المدرسة الوطنية العليا للعلوم السياسية

قسم العلاقات الدولية

الإرهاب الإلكتروني وتأثيراته الإستراتيجية على الأمن الأوروبي (1996-2022)

أطروحة مقدمة لنيل شهادة دكتوراه الطور الثالث (ل.م.د) في العلوم السياسية

تخصص: دراسات استراتيجية

إعداد الطالب:

علاء الدين فرحات

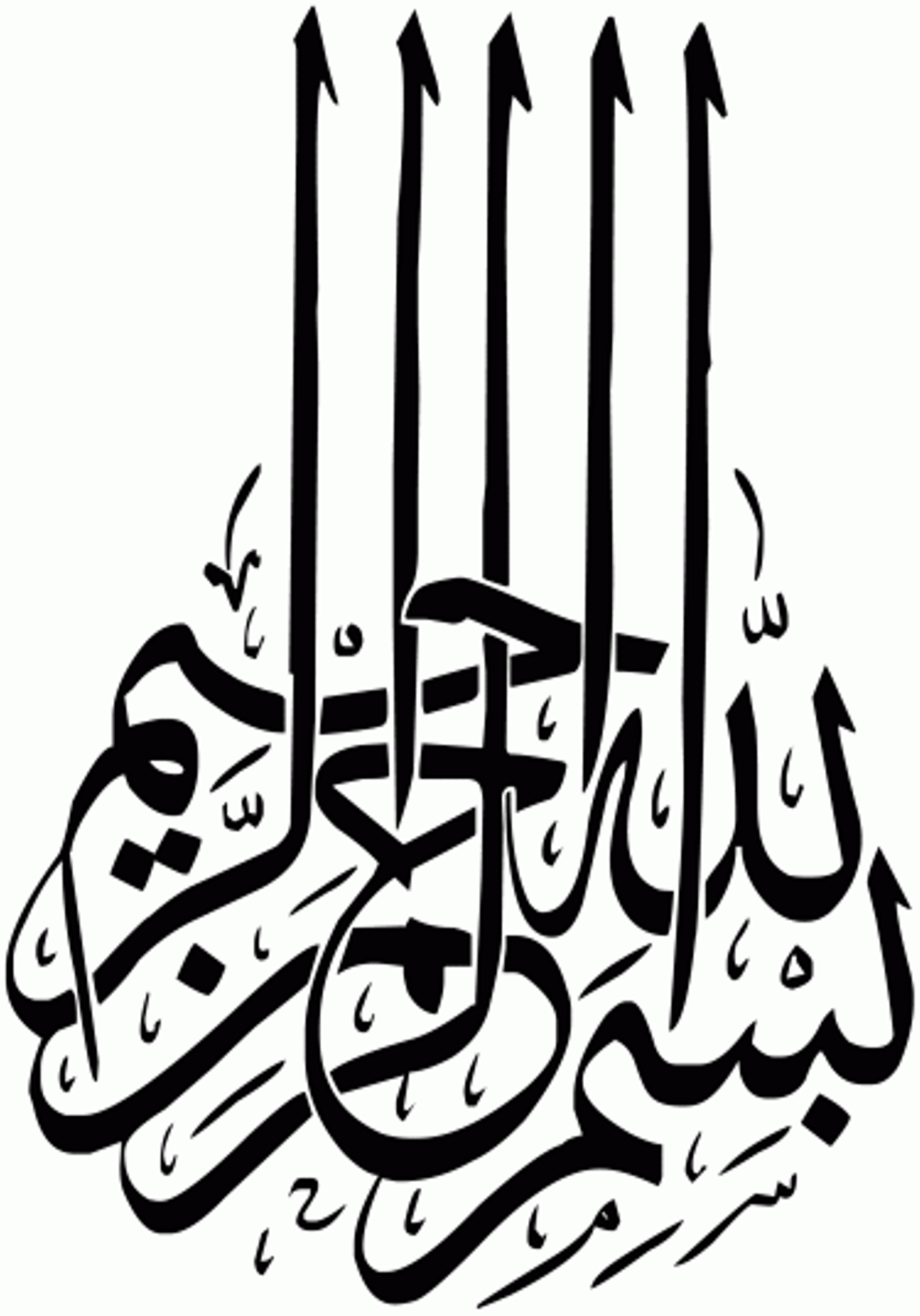
إشراف الاستاذ الدكتور:

حكيم غريب

أعضاء لجنة المناقشة

الأستاذ	مؤسسة الانتساب	الصفة
أ.د. فتحي بولعراس	المدرسة الوطنية العليا للعلوم السياسية	رئيسا
أ.د. حكيم غريب	المدرسة الوطنية العليا للعلوم السياسية	مشرفا ومقررا
أ.د. حمياز سمير	جامعة أمحمد بوقرة بومرداس	مناقشا
أ.د. مراد حجاج	جامعة أمحمد بوقرة بومرداس	مناقشا
أ.د. فليسي نرجس	المدرسة الوطنية العليا للعلوم السياسية	مناقشا
د. هارون مليكة	المدرسة الوطنية العليا للعلوم السياسية	مناقشا

السنة الجامعية: 2021 /2022


بسم الله الرحمن الرحيم

شكر وتقدير

الحمد لله حمدا لا حدود له، والشكر لله إسرارا وإعلانا.

الشكر للأستاذ المشرف حكيم غريب الذي قبل الإشراف على هذا العمل.

الشكر موصول لأعضاء هيئة التدريس في قسم العلاقات الدولية بالمدرسة الوطنية العليا للعلوم السياسية، وخاصة للكادر الاستثنائي لتخصص الدراسات الاستراتيجية.

الشكر للدكتورة عمارية عمروس على مساعدتها في إخراج هذا العمل في شكله الحالي.

الشكر موصول لكل من عرفت في المدرسة الوطنية العليا للعلوم السياسية من طلبة وعمال دون استثناء.

إهداء

إلى والداي

أمّة في شخصين

إليك أيتها الطّاهرة كماء السماء "أمي" فلا اقتباس ينصفك، ولا نص يكفي للحديث عنك، أنت الفضل، أنت الخير، أنت الكل... لك فيوضُ الدعاءِ أيّتها السّورة في مصحفِ حياتي.

إليكَ . . . العظيم "والدي".

أخوتي وأخواتي جميعا، كل باسمه..

احتراما وفخرا

خطة الدراسة

خطة الدراسة

مقدمة

الفصل الأول: الأبعاد المعرفية والمفاهيمية للإرهاب الالكتروني في سياق تحول مفهوم الأمن.

المبحث الأول: ماهية الارهاب الالكتروني.

المطلب الأول: الإرهاب الالكتروني وجدلية التعريف.

المطلب الثاني: دوافع الإرهاب السيبراني.

المطلب الثالث: خصائص الإرهاب الالكتروني.

المطلب الرابع: المفاهيم المرتبطة والمتداخلة مع الإرهاب الالكتروني.

المبحث الثاني: الإرهاب الإلكتروني القدرات وملامح الفاعلين.

المطلب الأول: القدرات السيبرانية للمجموعات الإرهابية.

المطلب الثاني: أهداف الإرهاب الإلكتروني الداخلية والخارجية.

المطلب الثالث: الاستخدامات السيبرانية للجماعات الإرهابية: فحص للتقنيات والتكتيكات.

المبحث الثالث: اتجاهات التنظير في الفضاء السيبراني: الحاجة إلى إعادة تموضع النظريات التقليدية.

المطلب الأول: الإرهاب السيبراني ونظريات العلاقات الدولية.

المطلب الثاني: الأمن السيبراني في دراسات الأمن الموسع: مدرستان للأمن وتوليف المؤسسة النظرية "مدرسة كوبنهاغن ومدرسة باريس".

المطلب الثالث: التحول في أبعاد القوة.

الفصل الثاني: الإرهاب الالكتروني في استراتيجية الأمن الأوروبي

المبحث الأول: الفضاء السيبراني وإدارة السياسات الأمنية.

المطلب الأول: الفضاء السيبراني كعنصر من عناصر الدولة.

المطلب الثاني: الثورة التكنولوجية وظهور مجتمع المخاطر الالكتروني.

المطلب الثالث: فضاء القتال الجديدة: الانتقال من فضاء حقل المعركة إلى الفضاء السيبراني.

المبحث الثاني: توظيف جماعات العنف للإرهاب السيبراني عبر الفضاء الأوروبي.

المطلب الاول: الإرهاب الجهادي.

المطلب الثاني: الإرهاب العرقي القومي والانفصالي.

المطلب الثالث: الإرهاب اليساري والأناركي.

المطلب الرابع: الإرهاب اليميني.

خطة الدراسة

المبحث الثالث: الإرهاب الالكتروني وتداعياته على الأمن الأوروبي.

المطلب الأول: الهجمات السيرانية وانعكاساتها على السيادة السيبرانية الأوربية.

المطلب الثاني: التداعيات على الأمن المجتمعي.

المطلب الثالث: التداعيات على الأمن الطاقوي.

المطلب الرابع: المخاطر الأمنية والسياسية.

الفصل الثالث: إشكاليات بناء الأمن الجماعي الأوربي (الانتقال من الأمن الصلب إلى الأمن الرخو) .

المبحث الأول: تبلور الخطاب الامني الأوروبي بشأن الإرهاب السيبراني.

المطلب الأول: بنية الخطاب الأمني للدولة الحديثة: مقاربة نقدية.

المطلب الثاني: تاريخ الهجمات السيبرانية في أوربا.

المطلب الثالث: أمن الدولة الأوربية في عصر الرقمنة.

المطلب الرابع: البنية التحتية الحرجة: الفجوة الرخوة للأمن والتكنولوجيا في المنطقة الأوربية.

المبحث الثاني: محددات الأمن الجماعي الأوربي.

المطلب الأول: جينالوجيا مفهوم الأمن الجماعي.

المطلب الثاني: الأمن الجماعي الأوروبي والتحول في طبيعة التهديدات الأمنية.

المطلب الثالث: فهم المخاطر السيبرانية المشتركة.

المطلب الرابع: الثابت والمتغير في تصور الأمن الجماعي الأوروبي.

المطلب الخامس: بين أمننه الانترنت وحقوق الإنسان .

المبحث الثالث: الأمن السيبراني الأوربي بين ثغرات السياسات والتدابير التقنية والإجرائية.

المطلب الأول: إنشاء المجال العام في الفضاء السيبراني الأوربي.

المطلب الثاني: قراءة في ملامح الدفاع السيبراني الأوربي.

المطلب الثالث: استراتيجيات الأمن والحوكمة السيبرانية.

الفصل الرابع: استراتيجية بناء الأمن السيبراني الأوربي الرهانات والتحديات.

المبحث الأول: النهج الأوروبي التعاوني الوطني وعبر الوطني لأمن الشبكات والمعلومات.

المطلب الأول: الشراكة بين القطاعين العام والخاص بشأن الأمن السيبراني.

المطلب الثاني: التعاون الدولي وثقافة الأمن السيبراني المتعدد المستويات.

خطة الدراسة

المطلب الثالث: الدفاع الحربي لحلف شمال الاطلسي وسياسات الدفاع السيبراني.

المبحث الثاني: الصكوك القانونية في أوروبا وإعادة بناء القدرات.

المطلب الأول: رؤية أوروبية جديدة لملء الفراغ القانوني في الفضاء السيبراني.

المطلب الثاني: الثقافة الوطنية للسلامة السيبرانية.

المبحث الثالث: نحو تطوير جدول أعمال بحثي حول الإرهاب السيبراني – التحديات التقنية والحلول.

المطلب الأول: تطوير السياسات وخرائط الطريق لأبحاث الجريمة الإلكترونية والإرهاب الإلكتروني.

المطلب الثاني: الطريق السيبراني إلى المستقبل – منهجية تطوير السياسات وخرائط الطريق للأمن السيبراني الأوربي.

المطلب الثالث: امكانية الوصول إلى النضج السيبراني.

خاتمة.

مقدمة

تمهيد:

مع استمرار الإنترنت والتكنولوجيات الرقمية المرتبطة في توسيع نطاقها، أصبحت البادئة "cyber" مطبقة على قائمة متزايدة من الأنشطة والظواهر المتنوعة. هذا التعدي قد فرض مجالات جديدة من الوجود الاجتماعي والسياسي وعزز مكان الإنترنت كطفل للعولمة التي غيرت بدورها القواعد والأعراف الدولية، من أجل تسهيل التدفق السريع لرأس المال والتكنولوجيا، من خلال التخفيف من الحواجز الوطنية، في حين أصبحت الجهات الفاعلة غير الحكومية تلعب دورًا أساسيًا في السياسة الدولية.

وفي اتجاه مواز للعولمة بدأ دور الدولة يعاني من عديد التغييرات. كما تم معارضة المفهوم التقليدي المقبول للسلطة، وظهر بُعد آخر أكثر إزعاجا للمنظومات الأمنية للدول، فبرز جراء التقارب بين العالمين المادي والافتراضي "تهديد جديد" يسمى الإرهاب الإلكتروني، وهو المتعلق بانتشار الأفكار الإرهابية والتخطيط للعمليات العدوانية عبر الآليات التكنولوجية الحديثة. ونتيجة لذلك، نما الخوف من أن يتمكن الإرهابيون من استغلال هذا الترابط بين العالمين ليتسببوا في الفوضى مستغلين الفضاء الإلكتروني لاستهداف البنى التحتية الحيوية، خاصة وأن مَواطن الضعف في هذا الفضاء وفيرة، والعواقب تنطوي على احتمال أن تكون مرتفعة، فالإنترنت وفر وصولاً لا مثيل له للمعلومات، سواء أكانت مشروعة أو غير مشروعة، مما يفتح فرصًا لإضفاء الطابع الراديكالي على نطاق أوسع من الناس.

في مثل هذه الظروف، أصبح عالم الإنترنت هدفًا مغريًا ومربحًا للمشروع الإرهابي الحديث، وبرز ضمن الإشكاليات العريضة التي باتت تهدد الأمن والسلم الدوليين في العقود الأخيرة. فظاهرة الإرهاب الإلكتروني كظاهرة ذات ديناميكية بارزة للغاية، مثلها مثل الظاهرة الإرهابية التي تشكل المرشح الأكبر للأمننة الكاملة، والتي تغيرت نشأتها التاريخية عدة مرات في الشكل والمحتوى، تعد إحدى أبرز الظواهر التي نتجت عن اتساع استخدام الفاعلين من غير الدول للفضاء السيبراني.

ومع ذلك فإن الإيديولوجية الإرهابية العالمية التي تجلت منذ أكثر من عقد من الزمن شهدت توسعًا في السنوات القليلة الماضية ما جعل الإرهاب أولوية أمنية عالمية، وقد أدى ذلك إلى إدخال شكل ومحتوى إرهابي "جديد" نظرًا لاتساع نطاق التهديدات اللاتماثلية، حيث لا يقتصر جوهرها الأساسي على فكرة الجرائم التقليدية، بل تمتد هذه التهديدات إلى ما هو أبعد كالتهديدات الناشئة للإرهاب السيبراني والحرب الإلكترونية. في هذا السياق، تتطور طبيعة الإرهاب بسبب الفضاء الإلكتروني، حيث تتوفر آلية

لنشر الايديولوجيا والخطاب المتطرف، وتجنيد الأفراد وإكراههم وتدريبهم، ومنصة لتخطيط وتنفيذ الهجمات ضد الحكومات والشركات والبنية التحتية الحيوية.

انطلاقا من ذلك، كان من الأهمية بمكان مُدارسة هذا الموضوع من حيث المسببات والآثار الإستراتيجية، لأن طبيعة هذه الظاهرة الصاعدة على المستوى الاستراتيجي الدولي متسمة بالتعقيد وتعدد الأبعاد، نظرا لأن زيادة الاعتماد على الفضاء الإلكتروني مرئية في جميع القطاعات العامة والخاصة وكذا العمليات الحكومية في كل الدول بما فيها أوروبا، فضلا عن الاتصالات بين المجموعات والأفراد، ونتيجة لذلك يتزايد خطر الهجمات الإلكترونية.

أصبحت أوروبا في بضع سنوات قاعدة للجماعات الإرهابية، والتي أخذت على عاتقها تطوير تكتيكاتها بما يتوافق والعصر الرقمي، كما أن أحد ملامح هذه التهديدات التي تواجه أوروبا بروز أطياف مختلفة لمجموعات تتبنى الفكر الإرهابي وجدت في التقنية سبيلا للترويج لأفكارها، أو لاستعمالها كسلاح لشن هجمات سيبراني. عزز هذا الأمر المخاوف من تحولات البيئة الرقمية حيث أصبح لدى جميع الفاعلين داخل مجتمع المعلومات العالمي القدرة على شن هجمات سيبرانية، كما صار الفضاء غير المادي مجالا لاستخدام شتى أسلحة التدمير السياسي والاقتصادي، المالي، النفسي والعسكري.

كل ذلك جعل الفضاء الالكتروني يتصدر على نحو متزايد أجندات الأمن القومي للحكومات، ولا أدَلُّ على ذلك من التركيز عليه في إستراتيجية الأمن القومي الأوربي، لما تواجهه أوروبا ودول الاتحاد الأوروبي من هجمات في الفضاء الإلكتروني على نطاق غير مسبوق، بوتيرة متسارعة، وبتعقيد يتراوح ما بين نشاط إجرامي خفيف المستوى وعمليات أكثر تطورا. وفق هذا وجب على دول المنطقة الأوروبية، أسوة بغيرها من دول العالم، الدخول في رهان مزدوج: (تقني–سياسي) و(قانوني–تشريعي) لحماية نفسها من الهجمات الإرهابية الإلكترونية وتأمين وجودها.

<u>مبررات اختيار الموضوع:</u>

يأتي اختيار موضــوع الدراســة انطلاقا من مبررات متنوعة، بعضــها ذاتي والآخر موضــوعي. بالنســـبة للمبررات الذاتية فهي ترتبط بالاهتمام الفكري والأكاديمي للباحث بدرجة أولى، خاصـــة وأن تخصص الدكتوراه هو الدراسات الإستراتيجية حيث يندرج موضوع الدراسة وتبرز أهميتُه.

أما المبررات الموضـــوعية والعلمية فتقترن بأهمية وراهنية الموضـــوع محل الدراســـة، فمع تطور أشـــكال التهديدات الأمنية وأشـــكال الحروب بالموازاة مع تطور تكنولوجيا المعلومات والاتصـــالات، بات موضـوع الأمن السـيبراني والتصـدي للإرهاب في الفضـاء السـيبراني مطروحا بقوة على أجندة السـياسـات الأوروبية، مما حفّز الباحث على اختيار هذا الموضـــوع مســـتهدفًا تقديم رؤية شـــاملة، متوازنة، وتقديم إضافة أكاديمية قد تستفيد منها مراكز البحث العربية ومؤسسات صنع القرار.

<u>أدبيات الدراسة:</u>

سيتم مراجعة النتائج والتقارير والمقالات السابقة التي كتبها باحثون آخرون، وتحليل النتائج التي توصلوا إليها قبل التوصل إلى مزيد من الاستنتاجات، فهناك عدّة دراسات قيّمة تناولت موضوع الإرهاب السيبراني والسياسات الأمنية الأوربية المتخذة لمجابهته، حيث تمت كتابة الكثير من الأعمال التي تتناول هذا الهاجس الأمني في العشرين عامًا الماضية أو نحو ذلك. ومن بين أهم المنشورات حول تأثير الإرهاب الإلكتروني على الأمن الأوربي ما يلي:

- أطروحة دكتوراه للباحثة "تين مونك" Tine Højsgaard Munk، والموسومة بـ الأمن السيبراني في المنطقة الأوروبية: الحوكمة والممارسات الاستباقية Cyber-Security in the European Region: Anticipatory Governance and Practices،[1] والمقدَّمة في كلية الحقوق بجامعة مانشستر سنة 2015. تشكل هذه الدراسة إطارا عاما للحوكمة الأوربية ومجمل التطبيقات الإجرائية المتخذة على المستوى الأوربي في مجال التشريع بالنسبة للفضاء السيبراني. ستتقاطع عديد النقاط مع هذه الأطروحة، فالبناء على تحليلاتها وأفكارها اعتبر لبنة مساعدة على بناء الأفكار المتعلقة بالموضوع المراد دراسته في هذه الأطروحة، كما تم الاستناد عليها في هندسة بعض جوانب الإطار النظري.

ترى الباحثة أن الحوكمة هي النموذج المفضل لإدارة المخاطر السيبرانية، إلا أنه لا تزال هناك مشاكل في تطوير نظام شامل قائم على الحوكمة والممارسات الاستباقية المقدمة لزيادة المرونة تجاه المخاطر السيبرانية. كما تزعم أن هذه المنطقة الأوروبية في شكلها الحالي متخلفة، فهي عالقة بين تدابير مكافحة الإرهاب التقليدية وأشكال إدارة الجرائم الإلكترونية، وهذا يخلق تحدّ فكري لفهم العلاقة المتناقضة

[1] Tine Hojsgaard Munk, ***Cyber Security in the European Region: Anticipatory Governance and Practices***, A thesis submitted for the degree of Doctor of Philosophy. University of Manchester: Faculty of Humanities, School of Law, 2015.

بين الإطارين التشريعيين. كما ترى أن تطوير حوكمة وممارسات الإرهاب السيبراني عالقٌ بين الأمننة واستخدام الحوكمة العقدية. ومن الواضح أن هناك مشكلة تتعلق بعدم وجود سياسات مصاغة بوضوح، ونتيجة لذلك يظل الإرهاب السيبراني مجزأً ومتباينًا. علاوة على ذلك فإن الإرهاب السيبراني، ظاهريا، في مأزق، حيث يُنظر إليه جوهريًا بأنه مفهوم محورُه الدولة، ومن ناحية أخرى، سعت الباحثة إلى فهم استراتيجيات الأمن السيبراني الأوروبي وأشكال الحوكمة التي طورها مجلس أوروبا والاتحاد الأوروبي، من خلال معالجة وتحليل الاستراتيجيات الحالية وأشكال الحوكمة في إطار حلف شمال الأطلسي.

بالنسبة لهذه الأطروحة فهي تركز على التأثير الاستراتيجي للإرهاب الالكتروني على المستويين الداخلي والإقليمي، في محاولة طموحة للجمع بين الرؤى البديلة، ومحاولة فهم المقاربات الأوربية للكيانات فرادى أو ضمن مركبات أمنية كالاتحاد الأوربي أو حلف شمال الأطلسي، لكي تكون قادرة على ضمان سلامة أنظمة الدول القومية، عبر آليات الدفاع السيبراني وترسانة الوسائل القانونية التي يمكن أن تلعب دورا تكميليا لليقظة والاستعداد السيبرانيين، كما تحاول هذه الأطروحة تقديم رؤية مختلفة للتأثيرات بعيدا عن الجدل المعتاد لأولئك الذين ينادون بتفوق الدولة الأوروبية.

- دراسة أخرى للكاتب الانجليزي Mikkel Vedby Rasmussen، تقدّم بها في جامعة كامبريدج عام 2006، والموسومة بـ "مجتمع المخاطر في الحرب. الإرهاب والتكنولوجيا والإستراتيجية في القرن الحادي والعشرين[2]" The Risk Society at War. Terror, Technology and Strategy in the Twenty-first Century هذه الدراسة المهمة تقدم إطارا عاما للمخاطر الأمنية التي تتشكّل جرّاء التزاوج بين الحرب والإرهاب والتطور الهائل في المجال التكنولوجي، في حين هذه الأطروحة تجمع صراحة بين تحليل الأمن السيبراني ومكافحة الإرهاب، الأممر الذي جعلها أكثر تخصصية ودقة في مدارسة أوجه التحدي والاستجابة الأوروبية جراء تأثيرات الإرهاب الالكتروني، وتسعى في نهاية المطاف إلى فهم المجتمع الأمني الأوروبي، حيث تلتقي القطاعات الخاصة بالعامة وكل الهياكل المعيارية المختلفة حول مجموع المعايير وقواعد السلوك الأمني لحماية البنى والقيم الأوروبية من التهديدات السيبرانية.

[2] Mikkel Vedby Rasmussen, ***The Risk Society at War Terror, Technology and Strategy in the Twenty-First Century***,(UK: Cambridge University Press, 2006).

- مقال سارة سكاليت Sarah D. Scalet رئيسة تحرير مجلة CSO، والمساهمة في مجلة CIO، وخبيرة أمن المعلومات، بعنوان : "الإرهاب الإلكتروني هو حرب الجميع"[3] Cyberterrorism Is Everyone's War (أكتوبر 2001)، حيث تناولت مقدمة عامة توضح أن عنصر المفاجأة كان أفضل سلاح يستخدمه الإرهابيون حتى الآن. وشددت على الحاجة إلى المؤسسات الأمنية التي تحكم الإنترنت لإعداد نفسها لاحتمال أن يستخدم الإرهابيون الإلكترونيون نفس العنصر ويهاجموا الأنظمة الإلكترونية الحاسمة في أي مكان وفي الوقت الأقل توقعًا. ومع ذلك، تعترف الكاتبة بأن احتمال وجود عمل مفصل للإرهاب السيبراني لا يزال إلى حد كبير احتمالًا متخيلًا، أما مسعانا البحثي فقائم على فحص الدلالات الضبطية التي يقدمها مفهوم الإرهاب البسيبراني في الفضاء الأوروبي وهذا بتقديم تفسيرات تقنية، سياسية، أمنية لفعاليته وفاعليته، وكذا تحليل لتوجهات الحوكمة الأمنية الأوروبية المتعددة الأطراف في سياق بعد الحوادث التي شهدت استخدام الإرهابيين للتقنية كوسيلة أو كهدف، وتقديم محاولة لصياغة فهم امبريقي لمستويات التفاعل بين القطاعات في سياق تنظيم الفضاء السيبراني وبناء منظومة مؤسساتية وقانونية رادعة.

ثاني جناح لفكرة التأثير الاستراتيجي للإرهاب الالكتروني على البنى التحتية الرقمية الأوربية يمثله بعض الباحثين الذين ينفون فكرة وجود تأثير استراتيجي للإرهاب السيبراني على الأمن الأوربي، مثل دراسة للباحث في معهد الولايات المتحدة للسلام غابرييل وايمان Gabriel Weimann، والذي يرى في مجمل دراسته الصادرة في ديسمبر 2004 والموسومة بـ 'Cyberterrorism – How real is the threat'[4]، حيث رسم هذا التقرير صعود الانجراف السيبراني إذْ يفحص الكاتب الأدلة التي استشهد بها أولئك الذين يتوقعون حدوث كارثة سيبرانية وشيكة. ويؤكد غابرييل أن العديد من هذه المخاوف مبالغ فيها، حيث لم يتم حتى الآن تسجيل أي حالة من حالات الإرهاب السيبراني.

ينطلق الكاتب في تحليل الموضوع من خلال محاولة تفسيره لفكرة أن الدفاعات الإلكترونية أقوى مما يفترض الارهابيون عمومًا. ومع ذلك، فإن التهديد المحتمل لا يمكن إنكاره ويَظهر أنه من المرجح أن يزداد، مما يجعل الأمر أكثر أهمية للتغلب على الخطر دون تضخيمه أو التلاعب به.

---

[3] Sarah D. Scalet, Cyberterrorism Is Everyone's War, in: CSO (11 October 2001), In: http://www.csoonline.com/alarmed/10112001.html

[4] Gabriel Weimann, ***Cyberterrorism – How real is the threat***, United States Institute of Peace, Volume 31, 2004.

وهو ما تناوله هذه الأطروحة في بعض جزئياتها، فالإرهابيون استعملوا التقنية بشكل بدائي لحد الآن على أصعدة وأوجه محددة، يظهر من خلالها أن إلحاق إصابات جماعية وأضرار مادية غير مرجح إلى حد ما من خلال فيروسات وشبكات الكمبيوتر. ومع ذلك، تجادل الدراسة بأن التهديد الحقيقي للإرهاب السيبراني يكمن في استخدام الإنترنت من قبل المنظمات الإرهابية للتواصل، التجنيد، جمع الأموال والمعلومات الاستخبارية حول الأهداف المستقبلية المحتملة. هذا يستبعد الضرر المادي المحتمل الذي يمكن أن تسببه فيروسات الكمبيوتر المصممة لهذا الغرض لكن لا ينفيه، وسيتم تقديم سيناريوهات محتملة لما يمكن أن تسببه الاستخدامات الإرهابية للأنترنت، فهناك بوادر لتطور وتوسيع نشاطاتهم في البيئة الرقمية نظرا لعامل الجذب الذي يوفره الفضاء السيبراني، كما أن هذه الأطروحة تقدم دراسة معمقة للأمن السيبراني الأوربي والميكانيزمات التي تعالج الحصانة السيبرانية التي تمثلها آليات الإنذار المبكر والاستجابة.

<u>إشكالية الدراسة:</u>

انطلاقا مما سبق فإن مَشْكَلة «Problématisation» هذا الموضوع، من هذه الزاوية، تمكّننا من فهم الأثر الاستراتيجي للإرهاب الالكتروني على أمن واستقرار الدول الأوروبية من خلال تلك المشاكل والتحديات التي ولّدها التزاوج بين الفكر الإرهابي وثورة تكنولوجيات المعلومات والاتصالات والرقميات. وبالتحليل، ستدرس هذه الأطروحة واقع الأمن الأوربي وبعض الحالات التي تتقاطع ومضمون الأطروحة، المقاربة الأمنية الأوربية وكذا الاستجابة لتلك التحديات الإستراتيجية، ووفقا لذلك تأتي هذه الدراسة لتعالج الإشكالية التالية:

- **هل استطاعت أوروبا بناء إستراتيجية متماسكة لأمنها الجماعي لمجابهة التأثيرات الأمنية للإرهاب السيبراني؟**

وتتفرع عن الإشكالية الرئيسة للبحث مجموعة من الأسئلة والتساؤلات الفرعية كما يلي:

- ما المقصود بالإرهاب الإلكتروني؟
- ما الآلية التي تلجأ إليها الجماعات الإرهابية لتحقيق أهدافها عبر الانترنت؟ بعبارة أخرى، كيف يؤدي الانترنت دوره السلبي في تحقيق أهداف الجماعات الإرهابية؟

- ما هي الأهداف الأكثر ضعفا للإرهابيين السيبرانيين؟ وما الذي يشكل أهمية الأهداف وحجم التهديد؟
- كيف أثّر الإرهاب الإلكتروني على الأمن الأوربي؟ وما هي أبرز صور الاستجابة؟
- هل يمكن اعتبار نجاعة ترسانة القوانين والتشريعات الحالية للاتحاد الأوروبي في مجال الأمن أداةً فعالة في مكافحة الإرهاب السيبراني؟

فرضيات الدراسة:

للإحاطة بجوانب الدراسة يمكن البناء على الفرضيات التالية كمنطلق لعملية تحليلية للخطاب الأمني الأوربي تجاه ظاهرة الإرهاب الالكتروني:

- **ترتبط تأثيرات الإرهاب السيبراني على الأمن الأوروبي بشدة التهديد وحدود انتشاره، وبمدى قوة منظومة الأمن الجماعي الأوروبي.**

أما الفرضيات الفرعية فهي كالآتي:

– بفعل التشابك الحاصل في جوهر ظاهرة الإرهاب غير المتفق على تعريفها في المجتمع العلمي وتداخلها مع مصطلحات أخرى يصعب فهم الأبعاد الأنطولوجية والابستيمولوجية والأكسيولوجية لموضوع الإرهاب السيبراني.

– ترتبط رهانات وتحديات السياسات الأوروبية الخاصة بالأمن السيبراني بخصوصية التهديد من جهة، والثغرات القانونية والإجرائية من جهة أخرى.

– ترتبط الاستجابة الأمنية الأوربية السيبرانية بوجود تأثير استراتيجي للإرهاب السيبراني والذي فرض تغيرات جذرية على منظومة الأمن والفكر الأمني الأوربي.

– بفعل الجهوزية الأمنية الإلكترونية للدول الأوربية لم تتأثر البنى الحيوية (الأمنية، السياسية والاجتماعية).

حدود الدراسة:

في سعينا إلى رسم حدود الدراسة وتفاديا لخروج المسعى البحثي المقدم عن أطره الناظمة، ارتأينا ضـــبط المضـــمون من خلال فترة زمنية تمتد من بداية الألفية حتى وقت كتابة هذه الدراســـة، وقد وقع

الاختيار على هذه الفترة لأنها تُبرز بوضوح بدايات الاهتمام الأوروبي بالتهديدات السيبرانية وفي مقدمتها الإرهاب الإلكتروني، سواء من حيث النصوص القانونية، السياسات، الهياكل والمؤسسات، وغيرها من التدابير، بداية من مدارسة الموضوع كتهديد أمني ناشئ في مؤتمر وزراء خارجية الدول الأوربية الذي ناقش قضية الإرهاب في باريس 1996، ووافق المؤتمر على إصدار نداء إلى كل دول العالم لملاحظة أخطار الإرهاب الالكترونية، والإرهاب المتشابك عبر الأنظمة وشبكات الاتصال لتنفيذ أعمال إجرامية، ودعى إلى ضرورة إيجاد وسائل متسقة مع القانون الدولي لمنع مثل هذه الجرائم، لتمتد حدود دراستنا لوقتنا الراهن[5].

بالنسبة للحدود المكانية في ظل بيئة أمنية أوروبية تراوح في هندستها بين نظام وستفالي بفواعل أوروبية خارج الاتحاد الأوروبي لكنها تعتبر جزء من المعادلة، أسس لها النظام بعد الوستفالي وقارب لها، وبين نظام يسوق لهوية أمنية ما بعد وستفالية بمؤسساته واستجابته الأمنية، لهذا فقد جرت مدارَسة الموضوع من خلال الاتحاد الأوروبي باعتباره الوعاء او الحيز الجغرافي الخاص للدراسة، كبنية وظيفية، وككيان سياسي جامع، إلا أنه، ولضرورات بحثية، تم التطرق إلى أنساق التأثير والاستجابة للوحدات السياسية الأوروبية (الدول الأوروبية فُرادى) داخل الاتحاد، مع الإشارة إلى بعض الحالات الأوربية خارج الاتحاد للضرورة البحثية.

أما حدود الدراسة الموضوعية فتتمثل في ضبط مقاصد الموضوع ودلالاته بناءً على السياقات المعرفية وفهم وحدات التحليل التي تساعد على دراسة أنماط الاستجابة الأمنية الأوروبية لاستيعاب خطر الهجمات السيبرانية الإرهابية، الأمر الذي يعيد النظر في صناعة السياسات، العمليات والممارسات الأمنية الأوروبية لمواكبة هذه التغيرات في التهديدات، استنادا على تغير أشكال ووكلاء التهديد على عدة مستويات وطنية، إلى أخرى اقليمية وعالمية، بما يستلزم قابلية تجزؤ المساهمات الأمنية بين عدة فواعل، بما يشمله ذلك من سياسات وتشريعات لمواجهة تأثيرات هذا التهديد على نطاق واسع داخل المنظومة الأوروبية.

[5] أحمد محمد صالح، ***أنفوغرافيا الأنترنت وتداعياتها الاجتماعية والثقافية والسياسية***، (القاهرة، دار كتب عربية، 2007)، ص 417-419.

الإطار النظري:

تعتمد دراسة الإرهاب بشكل عامّ على أُطر نظرية تتداخل فيما بينها، بهدف بلورة تحليل يساعد على فهم وتحليل الظاهرة موضوع الدراسة. فيما يخص هذه الأطروحة، ولتحليل الاستراتيجيات الأوربية الأمنية القائمة، جرى الاعتماد على الإطار النظري التالي:

- **النظرية الواقعية:**

جرى اعتماد النظرية الواقعية بقدرتها التفسيرية التي تناسب طبيعة البحث، حيث يرى الواقعيون في الإنترنيت نظام فوضوي يتطلب استعمال القوة لردع التهديدات فيه، وأن الفضاء السيبراني ككل أصبح ساحة صراع لا تختلف عن ساحة الصراع التقليدية، كما تحاجج بوجود دول تتوخى الحذر وتعامل غيرها من الدول بعدم الثقة، بما يعني أنها تزيد من قدراتها الدفاعية (المعضلة الأمنية).

- **النظرية الليبرالية:**

الاعتماد على التصور الليبرالي يقود إلى الحديث عن التعاون الدولي كسبيل للحد من مخاطر الإرهاب السيبراني وتأمين المجال الإلكتروني، مع إشارة إلى تعدد الفاعلين (منظمات دولية حكومية وغير حكومية على سبيل المثال) إضافة إلى الدولة التي تظل محور العلاقات الدولية، التي لن تستطيع أن تحفظ أمنها بمعزل عن التعاون المؤسساتي، لهذا كان توظيف النظرية اللبرالية وفق ميتا منظار عقلاني أساسي في حقل العلوم لسياسية بأدواته التفسيرية التي أعطت قوة تفسيرية يُفْهَمُ من خلالها الإجماع الأوروبي كضرورة حتمية لمواجهة المخاطر السيبراني وعلى رأسها الإرهاب.

- **النظرية البنائية:**

وفقا للبنائية فإن الإنترنيت أداة هامة لتطوير هوية رقمية لأي دولة أو أي جهة فاعلة، كما تؤكد على أهمية الرموز والأفكار في صلتها بثقافة الإنترنت، وبالتالي ضرورة أن تتطور التفاعلات بين الفاعلين (من الدول وغير الدول) بما يناسب العصر الرقمي، الأمر الذي يجعل من توظيف طروحات البنائية رافعة نظرية تؤدي إلى فهم معمق لبنية الظاهرة الإرهابية في الفضاء السيبراني، كما تنادي البنائية بضرورة تفعيل آليات الدبلوماسية الرقمية لخلق بيئة ثقة في هذا العالم الافتراضي.

- **مدرسة "كوبنهاغن*":**

سعت هذه المدرسة الفكرية إلى معالجة جانب من الفجوة في الدراسات الأمنية ممثلة في النّزعة نحو توسيع وتعميق سرديات الامن، واحداث نقلة ابستيمولوجية عبر تنقيح وإعادة صياغته ليتماشى مع التّحول الاستراتيجي الذي مثّلته نهاية الحرب الباردة و " تفسير الوضع الأمني بناءا على تحول وحدات التحليل الأمني، ففهمها للأمن كطريقة استطرادية ذات هيكل بلاغي وتأثير سياسي معين يجعلها مناسبة بشكل خاص لدراسة تشكيل وتطور خطاب الأمن السيبراني الأوربي. كما أنها تعنى بمفهوم الأمن المجتمعي والذي يعرّفه "أولي وايفر" Ole Waever بأنه "قدرة المجتمع على استمرار وتماسك شخصيته الأساسية في ظل الظروف المتغيرة والتهديدات المحتملة أو الفعلية"، إلى جانب مفهوم "الأمننة" Securitization الذي يراد به إضفاء البُعد الأمني على مسألة ما (غير أمنية)، وتصويرها كتهديد وجودي شامل لدولة ما أو أمة.

انطلاقا من ذلك فإن فهم بناء التهديدات السيبرانية من خلال التعرف على القطاع السيبراني يعطي ديناميكية معينة لعملية الأمننة، ويسمح أيضًا بالتمييز بين اتجاهات الأمننة والعسكرة التي أتاحت البناء الأوسع للتهديدات في الفضاء الإلكتروني. وقد أضفت مدرسة كوبنهاغن الطابع الأمني على الفضاء الإلكتروني حيث تجادل بأن التهديد الأمني هو بناء اجتماعي لا يخضع للأنطولوجيا البنيوية[6]، وأن التحيز العسكري والدولي للدراسات الإستراتيجية مفتوح هنا لأشياء مرجعية جديدة ومتنوعة ونظرة نقدية، بنائية/ما بعد بنيوية، بما يجعل ذلك وثيق الصلة بموضوع الاطروحة.

---

*عادةً ما تُؤخذ مدرسة كوبنهاغن للإشارة أولاً وقبل كل شيء إلى العمل الذي قامت به منذ عام 1985 مجموعة بحث "الأمن الأوروبي" في معهد أبحاث السلام في كوبنهاغن، ولا سيما سلسلة الكتب الجماعية الخاصة بها Egbert Jahn :و Pierre Lemaitre و Buzan, Ole Wæver، تم بناء ما يسمى بمدرسة كوبنهاغن في الدراسات الأمنية حول ثلاث أفكار رئيسية: 1) الأمننة ، 2) القطاعات الأمنية و 3) المجمعات الأمنية الإقليمية، صاغ بيل مكسويني Bill McSweeney اسم مدرسة كوبنهاغن في مقال مراجعة نقدي تحول إلى: بيل مكسويني "**الهوية والأمن: بوزان ومدرسة كوبنهاغن**" ، في دورية الدراسات الدولية.

أنظر:

Bill McSweeney, "Identity and security: Buzan and the Copenhagen school", ***Review of International Studies,*** Vol. 22, N1 (1996), pp.81-94

[6] Ole Wæver, Aberystwyth, Paris, Copenhagen New 'Schools' in Security Theory and Their Origins between Core and Periphery. Paper presented at the annual meeting of the International Studies Association, Montreal, March 17-20, 2004, p. in: https://cutt.us/tLfV2

ويستلزم استخدام نظرية الأمننة الاعتراف بحدودها النظرية، وفهم كيفية ارتقاء موضوع معين إلى الأجندة الأمنية، ويشمل هذا النهج المتغيرات المجتمعية للأمن، إلى جانب عملية تكوين التهديدات. ومن الممكن تطوير إطار نظري في هذا الصدد يسهّل فهم الروابط بين الخطابات الأمنية وكذلك الآثار السياسية والمعيارية* لبناء القضايا السيبرانية كمشكلات أمنية بدلاً من كونها سياسية واقتصادية وإجرامية، أوتقنية "بحتة".

- **مدرسة باريس الأمنية:**

تغطي هذه الدراسة جوانب مختلفة من جدول أعمال الأمن، حيث قدّمت استبصاراتها في هذا الشق من خلال إدماج ما يسمى بمقاربة "مهنيّي الأمن" التي تُعنى بمواجهة التهديدات الأمنية المعاصرة بحوصلة من التقنيات والاستراتيجيات المختلفة، والتي تحاول تكييف مفهوم الأمن مع التطورات التكنولوجية المستجدة وطبيعة التحديات المعاصرة التي تواجه الدُول في عصر العولمة، كما تعنى بمدارسة الدمج بين الأمن الداخلي والخارجي، والذي يعد بمثابة قلب هذا الحقل الأمني نظرا للأدوار التي تلعبها الوكالات الأمنية والتي تبدو مناسبة للتخفيف من حدة التهديدات، وذلك بهدف إدارة المخاطر القائمة على قياس وتقييم والتقليل من حدة المخاطر، فالإستراتيجية المتبعة في عالم ما بعد الحادي عشر من سبتمبر 2001 تقوم ليس على أساس مواجهة خطر ملموس وإنما التدخل قبل أن يتفاقم هذا الخطر ويتحول الى تهديد يصعب حله.

وعليه، ووفقا لمدرسة باريس وعن طريق أتمتة قطاع الشرطة والقطاعات المتقاطعة معه، ستحاول في ذلك تحديد اليات المراقبة التي وفرها وأسس لها الذكاء الاصطناعي كأداة أساسية في تحديد هوية مرتكبي أعمال العنف والحوادث الإرهابية، ومنه يتوجب على الدول الأوربية الأخذ بهذه الأفكار عبر التنسيق بين مختلف المهن الأمنية لمواجهة التهديدات السيبرانية الإرهابية، وإيجاد استجابة أمنية مناسبة عبر تفعيل المخابر العلمية وتكثيف التعاون في مجال المراقبة، وكذا العمل وفق آليات تكنولوجية ردعية مناسبة.

بالإضافة إلى ما ذُكر آنفًا، تتم الاستعانة بما يلي:

*نستخدم كلمة "معيارية" للإشارة إلى السياسات والهويات وأنماط الحكم التي تستدعيها عمليات الأمننة.

- نظرية مركب الأمن الإقليمي Regional Security Complex Theor : وذلك نظرا لتعدد مستويات التحليل في العلاقات الدولية، والحاجة إلى نظرية يمكن إسقاطها على الأمن الأوروبي في ظل التهديدات المشتركة التي تواجهها القارة ككل.

بالتالي فقد سمح الجمع بين هذه النظريات بمقاربة شاملة لدراسة ظاهرة معقدة مثل الإرهاب السيبراني، لتحديد خصائصها من بين الظواهر والتهديدات الأمنية الأخرى، وتحديد المجالات ذات الأولوية لمكافحتها.

الإطار المنهجي:

تدفع الخلفيات والأبعاد السياسية والاجتماعية والاستراتيجية، وكذا الأمنية المتعلقة بدراسة الإرهاب الإلكتروني المعقدة، بالإضافة إلى تتبع العوامل المتدخلة في صيرورة الأحداث داخليا، إقليميا ودوليا، والتداخل فيما بينها، إلى الاعتماد على أكثر من منهج، بهدف دراسة وتحليل موضوع البحث، بشكل يسمح بإجابة منطقية على الإشكالية المطروحة واختبار للفرضيات الموضوعة. ونظرًا لطبيعة الموضوع، وتحقيقًا لأهدافه، فقد تم الاعتماد على المناهج العلمية التالية:

- **المنهج الوصفي:** يقوم على دراسة الواقع، ويهتم بوصفه وصفًا دقيقًا، كما يعبر عنه كميًا لأن التعبير الكمي يعطي وصفًا رقميًا يوضح مقدار الظاهرة أو حجمها ودرجات ارتباطها مع الظواهر المختلفة الأخرى. لهذا فهو مناسب لمعرفة الظاهرة الإرهابية، وكمحاولة لاستجلاء تجلياتها السيبرانية وكشف أبعادها، وإماطة اللثام عن المخاطر الكامنة وراءها.
- **منهج دراسة الحالة:** ولأن كل ظواهر العلوم السياسة تدخل ظمن دراسات الحالة، استخدعم من الناحية العملية هذا المنهج تركيز البحث على دراسة المنطقة الأوربية، رغبةً في الحصول على نتائج ومعلومات تفصيلية في بيئتها الأمنية، الاقتصادية، الاجتماعية والثقافية، مع التركيز على للاتحاد الأوربي كوحدة وفاعل أمني، وبمؤسساته كمصدر للاستجابة الأمنية والتشريع.
- **المنهج التحليلي:** هو منهج عام يراد به تقسيم الكل إلى أجزائه وردّ الشيء إلى عناصره المكونة له، فالتحليل يعني تقسيم الكل أو الظاهرة المعقدة وتفكيكها إلى الأجزاء التي تكونها. وفقا لذلك سيتم تحليل كافة مستويات التأثير الأمني، إضافة إلى استقراء الوقائع الجزئية (المنهج الاستقرائي) وترتيبها داخل نسق ينتهي إلى آليات للتنفيذ، وسيكون من شأن ذلك أن يسهم في تقديم الحلول الملائمة للمشكلة محل الدراسة.
- **المنهج التاريخي:** بحيث يتم الاعتماد على بعض تقنياته للضرورة البحثية وبما يفيد سياق الدراسة.

الإطار المفاهيمي:

تعد عملية ضبط المفاهيم المركزية التي تهيكل موضوع البحث خطوة غائية ودالة تجنّب الباحثَ التأويلات المتباعدة في المعنى والفهم، وتمكّنه من تَمَثُّل مدلول المفاهيم على وجه الدقة والمضبوطية[7]. على هذا الأساس، سيتم التركيز على ثلاثة مفاهيم محورية جرى البحث في مضامينها في سياق هذه الدراسة وهي كالآتي:

- **الإرهاب الالكتروني:**

هو مفهوم صاغه باري كولين Barry Collin ، زميل أبحاث أول في معهد الأمن والاستخبارات في كاليفورنيا، في ثمانينات القرن الماضي، ويقصد بمصطلح "الإرهاب الإلكتروني Cyberterrorism " الإشارة إلى التقاء الفضاء الإلكتروني والإرهاب. وفي عام 1998، نشر المشروع العالمي للجريمة المنظمة التابع لمركز الدراسات الإستراتيجية والدَّولية في واشنطن CSIS تقريرًا بعنوان "جرائم الإنترنت والإرهاب الإلكتروني والحرب الإلكترونية: تجنب حدوث ووترلو إلكترونية 'Cybercrime, Cyberterrorism and Cyberwarfare: Averting an Electronic Waterloo'، كان أولَ مساهمة رئيسة في هذا المجال.

لتأتي بعده عديد المساهمات التعريفية، والتي أكدت أنه مثله مثل مفهوم الارهاب مفهوم محمّل بالقيمة، ومتأثر بالآراء والأفكار الشخصية[8]، ومثير للجدل، رغم هذا يمكن تعريف الإرهاب الالكتروني او السيبراني على أنه استخدام الجماعات المتطرفة والارهابية للوسائل التقنية والتكنولوجية كهدف، أو كوسيلة بدوافع سياسية، أو عرقية أو دينية عن طريق التجنيد، التمويل، الدعاية بغية الوصول لأهداف سياسية.

---

[7] بلقاسم أمين بن عمرة، "مقترب ايتيقي للفضاء السيبراني نظرية العدالة عند جون راولز أنموذجا"، ***مجلة الناصرية للدراسات الاجتماعية والتاريخية***، مجلد 10، عدد 2 (ديسمبر 2019)، ص 680-727.

[8] أسامة إفراح، "الظاهرة الإرهابية أجيال الحروب الجديدة العلاقة التفاعلية"، ***مجلة السياسة العالمية***، مجلد 6، العدد 1،(2022)، ص: 789-801.

- **الفضاء السيبراني:**

تم تعريف "الفضاء الإلكتروني" بأنه "مجال عالمي داخل بيئة المعلومات، يتكون من شبكة مترابطة من البنى التحتية لتكنولوجيا المعلومات، بما في ذلك الإنترنت وشبكات الاتصالات وأنظمة الكمبيوتر والمعالجات ووحدات التحكم المضمنة"، كما يشار إليه بوصفه أنه: "ليس مكانًا ماديًا، بل إنه يتحدى القياس في أيّ بُعد مادي أو متواصل في الفضاء الزمني، فهو مصطلح مختصر يشير إلى البيئة التي تم إنشاؤها عن طريق التقاء الشبكات التعاونية من أجهزة الكمبيوتر وأنظمة المعلومات والبنى التحتية للاتصالات التي يشار إليها عادة باسم شبكة الويب العالمية[9].

كما يمكننا القول أن الفضاء السيبراني يعتبر المجال الرقمي الذي قامت الدول بترقيته ليصبح فضاء أمني، يُخاض فيه العديد من الحروب والهجمات الرقمية، وهو مجال مركّب يشمل كل البنى التحتية الحرجة من (أجهزة الكمبيوتر، أنظمة الشبكات والبرمجيات، حوسبة المعلومات، نقل وتخزين البيانات)، كما يمكن القول أن مسألة تحديد مفهوم (الفضاء السيبراني) هي مسألة نسبية تتوقف على طبيعة إدراك وفهم كل دولة لأمنها القومي

- **الأمن السيبراني:**

تعرّف الوكالة الأوروبية (ENISA) الأمن السيبراني بأنه "حماية المعلومات، أنظمة المعلومات، البنية التحتية والتطبيقات التي يتم تشغيلها علاوة على ذلك من تلك التهديدات المرتبطة بملف البيئة"[10]

كما يعرف الأمن السيبراني على أنه مجموع الآليات والسياسات والمفاهيم الأمنية التي تهدف إلى حماية الأصول والبنى التحتية الحيوية من أي هجوم محتمل، أو من التلف أو الوصول غير المصرح به لقواعد البيانات، لضمان وجود واستمرارية مجتمع المعلومات لدولة ما، أو مجموعة من الدول، وضمان وحماية الفضاء الإلكتروني من الإرهابيين او المجرمين أو الاستخدام غير المصرح به للبيانات

[9] Heinegg, Wolff Heintschel von, "Legal Implications of Territorial Sovereignty in Cyberspace", 4th International Conference on Cyber Conflict", Faculty of Law Europa-Universität, Frankfurt (Oder), Germany, 2012, p-p :7-19

[10] Dominika Giantas, Cybersecurity in the UE: Threats, Frameworks and Future Perspectives, Laboratory of Intelligence and Cybersecurity: Working paper series N.1 (September 2019), p.8.

الإلكترونية[11]، كما يمكن تعريفه بأنه "النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن إمكانات الحد من الخسائر والأضرار التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ما كان عليه بأسرع وقت ممكن، بحيث لا تتوقف عجلة الإنتاج، ولكي لا تتحول الأضرار إلى خسائر دائمة"[12].

أهمية الدراسة:

يقدم البحث نفسه كمساهمة في اثراء الدراسات الأمنية، فتكمن قيمته المعرفية في استحضار المتغيرات التي يتضمنها العنوان، من "الإرهاب الالكتروني" و"الأمن الأوروبي"، وكذا التوليف بين متغيرين شكلا معا مادة ابستمية دسمة حاولت ضبط مفهومين لموضع تداول اكاديمي لطالما أثير خلال العقدين الماضيين، فقد أدى كلاهما إلى انتاج أدبيات واسعة، يأتي بحثنا يكون أحدها، يجب أن يكون واضحًا أن الأمن السيبراني والهجمات الإرهابية الإلكترونية وأمن الشبكات واستراتيجيات الدفاع هي بعض الاهتمامات الحكومية والأمنية المركزية في القرن الحادي والعشرين، الأمر الذي يؤكده إدوارد سنودن Edward Snowden، المتعاقد السابق مع وكالة الأمن القومي، عند حديثه عن الأهمية التي توليها الجهات الأمنية في "إتقان الإنترنت" من أجل ضمان حصرية السيطرة على بنيتها التحتية.

على أساس ذلك، تنبع أهمية الدراسة من كونها ستحاول تقديم رؤية دقيقة وتصور شامل للتأثير الذي يحدثه الإرهاب الالكتروني، ومنه الاطلاع على التصور الأوربي لمجابهته، كما تُعتبر الدراسة استكشافيةً تسعى إلى رصد جريمة الإرهاب الإلكتروني، وديناميكيات وتعقيدات استراتيجيات الأمن السيبراني في أوروبا، وهي أيضا دراسة تقييمية تسعى إلى تقييم جهود الدول الأوربية في مجال مكافحة جريمة الإرهاب الإلكتروني، الأمر الذي يتطلب أطرا تحليلية جديدة تساعد في فهم الأحداث والمتغيرات.

---

[11] بارة سمير، "الأمن السيبراني في الجزائر"، ***المجلة الجزائرية للأمن الانساني***، العدد الرابع،) جويلية 2017), ص ص : 255 – 280.

[12] زينب الحيدري، ***الأمن السيبراني المخاطر التحديات، المواجهة***، (مصر: دار الشرق للطباعة والنشر والتوزيع، 2019) ، ص 43.

أهداف الدراسة:

هناك القليل من الأبحاث حول استجابة الاتحاد الأوروبي لقضية الإرهاب السيبراني، لذلك تساهم هذه الأطروحة في مجال صغير ولكنه متزايد من الأدبيات التي تحلل دور الاتحاد الأوروبي كجهة فاعلة إقليمية في مجال الأمن السيبراني، من خلال تقديم تحليل معمق لكيفية تصور الاتحاد الأوروبي للتهديد الناجم عن الإرهاب السيبراني وسبل الاستجابة له، كما تسعى هذه الدراسة إلى بلوغ مجموعة أهداف علمية وأخرى عملية، عبر محاولة معالجة واستكشاف بعض المخاوف المتعلقة بالتهديدات غير التقليدية التي أبرزها العصر الرقمي. وبالتالي الإحاطة بالتهديدات والآثار التي يشكلها الإرهاب السيبراني بالنسبة للدول الأوربية، خاصة وأن الإرهاب قد بدأ يحظى باهتمام أكاديمي وأمني أوسع في أعقاب هجمات الحادي عشر من سبتمبر 2001.

الأهداف العلمية:

تتمثل في الآتي:

- تقديم رؤية عميقة لظاهرة الإرهاب الإلكتروني من حيث جذورها وتتبُّع مسارها، سواء من حيث التقنيات والأساليب والأهداف، أو من حيث الأُطُر النظرية للفضاء السيبراني ككل وموقع الإرهاب الإلكتروني في ساحة الصراع الدولي.
- معرفة كيف يمكن للهجمات والتهديدات الإرهابية السيبرانية أن تكون مسيئة ومنتهكة لأمن الدول ومستخدمي الانترنت.
- التعرف على التحديات الرئيسَة للفضاء السيبراني وتأثيرات الإرهاب الإلكتروني على البنى التحتية والمجتمعية في البلدان الأوربية، وبالتالي السياسات والاستراتيجيات التي يتبعها الاتحاد الأوروبي من أجل أن تكون أكثر فاعلية واستدامة للدفاع عن قيمه ومواطنيه في الفضاء السيبراني.

الأهداف العملية:

تبرز في توضيح مدى نجاعة الفهوم التي تقدمها "الاستجابة الأمنية الأوروبية"، من خلال آليات التعاون الأمني بين القطاعات، والقدرة على استيعاب التحول نحو التفاعل الشبكي بين مختلف الفواعل العامة والخاصة، الدولاتية واللادولاتية، كما توفر هذه الأطروحة رؤية معمقة للتحديات المعاصرة فيما يتعلق بالإرهاب السيبراني، مما يوفر نقطة انطلاق بحثية لمساعدة الباحثين والممارسين وصانعي السياسات

في تطوير استراتيجيات الأمن السيبراني الخاصة بهم. بالتالي، يُعتبر تحليل الوضع الأمني في هذه الدراسة، وعبر الاستناد إلى أفكار الأمن الموسع وأُطره المنهجية، محاولةً لإثراء حقل الدراسات الأكاديمية ليكون هذا البحث بمثابة مرجع مفيد في التحليل ووحدة مساعدة للبحث العلمي، خاصة أن المراجع باللغة العربية التي تختص بموضوع الإرهاب السيبراني، بما في ذلك ما يمس المنطقة الأوروبية، تكاد تكون شحيحة. بالتالي فإن الأهداف العملية للدراسة تدور حول إثراء الحقل النظري وتقديم رؤية وتصور معمقين قد يستفيد منهما الباحثون في الوطن العربي.

صعوبات الدراسة:

تواجه أبحاث الجريمة الإلكترونية والإرهاب السيبراني عددًا من التحديات، مثل معدل التغير في التكنولوجيا والتعقيد الميداني وتعدد التخصصات، كما أن أطروحة الدكتوراه هي بالتأكيد مهمة معقدة وتستغرق وقتًا طويلاً، لاسيما مع موضوع توضيحي مثل الإرهاب السيبراني. ونظرًا لطبيعة البحث والحساسية التي تحيط بالإجابات المطلوبة، فإن العديد من الباحثين الأوربيين الذين تم الاتصال بهم لم يكونوا مستعدين للمشاركة لإعطاء صورة ميدانية لما يحدث على أرض الواقع في كل ما يتعلق بمجال بحثنا. إضافة لكون المتغير المستقل للأطروحة (الإرهاب السيبراني) كمفهوم مجرد هو مفهوم غير متفق عليه من قبل المجتمع البحثي، أو كما يقال مفهوم مطاطي، إضافة لكونه غير ثابت إيتيقيا، وكل محاولة لضبطه ستخلو من الحيادية والموضوعية، وستخضع حتما لتأويلات أيديولوجية بحتة.

كما أن محاولة دراسة الإستراتيجية الأوروبية من خلال فهم وتحليل الإرهاب السيبراني كبنية ووظيفة وتأثير، صعّب من القدرة على التحكم بالموضوع من خلال معالجته بمنظور كلاني Holism، فالتفاوت في القدرات الأمنية والتقنية داخل الكيانات الأوروبية (الدول الأوروبية فرادى) أحالَ إلى مقاربات تجزيئية لوحدات سياسية أوروبية في بعض أجزاء البحث مما قد يتعارض مع إستراتيجية الاتحاد الأوروبي ككيان جامع.

تقسيم الدراسة:

في سعينا للإجابة على الإشكالية وكذا اختبار فروضها، ارتأينا تقسيم الخطة إلى أربعة فصول مبنية على مباحث ومطالب، بحسب مقتضيات الحتمية البحثية، ومن حيث الهيكل، وبعد مقدمة الدراسة، يأتي الفصل الأول مستكشفا "الأبعاد المعرفية والمفاهيمية للإرهاب الإلكتروني في سياق تحول مفهوم

الأمن"، انطلاقا من تحديد المصطلحات الأساسية قبل تسليط الضوء على أهمية الإنترنت كمجال لنشاط كل من التطرف والإرهاب. في المبحث الأول من الفصل تم تقديم ماهية جريمة الإرهاب الإلكتروني، وفي المبحث الثاني جرى تناول إستراتيجية الإرهاب الإلكتروني من خلال تحليل القدرات وملامح الفاعلين، في حين تناول المبحث الثالث اتجاهات التنظير في الفضاء السيبراني أين تم استعراض توليفة نظرية لمدرستين أمنيتين (مدرسة كوبنهاغن ومدرسة باريس)، كما تطرق الباحث وبالتحليل الحاجة إلى إعادة تموضع النظريات التقليدية في تفسيرها للتهديدات اللاتماثلية خاصة في ظل القفزة الابستيمولوجية التي أحدثتها الآليات التفسيرية للنظريات النقدية.

أما الفصل الثاني، والذي يركز في مجمله على تحليل الإرهاب الالكتروني في إستراتيجية الأمن الأوربي الجماعي، جاء المبحث الأول ليخوض أكثر في التفاعل الحاصل بين الفضاء السيبراني وإدارة السياسات الأمنية، وفي المبحث الثاني من الفصل درس الباحث –وفق منطق تفكيمي– توظيف جماعات العنف للإرهاب السيبراني عبر الفضاء الأوروبي. كالإرهاب الجهادي، الإرهاب العرقي، القومي والانفصالي، الإرهاب اليساري والأناركي، والإرهاب اليميني، في حين يأتي المبحث الثالث ليفحص تأثيرات الإرهاب الالكتروني على الأمن الأوربي من خلال التهديدات التي مست أو قد تمس السيادة السيبرانية، وكذا الأمن في أبعاده المختلفة: المجتمعية، الطاقوية، السياسية، والعسكرية.

في حين ينطلق الفصل الثالث والمعنون بـ: "إشكاليات بناء الأمن الجماعي الأوربي (الانتقال من الأمن الصلب إلى الأمن الرخو)، من فهم بدايات تبلور الخطاب الأمني الأوروبي بشأن الإرهاب السيبراني، وأتى المبحث الثاني الموسوم بـ: محددات الأمن الجماعي الأوروبي عبر تقديم جينالوجيا مفهوم الأمن الجماعي، والمخاطر السيبرانية المشتركة والمتغيرات التي فسرت الأمن الجماعي الأوروبي، والثغرات الموجودة بين الجانب المعياري والاخلاقي وبين الممارسة الأوروبية التي تتقاطع مع الحماية وحرية التعبير، الخصوصية الفردية والجماعية، فيما صيغ الميحث الثالث بعنوان الأمن السيبراني الأوروبي بين ثغرات السياسات والتدابير التقنية والاجرائية.

في الفصل الرابع، حاولنا من خلاله تفكيك سرديات البيئة الأمنية السيبرانية الأوروبية من حيث الرهانات والتحديات متضمنا ثلاثة مباحث تناول المبحث الأول النهج الأوروبي التعاوني الوطني وعبر الوطني لأمن الشبكات والمعلومات، ليأتي المبحث الثاني برؤية قانونية معالجا الصكوك القانونية في أوروبا وإعادة بناء القدرات، ويستعرض المبحث الثالث سبل تطوير جدول أعمال بحثي حول الإرهاب

السيبراني مشيرا إلى جانب من التحديات التقنية والحلول، كما جاء ليبرز خارطة الطريق نحو رسم سياسات مستقبلية لتحقيق الأمن السيبراني الأوروبي، إضافة دراسة إمكانية الوصول للنضج السيبراني.

وفي الختام، حاولنا رصد أفكار متسلسلة حول ما تم تناوله في الفصول الثلاثة، وكانت عبارة عن إجابات لفرضيات الدارسة.

الفصـــل الأول:

الفصل الأول: الإرهاب الإلكتروني- الأبعاد المعرفية والمفاهيمية في سياق تحول مفهوم الأمن

المبحث الأول: ماهية جريمة الإرهاب الإلكتروني.

المبحث الثاني: الإرهاب الإلكتروني القدرات وملامح الفاعلين.

المبحث الثالث: اتجاهات التنظير في الفضاء السيبراني: الحاجة إلى إعادة تموضع النظريات التقليدية.

تمهيد الفصل:

عرفت فترة ما بعد الحرب الباردة تحولات كثيرة انعكســـت على طبيعة القوة في العلاقات الدولية وعلى نمط التهديدات الأمنية، فبعد أن كانت قوة الدول مقترنة بالجانب العسكري (الأمن الصلب) أصبحت تتوزع على جوانب عديدة، وبعد أن كان التهديد عســكريا بات أقلّ قهرية وأقلّ ملموســية بتعبير "جوزيف ناي" (Joseph Nye)، مما جعل الأمن في حد ذاته يعرف تحولا عميقا ليتضـــمن أبعادا أخرى (الأمن اللين) بالتزامن مع الثورة في تكنولوجيا الإعلام والاتصـــالات، ومع انتقال الإنترنت من هامش الحياة إلى عنصــر هام في حياة الأفراد والمجتمعات والدول، وانتشــارها بســرعة كإحدى ملامح أو مظاهر العولمة، خلقت فرصا للجريمة المستحدثة، والتي لها صور عدة من أبرزها الجريممة الإرهابية السيبرانية.

أصــبحت ظاهرة الإرهاب الســيبراني واحدة من أكثر التهديدات خطورة في الوقت الراهن، خاصــة وأنها تمثل الجانب السلبي من التطور التكنولوجي والثورة المعلوماتية، مما جعل تأثيراتها على صـعيد أمن الدول والحكومات والنظام الدولي ككل تأخذ أبعادا متنوعة في ظل تحول ساحة القتال والصراع من الفضاء المادي إلى الفضــاء الســيبراني. والبحث في هذا النمط الجديد من التهديدات الأمنية يســتدعي –بادئ ذي بدء– بحثا في ماهية الإرهاب الإلكتروني.

يتناول هذا الفصـــل مقاربة معرفية ومفاهيمية للإرهاب الإلكتروني، وذلك بالتعرف على مفهومه وخصــائصــه ودواعيه، وأهم الأســاليب أو الإســتراتيجيات التي تعتمد عليها الجماعات الإرهابية في هذا الإطار، بالإضـــافة إلى تحديد بعض المفاهيم المتداخلة مع مفهوم الإرهاب الإلكتروني مثل: الحرب الســيبرانية، الجريمة الســيبرانية والجهاد الســيبراني. كما يتناول الفصــل مقاربة نظرية للأمن الســيبراني في ســـياق تحولات مفهوم الأمن والتنظير في حقل العلاقات الدولية تزامنا مع الاجتهادات النظرية النقدية في مجال الأمن، حيث ســيتم التطرق إلى مدرســتي "كوبنهاجن" و"باريس" اللتين ســاهمتا بشــكل ملحوظ في تطوير الدراسات الأمنية ومن خلال ذلك التفطن إلى ضرورة الاهتمام بموضوع الفضاء السيبراني.

انطلاقا من ذلك، يعكف هذا الفصـــل على تقديم مقاربة متكاملة للإحاطة بموضـــوع الإرهاب الإلكتروني في ســـياقه العام من جهة، وفي ســـياق التحول في مفهوم الأمن وبروز الفضـــاء الإلكتروني كساحة للصراع والتهديد من جهة ثانية.

المبحث الأول: ماهية الإرهاب الإلكتروني.

في سياق إعداد هذه الدراسة كان من المهم البحث في ماهية الإرهاب الإلكتروني كمفهوم وظاهرة، وذلك لأن ضـبط المفاهيم والمصـطلحات في أيّ بحث أكاديمي محطة هامة خاصـةً عندما يتعلق الأمر بمفهوم يطرح إشـكالية في تعريفه. يتناول هذا المبحث تعريفا بجريمة الإرهاب الإلكتروني، الأسـباب التي تحفزها، خصائص الإرهاب الإلكتروني وبعض المفاهيم المتشابهة والمتداخلة مع هذا المفهوم.

المطلب الأول: الإرهاب الإلكتروني وجدلية التعريف.

بالنظر إلى كون مفهوم الإرهاب من المفاهيم المتنازع عليها بالضرورة*، بالنظر لغياب تعريف جامع، فالظاهرة الإرهابية تظهر اليوم على أنها سديم مفاهيمي، يصعب تعريفها لأنها تتميز بتنوعها الشديد في الزمان والمكان[1]، ولكي نفهم الإرهاب كظاهرة يجب تقييم وجهات النظر المختلفة حول ما يشكله مصطلح الإرهاب بالضبط حتى الوقت الحاضر، ولا يبدو أن هناك تعريف دولي واحد يرضي الجميع.

في ضوء ما تقدم، يبدو أن الإرهاب مصطلح يصعب التحايل عليه لأنه لا يوجد إرهاب واحد بل عدة أنوع من الإرهاب. ومع ذلك، كان بعض المؤلفين قادرين على إعطار قراءات للمفهوم يمكن البناء عليه.

أ. مفهوم الإرهاب:

قبل القفز إلى مفهوم الإرهاب السيبراني، يجب أن يكون لدى المرء فهم أساسي للإرهاب، والمناقشة الواردة في هذه الأطروحة حول الإرهاب العام محدودة ومختصـــرة للغاية وتُؤخَذ فقط كمعلومات أساسية.

---

* هي المفاهيم التي تحمل في مضمونها ما يجعلها موضع تنازع أنطولوجي دائم وحتمي، وبالنسبة لمصطلح الإرهاب لا يوجد لحد الان إجماع كبير على معناه واستخدامه الصحيح، في ظل وجود توتر كبير بين الفهم الضيق والواسع له (التمدد المفاهيمي Conceptual Stretching والإجهاد المفاهيمي Conceptual Straining أي المفاهيم الغامضة وغير المتبلورة). للاستزادة أُنظر:

Giovanni Sartori, Concept Misformation in Comparative Politics***, The American Political Science Review***, Vol 64, N 4 (Dec 1970), pp. 1033-1053, in: http://www.jstor.org/stable/1958356 (21/06/2020)

[1] Piero-D. Galloro, ***Conflictualités, représentations et médiatisation de la violence et de la radicalisation: Radicalisme(s), radicalisation(s), radicalité(s), violence(s)***, (France: Editions L'Harmattan, 2019), p 2.

من ناحية أصل الكلمة يرتبط "**الإرهاب**" بالكلمة اللاتينية (TERREUR) وهي بدورها مشتقة من أصـــــل لاتيني هو (TERRERE-TERSERE) بمعنى "جعلــه يرتجف". كمــا أن كلمــة (TERRORISER) كما جاءت في قاموس المنهل هي أَرْهَبَ، رَوَّعَ، وجاء تصـــريفها " إرهاب، ترويع (TERRORISM) ، إرهابيّ[2] (TERRORISTE).

أما لفظة الإرهاب في اللغة العربية فتعني الخوف والخشية، وهو ما جاء في القرآن الكريم الذي أعطانا تحديدا لغويا لكلمة "**رهبة**"، ومشتقاتها في الكثير من السور، مثال في سورة الأنفال، الآية 60، حيث يقول الله تعالى: "**وَأَعِدُّوا لَهُمْ مَا اسْتَطَعْتُمْ مِنْ قُوَّةٍ وَمِنْ رِبَاطِ الْخَيْلِ تُرْهِبُونَ بِهِ عَدُوَّ اللَّهِ وَعَدُوَّكُمْ وَآخَرِينَ مِنْ دُونِهِمْ**"[3]. وفي قوله: "**وَأَوْفُوا بِعَهْدِي أُوفِ بِعَهْدِكُمْ وَإِيَّايَ فَارْهَبُونِ**"[4]".

فالترهيب له بعد نفسـي يتصـل بإثارة مشـاعر الخوف والفزع لدى الآخر والخشـية من العذاب كما ورد في القرآن الكريم.

تجدر الإشارة إلى أن مصطلحي "الإرهاب" و "الإرهابي" ظهرا خلال الثورة الفرنسية مع نظام إرهاب روبسبير[5]، وما عُرف بعهد الإرهاب مع "روبسبير" (1793–1794م)، حيث ربطوا معانيهما بالمرحلة الثورية وقيمها، إذ جرى إعدام الآلاف بواسطة المقصلة، وتذكر المراجع أن عددهم بلغ 40 ألف شخص[6].
ثم دخل المعاجم والقواميس وشاع استخدامه، فظهرت محاولات كثيرة لتعريفه من بينها ما يلي:

- تعريفه في المادة الأولى من اتفاقية جنيف لقمع الإرهاب ومكافحته (1937)[7]:

---

[2] ثامر إبراهيم الجهماني، "مفهوم الإرهاب.. كتاب في القانون الدولي"، مركز الدراســـات والأبحاث العلمانية في العالم العربي، 14-07-2014، في: https://cutt.us/djYU (2021/08/25)

[3] سورة الأنفال، الآية 60.

[4] سورة البقرة، الآية 40.

[5] Piero-D. Galloro, ***Op.cit***, p 3.

[6] مصطفى يوسف كافي، وآخرون، ***الإعلام والإرهاب الإلكتروني*** (الأردن: دار الإعصار العلمي للنشر والتوزيع، 2015)، ص34.

[7] محمود يوسـف الشـوبكي، "مفهوم الإرهاب بين الإسـلام والغرب"، ورقة مقدمة إلى مؤتمر: الإسـلام والتحديات المعاصـرة، الجامعة الإسلامية: كلية أصول الدين، ابريل 2007، ص22.

"الأعمال الإجرامية الموجهة ضـــد دولة ما وتســـتهدف خلق حالة رعب في أذهان أشـــخاص معينين أو مجموعة من الأشخاص أو عامة الجمهور".

- تعريف لجنة الإرهاب الدولي التابعة **لمنظمة الأمم المتحدة** (1980)[8]:

"يعد الإرهاب الدولي عملا من أعمال العنف الخطير أو التهديد به، يصـــدر من فرد أو جماعة ســـواء كان ضد الأشخاص أو المنظمات، أو المواقع السكنية، أو الحكومية، أو الدبلوماسية، أو محاولة ارتكاب، أو الاشتراك في الارتكاب، أو التحريض على ارتكاب الجرائم يشكل أيضا جريمة الإرهاب الدولي".

يتضـح من خلال هذا التعريف أن العمل الإرهابي يتظمن عنصـر العنف أو التهديد به، ويكون موجها إلى أشـــخاص أو مؤســـســـات مختلفة، ولكنه أغفل عنصـــر التخطيط والتنظيم والأثر الناتج عن الفعل الإرهابي، وأيضا الغاية، وهي عناصر أساسية له.

- تعريف الاتفاقية العربية لمكافحة الإرهاب (1998) في المادة الأولى[9]:

"كل فعل من أفعال العنف أو التهديد أيا كانت بواعثه أو أغراضـه، يقع تنفيذا لمشروع إجرامي فردي أو جماعي ويهدف إلى إلقاء الرعب بين الناس أو ترويعهم بإيذائهم أو تعريض حياتهم أو حريتهم أو أمنهم للخطر، أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها أو تعريض أحد الموارد الوطنية للخطر".

يشير هذا التعريف إلى أن العمل الإرهابي له أسبابه المختلفة، وقد كان أكثر وضوحا من سابقه، ولكنه أغفل بدوره عنصر التخطيط والتنظيم والهدف من الفعل الإرهابي.

وعلى مســـتوى المحاولات الفردية لتعريف الإرهاب يعد "هاردمان" (Hardman) من أوائل من قاموا بتعريفه في مقال له سنة 1930 حيث قال: "هو المنهج أو النظرية الكامنة وراء النهج الذي بمقتضاه

---

[8] إدريس عطية، ***التهديدات الإرهابية الجديدة في إفريقيا: دراسة في توظيف الظاهرة وتموضعها الجيوبوليتيكي***، ط1، (الأردن: دار الإعصار العلمي، 2018)، ص26.

[9] عبد الحميد راجح كردي، "إشـكالية مصـطلح الإرهاب بين الحقيقة اللغوية والشـرعية والواقع المعاصـر"، ***مجلة البلقاء للبحوث والدراسات***، المجلد 22، العدد 1(2019)، ص113.

تسعى مجموعة منظمة أو حزب إلى الوصول إلى أهدافه المعلنة بالاستخدام المنهجي للعنف بصورة أساسية"[10].

يعد هذا التعريف دقيقا إلى حد ما بالنظر إلى الفترة التي ظهر فيها، ولكنه أغفل عنصر الفرد كفاعل إرهابي، ولم يحدد طبيعة الأهداف المرجوة خاصة وأن للإرهاب هدف سياسي بالدرجة الأولى.

- تعريف الإرهاب في موسوعة عبد الوهاب الكيالي[11]:

"استخدام العنف غير القانوني أو التهديد به، بأشكاله المختلفة، كالاغتيال والتشويه والتعذيب والتخريب والنسف، بغية تحقيق هدف سياسي معين، مثل كسر روح المقاومة والالتزام عند الأفراد، وهدم المعنويات عند الهيئات أو المؤسسات، أو كوسيلة من وسائل الحصول على معلومات أو مال، وبشكل عام استخدام الإكراه لإخضاع طرف مناوئ لمشيئة الجهة الإرهابية".

ويتضح من التعريفات المقدمة وجود قواسم مشتركة تميز الفعل الإرهابي، مع أن المحاولات جميعها لم تفلح في تمرير تعريف يحظى بالإجماع الدولي. وعند الحديث عن العناصر المشتركة في العمل الإرهابي تجدر الإشارة إلى اجتهادات الباحث الأمريكي المتخصص في قضايا الإرهاب "ألكس شميد" (Alex Shmid)، والذي عمل برفقة زميله "جونغمان" (Albert Jongman) على جمع 109 تعريف لباحثين في الإرهاب ثم استخراج العناصر الأساسية وأهمها: توظيف العنف، العنصر السياسي، استخدام التهديد، الآثار النفسية، وضوح الهدف، التخطيط والتنظيم

[10] إدريس عطية، ***مرجع سابق***، ص: 28، 29.

[11] عادل عبد الله بركة المطيري، ***التهديدات غير التقليدية على أمن دول مجلس التعاون الخليجي (2003-2016)***، ملخص رسالة ماجستير في العلوم السياسية (الكويت: مركز دراسات الخليج والجزيرة العربية، 2020)، ص23.

[1]. وقد وجد شـــميد وجونجمان 22 كلمة محددة في تعريفات مختلفة لوصـــف الإرهاب، وكانت الكلمات الأكثر اســـتخدامًا هي بترتيب تنازلي: عنف، قوة (83.5٪)، ســـياســـي (65٪)، خوف، إرهاب (51٪)، تهديد (47٪)، تأثيرات وردود فعل (41.5٪)[2].

وقبل الانخراط في تحليل الإرهاب، على المرء أن يفهم طبيعته الحقيقية. فهناك العديد من المناهج المختلفة –المتناقضـــة في كثير من الأحيان–، ولم يقم المتخصـــصـــون في المجال بصـــياغة أي تعريف شـــامل ومقبول على نطاق واســـع[3]، كما أن عدم وجود تعريف واحد ودقيق للإرهاب يطرح إشـــكالية على صـعيد تحديد من هو الإرهابي سواء كان فردا أو جماعة أو تنظيما، مع الإشـارة هنا إلى إهمال التعريفات جميعها لوصف "إرهاب الدولة"[4].

في دراسـة لها، طرحت ماريا خوسـيه مويانو Maria Jose Moyano مقاربة أخرى للإرهاب من خلال الجمع بين بعض التعريفات، وهي تصـــف الإرهاب بدلاً من تعريفه على أنه "اســـتخدام العنف أو التهديد باستخدامه لتحقيق أهداف سياسية، عندما يكون هذا العنف يهدف إلى السيطرة على السكان من خلال الخوف أو إجبار الحكومة على منح تنازلات معينة بالرغم من أنها تميز بين التهديد باســـتخدام العنف والاســـتخدام الفعلي للعنف، إلا أنها لا تشـــرح كيف يعتبر التهديد بالعنف عملاً إرهابيا، فهل كل ابتزاز هو آليا عمل إرهابي؟ إذا لم يكن كذلك، فكيف يمكن للمرء أن يميز هذه الأفعال عن بعضـــها البعض؟ كما أنها تركز على "نية السـيطرة على السـكان"، ومع ذلك فإن مصـطلح السـيطرة هو مبالغة، ويريد الإرهابيون تهديد عدد كافٍ من الناس، وبذلك يجبرون الحكومة على تلبية متطلباتهم؛ أو لمعاقبة بعض السياسيين؛ أو ببساطة للفت الانتباه إلى أنفسهم[5].

