المدرسة الوطنية العليا للعلوم السياسية

قسم الدراسات الإستراتيجية والعسكرية

الإرهاب السيبراني وتداعياته على الأمن الدولي

مذكّرة مكملة لنيل متطلبات شهادة الماستر في العلوم السياسية

تخصص دراسات إستراتيجية ودولية

إعداد الطالب : **تحت إشراف الدكتور:**

فوضيل زعيط **حكيم غريب**

أعضاء لجنة المناقشة

الدكتور: غريب حكيم	**مشرفا ومقررا**
الأستادة : عقة نسيمة	**رئيسة**
الأستاد: داود علي	**ممتحنا**

تاريخ المناقشة:2017/06/13

شـــكـــــر

❖ أشكر لله عز وجل الذي أعانني و وفقني لإتمام هذا المجهود.

❖ كما أتقدم بالشكر الجزيل إلى الأستاذ المشرف الدكتور غريب حكيم

❖ و أتوجه بالشكر أيضا إلى كل إطارات وموظفي مديرية الأمن العمومي على دعمهم و توجيهاتهم خلال فترة التربص بالمديرية

❖ دون أن أنسى كل الأساتذة المحترمين على كل ما قدموه من نصح وإرشاد وبذلوه من جهد من أجلنا طيلة المسار الدراسي.

❖ وفي الأخير أشكر كل من ساعدني في إنجاز هذا المذكرة سواء من قريب أو من بعيد.

الإهـــداء

أحمد و أشكر المولى جل شأنه بديع السموات و الأرض أن شق سمعي و بصري بحوله و قوته و فضله و توفيقه في إخراج هذا الجهد و العمل إلى النور.

أهدي ثمرة جهدي بشكل خاص إلى زوجتي الغالية على دعمها و صبرها علي طوال فترة الدراسة.

- إلى إخوتي وأخواتي كل بإسمه.

- إلى جميع أفراد العائلة الكريمة.

- إلى كل الأصدقاء و زملاء المشوار الدراسي.

ملخص الدراسة:

هده الدراسة هي محاولة لإبراز المخاطر التي تواجه الأمن الدولي نتيجة التوظيف السلبي للفضاء السيبراني من طرف الدول و التنظيمات الإرهابية في سعيها لتحقيق إستراتيجياتها.

حيث أن التطور التكنولوجي في جميع نواحي الحياة نتج عنه ،بروز إستعمالات متعددة برز من خلالها الإرهاب السيبراني, وشاع إستخدامه, كما زادت خطورة الجرائم الإرهابية وتعقيدها, سواء من حيث تسهيل الإتصال بين الجماعات الإرهابية وتنسيق عملياتها, أو من حيث المساعدة على إبتكار أساليب وطرق إجرامية متقدمة, وهو الأمر الذي حتَم على المجتمع الدولى السعي وراء إيجاد ميكانيزمات كفيلة بمجابهة هده الظاهرة،خاصة مع تزايد توظيفها من طرف جميع الفواعل في العلاقات الدولية تحقيقا لمصالح متباينة .

ونظرا لغياب أو تغييب تشريعات دولية للتصدي لظاهرة الإرهاب السيبراني ، و خروجها عن السيطرة وعدم كفاية وسائل الحماية المستعملة وتحول هده الظاهرة إلى حرب بالوكالة يتم توظيف الفضاء السيبراني لتحقيق ما لايمكن تحقيقه عن طريق السلاح ،كل هدا جعل المجتمع الدولي يحاول إيجاد أرضيات للإنطلاق في سن تشريعات دولية تقنن إستخدام الفضاء السيبراني وتمكن من الكشف عن الفاعلين الحقيقين بعيدا عن التراشق بالتهم والتنصل من المسؤوليات .

ورغم كثرة المساعي الدولية في هدا الشأن إلا أن غياب الإرادة السياسية الدولية حال دون إيجاد توافق دولي من شأنه أن يؤدي إلى توحيد أساليب الحماية وتقنيين إستخدام الفضاء السيبراني.

الكلمات المفتاحية :الإستراتيجية ، الإرهاب ،الفضاء السيبراني، الأمن الدولي

Abstract:

This study is an attempt to highlight the dangers facing international security as a result of the negative recruitment of cyberspace by states and terrorist organizations in their pursuit of their strategies,

The development of technology in all aspects of life has resulted in the emergence of multiple uses of cyberspace. It has become more common, and has increased the seriousness and complexity of terrorist crimes, both in terms of facilitating communication between terrorist groups and coordinating their operations, Which has forced the international community to seek to create mechanisms capable of confronting this phenomenon, especially as it is increasingly being exploited by all actors in international relations to achieve different interests.

In the absence of international legislation to address cybercrime and its out-of-control and inadequate means of protection and the diversion of the phenomenon to proxy warfare, it is the space that uses the Internet to achieve what can not be achieved. All this makes the international community trying to find the floor for international legislation codifying the use of cyberspace And was able to expose the perpetrators away from the legitimate wrangling of charges and evading responsibilities.

Despite the large number of international efforts in this regard, but the lack of international political will prevented the finding of an international consensus that would lead to the standardization of methods of protection and the use of cyberspace

.Keywords: Strategy, Terrorism, Cyberspace, International Security

خطة الدراسة

مقدّمة

الفصل الأول :الإطار المفاهيمي للدراسة : مفهوم الإرهاب السيبراني

المبحث الأول: مفهوم الإرهاب.

المبحث الثاني : مفهوم الإرهاب السيبراني.

الفصل الثاني تداعيات الإرهاب السيبراني على الأمن الدولي

المبحث الأول :مظاهر تهديد الإرهاب السيبراني للأمن الدولي.

المبحث الثاني : الإرهاب السيبراني كشكل جديد من أشكال الصراع الدولي .

المبحث الثالث:طبيعة و أنماط توظيف الفضاء السيبراني في الصراع الدولي.

الفصل الثالث:الجهود الدولية لتأمين الإستخدام السلمي للفضاء السيبراني.

المبحث الأول : جهود هيئة الأمم المتحدة

المبحث الثاني:الجهود والمبادرات الدولية لمكافحة الإرهاب السيبراني

المبحث الثالث :تحديات معالجة الإرهاب السيبراني

والإقتراحات الخاتمة

مقدمة:

في كل مرحلة من مراحل تطورات النظام الدولي، تسود منظومة فكرية مهيمنة، تشكل الأساس في تفسير واقع العلاقات الدولية، فالعصر الوسيط شهد هيمنة الكنيسة ودفاعها عن فكرة الدين، ثم جاء عصر التنوير ليشهد هيمنة العقل، بعد ذلك جاءت مرحلة القرنين التاسع عشر والعشرين، لتشهد هيمنة النزعة القومية، إلى أن وصلنا إلى الألفية الثالثة، لتهيمن عليها العلوم والتكنولوجيا التي تمتلك نسقين متوازيين، الأول يصب في التطور الرقمي لخدمة البشرية، والثاني يصب في تطور أسلحة غير مألوفة ربما تؤدي إلى دمار البشرية.

ولكون العصر الحالي هو عصر الفضاء السيبراني فقد إتجهت معظم الدول والحكومات لتبني مسعى الوصول إلى الحكومات الذكية أو مايسمى بالحكومة الإلكترونية ودلك بالنظر للإمتيازات العديدة التي تمنحها الوسائل التكنولوجية للدول في مجال التسيير الفعال ،ومن تم سارعت العديد من الدول كل حسب قدرته إلى السعي وراء توظيف هدا المعطى الجديد خدمة لمصالحها الوطنية، و كنتيجة لدلك قامت العديد من الدول ببناء مدن دكية، وتوظيف الوسائل التكنولوجية في جميع مناحي الحيات المدنية والعسكرية ، خاصة إدا علمنا أن هده الوسائل توفر إمتيازات عديدة من حيث الزمن والتكلفة .

كل هدا تزامن مع ربط العالم بشبكة الأنترنت والتي أصبحت مفتوحة أمام جميع سكان العالم بالشكل الدي سهل عملية الوصول إلى المعلومات وحيازتها ونقلها أو التلاعب بها ، ومن هنا أصبح العالم أمام أخطار جمة تهدد الأمن الدولي خاصة إدا علمنا بصعوبة معرفة الجاني في الفضاء السيبراني كون الأمر يتعلق بوسائل إلكترونية لا تحمل هوية معترف بها دوليا .

ومع سهولة الإستخدام ورخص التكلفة، وعظم العائد و إرتباط معظم الخدمات وقواعد البيانات والبنى التحتية والأنظمة المالية والمصرفية بشبكة الأنترنت. وغياب تشريعات دولية تقنن إستعمال هده الشبكة سارعت الدول والتنظيمات الإرهابية إلى توظيف الفضاء السيبراني سلبا و إيجابا في تحقيق مكاسب لم يكن من السهل تحقيقها لولا هده الثورة التكنولوجية .

ومن الطبيعي أن يؤدي التوظيف السلبي للفضاء السيبراني للإخلال بالأمن الدولي ،خاصة في ضل ربط معضم البنى التحتية الحرجة بالأنترنت وإمكانية إختراقها وإلحاق أضرار بها كما هو الشأن بالنسبة لمحطات الطاقة الكهربائية والنووية والسدود والتعاملات الإقتصادية والتجارية.

كل هده المخاطر ولدت وعيا دوليا بظرورة مجابهتها وتعزيز الجانب القانوني بالجانب التقني ومحاولة بناء منطلقات فكرية وقانونية وحلول تقنية لمحاصرة تفشي الإستخدام السلبي للفضاء السيبراني .

1) المشكلة البحثية:

وسنحاول في هذه المذكرة إلقاء الضوء على بعض الجوانب المرتبطة بتوظيف الإرهاب السيبراني في التفاعلات الدولية وتداعياته على الأمن الدولي منطلقين من التساؤل الأتي:

كيف ساهم تنامي الإرهاب السيبراني وتوظيفه من طرف مختلف الدول والتنظيمات الإرهابية في تهديد الأمن الدولي ؟

تتفرع عن التساؤل الأساسي **الأسئلة الفرعية** الأتية :

هل هناك إجماع دولي حول مفهوم موحد للإرهاب والمفاهيم المرتبطة به ؟

ماهي تداعيات الإرهاب السيبرني على الأمن الدولي ؟

ماهي أبرز الجهود الدولية لمكافحة هده الظاهرة ؟

2) الفرضيات:

وكإجابة أولية عن تساؤلات الدراسة ننطلق من الفرضيات التالية :

أ- الفرضية الأساسية:

وجدت بعض الدول والتنظيمات الإرهابية في اللاتوافق الدولي حول كيفيات معالجة ظاهرة الإرهاب السيبراني الأرضية الخصبة لتنفيد إستراتيجياتها و تهديد الأمن الدولي .

ب- الفرضيات الفرعية:

*أدى تضارب المصالح الدولية إلى عدم الإجماع حول مفهوم موحد للإرهاب.

*يشكل توظيف الإرهاب السيبراني المهدد الأول للأمن الدولي.

*تلعب هيئة الأمم المتحدة الدور المحوري في التصدي للإرهاب السيبراني.

3 أهداف الدراسة:

في كل دراسة علمية يتم تحديد مجموعة من الأهداف نعمل من خلال البحث والوصف والتحليل للوصول إليها. وأهداف هذه الدراسة تتمثل في مجموعة من النقاط الهامة وهي:

- محاولة إثراء المجال المعرفي لموضوع الإرهاب السيبراني ومايحيط به من مفاهيم ، والإلمام ببعض محاوره ، وذلك لتغطية النقص الواضح للكتابات والبحوث والدراسات وإهتمامات الباحثين في الجزائر حول هذا الموضوع، ولو في إطاره النظري المفاهيمي.
- الكشف عن كيفية توظيف هدا النوع من الإرهاب من طرف الأفراد والمنظمات والدول بالشكل الدي يحقق أهداف وإستراتيجيات مسطرة مسبقا .
- إدراك تأثير الإرهاب السيبراني على الأمن الدولي .
- الكشف عن التحديات التي تواجه المجتمع الدولى وكدا الجهود الدولية للتصدي لهده الظاهرة.

4 أهمية الدراسة:

هذه الدراسة هي محاولة لتقديم وصف تحليلي وتقييم لظاهرة الإرهاب السيبراني على إعتبار أنها إحدى الوسائل والميكانيزمات التي تشكل تهديدا صريحا وصارخا للأمن الدولي نتيجة الضبابية المحيطة بها سواءا من خلال عدم القدرة على تحديد المسؤوليات أو من خلال عدم وجود تشريع دولي موحد لمجابهة هده الظاهرة .

5 مبررات اختيار الموضوع:

مبررات إختيار الموضوع تنبع من عدة اعتبارات موضوعية وأخرى ذاتية، تزيد من دفع الباحث إلى محاولة الوصول إلى نتائج علمية هادفة.

أ- **مبررات موضوعية:** ما دفعني إلى إختيار هذا الموضوع، هو كون توظيف الفضاء السيبراني هو إحدى المسائل التى تحضى بالإهتمام من طرف الدول والفواعل الأخرى في النظام الدولي لسهولة إستعمالها والأضرار الكبيرة التي تخلفها ،خاصة في ضل الطفرة التكنولوجية الحديثة وما خلفته من الإعتماد بشكل واسع على الوسائط التكنولوجية في جميع المجالات .

ب-**مبررات ذاتية:** تتعلق بميولي الشخصي العلمي بمجال التكنولوجيات الحديثة وإدراكي التام بأنه في ضل محاولات تقنين ظاهرة الإرهاب وكدا السعي الدولي من أجل تقييد إستعمال القوة الصلبة في العلاقات الدولية فإن المخرج بالنسبة للدول والفواعل الأخرى يتمثل في الإعتماد على القدرات السيبرانية للمزايا العديدة التي توفرها ،وأهمها عدم القدرة على تحديد المسؤولية من وراء الأفعال .

6 حدود المشكلة:

أ- **زمانيا:** تمتد الفترة الزمانية للدراسة من بداية الألفية الثالثة وتحديدا إنطلاقا من بداية الإهتمام الدولي بالظاهرة إنطلاقا من أحداث سبتمبر 2001 إلى غاية سنة 2016.

ب- مكانيا: يأخذ البحث منهج علمي تحليلي لظاهرة مستمرة ومتصاعدة ومتشابكة من حيث حدود الزمان والمكان فالبحث معني من ناحية الحدود المكانية بأثر هذه الظاهرة على الأمن الدولي (البنى التحتية للمجتمع المعلوماتي العالمي) .

7 المناهج المستخدمة:

إن الظواهر السياسية والاجتماعية هي ظواهر معقدة ومركبة متعددة الأبعاد والمتغيرات، وبالتالي قد يكون من الصعب دراستها بالاعتماد على منهج واحد. الأمر الذي دفعنا إلى الاستعانة في دراستنا بأكثر من منهج. ومن تلك المناهج:

أ- **المنهج التاريخي:** من خلال الوقوف على أهم مراحل التطور التي مرّ بها مفهوم الإرهاب والإرهاب السيبراني ، وكذا بعض الأحداث التي تدخل ضمن نطاق الدراسة . فالمنهج التاريخي طريقة علمية صحيحة ومؤكدة للكشف عن الحقائق التاريخية، وقد ساعدنا هذا المنهج، من منطلق أن دراسة الحاضر وفهمه لا تتم

إلا من خلال فهم الماضي وإستيعابه.

ب- **المستوى الوصفي التحليلي:** باعتباره طريقة من طرق التحليل والتفسير يستخدم الأسلوب العلمي المنظم من أجل الوصول إلى حقائق معينة حول أي قضية، وبالتالي من الضروري إستخدامه في هذه الدراسة في محاولة لتقديم وصف وتقييم لظاهرة الإرهاب السيبراني وتداعياتها على الأمن الدولي .

8 الدراسات السابقة :

إن الدراسات السابقة التي تعرضت إلى هذا الموضوع باللغة العربية وبهذه الصيغة (الإرهاب السيبراني وتداعياته على الأمن الدولي)، تكاد تكون منعدمة . فأغلب الدراسات عالجت الموضوع من الجانب القانوني على أساس عدم وجود تشريعات دولية للتصدي لهذه الظاهرة ، إلا أن هذا لا يعني عدم وجود دراسات في هذا المجال ولكن بطريقة مختلفة، سواء من ناحية التسمية أو من ناحية المحتوى ونذكر منها على سبيل المثال لا الحصر:

أ- دراسة **للدكتور عادل عبد الصادق** تحت عنوان ***بئلأ ذهئ اىئلأ قةنهمى ولقهب غىلظعلإفئ قاظخهي ب*** والصادرة ضمن إصدارات مركز الأهرام للدراسات السياسية والإستراتيجية في العام 2009 لتشير إلى هذا النمط الجديد من الإرهاب وتبرز مختلف الجوانب المتعلقة به وأثره على الصراعات بين مختلف دول العالم عبر مقدمة وخمسة فصول شكلت هيكل الدراسة الرئيس. وملخص الدراسة يدور حول أنه رغم تعدد الإستخدامات السلمية ذات الطابع المدني التي قدمها، ولا يزال يقدمها الفضاء الإلكتروني والمعلوماتي عبر شبكة الأنترنت، إلا أنه ظهرت إستخدامات أخرى غير سلمية لهذا الفضاء المتشعب الإتجاهات بإستغلاله كساحة جديدة للصراعات الدولية، بحيث شكلت هذه الصراعات ما يسمى بظاهرة الإرهاب الإلكتروني الناشئة في الأساس من التزاوج بين تكنولوجيا الإتصال والمعلومات من جهة والإرهاب والحرب من جهة ثانية مما أفرز قضايا معقدة وتحديات مختلفة أمام كافة الفاعلين من الدول والجماعات والأفراد.

ولقد وفق الكاتب إلى حد بعيد في إبراز تأثير الإرهاب الإلكتروني على موازين القوى العالمية.

ب- دراسة **للدكتور مصطفى محمد موسى** تحت عنوان***ىئلأنئ اىئلأقةنهمى*** والصادرة سنة 2009 حيث ركز على مختلف التعاريف المتعلقة بالموضوع كما أبرز وسائل الحماية المستعملة والتى يجب أن تستعمل وكأن بحثه موجه لمجموع الخبراء المكلفين بحماية المنشأت التحتية التي من شأن الهجمات السيبرانية أن تطالها .

إهتم الكاتب بالجانب التقني للموضوع ،وأهمل الجانب السياسي للموضوع من خلال دكر محاولات توظيف هده الظاهرة في التفاعلات الدولية.

ت- دراسة قدمها كل من **P .W Singer & Allan Friedman**, تحت عنوان : ***"Cyber security and Cyberwar: What everyone needs to know",*** والصادرة سنة 2014 من جامعة أكسفورد ،ركزت على هاجس الأمن السيبراني والصعوبات التي تواجهها الدول في الحفاظ على أمن منشأتها وإستغلال الثغرات الموجودة من طرف التنظيمات الإرهابية المدعومة غالبا من طرف قوى عظمى بالشكل الدي سوف يؤدي لامحالة إلى حروب سيبرانية مدمرة أكثر من الحروب التقليدية.

تميزت هده الدراسة بالشمول والدقة بحيث تطرقت إلى جميع جوانب الموضوع ماعدا عدم تركيزها على الجهود الدولية لتقنين إستخدام الفضاء السيبراني.

9 **الإطار المفاهيمي للدراسة :**

الإستراتيجية: هي مفهوم ذو دلالة عسكرية، لذلك تعتبر الإستراتيجيّة من الفنون العسكرية.

من التعاريف الخاصة بالإستراتيجية نجد كلاوزفتز حيث عرفها بأنها: (فن إستخدام المعارك كوسيلة

للوصول إلى هدف الحرب) أما بالنسبة لمولتكه فقد عرفها بأنها: "إجراء الملائمة العملية للوسائل الموضوعة تحت تصرف القائد للوصول إلى الهدف المطلوب" بينما عرفها ليدل هارت بأنها: "فن توزيع وإستخدام مختلف الوسائط العسكرية لتحقيق هدف السياسة" وأما الجنرال باليت فقد عرفها بأنها: "فن تعبئة وتوجيه موارد الأمة أو مجموعة من الأمم – بما فيها القوات المسلحة – لدعم وحماية مصالحها من أعدائها الفعليين أو المحتملين"([1])

الحرب السايبرية:

الحرب السيبرانية هي مجموعة الوسائل والإجراءات الرامية إلى إستخدام التقنيات والمنظومات الإلكترونية بشكل أساسي في مواجهة "العدو"، خاصة في مجال القيادة والسيطرة والإستطلاع، وفي مجال التأثير النفسي والإعلامي السلبي على العدو وجمهوره والتأثير الإيجابي على الصديق، كما تركزت الحرب الإلكترونية على إستخدام المنظومات الإلكترونية في إعاقة منظومات الدفاع الإلكتروني للعدو ([2]).

الأمن السيبراني:

الأمن السيبراني هو عبارة عن مجموع من التدابير والوسائل التقنية والتنظيمية والإدارية التي يتم إستخدامها للحيلولة دون الإستخدام السلبي للوسائل التقنية في إلحاق الأدى أو الدخول الغير مصرح به لقاعدة بيانات البنية التحتية المعلوماتية.

10 صعوبات الدراسة:

إعترضتنا أثناء الدراسة العديد من الصعوبات لعل أهمها:

1 شساعة الموضوع وصعوبة التحكم في جميع المعطيات ومن تم الخروج بخطة تخدم البحث .

[1] محمد بحراوي ، "الإستراتيجية العسكرية (مفهوم)"،في:-***http://strategy.ahlamontada.com/t18-topic***،(2016/12/5).

[2] بدر أحمد ،الإرهـــاب الإلكتروني).. أدواته وآثاره..أساليب الوقاية والعلاج ، في : ***&http://baathparty.sy/site/arabic/index.php?node=552&cat=15369***،(2017/1/12).

2 قلة المراجع التي تخدم الموضوع بالغة العربية مع غزارة في المعلومات الصحفية المتضاربة الأرقام والتحاليل في أغلب الأحيان .

3 ضيق الوقت وبروز إنشغالات شخصية طارئة وملحة أخدت الوقت الكبير من جهدي وتفكيري بالشكل الدي أثر سلبا على إستكمال المدكرة على أرقى وجه .

11 هيكلة الدراسة:

قمنا بتقسيم الدراسة إلى ثلاث فصول

تناولنا في **الفصل الأول الإطار المفاهيمي للدراسة** من خلال مبحثين إستعرضنا في المبحث الأول التعريف بمفهوم الإرهاب أما المبحث الثاني فخصصناه لمفهوم الإرهاب السيبراني ودلك من أجل إعطاء نظرة عن الإرهاب والإرهاب السيبراني وإزالة بعض أشكال اللبس خاصة من خلال إبراز عدم التوافق الدولي حول تحديد جميع الأمور التي تدخل ضمن مفهوم الإرهاب ومن تم مفهوم الارهاب السيبراني ،

الفصل الثاني فخصصناه لتداعيات توظيف الإرهاب السيبراني على الأمن الدولي بحيث حاولنا إبراز مدى خطورة التوظيف السلبي للفضاء السيبراني على الأمن الدولي خاصة في ضل غياب تشريعات دولية لتأطير مختلف العمليات التي تتم فيه ولجوء التنظيمات الإرهابية لتوظيف هدا الفضاء من أجل تحقيق أهداف متنوعة وتناولناه من خلال **ثلاث مباحث** بحيث خصصنا المبحث الأول لمظاهر تهديد الإرهاب السيبراني للأمن الدولي و في المبحث الثاني تكلمنا عن الإرهاب السيبراني كشكل جديد من أشكال الصراع الدولي ،

أما المبحث الثالث فخصصناه لطبيعة أنماط توظيف الفضاء السيبراني في الصراع الدولي ،

أما **الفصل الثالث فخصصناه للجهود الدولية لتأمين الإستخدام السلمي للفضاء السيبراني** من خلال محاولة سن تشريعات دولية للتصدي لظاهرة الإرهاب السيبراني. وعليه قسمناه إلى ثلاثة مباحث ،في المبحث الأول دكرنا جهود هيئة الأمم المتحدة ،أما المبحث الثاني فخصصناه للجهود والمبادرات الدولية ،وفي المبحث الثالث تكلمنا عن تحديات معالجة الإرهاب السيبراني .

من المتعارف عليه لدى دارسي العلوم السياسية أن مفهوم الإرهاب هو من المفاهيم التي بقي يحيطها بعض الغموض من حيث عدم إجماع الدول والمنظمات الدولية على وضع تعريف موحد له ،ومن أجل توضيح بعض جوانب الموضوع نتناول في هدا الفصل أهم التعاريف المتعلقة بمصطلح الإرهاب كما نتطرق إلى أشكال الإرهاب ومختلف التصنيفات المرتبطة به وصولا إلى إعطاء لمحة عن الأسباب الكامنة وراء هده الظاهرة ، ثم نعرج على الإرهاب السيبراني كأحد أشكال الإرهاب المرتبطة بالتطور الحاصل في مجال التكنولوجيات الحديثة لنبين ماهيته وكدا أشكاله وأساليبه ، وسوف يمكننا هدا الفصل من معرفة الجانب المفاهيمي للبحث ومن تم إدراك جميع الأمور المتعلقة بالموضوع خاصة وأن إشكالية الإجماع حول المفاهيم هي إحدى الإشكاليات المطروحة في العلاقات الدولية .

المبحث الأول: مفهوم الإرهاب.

نستعرض في هدا المبحث مختلف التعاريف المتعلقة بالإرهاب وكدا أنواع الإرهاب والأسباب الكامنة وراء بروز و إنتشار هده الظاهرة .

المطلب الأول : تعريف الإرهاب.

إن الدارس لظاهرة الإرهاب يلاحظ الإختلاف الكبير بين فقهاء القانون الدولي والسياسيين في تعريف هده الظاهرة ،على إعتبار أن المنطلقات الفكرية للدارس وخلفياته تطغى على إعطاء هده الظاهرة مفهوما موحدا

فما يزال تعريف الإرهاب حتى يومنا هذا يمثل مشكلة كبرى أمام الباحثين في هذه الظاهرة([1]).

المعنى اللغوي للإرهاب:

لم تذكر كلمة إرهاب في المعاجم العربية القديمة. [(2)]

ولكن يوسف الخياط عرف الفعل رهب – يرهب، رهبة بمعنى الخوف والفزع، أرهب. أما لفظ (الإرهاب) في المعاجم فلم يظهر الاحديثا([3])

[1] Pour plus d'informations voir: LUDOVIC HENNEBEL et GREGORY LEWKOWICZ ***le probleme de ladefinition du terrorisme*** sur ***http://www.philodroit.be/IMG/pdf/Lewkowicz_et_al_-le_probleme_de_la_definition_du_terrorisme_web.pdf le*** **(**29-4-2017 **)**

[2] محمد الباشاء، ***المعجم الكافي : عربي حديث،*** (لبنان : شركة المطبوعات للتوزيع والنشر،ط 2 ، 1992)، ص 67.

[3] يوسف الخياط، ***لسان العرب المحيط*** ، (بيروت :دار الجيل، 1998)، ص 1237.

والإرهابي هو من يلجأ إلى العنف في أفعاله، تعمد إليه حكومات وجماعات ثورية لتحقيق أهداف سياسية فالإرهاب إذن هو إستخدام العنف – غير القانوني – أو التهديد به لتحقيق أهداف سياسية سواء من الحكومة أو الأفراد أو الجماعات الثورية والمعارضة.[1]

ورد لفظ الإرهاب في المعاجم المترجمة إلى اللغتين الإنجليزية والفرنسية، بما يفيد أنة وسيلة لنشر الذعر والتخويف بإستعمال وسائل عنيفة لتحقيق غايات سياسية.[2]

وقد يتم إستخدام العنف سواء من جانب الحكومة أو الأفراد، و(terrorize – Terroriser) أرهب أو روع أو نشر الذعر والإرهاب، يعنى إستعمال القوة لإخضاع شيئ أو إنسان . ويشير لفظ الإرهاب إلى الخوف والهلع.([3])

فالإرهاب هو دلك التوظيف المنظم للعنف والترهيب والتخويف لتحقيق أهداف ما، والإرهابي (terrorist)هو الذي يقوم بهذه الأعمال والتصرفات. ([4])

وتكتسي أهمية التعريف اللغوي للإرهاب حدا كبيرا دفع البعض إلى أن يجعله أساساً لتعريفه إصطلاحيا وإستنباط عناصره وخصائصه التي تميزه عن غيرة من الظواهر التي قد تختلط به.

وهناك محاولات كثيرة قدمت بعض الإجتهادات من أجل تعريف الإرهاب ومنها:

1– المحاولات السياسية:

عرف جاك شيراك رئيس فرنسا الأسبق الإرهاب حيث قال بأن(الإرهاب هو الحرب).[5]

والجدير بالدكر هنا أن المحاولات السياسية لتعريف الإرهاب لا يمكن الإعتماد عليها ،على أساس أن هده المحاولات تختلف من مناسبة إلى أخرى وتتغير بتغير الزمان والمكان ،وهنا أصبح الخلط بين الإرهاب والمقاومة بحيث يخضع دلك إلى إعتبارات شخصية مصلحية .

2

---

[1] عبد الوهاب الكيالي، ***موسوعة السياسة،*** (بيروت :المؤسسة العربية للدراسات والنشر، ط2، 1985)، ص 153.
[2] سهيل إدريس، ***قاموس المنهل (فرنسي – عربي)،*** ، (بيروت : دار الآداب ،ط12، 1994)، ص 1015 .
[3] جميل حزام يحيى الفقية،***مفهوم الإرهاب في القانون الدولي العام***،في:
http://www.adelamer.com/vb/showthread.php?18284 ، (2017 /4/30).
[4] ***المرجع نفسه*** . (موقع إليكتروني).
[5] أمل اليازجي، ***الإرهاب الدولي والنظام العالمي الراهن***،(دمشق، 2002)، ص 61.

– المحاولات القانونية:

جاء في إتفاقية جنيف لقمع ومعاقبة الإرهاب لعام 1937، أن الأعمال الإرهابية هي (الأعمال الإجرامية الموجهة ضد دولة ما وتستهدف، أو يقصد بها، خلق حاله من الرعب في أذهان أشخاص معينين، أو مجموعة من الأشخاص، أو عامة الجمهور).[1]

و عرفت الإتفاقية العربية لعام 1998، الإرهاب في مادتها الأولى فقرة (2) بأنه(كل فعل من أفعال العنف أو التهديد أيا كانت بواعثه أو أغراضه، يقع تنفيذا لمشروع إجرامي فردي أو جماعي، ويهدف إلى إفشاء الرعب بين الناس، أو ترويعهم بإيذائهم أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر، أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة، أو إحتلالها أو الاستيلاء عليها، أو تعريض أحد الموارد الوطنية للخطر). [2]

وحسب تعريف عدد من الفقهاء مثل (جلاسر، سالدن، سيبربولس) فإن الارهاب جريمة دولية و هي : (الفعل الذي يرتكب إخلالا بقواعد القانون الدولي، ويكون ضارا بالمصالح التي يحميها ذلك القانون، مع الاعتراف لهذا الفعل بصفة الجريمة وإستحقاق فاعلة للعقاب) أو هي: (واقعة إجرامية مخالفة لقواعد القانون الدولي، وتضر بمصالح الدول التي يحميها هذا القانون).[3]

وفي نفس الإطار يري الدكتور (رمسيس بهنام) أن الجريمة الدولية هي: (سلوك بشري عمدي يراه المجتمع ممثلا في أغلبية أعضائه – مخلا بركيزة أساسية لكيان هذا المجتمع (أي لقيام التعايش السلمي بين الشعوب) أو بدعامة معززة لهذه الركيزة ويكون منافيا للضمير البشري العالمي لذلك المجتمع).[4]

أما الدكتور(شفيق المصري) فيعرف الإرهاب على: (أنه إستخدام غير شرعي للقوة أو العنف أو التهديد بإستخدامها بقصد تحقيق أهداف سياسية. والإرهاب في هذا الإطار هو الذي يتعدى العمل المخالف للقوانين الداخلية للدولة، أو حتى ذلك الذي لايخالفها، إلى كونه مخالفا لمبادىء القانون الدولي وقواعده. ولهذا فهو يعرف عادة بالإرهاب الدولي). [5]

---

1 أنظر: أنس السلطان،"الإرهاب الدي لا نعرفه"، في ***http://www.masralarabia.com:*** (2017/1/30).

