الإرهاب السيبراني وتحدّيات الدُول
دراسة مقارنة مع الاتفاقيات الدولية

Cyber terrorism and the challenges of States Comparative study with international conventions

العشعاش إسحاق: طالب دكتوراه
كلية الحقوق جامعة الجزائر 1

الملخص

تهدف هذه الورقة البحثية الى معالجة أكثر المواضيع إثارة للاهتمام في الوقت الراهن، وتشمل أساساً الاجرام السيبراني (الالكتروني) في احدى اشكاله وهو الإرهاب السيبراني الذي يشكّل خطرًا جسيما وعائقا امام عصرنة الدُول في ظلّ توجّه مضطرد نحو حكومات الكترونية ورقمية، اذ سنحاول الإجابة على اهم النقاط الأساسية ذات الصلة بهذا المفهوم من خلال إزالة بعض الغموض حول تلك المصطلحات القانونية الجديدة، او تلك الوسائل المُستعملة في أي اعتداء إرهابي يطال أنظمة الدول الحيوية او تلك التي تشكّل خطرًا أيديولوجيا لا يكفي مجابهتها بوسائل تقنية، من خلال صورة نمطية عن الواقع الدولي (نموذج الدولة الإسلامية في العراق والشام)،وأخيرا ضرورة معرفة اشكال المُواجهة على الصعيد الوطني (الجزائر) بصفة خاصة والدولي بصفة عامة.

الكلمات المفتاحية

الإرهاب الإلكتروني. الفضاء السيبراني. المقاربة الجزائرية لمكافحة الإرهاب.

Abstract

The purpose of this research is to study the most controversial issues at the moment, cybercrime (CYBER SECURITY) in one of its forms is cyber terrorism, which poses a serious threat to the development of modern means, with an accelerating trend toward digital governments. This research has also for objective, to Answer the most important points related to this new concept, or means used in any terrorist attack affecting the vital systems of States, Through some cases of international reality (The model of the Islamic state in Iraq and Sham). Finally, it is necessary to know the Forms of confrontation at the national (Algeria), and international levels in general.

Key word

Cyber Terrorism. Cyberspace. The Algerian approach to fight against terroris.

المقدمة

إلى غاية اليوم، لم يحصل بعدُ أي اتفاق دولي بخصوص وضع تعريف جامع ومانع لظاهرة الإرهاب سواء الداخلي منه أو ذو الطابع الدولي، بل وان الاتفاق ذاته لم يحصل بعدُ في تفنيدِ أبعاد هذه الظاهرة وتحديد خصائصها، بالرغم من أنها أخذت أبعادًا خطيرة ومُقلقة ترتقي إلى ذروة ضارية من العنف والترهيب عن طريق الهجمات الموسعة فالعالم اليوم يشهد بلا شكّ تطوّرا هائلا في وسائط الاتصال وتقنيات المعلومات حتى أصبح يُطلق عليه "عصر الثورة المعلوماتية" التي شملت مُعظم جوانب حياة البشر، وصارت أشبه بما تكون حربًا تكنولوجية متعدّدة والاستخدامات في ظل الحديث عن حروب من نوع آخر تُستخدم فيها تلك الوسائط على نحو لم يسبق له مثيل، وهو الأمر ذاته بالنسبة للجماعات الإرهابية أيًّ كانت غاياتها ودوافعها فهي لم تعُد تعتمد فقط على الأساليب التقليدية في القتال والهجوم والترويع والتحريض، بل صارت تلجأ إلى أساليب أكثر حداثة لا تحدّها حدود إقليمية ولا تأخذ بالمكان والزمان قيدًا أو عائقا وخير دليل على ذلك هو الاعتماد المتزايد من قبل الجماعات الإرهـــابية على استخـــدام الفضاء السيبـــراني كمنصة انطـــلاق لتنفيذ أعمالها غير المشروعة.

لذلك برز مصطلح الإرهاب الإلكتروني Cyber Terrorism (الإرهاب الرقمي، السيبراني) وشاع استخدامه بالموازاة مع زيادة خطورة تلك الجرائم وتعقيدها، سواء من حيث سهولة الاتصال بين الجماعات الإرهابية وانسياب التنسيق

بينها ، او من خلال ابتكار أساليب وطرق إجرامية متقدمة تعتمد في الأساس على هذا الفضاء الواسع نظر لغياب حدود فاصلة بين الدول، في ظل تطوّر مفهوم الحروب وظهور الجيل الرابع منها أين لم تعد الأسلحة التقليدية كافية لوحدها لإخضاع الطرف المستهدف سواء كانت دولا او أفراد، فالتحريض والحرب الفكرية وتسليط ظروف قاهرة أصبحت وسائل وبل أسلحة العصر التي تعتمدها الدول على غرار الجماعات الإرهابية ذاتها.

في ظل هذه الظروف أصبح تواجد الإرهاب في الشبكة العالمية مكثفًا، بحيث تزايدت المواقع التي تديرها جماعات إرهابية من 12 موقع سنة 1996 إلى 4800 موقع في الوقت الحالي[1] دون ذكر مواقع التواصل الاجتماعي التي تعرف تسيّبًا كبيرًا، كما أن الشبكات الموازية أو ما تُعرف بالأنترنت المظلم Dark Net او الانترنت العميق Deep Web والذي يتميز بانعدام الرقابة فيه، يعرف هو الآخر حضورا قويا لتلك الجماعات الإرهابية وأخرى تابعة لأفراد الجريمة المنظمة العابرة للحدود الوطنية أو ما أصبح يُعرف بالجريمة المنظمة الإلكترونية.

ولما كانت الظاهرة الإرهابية بصفة عامة تستفيد أكثر فأكثر مما توصلت إليه المعرفة البشرية والتراكمات العلمية بفعل الثورة المعلوماتية والتكنلوجية الهائلة، أصبح العنف والإرهاب بدوه "مُعولماً" ولم يعد حكرًا على جماعات أو أفراد أو دولا، وعليه تبقى الحاجة مُلحة إلى وسائل عقلانية وفعالة من اجل مكافحة هذه الآلة الشرسة والعنيفة ولاتي لا تستثني أحدا، فالقوانين الداخلية للدول لم تعُد وحدها قادرة على مجابهة وكبح آلة العنف هذه. ومن هنا تبرز الوسائل التعاونية بين الدول والتكتلات الأمنية إقليميا أو عالميا، كما أن مجابهة هذا الإجرام قد يؤثر بصفة مباشرة على الحريات الأساسية للأفراد وهذا عن طريق التعسّف أو التطبيق غير الملائم لوسائل المكافحة من طرف سلطات الدول وأجهزتها الأمنية.

والحقيقة أن هذه الدراسة تثير الكثير من الإشكالات القانونية والتقنية التي سنحاول من خلالها معالجة بعضها انطلاقا من منظور القانون الدولي والوطني، بحيث سنحاول تسليط الضوء على مثال الإرهاب الدولي المتمثّل أساسًا بما يقوم به تنظيم "الدولة الإسلامية في العراق والشام" أو ما اصْطُلح عليه بـ"داعش"، وستتناول الدراسة بالتحديد المسائل الجوهرية المتعلقة بالمفاهيم والمصطلحات، ووسائل الإرهاب السيبراني وأخير أشكال المُواجهة على الصعيد الدولي والوطني من خلال المقاربة الجزائرية لمكافحة الإرهاب بصفة خاصة، كما يلي:

المبحث الاوّل: خصوصية مفهوم الإرهاب السيبراني وتعقيد أساليب استخدامه.

المبحث الثاني: أشكال مواجهة الإرهاب السيبراني واشكالية حقوق الانسان.

المبحث الأول: خصوصية مفهوم الإرهاب السيبراني وتعقيد أساليب استخدامه

يعدّ الإرهاب من أخطر الجرائم التي عرفتها البشرية، وهذا بالنظر إلى الآثار الخطيرة التي يرتّبها هذا الفعل غير المشروع، وكما أسلفنا الذكر فإن المجتمع الدولي فشل في وضع تعريف جامع ومانع متفق عليه دُوليا حول ماهيته وما خصائصه، ومن هذا المنطلق تبرز صعوبة وضع معايير التفرقة (المطلب الاول) وكذا فهم أساليب ووسائل استخدام هذا الفضاء لأغراض إرهابية (المطلب الثاني).

المطلب الأوّل: إشكالية تعريف الإرهاب السيبراني.

لقد تطوّر مفهوم الإرهاب تطوراً مطرداً على مدار العقود الأخيرة، وتداخلت معه عديد العوامل بما صعّب إمكانية تعريف أحد تجلياته المتمثلة في "الإرهاب السيبراني"، الأمر الذي يتطلب إعادة قراءة والتوقف عند مدلوله في العالم المادي قبل الانتقال به إلى العالم الافتراضي إلّا بالقدر الكافي لبيان أبعاده.

الفرع الأول: تـــباين في المفاهيم.

يعدّ الإرهاب السيبراني مفهوما هجيناً بالنظر إلى الإرهاب التقليدي، أين سنحاول إيضاح بعض مفاهيم هذا الأخير مُكتفين هنا برصد بعض التعاريف على سبيل المثال لا الحصر. لعلّ أفصح وصف وُضع لغتًا هو الوصف الذي أطلقه مجمع اللغة العربية في معجمه الوسيط على الإرهابيين حين ذكر "انه وصف يطلق على الذين يسلكون سبيل العنف لتحقيق أهدافهم" [2] وعليه فقد رافقت هذه الأعمال، المجتمعات البشرية منذ ظهورها، وترجمت عمليا من خلال لجوء فرد معيّن أو مجموعة منظمة إلى بثّ الرعب والخوف لدى أفراد.

غير ان ممارسة تلك الاعمال لاسترجاع حقوق ضائعة او ارض او ممتلكات قد نُهبت او سلطة قد اختُصِبت، اوجدت خلافا حول النظرة إليه، وحول شرعية الاعمال المُقدم عليها، فعلى سبيل المثال فالأعمال الموصوفة تلك والتي يمارسها المقاومون في أرض الاحتلال تبقى غير مشروعة إلّا إذا مورست وفق شروط حدّدها القانون وكذلك الحال بالنسبة للتمرّد الذي يقع داخل الدولة الواحدة. وهنا تتداخل الاعتبارات السياسية والقانونية ليس اقلها أعمال المقاومة الفلسطينية ضد الاحتلال الإسرائيلي

والتي يعتبرها الأخير إرهابًـــا يُستوجب القضاء عليه. فالاختلاف يعود إلى جذور ثقافية ودينية وسياسية وفكرية.

