" الجوانب القانونية الدولية لجريمة الإرهاب الالكتروني "

الدكتورة: سحر جمال عبد السلام زهران (١♣)

الملخص:

يعتبر الإرهاب الإلكتروني من أكثر المخاطر الاستراتيجية التي تواجه العالم اليوم في ظل ظهور فئة جديدة من المجرمين تستخدم ما يعرف الذكاء الاصطناعي في تحديث الأسلحة الإلكترونية. الاستخدام الضار سيؤدي إلى شل قدرة الدول على صد الهجمات الالكترونية في العالم فاستخدام الذكاء الاصطناعي في العمليات الإرهابية يزيد من المخاطر الأمنية، مما يستدعى ضرورة التعاون القانوني الدولي لإبرام اتفاقيات لتنظيم الجرائم الإرهاب الالكتروني وفرض القوانين والعقوبات على المجرمين، ويطرح الإرهاب الالكتروني تحديات حول دور القانون الدولي الإنساني في فرض قوانين وقواعد قانونية دولية تنظم استخدام الأسلحة العشوائية وتحدد أسس التنظيم القانوني الدولي للتمييز بين الأهداف العسكرية والمدنية في الهجوم الالكتروني بالتكنولوجيا الحيوية والذكاء الصناعي والطائرات بدون طيار، ويعد من أخطر أنواع الإرهاب في ظل الحروب غير متكافئة بين الدول المتقدمة والنامية نتيجة الفجوة في الثورة التكنولوجية الجديدة في ظل ظهور الجيوش المنظمة من الروبوتات والهجوم بالتكنولوجيا الحيوية، مما يستدعي إعادة تغيير وتعريف لمصطلح الحروب والعدوان في منظمة الأمم المتحدة.

كلمات مفتاحية: الإرهاب الالكتروني ـ القرصنة والتكنولوجيا – الذكاء الصناعي.

(♣) أستاذ مساعد القانون الدولي العام كلية القانون والدراسات القضائية – جامعة جدة

Abstract:

Cyber-terrorism is one of the most strategic threats facing the world today with the emergence of a new class of criminals using what is known as artificial intelligence to modernize cyber weapons. Harmful use will paralyze countries' ability to repel cyberattacks in the world. The use of artificial intelligence in terrorist operations increases security risks, necessitating international legal cooperation to conclude conventions to regulate cybercrime and impose laws and penalties on criminals. Humanitarian law in imposing international legal laws and rules governing the use of indiscriminate weapons and defining the foundations of international legal organization to distinguish between military and civilian targets in cyber attack with biotechnology and intelligence. It is one of the most dangerous types of terrorism under unequal wars between developed and developing countries as a result of the gap in the new technological revolution in light of the emergence of organized armies of robots and the attack of biotechnology, necessitating a redefinition of the term war and aggression in the United Nations.

Keywords: Cyber Terrorism - Piracy and Technology - Artificial Intelligence.

مقدمه:

يشكل الإرهاب الإلكتروني هاجسًا دوليا على المستوى الاقليمى والدولي الذي يتعرض لهجمات غير مسبوقة من الإرهاب الإلكتروني، وأصبحت الجرائم الإلكترونية تؤثر على امن واستقرار الدول،وأصبحت المنظمات الإرهابية تشن الهجمات الإرهابية عن طريق التجنيد الإلكتروني والقرصنة والتكنولوجيا الحيوية والذكاء الصناعي، وأخيراً بالتهديد والترويع الإلكتروني، مما يستدعى ضرورة التعاون القانوني الدولي لإبرام اتفاقيات لتنظيم الجرائم الإرهاب الالكتروني وفرض القوانين والعقوبات على مرتكبي الإرهاب الإلكتروني في القضاء الالكتروني، ودعم الجهود التشريعية والأمنية للدول والشركات وتصميم الشركات لبرامج حماية ضد تلك الجرائم التي ترتكب امن الشركات الالكتروني والمجال الفضاء الالكتروني للدول، في ظل الخلاف الدولي حول إسناد قواعد المسؤولية الدولية في عمليات الإرهاب الإلكتروني خاصة جرائم ظل جرائم التجسس الإلكتروني بين الدول الكبرى وتبادل الاتهامات حول اختراق الجيوش الالكترونية لسيادة الدول الالكترونية وسيطرة المنظمات الإرهابية على المشهد الدولي منذ قيام ثورات الربيع العربي والتي شكلت لاعب أساسي لظاهرة التطرف والعنف الذي يشهده الواقع الذي نعيشه.

إشكالية الدراسة:

- إعادة صياغة تعريف جريمة العدوان والإرهاب الإلكتروني للحد من استخدام القوة وفقا لقواعد القانون الدولي، إبراز خطر الاستخدام العشوائي للأسلحة الالكترونية والهجمات باستخدام التكنولوجيا الحيوية والهجمات الخبيثة وعدم التمييز بين المقاتلين والمدنيين والأهداف العسكرية والمنشآت المدنية عند شن هجمات الإرهاب الالكتروني.
- ما مدى مشروعية استخدام الأسلحة الالكترونية الجديدة بحجة الدفاع الشرعي عن النفس في الهجمات الالكترونية و مع ضرورة وجود تنظيم للفضاء قانوني دولي يحكم الفضاء الالكتروني وقضاء جنائي دولي الكتروني للتدخل السريع في الحروب الالكترونية.

أهمية البحث:

يطرح الإرهاب الالكتروني تحديات حول دور القانون الدولي الإنساني في فرض قوانين وقواعد قانونية دولية تنظم استخدام الأسلحة العشوائية و تحدد أسس التنظيم القانوني الدولي للتمييز بين الأهداف العسكرية والمدنية والهجوم الالكتروني بالتكنولوجيا الحيوية والذكاء الصناعي والطائرات بدون طيار.

أهداف البحث:

جرائم الإرهاب الإلكتروني الدولي من أخطر أنواع الإرهاب في ظل الحروب غير متكافئة بين الدول نتيجة الفجوة في الثورة التكنولوجية الجديدة ويطلق عليها الحروب الالكترونية في ظل ظهور الجيوش المنظمة من الروبرتات والهجوم بالتكنولوجيا الحيوية، مما يستدعي إعادة تغيير وتعريف لمصطلح الحروب والعدوان في منظمة الأمم المتحدة في ظل التحديات التي يواجها القانون الدولي التقليدي والجنائي والإنساني الدوليين وأثرة علي السلم والأمن الدوليين وكيفية تطبيقه في الفضاء الالكتروني.

منهج البحث:

منهج التحليل القانوني للظاهرة ومنهج تحليل النظام الدولي لبيان تأثير التكنولوجية على مرتكزات النظام الدولي والمنهج الاتصالي باعتبار الفضاء الإلكتروني منظومة اتصالية.