2 فريحة حسين،"الإرهاب في أحكام القانون الدولي الجنائي"،**مجلة دفاتر السياسة والقانون**، جامعة المسيلة،(عدد 5 جوان 2011)،ص ص 160-181.

3 د / محمد محي الدين عوض، ***الجريمة الدولية، تقنيتها والمحاكمة عليها***، (القاهرة، 1987)، ص 18.

4 حزام يحيى الفقية، ***مرجع سابق.*** (موقع إليكتروني).

5 شفيق المصري، ***مكافحة الإرهاب في القانون الدولي***،(القاهرة، 1998)، ص15.

أما الدكتور كمال حماد فيعرف الإرهاب على أنه: (نوعا من إستخدام لطرق عنيفة كوسيلة، الهدف منها نشر الرعب في المجتمع لإضعاف الحكم وتحقيق تغيرات سياسية).[1]

وفي إطار ضرورة التمييز بين إرهاب الأفراد وإرهاب الدولة، تمسكت مجموعة عدم الإنحياز بهدا الأمر ، وتقدمت باقتراح يعتبر من أفعال الإرهاب الدولي : (أعمال العنف والقمع والتي تمارسها الأنظمة الإستعمارية والعنصرية الأجنبية ضد الشعوب التي تكافح من أجل التحرير والحصول على حقها المشروع في تقرير المصير والإستقلال ومن أجل حقوق الإنسان وحرياته الأساسية الأخرى، وهناك أيضا قيام دول معينة تعمل على تقديم المساعدة لبقايا التنظيمات الفاشية أو المرتزقة التي تمارس أعمالها الإرهابية ضد دول أخرى ذات سيادة، أو غض الطرف عن ممارسات هذه التنظيمات. ومن هذه الأفعال أيضا أعمال العنف التي يمارسها أفراد أو جماعات والتي تعرض للخطر حياة الأبرياء أو تنتهك الحريات السياسية، دون إخلال بالحقوق غير القابلة للتصرف في حق تقرير المصير والإستقلال لكل الشعوب الخاضعة لسيطرة الأنظمة الإستعمارية والعنصرية أو لأية أشكال أخرى من السيطرة الأجنبية أو لحقها المشروع في الكفاح، وعلى وجه الخصوص كفاح حركات التحرر الوطني طبقا لأهداف ومبادئ ميثاق الأمم المتحدة ([2]).

ويوصف التعريف الدي قدمته مجموعة عدم الإنحياز بأنه ميز بين إرهاب الدولة الذي سوف نتناوله في أشكال الارهاب الذي ترتكبه الدول، وإرهاب الأفراد، كما أنة يستثنى كفاح حركات التحرر الذي يعتبر عملا مشروعا وفق القانون الدولي وميثاق الأمم المتحدة وقراراتها، في الوقت الذي تزعمت الولايات المتحدة إتجاها مضادا يستبعد إرهاب الدولة، ويلقي الشبهة على الأفراد والحكومات،وساندتها في دلك العديد من الدول الغربية ،من أجل تبرير بعض الأعمال التي تقوم بها أمريكا والحلف الأطلسي ، وإدانة حركات التحرر الوطني، كما يرتكز المشروع الأمريكي على الإرهاب الفردي، فقد أعتبر أن (كل شخص يقوم في ظروف غير مشروعه بقتل آخر أو إحداث ضرر بدني فادح له أو يقوم بإختطاف أو يحاول إرتكاب هذا الفعل، فإنه يرتكب جريمة ذات بعد دولي).[3]

ويعتبر المشروع الأمريكي أن الجريمة في هذا الحال ذات بعد دولي إذا ما كان العمل[4]:

---

[1] كمال حماد، ***الإرهاب والمقاومة في ضوء القانون الدولي العام*** ،(الجزائر: المؤسسة الجامعية للدراسات والنشر ، 2002)، ص 23 ،24.

[2] حزام يحيى الفقية ، ***مرجع سابق***. (موقع إليكتروني).

[3] محمد تاج الدين الحسيني، ***مساهمة في فهم ظاهرة الإرهاب الدولي***،(الرباط ، 1990)، ص24 .

[4] حزام يحيى الفقية ، ***مرجع سابق***. (موقع إليكتروني).

أ– أن يرتكب الفعل الإجرامي خارج نطاق الدولة، متناسيا في ذلك الأعمال الإرهابية التي تمارسها المنظمات الإرهابية أمريكية المنشأ في بلادها.

ب – أن يوجه العمل الإجرامي إلى أفراد الدولة خلال المنازعات.

ج – إذا كان العمل يستهدف المساس بمصالح أو الحصول على تنازلات من دولة أو منظمة دولية.

وفي إطار تعريف الإرهاب كان أقرب التعاريف لظاهرة الإرهاب منطقية أكثر من غيرها التعريف الدي جاءت به منظمة المؤتمر الإسلامي في مؤتمرها المنعقد على مستوى وزراء خارجية المنظمة في عام 2001، في الدوحة في قطر، ، حيث عرف الإرهاب هنا على أنه: (رسالة عنف عشوائية من مجهول بغير هدف مشروع أو قضية عادلة وهو بهذا مخالف للشرائع السماوية والأعراف الدولية، كما لايجوز الخلط الذريع بين الكفاح المسلح الذي يراد به خدمة القضايا العادلة ومجابهة الظلم والإحتلال كما يحدث في فلسطين ولبنان)([1]).

المطلب الثاني :أشكال الإرهاب

يتخد الإرهاب أشكالا عديدة تختلف وفقا لإختلاف مرتكبيه وكدا الغرض من دلك فقد نجد إرهابا ممارسا من طرف نظام حكم معين ضد أفراده أو ضد دول أخرى كما نجد إرهابا تقوم به تنظيمات إرهابية لها أهداف متباينة مكانيا وزمانيا ،وعلى هذا الأساس لابد من تناول الموضوع على الشكل التالي:

أ) أشكال الإرهاب وفقا لمرتكبيه:

يمكن تقسيم الإرهاب من حيث القائمين به إلى نوعين هما:

– **إرهاب نظام الحكم، وإرهاب الأفراد والمجموعات.** ، فنظام الحكم يرتكب الإرهاب بنفسه أو بواسطة دعمه لبعض الأفراد أو الجماعات ليضعف بعض الدول الأخرى المنافسة، كم أن الجماعة الإرهابية إذا نجحت وسيطرت على مقاليد السلطة قد تستمر في إستخدام العنف والإرهاب وهي في السلطة.[(2)]

ويمكن التطرق لهما كما يلي:

---

[1] حزام يحيى الفقية ، ***مرجع سابق***. (موقع إلكتروني).

[2] إمام حسانين خليل، ***الإرهاب بين التجريم والمشروعية***،(القاهرة ، 2001)، ص 53 .

1 – إرهاب نظام الحكم (إرهاب الدولة):

إستخدمت الأنظمة الدكتاتورية تاريخيا الرعب كأداة للقمع والتحكم، ودلك من أجل ضمان بقائها والحيلولة دون قيام أي نزعة ثورية ضدها ،ولدلك قد تلجأ إلى القيام بأعمال إرهابية داخل أقاليم الدول المناوئة لها .

ويجب هنا التمييز بين عبارة دولة إرهابية ووسيلة حكم إرهابية فالدولة بمعزل عن كل وصف يوسمها بالإرهابية وهي فوق كل الشبهات، ويرى البعض أن إرهاب الدولة هو أحد المحركات الأساسية لإرهاب الأفراد والجماعات ويتواكب دائما تصاعد إرهاب الأفراد والجماعات مع تصاعد الإرهاب الحكومي.

إن الإرهاب الذي تمارسه أنظمة الحكم، وخاصة من خلال دعمها للعناصر الإرهابية ماديا أو معنويا، قد يؤدي إلى المواجهة العسكرية المباشرة مع الدولة الخصم، ولاسيما إذا كانت تمارسه ضد دولة كبرى.[1]

ولعل الحرب التي تشنها إيران في الأرض العراقية ضد الجيش الأمريكي لمثال حي على دلك وكذلك الحرب التي شنتها أمريكا نفسها في دعمها للحركات الإنفصاليه في عدد من دول العالم ضد حكوماتها بالإضافة إلى الحرب التي قادتها ومولتها الولايات المتحدة الأمريكية ضد الإتحاد السوفيتي السابق في أفغانستان في ثمانينات وتسعينات القرن الماضي.([2])

وهناك من يرفض وصف الدول بالإرهابية ويحذر آخرون من الإنغماس في إتهام الدولة بالإرهاب لأن دليل تورطها يكون مجرد إنطباع عادي، وقد يفتح المجال لإتهام الدول الديمقراطية بممارسة الإرهاب ودعمه، والمقصود هنا الدول الغربية. ويعرض البعض لأشكال الإرهاب من مجموعات غير الدول مغفلا أيضا إرهاب الدولة.([3])

وإذا كانت الغالبية من الفقهاء تؤيد وجود إرهاب الدولة إلا أنهم اختلفوا في تعريفاتهم للمقصود منه، كما، أنهم عددوا صورا مختلفة لإرهاب الدولة.[4]

فالبعض يعرفه بأنه إستعمال الدولة لوسائل العنف بإنتظام لإثارة الرعب لتحقيق أهداف سياسية.

---

[1] أنظر عبد الناصر حريز، ***مرجع سابق***، ص 177 .

[2] للتعمق أكثر في الموضوع أنظر : معتز سلامة ، ***العلاقات-السياسية-العراقية--الأمريكية-1979-2003***، ***http://www.aljazeera.net/specialcoverage/coverage2003***،(29 /4/ 2017).

[3] حزام يحيى الفقية ،***مرجع سابق***. (موقع إلكتروني).

[4] خليل، ***مرجع سابق*** ، ص 56.

وهذه الأهداف قد تكون الإحتفاظ بالسلطة أو قمع المعارضة، فالإرهاب يساعد الدولة على تحقيق بعض الأهداف التي تعجز الطرق السلمية عن تحقيقها، وإرهاب الدولة يسمى أيضا إرهاب المؤسسة أو الإرهاب السلطوي أو المؤسسي نظرا لأنه يحافظ على السلطة والشرعية والمؤسسات.

وهذا الإرهاب تمارسه دول العالم كافة دون إستثناء، وضمن المجتمع الواحد، والدولة الواحدة، وبين الدول أيضا منذ القدم وحتى الآن.

ولدلك وعلى ورغم أن نظام الحكم هو الواجهة الأساسية للدولة يلقى تأييدا شعبيا واسعا في جميع أعماله فحسب رأيي لايمكن وصف دولة بأنها إرهابية بالشكل الدي يجعل جميع الأفعال التي يقوم بها المجتمع الدولي مباحة ، وإنما يمكن أن تشتمل الدولة على وسيلة حكم إرهابية قد تلقى تأييدا من طرف فئة من الشعب على أساس تقديمها لطروحات ونظرة معينة لأعمالها تلقى من خلالها دعما من هده الشريحة ، وعليه فإن الواجب هنا هو الحديث عن وسيلة الحكم دون وصف الدولة بالإرهابية .

ب) إرهاب الأفراد والجماعات:

يتولد عن العنف الممارس من طرف السلطة الحاكمة ،عنفا مضاضا بأساليب مختلفة قد تكون أكثر عنفا وأكبر مدة ،لأن الدوافع النفسية لا تزول إلا بتحقيق الغاية من دلك وهي إسقاط النظام في غالب الأحيان .

والجدير بالدكر هنا أن إرهاب الأفراد والجماعات يتخد صورا عديدة يوجزها الدكتور جميل حزام يحيى الفقية في أربع صور وهي([1]):

1 – الإرهاب الثوري، وهو الإرهاب الذي يهدف إلى إحداث تغيير شامل وكامل في التركيبة السياسية والإجماعية للنظام القائم، وقد يكون في إطار حركه عالمية أو في إطار داخلي.

2 – الإرهاب شبة الثوري، والذي يهدف بدورة إلى إحداث بعض التغيرات البنائية والوظيفية في نظام سياسي معين، وقد يصبح جزاء من برنامج أكثر إتساعا للتغيير السياسي.

[1] حزام يحيى الفقية ، ***مرجع سابق***. (موقع إلكتروني).

3 – الإرهاب العدمي، ويستهدف إستئصال النظام القائم دون وجود تصور لنظام بديل، فهو لايستهدف التغيير فقط بل التدمير، وهذه الفئات لاتسبب تحديات كبيرة للدولة كما لايوجد لها أمثلة معاصرة، ولكنها وجدت إبان الثورة الفرنسية.

4 – الإرهاب العادي، وهو الذي يمارسه الأفراد لتحقيق مصالح شخصية، إقتصادية، أو إجتماعية، فهو بعيد عن الهدف السياسي ويتجلى في أعمال الخطف والإحتجاز .

أشكال الإرهاب وفقا لنطاقه:

هنا يمكن تقسيم الإرهاب إلى نمطين هما: إرهاب محلي يمارس نشاطه داخل الدولة وإرهاب دولي يمتد عبر الدول ، وفيما يلي تفصيلا لدلك:

أ – الإرهاب المحلي:

إن وصف الإرهاب بالمحلي يعني أن نشاطه يرتكز داخل إقليم معين تحقيقا لأهداف محلية معينة مثلما حدث في الجزائر سنوات التسعينيات، ويمارس الإرهاب هنا سواء من طرف جماعات ضد الدولة أو من طرف النظام الحاكم ضد جماعات عرقية معينة كما هو الحال بالنسبة لبعض الأنظمة المتسلطة.

ويعتبر الإرهاب المحلي خطرا محدقا بكيان الدولة بحيث قد يتطور ويلقى دعما من الخارج لتتغير مطالبه بالشكل الدي يخدم أجندات خارجية كالمطالبة بالإنفصال أو طلب التدخل الأجنبي تحت غطاء إنساني، وهو ما نشهده اليوم من تكالب الدول الغربية على دول العالم الثالث تحت غطاء محاربة الإرهاب وحماية حقوق الإنسان.

ب – الإرهاب الدولي:

وهو الإرهاب الذي تتوافر له الصفة الدولية في أحد عناصره ومكوناته، وذلك عندما يكون أحد الأطراف دوليا سواء أشخاص أو أشياء أو أماكن، أو يكون الهدف دوليا مثل إساءة العلاقات الدولية([1]).

ويتخد الإرهاب الدولي أشكالا عديدة تختلف بإختلاف النوايا الكامنة وراءه بحيث يخترق الحدود الوطنية ليأثر على الأمن الإقليمي أو الدولي .

[1] حزام يحيى الفقية، ***مرجع سابق*** . (موقع إلكتروني).

المطلب الثالث : النظريات المفسرة لأسباب ظهور الإرهاب.

.تعتبر جرائم التمييز العنصري والتفرقة على أساس العنصر أو الجنس من الجرائم ضد الإنسانية التي تهدد السلم والأمن الدوليين، ولكن مازالت بعض الدول تمارس إلى الآن الإرهاب العنصري سواء من خلال سلطاتها الرسمية أو من خلال بعض الجماعات المتخصصة فيها، ومثال الأولى: إسرائيل ضد الفلسطينيين التي تقوم بحملة تجويع وتشريد وطرد واسعة النطاق ضدهم، ومثال الثانية جماعة (الكلوكلولان) الأمريكية التي تمارس عملياتها ضد السود([1]).

إن ظاهرة الإرهاب ليست جديدة على المجتمع الدولي و قد تأثرت على مر العصور بالظروف التي مربها المجتمع الدولي. وتؤثر الأوضاع الدولية السياسية والإقتصادية والإجتماعية على الإرهاب سلبيا أو إيجابيا، ذلك يرجع بصفة خاصة إلى إكتساب الإرهاب بعدا دوليا.([2])

وقد حاولت العديد من النظريات تفسير أسباب ظهور وتفشي ظاهرة الإرهاب إستنادا إلى منطلقات معينة نوجز أهم أفكارها فيما يلي([3]):

1- النظرية الماركسية : هي نظرية صراعية فحواها أن الصراع الطبقي يحدث في مرحلة معينة من تطور المجتمعات، وتظهر التناقضات بين القوى الإجتماعية بناء على التنافس حول ملكية وسائل الإنتاج. وهذا التناقض الطبقي يؤدي إلى عنف سياسي يتمثل في ثورة البروليتاريا على الطبقة البورجوازية المالكة لوسائل الإنتاج.ومع تعنت هده الأخيرة وتمسكها بالحفاظ على ممتلكاتها تلجأ طبقة العمال إلى أساليب عنف مبتكرة تشكل فيما بعد ظاهرة الإرهاب، ومن جهتها تقوم الدولة بأعمال إرهابية للدفاع عن مكتسبات الطبقة البورجوازية.

2- النظرية الوظيفية: تنطلق هده النظرية من وجود خلل وظيفي في بنية النظام الدولي ينجر عنه السلوك الإرهابي فالأوضاع الثورية على حد تعبير ثالكوت بارسنز تأتي عندما يكون النسق السياسي بمجمله غير متسق مع المجتمع، وهذا يحدث عندما يعاني المجتمع من حالات العجوزات الوظيفية المتعددة؛ وبالتالي لا يستطيع القيام بوظائفه مما يترتب عليه التعرض لضغوط متعددة من أجل

---

[1] محمد عزيز شكري ،أمل اليازجي، ***الإرهاب الدولي والنظام العالمي الراهن***،(سوريا :دار الفكر المعاصر، 2002)، ص9.

2عصام فاعور ملكاوي ،***واقع الإرهاب الدولي*** ،(الرياض ،2013)،ص ص 9-18.

[3] عبده مختار موسى، ***كافحة الإرهاب المفاهيم والاستراتيجيات والنماذج***،(دبي:مركز المسبار للدراسات والبحوث 2015)،ص ص 15-34.

التغيير،هدا التغيير يتخد مسارات عديدة وكيفيات متعددة تتجسد في أغلبها عن طريق أعمال عنف ([1]).

3- نظرية الحرمان النسبي([2]):تلعب الضغوط الاجتماعية أو الشدائد إحدى أهم المحاور التي ترتكز عليها هذه النظرية ، وهذه الضغوط ينظر إليها على أنها المحرِّض المباشر والنهائي لأعمال العنف ضد النظام الاستعماري، أو الحكومة المستبدة الطاغية في الدولة المستقلة.

4- النظريات الاقتصادية: تقوم على افتراض وجود تأثير متبادل بين الأوضاع الاقتصادية والاستقرار السياسي في الدولة.

5- النظريات السياسية الصراعية: تلعب عملية التنافس السياسي على السلطة الدور الكبير والأساسي في توليد العنف حسب هده النظريات فالرغبة الإنسانية في تقلد المناصب السياسية هي التي ولدت أشكالا عديدة من العنف خاصة مع تمسك صاحب السلطة بها ورفضه لأي شكل من أشكال التغيير الديموقراطي.

6- نظرية الثقافة السائدة : تركز هده النظرية على عنصري الثقافة والدين بحيث ترجع أسباب السلوك الإرهابي إلى عوامل ثقافية تساعد على تفشي هده الظاهرة وتتغدى من تراث ثقافي وديني معين([3]) .

من خلال هده النظريات وغيرها يمكن إبراز أهم الدوافع الكامنة وراء السلوك الإرهابي وهي:

1) الدوافع السياسية الدولية للإرهاب:

ويمكن إيراد بعض هذه الدوافع السياسية على النحو التالي([4]):

- زوال الثنائية القطبية إنفراد الولايات المتحدة بإدارة النظام الدولي ،مما خلق لدي نوع من الإمتعاص لدى المجتمع الدولي ومن تم بدأ البحث على إعتناق إيديولوجيات كفيلة بإعادة التوازن للنظام الدولي.

- تزايد حدة الصراعات العرقية والإثنية حول العالم وظهور حركات سياسية دينية.

---

[1] أحمد فلاح العموش ،***مستقبل الإرهاب في القرن الواحد والعشرون***،(الرياض:جامعة نايف للعلوم الأمنية،2006)،ص ص19-45.

2 بشرى عناد، "التعصب وعلاقته بالهوية الاجتماعية والمكانة الإجتماعية لدى العاطلين عن العمل" ،***مجلة الفتح*** ،(ع 53،افريل 2013)، ص ص71-112.

[3] ***المكان نفسه.***

[4] حزام يحيى الفقية،***مرجع سابق*** . (موقع إلكتروني).

– عدم مساهمة المجتمع الدولي في القضاء على بعض أنواع الإستعمار التي لا تزال موجودة كما هو الحال بالنسبة لفلسطين والصحراء الغربية.

– توظيف الإرهاب كبديل عن الحرب التقليدية، بوصفة أسرع تأثيرا، وأقل تكلفة خاصة في ضل تدييق النطاق على إستخدام القوة في العلاقات الدولية .

– وجود بؤر للتوتر في معظم دول العالم سواء في الشرق الأوسط أو أمريكا اللاتينية أو أوروبا، فضل عن المخلفات الإستعماريه، الأمر الدي شجع تنامي دور التنظيمات الإرهابية.

– النجاحات التي حققتها بعض الحركات التحررية.

– الأوضاع الدولية غير العادلة، وسياسة الكيل بمكيالين المنتهجة على الصعيد العالمي .[1]

–التوسع الإمبريالي الدي يشجع حركات العنف والإرهاب.

والجدير بالدكر أن الإرهاب هو صناعة غربية للسيطرة على ما تبقى من خيرات الدول المتخلفة.[2]

2) الدوافع الاقتصادية للإرهاب:

إن الأوضاع الإقتصادية على المستوى الدولي تؤثر بشكل أو بآخر على إتجاه بعض الجماعات والدول إلى الإرهاب، والدليل على ذلك هو ظهور المنظمات اليسارية الشيوعية بقصد القضاء على الأنظمة الرأسمالية، بوصفها تمثل الإحتكار وعدم العدالة وإنعدام المساواة،وهو مادهبت إليه المدرسة الماركسية في تفسيرها لظاهرة الإرهاب وفي المقابل ظهرت تيارات تقاوم هذه المنظمات وتعمل على الحفاظ على الأوضاع القائمة في المجتمع، ومن هنا يتولد العنف والعنف المضاد، فعملية التحول الإشتراكي في نهاية الستينيات من القرن الماضي أثارت قلقا واسعا لدى الملاك ، هدا القلق ترجم في عديد الأحيان إلى أشكال مختلفة من العنف والإرهاب.

ومع إزدهار إقتصاديات بعض الدول ،وعجز أخرى عن مجاراتها ،سعت كل واحدة منها إلى ضرب مصادر الدخل القومي ومن تم تحقيق نوع من الإزدهار على حساب الطرف الأخر ،ومن هنا أصبح العامل

[1] سالم إبراهيم بن عامر، ***العنف والإرهاب***،(ليبيا :المركز العلمي للدراسات والأبحاث ، 1988)، ص 31 .
[2] عبد العزيز عبد الهادي مخيمر، ***الإرهاب الدولي***،(القاهرة: دار النهضة العربية ، 1986)، ص 97.

الإقتصادي على المستوى الدولي دافعا قويا للإرهاب ، حيث أن معظم الجماعات والدول المنخرطة في أعمال الإرهاب هي من الجماعات والدول الفقيرة نتيجة تدهور إقتصادها. بل إن هناك إقتصاديات بعض الدول تقوم على الأنشطة الإجرامية، ومن ثم فإن هذه الدول تكون بيئة صالحة للإرهاب، من أجل الحصول على الدور الذي تبتغيه على المستوى الدولي، بعد أن أيقنت بعدم قدرتها على التأثير لضعف مواردها الإقتصادية. ويمكن أن تتم ممارسة الإرهاب على مستوى الدولة بقصد التخلص من الإستغلال الأجنبي لمقدرات الشعوب ومواردها، أو للإضرار باقتصاديات دولة معينة، بتدمير منشأتها الصناعية والتجارية مما يشكل وسيلة ضغط عليها لتغيير مواقفها السياسية والاقتصادية.([1]) كما قد تستخدم المساعدات الإقتصادية لبعض الدول كذريعة للتدخل في شؤونها الداخلية أو المحافظة على الإستقرار الدولي وحماية الأقليات، الأمر الذي يقابل بالرفض من جانب البعض ويدفعه إلى الوقوف ضده من خلال أعمال العنف.[(2)]

3) الدوافع الثقافية الدولية للإرهاب:

مما لا ريب فيه أن العوامل الثقافية تؤثر على فكر الإنسان قد تدفعه أحيانا إلى إرتكاب الجريمة، وينطبق هذا القول على المستويين الوطني والدولي، ونتيجة التداخل بين الثقافات وبروز ثقافات هجينة تستند إلى تشريعات مستحدثة برزت أنماط جديدة من السلوك الإنساني تدعو إلى إستعمال العنف بدون قيود في مواجهة ثقافات أخرى تحت شعارات مختلفة ([3])،وترتبط الثقافة أحيانا بالجانب الديني، وما يظهر من حركات تعصب ديني في بعض المناطق نتيجة إذكاء روح التطرف والغلو في الدين، وتشهد لذلك أمثلة عديدة في مختلف دول العالم منها: المتطرفين في إسرائيل السيخ في الهند واليهود ، تنظيمي القاعدة وداعش بالنسبة لنموذج الجماعات الإسلامية. [(4)]

ولما كان إي تهديد للقيم ، مثل اللغة والإنتماء والأرض،يلقى إستنفارا كبيرا من جميع أفراد المجتمع فإحتمال فقدان أي من هذه العناصر قد يفجر ردود فعل غاضبة ونشأت على أثر ذلك العديد من جماعات العنف والتطرف في مختلف دول العالم. وخلاصة القول أن الخوف من الغزو الثقافي يقود إلى العنف، ، والدين هو

[1] ملكاوي ،***مرجع سابق*** ،ص 17.
[2] خليل، ***مرجع سابق***، ص 102.
3 رقية السيد الطيب عباس،***الإرهاب الأسس الثقافية والنفسية***، (الأردن :منشورات جامعة فيلديفيا ،2007)، ص15،16 .
4 سعيد مراد، "مواجهة الإرهاب مسئولية مشتركة لكل الأطراف على جميع المستويات"، ***جريدة الأهرام المسائي***، القاهرة،(عدد7899 ، 12 ديسمبر 2012)،ص12.

أكثر القيم الثقافية تأثيرا، فالتهديد الموجه لديانة الفرد لاتضع الحاضر فقط في خطر، ولكن الماضي الثقافي للفرد والمستقبل أيضا، فالديانات واثقة أنها على حق([1]).

كما ساعدت بعض الدول الجماعات الإرهابية وذلك بعد أن وفرت الدعم المالي والتدريب الراقي والتخطيط الدقيق لعملياتهم وساعدتهم على تحقيق الإتصال بينهم في كثير من دول العالم، بالإضافة لدورها في إيواء عناصر الإرهاب بعد تنفيذ عملياتهم وهروبهم، ورفضها تسليمهم للسلطات المختصة لمحاكمتهم.[2]

ولدى الدول التي تساعد الإرهاب قناعة بقدرتها على إستخدام هذه الجماعات في إحراج السلطة السياسية والضغط عليها في أي وقت لتحقيق مطالبها.[3]

وقد ثبت أن هناك شبكات دولية في دول أوروبا تقوم بتمويل ومساندة وإيواء عناصر الإرهاب، وأنها على إتصال دائم بها من خلال دول كبرى. بل إن الدول والأنظمة السياسية تتبنى وترعى الإرهاب وتلعب دورا مباشرا أوغير مباشر في صنعة.

بل إن هناك من الدول من تتبع الإرهاب منهجا وأسلوبا في سياستها في ظل إدعاء واسع بالديمقراطية والمثال الواضح عليها إسرائيل وممارساتها التعسفية والقمعية في الأراضي العربية المحتلة.

لايمكن فصل التدابير التي ينبغي إتخاذها لمكافحة الإرهاب الدولي عن أسبابه ، فدراسة الأسباب شرط مسبق للتدابير، وهناك ظروف عامه هيأت الفرصة لهذا الإرهاب، مثل([4]):

أ) نجاحه في كسب أهداف قصيرة الأجل تشجع على المنافسة والبقاء.

ب) إنسياب المعلومات وإنتشارها حول التكنولوجيا والتكتيكات المسلحة من خلال وسائل الإعلام وثقافة الإرهابي.

ج) تفادي الدخول في حروب دولية غير مأمون عواقبها.

د) تشجيع الدول للإرهاب وتقديمها التسهيلات التدريبية للحركات الإرهابية.

---

[1] حزام يحيى الفقية، ***مرجع سابق***. (موقع إلكتروني).

[2] خضر الهواري، "إنتشار الإرهاب الدولي"، ***السياسة الدولية***، (عدد 77، جويلية، 1984)، ص ص 145-151.

[3] خليل، ***مرجع سابق***، ص 104.

[4] حزام يحيى الفقية، ***مرجع سابق***. (موقع إلكتروني).

هـ) التطور الهائل في وسائل الإعلام، وتكاثر الأخبار الدولية التي تغطي أحداثة مما زاد من فرص الإرهابيين وشهيتهم.

وعلى العموم فإن الإرهاب كظاهرة عالمية معاصرة ماهو إلا إنعكاس لأزمة ضمير وأزمة إخلاقيات حادة ومستحكمة يشهدها النظام السياسي العالمي، وإقتصاده ، زيادة عن خضوع العديد من الدول والحكومات أو تواطؤها مع منظمات الإرهاب الدولي خدمة لمصالحها بعيدا كل البعد عن أحكام الشرعية الدولية وما تتغنى به العديد من الدول في المحافل الدولية مما يضع تحت أيدي هذه المنظمات إمكانيات واسعة تساعدها على تنفيذ المخططات الإرهابية، وكذلك التكامل والتنسيق والتبادل بين منظمات الإرهاب، والتقدم التكنولوجي، ويضاف إلى ذلك المواقف السلبية للدول في مواجهة الإرهاب وعدم المشاركة الجدية في مكافحته مما كان له أثر مهم في إتساع ظاهرة الإرهاب.[1]

وفي محاولة للتسوية شرح القرار الأممي رقم (40 / 61 لعام 1985م، مفهوم الإرهاب، ودعى جميع الدول إلى أن تهتم بالقضاء التدريجي على الأسباب الكامنة وراء الإرهاب الدولي (إرهابا رسميا) وهذه الحالات هي: الإستعمار والعنصرية، والحالات التي تنطوي على إنتهاكات عديدة وصارخة لحقوق الإنسان والحريات الأساسية، والحالات التي يوجد فيها إحتلال أجنبي.[2]

ولعله من أسباب إنتشار الإرهاب الدولي كذلك، هو عدم كفاية المعايير الدولية الموجودة الآن في بعض المجالات. ومن المسائل التي تثير القلق في هذا المضمار مايلي: سياسات الدولة وممارستها التي يمكن أن تعتبرها الدول الأخرى إنتهاكا للإلتزامات التي تقضي بها المعاهدات الدولية، كما أن عدم وجود معايير تحدد مسؤولية الدولة عن عدم الوفاء بالإلتزامات الدولية القائمة، وإساءة إستعمال السلطة الممنوحة لها دوليا، وعدم وجود معايير بشأن مسؤولية الدول عن أعمال لايحضرها القانون الدولي، وإنعدام هيئة تشرف على التنظيم والمراقبة الدوليين لعمليات نقل الأسلحة والإتجار بها، وقصور تجميد فاعلية الآليات الدولية المعنية بتسوية النزاعات بالطرق السلمية وبإنفاذ حقوق الإنسان المحمية دوليا وإقتصار دلك على مجلس الأمن الدولي ، وقصور التعاون الدولي في مجال منع ومكافحة كل أشكال ومظاهر العنف الإرهابي بطريقة فعالة وموحدة.[3]

---

[1] إبراهيم نافع، ***كابوس الإرهاب وسقوط الأقنعة*** ، (القاهرة : مركز الأهرام للترجمة والنشر، ،2002)، ص24.

[2] ***المكان نفسه.***

[3] نافع ، ***مرجع سابق*** ، ص 110.

المبحث الثاني : مفهوم الإرهاب السيبراني.

المطلب الأول : تعريف الإرهاب السيبراني.