فالدول لم تتفق حتى اليوم على تعريف محدّد ، فبعض الدول تُصرّ على إدراج

إرهاب الدولة ضمن أي تعريف يوضع، بينما اكتفت دول أخرى بتحديد عناصره[3]وعلى خط الموازاة فقد اعتمدت الدول تعريفات معينة سواء فردية او في إطار تكتلات، مثل الاتحاد الأوربي الذي صنّف الجناح العسكري "لحزب الله" على انه تنظيم إرهابي بينما مُنع ذات التصنيف على جناحه السياسي.[4]

فيما يخص الجزائر فقد عرفت أبشع صور الإرهاب في تسعينيات القرن الماضي بلغت أشدها عام 1992 ودفعت المشرع الجزائري لسن عدة قوانين مُستعجلة إلى أن اصدر أمرا رئاسيا في 25 فبراير سنة 1995 ألغى بموجبه المراسيم السابقة [5]ثم عدل هذا الامر عدة مرّات بموجب قانون العقوبات التي أدرجت ضمنه جريمة الإرهاب (خاصة المادة الأولى من المرسوم التشريعي 92-03) الذي عرّف مفهومها بالنشاط الإنساني الذي يحدث في العالم الخارجي، أي العمل الذي له أثر مادي خارجي لا ان يبقى مكنون نفسية الجاني كبث الرعب وعدم الامن في أوساط السكان من خلال الاعتداء على الأشخاص او تعريض حياتهم او حريتهم او امنهم للخطر، او لمس ممتلكاتهم وعرقلة النظام العام والسير العادي للمؤسّسات العمومية وموظفيها. ومن ثم جاء النص على تلك الاعمال بالموصوفة بأفعال إرهابية او تخريبية في القسم الرابع مكرّر في المواد من 87 مكرّرًا الى 87 مكرّرًا 10، لتعدّل العقوبات الناتجة عنها بموجب القانون 06-23 المؤرخ في 20 ديسمبر 2006. والظاهر ان المشرّع الجزائري هو الآخر قد عجز عن إيجاد تعريف دقيق ومحدّد لظاهرة الإرهاب.

فإذا كنّا نتحدث عن الإرهاب السيبراني فإنه من الواجب التعريج على بعض المفاهيم القريبة منه وإيضاح الغموض في المصطلحات المستعملة هنا، او التي تُسمع أحيانا في مواضع كثيرة وليس الهدف هنا التعمّق في تحليل تلك المعاني بل يكفينا الإشارة إلى التباين والاختلاف الواضح بين الاعتداء الالكتروني والسيبراني، فالأول (الالكتروني) هي كل ما يتعلّق بالتكنلوجيا الالكترونية كفرع من فروع علم الفيزياء، ذلك ان القسم العسكري منه يكون باستخدام إلكترونيات تهتم بالإجراءات التي تتّخذ لمنع او تقليل استخدام العدوّ لطاقته الكهرومغناطيسية الفعّالة المنبعثة، [6] وهو التعريف الذي وضعه حلف شمال الأطلسي "NATO" والمعتمد لدى

وزارة الدفاع الامريكية، فالكشف والاستطلاع ومراقبة وتحليل موجات العدّو الصادرة المنبعثة من اجهزته اللاسلكية هي صور من صور النزاع المسلّح التي تستخدم فيه وسائل إلكترونية[7] كما هنالك تعريف آخر اكثر دقة يصف الحرب الالكترونية بالتقنيات والأجهزة الالكترونية التي تستخدم لأغراض: - تحديد وجود المساندة الالكترونية المعادية في العمليات الحربية، تدمير وافساد المساندة الالكترونية الفعالة المعادية منع تدمير المساندة الالكترونية الفعالة الصديقة.[8]

اما الثاني (السيبرانية) فهي حرب تخيلية تقع في الفضاء الشبكي غير الملموس تحاكي الواقع بشكل تام، إذ تتلخص وسائل الصراع فيها بالمواجهات الرقمية والبرمجيات التقنية، والجنود الافتراضيون، وطلقات من لوحات المفاتيح، ونقرات المبرمجين، في بيئة افتراضية تصل آثارها إلى ملامح الحياة المادية، إذا هي حرب بلا دماء، [9] فهي عمليات تشن ضد او عبر حاسوب او نظام حاسوبي بواسطة تيار البيانات الرقمية، وحتى نكون في الصورة فإنّ المصطلح بالإنجليزية (CYBER) لا مُقابل له في اللغة العربية غير انّ الترجمة الغالبة هي "الالكترونية" وهي ترجمة غير صائبة بدليل ما سبقنا شرحه. وفي انتظار التطرّق له من قبل المختصين في اللغة خاصة مجمّع اللغة العربية، لا نرى حرجًا من استخدام مصطلح "السيبرانية" بما انّ منظمة الأمم المتحدة وبعض القوانين العربية اتخذته كمُقابل بمصطلح (CYBER).[10]

الفرع الثاني: ظهور المصطلح.

بدأ ظهور الإرهاب السيبراني بظهور الفضاء السيبراني وتوسّع الاعتماد على تقنيات المعلومات والاتصالات في تنفيذ الشؤون اليومية للأفراد والمؤسّسات والدول. فهو يرتبط بالبيئة التي يُمارس فيها ومن خلالها. من هنا، يمكن تعريف الإرهاب السيبراني انطلاقا من تلك الوسائط التي يتم التنفيذ من خلالها.

فقد عرّفته هيئة الأمم المتحدة في أكتوبر سنة 2012 بأنّ "الإرهاب الالكتروني هو استخدام الانترنت لنشر الاعمال الإرهابية"، [11] وبحسب التعريف المعطى له في القانون الأمريكي المنشور على صفحة المكتب الفيدرالي للتحقيقات، هنالك تمييز بين الإرهاب الدولي والوطني، ويقصد بالإرهاب السيبراني، حسب المصدر "كل اعتداء قصدي، ذي دوافع سياسية، على المعلومات او النظام المعلوماتي، او البرامج او البيانات ينتج عنه اعمال عنف ضد المدنيين، سواء ارتُكب من قبل مجموعة وطنية او عملاء غير مرئيين"، من جهته اعتمد حلف شمال الأطلسي تعريفًا

اعتبره "أي هجوم سيبراني، يُستخدم او يستغل شبكات المعلوماتية او شبكات الاتصال، لإحداث تدمير كاف لإثارة الرعب، وإرهاب مجتمع، لأهداف إيديولوجية".[12]

قياسا على ذلك، -من جانبنا- يمكن القول ببساطة ان الإرهاب السيبراني هو "الإرهاب الذي يُقترف في الفضاء السيبراني، وهو بدوره يُفهم على انه الاستخدام المنظم للعنف مما يثير الرعب لتحقيق اهداف سياسية وايديولوجية الذي يحدث في الفضاء السيبراني"

كما ان ذات الاعمال الإرهابية قد لا يكون لها أي أثر مادي، غير ان الأثر الأيديولوجي قد يكون أخطر بكثير، مثل التحريض او التجنيد وهنا ينبغي التمييز بين النضال السيبراني من اجل جلب الاهتمام إلى قضية ما مثل جماعات Anonymous، والذي يستخدم نفس الوسائل لكنّه لا يهدف إلى تدمير او تعنيف افراد المجتمع او مؤسّسات الدولة، كما يمكن التمييز بين الإرهاب السيبراني والحرب السيبرانية والتي تكون هذه الأخيرة ضمن نزاع مسلّح دولي او غير دولي والتي يمكن تطبيق قواعد القانون الدولي الإنساني عليها.[13]فحتى وان سلّمنا جدلا ان الارهاب السيبراني أخطر واشد الاعتداءات السيبرانية خطورة، إلّا ان التعريف المقدم لا يمكن اسقاطه لوصف جميع الاعتداءات السيبرانية التي لها نفس الآثار الوخيمة، إلّا متى توافرت بها عناصر محدّدة، مثل الهدف السياسي وهوية المعتدي او المحرض عليه، ونقطة انطلاقه وغاياته. فالجريمة السيبرانية [14] تختلف جوهريا عن الجريمة الإرهابية السيبرانية، إذ يرتكز هذا التمييز إلى اهداف كل منها فالأولى تسعى الى كسب المال والارباح او اثارة الاهتمام، اما الثانية فتسعى إلى الضغط وفرض شروط معيّنة عبر استعراض قوّة تثير الرعب والهلع.

المطلب الثاني: أساليب الاستخدام ومحاذيره

يُعتبر الفضاء السيبراني منبرا هاما تطُلّ من خلاله الجماعات الإرهابية، سواء لإدارة عمليات في أماكن مختلفة، او من اجل الترويع والتحريض والتجنيد والحشد وبثّ ثقافة او فكر إيديولوجي، بحيث تتنوع الاستخدامات حسب تنوع الأهداف في الزمان والمكان لذلك يُلاحظ ان الوجود الإرهابي على شبكة الانترنت والفضاء السيبراني ككلّ أصبح يُشّكل خطرا على الاستخدام السلمي لوسيلة الاتصال هذه، وسنفصل في بعض صور استخدام الجماعات الإرهابية للفضاء السيبراني.

الفرع الأول: الأساليب التقنية عالية الدقة

تستخدم الجماعات الإرهابية في العالم تقنيات رقمية غاية في التعقيد والتطوّر بدءً بالأنترنت المظلم (Dark Net) الذي يعتبر وسيلة للمجهولية (Anonymat)[15] واخفاء

الأثر مما يجعل الدول والسلطات تجد صعوبة هائلة في مصدر التهديدات، ثم ان الإرهاب لم يقتصر وجوده في المواقع المخفية بل انتقل إلى الفضاء المفتوح او الشبكة العالمية للأنترنت. وفي كل الاحول فتلك الأساليب لا تختلف في مضمونها مع تلك المستخدمة في الجرائم السيبرانية المنظمة او العادية ضدّ الأشخاص او الشركات.