خطة البحث:

- **المبحث الأول: ماهية لإرهاب الالكتروني في إطار قواعد القانون الانسانى الدولي**
  - **المطلب الأول: تعريف الإرهاب الالكتروني**

– أولا: مفهوم الإرهاب الالكتروني في إطار قواعد القانون الدولي الإنساني

– ثانيا:الإرهاب الالكتروني والحرب الروبوتية

- ثالثا: التكييف القانون لهجوم القراصنة الالكترونية أثناء النزاع المسلح

- **المطلب الثاني: الحروب الالكترونية في إطار قواعد القانون الدولي الإنساني**

- أولا: مبدأ التمييز وحظر الهجمات العشوائية غير المتناسبة مع رد الفعل
- ثانيا:الإرهاب الالكتروني ومشروعية استخدام القوة

- **المبحث الثاني: التكييف القانوني للإرهاب الالكتروني في اطار ميثاق الأمم المتحدة**

- **المطلب الأول: الإرهاب الكتروني والدفاع الشرعي في إطار قواعد القانون الدولي**
- **المطلب الثانى: مبدأ عدم التدخل في اطار التدابير المضادة في القانون الدولي**

- **المبحث الثالث: تحديات الإرهاب الالكتروني علي الأمن العالمي**

- **المطلب الأول: الأمن السيبراني وهجمات الإرهاب الالكتروني**

- أولا: الصراع السيبرالي بين الدول الكبرى وأثره علي الأمن الدولي
- ثانيا:حروب الشركات الالكترونية وأثرها علي الأمن الدولي
- ثالثا: الإرهاب الالكتروني والتجسس والعدوان

- **المطلب الثاني: اثر المنظمات الإرهابية الالكترونية علي الأمن الدولي**

- أولا:الإرهاب الالكتروني المنظم وأثره علي الأمنالدولي
- ثانيا تنظيم وتمويل المنظمات الإرهابية وشن الهجمات الالكترونية والأزمات الدولية
- ثالثا: أثر الذكاء الصناعي وجيوش الروبرتات على الامن الالكترونى
  - الروبرتات والأمن الإلكتروني
  - الحروب الالكترونية غير المتكافئة

المبحث الأول

ماهية الإرهاب الالكتروني في إطار قواعد القانون الانسانى الدولي

شهدت السنوات الأخيرة تطورات مهمة في تطور المبادرات القانونية ومكافحة الإرهاب على الصعيدين الوطني والدولي نتيجة القصور في النصوصالقانونية الدولية للاستجابة بفعالية للهجمات الإرهابية الشرسة لخطورتها على الأمن الاستراتيجي العالمي والاقليمى في ظل تصاعد وتيرة الجرائم القراصنة والمنظمات الإجرامية الدولية عبر الفضاء الإلكتروني(i).

المطلب الاول

تعريف الإرهاب الالكتروني

ينصرف الإرهاب الإلكتروني بقيام دولة أو عناصر إجرامية من غير الدول بشن هجمات إلكترونية في إطار متبادل لها يعتمد على الترويع وبث الخوف، وبالتالي فإن أي عمل إجرامي يتوج بنتيجة محددة في ضوء معايير القانون الجنائي الدولي يكون عملاً إرهابياً – سواء أكان ممكناً أم لا. وقد نصت بعض التشريعات الدولية علي تجريم الإرهاب الالكتروني وبعض القوانين لم تجرم الأعمال الإرهابية التي تستغل وسائل وتدابير الفضاء الالكتروني على وجه الخصوص(ii).

أولا: مفهوم الإرهاب الالكتروني في إطار قواعد القانون الدولي الإنساني

يشير مفهوم الإرهاب الالكتروني الي أساليب الحرب ووسائلها التي تعتمد على تكنولوجيا المعلومات وتُستخدم في سياق النزاع المسلح في القانون الدولي الإنساني، بخلاف العمليات العسكرية الحركية التقليدية(iii)، فوفقا للمفهوم التقليدي للحرب، فإنها تنطوي على هجمات الجيوش النظامية، ويسبقها إعلان واضح لحالة الحرب، وساحة للميدان قتال محدده، بينما هجمات الفضاء الإلكتروني غير محددة وغامضة الأهداف كونها تتحرك عبر شبكات المعلومات والاتصالات وعابرة للحدود الدولية بالإضافة إلى استخدام أسلحة تكنولوجية إلكترونية جديدة يتم توجيها ضد المنشآت الحيوية أو دسها عن طريق عملاء لأجهزة الاستخبارات(iv) وتدخل هذه الأعمال العدائية في إطار ما

يعرف "الحروب غير المتكافئة"، في ظل عدم القدرة على التمييز بين الأهداف المدنية أو العسكرية في هجمات الحروب الإلكترونية مما يصعب من فرض حماية دولية(v).

ثانيا: الإرهاب الالكتروني والحرب الروبوتية:

اكتسبت الروبوتات العسكرية اهتماماً متزايداً في ظل السعي لدراسة الآثار الأخلاقية لاستخدامها في مجال الحروب، ومدى امتثالها لمتطلبات القانون الدولي الإنساني.وفي هذا الصدد، يُثار خلاف أكاديمي حول مدى أخلاقية استخدام الروبوتات في المجال العسكري، فالبعض يتوقع أنها ستكون أفضل من الجنود في تسيير الحرب في الظروف المعقدة، بل ويمكن أن تكون أكثر إنسانية في ساحة المعركة من البشر، وفي المقابل، اعتبر آخرون الروبوتات العسكرية من الأسلحة الفتاكة(vi). فى ظل عدم وجود أسلحة "ذاتية التحكم تماماً" – أي الأسلحة التي يمكن أن تختار أو تنفذ أهدافها بدون تدخل بشري(vii)، وفي مايو ٢٠١٤، ووقعت الدول الأعضاء في اتفاقية الأمم المتحدة بشأن الأسلحة التقليدية اجتماعاً في جنيف حول "أنظمة الأسلحة الفتاكة ذاتية التحكم" من أجل وضع الروبوتات القاتلة على قائمة الاهتمام الإنساني الدولي.

في عام ٢٠١٣ تنافست الشركات والدول وتسابقت وتيرة إدماج القطاع الخاص في إنتاج الروبوتات، خاصةً العسكرية حيث أعلنت جوجل شرائها لشركة Boston Dynamic المتخصصة في صناعة الروبوتات العسكرية. وفي يناير ٢٠١٤، أعلنت جو جل شراء شركة Deep Mind المتخصصة في تقنيات الذكاء الاصطناعي الذي يقود نقل أبحاث الروبوتات العسكرية من الهيئات العلمية التابعة للجيش الأمريكي مثل وكالة دربا إلى عمالقة التكنولوجيا مثل شركة Google، إلى توقع تقصير المدى الزمني لتحويل الأبحاث إلى منتجات حقيقية في الأسواق ومجال المعركة(viii)، من ناحية أخرى، لا يوجد الكثير من الروبوتات العسكرية التي تستخدم في أغراض غير مدمرة؛ مثل الروبوتات المخصصة لحماية القوات في أرض المعركة، أو التي تستخدم في انتشال الجنود الجرحى، أو مساعدة الجنود على اجتياز التضاريس الوعرة، أو الكشف عن العبوات الناسفة والمتفجرات وفكها.

ثالثا: التكييف القانون لهجمات القراصنة الالكترونية أثناء النزاع المسلح:

يطلق مصطلح "القراصنة" على الكثير من المجرمين الدوليين الذين يشنون أنشطة مختلفة بدرجة متفاوتة ويمكن القول بأن عمليات الهجوم القراصنة لا تتصل بمعظم العمليات الإلكترونية بالنزاع المسلح، ومن ثم فإن القانون الدولي الإنساني لا يطبق عليها(ix). ولكن الوضع يختلف إذا شارك القراصنة بشكل مباشر في العمليات العدائية من خلال هجمات سيبرانية لدعم أحد طرفي النزاع المسلح، ففي هذه الحالة لا يتوقع القراصنة أن يظل العدو ساكنًا وهم يخسرون الحماية القانونية المكفولة لهم ضد الهجوم المباشر أثناء تنفيذ الهجوم السيبراني والإجراءات التحضيرية التي تشكل جزءًا لا يتجزأ من هذا الهجوم على سبيل المثال في سبتمبر / أيلول ٢٠١٦ أدانت محكمة مقاطعة أمريكية أرديت فيريزي أحد القراصنة في جريمة القتل"، الذي حُكم عليه بالسجن لمدة عشرين عامًا بتهمة للوصول إلى جهاز كمبيوتر محمي دون ترخيص وتقديم الأسماء وعناوين البريد الإلكتروني وكلمات المرور والمواقع أرقام الهواتف من ١،٣٥١ من الأفراد العسكريين وغيرهم من موظفي الحكومة الأمريكية إلى داعش، وأدين فيريزي على أساس من الولايات المتحدة بعد أن أدرجت مثل هذا النشاط الإرهابي ضمن تقنين جرائم الإنترنت في القانون الجنائي الامريكى وبالتالي استطاعت محاكمته في نهاية المطاف(x).