إن أول إشكالية تظهر عند الحديث عن الإرهاب السيبراني هي إشكالية تحديد مفهوم العنف الممارس في الفضاء الإفتراضي ومدى صلته بالعنف المعرف في الواقع ، وهنا إدا إعتمدنا على تعريف جون قالتونغ للعنف ([1]) يمكننا تلخيصه بشكل عام على أنه "الإهانات التي يمكن تجنبها، الموجهة للإحتياجات الإنسانية الأساسية وبشكل أعم للحياة والتي تخفض مستوى تلبية الإحتياجات الحقيقية إلى مادون المستوى المحتمل والمتوقع " وبكلام أوضح فكل فعل يمارس ضدنا ويكون بالإمكان تجنبه وتكون نتيجته حرماننا من الإحتياجات التي نتوقها ، يدخل في خانة العنف.

ولعل التوضيحات التي أضافها بونتارا ([2]) لمفهوم العنف جعلته أكثر وضوحا بأن أشترطت أن يكون بالفعل غير مصرح به أو لا يتمتع بمشروعية إقراره من سلطة شرعية محلية أو دولية كما لا تشترط توضيحات بونتارا أن يقترن الفعل العنيف بإحداث ضرر مباشر وملموس.

وهنا يجب التمييز بين ثلاثة مستويات لتعريف الفعل الإجرامي في الفضاء الإفتراضي ([3]):

الأول:الجريمة الإلكترونية وهي الأفعال التي يعاقب عليها القانون وتعتبر شبكة الإنترنت والفضاء السيبراني أداتها وساحتها وهدفها و يدخل تحت هده الخانة عدد واسع من الجرائم الإلكترونية كالقرصنة التجسس،النصب ، سرقة المعلومات إلى أخر هده الأفعال الإجرامية.

---

[1] Galtang.J",cultural violance,"***Journal of peace research***,(vol 27,no 3 ,1990)pp.289 -291

[2] Pontara.G, "the concept of violance," ***Journal of peace research***,(vol15, n,1,1978) .pp 19. 32.

[3] رائد العدوان ، ***المعالجة الدولية لقضايا الإرهاب الإلكتروني***،(الرياض ، 2013)، ص 7،8.

الثاني :الأعمال الإرهابية التي تمارس عبر شبكة الأنترنت ، ويقصد بها الأنشطة التي تقوم بها منظمات أو جماعات إرهابية تقليدية من أجل تدعيم أعمالها على أرض الواقع وتشمل من بين أنشطة : التجنيد ، الدعاية ، الموارد التعليمية الخاصة بالأعمال الإرهابية ، التمويل ، تبادل الأوامر .....إلخ[1]

الثالث :الإرهاب الإلكتروني وهي الأعمال والأنشطة التي تقوم بها أفراد أو جماعات بإستخدام تكنولوجيا المعلومات والشبكة العنكبوتية بقصد إحداث دمار للبنى التحتية المرتبطة والمدارة بواسطة مثل هده التكنولوجيا كشبكات توزيع المياه والكهرباء ،أنظمة الخدمات المصرفية، السجلات الصحية ،الأنظمة العسكرية ، وغيرها من البنى التحتية التى من شأن تدميرها أن يحدث أضرارا مباشرة وغير مباشرة بالمواطنين والدول([2]).

وعليه يقترح أركيلا و رونفلدت **Arquilla.J.and Ronfeldt .D** ([3]) توزيع الناشطين عبر الأنترنت على ثلاث مجموعات مع إقامة الفارق بينهم :

1 الناشطون activist :وهم الدين يستخدمون الأنترنت لقضية سياسية معينة أو يدافعون عن إيديولوجيا معينة.

2 القراصنة hakers: وهم الدين يهاجمون مواقع الأنترنت لتعطيلها دون النية أو القدرة على إحداث دمار كبير فيها.

3 الإرهابيون cyber–terrorist:وهم أشخاص يحركهم دافع سياسي ،يهاجمون المواقع الإلكترونية وأنظمة معلومات البنية التحتية المرتبطة بالأنترنت بغية إحداث دمار كبير بشري أو مادي.

هناك تداخل بين مفهوم الإرهاب السيبراني وبين عدد من المفاهيم الأخرى سنتعرض لها بإيجاز وهي([4]):

الصراع الإلكتروني:

[1] العدوان ،***مرجع سابق*** ، ص 8.
[2] العدوان ،***مرجع سابق*** ، ص 8.
[3] Arquilla.J., Ronfeldt .D ,***networks and netwars*** , (rand.santa monica. 2001). p56.
[4] ريهام عبدالرحمن رشاد العباسى، "أثر الارهاب الالكترونى على تغير مفهوم القوة فى العلاقات الدولية دراسة حالة: تنظيم "الدولة الاسلامية""،(المركز الديمقراطى العربى ،2016)، في :***http://democraticac.de/?p=34528*** (29 /4/ 2017).

للصراع الإلكتروني أدوات وأشكال جديدة فى عصر الثورة المعلوماتية ومثل الفضاء الإلكتروني ساحة لنقل الصراعات من خلاله أو إستخدامه كوسيلة من وسائل الصراع، وبالتالى فالصراع الإلكتروني هو الذى يمكن أن ينشب فى بيئة الفضاء الإلكتروني ويمتد الصراع عبر الفضاء الإلكتروني إلى شتى المجالات، ويتجاوز الصراع الإلكتروني الحدود التقليدية وسيادة الدول وذلك يؤثر على إمتداد الصراع ونطاقه ومن ثم تفاقم تداعياته وآثاره.([1])

الجريمة الإلكترونية:

تشير إلى نشاط غير شرعي من قبل أطراف معينة ويتم إرتكابها عن طريق الشبكات الإلكترونية العالمية، أي أنها جريمة ترتكب فى بيئة الفضاء الإلكتروني (النت– شبكات الكمبيوتر)، وقد تكون الجريمة بمعنى سرقة البرمجيات أو أن يخضع الكمبيوتر للجريمة أو أن يكون الكمبيوتر هو أداة الجريمة([2]).

حرب المعلومات: وتنقسم إلى نمطين: نمط هجومى ونمط دفاعى.

الهجومى: تقوم به الدولة وأجهزتها المختلفة نظراً لإمتلاكها إمكانيات ضخمة تؤهلها للقيام بذلك وتستخدم لأهداف سياسية أو عسكرية أو الردع بمعنى إظهار الدولة لقدراتها على القيام بذلك وتقوم بتعطيل نظم المعلومات والتجسس وسرقة البرامج الحاسوبية.([3])

الدفاعية: الحد والوقاية من أعمال التخريب التى تتعرض لها وتختلف وسائل الدفاع باختلاف أنواع التخريب وطبيعة الأضرار التى تتسبب فيها، وتستخدم لأسباب إستراتيجية لتحقيق أهداف قومية .

يمكن تبني تعريف الإرهاب الإلكتروني الدي جاء به محمد بن عبد العزيز العقيل بأنَّه:

(نع ًا تمسن خك بً آه جلئعب آه آغفخ ّ زنيي قئم ة آه عكي ِب ع مضنيف ىئزةخجل
لكهزئكىألقةنمي ب لئقك آهكةخني ا آهىألغزئخ اآى شمبٌّ لم شمن آهىك ةيخ ِخ اسى؟ لم كق صخ
لكزكن بلكسنعي ِب) ([4]).

---

[1] رشاد العباسى ، ***مرجع سابق***. (موقع إلكتروني).
[2] لمزيد من المعلومات حول الجريمة الإلكترونية أنظر : محروس نصار غايب ،***الجريمة المعلوماتية*** ،(العراق ،المعهد التقني الأنبار، 2011)، في: ***http://www.iasj.net/iasj?func=fulltext&aId=28397***.(27 /4/ 2017).
[3] رشاد العباسي ،***المرجع نفسه***. (موقع إلكتروني).
[4] محمد بن عبد العزيز العقيل ، ***التحريض الإلكتروني على الإرهاب تكييفه الفقهي وحكمه (تويتر نمونجًا)***،(الرياض:جامعة الإمام محمد بن سعود الإسلامية ، 2014)،ص14.

من جهة أخرى يعرفه الدكتورهشام بشير بأنه (العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول أو الجماعات أو الأفراد على الإنسان في دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق، باستخدام الموارد المعلوماتية والوسائل الإلكترونية بشتى صنوف العدوان وصور الإفساد).([1])

وهو كذلك (هجمات غير مشروعة أو تهديدات بهجمات ضد الحواسيب أو الشبكات أو المعلومات المخزنة إلكترونياً، توجه من أجل الإنتقام أو إبتزاز أو إجبار أو التأثير في الحكومات أو الشعوب أو المجتمع الدولي بأسره لتحقيق أهداف سياسية أو دينية أو إجتماعية معينة، وبالتالي فلكي ينعت شخص ما بأنه إرهابي على الإنترنت، وليس مخترقاً فقط، فلابد أن تؤدي الهجمات التي يشنها إلى عنف ضد الأشخاص أو الممتلكات، أو على الأقل تحدث أذى كافياً من أجل نشر الخوف والرعب). فالإرهاب الإلكتروني يعتمد على استخدام الإمكانات العلمية والتقنية، واستغلال وسائل الاتصال والشبكات المعلوماتية من أجل تخويف وترويع الآخرين وإلحاق الضرر بهم أو تهديدهم.([2])

ويعرفه الكاتب cedric thevenet بأنه "إستخدام أو إستهداف الحواسيب وأجهزة الإتصال السلكية واللاسلكية تحت تأثير دوافع دينية أو سياسية بهدف ممارسة العنف ضد المدنيين من أجل التأثير على الرأي العام والحكومة ".([3])

المطلب الثاني : خصائص الإرهاب السيبراني وأشكاله :

1 خصائص الإرهاب السيبراني:

تتلخص خصائص الإرهاب السيبراني في النقاط التالية([4]):

1 **من حيث الإثبات:** تتميز جرائم الإرهاب السيبراني بأنها صعبة الإثبات، وتعتبر هذه الخاصية من أهم الخصائص المميزة لهذه الجرائم عن غيرها من الجرائم، وخصوصاً تلك التقليدية.

---

1 محمد قاياتي ،" إرهاب المستقبل"، في:
http://www.anntv.tv/new/showsubject.aspx?id=96994 (2017/4/4).

[2] د هشام بشير ،"الإرهاب الإلكتروني في ضل ثورة المعلومات" ، ***مجلة آراء حول الخليج*** ،(العدد 118 ، 2014)،ص11.

[3] Cedric Thevenet ,***cyberterorrisme , mythe ou realite ?,*** (universite de marne la vallee ,2005),p.6.

[4]" الإرهاب الإلكتروني جولة في عقل متطرف***"، جريدة العرب*** ، (عدد 9561، 2014/5/17)، ص18.

2 **من حيث الجناة:** إن مستخدمي هذا النوع من الإرهاب يمتازون بخلفيات وخبرات في إستخدام الأجهزة والتقنيات الحديثة هذا من جهة، ومن جهة أخرى نجد نقصاً كبيراً في الخبرات لدى الجهات الأمنية المسؤولة عن كشف المخططات الإرهابية الرقمية.

3 **من حيث أداة ارتكاب الجريمة:**يتم إرتكاب هذه الجرائم عن طريق أجهزة الإعلام الألي ،الموصولة بالأنترنت .

4 **بيئة هادئة:** إن الإرهاب السيبراني يحدث في بيئة هادئة لا يستخدم القوة والعنف وإستعمال الأسلحة، وإنما كل ما يحتاج إليه هو جهاز إعلام ألي ، وبعض البرامج وشبكة إنترنت، ولذلك يطلق على جرائم الإرهاب السيبراني الجرائم الناعمة إلا أن الإرهاب الإلكتروني قد يؤدي وبطريقة غير مباشرة إلى قتل ودمار إذا ما تم التلاعب وتحريف نظم الحاسب في الصناعات الغذائية مثلاً أو الطيران... إلخ([1]).

5 **من حيث مدى التعاون بين الجناة:** بصفة عامة فإن هذه الجرائم – التي تعد من جرائم التكنولوجيا الحديثة– تتميز بأن مرتكبيها قد يحدث بينهم تعاون على إرتكابها إضراراً بالجهة المجني عليها، وغالباً ما يكون فيها متخصص في الحاسبات يقوم بالجانب الفني من المشروع الإجرامي، وشخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب إليه ([2]).

2 أشكال الإرهاب السيبراني :

يتخذ الإرهاب السيبراني أشكالاً وطرقاً عدة إعتماداً على الجناة وعلى أهدافهم، فالإرهاب **السيبراني** لا يستهدف البيئة السبرانية فحسب، وإنما البيئة المادية التي تدعم العمليات السيبرانية، وقد تكون أسلحة الإرهاب **السيبراني** وهجماته أسلحةً من إنتاج الحاسب، أو تعتمد على تعديات تقليدية من خلال تطبيق تفجير سيارة عن بعد، هجوم بالغاز السام، حيث تتوقف خدمات أخرى في البناء التحتي الحساس، مثل برج المراقبة في المطار، ويمكن إستخدام الأسلحة التقليدية في تدمير نظم المعلومات الوطنية.

[1] هشام بشير ،"الإرهاب الإلكتروني في ضل ثورة المعلوملت "،في :
http://www.araa.ae/index.php?view=article&id=244:2014-06-13-16-21-31&Itemid=294&option=com_content،(2017/3/23).

[2] **المكان نفسه.**

وفي الحقيقة من الصعب تحديد أشكال الإرهاب السيبراني؛ فطبيعة الإرهاب **السيبراني** تتطلب اللامحدودية في التصنيف، نظراً لأنها تستخدم تكنولوجيا تتطور يوماً بعد آخر، لكن الأشكال التالية يمكن أن تصنف على أنها أشكال وأنواع الإرهاب **السيبراني** كالآتي:

1. **التهديد الإلكتروني** :تعددت الأساليب الإرهابية في التهديد عبر الأنترنت من التهديد بالقتل لشخصيات سياسية إلى التهديد بتفجيرات في مراكز سياسية أو تجمعات رياضية، ثم التهديد بإطلاق فيروسات لإتلاف الأنظمة المعلوماتية في العالم، ومن أمثلة التهديد الإلكتروني ما قام به شاب أمريكي يدعى (جاهابر جويل) البالغ 18 عاماً، حيث هدد كلاً من مدير شركة (مايكروسوفت) والمدير التنفيذي لشركة (M.P.I)بنسف شركتيهما إذا لم يتم دفع خمسة ملايين دولار، وقد قامت الشركة بتفتيش منزل المذكور بعد القبض عليه، وعثروا في حاسبه الآلي على ملفات رقمية عدة تحتوي على معلومات عن تصنيع القنابل تم إنزالها عبر الإنترنت.([1])

2. **القصف الإلكتروني([2])**: وهو أسلوب للهجوم على شبكة المعلومات عن طريق توجيه مئات الآلاف من الرسائل الإلكترونية إلى مواقع هذه الشبكات، ما يزيد الضغط على قدرتها على إستقبال رسائل من المتعاملين معها، والذي يؤدي إلى وقف عمل الشركة.

3. **تدمير أنظمة المعلومات:** هو زرع مجموعة من الفيروسات داخل أنظمة المعلومات بغرض تعطيلها أو إلحاق أضرار كبيرة بمحتوياتها ([3]).

4. **التجسس الإلكتروني([4])**: التجسس هو محاولة الوصول إلى معلومات محمية لا يمكن الإطلاع عليها ومن تم كسب نوع من المعلومات تمكن المتجسس من تبني إستراتيجيات أخرى .

وإجمالاً، فبالرغم من كون الفضاء السيبراني له إستخداماته السلمية ، إلا أنه ظهرت إستخدامات أخرى غير سلمية لهذا الفضاء المتشعب الإتجاهات بإستغلاله كساحة جديدة للصراعات الدولية، بحيث شكلت هذه الصراعات ما يسمى ظاهرة الإرهاب السيبراني، والتي نشأت في الأساس من التزاوج بين تكنولوجيا الإتصال

---

[1] د حسن علي محمد ،" الإعلام والإرهاب .. الإشكاليات والتحديات" ،في:
http://www.arabmediasociety.com/?article=933 (18 /4/ 2017).

[2] علي محمد، **مرجع سابق.** (موقع إلكتروني).

[3] خالد وليد محمود،"الهجمات عبر الانترنت :ساحة الصراع الإلكتروني الجديدة"، ***المركز العربي للأبحاث ودراسة السياسات***، 2013 .ص ص 4-37.

[4] **المكان نفسه.**

والمعلومات من جهة، والإرهاب من جهة ثانية، ما أفرز قضايا معقدة وتحديات مختلفة أمام جميع الفاعلين من الدول والجماعات والأفراد.

وهنا يجب التأكيد على أهمية دور وسائل الإعلام في بلورة إستراتيجيات للتصدي لمزاعم الإرهابيين، وتشجيع وسائل الإعلام على وضع قواعد إرشادية للتقارير الإعلامية والصحفية بما يحول دون إستفادة الإرهابيين منها في الإتصال أو التجنيد أو غير ذلك، إضافة إلى أهمية تشجيع البحوث والدراسات، وعقد المؤتمرات والندوات وورش العمل وحلقات النقاش في مجالات ظواهر الغلو والتطرف والإرهاب بصفة عامة والإرهاب الإلكتروني بصفة خاصة، والتعرف إلى مصادرها ومناهجها وأسبابها ودوافعها ومخاطرها، ووضع الحلول الفعالة لمواجهتها والحد من إنتشارها([1]).

المطلب الثالث :أدوات الإرهاب السيبراني وآلياته.

يتم توظيف الفضاء السيبراني فى الإرهاب بصورة غير مباشرة عن طريق تسهيل عملية تنفيذ العمل الإرهابي من خلال توفير المعلومات والحصول على التمويل ، وكذلك يتم إستخدامه لنشر الخوف والفزع والرعب وبث الكراهية، أو عن طريق إستخدام أدوات ذات طابع إلكتروني فى الصراع وسوف نتعرض تفصيلا لهذه الأليات كما دكرتهاالباحثة ريهام رشاد العباسي ([2]):

إختراق المواقع الإلكترونية:يتم إختراق المواقع الإلكترونية لتغيير محتوياتها أو سرقة معلومات سرية أو تعطيل الموقع عن العمل والسيطرة عليه بشكل كامل، وبعد نجاح إختراق الموقع يضع المهاجمون رسائل فى الموقع تعلن إختراقه وكأنه بمثابة رفع راية النصر .

الفيروسات : هي عبارة عن برامج تعمل وفق نظام معين وتستنسخ نفسها في الجهاز وتتكاثر وعندما تنشط هذه الفيروسات تحدث تغييرات في البرامج أو في البيئة التى تعمل فيها ولها أضرار مختلفة تتمثل فى فقد الملفات المخزنة وقد تصل تلك الأضرار إلى تحطم نظام التشغيل فى الجهاز.فيروسات الإعلام الألي تنتشر بسرعة كبيره عن طريق شبكة الأنترنت وذلك يرجع إلى عدد الملفات الهائل التى يتم تبادلها بين مستخدمي الشبكة العنكبوتية، وهذه الفيروسات([3]) .

[1] بشير ،**مرجع سابق** ،(موقع إلكتروني).
[2] رشاد العباسى، ***مرجع سابق.*** (موقع إلكتروني)
[3] Pour plus d'informations voir :" Sécurité informatique: connaître les dangers" ,sur ***:*** ***http://briand-lyc.spip.ac-rouen.fr/IMG/pdf/b2i_securite_1.pdf,***(12/l5/2017).

أحصنة طروادة: عبارة عن شفرة أو برنامج صغير مختبئ فى برنامج أكبر، هذه الأحصنة تؤدى مهام خفية فعلى سبيل المثال تكون مهمتها إطلاق فيروس أو دودة، وتقوم بإرسال البيانات عن الثغرات الموجودة في النظام، وإرسال كلمات المرور السرية الخاصة بالهدف.

القنابل المنطقية: نوع من أحصنة طروادة يزرعها المبرمج داخل النظام الذى يطوره أو أن تكون برنامج مستقل، وتستخدمه الدول فى شن حروب إلكترونية والتجسس على الدول المعادية لها.

الأبواب الخلفية: ثغرة تترك عن عمد من مصمم النظام للتسلل إليه عند الحاجه، والجدير بالذكر أن الكثير من البرامج والنظم التى تتطورها الولايات المتحدة الأمريكية تحتوى على أبواب خلفية تستخدمها عند الحاجة مما يسمح لها بالتجول الحر داخل نظام أي دولة أجنبية.

الاختناق المرورى الإلكتروني: سد وخنق قنوات الإتصالات لدى المستهدف بحيث لا يمكنه تبادل المعلومات، أو إستبدال المعلومات وهي في الطريق بين المرسل والمستقبل بمعلومات مضللة. ([1])

الهاكرز: أفراد عاديين لديهم قدرات ومهارات عالية في إستخدام الكمبيوتر لتحقيق أهدافهم أياً كانت سياسية أو غيره ويرغبوا فى إثبات قدرتهم وبالتالي يتم ذلك بطرق غير شرعية.

الحرب الإعلامية:الفضاء الإلكتروني له تأثير هائل على الرأى العام العالمى لأنه يخاطب ملايين المستخدمين للشبكة العنكبوتية من شتى أنحاء العالم بوسائل مختلفة" الصوت– الصورة– النص"، وبالتالى أي جماعة أو منظمة يمكن لها إنشاء مواقع إلكترونية تروج أفكارها وتنشرها فى مختلف أنحاء العالم. ([2])

التجسس الإلكترونى: لقد نجحت العديد من الحكومات فى إستخدام تقنيات متطورة للتجسس من خلال الشبكة العنكبوتية على الدول أو المنظمات ومراقبة المعلومات التى يتم تداولها حول العالم ([3]).

التهديد الإلكتروني: يوجد العديد من الأساليب التى تستخدم في التهديد عبر الشبكة العنكبوتية، وتتنوع تلك الأساليب بين تهديدات بإغتيال شخصيات سياسية، تهديدات بتفجيرات في مراكز سياسية أو هيئات حكومية، أو التهديد باطلاق الفيروسات التي من شأنها تدمير أنظمة معلومات بالكامل.

---

[1] رشاد العباسى، ***مرجع سابق*** .(موقع إلكتروني).

[2] Pour plus d information voir : François-Bernard Huyghe ," Qu'est-ce que la guerre de l'information ?",sur : ***http://www.huyghe.fr/dyndoc_actu/4451ebfb7de54.pdf,***(23/2/2017).

[3]حسن بن أمحد الشهري ،"الإنظمة الإلكترونية الرقمية المتطورة لحفظ وحماية سرية المعلومات من التجسس"، **المجلة العربية للدراسات الأمنية والتدريب**، (العدد 56)، ص 4،5.

القصف الالكترونى: يشير إلى الهجوم على شبكة المعلومات عن طريق توجيه مئات الآلاف من الرسائل الإلكترونية إلى مواقع هذه الشبكات، وبالتالى تسبب ضغط كبير على هذه المواقع، وتفقدها قدرتها على إستقبال الرسائل من العملاء، ويؤدى ذلك إلى التوقف عن العمل تماماً.

خلاصة الفصل الأول:

إن إشكالية تحديد مفهوم الإرهاب والمفاهيم المرتبطة به وعدم الإجماع الدولي حول دلك جعل من عملية حصر أعمال العنف المرتبطة بممارسات الأفراد والدول ووصفها بالإرهاب من عدمه يخضع إلى معايير شخصية تتغير بتغير الزمان والمكان ،بحيث أصبحت عملية تكييف الفعل الإرهابي تخضع لرأي ورغبة القوي ولما كانت الولايات المتحدة هي القائد الحالي للنظام الدولي بمشاركة بعض الدول الغربية فقد طغت نظرتها للإرهاب على جميع المساعي الدولية لتعريف وتفسير هده الظاهرة والظواهر المرتبطة بها.

إن الجزم بأنه لا يوجد تعريف للإرهاب الدولي فيه نوع من المبالغة . فالواقع، كما تبيَّن لنا، أن ثمة تعريفات مختلفة للإرهاب الدولي وأن الإتفاقيات الدولية أوردت تعريفًا للإرهاب الدولي مرتبطًا بالحالات التي تصفها كأعمال محظورة ومخالفة للقانون. والأمر داته بالنسبة للإتفاقيات أو الأعراف الدولية المتعلقة بالإرهاب الدولي بدءًا من القرصنة البحرية وصولاً إلى الإرهاب السيبراني .

ومع أن بعض القرارات الدولية قامت بتعريف للإرهاب الدولي إستنادا إلى أحكام الفصل السابع من ميثاق الأمم المتحدة، إلا أنها أغفلت أمرا أساسي وهو التمييز بين الإرهاب الدولي والمقاومة الوطنية.

ولما كانت المقاومة الوطنية من أجل تقرير المصير أو من أجل رفع الاحتلال مشروعة في القانون الدولي فإن دلك يحتم ظرورة صياغة نصوص قانونية تستثنيها من مفهوم الإرهاب الدولي.

وبظهور التكنولوجيات الحديثة وتعميم إستخدامها برزت أشكال جديدة من الإرهاب ،تصدرها الإرهاب السيبراني وبرزت مخاطره على جميع النواحي الإجتماعية والثقافية والسياسية والتقنية،وتحلى بخصائص عديدة وتبلور وفق أشكال عدة وإستعان بوسائل تقنية عديدة ،ليشكل بدلك جنبا إلى جنب مع الإرهاب التقليدي إحدى الهواجس الكبيرة والتحديات العصيبة أمام الأمن الدولي .

إن تفشي توظيف الإرهاب السيبراني في التفاعلات الدولية تمخض عنه العديد من التداعيات على الأمن الدولي بحيث أصبح أكبر هاجس أمام المجتمع الدولي وأفرز العديد من المظاهر بحيث ولد الإرهاب السيبراني صراعا دوليا أخد طابع الحرب الباردة في بعض الأحيان وإشتدت حدته في أحيان أخرى .

وسنحاول في هدا الفصل إبراز أهم الأخطار والتداعيات التي جلبها توظيف الدول والتنظيمات الإرهابية للفضاء السيبراني وخطورة دلك على الأمن الدولي ، بحيث أصبح تهديد الإرهاب السيبراني أكبر من أي تهديد عرفه النظام الدولي الحالي ويفوق حتى خطر أسلحة الدمار الشامل ، على إعتبار أن هده الأخيرة يمكن تفعيلها عن طريق هدا النوع من الإرهاب الدي يصعب معرفة مصدره وكدا الدوافع الكامنة وراءه.

لدلك قسمنا هدا الفصل إلى ثلاث مباحث ،نتطرق **في** المبحث الأول الى **مظاهر تهديد الإرهاب السيبراني للأمن الدولي** وفي المبحث الثاني **ندكر الإرهاب السيبراني كشكل جديد من أشكال الصراع الدولي** أما المبحث الثالث **فنستعرض فيه طبيعة و أنماط توظيف الفضاء السيبراني في الصراع الدولي.**

المبحث الأول :مظاهر تهديد الإرهاب السيبراني للأمن الدولي.

في هذا المبحث يتم تناول مظاهر تهديد الإرهاب السيبراني لأمن المجتمع الدولي و يتم ذلك من خلال التعرض لملامح التأثير و التفاعل المتبادل بين تلك الظاهرة و البنية التحتية الكونية للمعلومات و كيف مثل الفضاء السيبراني ساحة جديدة للصراع الدولي و ظهور نمط جديد من الإرهاب عن طريق التزاوج ما بين التكنولوجيا و الإرهاب و يتم التعرض لذلك من خلال أولا: **الإنكشاف الأمني للدولة نتيجة الإعتماد المتزايد على الفضاء السيبراني** ، و ثانيا **توظيف الفضاء السيبراني كساحة للصراع و التنافس الدولي،** و نتناول ثالثا **توظيف الإرهاب الجديد للتكنولوجيات الحديثة.**

المطلب الأول: الإنكشاف الأمني للدولة نتيجة الإعتماد المتزايد على الفضاء السيبراني

زادت حالة الإنكشاف الأمني للدول و ذلك بإعتمادها المتزايد على الفضاء السيبراني ودلك بعد أن تبنت العديد من دول برامج تعتمد عل أليات إلكترونية كبرنامج الحكومات الإلكترونية و التي تصبح عرضة للاختراق و الهجوم بالفيروسات و سرقة المعلومات أو إتلافها و بالتالي تهديد للأمن الوطني ، و من ثم

إختلف مفهوم الأمن بتحوله إلى نوع جديد يعتمد على الشبكات و الأنترنت ، و دفع ذلك لبروز الخوف من دور الجماعات الإرهابية في التأثير على الفضاء السيبراني،وتوظيفها للتكنلوجيات الحديثة في زعزعة الأمن والإستقرار الدوليين.

على الرغم مما وفره هدا الفضاء من إمكانية تواصل الفرد مع الأخريين وتجاوز مسألة المسافات إلا أنها زادت في الوقت نفسه من عزلة الفرد داخل مجتمعه سعيا وراء عالمه الخاص الذي يتلاءم مع ميوله و إتجاهاته التي قد لا تتفق مع ما يحيط به مما ولد أفكار جديدة غلب عليه طابع العنف ،هذا ما قد يعمل على الإصطدام بين ما يريده الفرد و ما يريده المجتمع و يفرضه من قيود، كما عمل الفضاء السيبراني على الكشف المستمر عن مطالب و إحتياجات المواطنين و التي تكون بشكل يفوق قدرة النظم السياسية على تلبيتها مما قد يبدو على أنه عجز و فشل تلك النظم في تلبية مطالب شعوبها، الأمر الذي قد يدفع للشعور بالإحباط المولد للعنف، و قد شهدت أوروبا الغربية إبان تحولها ظهور العديد من الجماعات الإرهابية و التي ما لبثت أن تلاشت بعد مرحلة الإنفتاح السياسي و الاقتصادي الذي إستطاع أن يمتص تلك الجماعات و ساعدت على دعم الإستقرار السياسي بها، و تمخض عن الثورة التكنولوجية ثورة أخرى هي الثورة في الشؤون العسكرية و تطور تقنيات الحرب بشكل أصبحت أداة من أدوات حروب المستقبل[1].

و أصبحت الدولة تمتلك التقنية و تستخدم العمليات المعلوماتية كسلاح ردع و تسيطر على أنظمة المعلومات العالمية ، و جاء ذلك مع ضعف السيطرة على إنتشار المعلومات ، حيث يزداد القلق لدى الدول المتقدمة من تعرضها لعمليات تخريب لبنيتها التحتية للمعلومات.[2]

و على المستوى المدني نجد قابلية البنية الأساسية التي تعتمد في عملها على الشبكات و تكنولوجيا الإتصال و المعلومات للتعرض لهذا الخطر، و التي تتراوح ما بين الإتصالات إلى خدمات الطوارئ و من الصفقات المالية إلى العمليات العسكرية و الخدمات الحكومية و خاصة مع إندماج الخدمات وترابطها حيث أصبحت التحويلات المالية تتم عبر الهاتف المحمول و خدمة الأنترنت و تقديم الخدمات التكنولوجية و التجارة الإلكترونية و هذا ما قد يتسبب في حالة إي عطب قد يصيب الكابلات البحرية في أحداث خسائر إقتصادية ضخمة.

---

[1] Jennie M. Williamson, ***Information Operations: Computer Network Attack in the 21st Century***, (Carlisle Barracks, PA, U.S. Army War College,2002), pp 15- 22.

[2] T. G. Lewis, ***Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation***.(NJ: Hoboken, , Wiley-Interscience,2006), pp 230- 274 .

و تصبح البنية التحتية الكونية للمعلومات التي تعتمد على أنظمة الكمبيوتر معرضة لأخطار عدة تصيب القدرة على الحفاظ على الوصول و السرية و السلامة، إما عن طريق تدمير المعلومات أو البرامج أو الأدوات المادية، أو عن طريق التدخل في نظام الكمبيوتر لدرجة أن يصبح النظام مشكوكا فيه و عديم الفائدة، أو عن طريق التدخل في ذاكرة النظام أو المعلومات.

