جـامـعـة 20 أوت 1955 –سـكـيـكـدة –

كليةالحقوق والـعـلـوم الـسـيـاسية

قسم العلوم السياسية والعلاقات الدولية

متطلبات الأمن السيبراني في السياسة الدولية بين النظري و التطبيق

مذكرة مكملة لنيل شهادة الماستر في العلوم السياسية

تخصص: علاقات دولية

إعداد الطالبتين

– طيبي سمية

– موات ايناس

إشراف الأستاذة:

– وسام ميهوب

أعضاء لجنة المناقشة

إسم ولقب الأستاذ(ة)	الدرجة العلمية	المؤسسة الجامعية	الصفة
د/ بويبة نبيل	أستاذ محاضر (أ)	جامعة 20 أوت 1955 سكيكدة	رئيسا
أ/ وسام ميهوب	أستاذة مساعدة (أ)	جامعة 20 أوت 1955 سكيكدة	مشرفا ومقررا
أ/ قربوع زهية	أستاذة مساعدة(أ)	جامعة 20 أوت 1955 سكيكدة	ممتحنا

الموسم الجامعي:2020/2019 م الموافق لـ 1441/1440 هـ

الإهداء

أولا وقبل كل شيء الشكر لله تعالى الذي أعانني على إتمام هذا العمل

إلى الوالدين الكريمين حفظهما الله تعالى وأطال في عمرهما وأدامهم تاجا فوق رأسي.

إلى إخوتي عاطف،موسى ،بلال وزوجاتهم وأولادهم وأخواتي حياة وداد وأولادهم وأزواجهم وجميع أفراد العائلة كبيرا وصغيرا.

إلى زوجي الكريم وعائلته كبيرا وصغيرا

إلى كل الأهل والأقارب و الأصدقاء إلى جميع زملائي في دفعة الماستر تخصص علاقات دولية.

إلى كل أساتذة وموظفي قسم العلوم السياسية بجامعة 20 أوت 1955 سكيكدة لهم مني أطيب عبارات الاحترام والتقدير

الطالبة:

سمية طيبي

الإهداء

بسم الله الرحمان الرحيم

أشكر الله عز وجل الذي وفقني في إنجاز هذا العمل المتواضع

إلى من ذكرهم جل جلاله في كتابه الكريم وقال:"وأخفض لهما جناح الذل من الرحمة وقل ربي إرحمهما كما ربياني صغيرا"الإسراء 24،والدي الكريمين اللذان ضحا بوقتهما ومالهما من أجل بلوغي أقصى الغايات وأسمى الأهداف،مهما شكرت لن أوفيكما حقكما أدامكما الله تاجا فوق رأسي .

إلى أختاي اللؤلؤتان أميرة ونورهان اللتان كانتا لي دعما وسندا،إلى الروح الطاهرة أختي أمينة رحمها الله.

إلى كل الأهل والأقارب كبيرا وصغيرا وأخص بالذكر الكتكوتة الصغيرة بتول. إلى كل زملائي في مرحلتي ليسانس والماستر.

كما أهدي ثمرة جهدي هذه أيضا إلى جميع أساتذة قسم العلوم السياسية والعلاقات الدولية بجامعة 20 أوت 1955 سكيكدة.

الطالبة:

إيناس موات

شكر وعرفان

الحمد لله والشكر له أولا الذي شرح لنا صدرنا ويسر لنا أمرنا وخفف عنا وزرنا وأحلل عقدة من لساننا،فالحمد لله ربي أنعمت علينا من فضلك،وأرشدتنا إلى السبيل وألهمتنا الهمة لإتمام عملنا هذا نبتغي به رضاك لا إله إلا أنت نشكرك ونستعين بك وتوكلنا عليك فأنت خير المتوكلين.

كما نتقدم بجزيل الشكر وعظيم الإمتنان إلى الأستاذة الفاضلة "وسام ميهوب" لقبُولها الإشراف على هذه المذكرة ولمساعدتها لنا بتوفير العديد من المراجع، ولما قدمته لنا من نصائح وتوجيهات قيمة طيلة فترة إنجازنا لهذه الدراسة.

كما نتقدم بالشكر لأعضاء لجنة المناقشة على جهدهم ووقتهم لقراءة المذكرة وكافة ملاحظاتهم القيمة بغرض إثراء وتقويم هذه الدراسة.

كما لا يفوتنا أن نتقدم بالشكر والعرفان لكافة أساتذة قسم العلوم السياسة بجامعة 20 أوت 1955 سكيكدة، وكذا جميع موظفي القسم على كل التسهيلات التي قدموها لنا طيلة مشوارنا الدراسي بالجامعة.

خطة الدراسة

مقدمة

أحدثت ثورة المعلومات والاتصالات قفزة نوعية خاصة مع بداية بروز النظام الدولي الجديد،حيث عرفت البيئة الدولية مجموعة من التغيرات والأحداث التي مست جميع المجالات والميادين الاقتصادية والسياسية والاجتماعية وحتى العلمية، فعلى المستوى الإجتماعي كان لها واقع كبير على سلوكيات المجتمع حيث ظهرت معطيات وقضايا جديدة لم تكن في السابق ذات تأثير على العلاقات بين الدول ، كما نجد أن مختلف المواضيع في العلاقات الدولية ذات الطابع السياسي بدأت تتوسع من حيث المفاهيم،الإختصاصات ...،فعلى سبيل المثال مفهوم الأمن كان يعنى فقط بالجانب العسكري كما يدرس مستويات معينة كالأمن الغذائي، الأمن القومي،الأمن الإنساني .

ولكن رغم هذه التطورات الحاصلة في هذه الفترة توسع مفهوم الأمن ليشمل مستوى أعمق كالأمن السيبراني الذي يهتم بالقضايا المعلوماتية أو الإلكترونية للبنى التحتية للدول ومع تزايد المخاطر الأمنية وخاصة القرصنة الالكترونية والجوسسة أو ما يعرف بالإرهاب الالكتروني أو حتى الجريمة والحرب السيبرانيين كل هذه المخاطر أصبحت بمثابة قضايا جوهرية ذات تأثير عالمي لا يمس أمن الفواعل الدوليين فقط بل تجاوز هذا الحد إلى الفواعل من غير الدول كالشركات متعددة الجنسيات وغيرها. هذا مادفع الدول والمنظمات الدولية تعيد النظر في استراتيجياتها الأمنية خاصة وأن مثل هذه التهديدات الأمنية تحدث بصفة مباغتة يصعب التحكم فيها ولا تحديد مصدرها وهوية من يقوم بها ،فإن البحث في القضايا السيبرانية والتحديات الأمنية يفرض علينا البحث في المجتمع الرقمي بتوصيف بنية هذه التهديدات الأمنية السيبرانية.

ومنه يمكن اعتبار تحديات الأمن السيبراني أعلى تحديات الأمن القومي في ظل النظام الدولي الجديد الذي يشمل جميع الجوانب المجتمعية الأخرى، بل واكب ويواكب كل التهديدات والتحديات الأمنية التي يمكن أن تشكل عائق أمام الاقتصاد الرقمي فقد أسقطت تكنولوجيا المعلومات جميع الفوارق والحدود الجغرافية والسياسية بين الدول ما يضع السيادة الوطنية على المحك،خاصة مع اختراق المواقع الحكومية والتجسس المعلوماتي بين الدول.

ويبرز التحدي الفكري والثقافي أهم المسببات لتهديدات الأمن السيبراني، ما يعرف مستقبل تكنولوجيا المعلومات تهديدات سيبرانية كبيرة تزرع فيها المخاوف لدى جميع الأطراف والجهات وهي الاخرى بدورها ستشكل فرص استثمارية لمؤسسات الأمن الالكتروني المعلوماتي الأمر الذي يدفع إلى التعامل مع قضايا الأمن السيبراني بمرونة تامة ونظرة استباقية للموضوع محل الاهتمام والدراسة.

أهمية الدراسة:

إن الاهتمام بهذا الموضوع له أهميتين علمية وعملية يمكن تلخيصها فيما يلي:

1- الأهمية العلمية:

- ترتبط الأهمية العلمية في دراسة الموضوع لإعتبارات الجدة والحداثة في دراسة مثل هذه المواضيع ذات الصلة بالأمن السيبراني في حقل العلاقات الدولية في إطار تحليل وتفسير الظاهرة في حقل العلاقات الدولية، مع تزامن ظهوره مع الثورة المعلوماتية والتكنولوجية.
- تأثير تداعيات العولمة المختلفة على مجال دراسة ومفهوم الأمن، أين تم الانتقال من المفهوم التقليدي الذي يعتمد بالأساس على القدرة العسكرية للدولة وقوتها الى مفهوم جديد وموسع في حقل الدراسات الأمنية والاستراتيجية عن طريق التحول إلى المفهوم الجديد للأمن من حيث المفاهيم ومن حيث مستويات التحليل.

2- الأهمية العملية:

- تتمثل في تطور ظاهرة الأمن السيبراني على مستوى حقل العلاقات الدولية والتي أدت الى ظهور نوع جديد من الهجمات تختلف عن سابقاتها التقليدية وبالتالي تكريس مبدأ الأمن الجماعي الذي أضحى ضرورة ملحة على اعتبار وجود حركة إلكترونية عابرة للحدود الدولية.
- بات البعد السيبراني يشكل تحديا أمنيا بالنسبة للأمن المجتمعي والدولي حيث أصبحت الحكومات تبحث عن آليات للتعامل معه ومحاولة ضبطه خصوصا مع ما تخشاه الهيئات الحكومية وغير الحكومية من مضاعفات هذا التحول على استقرار المنظومة الوطنية والدولية؛ ومن هنا تبرز الأهمية العملية لهذه الدراسة.

أهداف الدراسة

- تهدف الدراسة الى إعطاء رؤية توضيحية لمفهوم الأمن السيبراني والمفاهيم المرتبطة به إضافة إلى إبراز أهمية الموضوع في السياسة الدولية من خلال التعرف على محاولات خلق الوعي الجماعي بشأن الظاهرة و تأثيراتها على أمن الدول.
- ترشيد آليات ترشيد العمل الحكومي وغير الحكومي في محاولة احتواء مخاطر الأمن السيبراني على اعتبار أن أغلب الاضطرابات الدولية الراهنة ترجع أساسا إلى استخدام التكنولوجيا في ضرب أمن واستقرار الدول.

- التطرق إلى عمل الشبكات أو الوحدات الدولية من أجل احتواء التهديدات السيبيرانية، وكذا الرقابة على الشركات الأمنية الخاصة والتجارية التي تروج أو تتاجر بمعلومات حول الأفراد والدول على حد سواء ومنه يمكن التعرف على الآليات التي بالإمكان تفعليها في السياسة الدولية لتجسيد الأمن السيبراني على المستوى عبر الوطني.

مبررات اختيار الموضوع:

تتجلى مبررات اختيار الموضوع في مبررات موضوعية وأخرى ذاتية يمكن إجمالها فيما يلي:

1- المبررات الموضوعية:

نظرا للأهمية البالغة لموضوع الأمن السيبراني وتأثيره في السياسة الدولية على الفرد، الجماعة و الدولة، وجب البحث في هذا الموضوع للتعرف عن قرب على آثاره ومدى مساهمته في السياسة الدولية وفي زيادة انتشار التهديدات الأمنية السيبرانية.

كما تسعى الدراسة أيضا لتقديم تصور تحليلي للأمن السيبراني في السياسة الدولية من خلال توضيح المفاهيم والتهديدات السيبرانية في السياسة الدولية.

المبررات الذاتية:

الإهتمام بالمواضيع ذات البعد الأمن ي والإستراتيجي.

يعد من بين المواضيع الحديثة في الوسط الأكاديمي.

يعد الاهتمام بموضوع الأمن السيبراني في الساحة الدولية نتيجة للرغبة الذاتية في معرفة أبعاده في السياسة الدولية على اعتباره البعد الأمني الجديد الذي أصبح حاسما في العلاقات الدولية مع التطور التكنولوجي في العالم ومن هذا المنطلق تولدت لدينا الرغبة الملحة في معرفة الدور الذي يقدمه أو يلعبه الأمن السيبراني في السياسة الدولية وعلى أساسها الإحاطة بآلياته ومتطلباته بحداثة الموضوع وارتباطه بالحقل المعرفي المدروس.

- محاولة إثراء المكتبة العلمية بمراجع أكاديمية تصف وتحلل الأمن السيبراني ونتائجه على الأمن الدولي، على اعتبار أن الأمن السيبراني من أفكار وتطورات معرفية في مجال الحقل المعلوماتي الإلكتروني.
- أضف إلى ذلك الرغبة في تتويج المسيرة العلمية المتواضعة بعمل أكاديمي، نحاول من خلاله تقديم إضافة وإن كانت مبسطة للمهتمين بالأمن السيبراني في السياسة الدولية ولمساعدة الطلبة في مسيرتهم الدراسية والبحثية في المستقبل.

إشكالية الدراسة:

تتمحور الإشكالية الجوهرية لهذه الدارسة في محاولة تفكيك وفهم متطلبات الأمن السيبراني بالتركيز على مختلف أبعاده الموظفة في السياسة الدولية ومعرفة الأدوار والآليات التي تنتهجها الوحدات السياسة في بيئة دولية غير آمنة باعتمادها على متطلبات أمنها السيبراني.

ومن هذا المنطلق نطرح الإشكالية التالية: **كيف يمكن للفواعل الدولية ضمان متطلبات الأمن السيبراني في ظل بيئة دولية غير مستقرة؟**

الأسئلة الفرعية:

ولمعالجة الإشكالية السابقة نطرح جملة من الأسئلة الفرعية على النحو التالي:

1- كيف يمكن التأّصيل للأمن السيبراني وفقا لمداخل مفاهيمية وأسس نظرية علمية؟

2- فيما تكمن الفواعل في مجال القوة السيبرانية؟

3- ماهي أبعاد التهديدات السيبرانية المؤثرة في السياسة الدولية عامة والسياسة الوطنية على وجه الخصوص؟

4- ما مدى نجاعة سياسات الوحدات السياسية الدولية لضمان أمنها السيبراني؟

فرضيات الدراسة:

بغرض الإجابة عن الإشكالية المطروحة تم صياغة الفرضيات التالية:

1- التزايد الهائل في التطور التكنولوجي يؤدي الى تعميق حدة التهديدات السيبرانية بأبعادها المختلفة على الوحدات السياسية.

2- تحقيق الأمن السيبراني للوحدات السياسية يتطلب تظافر الجهود الوطنية والدولية في مواجهة التهديدات السيبرانية في الفضاء الدولي.

3-تراجع الأمن السيبراني للوحدات السياسية مرتبط بالتزايد الهائل في التطورات التكنولوجية وهو بدوره يؤدي إلى تصاعد التأثيرات السيبرانية.

المقاربة المنهجية والنظرية:

سيتم الإستعانة في هذه الدراسة بمقاربة منهجية ونظرية مركبة من:

1- المدخل التاريخي:

يُتيح المدخل التاريخي إمكانية حل مشكلات معاصرة في ضوء الخبرات الماضية، كما يُتيح استخدام التاريخ القدرة على توظيف الماضي للتنبؤ بالمستقبل وكذا استخدام الحاضر لتفسير الماضي[1]. ويسمح هذا المدخل في الدراسة بمعرفة التطور التاريخي للاهتمام بالأمن السيبراني، وهذا المقترب يعد أهم المقتربات وأهمها لمعالجة جميع الدراسات في شتى العلوم وبدوره يؤدي إلى معرفة مسار تطور مفهوم الأمن السيبراني.

2- مقاربة الأمن المجتمعي:

وهذه المقاربة لباري بوزان، وذلك من خلال توسيع مفهوم الأمن الذي كان يقتصر في بداياته على البعد العسكري ليتوسع بعدها ويشمل أبعاد جديدة منها السياسية الاقتصادية البيئية... فخرج مفهوم الأمن من الطابع التقليدي الذي كان يركز على الجانب العسكري إلى مجال أوسع أدى إلى ظهور مستويات جديدة غير الدولة بل تعداه إلى أمن المجتمعات و الأفراد.

3- المقاربة البنائية:

تركز المقاربة البنائية على جملة من المفاهيم التي تتقاطع مع مؤشرات وخصائص الأمن السيبراني حيث تسهم هذه المقاربة في توضيح البعد الاجتماعي كالخطاب والهوية إضافة الى مصطلحات جديدة كالحرب السيبرانية، حرب المعلومات، كذلك الرموز...

- **أدبيات الدراسة:**

لا يمكن حصر جميع الدراسات التي تناولت الأمن السيبراني ومتطلباته ضمن السياسة الدولية إلا أننا سنذكر أهمها:

1-منى الأشقر جبور،"السيبرانية هاجس العصر"،حيث تناولت الكاتبة في هذا الكتاب الحديث عن الأمن السيبراني وأبعاده المختلفة كذلك المخاطر والجرائم السيبرانية المتمثلة في الأرهاب السيبراني والقرصنة الالكترونية، كما تطرقت أيضا لمفهوم الحرب السيبرانية وأدواتها والتقنيات المستخدمة في عملية القرصنة،بالإضافة إلى هذا تناولت سبل تحقيق الأمن السيبراني من جهود دولية وإقليمية ومبادرات فردية.

[1]- عبد الغفار رشاد القصبي، **مناهج البحث في علم السياسة**، (القاهرة: مكتبة الآداب، ط1، 2004)، ص.225.

2- نوران شفيق،"أثر التهديدات الإلكترونية على العلاقات الدولية دراسة في أبعاد المن الالكتروني"حيث تناول الكاتب في هذا المؤلف أشكال التهديدات السيبرانية وآثارها على السياسة الدولية وأبرز الهجمات السيبرانية التي مست البنى التحتية المعلوماتية للدولة أو المجتمع المدني،وتطرق أيضا للجهود والاستراتيجيات التي وضعتها الدول والمنظمات الدولية والإقليمية الحكومية وغير الحكومية لمواجهة هذه المخاطر السيبرانية.

3-عبير شفيق الرحباني،الجرائم الالكترونية ومخاطرها التي تناولت أبرز الجرائم الالكترونية من مخاطر وأبعاد.

3- عادل عبد الصادق،"أسلحة الفضاء الالكتروني في ضوء القانون الدولي"الذي في هذه المجلة تناول موضوع المجال الالكتروني.

4- A Clarke, Richard Robert Knake, **CYBER WAR:the next threat to national Security and What Do About IT.** وقد تناولا الكاتبين الحرب السيبرانية بكل الجوانب المتعلقة بالمجال السيبراني .

5- Joseph .S.Ney ,jr**,cyber power** فقد تناول الباحث القوة السيبرانية والحرب،كذلك تحدث عن أبعاد الأمن السيبراني.

6- Martti Lehto ,and Pekka Neinaamaki, Cyber Security :Analyics ,Technology and Automation,(Department Of Mathematical Information Technology, University of Finland).2014.

7- صعوبات الدراسة:

وقد تعرضنا للعديد من الصعوبات التي واجهتنا في إعداد هذه المذكرة وتبرز أهم هذه الصعوبات في ضيق الوقت إلى جانب تزامن توقيت إعداد المذكرة مع ظهور الظروف الإستثنائية التي فرضتها جائحة كورونا إلى جانب حداثة الموضوع وقلة الدراسات التي تناولت مفهوم الأمن السيبراني في السياسة الدولية من جهة، إضافة إلى تشابك وتشابه المصطلحات وتداخلها مع بعضها من جهة ثانية.

التقسيم البحثي:

تم الاعتماد في موضوع هذه الدراسة على تقسيم بحثي ثلاثي للفصول وهذا على النحو التالي:

الفصل الأول: والذي خصص لدراسة الجانب المفاهيمي والنظري للأمن السيبراني في العلاقات الدولية؛ بداية بتحديد مفهوم الأمن السيبراني والتأصيل التاريخي مع الحديث عن العوامل التي أدت للاهتمام بهذا البعد في العلاقات الدولية، والمقاربات النظرية المفسرة للأمن السيبراني في العلاقات الدولية، كما سيتم تناول الأمن السيبراني من الناحية المفاهيمية والنظرية وهذا بعرض أبرز المقاربات النظرية الجزئية منها والعامة التي فسرت وحللت ظاهرة الأمن السيبراني.

الفصل الثاني: وفي هذا الفصل المعنون تحت فواعل ووسائل التهديدات السيبرانية في السياسة الدولية الذي يتناول الوسائل المهددة للأمن السيبراني مع إبراز أهم الفواعل ،ويتم عرض الخصائص والوسائل التي تستعمل في ظل التهديدات الراهنة فقد تناولنا في المبحث الأول الجريمة السيبرانية من مفهوم وخصائص وصولا إلى الوسائل والأدوات المستعملة في الجريمة السيبرانية، أما في المبحث الثاني فقد تناولنا الإرهاب السيبراني من تعريف مع ذكر التطور التاريخي للمصطلح مع ذكر الخصائص والأدوات والوسائل التي يستعملها الإرهابي،أما في المبحث الثالث فقد تطرقنا إلى الحرب السيبرانية وتناولنا فيه التعريف مع ذكر الخصائص وإبراز أهم الوسائل المستعملة من طرفهم، وكحوصلة لهذا الفصل تناولنا في المبحث الرابع مقارنة لأبرز هذه التهديدات السيبرانية.

الفصل الثالث: وفي هذا الفصل تناولنا نماذج مختارة متعلقة بالأمن السيبراني في السياسة الدولية إضافة إلى أبرز التوصيات الدولية والوطنية المتعلقة بالأمن السيبراني،وأبرز الجهود الدلية والعالمية المتعلقة بمجال الأمن السيبراني في ظل بيئة سياسية متغيرة.

الفصل الأول

في ظل التغيرات الحاصلة في الساحة الدولية وبروز العديد من التهديدات التي لم يشهدها المجتمع الدولي من قبل خاصة في القرن العشرين مع إنفجار الثورة المعلوماتية أصبح حقل السياسة الدولية مسرحا للعديد من التفاعلات بين مختلف الفواعل (الدولة، الجماعات، الأفراد) حيث جسد جانب الممارسات المعلوماتية التي تسعى من خلالها الوحدات الدولية لتحقيق أهدافها ومصالحها عبر العديد من الوسائل والآليات التي ترافق توجهاتها في ظل السياسة الدولية، وعلى هذا الأساس تتمحور دراستنا في هذا الفصل المعنون بمدخل مفاهيمي ونظري للأمن السيبراني في العلاقات الدولية حول مفهوم الأمن السيبراني ومختلف المفاهيم ذات الصلة به وأبعاده في السياسة الدولية.

سنحاول هنا الإحاطة بمختلف الجوانب التحليلية لمفهوم الأمن السيبراني، وهذا بالتركيز على النواحي المفاهيمية بمختلف عناصرها بغرض إزالة الغموض عنها كالأمن والسيبرانية والمفاهيم المتعلقة بها، إلى جانب التطرق إلى الناحية النظرية أين سيتم التركيز على أبرز المقاربات والمداخل النظرية التي تمكننا من وضع صورة أكثر وضوحا وتفسيرا للأمن السيبراني.

المبحث الأول: من الأمن التقليدي إلى الأمن السيبراني.

يبدو جليا أن الأمن السيبراني يمس أمن الثورة الرقمية والثقافية للأفراد والمنظمات والدول، وهو المجال الجديد للحروب الحديثة بعد الحروب البرية والبحرية والجوية والفضاء الحقيقي، وهو يمثل جميع شبكات الحاسب الآلي الموجودة حول العالم ويشمل ذلك الأجهزة الإلكترونية المرتبطة من خلال شبكة الألياف البصرية والشبكات اللاسلكية للفضاء السيبراني ليس الانترنيت فقط وإنما شبكات أخرى كثيرة متصلة به.

وقبل الفصل في مفهوم الأمن ارتأينا إدراج التسلسل في السياق التاريخي التدرجي من مفاهيم الحرب إلى مفاهيم الأمن؛ فإذا كانت الحرب تعبر عن استمرار الممارسة السياسية لكن بوسائل وأدوات مختلفة ففي الآونة الأخيرة لم تعد مجرد حروب تقليدية يكون فيها العدو واضح المعالم وتتحدد فيها الأهداف وحتى الوسائل بل أخذت طابعا جديدا مغايرا تماما لما عرفته الدول سابقا، كما بفضل تطور البنى الاقتصادية والصناعية والأهم التكنولوجية التي عرفها المجتمع الدولي عبر مختلف المراحل الزمنية

نجد أن تطور الحرب عرف أجيال مختلفة كل جيل يتميز بميزات وخصائص وهذه مراحله:

الجيل الأول: وهو جيل الحروب الكُتلية ويعني أن الحرب تحسمها القوة البدنية للبشر، كما أن هذا الجيل استخدمت فيه الأسلحة التقليدية كالرماح، السيوف، السهام... ويركز على الطاقات البخارية، أما بالنسبة **للجيل الثاني:** فقد كان مع بداية اختراع الإنسان للبارود والأسلحة القاذفة للنار... وفي هذا الجيل من الحروب لم يعد المقاتل ذو التدريب العالي هو المطلوب فقط لخوض غمار الحرب، بل ظهر بما يسمى بالجيوش الشعبية مثل ما كان في عهد لويس السابع عشر نهاية القرن الثامن عشر وحتى مطلع القرن العشرين[1].

وفي الربع الثاني من القرن التاسع عشر ظهر **جيل ثالث** للحروب وكان ذلك مع قيام الألمان بتطبيق الحروب الخاطفة، وقد ساهم في ظهور هذا الجيل عاملان أساسيان هما التطور التكنولوجي والذي نتج عنه ظهور أسلحة جديدة مثل الدبابات، والطائرات المقاتلة، كذلك العامل الثاني الذي يركز على نظم الاتصالات وقد ساعد على قيام المناورات العسكرية بطرق حديثة ويرتبط هذا الجيل بفترة

[1] شادي عبد الوهاب منصور، **حروب الجيل الخامس أساليب "التفجير من الداخل" على الساحة الدولية** (الإمارات: مركز التفكير 2014).ص ص.15 25.

الحرب العالمية الثانية[1]، وبعد الحرب العالمية الثانية انتقلت إلى مرحلة أخرى مغايرة عن الفترات السابقة، حيث ظهر جيل جديد وهو **الجيل الرابع** ومن ميزاته أن الحروب تكون ذات طابع سياسي وليس عسكري والهدف هو تحقيق نصر سياسي من خلال كسر عزيمة الخصم ودفع تكلفة استمراره في الحرب ،كالردع المطبق في الحرب الباردة وتعتمد على التكنولوجيا الحيوية أما فيما يتعلق **بالجيل الخامس** فهي حروب هجينة لا تماثلية، السمة الغالبة الرئيسية لهذه الحروب في القرن الحادي والعشرين هو الاعتماد على شبكات الكمبيوتر في البنية التحتية المعلوماتية العسكرية، ويتمتع المهاجم بأفضلية واضحة عن المدافع لأنها تتميز بالسرعة والمراوغة ويستهدف كذلك البنى التحية المدنية بفعل فيروسات إلكترونية يمكنها إحداث الضرر وقد برزت أساسا بعد أحداث سبتمبر 2001 ولعل أبرزها هو هجوم إستونيا 2007 الذي استخدم لتعطيل المواقع الحكومية والتجارية والمصرفية والاعلامية، وكذلك فيروس ستاكست وهو برنامج خبيث يهاجم أنظمة التحكم الصناعية وبرز في إيران في 2010 فهذه الهجمات باتت أكثر خطرا من سابقاتها بعد البر والبحر والجو والفضاء.

ومنه يمكن أن نقول أن الجيل الأول كان يركز على الميكانيكا وماكينة البخار والوسائل البدائية والثاني ذهب إلى إنتاج المحركات والتطوير في الأسلحة المستخدمة أما فترة ما بعد الحرب الباردة فقد تطور إلى التشغيل الآلي والالكترونيات وفي الجيل الرابع انترنيت البيانات والتكنولوجيات الحيوية والذكاء الاصطناعي الذي قادنا إلى الجيل الخامس أو ما يعرف بالأمن السيبراني وهناك من ذهب إلى أنه في وقتنا الحالي(2020) ظهور ما يطلق عليه الثورة البيولوجية.

المطلب الأول: مفهوم الأمن و السيبرانية

وفي هذا المطلب نتناول شقين نستهلها أولا بالأمن ومفهومه أما في الشق الثاني فنتناول مفهوم السيبرانية والمفاهيم المشابهة لها والمتعلقة بها.