أولا : الانترنت العميق والانترنت المُظلم:(Dark&Deep Web)

الانترنت المُظلم هو جزء من الانترنت الخفي (Hiden Net) الذي لا يمكن الوصول إليه باستخدام المتصفحات العادية (Navigateur) او محركات البحث (Moteur de Recherche) مثل "Google" و"Yahoo" او غيرها، فلهذا النوع من الاستخدام متصفحات خاصة مثل "TOR" [16] و"Freepto" [17]او "FreeNet" وغيرها، اما الميزة الأساسية لهذه المتصفحات فهي إخفاء الأثر الذي يمكن ان يتركه المتجوّل على الانترنت، ومنع تعقّب الأجهزة الأمنية ومراقبته مما يتيح له حماية هويته ومعلومات عن مصدر اتصاله، انشاء مواقع على الانترنت دون الكشف عن المنشئ، تجاوز برامج الحجب التي تستخدمها الدول لحجب بعض المواقع وتكوين شبكة اتصال آمنة وغير مرئية تذلّل عقبات إرسال المعلومات السريّة، ويتم تأمين ذلك عبر تقنية ترتكز أساسا على نظام تشفير للبيانات وعلى شبكة مؤلّفة من آلاف والموزعات حول العالم، التي تستقبل طلبات الدخول إلى المواقع، إذ تقوم بترميزها قبل إعادة إرسالها، وهذا ما يؤمن إخفاء الهوية وسرية التصفح والحركة. كما تجدر الإشارة إلى ان معظم هذه البرمجيات بدأت كمشاريع بحث تابعة للقوات البحرية الامريكية على عكس الانترنت التي يعتقد الكثير خطأً انّ نشأتها كانت موجّهة في المقام الاوّل للاحتياجات العسكرية غير ان الصواب هو انّها كانت موجّهة لأغراض علمية وبحثية من خلال مشروع Arpanet Advanced Research Projects Agency Network(شبكة وكالة مشاريع البحوث المتقدّمة) بدعم وتمويل مالي من وزارة الدفاع الأمريكية ومع ذلك فقد تمّ تطويرها داخل جامعات ومؤسّسات بحثية لتكون أداة للعلماء لمشاركة المواد العلمية لغير الأغراض العسكرية، [18] وهذا قصد تأمين خصوصية الاتصالات والمعلومات التابعة للأجهزة المتصلة بها، ثم بدأ تعميم هذه الميزة إلى موظفي المنظمات

الدولية والهيئات الحكومية والأجهزة الأمنية، إلّا انها لم تتأخر بالوصول إلى مجرمي الفضاء السيبراني وبالتالي إلى الجماعات الإرهابية بصفة عامة، فقد استُخدمت في الاتجار بالمخدرات والأسلحة وتأمين المرتزقة وجرائم القتل والاتجار بالبيانات العسكرية وغيرها. غير ان الإرهاب السيبراني أصبح علنيا من خلال الانترنت المفتوح بحيث أصبح يؤمّن عملياته العدائية من خلال الانترنت المظلم بينما يقوم بنشر أفكاره على الانترنت المفتوح من خلال صفحات التواصل الاجتماعي والمواقع العلنية، ثم ان الصعوبة ذاتها تتلقاها الأجهزة الأمنية في تتبع وحجب تلك المواقع، حيث تقوم تلك الجماعات باستخدام أسلوب الكرّ والفرّ لتختفي وتعود للظهور بعناوين جديدة.

ثانيًا: الشبكة العالمية للمعلومات (الانترنت)

بعيدا عن استخدام الانترنت المظلم يلجأ الارهابيون إلى الشبكة العالمية للمعلومات، والتي يتواصل فيها جميع المستخدمين حول العالم، وتستخدمها الجماعات الإرهابية ليس للتنسيق بين أعضاءها فقط بل للتواصل مع العالم حيث يوجّه الإرهاب السيبراني رسائله إلى الاعلام والدول والشعوب، بهدف نشر الرعب والترهيب وشن الحملات النفسية واستقطاب الأعضاء الجدد ثم تجنيدهم والتحريض العلني على القيام بهجمات ضد أعداء التنظيم الإرهابي وإثارة تعاطف الشعوب، فالشبكة العالمية هي المجال الذي يتفاعل فيه جميع المستخدمين سواء العسكريين او المدنيين او الحكومات. وليس هذا الإطار المناسب للتعمق أكثر في أساليب الاستخدام عبر الشبكة العالمية نظرًا لسعّة الموضوع فالقنابل المنطقية او القصف الالكتروني او الفيروسات ما هي إلا صور للاعتداء السيبراني.

ثالثا: تطبيقات الشبكات الاجتماعية

ومثالها تطبيق "تيليجرام" "Telegram" لمطوّره "بافيلدوروف" وهو من اكثر المنصات المشفرة الذي باتت تستحوذ على مساحة هامة من أنشطة التنظيمات الإرهابية وذلك على حساب الشبكات الاجتماعية التقليدية مثل "التويتر" او الفايسبوك" اين اتجهت الشركات المالكة لهذه الاخيرة لتضييق الخناق على تلك الأنشطة الإرهابية السيبرانية، ويعتبر تطبيق "تيليجرام" في مفهوم الامن العملياتي للجماعات الإرهابية "Operational security" منصة موائمة لتلك العمليات لما يمتاز بفكرة التشفير Encryption ومعدلات الحماية الهائلة بخاصية تشفير الرسائل من النهاية إلى النهاية End to End encrypted messanging Apps لتجنب انكشاف الاتصالات من قبل

الأجهزة الأمنية، وقد ظهرت بصمات التطبيق في عديد الهجمات الإرهابية التي شهدتها دول مختلفة على غرار هجمات باريس 2015، وهجوم عيد الميلاد في برلين 2016، وهجوم رأس السنة على ملهى "رينا الليلي" في إسطنبول سنة 2017، كما تستخدم وكالة "أعماق" التابعة لداعش ذات التطبيق من اجل الإعلان عن "فتوحاتها".

الفرع الثاني: الخطر الإيديولوجي.(نموذج الدولة الإسلامية في العراق والشام)

تستخدم الجماعات الإرهابية الانترنت المفتوح للتنقيب عن المعلومات وجمع الاخبار والمعلومات الخاصة بمواقع المنشآت الحكومية مثل المطارات والمنشآت العسكرية والمدنية ومنشآت الطاقة وغيرها. كما تستخدم الفضاء السيبراني في سبيل الاتصال والتنسيق مع افراد ومجموعات إرهابية أخرى وتوزيع المهام وتنفيذها ليس في العالم الافتراضي فقط بل العالم المادي. وهذا ما سنرصده من خلال هذا الجزء.

أولا: التحريض على الإرهاب

التحريض هو كل نشاط عمدي يهدف به صاحبه إلى دفع شخص ما إلى ارتكاب فعل يؤدي إلى وقوع جريمة، فالمحرض قد يفوق في الخطورة الفاعل للجريمة، خصوصاً في الحالات التي يكون فيها فاعل الجريمة ليس إلا منفذاً (حسن النية) أو يكون حاله غير ذي أهلية جنائية.

فمن المُستبان جليّا ان القانون الدولي العام قد جرّم كل اشكال التحريض على العنف مهما كانت وسيلته، والرأي القائل بأن وسائل الاتصال عبر الفضاء السيبراني هي الأخطر من حيث الكمّ والكيف، هو الرأي الاجدر بالتأييد نظرا للواقع المُعاش، ومهما يكن فالواضح ان النموذج قيد الدراسة يوضح جلّيًا مدى اعتماد تلك الجماعات على الفضاء السيبراني في بثّ سموم فكرها وشحن الافراد خاصة الشباب منهم على ممارسة العنف[19] فليس التحريض على الإرهاب كالتحريض على المقاومة وردّ العدوان الذي تضمنّته الشريعة الإسلامية الغرّاء بالقرآن الكريم والسنة النبوية الشريفة لخير دليل على ذلك.[20]

ومن خلال دراسة تحت عنوان "الخلافة الافتراضية. فهم استراتيجية الدعاية لدى تنظيم الدولة الإسلامية" لمؤسّسة "كويليام للأبحاث" [21] البريطانية لمكافحة التطرّف، أظهرت النتائج ان مواقع التواصل الاجتماعي أصبحت أشبه بـ "مساجد افتراضية" للمتشدّدين وعنصرًا حاسما في نشر التطرّف وتجنيد المقاتلين على نحو يفوق ما كانت تقوم به المساجد والكتب -المتطرّفة- حيث لم تعُد المساجد المكان المفضّل للتحريض والتعبئة بل أصبحت الحواسيب المتصلة بالأنترنت السبيل الأمثل لبثّ فكر

الجهاد المتطرّف، حيث يرى افراد التنظيم ان التأثير الرمزي يبسط سلطة ملموسة لدى الجماهير العربية وخاصة الغربية بعد التوجّه إليهم برسائل قابلة للاستهلاك المُباشر وهذا من اجل تعزيز جاذبية المحتوى وخلق هالة إعلامية تصوّر التنظيم على انّه قوة لا تقهر، تلك الفكرة ترجمت إلى قوة من خلال الصوت والصورة في محتوى فوتوغرافي عالي الجودة يتم نشره باستمرار، ومثل تلك الرسائل مكنت من تجميع المتعاطفين والمجندين المحتملين الذين يرجون شرف الانتماء إلى التنظيم ذلك ان تلك الصور أصبحت منتشرة على الأنترنت على أوسع نطاق وبالتالي لم تعُد الجهود التقليدية التي تبذلها الدول للحدّ من آثارها كافية، بل ينبغي الاخذ بوسائل مُبتكرة من اجل الوصول إلى الهدف، هذا ما يخلق تحدّيات جديدة على الدول.

ثانيا : التجنيد في صفوف الإرهاب

ان الحديث عن التجنيد يعني تبيان الاختلاف بين المُرتزق والفرد الإرهابي في الغاية التي يصبو إليها كل واحد، فالأول يسعى الى تحقيق مغنم شخصي او مكافئة مادية قيمة تفوق بكثير من المقابل الذي يتحصّل عليه مقاتل شرعي.[22] وبالتالي فلا يتمتع المرتزق بأية حماية وفق قانون الحرب.

اما الثاني فغايته غير مادية بل قد تكون أيديولوجية ام سياسية ام دينية او من غير ذلك، وتثار في هذه الحالة عدة مسائل مُبهمة بخصوص تكييف الحرب على الإرهاب، فالسؤال هنا -أي وضع قانوني ينطبق على الفرد الإرهابي؟ - ليكفينا هنا القول ان الإرهابي ليس له وضع قانوني بموجب القانون الدولي للنزاعات المسلحة، ولا يعني هذا ان لا تكييف له بل يجوز مقاضاته بموجب القوانين الجنائية الوطنية إذا شارك في أي عمل عدائي، بيد انّ القانون الدولي الإنساني في مادته الثالثة مشتركة لاتفاقيات جنيف سنة 1949 بالإضافة الى القانون الدولي لحقوق الانسان والقانون الوطني المُطبّق، كلها قوانين تصبح نافذة فيما يخصّ ظروف الاحتجاز والمعاملة الإنسانية وحقوق المحتجزين وفقا للإجراءات المتبعة.[23]

غير ان الواقع أكثر تعقيداً من ذلك فالولايات المتحدة الامريكية أعلنت عقب أحداث سنة 2001 انها تخوض حربًا على الإرهاب مصنّفة ذلك على انّها نزاع مُسلّح دولي في جميع انحاء العالم ضدّ فاعل من غير كيان الدول (تنظيم القاعدة) لذا نشأ بعد هذا جدل طويل الأمد لم تفصح الدول عن ردود فعلها بخصوص هذا الادعاء الغامض.[24] وكخير دليل على ذلك فان اللجنة الدولية لطالما سعت الى تذكير

الولايات المتحدة الأمريكية بضرورة وضع تكييف قانوني لتلك الحرب وأولئك المحتجزون وكان من الواضح ان بعض الاتفاقيات الدولية القائمة بشأن الإرهاب تسمح للجنة الدولية للصليب الأحمر بالوصول إلى الأشخاص المحتجزين للاشتباه في ضلوعهم في اعمال إرهابية كدليل آخر على ما أوردناه بخصوص ظروف الاحتجاز والمعاملة الانسانية.[25] وهذا ما يدفعنا بالتدبر في مسألة حربٍ بلا عُنوان.

الى هنا يمكن القول ان هذا التكييف القانوني كافٍ لأن يطبّق على الفرد الإرهابي الافتراضي ما ان ثبت تورّطه في تلك الاعمال لتبقى صعوبة اثبات ذلك راجعة الى خصائص تلك الجريمة (السيبرانية) وإمكانية الدولة المُكافِحة للإرهاب في ذلك عبر وسائلها التقنية والأمنية.

