات غير مشروعة تستهدف التحايل على أنظمة المعالجة الآلية للبيانات لكشف البيانات الحساسة(المصنفة) أو تغييرها والتأثير على سلامتها أو حتى إتلافها.

فالقرصنة الإلكترونية أو المعلوماتيَّة هي عمليَّة اختراق لأجهزة الحاسوب تتمُّ عبْر شبكة الإنترنت غالبًا؛ لأنَّ أغلب حواسيب العالَم مرتبطة عبْر هذه الشَّبكة، أو حتَّى عَبْر شبكات داخليَّة يرتبط فيها أكثرُ من جهاز حاسوب، ويقوم بِهذه العمليَّة شخصٌ أو عدَّة أشخاص متمكِّنين في برامج الحاسوب وطرُقِ إدارتِها؛ أيْ: إنَّهم مُبَرْمِجون ذوو مستوًى عالٍ يستطيعون بواسطة برامج مساعدة اختراق حاسوب معيَّن والتعرُّفَ على محتوياته، ومن خلالها يتم اختراق باقي الأجهزة المرتبطة معها في نفس الشبكة. [2]

كما يصنف تصنيف قراصنة المعلومات:

1. **الْهُواة الهاكرز**:Hackers
2. **المحترفون الكراكرز**:Crackers

---

[1] سلوى حلمي يوسف، **مرجع سابق ذكر**، ص 62-63.

[2] القرصنة ثمن باهظ، تم التصفح يوم 23-02-2019، على الساعة 15:30 على الرابط الإلكتروني: https://elaph.com/Web/Technology/2009/9/486426.html

- **وسائل وأساليب القرصنة الإلكترونية:**

تتعدد وسائل وأساليب القرصنة في اختراق الأمن المعلوماتي للمواقع الإلكترونية ومن أهم الطرق والأساليب مايلي:

أ. **الفيروسات:** هو برنامج خارجي صنع عمداً بغرض تغيير خصائص الملفات التي يصيبها لتقوم بتنفيذ بعض الأوامر إما بالإزالة أوالتعديل أو التخريب وما شابهها من عمليات أي أن فيروسات الكمبيوتر هي برامج تتم كتابتها بواسطة مبرمجين محترفين بغرض إلحاق الضرر بكمبيوتر آخر، أو السيطرة عليه أو سرقة بيانات مهمة، وتتم كتابتها بطريقة معينة.

ب. **الإغراق بالرسائل:** تعني إرسال كم هائل من الرسائل عبر البريد الالكتروني لأجهزة الحاسوب الألية المراد العمل على تعطيلها وتوقيفها على العمل، حيث أنها تصل إلى الجهاز بشكل سريع مما يسبب توقيف الاجهزة عن العمل.

ت. **خداع بروتوكول الانترنت:** ويتم ذلك عن طريق استغلال برتوكولات النقل بأن ينتحل المخترق صفة مستخدم آخر ويقوم بتزوير العنوان الصحيح للمرسل من داخل الشبكة وبذلك يسمح النظام لحزمة البيانات بالمرور باعتبارها حزمة مشروعة.

- **مخاطر القرصنة الإلكترونية على الأمن الإلكتروني:**

من خلال استعراض وأساليب القرصنة على الأمن الإلكتروني للدول، يمكن تلخيص التأثيرات الضارة للقرصنة وخطورتها على الأمن الإلكتروني فيما يلي:

أ. **تدمير المواقع:** مثلما هو الحال عند ضخ مئات الآلاف إلى الموقف وفي الواقع هنالك أسباب مساعدة للقرصنة في تدمير المواقع، منها ضعف الكلمات السرية المستخدمة.[1]

ب. **تسوية المواقع:** يوجد تشابه كبير بين ما يحصل في العالم الافتراضي من عمليات تشويه المواقع عندما يتم إنزال علم الدولة ما من السفينة ورفع علم القراصنة مكانة حيث أن عملية التشويه في أغلب الأحيان ليست سوى تغيير الصفحة الرئيسية للموقع في الصفحة، يعلن المخترق فيها إنتصار على نظام مزود بإجراء أمنية لشبكة يقصد من ورائها إبراز قدراته التقنية.[2]

ت. **العبث بالبيانات:** وذلك لتغيير البيانات أو إنشاء في مراحل الإدخال أو التخزين .

[1] فتيحة ليتيم، نادية ليتيم، **(الأمن المعلوماتي للحكومة الإلكترونية وإرهاب القرصنة، مجلة الفكر)**، العدد 12، ص 245.

[2] فتيحة ليتيم، نادية ليتيم، **مرجع سابق الذكر**، ص 246.

ث. **الأخطار المادية للقرصنة:** يترتب على القرصنة خسائر مادية جسمية تتكبدها الحكومات الإلكترونية، الحكومات ككل وليس فقط الإلكترونية. [1]

ثانيا: الجريمة الإلكترونية.

1. التطور التاريخي للجريمة الإلكترونية:

يتجلى صراع الإنسان من أجل حاضره ومستقبله في حاجته الدائمة إلى اتخاذ القرارات السلمية وتتوقف صحة القرارات على مدى توافر المعلومات المتصلة بالمشكلة المطروحة، ومن هنا يكمن الدافع الأساسي وراء حرص الإنسان على تجميع المعلومات المرتبطة بالجنازات السابقة وأهمية تنظيمها، ومفهوم جريمة الكمبيوتر مر بتطور تاريخي تبعا لتطور التقنية واستخداماتها ويمكن تقسيمها إلى ثالثة مراحل:

المرحلة الأولى: من شيوع استخدام الكمبيوتر في الستينات ومن ثم السبعينات : بظهور استخدام الكمبيوتر و ربطه بالشبكة في الستينات إلى السبعينيات ظهرت أول معاجلة لجرائم الكمبيوتر في شكل مقالات صحفية تناقش التلاعب بالبيانات المخزنة وتدمر أنظمة الكمبيوتر و التجسس المعلومات.[2]

المرحلة الثانية: وفي الثمانينات ظهر نوع جديد من الجرائم ارتبط بعمليات اقتحام نظم الحاسوب عن بعد ونشر الفيروسات عبر شبكات الكمبيوتر ،الذي سبب تدمر الملفات و البرامج أين شاع اصطلاح "الهاكرز"، المعبر عن مقتحمي النظم.[3]

المرحلة الثالثة: شهدت التسعينات تناميا هائلا في حقل الجرائم التقنية وتغيرا في نطاقها ومفهومها، وكان ذلك بفعل ما أحدثته شبكة الإنترنت من تسهيل لعمليات دخول الأنظمة واقتحام شبكات المعلومات، فظهرت أمناط جديدة كأنشطة إنكار الخدمة، التي تقوم على فكرة تعطيل النظام ومنعه من القيام بعمله المعتاد.[4]

---

[1] **نفس المرجع**، 247.

[2] نائلة قورة، **جرائم الحاسوب الاقتصادية**، القاهرة: دار النهضة العربية، 2004، ص21.

[3] يونس عرب، "**جرائم الكمبيوتر والإنترنت إيجاز في مفهوم النطاق والخصائص والصور والقواعد الإجرامية للملاحقة والإثبات**"، ورقة مقدمة في المؤتمر الأمن العربي ، 10-12-2002، ص 08.

[4] **المرجع نفسه**، ص08

2.تعريف الجريمة الإلكترونية:

المعلوماتية يقصد بها المعالجة الآلية للمعلومات، وهي ترجمة للمصطلح الفرنسي **informatique**، وتعني تكنولوجيا تجميع ومعالجة وإرسال المعلومات بواسطة الكمبيوتر، وقد أستعمل مصطلح **traitematique domnes des outomatise**، ويعني المعالجة الآلية للبيانات و مصطلح **telematique** أي اتصالات، وهي تعادل مصطلح **télématique** في اللغة الإنجليزية وإن كان ليس لها أصل في القاموس الإنجليزي، مستمدة من اللغة الفرنسية.[1]

الجريمة الإلكترونية هى الجريمة التي تتم باستخدام جهاز الكمبيوتر من خلال الاتصال بالإنترنت ويكون هدفها اختراق الشبكات أو تخريبها أو التحريف أو التزوير أو السرقة والاختلاس أو قرصنة وسرقة حقوق الملكية الفكرية ويشكل السلوك الإنحرافي جريمة بأركانها المادية والمعنوية.[2]

3. الجريمة التقليدية والجريمة الإلكترونية:

تتشابه الجريمة الإلكترونية مع الجريمة التقليدية من مجرم وضحية والذي قد يكون شخص طبيعي أو شخص اعتباري، أما الاختلاف الحقيقي بين نوعي الجريمة في أداة الجريمة ومكانها، ففي الجريمة الإلكترونية الأداة ذات تقنية عالية وأيضا مكان الجريمة لا يتطلب انتقال الجاني وإنما هي الجرائم تتم عن بعد أي بدون وجود الجاني والمجني عليه في نفس المكان.[3]

تتميز الجريمة الإلكترونية بطبيعة خاصة تميزها عن غيرها من الجرائم التقليدية، وذلك نتيجة ارتباطها بتقنية المعلومات و الحاسب الآلي مع ما يتمتع به من تقنية عالية، وقد أضفت هذه الحقيقة على هذا النوع من الجرائم عدد من السمات والحقائق، والتي انعكست بدورها على مرتكب هذه الجريمة الذي أصبح يعرف بالمجرم المعلوماتي لتميزه أيضا عن المجرم التقليدي

---

[1] نهلا عبد القادر المومني، **الجرائم المعلوماتية**، دار الثقافة للنشر والتوزيع ، 2008 ، ص 20

[2] جمال صابر نعمان أحمد نعمان نعمان، " ماهي الجريمة الإلكترونية وما أنواعها؟"، على الرابط الإلكتروني: https://specialties.bayt.com/ar/specialties/q/11929/%D9%85%D8%A7%D9%87%D9%8A-%D8%A7%D9%84%D8%AC%D8%B1%D9%8A%D9%85%D8%A9-%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9-%D9%88%D9%85%D8%A7-%D8%A3%D9%86%D9%88%D8%A7%D8%B9%D9%87%D8%A7/

[3] يونس عرب، **مرجع سابق الذكر**، ص09.

وقد كان لظهور شبكة المعلومات و تطورها إلى الصورة التي أصبحت عليها الآن فيما يعرف بالأنترنت أثره في إعطاء شكل جديد للجريمة المعلوماتية.[1]

ولعل أهم ما أضفته شبكة المعلومات على الجريمة المعلوماتية هو الطبيعة الدولية أو متعددة الحدود للجريمة.

4. دوافع ارتكاب الجريمة الإلكترونية:

تتنوع دوافع الاقدام على الجريمة الالكترونية باختلاف منفذيها وتبعا لطبيعة ودرجة خبرته في مجال المعلوماتية، التي سوف نتطرق لها:

- **ارتكاب الجرائم كوسيلة للتسلية والدعابة:** دافع المزاح والدعابة يعتبر من الدوافع التي تجعل الشخص يقوم بتصرفات وإن كان لا يقصد من ورائها إحداث جرائم وإنما بغرض التسلية والمزاح فقط.
- **الانتقام:** دافع الانتقام من أخطر الدوافع التي يمكن أن تدفع الشخص إلى ارتكاب جريمة لأن دافع الانتقام غالبا ما يصدر من شخص يملك معلومات كبيرة عن المؤسسة التي يعملها.
- **تحقيق المكسب المادي:** مرتكب الجرائم المعلوماتية يقوم بما لديه من خبرة ومهارة في المجال التكنولوجي بتوجيه هذه الإمكانيات نحو المؤسسات المالية لمحاولة تحقيق المكاسب المادية، وذلك إما بسرقة تلك الأموال أو بتحويلها لحسابه الشخصي داخل البنك.[2]

ثالثا: التجسس الإلكتروني:

1. مفهوم التجسس الإلكتروني:

لا يوجد تعريف محدد للتجسس الإلكتروني فالتجسس في حد ذاته كلمة متشعبة لا يمكن حصرها بتعريف واحد يمكن أن نعرف التجسس الإلكتروني بأنه شكل آخر من الإرهاب يقوم

[1] سفيان سوير، **جرائم المعلوماتية**، (رسالة ماجستير منشورة)، تلمسان، 2010-2011، ص 17.

[2] فتيحة رصاع ،**الحماية الجنائية للمعلومات على شبكة الإنترنت**، (رسالة ماجستير منشورة)، تلمسان، 2001-2012، ص 55.

باستخدام التكنولوجيا الضارة بشكل سلبي من أجل إحداث آثار مدمرة وأضرار بالغة وكبيرة لمحطات التحكم وأجهزة الكمبيوتر وشبكات الاتصال بدوافع سياسية أو عرقية أو دينية.

أما المعنى الاصطلاحي للتجسس الإلكتروني الاطلاع على معلومات خاصة للغير محفوظة على جهاز إلكتروني وليس مسموحا لغير المخول بالإطلاع عليها.

كما هو استخدام وسائل الكترونية تقنية للمعلوماتية الحديثة للدخول بشكل غير مسموح وغير قانوني إلى أنظمة المعلومات الإلكترونية الخاصة.

2. أركان التجسس الإلكتروني:

للتجسس الإلكتروني ركنان وهما:

- **الركن المادي:** هو السلوك الذي يتبعه المجرم في جمعه للمعلومات المهمة والحساسة بطريقة غير مشروعة وبوسائل تقنية المعلومات والتجسس عليها وهي تتطور كلما تطورت التقنية بشكل مساير لها .[1]
- **الركن المعنوي:** تعتبر جريمة التجسس من الجرائم مخالفة للقانون وذلك بدخول المجرم إلى نظام إلكتروني غير مصرح له وإطلاعه على معلومات سرية تتعلق بالاقتصاد أو الأمن والدفاع أو السياسة أو السكان لبلد ما، فالمجرم يعلم بأن انتهاكه يعاقب عليه القانون .[2]

رابعا: الإرهاب الإلكتروني:

1. جذور الإرهاب الإلكتروني:

تمتد جذور الإرهاب بكل صورة عميقة في تاريخ الحضارات والشعوب، فهو مرتبط بالإنسان ونزعاته غير المشروعة وعلى امتداد هذه الرحلة التاريخية للإرهاب لم يكن الإرهاب الإلكتروني إلا صورة حديثة النشأة من صور ذلك الإرهاب التقليدي، فكان هذا الشكل الجديد للإرهاب إذ وجد فيهم الإرهابيون مكانا لتحقيق أغراضهم بوسائل متطورة ومتنوعة وبعيدا عن الرقابة والملاحقة.

---

[1] التجسس على البريد الالكتروني : تم التصفح في 23-05-2019، على الرابط الإلكتروني : http://yemen-press.com .

[2] عمار عباس الحسيني، **جرائم الحاسوب والانترنت: الجرائم المعلوماتية**، ط01، بيروت: مكتبة زين الحقوقية، 2017، ص 334.

ولقد كانت البداية المؤشرة كنقطة مروعة للتنظيمات الإرهابية في الفضاء الالكتروني في بريطانيا منتصف التسعينات من القرن السادس عشر، إذ كشفت تقارير بريطانية عن تطوير الجيش الجمهوري الايرلندي لنظام معلومات معقد تمكن من الوصول إلى هواتف العملاء البريطانية وملفات الصحة لعملاء أحد أكبر المؤسسات الصحية الخاصة في بريطانيا إضافة إلى الملفات عملاء **شركة توماس كوك**.[1]

كما وقد سجل عام 1996 البداية الحقيقية والشرسة للهجمات الإرهابية الإلكترونية المنظمة على الشبكة الإلكترونية الدولية حينما نفذت حركة البيض العنصرية المتطرفة في الولايات المتحدة الأمريكية أكبر هجوم إلكتروني لتعطيل إتلاف جزء من نظام حفظ البيانات الخاص **بالولاية شياباس** المتمردة في المكسيك.

ومنذ ديسمبر 1997 دخلت الشبكة الدولية للمعلومات القوة على خط المواجهة الشعبية للحكومات لتسجل منعرجا تاريخيا مهما في سياق تطور الإرهاب الالكتروني، ولقد امتدت هته الهجمات الإلكترونية على الشبكة الدولية للمعلومات من النطاق الوطني المحلي.[2]

2. تعريف الإرهاب الإلكتروني:

تجمع قواميس اللغة العربية على أن كلمة الإرهاب تعني الفزع والخوف والرعب وكلمة إرهاب مشتقة من الفعل أرهب ويقال أرهب فلان أي خوفه وأفزعه وأما بالنسبة للشق الثاني من العبارة ونقصد به الإلكتروني فهي مفردة دخيلة على اللغة العربية وقد جرى تعريبها لمواكبة التطورات التقنية التي عاشها العالم في ظل المعلومات المعاصرة.[3]

ومع دخول الإرهاب على الفضاء الرقمي الإلكتروني نشأ الإرهاب الإلكتروني بعد أن جرى تداوله بصورة مكثفة في هذه الأدبيات ليعكس تطورا متناميا في رصد ومتابعة هذا النوع من الإرهاب في الفضاء الإلكتروني.[4]

---

[1] حسام الفوزان، **(برمجيات التجسس : القليل من المعرفة شي رائع،مجلة الثقافة المعلوماتية)**،العدد03، 2007، ص، ص 17،18.

[2] سامر مؤيد عبد اللطيف، **(الإرهاب الالكتروني وسبل المواجهة، مجلة جامعة كربلاء العربية)**، المجلد 04، العدد03، 2016، ص 60-61.

[3] https://www.almaany.com/ar/dict/ar-en/electronic/

[4] http://www.ibtesamah.com/showthread-t_10265.html

و وفقا لمكتب التحقيقات الفدرالي فإن الإرهاب الإلكتروني هو هجمات ذات دوافع سياسية ضد المعلومات أو الأنظمة لإحداث أضرار ضد أهداف غير قتالية من قبل جماعات من قبل الجماعات شبه القومية أو عملاء سريين. كما وقد صاغ مركز الدراسات الإستراتيجية CSISتعريف للإرهاب الإلكتروني بأنه استخدام أدوات أن شبكة الأنترنت لإغلاق البنى التحتية الوطنية الهامة أو لإكراه أو ترهيب الحكومة أو المدنيين.

وكان التعريف الأكثر انتشارا هو الذي قدمه **دورثي Dorthy أي دينينغ Dining**، والذي عرفه بأنه الهجمات أو التهديدات للهجوم غير المشروعة ضد أجهزة الكمبيوتر والشبكات والمعلومات المخزنة فيها بقصد تخويف أو إجبار حكومة أو شعبها لتحقيق أهداف سياسية أو اجتماعية.

ومما تقدم يمكن الخروج إلى تعريف للإرهاب الإلكتروني بأنه الهجمات الغير مشروعة ضد حسابات أو شبكات مخزنة إلكترونيا توجد من أجل الانتقام أو الابتزاز أو الاجبار أو التأثير في الحكومة وشعوبها.[1]

3. خصائص الإرهاب الإلكتروني وأهدافه:

- **خصائص الإرهاب الالكتروني:**

يتميز الإرهاب الإلكتروني بعدد من الخصائص والسمات التي يختلف فيها عن بقية الجرائم الأخرى ، ويمكن إنجازها فيما يلي:

- ❖ أن الإرهاب الإلكتروني لا يحتاج في ارتكابه إلى العنف والقوة، بل يتطلب حاسب آلي متصل بالشبكة المعلوماتية.
- ❖ يتسم الإرهاب الإلكتروني بكونه جريمة إلكترونية متعددة للحدود كون أن أثره لا يمكن أن يحده مكان فهو عابر للقارات.
- ❖ صعوبة اكتشاف جرائم الإرهاب الإلكتروني.

[1] سامر مؤيد عبد اللطيف، **مرجع سابق الذكر**، ص 59-60.