المطلب الثانى

الحروب الالكترونية في اطار قواعد القانون الدولي الإنساني

ينطبق القانون الدولي الإنساني علي الحروب الالكترونية على النزاع مسلح، سواء بين دول أو بين دول وجماعات الإرهابية منظمة، وبناء علي ذلك يجب التمييز بين الهجمات العامة الالكترونية وبين الهجمات الالكترونية الخاصة بالعمليات السيبرانية في حالة النزاع المسلح حيث أن "الهجمات سيبرانية" "الإرهاب السيبراني" تعتبر وسائل حرب، ينطبق القانون الدولي الإنساني عندما تلجأ الأطراف إلى أساليب الحرب

ووسائلها التي تعتمد على العمليات سيبرانية(xi)، بينما الهجمات الخاصة لا يطبق عليها قواعد القانون الانسانى الدولى.

أولا: مبدأ التمييز وحظر الهجمات العشوائية غير المتناسبة مع رد الفعل:

يتطلب مبدأ التمييز، بين أطراف النزاعات بين الهجمات الالكترونية على المدنيين والمقاتلين، وبين الأهداف المدنية والأهداف العسكرية، وقد تكون الهجمات الالكترونية موجهة ضدّ المقاتلين أو الأهداف العسكرية فحسب، وتُحظر الهجمات الالكترونية العشوائية التي تُوجه ضدّ هدف عسكري محدد أو لا يمكن الحد من آثارها وفقا قواعد القانون الدولي الإنساني التي تُحظر الهجمات ضدّ الأهداف العسكرية أو المقاتلين بالمثل إذا كان يُتوقع أن تتسبب بإصابات أو أضرار مدنية عرضية، مقارنة بالمكاسب العسكرية المتوقعة الملموسة المباشرة (المعروفة بالهجمات غير المتناسبة)(xii)، تكمن خطورة القلق الإنساني في هذا الصدد في أن الفضاء الالكتروني يتميّز بالتوصيل بين نظم الحواسيب، ويتألف هذا الفضاء من عدد لا يُحصى من نظم الحواسيب المتصلة يبعضها البعض في أرجاء العالم وغالباً ما يبدو أن نظم الحواسيب العسكرية تتصل بالنظم التجارية والمدنية وتعتمد عليها كلياً أو جزئياً، وبالتالي قد يكون فعلاً من المستحيل شنّ هجوم سيبرآني على بنية تحتية عسكرية وجعل الآثار تقتصر على هدف عسكري فحسب. وعلى سبيل المثال من شأن استخدام للهجمات الخبيثة بالتكنولوجيا الجديدة عندما لا يمكن السيطرة عليها وتتسبب بأضرار كبيرة في بنية تحتية مدنية لدولة ويعتبر ذلك خرقا لمبادئ القانون الدولي الإنساني يتطلب من الطرف المسئول شن هجوم مضاد للدفاع الشرعي ودرئا للعدوان لتخفيف الأضرار على البنية التحتية المدينة التي شنت على المدنيين ويتطلب التحقق من طبيعة النظم التي تعرضت للهجوم والأضرار المحتملة التي قد تنجم عن أحد الهجمات، وهذا يعني أيضاً أنه عندما يصبح جلياً أن هجوماً سيتسبب بإصابات أو أضرار مدنية عرضية وكيفية التصدي له بالهجمات الالكترونية للحد من عمليات العدوان الالكتروني(xiii). وعلى صعيد آخر قد تساهم تكنولوجيا المعلومات أيضاً في الحد من الأضرار العرضية التي تلحق بالمدنيين

أو البنية التحتية المدنية، فعلى سبيل المثال، قد يلحق تعطيل خدمات معينة تُستخدم لأغراض عسكرية ومدنية أضراراً أقل مما يُلحق تدمير البنية التحتية تماماً وفي هذه الحالات يفرض مبدأ الاحتياط القابل للجدل التزاماً على الدول باختيار الوسائل الأقل ضرراً بغية تحقيق أهدافها العسكرية.

ثانيا: الارهاب الالكتروني ومشروعية استخدام القوة:

يحق لدولة لحق بها ضرر من ارتكاب أفعال غير قانونية اتخاذ تدابير مضادة لخرق القانون الدولي ضد دولة أخرى كرد فعل على النشاط غير القانوني للدولة المخالفة والغرض من ذلك هو إجبار الدولة المخالفة على وقف نشاطها غير القانوني ضد الدولة المعتدى عليها، ويشترط لاستخدام التدابير المضادة أن تكون متناسبة مع الضرر مع مبدأ حظر استخدام القوة المشروع(xiv)، و ويشكل مبدأ حظر استخدام القوة مبدأ عام في القانون الدولي وبناء علي ذلك في شن الحرب السيبرانية ضد دولة أخرى رداً على انتهاك ان يكون وفقا لقواعد القانون الدولي إلى ردا "الاستخدام القوة" غير المشروع في إطار القانون الدولي، وتستمد مشروعية استخدام القوة بموجب القانون الدولي على أساس الدفاع عن النفس المنصوص عليها فى المادة ٥١ من ميثاق الأمم المتحدة لكي تكون مشروعة كأن يشكل الخرق "هجومًا مسلحًا" على دولة لاستيفاء الشروط الأخرى لقواعد الدفاع عن النفس بما في ذلك متطلبات الضرورة والتناسب وبالإضافة إلى عامل آخر يتعلق بالهجمات الالكترونية في حالة عدم قيام الدولة باتخاذ هجمات الكترونية انتقامية بمقتضى مبدأ الاستخدام المشروع للقوة، درئ الخطر من قبيل طبقا لقواعد الدفاع الشرعي في مواجهة الدولة المستهدفة في الإطار المشروع في المجتمع الدولي ككل بمشروعية استخدام القوة الالكترونية لصد الهجوم الإلكتروني حتى لا يؤدى ذلك إلى تصعيد الوضع(xv).

والسؤال الذي يطرح نفسه على بساط البحث هو:هل يمكن أن يؤدي تدمير البيانات أو اختراق مواقع الويب أو الانقطاع الدوري للخدمات عبر الإنترنت إلى انتهاك للحظر المفروض على استخدام القوة؟

والحقيقة أنه من غير المحتمل أن يحدث الهجوم من قبل فرد وعادة ما يكون بينما أفعال تشكل جريمة وتدخلاً في الشؤون السيادية لدولة أخرى بالإضافة إلى احتمال أن يكون له تداعيات بموجب القانون الدولي لحقوق الإنسانان تؤدي الي نزاع وهجوم المسلح بين أطراف النزاع، إن الحد الأدنى لما يشكل "استخدام القوة" من حيث العمليات السيبرانية أقل وضوحا بكثير مقارنة بالأسلحة التقليدية الحركية، وهذا مجال آخر فشلت فيه منظمة الأمم المتحدة في التوصل إلى اتفاق بشأن تنظيم استخدام القوة التكنولوجية الجديدة برفض النص المقترح من قِبَل عدد قليل من الولايات (بما في ذلك كوبا وروسيا والصين) جعلت عملية إصدار اتفاقية بشأن التنظيم القانوني للفضاء الالكتروني فيما يتعلق باستخدام القوة الالكترونية التكنولوجية في طريق مسدود فعلى سبيل المثال حث تقرير من مايكروسوفت الدول على ممارسة ضبط النفس في إجراء العمليات الهجومية مشيراً إلى أن الهدف النهائي للقواعد التي توجه العمل الهجومي يجب أن يكون للحد من النزاعات بين الدول.

