المعهد القومى للملكية الفكرية
The National Institute of Intellectual Property
Helwan University, Egypt

المجلة العلمية للملكية الفكرية وإدارة الابتكار

دورية نصف سنوية محكمة يصدرها

المعهد القومي للملكية الفكرية

جامعة حلوان

العدد الثالث

يناير ٢٠٢٠

الهدف من المجلة:

تهدف المجلة العلمية للملكية الفكرية وإدارة الابتكار إلى نشر البحوث والدراسات النظرية والتطبيقية فى مجال الملكية الفكرية بشقيها الصناعي والأدبي والفني وعلاقتها بإدارة الابتكار والتنمية المستدامة من كافة النواحي القانونية والاقتصادية والادارية والعلمية والأدبية والفنية.

ضوابط عامة:

- تعبر كافة الدراسات والبحوث والمقالات عن رأى مؤلفيها ويأتي ترتيبها بالمجلة وفقا لإعتبارات فنية لا علاقة لها بالقيمة العلمية لأى منها.
- تنشر المقالات غير المحكمة (أوراق العمل) فى زاوية خاصة في المجلة.
- تنشر المجلة مراجعات وعروض الكتب الجديدة والدوريات.
- تنشر المجلة التقارير والبحوث والدراسات الملقاه في مؤتمرات ومنتديات علمية والنشاطات الأكاديمية في مجال تخصصها دونما تحكيم في أعداد خاصة من المجلة.
- يمكن الاقتباس من بعض مواد المجلة بشرط الاشارة إلى المصدر.
- تنشر المجلة الأوراق البحثية للطلاب المسجلين لدرجتى الماجستير والدكتوراه.
- تصدر المجلة محكمة ودورية نصف سنوية.

ألية النشر فى المجلة:

- تقبل المجلة كافة البحوث والدراسات التطبيقية والأكاديمية في مجال حقوق الملكية الفكرية بكافة جوانبها القانونية والتقنية والاقتصادية والادارية والاجتماعية والثقافية والفنية.
- تقبل البحوث باللغات (العربية والانجليزية والفرنسية).
- تنشر المجلة ملخصات الرسائل العلمية الجديدة، وتعامل معاملة أوراق العمل.
- يجب أن يلتزم الباحث بعدم إرسال بحثه إلى جهة أخرى حتى يأتيه رد المجلة.
- يجب أن يلتزم الباحث بإتباع الأسس العلمية السليمة في بحثه.
- يجب أن يرسل الباحث بحثه إلى المجلة من ثلاثة نسخ مطبوعة، وملخص باللغة العربية أو الانجليزية أو الفرنسية، فى حدود ٨ ـ ١٢ سطر، ويجب أن تكون الرسوم البيانية والإيضاحية مطبوعة وواضحة، بالإضافة إلى نسخة إلكترونية Soft Copy، ونوع الخط Romanes Times New ١٤ للعربى، و١٢ للانجليزي على B5 (ورق نصف ثمانيات) على البريد الالكتروني: ymgad@niip.edi.eg
- ترسل البحوث إلى محكمين متخصصين وتحكم بسرية تامة.
- في حالة قبول البحث للنشر، يلتزم الباحث بتعديله ليتناسب مع مقترحات المحكمين، وأسلوب النشر بالمجلة.

مجلس إدارة تحرير المجلة	
أ.د. ياسر محمد جاد الله محمود	أستاذ الاقتصاد والملكية الفكرية وعميد المعهد القومي للملكية الفكرية (بالتكليف) - رئيس تحرير المجلة
أ.د. أحمد عبد الكريم سلامة	أستاذ القانون الدولي الخاص بكلية الحقوق بجامعة حلوان والمستشار العلمي للمعهد سلطان عضو مجلس إدارة تحرير المجلة
أ.د. وكيل المعهد للدراسات العليا والبحوث	سكرتير تحرير المجلة
أ.د. جلال عبد الحميد عبد اللاه	أستاذ الهندسة الانشائية بكلية الهندسة بالمطرية بجامعة حلوان - عضو مجلس إدارة تحرير المجلة
أ.د. هناء محمد الحسيني	أستاذ علوم الأطعمة بكلية الاقتصاد المنزلي بجامعة حلوان - عضو مجلس إدارة تحرير المجلة
أ.د. وزير مفوض/ مها بخيت محمد زكي	مدير إدارة الملكية الفكرية والتنافسية بجامعة الدول العربية - عضو مجلس إدارة تحرير المجلة
اللواء أ.د. عبد القدوس عبد الرزاق العبيدلي	رئيس مجلس إدارة جمعية الامارات للملكية الفكرية - عضو مجلس إدارة تحرير المجلة
Prof Dr. Alexander Peukert	أستاذ القانون المدنى بجامعة جوته فرانكفورت أم ماين – ألمانيا - عضو مجلس إدارة تحرير المجلة
Prof Dr. Andrew Griffiths	أستاذ القانون التجارى بجامعة نيو كاسل - بريطانيا - عضو مجلس إدارة تحرير المجلة

المراسلات

ترسل البحوث إلى رئيس تحرير المجلة العلمية للملكية الفكرية وإدارة الابتكار بجامعة حلوان
جامعة حلوان - ٤ شارع كمال الدين صلاح - أمام السفارة الأمريكية بالقاهرة -جاردن سيتى
ص.ب: ١١٤٦١ جاردن سيتي
ت: ٠٢٥٤٨١٠٥٠ ٢٠٢ + محمول: ٢٠١٠٠٠٣٠٠٥٤٨ + ف: ٠٢٧٩٤٩٢٣٠ ٢٠٢ +
http://www.helwan.edu.eg/niip/
ymgad@niip.edu.eg

المواجهة القانونية لظاهرة الإرهاب السيبراني

باسم نبيل السيد محمد التركي

المواجهة القانونية لظاهرة الإرهاب السيبراني

باسم نبيل السيد محمد التركي

مقدمة وتقسيم:

يعد من نافلة القول الحديث عن اعتبار الجرائم السيبرانية من الجرائم المستحدثة. إذ هي منتشرة منذ نشأة مفهوم السيبرانية ذاته والوسائط الرقمي؛ إما كامتداد طبيعي للأنشطة الإجرامية في الواقع (كالسرقات التي تحدث في الواقع أو عبر الوسائط الرقمية) أو ما ارتبط مع نشأة السيبرانية من أوجه جديدة للتجريم(مثل سرقة الهويات الرقمية أو اختراق الشبكات وتعطيلها).

لكن مع تغير مفاهيم الجريمة الالكترونية وبزوغ الفكر الإرهابي في استخدام كل الإمكانيات الممكنة لتحقيق أغراضه كان الحديث حول كيفية مواجهة الإرهاب السيبراني؛ خاصة بين منكر له ومؤيد لاعتباره خطر داهم.