❖ إن مرتكب الإرهاب الإلكتروني يكون في العادة من ذوي الاختصاصات في مجال تقنية المعلومات.[1]

- **أهداف الإرهاب الإلكتروني:**

يهدف الإرهاب الإلكتروني إلى جملة من الأهداف غير المشروعة ويمكن إبرازها فيما يلي:

❖ نشر الخوف والرعب بين الأشخاص والدول والشعوب المختلفة.
❖ الاخلال بالنظام العام والأمن المعلوماتي.
❖ تعريض سلامة المجتمع وأمنه للخطر.
❖ تهديد السلطات العامة والمنظمات الدولية وابتزازها.
❖ جمع الأموال والاستيلاء عليها.[2]

4. الأسباب المؤدية إلى نشوء الإرهاب:

لا ينكر أنه ثمة تنوعا علني للأسباب المؤدية إلى نشوء ظاهرة الإرهاب ومرد ذلك إلى التطورات الحاصلة في العالم التي لحقت بها الظاهرة من جراء توظيفها للفضاء الالكتروني:

➢ **الأسباب العامة لظاهرة الإرهاب:**

- **الأسباب السياسية:** من بين أهم الدوافع المحفزة للإرهاب ما يلي:

❖ التطلع إلى السلطة والتنافس للاستحواذ عليها عبر استغلال العمليات الإرهابية.
❖ محاولة فرض رؤية أو إيديولوجية معينة.
❖ الاضطهاد الدينيي والطائفي والقومي داخل الدولة.
❖ النزاعات القائمة بين الدول.
❖ سياسات الهيمنة واستحواذ القوة والتدخلات الدولية.

- **الأسباب الاقتصادية:** يمكن إيجازها فيما يلي:

❖ معاناة الأفراد من المشكلات الاقتصادية المتعلقة بالفقر.

---

[1] عبد الرحمان المسند، "**وسائل الارهاب الالكتروني : حكمها في الإسلام وطرق مكافحتها**"، الرياض، السجل العلمي لمؤتمر موقف الإسلام من الإرهاب، 2004، ص 147.

[2] محمد مؤنس محب الدين، **(الإرهاب والعنف السياسي"، مجلة الأمن العامة)**،العدد 24، 1981، ص 44.

- ❖ انتشار البطالة في المجتمع.
- ❖ الطور اللامتكافي بين الدول المتقدمة والمتخلفة.

- **الأسباب الاجتماعية والنفسية:** يمكن إيجازها فيما يلي:

- ❖ الظروف الحياتية المعقدة.
- ❖ التفكك الأسري والاجتماعي.
- ❖ فقدان الهوية المجتمعية.
- ❖ تفشي ظواهر العنف والجريمة والفوضى.
- ❖ الاحباط وافتقاد الشخص لأهمية دوره في الأسرة والمجتمع.[1]

وباعتبار أن الإرهاب جزء لا يتجزأ من الإرهاب الدولي كظاهرة فإنه يشترك معه في نفس الأسباب السابقة، لكن في المقابل هنالك أسباب أخرى خاصة لإنتاج الإرهاب الإلكتروني وتتمثل فيما يلي:

➢ **الأسباب الخاصة للإرهاب الإلكتروني:**

- ضعف بينة الشبكات المعلوماتية وقابليتها للاختراع.
- غياب الحدود الجغرافية وتدني مستوى المخاطرة.
- سهولة الاستخدام وقلة التكلفة.
- الفراغ التنظيمي والقانوني وغياب السيطرة والرقابة على الشبكات المعلوماتية.[2]

5. صور الإرهاب الالكتروني:

يمكن استخدامها بحسب الوسائل المستخدمة على نوعين أحدهما مباشر وأخرين غير مباشرين:

- **الاستخدام المباشر لشبكة المعلومات في الأنشطة الإرهابية:**

✓ **التهديد الإلكتروني:** في هذا المجال تقوم المنظمات والجماعات الإرهابية.

✓ **القصف الإلكتروني:** هو أسلوب تلجأ إليه المنظمات الإرهابية للهجوم على شبكة المعلومات عن طريق التوجيه لمئات الآلاف من الرسائل الالكترونية.

[1] سائر مؤيد عبد اللطيف، **مرجع سابق الذكر**، ص 61-62.

[2] سائر مؤيد عبد اللطيف، **المرجع نفسه**، ص 62-63.

- ✓ **تدمير أنظمة المعلومات:** يقصد به محاولة اختراق تقوم بها التنظيمات الإرهابية عبر شبكة المعلومات الخاصة بالأفراد أو المؤسسات العامة.

6. وسائل الإرهاب الإلكتروني:

1. **البريد الإلكتروني:** خدمة تسمح بتبادل الرسائل والمعلومات مع الآخرين عبر شبكات المعلومات ويمكن الاطلاع عليها وقراءتها في أي مكان من العالم.

2. **إنشاء مواقع على الانترنت:** يقوم الإرهابيون بإنشاء وتصميم مواقع لهم على شبكة المعلومات لنشر أفكارهم والدعوة إلى مبادئهم.

3. **اختراق المواقع:** إن عملية الاختراق الإلكتروني تتم عن طريق تسريب البيانات الرئيسية ورموز خاصة بالبرامج الأنترنت أو عن طريق نشر الفيروسات وهي عملية تتم في أي مكان من العالم.[1]

خامسا: الحرب الإلكترونية:

1. جذور الحرب الإلكترونية:

يُعَدُّ ظهور ثورة تكنولوجيا الإلكترونيَّات واستخدامها في الأغراض العسكرية – نقطة تحوُّل كبيرة؛ سواء في فنِّ الحرب، أو في إدارة الصراع المسلَّح، فقد أخَذت أسلحة القتال الحديثة ومعداته مكان الصدارة في حسْم أيِّ صراعٍ مسلَّحٍ، وخاصة أسلحة الهجوم الجوي الحديثة؛ لاعتمادها على نُظم السيطرة والتوجيه الإلكتروني، التي تمكِّنها من تنفيذ المهام المطلوبة منها بكفاءة، وإصابة أهدافها بدقَّة عالية؛ نظرًا لاستخدامها نُظُمَ ووسائل الكشْف والتوجيه والتحكُّم.

كانت أساليب الحرب الإلكترونيَّة تستعمل منذ بداية هذا القرن، وبالأخص عندما استُخْدِمت أجهزة الاتِّصالات اللاسلكية في الحروب، ولكن منذ الحرب العالمية الثانية أصبَح موضوع الحرب الإلكترونية محلَّ الاهتمام، من حيث المعدات والأساليب.

[1] وسائل الإرهاب الإلكتروني، تم التصفح في 18-03-2019 على الرابط الإلكتروني :
http://shamela.ws/browse.php/book-1244/page-9

تفيد المصادر أن أوَّل عمليَّة في مجال الحرب الإلكترونية كانتْ في عام 1905م خلال الحرب الروسية اليابانيَّة في معركة(**tsushima**)، عندما كانت سُفن الاستطلاع اليابانية تُراقب الأسطول الروسي عن كثبٍ، وتُرسل جميع المعلومات بالراديو إلى القيادة الرئيسية اليابانية.

2. تعريف الحرب الإلكترونية:

وجود مادي ملموس على أرض الواقع، لكنها تحاكي هذا الواقع تماماً، وهي حرب بلا دماء لكونها صراعاً بين الموجات والإلكترونيات والبرمجيات فقط، وجنودها يعملون من لوحات المفاتيح وأزرار الكومبيوتر. وميادين القتال فيها هي الأسلاك والفضاء الالكتروني، وربما الهواء، وأسلحتها فيروسات الكمبيوتر، والنبضات الإلكترونية.[1]

كما تعرف بأنها الحرب التي تستهدف المعلومات وهي تعبير عن الاعتداءات التي تطال مواقع الانترنت والبيانات الموجودة على الشبكات.[2]

3. أسلحة الحرب الإلكترونية:

تتسلح الحروب الإلكترونية بالعديد من الأدوات والوسائل التّقنية والرقمية، والتي يتم توظيفها في الصراعات الافتراضية الدائرة عبر الفضاء الإلكتروني، يمكن إجمالها فيما يلي:

- ✓ **الاختراق الإلكتروني:** وهي عبارة عن إنشاء نظامٍ أو برنامجٍ إلكتروني يهدف إلى استغلال معلومات الخصم وتدميرها، إضافةً إلى إفساد نظامه الحاسوبي والآلي، وذلك بهدف التقدم عليه أمنياً وعسكرياً واقتصادياً وسياسيا.
- ✓ **زرع الفيروسات التّقنية في البيئات المعلوماتية:** وهي عبارة عن برامج إلكترونية مدمرة، تعمل ضمن آلية معينة يحددها صانع هذه البرامج تهدف هذه الفيروسات الإلكترونية إلى إحداث فوضى في نظام تشغيل الضحية المنوي ضربه إلكترونياً.
- ✓ **القرصنة الإلكترونية:** تُعتبر القرصنة، من أضخم وأشمل الأسلحة الإلكترونية المستخدمة عبر الفضاء الرقمي.
- ✓ **وسائل الإعلام:** تلقى هذه الوسائل إقبالاً عالياً من قبل الجمهور المتلقي، نظراً لسرعة انتشارها، وكثرة متابعيها، و تأثيرها على النفس البشرية.

---

[1] كمال مساعد،(**الحرب الافتراضية سيناريوهات محاكاة الواقع، مجلة الجيش اللبناني**)، العدد 253، 2006، تم التصفح في 20-04-2019، على الرابط: https://www.lebarmy.gov.lb/ar/content

[2] عبد الكريم محسن، ساحة المعارك العظمى التالية: الفضاء الإلكتروني، تتم التصفح في 20-04-2019، على الرابط: http://www.ahewar.org/debat/show.art.asp?aid=291166&r=0

- ✓ **شبكات التواصل الاجتماعي:** وهي تركيباتٌ اجتماعيةٌ تّقنيةٌ ذات محتوى رقمي، تقوم بربط الحلقات الاجتماعية بعض ها ببعض.
- ✓ **الأقمار الاصطناعية:** وهي أسلحةٌ ذات دلالاتٍ استحواذية، هدفها السيطرة على أكبر قدرٍ ممكنٍ من المعلومات، وذلك عبر التقاط ملايين الصور للهدف.
- ✓ .**الخداع الإلكتروني:** وهو من أهم وسائل تأمين الصراعات الإلكترونية، وبه تُحقق المعارك الإلكترونية عنصر المفاجأة.
- ✓ **الغزو الفكري عبر الوسائط المفتوحة:** يقصد بالمصادر المفتوحة، تلك المصادر المعلوماتية العامة والمتاحة للجميع، خاصةً المنتشرة على شبكة الإنترنيت.[1]

4.مجالات الحرب الإلكترونية:

- **مجال الاتصالات والمعلومات:** يشمل هذا القطاع جميع شبكات الاتصالات العامة للدولة، وعلى رأسها الأنترنيت، والحاسبات، والشبكات الحكومية والأكاديمية والمدنية والتجارية، والشبكات المحلية والخارجية، ومحطات البث التلفزي، وشبكات الخلوي، ومراكز استقبال الموجات السلكية واللاسلكية، والألياف الضوئية، وجميع ما يمكن أدراجه تحت هذا القطاع الاتصالي والمعلوماتية.[2]

- **مجال الأعمال العسكرية والحربية:** شهدت القطاعات العسكرية والحربية تطوراتٍ عديدةٍ جعلت منها مجالاتٍ ذات اعتماديةٍ كبيرةٍ على عنصر المعلوماتية والرقمية، وحولتها إلى بناءاتٍ تتسلح بأجيالٍ جديدةٍ من الأسلحة التكنولوجية والاتصالية، وزادت من قدراتها وفاعليتها على الدعم اللوجيستي، والتواصل المعلوماتي والاستخباراتي القائم على توفر عنصر التّقنية الحديثة، والذي أضفى على الوسائل والأدوات العسكرية والحربية قدراً كبيراً من الدقة والجاهزية.[3]

- **مجال الأعمال والأنظمة الحكومية وغير الحكومية:** كما هو الحال في جميع القطاعات الإلكترونية المحوسبة، والتي تُعتبر هدفاً مباشراً لنيران وقذائف الحروب الإلكترونية؛ فإن

---

[1] وليد غسان سعيد جلعود، **دور الحرب الإلكترونية في الصراع العربي الإسرائيلي**، (رسالة ماجستير منشورة)، فلسطين، 2013، ص 98-103.

[2] ذياب موسى البداينة، **الأمن وحرب المعلومات**، ط01، عمان: دار الشروق للنشر والتوزيع، 2006، ص 37.

[3] وليد غسان سعيد جلعود، **مرجع سابق الذكر** ص 92.

الطبيعية، ومصادر توزيع الطاقة، وبنوك الأهداف المعلوماتية، وغيرها الكثير من الإدارات المسؤولة عن قطاعات توليد الطاقة داخل أي بلدٍ في العالم.

- **مجال المعلومات الإعلامية والمجتمعية:** تشترك الصحافة ووسائل الإعلام مع باقي أدوات الاتصال في تقديم العديد من المعلومات والبيانات للجمهور المتلقي، وذلك عبر الوسائل التّقنية والرقمية الحديثة، والتي تُغذي البشرية بكل ما يجول في عالمها الحاضر، بحيث تختزل المسافات والأحداث للإنسان، وتُقدمها له بقالبٍ معلوماتيله أهميته الكُبرى في ديمومة بقائه بصدارة ما يجري من أحداثٍ في عالمه بشكلٍ إلكتروني.[1]
- **مجال الاقتصاد والمال والأعمال:** تحظى قطاعات المال والأعمال في عقدنا الحالي بأهميةٍ كبيرة، خاصةً بعد التحولات الاقتصادية والرأسمالية التي شهدها العالم في عقده الأخير، واندفاع البشرية نحو العمل الاقتصادي والمالي، وسهولة التبادلات التجارية المعتمدة على التجارة الإلكترونية والإدارة الدولية، وانتشار القيم الرأسمالية الداعية للاستهلاك، والانفتاح الاقتصادي المرتكز على العنصر التكنولوجي، والذي أدخل البشرية جمعاء في عصرٍ اقتصادي معتدٍ بالرقميات التكنولوجية والإلكترونية الحديثة.[2]
- **مجال الإنسانية والاجتماعية:** تتحلى هذه القطاعات بالطابع المعنوي، والذي يقوم بتعزيز القيم الإنسانية، والاعتبارات الوطنية والاجتماعية، والولاء للدولة، والأمن الفكري، وغيرها من القيم التي يحتاجها الإنسان لتعزيز صموده في ظل التأثيرات التي قد يتعرض لها أثناء تجواله عبر للفضاء الإلكتروني. تأخذ هذه القطاعات شكل مواقع التواصل الاجتماعي المنتشرة عبر الإنترنيت، والمدونات الاجتماعية والسياسية، وقنوات التواصل الرقمية، والفضائيات التلفزيونية، والتي تُعتبر متنفساً سياسياً واجتماعياً في كثيرٍ من بلدان العالم، ووسائل جماهيريةً وشعبيةً لإيصال الرسائل المجتمعية لصانعي القرارات.[3]

---

[1] خالد معالي، **أثر الصحافة الإلكترونية على التنمية السياسية في فلسطين (الضفة الغربية وقطاع غزة 1996-2007)**، (رسالة ماجستير منشورة)، نابلس، 2008، ص 11.

[2] وليد غسان سعيد جلعود، **مرجع سابق الذكر**، 90،91.

[3] وليد غسان سعيد جلعود، **المرجع نفسه** ، ص96.

- **مستويات التهديدات الإلكترونية:**

من خلال طرح أنواع التهديدات الإلكترونية نستنتج مستويات هذه التهديد من خلال محتواها كما بلي:

القرصنة الإلكترونية تقع في المستوى الأول ومن أمثلتها القيام بعمليات قرصنة المواقع الإلكترونية أو بتعطيل الحواسيب الخادمة من خلال إغراقها بالبيانات.

الجريمة الإلكترونية والتجسس الإلكتروني يقعان في المستوى الثاني والثالث وغالبا ما يستهدفان الشركات والمؤسسات وفي حالات نادرة بعض المؤسسات.

الإرهاب الإلكتروني ويقع في المستوى الرابع ويعبر عن الهجمات غير الشرعية والتي ينفذها فاعلون غير حكوميين ضد أجهزة الكمبيوتر والشبكات والمعلومات المخزنة.

الحرب الإلكترونية وهي المستوى الأخطر للنزاع في الفضاء الإلكتروني وتهدف إلى التأثير على ارادة سياسية للطرف المستهدف وقدرته في عملية صنع القرارات وكذلك التأثير فيما يتعلق بالقيادة العسكرية التي توجهها المدنيين في مسرح العمليات الالكترونية

المطلب الثالث: الجهود المبذولة لمحاربة التهديدات الإلكترونية:

- **الجهود المبذولة لتأمين الفضاء الالكتروني:**

وكالة الاستشارات الأمنية "**زيكوريون**" الاستشارية في تحليل المعلومات والتي مقرها موسكو تتبوأ مرتبة في خدمات القرصنة كواحدة من أفضل خمس جيوش إلكترونية في العالم، روسيا زادت تمويل قدرات الإنترنت الدفاعية بعد سلسلة من الهجمات الإلكترونية الأمريكية والإسرائيلية على المواقع النووية الايرانية في عام 2010.

كما يحتل الجيش الإلكتروني الروسي المرتبة الخامسة في العالم، حيث تظهر التقارير أن قوات الأمن الإلكتروني الروسية وصلت إلى 1000 موظف، وتنفق وزارة الدفاع الروسية حوالي 300مليون سنويا على مثل هذه الأنشطة.[1]

[1] أفضل 10 جيوش إلكترونية في العالم، تم التصفح في 27-04-2019، على الرابط الإلكتروني: https://katehon.com/ar/article/mhy-fdl-khms-jywsh-lktrwny-fy-llm-wm-trtyb-ljysh-lsybrny-lrwsy

أولا: الجهود الوطنية لتأمين الفضاء الإلكتروني:

- **بناء الجيوش الإلكترونية:**

كان للتطور السريع للتكنولوجيا، خاصة الحرب الإلكترونية تحديا لمفاهيم الأمن القومي، حيث أصبحت قضية الدفاع عن البنية القومية للمعلومات ذات أهمية قصوى، وعليه سعت معظم الدول إلى تشكيل جيوش إلكترونية ورصدت ميزانيات ضخمة للتطوير في مجال الهجوم والدفاع والحماية.

- **تشكيل هيئات وطنية للأمن الإلكتروني:**

بما أن التهديدات الإلكتروني لا تفرق بين مدني وعسكري، سعت الدول إلى تشكيل هيئات متخصصة في الأمن الإلكتروني ، تكون مهمتها :

إعداد الإستراتيجية الوطنية للأمن الإلكتروني ،

والإشراف على تنفيذها .

وضع سياسات وآليات الحوكمة والإرشادات المتعلقة بالأمن الإلكتروني وتعميمه .

وضع أطر إدارة المخاطر المتعلقة بالأمن الإلكتروني .

وضع أطر الاستجابة للحوادث والاختراقات .

وضع السياسات والمعايير الوطنية للتشفير .

رفع مستوى الوعي بالأمن الإلكتروني.

- **التشريعات الوطنية للأمن الإلكتروني:**

سن العديد من دول العالم قوانين لمواجهة التهديدات الإلكترونية، بعد أن ظهر جليا مدى سرعة انتشارها وفداحة الخسائر الناتجة عنها، وأجمع أغلب هذه القوانين أن هذه التهديدات ماهي إلى تعدي على الآخرين وعلى ممتلكات العامة والأنظمة بواسطة استخدام التقنية وخصص جزء كبير من هذه القوانين عقوبات رادعة.[1]

[1] سليم دحماني، **أثر التهديدات السيبرانية على الأمن القومي الدولي الولايات المتحدة الأمريكية –أنموذجا–**، (مذكرة ماستر منشورة)، المسيلة، 2017–2018، ص 52.

