أثر الفضاء الالكترونى على مستقبل العلاقات الدولية

" دول الشرق الأوسط نموذجاً"

إعـــداد

المستشار الدكتور

أبوبكـــر محمد الديـب

دكتوراه في القانون الدولي

الدكتورة

ياسمين أحمد اسماعيل صالح

مدرس العلوم السياسية

بكلية السياسة والاقتصاد جامعة بنى سويف

الملخص:

أضحى الفضاء الإلكترونى فى الآونة الأخيرة أحد مرتكزات القوة التى تسعى الدول إلى امتلاكها و توظيفها فى تحقيق مصالحها القومية، إذ نجحت هذه الدول– والتى تمتلك العلم والمعرفة– فى مواكبة التكنولوجيا لدرجة تصل إلى استخدام الفضاء الإلكترونى والاستفادة منه فى كافة مجالات الحياة كالتعليم والصحة، فضلاً عن استخدامه لتحقيق المصالح القومية لهذه الدول، بشكل جعل من الفضاء الإلكترونى ساحة للتنافس والصراع، الأمر الذى من شأنه أن ساهم فى إحداث تغيير فى موازين القوى، وبالتالى كان له تأثير كبير على مستقبل العلاقات الدولية؛ لذا جاءت هذه الدراسة لتلقى الضوء على مفهوم الفضاء الإلكترونى، مع الإشارة الى أهميته، وطبيعة المنافسات التى تشهدها ساحة الفضاء الإلكترونى، وتأثير استخدام الفضاء الالكترونى على مستقبل العلاقات الدولية، وذلك بالتطبيق على دول الشرق الأوسط، والتى تتمتع بأهمية استراتيجية تسعى الكثير من دول العالم للاستفادة منها .

Abstract:

Cyberspace has recently become one of the pillars of power that countries seek to possess and employ in achieving their national interests, as these countries that possess science and knowledge have succeeded in keeping with technology to the point of using and benefiting from cyberspace in all areas of life such as education and health, in addition to using it to achieve the national interests of these countries in a way that made the cyberspace an arena for competition and conflict, which would have contributed to bringing about a change in the balance of power, and thus had a major impact on the future of relations International. So this study came to shed light on the concept of cyberspace, with reference to its importance, the nature of the competitions taking place in the cyberspace arena, and the impact of the use of cyberspace on the future of international relations, by applying to the countries of the Middle East, which have strategic importance, many countries of the world seek to take advantage of it.

مقدمة الدراسة:

مع منتصف العقد الأول من الألفية الثالثة، تسارعت وتيرة وسائل الاتصال بشكل ملحوظ؛ لينتج عنها مصطلح جديد، وهو الفضاء الإلكترونى، والذى بات له أهمية كبيرة فى كافة المجالات السياسية والاقتصادية والعسكرية والاجتماعية وغيرها، وخاصة فى ظل جائحة كورونا، والتى فرضت تحدياً أمنياً إلى جانب التحديات الاقتصادية والاجتماعية التى يتعين على الدول مواجهتها، إذ أصبحت مرتكزات الحياة - كالصحة والتعليم وغيرها- تعتمد بشكل كبير على الفضاء، إلا أن بعض القوى الكبرى سعت إلى توظيف الفضاء الإلكترونى لتحقيق مصالحها، الأمر الذى جعل من الفضاء الإلكترونى ساحة للصراع وأحد مرتكزات القوة التى تسعى الدول لامتلاكها لفرض هيمنتها وسيطرتها على دول العالم كافة.

لذا؛ جاءت هذه الدراسة لتوضح المقصود بالفضاء الإلكترونى، وأهميته، مع الإشارة إلى طبيعة المنافسات التى شهدها الفضاء الإلكترونى؛ من أجل تنفيذ السياسات ذات الطبيعة الاستراتيجية، وتأثير الفضاء الالكترونى على مستقبل العلاقات الدولية، وذلك بالإشارة إلى دول الشرق الأوسط كنموذج لتبيان الانعكاسات و التأثيرات المتحصلة من استخدام الفضاء الإلكترونى على علاقات القوى الكبرى بدول المنطقة.

المشكلة البحثية:

مع تسارع وتيرة التقدم التكنولوجى والتى شهدتها البشرية فى الآونة الأخيرة خاصة فى ظل جائحة كورونا، حيث بات التحول الرقمى أمراً هاما وملحاً للتعايش مع هذه الأزمة، سعت حكومات الدول إلى توظيف التكنولوجيا فى كافة مناحى الحياة، بشكل ساهم فى إبراز أهمية الفضاء الإلكترونى، والتى أصبحت مرتكزات الحياة

كالتعليم والصحة تعتمد عليها بشكل كبير، إلا أن بعض القوى الكبرى والفاعلين من غير الدول عملوا على توظيف الفضاء الإلكترونى فى تحقيق مصالحهم؛ ليصبح أحد مرتكزات القوة التى تتنافس الكثير من الدول على امتلاكها لتعزيز نفوذها وفرض هيمنتها على دول العالم كافة؛ لذا جاءت هذه الدراسة لتجيب عن تساؤل رئيسى وهام : ماهو تأثير الفضاء الإلكترونى على مستقبل العلاقات الدولية ؟

ويتفرع عن هذا التساؤل العديد من التساؤلات الفرعية:

- ما المقصود بالفضاء الالكترونى ؟
- ما أهمية الفضاء الالكترونى ؟
- ما طبيعة المنافسات التى شهدها الفضاء الالكترونى من أجل تنفيذ السياسات ذات الطبيعة الاستراتيجية؟
- الى أى مدى أثر استخدام أسلحة الفضاء الالكترونى على مستقبل العلاقات بين القوى النافذة فى السياسة الدولية ودول الشرق الأوسط؟

منهج الدراسة :

تم الاعتماد على منهجى المصلحة الوطنية ودراسة الحالة فى تناول هذه الدراسة، وذلك على النحو التالى:

أولا – منهج المصلحة الوطنية : يُعد هذا المنهج من أهم المناهج المستخدمة فى دراسة علم العلاقات الدولية، حيث يركز على مفهوم المصلحة الوطنية، وهو من المفاهيم المحورية للنظرية الواقعية، فالمصلحة الوطنية للدولة هى التى تحدد سلوك الدولة فى سياستها الخارجية لتحقيق مصالحها، وهنا تجدر الاشارة الى أن تصادم المصالح الوطنية للدول من شأنه أن يؤدى الى اندلاع الصراعات بين هذه الدول؛ لذا

نجد أنه فى ضوء التقدم التكنولوجى والعلمى الذى عرفته البشرية فى العصور الحديثة بات الفضاء الالكترونى ساحة للصراع والتنافس، إذ سعت العديد من الدول إلى توظيفه فى تحقيق مصالحها وبسط نفوذها بالشكل الذى يحقق لها الهيمنة والسيطرة على العالم ككل، فأصبح الفضاء الالكترونى أحد مرتكزات القوة التى تتبارى الدول فى امتلاكها لتحقيق مصالحها القومية.

ثانياً- منهج دراسة الحالة : وهو المنهج الذى يقوم على جمع البيانات بوحدات التحليل، حيث تم اختيار دول الشرق الأوسط كنموذج لتوضيح تأثير الفضاء الالكترونى على مستقبل العلاقات بين بعض القوى التى تمتلك من المعرفة والعلم مايمكنها من استخدام الفضاء الإلكترونى وتوظيفه فى تحقيق مصالحها القومية ودول الشرق الأوسط.

أهمية الدراسة:

تنبع أهمية الدراسة من كونها جاءت لتوضح تأثير الفضاء الالكترونى على مستقبل العلاقات الدولية، وتحديداً العلاقة بين الدول التى تمتلك القدرة على مواكبة التكنولوجيا وتوظيف الفضاء الالكترونى فى تحقيق مصالحها و دول الشرق الأوسط، حيث بات الفضاء الالكترونى- فى ظل التقدم التكنولوجى والعلمى الهائل والذى عرفته البشرية فى العصور الحديثة- ساحة للتنافس والصراع، إذ أخذت الدول تتبارى فى توظيف الفضاء الإلكترونى لتحقيق مصالحها القومية، الأمر الذى من شأنه أن يساهم فى إحداث تغيير فى موازين القوى؛ لذا جاء التركيز فى هذه الدراسة على طبيعة الفضاء الالكترونى وأهميته، وكيف استطاعت بعض الدول توظيفه لتحقيق مصالحها القومية.

أهداف الدراسة:

تهدف الدراسة إلى توضيح تأثير استخدام الفضاء الالكترونى على مستقبل العلاقات الدولية، ففى ظل التقدم التكنولوجى والعلمى الهائل والذى عرفته البشرية فى العصور الحديثة، استطاعت بعض الدول- التى تمتلك العلم والمعرفة- مواكبة هذه التكنولوجيا، إذ نجحت فى استخدام الفضاء الإلكترونى فى تحقيق مصالحها القومية؛ لذا تهدف هذه الدراسة إلى :

- **التعرف على المقصود بالفضاء الإلكترونى .**
- **توضيح أهمية الفضاء الإلكترونى.**
- **استعراض نماذج لبعض الدول التى استطاعت توظيف الفضاء الالكترونى فى تحقيق مصالحها القومية.**
- **تأثير استخدام الفضاء الالكترونى على مستقبل العلاقات بين هذه الدول، التى تمتلك القدرة على استخدام الفضاء الالكترونى ودول الشرق الأوسط.**

تقسيمات الدراسة :

لا يستطيع أحد أن ينكر تأثير الفضاء الإلكترونى في العلاقات الدولية، لكن هذا المؤثر القوى ما لبث أن ظهر منذ بضعة عقود قليلة، بحيث يمكننا القول أن ركائزه لم تتأسس بعد بشكل كبير، بل لا زال مجتمع المعلومات ينظر فى حدوده و أبعاده، و ما ساعد علي هذا – و خاصة فى إطار هذه الدراسة – عدم استقرار المجتمع الدولى بعد على مفهوم مترسخ للإرهاب ذاته، فبات الفضاء الإلكترونى و عوامله – ممثلة فى أسلحته و سماته الإرهابية محمولا ومتعلقا بالمفهوم المرصود للفضاء الإلكترونى.

وعلي ذلك تنقسم الدراسة إلى عدة محاور رئيسة :

المحور الأول : التأصيل النظرى لمفهوم الفضاء الالكترونى .

المحور الثانى : تأثير الفضاء الالكترونى فى العلاقات الدولية.

المحور الثالث: التأثيرات والانعكاسات المتحصلة من استخدام الفضاء الالكترونى (دول الشرق الأوسط نموذجاً).

المحور الأول

التأصيل النظرى لمفهوم الفضاء الالكترونى

يستلزم تأصيل المفهوم النظرى لموضوع دراستنا التعرض لتحديات الفضاء الإلكترونى بعد التعرف على مفهوم الفضاء الإلكترونى، و ذلك على النحو التالى:

أولا

مفهوم الفضاء الالكترونى

اصطلاحاً:

اشتهر هذا المصطلح فى التسعينات بعدما أصبحت استخدامات الانترنت والشبكات والاتصال الرقمى تنمو بشكل كبير، وأصبح مصطلح الفضاء الالكترونى قادراً على تمثيل العديد من الافكار والظواهر الجديدة التى ظهرت .

لغوياً:

يأتى أصل الكلمة Cyper من اللغة اليونانية القديمة (kybernētēs) بمعنى »الحاكم» أو «الرائد» أو [قائد الدفة] [(١)]، حيث تستخدم مجازاً للمتحكم"governor"إلا أن اللفظ التصق لاحقاً بكل ما يخص الفضاء، واستخدم فى كل ما يتعلق بالانترنت واستخدامه بشكل كبير .

---

(١) الموقع الالكترونى ويكيبديا العالمى، متاح علي: https://ar.wikipedia.org/wiki/

د. **سمير فرج**، الفضاء السيبرانى – جريدة الاهرام المصرية ٣٠ يوليو ٢٠٢٠- مقال بالموقع الالكترونى.

د. **ياسر محمد عبد السلام**، الرقابة السيبرانية وتهيئة البيئة السيبرانية الامنة، مجلة القانون والتكنولوجيا – المجلد الثانى، العدد١، إبريل ٢٠٢٢، ص ١٤٥.

و قد استخدم مصطلح الفضاء الإلكتروني للمرة الأولى ويليام جيبسون (William Gibson) وهو كاتب في الخيال العلمي وبالأخص في نوع الأدب الذي يعرف باسم " الشر الإلكتروني" ، إلا أن المفهوم كان قد تم شرحه سابقا، مثلا في رواية جون فوردز (John M. Ford's) بيت الملائكة العنكبوتي (Web of Angels)ولكن يتم استخدامه الآن من قبل استراتيجيي التكنولوجيا وخبراء الأمن والقادة العسكريين وقادة الصناعة ورجال الأعمال لوصف مجال بيئة التكنولوجيا العالمية(١) .

و يخلط البعض بين مفهومي الفضاء الإلكترونى والإنترنت، ويعتقدون أنّهما يعبّران عن نفس المفهوم، وهو أمر غير صحيح؛ فالإنترنت (إحدى الشبكات العالمية) التي تنشأ من خلال ربط شبكات أصغر من الحواسيب والخوادم، بينما الفضاء السيبراني حيّز رمزي أو (افتراضي يوجد ضمن نطاق الإنترنت) (٢)، ومرّة أخرى، قد يخطئ البعض في الاعتقاد أنّ كلًا منهما نظام مختلف تمامًا في عالم التكنولوجيا، وأنه لا يوجد ترابط بينهما، بينما الحقيقة وجود ترابط وثيق بينهما؛ نظرًا لوجود الفضاء السيبراني داخل نطاق شبكة الإنترنت، وإنجاز جميع العمليات داخل حيّزه عن طريق شبكة الإنترنت، مثل: إرسال البريد الإلكتروني، أو فتح مواقع الويب. إن استخدام تقنيات المعلومات وخاصة الاتصال في الفضاء الإلكتروني له إيجابيات عدة يمكن لتقنيات الاتصال الحديثة على غرار الأدوات الأخرى أن تعمل كخادم جيد، نذكر منها ما يلى:

(1) cyper security intelligence in 22/5/2017 retrieved edited in 10/11/20211"The Difference Between Cyberspace & The Internet . "

مجلة الفضاء السيبرانى –منشور فى ٢٠٢١/٥/٢٢ وتم تعديله فى ٢٠٢١/١١/١٠-

١-الزمن، عندما نتواصل في الفضاء الإلكتروني نشهد تسريعًا هائلاً في نقل المعلومات والذي يصل في الوقت الحاضر إلى سرعة الضوء تقريبًا، ثم هناك زيادة هائلة في كمية المعلومات، والتي لا تزال تنمو باطراد، وهذا يعني أنه يمكن الوصول إلى أي معلومات تقريبًا بسرعة ولكن الاختيار والمعالجة يتطلبان وقتًا أكبر ويستغرقان وقتًا طويلاً، مما يؤدي إلى رسم تخطيطي.