مع هذا النقاش يتطرق البحث القائم إلى محاولة وضع تصور لماهية الإرهاب السيبراني، ثم الانتقال إلى تجارب الفقه القانوني المقارن التي نلتمس فيها البحث عن الحلول التشريعية ومعالمها وتقيمها، بالإضافة إلى البحث في المعاهدات الدولية عن أجوبة للأسئلة المطروحة: هل من توصيف للمشكلة؟ وما هي الحلول الموجودة في القانون الدولي؟ وكيف كانت التجربة الوطنية للحل؟ وعلى الصعيد الدولي كيف يرى أفراد المجتمع الدولي المسألة؟ وما هي مساعيهم للقضاء على المشكلة؟

في ضوء ما سبق فإن البحث الحالي يقسم إلى ٣ مطالب رئيسية وهي:

المطلب الأول: ماهية الإرهاب السيبراني.
المطلب الثاني: الإرهاب السيبراني في القانون المقارن.
المطلب الثالث: الإرهاب السيبراني في المعاهدات والاتفاقيات الدولية

المطلب الأول

ماهية الإرهاب السيبراني

يتناول هذا المطلب الأفكار الأساسية التي تساعد على تكوين صورة واضحة حول فكرة الإرهاب السيبراني بداية من مفهومه ونطاقه وما يتشبه به من أفكار أخرى قد تختلط به والصعوبات المرتبطة بذلك من خلال النظر في الفقه المحلل للمسألة سواء المعترف بحقيقة وجود الإرهاب السيبراني أو من خالفهم الرأي واعتقد في عكس ذلك.

أولا: المقصود بالإرهاب السيبراني:

بداية فإن الفقه في مجموعه يشير إلى عدم وجود تعريف جامع مانع متفق عليه بشأن تعريف الإرهاب السيبراني[1] وبالتالي تقتصر هذه المسألة الفرعية على عرض التعريفات التي أعدتها الجهات المعنية والمراكز البحثية فيما يلي:

يعرف مركز واشنطن للدراسات الإستراتيجية والدولية الإرهاب السيبراني بأنه "استخدام أدوات شبكات الكمبيوتر لتعطيل البنية التحتية الحيوية مثل الطاقة والنقل والعمليات الحكومية أو لإكراه أو تخويف الحكومة أو المدنيين".[2]

يتضح من هذا التعريف أنه اتجاه موسع في التعريف –أقرب إلى مفهوم الهجمات الإلكترونية Cyber attack– قائم على عنصرين هما الأداة المستخدمة وهي شبكات الكمبيوتر وثانيهما وهو عنصر الهدف إما إحداث أضرار بالبنية التحتية مثل المرافق أو يكون الهدف إكراه أو تخويف الحكومة أو المدنيين.

أما مكتب التحقيقات الفيدرالية الأمريكي (FBI) فإن تعريفه للإرهاب السيبراني هو "هجوم متعمد من قبل عناصر غير وطنية أو

[1]) Wilson,Clay(2014),"Cyber threats to critical information infrastructure" in "cyber terrorism: understanding, Assessment, and Response" , Chen Thomas M. ,Jarvis Lee and Macdonald Staurt (Editors),Springer, New york, USA PP:123

[2] Lweis ,Jamis A(2002)"Assessing the risks of cyber terrorism, cyber war and other cyber threats", center for strategic and international studies ,Washington DC,USA, PP:1

عملاء سريين لدوافع سياسية يستهدف بيانات ومعلومات وأنظمة وبرامج الكمبيوتر يترتب عليه عنف ضد أهداف غير قتالية.[1]

يظهر من هذا التعريف أنه أكثر وضوحا من التعريف السباق بشأن الفاعل والأهداف وإن كان يختلف من حيث الأهداف، إذ يكفي أن تكون النتيجة عنف ضد أهداف غير مقاتلة، وكذلك استبعاد الإكراه والتخويف مع اعتبار النتيجة المتحققة هي عنف وليس ضرر. لكن يشوب هذا التعريف خلطه بين مفاهيم أخرى قريبة الصلة بالإرهاب السيبراني مثل الهجمات السيبرانية والحرب الإلكترونية ومصطلحات أخرى قريبة يتعرض لها البحث في موضع لاحق لكن يبدو أنه انتصر للفقه القائل بضرورة وجود الدافع السياسي كمعيار للإرهاب ذاته وبالتبعية للإرهاب السيبراني.

أخيرًا فإن مكتب الأمم المتحدة المعني بالمخدرات والجريمة رصد في تقريره أن المنظمات الإرهابية تستخدم الأدوات التكنولوجية وفي المقدمة منها السيبرانية لأغراض متعددة، منها: الدعاية وجمع المعلومات والتدريب وتنظيم الأنشطة غير المشروعة ونشر المعلومات بقصد التجنيد والتحريض ولأغراض خزن المعلومات وإرسالها ومهاجمة الشبكة الحاسوبية نفسها.[2]

ثانيا: نطاق الإرهاب السيبراني

إذا كانت التعاريف السابقة وهي محاولة لتحديد المقصود بالإرهاب السيبراني أجمعت على الاستخدام غير المشروع للأنظمة السيبرانية فهل بالتبع يفهم أن الإرهاب السيبراني هو مجرد مزيج بين الإرهاب والفضاء السيبراني؟

[1] Kittichaisaree,Kriangsak (2017)"Public international law of cyber space" Springer, Gewerbestrasse, Switzerland, PP:297

[2] المجلس الإقتصادي والإجتماعي, الأمم المتحدة (٢٠١١) تقرير خبراء الفريق الحكومي الدولي المفتوح العضوية عن الدراسة الشاملة لمشكلة الجريمة السيبرانية وتدابير التصدي لها من جانب الدول الأعضاء والمجتمع الدولي والقطاع الخاص، اتجاهات الجريمة على الصعيد العالمي والمسائل المستجدة وتدابير التصدي في مجال منع الجريمة والعدالة الجنائية فيينا النمسا ص ٢

لتحليل المسألة إلى عناصرها الأولية نحدد المقصود بالإرهاب ثم الفضاء السيبراني، لكن الإشكالية تكمن في عدم وجود تعريف متفق عليها من قبل الفقه لتحديد ما المقصود بالإرهاب ذاته فهو مصطلح نال قسطا كبيرا من الاختلاف الفقهي حوله وبالتبع الإرهاب السيبراني.[١]

بخصوص المقصود بالإرهاب فإنه لايوجد توافق دولي حول المقصود به[٢] لكن وثائق القضاء الدولي تمدنا بتعريف للإرهاب في زمن السلم "بأنه بناء على المعاهدات وقرارات الأمم المتحدة والممارسة التشريعية والقضائية للدول، ظهرت أدلة مقنعة على ظهور قاعدة عرفية في القانون الدولي بشأن الإرهاب في زمن السلم تشترط وجود العناصر التالية:١- النية (القصد) في الجريمة الضمنية ٢- القصد الخاص والمتمثل في نشر الخوف أو إكراه السلطات ٣- ارتكاب عمل جنائي ٤- كون العمل الجنائي عابر للحدود الوطنية."[٣]

إن تحديد مفهوم الإرهاب السيبراني اعتمادا على رصد الظاهرة لأصلها مع غياب اليقين حول توافق دولي على المصطلح لا يصلح أساسا لتحديد المصطلح الجديد، إنما يكون تفسيره من خلال التعرف على أركانه ما يدفع إلى تحديد مفهوم الفضاء السيبراني فيما يلي:

يميز الفقه بين الفضاء السيبراني والإنترنت[٤]، فالفضاء السيبراني مفهوم أوسع من الإنترنت الذي يشكل جزءً واحدا مع أجزاء أخرى تشكل مفهوم الفضاء السيبراني، فالفقه يرى أن الفضاء السيبراني يشمل: شبكات مفتوحة متعددة الوظائف وهي الإنترنت، بالإضافة إلى شبكات أخرى مغلقة محددة الوظائف مثل أنظمة المراقبة الجوية، وكل من الشبكات له أنظمة مختلفة متعددة.