---

[1] إدريس عطية، "تهديدات الإرهاب الدولي في منطقة شمال إفريقيا"، ***المجلة الجزائرية للدراسات السياسية***، العدد 4 (ديسمبر 2015)، ص37.

[2] Jarkko Moilanen, ***Realms of cyber warriors - Definitions and Applications***, Master´s thesis in Political Science, University of Tampere Department of Political Science and International Relations, August 2009, p 24

[3] Maria J. Moyano, Argentina's Lost Patrol, ***Armed Struggle, 1969-1979***, (Yale University Press, New Haven and London, 1995), pp. 3.

[4] علي العبيدي، ***في الحرب على الإرهاب: من إرهاب المفهوم إلى إرهاب المقاربة***، ط1، (تونس: دار المنتدى، 2018)، ص110.

[5] Mieczyslaw Malec, ***Security Perception within and beyond the Traditional Approach, Monterey, California. Naval Postgraduate School***, Master of Arts in National Security Affairs, Naval Postgraduate School, juin 2003 , p 49. available on: http://hdl.handle.net/10945/951

في سياق متصل، عمل الاتحاد الأوروبي على وضع تعريف مشترك للإرهاب، من أجل تنسيق وجهات النظر والسياسات بالنسبة للدول الأعضاء، ولاقتناعه بأن تقديم تعريف للإرهاب ستكون له أهمية في الجانب العملي، ولذلك قام بإدراج الجرائم الإرهابية في قرارات المجلس الأوروبي منذ عام 2008، ويُعرَّف الإرهاب حسب الرؤية الأوروبية بأنه "الهجمات ضد حياة الشخص، كأفعال متعمدة يمكن وصفها بأنها جرائم إرهابية إذا ارتُكبت لهدف إرهابي محدد هو ترهيب السكان، لإجبار الحكومة أو منظمة دولية على أداء أو الامتناع عن القيام بأي عمل أو لزعزعة الاستقرار أو تدمير البنى الأساسية السياسية، الدستورية، الاقتصادية أو الاجتماعية"[1].

ويؤكد "شميد" أن مصطلح الإرهاب هو الأكثر أهمية في السياسات الوطنية[2]، بما أنه موضوع أمني يحظى بإجماع واسع، فالإرهاب ليس أيديولوجية بقدر ما هو إستراتيجية للعمل العنيف[3]، هذا الاجمال لا ينطبق على المجال الأكاديمي، فأهمية ضبط مصطلح الإرهاب تنبع من اعتبارات أساسية يحددها الأستاذ علي العبيدي، الحقوقي والباحث التونسي، كما يلي[4]:

- على مستوى البحث العلمي:

انطلاقا من أن تحديد المصطلحات ضرورة أكاديمية أولا، وبالتالي فإن وضع تعريف للإرهاب أمر ضروري في إطار عملية البحث وفهم الظاهرة وإيجاد سبل لمواجهتها.

- على المستوى القانوني:

باعتبار أن وجود تعريف متفق عليه سيكون كفيلا بتجاوز التحديات التي تواجه التشريعين الوطني والدولي، مع السعي نحو اتفاقية دولية لمكافحة الإرهاب.

- على المستوى القضائي:

تعريف مصطلح الإرهاب سيعزز الجهود الدولية والتدابير القضائية لمكافحة الظاهرة الإرهابية بعيدا عن أيّ ذاتية.

---

[1] Teemu Tammikko & Tuomas Iso-Markku, ***THE EU'S EXTERNAL ACTION ON COUNTER-TERRORISM: DEVELOPMENT, STRUCTURES AND ACTIONS***, FIIA Report (June 2020), P.24.

[2] Alex Shmid, « Terrorism : Definitional Problem », ***Journal of International Law***, Vol.36, Issue 02 (2004), p-p : 376-377.

[3] ***Report of the Working Group on Countering the Use of the Internet for Terrorist Purposes, Counter-Terrorism Implementation Task Force*** (CTITF), February 2009, p4

[4] علي العبيدي، ***الإرهاب واستعصاء المفهوم***، ط1، (تونس: دار المنتدى، 2018)، ص: 07–09.

- على المستوى السياسي:

انطلاقا من أن الاتفاق على تعريف دقيق وموضوعي سيفضح الاعتبارات السياسية والإستراتيجية التي على أساسها يتم تصنيف الإرهاب وإطلاق صفة إرهابي على طرف دون سواه، في إطار صراع سياسي وأهداف إستراتيجية معينة.

ومن بين العوامل الخطيرة، كما يذكر "شميد"، التي تشجع مزيدا من الإرهاب غيابُ تعريف واحد له، والاختلاف حول عوامله، إضافة إلى إضفاء صفة الدين عليه في الغالب، إلى جانب "ارتفاع تكلفة الأمن في الديمقراطيات"، وتتمثل أهمية التوصل إلى تعريف دولي موحد للإرهاب في جعل الاتفاقيات الدولية بشأنه أكثر فعالية، فضلا عن دور ذلك في مكافحة الظاهرة بصورة أكثر حسما[1].

تجدر الإشارة هنا، إلى أن الدراسات النقدية للإرهاب أيضا تحتاج إلى مراجعة وإعادة النظر في "تعريف كيفية تعريف الإرهاب" Define how to Redefining وهي خطوة تأملية Reflexive ضرورية شبيهة بما يسميه الإبستيمولوجيون "فهم الفهم" أو "التنظير حول التنظير"، ويقدم جوزيف أيسون Joseph Easson وألكس شميد Alex Schmid مسحا غير حصري يشتمل على مائتين وخمسين تعريفا للإرهاب، ويعزى مصدر الاستعصاء في التعريف هنا لكون مصطلح الإرهاب توصيفا أكثر من كونه مفهوما قابلا للضبط والاستعمال من دون محاذير معرفية وسياسية تذكر[2].

وبالتالي، فإن تعقيد تعريف مفهوم "الإرهاب" يتحدد من خلال حقيقة أنه لا يستخدم كحقيقة علمية، بل هو جزء من السياق الإيديولوجي والاجتماعي والنفسي والسياسي. فالتعاريف المختلفة المقدمة آنفا للإرهاب تعكس المفهوم الذي يضعه المجتمع في استخدام مصطلح "الإرهاب".

- وكتعريف إجرائي يمكن القول أن الفعل الإرهابي يجب أن تتوفر فيه مجموعة من المؤشرات الملموسة، بداية بعنصر العنف والقوة غير المشروعين، بحيث يعد الإرهاب خرقا للنظام العام في الدولة والمجتمع، يقف وراءه أفراد أو مجموعات أو حتى دول، ويتسبب في أضرار كبيرة على المستويات كافة، بما في ذلك الضرر النفسي. ولا يمكن حدوث الفعل الإرهابي دون تخطيط مسبق

[1] Alex Shmid, ***Op.cit***, p-p: 378-379.

[2] محمد حمشي، الدراسات النقدية للإرهاب بوصفه حقلا معرفيا ناشئا مراجعة "دليل راوتليج إلى الدراسات النقدية للإرهاب"، ***سياسات عربية***، العدد 31 (مارس 2018)، ص: 119–128.

وهدف محدد، ودون توظيف وسـائل تخدم العملية الإرهابية، بما في ذلك دور وسـائل التكنولوجيا الحديثة.

ب- تطور ظاهرة الإرهاب العالمي: ديفيد رابوبورت David Rapoport ودراسـة موجات الإرهاب الدولي.

يفترض رابوبورت أربع موجات إرهابية لكل منها حدث وتكتيكات وأسـلحة مميزة، وانحدار تدريجي حتمي يبلغ ذروته عند ولادة موجة أخرى، وهي: الموجة الأناركية (1878-1919)، الموجة المناهضـة للاسـتعمار (1920- أوائل السـتينيات)، الموجة اليسـارية الجديدة (منتصـف السـتينيات- التسـعينيات)، الموجة الدينية (1979-مسـتمرة)[1]. في حين أن توقع الموجة التالية يفتح باب النقاش حول آفاق الموجة الخامسـة، وفي هذا الشـأن يكتب جوناثان فوكس أنه قبل انتهاء الموجة الرابعة، "من المرجح أن تظهر موجة خامسـة بأيديولوجية جديدة، ربما تكون على أسـاس الجماعات الفوضـوية الجديدة التي تحتج حاليًا على العولمة"[2]. لقد تغيرت طبيعة الإرهاب في السـنوات الأخيرة لأن الأهداف الدينية حلت محل الأهداف العلمانية أو السياسية للعديد من الجماعات[3]، حيث سيطرت الأيديولوجية والأصولية الدينية على الموجات الأربع السـابقة، وبدلاً من ذلك سـيكون الدور المؤثر للتكنولوجيا هو السـمة المميزة للموجة الخامسـة، وهذا خروج عن نظرية موجات رابوبورت التي كانت تتمحور حول **الأفكار والأيديولوجيات**، وبالتالي فإن فهم العلاقة بين التكنولوجيا والإرهاب هو مفتاح لفهم ديناميكيات الموجة الخامسة.

- **الموجة الخامسة من الإرهاب العالمي: الإرهاب التكنولوجي.**

سيكون من الصـعب الخلاف على حقيقة أننا اليوم في خضـم ثورة تكنولوجية ومعلوماتية تؤثر في جميع جوانب الحياة، بما في ذلك ديناميكيات الإرهاب العالمي، فلطالما ارتبط الإرهاب بمسـيرة التكنولوجيا التي لا رجعة فيها، ويشير رابوبورت إلى الكيفية التي ساعدت بها التغييرات في أنماط الاتصال والنقل، ولا سيما استخدام التلفاز والصحف من قبَل التنظيمات الارهابية لكي تصبح قادرة على الاستفادة منها لتحقيق

1 Jeffrey Kaplan, "Waves of Political Terrorism", Oxford Research Encyclopedias, Politics, 29 October 2021, in : https://cutt.us/ZfHzc(08/12/2021)

2 Jeffrey D. Simon, « Technological and Lone Operator Terrorism: Prospects for a Fifth Wave of Global Terrorism", in : ***Terrorism, Identity and Legitimacy the four waves theory and political violence***, ed. Jean E. Rosenfeld, (New York: Routledge, 2011), pp 44-65.

3 David C. Rapoport, "Terrorrism and Weapons of the Apocalypse", January 1999, in : https://cutt.us/2fAMK (accessed 09/12/2021)

أهدافها الخاصـــة، وقد كتب رابوبورت: "اســـتمرت الابتكارات [التكنولوجية] اللاحقة في تقليص الزمان والمكان".[1]

وعلى عكس الفترة الســـابقة، أعطى ظهور الإنترنت وتقنيات عصـــر المعلومات الأخرى منذ التسعينيات المتطرفين المحليين وصولاً أكبر إلى المعلومات المتعلقة بصنع القنابل والتدريب على الأسلحة والتكتيكات، فضلاً عن استهداف الأفراد والمنظمات والمرافق[2].

إن الارتباط بين الإرهاب والتكنولوجيا يقوم على مبدأ بســـيط ألا وهو أن التقدم التكنولوجي في جميع المجالات لا يميز بين المســتخدمين، فالابتكارات في الأسـلحة والاتصـالات وأنظمة المعلومات وما إلى ذلك متاحة للجميع للاســـتفادة منها، بما في ذلك الإرهابيون، فالتكنولوجيا زودت الإرهابيين بتحســـين مســـتمر في أســـلحتهم، بدءًا من الخناجر القديمة ثم البنادق والديناميت ومؤخراً المتفجرات البلاســـتيكية والأسـلحة المضـادة للطائرات المحمولة على الكتف والعبوات الناسـفة المتطورة وصـولا لاسـتعمال وسـائل التواصـــل الاجتماعي ومنها لتقنيات الحاســـوب الأخرى. حتى أن **جيفري دبليو لويس** يجادل بأن تكتيك التفجيرات الانتحارية هو شكل من أشكال التكنولوجيا نفسها، مع تعريف التكنولوجيا على أنها:

> **" تفاعلية ديناميكية تضـــم كلاً من العناصـــر المادية وغير المادية. يكون البشـــر في عمليات التفجير الانتحاري، ســـواء على الأقدام أو في شـــاحنة أو في قارب أو في طائرة، هم أدوات العيش التي تتحكم في الذخائر وتوجهها بنفس الطريقة التي توجه بها الإلكترونيات والبرامج والذخائر الأمريكية الدقيقة."**

تبعا لذلك، يمكن اعتبار الإرهاب أيضًـا سـباقًا تكنولوجيًا لا نهاية له حيث تحاول سـلطات مكافحة الإرهاب البقاء متقدمة على الإرهابيين بخطوة، وبمجرد تصميم الأجهزة الجديدة وتركيبها لاكتشاف الأسلحة أو الحماية من هجوم، يمكن للإرهابيين تغيير تكتيكاتهم أو اســـتخدام أســـلحة أكثر تطوراً وفتكا لهزيمتهم، وبينما لعبت التكنولوجيا دورًا مهمًا في الإرهاب لفترة طويلة، فقد تصـــبح أكثر أهمية في الموجة الخامســـة حيث ترتفع الابتكارات التكنولوجية إلى طليعة النشاط الإرهابي والاستجابة لمكافحة الإرهاب.

---

[1] Jeffrey D. Simon, ***op.cit.,***

[2] David C. Rapoport, Terrorism as a Global Wave Phenomenon: Religious Wave, Oxford University Press (26 October 2017), in: https://cutt.us/tOX5Y (08/12/2021)

وبغض النظر عن المسار المستقبلي للموجة الدينية، بدأت الموجة التكنولوجية بالفعل في إحداث بصماتها، وإذا جرى بتوسيع رؤية **رابوبورت** للموجة لتشمل طيفًا كاملاً من أنشطة الإرهاب ومكافحة الإرهاب، حينها يصبح من الواضح أننا على حافة، وربما بالفعل داخل الموجة التكنولوجية[1].

يركز آخرون، أمثال اندرس وساندلر Enders and Sandler على الدورات قصيرة المدى التي تحدث داخل الموجات التي وصفها Rapoport، وتستند هذه الدورات حول التكتيكات التي يستخدمها الإرهابيون والتكتيكات المضادة التي تستخدمها الحكومات لوقف الإرهابيين الذين يطورون تكتيكًا جديدًا لا تكون الحكومات مستعدة له، مما يؤدي إلى زيادة الهجمات الإرهابية الناجحة، وفي المقابل تطور الحكومات تكتيكات مضادة تقلل من فعالية هذه الهجمات وتجبر الإرهابيين على تطوير تكتيكات جديدة، وبالمثل تظهر مجموعات أو خلايا إرهابية جديدة وتقوم بهجمات إرهابية، وتصبح الحكومات على وعي بهذه الجماعات أو الخلايا وتقوم بمضايقتها بوسائل مختلفة لتقليل فعاليتها[2]. هكذا تبنى الموجات التي تستمر لمدة جيل تقريبًا*، والتي تشكل دورة نشاط في فترة زمنية معينة تتميز بمراحل من التوسع والانكماش، ويعرف **رابوبورت** هذه الدورة بأن لها طابعا دوليا حيث تحدث الأنشطة المماثلة في العديد من البلدان لأنها مدفوعة بالطاقة السائدة المشتركة التي تشكل المجموعات المشاركة وعلاقاتها المتبادلة، مع العلم أن موجات الإرهاب هذه تتكون من منظمات تميل إلى أن يكون لها عمر أقصر من الموجة التي ترتبط بها ولكنها تميل إلى ظهور مجموعات منشقة أو لاحقة تواصل حملاتها الأيديولوجية والإرهابية،وعندما لا تكون طاقة الموجة قادرة على إلهام تشكيل منظمات جديدة، تتبدد الموجة، بالتالي

---

[1] Jeffrey D. Simon, ***op.cit.***

[2] Jonathan Fox, "The Future of Religion and Domestic Conflict," in: ***Religion, International Relations and Development Cooperation***, (ed .)Berma klein Goldwijk, (Wageningen Academic Publishers, 2007) pp129-152.

* يعتمد المؤرخ الشهير وكاتب الخطابات ومستشار الرئيس كينيدي، آرثر إم شليزنجر جونيور *Arthur M. Schlesinger* في كتابه: "دورات التاريخ الأمريكي" *The Cycles of American History* على عقود من الملاحظة الذكية لبناء ديالكتيك للسياسة الأمريكية، يتأمل شليزنجر في بزوغ فجر الألفية الجديدة وكيف يمكن للثورات الاجتماعية والتكنولوجية الجديدة أن تؤدي إلى ثورة في الدورات السياسية الأمريكية عبر موجات تغيير جيلي، الأمر المطابق لتفسيرات رابوبورت لمنظور التطور الزمني والتكنولوجي للموجات الأربع لتطور الإرهاب الدولي، للاستزادة أنظر:

De Arthur Meier Schlesinger, ***The Cycles of American History***, (A mariner book Houghton Mifflin Company, Boston New York,1999), p 23.

تتبع هذه الموجات دورة حياة جيلية تشبه دورة حياة الإنسان، وبناءً على هذه النظرية نقترب حاليًا من ذروة الموجة الدينية في منتصف الطريق تقريبًا بين تشكيلها والانحسار النهائي[1].

ج–في مفهوم السيبرانية والفضاء السيبراني:

مفهوم **السيبرانية** أو السيبرنطيقا يعود إلى الأصل اليوناني للكلمة: kebernetes، وكان يعني "إدارة القوارب"، ثم في القرن التاسع عشر استخدمه "أمبير" تعبيرا عن "علم خاص للإدارة الاجتماعية والسياسية"، وهو انطلاقا من مفهوم الإعلام "علم لعمليات استلام (جمع)، إرسال (نقل)، إعادة تشكيل (تحليل)، حفظ واستعمال المعلومات في الجمل الديناميكية المعقدة"[2]. ثم اشتهر مع أستاذ الرياضيات في معهد ماساشوستس "نوربرت واينر" (Norbert Wiener) عام 1948، والذي استخدمه في كتابه: Cybernetics : or Control and Communication in the Animal and Machine، ليشير من خلاله إلى القيادة والسيطرة والاتصالات في عالم الحيوان أو العالم الميكانيكي[3]. وعرّفها الدكتور "لومير كلونس" (Lumir Klunes) في 1983 في قاموس الكلمات الأجنبية بأنها "حقل علمي يتعامل مع المبادئ العامة للتحكم في المعلومات ونقلها في الآلات والكائنات الحية"[4]. كما ارتبط المفهوم بالخيال العلمي مع الكاتب "ويليام جيبسون"، وهو صاحب مصطلح الفضاء السيبراني، من خلال كتابه "نيورومانسر" لعام 1984[5].

بالنسبة لكل من بيتر وستيفنز David J. Betz and Tim Stevens يُعد إيجاد تعريف للفضاء السيبراني ذا دلالات في كيفية استخدام القوة والتي تحدّد استراتيجيات الفضاء السيبراني، واستخدام القوة

---

[1] Jeffrey Kaplan, ***Op.cit.***

[2] م.يانكوف، ل.يوتوف، ***السيبرنتيك والإعلام***، تر. برهان القلق، ط1، (بيروت: دار الطليعة للطباعة والنشر، 1979)، ص: 07، 10.

[3] Lion Tabansky, « Basic Concepts in Cyber warfare », ***Military and Strategic Affairs***, Vol.3, No.1, (May, 2011), p.76.

للمزيد أُنظر:

Norbert Wiener, ***Cybernetics : or control and communication in the animal and the Machine***, ed.4 (USA : The M.I.T. Press, 1985).

[4] « Definitions of Cybernetics in the Course of the Century », Department of Cybernetics, in: http://www.kky.zcu.cz/en/definitions-of-cybernetics

[5] Stéphan Leman-Langlois, « Questions au Sujet de le Cybercriminalité, le Crime Comme moyen de Contrôle du Cyberspace Commercial ». ***Criminologie***, VOL 39.N 1, (Jun 2006), p.65.

فيه، وفي هذا الإطار قدما مفهومين أساسيين للفضاء السيبراني: الأول يستبعد البنى التحتية، والثاني يشملها، فالأول وهو "النموذج الحصري" يقدم الفضاء السيبراني على أنه فضاء مبني على مكونات شبكات الكمبيوتر، فهو وفق هذا المعنى ليس بالمعنى الجغرافي التقليدي، أما الثاني فهو "النموذج الشامل" الذي يمثل الطبقة المعلوماتية "الافتراضية" المركبة فوق طبقة مادية من الأجهزة[1].

ولعل التعريف الأقرب للواقع هو الذي حدده فريد سكرير Fred Schreier بقوله: "إن الفضاء السيبراني هو عبارة عن أنظمة معلومات متشابكة ومتصلة، تسكن في الفضاءين المادي والافتراضي، داخل وخارج الحدود الجغرافية، تضم مستخدمين من دول، ومؤسسات تابعة لها، إضافة إلى مجتمعات، وأفراد، ومجموعات عبر قومية، لا تعلن ولاءها لأيّة منظمة تقليدية أو كيان وطني، وهي تعتمد في ذلك على أبعاد ثلاثة، مختلفة لكن مترابطة: مادية، معلوماتية، ومعرفية تؤلف معًا بيئة المعلومات العالمية[2].

في حين قدّمت وزارة الدفاع الأمريكية في شأن الفضاء السيبراني عددا من التعريفات، من بينها تعريفه بأنه "بيئة قومية يتم فيها إرسال البيانات الرقمية على شبكات من الحواسيب"، أو هو "مجال يتميز باستخدام الإلكترونيات والمجال الكهرومغناطيسي"، لكن تم رفض مثل هذه التعريفات باعتبارها ناقصة وغير شاملة لمكونات الفضاء الإلكتروني، ثم عرفته ذات الوزارة في 2008 بأنه[3]:

"المجال العالمي الذي فيه بيئة من المعلومات تتألف من ترابط شبكة البنى التحتية للمعلومات، التي تتضمن الإنترنت وشبكات الاتصالات السلكية واللاسلكية وأنظمة الحواسيب وما ضمّ معالجات وأجهزة تحكّم".

كما عرفته الوكالة الفرنسية لأمن أنظمة الإعلام والفضاء السيبراني بأنه "فضاء التواصل المشكّل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية"[4]. ويعرّفه الاتحاد الدولي

---

[1] أنديرا عراجي، ***القوة في الفضاء السيبراني فصل عصري من التحدي والاستجابة***، رسالة لنيل دبلوم دراسات عليا في العلوم السياسية والإدارية، كلية الحقوق والعلوم الإدارية، الجامعة اللبنانية، 2016، ص 12.

[2] أنديرا عراجي، ***المرجع نفسه***، ص 13.

[3] مجاهد فخر الدين قاسم أحمد، ***ترجمة الصفحات: 1-66 من كتاب الأمن الإلكتروني والحرب الإلكترونية، ما ينبغي أن يعرفه كل شخص، لبيتر وارن سينغر والن أ. فريدمان***، بحث تكميلي لنيل درجة الماجستير في الترجمة، (السودان: جامعة السودان للعلوم والتكنولوجيا، كلية الدراسات العليا، د.س.ن)، ص: 17، 18.

[4] لطفي لمين بلفرد، "الفضاء السيبراني: هندسة وفواعل"، ***المجلة الجزائرية للدراسات السياسية***، العدد 5، (جوان 2016)، ص147.

للاتصـــالات (ITU) بأنه "المجال المادي وغير المادي الذي يتكون وينتج عن عناصـــر هي: أجهزة الكمبيوتر، الشـبكات، البرمجيات، حوسـبة المعلومات، المحتوى، معطيات النقل والتحكم، ومسـتخدمو كل هذه العناصـــر"، ويعد الفضـــاء الإلكتروني أو الســـيبراني البعد الخامس للحرب بعد البر والبحر والجو والفضاء الخارجي[1].

وعرّفه "أندرو كريبينفيتش" (Andrew Krepinevich) بأنه "شبكات الكمبيوتر العالمية، المفتوحة والمغلقة، بما في ذلك أجهزة الكمبيوتر وشبكة المعاملات التي تنقل البيانات المتعلقة بالتعاملات المالية والشبكات ذات أنظمة التحكم التي تتيح للآلات التفاعل"[2].

تتكون بيئة أنظمة المعلومات التي تشكل فضاء المعارك السيبرانية من ثلاث طبقات: **المادية، التشابكية، والدلالية**، تعمل القدرات الهجومية السيبرانية وعمليات الدعم للعمليات التي تتمحور حول الشبكة في هذا المشهد ثلاثي الطبقات، فتشير **الطبقة المادية:** إلى أجهزة الكمبيوتر، والكابلات، والموجهات التي يختلف تداولها من تردد لاسلكي إلى طاقة إلى إشارات كهربائية وفوتونات، وخيارات الضربات العميقة وعمليات القوات الخاصة وقدرات التخفي، والتي في مجملها تشكل البنية التحتية الحيوية التي تتحكم في عملية الإرسال والاستقبال[3]، فيما تشير **الطبقة التشابكية:** إلى الأوامر التي توجه أنظمة المعلومات بالمهام من خلال وحدات "البت" التي تنتشر عبر النظام المادي، هذه الطبقة ستبقى عرضة لنشاط القراصنة العدائي، وستكون هناك حاجة إلى قدرات إلكترونية دفاعية لحماية أنظمة المعلومات[4]، ومن خلالها يتم التحكم في الطبقة المادية والمعلومات المخزنة[5].

أخيرًا، توفر **الطبقة الدلالية** معنى لمحتوى المعلومات، مما يجعلها عرضة للأنشطة الخادعة، في هذا الصدد، يجب التأكيد على أن المعايير العسكرية المعاصرة تنذر بـ "حروب غير واضحة" تكون فيها "هوية الطرف المتحارب وحتى حقيقة الحرب غامضة تمامًا" بسبب التحولات التكنولوجية والتنظيمية.

---

[1] إسـماعيل زروقة، "الفضـاء السـيبراني والتحول في مفاهيم القوة والصـراع"، ***مجلة العلوم القانونية والسياسية***، المجلد 10، العدد 1 (ابريل 2019)، ص1017.

[2] John J. Klein, « La Rétribution et la Dissuasion du Cyber Terrorisme », ***Afrique et Francophonie***, (2018), p.23.

[3] Lion Tabansky, ***Op.cit***, p.77

[4] Salih Bıçakcı, Ahmet K . Hanm, ***A Primer on Cyber Security in Turkey and the case of Nuclear Power***, Istanbul: Center for Economics and Foreign Policy Studies, 2015, p.7.

[5] Lion Tabansky, ***Op.cit***, p.78.

وبالتالي، يساعد تصنيف ساحة المعركة في الحرب الإلكترونية صانعي القرار في صياغة عمليات الحرب الإلكترونية والتضاريس المستقبلية. على الرغم من أن الفضاء الإلكتروني يُنظر إليه على أنه مجال جديد للحرب، إلا أن الطبقة المادية لبيئة أنظمة المعلومات لا تزال تتطلب مشاركة الأصول البرية والبحرية والجوية والفضائية التقليدية من أجل تعزيز قدرة دفاعية وهجومية فعالة. علاوة على ذلك، ترتبط العمليات السيبرانية في الطبقات التشابكية والدلالية ارتباطًا وثيقًا لأن نشاط المتسلل العدائي قد يقترن بعمليات نفسية غير حركية ومضللة تُمَكّنْ لشكل جديد من "العمليات المشتركة" في الفضاء الإلكتروني، والذي سيحدث في نفس الوقت في الطبقات المادية والنحوية والدلالية ، أن يغير بشكل جذري نطاق العمليات السيبرانية الهجومية والدفاعية[1].

د– الإرهاب السيبراني:

الإرهاب السيبراني مصطلح صاغه باري كولين Barry Collin في ثمانينيات القرن الماضي من خلال لطرحه لمفهمة يقترن فيها الإرهاب بالفضـــاء الإلكتروني[2]، كما ناقش ديناميكية الإرهاب باعتبارها التعالي من العالم المادي إلى العالم الافتراضـــي و"التقاطع والتقارب بين هذين العالمين[3] ..."، وحظي هذا المصطلح باهتمام متزايد في السنوات الأخيرة لدى وسائل الإعلام، آخذا عدة تسميات، كالإرهاب الشبكي، الإلكتروني، الرقمي، السيبيري، وغيرها من التسميات.

كانت الأوساط الأكاديمية مبعثرة من حيث نطاقها وتفاصيلها وتركيزها في محاولة تعريفها للإرهاب كظـاهرة وكمفهوم[4]، فبـالنظر إلى كون مفهوم الإرهـاب من المفـاهيم التي لا يتفق المجتمع العلمي على تعريفها، فليس من المستغرب أن تكون تعريفات الإرهاب السيبراني متباينة بنفس القدر، بالإضافة إلى ذلك فإن عدم وجود حدث كبير لإثارة النقاش العام قد جعل الحافز لدى المشـــرعين ضـــئيلا في تحديد هذه

[1] Salih Bıçakcı, Ahmet K. Hanm, ***Op.cit.***, p7.
[2] Barry C. Collin, "The Future of Cyberterrorism", Paper presented at the 11th Annual International Symposium on Criminal Justice Issues, University of Illinois at Chicago, 1996, in: http://afgen.com/terrorism1.html (21/09/2021).
[3] William L. Tafoya , "Cyber Terror. The Federal Bureau of Investigation", November 1, 2011, Available on: https://leb.fbi.gov/articles/featured-articles/cyber-terror (10/11/2021).
[4] Choi, Kyung-shick; Lee, Claire Seungeun; and Cadigan, Robert (2018) Spreading Propaganda in Cyberspace: Comparing Cyber-Resource Usage of Al Qaeda and ISIS, ***International Journal of Cybersecurity Intelligence & Cybercrime***, 1(1), p-p: 21-39. In: https://www.doi.org/10.52306/01010418ZDCD5438 (06/07/2021).

الجريمة بعينها ومعالجتها، ومع ذلك فإنه لوضـــع إطار قانوني يســـاعد على منع ارتكاب عمل إرهابي إلكتروني وردعه والدفاع عنه، يجب أن تكون الخطوة الأولى المناســـبة هي وضـــع تعريف علمي عملي يحدد بدقة نوع الهجمات التي ينبغي اعتبارها إرهابًا إلكترونيًا[1].

وكما جرى الإشارة إليه سابقا، ترجع نشأة مفهوم الإرهاب الإلكتروني (Cyber-terrorism) إلى فترة الثمانينيات من القرن الماضـــي مع "باري كولين" (Barry Collin)، الباحث في معهد الأمن والاستخبارات بكاليفورنيا[2]. وفي سياق الحديث عن نشأة الإرهاب السيبراني كمفهوم وظاهرة، وجبت الإشارة إلى الجهود الأمريكية، ففي 1997 عملت وزارة الدفاع الأمريكية على اختبار أمنها السـيبراني، وأصـبحت التهديدات الســـيبرانية في منظورها على قائمة التهديدات الجديدة. وفي 1999، أجرت الكلية البحرية للدراسات العليا أول دراسة جادة تخص الإرهاب الإلكتروني، وذلك لصالح استخبارات الدفاع الأمريكية. ولكن تعريف الدراسة للإرهاب السيبراني بدا ضيقا، إذ تم وصفه بأنه "التدمير غير القانوني أو تعطيل الملكية الرقمية لتخويف أو إجبار الحكومات أو المجتمعات ســعيا لتحقيق أهداف ســياســية أو دينية أو أيديولوجية"، والملاحظ في التعريف المقدم حينها اســتبعادُ توظيف الجماعات الإرهابية لتكنولوجيا المعلومات، وبحسب تعريف "جونالان بريكي" (Jonalan Brickey) يشير هذا النمط من الإرهاب إلى "استخدام القدرات السيبرانية لإجراء وتمكين العمليات العسكرية والتدميرية في الفضاء الإلكتروني، لخلق واستغلال الخوف عبر العنف أو التهديد به سعيا للتغيير السياسي"، وفي كتابه: "الإرهاب السيبراني– دراســات حالة" (Cyber Terrorism : Case Studies) الصـــادر عام 2014، ذكر الباحث بعض الأمثلة عن الإرهاب السيبراني ولكنها لم تخرج عن دائرة الاختراق والجريمة الإلكترونية، وغيرهما[3].

فيما ذهب البعض إلى تعريف الإرهاب السيبراني بشكل ضيق بوصفه "التدمير غير القانوني أو تعطيل الملكية الرقمية لتخويف أو إجبار الحكومات أو المجتمعات في السعي لتحقيق أهداف سياسية أو دينية أو أيديولوجية[4].

---

[1] Jeffrey Thomas Biller, ***Cyber-Terrorism: Finding a Common Starting*** Point, Master Thesis of Laws, George Washington University Law School,United States , 2012, p 16.

[2] Rabiah Ahmad, ZahriYunos, « A Dynamic Cyber-Terrorism Framework », ***International Journal of Computer Sciences and Information Security,*** Vol.30, No.30 (2012), p.01.

[3] Stefan Soesanto, « Cyber Terrorism: Why it exists ? Why it doesn't ? and Why i twill ? », realinstitutoelcano, in :https://cutt.us/PfXHT (17/04/2020)

[4] Ibid.

في حين قامت العديد من الحكومات بدمج مصطلح الإرهاب السيبراني في وثائقها الإستراتيجية لسبب أو لآخر. مثلا: تُعرِّف استراتيجية الأمن السيبراني في النمسا لعام 2013 الإرهاب الإلكتروني بأنه "جريمة ذات دوافع سياسية ترتكبها جهات حكومية و/أو جهات غير حكومية ضد أجهزة الكمبيوتر والشبكات والمعلومات المخزنة فيها. هدفها هو إثارة اضطراب شديد أو طويل الأمد للحياة العامة أو التسبب في ضرر جسيم للنشاط الاقتصادي بقصد تخويف السكان، أو إجبار السلطات العامة أو منظمة دولية على القيام بفعل أو التغاضي عنه أو إهماله. كما أنه يشير الى الإخلال العميق بالأسس السياسية أو الدستورية أو الاقتصادية أو الاجتماعية لدولة أو منظمة دولية أو تدميرها. تشكل هذه الأعمال تخريبًا إلكترونيًا منظمًا، تسببه الجماعات الأصولية السياسية أوالأفراد؛ ضد دول أو منظمات أو مؤسسات"[1].

وفي أعمالهم الأخيرة ضمن مؤسسة راند، أشار جون أركيلا John Arquilla وديفيد رونفلدت David Ronfeldt وميشيل زانيني Michele Zanini إلى ظهور أشكال جديدة من التنظيم الإرهابي تتناسب مع عصر المعلومات، مؤكدين أن "الإرهابيين سيستمرون في الانتقال من التسلسل الهرمي إلى شبكات دولية قائمة على المعلومات"[2].

تبعا لذلك، استغلت الجماعات الإرهابية التطور الكبير الذي حققته تكنولوجيات المعلومات وشبكة الانترنت، من خلال الولوج إلى المعلومات الحكومية المخزنة إلكترونيا، واستخدامها كوسيلة لابتزاز الحكومات والتأثير فيها، لتحقيق أهدافها وإيديولوجيتها العدائية، الأمر الذي استدعى مكافحة الإجرام عبر الانترنت، وهذا ما تحقق أخيرا عام 2001 عندما أُبرمت "**اتفاقية بودابست الأولى لمكافحة الإجرام عبر الانترنت**"[3].

كما يعرف الإرهاب الإلكتروني بأنه هجمات تستهدف نظم الكمبيوتر والمعطيات لأغراض دينية أو سياسية أو فكرية أو عرقية، وفي حقيقتها جزء من الجرائم الالكترونية cyber crime باعتبارها جرائم إتلاف

---

[1] Federal Chancellery, "Austria Cyber Security Strategy", 2013, p. 21, in : Austrian Cyber Security Strategy (bmi.gv.at)

[2] Maura Conway, "Reality bytes: Cyberterrorism and Terrorist of the Internet", ***First Monday***, 7(11).(2002), In : https://doi.org/10.5210/fm.v7i11.1001

[3] أمير فرج يوسف، ***مكافحة الإرهاب الالكتروني: الإرهاب الرقمي في ظل اتفاقية دول مجلس التعاون الخليجي لمكافحة الإرهاب*** (الإسكندرية: دار الكتب والدراسات العربية، 2015)، ص 125-127.

للنظم والمعطيات أو جرائم تعطيل المواقع وعمل الأنظمة، لكنها تتميز عنها بسمات عديدة، أبرزها أنها ممارسة لذات مفهوم الأعمال الإرهابية لكن في بيئة الكمبيوتر والانترنت وعبر الاستفادة من خبرات الكريكرز (أي مجرمي الكمبيوتر الحاقدين)، وفي إطار ذات السمات التي تتوفر في جماعات الجريمة المنظمة[1].

إرهاب الانترنت بذلك لا يختلف في معناه عن الإرهاب التقليدي وإن اختلف عنه في الوسيلة وبعض الأهداف، حيث يعبر إرهاب الانترنت عن استخدام الانترنت بوصفه وسيلة يمكن من خلالها شن هجوم واختراق أنظمة الأمن والشبكات أو توزيع فيروس كمبيوتري قوي واختراق شبكات الأمان للدول[2]. وتجب الإشارة إلى أنه لا يكفي أن يتواجد الإرهابي في الفضاء السيبراني، وإنما يجب وقوع شرط استخدام هذا الفضاء لأغراض إرهابية حتى نتحدث عن إرهاب إلكتروني[3].

تجادل سارة جوردون وريتشارد فورد بأن الإرهاب الذي يستهدف أجهزة الكمبيوتر والشبكات والمعلومات المخزنة فيها يمكن اعتباره "إرهابًا إلكترونيًا خالصًا"، بينما يعد "إرهابًا إلكترونيًا تقليديًا" عندما يحاول الإرهابيون الاستفادة من "العديد من عوامل وقدرات العالم الافتراضي (..) من أجل إكمال مهمتهم"، وفي هذا السياق يُعرّف الإرهاب الإلكتروني حسبهما باستخدام تكنولوجيا المعلومات من قبل الجماعات الإرهابية والأفراد لدعم أجندتهم، ويمكن أن يشمل ذلك استخدام تكنولوجيا المعلومات لتنظيم وتنفيذ هجمات ضد الشبكات وأنظمة الكمبيوتر والبنى التحتية للاتصالات، أو لتبادل المعلومات أو توجيه التهديدات إلكترونيًا[4].

---

[1] جعفر حسن جاسم، ***حرب المعلومات بين ارث الماضي وديناميكية المستقبل***، ط1، (عمان: دار البداية للنشر والتوزيع، 2010)، ص 64.

[2] رامي عطا صديق، فاطمة شعبان أبو الحسن، ***الإعلام والتنمية في مواجهة الإرهاب***، ط1، (مصر: دار أطلس للنشر والإنتاج الإعلامي، 2016)، ص 55– 56.

[3] Lillian Ablon, ***The Motivations of Cyber Threat Actors and their use and Monetization of Stolen Data,*** RAND Corporation, Testimony Presented before the House Financial Services Committee, Subcommittee on Terrorism and Illicit Finance (March 15th, 2018), in : www.rand.org/pubs/testimonies/CT490.html , p-p : 2-3.

[4] Dennis Broeders, and Others, « Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy », 02/06/2021, in: https://www.tandfonline.com/doi/full/10.1080/1057610X.2021.1928887 (15/11/2021)

وعرفه مكتب التحقيقات الفيدرالي (FBI) بأنه "هجوم مخطط، ذو دوافع سياسية، يستهدف المعلومات والأنظمة الإلكترونية وبرامجها وبياناتها، ويترتب على ذلك استخدام العنف ضد أهداف غير قتالية، بواسطة مجموعات وطنية فرعية أو عملاء سريين"[1].

فيما ذهب آخرون إلى أنه: "استخدام تكنولوجيا المعلومات من قبل جماعات إرهابية أو أفراد من أجل تحقيق أهدافهم"، وهذا يتضمن توظيف تكنولوجيا المعلومات لتنفيذ هجوم ضد الشبكات أو أنظمة الحاسوب والبنية التحتية للاتصالات[2]. كما يُنظر إلى الإرهاب السيبراني بوصفه استخدام الانترنت كوسيلة وهدف للقيام بأعمال إرهابية، أو هو "مجموع العمليات الإرهابية السيبرانية التي تهدف إلى زعزعة نظام الدولة"[3].

واقترح مارك بوليت Mark Pollitt الوكيل الخاص السابق لمكتب التحقيقات الفيدرالي، أحد التعريفات العملية الأولى كالآتي: "الإرهاب الإلكتروني هو الهجوم المتعمد بدوافع سياسية ضد المعلومات وأنظمة وبرامج الكمبيوتر والبيانات التي تؤدي إلى عنف ضد أهداف غير قتالية من قبل مجموعات فرعية وطنية أو سرية أو وكلاء[4].

---

[1] بيتر سينجر، "الإرهاب الإلكتروني: خرافات، وحقائق، وفيروس ستوكسنت، وتنظيم داعش، ووسائل الإعلام الاجتماعي، ومسرح المواجه"، سلسلة محاضرات الإمارات، أبو ظبي: مركز الإمارات للدراسات والبحوث الإستراتيجية (أوت 2018)، ص03.

[2] Mitko Bogdanoski, Drage Petreski, « Cyber-Terrorism : Global Security Threat », ***International Scientific Defense***, Security and Peace Journal, p.59.

[3] Carolle Vodouche, ***La Contribution des Dynamiques Internationales Formelles au Renforcement de la Cybersécurité Canadienne***, Mémoire présenté à la faculté des études supérieures, Université de Montréal, en vue de l'obtention du garde de maitrise en droit (LL.M.), Option : Droit des technologies de l'information (Mai 2015), p-p : 16-17.

[4] Aziz Douai, Technology and terrorism: Media symbiosis and the "dark side" of the web, in: Lorenzo Cantoni and James A. Danowski, ***Communication and Technology***, (De Gruyter Mouton , 2015), p 448.

وقد ظهرت مدرستان فكريتان اهتمتا به: الأولى تتزعمها "دوروثي دنينغ*" الخبيرة في أمن المعلومات، والثانية يمثلها مسؤولون حكوميون وعسكريون يعرفونه بأنه "أي هجوم إلكتروني يهدد أجهزة الحاسوب وشبكات المعلومات"[1].

وانطلاقا من أعمال الأستاذة دوروثي دينينج "DorothyDeening"، يُعرّف الإرهاب السيبراني بأنه "نقطة التّماس بين الإرهاب والفضاء الإلكتروني"، وهو يشير إلى الهجمات غير القانونية والتهديدات بالهجوم على أجهزة الكمبيوتر والشبكات والمعلومات المخزنة فيها عند القيام بذلك لتخويف أو إكراه حكومة أو شعبها من أجل تحقيق أهداف سياسية أو اجتماعية، كما يمكن أن تكون الهجمات الخطيرة ضد البنى التحتية الحيوية أعمال إرهاب إلكتروني، اعتمادًا على تأثيرها، أما الهجمات التي تعطل الخدمات غير الأساسية أو التي تشكل مصدر إزعاج غير مكلف بشكل أساسي (أي غير مصحوبة بالعنف والإكراه المادي) فلن تكون كذلك"[2]. معنى ذلك ضرورة أن يؤدي هذا النمط من الهجمات إلى عنف مادي ضد الأفراد أو الممتلكات، أو يكون حجم الضرر كافٍ لإنتاج حالة من الرعب[3]. وتستشهد "دنينغ" ببعض الأمثلة في هذا الصدد مثل: هجوم نمور التاميل على مواقع سفارات سريلانكا في عام 1998، عبر رسائل البريد الإلكتروني لتعطيل الخدمة، وأيضا الهجمات الاحتجاجية على إثر قصف حلف الشمال الأطلسي (الناتو) لكوسوفو في عام 1999[4].

• **دوروثي إليزابيث دينينج** Dorothy Elizabeth Denning ، المولودة في 12 أغسطس 1945، هي باحثة أمريكية في مجال أمن المعلومات، معروفة بالتحكم في الوصول المعتمد على الشبكة lattice-based access control (LBAC) وأنظمة كشف التسلل intrusion detection systems (IDS)، وغيرها من ابتكارات الأمن السيبراني. نشرت أربعة كتب وأكثر من 200 مقال، وتم إدراجها ضمن القائمة الوطنية لمشاهير الأمن السيبراني عام 2012، وهي الآن أستاذة فخرية متميزة في تحليل سياسات الدفاع بكلية الدراسات العليا البحرية. أُنظر: https://faculty.nps.edu/dedennin/

[1] أحمد محمد وهبان، ***ظاهرة الإرهاب بين صورها التقليدية وأنماطها المستحدثة*** (المملكة السعودية: إصدارات الجمعية السعودية للعلوم السياسية، 2015)، ص26.

[2] Dorothy Denning,. "Cyberterrorism", ***Global Dialogue*** (Autumn), 24 August 2000, in :Cyberterror-Denning.pdf - Cyberterrorism DOROTHY E DENNING This is a prepublication version of a paper that appeared in Global Dialogue Autumn 2000 In | Course Hero

[3] Rabiah Ahmad, Zahri Yunos, ***Op.cit***, p.02.

[4] أحمد محمد وهبان، ***مرجع سابق***، ص30.

لقد أصـــبحت جريمة الإرهاب الإلكتروني في مقدمة الجرائم الخطيرة محليا ودوليا، خاصـــة وأنها تهدد خصـوصـية الفرد وأمنه الشـخصـي وقيم المجتمع، وبمقدورها أيضـا أن تمسّ البنية التحتية لقطاعات كبيرة في الدولة. وهو ما يعزز فكرة العدو غير التقليدي، الذي قد لا نعرف عنه أشـــياء كثيرة ولكنه يملك مفاتيح نشـر الخوف والرعب لدى ضـحاياه ومن ضـمن هذه المفاتيح اسـتغلال التطور التكنولوجي وثورة المعلومات في التهديد والتخفي وإلحاق الضرر.

والفضـاء السـيبراني "يتوسـع ويتمدد بشـكل سـريع، وبنهج غير مرئي، وضـمن نسـيج دقيق لا يمكن توقعه وينخر في أشدّ الأبنية المعرفية قوة وتماسكا"[1]. من هنا يظهر حجم الخطر والتهديد.

وجاءت في مقدمة تقرير مكتب الأمم المتحدة المعني بالمخدرات والجريمة لعام 2012[2] مقولة للأمين العام السابق لمنظمة الأمم المتحدة "بان كي مون":

"الإنترنت هي خير مثال يوضـح كيف يمكن للإرهابيين أن يمارسـوا نشـاطهم على نحو عابر للحدود حقا، وتصديا لذلك ينبغي للدول أن تفكر وتعمل على نحو عابر للحدود أيضا".

تعكس هذه المقولة بالفعل حجم الخطر الذي باتت تشـكله الشـبكة العنكبوتية في فضـــاء يتجاوز منطق الحدود الوطنية، حتى أصـبح سـاحة ووسـيطا لممارسـة شـكل جديد من الإرهاب في صـورة إرهاب إلكتروني وتهديدات سيبرانية على نطاق واسع.

وتأسـيسـا على ما ذُكر سـلَفًا، يظهر أن التعريفات الحالية للإرهاب السـيبراني متباينة على نطاق واســـع في نطاق الإجراءات التي تندرج تحت تعريفها، وهذا الاختلاف يجعل من الصـــعب وضـــع استراتيجيات وتكتيكات مشتركة لردع الإرهاب السيبراني، ومع ذلك فإنه لوضـع إطار قانوني يسـاعد على منع ارتكاب عمل إرهابي إلكتروني يجب أن تكون الخطوة الأولى المناسبة هي وضـع تعريف علمي عملي يحدد بدقة نوع الهجمات التي ينبغي اعتبارها إرهابًا إلكترونيًا[3].

---

[1] إســـماعيل أوقادي، "الفضـــاء الرقمي والحاجة إلى باراديغم قانوني جديد"، (المغرب: مركز تكامل للدراســـات والأبحاث، 2020)، 2021/01/15 https://www.takamoul.org/author/author02/ (2021/10/16)

[2] مكتب الأمم المتحدة المعني بالمخدرات والجريمة، ***مرجع سابق***، ص05.

[3] Jeffrey Thomas Biller, ***Cyber-Terrorism: Finding a Common Starting Point,*** Master Thesis of Laws, George Washington University Law School, United States , 2012, p 16.

بناءً على ذلك، يمكن تقديم **تعريف إجرائي للإرهاب الإلكتروني** كما يلي:

هو استخدام الوسائل الإلكترونية، من أجل تخويف وترويع الآخرين، وإلحاق الضرر بهم أو تهديدهم، وذلك بدوافع سياسية أو أيديولوجية غالبا.

وتجب الإشارة هنا إلى أن الهجمات الإرهابية الإلكترونية متعمدة ويتم التخطيط لها، وهي تهدف إلى تعطيل أو تدمير أنظمة الكمبيوتر، إلى جانب أهداف أخرى سياسية وأيديولوجية، وغالبا ما تستهدف المصالح المدنية لتنتج على الأقل ضررا ما يولّد الخوف[1].

وفي ظل الجدل الدائر حول المفهوم والماهية، يمكن تمييز صنفين من الإرهاب الإلكتروني هما[2]:

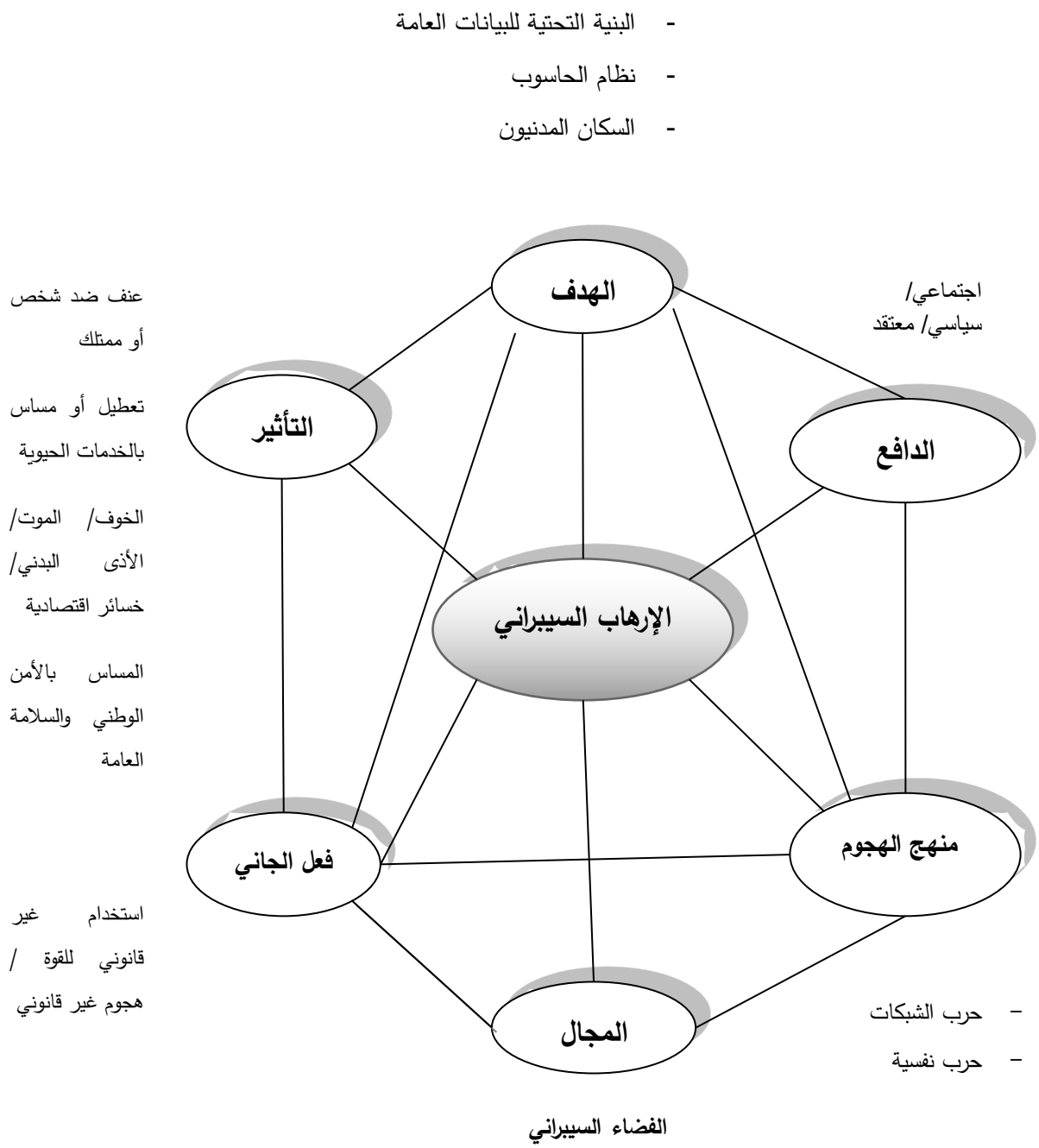
- **الإرهاب الإلكتروني الهجين** (Hybrid Cyberterrorism): ويشـــمل تكتيكات واســـتخدامات التكنولوجيا لدى الجماعات الإرهابية، إذ أصبح الاعتماد على تقنيات التواصل المتطورة ومنصات التواصل الاجتماعي في الدعاية والتجنيد ونشر التطرف حلقة محورية في نشاط الجماعات الإرهابية.
- **الإرهاب الإلكتروني المحض** (Pure Cyberterrorism): وهو ذلك النمط من الهجوم السيبراني الذي يمس مباشرة البنية التحتية الإلكترونية للضحية أو الشبكات والمعلومات.

يوضح المخطط التالي عناصر الإرهاب السيبراني وتفاعلاتها الوظيفية والبنيوية:

[1] Jarkko Moilanen, ***Op.cit***, p 29.

[2] Mayssa Zerzki, ***The Threat of Cyberterrorism and Recommendations for Counter Measures, Perspectives on Tunisia***, Center for Applied Policy Resarch-CAP (April, 2017), p-p: 2-3.

الشكل (1): مخطط يوضح عناصر الإرهاب السيبراني.



Source: Rabiah Ahmad, Zahri Yunos, « A Dynamic Cyber-Terrorism Framework », International ***Journal of Computer Sciences and Information Security***, Vol.30, No.30 (2012), p.06.

المطلب الثاني: دوافع الإرهاب السيبراني.

تتنوع أسباب الإرهاب الإلكتروني، وقد تكون نفسها أسباب الإرهاب العادي أو التقليدي، ولكن الفرق يكمن في الوسيلة المستخدمة لتحقيق الهدف. ومن المعلوم أن عوامل عديدة تؤدي إلى تحول الشخص العادي إلى شخص إرهابي، ثم تدفعه إلى تطوير أساليب نشاطه وفقا لظروف معينة. فالإرهاب ظاهرة مركبة ومعقدة، ليس لها دافع واحد وإنما مجموعة من الدوافع والأسباب قد يختلف تأثيرها نسبيا، ولكن في حالة الإرهاب الإلكتروني يبرز دور التكنولوجيا باعتباره تهديدا جديدا يندرج في إطار الموجة الخامسة التي تعتمد على التطور التقني والمعلوماتي بصورة أساسية.

وإذا كانت نظرية النشاط الإجرامي الاعتيادي تقول ان احتمال الجريمة يرتبط بثلاثة عناصر هي: **الدافع، الهدف وغياب الرقيب**[1]، فإن أسباب الإرهاب الإلكتروني كثيرة ومتنوعة، ويمكن تصنيفها كما يلي:

أ. أسباب اجتماعية واقتصادية:

يجري الربط بين العامل النفسي والاجتماعي في فهم التحول نحو ممارسة أشكال العنف السياسي ومن بينها الإرهاب، ويعد الحرمان النسبي من الحاجات الأساسية (اجتماعية كانت أو اقتصادية) نقطة أساسية في ذلك، "وكلما ازدادت شدة السخط ازداد احتمال حصول العنف، وتتحدد خصوصية هذا الدافع إلى العمل بما يعتقد الناس أنه مصدر الحرمان، وأنه المبرر المعياري والنفعي لأعمال العنف الموجه إلى المسؤولين عنه"[2]. وتناولت نظرية "تيد روبرت غير" (Ted Robert Guerr) بخصوص الحرمان النسبي، والتي طورها مطلع السبعينيات، مسألة العلاقة بين العامل الاقتصادي والاجتماعي والعنف السياسي، كما اهتم باحثون آخرون بهذا العامل في فهم وتفسير الظاهرة الإرهابية[3].

---

[1] مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية، البند 5 من جدول الأعمال المؤقت، "النهج الشاملة المتوازنة لمنع ظهور أشكال جديدة ومستجدة للجريمة العابرة للحدود الوطنية والتصدي لها على نحو ملائم"، الدوحة: 12–19 ابريل 2015، ص10.

[2] تيد روربرت غير، ***لماذا يتمرد البشر؟***، تر: مركز الخليج للأبحاث، ط1، (الإمارات العربية المتحدة: مركز الخليج للأبحاث، 2004)، ص53.

[3] سمر حسن الباجوري، "الأسباب الاقتصادية لتنامي ظاهرة الإرهاب في إفريقيا جنوب الصحراء"، 31 ماي 2016، https://mpra.ub.uni-muenchen.de/74740، (3 ماي 2021).

تعد الظروف الاجتماعية والاقتصـــادية للفرد محفزا على الفعل الإرهابي، وذلك تعبيرا عن رفض الواقع والشعور بحالة من الاغتراب والحرمان من الحاجات الأساسية والحق في العيش الكريم، خاصة مع وجود فرق واضح بين مستوى معيشة الفرد ومستوى معيشة الحكام والمسؤولين في بلده وغياب العدالة في توزيع الثروة، وفشل برامج التنمية خاصة مع اعتماد دول الجنوب على اقتصاد النفط، حيث "اتسعت الفجوة بين الواقع الاجتماعي وبين الحكام فغابت العدالة ونشـــأت الاختلالات الاقتصـــادية والاجتماعية"[1]. وقد تؤدي السياسات الاقتصادية إلى زيادة الفجوة والحاجة لدى الفرد، فتنتشر البطالة والفقر وينهار مستوى المعيشة[2].

ولا يتوقف تأثير العوامل الاجتماعية والاقتصادية في نشأة الإرهاب على النطاق الداخلي المحلي، وإنما له ارتباط أيضا بالظروف الدولية. فتقلبات الاقتصاد العالمي وتناقضات العولمة ونزعة السيطرة لدى الرأسمالية، كلها عوامل ساهمت في ظهور موجة الإرهاب الدولي بصفة عامة[3]. والعولمة، بما فرضته من اندماج لاقتصاديات الدول عبر التجارة والاستثمار وتدفق رأس المال، أدت بالموازاة إلى انتقال الجرائم من طابعها الوطني المحدود إلى العابر للحدود[4].

وجاء على لســـان الأمين العام للأمم المتحدة "أنطونيو غوتيرش" (Antonio Guterres): "إن خلق مجتمعات تعددية شاملة مفتوحة منصفة، تقوم على أساس الاحترام الكامل لحقوق الإنسان، وتضمن العدالة الاقتصـادية للجميع، يمثل بديلا ملموسـا وهادفا، لحماية الشـخص من السـير في طريق التطرف العنيف"[5]. وهو تأكيد صريح على دور البيئة الاجتماعية والاقتصادية للفرد في تحديد سلوكه ونشاطه.

---

[1] إدريس عطية، التهديدات الإرهابية.. ***مرجع سابق***، ص: 49، 50.

[2] علي العبيدي، الإرهاب واستعصاء المفهوم، ***مرجع سابق***، ص140.

[3] إدريس عطية، ***مرجع سابق***، ص: 48، 50.

[4] مؤتمر الأمم المتحدة الثالث عشر، مرجع سابق، ص: 06-07.

[5] خالد ســـعيد، بثينة صـــلاح، "التهميش والحرمان أقوى دوافع التطرف"، 9 نوفمبر 2017، https://cutt.us/ACclh، (3 ماي 2021).

ب. أسباب سياسية:

تتمثل الأسباب السياسية التي تشجع على تفشي الهجمات الإرهابية الإلكترونية في قمع السلطة والتضييق على المشاركة وممارسة الحريات السياسية، والذي تتعرض له بعض الأطراف والجماعات في الدولة، سواء لكونها تحمل فكرا مختلفا ومتطرفا، أو لأنها فئات معارضة سياسيا ويُراد إقصاؤُها في ظل سيطرة نظام حكم مستبد. ويلعب الدافع السياسي دورا هاما في نشأة الإرهاب كأسلوب مواجهة وانتقام أو حتى تغيير، باستخدام أساليب الاغتيال ووصولا لممارسة الإرهاب الإلكتروني واستهداف أمن الدولة والبنى التحتية الحساسة عن طريق الوسائل التكنولوجية.

من جهة أخرى، يمكن أن يرتبط الدافع السياسي بالتدخل الخارجي، كما كان الحال مع العراق على إثر غزوها في 2003، أو مع ليبيا منذ 2011، حيث تُجمع بعض الدراسات على أن التدخل الأجنبي هو عامل أساسي في نشأة وانتشار الظاهرة الإرهابية بكل أشكالها.

ت. أسباب إيديولوجية:

تتمثل الدوافع الإيديولوجية في الأفكار المسيطرة على جماعة أو تنظيم ما، والتي تأخذ أحيانا طابعا دينيا ومضمونا متطرفا نابعا من الفهم الخاطئ للدين. وتعد الفكرة ذات تأثير خطير على الفرد والمجتمع، وفي التاريخ القديم والمعاصر أمثلة كثيرة على ذلك، كما أن انتشار الفكر المتطرف والنشاط الإرهابي بسرعة ملحوظة خلال الأعوام الأخيرة (كما كان الحال مع تنظيم الدولة "داعش" الإرهابي)، بالاعتماد على الوسائط التكنولوجية وغيرها من إستراتيجيات الاستقطاب، لَدليلٌ على دور الدوافع الإيديولوجية في تحفيز الإرهاب بكل أشكاله، وحتى الإرهاب الإلكتروني المدفوع سياسيا وفكريا لا يخرج عن هذا السياق.

ث. أسباب تتصل بالتكنولوجيا:

أدى التطور التكنولوجي وانتشار تكنولوجيا المعلومات والاتصالات الجديدة إلى تغيير أسلوب الحياة، فمع انتشار الحواسيب والهواتف المحمولة وشبكة الإنترنت برز مظهر من مظاهر عصر جديد يختلف عن العصور السابقة، وهو عصر تحتل فيه التكنولوجيا والمعلوماتية مكانا بارزا في تقدّم الشعوب والدول، ولكن هذا التطور أصبح له أثر عكسي؛ففي مقابل سهولة الاتصالات واختصار المسافات وتحول

العالم إلى قرية كونية، ظهر تهديد جديد متمثل في الإرهاب الإلكتروني، ويمكن ذكر أهم أسـبابه المرتبطة بالتكنولوجيا كما يلي:

- لقد كانت الفواصل الجغرافية في الماضي مصدرا للحماية من التهديدات، أما مع ظهور الفضاء الرقمي فقد أصبحت ميزاته العالمية والعابرة للحدود مصدرا للتهديد مادام الإبحار فيه متاحا لأي شخص[1]، كما أن كل القطاعات والمجالات تعتمد اليوم على الفضـاء السـيبراني (الدفاع الوطني، البنوك، الضـرائب، العدالة..)، مما يشجع الإرهابيين على استغلاله في مهاجمة الحكومات واستهداف قيم المجتمعات.
- تؤكد تقارير الأمم المتحدة على دور "الموصـــولية العالمية" في تحفيز الفعل الإجرامي من خلال تبادل المعلومات والخبرات عبر الوسائط الإلكترونية، في ظل الاستفادة من انتشار استخدام وتدفق الإنترنت. والفضـاء السـيبراني قد أتاح بالفعل الفرصـة لارتكاب جرائم مسـتحدثة على غرار الإرهاب الإلكتروني، حيث لم يكن بالإمكان ارتكابها في الفضـاء المادي التقليدي، مع الاسـتفادة من "إمكانية اتخاذ هويات غير ثابتة، وإخفاء الهوية، وغياب الرادع"[2].
- التكلفة في حالات الإرهاب الإلكتروني تكون أقل منها في حالة الإرهاب التقليدي، ففي الأولى يكفي أن يمتلك الشخص جهاز حاسوب ويتصل بالأنترنت ليستخدمه بالطريقة التي تخدم الهدف المرجو3. لذلك فإن انخفاض التكلفة في العادة، وسـهولة اسـتخدام الوسـائل التكنولوجية، يشـجعان الإرهابي على اسـتغلالها[4]. ولا ينقصـه في ذلك سـوى الذكاء والاحترافية في التعامل مع شـبكة الإنترنت وجهاز الحاسوب مثلا، بالتالي فإن عدم الحاجة إلى معدّات ولوازم مادية كثيرة وأموال كبيرة لتنفيذ عمل إرهابي عبر الوسائط الإلكترونية يُعد على قائمة الأسباب المحفزة لممارسة الإرهاب الإلكتروني.
- ضعف بنية شبكة المعلومات عبر توفرها على ثغرات، مما يجعلها عرضة للتلاعب والاختراق، وهو ما تستغله الجماعات الإرهابية في ضرب الدول عبر الوصول إلى بيانات حساسة وتنفيذ أعمال تخريب[5].

---

[1] The White House, ***The National Strategy to Secure Cyberspace*** (Washington, February 2003), p.7.

[2] مؤتمر الأمم المتحدة الثالث عشر، مرجع سابق، ص: 10-11.

[3] John J. Klein, Op.cit, p.25.

[4] مصطفى يوسف كافي، ***مرجع سابق***، ص151.

[5] عنترة بن مرزوق، "جريمة الإرهاب الإلكتروني: الأسباب وآليات العلاج"، ***مجلة الحقوق والعلوم الإنسانية***، العدد 2 (جوان 2018)، ص513.

- سـهولة أو إمكانية التخفي عبر إنشـاء هوية افتراضـية زائفة، مما يجعل الإرهابي الإلكتروني يفلت من رقابة الدولة، وهو ما يشكل صـعوبة أيضـا في عملية إثبات وقوع جريمة في هذا الفضـاء[1]. وهذا سبب كفيل لأن يدفع بالإرهابيين إلى الاعتماد على تكنولوجيا المعلومات كأسـلوب بديل بعد حملة التتبع ومواجهات الدول أمنيا للجماعات والتنظيمات الإرهابية في أماكن تواجدها واختبائها.
- أصبحت وسائط التكنولوجيا ومنصات التواصل الاجتماعي (فيسبوك، تويتر..) خلال السنوات الأخيرة وسيلة فعالة لنشر الفكر المتطرف وتشجيع الإرهاب في المجتمعات، وهو ما ظهر بوضوح مع تنظيم "داعش" الإرهابي الذي اعتمد في إستراتيجيته على الإنترنت في التجنيد الإلكتروني والدعاية لمشروعه، واستطاع بذلك أن يستقطب عشرات الآلاف من المقاتلين المنخرطين في صفوفه.
- إيجاد قنوات جديدة للحصـول على الأموال وعقد صـفقات غير مشـروعة، بالإضـافة إلى تدريب الأفراد على العمل الإرهابي.

انطلاقا من ذلك فإن الأسـباب التي تتصـل بالتكنولوجيا أسـاسـية وهامة في النشـاط الإرهابي الإلكتروني، والإرهابيون يسـعون باسـتمرار لاسـتحداث طرق وأسـاليب عمل للتغلب على التحديات التي تواجه الجماعات الإرهابية وتعرقل نشاطها.

ج– أسباب أمنية:

يقصـد بالأسـباب الأمنية حملات المطاردة للجماعات الإرهابية والإجرامية على الصـعيد الوطني والدولي، مما دفع بها منطقيا إلى استغلال تكنولوجيا المعلومات المتطورة واتخاذ الفضـاء السيبراني ساحة جديدة للتواصـل فيما بينها والتحرك والنشـاط. وبالنظر إلى غياب الحدود في المجال الإلكتروني وغياب الرقابة أو عجز الحكومات عن تأمينه، أصـبح بمنزلة الملجأ والملاذ الأكثر أمنا بالنسـبة للجماعات الإرهابية، سواء في التواصل فيما بينها بحسابات زائفة ولغة مشفرة أو في نشر الفكر المتطرف والسعي إلى تصـديره إلى أكبر شـريحة ممكنة من المجتمع لاسـتقطاب الأفراد والتأثير في تماسـك العلاقات الاجتماعية وعلاقات المواطنين بالحكومة.

[1] ***المرجع نفسه***، ص 513

ح. دوافع تتعلق بهدف التأثير:

ويشـــمل ذلك التأثير على الأفراد وقراراتهم[1]، وهو كما تمت الإشـــارة إليه أعلاه مرتبط بالتغلغل الفكري واسـتقطاب أكبر فئة من الجمهور المسـتهدف بصـورة تجعله مناصـرا أو منتميا إلى الجماعة أو التنظيم الإرهابي.

بشكل عام، هناك العديد من الأسباب التي تجعل الهجمات الإلكترونية خيارًا جذابًا للإرهابيين:

- نظرًا لأن الإرهابيين لديهم كمية محدودة من الأموال، فإن الهجمات الإلكترونية تكون أكثر إغراءً لأنها تتطلب عددًا أقل من الأشخاص وموارد أقل (مما يعني أموالًا أقل). من ناحية أخرى، يمكنهم استهداف والتأثير على أعداد كبيرة من الأشـخاص الذين لديهم نفس القدر من الأموال، وبعبارة أخرى، فإن نسـبة الفائدة إلى التكلفة مرتفعة للغاية.
- تمكن الإرهابيين من البقاء مجهولين، حيث يمكن أن يكونوا بعيدين عن المكان الفعلي الذي يتم فيه تنفيذ الهجوم الإرهابي.
- لا توجد حواجز مادية أو نقاط تفتيش يتعين عليهم عبورها.
- لا تعتمد سرعة الهجمات وشكلها على سرعة اتصال المهاجم،كما يمكن استغلال سرعة اتصال أجهزة الكمبيوتر الضحية التي تم التقاطها بشكل كامل.
- يُعتقد أن الجمع بين كل من الإرهاب المادي والإرهاب السيبراني هو الاستخدام الأكثر فعالية للإرهاب السيبراني[2].

ومن خلال عرض بعض دوافع الإرهاب بصفة عامة والإرهاب الإلكتروني بصورة خاصة يتضح كيف أن الظاهرة الإرهابية شديدة التعقيد والخطورة، وكيف أن الإرهاب الإلكتروني خطرٌ يفرض نفسه في الوقت الراهن ويفرض على الحكومات استحداث وتطوير السياسات والآليات للتصدي له.

[1] Rabiah Ahmad, Zahri Yunos, ***Op.cit,*** p.7.

[2] Murat Dogrul, Adil Aslan, Eyyup Celik, "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism", ***3rd International Conference on Cyber Conflict***, C. Czosseck, E. Tyugu, T. Wingfield (Eds.) Tallinn, Estonia, 2011, pp 32-33.

المطلب الثالث: خصائص الإرهاب السيبراني.

للإرهاب الإلكتروني خصائص تجعله مختلفا عن جريمة الإرهاب في صورتها التقليدية المعروفة، وهي تتمثل بوجه عام فيما يلي:

- خاصية تتعلق بطبيعة المجال:

إذا كان العالم المادي يتميز بوجود حدود وأقاليم جغرافية، فإن العالم السيبيري لا سيادة فيه ولا حدود، وإنما هو متعدد القوميات multinational، عابر لها trans–national، وفوق القوميات supranational. يضاف إلى ذلك خاصية غياب النظامية، غياب المركزية، تجاوُز المحلية، كل ذلك بالإضافة إلى نمو مجتمعات افتراضية داخل المجال غير المادي[1]. فالإرهاب الإلكتروني جريمة تتخذ من الفضاء السيبراني مسرحا لها كبديل أو مكمل للفضاء المادي التقليدي، ومن وسائط التكنولوجيا وشبكة الإنترنت وسيلة في تنفيذ مبتغاها. وتستفيد في ذلك من الخصائص التي يتمتع بها هذا الفضاء وفي مقدمتها غياب الحدود الجغرافية وسهولة الحركة. فالجماعات الإرهابية التي تقوم بهذا النوع من الجرائم تجد سهولة في الإبحار في فضاء بلا حدود، ومن هذا المنطلق يمكن للإرهاب السيبراني أن يأخذ الطابع الدولي العابر للحدود.

- خاصية تتعلق بسهولة التخفي وصعوبة الإثبات:

من خصائص الإرهاب الإلكتروني، إضافة إلى كونه جريمة عابرة للحدود، السرعة والمرونة وسهولة التخفي ومحو الأثر، وهي خصائص الجرائم الإلكترونية عموما، مما يطرح إشكالية الإثبات والمتابعة القضائية[2]، انطلاقا من "الخاصية الديناميكية للفضاء الرقمي في مقابل الطابع السكوني نسبيا للقانون"[3]. وبالحديث عن المنظومة القانونية وَجَب أن يتكيف التشريع المحلي والدولي باستمرار مع التحول في طبيعة التهديدات والتطور في الجرائم المستحدثة، خاصة وأنها تتطور بشكل سريع.

---

[1] Chems Eddine Chitour, ***Mondialisation : l'Espérance ou le Chaos ?*** (Alger : ANEP, 2002), p-p : 189-190.

[2] روان بنت عطية الله الصحفي، "الجرائم السيبرانية"، ***المجلة الإلكترونية الشاملة متعددة التخصصات***، العدد 24 (مايو 2020)، ص: 11، 12.

[3] إسماعيل أوقادي، مرجع سابق، ص12.

- الإرهاب الإلكتروني جريمة ناعمة:

فهو نمط من الجرائم التي "لا تُمارَس بالعنف، ولا تحتاج إلى أدنى مجهود عضلي، بعكس بعض الجرائم التقليدية"[1]، وبعكس الأعمال الإرهابية في صورتها التقليدية التي تتطلب العنف كشرط وعنصر ثابت. فالإرهاب الإلكتروني لا يتسبب بالضرورة في عنف وضرر جسدي للضحية، وإنما يشكل تهديدا كبيرا لسرية المعلومات وخصوصيتها والبنية التحتية لها واستقرار المجتمعات عبر نشر الفكر المتطرف، مما ينتج حالة من الرعب وهاجسا أمنيا متواصلا.

- خاصية تتعلق بالسمات الشخصية لمرتكب الجريمة:

حيث يتمتع مرتكبو الإرهاب السيبراني بقدرة عالية ومهارة وذكاء ودرجة من الاحترافية في التعامل مع الوسائل التكنولوجية المتطورة كالحواسيب وأجهزة الهاتف الذكية، ولهم خبرة وتخصص في توظيف شبكة الإنترنت لأغراض غير نبيلة، وهذا ما يميز الإرهابي الإلكتروني عن الإرهابي العادي الذي يكفي أن يتحكم في استخدام السلاح التقليدي ويحافظ على سرية العمل. وفي مقابل تلك الخاصية، تظل خبرات الأجهزة الأمنية ناقصة في كشف جريمة الإرهاب السيبراني[2].

- خاصية تتعلق بطبيعة الفواعل في الفضاء الإلكتروني:

المعروف هو أن الفضاء السيبراني لا تستخدمه الدول فحسب، وإنما تتعدد فيه الفواعل من غير الدول، مما يجعل تأثيراته خطيرة[3]. فمن الممكن أن يكون فرد واحد أو جماعة من ضمن الفواعل المهددة لأمن الدول والمجتمعات في هذا الفضاء، وهو ما ينطبق على الجماعات المتطرفة والتنظيمات الإرهابية.

---

[1] روان بنت عطية الله الصحفي، ***مرجع سابق***، ص13.

[2] راجع: هشام بشير، "الإرهاب الإلكتروني في ظل ثورة المعلومات"، 1 مايو 2012، https://araa.sa/index.php?option=com_contentview=articleid=244:2014-06-13-16-21-31catid=132:articlesltemid=294 (25 ابريل 2021).

[3] إسماعيل زروقة، ***مرجع سابق***، ص1020.

وتعدد الفواعل في الفضاء الرقمي نابع أيضا من خصوصية ثورة المعلومات التي أتاحت للجميع الاستفادة منها واستغلالها، فقد تكون هذه الفواعل مؤسسات رسمية أو جماعات منظمة أو أفرادا[1].

- خاصية تتعلق بهشاشة الفضاء الإلكتروني وهشاشة الأمن داخله:

الفضاء السيبراني مختلف عن الفضاء المادي، من حيث الخضوع لقوانين ذات طبيعة مختلفة، حيث يتقلص الزمن والمكان وتتلاشى الحدود، ويصعب التعرف على مرتكبي الهجمات الإلكترونية. وتبقى الصفة الغالبة على هذا الفضاء هي الهشاشة، من منطلق التطور المستمر في تكنولوجيا المعلومات والتعقيد المستمر الذي يميز هذا الفضاء، وتأثير ذلك على مستوى الأمن داخله[2].

وكخلاصة لهذا العنصر المتعلق بخصائص الإرهاب الإلكتروني يمكن القول بأن هذا النمط من الإرهاب قد استفاد من الميزات التي تتصل بالفضاء الإلكتروني، وبالتالي انعكست تلك الميزات على خصوصية الجريمة والتهديد وخصوصية مرتكبيها.

المطلب الرابع: المفاهيم المرتبطة والمتداخلة مع الإرهاب الإلكتروني.

يتداخل مع مفهوم الإرهاب السيبراني عددٌ من المفاهيم مثل: الحرب السيبرانية، الجريمة السيبرانية والجهاد السيبراني. بالتالي كان من الضروري محاولة تمييز هذه المفاهيم عن بعضها البعض، وإن كانت تشترك في الصفة نفسها (السيبرانية) أي أن الظواهر ذاتها تحدث في الفضاء نفسه وهو الفضاء السيبراني، كما تتداخل معرفيا وواقعيا كما سنرى.

أ. الحرب السيبرانية:

ينطلق كلاوزفيتز K.V.Clawsewitz في تحديده لطبيعة الحرب في مقارنتها مع المبارزة، التي يعرفها على أنها صراع بين طرفين حيث يحاول كل طرف إخضاع خصمه لإرادته، وهكذا الحرب صراع واشتباك وقتال على نطاق واسع بين طرفين –دولتين– لكي يخضع كل طرف خصمه لإرادته. الحرب

[1] Angela Gendron, Martin Rudner, ***Evaluation des Cybermenaces Pesant Contre les Infrastructures du Canada,*** Rapport Préparé pour le Service Canadien du Renseignement de Sécurité (Mars 2012), p.25.
[2] Philippe Wolf, Luc Valée, ***Cyber-Conflits, Quelques Clés de Compréhension***, INHESJ/ONDRP (2011), p-p : 791-792.

وفق كلاوزفيتز إذًا مبارزة كبرى[1] في حين أن أبرز تحدٍ للاستراتيجيين هو تحديد هدف الحرب، ويدرك من قرأ أعمال كلاوزفيتز أن هذه المسألة تحتل موقع القلب من اشتباكه النظري مع موضوع الحرب، فبعد توصل كلاوزفيتز إلى أن العمليات العسكرية كافة يجب أن تكون موجهة –كما يفرضه المنطق– نحو نزع سلاح العدو بأقصى سرعة ممكنة، قضى وقتا طويلا، وبذل جهدا كبيرا محاولا تفسير تعذر تحقيق هذا الهدف في معظم الأحيان، وساعيا إلى إيجاد حل بديل، والنتيجة أنه أدرك أن الحرب عمل سياسي محض[2]، فعرفها بأنها استمرار للسياسة بوسائل أخر[3]، تشن لتحقيق أهداف محددة، فلا بد من أن تُرى ضمن نطاق أهدافها وضمن طبيعة القوى التي تشنها[4].

ولأن الحرب عمل يقوم به طرفان، سيتسابق كلاهما لتدمير الآخر بما له من تقنيات، هذا يعني أن كلا الطرفين يعمل على تدميره نظيره قبل أن يقوم هو بذلك.