ثانيا: الجهود الدولية للحفاظ من أجل فضاء إلكتروني آمن:

الطريقة الرئيسية التي تمكن المجتمع الدولي من تعزيز التهديدات الإلكترونية زهي إيجاد بيئة مواتية وتسمح لكل دولة بضمان أمن المعلومات الخاص بها وتطوير التعاون الفعال في هذا الصدد، لذلك يجب على المجتمع الدولي اتخاذ التدابير التالية:

- اتخاذ بآليات استشارية للتعاون في مجال الدفاع عن الفضاء الإلكتروني لتسهيل تبادل الخبرات.
- إنشاء نظم لتبادل المعلومات بشأن رصد الفضاء الإلكتروني وللإخطار المبكر بالهجمات الإلكترونية وتتبع مصادرها.
- التعاون في مجال معاجلة الآثار الناجمة عن التهديدات الإلكترونية.
- وضع برامج تدريب مشتركة للعاملين على الأجهزة التقنية.
- حضور الندوات والحلقات الدراسية والمؤتمرات المشتركة المتعلقة بمكافحة الجرائم الالكترونية.[1]

[1] الجمعية العامة للأمم المتحدة، ص 22-23.

خلاصة الفصل

في نهاية الفصل الأول، نستنتج أن مفهوم الأمن القومي قد طرأ عليه الكثير من التعديل والتغيير، فضبط تعريف للمفهوم لا يعد أمرا هينا، كما وقد تعددت الاتجاهات النظرية للدراسات الأمنية بين الاتجاه التقليدي الذي يهدف إلى حماية مصالح الدولة من التهديدات الخارجية باستخدام القوة العسكرية، والاتجاه المعاصر الذي ارتبط فيه مفهوم الأمن بالتطورات والتغيرات التي مست شكل وجوهر النظام الدولي والإفرازات التي نتجت عنها.

فتوسع الأمن القومي في مفهومه ليشمل جميع المجالات، وتوجه تركيزه على أمن الأفراد والمجتمعات، كما وقد دخلت وسائل تكنولوجيا الاتصالات والمعلومات الحياة الإنسانية لتكتب بداية لعصرنا الحالي بلغة إلكترونية؛ ولتحدث ثورة معلوماتية كبيرة في جميع القطاعات العسكرية، السياسية، الاقتصادية، الثقافية، الاجتماعية، والأمنية.

وعليه كلما زادت هيمنة وسائل تكنولوجيا المعلومات والاتصالات كلما زادت مخاطر التهديدات الإلكترونية وتعددت أنواعها وفي المقابل زادت آثارها وانعكاساتها.

وبهذا أصبح الأمن الإلكتروني أحد أعلى تحديات الأمن القومي، وأصبح من اللازم على الدول وضع إستراتيجيات وآليات للحد من المخاطر والتهديدات الإلكترونية ومواجهتها والقضاء عليها.

الفصل الثاني
الثورة الإلكترونية والأمن القومي

تمهيد:

كان قيام الدراسات المهتمة بالأمن القومي متوافقاً مع ظروف عالمية سياسية وعسكرية جديدة أعقبت الحرب العالمية الثانية والتوازنات والتكتلات والمحاور التي نتجت عن الحرب بين القوى الدولية، بالإضافة إلى الانتشار الكثيف للأسلحة والتطور النوعي الذي شهدته هذه الأخيرة، والذي أدى إلى تعديلات في النظام الدفاعي العالمي وثوابته التقليدية الموروثة، وفرض رؤية جديدة للأمن، وتحديداً جديداً للمجال الأمني للدول.

فارتبط ارتباطا وثيقا بالثورة الالكترونية نظرا لتطور وسائل تكنولوجيا المعلومات والاتصالات وهيمنتها على جميع قطاعات الحياة البشرية. فأصبحنا أمام جرائم إلكترونية حقيقية أثرت على الكثير من الدول من بينها الولايات المتحدة الأمريكية الجزائر وروسيا وإسرائيل.

وفي هذا الإطار يقسم الفصل إلى مبحثين كالتالي:

المبحث الأول: المخاطر الإلكترونية على المجتمع والسيادة.

المبحث الثاني: نماذج عن التهديدات الإلكترونية.

المبحث الأول: المخاطر الإلكترونية على المجتمع والسيادة:

إن التطور الهائل في تكنولوجيا الاتصال الحديثة غيرّ أنماطا كثيرة في حياة الناس، مما أدى إلى إقبال أفراد المجتمع على مواقع التواصل الاجتماعي يوما بعد يوم نظرا لسرعة وسهولة استخدامها وبغض النظر عن ما خلفته من تهديدات داخلية وخارجية داخل المجتمع؛ كما ساهمت هذه التكنولوجيا في إفراز تهديدات الكترونية عديدة أثرت على قضايا السيادة الدولية، وساهمت أيضا حتى بالقضايا التي ترتبط حتى بالعلاقات المجتمعية، وسنقوم في هذا المبحث بتعريف مواقع التواصل الاجتماعي وكذا نشأتها والخصائص وأثرها على الأمن المجتمعي إضافة إلى أثر التهديدات الإلكترونية وعلاقتها بالأمن القومي.

المطلب الأول: أثر مواقع التواصل الاجتماعي على الأمن المجتمعي:

يتضمن هذا المطلب مفهوم مواقع التواصل الاجتماعي؛ نشأته وخصائصه؛ وأثره على البنية المجتمعية.

- **مواقع التواصل الاجتماعي : ضبط مصطلحي:**

أولا: تعريف مواقع التواصل الاجتماعي:

وتتعدد تعريفات مواقع التواصل الاجتماعي وتختلف من باحث إلى آخر وذلك راجع إلى الخلفيات الفكرية والتخصصات في مجال الدراسة والبحث؛ حيث تم تعريفها كما يلي:

يعتبر **جون بارنز John barnes** من الأوائل الذين حاولوا تعريف الشبكات الاجتماعية: حيث قدم مجموعة من التعاريف لها دلالات مختلفة بما يتعلق بشبكات التواصل الاجتماعي من

هذه التعاريف أن شبكات التواصل الاجتماعي هي وسيلة تتيح لنا معرفة طبيعة الجماعة الاجتماعية.[1]

هي منظومة من الشبكات الالكترونية التي تسمح لمشرك فيها بإنشاء حساب خاص به ومن ثم ربطه ،[2] من خلال نظام اجتماعي الكتروني مع أعضاء آخرين لديهم نفس الاهتمامات والهوايات أو جمعه مع أصدقاء الجامعة أو الثانوية.[3]

يعرفها **محمد عواد** :" بأنها تركيبة اجتماعية الكترونية تتم صناعتها من أفراد أو جماعات أو مؤسسات، و تتم تسمية الجزء التكويني الأساسي.[4]

يعرف **بريس bruce** و **مالوني كريشمار Maloney Krichmar** مواقع التواصل الاجتماعي على أنها مكان يلتقي فيه الناس لأهداف محددة وهي موجهة من طرف سياسات تتضمن عدد من القواعد والمعايير التي يقترحها البرنامج.[5]

تعرف بأنها عبارة عن تطبيقات تكنولوجية مستندة إلى الويب، تتضمن التواصل والتفاعل بين المستخدمين، وتسمح بنقل البيانات الإلكترونية وتبادلها بسهولة[6].

---

[1] نسيم بورني، **(مواقع التواصل لاجتماعي وتأثيرها على المراهقين، مجلة العلوم الإنسانية)** ، أم البواقي، جامعة أم البواقي، 2018، ص 223.

[2] وائل مبارك خضر فضل الله، **أثر الفيسبوك على المجتمع**، ط 01، الإسكندرية : مدونة شمس النهضة، 2011، ص 07.

[2] أحمد عصام، **تأثير مواقع التواصل الاجتماعي على خصوصية الفرد الجزائري : دراسة وصفية حول الخصوصية و البنية و القيمية للأفراد طلبة جامعة المسيلة**، (مذكرة ماستر منشورة)، قسم الإعلام والاتصال، المسيلة، 2013، ص 27.

[4] محمد المنصور، **تأثير شبكات التواصل الاجتماعي على جمهور المتلقين– دراسة مقارنة للمواقع الاجتماعية والمواقع الإلكترونية**، (رسالة ماجستير في الإعلام والاتصال)، الأكاديمية العربية في الدانمرك ، 2012،ص 27.

[5] Wasinee Kittiwongvivat, Pimonpha Rakkanngan, **facebooking your dream**, Master Thesis;2010, p20

[6] ماطر عبد الله حمدي، **اعتماد الشباب الجامعي على مواقع التواصل الاجتماعي في التزود بالمعلومات: دراسة مسحية في جامعة تبوك السعودية**، (رسالة ماجستير منشورة، قسم الصحافة والإعلام)، جامعة الشرق الأوسط، 2018، ص17.

ويشير مصطلح مواقع التواصل الاجتماعي أيضا إلى تلك المواقع التي تشكل مجموعات افتراضية ضخمة تقدم مجموعة من الخدمات التي من شأنها تدعيم التواصل والتفاعل بين أعضاء الشبكة الاجتماعية من خلال التواصل في بيئته الافتراضية.[1]

من خلال التعريفات السابقة نخلص إلى **تعريف إجرائي** أن: " مواقع التواصل الاجتماعي هي شبكات للتواصل الاجتماعي والتطبيقات التكنولوجية المستخدمة في شبكة الانترنت (الويب) من قبل جميع فئات المجتمع على حد سواء مثل: الفيسبوك والتويتر ....إلخ.

ثانيا: نشأة مواقع التواصل الاجتماعي:

مرت مواقع التواصل الاجتماعي في نشأتها وتطورها بمرحلتين أساسيتين، الأولى هي مرحلة الجيل الأول للويب **web 1.0** والمرحلة الثانية هي الجيل الثاني للانترنيت **web 2.0** غير أن أكثر مواقع التواصل الاجتماعية جماهيرية ظهرت خلال المرحلة الثانية.

- **المرحلة الأولى:**

بدأت مواقع التواصل الاجتماعي بالظهور في أواخر التسعينيات من القرن الماضي كان الغرض منه ربط زملاء الدراسة مع بعضهم البعض حيث ظهرت في تلك المواقع الملفات الشخصية للمستخدمين و خدمة إرسال الرسائل الخاصة لمجموعة من الأصدقاء، ثم بعد ذلك ظهرت مجموعة من المواقع الاجتماعية التي لم تستطع أن تحقق نجاحا كبيرا بين الأعوام 1999-2004.[2]

[1] فريدة صغير عباس، فطيمة أعراب، **(مواقع التواصل الاجتماعي وانعكاساتها على التنشئة الاجتماعية لدى الشباب وفق منظور الاستخدامات و الإشباعات: دراسة مسحية على عينة من الشباب بولاية الجزائر العاصمة"، مجلة بحوث)**، العدد11، جامعة الجزائر 01، 2018، 174.

[2] أحمد كاظم حنتوش، **(مواقع التواصل الاجتماعي ودورها في قطاع التعليم الجامعي كلية الطب البيطري : جامعة القاسم الخضراء أنموذجا، مجلة مركز بابل للدراسات الإنسانية)**، العدد 04، العراق، 2017، ص 201.

حيث برزت عدة مواقع إلكترونية منها: موقع **كلاس ميتس Class Meats** الذي سمح للمشتركين فيه بعمل قوائم أصدقاء ، ولم تكن مرئية للآخرين، حيث جذب الملايين من المستخدمين لكن أغلقت الخدمة عام 2000، كما ظهرت شبكات أخرى مثل موقع **لايف جورنال Live Journal** وموقع **بلاك بلانت Black Planet** وغيرها.[1]

- **المرحلة الثانية:**

وهي المرحلة التي ظهرت بها الويب **web 2.0**، وهي تحتوي على مجموعة من التطبيقات التي أثرت بدرجة كبيرة وبشكل واضح وملحوظ بشبكات التواصل الاجتماعي، وأضافت الويب 2 شعبية كبيرة لها على الانترنت وذلك بسبب التطبيقات المعاصرة لها: المدونات ومشاركة الفيديو والصور و الملفات والمعلومات، وحولت هذه التطبيقات شبكات التواصل الاجتماعي من الجمود إلى الحياة والتفاعلية،[2] وبالتدرج استطاع مطورا الانترنت أن يستخدموا متصفحات الانترنت لإرسال واستقبال البيانات في نفس الوقت، بدلا عن دورها الأصلي كمستقبل للبيانات، بداية بتطبيقات البريد الالكتروني، الدردشة، ومنتديات الحوار، وانتهاء بالتطبيقات الالكترونية الأكثر حداثة و ثورية مثل موسوعة الويكيبيديا، وقد كانت هذه الفترة في تغيير طريقة التعامل مع متصفحات الانترنت هي البداية الحقيقية لما يعرف بتطبيقات الويب.[3]

---

[1] خديجة عبد العزيز علي إبراهيم، **واقع استخدام شبكات التواصل الاجتماعي في العميلة التعليمية : دراسة ميدانية**، مصر: جامعة الصعيد، 2014، ص 428، 429.

[2] خديجة عبد العزيز إبراهيم، **مرجع سابق الذكر**، ص 429-430.

[3] وائل مبارك خضر فضل الله، **مرجع سابق الذكر**، ص 07-08.

ثالثا: خصائص مواقع التواصل الاجتماعي:

تتمثل مميزات مواقع التواصل الاجتماعي فيما يلي :

- ✓ **شاملة:** حيث تلغى الحواجز الجغرافية والمكانية، تلغى من خلالها الحدود الدولية، حيث يستطيع الفرد في الشرق التواصل مع الفرد في الغرب من خلال الشبكة بكل سهولة.
- ✓ **التفاعلية:** فالفرد فيها كما أنه مستقبل وقارئ فهو مرسل وكاتب ومشارك فهي تلغي السلبية المقيتة في الإعلام القديم.
- ✓ **تعدد الاستعمالات:** مواقع التواصل سهلة ومرنة ويمكن استخدامها من قبل الطلاب في التعليم، والعالم لبث علمه وتعليم الناس والكاتب للتواصل مع القراء وأفراد المجتمع للتواصل وهكذا.
- ✓ **سهولة الاستخدام:** فالشبكات الاجتماعية تستخدم بالإضافة للحروف وبساطة اللغة، وتستخدم الرموز والصور التي تسهل للمستخدم نقل فكرته والتفاعل مع الآخرين.[1]
- ✓ **اقتصادية في الجهد والوقت والمال:** في ظل مجانية الاشتراك والتسجيل، فالكل يستطيع امتلاك حيز الشبكة للتواصل الاجتماعي وليس ذلك حكرا على أصحاب الأموال.
- ✓ **العالمية:** حيث تلغي الحواجز الجغرافية والمكانية، وتتحطم فيها الحدود الدولية فيستطيع الفرد في الشرق التواصل مع الفرد في الغرب ببساطة وسهولة.[2]

[1] عبد الرحمان بن إبراهيم الشاعر، **مواقع التواص الاجتماعي والسلوك الإنساني**، عمان : دار صفاء للنشر والتوزيع، 2015، ص 67.

[2] رشا أديب محمد عوض، **آثار استخدام مواقع التواصل الاجتماعي على التحصيل الدراسي للأبناء**، (مشروع تخرج للحصول على درجة البكالوريوس)، جامعة القدس المقترحة، 2013-2014، ص 23.

رابعا: نماذج عن مواقع التواصل الاجتماعي:

تختلف استخدامات مواقع التواصل الاجتماعي وفق الموضوع أو الزمان أو المكان، وعليه فإن أشهر مواقع التواصل الاجتماعي في العالم ما يلي:

1.الفيسبوك (Facebook):

هو شبكة اجتماعية استأثرت بقبول وتجاوب كبير من الناس خصوصاً من الشباب في جميع أنحاء العالم، وهي لا تتعدى حدود مدونة شخصية في بداية نشأتها في شباط عام 2004، في جامعة هارفارد في الولايات المتحدة الأمريكية، من قبل طالب متعثر في الدراسة يدعى **مارك زوكربيرج Mark Zuckerberg** ، وكانت مدونته "**الفيس بوك**" محصورة في بدايتها في نطاق الجامعة وبحدود أصدقاء **زوكربيرج**، الطالب المهووس في برمجة الكمبيوتر، ولم يخطر بباله هو وصديقين له إن هذه المدونة ستجتاح العالم الافتراضي بفترة زمنية قصيرة جداً، فتخطت شهرتها حدود الجامعة وانتشرت في مدارس الولايات المتحدة الأمريكية المختلفة، وظلت مقتصرة على أعداد من الزوار ولو أنها كانت في زيادة مستمرة.[1]

حيث تحتل شبكة الفيسبوك حاليا من حيث الشهرة والإقبال المركز الثالث بعد موقعي جوجل وميكروسوفت، وبلغ عدد المشاركات أكثر من 8000 مليون شخص وه في تزايد مستمر.

[1] ماطر عبد الله حمدي، **مرجع سابق الذكر**، ص 22.

2.التويتر (Twitter) :

ظهر موقع التويتر في مارس 2006 على يد **جاك دورزي Jack Dorsey**، بيز ستون **biz stone** و **ايفان ويليام Williams Evan** و أتيح للجمهور في جويلية 2006 وعبارة عن شبكة اجتماعيو و خدمة للتدوين المصغر **Micro Blogging** تسمح لمستخدميها بإرسال تحديثات و تدوينات مصغرة لا تجاوز 1470 حرف ، و يمكن إرسال التحديثات وفق 03 طرق هي:

- ✓ عبر نموذج الويب: من خلال الموقع أو بعض التطبيقات التي تسمح بذلك
- ✓ عبر رسالة قصيرة: و ذلك بإرسال SMS من الهاتف النقال للحساب الشخصي على الموقع .
- ✓ عبر رسالة فورية: من برنامج الرسائل خلال الفورية.

التويتر هو خدمة على شبكة الإنترنت حيث يمكن للمستخدمين إرسال رسائل قصيرة تسمى تغريدات باستعراضات 140حرفا.

ويعتبر البعض تويتر منصة التدوين المصغر، و تعتبر خدمة التدوين المصغر هي خدمة على شبكة الإنترنت والذي يسمح للمستخدمين لنشر الرسائل القصيرة للمشتركين أخرى من الخدمة، في الواقع، التدوين المصغر له جذوره في تتابع الدردشة الفورية، والرسائل الفورية والهواتف النقالة SMS. وأكثر تركيزا على الجوانب التقنية من التويتر.[1]

[1] مريم نريمان نومار، **استخدام مواقع الشبكات الاجتماعية وتأثيره في العلاقات الاجتماعية دراسة عينة من مستخدمي موقع الفايسبوك في الجزائر**، (رسالة ماجستيلر منشورة)، باتنة، 2011-2012، ص83.

3.الأنستغرام (Inastagram) :

هو برنامج مجاني طرح في ولاية سان فرانسيسكو الأمريكية في شهر أكتوبر من عام 2010 من قبل المطور التقني **كيفن سيستورم Kevin Systrom** وكان موجها فقط لأجهزة الآيفون و الآي باد والآي بود وغيرها من منتجات شركة أبل وفي شهر ابريل من عامنا الحالي 2012 طورت الشركة المنتجة (تتكون من 13 موظف فقط) البرنامج ليعمل على أجهزه الهواتف التي تعمل بنظام اندريود 2.2، كأجهزة السامسونج جلا كسي وغيرها. تستطيعون إنزالها عن طريق الابل ستور لأجهزة الآي فون وعن طريق الأجهزة الاندرويدGoogle Play.[1]

4.اليوتيوب (you tub) :

هو أشهر موقع ويب إلكتروني لعرض الأفلام بأنواعها المختلفة العلمية، والثقافية، والاجتماعية، والثورية، والفنية .. إلخ، وقد تأسس سنة 2005م، على يد مجموعة موظفين سابقين في شركة باي بال، حيث يقوم على السماح لمستخدميه برفع الفيديوهات والتسجيلات المصورة، ويتيح لهم أيضاً مشاهدة فورية دون الحاجة إلى تحميل لأي فيديو مرفوع على الموقع بشكل مجاني. علماً أن التسجيل في الموقع اختياري وليس إجبارياً، كما يتيح لهم خاصية الإعجاب والتعقيب عليها، ويستخدم في ذلك تقنية الأدوبي فلاش لفتح وعرض المشاهد المصورة المتحركة، إضافةً إلى أن موقع يوتيوب يحتوي على 62 واجهة للغة.[2]

[1] https://instaview.me/ar

[2] اليوتيوب، تم التصفح يوم 18-04-2019، على الرابط:
https://mawdoo3.com/%D8%A8%D8%AD%D8%AB_%D8%B9%D9%86_%D8%A7%D9%84%D9%8A%D9%88%D8%AA%D9%8A%D9%88%D8%A8

- **موقع لينكد إن:**

هي شبكة اجتماعية مختصة بالعمل والتجارة تضم العديد من المحترفين والمحترفات في العديد من الآلات و يتشاركون مجموعة اهتمامات.