---

[1]) W. Brunst, Phillip,(2009) Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet. In" A War on Terror?" Wade, Marianne and Maljević, Almir (editors) Springer, New York, USA

[٢] مكتب الأمم المتحدة للمخدرات والجريمة (٢٠١١) مداولات الاجتماع الأول لفريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية, فيينا, النمسا ص ٥

[٣] المحكمة الجنائية الخاصة بلبنان, إعداد "STL-11-01/I" الدعوي" مجموعة اجتهادات المحكمة الخاصة بلبنان : هولندا , بدون دار نشر ٢٠١١ ص ٣٣

[4] A.Yannakogeorgos,Panayotis (2014) "Rethinking the threat of cyber terrorism" in "cyber terrorism: understanding, Assessment, and Response",ibid. PP:44.

بناء على هذه التفرقة، فالإرهاب السيبراني قد يقع عبر الإنترنت أو غيره من الشبكات المفتوحة أو المغلقة، والنتيجة المترتبة على هذه التفرقة غاية في الأهمية، إذ يمكن أن تبرر الهجمات ضد الطيران المدني أو الملاحة العالمية البحرية أو غيرها باعتبارها من صور الإرهاب السيبراني.

إذن فالفقه محق في دعوته إلى ضرورة تبني تعريف مستقل للإرهاب السيبراني عن مجرد خلط لمفاهيم الإرهاب مع الفضاء السيبراني[1]، والتخلي عن اعتبار أن المفهوم الجديد هو محض دمج مفاهيم قديمة غير متفق على تحديدها من الأساس لتكوين مفهوم جديد من الصعوبة تعريفه إلا بعد دراسته بشكل واضح والوقوف على أركانه الجوهرية الخاصة.

ثالثا: تمييز الإرهاب السيبراني عما يشبهه من مصطلحات:

لتوضيح الماهية بشكل أفضل فإنه قد خصصت هذه المسألة الفرعية لتمييز الإرهاب السيبراني عما يتشابه معه من أفعال غير مشروعة أخرى عبر وسيط سيبراني أو رقمي؛ فيما يعرف باختفاء الحواجز بين المصطلحات[2].

(أ)الجريمة السيبرانية والإرهاب السيبراني:

تعتبر الجريمة السيبرانية هي المفهوم الأوسع والأعم لكافة أشكال الأعمال غير المشروعة التي تتم عبر الوسائل الرقمية، لكن ماذا يعنى مصطلح الجريمة السيبرانية تحديدًا؟

يطرح الفقه فكرة أن معيار تحول الجريمة إلى جريمة سيبرانية هو حوسبة الوسائل والأدوات المستخدمة لتقع جريمة من قبل جهاز كمبيوتر – أو ما يقوم مقامه مثل الهواتف الذكية– ضد جهاز كمبيوتر أخر مع مراعاة أن الجريمة السيبرانية قد تكون جريمة بكافة أركانها

[1]Pualus,Sachar, Pohlmann,Norbert, and Reimer,Helmut(2004)",Securing electronic business processes" ,Friedr,Wiesbaden, Germany, PP:32

[2] Jarvis,Lee ,Nouri,Lella and Whiting,Andrew(2014) "understanding, locating and constructing cyber terrorism" *in*" "cyber terrorism: understanding, Assessment, and Response" ,lbid.29

وقعت عبر وسيط رقمي، أو أنه تم استخدام وسيط رقمي فى أحد المراحل فقط مثل الاتفاق عبر الإنترنت على مكان وزمان اللقاء لشراء المواد المخدرة، أو أخيرًا أن الجريمة تقع كاملة لكن يكون للوسائل الرقمية فقط دور في إثباتها مثل اعتراف شخص لآخر عبر الرسائل الرقمية بارتكابه إحدى الجرائم.[1]

(ب)الهجمات السيبرانية والإرهاب السيبراني:

تدق المسألة وتأخذ منحى أكثر تعقيدا بشأن التفريق بين الهجمات السيبرانية والإرهاب السيبراني، فالمشكلة تكمن في أن مفهوم الهجمة السيبرانية شديد القرب من الإرهاب السيبراني بحيث ربما لا يفلح التمييز بينهم إلا بواسطة الرجوع إلى معيار آخر مكمل.

فيقصد بالهجمات السيبرانية Cyber attack "مجموعة من الأنشطة المضرة والخبيثة تتم عبر استخدام تكنولوجيا المعلومات والاتصالات."[2]

يظهر من هذا التعريف أن مفهوم الهجمات السيبرانية شديد الاتساع بحيث يشمل أى نشاط مضر يتم عبر وسيط رقمي أو سيبراني بحيث يتسع للإرهاب السيبراني أو غيره من الأنشطة غير المشروعة.

(ج)الحرب السيبرانية والإرهاب السيبراني:

يقصد بمصطلح الحرب السيبرانية وفقًا للجنة الدولية للصليب الأحمر "وسائل وأساليب الحرب التي تعتمد على وسائل وتكنولوجيا المعلومات وتستخدم في حالات النزاع المسلح، وتستخدم إما بشكل هجومي أو دفاعي".[3]

---

[1] Kävrestad, Joakim(2018) "Fundamentals of digital Forensic:Theory, methods, and real-life application" Springer,Cham, Switzerland PP 10:11

[2] Fox Jane,Sarah, (2016) "Flying challenges for the future: Aviation preparedness in the face of cyber-terrorism" Springer ,New York Published online PP:197 منشور عبر الموقع https://link.springer.com/content/pdf/10.1007/s12198-016-0174-1.pdf

تم زيارة الرابط بتاريخ ١١ يناير ٢٠٢٠

[3] https://casebook.icrc.org/glossary/cyber-warfare

تم زيارة الموقع بتاريخ ٧ يناير ٢٠٢٠

ويذهب بعض الفقه إلي أن معيار التفرقة بين الحرب السيبرانية والإرهاب السيبراني هو بحسب الفاعل، فإذا كان مفهوم الإرهاب يتم تحليله انطلاقًا من ألّا يوصف بالإرهاب إلا الجماعات غير الوطنية، بعكس الدول لا توصف بالإرهاب[1]، بل إن ما قد تقوم به الدول من هجمات إلكترونية يدخل تحت مفهوم الحرب السيبرانية.[2]