المبحث الثاني

التكييف القانوني للإرهاب الالكتروني في إطار ميثاق الأمم المتحدة

المطلب الأول

الإرهاب الكتروني والدفاع الشرعي في إطار قواعد القانون الدولي

أكد فريق الخبراء الحكوميين التابع للأمم المتحدة المعني باستخدام التكنولوجيات الإلكترونية، تطبيق القانون الدولي الحالي على الأنشطة الإلكترونية للدول. في ٢٦ يونيو ٢٠١٥، أقر فريق الخبراء، بما في ذلك ليس فقط المملكة المتحدة والولايات المتحدة الأمريكية و أيضا روسيا والصين بأن ميثاق الأمم المتحدة ينطبق بالكامل على الفضاء الالكتروني، وان الأساس القانوني الدولي لهذا الحق ينصرف إلى أهمية الحق المتأصل لدولة ما في التصرف دفاعًا عن النفس رداً على الهجوم الإلكتروني ردا على هجوم مسلح، بالإضافة إلى ذلك أكد تقرير ٢٠١٥ أن الحماية الأساسية للقانون الدولي

الإنساني إلى" الضرورة والتناسب والإنسانية والتمييز، تنطبق في الفضاء الالكتروني(xvi) وحدد ميثاق الأمم المتحدة قواعد ذات أهمية خاصة كالاتى:

أولا: قاعدة حظر التدخل في الشؤون الداخلية للدول بموجب المادة ٢ (٧) من الميثاق وفي القانون الدولي العرفي و يعني هذا الحظر أن أي نشاط في الفضاء الالكتروني يصل إلى مستوى معين من التدخل غير المشروع من قبل الدولة لا يمكن إلا أن يكون مسموحا به ولو كان استجابة للدول مسبقة من قبل دولة أخرى، والقاعدة الثانية والتي يرتبط بها البند التالي ذي الصلة من ميثاق الأمم المتحدة هو في المادة ٢ (٤) التي تحظر التهديد أو استخدام القوة ضد الاستقلال الإقليمي أو السلامة السياسية لأية دولة. أي نشاط من قبيل ذلك لا يعد مشروع إلا في إطار الاستثناءات المعتادة استجابة لهجوم مسلح دفاعا عن النفس أو كإجراء من المنصوص عليه في الفصل السابع يأذن به مجلس الأمن. إضافة إلى ذلك إلى أنه يجب أن يكون مسموح بموجب القانون الدولي وينطبق في ظروف الاستثنائية استجابة لمبدأ ضرورة استخدام القوة إلى أساس التدخل الإنساني لتفادي كارثة إنسانية طاحنة([xvii]).

ثانيا: القاعدة الثانية تتعلق بوجوب أن تؤدي الهجمات الالكترونية الي تهديد أو تعرض تهديدًا وشيكًا للموت والدمار على نطاق متكافئ للهجوم المسلح للقيام بإجراءات الدفاع عن النفس المنصوص عليه في المادة ٥١ من ميثاق الأمم المتحدة[xviii]، فإذا قامت دولة في تشغيل أحد مفاعلاتها النووية بشكل يعرض إلى خسائر كبيرة في الأرواح، فإن حقيقة الفعل يشكل عملية إلكترونية تنطوي على الاستخدام غير المشروع للقوة أو هجوم مسلح ومن شأنه ذلك خرق قواعد القانون الدولي وترتب علي ذلك تفجير برج مراقبة جوي وإسقاط الطائرات المدنية يعتبر خرقًا للقانون الدولي لهجمات الكترونية لتعطيل أنظمة مراقبة الحركة الجوية ونرتب عليها في نهاية المطاف آثار تدمير وتخريب وقتل مثل أعمال تستهدف الخدمات الطبية الأساسية يعتبر تدخلا محظورا من قبيل العدوان المسلح للدولة على دولة مما ينص عليه الاستخدام المشروع للقوة الالكترونية لصد الهجمات الالكترونية وبالإضافة فإن تطبيق القانون الإنساني الدولي على العمليات الالكترونية في النزاعات المسلحة يوفر الحماية والوضوح عندما تشارك

الدول في النزاع المسلح فإن هذا يعني أنه يمكن الاستخدام المشروع للعمليات الالكترونية لعرقلة قدرة الجماعات المعادية مثل داعش على تنسيق الهجمات وحماية قوات التحالف في ساحة المعركة ويترتب عليها مسؤولية الدول الأخرى عن الهجمات الالكترونية ويعني ذلك انه في ساحات الحروب الالكترونية الجديدة في الفضاء الإلكتروني بأن هناك مجموعة من المبادئ والقواعد التنظيمية التي تسعى إلى تقليل الآثار الإنسانية للصراع. والسؤال الأخر الذي يطرح نفسه على بساط البحث كيف يتصدى القانون الدولي لتنتظم الأنشطة الإلكترونية في وقت السلم والحرب مع ضرورة تنظيم قواعد دولية جديدة تحظر التدخل في الشؤون الداخلية للدول في الفضاء الالكتروني؟ الاجابه علة هذا السؤال في المطلب التالي.

المطلب الثاني

مبدأ عدم التدخل في إطار التدابير المضادة في القانون الدولي

الحقيقة انه بموجب حق الدفاع الشرعي الذي يخول للدول الضحية اتخاذ تدابير مضادة ردا على الدول المعتدية هناك خلاف قانوني في الفقه الدولي حول تفسيره ذلك بأنه غير مشروع إذا قامت دولية بتدخل في شؤون دولة أخرى واستخدمت القوة الالكترونية ويهدف إلى إعادة العلاقات بين الدولة المعادية والدولة الضحية إلى دائرة الامتثال المشروعية الدولية ووضع حد لهذا الفعل غير القانوني السابق، وهذا العمل مسموح به بموجب استخدام لمبدأ القانون الدولي الخاص بالتدابير المضادة، إذا قامت دولة معادية بخرق قواعد القانون الدولي واتخاذ إجراءات قسرية ضد الحريات السيادية للدولة المستهدفة، عندئذ يمكن للدولة الضحية اتخاذ إجراءات لإجبار تلك الدولة المعادية على التوقف،وتمشيا مع الطبيعة قواعد للقانون الدولي، هناك قيود واضحة على الإجراءات التي يمكن لدولة ضحية أن تتخذها بموجب مبدأ التدابير المضادة، لا يمكن اتخاذ إجراء مضاد إلا بسبب فعل غير مشروع دوليًا سابقًا ارتكبته دولة ما، ويجب ألا يتم توجيهه إلا إلى تلك الدولة، وهذا يعني أن الدولة الضحية يجب أن تعلن

إسناد ذلك الفعل إلى دولة معادية قبل أن تتخذ إجراءً في الرد في الفضاء الإلكتروني لأنه يترتب عليه إجراءات خطيرة في لحظات قليلة نظرا لأنها تنطوي على التدابير المضادة على استخدام القوة، ويجب أن تكون ضرورية ومتناسبة مع غرض حمل الدولة المعادية على الامتثال لالتزاماتها بموجب القانون الدولي(xix).