و يتم توظيف الهجمات بشكل بسيط و رخيص و بشكل متسع في مجال التأثر ، كما أن عملية إحتوائه تكون صعبة التحديد، ، و إتخذت تلك الحروب أشكالا جمعت بين الضربات الإستباقية التي تهدف لمواجهة تهديد محتمل ، و الحروب بالوساطة ، و الحروب "السرية" ، إضافة إلى هجمات "الهاكرز" المنسقة والمعارك التي لاتهدأ بين شركات برامج حماية الكومبيوتر وصناع الفيروسات المعلوماتية من الجهة الأخرى.[1]

وحدث دمج بين الفضاء السيبراني مع التكتيك المستخدم في الصراع ليصبح الإرهاب السيبراني يتم عبر صراع إلكتروني بين القيادات الصديقة و القيادات المعادية بهدف التأثير على قدرات الخصم و إختراق كيانه الإلكتروني و إستخدام المعلومات كسلاح رئيسي و حاسم لمهاجمة جهاز المعلومات المعادي و إفشاله في إطار حرب المعلومات .[2]

و إذا كان الكثير من الدول تستطيع خوض حروب حقيقية و الإنتصار فيها، فإن الفوز في الحروب الإلكترونية عبر الفضاء السيبراني صعبة بسبب عدم معرفة ماذا سيحدث ، و من أين و متى و كيف و ما هو حجم "الجيش" الذي ستواجهه الدول و ما هي طبيعة التداعيات التي قد تسفر عن المواجهة و كيف يمكن تحجيمها ، و ما هو مقدار تكرار الهجمات بما يعكس وجود فوضى أمنية داخل الفضاء السيبراني ، و بما ينعكس على أمد الصراع خاصة مع سهولة عمليات الإتصال و التخطيط و تسيير العمليات بشكل دقيق و ضعف مراقبة سير المعلومات الهائل الذي يسير بشكل يومي عبر الفضاء السيبراني ، كما أنه بالإمكان إخفاء المعلومات وراء غطاء بريء ([3]).

---

[1] Bonnie N. Adkins, ***The Spectrum of Cyber Conflict from Hacking to Information Warfare: What is Law Enforcement's Role?,*** (Alabama :Maxwell Air Force Base, April 2001) ,p 11

[2] Wang Baocun , Li Fei," Information Warfare",in : ***https://fas.org/irp/world/china/docs/iw_wang.ht***.(2017/3/4)***.***

[3] عادل عبد الصادق ،"الفضـــاء الإلكتروني وأسلحـــة الانتشـــار الشـــامـــل بين الردع وسباق التسلح" ، في**:** ***https://seconf.wordpress.com***، (13 /4/ 2017).

وتختلف هجمات الفضاء السيبراني عن شكل النزاع التقليدي فقد تقوم القوات الخاصة لأي دولة بشن هجمات بإستخدام الأسلحة الإلكترونية في مهاجمة البنية التحتية السيبرانية لدولة أخرى بالشكل الدي يحدث دمارا غير متوقع . [1]

و يزداد حجم الإنكشاف الأمني بتزايد حجم اللتحديات التي تواجه الفضاء السيبراني لعل أهمها ما يلي:

- تحديات زيادة الإستخدام والإنتشار:

- خطر الكوارث الطبيعية أو العرضية للكابلات البحرية.[2]

- القراصنة وتهديد أمن الشبكة الدولية.

- خطر التعرض للحرب الإلكترونية في الفضاء السيبراني أوالتعرض لهجمات إرهابية.

المطلب الثاني : توظيف الفضاءالسيبراني في الصراح والتنافس الدولي:

يعد الصراع في الفضاء السيبراني نموذجا آخر ذا طابع رقمي يعكس النزاعات التقليدية التي تخوضها الدول أو الحركات الراديكالية على خلفيات دينية أو عرقية أو إيديولوجية. ولأن الصراعات "الفعلية " تستعمل شتى أنواع أسلحة التدمير الإقتصادية والإلكترونية والسياسية والإعلامية، فإنها لم تتوان عن إسخدام الفضاء الإلكتروني، بما له من تأثير نفسي ومعنوي وإعلامي، وشيئا فشيئا، زحفت جبهات القتال التقليدية لتصنع مجالا موازيا لها في الفضاء السيبراني.[3]

وما الصراع الإلكتروني إلا صراع تحركه دوافع سياسية ويتم فيه إستخدام قدرات هجومية ودفاعية عبر الفضاء الإلكتروني وذلك بهدف إفساد النظم المعلوماتية والشبكات والبنية التحتية وبما يتضمن إستخدام أسلحة وأدوات إلكترونية من قبل فاعلين داخل المجتمع المعلوماتي أو من خلال التعاون ما بين قوى أخرى لتحقيق أهداف سياسية، وهناك صراع إلكتروني بوجه آخر مرن عن طريق الصراع حول الحصول على

[1] Mark R. Shulman," Discrimination in the Laws of Information Warfare",School of Law Faculty Publications,(Pace University,Columbia Journal of transnational Law ,1999),p 937 . in : ***http://digitalcommons.pace.edu/lawfaculty/224***.(2017/4/3)**.**

[2] عادل عبد الصادق، "من قطع كابلات الأنترنت عن الشرق الأوسط" ،ملف الأهرام الإستراتيجي، مركز الدراسات السياسية والإستراتيجية ، ***جريدة الاهرام*** ،(العدد 160 أفريل 2008)،ص 45،46.

[3] عادل عبد الصادق " هل يمثل الإرهاب الإلكتروني شكلا جديدا من أشكال الصراع الدولي" ملف الأهرام الإستراتيجي، مركز الدراسات السياسية والإسترتيجية ،***جريدة الأهرام*** ،(العدد 156، ديسمبر 2007)،ص 21.

المعلومات والتأثير في المشاعر والأفكار وشن حرب نفسية وإعلامية. ويعد الصراع الإلكتروني إنعكاس للصراعات التي تدور على أرض الواقع وتكشف عن طبيعة الفاعلين وأنماط هذا الصراع، ويعد الصراع حالة سببها تعارض حقيقي أو متخيل للإحتياجات والقيم والمصالح. [1]

والصراع الإلكتروني هو ذلك الصراع الذي يمكن أن ينشب في بيئة يكون وسيطها الفضاء السيبراني حيث يشهد حركة التفاعلات بين مختلف الصراعات والتي قد تنشب من كل أنواع البيئات الأخرى غير المتصلة بالفضاء السيبراني وإنما تؤثر فيه كالنزاعات بين الأفراد والصراع ذو الطابع القانوني والتجاري أو الصناعي ويمتد ليشمل كافة مجالات الحياة، وهناك صراع يأخذ طابعا تنافسيا حول الإستحواذ على سبق التقدم التكنولوجي وسرقة الأسرار الإقتصادية والعلمية إلى أن يمتد ذلك الصراع إلى محاولة السيطرة على الإنترنت من خلال السعي للسيطرة على أسماء النطاقات وعناوين المواقع، والتنافس للسيطرة على سوق إستضافة المواقع عبر الخوادم التقنية والتوجه أحيانا للتحكم بالمعلومات وطرق تبادلها عبر التحكم بالحلول التقنية وإحتكارها لتكون وسيلة التحكم بمصادر المستخدمين وأداة السيطرة الفعلية، وذلك مع غياب المركزية وغياب السلطة التحكمية التي تنظم عمل هذا المجال الحيوي والذي يتعرض لإعتداء عسكري أو إرهابي بدون إستخدام طائرات أو متفجرات أو حتى إنتهاك للحدود السيادية بل سيكون هجوما في الفضاء السيبراني يشنه قراصنة الكمبيوتر وتدمير المواقع والتجسس وإقامة مراكز لمواقع إرهابية، والقدرة على تدمير الإقتصاد والبنية التحتية بنفس القوة التي قد يسببها تفجير تقليدي مدمر. [2].

تاريخيا تطورت الهجمات السيبرانية من مجرد عمليات بسيطة، إلى عمليات جيدة التمويل والتنظيم من التجسس السياسي والعسكري والإقتصادي والتقني. وأصبح الفضاء السيبراني مجالا للصراع والتنافس ويستخدمه الفاعلون فيه من الدول أو من غير الدول للتعبئة والحشد والتنظيم والدعاية ويستخدمها أيضا المعارضة ضد النظم السياسية أو نشطاء الإرهاب أو الجريمة، وهناك صعوبة الفصل ما بين النشاط الذي يتعلق بالاستخبارات وجمع المعلومات وحرب الفضاء السيبراني والإستخدام السياسي له في الصراع، وخاصة مع ما يمثله من بيئة مثالية لعمل الجماعات المختلفة والقدرة على تشكيل شبكة عالمية بدون سيطرة مباشرة بالإضافة إلى رخص تكلفة وسهولة إتصال وضعف الرقابة التقليدية عليه، ومثلت تلك الخصائص عنصر

---

[1] Athina Karatzogianni,(ed), ***Cyber-Conflict and Global Politics***, (usa: Routledge and Taylor & Francis Group, 2009), p 59.

[2] انظر : خالد وليد محمود ،"الهجمات عبر الأنترنت ساحة الصراع الإلكتروني الجديدة" ،***مجلة سياسات عربية*** ،(العدد 5، 2013)،ص 6.

جذب هام لإستخدامها وتوظيفها لتحقيق الأهداف السياسية حيث أصبح الفضاء السيبراني ساحة لنقل الإختراعات وأشكالها وتتراوح من حرب الأفكار والأفكار المضادة إلى التوظيف العملي للصراع بما قد ينطوي عليه من عمل عنيف([1]).

تلعب البيئة المحلية والسياق الدولي للفضاء الإلكتروني دورا كبير في بروز الصراعات وفي دعم الهيكل التنظيمي والإتصالي داخل الجماعات كما أن لها دورا في عمليات التجنيد والحشد والتعبئة والتمويل ووضع التكتيكات، وتشكيل أولويات القضايا الإستراتيجية وتأثيرها على الهوية وعلى هيكل الفرص السياسية، وفي تفعيل دور النشطاء السياسيين، وظهرت صراعات إلكترونية ذات طابع ديني أو عرقي وكذلك الصراعات ذات الطابع العنصري والصراع الذي يظهر في شكل ظاهرة الإرهاب الإلكتروني.[(2)] وكان للفضاء السيبراني دورا في حل الصراعات والمصالحة، وأصبح وسيطا في الصراع عن طريق قدرته على بناء الهويات الإجتماعية والعلاقات الاجتماعية، والقدرة على التحكم في المعلومات والأحداث، بالإضافة لدور الفضاء الإلكتروني كوسيلة إعلام وتأثيرها على البعد الإستراتيجي والتكتيكي للصراع. ويمكن للصراع السيبراني أن يحدث داخل أو عبر كل جهاز عام أو خاص وتمدد داخل شبكات الإتصال والمعلومات متجاوزا الحدود التقليدية وسيادة الدول، ويؤثر ذلك في إمتداد مجال الصراع فيه وبما يؤثر على تفاهم تداعياته أو أثاره حيث يتم الإستخدام المتعدد للصراع من وجهة نظر الإقتصاد والسياسة والإجتماع أو الأمن أو الثقافة، فهناك الصراع ضد العولمة والحركات المعادية للرأسمالية حيث تتم المطالبة ببرنامج بديل للإصلاح.

و تصبح الدولة ضحية إذا ما تم مهاجمة نظم شبكاتها الإلكترونية وتأثر هذا الهجوم على المؤسسات المالية والمصرفية والتحكم في الطيران المدني والنظم المالية، بدون معرفة من ورائه وكيفية نجاحه وطرق تنفيذه و أطرافه الحقيقة ، مما يجعله قضية متشابكة و تأتي عملية الإستجابة للهجمات و عملية رد الفعل مع ضعف إجراءات الوقاية ضد التعرض لمثل تلك الهجمات ، و التي يمكن أن يتم شنها عبر الفضاء السيبراني و الشبكات ، أو من خلال إستخدام الهجوم العسكري التقليدي ، و للحصول على تأييد دولي للإجراءات الوقائية السلبية تكون هناك حاجة ملحة إلى تقديم الدليل وإثبات تورط طرف ما في مثل هذا الهجوم (و الذي يكون من الصعب التأكد بشأنه) بما يشكل ضمانه بوجود إجماع دولي للتعاون في المكافحة أو الحرب ضد طرف آخر أو فرض عقوبات دولية ما ، حيث تكون الدول معرضة لإنتهاك لسيادتها و أمنها الداخلي .

---

[1] أنظر : ربيع محمد يحيى ،"إسرائيل وخطوات الهيمنة على ساحة الفضاء السيبراني في الشرق الأوسط"،**مجلة رؤى إستراتيجية** ،(جويلية 2013)، ص ص 1-26.

[2] عادل عبد الصادق ،" هل يمثل الإرهاب الإلكتروني شكلا جديدا من أشكال الصراع الدولي"، ***مرجع سابق*** ،ص14.

و ما يكون له من إنعكاس على المستوى الدولي مع عولمة الشبكات و الأنترنت و إرتباطها بالإقتصاد العالمي قاطبة ([1])، من ثم فإن الدولة الضحية يتم إصابتها دون النظر إلى حدودها أو نطاقها الجغرافي بل و من الممكن أن يكون الهجوم من الداخل من قبل عملاء دولة ما أو عملاء مقيمين في دولة أخرى يقومون بشن هجمات من خلال نطاقها الجغرافي دون تورط تلك الدولة في دعم مباشر لها و ما يتعلق بإشكالية المسؤولية القانونية عن تلك الهجمات . و يواجه الفضاء الإلكتروني بتحديات تتعلق بدورة الإستراتيجي و الحيوي في النظام الدولي منها ما يتعلق بعوامل ذاتية و أخرى خارجية و أخرى ترتبط بالتفاعل ما بين البعد الخارجي و الطبيعة الذاتية له [(2)]

المطلب الثالث : هجمات الإرهاب السيبراني : حرب غير متماثلة و حرب غير تقليدية.

1- الفضاء السيبراني والحرب غير المتماثلة:

إن الحرب غير المتماثلة هي شكل غير تقليدي من الحرب حيث يستخدم الطرفان أسلحة غير متماثلة ويمتاز العدو بإرادة قوية وإصرار على تحقيق الأهداف.[(3)]

إعتمدت الحروب القديمة على تشكيلات عسكرية ذات تنظيم عمودي أو قد تشمل وحدات منشقة عن الجيش وزعماء ميلشيا ومرتزقة ومافيا إجرامية وإستخدام حتى جماعات إرهابية وهي ذات تنظيم لا مركزي تنشط بمزيج من المواجهة والتعاون بين وحدات الجيش المختلفة عبر وسائل الإتصال الحديثة.[(4)] وعملت الثورة التكنولوجية على إعادة التفكير في حركية وديناميكية الصراع. وظهر ما يعرف بـ "عصر القوة النسبية" على حد تعبير وليد عبد الحي التي يعني بها عجز القوة العسكرية عن تأمين الأهداف السياسية المترتبة عليها،خاصة بعد بروز قوى عالمية تعتمد على معطيات تكنولوجية إقتصادية مما يخلف آثارا إستراتيجية هائلة على مستوى تركيبة وتوازنات النظام الدولي، وتغير "براديم" الحرب جذريا بإنتقاله من نسق "الحروب الصناعية بين الدول" إلى نسق "الحرب في وسط الشعوب". ففي الحروب القديمة كان الغرض هو تدمير

---

[1] أنظر:هاشم بن محمد الزهراني،***الأثار الأمنية للعولمة*** ،رسالة ماجستير في علوم الشرطة ،(أكاديمية نايف العربية للعلوم الأمنية،الرياض ،2002)،ص ص68-72.

[2] عبد الصادق، " هل يمثل الإرهاب الإلكتروني شكلا جديدا من أشكال الصراع الدولي" ،**مرجع سابق** ،ص 15،16.

[3] محمد عبد السلام، "الحرب غير المتماثلة بين الولايات المتحدة والقاعدة"، ***مجلة السياسة الدولية***،(العدد 14 جانفي2002)،ص 102.

[4] Lawrence T. Greenberg, Seymour E. Goodman, Kevin J. Soo Hoo," Information Warfare and International Law",In : ***www.iwar.org.uk/law/resources/iwlaw/iwilindex.htm - 19k*** .(*2017/3/5*)***.***

الخصم، إما بإحتلال أرضه أو الإستيلاء على موارده، بينما أصبح في الحرب الجديدة هو التحكم في إرادته وخياراته، ومن ثم كان الدور المحوري للشعوب في هذا الصنف الجديد من الحروب، سواء تعلق الأمر بالسكان المستهدفين في أرضية المواجهة، أو بالرأي العام في البلد الذي يشن الحرب، أو بالرأي العام الإقليمي والدولي. فأهداف الحرب هنا أصبحت أقل مادية، يؤدي فيها العامل النفسي والدعائي دورا محوريا، وسببه تنامي التغطية الإخبارية السمعية البصرية المباشرة للأحداث لحظة وقوعها.

تسعى الجيوش النظامية بإستغلال تفوقها التقني العسكري الإعلامي الكاسح، لحسم حرب بأقل ثمن وفي اقصر وقت ممكن ، بينما تقوم إستراتيجية التنظيمات المسلحة المقاومة لها هي الإستخدام المعاكس لهذه الميزات التقنية، بالتسلل إلى وسط السكان و نهج سبيل حرب العصابات والإحتماء بهم وبالتالي تحويلهم إلى أرضية مواجهة ومن ثم توجيه سلاح الصورة إلى مآسي الحرب وجرائمها الإنسانية([1]).

2- التحول من الحرب التقليدية إلى غير التقليدية:

تتميز الحرب التقليدية بأنها تشكل تحديا عسكريا فقط في حين تمثل الحرب الغير تقليدية متعددة الأوجه ومتشابكة مع غيرها ومن ثم تكون تفاعلاتها كبيرة بخلاف الحرب التقليدية التي تكون تفاعلاتها محدودة، كما أن الحرب المعلوماتية تصبح متشابكة مع غيرها من الحرب الإعلامية وحرب الشبكات والإتصالات والحرب السياسية والسيكولوجية والحرب التكنولوجية والإرهاب.[(2)]

وفي دراسته بعنوان "تحديات الحرب غير التقليدية: نظرة للأمام ونظرة للخلف" قام "كيفين كولمان Kevin Coleman " [(3)] بتحديد 14 نوعا من الحروب غير التقليدية كان هناك ما لا يقل عن ستة أنواع ترتبط إرتباطا مباشرا بالإرهاب الإلكتروني وهي حرب المعلومات والحرب الإعلامية وحرب الشبكات والإتصالات والحرب السياسية والحرب السيكولوجية والحرب التكنولوجية وبالطبع الإرهاب، في حين يرتبط الإرهاب الإلكتروني بالأنواع الأخرى بطريقة غير مباشرة. وقام كولمان في دراسته عن "الحرب العالمية الثالثة: هل بدأت حرب الفضاء السيبراني" بتحديد خصائص الأسلحة الإلكترونية وأضرارها وعملية تطويرها وتنفيذها مع الإشارة إلى نموذج إستونيا وترسانة الأسلحة الإلكترونية، وقام كولمان في تلك الدراسة بتطبيق معايير كمية

[1] عادل عبد الصادق ،" الصراع الإلكتروني وتحولات الأمن العالمي" ، في *:* ***http://www.accronline.com/print_article.aspx?id=21782***(2017/3/4).

[2] Kevin Coleman ," The Challenge of Unrestricted Warfare - A Look Back and a Look Ahead",in : ***www.directionsmag.com***,(2017/4/3)

[3] ***Loc .cit.***

على هذا النوع الجديد من الصراع حيث ربط بين الإرهاب الإلكتروني والحرب الإلكترونية والحرب غير التقليدية، وأنها مرشحة للزيادة في غضون السنوات القادمة، وقد قام "كيفين كولمان" Kevin Coleman" بعمل مصفوفة عبر فيها عن تحليل كمي للخطر يتراوح من الدرجة (1) إلى الدرجة (5) من خطر منخفض إلى خطر مرتفع ومستندا على دراسة الدوافع والإمكانيات لكل خطر من أخطار الحرب غير التقليدية، وقام بتقسيمها إلى الخطر الحالي والخطر المتوقع في المدى القصير وفي المدى الطويل وتداعياتها في الوقت الحالي والمدى القصير والطويل وكذلك قام بقياس القدرة على الدفاع ضد تلك الأخطار ودرجة التغير في الخطر.[1] وأوضحت دراسة كولمان أن كل ما يرتبط بالخطر الحالي يتركز في الحرب الشبكية والإتصالات والحرب التكنولوجية والحرب على الإرهاب والحرب القذرة والمخدرات والجريمة المنظمة حيث وصلت إلى درجة عالية من التهديد (4) وكذلك الحرب المالية والإعلامية والمعلوماتية حيث وصلت إلى الدرجة (3).

أما عن التهديدات في الأجل القصير فحصلت تهديدات الحرب التكنولوجية والحرب على الإرهاب على أعلى درجة من الخطورة هي الدرجة (5) في حين تأتي أكبر إنعكاسات تلك التهديدات الخاصة بالمساعدة الإقتصادية والصراع المالي وحرب المعلوماتية ووسائل الإعلام وحرب الشبكات والإتصالات في الدرجة (4). أما في الجل الطويل فإن تهديدات الحرب الشبكية والإتصالات والحرب على الإرهاب والحرب التكنولوجية ستصل إلى ذروتها (5)، في حين تأتي أكبر انعكاسات تلك التهديدات من الإرهاب الإلكتروني والإتصالات في الوقت الحالي ويأتي بعد الحرب التكنولوجية والإرهاب، أما عن التداعيات في الأجل القصير فإنها ستصل إلى ذروتها في الحرب الشبكية و الإتصالات والإرهاب (5) ويأتي بعد الحرب التكنولوجية والمالية، أما في الأجل الطويل فتصل تلك التهديدات إلى ذروتها وهي خطر الإرهاب والحرب التكنولوجية والإرهاب الإلكتروني([2]).

[1] Kevin G. Coleman, ***The world war,A Cyber War has begun, Cyber Warfare***, in : ***http://www.technolytics.com/Technolytics_Cyber_War.pdf***,(2017/1/22).

[2] Fred Schreier, ***On Cyberwarfare***, (DCAF HORIZON WORKING PAPER No. 7,2017),p18 .

المبحث الثاني : الإرهاب السيبراني كشكل جديد من أشكال الصراع الدولي .

يتناول هذا المبحث مظاهر صراع جديدة و بأليات جديدة و فاعلين جدد و على درجة كبيرة من التنوع ما بين دور الحكومات و الدول إلى دور الإفراد و الجماعات الإرهابية كما يتم تناول في هذا المبحث نماذج من ذلك الإستخدام حيث يتم عرض نموذج لإستخدام الدول و نموذج أخر لإستخدام الجماعات و الأفراد و يتم عرض ذلك من خال تناول أولا، **توظيف أجهزة الاستخبارات الدولية للفضاء السيبراني** ، و ثانيا: **توظيف الجماعات الإرهابية للفضاء السيبراني** و ثالثا: **توظيف تنظيمي القاعدة وداعش للفضاء السيبراني.**

المطلب الأول: توظيف أجهزة الإستخبارات الدولية للفضاء السيبراني.

أخذ الإهتمام العالمي بالبعد الأمني لشبكة الأنترنت يتزايد بعد أحداث 11 سبتمبر 2001 و الحملة الأمريكية على الإرهاب و ما مثله ذلك من تحديات جديدة لأنظمة الحكم في العالم ، و كان نجاح تنظيم القاعدة في إستخدامه للأنترنت كاشفا من ناحية لقدرة الفاعلين من غير الدول سواء أكانوا جماعات أو أفراد على التحكم في المعطيات التكنولوجية و من ناحية أخرى فجر الطابع الإستخباراتي لشبكة الأنترنت الذي طالما حاولت الدول الكبرى إخفاءه حيث تمتلك الدول الفرص الأكبر في إستخدام الفضاء الإلكتروني بما تملكه من قدرات فنية و مالية مقارنة بالجماعات الإرهابية التي نجحت في إستخدامه هي الأخرى ، حيث تمتلك الدول أجهزة إستخباراتية قوية و خاصة الدول المتقدمة في تكنولوجيا الإتصال و المعلومات فضلا عن التقدم في مجالات التجسس بالأقمار الصناعية و الموجات و الإتصالات السلكية و اللاسلكية([1]).

تقدم الأنترنت سيلا هائلا من المعلومات المتدفقة حول دول العالم وهي تلك المعلومات التي لا تقتصر على وجهة النظر الرسمية بل تتعداها إلى دور الأفراد في إنتاج المعلومات و الترويج لها عبر الأنترنت و وجود كم هائل من التحليلات الصحافية و السياسية فضلا عن التقارير الإقتصادية و تعبير كافة التيارات السياسية و الفكرية و الدينية عن نفسها من خلال الأنترنت و وجود الخرائط الفضائية للأرض على الأنترنت بما فيها المنشأت المدنية الحيوية و العسكرية و شكل ذلك ثورة معلوماتية طالما عكفت أجهزة الإستخبارات في العالم

1 See : P. W. SINGER , ALLAN FRIEDMAN , ***CYBERSECURITY AND CYBERWAR WHAT EVERYONE NEEDS TO KNOW*** **,(** oxford press ,2014),pp 67-112 .

على الحصول عليها مع إمكانية البحث الهائلة لدى محركات مثل جوجل أو ياهو لديها القدرة على تصنيف المعلومات و تبويبها و سهولة الوصول إلى موضع البحث([1]).

و مع هذا الخضم الهائل من المعلومات ظهر الدافع لدى العديد من دول العالم لإستخداماته السلمية و الأخرى المخابراتية حيث تعتبر الأخيرة أداة سلطة الدولة على المعلومات و أحد فنون الحكم القائمة على معرفة الأصدقاء و الأعداء فهي أداة تحمل عدة تناقضات حيث يتم فيها استخدام الألفاظ و الصور و التقديرات و الايماءات و التحريض و فيها الحقائق و الأكاذيب، و لان المخابرات هي أداة غير مادية فهي لا تجرح و لكنها تسبب في إلحاق خسائر مادية و نفسية، و تتكون المخابرات من أربعة مكونات أساسية هي جمع المعلومات و الإستخبار المضاد و التحليل و التحرك المستتر.[(2)]

و يتم إستخدام الفضاء السيبراني في مسالة تعميم المعلومات و تبادلها بين أجهزة المخابرات داخل الدولة ذاتها أو بينها و بين دول أخرى حليفة لها لخلق تعاون و مبادرات مشتركة لمواجهة تهديد مشترك، و إستخدام الأنترنت في التحويلات المالية للعملاء و إستخدام غسيل الأموال كغطاء لعمليات التخابر و دفع الأموال، و الإستفادة من التداخل بين الفضاء السيبراني و الفضاء الخارجي في عمليات التجسس على المنشأت المدنية الحيوية و العسكرية و خاصة مع دخول التكنولوجيا الإتصال و المعلومات للمنظومة العسكرية لتحدث ثورة أخرى في الشؤون العسكرية ، و قد يشمل التجسس بث برامج على الجهاز في حال إتصاله بشبكة الأنترنت يتم من خلال كشف سرقة المعلومات التي بداخله أو عن طريق بث برامج خفية في ما بعد مرحلة تصنيع جهاز الكمبيوتر و تصدر إلى منشات حيوية في بلد ما و ذلك لسرقة معلومات عسكرية أو إقتصادية [(3)].

و تتميز حرب المعلومات و هجمات الإرهاب السيبراني بأنها ليست مقيدة في المجال و المدى، و هدفها غير مأمون العواقب و قد يستغرق عدة دقائق، و تعدد أطرافها و هناك صعوبة في إكتشاف الهجوم و الذي يظهر متأخرا بعد تفاقم المشكلة و خاصة مع صعوبة تحديد هوية المهاجم ، و تنقسم حرب المعلومات إلى نمطين هجومي و دفاعي تقوم بالهجومي في الغالب الدولة و أجهزة إستخباراتها لما تملكه من إمكانيات ضخمة تأهلها للقيام بذلك من أجل تحقيق أهداف سياسية و عسكرية أو لمجرد الإثارة و إظهار القدرات، و

---

[1]Schreier ,***op .cit*** .P21 .

[2]انجيليو كودفيلا، ***المخابرات وفن الحكم*** ،مترجم محمد صبري الصاوي،(القاهرة: الهيئة المصرية العامة للكتاب ، 2006).ص 154.

[3] Cullather Nick, "Bombing at the Speed of Thought: Intelligence in the Coming Age of Cyber war," ***Intelligence & National Security,*** (No.18,Winter 2003),pp141-154

أما الحرب الدفاعية فهي تعمل على الحد من أعمال التخريب التي يتعرض لها و تختلف الوسائل الدفاعية بإختلاف أدوات التخريب و طبيعة الأضرار التي تحدثها. و ذلك في حالة إذا ما تم إستخدامها بجانب العمليات العسكرية التقليدية ، أو حتى كسلاح مختار في الصراع بين عناصر ضد عناصر داخل الدولة كالقطاع الخاص أو ضد قوى خارجية ، أو حتى إستخدام الدول للمنظمات الإرهابية أو حتى أفراد أذكياء كبديل للحرب ضد الدول الأخرى و تصبح الأهداف السياسية هي الغاية و الحرب و الإرهاب عبر الفضاء السيبراني هي الأداة [1].

وعلى سبيل المثال تبنت إسرائيل "إسراتيجية الطين" « MUD Approach » وهي ثلاثة أحرف تمثل ثلاثة أساليب هي (الرصد، الإستخدام، العرقلة) Monitoring Using and Disrupting.([2]) ويقصد بـ (الرصد)، رصد الأفكار والدوافع وطريقة التفكير لدى زوار و مستخدمي هذه المواقع من أجل تحديد الأهداف و الخطط أو أي هجوم محتمل يفكر به طرف ما 'الإرهابيون" و تقوم عملية الرصد أيضا بمتابعة الخلافات و المناقشات الداخلية التي تدور بين الجماعات و الأفراد، لمعرفة إتجاهات التفكير و معرفة المعتدلون و "المتطرفون".

المطلب الثاني : توظيف الجماعات الإرهابية للفضاء السيبراني:

يعتبر الإرهاب سلاح الضعيف الذي لا يقدر على شن حرب ضد الدولة، فعن طريق الإرهاب يمكن إلحاق الأذى ومحاولة هزيمة القوة العظمى، وهذا ما يتضح في الجماعات والميليشيات العنصرية والأصوليات الدينية وبعض الأقليات التي لا تملك القوة ويكون الإرهاب وسيلة لتأكيد الهوية وجذب الإنتباه والإهتمام وقد يكون وسيلة من وسائل الصراع أو يكون من وجهة نظر من يقومون به نهاية الصراع حيث تدمير هوية العدو ويتعلق بالسماوات المفتوحة والفضاءات التكنولوجية، وكذلك بكون وسيلة لتحقيق أهداف مستقبلية عبر تحطيم الحاضر للوصول إليها، حيث التحطيم يكون بداية لظهور شيء معين من بين ركامه، و يكون مدفوعا بقيم أخلاقية أو ثقافية.[3]

---

[1] عادل عبد الصادق، "الأنترنت .. ساحة جديدة للتجسس الدولي" دراسات سياسية، ***جريدة الاهرام***،(5 ماي 2007)،ص 16.

[2] عمر عبد العزيز مشوح ،"إستراتيجية (الطين) الصهيونية لتطويق المواقع الإسلامية" ،في: ***http://www.maxforums.net/showthread.php?t=84500***, (2017/1/22).

[3] حسن الشامي ،***وسائل الاتصال وتكنولوجيا العصر***، (القاهرة: الهيئة المصرية العامة للكتاب، 1997)، ص 30.

و قد إستفاد الإرهابيون أيضا من ذلك التطور السريع في تكنولوجيا الإتصال حيث يستطيعون ببساطة شراء المنتجات التكنولوجية التجارية و الإستفادة مما تم إنفاقه في البحث و التطوير، و ليتمكنوا من الحصول على أجهزة كونية المدى فائقة السرعة متنوعة و معقدة و مشفرة و بدون أية تكاليف باهظة، و أتاحت شبكة الأنترنت الفرصة للحصول على أسهل الوسائل لإكتساب المعلومات و إصدار الأوامر و السيطرة على عملياتهم المخططة [1].

و بعد أحداث الحادي عشر من سبتمبر 2001 ظهر التزاوج بين الأنترنت و الإرهاب بشكل أكثر وضوحا ، و ما تلا ذلك من الحملة الأمريكية على الإرهاب و حدوث مواجهة بين تنظيم القاعدة و حلفائه من جانب و الولايات المتحدة و مؤيديها من جانب آخر و إنتقلت تلك المواجهات إلى الفضاء السيبراني و شنت حملة إعلامية مواكبة للحملات العسكرية من جانب الطرفين تم فيها إستخدام الأنترنت .