٢-الفضاء، يتمثل أحد الجوانب الإيجابية للاتصال في الفضاء الإلكتروني في قدرته على هزيمة المواقع الجغرافية، إذ يمكن الآن التواصل مع شخص يعيش في أي منطقة من العالم ليس فقط شفهيًا ولكن أيضًا بصريًا، يمكن حتى مشاهدة الأحداث التي تحدث في أماكن مختلفة من العالم.

وبالنسبة إلى الجوانب السلبية: قد يؤدى هذا إلى فقد الإحساس بقيمة المحيط الحقيقي والتقاليد والثقافة فى مكان معين، فمع الاتصال عبر الإنترنت تتدهور أهمية مثل هذا المكان، ويفقد الناس جذورهم، فلقد أصبح الإنترنت يمزق الرابط بين الموقع الجغرافي والدور الاجتماعي، مع عدم وجود جذور جغرافية واجتماعية يمكن بسهولة أن يصبح المرء بلا مأوى فى الفضاء الإلكترونى[١].

(١) **عبد الله احمد القرنى**، بحث فى (التفاعل الاجتماعي في المجتمعات الافتراضيه) ، مجلة العربى، فى ٢٦ /٢٠٢١/٩ .

ثانيا
تحديات الفضاء الالكترونى
الخطر الإلكترونى (السيبرانى)

تناولنا فى السابق التعرف على الفضاء الالكترونى، إلا أنه يجب أيضا التعرف على الخطر الالكترونى (السيبرانى) ، وما المقصود بالمخاطر السيبرانية ؟ وماهى الحوادث التقنية ؟

سوف نعرض بداءة لمفهوم السيبرانية، وما هو أصل كلمة سيبرانية؟ ، كالآتى:

لغوياً:-

جاءت سيبرانية من الفعل (سَيَبَ) أى تركه، وأطلق سراحه أى يذهب حيث يشاء، و جاءت من الاسم (تسيب) وجمعها (تَسيوب)، والسَيبُ :هو كل ما سِيَبَ وخُلّيِ فساب، ومعناه العطاء.

اصطلاحاً:

هو عبارة عن علم أو منظومة ظهر مع ظهور الأجهزة الإلكترونية المتطورة مثل أجهزة الكمبيوتر، الهواتف الذكية وتطبيقاتها، وغيرها من الأجهزة المرتبطة بالإنترنت.

أما الهجمات السيبرانية فيمكن تعريفها بكونها" : فعلاً يقوّض من قدرات و وظائف شبكة الكمبيوتر لغرض قومي أو سياسي، من خلال استغلال نقطة ضعف معينة تُمكّن المهاجم من التلاعب بالنظام"، او تعرف بالاستغلال غير مشروع لأنظمة الحاسب، والشبكات، والمنظمات التي تعتمد فى عملها على تقنية المعلومات والاتصالات الرقمية؛ بهدف إحداث أضرار، وتشمل أي نوع من الأنشطة الخبيثة التي

تحاول الوصول غير المشروع أو تعطيل، أو منع، أو تدمير موارد النظم المعلوماتية، أو المعلومات نفسها(١).

و قد عرف بعض الباحثين الخطر السيبرانى بأنه " خطر جديد يواجه المؤسسات وجهات الإدارة ويكون مرتبطاً بالتطور التكنولوجى وتدفقات المعلومات" ، وهناك ما يعرف بالحوادث التقنية : أى حادثة تواجه الخدمات الإلكترونية المالية و ينتج عنها انقطاع أو مشاكل تقنية أخرى وتمنع العملاء الاستفادة منها (٢).

وتتعدد أشكال الخطر السيبرانى ما بين " التهديد بالاضطراب فى تدفق المعلومات، أو استغلال المعلومات السرية والحساسة، أو الملكية السيبرانية، أو التهديد بإنتقاء المعلومات لتحقيق أغراض غير مشروعة، أو التهديد بتدمير المعلومات.

و على ذلك فإن الخطر السيبرانى هو خطر محتمل يهدد المؤسسات والهيئات الحكومية و غير الحكومية وجهات الإدارة، ويمتد ليشمل الأفراد كذلك، حيث يتعلق بالبيانات والمعلومات الرسمية و غير الرسمية، هدفه التغيير والتأثير لتحقيق أغراض غير مشروعة (كالإبتزاز المالى، أو إثارة البلبلة، أو التجسس) .

---

(١) المعجم الوسيط . اللغه العربية .

و الموسوعة السياسية، https://political-encyclopedia.org/

و أنظر: د. **محمد فارس الزغبى**، الحماية القانونية لقواعد البيانات وفقا لقانون حق المؤلف – دراسة مقارنة بين النظام اللاتينى والنظام الأنجلو أمريكى، ص ٨٥.

(٢) د. **ياسر عبد السلام رجب**، دور الضبط الادارى الالكترونى فى الرقابة السيبرانية، المجلد ٢، العدد ١، إبريل ٢٠٢٢، صفحات ١٤٥- ١٤٩.

د. **محمد على فارس**، الحماية القانونية لقواعد البيانات فقاً لقانون حق المؤلف – دراسة مقارنة بين النظام اللاتيني والنظام الانجلو أمريكى، ص ٨٥ .

وقد ذهب البعض الي القول بأن التقدم التكنولوجي أدي إلي حدوث ثورة في نطاق المجال الذي يتم فيه إدارة المعارك، حيث تم إضافة المجال الالكتروني وهو المجال الذي لم يكن متصورا عند توقيع الاتفاقيات التي تنظم حالات الحرب، وهو المصطلح الذي يعبر عن البيئة التي يتم من خلالها التواصل بين أجهزة الحاسب الألي في أماكن متفرقة(١).

وتعد الهجمات السيبرانية في الوقت الحاضر من أبرز التحديات التي يواجهها المختصون في القانون الجنائي، ولعل السبب في ذلك يرجع إلي صعوبة تحديد طبيعة وعناصر تلك الهجمات وما يترتب عليها من مسؤولية جنائية لاسيما وأن تلك الهجمات قد يلجأ اليها الافراد او الدول من أجل تحقيق بعض المكاسب مثل الهيمنة على واقع النزاع المسلح أو القيام بتوجيه بعض التهديدات السياسية أو العسكرية، وذلك بخلاف النتائج السلبية من التهديدات الإجرامية والإرهابية التي قد تترتب عليها حال ارتكاب تلك الهجمات بواسطة مجموعات فردية بقصد الحصول على بعض المزايا السياسية أو الاقتصادية(٢) .

ويعتبر الفضاء الإلكتروني ساحة لارتكاب بعض الجرائم الأخرى التي تختلف في طبيعتها عن الهجمات السيبرانية مثل جريمة الابتزاز الالكتروني والاحتيال الالكتروني وسرقة البيانات، كما أن الهجمات السيبرانية – التي تقع على المواقع الالكترونية– قد يتم ارتكابها من داخل الدولة، ومن الممكن ايضا أن يتم ارتكابها من

(1) Research Handbook on International Law and Cyberspace, (Nicholas Tsagourias & Russell Buchan Eds. Elgar, 2015, pp. 14-24.

(٢) **طلال ياسين العيسي**، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي، مجلة الزرقاء للبحوث والدراسات الإنسانية، جامعة الزرقاء عمادة البحث العلمي، المجلد ١٩، العدد الاول، ٢٠١٩، ص٨٢.

خارج الدولة، حيث تعد جريمة الهجمات السيبرانية من الجرائم العابرة للحدود.

-السيبرانية في اللغة:

تعد كلمة سيبرانية ترجمة حرفية لكلمة (cyber) وهي مشتقة من كلمة (cybernetics) وقد تم استخدام هذا المصطلح الأخير أكاديميا – و سلأول مرة– من قبل عالم الرياضيات الأمريكي نوربرت وينر في عام ١٩٤٨ وذلك في كتابه الشهير" علم التحكم الآلي او التحكم والاتصال في الحيوان والألة "وذلك من أجل الإشارة إلى التنظيم الذاتى(١).

ومن خلال البحث فى معاجم اللغة العربية عن مصدر كلمة سايبر فإنه لا يوجد مصطلح مقارب لها، الا أن معني تلك الكلمة قد جاء في قاموس المورد الحديث بالكمبيوتري أو العصري جدا كما جاء مصطلح (cybernetics) بمعني علم الضبط أو علم التحكم الأوتوماتيكي(٢)، كما ورد في قاموس المعاني أن الكلمة تعني "تخيلي".

ومن خلال الاطلاع على الوثائق الصادرة عن منظمة الأمم المتحدة نجد أن تلك الوثائق قد استخدمت نفس المصطلح كما تم استخدام ذات المصطلح من اللجنة الدولية للصليب الأحمر.

(١) **نور أمير الموصلي**، الهجمات السيبرانية في ضوء القانون الدولي الإنساني، رسالة ماجستير في القانون الدولي الإنساني، الجامعة الافتراضية السورية، ٢٠١٠، ص٨.

(٢) **منير البعلبكي ورمزي منير**، المورد الحديث، دار العلم للملاين، بيروت، ٢٠٠٩، ص٣٠٧.

المحور الثانى

تأثير الفضاء الالكترونى فى العلاقات الدولية

شهد الفضاء الالكتروني العديد من الهجمات السيبرانية في السنوات الأخيرة؛ نظرا لتعدد التهديدات السيبرانية، والتي ضمت الحروب و الإرهاب والاختراق والتجسس الرقمي وغيرها، الأمر الذى يصعب معه تحديد الحجم الحقيقي لتلك الهجمات، لاسيما أن العديد من تلك الهجمات لا يتم الإبلاغ عنها، و رغم اختلاف الغرض في الهجمات السيبرانية إلا أن ما يجمع بينها هو العمل على استغلال الثغرات الموجودة في المجال السيبرانى؛ من أجل اختراق أجهزة الكمبيوتر وشبكات الحاسب[١] .

و ترتكب جرائم الإرهاب السيبرانى بواسطة أسلحة الفضاء الإلكترونى، و لا شك أن بيان دور الإرهاب الإلكترونى فى العلاقات الدولية يقتضى- بداءة- تحديد ماهية هذا النوع من الإرهاب، و أهم خصائصه – و مخاطره بعد الإشارة إلي أهم الأسلحة المستخدمة فيه وتحديدها،

و نتناول أهم المنافسات الدولية فى ظل الفضاء الالكترونى علي النحو الأتى:

(١) **رغدة البهي**، الردع السيبراني: المفهوم والإشكاليات والمتطلبات، المركز الديمقراطي العربي، العدد الاول، مجلة العلوم السياسية والقانون، القاهرة، ٢٠١٧، ص٣.

أولا
أسلحة الفضاء الإلكترونى

يؤكد خبراء الإستراتيجيات العسكرية أن أجهزة الحاسوب تمثل أكبر تهديد للأمن القومى فى المستقبل، إذ يمكن أن تؤدى الهجمات [١] الحاسوبية إلي تدمير البنية الأساسية وتخريب الاتصالات وقوي الطاقة، وتعطيل الأنظمة العسكرية بأكملها، وتعتبر حرب كوسوفو ١٩٩٨ مثالاً واضحاً لاستخدام حرب المعلومات، حيث قامت أجهزة الدعاية الصربية بإغراق نظم الحاسوب لحلف شمال الأطلسي"الناتو" بعشرة آلاف بريد إلكترونى شلت عملها لعدة ساعات[٢].

وتشتمل أسلحة حروب المعلومات [٣] علي العديد من الوسائل التى تحقق لمن يمتلكها إمكانية إحداث خلل كبير يفقد العدو قدرته على تبادل المعلومات داخل نظمه، ويعوق تكامل المعلومات، وفي الوقت نفسه، يخضعه لتأثير الحرب النفسية، وتتمثل فى فيروسات الحاسب، والديدان، وبرامج التجسس، والقنابل المنطقية،

---

(١) الهجمات "Attacks" هو اصطلاح لوصف الاعتداءات بنتائجها أو بموضع الاستهداف، تفصيلا، **د .أحمد الشربيني و د. وفائي بغدادي**، حماية وتأمين الإنترنت، التحدي القادم وأساليب المواجهة، الهيئة المصرية العامة للكتاب، ٢٠١٠، ص٧.

(2) Cordesman, Anthony H. and Justin G. Cordesman, Cyberthreats, Information Warfare , and Critical Infrastructure protection (London: Praeger, 2002),36

مشار إليه في: د. **صفات أمين سلامه**، أسلحة حروب المستقبل بين الخيال والواقع، العدد ١١٢، مركز الإمارات للدراسات والبحوث الإستراتيجية، بدون سنة نشر، ص ٤٠.

(٣) ونود الإشارة إلي أن مرجع استخدام اصطلاح " الفضاء الالكتروني " كان مجازياً وليس حقيقياً، إلا أنه يعبرعن إنتشار الأسلحة الإلكترونية في البيئة الفضائية السيبرانية المحيطة بالبشر والتي تتمتع بقدر من اللامحدودية مثلها مثل الفضاء الطبيعي .

والأبواب الخلفية، والرقائق[١].

وتستخدم الأسلحة الإلكترونية للحصول على المبادأة فى ميدان المعركة بوحدات كمبيوترية، كالوحدات الأساسية فى القوات المسلحة، وذلك بالاستخدام الصحيح والمتقن عبر صراع إلكترونى بين القيادات الصديقة والقيادات المعادية؛ بهدف التأثير على قدرات الخصم واختراق كيانه الإلكترونى[٢].

وقد نالت أسلحة الفضاء الإلكترونى- مع حداثتها – اهتمام علماء القانون الدولى، وسارعوا إلى وضع النظريات القانونية، و أوصت الدراسات القانونية – التى أعدت فى هذا الشأن- بضرورة العمل على تضمين الأسلحة السيبرانية فى مجال اتفاقيات الحد من التسلح، وأن يتم التوصل إلى اتفاقية خاصة بالحد من الأسلحة [٣] السيبرانية [٤]، كما تناولتها بعض الدراسات العربية بالبحث، مركزة علي طبيعة

---

(١) د. **صفات أمين سلامة**، المرجع السابق، ص٤٣، ويتسع لذلك اصطلاح حرب المعلومات "Information Warfare" وهو اصطلاح ظهر في بيئة الإنترنت للتعبير عن اعتداءات تعطيل المواقع وإنكار الخدمة والاستيلاء علي المعلومات. انظر: د. **أحمد الشربيني ود. وفائي بغدادي**، المرجع السابق، ص٧.

(٢) د.**عادل عبد الصادق**، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، سلسلة أوراق، سلسلة تصدر عن وحدة الدراسات المستقبلية بمكتبة الإسكندرية، العدد الثالث والعشرون، ص ٥٧.