ويعرف الفقه هذه العمليات تحت مسمى Cyber operation، ويضرب لها مثال استخدام الإنترنت ووسائل التواصل الاجتماعي للتأثير على الأفراد والتلاعب بانفعالاتهم؛ بقصد دفع الأفراد إلى التحرك بشكل معين يؤدي بعد ذلك إلى وقوع أضرار مادية حتى بدون وجود حضور حقيقى من قبل المحرضين.[3]

رابعا: موقف الفقه من فكرة الإرهاب السيبراني

إن موقف الفقه المحلل للمسألة يشهد تباعد شديد بين الآراء، فالبون شاسع بين من يرى الإرهاب السيبراني حالة حقيقة ومن يرى فيه صورة لا أكثر من صور الإرهاب مع تجديد للأدوات وأخيرا فقه منكر للأمر برمته، ويفصل هذا فيما يلي:

أولا: الفقه المنكر لوجود الإرهاب السيبراني

يذهب هذا الرأي إلى أن الإرهاب السيبراني هو أسطورة، فالأدلة الملموسة على وجوده ضئيلة للغاية، بل يتطلب الأمر لإحداث أضرار خطيرة تكلفةً ماديةً عاليةً وتقنيات متقدمة، وأن مخاوفنا من الإرهاب

---

[1] Stohl,Michael" (2014) "Dr. Strangeweb: Or How They Stopped Worrying and Learned to Love Cyber War in" cyber terrorism: understanding, Assessment, and Response",lbid. PP:87.

[2] Ad Ariely,Gil, (2014) "Adaptive responses to cyber terrorism" *in* "cyber terrorism: understanding, Assessment, and Response", lbid. PP:186

[3]) A.Yannakogeorgos,Panayotis, ibid. P 57

يبدو أن هذه المسألة يعرفها فقهاء علم الإجرام تحت مسمي "جرائم التجمعات" ويقصد بها الفعل الإجرامي أو مجموعة الأفعال الإجرامية التي يرتكبها حشد من الأفراد المتجمعين سواء كان ذلك بصورة تلقائية أو بناء على طلب أو إيحاء من متزعمي التجمهر. ويفسر البعض مسلك هؤلاء الأفراد بتأثير الإيحاء الجماعي الذي يمارسه الجمهور عليهم أو بالنظر إلى أنه من قبيل الجريمة العاطفية. إلا إن الصورة السابقة التى ضربها الفقه تتميز باستخدام وسائل سيبرانية للتحريض دون تدخل حقيقي من قبل المحرضين

أنظر فى هذا المعني : عبدالمنعم, سليمان. أصول علم الإجرام والجزاء. الإسكندرية: دار المطبوعات الجامعية, ٢٠١٥. ص ٢٥٦

السيبرانى مبالغ فيها. فالحقيقة أن الإرهاب السيبراني هو مصطلح سياسي بالأساس يتم الترويج له لأغراض مادية.[١]

ثانيا: الفقه المعتبر للإرهاب السيبراني صورة متطورة للإرهاب

ينطلق هذا المذهب من أن مجرد استخدام الجماعات الإرهابية للأدوات السيبرانية لا يعنى في ذاته نشوء إرهاب من نوع مختلف، بل هو مشكلة قديمة في ثوب جديد، فالإرهاب ذاته يستخدم تقنية حديثة لتحقيق نفس الأغراض.[٢] إن مجرد استخدام مصلح سيبراني لا يرقى بذاته دليلا على أننا بصدد معضلة مختلفة عما نواجهه[٣] وإلا كيف تكون التفرقة لمجرد استخدام أدوات سيبرانية؟

وبالتالي إن الإجابة على هذا التساؤل تتطلب أن تكون المواجهة ضمن خطة شاملة لمكافحة الإرهاب، وليست إجراءات مخصوصة لمجابهة الإرهاب السيبراني.[٤]

ثالثا: الفقه المؤيد لمفهوم الإرهاب السيبراني

يبارك هذا الفقه مفهوم الإرهاب السيبراني ويعتبره تهديدا حقيقيا قائما صرحت الدول بإطلاق تحذيرات منه للعسكريين[٥] إما باستهدافهم أو الكشف عن مواقع وحداتهم بناء على معلومات يتم جمعها عن طريق تحليل بيانات هواتفهم الذكية. بل يذهب هذا الفقه أبعد من ذلك إلى حد اعتبار خطره يقارب خطر امتلاك أسلحة الدمار الشامل.[٦]

لكن الفقه المؤيد والداعم لهذه الفكرة يختلف فيما بينه بشأن وقوع الأفعال التي تسمح بإطلاق وصف الإرهاب السيبراني، وذلك فيما يلي: (أ) من يرى ضرورة أن يكون الفعل يرتب ضرر بما يكفي لإحداث حالة من

---

[1] R. McGuire, M(2014)," Putting the 'Cyber' into Cyberterrorism: Re-reading technological Risk in a Hyperconnected World" *in*"cyber terrorism: understanding Assessment, and Response",ibid. PP63

[2] Stohl,Michael ,lbid. P:88

[٣] Chen Thomas M. ,Jarvis Lee and Macdonald Staurt (2014) cyber terrorism: understanding, Assessment, and Response", ibid. PP:198

[4] Ad Ariely,Gil, lbid. PP:182

[5] R. McGuire, M, ibid. PP78

[6] Stohl,Michael, lbid. P:95

الخوف يمكن مقارنتها بالخوف الناتج من الإرهاب في العالم الحقيقى، وأن يكون هذا الفعل مرتكب لدوافع سياسية واقتصادية.[1]

(ب) من يفرق بين استخدام الأدوات السيبرانية أو الحاسوبية كسلاح أو هدف أو مجرد عامل مشارك: فإذا تم استخدام الأدوات السيبرانية كعامل مشارك لاستهداف جهات مادية فهو إرهاب تقليدى في شكل معلوماتي، أما حين تكون الأدوات السيبرانية سلاح وهدف في آن واحد فهو إرهاب معلوماتي محض Pure information terrorism، ويضرب لنا الفقه مثلا بهذا الإرهاب المعلوماتي المحض استخدام إحدى البرمجيات الخبيثة Trojan horse مثلا لاستهداف شبكة أنظمة معلومات عامة.[2]

(ج) الاتجاه الموسع للإرهاب السيبراني، وهو الاتجاه الذى يعرف الإرهاب السيبراني بأنه كل خلط بين الإرهاب وأي تقنية سيبرانية.[3]

يبدو أن الاتجاه فى تعريفه للمصطلح قد استخدم معيار موسع للمفهوم يعقد الأمور بشكل أكبر، فمفهوم الإرهاب ذاته لا يوجد اتفاق حول مدلوله، بل يعود إلي نقطة الصفر حول ضرورة إيجاد تعريف مستقل وجديد للمسألة بعيدا عن دمج تعريفين غير منضبطين–على أقل تقدير–لإنشاء تعريف جديد.