وموقع لينكدن هو شبكة اجتماعية مهنية، ففي الوقت الذي تركز فيه مواقع الشبكات الاجتماعية مثل "فايسبوك" **وماي سبيس My Space** على العلاقات الشخصية والاجتماعية، لينكدن يسمح للمهنيين بإنشاء أعمالهم.

ورغم بداياته في 2002 إلا أنه اليوم أصبح من بين أهم الشبكات الاجتماعية المهنية . و يعرفه موقع تكنوبيديا على أنه موقع يضع فيه المستخدمين معلومات مهنية شخصية تتضمن تفاصيل مثل الخلفية التعليمية، التاريخ الوظيفي والعملي وكذا قائمة المشاريع المهنية الكبرى إلى جانب الشهادات المهنية والعضوية المهنية وكل هذه المعلومات توضع في الملف الشخصي الذي يمثل دليل المستخدم.[1]

خامسا: أثر مواقع التواصل الاجتماعي على الأمن المجتمعي:

أصبحت مواقع التواصل الاجتماعي من أهم الوسائل التي ارتكزت عليها المخططات الإستراتيجية الإرهابية لنشر العنف والفوضى والإرهاب والأعمال الإجرامية، ونشر الشائعات والأخبار المغلوطة، وزعزعة القناعات الفكرية والثوابت العقائدية والمقومات الأخلاقية والاجتماعية التي من شأنها إحداث بلبلة داخل المجتمع وخلق حالة لأمن، مما جعلها تشكل خطرًا على الأمن القومي الخاص بكل الدول النامية بصفة خاصة.

نظرا لنقص الإمكانيات والتدابير لمكافحة هذه الظاهرة الخطيرة علي الامن المجتمعي،وخاصة في الفترة ما عرف بالربيع العربي، وظفت الجماعات الجهادية المتطرفة التي تتخذ من الإسلام ستارًا للاختباء وراءه، فضلًا عن بعض الأفراد من ذوى الأفكار الهدامة مواقع التواصل الاجتماعي في مواجهة الدول وزعزعة الأمن وزرع الفتن، وتدمير مرتكزات التنمية ونشر الفوضى والدماء ونشر الشائعات المغرضة ؛ لتضليل الأجهزة الأمنية التي من شأنها

[1] https://www.techopedia.com/definition/26940/linkedin-li

تهديد أمن المجتمع واستقراره السياسي ونسيجه الاجتماعي وبث الرعب بين المواطنين وترويعهم لإظهار عدم أمن واستقرار البلاد، وتنسيق العمليات الإرهابية والهجمات العنيفة التي تشنها ضد مؤسسات الدولة ومؤسساتها الأمنية والعسكرية والقضائية، وإفشاء المعلومات العسكرية السرية، كما تستخدم في التجسس وفي دعم المسلحين ، من خلال النشر المكثف للصور وملفات الفيديو والوثائق التي تدعم الأفكار التي تروج لها، وتعطيل أنظمة قطاعات حكومية وحيوية.[1]

المطلب الثاني: التهديدات الإلكترونية الدولية وقضايا السيادة:

تغيرت مفاهيم السيادة في دول العالم بفعل التطورات التّقنية والإلكترونية التي طرأت على حياة الأفراد والمؤسسات والحكومات والمجتمعات، لتوجد التطورات التكنولوجية الهائلة ساحاتٍ سياديةٍ جديدةٍ دفعت دول العالم لفرض رقابتها الأمنية عليها .

فلم يعد الأمر مقتصراً على المحيط الجغرافي أو المائي أو حتى الجوي للدول؛ بل عملت وسائل الاتصال الحديثة على خلق فضاءٍ جديدٍ يختلج كمياتٍ كبيرةٍ من المعلومات التي تخص الأمن القومي لدول العالم.

شكلت هذه الوسائل التّقنية والرقمية الحديثة، والتي تفاعلت مع اقتصاديات المعرفة الرقمية؛ حالةً من الانفتاح العالمي و الأممي، ليتحول العالم بأسره إلى سوقٍ واحدة، تحكمه مجموعةً من الشركات العملاقة المعتمدة على وسائل التّقنية الحديثة في نشر منتجاتها حول العالم، كشركات السيارات العالمية، وشركات الأجهزة الإلكترونية الكُبرى، وشركات الأغذية، وشركات الحواسيب وتوابعها، وغيرها من الشركات العابرة للقارات والدول والقوميات.[2]

[1] Julian Saada, **révoltes dans le monde arabe : une révolution facebook ?**,Raoul Dandurand Chair , 21 avril 2011, p32.

[2] بيتر مارين، هانس. شومان، هارالد، **فخ العولمة**، ترجمة : رمزي زكي ، الكويت : المجلس الوطني للثقافة والفنون والآداب سلسلة كتاب عالم المعرف، أكتوبر 1998 ، ص ص309،307.

طغى هذا المشهد التطوري على السيادة القومية والجغرافية والسياسية للدول، ليشكل ما يعرف بِـ (**سيادة الفضاء Cyber Space**) والذي ما فتئ وأن أصبح الوطن الجديد للإنسان، والدولة الحديثة للبشرية في عصرها الرقمي.

يتميز هذا الوطن الإلكتروني بمعدومة الحدود والتراث والسيادة القومية، وتتبناه شبكات الانترنيت المنتشرة عبر أرجاء المعمورة دون حدودٍ أو قيود.[1]

وهو شأن دفع العديد من دول العالم لوضع مفهومٍ محددٍ لأمن معلوماتها الإلكترونية والقومية، يتمثل في الخطط الإستراتيجية والأمنية الاستباقية النابعة من داخل أروقة صنع القرار السياسي، والهادفة لحماية بياناتها ومعلوماتها المنتشرة عبر الفضاء الإلكتروني و المعلوماتي.

في خضم هذا الوعي التّقني و المعلوماتي والإلكتروني الذي أوجدته تكنولوجيا المعلومات في عالمنا المعاصر؛ تحولت البشرية بأسرها إلى منتجة ومتلقيةٍ ومستخدمةٍ لوسائل الاتصال الحديثة بشكلٍ كبير، والتي عملت بدورها على إحلال الأنظمة الإلكترونية الرقمية، من هواتف محمولة، وحواسيب متطورة، وشبكاتٍ تكنولوجيةٍ متصلةٍ بالإنترنيت، وأنظمةٍ للتشغيل ذات طاقةٍ عاليةٍ، مكنت الإنسان من الاطلاع على عالمه الخارجي بشكلٍ أكثر وضوحاً ونقاء.[2]

رفعت هذه التطورات الاتصالية الهائلة من شأن المعلومات في حياة المجتمعات المعاصرة، وحولتها إلى مصدرٍ للثروة البشرية اللازمة للانطلاق ق نحو عصر المعرفة .

ساهم هذا التحول، وبشكلٍ ضخمٍ، في جعل المعلومات الإلكترونية والرقمية السارية في القنوات التكنولوجية رأس مالٍ مهماً يفوق الأهمية التي تتحلى بها رؤوس الأموال الاقتصادية والمالية في وقتنا الحالي، مما دعا إلى ضرورة التفكير في حمايتها – أي المعلومات الإلكترونية

---

[1] محمد عابد الجابري ، **قضايا الفكر المعاصر: العولمة- صراع الحضارات- العودة إلى الأخلاق - التسامح - الديمقراطية ونظام القيم- الفلسفة والمدنية**، بيروت: مركز دراسات الوحدة العربية، 1997م، ص ص147، 149.

[2] سميرة شيخاني ، **(الإعلام الجديد في عصر المعلومات ، مجلة جامعة دمشق)**، لعدد 01-02، 2010، ص 430، 445، 456.

_ من أي هجومٍ قد يعترض سير عملها في بيئتها الرقمية والتكنولوجية المليئة بالمخاطر والتهديدات .

نسجت الحاجة إلى أمنية المعلومات في عقدنا الحالي لإحداث طفرةٍ واسعةٍ في كيفية استخدام وسائل الاتصال الجماهيري الحديثة، خُصوصاً تلك التي تتسم بالطابع الدولي والعالمي، والتي باتت تؤثر على صنع القرارات السياسية والاجتماعية والثقافية والاقتصادية والأمنية للدول المعاصرة، في مشهدٍ أتاح الفرصة للبشرية للاشتراك في صنع قرارها الأممي.

خلاصة القول؛ يمكننا التنويه هنا، وفي وطأة هذا التلاحم الإنساني والرقمي، أنه بات على دول العالم حماية أمن معلوماتها الإلكترونية، والذي راح يشكل خطراً كبيراً على أمنها القومي، وبالتالي تهديد وجودها في عالمٍ تكنولوجي ومعرفي تسوده المخاطر من كل حدبٍ وصوب.[1]

المطلب الثالث: علاقة الأمن الإلكتروني بالأمن القومي:

أصبح للفضاء الإلكتروني دور في حركة التفاعلات والتحولات البنيوية كمجال جديد في العلاقات الدولية وبدأ ينتقل تأثير المتغيرات الهيكلية وتحتية إلى أحدى التغيرات الكيفية في النظام الدولي، وأصبح العالم في تطور في المخاطر الأمنية مع التطور التكنولوجي السريع.

و أصبحت قضية الأمن الإلكتروني تلقى اهتماما متصاعدا على أجندة الأمن الدولي وذلك في محاولة لمواجهة تصاعد التهديدات الالكترونية ودورها في التأثير على الطابع السلمي للفضاء الإلكتروني؛ وباتت العلاقة بين الأمن والتكنولوجيا في تزايد مستمر.[2]

---

[1] وليد غسان سعيد جلعود، **دور الحرب الإلكترونية في الصراع العربي الإسرائيلي**، (رسالة ماجستير منشورة)، جامعة النجاح الوطنية كلية الدراسات العليا، فلسطين ، 2013، ص 50.

[2] عادل عبد الصادق، **(القوة الالكترونية أسلحة الانتشار الشامل في عصر الفضاء الالكتروني)، سلسلة قضايا إستراتيجية**، 2012، ص02.

وذلك من منطلق أن مفهوم الأمن القومي لم يعد متعلقاً بذلك الكيان المادي فقط والحدود والحفاظ على عناصر قوة الدولة والمقدرات القومية لها ، وارتبطت القوة العسكرية بالتحكم في أربعه مجالات تتشكل من القدرة على السيطرة على البر والبحر والجو والفضاء الخارجي، وكان الفكر الأمني مرتبطاً بمسالة الدفاع والهجوم عن طريق الجيوش التقليدية أو دعم الحلفاء وكان يتحقق ذلك الأمن عن طريق عده عناصر سياسية واقتصادية ودبلوماسية وتكنولوجية وعسكرية، و كانت تلك العناصر ذات عالقة ترابطية فيما بينهما حيث يدعم كل منهما الأخر، حيث يؤدي الضعف في احدها الى ضعف العناصر الأخرى والعكس، وكانت الدول في السابق أكثر انعزال عن بعضها البعض، وكانت مسالة الدفاع عن حدودها القومية جزءا هاما من حماية عناصر قوتها القومية.وجاء الفضاء الالكتروني بخصائص وعناصر مميزة ، وليكون له تأثير على الأمن.[1]

بل وأصبح المفهوم الجديد للأمن القومي يدور في فلك الحفاظ على سالمة الدولة في ظل تلك التطورات التكنولوجية ومن انعكاسا طبيعة الصراع الدولي في ظلً ثم اختلفت آليات التعامل معها؛ وانعكس ذلك في تغير طبيعة الصراع والقوة وممارستها وفي إحداث تغييرات داخل البيئة الأمنية للنظام الدولي.

أوجب هذا على الدول والحكومات أن تغير مفاهيمها التقليدية وأن تتبنى مفاهيم تتلاءم مع عصر جديد يمكن تسميته بالعصر الالكتروني وأن تضع سياسات تمكنها من الاستفادة من الانترنت وتفادي مخاطرها.[2]

إذا كان الأمن القومي يعنى بالحماية وغياب التهديد لقيم المجتمع الأساسية وغياب الخوف من خطر تعرض هذه القيم للهجوم، فإن الفضاء الإلكتروني قد فرض إعادة التفكير في مفهوم الأمن، والذي يتعلق بدرجة تمكن الدولة من أن تصبح في مأمن من خطر التعرض

[1] عادل عبد الصادق، **(الفضاء الإلكتروني وتهديدات جديدة للأمن القومي، قضايا إستراتيجية)**، 2010، ص 02.

[2] إيهاب خليفة، **(كيف تدير الدولة شؤونها في عصر الانترنت، مركز المستقبل للدراسات والأبحاث المتقدة، دورية اتجاهات حديثة**، العدد06، 2015، ص 11.

للهجوم، للتهديد، من وإجراءات الحماية ضد تعرض المنشآت الحيوية للبنية التحتية خلال الاستخدام السيئ لتكنولوجيا الاتصال والمعلومات.[1]

إن العلاقة بين الأمن الإلكتروني والأمن القومي تزداد كلما ازداد تضخم المحتوى المعلوماتي العسكري والأمني والفكري والسياسي والاجتماعي والاقتصادي والخدمي والعلمي والبحثي.[2]

[1] سليم دحماني ، **مرجع سابق الذكر** ، ص37.

[2] إيهاب خليفة، **مرجع سابق الذكر**، نفس الصفحة.

المبحث الثاني: نماذج عن التهديدات الإلكترونية:

بعد التطرق لمفهوم التهديدات الالكترونية، أنواعها و أثارها و انعكاساتها سنستعرض في هذا المبحث نماذج مختلفة عن التهديدات الالكترونية.

المطلب الأول: الجريمة الإلكترونية في التشريع الجزائري:

برز إلى الوجود نوع جديد من الجرائم وهو ما يصطلح على تسميته بالجرائم الإلكترونية ومجالها جهاز الكمبيوتر المستخدم لاختراق شبكة الإنترنت لذلك يمكن القول أن كل تطور ايجابي لا يخلو من سلبيات والآثار السلبية للانترنت كبيرة وخطيرة ذلك هو الأمر الذي ألقى رجال القانون مسؤولية تاريخية وإنسانية تجاه هذا الخطر الدائم إذ لا يخفى على أحد بأن الجرائم الإلكترونية لم تعد مقتصرة على القرصنة لسرقة المعلومات والسطو على أرقام بطاقات الائتمان لاستخدامها والاستغلال الجنسي للأطفال والإخلال بالآداب العامة ناهيك عن جرائم التجسس والإرهاب شملت مختلف المجالات.

أولا: تعـريف المشـرع الجـزائري للجـريمة الإلكتـرونية:

سنتطرق هنا إلى تعريف الجريمة الالكترونية في التشريع الجزائري تعريفا فقهيا وأكاديميا وقانونيا:

1. **التعـريف الفقهـي:** تعرف على أنها: " كل عمل أو امتناع عن عمل يقوم به شخص إضرارا بمكونات الحاسب المادية والمعنوية، وشبكات الاتصال الخاصة به، باعتبارها من المصالح والقيم المتطورة التي تمتد مظلة قانون العقوبات لحمايتها.[1]

أو أنها: " استخدام الأجهزة التقنية الحديثة مثل الحاسب الآلي و الهاتف النقال، أو احد ملحقاتها أو برامجها في تنفيذ أغراض مشبوهة وأمور غير أخلاقية لا يرتضيها المجتمع.[1]

[1] سعيدة بعرة، **الجريمة الإلكترونية في التشريع الجزائري: دراسة مقارنة**، (مذكرة ماستر منشورة)، بسكرة، 2015-2016، ص 29.

ومن خلال هذه التعاريف تبنى الفقه الجزائري تعريف المؤتمر العاشر للأمم المتحدة لمنع الجريمة حول جرائم الحاسب الآلي وشبكاته إذ عرف الجريمة المعلوماتية بأنها جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوب وتتمثل من ناحية المبدئية ، جميع الجرائم التي بمكن ارتكابها في بيئة إلكترونية.[2]

2. **التعـريف الأكـاديمي:** كل فعل إجرامي متعمد أي كانت صلته بالمعلوماتية ، ترتبت عته خسارة تلتحق بالصحية أو مكسب يحققه الجاني،[3] كما يمكن الاعتماد في التعريف الواسع للجريمة المعلوماتية على :

– على ما تكون المعلوماتية موضوعا للاعتداء عندما تقع الجريمة على المكونات المادية للأجهزة والمعدات المعلوماتية .

– عندما تكون المعلوماتية أداة ووسيلة للاعتداء عندما يستخدم الجاني أو جهاز معلوماتي لتنفيذ جريمته.[4]

3. **التعـريف القـانوني:** تبنى المشروع الجزائري للدلالة على الجريمة مصطلح المساس بأنظمة المعالجة الآلية للمعطيات معتبرا أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية محلا للجريمة، بحيث لم يتخلف المشرع الجزائري بدوره عن ركب التشريعات التي وضعت تعريفا لنظام المعلومات حيث أنه عرف من خلال نص المادة (2) من الفقرة من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها؛مسميا إياه :"المنظومة المعلوماتية " وهي أي نظام

---

[1] عبد العزيز بن غرم الله الغامدي، **جرائم الإنترنت وعقوباتها: وفق نظام مكافحة الجرائم المعلوماتية 1428: دراسة مقارنه**، ط 01، الرياض: دار الكتاب الجامعي للنشر والتوزيع، 2017، ص 75.

[2] زبيخة زيـدان، **الجريمة المعلوماتية في التشريع الجزائري و الدولي** ، الجزائر: دار الهدى، 2011، ص44.

[3] سعيدة بعرة، **مرجع سابق الذكر**، ص 30.

[4] نوفل علي عبد الله الصفوة، محمد عزت فاضل الطائي،**(جريمة الإخلال بالآداب العامة بواسطة وسائل تقنية المعلومات: دراسة مقارنة، مجلة بحوث مستقبلية)**، العدد 29-30، كلية الحدباء الجامعة، 2010، ص 64-65.

منفصل أو مجموعة من الأنظمة المتصلة مع بعضها البعض أو مترابطة، يقوم واحد منها أو أكثر معالجة الآلية للمعطيات تنفيذا لبرنامج معين.[1]

ثانيا: موقف المشرع الجزائري من الجريمة الإلكترونية:

من خلال ما تقدم من تعريفات الجريمة الالكترونية في التشريع الجزائري نستنتج موقف المشرع من هذه الجريمة، وهذا الموقف متمثل في أن التقدم التكنولوجي وانتشار وسائل الاتصال الحديثة أدى إلى بروز أشكال جديدة من الإجرام، مما دفع الكثير من الدول إلى النص على معاقبة هذا النوع من الجرائم، تسعى من خلال هذا المشروع إلى توفير حماية الجزائية للأنظمة المعلوماتية وأساليب المعالجة الآلية للمعطيات.

وبالتالي قام المشرع الجزائري بتعديل قانون العقوبات لسد الفراغ القانوني في هذا المجال وكان ذلك بموجب القانون رقم 15/04 المؤرخ في 2004/11/10 المتمم والمعدل لأمر 66/156المتضمن لقانون العقوبات والذي أقر له القسم السابع مكرر منه تحت عنوان :المساس بأنظمة المعالجة الآلية للمعطيات، فقد أثار المشرع الجزائري استخدامه لمصطلح لدلالة على كلمة المعلومات والنظام الذي يحتوي عليها ويخرج بذلك من نطاق التجريم تلك الجرائم التي يكون النظام المعلوماتي وسيلة وحصرها فقط في صور الأفعال التي تشكل اعتداء على النظام المعلوماتي، أي الجرائم التي يكون النظام المعلوماتي محلا لها.[2]

وقد قدر المشرع في تدخله هذا أن جوهر المعلوماتية هو المعطيات التي تدخل إلى الحاسب الآلي فتحولها إلى معلومات بعد معالجتها وتخزينها ، فقام بحماية هذه المعطيات من أوجه عدة.