الفرع الأول: مفهوم الأمن

أدت نهاية الحرب الباردة إلى ظهور نظام عالمي جديد أدى بدوره إلى بروز معطيات أمنية جديدة لذلك وجب على الباحثين في العلاقات الدولية أن يعيدوا النظر في تصورهم حول مفهوم الأمن، يعتبر الأمن مطلبا إنسانيا لما هذا اللفظ من مستويات عدة سواء على المستوى الفردي أو الدولي وحتى

[1] مركز نورس للدراسات:**الحرب السيبرانية (الالكترونية)نقلة نوعية في الاستراتيجيات العسكرية و آثر ملحوظ على العلاقات الدولية** ،مركز نورس 2019.ص2

على مستوى النظام الدولي لذلك فقد تعددت وتنوعت الدراسات الخاصة بهذا المفهوم فهو من المفاهيم الأساسية في حقل العلاقات الدولية، ولقد تطور لارتباطه بأمن الدول والأفراد، وهناك جملة من التعريفات للمصطلح من حيث المضمون والمستوى إلى غير ذلك.

1- نشأة وتطور مفهوم الأمن:

يعتبر الأمن Security على مر العصور والأزمنة الهاجس الأكبر لكل صناع القرار في الدولة والعسكريين و الأكاديميين حيث أكدوا أن بقاء الدولة وسلامتها من كل التهديدات واستمرارها هو الهدف الأساسي والأسمى لكل من له علاقة بصناعة القرار، فأمن الأفراد والجماعات هو من أمن دولهم وسلامة التراب والسيادة فعلى الرغم من الجهود التي يبدلها الاكاديميون[1] وصناع القرار من أجل وضع تعريف دقيق للأمن .

ونجد أن الدراسات الأمنية كتخصص في حقل العلاقات الدولية هو وليد الحرب الباردة، أما مصطلح الأمن فقد تم تداوله عبر التاريخ، فمنذ القرن الثاني عشر إلى غاية القرن العشرين ارتبط مفهوم الأمن في هذه الفترة بالجانب العسكري، ولكن لقد تطورت ظاهرة الأمن منذ القدم مع الوجود الإنساني، ومع تطور التنظيم الدولي ونشأة الدولة القومية خاصة بعد معاهدة واستفاليا 1648، كما نجد العديد من النظريات المرتبطة بالدولة والأمن منها هوبز الذي يميز بين المجتع والطبيعة، وهناك العديد من البحوث والدراسات في مجال الأمن، حيث تزامنت مع الظروف التي أعقبت الحرب العالمية الثانية واستخدم لأول مرة آنذاك في مجلس الأمن القومي الأمريكي 1947 حيث ارتبط بالقوة العسكرية[2]، فمعظم الدول تسعى لتعظيم قوتها العسكرية وضمان أمنها وبقائها من كل التهديدات وهو ما يعكس مدى سيطرة النظرية الواقعية في تلك الفترة، وارتبط بدراسات هانس مورغنتو Morgentheau.) وكنيث والتز (K.Waltaz)....

أما مع بداية تسعينات القرن العشرين لم يعد مفهوم الأمن مقتصرا على الجانب العسكري فقط بل تعداه ليشمل جوانب أخرى من التهديدات الأمنية الجديدة خاصة مع نهاية الحرب الباردة حيث يرى

---

[1]- ملك عوني،"رهان الثورات...تصاعد الأمن غير التقليدي في المنطقة العربية"، **مجلة السياسة الدولية**، مركز الأهرام للدراسات السياسية و الاستراتيجية، القاهرة، (العدد 186)، (أكتوبر 2011)، ص 3.

[2]- نسيم بلهول ، **فهم الأمن القومي الجزائري من مدخلي الأمن الوطني والدفاع الوطني** (عمان: دار حامد للنشر والتوزيع، 2015)،ص 37.

باري بوزان Barry Buzan" في المستوى الإقليمي أن التحول في طبيعة النزاعات التي غلب عليها نمط الصراعات الداخلية، مع تراجع حدة النزاعات بين الدول، وبروز وتطور ظاهرة العولمة بكل أبعادها وهذا ما أدى إلى الحاجة لتوسع مفهوم الأمن وتبنيه في تحليله ثلاث مستويات: الأفراد، الدول، والنظام الدولي، وبالرغم من هذا يؤكد على أن الأمن يعني البقاء وقد ميز بين خمسة أبعاد أساسية للأمن وهي:

– الأمن العسكري: ويتعلق بمستوى التفاعل والتقابل للهجوم المسلح والقدرات الدفاعية، ومعرفة الدول بنوايا بعضها البعض.

– الأمن السياسي: ويخص الاستقرار الذي تتمتع به مؤسسات الدولة و نظم الحكم التي تستمد منها شرعيتها بالحفاظ على كيانها السياسي.

– الأمن الاقتصادي: توفير المناخ المناسب لتحقيق احتياجات الشعوب المرتبط بالموارد والأسواق الضرورية للحفاظ على مستويات مقبولة من الرفاهية وسلطة و قوة الدولة.

– الأمن الاجتماعي: ويخص قدرة المجتمعات على إنتاج أنماط خصوصياتها في اللغة والثقافة، الهوية الوطنية والدينية والشعور بالولاء والانتماء في إطار شروط مقبولة لتطورها واستمرارها.

– الأمن البيئي: ويتعلق بالمحافظة على المحيط المحلي والكوني لكل نشاط إنساني ضد الأخطار البيئية.[1]

وهناك من يرجع الأمن الإنساني كبديل لأمن الدولة بأبعاده السبعة وهي: الأمن الشخصي، الاقتصادي، الغذائي، البيئي، السياسي، الصحي والمجتمعي. التوسع والتعمق في مضامين الأمن لخصها تيري بالزكا thierry Balzaca[2] في مخطط يوضح فيه كيفية توسع مفهوم الأمن، وذلك من خلال عنصرين الأول عمودي يخص مستويات التحليل والمتمثلة في الفرد،المجتمع الوطني،الإقليم....،أما الثاني فهو الأفقي يعنى بالتوسع في قطاعات الأمني،العسكري،السياسي،الاقتصادي....

والجدول التالي يوضح قطاعات الأمن وتوسعها.

[1]– عبد النور بن عنتر، "تطور مفهوم الأمن في العلاقات الدولية"، **مجلة السياسة الدولية**، (العدد 160)، (أفريل 2005)، ص 7.

[2] أمينة دير،**أثر التهديدات البيئية على واقع الأمن الإنساني في إفريقيا دراسة حالة–دول القرن الإفريقي**،مذكرة مقدمة لنيل شهادة الماجيستر(بسكرة:جامعة محمد خيضر،كلية الحقوق والعلوم السياسية،2013/**2014**).ص،14.

الجدول رقم (1): قطاعات الأمن

		قطاعات الأمن						
التوسع / التعميق		قطاع عسكري	قطاع اقتصادي	قطاع سياسي	قطاع اجتماعي	قطاع بيئي	قطاع غذائي	قطاع صحي
مستويات التحليل	عالمي							
	إقليمي							
	دولي							
	وطني							
	مجتمعي							
	فردي							

المصدر :أمينة دير،أثر التهديدات البيئية على واقع الأمن الإنساني في إفريقيا دراسة حالة–دول القرن الإفريقي– ،مذكرة مقدمة لنيل شهادة الماجيستر(بسكرة:جامعة محمد خيضر،كلية الحقوق والعلوم السياسية،قسم العلوم السياسية.2014/2013.

أ–التعريف اللغوي للأمن:

يعرف الأمن في اللغة بأنه نقيض الخوف، أي بمعنى السلامة، والأمن مصدر للفعل أَمِنَ أي حقق الأمان فقال ابن منظور: "أمنت فأنا آمن، وأمنت غيري أي ضد أخفته، فالأمن ضد الخوف، والأمانة ضد الخيانة، والإيمان ضد الكفر، والإيمان بمعنى التصديق، وضده التكذيب، فيقال آمن به قوم وكذب قوم[1]. ويقال أَمْناً وأَمَانًا وأَمَنَةً: أي اطمئنان النفس وسكون القلب وزوال الخوف، ويقال : أَمِنَ من الشر، أي سَلِمَ منه و كما جاءت معانيه في القرآن الكريم وهو ضد الخوف فقد ورد في الآية الكريمة من سورة قريش"الذي أطعمهم مّن جوعٍ وآمنهم مِنْ خَوفٍ"الآية 4،[2] وكذلك قوله تعالى في سورة النور"وليبدلهم من بعد خوفهم أمنا"الآية 24. [3]وقوله تعالى"الذين آمنوا ولم يلبسوا إيمانهم بظلم أولئك لهم الأمن وهم مهتدون"[4].

[1]– لسان العرب، **ابن منظور**، تحقيق عبد الله علي الكبير(القاهرة: دار المعارف د ،س ،ن)، ص 140.

[2]– سورة قريش، الآية(4) .

[3]– سورة النور، الآية (24) .

[4]– سورة الأنعام، الآية(82).

ب-التعريف الاصطلاحي للأمن:

لقد تعددت واختلفت آراء الباحثين والمفكرين حول مفهوم الأمن، حيث كان مرتبط بالبعد العسكري واستخدام القوة العسكرية للحفاظ على أمن وبقاء الدول، فهو بذلك يعني حماية مصالح الدولة الوطنية من التهديدات الخارجية باستخدام القوة العسكرية[1].

أما **دائرة المعارف البريطانية** عرفته بأنه: "حماية الدولة من السيطرة عليه بواسطة قوى أجنبية"[2] ولكن هذا المصطلح ارتبط بحالة الأمن الناتج عن التهديد العسكري لما بعد الحرب العالمية الثانية كالسباق نحو التسلح وتم إهمال المعاني التي يحملها الأمن من معناه الإنساني.

ويعرفه هنري كيسنجر وزير الخارجية الأمريكي "بأنه تصرف يسعى الجميع عن طريقه لتحقيق حقه في البقاء"[3]

وهناك العديد من باحثي العلاقات الدولية الذين أعطوا تعريفات للأمن، والتر ليبمان" Walter Lippman" عرفه بأنه حفاظ الأمة على قيمها الأساسية وقدرتها على صياغة هذه القيم حتى وإن دخلت حربا لصيانتها[4]. ويقصد به من وجهة النظر الموضوعية "عدم وجود تهديد للقيم المكتسبة أما من وجهة النظر الذاتية فيعني عدم وجود مخاوف من تعرض هذه القيم للخطر"[5]

أما باري بوزان "Barry Buzan" فيقول عنه "أنه قدرة الدول والمجتمعات على الحفاظ على كيانها المستقل وتماسكها الوظيفي ضد قوى التغيير التي تعتبرها معادية"[6].

---

[1]– ثامر كامل، **دراسة في الأمن الخارجي العراقي واستراتيجية تحقيقه، (العراق: وزارة الثقافة والإعلام، 1985)، ص 24.**

[2]-Wolfers Arnold (1952),**National Security as an Ambiguous Symbol** , Dans Wolfers (Arnold) (Discord And Collaboration Baltimore ,Johns Hopkins University Press,1962.p148.

[3]– رفعت سيد أحمد، الأمن القومي العربي بعد حرب لبنان: دراسة في تطور المفهوم، **مجلة شؤون عربية**، (العدد 35)، (تونس،1984) .ص 80.

[4]-John Baylis and Steve Smith, "**Globalization of world politics**", second edition, new York: Oxford University Press, 2001, p 255.

[5]– جون بيليس، ستيف سميث، **عولمة السياسة العالمية**، (دبي: مركز الخليج للأبحاث، ط1، 2004)، ص 414.

[6]– واري عبد الكريم، **الحلف اللأطلسي وإجراءات بناء الثقة في الفضاء المتوسطي**، مذكرة مقدمة لنيل شهادة الماجيستر في العلوم السياسية والعلاقات الدولية (جامعة: مولود معمري تيزي وزو، كلية الحقوق والعلوم السياسية، 2014/2013)، ص.39.

ويعرفه أرنولد وولفر"في حالة الأمن يكون النقاش دائرا على السعي للتحرر من التهديد أما إذا كان هذا النقاش في إطار النظام الدولي فإن الأمن يتعلق بقدرة الدول والمجتمعات على صون هويتها المستقلة وتماسكها العلمي"[1].

ومن خلال هذه التعاريف نستنتج أن الأمن هو القدرة على التحرر من تهديد رئيسي للقيم العليا الفردية والجماعية، وذلك من خلال جميع الوسائل الممكنة للحفاظ على حق البقاء على الأقل وهو غياب التهديد للقيم الأساسية التي تعترض استقرارها وطمأنينتها على المستوى الدولي.

الفرع الثاني: مفهوم السيبرانية والمفاهيم المشابهة لها

إن كلمة السيبرانية مؤخودة من كلمة سيبر cyber وهي صفة لأي شخص مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الإفتراضي؛ فالسيبرانية تعني فضاء الأنترنت وكذلك من كلمة "kybernetes" بمعنى الشخص الذي يدير دفة السفينة، حيث تستخدم مجازاً للمتحكم "Governor كما أن العديد من المؤرخين يرجعون أصلها إلى عالم الرياضيات الأمريكي 1964_1894 Norbert Wiener ذلك استخدمها للتعبير عن التحكم الآلي، فهو الأب الروحي المؤسس للسبرنيثيقية من خلال مؤلفه الشهير : Cybernetics or control and communication in the animal the machine و أشار في كتابه إلى أن السبرنيتيقية هي التحكم و التواصل عند الحيوان والآلة و الإنسان ليستبدل مصطلح الآلة بعد الحرب العالمية الثانية ليحل محله الكمبيوتر[2].

فأصبحت كلمة سايبر توضع أمام كل ما هو مرتبط بالإنترنيت، فهذا يعني ان المصطلح ظهر مع ظهور الإنترنيت وتعميم استخدام الرقمنة، في حين أن الأمن السيبراني ظهر حديثا وهو يعني مجمل القوانين السياسية، الأدوات، النصوص، وميكانيزمات الأمن وطرق تسير الأخطار والممارسات التكنولوجية المتعلقة بتكنولوجيات المعلومات والاتصالات المستخدمة لحماية الأفراد والدول والمنظمات، كما يعرف بأنها الحالة المرغوب فيها لعمل أنظمة المعلومات والاتصالات التي تمنحها القدرة على المقاومة لكل ما

[1]– جون بيليس، ستيف سميث، نفس المرجع، ص414.

[2]- جهاد ملحم، السوبرنية ضد قوانين الفزياء! عن الموقع:

http://wehda: alwehda . gov.sy / node :/3930792020/03/30).

ينجم عن هذا المجال السيبراني، و الذي من شأنه أن يعرض المعلومات المحزنة أو المعالجة أو المنقولة للتلف أو التغير أو التجسس[1].

1- القوة السيبرانية:

مما نلاحظه من الأمور المستقرة في العلاقات الدولية أن مصادر قوة الدولة وأشكالها تتغير، فإلى جانب أن القوة الصلبة المتمثلة في القدرات العسكرية والاقتصادية تزايد الاهتمام بالأبعاد غير المادية للقوة ومن ثم بروز القوة الناعمة، ومع ثورة المعلومات ظهر شكل جديد من أشكال القوة وهو القوة السيبرانية (Cyber Power) التي لها تأثير كبير على المستوى المحلي الدولي، فهو الذي أدى إلى إنتشار وتوزيع القوة بين عدد أكبر من الفاعلين مما جعل قدرة الدولة على السيطرة موضع شك، ومن جهة أخرى منحت الفاعلين الأصغر قدرة أكبر على ممارسة كل القوة الصلبة والناعمة عبر الفضاء السيبراني، وهذا ما يعني تغير في علاقات القوى في السياسة الدولية.

ويعد جوزيف .س.ناي Joseph .S. Ney من أبرز المهتمين بالقوة السيبرانية حيث يعرفها على أنها "القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني، أي أنها القدرة على استخدام الفضاء السيبراني لإيجاد مزايا الدولة والتأثير على الأحداث المتعلقة بالبيئات التشغيلية الأخرى وذلك عبر أدوات سيبرانية"[2]. كما يوضح أن مفهوم القوة السيبرانية يشير إلى "مجموعة الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات والشبكات الالكترونية والبنية التحتية المعلوماتية والمهارات البشرية المدربة للتعامل مع هذه المسائل".

ويتناول مفهوم القوة السيبرانية مجمل القضايا التي تتعلق بالتفاعلات الدولية العسكرية، الاقتصادية، السياسية، الثقافية والاعلامية...، ولممارسة نفوذ الدولة داخليا وخارجيا عبر القوة السيبرانية يجب توفر عناصر هي[3]:

- بنية مؤسسية: تتولى مهمة ممارسة القوة السيبرانية وتحقيق الأمن السيبراني للدولة .

- بنية تشريعية: تكون ضامنة ومحددة لاستعمال القوة السيبرانية .

[1]- ج رضوان، الأمن السيبراني: أولوية في استراتجيات الدفاع، **مجلة الجيش**، الصادرة عن مؤسسة المنشورات العسكرية، (العدد 630)، (جانفي 2016)، ص،40.

[2] Joseph .S.Ney ,jr**,cyber power**, harvard kennedy school, 2010. p4.

[3]Ibid,p10.

– بنية تحتية سيبرانية: تشمل أجهزة الكمبيوتر، شبكات الاتصالات والبرمجيات وقواعد البيانات لمختلف الأنظمة والقطاعات.

– استراتيجية بأهداف واضحة: تحدد طرق العمل والأهداف المرجوة .

2_ الفضاء السيبراني:

يعد الفضاء السيبراني فريد من نوعه حيث أنه حديث النشأة كما أنه يخضع للتغيرات التكنولوجية، وكان لظهور الانترنت وثورة المعلومات الفضل في بروز السيبرانية أو السيبيري وخلق عالم جديد وهو الفضاء السيبراني.

فالفضاء السيبراني هو مجال افتراضي من صنع الإنسان يعتمد على نظم الكمبيوتر وشبكات الأنترنيت ومجموعة هائلة من الأجهزة والمعلومات والبيانات فحسب عباس بدران هناك من عرف الفضاء السيبراني[1] بوصفه الذراع الرابع للجيوش الحديثة، وكذلك هناك البعض الآخر الذي يرى بأنها البعد الخامس للحرب وهذا التعريف يحصر الفضاء السيبراني في الجانب العسكري دون الولوج إلى المجالات الأخرى.

كما عرفته الوكالة الفرنسية لأمن أنظمة الإعلام (ANSSI) وهي وكالة حكومية فرنسية مهمتها الدفاع السيبراني الفرنسي وتعرفه على أنه "فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية"[2] فهذا التعريف يركز على الجانب التقني كما يغفل العامل البشري والذي يعد جزء جد أساسي في فهم الفضاء السيبراني.

ويعرفه الإتحاد الدولي للاتصالات على أنه: "المجال المادي وغير المادي الذي يتكون وينتج من عناصر هي: أجهزة الكمبيوتر، الشبكات، البرمجيات، حوسبة المعلومات، المحتوى، معطيات النقل والتحكم ومستخدموا كل هذه العناصر"[3].

[1]- عباس بدران، **الحروب الالكترونية.الاشتباك في عالم متغير**، (بيروت: مركز دراسات الحكومة الالكترونية، 2010).ص،4.

[2]– اسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، **مجلة العلوم القانونية والسياسية**، (م 10)،(ع 1)، (أفريل 2019).ص،1017.

[3]-The International Telecommunication Union (ITU), Toolkit For Cyber Crimel Legisalation, Geneva, 2010. P,12.

ومنه فالفضاء السيبراني هو بيئة تفاعلية حديثة تشمل عناصر مادية وغير مادية، مكون من مجموعة من الأجهزة الرقمية وأنظمة الشبكات والبرمجيات والمستخدمين سواء مستعملين أو مشغلين، ومنه فمسألة تحديد المفهوم "الفضاء السيبراني"، هي مسألة نسبية تتوقف على طبيعة إدراك وفهم كل من الدول والهيئات، كل حسب رؤيته واستراتيجيته وقدرته على استغلال المزايا المتاحة ومواجهة المخاطر الكامنة في هذا الفضاء.

المطلب الثاني: مفهوم الأمن السيبراني

تتنوع المفاهيم والتعاريف التي تدور حول مفهوم الأمن السيبراني بتعدد المفكرين والباحثين في هذا المجال وكذلك المفاهيم المرتبطة والمشابهة له وسنحاول التطرق إليها من خلال مايلي:

الفرع الأول: تعريف الأمن السيبراني

تتعدد وتختلف التعريفات حول مفهوم الأمن السيبراني وتعتبر مهمة ضبط المفاهيم والمصطلحات تحديا يواجه مختلف الباحثين والدارسين في مختلف التخصصات إذ من الصعوبة في حديد والاتفاق على تعريف واحد وشامل بين الجميع ويعتبر الأمن السيبراني أحد المفاهيم المعقدة التي قدمت لها العديد من التعريفات المختلفة .

السيبراني هو واحد من المصطلحات الأكثر ترددا في معجم الأمن الدولي، و تشير كلمة "cyber" إلى أنها لفظة يونانية الأصل مشتقة الآلة [1]،بمعنى التوجه والسيطرة والإنسان والآلة ليستبدل مصطلح الآلة بعد الحرب العالمية الثانية بالحاسوب، أما اصطلاحا: فهناك العديد من التعريفات التي قدمت لمفهوم الأمن السيبراني منها:

-يعرف على أنه مجموعة من الإجراءات المتخذة دفاعا ضد الهجمات الالكترونية وعواقبها ويشمل ذلك تنفيذ التدابير المضادة المطلوبة،فهو مبني على تحليل التهديدات لمنظمة أو مؤسسة .وحسب الاتحاد الدولي للاتصالات فإن الأمن السيبراني ليس غاية في حد ذاته فهو يعد وسيلة لتحقيق غاية[2]

[1]-ـــــ، الموسوعة السياسية، الأمن السيبراني/https://political-encyclopedia.org/dictionary، (2020/02/25)، الساعة 21:17.

[2]Martti Lehto ,and Pekka Neinaamaki, Cyber Security :Analyics ,Technology and Automation,(Department Of Mathematical Information Technology, University of Finland).2014.p25.

– تعريف ريتشارد كمرر richard a Kemmerer الذي يرى أنه عبارة عن وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القراصنة[1].

– يعرفه إدوارد أمورسو على أنه وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات وتشمل تلك الوسائل والأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها[2].

– يعرفه الإتحاد الدولي للاتصالات في تقرير له حول "اتجاهات الإصلاح في الاتصالات لعام 2010–2011" على أنه مجموعة من المهمات مثل: تجميع وسائل وسياسات وإجراءات أمنية ومبادئ توجيهية ومقاربات لإدارة المخاطر وتدريبات وممارسات فضلى وتقنيات يمكن استخدامها لحماية البيئة السيبرانية [3] إلى جانب موجودات المؤسسات والمستخدمين فيها.

– تعرف وزارة الدفاع الأمريكية "البنتاغون" الأمن السيبراني أنه جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والإلكترونية من مختلف الجرائم وهجمات التخريب والتجسس [4].

مفهوم الأمن السيبراني:

هو مفهوم ظهر بعد الحرب الباردة استجابة للمزيد من الابتكارات التكنولوجية والظروف الجيوسياسية المتغيرة تم استخدامه لأول مرة من علماء الكمبيوتر في أوائل التسعينات للتأكيد على سلسلة من حالات عدم الأمان المرتبطة بأجهزة الكمبيوتر لكنه تجاوز مفهومها التقني لأمن الكمبيوتر عندما حث المؤيدون على أن تهديدات الشاشة والتقنيات الرقمية يمكن أن يكون لها آثار اجتماعية مدمرة.

كما يعرف أيضا لعملية أو قدرة الدولة، والتي بموجبها حماية أنظمة الاتصالات والمعلومات الواردة إليها والدفاع عنها ضد الضرر أو الاستخدام غير المصرح به. والأمن السيبراني هو أمن الشبكات والأنظمة المعلوماتية والبيانات والمعلومات والأجهزة المتصلة بالانترنيت.

---

[1]-Richard A Kemmerer**, Cyber Security**, University Of California Santa Barbara, Department Of Computer Science 2003, p3.

[2]-Edward amoroso, **cyber security**, silicon press ,2007, p10.

[3]-ITU ,**Cyber Security**, Geneva: International Telecommunication Union (ITU),2008,p.

[4] -ـــــ، الموسوعة السياسية، الأمن السيبراني/https://political-encyclopedia.org/dictionary، (2020/02/25)، الساعة 21:10.نفس المرجع.

ومن خلال هذه التعاريف يمكن إعطاء تعريف للأمن السيبراني على أنه النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات ويضمن إمكانات الحد من الخسائر والأضرار التي تترتب في حال تحقيق المخاطر والتهديدات كما يتيح إعادة الوضع إلى ما كان عليه بأسرع وقت ممكن بحيث لا تتوقف عجلة الإنتاج بهدف ضمان توافر استمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني وكل الأجهزة المرتبطة بالانترنيت.

ومن خلال هذه التعاريف نستنتج أن هدف الأمن السيبراني هو القدرة على مقاومة التهديدات المتعددة، وبالتالي من الخطر أو الأضرار الناجمة عن تعطيل أو إتلاف تكنولوجيا المعلومات والاتصالات[1] وهذا ما يؤدي بالضرورة إلى حماية الشبكات وأجهزة الكمبيوتر والبرامج والبيانات من الهجوم أو الضرر.

ومنه نتيجة لأهمية الأمن السيبراني في واقع مجتمعات اليوم فقد جعلته العديد من الدول على رأس أولوياتها خاصة بعد الحرب الإلكترونية التي بدأت تظهر تجلياتها في الآونة الأخيرة بين الدول الكبرى، في إشارة إلى نهاية الحرب التقليدية ذات الأسلحة إلى حروب جديدة هي الحروب الالكترونية[2]، ولهذا أصبح لازما على الدول التي تريد الحفاظ على أمنها واستقرار سيادتها أن تهتم اهتماما بالغا بمسألة تحقيق الأمن السيبراني.

الفرع الثاني: المفاهيم المشابهة للأمن السيبراني

1- الصراع السيبراني:

يختصر الفضاء السيبراني حاجز الزمان والمكان ويخلق مساحات للتفاعلات الداخلية والدولية في الواقع الإفتراضي ومن ثم برزت فضاءات جديدة للصراع بأدوات مختلفة وأنماط جديدة تختلف عن الصراعات التقليدية، فبعد أحداث 11 سبتمبر 2001 كان الفضاء السيبراني ساحة الصراع والقتال بين تنظيم القاعدة والولايات المتحدة الأمريكية، وجاء الهجوم بفيروس "ستاكسنت" على برنامج إيران النووي في 2012 ليبرز قوة الأسلحة السيبرانية في الصراعات الدولية.

[1]- بن مرزوق عنتر، **الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية**،ورقة بحثية قدمت في ملتقى (المسيلة: جامعة محمد بوضياف، كلية الحقوق والعلوم السياسية) ص67.

[2]- مرجع سابق ،ص،67.

فأية محاولة بحثية لفهم طبيعة الصراع السيبراني تستلزم بالأساس نمطا من المقاربات العابرة للتخصصات الإنسانية والتقنية نظرا لتمازج أهداف البيئتين الإفتراضية والواقعية عند نشوب التنازع الإلكتروني وهذا ما أدى إلى تداخل الصراعات السيبرانية التقليدية والحديثة.

وحسب عادل عبد الصادق فإن أبرز ما يعزز انتشار الأسلحة غير السلمية في الفضاء السيبراني هو:

1_ ارتباط العالم المتزايد بالفضاء السيبراني وزيادة خطر تعرض البنية التحتية الكونية للمعلومات لهجمات سيبرانية.

2_ استخدام الفاعلين من غير الدول للفضاء السيبراني لتحقيق أهدافهم وتأثير ذلك على سيادة الدولة.

3_ انسحاب الدولة من قطاعات استراتيجية لصالح القطاع الخاص.

4_ إشكالية تعامل الدول مع الشركات التكنولوجية متعددة الجنسيات والتي أصبحت تفوق قدرتها[1] مثل: مواقع التواصل الاجتماعي التي أصبحت فواعل دولية بامتياز.

ومنه فقد أصبح الفضاء السيبراني ساحة جديدة للصراع بشكله التقليدي ولكنه ذو طابع سيبراني يعكس النزاعات التي تخوضها الدول أو الفاعلين من غير الدول على خلفيات دينية أو عرقية أو آديولوجية أو اقتصادية أو سياسية، و يتمدد الصراع السيبراني بداخل شبكات الإتصال والمعلومات متجاوزا الحدود التقليدية وسيادة الدول.

وكشف استخدام الفضاء السيبراني عن حالة التعارض الحقيقي للإحتياجات والقيم والمصالح بين العديد من الفاعلين، وساعد ذلك على ظهور أساليب جديدة للصراع الدولي، تنوعت بين الطابع التقني والتجاري والاقتصادي والعسكري، إلى جانب ظهور طرق بديلة عن الحرب المباشرة بين الدول عبر شبكات الاتصال والمعلومات.

فهناك صراع سيبراني تحركه دوافع سياسية ويأخذ شكلا عسكريا ويتم فيه استخدام قدرات هجومية ودفاعية عبر الفضاء السيبراني، كما يوجد صراع سيبراني ذو طبيعة ناعمة حول الحصول على المعلومات والتأثير في المشاعر والأفكار وشن حروب نفسية وإعلامية، كما يأخذ الصراع السيبراني طابعا

[1] عادل عبد الصادق،**أسلحة الفضاء الالكتروني في ضوء القانون الدولي**،سلسلة أوراق(العدد23)،2016،ص ص.11،10.