المبحث الثاني :أشكال مواجهة الإرهاب السيبراني

لم تنقطع الجهود الدولية الرامية لمواجهة انتشار التطرّف ومنظومة الاعلام (المُتطرّف) عبر الفضاء السيبراني، اين اكتسبت زخمًا غير مسبوق عقب تصاعد قوى تنظيم الدولة الإسلامية في العراق والشّام، عبر استراتيجية الترويج والاستقطاب الإعلامي للمُتعاطفين معه.

دفع هذا الوضع الدول فُرادى (المطلب الأوّل) وجماعات(المطلب الثاني) للإعلان عن خطة موحدة للمُواجهة، ما يستوجب توحيد الإطار القانوني لمكافحة الظاهرة، فإذا سلّمنا ان القانون الوطني هو المُنطبق في حالات الاعمال الإرهابية التي لا تعدو خارج حدود الوطن وآن مجموعة الاتفاقيات الدولية والمعاهدات الأممية كفيلة لمواجهة الإرهاب العابر للحدود الوطنية. فمـــا هو التكييف القانوني للإرهاب السيبراني الذي يجمع بين خصائص الاوّل والثاني. للإجابة عن هذا التساؤل فإنّ التحليل القانوني السالف ليس إلّا تفسيرًا لفهم الوضع القانوني التالي الذي وُضع لمُواجهة الظاهرة.

المطلب الأوّل: الجُـــهود الفردية للدُول (الجـــــــــزائر)

بعد مُعاناة دامت أكثر من عشر سنوات من الجحيم، أُخمدت نار الحرب الأهلية بفضل حكامة الشعب الجزائري، ومن نتائج تلك المأساة ان أصبحت الجزائر حِصنًا منيعًا امام محاولات تكرار تلك الأفعال، فالخطر الأيديولوجي لم يعُد محدقا بفضل

وعي الشعب الجزائري بخطورة المرحلة، غير ان الخطر الأمني السيبراني لايزال رهانًا ترفعه جلّ الدول على غرار الدولة الجزائرية التي تسعى بكافة السُبل إلى تأمين مُنشآتها الحيوية المدنية منها والعسكرية، عبر ترسانة من الأجهزة والقوانين الرادعة في ظل توجّه الدولة نحو مشروع عصرنة كل القطاعات الحكومية التي اتضحت ملامحه حين وُضع مشروعE-Algérie سنة 2013 بربط كل الفواعل بالشبكة السيبرانية.[26]

هذا ما دفع الدولة الجزائرية الى ابتكار أجهزة ومؤسّسات تسهر على تأمين الفضاء السيبراني بما يسمح لها بالمضي قُدمًا نحو الحكومة الالكترونية التي لازالت اليوم في مرحلة الرقمنة في انتظار بلوغ مرحلة استخدام تكنولوجيات الاعلام والاتصال TIC في كافة المجالات المدنية والعسكرية بما تشمل حماية محتوى للبيانات الوطنية. وفيما يلي وصف لما تم احرازه في البُعد القانوني والهيكلي (التنظيمي):

الفرع الأوّل: البُعد القانوني والقضائي

حظيت الجريمة السيبرانية باهتمام المشرع الجزائري وهذا بعدما أظهرت الاحصائيات الأمنية تنامي الظاهرة خاصة الصنف الأخطر منها وهو الإرهاب واستهلاك الرسائل المُميتة القادمة من مشايخ زائفين يدعون الى الفتنة وغيرها، كما زادت الحاجة الى حماية المُحتوى الوطني للبيانات تماشيا مع النسق الدولي. وقد قام المشرّع الجزائري بإصدار ترسانة من قوانين الوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال[27] مركّزًا في ذلك على الاعتداءات الماسة بالأنظمة المعلوماتية، اذ نذكر منها:

أولا: قانون العقوبات وقوانين الإجراءات القضائية

نصت عليها المواد من 87 مكرر الى 87 مكرر 6 من قانون العقوبات واشارت إلى الانخراط والتحريض والتشجيع والمشاركة والتعاطف والدعم والتمويل والنشر لصالح الجماعات الإرهابية، ونُشيرُ الى ان المشرّع لم يَقْرنْ صراحة تلك الأفعال بالعالم الافتراضي الّا ان معرفة الغرض وأساليب النشاط يكفي لجعلها طائلة في حق مرتكبها متى اقتُرنت بهدفها الاجرامي داخلية كانت او خارجية.

والمواد من 394 مكرّر إلى 394 مكرّر 7 من قانون العقوبات نظم القسم السابع مكرّر الذي تمم قانون العقوبات بموجب القانون 04-15 المؤرخ في 10 نوفمبر 2004 العقوبات الطائلة للأفعال المجرمة الماسة بأنظمة المعالجة الالية للمعطيات، وقد صنّفها المشرّع الجزائري بأسلوب تقني دون التعرّض للغرض من وراءها، غير انّه

ضاعف العقوبات في حالة استهدافها للدفاع الوطني او المؤسّسات العمومية. وبالتالي يكفي ربط الغاية من الجريمة بالوسيلة المُقامة لذلك حتى يتم تكييف العمل الإرهابي في اطراه الافتراضي.

غير ان التعديل الذي أتى به القانون رقم 16-02 المؤرخ في 19 يونيو سنة 2016 المعدّل لقانون العقوبات قد أضاف المادة 87 مكرّر 11 التي تعاقب كل جزائري او أجنبي يرتكب أفعال إرهابية (او يدبّرها او يعدّ لها او يشارك فيها او يدرّب عليها او يتلقّى تدريبا عليها) باستخدام تكنولوجيات الاعلام والاتصال (مطة 3 فقرة 2).

وأضاف التعديل المذكور المادة 87 مكرّر 12 التي تنص على ان القانون يعاقب كل من يستخدم تكنولوجيات الاعلام والاتصال من اجل دعم تلك الاعمال او تنظيمها او نشر افكارها بطريقة مباشرة او غير مُباشرة، أو تجنيد الأشخاص لصالح جمعية او تنظيم او جماعة او منظمة يكون غرضها الإرهاب.

ليفضي ذات التعديل إلى نـــص قانوني في المادة 394 مكرّر 8 يعاقب من خلاله مقدّم خدمات الانترنت بمفهوم المادة 2 من القانون 09-04 (المذكور أدناه) الذي لا يقوم بـــ - رغم اعذاره من الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال او صدور أمر او حكم قضائي يلزمه بـــ - التدخل الفوري لسحب او تخزين المحتوى الذي يشكل جرائم منصوص عليها قانونًا- او يمتنع عن وضع ترتيبات تقنية تسمح بسحب او تخزين المحتويات التي تتعلق بتلك الجرائم سالفة الذكر.

كذلك المواد15 و16 و37 و40 و41 و51 و65من قانون الإجراءات الجزائية التي أُدرجت بموجب القانون 04-14المؤرخ في 10 نوفمبر 2004، للنظر في الجرائم الماسة بأنظمة المعالجة الآلية للمُعطيات. ليوسع من الاختصاص الإقليمي حسب المرسوم التنفيذي 06-384 المؤرخ في 05 أكتوبر 2006. [28]

والملاحظ بشأن هذه النصوص انّها لم تصنّف الجرائم السيبرانية بل تركت الباب واسعًا للتكييف القضائي وبالتالي فإن كل الجرائم وفقًا لقانون العقوبات والمرتكبة عن طريق تكنولوجيات الاعلام والاتصال تصنّف ضمن الجرائم السيبرانية، وهو عكس ما تضمنته الاتفاقية الأوروبية بشأن الجريمة السيبرانية اين ذكرت تلك الجرائم على سبيل الحصر في أربع جرائم. ويمكن توضيح هذا من خلال

مثال جريمة السب والشتم التي تفرض تدخّل الشرطة القضائية كلما وقعت باستخدام تكنولوجيات الاعلام والاتصال، ويبقى هذا مستحيلاً نظرًا لانتشارها في الانترنت على الرغم من ان الاحصائيات أظهرت عديد المتابعات في هذا الخصوص، فما هو المعيار الذي تم من خلاله تجريم تلك الأفعال؟

ثانيا: القانون 09-04 المتضمن قواعد الوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومُكافحتها:

لم يُشر هذا القانون الى الجريمة الإرهابية السيبرانية بصفة خاصة غير انّه أشار الى مفهوم الجرائم المرتبطة بتكنولوجيات الاعلام والاتصال وهي الجرائم الماسة بأنظمة المُعالجة الآلية للمعطيات او التي ترتكب عن طريق منظومة معلوماتية او نظام اتصالات الكترونية وقد تضمن القانون إجراءات المراقبة والتفتيش والتحري والتحقيق القضائي بالإضافة الى المساعدة الدولية المُتبادلة، لتضيف المادة 15 منه إمكانية نظر المحاكم الجزائرية في أي جريمة وقعت خارج الوطن مُستهدفة مؤسّسات الدولة الجزائرية او الدفاع او المصالح الاقتصادية للدولة.

ثالثا: النصوص القانونية الخاصة بالوقاية من المخاطر والكوارث الكُبرى:

نظم المشرّع الجزائري مجموعة من القوانين المحدّدة لمجموعة الإجراءات المُتخذة في حالة وقوع كوارث طبيعية او تكنلوجية او صحية او بيولوجية او غيرها، بما فيها الاعتداءات على الأنظمة المعلوماتية المسيّرة للمصالح الحيوية الكبرى في الدولة مثل منشآت الطاقة الكهربائية والنووية والمائية وغيرها من المصالح.[29]

الفرع الثاني: البُعد التكنو هيكلي (التنظيمي)

تنقسم الجريمة الرقمية وفق القانون الجزائري إلى قسمين الأول يتعلّق بأي جريمة متصلة بتكنولوجيا الاعلام والاتصال، أي الجرائم التي تتم عبر الانترنت ووسائل الاتصال من قُبيل المساس بحرمة الأشخاص والهيئات العامة او التحريض للإرهاب او غيرها اما القسم الثاني فهو كل ما تعلّق بالمساس بأنظمة المعالجة الآلية للمعطيات التي تستهدف الأنظمة المعلوماتية من خلال الولوج لها وتعطيلها او تعديلها وغيرذلك.

وقد تم هندسة منظومة هيكلية مُحكمة لمجابهة تلك الجرائم بما في ذلك الإرهابية منها، نذكر منها:

أولا : الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال.