ونري ان التدابير المضادة الضرورية يجب ان تكون متناسبة مع عدم شرعية الفعل الأصلي و ان أي خرق للقانون الدولي يحق للدول اتخاذ الإجراء المضاد الذي قد يكون غير قانوني في الرد، لكن هناك مجال آخر متنازع عليه بين تطبيق القانون الدولي على الفضاء الإلكتروني هو تنظيم الأنشطة التي تقع تحت عتبة التدخل المحظور، والذي ينظر إليه على أنه يؤثر على السيادة الإقليمية لدولة أخرى بدون موافقة مسبقة من تلك الدولة. ويجب ألا تستخدم الدول مبدأ السيادة لتقويض الحقوق والحريات الأساسية ويجب الموازنة الصحيحة بين الأمن القومي وحماية الخصوصية وحقوق الإنسان،لأنه لا يوجد أي التزام قانوني يفرض على الدولة أن تكشف علنًا عن المعلومات الأساسية التي يستند إليها قرارها بإسناد نشاط معادٍ، أو أن تنسب علنًا نشاطًا عدائيًا عبر الإنترنت في جميع الظروف،ومع ذلك يمكن أن تنسب النشاط الإلكتروني الخبيث حيث نعتقد أنه من مصلحتها أن نفعل ذلك وتعلن عن تبرير ذلك عن تعزيز التزامها الى الاستقرار الامنى في الفضاء الالكترونى. والحقيقة أنها أحيانا تقوم بذلك علنا وأحيانا يقوم بذلك فقط البلد المعني فعلى سبيل المثال أثر هجوم WannaCryRansomware على ١٥٠ بلدًا بما في ذلك ٤٨ صندوقًا وطنيًا للخدمات الصحية في المملكة المتحدة، وكان واحدا من أهم الهجمات التي ضربت المملكة المتحدة من حيث الحجم والاضطراب، في كانون الأول ٢٠١٧، تعمدت بريطانيا بالتعاون مع الولايات المتحدة وأستراليا وكندا ونيوزيلندا والدنمرك واليابان إلى اسناد هذا الهجوم إلى ممثلين كوريين شماليين، بالإضافة إلى ذلك، تعرض ١١ دولة أخرى، للهجوم الإلكترونيNot Petya المدمر (xx).

المبحث الثالث

تحديات الإرهاب الالكتروني علي الامن العالمي

المطلب الاول

الأمن السيبراني وهجمات الإرهاب الالكتروني

تحولت طبيعة الحرب من الحروب التقليدية إلى الإنترنت، وشاهدت طوفانا من الهجمات السيبرانية التي ترعاها الدولة على الغرب وظهر اثر ذلك بوضوح تحت دائرة الضوء العالمي ٢٠١٨عندما قدمت المملكة المتحدة والولايات المتحدة بإصدار بيانا مشتركا لم يسبق له مثيل يلوم روسيا على الهجمات السيبرانية على الشركات والمستهلكين وكان الإعلان للمرة الأولى يتجمع فيه دولتان لإظهار التضامن في هذا المجال رأى المركز الوطني للأمن الإلكتروني (NCSC)، ووزارة الأمن الداخلي الأمريكية، ومكتب التحقيقات الفيدرالي (FBI) يحذر الشركات والمواطنين من أن روسيا تستغل أجهزة البنية التحتية للشبكات مثل كموجهات حول العالم وكان الهدف وضع الأساس للهجمات المستقبلية على البنية التحتية الحيوية مثل محطات الطاقة وشبكات الطاقة.

أولا: الصراع الالكتروني بين الدول الكبرى وأثره علي الأمن الدولي:

في أبريل ٢٠١٨، قامت حكومتا الولايات المتحدة والمملكة المتحدة بضرب شركة الاتصالات الصينية المملوكة للدولة ZTE، مع كتابة NCSC لمزودي خدمات الاتصالات في المملكة المتحدة للتحذير من أن استخدام معدات وخدمات الشركة يمكن أن يشكل خطرا على الأمن القومي(xxi). كانت هناك أيضًا تقارير متعددة عن الهجمات إلكترونية التي استهدفت محطات الطاقة والشبكات الكهربائية وألقت الولايات المتحدة باللوم على روسيا في توجيه ضربة أخيرة لشبكتها الكهربائية، في حين أن مجلس الأمن القومي ألقى على الكرملين مسؤولية عدة محاولات لتعطيل البنية التحتية في المملكة المتحدة، وفي أغسطس من ٢٠١٨عام تعرضت شركة للبتر وكيماويات مع مصنع في المملكة العربية السعودية لهجوم يهدف إلى إحداث انفجار، كما شملت الخدمات لموجه خطيرة من هجوم الإلكتروني في قطاع الصحة والمؤسسات المالية

حيث كان جهاز cryptoworm قام بتمزيق نظام NHS في المملكة المتحدة بمثابة تحذير آخر للضرر المحتمل من هجوم دولة عندما تعرضت مئات الآلات للأضرار دون اتصال وتم إلغاء العمليات، في الوقت نفسه إذا نجح أحد الخصوم في التلاعب في البورصة فإنه يمكن يدمر اقتصاد الدولة، ويترتب عليه حدوث ضرر كبيرًا على أنظمة الهجوم بشكل مباشر يتحقق الهدف بتعطيل الدول الأخرى لتحقيق مكاسب سياسية من خلال حملات التضليل مثل الأخبار المزورة، كما تبذل الشركات جهداً لكن المهاجمين في بعض الأحيان قادرون على الوصول إلى الأنظمة بسبب أخطاء بسيطة وبالاعتداءات الإلكترونية على الموظفين الذين يتم استهدافهم عبر رسائل البريد الإلكتروني المزعجة بما في ذلك تنزيل أو رابط إلى موقع ضار، شنت الهجمات الإلكترونية من جهات بارزة فاعلة تابعة للدولة، ولكنها استهدفت في كثير من الأحيان الشركات وغيرها من المنظمات غير الحكومية، في عام ٢٠١٤، هاجم قراصنة الكمبيوتر في كوريا الشمالية شركة Sony Pictures وهددوا بتسريب رسائل البريد الإلكتروني والأفلام التي لم تصدر بعد في حين سرق مخترقو جيش التحرير الشعبي في الصين أسرارًا تجارية من الشركات الأمريكية لردع الهجمات الإلكترونية المستقبلية، وشدد رئيس التحقيقات إلى ضرورة تحديد هوية الجناة بشكل علني وزيادة العقوبات حتى تتوقف الهجمات(xxii).

ثانيا: حروب الشركات الالكترونية وأثره علي الأمن الدولي:

يعد هجوم الواسع من الفيروسيات في عام ٢٠١٧ الذي أشار رئيس مايكروسوفت براد سميث إلى أن الفيروس استهدف نقطة ضعف في برمجيات Microsoft التي سبق أن اكتشفها وكالة الأمن القومي الأمريكية (NSA) والتي تم تسريبها بعد ذلك إلى المجال العام و كانت وكالة الأمن القومي قد أفادت بوجود ثغرة في Microsoft عندما تم تحديدها لأول مرة ومن المحتمل أن تكون الشركة قد أصدرت تحديثًا أمنيًا لعشرات الملايين من أجهزة الكمبيوتر التي تستخدم برامجها مما تسبب في أضرار واسعة النطاق تحتاج الحكومات إلى إتباع نهج مختلف للفضاء الالكترونى وتطوير قواعد

مماثلة لتلك التي تحكم الأسلحة البيولوجية والكيميائية في العالم المادي. بالإضافة إلى ذلك، يتنامى التفاهم من جانب صانعي القرار حول الإمكانات التدميرية الشديدة لأعمال الإرهاب التي قد يتم تنفيذها في نهاية المطاف عبر الفضاء الالكتروني إما ضد الأهداف التي تتألف بشكل حصري من البيانات، مثل النظم المالية والصحية أو أهداف البنية التحتية الحيوية المادية التي تعتمد على الإنترنت لتشغيلها مثل أنظمة المياه وحركة الطيران(xxiii). من الواضح أن هذه الهجمات لم يصرح بها الإرهابيون على الرغم من أنها نفذت من قبل جهات فاعلة تابعة للدولة وغير تابعة للدولة إلا أن القادة الوطنيين والدوليين أعربوا عن قلقهم من أن الهجمات الإرهابية الإلكترونية هي "إمكانية متزايدة". مثل هذه الهجمات على البنية التحتية الحيوية والبيانات الهامة ليست سوى مسألة وقت، وهكذا يطرح سؤال بشأن مدى استعداد النظم القانونية الوطنية والدولية لمواجهة هذا التحدي المقبل(xxiv)، إضافة إلى المخاطر في القطاعات الحساسة التي تشير إلى أن "هناك قدر كبير من CNIيسند الى القطاع الخاص، والهجمات من المرجح أن تكون ناجحة عند استهداف سلاسل التوريد CNI، ولا سيما تلك الموجودة في الخارج أو التي تحتفظ بها الشركات الصغيرة مع أقل نموا أو سياسات أمنية متطورة على الإنترنت(xxv). يجب ان تقوم الشركات بتدريب إلى هذه التهديدات حيث أنها استخدمت أنظمة الصناعية شكلت خطرا لسنوات دون أن يتم رصدها، كما تقول أميلي أورتن، الشريكة في مؤسسة Darktrace نحن بحاجة إلى إستراتيجية دفاعية أكثر تطوراً لحماية الشبكات الصناعية من التهديدات الالكترونية التي تمكنت من التسلل إلى هذه الأنظمة الحرجة ويجب أن نمسك بها في وقت مبكر، في حين يمكن للشركات الخاصة في ظل ظروف معينة مشاركة سجلات البريد الإلكتروني، أو GPS، أو غيرها من البيانات ذات الصلة بالملاحقة القضائية المحلية، يجب على المحققين استخدام معاهدة المساعدات القانونية المتبادلة (MLAT) لإجبار شركة مقرها في الخارج لتوفير الأدلة الرقمية الأساسية. MLATs معروفة بآليات تستنفذ وقتا طويلا وشاقا، وليس مصممة لعالم متصل رقميا، وهذا مجال واحد فقط يجب أن تتطور فيه المعايير والأدوات القانونية الدولية لمواكبة ملاحقة الجرائم عبر الوطنية. وتشكل قدرة