تبعا لذلك نجد أن بين المفاهيم الجديدة التي فرضت نفسها في نطاق الصراع بين الدول مفهوم الحرب السيبرانية (Cyber Warfare)، إذْ أصبح الفضاء الإلكتروني ساحة جديدة للصراع والحرب على غرار المجال المادي، مع اختلاف طبيعة الحرب السيبرانية وخصائصها عن الحروب التقليدية.

ومن الأفضل فهم مصطلح "الحرب الإلكترونية" على أنه يشير إلى فعل عدواني، يرتكب من خلال شبكة رقمية، يهدف إلى التسبب في أضرار في العالم الحقيقي، سواء عبر أهداف مدنية أو عسكرية، من أجل إجبار دولة ذات سيادة على التصرف أو الامتناع عن التمثيل.

وكنتيجة طبيعية، يجب أن تكون الجهة الفاعلة هنا دولة أخرى، نظرًا لأن تصرفاتٍ مماثلة من قِبل فرد يُطلق عليها على الأرجح "الإرهاب السيبراني" بالطريقة نفسها التي يطلق على الممثل من غير الدول الذي يهاجم الأصول المادية لدولة ما إرهابي، بغض النظر عن السلاح المستخدم[5].

---

[1] Carl Von Clausewitz, ***De la guerre,*** Trad. Nicolas Waquet (paris: rivages poche, 2006), p.19.

[2] جون ستون، ***الإستراتيجية العسكرية سياسة وأسلوب الحرب***، ط1، (الإمارات العربية المتحدة: مركز الإمارات للدراسات والبحوث الإستراتيجية، 2014)، ص 7.

[3] سعد حقي توفيق، ***مبادئ العلاقات الدولية*** (عمّان: دار وائل للنشر، 2000)، ص 211.

[4] منير شفيق، ***الإستراتيجية والتكتيك في فن علم الحرب***، ط1، (بيروت: الدار العربية للعلوم ناشرون، 2008)، ص 15.

[5] Daniel Dobrygowski, "What would a cyberwar look like?", World Economic Forum, 25 Avril 2018, in: https://cutt.us/qLMXI (05/12/2021)

ومن بين التعريفات المقدمة في شأن الحرب الإلكترونية ما يلي:

- تعريف "ريتشارد كلارك" و"روبرت كناكي": "أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى، بهدف تحقيق أضرار بالغة أو تعطيلها"[1].
- هي "أي نزاع يحدث في الفضاء الإلكتروني ويكون له طابع دولي"[2].
- هي "مهاجمة المعلومات أو الدفاع عنها وعن شبكات الكمبيوتر في الفضاء السيبراني، مقابل إنكار ومنع الخصم من فعل الشيء نفسه". ومن خلال هذا التعريف يمكن الكشف عن عنصرين هما[3]:
  * الهجوم: ويشمل سرقة المعلومات، مهاجمة الشبكات والبنية التحتية.
  * الدفاع: ويشمل حماية المعلومات من السرقة، حماية العمليات والشبكات، وحماية البنية التحتية.

وتُصنف الحرب الإلكترونية في المستوى الخامس من حيث الخطورة وحجم التهديد، بعد كل من القرصنة الإلكترونية (المستوى الأول)، الجريمة الإلكترونية (المستوى الثاني)، التجسس الإلكتروني (المستوى الثالث)، والإرهاب الإلكتروني (المستوى الرابع)[4]. بالتالي فإن الإرهاب الإلكتروني يمكن اعتباره وسيلة من وسائلها مادام يقع في المرتبة السابقة لها من حيث الخطورة والتهديد، وهما يتداخلان أيضا من حيث الوسائل والأدوات التي يتم توظيفها وخاصة الحرب النفسية واستهداف البنى التحتية، إلى جانب الهدف السياسي.

ويُعد الإرهاب الإلكتروني نمطاً جديداً من الحروب التي لا تعتمد على استخدام الأسلحة والمتفجرات، وينطوي على استخدام أو استغلال المجرمين لعدم حماية أو قابلية الأنظمة المدنية والعسكرية للمخاطر على النحو الذي يؤدي إلى التأثير على الأمن الوطني والعالمي، لذلك سيشهد المستقبل أسوأ أنواع الإرهاب[5]. وهذا الخطر المتنامي للإرهاب عبر الإنترنت ينبئ بأنه سيكون الخطر القادم، وأن الوسائل والأساليب التي

---

[1] فيصل محمد عبد الغفار، ***الحرب الإلكترونية***، ط1، (الأردن: الجنادرية للنشر والتوسيع، 2016)، ص10.

[2] عادل عبد الصادق، "الفضاء الإلكتروني وأسلحة الانتشار الشامل: بين الردع وسباق التسلح"، 2015/05/15، (2021/10/24) https://bit.ly/3fiTkuT

[3] SANS Institute, Global Information Assurance Certification Paper (GIAC), ***Information Warfare : Cyber warfare is the Future Warfare*** (2004), p-p : 3-4.

[4] فيصل محمد عبد الغفار، ***مرجع سابق***، ص: 10، 11.

[5] أحمد فلاح العموش، ***مستقبل الإرهاب في هذا القرن***، ط1، (الرياض: جامعة نايف العربية للعلوم الأمنية، 2006)، ص 89– 90.

يجير تطويرها للوقاية تقابلها مماثلة في أساليب التغلب على تلك الدفاعات التي قد تتهاوي أمام ضربات المحترفين الذين يوظفون هذه التقنية للحروب أو للإرهاب الالكترونيين، فكلاهما يشترك في استخدامات التقنية، مع اختلاف الفواعل[1].

ب– الجريمة السيبرانية:

مفهوم الجريمة الإلكترونية (Cybercrime) من المفاهيم التي لا تحظى بالإجماع والاتفاق، بالرغم من خطورتها، فقد عرفها البعض بأنها نشاط غير مشروع يمس "المعالجة الآلية للبيانات، أو نقل هذه البيانات"، كما عرفها آخرون بأنها نشاط "موجه إلى نسخ أو تغيير أو حذف، أو الوصول إلى المعلومات المخزنة داخل الحاسوب، أو التي تُنقل عن طريقه"[2].

وكان تقرير الأمم المتحدة لعام 2015 حول "النهج الشاملة المتوازنة لمنع ظهور أشكال جديدة ومستجدة للجريمة العابرة للحدود الوطنية والتصدي لها على نحو ملائم" قد ذكر بأن مفهوم الجريمة السيبرانية "يشمل عموما الجرائم التي تكون فيها النظم أو البيانات الحاسوبية موضوع الجريمة، وأيضا الجرائم التي تستخدم فيها النظم أو البيانات الحاسوبية وسيلة لارتكاب الجريمة"[3].

وخلال المؤتمر العاشر للأمم المتحدة المتعلق بالوقاية من الجريمة، تم تناول تعريفين أحدهما يتعلق بالجريمة الإلكترونية في معناها الضيق (جرائم الكمبيوتر)، وهي كل سلوك غير قانوني موجه عبر عمليات إلكترونية تستهدف أمن أنظمة الجهاز والبيانات المعالجة بواسطتها، والآخر يخص الجريمة السيبرانية بمعناها الواسع (الجرائم المتعلقة بالحاسوب)، وتعني كل سلوك غير قانوني يرتكب عن طريق أو يتعلق بنظام الكمبيوتر أو الشبكة، بما في ذلك الحيازة غير القانونية وتقديم معلومات أو توزيعها عبر

---

[1] عبدالحفيظ عبدالله المالكي، ***نحو مجتمع آمن فكرياً: دراسة تأصيلية واستراتيجية وطنية مقترحة لتحقيق الأمن الفكري***، ط1، (الرياض: مطابع الحميضي، 2010)، ص 254.

[2] ربيع محمد يحي، "إسرائيل وخطوات الهيمنة على ساحة الفضاء السيبراني في الشرق الأوسط: دراسة حول استعدادات ومحاور عمل الدولة العبرية في عصر الإنترنت (2002 – 2013)"، ***مجلة رؤى إستراتيجية*** (يونيو 2013)، ص75.

[3] مؤتمر الأمم المتحدة الثالث عشر، مرجع سابق، ص05.

نظام الجهاز أو الشبكة. أما التعريف الأكثر شمولا فهو اعتبار الجريمة السيبرانية نشاطا تكون فيه أجهزة الكمبيوتر أو الشبكات أداة، هدفا أو مكانا لارتكاب الجريمة[1].

ويمكن تصنيف الجرائم الإلكترونية كالآتي[2]:

- جرائم ضد سرية وسلامة البيانات وأنظمة الحاسوب.
- جرائم تتعلق بالحاسوب.
- جرائم تتعلق بالمحتوى.
- جرائم تمس حقوق المؤلف.

والملاحظ في الجرائم الإلكترونية على اختلاف أنواعها أن معظمها جرائم تقليدية تطورت بفعل تطور التقنيات التكنولوجية فصارت جرائم تقع في الفضاء الافتراضي، في حين أنه ظهرت جرائم حديثة ترتبط كليا بالفضاء السيبراني، ومن بينها الهجمات التي تستهدف موزع الخدمة[3]. بالتالي فإنه في سياق الحديث عن الجرائم والجرائم المستحدثة، تجب الإشارة إلى وجود خانتين كبيرتين للتصنيف: الخانة الأولى تشمل هجمات جديدة باستخدام التكنولوجيا، أما الثانية فتشمل هجمات أو جرائم قديمة باتت تستخدم التكنولوجيا نظرا لسهولة المهمة من خلالها[4].

ويتمثل الفرق بين الجريمة السيبرانية والإرهاب السيبراني أساسا في طبيعة الهدف والدافع، فالهدف في حالة الإرهاب الإلكتروني إما سياسي أو أيديولوجي، أما الوسيلة فتظل نفسها مادام كلاهما يعتمد على وسائل التكنولوجيا والمعلوماتية[5]. وهدف مرتكبي الجريمة الإلكترونية يكون في الغالب ماديا متصلا بالمال والثروة، ولذلك تحدث القرصنة وسرقة بطاقات الائتمان وابتزاز الضحايا[6]. هذا لا يمنع من اعتبار

[1] ITU, ***Understanding Cybercrime : Phenomena, Challenges and Legal Response*** (September, 2012), p.11.
[2] ***Ibid***, p.12.
[3] Stéphan Leman-Langlois, ***Op.cit***, p : 68, 73.
[4] Home Office, Secretary of State for the Home Department, ***Cybercrime Strategy*** (UK, 2010), p.09.
[5] Jugoslav Achkoski, Metodjia Dojchinovski, "Cyberterrorism and Cybercrime: Threats for Cybersecurity", p-p: 4-5, in: https://bit.ly/3xi4ec3 (16/03/2022)
[6] Maura Conway, ***Op.cit,*** p-p: 13-14.

وتصـــنيف جريمة الإرهاب الإلكتروني كنوع من أنواع الجرائم الســـيبرانية، منا أن هناك حدود فاصـــة بين المفهومين نوجزها كالتالي:

- يجب أن تحتوي هجمات الفضـــاء الإلكتروني على عنصـــر "إرهابي" حتى يتم تصـــنيفها على أنها إرهاب إلكتروني.
- يجب أن تغرس الهجمات الإرهاب كما هو مفهوم بشـــكل عام (أي تؤدي إلى موت و / أو دمار واسع النطاق)
- يجب أن يكون لها دافع سياسي.

فيما يتعلق بالتمييز بين اســـتخدام الإرهابيين لتكنولوجيا المعلومات والإرهاب الذي ينطوي على اســـتخدام تكنولوجيا الكمبيوتر كســـلاح / هدف، يمكن القول إن"اســـتخدام" الإرهابيين لأجهزة الكمبيوتر كميســـر لأنشطتهم، سواء للدعاية أو الاتصال أو لأغراض أخرى[1].

وفي دراســة نُشــرت عام 2006 للباحثة "ســوزان برينر" (Susan Brenner)، تؤكد أن الجريمة الإلكترونية عمل شــخصــي، وبالتالي فإن أهدافها شــخصــية في العادة، بينما الإرهاب الإلكتروني مدفوع سـياسـيا، ومع ذلك بينهما قواسـم مشـتركة. وكأمثلة على الدافع والهدف الشـخصـي في صـلتهما بارتكاب الجريمة الإلكترونية تذكر أنه في عام 1997 أقدم شـــخص أســـترالي على اختراق نظام إدارة النفايات، متسببا في تلويث حظائر وأنهار. وفي عام 2000 قام شخص في ماساشوستش باستهداف الاتصالات في برج مراقبة إدارة الطيران الفيدرالي لمدة ستّ ساعات[2].

ويُصنف مرتكبو الجرائم السيبرانية كما يلي[3]:

* من يرتكبونها بدافع التسلية (pranksters).
* المخترقون (hackers).

---

[1] Maura Conway, ***Op.cit.***

[2] Susan W.Brenner, « Cybercrime, Cyberterrorism and Cyberwarfare », ***Revue Internationale de Droit Pénal***, vol.77, n.3-4 (2006), in : http://www.cairn.info/revue-internationale-de-droit-penal-2006-3-page-453.htm (07/08/2020).

[3] شيخة حسين الزهراني، "الطبيعة القانونية للهجوم السيبراني وخصائصه"، ***مجلة جامعة الشارقة للعلوم القانونية***، المجلد 17، العدد 1 (جوان 2020)، ص: 784–785.

* المخترق المؤذي (malicious hacker).
* من يرتكبها بهدف حل مشاكل شخصية (personal solving problems).
* المجرم المحترف (career criminal).
* المتطرفون (extremists).

وفي دراســـة قدمها مكتب الأمم المتحدة المعني بالجريمة والمخدرات في 2013، تحت عنوان: "دراسة شاملة عن الجريمة"، يؤكد أن الجريمة السيبرانية وتطورها في المجتمع المعاصر مرتبط بالموصولية العالمية التي يقصد بها معدل الربط بالإنترنت، بالإضافة إلى أن هذا النوع من الجرائم بات عابرا للحدود[1]. وانطلاقا من ذلك تتضـح بعض القواسـم المشـتركة بين الإرهاب الإلكتروني والجريمة الإلكترونية، فكلاهما يقع في فضـــاء (افتراضـــي/إلكتروني) لا يوفر أي أثر مادي في الغالب (كالبصـــمات) أو يكون بإمكان الجاني إخفاؤه، بالتالي يصـعب إثبات الجريمة بما فيها جريمة الإرهاب الإلكتروني. هذا إلى جانب التطور المســتمر للجرائم المســتحدثة، مقابل عدم مواكبة التشــريعات الوطنية وتكيُّف المنظومة القانونية مع هذا التطور[2].

بالنسبة للفرق الجوهري بين المجرمين والجماعات الإرهابية، يبقى عنصر الأيديولوجيا محوريا عند الإرهابيين، ولهذا يكثر الحديث عن الخلايا النائمة لهذه الجماعات، في إشـــارة إلى الفكر المتطرف والظروف الملائمة والبيئة الحاضنة للعمل الإرهابي.

وتميل الفروق بين الجريمة والإرهاب والحرب إلى التعتيم عند محاولة وصــف هجوم على شــبكة الكمبيوتر بطرق موازية للعالم المادي، فعلى سـبيل المثال، يمكن اعتبار الهجوم الإلكتروني المنسـوب إلى جماعة إرهابية إرهابًا إلكترونيًا إذا وصـــل الضـــرر إلى مســـتوى معين، فيما قد يُطلق على هذا الهجوم الإلكتروني نفســـه، إذا نُســـب إلى دولة قومية اســـم حرب إلكترونية، ومع ذلك، فإن الإرهابيين ليســـوا

[1] مكتب الأمم المتحدة المعني بالمخدرات والجريمة، ***دراسة شاملة عن الجريمة*** (نيويورك، فبراير 2013)، ص06.

[2] حورية بن سـيدهم، رقية عواشـرية، "الأمن الفضـائي السـيبراني: التحديات والحلول"، ***المجلة الجزائرية للأمن الإنسـاني***، المجلد 5، العدد 2 (2020)، ص: 134-135.

متجانســـين، وقد يتخذ الفرد المتطرف إجراءات خارجة عن ســـيطرة الحكومات أو الجماعات الإرهابية التقليدية[1].

كما أنه على الرغم من أن الجماعات الإرهابية حاليًا غير قادرة على تنفيذ هجمات تتعلق بالحرب السيبرانية، فإنها تنوي تطوير قدراتها في هذا الاتجاه، خاصة وأن الهجوم السيبراني المعقّد ضد البنية التّحتية الحيوية يتطلب مستوى عالٍ من المعرفة التقنية، في حين يقدم مجرمو الإنترنت خدمات مختلفة يمكن استخدامها في الهجمات الإلكترونية الإرهابية الخطيرة. في هذا الشأن، حدد تقييم تهديد الجريمة المنظمة عبر الإنترنت الذي نشره اليوروبول في عام 2016 المجال السيبراني والإرهاب كأحد النقاط الرئيسية التي يركز عليها منفذو الجرائم الالكترونية وأكد على ترابطها[2]، في حين تختلف جرائم الإنترنت والإرهاب عبر الإنترنت فقط على أساس دافع ونية الجاني، ويميز فورنيل، ووارن S. Furnell, M. Warren بين المتسللين الكلاسيكيين والإرهابيين الإلكترونيين، حيث يعمل الإرهابيون وفق أجندة سياسية أو أيديولوجية محددة لدعم أفعالهم وهو ما يميزهم عن غيرهم[3].

ج– الجهاد السيبراني.

التعرف على مصطلح الجهاد يتطلب الانطلاق من ثلاثة مستويات هي[4]:

- مستوى أنطولوجي (وجودي)، يرتبط بوجود الإنسان وكفاحه المستمر في الحياة (فلسفة الفعل).
- مستوى يتصل بالقيم والأخلاق التي ارتبطت بالثقافة الإسلامية.
- مستوى يربط مصطلح الجهاد بالحرب.

فقد تم تقديم ظاهرة النشاط عبر الإنترنت باسم الإسلام فيما يتعلق بالبيئات الإسلامية السيبرانية في الواقع الإسلامي كمجال قد تتصاعد فيه التوترات، حيث تصبح تكنولوجيا الإنترنت متاحة على نطاق

[1] Clay Wilson, Cyber Threats to Critical Information Infrastructure, in: Thomas M. Chen · Lee Jarvis Stuart Macdonald, ***Cyberterrorism: Understanding, Assessment, and Response,*** (UK: Springer, 2014), p 123.

[2] The Internet Organised Crime Threat Assessment (2016), (Hague: Europol, 2017), in : www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assess-ment-iocta-2016

[3] Jarkko, ***Op.cit.***

[4] Centre de Recherches Internationales, Centre d'Etudes Européenne et de Politique Comparée, Compte-rendu de la 45ème séance, ***Djihad : Une Définition Scientifique est-elle Possible ? Les Sciences Sociales en Question : Grandes Contreverses Epistémologiques et Méthodologiques***, p.03.

واسع ويمكن الوصول إليها، وقد أثبتت مجموعات "إسلامية" مختلفة ذلك (خاصة فيما يتعلق بالصراعات في الشيشان وفلسطين وكشمير وأفغانستان) في حملات عبر الإنترنت تسعى للترويج لقضيتها، وفي بعض الأحيان تعطل الأنشطة عبر الإنترنت لخصومها الأيديولوجيين والعسكريين، والظاهر أن مصطلح الجهاد الإلكتروني يتمتع ببعض المرونة؛ فيمكن أن يكون مرتبطا بالقرصنة والتطبيق التقني التخريبي؛ على نطاق أوسع، كما يمكن أيضًا تطبيقه كشكل من أشكال الدعاية (أو الدعوة الإلكترونية) من أجل تقديم وجهات نظر عالمية محددة لجمهور انتقائي، ولكن أيضًا لجمهور عالمي أوسع (مسلم وغيره)[1].

كما يمكن أن يمتد الجهاد الإلكتروني إلى المناقشات حول الطريقة التي يتم بها استغلال تقنية المعلومات من قبل مجموعات مثل القاعدة وتنظيم "داعش" الإرهابي من أجل التنظيم اللوجستي، من خلال استخدامهم البريد الإلكتروني، وسائل التواصل الاجتماعي، والملفات المشفرة، واعتبارها كوسيلة لتطوير إستراتيجية رقمية خاصة بهم،ويلجأ"الجهاديين" إلى الأساليب الإلكترونية للترويج لأهدافهم العنيفة،كما يمكن إخفاء معظم اتصالات الإنترنت بما في ذلك البريد الإلكتروني والرسائل ومجموعات الدردشة وتطبيقها في مجموعة متنوعة من السياقات التي تخدم أجندة معينة عبر الإنترنت.[2].

كما أن الفرد المنخرط فيها تصبح له هوية أخرى تفرضها الجماعة، فينتقل بذلك من موقع الضعيف إلى القوي[3]. ويتصل مفهوم الجهاد الإلكتروني بمفهوم التجنيد الإلكتروني، والذي يمكن تعريفه بأنه عملية استقطاب وحشد للأفراد لكي ينخرطوا فعليا في الجماعة أو التنظيم الإرهابي، سواء كان ذلك طوعا، أي بمحض الإرادة، أو قسرا[4]، مما يجعل دائرة الجماعة الإرهابية تتوسع ودائرة الفكر المتطرف تنمو فينتشر بصورة مضاعفة.

---

1 Gary R.Bunt, ***Islam in the Digital Age E-Jihad, Online Fatwas and Cyber Islamic Environments*** (London: Pluto Press,2003), pp 25-26.

2 Raphael Cohen-Almagor , "In Internet's Way: Radical, Terrorist Islamists on the Free Highway", September 2013, in :https://cutt.us/uVMol

3 Denis Jeffrey, « La Radicalisation des Jeunes Djihadistes », Denis Jeffrey, et autres, ***Jeunes et Djihadisme : Les Conversions Interdites*** (Canada : Presses de l'Université Laval, 2016), p-p : 22, 25.

4 مكتب الأمم المتحدة المعني بالمخدرات والجريمة، ***دليل بشأن الأطفال الذين تجندهم وتستغلهم الجماعات الإرهابية والجماعات المتطرفة العنيفة.. دور نظام العدالة*** (فيينا، 2018)، ص07.

فيما قد يفهم وفق وجهات نظر أخرى أن الجهاد الإلكتروني هو وضع منشورات والإشراف على مواقع وصفحات خاصة بالتعريف بالفكر المتطرف واستمالة الأفراد فكريا وعاطفيا، وإنما يكون الهدف الموالي لاستقطاب هؤلاء جعلهم يؤمنون بالأعمال الانتحارية أو ما يسميه أنصار هذا التيار بالعمل الاستشهادي بوصفه مقدسا باسم الدين وفي سبيل الله، وإن كانت تكلفته هي التضحية بالنفس البشرية، ولأسامة بن لادن في هذا السياق عبارة شهيرة متوجها بكلامه إلى الولايات المتحدة الأمريكية: "نحن نحب الموت أكثر مما تحبون الحياة"[1].

ومع ذلك فإن التعرف على مفهوم الجهاد الإلكتروني يبدأ كمؤشر نسبي لأهمية الجهاد، من خلال تحليل السياقات الاجتماعية والاقتصادية والتاريخية والسياسية واللاهوتية للجهاد والتي تم وضعها كمضامين له، ليس فقط من زوايا ضيقة استخداما وتداولا كالتي تتبناها الجماعات والتنظيمات الإرهابية بهدف إضفاء الطابع الديني وعدالة القضية على النشاط غير المشروع أو المبرر.

وقد تصنف الهجمات الإلكترونية الخطيرة في خانة الحرب إلكترونية. ففي الفضاء الإلكتروني تنتشر التكنولوجيا على نطاق واسع، كما يجري استخدام الأسلحة نفسها من قبَل القراصنة والمجرمين الإلكترونيين، والجواسيس والإرهابيين، وهؤلاء يستغلون ثغرات الفضاء الرقمي لتحقيق الهدف المرجو وإنتاج الأثر نفسه تقريبا (أي الفزع العام).

وبالرجوع إلى مقارنة المفاهيم الأربعة: الإرهاب السيبراني، الجريمة الإلكترونية، الحرب السيبرانية والجهاد الإلكتروني، يمكن القول كملاحظة أولية أنه لا توجد تعريفات واحدة ودقيقة بشأن كل هذه المفاهيم، وما لا يمكن إنكاره هو وجود تداخل بين الإرهاب الإلكتروني (إذ يقع في المستوى الرابع وما قبل الأخير من حيث درجة التهديد السيبراني والخطورة)، والجريمة الإلكترونية (إذ أن الإرهاب الإلكتروني هو نمط من أنماطها كما يشتركان في الوسيلة والخصائص)، والحرب السيبرانية (إذ تقع في المستوى الأخير من حيث التهديد والخطورة)، أما الجهاد الإلكتروني هناك أوجه تشابه واضحة بينه وبين والإرهاب السيبراني، وكلاهما يفتقر إلى بنية متماسكة؛ كلاهما عالمي وفوضوي تمامًا، خاصة عندما يتعلق الأمر بالمضمون الروحي والديني فقد يرتبطان بنشاط الجماعات المتطرفة والتنظيمات الإرهابية التي تسعى من

[1] Denis Jeffrey, ***Op.cit,*** p 29-30.

خلال الانترنت إلى نشـر التطرف وجذب المناصـرين، فهو–وفق رؤيتهما– شـكل متطور ومسـتحدَث من الجهاد التقليدي.

في الأخير يمكن القول إن الإرهاب السـيبراني هو أحد مكونات الحرب الالكترونية، لكن الحروب الالكترونية ليست إرهابًا إلكترونيًا، ولهذا السبب من الضروري تحديد هذه الموضوعات ككيانات منفصلة، وبالتالي فإن التمييز بين المفاهيم والمصطلحات أمر مهم. فالهجمات في الفضاء السيبراني يمكن أن تأخذ طابع الإرهاب كما يمكنها أن تتصـف بأنها حرب حسـب الطرف الذي يقوم بها (الدولة في حال حربٍ سـيبرانية)، فضـلا عن الاختلاف في الخصـائص والإعداد وطبيعة الضـحايا وشـكل وطبيعة المواجهة ونطاقها.

كما يمكن أن تُعتبر **هجمات الفضاء السيبراني حربا بالوكالة**، حيث تستطيع الدول أن تبدأ بسريّة، وتمول، وتتحكم بالهجمات السـيبرانية من خلال قيام اللاعبين من غير الدّول بتنفيذ هذه الهجمات بدلا عنها، مخففة من خلال ذلك من التأثيرات السـياسـية لهذه الهجمات، ومحققة لأهدافها دون عبء الالتزام بأحكام قانون الصـراع المسـلح، فتوظيف اللاعبين من غير الدول في عمليات في الفضـاء السـيبراني أمر يجذب الدول لاسيما في سعيها نحو تحقيق أهداف إستراتيجية محدودة[1].

لقد أصبح الفضاء السيبراني مجالا للصراع والتنافس يستخدمه الفاعلون فيه من الدول أو من غير الدول للتعبئة والحشـد والتنظيم والدعاية، وتسـتخدمه أيضـا المعارضـة ضـد النظم السـياسـية أو نشـطاء الإرهاب أو الجريمة، كما أن هناك صـعوبة الفصـل ما بين النشـاط الذي يتعلق بالاسـتخبارات وجمع المعلومات وحرب الفضـاء السـيبراني والاسـتخدام السـياسـي له في الصـراع، خاصـة مع ما يمثله من بيئة مثالية لعمل الجماعات المختلفة والقدرة على تشـكيل شـبكة عالمية بدون سـيطرة مباشـرة، بالإضـافة إلى التكلفة المنخفضـة وسـهولة الاتصـال وضـعف الرقابة عليه، ومثلت تلك الخصـائص عنصـر جذب هام لاستخدام الهجمات السيبرانية وتوظيفها لتحقيق الأهداف السياسية من قبل الدول أو الجماعات الإرهابية[2].

[1] أنديرا عراجي، ***مرجع سابق***، ص125.

[2] ربيع محمد يحي، ***مرجع سابق***، ص 26.

يُفهم من خلال التحليلات السـابقة أن الإرهاب الإلكتروني يتم التأسـيس له أيديولوجيًا وتوجيهه بطريقة سياسية، لهذا يبقى العامل الفكري في صلته بالهدف السياسي معيارا محوريا.

المبحث الثاني: الإرهاب الإلكتروني القدرات وملامح الفاعلين.

يتناول المبحث الثاني من هذا الفصل إستراتيجية الإرهاب الإلكتروني، من حيث التعرف على أهم محددات القدرات السـيبرانية للجماعات الإرهابية، والأهداف المرجوة من خلال توظيف أسـلوب الإرهاب الإلكتروني، مما يكشـف خطورته وأهميته بالنسـبة للجماعات والتنظيمات الإرهابية التي باتت تعتمد بكثرة على الفضاء الإلكتروني وشبكة الانترنت.

المطلب الأول: القدرات السيبرانية للمجموعات الإرهابية.

بالنظر إلى أن عدد مستخدمي الإنترنت قد تضاعف أكثر من ثلاثة أضعاف في العقد الماضي، من مليار في عام 2005 إلى ما يقدر بنحو 3.2 مليار في نهاية عام 2015، فمن المنطقي القول أن الإرهابيين سيصبحون في نهاية المطاف أكثر ميلًا إلى التفكير السيبراني[1].

فسواء في صورته الهجينة أو المحضة، يتوقف الإرهاب الإلكتروني على قدرة الجهة التي تتبناه وتمارسـه على التعامل مع الوسـائل التكنولوجية المتطورة والتحكم في المعلوماتية وشـبكة الإنترنت، بالإضافة إلى قدرة هذه الجهة على التأثير في الضحية أو الجهة المستهدَفة بشكل ما. بالتالي فإن الحديث عن وجود قدرات سـيبرانية للجماعات الإرهابية هو أمر واقع جعلها تنافس الدولة في التحكم في الفضـاء السيبراني واتخاذه مجالا للصراع والتهديد. ويشير مفهوم القدرة السيبرانية إلى وجود قدرة تتصل بخصائص الفضاء السيبراني وتتخذها عنصرا معززا للكفاءة والتأثير في إطار الصراع داخل هذا الفضاء.

يعرف "جوزيف ناي" (Joseph Nye) القدرة السـيبرانية بأنها "القدرة على الحصـول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني، أي أنها القدرة على استخدام الفضـاء السـيبراني لإيجاد مزايا للدولة، والتأثير على الأحداث المتعلقة بالبيئات التشـغيلية الأخرى وذلك عبر أدوات سـيبرانية"، كما أنها "مجموعة الموارد المتعلقة بالتحكم والسـيطرة على أجهزة الحاسـبات

[1] Levi Maxey, "Terror Finance in the Age of Bitcoin", ***Indian Strategic Studies,*** 16 JUNE 2017, in: https://www.strategicstudyindia.com/2017/06/terror-finance-in-age-of-bitcoin.html?m=1

والمعلومات والشـبكات الإلكترونية والبنية التحتية المعلوماتية والمهارات البشـرية المؤدية للتعامل مع هذه الوسائل"[1].

وفي تناوله للأطراف التي تمتلك الأدوات أو القدرات السيبرانية، يذكر "ناي" ما يلي[2]:

- الدول باختلاف وزنها، وفي المقابل تحتاج الهجمات السـيبرانية في الغالب إلى قدرات أكبر لا تملكها جميع الدول، خاصة وأن طبيعة التهديد في الفضاء الإلكتروني مختلفة عن التهديدات التقليدية مما يتطلب سياسات ورؤية تختلف من أجل التصدي الجيد لها.
- فواعل غير دولاتية، وإن كانت قدراتها أقل من الدول غير أنها قادرة على اختراق المواقع والقيام بهجمات وتهديدات، ويدخل في هذا الإطار الجماعات والتنظيمات الإرهابية العابرة للحدود الوطنية.
- وسائل التواصل الاجتماعي، وما لها من تأثير واسع في المجتمعات وصناعة الرأي العام.
- الجماعات الإرهابية، ومما لا شـك فيه أنها تمتلك قدرات سـيبرانية، فلولا ذلك لما اسـتطاعت تنظيمات مثل القاعدة وتنظيم "داعش" الإرهابي أن تتغلغل في المجتمعات وتستقطب عشرات الآلاف من المناصرين لأيديولوجيتها والمنضمين إلى صفوفها من كل المناطق عبر العالم.
- الفرد العادي، وهنا يجب التذكير بتسـريبات "ويكيليكس" مثلا وما أدت إليه من توترات إقليمية ودولية، وهو ما يعكس قوة المعلومة وقوة تأثير التكنولوجيا وحتى الفرد العادي.

ويمكن التعرف على محددات القدرات السيبيرية للجماعات الإرهابية من خلال العناصر التالية:

أ- <u>التحكم في التكنولوجيا والمعلوماتية:</u>

على عكس ما كان يعتقده البعض فإن الجماعات الإرهابية لا تضم عناصر غير متعلمة أو ذات مسـتوى تعليمي وثقافي محدود، بل تهتم بأن يكون من أعضـائها أفرادٌ متحكمون في اسـتخدام أجهزة الكمبيوتر والهواتف الذكية ومتخصصون في تكنولوجيا المعلومات. لقد تخطّت الجماعات الإرهابية وسائل الإعلام التقليدية (إذاعة، تلفزيون، منشـورات وكتب ورقية، أشـرطة سـمعية..)، لتجد ضـالتها في التطور

[1] إسماعيل زروقة، ***مرجع سابق***، ص1018.

[2] راجع: إميل أمين، "الأمن السـيبراني العالمي: حروب خلفية ومسـاحات إرهابية.. خمسُ قوى تهدد اسـتقرار المجتمعات عبر شـبكات الإنترنت وبتقنيات عالية الدقة"، 2020/02/12، https://bit.ly/3hVxIGy

التكنولوجي من خلال فضاء بعيد عن الرقابة المستمرة والقيود، وهو ما جعلها تتمكن من منافسة الدول في السيطرة على هذا الفضاء ولو نسبيا، من خلال امتلاكها أدوات ممارسة الإرهاب الإلكتروني والتأثير في المستخدمين فكريا ونفسيا.

وتجب الإشـــارة إلى أنه قد جرى تجنيد خبراء في الكمبيوتر خلال ما عرف بمرحلة الجهاد في أفغانستان خلال الثمانينيات، وكان الهدف من وراء ذلك الاستعانة بهم في إنشاء مواقع للتواصل ونشر إعلانات التنظيم[1].

ب– نوعية الخطاب الموجه الذي تتبناه الجماعات الإرهابية:

ينطلق خطاب الجماعات الإرهابية من استغلال حالات الكبت والحرمان والصراعات السياسية والطائفية في المجتمع، محاولا إظهار الجماعة أو التنظيم الإرهابي بمظهر المنقذ والمدافع عن قضـــايا المجتمع العادلة خاصة ما يتصل منها بالبعد الديني. وبالرغم مما يحمله خطاب الجماعات الإرهابية من لهجة شديدة وترهيب للعدو إلا أنه يتصف بالمرونة أحيانا في سبيل إقناع الأفراد من كل شرائح المجتمع بضرورة دعم الإيديولوجية المتطرفة والانخراط في النشاط الإرهابي، بالاعتماد على مصطلحات وعبارات تتكرر كثيرا.

في 2007 عبّر وزير الدفاع الأمريكي الأســـبق "روبرت غيتس" (Robert Gates) قائلا إن تنظيما كالقاعدة هو أفضـــل من الولايات المتحدة الأمريكية من حيث قدرته على إيصـــال رســـالته عبر الانترنت[2]، وهي شهادة تعكس عمق التأثير وخطورة التهديد الذي يمارسه الخطاب المتطرف.

أ– القدرة على جذب الجماهير:

إن اعتماد الجماعات الإرهابية على الفضـــاء غير المادي كان انطلاقا من ميزاته وخصـــائص الانترنت، وقد وردت عبارة تكشف عن القدرات السيبيرية لهذه الجماعات في استغلال الفضاء الرقمي، وهي للباحث "دوروثي دنينغ" عندما وصف تحكمها فيما يريد أفرادها إظهاره للرأي العام عبر الشبكة من

[1] بروس هوفمان، "شكل من أشكال الحرب النفسية"، ***مجلة اي جورنال*** (ماي 2007)، ص11.

[2] Christina M. Knopf, Eric J. Ziegelmayer, « La Guerre de Quatrième Génération et la Stratégie des Médias Sociaux des Forces Armées Américaines », ***Afrique et Francophonie***, 2012, p.9.

خلال عبارة "إدارة الفكرة المدرَكة"، ولا يكون ذلك بمعزل عن الحرب النفسية، فالحرب النفسية كما يصفها "بروس هوفمان" هي "الدعامة الأساسية للأهداف والقدرات الإرهابية"، وخاصة مع التطور المستمر لتقنيات التواصل[1].

لا يمكن الاستهانة بالدور الذي تلعبه الشبكة العنكبوتية في استمالة الأشخاص وجعلهم يتجهون نحو التطرف، ولتقنية الصوت والصورة أثر كبير في جعلهم يتعاطفون مع الجماعات الإرهابية وفكرها، مع الاستفادة من خاصية سهولة استخدام الانترنت والتواصل من خلاله في مقابل صعوبة التحكم فيه[2]. كما أن سهولة استخدام منصات مثل فيسبوك وتويتر ويوتيوب قد جعلتها منصات مفضلة لنشر الأخبار ومشاركة الأفكار والفيديوهات، مما أتاح مجالا واسعا للتعاطف مع الجماعات الإرهابية وتوسيع دائرة فكرها ودائرة المنخرطين في صفوفها. وتعمل الجماعات الإرهابية على تشكيل هوية افتراضية جماعية من خلال استعطاف الأفراد، مما يسهّل تجنيدَهم وانصهارهم في هوية الجماعة، ليصبحوا بذلك ذوي انتماء جديد.

وبحسب الباحث في الشؤون الأمنية "جيف باردين" (Jeff Bardin) فإن تنظيم "داعش" الإرهابي قد امتلك أكثر من 50 ألف موقع إلكتروني، وهو ما ساهم بشكل فعال وملحوظ في تجنيد الأفراد في صفوفه بمعدل 3400 فرد شهريا، من كل ربوع العالم[3].

ب– القدرة على التوسع والانتشار في الفضاء السيبراني كما في الفضاء المادي:

من خصائص الظاهرة الإرهابية في الفترة المعاصرة، وتحديدا بعد نهاية الحرب الباردة وانتشار العولمة، أنها تحولت إلى تهديد عابر للحدود الوطنية، فتواجُد جماعة إرهابية في مكان ما من العالم لا يعني عدم إمكانية وجود مناصرين لها أو أفراد منتمين إليها فكريا وتنظيميا في مناطق أخرى، وهو ما زاد خطورة التهديد الإرهابي، وبالتالي قابلية الجماعات الإرهابية للانتشار والتمدد افتراضيا وواقعيا. وكان انتشار استخدام الانترنت بالتأكيد محفزا ومؤثرا في واقع وإستراتيجية هذه الجماعات، مما منحها قدرة على الوصول إلى أكبر عدد من رواد منصات التواصل الاجتماعي والتعريف بأيديولوجيتها، وكذا استقطاب

[1] بروس هوفمان، ***مرجع سابق***، ص: 10–11.

[2] Sénat de Canada, ***Liberté, Sécurité et la Menace Complexe du Terrorisme : Des Défits pour l'Avenir***, Rapport Intérimaire du Comité Sénatorial Spécial sur l'Anti-terrorisme (Mars 2011), p-p : 16-17.

[3] عنترة بن مرزوق، ***مرجع سابق***، ص: 511–512.

منضمين جدد من كل الجنسيات والفئات العمرية بفضل التطور التكنولوجي وباستغلالها للفضاء الرقمي، مما أتاح التحول إلى شبكة عالمية تستقطب أفرادا من كل مكان، في صورة تعكس وجود مجتمع يوازي المجتمعات في العالم المادي.

لا يمكن إنكار دور الإنترنت في تطور تكتيكات الجماعات الإرهابية وتعزيز قدراتها السيبرانية، فبفضله استطاعت الاستثمار في عدد من الخصائص مثل سرعة التواصل وإيصال المعلومة والتفاعل، إضافة إلى لامركزية الشبكة التي تتيح المجال للتحكم الفردي، ولولا تلك الخصائص لبقيت الجماعات الإرهابية ذات تأثير محدود. بالتالي، يُنظر إلى الإنترنت كخطر، وذلك في صلته بنشر التطرف والشائعات والفيروسات الخطيرة. وتشير الدراسة التي أعدّها مجموعة من الباحثين ومن بينهم الباحثة "سيغافان الافا" (Séraphin Alava)، في عام 2018 تحت إشراف منظمة اليونسكو (UNESCO)، إلى أنه خلال الفترة: 2005–2011 ركزت معظم الدراسات التي تناولت موضوع الإنترنت على دوره الإيجابي في الحياة[1]، مع أن تلك الفرضيات أثبتت نسبيتها عندما أصبح التداخل بين إيجابيات وسلبيات الفضاء الإلكتروني عموما من ضمن التهديدات لأمن الدول واستقرار المجتمعات عبر العالم.

وبعد عرض محددات القدرات السيبرانية للجماعات الإرهابية، تتضح درجة التهديد المحتمل عن طريق الفضاء الإلكتروني، وهو التهديد الذي يتخذ أنماطا ومستويات متنوعة من خلال أسلوب الإرهاب الإلكتروني.

المطلب الثاني: أهداف الإرهاب الإلكتروني الداخلية والخارجية.

مع زيادة استخدام الانترنت منذ بداية تسعينيات القرن الفارط ونمو النقاش حول مجتمع المعلومات، كان مصطلح الإرهاب السيبراني في طور التبلور، وبالتزامن مع ذلك وضعت الأكاديمية الأمريكية الوطنية للعلوم تقريرا حول أمن الكمبيوتر ورد فيه الآتي: "نحن في خطر.. إرهابي اليوم يستطيع

[1] Séraphin Alava, et autres, ***Les Jeunes et l'Extrémisme Violent dans les Médias Sociaux, Inventaire des Recherches***. Organisation des Nations Unies pour l'Education, la Science et la Culture (France, 2018), p-p : 15-16.

إحداث ضـرر أكبر بواسـطة لوحة مفاتيح مقارنةً بقنبلة"[1]. انطلاقا من هذه العبارة يمكن اسـتنتاج الأهداف الخطيرة التي يتوخى الإرهابيون السيبرانيون تحقيقها.

تتنوع الأهداف التي تجعل الأفراد يعتمدون على أسـلوب الإرهاب الإلكتروني، وهي تتراوح بين أهداف داخلية وأخرى خارجية، ويجب أن نشـير في البداية إلى أن تصـنيف الأهداف على هذا النحو يحتمل معنيَين: فالداخلية إما أن تعني كونها أهدافا تتعلق بداخل الفضـاء الإلكتروني أو بداخل نطاق الدولة كاسـتهداف منشـاتها التحتية من طرف جماعة محلية، والخارجية إما أن تشـير إلى كونها أهدافا تتجاوز نطاق الفضـاء السـيبيري لتضـرّ بالمجال المادي أو تعني الأهداف التي تتجاوز النطاق الجغرافي للدولة الواحدة فتكون أهداف الإرهاب الإلكتروني في هذه الحال أوسع وأكثر ضررا.

وعموما، يمكن ذكر أهم أهداف الإرهاب الإلكتروني وأشهرها كالآتي:

أ- الأهداف الداخلية للإرهاب الإلكتروني:

يمكن تلخيصها كما يلي:

- من الأهداف الداخلية الأولى للإرهاب السـيبراني اسـتهدافُ أجهزة الحاسـوب وخدمة الانترنت للحكومات والأشخاص، للوصول إلى بيانات مهمة وصور أو قطع التزويد بخدمة الانترنت أو التشـويش عليها. ويكون ذلك في أطار تخطيط محكم من لدُن جماعة معارضـة داخليا أو تنظيم إرهابي محلي بغرض تشويه صورة الحكومة وفضح تجاوزاتها.
- في حالة الإرهاب السـيبراني المحض (Pure Cyberterrorism) تكون البنية التحتية السيبرانية هي الهدف المركزي، فيتم العمل على استهداف أنظمة المعلومات وحجب المواقع[2].
- يعد "التواصـل الآمن" بين أعضـاء الجماعة الإرهابية من خلال خدمات الانترنت هدفا محوريا، فمن خلاله يتم تبادل المعلومات والتنسـيق بين أفراد المجموعة للقيام بجريمة إرهابية محلية

[1] Gabriel Weiman, ***Cyber Terrorism: How Real is the Threat?*** (Special Report, n119), U.S Institute of Peace (December 2004), p.2.

[2] عبد الستار عبد الرحمن، "الإرهاب السيبراني.. خطر يهدد العالم"، 23/02/2020 ، في: https://www.imctc.org/ar/eLibrary/Articles/Pages/Articles2322020.aspx (12 جويلية 2021)

أو داخلية. ويعد تأمين الأشخاص في الفضاء الافتراضي حاجة أساسية، لذلك يتم التواصل فيما بينهم بحسابات مجهولة الهوية أي باستخدام أسماء مستعارة وذكر بيانات مغلوطة في الحسابات الشخصية لغرض التمويه.

- الدعاية للنشاط الإرهابي على الصعيد الوطني بدايةً، واستقطاب الأطفال والمراهقين ومختلف شرائح المجتمع للانخراط في صفوف التنظيمات الإرهابية، باستغلال حالات الإحباط النفسية والحرمان والصراعات السياسية والثغرات الأمنية، مثلما حدث في سوريا والعراق.

ب– الأهداف الخارجية للإرهاب الإلكتروني:

يأتي في مقدمتها الاختراق الإلكتروني، بمعنى اختراق مواقع حساسة للحكومات تحتوي على بيانات هامة، وقد يقع من خلال تسريبها الإضرارُ بهذه الحكومات أو بشخصيات نافذة في الدولة. والاختراق ذو صلة بالتجسس، فكلاهما يهدف إلى تجميع بيانات وأدلة حساسة وخطيرة تكون في صالح العدو بغرض تهديد الخصم أو تشويه سمعته الدولية، أو جعله يقدم تنازلات في قضايا معينة.

وفي سياق الحديث عن التجسس الإلكتروني، يمكن الإشارة إلى حادثة التجسس المغربي على الجزائر وفرنسا من خلال عدد من الشخصيات السياسية والعسكرية، وذلك باستخدام برنامج "بيجاسوس" (Pegasus) الإسرائيلي، وهو ما يعد هدفا من الأهداف الخارجية للهجمات السيبيرية على اختلاف أنماطها ومستوياتها.

وتعد مهاجمة أنظمة البيانات والبنى التحتية الحرجة لأغراض تخريبية هدفا محوريا، وكمثال فقد تعرضت شركة "أرامكو" النفطية إلى هجوم سيبراني في أوت 2012، إذ تمكن المهاجمون من محو بيانات مخزنة وتعطيل أجهزة الحاسوب[1]، وقبل ذلك استهدف عدد من الفيروسات والبرامج الخبيثة خدمات الانترنت، مثل فيروس "مايكل انجلو" (MS.Dos) لعام 1991، وكان بهدف تدمير البيانات، فيروس "أحبك" لعام 2000 وهو على شكل رسالة غرامية تخريبية، فيروس "ماي دووم" لعام 2004 والذي

[1] ربيع محمد حيى، ***مرجع سابق***، ص75.

استهدف البريد الإلكتروني للمستخدمين، فيروس "ستوكسنت" الذي كان هدفه التجسس والتدمير[1] واستهداف المنشآت الحيوية النووية لإيران.

وقد يحتاج المهاجمون إلى فترة طويلة من استهداف البنى التحتية لغرض خلق تأثير خطير ونشر الرعب على نطاق واسع. وتشمل البنى التحتية أنظمة متنوعة ومختلفة ذات أهمية إستراتيجية وحيوية بالنسبة للدولة والمجتمع، كنظام الطاقة الكهربائية، وشبكة المياه، والخدمات الضرورية بما فيها التزويد بالإنترنت[2]. فبما أن البنى التحتية، بما فيها الحساسة والعسكرية، باتت تعتمد على الفضاء السيبراني فقد أصبحت في المقابل هدفا لنشاط الإرهاب الإلكتروني من خلال مهاجمة شبكة المعلومات المتعلقة بالبنى التحتية الحرجة، نظرا لما يخلفه ذلك من خسائر وأضرار للدولة والمجتمع والاقتصاد الوطني. والملاحَظ هنا أن الشبكة العنكبوتية بالنسبة للجماعات الإرهابية وللإرهابي السيبراني وسيلة وهدف في آن واحد.

وتكون محطات توليد الطاقة الكهربائية في الغالب هدفا أساسيا للإرهاب السيبراني، وكشف تقرير أمريكي أن "70 بالمائة من هذه المحطات عانت هجمات جادة" (severe attacks) بالولايات المتحدة خلال النصف الأول من عام 2002[3]. وتتمثل أهمية مهاجمة أنظمة الطاقة الكهربائية في كونها مرتبطة بخدمات وقطاعات أساسية قد تكون حيوية، كالإنترنت والبرامج النووية، وهنا يجب التذكير بالهجمات المتكررة التي تقوم بها دولة الكيان الصهيوني (إسرائيل) مستهدفةً محطات توليد الكهرباء الإيرانية وبالتالي البرنامج النووي الإيراني، مثال ذلك ما حدث في شهر ابريل 2021.

ويجد الإرهابيون السيبرانيون في تهديد الخصم عن طريق الردع السيبراني هدفا وضرورة لإظهار القوة السيبرانية للمهاجم، ويقع ذلك في إطار ما سماه بحث للمعهد الألماني للشؤون الأمنية والدولية ب

[1] سعد عطوة الزنط، "الإرهاب الإلكتروني وإعادة صياغة إستراتيجيات الأمن القومي"، ورقة مقدمة إلى مؤتمر: الجرائم المستحدثة– كيفية إثباتها ومواجهتها، 15–16 ديسمبر 2010، ص3.

[2] James A.Lewis, ***Assessing the Risk of Cyberterrorism, Cyber War and Other Cyber Threats***, Center for Strategic and International Studies (CSIS), (Washington, December 2002), p-p : 2-3.

[3] ***Ibid***, p.5.

"الردع بالمنع" في مقابل "الردع بالانتقام"، بمعنى تقويض قدرات العدو وتهديده أو صـــدّه عن مزيد من الهجمات السيبرانية[1].

من الأهداف الخارجية الأخرى للإرهاب السيبراني نجد الدعاية للنشاط الإرهابي، وظهر ذلك بشكل كبير مع تنظيم القاعدة ثم "داعش" الإرهابي، فداعش وحده امتلك ســـبعَ وكالات إعلامية وأكثر من 30 مكتبا في بلدان مختلفة[2]، الأمر الذي جعله يتمكن من تجنيد فئات واسعة من الأفراد عبر العالم بالاستعانة بتكنولوجيا الاتصالات وشبكات التواصل الاجتماعي.

كما توجد أهداف أخرى للإرهاب السيبراني يمكن اختصارها فيما يلي:

- التدريب على استخدام الأسلحة وصناعة المتفجرات والقيام بهجمات سيبرانية متعددة، وهو ما لوحظ مع تنظيمات إرهابية.
- إيجاد مصـــدر تمويل عبر الانترنت للنشـــاطات الإرهابية التقليدية (أي في المجال المادي)، حيث يتم اللعب على وتر العاطفة لاستقطاب أموال المتبرعين والمناصرين للمجموعة الإرهابية.
- شلّ قدرة الخصـم على الاسـتمرار في سـياسـة معينة أو برنامج يضـر بمكانة ومصـالح وقدرات فواعل إقليمية ودولية، تماما كما يجري مع الملف النووي الإيراني المستهدَف باستمرار.

من خلال عرض أهم الأهداف التي يســعى الإرهابيون الســيبرانيون إلى تحقيقها على الصــعيدين الداخلي والخارجي، يتبين حجم الخطر والتهديد الذي يشـــكله هذا النوع من الإرهاب الجديد وعلى نطاق أوسع يتجاوز حدود الدولة الوطنية.

[1] عبد الغفار الديواني، "القرن الســيبراني: الدفاع الإلكتروني بين المنع والانتقام"، عرض لتقرير صـــادر عن المعهد الألماني للشـــؤون الأمنية والدولية، مركز المســـتقبل للأبحاث والدراســـات المتقدمة، 04,06,2015، في: https://bit.ly/3iKVchF (12 جويلية 2021).

[2] عبد الستار عبد الرحمن.

من خلال ما سبق، يرى مركز التميز للدفاع السيبراني التعاوني التابع لحلف الناتو(CCDCOE) ، أن هناك ثلاث مقاربات أساسية للتعاطي مع ظاهرة الإرهاب الإلكتروني، وهي[1]:

- **المقاربة الأولى:** وهي تقوم على (سيبرانية **الهدف**)، أي استهداف البنى التقنية للدولة من أجهزة، وخوادم، وشبكات، وقواعد بيانات بغرض الإضرار بمصالحها، أو إثارة الفزع بين المواطنين، وهي المقاربة التي اتبعتها إستراتيجية النمسا للأمن الإلكتروني (2013)، والسياسة الوطنية للأمن السيبراني بجنوب إفريقيا (2011)، ومنظمة الأمن والتعاون في أوروبا(OSCE)
- **المقاربة الثانية:** وهي تركز على (سيبرانية **الأداة**)، بمعنى استخدام الأدوات التقنية الضارة في تحقيق الأهداف الإرهابية، مثل الفيروسات الدودية، والهجمات البرمجية لحجب الخدمات (DDOS) وشفرات حصان طروادة، وهي المقاربة التي تعتمدها عدة دول.
- **المقاربة الثالثة:** وهي تقوم على (سيبرانية **المجال**)، أي تحقيق الأهداف الإرهابية في مجال إلكتروني، أي أنه لا يشترط أن تكون تلك الأهداف مرتبطة بهجمات على قواعد بيانات أو شبكات، أو تكون الأدوات المستخدمة ذات صفة تخصصية معقدة، ولكن يكفي أن يتم تحقيق الأهداف الإرهابية عبر المجال الإلكتروني، وهو ما يستلزم بالتبعية استخدام أدوات سيبرانية، وهي المقاربة التي اتبعتها دول، مثل روسيا، بالإضافة إلى دول أخرى مثل إيطاليا، وبولندا، وجمهورية الجبل الأسود.

المطلب الثالث: الاستخدامات السيبرانية للجماعات الإرهابية: فحص للتقنيات والتكتيكات.

يذهب بيلوبيرا Bjelopera إلى حد القول بأن: التفاعل عبر الإنترنت يطمس الخطوط الفاصلة بين القراء والمؤلفات، والحاجز الذي واجهته الأجيال السابقة من الإرهابيين والمتعاطفين مع الكتيبات والصحف والنشرات الإخبارية، وهذا الأمر سهل للمتعاطفين الذين يرون أنفسهم بسهولة أكبر كجزء من الحركات الجهادية الأوسع وليس فقط متفرجين على الإنترنت، لهذا وُصف الإنترنت بأنه "غرفة الصدى".

يسلط "بيلوبيرا" الضوء على دور الإنترنت باعتباره تطبيعا للسلوكيات والمواقف التي قد تحمل خطر اعتبارها غير مقبولة أو غير مناسبة في العالم المادي، بما يوفر ميزة إخفاء الهوية المفترضة،

[1] إبراهيم بولمكاحل، "تجليات الإرهاب السيبراني .. داعش ونهج "الخلافة" الرقمية"، في: ***العلاقات الدولية في عصر التكنولوجيات الرقمية: تحولات عميقة، مسارات جديدة*** (الأردن: مركز الكتاب الأكاديمي، 2021)، ص 145.

ودرجة من الحماية والأمان من الكشـف لأن المعلومات غير خاضـعة للرقابة وغير هرمية[1]. الأمر الذي ساعد على انتشار و تطير تكتيكات العمل الإرهابي بشكل كبير، حيث تمكنت تنظيمات مثل القاعدة من جعل نشاطها أكثر مرونة من خلال التحول إلى "شبكة عالمية" واعتماد أسلوب الخلايا[2]، وهو في الوقت نفسـه أسـلوب جديد لتفادي الملاحقات الأمنية والسـعي إلى فرض الوجود في المجالين المادي وغير المادي.

وبحسب الباحثة "سيغافان الافا" فإن الإرهابيين يصنفون إلى أربع مجموعات هي[3]:

- فئة النشطاء المتصلين بالشبكة أو من يشرفون على الأخبار والمواقع والمراسلات.
- قراصنة الإنترنت، وهدفهم الاستيلاء على المعلومات، ونشر الشائعات والأخبار المضللة.
- مجموعة مكلفة بتجنيد الأفراد للعمل الإرهابي.
- مجموعة تستهدف الدخول بصورة عنيفة لتدمير الجهاز أو تعطيل البيانات.

وانطلاقا من ذلك يمكن تحديد أهم التقنيات التي يعتمد عليها الإرهاب الإلكتروني وطرق اسـتخدام الانترنت لأغراض إرهابية كما يلي:

أ- مواقع التواصل الاجتماعي:

ويُقصد هنا تطبيقات مثل فايسبوك، وتويتر، ويوتيوب، وغيرها من تطبيقات الوسائط الاجتماعية الأخرى، والتي تعرف بأنها شبكة من التفاعلات الاجتماعية والعلاقات الشخصية التي تمكن المستخدمين من التواصل مع بعضهم البعض عن طريق نشر المعلومات والتفاعل بتبادل التعليقات والرسائل والصور وما إلى ذلك، فمن خلال هذه الوسائط والمنصات يبث الإرهابيون أخبارهم بالصوت والصورة، كما يتوفر لديهم مصدر معلومات خفيّ (آني) يساعد في تنفيذ العمليات الميدانية الإرهابية، هذا ويتم استغلالها بشكل

[1] Ines Von Behr, and Others, ***Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism*** **(**Brussels: Rand Europe, 2013), p 18.
[2] Angela Gendron, Martin Rudner, ***Op.cit***, p.27.
[3] Séraphin Alava, ***Op.Cit.***

كبير في نشر الأفكار المتطرفة واستقطاب الجماهير والدعاية، في ظل سهولة الوصول لمختلف الفئات دون أية قيود مكانية[1].

ب–خدمة البريد الإلكتروني:

البريد الإلكتروني يأتي في مقدمة الخدمات التي استعانت بها المجموعات الإرهابية، بحيث يتم توظيفه كوسيلة للتواصل وتبادل المعلومات بين أفراد الجماعة، أو يكون هدفا للاختراق[2].

ج– خدمات المواقع الإلكترونية:

في 1998 كان أقل من نصف عدد المنظمات التي صنفت إرهابية يمتلك مواقع إلكترونية، وفي 1999 ارتفع عدد المواقع ذات الصلة بالجماعات أو التنظيمات الإرهابية، وبعد 2005 ارتفع عددها بصورة متواصلة وغير مسبوقة[3]. ينشئ الإرهابيون مواقع خاصة لتشجيع الانخراط في الفعل الإرهابي، سواء من خلال التدريب على صناعة المتفجرات واستخدام الفيروسات واختراق المواقع، أو لغرض تبادل الأفكار واستقطاب الأفراد فكريا وعاطفيا. ويتم اختراق المواقع عبر استغلال ثغرة من ثغرات الفضاء الإلكتروني، أو عبر إرسال رسائل كثيرة جدا إلى بريد المستخدم بحيث تؤثر في سعة بريده التخزينية فيسهل تدميره[4].

كما يجري تنفيذ هجمات الحرمان من الخدمة (Denial of Service-DoS)، وتتمثل في إغراق المواقع الإلكترونية ببيانات تجعلها بطيئة فيصعب وصول المستخدم إليها[5]، وكمثال على ذلك أنه في 1988 قامت مجموعة إرهابية بإغراق سفارات سريلانكا ب 800 بريد في اليوم، وكانت الرسالة الموجهة من خلال ذلك هي: "نحن نمور الانترنت السود، ونفعل هذا لتعطيل اتصالاتكم"[6].

---

[1] إبراهيم بولمكاحل، ***مرجع سابق***، ص149.

[2] سعد عطوة الزنط، ***مرجع سابق***، ص: 03–04.

[3] غابريال وايمن، "مسرح وسائل الإعلام"، ***مجلة أي جورنال*** (ماي 2007)، ص30.

[4] سعد عطوة الزنط، ***مرجع سابق***، ص: 04–05.

[5] خالد وليد محمود، "الهجمات عبر الانترنت: ساحة الصراع الإلكتروني الجديدة"، ***دورية سياسات عربية***، العدد 5 (نوفمبر 2013)، ص118.

[6] Mitko Bogdanoski, Drage Petreski, ***Op.cit,*** p.61.

د- الانترنت المظلم (Dark Web) أو العميق (Deep Web):

ويشـار بهذه التسـمية إلى المواقع الإلكترونية غير المفهرسـة، مما يجعل المعلومات داخلها على درجة من السرية، وهو ما يتيح للجماعات الإرهابية تبادل المعلومات وجمع التبرعات دون تتبع[1].

هـ- نُظم المعلومات الجغرافية:

بإمكان الجماعات الإرهابية قرصـنة نُظم المعلومات الجغرافية (خرائط المواقع والمدن مثل خرائط غوغل) بهدف الاستيلاء على معدات ضرورية التحكم فيها (سفن، طائرات..)[2].

و- تقنيات التخفي عبر الأدوات التكنولوجية:

من بين التقنيات التي تعتمد عليها الجماعات الإرهابية إخفاء البيانات الحسـاسـة وكل ما يتعلق بسـرية التنظيم أو الجماعة، وهو ما يندرج في إطار أمن المعلومات بوجه عام. فعلى سـبيل المثال، تم العثور في 2012 بحوزة شاب نمساوي قدم إلى ألمانيا من باكستان على بطاقة ذاكرة (Memory Card) مشـفرة تحتوي على بيانات وملفات خطيرة وبعضـها إباحي، تتعلق بتنظيم القاعدة[3]. وقد تبين منذ أحداث 11 سـبتمبر 2001 أن الجماعات والتنظيمات الإرهابية اعتمدت مرارا على تقنية ما يعرف بـ Steganography، وهي تقنية قائمة على الرسـائل المخفية (التشـفير الرقمي) والسـرية في تبادل المعلومات والتواصـل بين طرفين، بهدف حماية محتوى الرسـالة والمعلومة، واسـتخدام هذه التقنية لإخفاء البيانات تم تناوله لأول مرة في صـحيفة "أمريكا اليوم" (USA today) بتاريخ: 5 فبراير 2001، وفي أكتوبر 2001 ذكرت "نيويورك تايمز" (New York times) أن تنظيم القاعدة اعتمد على تقنية "ستيغانوجرافي" لتشفير بيانات مرسلة كانت ذات دور أساسي في تفجيرات 11 سبتمبر 2001[4].

أما بخصوص **التكتيكات** التي يعتمد عليها الإرهاب الإلكتروني فيمكن تحديدها فيما يلي:

---

[1] إبراهيم بولمكاحل، ***مرجع سابق***، ص149.

[2] إبراهيم بولمكاحل، ***مرجع سابق***، ص151.

[3] Mitko Bogdanoski, Drage Petreski, ***Op.cit.*** p.63.

[4] ***Ibid***, p.64.

أ- التجسس الإلكتروني:

هو التجسس عبر الوسائط الإلكترونية، من أجل الحصول على معلومات مهمة يتم الاستفادة منها لغايات إستراتيجية. يعد مستوى هاما من مستويات النشاط الإرهابي، فعلى أساسه تتحدد الإستراتيجية والتكتيكات التي تعتمدها الجماعات الإرهابية. ويعد الفضاء الإلكتروني ذا أهمية إستراتيجية بالنسبة لهذه الجماعات، لكونه يحتوي على معلومات هامة تخص الدول والجوانب العسكرية، ولا يمكنها الاستغناء عنه باعتباره وسيلة تواصل سهلة وفعالة، وإن كان ذلك يتم بصورة مشفرة تفاديا لأي متابعة من قبل أجهزة الدولة.

ب-أسلوب الدعاية للنشاط الإرهابي:

تعد الدعاية بالنسبة للجماعات الإرهابية هدفا بحد ذاتها ووسيلة أيضا للتغلغل في المجتمعات، والدفع باتجاه التطرف والتحريض على الإرهاب فمن خلالها يستهدف الإرهابيون نشر أفكارهم والترويج لها بوصفها طريقة ناجعة لنشر الخطاب المتطرف، ويتأتّى ذلك عبر مواقع الشبكة العنكبوتية ومنصات التواصل الاجتماعي من أجل التعريف بفكر الجماعة أو التنظيم، وهو يعد سبيلا لوصول الأفكار إلى شريحة واسعة من المجتمعات وبالتالي استقطاب قدر أكبر من الأفراد للانضمام إلى صفوف الجماعات المتطرفة والتنظيمات الإرهابية، بسهولة وبأقل تكلفة.

ويمكن تصنيف أنواع الجماهير المستهدفة من قبَل المجموعات الإرهابية كما يلي[1]:

- ✓ فئة المؤيدين أو المتعاطفين.
- ✓ الرأي العام العالمي.
- ✓ الأعداء، وهم الأنظمة الحاكمة والحكومات الغربية.

[1] علي إبراهيم مشجعل المعموري، أسعد طارش عبد الرضا، "الأمن السيبراني ودوره في انتشار ظاهرة الإرهاب الإلكتروني في العراق بعد العام 2003"، ***مجلة دراسات دولية***، العدد 80، ص165-166.

كما يمكن أن تنقسم الدعاية الإرهابية إلى ثلاث فئات أساسية: الدعاية الموجهة للجمهور الأوسع، والدعاية لـ "جمهور" الإرهابيين، والدعاية الموجهة لأعضاء الجماعة الإرهابية نفسها[1].

ويعد الفضاء الرقمي وسيطا هاما لإثبات وفرض وجود الإرهابيين، ولذلك توصف الدعاية بكونها حربا نفسية تمارسها الجماعات الإرهابية على خصومها والفئات المستهدفة للجذب والتغلغل في أوساطها[2]، بالتالي يعد الاعتماد على منصات التواصل الاجتماعي غنيمة بالنسبة للإرهابيين، وتتمثل مجالات أو أبعاد استخدام هذه المنصات بالنسبة لهم فيما يلي[3]:

- إنشاء منصات تفاعلية وسهلة الاستخدام، من أجل استقطاب الشباب.
- توفير فضاء للتواصل السري وتبادل الأفكار.
- نشر محتوى متطرف ومحفز على الإرهاب.
- التعرف على المناصرين وتوجيههم نحو فضاءات افتراضية تدعم قضية الجماعة الإرهابية.
- الدعاية للنشاط الإرهابي.
- اقتراح فرص للمشاركة في النشاط الإرهابي عبر الإنترنت وخارجه.
- نشر الأخبار الكاذبة وجعلها تظهر بمظهر الحقيقة.
- استمرارية العملية الراديكالية حتى بعد تجنيد الأفراد من خلال الإنترنت.
- الاتصال بين الأفراد لتعزيز شبكة العلاقات.
- وضع قطيعة مع الواقع الاجتماعي، والربط أكثر بالجماعة الإرهابية منعا لأيّ انشقاق.

ج– التجنيد الإلكتروني:

إن استخدام الانترنت كوسيلة للتجنيد هو محطة أساسية بالنسبة للإرهابيين، وليس التجنيد مرتبطا بالتطور التكنولوجي فحسب، وإنما ظل حاضرا بمختلف قنواته حتى قبل انتشار الانترنت.

والفضاء السيبراني هام جدا في عملية التجنيد أو ما بات يُعرف بالتجنيد الإلكتروني، في ظل استغلال حالة التعاطف السائدة لدى فئات من الأفراد واستغلال الظروف المحفزة على التوجه نحو التطرف

[1] ***Report of the Working Group on Countering the Use of the Internet for Terrorist Purposes***, Counter-Terrorism Implementation Task Force (CTITF) February 2009, p. 15.
[2] Rabiah Ahmad, Zahri Yunos, ***Op.cit,*** p.7.
[3] Séraphin Alava, rapport, ***Op.cit***, p-p : 21-22.

مثل الظلم والإقصاء الاجتماعي، ولا يُستثنى من ذلك تجنيد القُصّر بهذه الطريقة. وفي سياق تناول التجنيد الإلكتروني يمكن الحديث عمّا يلي:

1- تجنيد القصّر:

يتم استخدام الرسوم المتحركة والألعاب من خلال الوسائط الإلكترونية في استقطاب الأطفال، بمزجها بمادة تمجيد الفعل الإرهابي كالصوتيات والأناشيد الحماسية (مثال صليل الصوارم بأجزائه الأربعة). كما يتم استغلال فئة القصّر في تعزيز رسالة الجماعة الإرهابية أو كما كان الحال مع تنظيم "داعش" الإرهابي، حيث يجري توظيف تلك الصورة لبث الرعب من جهة وإظهار القوة واستقطاب الأفراد من جهة أخرى. ويعد استغلال تجنيد الأطفال في الدعاية للنشاط الإرهابي تكتيكا ذا أهمية للجماعات الإرهابية، خاصة وأنها تسعى إلى الظهور دوما بمظهر الضحية. بالتالي، لا يختلف اثنان على أن الإنترنت وسيط فعال لتجنيد الأفراد حتى لو كانوا أطفالا، وذلك عن طريق استمالتهم والتعرف على توجهات البعض من أجل التحكم في نوعية المادة المقدمة[1].

2- تجنيد النساء:

كما عُرفت ظاهرة تجنيد النساء في صفوف التنظيمات الإرهابية، حيث بلغ عددهن في سوريا والعراق ما يقارب 30 بالمائة من مجموع المقاتلين الأجانب. ويتمثل دور المرأة في هذه التنظيمات في الترويج للفكر المتطرف وتنشئة جيل جديد من المتشبعين بالأفكار المتطرفة، فضلا عن استقطاب نساء أخريات.

بالنسبة للفتيات المراهقات فقد تجري استمالتهن عبر شبكات التواصل الاجتماعي بأساليب ذكية، مثل استغلال الجانب العاطفي وجعل الفتاة تتعلق بفرد من أعضاء الجماعة الإرهابية. كما أن وظيفتهن تتمثل في إشراكهن لاحقا في تجنيد أخريات، أو تنفيذ هجمات انتحارية خاصة بالنسبة للأطفال، أو استغلالهن جنسيا والاتجار بهن، ويذكر تقرير مكتب الأمم المتحدة المعني بالمخدرات والجريمة لعام 2018، والمتعلق بتجنيد الأطفال في الجماعات الإرهابية، أنه خلال الفترة: يناير 1014- فبراير 2016 شكّلت الفتيات المجندات ثلاثة أرباع (4/3) الهجمات الانتحارية التي قام بها الأطفال لصالح جماعة

[1] مكتب الأمم المتحدة المعني بالمخدرات والجريمة، دليل بشأن الأطفال، ***مرجع سابق***، ص: 10، 13.

"بوكو حرام" الإرهابية[1]. ومن التناقض أن تجد الجماعات نفسها تروج لفكرة الدفاع عن حقوق المرأة والظهور بمظهر من يعطي للمرأة قيمتها في المجتمع.

د– **التمويل، التدريب والتخطيط:**

تختلف طرق وأساليب تمويل الجماعات المتطرفة تبعا لنوع النشاط الإرهابي الذي تمارسه، ومع ذلك يوجد نوعان من أساليب التمويل[2]:

- **الأول:** هو التمويل المباشر بالأموال التي تقدمها دول وأفراد.
- **الثاني:** يتمثل في التمويل والتدريب الذي يتخذ صورة دعم عيني كتأمين الأسلحة بمختلف أنواعها، والتدريب للجماعات المتطرفة الإرهابية للقيام بعمليات تخريبية.

وكلا النوعين يعتمد على استخدام التقنيات التي تتيحها شبكة الإنترنت، مثلا من خلال جمع التبرعات لمؤسسة خيرية ظاهريا، في حين أنها غطاء للعمل الإرهابي.

وقد ظهرت قدرة الجماعات الإرهابية على استحداث مصادر تمويلها عبر الفضاء السيبيري من خلال طلب التمويل المباشر، أو بيع سلع عبر الإنترنت كالكتب والأشرطة السمعية، أو تبييض الأموال[3]. في سياق متصل، وعلى سبيل المثال: استُعمل موقع "المنبار" لجمع التبرعات وبث مشاهد الرعب عبر عمليات الذبح والقتل، وكان من بين تلك العمليات حادثة مقتل الطيار الأردني "معاذ الكساسبه" على يد أعضاء تنظيم "داعش" الإرهابي[4]، كما جمعت المنظمات الإرهابية الأموال عن طريق ألعاب الكمبيوتر والتصيد الاحتيالي[5].

---

[1] ***المرجع نفسه***، ص: 14–15.

[2] نايف بن محمد المرواني، "تمويل الإرهاب الكترونيا التحديات وطرق المواجهة "التجربة السعودية"، ***المجلة العربية للدراسات الأمنية والتدريب***، المجلد 29، العدد 58، (ديسمبر 2013)، ص 14.

[3] علي إبراهيم مشجعل المعموري، أسعد طارش عبد الرضا، ***مرجع سابق***، ص: 164–165.

[4] نهى بلعيد، "تطور استخدامات مواقع التواصل الاجتماعي في العالم العربي"، ***مجلة الإذاعات العربية*** (ابريل 2016)، ص19.

[5] Report of the Working Group on Countering the Use of the Internet for Terrorist Purposes, ***Op.cit***, p.4.

- **تمويل الإرهاب إلكترونيا: العملات الافتراضية.**

أصبحت **البيتكوين Bitcoin** عملة متاحة للأنشطة الإجرامية، لما لها من قدرات تشفيرية عالية، كما أنها لا تتطلب البيانات الشخصية للمستخدم، فأي مالك لعملة البيتكوين هو مجرد 'رقم' يمثل المحفظة المالية التي سيتم تحويل النقود منها وإليها، وبالتالي فهي توفر خاصية التخفي وعدم التعقب، وقد لجأت بعض التنظيمات المتطرفة لطلب تبرعات لها عبر الانترنت بعملة الببيتكوين معلنة عن محفظة إلكترونية للتبرع من خلالها، للحصول على التمويل اللازم للعمليات الإرهابية، بل إنها تقوم أيضا من خلال البيتكوين بشراء الأسلحة والمتفجرات والممنوعات من خلال المواقع الالكترونية في الإنترنت الأسود والذي يتم من خلاله تسويق هذه المنتجات بصورة غير شرعية[1].

إنّ الأدلّة على أن الإرهابيين يستخدمون عملات افتراضية على مستوى مؤثر قليلةٌ جداً، لاسيما بالمقارنة مع المنظّمات الإجرامية، وبالتالي فإنّ أفضل الأمثلة على ذلك إعلانات إلكترونيّة لأنصار مايسمّى بالدولة الإسلاميّة في العراق والشام، يحثون من خلالها على التبرع لهم باستخدام البيتكوين، وقد لاحظ آرون برانتلي Aaron Brantly –عضو أكاديميّة ويستبوينت العسكريّة– وجود أدلّة كافية على أنّ الإرهابيين يبحثون في استخدام العملات الرقميّة مثل العملة الرقميّة الإلكترونيّة، لتمويل أنشطتهم حتى أنّهم يستخدمونها في حالات محدودة، وفي حين أنّ هذه الأدوات اكتسبت شعبيّة في السنوات الأخيرة، فإنّ توسع نطاقها إلى المنظّمات الإرهابيّة المختلفة كان بطيئا ومتأنيا ولم يواكب وتيرة الاستخدامات الإجرامية العابرة للحدود للتقنيّات نفسها. كل هذا يُبرز قدرة المجموعات الإرهابيّة والمتمرّدة على زيادة نفوذها السياسي و/أو الاقتصاديّ عن طريق نشر العملات الافتراضيّة كوسيلة للعمليّات الاقتصاديّة العاديّة، مقابل استغلال العملات الافتراضيّة المنتشرة بالفعل، مثل البتكوين، كوسيلة من الوسائل غير المشروعة لتحويل الأموال وجمعها وتبييضها[2].

---

[1] إيهاب خليفة، ***مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي*** (القاهرة: العربي للنشر والتوزيع، 2018)، ص 128.

[2] جوشوا بارون، انجيلا أوماهوني وآخرون، ***تداعيات العملة الافتراضية على الأمن القومي، البحث في إمكانية النشر من جهة فاعلة غير حكومية***، مؤسسة راند، 2015، ص 20– 22

يمكن للجماعات المتطرفة أيضًا اللجوء إلى الأسواق غير المشروعة على شبكة الإنترنت المظلم للشراء والبيع لتلبية احتياجاتها التشغيلية ، ذلك باستخدام العملات المشفرة (شراء جوازات سفر مزورة لتمكين المتطرفين من عبور الحدود بسهولة واستئجار سيارات ومنازل آمنة)، كما أن توافر الأسلحة وإمدادات صنع القنابل والطائرات الصغيرة بدون طيار، وحتى البيانات الحساسة المسروقة على الأهداف يمكن أن يسهل العمليات بسبب عدم الكشف عن الهوية التي توفرها العملات المشفرة –خاصةً المونيرو Monero–، والتي على عكس البيتكوين لا تشير حتى إلى حسابات الإرسال والاستلام أو المبلغ.

يفهم من هذا أن العملات المشفرة ليست ببعيدة عن الفعل الإرهابي؛ فهي تشكل أساساً لأصول رقمية للتبادل وتعتمد على تكنولوجيا دفاتر الحسابات الرقمية الموزعة من أجل تأمين المعاملات المالية؛ بما يسمح بتعميمها وجعل تعقُّبها أمراً صعباً، وهذا ما يزيد من جاذبية استخدامها من قبل الجماعات الإرهابية. والمستغلون الأساسيون للعملة المشفرة هم في الواقع الجماعات الإجرامية المنظمة وليس الإرهابيون الفرادى؛ لأن استخدامها معقد فعلياً. ومع ذلك، فإن جمعية الصدقة السنغافورية المرتبطة بتنظيم القاعدة تسعى للحصول على تمويل بالبيتكوين، في حين أن تنظيم "داعش" الارهابي استخدم في سوريا خلال عامي 2014 – 2015 العملة المشفرة في المعاملات الصغيرة[1].

فيما يحاجج البعض بالقول أن العملة الافتراضية لم تصبح بعد أساسًا لتمويل الإرهاب لان طرق الدفع التقليدية لا تزال فعالة، ويحدث تمويل الإرهاب في الوقت الحاضر من خلال آلية غير رسمية لتحويل الأموال تعتمد على النقد وتُعرف باسم شبكات الحوالة، كما أن السيولة النقدية سائلة وسهلة الصرف ومجهولة المصدر ولا تتطلب البنية التحتية التقنية المفقودة في العديد من الأماكن التي يعمل فيها الإرهابيون، ولاسيما شمال نيجيريا واليمن والقرن الأفريقي[2].

بشكل عامّ، ينتج الاستعمال المحتمل لتكنولوجيا مماثلة عن حالات يكون فيها نشر البيانات والحفاظ عليها في مواجهة تحديّات أو في حالة قمع، لكنّ الوصول إلى البيانات لا يستبعد وحدة زمنيّة قدرها واحد على ألف من الثانية، وتشمل الأمثلة إستراتيجيات وتقنيات وإجراءات مصمّمة لتمكين الانشقاقيّين السياسيّين من استعمالها ونشر المنشورات الإرهابيّة، كمجلّة "إنسباير" التابعة لتنظيم القاعدة

[1] وجدان فهد، "الذكاء الاصطناعي بين التكتيكات الإرهابية والاستراتيجيات الوطنية"، 1 مارس 2022، في:
https://trendsresearch.org/ar/insight/ai-between-terrorist-actics-and-national-strategies/(08|03|2022)
[2] Levi Maxey, Op.Cit.

في شبه الجزيرة العربيّة أو مجلّة "دابق" التابعة لتنظيم الدولة الإسلاميّة في العراق والشام، أمّا الحصيلة الأخرى فهي الإتاحة المتزايدة لبرمجيّات التشفير المصمّمة بحرَفية –أو بصورة عامة رمز التشفير–، وهذه البرمجيات مصمّمةٌ لدعم العملات الافتراضيّة، حيث يمكن لمطوّري البرامج الأقلّ إلماما أن يستخدموها لتوفير قدر أكبر من الأمن، وفي الممارسة قد يسمح ذلك للمجرمين الإلكترونيّين والإرهابيّين، الذين يتمتّعون بمستوى أدنى من الإلمام التكنولوجي بأن يصلوا إلى عمليّات تواصُل أكثر أمنا وإلى خدمات إلكترونية أخرى، مما يصعّب على الحكومات ملاحقتهم وهزيمتهم[1].