تنافسيا حول الإستحواذ على التقدم التكنولوجي وسرقة الأسرار الاقتصادية والعلمية، والتحكم بالمعلومات والعمل على اختراق الأمن القومي للدول، كهجمات قراصنة الكمبيوتر بما له من تأثير على تدمير الإقتصاد والبنية التحتية بنفس القوة التي قد يسببها تفجير تقليدي مدمر، كذلك يمكن أن يستخدم الفضاء السيبراني كوسيلة من وسائل الصراع داخل الدولة بين مكوناتها، على أساس طائفي أو اقتصادي أو ديني.

ومنه يعرف الصراع في الساحة الافتراضية كونه استخدام تكنولوجيا الحاسوب في الفضاء السيبراني الإلكتروني لأغراض التدمير من أجل التخريب أو التغيير أو التعديل في التفاعلات الدبلوماسية والعسكرية بين الكيانات المختلفة.

2- الأمن المعلوماتي: ولقد شاع في عصرنا الحالي أن أمن المعلومات (Information Security) يحدث ثورة في عالم الإتصالات عموما وأمن المعلومات على وجه الخصوص وهو حسب خالد ابراهيم الذي تناوله في ثلاثة زوايا مختلفة وهي[1]:

أ- الزاوية الأكاديمية: ويقصد به العلم الذي يبحث في نظريات واستراتيجيات ووسائل حماية المعلومات من المخاطر التي تهددها وحمايتها من أي نشاط اعتدائي ضار قد يؤثر على جوهرها.

ب- الزاوية التقنية: وتشير إلى الإجراءات والأدوات التكنولوجية الواجب توافرها لحماية المعلومات من التهديدات سواء داخلية أو خارجية.

جـ - الزاوية القانونية: تتناول الدراسات وتدابير الحماية والسرية لتوفير الغطاء الأمني والقانوني للمعلومات، ومكافحة أي أنشطة تهدد لاستغلالها أو تنظيمها لارتكاب الجرائم وسن التشريعات القانونية الهادفة لحماية الأنشطة غير المشروعة.

ومنه فأمن المعلومات الإلكترونية هو عبارة عن البيانات في جميع أشكالها الإلكترونية والورقية وحسب (عليان ربحي) الذي يعرف أمن المعلومات على أنه "عمليات الحماية الأمنية والتقنية للمجتمعات التي يتعامل أفرادها ومؤسساتها مع المعلومات ووسائل الإتصالات خاصة في تسيير قطاعاتهم المختلفة، القطاعات الاقتصادية والاجتماعية والصحية والتربوية والثقافية والأمنية والسياسية "[2] ؛ ومنه فهذه

[1]- ابراهيم خالد، **أمن المعلومات الالكترونية**، (الاسكندرية: دار الجامعية للنشر، 2008). ص،27.

[2]- عليان ربحي، **مجتمع المعلومات والواقع العربي**، (عمان: دار جرير للنشر والتوزيع ، ط1، 2006). ص.28.

المجتمعات تتحول إلى مجتمعات الكترونية ومعلوماتية وبالتالي حماية مصالحها من أي خطر يهدد أمنها المعلوماتي.

وينقسم إلى قسمين:

الأول: أمن الوثائق العادية

تأمين الوثيقة يعني حمايتها من التزوير أو التزييف، وذلك بوضع عقوبات وصعوبات في طريق كل من يحاول تزويرها أو تزييفها حيث يسهل كشف التزوير في الوثيقة المزورة وإظهار فوارق واضحة بين الوثيقة الصحيحة والوثيقة المزيفة هذا ما يخص في حالة التزييف.

الثاني: أمن الوثائق والمعلومات الالكترونية

هو مجموعة الإجراءات والقواعد والتشريعات التي توضع للحفاظ على سلامة وتكامل نظام المعلومات من التخريب والبث والفقدان[1]، وكذلك من التغير و الإستعمال غير المسموح به سواء كان هذا التخريب أو التغيير مقصود أو غير مقصود.

3- الفرق بين أمن المعلومات والأمن السيبراني

إن أمن المعلومات والأمن السيبراني هما مصطلحان متشابهان لكنهما ليسا متطابقين؛ فأمن المعلومات من حيث التعريف هو أعم وأوسع من الأمن السيبراني ولعل التخصيص هنا يكمن بالتركيز على مجال الأمن السيبراني بوصفه مجالا من مجالات العلم فهو أمر مفيد للغاية فعلم الحاسب الآلي وعلم التشفير مثلا اشتق لأول مرة من علم الرياضيات التطبيقية لأهميتها ثم ما لبثت هذه المجالات العلمية حلقت في فضاء العلم الرحب لتتمدد وتتوسع وتخرج خارج الأطر العلمية لمجالها الأب وهو الأمر ذاته لمجال الأمن السيبراني ، ويعتبر مفهوم الأمن السيبراني أوسع من أمن المعلومات من حيث تأمين المعلومات التي تتداول عبر الشبكات الداخلية أو الخارجية والتي يتم تخزينها داخل أو خارج المنظمات من الاختراقات الالكترونية وهذا هو أحد أهم الأسباب لإنشاء الأمن السيبراني الذي يتمثل في حماية البيانات الالكترونية، وأمن المعلومات يهتم بحماية البيانات في جميع أشكالها.

[1]- ساسي محمد بشير، **الأمن في القصص القرآني**، بحث لاستكمال متطلبات الحصول على الماجيستر في التفسير، (الجامعة الاسلامية غزة: كلية أصول الدين، قسم التفسير 2012). ص.12.

المبحث الثاني: الأبعاد والمداخل النظرية للأمن السيبراني

ونتناول في هذا المبحث الأبعاد الأساسية التي بقوم عليها الأمن السيبراني وأهم المقاربات النظرية المفسرة لذلك.

المطلب الأول: أبعاد الأمن السيبراني

يدور الأمن السيبراني حول مسائل اقتصادية وعسكرية وسياسية... وانطلاقا من تعريفه فهو قدرة الدولة على حماية مصالح شعبها في مختلف مجالات الحياة، ونقصد به البيانات والمعلومات والقدرة على الاتصال والتواصل وهو المحور الذي يرتكز حوله الإنتاج والإبداع و القدرة على المنافسة ومنه نذكر أبعاد الأمن السيبراني كما يلي.

الفرع الأول: البعد العسكري

ويكمن هذا البعد في الحفاظ على قدرة الوحدات العسكرية على التواصل عبر الشبكات العسكرية، مما يسمح بتبادل المعلومات والأوامر وتدفقها والذي يرجح إلى أن بدايات الأنترنت كانت في بيئة عسكرية بشكل أساسي، لتنقل فيما بعد الى الأوساط العلمية والأكاديمية وتمثلت في الأبحاث التي تخدم القدرات العسكرية، وتطورها والإنجازات العلمية التي تسهم في تفوق بلد على آخر حيث كان التنافس على أشده خلال الحرب الباردة، في مجال الوصول الى الفضاء الخارجي وتطوير الأسلحة النووية[1] وإصابة الأهداف عن بعد، إلا أنها تمثل كذلك نقطة ضعف خاصة إذا لم تكن مؤمنة جيدا من الإختراق الذي قد يؤدي الى تدمير قواعد البيانات العسكرية أو قطاع الإتصال بين القيادة والوحدات العسكرية، فضلا عن إمكانية التحكم في بعض الأسلحة وخروجها عن السيطرة.

وتكمن الميزة النسبية للقوة السيبرانية في قدرتها على ربط الوحدات العسكرية ببعضها البعض عبر الشبكات العسكرية في الفضاء الإلكتروني بما يسمح بسهولة تبادل المعلومات وتدفقها و سرعة اتخاذ القرارات العسكرية ومن ثمة تحقيق الأهداف عن بعد ومن دون شك، فإن عدم استغلال هذه التقنية

[1] –سمير بارة ،"الأمن السيبراني في الجزائر السياسات والمؤسسات"، **المجلة الجزائرية للأمن الإنساني**، (العدد الرابع)، (جويلية 2017)، ورقلة: جامعة قاصدي مرباح، ص،260.

والتسلح بها أو تأمينها بشكل جيد من أي اختراق خارجي سيؤدي بالضرورة إلى شن هجمات إلكترونية مضادة على شبكات القوات العسكرية ومن ثم تدمير قواعد البيانات وما يلحقه من مخاطر[1].

ويعتبر فيروس ستا كسنت stuxent بداية لاستعمال القوة السيبرانية لتدمير البنية المادية في عملية تخصيب اليورانيوم و مثال على ذلك هذا الفيروس هاجم حواسيب أجهزة الطرد المركزي الإيرانية من قبل الشركة الألمانية سيمنز Siemens، وبعد أن قامت بعملية الاختراق قامت بالتحكم في سرعة أجهزة الطرد التي زادت من سرعتها إلى الحد الذي يلحق بها الضرر واستطاعت هذه الدودة أن تحمي نفسها، وقد كان للولايات المتحدة الأمريكية وإسرائيل دور إلا أنهما لم يعترفا بذلك إلا أن هناك عدة عوامل تؤكد أن هذا الهجوم تطلب إمكانات لا يمكن لفواعل من غير الدول أن تمتلكها وتتمثل في:

– عند القيام بهذا الهجوم كان لابد من توافر معلومات إستخبارية تقنية تتعلق بالتكنولوجيا التي تستخدمها إيران في منشآتها النووية، والتي يصعب على فواعل من غير الدول الحصول على هذه المعلومات.

– توافر قدرات برمجية وتجريبية متقدمة حتى يمكن تصميم دودة بهذه الدرجة من التعقيد.

ومنه نتاج هذا الهجوم أعلنت إيران في 2010 أن أجهزة الطرد للمفاعل النووي تم تدميرها، ولم تتمكن من افتتاحه في الوقت المحدد إذ تم افتتاحه في 2011، بعد خسارة مليارات الدولارات في إصلاح ما أفسدته هذه الدودة[2]. وهذا ما ذهب إليه حمدون توريه في البحث عن السلام السيبراني بقوله أن الهجمات يمكن أن تأتي دون مقدمات فالحواسيب والهواتف المحمولة تتوقف عن العمل فجأة، كما أن شاشات آلات الصرف والآلات المصرفية تنطفئ في وجه العملاء وتتعطل أنظمة مراقبة الحركة الجوية، البرية، البحرية، وتتوقف السلع عن السكان الجائعين، ومع اختفاء الكهرباء تذهب أو تزول جميع المساكن والمستشفيات والمراكز والمجتمعات بأكملها في غياهب الظلمات ولن تستطيع السلطات الحكومية معرفة مدى الضرر أو الاتصالات ببقية العالم للإبلاغ بالكارثة وحماية المواطنين الضعفاء من الهجمات وهذه هي التي يعاني منها أو يواجهها المجتمع بفعل تعرضه للشلل بسبب ضياع شبكاته الرقية في لحظة وهذا هو التدمير الذي يمكن أن ينجم عنه نوع جديد من الحروب ألا وهي الحروب السيبرانية.

الفرع الثاني: البعد الاقتصادي

[1]– محمد مختار، "هل يمكن أن تتجنب الدول مخاطر الهجمات الإلكترونية"، **مجلة اتجاهات الأحداث**، (العدد 6)، (يناير 2015)، ص ص.6_8.

[2]-Fred Schreier **, On Cyber warfare**, DCAF Horizon 2015 Working Paper Series , Issue 7. pp87-90.

لقد أصبح الفضاء الإلكتروني جاذبا لقطاعات المجتمع كافة وباتت المعرفة محرك الإنتاج والنمو الاقتصادي، كما أيقن الجميع أن مبدأ التركيز على المعلومات والتكنولوجيا أصبح عاملا من العوامل الأساسية للنهوض بالاقتصاد[1] وأصبحت الإنترنيت أساس المعاملات التجارية والمالية والاقتصادية كما تستعمل الحواسيب في تسيير وتطوير الصناعات وتحريك الاقتصاد، وأصبح الكل مترابطا عبر شبكات الكمبيوتر مما يستدعي الحديث عن أهمية تحقيق الأمن السيبراني في المجال الاقتصادي، لتعزيز الأمن الرقمي للمؤسسات والشركات الاقتصادية وليست الغاية تحقيق الكسب والأرباح الطائلة فقط وإنما تفادي السقوط في الخسائر المكلفة[2]، كما أن استخدام الكمبيوتر وشبكة الانترنت في تطوير الصناعات وإدارة الاقتصاد ومعالجة كل المعاملات الاقتصادية والمالية زاد من أهمية ضرورة توفير الأمن السيبراني لضمان حماية هذه المعلومات.

الفرع الثالث: البعد السياسي

تتمثل الأبعاد السياسية للأمن السيبراني بشكل أساسي في حق الدولة في حماية نظامها السياسي وكيانها ومصالحها الاقتصادية التي تفي حقها وواجبها في السعي إلى تحقيق رفاه شعبها في وقت تؤثر التقنيات في موازين القوى داخل المجتمع نفسه.

حيث أصبح بإمكان المواطن أن يتحول إلى لاعب أساسي في العملية السياسية[3]، وهناك أمثلة كثيرة تدفع نحو الاهتمام بالبعد السياسي للأمن السيبراني كالتسريبات المختلفة للوثائق والبيانات الحساسة للدولة والأفراد التي تؤدي إلى مشكلات عويصة جدا على المستوى الخارجي والدولي كما أنه لا ينكر الدور المتعاظم لشبكات التواصل الاجتماعية على المستوى السياسي .

ولا يتوانى العاملون في الشأن السياسي عن الإفادة بما تقدمه هذه التقنيات للوصول إلى أكبر شريحة ممكنة من المواطنين والترويج لسياستهم، مثال على ذلك استخدام أوباما لشبكات التواصل

[1] – بارة سمير، **مرجع سابق**، ص 261.

[2] – نضال ناجي بدوي بريوش، **الصراع السيبراني مع العدو الصهيوني**، بحث مقدم لاستكمال متطلبات الحصول على دبلوم الدراسات الفلسطينية، (أكاديمية دراسة اللاجئين الفلسطينيين: قسم الأبحاث والمشاريع، دبلوم الدراسات الفلسطينية، 2019/2018)، ص 17.

[3]– منى الأشقر جبور، "**الأمن السيبراني التحديات ومستلزمات المواجهة**"، جامعة الدول العربية، المركز العربي للبحوث القانونية والقضائية، اللقاء السنوي الأول للمتخصصين في أمن و سلامة الفضاء السيبراني، بيروت 27_28، أغسطس 2012.ص. 16.

الإجتماعي خلال الحملة الإنتخابية مما أدى ذلك الى حدوث تسريبات لآلاف الوثائق الدبلوماسية [1]، حيث تركت هذه التسريبات أثرا سلبيا على العلاقات بين الدول وعلى مصداقيتها.

الفرع الرابع: البعد الاجتماعي

تسمح طبيعة الأنترنيت المفتوحة عبر المدونات والشبكات الإجتماعية لكل مواطن بأن يعبر على تطلعاته السياسية والإجتماعية على مشاركة جميع شرائح المجتمع ومكوناته وسيلة لتطور المجتمع لأنه يتيح فرصة الإطلاع على الأفكار والمعلومات المختلفة، لأن انفتاح مجتمع ما على آخر يؤدي إلى تبادل الخبرات والأفكار وتكوين حاجات جديدة وآفاق تعاون وتكامل[2] في المجالات العلمية والثقافية والخدماتية بفضل تبادل المعلومات. وتقف هذه الأبعاد عند حدود توفير الإطمئنان للمواطن في حياته اليومية وصيانة القيم الجوهرية في المجتمع كالانتماء المعتقدات العادات والتقاليد .

ومن الضروري تعميم مفهوم الأمن الصحيح والسليم لكل المشتركين في الشبكة الدولية للمعلومات وينبغي التشديد على واجب الأمن وجعل الشبكة الدولية مجالا مفتوحا للجميع، وجعل كل المستخدمين والعاملين على الشبكة الدولية للمعلومات آمنين بعيدين عن الأخطار السيبرانية التي تهدد السلم والأمن المجتمعي وتحمل المسؤولية للأفراد والمجتمع تجاه ما يسمى الدولة والمجتمع من عدم احترام الالتزامات التي يوجبها الأمن.

الفرع الخامس: البعد القانوني

يرتبط النشاط الفردي والمؤسساتي والحكومي في المجال السيبراني عن نتائج قانونية تستدعي اهتماما خاصا بحل النزاعات التي يمكن أن تنشأ عنها[3]، وهو ما يستدعي مواكبة التحولات التي رافقت ظهور مجتمع المعلومات بفعل التطورات التكنولوجية المتسارعة التي تفرض مواكبة التشريعات القانونية لها لأن الجريمة السيبرانية تفتقد في معظم الحالات و البلدان أطر قانونية صارمة للتعامل معها وضرورة تفعيل التعاون على المستوى الدولي لمكافحتها التي تستدعي وجود ترسانة قانونية تنسجم مع التطورات الحاصلة كما توسعت بعض المفاهيم كحق النفاذ إلى شبكة المعلومات لتشمل أساليب الممارسة الجديدة

[1]– المرجع نفسه، ص،18.

[2]– نضال ناجي بدوي بريوش، مرجع سابق. ص 18.

[3]– منى الأشقر جبور، **الأمن السيبراني التحديات ومستلزمات المواجهة**، مرجع سابق، ص 17.

باستخدام تقنيات المعلومات والاتصالات كالحق في إنشاء المدونات الإلكترونية وإنشاء التجمعات على الأنترنت وله الحق أيضا في حماية ملكية البرامج المعلوماتية [1].

المطلب الثاني: المداخل النظرية للأمن السيبراني

هناك العديد من النظريات والمقاربات النظرية في تفسير الأمن في المجال السيبراني ما تعلق بالعلاقات الدولية أو السياسة الدولية على حد سواء خاصة منها في الجانب الأمني وتطوره في خضم هذه النظريات خاصة وأننا اعتمدنا على نظريات تقليدية وحديثة ومواكبتها لتطور الأمن السيبراني في السياسة الدولية و قد تناولنا المنظور الواقعي و المنظور الليبرالي و كذلك المنظور البنائي و نذكر منها:

الفرع الأول: المنظور الواقعي للأمن السيبراني في السياسة الدولية

ونتناول في هذه المقاربة ما يلي:

أولا: السياق التاريخي للنظرية للواقعية ومرتكزاتها

تعود أصول النظرية الواقعية السياسية إلى العهد اليوناني ويمكن إرجاعها إلى المؤرخ الإغريقي ثيوسيديدس–Thucydides، الذي عاش في القرن الخامس قبل الميلاد ويعتبر كتابه تاريخ الحرب البيلوبونيزية–History of The Peloponnesian، تأصيل للصراعات الدولية من حيث السياسة والقوة، فترجع الواقعية السياسة إلى اللاأخلاقية المكيافيلية–Machiavellanism لأن الواقعية مسترخية في قلب النظرية السياسية لـ: نيكولا مكيافيلي–Nicolas Machiavel لذلك يعتبر قطبا من أقطاب الواقعية السياسية لأن هذه الواقعية حسبه منبثقة من قلب النظرية السياسية[2].

كما يعد توماس هوبز–Thomas Hobbes من أبرز المساهين والمفسرين للفكر الواقعي بالأفكار التي قدمها عن حالة الطبيعة، فاعتمادها في دراسة العلاقات الدولية تبلور عنه عنصرين فالأول هو التمييز بين حقل السياسة الداخلية والخارجية للدول، والثاني هو أن العلاقات الدولية هي من اختصاص الدول ذات السيادة وصاحبة سلطة الإكراه[3].

---

[1]– منى الأشقر جبور،"**السيبرانية هاجس العصر**،"جامعة الدول العربية :المركز العربي للبحوث القانونية والقضائية. ص.31.

[2]–أنور محمد فرج،"**النظرية الواقعية في العلاقات الدولية**"،(كردستان: مركز كردستان للدراسات الاستراتيجية ،2007) .ص ص 175،184.

[3]– **المرجع نفسه**، ص.205.

ويعتبر هانز مورغانثو–Hans Morgenthau أب النظرية الواقعية السياسية ، ويقدم في كتابه "السياسة بين الأمم" ما يعتبره المبادئ الست في الواقعية وهي:

أن السياسة كالمجتمع والمصلحة هي أداة التحليل الرئيسية (أي بمفهوم القوة) وهي مفهوم متغير بتغير الزمان والمكان وكذلك لا يمكن تطبيق المبادئ الأخلاقية بمفهومها المجرد على الدول، كما ترفض أن تكون هذه المبادئ متطابقة مع قيم دولة ما وتركز على إستقلالية المجال السياسي [1].

أما عن النظرية الواقعية الجديدة فإن كينيث والتز–Kenneth Waltz في "كتابه نظرية السياسة الدولية–Theory of International Politics" المؤسس الفعلي للواقعية الجديدة فقد اعتمد فيها على الإختيار العقلاني لاستخدام القوة لتحقيق الأهداف المرجوة وتحديثه لنظرية النظام الدولي، ويقوم "والتز" بانتقاد الواقعيين من أمثال "هانز مورغانتو" و"هنري كسنجر–Henry Kissinger، وريمون آرون–Raymond Aron، وستانلي هوفمان–Stanely Hoffmann، لسماحهم بمزج السياسة الداخلية في نظرياتهم بالصراع أما هو فيسعى إلى تفسير السياسات الدولية على أساس بنية النظام وحدها دون أي اعتبار على الإطلاق للطابع الداخلي للأمم المكونة له[2].

من هذا المنطلق فإن الواقعية الجديدة عند "والتز" تقوم على الافتراضات الآتية:

إن الدولة هي الفاعل الرئيسي والوحيد في العلاقات الدولية، وفوضوية النظام الدولي والهدف الأساسي لهذه الدول هو الحفاظ على بقاءها عن طريق تعزيز أمنها ولا وجود للثقة بين الدول في سعيها نحو البقاء وتحقيق ذلك فهي إذن فاعل عقلاني تتعامل في ظل نظام دولي غير دقيق لأن معلوماته ناقصة[3].

ثانيا: الأمن السيبراني في النظرية الواقعية التقليدية والجديدة

إن النظرية الواقعية تنظر بشكل أساسي للدولة على أنها هي الأساس والمركز لأن وجود الفوضى الدولية هو ما يخلق المعضلة الأمنية ومنه يتقاطع أنصار هذا المنظور مع مجالات الفضاء السيبراني كما هو الحال في تعاملهم مع العديد من الظواهر كالإعتماد المتبادل والعولمة مثلا كتحديات

[1]– ناصيف يوسف حتي، "**النظرية في العلاقات الدولية**"، (بيروت: دار الكتاب العربي، ط1، 1985)، ص.27.

[2]– أنور محمد فرج، **مرجع سابق**، ص.362.

[3]– أحمد نوري النعيمي، "البنيوية العصرية في العلاقات الدولية "، **مجلة العلوم السياسية**، (العدد،46)، (2013)، ص.49.

جديدة في الساحة الدولية، فالجميع من وجهة نظرهم تؤثر في الدولة داخليا فهي لاتقلل لا من فوضوية النظام العالمي ولا من أهمية الدولة كفاعل رئيسي في مجال العلاقات الدولية حيث يرون من ذلك تهديدا للأمن القومي للدولة وهو مايهدد سلامتها وبقاءها ولذلك نجد أن ظاهرة الأمن أو الصراع في الفضاء السيبراني ضمن الدراسات الإستراتيجية والأمنية التابعة للمنظور الواقعي، حيث يعتبر الواقعيون هذا التغير تغير طبيعيا وليس مفاجئا خاصة في حقل العلاقات الدولية عامة والسياسة الدولية خاصة[1].

تنظر الواقعية سواء التقليدية أو الجديدة للأمن السيبراني باعتباره مجالات غير ملائمة للدراسة من قبل باحثي العلاقات الدولية، فهي مجالات تُحال دراستها لمختصي السياسة الداخلية وذلك اتساقا مع صيغة الفصل بين النظام الداخلي وبين الخارجي التي تتبناها الواقعية.

ينظر الواقعيون للأمن السيبراني بوصفه أداة توظيف سياسيةا من قبل الدولة –باعتبارها لاعبا احتكاريا ، يتمتع بإرادة واحدة – لتحقيق المصالح القومية ، فالدول ترى أن هذه الروابط التكنولوجية هي التي تحقق مصلحتها.

الفرع الثاني: المنظور الليبرالي للأمن السيبراني في السياسة الدولية

ونتناول في هذه المقاربة النظرية مايلي:

أولا: البناء المعرفي والنظري للنظرية الليبرالية والليبرالية الجديدة

عرفت أكاديميا كأولى المجالات التنظيرية للعلاقات الدولية بعد تأسيس حقل العلاقات الدولية في بداية القرن العشرين، وسعت إلى تغيير الوضع الدولي المليء بالصراعات والنزاعات واستبداله بعالم خال من الحروب يسوده السلام، ويتمحور هدف الليبرالية في البحث عن وسائل وآليات تعمل على نزع فتيل الحرب وتجنب الأسباب التي تؤدي إليها، بالإضافة إلى تأسيس العلاقات الدولية على قواعد جديدة تضمن عدم العودة للحروب، ويرتبط المنظور الليبرالي المنافس للواقعية بالمحللين الكلاسيكيين أمثال جون

[1]– سماح عبد الصبور، "الصراع السيبراني طبيعة المفهوم وملامح الفاعلين"، **مجلة السياسة الدولية:** اتجاهات نظرية في تحليل السياسة الدولية، (م 52)، (ع 208)، (أفريل 2017). ص 8.

لوك–John Locke، وجيرمي بنثام–Jeremy Bentham، وإيمانويل كانت–Emmanuel Kant، الذين مهدوا فكريا وفسلفيا لما دُعي فيما بعد بالمذهب الليبرالي[1].

وتنطلق النظرية الليبرالية من الافتراضات الآتية:

– تؤدي الدولة دورا فاعلا في العلاقات والسياسية الدولية ولها قوى فاعلة أخرى من غير الدولة تؤدي دورا في النظام الدولي، الذي تغيب عنه السلطة المركزية وهذا ما يؤدي إلى التعاون وهي تذهب إلي تحقيق المصلحة الوطنية التي تسعى لزيادة قوتها المطلقة وليست النسبية فصناعة القرار بالنسبة لليبراليين يأتي نتيجة مساومات وليس نتيجة حسابات عقلانية [2].

أما فيما يتعلق بالنظرية الليبرالية الجديدة فقد شهدت أواخر الستينيات من القرن العشرين عودة الإهتمام بالنظريات الليبرالية، وهناك ثلاثة وجهات من التفكير الليبرالي الجديد الاقتصادي والاجتماعي والسياسي والذي بدوره يرتبط أحدهما بالمؤسسات والآخر بالديمقراطية فهي بذلك تشير إلى الليبرالية المؤسسية الجديدة[3].

ومما سبق يمكن إجمال فرضيات الليبرالية الجديدة في أن الأفراد والدول يملكون القدرة على حل المشاكل من خلال العمل الجماعي، وكذا التعاون الدولي للاستفادة العامة وبروز الفاعلين من غير الدول، في حين أن الدولة هي متعددة المراكز وكذلك المكاسب النسبية في مقابل المكاسب المطلقة[4].

ثانيا: الرؤية الليبرالية للأمن السيبراني في السياسة الدولية

تتلخص عناصر الرؤية الليبرالية للدور الذي تلعبه في الأمن السيبراني في الساحة الدولية؛ فهذا المنظور يعتمد بالأساس على تعددية الفواعل في النظام الدولي و همية العوامل الداخلية في السلوك الخارجي للدولة على الرغم من تركيزه على المؤسسات الدولية ودراسات الظواهر عبر الدولية، وعلى الرغم

[1]– محمد الطاهر عديلة، **تطور الحقل النظري للعلاقات الدولية: دراسة في المنطلقات والأسس**، أطروحة مقدمة لنيل شهادة دكتوراه العلوم السياسية والعلاقات الدولية، فرع العلاقات الدولية، (باتنة: جامعة الحاج لخضر، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية، 2014–2015)، ص،ص.148،149.

[2]– خالد موسى المصري، "الوضعية ونقادها في العلاقات الدولية (دراسة نقدية للنظريات الوضعية)"، **مجلة جامعة دمشق للعلوم الاقتصادية والقانونية**، (م.30)،(ع.)1، (2014)، ص.333.

[3]– أنور محمد فرج، **مرجع سابق**، ص.396.

[4]– **المرجع نفسه**، ص.404.