إن الجرائم الذكية تحتاج إلى تشريعات أكثر ذكاءً لمواجتها إزاء كل الإشكاليات السابقة يدفع البحث إلى تسليط الضوء على التشريعات الوطنية وكيف تعاملت مع المسألة من خلال المطلب القادم.

---

[1] Conway,Maura(2014) "Reality Check: Assessing the (Un)Likelihood of Cyberterrorism" in "cyber terrorism: understanding, Assessment, and Response" ,lbid. PP:105

[2] Jarvis,Lee, Nouri,Lella and Whiting,Andrew, lbid. P:28

[3] Jarvis,Lee, Nouri,Lella and Whiting,Andrew, lbid. P:32

المطلب الثاني

الإرهاب السيبراني في القانون المقارن

تنطلق كل محاولة وطنية من منظور فريد يعكس أولوياتها وطرقها في حل الإشكاليات السابقة؛ وبالتالى تختلف الرؤى التشريعية في حلولها. من خلال هذا المطلب يتم تسليط الضوء على التجربة البريطانية وتليها الرؤية الهندية فيما يلي:

الإرهاب السيبراني في القانون الإنجليزي :

يمكن فهم المقصود بالإرهاب السيبراني بطريق غير مباشر باستقراء صوره مما وردت في النصوص التشريعية، ويعتبر التشريع الرئيسي الذى يتلمس البحث منه التجربة الإنجليزية هو قانون الإرهاب سواء الصادر في عام ٢٠٠٠,٢٠٠٦ تحت اسم Terrorism Act وذلك فيما يلي:

أولا: أشكال الإرهاب السيبراني:

(أ) فيما ورد بقانون سنة ٢٠٠٠[1]:

١-كل إجراء أو تهديد باتخاذ إجراءات من شأنها أن تؤدي إلى التدخل بشكل جاد في نظام إلكتروني أو تعطيله.[2]

٢-الجرائم المتعلقة بالبيانات،وتشمل نطاق عريض من الأفعال المجرمة وهي: تجميع أو تسجيل أو حيازة بيانات أو وثائق لمحتوي يمكن أن يكون مفيد لشخص يخطط أو يرتكب نشاط إرهابي.

وتمتد هذه الطائفة أيضا لتشمل أفعال الاطلاع أو الولوج عبر الإنترنت إلى وثائق أو معلومات من هذا القبيل، مثل تحميلها عبر الإنترنت ويشمل مفهوم التسجيلات النسخ الإلكترونية أو الفوتوجرافية على حد سواء.

---

[1] UK. Terrorism Act 2000
منشور عبر بوابة تشريعات الانجليزية بالرابط
http://www.legislation.gov.uk/ukpga/2000/11/contents
تم الزيارة بتاريخ ١٦ يناير ٢٠٢٠

[2] المادة(E/٢/١) من قانون الإرهاب سنة ٢٠٠٠

لكن إزاء هذا التشدد التشريعي أعقبه القانون بأسباب تمكن الفرد من دفع الجريمة عنه إذا أثبت أن لديه عذر مقبول لأفعاله أو حيازته للوثائق أو التسجيلات، وجعل مثال هذه الأسباب أن يكون الفرد وقت ارتكابه للنشاط المجرَّم أو حيازته للتسجيلات لم يكن يعلم وليس لديه سبب معقول يجعله يعلم أن هذه الوثائق أو المعلومات يمكن أن يستخدمها شخص ما في نشاط إرهابي، أو أن يكون حيازته أو اطلاعه على هذه التسجيلات مرتبط بطبيعة عمله كالصحفيين أو كان ذلك لأغراض تعليمية وأكاديمية.[1]

٣-تداول وتجميع أو الشروع في تجميع معلومات تخص أفراد بالنظر إلى مركزهم: فقد جرم القانون هذه المحاولات إذا كانت ترتبط بشخص كان أو لا يزال عضوا في قوات صاحبة الجلالة أو أجهزة المخابرات أو رجال الشرطة،إذا كان ذلك يمكن أن يكون مفيدا لشخص يرتكب أو يخطط لارتكاب نشاط إرهابي؛ ما لم يكن ذلك بعذر مقبول.[2]

(ب) فيما ورد بقانون سنة ٢٠٠٦[3]:

يختلف القانون في نسخة عام ٢٠٠٦ بأنه جرَّم أشكال التداول أو النشر أو التواصل بخلاف قانون ٢٠٠٠، ويمكن تحديد العمليات المرتبطة بالإرهاب السيبراني فيما يلي:

١-تجريم نشر وبث المنشورات الإرهابية بشكل إلكتروني، ويقصد بالمنشور المقالات أوالتسجيلات بأي شكل سواء مقروءة أو مسموعة أو متاحة للاطلاع أو المشاهدة.[4]

٢-تجريم إصدار الأوامر والتعليمات أو التدريب على أي مهارات إذا كان الفرد يعلم وقت إصداره لها أو التدريب عليها أن

---

[1] المادة ٥٨ من قانون الإرهاب سنة ٢٠٠٠

[2] المادة A٥٨ من قانون الإرهاب سنة ٢٠٠٠

[3] UK. Terrorism Act 2006
منشور عبر بوابة التشريعات بالرابط http://www.legislation.gov.uk/ukpga/2006/11/contents
تم الزيارة بتاريخ ١٦ يناير ٢٠٢٠

[4] المادة(D,E /٢/٢) من قانون الارهاب ٢٠٠٦

المتلقي أو المتدرب سيستخدمها في ارتكاب أو التخطيط لعمل إرهابي، أو تساعده أو تساعد غيره فى ذلك.[1]

٣- بالطريق المقابل فقد جرَّم المشرع تلقي تعليمات أو تدريبات على أي مهارات إذا كان الفرد يقصد مِن تلقيه التدريب أو التوجيه استخدام ذلك في القيام أو التخطيط أو الشروع في عمل إرهابي أو مساعدة نفسه أو غيره فى ذلك.[2]

ويقصد بالمهارات في المفهوم السابق أي مهارة أو تقنية أو وسيلة يمكن باستخدامها أن تصلح في القيام أو التخطيط أو الشروع أو التحضير أو تسهيل أو الاتفاق بشأن عمل إرهابي.[3]

إذا كانت جريمة إصدار التوجيهات أو التدريب أو تلقي الأوامر أو التدريب لم ينص المشرع على وقوعها بشكل إلكتروني أو سيبراني، لكن ذلك لا ينفي أن تكون مشمولة ضمنا فيه، خاصة مع استخدام المنظمات الإرهابية للأدوات السيبرانية الذى أصبح حقيقة واقعية[4] في التوجيه والتدريب ونشر الطرق المختلفة لصناعات المتفجرات وغيرها.

ثانيا: تحليل منهج القانون الإنجليزي:

إن قراءة مجموع النصوص السابقة يشير إلى أن المشرع الإنجليزي جرَّم الإرهاب السيبراني في شكلين: أولهما هو استخدام الفضاء السيبراني في تحقيق ضرر مباشر، وهو النص المتعلق بالتدخل أو تعطيل نظام إلكتروني، وثانيهما هو استخدام الإنترنت أو الوسائل الرقمية كوسيلة مساعدة في النشاط الإرهابي، وتتجلي فى تجريم تجميع المعلومات أو الوثائق أو إتاحتها أو توجيه الأفراد أو تدريبهم، وغير ذلك من باقى الأنشطة المجرمة التي ذكرها المشرع.