وقد يسمح الوصول المباشر إلى خدمات إلكترونيّة مرنة بتوفير بنية تحتيّة للاتّصالات، مرنة وعالميّة، وتتيح الاتصالات الخاصّة: اتصالات غير منقطعة ومغفلة ومشفّرة، وقد تخدم مثل هذه الاتصالات المماثلة حاجات الانشقاقيين السياسيّين في التواصل من دون تدخّل حكومتهم، وقد تكون التداعيات على وزارة الدفاع والمجتمع الاستخباراتي أنّه يجب تطوير الإستراتيجيّات والتقنيّات والإجراءات الجديدة التابعة لاستخبارات الإشارات من أجل التصدّي لهذا التهديد[2].

وإلى جانب التمويل، أصبح الفضاء الإلكتروني ساحة للصراع وساحة لتدريب أفراد الجماعات الإرهابية على حمل السلاح وصنع المتفجرات، والتخطيط وتنفيذ عمليات إرهابية. ويتم التخطيط باستخدام تكنولوجيا الاتصال المتطورة عبر التنسيق بين منفذي العملية كما حدث في تفجيرات 11 سبتمبر 2001.

وخلال مؤتمر أمن المعلومات بمدينة سان فرانسيسكو لعام 2011، تحدث نائب وزير الدفاع الأمريكي الأسبق "ويليام لين" قائلا: "من المحتمل أن تقوم مجموعة إرهابية بتطوير أدوات لشن هجوم إلكتروني سواء بمجهود ذاتي أو عبر شرائها من السوق السوداء"[3]، في إشارة إلى أن الفضاء السيبراني ساحة مفتوحة للصراع وامتلاك أسلحة غير تقليدية.

ويعد نموذج "الذئاب المنفردة" مثالا آخر لا يقل خطرا، بحيث لا يتصل الفرد المتطرف بجماعة أو تنظيم بالضرورة وإنما تكون له توجهات متطرفة ورغبة واستعداد لممارسة الفعل الإرهابي نتيجة التأثر

[1] إيهاب خليفة، ***مرجع سابق***، ص 60– 65.

[2] ***المرجع نفسه***، ص 66

[3] بيتر سينجر، ***مرجع سابق***، ص07.

بالمحتوى المنشور عبر الانترنت، ويكفي أن يصنع أسلحته بتكلفة بسيطة بعد مشاهدة فيديوهات تعليمية خاصة[1].

وبالرغم من مخاوف استخدام الإنترنت من قبل الإرهابيين ووفرة المواقع الارهابية، إلا أن معظم الإرهابيين لم يتقنوا التكنولوجيا اللازمة لشن هجمات واسعة النطاق، ومع ذلك تقدم بعض مواقع الويب تقنيات للتأجير على الإنترنت وتوفر معلومات للوصول إلى شبكات الروبوت لتنفيذ "هجمات رفض الخدمة الموزعة"، ونظرًا لأن الإرهاب السيبراني هو نقطة التقاء الإرهاب والفضاء الإلكتروني، فلا ينبغي اعتبار الهجمات الإلكترونية الإرهابية الوحيدة ذات القدرة التدميرية فحسب، بل وأيضًا الأعمال الإرهابية مثل الدعاية والتجنيد التي تتم على الإنترنت "إرهابًا إلكترونيًا". فمواقع المنظمات الإرهابية تعمل على إثارة الرأي العام، وتثقيف وتحفيز الأعضاء، والقيادة والتحكم في المنظمة، والدعاية للسكان المستهدفين، وتوفير المعلومات لتنفيذ هجوم إلكتروني، لذلك يجب التعامل مع الهجمات الإلكترونية الإرهابية واستخدام مواقع الإنترنت من قبل الإرهابيين معًا وتقييمها وفقًا لتعريف الإرهاب السيبراني[2].

من كل ما سبق، يمكن القول إن تكتيكات الإرهابيين تتطور مع الزمن. تمامًا كما رأينا تكيفًا للأساليب الإرهابية لبث الخوف وانعدام الثقة. كذلك، تتوفر آلات الدعاية الخاصة بهم لكسب تعاطف الجماهير عبر أنحاء العالم وخاصة في أوربا، ويقود هذا لنتيجة مفادها أن البيانات المطبوعة أو الكتيبات أو أشرطة الفيديو التقليدية قد ولى زمنها، وعوضتها المرونة وعدم الانكشافية في الإنترنت، فرسائل التجديد بكل صيغها، وتمويل الجماعات الإرهابية، كلها متاحة في المجال السيبراني.

[1] إيهاب خليفة، ***مرجع سابق***، ص124.

[2] Murat Dogrul, and Others, ***Op.cit,*** p32

المبحث الثالث: اتجاهات التنظير في الفضاء السيبراني: الحاجة إلى إعادة تموضع النظريات التقليدية.

يتناول هذا المبحث الإطار النظري للدراسة، بالتركيز على تطور مفهوم الأمن ومواضيعه بعد أن ارتبط لفترة طويلة من الزمن بالجانب العسكري ونطاق الحروب والمعارك بين الدول. فقد شهد مفهوم الأمن في حقل العلاقات الدولية تطورا مستمرا، بالتماشي مع اجتهادات الباحثين النظرية وتحولات النظام الدولي مع نهاية الحرب الباردة، موازاتا مع بروز عديد التهديدات اللاتماثلية العابرة للحدود، والتي يعد الإرهاب الالكتروني أحد أشكالها. وقد اهتمت بعض الاجتهادات النظرية في هذا السياق بالفضاء الإلكتروني وببُعد جديد للأمن (الأمن السيبراني) بالموازاة مع التحول في أبعاد القوة (القوة الإلكترونية)، وهو الأمر الذي جعل من الضروري للنظريات التقليدية أن تتكيف والواقع الأنطولوجي والابستيمولوجي الجديد، خاصة وأن ظهور الفواعل والتهديدات الجديدة جعل من المقاربة لها أمرا يستدعي تكيف هذه النظريات لإعادتها للتداول مجددا، فالتهديدات السيبرانية تستدعي إعادة تموقع النظريات الواقعية والليبيرالية بما يتماشى والواقع السياسي والأمني الجديد، لتأتي طروحات مدرستي "كوبنهاجن" و"باريس" في حقل الدراسات الأمنية في محاولة تقديم مقاربة نظرية وتوليفية تتناسب والتغيرات الحاصة في هذه البيئة الأمنية المعقدة والمتشابكة.

المطلب الأول: الإرهاب السيبراني ونظريات العلاقات الدولية.

ساد المفهوم التقليدي للأمن حتى منتصف ثمانينيات القرن المنصرم، وأتى "مرادفا لحماية وبقاء الوحدة السياسية المتمثلة في الدولة، إذ وظفه الباحثون لوصف الجهود التي تتخذها الدولة لتأمين وجودها في مواجهة التهديدات العسكرية للدول المنافسة"[1]. لقد ارتبط مفهوم الأمن لفترة طويلة جدا بالدولة، ومع ذلك فهو في الأصل مفهوم ديناميكي يتغير في الزمان والمكان، ونسبي أيضا مادامت الدولة تعمل دوما على زيادة قوتها في مقابل زيادة حالة انعدام الأمن نتيجة الخوف وعدم الثقة في العلاقات الدولية، بالإضافة إلى كونه مفهوما مركبا.

[1] سيد احمد قوجيلي، ***تطور الدراسات الأمنية ومعضلة التطبيق في العالم العربي*** (الإمارات: مركز الإمارات للدراسات والبحوث الإستراتيجية، ط1، 2012)، ص: 09-10.

وعرّف "والتر ليبمان" (Walter Lippman) الأمن القومي من خلال اعتبار أن الدولة "آمنة إذا لم تبلغ الحد الذي تضـــحي فيه بقيمها إن أرادت أن تتجنب الحرب"[1]. وكان تعريف "وولفرز" (Arnold Wolfers) للأمن في عام 1952 مقدمة للتطورات اللاحقة التي شـــهدها مفهوم وموضـــوع الأمن، فقد انطلق من طرح أسئلة محورية: الأمن لفائدة من؟ ولأيّ قيم؟ وتحسُّبا لأي مخاطر أو تهديدات؟[2].

فتعريف الأمن انطلاقا من المفهوم التقليدي ارتبط بنوعية التهديد (تهديدات عسكرية)، وبمصدره (الدولة القومية)، وآليات حفظه وضمانه (أي الآليات العسكرية). بعد ذلك، بدأ الباحثون في مراكز البحث الغربية يطرحون أسئلة على غرار: من يحقق الأمن؟ أو من يضمنه؟

وفي هذا الصدد يتبنى "جيمس آدامز" James Adams في مقالته: "**الدفاع الافتراضي**" نهجًا صارمًا للواقعية الجديدة للتعامل مع قضايا الإرهاب والأمن السيبراني، وبينما يخفف من المعضلة الأمنية، فإنه يخلق نظامًا دوليًا متوترًا وغير موثوق به وغير مستدام في نهاية المطاف، فيما يذهب يوهان إريكسون Johan Eriksson وجيامبيرو Giampiero وجيوكوميلو Giocomello إلى أنه للتعامل مع هذه التهديدات الأمنية، يجب أن يُنظر إلى الإنترنت كمجال له عاداته الخاصة، ويجب على الدول أن تجتمع لتعزيز تطورها وضمان أمنها فيه، وهو أمر ممكن من خلال الفكر النيوليبرالي والبنائي[3].

1- الواقعية والمعضلة الأمنية السيبرانية:

لطالما ارتبط مفهوم المعضلة الأمنية بالنظرية الواقعية في حقل العلاقات الدولية، حيث ظهر مفهوم المأزق الأمني للمرة الأولى مع "جون هارتز" John Hartz سنة 1950، ثم هربرت باترفيلد" في 1954، وهو يشير إلى حالة الفوضى التي تحكم العلاقات الدولية، حيث تضاعف كل دولة من قوتها العسكرية بدافع الخوف وعدم الثقة السائدين في إطار العلاقات بين الدول[4].

---

[1] سـليمان عبد الله الحربي، "مفهوم الأمن، مسـتوياته، وصـيغه، وتهديداته (دراسـة نظرية في المفاهيم والأطر)"، ***المجلة العربية للعلوم السياسية***، العدد 19 (صيف 2008)، ص: 10-14.

[2] محسن بن العجمي بن عيسى، ***الأمن والتنمية***، ط1، (الرياض: منشورات جامعة نايف العربية للعلوم الأمنية، 2011)، ص42.

[3] Constantine J. Petallides, "Cyber Terrorism and IR Theory: Realism, Liberalism, and Constructivism in the New Security Threat", VOL. 4 NO. 03 (2012), in: https://cutt.us/BpNG8

[4] ياســين طرشــي، توفيق حكيمي، "المعضــلة الأمنية الدولية"، في: https://qawaneen.blogpost.com/2010/06/blog-post_7365.html?m=1 (2021/09/16)

ينظر "جيمس آدمز" إلى الإنترنيت كنظام فوضوي، فالفضاء السيبراني ككل أصبح ساحة صراع لا تختلف عن ساحة الصراع الواقعية من حيث الفوضى، كما لا يختلف من حيث وجود دول تتوخى الحذر وتعامل غيرها من الدول بعدم الثقة، بما يعني أنها تزيد من قدراتها الدفاعية، تماماكما هو الحال في النموذج الواقعي، ويشير آدامز إلى أن "التفوق العسكري الساحق والميزة الرائدة في تكنولوجيا المعلومات جعلت الولايات المتحدة الدولة الأكثر عرضة للهجمات الإلكترونية[1]. ولأن قضايا الأمن والدفاع تأتي في مقدمة اهتمام الواقعيين، في إطار ما يعرف بالسياسات العليا، فإن قضايا الأمن السيبراني تدخل في هذا الإطار باعتبارها قد تتجاوز الأهمية الإستراتيجية لتصبح ضرورة حيوية للدولة[2]. وهنا تندرج أيضا مسألة السيادة "السيبرانية" التي تطرح بدورها إشكالا كبيرا.

انطلاقا من ذلك، أصبح الحديث عن وجود معضلة أمنية سيبرانية يفرض نفسه في العصر الرقمي، حيث تداخل التطور التقني والمعلوماتي مع التهديدات والهواجس الأمنية، مما استدعى وضع سياسات دفاعية سيبرانية وجعل ترسانة التصدي لأي هجوم سيبراني قيد التفعيل.

ومع ذلك، يبقى من المؤكد أنه كلما اتجهت الدولة نحو عصرنة قطاعاتها عبر الرقمنة، كلما زادت شدة التهديد (وهي معضلة أمنية فعلية) كما كان الحال مع إستونيا، مما يوضح أن "أزمة الدفاع في الفضاء السيبراني أزمة عميقة تتطلب مسايرة الأحداث والتطورات التكنولوجية خطوة بخطوة، خاصة مع الأسلحة السيبرانية التي تشهد تطورا كبيرا في كل وقت"[3].

ويناقش الواقعيون فكرة القدرة على الضربة الأولى كوسيلة لإنهاء معضلة أمنية وضمان عدم قدرة العدو على الانتقام، ولكن هذا يظل نسبيا في حالة الهجمات السيبرانية لما تتمتع به من خاصية عدم القدرة على معرفة العدو أو التنبئ بما سيقوم به في فضاء بهذا التعقيد. بالتالي أمكن القول بأن المنظور الواقعي

---

[1] Constantine J. Petallides, ***Op.cit.***

[2] مسعود ناجي إدريس، "تأثير السياسة السيبرانية على السياسة العملية ونظريات العلاقات الدولية (الجزء الأول)"، 2021/03/27، http://burathanews.com/arabic/studies/389167 (2021/09/25)

[3] فاتح حارك، رياض حمدوش، "الدولة بين الهيمنة وتحقيق الأمن في الفضاء السيبراني"، ***المجلة الجزائرية للأمن الإنساني***، المجلد 07، العدد الأول (يناير 2022)، ص140.

في السياق السيبراني يحتمل قابلية الإسقاط من جهة، ونسبية ذلك من جهة أخرى، خاصة عندما يتم تناول الرؤية الليبرالية والحاجة إلى تطوير رؤية جديدة للمجال السيبراني خارج مرتكزات المنظور الواقعي التقليدي.

2- التصور الليبرالي: التعاون المؤسسي.

الحديث عن التصور الليبرالي في هذا الصدد يقود إلى الحديث عن التعاون الدولي كسبيل للحد من مخاطر الإرهاب السيبراني وتأمين المجال الإلكتروني، مع إشارة إلى تعدد الفاعلين (منظمات دولية حكومية وغير حكومية على سبيل المثال) إضافة إلى الدولة التي تظل محور العلاقات الدولية.

في مقالهما المعنون: "ثورة المعلومات والأمن والعلاقات الدولية"، أكد يوهان إريكسون Johan) (Eriksson وجيوكوميلو (Giocomello) ، أكد الباحثان على أهمية التعـــاون لمواجهة التهديدات السـيبرانية، خاصـة وأن الدولة بمفردها لا يمكنها تأمين مجالها السـيبراني، وهو ما يقود إلى الحديث عن الليبرالية الجديدة التي تناولت مسألة إنشاء مؤسسات دولية، مما سيكون من شأنه تقليص حالة التهديد والضـعف في هذا المجال الجديد، ولكنه يتطلب كشـف كل عضـو (أي كل دولة) عن قدراته، وتبادل التقنيات والخبرات والمعلومات اللازمة، حتى تكون هنالك مساحة من الثقة وقدرة أكبر على تنسيق الجهود والقدرات، ولكن لا يجب التعاطي بدرجة أكبر من التفاؤل مع هذا التصور، فالدول قد تتعاطى بحساسية وغموض فيما يخص بعض الملفات الشديدة الأهمية (بالنسبة لها، وهو حق لها باعتبارها دولة سيدة)، مما يعيق التعاون الدولي ويجعل عنصر غياب الثقة في العلاقات بين الدول حاضرا دوما[1].

بالتالي يبقى المنظور الليبرالي بدوره نسبيا عند ربطه بالقضايا السيبرانية، فالمعوقات المذكورة تعبّر عن جانب من عدم وجود تعاون حقيقي وفعال بين الدول، سـواء في مجال الجريمة الإلكترونية، الهجمات السـيبرانية أو الإرهاب السـيبراني، وهذا يضـاف إلى المعوقات المتصـلة بخصـوصـية وتعقيد الفضـاء الإلكتروني.

3- التصور البنائي في السياق السيبراني:

يرى أنصار البنائية بأن الصراعات الاجتماعية تعتمد على عوامل معرفية كالأيديولوجيا، والقومية، والعرقية، والدين، وهي عوامل تعزز الاختلاف في المجتمع، في حين تتشكل حالة من التفاهم والتوافق بين

[1] إبراهيم بولمكاحل، ***مرجع سابق***، ص 154.

أعضاء جماعات معينة مثلما هو حال الجماعات المتطرفة والتنظيمات الإرهابية حيث يتم الجوء إلى تشكيل هوية جديدة انطلاقا من قيمة خاصة ومشترَكة[1].

ووفقا للبنائية فإن الإنترنيت أداة هامة لتبادل المعلومات، كما أنها وسيلة متميزة لتطوير هوية رقمية، مما يؤكد أهمية الرموز والأفكار في صلتها بثقافة الإنترنت، وبالتالي ضرورة أن تتطور التفاعلات بين الفاعلين (من الدول وغير الدول) بما يناسب العصر الرقمي، وكمثال حول الفاعلين الرقميين من غير الدول، والذين شكّلوا هوية خاصة في الفضاء السيبراني، ما يعرف بجماعة المجهولين (Anonymous) الذين نفذوا هجمات في أستراليا بتاريخ: 10 فبراير 2010، أدت إلى إسقاط مواقع حكومية وبرلمانية احتجاجا على تشريع الرقابة على الإنترنيت[2].

وكتقييم للنظريات الثلاث في سياق تناول الفضاء السيبراني، يمكن القول إن إسقاطها عليه يظل نسبيا في جميع الأحوال، فعدم الثقة بين الدول بالمنظور الواقعي يخلق معضلة أمنية سيبرانية، ورفض الدولة لمشاركة معلوماتها وخبراتها بصورة تامة يؤدي إلى إعاقة التعاون الدولي في الشؤون السيبرانية، كما أن الهوية الرقمية التي تتشكل جرّاء انتشار تكنولوجيا المعلومات والاتصالات بحاجة إلى التصدي الجيد لتأثيراتها السلبية، كما هو الحال مع الجماعات الإرهابية بالتوازي مع بروز ظاهرة الإرهاب السيبراني.

وفي الجانب المقابل، يتضح بأن التأسيس لرؤية تزاوج بين الواقعية والليبرالية هو الأنسب، ففي حين تهتم الدولة بتطوير سياستها الدفاعية في المجال السيبراني لا يوجد مانع من الدخول في سياسات تعاون مع الدول الصديقة على سبيل المثال، باعتبار أن التعاون ضرورة في هذا العصر من أجل تقليص تهديدات الإرهاب الإلكتروني والهجمات الأخرى في هذا الفضاء، أو قد يكون ذلك في إطار تكتل أو اتحاد حاصل فعلا كما هو الشأن مع الاتحاد الأوروبي الذي عمل على تطوير سياسات متنوعة في إطار رسم أسس إستراتيجية أوروبية للأمن والدفاع السيبراني، وهو ما سيتم عرضه بالتفصيل في الفصل الثالث من الأطروحة.

---

[1] Курылев Константин Петрович, ПОНЯТИЕ «МЕЖДУНАРОДНЫЙ ТЕРРОРИЗМ» СОГЛАСНО КОНСТРУКТИВИСТСКОЙ ШКОЛЕ МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ, ЖУРНАЛ ПОЛИТИЧЕСКИХ ИССЛЕДОВАНИЙ Том 3 № 1, 2019, доступны на: https://naukaru.ru/ru/nauka/article/28091/view

[2] إبراهيم بولمكاحل، ***مرجع سابق***، ص 155.

المطلب الثاني: الأمن السيبراني في دراسات الأمن الموسع: مدرستان للأمن وتوليف المؤسسة النظرية "كوبنهاجن وباريس".

- **الحاجة إلى توسيع مفهوم الأمن (الأمن الموسّع):**

يشير مفهوم توسيع الأمن إلى المستوى الأفقي في تناول موضوع الأمن، بمعنى القطاعات التي يمسها إلى جانب القطاع العسكري التقليدي. في حين يعني التعميق (deepenning) المستوى العمودي، أي بالانتقال من الدولة إلى الفرد مرورا عبر المجتمع، بوصفها مواضيع "مرجعية للأمن"[1]. وكان لدراسات السلام بعد الحرب العالمية الثانية أثرها في الدراسات الأمنية، حيث أعطت اهتماما للفرد والتعاون الدولي لتحقيق الأمن[2]، لذلك تجب الإشارة إلى جهود منظّري السلام أمثال: "كنيث بولدينغ" (Kennith Boulding) صاحب نظرية السلام المستقر و"يوهان غالتونغ" (Johan Galtung) صاحب نظرية السلام الإيجابي، في تطوير المفهوم والرؤية في حقل الدراسات الأمنية. كما تجب الإشارة إلى دور لجنة "بالم" (Palme Commission)، حيث تقدمت بتقرير إلى الجمعية العامة للأمم المتحدة عام 1982، تضمّنت ضرورة العمل الدولي المشترك في ظل حالة الفوضى وسباق التسلح[3].

إن أمن الدولة أو الوحدة السياسية قد لا يتطابق مع أمن الفرد والمجتمع إذا كانت هنالك ممارسات قمعية داخليا على سبيل المثال. وكانت هذه واحدة من المبررات التي جعلت إسهامات الباحثين تتمحور حول توسيع مواضيع الأمن وقضاياه، لتتجاوز بذلك فكرة أمن الدولة القومية دون أن تنفصل عنها تماما. وكانت إسهامات "باري بوزان" (Barry Buzan) في تطوير حقل الدراسات الأمنية بارزة، حيث أصبح هذا الحقل –إلى حد ما– متميزا عن الدراسات الإستراتيجية (هذا لا يعني كونَهما منفصلَين)، والذي ظل يُعنى تحديدا بالشؤون العسكرية والدفاعية.

ويعد كتاب "بوزان" المعنون: "الشعب، الدولة والخوف" (People, State and Fear)، الصادر سنة 1982، من الكتابات الأولى في مجال الأمن الموسع، إذ تطرق فيه "بوزان" إلى "مقاربة قطاعية

[1] سيداحمد قوجيلي، ***مرجع سابق***، ص13.

[2] محسن بن العجمي بن عيسى، ***مرجع سابق***، ص23.

[3] سيداحمد قوجيلي، ***مرجع سابق***، ص–ص: 13–15.

للأمن الموسع، بتوسيع نطاق التحليل ليشمل القطاعات السياسية، والاجتماعية، والاقتصادية، والبيئية" إضافة إلى القطاعات العسكرية[1].

- **مدرسة كوبنهاجن:**

اجتهدت مدرسة كوبنهاجن في وضع نموذج بنائي لدراسة الأمن بمفهومه الواسع[2]. ودام نشاط معهد كوبنهاجن لأبحاث السلام من 1985 إلى 2004، أسهم خلالها بمجموعة من البحوث الثرية على الصعيد الفكري والتنظيري، خاصة مع تبلوُر نظرية الأمن المجتمعي (Societal Security) ونظرية الأمننة (Securitization). لقد شكّلت أعمال "بوزان" و"وايفر" (Ole Waever) طفرة نوعية في الدراسات الأمنية من خلال انضمامهما إلى المعهد، وكان "بوزان" في نهاية الثمانينيات مسؤولا عن مشروع "السمات غير العسكرية للأمن الأوروبي"، ثم طور الباحثان معًا نظرية الأمن المجتمعي، وطور "وايفر" في المقابل نظرية الأمننة[3].

يرى "بوزان" أن الأمن "مفهوم معقد، وينبغي لتعريفه الإحاطة بثلاثة أمور على الأقل، بدءًا بالسياق السياسي للمفهوم، ومرورا بالأبعاد المختلفة له، وانتهاءً بالغموض والاختلاف الذي يرتبط به عند تطبيقه في العلاقات الدولية"[4]. وتتمثل أبعاد الأمن عند "بوزان" في: البعد المجتمعي، الاجتماعي، العسكري، السياسي، الاقتصادي والبيئي[5].

يعرف "بوزان" الأمن المجتمعي بأنه "الاستمرارية ضمن الشروط المقبولة للتطور، للأنماط التقليدية للغة والثقافة والهوية الدينية والقومية والعادات"، بمعنى أن الهوية هي في صلب موضوعات الأمن، وأي تهديد يمسها يعد إخلالا بالأمن في بعده المجتمعي، أما الأمننة فتعني إضفاء الطابع الأمني على مشكلات معينة تحددها النخبة الحاكمة انطلاقا من فعل الخطاب (الكلام): "إضفاء الطابع الأمني على

---

[1] سيد احمد قوجيلي، ***الدراسات الأمنية النقدية: مقاربات جديدة لإعادة تعريف الأمن***، ط1، (الأردن: المركز العلمي للدراسات السياسية، 2014)، ص18.

[2] محسن بن العجمي بن عيسى، ***مرجع سابق***، ص29.

[3] قوجيلي، تطور الدراسات الأمنية..، ***مرجع سابق***، ص25.

[4] سليمان عبد الله الحربي، ***مرجع سابق***، ص10.

[5] محسن بن العجمي بن عيسى، ***مرجع سابق***، ص: 31-32.

قضـــية لم تكن تعتبر أمنية قبل التكلم عنها"، وبهذا المعنى يصـــبح مفهوم الأمن أوســـع، وقضـــاياه أو موضوعاته كذلك[1]. وتتضمن عملية الأمننة ثلاثة عناصر محورية هي[2]:

- إثبات أن مسألة معينة تشكل تهديدا للدولة والأفراد.
- تقديم حلول للتصدي لهذا التهديد.
- العمل على تعبئة الأفراد لمواجهة التهديد.

– مدرسة باريس:

تنطلق في دراسـة الأمن من تقنية الحكومة، بالتالي فإن "الأمن في مدرسـة باريس نمط من أنماط الحوكمة يختزل في ممارســـة الشـــرطية عبر تقنيات المراقبة"، وهذا ما يقود إلى الحديث عن "العين الإلكترونية" بتعبير "دافيد ليون" (David Lion)، ومفادها أن "الســـلطة يجب أن تكون منظورة وغير ملموسة" من خلال استخبارات الاتصالات والرادار والصور، وغير ذلك. بالتالي فإن تصور مدرسة باريس للأمن يدور حول: تقنية الحكومة، فاعلية الشـــرطية، تقنيات المراقبة، المعرفة المحتكَرة، وذلك كله "لتحديد طبيعة التهديد وشكل الحقيقة الأمنية"[3].

لقد اهتمت مدرسـة "باريس" في حقل الدراسـات الأمنية النقدية بالجريمة كمسـتوى أقل من الحرب، وذلك على عكس الدراسات الأمنية والإستراتيجية التقليدية. فاهتمت بمسألة مراقبة الحدود وتهديدات الأمن الجديدة. تنطلق مدرســـة "باريس" من تقنية الحكومة كمحدد للأمن، وذلك عبر الاعتماد على الشـــرطية وممارســـة الرقابة، ولا يتأتّى هذا إلا بتوظيف التكنولوجيا في عملية المراقبة والضـــبط الاجتماعي، عبر الكاميرات وأجهزة تحديد الهوية وغيرها من التقنيات المتطورة، إضـــافة إلى الاعتماد على شـــبكة مهنيّي الأمن (Security Professionals)، وهم الخبراء في المجال ميدانيا مثل الشـــرطة والدرك والجمارك، إلخ. اهتمت المدرســـة بالصـــلة بين الأمن الداخلي والخارجي، في مقابل عجز الدولة عن مواكبة والتكيف مع تهديدات الأمن الجديدة، بالتالي رأت أن دمج الأمن الداخلي والخارجي ضـــرورة لأنه من ناحية يعيد

[1] سيداحمد قوجيلي، تطور الدراسات الأمنية..، ***مرجع سابق***، ص: 27–28.

[2] Mathieu Labrie, ***La Sécurisation du Cyberterrorisme aux Etats-Unies***, Mémoire présenté comme exigence partielle de la maitrise en Science Politique, Université de Québec à Montréal (Janvier 2011), p.12.

[3] قوجيلي، تطور الدراسات الأمنية..، ***مرجع سابق***، ص: 34–36.

الاعتبار لفواعل هامة لم تلقَ اهتماما في الماضي، كالشرطة والدرك، ومن ناحية أخرى فإن ذلك يوسع موضوعات الأمن وآليات التعاطي مع التهديدات الأمنية[1].

وتتولى الحكومة أو السلطة تحديد المشكلة الأمنية، مما يجعل التهديد الأمني من عدمه يخضع لانتقائية أكبر، كما أنه يجعل الحكومة تقوم بتفعيل تدابير استثنائية تجاه تلك التهديدات[2]. والأمثلة ها هنا كثيرة، ويمكن الاستشهاد بملف اللجوء والهجرة في دول أوروبية مثل فرنسا وألمانيا والدانمارك، بحيث أنه مع صعود التيار اليميني المتطرف خلال السنوات الأخيرة أصبح خطاب الأمننة متمركزا حول اللاجئين والمهاجرين باعتبارهم تهديدا للأمن المجتمعي في أوروبا وللأمن الوطني.

وبالرجوع إلى التوليفة النظرية بين مدرستي كوبنهاجن وباريس وإدراج موضوع الأمن السيبراني كبُعد جديد للأمن، أمكن القول بأن الأمن المجتمعي لم يعد بالإمكان فصلُه عن أمن الفضاء الإلكتروني بما يشمله هذا الفضاء من أمن المستخدمين له (الجانب البشري)، فمن المعلوم أن هذا الفضاء بات – بشكل أو بآخر– مهددا للهوية وقيم المجتمعات على اختلاف مشاربها الفكرية والثقافية والدينية، سواء من خلال انتشار أفكار متطرفة ودخيلة على المجتمع أو أنماط ثقافية تخترق خصوصيات الثقافات البشرية المتنوعة وتهدد بقاءَها، وهذا يندرج في إطار التهديدات الخارجية للقيم والهوية والثقافة. وقد تحول موضوع الأمن السيبراني والتصدي للإرهاب الإلكتروني إلى موضوع الساعة، فجميع الحكومات أقرّت بخطورة التهديدات التي يكون مصدرها الفضاء الإلكتروني، فتم إضفاء الطابع الأمني على هذا النمط من التهديدات كسبيل للتكيف مع التحول في طبيعتها وأبعادها.

وتسعى الدول إلى جعل التكنولوجيا خادمةً للحوكمة الأمنية[3]، وهو ما تناولته مدرسة باريس بوصف التكنولوجيا عنصرا أساسيا في المراقبة والضبط الاجتماعي وتأمين الحدود، خاصة وأن عصر العولمة قد فرض تحديات كثيرة على الجانب الأمني ولم يعد بالإمكان الحديث عن أمن داخلي دون ربطه بالأمن الخارجي.

---

[1] قوجيلي، الدراسات الأمنية النقدية..، ***مرجع سابق***، ص: 59–63.

[2] ***المرجع نفسه***، 88.

[3] محمد حمشي، "مدرسة باريس للدراسات لأمنية وإشكالية مستوى التحليل في العلاقات الدولية"، ***مجلة السياسة الدولية***، م53، العدد 212 (ابريل 2018)، ص.176.

وفي سـياق أمننة الظواهر، "يعمل الخطاب على الاسـتدلال بوجود تهديد يمس البقاء (المادي أو المعنوي) لموضـوع مرجعي ما (قد يكون الدولة، الفرد، الجماعة أو الهوية)"، فتصـبح تدابير الوقاية والتصـدي ضـرورية لمواجهة هذا النمط من المشـكلات المؤمننَة. وانطلاقا من الجمع بين عصـارة فكر مدرسة كوبنهاجن وفكر مدرسة باريس في حقل الدراسات الأمنية، وإسقاط ذلك على الأمن السيبراني كبعد جديد للأمن، يمكن اسـتخلاص أن القيمة المهدَّدة في وجودها قد تكون الهوية بدرجة أولى وسـيادة الدولة بدرجة ثانية أو العكس، بعد أن كانت السـيادة هي القيمة المحورية المهددة عندما سـاد المفهوم التقليدي للأمن[1].

ولأن الفضاء السيبراني، من خلال خصائصه وتعقيداته، يجعل النظام الدولي أكثر فوضى بسبب عدم وجود قانون دولي يضـبط النزاعات السـيبرانية، وأيضـا لأن الجرائم الإلكترونية تتصـل بالمسـتويات الوطنية، فضـلا عن التطور المسـتمر في التكنولوجيا الرقمية وبالتالي في أشـكال التهديدات عبر المجال السـيبراني، هذا كله يشـكل تحديات على صـعيد التدابير الوقائية التي تتخذها الدول لمواجهة التهديدات السيبرانية وحماية الأمن السيبراني.

في الجانب المقابل، رأى الدارسـون أنه يمكن الاسـتعانة ببعض النظريات في العلاقات الدولية لغرض تفسير وفهم ما يجري من حركية في الفضاء السيبراني، فالواقعية تبقى قابلة للتطبيق حتى في هذا الفضـاء غير المادي بكل ما يحمله من خصـوصـيات وتحولات على صـعيد مضـامين الأمن وسـلوكيات الفواعل الدولاتية وغير الدولاتية، من خلال الاسـتعانة بتفسـيرها لقضـايا الردع وإدارة النزاعات والصـراعات وكيفية الاسـتفادة من التكنولوجيا الرقمية في تعزيز الأمن[2]. وبالرجوع إلى الفكر الليبرالي في العلاقات الدولية، يمكن القول إن الإنترنت لها أدوار هامة بالمقابل في تعزيز السيادة والتعاون الدولي على الأصعدة كافة[3]، ولكن هذه الفرضـية تظل على المحكّ في جميع الأحوال بالنظر إلى ما أفرزه الفضـاء الإلكتروني

[1] محمد حمشـي، "مدخل إلى المدارس الأوروبية فيالدراسـات الأمنية النقدية"، ***المجلة الجزائرية للأمن الإنسـاني***، العدد6 (جويلية 2018)، ص، ص: 341، 345.

[2] Robert Reardon, Nazli Choucri, « The Role of Cyberspace in International Relations : A View of the Literature », Paper Prepared for the 2012 ISA Annual Convention, (San Diego, April 2012), p-p : 6-7.

[3] Henry Perritt, « The Internet as a Threat to Sovereignty ? Thoughts on the Internet's Role in Strenthening National and Global Governance », ***Indiana Journal of Global Legal Studies,*** Vol.05, Issue 02 (1998), p.437.

من تهديدات خطيرة، ليس فقط بالنسبة لمفهوم السيادة بمعناها التقليدي ومفهوم الحدود أيضا، وإنما بالنسبة لقيم المجتمع والتهديدات الأمنية كذلك.

وفي السياق ذاته رأت بعض الأبحاث أن نظريات العلاقات الدولية تبقى قاصرة أمام دراسة وفهم النزاع والصراع في الفضاء الإلكتروني، وقد يكون ذلك بسبب التطور المستمر والهائل في تكنولوجيا المعلومات وبالتالي التطور في طبيعة التهديدات السيبرانية مما سيوسّع نطاق الضرر في العلاقات الدولية[1]. هذا ما تمت مناقشته آنفا.

المطلب الثالث: التحول في أبعاد القوة.

- **القوة الإلكترونية:**

هناك من يدحض مقولة معظم الليبراليين والبنائيين بأن الدولة اليوم فقدت موقعها المركزي لصالح لاعبين آخرين من شركات متعددة الجنسيات ولاعبين من غير الدول، وذلك بسبب تزايد ظاهرة الاعتماد المتبادل عالميا، بل يُنظر إلى أن الجماعات الإرهابية يمكنها أن تلحق أضرارا متعددة المستويات وعلى مختلف البنى في دولة ما، ولكنها لا تعدو أن تكون "بلطجة رقمية"Digital thugs، وأنها كبقية الجرائم الرقمية مجرد مشاكل عادية تواجهها الدولة، لكنها لا تشكل تهديدا لوجودها، إلا عندما ترعاه أو تنفذه دولة أخرى، عندها يصل التهديد لمستويات الأمن القومي العليا[2].

ومع ظهور الفضاء السيبراني كمجال خامس للقوة والسيطرة والصراع، بعد البر والبحر والجو والفضاء الخارجي، أصبح مفهوم القوة الإلكترونية محوريا في سياسات الدول الكبرى، إذ إن الدولة القوية في هذا العصر ليست فقط تلك التي تمتلك أكبر ترسانة عسكرية وقوة اقتصادية، وإنما وجب عليها أيضا أن تمتلك القوة الإلكترونية التي تجعلها تتحكم في حركية التهديدات الحاصلة أو المحتملة في الفضاء الرقمي.

[1] Brandon Valeriano, Ryan C. Maness, "International Relations Theory and Cyber Security : Threat, Conflict, and Ethics in an Emergent Domain", p.264, April 2018, in: https://www.researchgate.net/publication/326845990_International_relations_theory_and_cyber_security_Threats_conflicts_and_ethics_in_an_emergent_domain (04/012/2021)

[2] أنديرا عراجي، ***مرجع سابق***، ص 23

وإذا كان من الطبيعي أن تهتم الدول بالتسليح وزيادة القوة العسكرية باعتبار ذلك ذا أهمية وضرورة حيوية وإستراتيجية، فإنه مع انتقال الصراعات والمعارك إلى الفضاء الإلكتروني بات اكتساب أدوات القوة داخل هذا الفضاء مطلبا لا يقل أهمية عن القوة في الفضاء المادي. كما أن التحول في طبيعة القوة جعل الدول تسعى إلى ربط الصلة بينها وبين القوة البرية والجوية والبحرية وقوة الفضاء أثناء العمليات العسكرية[1]. في السياق ذاته يظهر أن القوة كمفهوم وكواقع نسبية، فهي تتضمن أبعادا عديدة ومتنوعة.

يمكن تعريف القوة بوجه عام بوصفها "مجموعة الوسائل والطاقات والإمكانيات المادية وغير المادية، المنظورة وغير المنظورة، التي بحوزة الدولة، يستخدمها صانع القرار في فعل مؤثر يحقق مصالح الدولة، وتؤثر في سلوك الوحدات السياسية الأخرى"[2]. أما القوة السيبيرية فهي "مجموع التأثيرات الإستراتيجية الناتجة عن العمليات السيبرانية في الفضاء السيبراني وانطلاقا منه"[3].

ويصف "ناي" القوة بقوله: "إنها مراوغة بشكل مفاجئ ويصعب قياسها"، وهو يرى في الفضاء السيبراني مجالا مؤثرا في توزيع القوة داخله، وانطلاقا من ذلك يرى أن القوة أو القدرة السيبرانية تتصل بالموارد المتاحة داخل هذا الفضاء[4]. والمجال السيبراني "يتطلب توافر هيكل مادي لبنائه، وهذا ما تشكله أجهزة الكمبيوتر ووسائط الاتصالات عبر الانترنت. ومن ثم فإن ما يعمل داخل هذه الأجهزة يمثل نمطا من القوة والسيطرة.."[5]. فالقوة الإلكترونية تقوم على خصائص الفضاء غير المادي وأدوات التطور التكنولوجي المادية لتمارس نوعا من التأثير أو السيطرة على المجتمع أو أطراف خارجية قد تكون دولا أو جماعات عابرة للقوميات كالجماعات الإرهابية.

والقوة الإلكترونية لا تكون من نصيب الدول فحسب، فعالم اليوم يعرف تعددا في الفواعل الدولية والفواعل من غير الدول، وفي هذا السياق يوضح الجدول الآتي أهم أشكال الهجمات الإلكترونية، بما فيها

---

[1] عادل عبد الصادق، ***مرجع سابق.***

[2] ***المرجع نفسه.***

[3] Breno Pauli Medeiros, Luiz Rogério Franco Goldoni, « The Fundamental Conceptual Trinity of Cyberspace », ***ContextoInternacional***, 42 (1), Jan/Apr 2020, p.36.

[4] Joseph S.Nye, ***Cyber Power***, Belfer Center for Science and International Affairs, Harvard Kennedy School (May 2010), p-p : 2-3.

[5] محمد بري، ***السيبرنيطيقا (السيبرانية): علم القدرة على التواصل والتحكم والسيطرة***، ط1، (بيروت: المركز الإسلامي للدراسات الإستراتيجية، 2019)، ص44.

الهجمات التي تتولاها الدول والجماعات الإرهابية والأشـــخاص العاديون الذين يمتلكون جانبا من القوة في الفضاء الإلكتروني من خلال التحكم في المعلوماتية، ومن خلال الجدول يظهر الفرق بين الجهات الثلاث المذكورة التي تنفذ هجمات في الفضاء غير المادي من حيث الدافع والهدف، مع تدعيم ذلك بأمثلة للشرح. ويتمثل الهدف من الاســـتشـــهاد بهذا الجدول في التعرف على أهم الجهات التي بإمكانها امتلاك قوة في الفضاء السيبراني، فيكون التأثير على قدر القوة المكتسبة والهدف المرجو.

الشكل (2): جدول يوضح أهم أنماط الهجمات السيبرانية من حيث الجهة المسؤولة، الدافع، الهدف، مع بعض الأمثلة.

الجهة التي تقف وراء التهديد	الدوافع	الأهداف	أمثلة
دول قومية، مجموعات ترعاها دول	جغرافية، سياسية، إيديولوجية	الاضطراب، التدمير، الضرر، السرقة، التجسس، الكسب المالي	تلف البيانات الدائم، الضرر المادي المستهدف، تعطيل شبكة الكهرباء، تعطيل نظام الدفع، التحويلات الاحتيالية، التجسس
مرتكبو الجرائم الإلكترونية	الإثراء	السرقة، الكسب المالي	سرقة الأموال النقدية، التحويلات الاحتيالية، سرقة بيانات الاعتماد
الجماعات الإرهابية، القراصنة، التهديدات الداخلية	إيديولوجية، الاستيلاء	الاضطراب	التسريبات، التشهير، الهجمات الموزعة لتعطيل تقديم الخدمة

المصدر: تيم مورر، ارثر نيلسن، التهديد السيبراني العالمي.. التمويل والتنمية (مارس 2021)، ص25.

نقلا عن: المجلس الأوروبي للمخاطر النظامية، "المخاطر السيبرانية النظامية"، https://cutt.us/VN5rl

إن القوة الإلكترونية حســـب رؤية "ناي" (Joseph Nye) ترتبط بدور الإنترنت في التأثير في تفاعلات الأطراف، كما أن تأثير القوة في الفضـــاء الســـيبراني قد يكون ناعما (Soft Power) من خلال جذب أفراد في مكان آخر (يمكن الرجوع إلى المطالب الســـابقة حيث تم الحديث عن الدعاية الإلكترونية

للجماعات الإرهابية من أجل اســـتقطاب مقاتلين إرهابيين)، كما قد يكون صـــلبا (Hard Power) عبر استهداف خلق ضرر مادي[1].

ولأن الفضـــاء الافتراضـــي قد أفرز تحولات نوعية وتطورات في أبعاد القوة والصـــراع فإن للقوة السيبرانية مسارات تتخذها لتعكس تحولا عميقا في أبعاد القوة، ويحدد الدكتور عادل عبد الصادق مسارات القوة الإلكترونية كما يلي[2]:

- نقل الأحداث من الفضـــاء المادي إلى المجال الســـيبراني، وكمثال على ذلك الصـــراع بين تنظيم القاعدة والولايات المتحدة الأمريكية، أو الصراع بين الكوريّتين وبين الصين وتايوان.
- نقل أحداث من الفضـــاء الإلكتروني إلى المادي، ويظهر ذلك من خلال تأثير ما يتم تداوله إلكترونيا على حالات السلم في العالم (مثال الرسوم الكاريكاتيرية لمحمد عليه الصلاة والسلام وما خلّفته من ردود غاضبة في العالم الإسلامي).
- توظيف الفضاء السيبراني كوسيط إعلامي لبث ما يقع في الفضاء المادي من حروب وغيرها.
- المسار الرابع يتعلق بنطاق الفضاء الإلكتروني، وقد يشمل أنشطة القرصنة والتجسس.

ولأن طبيعة القوة وســـاحة الصـــراع تحولت وانتقلت في القرن الحادي والعشـــرين إلى المجال السيبراني، فحتى القانون الدولي الإنساني أصبح "ينطبق على العمليات السيبرانية خلال النزاعات المسلحة، على أساس أن هذا التأكيد لا يشجع عسكرة الفضاء السيبراني ولا يضفي الشرعية على الحرب السيبرانية"[3]، ومع ذلك فهو تأكيد على الجانب الســلبي والخطر في الفضـــاء الإلكتروني، والذي يجعل القوة الإلكترونية بالتالي ســـلاحا متعدد الأبعاد يمكن توظيفه للتحكم في هذا الفضـــاء وتعزيز الأمن الوطني واســـتقرار المجتمع، كما يمكن اســـتخدامه لتنفيذ هجمات إلكترونية على دول أو أطراف معادية. وبالفعل، جرى استغلال البيئة السيبرانية كفضاء لهجمات متعددة الأبعاد، بما فيها تلك التي تستهدف البنى التحتية دونما

---

[1] Joseph Nye, ***Op.cit***, p.6.

[2] عادل عبد الصادق، ***مرجع سابق.***

[3] "القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة"، ورقة موقف اللجنة الدولية للصليب الأحمر، مقدمة إلى فريق العمل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وإلى فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في ميدان الفضاء السيبراني في سياق الأمن الدولي، نوفمبر 2019، ص09.

حاجة إلى التعرض لها بصـــفة مادية، وكان برنامج "ســـتوكس نت" (Stuxnet) الخبيث في عام 2010 نموذجا حقيقيا لاســـتهداف الفضـــاء المادي (المنشـــآت النووية الإيرانية) انطلاقا من البيئة الإلكترونية، وكمثال آخر قامت دولة الكيان الصـهيوني (إسرائيل) بمهاجمة منشأة "نطنز" في ابريل 2021 متسببةً في قطع التيار الكهربائي عنها.

خاتمة الفصل واستنتاجاته:

يعد مفهوم الإرهاب الإلكتروني من المفاهيم التي تطرح جدلا كبيرا في أوساط الدارسين وذوي الاختصاص، وهذا لأنه لا يوجد تعريف موحد وواضح ليزيح الغبار عن ماهية الإرهاب الإلكتروني، كما لا يوجد – في الجانب المقابل– تعريف موحد لمصطلح الإرهاب الذي بقي تعريفه لعقود طويلة قاصرا عن توضيح المعنى الفعلي للظاهرة الإرهابية أنه مفهوم مطاطي قابل للتأويل. من هذا المنطلق، أتى هذا الفصل ليؤسس لمقاربة معرفية ومفاهيمية شاملة لظاهرة الإرهاب السيبراني في ظل تحولات الأمن والتهديدات الأمنية.

ومن خلال جملة التعريفات التي تم استعراضها في هذا القسم، تم الكشف عن وجود صنفين أساسيين من الإرهاب الإلكتروني، أحدهما محض والآخر هجين. ففي حين يتصل الإرهاب الإلكتروني المحض باستهداف مباشر للبنية التحتية الحيوية للشبكات والمعلومات، يتضمن النمط الثاني (أي الهجين) توظيف التكنولوجيا بما يخدم أيديولوجيا وأهداف الجماعات الإرهابية، أي أنه يقترن بالإرهاب عبر الإنترنت. وبإسقاط أهم عناصر الفعل الإرهابي (القوة، العنف غير المشروع، طبيعة الهدف، التخطيط، التنظيم والتأثير) على ظاهرة الإرهاب السيبراني يتضح أن العناصر هي نفسها، أما الاختلاف فتصنعه الوسيلة (التكنولوجيا) والمجال (الفضاء السيبراني) والخصائص.

ويمكن ذكر أهم استنتاجات الفصل الأول من الدراسة كما يلي:

- يمكن التعرف على ظاهرة الإرهاب السيبراني كموجة خامسة للإرهاب العالمي من خلال الدافع، الهدف المقصود، التأثير المرجو، المنهج المستخدم للهجوم (تفاعل الوسائل التكنولوجية مع الحرب النفسية)، المجال (أي الفضاء الإلكتروني) وفعل الجاني (أي الإرهابي السيبراني)، مع التأكيد دوما على الصنفين المذكورين آنِفًا (إرهاب إلكتروني محض وآخر هجين).
- خصائص الإرهاب السيبراني متنوعة، وهي تجعله تهديدا شديد الخطر خاصة لارتباطه بالفضاء السيبراني الذي يتميز بدوره بمواصفات فريدة أهمها هشاشة الأمن داخله، وهذا انطلاقا من حالة الانكشاف (إن صح التعبير) التي تفرضها طبيعته، مما يجعل من الإرهاب الإلكتروني تهديدا ناعما بدرجة أُولى، كما يمنح للإرهابي في هذا الفضاء مرونة أكبر وقدرة على التلوّن والتخفي.

- من خلال الدراسة تَبيّن أن الإرهاب السيبراني قد يكون أداة من أدوات الحرب السيبرانية التي تحدث بين الدول، وإن كانت أهدافه أكثر ارتباطا بالجانب السياسي والأيديولوجي، كما أن الفاعل مختلف (فرد أو جماعة في حالة الإرهاب الإلكتروني، ودولة في حالة الحرب السيبرانية)، كما أنه يتداخل مع الجريمة الإلكترونية من حيث المجال والوسيلة، وإن كان هذا النوع من الجرائم أكثر ارتباطا بالهدف المادي. أما الجهاد السيبراني فهو الآخر مفهوم جدلي، ويرتبط بفكر الجماعات المتطرفة والتنظيمات الإرهابية في المنطقة العربية بوجه خاص، مثل القاعدة وتنظيم "داعش" الإرهابي، ويمثل تعبير "الجهاد" حالة روحية وفكرية يُعطى لها طابع من القداسة باسم الدين، وقد تطورت هذه الحالة ليصبح المجال السيبراني وشبكة الإنترنت ومنصات التواصل الاجتماعي ساحةً لها.
- يعتمد الإرهاب السيبراني على إستراتيجيات وتقنيات عديدة ومتنوعة، يأتي في مقدمتها التحكم والاستفادة من التطور التقني والمعلوماتي، ونشر الدعاية الإرهابية والخطاب المتطرف عبر شبكة الإنترنت، واستقطاب المناصرين للفعل الإرهابي، مما يجعل قاعدة انتشار الإرهاب أوسع بكثير، أيديولوجيًا وجغرافيا. إن القدرات السيبرانية للجماعات الإرهابية ليست بالأمر البسيط، فهذه الجماعات تضمّ أفرادا على كفاءة عالية وذكاء كبير بما يسمح باستغلال الفضاء الإلكتروني لتوجيه ضربات مادية أو معنوية للحكومات، وهنا تتنوع الأهداف بين أيديولوجية وسياسية، وأخرى قد تصل إلى استهداف البنية التحتية الحيوية وتدمير أنظمة المعلومات الحساسة للدولة.
- في الجانب التنظيري، بات من الضروري دمج البعد الإلكتروني أو السيبراني في دراسات الأمن والعلاقات الدولية وهو ما حاولت النظريات الأمنية التكيف معه، فالتهديد المرتبط بالمجال السيبراني يعرف تصاعدا مستمرا، وفي المقابل ترتفع حدة التأثيرات، وبالتالي ضرورة "أمننة" القضايا السيبرانية ومن بينها ظاهرة الإرهاب السيبراني. وكانت مدرسة باريس للأمن أكثر تدقيقا وكشفا عن البعد الإلكتروني من خلال تناول مسألة مراقبة الحدود والاهتمام بمهنيّي الأمن، وقد أثبت العصر الراهن كيف أن هذا البعد أصبح محوريا في تأمين الدولة وتحقيق الأمن السيبراني. ومع ذلك، يلاحَظ وجود نوع من المعضلة والهشاشة النظرية من جهة، والأمنية من جهة ثانية، وهذا يُردّ إلى خصوصيات المجال السيبراني بحد ذاته والحاجة إلى بلوغ مرحلة من التعاون الدولي الفعال لمواجهة التهديدات المنبعثة من خلاله.

- انطلاقا من ذلك، كان الفصل الأول من الدراسة محاولةً لتأسيس مقاربة معرفية متنوعة للإرهاب السيبراني، وللأهمية التي يحظى بها الفضاء السيبراني كمجال جديد في سياق تحولات الأمن كمفهوم وظاهرة معًا.

الفصـــل الثانـــي

الفصل الثاني: الإرهاب الالكتروني في استراتيجية الأمن الأوربي

المبحث الأول: الفضاء السيبراني وإدارة السياسات الأمنية.

المبحث الثاني: توظيف جماعات العنف للإرهاب السيبراني عبر الفضاء الأوربي.

المبحث الثالث: الإرهاب السيبراني وتداعياته على الأمن الأوروبي

تمهيد الفصل:

تاريخيًا، كان تصور كل من الأيديولوجيين والمراقبين للإرهاب استعراضًا ماديًا للدمار الكارثي، مما رسخ في الاعتقاد بأن الأدلة على الأضرار التي لحقت الهياكل المادية وفقدان الأرواح البشرية كانت مرتبطة ارتباطًا جوهريًا بمقياس الفعالية التشغيلية للإرهاب التقليدي، لكن عالم ما بعد الدولة الوستفالية أسس لوضع أمني جديد تلعب فيه الجماعات الإرهابية دورها كمهدد للأمن والسلم العالميين، ومع استحداث طرق جديدة بفضل الثورة الرقمية تركزت المناقشات وردود الفعل على الهجمات الارهابية الأيديولوجية و/ أو ذات الدوافع السياسية بشكل حصري تقريبًا على ضعف البنية التحتية الحرجة، وحمايتها من التهديدات السيبرانية، التي كان التطرف القلب التفسيري لأغلبها.

هذه الصورة الثابتة هيمنت على المفهوم الأمني العام الذي يصور الاتحاد الأوروبي كجهة فاعلة إقليمية في مجال الأمن السيبراني، يستمر التحليل من خلال دراسة أشكال التهديدات السيبرانية على مختلف البنى التي تمس الأمن الأوربي، كما يعالج هذا الفصل اشكاليات بناء الامن الجماعيمن خلال تقديم تحليل لكيفية تصور الاتحاد الأوروبي للتهديد الناجم عن الإرهاب السيبراني.

على هذا النحو، هذا الفصل له هدفان رئيسيان:

- **أولاً:** إجراء تحليل للبناء الإرهابي الناشط في أوروبا، وفهم تأثيراته.
- **ثانيًا:** تقييم العلاقة بين البناء الاستطرادي لتهديد الإرهاب الإلكتروني، وصياغة سياسات الأمن السيبراني على المستوى الأوروبي، خاصة مع اعتماد أوروبا المتزايد على الاتصالات والبنية التحتية للمعلومات، الأمر الذي يعرض الأمن المجتمعي، الاقتصادي والسياسي والعسكري للخطر.

المبحث الأول: الفضاء السيبراني وإدارة السياسات الأمنية.

يتم التطرق في هذا المبحث إلى جانب من العلاقة بين الفضـاء السـيبراني وإدارة العلاقات الدولية، وذلك بتناول هذا الفضـاء كعنصـر من عناصـر الدولة بحيث تسـعى الدول إلى التحكم فيه وجعله خاضـعا لرقابتها ومصـدرا من مصـادر القوة، بالإضـافة إلى ما أنتجه من تحولات في مفاهيم الحرب وإدارة المعارك، فهو اليوم ساحة جديدة للقتال والصراع وإنتاج الفوضى في المجتمع الدولي بوجه عامّ.

المطلب الأول: الفضاء السيبراني كعنصر من عناصر الدولة.

أصـبح الفضـاء السـيبراني المجال الخامس من مجالات الدولة بعد المجال البري والبحري والجوي والخارجي، بالتالي فمن حق الدولة أن تنظر إليه كعنصر من عناصرها بالرغم مما تفرضه خصوصياته من تحديات ومعوقات للتحكم فيه وفرض حدود وسيادة داخله.

وبالنظر لما أنتجه المجال الافتراضـي من مسـاحات للحرية وتأثير سـياسـي، أصـبحت الدول أكثر اقتناعا بضـرورة "توطين" هذا المجال وممارسـة الرقابة داخله باعتباره ضـمن مجالات سـيادتها، مع الإشـارة إلى أن السـيادة السـيبرانية تعني "السـيطرة على الفضـاء الافتراضـي، شـاملا التفاعلات وتدفقات البيانات والاتصـالات"[1]. قبل عصـور خلت كان يكفي أن تحمي الدولة حدودها وتتحكم في استقرارها الداخلي وتتمكن من هزيمة عدوها الخارجي لكي يقال أنها دولة آمنة[2]، أما الآن فمفهوم الأمن قد تغير وتحول واتخذ أبعادا أخرى من بينها أمن الدولة في الفضاء السيبراني، مما يفسر ويعلّل حاجة الدول إلى مراقبة ما يجري في هذا الفضاء وما يُحتمل حدوثُه من تهديدات لاستقرار المجتمع والدولة معا، ولكنّ ذلك يطرح في المقابل إشكالية الخصوصية بالنسبة لمستخدمي الانترنت وشبكات التواصل الاجتماعي.

ومن بين الدول التي تهتم بالمجال السيبيري كعنصر من عناصرها نجد الولايات المتحدة الأمريكية، وقد تضـمنت إسـتراتيجية الأمن القومي الأمريكية لعام 2010 ما يلي: "تمثل تهديدات الأمن السـيبراني أحد أخطر التهديدات المتعلقة بالأمن القومي، السـلامة العامة والتحديات الاقتصـادية التي نواجهها كأمة"[3]. وفي ذلك تأكيد على حجم التهديد الذي يكون هذا المجال ساحة ووسيلة له، وإشارة إلى الأبعاد أو الأشكال التي يتخذها التهديد السيبراني ومن بينها البعد الاقتصادي.

---

[1] رغدة البهي، "كيف تفرض الدول سيادتها على الفاعلين في المجال الافتراضي؟"، ***سلسلة دراسات خاصة***، العدد 24، مركز المستقبل للأبحاث والدراسات المتقدمة (24 يونيو 2021)، ص: 3-4.

[2] سعد عطوة الزنط، مرجع سابق، ص11.

[3] Timothy M.LcKenzie, ***Is Cyber Deterrence Possible ?*** Air Force Research Institute Papers (Alabama : Air University Press, 2017), p.1.

وترى الصين في الفضاء السيبراني مجالا هاما من مجالات أمنها القومي ونموها الاقتصادي، وهو في المقابل يشكل تهديدا لها على غرار دول كثيرة[1]. وتركز رؤية الصين للسيادة في الفضاء الإلكتروني على المساواة بين الدول في مجال إدارة الانترنت، التزام الدول بعدم الانخراط في أنشطة سيبرانية تهدد غيرها، بالإضافة إلى "حق الدول في اختيار مساراتها الخاصة للانترنت، ونماذج تنظيمه، وسياساتها العامة تجاهه، وعدم التدخل في الشؤون الداخلية للدول الأخرى"[2].

كما أصبح الفضاء الإلكتروني يمثل بالنسبة لإسرائيل مجالا حيويا، لذلك تسعى إلى تأمينه، كما أن "تكنولوجيا المعلومات تساهم مساهمة مباشرة في نمو الاقتصاد الإسرائيلي"، وقد تم إنشاء هيئة السايبر المختصة في التحكم في نشاطات الجيش داخل هذا الفضاء والدفاع أو الهجوم حسب الضرورة الإستراتيجية. وذكر رئيس الوزراء السابق "بنيامين نتانياهو" أن هيئة السايبر الوطنية التي تم إنشاؤها في 18 مايو 2011 تهدف إلى تعزيز قدرة إسرائيل الدفاعية في وجه هجمات الإرهاب الإلكتروني[3].

ويمكن أيضا تناول مسألة التجسس الإلكتروني الذي تعتمد عليه الدولة تكملةً للتجسس في صوره التقليدية، ويكون ذلك لأغراض إستراتيجية من أجل الحصول على معلومات وتعزيز الأمن الوطني[4]، ولأن الدولة ترى في الفضاء الإلكتروني عنصرا إستراتيجيا وحيويا وجب الاستفادة منه.

الملاحظ أنه في مقابل تعقيدات الفضاء السيبراني وخصوصياته وطبيعته غير المادية، يمكنه أن يكون مصدر قوة للدولة متى تمكنت من التحكم فيه، بالرغم مما يحيط بذلك من صعوبة، حيث "تم الانتقال من مستوى التعاملات المادية البسيطة إلى مستويات افتراضية تستعصي على الضبط، ويكمن أصل التعقيد في كون الفضاء الرقمي قد نشأ وتطور بشكل فوضوي غير متوقع خارج هياكل الدولة"[5].

وعلى صعيد سيادة الدولة، كان لتطور تكنولوجيا المعلومات وظهور الفضاء الإلكتروني كفضاء مواز للفضاء المادي أثره في وظائف الدولة التقليدية وهي ثلاث كالآتي[6]:

- وظيفة حماية الأمن الوطني.
- وظيفة تنظيم النشاط الاقتصادي.

---

[1] Breno Pauli Medeiros, Luiz Rogério Franco Goldoni, ***Op.cit,*** p.35.

[2] رغدة البهي، ***مرجع سابق***، ص05.

[3] محمد محارب، "إسرائيل والحرب الإلكترونية: قراءة في كتاب: حرب في الفضاء الإلكتروني (اتجاهات وتأثيرات على إسرائيل) للباحثين: شاموبل ايفن ودافيد بن سيمان–طوف"، 10 اوت 2011،

https://www.dohainstitute.org/ar/ResearchAndStudies/Pages/Israel_and_Cyber_Warfare.aspx

(2021/11/03)

[4] Carolle Vodouche, ***Op.cit***, p-p : 31-32.

[5] إسماعيل أوقادي، ***مرجع سابق***، ص06.

[6] Henri Perrit, ***Op.cit***, p-p : 427-428.

- وظيفة حماية القيم السائدة في المجتمع.

بالنسبة للوظيفة الأولى، يمكن القول إن حصر رؤية الدولة لأمنها في أمن الحدود المادية (التقليدية) هو فهم محدود، فمع تطور تكنولوجيا المعلومات والاتصالات أصبح الفضاء الإلكتروني مجال خصب للتهديدات الأمنية، مما بات يفرض على الدولة تعزيز وظيفتها التقليدية في حماية الأمن الوطني برؤية أشمل ومواكَبة مستمرة لكل التحولات في طبيعة التهديدات (بما فيها السيبرانية) عبر سياسات وتدابير لا تقتصر على الجانب الأمني (الضيق). كما أن النشاط الاقتصادي المنظم باتت تنافسه نشاطات اقتصادية وتجارية ومالية تتم عبر الوسائل الرقمية، وبدون رقابة وتنظيم أحيانا. أما بالنسبة لوظيفة حماية القيم السائدة في المجتمع فالدولة اليوم لم تعد قادرة على التحكم في هذه القيم، نظرا لعوامل متعددة يأتي في مقدمتها العامل التكنولوجي ودور الفضاء السيبراني في خلق هوية افتراضية للأفراد خاصة عبر شبكات التواصل الاجتماعي المعروفة، وإمكانية التأثير والتأثر بأفكار وقيم متطرفة تحضّ على القتل والإرهاب تحت مبررات مختلفة. وباختصار، أدى ظهور المجال السيبراني إلى تشكيل شرخ في وظائف الدولة التقليدية، ذلك ما جعل مراقبة الدولة وتحكمها في هذه الوظائف الأساسية والمركزية في حدود إقليمها مهمة صعبة جدا.

إن "التطورات العلمية التي تسمح باستخدام الفضاء السيبراني، وبعبور شبكة الاتصالات الوطنية أحيانا، تجعل من الصعب، عمليا، ممارسة السيادة الوطنية على هذا المجال السيبراني، وإخضاعه أو إخضاع أي جزء منه للتشريعات أو المراقبة المحلية"[1]. بالإضافة إلى أن الفواعل غير الدولاتية باتت قادرة على التأثير في قرارات الشعوب والحكومات، من خلال امتلاكها قوة نسبية عبر الفضاء الرقمي جعلتها منافسة للدولة[2].

وعلى الصعيد الدولي، تمكّن الفضاء الإلكتروني من فرض أهميته ضمن حركية العلاقات الدولية، وفي المقابل فرض مخاطره، فقد "أصبح العالم يشهد تطورا في المخاطر الأمنية مع تطور مراحل النضج التكنولوجي، مع الانتقال من مرحلة النمو السريع إلى مرحلة الاستخدام الكثيف"، ومن بين هذه المخاطر تحول طبيعة الصراع والنزاع الدولي، وتحول الفضاء الإلكتروني إلى وسيلة وساحة له. وكانت أحداث 11 سبتمبر 2001 محطة انتقال فعلية في الاهتمام بالمجال السيبيري كساحة لتهديد أمن الدول، ثم زادت حدة الهواجس الأمنية في ظل الصراع بين إستونيا وروسيا (2007) والحرب بين روسيا وجرجيا (2008)، وظهور فيروس "ستوكسنت" (Stuxnet) في عام 2010[3].

---

[1] محمد بري، ***مرجع سابق***، ص142.

[2] إيهاب خليفة، ***مرجع سابق***، ص28.

[3] عادل عبد الصادق، ***مرجع سابق***.

وكانت تسريبات "ويكيليكس" الشهيرة نقطة تحول أخرى في علاقة الفضاء السيبراني بالواقع المعيش، من خلال تسريبات مسّت وثائق رسمية بين الخارجية الأمريكية وبعثاتها عبر العالم، مما أثر بشكل كبير في العلاقات بين الدول وبين الحكومات وشعوبها أحيانا[1]، كما عدّت تسريبات "بنما" ذات تأثير خطير في العلاقات بين الدول، وقد تضمنت أسماء لحكام عرب وقتها[2].

وحسب الدكتور عادل عبد الصادق، الباحث المصري في الشؤون الإستراتيجية، فإن الفضاء السيبراني بات يطرح هواجسه الأمنية انطلاقا من الآتي[3]:

- نمو استخدامه والاعتماد عليه، مما زاد احتمالات وقوع هجمات سيبرانية تستهدف البنى التحتية للمعلومات.
- استخدام الفضاء الإلكتروني لا يقتصر على الدولة، فإلى جانبها توجد فواعل أخرى متنوعة وغير دولاتية.
- تسجيل ظاهرة "انسحاب الدولة من قطاعات إستراتيجية لصالح القطاع الخاص وخاصة بالمنشآت الحيوية".
- ظهور الحرب الإلكترونية كنمط جديد من الحروب غير التماثلية.
- دور الشركات المتعددة الجنسيات (مثل فيسبوك وتويتر ويوتيوب) في تقويض قدرة الدول على التحكم في المجال الخامس متمثلا في الفضاء الإلكتروني.

انطلاقا مما سبق، يمكن القول إن الفضاء السيبراني مجال إستراتيجي وحيوي بالنسبة لأي دولة، سيادة الدول فيه تبقى نسبية جدا، وإمكانية فرض السيادة المطلقة عليه لا يمكن تحقيقها لعدة مسببات تم طرحها آنفا، فخصائص هذا الفضاء غير المادي وغياب حدود مرئية داخله تجعله مختلفا تماما وشديد التعقيد، وفي المقابل فإن التهديدات التي تقع داخل أو عبر الفضاء الإلكتروني هي تهديدات خطيرة وجب التكيف معها ومعالجتها حينا بحين.

---

[1] خالد وليد محمود، ***مرجع سابق***، ص117.

[2] محمد بري، ***مرجع سابق***، ص54.

[3] عادل عبد الصادق، **مرجع سابق**.

المطلب الثاني: الثورة التكنولوجية وظهور مجتمع المخاطر الإلكتروني.

- معالم مجتمع المخاطر: منطق ومتغيرات توزيع المخاطرة.

مجتمع الخطر هو مفهوم صـــاغه عالم الاجتماع الألماني ""اولريش بيك" Ulrich Beck[1*] في كتاب له نشـــر بالألمانية وترجم لعدة لغات، وهو يتحدث عن الخطر باعتباره الســـمة الرئيســـية للمجتمع الإنساني المعاصر، بعد اختفاء الأمن النسبي[2]، وفي معرض حديثه عن الخريطة المعرفية للمجتمع العالمي التي طالما دعا إليها منذ التحولات الكبرى التي لحقت بالنظام الدولي، يقول إن هنالك تحولات جوهرية داخل البلد الواحد في مجال الاتصـالات والمعلوماتية مع بروز ظاهرة العولمة وظهور "مجتمع المعرفة"، وتداعيات ذلك كله على المجتمع والدولة[3]، حيث يرى أولريش بيك أن التغير التكنولوجي في تقدمه المتســـارع يجلب معه أنواعا جديدة من المخاطر التي تتولد بشكل نسقي خلال صيرورة التحديث المتقدم، والتي بدورها تطرح تحديات مركبة على الأفراد والمجتمعات[4].

ويمكن تلخيص هذا الطرح فيما رسمه الأستاذ "السيد أمين" للملامح الرئيسية لخريطة التحولات العالمية التي صاحبت العولمة في النقاط التالية[5]:

- **التغير الأول:** الانتقال من النموذج المعرفي للمجتمع الصناعي إلى النموذج المعرفي لمجتمع المعلومات، وقد أنشأ مجتمع المعلومات العالمي مجالا عاما جديدا غير مسبوق في تاريخ الإنسانية هو الفضاء الافتراضي الذي تتدفق فيه المعلومات وتتم فيه التفاعلات الاقتصادية، السياسية والثقافية.
- **التغير الثاني:** الانتقال من الحداثة إلى العولمة بتجلياتها السياسية والاقتصادية وكذا الثقافية.
- **التغير الثالث:** وهذا التغير يأتي كمحصلة للتحولات العالمية في الاقتصاد والسياسية والثقافة والمعرفة والتكنولوجيا.

---

[*] أولريش بيك منظر معاصـــر للحداثة وعالم اجتماع ألماني، ولد في مدينة ســـتولب البوميرانية بألمانيا العام 1944، كتب الكثير عن العولمة والمخاطر، وهو يجادل في نظريته العامة للمجتمع بأن التغير التكنولوجي ولّد أخطار متأصـــلة أعادت تشـــكيل مجتمع خطر عالمي.

[2] السيد ياسين، "مجتمع الخطر ودورة الخوف"، موقع جريدة الاتحاد، 10 اوت 2005، https://cutt.us/FtvM9 (2021/11/24)

[3] منير الحمش، "مجتمع المخاطر في ظل التحولات الاقتصـادية والاجتماعية"، مداخلة في ندوة الاقتصـاد الرابعة والعشـرون حول التنمية الاقتصـادية والاجتماعية في سـورية، جمعية العلوم الاقتصـادية السورية، دمشق : 2011، ص 4.

4 جلود رشيد، مقاربات سوسيولوجية معاصرة: مجتمع المخاطرة عند "أولريش بيك" أنموذجاً، *مجلة العلوم الانسانية لجامعة أم البواقي*، المجلد 8، العدد1 (مارس 2022)، ص 433-442

5 منير الحمش، *مرجع سابق*، ص 5-6

وكان عالم الاجتماع الألماني "أولريش بيك" قد تحدث عن التغير الذي يجعلنا ننتقل من الأمن النسبي إلى الخطر المطلق، لأن المجتمع الحديث المتطور وفقه هو تكوين مليء بالصراع مع عدم الشعور بالأمان والمخاطر الاصطناعية[1].

- **التغير الرابع:** والذي تجلى سقوط النموذج القديم للأمن القومي وبروز نموذج جديد هو الأمن القومي المعلوماتي.
- **التغير الخامس:** هو بروز قيم حضارية جديدة في جميع أنحاء العالم، أبرزها "المسح العالمي للقيم" الذي أشرف عليه عالم الاجتماع الأمريكي "انجل هارت" Angel Heart، مما يكشف بروز وعي كوني جديد، من علاماته ظهور القرصنة الإلكترونية وتخريب قواعد البيانات واستخدام الجماعات الإرهابية لشبكة الانترنت في التواصل[2].

كل هذه التغيرات يجعلنا أمام مساءلة الأفكار الرئيسية لعقد المخاطرة*، والخاصة بمدى القدرة على التحكم في التهديدات والأخطار الناجمة عن الصناعة والقدرة على تعويضها، ويتضح هذا في أن ديناميكية مجتمع المخاطرة تستند بدرجة أقل على الافتراض الذي يجعلنا نضطر اليوم وفي المستقبل للعيش في عالم مخاطر، عالم يخضع لشروط المصنّع والمُصنّع ذاتيا، ويندرج ضمن هذا كونُ العالم لم يعد قادرا على التحكم في الأخطار التي تنجم عن الحداثة.

ويمكن للمجتمع المعاصر التحكم في الأخطار التي يتسبب فيها، وهو اعتقاد قابل للدحض ليس بسبب الإخفاقات والهزائم التي عرفتها الحداثة، بل بسبب انتصاراتها[3]، خصوصا ما خلفته الطفرات التكنولوجية وما صاحبها من ثورة رقمية (النمط الرابع في سلسلة الثورات التي عرفتها عملية الاتصال بين الأفراد والمجتمعات عبر التاريخ)[4]، الأمر الذي جعل المجتمعات تتطلب آليات وسياسات حوكمة، وقيما

---

[1] أولريش بيك، ***مجتمع المخاطر العالمي، بحثا عن الأمان المفقود***، تر. علا عادل وآخرون، ط1، (القاهرة: المركز القومي للترجمة، 2013)، ص 28.

[2] منير الحمش، ***مرجع سابق***، ص 6.

* يقصد أولريش بيك بعقد المخاطرة تلك التحولات التي تنشأ جراء ديناميكية صراع يعكس التصور العالمي للدول والتكهنات المحتملة الناجمة عن هذا التصور، وهو ما يدمر المؤسسات الغربية، كما يرى أن المخاطر هنا تعني التهديد السريع للحضارة الإنسانية وإمكانية تحول التقدم بفعل مسببات معينة إلى همجية بصورة كارثية.

[3] أولريش بيك، ***مرجع سابق***، ص 29.

[4] عصام سليمان الموسى، "الثورة الرقمية تصنع الإعلام العربي على مفترق الطرق"، ***مجلة المستقبل العربي***، مركز دراسات الوحدة العربية، بيروت، العدد 376(2010)، ص: 100-101.

مؤسسية، وتتبعا للمستخدمين وسياسات للرقابة الوطنية المتنوعة على الشبكات لتحكم بالمخاطر المستحدثة[1]، وهو الأمر الذي قامت عليه مدرسة باريس.

فمنذ ظهور الإنترنت بات واضحا بأنها ظاهرة مختلفة في خصائصها عن ظواهر التقدم العلمي الذي سبقها، خاصة وأن عالم الإنترنت يتصف بغياب الحدود (حدود غير مرئية أو ملموسة)، مما يجعل تأثيرها على السيادة الوطنية واضحا، كما قد كسر الفضاء الإلكتروني من خلالها (أي الإنترنت) مبدأ الحدود والجغرافيا، وكرس لما يمكن تسميته بـــ: "الثقافة السيبرانية" التي عزّزت حرّية الفرد انطلاقا من انخراطه في النّشاط داخل الفضاء السيبيري[2].

بالإضافة إلى كون المجتمع الحديث يتفرد بعدة ميزات، مثل إنشائه وتركيزه في المناطق الحضرية المكتظة بالسكان، واعتماده على التكنولوجيا المتطورة وزيادة مستوى التنقل للأفراد والسلع والمعلومات، ومع الازدهار السكاني العالمي الذي وصل إلى قرابة 7 مليارات، فإن عدد أولئك الذين قد يتأثرون ويتعرضون للتهديد يتزايد، وبالمثل يتزايد عبء حكومات الدول القومية.

ومن المثير للاهتمام أن الرّاحة التي توفرها التكنولوجيا الحديثة وطبيعة المجتمع الحديث ستجعل الأمر أرخص وأسهل نسبيًا لهؤلاء الإرهابيين المحتملين لتنفيذ مخططاتهم الإجرامية، مقارنة بالمبلغ الذي يتم إنفاقه على منع الهجوم حيث يمكن إطلاق هجوم إلكتروني من أي جهاز كمبيوتر في جميع أنحاء العالم[3].

وفي ضوء ذلك، فالعولمة التي يمكن ربطها بمصطلح "مجتمع المعلومات" والتحولات التي عرفها المجتمع اجتماعيا واقتصاديا نتيجةٌ لمسارات التحديث في المرحلة ما بعد الصناعية[4]. هذا الربط يجعلنا نقول إن ثورة المعلومات والتكنولوجيا هي التي عزّزت الفكرة القائلة بأن "المسافات الجغرافية البعيدة باتت مختزَلة، والاتصالات باتت سهلة ومرنة، بالإضافة إلى الأنماط الثقافية المخترقة لخصوصيات المجتمعات المتمايزة".

وعليه، يتم في الفضاء السيبراني إعادة إنتاج بيئة تحاكي الوجود المادي في العالم الحقيقي[5]، وهو ما أعطى مفهوما جديدا للزمان والمكان[6]. فقد ساهم تطور تكنولوجيا المعلومات والاتصال في تسريع حركية

---

[1] بيتر بي سيل، ***الكون الرقمي.. الثورة العالمية في الاتصالات***، تر. ضياء وزّاد (المملكة المتحدة: مؤسسة هنداوي سي آي سي، 2017)، ص 339.

[2] Henri Perrit, ***Op.cit,*** p-p : 426-427.

[3] Awang Dzul-Hashriq Dharfizi, "Non- Conventional Security Risks of the 21st Century", ***International Security***, 15 DECEMBER 2011, in: https://www.academia.edu/5451801/Non_Conventional_Security_Risks_of_the_21st_Century?email_work_card=title (28/03/2021).

[4] إيهاب خليفة، ***مرجع سابق***، ص: 21-21.

[5] Janice Richardson, et autres, ***Manuel de Maitrise de l'Internet : Accompagner les utilisateurs dans le Monde en Ligne,*** Conseil de l'Europe (Décembre 2017), p.163.

[6] إسماعيل أوقادي، ***مرجع سابق***، ص07.

العولمة وبروز مجتمع واقتصاد رقميين قابلين للاختراق والتفكك النظمي السريع، كما أن الانترنت ساهمت في خلق فضاء أسّس لنمط حياة مختلف على الأصعدة كافة[1].

كما لا يمكن فهم حركية العولمة دون فهم البنية الجديدة للنظام الدولي والعلاقات الدولية، وما تفرضه فكرة تلاشي الحدود الدولية وتجاوز المعنى التقليدي المرتبط بالجغرافيا، ونمو تأثير المتغيرات الاجتماعية والثقافية والاقتصادية في السياسة والأمن[2]، وهو ما أطلق عليه المفكر والمنظّر الأمريكي في حقل العلاقات الدولية "جوزيف ناي" (Joseph Nye) تسمية "تأثير النظام"[3].

من جهة أخرى، يعد تطور وسائل الإعلام والاتصال التي عرفت تحولات نوعية وثورة كبيرة في عصر التطور التقني والمعلوماتي، ذا أثر كبير في الواقع الاجتماعي والسياسي للفرد، فقد أفرز هذا التطور تناقضات عديدة، تراوحت بين سهولة التزوُّد بالمعلومة وحرية التعبير، وفي المقابل الاستخدام السيء لهذه الوسائط، ومن ذلك استغلالُها في نشر التطرف الديني والكراهية بين أفراد المجتمع[4]، وبالموازاة مع ذلك لم يعد هنالك مجال للشك بأن "المجال العمومي الافتراضي محكوم كذلك بالصراعات ذاتها التي تحكم المجال العمومي الكلاسيكي"، كما أن الفضاء السيبراني بوجه عام بات مهددا لقيم المجتمع وهويته الوطنية مكرسا بذلك لمخاطر جديدة أصبحت هذه الشبكات محركها[5]، فوسائل الاتصال الحديثة تنطوي على عنصر التفاعل، وهي بذلك أكثر تأثيرا في الحياة العامة على مستويات متعددة[6].