من أهمية الدولة كفاعل خاصة عند الواقعين إلا أن الليبراليين يرون بأن هناك فاعلين آخرين لا يقلون أهمية في تفاعلات السياسة الدولية، وهم برزوا بالأساس نتاج للتطورات الحاصلة في الساحة الدولية، فبعضها ذو طبيعة تكنولوجية والآخر نتاج لتحديات البيئة الأمنية على الأفراد والدول، وهو ما يبرز وجود علاقات عابرة للدول وبالتالي أهمية العلاقات الاعتمادية والتواصلية العابرة لحدود الدولة خاصة بتطور تكنولوجيا المعلومات العابرة للحدود هي كذلك مثل: شبكات الجريمة والقرصنة الإلكترونية العابرة للحدود هذا ما أدى إلى تراجع سيادة الدولة وفرض تحديات عديدة في الحفاظ على الأمن السيبراني العالمي[1].

الفرع الثالث: المنظور البنائي للأمن السيبراني في السياسة الدولية

و تندرج تحت هذا المنظور ما يلي:

أولا: المرجعية المعرفية للنظرية البنائية

ظهرت البنائية في العلاقات الدولية في نهاية الثمانينات كانتقاد للاتجاهات التي كانت سائدة في العلاقات الدولية وكان نيكولاس أنوف–Nicholas Onuf، أول من استعمل المصطلح في كتابه "عالم من صنعنا–World of Our Making"، حيث ركز على انتقاد أعمال الواقعية البنيوية ، وبرزت مع ألكسندر وندت–Alexandr Wendt الملقب بأب البنائية الصادر عام 1992 م والمعنون بـ: "الفوضى هي ما تصنعه الدول: التفسير الاجتماعي لسياسة القوة– Anarchy is What States Make of it: The Social Construction of Power Politics"[2].

وتزامن ظهور هذه النظرية مع نهاية الحرب الباردة، التي شكلت عقبة أمام فشل العديد من النظريات وخاصة النظرية الواقعية، في التنبؤ بنهاية هذه الحرب بطريقة سلمية ، كما ساهمت هذه الحرب في إضفاء الشرعية على النظرية البنائية لأن الواقعية والليبرالية أخفقتا في استباق هذا الحدث كما أنهما وجدتا صعوبة كبيرة في تفسيره، وجاءت هذه النظرية لتتحاور مع النظريات التقليدية وتنتقدها بأن هذه النظرية البنائية تمتلك تفسيرا في التنبؤ بنهاية الحرب الباردة مختلف خصوصا ما يتعلق بالثورة التي

[1] –سماح عبد الصبور، **مرجع سابق** .ص،8.

[2]– إنعام عبد الكريم أبو مور، **مفهوم الأمن الإنساني في حقل نظريات العلاقات الدولية**، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير في العلوم السياسية، (غزة: جامعة الأزهر، كلية الاقتصاد والعلوم الإدارية، قسم العلوم السياسية، 2013)، ص.126.

أحدثها ميخائيل غورباتشوف–Mikhaïl Gorbatchev، في السياسة الخارجية السوفيتية باعتناقه أفكار جديدة كالأمن المشترك[1].

توظف النظرية البنائية بعض المفاهيم المشتركة مع النظريات الأخرى وإن اختلفت رؤيتها في معنى هذه المفاهيم ودورها وتتمثل في أنها لا تركز على مفهوم الدولة والقوة فقط بل تركز على مبادئ و مفاهيم أخرى،و كذلك فيما يتعلق بالمصلحة الوطنية الذي تنظر إليه على أنه شيء تمتلكه الدول وهو من أهم المفاهيم أكثرها غموضا تركز على دور الهوية في تشكيل الفعل السياسي من خلال أن هذه المصلحة والهوية تتفاعل لتحدد دور الفاعل في العلاقات الدولية [2].

و لقد اهتم أنصار المنظور البنائي بدراسة الأمن والسلام وتركيزهم على الأمن القومي للدول الذي ظهر مع مفهوم الأمن الإنساني، الذي يعتبر أساس الدراسات الأمنية الذي يكون بالأساس الإنسان وليس المادة[3].

ثانيا: افتراضات النظرية البنائية

يشير كل من بول فيوتي–Paul Viotti ومارك كوبي–Mark Kauppi في كتابهما "نظرية العلاقات الدولية–International Relation Theory"، إلى أن هناك افتراضات تنطلق منها البنائية وهي اهتمامهم بالقوى الفاعلة من غير الدولة كالمنظمات الدولية والمنظمات غير الحكومية، كما تركز كذلك على العوامل المعرفية والذاتية و تفاعل هذه الوحدات، كما يركز كذلك البنائيون على بنية النظام الدولي بأنها بنية اجتماعية تؤثر في هوية ومصلحة الفاعلين، وتنظر له كذلك بأن العالم هو قضية متجددة، وقدم أنصار المنظور البنائي إسهامات في الجدال الإبستمولجي والأنطولوجي في العلاقات إذ يرفض البنائيون الافتراضات بوجود قوانين وشبه قوانين تحكم الظاهرة الاجتماعية والسياسية بعيدة عن إرادة الفاعل وقدرته في التأثير في محيطه، كما ترفض البنائية افتراضات فصل الذات عن الموضوع[4].

---

[1]– ستيفن وولت، "**العلاقات الدولية: عالم واحد نظريات متعددة**"، ترجمة: عادل زقار، زيدان زياني، في: 2020/03/01 http://www.geocities.com/adelzeggagh/IR

[2]– خالد موسى المصري، "النظرية البنائية في العلاقات الدولية"، **مجلة جامعة دمشق للعلوم الاقتصادية والقانونية**، (م.) 30 ، (ع.2)، (2014)، ص–ص.324–326.

[3]–**المرجع نفسه**، ص،ص.327،328.

[4]-Paul Viotti , Mark Kauppi, **International Relation Theory**, (New York: Pearson, 5.E, 2010), P.278.

ثالثا: مكانة الأمن السيبراني في النظرية البنائية

فهذا المنظور الذي يركز أو يرى أن الحقائق الاجتماعية مثل: المصالح والهويات لا يمكن أن ينظر إليها على أنها ثابتة ويجب أن نتساءل لماذا تصبح هذه الحقائق هكذا أو على ماهي عليه، ومنه يرى البنائيون دراسات الصراعات أو الأمن الإلكترونية أنها حرب معلومات تعكس نوعا من حروب الهوية والتي تتعدى الحدود المتعارف عليها؛ إذ تصبح مثلا هوية الدولة الأصلية على المحك من قبل هويات جديدة وناشئة ومتصارعة في الفضاء السيبراني في حين كذلك تركز البنائية في دراسة هذا المجال على أهمية الصور والرموز جنبا إلى جنب مع البيئة المادية من أجهزة وكابلات من خلال اقتراب السياسات الرمزية The Symbolic Politics Approach.[1]

ويساهم هذا المنظور في توضيح وظيفة وتأثير اللغة في الأمن من خلال العصر الرقمي باستخدام مصطلحات مثل حرب المعلومات والجريمة الإلكترونية فهو ينقل معاني خاصة في حقل السياسة الدولية ومنه فتحليل المنظور البنائي يساهم في الكشف عن أهمية هذه الخطابات والسياسات الرمزية والصورية في صراعات وأمن المجال السيبراني في السياسة الدولية.

وفي ختام هذا الفصل المفاهيمي المتعلق بمفهوم الأمن والتسلسل الزمني الذي مرى به من نشأة وأجيال إلى التعريف المتعلق بالأمن السيبراني والمفاهيم المشابهة له من قوة وصراع،أمن المعلومات إلى فضاء سيبراني ،وفي هذا الفصل كذلك تطرقنا للأبعاد والمداخل النظرية من بعد اقتصادي،عسكري،سياسي،إلى اجتماعي وقانوني ومداخله النظرية من المنظور الواقعي والليبرالي والبنائي وكيف كان تفسير الأمن السيبراني لواقع السياسة الدولية.

[1] - سماح عبد الصبور،**مرجع سابق**.ص،9.

الفصل الثاني

يتناول هذا الفصل البحث في فواعل ووسائل التهديدات السيبرانية في السياسية الدولية ولقد ظل الحوار دائرا حول مكانة الدولة في ظل هذه الأخطار التي تهدد الأمن السيبراني في النظام الدولي وما ينجر عن هذه المكانة من علاقات بمحيطها الإفتراضي وهذا منذ بداية بلورته نهاية الحرب الباردة وما أفرزته من تغيرات وتحولات على العالم، وقد فرضت هذه التغيرات على العالم والفضاء السيبراني تغيرا في الساحة الدولية ومن ثم تحديد أولويات الدول وتطور هذه التهديدات.

ويقودنا الحديث في هذا المقام عن مهددات الأمن السيبراني في السياسة الدولية من الخصائص إلى الوسائل والأدوات المستعملة ودورها وتأثيرها في السياسة الدولية وهو ما يتناوله الفصل الثاني من الدراسة.

ولتوضيح ذلك سيتم تناول هذا الفصل المعنون بفواعل ووسائل الأمن السيبراني في السياسة الدولية من خلال ثلاثة مباحث تركز على الأخطار الناجمة عن الأمن السيبراني التي تتطور من الجريمة السيبرانية إلى الإرهاب السيبراني لتنتهي عند الحروب السيبرانية كأعلى درجات الصراع في السياسة الدولية.

المبحث الأول: مفهوم الجريمة السيبرانية

الجريمة ظاهرة موجودة في كل المجتمعات ولا يكاد يخلُ منها مجتمع على وجه الأرض فهي السلوكيات والأفعال الخارجة عن القانون، وهي مفهوم نسبي تختلف باختلاف الأزمنة واختلاف المجتمعات بل وحتى داخل المجتمع الواحد، وتخضع لقيم المجتمع وتوجهاته بمرور الزمن وقد تعددت أنواع الجرائم وصولا إلى الجريمة السيبرانية التي تعبر عن مخالفات تُرتكب ضد الأفراد أو المجموعات بدافع الجريمة.

المطلب الأول: تعريف الجريمة السيبرانية

يمكن تعريف الجريمة السيبرانية بالمعنى الضيق على أنها "جريمة الكمبيوتر" وهي أي تصرف غير قانوني موجه ضد الجهاز النظام أو المعلومات التي تحويه، أما بمعناها الواسع فهي الجريمة المتصلة باستخدام الكمبيوتر وهي بذلك تعبر عن تصرف غير قانوني يُرتكب باستخدام تقنيات المعلومات والإتصالات بما فيه حيازة مواد ممنوعة أو توزيعها أو عرضها[1].

وتحدد لجنة الجرائم الالكترونية في المجتمعات الأوربية أن الجريمة الالكترونية تفهم على أنها أعمال إجرامية ترتكب باستخدام شبكات الاتصالات الإلكترونية وأنظمة المعلومات أو ضد هذه الشبكات والأنظمة[2]

كما تُعرف أيضا على أنها "مجموعة الأفعال والأعمال غير القانونية التي تتم عبر معدات أو أجهزة إلكترونية أو شبكة الأنترنيت أو تبث عبر محتوياتها، وهي ذلك النوع من الجرائم التي تتطلب الإلمام الخاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها"[3]. فالجريمة السيبرانية هي عبارة عن نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي.

---

[1] منى الأشقر جبور، **مرجع سابق**. ص،50.

[2] Martti lehto and Pekka Neittaanmaki.op.cit.p,11.

[3] عبد الفتاح مراد، **شرح جرائم الكمبيوتر والانترنيت**، (مصر: دار الكتب والوثائق المصرية، د ط، د س ن).ص38.

ويعرفها أحمد صياني "بأنها تصرف غير مشروع يؤثر في الأجهزة والمعلومات الموجودة عليها"[1]، كما يعرفها محمد أبوصبحة على أنها "استخدام برامج الحاسوب وتقنيات التكنولوجيا الحديثة بطريقة تسبب ضررا معنويا أو ماديا لإنسان آخر أو تتسبب بتلف وتعطيل أجهزته الالكترونية مثل جهاز الحاسوب البيتي أو النقال، بكل أنواع الضرر من حذف للمعلومات وسرقة بيانات خاصة أو تخريب هذه البيانات وهذه الجرائم تتخذ أشكالا وأنواعا كثيرة حسب الجهة المتسببة بالضرر وحسب الجهة التي تضررت"[2].

وتشكل الجريمة السيبرانية تحديا كبيرا للبيئة التي تُرتكب فيها، إذ يمكن لمجرمي الأنترنيت العمل من أي مكان في العالم واستهداف أعداد كبيرة من الناس أو الشركات عبر الحدود الدولية وتزداد التحديات التي تفرضها، استنادا إلى نطاق وحجم الجريمة والتعقيد التقني لتحديد هوية الجناة وكذلك ضرورة العمل على الصعيد الدولي لتقديمهم إلى العدالة، فالأنترنيت تفتح فرصا جديدة لمجرميها على أساس الإعتقاد بأن إنفاذ القانون لا يعمل في عالم الأنترنيت[3].

المطلب الثاني: خصائص الجريمة السيبرانية

إن ارتباط الجريمة السيبرانية بالأنترنيت ميزها عن الجريمة التقليدية بعدة خصائص أهمها:

- الجريمة السيبرانية لا تتطلب الإزالة فيمكن نسخها فقط.

- توافر المعلومات في كل مكان.

- الجريمة السيبرانية قيمة من حيث المعلومات وممتعة من حيث السرقة.

- ديمومة المعدات والبرامج المسروقة يمكن أن يستخدم لفترة طويلة.

- سرعة التنفيذ حيث لا يتطلب تنفيذ الجريمة السيبرانية الوقت الكثير وبكبسة زر واحدة يمكن أن تنتقل ملاين الدولارات من مكان إلى آخر، والتنفيذ لا يتطلب وجود الفاعل في مكان الجريمة بل يمكن للفاعل تنفيذ جريمته عن بعد.

---

[1] إسراء جبريل رشاد مرعي،"الجرائم الإلكترونية: الأهداف، الأسباب، طرق الجريمة ومعالجتها"، **مجلة الدراسات الإعلامية**"،ع 1، جانفي 2018، ص 426.

[2] عبير شفيق الرحباني، **الجرائم الإلكترونية ومخاطرها**، (عمان: دار الثقافة للنشر والتوزيع، ط1، 2020)، ص.28.

[3] بارة سمير، مرجع سابق.ص،259.

– الجرائم مخفية إذ لايمكن أن تلاحظ آثارها أو التخمين بوقوعها.

– الجريمة السيبرانية عابرة للحدود الدولية، تمتاز بأنها جرائم ناعمة لا تتطلب العنف مع صعوبة إثباتها لأنه لا وجود لدليل ضدها[1]،لأن المجرمين على درجة كبيرة من الذكاء والتطور التكنولوجي.

– قلة التبليغات عن الجرائم بسب الخوف من التشهير وفقدان السمعة إضافة إلى نقص الخبرة في هذا المجال وعدم كفاية القوانين القائمة.

– تعتمد على أساليب الدهاء والذكاء مما يسهل الوقوع في فخها.

ومن خلال هذه الخصائص نستنتج مجموعة من أهداف الجريمة السيبرانية تتمثل في:

– التمكن من الوصول إلى المعلومات بشكل غير شرعي كسرقة المعلومات أو الاطلاع عليها أو حذفها أو تعديلها بما يحقق هدف المجرم.

– التمكن من الوصول عن طريق الشبكة العنكبوتية إلى الأجهزة الخادمة الموفرة للمعلومات وتعطيلها.

– الحصول على المعلومات السرية للجهات المستخدمة للتكنولوجيا كالمؤسسات والبنوك والجهات الحكومية والأفراد وابتزازهم بواسطتها.

– الكسب المادي أو المعنوي أو السياسي غير المشروع عن طريق تقنية المعلومات مثل:عمليات اختراق وهدم المواقع على الشبكة العنكبوتية وتزوير بطاقات الإئتمان وسرقة الحسابات المصرفية.

وتهدف كذلك الجرائم الإلكترونية حسب (محمد مختار) إلى تعطيل الخدمة، إتلاف المعلومات أو تعديلها، التجسس على الشبكات وتدمير الأصول والمعلومات[2].

المطلب الثالث:أدوات ووسائل الجريمة السيبرانية

أولا: أدوات الجريمة السيبرانية

وحتى يتمكن المجرمون السيبرانيون من تنفيذ جريمتهم يستلزم ذلك توفر أدوات لذلك يستعملها بالأخص القراصنة منها:

[1] إسراء جبريل رشاد مرعي، مرجع سابق، ص ص.439-445.

[2] محمد مختار، مرجع سابق، ص.6.

- الإتصال بشبكة الأنترنيت تعتبر أداة رئيسية لتنفيذ الجريمة.

- توفر برمجيات خاصة لنسخ المعلومات المخزنة عند المستخدم على جهاز الحاسوب.

- وسائل التجسس ومنها ربط الكاميرات بخطوط الإتصال الهاتفي.

- البار كود وهي عبارة عن أدوات تستخدم لمسح الترميز الرقمي وفك شيفرة الرموز[1].

- الطابعات

- هواتف رقمية ونقالة.

- برامج ضارة إذ تتمثل وظيفتها في خداع الضحية وتشجعه على تشغيلها فتلحق الضرر الشامل بالحاسوب والملفات الموجودة عليه.

ثانيا: وسائل الجرائم السيبرانية

تتعدد وتتنوع وسائل الجريمة السيبرانية فمنها ما يقع على المستوى الفردي ومنها يقع على المستوى المجتمعي وهناك من يذهب بالقول أنها تقع أيضا على المستوى الكوني.

1- على المستوى الفردي:

وهي البحث عن التقدير ويقوم بها الشباب صغير السن وذلك من باب التحدي والظهور في الاعلام، وهذا ما وفر فرصا غير مسبوقة لانتشار الجريمة وبفضل تطور تكنولوجيا المعلومات والاتصالات سهل نمو الجريمة على الأنترنيت، وهذا كله بسب ضبط الذات المنخفض لتحقيق الرغبات الذاتية للسلوك الطائش، وهذا بفعل النشاط الروتيني من خلال التغير في أنشطة الناس خاصة مع ظهور الأنترنيت.

2- على المستوى المجتمعي:

ومن أهم أبرز هذه الأسباب هو التحضر أي الهجرة من الريف إلى المدينة وهذا النوع من الشباب يكون غير متمكن من مواجهة متطلبات الحياة الحضرية باهظة التكاليف مما يجعلهم يلتفتون إلى

[1] إسراء جبريل رشاد مرعي، مرجع سابق،ص,431.

الجريمة الإلكترونية حيث لا تتطلب رأس مال كبير، كذلك نجد البطالة إذ ترتبط بها مثلها مثل الجريمة التقليدية ولذا فإن الشباب الذين يملكون المعرفة يستثمرونها في النشاط الإجرامي السيبراني. الضغوط العامة التي يتعرض لها المجتمع من فقر وبطالة وأمية عوامل ضاغطة على المجتمع عامة وعلى قطاع الشباب خاصة وهذا ما يدفعهم إلى البحث عن الثراء لأن الإنسان بطبعه يسعى إلى المتعة ويتجنب الألم وهذا أدى إلى ضعف إنفاذ القانون وتطبيقه.

3- على المستوى الكوني:

منها التحول للمجتمع الرقمي ولديه سمات وهي تغيرات كمية في مقدار المعلومات المتدفقة ونوعها، إرسال المعلومات إلى العديد من الأطراف كذلك وجود الشبكات حيث يتم تداول المعلومات بين جميع الاطراف كالبريد الالكتروني، بفضل دخولنا في عصر المعلوماتية الجديد فالناس يقضون جزءا من حياتهم اليومية في الفضاء الإلكتروني بفضل شبكة الأنترنيت، وهو ماخلق ظواهر جديدة متميزة عن وجود أنظمة الكمبيوتر والفرص المباشرة للجريمة التي توفرت بفضل هذه الأجهزة فهذا العصر يتطلب مؤسسات أمنية مصممة للتعامل مع التغير السريع تركز على الإبداع والشفافية وذات سرعة عالية في نشر المعلومات وإعلام الجمهور بأنها مؤسسات قادرة على إعادة تصميم ذاتها لمواجهة المستجدات السريعة في عالم الجريمة السيبرانية.

الترابط الكوني هو عامل يمكن أن يساهم في دفع مستويات الجريمة في ظهور الترابط العالمي فبحلول عام 2050 فإن العالم سوف يشهد تضاعف عدد السكان وهو ما يؤكد أن فضاء الأنترنيت قد خلق فرصا جديدة للمجرمين في التواصل مع الضحايا وقد بين أن السمات الفريدة للأنترنيت وهي عدم الكشف عن اسم الشخص[1]، وسهولة الإستخدام قد وفرت طرق جديدة للمجرمين لارتكاب جرائمهم إضافة إلى التواصل بسرعة عالية في نقل المعلومات عبر الدردشة والبريد الإلكتروني ومواقع الويب وأجهزة الكمبيوتر المتصلة بالأنترنيت.

تفاوت انكشاف البنية التحتية المعلوماتية الكونية بدرجة إلى الكوارث الطبيعية والإهمال البشري وتتمثل خاصة في قطاع الاتصالات والمعلومات، قطاع التوزيع المادي ويشمل الطرق السريعة للمواصلات وقطاع الطاقة وقطاع المال والبنوك والخدمات الإنسانية الحيوية.

[1] نفس المرجع، ص.438.

المطلب الرابع: أنواع الجرائم السيبرانية

مع تصاعد الاعتماد على الأنترنيت والاتصالات تتصاعد مخاطر واحتمالات الجريمة السيبرانية وتذهب بنا الحاجة إلى معرفة أنواع هذه الجرائم خاصة ما تعلق بالأبعاد الدولية، فبالإضافة إلى الأشخاص تستهدف الجريمة السيبرانية المنشآت الحيوية والحساسة ويمكن تمييز أنواع الجرائم من حيث جرائم تستهدف الأفراد والملكيات والدولة.

1- جرائم تستهدف الأفراد: إذ يؤدي انتشار الجريمة السيبرانية إلى خلل عام قد يهدد المجتمع كله في اقتصاده وسيادة أمنه الوطني ويطلق عليها أيضا بجرائم الأنترنيت الشخصية والتي تقتضي على الحصول بطريقة غير شرعية على هوية الأفراد الالكترونية وسرقة كلمة السر الخاصة بهم وانتحال الشخصية بصفة الكترونية[1]. وتسيء هذه الجرائم بشكل أساسي إلى كرامة الإنسان وسلامته الشخصية عندما تترجم من خلال الاتجار بالبشر،الدعارة ،الإرهاب و التحرش...ويعتبر غياب القوانين الرادعة واتفاقيات التعاون بين البلدان المختلفة من أهم الأسباب التي تشجع على هذه الجرائم إذ ينتقي المجرمون البلدان التي لا إطار قانوني فيها، وساهم انتشار وسائل الإتصال بالشكل الكثيف إلى تعريض مستخدمي الانترنيت إلى جميع أنواع الم حتوى السيئ غير الأخلاقي وغير المشروع. وتزيد إخفاء الهوية الحقيقة وانتحال هوية مزيفة من خطورته ما تسمح للمعتدي بارتكاب مالا يجرؤ على ارتكابه في العالم المادي، ما يزيد في ارتفاع حظوظ التعرض للاعتداءات بفضل الانتشار الواسع للتطبيقات المعلوماتية، كذلك يسمح بإخفاء الهوية التي تتيحه التقنيات للمترصدين والمجرمين باستدراج مستخدمي الأنترنت إلى الإفصاح عن بياناتهم الشخصية، إضافة إلى استغلال الأطفال والقاصرين في مواد إباحية وهم الأطفال الذين تقل أعمارهم عن 18 سنة ،كما يلاحق الخطر أيضا لبالغين إذ تسمح الانترنيت بتكوين مجموعات حول اهتمامات مشتركة يمكن أن تكون غير شرعية وتستعمل في نشر السلوك العدائي من قبل فرد أو حتى جماعة بهدف ايذاء اللآخرين فيما يعرف بالتنمر السيبراني، الترصد السيبراني أو المطاردة السيبرانية.[2] وهي في الغالب ما تتضمن عملية المطاردة والتهديد وسرقة الهوية. أما أنواع الجرائم التي يتعرض لها الأشخاص هي النصب والاحتيال الالكتروني،التشهير والابتزاز،السرقة الالكترونية والاختراق والتخريب.

[1] نفس المرجع، ص.443.

[2] منى الأشقر جبور، مرجع سابق.ص ص.52-56.

2- الجرائم الواقعة على الأصول والممتلكات:ويستهدف هذا النوع من الجريمة الجهات الحكومية والخاصة والفردية دون استثناء إذ أنها تركز على تدمير الملفات الهامة أو البرامج ذات الملكية الخاصة لحقوق الملكية الفكرية والصناعية وذلك عبر برامج ضارة، يتم نقلها إلى الأجهزة بطرق مختلفة منها البريد الالكتروني.

وتتمحور الاعتداءات في هذا الإطار على استغلال وجود المؤسسات المختلفة على الانترنيت واتصال النشاطات المالية بالشبكة حيث تستعمل أنظمة الدفع الالكتروني والتجارة ليس فقط عبر التسلل للأنظمة وإنما أيضا من خلال استخدام بيانات شخصية للأفراد المسؤولين عن إدارة الأموال وتحويلها إلى حساباتهم الشخصية أو إلى حسابات أخرى ،ولعل أبرز المخاطر التي يمكن أن تواجه الاقتصاد الرقمي[1] هي التي تواجه الاقتصاد التقليدي ألا وهي تبيض الأموال.

3-الجرائم التي تستهدف الدولة: فالمخاطر السيبرانية لا تقتصر فقط على الحقوق والحريات الشخصية وإنما تتعداه إلى مصالح الدول وأمنها والمؤسسات والأنظمة، فلا يمكن لأي دولة أن تنأ بنفسها عن الهم الذي يمثله اختراق الشبكات وبالتالي على هذه الحكومات تأمين القطاعين الخاص العام و الدور هنا هو دور التقنين على الرغم من أنه ليس السبيل الحازم في تحقيق الأمن لأن هذه الأطراف تركز جهودها على الإطار التشريعي والتعاون الدولي ،ويمكن تصنيف هذه الاعتداءات التي تستهدف المؤسسات الحكومية والدولية منها[2]: التلاعب بالمعلومات، حرب المعلومات، التسلل إلى أنظمة البيانات الحكومية والأجهزة وتدمير البنى التحتية الرقابة والتجسس، الحرب السيبرانية، الإرهاب السيبراني، تسريب المعلومات واختراقها.

وهناك من يصنفها إلى الجرائم التي تتمثل في: استغلال البيانات المخزنة عللى الكمبيوتر بشكل غير قانوني،كذلك الجرائم التي يتم اختراق الكمبيوتر من خلالها لتدمير البرامج والبيانات الموجودة في الملفات المخزنة عليه وتدخل ضمن الفيروسات الالكترونية،كذلك الجرائم التي يتم فيها استخدام الكمبيوتر لارتكاب جريمة معينة أو التخطيط لها وأخيرا الجرائم التي يتم فيها استخدام الكمبيوتر بشكل غير قانوني من قبل الأفراد المرخص لهم باستعماله.

وللجرائم السيبرانية أنواعا أخرى من حيث الاستخدامات وهي:

[1] نفس المرجع .ص ص.56-57.

[2] نفس المرجع.ص ص.57-60.

-استخدام الحاسوب دون إذن صاحبه كسرقة اسم المستخدم مثلا.

-القيام ببرمجة برامج يكون دورها تخريب الاجهزة الأخرى مثل الفيروسات.

-سرقة الكمبيوتر الخاصة بأشخاص مهمين أو لديهم معلومات قيمة على هذه الاجهزة[1].

-السرقة كسرقة أجهزة الهاتف الذكية .

-إرسال رسائل بالبريد الالكتروني بحيث يم إرسال الرسالة وفيها عنوان مرسل مزيف.

-التخريب.

-برامج الرسم والتصميم.

المبحث الثاني: الإرهاب السيبراني

تعد المجتمعات الإرهابية أو الإرهاب من أبرز الفواعل الدولية خاصة بعد أحداث 11 سبتمبر حيث تستغل الفضاء السيبراني في عمليات التجنيد والتعبئة، كما تحاول جمع المعلومات حول الأهداف العسكرية وكيفية التعامل مع الأسلحة وتدريب المجندين الجدد عن بعد رغم أنها لم تصل بعد إلى مرحلة القيام بهجوم سيبراني حقيقي من منشآت الدول فالإرهاب السيبراني يقع في المستوى الرابع بعد كل من القرصنة والجريمة والتجسس السيبراني وهو يعبر عن الهجمات غير الشرعية التي ينفذها فاعلون غير حكوميون ضد أجهزة الكمبيوتر وشبكات المعلومات فالدول لا تملك أن تحجب المواقع الإلكترونية التي تروج لأفكار الجماعات الارهابية بشكل استباقي فكل ما تملكه هو استخدام الأدوات الإستخباراتية التي تتعقب المكاتب والمكالمات الإلكترونية التي تستخدم كلمات بعينها تتضمن العنف والتخريب لتتبع تلك المواقع تمهيدا لإغلاقها.