[1] المادة (١/٦) من قانون الارهاب ٢٠٠٦
[2] المادة (٢/٦) من قانون الارهاب ٢٠٠٦
[3] المادة (٣/٦) من قانون الارهاب ٢٠٠٦

[4] Wilson,Clay, ibid. P 132

كانت النتيجة المترتبة على ذلك التوسع في تجريم الأفعال التحضيرية[1] فمجرد تجميع المعلومات أو الوثائق فعل مجرم.

إن التشريع الإنجليزي في محاولته لتضيق الخناق على الأفعال الإرهابية قد وسع من مفهوم الفاعل، إذ يكفي أن تكون الوثائق أو المعلومات أو التسجيلات التي تم تجميعها يمكن أن يستخدمها شخص آخر في القيام أو التحضير لفعل إرهابي.

كان موقف مجلس اللوردات أكثر تشددا أمام النص السابق، فقد اكتفي بأن يتوافر ركن مادي ومعنوي لقيام الجريمة، أما المادي أن تكون المعلومات مفيدة لشخص يخطط أويقوم بعمل إرهابي وتكون المعلومات بطبيعتها تدل على ذلك مثل معلومات تخص صناعة المتفجرات، أما الركن المعنوي فلابد للفرد أن يعلم حيازته أو امتلاكه للمعلومات أو الوثائق وأن يكون على علم بطبيعة المضمون، ويكفي ذلك لقيام الجريمة ولو لم تتوافر لديه قصد خاص أي نية إرهابية.[2]

كذلك يُظهِر منهج القانون الإنجليزي الاعتداد بالركن المعنوي بشكل كبير، في كل مرة يكفي أن تكون لدى الفرد إما معرفة بأن ما يجمعه من تسجيلات يمكن أن تكون مفيدة لشخص آخر .وفي جرائم إصدار الأوامر والتدريبات وتلقيها يكون مُصدِر الأوامر على علم بأن متلقي الأوامر يستخدمها لغرض إرهابي أو تسهيل ذلك، وبالمثل في تلقي الأوامر تكون نية الفرد أن يستخدم الأوامر أو التدريبات في غرض إرهابي.

أخيرًا يبدو أن المشرع الإنجليزي قد انتهج مبدأ معاكسا لقرينة البراءة، مفاده نقل عبء الإثبات من المدعي إلى المتهم؛ فلكي يدفع عن نفسه الجريمة عليه هو أن يثبت أن ما جمعه من معلومات أو وثائق أو تسجيلات كان لعذر مقبول وليس لديه دافع يُعتقد في إمكان استخدامها من فرد آخر لغرض إرهابي.

[1] Carlile Lord and Macdonald Stuart(2014) in "cyber terrorism: understanding, Assessment, and Response" lbid PP:163
[2] Carlile Lord and Macdonald Stuart, lbid. P:164

ثانيا: الإرهاب السيبراني فى القانون الهندي

يجرم التشريع الهندي الإرهاب السيبراني بالاسم[1] إذ خصص له مادة مستقلة في قانون تكنولوجيا المعلومات Information technology Act لسنة ٢٠٠٠[2] تحت اسم عقاب الإرهاب السيبراني وتناقش الفقرات التالية أحكامه فيما يلى:

أولا: جرائم الإرهاب السيبراني في التشريع الهندي:[3]

يمكن تقسيم جرائم الإرهاب السيبراني -تجاوزًا- إلى جرائم ترتكب ضد أمن الدولة من جهة الداخل وجرائم ضد أمن الدولة من جهة الخارج وهي على ما يلي:

١-الإرهاب ضد أمن الدولة من جهة الداخل، ينص القانون علي عقاب كل شخص يحاول اختراق أو الوصول إلى مصادر حاسوبية دون إذن، أو تجاوز الإذن المسموح له بالوصول، أو يتسبب أو يُدخِل برامج حاسوبية مضرة؛ ويترتب علي ذلك أو يحتمل أن يسبب ذلك وفاة أو إصابة أشخاص أو إلحاق الضرر أو تدمير الممتلكات أو تعطيلها، أو يمكن أن يسبب سلوكه ضررا أو تعطيلا للإمدادات أو الخدمات الضرورية لحياة المجتمع أو يؤثر سلبا علي البنية التحتية المعلوماتية، إذا كان ذلك بقصد تهديد وحدة أو استقلال أو سلامة وسيادة البلاد أو نشر الإرهاب في الشعب أو في طائفة منه.

٢-الإرهاب ضد أمن الدولة من جهة الخارج، وهذه الطائفة يمكن تقسيمها إلي فئتين: الفئة الأولي هي الاختراق العمدي أو الوصول إلى مصادر حاسوبية مقيدة دون إذن، أو تجاوز الإذن

---

[1] Kittichaisaree,Kriangsak, ibid. p324

[2] India. Information technology Act 2000
منشور عبر بوابة التشريعات الهندية بالرابط
https://www.indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf
تم الزيارة بتاريخ ٩ يناير ٢٠٢٠

[3] المادة (١/٦٦F) من قانون تكنولوجيا المعلومات لسنة ٢٠٠٠

المسموح للحصول علي معلومات أو بيانات مقيدة لأسباب تتعلق بأمن الدولة أو العلاقات الخارجية.

أما الفئة الثانية فتشمل الاختراق العمدي أو الوصول إلى بيانات أو معلومات أو قواعد بيانات مقيدة، أو تجاوز الإذن المسموح مع وجوب الاعتقاد بأن الحصول عليها يسبب أو يمكن أن يسبب ضررا لسيادة البلاد أو سلامتها أو أمن البلاد أو العلاقات الودية مع الدول الأجنبية أو النظام العام أو الآداب العامة أو ما يرتبط بانتهاك حرمة المحاكم أو التشهير أو التحريض على جريمة، أو لصالح دولة أجنبية أو مجموعة من الأفراد أو غير ذلك.

ثانيا: تحليل منهج القانون الهندي

أولا: يقيم القانون كل الجرائم على ركنين: مادي ومعنوي، لكن الملاحظ بالنسبة للركن المادي يستوي أن يرتب النتيجة أو إمكان إحداثه لها، أما الركن المعنوي فيشمل القصد العام العمدي في جريمة الوصول إلى بيانات مقيدة لأسباب تتعلق بأمن الدولة، ويضاف إلى القصد العام القصد الخاص فى جريمة الإضرار بأمن الدولة من جهة الداخل، فيكون القصد الخاص تهديد وحدة وسلامة واستقلال وسيادة البلاد أو نشر الإرهاب، أما الجريمة الثالثة فيكفي الاعتقاد بأن ما تم الحصول عليه من بيانات يمكن استخدامه أو تسببه في النتيجة المذكورة.