أنشأت بموجب القانون 09-04 لتسهر على حماية وتنسيق عمليات الوقاية، والمساعدة التقنية للجهات القضائية والتقنية، تفعيل التعاون القضائي والامن الدولي. ويُسمح لها بالمراقبة الالكترونية لأغراض وقائية لا سيما بما تعلّق بالجرائم الإرهابية والماسة بأمن الدولة عن طريق اذن من النائب العام لدى مجلس قضاء الجزائر لمدة ستة أشهر قابلة للتجديد. وبإذن من السلطة القضائية المُختصة في حالة الوقاية من اعتداءات على منظومات معلوماتية على نحو يهدّد مؤسّسات الدولة او الدفاع الوطني او المصالح الاستراتيجية للاقتصاد الوطني.[30]

وقد نظمها المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر سنة 2015، الذي حدّد تشكيلتها وكيفيات سيرها باعتبارها سلطة إدارية مستقلة تتمتع بالاستقلال المالي والشخصية المعنوية، لتوضع لدى الوزير المُكلّف بالعدل مع الإشارة هـــنا إلى انّها ليست سلطة او هيئة قضائية بل هيئة مساعدة لها وللأجهزة الأمنية الأخرى كالشرطة القضائية والدرك والمصالح العسكرية للاستعلام والامن.

ثانيا : التشكيل الأمني المختص للردع والوقاية من الجرائم السيبرانية. (الشرطة الالكترونية)

وهذا من خلال انشاء المصلحة المركزية للجريمة الالكترونية سنة 2011 التابع لمديرية الشرطة القضائية والتي كانت فصيلا امنيا على مستوى المديرية العامة للأمن الوطني لتدمج التشكيلتان في سنة 2015 ويتم لاحقا تشكيل فصائل فرعية على مستوى الولايات كافة.

ثالثا : الأجهزة التابعة للإدارة المركزية لوزارة البريد وتكنولوجيات الاعلام والاتصال.

لا جدال في ان الوزارة هي المسؤول ايضا عن كل ما تعلّق بالفضاء السيبراني ولهذا فقد ضمّت ادارتها المركزية بعض "[31]

رابعًا : مركز البحث في الاعلام

الهياكل المسؤولة عن اليقظة الالكترونية ومنها المديرية العامة لتكنولوجيات الاعلام والاتصال والتي تضمّ المديرية الفرعية لتأمين المنشآت الأساسية لتكنولوجيات الاعلام والاتصال، بالإضافة الى مديرية الاتصالات اللاسلكية والتجهيزات الحسّاسة للمواصلات السلكية واللاسلكية، كذلك المديرية العامة لمجتمع المعلومات المساهمة في اعداد "الإطار القانوني للأمن السيبراني

العلمي والتقنيCERIST

هو الجهاز الذي يسهر على متابعة وربط الهياكل التعليمية والبحثية والوطنية، والبحوث في مجال الأمن المعلوماتي للشبكات، وتطوير البنية التحتية السيبرانية.

خامسًا: أجهزة امنية مُختصة تابعة للدرك الوطني

وهو مركز الوقاية من جرائم الاعلام الآلي والجرائم المعلوماتية الذي يقع مقرّه بالعاصمة، كذلك المعهد الوطني للأدلة الجنائية وعلم الاجرام التابع أيضا للدرك الوطني.

سادسًا: الأجهزة التابعة للجيش الوطني الشعبي

تسعى الجزائر الى الحفاظ على سيادة إقليمها جوّا وبحرًا وبرًّا وفي الفضاء الخارجي من خلال قوّات الجيش الوطني الشعبي والأجهزة التابعة له، ومع بروز البعد الخامس وهو المجال السيبراني اسّس الجيش أجهزة عملياتية لتتبّع الاخطار السيبرانية مثل مصلحة الدفاع السيبراني ومراقبة امن الأنظمة التابع لدائرة الاستعمال والتحفيز. وبهذا فقد دخلت الجزائر في النمط الجديد من الامن السيبراني.

الفرع الثالث: تحدّيات الدولة الجزائرية في مجال الامن السيبراني. (واقع وآفاق)

ان تشخيص واقع الامن السيبراني في الجزائر يُشير الى ان الترتيب لا يزال مُتدنيًا نوعًا ما مقارنةً بالإمكانات المادية والبشرية التي تزخر بها الدولة، اذ تُشير الدراسات ان الجزائر تحتل المرتبة 68 عالميًا من أصل 168دولة بعد ان كانت في الترتيب 123 عالميا سنة 2015، والتاسعة عربيًا من أصل 22 دولة حيث حافظت عُمان على تفوّقها عربيًا في المرتبة الأولى وعالميًا في المرتبة الرابعة، فيما بقيت دولة موريشيوس تحتل المرتبة الأولى افريقيًا في حين ان الجزائر احتلت المرتبة السابعة في افريقيا (دون الدول العربية). بينما صعدت دولة سنغافورة لتحتل المرتبة الأولى عالميًا في مقابل تراجع الولايات المتحدة الامريكية التي تلتها،[32] ولعلّ تفوّق سلطنة عُمان عربيا وعالميا باعتبارها نموذجا للمُمارسات الجيّدة في المجال راجع الى الاستراتيجية الأمنية رفيعة المستوى التي أتت عن طريق خارطة طريق تشمل الميادين الخمس التالية:الهيكل التنظيمي– التدابير القانونية –بناء القدرات –التدابير التقنية والاجرائية –والتعاون الدولي والإقليمي.[33]

1) تعني التدابير القانونية كل من التشريع الجنائي كالمعاقبة على النفاذ غير المُخوّل (دون اذن او تصريح) الى الأجهزة وأنظمة وبيانات الحاسوب المحمي والاحتيال والتزوير والتشويش او التنصّت، او التشريع الإجرائي أي قواعد القضاء الإجرائية

المتبعة في هذا الشأن، ويشير المؤشّر الى ثلاث مستويات: المنعدم أو الجزئي او الشامل (المستقلّ) ومثاله القانون البريطاني بشأن إساءة استعمال الحاسوب الصادر سنة 1990، على عكس القانون الجزائري الذي اتى في شكل جُزئي مُتفرّع في قوانين عديدة، مع الإشارة إلى وجود فراغ تنظيمي متعلق بالقانون 09-04 المذكور نظرًا لعدم وجود اية نصوص تنظيمية لاحقة الى غاية اليوم، اما الجزء الأهم من التدابير القانونية هو معيار التنظيم والالتزام الذي يأتي في الثلاث مُستويات المذكورة.

2) اما التدابير التقنية فهي التكنولوجيا الفنية اي الغاية والوسيلة في آن واحد كوسائل وتقنيات الكشف عن الاعتداءات والردّ عليها، أي المراقبة والانذار والاستجابة ويمكن قياس هذه التدبير بمستوى تواجد المؤسّسات الأمنية عددًا وعُدّة كفرق الاستجابة للطوارئ الحاسوبية CERT وفرق الاستجابة للحوادث الحاسوبية CIRTوفرق الاستجابة للحوادث الأمنية الحاسوبيةCSIRT، اما المعايير فهي احترام تلك المعايير التي تضعها الوكالات الدولية مثل المنظمة الدولية للتوحيد القياسي ISO، والاتحاد الدولي للاتصالاتITU ، وفريق مهام هندسة الانترنتIETF ، وغيرها من المؤسّسات المُعتمدة دُوليًا. بالإضافة الى الشهادات او الرُخص العالمية المعترف بها دوليا التي تحظى بتأييد او اعتماد من طرف الحكومات مثل شهادة امن الحوسبة السحابية والتحليل الجنائي في مجال الامن السيبراني وغيرها. في هذا الإطار فان الجزائر لم تعتمد أي فرق حكومية للطوارئ او الحوادث الأمنية الحاسوبية، ما عدا الجهاز الذي يتبع مركز CERIST والذي يُعرف بـ DZ-CERT بيد انّه غير مُفعّل وبذلك فإن على الجزائر العمل بجهد أكبر في هذا الشأن فالاعتماد وفقط على هذه الفرق أصبح من النمط القديم الذي ظهر في تسعينيات القرن الماضي ومن الواضح ان هذا النمط لم يعُد يتماشى والنمط المُتقدّم لأسباب عديدة ليس اقلّها ان النمط الاخير يعتمد على عددًا وعديدًا من أصحاب الكفاءات للاهتمام بوضع استراتيجية هجومية ودفاعية سيبرانية كجزء من إمكاناتها العسكرية لمواجهة اية حرب سيبرانية مُحتملة وكمكّمل للحرب التكنولوجية وتمييز الهجمات العسكرية من الاعتداءات والاختراقات الاجرامية العادية.

كما ان الدولة لم تعتمد أي معايير دولية كمعيار ISO/IEC 27001 او غيره، كما لم تعتمد الجزائر أي شهادات دولية في هذا المجال، فيما اعتمدت الدولة بوابة

وطنية للوقاية من حوادث الانترنت سُميت بوقاية ناتWikaya Net تابعة لمركز CERIST فرع الامن المعلوماتي.

3) فيما تشمل التدابير التنظيمية والاستراتيجية ضرورة تنفيذ المشاريع الوطنية والمبادرات الدولية في المجال وهذا من خلال وضع الخطط الكاملة والاستراتيجيات الفعّالة (المستقلة) للتنفيذ والقياس عن طريق توفير الهياكل والمؤسّسات اللازمة كما تشمل أيضا وضع سياسة امنية أولية قريبة المدى ثم العمل على وضع سياسات متوسطة وبعيدة المدى بإشراك كافة الفواعل الوطنية الحكومية والخاصة وبالتعاون مع الجهات الإقليمية والدولية بتبادل المعلومات الأمنية والقضائية وهذا كلّه بعد تحديد معايير وطنية موائمة.

4) كما حدّد المؤشّر تدابير بناء القدرات التي تشمل التدابير السابقة لتحسين الأداء وفق كل مرحلة من المراحل بوضع استراتيجيات أفضل واهداف اذكى SMART حسب درجة النُضج والمعرفة التي تكون نتيجة البحث والتطوير والتدريب والتخصّص وتنمية القوى العاملة عن طريق مضاعفة بذل الجُهد المادي والبشري ونشر الوعي وتعزيز الثقة وفرض سلوك سيبراني آمن ومحفّز. وفي هذا الإطار فان الجزائر لم تعتمد استراتيجية وطنية للأمن السيبراني وبقيت كل الجهود سوى مُبادرات منفردة من بعض القطاعات والمراكز، كما لم تعتمد خارطة طريق لحوكمة الفضاء السيبراني الجزائري، والى غاية 2015 لم تُنشأ هيئة وطنية مُختصة في فرض استراتيجية وطنية لتلك السياسة، ذلك أنّ انشاءها قد يشكّل مُنعرجًا حاسما لتطوير تلك القُدرات في المُستقبل.

5) هذا بالإضافة الى تدابير التعاون التي تقتضي وضع شراكات بين القطاع الخاص والعام PPP داخل المجال الوطني بالإضافة الى خلق حيّز من التعاون والتداخل بين الوكالات الوطنية العمومية وأخيرا التعــاون الدولي إقليميا وعالميا كهيئة الأمم المتحدة والاتحاد الدولي للاتصالات وغيرها.

ان قياس مدى جاهزية الجزائر لمُجابهة تحدّيات العصر التكنلوجي تتوقف على ما حقّقته وما ستحقّقه على ارض الواقع انطلاقـًا من استراتيجية وطنية فعّالة للتحضير لسياسات سيبرانية تمسّ مُختلف القطاعات والمجالات الاقتصادية خاصة والاجتماعية والأمنية والتعليمية وغيرها في ظل اقتصاد معرفي يتطوّر أكثر فأكثر.