وما يؤكد صدقية على الأمر ارتفاع معدل استخدام الانترنت في العالم بنسبة فاقت 50 بالمائة في 2016، وبنسبة 73,9 بالمائة في أوروبا في نفس العام، كما بلغ عدد مستخدمي الفيسبوك 1,71 مليار، ومليار شخص بالنسبة لتطبيق واتس آب، و313 مليون مستخدم بالنسبة لتويتر[7].

في غضون ذلك، كانت التوقعات المستقبلية تشير إلى أنه سيكون هنالك 50 بليون جهاز متصل بالأنترنت، مما يجعل هذا الانتشار الواسع لاستخدام الشبكة مهددا لاحتمالية تزايد عمليات الاختراق

---

[1] محمد بري، ***مرجع سابق***، ص: 42-43.

[2] Hakem Ghasemi, "Globalization and International Relations : Actors Move from Non- Cooperative to Cooperative Games", p-p : 7-10, in: https://bit.ly/3MqnABe (15/08/2021)

[3] سماح عبد الصبور، "الإرهاب الرقمي: أنماط استخدام الإرهاب الشبكي"، في: 2019/01/18، https://futureuae.com/ar/Mainpage/Item/227

[4] عائشة لصلج، "العنف الرمزي عبر الشبكات الاجتماعية الافتراضية: قراءة في بعض صور العنف عبر الفيسبوك"، في: 2018/07/23، https://mominoun.com/articles/..B1-4065

[5] نهى بلعيد، ***مرجع سابق***، ص: 10، 18.

[6] حفيظ هروس، "سلطة الافتراضي؟"، 15 يناير 2021، ص4، https://www.takamoul.org/?p=553 (2021/03/10)

[7] Délégation Ministerielle aux Industries de Sécurité et à la Lutte contre les Cybermenaces, ***Etat de la Menace Liée au Numérique en 2017***, Rapport n1 (Janvier 2017), p.24.

وصعوبة تأمين الفضاء الإلكتروني[1]، ومع انتشار نماذج للسوق الإلكترونية وانتشار استعمالات انترنت الأشياء كانت الفرضية السائدة مطلع الألفية الجديدة هي عدم التحكم في المجتمعات والأسواق في شكلها الرقمي وخروجها من مجتمعات الرقابة إلى المجتمعات المنكشفة.

ومع كل مظاهر العولمة تلك، واستنادا لما توفره البيئة الرقمية من ملاذ آمن للمجموعات الإجرامية والمتطرفين، توسعت مصادر الخطر وأصبحت متعددة في الواقع، ولعل أبرزها ظاهرة الإرهاب الذي تعدى مرحلة المحلية وانتقل إلى العالمية بحيث أصبح إرهاباً "معولما".

وقد استطاعت الجماعات الإرهابية استخدام الفضاء المعلوماتي في الاتصال ونشر ثقافة الإرهاب وتبادل المعلومات، كما أدت بعض الصراعات الدولية إلى أن تصبح بعض البلدان، مثل العراق وسوريا، أرضا خصبة لتنمية كوادر الإرهابيين الذين يستطيعون الانتقال بإرهابهم إلى بلاد أخرى.

وهناك شواهد على أن هناك جماعات من الإرهابيين ينتمون إلى جنسيات مختلفة، مستعدون للذهاب إلى أي بلد في العالم باسم ."الجهاد" ضد أعداء الإسلام، مما ولد مخاوف مجتمعية شديدة في البلدان الغربية من احتمال أن يلجأ الإرهابيون لاستخدام السلاح ضد أهداف مختارة بعناية.

وإذا أُضيفت احتمالات اختراق العصابات الإرهابية لشبكات المعلومات في الدول الغربية وتخريبها، فهذا يؤسس لمجتمع مخاطر عالمي تتخطى حيثياته بلدان المصدر إلى دول أوربا، مستغلين التكنولوجيا لتنفيذ أجندات معينة[2].

المطلب الثالث: فضاء القتال الجديدة: الانتقال من فضاء حقل المعركة إلى الفضاء السيبراني

يتم التركيز في هذا العنصر على الفضاء الإلكتروني كمجال وساحة جديدة للقتال والحرب، بحيث تسعى الإستراتيجيات العسكرية إلى توظيفه والاستفادة منه ومن خصائصه، وتعمل الدول المتطورة على تأمينه في مواجهة الهجمات والحروب السيبرانية والإرهاب الإلكتروني.

إن حروب الجيل الخامس نتاج الثورة في الشؤون العسكرية (RAM)، والتي تشير إلى "تحول جذري في طبيعة الحرب، ناتج عن اختراقات تكنولوجية تتصل بتغييرات عميقة في العقيدة العسكرية والمفاهيم التنظيمية، وتعديل محوري في سلوك وإدارة العمليات العسكرية.." . وانطلاقا من ذلك فقد أصبحت المعلوماتية اليوم هي العنصر المحوري والحاسم في الحروب، وهو ما يجعلنا نستحضر ما تناوله "توفلر" (Alvin Toffler) في كتابه الشهير: الموجة الثالثة، حيث قال إن المجتمعات البشرية مرت بثلاث موجات كبرى هي: الموجة الزراعية، فالصناعية، ثم المعلوماتية حيث تصبح المعرفة هي العامل المتحكم في كل شيء[3].

---

[1] V.T.Tsakanyan, « The Role of Cybersecurity in World Politics », ***Vestnik RUDN***, VOL 17 , N02, (December 2017), p-p : 339-348

[2] السيد ياسين، مرجع سابق.

[3] Mathieu Labrie, ***Op.cit***, p-p : 26-27.

وتشـير البحوث إلى بدايات الحرب الإلكترونية مع النصـف الثاني من القرن 19م، وتحديدا خلال الحرب الأهلية الأمريكية (1861–1865) عندما كان يُستخدم التلغراف كوسيلة اتصالات متطورة حينها، وكان يتم التصنت أيضا على الاتصالات اللاسلكية[1]. ومع ابتكار اللاسلكي جرى استخدامه في المعارك والحروب البرية والبحرية في الاتصالات والتصنت والتشويش على العدو، مثلما حدث بين روسيا القيصرية واليابان في معاركهما البحرية سنة 1904 و1905 على التوالي. وخلال الحرب العالمية الأولى أيضا تم الاعتماد على الاتصالات اللاسلكية في الاستطلاع وتبادل المعلومات حول العدو وأرض المعركة. ثم اكتُشف الرادار وأصبح تقنية متطورة في المجال العسكري حينها[2]. وتذكر الأبحاث المتخصصة أن أول عملية يمكن وصفها بالحرب الإلكترونية وقعت خلال المعركة المسماة "تسوشيما" (Tsushima) بين روسيا واليابان في 1905[3].

وكانت حرب الخليج الثانية محطة محورية في تحولات الحرب من حيث الأدوات والأساليب والتكتيكات التي تم اعتمادها بالنسبة للدول التي شكلت تحالف العدوان على العراق بعد غزوه الكويت في صيف 1990، فقد برزت ملامح جيل جديد من الأسلحة والحروب، وتم استخدام أنظمة الكمبيوتر في الاستخبارات وجمع المعلومات[4]، وبالتالي تغيير قواعد الاشتباك.

يوصف الفضاء السيبراني بكونه "الذراع الرابعة للجيوش الحديثة"[5]، أو المجال الخامس للحروب، ويمكن تعريف الحرب السيبرانية أو الإلكترونية بأنها "التطبيقات العسكرية للفضاء الإلكتروني"[6]. ومهما يكُن فقد تطورت الحروب الإلكترونية، ولم تعد حكرا على عوامل التشويش من خلال أجهزة الاتصالات والإنذار والرادارات، وإنما باتت أكثر توسعا وتعقيدا وتأثيرا من خلال الفضاء السيبراني الذي تحول إلى ساحة قتال جديدة بدون منازع، والمعلومات الموظفة في الصراعات السيبرانية تحتل مكانة محورية في مواجهة الطرف المعادي.

في حين أن طريقة التفكير هذه هي نتيجة طبيعية للاعتراف بالفضاء السيبراني كمجال آخر للحرب، إلا أنها تزيد أيضًا من عدد الخيارات لبدء العمليات في إطار عمل الدفاع الجماعي. من الضروري أن تضع

---

[1] سامر مؤيد عبد اللطيف، "الحرب في الفضاء الرقمي: رؤية مستقبلية"، ***مجلة رسالة الحقوق***، العدد 2 (2015)، ص: 81–82.

[2] فيصل محمد عبد الغفار، ***مرجع سابق***، ص–ص: 18–26.

[3] جاسم محمد البصيلي، ***الحرب الإلكترونية: أسسها وأثرها في الحروب*** (بيروت: المؤسسة العربية للدراسات والنشر، ط2، 1989)، ص41.

[4] سامر مؤيد عبد اللطيف، ***مرجع سابق***، ص: 84–85.

[5] ربيع محمد يحيى، ***مرجع سابق***، ص67.

[6] عادل عبد الصادق، مرجع سابق.

في اعتبارك أن الأنشطة التي تتم في الفضاء السيبراني، الإجراءات التقليدية. وهذا يعني أن الاستجابة التقليدية (الحركية) للعمليات السيبرانية هي وجهة نظر كل من الردع والدفاع[1].

أ- خصائص الحروب الإلكترونية:

الحرب الإلكترونية هي نوع من أنواع التهديدات الجديدة اللاتناظرية والهجينة، ومن خصـــائص التهديدات الجديدة للأمن أنها عابرة للحدود، ولا تقتصـر على الجانب العسـكري وإنما تتعداه، بالإضـافة إلى أن طبيعة الفواعل ليســت دولاتية بالضــرورة أو في مقام أول، كما أن تأثير التهديدات غير التقليدية يكون غير محدود، وتجب الإشـــارة إلى أن أول اســـتخدام لتعبير "التهديد الهجين" (Hybrid Threat) كان من خلال مقال صـــدر في عام 2005، للجنرال "جيمس ماتيس" (James Matis) "عن ظهور طرق غير منتظمة لتهديدات مثل الإرهاب وأعمال التمرد وتجارة المخدرات". ويعتمد هذا النمط على حرب المعلومات والوسـيلة الإعلامية، بالتالي فهو يشـير إلى "إسـتراتيجية عسـكرية تمزج بين مفاهيم الحرب التقليدية ومفاهيم الحرب غير النظامية والحرب الإلكترونية"[2].

وتعد الحرب الإلكترونية المستوى الأخير أو الأخطر من التهديدات السيبرانية، وما يجعلها كذلك هو خصـائصـها وأبعادها الإستراتيجية، والاستخدام المتزايد لتكنولوجيا الاتصـال في مجالات الحياة المختلفة وفي كل قطاعات الدولة. والجيل الخامس من الحروب قائم على عدم التكافؤ والتماثل في القوة والأدوات، في مقابل تغليب عنصـر الذكاء والاحترافية والتحكم في التكنولوجيا كمحور أسـاسـي (أي الجانب النوعي للقوة)، بالإضـــافة إلى أن الحســـم الإســـتراتيجي في هذا النوع من الحروب يكون بأقل التكاليف مقارنة بالحروب التقليدية والدمار الذي تخلّفه.

فلا حدود جغرافية في الحرب السيبرانية، وطبيعة العدو تختلف، إذ لا يكون دولة بالضـرورة وإنما قد يكون في صـورة جماعة لها نفس التوجه والهدف، بالإضـافة إلى مميزات أخرى ترتبط بقلة التكلفة وسـهولة العمل وغيرهما[3]. فمن الخصـائص الإستراتيجية للحرب الإلكترونية أنها تقع في الفضـاء غير المادي معتمدة على التطور التقني، وهي حرب لاتناظرية ولا تحتاج إلى تكلفة مادية كبيرة جدا لتنفيذ هجوم أو تشكيل تهديد لمصالح الدول المستهدفة. كما أن المهاجم يتفوق على المدافع من الناحية الإستراتيجية، خاصة وأن الفضاء السـيبراني يمنحه ميزات إضـافية تتمثل في المرونة والمراوغة، مما يجعل عملية الردع صـعبة في الغالب

[1] Wiesław Goździewicz, and others, "*NATO Road to Cybersecurity",* Joanna Świątkowska (Edit), The kosciuszko institute, 2016, p6, in :https://www.coursehero.com/file/70676850/NATO-Road-to-Cybersecuritypdf/

[2] عادل عبد الله بركة المطيري، ***مرجع سابق***، ص: 4346.

[3] SANS Institute, ***Op.Cit***, p-p : 7-8.

على عكس المجال التقليدي للحروب والمعارك، وكل ذلك يجعل الحرب السـيبرانية بمثابة "حرب هُلامية الشكل والملامح" ولكن قدراتها التدميرية عالية مقارنة بالحروب التقليدية[1].

وما يميز الحروب الجديدة في هذا الفضاء أنها غير محددة من حيث الإطار أو المجال أو الهدف، وإنما تتكيف باسـتمرار مع طبيعة السـلاح المسـتخدم إلكترونيا بما يواكب التطور التقني في هذا العصـر، بالإضافة إلى "الجاهزية الإلكترونية" وسهولة الانتشار والذكاء في الهجوم[2]. مع ضرورة التذكير بالاختلاف بين البيئة الإستراتيجية الإلكترونية والمادية، بالإضافة إلى أن الردع يظل نسبيا أو صعبا نظرا لأن المهاجم قد يكون مجهولا أو غامض الهوية.

وفي حالة الحرب السيبرانية فإن التمييز بين حالتي السلم والحرب يكون صعبا[3]، ذلك نتيجة التطور في مضـمون الحرب وأدواتها، وانتقالها من طبيعتها التقليدية القائمة على القوة العسـكرية إلى طابع جديد متأثر بالتطور التكنولوجي، فعرفت بذلك تحولا في الأدوات والتكتيكات لتنتقل إلى صـورة الحروب الهجينة (Hybrid Warfares) وامتزاج حالتي الحرب والسلم[4]. فالفضاء السيبيري هو ساحة جديدة للمعارك، "بما له من تأثير نفسـي ومعنوي وإعلامي ثم أصـبح له تأثير أمني وعسـكري، لتزحف جبهات القتال التقليدية بشكل مواز لها إلى ساحة الفضاء الإلكتروني"، ولكن يجب التمييز بين الحرب السيبرانية الباردة حيث يكون التركيز منصـبا على الحرب النفسـية والاختراق والتجسـس، والحرب الإلكترونية السـاخنة حيث يتم توظيف الأسلحة الإلكترونية بالموازاة مع حرب في الفضاء المادي التقليدي[5]. يضاف إلى ذلك أن خصوصية البيئة في الفضـاء الإلكتروني تجعله أكثر تهديدا، وفي هذا الشـأن يقول "ناي": "جغرافية الفضـاء السـيبراني أكثر قابلية للتغير من البيئات الأخرى. فمن الصـعب تحريك الجبال والمحيطات، ولكن يمكن تشـغيل وإيقاف تشغيل أجزاء الفضاء الإلكتروني بنقرة زر"[6].

ب-أدوات الحرب الإلكترونية وسباق التسلح في المجال السيبراني:

إن السياسة هي التي تحدد طبيعة الحرب إذا انطلقنا من مقولة "كلاوزفيتز" الشهيرة والتي مفادها أن الحرب امتداد للسياسة بطرق أخرى، وأنها تقع نتيجة أسباب سياسة[7].

---

[1] سامر مؤيد عبد اللطيف، ***مرجع سابق***، ص: 78-79.

[2] عادل عبد الصادق، ***مرجع سابق.***

[3] Andrew F.Krepinevich, ***Cyber Warfare : A Neclear Option ?***, Center for Strategic and Budgetary assessments, 2012, p.147.

[4] شادي عبد الوهاب منصور، ***حروب الجيل الخامس: أساليب التفجير من الداخل على الساحة الدولية، ط1،*** (د.ب.ن: العربي للنشر والتوزيع، 2019)، ص: 09-10.

[5] عادل عبد الصادق، ***مرجع سابق.***

[6] Joseph Nye, ***Op.cit,*** p.4.

[7] Christina M. Knopf, Eric J. Ziegelmayer, ***Op.cit***, 2012, p.6.

وتتنوع أدوات الحرب السيبرانية، بين التجسس الإلكتروني واستخدام الفيروسات والبرامج الضارة لإتلاف المعلومات، ويعتبر فيروس "ستوكسنت" أول سلاح سيبراني بالغ الخطورة، يستهدف بالتجسس والتدمير أنظمة التحكم الصناعية وقدرتها على تدمير الأهداف المادية غير محدودة، وكان الخبير الروسي في مجال أمن المعلومات، "اوجان كاسبرسكي" (Eugene Kaspersky)، قد أكد أن تطوير الأسلحة السيبرانية كفيل بتغيير العالم[1].

ويعد الإرهاب الإلكتروني وسيلة هامة وخطيرة في الصراع السياسي والحرب السيبرانية، فضلا عن كونه يسبب التفرقة والانقسام والتطرف في أوساط المجتمعات. وعسكريا، طرح هذا الشكل من الإرهاب تحديات جديدة للأمن الوطني خاصة مع غياب الحدود داخل الفضاء الإلكتروني، بما جعل الإرهابيين يستفيدون في الوصول إلى قواعد البيانات حساسة جدا واستهداف البنية التحتية للمعلومات مع إمكانية الإضرار بالاقتصاد الوطني، مما يجعل الفضاء السيبراني ساحة خطيرة للحرب والصراع[2].

وفي إطار الحروب الجديدة، كثّفت الولايات المتحدة الأمريكية مثلا من عملية التجسس الإلكتروني على إثر أحداث 11 سبتمبر 2001، وذلك بهدف اكتشاف المجموعات الإرهابية وخططها[3].

انطلاقا من ذلك، يمكن القول بأن امتلاك أدوات الحرب الإلكترونية والصراع السيبراني بات ضرورة حتمية في ظل التطور المستمر للحروب وانتشار التهديدات العابرة للحدود، بما فيها التهديدات السيبرانية. كما أن سباق التسلح حاضر في الفضاء غير المادي، خاصة بالنسبة للدول الكبرى التي تسعى إلى تأمين مجالها السيبراني باستمرار.

ج- هجمات الفضاء السيبراني ما بين توصيف الإرهاب ومدلول الحرب:

أصبح الإرهاب ظاهرة مميزة كونه يعكس اتجاهات أوسع في الحرب غير النظامية التي بدأت مع نهاية الحرب الباردة، ففي تلك الحالة لا يدور الصراع بين جيوش نظامية يمكن تطبيق اتفاقيات جنيف بخصوص الحرب عليها، وحتى لو أن للقوات النظامية دورا فإنه يقتصر على وضع الاستراتيجيات والخطط، وبذلك يصعب تحميل أي شخص مسؤوليتها، ويأتي التهديد من الجماعات والمنظمات وحتى من أفراد، ويمكن أن تنتشر حرب المعلومات بسرعة عالية، ويمكن أن يشنها شخص على اتصال بالإنترنت ويستطيع تتبع التعليمات البسيطة المعروضة أمامه على شاشة الكمبيوتر، وقد يؤدي منحى تزايد نقاط الضعف -مقرونا

[1] ربيع محمد يحيى، ***مرجع سابق***، ص: 72-77.

[2] علي إبراهيم مشجل المعموري، ***مرجع سابق***، ص: 168-172.

[3] سامر مؤيد عبد اللطيف، ***مرجع سابق***، ص92.

بمدى ملاءمة الهجوم وقدرته على حرمان الخصم من معلومات عن المهاجم– إلى اندلاع حرب المعلومات بمشاركة أفراد ومجتمعات وشركات ودول تحالفات.

كما أصبح مفهوم الهجوم يختلف عن شكله التقليدي، فقد يُستخدم جهاز لمهاجمة أجهزة أخرى، مع إمكانية إصابة الهدف بسهولة عن طريق هجوم الفضاء الالكتروني وخاصة إصابة مراكز القيادة والسيطرة الخاصة بالبنية التحتية الحرجة مثل محطات الطاقة، بالإضافة إلى أنظمة التسلح. وساعد انتشار تكنولوجيا المعلومات وعلاقتها المباشرة بالجوانب المدنية والعسكرية على اتساع ميدان الحرب لتمتد إلى حرب وهجمات متعددة الأبعاد، تشمل الأرض والبحر والمجال الجوي والفضاء الخارجي والإلكتروني.

ويتميز الإرهاب –سواء قامت به دول أم أفراد أم جماعات– بقدرته على التلون والتشكل وفق مقتضيات العصر، بما يتلاءم مع تحقيق الهدف من ورائه وجاء الانترنت وسيلة من الوسائل التكنولوجية الحديثة التي يمكن استخدامها وبكفاءة، وجاءت الجماعات بجميع أشكالها وأطيافها السياسية لتمارس هذا النوع من الإرهاب الجديد عبر الفضاء الالكتروني، إما ببث الكراهية الدينية والتحريض أو المساعدة في العمل الإرهابي التقليدي أو شن حرب الكترونية خالصة[1].

وفي هذا الصدد، تؤكد الكاتبة "إليزابيث برو" في مقال بصحيفة "تايمز" البريطانية على خطورة تلك الحرب الإلكترونية التي لا تقل بأي شكل عن الهجمات المسلحة، وطالبت بناءً على ذلك بوضع تعريف جديد للحرب قائلة:

> **"المخترق أو جندي المعلومات لا يعبر الحدود حاملا أسلحة، لكن زعزعة استقرار دولة أخرى من خلال الاختراق الإلكتروني هي مثل عدائية نشر قوات عسكرية على طول حدودها".**

ولأن المخترق أو جندي المعلومات لا يعبر الحدود حاملا أسلحة فهذا لا يسمى حربا أو عدوانا في حدوده المادية، فوفق التعريفات العسكرية الحالية فإن الحرب هي الصراع على الأراضي، لكن زعزعة استقرار دولة أخرى من خلال الاختراق الإلكتروني توازي نشر قوات عسكرية عدائية على طول حدودها.

تبعا لذلك يقول أستاذ الأمن الإلكتروني في جامعة آلتو في فنلندا "جارنو ليمنل" Jarno Limnéll: "في المستقبل فإن كل جانب في مجتمعاتنا سيكون تقريبا رقميا"، ويضيف: "سنحتاج إلى الحديث عن كيفية حماية الكابلات البحرية وغيرها من البنى التحتية، خاصة أنه سيكون هناك انفجار في المعلومات بالسنوات القادمة"، ولهذا يجب علينا وضع تعريف جديد للحرب يتماشى وترقية الفضاء الإلكتروني إلى المجال التشغيلي، مما يمنحه نفس أهمية الجو والبحر والبر[2].

---

[1] عادل صادق، ***استخدام الإرهاب الالكتروني في الصراع الدولي*** (القاهرة: دار الكتاب الحديث ،ط1، 2015)، ص99–102.

[2] إليزابيث برو، "الحرب الإلكترونية لا تقل خطورة عن الهجمات المسلحة" الجزيرة للدراسات، https://goo.gl/NnYnbb (2021/01/21)

المبحث الثاني: توظيف جماعات العنف للإرهاب السيبراني عبر الفضاء الأوربي.

إن فهم كيفية تشكيل المستقبل كمبدأ تنظيمي لإستراتيجية المنظمات الإرهابية ووضعها، يوضح أن المنظمات الإرهابية التي تفتقر إلى مثل هذا المفهوم ستفقد جاذبيتها بشكل أسرع من تلك التي تفعل ذلك[1]، لهذا عملت التنظيمات الإرهابية على هيكلة نفسها بما يتماشى وتغيرات التي فرضتها العولمة، فعلى الرغم من عدم تحديد مفهوم الإرهاب الإلكتروني بشكل قاطع، وعدم وجود حادثة يمكن تسميتها بـ: "الإرهاب السيبراني" في حد ذاتها، يمكننا التحدث عن إجماع فضفاض في إطار دراسات الإرهاب السيبراني على أن "الهجوم السيبراني" من قبل الكيانات الإرهابية يستتبع هجومًا حول البنية التحتية الحيوية[2].

ومن هذا المنطلقمن المهم أن نلاحظ أن أغلب التقارير المنشورة في الدراسات الأمنية الغربية تركز فقط على التطرف العنيف والإرهاب الإسلاميين ولا تفحص جميع أشكال ومجموعات التطرف العنيف الأخرى لهذا سنحاول التطرق للجماعات الإرهابية الأخرى المنتشرة عبر الفضاء السيبراني والناشطة أوروبيا.

ومن خلال هذا جاءت الأجندة الأمنية للدول الأوروبية تماشيا وحجم هذه التهديدات الناشئة.

المطلب الأول: الإرهاب الجهادي.

سرعان ما لجأت الجماعات الإرهابية إلى إطلاق مواقع الكترونية خاصة بها لبث ثقافتها الإرهابية، ولعل تنظيم "داعش" الارهابيأبرز تلك الجماعات في إصدار تلك المواقع والمنتديات لبث أفكاره المتطرفة، حيث امتلك العديد من مؤسسات الإنتاج المرئي، كما أن لديه مواقع متغيرة وتتبدل روابطها باستمرار لتلافي الملاحقة والإغلاق، تلك المواقع الافتراضية متوفرة بلغات عدة منها الانجليزية والفرنسية، ولعل أبرزها: موقع الخلافة الإسلامية، أنصار المجاهدين للإنتاج الإعلامي، شبكة الجهاد العالمي، مركز الفجر للإعلام، تمكن من خلالها التنظيم من بث أفكاره وايديولوجيته العنيفة[3].

---

[1] Florence Gaub, "HOW THE ISLAMIC STATE SEES THE FUTURE Why the end of times does not mean the end", 21 April 2021, in: How the Islamic State sees the future | European Union Institute for Security Studies (europa.eu)(09/02/2022).

[2] Christopher Baker-Beall, "Understanding the European Union's Perception of the Threat of Cyberterrorism: A Discursive Analysis",https://onlinelibrary.wiley.com/doi/10.1111/jcms.13300 (10/12/2021)

[3] سمير إبراهيم محمد، "دور الإرهاب الالكتروني في تقويض الأمن القومي دراسة حالة دول ثورات الربيع العربي"، ***مجلة كلية السياسة والاقتصاد***، العدد الرابع (أكتوبر 2019)، ص 89-114.

ليس من المبالغة أن نقول إن مواقع الشبكات الاجتماعية قد استخدمت من قبل الجماعات الإرهابية الإسلامية بطريقة تحول نموذجي،مكنت للإرهابيين من استخدام هذه المواقع للأغراض التالية:(الحصولعلى المعلومات، الهندسة الاجتماعية، الاتصال، الدعاية، استقبال المؤيدين، القيام بعمليات نفسية، وتنفيذ الهجمات الإلكترونية[1]).

كما لجأت هذه التنظيمات، خاصة تنظيم "داعش" الإرهابي، إلى الفضاء السيبراني وذلك للقيام بوظائف متعددة، منها تزويد أتباعهم بالمعلومات اللازمة، ونشر التطرف، وتجنيد العناصر المتعاطفة وتحويلهم لتنفيذ عمليات إرهابية، وجمع التبرعات من الداعمين للتنظيم، وأخيراً تنسيق العمليات الإرهابية[2].

وعلى الرغم من أن أهمية الدولة الإسلامية والقاعدة قد تضاءلت بشكل كبير اليوم، فإن الإجراءات والتقنيات المستخدمة من قبلهم، يمكن اعتبارها أمثلة على كيفية استخدام الجماعات الإرهابية المستقبلية لمواقع التواصل الاجتماعي[3]، كما ان الجهاديين والأشخاص المرتبطين أو المتعاطفين مع هذين التنظيمان الارهابيانلا يمثلون التهديد الوحيد المحتمل للإرهاب الإلكتروني. لكن لم تُظهر أي جماعة إرهابية قدرًا كبيرًا من القدرة أو الاهتمام باستخدام الفضاء الإلكتروني للتحريض على الإرهاب في أوربا أكثر منهما، فالتنظيمان يستخدمان الفضاء الإلكتروني لنشر رسائلهم والانخراط في أنشطة أخرى تدعم أهدافهم العامة[4].

هذا لا يعني أن الفضاء الإلكتروني كان خاليًا من التهديدات الخطيرة. على العكس من ذلك، أظهر العقد الماضي مدى تعرضه للخطر وكيف يمكن أن تكون الهجمات مدمرة. لكن الأحداث التي تمت حتى الآن توصف بشكل مناسب بأنها جرائم إلكترونية أو تجسس أو احتجاج أكثر من وصفها بأنها إرهاب إلكتروني[5].

تستخدم المنظمات الجهادية مواقع الويب المحمية بكلمة مرور ومجموعات الدردشة عبر الإنترنت ذات الوصول المقيد للتجنيد السري، حيث يوفر الوصول إلى الإنترنت للمنظمات الإرهابية والمتعاطفين معها مجموعة عالمية من المجندين المحتملين، فالمنتديات الإلكترونية ذات الوصول المقيد توفر مكانًا لتبادل الملاحظات وصقل الاستراتيجيات والتكتيكات، كما أدى استخدام الحواجز التكنولوجية للوصول إلى منصات التوظيف إلى

---

[1] Péter Bányász, Social media and Terrorism, ***AARMS***, Vol. 17, No. 3 (2018) 47–62.

[2] شادي عبد الوهاب، الإرهاب عن بعد:نمط تنظيمي جديد لاستهداف الدول الغربية والآسيوي، **اتجاهات الأحداث: مركز المستقبل للأبحاث والدراسات المتقدمة**، العدد 24، نوفمبر 2017، ص 50-53.

[3] Péter Bányász, ***Op.cit.***p-p 47–62.

[4] Lorraine Bowman Grieve,"Cyber-terrorism and Moral Panics: A Reflection on the Discourse of Cyber-terrorism. In L. Jarvis, S. MacDonald & T. Chen (Eds), Terrorism Online: Politics, Law and Technology. Oxon: Routledge. (2015), in: https://cutt.us/pIYML

[5] Lorraine Bowman-Grieve, ***Op.Cit.***

زيادة تعقيد تتبع النشاط المرتبط بالإرهاب،كما يستخدم الإرهابيون الإنترنت لمشاركة أدلة التدريب العملي في شكل كتيبات على الإنترنت ومقاطع صوتية ومرئية ومعلومات ونصائح مستغلين الدعاية الإرهابية للتأثير على الفئات الضعيفة والمهمشة في المجتمع، عبر توفيرهم منصات وتعليمات مفصلة بصيغة وسائط متعددة يسهل الوصول إليها وبلغات متعددة(تعليمات حول كيفية الانضمام إلى المنظمات الإرهابية؛ كيفية صنع المتفجرات أو الأسلحة النارية أو غيرها من الأسلحة أو المواد الخطرة؛ وكيفية تخطيط وتنفيذ الهجمات الإرهابية، تعمل المنصات كمعسكرات تدريب افتراضية وتوفر أساليب أو تقنيات أو معرفة تشغيلية محددة لغرض ارتكاب عمل إرهابي).[1]

- **الإرهاب عن بعد: نمط تنظيمي جديد لاستهداف الدول الأوربية.**

شهد عدد من الدول الأوربية ظاهرة أطلق عليها" الإرهاب **الموجه عن بعد**"، وهو نمط من الإرهاب ابتدعه تنظيم "داعش" الارهابي لاستهداف هذه الدول، من خلال قيام أحد أعضاء التنظيم بتجنيد وتوجيه المتعاطفين عبر المجال السيبراني لتنفيذ عمليات إرهابية داخل هذه الدول، فالتحقيقات المتعلقة بالعمليات الإرهابية التي قام بها "داعش" في عدد من الدول الأوربية كشفت أن عدداً من العمليات التي نظر إليها في البداية على أنها تندرج ضمن "**إرهاب الذئاب المنفردة**" اتضح أنها –بعد مزيد من التحقيقات– تمت بتوجيه وإرشاد كامل من قبل عناصر تنظيم "داعش" الارهابي في سوريا والعراق[2].

وحيث يمكن للإنترنت أن تنقل المجاهد المحتمل المعزول إلى الجهاد العالمي، قد يبدأ الاتصال بين الأشخاص على مواقع الشبكات الاجتماعية أو الإنترنت المظلم Dark web كموطن للمعلومات والاتصالات الجهادية غير المشروعة، وفي سياق متصل تسمح مواقع الويب الجهادية للشباب المنعزلين بالانخراط مع شبكة عالمية من الأشخاص المتشابهين في التفكير الذين يناضلون ضد ما يعتبرونه عدوًا مشتركًا وبوحدة هدف واحدة.

بالإضافة إلى الاتصالات المشفرة، تستضيف المواقع الإلكترونية التابعة للقاعدة كتيبات تدريب الإرهابيين وتعليمات صنع القنابل ، وشارك المتعاطفون مع التنظيم في "رفض الخدمة" وهجمات تشويه الويب web-defacement attacks*. في حين أن غرضها العلني يشمل التنظيم والتواصل والتجنيد، فإن هذه

[1] TughralYamin, "Combating Cyber Terrorism through an Effective System of Cyber Security Cooperation", Terrorism Expert Conference, Ankara; October 2015,in: https://cutt.us/oKGxX

[2] شادي عبد الوهاب، الإرهاب عن بعد:نمط تنظيمي جديد لاستهداف الدول الغربية والآسيوي، **مرجع سابق**، ص 50-53.

* تشويه الويب هو هجوم يقوم فيه الفاعلون السيئون بحذف أو تعديل المحتوى على الموقع، واستبداله برسائلهم الخاصة.

الأنشطة لا قد تتوافق مع تعريف الإرهاب الإلكتروني على أنه "إرهاب السكان" لتحقيق أهداف اجتماعية وسياسية. في الواقع ، قد يكون هؤلاء الجهاديون السيبرانيون منخرطين في أنشطة بوساطة الكمبيوتر والتي يمكن وصفها على أفضل وجه بأنها "القرصنة"[1].

- **أبعاد الإرهاب الموجه:**

ذكرت الأدبيات المعنية بدراسة الإرهاب ظاهرة "الإرهاب الموجه عن بعد" منذ أواخر عام 2016، وأشار إليها باستخدام مصطلحات متعددة أبرزها "العمليات الإرهابية عن بعد Terror Plots from Afar، أو "التخطيط الافتراضي Virtual Planners، بينما أشارت السلطات الأمنية الفرنسية والألمانية إلى هذا النمط الجديد من العمليات الإرهابية باستخدام مصطلح " المؤامرات الإرهابية الموجهة عن بعد Plots Remote Controlled "، إذ كشف تحليل حديث لحوالي 38 عملية إرهابية تبناها تنظيم "داعش" الارهابي، ووقعت في الفترة بين عام 2014 وأكتوبر 2016، أن حوالي 19 عملية منها تضمنت توجيهات من تنظيم "داعش" الإرهابي عبر الفضاء السيبراني. وقد كان أحد أبرز الأمثلة في هذا السياق العملية التي تمت في ربيع عام 2015عندما قام طالب في تكنولوجيا المعلومات يسمى "سيد أحمد غام" بإطاق النار على كنيسة في باريس بعد أن تلقى توجيهات من قبل أحد عناصر تنظيم "داعش" الارهابيعبر الإنترنت، ويمكن تعريف "الإرهاب الموجه عن بعد" بأنه "تلك الهجمات التي لم يسبق لمنفذيها أن سافروا إلى مناطق الصراعات، أو انضموا إلى تنظيم إرهابي، ولكنهم مع ذلك، كانوا على تواصل دائم مع عناصر الجماعات الإرهابية من خال استخدام منصات وسائل الاتصال المشفرة، وذلك لتوفير الدعم والنصيحة للمهاجم في كل مرحلة من مراحل الإعداد للعملية الإرهابية"، كما لوحظ أنه في بعض الحالات تم توفير الدعم المالي للقيام بعملية إرهابية، بل وفي انتقاء المناطق التي سيتم استهدافها[2].

وفي ضوء التعريف السابق، يمكن القول إن الإرهاب الموجه عن بعد هو شكل هجين لنمطين سابقين من الإرهاب في الدول الغربية، وهما الإرهاب الشبكي وإرهاب الذئاب المنفردة. فهو يتشابه مع الأشكال الشبكية من الإرهاب في وجود بعض الصلات بين منفذي الهجوم الإرهابي والتنظيم الإرهابي، غير أنه يختلف عنها

[1] Aziz Douai, Technology and terrorism: Media symbiosis and the "darkside"of the web, in: Lorenzo Cantoni and James A. Danowski, ***Communication and Technology***, (Switzerland: De Gruyter Mouton, 2015), p :450.

[2] شادي عبد الوهاب، **مرجع سابق**، ص 50.

في محور واحد، وهو أن هذه الصلات ليست تنظيمية، بل افتراضية، أي أن العنصر الإرهابي تم توجيهه من خال الفضاء السيبراني.[1]

قد تسيءالجماعات الجهادية استخدام عناصر الفضاء الإلكتروني وهذا من خلال:

1- التأثير السيبرانيCyber Influence:

إساءة استخدام الفضاء السيبراني للتأثير على السكان من خلال الدعاية، قد يكون هذا لخلق متعاطفين مع قضيتهم، وتشمل هذه الفئة عملية التطرف والتجنيد عبر المجال السيبراني.

2- التخطيط السيبراني Cyber Planning:

صاغ تيموثي توماس Timothy Thomas مصطلح التخطيط السيبراني على أنه "تنسيق رقمي لخطة متكاملة تمتد عبر الحدود الجغرافية والتي قد تؤدي إلى إراقة الدماء"، يتضمن تعريف توماس في عمله أمثلة على كل من تأثير وتنفيذ الهجوم، حيث يمكن للمرء أن يجادل بأن التجنيد والقيادة والسيطرة على عملية ما عبر الفضاء الإلكتروني لا يرقى إلى مستوى التخطيط، بل هو أقرب هنا إلى الاستخبارات والمراقبة والاستطلاع.

3- التنفيذ التشغيلي Operational Execution:

يمكن اعتباره إساءة استخدام الفضاء الإلكتروني بغرض إحداث تدمير مادي، وهذا يتجاوز نطاق الافتراض عندما يتعلق الأمر بتفكيك الأجهزة المتفجرة المرتجلة عبر التقنيات الخلوية، وما لم يتم ملاحظته بعد هو قدرة الإرهابيين على مهاجمة أنظمة التحكم الصناعية بالوسائل الإلكترونية لإحداث آثار مادية[2].

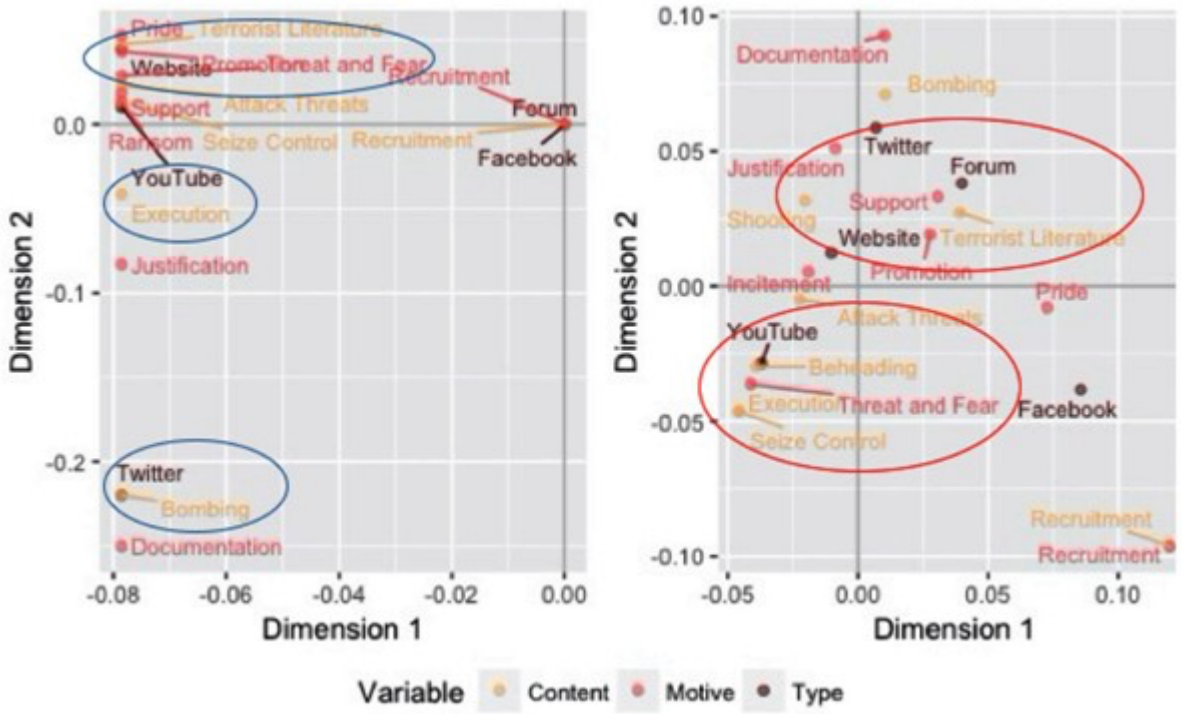
يستخدم الإرهابيين والمنظمات الإرهابية الأنترنت لنشر وإدارة دعايتهم من خلال حرب المعلومات، لنقل أيديولوجيتهم، وشن حرب نفسية بالإضافة إلى التطرف وتجنيد أعضاء جدد من جميع أنحاء العالم، من خلال مواقع الويب الإرهابية والمجلات على الإنترنت، ومنصات الوسائط المتعددة المتنوعة (مثل Facebook، و Twitter، و Instagram ، و Tumblr ، و VKontakte ، و justPaste.it، و youtube ، وما إلى ذلك). على سبيل المثال، كان لدى تنظيم "داعش" الارهابي سبع وكالات إعلامية تحت قيادتها المركزية لوسائل الإعلام (Amaq هي الأبرز)، و 37 مكتبًا إعلاميًا يعمل في بلدان مختلفة. وبالمثل، شكلت القاعدة ذراعًا

[1] شادي عبد الوهاب، ***المرجع نفسه*** ، ص 50.

[2]Panayotis A. Yannakogeorgos, Rethinking the Threat of Cyberterrorism, in Thomas M. Chen Lee Jarvis Stuart Macdonald Editors, Cyberterrorism Understanding, Assessment, and Response, Springer New York ,2014, p 46.

إعلاميًا عُرف باسم السحاب وجبهة الإعلام الإسلامي العالمي (GIMF)، بالإضافة إلى مجلات على الإنترنت مثل "إلهام وانبعاث" لتعزيز دعايتها. بالإضافة إلى ذلك، تستخدم المنظمات الإرهابية تطبيق Telegram منذ نهاية عام 2015 بسبب التشفير والاستخدام الآمن، وبسبب الإغلاق المتزايد للحسابات الإرهابية على Facebook و Twitter. في أغسطس 2016، على سبيل المثال، نشرت مؤسسة إعلامية جهادية، تطلق على نفسها اسم "الصمود" دعماً لدعاية لتنظيم داعش" الإرهابي على قناة " Omar – Orlando Channel Mateen" على تلغرام تضمنت منشورات تشجع المسلمين في أوروبا على شن هجمات منفردة من خلال السماح للزوار بتنزيل برنامج كمبيوتر يسمى pro2، وهو برنامج أظهر مرونته في الحفاظ على التوزيع المستمر للدعاية الخاصة به وقدرته على التكيف مع إزالة المحتوى الجهادي عبر الإنترنت الذي فرضته مؤسسات انفاذ القانون الأوروبية[1]. والشكل التالي يبرز نوع ومحتوى ودافع الدعاية من قبل أشهر تنظيمين للجهاد الاسلامي: القاعدة، و تنظيم "داعش" الإرهابي.

الشكل (3). نوع ومحتوى ودافع الدعاية من قبل القاعدة (على اليسار) وتنظيم "داعش" الإرهابي (على اليمين).



Source :Choi, Lee, and Cardigan, Spreading Propaganda in Cyberspace: Comparing Cyber Resource Usage of Al Qaeda and ISIS, ***International Journal of Cybersecurity Intelligence and Cybercrime***, Vol. 1, Issue. 1, 2018, p. 21-39.

[1] Mayssa Zerzri, ***The Threat of Cyber Terrorism and Recommendations for Countermeasures***, Policy Advice and Strategy Development, Center for Applied Policy Research 04.2017, p. 2

تظهر دعاية القاعدة وتنظيم "داعش" الارهابي خصائص مختلفة حسب النوع والمحتوى والدافع. استخدم تنظيم القاعدة موقع تويتر لنشر حالات التفجير، بينما استخدم موقع يوتيوب بشكل أساسي لنشر رسائل دعائية تتعلق بعمليات الإعدام، في حين تم نشر العمليات الإرهابية والترويج لها عبر مواقع الإنترنت من قبل مجموعات القاعدة، كما استخدم تنظيم "داعش" الارهابي تويتر والمنتديات على الإنترنت والمواقع الإلكترونية لدعم وتعزيز أيديولوجياتهم. في حين تم استخدام تويتر والمنتديات عبر الإنترنت لإظهار التفجيرات وتبرير أعمال تنظيم "داعش" الإرهابية.

نخلص الى أن القاعدة استخدمت الانترنت للترويج لأيديولوجياتها الإرهابية. في المقابل، ركز تنظيم "داعش" الارهابي على الأعمال الإرهابية الدرامية عبر جل المنصات الإلكترونية لخلق الخوف وتبرير أفعالهم في المقام الأول[1].

في فترات سابقة راجت المواقع الجهادية بامتداداتها الأوربية، واحد من أكبر المواقع المرتبطة بالجهاد هو موقع "عزام دوت كوم" الموقع تديره منشورات عزام ومقرها لندن، متاح بأكثر من اثنتي عشرة لغة ويقدم كتابات تمهيدية بما في ذلك "كيف يمكنني تدريب نفسي على الجهاد؟"، بعد تتبع الموقع تم إغلاق عدد من الشركات التابعة لعزام بعد أن اشتكى الأشخاص إلى مزودي خدمة الإنترنت الذين يستضيفون المواقع[2].

يعكس هذا سياسة تنظيم "داعش" الارهابي الإلكترونية التي اعتمدت على الدفع بمعلومات هائلة من حيث الإنتاج والمحتوى، من أجل استدراج الفئات الشبابية في أوروبا، خاصة أولئك الذيم لديهم فهم سطحي للإسلام (المسلمين حديثا)، والعمل على جذب شريحة كبيرة من المتعاطفين معهم داخل الدول الاوروبية، وحثهم على الجهاد لقيام دولة الخلافة المزعومة، من خلال نشر التنظيم لمغالطات تؤجج لديهم رؤية مزيفة عن تعاليم الدين الاسلامي في الفضاء الإلكتروني[3].

في سياق متصل، وفي دراسة للباحثة مها عبد المجيد صلاح أجرتها سنة 2014، بعنوان: استراتيجيات الاتصال في مواقع الجماعات الإرهابية على شبكة الإنترنيت، بحثت فيها إشكالية توظيف

---

[1] Choi, Lee, and Cardigan, Spreading Propaganda in Cyberspace: Comparing Cyber Resource Usage of Al Qaeda and ISIS, International Journal of Cybersecurity Intelligence and Cybercrime, Vol. 1, Issue. 1, 2018, p. 21-39. in: https://vc.bridgew.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1000&context=ijcic(06/07/2021).

[1]Maura Conway, Op.cit.

[3]إبراهيم بولمكاحل، **مرجع سابق**، ص 158.

المنظمات الإرهابية للمزايا والإمكانات التي يوفرها تطور تكنولوجيا الاتصال في دعم الأنشطة الإرهابية، ونشر ثقافة العنف والإرهاب، وكشفت أن البنية الاتصالية التي تعتمد عليها الجماعات الإرهابية تستفيد من الإنترنت في تحولها إلى النمط اللامركزي في تبادل المعلومات، والاعتماد على شبكة اتصال مفتوحة، ومعقدة التركيب، ما يرفع من درجة تعقيد العمليات الإرهابية وتخطيطها.

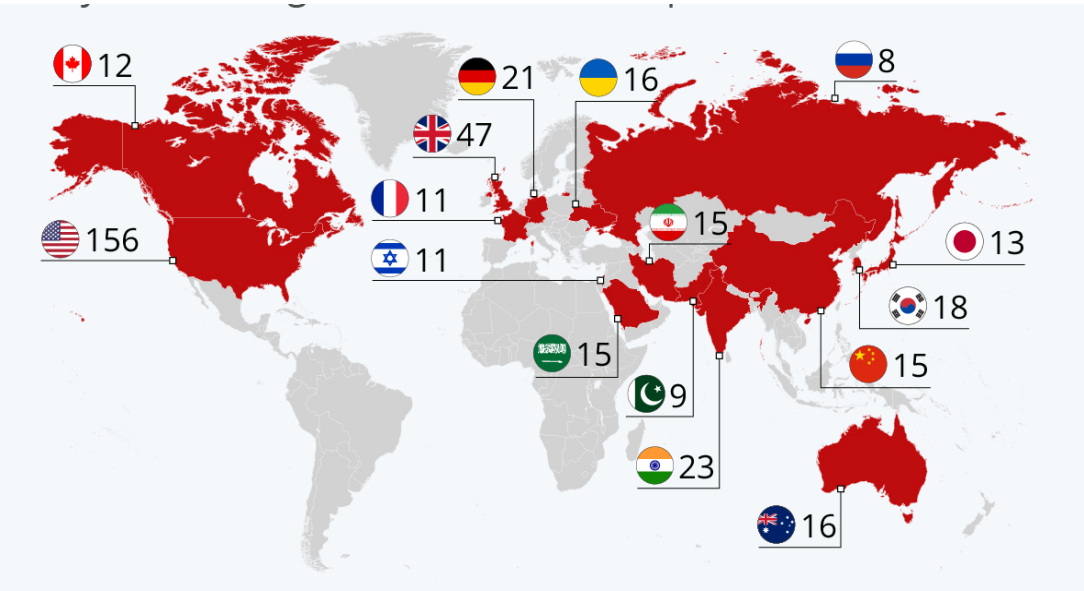
يأتي كل هذا في سياق ما يعرف إعلاميا بـ صناعة الصورة، بحيث يسعى تنظيم "داعش" الارهابي عبر مختلف الأدوات الإعلامية المتاحة لإنشاء فضاء جهادي إلكتروني متطور واسع الانتشار، للتأثير في محيطه وفي كل المناطق والفئات المستهدفة في العالم، مستغلا الأدوات التكنولوجية المتاحة في الفضاء السيبراني، وذلك عبر النشر المكثف والمنظم للمعلومات والأفكار بين أنصار التنظيم الحاليين والمحتملين، ومواجهة الدعاية السلبية التي تروج لها في أوروبا (العدو في نظر تنظيم "داعش" الارهابي)، والعمل على خلق صورة جذابة لشكل الحياة اليومية في أقاليم الدولة الإسلامية، بالإضافة إلى نشر الأفكار التي تستخدم في الدعاية، كتعظيم الرغبة في الشهادة والاحتفاء بها، وتتوافر معظم هذه المادة الإعلامية باللغتين العربية والإنجليزية، وكثير منها متوافر بلغات أخرى كالروسية، إضافة إلى ذلك، يسعى التنظيم إلى نشر الخوف بين أعدائه ومعارضيه بنشر الفيديوهات شديدة الوحشية كالفيديو الخاص بحرق الطيار الأردني معاذ الكساسبة حيا[1].

يعكس هذا تطور المنظمات الإرهابية من هيكلها الهرمي إلى الشبكات الأقل مركزية القائمة على الخلايا، هذا النهج غير المتبلور يحمي الأعضاء بشكل أكثر فعالية من الكشف ويحمي المنظمة ككل، وأصبح مقبولًا بسبب التقدم في تكنولوجيا الاتصالات وطبيعة الإنترنت اللامحدودة وما صاحبها من هجمات إلكترونية مستغلة هذه السيولة والهشاشة الأمنية[2]، وفيما يلي بعض تجليات ذلك تعكسها الخريطة أسفله.

[1] إبراهيم بولمكاحل، ***مرجع سابق***، ص 161.

[2] Marjie T Britz, "Terrorism and technology: Operationalizing cyberterrorism and identifying concepts." ***Crime on-line: Correlates, causes, and context***, Carolina Academic Press, (2010), p. 193-220.

الخريطة رقم (1): الدول الأكثر تضررا من الهجمات الإلكترونية للتنظيمات الارهابية بين 2006- 2020



Source : Tristan Gaudiaut, Les pays les plus touchés par des cyberattaques massives, Specops Software, 14 janv. 2022, Available on : https://cutt.us/vM7S7

تكشف البيانات التي نشرتها شركة Specops Software عن البلدان الأكثر تضررًا من الهجمات الإلكترونية الكبرى على مدار العقدين الماضيين، تركز الدراسة بشكل أكثر تحديدًا على الفترة 2006-2020 وتحدد هجمات الكمبيوتر التي تستهدف الحكومات وكذلك شركات التكنولوجيا والدفاع التي تسببت في خسائر تزيد عن 870.000 يورو، كما تبرز الولايات المتحدة كونها الدولة الأكثر استهدافًا إلى حد بعيد، حيث تم توثيق 156 هجومًا إلكترونيًا من هذا القبيل، وهذا يمثل 11 هجومًا كبيرًا في المتوسط سنويًا، وهو نفس الرقم الذي سجلته فرنسا خلال خمسة عشر عامًا، و من بين الأهداف التي يتم استهدافها في أغلب الأحيان المملكة المتحدة 47 هجوما، وألمانيا 21 هجوما، ومع تعرض 11 هجومًا إلكترونيًا رئيسيًا منذ عام 2006 تعد فرنسا واحدة من أكثر 15 دولة تضررًا [1].

وفي عام 2020 لوحده عانت ثلاث دول أعضاء في الاتحاد الأوروبي (النمسا وفرنسا وألمانيا) من 10 هجمات جهادية. أسفرت الهجمات المكتملة في الاتحاد الأوروبي عن مقتل 12 شخصًا وإصابة أكثر من 47 آخرين، تم تسهيل الكثير من اتصالاتهم في المراحل النهائية من التخطيط للعمليات الإرهابية من خلال غرف الدردشة عبر الإنترنت، وتم إحباط أربع مؤامرات جهادية بنجاح في بلجيكا وفرنسا وألمانيا[2]. قيمت الدول الأعضاء في الاتحاد الأوروبي أن الإرهاب الجهادي لا يزال يمثل أكبر تهديد إرهابي في الاتحاد الأوروبي،

[1] Tristan Gaudiaut, Les pays les plus touchés par des cyberattaques massives, Specops Software, 14 janv. 2022, Available on : https://cutt.us/vM7S7 (15/01/2022).
[2] Europol (2021), European Union Terrorism Situation and Trend Report (TE-SAT), Publications Office of the European Union, Luxembourg, P17

وفي المملكة المتحدة تم تنفيذ ثلاث هجمات إرهابية جهادية مكتملة، تم إحباط مخططين جهاديين، في حين تعرضت سويسرا لهجومين لعب فيهما الدافع الجهادي دورًا كبيرا، وهذا يعني أن عدد الهجمات الجهادية المكتملة في أوروبا (الاتحاد الأوروبي وسويسرا والمملكة المتحدة) في عام 2020 أكثر من ضعف ما كان عليه في عام 2019 في الاتحاد الأوروبي، وبين عامي 2018 و2019 تم إحباط ثلثي الهجمات الإرهابية الجهادية في أوروبا قبل تنفيذها. هذا وبلغ عدد العمليات الإرهابية المكتملة للجهاديين في عام 2020 أكثر من ضعف المخططات التي تم إحباطها (10 إلى 4).

كما أعلن تنظيم الدولة الإسلامية مسؤوليته عن هجوم فيينا، ونشر موقع "أعماق" الإخباري التابع له مقطع فيديو للمهاجم يبايع زعيم تنظيم الدولة الإسلامية، واستغل أنصار التنظيم لقطات للهجوم نشرها شهود عيان على مواقع التواصل الاجتماعي لإنتاج ملصقات ومقاطع فيديو ومنشورات تشيد بالهجوم، كما نشرت النشرة الإخبارية الأسبوعية لـ "النبأ" التابعة لتنظيم الدولة الإسلامية مقالاً عن الهجوم، بعدها أمرت السلطات النمساوية بإغلاق مسجدين اعتقد أنهما ينشران خطاب متطرف ألهم المهاجم. وقعت هجمات سبتمبر في باريس وكونفلانس سانت أونورين Conflans-Sainte-Honorinee، ونيس على خلفية التعبئة الضخمة المناهضة للفرنسيين بعد إعادة نشر تشارلي إيبدو Charlie Hebdo للرسوم الكاريكاتورية التي تسيئ للنبي محمد ﷺ، والتي تم استخدامها لتبرير الهجوم على الصحيفة في عام 2015.[1]

في عام 2007، كان تسولي مسؤولاً عن إنشاء شبكة دعم افتراضية عالمية للإرهابيين في البوسنة، والدنمارك، وتحقيقا لهذه الغاية، استخدم تسولي منتدى الإنترنت الإرهابي، منتدى الأنصار، من أجل[2]:

1. نشر الرعب الناجم عن قطع الرؤوس المتنوعة المسجلة بالفيديو.
2. تبني المسؤولية عن هجمات متنوعة.
3. الترويج لإيديولوجيات زعيم القاعدة أبو مصعب الزرقاوي.
4. توفير آلية آمنة للاتصال عبر الإنترنت بين العملاء؛
5. نشر أشرطة فيديو للتدريب.

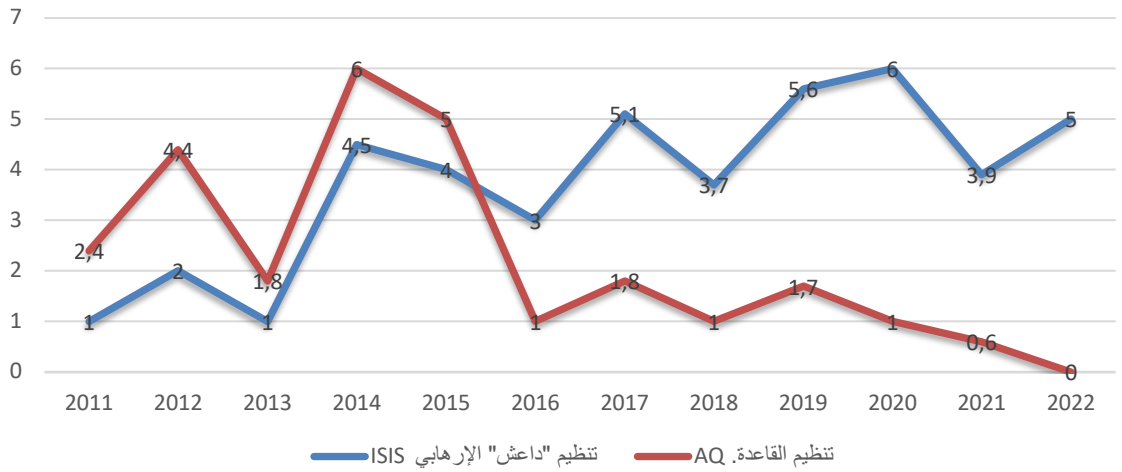
[1] Europol (2021), ***Op.cit.*** p 46.

[2] Marjie T Britz, ***Op.cit.***

في مدريد سنة 2020، تم إلقاء القبض على شخص مغربي كان يعمل مدرّسا وإماما، انخرط في النشاط الإرهابي لتنظيم "داعش" عن طريق الانترنت وكان عنصرا نشيطا على الشبكة العنكبوتية، ويذكر أنه ساعد أحد الأفراد من المقاتلين الأجانب للعودة من سوريا[1].

توضح كل هذه الأحداث قوة الإنترنت إذا ما استخدمت كآلية أو كهدف للجماعات الإرهابية، مستغلين الطبيعة اللامركزية وغير الخاضعة للرقابة أو الحدود، مما يخلق مجتمعًا من الجهاديين الراديكاليين/ والشكل أسفله يبين النشاط الإرهابي للقاعدة وتنظيم "داعش" الإرهابي على المستوى الأوربي خلال آخر عشر سنوات، لاختبار صدقية ما تم طرحه سابقا.

الشكل (4). الأنشطة الإرهابية السيبرانية لكل من القاعدة وتنظيم "داعش" الارهابي



المصدر: من إعداد الباحث.

يبين الشكل أعلاه استخدامات القاعدة و تنظيم "داعش" الإرهابي لموارد سيبرانية مختلفة وأنماط نشاط تتعلق بالإرهاب في الفضاء السيبراني على المستوى الأوربي بناء على عدة قراءات للأحداث والهجمات، في مدة زمنية تبدأ من 2011 الى غاية 2022، كما يشير إلى الانتشار المتسارع للإرهاب الإلكتروني من قبل القاعدة من عام 2011 إلى عام 2015 ليبدأ بالتراجع بعد ذلك، فيما تركزت معظم أنشطة الإرهاب السيبراني من قبل تنظيم "داعش" الارهابي بشكل كبير منذ عام 2013، حيث أصبح تنظيم "داعش" الارهابي نشطًا في الغالب من 2014. خاصة مع زيادة جاذبية الانضمام كمنظمة إرهابية متزايدة الفعالية وبعيدة المدى من قبل

[1] ***ibid***, P.21.P.50.

الفئات الشبانية في أوروبا، كما أدت النجاحات الكبيرة التي حققها تنظيم "داعش" الارهابي إلى زيادة التواجد عبر منصات وسائل التواصل الاجتماعي.

- الإرهاب الجهادي في ظل جائحة كورونا:

في ظل الجائحة، بات التفاعل والتواصل مقتصرا على الانترنت ووسائط التواصل الاجتماعي، وقد لوحظ في لوكسمبورغ اهتمام الجماعات الجهادية المتطرفة باستخدام تطبيقات مثل "زوم" Zoom، في هذا السياق ذكرت رومانيا أن الانترنت هي الفضاء المركزي لنشر التطرف في ظل الجائحة[1]، مؤكدين على صعوبة تتبع المحتوى المتطرف والإرهابي[2].

في نفس السياق كشفت تقارير عن أن تنظيم "داعش" الإرهابي قد عاد إلى النشاط والدعاية عبر الانترنت، في أعقاب جائحة كوفيد 19، مستغلا انشغال الحكومات الأوروبية في مواجهة الجائحة، ومعتمدا على منصات شهيرة أبرزها فيسبوك، ومن بين المنصات الجديدة للتنظيم منصة "الذئاب المنفردة" التي أوصت باستخدام التسميم والصعق الكهربائي والمناطيد والبالونات الحارقة، كما تم استغلال تطبيق "تام تام Tam) " (Tam الروسي وبعض التطبيقات الأخرى "الآمنة" والتي توفر حماية من الرقابة الحكومية[3]، كما عمل إرهابيو تنظيم "داعش" الإرهابي على عودة نشاطهم عبر الانترنت على نفس التطبيق بعد أن تم إزالة محتواهم المتطرف على تلغرام في نوفمبر 2019[4]، كما يستغل الارهابيون تطبيقات نظام المراسلة المشفرة (مثل Kik و SuperSpot و Wickr و Whats app و Gajim) وغرف دردشة الألعاب عبر الإنترنت ورسائل مشتركة أو إخفاء المعلومات للمناقشات السرية، أغراض الاتصالات المباشرة والخاصة[5].

---

[1] Choi, Lee, and Cardigan, ***Op.cit.*** P.21.P.55.

[2] ***ibid***, P.21. P.57.

[3] جاسم محمد، ***الإرهاب والتطرف في أوروبا من الداخل تهديدات الجماعات الجهادية، الإسلام السياسي اليمين المتطرف، إيران وتركيا.*** ط1،(القاهرة: المكتب العربي للمعارف، 2021) ، ص 60-62.

[4] Choi, Lee, and Cardigan***, Op.cit.***p17.

[5] MayssaZerzri, ***Op. cit***. p 3.

المطلب الثاني: الإرهاب العرقي القومي والانفصالي.

طغى على الإرهاب القومي العرقي والانفصالي*وصف "الإرهاب ذو القضية الواحدة "**يوفر أيضًا مصدرًا مهمًا للعنف السياسي اليوم. هناك أيضًا احتمال أن تتنامى الأصوات المنادية بالانفصال في المستقبل القريب، ومنه يمكن أن توفر هذا التصعيد سبيلًا للأيديولوجيات المتطرفة وتهيئ الظروف للإرهاب، ففي إسبانيا على سبيل المثال، حيث تمكنت جماعة الباسك الانفصالية الضعيفة "إيتا" تواصل حملة طويلة وعنيفة ضد الحكومة الإسبانية[1]، لا يمكن الجزم بأن هذه النزعات الانفصالية قد تتطور لتكون ظاهرة إرهابية، لكن قد يستغل الانفصاليون والمتمردون الإنترنت كسلاح أكثر نشاطًا مما يمكّنهم من تضخيم التأثير الرمزي لمطالبهم التي قد تأخذ طابع العنف، التطرف، أو الإرهاب.

من الواضح، إذا كان "مجال المعلومات" هو بالفعل "مساحة غير خاضعة للحكم"، فهو مكان حيث يكون المتمرد عازمًا على القتال والفوز في "ساحة المعركة". كتب ستيفن ميتزSteven Metz "تمرد القرن العشرين"، "سعى إلى إخراج الدولة من الفضاء الذي تسيطر عليه (عادةً الأراضي المادية) إلى التمرد المعاصر هو تنافس على المساحات الخارجة عن السيطرة ".

ولأن الارهاب والتمرد Insurgency متمايزان في هذه النقطة وفي كثير من النواحي الوظيفية، الا أنهما يرتبطان بالتطرف الأيديولوجي والسياسي، كما أن الكثير مما يمكن قوله عن الإرهاب السيبراني يمكن أن يقال أيضًا عن التمرد السيبراني، فالترابط وتكنولوجيا المعلومات هي جوانب جديدة لهذه الموجة المعاصرة من حركات التمرد التي تستخدم الإنترنت، ويمكن للمتمردين الآن الارتباط فعليًا مع الجماعات المتحالفة في جميع أنحاء العالم، وغالبًا ما ينضم المتمردون إلى منظمات فضفاضة ذات أهداف مشتركة ولكن بدوافع سياسية

---

*كان هناك نقاش حول المصطلحات المناسبة، فالمصطلح الأمريكي "التطرف العنيف بدوافع عنصرية وعرقية Racially (**REMVE**) Violent Extremism Motivated and Ethnicallyقد يسـبب التباسًـا مع نوع الإرهاب الذي ترتكبه منظمات مثل إيتا أو الجيش الجمهوري الإيرلندي في أوروبا.

**من ناحية أخرى، فإن الإرهاب الإثني القومي والانفصالي له تركيز وطني أو إقليمي بطبيعته، حتى لو كان الإرهابيون الانفصاليون يعملون أحيانًا خارج الحدود الوطنية للتحضير لهجمات محددة وتنفيذها.

[1] Jeffrey D.Simon, Technological and Lone Operator Terrorism: Prospects for a Fifth Wave of Global Terrorism, in ***Terrorism, Identity and Legitimacy***, ed. Jean E.Rosenfeld (New York: Routledge, 2011), p51

مختلفة وهيئة تحكم غير مركزية، مما يجعل تحديد القادة أمرا صعبًا، وهو نفس تفصيل الجماعات الإرهابية، ونفس الشعور بالحرمان النسبي الذي يغذي الشعور بالكراهية والعداء للإرهابي[1].

لم يعد التطرف الأيديولوجي اليوم في الاتحاد الأوروبي مقتصرا على التطرف" الكلاسيكي " أو التطرف الجهادي، فبعض الحركات الانفصالية المعادية للأنظمة الحديثة لديها إمكانية واضحة للعنف؛ ملهمة من خلال نظريات المؤامرة، فهي تتحدى الحكومات والتدابير التقييدية المطبقة، من خلال التحريض على العصيان المدني والاضطرابات. وعلى الرغم من صعوبة تصنيفها، إلا أنها تحتاج إلى معالجتها لأنها تشكل تحديات أمنية للدول الأعضاء في الاتحاد الأوروبي "[2].

هذا وتتمتع أوروبا بديناميكيات إقليمية قوية في القطاع المجتمعي، بحيث يتم تضمين قضايا الأقليات والدول في كوكبة من الهويات متعددة الطبقات، وبالتالي يتحدد الأمن إلى حد كبير من خلال مصير هذه الكوكبة. ومع ذلك، هناك خطر يتمثل في أن بعض الهويات سوف ينظر إليها الآخرون على أنها تهدد بشدة الامن الأوروبي، فمسائل الهوية تمس الأفراد والجوانب الاقتصادية لحياتهم، بينما يشير الأمن الاجتماعي إلى الجماعات وهويتهم، أو بسبب عملية انفصالية "إقليمية" (على سبيل المثال إقليم كتالونيا)، على الرغم من تميزها من الناحية التحليلية، إلا أنه في الممارسة العملية يمكن دمج هذه الأنواع الثلاثة من التهديدات للهوية بسهولة ووضعها على نطاق واسع يتراوح من المقصودة والبرنامجية إلى غير المقصودة والهيكلية[3].

[1] Paul Cornish and others, "Cyberspace and the National Security of the United Kingdom Threats and Responses", A Chatham House Report, the Royal Institute of International Affairs, March 2009, in: https://www.academia.edu/1242679/Cyberspace_and_the_National_Security_of_the_United_Kingdom (12/02/2022)

[2] EU: “Growing online censorship of presumed -violent extremism- of all ideological varieties", 04 June 2021, in: https://cutt.us/krorn(12|01|2022).

[3] Mieczyslaw Malec,"Security perception within and beyond the traditional approach", Monterey, California. Naval Postgraduate School, Master of Arts in National Security Affairs, Naval Postgraduate School, juin 2003, p40, in: http://hdl.handle.net/10945/951 (23|02|2022)

المطلب الثالث: الإرهاب اليساري والأناركي.

يُعرّف المتطرفين اليساريين بأنهم مجموعات أو أفراد يعتنقون الأفكار الراديكالية للحركات الأناركية وغالبًا ما يكونون على استعداد لانتهاك القانون لتحقيق أهدافهم، في هذا الشأن تشير عدد من الاتجاهات الناشئة إلى أن المتطرفين اليساريين ينضجون ويوسعون قدراتهم على الهجوم السيبراني على مدى العقد المقبل بهدف مهاجمة أهداف حيوية، يندرج هذا ضمن التصور القائل بأن الهجمات الإلكترونية غير العنيفة تتماشى جيدًا مع المعتقدات الأيديولوجية والأهداف الإستراتيجية والتكتيكات للعديد من المتطرفين اليساريين، والتي من بينها:

- الاعتماد المتزايد للحكومات، الشركات التجارية والمؤسسات الأخرى على التقنيات الإلكترونية، بما في ذلك الشبكات المترابطة والوصول عن بعد، وتخزين البيانات الحيوية، والاتصالات، وإدخال نقاط ضعف جديدة وموسعة سيستغلها المتطرفون اليساريون البارعون تقنيًا.
- يحفز انتشار التقنيات والخبرات الإلكترونية بالإضافة إلى توفر أدوات القرصنة عبر الإنترنت و "المتسللين المؤجورين"المتطرفين اليساريين لتبني إستراتيجية هجوم إلكتروني.
- الهجمات الإلكترونية هي خيارات جذابة للمتطرفين اليساريين الذين يرون أن الهجمات على الأهداف الاقتصادية تتماشى مع عقيدة "عدم الإضرار" اللاعنفية وتكتيك "العمل المباشر".
- يستخدم المتطرفين اليساريين أسلوب العمل المباشر لإلحاق أضرار اقتصادية بالشركات والأهداف الأخرى لإجبار المنظمة المستهدفة على التخلي عما يعتبره المتطرفون مرفوضًا.
- يعمل بعض المتطرفين على تحسين قدراتهم في الهجوم السيبراني، وربماسيشجع هذا الأمر تجنيد الأفراد ذوي التقنيات والمهارات المتطورة في استخدام الانترنت في دوائرهم الموثوقة، علاوة على ذلك، يمكن للمتطرفين تطبيق مهاراتهم الإلكترونية لدعم عدد من الحركات اليسارية المختلفة[1].
- الإرهاب اليساري والاناركي يستهدف الثورة على المنظومة الاجتماعية والسياسية والاقتصادية، تمهيدا للقضاء على الطبقية بالمنظار الاشتراكي، وهذا استنادا إلى أيديولوجية ماركسية– لينينية في الغالب (مثال الألوية الحمراء الإيطالية، المنظمة الثورية اليونانية "17 نوفمبر"[2].

[1] (U//FOUO)",Leftwing Extremists Likely to Increase Use of Cyber Attacks over the Coming Decade", U.S. Department of Homeland Security :The Strategic Analysis Group, Homeland Environment andThreat Analysis Division, 09/01/2019, in: https://irp.fas.org(08|07|2021)

[2]Europol, ***European Union Terrorism Situation and Trend Report (TE-SAT), Op.cit***. P21.P94.

يمكن القول أن الإرهاب الاناركي تعبير توصف به أعمال العنف التي تكرّس لغياب السلطة في المجتمع وللرأسمالية والاستبداد (مثال الاتحاد الاناركي غير الرسمي في إيطاليا Anarchica Federazione Informale، ومؤامرة خلايا النار في اليونان Fotias Pyrinontis Synomosia[1].

وجد الإرهابيون الاناركيون قوتهم المتزايدة من خلال تطوير أدوات تكنولوجية محسّنة، كما قال المؤرخ مايكل بيرلي Michael Burleigh في كتابه الأخير "الدم والغضب" تاريخ ثقافي للإرهاب، كان تداول وصفات تصنيع القنابل في الدوائر الأناركية "توقعًا للسهولة التي يمكن للإرهابيين المعاصرين من خلالها الوصول إلى المعلومات حول المتفجرات على الإنترنت". في الواقع، يرتبط الإرهاب المعاصر ارتباطًا وثيقًا بتطور الإنترنت، مع مخاوف واسعة النطاق من الإرهاب السيبراني الذي أصبح الشكل الأكثر شيوعًا، فالإنترنت اليوم تستخدم لأغراض التجنيد أو لمجرد نقل المعلومات. وبالمثل، كان اللاسلطويون يدركون تمامًا الأهمية المركزية للتواصل الفعال للدعاية والحصولعلى تعليمات لتصنيع القنابل[2].

لا يزال العنف بدافع من اليسار والتطرف الأناركي يمثل مشكلة في أجزاء من الاتحاد الأوروبي، لفترة طويلةظل تهديد التطرف اليساري والفوضوى العنيف مستقرًا عند مستوى منخفض ولكن هناك مؤشرات مبكرة على أنه كان يتزايد في بعض الدول الأعضاء في الاتحاد الأوروبي خلال الأزمة الصحية الحالية. لذلك، لهذا تصاعدت تقارير بوجوبادراج مبادرة محددة لمكافحة التطرف اليساري والفوضوي العنيف والإرهاب في سياساتالاتحاد الأوروبي المتعلقة بمكافحة الإرهاب والوقاية من التطرف.

قد يقرر فريق العمل المعني بالإرهاب (TWP) بشأن هذه المسألة أن التطرف العنيف والإرهاب اليساري والفوضوي قد تمت تغطيتهما بالفعل بشكل كافٍ من خلال استراتيجية الاتحاد الأوروبي الشاملة لمكافحة الإرهاب، إذا قررت TWP أن القضية تتطلب اهتمامًا أكبر ، فيمكن النظر في عدد من الإجراءات المحددة والتي يمكن دمج بعضها مع العمل المستمر على التطرف اليساري العنيف، يمكن أن يشمل ذلك

[1] ***Ibid***.

[2] Constance Bantman, For Jihadist, read Anarchist? The Anarchist Stereotype then and now, Institutt for kriminologi og rettssosiologi, Oslo, mars 2011, in: https://cutt.us/frxyB (10/11/2021)

مبادرات لمكافحة انتشار خطاب الكراهية، والمعلومات المضللة عبر الإنترنت، ورسم خريطة ومعالجة التهديد المحتمل الذي يشكله الأوروبيون غير الجهاديين الذين يقاتلون في سوريا[1].

إن العديد من الدول الأوروبية تواجه استقطابًا متزايدًا وتهديدًا متزايدًا من المتطرفين العنيفين،ففي ماي 2019، أكد تقييم التهديد الذي وضعه الاتحاد الأوروبي في مجال مكافحة الإرهاب على الحاجة إلى معالجة التطرف العنيف والإرهاب بدوافع سياسية أو أيديولوجية بجميع أشكاله، خاصة ذلك الذي يمس القيم الأوروبية وعوامل التماسك فيها عبر استخدامه للوسائل التكنولوجية لتمرير ايديولوجيته التي قد تتضارب مع الفكر الجمعي الأوروبي.

إن تهديد الإرهاب الناجم عن التطرف اليساري العنيف والفوضوي موجود بدرجات متفاوتة في أجزاء مختلفة من الاتحاد الأوروبي. يشير أحدث تقييم للتهديدات الأوروبية في مجال مكافحة الإرهاب، استنادًا إلى تقارير يوروبول و EU INTCEN إلى أن "المشهد المتطرف العنيف اليساري والفوضوي [...] زاد من أنشطته في النصف الثاني من عام 2020، على الرغم من عدم تنفيذ أي هجمات إرهابية"، و"التهديد الناجم عن التطرف اليساري العنيف غير المتجانس والتطرف الأناركي (VLWAE) لا يزال منخفضًا ولكنه متزايد، نظرًا لحقيقة أن المزيد من الدول الأعضاء قد تأثرت في عام 2020"كما يصف تقرير اليوروبول حالة الإرهاب واتجاهه لعام 2021 الصادر في 22 يونيو 2021 الوضع بمزيد من التفصيل[2].

شهدت أوروبا عديد الهجمات الإرهابية التي ارتكبتها الجماعات اليسارية التي غذيت بفكر وممارسة إرهابي للدفاع عن قضاياها مثل الألوية الحمراء (إيطاليا) ، وعصابة بادر (ألمانيا[3])، تتركز الأحداث الإرهابية التي يحفزها التطرف اليساري والفوضوي في أوروبا حاليًا في إيطاليا واليونان، وبدرجة أقل إسبانيا، وبحسب تقرير اليوروبول فإن 24 من 25 هجومًا نفذتها منظمات يسارية متطرفة في أوروبا العام الماضي وقعت في

[1] EU action to counter left-wing and anarchist violent extremism and terrorism: Discussion paper (Council doc. 10101/21, LIMITE, 28 June 2021, pdf), in: https://cutt.us/hrTEt (11|04|2022)
[2] EU action to Violent left-wing extremism andanarchism - discussion paper (Council doc. 10180/21, LIMITE, 28 June 2021, pdf), in:https://cutt.us/NaZnI(11|04|2022)
[3] Piero-D. Galloro,***Op.cit.***

إيطاليا، مع هجوم آخر في فرنسا[1]، في حين يذكر تقرير اليوروبول الصادر سنة 2011 أن معظم الهجمات الإرهابية التي نُسبت إلى اليسار والجماعات الأناركية في 2020 تحمل طابعا عنيفا خاصة في إيطاليا[2].

المطلب الرابع: الإرهاب اليميني.

يمكن تعريف اليمين المتطرف في أوروبا بأنه "ظاهرة تجمع بين التشدد فكرا ورؤية وسياسة وبين تطرف أطروحات تساهم في رفض الآخر"، مما جعله محطة انتقالية في التاريخ الأوروبي المعاصر، تغذيه صفة التعصب والعنصرية والعمل على إقصاء كل ما يُنظر إليه من قبَل هذا التوجه كمهدد للهوية الأوروبية والاندماج[3]،وقد أصبح التطرف ظاهرة "لا تهدد السلم المجتمعي والحياة العامة والعلاقات بين الناس فحسب، بل السلم والأمن الدوليين، خصوصا إذا ما تحولت من الفكر والتنظير إلى الممارسة والتنفيذ"[4]، كما أن مفهوم التطرفيشير إلى مجاوزة الوسطية والاعتدال في التفكير تجاه مسائل وقضايا مختلفة، قد تكون دينية أو سياسية غالبا، وقد يتضمن ذلك صفة الإقصاء والعمل على استئصال فئة المخالفين بإبعادهم عن الساحة.