ثانيا: يسوي القانون بين الوصول غير المشروع سواء كان كليًا بطريق غير مشروع أو بتجاوز الحد المسموح به للوصول؛ أي إنه يكفي أن يتم الوصول إلى قواعد بيانات أو معلومات مقيدة الوصول لتقع الجريمة.

ثالثا: يمكن ملاحظة أن المشرع قد انتهج ما يطلق عليه الفقه "جرائم القالب الحر"[1] إذ إنه يقنع بتجريم كل سلوك من شأنه أن يؤدي

[1] عبدالمنعم, سليمان.(٢٠١٤) النظرية العامة لقانون العقوبات. الإسكندرية: دار المطبوعات الجامعية, ص ٤٠٠.

إلى النتيجة المحظورة دون أن يبين على وجه الدقة مظاهر هذا السلوك، فمثلا يكتفي أن تقع الجريمة بالدخول إلى قواعد بيانات مقيدة دون تحديد الطرق، أو تكون النتيجة تهديدا لأمن وسلامة البلاد أو النظام العام إلى آخر ما ذكره المشرع من سلوكيات محظورة.

المطلب الثالث

الإرهاب السيبراني في المعاهدات والاتفاقيات الدولية

يناقش المطلب في الفقرات التالية مدى حرص المجتمع الدولي على مواجهة الإرهاب السيبراني من خلال الاتفاقيات والمعاهدات الدولية، خاصة أنه يشكل خطرا عالميا؛ فإذا كانت التشريعات الوطنية تعكس رؤية داخلية للحل فهل من منظور دولي للمشكلة أو حلها؟

بدايةً فإن المعاهدات والاتفاقات الدولية أكدت على حظر إرهاب المدنيين، فالبروتوكول الإضافي الثاني لاتفاقية جينيف ١٩٤٩ والخاص بحماية ضحايا المنازعات المسلحة غير الدولية نص في الفقرة ٢/١٣ على ضرورة حماية السكان والمدنيين من أن يكونوا محل لهجوم أو عنف أو التهديدات المقصود منها نشر الإرهاب بينهم.[١] لكن تظل الإشكالية محل البحث هي مدى وجود قواعد خاصة في الاتفاقات والمعاهدات الدولية تحمي الأفراد أو الممتلكات أو الأموال من خطر الإرهاب السيبراني الذي يكون محل البحث في الفقرات الآتية.

يعتنق بعض الفقه مذهبا مفاده أن بعض الاتفاقيات الدولية أثبت فاعلية في مواجهة الحرب السيبرانية أو المعلوماتية، لكن تبقى معضلة عدم إمكان تطبيقها بصدد الجرائم الإلكترونية أو الإرهاب السيبراني أو المعلوماتي.[٢]

---

[1] https://ihl-databases.icrc.org/ihl/WebART/475-760019
تم زيارة الموقع بتاريخ ٧ يناير ٢٠٢٠

[2] W.Aldrich, Richard,(2000),Cyberterrorism and Computer Crimes:Issues Surrounding the Establishment of an international regime, Information operation series, INSS Occasional ,32, Institute for national security studies, Colorado, USA,pp59

أولا: الإرهاب السيبراني في اتفاقية جامعة الدول العربية لمكافحة جرائم تقنية المعلومات:

حررت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في القاهرة بتاريخ ٢٠١٠/١٢/٢١ ودخلت حيز النفاذ بتاريخ ٢٠١٤/٢/٧، وقد وقعت عليها كافة الدول العربية فيما عدا جمهورية جيبوتي, وجمهورية الصومال وجمهورية القمر المتحدة والجمهورية اللبنانية[١]، وقد صدقت مصر عليها بتاريخ ٢٠١٤/٩/٨[٢].

أما عن أحكامها المتعلقة بالإرهاب السيبراني فإنها تنص على التزام كل دولة طرف بتجريم الأفعال المبينة فيها، وفقًا لتشريعاتها وأنظمتها الداخلية. وما يرصده البحث هو الإرهاب السيبراني فإن المادة ١٥ نصت على تجريم الجرائم المتعلقة بالإرهاب المرتكب بواسطة تقنية المعلومات،وشملت ٤ بنود فرعية (أ) نشر أفكار ومبادئ جماعات إرهابية والدعوة لها. (ب) تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية. (ج) نشر طرق صناعة المتفجرات والتي تستخدم خاصة في عمليات إرهابية. (د) نشر النعرات والفتن والاعتداء على الأديان والمعتقدات.

والتزامًا من مصر بتنفيذ تعهداتها الدولية، فإنها حسنًا فعلت حين صدر قانونا مكافحة الإرهاب رقم ٩٤ لسنة٢٠١٥ ومكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨، إذ تغطي نصوصهما مجتمعة كافة الجرائم التي جاءت بها نصوص الاتفاقية، مع مراعاة أن

---

١ http://www.lasportal.org/ar/legalnetwork/Documents/%D8%A7%D9%84%D8%AA%D8%B5%D8%AF%D9%8A%D9%82%20%D8%B9%D9%84%D9%89%20%D8%A7%D9%84%D8%A7%D8%AA%D9%81%D8%A7%D9%82%D9%8A%D9%87%20%D8%A7%D9%84%D8%B9%D8%B1%D8%A8%D9%8A%D8%A9%20%D9%84%D9%85%D9%83%D8%A7%D9%81%D8%AD%D8%A9%20%D8%AC%D8%B1%D8%A7%D8%A6%D9%85%20%D8%AA%D9%82%D9%86%D9%8A%D8%A9%20%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA.pdf

تم زيارة الرابط بتاريخ ٣ فبراير ٢٠٢٠

٢ جمهورية مصر العربية. قرار رئيس الجمهورية بشأن الموافقة علي إنضمام جمهورية مصر العربية الي الاتفاقية العربية لمكافحة جرائم تقنية المعلومات رقم (٢٧٦) لسنة٢٠١٤. (الجريدة الرسمية : العدد ٤٦. بتاريخ ٢٠١٤/١١/١٣)

بعض ما جاء يعتبر بالنسبة للقانون المصري من جائم تقنية المعلومات وليس الإرهاب السيبراني، وكذلك فإن نشر النعرات والفتن والاعتداء على الأديان والمعتقدات مجرم وفقًا لقانون العقوبات المصري.

لكن يبقي الإشارة إلى أن الاتفاقية تشير إلى تطبيق أحكامها على الجرائم بهدف منعها والتحقيق فيها وملاحقة مرتكبيها في حال تناثر أركان الجريمة بين أكثر من دولة طرف؛ سواء التخطيط أو التحريض والإشراف أو التنفيذ أو كان الفاعل جماعة منظمة تمارس أنشطتها من دولة أخري أو كانت الجريمة ترتب آثارا شديدة في دول أخرى، وبالتالي يبقي أن يتم تفعيل آليات التعاون القضائي الدولي بين الأعضاء.