المطلب الأول: تعريف الإرهاب السيبراني

وسنتناول في هذا المطلب الشق اللغوي والشق الاصطلاحي للإرهاب السيبراني

1- التعريف اللغوي للإرهاب:

[1] عبير شفيق الرحباني، مرجع سابق.ص ص.36-39.

في اللغة العربية اشتق لفظ إرهاب من الفعل المزيد أرهب بمعنى أخاف وأفزع [1]، وأوضح المعجم اللغوي بأن الإرهاب وصف يطلق على الذين يسلكون سبل العنف ويستخدمونه لإحداث فزع [2].

وقد وردت الرهبة ومشتقاتها في القرآن الكريم في عدة مواضع للتعبير عن معاني الرعب والخوف والخشية والفزع في قوله تعالى "وأعدوا لهم ما استطعتم من قوة ومن رباط الخيل ترهبون به عدو الله وعدوكم وآخرين من دونهم لا تعلمونهم الله يعلمهم"[3].

وحسب قاموس أوكسفورد (OXFORD) يعرف على أنه "استخدام العنف أو التخويف لتحقيق أغراض أو أهداف سياسية"[4].

وحسب (قاموس لاروس هو استعمال للعنف لزرع الفزع والترهيب فهو إذن"الاستخدام المنظم للعنف من خلال استهداف المدنيين من أجل تحقيق أهداف سياسية وينتج في الغالب من نشاط الجماعات الصغيرة التي تناضل ضد النظام السياسي[5] .

ويعرف مكتب التحقيقات الفيدرالي الأمريكي FBIالإرهاب السيبراني بأنه نشاط إجرامي يستخدم أجهزة الكمبيوتر وأدوات الشبكة بطريقة تؤذي إلى الإرتباك أو الإضرار بالخدمات الرقمية ويتم ذلك عن طريق خلق الفوضى بين السكان والمدنيين بهدف الترهيب أو إكراه الحكومة وشعبها من أجل تحقيق أهداف سياسية واجتماعية وإيديولوجية[6]

2- التعريف الاصطلاحي للإرهاب السيبراني:

عدم وجود تعريف موحد متفق عليه أدى إلى عرقلة وضع إستراتيجية فعالة لمكافحة الإرهاب على المستوى الوطني والدولي، ومنه فالإرهاب تأثر بشكل كبير بالجانب السياسي إلا أنه تكيف مع التقدم والتفوق النوعي الحاصل لم يعد يقتصر على الهجمات والتقنيات التقليدية بل أدخل في قواميسه عدة هجمات جديدة أبرزها الهاكر (Hacker) والسيبرانية (Cyber) ناهيك عن عدة أساليب ووسائل مست هيكله. وما سوف نتطرق إليه هو الذي يسمى في الكثير من الأدبيات "الإرهاب الصامت" وهو أرقى

[1]- العياشي وقاف، **مكافحة الإرهاب بين السياسة والقانون**، (الجزائر: دار الخلدونية للنشر والتوزيع ،2006).ص ،12.
[2]- أحمد أبو الروس، **الإرهاب: التطرف والعنف**، (الإسكندرية: دار المكتب الجامعي الحديث، 2011) .ص،24.
[3]- سورة الأنفال، الآية (60).
[4] Oxford Advanced learner's Dictionary of current English ,(Oxford univ, press , 2008),p459.
[5] larousse , Super major. (Paris,cedex, Larousse,1989); P1030.
[6] Martti Lehto,and Pekka Neittaanmaki.op.cit.p13.

صور الإرهاب المعاصر فهو لا يعتمد على الوسيلة بل يسعى دائما إلى الهدف، لأن الوسيلة المستعملة هي الصوت والضوء والموسيقى والقلم...بدلا من القنبلة التقليدية.

ويعتبر الأنترنيت من أبرز الأسلحة الناعمة المستخدمة في الأنشطة الإرهابية الحالية والدمج بين الإرهاب والأنترنيت ولد مايسمى "بالإرهاب السيبراني" (Cyberterrorisme)، إذ تم صياغة هذا المصطلح لأول مرة عام 1980 من قبل باري كولين Barry Collin وهو حسبه يمثل الاندماج بين العالمين الواقعي والافتراضي[1]، إذ يتم استخدامه بصفة غير مكلفة وتكون موجهة لخصم معين عبر شكلين: فالأول يكون بمهاجمة البيانات وسرقتها وتخريب الخدمة، والثاني بمهاجمة أنظمة التحكم وكيفية تعطيلها،[2]وهذا النوع من الإرهاب يساهم في إلحاق الشلل في أنظمة القيادة والسيطرة على الإتصالات أو بالأحرى السيطرة على كل المجالات والميادين.

ومنه حسب تعريف (تغريد معين حسن المهدي)" فإن الإرهاب السيبراني هو "الهجوم ذو الدوافع السياسية أو التهديد بالهجوم على أجهزة الكمبيوتر أو الشبكات أو أنظمة المعلومات من أجل تدمير البنية التحتية وترهيب الحكومة أو المواطنين وإجبارهم على تحقيق أهداف سياسية واجتماعية بعيدة المدى، وبمعنى أوسع فإن الإرهاب السيبراني يعني استخدام الأنترنيت للتواصل والدعاية والتضليل من قبل المنظمات الإرهابية[3]. ويستخدم الإرهابيون الأنترنيت في كسب التأييد من طرف الرأي العام لنشر الفكر المتطرف، وكذا في التواصل والتنسيق بين الجماعات الإرهابية وكذلك في تنفيذ الهجمات وتجنيد الإرهابيين.

ويعرفه (جيمس أ.لويس) من مركز الدراسات الاستراتيجية والدولية "فيعرفه على أنه استخدام أدوات شبكات الكمبيوتر لتعطيل البنية التحتية القومية (مثل: الطاقة، المواصلات، عمليات الحكومة) أو إكراه الحكومة أو السكان المدنيين[4].

---

[1] فاطمة الزهراء عبد الفتاح، تطور توظيف جماعات العنف والارهاب السيبراني، **مجلة السياسة الدولية**، (العدد 208)، أفريل 2008 .ص 25.

[2]-محمد مؤنس محي الدين، **تحديث أجهزة مكافحة الإرهاب وتطوير أساليبه** (عمان: دار الحامة للنشروالتوزيع ،2014).ص،115.

[3]-تغريد معين حسن المهدي، الأثر العسكري للأمن السيبراني، **مجلة البحوث الجغرافية** (العدد 30).ص،242.

[4] عادل عبد الصادق، **الارهاب الالكتروني (القوة في العلاقات نمط جديد وتحديات مختلفة)**، (القاهرة: مركز الأهرام للدراسات السياسية والإستراتيجية،2009) ص 113.

ويعرف الارهاب على أنه هو العدوان أو التخويف أو التهديد ماديا أو معنويا باستخدام الوسائل الإلكترونية الصادر من الدول أو الجماعات أو الأفراد عبر الفضاء الإلكتروني أو أن يكون هدفا لذلك العدوان بما يؤثر على الإستخدام السلمي له[1]. ومنه فالإرهاب السيبراني (الإلكتروني) يعرف في صورة القيام بالهجوم أو نشاط معتمد ذو دوافع سياسية بغرض التأثير على القرارات الحكومية أو الرأي العام باستخدام الفضاء الإلكتروني كعامل مساعد ووسيط في عملية التنفيذ للعمل الإرهابي أو الحربي من خلال هجمات مباشرة بالقوة المسلحة على مقدرات البنية التحتية للمعلومات، أو من خلال ما يعد تأثيرا معنويا ونفسيا من خلال التحريض على بث الكراهية الدينية وحرب الأفكار أو أن يتم في صورة رقمية من خلال استخدام آليات الأسلحة الإلكترونية الجديدة في معارك تدور رحالها في الفضاء الإلكتروني والتي قد يقتصر تأثيرها على بعدها الرقمي أو قد تتعدى لإصابة أهداف مادية تتعلق بالبنية التحتية الحيوية.

المطلب الثاني: وسائل و أدوات الإرهاب السيبراني

تتعدد وتتنوع وسائل وأدوات الإرهاب الإلكتروني وكل حسب درجة الخطورة والتهديد ومنها نجد:

أولا: وسائل الإرهاب السيبراني

هناك وسائل عديدة أدت إلى ظهور الإرهاب في شكله الحديث والرقمي، منها أسباب فردية وأخرى اجتماعية ومن أهم الأسباب التي أدت إلى انتشاره هي ضعف بنية الشبكات المعلوماتية، بحيث أن ضعف مثل هذه البنى المعلوماتية يؤدي إلى عدم خصوصيتها وبالتالي قابليتها للإختراق بسهولة ويعود السبب في ذلك أن الشبكات مصممة في الأصل بشكل مفتوح دون بوادر أمنية[2]، وبالتالي فهي تحتوي على ثغرات معلوماتية تساعد المخترقين وحتى الجماعات الإرهابية من اختراقها واستغلالها للقيام بأعمال إجرامية وتخريبية، كذلك نجد غياب الرقابة وتذهب إلى سهولة الاستخدام التقني وقلة التكلفة المادية وهذا راجع إلى أن شبكات التواصل الاجتماعي أصبحت متوفرة في متناول الجميع إضافة إلى صعوبة تكلفتها، وكذا صعوبة اكتشاف وإثبات الجريمة الإلكترونية حيث يصعب تحديد هوية المخترقين إلا من خلال أجهزة معينة تمتلكها بعض المؤسسات الأمنية أما الأفراد العاديون فلا يمكنهم تحديد ذلك.

[1] نفس المرجع ،ص 116 .

[2] عبير شفيق الرحباني، مرجع سابق.ص ص290،289.

البريد الالكتروني: ويعد من أهم وأبرز وسائل الإرهاب السيبراني ،حيث يستخدم هذا البريد في التواصل بين الجماعات الارهابية وتبادل المعلومات والشيفرات بينهم، وقلص عنهم تكلفة التنقل وخطر الإمساك بهم.

إنشاء مواقع الأنترنيت: وهذه الأخيرة سهلت من عمل المنظمات الارهابية في توسيع نشاطها من خلال تبادل الأفكار والمعلومات وخبراتهم مع بعضهم البعض.

اختراق وتدمير المواقع الإلكترونية: وتتم عملية الإختراق السيبراني للمواقع عن طريق تسريب البيانات الرئيسية والرموز الخاصة ببرامج شبكة الأنترنيت وتدمير المواقع هو الدخول غير المشروع بهدف تخريب الموقع أو نشر رسائل تشيد بالإرهاب.[1]حيث يقوم شخص أو مجموعة من الأشخاص باختراق موقع لتغير محتواه أو سرقة معلومات سرية أو الاستيلاء عليه بشكل كامل ويضعون رسائل في الموقع تعلن اختراقه[2].

الفيروسات: حيث تنتشر هذه الفيروسات بسرعة كبيرة نظرا للحجم الكبير لتبادل الملفات والبرامج بين المستخدمين، والفيروسات هي برامج تستنسخ نفسها في الجهاز المصاب وتؤدي إلى أضرار وتظهر برسائل مزعجة أو فقدان ملفات مخزنة وقد تصل إلى نظام التشغيل في الجهاز.

الحرب الإعلامية: وقد أصبح وسيلة مهمة للتأثير على الرأي العام ومخاطبة ملايين المستخدمين، فيمكن تأسيس مواقع لتصبح منبرا إعلاميا تساعد على إيصال الصورة للعالم لكسب تأييد الرأي العام العالمي لمساندة قضيتهم أمام المهتمين.

التجسس الإلكتروني: حيث برعت حكومات كثيرة في استخدام تقنيات متطورة للتجسس على الشبكة العنكبوتية خاصة أن هذه المعلومات عبر الشبكات يمكن اعتراضها والتجسس عليها وتشمل أهداف هذه الهجمات حسب (عادل عبد الصادق) في: القيام بهجمات رقمية حيث يتم شن عمليات التدمير والهجوم إلكترونيا، المجال الإلكتروني عامل مساعد في العمل الإرهابي عن طريق تسهيل الحصول على المعلومات، شن الحرب النفسية ونشر المعلومات الخاطئة والكراهية وما يقابلها من انتهاكات لحقوق الانسان.

ثانيا: أدوات الإرهاب السيبراني

[1]éAlix Desforges, **rimétre**? **Cyber terrorisme :** Fiche de l'iresm n°11,2011,p3.

[2] عفاف خذيري، **الحماية الجنائية للمعطيات الرقمية**، أطروحة مقدمة لنيل شهادة الدكتوراه ،(جامعة تبسة: كلية الحقوق والعلوم السياسية،2019/2018)، ص.119.

يفعل الإرهاب الالكتروني –السيبراني– من خلال طرق ووسائل الهجوم باستخدام أدوات والتي منها تعطيل الخدمة وإضافة إلى ذلك تعطيل الهدف وتشمل البنية التحتية للمعلومات وصولا إلى التأثير الذي يكون له أبعاد داخلية وخارجية إلى غاية التداعيات التي تشمل انهيار شبكات المعلومات بظهور أدوات وآليات تعد أسلحة للهجوم كالقنابل المنطقية والديدان والقراصنة .

فالقراصنة hackers وهم أفراد من أوساط الناس لديهم مهارات عالية في الكمبيوتر والرغبة لاختبار قدراتهم لذلك يلجأون إلى إثباتها بطرق غير شرعية[1]، ويسعى القراصنة إلى محاولة الوصول للبيانات والملفات والأنظمة المتعلقة بالحواسيب الآلية بهدف تعطيل وتدمير شبكات الحاسب الآلي[2]. وتختلف الآراء حول مدى خطورة هذه الهجمات فالبعض يعتبر على أنها ليست على درجة عالية من التهديد والبعض الآخر يلاحظ على أنها لا تقل أهمية وعادة ما تكون أهداف القراصنة هي تحقيق الشهرة والكاسب المالية[3].

وهناك كذلك فيروسات الكمبيوترVirus وهي عبارة عن برامج صغيرة تستخدم لتعطيل شبكة الخدمات والبنى التحتية، الديدان Worms وهي برنامج مستقل يتكاثر بنسخ نفسه عن طريق الشبكات وإذا لم تدمر الدودة البيانات فهي قادرة على قطع الإتصالات ولها القدرة على تغيير شكلها وتستهدف في الغالب الشبكات المالية التي تعتمد على الكمبيوتر مثل البورصات و الشبكات المصرفية. أحصنة طروادةTrojan Horses وهي عبارة عن جزء صغير من شيفرة أو برنامج مختبئ في برنامج أكبر ويكون واسع الإنتشار و الشهرة ومهمته هو إضعاف الهدف قبل بداية الحرب عن طريق إرسال فيروسات إلى البيانات الموجودة بها ثغرات، القنابل المنطقية Logic Bombs وهو نوع من أحصنة طروادة يزرعها المبرمج داخل النظام الذي يطوره ويستخدم لشن الحروب الالكترونية والتجسس.الأبواب الخلفية Backdoors وهي ثغرة تترك عمدا من مصمم النظام للتسلل إليه عند الحاجة وهو ما يسمح لهيئة أركان حرب المعلومات من التجوال داخل أي نظام لدولة أجنبية. الإختناق المروري الإلكتروني Electronic Jamming يسمح بسد وخنق قنوات الإتصالات لدى الهدف بحيث لا يمكنه تبادل

[1] عادل عبد الصادق ،مرجع سابق،ص.128.

[2] نوران شفيق، **السياسة الدولية والإستراتيجية أثر التهديدات الالكترونية على العلاقات الدولية**، (القاهرة: المكتب العربي للمعارف، ط1 2016)، ص.46.

[3]Paul Cornish , **Cyberspace and the National Security of the United Kingdom** :Threats and Responses .Op.cit.9-11.

المعلومات وتم تطوير هذه الخطة بخطوة أكثر فائدة هي استبدال المعلومات وهي في الطريق بين الطرف المستقبل والمرسل بمعلومات مضللة[1].

وتستخدم الجماعات الإرهابية الأنترنيت وخاصة ما يعرف بالأنترنيت المظلم لأنه يكون مجهول ويساعد على إخفاء الأثر لأنه انترنيت خفي لا يمكن الوصول إليه عبر متصفحات البحث العادية فهو لديه متصفحات خاصة وميزته الأساسية تكمن في إخفاء الأثر الذي يمكن أن يتركه المتصفح، ومنع تعقبه وملاحقته ما يتيح له حماية هويته ومعلوماته، إنشاء مواقع على الأنترنيت دون كشف هويته أو مكان تواجده[2]، تجاوز برامج الحجب المستعملة في بعض البلدان، تكوين شبكات تبادل معلومات آمنة وإرسال معلومات سرية ويتم تأمين ذلك عبر تقنية ترتكز بالأساس على تشفير البيانات.

جدول رقم (2):يوضح الاختراقات الالكترونية على مستوى العالم

الإقليم	السكان	عدد مستخدمي الأنترنت	حجم الإختراقات الالكترونية(كنسبة من عدد السكان)
إفريقيا	1،073،380،925	676،167،335	%15،6
آسيا	3،922،066،987	1،076،681،059	%27،5
أوروبا	820،918،446	518،512،109	%63،3
الشرق الأوسط	223،608،203	90،000،455	%40،2
أمريكا الشمالية	348،280،154	273،785،413	%78،6
أمريكا اللاتينية/الكاريبي	593،688،638	254،915،745	%42،9
أوقيانوسيا/أستراليا	53،903،569	24،287،919	%67،6
الإجمالي العالمي	7،017،846،922	2،405،5018،376	%34،3

المصدر:نوران شفيق ،السياسة الدولية والاستراتيجية آثر التهديدات الالكترونية على العلاقات الدولية(القاهرة:المكتب العربي للمعارف،ط 1،2016) ص 117.

[1] عادل عبد الصادق نفس المرجع 128.

[2] منى الأشقر جبور،مرجع سابق.ص.87.

ويتضح من خلال هذا الجدول أن الدول المتطورة على غرار أمريكا الشمالية وأستراليا وأوروبا هي أكثر الدول التي يتعرض سكانها للإختراقات الالكترونية،ونلاحظ أن إفريقيا هي المنطقة التي تعاني من أدنى نسبة إختراق بما يعادل 15%من هذه الاختراقات.

المطلب الثالث: خصائص الإرهاب السيبراني

لم تعد الحرب تقتصر على القوة العسكرية وقصف المواقع بل تعدت ذلك بفضل التطور المعلوماتي والإعتماد المتزايد للدول على التكنولوجيا فأصبحت الحرب هي الدخول إلى المواقع وتدميرها بفضل مجموعة من الخصائص وهي:

1. الإرهاب الالكتروني أداة من أدوات إرهاب الدولة وشن الحرب: فهذا النوع تقوم به الدولة من أجل بث الرعب والخوف والفزع في نفوس المواطنين، وهي عادة ما تلجأ لممارسة الإرهاب على وجه غير مباشر وذلك من خلال دعمها وتأييدها لمنظمة إرهابية[1].

2. يتوقف التهديد وتقيمه على حمله لنوايا إرهابية: يتوقف الفعل الإرهابي على درجة التقييم للنوايا وقدرات المهاجمين ودوافعهم السياسية وراء بث الرعب والخوف وإلحاق الأضرار المادية بهم.وهناك من يضع محددات أمام استخدام الجماعات الإرهابية لأدوات المجال الإلكتروني[2]، أي أن الإرهابيين قد يكون لديهم القدرة الفنية العالية التي تمكنهم من استخدام هذه الأدوات في الحرب واستخدام هذه الهجمات لا يكون وسيلة متاحة لجميع الإرهابيين.

3. عدم توافر درجة عالية من اليقين بشأن نتائج تلك الهجمات مقارنة مع الهجمات التقليدية.

4. القدرة على التخفي وتجهيل مصدر الهجمات: لعدم وجود أدلة مادية واضحة كما في الهجمات التقليدية،أما في الإلكترونية فتحسم المعركة في مدى الضرر الذي يصيب البنية التحتية للمعلومات.

5. سهولة التعرض للأخطار: فيلعب الحاسب الآلي دورا كبيرا في تسير الحياة المعاصرة نظرا لكفاءته العالية في معالجة البيانات.

[1] عبد الناصر حريز،"**الارهاب السيبراني دراسة تحليلية** "،(القاهرة:مكتبة مدبولي، ط1،1996).ص ص.278-230.

[2] عادل عبد الصادق،مرجع سابق.ص.121.

6. الأثر التدميري الضخم والأثر النفسي: وهذا بفضل إهتمام جميع وسائل الإعلام والمجتمع الدولي بتكنولوجيا المعلومات.

7. الهجوم المعتمد ذو دوافع سياسية.

8. الحاسب الآلي هو الأداة في القيام بهجمات الإرهاب الإلكتروني: ويقوم به الأشخاص ذوو خبرة وكفاءة فنية.

9. التكتيك والمناورة

المبحث الثالث: الحرب السيبرانية

الحرب هي مفهوم تقليدي يرتكز بالأساس على استخدام الجيوش النظامية وكان يسبقها إعلان واضح لحالة الحرب وميدان محدد للقتال، أما اليوم في هجمات الفضاء الإلكتروني فإنها غير محددة الأهداف لأنها تتحرك عبر شبكات المعلومات والإتصال المتعدية للحدود الدولية واعتمادها على الأسلحة الإلكترونية، وتشير الحرب السيبرانية إلى أي نزاع يحدث في الفضاء الالكتروني ويكون له طابع دولي.

المطلب الأول: تعريف الحرب السيبرانية

ومنه حسب (روبنسون بول) فالحرب السيبرانية لها عدة مسميات منها الحرب الإفتراضية، الحرب الرقمية، الحرب الإلكترونية...وقد عرفها "على أنها الحرب التي يتم شنها من خلال أجهزة الحاسوب وشبكة الانترنيت وهي تشمل على حد سواء إجراءات هجومية لإلحاق الضرر بنظم معلومات الخصوم أخرى دفاعية لحماية النظم الخاصة بالمهاجمين لحماية نظمهم من أي مهاجمة أخرى"[1].

وقد عرفها البعض "أنها تعني قيام دولة أو فواعل من غير الدول بشن هجوم إلكتروني في إطار متبادل أو من قبل طرف واحد"[2]. وعرف آخرون الحرب السيبرانية بأنها "مفهوم يشير إلى أي نزاع يحدث في الفضاء الإلكتروني ويكون له طابع دولي"[3]. فالحرب السيبرانية هي مجموعة من الإجراءات التي تنفذ بهدف الاستطلاع الإلكتروني للنظم والوسائل الإلكترونية المعادية وإخلال عمل هذه النظم والوسائل

[1] عبير شفيق الرحباني ،مرجع سابق،ص.256.

[2] نضال ناجي بريوش،مرجع سابق.ص.11.

[3] نفس المرجع.ص.11.

الإلكترونية ومقاومة الاستطلاع الإلكتروني المعادي وتحقيق استقرار عمل هذه النظم الصديقة تحت ظروف استخدام العدو أعمال الإستطلاع والإعاقة الإلكترونية[1].

وتعتبر الكاتبة الإسبانية يولاندا كينتانا(Yolanda Quintana) الحرب الإلكترونية بأنها" شكل من أشكال الإرهاب الإلكتروني خاصة وإن الهدف من هذه الحرب هو التدمير والسيطرة على العالم"[2]. وتعريف وزارة الدفاع الأمريكية للحرب السيبرانية "على أنها استخدام أجهزة الكمبيوتر والأنترنيت لإجراء الحرب في الفضاء الإلكتروني"

وتعريف ريتشارد كلارك و روبرت كناكي الذي ينظر لها على أنها "أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها"[3]، في حين يقترح البعض أنه بدلا من التركيز على أشكال وأنواع النزاع التي تحصل في الفضاء السيبراني ويحددون مستوياتهم على النحو التالي: فالقرصنة السيبرانية تقع في المستوى الأول، والجريمة السيبرانية تقع في المستوى الثاني والتجسس في المستوى الثالث في حين أن الإرهاب السيبراني يقع في المستوى الرابع وصولا إلى أخطر مستوى في النزاع ألا وهو الحرب السيبرانية.

المطلب الثاني: خصائص الحروب السيبرانية –الإلكترونية–

وتتميز هذه الحروب بجملة من الخصائص تتمثل أهمها في:

أنها حروب متسعة في الفضاء الإلكتروني أي أنها غير محدودة لا زمنيا ولا مكانيا، وتتميز كذلك بالتعقيد وقصر المدى وتتم بصورة مفاجئة وأفرادها قليلو العدد[4].

ومن خصائصها أيضا أنها حروب لا تناظرية فالتكلفة المتدنية نسبيا للأدوات اللازمة لشن هكذا حروب يعني أنه ليس هناك حاجة لدولة معينة أو منظمة أو حتى لقدرات ضخمة لتشكل تهديدا حقيقيا

[1] عبير شفيق الرحباني،نفس المرجع.261.

[2] نفس المرجع .ص،307.

[3] Richard A Clarke & Robert Knake, **Cyber War: The Next Threat to National Security and What Do About It ,** Harper Collins,2010,p,6.

[4]عبير شفيق الرحباني، نفس المرجع. ص،266.

وخطيرا على دولة عظمى[1] مثل الولايات المتحدة الأمريكية على سبيل المثال. ويتمتع المهاجم بأفضلية واضحة لأن هذه الحروب تتميز بالسرعة والمرونة والمراوغة.

كذلك تتعدى المخاطر باستهداف المواقع العسكرية إذ هناك جهود متزايدة لاستهداف البنى التحتية والمدنية الحساسة أو بواسطة فيروس يمكنه إحداث أضرار مادية حقيقية تؤدي إلى الدمار الشامل[2].

وتقوم الحروب الإلكترونية بمجموعة من العمليات من بينها:

– عمليات المراقبة الإلكترونية تتمثل في التنصت ورصد جميع الموجات الكهرومغناطيسية المعادية وتحليلها والإستفادة منها.

– عمليات التشويش الإلكتروني وتتم مثل هذه العمليات على نظم الكشف والإنذار والإستطلاع والتوجيه والإتصالات.

– عمليات الحماية وهي عمليات ضد المراقبة والتشويش الإلكتروني المعادي لتأمين النظم والمعدات المختلفة، وعدم إعطاء الفرصة للعدو للتشويش على النظم الأخرى المختلفة[3].

كما أن هذه الحروب تتميز بأنها قليلة التكلفة، فقد يتم شن حرب بتكلفة دبابة عبر أسلحة جديدة ومهارات بشرية ويتم استخدامها في أي وقت سواء كان وقت سلم أو حرب أو أزمة ولا تتطلب لتنفيذها سوى وقت زمني محدد وتعد تكلفة إطلاق تلك الهجمات أقل من أي سلاح تقليدي آخر. وتعد الحرب السيبرانية جزءا من عمليات المعلومات المستخدمة في مستويات ومراحل الصراع المختلفة سواء كان ذلك على الجانب الإستراتيجي أو التكتيكي أو العملياتي ضف إلى ذلك التأثير بشكل سلبي في المعلومات ونظم عمله في استخدام الفضاء السيبراني لإيجاد ميزة أو تفوق أو تأثير في البيئات المختلفة وعبر أدوات القوة.

المطلب الثالث: وسائل وأدوات الحرب السيبرانية

[1] اسماعيل زروقة، مرجع سابق، ص.1028.

[2] المجال الخامس. الحروب الالكترونية في القرن ال21، مركز الجزيرة للدراسات، على الموقع:
http://studies.aljazeera.net/ar/issues/2010/20117212274346868.html

[3] عبير شفيق الرحباني مرجع سابق،ص.264.

بعد المرور بالجريمة والإرهاب نصل الى الحرب كأعلى درجات الصراع فتتعدد وتتنوع وسائل وأدوات الحرب، ففي الحرب السيبرانية يتم توظيف وسائل وأدوات مغايرة عن الأدوات المستخدمة في الحروب التقليدية ومن بين هذه الوسائل نجد:

– **الفيروسات:** وهي عبارة عن برامج تصمم خصيصا لإحداث تدمير أو تعطيل برمجة الحواسيب دون علم أصحابها، وتختلف هذه الفيروسات من فيروس إلى آخر فمنها من هو صعب التحديد وهناك من هو سهل التحديد، ومنها ما هو باطني الإنتشار وهو لا يحدث تدمير أو تعطيل على مستوى الأجهزة[1] بل يحدث إزعاج وارتباك.

–**البريد الإلكتروني:** يعتبر من الوسائل المستخدمة في الحروب والجرائم وحتى كما يعرف بالإرهاب الإلكتروني أو السيبراني فهو أداة للتواصل بين الإرهابين وتبادل المعلومات فيما بينهم، فالبريد الإلكتروني يمكنهم من نشر أفكارهم والترويج لها[2]ومنه تعاطف الرأي العام وخاصة الأشخاص فئة الشباب، كذلك يساعد البريد الإلكتروني المخترقين في عملية التصيد وذلك من خلال إرسال رسائل إلكترونية تحمل فيروس بإمكانه نسخ جميع المعلومات للطرف المراد اختراقه.