(٣) وقد تناولت الدراسة جوانب عديدة مهمة، من بينها: الفضاء الإلكتروني، والتحول في مفهوم الأمن والقوة والصراع العالمي- الهيمنة السيبرانية cybernetics والمزايا الإستراتيجية للأسلحة الإلكترونية- أثر الفضاء الإلكتروني في القانون الدولي العام وقانون الحرب - تطبيقات القانون الدولي الإنساني علي استخدامات الأسلحة الإلكترونية - التحديات الإشكاليات في سبيل التعاطي القانوني مع الأسلحة الإلكترونية، د. **عادل عبد الصادق**، المرجع السابق، ص ١٥٥.

(٤) أما **السبرانية**؛ فقد استخدم العلماء هذا المصطلح قديماً لمساواة معالجة المعلومات بآلية التغذية الراجعة الطبيعية، ووضع الباحثون نظرية مفادها أن الكائن الحى ينظم نفسه ذاتياً للبحث عن مستوى النجاح أو الإخفاق لسلوك معين ويستخدم نتيجته كأساس لتعديل السلوك المستقبلى، وجادلوا بأن الأجهزة الميكانيكية يمكنها أن تعمل بنفس الطريقة. انظر: **ليزانوكس**، قصة تكنولوجيا الروبوتات، الدار العربية للعلوم، ناشرون، ٢٠١٢، ص١٢٦.

الهجمات التى تقوم بها [١] ومدى خضوعها لقواعد المسئولية [٢] الدولية.

كما أصبح مفهوم الهجوم مختلفاً عن شكله التقليدى، حيث أصبح جهاز يستخدم لمهاجمة أجهزة أخرى، و إمكانية إصابة الهدف بسهولة عن طريق هجوم الفضاء الإلكترونى، وخاصة إصابة مراكز القيادة والسيطرة الخاصة بالبنية التحتية الحرجة كمحطات الطاقة، بالإضافة إلى أنظمة التسلح، وفى العمليات الحربية العدائية، وساعد انتشار تكنولوجيا المعلومات – وعلاقتها المباشرة بالجوانب المدنية والعسكرية– إلى اتساع ميدان الحرب، لتمتد إلى حرب وهجمات متعددة الأبعاد، والتى تشمل الأرض والبحر، والمجال الجوى والفضاء الخارجى والإلكترونى [٣].

لذا بات من الأهمية بمكان الحديث عن أسلحة الفضاء الالكترونى، مع الإشارة إلى أوجه الاختلاف بينها وبين ما قد يشتبه بها من أسلحة، ومخاطر أسلحة الفضاء الالكترونى وهو ما سوف نتطرق اليه على النحو التالى:

تحديد أسلحة الفضاء الإلكترونى

قد تختلط المفاهيم من ناحية التعرف علي كنه الأسلحة محل البحث وطبيعتها؛ لذا كان من اللازم التفريق بينها و بين ما يشتبه بها من أسلحة، و يلعب العامل

(١) إذ تعرض مصطلح الهجوم السيبراني إلي تعاريف عدة من زوايا مختلفة، وإن كانت مشتركة علي مضمون متقارب في المعني، وهو استهداف مواقع الكترونية من خلال عدة وسائل اتصال الكترونية أخري . انظر: د. **أحمد عبيس**، الهجمات السيبرانية، مفهومها والمسئولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، بحث منشور بمجلة المحقق الحلي للعلوم القانونية والسياسية، العدد الرابع، السنة الثامنة، ٢٠١٦، ص ٦١٦.

(2) See. Ugo Pagallo, the laws of robots " crimes, contracts, and torts, law, governance and technology series, volume 10, 2013. P35.

(٣) د.**عادل عبد الصادق**، الإرهاب الإلكتروني- القوة في العلاقات الدولية: نمط جديد وتحديات مختلفة، مركز الدراسات السياسية والاستراتيجية، ٢٠٠٩، ص ١٠٨.

التكنولوجى دورا بارزا فى وضع التباس بين الأسلحة الذكية و بين أسلحة الفضاء الإلكترونى من ناحية، و من ناحية ثانية فإن تطورات الذكاء الاصطناعى التى أدت إلى استحداث أسلحة قتالية[١] – أطلق عليها الأسلحة ذاتية التشغيل- قد يشكل موضع التباس بسبب اشتراكهما فى الاعتماد على التكنولوجيا الحديثة مما يستلزم فض هذا الالتباس علي النحو الأتي:

١- أسلحة الفضاء الإلكترونى والأسلحة ذاتية التشغيل

اعتبر البعض أن الفضاء الخارجى سيصبح مسرح العمليات العسكرية فى القرن الحادى والعشرين، ولهذا فليس من المستغرب أن يوضع التسلح الفضائي على قائمة الأولويات المهمة فى الإستراتيجيات العسكرية فى المستقبل[٢]،

و اعتبر البعض الخطر الأكبر المحتمل من الأسلحة ذاتية التشغيل هجمات القرصنة، والتى من الممكن أن تؤدى إلى كارثة حقيقية من سيطرة طرف آخر على الأسلحة بعد التطور الكبير فى مجال الفضاء السيبرانى، و إعطاءها أوامر مضادة أو

---

(١) و من اللازم في هذا السياق لفت الانتباه إلى اختلاف الأسلحة ذاتية التشغيل عن الأسلحة الذكية، و قد تناولنا تحليلا مفصلا للعلاقة بينهما و أوجه الشبه و الاختلاف حتى بدا لنا - بمنتهي البساطة- أنه و إن كانت الأسلحة الذاتية التشغيل تعمد علي التشغيل الذاتي في استقلالية عن التدخل البشري؛ فان الأسلحة الذكية هي أسلحة موجهة، تتميز بدقتها الشديدة، وهذا هو مظهر الذكاء فيها . انظر : **د.أبوبكر محمد الديب**، التطبيقات العسكرية للذكاء الاصطناعى، دار النهضة العربية، ٢٠٢١، المطلب الأول من المبحث الأول من الفصل الأول من الباب الثانى.

(٢) د. **صفات أمين سلامة**، المرجع السابق، ص٣٧. وحول **استخدامات الروبوتات في الاستكشاف الكوكبي**، انظر: **ليزانوكس**، المرجع السابق، ص٢٤٥. وفي تقرير لمجلة Computer World أشارت فيه إلي أن التطور في مجال الروبوتات يمكن أن يكون له عواقب وخيمة علي البشر في١٠ مهن منها: رائد الفضاء، فالروبوت "روبونوت ٢" Robonaut2 من وكالة الفضاء الأمريكية " ناسا " هو روبوت بارع شبيه بالبشر، أرسل في عام ٢٠١١ إلي محطة الفضاء الدولية في الفضاء الخارجي في مهمة لمساعدة روادها علي القيام بالمهمات الخطيرة والروتينية كالتنظيف، وحاز الروبوت جائزة ١" الروبوتات وأتمتة الفضاء " في عام ٢٠١٣ من المعهد الأمريكي لريادة الفضاء، انظر في ذلك: د. د. **صفات أمين سلامة، وخليل قورة**، تحديات عصر الروبوتات وأخلاقياته، مركز الإمارات للدراسات والبحوث الإستراتيجية، ص٥٩.

تعليمات بقتل المدنيين [١].

وتشترك أسلحة الفضاء الإلكترونى مع الأسلحة ذاتية التشغيل فى مخاطر التسلل واختراق الأنظمة الإلكترونية والتحكم بها عن بعد[٢]**، كما يثور بالأذهان ما إذا كان صناعها قد أولوا اهتماماً بالجانب الأخلاقى** [٣] **الذى حظي باهتمام صناع الروبوتات** [٤] **والآليات ذاتية التشغيل .**

كما يشتركان فى إمكانية التعرض للاختراق والقرصنة، لكن المشاكل القانونية المتوقع إثارتها بسبب استخدام هذه الأسلحة قد تكون أكثر عمقاً عند استخدام أسلحة الفضاء الإلكترونى بسبب عملها فى بيئته اللامحدودة، فى حين يمكن تقييد نطاق استخدام الأسلحة ذاتية التشغيل بشكل أكبر.

بيد أن الخلاف الرئيس بينهما يكمن فى اعتماد الأسلحة ذاتية التشغيل على تقنية الذكاء الاصطناعى *دون غيرها من الأسلحة* [٥] **.**

---

(1) Micheal N.Schmitt, Featuress Autonomous, op.cit, p7.

(٢) حول التحديات الهائلة في هذا الشان في مجال الروبوتات، انظر: د. **صفات أمين وخليل أبوقورة**، المرجع السابق، ص٤١.

(٣) حول الجوانب الأخلاقية للتقدم التكنولوجي، انظر: **رأوبلود**، ترجمة أسامه أمين الخولي، محمد مرسي أحمد، الإنسان والطاقة، مكتبة الأسرة، ص١٢١.

(٤) برزت علي السطح مجالات بحثية حديثة ومثيرة للاهتمام في البحوث العلمية الفلسفية تعرف باسم: " أخلاقيات الروبوت" Roboethics، والتي تهتم بإعطاء الآلات المباديء الأخلاقية أو الإجراءات اللازمة لاكتشاف أساليب لحل المعضلات الأخلاقية من خلال صنع قراراتها بنفسها، كما يقصد بأخلاقيات الروبوت أخلاقيات البشر من مصممي الروبوتات ومصنعيها ومستخدميها. انظر: " د. **صفات أمين وخليل أبوقورة**، المرجع السابق، ص٤١.

(٥) لكن هذا لا يمنع من إضافة تقنية الذكاء الاصطناعى إلى أسلحة الفضاء الالكترونى، وطالما أنها تقنية مضافة فهذا لا يغير من طبيعتها بل تبقي منسوبة إلي اسلحة الفضاء الالكترونى.

٢- أسلحة الفضاء الإلكتروني و الأسلحة الذكية

من المؤكد أن الأسلحة الذكية باتت تمثل قوة تدميريةً كبيرة الأهمية؛ لذا تتسابق على اقتناءها معظم الجيوش، وذلك على الرغم من تكاليفها العالية، فبالإضافة إلى قدرتها التدميرية و دقة أداءها وتمييزها، فهى أيضا تتمتع بخواص القيام بتوجيهها ناحية أهدافها بدقة بالغة، فضلاً عن سرعتها الكبيرة التى زادت عن سرعة الصوت، مما جعل أهدافها تقف مكتوفة الأيدى وعاجزة تماما عن المراوغة أو الهروب منها استعداداً للتدمير، ولذلك باتت الصواريخ بالأخص تتزايد قوتها التدميرية، وذلك فى حالة مقارنتها بالصواريخ أو القذائف الموجهة فى الحرب العالمية الثانية ١٩٣٩ إلى ١٩٤٥ [(١)] .

و رأى البعض فى الأسلحة الذكية حلماً من أحلام البشرية [(٢)]، بالنظر إلى المزايا التى من الممكن أن تحققها، إذ أصبح المطلوب – سياسياً وعسكرياً- هو أسلحة وتكتيكات من شأنها أن تمنع – قدر الإمكان- الخسائر بين أفراد الجيش المحارب، وتصيب الأهداف العسكرية، وتقلل الوفيات والإصابات والأضرار العرضية إلي الحد الأدني المطلق، ومن ثم، ثار التساؤل عن الأسلحة الذكية، هل هى العلاج الشافى[(٣)] ؟

---

(١) **رضا إبراهيم محمود**، الأسلحة الذكية تصلح للجيوش الذكية، مجلة المسلح، الحادي عشر من يوليو ٢٠١٣، ص٢.

(٢) كتب بلاي وايتباي **أننا بصدد الدخول في عصر سوف يكون اعتمادنا الأول فيه علي الآلات الذكية شديدة التطور لمساعدتنا في أداء العديد من المهام الفكرية، وتشير جميع الشواهد إلي استخدام هذه الآلات كنقطة انطلاق إلي مزيد من التقدم والتطور في العلوم البشرية.** انظر: **بلاي وايتباي**، الذكاء الاصطناعي، دار الفاروق، ٢٠٠٨، ص١٣.

(٣) **أ.ب. روجرز**، خوض الحرب بلا خسائر في الأرواح، المجلة الدولية للصليب الأحمر، مختارات من أعداد عام ٢٠٠٠، ص ٢٥.

وتتميز الأسلحة الذكية بأن إمكانية اتخاذ الاحتياطات تتطور من خلال الخبرة، وعلى المقاتلين الالتزام بالتنبؤ بالإجراءات ذات الصلة، لتجنب وقوع الحوادث فى المستقبل(١)، إذ أنها تزيد من الخيارات المتاحة للمهاجم، فالمهاجم ليس مطالباً – فحسب– بتقدير الاحتياطات العملية التى يمكن اتخاذها لتقليل الخسائر العرضية إلى الحد الأدنى، وإنما يتعين عليه – أيضا– أن يعقد مقارنةً بين التكتيكات أو الأسلحة المختلفة، بحيث يستطيع أن يختار المسار القتالى الذى تنجم عنه أقل الأضرار، والقادر فى الوقت نفسه على تحقيق النجاح العسكرى(٢).

فأثناء حرب الخليج عام١٩٩١، استخدمت فى البداية طائرات "التورنادو" التابعة للسلاح الجوى البريطانى، لمهاجمة المطارات العراقية بإسقاط قنابل jp233 من ارتفاع منخفض فوق الهدف، وكان الغرض من الهجوم من ارتفاعات منخفضة هو تفادى رادارات العدو وزيادة عنصر المفاجأة، ولكن السلاح الجوى البريطاني فقد خمس طائرات خلال سبعة أيام، مما أدى إلى استخدام هذه الطائرات فى إلقاء قنابل حديدية زنة ١٠٠٠ رطل من ارتفاع ٢٠ ألف قدم، وهو ارتفاع يجعلها خارج مدى المدافع المضادة للطائرات، لكنه يجعل تصويب القنابل أقل دقة، وإزاء المطالبة باستخدام تكنولوجيا ذكية، قام السلاح الجوى البريطاني باستخدام طائرات من طراز "بوكانير" مزودة بأجهزة ليزرية (٣) لتعيين الهدف، إلي جانب طائرات " تورنادو" تحمل

---

(١) **ماركوساسولي**، المرجع السابق، ص١٦٢.

(٢) **أ.ب. روجرز**، المرجع السابق، ص٣١ .

(٣) وتعمل أنظمة المدي الليزرية علي مبدأ انعكاس ضوء الليزر علي سطح الجسم، ليقوم حساس ضوئي باستلام هذا الضوء المنعكس، ثم يقيس الوقت أو المدة بين الإرسال والاستقبال لكي يحسب العمق، انظر: د. **بشير علي عرنوس**، الذكاء الاصطناعي، دار السحاب للنشر والتوزيع، الطبعة الأولي، ٢٠٠٨، ص٢٢٢.