وتمكنت الجماعات المتطرفة بجميع أشكالها و مختلف توجيهاتها السياسية من إمتلاك مواقع على شبكة الأنترنت و منها من يمتلك أكثر من موقع يقدم خدماته بأكثر من لغة، و تهدف إلى التعريف بالتنظيم وتاريخه، ومؤسسيه وأبطاله وأنشطته وخلفياته السياسية والإجتماعية وأهدافه السياسية والإيديولوجية وأحدث الأخبار والنقد الشديد للأعداء كما تهدف رسالة المواقع بصور متعددة منها الدعم الفكري لهذه التنظيمات وتبجيل أفرادها أو مهاجمة المعتدلين والمفكرين أو مهاجمة الحكومات والأجهزة الأمنية، وقد تسعى تلك المواقع للتغطية على موقفها الداعم للإرهاب بالسماح بنقد يسير والإستناد في ترويج فكرها إلى بعض الكتابات الإيديولوجية والدينية وإلحاقها بتفاسير معينة وقصص تاريخية وضعت ضمن تأويل متعسف لكي تقنع الملتقى بمشروعية عملها حيث يتم إستغلال الدين باعتباره مظلة إيديولوجية تؤهلها لاستقطاب عناصر جديدة، كما يتم نشر تلك الأفكار وإدارتها من قبل أشخاص ذوي أفكار أحادية لا تسمح بوجود أحد ينافسها أو يعرض رأيا يخالفها. [2]

تهدف الرسالة الخاصة بتلك المواقع ثلاثة أنماط من الجمهور:

النمط الأول هو جمهور المؤيدين الحاليين والمحتملين وذلك عبر تقديم الموقع لهم معلومات مفصلة حول أنشطة المنظمة وسياساتها الداخلية وحلفائها ومنافسيها وعادة ما يكون هذا الجمهور هو جمهور محلي،

[1] حسن أبو طالب " تقرير اللجنة القومية الامريكية عن الهجمات على الولايات المتحدة. "، مركز الدراسات السياسية والإستراتيجية ، ***جريدة الاهرام***، (القاهرة، ماي 2006)، ص 132.

[2] عادل عبد الصادق، "المتطرفون وحرية التعبير على الأنترنت بين الأمن والإنفتاح" ،***مرجع سابق***.(موقع إلكتروني).

والنمط الثاني من الجمهور هو الرأي العام العالمي وهو غير المتورط مباشرة في الصراع، ولكن لديه بعض المصالح في القضايا المطروحة.[1] ويضم هذا الجمهور المستهدف الصحفيين ووسائل الإعلام التي تستخدم مواقع هذه التنظيمات للحصول على وجهات نظرها ويساعدهم في ذلك طرح خدمات المواقع بلغات عدة، وأخيرا يتمثل النمط الثالث في الأعداء وتسعى مواقع هذه التنظيمات من استهدافهم إلى إضعاف معنوياتهم من خلال توجيه التهديدات وتعزيز الشعور بالذنب لديهم إزاء التصرفات والدوافع. [2]

لكنها ليست أبدا الوحيدة التي تستخدم آلية التحريك والتنظيم الجديدة وأصبحت الحركات الإجتماعية وكذلك الأفراد قادرين على التأثير على وسائل الإعلام الكبرى والتحكم في المعلومات وتكذيبها إذ لزم الأمر أو حتى إنتاجها.[3]

ويتفق كل من تكنولوجيا المعلومات والدين في الرغبة في الإنتشار عبر الكون بينما يختلفان في الاستجابة السريعة للتغير ، فالدين بطبيعته يستند إلى مجموعة من القواعد والمعايير الأخلاقية التي لا تقبل التطور أو الذود عنها لأنها تكون من أسس ذلك الدين، أما التكنولوجيا فإنها بطبيعتها متغيرة غير ثابتة بتغير الإبتكارات والمهارات الفردية، إذا فإننا أمام جانب يميل للمحافظة بطبيعته وجانب يميل إلى التغير بإستمرار حيث لا ترتبط إلا بمعايير السوق والمال والإبتكار.[4]

يتسم الفضاء السيبراني كوسيلة إعلام دولية الطابع بعدة خصائص تنافسية بشكل جعلها عنصر جذب للإرهابيين بحيث بإمكانهم الإستفادة منها في مجال التصوير مثلا، دون أن يعرقل ذلك تفحص وسائل الإعلام الرسمية لذلك التصوير أو غربلته أو تحريره [5]. وقد بدأ الإرهابيون بالفعل في إستخدام الفضاء السيبراني في التأثير على الرأي العام وتجنيد أعضاء جدد عن طريق إقناعهم بشكل فردي وجمع الأموال سواءا عن طريق إشتراكات معينة أو عن طريق عمليات القرصنة وتحويل الأموال أو الإبتزاز الإلكتروني . وأصبحت مسألة نشر الرسالة والحصول على تغطية إعلامية إخبارية واسعة عنصرين مهمين لإستراتيجية

[1] حسن عماد مكاوي، ليلة حسين السيد ،***الاتصال ونظرياته المعاصرة*** ،(القاهرة :الدار المصرية اللندنية، 1998) ،ص 23.

[2] Gabriel Weidman, ***How Modern Terrorism Uses the Internet***,(The United States Institute of Peace, Special Report No. 116, March 2004)in : ***www.terror.net***(12/3/2017).

[3] مانويل كاستلز، "وسائل الإتصال الجماهيرية الفردية الجديدة" ***مجلة لوموند دبلوماتيك***،(أوت 2006)،ص 22.

[4] عادل عبد الصادق، "حقيقة دور الأنترنت في بث الكراهية الدينية في العالم، ملف الأهرام الإستراتيجي، مركز الدراسات السياسية والإستراتيجية ،***جريدة الاهرام***، (عدد 144، ديسمبر 2006)، ص 24.

[5] Dorothy Denning, ***Information Warfare and Cyber-terrorism***, Women in International Security (WIIS) Seminar, (Washington, D.C. 15 December 1999).p 54 .

الإرهاب، بالإضافة لوسائل الإعلام التقليدية، ويوفر الفضاء الإلكتروني للجماعات الإرهابية طريقة بديلة للوصول للجمهور وسيطرة مباشرة على الرسالة الإعلامية وشن الحرب النفسية والدعاية.[1]

تستخدم الجماعات الإرهابية الفضاء السيبراني من أجل تنفيد إستراتيجيتها عبر ثماني طرق مختلفة وإن كانت متداخلة أحيانا فيما بينهاوهي [2]:

الحرب النفسية، الدعاية والإعلان،التنقيب عن المعلومات،التمويل، التجنيد والحشد،الترابط، تبادل المعلومات والأفكار، التخطيط والتنسيق.

المطلب الثالث : توظيف تنظيمي القاعدة وداعش للإرهاب السيبراني:

برزت قدرة تنظيم القاعدة على التعامل مع وسائل التكنولوجيا من خلال أحداث سبتمبر 2001 حيث تم التخطيط والتنفيذ لها بالإعتماد على جزء كبير من التكنولوجيا المعلوماتية ووسائلها، والتي تضمنت ما يمكن أن نطلق عليه أسلحة إفتراضية من نوع خاص، فكان الكمبيوتر وبرامجه والبريد الإلكتروني ونظم محاكاة الطيران Flight Simulator وأجهزة المحمول والرسائل القصيرة SMS وشبكات الأنترنت وأجهزة الصرف الآلي ATM والتحويلات المالية عبر الأنترنت والمساعدات الرقمية الشخصية Personal Digital Assistant بالإضافة إلى كمبيوترات الجيب Hand Held. وهذا ما يشكل صورة إرهاب جديد يطلق عليه الإرهاب الإلكتروني أو الشبكي Cyber Terrorism .([3])

وكان تنظيم القاعدة هو أول حركة تمارس نشاطا إرهابيا بالإنتقال من الفضاء الأرضي إلى الفضاء المعلوماتي والأنترنت ولتنتقل من منظمة عاملة إلى منظمة دعاية. وأصبحت شبكة الأنترنت وسيلة تعبير وإتصال شائعة الإستخدام بين المتطرفين الإسلاميين في كل من العالم الإسلامي والأقليات الإسلامية

---

[1] Michele Zanini, Sean J.A. Edwards, "The Networking of Terror in the Information Age," in John Arquilla and David Ronfeldt (eds.), Networks and Netwars: ***The Future of Terror, Crime and Militancy*** (Santa Monica, CA: RAND, 2001, MR-1382-OSD), p43.

[2] عادل عبد الصادق، "المتطرفون وحرية التعبير على الأنترنت بين الأمن والإنفتاح، دراسات سياسية، ***جريدة الأهرام*** (21 فبراير 2005)،ص15.

[3] وقد ثبت إستخدام خالد شيخ محمد المتهم الرئيسي في أحداث 11 سبتمبر 2001 ما يسمى "بالقنطرة الخفية" على الأنترنت لمنع كشف الرسائل الإلكترونية عن طريق فتح حساب في الهوت ميل Hotmail أو غيرها يتم حفظ الرسالة كمسودة بالإيميل بدون إرسالها، ويتم تبادل كلمة المرور من خلال المنتديات أو الدردشة، بذلك لا يتم إرسالها ويصعب مراقبتها، أو إستخدام عدد من الرسائل غير المرغوبة للتغطية على رسالة واحدة وهذا ما جعل هناك صعوبة في جمع المعلومات الإستخباراتية. خاصة مع إفتقاد أجهزة المخابرات الأمريكية لكوادر تتقن اللغة العربية.

المهاجرة في الغرب. وليس من الصعب معرفة السبب الكامن وراء هذه الشعبية الفائقة للأنترنت وسط الأصوليين والمتطرفين الإسلاميين، فالأنترنت يوفر مساحة حرة للإتصال تربط ما بين الجماعات الإسلامية المتعددة.[1]

وقد دفع دلك إلى لجوء الولايات المتحدة لغلق المواقع التي تراها توفر معلومات أساسية عن صنع القنابل أو أساسيات صنع القنبلة الذرية أو تفصيلات المرافق الحيوية وخرائطها وذلك منعا من إستغلال ذلك في التنفيذ لعمل إرهابي.[2] ويستخدم الجهاديون ثلاث وسائل للمساعدة في تنفيذ أهدافهم عبر الفضاء الإلكتروني الأولي هي المنتديات وهي بمثابة مساحات مفتوحة للمشاركة. ويمكن للشخص من خلال مشاركته فيها أن يصبح قادرا على نشر رسائله وأفكاره وبالتالي فإن بعضها يتم إستعماله لنشر بيانات القاعدة "أما الوسيلتين المتبقيتان فهما "الدردشة chat، التي باتت تستعمل كوسيلة للتجنيد الفكري والعسكري" و"الغرف الصوتية" التي تسمح للمشاركين فيها بالتواصل صوتيا على شبكة الأنترنت. وأصبحت القاعدة التي كانت تدون في السابق كل تقاريرها وبياناتها باتت تستعمل النظم المعلوماتية وتنشر على الأنترنت "كتبا إلكترونية" تشرح عقيدتها "من أولها إلى آخرها"، وتنشر طرق تصنيع المتفجرات بواسطة مواد كيميائية متوفرة في الأسواق.[3]

وكنتيجة لتطور الفكر التكفيري ومنذ أحداث الحادي عشر من سبتمبر 2001 تضاعفت أعداد المواقع التي تمارس "الجهاد الإكتروني" بشكل كبير، وتمكن الموصوفون بالأصوليون والإرهابيون من إيصال ونشر أخبارهم في المواقع والمنتديات وغرف الدردشة، و تمكنوا من إنشاء مواقع خاصة بهم تنشر أفكارهم ، كما أنها تنشر محتويات تسجيلات و خطب و صورا لعمليات ضد قوات الإحتلال في العراق و فلسطين ، مما جعل " الأصوليين الإسلاميين" من بين أكبر المستفيدين على الإطلاق من ثورة المعلومات و الإتصالات التي يشهد العالم تسارعا كبيرا في نموها. و لا تخلو (مواقع الجهاد الإلكتروني) من مواد تعلم روادها فنونا قتالية ، بل و ترشدهم إلى كيفية صناعة القنابل و غيرها من وسائل القتال ([4]).

---

[1] Timothy L. Thomas, ***Al Qaeda and the Internet: The Danger of "Cyber planning",*** (From Parameters, Spring 2003), pp112-150.

[2] Weidman ,***Op.Cit***

[3] Thomas, ***Op.Cit***,p 153 ***.***

[4] Seee : Christina Schori Liang, ***Cyber Jihad: Understanding and Countering Islamic State Propaganda***, (GCSP Policy Paper 2015/2 - February 2015).pp1-12 .

و هناك مواقع توفر كتابات نظرية متنوعة و إجتهادات فقهية لكبار منظري التيارات الجهادية، أمثال الأردنيين " أبو مصعب الزرقاوي " و " أبو محمد المقدسي". و تبرز كذلك كتابات المصري " سيد إمام شريف"، و من بينها مجلد " الجامع في طلب العلم الشريف" الذي يتجاوز الألف و ستمائة صفحة من القطع الكبير و الذي يتناول جوانب فكرية متعددة عن الإسلام السلفي المتشدد، بالإضافة إلى كتاب أخر مخصص للجهاد فقط بعنوان " العمدة في إعداد العدة " يتألف من مئات الصفحات أيضا. و هناك فئة منفصلة من الكتابات الغزيرة مخصصة للتصدي و الرد على الشيوخ و الإسلاميين المعتدلين الذين يعارضون الجهاد كليا أو جزئيا([1]).

و يحوي أحد هذه المواقع كتابا عن تمرينات اللياقة البدنية للنساء المجاهدات. و في المنتديات و غرف الدردشة الإسلامية المتطرفة يتم تبادل وجهات النظر ، و مناقشة الموضوعات العملية المتعلقة بالجهاد، إضافة للفتاوى حول الجهاد و غيره من القضايا الإسلامية من قادة الحركات الجهادية و فقهائها حول أسئلة مثل : " وجهة نظر الإسلام في الذهاب للجهاد من دون إذن الوالدين" و " حكم الإسلام فيمن يعمل إماما بمسجد يموله الكفار".

و يعد الأنترنت كذلك وسيلة ينشر من خلالها المئات من الأشرطة المسموعة و المرئية التي تحوي مواعظ دينية لمشاهير الوعاظ، كما تضم أشرطة عمليات عسكرية جهادية مثل ما تفعله شركة "سحاب" التي تنتج أشرطة فيديو ل " أسامة" بن لادن" و كثير من الهجمات الإرهابية و التفجيرات في المملكة العربية السعودية أكثر من أربعة ألاف موقع إلكتروني لها علاقة بالنشاطات الإرهابية، و يعتقد أن هذه المواقع تمتلك القدرة على التوالد، و قد قامت مجموعة تابعة لمنظمة " القاعدة" عبر موقع Al–jinan.Org بتطوير برنامج "الجهاد الالكتروني Electronicjihad» الذي يسمح لجميع مستخدمي الأنترنت حتى و لو كانت معلوماتهم التقنية صفرا، أن يقوموا بشن الهجمات على قائمة من المواقع المخزنة فيه، و التي يتم تحديثها بشكل دوري([2]).

وإنتقلت ساحة المواجهة الأمريكية مع تنظيم القاعدة في إطار حرب أفكار متبادلة وتنافسا حول جمهور عالمي واسع يستقبل الرسالة الإعلامية على شبكة الأنترنت والتي أصبحت مصدرا للأخبار للعديد من وسائل

[1] Thomas, ***Op.Cit***,p 153 **.**

[2] أنظر:كول بانزل ،"المملكة ودولة الخلافة :مبارزة بين الدولتين" في :-***http://carnegie-mec.org/2016/02/18/ar-pub-62893***(2017/5/22).

الإعلام.[1] وفي حين ركزت الإدارة الأمريكية جل إهتمامها على عملياتها العسكرية فإن تنظيم القاعدة ركز بصورة أكبر على الجانب الإعلامي من عملياته كجزء من المواجهة وحتى سياسة حجب المواقع التابعة لتنظيم القاعدة لم تؤد إلا إلى توالد العديد من المواقع الأخرى بشكل إقترب فيه تنظيم القاعدة من النجاح إعلاميا ومخاطبة الغرب والعمل على عزل القيادات الأمريكية وحلفائها عن شعوبها بتكوين إعلام آخر مختلف عما تروجه وسائل الإعلام الأمريكية للشعب الأمريكي وخلق شبكة مؤيدين عالميين عبر الخلايا النائمة في العالم.

أما تنظيم داعش فقد إستثمر (الفضاء السيبراني) فى الترويج والتخطيط والتنفيذ لأعماله المشينة أسوة بـ(تنظيم القاعدة) منذ عام 2014 تقريباً, ولكن مع التوسع بالطبع فى إستخدام كل التقنيات الحديثة الى ظهرت لاحقاً.

فعلى مستوى وسائل التواصل والإعلام الاجتماعى مثلاً نجد أنه وظف تقنياته الحديثة بشكل جيد جداً سواء للمطالبة بدعم التنظيم «فهناك وسم شهير على الأنترنت حقق حوالى 20 ألف إشارة فى أقل من 24 ساعة كان يطالب فيه التنظيم كل من يدعم (داعش) برفع العلم الأسود الخاص بالتنظيم تعبيراً عن هذا الدعم»,([2]) أيضاً نجدهم يستخدمون شبكات التواصل الإجتماعى والمواقع الإلكترونية فى تلك الجزئية من أجل الترويج لمدى قوة مقاتليهم وكذلك للإحتفاء بإنتصاراتهم مستخدمين كما أشارنا الوسوم الأكثر إنتشار على الشبكة العنكبوتية لضمان الوصول لأكبر عدد ممكن الناس. هذا أيضاً إلى جانب تكتيك خطير أشبه بغسيل المخ وكان ولا يزال له دور كبير فى تجنيد المزيد من المقاتلين, حيث يلعب هذا التكتيك على نقطة أساسية وهى تبديد الصورة التقليدية للإرهابى فيظهره عبر حسابه الشخصى وهو يأكل الشيكولاتة, أو يطعم بعض الحيوانات كالقطط أو الكلاب مثلاً, و..... فهنا هو يركز على الجانب الإنساني والشخصي مما يعكس إدراك واعي منه بالطبيعة الإجتماعية لتلك المواقع الإلكترونية.

برع «تنظيم داعش» فى إستخدام تطبيق «تلجرام» ([3])لربما لأنه من أكثر التطبيقات التى تتيح خاصية التشفير, فقد روج من خلال هذا التطبيق والذي يعد الأكثر أمناً لفيلم «لهيب الحرب», الذى تم بثه باللغة الإنجليزية وحوى مشاهد لإشتباكات مع الجيوش العراقية والسورية, مستخدماً فيه تقنيات عالية فى التصوير وخاصة تلك المتعلقة بالحركة البطيئة, إضافة إلى إعلانه هنا أيضاً مسئوليته عن إسقاط الطائرة الروسية في

[1] محمد الجمال راسم ،***نظام الاتصال والإعلام الدولي: الضبط والسيطرة،*** (القاهرة :الدار المصرية اللبنانية، 2005)،ص156.

[2] هبة عبد العزيز ، "داعش والإرهاب الإلكتروني "،في ***https://alwafd.org/essay/20595:*** (2017/4/24).

[3] تم إنشاء تطبيق التواصل الإجتماعي "تيليجرام " في 14 أغسطس 2013 وكانت بداية التجربة مع النسخة الخاصة بالآيفون، وفي يوم 20 أكتوبر من نفس السنة انطلقت النسخة الخاصة بالأندرويد.

سيناء, ومن بعدها هجمات باريس الأمر الذى دعا إدارة «تلجرام» للإعلان عن إغلاق حوالى 78 حساباً تابعاً للتنظيم([1]).

وهناك كذلك ما هو أكثر إنتشاراً وبالتالى خطورة وهو جمع الأموال من المتعاطفين وذلك من خلال إستخدام العملات الرقمية مثل «البتكوين» لشراء الأسلحة, فقد رصد معهد الإتحاد الأوروبى لدراسات الأمن فى عام 2015 ما يقرب من 40 موقعا تابع للتنظيم, وأن السلاح الذى تم إستخدامه فى هجمات «تشارلى إبدو» قد تم شراؤه و بيعه عبر الفضاء الإلكتروني بمبلغ 550 يورو من موقعه «إيرو أرمز» أحد أكبر الأسواق السوداء لبيع السلاح([2]).

المبحث الثالث:طبيعة و أنماط توظيف الفضاء الإلكتروني في الصراع الدولي.

المطلب الأول : إستخدام أسلحة و هجمات الفضاء السيبراني في الصراع الدولي:

كما هو الحال في أية حرب فإن الجيوش المتصارعة تستهدف دوما ثلاثة عناصر أساسية من أجل كسب المعركة، و هي العناصر العسكرية، و الإقتصادية ، و السياسية أو بكلمات أخرى إرادة الخصم، و في عالم حروب المعلومات تجد العناصر الثلاثة ذاتها و على رأسها مراكز القيادة و التحكم العسكرية ، و البنوك و المؤسسات المالية، و مؤسسات المنافع كمؤسسات المياه و الكهرباء و ذلك لإخضاع إرادة الشعوب. و إذا قامت دولة بتدمير شبكة الانترنت بشكل متعمد فان دولة أخرى قد تعتبر هذا الأمر عملا عدائيا، و قد لا يكون الهدف هو تدمير الشبكة كليا أو تعطيلها حيث أنها تساعد حتى الطرف المعتدي في مراقبة المحادثات بين الأعداء أو نشر معلومات خاطئة. حيث يعتبر ذلك فرصة إستخباراتية مذهلة ، كما أن إستخدام الأنترنت من أجل السيطرة على المعلومات يمكن أن يعود بفائدة أكبر من تعطيل الشبكة نفسها أو تعرضها للهجوم، عندما يتعلق الأمر بالإستراتيجية العسكرية. و العمل على أضعاف إرادة المحاربين و شن حرب نفسية و التحكم في المعلومات .[(3)]

و تتضمن هجمات الكمبيوتر حدوث هجوم و ذلك عبر الشبكات الدولية للمعلومات العابرة للحدود و من خلال موجات الراديو أو الشبكات الدولية للإتصالات بدون تدخل مادي أو طبيعي في الأراضي الخاصة

[1] "تلغرام يعلن عن غلق 78 قناة تابعة لتنظيم داعش الإرهابي "،***جريدة الشرق الأوسط***،(عدد 3506 ،2015/11/20)،ص12

[2] عبد العزيز ،***مرجع سابق*** .(موقع إلكتروني).

[3] Rebecca Grant, ***Victory in Cyberspace***, (USA : The Eaker Institute, October 9, 2007).P23 .

بدولة أخرى أو القيام بغزوة تقليدية، و على الرغم من الإستخدامات الحديثة لهجمات الفضاء السيبراني في الصراعات الحديثة في عصر المعلومات إلا أنه لم يتم إدماجها بشكل كامل في العقيدة العسكرية للجيوش الحديثة، و إن كان يعد بداية لأخذها في الإعتبار في سبيل الإستحواذ على القوة و إمتلاكها من خلال تطوير أسلحة الفضاء السيبراني لكي يتم إستخدامها في حروب المستقبل و بما ينطوي عليه تغيير المبادئ الخاصة بشن الحرب و ميدان الحرب و الطرق و الوسائل الحربية المتاحة، و هي هجمات يمكن أن تحدث سواء في أوقات السلم أو الأزمات الدولية [1].

ظهر الفضاء السيبراني كأحد مجالات الحرب مثل الجو و الفضاء الخارجي و الأرض و البحر، و أصبح الفضاء السيبراني يستخدم في المجال العسكري و غير السلمي، و قد لا تؤدي الحرب في الفضاء السيبراني إلى مأساة إلكترونية بالضرورة بل إلى فرض نوع من السيطرة على مجرى الأحداث في العالم وفق مصلحة من يقوم بها على جبهة واسعة النطاق من السهل الإختفاء بها، كما أن أثار الهجوم قد لا تتساوى مع تكاليفه مع صعوبة تحديد هوية مصدر الهجوم ، الذي يصدر من جانب واحد مما يجبر ضحايا الهجوم على إتخاذ وضع الدفاع ، و عدم قدرتهم على شن هجوم مضاد و إن حدث يكون تأثيره محدود لعدم معرفة مصدر الهجوم.[2] و كانت المعلومات و المعرفة على مدار التاريخ البشري قد لعبت دورا هاما و حيويا في تشكيل القوة فإن التطور السريع لتكنولوجيا الكمبيوتر و خاصة في الشبكات قد أحدث تحولا كبيرا في مفهوم القوة ترتب عليه دخول المجتمع الدولي في مرحلة جديدة تلعب فيها هجمات الفضاء السيبراني دورا أساسيا في تعظيم القوة و إستحواذها، و كنتيجة مباشرة لذلك أصبحت القدرة التي أتاحتها التكنولوجيا الحديثة للدول تستخدم تعظيم إمكانياتها في إمتلاك أدوات حرب المعلومات و تقنياتها في ترسانتها العسكرية.[3]

وظهرت أسلحة إلكترونية جديدة ومتعددة كالفيروسات وهجمات إنكار الخدمة والإختراق وسرقة المعلومات والتشويش، وتلعب القنابل الإلكترونية دور في تنفيذ عدد من المهام الإستراتيجية مثل تعطيل الإتصالات والتشويش عليها والتنصت على المكالمات وبث معلومات مضللة عبر شبكات الحاسب والهاتف ومنها

[1] عادل عبد الصادق، "أمريكا وتشكيل قيادة عسكرية في الفضاء الإلكتروني.. هل بدأ الإستعداد لحروب المستقبل"، ***مجلة تعليقات مصرية*** ، (العدد 130، 12 يوليو 2009) ،ص 15.

[2] Kevin G. Coleman***, A Cyber War has begun, Cyber Warfare***,(usa :The Technolytics Institute, September 2007).(22/3/2017) .

[3] Dimitrios Delibasis," State Use of Force in Cyberspace for Self-Defence: A New Challenge for a New Century", ***Peace Conflict and Development: An Interdisciplinary Journal***,(Issue 8, February 2006), in : ***http://www.peacestudiesjournal.org.uk***.(2017/3/22)

تقليد بصمات الأصوات وخاصة أصوات القادة العسكريين وعن طريق ذلك يمكن إصدار أوامر ضارة بالقوات وإستهداف شبكات الحاسب بالتخريب عن طريق نشر الفيروسات ومسح الذاكرة الخاصة بالأجهزة المعادية ومنع تدفق الأموال وتغيير مسار الودائع وإيقاف محطات الكهرباء عن العمل([1]) .

ويكون تأثير إستخدام الفيروسات مضاعفا نتيجة لما ينطوي عليه من توجيه "جيش" يضم مجموعة كبيرة من أجهزة الكمبيوتر المرتبطة بشبكة واحدة والمحملة بالفيروسات، يتم التحكم فيها عن بعد، لمهاجمة النظام المستهدف بعدد من الأوامر والطلبات في نفس الوقت ونشر الفيروسات فيه بهدف شله.

وفي خلال السنوات الماضية تمكنت فيروسات "سارس" و"لف" من الإنتشار في نصف مليون جهاز كمبيوتر في أقل من أربع ساعات وأصبحت هذه الهجمات تستخدم تعبيرا أيضا عن صراعات دولية كما إستخدمت في حرب الناتو على صربيا وفي الحرب في كوسوفو وما بين التنافس بين الصين وروسيا والولايات المتحدة وأستراليا وفي حرب العراق وفي الصراع العربي الإسرائيلي [(2)].

وقد تستخدم الدول هجمات الإرهاب السيبراني ضد دول أخرى أو قد تستخدمها الجماعات الإرهابية، وفي السيناريو الأول قد تقوم الدولة (أ) بإستخدام هجمات الفضاء السيبراني ضد الدولة (ب) دون أن تتورط بشكل رسمي ومباشر في حرب معلنه حيث يمكنها أن في هذه الحالة من تحقيق الأهداف ذاتها التي يمكن أن تحققها الحرب التقليدية، وهناك سيناريو ثان وهو: أن تقوم الدولة (أ) بإستخدام هجمات الفضاء السيبراني كجزء من الإستعداد لنشوب صراع وحرب وهجوم تقليدي ضد الدولة (ب)، وتعد هجمات الفضاء السيبراني أقرب إلى مفهوم "الحرب غير المتماثلة" وهو مفهوم عسكري يشير إلى الإستخدام غير المباشر للقوة وذلك بدلا من إستخدام القوة بصورة مباشرة في مواجهة قوة مقابل قوة أخرى [(3)].

المطلب الثاني : نمادج عن الحرب السيبرانية الباردة :

يمكن أن يتم تصنيف تعرض الفضاء السيبراني لأنماط الحرب والصراع إلى صراع مرتفع الشدة وآخر صراع منخفض الشدة، ويمكن التعرض لبعض أنماط الصراع المنخفض الشدة على النحو التالي:

[1] عبد الصادق،" أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني "، ***مرجع سابق*** .(موقع إلكتروني).
[2] عبد الصادق، "هل يمثل الإرهاب الإلكتروني شكلا جديدا من أشكال الصراع" ،***مرجع سابق*** .(موقع إلكتروني).

[3] Richard A. Lipsey, ***Network Warfare Operations: Unleashing the Potential***,(USA :Center for Strategy and Technology, Air War College, Air University, November 2005)p.45.

شهدت حرب البلقان في نهايات القرن الماضي والتي شنهاحلف الناتو ضد الصرب إعلان دخول التقنيات الرقمية ميادين الحروب فيما سمي "بالقنابل المعتمة"([1]) وقد أدى هذا الهجوم الإلكتروني إلى توقف شبكة الحاسب الرئيسية مما أصاب نظم الكمبيوتر الخاصة بوزارة الدفاع اليوغسلافية بالشلل التام وإستطاعت القنابل الإلكترونية تعطيل الإتصالات عبر التشويش على شبكة الإتصالات الهاتفية الرئيسية "الثابتة" مما دفع القيادة في بلجراد إلى الإتصال بقواتها عبر الهواتف الجوالة، وبالتالي أصبح يسيرا على قوات الحلف مهمة إختراق المكالمات. وما تشهده الهند وباكستان من إمتداد لصراعهما في الفضاء الإلكتروني عبر إستخدام الفيروسات ذات الطابع القومي والتي أستخدمت في تنفيذ هجمات متبادلة مضادة فيما بينهما حيث تم شن هجمات ضد أهداف تحمل مصالح وطنية وجيوبلوتيكية. وفي حرب كوسوفو قامت الولايات المتحدة بإستخدام النبضات الكهرومغناطيسية لإيقاف كل وسائل الإتصال السلكي واللاسلكي المدنية والعسكرية، وإستخدام الأقمار الصناعية في ضرب الولايات المتحدة معاقل المحاكم الإسلامية في الصومال، وكذلك في تحقيقات إغتيال رفيق الحريري رئيس وزراء لبنان الأسبق. وقد رصدت وكالة الإستخبارات الأمريكية حالة نجاح في إستخدام هجمات الكمبيوتر في إصابة البنية التحتية خارج الولايات المتحدة [(2)]. وفي عاصفة الصحراء عام 1991 قام قراصنة من هولندا بإختراق مواقع الجيش الأمريكي ونظم الإمداد والحصول على المعلومات عن مواقع الجيش الأمريكي وأسلحته وحركة السفن الحربية، وقد كانت حرب عاصفة الصحراء 1991 في الخليج طورا إنتقاليا بين حروب الثورة الصناعية وحروب المعلومات، فقد تواجد ما يزيد على 3000 حاسب متصل بحاسبات أخرى في الولايات المتحدة بينما وصفها البعض بأنها حرب مزدوجة الأساليب، وتمكن الإستخبارات المركزية الأمريكية من إختراق الشبكة اللاسلكية للجيش العراقي([3]).

و قامت وكالة الأمن الإسرائيلية "شاباك" بإغتيال الفدائي "يحي عياش" في عام 1996([4]) عن طريق الهاتف المحمول، و في عام 2000، قامت مجموعة من الإسرائليين بالهجوم على موقع لمجموعة تابعة ل"حزب الله" في لندن، الأمر الذي قوبل بمهاجمة العرب للموقع الرئيسي للحكومة الإسرائيلية و موقع وزارة الخارجية الإسرائيلية، بالإضافة إلى مهاجمة بعض الشركات الأمريكية التي تتعامل مع إسرائيل مثل شركة "لوسينت تكنولوجيز" للتأثير على إقتصاد إسرائيل الذي يعتمد بشكل كبير على الأنترنت.