–**التجسس الإلكتروني:** ويتم ذلك بواسطة الشبكة العنكبوتية والتجسس على الدول وحتى المنظمات[3]، ومراقبة المعلومات التي يتم تداولها بين الدول.

كما نجد أن الحرب السيبرانية لا تقتصر فقط على الفيروسات والبرامج العادية بل هناك وسائل أخرى كالتشويش المادي المباشر والمتعلق بموجات البث السلكي واللاسلكي وشبكات الطاقة وغيرها...[4]

المبحث الرابع: مقارنة بين التهديدات السيبرانية الثلاث (الجريمة، الإرهاب والحرب)

وكحوصلة لهذا الفصل قمنا بإجراء مقارنة بين كل من الجريمة والإرهاب والحرب السيبرانين، بحيث تلتقي الجريمة السيبرانية مع الإرهاب السيبراني إذ أنها تستغل آليات الإرهاب في تحقيق أهداف

[1] ـــــــ،**استعمال الانترنيت في تمويل الارهاب وتجنيد الإرهابين**، مركز الدراسات والبحوث، (السعودية: جامعة نايف العربية للعلوم الأمنية ،11 ماي 2011) ص 223.

[2] أيسر محمد عطية، **دور الآليات الحديثة للحد من الجرائم المستحدثة: الإرهاب الالكتروني وطرق مواجهته**، (الأردن: كلية العلوم الاستراتيجية،2014/09/04).ص،15.

[3] ريهام عبد الرحمان رشاد،الارهاب الالكتروني على تغير مفهوم القوة في العلاقات الدولية، دراسة حالة تنظيم الدولة" **المركز العربي الديمقراطي للدراسات الاستراتيجية والسياسية**"،(عدد375)،(2016/07/24)،ص 38.

[4] منى الأشقر جبور،نفس المرجع.ص.68.

ربحية مادية، بالتعاون مع المنظمات الإرهابية في تحقيق أهدافها مقابل الحصول على المال كالمنظمات العاملة في غسيل الأموال أو تجارة المخدرات والسلاح...

حيث يكون الترابط بين أعمال الإرهاب وارالجريمة السيبرانية من المرجح أن يزدهر في المستقبل فهم يتفقون في الوسيلة ويختلفون في الغاية، وهناك العديد من الجرائم التي تجمع الجريمة بالإرهاب السيبراني مثل: التجسس والقرصنة والجرائم المنظمة، غسيل الأموال...

وتتميز الجريمة السيبرانية بقدرة مرتكبيها الفائقة على إلحاق خسائر كبيرة وتأتي الجريمة في عدة أشكال من الإرهاب والتجسس والقرصنة والجرائم المنظمة والفيروسات، وتواجه الجهات القانونية صعوبة في ضبط الجرائم بسبب أنها تقوم بصورة مستترة وغياب الدليل المرئي، وعدد كبير من البيانات، وتقع الجريمة في استخدامات شبكة الاتصالات ويتعدى إلى الوصول بالمساس بحق الحياة والترويج لمنتجات غير أخلاقية واستخدام الأنترنيت في ارتكاب الجرائم المنظمة والإرهابية من خلال تبادل المعلومات والشيفرة[1]، وتتعلق مشكلة التعاون الدولي في مجال الجريمة السيبرانية بأنه لايوجد إجماع عالمي حول نوعية السلوك الذي يشكل الجريمة وعدم وجود خبرة في المجال الأمني والقانوني.

كما أن هناك اختلاف بين الإرهاب السيبراني والحرب السيبرانية تنقسم هذه الأخيرة إلى نمط دفاعي وهجومي؛ فالهجومي تقوم به الدول وأجهزة استخباراتها وتستخدم لأهداف سياسية وعسكرية لتحقيق أهداف إجرامية ويستحوذ على المعلومات وتعطيل نظمها، أما الدفاعية تعمل على الحد والوقاية من أعمال التخريب التي قد تتعرض لها. وتستخدم الحرب لتحقيق الأهداف القومية، أما على المستوى العملياتي فإنها تستخدم للتأثير على شبكات الإتصال وهنا يبرز الفرق بين الحرب السيبرانية والإرهاب السيبراني في شكل استخدام القوة، وتتميز الحروب السيبرانية المعلوماتية بتعدد الفاعلين من الدول أو الجماعات الإرهابية أو أفراد وتتعدد الوسائل والغايات ومنه يمكن القول بأن هناك علاقة وثيقة بين الحرب والإرهاب السيبراني[2]، حيث أن الفاعلين في الإهاب يمكن أن يستخدموا الحرب المعلوماتية كأداة لتنفيذ أهدافهم، وكذلك قد تتحول الحرب إلى فعل إرهابي إما بمن يقف وراء استخدامها كالجماعات الإرهابية من خلال الحكم عليها وفقا لطريقة التنفيذ التي تأخذ نفس تقنيات العمل الإرهابي التي تعتمد على هجمات الخوف والترويع والكر والفر.

[1] جريدة عالم اليوم،**صفحة عالم الكمبيوتر**، 1 نوفمبر 2005 .

[2] عادل عبد الصادق مرجع سابق.ص –ص 13-135.

نجد أن الجريمة السيبرانية تسعى إلى المال والأرباح بينما الإرهاب الإلكتروني هدفه ممارسة الضغط السياسي، فرض شروط على السلطة من خلال نشر الذعر والهلع، كما نجد هناك تداخل بين المفهومين فالجريمة ترى في الإرهاب مصدر للمال والسلطة والإرهاب يرى في الجريمة على أنها وسيلة لجمع وتأمين الموارد[1].

الإختلاف يكون في الوسائل والأدوات المستخدمة، كذلك نجد بأن الإرهاب عبارة عن هجوم أو تهديد بالهجوم على أجهزة الكمبيوتر بهدف تدمير أو تعطيل البنى التحتية للدول وترهيب المواطنين وإجبارهم على تحقيق أهداف سياسية اجتماعية كما أنه يستخدم الأنترنيت من أجل الدعاية والتضليل.

أما الجريمة فهي نشاط غير مشروع تقوم بنسخ أو تغير أو حذف أو الوصول الى المعلومات المخترقة في الحواسيب، فهي إذن متعلقة بالمعالجة الآلية للبيانات أو نقلها[2]، كذلك تعتبر الحرب شكل من أشكال الإرهاب الإلكتروني خاصة وأن الهدف منها هو التدمير والسيطرة على العالم[3].

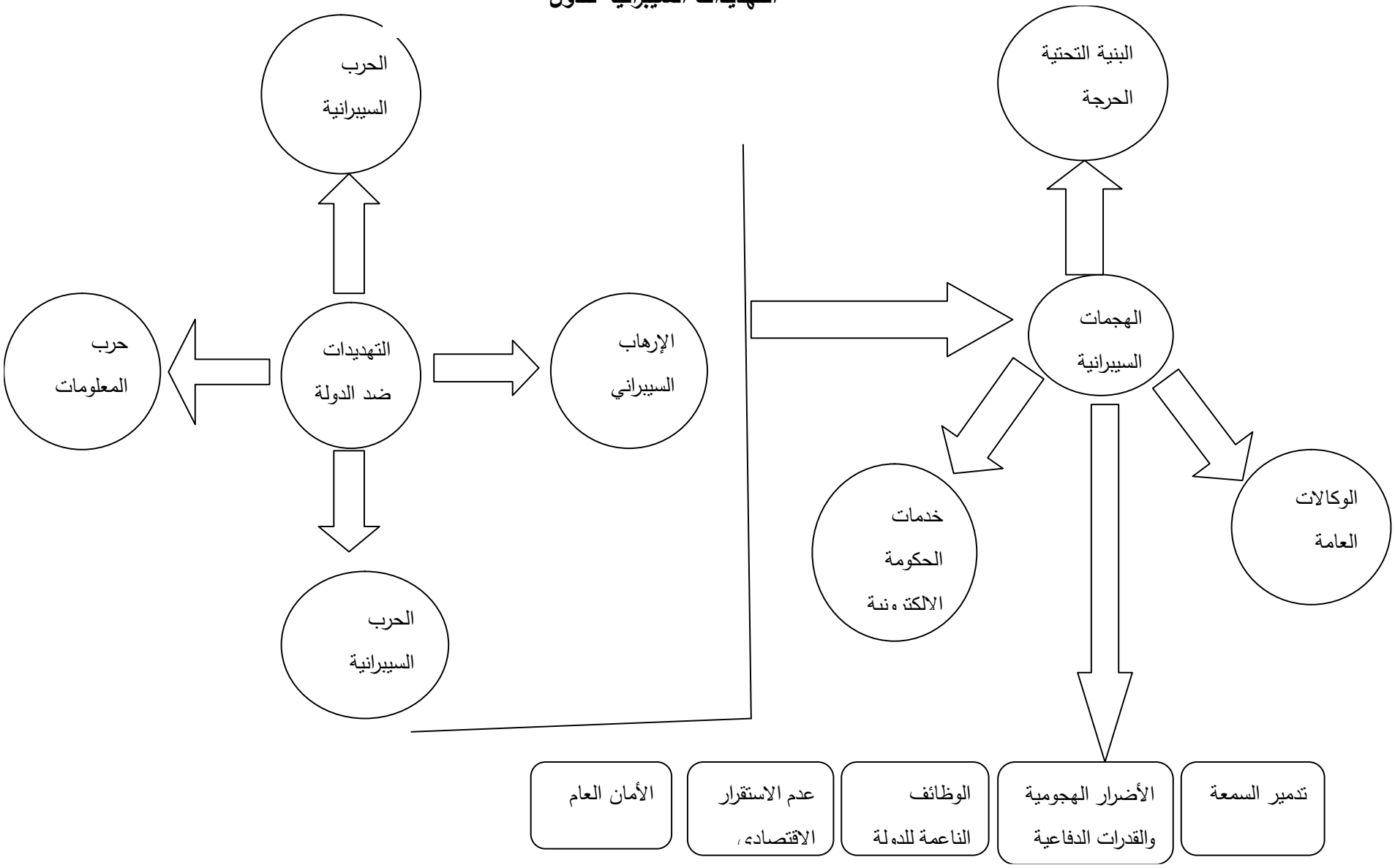
مخطط يوضح التهديدات السيبرانية للدول

[1] منى الأشقر جبور مرجع سابق.ص ص .86 87.

[2] تغريد معين حسن المهدي،"الأثر العسكري للأمن السيبراني في الجغرافيا السياسة للدولة"،**مجلة البحوث الجغرافية**،(ع30)،جامعة الكوفة :كلية الآداب ،قسم الجغرافيا.ص242.

[3] عبير شفيق الرحباني،مرجع سابق،ص،307.

التهديدات السيبرانية للدول



المصدر:سماح عبد الصبور،الصراع السيبراني التنازع العالمي على قوة الفضاء الالكتروني ،مجلة السياسة الدولية عدد أفريل 2018.ص 7.

ونلاحظ من خلال هذا المخطط أن التهديدات ضد الدولة تأتي في أشكال عديدة قد تكون حرب سيبرانية أو إرهاب سيبراني أو حرب سيبرانية...وتستهدف هذه التهديدات البنية التحتية والوكالات العامة أو حتى الخدمات الالكترونية للدول وخذا ما يؤدي إلى تدمير السمعة ،عدم الاستقرار الاقتصادي ،خلل في الأمان العام.

وكحوصلة لهذا الفصل نستنتج أنه بالرغم من التطور الحاصل في الميدان التكنولوجي وخاصة المجال السيبراني هناك العديد من التهديدات التي تواجه الدول أو المنظمات الدولية على حد سواء كالجريمة والإرهاب والحروب السيبرانية ولم تقتصر هذه الأخيرة على الدول فقط بل تعدت إلى فوق دولية شركة مقابل دولة أو حتى فرد مقابل دولة ،فبالرغم من أن ميدان تكنولوجيا المعلومات يعد نعمة إلا أنه وفي نفس القت نقمة بفعل هذه التهديدات السيبرانية التي يشكلها على الدولة والفرد على حد سواء في جميع المجالات والميادين.

الفصل الثالث

نتناول في هذا الفصل المعنون بـ: الأمن السيبراني في السياسة الدولية: نماذج وتوصيات ثلاث مباحث رئيسية خصص الأول للحديث عن بعض النماذج عن الهجمات والحروب السيبرانية تم فيه مرعاة التماثلية منها وغير تماثلية، أما المبحث الثاني فتناول الجهود الدولية المتعلقة بميدان الأمن السيبراني من مخرجات لمؤتمرات وقرارات تكللت بجهود دولية ووطنية، و اهتم المبحث الثالث بدراسة أهم التوصيات والمقترحات المتعلقة بمجال الأمن السيبراني في ظل هذه البيئة السياسية متجددة في عالم منغير خاصة في مجالات الاتصال والمواصلات المتعلقة بالجوانب المعلوماتية للانترنيت.

المبحث الأول: نماذج مختارة عن الأمن السيبراني في السياسة الدولية

وسنتناول في هذا المبحث بعض النماذج المتعلقة بالأمن السيبراني من نماذج تماثلية تتقابل فيها الدولة بمثيلتها من الدولة وكذا نماذج غير تماثلية تتواجه فيها الدولة مع شركة متعددة الجنسيات وهذا بما شهدته الساحة الدولية من تزايد في النشاطات السيبرانية في السياسة الدولية.

المطلب الأول:الحروب السيبرانية ممثلة وفقا للثنائية (دولة_دولة):(إيران–أمريكا)

عرف المجتمع الدولي العديد من الهجمات الالكترونية التي استهدفت أرضية بيانات الدول وحتى الشركات الاقتصادية والتجارية وأبرز هذه الهجمات هو هجوم دودوة ستاكنست Stuxnet على الأجهزة النووية الإيرانية وحسب الخبراء صنف هذا الفيروس من أخطر وأعقد البرامج الالكترونية الخبيثة.

في سنة 2010 تعرض البرنامج النووي الإيراني لهجوم إلكتروني مدمر كان غرضه إيقاف أنشطة إيران النووية، ووجهت أصابع الاتهام لكل من أمريكا،بريطانيا،فرنسا،ألمانيا وحتى إسرائيل ولكن أبرزها الولايات المتحدة الأمريكية وإسرائيل وهذا راجع لعدم جدوى العقوبات الاقتصادية المفروضة على إيران[1].

وقد أدى هذا الفيروس إلى تعطيل معمل أصفهان لتبديل ثاني أكسيد اليورانيوم إلى اليورانيوم الطبيعي وذلك من خلال ضرب البرامج المعلوماتية،وهذا ما تسبب في تعطيل أكثر من 30 ألف حاسوب بمفاعل"نطنز"[2]كما دمر أيضا حوالي 100 جهاز طرد مركزي في "نطنز"،ولم تتمكن إيران من افتتاح المفاعل في أوت 2010 كما كان مقررا من قبل بل تم افتتاحه في سبتمبر 2011،بعد مرور عام من تاريخ الهجوم أي بعد خسارة مليارات الدولارات في إصلاح ما أفسده فيروس "ستاكنست"[3].

لم يتوقف الهجوم السيبراني على إيران عند هذا الحد بل شهدت هجوما آخر لبرنامجها النووي سنة 2012 بواسطة فيروس آخر يدعى فيروس"فلايم"أو الشعلة[4] والغرض من هذا الفيروس هو التجسس وليس التدمير،وذلك من خلال سرقة البيانات والتسجيلات الصوتية بواسطة الميكروفونات الداخلية في

---

[1] نوران شفيق،مرجع سابق.ص153.

[2]نبيل العتوم،هجوم إلكتروني على إيران والرد قادم ضد المحور الخليجي :مركز أمية للبحوث والدراسات الاستراتيجية في:
http://www.umayya.org/articles/umayya-articles/14092,(25/06/2020)

[3] نوران شفيق،نفس المرجع.ص،153.

[4] نبيل العتوم،نفس المرجع

الأجهزة ،تسجيل حركات الضغط على لوحة المفاتيح Keystrokes وأخذ صور من الرسائل النصية على الجهاز[1].

هذا وقد تجددت على إيران الهجومات الإلّكترونية في يونيو 2019،حيث قامت إدارة ترامب بشن هجوم إلكتروني على قاعدة بيانات الحرس الثوري المستخدمة لشن هجومات على ناقلات النفط ،مما تسبب في مسح شاشات الحرس الثوري.كما عاودت الولايات المتحدة الأمريكية هجوما آخر في سبتمبر 2019،بعد أن أطلقت إيران طائرات دون طيار وصواريخ كروز على منشأتين نفطيتين[2]،وفي مقابل تلك الهجمات قامت إيران هي الأخرى بتوجيه ضربات أو هجمات إلكترونية من أجل رد الإعتبار ومن بين أبرز تلك الهجمات عملية أبابيل سبتمبر 2013/2012 والتي استهدفت المؤسسات المالية الأمريكية وتزامن وقوع هذه العملية مع الفترة التي كانت واشنطن تفرض فيها عقوبات على البنك المركزي الإيراني وتم استخدام هجمات موزعة للحرمان من الخدمات وذلك من أجل تعطيل وعرقلة برامج الخدمات المصرفية عبر الأنترنيت إضافة إلى توقيف بعض الوظائف التجارية لإحدى الركائز الحساسة في الاقتصاد الأمريكي مما تسبب في خسائر وأضرار بلغت عشرات ملايين الدولارات،وبالرغم من أن هذه الهجومات تنسب إلى المقاتلين الإلكترونين في كتائب عز الدين القسام لكن يرجح بأن الحكومة الإيرانية وراء ذلك[3].

وفي27 سبتمبر 2013 عاودت إيران الكرة وذلك حين قام قراصنة إيرانيون باختراق أجهزة الكمبيوتر التابعة للبحرية الأمريكية،ولم تكتف إيران بهذا بل قامت أيضا في السنة الموالية أي عام 2014 باستهداف شركة "لاس فيغاس ساندر كلوب" ونتج عن هذا الهجوم غلق أنظمة الاتصالات ومسح محركات الأقراص الصلبة[4].

ولم تكتفي إيران بهذا القدر من الهجومات السيبرانية على الولايات المتحدة الأمريكية بل واصلت أعمالها الهجومية والمقرصنة وأبرز مثال على ذلك فيروس شمعون بحملاته الثلاث،وآخرها كان في سنة

---

[1] نوران شفيق،نفس المرجع.ص،156.

[2] ضربات أمريكية سيبرانية موجعة لإيران في:

http://makkah news paper.com/article/1502614(30/06/2020)

[3] ميكا لوديرميلك–الأزمة الإيرانية تنتقل إلى الفضاء السيبراني،حقوق الطبع والنشر 2018من قبل معهد واشنطن http://www.washingtoninstitute.org/ar/policy-analysis/view/iran-crisis-moves-into-cyberspace.(02/07/2020)

[4] ضربات أمريكية سيبرانية موجعة لإيران،نفس المرجع.

2016 بعدها عرفت العلاقات الإيرانية الأمريكية نوعا ما فترة من الهدنة أو الاستقرار لتعود للواجهة مرة أخرى، حيث تزامن ذلك مع انسحاب إدارة دونالد ترامب من الصفقة النووية لسنة 2018 حيث حذرت شركة كروبد ستريك للأمن السيبراني عملائها بأن تزايدت بشكل ملحوظ عمليات الاختراق والتصيد من قبل إيران وفي سنة 2019 ادعت شركة مايكروسفت بأن هناك محاولة اختراق لحسابات البريد الالكتروني التي تتعلق بمسؤولين وصحفيين للحكومة الأمريكية [1]والحملة الرئاسية بصفة عامة وهذه الاختراقات قام بها مجموعة من الهاكرز وكما يطلق عليها باسم "الفوسفور "التابعين للحكومة الإيرانية.

وفي مطلع سنة 2020 شهدت إيران حادثة إغتيال قاسم سليمان وهو قائد فيلق القدس التابع للحرس الثوري وهو ما أسهم في تأجيج الصراع بين الطرفين (إيران والولايات المتحدة الأمريكية) وزاد من معدل الهجمات السيبرانية الإيرانية. حيث أنه في اليوم الموالي أي بعد وقوع الحادثة بيوم قامت إيران بعملية إختراق الموقع الالكتروني لبرنامج مكتبة الإيداع الفيدرالية الأمريكية هذا مازاد من احتمال حدوث تصعيد التوتر بين الطرفين مع إمكانية حدوث حرب إلكترونية حقيقية خاصة بعد إعلان إيران عن نيتها في الانتقام وشن هجمات جديدة تمس البنوك، المرافق والقطاعات الحيوية... وبالرغم من أن إيران ليست لديها نفس درجة التقدم والخبرة التي تمتلكها الولايات المتحدة الأمريكية في مجال الأمن السيبراني خاصة وأن هذه الأخيرة (الولايات المتحدة الأمريكية) لديها ترسانة دفاعية سيبرانية تمكنها من صد أي هجوم الكتروني لكن كل هذا لا يمنع إيران من تطوير أنظمتها الإلكترونية التي تؤهلها للقيام بالهجمات السيبرانية مستقبلا. كما نستخلص أيضا بأن هذه الحرب بين الدولتين ليست مرهونة بزمن معين أو محدد فهي مازالت مستمرة ومازالت ردود الإنتقام متواصلة من قبل الطرفين لكن يبقى هناك إحتمال العدول وعدم تصعيد الأزمة والتي يمكن من خلالها حدوث التصادم المباشر.فكل هذه الاحتمالات مرهونة بالأوضاع السياسية والاقتصادية الدولية في السنوات القادمة[2].

المطلب الثاني: الحروب السيبرانية ممثلة وفقا للثنائية (دولة–شركة دولية): (الصين–شركة غوغل)

شهدت العلاقات الأمريكية الصينية على مر العصور توترات وصلت إلى حد الصراع في جميع المجالات فبعدما كان صراعا عسكريا،جيوبوليتكيا أصبح تجاريا،إقتصاديا سيبرانيا يخص مجال الفضاء الالكتروني ومع مبدأ انعدام الثقة في الطرف الاخر حسب ماتؤمن به المقاربة الواقعية،بأن الطرفين

[1] نفس المرجع

[2] ياسمين أيمن،هل تشتعل الحرب بين أمريكا وإيران بعد مقتل سليماني في(12/07/2020)http://al-ain-com/article-iran

أصبحا يشككان في نوايا بعضهم البعض وأي محاولة يقوم بها الطرف (أ)هي بمثابة عملية تجسس ومحاولة إختراق للطرف(ب)،خصوصا بعد استثمار كلا الدولتين في الأنظمة الشبكية أو كما يسميها xinxibia أو.informatization مارستا الدولتان التجسس الالكتروني ضد بعضهما البعض ولأسباب عديدة[1].ومن أشهر الهجمات السيبرانية اللاتماثلية التي حدثت في العقود الأخيرة هي الهجوم أو النزاع السيبراني بين الصين وشركة غوغل الأمريكية.

فمنذ دخول شركة غوغل لسوق الصين في عام 2006،حدث إشتباك بين محرك البحث العملاق غوغل وحكومة جمهورية الصين بخصوص الرقابة وقضايا أخرى.وقد تطور مخرك البحث"google" الصيني ليصبح بذلك ثاني أكبر خدمات جمع المعلومات استخداما في الصين بعد الشركة الصينية Baidu ،وكان أيضا أقل تعرضا للرقابة كما أن شركة غوغل حاولت الامتثال لسياسات الرقابة في جمهورية الصين الشعبية فحددت خدماتها فقط كمحرك بحثي،دون تقديم خدمات البريد الالكتروني،كما أنها كانت تضع أو تقدم رسائل للمستخدمين الصينين تفيد بأن أحد المواقع المحجوبة أصبح غير متاح بسبب القوانين واللوائح والسياسات المحلية،مما يوحي للمستخدم الصيني بوجود معلومات،لكن الحكومة الصينية أغلقت الوصول إلى هذا الموقع .

وفي 2010 هددت غوغل Google بوقف تصفية محرك البحث الصيني الخاص بها أو الانسحاب من الصين،وأكدت الشركة أنه في ديسمبر 2009 هاجم قراصنة صينيون خدمة Gmail الخاصة بها وشاركوا في دمج الشبكة بالإضافة إلى أنظمة الكمبيوتر للعديد من الشركات الأمريكية الكبيرة الأخرى في الصين في ما أطلقت عليه الصحافة اسم "عملية فجر""auroia operation"والتي تم فيها إختراق الأجهزة الالكترونية التابعة للشركة وذلك من أجل سرقة المعلومات الموجودة فيها،كذلك اختراق حسابات Gmail لنشطاء حقوق الإنسان الصينين،ومسؤولين في الإدارة الأمريكية وبالرغم من أن Google أكدت في فبراير 2010 بأن الهجمات جاءت من الصين،إلا أن بكين نفت تورطها ودافعت عن سياسات الانترنيت الخاصة بها.وذكرت وزارة الخارجية للصين أن الشركات الأجنبية بما في ذلك غوغل Google يجب أن تحترم القوانين واللوائح كما تحترم المصلحة العامة للشعب الصيني وثقافة وعادات الدولة الصينية.وردا على هذا قامت شركة غوغل بتحويل محركها البحثي للمستخدمين في الصين إلى

[1] سكوت وارين هارولد،مارتن سي ليبيكي، استريد ستوت سيفالوس،"التوصل إلى إتفاق مع الصين بشأن الفضاء الالكتروني،2016" www.rand.org/t/rr1335.

آخر في هونغ كونغ غير خاضع لأي شكل من أشكال الرقابة ومن خلال هذا اعتبر الاعلام الصيني أن ماتقوم به شركة غوغل هو جزء من مؤامرة أمريكية على الصين[1].

وبالرغم من إدعاء الحكومة الصينية و الإعلام الصيني بأن هناك مؤامرة تحاك من قبل الولايات المتحدة الأمريكية وإتهامها بالتجسس.لا يعتبر مبررا قويا لتلميع صورتها أمام الرأي العام العالمي،فهي متهمة أيضا من طرف عدة دول ليس فقط الولايات المتحدة الأمريكية بل أيضا ألمانيا،فرنسا،المملكة المتحدة وغيرها من الدول الأخرى.

ومن خلال هذا التنازع بين شركة غوغل والصين نستنتج بأن العلاقات بين الدول لاتتأثر فقط بالفواعل الدوليين،وإنما تتأثر وتتوتر حتى بين فواعل غير دولية أو فواعل غير متماثلة (دولة في مقابل شركة)ما يحدث علاقات على مستوى العلاقات بين الدول ويتعداه كذلك إلى مستويات ومجالات أخرى تؤثر في هيكلة النظام الدولي أو حتى في قضايا السياسة العالمية.

إضافة إلى هذين الهجومين عرفت البيئة الدولية هجومات سيبرانية عديدة نذكر منها:

_دولة إستونيا ففي عام 2007 تعرضت لهجوم إلكتروني مس المواقع الخاصة للبنوك،والجرائد والخدمات الحكومية الالكترونية ما أدى إلى تعطيل وإيقاف تلك المواقع على تقديم خدماتها وأيضا تعطيل كافة أجهزة الدولة،ماجعل من دولة إستونيا أن تستعين بحلف الناتو NATO من أجل مواجهة هذه الهجومات وقد وجهت إستونيا اتهامات للحكومة الروسية بكونها هي من قامت بتلك الهجمات ،وذلك بعدما اكتشفت إستونيا أن أنظمة التحكم التي تم شنها موجودة في روسيا وبالرغم من إنكارها لعلاقتها بالهجوم ،إلا أنها إعترفت بأنه من الممكن أن يكون قد شن من داخل روسيا وذللك من قبل منظمات إجرامية ،وانه ليس هناك دخل ولا صلة للحكومة الروسية بهذا الهجوم لكن كل هذا النفي والإنكار لم يخدم روسيا خاصة أمام المجتمع الدولي فأغلب الدول وجهت أصابع الإتهام لروسيا[2].

_الهجوم الالكتروني اللاتماثلي (كوريا الشمالية ضد شركة صوني بيكتشرز للأفلام السينمائية والأعمال التلفزيونية والتوزيع) على غرار شركة غوغل لم تسلم شركة صوني بيكتشرز هي الأخرى من الهجمات السيبرانية،وقد كان هذا في نوفمبر من عام 2014 بسب فيلم المقابلة(the interview) الكوميدي الذي

[1] Thomas Lumetal ,China Internet Freedom and US.Policy,Congressional Reserch Service,Julay,13,2012.pp8,9.

[2] نوران شفيق،نفس المرجع.ص ص.140،142.

تدور أحداثه حول مسألة إغتيال زعيم كوريا الشمالية كيم جونغ أون(Kim jong-un) وقد أدى هذا الهجوم إلى نشر معلومات حساسة خاصة بالاستوديو السينمائي والتي تشمل معلومات شخصية ورسائل الموظفين الالكترونية،إضافة إلى أفلام لشركة صوني للأفلام السينمائية و الأعمال التلفزيونية والتوزيع لم تعرض بعد كما قد تعرضت أعمال الشركة بدرجة كبيرة.وقد تبنت هذا الهجوم مجموعة أطلقت على نفسها اسم حراس السلام(Guardian of peace) كما هددت أيضا بتنفيذ هجومات أخرى من بينها هجمات مادية على صالات العرض وهذا إذ واصلت شركة صوني بيكتشرز للأفلام السينمائية والأعمال التلفزيونية والتوزيع خطتها لإطلاق فيلم المقابلة[1].