---

[1] **الجمهورية الجزائرية الديمقراطية الشعبية**، قانون رقم 09-04 المؤرخ في 14 شعبان 1430 سنة 2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها ح رع 47، صادر بتاريخ 2009/08/16، ص 05.

[2] نعيم سعيداني، **آليات البحث وتحدي عن الجريمة المعلوماتية في القانون الجزائري**، (رسالة ماجستير منشورة)، باتنة، 2012-2013، ص 41.

تم في مرحلة لاحقة اختيار المشرع الجزائري للتعبير عن الجريمة المعلوماتية مصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بموجب القانون رقم 04/09 المتضمن من جرائم مكافحتها، كما ونجد المشرع الجزائري تطرق إلى تعريف الجريمة المساس بأنظمة المعالجة الآلية للمعطيات في المادة 2 من قانون رقم 04/09 وجرم الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات في مواد من 394 مكرر إلى 394 مكرر 7 من قانون العقوبات.[1]

ثالثا: الطبيعة القانونية الخاصة للجريمة الإلكترونية:

إن دراسة الجريمة الالكترونية بشكل خاص تدخل ضمن قسم من أقسام قانون العقوبات وهو قسم الخاص وهو ذلك الفرع الذي يدرس كل جريمة على حده، متناولا كل عناصرها الأساسية والعقوبة المقررة لها، فالجريمة تتعلق بالقانون المعلوماتي لأنها ظاهرة إجرامية ذات طبيعة خاصة .

إن هذا النوع من الجرائم يرتكب ضمن نطاق المعالجة الإلكترونية للبيانات سواء أكان في تجميعها أو تجهيزها أم في إدخالها إلى الحاسب المرتبط بشبكة المعلومات ولغرض الحصول على معلومات معينة.[2]

وتكمن الطبيعة الخاصة لهذه الجرائم في قدرة شبكة المعلومات على نقل وتبادل معلومات ذات طابع شخصي وعام في آن واحد، مما يؤدي إلى الاعتداء على الخصوصية والسبب في ذلك توسع بنوك المعلومات بأنواعها علاوة على رغبة الأفراد وسعيهم إلى ربط حواسيبهم بالشبكة.

وبالتالي هذه الطبيعة الخاصة للأفعال المجرمة تحدد المسؤولية التي يفترض تطبيقها على الأشخاص المسئولين، ومن خلال المجال التي ترتكب فيه الجريمة المعلوماتية والمحل الاعتداء عليها وبهذا تظهر لنا الطبيعة القانونية الخاصة للجريمة الالكترونية.[1]

[1] نعيم سعيد، **مرجع سابق الذكر**، ص 41.

[2] سعيدة بعرة، **مرجع سابق الذكر**، ص 33.

إن التطور المعلوماتي يفتح المجال لاقتناء وسائل الكترونية تمكن المتجاوزين لاستخدامها في ارتكاب جرائم مختلفة، لأن الإجرام المعلوماتي يتعلق بكل سلوك غير مشروع فيها يتعلق بالمعالجة الآلية لبيانات، وإدخال المعلومات، ونقلها ومن ثم يتحتم ضمه إلى نطاق القانون الجنائي على الرغم من أن معظم نصوصه المقارنة عاجزة عن مواكبة التطور المعلوماتي أو بما يحويه من فراغ تشريعي في هذا المجال.[2]

أما من حيث تكييف القانوني فتتخذ هذه الجرائم طبيعة خاصة إذا لم تكن القواعد التقليدية مخصصة لهذه الظواهر الإجرامية المستحدثة، إن تطبيق النصوص التقليدية على الجرائم المعلوماتية يثير مشاكل عديدة في مقدمتها مسألة الإثبات وصعوبة إيجاد دليل مادي يدين مرتكب الجريمة، لأنه من السهل على الجاني محو أدلة الإدانة في وقت قصير لا يتجاوز لحظات وخاصة في حالة تفتيش الشبكات أو عمليات اعتراض الاتصال قد تكون البيانات التي يجري البحث عنها مشفرة ولا يعرف شفرة الدخول إلا أحد العاملين على الشبكة و من هنا تثار مسألة مدى مشروعية إجباره على فك الشفرة.

ومن صعوبة ملاحقة مرتكبي الجرائم المعلوماتية الذين يقيمون في دولة أخرى دون أن ترتبط هذه الدولة باتفاقية مع الدولة التي تحقق فيها السلوك الإجرامي أو جزء منه وفي ضوء الاعتبارات السابقة يمكن القول بأن هذه الجرائم تتمتع بطبيعة قانونية خاصة.[3]

---

[1] محمد زكي أبو عامر، علي عبد القادر القهوجي، **قانون العقوبات، القسم الخاص**، القاهرة: دار النهضة العربية، 1993، ص09.

[2] محمد علي سالم، حسون عبيد هجيج، **(الجريمة المعلوماتية، مجلة جامعة بابل: العلوم الإنسانية)**، المجلد 14، العدد06، العراق، 2007، ص 91.

[3] محمد علي سالم، حسون عبيد هجيج، **مرجع سابق الذكر**، ص 91-92.

رابعا: قوانين مكافحة الجريمة الإلكترونية:

الدستور الجزائري: نصت المادة 38 منه على القانون يحمي حقوق المؤلف ولا يجوز حجز أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ والإعلام إلا أمر قضائية.

نصت المادة 39 منه " لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميها القانون ." سرية المراسلات والاتصالات الخاصة بكل أشكال مضمونة.[1]

قانون رقم 2000-03 المؤرخ في 2000/8/5 والذي يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية : تسارع هذا القانون الى مواكبة التطور الذي شهدته التشريعات العالمية مسايرة التطور التكنولوجي لذلك بات من السهولة بمكان إجراء التحويلات المالية عن الطريق الالكتروني ذلك ما نصت عليه المادة 87 من هذا القانون بالقول " يمكن أن ترسل الأموال ضمن النظام الداخلي بواسطة الحوالات الصادرة عن المتعامل والمحولة بالبريد أو البرق أو عن الطريق الإلكتروني.[2]

نصت المادة 2/84 منه بقولها " تطبق أحكام المادة 89 من هذا القانون عن استعمال جوالات دفع عادية أو الكترونية أو برقية." نصت المادة 105 الفقرة الأخيرة على أنه " لا يمكن بأي حال من الأحوال انتهاك حرمة المراسلات".[3]

رتبت **المادة 127** منه جزاء كل من تسول له نفسه ويحكم مهنته أن يفتح أو يحول أو يخرب البريد أو ينتهك حرية المراسلات بنصها : " كل موظف أو عون من أعوان الدولة أو مستخدم أو مندوب عن مصلحة البريد يقوم اختلاس أو إتلاف رسائل مسلمة إلى البريد أو يسهل فضها

[1] مولود ديدان، **الدستور، تعديل نوفمبر 2008**،الجزائر: دار بلقيس، ص 16

[2] **المادة 87،** قانون رقم 2000-03 المؤرخ في 5أوت 2000 والذي يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية.

[3] المادة 2/84 ، **نفس القانون.**

أو اختلاسها أو إتلافها يعاقب بالحبس من ثلاثة أشهر إلى خمس سنوات وبغرامة من 30.000دج إلى 500.000 دج.

ويعاقب بالعقوبة نفسها كل مستخدم أو مندوب في مصلحة البرق أو يختلس أ يتلف برقية أو يذيع محتواها، ويعاقب الجاني فضلا عن ذلك بالحرمان من كافة الوظائف أو الخدمات العمومية من خمس إلى عشر سنوات.

قانون رقم 08 ـ01: المؤرخ في 23/1/2008والمتم لقانون رقم :83 ــ 01 متعلق بالتأمينات : المادة 6 مكرر 1 نصت على أنه البطاقة الالكترونية تسلم للمؤمن له اجتماعيا مجانا من طرف هيئات الضمان الاجتماعي وهي صالحة في كل التراب الوطني وهي تقدم لكل مقدم علاج أو مقدم خدمات مرتبطة بالعلاج وهذا الأخير يزود الكترونيا يسمى " المفتاح الالكتروني لهيكل العلاج " حسب نص المادة 65 مكرر.[1]

نصت المادة 93 مكرر 2 منه على: معاقبة كل من يسلم أو يستلم البطاقة الالكترونية بغرض استعمالها بطريقة غير مشروعة وجاءت كما يلي:"دون الإخلال بالعقوبات المنصوص عليها في التشريع المعمول به، يعاقب بالحبس من سنتين إلى خمس سنوات وبغرامة من .دج 200.000 إلى دج 100.000 كل من يسلم أو يستلم بهدف الاستعمال غير المشروع البطاقة الالكترونية للمؤمن له اجتماعيا أو المفتاح الالكتروني لهيكل العلاج أو المفتاح الالكتروني لمهن الصحة ".

نصت المادة 93 مكرر3 على: أنه من يقوم عن طريق الغش بتعديل أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الالكترونية للمؤمن له اجتماعيا أو في المفتاح الالكتروني لهيكل العلاج أو في المفتاح الالكتروني لمهن الصحة وهي نفس العقوبة التي تطلق كذلك على كل من قام بتعديل أو نسخ وبطريقة غير مشروعة البرمجيات التي

[1] زبيحة زيدان ، **مرجع سابق الذكر** ، ص 77 ، 78.

تسمح بالوصول أو باستعمال المعطيات المدرجة في البطاقة الالكترونية للمؤمن له اجتماعيا أو في المفتاح الالكتروني لهيكل العلاج أو مهن الصحة.

قانون 09-04 مؤرخ في 14 شعبان 1430 الموافق 5 أوت 2009 للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[1] :

نصت المادة2 منه على مفهوم كل من: الجرائم المتصلة بتكنولوجيا الإعلام والاتصال . منظومة المعلوماتية، معطيات معلوماتية، مقدمو الخدمات، المعطيات المتعلقة بحركة السير، الاتصالات الإلكترونية.

نصت المادة 4 منه على: مراقبة الاتصالات الإلكترونية الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية .

نصت المادة 5 منه على: القواعد الإجرائية تفتيش المنظومات المعلوماتية.

نصت المادة 6 منه على: حجز المعطيات المعلوماتية.

المادة 7 نصت على: الحجز عن طريق منع الوصول إلى المعطيات

المادة 8 نصت على: المعطيات المحجوزة ذات المحتوى الإجرام.

المادة 9 نصت على: حدود استعمال المعطيات المتحصل عليها .

المادة 10 نصت على: التزامات مقدمي الخدمات مساعدة السلطات .

المادة 11 نصت على: حفظ المعطيات المتعلقة بحركة السير .

المادة 12نصت على: الالتزامات الخاصة بمقدمي خدمة الإنترنت.

المادة 13 و14 نصت على: إنشاء مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

[1] قانون 09 -04 ، **مرجع سابق الذكر**.

المطلب الثاني: الإرهاب الإلكتروني في الولايات المتحدة الأمريكية:

أولا: الإرهاب الإلكتروني:

يعد الإرهاب الإلكتروني مثله مثل أي اعتداء من قراصنة هدفهم التخريب أو السرقة للبيانات، ولكن الهدف الأساسي سياسي ويسعى الإضرار بالأمن القومي للدولة وليس الحصول على بعض المكاسب الشخصية بصورة غير شرعية أو مجرد جذب الانتباه.[1]

حيث يمكن استخدام الفضاء الالكتروني في العمليات الارهابية من خلال:

- التجنيد والتبعية والدعاية والإعلان وجمع التمويل.
- التواصل والتخطيط وإدارة الاجتماعات وجمع المعلومات وإرسالها.
- تقديم الوصفات الجاهزة لصناعة القنابل والمتفجرات.
- مهاجمة نظم التحكم في الطيران لإحداث تصادم سواء بالطائرات او قطارات السكك الحديدية.
- تعطيل البنوك وعمليات التحويل المالي.
- تعديل ضغط الغاز عن بعد لضغط أنابيب الغاز لتعطيلها.
- التلاعب في نظم السلامة للمصانع الكيماوية لإحداث أضرار كارثية بالمواطنين.
- التحكم في نظم المعلومات خاصة على الطرق السريعة والأنفاق الكبرى .
- السيطرة على شبكات الربط الكهربائي المتصلة بالانترنت عبر الأنظمة.

[1] إيهاب خليفة، **القوة الإلكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الإنترنت" الولايات المتحدة نموذجا"**، القاهرة: دار العربي للنشر والتوزيع، 2017، ص 118-119.

ثانيا: أبرز الأهداف الإلكترونية التي يتم استهدافها في الولايات المتحدة الأمريكية:

1. التهديدات الاقتصادية:

تعتبر الهجمات الإلكترونية ذات الطابع الاقتصادي من أخطر الهجمات التي تتعرض لها الولايات المتحدة الأمريكية وذلك لان النظم المالية والمصرفية والتجارية جميعها متصلة بالانترنت كما أن شركات التكنولوجيا العملاقة بما تحتويه أنظمتها الإلكترونية من براءة الاختراع وسرقة هذه المعلومات لصالح دول أو شركات منافسة في السوق الدولية.

وتعد الصين من أهم الدول التي قد تلحق بالولايات المتحدة الخسائر الاقتصادية بل والعسكرية ايضا عبر الفضاء الالكتروني سواء من خلال سرقة البيانات الاقتصادية أو الحقوق الملكية الفكرية وبراءة الاختراع حيث ان الاعتداءات المستمرة على شبكات المعلومات ومحاولة اختراق الأخرى لدى الحكومة الأمريكية خاصة بدولة مثل الصين وروسيا تجعل الولايات المتحدة الأمريكية عرضة لأي اختراق خارجي، ومن ثم تفقد ميزتها النسبية من خلال سرقة البيانات والمعلومات الاقتصادية والعسكرية.

2. التهديدات العسكرية:

وعلى الرغم من ان القوة الالكترونية لم ترتق لتتساوى مع القوة البحرية والجوية في حسم المعارك العسكرية فإن ميزتها تكمن في ربط الوحدات العسكرية بعضها ببعض بالأنظمة العسكرية الإلكترونية بما يسمح بسهولة تبادل المعلومات وتدفقها، وسرعة إعطاء الأوامر العسكرية والقدرة على إصابة الهدف وتدميره ، وقد تتحول هذه الميزة إلى نقطة ضعف ان لم تكن مؤمنة بشكل جيد من الاختراق الخارجي منعا للتجسس أو التلاعب بالبيانات أو تدميرها أو التلاعب بالأنظمة العسكرية وإعادة توجيه أسلحة الخصم وأهدافه إلى صديقه. [1]

وقد انطلقت في 2008 واحدة من أخطر الهجمات ضد أنظمة حواسيب الجيش الأمريكي من خلال وصلة USBبسيطة متصلة بكمبيوتر محمول تابع للجيش في قاعدة عسكرية موجودة

[1] "الحرب الإلكترونية أخطر تهديد إيراني"، موقع cnn ، تم الإطلاع عليه في 28-04-2019، على الرابط الإلكتروني: http://archive.arabic.cnn.com/2012/scitech/11/6/ iran-cyberattack/index.html

في الشرق الأوسط، ولم يتم اكتشاف برامج التجسس في كل الأنظمة الأمريكية السرية وغير السرية في الوقت المناسب، ومنذ ذلك الوقت أصبح التجسس الإلكتروني هاجسا يؤرق الدول وخاصة الولايات المتحدة الأمريكية.

وفي السياق ذاته يمكن القول انه إن لم تكن هذه الحوادث تحمل تهديد كافي فإن التطور النوعي والكمي في القدرات المدمرة للحرب الإلكترونية فعلى سبيل المثال أدى **فيروس ستاكنست** إلى تحول من إصابة البعد المعلوماتي إلى إصابة البعد المادي حيث اعلنت الاستخبارات الإيرانية أن هذا الفيروس قد أصاب ما يقدر ب 16 الف كمبيوتر وتسبب في تدمير آلاف أجهزة الطرد المركزي بالبرنامج النووي الإيراني.[1]

3. تهديد البنى التحتية:

تعتبر من بين أكبر الاهداف التي تهدد الأمن الإلكتروني التي يترتب عليها خسائر فادحة لأنها تلا تقتصر على الاستخدامات المدنية فقط بل تتعداها إلى تهديد مختلف المصالح الحيوية للدولة.

ويمكن تعريف البنية التحتية الحرجة للولايات المتحدة بأنها عبارة عن النظم والأصول سواء كانت مادية أو افتراضية والتي يتسبب تدميرها إلى تهديد للأمن القومي الأمريكي أو الاقتصادي أو الرعاية الصحية أو الأمن العام.[2]

كما تقوم الشركات الكبرى والمؤسسات التي تخدم الجمهور بحفظ قواعد البيانات الخاصة بالمواطنين على أجهزة كمبيوتر الخوادم وتتم عملية الربط بينهم عبر شبكات الإنترنت وهو ما يعرضها لخطر القرصنة وسرقة المعلومات والتلاعب بها خاصة إذا كان الأمر يتعلق بالمسائل المالية والحسابات البنكية.

---

[1] التهديدات الجديدة: الأبعاد الإلكترونية، **مجلة حلف الناتو**، تم الإطلاع عليه في 28-04-2019، على الرابط الإلكتروني: https://www.nato.int/docu/review/2011/11-september/Cyber-Threads/AR/index.htm

[2] Critical infrastructure, **Threats and Terrorism**, 2006,p 01.

4. التلاعب بالبيانات الشخصية وتهديد أمن المواطنين:

نتيجة لسهولة ورخص الدخول إلى الفضاء الإلكتروني وإمكانية الدخول عليه من مختلف الوسائل التكنولوجية بداية من الجهاز الإلكتروني إلى غاية الهاتف المحمول واللوحات الإلكترونية نهاية بالخوادم اللاسلكية التي تعتمد على شبكات التلفون المحمول، فإن جميع الأفراد أصبحوا عرضة للهجمات الإلكترونية والتلاعب ببياناتهم الشخصية وسرقتها وانتحال شخصياتهم.

ثالثا: الخطط والاستراتيجيات الأمريكية لتحقيق الأمن الإلكتروني: [1] ولمواجهة هذه المخاطر قامت الولايات المتحدة الأمريكية بوضع العديد من الخطط والإستراتيجيات تسعى إلى تحقيق الأمن الإلكتروني من خلال التالي:

- التحرك نحو إدارة شبكة فدرالية واحدة.
- نشر أنظمة التحري والكشف عن الهوية.
- تطوير ونشر أدوات منع الاختراق.
- إعادة توجيه مجالات البحوث وإعادة النظر في تمويلها.
- الربط الشبكي لمراكز العمليات الإلكترونية للحكومة الاتحادية.
- تطوير خطة حكومية قائمة على مخابرات إلكترونية واسعة.
- زيادة أمن شبكة السرية.
- توسيع نطاق التعليم الالكتروني .
- تحديد التكنولوجيات المستقبلية التي تجعل الولايات المتحدة متقدمة عن غيرها.
- تحديد الأدوات ذات الردع الإلكتروني.
- وضع مناهج متعددة الجوانب لزيادة كفاءة عملية إدارة المخاطر.

[1] الإستخبارت الأمريكية تخشى وجود إدوارد سنودن آخر في صفوفها، **موقع جريدة التحرير**، تم التصفح في 04-03-2019، على الرابط الإلكتروني": http://www.altahrironline.com/ara

- تحديد الأمن الإلكتروني في مجلات القطاع الخاص.