الجماعات الإرهابية على تكييف أحدث التكنولوجيات المتاحة لأغراضها التي تشكل تحديا خطيرا لتطبيق الآليات القانونية الدولية لإجراءات قانونية غير ملائمة(xxvi).

ثالثا: الارهاب الالكتروني والتجسس والعدوان:

تتنوع أساليب الإرهاب الإلكتروني لتشمل الحرب الإلكترونية السرية، وهي التي تتم من خلال زراعة برامج تجسسية مشفرة في أجهزة المستهدفين تخدم مصالح الجهة المهاجمة، إضافة إلى الهجمات على الأهداف الاقتصادية والتي تستهدف الأهداف المرتبطة بعالم المال والأعمال، مما يؤدي إلى التشكيك في صحة المعلومات المطروحة في الشبكة الاقتصادية، والهجمات على شبكات الطاقة الكهربائية حيث أصبح الاعتماد على شبكات المعلومات خاصة في الدول المتقدمة من الوسائل المهمة لإدارة نظم الطاقة الكهربائية، علاوة على الهجمات على الأهداف المدنية مثل شبكات المعلومات الطبية، والتي يمكن مهاجمتها واختراقها ما يؤدي إلى خسائر في أرواح المرضى من المدنيين وفي ضوء دور الإرهاب في عمليات التجسس ما اعلنته الولايات المتحدة الأمريكية حيث ألقى البيت الأبيض بإسناد المسؤولية على روسيا في الهجوم الإلكتروني المدمر الذي عرف باسم (نوتبيتيا) عام ٢٠١٧ لينضم إلى الحكومة البريطانية في إدانة موسكو لإطلاقها الفيروس الذي أصاب بالشلل أجزاء من البنية التحتية في أوكرانيا وعطل أجهزة كمبيوتر في دول مختلفة على مستوى العالم،وما شنّه الجيش الروسي في يونيو حزيران ٢٠١٧ "وانتشر على مستوى العالم وألحق أضرارا بمليارات الدولارات في مختلف أنحاء أوروبا وآسيا والأمريكيتين، "كان هذا ضمن جهود الكرملين المستمرة لزعزعة استقرار أوكرانيا ويظهر بوضوح شديد ضلوع روسيا في الصراع القائم" وكان أيضا هجوما إلكترونيا طائشا وعشوائيا ترتب عليه عواقب وخيمة وأعلن الجيش الروسي مسئوليته عن الهجوم الذي كانت "أهدافه الأولية هي القطاعات المالية وقطاعات الطاقة والحكومة الأوكراني.

المطلب الثاني

اثر المنظمات الإرهابية الالكترونية علي الامن الدولي

أولا: الإرهاب الالكتروني المنظم واثره علي الامن الدولي:

تقوم المنظمات الإرهابية بتنظيم وتنسيق عملياتهم المتفرقة والمنتشرة حول العالم، فالوجود الإرهابي النشط على الشبكة العنكبوتية بصورة كبيرة ومن الأمثلة على بعض المواقع الإلكترونية العربية التي قام بإنشائها وتصميمها بعض التنظيمات الإرهابية ما يأتي:

- موقع النداء :وهو الموقع الرسمي لتنظيم القاعدة بعد أحداث الحادي عشر من سبتمبر عام ٢٠٠١م، ومن خلاله تصدر البيانات الإعلامية للقاعدة.
- ذروة السنام: وهي صحيفة إليكترونية دورية للقسم الإعلامي لتنظيم القاعدة.
- صوت الجهاد: وهي مجلة نصف شهرية، يصدرها ما يسمى بتنظيم القاعدة في جزيرة العرب، وهي تصدر بصيغتي وورد، بى، دى،اف (تتضمن مجموعة من البيانات والحوارات مع قادة التنظيم ومنظريه.
- البتار: وهي مجلة عسكرية إليكترونية متخصصة، تصدر عن تنظيم القاعدة، وتختص بالمعلومات العسكرية والميدانية والتجنيد.

ومن أهم العناصر الأساسية لاستخدام الإنترنت في أغراض إرهابية:

- **البحث عن المعلومات** :إن شبكة الانترنت في حد ذاتها تعتبر مكتبة إلكترونية هائلة الحجم، وتكتظ بالمعلومات الحساسة التي يسعى الإرهابيون للحصول عليها مثل أماكن المنشآت النووية، والمطارات الدولية، والمعلومات المختصة بسبل مكافحة الإرهاب، وبذلك يكون ٨٠ % من مخزونهم المعلوماتي معتمداً في الأساس على مواقع إلكترونية متاحة للكل، دون خرقاً لأي قوانين أو بروتوكولات الشبكة.
- **الاتصالات:** تساعد شبكة الانترنت المنظمات الإرهابية المتفرقة في الاتصال يبعضها البعض والتنسيق فيما بينها، وذلك نظراً لقلة تكاليف الاتصال باستخدام

الانترنت، مقارنة بالوسائل الأخرى، كما أنها تمتاز بوفرة المعلومات التي يمكن تبادلها، وقد أصبح عدم وجود زعيم ظاهر للجماعة الإرهابية سمة جوهرية للتنظيم الإرهابي الحديث، مختلفاً بذلك عن النمط الهرمي القديم للجماعات الإرهابية[xxvii].

- **التعبئة وتجنيد إرهابيين جدد:** إن استقدام عناصر جديدة داخل المنظمات الإرهابية، يحافظ على بقائها واستمرارها، وهم يستغلون تعاطف الآخرين من مستخدمي الانترنت مع قضاياهم، ويجتذبون هؤلاء السذج بعبارات براقة وحماسية من خلال غرف الدردشة الإلكترونية، ونحن نعلم أن تسلية الشباب والمراهقين هي الجلوس بالساعات الطويلة في مقاهي الانترنت للثرثرة مع جميع أنواع البشر في مختلف أنحاء العالم.
- **إعطاء التعليمات والتلقين الإلكتروني:** يمتلئ الانترنت بكم هائل من المواقع التي تحتوي على كتيبات وإرشادات تشرح طرق صنع القنابل، والأسلحة الكيماوية الفتاكة، وعند استخدام محرك البحث "غوغل Google "عام ٢٠٠٥ للبحث عن مواقع تضم في موضوعاتها كلمات مثل "إرهابي terrorist و"دليل " handbook، فكانت نتائج البحث ما يقرب من ثمانية آلاف موقع.