أسلحة موجهة بالليزر[١]، " TIALD "، و أدت هذه التغييرات إلى تحسن مشهود في دقة التصويب على الأهداف[٢].

و استشرافا لمستقبل الذكاء الاصطناعى يمكن *للروبوت الذكى* *Intelligent robot* – ذاتياً- اتخاذ القرار بشأن العملية المقدم عليها، في ضوء المعلومات التى يقوم بتجميعها عن الظروف المحيطة به، مستخدماً مستشعراته اللمسية والبصرية والصوتية وأحيانا السمعية، ويزود هذا الروبوت عادةً بحاسوب متقدم وببرامج جاهزة لمنظومات الذكاء الاصطناعى التى يمكنها تغيير مدخلاتها وفقاً للإشارات المرتدة من المستشعرات sensors [٣]، ومؤخراً، تحولت فكرة الآلات الذكية إلى الآلات [٤] فائقة الذكاء [٥].

وقبل ظهور أسلحة الفضاء الإلكترونى، أشار البعض أن الأسلحة الموجهة عن بعد تجرد الحرب من أى عنصر إنسانى، حيث تتحول الحرب –عندئذ- إلى نشاط بارد خال تماماً من المشاعر، يتم تنفيذه بدقة عالية، فكلما ازداد المهاجم بعداً عن

---

(١) حول الليزر، انظر: د.**محمد أديب رياض غنيم**، التطور التكنولوجي في مصر، الهيئة المصرية العامة للكتاب، ٢٠١٢، ص٣٥٧ .

(٢) للمزيد، انظر: **أحمد حجاج**، القنابل العنقودية - الأبرياء يدفعون الثمن، مجلة السياسة الدولية، العدد ١٦٦، أكتوبر٢٠٠٦، المجلد الحادي والأربعون، ص ١٥٤، ويشار إلي أن العلميين أشاروا إلي أن أغلب الماسحات الليزرية تعمل علي مسافات بعيدة " خمسة عشر مترا " ولذلك ينقصها مهام الرؤية المفصلة، د. **بشيرعرنوس**، المرجع السابق، ص٢٢٢.

(٣) د. **أنور محمود عبد الواحد، ود. أحمد أمين عبد المجيد**، الروبوت بين الخيال والعلم، ١٩٩٦، مركز الأهرام للترجمة والنشر، الطبعة الأولي، ١٩٩٦، ص٥٠ .

(٤) وما يبدو بمنتهي البساطة أنه وإن كانت الأسلحة ذاتية التشغيل تعتمد علي التشغيل الذاتي في استقلالية عن التدخل البشري، فإن الأسلحة الذكية هي أسلحة موجهة، تتميز بدقتها الشديدة، وهذا هو مظهر الذكاء فيها.

(٥) د. **صفات أمين، وخليل أبوقورة**، المرجع السابق، ص٨١ .

الهدف الذى يريد إصابته، كلما قل إدراكه للخسائر الإنسانية التى يمكن أن تنجم عن عمله، ذلك أنه لا يرى الآثار التى يحدثها الهجوم، ويقال أحيانا أن هذا يؤدى إلي تجريد الحرب من أى طابع إنسانى(١) .

وقد تساءلت مؤسسات دولية عما إذا كان ينبغي اعتبار نظم الأسلحة الموجهة عن بعد أسلحة قانونية فى سياق إنفاذ القانون دون نقاش، مثلما هى فى النزاعات المسلحة، فالعلاقة بين الدول ومن يخضعون لحمايتها مختلفة جداً عن علاقتها بمن تعتبرهم أعداءها أثناء نزاع مسلح(٢).

أ- مخاطر أسلحة الفضاء الإلكترونى :" الهجمات السيبرانية و خصائصها "

يعتبر مفهوم الهجمات السيبرانية من المفاهيم الحديثة نوعا ما، وهى تشير إلى أساليب الجريمة التى تعتمد – فى الأساس– على تكنولوجيا المعلومات وهى تستهدف الحاسبات والمواقع الإلكترونية، كما أنها تتضمن عمليات التسلل إلى أنظمة الحاسب الألى والقيام بجمع البيانات ومحاولة تصدير تلك البيانات أو إتلافها أو تغييرها، كما أن تلك الهجمات تتضمن القيام بعمليات زرع برمجيات ضارة بغرض التجسس(٣) .

وتعد الهجمات السيبرانية حديثة، حيث ارتبطت بالثورة التكنولوجية التى عرفها المجتمع مع تزايد اعتماد الأفراد على وسائل التكنولوجيا والاتصال وما واكبها من تحديات كبرى، وتختلف تعريفات الهجمات السيبرانية حسب طبيعة كل دولة وكذلك

(١) **أ.ب. روجرز**، المرجع السابق، ص٢٦ .

(2) A/69/265 p 19.

(٣) **عمار ياسر محمد زهير**، التحديات الأمنية المعاصرة للهجمات السيبرانية، القيادة العامة لشرطة الشارقة مركز بحوث الشرطة، المجلد ٣٠، العدد ١١٨، ٢٠٢١، ص٢٧.

الاستراتيجية التى تعتمد عليها ومدى ارتباطها بالعالم الرقمى، والتى تعتمد على مدى تفعيل الحكومة للنظم الإلكترونية وكيفية توظيف شبكات المعلومات ووسائل الاتصال، وتوصيل الخدمات للمواطنين داخل الدولة فى مجالها المدنى من جهة واستخدام تلك التكنولوجيا فى المجالات العسكرية والنواحى الدفاعية من جهة أخرى(١).

١-خصائص الهجمات السيبرانية:

مع تنامى الثورة التكنولوجية والمعلومات برزت مخاطر الهجمات الإلكترونية كواحدة من أهم المخاطر التى تواجه الدول؛ وذلك بسبب ازدياد التقارب التكنولوجى العالمى الذى أدى إلى تبديد الفواصل المادية والرقمية بين الدول، وقد أشار المنتدى الاقتصادى العالمى - فى تقريره عن المخاطر الدولية- إلى ارتفاع المخاوف من المخاطر التكنولوجية لا سيما الهجمات السيبرانية، كما تصدرت الهجمات السيبرانية القائمة العالمية فى المخاطر التى تواجه النظام العالمى فى عام ٢٠١٨(٢) .

وتتسم الهجمات السيبرانية ببعض الخصائص يمكن تحديدها على النحو الأتى(٣):

(١) **سحر قدوري الرفاعي**، الحكومة الالكترونية وسبل تطبيقها: مدخل استراتيجي، مجلة اقتصاديات شمال افريقيا، العدد السابع، جامعة حسيبة بو على، ٢٠١٦، ص٣٠٨.

(٢) **علم الدين باتقا**، مخاطر الهجمات الالكترونية (السيبرانية) وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجي، دراسات تنموية، المعهد العربي للتخطيط، الكويت، العدد٣٦، ٢٠١٩، ص١٠.

(٣) **نور أمير الموصلي**، الهجمات السيبرانية في ضوء القانون الدولي الإنساني، رسالة ماجستير، الجامعة الافتراضية السورية، ٢٠٢١، ص١١.

١-تعد الهجمات السيبرانية سهلة الاستخدام، كما أنها متوفرة على نطاق واسع، كما أنها تمكن مستخدميها من القيام بهجمات متعددة تتجاوز مستوى قدراتهم الحقيقية.

٢-تخضع الهجمات السيبرانية لعمليات تحديث وتطوير دائم؛ الأمر الذى يترتب عليه زيادة القدرة التدميرية لتلك الهجمات وفاعليتها.

٣-تتسم الهجمات السيبرانية بالقدرة على اختراق أكثر أنظمة الحماية تعقيدا، بالإضافة الي قدرة تلك الهجمات على إصابة أنواع مختلفة من الأجهزة الإلكترونية سواء كانت تلك الأجهزة حاسبا أليا أو مقدم خدمة أو أى جهاز متصل بشبكة إلكترونية(١).

٤-تتسم الهجمات السيبرانية بصعوبة تحديد مصدرها حيث لا يعلن منفذ تلك الهجمات – فى أغلب الاحوال- عن تلك الهجمات فتظل مجهولة المصدر.

٥-في الهجمات السيبرانية يختفى العامل الجغرافى بحيث يصبح أى مركز أو منشأة تحت تهديد تلك الهجمات و لا يقتصر على الأرض، بل إن التهديد بتلك الهجمات قد يصل إلى الفضاء من خلال إرسال فيروسات إلى الأقمار الصناعية؛ من أجل محاولة تعطيلها أو سرقة البيانات الموجودة فيها.

٦-تعتبر الهجمات السيبرانية أقل كلفة من الحروب التقليدية، كما أن تلك الهجمات تعتبر عاملا مساعدا فيها، كما تعتبر الهجمات السيبرانية أداة مؤثرة فى السياسة والاقتصاد على الصعيد الدولى، ولعل السبب فى ذلك يرجع إلى انتقال جزء كبير من الصراعات بين الدول إلى الفضاء الإلكترونى مع تزايد ارتباط العالم بالفضاء الإلكترونى تزامنا مع تراجع دور الدولة فى ظل العولمة وانسحابها مع بعض

(١) **طلال ياسين العيسي**، المرجع السابق، ص٨٦.

القطاعات الاستراتيجية لمصلحة القطاع الخاص، بالإضافة إلى تصاعد أدوار الشركات متعددة الجنسيات لا سيما التى تعمل منها فى مجال التكنولوجيا.

٧-يترتب على الهجمات السيبرانية خسائر مالية ضخمة، كما أنها قد تؤدى إلى خسائر فى الأرواح فى حالة تجاوز تلك الهجمات قطاعات حساسة مثل أنظمة المستشفيات وأنظمة التبريد فى المفاعلات النووية.

٨-تتميز الهجمات السيبرانية بأنه لا يسبقها أى مؤشرات حيث أنها قد تحدث فى أى مكان وفى أى وقت وبسرعة كبيرة.

٢-أنواع الهجمات السيبرانية:

يقوم الأفراد بشن تلك الهجمات على المواقع التابعة للحكومة أو المواقع التابعة للأفراد؛ من أجل اختراق تلك المعلومات والحصول على المعلومات والبيانات التى تحتوى عليها تلك المواقع.

وتتنوع الهجمات السيبرانية، على النحو الأتى:

-هجمات الحرمان من الخدمة:

ويهدف هذا النوع من أنواع الهجمات السيبرانية إلى حرمان المستخدمين من خدمات معينة، أو التأثير على تلك الخدمات و وصولها بشكل ضعيف إليهم، ويطلق على أخطر أنواع هذا الهجوم اسم (DDOS-D ISTRIBUTED DENIAL OF SERVICE) ويعنى رفض الخدمة الموزعة، وفى ذلك النوع من الهجوم يقوم المهاجم باستغلال مجموعة من أجهزة الحاسب الألى لأشخاص لا يعرفهم، إلا أنه قام باستغلال بعض الثغرات الموجودة فى تلك الأجهزة فى أكثر من مكان، ويقوم المهاجم

بمهاجمة سيرفر معين أو شبكة معينة باستخدام تلك الأجهزة دون علم أصحابها[١].

ومن أبرز الأمثلة علي ذلك النوع من الهجوم ما تعرضت لها إستونيا فى عام ٢٠٠٧ من ذلك النوع من الهجمات والتى استهدفت البنية التحتية والمواقع الإلكترونية الخاصة برئيس الوزراء والبرلمان وعددا من الوزارات والبنوك، ولقد جاء ذلك فى ظل الاضطرابات التى شهدتها إستونيا فى تلك الفترة من الروس الموجودين فى إستونيا وتوجيه الحكومة الروسية لانتقادات شديدة للحكومة لإستونيا، كما تعرضت هيئة الإذاعة البريطانية bbc إلى هجوم فى ديسمبر عام ٢٠١٥ وكان الهجوم بسعة ٦٠٠ جيجابت فى الثانية وقد كان هذا أكبر هجوم تم تسجيله[٢] .

-الفايروسات او البرامج الخبيثة:

تعد الفيروسات برامج مثلها مثل أى برامج أخرى، ولكن تم تصميمها من قبل أحد المخربين بهدف إحداث أكبر قدر من الضرر للنظام بعد أن يتم ربطه بالبرامج الأخرى، وهو يمتلك القدرة على تكرار نفسه حتي يبدو وكأنه يتوالد ذاتيا، مما يمنحه القدرة على القيام باستهداف برامج أخرى فى الحاسب ومواقع أخرى فى الذاكرة؛ من أجل العمل على تدميرها، وتضاف الفيروسات إلى أحد البرمجيات أو إلي نظام تشغيلى من نظام تشغيل الحاسب الألى ويقوم ذلك البرنامج الدخيل بمجموعة من العمليات التى تؤثر – بصورة مباشرة أو غير مباشرة– فى خصائص نظام التشغيل أو المعلومات المخزنة[٣] .

---

(١) **نور أمير الموصلي**، المرجع السابق، ص١٦.

(٢) **عمار ياسر محمد زهير**، التحديات الأمنية المعاصرة للهجمات السيبرانية، المرجع السابق، ص٣٦-٣٧

(٣) **حسن مظفر الرزو**، الفايروسات والحاسب الإلكتروني: المخاطر المحتملة وسبل الحد منه، المجلة العربية العلمية للفتيان، المنظمة العربية للتربية والثقافة والعلوم، المجلد الاول، العدد الثاني، ١٩٩٧، ص٤.

وقد حدد المركز القومي للحاسبات فى الولايات المتحدة الامريكية الفيروسات على أنها برامج مهاجمة تقوم بإصابة أنظمة الحاسب بأسلوب يشبه – وبشكل كبير- الفيروسات الحيوية التى تصيب جسم الإنسان، و تتمثل أبرز خصائص الفيروسات – بصورة عامة- فى قدرة تلك الفيروسات على الاختفاء وسرعتها فى الانتشار وقدرتها على اختراق المواقع الإلكترونية وتدميرها(١).

ومن الأمثلة علي ذلك ما قام به مجموعة من الهاكرز من روسيا بزراعة برنامج خبيث فى نظام تابع لشركة solar winds، وعندما قامت الشركة بعمل تحديث لبرنامجها الذى يتم استخدامه من قبل أكثر من ٣٠٠٠٠٠ عميل حول العالم قامت الشركة بإرسال التحديث لعملائها محملا بالفيروس الذى زرعه الهاكرز داخل النظام، وقد فتح هذا الفايروس بابا خلفيا فى أنظمة الجهات التي استقبلت التحديث، وقد استغل الهاكرز هذه الثغرات لتركيب برمجيات إضافية علي الأجهزة والأنظمة التى أصيبت بذلك الفيروس الذى تم تحميله مع التحديث، والذى سمح للهاكرز بأن يقوموا بالتجسس على أنظمة الجهات التى قامت باستقباله، وقد أعلنت شركة solar winds أن هناك أكثر من ١٨٠٠٠ عميلا قاموا بتحميل التحديث على أنظمتهم وهم عرضة للاختراق(٢) .