وخلاصة القول ان الجزائر لا تزال في بداية الشوط من اجل التحكم بشكل فعّال في فضاءها السيبراني مما يتيح لها ضمان امنها القومي بالموازاة مع ضمان

خصوصية وحقوق مواطنيها، فمن وجهة نظر الباحث فإنّ عدم حصر الجرائم السيبرانية قد يؤدّي إلى التمادي في التجريم على خلاف مبدأ الشرعية في المُسائلة والعقاب، وهنا تبرز أهمية تعريف الإرهاب وتحديده بشكل دقيق ثم تعداد الجرائم السيبرانية للحلول دون تثبيط وكبح لإمكانية الوصول إلى المحتوى، فالحقيقة ان هذا المنطق القانوني غير المستقر يعقّد من استراتيجية تعامل السلطة مع الفضاء السيبراني ويبتعد اكثر فأكثر عن حوكمة الانترنت، فقد صنّفت المنظمة غير الحكومية المستقلة Freedom House الجزائر بالدولة غير الحرّة في التعامل مع الفضاء السيبراني، كما سجّلت منظمة العفو الدولية سبع ملاحظات لا تتفق فيها الاتفاقية العربية لمكافحة الإرهاب (التي صدّقت عليها الجزائر) مع القانون الدولي ومواثيق حقوق الانسان مثل التعريف الواسع الذي قد يُستغل من اجل قمع الحريات، فلا ينبغي حماية الأمن العمومي بمعزل عن الحقوق الأساسية والحريات المدنية للمواطن، ولا بدّ من مراعاة توازن يضمن عدم دفع الأخيرة إلى مستوى متدنٍّ من اجل تأمين مستوى عالي من الامن، كما يجب الابتعاد عن منطق "إذا لم يكن لديك شيء تخفيه، فليس لديك شيء تخافه" الشعار الذي تبنّته الحكومة البريطانية عند وضعها استراتيجية لتصفية وفلترة المحتوى على الانترنت الذي أثار الجدل ليتم التخلي عنه فيما بعد.

المطلب الثاني: الجهود الدولية لمكافحة الإرهاب السيبراني

مما لا شكّ فيه، ان الخطوة الأولى للشفاء هي الإقرار بوجود الدّاء، من هُنا بدأ الوعي بخطر الإرهاب السيبراني يتنامى لدى الدول فُرادى وجماعات، بل ان الوعي ذاته احتضنته جماعات من الهاكرز (قراصنة الواب) لمُطاردة الجماعات الإرهابية عبر الفضاء السيبراني مثل Anonymous [34] غير ان المسؤولية تقع بالأساس على عاتق الدول والمنتظمات الدولية العالمية منها والإقليمية لبذل جهد مشترك من اجل القضاء على الظاهرة.

وقد شكّل احد التقارير(A/68/98)2013الصادر عن فريق الخبراء الحكومي المعني بالتطوّرات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، التابع للجمعية العامة للأمم المتحدة- شكّل – منعرجًا حاسماً فيما يخص الموضوع، إذ خلُص إلى ان القانون الدولي وبخاصة ميثاق الأمم المتحدة ينطبق على استخدام الدول لتكنولوجيات المعلومات والاتصال وهو عنصر لا بدّ من المحافظة عليه من اجل حفظ السلام والاستقرار وتهيئة بيئة تكنولوجية منفتحة ومأمونة، وقد أتت هذه الحوصلة كخلاصة لنداءات عديد الدول، بيد انّ المجتمع الدولي عامة

والمنظمات الدولية بخاصة لم تخطو خطوات جادة في هذا الموضوع وهذا راجع إلى تعقيد المجال وتداخله وعدم بروز مفاهيمه على عكس بعض التكتلات الإقليمية الخاصة مثل حلف شمال الأطلسي الذي نظم دليلًا متكاملا يخصّ قواعد القانون الدولي الإنساني المنطبقة في حالة نشوء حرب سيبرانية دولية او غير دولية، وقد عالج هذا الدليل مسائل لها علاقة بالإرهاب السيبراني.ومن خلال هذا الجزء من الدراسة سنركز على سرد الجهود الدولية في إطار المنظمات العالمية والإقليمية والمبادرات والشراكات الخاصة بين الدول والقطاع الخاص.

الفرع الاوّل: الجهود في إطار المنظمات الدولية العالمية

أولا: هيئة الأمم المتحدة (الجمعية العامة والأمانة العامة)

اقرّ الأمين العام للأمم المتحدة بخطورة الإرهاب السيبراني واعتبر هذا الفضاء مرتعًا خصبا لعمل الإرهابيين بطريقة عابرة للحدود وعليه فقد حثّ الدول للعمل بطريقة موحدة وكان اول تصريح للأمين العام في 15 مايو 2006 حول خطورة الهجمات الإرهابية في الفضاء السيبراني، فقد جاء هذا النداء ضمن تقرير صادر عن الأمم المتحدة موسوم بـ" استخدام الانترنت لأغراض إرهابية"[35] وقد كان هذا التقرير اول عمل منهجي تنتهجه هيئة الأمم المتحدة بخصوص الإرهاب السيبراني كما يعتبر التقرير مُرشدًا تقنيًا وفنيًا وعلميًا عالي المستوى يضم توصيات وايضاحات ومُمارسات جيدة وسُبلٍللتعاون الأمني والقضائي.

كماأصدرت الجمعية العامة قرارين عملًا بالبُند 97 من قرار مجلس الأمن 2253 لسنة 2015، حول "الإمارة الإسلامية" يخصّ تجنيد الإرهاب عبر الانترنت إذْ اوصت الدول باستحداث إجراءات محلية عاجلة للحدّ من الظاهرة، حيث أظهرت تقديراتها ان نسبة المجندين في صفوف الجماعات الإرهابية قد بلغ 30000 شخص قادمًا من أكثر من 100 دولة عضو في هيئة الأمم المتحدة، وبالتالي دعت الشركات العالمية مثل "فايسبوك" إلى التعاون مع الدول من اجل حذف المحتوى او انهاء حسابات المستخدمين.[36] ويلاحظ ان القرار تطغى عليه الإجراءات الوقائية مثل التعليم ومحاربة دواعي العنف الكامنة واستئصالها وجذب الشباب والوقاية الدعائية للحدّ من الأفكار المتشدّدة، ودعم نشاطات اليونسكو.

ثانيا : دور مجلس الامن

فرض مجلس الامن تدابير على الدول بخصوص التضييق على الإرهاب الالكتروني بموجب القرار 2161 لسنة 2014 بعد ان أنشأ لجان للعمل عملاً بالقرارين 1267 لسنة 1999 وسنة 2011 بشأن تنظيم القاعدة و2253 سنة 2015 بشأن تنظيم الدولة الإسلامية في العراق والشام، بحيث تعمل اللجان على الوقاية من التطرف، وتقليص أثره وانعكاسه على المُجتمعات بإشراك الأخيرة.

ثالثًا : دور الاتحاد الدولي للاتصالات

الاتحاد الدولي للاتصالات وكالة خاصة تابعة للمجلس الاقتصادي الاجتماعي الجهاز التابع للأمم المتحدة، وقد عني الاتحاد بوضع سياسات الامن السيبراني وتحفيز الدول للتعاون من اجل بناء الثقة والرفع من درجة الحماية خاصة للمنشآت الحرجة المتعلقة بالدول، حيث اصبح الاتحاد الدولي ملتقى دولي رئيسي لهته الأنشطة اذ يتعاون بشكل خاص مع مكتب الأمم المتحدة لمكافحة الإرهاب، وينشر الاتحاد دليلًا امنيا (الامن وتكنولوجيات المعلومات والاتصال) لمساعدة الدول في تعزيز امنها السيبراني كما يضع الاتحاد اطارًا لتعزيز الامن (برنامج الامن السيبراني العالمي) بحيث تم تعيين خبراء في المجال من اجل إسداء المشورة للدول، كما تضمن القمة العالمية لمجتمع المعلومات التي يرعاها الاتحاد الدولي للاتصالات توصيات في هذا الشأن .

الفرع الثاني: المبادرات والشراكات الدولية

- أعلن الانتربول سنة 1981 عن اول مبادرة من اجل مواجهة الجريمة الالكترونية والإرهاب. ثم تم انشاء معهد قانون الفضاء الالكتروني في جامعة جورج تاون سنة 1995.
- وفي سنة 2000 أصدرت جامعة ستانفورد مسودة اتفاق عالمي حول الجريمة والإرهاب السيبراني شملت عدة مبادئ مثل ما نص عليه البند 12 بإنشاء وكالة لحماية البنية التحتية الكونية للمعلومات.
- أعلنت ماليزيا في بادرة فريدة من نوعها عن مبادرة الشراكة الدولية متعددة الأطراف لمكافحة الإرهاب السيبراني IMPACT وهذا على هامش انعقاد المؤتمر الخامس عشر حول تكنولوجيات المعلومات، بهدف حشد الجهود من جانب

القطاعات العمومية والخاصة والمجتمع المدني لمواجهة خطر الإرهاب السيبراني لتنشئ بعد ذلك في او مؤتمر لها سنة 2008 أربع مراكز مختصة يهتم احداها بالاستجابة للطوارئ الدولية.[37]

- إنشاء مواقع الانترنت لمكافحة الإرهاب السيبراني مثل مجموعة SITE للاستخبارات الذي يعد كجهاز استخبارات مختص في رصد الإرهاب عبر الفضاء السيبراني ومراقبته ودراسته ومحاربته.[38]
- التدريبات والمناورات مثل المناورة التي قامت بها الولايات المتحدة الامريكية 2006 و2008 بالتعاون مع اللجنة الدولية للصليب الأحمر ووكالات ودول اجنبية أخرى وأطلق على المناورة السيبرانية عنوان "عاصفة الحواسيب Cyber Storm "حيث وضعت أجهزة الاستخبارات الامريكية البنى التحتية والمنشآت الحرجة تحت محاكات هجومات سيبرانية على مدى أسبوع كامل.[39]
- كما تم انشاء المركز العالمي للاستجابة للطوارئ الذي يعمل على نظام شبيه للنظام القانوني للجرف القاري في إطار القانون الدولي للبحار، فالعديد من المدارس القانونية والفقهية تدعو لاعتبار الفضاء السيبراني (الانترنت) تراثا مشتركا للإنسانية مثله مثل أعالي البحار والفضاء الخارجي.[40]

الفرع الثالث: الجهود الإقليمية

- يسعى جهاز الانتربول لمكافحة الظاهرة من خلال التدخل والمتابعة والتحقيق، مثل قرار عملية الانتربول سنة 2005 المعتمدة من قبل الجمعية العامة للإنتربول-AG 10-RES-2005 في برلين.
- دعت مجموعة الثماني G8 في 11 مايو 2004 إلى التصدي للإرهاب السيبراني ضمن خطط وطنية واضحة المعالم وأخرى تعاونية فيما بين تلك الدول، فيما دعت مجموعة السبع G7 إلى التعاون مع الانتربول من اجل التصدي للظاهرة في 20 أكتوبر 2017.
- الاتفاقية الاوربية لمكافحة الجريمة السيبرانية بودابست 2001. والبروتوكول الإضافي لها سنة 2003، التي انضمت اليها دول غير اوربية مثل الولايات المتحدة الامريكية واليابان وأستراليا وغيرها.
- فيما يخص حلف الناتو فقد أظهر قدراته السيبرانية خاصة مع الهجوم السيبراني التي تعرّضت له أستونيا سنة 2007 بحيث تبنى سياسة دفاعية عالية المستوى وأنشأ مركزًا للبحث المتقدم للدفاع السيبراني في عاصمة استونيا تالين، كما يعقد

المركز المؤتمر الدولي للنزاعات المسلحة الدولية السيبرانية (CYCON) International Conference On Cyber Conflict والتي كان آخرها الأول من يناير سنة 2018، اين تناول المؤتمر عديد المواضيع من بينها خطورة وضرورة التصدي لظاهرة الإرهاب السيبراني، وتجدر الإشارة إلى ان المركز كان اطاراً لفريق الخبراء الذي أصدر دليل تالين لقواعد القانون الدولي الإنساني المنطبقة في الحرب السيبرانية.