رابعا: تسريب البيانات المتعلقة بالأمن القومي الإلكتروني:

يعد تسريب البيانات أحد التهديدات الرئيسية التي تواجه الأمن القومي الأمريكي، خاصة البيانات الخاصة للأمن القومي الأمريكي والتي تتعلق بالخطط التجارية والإستراتيجيات الاقتصادية وخطط التسلح والتطوير العسكري، وحقوق الملكية الفكرية وبراءات الاختراع، فضلا عن المراسلات السرية بين الحكومة الأمريكية وموظفيها وعملائها داخل وخارج الولايات المتحدة، ولعل أبرز الأمثلة على ذلك هو قيام **إدوارد سنودن** الموظف السابق في وكالة الاستخبارات الأمريكية المتعاقد مع وكالة الأمن اقومي الأمريكي بعدما اتجه للقطاع الخاص وهو ما يجعل الحفاظ على سرية البيانات، خاصة المتعلقة بالأمن القومي الأمريكي تحدي رئيسي للحكومات الأمريكية، ومصدر تهديد إلكتروني.[1]

المطلب الثالث: القرصنة الإلكترونية في روسيا:

في يناير (كانون الثاني) عام 2017، أصدر مكتب مدير الاستخبارات الوطنية الأميركي (الذي يضم 17 وكالة ومنظمة من بينهما وكالة الاستخبارات المركزية ومكتب التحقيقات الفيدرالية ووكالة الأمن الوطني) تقريرا لتوضيح الحملة الروسية التي استهدفت التأثير على الانتخابات الرئاسية الأميركية. ووفقا لما ورد في التقرير، تعتقد وكالات الاستخبارات الأميركية أن الرئيس الروسي فلاديمير "بوتين" في الواقع أصدر أوامره بالسعي إلى التأثير على الانتخابات الرئاسية الأميركية لعام 2016 [2].

كانت أهداف روسيا إضعاف ثقة الشعب في العملية الديمقراطية الأميركية وتشويه صورة الوزيرة كلينتون والإضرار بترشحها وفرصها في الفوز بالرئاسة. ونقرر أيضا أن "بوتين"

[1] ثائر خليل حمد ، **الأمن القومي الأمريكي و التغيير في المنطقة العربية** ، ط1 ، دار الحامد للنشر و التوزيع ، 2016 ، 135 .

[2] الإستخبارت الأمريكية تخشى وجود إدوارد سنودن آخر في صفوفها ،**مرجع سابق الذكر**.

والحكومة الروسية كشفا عن تفضيل واضح للرئيس المنتخب "ترمب"... وجاءت حملة التأثير التي شنتها موسكو بعد استراتيجية روسية لإرسال الرسائل تجمع بين عمليات استخباراتية سرية – مثل النشاط الإلكتروني – والمساعي المعلنة التي تبذلها الأجهزة الحكومية الروسية ووسائل الإعلام التي تمولها الدولة ووسطاء من دول أخرى ومستخدمي وسائل التواصل الاجتماعي و دافعي الأجر أو متصيدي الإنترنت .أصابت تلك الأنباء كثيرا من الأميركيين بالصدمة. ومما أثار القلق بوجه خاص أن القراصنة الروس سربوا معلومات سرية خاصة "بهيلاري كلينتون" والحزب الديمقراطي إلى موقع «ويكيليكس». لم تكن الولايات المتحدة هدفا لمثل هذا التدخل الروسي السافر من قبل، ولكن هذا النوع من السلوك ليس غريبا على روسيا. على أي حال حاولت الحكومة الروسية بالفعل شن حرب إلكترونية ونجحت في ذلك.

1. الهجمات الإلكترونية على أستونيا عام 2007" الحرب الإلكترونية الأولى":

قبل بدء السباق الرئاسي الأميركي بتسعة أعوام، كانت روسيا متورطة في فضيحة أخرى كبيرة تتعلق بأستونيا. تعد أستونيا، الدولة الأوروبية الصغيرة، التي كانت جزءا من الاتحاد السوفياتي سابقا وأصبحت في الوقت الحالي عضوا في كل من الاتحاد الأوروبي وحلف الناتو، أحد مؤيدي الحوكمة الإلكترونية. وفقا لخطة «أستونيا الإلكترونية»، تحولت الدولة إلى «مجتمع إلكتروني» بمعنى أن جميع أعمال الحكومة والبنوك تتم دون إجراءات ورقية. وحتى التصويت في الانتخابات يتم عبر الإنترنت.[1]

وكانت الدولة التي يبلغ تعدادها 1.3 مليون نسمة أول بلد يجعل الاتصال بالإنترنت حقا إنسانيا. وفي عام 2016، كانت 99.6 في المائة من التعاملات تتم عن طريق خدمات مصرفية إلكترونية، وأعلن 96 في المائة من السكان عن دخلهم إلكترونيا، ولكن أدت طموحات أستونيا بإحداث ثورة في الحوكمة الإلكترونية إلى تعرُّض البلاد إلى مخاطر غير مسبوقة. في عام 2007، في جزء من محاولاتها للتخلي عن إرثها من الاتحاد الأوروبي، قررت الحكومة

[1] **مرجع سابق الذكر.**

نقل نصب تذكاري من الحرب السوفياتية من وسط مدينة تالين. ثار الغضب الروسي وانهالت تهديدات بفرض العقوبات عقب تلك الخطوة. واعتدى مشاغبون على السفير الأستوني في موسكو، وسريعا ما أصيبت مواقع الأجهزة الحكومية الأستونية والصحف والبنوك في البلاد بالتعطل. استمرت الهجمات الإلكترونية لمدة ثلاثة أسابيع، وكانت تأتي على دفعات لتصيب أستونيا بشلل فعلي. أرسل مخترقو الإنترنت كميات كبيرة من المعلومات إلى المواقع الإلكترونية المستهدفة في وقت واحد، مما أدى إلى زيادة الأحمال عليها وتوقفها في النهاية. ووردت تقارير بأن قراصنة الإنترنت اخترقوا ما يصل إلى ربع أجهزة الكومبيوتر في العالم (حيث حولوها إلى أجهزة زومبي)، واستعانوا بروبوت برمجي لإغراق المواقع الأستونية بمعلومات وهمية عن وقوع هجوم حجب الخدمة (وهو هجوم يستهدف وقف خدمة إلكترونية ما بإغراقها بسيل من المعلومات من مصادر متعددة). بالإضافة إلى ذلك، انضم إلى القراصنة أشخاص عاديون حصلوا على تعليمات من مواقع روسية بشأن كيفية شن هجوم حجب الخدمة. وتم اختراق بعض المواقع وإعادة توجيه مستخدميها إلى صور لجنود سوفيات ومقولات لمارتن لوثر كينغ عن مقاومة «الشر». تزامن مع تلك الهجمات نشر معلومات خاطئة، حيث نشرت مواقع إلكترونية أخرى مخترقة أخبارا كاذبة بأن الحكومة الأستونية طلبت العفو من روسيا ووعدتها بإعادة النصب التذكاري إلى موقعه الأصلي.[1]

شبهت حكومة أستونيا هذه الهجمات الإلكترونية التي استغرقت ثلاثة أسابيع بالأعمال الإرهابية. وكانت تلك العمليات أولى حالات «الحرب الإلكترونية» وكان ذلك المصطلح حديثا في عام 2007، كما كان الحال مع «الإرهاب الإلكتروني». وفي حين استطاع مسؤولون أستونيون تعقب بعض عناوين الآي بي الأصلية الخاصة بالمخترقين وصولا إلى الحكومة الروسية والإدارة الرئاسية، فإنهم واجهوا صعوبة في إثبات تنفيذ الحكومة الروسية لتلك الهجمات. ومع ذلك تقدمت أستونيا بطلب رسمي إلى الناتو لتفعيل المادة الخامسة التي تلزم الحلف بالرد على أي هجمات تستهدف أيا من الدول الأعضاء. وكشف ذلك الحادث عن نقاط

[1] ثائر خليل حمد، **مرجع سابق الذكر**، ص139 .

ضعف مهمة في النظام الذي يقوم على القواعد الدولية. لقد اتضح أن تلك القواعد ليست مصممة على نحو يتناسب مع تحديات القرن الحادي والعشرين، مثل الحرب الإلكترونية. وكان إخفاء الهوية في هذا النوع من الإرهاب الإلكتروني مناسبا للمسؤولين الروس الذين نفوا تورطهم به[1].

في عام 2007، كتبت **آن أبلباوم Anne Applebaum** أن «الهجمات كانت اختباراً روسياً لاستعداد الغرب للحرب الإلكترونية في العموم، ولالتزام الناتو تجاه أحدث وأضعف أعضائه بوجه خاص». في ذلك الحين، أخفق الغرب في الاختبار، حيث استطاعت روسيا الخروج من المأزق في النهاية بلا مساس. وكانت صلاحية المادتين الرابعة والخامسة من حلف الناتو غير واضحة بما يكفي لاتخاذ رد فعل ممكن تجاه هذا النوع من المواقف.

ومع ذلك، تلقى المجتمع الدولي بعض الدروس المستفادة من «الحرب الإلكترونية الأولى» في أستونيا. في قمة بوخارست التي عقدها الناتو في عام 2008، أنشأ الحلف مركز تميز الدفاع الإلكتروني التعاوني في تالين بأستونيا. وأنشأ أيضا سلطة جديدة لإدارة الدفاع الإلكتروني في بروكسل. وعلى مدار الأعوام التالية، تأثر عمل الناتو نحو تحسين الأمن الإلكتروني للدول الأعضاء بتجربة أستونيا. سمح ذلك لأستونيا بمواصلة التحول الرقمي لحكومتها ومجتمعها دون حدوث اضطرابات أخرى. وتعد الدولة حاليا من أبرز أعضاء الناتو في مجال الحوكمة الإلكترونية والأمن الإلكتروني.[2]

[1] مؤتمر ميونيخ يناقش جدوى الجيوش الإلكترونية، تم التصفح: 24-04-2019، على الرابط: https://arabic.euronews.com/2018/02/16/eu-munich-robot-soldiers،

[2] الإستخبارت الأمريكية تخشى وجود إدوارد سنودن آخر في صفوفها ، **مرجع سابق الذكر.**

2. هل تقوم حرب إلكترونية ثانية؟:

إذا ما نظرنا إلى التهديدات الإلكترونية الروسية المستمرة، تظل أصداء تحذير أبلباوم في عام 2007 تتردد حتى اليوم: «(ولكن) هذا ما ينتهي إليه الأمر – حتى يعود من أجبر الحكومة الأستونية على الخروج من الفضاء الإلكتروني إلى الشبكة مرة أخرى بعتاد أفضل من أجل المعركة القادمة.

بالفعل جاءت روسيا بعتاد واستعداد أفضل هذه المرة. تحولت صيغة «الحرب الإلكترونية» السابقة إلى أسلوب «حرب هجينة» أكثر تعقيدا للتأثير في الغرب. وكان أول تدخل روسي معلن على نطاق واسع في صورة الـ«بريكست». هنا تم توجيه الدعاية الروسية، التي بدأت في مطلع عام 2015، نحو التحريض على كراهية المهاجرين والخوف من الإرهاب – وهي المشاعر التي أدت في النهاية دورا حاسما في التصويت بالخروج من الاتحاد الأوروبي[1] .

في مقال نشر مؤخرا، وثَّق **كلينت واتس Wats Client** و**أندرو ويسبيرد Andro Wisbard** الخطوات التي كان على روسيا اتخاذها للتلاعب في الانتخابات الأميركية دون تزوير مباشر للأصوات.

في الولايات المتحدة استخدمت حسابات روسية شبه معلنة وأخرى خفية على مواقع التواصل الاجتماعي وعبارات منتشرة لإظهار ما يبدو أنهم مؤيدو ترمب المحافظون أو مشجعون يمينيون متطرفون. تلك الشخصيات على وسائل التواصل الاجتماعي، والتي تمتلئ تعريفاتهم الشخصية بكلمات مثل (الدولة)، (المسيحية)، (أميركا)، (الجيش)، ثم يدفعون به إشاعات مؤيدة لترمب مع أخبار كاذبة وملتوية إلى الجمهور الأميركي، مما ساعد على إحداث حالة من التأييد لترمب والتشكيك في الحكومة الأميركية.« يوضح **واتس** و**ويسبيرد** أيضا كيف ساعدت روسيا مؤيدي **بريكست:**"رصدت المملكة المتحدة

[1] مؤتمر ميونيخ يناقش جدوى الجيوش الإلكترونية، **مرجع سابق الذكر**.

أيضا حملة مشابهة. منذ بدايات عام 2015، حرضت وسائل الإعلام الروسية على الخوف من المهاجرين وروجت للاتهامات التي أطلقها **نايغل فاراج Nigel Farage** المؤيد **للبريكست** عن الاستغلال الأميركي لتغذية التأييد الشعبي لخروج بريطانيا من الاتحاد الأوروبي".[1]

نشر و**يسبيرد** و **واتس** تقريرا شاملا يبحث في ممارسات تصيد الإنترنت (التروليغ) في الغرب. بعد أن أمضى الفريق 30 شهرا في متابعة عن قرب لعمليات التأثير الروسية عبر الإنترنت، ومراقبة نحو 7 آلاف حساب، تبعث رسالة الفريق الأساسية على الخوف: «ترمب ليس نهاية الحرب المعلوماتية الروسية ضد أميركا. إنه مجرد بداية.[2]

بعد اتضاح مسألة الانتخابات الرئاسية الأميركية، لم يعد هدف روسيا تعطيل المواقع الإلكترونية أو إصابة الحكومات والبنوك بالشلل كما فعلت أثناء تجربتها في أستونيا. إن الضرر الأكبر حاليا يتم عبر الحروب المعلوماتية. يُمكِّن اختراق قواعد البيانات وتسريب الوثائق السرية حكومة بوتين من استغلال آراء الناس وأفعالهم في دول أخرى. كذلك ساعدت مميزات مواقع التواصل الاجتماعي روسيا على الترويج للأفكار التي تخدم مصالحها. لا يوجد دليل حقيقي يمكنه إثبات ذلك دون إجراء تحقيقات شاملة وباهظة مثل تلك التي أجراها واتس وفريقه. وحتى مع هذا، لم توضع القوانين الدولية لمعاقبة مثل ذلك السلوك.لا يعد إنشاء حسابات مزيفة على «تويتر» ونشر أخبار كاذبة على مواقع التواصل الاجتماعي مخالفا للقانون.

لحسن الحظ أن تجربة أستونيا سمحت للمجتمع الدولي بتطوير إمكانات قوية لتعقب المتصيدين وتحديد هوية المخترقين. عقب جمع أدلة كافية لإثبات مسؤولية روسيا عن عمليات اختراق ضد اللجنة الوطنية للحزب الديمقراطي، أصدر أوباما عقوبات ضد مسؤولين استخباراتيين روس،

[1] **مرجع سابق الذكر.**

[2] الإستخبارت الأمريكية تخشى وجود إدوارد سنودن آخر في صفوفها ، **مرجع سابق الذكر.**

وطرد 35 دبلوماسيا روسيا للاشتباه في قيامهم بالتجسس، وأغلق منشأتين روسيتين في الولايات المتحدة.[1]

3. التقدم للأمام:

في خطاب ألقته **سامانثا باور Samantha Power**، مندوبة الولايات المتحدة الدائمة في الأمم المتحدة، في 17 يناير (كانون الثاني)، شجعت الأميركيين على «مكافحة المعلومات المغلوطة بالمعلومات؛ والخيال بالحقيقة». تعلم الغرب من تجربة أستونيا كيفية التعامل مع حالات الهجمات الإلكترونية. ولكن في الوقت الحالي، أصبحت تكتيكات الحرب الإلكترونية الروسية تحتوي على عنصر دعائي، والذي لم تتم مواجهته على نحو مناسب حتى اللحظة الراهنة. ذكَّرت السفيرة باور الأميركيين بأن الحكومة الروسية أنفقت ما يصل إلى مليار دولار في العام على أدوات دعائية مثل قناة «آر تي» التلفزيونية. وسوف يكون على البلدان الغربية إنشاء استثمارات مالية كبيرة ضمن جهودهم للدعاية المضادة للحاق بآلة الدعاية الروسية المُطوّرة

. ذكر تقرير وكالة الاستخبارات الوطنية الصادر في يناير (كانون الثاني) 2017 أن «موسكو سوف تطبق دروسا مستفادة من حملتها التي أمر بها بوتين والتي استهدفت الانتخابات الرئاسية الأميركية على محاولات التأثير المستقبلية في جميع أنحاء العالم، بمن فيه ذلك حلفاء أميركا وعملياتهم الانتخابية». من حلفاء أميركا الذين سيتم استهداف عملياتهم الانتخابية في الفترة المقبلة فرنسا وألمانيا وهولندا وغيرها. من المقرر أن تجري الدول الثلاث انتخاباتها الوطنية في 2017، وفي ثلاثتها وردت تقارير عن تمويل روسي للأحزاب القومية اليمينية المتطرفة، بالإضافة إلى الدعاية الإعلامية الروسية. وهكذا تسنح الفرصة أمام الغرب لكي يتعلم ويثبت استفادته من التجارب المؤلمة التي وقعت في عام 2016.[2]

[1] مؤتمر ميونيخ يناقش جدوى الجيوش الإلكترونية، **مرجع سابق الذكر.**
[2] الإستخبارت الأمريكية تخشى وجود إدوارد سنودن آخر في صفوفها ، **مرجع سابق الذكر.**

المطلب الرابع: الشباب العربي الإسلامي و الحرب الإلكترونية على الاحتلال الإسرائيلي:

أضرت الحرب الإلكترونية التي شنها الشباب العربي والإسلامي بإسرائيل، فعدا عن النجاحات الإلكترونية التي حققها الشارع العربي والإسلامي في الفضاء الإلكتروني، وانتصاره على إسرائيل افتراضياً ورقمياً؛ إلا أن هناك تأثيراتٍ أخرى لحقت بإسرائيل، خاصةً في قطاعاتها الاقتصادية، والاجتماعية والنفسية، والسياسية والإعلامية أيضاً.

أولا: التأثيرات الاقتصادية للحرب الإلكترونية على الاحتلال الإسرائيلي:

منذ أن قامت إسرائيل بحوسبة قطاعاتها المختلفة، وربطت اقتصادها بالتطورات التّقنية والرقمية، واتصاله بشكلٍ مباشرٍ بالشبكات الإلكترونية، ووسائل الاتصالات الحديثة، كالحواسيب، والانترنت، والأجهزة الذكية وغيرها؛ أصبحت الحياة الاقتصادية والاجتماعية الإسرائيلية مرتبطةً بشبكات الاتصال بشكلٍ وثيق ، كمواقع البورصة، وبطاقات الائتمان، وبيانات الأفراد والبنوك، وغيرها من المرافق الاقتصادية الأخرى، الأمر الذي جعلها هدفاً رئيسياً، وصيداً مستهدفاً لعمليات القرصنة الإلكترونية على الفضاء الإلكتروني الإسرائيلي . تُعتبر المواقع الإلكترونية الاقتصادية الإسرائيلية أكثر القطاعات استهدافاً من قبل الشباب العربي الإسلامي . فمثلاً تعرضت كُبريات المواقع الاقتصادية في إسرائيل للاختراق الإلكتروني مراراً وتكراراً، كمواقع البورصة الإسرائيلية، وضرب خوادم إلكترونية حساسة لاثنين من أهم واكبر البنوك الإسرائيلية، وهما **بنك مسيد (Bank Msid)** ، و **بنك أوتسير هاحيال Bank Otser Hahial**، مما يعني أن القطاع الاقتصادي الإسرائيلي معرض للهجات الإلكترونية، الأمر الذي قد يكلف إسرائيل بعضاً من الغرامات المالية والاقتصادية والأمنية في عالم الاتصالات وتكنولوجيات المعلومات.[1]

[1] يحي دبوق،"الحرب الالكترونية تستعر ضد اسرائيل...و تضرب الاقتصاد"، تم التصفح في 15-04-2019 ، على الرابط: http://al-akhbae.com/Palestine/63832 .

ثانيا: التأثيرات النفسية للحرب الإلكترونية على الاحتلال الإسرائيلي:

ما إن اشتدت الهجمات الإلكترونية على الساحة الإسرائيلية، حتى انتشر الذعر والهلع بين الإسرائيليين، والتأكد فعلياً من نجاح الشباب العربي والإسلامي في اختراق كُبريات المواقع الإلكترونية الحساسية في إسرائيل، خاصة الاقتصادية والأمنية منها. فمثلاً، تلقت غُرفة الطوارئ في البنك المركزي الإسرائيلي عشرات الآلاف من المكالمات من الإسرائيليين الذين اكتشفوا أن حساباتهم البنكية قد تعطلت، خاصةً أن بعض هذه الحسابات البنكية المهددة بالاختراق تُقدر بمبالغ مالية كبيرة، الأمر الذي دفع البنوك والشركات الإسرائيلية إلى توقيف عمل هذه البطاقات، مما أدى إلى انتشار حالة من الذعر الاجتماعي والنفسي بين جموع الإسرائيليين.