-برامج القنابل المعلوماتية:

وهي نوع أكثر تقدما من البرامج الخبيثة، وهى عبارة عن تعليمات برمجية

(١) ويعود الفضل فى وضع أول تصور لفيروس معلوماتى إلى الدكتور "فريد كوهن" وذلك فى الحلقة الدراسية التى قام بإلقائها فى الولايات المتحدة الأمريكية بجامعة كاليفورنيا، والتى تناولت أمن الحاسب الألى،**عمار عباس الحسيني**، جرائم الحاسوب والانترنت (الجرائم المعلوماتية) الطبعة الأولي، منشورات زين الحقوقية،لبنان، ٢٠١٧، ص١٤١.

(٢) **عمار ياسر محمد زهير البابلي**، التحديات الأمنية المعاصرة للهجمات السيبرانية، ص٣٩-٤٠.

ضارة مصممة بحيث تعمل عند حدوث أحداث معينة أو تحت ظروف معينة أو لدي تنفيذ أمر معين، وتقوم بتخريب ومسح البيانات أو تعطيل النظام، وقد تظل لفترة طويلة من الزمن ثم يتم تفعيلها، وقد تسبب أضرارا بالغة لجهاز الحاسب الألى المصاب مما يجعله غير صالح للاستعمال(١) .

و يتم استخدام هذه البرامج من أجل تدمير المعلومات والبيانات وتغيير برامج ومعلومات النظام، كما يمكن استخدامها لغرض حماية بعض برامج الملكية من خطر الاختراق، ويظهر ذلك بصورة واضحة فى الحملات الإعلانية كما هو الشأن فى المجلات التى يوزع معها بعض الأقراص كهدية وتحتوى على برامج، بالإضافة إلى وجود تلك البرامج الخبيثة فى عدد من مواقع الإنترنت، كما أنه من الممكن أن تظهر فى بعض البرامج المؤجرة، و التى لا يفقد مالكها حقوق الملكية الواردة عليها، وفى تلك الأحوال إذا توقف المستأجر عن دفع القيمة الإيجارية التى تم الاتفاق عليها بينهما فيقوم المالك بإرسال قنابل البرامج المعلوماتية والتي قد تكون موجودة أصلا فى البرامج المستأجرة، ومن ثم فإن المالك لا يقوم بإرسال ما يوقف انفجارها(٢).

ومن الأمثلة عليها الهجوم الإلكترونى الذى حدث فى عام ٢٠١٦، والذى استهدف الهيئة العامة للطيران المدنى السعودى وعددا من المؤسسات الحكومية، وكان عبارة عن قنبلة إلكترونية موقوتة تم زرعها مسبقا وبدأت البرمجيات الخبيثة

(١) **طلال محمد الحاج ابراهيم**، الهجمات الالكترونية والمسؤولية الجنائية للقادة، المجلة القانونية والقضائية، وزارة العدل-مركز الدراسات القانونية والقضائية، السنة ١٢، العدد الأول، ٢٠١٨، ص٣٠٥.

(٢) **عمار عباس الحسيني**، التحديات الأمنية المعاصرة للهجمات السيبرانية، المرجع السابق، ص١٤٤.

بمحو البيانات المخزنة فى أجهزة الكمبيوتر ثم سيطرت هذه البرمجيات على أجهزة الكمبيوتر ومنعت إعادة تشغيلها (١).

-برامج الدودة:

يقصد ببرامج الدودة: تلك البرامج التي تستفيد من الثغرات الموجودة فى أنظمة تشغيل الحاسب الألى، والتى تنتقل من جهاز إلى أخر؛ الأمر الذى يترتب عليه احتلال الشبكة بالكامل، وتتسبب فى أثار مدمرة، وبفضل الوصلات التى تربط تلك الحواسب ببعضها البعض فإنها تتمكن من الانتقال من شبكة إلى أخرى، ومن أهداف تلك البرامج شغل أكبر قدر ممكن من سعة الشبكة وبالتالي العمل على تقليل أو خفض كفاءة تلك الشبكات، كما أن أهداف برامج الدودة قد تتعدي ذلك لتبدأ التكاثر والانتشار وتقوم بالتخريب الفعلي للملفات والبرامج وأنظمة التشغيل وبروتوكولات الاتصال(٢).

ومن أكثر الطرق وضوحا لنشر برامج الدودة مرفقات البريد الإلكترونى المصابة والتنزيلات التلقائية التى تحدث عند القيام بزيارة بعض المواقع على الإنترنت أو التسلل عبر الثغرات الأمنية فى أنظمة التشغيل أو برامج الحماية، كما تتجلى أضرار برامج الدودة فى أنها تسمح للمهاجم باستخدام الحاسب الألى المصاب؛ ليقوم -من خلاله- بمهاجمة مواقع الإنترنت أو إرسال بريد إلكترونى يحتوى على تلك البرامج أو القيام بتنزيل برامج ضارة إليه(٣).

---

(١) **إبراهيم محمد بن حمود الزنداني**،الجرائم الإلكترونية من منظور الشريعة الإسلامية وأحكامها في القانون القطري والقانون اليمني: دراسة مقارنة، جامعة فطاني، ٢٠١٨، ص٦٨.

(٢) **نور أمير الموصلي**، المرجع السابق، ص١٨.

(٣) **عمار عباس الحسيني**، التحديات الأمنية المعاصرة للهجمات السيبرانية، المرجع السابق،

وقد أطلقت دودة الإنترنت عن طريق طالب فى قسم علوم الكمبيوتر بجامعة كورنيل بولاية نيويورك، حيث تعمد الطالب بث برنامج دودة الإنترنت ليثبت عدم ملاءمة أساليب وسائل الأمان فى شبكات الحاسوب ولكنه تسبب فى تدمير الألاف من شبكات الحواسيب المنتشرة فى الولايات المتحدة، بالإضافة إلى إعاقة طريق ومسلك الشبكات بخلاف الخسائر المالية الكبيرة التى تسبب فيها[١] .

ومن الملاحظ أن الهجمات السيبرانية تتخذ صورا و أشكالا عديدة ولا تقتصر على نوع واحد، حيث أنه وبفضل التطور التكنولوجى الذى يشهده العالم تطورت تلك الهجمات، ومن المحتمل أن تظهر أنواع جديدة من تلك الهجمات فى المستقبل وقد تكون أكثر خطورة من تلك الهجمات، الأمر الذى يتطلب السعى نحو الحد من تلك الهجمات.

ص١٤٥.

(١) **محمود مدين**، فن التحقيق والاثبات في الجرائم الالكترونية، بدون دار نشر، ٢٠٢٠، ص٥٤.

ثانيا
الإرهاب الإلكترونى

أضحى الإرهاب الآن هو الهاجس الذى تعيشه جميع الدول ويتخوف منه الأفراد، حتى أصبح جزءاً من الحياة اليومية، و لا يكاد يمر يوم دون أن تقع عملية إرهابية فى مكان ما من العالم، وأصبحت أنباء وأخبار الإرهاب تحتل الصدارة وتحظى بجذب انتباه الناس على اختلاف مستوياتهم الثقافية وميولهم السياسية ومواقع وجودهم على ظهر الأرض .

و رغم أن الإرهاب قديم قدم التاريخ إلا أنه اتخذ – فى الوقت الحاضر– بعداً جديداً مثيراً للقلق، خصوصاً بعد انتشار التقنية الحديثة بصورة مذهلة بشكل مكن الإرهابيين من تنفيذ عمليات دموية مدمرة بأقل مجهود و دون تمكن الجهات الأمنية من منعهم إبتداءاً أو ضبطهم بعد ذلك، ولقد كان لظهور شبكة المعلومات (الإنترنت) دور كبير فى تنفيذ الإرهابيين لعملياتهم المدمرة .

فالعالم يدخل الألفية الثالثة بثورة متنامية فى تكنولوجيا المعلومات و الاتصالات، و تعتمد هذه الثورة العلمية على التقدم العلمى فى علوم الحاسب و نظم التحكم الرقمى(١).

ويُعد الإرهاب الإلكترونى أحد الموضوعات التى تحتل حيزاً مهماً فى النقاشات المُثارة على الساحة الدولية خلال الفترة الأخيرة، ليس لكونه أمراً غير اعتيادي فى طبيعته، بل لأسباب وحجم التهديدات التى يفرضها على المستويات المختلفة "الدول،

(١) **د.عبد المقصود حجو**، نظم التحكم الألى الرقمية الحديثة، دار الكتب العلمية للنشر والتوزيع، ص ٧.

والشركات، والأفراد" [١].

كما أن التهديدات التى يقوم بها إرهابيو الإنترنت "الإرهابيون السيبرانيون" تمثل تحدياً مضاعفاً؛ لأنها تتطلب، عند تحليلها، الأخذ فى الاعتبار عدة عوامل أهمها: دوافع الإرهابيين، وكذلك قدراتهم على إحداث الضرر، وأهم نقاط ضعفهم، ومدى قدرتنا على الدفاع عن أنفسنا فى مواجهة مثل تلك التهديدات[٢].

وتعود إلى أسباب متشابكة، سياسية واقتصادية وثقافية، تتفاعل فى إطار سنة التدافع بين الأمم والشعوب، وما لم ينهض العالم بدوره فى التصدي لمشكلاته بنفسه، وإعطاء الشعوب حقها فى الكرامة والعدالة والحرية، والدفاع عن المقدسات والمصالح المشروعة فى إطارٍ من التوازن والعدل، ما لم يتمّ ذلك فسنظل نعاني من اختلالٍ فى أوضاعها وستظل البشرية تواجه حالة من التصادم تعكّر صفو العيش المشترك فى ظل السلام والوئام[٣].

وقد سيطرت على مُخيلة العامة – بشكل كبير – فكرة تسبب الإرهابيين فى خسائر كبيرة فى حياة المواطنين، وقدرتهم على إحداث فوضى اقتصادية عالمية، واختراق البنية الإلكترونية التحتية للعديد من المؤسسات المهمة فى الدول، الأمر

---

(1) Thomas m. Shin, Lee Jarvis, and Stewart McDonagh, op.cit.

future for adnanced research and studies **استراتيجيات الدول لمواجهة الإرهاب الإلكترونى،**

متاح علي :https://futureuae.com/m/Mainpage/Item/617/cyberterrorism

(2) Thomas m. Shin, Lee Jarvis, and Stewart McDonagh, op.cit.

(٣) الإعلام الجديد فى مواجهة تحديات الإرهاب الإلكترونى

Author: Lalu Supriadi Bin Mujib Author's Affiliation: Universitas Islam Negeri Mataram Email : nasabila46@gmail.com

الذي استدعى من الحكومات ضرورة سن قوانين تُمكنها من حماية نفسها فى مواجهة تلك الهجمات الإرهابية، وبما لا يقلل – فى الوقت نفسه- من استخدامات الكمبيوتر والتكنولوجيا لمواطنيها، وفى هذا الصدد، يشار إلى نماذج القوانين الموجودة فى أربعة من دول الكومنولث، وهى "بريطانيا واستراليا وكندا ونيوزيلاندا"، وذلك من خلال الإجابة على تساؤلين: ما استخدامات الكمبيوتر والإنترنت التى تعتبرها القوانين المحلية أفعالاً إرهابية Acts of Terrorism؟وهل تكفى تلك القوانين لمواجهة هجمة إلكترونية إرهابية جادة محتملة[1]؟

فى عصر تزايد النشاط الإرهابى عبر الإنترنت، أصبح الخوف من الإرهاب الإلكترونى قائماً، كونه جريمة حديثة ترتكب بواسطة تكنولوجيا الحاسوب، وذات طبيعة عابرة للحدود الوطنية، ونظراً لغياب إطار قانونى دولى شامل يتناول –على وجه التحديد- مكافحة هذا التهديد العالمى، تواجه السلطات و الحكومات فى جميع أنحاء العالم تحديات بالغة فى العثور على المجرمين ومحاكمتهم؛ لذلك كان لا بد للدول والمنظمات الدولية والإقليمية أن تتخذ خطوات قانونية وتكنولوجية لمكافحة هذا التهديد العالمى، مما يتطلب التعاون الدولى الفعال، ومن هنا يحاول هذا البحث أن يوضح أحد أوجه تأثير الإرهاب الإلكتروني و خاصة أثره فى العلاقات الدولية ..

ويعد الإرهاب الإلكترونى مفهوماً هجيناً، بما يُصّعِب من إمكانية وجود حد أدنى من الاتفاق على تعريفه، ومن ثمَّ يفترض وجود ثلاثة طرق، تتنافس فيما بينها، للتعامل مع هذا الأمر، أولاها ببساطة، إما التخلى عن التسمية الخاطئة للأنشطة الإلكترونية بوصفها إرهاباً إلكترونياً، أو ثانياً الدخول فى مزيد من العمل التعريفى

(1) Thomas m. Shin, Lee Jarvis, and Stewart McDonagh, op.cit.

لتوضيح ما قد يشير إليه الإرهاب الإلكترونى تحديداً، أو ثالثاً، وهو الأكثر تفضيلاً، أن يتم تجنب مسألة التعريف تماماً، وأن يتم التعامل مع الإرهاب الإلكترونى كبناء اجتماعى بدلاً من التعامل معه ككيان مستقر ومتماسك(١).

وقد تعددت تعاريف الإرهاب واختلفت وتباينت فى شأنه الاجتهادات، ولم يصل المجتمع الدولى – حتى الآن– إلى تعريف جامع مانع متفق عليه للإرهاب، ويرجع ذلك إلى تنوع أشكاله ومظاهره وتعدد أساليبه وأنماطه، واختلاف وجهات النظر الدولية والاتجاهات السياسية حوله، وتباين العقائد والأيديولوجيات التى تعتنقها الدول تجاهه، فما يراه البعض إرهاباً يراه الآخر عملاً مشروعا(٢).

وكان القانون يسرى تقليديا فى المجال الوطنى أو الإقليمى الخاضع للسيادة الوطنية، رغم تواجده بجانب القانون الدولى، الذى كان يغير الوضع بقوة فى بعض الحالات، و لقد ساهمت التكنولوجيا فى قلب ترتيب المجالات؛ لأنها لا تخضع للحدود السياسية بين الدول(٣)، و خير مثال على ذلك هو الشبكة العنكبوتية و الإعلام السمعى البصرى و الاتصالات بكل حواملها.

وتفرض الدراسة في هذا المحور تناول نقطتين بحثيتين هما :

-مفهوم الإرهاب الإلكترونى

-أسباب الإرهاب الإلكترونى وخصائصه وأهدافه

---

(1) Thomas m. Shin, Lee Jarvis, and Stewart McDonagh,op.cit.