- منظمة الدول الأمريكية أعلنت في 30 أبريل 2004 قرارها تبني الاتفاقية الاوربية لمكافحة الجريمة السيبرانية ومبادئها ودعم الجهود الدولية لمجابهة ظاهرة الإرهاب السيبراني.
- منظمة التعاون الاقتصادي لآسيا والمحيط الهادي ESCWA هي الأخرى تؤطر الأمن السيبراني لأعضائها عن طريق جملة من القرارات والتوصيات.
- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحرّرة في القاهرة بتاريخ 21 ديسمبر 2010 حيث صدّقت عليها الجزائر بموجب المرسوم الرئاسي رقم 14-252 المؤرخ في 8 سبتمبر 2014، حيث نصت في مادتها 15 على الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات مشيرة إلى ان التجريم يقوم في حالة نشر أفكار ومبادئ إرهابية والدعوة لها (دون تحديدها) وتمويل الجماعات الإرهابية والتدريب وتسهيل الاتصال بينها، ونشر طرق صناعة المتفجرات ونشر النعرات والفتن والاعتداء على الأديان والمعتقدات .
- المركز العربي الإقليمي للأمن السيبراني الذي ينظم مؤتمرات إقليمية عربية للأمن السيبراني والتي كان آخرها في نوفمبر سنة 2017 بخصوص البنى التحتية الحرجة.
- مبادرة التعاون الخليجي GCC CERT ومبادرة منظمة التعاون الإسلامي CERT OICمن اجل التعاون التقني بين فرق الاستجابة للطوارئ الحاسوبية اين تولي اهتمام خاص للإرهاب السيبراني.
- مبادرة مركز البحوث والدراسات القانونية والقضائية العربي بمشاركة المرصد العربي للسلامة والامن في الفضاء السيبراني الذي بادرا بعدة مشاريع منها مشروع الاتفاقية العربية لضمان امن وسلامة الفضاء السيبراني، وكذلك مشروع بناء الثقة في الفضاء.

- أقرت المجموعة الاقتصادية لغرب افريقيا اتفاقية توصية لمكافحة الجريمة السيبرانية بما فيها الإرهاب السيبراني سنة 2011 تضمنت القواعد الإجرائية كالإثبات وجمع الأدلة الرقمية والمواد التجريمية.

الخاتمة

يمكن القول ان الإرهاب السيبراني أصبح من أكثر المواضيع إثارة للجدل مما تنصرف تأثيراته على الجانب الأمني والدفاعي لدى الدول، ولعلّ المقاربة الجزائرية في مواجهة ظاهرة الإرهاب بصفة عامة جعلت من المُمارسة نموذجًا عالميًا تسعى الدول إلى حذوه، وبخصوص الفضاء السيبراني فإن الدولة الجزائرية تسعى بكل جهد للوصول إلى حوكمة شاملة للفضاء السيبراني بما يضمن الامن والتطور على السواء، فالوعي المُسبق لأجهزتها الأمنية بخبايا واستراتيجيات الجماعات الإرهابية في الفضاء السيبراني خاصة فيما يخص التجنيد والتحريض جعلها تُحكم سيطرتها على الوضع لتمنع تحويل البلاد إلى رماد مثلما حدث للدُول التي أعاث فيها الإرهاب فسادًا.

فالتجربة التي عرفتها البلاد أضحت جرحً غائر في نفسية الشعب مما جعله حصنًا منيعًا يقف في وجه محاولات بثّ الأفكار المتطرّفة، كما ان وعي السلطات وحنكتها في مواجهة الازمات الاجتماعية نجحت في تجنّب أسباب ظهور الفكر الإرهابي الذي ينطلق بالأساس من الضغط الاقتصادي السلبي على الفئات الهشّة واللاعدالة المُجتمعية، بالإضافة إلى الدور الفعّال الذي تضطلع به الأجهزة الأمنية وفي مقدّمتها الجيش الوطني الشعبي، فسياسة المُصالحة الوطنية والوئام المدني والرحمة والسياسات التنموية في التشغيل والتعمير كانت دافعًا لتجنب أزمات اجتماعية قاسية، كما ان الفكر والدين عن طريق الوسطية وتفادي التطرف شكّل صنبورًا للأمان وحطّم عديد دعوات التطرّف والتجنيد في صفوف الجماعات المسلحة العابرة للحدود.

ومن النتائج المُتوصّل إليها هي انّ الإرهاب السيبراني لا يُشكّل خطرًا تكنولوجيًا (على الأقل في الدول الأقل نُموًا من الناحية التقنية مثل الجزائر) بالقدر ما يُشكّلهُ من تحدّيات إيديولوجية ونفسية بالنسبة لأفراد المُجتمع، ولعلّ الجزائر اليوم مُطالبة أكثر من أي وقت بالاتجاه وبصفة حقيقية نحو حوكمة الفضاء السيبراني وبناء مُؤسّسات عصرية تعتمد بالأساس على الوسائل التقنية والرقمية حتى تُلافي شبح الخمول والبداوة في عملها، فالعالم اليوم يشهد من دون شكّ تطوّرات تقنية مُضطردة وصلت إلى ذروة التسلّح السيبراني والهجمات السيبراني التي تمسّ البُنى التحتية

الحرجة للدُول، وهذا ما يخلق تحدياً يكمن في التوجّه نحو العصرنة بالموازاة مع خلق نظام أمني سيبراني حقيقي مُجابه لتلك الأخطار عن طريق استراتيجية وطنية تعتمد أساساً على القدرات الفنية والتقنية.

الهوامش

1- GABRIEL WEIMANN, www.terror.net How Modern Terrorism Uses the Internet, SPECIAL REPORT, united states institute of peace, vol. 31, DIANE Publishing, 2004, p 02.

https://books.google.dz/books?id=a_cugt6quTYC تم الاطلاع عليه يوم 2017/03/17.

2- يُنظر المُعجم الوسيط (1) ص 376.

3- مثل اتفاقية المجلس الأوربي الصادرة بتاريخ 10 نوفمبر 1976 لقمع الإرهاب، او اتفاقية الأمم المتحدة الصادرة بتاريخ 17 ديسمبر 1979 الخاصة باختطاف الرهائن، والاتفاقية الخاصة بقمع الإرهاب والتفجيرات الإرهابية الصادرة عن الأمم المتحدة عام 1997، واتفاقيات أخرى في خاصة باختطاف الطائرات وغيرها.

4- The US, Canada and Australia have also listed Hezbollah as a «terrorist» group. The EU has blacklisted its military wing.

http://www.aljazeera.com/news/2016/03/gcc-declares-lebanon-hezbollah-terrorist-group-160302090712744.html تم الاطلاع عليه يوم 2017/04/03

5- الامر رقم 95-10 المؤرخ في 25 فبراير 1995 يعدل ويتمم الامر 66-155 المؤرخ في 08 يونيو 1966 المتضمن قانون الإجراءات الجزائية.

6- جاسم محمد البصيلي، الحرب الالكترونية أسسها وأثرها في الحروب، مراجعة الدكتور مالك غلوم حسين، المؤسّسة العربية للدراسات والنشر، الطبعة 2، بيروت 1989، ص 30.

7- جاسم محمد البصيلي، الحرب الالكترونية، استغلال نقاط القوة والضعف في التكنلوجيا، شركة السلاسل للطباعة والنشر والتوزيع، الكويت، 1993، ص 248-245.

8- وليام كيندي، الحرب الذكية Intelligence Warfare، كتاب صدر سنة 1983، ص 87.

9- مساعد كمال، الحرب الافتراضية وسيناريوهات محاكاة الواقع، مجلة الجيش عدد253، تموز2006 http://www.lebarmy.gov.Lb/article.asp?ln=ar&id=115752 يوم 2017/04/04

10- علي مطر، الإرهاب الالكتروني في القانون الدولي، مقال مُتاح على موقع السكينة الالكتروني.
http://www.assakina.com/book/6028.html تم الاطلاع عليه يوم 2018/01/23

11- تذكر المراجع العلمية ان عالم الرياضيات نوربرت وينر Norbert Wiener هو اوّل من استخدم المصطلح في سنة 1984 اثناء دراسته للقيادة والسيطرة والاتصال في عالم الحيوان والهندسة الميكانيكية. اما اصل المُصطلح فيعود الى اللغة اليونانية kybernetes وتعني التحكم عن بُعد، اما في علم اللغة فلا اثر لها الّا ما ورد في قاموس المورّد والذي اتى بوصفها على انها ضبط للأشياء عن بُعد والسيطرة عليها، اما في ما يخص اللغة العربية فنعتقد -من جانبنا- ان اصطلاح مُصطلح "الالكترونية" بدل "السيبرانية" قد جانب الصواب ذلك بالرجوع الى عدم وجود ما يقابلها في اللغة العربية في اعتقادنا ومثال ذلك ترجمة الاتفاقية الاوربية للجريمة السيبرانية (convention on cybercrime) قد تُرجم الى (الاتفاقية المتعلقة بالجريمة الالكترونية) لهذا فإنّا نفضل استخدام مصطلح السيبرانية نظرًا لعدم وجود اتفاق الى حدّ اليوم وذلك بدليل اعتماد المُصطلح من قبل هيئة الأمم المتحدة في ترجمتها للنصوص القانونية والقرارات الدولية، فضلا عن معظم المنظمات الدولية ويأتي في أولها الاتحاد الدولي للاتصالات واللجان الدولية التابعة للأمم المتحدة وغيرها.