وبخصوص مصدر هذا الهجوم ومن كان وراءه،ثم توجيه أصابع الإتهام لكوريا الشمالية وهذا بعد تدخل الولايات المتحدة الأمريكية وقيامها بفتح تحقيق حول مصدر الهجوم ودوافعه وهذا بالتعاون مع شركة صوني بيكتشرز للأفلام السينمائية والأعمال التلفزيونية والتوزيع،وقد خلص هذا التحقيق إلى بيان صدر عن مكتب التحقيقات الفيدرالي الأمريكيFBI بأن كوريا الشمالية هي من تقف وراء هذا الهجوم وهي المسؤول الأول عن هذه الهجمات كون أن هذه الأخيرة سبق لها وأن استخدمت وسائل التسلل والقرصنة الكترونية مماثلة في هجمات سابقة قامت بها ومن بينها دولة كوريا الجنوبية.

المبحث الثاني: الجهود الدولية والوطنية في تحقيق الأمن السيبراني ومواجهة التهديدات السيبرانية

سنتطرق في هذا المبحث لأهم وأبرز الإتفاقيات والمؤتمرات من جهود دولية ووطنية في مجال تحقيق الأمن السيبراني وسبل مواجهة هذه التهديدات.

المطلب الأول: الجهود الدولية والإقليمية لمواجهة التحديات السيبرانية

أولا: إتفاقية المجلس الأوروبي للجريمة الالكترونية

تعد أول مبادرة عالمية وأنجح مثال للتعاون الدولي في مجال الفضاء الالكتروني لمكافحة التهديدات الالكترونية.وتعد الاتفاقية الدولية الوحيدة الملزمة ، بدأ توقيع هذه الاتفاقية في 8 نوفمبر 2001

[1] تهديدات مجهولة المصدر نحو مساءلة دولية في الفضاء الالكتروني John S Davis//ct Benjamin Bourdeaux ex.www.rang.org/t/r 2081.2017.

ودخلت حيز التنفيذ عام 2004.وكان لها دور كبير في إبراز مدى إدراك الدول لأهمية الأمن الإلكتروني وضرورة مجابهة أنواع التهديدات التي تعترض أمنها القومي[1].

تسعى هذه الاتفاقية إلى إعداد نظام فعال وسريع للتعاون الدولي، كذلك تحقيق التوافق والانسجام بين الدول الموقعة مع إقرار قانون جنائي مشترك هدفه حماية المجتمع الدولي من مختلف الجرائم الالكترونية[2].

وبالرغم من أن هذه الاتفاقية تعد النموذج الأصلح والأمثل في التعاون الدولي للتصدي للهجمات الالكترونية إلا أنها تحتوي على قصور في بعض الجوانب فعدم المصادقة عليها ودخولها حيز التنفيذ في الوقت الوجيز والمحدد الذي أدى إلى عرقلة الوصول للهدف الأساسي وهو التعاون الدولي في وقت زمني قياسي الذي قارب 10 سنوات، ما جعل من الجريمة الالكترونية بمختلف أنواعها تنتشر وتتوسع أكثر. ما جعلها تتسبب في إحداث خسائر مادية كبيرة حيث وصلت في عام 2013 إلى أكثر من 450 مليار دولار[3]، بالإضافة إلى غياب بعض الدول الكبرى ذات الوزن المحوري في النظام الدولي وخاصة في الفضاء السيبراني عن عضويتها مثل الصين وروسيا، لكن الدول الأوروبية والولايات المتحدة الأمريكية لم توقع على هذه الاتفاقية بالرغم من أن العديد من الهجمات السيبرانية مصدرها هاتين الدولتين ودائما تضعها محل اتهام الكثير من الدول هذا إلى جانب غياب الدول الآسيوية والإفريقية وحتى دول أمريكا الجنوبية الغربية[4]،فكل هذا التباطؤ من قبل الدول للانضمام إلى الاتفاقية والمصادقة على تنفيذها أدى إلى إرتفاع نسبة الجرائم السيبرانية مما جعلها تخرج عن سيطرة الدول لكبح مخاطرها.

وأيضا من ضمن الجهود الدولية لمكافحة الجرائم السيبرانية تم إطلاق برنامج اليوم العالمي لأمن الانترنيت Safer Internet Day[5] والذي يصادف شهر فيفري من كل سنة وكانت الإنطلاقة لأول مرة في عام 2004 وهذا كمبادرة من الإتحاد الأوروبي والمنظمة الأوروبية لتوعية لشبكة الأنترنيت "إنسيف"المهتمة بالقضايا ذات الصلة بالانترنيت والهدف من هذا البرنامج (اليوم العالمي) هو زيادة

---

[1] نوران شفيق،مرجع سابق.ص96.

[2] ـــ،الجريمة الالكترونية في المجتمع الخليجي وكيفية مواجهتها2016(سلطنة عمان:مجمع البحوث والدراسات أكاديمية السلطان قابوس لعلوم الشرطة).ص،61.

[3] نفس المرجع،ص،65.

[4] نوران شفيق،نفس المرجع.ص،97.

[5] ليلى الجنابي،"فعالية القوانين الدولية في مكافحة الجرائم السيبرانية"في:
http://www.ssrcaw.org.art.asp?aid=571423&ac=2(15/07/2020)

مستوى الوعي بمخاطر الانترنيت جراء سوء الاستخدام، كذلك وضع أدوات وبرامج علمية وتقنية هادفة ،إضافة إلى تعزيز التعاون المشترك والعمل على إيجاد آليات لاستخدام آمن للانترنيت[1]

ثانيا: الاتحاد الدولي للاتصالات

هو أحد الأجهزة المنظمة للأمم المتحدة مختص بتنظيم الاتصالات.ومع توسع نطاق اختصاصه أصبح يشمل الأمن السيبراني ليختص بذلك دراسة المواضيع ذات الصلة بالأمن السيبراني من بينها تدريب الدول النامية على مواجهة أخطار الفضاء السيبراني، ففي عام 2007 أصدر الإتحاد الدولي للاتصالات بما عرف "الأجندة العالمية للأمن الالكتروني" والتي تحاول خلق إطار للتنسيق والتعاون بين الدول لمواجهة المخاطر السيبرانية، وكذلك بناء الثقة بين الفواعل الدولية مع تطوير أنظمة للإنذار المبكر[2].

ثالثا: جهود الاتحاد الإفريقي

قدم الاتحاد الإفريقي هو الآخر استراتجيات بشأن الأمن الرقمي في إفريقيا إضافة إلى بعض المشاريع والمؤتمرات بسب العجز الذي تعرفه افريقيا في مختلف المجالات والقطاعات وكان سببا في عرقلة طريق تطورها، لكن بالرغم من ذلك تحدت بعض حكومات الدول الإفريقية الوضع وساهمت في إنعاش بعض القطاعات أهمها قطاع تكنولوجيا المعلومات والاتصالات وبدأ التفكير في استراتيجية للتحول من الاهتمام بالجانب التقليدي واستخدام الوسائل البسيطة نحو قطاع حديث رقمي مع إحداث ثورة في القارة مستقبلا.

هذا ماجاء في تقرير اجتماع الخبراء للدورة الثالثة للجنة الفنية المتخصصة للاتصال وتكنولوجيا المعلومات والاتصالات للاتحاد الافريقي والذي تم عقده من 22 إلى 24 أكتوبر 2019 بمصر كما تم وضع استراتجيات للتحول الرقمي الشامل في إفريقيا وذلك من 2020 حتى 2030 كما قامت أيضا مفوضية الإتحاد الافريقي سميت "باتفاقية مالابو" والتي عقدت بمالابو في 2014 وذلك في الدورة الثالثة والعشرين لمؤتمر رؤساء دول وحكومات الاتحاد الافريقي بخصوص الأمن السيبراني وحماية البيانات الشخصية وهذا من أجل تعزيز ثقافة الأمن السيبراني وأيضا تعزيز القدرات السيبرانية للدول كإعداد

[1] نفس المرجع.

[2] نوران شفيق،نفس المرجع.ص109.

إستراتيجيات وآليات الاستجابة للحوادث مثل: فرق التصدي للحوادث الحاسوبية كذلك منع الجرائم السيبرانية إضافة إلى تلك الأهداف وضعت مفوضية الاتحاد الافريقي مبادئ توجيهية بخصوص أمن البنية التحتية للانترنيت في افريقيا وكذلك حماية البيانات الشخصية[1].

ولم يكتف الإتحاد الافريقي بهذه الاتفاقية بل واصل في متابعة ودراسة الأوضاع في الفضاء السيبراني الافريقي ووضع استراتيجيات لمواجهتها وكذلك تكثيف جهود الدول الأعضاء واهتماماتهم، حيث أنه وفي سنة 2016 وبالتعاون مع شركة سيمانتيك ووزارة الخارجية الأمريكية،نشرت مفوضية الاتحاد الافريقي تقريرا عن اتجاهات الأمن السيبراني والجرائم السيبرانية في افريقيا. وفي عام 2018 أجاز المجلس التنفيذي للاتحاد الافريقي اعلان بخصوص إدارة الانترنيت وتطوير الاقتصاد الرقمي كما جعل الأمن السيبراني مشروعا رئيسيا لأجندة 2063[2].

كذلك هناك جهود أو تعاون دولي إقليمي منها:

1_**مؤتمر الأمن السيبراني جامعة نيويورك للتكنولوجيا** 18 سبتمبر 2014 شارك فيه مجموعة من خبراء الانترنيت والشركات وحتى الحكومات وتطرق هذا المؤتمر لموضوعات تتمثل في:

–أنظمة الأمن والانترنيت والابتكارات في المؤسسات الأجنبية،حماية البنية التحتية الحساسة كذلك حماية المنظمات والحكومات والأفراد من الهجمات السيبرانية[3]

2_**مؤتمر قمة الأمن السيبراني مينابولس مينيسوتا الولايات المتحدة الأمريكية:** مابين 21 و22 أكتوبر 2014 شارك فيه ممثلي القطاع العام والقطاع الخاص من أجل معالجة ومناقشة التدابير والإستراتيجيات المضادة للتهديدات السيبرانية، كذلك تطوير مهارات التحقيق التقنية والأدلة العلمية إضافة إلى الإستراتيجيات الشاملة لمواجهة خطر الجريمة الإلكترونية وعلاوة على هذا قياس مدى تأمين برامج الحاسب الآلي ضد الهجمات السيبرانية، ومن بين التدابير المهمة التي نوقشت في هذا المؤتمر هي تعزيز أمن القطاعين العام والخاص في مواجهة مختلف الجرائم الالكترونية[4].

---

[1] ليلى الجنابي،فعالية القوانين الوطنية والدولية في مكافحة الجرائم السيبرانية،مرجع سابق.

[2] نفس المرجع.

[3] ___،الهجمات السيبرانية في المجتمع الخليجي وكيفية مواجهتها، نفس المرجع .72.

[4] ليلى الجنابي"فعالية القوانين الوطنية والدولية في مكافحة الجرائم السيبرانية "مركز الدراسات والأبحاث العلمانية في العالم العربي،2017/7/8: في .http://www.ssvcaw.org/ar/art/show-art.asp?aid=571423

3_**المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية:** والذي نظمته جامعة الإمام محمد بن سعود الإسلامية،المتمثلة في كلية علوم الحاسب والمعلومات في 10–12نوفمبر 2015.

4_ **مؤتمر لندن للفضاء الالكتروني نوفمبر 2012:** تم معالجة أو التطرق من خلال هذا المؤتمر إلى القضايا الالكترونية وذلك عن طريق إجراء حوار سياسي،خلص بوضع أجندة تتطلع من خلالها لزيادة العمل التعاوني بين الدول من أجل ضمان تحقيق الأمن الالكتروني.

بالإضافة إلى هذا هناك مؤتمر آخر عقد في برلين بعنوان "تحديات الأمن الالكتروني" جمع بين ممثلين من القطاع الخاص والمجتمع المدني إضافة إلى الحكوميين والأكاديمين في محاولة منهم للوصول إلى طرق تعاونية لمجابهة التحديات الأمنية السيبرانية، ومن بين الأهداف أيضا تطوير آليات إدارة الأزمات في المجال السيبراني، كذلك الشفافية في وضع وتنفيذ الاستراتجيات الدفاعية[1]. إلى جانب المؤتمر العالمي الرابع للفضاء الالكتروني المنعقد في مدينة لاهاي هولندا في 16_17 أفريل 2015.[2]

هذا وقد أقيمت عديد المؤتمرات في منطقة الخليج العربي (مجلس التعاون) ومن أهم المؤتمرات نجد:

1_**مؤتمر أبو ظبي العالمي للأمن السيبراني 25 مارس 2014:** عقد هذا المؤتمر بمشاركة وتمويل معهد نيويورك للتكنولوجيا والكلية العالمية للتكنولوجيا أبو ظبي ومن خلاله تم التطرق لمناقشة التهديدات الاقتصادية والاجتماعية والأمنية للجريمة الالكترونية وكذلك وسائل الحماية واستعراض التجارب والخبرات المكتسبة في مجال مكافحة الجريمة السيبرانية[3]

2_**مؤتمر الأمن السيبراني مسقط من 22 إلى 24 مارس 2014:** تم عقد هذا المؤتمر في سلطنة عمان وذلك من أجل مناقشة أهمية الأمن السيبراني في المنطقة ويرجع ذلك إلى الاستخدام المتزايد للوسائل التكنولوجية،وبالتالي صار الأمر ضروريا لمواجهة الجرائم السيبرانية في المنطقة،كما انبثق عن هذا المؤتمر لجان على مستوى خبراء الأمن الالكتروني من الجهات الحكومية كوزارة الدفاع ...بالإضافة إلى

[1] نوران شفيق،مرجع سابق.ص،110.

[2] ليلى الجنابي،نفس المرجع.

[3] المرجع نفسه.

شركات صناعية نفطية وهذا من أجل تحديد التحديات الأمنية على الانترنيت وكيفية مجابهتها مع إيجاد حلول أيضا[1].

المطلب الثاني: الجهود الوطنية لمواجهة التهديدات السيبرانية

فيما يتعلق بالجهود الوطنية نجد أنه بالرغم من تكتل الدول والمنظمات الدولية الحكومية وغير الحكومية في إطار دولي وإقليمي لوضع استراتيجيات بخصوص الأمن السيبراني أو التهديدات التي تنجم عنه، لم يمنع هذا الدول فرادى أن تضع هي الأخرى استراتيجيات تخص أمنها القومي، فعلى سبيل الذكر نجد الولايات المتحدة الأمريكية بالرغم من أنها تعد قوة كبرى إضافة إلى تحكمها في المجال التكنولوجي إلا أنها قامت بوضع استراتيجيات لمجابهة الأخطار التي تنجم عن الهجمات السيبرانية خصوصا وأننا في عصر الحروب الذكية والتي تعتمد بالدرجة الأولى على الأسلحة الالكترونية لمواجهة العدو دون قدرته على تحديد مصدر الهجوم أو حتى اكتشافه في بعض الأحيان إلا بعد فوات الأوان.

ومنه نجد الولايات المتحدة الأمريكية تضع الأمن الالكتروني على قمة أولويات الأمن القومي الأمريكي، حيث يرى المسؤولون في الولايات المتحدة الأمريكية أن هذه التهديدات السيبرانية يمكن أن تتجاوز ظاهرة الإرهاب خلال السنوات القادمة، كما أن أغلب التقارير والدراسات التي تعنى أو تهتم بمناقشة قضايا التهديدات الالكترونية والتي تتوقع حدوث حرب سيبرانية في العقود القادمة هي دراسات أمريكية كما أن بعضها صادر عن المؤسسات الرسمية.

ومن أهم الإدارات التي تعنى بالأمن الالكتروني على المستوى الفدرالي نجد وزارات الداخلية والدفاع، كذلك مكتب الأمن الإلكتروني والاتصالات كذلك مركز حماية البنى التحتية الوطنية،بالإضافة إلى قطاع جرائم الحاسب الآلي[2]، كما قامت وزارة الدفاع بإنشاء قيادة فرعية تحت اسم "وحدة القيادة الالكترونية" وتعمل هذه الوحدة للقيادة الالكترونية على تحقيق خمسة أهداف أساسية أولها اعتبار مجال الفضاء السيبراني مجال عملياتي مثله مثل الجيش والمجالات الجوية،البرية والبحرية أيضا استخدام مفاهيم جديدة لمصطلح الأمن وهذا يشمل كافة الأبعاد ومن بينها البعد الالكتروني ومن بين الأهداف أيضا بناء علاقات مع شركاء دوليين، كذلك التعاون مع القطاع الخاص. كما تهدف أيضا وحدة القيادة إلى اكتساب

[1]. نفس المرجع .

[2] نوران شفيق ،مرجع سابق.ص ص، 71 73.

الخبرة والمهارات اللازمة والتي تمكن الجيش الأمريكي من تحقيق انتصارات في هذا المجال[1]، ومن بين الاستراتيجيات أيضا التي تضعها الولايات المتحدة المريكية لضمان فضاء سيبراني آمن خال من الافتراءات والجوسسة.

وعلى غرار كل هذا نجد أن الولايات المتحدة الأمريكية قد بادرت باستراتيجيات لنشر قدرات الدفاع السيبرانية الحالية للدفاع بشكل استباقي عن الوكالات الحكومية المدنية،والبنية التحتية الحيوية.كذلك التفكير في إنشاء خدمة الأمن السيبراني الإتحادي للانخراط في الوقت المناسب في العمليات الدفاعية، إعطاء أولوية أكبر للوكالات الاستخباراتية الأمريكية وذلك من أجل جمع المعطيات الاستخباراتية التكتيكية على الانترنيت لمجابهة أي تهديد على الحكومة ومختلف البنى التحية الحيوية للدولة ،كما قامت أيضا بإنشاء إطار دائم للشراكة بين القطاعين العام والخاص، وهي الأخرى سعت أيضا إلى دمج الحماية ضد مشاركة الدولة في سرقة الانترنيت في الاتفاقيات متعددة الأطراف[2].

هذا فيما يتعلق بالاستراتيجية الأمريكية أما فيما يتعلق بالاستراتيجية الروسية فهذه الأخيرة إستراتيجيتها الأمنية المتعلقة بالأمن السيبراني تختلف عن الاستراتيجية الأمنية الأمريكية فهي تؤمن بضرورة تحقيق السيادة الوطنية في مجال الانترنيت Internet Sovereignty كما تعتمد روسيا في استراتيجيتها على استخدام الوسائل الالكترونية الهجومية.فهي تعمل على تعطيل البنية التحتية المعلوماتية للخصم، وكذلك الاتصالات المدنية والعسكرية له قبل الخوض في العمليات العسكرية التقليدية[3].

بالإضافة إلى الولايات المتحدة وروسيا وضعت بريطانيا هي الأخرى استراتيجية جديدة للأمن السيبراني تقوم على ثلاثة أركان تتمثل في الدفاع،الردع والتطور، فالبنسبة للدفاع تهدف بريطانيا إلى تعزيز الأنظمة البريطانية الخاصة بحماية الشبكات والمستخدمين في بريطانيا، كذلك زيادة نطاق وتطوير مقرات الاتصالات الحكومية بوزارة الدفاع والوكالة الوطنية للجرائم وهذا لمنع الهجمات السيبرانية على الدولة.أما بخصوص الركن الثاني للإستراتيجية ألا وهو الردع هدفت من خلاله إلى زيادة قدراتها من أجل

[1]. نفس المرجع.ص 84

[2] باسم علي خريسان،الاستراتيجية الأمريكية للفضاء السيبراني تعزيز الحرية الأمن والإزدهار2017/10/20/بتاريخ2020/08/20في: http:/mcsr.net/news331.

[3] نوران شفيق،مرجع سابق.ص ص.70 71.

مواجهة هذه التهديدات كما صعبت عملية إفتراق الدولة كذلك سعت أيضا إلى تأسيس أنظمة متخصصة بالجرائم السيبرانية[1].

جدول رقم(3): يوضح الدول العشر الأكثر قدرة على مواجهة التهديدات السيبرانية

الدولة	التدابير القانونية	التدابير الفنية	التدابير التنظيمية	بناء القدرات	التعاون	عوامل النجاح الرئيسية
سنغافورة	0.95	0.96	0.88	0.97	0.87	0.92
الولايات المتحدة الأمريكية	1	0.96	0.92	1	0.73	0.91
ماليزيا	0.87	0.96	0.77	1	0.87	0.89
سلطنة عمان	0.98	0.82	0.85	0.95	0.75	0.87
استونيا	0.99	0.82	0.85	0.94	0.64	0.84
موريشيوس	0.85	0.96	0.74	0.91	0.70	0.82
استراليا	0.94	0.96	0.86	0.94	0.44	0.82
جورجيا	0.91	0.77	0.82	0.90	0.70	0.81
فرنسا	0.94	0.96	0.60	1	0.61	0.81
كندا	0.94	0.93	0.71	0.82	0.70	0.81

المصدر: _____،الجريمة الالكترونية في المجتمع الخليجي وكيفية مواجهتها 2016 (سلطنة عمان:مجمع البحوث والدراسات ،أكاديمية السلطان قابوس لعلوم الشرطة).ص33.

نلاحظ من خلال هذا الجدول مستوى الوعي للأمن السيبراني الذي يشمل مجال واسع للتطبيق يشمل العديد من القطاعات وإختبار أفضل الدول استعدادا لمواجهة الهجمات الالكترونية هو استخدام مؤشر الأمن السيبراني الذي قام على ركائز أساسية وهي التدابير القانونية والفنية والتنظيمية بالإضافة إلى بناء القدرات والتعاون وهي التي تمثل عوامل النجاح لمواجهة التهديدات السيبرانية.

[1] المراجعة الدفاعية والأمنية الاستراتيجية لعام 2015/بريطانيا تعتمد استراتيجية أمن سيبراني جديدة 2016/12/10 بتاريخ 2020/08/30في: https:/sdarabia.com/2016:

المبحث الثالث: مستقبل الأمن السيبراني في ظل بيئة دولية متغيرة

قدم المركز العربي للبحوث القانونية والقضائية جملة من التوصيات التي كانت تعبيرا عن مخرجات المؤتمر الرابع للمتخصصين في أمن وسلامة الفضاء السيبراني الذي انعقد في بيروت بين 17– و19 أوت 2015 نجد منها:

- متابعة دراسة مشروعي الإتفاقية العربية لحماية أمن وسلامة الفضاء السيبراني في التشريع التنظيمي النموذجي للأمن السيبراني بعد مراجعة ذلك من المؤتمر على ضوء الملاحظات الواردة من الدول العربية الأعضاء.
- الأخذ بعين الإعتبار الملاحظات والتعديلات المقترحة على مشروع الإتفاقية.
- يرجى من الدول العربية إبداء ملاحظاتها بشكل دقيق يتناول المواد الواردة في الإتفاقية والنص المقترح تعديله أو إلغائه.
- استكمال اجتماعات المؤتمر الرابع في موعد يحدد في ضوء استكمال الردود على أن يعقد قبل منتصف أكتوبر.
- التمني على الدول العربية تزويد المركز العربي للبحوث القانونية والقضائية بالقوانين أو مشاريع القوانين الخاصة بحماية وسلامة الفضاء السيبراني.
- التمني على الدول العربية استكمال دراسة مسودة مشروع القواعد والضوابط الأخلاقية لاستخدام الفضاء السيبراني.
- الحث على إيجاد آلية لتفعيل التعاون العربي وتبادل الخبرات والزيارات في مجال حماية أمن وسلامة الفضاء السيبراني ووضع خطط لتفعيل التدريب.

ونذكر بعض التوصيات المتبناة للسلامة والأمن في الفضاء السيبراني وذلك حسب منى الأشقر جبور أهمها:

- الإلتزام بالقرارات الصادرة عن الأمم المتحدة وعن القمة العالمية لمجتمع المعلومات والداعية إلى نشر ثقافة الفضاء السيبراني.
- إتخاذ تدابير تعتمد الأمن كعنصر ضروري في الإنتاج لاسيما مايخص البرامج والأجهزة المستخدمة في تقنيات الاتصال.
- وضع إطار تعاون يضمن تبادل المعلومات،ونقل الممارسات الفضلى في المجال الأمني.

- تأمين انسجام الأنظمة القانونية لمكافحة الجرائم السيبرانية بما يمنع قيام جنات رقمية.
- وضع استراتيجية لنشر الوعي وبنائه لدى مختلف شرائح المجتمع، سواء منهم المستخدمون العاديون أو المهنيون أو متخذو القرار والمسؤولون عن سياسات الأمن والسلامة.
- اعتماد مبادئ خلقية للسلوك السيبراني مثال على ذلك خلفيات وأصول التعامل القائمة في المجتمع التقليدي تكون بمثابة عقد اجتماعي يؤسس لسلوك يضمن سلامة الجماعة وسلامة مواردها.
- وضع استراتيجية سياسية أمنية واضحة وملزمة لكل المعنيين بصناعة المعلومات، وبإدارة وسائل الإتصالات والبنى التحتية كما لأولئك المعنيين بصناعة أدوات وبرامج الإتصال وتخزين المعلومات ومعالجتها، وتحويل الأمن السيبراني إلى جزء من خطط التنمية والتطوير كافة.
- أخذ جميع أبعاد الأمن السيبراني بعين الإعتبار لدى وضع أي خطة استراتيجية أو سياسية بما في ذلك حاجات المواطنين والمؤسسات من حقوق وواجبات بحيث تأتي الخطة متكاملة ومنسجمة مع ما يمكن توقع الإلتزام به من قبل المعنيين بأمن مجتمع المعلومات.
- الإقرار بالمسؤولية عن تحقيق الأمن السيبراني كجزء لا يتجزأ من الأمن القومي والوطني.
- إنشاء مراكز للسلامة المعلوماتية ولطوارئ الإتصالات لتعاون فيما بينها وفق آلية واضحة وشفافة وفاعلة.
- تدريب وتأهيل وحدات عسكرية وأمنية خاصة يمكنها مراقبة البنى التحتية للإتصالات بحيث تقوم بتحديد المخاطر المحتملة وإزالتها.
- تأهيل وحدات أمنية وعسكرية خاصة تتولى التعاون على المستوى الخارجي مع الهيئات العاملة على مكافحة المخاطر والحد منها ومن آثارها.
- تأهيل الأجهزة القضائية المختصة والشرطة القضائية بحيث تتمكن من القيام بواجبها في مجال ملاحقة ومحاكمة المجرمين السيبرانين.
- توجيه دعوة من خلال جامعة الدول العربية إلى دول العالم لمناقشة إقرار معاهدة دولية تنطلق ديباجتها من مقررات القمة العالمية لمجتمع المعلومات إضافة إلى الإقرار بضرورة عدم تحويل الفضاء السيبراني إلى مجال يهدد السلم الدولي، مع الإلتزام بعدد من المبادئ وفي مقدمتها مبدأ سيادة الدول والمساواة فيما بينها، حق كل دولة من الإستفادة من قدرات تقنيات المعلومات والإتصالات بما يضمن قدرتها على المنافسة في هذا المجال وتحقيق رفاه شعوبها.

- إنشاء هيئات تحكيم وطنية متخصصة في القضايا السيبرانية وخدمات واستشارات مسبقة ولاحقة لأي نشاط إلكتروني يمكن لمن يرغب اللجوء إليه[1].

أما فيما يتعلق بالجهود الوطنية لمواجهة التهديدات السيبرانية نجد أنه

- على الدولة بناء الجيوش السيبرانية.

- تشكيل هيئات وطنية للأمن السيبراني مهمتها تكمن في: إعداد الإستراتيجية الوطنية للأمن السيبراني والإشراف على تنفيذها كذلك وضع السياسات وآليات الحكومة والإرشادات المتعلقة بالأمن السيبراني وتعميمه، وضع أطر الإدارة المتعلقة بالأمن السيبرالني، وضع أطر الاستجابة للحوادث والاختراقات ووضع السياسات والمعايير الوطنية للتشفير ورفع مستوى الوعي بالأمن السيبراني.

- التشريعات الوطنية للأمن السيبراني .

كذلك من بين الجهود الدولية نجد الحد من سباق التسلح السيبراني حيث تتبنى الدول استراتيجية الحرب السيبرانية كحرب للمستقبل واعتبار أن النصر في المعركة حليف من يقدر على شل القوة والتشويش على المعلومة[2]، ولقد بدأ السباق نحو التسلح السيبراني مع الصراع الروسي الإستوني واتجهت الدول لتعزيز قدراتها السيبرانية سواء دفاعيا أو هجوميا، والمشكلة في السباق نحو التسلح تكمن في تحديد ماهية تلك الأسلحة. ونجد من بين هذه الجهود الإتفاقيات الإقليمية والدولية للأمن السيبراني.