(2) Author: Lalu Supriadi Bin Mujib Author's Affiliation,op.cit.

(٣) **عبد الرحيم رجوانى**، عصر المعلومات، جموح تكنولوجيا المعلومات فى ظل العولمة، سلسلة المعرفة للجميع، رقم ٩، سبتمبر ١٩٩٩، مطبعة النجاح، الدار لبيضاء.

أ- مفهوم الإرهاب الإلكترونى

يواجه الإرهاب الإلكترونى- حتى الآن- مشكلة أساسية تكمن فى عدم وجود اتفاق حول ماهيته، خصوصاً أن مفهوم الإرهاب تطور على مدار السنوات الأخيرة، وتداخلت معه العديد من العوامل، بما صعَّب من إمكانية تعريف أحد تجلياته المتمثلة فى "الإرهاب الإلكترونى"، الأمر الذى يتطلب إعادة قراءته من جديد لمحاولة فهمه وتحديد أبعاده وطبيعة تهديداته، والاستراتيجيات التى يجب أن تُتبع للتعامل مع تلك التهديدات، سواء من جانب الدول أو الشركات أو الأفراد [١].

وعلى الرغم من ظهور المفهوم بشكل متزايد فى السنوات اللاحقة، فقد أضحى معناه مُتنازَعاً عليه، خصوصاً أن التعامل مع الأنشطة الإلكترونية- أياً كان نوعها- تم إدراجها في إطار المعنى الواسع للإرهاب، وهو ما يعتبر أمراً غير مفيد، وغير مرغوب فيه، فيما يتعلق بهذا المفهوم [٢].

وتعد كلمتا "الإرهاب" و "مكافحة الإرهاب" من المصطلحات الشائعة دورانها فى هذه الآونة، وقد أقيمت عدة من المؤتمرات والندوات وطنيا ودوليا للبحث حول هذا الموضوع، عرف " الإرهابى" بأنه فاعل للعملية الإرهابية وأطلقت الكلمة مفردة، أما الجمع فقد وردت فيه كلمة "الإرهابيون" بينما الإرهابية هى الفكرة التى تنتمى إلى إيدولوجيات تبيح العملية الإرهابية بجميع أنواعها وأشكالها من التهديد و التخويف والإفزاع والعنف وشتى الصور الفظيعة المستهدفة للمجتمع لأسباب ودوافع معينة[٣].

---

(1) Thomas m. Shin, Lee Jarvis, and Stewart McDonagh, op.cit.

(2) Thomas m. Shin, Lee Jarvis, and Stewart McDonagh, op.cit.

(3) Author: Lalu Supriadi Bin Mujib Author's Affiliation: Universitas Islam Negeri Mataram Email : nasabila46@gmail.com

وينطلق الإرهاب – بجميع أشكاله وشتى صنوفه– من دوافع متعددة، ويستهدف غايات معينة، ويتميز الإرهاب الإلكترونى –عن غيره من أنواع الإرهاب– بالطريقة العصرية المتمثلة فى إستخدام الموارد المعلوماتية والوسائل الإلكترونية التى جلبتها حضارة التقنية فى عصر المعلومات؛ لذا فإن الأنظمة الإلكترونية والبنية التحتية المعلوماتية هى هدف الإرهابيين .

ويعتبر الإرهاب الإلكترونى من أخطر الهجمات السيبرانية الخارجية التى قد تتعرض لها المواقع الإلكترونية الحكومية، وقد أضحي الإرهاب الإلكترونى هاجسا يخيف العالم بأسره؛ نظرا لاستخدام التكنولوجيا الحديثة فى بث الافكار المسمومة، وما يزيد الأمر تعقيدا هو أن التقدم التكنولوجي لا يتوقف، مما يصعب معه على المؤسسات والأفراد أن تواجه خطر تلك الهجمات.

ب- أسباب الإرهاب الإلكترونى وخصائصه وأهدافه

تزداد خطورة الإرهاب الإلكترونى فى الدول المتقدمة والتى تدار بنيتها التحتية بالحواسيب الآلية والشبكات المعلوماتية، مما يجعلها هدفا سهل المنال، فبدلاً من إستخدام المتفجرات تستطيع الجماعات الإرهابية – من خلال الضغط على لوحة المفاتيح– تدمير البنية المعلوماتية، وتحقيق آثار تدميرية تفوق مثيلتها المستخدم فيها المتفجرات، حيث يمكن شن هجوم إرهابى لإغلاق المواقع الحيوية وإلحاق الشلل بأنظمة القيادة والسيطرة والإتصالات، أو قطع شبكات الإتصال بين الوحدات والقيادات المركزية، أو تعطيل أنظمة الدفاع الجوي، أو إخراج الصواريخ عن مسارها، أو التحكم فى خطوط الملاحة الجوية والبحرية، أو إختراق النظام المصرفى وإلحاق

أحمد فنانى، المعجم الإندونيسي المعاصر (يوغياكرتا: مترا فلاجر، عام ٢٠٠٩م)، ص ٣٦٦.

الضرر بأعمال البنوك وأسواق المال .

ولقد زادت الخطورة الإجرامية للجماعات والمنظمات الإرهابية، فقامت بتوظيف طاقتها للإستفادة من تلك التقنية واستغلالها فى إتمام عملياتها الإجرامية وأغراضها غير المشروعة .

وتأسيساً على ما سبق، يمكننا القول بأن الإرهاب الحالى الإلكترونى هو إرهاب المستقبل، وهو الخطر القادم؛ نظراً لتعدد أشكاله وتنوع أساليبه، واتساع مجال الأهداف التى يمكن – من خلال وسائل الإتصالات وتقنية المعلومات- مهاجمتها فى جو مريح وهادئ، وبعيد عن الإزعاج والفوضى، مع توفير قدر كبير من السلامة و الأمان للإرهابين .

و لمزيد من التفاصيل، سوف نتناول :

- أسباب الإرهاب الإلكترونى ودوافعه .

- أهداف الإرهاب الإلكترونى و خصائصه.

١-أسباب الإرهاب الإلكترونى و دوافعه

تختلف أسباب الإرهاب ودوافعه فى درجة أهميتها حسب الاتجاهات السياسية والظروف الاقتصادية والأحوال الاجتماعية وكذلك الاختلاف الدينى والعقائدى .

ويمكننا إيجاز أسباب ظاهرة الإرهاب فى : الدوافع الشخصية، التى تتعدد، ويمكن بيان أبرزها فى: افتقاد الشخص لأهمية دوره فى الأسرة والمجتمع وفشله فى الحياة الأسرية، مما يؤدى إلى اكتساب بعض الصفات السيئة ومن ضمنها عدم الشعور بالانتماء و الولاء للوطن،-الرغبة فى الظهور وحب الشهرة بحيث لا يكون

الشخص مؤهلا فيبحث عما يؤهله باطلا فيشعر ولو بالعدوان والتخريب والتدمير، – نقمة الشخص على المجتمع الذى يعيش فيه نتيجة للظلم وإهدار الحقوق .

فضلا عن الدوافع الفكرية، التى يمكن بيان أهمها فى : الفهم الخاطئ للدين، وتفسيره تفسيرا خاطئا، الانقسامات الفكرية المختلفة بين التيارات المتنوعة والمختلفة، التطرف وهو أمر بالغ الخطورة فى أى مجال من المجالات وخاصة المجالات الفكرية .

بالإضافة إلى الدوافع السياسية، التى تكمن فى غياب العدالة الاجتماعية، وعدم المساواة فى توزيع الثروة الوطنية، والتفاوت فى توزيع الخدمات والمرافق العامة، والتقصير فى أمور الرعية، معاناة بعض المجتمعات والشعوب الدولية من الظلم والاضطهاد والسيطرة الاستعمارية وسلب الأموال وخرق القوانين والمواثيق الدولية مما يدفع الشعوب إلى التشدد والتطرف .

و هكذا، ينفرد الإرهاب الإلكترونى بعدد من الخصائص التى يختص بها دون سواه، ويتميز بها عن غيره من الظواهر الإجرامية الأخرى، كما يسعى إلى تحقيق جملة من الأهداف والأغراض غير المشروعة .

وترجع أسباب انتشار الإرهاب الإلكترونى إلى الأتى[١]:

–ضعف بنية الشبكات المعلوماتية وعدم تمتعها بالخصوصية وسهولة اختراقها، حيث أن شبكات المعلومات تم تصميمها بشكل مفتوح دون وضع قيود أو حواجز

(١) **عمار ياسر محمد زهير البابلى**، آليات التأمين والوقاية من الهجمات السيبرانية بالتطبيق على معايير الجودة الخاصة بالمواصفات القياسية لنظام إدارة أمن المعلومات ISO 27001 للحماية من مخاطر الإرهاب الإلكتروني، ص٢٦٣.

أمنية عليها؛ وذلك من أجل التوسع وجعل دخول المستخدمين إليها يتم بسهولة، وتتضمن الأنظمة الإلكترونية بعض الثغرات التى تمكن المنظمات الإرهابية من التسلل إلى البنية المعلوماتية التحتية إليها وممارسة أنشطتها الإجرامية.

-سهولة الاستخدام التقنى وقلة التكلفة المادية، حيث أضحت كافة وسائل التواصل الإلكترونى قليلة التكلفة ومتوفرة فى كافة بلدان العالم، كما أن سمة العولمة التى تمتاز بها شبكة المعلومات فى كونها وسيلة سهلة الاستخدام وقليلة التكلفة [١] هيئت للمنظمات الإرهابية الفرصة للوصول إلى الأهداف غير المشروعة دون أن تحتاج إلى مصادر تمويل؛ من أجل القيام بشن هجمات إرهابية إلكترونية، فأصبح الأمر لا يتطلب أكثر من وجود جهاز حاسب ألى متصل بالشبكة المعلوماتية.

-صعوبة اكتشاف و إثبات الجريمة الإرهابية الإلكترونية، ففي الشبكة المعلوماتية يكون من الصعب تحديد هوية مرتكب الجريمة إلا من خلال الاعتماد على أجهزة معينة تمتلكها بعض المؤسسات الأمنية، أما بالنسبة للأفراد فإنهم لا يستطيعون تحديد ذلك[٢].

٢-أهداف الإرهاب الإلكترونى و خصائصه

أهداف الإرهاب الإلكتروني :

يهدف الإرهاب الإلكترونى إلى تحقيق جملة من الأهداف غير المشروعة، ويمكننا بيان أبرز تلك الأهداف:

(١) **ممدوح عبد الحميد**، البحث والتحقيق الجنائى الرقمى فى جرائم الحاسب الألى والإنترنت، دار الكتب القانونية، ٢٠١٠، ص٩٠.

(٢) **عمار ياسر محمد زهير البابلي**، المرجع السابق، ص٢٦٥.

١. نشر الرعب والخوف بين الأشخاص والدول والشعوب المختلفة والإخلال بالأمن العام و زعزعة الطمأنينة

٢ ـ إلحاق الضرر بالبنية التحتية المعلوماتية وتدميرها، والإضرار بوسائل الإتصالات وتقنية المعلومات، أو بالأموال والمنشآت العامة والخاصة .

٣ـ جمع الأموال اللازمة لتمويل العمليات الإرهابية .

و قد ارتكزت معظم محاولات التفكير فى التهديدات التى يفرضها الإرهاب الإلكترونى حتى الآن على أمرين، يتمثل أولهما فى مدى وجود هذا الإرهاب فعلياً، أو على الأقل وجوده بشكل يختلف جوهرياً عن أشكال الإرهاب الأخرى، أما الأمر الثانى فينصرف إلى القدرة التدميرية لهذا الإرهاب ونوعية الأهداف التى يسعى لتدميرها؛ لذا يشار إلى أنه لفهم التهديدات الإلكترونية بشكل جيد، لابد من الربط بين تكنولوجيا المعلومات من ناحية، وبين نوايا الإرهابيين المحتملين من ناحية أخرى، ويرتكز فى تحليل هذا الأمر على توضيح بعض الالتباسات المتكررة حول القدرات الإجرامية للتكنولوجيا عموماً، وإمكانية توظيفها بشكل سيئ يضر بالآخرين على وجه الخصوص(١) .

خصائص الإرهاب الإلكترونى :

يتميز الارهاب الإلكترونى بعدة خصائص وسمات :

١ – الإرهاب الإلكترونى لا يحتاج عند ارتكابه إلى العنف والقوة بل يتطلب حاسبا أليا متصلا بالشبكة المعلوماتية ومزودا ببعض البرامج اللازمة.

(١) op.cit.Thomas m. Shin, Lee Jarvis, and Stewart McDonagh,

٢- يتميز الارهاب الإلكترونى بأنه جريمة إرهابية متعدية الحدود وعابرة للدول والقارات وغير خاضعة لنطاق إقليمي محدود .

٣- صعوبة اكتشاف جرائم الإرهاب الإلكترونى ونقص الخبرة لدى بعض الأجهزة الأمنية والقضائية فى التعامل مع مثل هذه الجرائم.

٤- صعوبة الإثبات فى الإرهاب الإلكترونى؛ نظرا لسرعة غياب الدليل الرقمى وسهولة إتلافه وتدميره.

٥- يتميز الإرهاب الإلكترونى بأنه يتم بتعاون أكثر من شخص على ارتكابه.

٦- يكون مرتكب جريمة الإرهاب الإلكترونى من ذوى الاختصاص فى مجال تقنية المعلومات أو من شخص لديه -على الأقل- قدر من المعرفة والخبرة فى التعامل مع الحاسب الألى والشبكة المعلوماتية .

ويتخذ الإرهاب الإلكتروني عدة أشكال تختلف على حسب الجناة وأهدافهم، وهى على النحو الأتى:

-التهديد الالكترونى، وتختلف أساليب التهديد الإلكترونى على الشبكة المعلوماتية من القيام بتهديد بعض الشخصيات بالقتل إلى التهديد بتفجير بعض المراكز السياسية أو التجمعات أو التهديد بإطلاق فيروسات تهدف إلى تخريب الأنظمة المعلوماتية.

-القصف الإلكترونى، ويعد من أساليب الهجوم على شبكة المعلومات، ويتم ذلك من خلال القيام بتوجيه العديد من الرسائل الإلكترونية إلي الموقع، الأمر الذى يشكل ضغطا كبيرا على الموقع؛ نتيجة لاستقباله تلك الرسائل، مما يؤدى إلى توقف العمل.

-تدمير أنظمة المعلومات، ويتم ذلك من خلال اختراق شبكة المعلومات الخاصة بالمؤسسات أو الأفراد؛ من أجل تدمير النظام، ويتم من خلال إعداد أنواع جديدة من الفيروسات التى يعجز النظام فى التصدى لها، مما ينتج عنه ضرر لأجهزة الحاسب وفقدان البيانات والمعلومات المخزنة.