---

[1] يحي مفرح الزهراني،" الأنترنت والحروب المستقبلية"،في:
http://www.aleqt.com/2017/03/28/article_1159071.html، *(2017/4/30).*

[2] Tom Espiner," CIA: Cyberattack caused multiple-city",in : ***https://www.cnet.com/news/cia-cyberattack-caused-multiple-city-blackout/***, (23/11 /2016).

[3] **LOC .CIT** .

[4] لمزيد من المعلومات انظر :***يحي - عياش*** ***https://ar.wikipedia.org/wik***i (2017/4/24).

و في 07 ديسمبر 2005 أعلنت الإدارة الأمريكية عن تحول مهمة القوات الجوية الأساسية إلى "الطيران و القتال في الجو و الفضاء السيبراني" و جاء ذكر الفضاء السيبراني بشكل مستقل كتعبير عن الاعتراف بإستقلالية تداخل المجالات و التفوق الإلكتروني، و يشير لدورة في فاعلية مجالات العمليات الإسراتيجية، و إضفاء أهمية إستراتيجية للفضاء الإلكتروني كغيره مثل المجال الجوي و الفضاء الخارجي.[1]

و قد حضيت الهجمات ضد إستونيا في 2007 بإهتمام الخبراء من حلف شمال الأطلنطي و الإتحاد الأوروبي و الولايات المتحدة و إسرائيل و السفر إلى تاليين عاصمة إستونيا للوقوف على مجريات تلك الواقعة و عرض المساعدة و التعليم و التدريب عن الحرب الجديدة في الفضاء السيبراني في عصر المعلومات الذي تميز بإستخدام متزايد لشبكات الإتصالات الفضائية و الأرضية في الحروب .[2]

و في سبتمبر 2007 إتهمت الصين بأنها تقف وراء هجمات إختراق أجهزة الكمبيوتر الخاصة بوزارة الدفاع الأمريكية، كما إتهمت بالمسؤولية عن هجمات مماثلة على ألمانيا و فرنسا و بريطانيا و نيوزيلاندا، و تعلن الصين أنها تقع هي الأخرى ضحية لهجمات و ذلك لسرقة معلومات و أسرار صناعية عسكرية بما أدى لتعطيل خدمات الموقع مع إستمرار حرب الإختراقات بين المخابرات المركزية الأمريكية و جيش التحرير الصيني [3].

مكن إستخدام الإرهاب الإلكتروني في نشر الشائعات و العنصرية و الكراهية الدينية إلى جانب نشر عمليات رد الفعل كما حدث في أزمة الرسوم الكاريكاتورية المسيئة للرسول (ص) حيث تداولها و إنتقالها من مجرد رسوم محلية في صحيفة محلية في الدنمارك إلى إنتشارها عبر الفضاء الإلكتروني مما ساعد على قيام العديد من الإحتجاجات و تصاعد المقاومة ضد الوجود الأمريكي في أفغانستان و العراق كما تم القيام عبر الأنترنت بحملة مضادة لتلك الرسوم من جانب المسلمون لرد الإساءة.

و في 27 مارس 2008 كان هناك واقعة أخرى فبعدما تم رفض الحكومة الهولندية إذاعة فيلم "فتنة" للإسلام و مدته 15 دقيقة على المحطات التلفزيونية لجأ مخرجة النائب الهولندي المتطرف "جيلدر فيلدرز" إلى

---

[1] Courville Shane P, ***Air Force and the Cyberspace Mission: Defending the Air Force's Computer Networks in the Future***, (Maxwell Air Force Base, AL, Center for Strategy and Technology, Air War College, 200).,pp53- 67

[2] Robert Vamosi," Cyber attack in Estonia--what it really means", in : ***https://www.cnet.com/news/cyberattack-in-estonia-what-it-really-means***/(12/11/2016).

[3] "China 'hacked' into Pentagon defense system", ***The Financial Times***, (September 4 2007)p43

عرضه على الأنترنت عبر موقع بريطاني شهير [1] وكنتيجة لدلك توالت ردود الأفعال الإسلامية و أصبحت هناك عملية الإستيلاء على الموقع و التحكم فيه و تدمير محتوياته و قصفها و بث رسائل معادية كما أصبح هناك عمليات تجنيد متبادلة لتحسين القدرة على ضرب و إختراق تلك المواقع على الأنترنت.

و تلك الهجمات ما هي إلا إنعكاس لما يدور في الساحة الإسلامية من مجال بين رموز في التيارين السني و الشيعي حول التبشير الطائفي و إمتداد لحالة الصراع داخل المجتمعات الإسلامية [2].

تبنت الصين إستراتيجية حرب المعلومات كحرب للمستقبل و التي يتم خوضها لتشتيت و إثارة الإضطرابات في عملية صناعة القرارات عبر الدخول إلى أنظمة الطرف الآخر و إستخدام و نقل معلوماتهم بعد الأهمية المتزايدة للفضاء الإلكتروني [3].

و يتم تدريس الحرب عبر الفضاء الإلكتروني كمادة في كليات الصين العسكرية [4].

و يوجد لدى الصين جيش من "الهاكرز" وترسانة من الفيروسات[5]القابلة للتجنيد في أي وقت بما يعد بمثابة جيش إحتياطي متمرس و مهيا للتدخل في أي لحظة في المعركة و وظيفته ليس ضرب أنظمة المعلومات للبنية العسكرية الأمريكية فحسب و أنما ضرب قنوات الإتصال المدنية

و يأتي إتهام الصين بشن هجمات الفضاء الإلكتروني في إطار جزء من خطط بكين لفرض "هيمنة إلكترونية" على خصومها العالميين بحلول عام 2050 في مواجهة الولايات المتحدة و بريطانيا و روسيا و كوريا الجنوبية، و أعلنت وزارة الدفاع الأمريكية بأن الجيش الصيني يعتبر هجمات المعلوماتية مهمة للغاية لكسب المبادرة في المراحل الأولى من أي حرب و أن هناك قراصنة صينيون أعدوا دليلا إفتراضيا لشن حرب

---

[1] الموقع الذي تم فيه إذاعة الفيلم وهو موقع بريطاني شهير هو ***http://www.likelike.com***

[2] عادل عبد الصادق، "إختراق مواقع الإنترنت بين السنة والشيعة.. عندما تسيطر السياسة على الدين"، ***مجلة تعليقات مصرية***، مركز الدراسات السياسية والإستراتيجية بالأهرام، (العدد 112، 15 أكتوبر 2008) ،في: ***http://acpss.ahram.org.eg/Ahram/2008/10/15/COMM0.HTM***، (2016/10/2).

[3] حنان سليمان، "الصين تستهدف الجيش الامريكي الكترونيا ***تقرير واشنطن***، (العدد 143، 26 يناير 2008)، ص 14.

[4] أنظر : ستيفان مارشان Stephane Marchand "حين تقرر الصين أن تنتصر"، (فرنسا: دار "فايار" 2007)،ص123.

[5] أحد هذه الفيروسات هو فيروس "Myfip" المناسب تماما لحرب المعلومات لقدرته على سرقة أنواع مختلفة من الملفات مثل pdf وملفات الوورد والرسومات. ولهذا فإن أي شبكة إلكترونية تصاب بهذا الفيروس فإنها ستفقد وثائقها وخططها وإتصالاتها وقاعدة بياناتها كما ستكون هذه المعلومات معرضة للسرقة. وخلال الأعوام الأخيرة، أجرى بعض القراصنة الصينيين تجارب لإختبار الأنظمة الإلكترونية الدفاعية الأمريكية على دائرة أصغر دون اللجوء إلى هجوم قوي. هذه التجارب كانت أيضا بهدف التعرف على نقاط الضعف في الأنظمة الأمريكية ليسهل إختراقها في ما بعد.

إلكترونية و للتشويش بعد أن درسوا كتب إرشادات وضعها حلف الأطلسي و الولايات المتحدة حول الأساليب العسكرية.([1])

وفي الولايات المتحدة إستحدث البنتاجون في 22 يونيو 2009 قيادة عسكرية أمريكية في الفضاء الإلكتروني مهمتها الرد على هجمات قراصنة المعلوماتية وتنفيذ عمليات في الفضاء الإلكتروني والتي ستدخل العمل في شهر أكتوبر 2009 [(2)].

في إسرائيل وحدة خاصة تدعى "رام" لمواجهة حملات "الغزو الإلكتروني" وتركز هذه المراكز في "مزرعة خاصة" تحت رعاية وزارة المالية وتخضع لرقابة وحراسة أمنية مشددة –فيزيائية وإلكترونية– وتتابع "المهاجمين" خاصة من حملة الهوية الإسرائيلية العرب [(3)].

ونتيجة لخلاف بين روسيا و إستونيا تم شن الهجوم على الكمبيوتر والشبكات من أكثر من 50 دولة والذي أخذ شكل موجات حيث يبدأ الهجوم ثم ينتهي فيعقبه هجوم آخر [(4)]. وأتاح إرتباط إستونيا القوي بشبكات الإتصال والمعلومات وجود مجال واسع من الأهداف أصبحت عرضة للهجوم مع قدرة المهاجمين على ضرب المؤسسات الرسمية للدولة وإصابة وإفساد المواقع الحكومية [(5)].

وإستطاعت مجموعة من الهاكرز من إستونيا الرد على هذا الهجوم عن طريق تعطيل منظومة الأنترنت في موسكو لمدة أسبوع .

---

[1] مارشان ،***مرجع سابق*** ،ص127.

[2] عبد الصادق، "أمريكا وتشكيل قيادة عسكرية في الفضاء الإلكتروني .. هل بدأ الإستعداد لحروب المستقبل "،***مرجع سابق***.(موقع إلكتروني).

[3] وديع عووادة، "الجهاز الإلكتروني العربي يثير مخاوف اسرائيل"، في:
http://www.aljazeera.net/NR/exeres/A5B34FD6-A61F-457B-8456-2008F1CC24EC5794.htm،(2017/2/24).

[4] "Cyber Attacks Force Estonian Bank to Close Website," ***Agence France Presse***, (May 16, 2007),p 13.

[5] Peter Finn, "Cyber Assaults on Estonia Typify a New Battle Tactic," ***Washington Post***,(May 19, 2007), p23.

المطلب الثالث : نمادج عن الحرب السيبرانية الساخنة :

يعد إستخدام الحرب عبر الأنترنت ميزة عسكرية للأطراف المتحاربة و التهديد بإستخدام أسلحة الفضاء الإلكتروني ضمن ترسانة الحرب الحديثة و قد يستخدم الفضاء الإلكتروني في الصراع بطريقة موازية للحرب التقليدية كما حدث في حالة الحرب الجورجية الروسية في أغسطس 2008.

1- حالة يوغسلافيا السابقة و تطور الحرب الإلكترونية: [1]

أثناء هجمات حلف الأطلسي عام 1999 على يوغسلافيا إستخدمت الحرب السيبرانية في أول أيام الحرب لخلع الرئيس سلوبودان ميلوسيفيتش. ولم ترصد قنابل أو صواريخ في الأجواء، حتى الدوي لم يكن مسموعا وجاء إعلان وزارة الدفاع الأمريكية أن سلاحا جديدا تمت تجربته للمرة الأولى في أرض معركة حقيقية و يستهدف هذا السلاح شبكات الإتصالات و يعطلها ما يؤدي تلقائيا لتوقف شبكات الجيش[2]، و هذا ما حصل مع الجيش اليوغسلافي الذي تعطل نظام كمبيوتر أساسي لديه نتيجة ما أسماه الإعلام اليوغسلافي بصاعقة كهربائية دخلت شبكة الإتصالات و إنتشرت في كل نقطة تتصل بها و من ضمنها الكمبيوترات العسكرية و أدى الهجوم لتوقف الشبكة الرئيسية في يوغسلافيا، و توقف نظم الكمبيوتر الخاصة بالدفاع الجوي، التي كانت مهمتها إستهداف طائرات حلف الأطلسي بالصواريخ.

و حدث إستهداف لشبكة الهاتف الرئيسية بهدف دفع القيادة الصربية في بلجراد إلى الإتصال بقواتها عن طريق الخلوي حيث رصد المكالمات و مراقبتها و أتاح الفرصة للتجسس من مركز إيشلون الأمريكي للتنصت و المراقبة الموجود في أوروبا، و كانت مراقبة الإتصالات الخلوية أسهل لأن عدد حملة الهاتف المحمول في يوغسلافيا يومها كان يقتصر على أركان النظام الحاكم و رجال الأعمال([3]).

2 . حالة روسيا و الولايات المتحدة :

يعلن الإعلام الأمريكي أسبوعيا عن عملية سرية أخرى للخدمات الخاصة الروسية في شبكة الإنترنت. بحيث يولي القراصنة الروس إهتمام كبير بإختراق خوادم الهيئات الإدارية للحزبين الديمقراطي والجمهوري، وسرقة

---

[1] لمزيد من المعلومات انظرموسوعة مقاتل، في :
http://www.moqatel.com/openshare/Behoth/Askria6/ElectroWar/sec29.doc_cvt.html .(2017/1/30)

[2] Florian Bieber, ***Cyber war or Sideshow? The Internet and the Balkan Wars***, (**Philadelphia ,**Mar 1, 2000). p124

[3] Bieber, ***op.cit***.p122.

البرامج الخبيثة من وكالة الأمن القومي الأمريكية، وتنفيذ هجوم على قاعدة البيانات العالمية لوكالة مكافحة المنشطات، ومتهمة كذلك بنية تعطيل عملية فرز الأصوات في الإنتخابات الرئاسية في الولايات المتحدة([1]).

وقد كان القراصنة الصينيون هم أشرار الأنترنت في وسائل الإعلام الأميركية من خلال مسارعتهم في البحث عن الأسرار التجارية. ولكن لا يكاد الصينيون يُذكرون الآن، أمام الإجتياح الروسي .

إتهم القراصنة الروس بإختراق خادم البريد الإلكتروني للجنة الوطنية للحزب الديمقراطي الأمريكي، وتسريبها لـ"ويكيليكس" مع آلاف رسائل البريد الإلكتروني التي تحتوي على معلومات حساسة([2]).

موسكو أعلنت عدم صلتها بهذه الحوادث. وأكد فلاديمير بوتين في مقابلة أجراها مؤخرا مع "بلومبرغ"، أنه لا يعرف شيئا حول هذا الموضوع.

لا يعتبر السياسيين والخبراء الأمريكيين إمكانية التأثير الروسي على حملتهم الإنتخابية غير مهمة. فظهرت نداءات لمساءلة الروس. على سبيل المثال، فرض عقوبات جديدة ضد موسكو. ولحسن الحظ، الحق في فرض تدابير تقييدية ردا على هجمات سيبرانية من قبل دولة أخرى، يملكه فقط الرئيس باراك أوباما بعد أن منح نفسه هذه الصلاحية في العام 2015. ([3]).

[1] "الفضاء السيبراني.. ساحة حرب جديدة قد تشعل العالم"،في: ***http://katehon.com/ar/article/lfd-lsybrny-sh-hrb-jdyd-qd-tshl-llm*** (2017/4/30).

[2] **المكان نفسه.**

[3] **المكان نفسه.**

خلاصة الفصل الثاني :

أدى الإعتماد المفرط على الفضاء السيبراني إلى إنكشاف أمني لجميع الدول ،خاصة تلك التي وضفت التكنولوجيات الحديثة في تسيير أمورها ،وإستغلت الدول والتنظيمات الإرهابية هدا الإنكشاف في تمرير أهدافها وتحقيق إستراتيجيات كان من الصعب تحقيقها في غياب هده الوسائل التكنولوجية .

ومن تم برز صراع دولي حامي الوطيس في الفضاء السيبراني ،سواء من خلال السعي إلى شن هجمات على مواقع دولية والتأثير في البنية التحتية المعلوماتية أو من خلال السعي وراء حماية هده البنية التحتية من هجمات سيبرانية أكثر خطورة من الهجمات التقليدية .

وهنا برز دور أجهزة الإستخبارات الدولية في التنافس من أجل ممارسة نشاطات تخريبية أو حمائية في هدا الفضاء ،وظهر دلك جليا من خلال سعي جهاز الإستخبارات الأمريكي لتقصي أثار محاولات توظيف الأجهزة الإلكترونية في شن هجمات على الولايات المتحدة ، وسلكت هدا النهج جميع أجهزة الإستخبارات الدولية.

في خضم هدا التنافس الدولي ،وجدت التنظيمات الإرهابية غايتها في هدا الفضاء خاصة بالنظر إلى المزايا العديدة التي يوفرها من سهولة الإستخدام وصعوبة تقفي أثارهم ،و برز دلك من خلال سعي تنظيم القاعدة إلى جلب أعداد من المتطوعين ،ونشر بياناته ،وشن هجمات على مواقع حكومية في العديد من الدول ،وسلك تنظيم داعش نفس النهج لكن بوسائل متطورة وبتقنيات أكثر حداثة.

كل هدا الوضع ولد أنماط من الصراعات الساخنة والباردة بحيث تجسدة حروب سيبرانية حقيقية من خلال شن هجمات دولية على البنية التحتية مثلما حدث في الحالة اليوغسلافية او من خلال شن هجمات مجهولة المصدر مثلما حدث في إستونيا .

أمام الأخطار التي نتجت عن توظيف الفضاء السيبراني في التفاعلات الدولي ،وإدراك جميع الفاعلين في هدا المجال بإستحالة التصدي للأخطار الناتجة عن دلك،كان لزاما على المجتمع الدولي السعي وراء إيجاد ميكانيزمات كفيلة بمحاصرة العمليات الهدامة في الفضاء السيبراني وإيجاد صيغ قانونية وتقنية كفيلة بالحد من التأثيرات السلبية للظاهرة على الأمن والسلم الدوليين .

وسنتناول في هدا الفصل الجهود الدولية لمكافحة ظاهرة الإرهاب السيبراني إنطلاقا من الجهود المبدولة في إطار هيئة الأمم المتحدة وصولا إلى إبراز مختلف العراقيل التي تقف وراء ايجاد حلول جدرية لهده الظاهرة وكدا التحديات المستقبلية الناتجة عن تزايد توظيف الفضاء السيبراني في التفاعلات الدولية بمختلف اشكالها من أجل دلك قسمنا هدا الفصل إلى ثلاث مباحث.

نستعرض في المبحث الأول **الجهود المبدولة في إطار هيئة الأمم المتحدة** لاسيما من خلال القمة العالمية لمجتمع المعلومات وكدا الإتحاد الدولي للإتصالات أما المبحث الثاني **فنستعرض فيه جهود ومبادرات الفاعلين في مجتمع المعلومات العالمي** من خلال إبراز مختلف الجهود التي قامت بها بعض الدول المسيطرة على هدا المجال ومختلف المبادرات التي برزت كحلول لهده الظاهرة ، وفي المبحث الثالث نوجز **بعض الأساليب المختلفة لمعالجة هده الظاهرة** من خلال إبراز اساليب الوقاية وأساليب العلاج .

المبحث الأول : جهود هيئة الأمم المتحدة :

أدت الأخطار الناتجة عن الإرهاب السيبراني وتعدُّد الفاعلين وتنامي درجات الخطر إلى الحاجة إلى دور الأمم المتحدة عبر منظماتها وجهودها، لما تتمتع به المنظمة الدوليَّة –لدرجة ما– من مصداقية في مجال تعزيز التعاون الدولي. من أجل ذلك تم التطرق لجهود الأمم المتحدة من خلال إبراز الأمن السيبراني في أجندات هيئة الأمم المتحدة والحديث عن دور القمة العالمية لمجتمع المعلومات وإدارة الإنترنت، وكدا الإتحاد الدولي للإتصالات والمبادرة الخاصة بالأمن الإلكتروني.

المطلب الأول : الأمن السيبراني في أجندات هيئة الأمم المتحدة:

إن ميثاق الأمم المتحدة لم ينصّ صراحة على تجريم إستخدام حرب المعلومات كأداة إرهابية أو ما يُعرف بالإرهاب السيبراني؛ نظرًا لأن روح الميثاق تتفق مع تجريم إستخدامه بإعتباره يمثل إنتهاكًا لما ورد في الميثاق بخصوص "التهديد أو إستخدام القوة ضد السلامة الإقليمية أو الإستقلال السياسي لأي دولة".

ولدلك فالإرهاب السيبراني وحرب المعلومات تقع ضمن ميثاق ومقاصد الأمم المتحدة، كما ورد في الفصل السابع من ميثاق الأمم المتحدة فيما يتخذ من الأعمال في حالات تهديد السلم والإخلال به ووقوع العدوان في المادة 39 التي تنصُّ على: "يقرر مجلس الأمن ما إذا كان قد وقع تهديد للسلم أو إخلال به أو كان ما وقع عملا من أعمال العدوان، ويقدم في ذلك توصياته أو يقرر ما يجب إتخاذه من التدابير طبقًا لأحكام المادتين 41 و42 لحفظ السلم والأمن الدولي أو إعادته إلى نصابه"(1).

وجاء في المادة الثانية فقرة (3) من ميثاق الأمم المتحدة ما نصُّه: "يفضُّ جميع أعضاء الهيئة منازعاتهم الدولية بالوسائل السلمية على وجه لا يجعل السلم والأمن والعدل الدولي عرضة للخطر".(2)

بعد أحداث الحادي عشر من سبتمبر 2001 وفي نطاق الأمم المتحدة أنشئت لجنة لمواجهة الإرهاب ، طلبت من مكتب الأمم المتحدة للمخدرات والجريمة في فيينا وضع إرشادات للدول عند تشريع وتطبيق وسائل محاربة الإرهاب. ومن أجل لذلك وضع المكتب سنة 2006 قائمة بالإرشادات تضمنت أربعة أقسام: الأول منها في الأعمال المجرَّمة، الثاني في الوسائل التي تضمن التجريم الفعال، الثالث في القانون الإجرائي، الرابع في وسائل التعاون الدولي في المسائل الجنائية. ووضع المكتب في نهاية الإرشادات مشروع قانون ضد الإرهاب.([3])

و عبر الجمعية العامة أصدرت الأمم المتحدة عددًا من القرارات التي تبين مدى تصاعد الإهتمام العالمي بإستخدام تكنولوجيات الإتصال و الإعلام وإستخدامها إستخدامًا غير سلمي. جاء ذلك عبر سلسلة من القرارات، التي منها: قرار الجمعية العامة في الدورة 28/55 في ديسمبر 2000، والدورة 19/56 في 19 من ديسمبر 2001 بشأن إرساء الأساس القانوني لمكافحة إساءة إستعمال تكنولوجيا الإتصال والمعلومات

1 المادة 39 من الفصل السابع من ميثاق الأمم المتحدة

2 المادة 2 فقرة 3 من الفصل الاول لميثاق الأمم المتحدة.

3 عبد الصادق ،" الأمم المتحدة ودعم الإستخدام السلمي للفضاء الإلكتروني" ، ***مرجع سابق*** .(موقع إلكتروني)

في أعمال إجرامية. وجاءت القرارات في الدورة 70/53 في 4 من ديسمبر 1998 وفي الدورة 49/54 في ديسمبر 1999، والدورة 28/55 في 20 من نوفمبر 2000، والدورة 19/56 في 29 من نوفمبر 2001، والدورة 53/57 في 22 من نوفمبر 2002 بشأن التطورات الحادثة والمتوقعة في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي([1]).

و يدعو القرار جميع الدول إلى: مواصلة موافاة الأمين العام بتقييمها لمسائل أمن المعلومات، تعريف المفاهيم الأساسية المتصلة بأمن المعلومات، دراسة الأخطار القائمة والمحتملة في مجال أمن المعلومات والتدابير التعاونية التي يمكن إتخاذها للتصدي لها، العمل على تشكيل فريق من الخبراء الحكوميين(2).

وفي الدورة 199/58 المنعقدة بتاريخ 23 من ديسمبر 2003جاء قرار الجمعية العامة للأمم المتحدة بإرساء ثقافة عالمية للأمن الإلكتروني. بما يمثل واحدًا من القرارات المهمة التي إستهدفت: العمل على حماية البنية التحتية الحيوية للمعلومات، حثَّ وتفعيل دور المنظمات الدولية ذات الصلة، دعوة الدول إلى وضع إستراتيجيات لتقليل حجم التعرض للأخطار التي تشكل تهديدًا للبنية التحتية الحيوية للمعلومات(3).

وفي 31 من يناير 2002اتخذت الجمعية العامة للأمم المتحدة في الدورة 258/56 قرارًا يدعو إلى إستخدام تكنولوجيا الإتصال والمعلومات من أجل التنمية(4). هذا بالإضافة إلى قرارين صدرا من الجمعية العامة للأمم المتحدة بالدعوة إلى القمة العالمية لمجتمع المعلومات في دورتها 56 في 31 من يناير 2002والدورة 57 في 31 من يناير 2003(5).

وعلى الرغم بعض النجاحات، فإنها فشلت في التوصل إلى مسودة للقرار، وإصطدمت بإشكالية في حالة الإستخدام العدائي لتكنولوجيا الإتصال والمعلومات عن طريق توظيفها للأغراض العسكرية والسياسية إذا ما كان القانون الدولي الإنساني أو القانون الدولي تحديدًا يمكنه أن ينظم الأبعاد الأمنية للعلاقات الدولية. ومن ثمَّ أصبح عمل مجموعة الخبراء الحكومية الدولية، بلا جدوى على الرغم من نجاحها بداية في رفع حالة

[1] عبد الصادق ،" الأمم المتحدة ودعم الإستخدام السلمي للفضاء الإلكتروني "، ***مرجع سابق***. (موقع إلكتروني)
[2] قرار الجمعية العامة للأمم المتحدة في الدورة 53/57، الصادر في 22 من نوفمبر 2001.
[3] قرار الجمعية العامة للأمم المتحدة 199/58 المؤرخ في 23 من ديسمبر 2003.
[4] قرار الجمعية العامة للأمم المتحدة في الدورة 258/56 الذي تم اتخاذه في 4 من أبريل 2002.
[5] للمزيد حول وثائق القمة العالمية لمجتمع المعلومات والبيان الختامي لها والأعمال التحضيرية يمكن الرجوع إلى: ***http://www.un.org/arabic/conferences/wsis/docs.htm***،(2017/3/12).

الوعي بأمن المعلومات على الأجندة الدولية. وقد قررت الجمعية العامة للأمم المتحدة إستمرار جهودها لدراسة هذه المشكلة، والعمل على إنشاء مجموعة خبراء تبدأ عملها في عام 2009.(1)

وفي إطار المساعي الأممية لإيجاد حلول لمشاكل إدارة الأنترنت شكَّل الأمين العام للأمم المتحدة "كوفي عنان" في بداية العام 2004 ، فريقًا دوليًّا لدراسة قضية إدارة الإنترنت، وقد إنتهى فريق العمل إلى إيجاد أربعة تصورات، يتبلور التصور الأول في: إقامة مجلس عالمي للإنترنت يتألف من أعضاء الحكومات ويوفر تمثيلا مناسبًا عن كل منطقة ويكون له علاقة بمؤسسات الإنترنت وربطه بالأمم المتحدة، ويكون للقطاع الحكومي دور قيادي وللقطاع الخاص والمدني دور استشاري. والتصور الثاني تمثل في توسيع دور اللجنة الاستشارية الحكومية لهيئة الإنترنت. ودعا التصور الثالث إلى: تشكيل مجلس دولي للإنترنت ينهض فيما يتعلق بالسياسات التي تمسُّ المصالح الوطنية للدول عبر الوظائف الموازية لاختصاص هيئة الإنترنت. أما التصور الرابع فقد اقترح إقامة ثلاثة كيانات مؤسسية عالمية لمعالجة إدارة ورسم السياسات، الإشراف على الهيئة والتنسيق العالمي. هذه التصورات الأربعة عكست رغبة ضمنية في التخفيف من سطوة الولايات المتحدة على عمل الشبكة، التي أصبحت وسيلة لا غنى عنها للعالم كله([2]).

إلى جانب المواقف الحكومية، أخذ العديد من منظمات المجتمع المدني الدولي في ممارسة الضغوط في سبيل إنهاء السيطرة الأمريكية على الإنترنت، باعتبارها تمثل تهديدًا للحقوق الرقمية، التي من ضمنها: الحقُّ في تداول المعلومات ونقلها، حرية التعبير والمشاركة الإتصالية، حرية الإختيار والدخول، الحقُّ في الخصوصية (التي تم تضمينها في التشريعات الإنسانية الكبرى مثل: الإعلان العالمي لحقوق الإنسان، الميثاق الدولي للحقوق المدنية والسياسية، إتفاقية الحقوق والحريات الأمريكية، الميثاق الأفريقي لحقوق الإنسان والشعوب، الإتفاقية الأوروبية لحماية حقوق الإنسان وحرياته الأساسية، بالإضافة إلى العديد من المواثيق والدساتير الإقليمية).(3)

---

[1] See :General Assembly, ***Developments in the Field of Information and Telecommunications in the Context of InternationalSecurity***, (UN :document A/RES/61/54, 19 December 2006).

[2] عادل عبد الصادق ، "الأمم المتحدة ودعم الإستخدام السلمي للفضاء الإلكتروني" ، ***مرجع سابق.*** (موقع إلكتروني).

[3] عادل عبد الصادق، "قمة تونس العالمية للمعلومات: إستمرار الوضع الراهن!" ، في :***www.ahram.rg.eg/acpss/Ahram\2005\11\22\COMM0.HTM*** (2017/1/12)***.***

في 15 من مايو 2006تحديدًا جاء أول تصريح رسمي فيما يتعلق بالإرهاب السيبراني في رسالة أمين عام الأمم المتحدة "كوفي عنان" جاء فيه "في عالم يتزايد فيه الترابط وإقامة الشبكات، أضحى من المهم للغاية ضمان سلامة نظمنا وهياكلنا التحتية الحيوية من هجمات مجرمي الفضاء الإلكتروني، والعمل في الوقت نفسه على بثِّ الثقة في التعاملات الإلكترونية وغيرها من الخدمات والتطبيقات الإلكترونية الأخرى"([1]).

تمحور موقف الأمم المتحدة عبر أمينها العام حول أنه "طالما يتوقف الأمر على الممارسات الأمنية، التي يتبعها كل من البلدان والشركات والمواطنين المرتبطين بالشبكات، فإن هذا يجعل الخطر ذا طابع دولي يتطلب إرساء ثقافة عالمية لأمن الفضاء السيبراني". وعليه طالب كوفي عنان الدول الأعضاء وأصحاب المصلحة بالمساعدة في زيادة الوعي العالمي بأمن الفضاء السيبراني ،ودلك عن طريق إنشاء شبكة دولية للمبادرات والتدابير المضادة القائمة على تكنولوجيا المعلومات والإتصالات لتعزيز الأمن وبناء الثقة في إستعمال تكنولوجيات المعلومات والإتصالات. وأكد الأمين العام أن هذا الأمر لا مناص منه لإستمرار نمو الإقتصاد الدولي وتطوره خاصة بالنسبة للبلدان النامية.(2)

في نفس السياق ، تمَّ إستحداث منصب رئيس مكافحة الإرهاب الجديد في الأمم المتحدة ومساعد الأمين العام، ومنوط به تعزيز القدرة على مكافحة الإرهاب بين الدول الأعضاء، وتشجيع التعاون بشأن الإجراءات التي يقررها مجلس الأمن.(3)

المطلب الثاني :القمة العالمية لمجتمع المعلومات وإدارة الإنترنت:

القمة العالمية لمجتمع المعلومات، هو مؤتمر برعاية الأمم المتحدة حول المعلومات والإتصالات، جرت القمة مرتين الأولى في جنيف في ديسمبر 2003 إنتهت بدون ضمان إتفاق نهائي حول إدارة حكم الأنترنت

[1] عادل عبد الصادق ، الأمم المتحدة ودعم الإستخدام السلمي للفضاء الإلكتروني ، ***مرجع سابق***(موقع إلكتروني).

[2] كان ذلك في رسالة الأمين العام "كوفي عنان" بمناسبة توقيع مدير عام المنظمة الإسلامية للتربية والثقافة والعلوم (إيسيسكو)، عبد العزيز عثمان التويجري، ومدير عام منظمة التربية والعلوم والثقافة (يونسكو)، كويشيرو ماتسورا، في 15 من مايو 2006 في باريس، برنامج تعاون جديدًا لعامي 2006-2007 .للمزيد يمكن الاطلاع على الرابط التالي : (2017/4/20).***http://www.un.org/arabic/news/fullstorynews.asp?newsID=5690***

[3] للمزيد حول شروط التدابير المضادة وعناصرها وأهميتها في تعزيز الأمن الجماعي أنظر: .عابدين عبد الحميد حسن قنديل، "التدابير المضادة في النظام القانوني الدولي: دراسة نظرية وتطبيقية"، رسالة دكتوراه غير منشورة، (جامعه القاهرة: كلية الاقتصاد والعلوم السياسية،2011)، ص ص 427-433.