12- NATO Glossary of Terms and Definitions, AAP-06 Edition 2012 Version 2. (NATO) defines terrorism as “the unlawful use Or, threatened use of force or violence against individuals or property to coerce or intimidate governments or societies to achieve political, religious or ideological objectives“.https://ccdcoe.org/cyber-definitions.html2017/04/06 تم الاطلاع عليه يوم

13- تقرير المؤتمر الحادي والثلاثون للصليب الأحمر والهلال الأحمر، تحت عنوان القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، جنيف 28 من نوفمبر إلى 01 ديسمبر 2011، متوفر على موقع اللجنة الدولية للصليب الأحمر.
https://www.icrc.org/en/war-and-law/conduct-hostilities/cyber-warfare
تم الاطلاع عليه في 2017/04/06

14- منير محمد الجنبهي، امن المعلومات الالكترونية، دار الفكر الجامعي، مصر، 2002، ص 126.

15- محمد بسيوني، تهديدات مشفّرة، مقال منشور على موقع مركز المستقبل للأبحاث والدراسات، بتاريخ الخميس 11 يناير 2018. https://futureuae.com/ar-AE/Mainpage/item/3610 تم الاطلاع عليه في 2018/02/02

16- هي برمجية صممت لزيادة مجهولية المستخدم على الانترنت، فهي تُنكر هوية ونشاط المستخدم لمقاومة أساليب كثيرة من تقنيات التعقّب ومراقبة الاستخدام وفلاتر حجب المواقع.

17- FREEPTO is a Debian based operating system on a USB stick developed by hacktivist group AVANA and used, in between others, by various anarchist groups like the Spanish CNT group in Madrid selling USB thumb drives with Freepto loaded and hacker spaces in Greece and Italy that do Freepto presentations during digital security training. https://www.hacker10.com/internet-anonymity/encrypted-operating-system-for-activists-freepto2017/04/07 تم الاطلاع عليه يوم

18- أنـــــظر على سبيل المثال: دوتون، استخدام بيئة الألاعيب في دراسة سياسات الاتصالات وتطوير الإنترنت، جريدة معلومات اليوم (Information Today) 1992، نيوجيرسي، 499-517.

19- أصدر الكاتب والصحفي "عبد الباري عطوان" في عام 2015 كتابا تحت عنوان "الدولة الإسلامية.... الخلافة الرقمية"The Digital Caliphate فصّل من خلاله الاستراتيجية الالكترونية "لداعش" الدولة الإسلامية بالعراق والشام، وتناول بالتدقيق تلك الاستراتيجية بالتحليل في عدة فصول من كتابه، مفصّلا ان التنظيم الإرهابي استغل البيئة الفوضوية التي أعقبت الثورات العربية بعد عام 2011، ويرى عطوان أن تنظيم الدولة الإسلامية تتوافر لديه عناصر الدولة الثلاث من شعب وإقليم وحكومة؛ وان المشروع التي تنفذه ما هو إلّا الاستراتيجية التي بناها وسطّرها أحد منظري التنظيم "أبي بكر ناجي" في كتابه "إدارة التوحّش" الذي يناقش فيه كيفيات استخدام العنف والتوحّش من خلال مراحل تفضي في الأخير إلى بناء الدولة الإسلامية الكبرى. وقد تناول الكاتب في كتابه الأساليب التي ابتكرها التنظيم في مجال الحرب السيبرانية او الالكترونية والتي لولاها لكان من الصعب جدًّا قيام تنظيم مثل هذا الحجم في مدة زمنية قصيرة، ويرجع هذا بالأساس إلى تجنيده "لجيلا رقميًّا" بامتياز وبالاعتماد على أحدث

التكنولوجيات في التواصل او نشر الأفلام او غيرها من وسائل التنظيم في تسيير وقيادة للحرب الرقمية.

20- السند عبد الرحمن بن عبد الله، وسائل الإرهاب الالكتروني حكمها في الإسلام وطرق مكافحتها، الكتاب منشور على موقع حملة السكينة على الانترنت، بتاريخ 17 ديسمبر 2010.

21- سُمّيت "كويليام" تيّمُناً بـ -عبد الله كويليام- البريطاني الذي اعتنق الإسلام وأسّس عام 1889 أوّل مسجد ومعهد إسلامي في بريطانيا، فالهيئة مؤسّسة أبحاث مستقلة لها تأثير مهم في الخطاب العام خاصة وان العديد من الباحثين والأئمة من شتى بقاع العالم يشاركون دوريا في الدراسات التي تجريها المؤسّسة في سبيل "اقتلاع التطرّف" والتكاتف من اجل القضاء على الإرهاب، غير ان المؤسّسة تبقى لها اراء سياسية يعارضها البعض ويؤيّدها البعض الآخر.للمزيد من التفصيل انظر:

https://www.quilliaminternational.com/about

22- المادة الأولى فقرة 1(ب) من الاتفاقية الدولية لمناهضة تجنيد المرتزقة واستخدامهم وتمويلهم وتدريبهم لعام 1989.

23- اللجنة الدولية للصليب الأحمر، ملائمة القانون الدولي الإنساني في حالات الإرهاب، مقال منشور على موقع اللجنة بتاريخ 01 جانفي 2011.

https://www.icrc.org/ara/resources/documents/misc/terrorism-ihl-210705.htm

24- للاطلاع أكثر على موقف الولايات المتحدة الامريكية، انـــظر:

White House, Memorandum of February 7, 2002, Appendix C to Independent Panel Review DoD Detention Operations, Chairman the Honorable James R. Schlesinger to US Secretary of Défense Donald Rumsfeld, August 24, 2004, available online at يوم: 2017/7/22

www.defenselink.mil/news/Aug2004/d20040824finalreport.pdf

25- تقوم اللجنة الدولية للصليب الأحمر بزيارة المحتجزين الذين ألُقى القبض عليهم في إطار مكافحة الإرهاب في أماكن تحت سلطة القوات الامريكية في أفغانستان وخليج غوانتانامو منذ سنة 2002، ففي هذا الإطار صدر امر تنفيذي من رئيس الولايات المتحدة الامريكية "أوباما" سنة 2009 يؤكّد على انطباق المادة

الثالثة مشتركة من اتفاقيات جنيف 1949 لاحترام الحد الأدنى من المعاملة الإنسانية، واحترام مبدأ عدم الإعادة القسرية (يقضي بنقل المحتجزين الى سلطة قد يتعرّضون لديها لسوء معاملة)

26- بدأ مشروع الجزائر الالكترونية سنة 2009 تحت اشراف وزارة البريد وتكنولوجيات الاعلام والاتصال، وقد ضمّ البرنامج عدّة محاور من بينها التعليم الالكتروني مثل شبكة ARN كأكبر مشروع في قطاع التعليم العالي ومشروع التعليم عن بُعد Télé-Enseignement والمكاتب الافتراضية وغيرها وقد كانت آخر نتائجها الانطلاق سنة 2017 في التكوين عن بعد في الطور الثاني (الماستر) في عديد الكليات عبر الوطن، كما ضمّ المشروع تطوير خدمات مركز البحث في الاعلام العلمي والتقني CERIST وعديد الهياكل الأخرى، اما فيما يخصّ التجارة الالكترونية اين كان اول ظهور لها بالجزائر سنة 1997 عن طريق شركة "جيوكس" وتجدر الإشارة الى ان بريد الجزائر قد دخل غمار المنافسة متأخرًا بمشروع BARIDI NET غير ان الأوضاع لاتزال قيد التجربة وبالتالي الحاجة للاستثمار في هذا المجال تبقى مُلحّة، هذا على غرار عديد القطاعات الأخرى مثل الصحة ببطاقة الشفاء وقطاع العدالة بعصرنة الخدمات مثل السوار الالكتروني وغيرها بالإضافة إلى بطاقات التعريف الوطنية البيوميترية وكذا جوازات السفر، وبهذا فقد برهنت الجزائر على انها تسير بخطى مستقرة نحو الحكومة الالكترونية بيد ان هذا يحتاج بالتأكيد إلى خريطة تأمين لمعلومات هذا المجتمع الرقمي النامي والمتقدّم.

27- المؤشّر العالمي للأمن السيبراني لسنة 2017، اعداد مؤسسة ABI للبحوث بالتعاون مع الاتحاد الدولي للاتصالات. مُتاح على الرابط:

https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

28- للمزيد حول نظام المعالجة المعلوماتية والالية للمعطيات يُرجى الاطلاع على: درار نسيمة، الامن المعلوماتي وسبل مواجهة مخاطره في التعامل الالكتروني، رسالة دكتوراه في القانون، جامعة ابوبكربلقايد، تلمسان الجزائر، 2016، 314 ومـا بعدها.

29- من بين تلك التنظيمات، المرسوم التنفيذي رقم 04 – 181 المؤرخ في 06 جمادى الأولى 1425، الموافق لـ 24 جوان 2004 المتعلق بإحداث لجنة الاتصال، المرتبطة بالأخطار الطبيعية والتكنولوجية الكبرى.

30- Meriem ALI MARINA, Centre de prévention et de lutte contre la criminalité informatique et la cybercriminel « Les gendarmes du Net »،EL DJAZAIR magazine.
http://www.eldjazaircom.dz/index.php?id_rubrique=314&id_article=4567
تم الاطلاع عليه يوم 2017/08/20

31- لقد استعمل المشرّع الجزائري مصطلح السيبرانية لأوّل مرّة في القوانين الجزائرية ذات الصلة في قانون الاتصال والبريد الصادر في 2018 وبالتالي يمكن اعتبار ان المشرع قد تبنى المصطلح بصفة رسمية، غير انّه لم يوضح الى ماذا يرمي بالضبط

32- المؤشّر العالمي للأمن السيبراني لسنة 2017، مرجع سابق، ص 41.

33- المؤشر العالمي للأمن السيبراني، نفس المرجع، ص 56.

34- Anonymous declares December 11 ‹Isis Trolling Day .
http://www.wired.co.uk/article/anonymous-isis-trolling-day تم الاطلاع عليه يوم: 26 أوت 2017.

35- UNITED NATIONS OFFICE ON DRUGS AND CRIME Vienna - The use of the Internet for terrorist purposes-The Internet is a prime example of how terrorists can behave in a truly transnational way; in response, States need to think and function in an equally transnational manner".
http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

36- تقرير الأمم المتحدة الأول عن الامارة الإسلامية، الصادر بتاريخ: 15 فبراير 2016.
www.voltairenet.org/article190295.html.
قرار الأمم المتحدة الثاني عن الامارة الإسلامية، صادر بتاريخ 31 مايو 2016.
www.voltairenet.org/article1921133.html تم الاطلاع عليه يوم 27 اوت 2017

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

38- http://www.siteintelgroup.org تم الاطلاع على الموقع يوم 17 فيفري 2018.

39- Cyber Storm Exercise Report," Department of Homeland Security National Cyber Security Division", DHS, September 12, 2006. www.dhs.gov/xlibrary/assets/prep_cyberstormreport_sep06.pdf

تم الاطلاع عليه يوم 18 فيفري 2018.

40- Anna Maria Balsano, Un instrument juridique international pour le cyberespace? Analyse comparative avec le droit international de l'espace Extra-atmosphérique, Collection : Droit du cyberespace, UNESCO, 2000, P 15