-التجسس الإلكترونى، وهو يعنى التلصص على المعلومات الخاصة بالأفراد أو المؤسسات، وتتعدد أهداف التجسس الإلكترونى، حيث أنها قد تكون من أجل الحصول على معلومات اقتصادية أو معلومات سياسية أو عسكرية يؤدى افشائها أو معرفتها إلى حدوث خسائر ضخمة للمؤسسة أو الأفراد[١].

وهنا تبرز ظاهرة عسكرة الفضاء الالكترونى والحروب الالكترونية، فقد سعت العديد من القوى المؤثرة فى السياسة الدولية إلى استخدام الفضاء الالكترونى فى شن العديد من الهجمات الإلكترونية، والتى من شأنها أن تدمر البنى التحتية للدول، فما فعلته الولايات المتحدة من إطلاق المركبة التى تحمل اسم"x-37 BO TV فى عام ٢٠١٠ يُعد جزءا من عسكرة الفضاء، إذ بإمكان هذه المركبة إسقاط الأقمار الصناعية المعادية، كما أنها تُعد أداة قادرة للرد السريع ضد الخصوم[٢] .

لقد ساهمت هذه الظاهرة – بلا شك– فى إحداث تغيير فى موازين القوى، فإلى جانب عناصر القوة التقليدية كالقدرات السياسية والاقتصادية والعسكرية، باتت القوة التكنولوجية من أهم عناصر القوة التى تسعى الكثير من الدول لامتلاكها لتحقيق أهدافها ومصالحها القومية، وكذا أيضا الأفراد، إذ لم يعد اقتصار استخدام هذا النوع

---

(١) **عمار ياسر محمد**، المرجع السابق، ص٢٦٦.

(٢) **أيمن حسين**،"هل بدأت أمريكا عسكرة الفضاء"، مجلة العربى – الكويت، العدد(٦٢) يوليو٢٠١٠، ص٥، متاح على الرابط :https://www.alarabimag.com/books/17813-

من القوة على الدول، بل شاهدنا فاعلين من غير الدول كالتنظيمات الإرهابية تسعى لاستخدام القوة التكنولوجية فى تحقيق أهدافها من خلال الوصول لأكبر عدد من المستهدفين وخاصةً من الشباب للترويج لأفكارهم وبث الكراهية وعدم الثقة فى قدرات حكومات الدول على مواجهة الأزمات، ومن ثم قد تؤدى هذه الأفعال غير المشروعة من الفاعلين من غير الدول الى تدمير البنى التحتية للدول، وانتهاك سيادة الدول، وزعزعة أمن واستقرار الدول، الأمر الذى يُنذر بوجود نزاعات دولية؛ وذلك بسبب غياب التفاهم المشترك والقواعد الضرورية لتنظيم استخدام الفضاء الإلكترونى فى خدمة البشرية.

لذا أصبح استقرار النظام الدولى يعتمد على ممارسات الفاعلين حتى لو كانوا من غير الدول، فقد شهد النظام الدولى العديد من التغيرات فى إطار بزوغ القوة التكنولوجية وتسارع وتيرتها بشكل ساهم فى التأثير على مستقبل العلاقات الدولية، وهو ماسنقوم بتوضيحه فى المحور الثالث.

المحور الثالث

التأثيرات والانعكاسات المتحصلة من استخدام الفضاء الالكترونى

" دول الشرق الأوسط نموذجًا "

تتمتع منطقة الشرق الأوسط بأهمية جيو استراتيجية جعلت منها موضعا لتنافس العديد من القوى الكبرى، والتى تسعى لبسط هيمنتها وسيطرتها على المنطقة لتحقيق أهدافها ومصالحها القومية، حيث عملت هذه القوى على توظيف الكثير من الأدوات – سواء السياسية أو الاقتصادية أو العسكرية أو التكنولوجية– لإحكام سيطرتها على المنطقة بالشكل الذى يمكنها من تحقيق أهدافها ومصالحها، فقد نجحت هذه القوى فى مواكبة التقدم التكنولوجى والعلمى، حيث تمكنت من استخدام الفضاء الالكترونى فى شن العديد من الهجمات الالكترونية، والتى من شأنها أن تساهم فى تدمير البنى المعلوماتية للعديد من دول العالم عامةً و دول الشرق الأوسط خاصةً، الأمر الذى من شأنه أن يؤدى إلى المساس بأمن واستقرار الدول وينتهك سيادتها؛ لذا جاءت هذه الدراسة لتلقى الضوء على طبيعة التأثيرات والانعكاسات المتحصلة من استخدام الفضاء الإلكترونى، وذلك بالتطبيق على دول الشرق الأوسط نموذجاً للدراسة.

الشرق الأوسط والفضاء الالكترونى :

شهدت العصور الحديثة تقدما فى المجال التكنولوجى والعلمى، إذ سعت العديد من الدول إلى مواكبة هذه التقنيات الحديثة و العمل على توظيفها فى شتى المجالات، فظهر مايسمى بالفضاء الإلكترونى، والذى سعت العديد من الدول – التى تمتلك مثل هذه التقنيات التكنولوجية الحديثة– إلى توظيف الفضاء الالكترونى فى

تحقيق أهدافها ومصالحها القومية؛ لذا تحول الفضاء الالكترونى لساحة تنافس للعديد من الدول التى تمتلك القدرة على استخدام الفضاء الالكترونى، الأمر الذى من شأنه أن ساهم فى إعادة توازن القوى .

وهنا تجدر الاشارة الى أن دول الشرق الأوسط، وهي المنطقة الجغرافية الواقعة ما حول وشرق وجنوب البحر الأبيض المتوسط، وتمتد إلى الخليج العربي من الدول التى سعت الى استخدام الفضاء الالكترونى، اذ أخذ شكل التعامل مع الفضاء الإلكترونى مهمتين متعارضتين مع بعضهما البعض:

المهمة الأولى: العمل على مواكبة التكنولوجيا والتقدم العلمى، وتوظيفها فى كافة مناحى الحياة .

المهمة الثانية: العمل على دعم البنى المعلوماتية وتحصينها من أية اختراقات قد تتعرض لها بشكل يهدد أمن واستقرار هذه الدول(١).

فقد شهدت دول المنطقة -منذ انتهاء الحرب الباردة- العديد من الحروب شنتها القوى الكبرى، والتى عملت على استخدام أسلحة الفضاء الالكترونى فى تحقيق أهدافها ومصالحها القومية المتمثلة فى الاستفادة من ثروات المنطقة وموقعها الجغرافى المتميز، والذى يمكنها من فرض هيمنتها ونفوذها على الكثير من دول العالم، كما حرصت على متابعة التقدم والتطور التكنولوجى الذى وصلت إليه دول الشرق الأوسط، ونظرا لأن الولايات المتحدة من أكثر الدول المعنية بثروات المنطقة وأهميتها الاستراتيجية، فضلاً عن حماية و أمن اسرائيل، فقد أوكلت الإدارة

(١) د. **حميد حمد السعدون**، "التنمية السياسية و التحديث" العالم الثالث، الذاكرة للنشر والتوزيع، عمان ٢٠١١، ص١٣٦.

السياسية العليا الأمريكية "NSA" مهمة متابعة التطور والتقدم التكنولوجى الذى وصلت إليه دول المنطقة، حيث تزايد اهتمامها بهذا النشاط فى المجمع الاستخبارى الأمريكى بعد الحرب الباردة؛ بسبب طبيعة التطورات الالكترونية والتقنية والتى باتت جزءا أساسيا من مهام الوكالة، والتى تؤدى دورا استراتيجيا فى مجال الأمن القومى الأمريكى من خلال التصدى لما يسمى بالإرهاب الالكترونى، والذى يعتمد على اختراق أنظمة المعلومات، الأمر الذى من شأنه أن يؤدى إلى التأثير على الهيكل التنظيمى الذى تقوم عليه المؤسسات الأمريكية فى هذا الشأن(١).

هذا وتعد الحرب التى شنتها الولايات المتحدة الأمريكية ضد العراق فى عام ١٩٩١ نموذجاً للحروب الالكترونية التى شهدتها المنطقة فى هذه الفترة، وكذا أيضاً خلال فترة الحصار، والتى امتدت لأكثر من ١٢عاماً، حيث أدت فرق التفتيش الدولية دوراً فاعلاً فى اختراق المنظومة السيادية العراقية بتقنياتها المتطورة(٢).

كما تعرضت شركات إيرانية وشركات نفط سعودية وقطرية لاختراق لأنظمة المعلومات الخاصة بهم من خلال إطلاق فيروس"stuxnet" و"flem"، الأمر الذى تسبب فى إتلاف كل أنظمة المعلومات لهذه الشركات، ففيروس "stuxnet" من الفيروسات الخبيثة التى يمكن من خلالها شن هجمات على ثلاث مراحل : الأولى تستهدف الألات العاملة على نظام "Micro soft windows" بحيث يدفعها الى أن تقوم بالتكرار لاعادة نسخ ذاتها ثم تتوجه إلى برنامج"semens step 7" ، والذى

(١) Colin S. Gary, Strategy for chaos :Revolutions in Military Affairs and the evidence of history, with a foreword by Williamson Murray ,London, Portland OR frank cass 2003, p192.

٣- **توماس كوبلاند"**محرر"، ثورة المعلومات والأمن القومى"، سلسلة دراسات عالمية، مركز الإمارات للدراسات والبحوث الاستراتيجية، العدد(٤٦)، أبوظبى ٢٠٠٣، ص٩٤.

يستخدم نظم التحكم الصناعية البرمجية التى تشغل معدات كأجهزة الطرد المركزى ثم يقوم فى المرحلة الثالثة بالمساس بالمتحكمات المنطقية المبرمجة(١).

و قد استطاع مخترعو هذا الفيروس اختراق أجهزة الكمبيوتر المحلية دون الحاجة إلى توصيلها بالإنترنت، ومن ثم إمكانية انتشارها داخل الشبكات المحلية سريعة التحقيق، كما يتم دون إثارة أى شكوك أو شبهات، وهنا أدركت إيران مخاطر استخدام الفضاء الإلكترونى عام ٢٠٠٩، إذ استخدم محتجون مناهضون للحكومة خدمة الإنترنت لتنظيم احتجاجات ضد نتائج الانتخابات الرئاسية التى نتج عنها وصول "محمود أحمدى نجاد" لسدة الحكم؛ لذا أوكل للحرس الثورى الإيرانى مهمة مراقبة الإنترنت وحجب بعض المواقع وتعطيل أخريات(٢).

أما إسرائيل، فقد سعت بالتعاون مع الولايات المتحدة الأمريكية إلى استخدام هذه الفيروسات فى اختراق أنظمة المعلومات لكثير من الدول، حيث أكد مجموعة من الخبراء المتخصصين فى مجال المعلوماتية أن الاستخبارات الأمريكية – بالتعاون مع الاستخبارات الاسرائيلية– هى التى طورت فيروسى"stuxnet و"flem" واللذين تم استخدامهما فى استهداف العديد من الشركات النفطية والعسكرية والنووية الإيرانية؛ الأمر الذى ترتب عليه قيام إيران بشن العديد من الهجمات الإلكترونية التى استهدفت العديد من المؤسسات الاسرائيلية (٣).

---

(١) **ستكسنيت**...قصة الدودة الالكترونية المخربة للمشروع النووى الايرانى، صحيفة الشرق الأوسط، لندن، العدد(١٢٥٤١) فى ٢٠١٣/٣/٣٠.

(٢) المرجع السابق.

(٣) **محمد على صالح**، التحقيق مع جنرال أمريكى متقاعد فى قضية الحروب الالكترونية ضد ايران، صحيفة الشرق الأوسط، لندن، العدد(١٢٦٣٢) فى ٢٩-٦-٢٠١٣.

وهنا يتضح لنا مماسبق عرضه من معلومات أن الحروب الالكترونية هى حروب تعتمد على توظيف التكنولوجيا فى شن هجمات على الدول تستهدف البنى المعلوماتية بشكل أساسى، الأمر الذى من شأنه أن يهدد أمن واستقرار الدول، وينتهك سيادتها، فضلاً عن كونها سهلة التنفيذ وتمتد آثارها إلى دول أخرى، كما أنه من الصعب اثبات مرتكب هذه الجرائم الإلكترونية، هذا بالإضافة الى أن القواعد الحاكمة فى الفضاء الإلكترونى هى أبعد ما تكون عن الوضوح، فالحروب الالكترونية حروب صامتة غير مرئية، لكنها مستمرة بشكل فعال، وهنا تستشعر الدول عدم وجود قيود على استخدام أسلحة الفضاء الالكترونى، وفى ذلك مخاطر كثيرة على مستوى العلاقات الدولية والمجتمع الدولى.

خاتمة الدراسة:

ما لم ينهض العالم بدوره فى التصدى لمشكلاته بنفسه، وإعطاء الشعوب حقها فى الكرامة والعدالة والحرية، والدفاع عن المقدسات والمصالح المشروعة فى إطارٍ من التوازن والعدل، فسنظل نعانى من اختلالٍ فى أوضاعها وستظل البشرية تواجه حالة من التصادم تعكّر صفو العيش المشترك فى ظل السلام والوئام.

وقد تبين لنا أن الفضاء الالكترونى هو المجال الذى تعمل فيه شبكات الحواسيب الإلكترونية فى العالم كله والذى يشتمل على (أجهزة الكمبيوتر، وأنظمة الشبكات والبرمجيات والتقنية المعلوماتية والتى تشمل نقل المعلومات وتخزينها، وكذلك مستخدمى هذه الشبكات حول العالم كله، سواء كان المستخدمون من البشر أو الهيئات أو المؤسسات الحكومية وغير الحكومية والرسمية وغير الرسمية، فهو تعريف جامع شامل للأنظمة والشبكات ومستخدميها .

لـذا سـعت دول العـالم إلـى الاسـتفادة مـن هـذه التقنيـات الحديثـة ومواكبـة التكنولوجيا وتوظيفها فى كافة مناحى الحياة، فالولوج المتزايد للفضاء الالكترونى، مكن الجميع من التواصل، كما ساهم فى خلق ساحات جديدة لمطالب جماعية بحل أزمات ومشكلات إنسانية مشتركة خاصةً فى ظل جائحة كورونا، والتى فرضت العديد من التحديات على الدول تعين مواجهتها، ومن ثم بات التحول الرقمى أمراً ملحاً للتعايش مع هذه الأزمة، الا أن بعض القوى المؤثرة فى السياسة الدولية - والتى تمتلك المزيد من العلم والتكنولوجيا- سعت إلى استخدام الفضاء الإلكترونى فى شن العديد من الهجمات الإلكترونية والتى قد تتصاعد لتنذر بقيام العديد من النزاعات الدولية، الأمر الذى من شأنه أن يؤثر على مستقبل العلاقات الدولية، وذلك بسبب غياب القواعد الضرورية لتنظيم استخدام الفضاء الإلكترونى بما يخدم البشرية.