بعدما عارضت الو م أ مقترح الإتحاد الأوربي الرامي إلى وضع نموذج جديد للتعاون في مجال الإنترنت والذي سينهي هيمنة الولايات المتحدة على الأجزاء الحيوية من الأنترنت والثانية في تونس نوفمبر 2005 والتي أقرت بعض المبادئ والقرارات التي من شأنها تفعيل الأهداف التي انعقدت من أجلها والتأكيد على ضرورة التعاون بين البلدان من أجل تسخير التكنولوجيات الحديثة لخدمة البشرية وإلتزامها بإنجاز مقررات القمة.

إتفقت جميع الحكومات في المرحلة الأولى للقمة العالمية في ديسمبر 2003 على أن: "السلطة السياسية على قضايا السياسات العامة المتصلة بالإنترنت تعتبر حقًّا سياديًا للدول؛ إذ تملك حقوقًا ومسئوليات بشأن قضايا السياسات العامة الدولية المتصلة بالإنترنت". وطالبت حكومات الدول الأمين العام للأمم المتحدة بضرورة البحث في مسألة إدارة الإنترنت بدءًا من (صياغة تعريف لهذه العبارة) كنقطة إنطلاق للبحث في غير ذلك من الموضوعات.(1)

وترى الولايات المتحدة أنه لا يمكنها أن تضحى بسيطرتها على عملية تنظيم أسماء المواقع على الشبكة لجهاز بيروقراطي مجهول، لاسيما وأن الدول النامية التي طرحت مطلبها بالمشاركة في إدارة الإنترنت لم تكن على أتمِّ الاستعداد سواء من الناحية الفنية أو السياسية. والمرجح أنها كانت تهدف إلى الضغط على الولايات المتحدة وحلفائها لتوفير التمويل اللازم لصندوق التضامن الرقمي الذي عهدت به قمة جنيف على إثر اقتراح الرئيس السنغالي.([2])

كانت هناك جهود دولية لإخضاع الشبكة الدولية للمعلومات لرقابة الأمم المتحدة وعلى الرغم من المساعي الدولية لسحب الرقابة الأمريكية على شبكة الإنترنت، فإنه واجه بعض الصعوبات التي تتمثل في تشدد الإدارة الأمريكية في موقفها.(3)

---

[1] هناك 13 خادمًا جذريًّا حتى الآن، 10 منها موجودة في الولايات المتحدة لأسباب تاريخية ليس إلا. وهي مثار جدل حتى في مسألة تعريفها وتحديد خصائصها العالمية والإقليمية على السواء. خاصة أن مطلب الدول في قمة جنيف الأولى كان توفير مسيرات خوادم إقليمية!! ولن تقم الدول بتحديد تعريف للخادم الجذري الإقليمي أو الدولي. ومع ذلك فإنه قبل انعقاد القمة تم استخدام نظام استنساخ الخوادم الجذرية حول العالم، فأضحى هناك أكثر من خادم يحوي ما هو موجود في الخوادم الـ13 المذكورة ذاتها. لذلك فالاعتقاد السائد الآن أن ما تردد في إعلان المبادئ في قمة جنيف هو تكرار وتحصيل حاصل.

[2] عادل عبد الصادق ، "التخلي الأمريكي عن منظمة "الأيانا"و فرص التحول الى التعددية في إدارة الأنترنت"،في : ***http://www.accronline.com/print_article.aspx?id=18816*** (2017/4/4).

[3] عبد الصادق، "قمة تونس العالمية للمعلومات: إستمرار الوضع الراهن"، ***مرجع سابق***.(موقع إليكتروني).

ومن أجل تحقيق هده المساعي تمَّ إستعراض نماذج تنظيمية مختلفة ، ووقع الإختيار على أربعة نماذج لكي تكون موضوعًا للبحث والنظر. وشملت هذه الخيارات: سيناريوهات مختلفة يدعو بعضها إلى مزيد من التدويل للإشراف على الإنترنت، مع تعزيز المشاركة الحكومية، لاسيما ما يخصُّ مسائل السياسة العامة، وفقًا لما تنشده بلدان كثيرة.. أو إنجاز ذلك في سياق الهياكل القائمة، و تحبذ الولايات المتحدة وبعض الحكومات الأخرى. ولم يقترح أيٌّ من هذه الخيارات أن تتولى الأمم المتحدة دور الهيئات التقنية المعنية بإدارة موارد الإنترنت، ولم يؤيد أي منها إنشاء وكالة جديدة تابعة للأمم المتحدة؛ بل إن بعضها لم يشر قط إلى دور للأمم المتحدة(1).

كان من أهم نتائج القمة العالمية لمجتمع المعلومات التي عُقدت في تونس 2005: العمل على إيجاد مدخل رعاية صحية تفاعلي لتبادل البيانات بين البلدان منخفضة الدخل ومرتفعة الدخل، وضع نظم للتنبؤ بالكوارث الطبيعية والكوارث الناجمة عن النشاط البشري، رصد التأثيرات البيئية وتطوير مشاريع للتخلص الآمن بيئيًّا من معدات الحاسوب وإعادة تصنيعها، إقامة شراكات لتبادل المعلومات بشأن الزراعة ومصائد الأسماك والغابات، وضع إجراءات وقائية للأمن الحاسوبي بالتركيز على المصارف لإجراء معاملات موثوق بها مباشرة على الإنترنت، تشجيع البلدان على صياغة تشريعات أمنية تتعلق بتكنولوجيا المعلومات، إقامة جهاز اتصال لمعالجة الحوادث والاستجابة لها في الوقت الحقيقي، وضع شبكة تعاونية لتبادل المعلومات.(2)

المطلب الثالث : مبادرة الإتحاد الدولي للإتصالات للأمن الإلكتروني:

طرأت العديد من التطورات على قانون الاتصالات ليصبح الآن قانون إتصالات حديثًا تحت قيادة الاتحاد الدولي للإتصالات([3])، والذي تحوَّل لمنظمة متخصصة في تكنولوجيا المعلومات والإتصال. وتنصُّ المادة 35 من ميثاق الإتحاد الدولي للإتصالات على عملية التدخل في عمل الإتصالات.

وجاء في الإعلان الخاص بالقمة العالمية لمجتمع المعلومات(1) "بناء الثقة والأمن في إستخدام تكنولوجيا الإتصال والمعلومات". وقد تولى الإتحاد الدولي للإتصالات القيام بهذه المهمة. وإنطلاقًا من ذلك، دعَّم

[1] للمزيد حول هذا الموضوع يمكن الاطلاع على وثائق القمة العالمية لمجتمع المعلومات في دورتيها الأولى والثانية على الموقع التالي : ***http://www.un.org/arabic/conferences/wsis*** (2017/4/5).

[2] عبد الصادق، "قمة تونس العالمية للمعلومات: استمرار الوضع الراهن"، ***مرجع سابق***.(موقع إلكتروني).

[3] للإطلاع على نبدة عن الإتحاد الدولي للإتصالات أنظر :
http://www.itu.int/ar/about/Pages/default.aspx(2017/4/5).

الإتحاد الدولي التعاون ما بين الشركات الخاصة والقطاع العام من أجل: تنسيق الجهود، العمل على تبني إستراتيجية عالمية للأمن الإلكتروني، إنشاء بوابة إلكترونية للأمن الإلكتروني.

أصبح الإتحاد الدولي للإتصالات بمثابة ملتقى دولي رئيسي لهذه الأنشطة، وتم عقد المؤتمر الإقليمي حول الأمن الإلكتروني بالتعاون مع الإتحاد الدولي للإتصال في قطر في فبراير من العام 2008، الذي جاء ضمن إحدى توصيات إعلان الدوحة الصادر عن المؤتمر العالمي لتنمية الإتصالات المنعقد بالدوحة في مارس من العام 2006.

وقد إعتمد المؤتمر الدوحة ما يسمى بـ"خطة عمل الدوحة"، ويقوم فريق عمل رسمي من الإتحاد الدولي للإتصالات بتطوير "تقرير حول أفضل الممارسات لمنهج وطني للتعامل مع قضايا الأمن الإلكتروني".[2]

تمَّ الحث على إقامة تعاون بين الحكومة والصناعة ووضع إستراتيجية وطنية للأمن الإلكتروني في مواجهة الجريمة الإلكترونية، إستحداث إدارة وطنية لإدارة الحوادث، دعم الحوار في الأمن الإلكتروني. وأقرَّ المؤتمر دعوة جميع الدول لوضع وتنفيذ إطار وطني للأمن الإلكتروني وحماية البنية التحتية الحرجة للمعلومات، والتي تُعَدُّ بمثابة خطوة أولى في سبيل التصدي للتحديات التي تواجهها جراء إتصالها بتكنولوجيا المعلومات والإتصال.[3]

كان تأمين الشبكات من أهم نتائج القمة العالمية لمجتمع المعلومات، وتم تعيين الإتحاد الدولي للإتصالات بوصفه الميسِّر (المسيِّر) الوحيد لخط العمل (ج 5)، "بناء الثقة والأمن في إستعمال تكنولوجيا المعلومات والإتصالات".

ويمكن للهجمات الإلكترونية أن تُلحق أضرارًا هائلة ببلدان متعددة في غضون دقائق معدودات[4].

---

[1] للمزيد حول إعلان القمة يمكن الاطلاع على موقع القمة على الإنترنت على العنوان التالي:
www.un.org/arabic/conferences/wsis(2017/4/5)

[2] See ITU website: ***http://www.itu.int/net/about/index.aspx***(2017/4/5)

[3] المجلس الأعلى للاتصالات وتكنولوجيا المعلومات في قطر يمكن زيارة موقعه على الإنترنت على العنوان التالي:
http://www.ict.gov.qa/output/Page635.asp (2017/4/5).

[4] للمزيد حول الإعلان الختامي للمؤتمر يمكن الاطلاع عليه على الرابط التالي:
http://www.ituarabic.org/2008/CIIP/Doha_Declaration.pdf.(2017/4/5)

وقد مكّنت أعمال الإتحاد في مجال التصديق الإلكتروني الولايات القضائية حول العالم من الإعتراف بوثائق البريد الإلكتروني بإعتبارها مستندات قانونية، ومن منح التوقيعات الإلكترونية صفة قانونية. وينفرد قطاع تقييس الإتصالات في الإتحاد بوضع يهيئ له أن يجمع بين القطاع الخاص والحكومات لتنسيق الأعمال في مجال مواءمة السياسات الأمنية العامة والمعايير الأمنية حول العالم.

ويعمل الإتحاد بصورة وثيقة مع المنظمات الأخرى المعنية على: وضع المعايير المتعلقة بالأمن ورصد الأعمال المضطلع بها في مجال الأمن، كما يستضيف ورشة عمل مشتركة تُعقد بصورة منتظمة لتنسيق الأعمال بين مختلف المنظمات الأخرى المعنية بوضع المعايير. ويقوم الإتحاد، بالإشتراك مع الوكالة الأوروبية لأمن الشبكات والمعلومات، وفريق التوجيه المعني بأمن الشبكات والمعلومات، بنشر خريطة الطريق المتعلقة بمعايير الأمن في مجال تكنولوجيا المعلومات والاتصالات، التي تسلّط الضوء على: المعايير الحالية، الأعمال الجارية، المعايير المتوخاة في المستقبل فيما بين المنظمات الرئيسة المعنية.

وتنشر اللجنه بإنتظام دليلا أمنيًّا بشأن "الأمن في تكنولوجيا المعلومات والإتصالات" وهو يعد بمثابة إستعراض عام للمسائل الأمنية وتوصيات قطاع تقييس الإتصالات بالإتحاد من أجل تأمين الإتصالات (صدرت النسخة الثالثة من هذا الدليل في أغسطس من العام 2006)، وعلاوة على نشر خلاصة أمنية تتضمن قائمة بالتوصيات التي أقرّها قطاع تقييس الإتصالات بالإتحاد فيما يتصل بأمن الإتصالات. ويسعى الإتحاد الدولي للإتصالات اللاسلكية ITU –الذي يضم بين صفوفه 191 دولة تستخدم نظام الهاتف العالمي– إلى أن يأخذ زمام المبادرة للمطالبة بمعاهدة عالمية ضد الجريمة الإلكترونية، بالإضافة إلى المبادرات الدولية السابقة.[1]

ويشارك الإتحاد أيضًا في تقديم المساعدة التقنية المباشرة من أجل بناء قدرات الدول الأعضاء –ولاسيما البلدان النامية– على تنسيق الإستراتيجيات الوطنية وحماية البني التحتية للشبكات ضد المخاطر. ويلزم وضع أطر عمل وإستراتيجيات وطنية تتيح لأصحاب المصلحة إستعمال جميع الأدوات التقنية والقانونية والتنظيمية المتاحة في مجال تعزيز ثقافة للأمن الإلكتروني.

[1] الإتحاد الدولي للإتصالات - **التقرير السنوي للإتحاد**، 2007، ص38، في :
ttp://www.itu.int/aboutitu/annual_report/2007/pdf/2007-ar.pdf.(2017/4/5)

وطالبت القمة العالمية لمجتمع المعلومات في تونس في نوفمبر 2005، بأن ينسق الإتحاد الدولي للإتصالات آلية لبناء الثقة والأمن في مجال إستخدام تكنولوجيا الإتصال والمعلومات. ويوفر الإتحاد الدولي للإتصالات المنظور العالمي والخبرة المطلوبة لمواجهه التحديات، وأطلق برنامج الأمن الإلكتروني العالمي.

توجد خمس ركائز لبرنامج الأمن الإلكتروني العالمي للإتحاد الدولي للإتصالات([1])، هي: التدابير القانونية، التدابير التقنية والإجرائية، الهياكل التنظيمية، بناء القدرات، التعاون الدولي.

ويتضمن البرنامج سبعة أهداف إستراتيجية، هي:

1. وضع إستراتيجيات لإستحداث تشريع نموذجي لمكافحة الجريمة الإلكترونية يمكن تطبيقه عالميًا وقابل للإستخدام مع التدابير التشريعية القائمة على الصعيدين الوطني والإقليمي.

2. وضع إستراتيجيات عالمية لإيجاد الهياكل التنظيمية والسياسات العامة الملائمة على الصعيدين الوطني والإقليمي بشأن الجريمة الإلكترونية.

3. وضع إستراتيجية لصوغ معايير أمنية دنيا وخطط إعتماد للأجهزة والبرمجيات والأنظمة تكون مقبولة عالميًا.

4. وضع إستراتيجيات لإيجاد إطار عالمي للرصد والإنذار والإستجابة للحوادث؛ لضمان التنسيق عبر الحدود بين المبادرات الجديدة والقائمة.

5. وضع إستراتيجيات عالمية لإنشاء وإقرار نظام هوية رقمية عام عالمي، والهياكل التنظيمية اللازمة لضمان الاعتراف بوثائق التفويض الرقمية عبر الحدود الجغرافية.

6. وضع إستراتيجيات عالمية لبناء القدرات البشرية والمؤسسية من أجل تعزيز المعارف والمهارات.

7. وضع مقترحات بشأن إطار لإستراتيجية عالمية لأصحاب المصلحة المتعددين لتحقيق التعاون والحوار والتنسيق على الصعيد الدولي في جميع المجالات ([2]).

[1] عبد الصادق ، "الأمم المتحدة ودعم الإستخدام السلمي للفضاء الإلكتروني" ، ***مرجع سابق***،(موقع إلكتروني).

[2] للمزيد حول إستراتيجية الإتحاد يمكن الإطلاع على الرابط التالي:

http://www.itu.int/osg/csd/cybersecurity/gca/overview/index.html(2017/4/5).

المبحث الثاني:الجهود والمبادرات الدولية لمكافحة الإرهاب السيبراني :

يتناول هذا المبحث فرص و تحديات تعزيز الأمن الإلكتروني الدولي و الذي شكل قضية دولية مرشحة للإهتمام المتصاعد في المستقبل مع تعاضم الإعتماد الدولي على تكنولوجيا الإتصال و المعلومات في المرافق الحيوية و يوضح من خلال تناول عدد من النقاط المحورية الهامة التي تتعلق بملامح المجتمع الدولي الحديث و مكونات تبني إستراتجية الأمن الإلكتروني الدولي .

و نستعرض أولا : الجهود الدولية في مكافحة الإرهاب الإلكتروني ، ثانيا : المبادرات الدولية لتعزيز أمن الفضاء السيبراني.

المطلب الاول : الجهود الدولية في مكافحة الإرهاب السيبراني.

كانت أول الجهود الدولية التي هدفت لمواجهة الجريمة الإلكترونية و الإرهاب تعود إلى ثلاثة عقود ماضية حين ناقش الأنتربول الدولي إمكانية إيجاد تشريع قانوني حول الجريمة الإكترونية في عام 1981 ([1]). و بدأ التقدم بطيئا و لكنه أخذ في التسارع ببطء بعد إنتهاء الحرب الباردة ، و لعل إنشاء معهد قانون الفضاء الإلكتروني في جامعة جورج تاون الأمريكية عام 1995 يدل على نمط المشكلة ، حيث يوجد ثلاثون متخصصا من الذين يعملون على تحديد كيفية التعامل مع مشكلات الفضاء الإلكتروني ([2]).

و سعت العديد من الدول العالم المتقدم الى تبني إستراتجية قومية في مجال تأمين الفضاء الإلكتروني فهناك من الدول من سن وقوانين و تشريعات وطنية تهدف الى تعزيز التعاون الدولي و الإقليمي في مجال المكافحة ، و تم تضمين خطر التعرض لهجمات الفضاء الإلكتروني ضمن إستراتيجيات الأمن القومي ، بل إتجه بعض مراكز الأبحاث إلى إنجاز مسودة إتفاق دولي تختص بتأمين الفضاء الإلكتروني مثل مسودة سيمون جودمان لإنجاز إتفاق دولي ، وفي عام 1997 قامت مجموعة الثماني الصناعية بإنشاء مجموعة فرعية للجريمة عالية التقنية وتبنت ما عرف بالمبادئ العشرة ([3]).

---

[1] Stein Schjolberg, Chief Judge, Moss Tingrett Court Norway, “Law Comes to Cyberspace,” ***A presentation at the 11th UN Criminal Congress***,(Bangkok, Thailand. Workshop 6: Measures to combat computer-related crime. Apr. 18-25, 2007),p23

[2] د وليد عبد الحي ،"***مداخلة بعنوان :إشكالية الفضاء الإلكتروني في حقوق الملكية الفكرية"*** ، المؤتمر العلمي الأول حول الملكية الفكرية ،جامعة اليرموك، الأردن، (10-2000/7/11) ،ص 2 .

[3] العدوان ،***مرجع سابق*** ،ص 10.

صدرت مسودة إتفاق عالمي حول الجريمة والإرهاب السيبراني في عام 2000 من جامعة إستاند فورد تظمنت خطة تشتمل على العديد من النقاط من أجل الوصول إلى إتفاق عالمي وتعاون دولي لتأمين الفضاء السيبراني وتضمنت المادة 12 من تلك الخطة إقتراح إقامة وكالة دولية لحماية البنية التحتية الكونية للمعلومات([1]).

وأخد الإهتمام العالمي يتزايد بعد 11 سبتمبر 2001 والتي أعقبها التوصل لإتفاقية مجلس أوروبا حول الجريمة الإلكترونية في نوفمبر 2001 وبعدها وضع البنتاغون خطة بعنوان خارطة الطريق لعمليات المعلومات وهي تستهدف مراقبة الإنترنت والتعامل معه كمنظومة سلاح معادية وعمل مكتب التحقيقات الفيدرالي على زيادة تحقيقاته حول الأمن المعلوماتي وشكل لجنة متابعة على مدار الساعة .

وأجرت الولايات المتحدة سنة 2002 محاكاة للتعرض لهجوم في الفضاء السيبراني سميت بيرل هاربر الإلكتروني بالإضافة إلى مشاريع أخرى مثل أيشلون وكارنيفور وغيرهما وإنتشرت في أجهزة الأمن الأمريكية المختلفة وحدات خاصة بالإرهاب السيبراني وقامت fbi بملاحقة المخترقين والقراصنة على أنواعهم ، اما سلاح الجو الأمريكي فأسس فرق هندسة الامن الإلكتروني ESETs ومهمتها محاولة إختراق أنظمة وشبكات عسكرية بحيث إستطاعت إختراق 30% من شبكات الأجهزة العسكرية في العالم .([2])

في نفس الإطار قامت الولايات المتحدة بإنشاء وزارة الأمن الداخلي في عام 2003 كخطوة ضمن الخوف المتزايد من تعرض البنى الحساسة لهجوم إلكتروني ،وظهرت مطالب داخل الولايات المتحدة بعد وصول أوباما للحكم بضرورة إستحداث منصب مساعد الرئيس لشؤون الإنترنت ودلك بعد عجز وزارة الأمن الداخلي عن مواجهة الإرهاب الإلكتروني([3]).

وفي إجتماع وزراء خارجية منظمة المؤتمر الإسلامي سنة 2007 في باكستان طرحت مصر مبادرة لإستصدار قرار لمكافحة إستخدام الإرهابيين لشبكة الأنترنت ونجحت السعودية في الإطاحة بثلاثة من رموز

---

[1] العدوان ،***مرجع سابق*** ،ص 10.

[2] عادل عبد الصادق ، ***الإرهاب الإلكتروني: القوة في العلاقات الدولية. نمط جديد وتحديات مختلفة***،(القاهرة: مركز الأهرام للدراسات السياسية والإستراتيجية ، 2009)،ص ص 348-361.

[3] **المكان نفسه.**

الترويج لتنظيم القاعدة ، وفي 18 افريل 2008 قرر وزراء العدل في الإتحاد الأوروبي تجريم التحريض على إرتكاب أعمال ارهابية عبر الأنترنت([1]) .

و تسعى روسيا لصياغة مقترحات للتشديد العقوبات على إستخدجام إرهابيين لشبكة الإنترنت ، و إتخاذ تدابير صارمة لإيقاف إنتشار أفكار الإرهاب و التطرف، و إقترح أحد الخبراء الروس إرساء جهاز للأمن على غرار جهاز يوروبول للشرطة الأروبية مكلفا بحراسة و مراقبة شبكة الإنترنت بما فيها عمليات التحايل و القرصنة التي تتعرض لها في المستقبل ، و قامت المفوضية الأروبية في بروكسل بتنظيم مؤتمر أروبي عام حول هذه المسألة في شهر نوفمبر 2008 و هو مؤتمر جمع مختلف الأجهزة الأمنية الأروبية و المتعاملين الرئسيين لشبكة الأنترنت و بعض الخبراء المختصين و المراقبين عن الدول الأجنبية([2]).

و تمتلك أروبا موحدة حاليا شبكة خاصة تسمى الوكالة الأروبية للأمن المعلوماتية enisa (the european network and information security agency) و مقرها أثينا باليونان و مكلفة بمراقبة القرصنة الإلكترونية داخل المجال الأمني الأوروبي و كانت المملكة المتحدة قد إقترحت قيام منظمة دولية للأمن (wso world) security organisation ، تعني بمكافحة هجمات الفضاء الإلكتروني و توفير الأمن للمستخدمين و الحكومات و ذلك على سياق الجهود الدولية في مواجهة الأخطار التي تأتي من مجالات الجو البحري و الفضاء و تم عقد إجتماع كان محل إهتمام رجال الأعمال و القطاع الخاص و أجهزة الإستخبار و الشركات العاملة في تكنولوجيا المعلومات و الأكاديميين و السياسيين ، و ذالك بهدف إطلاق مبادرة عالمية أقوى من الأنتربول" interpol" .([3])

وقد ركز المكتب الإتحادي للأمن و تكنولوجيا المعلومات الذي أسسته ألمانيا بشكل خاص على كل ما يتعلق بتأمين البنية التحتية لتكنولوجيا المعلومات . و قد خصصت وزارة الأمن الداخلي الأمريكي 5.12 مليون دولار عام 2004 للأمن الرقمي و في عام 2005 وصلت ل 5.17 مليون دولار و 15 مليون دولار عام 2006 و 2007 و هذا يعكس خطة أمنية إستراتجية ضد الإرهاب الإلكتروني([4]).

[1] عبد الصادق ،الإرهاب الإلكترونى: القوة فى العلاقات الدولية. نمط جديد وتحديات مختلفة ***،مرجع سابق،*** ص ص 348-361.

[2] **المكان نفسه.**

[3] Will Sturgeon," Cyber-terror plan panned as "barmy",in : ***http://www.crime-research.org/news/10.02.2005/952/,(***12/4/2017).

[4] Sturgeon,***op .cit***

و أخذت الجهود الإقليمية في الاهتمام على مستوى المنظمات كمنظمة المؤتمر الاسلامي التي تبنت الدعوة الى تجريم استخدام الانترنت في العمل الارهابي في قمتها ببكستان عام 2007 و كذالك على مستوى جامعة دول العربية و خاصة على مستوى اجتماعات وزاري الداخلية العرب .

المطلب الثاني : المبادرات الدولية لتعزيز أمن الفضاء الإلكتروني.

كان هناك العديد من المبادرات التي تم إتخاذها لمواجهة ظاهرة الإستخدام غير السلمي للفضاء الإلكتروني و تنوعت تلك المبادرات من جانب الحكومات و القطاع الخاص و المجتمع المدني و المنظمات الدولية و التي من أهمها و من ضمنها :

1.مبادرة الشراكة الدولية متعددة الأطراف لمكافحة الإرهاب الإلكتروني impact ([1])

في بادرة هي الأولي من نوعها في العلاقات الدولية أعلنت ماليزيا إطلاق مبادرة في مايو 2006 تحت مسمى " الشراكة الدولية متعددة الأطراف لمكافحة الإرهاب الإلكتروني impact و ذالك على هامش إنعقاد المؤتمر الدولي الخامس عشر حول تكنولوجيا المعلومات ، و تهدف هذه المبادرة لحشد الجهود الدولية من جانب القطاعات الحكومية و القطاع الخاص و المدني لمواجهة تزايد الأخطار التي يمثلها الإرهاب الإلكتروني ،كما هدفت المبادرة إلى جمع الرؤى و الأفكار حول التدريب وتبادل الخبرات ،وتعمل كمنظمة دولية غير هادفة للربح و تهدف إلى جمع الحكومات و القطاع الخاص و الأكاديميين و قادة صناع تكنولوجيا الإتصال و خبراء أمن المعلومات لدعم قدرة المجتمع الدولي في عملية الوقاية من الأخطار الإلكترونية و تمكنت تلك المبادرة من إنشاء أربعة مراكز هي مركز تنمية المهارات و التدريب و مركز لشهادات الأمن و البحث و التنمية و مركز دعم التعاون الدولي و مركز الإستجابة و الطوارئ الدولية ([2]). و جدبت تلك المبادرة العديد من الشركاء الدوليين و ضمت ما يزيد على300 عضوا من أعضاء الإتحاد الدولي للإتصالات ،من أجل تحسين قدرات العلم على مواجهة خطر الإرهاب عبر الأنترنت و تم عقد القمة الأولى للأمن الإلكتروني في العاصمة الماليزية كوالالمبور في 23مايو2008 وضمت خبراء من كافة دول العالم لبحث كيفية مواجهة الإرهاب الإكتروني.وتقوم مؤسسة "إمباكت"بالعمل على مساعدة أعضائها بالتدريب و بنتمية قدراتهم ،كما ستعمل على دعم القوانين و تطبيقها بشأن الإرهاب الإكتروني .و قد ساهمت ماليزيا

[1] عبد الصادق ، *"الإرهاب الإلكتروني: القوة في العلاقات الدولية. نمط جديد وتحديات مختلفة"* ،***مرجع سابق***،ص362 .

[2] New Global Partnership to Fight Cyber Terrorism Seeks the Business., Zeichner Risk Assessment Newsletters , "(Vol. 1, No. 30 - May 30, 2008) .

ماديا في إنشاء إمباكت ،وبقى دور الولايات المتحدة و أوروبا و دول الشرق الأوسط في تقديم المساعدة للمنظمة،إذ أن كل دول العالم المتحضر تشترك فيما بينها في الإهتمام بضرورة مواجهة أخطار الإرهاب الإلكتروني و حماية أمن و سلامة العالم القائم على تقنية المعلومات

2إنشاء مواقع على الإنترنت لمكافحة و الرصد و مراكز الأبحاث و الرصد و التحليل:

تم إنشاء العديد من مواقع الأنترنت لمكافحة الإرهاب الإلكتروني و الأمن الرقمي حيث أصبحت بمثابة مؤسسات فكرية و فنية لدعم الأمن الرقمي و كانت تلك المواقع إما بمبادرة حكومية أو من جانب القطاع الخاص أو من جانب المجتمع المدني .بالإضافة إلى مواقع الشركات العاملة في تكنولوجيا الإتصال و المعلومات. ([1])

3 تعزيز الإتفاقيات الدولية:

أكدت كافة التفاعلات الدولية على أهمية تفعيل الإتفاقية الأوروبية لمكافحة الجريمة الإلكترونية بإعتبارها تشكل الأساس الدولي للنظر في القوانين الوطنية بما يتلائم مع طرق مواجهتها،و خاصة أنه لاتوجد دولة واحدة لديها القدرة على السيطرة الكاملةعلى الفضاء الإلكتروني .([2])

4 المناورات و التدريب

في محاولة لإختبار جاهزية النظم الإلكترونية لمواجهة هذا الخطر قامت الولات المتحدة بعقد"مناورة إلكترونية" في فبراير2006 ([3]) لمدة أسبوع كامل ،و سميت بعاصفة الحواسب (cyber storm 1) ،حيث قامت بها أجهزة الإستخبارات الأمريكية حيث وضعت البنى التحتية الحيوية الأمريكية التي تشمل شبكات الكهرباء و النظم المصرفية تحت محاكاة لهجوم على مدار أسبوع كامل تحت رعاية وزارة الأمن الداخلي و إشترك في لعبة الحرب هذه 115وكالة تراوحت من وكالة الإستخبارات المركزية و مكتب التحقيقات الفدرالي إلى الصليب الأحمر الدولي.

5دور المظمات الإقليمية:

أصبح هناك العديد من المنظمات التي تم إنشاؤها بمبادرة من الحكومات أو من القطاع الخاص و بالتعاون فيما بينها أو بدعم من الإتحاد الدولي للإتصالات أو الأمم المتحدة ،و منظمة الأمن و التعاون الإقتصادي و

---

[1] عبد الصادق ،*"الإرهاب الإلكتروني: القوة في العلاقات الدولية .نمط جديد وتحديات مختلفة" ،**مرجع سابق**،*ص 363 .

[2] ***المكان نفسه.***

[3] Cyber Storm Exercise Report ," Department of Homeland Security National Cyber Security Division", DHS, (September 12, 2006).

التي كانت أكثر فاعلية في مجال الأمن الإكتروني و خاصة ما يتعلق بالموازنة ما بين الحفاظ على الأمن و حماية الخصوصية و عملت على تطوير مجموعة من الوسائل مكافحة الإرهاب الإلكتروني و فيروسات الكمبيوتر و القرصنة و الأخطار التي ترتبط بها. ([1])

6 موقف حلف الشمال الأطلنطي من هجمات الفضاء الإلكتروني([2]):

جاء إهتمام حلف الناتو بإعتباره المظلة الأمنية لأوروبا في شكل خطوات عملية تمثلت في نص الدليل السياسي الشامل لحلف الناتو الذي تبناه رؤساء دول و حكومات الحلف في نوفمبر 2006،على تعزيز القدرة على حماية أنظمة المعلومات ذات الأهمية الكبيرة بالنسبة للحلف ،ضد الهجمات على الأنترنت ، كما أن الهجوم على إستونيا أثار قدرة الحلف على الدفاع ضد تلك الهجمات و إمكانية تطبيق المادة (5) من إتفاقية الحلف التي تقر بأن أي إعتداء على أحد أعضاء الحلف يمثل إعتداء على باقي دوله ، و قد وصف Suleyman Anillرئيس وحدة الدفاع الإكتروني التابعة لحلف الناتو بأن الإرهاب الإلكتروني يفرض خطورة على الأمن القومي لا تقل خطورة عن هجمات الأسلحة الصاروخية ، و خاصة أن هجمات الفضاء الإلكتروني تستهدف البنية التحتية ولا يمكن عمليا إيقافها ،و من ثم فإن الدول بحاجة إلى تقوية نظمها المعلوماتية و مع ما يمثله الإرهاب الإلكتروني من مشكلة عالمية مستقبلية ، و قد قام الحلف بإنشاء وحدة عمل في قمة بوخارست في أفريل 2008 خاصة بدراسة إحتمال تعرض أعضاؤه لهجمات مماثلة لما تعرضت له إستونيا ([3]).