ثانيا تنظيم وتمويل المنظمات الارهابية وشن الهجمات الاكترونية والازمات الدولية

يستخدم الإرهابيون الرسائل الالكترونية العادية email وغرف الثرثرة chat rooms، لتدبير الهجمات الإرهابية وتنسيق الأعمال والمهام لكل عنصر إرهابي(xxviii).

يستعين الإرهابيون ببيانات إحصائية ويقومو بدفع تبرعات مالية لأشخاص اعتباريين يمثلون واجهة لهؤلاء الإرهابيين، ويتم ذلك بواسطة البريد الالكتروني بطريقة ماكرة لا يشك فيها المتبرع بأنه يساعد إحدى المنظمات الإرهابية،علي سبيل المثال تقدم تكنولوجيا المعلومات والاتصالات (ICT) واحدة من التحديات الحديثة الأكثر

أهمية للأمن العالمي. وتتنبأ تقييمات التهديد بأن الأزمة الدولية الرئيسية التالية قد تكون بسبب قيام دولة أو مجموعة إرهابية بتسليح تكنولوجيا المعلومات والاتصالات لتدمير البنية التحتية الحيوية أو الشبكات اللوجستية العسكرية لشيكات المعلومات والاتصالات مما يستلزم وضع مدونة دولية للسلوك السيبراني، في مايو ٢٠١٧ على سبيل المثال شنت سلسلة من الهجمات الإلكترونية باستخدام WannaCryRansomware (وهو نوع من فيروسات الكمبيوتر التي تشفر بيانات المستخدم وتطلقها فقط عند دفع فدية) أثرت على مئات الآلاف من أجهزة الكمبيوتر في جميع أنحاء العالم. وقدرت التكلفة الإجمالية لهجمات WannaCry، والتي تنسبها الولايات المتحدة والمملكة المتحدة وغيرها إلى حكومة كوريا الشمالية، بأكثر من مليار دولار. وسرعان ما تبعه هجوم مدمر للبرامج الخبيثة (نوع من الهجمات الإلكترونية التي تمسح أجهزة الكمبيوتر بشكل مباشر، وتدمر السجلات من الأنظمة المستهدفة دون جمع فدية) المعروفة باسم NotPetya / Petya. وقد أثر هذا التفشي القصير الواسع النطاق على العديد من المنظمات في جميع أنحاء العالم، وقدرت تكلفة شركة Maersk التي تعمل في تشغيل حاويات السفن بما يصل إلى ٣٠٠ مليون دولار من الإيرادات المفقودة(xxix).

ثالثا: أثر الذكاء الصناعي وجيوش الروبرتات على الامن الالكترونى

استأجرت وزارة الدفاع الأمريكية ١٠ ديسمبر ٢٠١٨ شركة في كاليفورنيا لتقليص الوقت التجميعي للروبرتات إلى شهر واحد فقط و باستخدام الذكاء الاصطناعية ترى الشركة، C3 في مدينة ريدوود سيتي بولاية كاليفورنيا، نفسها كنوع من خياط الذكاء الاصطناعي، حيث تقوم بتجميع منهجيات مختلفة من التعلم الآلي البسيط إلى التعلم العميق الأكثر تعقيدًا والجمع بين أشكال غير متجانسة من البيانات لا تلعب بشكل جيد معًا من الصور إلى التقييمات التشخيصية للنص في المنتجات الخاصة بهذه المشكلة،بما أن الهجمات الالكترونية في المستقبل تصبح أكثر تلقائية واستقلالية، يجب أن يكون الأمن الإلكتروني مستقبل الهجمات السيبراني يستخدم أدوات ذاتية مبرمجة مسبقًا تصيب شبكة منظمة ما، وتنتقل إلى أهدافها، وتسرقها أو تلحق بها الضرر في دقائق معدودة فقط(xxx).

- **الروبرتات والأمن الإلكتروني:**

الحقيقة ان نظام تتبع جى بى اس لإدارة الأزمات يتيح للقادة الموجودين في غرف العمليات استخدام نظام تتبع المواقع (GPS) لعرض خرائط مكان الأزمة ومعرفة موقع المركبات التي تم إرسالها إلى موقع الكارثة، ان استخدام الروبوتات والذكاء الاصطناعي وتستمد الروبوتات أهميتها من قدرتها على أداء مهماتها في البحث والإنقاذ في البيئات غير الآمنة، مثل البحث عن الناجين وإنقاذهم من تحت أنقاض المباني، أو تفقد الأضرار في المنطقة عند حصول تسرّب نووي، كما أن الإصدارات الصغيرة الحجم من الروبوتات والتي يمكن حملها في حقيبة الظهر، يمكن استخدامها في أراضي المعركة، فالجندي يمكنه تفقّد المباني، من خلال إخراج الروبوت من حقيبة الظهر الخاصة به، ووضعه داخل المبنى، ومن ثم التحكم به أثناء مشاهدة ما تراه الكاميرا الخاصة بالروبوت، مع ضرورة لفت النظر إلى ما ينتج عنه مشاكل أخرى متعلقة بالتجسس وتشويه المعلومات وغيرها من المشكلات من خلال التحكم الكامل في كل المعلومات الصادرة أو الواردة من هذا القمر، حيث أن الأقمار المتخصصة في هذا المجال على درجة عالية من الدقة والاحترافية في رصد وسائل الاتصالات وعملية تداول المعلومات والتصوير والمراقبة بكل أشكاله.

- **الحروب الالكترونية غير المتكافئة**

تكمن أهم نقاط الضعف لدى الدول النامية في الحروب الالكترونية انها غير متكافئة نتيجة عدم امتلاك تكنولوجيا خاصة بها، وتستوردها من آخرين، وهو الأمر مكمن الخطورة الذي يمنح مالك هذه التكنولوجيا صلاحية كبيرة على تخطيط وإنشاء وإدارة الشبكات ومراكز التحكم والصيانة، كما يمكن لمالك التكنولوجيا الوصول عبر نقاط الربط الرئيسية بالشبكة والتحكم في أجزائها، فضلا عن بعض أنظمة الحماية مصممة ها بعض الثغرات لتسهيل عمليات الاختراق.

والحقيقة انه باستخدام التكنولوجيا فى محاربة الإرهاب التي حفزت الابتكارات التكنولوجية في عدة اتجاهات، بدءاً من معالجة وتحليل البيانات بسرعات عالية جداً لم نكن نستطيع تخيلها قبل عقد من الزمان، مروراً بتصميم برامج مضمونة للتعرف على

الوجوه، انتهاء بتصميم ناطحات سحاب يمكنها أن تنجو من ذات مستوى التفجيرات التي أدت إلى إسقاط برجي التجارة العالميين أطول مباني العالم حينها.إليكم بعض الطرق التي ابتكرتها التكنولوجيا.

الخاتمة:

بعد استعراض الجوانب القانونية الدولية يمكن تحديد بعض الاستراتيجيات القانونية مكافحة للإرهاب الالكتروني نستنتج الاتى:

- ضرورة تحديد التعريف القانوني الدولي للهجمات الإرهابية الإلكترونية، تنظيم قواعد المسئولية الدولية من الدول والمنظمات والأفراد لردع للهجمات الالكترونية التي تشكل خطراً وانتهاكاً لسيادة الدول وتأثيرها على الأمن والسلم الدوليين
- ضرورة تنظيم مكافحة جرائم الكمبيوتر وحماية الحق في الخصوصية والقرصنة الالكترونية وضرورة اعتماد اتفاقيات في إطار القانون الدولى بشأن العقوبات على الهجوم بالأسلحة الالكترونية وما يتعلق بضرورة التعاون القضائي لضبط المجرمين الدوليين من الجماعات المنظمة والأفراد وغيرها.
- إدماج الفضاء الإلكتروني ضمن الأمن القومي للدول عبر تحديث الجيوش وتدشين وحدات متخصصة في الحروب الإلكترونية، وإقامة هيئات وطنية للأمن والدفاع الإلكتروني.
- إنشاء محكمة دولية للأمن الالكترونى للتعاون القضائي الجنائي الدولي والإبلاغ عن القضايا التي تؤثر على المستخدمين والشركات الدولية والمحلية لإنفاذ القواعد الدولية الالكترونية للإرهاب على الدول والمنظمات الإرهابية والأفراد.
- يجب أن تتطور المعايير القانونية الدولية ملاحقة الجرائم في الفضاء الالكترونى بحيث يمكن للشركات الخاصة في ظل حالات مشاركة سجلات

البريد الإلكتروني، GPS، أو غيرها من البيانات ذات الصلة إلى المقاضاة المحلية، يجب على المحققين استخدام معاهدة المساعدة القانونية المتبادلة (MLAT)لإجبار شركة مقرها في الخارج لتقديم الأدلة الرقمية الأساسية . MLATsمعروفة بآليات تستنفذ وقتا طويلا وشاقة، وليس مصممة لعالم متصل رقميا.