وهنا تجدر الإشارة إلى ما أسفرت عنه الدراسة من نتائج، وما أتت به من توصيات .

نتائج الدراسة :

أبانت لنا الدراسة عن بعض النتائج نوجزها فى :

-اتجاه الاتفاقيات الدولية إلى إلزام أطرافها بنشر نصوصها على أوسع نطاق ممكن فى بلدانها، فى وقت السلم و زمن الحرب، و بأن تدرج دراستها ضمن برنامج التعليم العسكرى و المدنى، حتى تكون معروفة لجميع السكان، و خصوصا القوات المسلحة، و أفراد الخدمات الطبية و الدينية.

- تُعد منطقة الشرق الأوسط من المناطق المعنية باهتمام العديد من القوى المؤثرة فى السياسة الدولية لاسيما الولايات المتحدة واسرائيل، لما تمتلكه هذه المنطقة من ثروات، وما تتمتع به من أهمية جيواستراتيجية .

- شهدت منطقة الشرق الأوسط ارتفاع وتيرة الهجمات الالكترونية والتى شنتها العديد من القوى المؤثرة فى السياسة الدولية، وذلك بهدف تدمير البنى المعلوماتية لدول المنطقة، وانتهاك سيادتها، و زعزعة أمنها واستقرارها.

- شهدت ساحة الفضاء الالكترونى تنافس العديد من القوى المؤثرة فى السياسة الدولية، إذ أصبحنا نتحدث عما يسمى ب"عسكرة الفضاء الالكترونى" الأمر الذى ينذر بوجود العديد من النزاعات الدولية، ويؤثر على مستقبل العلاقات الدولية.

التوصيات: توصى الدراسة بـ :

-التعريف بالإرهاب الإلكترونى و نشر خصائصه و أهدافه، مواكبة للتطورات الحادثة على الصعيد الدولى ينبغى أيضاً أن تعمّم الجهات المختلفة و تدعم الجهود الرامية إلى تحسين الثقافة الرقمية و الوعى بالأمن الرقمى لدى المجموعات الأشد حاجة إلى ذلك.

-شرح الجوانب القانونية والأمنية والتشريعية المتعلِّقة بمواجهة جرائم الإرهاب، والاهتمام بالإرشادات الخاصَّة بمسؤولية المواطنين في مواجهة الإرهاب، والاهتمام بالجانب الوقائي في مواجهة الإرهاب؛ لتقديم متابعة متكاملة، و رُؤًى تساعد الجمهورَ على تكوين رأي عامٍّ وطني يتحوَّل إلى موقف، ومن ثَم إلى سلوك إيجابي لمواجهة الإرهاب، واستخدام المصطلحات المحدِّدة والموضِّحة لمفهوم الإرهاب، وتوحيدُها؛ لتجنُّب استخدام مصطلحات تخدم عقيدةَ الجماعات والتنظيمات الإرهابية وأهدافها، والتقليل من إبراز التأثير النفسي للعمليَّات الإرهابية للحفاظ على معنويَّات الشعب، والاهتمام بالبيانات الرسمية؛ لأنها مصدرٌ موثوق لنشر المعلومات الصحيحة الخاصَّة بالعمليَّات الإرهابية.

-إعادة التفكير في تهديدات الإرهاب الإلكترونى، إذ أن محاولات التفكير فى التهديدات التى يفرضها الإرهاب الإلكترونى ارتكزت فى معظمها حتى الآن على

أمرين؛ يتمثل أولهما فى مدى وجود هذا الإرهاب فعلياً، أو على الأقل وجوده بشكل يختلف جوهرياً عن أشكال الإرهاب الأخرى، أما الأمر الثاني فينصرف إلى القدرة التدميرية لهذا الإرهاب ونوعية الأهداف التى يسعى لتدميرها؛ لذا فإنه لفهم التهديدات الإلكترونية بشكل جيد، لابد من الربط بين تكنولوجيا المعلومات من ناحية، وبين نوايا الإرهابيين المحتملين من ناحية أخرى.

- تضافر الجهود الدولية لسن مجموعة من التشريعات و وضع مجموعة من القواعد الضرورية لتنظيم استخدام الفضاء الإلكترونى بما يخدم البشرية، الأمر الذى من شأنه أن يساهم فى تدعيم العلاقات بين الدول، وصون السلم والأمن الدوليين.

بدلا من استخدام التكنولوجيا في الترهيب و الحروب، بات من الواجب أن تضطلع المعدات والبرمجيات التى تيسر إعداد المعلومات و إرسالها وتلقيها وحفظها و تخزينها- بدور متزايد فى حماية جميع حقوق الإنسان، بما فيها الحق فى الحياة، و يمكن استخدام المعلومات المسخَّرة على هذا النحو لضمان المساءلة.

قائمة المراجع:

أ.ب. روجرز، خوض الحرب بلا خسائر في الأرواح، المجلة الدولية للصليب الأحمر، مختارات من أعداد عام ٢٠٠٠.

إبراهيم محمد بن حمود الزنداني، الجرائم الإلكترونية من منظور الشريعة الإسلامية وأحكامها في القانون القطري والقانون اليمني: دراسة مقارنة، جامعة فطاني، ٢٠١٨.

أحمد الشربيني و د. وفائي بغدادي، حماية وتأمين الإنترنت، التحدي القادم وأساليب المواجهة، الهيئة المصرية العامة للكتاب، ٢٠١٠.

أحمد حجاج، القنابل العنقودية – الأبرياء يدفعون الثمن، مجلة السياسة الدولية، العدد ١٦٦، أكتوبر ٢٠٠٦، المجلد الحادي والأربعون.

أحمد عبيس، الهجمات السيبرانية، مفهومها والمسئولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، بحث منشور بمجلة المحقق الحلي للعلوم القانونية والسياسية، العدد الرابع، السنة الثامنة، ٢٠١٦.

أحمد فنانى، المعجم الإندونيسي المعاصر (يوغياكرتا: مترا فلاجر، عام ٢٠٠٩م).

أنور محمود عبد الواحد، ود. أحمد أمين عبد المجيد، الروبوت بين الخيال والعلم، ١٩٩٦، مركز الأهرام للترجمة والنشر، الطبعة الأولي، ١٩٩٦.

المعجم الوسيط، اللغه العربية .

أيمن حسين،"هل بدأت أمريكا عسكرة الفضاء"، مجلة العربى – الكويت، العدد(٦٢)يوليو ٢٠١٠، متاح على الرابط :
https://www.alarabimag.com/books/17813

بشير علي عرنوس، الذكاء الاصطناعي، دار السحاب للنشر والتوزيع، الطبعة الأولي، ٢٠٠٨.

بلاي وايتباي، الذكاء الاصطناعي، دار الفاروق، ٢٠٠٨.

توماس كوبلاند"محرر"، ثورة المعلومات والأمن القومى"، سلسلة دراسات عالمية، مركز الامارات للدراسات والبحوث الاستراتيجية، العدد(٤٦)، أبوظبى ٢٠٠٣.

حسن مظفر الرزو، الفايروسات والحاسب الإلكتروني: المخاطر المحتملة وسبل الحد منه، المجلة العربية العلمية للفتيان، المنظمة العربية للتربية والثقافة والعلوم، المجلد الاول، العدد الثاني، ١٩٩٧.

حميد حمد السعدون، "التنمية السياسية و التحديث" العالم الثالث، الذاكرة للنشر والتوزيع، عمان ٢٠١١.

سمير فرج، الفضاء السيبرانى – جريدة الاهرام المصرية ٣٠ يوليو ٢٠٢٠- مقال بالموقع الالكترونى .

رأوبلود، ترجمة أسامه أمين الخولي، محمد مرسي أحمد، الإنسان والطاقة، مكتبة الأسرة.

رضا إبراهيم محمود، الأسلحة الذكية تصلح للجيوش الذكية، مجلة المسلح، الحادي عشر من يوليو ٢٠١٣.

رغدة البهي، الردع السيبراني: المفهوم والإشكاليات والمتطلبات، المركز الديمقراطي العربي، العدد الاول، مجلة العلوم السياسية والقانون، القاهرة، ٢٠١٧.

ستكسنيت...قصة الدودة الالكترونية المخربة للمشروع النووى الايرانى، صحيفة الشرق الأوسط، لندن، العدد(١٢٥٤١) فى ٢٠١٣/٣/٣٠.

سحر قدوري الرفاعي، الحكومة الالكترونية وسبل تطبيقها: مدخل استراتيجي، مجلة اقتصاديات شمال افريقيا، العدد السابع، جامعة حسيبة بو على، ٢٠١٦.

صفات أمين سلامة، وخليل قورة، تحديات عصر الروبوتات وأخلاقياته، مركز الإمارات للدراسات والبحوث الإستراتيجية.

صفات أمين سلامه، أسلحة حروب المستقبل بين الخيال والواقع، العدد ١١٢، مركز الإمارات للدراسات والبحوث الإستراتيجية، بدون سنة نشر .

طلال محمد الحاج ابراهيم، الهجمات الالكترونية والمسؤولية الجنائية للقادة، المجلة القانونية والقضائية، وزارة العدل– مركز الدراسات القانونية والقضائية، السنة ١٢، العدد الأول، ٢٠١٨.

طلال ياسين العيسي، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي، مجلة الزرقاء للبحوث والدراسات الإنسانية، جامعة الزرقاء عمادة البحث العلمي، المجلد ١٩، العدد الاول، ٢٠١٩.

عادل عبد الصادق،

– أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، سلسلة أوراق، العدد رقم الثالث والعشرون، سلسلة تصدر عن وحدة الدراسات المستقبلية بمكتبة الإسكندرية.

– الإرهاب الإلكتروني – القوة في العلاقات الدولية: نمط جديد وتحديات مختلفة، مركز الدراسات السياسية والاستراتيجية، ٢٠٠٩.

عبد الرحيم رجوانى، عصر المعلومات، جموح تكنولوجيا المعلومات فى ظل العولمة، سلسلة المعرفة للجميع، رقم ٩، سبتمبر ١٩٩٩، مطبعة النجاح، الدار لبيضاء.

عبد الله احمد القرنى، بحث فى (التفاعل الاجتماعي في المجتمعات الافتراضيه)، مجلة العربى، فى ٢٦ /٢٠٢١/٩ .

عبد المقصود حجو، نظم التحكم الألى الرقمية الحديثة، دار الكتب العلمية للنشر والتوزيع.

علم الدين باتقا، مخاطر الهجمات الالكترونية (السيبرانية) وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجي، دراسات تنموية، المعهد العربي للتخطيط، الكويت، العدد٣٦ ، ٢٠١٩.

عمار عباس الحسيني، جرائم الحاسوب والانترنت (الجرائم المعلوماتية) الطبعة الاولي، منشورات زين الحقوقية، لبنان، ٢٠١٧.

عمار ياسر محمد زهير البابلى،

- آليات التأمين والوقاية من الهجمات السيبرانية بالتطبيق على معايير الجودة الخاصة بالمواصفات القياسية لنظام إدارة أمن المعلومات ISO 27001 للحماية

- التحديات الأمنية المعاصرة للهجمات السيبرانية، القيادة العامة لشرطة الشارقة مركز بحوث الشرطة، المجلد ٣٠، العدد ١١٨، ٢٠٢١.

ليزانوكس، قصة تكنولوجيا الروبوتات، الدار العربية للعلوم، ناشرون، ٢٠١٢.

متاح علي :https://futureuae.com/m/Mainpage/Item/617/cyberterrorism

مجلة الفضاء السيبرانى –منشور فى ٢٠٢١/٥/٢٢ وتم تعديله فى ٢٠٢١/١١/١٠-

محمد أديب رياض غنيم، التطور التكنولوجي في مصر، الهيئة المصرية العامة للكتاب، ٢٠١٢.

محمد على صالح، التحقيق مع جنرال أمريكى متقاعد فى قضية الحروب الالكترونية ضد ايران، صحيفة الشرق الأوسط، لندن، العدد(١٢٦٣٢) فى ٢٩-٦-٢٠١٣.

محمد على فارس، الحماية القانونية لقواعد البيانات فقاً لقانون حق المؤلف – دراسة مقارنة بين النظام اللاتيني والنظام الانجلو أمريكى .

محمد فارس الزغبى، الحماية القانونية لقواعد البيانات وفقا لقانون حق المؤلف – دراسة مقارنة بين النظام اللاتينى والنظام الأنجلو أمريكى.

محمود مدين، فن التحقيق والاثبات في الجرائم الالكترونية، بدون دار نشر، ٢٠٢٠.

ممدوح عبد الحميد، البحث والتحقيق الجنائى الرقمى فى جرائم الحاسب الألى والإنترنت، دار الكتب القانونية، ٢٠١٠.

منير البعلبكي ورمزي منير، المورد الحديث، دار العلم للملاين، بيروت، ٢٠٠٩.

الموسوعة السياسية ، https://political-encyclopedia.org/

نـور أميـر الموصـلي، الهجمـات السـيبرانية فـي ضـوء القـانون الـدولي الإنسـاني، رسـالة ماجستير في القانون الدولي الإنساني، الجامعة الافتراضية السورية، ٢٠١٠.

ياسر عبد السلام رجب، دور الضبط الادارى الالكترونـى فـى الرقابـة السيبرانية، المجلد ٢، العدد ١، إبريل ٢٠٢٢.

ياسر محمد عبد السلام، الرقابـة السيبرانية وتهيئـة البيئـة السيبرانية الامنـة، مجلـة القـانون والتكنولوجيا – المجلد ٢، العدد ١، إبريل ٢٠٢٢.

المراجع الأجنبية:

Author: Lalu Supriadi Bin Mujib Author's Affiliation: Universitas Islam Negeri Mataram Email: nasabila46@gmail.com

Colin S. Gary, Strategy for chaos :Revolutions in Military Affairs and the evidence of history, with a foreword by Williamson Murray ,London, Portland OR frank cass 2003,

Cordesman, Anthony H. and Justin G. Cordesman, Cyberthreats, Information Warfare , and Critical Infrastructure protection (London: Praeger, 2002),36

cyper security intelligence in 22/5/2017 retrieved edited in 10/11/20211"The Difference Between Cyberspace & The Internet "

future for adnanced research and studies **استراتيجيات الدول لمواجهة الإرهاب الإلكترونى،**

https://ar.wikipedia.org/wiki/%D9%81%D8%B6%D8%A7%D8%A1_%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A الموقع الالكترونى ويكيبديا العالمى....

-https://www.alarabimag.com/books/17813

Research Handbook on International Law and Cyberspace, (Nicholas Tsagourias & Russell Buchan Eds. Elgar, 2015.

Ugo Pagallo, the laws of robots " crimes, contracts, and torts, law, governance and technology series, volume 10,2013.