عقب الحرب العالمية الثانية، أصبحت أحزاب اليمين المحافظ واليسار الاشتراكي في أوروبا في واجهة اهتمام الناخبين، ثم "اضمحلت نقاط الاختلاف بين هذين التوجهين من حيث البرامج السياسية وتطبيقها، إذ أصبح اليسار التقليدي تيارا يمينيا رأسماليا بنكهة اجتماعية، وأصبح اليمين التقليدي تيارا يمينيا بنكهة ليبرالية متشددة"، وهذا بعد نهاية الحرب الباردة وسقوط المعسكر الشرقي (الشيوعي) في أوروبا، وقد عمل اليمين المتطرف على استغلال تنامي الحركات والأحزاب والتوجهات المختلفة في القارة، ليتمكن من الصعود والبروز بصورة مؤثرة، لتكون سنوات ما بعد 2014 بمثابة مرحلة الذروة بالنسبة لليمين المتطرف في أوروبا[5].

---

[1]Ömer Tuğrul Çam, EU official on rising ties between European extreme left, YPG/PKK, Anadolu Agency website;14.07.2021, in: https://cutt.us/bbtDf(14|07|2021)

[2]Europol (2021), European Union Terrorism Situation and Trend Report (TE-SAT), ***Op.cit***, P.21.

[3]نبيل شبيب، ***التقرير الارتيادي السنوي: أثر صعود اليمين المتطرف على مسلمي أوروبا، وكيف يتعامل المسلمون مع التطرف اليميني***، المركز العربي للدراسات الإنسانية، 2017، ص02.

[4] عبد الحسين شعبان، ***التطرف والإرهاب: إشكاليات نظرية وتحديات عملية مع إشارة خاصة إلى العراق***، (مصر: مكتبة الإسكندرية،2017)، ص11.

[5] نبيل شبيب، ***مرجع سابق***، ص4-5.

*ينتشر التوجه اليميني المتطرف في كل من فرنسا (حزب الجبهة الوطنية بزعامة "ماري لوبان")، إيطاليا (حزب الرابطة اليميني)، هولندا (حزب الحرية الهولندي)، ألمانيا (الحزب القومي الديمقراطي وحزب البديل من أجل ألمانيا منذ 2013)، بلجيكا، السويد، سويسرا وغيرها.

يمكن وصف اليمين المتطرف في أوروبا* أنه وبتطرفه في التعاطي مع مختلف القضايا الأمنية بات مختلفا عن التيار اليميني التقليدي، بالرغم من أن كليهما يدعو إلى حفظ قيم وتقاليد المجتمع في وجه التهديدات الخارجية[1]، من المهم أن نذكر منذ البداية أن اليمين المتطرف الحديث يمر حاليًا بتحول أوسع وأكثر جوهرية؛ أي ظهور تهديد عبر وطني وما بعد تنظيمي، فالمشهد الأوروبي لليمين المتطرف اليوم عبارة عن مزيج من الأحزاب السياسية اليمينية المتطرفة الرسمية، مثل الديمقراطيين السويديين، وفوكس في إسبانيا، و Lega في إيطاليا، وحزب البديل من أجل ألمانيا Deutschland Alternativefür، وسلسلة من الحركات اليمينية المتطرفة الناشطة في الفضاء الأوروبي.

في عصر الإنترنت شهدنا ظهور حركات متباينة مثل حركة "مكافحة الجهاد"Counter-jihad المناهضة للمسلمين واليمين البديل الدولي The international alt-right، في حين أن كل هذه المجموعات لها منظمات رسمية داخلها، إلا أنها غالبًا ما تكون ما بعد تنظيمية Post-organisational، يقدم الآلاف من الأفراد من جميع أنحاء العالم تبرعات لتحقيق أهداف سياسية مشتركة خارج الهياكل التنظيمية التقليدية تمامًا.

تفتقر هذه الحركات إلى قادة رسميين، لكنها تمتلك رموزًا صوريّة، غالبًا ما تكون مستمدة من مجموعة متزايدة من "المؤثرين" من اليمين المتطرف على وسائل التواصل الاجتماعي التي تمكن للنشطاء اليمينيين المتطرفين الانخراط في السياسة من خلال مشاهدة مقاطع فيديو على YouTube، وزيارة مواقع الويب اليمينية المتطرفة، والتواصل في المنتديات، والتحدث عن طريق خدمات الدردشة الصوتية مثل Discord، ومحاولة تحويل "الأعراف" إلى الاتجاه السائد عبر منصات التواصل الاجتماعي مثلTwitterوFacebook، كل هذا يمكن القيام به بشكل مجهول يقلل بشكل كبير من التكلفة الاجتماعية للنشاط[2].

يهدف الإرهاب اليميني إلى التغيير الاجتماعي، السياسي والاقتصادي داخل المجتمعات الأوروبية، انطلاقا من نظرة فوقية للذات (تمجيد الذات وكراهية الآخر)، وعلى هذا الأساس "تتغذى الأيديولوجيات المتطرفة

[1] عمّارة عمروس، "اللجوء الإنساني في الفضاء الأورو–متوسطي ومشكل الاندماج في المجتمعات الأوروبية – حالة اللاجئين السوريين في ظل صعود اليمين المتطرف"، دراسة غير منشورة بورشة عمل دولية بعنوان: "الهجرة القسرية في الدول العربية: الإشكاليات والقضايا" بيروت– تشرين الثاني/ نوفمبر 2019، ص 5–6

[2] Robert Lüdecke, "European State of Hate: How the Far-Right Is Organising Transnationally", The Amadeu Antonio Foundation, 16. February 2021, in: https://www.amadeu-antonio-stiftung.de/en/european-state-of-hate-how-the-far-right-is-organising-transnationally-66633/ (30 Mars 2022).

على مجموعة متنوعة من الثقافات الفرعية البغيضة"، فتتشكل كراهية الأجانب ويتم محاربة التنوع الثقافي داخل المجتمع والمساواة في الحقوق بين المواطن الأصلي والأجنبي المقيم[1].

وكما هو ملاحظ، تحتاج الجماعات المتطرفة لشن هذه الهجمات لتغطية حاجياتها اللوجستيكية وتجنيد الأفراد وتمويل نشاطها العملي، وقد يكون المصدر هنا ذاتيا بالاعتماد على الشخص نفسه (إذا كانت العملية الإرهابية على طريقة الذئاب المنفردة) أو من خلال عضوية الجماعة أو التنظيم (تبرعات الأعضاء)، وهو ما تقوم به التنظيمات اليمينية المتطرفة "العنيفة" في فنلندا والسويد حيث تعتمد على رسوم العضوية وتبرعات أفرادها[2].

يقول الكاتب والصحفي ديفيد نايورت الذي يكتب عن اليمين المتطرف منذ عقود: "بمجرد أن يسير الأشخاص في تيار التطرف، يصبح باستطاعتهم تكوين مجموعات [على الإنترنت] واجتذاب أتباع لهم عبر أنحاء العالم"، "من بين نتائج ذلك هو أن إرهاب اليمين المتطرف المحلي اتخذ بعدا تسلسليا: عملية عنف واحدة تصبح مصدر إلهام لعملية تالية، وهكذا دواليك[3]."

على سبيل المثال تبرز حادثة "توبياس ر" الرجل الذي كان وراء الهجوم الإرهابي الدموي الذي وقع يوم (19 فيفري 2020) في هاناو في غرب ألمانيا، قد نشر مقاطع فيديو عنصرية على الإنترنت، وهي تردد جنبا إلى جنب بيانه المزعوم بعض نظريات المؤامرة اليمينية المتطرفة المنتشرة على شبكة الإنترنت اليوم. من الواضح أنه أحد الأفراد الذين جرى دفعهم الى التطرف عبر الإنترنت.

في هذا الشأن يشير تحليل أجرته وكالة الاستخبارات الداخلية الألمانية عام 2019 إلى أنها تكافح لتتبع "الذئاب المنفردة" المتطرفة، تبعا لذلك ترى مؤسسة أماديو أنطونيو Amadeu Antonio Foundation ومقرها برلين، والتي تعمل على مواجهة التطرف اليميني، أنه يمكن للأفراد أن يصبحوا متطرفين بسهولة عبر الإنترنت، يقول ميرو ديتريتش Miro Dietrich، الذي أشرف على دراسة استغرقت عامين لمحتوى الوسائط الاجتماعية المتطرفة، إن هناك: "شبكة من المحتوى على الإنترنت تخاطب المجموعات المستهدفة المختلفة وتجذبهم إلى عالم بديل (متطرف)" و "منذ نشأة الإنترنت، تعلم النشطاء اليمينيون المتطرفون، على الرغم من "التجربة والخطأ"، تأطير المحتوى ورعايته لجذب المتطرفين، وأن هؤلاء النشطاء سارعوا بتجربة منصات جديدة

[1] Europol (2021), European Union Terrorism Situation and Trend Report (TE-SAT), ***Op,cit.*** P.21,80.

[2] Marjie T Britz, ***Op.cit.*** P.21, 31.

[3] المرصد الأوربي لمكافحة التطرف، "محاربة التطرف . ما الذي يمكن فعله للتصدي للجماعات المتطرفة على الإنترنت؟"، 20 ماي 2022، https://eocr.eu/?p=8624 (22ماي 2022)

على الإنترنت واعتمادها، وكذلك إنتاج مردود مادي، على سبيل المثال من خلال إعلانات "يوتيوب"، والتبرع، وحملات التمويل الجماعي، ويجادل بأن مستخدمي وسائل التواصل الاجتماعي يتواصلون بشكل متزايد مع بعضهم البعض على شبكات"Dark social"، والتي يصعب مراقبتها[1].

وتستفيض الدراسة عبر التأكيد على أن استخدام الإرهاب اليميني المتطرف في أوروبا للأنترنت قد زاد في 2020، وذلك ما اتضح من خلال نمو استخدام ألعاب الفيديو لنشر الدعاية الإرهابية وعبر منصات متنوعة بما فيها وسائل التواصل الاجتماعي وخدمات المراسلة، كما ظلت الإنترنت الوسيلة الأساسية لنشاط الإرهاب اليساري والأناركي في إطار الدعاية واستقطاب الأفراد ونشر خطاب الكراهية[2]، ووفق تقرير الاتحاد الأوروبي لمكافحة خطاب الكراهية: "لا يؤثر انتشاره غير القانوني عبر الإنترنت سلبًا على المجموعات أو الأفراد الذين يستهدفهم فحسب، بل يؤثر أيضًا سلبًا على أولئك الذين يتحدثون عن الحرية والتسامح وعدم التمييز في مجتمعاتنا المفتوحة وله تأثير مخيف على الخطاب الديمقراطي على منصات الإنترنت"[3].

فيمت يؤكد السياسيون الألمان والسلطات الأمنية وبشكلٍ مشترك منذ عام 2019، على أن التطرُّف اليميني يشكّل تهديداً خطيراً مثله مثل الجهاد المتشدّد[4]. ومما يثير القلق والمخاوف أن الجهات الأمنية وشركات التكنولوجيا أظهرت تقاعسا وبطئا في التصدي لهذا التهديد الجديد والمتنامي[5].

مع الأخذ في الاعتبار هذا الواقع الجديدمن الأهمية بمكان لفهم عمق التهديدات عبر الإنترنت اليوم ومدى استخدام المتطرفين للإنترنت والتكنولوجيا بشكل عام. لذلك، يجب أن تتحقق توازن كاف بين تحسين القدرة التشغيلية ومتطلبات الأمان الضرورية لأنشطةPCVE عبر الإنترنت "[6]، ومن الملامح التي تُبرز الدور

---

[1] كاي أليكساندرشوتس، "كيف يعزز الإنترنت التطرف اليميني؟"، مقال من موقع Deutsche Welle، 3|05|2020 (27|03|2022)https://p.dw.com/p/3YU0z

[2] Europol (2021), European Union Terrorism Situation and Trend Report (TE-SAT), ***Op.cit,*** P-p. 20, 22.

[3] The EU Code of conduct on countering illegal hate speech online, "The robust response provided by the European Union", in:https://cutt.us/JKv1I(10/10/2021).

[4] رافاييل بوسونج، "الخطوات التالية لسياسة الاتحاد الأوروبي لمكافحة الإرهاب.. التهديدات المتطورة للجهادية والتطرف اليميني والتعاون عبر الأطلسي"، في:https://asbarme.com/5716/ (2021/09/12)

[5] غوردون كوريرا، "التهديد المتنامي لليمين المتطرف عبر الانترنت"، موقع قناة بي بي سي،15 جويلية 2019، في: https://cutt.us/zAufh(22|02|2022)

[6] EU, "Growing online censorship of presumed -violent extremism- of all ideological varieties", 04 June 2021, in: https://cutt.us/krorn(12|01|2022)

الحاسم الذي يمكن أن يمارسه التطور التقني في ارتكاب الهجومُ الإرهابي اليميني المتطرف على كنيس يهودي في "هال" بألمانيا سنة 2019، عندما صنع الفاعل عدة بنادق باستخدام 3D.[1]

كما يذكر تقرير اليوروبول لسنة 2021 أن الدول الأعضاء في الاتحاد الأوروبي قد لاحظت زيادة في الأنشطة اليمينية عبر الإنترنت في وقت جائحة كورونا التي فرضت قيودا على حركة الأشخاص، وذلك لغرض نشر الدعاية للنشاط اليميني المتطرف، حيث استغلت جماعات اليمين المتطرف في أوروبا انتشار جائحة كورونا على نطاق واسع في محاربة الهجرة وانتشار المسلمين في القارة، كما استغلها المتطرفون اليساريون والفوضويون لانتقاد سياسات الحكومات في التصدي للجائحة[2].

ومع انتشار جائحة كورونا، بات من المتوقع أن يزيد نشاط جماعات اليمين المتطرف في أوروبا من خلال نشر خطاب الكراهية داخل المجتمع الواحد عبر الترويج لمعلومات مضللة تخص الجائحة، مما قد يؤدي إلى العنف وزيادة النشاط الإرهابي، وكمثال على ذلك فإن الجماعات اليمينية المتطرفة في ألمانيا تلقي اللوم على الحكومة في التهاون فيما يخص انتشار الجائحة، خاصة وأن البعض يروّج لفكرة أن كوفيد-19 تعبير عن مؤامرة وأنه مصنوع تحديدا لفرض شروط البعض على البعض الاخر[3].

[1] A Counter-Terrorism Agenda for the EU, p.3.

[2] Europol, ***European Union Terrorism Situation and Trend Report (TE-SAT)***, Publications Office of the European Union, Luxembourg, (2021), P-p : 26-27.

[3] جاسم محمد، ***مرجع سابق***، ص 38.

المبحث الثالث: الإرهاب الالكتروني وتداعياته على الأمن الأوروبي.

أصبحت الأنشطة المدنية والعسكرية تعتمد بشكل كثيف على تكنولوجيا الاتصال والمعلومات ومجموعة متنوعة من نظم المعلومات الرئيسية الأكثر ارتباطا فيما بينها، وأصبحت تدخل في البنية التحتية الحيوية وتمثل ركيزة لقيامها بخدماتها وفي دورها في نمو الدولة الاقتصادي، وفي الجيش والدفاع والاتصالات والتجارة وكافة مجالات الحياة، فالحوسبة تداخلت مع كل المرافق الحيوية كالكهرباء، وإمدادات المياه، السدود، وخزانات الطاقة والمطارات والإدارة الالكترونية ونقل المعلومات،والدفاع والبنوك والتجارة والمواصلات، وكذا عقد الصفقات والبورصات العالمية.

وحمل ذلك في طياته إمكانية التعرض للأخطار التي قد تهدد بالهجوم على الأهداف الإستراتيجية القومية، حيث بإمكان الفاعلين من الخارج أو الداخل في مجتمع المعلومات العالمي حيث يمكنهم القيام باعتداءات عن طريق استخدام أسلحة سيبرانية، بهدف إلحاق بالغ الضرر بالبرمجيات المشغلة أو ما يتعلق بالمعدات والبنية التحتية ونظم التحكم والإشراف عن العمليات الإنتاجية فيما يعرف بنظام "سكادا* SCADA"وارتباطه بعمليات إنتاج وتوزيع الكهرباء والمواصلات والخدمات المالية والاتصالات وامدادات المياه، وأصبحت تلك الأخطار لا يمثل مصدرها ليس الدول فقط بل الإرهابيون الإلكترونيون.[1]

المطلب الأول: الهجمات السيرانية وانعكاساتها على السيادة السيبرانية الأوروبية.

في هذا السياق الوطني والدولي المعولم والمهتز جيوسياسيا وجيواستراتيجيا، تآكل المفهوم والواقع الكلاسيكي الويستفالي لـ "السيادة الوطنية"؛ وتنامى الأخذ بفكرة وواقع "السيادة المتقاسمة"، إما كواقع أو كإمكانية أو كحتمية. نظرا لتعرضها لهزات أمنية شاملة، تتفاعل فيها التغيرات والديناميكيات المحلية، مع الوطنية، الإقليمية والكوكبية، نظرا لتوسع نطاقات الظاهرة الأمنية؛ كما تتفاعل فيها الأبعاد الاقتصادية والتكنولوجية والإعلامية والاتصالية والسياسية والعسكرية والثقافية والمعرفية سواء بسواء[2].

---

*يمكن تحقيق ذلك من خلال التلاعب بأنظمة "التحكم الإشرافي والحصول على البيانات" (أنظمةSCADA) التي تقيس وتتحكم في الأنظمة الأخرى، إذا كانت هذه الأنظمة متصلة بالإنترنت.

[1] عادل عبد الصادق، ***الارهاب الالكتروني والقوة في العلاقات الدولية نمط جديد وتحديات جديدة***، (القاهرة: مركز الدراسات السياسية والاستراتيجية، 2009) ، ص47.

[2] قاسم حجاج، "مدخل إلى تحليل نسقي للأسباب الهيكلية للهزات الأمنية الشاملة في المنطقة المغاربية–الساحلية"، مداخلة في المؤتمر المغاربي الدولي حول التهديدات الأمنية للدول المغاربية في ضوء التطورات الراهنة: الرهانات والتحديات، (جامعة باتنة، كلية العلوم السياسية 28/27 ماي 2013).

وجرى التشبث –بشكل كارثي– بفكرة العدو المركزي ومفهوم التركيز على الدولة، وكلاهما كان أكثر معقولية خلال الحرب الباردة، إذ ان مهاجمة الدول لم يعد لها أي مبرر أو فائدة الآن علاوة على النتائج العكسية التي تفرزها، في حين أن الأهمية المتزايدة للديناميات العابرة للحدود الوطنية (كما يلاحظ كارل كونيتا) تعني في دلالتها أن من المستحيل حصر مشاعر السخط والاستياء ضمن الصندوق الأسود للدولة الوطنية[1].

ففي السنوات الأخيرة شهد العالم تزايدا ملحوظا في اتساع دائرة التهديدات الإرهابية السيبرانية، والتي من شأنها أن تهدد أمن واستقرار الدولة القومية، كما يمكن لمتغير العولمة Mondialisation أن يجعل إفرازات هذه التحديات تتعدى الحدود الوطنية، جراء الانكشافية La Vulnérabilité التي خلفها التطور التقني المتسارع[2]، خاصة مع بروز المجال السيبراني كبعد خامس تسعى الدول لبسط سيادتها عليه، فبروزه كمساحة استراتيجية خلف أيضا تهديدات تتجاوز في خطورتها التهديدات في المساحات التقليدية، هذا الفضاء وفي إطار قدرته على استيعاب عدد أكبر من الفواعل –حتى خارج إطار النظام السياسي– مع قدرته على توفير قدر كاف من المعلومات لهم، كما يقوم بتقليل المسافات وتخطى حواجز الدولة القومية، والحواجز المادية والتقليدية، فيما بينها، لذا فإن جوزيف ناي يرى أن ما يوفره الفضاء الإلكتروني من مصادر قوة لمختلف الفاعلين على مختلف الأصعدة، يوسع من دائرة التهديدات الأمنية، والتي تنتج عن الأفعال العنيفة التي قد يمارسونها، وإن كان ذلك لا يعنى بالتأكيد تحقق المساواة الكاملة ما بين قدرات الدول، وقدرات الفواعل من غير الدول، إنما يعنى بالأساس تقليص الفارق بينهما في امتلاك القوة، والقدرة على إحداث العنف[3]، جراء هذه الفجوة الرقمية شدنا اضمحلال حدود الداخل والخارج، أي أصبحت هناك حالة من التأثير الشبكي المتزايد بين الدولة وخارجها حيث اتسع استخدام الأفراد، والجماعات، والدول للتكنولوجيا الحديثة المرتبطة بالفضاء السيبراني[4].

---

[1] ديفيد كين، ***حرب بلا نهاية: وظائف خفية للحرب على الإرهاب***، تر معين الإمام، ط 1(المملكة العربية السعودية: العبيكان للنشر، 2008)، ص 12.

[2] عادل زقاع، منصوري سفيان، الجريمة المنظمة بمنطقة الساحل الإفريقي: بانوراما سوسيو–أمنية، ***مجلة العلوم الإنسانية والاجتماعية*** 23(مارس 2016)، ص 155–166.

[3] نوران شفيق، "الفضاء الإلكتروني وأنماط التفاعلات الدولية"، (رسالة ماجستير بجامعة القاهرة: كلية الاقتصاد والعلوم السياسية، 2014)، ص 40: 42.

[4] علي عبد الكريم العبودي، هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين، ***مجلة قضايا سياسية***، العدد 57؛)(2018، ص 106.

تبعا لذلك،أصبح الإرهاب السيبراني قضية عالمية تتطلب من جميع البلدان أن تكون قادرة على السيطرة على عالم الإنترنت لاكتشاف الأعمال الإرهابية فيه، فتزامنا مع التطور التكنولوجيا في وسائل الإعلام الجديدة تبعها تطور التقانة التي يعتمدها الإرهابيون، وكلما زادت الأعمال الإرهابية التي يمكن أن تحدث. لذلك، من الضروري معرفة إلى أي مدى يتم تصنيف الإرهاب السيبراني على أنه جريمة عابرة للحدود، بالنظر إلى أن الفضاء السيبراني لا حدود له، وما أفرزته نظرية تهاوي الحدود التقليدية التي جعلت الفواعل اللادولاتية(الإرهابية) تعملوفق آليات مكّنت لها تكنولوجيات الانترنت من تقويض المؤسسات السياسية، الدستورية، الاقتصادية، الاجتماعية لدول أخرى[1]، فأجهزة الكمبيوتر التي تعمل على الإنترنت التي تستضيفها الحدود التقليدية التي تحمي الدولة القومية الإقليمية، و "البنية التحتية التي يتكون منها الفضاء السيبراني – البرمجيات والأجهزة – عالمية في تصميمها وتطويرها(مشاع)، وقد يعمل المهاجمون السيبرانيون على مسافة بعيدة "الهويات والمواقع ومسارات الدخول" لإعطاء إشارة إلى كيفية تجاوز هجوم للحدود الإقليمية[2]

وبالتالي، تتمتع السمات الكامنة في الشبكات بإمكانية كبيرة للتأثير على الوضع السياسي والاستراتيجي الراهن، حيث تتميز بعدم وجود حدود فاصلة بين الافتراضي والواقعي، لا سيما فيما يتعلق بالأسباب والعواقب التي تجعل البنية المادية وبروتوكولات البرامج التي تشكل الفضاء الإلكتروني من إخفاء الهوية أمرًا سهلاً، وعديد المزايا التي يتيحها الفضاء السيبراني التي تخلق بيئة تسمح للعملاء المجهولين – بشكل فردي أو باسم الحكومات –من اختراق الأنظمة والشبكات السرية، ويمكن تفسير مثل هذه الإجراءات على أنها تحديات لسيادة الدولة وأمن بيانات الأفراد والقطاع الخاص. نفهم من ذلك أنه و "في الفضاء السيبراني العالمي، يؤدي الاعتماد المتبادل والترابط بين المستخدمين والأجهزة المتصلة بالشبكة بشكل كبير إلى تغيير الديناميكيات التقليدية للسبب والنتيجة بشكل لا رجوع فيه"[3]

- تقويض المؤسسات الدستورية:

[1] Nadiah Khaeriah Kadir, and others, Terrorism and Cyberspace: A Phenomenon of Cyber-Terrorism as Transnational Crimes, ***FIAT JUSTISIA***, V13 N 4, (December 2019), pp. 333-344

[2] Lene Hansen and Helen Nissenbaum "Digital disaster, cyber security, and the Copenhagen School**",** ***International studies quarterly***, *53*(4), (2009), P-p1155-1175.

[3] Luisa Cruiz Lobato and Kai Michail Kenkel, Discourses of cyberspace securitization in Brazil and in the United States, Artigos, ***Politica Internacional***.. Vol 58, N2, (Jul-Dec 2015), P-p: 23-43.

.

كما تجدر الإشارة الى تركز التكتيكات الإرهابية الانتباه على أهمية المعلومات والاتصالات لعمل المؤسسات الديمقراطية؛ قد تدور النقاشات حول خطر التهديدات الإرهابية السيبرانية التي تعمل على تقويض الممارسات الديمقراطية حول قضايا حرية المعلومات[1]، عندماتتراجع مستوى شرعية السلطة، وثقة الجمهور بالمؤسسات السياسية بشكل عام، وسياسة النخبة الحاكمة بشكل خاص. تؤدي هذه الظواهر وغيرها إلى حد ما إلى بدء نشاط إرهابي إلكتروني مضاد، مما يزيد من إمكانات الإرهاب السيبراني كوسيلة للضغط على السلطات، لأنها غالبًا ما تؤدي إلى عدم الاستقرار في عمل النظام الاجتماعي والسياسي، وعدم الاتساق في تصرفات وتفاعلات السياسيين، وكذا المؤسسات والأشخاص الذين تتعلق وظائفهم بوضع وتنفيذ السياسات لمواجهة هذه الظاهرة[2].

رغبة الإرهابيين السيبرانيين في التأثير على تبني القرارات الحكومية من أجل إضعاف أنشطة وكالات إنفاذ القانون، ومنع المبادرات التشريعية، من خلال الأساليب العنيفة[3]، مستغلين خصائص الفضاء السيبراني وإمكانية التحرك بمرونة مع إمكانية التخفي وتزييف الهوية.

يفهم من كل ما سبق،أن فرضية حساسية الحدود التقليدية تحولت –شيئا فشيئا– إلى واقع تحت تأثير العولمة بمختلف أبعادها، وهو ما يذكّر بمقولة عالم الاجتماع الأمريكي "دانيال بال" (Daniel Bell) حينما وصف الدولة في هذا العصر بأنها "أصغر من أن تتعامل مع المشكلات الكبرى، وأكبر من أن تتعامل بفعالية مع المشكلات الصغرى" .

يقودنا هذا لفرضية أن الحود التي رسمها العالم الافتراضي تقوض تقليدًا كاملاً لأمن الدولة القائم على الحدود، أي ما يسميه فوكو "**حالة الإقليمية**"؛ الهدف من ذلك هو إبعاد الارهابيين السيبرانين عن المنطقة السيادية للدولة. فالحدود الجديدة تسمح للمعتدي بتنفيذ هجمات تقوض سيادة الدولة دون أن تكون موجودة على أرض الدولة التي تعرضت للهجوم[4].

---

[1] Maura Conway, 'Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet', *First Monday*, November 2002, Vol. 7, No. 11-4,.Reality Bytes (firstmonday.org) (07|05|2021)

[2] Екатерина Николаевна, Молодчая. ПОЛИТИКА ПРОТИВОДЕЙСТВИЯ КИБЕРТЕРРОРИЗМУ В СОВРЕМЕННОЙ РОССИИ: ПОЛИТОЛОГИЧЕСКИЙ АСПЕКТ, диссертации на соискание ученой степени кандидата политических наук Москва, РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ СОЦИАЛЬНЫЙ УНИВЕРСИТЕТ, 2011, p4.

[3] ***Ibid***, p22.

[4]جندلي، عبد الناصر ، "إشكالية تكييف المنظور الواقعي للعلاقات الدولية مع التحولات الدولية لما بعد الحرب الباردة"، ***مجلة المستقبل العربي***، العدد 376، (2010)، ص 29.

تبعا لذلك، تأسس وعي أمنيوإجماع متزايد بين خبراء الأمن السيبراني والوكالات الحكومية حول التأثير الوقائي المحدود لإعادة إنتاج منطق الحدود التقليدي على الفضاء السيبراني لحماية الشبكات الرئيسية مثل أنظمة المعلومات العسكرية أو الحكومية، في هذا الصدد يشير تقرير صدر عام 2008 عن حالة البحث والتطوير في مجال الأمن السيبراني نشرته الإدارة المركزية الفرنسية لأمن أنظمة المعلومات إلى أن تعيين "محيط الحماية" من خلال استخدام الأدوات التقنية مثل الجدران النارية يبدو أقل فاعلية منع الهجمات الإلكترونية، ويرجع ذلك إلى التنوع الكبير في "القنوات المخفية" المتاحة للمهاجم، والتي تمكنه من الوصول إلى هدفه وإلى "الثراء الدلالي للتدفق المصرح به" الذي يجعل من الصعب تصفية ماهية التهديد، وغايته. وهكذا، يميل الأمن السيبراني إلى قلب آليات أمن الدولة التقليدية في مجال العلاقات الدولية. يظهر الانفتاح، أي الاعتراف بعدم أهمية الإقليم كقاعدة، في حين أن الحدود على الأقل بمعناها التقليدي المتمثل في رسم خطوط ثابتة بين الخارج والداخل يصبح مفهوم مرن[1].

المطلب الثاني: التداعيات على الأمن المجتمعي.

وفق مدرسة كوبنهاغن يتم بناء التهديدات اجتماعياً وخطابياً، الأمر نتاج منافسة دلالية حول إقناع الجمهور فيما يتعلق بتسمية موضوع معين على أنه مسألة أمنية، هذا يوسع مفهوم الأشياء المرجعية خارج الدولة، وإحدى فضائل النظرية هي على وجه التحديد تركيزها على المجتمع كقطاع محدد من التحليل الأمني[2].

تبعا لذلك أثر الفضاء الالكتروني على المجال الاجتماعي في زيادة المعلومات التي يكون لها دور في ظهور أنماط تغير القيم والخطابات السائدة، وعلاقات العمل وهيكل القوة داخل المجتمع، والتأثير في المجال الإعلامي مع زيادة مؤسسات الإعلام والفاعلين فيه، وقدرته على الكشف عن قضايا المجتمع الدولي بصورة متنوعة وسريعة، واجراءالتبادل الذي يعتمد على المشاركة بين المرسل والمستقبل بأساليب متطورة دون وسائط بشرية، وكان من شأن كل تلك المظاهر أن كان لهادور بصفة عامة في تغير طبيعة المكونات والفاعلين وأجندة ونمط الاتصال والاستجابة داخل النظام الدولي[3].

---

[1] Memphis Krickeberg, ***Op.Cit.***

[2] Barry Buzan, Lene Hansen, ***The Evolution of International Security Studies***, (Cambridge: Cambridge University Press, 2009), p 368.

[3] عادل عبد الصادق، الارهاب الالكتروني والقوة في العلاقات الدولية، ***مرجع سابق***، ص 49.

فمثلا، وكتحليل للتداعيات المجتمعية نجد الحركات اليمينية المتطرفة التي تنشط عبر وطنيا تضع قضاياهم دائمًا في سياقها على المستوى القاري أو العالمي. وتعمل عبر الشبكات الفضفاضة كمشابك لتمرير المعلومات حول العالم. فالمتطرفون الذين يعانون من الإسلاموفوبيا في بلد ما، مثلا، يستغلون عداءهم في قضية تقديم الدجاج الحلال في مطاعمهم المحلية، وينشرون ذلك على وسائل التواصل الاجتماعي ومنه تنتشر القصة عبر الشبكة. خاصة إذا تم التقاطها من قبل "الشريك الفائق" (ناشط مؤثر بشكل خاص ولديه عدد كبير من المتابعين على وسائل التواصل الاجتماعي)، فإن القصة المحلية سيتم التقاطها من قبل الإسلاموفوبيا المتشابهين في التفكير في جميع أنحاء العالم وستكون بمثابة "دليل"Evidence أكثر وإقناعهم بتهديد "الأسلمة"Islamification[1]، مما يخلق شعورا معاديا ومتطرفا يولد فعلا إرهابيا وهو ما رأيناه في عديد الهجمات على مسلمين في أوربا وفي العالم ككل.

على سبيل المثال، تهتم جماعات اليمين المتطرف في أوروبا باستخدام الانترنت لنشر الكراهية والتحريض على التفرقة داخل المجتمعات، فحزب البديل الألماني مثلا لا يكتفي باستخدام الانترنت كوسيط للتواصل وإنما يكيّفه مع أهدافه في التنظيم والتخطيط أيضا بهدف عنصري تجاه الأجانب [2]، فغالبًا ما يتصرف اليمين المتطرف محليًا، لكنه يرى نفسه جزءًا من معركة دولية مناهضة للديمقراطية، وهي ظاهرة مقلقة تمثل تهديدًا جديدًا وحقيقيًا. تم توثيق هذا الاتجاه في التقرير الجديد "حالة الكراهية: التطرف اليميني في أوروبا"، الذي كتبته منظمات غير حكومية من جميع أنحاء أوروبا بتنسيق Hope not Hate بالمملكة المتحدة، Expo بالسويد، ومؤسسةAmadeu Antonio بألمانيا.

من الصعب تحديد الآثار طويلة المدى لهذا الأمر، لكن هناك بالتأكيد خطر يتمثل في أن مجتمعات نظرية المؤامرة على الإنترنت تقدم مسارات جديدة للتطرف، لا سيما تجاه نظريات المؤامرة المعادية للسامية بشكل علني[3].

فالتهديدات الإرهابية الناشئة عن التقنيات الرقمية يمكن أن يكون لها آثار مجتمعية مدمرة[4]،لأن الأعمال الإرهابية عادة ما تزيد من احتمال حدوث عواقب نفسية ضارة على ضحاياها، وجعل الهدف الحقيقي للإرهاب هو الرأي العام. ربما يكون هذا هو السبب وراء قيام الجماعات الإرهابية بتشغيل مواقع ويب نشطة، وإعلان

[1] Robert Lüdecke, ***Op.cit.***

[2] جاسم محمد، ***مرجع سابق***، ص 231.

[3] Robert Lüdecke, ***Op.cit.***

[4] Lene Hansen and Helen Nissenbaum "Digital disaster, cyber security, and the Copenhagen School*",* International studies quarterly, *53*(4), (2009), P-p 1155-1175.

مسؤوليتها عن الأنشطة الإرهابية من خلال هذه المواقع[1]، ومناقشة أفكارها وعرضها على المدونات فالتأثير في الوعي الجمعي ومحاولة تغيير أنماط تفكير محددة قد يخدم أجنداتها، ويزيد من قوة الجذب لديها[2].

يذكر تقرير اليوروبول الصادر في ديسمبر 2021، والذي يقدم نظرة واسعة عن وضعية الإرهاب في أوروبا خلال العام 2020، أن الجماعات الإرهابية وسعت نشاطها عبر المنصات الرقمية، وأن الدعاية للعمل الإرهابي أصبحت مشتتة بين منصات متنوعة، فقد أدت جائحة كوفيد19 والتدابير التي رافقتها في الاتحاد الأوروبي إلى جعل الإرهابيين يضاعفون نشاطهم عبر الانترنت، وبالتالي زيادة استهلاك أفراد المجتمع للمحتوى المتطرف[3].

كما استفادت هذه التنظيمات من الفضاء الإلكتروني بوصفه منصة لإطلاق الحرب النفسية ضد المجتمعات بتصوير مشاهد العنف ونشرها على نطاق واسع لبث الرعب والذعر[4]، كما يهدف المهاجمون عبر استخدام الفضاء السيبراني إلى أن يكونوا قوة سيبرانية مهمة قادرة على إنزال الأضرار النفسية والاقتصادية داخل المجتمعات الأوربية لخدمة أهدافهم ومناصرة حلفائهم، وكذا التأثير على الوعي الديني وتحريك الهويات الفرعية، وعلى الرغم من وجود فجوة كبيرة بين طموحات المهاجمين وقدراتهم الفعلية على تحقيقها، إلا أن هذه الفجوة في طريقها إلى التقلص خاصة مع التحوّل من العمل الإرهابي الفردي إلى عمل جماعي منظم، كما أن حدوث تبادل الخبرات والتدريب بين منفذي هذه الهجمات من شأنه تضييق الفجوة بين أهداف هذه المجموعات وقدراتها الفعلية على تنفيذ الهجمات ذات الطابع الفجائي، ويؤثر ذلك حتما على احتياطات الأمن والحماية التي تهددها القدرة الهائلة على الحشد والتعبئة، خاصة إذا ما تمّت هذه التعبئة بدافع ديني وإيديولوجي[5].

---

[1] Lloyd Muriuki, ***Terrorism and the Internet: How Weblogs are used to propagandise in the American led war on terrorism***, thesis submitted to the School of Arts and Sciences in partial fulfillment of the requirements for the degree of Master of Arts in International Relations, United States International University Africa Nairobi, July 2006, p 46.

[2] Europol (2021), ***European Union Terrorism Situation and Trend Report (TE-SAT)***, Publications Office of the European Union, Luxembourg, p-p: 8-9.

[3] ***Ibid.***

[4] العنف الرقمي... أحدث صيحات الحروب الجديدة، مجلة الإنسان عدد 59، 2015، تم تصفح الموقع يوم 17-03-2019 https://goo.gl/YRTBHQ

[5] عادل عبد الصادق، ***الإرهاب الالكتروني القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة***، ط 2،(القاهرة: المركز العربي لأبحاث الفضاء الالكتروني، 2013)، ص 263.

في هذا الشأن ذكر تقرير لمركز دراسات التطرف بلندن بأن تنظيم "داعش" الارهابي قد تمكن من استقطاب أكثر من 10 ألاف فرد للانخراط في صفوفه حتى منتصف عام 2014 وذلك من خلال منصات التواصل الاجتماعي، وهو ما يعكس حجم التداعيات السلبية على استقرار المجتمعات[1].

تبعا لذلك، ولاستيعاب هذا التحديات الأمنية، تتطلب عملية الأمننة قبول الجمهور للتهديد واعتباره تهديدا وجوديا[2]، ومن منظور هذه الصورة الجماعية، فإن التهديد الأساسي الذي يشكله الإنترنت هو احتمال تقويضه للهويات الوطنية الجماعية.

أصدرت العديد من الدول أو الوزارات والإدارات داخل أوروبا، مثل فرنسا وألمانيا تصريحات رسمية أظهرت شعورًا بالقلق إزاء التهديدات التي تتعرض لها الهوية الثقافية في بيئة الإنترنت، يبدو أن هذا الشعور بالقلق يتركز بشكل واضح على الهوية الوطنية والثقافية كما هو مفهوم تقليديًا، حيث يصعب فصل الاهتمام بالهوية الوطنية والثقافية عن الاهتمام بأمن الدولة أو النظام، وهي صورة جماعية واضحةمن هذه البلدان تختزل نظرتها للارهاب الذي يستغل الإنترنت على أنه تهديد كبير للأمن الثقافي[3].

المطلب الثالث: التداعيات على الأمن الطاقوي.

نتيجة للعدد الهائل من الأنظمة المترابطة على الإنترنت، تكشف البيئة السيبرانية مساحة واسعة ذات نقاط ضعف لا حصر لها مفتوحة للاستغلال، فأي هجوم ناجح ضد البنية التحتية للمعلومات(انظر للشكل اسفله) يمكن أن يؤدي إلى تأثيرات كارثية على البنية التحتية المادية[4].

---

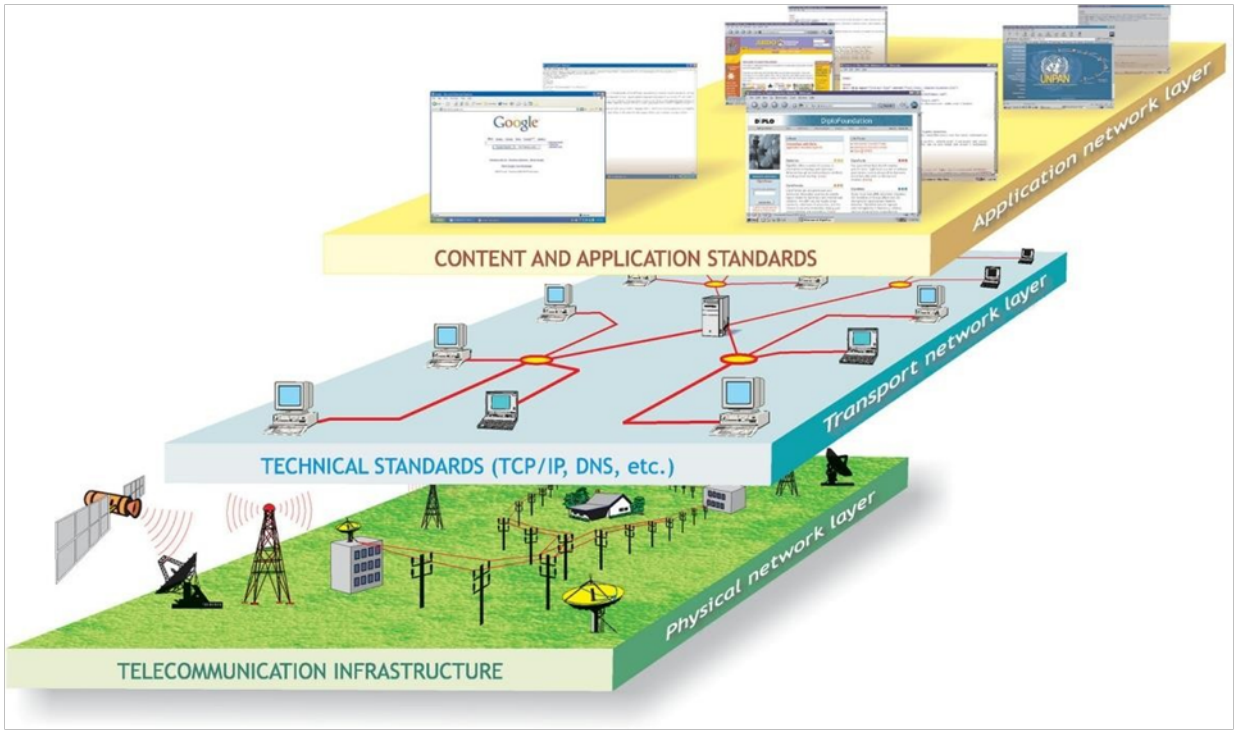
[1] عبد القادر جعيجع ، تيغزة زهرة، تطور الإرهاب وانعكاسه على استقرار المجتمعات: قراءة في ظاهرة الإرهاب الإلكتروني وإستراتيجيات المواجهة، ***مجلة دفاتر السياسة والقانون***، المجلد 13، عدد1، (جانفي 2021)،ص: 544-556.

2 Barry Buzan, Ole Wæver, Jaap De Wilde, ***Security: A New Framework for Analysis***. (USA:Boulder: Lynne Rienner, Library of Congress Cataloging-in-Publication Data, 1998), p 25.

[3] Deibert, Ronald J. "Circuits of Power: Security in the Internet Environment " ,In: ***Information Technologies and Global Politics, the Changing Scope of Power and Governance***, Rosenau, James N., and J.P Singh, eds. Albany, (New York: State University of NY Press, 2002). P-p. 115-142.

[4]JULIE E. MEHAN,***Cyberwar, Cyberterror, Cybercrime and Cyberactivism An in-depth guide to the role of security standards in the cybersecurity environment***, Second edition,(United Kingdom:Ely, Cambridgeshire, IT Governance Publishing, 2014), p 64.

الشكل رقم (5): البنية التحتية للمعلومات



Source: *Diplo Foundation, graphiclibrary* .*https://cutt.us/zKhVX* (21|03\2022)

لم يثبت لحد الان وجود تهديد للهجمات السيبرانية على أي بنية طاقوية أوربية، لكن يشير بعض الباحثين إلى أنه تم التذرع بتهديد الإرهاب السيبراني عبر مؤسسات الاتحاد الأوروبي وهياكله الاقتصادية كجزء من عملية إعادة إضفاء الشرعية على الحاجة إلى مشاركة عموم أوروبا في تأمين البنية التحتية الحيوية،خاصة في ظل الترابط المتزايد بين الوظائف الاجتماعية والاقتصادية والتقنيات الرقمية التي تدعمها المفوضية الاوربية؛ هذه الأخيرةجادلت بأن جائحة كوروناقد زادت من خطر الجهات الفاعلة الهجينة – بما في ذلك الجهات الفاعلة غير الحكومية مثل الإرهابيين – الذين يرتكبون هجمات ذات دوافع سياسية ضد الأنظمة الرقمية[1].

[1] Christopher Baker-Beall, Gareth Mott, ***Op.cit.***

- **الأثر الاقتصادي للتهديدات الإرهابية السيبرانية :**

تحولت المعرفة إلى قوة أساسية أقوى من قوى الإنتاج، وبذلك تحول الاقتصاد الدولي بشكل عام، والأوربي بشكل خاص، الى اقتصاد خدمي يعتمد على المعرفة وانتاج المعلومات والابتكار بخلاف الاقتصاد القديم الذي كان يتميز بالاعتماد على السوق التقليدية والكثافة العمالية والانتاج الوفير، وكانت فيه القوة الاقتصادية ترتبط بالقدرة على امتلاك المواد الخام والموارد الطبيعية.

ولكن ما يعرف بالاقتصاد الرقمي الجديد أصبح يرتبط بالتطور التكنولوجي والمعلوماتي وظهور مؤسسات عمل غير تقليدية ونظم ادارة الكترونية ومنتجات تعتمد على الابتكار والسرعة، وتضائل قيمة المكون المادي، وارتفاع قيمة المكون المعلوماتي[1]، يفهم من هذا أن تزايد القلق بشأن الضرر المحتمل من الإرهاب السيبراني تزايد مع النشاط الاقتصادي المعولم والمرتبط كليابالإنترنت[2].

في العالم التجاري، تشير دراسات لامكانية تعطيل للإرهابيين السيبرانيين للبنوك والمعاملات المالية الدولية وبورصات الأوراق المالية، كلها ستفقد المعلومات اللازمة لتبادل البيانات الاقتصادية،مما سيظهر مستوى معين من الفوضى[3]،أما بالنسبة للبنية التحتية الحيوية، مثل إمدادات الطاقة، والنقل، والتحكم الإلكتروني، تلعب أنظمة المعلومات أيضًا دورًا حاسمًا في الحفاظ على السلامة العامة والإمدادات المستقرة للخدمات التي لا غنى عنها للأنشطة الاقتصادية للأعمال التجارية والحياة اليومية للناس[4].

في مقالته الأخيرة بعنوان "الوحوش الرقمية والأجانب الثنائية – فيروسات الكمبيوتر والرأسمالية وتدفق المعلومات"، يقدم جوسي باريكا Jussi Parikka تحليلًا يفضح من خلاله زيف هذه الرؤى المثالية لاقتصاد المعلومات المعاصر من خلال إثبات أن نقاط الضعف في النظام وفيروسات الكمبيوتر لا تنتقص من التدفق الفعال لاقتصاد المعلومات الرأسمالي ولكنها في الواقع مكونات ضرورية لمنطق اقتصاد المعلومات "الفيروسي" الخاص[5]، من ناحية أخرى، يتم وصف الجماعات الإرهابية في كثير من الأحيان على أنها انتهازية، حيث

---

[1] عادل عبد الصادق، الإرهاب الالكتروني والقوة في العلاقات الدولية، ***مرجع سابق***، ص 49.

[2] Congressional Research Service, 'Terrorism Risk Insurance. Overview and Issue Analysis', December 27, 2019, p. 7.in :Terrorism Risk Insurance: Overview and Issue Analysis for the 116th Congress (07|05|2021).

[3] Jarkko Moilanen, ***op.cit.***

[4] Prime Minister's Office, 'Special Action Plan for Cyber Terrorism Countermeasures for Critical Infrastructure', December 15, 2000, in:https://cutt.us/OTgKv(01/06/2020).

[5] Casey Alt, Viral Load. The Fantastic Rhetorical Power of the Computer Virus in the Post-9/11 Political Landscape. Österreichische Zeitschrift für Geschichtswissenschaften, 16(3), (2005). 133–149, in: :https://doi.org/10.25365/oezg-2005-16-3-9(04/12/2021).

تختار استغلال نقاط الضعف الخفيفةلاقتصاد المعلوماتوالتي يتم كشفهافي عالم متصل بالشبكة و العثور بسرعة على أكبر عدد ممكن من أجهزة الكمبيوتر بنفس مشكلة عدم الحصانة، ثم تثبيت برنامج ضار تلقائيًا ينتظر بهدوء مزيد من الإرشادات من المهاجم[1].

يخرق الإرهابيون السيبرانيون أنظمة المعلومات للمؤسسات الاقتصادية ليس لتحقيق مكاسب مالية ولكن لإحداث الفوضى والتأثير على الجماهير المدنية. عكس ما يفعله عادة المتسللون العاديون من أجل المال، كما أن معظم أهداف الإرهاب السيبراني قليلة القيمة بالنسبة للقراصنة العاديين ولن يلاحق المتسللون العاديون هذه الأهداف على المدى الطويل. من الناحية النسبية، سيبذل الإرهابيون السيبرانيون جهدًا أكبر بكثير من المتسللين العاديين الذين قد لا يمتلكون الدعم والموارد المالية لشن هجوم متطور للغاية ضد الأنظمة شديدة الحماية، فعلى الرغم من افتراض أن الإرهابيين الإلكترونيين قد يكون لديهم تمويل محدود، لكنهم قادرين على جمع ما بين مئات الآلاف إلى بضعة ملايين من الدولارات ويكونون أيضًا على استعداد لإنفاق الأموال التي تم جمعها في تنفيذ هجماتهم[2]، يمكن أيضًا استخدام الضعف الواضح للأنظمة الحرجة[3] للنظام المصرفي لأغراض إرهابية مثل:

- اختراق النظام المصرفي وإلحاق الضرر بأعمال البنوك وأسواق المال.
- تعطيل عمليات التحويل المالي، مما قد يعطل الاستثمار الأجنبي لانعدام الأمن المعلوماتي، وما يسببه هذا من انعدام الثقة بالاستثمار عامة[4].

عبّر السناتور جوزيف ليبرمانJoseph Lieberman أثناء تقديمه لقانون الأمن السيبراني لعام 2012 عن ضرورة التحرك لمنع وقوع هجمات 11 سبتمبر إلكترونية، وأردف قائلا " تبحث الدول المتنافسة والجماعات الإرهابية والعصابات الإجرامية والمتسللون الأفراد كل يوم نقاط الضعف في شبكات الكمبيوتر الأكثر أهمية لدينا، والسعي لسرقة الأسرار الحكومية والصناعية، أو زرع فيروسات لتخريب النظم الإلكترونية التي تتحكم في أكثر البنى التحتية أهمية لدينا مما مكن العدو للسيطرة على شبكة الكهرباء أو نظام إمدادات

---

[1]Julie E. Mehan,Ibid, p 39-45.

[2] Jian Hua, Sanjay Bapna, "The economic impact of cyber terrorism Journal of Strategic Information Systems" ,22 (2013), pp 175–186. In : http://dx.doi.org/10.1016/j.jsis.2012.10.004 (7/07/2021).

[3] Miguel Alberto Gomez, Bias and Misperception in Cyberspace, CIBER elcano No. 53 - March 2020, in :https://cutt.us/c7loF (05/12/2021)

[4] خالد حسن أحمد لطفى، ***الإرهاب الالكتروني آفة العصر الحديث والآليات القانونية للمواجهة***، (الإسكندرية: دار الفكر الجامعي، 2019)، ص 76.

المياه في المدينة بلمسة مفتاح من أماكن بعيدة[1]"، يمكن أن يزداد نطاق وحجم الهجمات، مع استهداف البنية التحتية الرئيسية – مثل أسواق الأوراق المالية وأنظمة الاتصالات السلكية واللاسلكية وشبكات التحكم في الحركة الجوية والقنوات الحيوية الأخرى[2]

في هذا الصدد، وفي سياق متصل، يشكل الترابط بين أنظمة الكمبيوتر وغياب الحدود الفعالة هياكل متراخية تُستخدم لتعزيز الاضطرابات السياسية والعسكرية، لأنها تمتلك القدرة على "التحكم في الأشياء المادية مثل المحولات الكهربائية والقطارات ومضخات خطوط الأنابيب والأحواض الكيميائية والرادارات" وهي بعض التوقعات الكارثية التي قد تستخدمها الدول المتنافسة والإرهابيون والمجرمون للتسبب في المعاناة وتهديد البنى التحتية الحيوية لدول أخرى.

من ناحية أخرى، ان ربط أمن المعلومات وتأثيرات الهجمات المحتملة على المنشآت الصناعية والخدمات والإمدادات، ينضم الأمن السيبراني إلى الخطابات والاستراتيجيات الدفاعية للبلدان التي تستهدف هجمات إلكترونية ضخمة أو التي تعتمد بدرجات متفاوتة على الأنظمة المحوسبة[3]

وإضافة إلى ذلك، وفي أعقاب الهجوم الإرهابي على جسر لندن في الثالث من يونيو، بدت رئيسة الوزراء البريطانية تريزا ماي مؤيّدة لفرض قيود حكومية جديدة على المعلومات المتاحة على الإنترنت، حين دَعَت إلى عقد "اتفاقات دولية لتنظيم الفضاء الإلكتروني؛ لمنع انتشار التطرف والتخطيط للإرهاب[4]." فوصول الإرهابيين للبنى الحيوية يظل بإمكانهم اختراق شبكات الكهرباء، والطاقة، والمواصلات، بل –وفي سيناريوهات تشاؤمية– للمفاعلات النوويةكما بمقدرتهم الوصول للأسلحة الموجهة إلكترونيا، أو عبر الأقمار الصناعية، والسيطرة عليها أو تدميرها، الأمر الذي قد يسبب كارثة بشرية.[5]

---

[1] البيان الافتتاحي لجوزيف ليبرمان حول "تأمين مستقبل: قانون الأمن السيبراني الأمريكي لعام 2012": أمام مجلس الشيوخ لجنة الأمن والشؤون الداخلية.

Opening Statement of Chairman Joseph Lieberman “Securing ’s Future: The American Cybersecurity Act of 2012”: Before the Sen. Homeland Security and Governmental Affairs Committee, 112th Cong. (2012) (statement of Sen. Lieberman, Chairman).

[2] Deibert, Ronald J.***Op.cit.***.

[3] Luisa Cruiz Lobato and Kai MichailKenkel, Discourses of cyberspace securitization in Brazil and in the United States, Artigos, Rev. Bras. Polít. Int. 58 (2): 23-43, Jul-Dec 2015, in: https://doi.org/10.1590/0034-7329201500202 (06/12/2021)

[4] Steven Aftergood, "Cybersecurity: The cold war online, nature international journal of science", 06 July 2017, in:https://cutt.us/SLef1 (05/12/2021)

[5] أنديرا عراجي، ***القوة في الفضاء السيبراني: فصل عصري من التحدي والاستجابة***، (رسالة لنيل دبلوم الدراسات العليا في العلوم السياسية والإدارية بكلية الحقوق والعلوم السياسية والإدارية بالجامعة اللبنانية) 2016–2015، ص 121– 122.

مرد كل هذه المخاوف الأوروبية هو الارتفاع الكبير للأفراد ذوي الكفاءة داخل التنظيمات الإرهابية، مما أدى بالحكومات إلى إدراك خطورة المشكلة، ودفعها نحو زيادة الأمن السيبراني الإلزامي الذي يشمل الشبكات الحكومية والخاصة، كما ان أحد أهم المخاوف المدرجة للمشرعين الأوربيين ومسؤولي المخابرات والقادة العسكريين هو التهديد السيبراني المتزايد بسرعة، مستشهدين بالاعتقاد بأن أي هجوم إلكتروني ناجح على شبكة الكهرباء أو شبكات الاتصالات لديهم يمكن أن يشل الاقتصاد ويهدد الأمن القومي في أوربا[1]، خاصة مع ترابط البنى التحتية بعضها ببعض الأمر الذي يفسر كل هذه المخاوف الأوروبية.(أنظر للشكلين رقم 9 و 10)

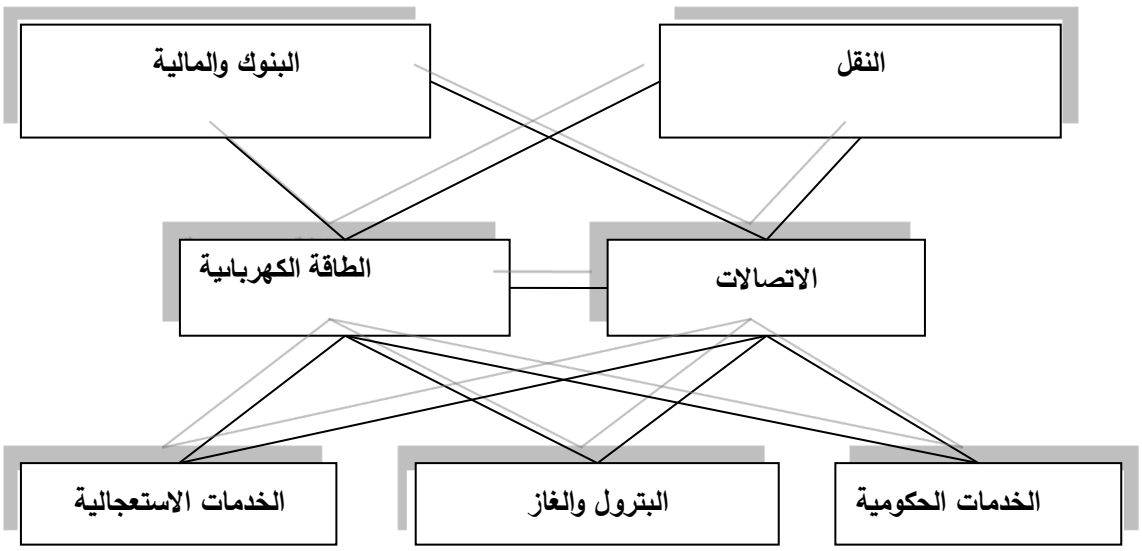
كما سجلنا القلق بشأن ضعف الاعتماد المتبادل الرقمي في المقتطف التالي من التقرير المرحلي الأول عن استراتيجية الاتحاد الأمني للاتحاد الأوروبي[2]:

"تعتمد الحياة اليومية للمواطنين على بنية تحتية مادية ورقمية متزايدة الترابط والاعتماد المتبادل، هذه البنية التحتية حيوية لسير الاقتصاد والمجتمع، دون إمدادات موثوقة من الطاقة، ووسائل نقل يمكن التنبؤ بها، وأنظمة صحية شاملة [.....]، الاتحاد الأوروبي أدرك المصلحة المشتركة في حماية البنية التحتية الحيوية من التهديدات، سواء كانت طبيعية أم هجمات إرهابية، كما تتعدد صور التهديد الحالي التي تواجه البنية التحتية الحيوية، وتشمل: الإرهاب، والهجمات الإلكترونية، والحوادث الداخلية، والتهديدات المرتبطة بالتقنيات الجديدة والناشئة ... لهذا تحتاج قواعدنا الحالية إلى التحديث والتوسيع".

[1]Jeffrey Thomas Biller, ***Op.cit.***

[2]Christopher Baker-Beall, Gareth Mott, ***Op.cit.***

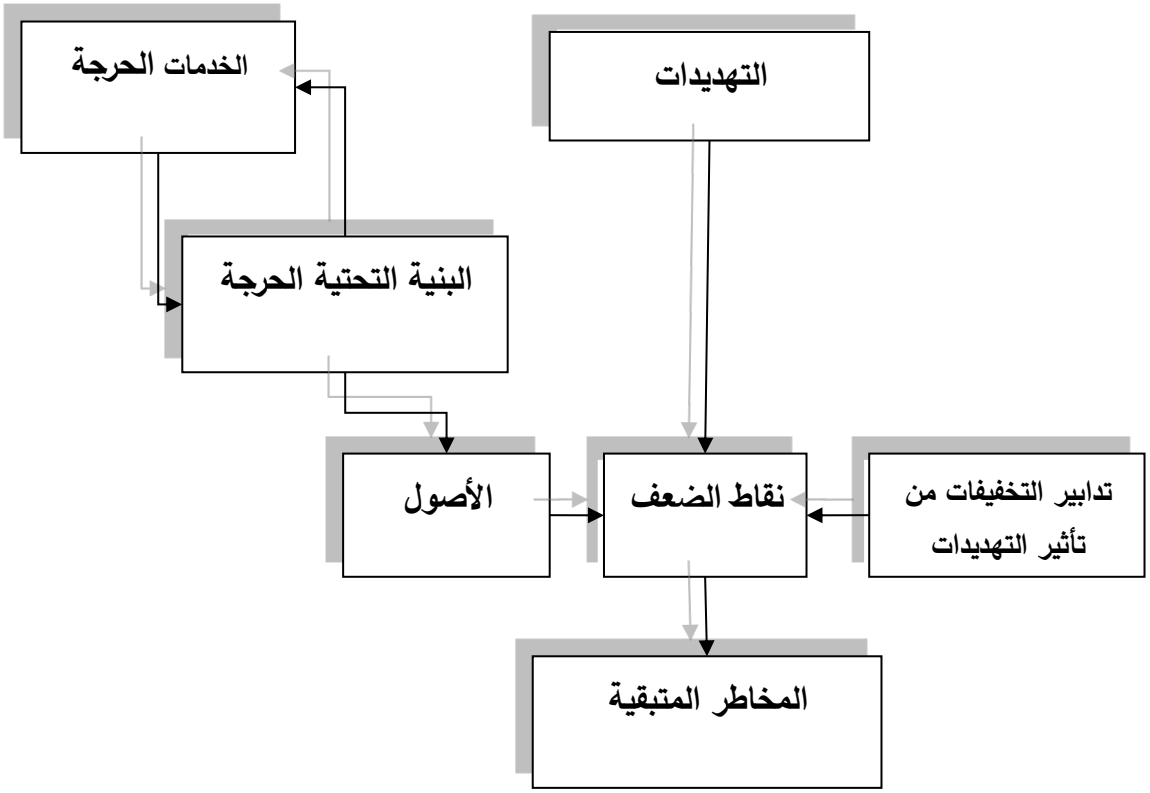
الشكل (6): ترابط البنية التحتية الحرجة



Source: Allan Charles Watt, ***New Zealand Government and Critical Infrastructure Ready Reaction to Cyber Terrorism***, A thesis submitted in fulfilment of the requirements for the degree of Master of Science in Forensic Science,The University of Auckland, 2008.P 85 https://researchspace.auckland.ac.nz/handle/2292/6758

بسبب هذا الترابط تم التعبير عن المخاوف الأوروبية من أن الحوافز الارهابيةاذا ملكت التكنولوجيا اللازمة قد تفوق آليات أمان البنية التحتية. لذلك يجب على الحكومة أن تنظر في كيفية التأكد من أن إدارة المخاطر كافية، يستعرض المخطط التالي التهديدات ونقاط الضعف داخل البنية التحتية الحيوية التي تعتبر مفتاح العمليات المحلية داخل البلد، ويوضح الرسم البياني التالي كيف تعتمد البنى التحتية الحيوية المختلفة على بعضها البعض.

الشكل (7): تهديدات البنية التحتية ونقاط ضعفها



Source: Allan Charles Watt, ***New Zealand Government and Critical Infrastructure Ready Reaction to Cyber Terrorism***, A thesis submitted in fulfilment of the requirements for the degree of Master of Science in Forensic Science,The University of Auckland, 2008.P 85 https://researchspace.auckland.ac.nz/handle/2292/6758

يوضح الرسم البياني في الشكل 11 الخدمات الحرجة اعتمادًا على البنية التحتية، حيث تعتمد بعض البنى نفسها على خدمات بنى أخرى وكلها تشكل مكونات البنية التحتية المشار إليها سابقا والتي قد تكون عرضة للضعف في حالة استغلال الثغرات الأمنية عن طريق التهديدات.

المطلب الرابع: المخاطر الأمنية والسياسية.

أحد وجوه الفهم الممكنة لتحليل الوضع الأمني هو أن يُنظر إلى الإرهاب السيبراني على أنه تهديد فريد بما يكفي لتبرير ذكره في عدة مناسبات، ولكن الأهم من ذلك، أن التهديد أثير باعتباره "حزمة" من المخاطر التي تواجه الدول الأوربية في سياق مختلط ومشتت بشكل متزايد[1]،أخذا بالنشر القائل بأن "إرهابي الغد قد يكون

[1] Christopher Baker-Beall, Gareth Mott, ***Op.cit.***

قادرًا على إحداث المزيد من الضرر باستخدام لوحة المفاتيح أكثر من القنبلة"[1]، فيمكن بسهولة رسم سيناريوهات نموذجية بسيطة تعكس المخاوف الأمنية التي قد يحدثنا الإرهاب السيبراني، كالهجمات الموجهة إلى أنظمة الكمبيوتر التي تتحكم في شبكة كهرباء إقليمية كبيرة، ومن الأمثلة الأخرى كسر نظام مراقبة الحركة الجوية الدولي أو الإقليمي والعبثبخطط الطيران أو تغييرها، الامر الذي يمكنهممن أن يصطدم بسهولة طائرتين أو أكثر ببعضهم البعض[2].

في سياقات منية أخرى، وعلى الرغم من وجود أصداء تصل إلى جميع أنحاء العالم، فقد أثيرت مخاوف بشأن الاستخدام المحتمل للإنترنت لأغراض عسكرية إستراتيجية، تم تضمين هذه المخاوف في نقاش شديد التفصيل داخل دوائر الاستخبارات العسكرية الأوربيةوالتي أسست لجدل حول الطبيعة المتغيرة لهذه الهجمات السيبرانية، مصدر قلق رئيسي ثان هو فقدان سلطة الدولة وسيادتها بسبب الخصائص الفريدة للفضاء السيبراني، ولا سيما الاستخدام الواسع لتقنيات التشفير. في حين أن هذه الصورة الجماعية لها بالتالي عدة أبعاد مترابطة، فإن كل منها يدرك أن هدف الدولة هو الأمن.[3]

هذا القلق يأتي ضمن جملة المخاطر الأمنية تسعى التنظيمات الإرهابية إلى تحقيقها وهي تشكل جملة المخاوف الأوربية من إمكانيات وصول الجماعات الإرهابية لهذه التقنيةالمتطورة، ونبرزها في التالي[4]:

- إلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات، أو قطع شبكات الاتصال بين الوحدات والقيادات المركزية، أو تعطيل أنظمة الدفاع الجوي، أو إخراجها عن مسارها.
- التسلل الالكتروني إلى الأنظمة الأمنية في دولة ما، وفك الشفرات السرية للتحكم بتشغيل منصاتإطلاق الصواريخ الإستراتيجية، والأسلحة الفتاكة، وتعطيل مراكز القيادة و السيطرة العسكرية.

هذا الخطاب الأمني استحضرته وثيقة المفوضية الأوروبية لعام 2004 واعتبرته خطرًا افتراضيًا يتمثل في إمكانية الجمع بين النشاط الإرهابي التناظري والرقمي، مع ملاحظة أن "الإرهاب الإلكتروني يمكن أن يؤدي أيضًا إلى تضخيم آثار الهجوم المادي" مما يشير إلى الضرر يمكن أن تؤدي أنظمة الاتصالات إلى تفاقم أعداد الضحايا والذعر العام، استندت وثيقة المفوضية لعام 2009 التي دعت إلى استمرار التعاون في حماية

[1] Lene Hansen and Helen Nissenbaum, ***Op. cit***. p 1161.
[2] Jarkko Moilanen, ***Op.cit.***
[3] Deibert, Ronald J. ***Op.cit***, P-p: 115-142.
[4] خالد حسن أحمد لطفى، ***مرجع سابق***، ص 75-76.

البنية التحتية الحيوية على مستوى الاتحاد الأوروبي إلى التهديد المتمثل في "الأنشطة الإرهابية التي تستهدف البنى التحتية للمعلومات الحيوية وتأثيراتها الأمنية والسياسية"[1].

كما تجدر الإشارة الى أن الإرهاب السيبراني يمكن أن يكون بمثابة أداة للتدخل في الشؤون الداخلية للدولة وتعطيل العلاقات الدولية القائمة بينها. وبالتالي، يمكن الاستنتاج أن الإرهاب السيبراني الدولي هو ظاهرة سياسية يجب النظر إليها من جانبين[2]:

1. التدخل في الشؤون الداخلية للدولة من أجل الإضرار بسمعة الأداء الفعال لأجهزة الدولة ووجود القانون والنظام؛

2. إثارة التوتر في العلاقات بين الدول بهدف إثارة النزاعات الدولية: فالجماعات الإرهابية اعتمدت أساليب جديدة لخلق الفوضى على الساحة الدولية

عملياً، ينطوي كل هجوم إرهابي على استخدام نوع تكنولوجي جديد، سواء بصورة سطحية أو جوهرية. وقد استفادت الجماعات الإرهابية من عصر التقدم التكنولوجي لشن هجمات سيبرانية مركزة، وكسب مصادر تمويل جديدة، واختراق النظم وقواعد البيانات الآمنة، وقد مكنت وسائل التواصل الاجتماعي الجديدة، مثل المدونات والمنتديات وتطبيقات الاتصال، المنظمات الإرهابية من تبادل المحتوى والتواصل بجماهير عالمية، والتأثير في مجموعات مختارة من الناس يتبنّون الأفكار نفسها، وإعطاء القضايا المحلية بُعداً عالمياً، وخلق إرهابيين افتراضيين يؤثرون بصورة أو بأخرى ومن خلال خطاب أيديولوجي معين في قضايا تخص الشأن الدولي[3].

لا يقتصر الأمر على أساليب الدعاية والتجنيد فقط، بل ذهب الارهابيون بعيدا في استخدامات التكنولوجيا، ففي مقال نشرته مجلة "ديفينس وان/ DEFENSE ONE" لأستاذ العلوم الأمنية في جامعة جورج تاون دافيد غارتيستين روس Daveed Gartenstein-Ross، بعنوان "الإرهابيون سيستخدمون الذكاء الاصطناعي" (Terrorists Are Going to Use Artificial Intelligence) أشار إلى أن المجموعات الإرهابية ستستغل الذكاء الاصطناعي، وخاصة مع ازدياد إمكانية وصول الأفراد إلى تكنولوجيا التعلّم الذاتي، واستخدام آليات التشفير الحديثة، مشيراً إلى أن المحللين في السابق قد أخطأوا في تقدير قدرة عناصر الميليشيات

[1] Christopher Baker-Beall, Gareth Mott, ***Op.cit.***

[2] Аккаева Халимат Алиевна, МЕЖДУНАРОДНЫЙ КИБЕРТЕРРОРИЗМ КАК ПОЛИТИЧЕСКИЙ ФЕНОМЕН, Социально-политические науки 1, (2018), стр 138-140.

[3] وجدان فهد، ***مرجع سابق.***

على استخدام تكنولوجيا الطائرات المسيَّرة. فقد اعتقدوا أن سلاح الطيران سيكون قادراً على إسقاطها من السماء، ولكن المنظمات الإرهابية كانت ذكية بما يكفي، فعملت على تكييف طائرات مسيرة صغيرة جداً، تتناسب مع أغراضها الهجومية، دون إمكانية الكشف عنها من قِبل الرادارات.

وعلى غرار الطائرات المسيرة، فمن المرجح أن تصبح تكنولوجيا الذكاء الاصطناعي متاحة على نطاق واسع في الأسواق التجارية وبتكلفة منخفضة، وربما يبدأ الإرهابيون بتخطيط شبكات اجتماعية ورسم خرائط مفصلة عبر مواقع التواصل الاجتماعي. كما تشير التقديرات إلى أن التنظيمات المسلحة ستبني جيلاً جديداً من الطائرات المعتمدة على الذكاء الاصطناعي، لتصبح أكثر فتكاً وقوة، وربما يصل الأمر بهم إلى استخدام سيارات ذاتية القيادة لإرسالها في عمليات الاغتيالات بعد تفخيخها.

ويعتبر تنظيم "داعش" الارهابي" من أكثر الجماعات التي تضم عناصر أوروبية وأمريكية لديها خبرة في عالم الفضاءات الرقمية، الأمر الذي مكّنها من تنظيم العديد من الهجمات الإرهابية باستخدام التكنولوجيا، ما يعني أن الذكاء الاصطناعي يخفف الآن على الجماعات المسلحة الإرهابية عبء الحصول على المعلومات الاستخباراتية، ويُعَبِّد الطريق أمام عملياتهم لإثارة النزاعات بين الدول وتأجيجها، أو لأن تكون طرفا فيها[1]، الأمر الذي يولد أشكالًا جديدة من التوترات الدولية التي لا يمكن اختزالها في منطق الصراع التقليدي والمعضلات الأمنية التي ترتبط عادةً[2]، وهذا يعني أن القلق من أن الإرهابيين الذين قد يشنون هجمات إلكترونية ناجحة ضد البنية التحتية الحيوية داخل دولة عضو أو شريك في الاتحاد الأوروبي هو خطر استباقي يتماشى مع الأطر الموجودة مسبقًا أو الناشئة منها، حيث يعمل شبح الإرهاب السيبراني على تعزيز الروايات الأوسع نطاقاً المتعلقة بالحاجة إلى تحسين وتوحيد النهج على مستوى الاتحاد الأوروبي لتأمين الأنظمة الحيوية[3].

وهكذا كانت تكتيكات الإرهابيين في استخدام الذكاء الاصطناعي الذي بدأ بوسائل التواصل الاجتماعي وانتهى بطائرات مسيرة هددت العديد من المناطق في العالم، تلك التكتيكات المستحدثة قد كانت البداية لبلورة استراتيجيات إرهابية واسعة النطاق تشكل تهديداً للأمن العالمي ككل ليس الأوربي فقط[4].

---

[1] وجدان فهد، **المرجع نفسه.**

[2] Memphis Krickeberg, ***Op.Cit.***

[3] Christopher Baker-Beall, Gareth Mott, ***Op.cit.***

[4] وجدان فهد، **مرجع سابق.**

- **استهداف منظومة الدفاع والتهيئة:**

ويعد هذا السيناريو من اخطر السيناريوهات المحتملة التي قد تعصف بالأمن الاوربي وتبدأ المرحلة الأولى باختراق المنظومات الخاصة بالأسلحة الإستراتيجية ونظم الدفاع الجوي والصواريخ النووية فقد تتوفر لقراصنة المعلومات فرصة فك الشفرات السرية للتحكم بتشغيل منصات إطلاق الصواريخ الإستراتيجية والأسلحة الفتاكة فيحدث ما لا يحمد عقباه على المستوى العالمي[1]، كما بإمكان الجماعات الإرهابية قرصنة نُظم المعلومات الجغرافية بهدف الاستيلاء على معدات ضرورية (سفن، طائرات)[2].

كما كان التحقيق الدولي عن هجوم Stuxnet الناجح ضد نظام "SCADA "air-gapped والذي يشغل أجهزة الطرد المركزي لليورانيوم في مفاعل نطنز(Natanz) بمثابة تغيير تدريجي في الاحتمالات المتصورة للهجمات الإلكترونية ضد الأنظمة الأمنية البالغة الأهمية، فعلى الرغم من أن الدول الأوربية كانت على دراية بإمكانية حدوث مثل هذه الهجمات – باستخدام برامج الهجوم والدفاع الإلكترونية الخاصة بها – فقد وفرت حادثة" Stuxnet مزلاجًا استطراديا أسس له أول هجوم إلكتروني كبير تم الكشف عنه علنًا تسبب في ضرر حركي لبنية حساسة، قدمت الحادثة بعض الشرعية للمحللين للتحدث عن "الإرهاب السيبراني" دون اللجوء إلى الخيال العلمي أو التخمين، كما أثارت موجة من التعليقات داخل هيئات الاتحاد الأوروبي، فيما يتعلق بقدرة الإرهابيين الإلكترونيين على تدمير البنية التحتية الحيوية والتسبب في مزيد من الاضطراب الدولي العام[3]، خاصة ان كان مستوى تطوير البنية التحتية المشتركة مرتفعًا أيضًا كحال البنية الأمنية في اوربا، فإن احتمالية الإرهاب السيبراني تكون أعلى.[4]

- **التأثير على نظم التفكير العسكرية (فن العمليات والمذاهب العسكرية وأدوات القتال).**

بعد فهم وتحليل قدرة الجماعات الإرهابية على إجراء الاختراقات الأساسية ضد الأنظمة الفردية، المؤسسية وحتى الدولية باستخدام الأدوات السيبرانية، وشن هجمات أكثر تعقيدًا ضد أنظمة أو شبكات متعددة، وربما تعديل أو إنشاء أدوات قرصنة أساسية قادرة على إحداث اضطراب شامل ضد الدفاعات المتكاملة وغير المتجانسة[5]، وجب على المنظومة الأمنية والعسكرية للدول استيعاب وإعادة التفكير في حجم الخطر الذي قد

---

[1] كريمة شافي جبر، "الإرهاب المعلوماتي"، ***مجلة كلية الآداب***، العدد 96،(2011)، ص635– 658.

[2] إبراهيم بولمكاحل، ***مرجع سابق***، ص 151.

[3] Christopher Baker-Beall, Gareth Mott***, Op.cit.***

[4] Jarkko Moilanen, ***Op.cit***, p30.

[5] ***Ibid***.

يصاحب اغفال أو التقليل من قدرات الجماعات الإرهابية، لهذا تعمد المذاهب العسكرية على مواكبة هذه التطورات في حجم وشدة التهديدات عن طريق ابتكار فن عملياتي مستحدث يتماشى والواقع الأمني الذي يوفر بيئة مناسبة لنمو الجماعات الإرهابية والمتطرفة.

ففي فرنسا مثلا هناك عدد من أصحاب المصلحة الرئيسيين الذين يقع الذكاء الاصطناعي في دائرة اختصاصاتهم قد كُلفوا من طرف المنسق الوزاري للذكاء الاصطناعي بتحليل ووضع مقترحات للتغيرات المتعلقة بالابتكار الرقمي المطبق على المجال الأمني، كما توجد في وزارة الدفاع الفرنسية وحدة لتنسيق الذكاء الاصطناعي الدفاعي ضمن وكالة الابتكار الدفاعي، وتعمل فرنسا على تكييف إطارها القانوني للسماح باستخدام آمن وفعال للتقنيات التي تدعم الذكاء الاصطناعي لحماية السكان وكذا البنى التحتية الرقمية في فرنسا، وفيما يتعلق بالتطورات السياسية نشرت فرنسا استراتيجيتها للذكاء الاصطناعي في مارس 2018 ومن أهدافها الرئيسية تحسين النظام الأمني الإيكلوجي (العلاقة بين البيانات الامنية والمعلومات) لتعليم الذكاء الاصطناعي والتدريب عليه لتطوير أفضل مواهب الذكاء الاصطناعي وجذبها، وإنشاء سياسة البيانات المفتوحة لتنفيذ تطبيقات الذكاء الاصطناعي في المجالات العسكرية.

في حين أعلنت المملكة المتحدة في فبراير 2018 على استراتيجية امنية تهدف الى تطوير أداة بيانية قائمة على التعلم الآلي لكشف محتوى تنظيم "داعش" الارهابيعبر الإنترنت، وتمتدريب البرنامج على تحديد العناصر السمعية والبصرية التي يمكن التعرف عليها في المحتوى الدعائي تنظيم "داعش" الإرهابي والإشارة إليه، وقد قامت وزارة الداخلية بتكليف تلك الأداة البيانية بالتعرف على أشد فيديوهات تنظيم "داعش" الارهابيجرأة وترويعاً وأوضحت شركة تطوير البرمجيات التي صممت الأداة أن الأمر لا يتعلق بالحجم بقدر ما يتعلق بمدة تأثيرها الأمني حسب اعتقادهم في معالجة مجموعات معينة من مقاطع الفيديو[1].

يعكس ما سبق التأثير الأمني على الدول الاوروبية التي ترى في الإرهاب السيبراني خطرا محتملا مكّن له الترابط الرقمي للمجتمع والاقتصاد الأوروبي، والذي بدوره (يعيد) خلق زخم للتغييرات التي يقودها الاتحاد الأوروبي في الممارسة والتي تهدف إلى تقليل الضعف وجعل المخاطر قابلة للحكم بشكل متزايد[2].