---

[1] Myriam Dunn, ***Towards an International Regime for the Protection of Cyberspace?***, (Swiss :Federal Institute of Technology, Volume 2, Number 11 , May 2004) ,pp10,11

[2] إيهاب خليفة، ***القوة الإلكترونية***، (القاهرة :دار العربي للنشر والتوزيع ،2017)،ص 202.

[3] Nick Heath," Nato: Cyber terrorism 'as dangerous as missile attack'" in :***http://software.silicon.com/security/0,39024655,39170300,00.htm***.(2017/7/6)

المبحث الثالث :تحديات معالجة الإرهاب السيبراني

أشرنا سابقا إلى أن الإرهاب الإلكتروني يتميز بمجموعة من الخصائص تجعل من عملية التحقيق في هذا النوع من الجرائم غاية في الصعوبة. فالإرهاب الإلكتروني من الجرائم العابرة للدول والقارات ، والتحقيق فيها وإثباتها أمر غاية في التعقيد ، بالنظر إلى سرعة غياب الدليل الرقمي من جهة ، وسهولة إتلافه وتدميره من جهة أخرى . ولذلك يرى الباحث أن أساليب مكافحة الإرهاب تنقسم إلى قسمين رئيسيين : أساليب وقائية ، وأخرى علاجية عقابية([1]).

المطلب الأول: أساليب الوقاية من الإرهاب السيبراني:

في ضوء الصعوبات التي تواجه التحقيق في جرائم الإرهاب السيبراني، تتبوأ الوقاية من هذه الجريمة أهمية كبيرة بين رجالات الفقه والقانون كوسيلة من وسائل مكافحة الإرهاب السيبراني ، واذا أردنا أن نتحدث عن طرق الوقاية من جرائم الإرهاب السيبراني ، يبرز إلى حيز الوجود الدور الذي يمكن أن يلعبه الإعلام الرسمي وغير الرسمي في مواجهة المواقع التي تروج للفكر المتطرف والإرهاب على شبكة الإنترنت.([2])

فالاعلام يلعب دورا محوريا هاما في مكافحة الإرهاب السيبراني . ولدلك فإن دور الإعلام يجب أن ينصب بالدرجة الأولى على الجوانب الإنسانية التي تهم المواطنين والأفراد في الدول . ويدخل في هذا النطاق تركيز الإعلام على ضحايا الإرهاب ، وفئاتهم وأعدادهم ، والتركيز على الضحايا من الأطفال والنساء ، حتى تكون الرسالة الإعلامية في هذا الشأن قوية وفعالة ومؤثرة في نفوس الجمهور والمواطنين.

ويجب أن لا يقتصر دور الإعلام على الإعلام الموجه ضد الجماعات المتطرفة أو الإرهابية ، إنما يجب أن يمتد ليشمل وضع ضوابط خاصة بالتغطية الإعلامية للجماعات الإرهابية أو المتطرفة . بحيث يجب أن تأخذ بعين الإعتبار وعلى سبيل المثال ما يلي :

- تجنب التغطية الإعلامية المبالغ فيها للهجمات الإرهابية بحيث يؤدي دلك إلى تحفيز الجماعات الإرهابة على المزيد من الهجمات .
- غربلة الرسائل الإعلامية التي ينشرها الإرهابيون قبل إيداعها .

[1] عبدالرزاق سندالي، ***التشريع المغربي في مجال الجرائم المعلوماتية***، ضمن أعمال الندوة الإقليمية حول «الجرائم المتصلة بالكمبيوتر»، (المملكة المغربية ،2008)، ص71.

[2] أنظر :مصطفى محمد موسى،***الإرهاب الإلكتروني***،(القاهرة:سلسلة اللواء الأمنية،2009) ،ص ص 145-165.

- تفعيل الجانب الإنساني من خلال إبراز مخاطر هده الهجمات على الأطفال والنساء والشيوخ.
- تحفيز عموم الشعب على ظرورة بدل مجهودات إضافية بمعية القوات الأمنية في التصدي لهده الهجمات.
- إبراز دور الأجهزة الأمنية في مكافحة الإرهاب الإلكتروني والتصدي له . ([1])

إن الوقاية من الإرهاب السيبراني تتطلب بذل كافة الجهود الممكنة ويجب أن تولي الأجهزة الأمنية في هذه المرحلة جل إهتمامها لعمليات الرصد والمتابعة للمواقع الإلكترونية وجمع المعلومات المتعلقة بها وبالقائمين عليها ، ووضع الخطط الإستراتيجية للتعامل مع هذه الجريمة وضبط القائمين عليها بفضل المعلومات المتوفرة مسبقا عن تلك الجماعات .ويمكن القول بان هذه المرحلة تعتمد وترتكز على عدة محاور يمكن إجمالها بمايلي :([2])

1 .إنشاء فرق متخصصة في الإرهاب الإلكتروني فقط مهمتها رصد ومتابعة المواقع الإلكترونية المشبوهة .

2. تثمين التعاون الإقليمي في مكافحة الإرهاب السيبراني .

3. إجراء الدراسات والبحوث المتعمقه حول الإرهاب السيبراني .

4 إنشاء فرق متخصصة للتحقيق في هذا النوع من الجرائم.

وعموما يمكن وضع إستراتيجيات للوقاية من الإرهاب السيبراني على المديين القصير والطويل عن طريق التعامل معه وفق الأساليب المكرسة بالنسبة للإرهاب التقليدي . فعلى المدى القصير يجب أن تعتمد إستراتيجية الوقاية من الإرهاب السيبراني على تشجيع العمل الأمني الإستباقي من خلال ضرب القيادات الإرهابية وتشجيع العمل الإستخباراتي الرامي إلى الكشف المبكر عن نواياها .([3])

أما على المدى الطويل فان إجراءات مكافحة الإرهاب يجب أن تتضمن وضع خطط إستراتيجية شاملة ومترابطة مبنية على دراسات وأبحاث ميدانية معمقة في مجال مكافحة الإرهاب العالمي بكافة أشكاله .([4])

---

[1] بدراحمد ، الإرهـــاب الإلكتروني.. أدواته وآثاره..أساليب الوقاية والعلاج ،في : ***baathparty.sy/site/arabic/index.php?node=552&cat=15369***&، (2016/11/12).

[2] عطية ،***مرجع سابق***،ص ص25-38

[3] عبد الرحيم صدق ، ***الإرهاب السياسي والقانون الجنائي*** ، (القاهرة: دار النهضة العربية ، 1985)، ص45.

[4] ***المكان نفسه***.

المطلب الثاني :أساليب مواجهة وعلاج الإرهاب السيبراني.

تتطلب عملية التصدي وعلاج الإرهاب السيبراني مسايرة المراحل التي يتم فيها تنفيد الهجمات السيبرانية

فعند مرحلة وقوع الجريمة والتي تبدأ من لحظة البدء في تنفيذ الركن المادي لجريمة الإرهاب السيبراني يجب إتجاد تدابير معينة ، لتفادي النتائج التي قد تحصل بعد وقوع الجريمة.

والجدير بالدكر هنا أن للتشريعات المختصة بهده الظاهرة دور بارز في التصدي لها.

إن المتتبع للتشريعات العربية يجد أنها لم تدرج الإرهاب السيبراني كجريمة مستقله قائمة بذاتها ،دلك لكون الدول العربية لا تقوم على حكومات إلكترونية و من تم عدم إهتمامها بهدا الموظوع سوى مؤخرا من خلال بعض الجهود من هنا وهناك ([1]).

وبالحديث عن أساليب الحماية يمكننا دكر بعض الوسائل المتعارف عليها حديثا في إنتظار ظهور أساليب جديدة تعوض النقص الحاصل في هدا المجال،ولعل أهمها:

تأمين خطوط الدفاع الأمامية بإستخدام تطبيقات الجدران النارية: تعمل برمجيات الجدران النارية كمصفاة تمنع وصول الطلبات المشبوهة إلى الأجهزة المزودة، وذلك بالإعتماد على مجموعة من السياسات التي يحدد بموجبها مدراء الشبكة طبيعة المعلومات التي يُسمح للعاملين بالمؤسسة النفاذ إليها.

خدمات الأدلة: هي عبارة عن قواعد بيانات خاصة، ذات مستو عال من الأمان عادة، ومصممة لجمع، وإدارة المعلومات المتعلقة بمستخدمي الشبكات. ولا يقتصر دور هذه البرمجيات على جمع كلمات السر وأسماء المستخدمين، بل تطورت اليوم لتشمل السمات البيولوجية للمستخدمين. [2]

الشبكات الإفتراضية الخاصة: لا توجد طريقة أكثر أمنا من الشبكات الإفتراضية الخاصة للتحكم في الأشخاص الذين يمكنهم النفاذ إلى شبكتك. وتتلخص هذه التقنية بإقامة قناة خاصة وسيطة عبر الشبكة العامة، لا ينفذ من خلالها إلا من يقوم بتحديده مدير الشبكة.

---

[1] أيسر محمد عطية،***دور الاليات الحديثة للحد من الجرائم المستحدثة***،(عمان:كلية العلوم الإستراتيجية،2014)، ص ص 34-29

[2] يمكن الحصول على المزيد من المعلومات عن تقنية المفتاح العام بالتوجه إلى الموقع: www.pkiforum.org

وهنا بعض الحلول التي دكرتها الباحثة **سراء جبريل رشاد مرعي** وهي ([1]):

– التشفير و هو تحويل المعلومة من نص واضح إلى آخر غير مفهوم و قد أستحسن هذا النوع من النظام لنجاعته في عدم كشف المعلومات على شبكة الأنترنت.

– التوقيع الرقمي و هي تقنية تفيد في إمكانية عدم تزوير الرسائل الإلكترونية.

– إ ستخدام أنظمة كشف الإختراقات و وضع حلول للثغرات الأمنية.

– وضع سياسة أمنية للشبكة و حشد كل الإمكانيات البشرية و المادية لتطبيقها.

– الإحتفاظ بنسخ إحتياطية لكل المعلومات الحساسة في أقراص إضافية ليست مرتبطة. بالشبكة.

– تنصيب برامج لمنع ظهور الصور الخلاعية و الإتصال بالمواقع الإرهابية.

– و يرى الدكتور عبد الفتاح مراد في كتابة التحقيق الجنائي الفني ضرورة إستخدام بعض البرامج التي صممت خصيصا للكشف و الوقاية من الفيروس و البعد عن إستعمال كلمة السر البسيطة.

– عند فتح البريد الإلكتروني يجب معرفة من المرسل خشية أن يكون فيروس.

[1] سراء جبريل رشاد مرعي، "الجرائم الإلكترونية " الأهداف – الأسباب – طرق الجريمة ومعالجتها""،في: ***http://democraticac.de/?p=35426***،(2017/5/3).

خلاصة الفصل الثالث:

بالرغم من الجهود الدولية التي بدلت من أجل الوصول إلى تقنين إستخدام الفضاء السيبراني إنطلاقا من الوعي التام بالمخاطر الناتجة عن سوء توظيفه ، سواءا كانت هده الجهود في إطار هيئة الأمم المتحدة والأجهزة التابعة لها أو بشكل إنفرادي من طرف بعض الدول التي لها شأنها في هدا المجال إلا أن توسع إستخدام هدا الفضاء لتحقيق مكاسب لا يمكن تحقيقها بالوسائل التقليدية قد زاد من صعوبة إيجاد مخارج من هدا النفق المظلم وبدلك أصبح العالم اليوم أمام تحد كبير ، يتطلب تنسيقا إلكترونيا عالي المستوى بين الأجهزة الأمنية في كافة الدول، فضلا تعزيز التعاون والتنسيق مع المؤسسات الدولية المعنية بمواجهة هذا المشكلة وبخاصة الإنتربول لمواجهة كافة أشكال جرائم الإرهاب على الإنترنت.

الخاتمة

نتج عن شيوع إستخدام التكنولوجيات الحديثة توظيفها سلبا من طرف العديد من الدول والتنظيمات الإرهابية ليبرز من خلال دلك مفهوم الإرهاب السيبراني كأحد انواع الإرهاب الجديدة ،ويستنفر الجهود الدولية لإيجاد ميكانيزمات كفيلة بالتصدي لتفشي هده الظاهرة .

وعلى الرغم من الجهود الدولية التي سعت إلى تقريب وجهات النظر حول مفهوم الإرهاب إلا أن الرغبة في إبقاء نوع من اللاإجماع طغت على هده المحاولات ،ودلك مرده لسياسة الكيل بمكيالين المنتهجة على الصعيد العالمي والتي يهمها بقاء هدا النوع من الغموض في المفاهيم حتى يتم تمرير سياسات وفق مفاهيم معينة تتكيف وفق الزمان والمكان.

ونتج عن توظيف الفضاء السيبراني سلبيا العديد من التداعيات على الأمن الدولي ، خاصة في ضل الترابطات الدولية الحالية عن طريق شبكة الأنترنت ،وتعمييم إستخدام التكنولوجيات الحديثة في جميع منحي الحياة وبالتالي أصبح التحكم في البنى التحتية الرقمية لايخضع بصفة تامة لإرادة الدولة إد يمكن إختراق هده البنى والتأثير عليها عن طرق زرع فيرسيات أو تعطيل خدمات معينة وغيرها من الأعمال التخريبة .

إن إدراك الدول والتنظيمات الإرهابية بهشاشة البنى التحتية الرقمية جعلها تدخل في صراع محتوم من أجل توفير سبل الحماية وإبتكار وسائل هجومية فيما يعرف بالحروب السيبرانية .

وتراوحت شدة هده الحروب بين حروب خفية وحروب ساخنة تستعمل فيها القدرات التكنولوجية للتأثير على إرادة الخصم وجبره على إنتهاج سياسات معينة ،وإستفادت التنظيمات الإرهابية بشكل كبير من هدا الفراغ الأمني بحيث إستطاعت تحقيق مكاسب مادية ومعنوية .

أمام هدا الوضع الدي لاتستطيع قوة معينة فرض إرادتها الكاملة فيه ،إنطلقت العديد من الصرخات الداعية إلى ظرورة تقنيق إستخدام الفضاء السيبراني ،ومن هنا برزت العديد من المحاولات في إطار هيئة الأمم المتحدة وكدا من خلال بعض الدول و المنظمات الفاعلة في النظام الدولي ،فبرزت لدينا العديد من التشريعات والمبادرات التي حاولت إعطاء حلول قانونية وتقنية للتصدي للظاهرة، لكنها لم تفلح في إيجاد توافق دولي حول كيفية التعامل مع هده الظاهرة وتأمين الفضاء السيبراني.

وكنتيجة لدلك يعد أمن الفضاء السيبراني أحد التحديات التي تلاحق المجتمع الدولي مطالبة أياه بظرورة إيجاد حلول تجنب العالم من الأخطار المستقبلية الناتجة عن شيوع إستخدام التكنلوجيات الحديثة في تسيير جميع مناحي الحياة على المستوى الدولي ،وتوظيف الدول والتنظيمات الإرهابية للثغرات الموجودة في البنية التحتية السيبرانية لخدمة أهدافها بالشكل الدي يؤثر سلبا على الأمن الدولي .

الإقتراحات :

من خلال دراسة بعض جوانب الموضوع ومعرفة الأخطار الناتجة عن سوء إستعمال الفضاء السيبراني في التفاعلات الدولية خلصنا إلى مجموعة من الإقتراحات يجب تطبيقها على المستويات الثلاث: الدولى ، الأقليمي ،الوطني وهي تتعلق إ جمالا بمايلي:

1. تعزيز التنسيق الدولي في مجال الكشف المبكر عن الهجمات السيبرانية.
2. حماية الأنظمةالإلكترونية عن طريق إبتكار وسائل حماية فعالة وهدا عن طريق تشجيع الإستثمار في التكنولوجيات الحديثة.
3. ضرورة إيجاد إرضية للتوافق الدولي حول تحديد المصطلحات وبالتالي فتح المجال أمام التشريع وتقنين ظاهرة الأرهاب السيبراني.
4. مشاركة القطاع الخاص في المشاورات المتعلقة بإبتكار وسائل الحماية.
5. دعم التنسيق الأمني بين مختلف الأجهزة الأمنية على الميتوى المحلي والدولي.
6. تشجيع إقامة بنى تحتية تعتمد على برامج محلية فعالة من خلال الإستثمار في االعنصر البشري.
7. إقامة هيئة دولية لها صلاحيات واسعة في مجال رصد ومكافحة الجرائم المتعلقة بتكنلوجيات الإعلام والإتصال.
8. تشجيع عمل مصممي برامج الحماية على المستوى المحلي والدولي.

المراجع

باللغة العربية

المعاجم :

1. إدريس سهيل، *فئلھ زيلثيلمك (غفمزى – عزاى)* ، بيروت : دار الآداب ، ط12، 1994.
2. الباشاء محمد*لثيلعلجلثيقئغى : عزاى حغيت* ، لبنان : شركة المطبوعات للتوزيع والنشر،ط 2 ، 1992.
3. **الخياط يوسف** *كزئىطيعزاطيلحيس* **، بيروت :دار الجيل ، 1998.**
4. الكيالي عبد الوهاب، *لھزھعبلثيزيئزب* بيروت :المؤسسة العربية للدراسات والنشر، ط2، 1985.

الكتب :

1. أنجيليو كودفيلا*لثيلخئلئة ھغطيحقى* ،مترجم محمد صبري الصاوي، القاهرة: الهيئة المصرية العامة للكتاب ، 2006.
2. بن عامر سالم إبراهيم *طيعھ .ئلأنمث ا*، ليبيا :المركز العلمي للدراسات والأبحاث ، 1988.
3. حسن الشامي *ھزئلثيئلإة شلك ھئقلثيھحيئطيع شذ*، القاهرة: الهيئة المصرية العامة للكتاب، 1997،.
4. الحسيني محمد تاج الدين ، *لزئہ ا بغى غلى طئ منبئلأنمث الطيخكى*، الرباط ، 1990،
5. حماد كمال *ئلأنمث ا لثيئيھ ا بغى صھ ثلقئمھ طيخكىيثيعلى* ، الجزائر: المؤسسة الجامعية للدراسات والنشر ، 2002
6. خليفة إيهاب ، القوة الإلكترونية، القاهرة :دار العربي للنشر والتوزيع ،2017.
7. خليل إمام حسانين *ئلأنمث ا لي طيكئجفيلثيلسنھيب*، القاهرة ، 2001.

8. راسم محمد الجمال، ***مطلىئالإة شنك ىئالأعالإطكخكى بتطعصطس طكزضبنب*** القاهرة :الدار المصرية اللبنانية، 2005.

9. سندالي عبدالرزاق ***طكةسفيظطكلغنالى غى اجكطكجةؤطكلعكهلثقي ب***، ضمن أعمال الندوة الإقليمية حول «الجرائم المتصلة بالكمبيوتر»، المملكة المغربية ،2008.

10. السيد الطيب عباس رقية ***ىئالأنمى اىئالآز زطكقئنعي بطكف زيب***، الأردن :منشورات جامعة فيلديفيا ،2007.

11. صدق عبد الرحيم ***ىئالأنمى اطكزيئزى طكقئمه طكجثئى*** ، القاهرة: دار النهضة العربية ، 1985.

12. العدوان رائد ***طكلعكج بطكخطكي بلقصثيئىئالأنمى اىئالكقةنهمى***، الرياض، 2013.

13. عبد الصادق عادل ***ىئالأنمى اىئالكقةنهمو بلقهب غوطكعلإفنة طكخطكي ب. مطس جخوخ هةخجئ ة لخكب***،القاهرة: مركز الاهرام للدراسات السياسية والاستراتيجية ، 2009 .

14. عصام فاعور ملكاوي ***هئفطئالأنمى اطكخطكى*** ،الرياض ،2013.

15. عطية أيسر محمد ***خهنىالإجئ طكخوتبكخ لطكجةؤطك لزةخترب***،عمان:كلية العلوم الاستراتيجية،2014.

16. العموش احمد فلاح ،***لزقلكىئالأنمى ا غىطكقذ طكهيحخ طكعسنه م***،الرياض:جامعة نايف للعلوم الامنية،2006.

17. عوض محمد محي الدين ***طكجني لبطكخطكي ب لقوىةئطك لحئقلب عكيهئ***، القاهرة، 1987.

18. مارشان ستيفان، ***حى م لىذنطكشي م آ م تمة ش***، فرنسا : دار فايار ،2007.

19. مصطفى محمد موسى ***ئالأنمى اىئالكقةنهمى***،القاهرة:سلسلة اللواء الأمنية،2009.

20. محمد بن عبد العزيز العقيل ***طكةخفيصرئالكقةنهمى عكوىئالأنمى ا ةفيف نظفق هى هحقلذ (تهيةذ ماهديئ)***،السعودية:جامعة الإمام محمد بن سعود الإسلامية ، 2014 .

21. محمد عزيز شكري وأمل اليازجي ***ىئالأنمى اطكخطكى طكمطكطكلىطكفهم***، سوريا :دار الفكر المعاصر، 2002 .

22. مخيمر عبد العزيز عبد الهادي ***ىئالأنمى اطكخطكى***، القاهرة: دار النهضة العربية ، 1986.

المراجع

23. المصري شفيق، لقئغح بئلأ ذئ ا غىيلىقمه طكخكى، القاهرة، 1998.

24. مكاوي حسن عماد، حسين السيد ليلىئلإة شلك همطفىئة نلك لعئ شلب ،القاهرة :الدار المصرية اللندنية، 1998.

25. موسى عبده مختار " قئغح بئلأ ذئ الكفلئىل هئلإ زلفقي جئ ة ولكملئلث ،دبي:مركز المسبار للدراسات والبحوث ،2015.

26. نافع إبراهيم ، قئله زئلأ ذئ ا هزقهىئلأفعب ، القاهرة : مركز الأهرام للترجمة والنشر، ،2002.

27. اليازجي أمل ئلأ ذئ الكخكى ولكمطلكلكلى لىلكىف ه م، دمشق، 2002.

المقالات :

1. " الإرهاب الإلكتروني جولة في عقل متطرف" جفئخطلىعز ا ، ع، 9561، 2014/5/17.

2. "الأمم المتحدة: الإنترنت سهلت عمل الجهاديين وتجب مراقبتها"، جفئخطلسنفىئلأمض 2007/11/14.

3. بشيرهشام ،"الإرهاب الإلكتروني في ضل ثورة المعلومات" ، لجب آئ؟ حلكلكخي ث ،العدد 118 ، 2014 .

4. حسن أبو طالب " تقرير اللجنة القومية الأمريكية عن الهجمات على الولايات المتحدة. "، مركز الدراسات السياسية والاستراتيجية ، جفئخىئلإ هظ، القاهرة، ماي 2006.

5. خالد وليد محمود ،"الهجمات عبر الأنترنت ساحة الصراع الإلكتروني الجديدة" ،لجقب زيئزغئ ة عظيب ،العدد 5، 2013 .

6. سعيد مراد، "مواجهة الإرهاب مسئولية مشتركة لكل الأطراف على جميع المستويات"، جفئخىئلآ هظ طلزئئى، القاهرة، 12 ديسمبر 2012.

7. سليمان حنان ، "الصين تستهدف الجيش الامريكي الكترونيا **تحقيق**، العدد 143، 26 جانفي 2008.

8. الشافعي بشير، "إرهاب الحكومة وإرهاب الأفراد والجماعات "، **الحياة**، 18 / 8 / 1992.

9. عبد الصادق عادل " هل يمثل الإرهاب الإلكتروني شكلا جديدا من أشكال الصراع الدولي" ملف الأهرام الإستراتيجي، مركز الدراسات السياسية والإستراتيجية **الأهرام**، العدد 156- ديسمبر 2007.

10. عبد الصادق عادل ، "الانترنت .. ساحة جديدة للتجسس الدولي" دراسات سياسية، **الأهرام**، 5 مايو 2007.

11. عبد الصادق عادل ، "إختراق مواقع الإنترنت بين السنة والشيعة.. عندما تسيطر السياسة على الدين"، **الشرق الأوسط**، مركز الدراسات السياسية والإستراتيجية بالأهرام، العدد 112، 15 أكتوبر 2008.

12. عبد الصادق عادل ، "المتطرفون وحرية التعبير على الأنترنت بين الأمن والإنفتاح، دراسات سياسية، **الأهرام** ،21 فيفري 2005.

13. عبد الصادق عادل ، "أمريكا وتشكيل قيادة عسكرية في الفضاء الإلكتروني.. هل بدأ الإستعداد لحروب المستقبل"، **الشرق الأوسط** ، العدد 130، 12 جويلية 2009 .

14. عبد الصادق عادل ، "حقيقة دور الإنترنت في بث الكراهية الدينية في العالم، ملف الأهرام الإستراتيجي، مركز الدراسات السياسية والإستراتيجية ،**الأهرام**، عدد 144، ديسمبر 2006.

15. عبد الصادق عادل ، "من قطع كابلات الانترنت عن الشرق الأوسط" ،ملف الأهرام الإستراتيجي، مركز الدراسات السياسية والإستراتيجية ، **الأهرام**، العدد 160 ،أفريل 2008 .

16. عبد الحي وليد ،مداخلة بعنوان :"إشكالية الفضاء الإلكتروني في حقوق الملكية الفكرية"، المؤتمر العلمي الأول حول الملكية الفكرية ،جامعة اليرموك، الأردن، 10.11/7/2000 .

17. عرومي جرج ، "الإرهاب بين صيانة القانون وغياب الإصرار الدولي، *جريدة الخليج*،20 / 7 / 1996.

18. مانويل كاستلز، "وسائل الإتصال الجماهيرية الفردية الجديدة" *المجلة العربية للثقافة*، أوت 2006 .

19. محمد عبد السلام، "الحرب غير المتماثلة بين الولايات المتحدة والقاعدة"، *المجلة السياسية الدولية*، العدد 14، يناير 2002.

20. الهواري خضر ، "إنتشار الإرهاب الدولي" *السياسة الدولية*، عدد 77، جويلية 1984.

.

المراجع باللغة الأجنبية:

Les livres :

1. Bieber Florian, ***Cyber war or Sideshow? The Internet and the Balkan Wars***, Philadelphia ,Mar 1, 2000.
2. Dunn Myriam, ***Towards an International Regime for the Protection of Cyberspace?***, Swiss :Federal Institute of Technology, Volume 2, Number 11 , May 2004.
3. Grant Rebecca, ***Victory in Cyberspace***, USA : The Eaker Institute, October 9, 2007.
4. J. Arquilla. , D.Ronfeldt ***.networks and netwars*** . rand.santa monica. 2001.
5. Karatzogianni,(ed) Athina ***Cyber-Conflict and Global Politics***, usa: Routledge and Taylor & Francis Group، 2009.
6. Kevin G. Coleman***, A Cyber War has begun, Cyber Warfare***, usa :The Technolytics Institute, September 2007.
7. Lipsey Richard, ***Network Warfare Operations: Unleashing the Potential***, USA :Center for Strategy and Technology, Air War College, Air University, November 2005.
8. N. Adkins, Bonnie, ***The Spectrum of Cyber Conflict from Hacking to Information Warfare: What is Law Enforcement's Role?,*** , Alabama :Maxwell Air Force Base, April 2001 .
9. Schreier Fred, ***On Cyberwarfare***, DCAF HORIZON WORKING PAPER No. 7,2017
10. Shane P Courville,. ***Air Force and the Cyberspace Mission: Defending the Air Force's Computer Networks in the Future.*** Maxwell Air Force Base, AL, Center for Strategy and Technology, Air War College, 2007.

11. SINGER P. W. , FRIEDMAN ALLAN, **CYBERSECURITY AND CYBERWAR WHAT EVERYONE NEEDS TO KNOW** , oxford press ,2014

12. T. G. Lewis, *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation* .NJ: Hoboken, , Wiley-Interscience,2006.

13. Thevenet Cedric ,*cyberterorrisme , mythe ou realite ?,* universite de marne la vallee ,2005.

14. Thomas Timothy L., *Al Qaeda and the Internet: The Danger of "Cyber planning"* From Parameters, Spring 2003.

15. Weidman Gabriel, *How Modern Terrorism Uses the Internet*, The United States Institute of Peace, Special Report No. 116, March 2004

16. Williamson Jennie M. *Information Operations: Computer Network Attack in the 21st Century*, Carlisle Barracks, PA, U.S. Army War College,2002.

17. Zanini Michele, J.A. Edwards Sean, "The Networking of Terror in the Information Age," in John Arquilla and David Ronfeldt (eds.), Networks and Netwars: *The Future of Terror, Crime and Militancy* Santa Monica, CA: RAND, , MR-1382-OSD. 2001.

les articles :

1. "Cyber Attacks Force Estonian Bank to Close Website," ***Agence France Presse***, May 16, 2007.
2. China 'hacked' into Pentagon defense system", ***The Financial Times***, September 4 2007.
3. Delibasis Dimitrios," State Use of Force in Cyberspace for Self-Defence: A New Challenge for a New Century", ***Peace Conflict and Development: An Interdisciplinary Journal***, Issue 8, February 2006.
4. Denning Dorothy, "Information Warfare and Cyber-terrorism", ***Women in International Security*** (WIIS) Seminar, Washington, D.C. 15 December 1999.
5. Finn Peter, "Cyber Assaults on Estonia Typify a New Battle Tactic," ***Washington Post***, May 19, 2007.
6. G, Pontara. "the concept of violance," ***Journal of peace research*** vol15, n,1,1978.
7. J ,Galtang." cultural violance,"***Journal of peace research***,vol 27,no 3 ,1990 .
8. Nick Cullather,"Bombing at the Speed of Thought: Intelligence in the Coming Age of Cyber war". ***Intelligence & National Security*** No.18,Winter 2003.
9. Stein Schjolberg, Chief Judge, Moss Tingrett Court, Norway. "Law Comes to Cyberspace," ***A presentation at the 11th UN Criminal Congress***, Bangkok, Thailand. Workshop 6: Measures to combat computer-related crime. Apr. 18-25, 2007.

Les cites :

1. Baocun Wang and Fei Li," Information Warfare"in : *https://fas.org/irp/world/china/docs/iw_wang.ht..*
2. Espiner Tom," CIA: Cyberattack caused multiple-city",in : *https://www.cnet.com/news/cia-cyberattack-caused-multiple-city-blackout/*,
3. G. Coleman Kevin," The world war,A Cyber War has begun, Cyber Warfare", in : *http://www.technolytics.com/Technolytics_Cyber_War.pdf*
4. G.Coleman Kevin ," The Challenge of Unrestricted Warfare - A Look Back and a: *www.directionsmag.com*,
5. Heath Nick," Nato: Cyber terrorism 'as dangerous as missile attack'" in :*http://software.silicon.com/security/0,39024655,39170300,00.htm.*
6. ITU website: *http://www.itu.int/net/about/index.aspx*.
7. LUDOVIC HENNEBEL et GREGORY LEWKOWICZ *le probleme de ladefinition du terrorisme* sur *http://www.philodroit.be/IMG/pdf/Lewkowicz_et_al_-le_probleme_de_la_definition_du_terrorisme_web.pdf means*/12/11/2016.
8. R. Shulman Mark," Discrimination in the Laws of Information Warfare",. in : *http://digitalcommons.pace.edu/lawfaculty/224*.
9. Robert Vamosi," Cyber attack in Estonia--what it really means", in : *https://www.cnet.com/news/cyberattack-in-estonia-what-it-really-*
10. Sturgeon Will," Cyber-terror plan panned as "barmy",in : *http://www.crime-research.org/news/10.02.2005/952*.
11. T. Greenberg Lawrence &, E. Goodman Seymour &, J. Soo Hoo Kevin," Information Warfare and International Law",In : *www.iwar.org.uk/law/resources/iwlaw/iwilindex.htm - 19k .*

فهرس المحتويات