ثانيا: حماية الطيران المدني من الإرهاب السيبراني:

يعتبر بروتوكول بكين الموقع في عام ٢٠١٠ أوضح صور المعاهدات والوثائق الدولية التي تعمل على حماية الطيران المدني من خطر الإرهاب السيبراني، وهو البروتوكول المكمل لاتفاقية"قمع الاستيلاء غير المشروع على الطائرات"الموقعة في لاهاي بتاريخ ديسمبر ١٩٧٠، وبالرغم من وضوح النص فيه إلا إنه لم يدخل حيز النفاذ حتى الآن.[١]

بخصوص أحكام البروتوكول فيما يخص الإرهاب السيبراني فقد نصت الفقرة الأولى منه على تعديل أحكام اتفاقية لاهاي المذكورة ليصبح النص كما يلي"يعد مرتكبًا لجريمة أي شخص يقوم عمدًا بالاستيلاء غير المشروع على طائرة، أو ممارسة السيطرة غير المشروعة على طائرة في الخدمة باستخدام القوة أو التهديد،أو بالإرغام، أو بأي شكل آخر من أشكال الترهيب، أو بأي وسيلة تكنولوجية."[٢]

[1] Kittichaisaree,Kriangsak , ibid. P: 307

[٢] النسخة العربية من البروتوكول متاحة عبر بوابة معاهدات الأمم المتحدة https://treaties.un.org/doc/Publication/UNTS/No%20Volume/12325/A-12325-0800000280507cc5.pdf
تم زيارة الرابط بتاريخ ٨ فبراير ٢٠٢٠

جليًا يجرم النص استخدام أي وسيلة تكنولوجية تفضي إلى النتائج المحظورة، وكذلك حظر النص بالفقرة التالية التهديد أو الشروع في ارتكاب الأفعال السابقة.

يفهم من النص السابق أنه أدخل مفهوم أي وسيلة تكنولوجية للاعتبارات الواقعية المرتبطة بصناعة الطائرات وتوجيهها خطورة العوامل التكنولوجية والسيبرانية في التأثير على الطائرات وأنظمة الملاحة؛ وبذلك يمثل نقلة نوعية عن المواثيق التي سبقته في حماية الطيران المدني.

إذا كان المطلب لم يتعرض سوى للاتفاقية العربية لمكافحة جرائم تقنية المعلومات وبروتوكول بكين المضاف لاتفاقية لاهاي بشأن قمع الإستيلاء غير المشروع علي الطائرات فإن ذلك ما أملته طبيعة الدراسة ذاتها؛ فالفضاء السيبراني موضوع مستحدث ربما لم تتشكل معالمه حتى الآن، فالفقه يشير إلى أن الفضاء السيبراني لا يزال غير محكوم، بل حتى الآن يخرج عن سيطرة الدول.[1] وبالتالي يكون البحث في المعاهدات الدولية عن أحكام تخص موضوع مؤرق للعالم(الإرهاب) وإضافته للبعد السيبراني مسألة معقدة للحد الذي لم تنظر إليها الدول بشكل مجمع للخروج بوضع تصور لمواجهتها.

خاتمة:

حاول البحث تسليط الضوء على خطر هجين(الإرهاب السيبراني) من خلال المحاور الثلاثة: مفهومه،والمواجهة التشريعية الوطنية، والمعاهدات والمواثيق الدولية.

لكن المسألة الكامنة وراء البحث ليست في مواجهة التحديات الحديثة، أنما في علاقة القانون ذاته بالتكنولوجيا الحديثة في ضوء تعقد العلاقات. فالآن لم تقتصر العلاقات الإنسانية بين الأفراد وبعضهم فحسب، فتخطتها إلى علاقة الإنسان بالآلات الذكية والحديثة، تذهب المسألة إلى ما وراء ذلك إلي علاقات الأجهزة الذكية

[1] Hoisington, Matthew (2017)" Regulating Cyber Operations Through International Law: In, Out or Against the Box?" *in* "Ethics and Policies for Cyber operations ",Taddeo, Mariarosaria and Glorioso, Ludovica(editors) Springer Switzerland, pp:94

والروبوتات والذكاء الصناعي ببعضها؛ وهو ما دفع الفقه الغربي إلى محاولة رسم تصورات ليست لتدخل القانون في التنظيم، بل في تأثر القانون ذاته بالتطورات العلمية الحديثة.

إذا كانت الجرائم الذكية تحتاج إلى تشريعات أكثر ذكاءً لمواجهتها؛ فإن ذكاء التشريعات لا يكون إلا بملاحقة التطورات الحديثة. فإذا كانت الإشكاليات مرتبطة بالفضاء السيبراني فالقانون ذاته بحاجة إلى استخدام أدوات الفضاء السيبراني ليتمكن القانون من التعامل مع المعطيات بنفس الأدوات الملائمة، فلا شك أن كل ذلك يحتاج إلى أدوات خاصة.

إن خطر الإرهاب السيبراني لا يمكن دراسته بمعزل عن فهم محيطه (الفضاء السيبراني ذاته) ورصد مشاكله التي يختلط فيها كل شيء. وقد نوهت الدراسة عن الهجمات الإلكترونية والجرائم السيبرانية لكن ما لم يُرصد خطره أكبر، فتشير الدراسات في مجال الفضاء السيبراني إلى مسائل أخرى أكثر تعقيدًا مثل: التجسس الإلكتروني، وحماية الخصوصية، ومشاكل يسميها الفقه بالتلوث الرقمي،وعلاقة القانون والذكاء الصناعي والروبوتات والرقمنة وحماية البيانات، وغير ذلك من مسائل دقيقة تحتاج إلى دراسات خاصة.

المراجع

أولا: المراجع العربية

(أ)الكتب

عبدالمنعم, سليمان(٢٠١٥). أصول علم الإجرام والجزاء. الإسكندرية: دار المطبوعات الجامعية.

عبدالمنعم, سليمان(٢٠١٤) النظرية العامة لقانون العقوبات. الإسكندرية: دار المطبوعات الجامعية.

ثانيا:المراجع الأجنبية

(أ)الكتب

Chen Thomas, M.,Jarvis Lee and Macdonald Staurt (Editors) (2014) "cyber terrorism: understanding, Assessment, and Response ",Springer, New york, USA.

Glorioso, Ludovica and ",Taddeo, Mariarosaria (editors) (2017) "Ethics and Policies for Cyber operations" Springer Switzerland.

Kävrestad, Joakim (2018) "Fundamentals of digital Forensic :Theory, methods, and real-life application" Springer,Cham, Switzerland.

Kittichaisaree,Kriangsak (2017)"Public international law of cyber space" Springer, Gewerbestrasse, Switzerland.

Pualus,Sachar, Pohlmann,Norbert, and Reimer,Helmut(2004)",Securing electronic business processes" ,Friedr,Wiesbaden, Germany.

Wade, Marianne and Maljević, Almir (editors) (2009)" A War on Terror?" Springer, New york, USA.

(ب)المقالات

Fox Jane,Sarah, (2016) "Flying challenges for the future: Aviation preparedness in the face of cyber-terrorism" Springer ,New York Published online.