[1] وجدان فهد، ***مرجع سابق.***

[2] Christopher Baker-Beall, Gareth Mott, ***Op.cit.***

خاتمة الفصل واستنتاجاته:

شهد العالم في السنوات الأخيرة تزايدا ملحوظا في اتساع دائرة التهديدات الإرهابية السيبرانية، والتي من شأنها أن تهدد أمن واستقرار الدولة القومية، كما يمكن لمتغير العولمة Mondialisation أن يجعل إفرازات هذه التحديات تتعدى الحدود الوطنية، جراء الانكشافية La Vulnérabilité التي خلفها التطور التقني المتسارع، خاصة مع بروز المجال السيبراني كبعد خامس تسعى الدول لبسط سيادتها عليه، وساحة جديدة للقتال، محصلة كل ذلك مجتمع للمخاطر العالمي مس كل الأصعدة الاجتماعية والسياسية والثقافية والاقتصادية والأمنية، حيث أصبح الأمن نسبيا، إلى أن انتقل الحديث عن حالة من "عسكرة" الفضاء السيبراني، وهو ما فسره هذا الفصل وخلص للنتائج التالية:

الاستنتاجات:

- وفقا للدراسة المسحية لبعض الهجمات الإرهابية في أوروبا نجد أن الإرهابيون يعتمدون بشكل متزايد على التكنولوجيا وشبكات التواصل الاجتماعي، كما يتم استخدام مواقع الويب والبريد الإلكتروني وغرف الدردشة ولوحات الرسائل الافتراضية لتجنيد أعضاء جدد ونشر الإجراءات وتوفير قاعدة إلكترونية للخطاب التنظيمي لتأمين اتصالاتهم.

- قيمت الدول الأعضاء في الاتحاد الأوروبي أن الإرهاب الجهادي لا يزال يمثل أكبر تهديد إرهابي في الاتحاد الأوروبي.

- يهدف المهاجمون عبر استخدام الفضاء السيبراني إلى أن يكونوا قوة سيبرانية مهمة قادرة على إنزال الأضرار النفسية والاقتصادية داخل المجتمعات الأوروبية لخدمة أهدافهم ومناصرة حلفائهم، وكذا التأثير على الوعي الديني وتحريك الهويات الفرعية، وعلى الرغم من وجود فجوة كبيرة بين طموحات المهاجمين وقدراتهم الفعلية على تحقيقها، إلا أن هذه الفجوة في طريقها إلى التقلص خاصة مع التحوّل من العمل الإرهابي الفردي إلى عمل جماعي منظم.

- أظهرت بعض الهجمات الإرهابية التي مست الأراضي الأوروبية قدرتها على التسبب بشكل مباشر أو غير مباشر في إلحاق الأذى على البنى السوسيو-سياسية والأمنية، على الرغم من درجة معينة من التحديد من خلال التركيز على العلاقة بين الإرهاب السيبراني والبنية التحتية الحساسة، والخطر المادي والافتراضي الذي يتمثل في إمكانية الجمع بين النشاط الإرهابي التناظري والرقمي، مع ملاحظة أن الإرهاب

الإلكتروني يمكن أن يؤدي أيضًا إلى تضخيم آثار الهجوم المادي، مما يشير إلى أن الضرر يمكن أن يمس أنظمة الاتصالات كما قد يؤدي إلى تفاقم أعداد الضحايا والذعر العام.

- لا يمكن نفي تأثير الهجمات الإرهابية السيبرانية، لكن يمكن القول أنه على الرغم من أن الإرهاب السيبراني لم يتم تعريفه بشكل قاطع من قبل الاتحاد الأوروبي، فقد تم التذرع بالتهديد كوسيلة لإضفاء الشرعية على الممارسات الأمنية الحالية والمستقبلية.

الفصـــل الثالـــث

الفصل الثالث: إشكاليات بناء الأمن الجماعي الأوربي (الانتقال من الأمن الصلب إلى الأمن الرخو)

المبحث الاول: تبلور الخطاب الامني الأوروبي بشأن الإرهاب السيبراني.

المبحث الثاني: محددات الأمن الجماعي الأوربي.

المبحث الثالث: الأمن السيبراني الأوربي بين ثغرات السياسات والتدابير التقنية والإجرائية.

تمهيد الفصل:

يهدف هذا الفصل إلى تقديم نظرة عامة على مشهد سياسي معقد ومتفاوت لإشكاليات بناء الأمن الجماعي الأوروبي، حيث يعتبر الأمن السيبراني من أهم التحديات التي تواجه الاتحاد الأوروبي في الوقت الحالي، فقي الوقت الذي تزداد فيه نسبة الهجمات الإلكترونية المتطورة بشكل ملحوظ على مؤسسات وشركات القطاع العام والخاص في الدول الأعضاء، تبرز حماية الأمن السيبراني كسلعة حيوية وجب على الدول الأوروبية توفيرها موازاة مع التطور التكنولوجي الحاصل وحمايته، الأمر الذي لا يعتمد فقط على التدابير التقنية والإجرائية المتعلقة بالحماية المتقدمة من الهجمات الإلكترونية، ولكنه يتطلب أيضًا تبني سياسات واضحة ومنسّقة على مستوى مؤسسات الاتحاد الأوروبي، عبر إعداد إستراتيجيات عملية لمواجهة التحديات السيبرانية المختلفة.

خاصة وأن أغلب الوحدات الأوروبية تعتبر الإرهاب السيبراني واحدا من أهم الأخطار والتحديات الأمنية التي تواجهها أوروبا وباقي دول العالم. ومن خلال ذلك برز خطاب أمني أوروبي يعالج هذا التحدي ويسعى إلى مكافحة الإرهاب السيبراني وتعزيز الأمن السيبراني في مختلف دول الاتحاد الأوروبي، وهذا ما سنسعى لإبرازه من خلال هذا الفصل.

المبحث الأول: تبلور الخطاب الأمني الأوروبي بشأن الإرهاب السيبراني.

يتناول هذا المبحث التطورات التي طرأت على الخطاب الأمني الأوروبي بخصوص الإرهاب السيبراني، والتي من خلالها باتت محددات التصور الأمني الأوروبي واضحة، وبالتالي تم التطرق إلى التفاعل الحاصل بين التهديد والبنى التحتية الرقمية الحرجة، ومعالجة ذلك في إطار دراسات الأمن الموسع، خاصة وأن أوروبا قد عرفت العديد من الهجمات السيبرانية التي جعلتها تطور خطابا أمنيا موازيا حيث تضافرت جهود القوى السياسية والاجتماعية والاقتصادية للترويج لخطاب أمني مفاده "فهم الإرهاب السيبراني كخطر ناشئ".

المطلب الأول: بنية الخطاب الأمني للدولة الحديثة (مقاربة نقدية).

إن تقفّي مسار تحول الأمن الدولاتي من التمركز State-centred نحو الأمن المجتمعي ودور خطاب الأمننة Securitization discourse في ذلك، ومحاولة إلقاء الضوء على تداعيات ذلك بالنسبة للسياسة العامة يعتبر من بين الانشغالات الأساسية لمختلف فواعل السياسة العامة في تجلياتها الداخلية والخارجية، كون الأمن يهتم بصيانة النظام العام الوطني والعالمي، باعتباره ركيزة البقاء بالنسبة لمجمل هؤلاء الفواعل، ومرادفا للمصلحة الوطنية[1].

تبعا لذلك، وبعد أحداث 11 سبتمبر 2001 التي أفرزت تهديدات جديدة وفاعلين جدد، سرعان ما تبعها وبشكل بارز خطاب أمني جديد في استراتيجيات الدول لمكافحة الإرهاب الدولي، كما كان هنالك أيضًا بُعد سياسي جديد للتركيز على الإرهاب السيبراني (المناقشات حول الأمن السيبراني) بما في ذلك أمن الفضاء الإلكتروني، بما يجذب دائمًا الجهات الفاعلة السياسية بأجندات تمتد إلى ما هو أبعد من القضايا المحددة والمطروحة، ولم يكن الجدل حول الإرهاب السيبراني استثناءً في هذا الإطار، حيث تضافرت جهود القوى السياسية والاجتماعية والاقتصادية للترويج لخطاب أمني مفاده "الخوف من الإرهاب السيبراني"، فمن منظور نفسي، يتم الجمع بين اثنين من أكبر مخاوف العصر الحديث في مصطلحي الإنترنت والإرهاب – الخوف من الضحية العشوائية العنيفة– فيمتزج ذلك بشكل جلي مع عدم الثقة والخوف من المخاطر التي صاحبت الثورة الرقمية.

كما يُنظر إلى التهديد غير المعروف على أنه أكثر تأثيرا من التهديد المعروف، على الرغم من أن الإرهاب السيبراني لا ينطوي على تهديد مباشر بالعنف، إلا أن تأثيره النفسي على المجتمعات يمكن أن يكون قويًا مثل تأثير القنابل الإرهابية، علاوة على ذلك فإن أكثر القوى تدميراً التي تعمل ضد فهم

[1] عادل زقاغ، "المعضلة الأمنية المجتمعية، خطاب الأمننة وصناعة السياسة العامة"، ***المجلة الجزائرية للسياسة العامة***، المجلد 1، العدد1 (سبتمبر 2011)، ص 60-72.

التهديد الفعلي للإرهاب السيبراني هي الخوف من المجهول ونقص المعلومات، أو الأسوأ من ذلك، الكثير من المعلومات المضللة.

هذا الوضع القائم الذي أوجدته حقيقة الإرهاب الإلكتروني كتهديد كرّس لخطاب أمنى شمل أبعادا عدة، فلم يصبح قضية مسيَّسة إلى حد كبير فحسب، بل أصبح أيضًا قضية مجزية اقتصاديًا، فظهرت صناعة بأكملها للتصدي لخطر الإرهاب السيبراني، كما أطلقت مراكز الفكر مشاريع مفصلة وأصدرت أوراقًا مثيرة للقلق حول هذا الموضوع الناشئ.

في سياق متصل، يقول ريتشارد كلارك Richard Clarke، منسق مكافحة الإرهاب السابق ورئيس مكتب أمن الفضاء الإلكتروني في البيت الأبيض: "**يمكن للإرهابيين الجلوس على جهاز كمبيوتر واحد متصل بشبكة واحدة ويمكنهم خلق سلوك عالمي**"، هذا السلوك ألزم الدول على وضع أجندات أمنية معينة في سياساتها العيا مخافة للاستجابة للتحديات الأمنية الناشئة التي أوجدتها تطورات الظاهرة الارهابية، كما حذر توم ريدجTom Ridge، مدير وزارة الأمن الداخلي في ملاحظة تمثيلية في أفريل 2003 قائلا: "**[إنهم] لا يحتاجون بالضرورة إلى قنبلة أو انفجار لعرقلة الاقتصاد أو إغلاق شبكة الكهرباء**"، هذه التحذيرات بالتأكيد تعبّر عن تأثير قوي على وسائل الإعلام والجمهور والإدارة[1].

ففي أوربا مثلا، وعبر مؤسسات الاتحاد الأوربي الذي يتكون من العديد من الوكالات المختلفة التي لها مصالح متنافسة واختصاصات مختلفة في مجال الامن، وباعتباره موقعًا للسلطة الخطابية، تماشيا مع التأثير العالمي للظاهرة الإرهابية، جرى البحث عن سبل الاتساق والاستجابة الكافيتين عبر مجموعة من الجهات الفاعلة المختلفة لتوفير خطاب مؤسسي مشترك وإطار عمل في مجالات الأمن السيبراني ومكافحة الإرهاب[2].

- تغييرات في النظام التنظيمي لأجهزة الأمن الوطني مع الإجراءات القتالية التي يستخدمها المهاجمون:

ان الهجمات الإرهابية الإلكترونية وما واكبها من خطاب رسمي مثير للقلق، مثل هذا الخطاب لديه القدرة على خلق "ذعر أخلاقي" جديد حول الإنترنت بالإضافة إلى تبرير المراقبة التدخلية لأنشطة المواطنين العادية على الإنترنت[3].

---

[1] Sanju Chaudhary, "Linkages between cyber terrorism and national security", ***International Peer Reviewed & Referred Scholarly Research Journal for Interdisciplinary Studies***, Volume 3, Issue 22. Released on 04/3/2015, p-p: 1389-1397, in: http://www.srjis.com/pages/pdfFiles/14671953634.%20SANJU%20CHAUDHARY.pdf

[2] Christopher Baker-Beall, Gareth Mott, ***Op.cit.***

[3] Aziz Douai, Technology and terrorism: Media symbiosis and the "dark side" of the web, in: Lorenzo Cantoni and James A. Danowski, ***Communication and Technology***, (Switzerland: De Gruyter Mouton, 2015), p :440.

علاوة على ذلك، فإن "الخوف من الإرهاب" ، مثله مثل الخوف من الجريمة، يؤثر على كل من السكان والقادة السياسيين من نواحٍ عديدة. لأن الخوف من الإرهاب يمكن أن يؤدي إلى الذعر العام و "الذعر الأخلاقي"، فإن شعور المواطنين العاديين بأنهم "تحت الحصار"، أو الشعور بأنهم عرضة لهجمات إرهابية لا يمكن التنبؤ بها، يمكن أن يؤثر على السلوكيات اليومية والحياة الاجتماعية لشعوب بأكملها في حين استخدم السياسيون هذا "الخوف من الإرهاب" لسن سياسات وتبرير الإجراءات التي تقيد الحريات المدنية.

التأثير الآخر لتلك الهجمات الإرهابية يكمن في إبراز قضية تحول التكنولوجيا إلى جبهة معركة جديدة بين الحكومات والشبكات الإرهابية،هذه الأخيرة تدرك تمامًا أن تقنيات الاتصال توفر طرقًا جديدة وفعالة للتواصل مع خلاياها، وتجنب الاكتشاف، وتنظيم هجمات جديدة مدمرة، وعلى نفس المنوال تدرك الحكومات والأجهزة الأمنية أن امتلاك التقنيات المتقدمة يمنحها ميزة على الإرهابيين من حيث الكشف والمراقبة والتصدي للأنشطة الإرهابية. ومع ذلك، تدرك هذه الحكومات والوكالات أن البنى التحتية التكنولوجية مثل شبكات الاتصالات الحيوية، معرضة للاستغلال والهجمات المفاجئة من قبل هذه الشبكات الإرهابية[1]، الأمر الذي يدفعها مطالبة بتحيين خطابها الأمني، قدراتها، واسنجابتها.

- **مساهمات مدرسة كوبنهاغن في تحليل خطاب الأمن السيبراني:**

في تسعينيات القرن الماضي، لم يكن منظرو الأمن السيبراني، مثل بوزانBuzan، ويفرWaever، ودي وايلد De Wilde ينظرون إلى الأمن السيبراني باعتباره تهديدًا وجوديًا للدول. ومع ذلك، ونتيجة لاعتماد المجتمعات البشرية المتزايد على الشبكات السيبرانية، أصبحت القضايا السيبرانية مؤمنة الآن، مما يشير إلى أن تجسيد هذه العملية يتم تسليط الضوء عليه من خلال تحليل السياسات والاستجابات المؤسسية والاستراتيجية[2].

هذا وتشير الخطابات التي تصف سمات الفضاء الإلكتروني على أنها ساحات محتملة لظهور تهديدات للأمن القومي إلى توسيع عملية الأمننة، بينما كان أمن الشبكات في نهاية الحرب الباردة أمرًا يخص قلة مختارة من خبراء الإلكترونيات، في النقاش الموسع اليوم، لا يمكن إنكار الدول والأفراد والشركات، أصبح الفضاء السيبراني حاسمًا للأمن[3]

في الخطاب الأمني، يتم تقديم قضية ما على أنها تشكل تهديدًا وجوديًا لشيء مرجعي معين،فتسمية أي تهديد على أنه وجودي يبرر استخدام تدابير غير عادية للتعامل معه، كان التذرع بالأمن هو المفتاح لإضفاء الشرعية على استخدام القوة، وفتح الطريق بشكل عام أمام الدولة للتعبئة أو الاستيلاء على سلطة خاصة،

[1] ***Ibid***.

[2] Luiza Cruz Lobato &Kai Michael Kenkel, "Discourses of cyberspace securitization in Brazil and in the United States", ***Revista Brasileira de Política Internacional***, 58(2), in: https://cutt.us/YjRuu (04|04\2022)

[3] ***Ibid.***

على سبيل المثال: استخدام التجنيد الإجباري والسرية والوسائل الأخرى المشروعة فقط عند التعامل مع "المسائل الأمنية"، فـ "الأمن" هنا هو نتيجة تحرك يأخذ السياسة إلى ما وراء القواعد المعمول بها، ويؤطر القضية على أنها فوق السياسة العادية، ولتسجيل فعل شيء ما يتم "أمننته"، المهمة هنا ليست تقييم بعض التهديدات الموضوعية التي تعرض للخطر بعض الأشياء، بل هي عمليات بناء فهم مشترك لما يجب مراعاته والاستجابة له بشكل جماعي باعتباره تهديدا،و"فعل كلام "Speech Act فالأمن هنا لا يشير الى شيء موضوعي أو مادي بل أصبح ذو مرجعية مؤسسة في الفاعل المؤمن، إنه ليس مثيرًا للاهتمام كعلامة تشير إلى شيء أكثر واقعية: إن الكلام نفسه هو الفعل[1].

وبالتالي، من المهم تحليل كيفية تنبيه الدول، التي تعمل كجهات فاعلة في مجال الأمننة، لمخاطر الهجمات الإلكترونية ومن ثم وضع أجندة محددة للتعامل مع التهديدات. في هذا السياق، فإن الحفاظ على فضاء إلكتروني آمن يضفي الشرعية على استخدام التدابير غير العادية، إن قدرة أي جهة فاعلة على أمننة قضية ما بنجاح تعتمد بشكل كبير على وضعها وفقًا لبوزان Buzan، تم إضفاء الطابع المؤسسي على الأمن إلى حد ما، وبالتالي، "يتم وضع بعض الجهات الفاعلة في مناصب السلطة بحكم كونها أصواتًا أمنية مقبولة بشكل عام، من خلال امتلاك القدرة على تحديد الأمن"، لذلك قد يبدو أن سياسة الأمن السيبراني التي تنتهجها الحكومات الأوروبية وسيلة مثالية للتعبئة، وربما أيضًا لإضفاء الشرعية على حركة الأمننة. في هذا الصدد، تعكس سياسات الأمن السيبراني في الوثائق الاستراتيجية، مثل الاستراتيجيات الوطنية واستراتيجيات الأمن السيبراني، عمليات تعريف الفضاء السيبراني كعالم يتطلب تدابير واستجابات أمنية[2].

بالنظر إلى ذلك، يتم تفعيل النهجين العسكري والمدني للأمن السيبراني من أجل تطبيق إطار العمل النظري لمدرسة كوبنهاجن على تحليلنا للأمن السيبراني. وبالتالي، في البلدان ذات النهج العسكري، يكون الهدف المرجعي فيها هو حماية البنى التحتية الحيوية والموارد الرقمية الحكومية، عادة ما تكون البلدان التي تطبق هذا النهج متقدمة من الناحية التكنولوجية ولديها اقتصادات أكبر وتعتمد بشكل كبير على الفضاء الإلكتروني، تبعا لذلك يكون الحفاظ على البنية التحتية الإلكترونية الحيوية شرطا رئيسيا للحفاظ على الأمن القومي. على العكس من ذلك، لا يوجد كائن مرجعي محدد تم تحديده من قبل البلدان ذات التوجه المدني. تعتقد هذه الدول أن المهاجمين الإلكترونيين الذين يسعون لتحقيق مكاسب مالية فورية أو يسعون لسرقة معلومات حساسة أو استفزازية نظرًا لأن التهديدات السيبرانية مرتبطة ارتباطًا وثيقًا بالأفعال الإجرامية، يختلف

[1] Ole Wæver, "Aberystwyth, Paris, Copenhagen New 'Schools' in Security Theory and their Origins between Core and Peripherym", Paper presented at the annual meeting of the International Studies Association, Montreal, March 17-20, 2004.

[2] Dusko Tomic and others,"Cybersecurity Policies of East European Countries,Handbook of Cyber-Development", Cyber-Democracy, and Cyber-Defense, pp 1-17, in: https://cutt.us/gWA8R (09|05|2021).

الكائن المرجعي الرئيسي من المعلومات الشخصية إلى الأداء السليم للمعلومات والمجالات الاقتصادية والاجتماعية وما يسمى بالقطاعات اللينة الأخرى[1].

مرحلة أخرى من عملية الأمننة هي قبول وإضفاء الشرعية على الإجراءات غير العادية التي تقدمها جهة الأمننة. لذلك، بناءً على هذا المنطق، يمكن النظر إلى المشاركة النشطة للمؤسسات العسكرية في إنشاء سياسة الأمن السيبراني وتنفيذها كإجراء استثنائي تتخذه الدول في عسكرة الفضاء الإلكتروني، الأمر الذي مرده الضغوط المتزايدة على الحكومات لتطوير خطابها الأمني وقدرتها على خوض الحروب وكسبها في هذا المجال، لذلك يجب اعتبار عسكرة الفضاء السيبراني حلاً وخطابا بديلا للدولة الحديثة استجابة لمختلف التهديدات السيبرانية[2]، خاصة وأن الدول الأوروبية أصبحت بيئة حاضنة لهذه التهديدات بفعل الرقمنة، رغم تطور استجابتها الأمنية ومرونتها، والتاريخ يثبت تكبد عديد الدول الأوربية الخسار الأمنية والاقتصادية جراء هذه الهجمات السيبرانية.

المطلب الثاني: تاريخ الهجمات السيبرانية في أوربا

شهدت أوروبا العديد من الهجمات السيبرانية على فترات متفرقة وأخرى متتالية، وكان أشهرها الهجوم الذي استهدف إستونيا في 2007، ثم تلته هجمات أخرى تتفاوت من حيث الشدة والخطر والتأثير الناتج عنها. وكانت الهجمات الإرهابية عبر الانترنت تهديدا لا يقل خطورة، فقد تعرض العديد من دول الاتحاد الأوروبي إلى هذا النوع من الهجمات في ظل تطور وسائل العمل الإرهابي ونشر الفكر المتطرف المتعدد الخلفيات، ويمكن ذكر بعض من أشهر الهجمات الإلكترونية التي تعرضت لها دول الاتحاد الأوروبي كما يلي:

<u>هجمات إستونيا سنة 2007:</u>

من أشهر الهجمات التي شهدتها دول الاتحاد الأوروبي هجمات موزع الخدمة في إستونيا سنة 2007، وكانت عبارة عن "هجمات قطع موزع الخدمة واسع النطاق على المواقع الإلكترونية الإستونية في إطار التوترات مع روسيا"، فكان أن اتُّهمت روسيا بمسؤوليتها عن تلك الأحداث[3].

كانت شرارة الهجمات قيام إستونيا بنقل تمثال الجندي البرونزي (النصب التذكاري لمحرّري تالين) من وسط المدينة إلى مقبرة عسكرية، مما أدى إلى احتجاجات عارمة تلاها هجمات على المواقع الإلكترونية للحكومة والبنوك وغيرها4. فقد أطلق الرعايا الروس في 2007 "هجمات رفض الخدمة الموزعة" (DDoS)

---

[1] K. Griffith, ***Op,cit***. p.13.

2Dusko Tomic, ***Op,cit.***

[3] جون إس.ديفيس الثاني واخرون، ***تهديدات مجهولة المصدر: نحو مساءلة دولية في الفضاء الإلكتروني***، (كاليفورنيا: منشورات مؤسسة راند، 2017)، ص07.

[4] K. Griffith, ***Op,cit***. p.13.

ضدإستونيا، مما تسبب في تعطيل خدمات الانترنت لمدة قاربت ثلاثة أسابيع، وأتىذلكعلىإثرالنزاعالروسي-الجورجيحولأوسيتياالجنوبية[1].

هجمات أوكرانيا:

أوكرانيا من الدول التي تعرف هجمات كثيرة وباستمرار، في 2015، هاجت روسيا دولة أوكرانيا سيبرانيا من خلال محطات توزيع الطاقة، وبالتالي انقطاع الكهرباء عن 225 ألف مواطن غرب أوكرانيا، وفي 2017 أيضا استخدمت برنامج الفدية "نوت بيتيا" (NotPetya) لضرب أوكرانيا قبل أن يأخذ هذا البرنامج بُعدَه العالمي وتكون له تأثيرات تتعدى حدود وقدرات الدول، وهو ما تكرر في جانفي 2022 عبر برنامج "ويسبرغات" (WhisperGate)الذي يستهدف البيانات، والذي قيل عنه إنه شبيه بسابقه (NotPetya) ولكنه أقل قدرة على الانتشار الواسع[2]. فقد اتهمت أوكرانيا روسيا بالتسبب في تعطيل 70 موقعا حكوميا قبل عودة الخدمة بعد ذلك بساعات، وهو ما أتى نتيجة للاستقطاب الغربي المتواصل لأوكرانيا في ظل مساعي انضمامها إلى الناتو[3]. وكذلك في 2016 عرفت هجوما سيبرانيا استهدف محطات توزيع الطاقة والكهرباء، مما أدى إلى انقطاع الكهرباء عن 225 ألف مستخدم حينها، وكانت روسيا المتهم الأول في ذلك[4].

هجمات TV5Monde بفرنسا:

عرفت القناة الفرنسية "تي في 5 موند (TV 5Monde) "في 8 ابريل 2015 هجوما أدى إلى انقطاع البث لمدة 18 ساعة، وتم اختراق حساباتها على منصات التواصل الاجتماعي، وعُدَّ تنظيم "داعش" الإرهابي المسؤول عن ذلك مما أثار هاجسا أكبر لدى الحكومات الأوروبية بخصوص القدرات السيبرانية للتنظيمات الإرهابية[5].

هجمات برامج الفدية:

شكلت الفترة: 2016-2017 نقطة فاصلة في ملف الأمن السيبراني ومكافحة الإرهاب السيبراني في الاتحاد الأوروبي، نتيجة الهجمات التي تعرّض لها على غرار دول كثيرة عبر العالم وعُرفت بهجمات برامج

---

[1] Luukas K. Ilves, and Others, "European Union and NATO Global Cybersecurity Challenges: A WayForward", PRISM, Vol. 6, No. 2 (2016) in: https://www.jstor.org/stable/10.2307/26470452 (04|11|2021)

[2] إيمان الشامخ، "بلا قنابل أو أسلحة.. هكذا يمكن لروسيا تدمير البنية التحتية في أوكرانيا"، موقع الجزيرة، في: (2022/02/22) https://bit.ly/36u9Y8S

[3] Joe Tidy, "Ukraine cyber-attack: Russia to blame for hack, saysKyiv", BBC,14 January, in: https://www.bbc.com/news/world-europe-59992531(22/02/2022)

[4] ديفيس الثاني واخرون، ***مرجع سابق***،ص08.

[5] ***المرجع نفسه***، ص: 07 و13.

الفدية، فهجوم "واناكراي" مثلا تسبب في تعطيل عمل 200 ألف جهاز كمبيوتر يعمل بنظام WindowsXP في أكثر من مائة (100) دولة، مما أثر في قطاعات عديدة من بينها الصحة والنقل والسياحة[1]. ومسّت الهجمات أكثر من ثلث خدمات الصحة الوطنية في بريطانيا على سبيل المثال[2]. ففي 12 ماي 2017 حدثت هجمات واسعة باستخدام برامج خبيثة على غرار "وانكراي" (WannaCry)، أدت إلى تعطيل عشرات الالاف من أجهزة الحاسوب عبر العالم، وذكر اليوروبول أن الهجمات السيبرانية مسّت العديد من الدول منذ بروزها، وذلك راجع إلى استغلال الثغرات في الفضاء الإلكتروني وأنظمة التشغيل على غرار "مايكروسوفت ويندوز"، وتعد برامج الفدية (نسبةً إلى اشتراط دفع فدية مقابل عودة الخدمة الإلكترونية) على درجة عالية من الخطورة لكونها مسّت مؤسسات وشركات أوروبية كبرى مثل "رونو" الفرنسية لتصنيع السيارات، وأيضا محطات القطار في ألمانيا من خلال استهداف اللوحات الإلكترونية التي تُظهر مواعيد السفر[3]. بالتالي، تصنف هذه الهجمات كهجمات عالمية، حيث إن هجوما مثل "WannaCry" استهدف خدمات الرعاية الصحية والنقل والبنية التحتية للاتصالات للعديد من الدول عبر العالم، واتهمت روسيا الولايات المتحدة في ذلك[4].

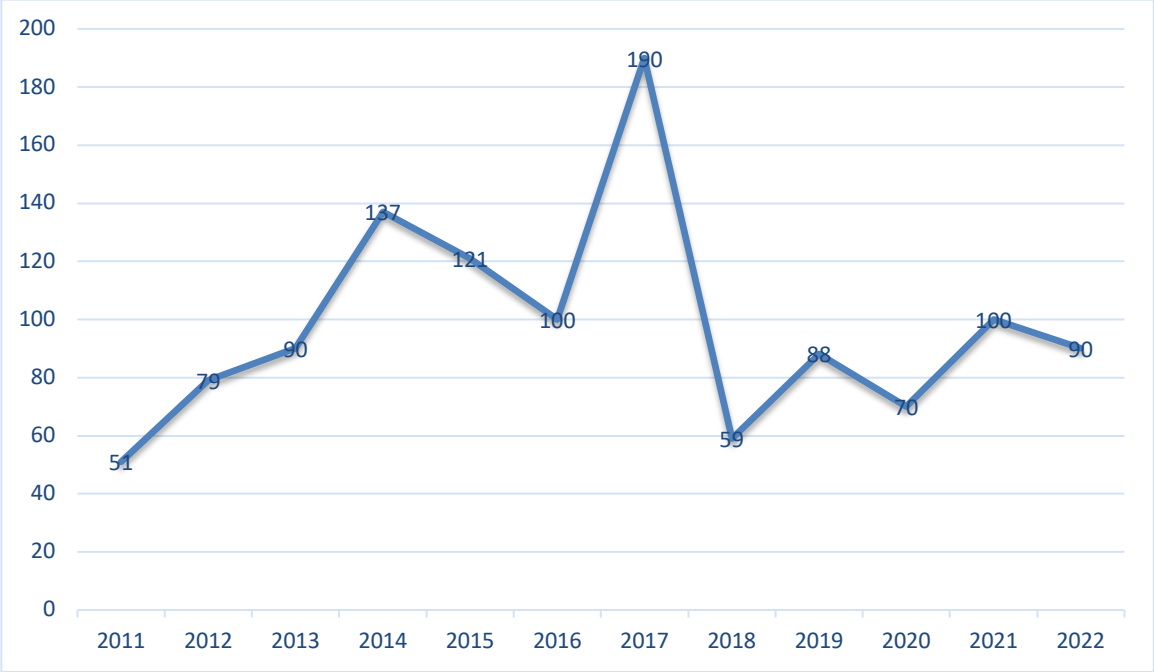
[1] Melissa K. Griffith, and Others, Strengthening the EU's Cyber Defence Capabilities, Report of a CEPS Task Force, Centre for European Policy Studies (CEPS) Brussels (November 2018), p-p: 10-11.

[2] ***Ibid***, p.14

[3] "أسرار أكبر هجوم إلكتروني في التاريخ استهدف 100 دولة"، 2017/05/13، https://bit.ly/3H0kQb6 (2021/11/24)

[4] ديفيس الثاني واخرون، ***مرجع سابق***، ص08.

الشكل (8): الحوادث الكبرى المعلن عنها من قبَل الوكالة الأوروبية لأمن الشبكات والمعلومات



المصدر: من إعداد الباحث، بناء على تقارير واحصائيات وكالة الأمن السيبراني (ENISA) والمفوضية الأوربية.

يوضح الشكل تطور الهجمات السيبرانية في دول الاتحاد الأوروبي من حيث العدد المعلن عنه من قبَل وكالة الأمن السيبراني (ENISA)، وتقارير المفوضية الأوروبية، وذلك خلال الفترة المذكورة أي: 2011-2022،سنة 2011 لأنها السنة الفارقة في الأحداث السياسية بداية الثورات العربية وموجة الانعكاسات التي مست كل الدول، وأوروبا ليست بمعزل عنها، خاصة موجات الهجرة وما صحبها من خطاب متطرف الذي كان سببا في بعض الهجمات الإرهابية على الأراضي الأوربية، فالأزمة السورية مثلا مسّت البنية المجتمعية الأوروبية من خلال التفاعلات المتنوعة التي أفرزتها الظاهرة الإرهابية في الشرق الأوسط (التجنيد، التمويل والتدريب عبر منصات التواصل الاجتماعي)، كما يبرز ارتفاع عدد هذه الهجمات بصورة تصاعدية بين عامي 2016 حتى منتصف عام 2017، ومرد ذلك تصاعد خطاب الكراهية من اليمين المتطرف، كما تجدر الإشارة إلى أن اكبر موجات اللجوء لأوروبا كانت خلال هذين السنتين، وما يراه هؤلاء بخصوص الغرب (الكافر) والمتسبب في خراب بلدانهم، وهو ما حفّز أكثر فأكثر الانخراط في أنشطة عدائية هناك، فكان أن ارتفع معدل الإرهاب السيبراني والجريمة الإلكترونية باختلاف أنواعها، كما يمكن إرجاعه إلى انتشار التطور التقني فيما يتصل بمجال المعلوماتية، الأمر الذي سمح لمجرمي الفضاء السيبراني بالتعدي على قيم وخصوصية الفضاء السيبراني ككل، دون إغفال تأثيرات العامل الخارجي ومن بينها مشكلة عودة المقاتلين الإرهابيين الأجانب (FTF) إلى دُول المنشأ.

يذكر الباحث "ريمي رافال Rémi Ravel بعض الأمثلة التي تبرز خطورة الهجمات والتهديدات السيبرانية التي تحدث عبر الفضاء السيبراني، مثل إستونيا التي تعرضت إلى هجمات واسعة في 2007، إضافة إلى الهجمات التي تعرضت لها أوكرانيا في 2017، حينما أدى ذلك إلى تعطيل أكثر من 70 بالمائة من أجهزة الحاسوب، بهدف التأثير في البنى التحتية الحرجة كالطاقة والنظام البنكي[1] .

وقد أدت هجمات مثل Mirai botnet و WannaCry وNotPetya إلى زيادة التركيز على الأنشطة السيبرانية الضارة وتأثيرها المحتمل على الاستقرار في الفضاء السيبراني، وفي المقابل استمر النقاش حول تطبيق القانون الدولي في هذا الفضاء، ومعايير سلوك الدولة المسؤول، وتدابير بناء الثقة في منظمة الأمم المتحدة ومنظمة الأمن والتعاون في أوروبا (OSCE)، وعلى الرغم من التقدم الكبير الذي أحرزته مجموعة الأمم المتحدة للخبراء في 2013و2015 لم تتم معالجة قضايا مثل العناية الواجبة من جانب الدول واستخدام التدابير المضادة، وفي عام 2018 لم تعلن سوى دول قليلة (كالولايات المتحدة والمملكة المتحدة وأستراليا) مواقفها بشأن تطبيق القانون الدولي في الفضاء السيبراني، وعلى الصعيد الأمني استمرت النقاشات داخل منظمة الأمن والتعاون في أوروبا، واعتُمدت مجموعة من أدوات الدبلوماسية السيبرانية في الاتحاد الأوروبي[2].

ويعد الإرهاب السيبراني تهديدا أمنيا خطيرا للدول الأوروبية، فقد عرفت دول عديدة تأثيرات كبيرة لظاهرة الإرهاب عبر الانترنت، ومن ذلك أنّ "قضية الهجمات التي ضربت فرنسا، كانت الدعوة إليها عبر الإنترنت، وتمت من خلال دعوة منظمات إرهابية للانتقام من إعادة نشر رسوم شارلي إيبدو[3].

المطلب الثالث: أمن الدولة الأوروبية في عصر الرقمنة.

تعيش الدول الأوروبية اليوم هاجس بلوغ الحد الأقصى من الأمن لما يتعلق الأمر بالتهديدات الإرهابية السيبرانية، ويقع على عاتقها بالتماشي مع ذلك تكييف سياساتها وإستراتيجياتها لاحتواء التهديدات غير التقليدية، كما أن الاعتمادية المتزايدة للمجتمعات الأوروبية على تكنولوجيا المعلومات أسس لظهور شكل

[1] Rémi Ravel, ***La Cyber-Coopération Européenne***, Les publications des jeunes IHEDN (Rapport, 2018), p.17.

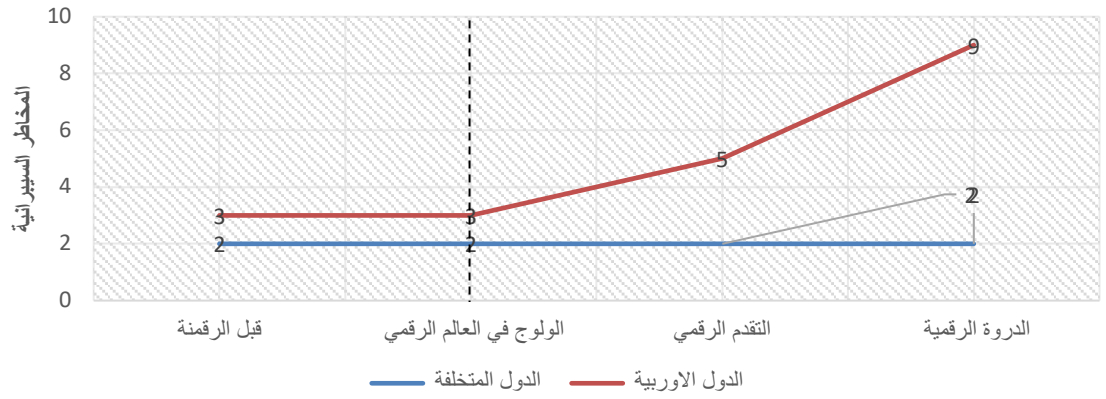
[2] Patryk Pawlak and Nathalie Van Raemdonck, "What if…the Sun led to a Cyberwar?", in Florence Gaub (Editor), "What If…? Scanning The Horizon: 12 Scenarios For 2021" (Paris: European Union Institute for Security Studies (EUISS), January 2019), p-p: 22-26. in: https://cutt.us/iVc4i

[3] جاسم محمد، "صناعة الكراهية داخل أوروبا... منصات التواصل الاجتماعي تؤجج العنف، دور الاتحاد الأوروبي محدود في إعادة تأهيل الإرهابيين"، 2021/06/17، https://bit.ly/3pjEQ2h(2021/12/15)

جديد من الضعف، مما قد يعطى الإرهابيين فرصة للاقتراب من الأهداف الحيوية مثل أنظمة الدفاع الوطني وأنظمة التحكم في حركة المرور الجوية.

فكلما كان البلد أكثر تطورًا من الناحية التكنولوجية، أصبح أكثر عرضة للهجمات الإلكترونية ضد مجتمعه وبنيته التحتية، ومن ثم فإن القلق بشأن الخطر المحتمل الذي يشكله الإرهاب السيبراني له ما يبرره. وهو ما يوضحه الشكل التالي:

الشكل 9 :قابلية العطب داخل الدولة قبل وبعد الدخول في العالم الرقمي



المصدر: من اعداد الباحث.

نلاحظ من خلال المخطط أن الدول الأوروبية وبالموازاة مع مسارات العولمة فهمت وفق مؤسسات الاتحاد الأوروبي –باعتباره فاعلًا سيبرانيا إقليميًا متماسكًا– ان الاعتماد على خدمات الأتمتة في كل القطاعات، وكذا على أنترنت الأشياء ينطوي على مخاطر عدة قد تحدث ضعف أكبر مما يجعل بنيتها التحتية قابلة للعطب، الأمر الذي يجعل أمنها الوطني والجماعي معرض لكل أصناف التهديدات السيبرانية عكس الدول الأخرى التي لم تخض في ضروب العولمة، مما يدفع الدول الأعضاء في **(EU)** إلى مراعاة العلاقة العكسية بين الازدهار والمخاطر. تماشياً مع الثورة الرقمية والتطورات الناتجة عنها[1].

[1] Christopher Baker-Beall, Gareth Mott, ***Op.cit.***

في هذا الإطار، من الضروري بالنسبة للأمن الوطني للدول الاوربية أن يتضمن العناصر [1]:

- **النسبية:** فالأمن نسبي، والدولة لا تكون قادرة دوما على تحقيقه دون الانخراط في التعاون الدولي.
- **المرونة:** بما يسمح له بمواكبة التحولات المستقبلية.
- **وضوح مصدر التهديد:** فمعرفة مصدر التهديد والتحدي، أو معرفة العدو، في الحاضر والمستقبل أمر ضروري لبناء الإستراتيجية.
- **التحكم الجيد والاستثمار في عوامل القوة على اختلافها.**

هذه العناصر أو الخصائص هي التي تجعل تصوّر الدولة لأمنها مطاطيا، مواكبا لكل التحولات والمستجدات، وإن كان الفضاء السيبراني يطرح إشكاليات أكبر تتعلق بغياب الحدود وتراجع مفهوم السيادة، والتعامل مع عدو مجهول الهوية أحيانا، خاصة وأن الفواعل في هذا الفضاء متنوعة (دولاتية وغير دولاتية في صورة أفراد وجماعات وتنظيمات عابرة للحدود الوطنية).

وقد تفطّنت الدول الأوروبية إلى حجم التهديد الذي يطرحه الفضاء السيبراني، فقامت بإدراجه في أجندة أمنها الوطني، لأن التهديدات التي تأتي من خلال هذا الفضاء تطرح تحديات أمنية واقتصادية كثيرة[2]، وذلك بالنظر إلى أن معظم الخدمات والبنى التحتية والمعلومات والأنظمة المالية ترتبط بالإنترنت[3].كما كيّفت الدول الأوروبية، على غرار إستونيا وفرنسا، رؤيتها الأمنية مع التهديدات الجديدة بعد أن عرفت إستونيا هجوما إلكترونيا في سنة 2007 مسّ مواقع حكومية وتضمّن حرمانَها من الخدمة[4].

جراء هذا أصبح أمن الدولة في عصر الثورة الرقمية شديد النسبية، وفي هذا السياق تناول كتاب "مستقبل العنف" لبنجامين ويتس Benjamin Wittes، وغابرييلا بلوم Gabriella Blum نواحي تأثير التطور التكنولوجي على الأمن القومي وعلى العلاقات الدولية، يحاجج الكاتبان على اعتبار شبكة الإنترنت

---

[1] محمد سعيد آل عياش الشهراني، ***أثر العولمة على مفهوم الأمن الوطني: دراسة مسحية على مجموعة من الأكاديميين في الرياض***، أطروحة ماجستير في القيادة الأمنية، قسم العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية. (2006)، ص 70-71

[2] Lior Talansky, Basic Concepts in Cyber Warfare, ***Military and Strategic Affairs***, Vol.03, N 1, (2011), p 79.

[3] محمود بريود، ***السيبرنيطيقا (السيبرانية): علم القدرة على التواصل والتحكم والسيطرة***،ط1 (*لبنان: المركز الإسلامي للدراسات الإستراتيجية، 2019*)، *ص 95.*

[4] لطفي لمين بلفرد ، الفضاء السيبراني: هندسة وفواعل، ***المجلة الجزائرية للدراسات السياسية***، المجلد *3*، *العدد 1*، (*2016*)، *ص: 145-154.*

"قادرة على إنتاج بيئة من الحرية غير المسؤولة" فتحت الباب لتهديدات جديدة متصلة بالتكنولوجيا نجحت في تحويل طبيعة العنف إلى نقطة أصبح فيها التمييز بين الأمن واللامن أقل وضوحا"[1]، بكون الفضاء السيبراني وسيلة ومسرحا لها، يؤسس هذا للعلاقة الوطيدة بين الأمن القومي والأمن السيبراني بكل صوره.

ووفقا لرونالد ديبير Ronald J. Deibert هناك أربع صور جماعية للأمن في بيئة الإنترنت(:الأمن القومي،الأمن السيبراني، الأمن الخاص، والعلاقات الدولية)، يمكن استخلاص استنتاجين بشأن العلاقة بين أمن الدولة والأمن السيبراني،والعلاقات الدولية من هذا المثال[2]:

- الترابط العالمي لا يقوض اعتبارات أمن الدولة القومي،كما أن التكنولوجيا نفسها لا تنشئ تلقائيًا شكلاً "عالميًا" جديدًا للأمن.
- ينقل الأمن السيبراني قضايا الأمن القومي إلى مجالات ومستويات جديدة، وبالتالي يتطلب النظر إلى أمن الدولة من خلال عدسات أخرى غير منظور الحرب أو أنواع المواجهات العنيفة الأخرى.
- أخيرا، يبدو أن تغييرًا جذريًا نموذجيًا يتعلق بوضع الدولة في العلاقات الدولية ينبثق من خطابات الأمن السيبراني.

بناء على ما سبق، يمكننا القول أن تحديد المسار الرئيسي للخطاب الأمني ظل متسقا مع تهديد الإرهاب السيبراني، وعبر تسليط الضوء على العديد من الخصائص الرئيسية التي تحاول الدول الأوروبية تقريب وجهات النظر من خلالها لكي تؤسس تصورًا وفهمًا مشتركًا للإرهاب السيبراني باعتباره نوعا هجينا من الهجمات الإرهابية، وتهديد متزايد للمجتمع الأوروبي، ولقيم الديمقراطية ايضا، تهديد لا حدود له في طبيعته، محتمل، لم يتحقق بعد بالقوة التي يصور بها، خطاب تعمل الدول الأوروبية من خلاله لتأمين الكائن المرجعي الأساسي (البنية التحتية الحيوية)[3]، فالخطاب الذي يحدد قابلية تعرض البنية التحتية الحيوية لحادث إرهابي إلكتروني محتمل يعتبر بمثابة منطق أساسي لإعادة إضفاء الشرعية على الممارسات الأمنية الأوسع المتعلقة بالأمن السيبراني ومكافحة الإرهاب على التوالي.

---

[1] عبد العليم، أحمد، (2015)، تهديدات غير تقليدية: مستقبل العنف في ظل التطورات التكنولوجية، المستقبل للدراسات والابحاث المتقدمة:https://bit.ly/3o0aOip(28|05|2021)

[2] Memphis Krickeberg, The Internet as a Slippery Object of State Security: The Problem of Physical Border Insensitivity, Anonymity and Global Interconnectedness, ***JOURNAL OF INTERNATIONAL AFFAIRS***, 2016, VOL. 2015/2016 Issue. 2, Pp 33-34, in:
:https://issuu.com/interstate1965/docs/20152016__issue_2_-_the_cyber_issue

[3] Christopher Baker-Beall, Gareth Mott, ***Op.cit.***

المطلب الرابع: البنية التحتية الحرجة: الفجوة الرخوة للأمن والتكنولوجيا في المنطقة الأوربية.

كانت الجهود التي بذلها صانعو السياسة في الاتحاد الأوروبي لتعريف الإرهاب السيبراني مدفوعة إلى حد كبير بتراكمية الأحداث الأمنية العالمية،فكان هجوم Stuxnet عام 2010، والمنسوب إلى الولايات المتحدة والموجه ضد إيران، هو الذي سلط الضوء على إمكانية التعرض للهجوم على أنظمة الكمبيوتر المرتبطة بالبنية التحتية الحيوية في الاتحاد الأوروبي.

في هذا الشأن، نصت ورقة مناقشة من منسق الاتحاد الأوروبي لمكافحة الإرهاب، في نوفمبر 2010، بوضوح على أن "حادثة Stuxnet قد أظهرت مرة أخرى أن البنى التحتية الحيوية يمكن أن تكون عرضة للهجمات على مكونات البنية التحتية الحرجة"، وأن "الإرهاب السيبراني والهجمات الإلكترونية عبر الإنترنتجذابة للجماعات الإرهابية للأسباب نفسها التي تجذب المجرمين أو غيرهم، وبالتالي كان من المهم أن يبدأ الاتحاد الأوروبي استعدادته قبل أن يكتسب الإرهابيون المعرفة أو القدرات لاستهداف بنيتنا التحتية"[1].

- **تعريف البنية التحتية الحرجة:Critical Infrastructure(CI)**

تعني في مجملها: "مجموعة من المنتجات والخدمات والعمليات الضرورية التابعة لعمل الدولة، وأنها ينبغي أن تكون آمنة وأن تتمكن من الصمود ومن التعافي بسرعة من جميع المخاطر المستحدثة"[2].

ويعرّف المجلس الأوروبي البنى التحتية الحيوية (CI) بأنها: "أصل أو نظام أو جزء منه موجود في الدول الأعضاء، وهي أمر ضروري للحفاظ على الوظائف المجتمعية الحيوية، والبنى المتعلقة بالصحة أو السلامة أو الأمن أو الرفاه الاقتصادي والاجتماعي للأشخاص، وتعطيلها أو تدميرها يكون له تأثير كبير في دولة عضو نتيجة الفشل في الحفاظ على تلك الوظائف"، معنى ذلك أن البنى التحتية الحرجة تعرّف على نطاق واسع بأنها الأصول الأساسية للوظائف الأساسية للمجتمع والتي من شأنها أن تسبب تأثيرًا خطيرًا إذا توقفت عن العمل، كما حدد المجلس الأوروبي مفهوم "البنية التحتية الأوروبية الحرجة" (ECI) ليعني "البنية التحتية الحيوية الموجودة في دول الاتحاد والتي سيكون لتعطيلها أو تدميرها أثرٌ كبير اقتصاديا واجتماعيا وأمنيا"، الامر الذي يجعل حجم الخطر مضاعَفا مستوى الترابط العالي بين الشركات المسؤولة عن البنى التحتية الحرجة وتكنولوجيا المعلومات والاتصالات، فبنية المعلومات الحرجة في الاتحاد الأوروبي تعتبر من الجوانب المهمة والحيوية في المجال السيبراني، وبالتالي تستدعي من الاتحاد ومن الدول الأعضاء حمايتَها[3].

---

[1] ***Ibid***.

[2] ميليسا هاثاواي، ""إدارة الخطر السيبراني الوطني"، https://cutt.us/rb3WF (11.12.2021)

[3] Mario Nicolas Castellon Machado, ***Cyber Security Governance: Securing the European Union's Cyber Domain*** , Master's Dissertation in Crisis and Security Management Programme (Leiden University : Faculty of Governance and Glabal Affairs, August 2015), p : 32, 36.

واليوم، أصبحت الأنظمة الأمنية والصناعية مدفوعة بشكل متزايد رقميًا، مما يعرضها للهجمات الإلكترونية، وفي مواجهة المخاطر المتزايدة فإن معرفة أساسيات الأمن السيبراني الصناعي فضلاً عن المصطلحات الفنية المتعلقة به، يعد شرطًا أساسيًا ضروريًا للتمكن من التعامل بشكل فعال مع التهديدات، بالنسبة للمصنعين تتعلق المخاطر الإلكترونية الرئيسية بوحدات الإنتاج التي يمكن للهجوم السيبراني بالفعل تعطيلها أو إتلافها أو حتى إيقافها، مع خسائر مالية فادحة في كثير من الأحيان، وفي بعض الحالات، آثار بشرية وبيئية[1].

تعد بيئة أنظمة التحكم الصناعي والإشرافي واكتساب البيانات ICS-SCADA هي المكون الأساسي للبنى التحتية الأوروبية والوطنية، تعتمد معظم القطاعات الأوروبية عليها لضمان مراقبة العملية والسلامة التي تضمن استمرارية الوظائف الحيوية الوطنية، حيث تعتمد القطاعات الحيوية مثل الطاقة والنفط والغاز والمياه أو المواد الكيميائية على أنظمة التحكم الصناعية للإشراف على عملياتها الرئيسية والتحكم فيها. نظرًا لأن الصناعات تميل إلى أتمتة العمليات والعمليات الخالية من الصيانة، فإن دور ICS-SCADA في جانب استمرارية الأعمال في تلك القطاعات يكون أكبر.

إن التحرك نحو ربط ICS-SCADA ببيئات تكنولوجيا المعلومات يؤدي إلى زيادة إمكانية حدوث الهجوم، وبالتالي تعريض الوظائف الحيوية لمخاطر أمنية أكبر على الإنترنت. تنتج أولوية أمن ICS-SCADA من التأثير الكبير على الوظائف الحيوية الوطنية والأوروبية، مما قد ينتج عن الترابط بين البنى التحتية الحرجة عبر الاتحاد الأوروبي تأثير متتالي وكبير في حالة هجوم إلكتروني ناجح.

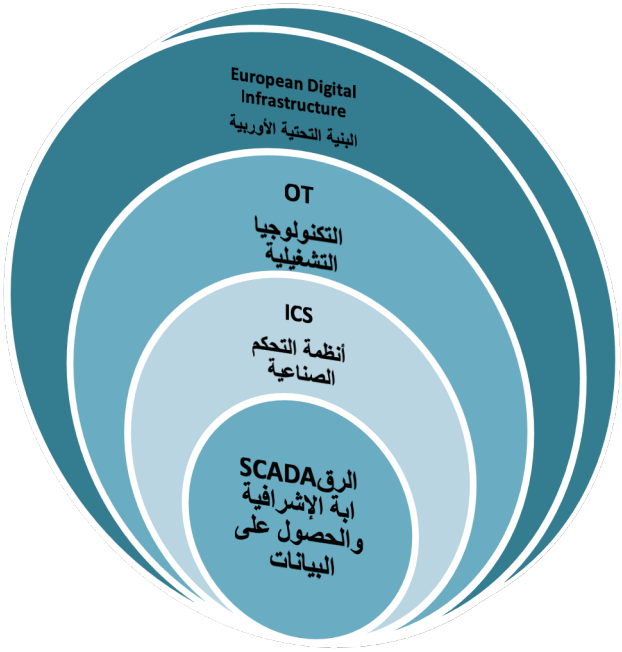
من ناحية أخرى، أصبحت الهجمات الإلكترونية أكثر قوة وتستهدف تقنيات أنظمة تحكم محددة، ثغرة Aurora وStuxnet هي أمثلة على الهجمات المتقدمة والمجهزة جيدًا، والتي كانت مخصصة لاستغلال نقاط الضعف غير المعروفة لأنظمة التحكم الخاصة[2]، يبين الشكل التالي البنية التشغيلية للنظام الذي تعمل به أوروبا.

---

[1] Khobeib Ben Boubaker ,"SCADA et cybersécurité industrielle : de l'importance de maîtriser le jargon,"sur: https://cutt.us/zGH0t(18| 11| 2021)

[2] Rossella Mattioli, Konstantinos Moulinos, ***Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors*** (Greece: ENISA, 2015), P.10.

الشكل (10): الكيانات التشغيلية للبنية التحتية الرقمية الأوروبية



المصدر: من إعداد الباحث

تشير **التكنولوجيا التشغيلية** (OT) إلى أنظمة الحوسبة المستخدمة لإدارة العمليات الصناعية بدلاً من العمليات الإدارية. تشمل أنظمة التشغيل إدارة خط الإنتاج، والتحكم في عمليات التعدين، ومراقبة النفط والغاز، إلخ.

تعد **أنظمة التحكم الصناعية** (ICS) جزءًا رئيسيًا في قطاع التكنولوجيا التشغيلية الحرجة. وهي تتألف من أنظمة تُستخدم لمراقبة العمليات الصناعية والتحكم فيها. قد تكون (أحزمة ناقلة في موقع المناجم، أو أبراج لتكرير النفط، أو استهلاك الطاقة على شبكات الكهرباء أو أجهزة الإنذار من أنظمة معلومات.

غالبًا ما تُدار أنظمة التحكم الصناعي (ICS) عبر أنظمة التحكم الإشرافي واكتساب البيانات (SCADA) التي توفر واجهة مستخدم رسومية للمشغلين لمراقبة حالة النظام[1].

لا يشير توجيه مجلس أوروبا في قرارة رقم114/2008 / EC الصادر في 8 ديسمبر 2008 بشأن تحديد وتعيين البنى التحتية الأوروبية الحرجة وتقييم الحاجة إلى تحسين حمايتها" إلى الحاجة إلى تعيين البنية التحتية الحيوية وحمايتها فحسب، بل يحدد أيضًا الجهات الفاعلة المسؤولة للأنشطة المختلفة على مستوى عال على مستوى الاتحاد الأوروبي، تعمل المفوضية الأوروبية كهيئة تنفيذية مسؤولة عن اقتراح التشريعات وتنفيذ القرارات، قد تدعم المفوضية أيضًا الدول الأعضاء في تحديد البنية التحتية الحرجة على أساس مستمر، ومع ذلك، فإن توجيهات المجلس تعمل فقط كإطار عام لحماية البنية التحتية الحرجة، في حين تقع مسؤولية

[1] Graham Williamson, "OT, ICS, SCADA – What's the difference?", kuppingercole Analysts, Jul 07, 2015, in: https://cutt.us/yXPP7 (24-12-2021)

تفاصيل اتخاذ إجراءات محددة على عاتق كل دولة عضو، يتضمن ذلك أيضًا مسؤولية تحديد متطلبات الأمن السيبراني ICS-SCADA لمشغلي CI[1].

- **الأثر التكنولوجي على الأمن: تصور الأمن السيبراني في سياق أمن الدولة**

يتميز انتقال أوروبا إلى مجتمع المعلومات بتطورات عميقة في جميع جوانب الحياة البشرية: في العمل والتعليم والترفيه، في الحكومة والصناعة والتجارة، تكنولوجيا المعلومات والاتصالات، التي لها تأثير ثوري وأساسي على اقتصاداتنا ومجتمعاتنا، فنجاح مجتمع المعلومات مهم لنمو أوروبا وقدرتها التنافسية وفرص العمل، وله آثار اقتصادية واجتماعية وقانونية بعيدة المدى، لكن لهذه البنى التحتية نقاط ضعف خاصة بها وتوفر فرصًا جديدة للسلوك الإرهابي، قد تتخذ هذه الأنشطة الارهابية مجموعة متنوعة من الأشكال، هذه التهديدات الارهابية تشكل تهديدًا لاستثمارات الصناعة وأصولها، وللأمان والثقة في مجتمع المعلومات[2].

يقودنا هذا الأمر لتسليط الضوء على عنصرين مهمين لتصور الأمن السيبراني في سياق أمن الدولة. **أولاً**، الدول الصناعية والمتقدمة معرضة بشكل غير متناسب للتهديدات السيبرانية، الإرهابية منها على وجه الخصوص، وهذا يعطل المعتقدات القديمة في العلاقات الدولية حول العلاقة بين التكنولوجيا والقوة.

فالاعتمادية الكبيرة للدول الأوربية على البنية التحتية للمعلومات الحيوية لديهم مع العديد من الوظائف التجارية والمدنية والحكومية التي تتم عبر الإنترنت فقط يجعلها قابلة للعطب، عكس العديد من دول العالم حيث معدلات الاختراق منخفضة بسبب التخلف التكنولوجي الحاصل (أنظر الشكل6 أعلاه)، وبالتالي فإن المخاطر قد تكون منخفضة، بالإضافة إلى ذلك، ففي نظام عالمي يتسم بتفاوت كبير في توزيع القدرات، هناك توقع متزايد بأن هؤلاء الفاعلين السياسيين الذين لديهم إمكانية الوصول إلى القليل من الموارد العسكرية التقليدية قد ينجذبون إلى الإمكانات غير المتكافئة للأسلحة السيبرانية[3].

العنصر **الثاني** الذي أبرزته بعض الهجمات السيبرانية هو التحدي الذي يواجه ترتيبات الأمن الجماعي مثل حلف الناتو في تجميع المفاهيم الحالية للحرب الحركية مع التهديدات الخاصة بعصر المعلومات. لكن

---

[1] Rossella Mattioli, ***Op.cit***, p-p : 25-26.

[2] European Commission. (2001c). Communication on creating a safer information society by improving the security of information infrastructures and combating computer-related crime" (eEurope 2002) COM(2000) 890 final, 26.01.2001. Brussels, Belgium: European Commission, p 2. in :https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0890:FIN:EN:PDF. (21/12/2021)

[3] Madeline Carr, "Crossed Wires: International Cooperation on Cyber Security", Interstate - ***Journal of International Affairs***,2016, issue 2, p2. in:

https://issuu.com/interstate1965/docs/20152016__issue_2_-_the_cyber_issue(20/10/2021).

البدء في توضيح بعض الانفصال بين مفاهيمنا عن العنف السياسي قبل تكنولوجيا الإنترنت وبعدها هو نقطة البداية. في هذه الحالة، يصبح فهم تأثيرات الهجمات الإرهابية السيبرانية على مختلف القطاعات الأمنية، أساسا لصياغة استجابة أمنية مناسبة.

المبحث الثاني: محددات الأمن الجماعي الأوربي

يتناول هذا المبحث جانبا من أهم المحددات للإشكاليات المطروحة على مستوى الأمن الجماعي الأوروبي، وهي التي تحدد التصور الأمني لأوروبا، وللاتحاد الأوروبي بوجه الخصوص، مما ينعكس على السياسات والاستراتيجيات المتبناة (كما سيجري تناوله في الفصل الرابع) في سبيل تأمين الفضاء الالكتروني ومكافحة الإرهاب السيبراني.

المطلب الأول: جينالوجيا مفهوم الأمن الجماعي.

تعود فكرة الأمن الجماعي الى الرابطة البحرية الأثينية، والتي بموجبها التزمت المدن اليونانية بعدم محاربة بعضها البعض، ثم تطور التركيز في هذا النظام إلىنوع من الحماية الدينية المشتركة، يُنظر إلى هذا الالتزام الجماعي كآلية مساءلة للأعضاء تحث على الحفاظ على معيار الأمن الداخلي باعتباره جوهر الأمن الجماعي. في هذا الصدد، يُذكر أن قوة وفلسفة الكنيسة الكاثوليكية جعلت العصور الوسطى فترة خصبة لتبلور هذه الفكرة في ألمانيا وفرنسا على وجه الخصوص، فأصدرت المجالس الدينية قوانين تُلزم الأمراء ورجال الدين بمقاومة الحرب بوسائل عنيفة ووضعت القوات المشتركة تحت قيادة دينية، وعلى مستوى أكثر تجريدًا، ناقش العلماء في ذلك الوقت المزايا النسبية للنظام الملكي العالمي ومؤتمر الأمراء للحفاظ على السلام في أوروبا.

في وقت لاحق، جلب عصر التنوير العديد من خطط الأمن الجماعي العلماني، والتي جادلت بأن القوى العظمى يجب أن تفرض السلام في أوروبا من خلال الإلتزامبالمعاهدات التي أنهت حرب الثلاثين عامًا التي أسست لشروط السلام وقتها، والتي ألزمت الموقعين عليها بالدفاع وحماية بعضهم البعض، يفهم من هذا أن الأمن الجماعي يرتبط بجهود مجموعة من الدول للعمل معًا من أجل الحفاظ على أمنهم بشكل أفضل. وبالتالي، فهو جزء من الدراسات الأمنية ومفهوم الأمن بشكل عام. لهذا السبب، يبدو أنه من المفيد عمليًا التطرق إلى مفهوم الأمن نفسه أولاً قبل مناقشة مفهوم الأمن الجماعي[1].

من المقبول عمومًا أن الأمن، سواء تم تعريفه بشكل ضيق أو واسع، هو السلعة الحيوية الأولى التي تلتزم الدول بتوفيرها، وترتبط بغياب التهديدات ضد القيم المركزية، وبمعنى ذاتي يعني غياب المخاوف من أن تكون تلك القيم محل تهديد[2].

فكما تم تناوله آنفا، يرى وولتر ليبمان :Walter Lippmann" أن الأمة تبقى في وضع آمن إلى الحد الذي لا تكون فيه عرضة لخطر التضحية بالقيم الأساسية إذا كانت ترغب بتفادي وقوع الحرب و تبقى

---

[1] *Ulusoy H. COLLECTIVE SECURITY* IN *EUROPE. PERCEPTIONS*: *Journal* of *International Affairs*. 2002, Vol 7, N4: in :https://dergipark.org.tr/en/pub/perception/issue/49013/625259 (04/12/2021).

[2] عبد النور بن عنتر، تطور مفهوم الأمن في العلاقات الدولية، **السياسة الدولية**، عدد 160، المجلد 40، (2005)،ص56.

قادرة لو تعرضت للتحدي على صون هذه القيم عن طريق انتصاراتها في حرب كهذه"[1]. يركز كلا التعريفان للأمن على البعد العسكري للدولة كركيزة أساسية لمواجهة أي خطر يهدد قيمها المركزية.

وعلى غرار الإشكالية المفاهيمية في تعريف الأمن، يظل التعريف الدقيق للأمن الجماعي بعيد المنال في النقاش العام والخطاب الأكاديمي، لا تختلف التعريفات فحسب، بل يتعارض بعضها أيضًا بشكل مباشر، وقد استخدم المصطلح لوصف كل شيء بدءًا من أنظمة التحالف الفضفاضة إلى أي فترة من التاريخ لا تتعارض فيها الحروب مع بعضها البعض، يرجع هذا النطاق الواسع أيضًا إلى طبيعة التهديدات الأمنية.

من ناحية أخرى، فإن أفضل مثال على الترتيبات الأمنية لمواجهة التهديدات الداخلية القادمة من أعضاء هيئة الأمن الجماعي هو "المجتمع الأمني"، وضع كارل دويتش Karl Deutch هذا المفهوم الذي قدمه فان واجنين Van Wagenen لأول مرة في عام 1957،حيث تشارك الدول في المجتمع الأمني بعضها البعض في مستويات عالية من الترابط الاقتصادي والاجتماعي والسياسي. ويستند استعدادهم للقيام بذلك على مجموعة من الوعود بعدم استخدام القوة فيما بينهم. يتم التعبير عن هذا الاستعداد إما من خلال اندماج الدول في هيئة مشتركة (مجتمع أمني مدمج Pmalgamated security community) أو من خلال التعاون بين الدول دون أي مأسسة رسمية (مجتمع أمني تعددي Pluralistic security community)

في وقت لاحق، قام أدلر Adler بإضافة القيم المشتركة كأساس لمثل هذا المجتمع، وقد طور مفهوم المجتمع الأمني. بالنسبة لأدلر، "يتشكل المجتمع الأمني من مجموعة من الدول الديمقراطية ذات السيادة التي وافقت على الدمار الذي لا يطاق للحرب الحديثة والقيم السياسية والاقتصادية والاجتماعية والأخلاقية المتوافقة مع الديمقراطية وسيادة القانون والإصلاح الاقتصادي، وقد نقلت الممارسات المحلية على الساحة الدولية وسمحت لمجتمعاتهم المدنية وكذلك مؤسساتهم بالتكامل إلى حد أن فكرة استخدام القوة تفقد أي معنى عملي وحتى تصبح غير واردة (الكل من أجل الواحد)، بينما تحتفظ الدول بقدر كبير من الاستقلالية في إدارة سياستها الخارجيةفإن المشاركة في منظومة أمن جماعي تتطلب التزامًا من قبل كل عضو للانضمام إلى تحالف لمواجهة أي معتد بقوة راجحة معارضة[2]. بهذا المعنى، يشير الأمن الجماعي إلىإضفاء الطابع

[1] ستيف سميث، جون بيليس، ***عولمة السياسة العالمية***، ترجمة: مركز الخليج للأبحاث، ط1،(الامارات العربية المتحدة، مركز الخليج للأبحاث، 2004)، ص414.

[2] *Ulusoy H.* ***Op.cit.***

المؤسسي على فكرة الكل ضد واحد، في خلق بيئة دولية ينشأ فيها الاستقرار من خلال التعاون وليس من خلال المنافسة[1].

لقد ثبت أن مفهوم الأمن هنا مستقر بشكل ملحوظ لأنه مرتبط بمبدأ سيادة الدولة الذي يقدم حلاً قويًا لمسائل الهوية والنظام والسلطة. ومع ذلك، في حين أن "الأمن" في شكل الطريقة السياسية للأمن القومي (أي التهديدات والمخاطر وقرارات الطوارئ) هو مرن مثل الدولة، فلا الدولة ولا "الأمن" غير متنازع فيهما أو لا جدال فيهما. فكلاهما يعتمد على الممارسات السياسية والأكاديمية لإعادة إنتاج وضعهم، وبالتالي يصبح السؤال هو ما إذا كان الخطاب حول الأمن السيبراني يعزز دور الأمة / الدولة ككائن مرجعي، وكيف يتم التعبير عن المسؤولية الفردية لدعم (أو تحدي) الأمن والسلطة الجماعية، وما إذا كان هذا يعيد صياغة فهم "السياسة الأمنية" نفسها[2].

وقد اتخذت دول أخرى طريقًا مشابهًا، معتقدة أن أفضل طريقة لحماية الهويات الثقافية من بيئة الإنترنت هي عزل المجموعة الثقافية تمامًا عنها. باختصار، تصور الصورة الجماعية للأمن القومي الإنترنت على أنها تهديد أمني محتمل للهويات الجماعية، حيث يُنظر إلى الأمة أو الثقافة على أنها الهدف الأساسي للأمن. في حين أن صورة الأمن الجماعي هذه لا تهيمن بالتأكيد على المشهد في سياسات الإنترنت، فقد صبغت وجهات نظر العديد من الوزارات الحكومية والبلدان في جميع أنحاء العالم. تراوحت خيارات السياسة المتبعة كدالة لهذه الصورة الجماعية من العزلة الكاملة والاحتواء إلى تدخل الدولة الفعال وتعزيز التعبير القومي على الإنترنت.

بالنسبة لمسؤولي إنفاذ القانون والاستخبارات، تشكل هذه التطورات تحديًا أساسيًا للرافعات التقليدية للسلطة، ولا سيما أشكال المراقبة المختلفة، وعلى نطاق أوسع، فإنها تمثل أيضًا مشكلات في تطبيق أنظمة الدولة التي بدورها يمكن أن تسهل الجريمة المنظمة والاحتيال، هذه المخاوف في مجال الاهارب السيبراني هي ببساطة أحد عناصر التهديد الأوسع الذي يشكله الإنترنت لسلطة الدولة[3]. انتقل فيها الأمن من مستويات الأمن الصلب بتهديداته التقليدية، إلى الأمن اللّين بتهديداته اللاتماثلية التي صاحبت موجة العولمة، والتي أصبحت فيها السيطرة على المعلومات المتدنية داخل الدول وخارجها لأسباب لا تخضع لمعايير قوة الدولة ومفدراتها بقدر ما تخضع لآليات التعاون الجماعي الفعال في مواجهة الإرهابي السيبراني، وتعزيز الروايات الأوسع نطاقاً المتعلقة بالحاجة إلى تحسين وتوحيد النهج التعاوني الجماعي على مستوى الاتحاد الأوروبي لتأمين أنظمته الحيوية.

---

[1] Dorussen, H., Kirchner, E., & Sperling, J. "Sharing the Burden of Collective Security in the European Union". ***International Organization***, Vol 63, N4, (2009), pp 789-810, in: https://www.researchgate.net/publication/46545054 (04|11|2021)

[2] Lene Hansen and Helen Nissenbaum, ***Op. cit.***

[3] Deibert, Ronald J. ***Op.cit***, 115-142.

المطلب الثاني: الأمن الجماعي الأوروبي والتحول في طبيعة التهديدات الأمنية

تستند سرديات الأمن السيبراني إلى تقديم إعادة صياغة مفاهيميةلأمن الدولة، والخروجمن الخطابات التي قدمت مفهومًا تقليديًا واقعيالفكرة أمن الدولة. بينما ينبغي أن يُظهر المزيد من البحث النقدي كيف أن ممارسات وخطابات الأمن السيبراني لا تولد بل تكتفي بتضخيم التمايز الذاتي لمجالات الأمن والإشارة إلى سرد "سلسلة التهديدات" التي ميزت تطور الأمن الدولي منذ بداية الألفية، والتأكيد على الاستمرارية التاريخية للتطورات الأمنية، والأمن الجماعي خطوة مرحب بها نحو مواجهة الخطابات الوطنية وعبر الوطنية التي تستخدم ما يسمى بـ "حداثة" التهديدات الإلكترونية لزيادة تأمين الإنترنت وتفكيك/إعادة هيكلة طابعها المفتوح[1].

وتبعا لذلك، تدعمت وجهة النظر الداعية إلى إعادة النظر في مفهوم الأمن من خلال تقرير "إيغون بار Egon Bahr "المقدم للجنة بالم Palme(1982) والذي عنونه "الأمن المشترك " Common Security ويرى فيه أن التركيز على القوة في عالم يتميز بمستويات عالية من التسلح وتضبطه حركية الاعتماد المتبادل غير مؤسس، فسعي الدول منفردة لتعزيز أمنها، سوف يقلص في نهاية المطاف أمن الدول الأخرى. وفضلا عن ذلك، فإن التركيز على المخاطر العسكرية في التعامل مع المعضلات الأمنية غير واقعي، إذ توجد أشكال أخرى من المخاطر التي تتهدد الدول وهي ذات طبيعة اقتصادية، بيئية وحتى ثقافية، كما وقد يكون وراءها فاعلين آخرين غير الدولة كشبكات "المافيا" والمنظمات الإرهابية[2].

أدى ذلك إلى تبني مفهوم أوسع للأمن أخذ تسميات متعدة كـ"الأمن المتكاملComprehensive " Security بحيث يتضمن كل أشكال التهديد، و"الشراكة الأمنيةSecurity Partnership" بحيث يتم إشراك الدول غير الغربي، و"الأمن المتبادل Mutual Security "إذ يتم التخلي نسبيا عن نزوع الدول منفردة إلى تعظيم أمنها على حساب الدول الأخرى، "الأمن التعاوني Cooperative Security " بحيث يتم تقاسم الأعباء الأمنية لاحتواء التهديدات. لكن ورغم تعدد هذه التسميات إلا أنها لا تتجاوز الحدود التقليدية للمفهوم، أين تلعب الدولة ومؤسساتها الرسمية دورا حصريا في تحديد ماهية التهديدات وسبل مواجهتها[3].

وبينما ارتكز الاهتمام على أن الأمن السيبراني يمثل مشكلة "ما بعد الدولة" بشكل واضح، فقد ثبت في الواقع أنه من الصعب للغاية تجاوز المفهوم الويستفالي للمشكلة أو للحلول الممكنة. يؤدي هذا إلى مفارقة مركزية حول الأمن السيبراني كما نتصوره حاليًا: فمن ناحية، تبيَّن أنها مسألة لا يمكن التعامل معها بشكل فعال من خلال أدوات الدولة مثل الجيش أو مؤسسات انفاذ القانون، ولكن على الرغم من ذلك، لا تزال هناك

---

[1] Memphis Krickeberg, ***Op.Cit.***

[2] عادل زقاغ، "المعضلة الأمنية المجتمعية، خطاب الأمننة وصناعة السياسة العامة"، ***المجلة الجزائرية للسياسة العامة***، المجلد 1، العدد1. (سبتمبر 2011) ، ص 60-72.

[3] عادل زقاغ، ***المرجع نفسه***، ص 60-72.

توقعات قوية أن تتحمل الدولة مسؤولية توفير الأمن في هذا المجال. وقد أدت هذه المفارقة إلى التركيز في وثائق سياسة الأمن السيبراني على ضرورة التعاون الدولي للوصول لبنية صلبة للأمن الجماعي[1].

ظهر هذا البناء الخطابي لضعف البنية التحتية الحيوية وانتشر منذ عام 2012 في المناقشات والبيانات المفتوحة التي يقدمها الاتحاد الأوربي بمختلف مؤسساته. فعلى سبيل المثال، جادل البرلمان الأوروبي بأنه فيما يتعلق بالإرهاب السيبراني والمخاطر التي تتعرض لها البنية التحتية الحيوية، هناك حاجة ملحة إلى تطوير تقنيات وقدرات جديدة، في إشارة إلى سياسة الأمن والدفاع المشتركة، واقترح تعزيز القدرات الأوربية فيما يتعلق بالهجمات الإلكترونية والإرهاب السيبراني، وأن خطة العمل ستمثل بداية تحرك نحو تكامل أكثر منهجية بين قضايا الدفاع السيبراني بين مؤسسات الاتحاد الأوروبي، بما في ذلك بناء استراتيجية أوروبية متماسكة لتأمين البنية التحتية الحيوية ضد الهجمات الإلكترونية، فالدعاية عبر الإنترنت والهجمات الإلكترونية" التي يقوم بها تنظيم الدولة الإسلامية عززت ليس فقط الحاجة إلى تعاون الاتحاد الأوروبي بشكل أكبر مع الشركاء الخارجيين لمنع التهديدات الإلكترونية بما في ذلك الإرهاب الإلكتروني، ولكن أيضًا حالة الاتحاد الأوروبي المعيارية لجوهر الإنترنت والبنية التحتية لتكون "منطقة محايدة" [2].

يلاحظ أيضا أن التآزر بين المنظمات الإجرامية والجماعات الإرهابية قد أدى إلى وضع يمكن فيه للمنظمات الإرهابية إعادة توظيف أدوات الهجوم السيبراني التي طورتها الجريمة المنظمة لاستهداف البنية التحتية الحيوية لأغراض سياسية، وهذا يتطلب دفعًا أكبر للتعاون الحالي داخل الاتحاد الأوروبي وخارجه، بما في ذلك ما يتعلق بتأمين البنية التحتية الحيوية، واستيعاب أفضل ممارسات الأمن السيبراني، وتعزيز شبكات الشرطة بين الدول الأعضاء[3].

- **البنية البلاغية للأمننة:**

تعتبر من أبرز المنظورات المهتمة بالقضايا الأمنية التي جاءت بها مدرسة كوبنهاغن، فالتحرك الأمني هو الذي يأخذ السياسة بعيدا عن القواعد المؤسساتية ويؤطر القضية كنوع خاص من السياسة أو فوق السياسة، كما أن الطبيعة الخاصة للتهديدات تبرر استخدام إجراءات استثنائية[4]، فالدول والمنظمات الدولية (الفواعل الأمنية) يمكن أن تتبنى لغة أمنية تقنع الجمهور بوجود تهديدات للكيان المرجعي، وتختلف هذه اللغة الأمنية في المراحل الثلاث لمسار الأمننة في **الأولى** مرحلة عدم التسييس لا تكون القضية من اهتمام الدولة

---

[1] Madeline Carr, "Crossed Wires: International Cooperation on Cyber Security", ***INTERSTATE - JOURNAL OF INTERNATIONAL AFFAIRS***, 2016, issue 2, p2, https://cutt.us/IIqA3(20/10/2021).

[2] Christopher Baker-Beall, Gareth Mott, ***Op.cit.***

[3] ***Ibid.***

[4] نوري عزيز، "الخطاب الأمني الأورو–متوسطي تجاه ظاهرة الإرهاب بين: الأمننة/اللاأمننة"، ***مجلة الحقوق والعلوم السياسية***، مجلد 5، عدد2، (جوان 2018)، ص 237.

ولا جزء من النقاش العام وعملية اتخاذ القرار، وفي **الثانية** مرحلة التسييس تصبح القضية جزء من السياسة العامة والقرارات الحكومية والخطابات التعبيرية. أما في **المرحلة الأخيرة** مرحلة التأمين فالفواعل الأمنية تعبر عن القضايا السياسية كتهديدات وجودية للكيان المرجعي[1].

المطلب الثالث: فهم المخاطر السيبرانية المشتركة.

تضع الدول سياساتها واستراتيجياتها الوطنية التي تغطي التدابير المضادة للأمن السيبراني بما في ذلك الدفاع السيبراني والردع ضد التهديدات السيبرانية، ولكن من الصعب التعامل مع التهديد من خلال سياسات واستراتيجيات الدفاع السيبراني "الوطنية" فقط، نظرًا لأن الفضاء الإلكتروني يمتد في جميع أنحاء العالم ويمكن أن يكون مصدر الهجوم في الخارج[2].