ومما لا شك فيه ، أن لإسرائيل تجارب في مجال الحروب النفسية الإلكترونية، فهي دائمة البحث عن مصطلحاتٍ للدعاية وبث المعلومات والأفكار عبر وسائلها الإلكترونية والمعلوماتية والإعلامية لتدعيم مواقفها، وإثبات مصداقية روايتها. فمثلا، تستخدم إسرائيل ما يعرف بالدعاية السوداء(**Black Propaganda**)، والتي تهدف من خلالها إلى نشر أكبر قدرٍ ممكنٍ من المعلومات المضللة، والهادفة إلى إرباك صفوف المقاومين، وذلك لاقتناص الفرص والمعلومات التي تُفيد إسرائيل في الكشف عن فحوى بنوك الأهداف المعلوماتية التي بحوزة خُصومها.[1]

ثالثا: التأثيرات الأمنية والسياسية للحرب الإلكترونية على الاحتلال الإسرائيلي:

يعتبر الأمن بالنسبة لإسرائيل محور وجودها، وتُسخر من أجله المال والوقت والجهد ، مجرد المساس به يعني لإسرائيل إعلان حرب، إذ تنظر الأخيرة للحروب الإلكترونية الموجهة صوبها بأنها بمثابة حربٍ عليها، وهذا ما ظهر جلياً في تهديدات نائب وزير الخارجية الإسرائيلية "داني ايالون"، بأن المساس بسيادة الفضاء الإلكتروني الإسرائيلي هو جزء من المساس بأمنها، وأنه من يتجرأ بفعل ذلك سيعرض نفسه لضربةٍ صاروخية .

[1] http://www.asharqalarabi.org.uk-/mu-sa2/b-mishacat-5352.htm .

تُشكل الحرب الإلكترونية تحدياً أمنياً جديداً لإسرائيل، فنجاح مثل هذه الهجمات يعني الطعن بنظريتها الأمنية، وبالتالي التشكيك بالقادة السياسيين والأمنيين الإسرائيليين الذين أعلنوا مراراً وتكراراً أن إسرائيل تمتلك قُدرةً دفاعيةً في كافة المجالات ، و أنه من الصعوبة المساس بها. فعلى الصعيد الإلكتروني مثلاً، أشار **عاموس يادلين Amos Yadlin** محاضرة له بِـ (معهد أبحاث الأمن القومي الإسرائيلي)،أن إسرائيل تواجه خطراً أمنياً و معلوماتياً يكمن في احتمالية اختراق مواقع وحواسيب الدولة الحساسة . لكن في المقابل، أكد يادلين أن هيئة السايبر في الجيش الإسرائيلي **Cyber Authority In The Israeli army** تمتلك القُدرات اللازمة لردع أي هجومٍ إلكتروني، إضافةً إلى مقدرة الهيئة على تنفيذ هجماتٍ إلكترونيةٍ على أهدافٍ معادية لإسرائيل. كما وصنف الجيش الإسرائيلي الحرب الإلكترونية كساحةٍ خامسةٍ للقتال تُضاف إلى الساحة البرية والبحرية والجوية والفضائية ، في صورةٍ تُشير إلى القلق الأمني الذي تُعانيه إسرائيل جراء هذه الهجمات.

سياسياً، وضعت هذه الهجمات الإلكترونية الساسة والقادة الإسرائيليين في موضعٍ صعب، فقد أُتهم القادة الإسرائيليون بأنهم يبالغون في وصف القدرة الإسرائيلية، وأنهم غير قادرين على حماية المواطن الإسرائيلي، وأنهم يعبثون بمشاعر المجتمع الإسرائيلي . إضافةً إلى اتهاماتٍ تمثلت بالتقصير في توظيف التّقنية الحديثة في منظومة الدفاع الإسرائيلي، الأمر الذي أدى إلى تبادل الاتهامات بين الساسة والقادة الإسرائيليين. ومثال ذلك ، ما حدث لوزير الدفاع الإسرائيلي السابق **أيهود باراك Barak Ehud** ، ووضعه أمام الكثير من التساؤلات عن مدى مقدرة المنظومة الدفاعية الإسرائيلية الإلكترونية في حماية إسرائيل الأمر الذي دفعه لتوجيه ميزانياتٍ لا بأس بها، وتجنيد أشخاصٍ قادرين على قيادة وإدارة الحروب الإلكترونية.[1]

[1] وليد غسان سعيد جعلود، **مرجع سابق الذكر**، ص 240.

خلاصة الفصل

في نهاية الفصل الثاني، نخلص إلى ان التطور الهائل لوسائل تكنولوجيا الاتصالات والمعلومات غير أنماطا كثيرة في الحياة البشرية، كان لها وقع كبير على سلوكيات المجتمع وهويته وانتشار آليات التشابك تجمع بين المجموعات البشرية متمثلة في مواقع التواصل الاجتماعي، والتي اصبحت من بين أهم الوسائل نظرا لسرعة وسهولة استخدامها، وبغض النظر عن ما تخلفه من تهديدات ومخاطر على الأمن المجتمعي.

فتزايدت العلاقة بين الأمن الإلكتروني والأمن الإلكتروني ومعها تزايدت إمكانية تعرض المصالح الإستراتيجية للدول، فقد ساهمت هذه التكنولوجيا في افراز العديد من التهديدات الإلكترونية، فأصبحنا أمام جرائم إلكترونية حقيقة عابرة للحدود القومية، أثرت على الأمن القومي للدول، وعلى قضايا السيادة الدولية.

ومن بين تلك التهديدات نذكر الجريمة الإلكترونية في التشريع الجزائري، الإرهاب الإلكتروني في الولايات المتحدة الأمريكية، القرصنة الإلكترونية في روسيا، الشباب العربي الإسلامي والحرب الإلكترونية على إسرائيل.

الخاتمة

كان الأمن ولا يزال الهدف الرئيسي للدول، وذلك بعد تشكل الدولة القومية وارتباطه بالمصلحة الوطنية، والتي تستخدم كأداة تحليلية لوصف وشرح وتقويم مصادر السياسة الخارجية للدولة، فمسألة ضبط تعريف للأمن لا يعد أمرا هينا، وذلك لأنه يفتقر لضبط معرفي، فاختلفت تعاريفه، وتعددت خصائصه وسماته وتمثلت في التركيب، الشمول، الثبات التنوع، واختلفت مجموعة محدداته بين البيئة الداخلية والبيئة الخارجية، كما وقد تنوعت أيضا مستوياته وتمثلت في: أمن الفرد، الأمن القومي الأمن الإقليمي، الأمن العالمي و الأمن الإنساني، أما الأبعاد فقد اختلفت بين العسكري، السياسي، الاقتصادي، الاجتماعي، والثقافي.

وعلى هذا الأساس ظهرت اتجاهات نظرية للدراسات الأمنية والمتمثلة في الاتجاه التقليدي الذي يهدف إلى حماية مصالح الدولة من التهديدات الخارجية باستخدام القوة العسكرية، والاتجاه المعاصر الذي ارتبط فيه مفهوم الأمن بالتطورات والتغيرات التي مست شكل وجوهر النظام الدولي والإفرازات التي نتجت عنه .

ومع هذه التصنيفات ظهرت أيضا نوعية جديدة من التهديدات الأمنية التي لم تكن معروفة من قبل، والمتمثلة في التهديدات الإلكترونية والتي تعتبر تهديدات خطيرة جدا غير ظاهرة وغير ملموسة وتنوعت هذه التهديدات مع تسارع درجة تطور وسائل تكنولوجيا الاتصالات والمعلومات فتعددت أشكال هذه التهديدات و تبايانت مستوياتها، وتمثلت في القرصنة الإلكترونية، وتقع في المستوى الأول من الهجوم ومن أمثلتها القيام بعمليات قرصنة المواقع الإلكترونية أو بتعطيل الحواسيب الخادمة من خلال إغراقها بالبيانات، الجريمة الإلكترونية والتجسس الإلكتروني يقعان في المستوى الثاني والثالث وغالبا ما يستهدفان الشركات والمؤسسات وفي حالات نادرة بعض المؤسسات، الإرهاب الإلكتروني ويقع في المستوى الرابع ويعبر عن الهجمات غير الشرعية والتي ينفذها فاعلون غير حكوميين ضد أجهزة الكمبيوتر والشبكات والمعلومات المخزنة، الحرب الإلكترونية وهي المستوى الأخطر للنزاع في الفضاء الإلكتروني وتهدف إلى التأثير على إرادة سياسية للطرف المستهدف وقدرته في عملية صنع القرارات وكذلك التأثير فيما يتعلق بالقيادة العسكرية التي توجهها المدنيين في مسرح العمليات الإلكترونية.

كما وقد شملت هذه التهديدات جميع المجالات مؤثرة بذلك على الأمن القومي للدول، فأصبحنا أمام جرائم إلكترونية حقيقية عابرة للحدود الدولية ومؤثرة على سيادتها واستقرارها؛ ومن أمثلة هاته الجرائم الجريمة الإلكترونية في التشريع الجزائري، الإرهاب الالكتروني في الولايات المتحدة الأمريكية، القرصنة الإلكترونية في روسيا، الشباب العربي الإسلامي والحرب الالكترونية على إسرائيل.

ومع التطور الهائل لهذه التكنولوجيا انتشرت آليات ووسائل جمعت المجموعات البشرية، تمثلت في مواقع التواصل الاجتماعي، وبغض النظر عن سهولة استعمالها وبساطتها إلا أنها خلفت مخاطر عديدة على الأمن المجتمعي والأمن القومي للدول.

وهكذا أصبح الأمن الإلكتروني إحدى أعلى أولويات الأمن القومي وأصبح من الواجب على الدول وضع إستراتيجيات وآليات لمواجهتها والقضاء عليها، والعمل مع بقية دول العالم من أجل تشارك قيم الأمن والاستقرار، ومن أجل فضاء إلكتروني آمن يعزز أمن الدول وتقدمها وازدهارها في جميع المجالات.

النتائج والتوصيات:

أولا: النتائج:

- في عصرنا الحالي، أصبح أمن الإلكتروني، إحدى أعلى أولويات الأمن القومي
- أصبح الفضاء الإلكتروني مجالا جديدا للتفاعلات الدولية، فانتشرت القوة الإلكترونية بينهم.
- تتميز التهديدات الإلكترونية بالتنوع، والشدة، والغموض، وتزداد كلما تسارعت وتطورت وسائل تكنولوجيا الاتصالات و المعلومات.
- تعتبر التهديدات الإلكترونية تهديدات خطيرة جدا تهدد الأمن القومي للدول، وتمس قضايا السيادة الدولية، وهي بذلك تهديدات عابرة للحدود الدولية القومية.

- تقوم الدول بوضع آليات و إستراتيجيات مختلفة الوطنية منها والدولية، وذلك من أجل مواجهة التهديدات الإلكترونية والقضاء عليها، وتحقيق أمنها القومي واستقرارها.
- تطورت التهديدات الإلكترونية وتنوعت أشكالها وتعددت آثارها و إنعكاستها لتشمل جميع المجالات، وعليه أصبحنا أمام جرائم حقيقية مست الأمن القومي للدول وأثرت عليه، ومن أمثلة تلك الجرائم، الجريمة الإلكترونية في التشريع الجزائري، الإرهاب الإلكتروني في الولايات المتحدة الأمريكية، القرصنة الإلكترونية في روسيا، الشباب العربي الإسلامي والحرب الإلكترونية على إسرائيل.

ثانيا: التوصيات:

- يرتبط الأمن الإلكتروني بقضايا التنمية السياسية، الاجتماعية،والاقتصادية فهو إحدى أهم عناصر الأمن القومي، يتأثر ويؤثر فيه.
- ضرورة وضع آليات وإستراتيجيات لمواجهة التهديدات الإلكترونية، وذلك بالتعاون الوطني والدولي من أجل تحقيق الأمن والاستقرار الدولي.
- وضع قواعد لترسيخ السلوك الجيد ونشر قيم وثقافة الفضاء الإلكتروني السلمي و الآمن.

قائمة المصادر

و المراجع

أولا : قائمة المصادر

1- **القرآن الكريم**.

2- القواميس:

- الرازي، محمد بن أبي بكر عبد القادر ، **قاموس مفتاح الصحاح**، القاهرة: مطبعة البابي الحلبي، 1990.

ثانيا: قائمة المراجع:

1- **باللغة العربية:**

أ- الكتب:

1- أية جودة، إلياس ، **الأمن البشري وسيادة الدول**، بيروت: مجد المؤسسات الجامعية للدراسات والنشر والتوزيع، 2008.

2- البداينة،ذياب موسى ، **5الأمن وحرب المعلومات**،ط01، عمان: دار الشروق للنشر والتوزيع، 2006.

3- //،// ، **الأمن الوطني في عصر العولمة**، الرياض: مؤسسات شباب الجامعة، 2009.

4- الجابري، محمد عابد، **قضايا الفكر المعاصر: العولمة- صراع الحضارات- العودة إلى الأخلاق - التسامح - الديمقراطية ونظام القيم- الفلسفة والمدنية**، بيروت: مركز دراسات الوحدة العربية، 1997.

5- الحسيني، عمار عباس ، **جرائم الحاسوب والانترنت: الجرائم المعلوماتية**، ط01، بيروت: مكتبة زين الحقوقية، 2017.

6- المشاط، عبد المنعم ، **نظرية الأمن القومي العربي**، القاهرة: دار الموقف العربي، 1989.

7- المشافية، أمين، شبلي، سعد شاكر ، **التحديات الأمنية للسياسة الخارجية الأمريكية في الشرق الأوسط في مرحلة ما بعد الحرب الباردة**،عمان: دار ومكتبة حامد للنشر والتوزيع، 2012.

8- الشاعر، عبد الرحمان بن إبراهيم ، **مواقع التواص الاجتماعي والسلوك الإنساني**، عمان : دار صفاء للنشر والتوزيع، 2015.

9- الغامدي، عبد العزيز بن غرم الله ، **جرائم الإنترنت وعقوباتها: وفق نظام مكافحة الجرائم المعلوماتية 1428: دراسة مقارنه**، ط 01، الرياض: دار الكتاب الجامعي للنشر والتوزيع، 2017.

10- بوحوش، عمار ، ذنيبات، محمد محمود ، **مناهج البحث العلمـــي**،الجزائر: ديوان المطبوعات الجامعية، 1997.

11- بيليس، جون ، سميث، ستيف ، **عولمة السياسة العالمية**، ترجمة: مركز الخليج للأبحاث: 2004.

12- بلقزيز، عبدالله، **الأمن القومي العربي**، القاهرة: الهيئة المصرية العامة للكتاب،1989.

13- بن جمعة بن جمعة ،علي ، **الأمن العربي في عالم متغير**، القاهرة: مكتبة مدبولي، 2010.

14- بن سلطان، بن عبد العزيز خالد ، **مقابل من الصحراء حقائق وذكريات ورؤيا مستقبلية لقائد القوات المشتركة ومسرح العمليات**، بيروت: دار الساقي للنشر والتوزيع، 1996.

15- ديدان، مولود ، **الدستور، تعديل نوفمبر 2008**،الجزائر: دار بلقيس.

16- ديبيل، تيري ، **إستراتيجية الشؤون الخارجية...منطق الحكم الأمريكي**، ترجمة: شحادة، وليد ، بيروت: دار الكتاب العربيومؤسسة محمد بن آل راشد آل مكتوم، 2009.

17- زيـــــدان، زبيخة، **الجريمة المعلوماتية في التشريع الجزائري و الدولي** ، الجزائر: دار الهدى، 2011.

18- زكي، أبو عامر محمد ، القهوجي، علي عبد القادر ، **قانون العقوبات، القسم الخاص**، القاهرة: دار النهضة العربية، 1993.

19- حامد، ربيع ، **نظرية الأمن القومي العربي**، القاهرة: دار الموقف العربي،1984.

20- حمد، ثائر خليل ، **الأمن القومي الأمريكي و التغيير في المنطقة العربية** ، ط1 ، دار الحامد للنشر و التوزيع ، 2016 .

21- كامل، تامر، **دراسة في الأمن الخارجي العراقي وإستراتيجية تحقيقه**، العراق: وزارة الثقافة والإعلام، 1979.

22- مارين ،بيتر ، هانس،شومان، هارالد، **فخ العولمـة**، ترجمـة : زكي، رمزي، الكويت: المجلس الوطني للثقافة والفنون والآداب سلسلة كتاب عالم المعرفة، أكتوبر 1998.

23- محمد أحمد عبد الله، آدم ، **العلاقات السودانية المصرية من منظور الأمن القومي والمصالح الإستراتيجية**، الخرطوم: شركة مطابع السودان، 2005.
24- صادق، عبد المجيد ، **أمن الدواة والنظام القانوني للفضاء الخارجي**، القاهرة: جامعة القاهرة، 1976.
25- صبري، مقلد إسماعيل ، **العلاقات السياسية الدولية: دراسة في الأصول والنظريات**، الكويت: منشورات ذات السلال، 1985.
26- عباس، علي مراد ، **الأمن والأمن القومي مقاربة نظرية**، الجزائر: ابن نديم للنشر والتوزيع، 2017.
27- عباس، علي مراد ، **مشكلات الأمن القومي: نموذج تحليل مقترح**، أبوظبي: مركز الإمارات للدراسات الإستراتيجية 2005.
28- //، //، **الأمن والأمن القومي:مقاربة نظرية**، الجزائر: ابن النديم للنشر والتوزيع، 2017.
29- عبد العزيز علي إبراهيم، خديجة ، **واقع استخدام شبكات التواصل الاجتماعي في العميلة التعليمية : دراسة ميدانية**، مصر: جامعة الصعيد، 2014.
30- عبد القادر المومني، نهلا ،**الجرائم المعلوماتية**، دار الثقافة للنشر والتوزيع ، 2008.
31- علام،أشرف ، **مشروع قناة البحرين والأمن العربي**، القاهرة: مجموعة النيل العربية، 2002.
32- عكروم، لندة، **تأثير التهديدات الأمنية بين شمال و جنوب المتوسط**،عمان: دار ابن بطوطة للنشر والتوزيع،2013.
33-
34- قورة، نائلة ،**جرائم الحاسوب الاقتصادية**، القاهرة: دار النهضة العربية، 2004.
35- ربلة، فكتور ، حمودة ،أحمد ، **التربية السكانية في الوطن العربي: واقعها واتجاهات تطويرها**، عمان: ورقة عمل للنشر والتوزيع، 1990.
36- شفيق، نوران ، **أثر التهديدات الإلكترونية على العلاقات الدولية: دراسة في أبعاد الأمن الالكترونية**، القاهرة: المكتب العربي للمعارف، 2018.
37- خليفة، إيهاب ، **القوة الإلكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الأنترنت" الولايات المتحدة نموذجا"**، القاهرة: دار العربي للنشر والتوزيع، 2017.

38- خضر فضل الله، وائل مبارك ، **أثر الفيسبوك على المجتمع**، ط 01، الإسكندرية : مدونة شمس النهضة، 2011.

ب-**المجلات و الدوريات:**

39- أدمام، شهرزاد ، **(الطبيعة اللاتماثلية للتهديدات الأمنية الجديدة، مجلة الندوة للدراسات القانونية)**، العدد01، 2013.

40- ابو عامود،**(المفهوم العام للأمن، مركز الإعلام الأمني)**، مصر، جامعة حلوان.

41- الزبيدي،فوزي حسن ، **(منهجية تقييم مخاطر الأمن القومي"، مجلة رؤى إستراتيجية)**العدد11،جويلية 2015.

42- الفوزان، حسام ، **(برمجيات التجسس : القليل من المعرفة شي رائع،مجلة الثقافة المعلوماتية)**، العدد03، 2007.

43- بورني، نسيم، (**مواقع التواصل لاجتماعي وتأثيرها على المراهقين، مجلة العلوم الإنسانية)** ، أم البواقي، جامعة أم البواقي، 2018.

44- حجاج قاسم، **(التدخل الإنساني للجيش الوطني الشعبي في مواجهة الكوارث الطبيعية، مجلة السياسة والقانون)**، العدد الرابع عشر، ورقلة، جانفي 2016.