المراجع:

(i) - See, for example, the 2015 Report to the UN Secretary-General of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, at para. 6 (<http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174>) ; the section entitled "Countering radicalization conducive to terrorism and the use of internet for terrorist purposes" of the G20 Leaders' Statement on Countering Terrorism, July 2017; and the G7 Declaration on Responsible States Behavior in Cyberspace, April 2017. The United Nations Security Council has also passed several Chapter VII resolutions compelling states to implement counter-terrorist efforts. For a comprehensive listing, see the website of the Security Council Counter-Terrorism Committee (< https://www.un.org/sc/ctc/resources/security-council/resolutions/>).

(ii) - For instance, the use of cyber capabilities for communication with terrorist operatives is detailed in Rukmini Callimachi, "Not Lone Wolves After All: How ISIS Guides Worlds' Terror Plots from Afar" ", New York Times, February 24, 2017, https://www.nytimes.com/2017/02/04/world/asia/isis-messaging-app-terror-plot.html?mcubz=0&_r=0>.

(iii) - World Economic Forum, Understanding Systemic Cyber Risk, White Paper, October 2016, at p. 13.

(iv) - Should terrorists "…acquire attack tools, they could carry out disruptive ICT activities" (Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/68/98, June 24, 2013) and ""[t]he use of ICTs for . . . terrorist attacks against ICTs or ICT-dependent infrastructure, is an increasing possibility" (Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/70/174, July 22, 2015).

(v) - This international legal analysis of terrorism in cyberspace reveals a conundrum. Plausible options for international legal action concerning terrorist cyberattacks exist, but, because such attacks have not occurred, states lack incentives to strengthen proactively the contribution international law can make." (David Fidler, "Cyberspace, Terrorism and International Law", Journal of Conflict and Security Law, Vol. 21 (3), 2016, Pages 475–493).

(vi) - RELATED: Lockheed Martin The US Air Force has installed an F-22-F-35 fighter jet dedicated to Japan

(vii) - Dan Goodin, piracy commercial aircraft with Android application (some conditionsApplication), A Restishnika (April 11, 2103), http://arststechnica.com/security/2013/04/hacking-commercial-Aircraft-with-robot-application-some conditions-apply / (discuss the weaknesses of the protocol used toAnd send data to commercial aircraft.

(viii) - Related: Air Force Chief Scientists: F-35, F-22 For artificial intelligence and UAV control Related: confirms the Chief of Air Force scientists F-35 will include artificial intelligence.

(ix) - David E. Sanger et al., The Chinese Army Unit Seen as Linked to Piracy Against the United States, New YorkT Ems (18 February 2013), http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-

(x) - the Criminal Complaint for Case #1:15 -MJ-515, United States District Court for the Eastern District of Virginia, United States of America v. ArditFerizi, < https://www.justice.gov/opa/file/784501/download>. The three crimes with which Ferizi was charged were unauthorized access to a computer, aggravated identity theft, and providing material support to a designated foreign terrorist group.

(xi) - Nancy K. Hayden, "Innovation and Learning in Terrorist Organizations: Towards Adaptive Capacity and Resiliency", August 16, 2013, Conference Proceedings of the 31st International Conference of the System Dynamics Society,http://www.systemdynamics.org/conferences/2013/proceed/papers/P1407.pdf.

(xii) – فلابد من التميز بين الأعمال الموجهة ضد المدنيين الأبرياء وغير الأبرياء، حسبما ذهب إليه الكثير من الدارسين، وقد ذهب د.احمد أبو الوفا إلى أن استخدام الإرهاب أي كانت نوعيته يعتبر غير مشروع إذا استخدم ضد الأشخاص الأبرياء بغض النظر عن بواعثه، إلا أن يكون معاملة بالمثل أو ردا على اعتداء قائم؛ هيثم حسن، المرجع السابق، ص ٦٣٢.

(xiii) - Bruce Schneier, Understanding Threats in Cyberspace, S CHNEIER. COM (October،2013) https://www.schneier.com/blog/archives/2013/10/understanding_t_2.html

(xiv) - Jackson NyamoyaMogoto& Stephen Freeland, Space & Intelligence and The UniteCharter of the United Nations System of force: thick legal fog or fading haze, 41 International law.١١٠٤ (٢٠٠٧).

(xv) – د. حامد سلطان ود. عائشة راتب ود. صلاح الدين عامر، القانون الدولي العام، دار النهضة العربية،١٩٨٧، ط ٤، ص ٢٤٥.

(xvi) - A brief review of the 13 December issue of the Defense Dossier, published by the American Foreign Policy Council (AFPC), which includes the following articles:

-Kelley Sayler, Nanotechnology and US. Military power

(xvii) – حامد سلطان ود. عائشة راتب ود. صلاح الدين مرجع سابق ص ٢٤٦.

(xviii) – د.محمد سامي عبد الحميد، أصول القانون الدولي – القاعدة الدولية، مؤسسة الثقافة الجامعية، ١٩٨٠ ط٥، ص ١٦٧.

(xix) – د. محمد خلف، حق الدفاع الشرعي في القانون الدولي الجنائي: دراسة تأصيلية تحليلية مقارنة، الطبعة الثانية مطابع دار الحقيقة، بني غازي، ص٤٨٥–٤٩٧.

(xx) - David Fidler, Richard Pregent and Alex Vandurme, "NATO, Cyber Defense, and International Law. Journal of International and Comparative Law, 4 (1) 2013, p. 15.

(xxi) - بريطانيا وأمريكا تُحمّلان روسيا مسؤولية هجوم إلكتروني مدمر وقع ٢٠١٧ https://www.dw.com 2018/a-42609967

(xxii) -." (David Fidler, "Cyberspace, Terrorism and International Law", Journal of Conflict and Security Law, op.cit,P 475–493.

(xxiii) - World Economic Forum, Understanding Systemic Cyber Risk, White Paper, October 2016, at p. 13.

(xxiv) -.David Fidler, "Cyberspace, Terrorism and International Law", Journal of Conflict and Security Law, op.cit.

(xxv) - David Fidler, Richard Pregent. Journal of International and Comparative Law, 4 /1/ 2013, p.16.

(xxvi) - World Economic Forum, Understanding Systemic Cyber Risk, White Paper, October 2016, at p. 13.

(xxvii) - Nancy K. Hayden, "Innovation and Learning in Terrorist Organizations: Towards Adaptive Capacity and Resiliency, op.cit

(xxviii) Should terrorists "…acquire attack tools, they could carry out disruptive ICT activities" (Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/68/98, June 24, 2013) op.cit.

(xxix) - الولايات المتحدةxxixhttps://www.france24.com/ar/20171219 تحمل بيونغ يانغ "مسؤولية مباشرة" عن هجوم "وانا كراي" الإلكتروني.

(xxx) - Said Richard Steinon, founder of an IT company. Harvest in Birmingham, Michigan reports ZDNet.