ومنه ومن خلال هذه التوصيات انبثقت عنها مجموعة من الحلول التي يمكن أن تحد من الجرائم والحروب السيبرانية كما أنه هناك بعض الحلول فيما يخص الإرهاب وجرائمه وذلك من خلال مجموعة من الخطوات أهمها:

1- رصد أنشطة الجماعات الإرهابية على الشبكات الاجتماعية وتحليل محتواها وأهدافها والاستراتيجيات المعتمدة.

2- رصد نشاط المتعاطفين مع الجماعات الإرهابية وتحليل خطاب العنف والكراهية والتحريض على الإرهاب.

[1] منى الأشقر جبور، **السيبرانية هاجس العصر**،مرجع سابق.165-166.

[2] عادل عبد الصادق، **أسلحة الفضاء الإلكتروني في ضوء القانون الدولي**، مرجع سابق.ص 64.

3- إشراك المجتمع المدني للتعاون عن نشر الثقافة الوقائية وتوعية المجتمع بمخاطر الإرهاب والتصدي له من خلال نبذ الكراهية والعنف ونشر ثقافة التسامح والحوار مع الآخر واحترام الديانات والحضارات.

4- سن قوانين وتشريعات لمعاقبة المجرمين والإرهاب وسبل التحقيق فيها بتنسيق وتوحيد الجهود من أجل سد منافذ الجريمة والإرهاب بإيجاد منظومة دولية قانونية تحت مظلة الأمم المتحدة يعهد إليها توثيق وتوحيد جهود الدول قدر المستطاع والعمل على ضبطها وإثباتها بالطرق القانونية والفنية.

5-التركيز على التعاون الدولي من خلال تبادل المعلومات والخبرات والاستفادة من المنظمات الدولية المختصة وذات الخبرة .

6- عقد الاتفاقيات وتعزيز التعاون الدولي من خلال مراقبة كل دولة للأعمال الإجرامية التخريبية الإلكترونية الواقعة على أراضيها ضد دول أو جهات أخرى.

7-تنظيم مؤتمرات وندوات علمية في الجامعات ومراكز البحوث في مختلف دول العالم تضم خبراء وباحثين ومختصين من مختلف التخصصات لدراسة المشكلة واقتراح الحلول الناجعة لمعالجتها[1].

8-التركيز على إجراء الدراسات والبحوث المتعلقة بالجريمة والحرب والإرهاب على حد سواء برفع التوصيات إلى الجهات المختصة لوضع التشريعات اللازمة للمواجهة[2]،ومن الضروري أن تعمل الدول على نشر ثقافة الأمن السيبراني مع ضرورة نشر وتطوير آلية المكافحة وزيادة الوعي بالأخطار لمواكبة التكنولوجيا الحديثة التي من شأنها أن تجعل الأنظمة أكثر أمنا وفاعلية وهذا بتكثيف الجهود الدولية عن طريق تنظيم دورات متخصصة لتدعيم الأمن السيبراني للدول التي بدورها لابد لها من وضع خطط لتطوير البنية التحتية لتكنولوجيا المعلومات والاتصالات، بما أن الأمن السيبراني منظومة ترتكز حول نشر الوعي بين الأفراد بضرورة التركيز على البحوث العلمية بالتعاون على المستوى المحلي والدولي وإيجاد حلول مبتكرة لحماية البنية التحتية بتعزيز حماية الشبكات والبرمجيات[3].

ومنه فالدول تحتاج إلى استعدادات كبيرة لمواجهة هذه المخاطر ما يتوجب على المنظومة الدولية تكثيف الجهود في التنسيق والتعاون خاصة الأمني بين القطاعات والحكومات،ما يلزم توعية الجمهور

[1] عبير شفيق الرحباني،مرجع سابق.ص ص.449-451.

[2] أيسر محمد عطية،ملتقى بعنوان:"**الجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية والدولية**"،الأردن:2-2014/9/4.ص 29.

[3] عبير شفيق الرحباني، نفس المرجع. ص ص.452-453.

والأفراد بهذه المخاطر بإيجاد وتجهيز فرق متخصصة للتحقيق مع ضرورة تزويد البلدان النامية بالموارد والتقنيات اللازمة لمعالجة هذه الأخطار ومكافحتها.

كذلك عسكرة الفضاء الالكتروني سعيا لدرء تهديداته على أمنه وبرز في هذا الإطار اتجاهات مثل التطور في مجال سياسات الدفاع والأمن،تصاعد القدرات في سباق التسلح السيبراني وتبني سياسات دفاعية سيبرانية لدى الأجهزة المعنية بالدفاع والأمن في الدول وتزايد الاستثمار في مجال تطوير أدوات الحرب السيبرانية داخل الجيوش الحديثة ،وذلك بالسعي إلى امتلاك التكنولوجيا وأنظمة الحماية وتطوير قدرات هجومية تعمل على تحقيق التفوق التقني،وتطوير القدرات الهجومية إما عن طريق بناء القدرات الذاتية أو بالاستعانة بالأفراد وتطوير القدرة على اختبار مدى الجاهزية لمواجهة هذه الهجمات ،والعمل على توفير الميزانيات المتخصصة لتطوير القدرات الهجومية والدفاعية خاصة وأنها أقل تكلفة مقارنة بالجيوش التقليدية.

ومنه وختاما لهذا الفصل نستنتج بأن الأمن السيبراني عبر العديد من الدول والمراحل الزمنية التي مرت بها والاستراتيجيات المتبعة لدى العديد من الدول وأبرزها الدول الكبرى أوالعظمى قد مارست سياسات جد هامة للحفاظ على البنى التحتية خاصة للدولة سواء كان متعلق بالدولة بصفة عامة أو المجتمع المدني والشركات بصفة خاصة وبالأخص وأننا قد تناولنا في هذا الفصل نماذج تماثلية دولة مقابل دولة، ودولة مقابل شركة والعديد من الجهود الدولية والوطنية بالإضافة إلى العديد من التوصيات المقترحة والناتجة عن المؤتمرات الدولية والوطنية والإقليمية في ظل بيئة سياسية متغيرة بفعل التطورات الحاصلة في الساحة السياسية الدولية.

خاتمة

لقد ساهمت الثورة التكنولوجية والمعلوماتية في إحداث نقلة نوعية على كافة الأصعدة،كما كان لها دور في تطوير مختلف العلوم والحقول المعرفية،ومن بين هذه الحقول نجد حقل العلوم السياسية عامة وحقل العلاقات الولية على وجه الخصوص والذي طرأ عليه سواء من حيث المفاهيم والأسلوب التي مست هذه المواضيع والمفاهيم التي أصبحت تهتم بكل ما هو إلكتروني هذا ما دفع بباحثي العلاقات الدولية في تطوير الجانب الميثودولوجي والإطار المفاهيمي ومن أبرز المفاهيم التي تعد ركيزة أساسية في هذا الحقل ،ألا وهو الأمن والذي تحول مع ظهور فضاء جديد جراء الثورة التكنولوجية .

فالفضاء السيبراني أصبح هذا المفهوم يعالج مواضيع ذات بعد إلكتروني سيبراني غير الأبعاد التقليدية،كما تغيرت أيضا أساليب تحقيق هذا المطلب الأساسي للأمن والذي أصبح مهدد أكثر مما كان عليه سابقا هذا بسب التهديدات الجديدة في الفضاء السيبراني كما أيضا تغيرت تغيرت أساليب الحروب بين الدول لتصبح هي الأخرى تعتمد على الوسيلة الاتصالية وتنتقل إلى الفضاء الرابع السيبراني بعدما كانت تقوم على الوسيلة العسكرية ونجد أن مفهوم القوة ايضا تغير من مفهوم القوة الصلبة إلى القوة الذكية هذا ماجعل من الدول تفكر في إعادة وضع إستراتيجيات جديدة في المجال الأمني،خاصة وأن أنواع القوة السيبرانية لم تعد وسيلة خاصة بالدول فقط،بل أصبحت متاحة لكل الفواعل وحتى الأفراد باتوا يشكلون تهديدا على الأمن القومي للدول.

هذا ماحال في مقابل هذا كله أن تزداد المخاطر التكنولوجية أو بالأحرى التكنولوجية كلما زادت هيمنة تكنولوجيا المعلومات والاتصالات على النسق العام للحياة فأصبحنا أمام جرائم حقيقية بجميع مقوماتها تتم عن طريق الشبكة المعلوماتية فهذه التهديدات التي تنوعت أشكالها وخطورتها،بدأت هذه الجرائم السيبرانية بأفراد ومنظمات إجرامية من تجسس وسرقة الأموال إلى تخويف وإبتزاز لتصل إلى الصراع بين الدول وهذا ما دفع إلى عدم تحقيق الأمن السيبراني المثالي في الفضاء السيبراني والهدف هو تقليل التهديدات للإستمرار نحو التقدم لأن هذه التكنولوجيا المعلوماتية التي وفرت كل شيء يريده المجتمع هي نفسها التكنولوجيا التي تريد أن تنتزع كل شيء فهذه التهديدات التي تمس الأمن السيبراني من جريمة وإرهاب وصولا إلى الحرب السيبرانية الموجودة في عالم اليوم الذي من الضروري مواجهتها استعدادا لتهديد الغد الذي قد يكون أقوى بتطوير الاستراتيجيات للمواجهة من أجل فضاء سيبراني يعزز أمن سيبراني مليء بالتقدم والإزدهار للجميع في المجتمع المعلوماتي .

وقد برزت هذه الصراعات السيبرانية بين دولة ودولة وهي تهديدات تماثلية،ولم تتوقف عند هذا الحد بل توسعت وشملت صراعات غير تماثلية بين دولة وشركة أو حتى بين الأفراد ،وفي ظل هذه التغيرات والظروف سعت الدول إلى وضع جهود واستراتيجيات في هذا العالم المتغير في جميع الميادين وخاصة الأمنية السيبرانية ما دفع للبحث عن حلول وتوصيات ونخلص في الأخير إلى مجموعة من التوصيات أهمها:

_أهمية خلق إطار مؤسساتي للأمن السيبراني وخلق جيوش سيبرانية.

_تعليم وتوعية الأفراد بنشر ثقافة سيبرانية.

_أدراك أن الأمن السيبراني عنصر رئيسي في الأمن القومي وله علاقة وطيدة مع التنمية بجميع أشكالها.

_أخذ التجارب السابقة في الميدان السيبراني كعبرة في المستقبل بفعل التطور التكنولوجي الحاصل.

الكلمات المفتاحية:

-السياسة الدولية:

قائمة المراجع

أولا: المراجع باللغة العربية:

أ- القرآن الكريم:

1-سورة الأنعام.

2- سورة الأنفال.

3-سورة النور.

4-سورة قريش.

ب-القواميس:

5-ابن منظور،لسان العرب،تحقيق عبد الله الكبير(القاهرة:دار المعارف،د س ن).

ج- الكتب بالغة العربية:

6- أبو الروس، أحمد، **الإرهاب: التطرف والعنف،** (الإسكندرية: دار المكتب الجامعي الحديث، 2011).

7- الأشقر جبور، منى،"**السيبرانية هاجس العصر**،"جامعة الدول العربية :المركز العربي للبحوث القانونية والقضائية.

8- بدران، عباس، **الحروب الالكترونية.الاشتباك في عالم متغير**، (بيروت: مركز دراسات الحكومة الالكترونية، 2010).

9- بلهول ،نسيم ، **فهم الأمن القومي الجزائري من مدخلي الأمن الوطني والدفاع الوطني** (عمان: دار حامد للنشر والتوزيع، 2015).

10- بيليس، جون ، ستيف سميث، **عولمة السياسة العالمية**، (دبي: مركز الخليج للأبحاث، ط1، 2004.

11- وقاف ،العياشي ، **مكافحة الإرهاب بين السياسة والقانون**، (الجزائر: دار الخلدونية للنشر والتوزيع،2006).

12- حريز،عبد الناصر ،"**الارهاب السيبراني دراسة تحليلية** "،(القاهرة:مكتبة مدبولي، ط1،1996).

13- حتى، ناصيف يوسف. **النظرية في العلاقات الدولية**. بيروت: دار الكتاب العربي، ط.1، 1985.

14- كامل، ثامر، **دراسة في الأمن الخارجي العراقي واستراتيجية تحقيقه، (العراق: وزارة الثقافة والإعلام، 1985)**.

15- محي الدين ،محمد مؤنس ، **تحديث أجهزة مكافحة الإرهاب وتطوير أساليبه** (عمان: دار الحامة للنشروالتوزيع ،2014).

16- محمد عطية ،أيسر، **دور الآليات الحديثة للحد من الجرائم المستحدثة: الإرهاب الالكتروني وطرق مواجهته،** (الأردن: كلية العلوم الاستراتيجية،2014/09/04).

17- منصور، شادي عبد الوهاب ، **حروب الجيل الخامس أساليب "التفجير من الداخل" على الساحة الدولية** (الإمارات: مركز التفكير 2014).

18- مراد،عبد الفتاح ،**شرح جرائم الكمبيوتر والانترنيت،** (مصر: دار الكتب والوثائق المصرية، د ط، د س ن).

19- محمد فرج،أنور ،**النظرية الواقعية في العلاقات الدولية،**(كردستان: مركز كردستان للدراسات الاستراتيجية ،2007).

20- عبد الصادق، عادل، **الارهاب الالكتروني (القوة في العلاقات نمط جديد وتحديات مختلفة)**، (القاهرة: مركز الأهرام للدراسات السياسية والإستراتيجية،2009)

21- ربحي،عليان، **مجتمع المعلومات والواقع العربي،** (عمان: دار جرير للنشر والتوزيع ، ط1، 2006).

22- الرحباني، عبير شفيق ، **الجرائم الإلكترونية ومخاطرها،** (عمان: دار الثقافة للنشر والتوزيع، ط1، 2020).

23- رشاد القصبي،عبد الغفار، **مناهج البحث في علم السياسة،** (القاهرة: مكتبة الآداب، ط1، 2004).

24- نوران شفيق، **السياسة الدولية والإستراتيجية أثر التهديدات الالكترونية على العلاقات الدولية،** (القاهرة: المكتب العربي للمعارف، ط1 2016)، ص.46.

25- خالد ،ابراهيم ، **أمن المعلومات الالكترونية،** (الاسكندرية: دار الجامعية للنشر، 2008).

26__،الجريمة الالكترونية في المجتمع الخليجي وكيفية مواجهتها2016(سلطنة عمان:مجمع البحوث والدراسات أكاديمية السلطان قابوس لعلوم الشرطة).

ب- المجلات والدوريات:

27-الأشقر جبور، منى، "**الأمن السيبراني التحديات ومستلزمات المواجهة**"، جامعة الدول العربية، المركز العربي للبحوث القانونية والقضائية، اللقاء السنوي الأول للمتخصصين في أمن و سلامة الفضاء السيبراني، بيروت 27_28، أغسطس 2012

28- بارة، سمير،"الأمن السيبراني في الجزائر السياسات والمؤسسات"، **المجلة الجزائرية للأمن الإنساني**، (العدد الرابع)، (جويلية 2017)، ورقلة: جامعة قاصدي مرباح

29_ين مرزوق ،عنتر، **الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية**،;ورقة بحثية قدمت في ملتقى (المسيلة: جامعة محمد بوضياف، كلية الحقوق والعلوم السياسية)

30- بن عنتر، عبد النور،"تطور مفهوم الأمن في العلاقات الدولية"، **مجلة السياسة الدولية**، (العدد 160)، (أفريل 2005)

31- جبريل ،رشاد مرعي، إسراء ،"الجرائم الإلكترونية: الأهداف، الأسباب، طرق الجريمة ومعالجتها"، **مجلة الدراسات الإعلامية**"،ع 1، جانفي 2018

32- زروقة، اسماعيل، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، **مجلة العلوم القانونية والسياسية**، (م 10)،(ع 1)، (أفريل 2019)

33-محمد عطية، أيسر، ملتقى بعنوان:"**الجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية والدولية**"،الأردن:2-2014/9/4.

34- معين حسن المشهدي،تغريد،"الأثر العسكري للأمن السيبراني في الجغرافيا السياسة للدولة"،**مجلة البحوث الجغرافية**،(ع30)،جامعة الكوفة :كلية الآداب ،قسم الجغرافيا.

35- مختار، محمد ،"هل يمكن أن تتجنب الدول مخاطر الهجمات الإلكترونية"، **مجلة اتجاهات الأحداث**، (العدد 6)، (يناير 2015)

36- المصري، خالد موسى. "النظرية البنائية في العلاقات الدولية"، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، م.30، ع.2. 2014.

37- النعيمي، أحمد نوري. "البنيوية العصرية في العلاقات الدولية"، مجلة العلوم السياسية، ع.46. 2013.

38- سيد أحمد، رفعت ،الأمن القومي العربي بعد حرب لبنان: دراسة في تطور المفهوم، **مجلة شؤون عربية**، (العدد 35)، (تونس،1984) ...

39- عوني، ملك،"رهان الثورات...تصاعد الأمن غير التقليدي في المنطقة العربية"، **مجلة السياسة الدولية**، مركز الأهرام للدراسات السياسية و الاستراتيجية، القاهرة، (العدد 186)، (أكتوبر 2011).

40- عبد الفتاح، فاطمة الزهراء، تطور توظيف جماعات العنف والارهاب السيبراني، **مجلة السياسة الدولية**، (العدد 208)، أفريل 2008.

41- عبد الصادق ،عادل ،**أسلحة الفضاء الالكتروني في ضوء القانون الدولي**،سلسلة أوراق(العدد23)،2016

42- عبد الصبور ،سماح ، "الصراع السيبراني طبيعة المفهوم وملامح الفاعلين"، **مجلة السياسة الدولية:** اتجاهات نظرية في تحليل السياسة الدولية، (م 52)، (ع 208)، (أفريل 2017).

43- عبد الرحمان رشاد، ريهام،الارهاب الالكتروني على تغير مفهوم القوة في العلاقات الدولية، دراسة حالة تنظيم الدولة" **المركز العربي الديمقراطي للدراسات الاستراتيجية والسياسية**"،(عدد375)،(2016/07/24)

44- رضوان، ج،الأمن السيبراني: أولوية في استراتجيات الدفاع، **مجلة الجيش**، الصادرة عن مؤسسة المنشورات العسكرية، (العدد 630)، (جانفي 2016).[1] ـــــــ،**استعمال الانترنيت في تمويل الارهاب وتجنيد الإرهابين**، 44-مركز الدراسات والبحوث، (السعودية: جامعة نايف العربية للعلوم الأمنية ،11 ماي 2011)

45- مركز نورس للدراسات:**الحرب السيبرانية (الالكترونية)نقلة نوعية في الاستراتيجيات العسكرية و آثر ملحوظ على العلاقات الدولية** ،مركز نورس 2019.

46- جريدة عالم اليوم،**صفحة عالم الكمبيوتر**، 1 نوفمبر 2005 .

ت- مذكرات وأطروحات التخرج:

47- بدوي بريوش ،نضال ناجي، "**الصراع السيبراني مع العدو الصهيوني**"، بحث مقدم لاستكمال متطلبات الحصول على دبلوم الدراسات الفلسطينية، (أكاديمية دراسة اللاجئين الفلسطينين: قسم الأبحاث والمشاريع، دبلوم الدراسات الفلسطينية، 2019/2018).

48- بشير،ساسي محمد ، "**الأمن في القصص القرآني**"، بحث لاستكمال متطلبات الحصول على الماجيستر في التفسير، (الجامعة الاسلامية غزة: كلية أصول الدين، قسم التفسير 2012).

دير، أمينة ،"**أثر التهديدات البيئية على واقع الأمن الإنساني في إفريقيا دراسة حالة-دول القرن الإفريقي**،"مذكرة مقذمة لنيل شهادة الماجيستر(بسكرة:جامعة محمد خيضر،كلية الحقوق والعلوم السياسية،2013/**2014**).

49- واري ،عبد الكريم، "**الحلف اللأطلسي وإجراءات بناء الثقة في الفضاء المتوسطي**"، مذكرة مقدمة لنيل شهادة الماجيستر في العلوم السياسية والعلاقات الدولية (جامعة: مولود معمري تيزي وزو، كلية الحقوق والعلوم السياسية، 2014/2013).

50- عبد الكريم أبو مور ،إنعام ،" **مفهوم الأمن الإنساني في حقل نظريات العلاقات الدولية**"، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير في العلوم السياسية، (غزة: جامعة الأزهر، كلية الاقتصاد والعلوم الإدارية، قسم العلوم السياسية، 2013).

51- عديلة،محمد الطاهر، " **تطور الحقل النظري للعلاقات الدولية: دراسة في المنطلقات والأسس**"، أطروحة مقدمة لنيل شهادة دكتوراه العلوم السياسية والعلاقات الدولية، فرع العلاقات الدولية، (باتنة: جامعة الحاج لخضر، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية، 2014-2015)

52- خذيري، عفاف،" **الحماية الجنائية للمعطيات الرقمية**"، أطروحة مقدمة لنيل شهادة الدكتوراه ،(جامعة تبسة: كلية الحقوق والعلوم السياسية،2019/2018)

53- ـــــــ،**استعمال الانترنيت في تمويل الارهاب وتجنيد الإرهابين**، مركز الدراسات والبحوث، (السعودية: جامعة نايف العربية للعلوم الأمنية ،11 ماي 2011).

ث- المواقع الإلكترونية:

54- أيمن ،ياسمين ،هل تشتعل الحرب بين أمريكا وإيران بعد مقتل سليماني في http://al-ain-com/article-iran)

55- الجنابي، ليلى،"فعالية القوانين الدولية في مكافحة الجرائم السيبرانية"في:
http://www.ssrcaw.org.art.asp?aid=571423&ac=2(15/07/2020)

56-الجنابي، ليلى، "فعالية القوانين الوطنية والدولية في مكافحة الجرائم السيبرانية "مركز الدراسات والأبحاث العلمانية في العالم العربي: في
http://www.ssvcaw.org/ar/art/show-art.asp?aid=571423

57- هارولد وارين ،سكوت ،مارتن سي ليبيكي، استريد ستوت سيفالوس،"التوصل إلى إتفاق مع الصين بشأن الفضاء الالكتروني،www.rand.org/t/rr1335"2016

58- وولت، ستيفن ، "**العلاقات الدولية: عالم واحد نظريات متعددة**"، ترجمة: عادل زقار، زيدان زياني، في:
http://www.geocities.com/adelzeggagh/IR

59-- لوديرميلك ،ميكا -الأزمة الإيرانية تنتقل إلى الفضاء السيبراني،حقوق الطبع والنشر 2018من قبل معهد واشنطن http://www.washingtoninstitute.org/ar/policy-analysis/view/iran-crisis-moves-into-cyberspace.

60-ملحم، جهاد ، السوبرنية ضد قوانين الفزياء! عن الموقع:
http://wehda: alwehda . gov.sy / node /393079 :/ .2020/03/30)

61- العتوم ،نبيل ،هجوم إلكتروني على إيران والرد قادم ضد المحور الخليجي :مركز أمية للبحوث والدراسات الاستراتيجية في: http://www.umayya.org/articles/umayya-articles/14092

62- خريسان، باسم علي ،الاستراتيجية الأمريكية للفضاء السيبراني تعزيز الحرية الأمن والإزدهار2017/10/20في: http:/mcsr.net/news331

63- المجال الخامس. الحروب الالكترونية في القرن ال21، مركز الجزيرة للدراسات، على الموقع:
http://studies.aljazeera.net/ar/issues/2010/20117212274346868.html

64- المراجعة الدفاعية والأمنية الاستراتيجية لعام 2015/بريطانيا تعتمد استراتيجية أمن سيبراني جديدة 2016/12/10 في https:/sdarabia.com/2016

65- ـ، الموسوعة السياسية، الأمن السيبراني:https://political-encyclopedia.org/dictionary

66- تهديدات مجهولة المصدر نحو مساءلة دولية في الفضاء الالكتروني John S Davis//ct Benjamin Bourdeaux ex.www.rang.org/t/r 2081.2017

67- ضربات أمريكية سيبرانية موجعة لإيران في:
http://makkah news paper.com/article/1502614

ثانيا: المراجع باللغة الأجنبية:

A- Les Dictionnaires:

68- larousse , Super major. (Paris,cedex, Larousse,1989).

69- Oxford Advanced learner's Dictionary of current English ,(Oxford univ, press , 2008).

B- Les Livres:

70−A Clarke, Richard & Robert Knake, **Cyber War: The Next Threat to National Security and What Do About It ,** Harper Collins,2010.

71- A Kemmerer**,** Richard **,Cyber Security**, University Of California Santa Barbara, Department Of Computer Science 2003.
72- Amoroso, Edward, **cyber security**, silicon press ,2007.

73- Arnold, Wolfers, (1952),**National Security as an Ambiguous Symbol** , Dans Wolfers (Arnold) (Discord And Collaboration Baltimore ,Johns Hopkins University Press,1962**.**

74- Baylis ,John and Steve Smith, "**Globalization of world politics**", second edition, new York: Oxford University Press, 2001.
75- Fred Schreier **, On Cyber warfare**, DCAF Horizon 2015 Working Paper Series , Issue 7.
76- Joseph .S.Ney ,jr**,cyber power**, harvard kennedy school, 2010.
77- Paul, Cornish , **Cyberspace and the National Security of the United Kingdom** :Threats and Responses.
78- Paul, Viotti , Mark Kauppi, **International Relation Theory**, (New York: Pearson, 5.E, 2010).
79_ Martti Lehto ,and Pekka Neinaamaki, Cyber Security :Analyics ,Technology and Automation,(Department Of Mathematical Information Technology, University of Finland).2014.

C- Les Périodiques :

81- éAlix Desforges, **rimétre**? **Cyber terrorisme :** Fiche de l'iresm n°11,2011.

82-Thomas Lumetal ,China Internet Freedom and US.Policy,Congressional Reserch Service,Julay,13,2012

73- The International Telecommunication Union (**ITU**), Toolkit For Cyber Crimel Legisalation, Geneva, 2010.
76- ITU ,**Cyber Security**, Geneva: International Telecommunication Union:: (ITU),2008

فهرس الجداول والأشكال

فهرس الجداول:

فهرس الأشكال:

فهرس المحتويات

فهرس المحتويات

الملخص

الملخص:

تغيرت ملامح البيئة الدولية بسبب الثورة التكنولوجية والمعلوماتية التي عرفها المجتمع الدولي، والتي بزغت من خلالها قضايا جديدة غير القضايا السابقة التي ترتكز بالدرجة الأولى على الأساليب التقليدية (عسكرية،اقتصلدية،سياسية...) فمن خلال الثورة التكنولوجية أصبح العالم بأسره يهتم بالمجال الرقمي المعلوماتي والالكتروني خاصة ،كما بدأ الاهتمام أيضا بالفضاء السيبراني الذي أصبح يعد من أولى أولويات الأمن القومي للدول .كما أن هذا الفضاء الجديد لم يخص الفواعل الدولية فقط بل الفواعل من غير الدول كذلك كالشركات متعددة الجنسيات والمنظمات بنوعيها الحكومية وغير الحكومية.

وقد نتج عن هذا الفضاء تهديدات سيبرانية عديدة تمثلت في: الاختراقات، التهديدات السيبرانية، الجوسسة الالكترونية، التنصت على الهيئات الحكومية وغيرها من التهديدات الأخرى وهذا راجع إلى الاستخدام السيئ للانترنيت والوسائل التكنولوجية الحديثة، هذا مادفع بالدول والهيئات الحكومية للتكتل والتعاون من أجل وضع استراتيجيات جديدة وفعالة للتصدي للهجمات السيبرانية مستقبلا خاصة ونحن في عصر يعتمد على الرقمنة والوسيلة الالكترونية في شتى المجالات .

_الكلمات المفتاحية: السياسة الدولية،الأمن السيبراني، الفضاء السيبراني، التهديدات السيبرانية.

Obstract:

The features of the international environment have changed due to the technological and information revolution that the international community has known ,through which new issues have emerged .The previous non-space ,which is based primarily on traditional methods (military, economic and political…),through the technological revolution ,the whole world became interested in the digital ,informational and electronic field in particular .Also ,interest in cyberspace ,which has become one of the top national security priorities of countries ,has also begun ,this new space does not concern international actors only ,but also non-state actors ,such as companies and companies and organizations ,both governmental ,both governmental and non-governmental.

This space has resulted in many cyber threats represented in penetrations,electronic threats ,electronic espionage ,eavesdropping on

government agencies and other other threats ,and this is due to the bad use of the Internet and modern technological means ,this is what pushed states and government agencies to co-operate in order to develop new and effective strategies to address the attacks we are in an era that depends on digitization and the electronic means in various fields.

Key word: Cyber security, Cyberspace, Cyber Threats, The international politics.