45- جارش، عادل ، (**مُقاربة معرفية حول التهديدات الأمنية الجديدة"، مجلة العلوم السياسية والقانون)** ،العدد الأول، 2017.

46- حيدر، محمود ، **(السيادة الدولية في تحولات العولمة: الدولة المغلولة، مجلة شؤون الأوسط)**، العدد100، 2004.

47- حلمي، علي يوسف سلوى ، **(واقع البلطجة الإلكترونية بين طلاب جامعة بنى سويف وإمكانية التغلب عليها، مجلة العلوم التربوية)**، العدد04، 2017.

48- كاظم، أحمد ، **(مواقع التواصل الاجتماعي ودورها في قطاع التعليم الجامعي كلية الطب البيطري : جامعة القاسم الخضراء أنموذجا، مجلة مركزبابل للدراسات الإنسانية)**، العدد 04، العراق، 2017.

49- ليتم، فتيحة ، ليتيم، نادية ، (**الأمن المعلوماتي للحكومة الإلكترونية وإرهاب القرصنة، مجلة الفكر)**، العدد 12.

50- مؤيد ،عبد اللطيف سامر ، **(الإرهاب الالكتروني وسبل المواجهة، مجلة جامعة كربلاء العربية)**، المجلد 04، العدد03، 2016.

51- مؤنس محب الدين محمد ، **(الإرهاب والعنف السياسي"، مجلة الأمن العامة)**،العدد 24، 1981.

52- عباس، صغير فريدة ، أعراب، فطيمة ، (**مواقع التواصل الاجتماعي وانعكاساتها على التنشئة الاجتماعية لدى الشباب وفق منظور الاستخدامات و الإشباعات: دراسة مسحية على عينة من الشباب بولاية الجزائر العاصمة"، مجلة بحوث)**، العدد11، جامعة الجزائر 01، 2018.

53- عبد الله الحربي، سليمان ،**(مفهوم الأمن: مستوياته وصيغه وتهديداته "دراسة نظرية في المفاهيم و الأطر"،المجلة العربية للعلوم السياسية**،) العدد 19،صيف 2008.

54- عبد الحي، وليد ، **(تأثير التكنولوجيا على العلاقات الدولية، المجلة الجزائرية للعلاقات الدولية)**،العدد04.

55- عبد الحفيظ، زكي، **(الأمن القومي قراءة في المفهوم والأبعاد، مجلة المعهد المصري للدراسات السياسية والإستراتيجية)**،9فيفري2016.

56- عبد الصادق، عادل ، **(الفضاء الإلكتروني وتهديدات جديدة للأمن القومي، قضايا إستراتيجية)**، 2010.

57- عبد الصادق، عادل ، **(القوة الالكترونية أسلحة الانتشار الشامل في عصر الفضاء الالكتروني)، مجلة السياسة الدولية**، العدد188، مؤسسة الأهرام، مصر، 2012.

58- علي عبد الله الصفوة، نوفل ، عزت فاضل الطائي محمد ، **(جريمة الإخلال بالآداب العامة بواسطة وسائل تقنية المعلومات: دراسة مقارنة، مجلة بحوث مستقبلية)**، العدد 29-30، كلية الحدباء الجامعة، 2010.

59- علي سالم، محمد ، عبيد هجيج، حسون ، **(الجريمة المعلوماتية، مجلة جامعة بابل: العلوم الإنسانية)**، المجلد 14، العدد06، العراق، 2007.

60- ربيع، حامد ، **(نظرية الأمن القومي : حول عمليات التأصيل الفكري لمنهجية تقنين مبادئ الأمن القومي والواقع العربي، دوريات آفاق عربية**،) عدد03، بغداد، 1984.

61- شيخاني، سميرة، **(الإعلام الجديد في عصر المعلومات ، مجلة جامعة دمشق)**، العدد 01-02، 2010.

62- شلوش، نورة ، **(القرصنة الإلكترونية في الفضاء السيبراني: التهديد المتصاعد لأمن الدولة، مجلة مركز بابل)**، المجلد 08، العدد 02، 2018.

63- خليفة إيهاب ، **(كيف تدير الدولة شؤونها في عصر الانترنت، مركز المستقبل للدراسات والأبحاث المتقدة، دورية اتجاهات حديثة**، العدد06، 2015.

ج- المذكرات و الأطروحات:

64- أديب، محمد عوض، رشا ، **آثار استخدام مواقع التواصل الاجتماعي على التحصيل الدراسي للأبناء،** (مشروع تخرج للحصول على درجة البكالوريوس)، جامعة القدس المقترحة، 2013-2014.

65- المنصور، محمد ، **تأثير شبكات التواصل الاجتماعي على جمهور المتلقين- دراسة مقارنة للمواقع الاجتماعية والمواقع الإلكترونية،** (رسالة ماجستير في الإعلام والاتصال)،الأكاديمية العربية في الدانمرك ، 2012.

66- بن عبد الرزاق،حنان ، **تأثير المأزق الأمني الإثني على الاستقرار الداخلي للدولة -دراسة للنموذج الإسباني منذ 1936،** (أطروحة دكتوراه منشورة)، بسكرة، 2016-2017.

67- بعرة، سعيدة، ، **الجريمة الإلكترونية في التشريع الجزائري: دراسة مقارنة،** (مذكرة ماستر منشورة)، بسكرة، 2015-2016.

68- جلعود، وليد غسان سعيد ، **دور الحرب الإلكترونية في الصراع العربي الإسرائيلي،** (رسالة ماجستير منشورة)، فلسطين، 2013.

69- دحماني، سليم ، **أثر التهديدات السيبرانية على الأمن القومي الدولي الولايات المتحدة الأمريكية –أنموذجا-،** (مذكرة ماستر منشورة)، المسيلة، 2017-2018.

70- حمدي ماطر، عبد الله ، **إعتماد الشباب الجامعي على مواقع التواصل الاجتماعي في التزود بالمعلومات: دراسة مسحية في جامعة تبوك السعودية،** (رسالة ماجستير منشورة، قسم الصحافة والإعلام)، جامعة الشرق الأوسط، 2018.

71- معالي، خالد ، **أثر الصحافة الإلكترونية على التنمية السياسية في فلسطين (الضفة الغربية وقطاع غزة 1996-2007)،** (رسالة ماجستير منشورة)، نابلس، 2008.

72- معمري، خالد ، **التنظير في الدراسات الأمنية لفترة ما بعد الحرب الباردة: دراسة في الخطاب الأمني الأمريكي بعد 11 سبتمبر،**(رسالة ماجستير منشورة)، باتنة، 2007-2008.

73- نومار، مريم نريمان ، **إستخدام مواقع الشبكات الاجتماعية وتأثيره في العلاقات الاجتماعية دراسة عينة من مستخدمي موقع الفايسبوك في الجزائر،** (رسالة ماجستير منشورة)، باتنة، 2011-2012.

74- عصام، أحمد ، **تأثير مواقع التواصل الاجتماعي على خصوصية الفرد الجزائري : دراسة وصفية حول الخصوصية و البنية والقيمية للأفراد طلبة جامعة المسيلة**، (مذكرة ماستر منشورة)، قسم الإعلام والاتصال، المسيلة، 2013

75- سوير، سفيان ، **جرائم المعلوماتية**، (رسالة ماجستير منشورة)، تلمسان 2010-2011.

76- سعيداني، نعيم ، **آليات البحث وتحدي عن الجريمة المعلوماتية في القانون الجزائري**، (رسالة ماجستير منشورة)، باتنة، 2012-2013.

77- رصاع، فتيحة ، **الحماية الجنائية للمعلومات على شبكة الإنترنت**، (رسالة ماجستير منشورة)، تلمسان، 2001-2012.

د- المؤتمرات:

78- الجمعية العامة للأمم المتحدة.

79- المسند، عبد الرحمان ، **"وسائل الارهاب الالكتروني : حكمها في الإسلام وطرق مكافحتها"**، الرياض، السجل العلمي لمؤتمر موقف الإسلام من الإرهاب، 2004.

80- عرب، يونس ،**"جرائم الكمبيوتر والإنترنت إيجاز في مفهوم النطاق والخصائص والصور والقواعد الإجرامية للملاحقة والإثبات"**، ورقة مقدمة في المؤتمر الأمن العربي 2002، 10-12-2002.

ه- القوانين و المراسيم:

81- **الجمهورية الجزائرية الديمقراطية الشعبية**، قانون رقم 09-04 المؤرخ في 14 شعبان 1430 سنة 2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها ح رع 47، صادر بتاريخ 2009/08/16.

82- **المادة 87**، قانون رقم 2000-03 المؤرخ في 5 أوت 2000 والذي يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية.

و- المواقع الالكترونية:

83- دبوق، يحي ،"الحرب الالكترونية تستعر ضد اسرائيل...و تضرب الاقتصاد"، تم التصفح في 15-04-2019 ، على الرابط الإلكتروني: http://al-akhbae.com/Palestine/63832

84- كريم، حميدة، "القرصنةالإلكترونية"على الرابط الإلكتروني: https://www.alukah.net/culture/0/52639/#ixzz5qIJFQjM5

85- محسن، عبد الكريم ، ساحة المعارك العظمى التالية: الفضاء الإلكتروني،على الرابط الإلكتروني: http://www.ahewar.org/debat/show.art.asp?aid=291166&r=0

86- مساعد،كمال ،**(الحرب الافتراضية سيناريوهات محاكاة الواقع، مجلة الجيش اللبناني)**، العدد 253، 2006، على الرابط الإلكتروني: https://www.lebarmy.gov.lb/ar/content

87- صابر، نعمان جمال، نعمان، نعمانأحمد ، " ماهي الجريمة الإلكترونية وما أنواعها؟"، على الرابط الإلكتروني: **https://specialties.bayt.com/ar/specialties/q/11929/%D9%85%D8%A7%D9%87%D9%8A-%D8%A7%D9%84%D8%AC%D8%B1%D9%8A%D9%85%D8%A9-%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9-%D9%88%D9%85%D8%A7-%D8%A3%D9%86%D9%88%D8%A7%D8http://www.ibtesamah.com/showthread-t_10265.html %B9%D9%87%D8%A7/**

88- علاء عبد الحفيظ، محمد، " تعريف مفهوم الأمن القومي وتحديد أبعاده"، **المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات**، على الرابط الإلكتروني: https://www.europarabct.com/%D9%85%D9%81%D9%87%D9%88%D9%85-%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D9%82%D9%88%D9%85%D9%8A-

%D9%88%D8%AA%D8%AD%D8%AF%D9%8A%D8%AF-
%D8%A3%D8%A8%D8%B9%D8%A7%D8%AF%D9%87/
89- عب العال عالي، طارق ، " مفهوم الأمن القومي... بين الحقيقة والخيال"، الرابط الإلكتروني:
https://www.almasryalyoum.com/news/details/1217546
90- شفيق، نوران ، آثار الهجمات الإلكترونية وخطورتها، على الرابط الإلكتروني:
https://www.europarabct.com/%D8%A2%D8%AB%D8%A7%D8%B1-
%D8%A7%D9%84%D9%87%D8%AC%D9%85%D8%A7%D8%AA-
%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9-
%D9%88%D8%AE%D8%B7%D9%88%D8%B1%D8%AA%D9%87%D8%A7%D8%8C%D9%86/
91- الإستخبارت الأمريكية تخشى وجود إدوارد سنودن آخر في صفوفها، **موقع جريدة التحرير**، تم التصفح في 04-03-2019، على الرابط الإلكتروني:
http://www.altahrironline.com/ara
92- "الحرب الإلكترونية أخطر تهديد إيراني"، موقع cnn ، على الرابط الإلكتروني:
http://archive.arabic.cnn.com/2012/scitech/11/6/_iran-cyberattack/index.html
93- اليوتيوب، على الرابط الإلكتروني:
https://mawdoo3.com/%D8%A8%D8%AD%D8%AB_%D8%B9%D9%86_%D8%A7%D9%84%D9%8A%D9%88%D8%AA%D9%8A%D9%88%D8%A8
94- المحرر السياسي، "القرصنة الروسية ليست جديدة... الحرب الإلكترونية الأولى في أستونيا"، ، على الرابط الإلكتروني:
https://arb.majalla.com/2017/037
95- القرصنة ثمن باهظ، على الرابط الإلكتروني:
https://elaph.com/Web/Technology/2009/9/486426.html

96- التجسس على الرابط الإلكتروني : على الرابط: http://yemen-press.com

97- التهديدات الجديدة: الأبعاد الإلكترونية، **مجلة حلف الناتو**، على الرابط الإلكتروني: https://www.nato.int/docu/review/2011/11-september/Cyber-Threads/AR/index.htm

98- أفضل 10 جيوش إلكترونية في العالم، علىالرابط الإلكتروني: https://katehon.com/ar/article/mhy-fdl-khms-jywsh-lktrwny-fy-llm-wm-trtyb-ljysh-lsybrny-lrwsy

99- وسائل الإرهاب الإلكتروني، على الرابط الإلكتروني: http://shamela.ws/browse.php/book-1244/page-9

100- مؤتمر ميونيخ يناقش جدوى الجيوش الإلكترونية، تم التصفح: 24-04-2019،على الرابط الإلكتروني: https://arabic.euronews.com/2018/02/16/eu-munich-robot-soldiers

101- " تعريف القومية"، على الرابط الإلكتروني: https://weziwezi.com/%D8%AA%D8%B9%D8%B1%D9%8A%D9%81-%D8%A7%D9%84%D9%82%D9%88%D9%85%D9%8A%D8%A9/

102- https://instaview.me/ar.

103- https://www.almaany.com/ar/dict/ar-en/electronic/

104- https://www.techopedia.com/definition/26940/linkedin-li

105- http://www.asharqalarabi.org.uk-/mu-sa2/b-mishacat-5352.htm

2- باللغة اللأجنبية:

أ-الكتب:

106- Buzan Barry, **people state and fear**, london :wheatshzaf books, 1983.

107- Charles philippe Davide**, la guerre et la paix, paris**, presse de science politique, 2000.

108- David W.Ziegtez,**war peace and international politics**,Boston:SME, 1984.

109- DOROTHY E. DENNING," Cyber terrorism"**, Global Dialogue**, Autumn, 2000.

110- Dougherty (James E.) &Pfaltzgraff (Robert L.), **Contending Theories of International Relations: A Comprehensive Survey** Fifth Edition , New York: Longman, 2001 .

111- Hans Gunter Brauch, **"Coping with Global Environmental Change, Disasters and Security**", USA: Verlag Berlin Heidelberg: Springer, 2011.

112- Jholsti K**, international politics ATromane work for analaysis**, U.S.E : hall international ;1995.

113- Julian Saada, **révoltes dans le monde arabe : une révolution facebook ?**,RaoulDandurand Chair , 21 avril 2011.

114- Wasinee Kittiwongvivat, Pimonpha Rakkanngan, **facebooking your dream**, Master Thesis;2010.

ب-المجلات والمقالات:

1- Thierry Balzacq , **(Que'est ce que la sécurité national,revue international et strategique)** , n52, 4-2003.

2- Jan Eichler, **(Comment apprécier les menaces et les risques du monde contemporain?, Défense nationale et sécurité collectiveà)**, vol.62, n°11, Novembre2006.

ج-المذكرات:

3- Krause Keith and William Michael, (ed.), **Critical Security Studies : Concepts and Cases**, Mineapolis: University of Minnesota Press, 1987.

د-القواميس:

4- Le Petite Robert**, Dictionnaire Alphabétique et Analogique de la Langue Française**, Paris, Editionfirmindidol, 1979.

فهرس المحتويات

المحتويات	الصفحة
الإهداء.	
الشكر والعرفان.	
مقدمة.	12-2
الفصل الأول: الإطار النظري والمفاهيمي للدراسة.	
تمهيد.	13
المبحث الأول: تطور مفهوم الأمن القومي.	14
المطلب الأول: مفهوم الأمن القومي.	14
أولا: بوادر ظهور مفهوم الأمن القومي.	14
ثانيا: تعريف الأمن القومي.	17
ثالثا: الارتباط بين الأمن القومي والمصلحة القومية.	21
رابعا: خصائص الأمن القومي.	22
خامسا: محددات الأمن القومي.	23
سادسا: مستويات وأبعاد الأمن القومي.	24
المطلب الثاني: أهم الاتجاهات في الدراسات الأمنية.	29

أولا : الاتجاه التقليدي للأمن القومي.	29
ثانيا: الاتجاه المعاصر للأمن القومي.	31
المطلب الثالث: مهددات الأمن القومي.	32
أولا :مفهوم التهديدات الأمنية.	32
ثانيا: تصنيفات التهديدات الأمنية.	35
المبحث الثاني: مفهوم التهديدات الإلكترونية.	39
المطلب الأول: تعريف التهديدات الإلكترونية.	39
المطلب الثاني: أنواع التهديدات الإلكترونية ومستوياتها.	41
أولا: القرصنة الإلكترونية.	41
ثانيا: الجريمة الإلكترونية.	43
ثالثا: التجسس الإلكتروني.	45
رابعا : الإرهاب الإلكتروني.	46
خامسا: الحرب الإلكترونية.	51
المطلب الثالث: الجهود المبذولة لمحاربة التهديدات الإلكترونية.	55
أولا : الجهود الوطنية لتأمين الفضاء الإلكتروني.	55

ثانيا : الجهود الدولية من أجل فضاء إلكتروني آمن.	57
خلاصة الفصل.	58
الفصل الثاني: الثورة الإلكترونية والأمن القومي.	
تمهيد.	60
المبحث الأول: المخاطر الإلكترونية على المجتمع والسيادة.	61
المطلب الأول: تأثير مواقع التواصل الإجتماعي على الأمن المجتمعي.	61
أولا: تعريف مواقع التواصل الاجتماعي.	61
ثانيا: نشأة مواقع التواصل الاجتماعي.	63
ثالثا: خصائص مواقع التواصل الاجتماعي.	65
رابعا: نماذج عن مواقع التواصل الاجتماعي.	66
خامسا: أثر مواقع التواصل الاجتماعي على الأمن المجتمعي.	69
المطلب الثاني: التهديدات الإلكترونية الدولية وقضايا السيادة.	66
المطلب الثالث: علاقة الأمن الإلكتروني بالأمن القومي.	70
المبحث الثاني: نماذج مختلفة عن التهديدات الالكترونية.	75
المطلب الأول: الجريمة الإلكترونية في الجزائر.	75

المطلب الثاني: الإرهاب الإلكتروني في الولايات المتحدة الأمريكية.	83
المطلب الثالث: القرصنة الإلكترونية في روسيا.	87
المطلب الرابع:الشباب العربي والحرب الإلكترونية على الاحتلال الإسرائيلي.	94
خلاصة الفصل.	97
الخاتمة.	98
قائمة المراجع.	102
فهرس المحتويات.	114
ملخص الدراسة.	119

ملخص:

إن تطور الأمن القومي أفرز أبعادا جديدة للمفهوم، فالتحولات العديدة في عالم ما بعد الحرب الباردة ساهمت في تحول الفواعل والعوامل والتهديدات الكبرى للأمن القومي،ومن بين هذه التهديدات أصبح التهديد الإلكتروني واحدا من أهم التحديات في هذا العالم الجديد المعقد.

نجادل في هذه الدراسة أن التهديد الإلكتروني، يؤثر بقوة على الأمن القومي للدول _على الأقل_ في الوقت الراهن، إذا أصبحت السياسات الامنية للدول تتضمن التركيز على مفاهيم أمنية جديدة مثل: الحرب الإلكترونية، الجوسسة الالكترونية، الجريمة السبريانية، جرائم الانترنت، القرصنة الالكترونية.

Abstract :

The evolution of national security of states create a new demontions of the consept, many changments in the post could war world has been changed the factors actors and major theats of states, between this threats: the electronic threat became one of the most importante changes in the new complicate world .

We agrue in this stady that electronic threat inpact strangly on the national security of states –at least- in this time then security policies of states became consontrate on a new security concepts as: electronic war electronic spy, cyber crim, internet crimes, electronic piracy.