وما يلاحظ على الاتحاد الأوروبي باعتباره موقعًا للسلطة الخطابية، مع الاتساق الكافي عبر مجموعة من الجهات الفاعلة المختلفة لتوفير لغة مؤسسية مشتركة وإطار عمل في مجالات الأمن السيبراني ومكافحة الإرهاب، هذه الخطابات الأمنية تذهب في مسارين رئيسيين ظلوا متسقين عبر جميع مؤسسات الاتحاد الأوروبي. **أولاً**، نوضح كيف يتسم الخطاب بعدم التناسق بين الدول الأوربية في تحديد الإرهاب السيبراني بوضوح، مع ملاحظة أنه لا يوجد توافق في تعريفه في أي من وثائق السياسة الأمنية الرئيسية ذات الصلة. ومع ذلك، في حالة عدم وجود تعريف، فإننا نسلط الضوء على العديد من الخصائص الرئيسية التي تعكس تصورًا مشتركًا أو فهمًا مشتركًا للإرهاب السيبراني على النحو التالي: نوع هجين من الهجمات الإرهابية، وتهديد متزايد للمجتمع الأوروبي، وتهديد للديمقراطية، وتهديد مستقبلي محتمل لم يتحقق بعد. في حين جرى تحديد المسار الرئيسي **الثاني** باعتبار أن الكائن المرجعي الأساسي الذي يجب تأمينه هو البنية التحتية الحيوية، كما أن الخطاب الذي يحدد قابلية تعرض البنية التحتية الحيوية لحادث إرهابي إلكتروني محتمل بمثابة منطق أساسي لإعادة إضفاء الشرعية على الممارسات الأمنية الأوسع المتعلقة بالأمن السيبراني ومكافحة الإرهاب على التوالي[3].

تبعا لذلك، ومن من أجل حماية مصالحها الحيوية، تركز العديد من الدول المعتمدة على التكنولوجيا على تنظيم سياسات الأمن السيبراني الخاصة بها كوحدات سياسية قبل الانخراط في سياسات أمنية جماعية يفرضها الاتحاد الأوروبي، وقد اتخذت معظم هذه الدول نوعا من الإجراءات القانونية والعسكرية الوطنية ولكن بدون تعاون دولي، إلا أن هذه الإجراءات الوطنية أثبتت أنها غير كافية ضد تصاعد الإرهاب السيبراني، لا توفر الشراكات الإقليمية أيضًا الأمن السيبراني الملائم، حيث يمكن أن تنشأ الهجمات الإلكترونية من دول خارج المنطقة أو خارج الشراكة الأوروبية، من أجل توفير تعاون أوروبي متناسق وبناء يجب تعريف مصطلح

---

[1] نوري عزيز، ***المرجع نفسه***، ص 238.

[2] Murat Dogrul,and others,"Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism", in: ***3rd International Conference on Cyber Conflict.*** C. Czosseck, E. Tyugu, T. Wingfield (Eds.), (Tallinn, Estonia: 2011)|, p29.

[3] Christopher Baker-Beall, Gareth Mott, **Op.cit.**

"الإرهاب الإلكتروني" بدقة ويجب تحديد الأنشطة التي تعتبر نشاطًا إرهابيًا كخطوة أولى. بعد ذلك، ينبغي مناقشة تطوير التعاون التشريعي والعسكري.[1]

وقد انعكس هذا الترتيب في الأولويات ليس فقط على مستوى المبادرات الجديدة المقترحة، ولكن أيضًا في الفكرة القائلة بأنه لكي يكون الاتحاد الأوروبي جهة فاعلة، وفعالة في مجال الأمن السيبراني، يجب أن يكون متماسكًا تمامًا، كما يشكك الأمن السيبراني في عدد من الثنائيات المهمة (داخلي/خارجي، عام/خاص، مدني/عسكري) بينما في نفس الوقت يطمس الفروق الجغرافية بين المستويات الوطنية والأوروبية والعالمية، كمنطقة أمنية، فهي توفر أرضية مثالية لتقييم تماسك القوة الأمنية للاتحاد الأوروبي[2].

بدأ الاتحاد الأوروبي لأول مرة في تطوير سياسة جماعية لمكافحة الإرهاب في عام 2001 في أعقاب هجمات 11 سبتمبر 2001 الإرهابية في الولايات المتحدة مباشرة، مع التركيز في البداية على التهديد الخارجي الذي يشكله الإرهاب، تم اعتماد خطة عمل الاتحاد الأوروبي الأولى لمكافحة الإرهاب في نوفمبر 2001 وتبعها الاتحاد الأوروبي لاحقًا بعد الهجمات الإرهابية في مدريد في 2004 ولندن في 2005، ضمن إستراتيجية مكافحة الإرهاب[3].

ومن هذا المنطلق أخذ القلق الأوروبي المشترك من مخاوف توظيف تكنولوجيات المعلومات والاتصالات في الأعمال الإرهابية في التصاعد، فظهر في البدايات مؤتمر وزراء خارجية الدول الأوربية الذي ناقش قضية الإرهاب في باريس 1996، ووافق المؤتمر على إصدار نداء إلى كل دول العالم لملاحظة أخطار الإرهاب الالكترونية، والإرهاب المتشابك عبر الأنظمة وشبكات الاتصال لتنفيذ أعمال إجرامية، ودعى إلى ضرورة إيجاد وسائل متسقة مع القانون الدولي لمنع مثل هذه الجرائم، واقترح أن تكون هناك استشارات ثنائية أو متعددة الأطراف ما بين الحكومات للسماح بالتشفير عند الضرورة، والسماح أيضا بالدخول \المنع القانوني إلى البيانات والاتصالات، والتحري عن الأعمال الإرهابية، وحماية سرية الاتصالات، وتكثيف تبادل المعلومات، خاصة تلك المتعلقة باستعمال تقنيات الاتصالات من قبل الجماعات الإرهابية.

وكذلك قمة رؤساء الدول الأوربية في ليون في جويلية 1996 والتي حثت على التعاون بين الدول لحماية الاتصالات المركزية العالية التقنية للتجارة العالمية والتعاون الدولي، وعلى مستوى البوليس في أوربا عقدت سلسلة مؤتمرات تحت رعاية المفوضية الأوربية، وتبادلوا فيها المعلومات التي رصدوها في افريل 1997 خلال مراقبتهم للمحتوى غير القانوني على الانترنت، وزاد القلق في بريطانيا التي كثفت الأنشطة

[1] Murat Dogrul, and others, **Op.cit**, p30.

[2] Helena Carrapico, André Barrinha,The EU as a Coherent (Cyber)Security Actor?, JCMS, 2017 ,Volume 55. Number 6. pp. 1254–1272, 10 May 2017, in: https://doi.org/10.1111/jcms.12575 (20/10/2021)

[3] Christopher Baker-Beall, Gareth Mott, ***Op.cit.***

المخابراتية لمراقبة معلومات ونشاطات الانترنت غير الشرعية، وفي أواخر 1998 عقدت أجهز الشرطة هناك اتفاقية مع مزودي خدمات الانترنت، لمراقبة الأنشطة الإرهابيةوالإجرامية في الانترنت[1].

فأوروبا أدركت ضرورة أن تفحص الحكومات الوطنية تشريعاتها القانونية الحالية لتحديد مدى كفايتها لمكافحة أنواع الإرهاب الجديدة، ففي تقرير عالمي حديث صدر في أواخر عام 2000، يدرس مدى كفاية التشريعات القانونية في 52دولة لمواجهة جرائم وإرهاب الإنترنت اتضح أن فقط عشر دول فقط قد عدلت قوانينها لتغطية أكثر من نصف تلك الجرائم[2]، لهذا سعى الاتحاد الأوروبي إلى تطوير قدراته ليكون جهة فاعلة إقليمية في مجال الأمن السيبراني، من خلال أولى الاتفاقيات العالمية المتعلقة بجرائم الانترنت، والتي وقعت في العاصمة المجرية بودابست في 23 نوفمبر 2001، بهدف التعاون والتضامن لمحاربة الجرائم السيبرانية[3]، ثم بتبنيه أول استراتيجية للأمن السيبراني (استراتيجية مكافحة الجريمة السيبرانية والهجمات الإلكترونية التي ترعاها الدولة) في فبراير 2013، تبع ذلك الأجندة الأوروبية للأمن في أبريل 2015، والتي سلطت الضوء على العمل الأوروبي المنسق في مجال الأمن السيبراني كأولوية للاتحاد الأوروبي في المستقبل القريب، ترافقت هذه الخطط لتعزيز سياسة الاتحاد الأوروبي للفضاء السيبراني مع تحسينات في الأحكام التشريعية للتصدي للتهديدات السيبرانية. وفي عام 2013، حدَّث الاتحاد الأوروبي توجيه 2005 بشأن الهجمات ضد أنظمة المعلومات ليتماشى وإعادة هيكلة المنظومة القانونية والتشريعية[4]،

غاب مفهوم الإرهاب السيبراني عن الإستراتيجية الأولى للاتحاد الأوروبي في مجال مكـــافحة الإرهاب، الصادرة في 2005، لأن الاهتمام حينها كام منصبّا على استغلال الانترنت من قبل الإرهابيين لغرض التجنيد والتمويل، ثم جرى تحديد مكافحة الإرهاب الإلكتروني كأولوية ضمن خطة عمل صادرة في 2006، كما شددن لجنة مكافحة الإرهاب على مستوى الاتحاد الأوروبي على وجوب التركيز على التعاون الدولي لمكافحة الإرهاب على ثلاث مجالات: منع التطرف والتجنيد، ومكافحة تمويل الإرهاب، ومنع الإرهاب السيبراني[5]،وفي عام 2019 اعتمد لائحة جديدة تحكم الوكالة الأوروبية للأمن السيبراني (ENISA) التي تستهدف شهادة الأمن السيبراني.

تشكل هذه التدابير جزءًا من سرد أوسع لمؤسسات الاتحاد الأوروبي (التي سنبرزها في الفصل الأخير) التي تعمل على تعزيز "النشاط" الأوروبي، وإنشاء "مركز" لمساعدة الدول الأعضاء على توحيد

---

[1] أحمد محمد صالح، ***أنفوغرافيا الأنترنت وتداعياتها الاجتماعية والثقافية والسياسية***،(القاهرة: دار كتب عربية،2007)، ص 417-419.

[2] ***المرجع نفسه***، ص 434.

[3] وفاء لطفي، "الجهود الدولية في مجال مكافحة جرائم الارهاب السيبراني: التجربة الماليزية نموذجا"، ***مجلة كلية الاقتصاد والعلوم السياسية***، المجلد 23، العدد 1، (يناير 202) ، ص: 151-178.

[4] Christopher Baker-Beall, Gareth Mott, ***Op.cit.***

[5] ***Ibid***.

المعايير وفهم المخاطر، بما في ذلك تنفيذ التدابير التي يمكن اتخاذها لمواجهتها، يتضمن هذا الدمج تهديدات منتشرة مثل الإرهاب، وتهديدات جديدة مثل تلك التي تشكلها أشكال مختلفة من الجرائم الإلكترونية، في الفترة منذ ذلك الحين، تطورت سياسة الاتحاد الأوروبي لمكافحة الإرهاب للتركيز بشكل شامل على كل من القضايا الأمنية الداخلية والخارجية التي تشمل مكافحة التطرف والردود على المقاتلين الأجانب وأمن الحدود كإجراء لمكافحة الإرهاب واستخدام الإرهابيين للإنترنت، خلال هذا التطوير لسياسة مكافحة الإرهاب في الاتحاد الأوروبي، تم التذرع بالتهديد من "الإرهاب الإلكتروني" بشكل متقطع باعتباره مصدر قلق مستقبلي محتمل للاتحاد الأوروبي في هذا المجال[1].

المطلب الرابع: الثابت والمتغير في تصور الأمن الجماعي الأوروبي.

أ- أمننة الأنظمة الرقمية: العناصر المرجعية للأمن السيبراني الأوروبية.

يُعد السوق الأوروبي فرصة عظيمة لمقدمي خدمات الأمن السيبراني، حيث تمثل أوروبا سوقًا يضم 500 مليون فرد وحوالي 26 مليون مؤسسة، وتقدر المنظمة الأوروبية للأمن السيبراني ECSOأن حجم السوق العالمي لمنتجات وخدمات أمن المعلومات والشبكات، باستثناء المنتجات العسكرية، تراوح من 46.9 مليار يورو إلى 76.3 مليار يورو في عام 2014. ووفقًا لشركة Gartner، بلغ الإنفاق العالمي على أمن المعلومات 81.6 مليار دولار أمريكي في عام 2016 .

فيما قدرت مؤسسة البيانات الدولية International Data Corporation (IDC) الإيرادات العالمية للأجهزة والبرامج والخدمات المتعلقة بالأمن بنحو 73.7 مليار دولار أمريكي في عام 2016،وتجاوز سوق الأمن السيبراني في جميع أنحاء العالم 100 مليار دولار أمريكي في عام 2020، بمعدلات نمو سنوية تتراوح بين 5 و10 في المائة، في حين قُدر سوق الأمن السيبراني الأوروبي، على وجه التحديد، بنحو 18.8 مليار يورو في عام 2014، وهو ما يمثل حوالي 26 في المائة من الإنفاق العالمي على الأمن السيبراني. في الآونة الأخيرة، قدرت (PWC)*الإنفاق على الأمن السيبراني في أوروبا الغربية بنحو 21.5 مليار دولار أمريكي. يتميز سوق الأمن السيبراني الأوروبي بالتجزؤ. في عام 2014، كان أكبر 15 مزودًا، معظمهم من غير الأوروبيين، يمثلون ثلث السوق فقط، بينما كان عدد كبير من مقدمي الخدمة الأصغر مسؤولين عن الثلثين الآخرين، السبب الرئيسي وراء هذا التجزئة هو أن مقدمي الخدمات الأوروبيين يركزون عادة على

[1] Christopher Baker-Beall, Gareth Mott, ***Op.cit.***

* PricewaterhouseCoopers: هي شبكة بريطانية من الشركات العالمية المتخصصة في مهام التدقيق والمحاسبة والاستشارات، وهي واحدة من أكبر أربع شركات تدقيق واستشارات جنبًا إلى جنب مع Deloitte و Ernst & Young و KPMG. وهي معروفة بشكل أساسي لعامة الناس بدورها في فضيحة "تسربات لوكسمبورغ.

الأسواق المحلية مع توفير مجموعة محدودة من منتجات وخدمات الأمن السيبراني، كما يمثل النمو المتوقع للسنوات القادمة فرصة عظيمة للصناعة الأوروبية لوضع نفسها كشريك رئيسي في النظام البيئي للأمن السيبراني الأوروبي.[1]

ب- النهج الأوروبي التعاوني لحماية البنى التحتية الحرجة:

تم وضع "البرنامج الأوروبي لحماية البنية التحتية الحرجة" (EPCIP) عقب بيان أوروبي يخصّ "حماية البنية التحتية الحرجة في سياق مكافحة الإرهاب"، والذي جاء باقتراحات حول كيفية منع الاتحاد الأوروبي لهجمات الإرهاب السيبراني المحتمَلة، يشمل برنامج حماية البنية التحتية الحرجة جملة من المبادرات أهمها:

- وضع تدابير تقييمية وأخرى معَدَّة للمساهمة في تنفيذ خطة عمل البرنامج.
- دعم الدول الأعضاء في الاتحاد الأوروبي لحماية البنى التحتية الحرجة الخاصة به.
- إنشاء مخطط للطوارئ.
- إنشاء ميزانية للتدابير المتعلقة بحماية البنى التحتية الحساسة.

بالإضافة إلى أن البرنامج قد مهّد لإنشاء الشبكة المعلوماتية لتحذير البنية التحتية الحرجة (CIWIN) التي تعتبر من اهم التدابير التي تبناها الاتحاد الأوروبي لغرض تبادل المعلومات حول التهديدات المشتركة ونقاط الضعف، ووضع الاستراتيجيات الملائمة للتخفيف من التهديدات التي قد تمس البنى التحتية لدول الاتحاد الأوروبي. تم تطوير هذه الشبكة كنظام حماية البنية التحتية الحرجة للمعلومات والاتصالات، يتبع المفوضية الأوروبية ويوفر لأعضاء الاتحاد الأوروبي الفرصةَ لتبادل ومناقشة المعلومات والدراسات والممارسات الجيدة المتعلقةبإدارة الأمن السيبراني عبر تسهيل الاتصال بين أعضائهفي جميع قطاعات النشاط الاقتصادي ذات الصلة. بالتالي، تعد هذه الشبكة ركيزة أساسية لجهود المفوضية الأوروبية في سبيل تحقيق الأمن الجماعي[2].

وفي هذا الإطار تم تحديد خطة عمل تتألف من ثلاثة مسارات رئيسَة[3]:

- **المسار الأول:** يشمل النواحي الإستراتيجية للبرنامج الأوروبي لحماية البنى التحتية الحرجة والتدابير اللازمة لتطبيقها.
- **المسار الثاني:** يشمل إجراءات التنفيذ على المستويات القطاعية.

[1] Rafael Rivera Pastor & others, ***Achieving a sovereign and trustworthy ICT industry in the EU***, EPRS | European Parliamentary Research Service Scientific Foresight Unit December 2017PE 6 (STOA) 14 . 531, in:https://cutt.us/o90NB(01/06/2020)

[2] Mario Nicolas Castellon Machado, ***Op.cit.*** p 77.

[3] ***Ibid***, p.76.

- **المسار الثالث:** دعم الدول الأعضاء في الاتحاد الأوروبي بشأن الأنشطة المتصلة بالقطاعات والمؤسسات الوطنية.

جـ –الأمن السيبراني: نظرة أوربية جديدة.

تعرّف الوكالة الأوروبية (ENISA) الأمن السيبراني بأنه "حماية المعلومات، أنظمة المعلومات، البنية التحتية والتطبيقات التي يتم تشغيلها علاوة على ذلك من تلك التهديدات المرتبطة بملف البيئة"[1]، غير أن تعريف الأمن السيبراني بحاجة إلى الأخذ بعين الاعتبار المجالات الخمسة التي يغطيها الأمن السيبراني، وهي حسب الوكالة الأوروبية ENISA كما يلي[2]:

- **أمن الاتصالات:** بمعنى الحماية من أي تهديد يمس البنى التحتية التقنية لنظام إلكتروني ويؤدي إلى تغيير خصائصه ونشاطه.
- **أمن العمليات:** ويعني الحماية من الفساد الذي قد يصيب العمليات الإلكترونية.
- **أمن المعلومات:** أي الحماية من سرقة، حذف وتغيير البيانات المخزنة في نظام إلكتروني.
- **الأمن المادي:** ويتمثل في الحماية من أي تهديد مادي قد يؤثر في النظام الإلكتروني.
- **الأمن العام/القومي:** أي الحماية من تهديد مصدره من داخل الفضاء السيبراني ولكن تأثيراته تمتد لتشمل الأصول المادية والسيبرانية ومختلف قطاعات البنية التحتية الحساسة.

ويتم تحقيق هذا عبر استراتيجية أوروبية مشتركة تمس جميع طبقات الامن السيبراني التي يبينها الشكل ادناه.

[1] Dominika Giantas***, Cybersecurity in the UE: Threats, Frameworks and Future Perspectives***, Laboratory of Intelligence and Cybersecurity: Working paper series N.1 (September 2019), p.8.

[2] Annamaria Bilaz, & Others, "Cybersecurity Strategy and Leadership Management Issues" , International May Conference on Strategic Management-IMCSM20 (Serbia: 25-27 September 2020),P.244.

الشكل (11): طبقات الأمن السيبراني وفق (ENISA)

Source : Dominika Giantas, Cybersecurity in the UE: Threats, Frameworks and Future Perspectives

يوضح الشكل أعلاه طبقات الأمن السيبراني وفق رؤية الوكالة الأوروبية لأمن المعلومات والاتصالات (ENISA)، ويلاحَظ أن الإستراتيجية الأوروبية، إلى جانب هدفها الأساسي في حماية الخدمات الرقمية والقطاعات الحيوية كالطاقة والنقل والمالية، تحاول ألا تهمل قيم الاتحاد الأوروبي المتمثلة في الديمقراطية وحقوق الإنسان، بحيث تأتي هذه القيم في قمة الهرم، كما تأتي سلامة مستخدمي الانترنت في قاعدته تحت مسمى حماية الأمن القاعدي، هذا راجع إلى التحدي المطروح بالنسبة للاتحاد الأوروبي بخصوص ضبط وتأمين الفضاء السيبراني من جهة والتداخل أو الإخلال المحتمَل وقوعه بشأن الخصوصية الفردية أو العامة في هذا الفضاء، والسعي الدائم لضمان الحوكمة فيه بما يحفظ الخصوصية والحرية على الانترنت بوصفه مجالا عاما جديدا (يقابل المجال العام التقليدي) للحوار والنقاش الديمقراطي المتزن.

ج- العبء الإجمالي لحوكمة الأمن الجماعي في الاتحاد الأوروبي.

إن مدارسة حوكمة الأمن في الاتحاد الأوروبي كمشكلة عمل جماعي وفق تحليل المنتج المشترك تجعلنا نخلص إلى أن الدول الأعضاء الأصغر في الاتحاد الأوروبي ليست حرة في رؤية سياسات الأمن

الجماعي، على عكس إحدى الفرضيات المركزية في أدبيات الاختيار العام التي توضح أن الدول الأعضاء في الاتحاد الأوروبي في الواقع تتقاسم التكاليف بالتساوي مع الأبعاد المختلفة للحوكمة الأمنية

لطالما اعتمدت امتيازات الاتحاد الأوروبي على تفويض سلطة الدولة العضو، ولكن تفويض السلطة في المسائل الأمنية غير مكتمل بشكل عام، وغير متساو في التطبيقفي كثير من الحالات، تختلف مساهمات الدول الأعضاء وغير الملزمة في حوكمة الأمن في الاتحاد الأوروبي، الحد من فعالية الاتحاد الأوروبي كجهة فاعلة أمنية ، وطرح سؤال مهم: هل تشارك الدول الأعضاء عبء حوكمة الأمن بالتساوي؟

نوضح بالتفصيل تقنيات الإنتاج المحددة لمهام حوكمة الاتحاد الأوروبي ونناقش الاختلافات في مستويات الإعلان عنها في القسم االأخحير من الدراسة، نستكشف كيف تعاملت الدول الأعضاء في الاتحاد الأوروبي مع مشاكل العمل الجماعي التي تواجه حوكمة الأمن جزئيًا تناقض التوقعات المبنية على نماذج المنافع العامة، فإن أعباء إدارة الأمن الجماعي يتم تقاسمها بشكل منصف إلى حد ما، على الرغم من أن أعضاء الاتحاد الأوروبي الأكبر والأكثر ثراء يبالغون في المساهمة في أنشطة الإجبار والوقاية، في حين أن أعضاء الاتحاد الأوروبي الأصغريتعاملون معها وفق استراتيجيات قصيرة تطبيقا لقرارات المفوضية أو مجلس أوروبا[1].

نظرًا لأن التهديد ضد أي عضو في الاتحاد الأوروبي يخاطر بالتصعيد و زعزعة الاستقرار السياسي في أوروبا، والقدرة على معالجة التهديد بشكل مشترك له جوانب تتعلق بالمصالح العامة، ومع ذلك، فإن الخط الفاصل بين التهديدات ضد المصلحة الوطنية الأساسية في مقابل المصلحة الأساسية للاتحاد الأوروبي غامض وقابل للنقاش، وبالتالي، فإنه كلما اختلفت الدول الأعضاء في تقييمهم للمخاطر، سيكون توزيع المنافع غير متكافئ، كما أن قيود الموارد تزيد من تعقيد العمل المشترك، والأهم من ذلك، أن أعضاء الاتحاد الأوروبي يختلفون اختلافًا كبيرًا في قدرتهم على المساهمة في الردع والإجبار، لهذا تم تقنين خطة الأمن والدفاع الأوروبية (ESDP) كبديل لتوزيع التكاليف التشغيلية.

أخيرًا، يمكن للحكومات جني فوائد خاصة من خلال الانخراط في سياسات الأمن الجماعي،فتقاسم الأعباء في حوكمة الأمن في الاتحاد الأوروبي يختلف عبر السياسات الأمنية والحصول على ائتمان لتقليل الجريمة محليًا وزيادة الأمن جماعيا،وهو الهدف الرئيسي لسياسات الحماية الجماعيةفيما يتعلق بتوفيره اللسلعة الحيوية الأولى وهي الأمن عبر آليات تعبر عن المنفعة العامة، من ناحية أخرى، الدول الأعضاء التي لديها أكثر قوانين العقوبات تساهلًا وأقلها استعدادًا لمشاركة المعلومات تحد من القدرة على تحقيق الهدف المشترك

[1] Dorussen, H., Kirchner, E, & Sperling, J. ***Op.cit.***

المتمثل في مكافحة الجريمة المنظمة أو الإرهاب السيبراني بشكل جماعي، كما تبحث الجريمة المنظمة والخلايا الإرهابية إلى البحث عن ملاذات آمنة تخلقها هذه البيئة وتستغلها للتخطيط لعمليات تؤثر على المواطنين في جميع أنحاء أوروبا ليس في تلك الدولة فحسب[1].

مما سبق نخلص إلى أن الدول الأوربية ألزمت نفسها بمواصلة تطوير قدراتها الوطنية للدفاع السيبراني وتعزيز الأمن السيبراني لشبكاتها، الاستراتيجية التي تعتمد التي تعد أولوية قصوى لضمان الدفاع عن شبكاتها الوطنية، لهذا الغرض تتعاون الدول الاوربية ضمن تحالفات (دول الاتحاد الاوربي وحلف الناتو) مع السلطات الوطنية لضمان مستوى مناسب من الدفاع الإلكتروني لرابطة الدول المستقلة الوطنية، يتم إضفاء الطابع الرسمي على هذا التعاون في مذكرات التفاهم الموقعة بين مجلس إدارة الدفاع السيبراني والدول المعنية، حيث تستند مذكرات التفاهم الخاصة بالدفاع السيبراني إلى نموذج تم تطويره في خطة عمل الدفاع السيبراني المشترك عبر وضع أسس الدعم المتبادل في مجال الدفاع السيبراني، بما في ذلك تبادل المعلومات والمشاركة في التدريب والتمارين، بالإضافة إلى توفير المساعدة المتبادلة في شكل استخبارات و "وتوقيع مذكرات تفاهم وتعاود لضمان الأمن الجماعي في شقه السيبراني[2].

المطلب الخامس: بين أمننه الانترنت وحقوق الإنسان

يتركز المنشأ الإشكالي للأخلاقيات في ظل البيئات السيبرانية في كيفيات وحدود استخدام التكنولوجيات والتطبيقات المتاحة وتجنب السلوكيات اللامعيارية Anti-normative behavior بحسب تعبير الباحثين Freestone and Mitchell والتي تعكس مختلف السلوكيات والممارسات التي ينخرط فيها المستخدم كفاعل أساسي خصوصا في ظل غياب الناظم والمنظم التقني والمعياري في غالب الأحيان.

إذ أن رقمنة Digitalization حضور الأفراد داخل الفضاء السيبراني أدى إلى استيلاد أشكال جديدة للفعل الاجتماعي وأنماط مستحدثة للسيرورات الجماعية وخلق مفاصيل سوسيو-نفسية خاصة بهذا المجال الاجتماعي الجديد New social realm، والذي أضحى مجالا للتعبير وإنتاج سلوكيات لا تمتثل لأي رادع، اذ يمكن للمستخدمين وفي ظل الحس الزائد بالحرية المفرطة Extreme sense of freedom، إنتاج أي خطاب في شكله السوي وغير السوي وفي الأخير الانسحاب بكل مرونة وبدون عواقب مترتبة على ذلك في الغالب، إضافة إلى ذلك، لا بد أن نسلم أيضا بوجود جملة من العوائق المفاهيمية والمنهجية والميتودو-تقنية التي تحد من دينامية التفكير الأخلاقي ethical reflection في الفضاء السيبراني وتعطل محاولات استقصاء المسارات المنعرجة للتفاعل التكنو-أخلاقي بداخله[3].

---

[1] Dorussen, H., Kirchner, E., & Sperling, J. ***Op.cit.***

[2] Wiesław Goździewicz, ***Op.Cit.***

[3] بلقاسم أمين بن عمرة، "مقترب ايتيقي للفضاء السيبراني نظرية العدالة عند جون راولز أنموذجا"، ***مجلة الناصرية للدراسات الاجتماعية والتاريخية***، مجلد 10، عدد 2 ديسمبر 2019، ص 680-727.

إضافة لذلك، فإن ضمان مصداقية الخدمات الرقمية أمر بالغ الأهمية لبناء نظام بيئي رقمي موثوق وصحي في أوروبا، والتي تعتمد على عنصرين رئيسيين:

- امتلاك الأدوات اللازمة للتعامل بشكل صحيح مع العدد المتزايد من التهديدات الإلكترونية على المستوى الأوروبي.
- ضمان الحق الأساسي للمواطنين الأوروبيين في الخصوصية، حرية التعبير، وحماية البيانات[1].

في هذا الصدد حاول الاتحاد الأوروبي والدول الأعضاء فيه معالجة التهديدات السيبرانية الجديدة، لكن هذه المعالجة السوسيو–أمنية تتقاطع في مضمونها مع مبادئ الديمقراطية والحقوق الأساسية للأفراد[2]، وقد تم استخدام الخطاب الرسمي حول المخاطر الحقيقية والمتخيلة للإرهاب السيبراني بشكل مماثل لتبرير "**المراقبة الرقمية**" العشوائية لعامة السكان، ظهرت بعض الأدلة على هذه المراقبة الجماعية بعد أن كشف إدوارد سنودنالمتعاقد السابق بوكالة الأمن القومي (NSA) في عام 2013 عن تسريبات عن جمع وتعدين البيانات الفوقية واتصالات الإنترنت من قبل أجهزة المخابرات البريطانية، تضمنت الجهود السرية للمراقبة الواسعة للإنترنت شركات الاتصالات السلكية واللاسلكية لمنحها وصول "باب خلفي" إلى أنظمتها بالإضافة إلى استخدام برامج سرية للغاية مثل "XKeyscore" لجمع "كل ما يفعله المستخدم تقريبًا على الإنترنت"، كما كشفت تسريبات سنودن من وكالة الأمن القومي، فإن تجميع جميع اتصالات الإنترنت قد انتقل بشكل كبير إلى ما هو أبعد من محاربة الشبكات الإرهابية إلى إنشاء "**نظم للمراقبة الجماعية**" التي تراقب المواطنين العاديين والقادة الأجانب على حد سواء، مما خلق مخاوف مشروعة بشأن "**دولة مراقبة**" تنفجر وتنتهك خصوصية المواطنين وحقوقهم الديمقراطية دون أي شبهات لخضوعم لمعايير تصنيفهم كإرهابيين.[3]

من ناحية أخرى، تظهر وثائق السياسة الأخيرة أنه "من المرجح أن تصبح القوات المسلحة أكثر انخراطًا في دعم مرونة قطاع الأمن المدني في الدولة والمجتمع ككل" ، وأن هناك علاقة أساسية دائمًا بين الأمن والمراقبة والخصوصية والحقوق الأساسية كما هو معترف به في وثائق سياسة الاتحاد الأوروبي ذات الصلة، كما أن زيادة "الوعي بأمن المعلومات أمر صعب في كثير من الحالات، حيث يرى الجمهور أن الأمن هو مراقبة تدخلية وتدخل غير مرغوب فيه في الحقوق والحريات الشخصية"[4]

وهذا يقودنا لجزئية التعارض بين الأمن والقيم الأوربية، وفي إطار ذلك سنناقش النقاط التالية:

---

[1] Rafael Rivera Pastor & others, ***Op.cit.***

[2] Jukka Ruohonen, "An Acid Test for Europeanization: Public Cyber Security Procurement in the European Union", ***European Journal for Security Research***, (2020) 5, Pp: 349–377,in:https://doi.org/10.1007/s41125-019-00053-w (21/09/2021)

[3] Aziz Douai***, Op.cit***, p 450.

[4] Jukka Ruohonen, ***Op.cit***. p 373

1- حقوق الانسان والأخلاقيات السيبرانية.

بدأت حركية التنظير للأخلاقيات السيبرانية في الانتشار مع بداية انتشار الحوسبة، حيث استخدم الباحث جيمس مور James Moor[1*] آنذاك مصطلح أخلاقيات الحاسوب Computer ethics للإحالة إلى المعايير الإيتيقية التي ينبغي الالتزام بها، لكن نتيجة للانتشار السريع لشبكة الانترنت بمنصاتها المختلفة وكثافة حضورها ونتيجة لظهور الكثير من الممارسات اللامعيارية واللاايتيقية المرتبطة بالتكنولوجيا، اتجه بعض الباحثين الى ضرورة أخلقة الانترنت، من أمثال الباحثين Kuiper,Volman & Jan Terwel ونجد أن من أدق التعاريف التي قدمت للأخلاقيات السيبرانية، تعريف الباحث Torun والذي يتمثل بمقتضاه الأخلاقيات السيبرانية ككيفيات التصرف التي ينبغي للأفراد الاحتكام إليها وتبنيها أثناء استعمالهم للأنترنت[2].

من هذه الناحية، من المهم النظر إلى الأخلاقيات السيبرانية ترتكز على جزئيتي الاعتماد المتبادل والعلاقات بين حقوق الإنسان المختلفة في سياق الإنترنت، حيث أن ضمان حماية الخصوصية مهمة في التعامل مع الأمن السيبراني. وهنا تشمل مختلف الحقوق الأخرى التي لم تتم مناقشتها هنا، مثل حرية تكوين الجمعيات، اضافة إلى تلك التحديات والقيود المباشرة، هناك تحديات أخرى غير مباشرة يتمثّل أهمها في التقاطع بين استخدام تطبيقات الذكاء الاصطناعي وغيرها من التقنيات الحديثة لأغراض أمنية، والمقومات الأساسية لحقوق الإنسان والخصوصيات الفردية والجماعية[3].

حرية التعبير:

تتضمن حرية التعبير أن يكون لدى الجميع الحق في حرية التعبير، يتضمن هذا الحق حرية البحث والتلقي ونقل معلومات جميع الأنواع والأفكار، ينبغي أن تكون هناك حد قيود على حرية التعبير هي الاستثناء وليس القاعدة، وحرية التعبير محمية بموجب الإعلان العالمي لحقوق الإنسان UDHR (المادة 19) والعهد الدولي الخاص بالحقوق المدنية والسياسية (المادة 19)، ينبغي لأي قيود على حرية المعلومات الامتثال للمادة 29 من UDHR والمادة 19 من العهد الدولي الخاص بالحقوق المدنية والسياسية.

كما خلصت الاتفاقية الأوروبية لحقوق الإنسان في (المادة 10)، والاتفاقية الأمريكية لحقوق الإنسان (المادة 13) على أن الآليات التي تنظم حرية التعبير أيضا على الإنترنت، تبعهما قرار مجلس حقوق الإنسان التابع

---

[*] جيمس مور James Moor هو أستاذ الفلسفة الفكرية والأخلاقية في كلية دارتموث Dartmouth College، والحاصل حصل على الدكتوراه في عام 1972 من جامعة إنديانا بالولايات المتحدة الأمريكية، قدم عام 1985 ورقته المشهورة "ما هيأخلاقيات الكمبيوتر؟" رسخه كواحد من المنظرين الرائدين في مجال أخلاقيات الكمبيوتر.

[2] بلقاسم أمين بن عمرة، ***مرجع سابق.***

[3] سامح راشد، "الذكاء الاصطناعي في مواجهة الإرهاب، فرص وتحديات"، ***مجلة درع الوطن***، 1\02\2022، في:https://cutt.us/EMG8d(2022/04/04)

للأمم المتحدة في سرده لمبادئ حقوق الإنسان على الإنترنت مؤكدا على "أن نفس الحقوق التي يجب أن يتمتع بها الأشخاص غير المتصلين عبر الإنترنت، في حرية التعبير الخاصة، تنطبق علىالأنترنت[1].

ومع تطور التهديدات ظهرت بوادر للمساس ببعض هذه القيم، فوضع الاتحاد الأوروبي نظاما أوليا منذ عام 1999 على نطاق الاتحاد برمّته لتنظيم الحريات المقبولة لمحتويات الانترنت والإجراءات ذات الصلة وقدم (برنامج انترنت أكثر أمانا)،الذي ينطلق من مبدأ التنظيم الذاتي واستبعاد المحتوى غير اللائق، بالموازاة مع التشريعات الوطنية[2]، فالنقاش داخل الدوائر الأمنية الأوربية أكد على إمكانية الشبكات الاجتماعية في أن "تُدعّم وتُعزّز وجود هوية جماعية ووجود إحساس وانتماء بين أفراد المجموعة الواحدة، بحيث تربطهم قضية واحدة، وهدف مشترك، وقيم متماثلة"، وهو ما يتضح من خلال الكم الهائل من الصفحات التي تجمع أفرادا لهم نفس الأفكار والتوجهات سياسيا، ثقافيا أو دينيا، ومن خلال حسابات الجماعات المتطرفة التي تجمعها أيديولوجيا وهوية واحدة[3]، وأن بعض القيم الدخيلة قد تمس قيم الأمن المجتمعي ومنه الأمن الجماعي.

تبعا لذلك تغيرت المعادلة من الحريةّ المطلقة إلى أمننة الانترنت، ففي 13 سبتمبر 2017، صرّح رئيس المفوضية الأوروبية قائلا بأن "الاتحاد الأوروبي مضى قُدُما نحو أمننة الانترنت، لكنه حذر من عدم التصدي الجيد للهجمات السيبرانية التي تهدد الديمقراطية والاقتصاد بشكل متزايد"، وكانت المفوضية قد أصدرت العديد من التوجيهات منذ بداية الألفية تتعلق بحماية الحقوق الأساسية وحريات المواطنين الأوروبيين في إطار النشاط عبر الانترنت، بما يشمل النشاط الاقتصادي والتجاري[4].

كما تشير الوقائع والدراسات إلى وجود تناقضات من حيث كيفية تطبيق القيم الأوروبية في سياق التقارب بين الأمن الداخلي والخارجي، على الرغم من أن الاتحاد الأوروبي يجادل بأنه ملتزم بشدة بدعم الديمقراطية وسيادة القانون والحقوق الأساسية، فليس من غير المعتاد ملاحظة تعاون الاتحاد الأوروبي مع الدول التي لا تشارك نفس الاحترام لهذه القيم من أجل معالجة التهديدات المشتركة على المستوى الوطني والإقليمي[5].

- **الخصوصية العامة والأمان:**

يطرح الفضاء الإلكتروني مشكلات قانونية كتلك المتصلة بالحياة الخاصة (الخصوصية) وحرية التعبير، بالرغم من أن الاتفاقية الأوروبية لحماية حقوق الإنسان والحريات الأساسية في مادتها العاشرة تكرّس لحرية

[1] CSTD (2015), Commission on Science and Technology for Development, ***Mapping of international Internet public policy issues***, Eighteenth session, Geneva, 4-8 May 2015, p 32.

[2] حمدون إ. توريه، فريق الرصد الدائم لأمن المعلومات، الاتحاد العالمي للعلماء، ***البحث عن السلام السيبراني***، (منشورات الاتحاد الدولي للاتصالات، يناير 2011) ، ص41.

[3] سماح عبد الصبور، ***مرجع سابق***.

[4] Deschaux-Dutard, ***Op.cit***. p. 19, 21.

[5] Helena Carrapico, André Barrinha, ***Op,cit.***

التعبير واعتناق الآراء، ومن أن المحكمة الأوروبية وصفت هذه الحرية بأنها من صميم قيم المجتمع الديمقراطي[1].

من ناحة أخرى، يرى الاتحاد الأوروبي في الإرهاب السيبراني ظاهرة تهدد قيم الديمقراطية وحقوق الإنسان في المجتمعات الأوروبية، ولهذا يجري التعامل مع مكافحة الإرهاب في شكله التقليدي والمستحدَث كأولوية بالنسبة للاتحاد، ويتم الاهتمام بالسياسات "الناعمة" كالتربية والتعليم والثقافة في التصدي لتهديد خطير ومستمر بهذا الحجم[2]. و هو ما جاء في أجندة الاتحاد الأوروبي لمكافحة الإرهاب (9 ديسمبر 2020) بعنوان: "**توقُّع، منع، حماية، استجابة**" ما يؤكد على اهتمام الاتحاد الأوروبي بأولوية قيمه في سياسات مكافحة الإرهاب[3].

كما نشير لأن قوانين الاتحاد الأوروبي تستبعد الاحتفاظ بالبيانات الشخصية العامة والعشوائية، ومع ذلك فقد تم تحديد بعض الحالات التي تبيح الاحتفاظ بالبيانات[4] (لغرض التحقيقات على سبيل المثال)، كما أنها تلزم مزودي الانترنت بتسليم السلطات الأوروبية أي بيانات يمكن ان يجمعوها عن الإرهاب، وهو ما اتبعته فرنسا في تحقيقاتها في جل الحوادث الإرهابية [5].

في أعقاب ما كشف عنه إدوارد سنودن Edward Snowden في عام 2013، أصبحت مسائل الخصوصية وحماية البيانات مصدر قلق متزايد للمجتمع اليوم، وبفضل المناقشات والإجراءات السياسية والاجتماعية المثمرة رفيعة المستوى، يُنظر إلى أوروبا باعتبارها صاحبة مصلحة موثوق بها في العالم عندما يتعلق الأمر بأمن البيانات والخصوصية، الوضع الذي يجب الحفاظ عليه وتطويره بدعم من سوق الأمن السيبراني الأوروبي القوي والمتنافس بما يتماشى مع متطلبات الخصوصية وحماية البيانات في الاتحاد الأوروبي[6]، يناقش هذا الأمر الحاجة والاجراءات الممكنة لمبادرة سياسية شاملة في سياق مجتمع المعلومات

[1] Nina Olesen, European Public-Private Partnerships on Cybersecurity - An Instrument to Support the Fight Against Cybercrime and Cyberterrorism, in: B. Akhgar and B. Brewster (eds.), ***Combatting Cybercrime and Cyberterrorism, Advanced Sciences and Technologies for Security Applications***, Switzerland : Springer International Publishing, 2016, p: 259- 278

[2] « 20 years after 9/11: Achievements and Challenges of EU Counter-Terrorism Efforts », in: https://www.consilium.europa.eu/en/events-gsc/live-show-counter-terrorism/(21/12/2021)

[3] European Commission, COMMUNICATION FROM THE COMMISSION:A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond, COM(2020) 795 final (Brussels, 9.12.2020), p.1.

[4] A Counter-Terrorism Agenda for the EU, p.19.

[5] حسن سعد عبد الحميد، مرجع سابق.

[6] Nina Olesen, ***Op.cit,*** p 259- 278

الأوسع وأهداف الحرية والأمن والعدالة لتحسين أمن البنى التحتية للمعلومات ومكافحة الجرائم الإلكترونية، وفقًا لالتزام الاتحاد الأوروبي باحترام حقوق الإنسان الأساسية[1].

يتقاطع هذا في جزئياته المعيارية مع معظم الجرائم التي تستهدف المحتوى غير القانوني والتي لها علاقة قوية بحرية التعبير، التي تعد عنصرًا أساسيًا في المجتمعات الأوروبية الديمقراطية والتعددية. وهذا مهم بشكل خاص في السياق الحالي لأن النشر الحر للمعلومات والأفكار هو أكثر الوسائل فعالية لتعزيز التفاهم والتسامح، والذي يمكن أن يساعد بدوره في منع الإرهاب. يتم تناول هذه الجوانب من خلال العديد من الإعلانات الدولية والأوروبية التي تعالج التوتر بين مكافحة الإرهاب وحماية حقوق الإنسان[2].

- **الأمن الخاص:**

لقد كان الاهتمام بحماية الخصوصية جزءًا لا يتجزأ من الفكر والممارسة الليبرالية الحديثة، حيث تم توجيه جوهرها الأساسي نحو حماية المجال الخاص مما يُنظر إليه على أنه القوى العامة القمعية المحتملة لبيروقراطيات الدولة والديمقراطية الجماهيرية، ربما يكون الاهتمام بالخصوصية أكثر وضوحا في أوروبا وفقا لتجربة دولها ، مع أحكامها الخاصة بالحقوق الفردية والضوابط والتوازنات المتعددة ضد تركزات القوة. ومع ذلك، فهو مصدر قلق يتجلى في جميع الدول الديمقراطية الليبرالية في جميع أنحاء العالم ويعتبر بشكل عام حقًا أساسيًا من حقوق الإنسان.

على الرغم من أن التهديدات المتصورة للخصوصية ليست جديدة، فقد جادل المدافعون في جميع أنحاء العالم بأن التقنيات الجديدة، بما في ذلك الإنترنت، قد زادت المخاطر بشكل كبير، ويمكن الآن رقمنة المعلومات المتعلقة بالأفراد، والتي كان من الممكن أن يتم جمعها يدويًا وحفظها وتخزينها في وقت ما، ومشاركتها بين قواعد بيانات الكمبيوتر الضخمة. علاوة على ذلك، نظرًا لأن المزيد من جوانب المجتمع والاقتصاد يتم دمجها في بيئة الوسائط التشعبية، يتم أيضًا طي كمية متزايدة من المعلومات الشخصية. على حد تعبير ليونLion،"**من نواح عديدة، أصبح ما كان يُعتقد أنه استثناء هو القاعدة، حيث تستخدم الوكالات المتخصصة للغاية وسائل متطورة بشكل متزايد لجمع البيانات الشخصية بشكل روتيني، مما يجعلنا جميعًا أهداف المراقبة**"[3]

يشمل مؤيدو هذه الصورة الجماعية كلاً من الجهات الحكومية وغير الحكومية على حدٍ سواء. من بين العديد من الدول الديمقراطية الليبرالية تم إنشاء مفوضي الخصوصية أو الوزارات التي وضعت قوانين ولوائح لحماية الخصوصية. ربما يكون أكثرها تفصيلاً هو توجيه حماية البيانات الأوروبية، الذي دخل حيز التنفيذ

[1] European Commission. (2001c). Communication on creating a safer information society by improving the security of information infrastructures and combating computer-related crime, ***Op.cit.***

[2] Ulrich Sieber, international cooperation against terrorist use of the internet, ***Revue internationale de droit pénal*** , Vol. 77, (2006|3|4), P-p:395 – 449.

[3] Deibert, Ronald J. ***Op.cit***, P-p:115-142.

في أكتوبر 1998، ينشئ هذا التوجيه مجموعة من الحقوق والحماية للخصوصية التي تشمل تدابير صارمة ضد تجارة المعلومات الشخصية مع الشركات أو البلدان خارج أوروبا التي لا تلتزم بشروط نظام الخصوصية.

بصرف النظر عن لوائح الخصوصية الرسمية المشار إليها أعلاه، فإن عنصر السياسة العامة الذي يوحد دعاة الخصوصية الإلكترونية هو الإلغاء الكامل لتقنيات التشفير – وهي خطوة تضعهم مباشرة في مواجهة وكالات إنفاذ القانون والاستخبارات التابعة للدولة. فيما يبدو أنه موقف متناقض، فإن الخصوصية الإلكترونية تدافع بقوة عن أي محاولات حكومية لتنظيم التشفير حتى أثناء الجدل بأن الإنترنت بطبيعته محصن ضد الدولة التنظيم.

- **الولاية القضائية كضابط لحدود الحرية السيبرانية:**

للدولة في ممارسة ولايتها القضائية (أي فرض وإنفاذ والحكم) على الأشياء والأشخاص الموجودين فعليًا (أو قانونيًا) في أراضيها. يبدو أنه لا جدال في أنه، ما لم تكن مقيدة بقواعد القانون الدولي المعمول بها (بما في ذلك قانون حقوق الإنسان على الأرجح)، فإن البنية التحتية الإلكترونية الموجودة داخل أراضي الدولة والأنشطة السيبرانية التي تحدث فيها تكون عرضة للتدابير الإلزامية والإنفاذ غير المحدودة تقريبًا من قبل الدولة المعنية. تشمل الولاية القضائية الإقليمية حق الدولة في تنظيم أو تقييد أو حظر الوصول إلى البنية التحتية الإلكترونية الخاصة بها سواء داخل أراضيها أو من خارج تلك المنطقة. يجب إعادة التأكيد على أن دمج المكونات المادية، أي البنية التحتية الإلكترونية الموجودة داخل أراضي الدولة، في "المجال العالمي" للفضاء الإلكتروني لا يمكن تفسيره على أنه تنازل عن ممارسة السيادة الإقليمية والولاية القضائية. في ضوء تنقل المستخدمين والأنظمة الموزعة على السحابة أو الشبكة، قد يكون من الصعب في كثير من الأحيان ممارسة الولاية القضائية الإقليمية بشكل فعال. ومع ذلك، فإن هذه الصعوبات لا تبرر الاستنتاج بأن الولاية القضائية الإقليمية، إذا طُبقت على الفضاء الإلكتروني تصبح غير ذات جدوى. بل على العكس من ذلك، أثبتت الدول بانتظام وبنجاح كبير – رغم عدم الإشادة بها دائمًا – استعدادها وتصميمها على إنفاذ قوانينها المحلية تجاه جميع أنواع الأنشطة السيبرانية.

من السمات المحددة للولاية القضائية الإقليمية ما يسمى بـ "عقيدة التأثيرات" التي بموجبها يحق للدولة ممارسة ولايتها القضائية على سلوك لا يحدث داخل إقليمها، ولكنه ينتج عنه آثار (ضارة) في تلك المنطقة.

في هذا الشأن قدم المدعي العام الأوروبي شرحًا مفيدًا لهذا المبدأ:

"القاعدتان غير المتنازع عليهما اللتان تقوم عليهما ولاية الدولة بموجب القانون الدولي هما الإقليمية والجنسية. يمنح القانون الأول الولاية القضائية على الدولة التي يوجد فيها الشخص أو البضائع المعنية أو وقع الحدث المعني. ويمنح هذا الأخير الولاية القضائية على مواطني الدولة المعنية. لقد أدت الإقليمية نفسها إلى ظهور مبدأين متميزين من مبادئ الولاية القضائية:

عند تطبيقه على المجال السيبراني، قد تؤدي عقيدة التأثيرات إلى ممارسة الولاية القضائية على الأفراد الذين أجروا عمليات إلكترونية ضد البنية التحتية الإلكترونية في دولة أخرى

باختصار، يمكن القول إن مبدأ السيادة الإقليمية والحق المترتب على ذلك لدولة ما في ممارسة ولايتها الإقليمية ينطبق على الفضاء السيبراني بقدر ما يتعلق الأمر بالبنية التحتية الإلكترونية داخل الإقليم (أو على المنصات التي تمارس عليها الدولة ولاية قضائية حصرية). وينطبق الشيء نفسه على الأفراد الموجودين في تلك المنطقة أو على السلوك الذي يحدث إما داخل تلك المنطقة أو ينتج عنه آثار (ضارة) عليها. إن ممارسة الولاية القضائية بموجب أي من القواعد المعترف بها بموجب القانون الدولي محدودة فقط إذا كانت هناك قواعد صريحة بهذا المعنى. لا تشكل خصائص الفضاء الإلكتروني عقبة أمام ممارسة السيادة الإقليمية والولاية القضائية[1].

[1]Wolff Heintschel von Heinegg, Legal Implications of Territorial Sovereignty in Cyberspace, 4th International Conference on Cyber Conflict, Faculty of Law Europa-Universität, Frankfurt (Oder), Germany, (2012), P-p: 7-19.

المبحث الثالث: الأمن السيبراني الأوروبي بين ثغرات السياسات والتدابير التقنية والإجرائية.

يُعَد هذا المبحث قراءة في إستراتيجية الأمن والدفاع السيبراني في أوروبا، ومحاولة للكشف عن الثغرات الموجودة في ظل عولمة التهديدات الأمنية ونمو خطر الإرهاب الإلكتروني، وبعد أن أصبحت فكرة إنشاء مجال عام في الفضاء غير المادي ضرورة فرضتها متطلبات الحوكمة الأمنية إلى جانب التحولات السياسية والاجتماعية والأمنية المرافقة للثورة التقنية والمعلوماتية. كما يتناول المبحث الشراكة بين القطاع العام والقطاع الخاص في مجال الأمن السيبراني، وفي الأخير تقييم أوّلي للسياسات الأوروبية المتبعة لضمان الأمن السيبراني وتعزيز واجهة الدفاع الإلكتروني، في مقابل الثغرات والتحديات الراهنة والمطروحة.

المطلب الأول: إنشاء المجال العام في الفضاء السيبراني الأوروبي.

أ- مفهوم المجال العام وظهور المجال العام السيبراني:

يعود استخدام مفهوم المجال العام (public sphere) إلى 1961 مع صدور كتاب "التحول البنائي للمجال العام" للمفكر والفيلسوف الألماني "يورغن هابرماس" (Jurgen Habermas) * ، ثم انتشر بداية من 1989 عندما صدرت النسخة الإنجليزية للكتاب[1]بعنوان: Structural Transformation of the Public Sphere. ويشير المفهوم إلى مجال يتوسط المجالين الرسمي والخاص، أي أنه يقع بين مجال الدولة والمجتمع ويرتبط بتكوين مواطن فاعل يشارك في المصلحة العامة للمجتمع[2]. لقد ربط "هابرماس" مفهوم المجال العام بمستوى الانفتاح الذي يميز الحوار والنقاش بين الأفراد، بعيدا عن ضغط المجتمع وسلطوية الدولة، حيث تسود حرية الرأي والتعبير، وتظل الدولة في المقابل "هيئة عامة، مهمتها تعزيز الرفاهية المشتركة أو العامة لأفرادها"، وانطلاقا من ذلك يمكن إعطاء تعريف له كما يلي[3]:

"ميدان عام، ليس جزءا من الدولة أو امتدادا لها، لكنه وسيط بين المجال الخاص بالفرد والمجال الخاص بالدولة.. فيلتقي فيه الأفراد لمناقشة القضايا المشتركة وتبادل الآراء، للوصول إلى موقف مشترك، وغالبا ما يلزم الأمر توليد ضغط لتحقيق تغيير سياسي أو قانوني".

---

[1] سارة البلتاجي، ***الأمن الاجتماعي- الاقتصادي والمواطنة الناشطة في المجتمع المصري***، ط1، (قطر: المركز العربي للأبحاث ودراسة السياسات، 2016)، ص35.

[*] "يورغن هابرماس" (1929-) فيلسوف ومفكر ألماني، أحد أشهر مفكري مدرسة فرانكفورت (النقدية الاجتماعية)، وهو صاحب نظرية الفعل التواصلي ومطور فكرة المجال العام.

[2] مهند مصطفى، "حول مفهوم وحدود المجال العمومي"، ***مجلة مدى الكرمل***، العدد 29 (يناير 2016)، ص: 1-4.

[3] سارة البلتاجي، ***مرجع سابق***، ص. 36-37.

[*] رأى البعض أن الترجمة الإنجليزية لكتاب هابرماس ولمفهوم المجال العام تحديدا كانت ضيقة وغير معبّرة عن حقيقة المفهوم كما جاء بلغته الأصلية (أي الألمانية). أُنظر:

Jostein Gripsrud, Hallvard Moe, ***The Dogital Public Sphere: Challenges for Media Policy*** (Sweden: Nordicom, 2010), p.28.

كما يُعرف مفهوم الفضاء العام* بأنه يرمز إلى مكان يجتمع فيه الأفراد (المواطنون) ليشكلوا الرأي العام من خلال مجموعة الأفكار ووجهات النظر التي تحمل المصلحة العامة، والتي يناقشونها باستقلالية ليمارسوا تأثيرا على المؤسسات السياسية وعلى المجتمع،وانطلاقا من هذا التعريف يوصَف المجال العام السيبراني بأنه مجال عام جديد New Public Sphere.[1]

ويتحدد الاختلاف بين المجال العام الواقعي والمجال العام السيبراني في جوانب عديدة، من بينها أن التفاعل في الأول مباشر (وجها لوجه)، في حين يكون التفاعل في الفضاء السيبراني العام عبر الوسائط الإلكترونية (ليس وجها لوجه)، وبعيدا عن أيّة قيود متصلة بالمكان والشكل والعمر، أو غير ذلك[2]. هذه الازدواجية لم تكرّس للقطيعة بين المجال العام التقليدي والافتراضي بقدر ما عزّزت مناخا متطورا لتبادل وجهات النظر والنقاش في القضايا الأساسية للمجتمعات، أوكما يقول "لامباش"** Daniel Lambache[3]:

"حيث يمكن إحضار الفضاء الإلكتروني إلى العالم الحقيقي من خلال الهواتف الذكية وشاشات العرض الضوئية وانترنت الأشياء وغيرها. وفي المقابل، يتم إحضار العالم الحقيقي إلى الفضاء السيبراني من خلال تقنيات تحديد الموقع الجغرافي، والتي غيرت بشكل جذري طابع الانترنت".

إن المجال العام غير محتكر في العالم المادي، فمع تطور تكنولوجيا الإعلام والاتصال بات الفضاء غير المادي أيضا ميدانا للحوار والنقاش وتشكيل الوعي العام بقضايا المجتمع، وهو ما أثار اهتمام الحكومات الأوروبية. لقد أعطت الانترنت للأفراد فرصا جديدة للتواصل والتفاعل والمشاركة بصورة أوسع بالمقارنة مع وسائل الإعلام التقليدية. فإذا كان الراديو كوسيلة سمعية يزودك بالأخبار والمعلومات، والتلفزيون كوسيلة سمعية–بصرية يتيح متابعة البرامج المتنوعة على مدار اليوم، فإن الانترنت، وما أفرزه من إعلام جديد، يسمح للمواطنين بالتواصل والتفاعل ومشاركة المعلومة والخبر بصفة أكثر حرية.

يوضح الشكل الآتي، بأسلوب بسيط، بعض العناصر المتدخلة في التحول النظري من نموذج يوضح الشكل الآتي، بأسلوب بسيط، بعض العناصر المتدخلة في التحول النظري من نموذج "هابرماس" إلى المجال العام الجديد (السيبراني):

---

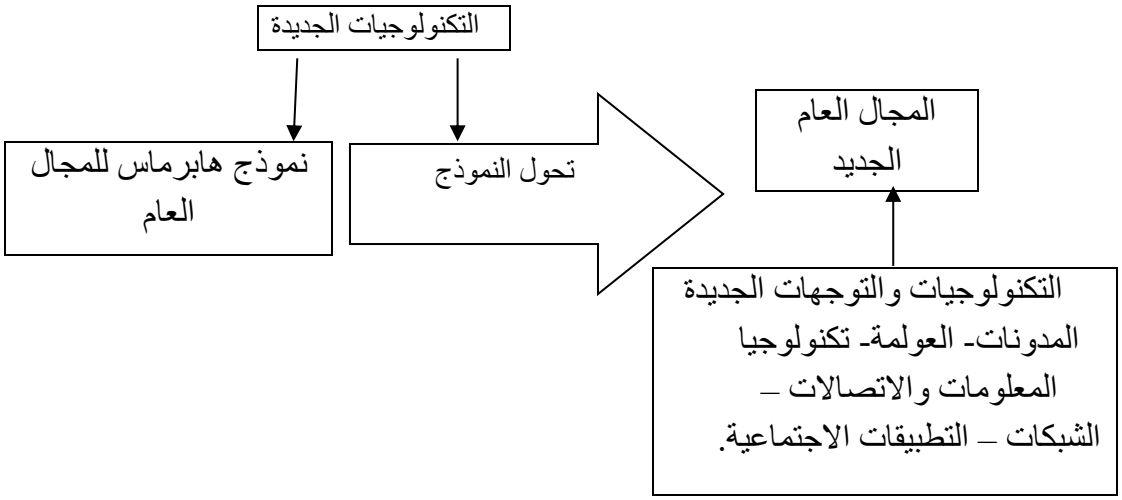
[1] Muhammad Zubair Khan, Iijaz Shafi Gilani, Allah Nawaz, « From Habermas Model to New Public Sphere: A Paradigm Shift », ***Global Journal of Human Social Science*,** vol.12, Issue 5 (2012), p-p: 43,45.

[2] Rick Frank Jorgensen, ***Internet and Freedom of Expression***,European Master Degree in Human Rights and Democratisation (Raoul Wallenberg Institute, 2000-2001), p.27.

[3] دانيال لامباش، "السيادة الإلكترونية: اتجاهات تشكيل مناطق سيبرانية تحت سيطرة الدول والشركات"، مركز الإمارات للدراسات والبحوث المتقدمة، 2020/09/23، https://bit.ly/3GjlbWx (2021/07/23)

** "لامباش" هو أستاذ وباحث ألماني، متخصص في العلاقات الدولية ومهتم بتأثير التكنولوجيا، عمل كأستاذ زائر بالجامعات الأوروبية.

الشكل (12): التحول النظري من نموذج "هابرماس" إلى المجال العام الجديد.



Source: Muhammad Zubair Khan, Iijaz Shafi Gilani, Allah Nawaz, « From Habermas Model to New Public Sphere: A Paradigm Shift », ***Global Journal of Human Social Science***, vol.12, Issue 5 (2012), p: 48.

من خلال الشكل يلاحَظ أن التكنولوجيا الجديدة للإعلام والاتصال، وفي سياق العولمة التي جعلت من العالم قريةً كونية أو كوكبا صغيرا، برز مجال عام جديد يرتبط بالفضاء الرقمي ومساحات التواصل والنقاش الافتراضية، مما عزّز التقابل والازدواجية وأثّر من ناحية التنظير وفي سياق الواقع المعاش.

ب- المجال العام في الفضاء السيبراني الأوروبي:

منذ أن أصبح العالم الافتراضي يوازي العالم المادي ويمارس تأثيرا واسعا متعدد الأبعاد، أدركت دول الاتحاد الأوروبي أن المجال العام الافتراضي بحاجة إلى الضبط والتقنين، لمجابهة التهديدات الحاصلة فيه أو بواسطته، وخاصة ما يتعلق بالتهديدات السيبرانية ومن ضمنها الإرهاب الإلكتروني. ولكن الحديث عن "إنشاء" (بهذا التعبير) المجال العام في الفضاء السيبراني الأوروبي يوحي بتدخل حكومي يضع حدودا لهذا المجال ويتحكم في الأشخاص الناشطين فيه، وهو أمر غير معقول لأن ضبط العالم الافتراضي يظل مسألة شديدة النسبية (يمكنك التحكم في السلوك المادي للفرد في حين لا يمكنك التحكم في أسلوبه في التفكير).

يعرّف "ترانز" Trenz المجال العام الأوربي بأنه "عملية توسيع نطاق الخطاب خارج الدولة القومية الإقليمية"، وقد يكون ذلك ذا صلة برؤية "هاس" * Ernst B. Haas في إطار الوظيفية الجديدة وحديثه عن انتقال الولاءات نحو مركز جديد (هو في هذه الحالة الاتحاد الأوروبي)[1]. وترى بعض الدراسات أن

[1] Jan Erick Kermer, Rolf A.Nijmeijer, « Identity and European Public Sphere in the Context of Social Media and Information Disorder », ***Media and Communication***, vol.8, Issue 4 (08/10/2020), p : 28, 31.

المجال العام، سواء الواقعي أو السيبراني، قد يعد تكريسا لجودة وفعالية الديمقراطية في أوروبا عموما، لهذا يقول "هابرماس": "لا يمكن القضاء على العجز في الديمقراطية إلا إذا ظهر المجال العام الأوروبي إلى حيز الوجود حيث تُدمَج العملية الديمقراطية"، ويرى في ذلك حلا لمشكلة عدم كفاية الاندماج الاجتماعي في عملية "الأَورَبة" (Europeanisation)[1].

لقد أصبحت الأنشطة السيبرانية الضارة أمرا عاديا في الحياة اليومية[2]، وحسب تقرير للاستخبارات الأمريكية في 2009 فإن "الفرد الرقمي المستخدم لوسائل التواصل الاجتماعي وشبكات الانترنت سيتحول إلى عنصر فاعل ولاعب مؤثر في اللعبة السياسية المحلية، وإلى شريك في رسم خارطة القوى الجيوسياسية الدولية"[3].

ويأتي خوف الحكومات الأوروبية من الانعكاسات السلبية التي تحملها الوسائط الإلكترونية ووسائل التواصل الاجتماعي على قيم الهوية والديمقراطية والأمن، فهي قد أصبحت –بشكل أو بآخر– وسيلة لنشر الأفكار المتطرفة والتغلغل بسهولة في أوساط المجتمعات لنشر خطاب الكراهية على أساس الدين والطائفة وحتى الجنس والنوع الاجتماعي، والأمر لا يتوقف عند ذلك وإنما يمكنه أخذ أبعاد أخرى أكثر ضررا من حيث المساس بالأمن القومي الذي بات يتصل أيضا بحماية المجال الافتراضي والسعي إلى ضبطه.

وخلال مؤتمر ميونيخ للأمن بألمانيا سنة 2017، تم التأكيد على أن الهجمات السيبرانية لا تستهدف البنى التحتية الحساسة للدولة فحسب، وإنما تستهدف أيضا استقرار النظام الغربي السياسي الأوروبي، بما يشير إلى قيم الديمقراطية والحرية وحقوق الإنسان حسب الرؤية الأوروبية[4].

ويطرح المجال العام في الفضاء الافتراضي تحديات على صعيد الهوية الوطنية والانتماء، فمن جهة عزّز الانترنت ظهور "مجتمعات افتراضية ضيقة"، مما يؤثر على التكامل الأوروبي ويجعل اختلاف الرؤى والتوجهات في تزايد، كما يكرس فرضية أن الانترنت سيفكك القرية العالمية، ومن جهة أخرى يمكن له تعزيز الولاء الجماعي والهوية الجامعة داخل الفضاء الأوروبي[5]. وفي جميع الأحوال يبدو أن المجال العام السيبراني الأوروبي مجزّأ وفوضوي[6]، خاصة وأن له تأثيرا في الهوية والقيم الديمقراطية ودرجة الاندماج

---

* "إرنست هاس" (1924-2003)، مفكر وعالم سياسة ألماني، له مساهمات بارزة في المدرسة الوظيفية الجديدة في عملية التكامل والاندماج.

[1] Georgios Papangnou, ***Digital Public Transnational Spaces : European Blogs and the European Public Sphere***, UNU-Cris Working Papers (2013), p.10.

[2] Eric Talbot Jensen, "The Tallinn Manuel 2.0 : Highlights and Insights", ***Georgetown Journal of International Law*****,** vol.48 p.736.

[3] علي لفتة العيساوي، "الفيسبوك- الوطن البديل للشباب وأثره السلبي على الشباب العراقي (دراسة وصفية تحليلية)"، ***سلسلة الاختراق الثقافي***، المركز الإسلامي للدراسات الإستراتيجية بالنجف-دولة العراق (2021)، ص58.

[4] Rémi Ravel, ***La Cyber-Coopération Européenne***, Les publications des jeunes IHEDN (Rapport, 2018), p.20.

[5] Jan Erick Kermer, Rolf A.Nijmeijer, ***Op.cit,*** p-p : 32-33.

[6] ***Ibid***, p.29.

والاستقرار في المجتمعات الأوروبية. هذا يدفع بنا إلى الحديث عمّا أسماه "جورج زاركاداكيس" George Zarkadakis * بالجمهورية السيبرانية، وهي نمط متقدم من الليبرالية حيث تتعزز الديمقراطية المباشرة بتقنيات "الأتمتة" (automation) لتكون أكثر إنصافا، وفي الجانب الآخر يواجه هذا النمط تحديات كثيرة ناتجة عن استخدام التكنولوجيا[1].

خلاصة القول هي أن مسألة إنشاء المجال العام في الفضاء السيبراني الأوروبي تتقاطع مع مجموعة من التحديات، وبالأخص ما يتعلق بحرية التعبير وقيم الديمقراطية بالمنظور الغربي- الأوروبي، ويمكن إضافة نقطة أخرى تتعلق بتنظيم هذا المجال، بما يشمله هذا التنظيم من جانب قانوني ووقائي، وهي مسألة تبقى نسبية في ظل انتشار التهديدات المتنوعة عبر الفضاء السيبراني وصعوبة التحكم فيها بصفة تامة.

المطلب الثاني: قراءة في ملامح الدفاع السيبراني الأوروبي.

أ- تعريف الدفاع السيبراني:

تعددت تعريفات الدفاع السيبرانيدون إيجاد تعريف شامل وأكثر دقة، ومن بين هذه التعريفات يذكر الدكتور إيهاب خليفة ما يلي[2]:

- ✓ "مجموعة القدرات النظامية التي تمتلكها القوات المسلحة للحماية من تأثيرات الهجمات الإلكترونية والتخفيف من حدتها والتعافي منها بسرعة".
- ✓ تعريف البرلمان الأوروبي: "عملية تطبيق الإجراءات الأمنية من أجل الحماية من الهجمات الإلكترونية والتعامل معها، وتستهدف تأمين البنية التحتية لنُظم الاتصالات والقيادة والسيطرة".
- ✓ تعريفه في الاستراتيجية البلجيكية: "تطبيق تدابير وقائية فعالة للحصول على مستوى مناسب من الأمن الإلكتروني، وتقليل المخاطر الأمنية إلى مستوى مقبول".

---

[1] جورج زاركاداكيس، "الجمهورية السيبرانية.. إعادة صياغة الديمقراطيات في عصر الآلات الذكية. كيف تواجه الأنظمة السياسية والاقتصادية تحديات الأتمتة؟"، عرض: هند سمير طه، في: 22 سبتمبر 2021، https://bit.ly/3ERlcPW (2021/10/15).

* "زاركاداكيس" (1964-)، باحث ومفكر يوناني خبير في مجال الذكاء الاصطناعي، له مجموعة مؤلفات قيمة في هذا المجال.

العنوان الأصلي للكتاب:

George Zarkadakis, ***Cyber Republic: Reinventing Democracy in the Age of Intelligent Machines*** (Londomn : the MIT Press, 2021).

[2] إيهاب خليفة، "تنامي التهديدات السيبرانية للمؤسسات العسكرية"، ***دورية اتجاهات الأحداث***، العدد 22 (جويلية- اوت 2017)، ص.54.

ما يمكن استخلاصه من التعريفات المقدَّمة هو أن الدفاع السيبرانييتمثل في حشد قدرات الدولة المختلفة وتفعيلها في البيئة الرقمية (عبر أساليب الوقاية والردع) لغرض حمايتها (أي حماية هذه البيئة) من التهديدات المستحدَثة المرتبطة بالفضاء الإلكتروني.

ب-الدفاع السيبراني الأوروبي:

توصف مؤسسات الاتحاد الأوروبي، مجلس أوروبا وحلف شمال الأطلسي بأنها مؤسسات إقليمية لها أدوار كبيرة في مجال الأمن والدفاع السيبراني، وهي بذلك الأكثر نشاطا وتحريكا لسياسات وآليات فعالة في هذا الصدد[1]. يمتلك الاتحاد الأوروبي وحدة للخبراء مكلفة بالجريمة الإلكترونية منذ 1996[2]، وتم تطوير سياساته في الفضاء الإلكتروني بالموازاة مع سياسة المفوضية الأوروبية لعام 1999 (eEurope) * والتي جعلت من البيئة الرقمية أولوية لحمايتها، ويمكن حصر إستراتيجية أمن الاتحاد الأوروبي في المجال السيبراني في ثلاث نقاط هي: مكافحة الجرائم الإلكترونية ومن ضمنها الإرهاب السيبراني، أمن الشبكات والمعلومات (NIS) وحماية البنى التحتية الحساسة (CIP)، إلى جانب الدفاع السيبراني[3].

ويعمل الاتحاد الأوروبي على تطوير سياسة دفاعية في إطار يتوافق مع سياسة الأمن والدفاع المشتركة، فالبعد الدفاعي أساسي في تصوّر الاتحاد الأوروبي، وهو قائم على الاستجابة الجيدة واحتواء التهديد الحاصل أو المحتمل بالتعاون مع الجهات المدنية والعسكرية وبين القطاعين العام والخاص، وبتأسيس سياسات دفاعية أوروبية تتماشى ومطلب المرونة السيبرانية Cyber Resilience (أي الاستجابة والتعافي من الهجمات الإلكترونية)[4]. وكانت المفوضية الأوروبية قد أعلنت عن إطلاق مشروع "الوحدة الإلكترونية

---

[1] Tin Hojsgaard Munk, ***Cyber Security in the European Region: Anticipatory Governance and Practices***, A thesis submitted for the degree of Doctor of Philosophy (University of Manchester : Faculty of Humanities School of Law, 2015), p.61.

[2] « Cybercriminalité : Un Défi à Relever aux niveaux National et International », www.senat.fr/rap/119-613/r19-6138.html (02.11.2021)

[3] Nurlan Karimov, « The European Union Cyber Security and Protection of Human Rights », 01/12/2019, https://www.academia.edu/41452957/The_European_Union_Cyber_Security_and_Protection_of_Human_Rights (11/08/2021), p-p : 55-56

* وضع الاتحاد الأوروبي الفضاء الإلكتروني ضمن أولوياته واهتماماته منذ التسعينات، على إثر هجمات القراصنة من صربيا على موقع القيادة العليا للقوات المسلحة في أوروبا (SHAPE) التابعة لحلف الناتو، ومع ذلك لم يرد ذكر التهديدات السيبرانية في إستراتيجية الاتحاد الأوروبي لعام 2003.

[4] Commission Européenne, La Haute Représentation de l'Union Européenne pour les Affaires Étrangères et la Politique de Sécurité, ***Stratégie de Cyber Sécurité de l'Union Européenne : un cyberspace ouvert, sur et sécurisé***, Communication conjointe au parlement Européen, au conseil, au comité économique et sociale Européen et au comité des régions, (Bruxelles, Juin 2013), p.12.

المشتركة" التي تتيح للدول الأعضاء طلب العون في حال التعرض لهجمات إلكترونية، بحيث أن هذه الوحدة تتضمن فرقا للتدخلات السريعة والطارئة[1].

ويمكن تقسيم الدول الأعضاء في الاتحاد الأوروبي من حيث قدرات الدفاع السيبراني كما يلي[2]:

أولا: دول لها أدوار بارزة وتاريخية في إطار التجربة الأوروبية التكاملية عموما، وهي الآن تمتلك قدرات سيبرانية رادعة ووقائية، ومؤسسات خاصة وإستراتيجية وطنية للأمن السيبراني. هذه الدول هي: فرنسا، بريطانيا (سابقا، قبل انفصالها عن الاتحاد الأوروبي)، وألمانيا. فرنسا مثلا لها قيادتان للدفاع السيبراني.

ثانيا: المجموعة الثانية تشمل دولة السويد، فنلندا ودول البلطيق الثلاث (إستونيا، ليتوانيا ولاتفيا).

ثالثا: تشمل هذه الفئة أغلبية الدول الأعضاء في الاتحاد الأوروبي، وتُوصف بأنها الأقل تطورا في مجال الدفاع السيبراني.

وتعد دول مثل مالطا، البرتغال وسلوفينيا، متأخرة نسبيا من حيث الأمن والدفاع السيبراني وذلك بمقارنة الموارد والثقافة السيبرانية لدول الاتحاد الأوروبي[3].

ج- نماذج من القدرات السيبرانية لبعض الدول الأوروبية:

أدى التركيز المتزايد للحكومات الأوروبية على تعزيز الأمن السيبراني لمكافحة الإرهاب السيبراني إلى نمو سوق الأمن السيبراني في هذا القطاع على مدى العقد الماضي، حيث أثار التهديد المحتمل للإرهاب السيبراني مخاوف واسعة النطاق. وفقًا للعديد من المتخصصين في مجال الأمن والمشرعين وغيرهم.

حيث يعتبر سوق مكافحة الإرهاب السيبراني مجزأ وتنافسي، حيث يضم العديد من اللاعبين العالميين والإقليميين، ففي ديسمبر 2021 أدى هجوم إلكتروني على وزارة الدفاع البلجيكية إلى إغلاق جزء من شبكة كمبيوتر الوزارة، بما في ذلك نظام البريد بالوزارة لعدة أيام. استخدم المتسللون ثغرة Log4j للوصول إلى الشبكة[4]، والخريطة أسفله تبين سوق الامن السيبراني.

---

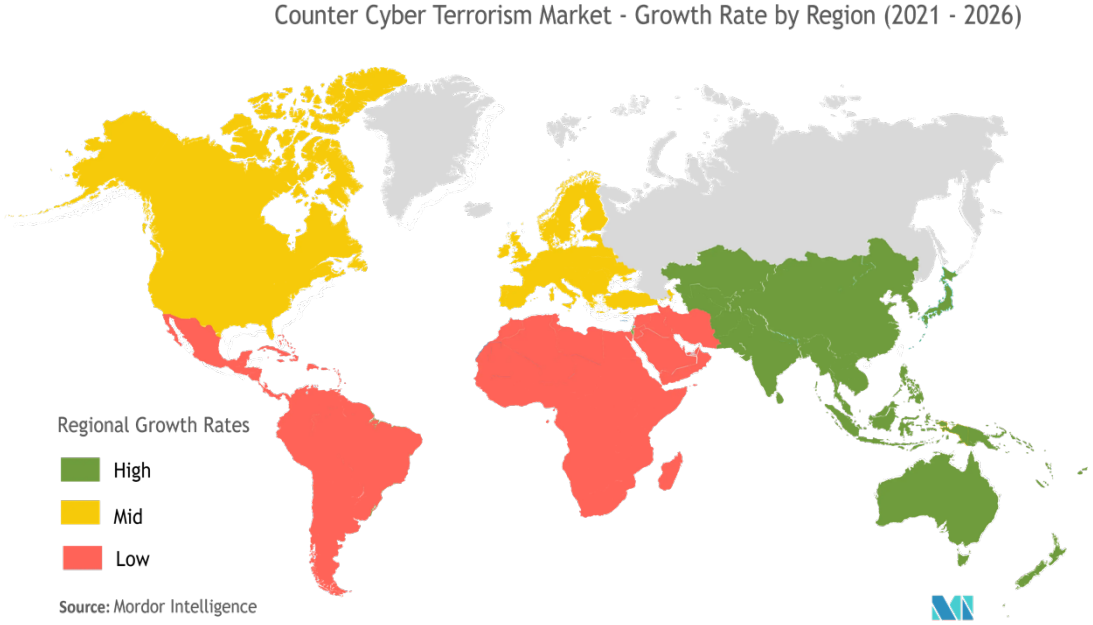
[1] محسن الرفاعي، "الاتحاد الأوروبي يطلق وحدة الأمن السيبراني للاستجابة السريعة"، موقع أورو-نيوز، في: 2021/06/21، https://arabic.euronews.com/2021/06/24/european-union-lanches-the-cybersecurity-rapid-response-unit (2021/09/12)

[2] Delphine Deschaux-Dutard, « L'Union Eueopéenne : une cyberpuissance en devenir ? Réflexion sur la cyberdéfence Européenne », ***Revue Internationale et Stratégique***, N°117 (1/2020),, p-p : 26-27.

[3] George Christou, ***Cybersecurity in the European Union : Resilience and Adaptability in Governance*** Policy, 1st edition (UK: Palgrave Macmillan, 2016), p.63.

[4] سوق مكافحة الإرهاب السيبراني – النمو والاتجاهات وتأثير COVID-19 والتنبؤات (2023 – 2028)، أنظر: https://cutt.us/tBDIX

الخريطة رقم (2): سوق مكافحة الإرهاب السيبراني: النمو والتنبؤات (2021–2026)



يلاحظ من هذه الخريطة نمو سوق محاربة الإرهاب السيبراني في المنطقة الأوروبية مقارنة ببقية دول العالم، وسيتم تسليط الضوء في هذا العنصر على بعض النماذج داخل الاتحاد الأوروبي وخارجه، وهي كالاتي: إستونيا، بريطانيا (قبل البريكسيت Brixit)، فرنسا، ألمانيا وأوكرانيا لكي نبرز أكثر وبالتحليل هذا النمو.

- إستونيا:

تعد إستونيا واحدة من أهم الدول في الاتحاد الأوروبي التي تمكنت من الاستثمار بشكل جيد في ثورة المعلومات والاتصالات، فأسست لحكومة واقتصاد وخدمات قائمة على استخدام التكنولوجيا[1]، وربطت بناها التحتية كالطاقة والبنوك والمياه بنظم المعلومات الرقمية، مع الإشارة أيضا إلى أن 97 بالمائة من تعاملاتها المصرفية تتم عبر الانترنت، لتوصف حكومة إستونيا انطلاقا من ذلك بالحكومة "اللاورقية"[2]. وحسب نتائج مؤشر الأمن السيبراني العالمي (GCI) لعام 2020، جاءت إستونيا في المرتبة الثالثة عالميا، وفرنسا في المرتبة التاسعة، في حين احتلت الولايات المتحدة الأمريكية المرتبة الأولى عالميا[3]. تتمتع إستونيا

[1] Stephen Herzog, « Country in Focus: Ten Yearsafter the Estonian Cyberattacks, Defense and Adaptation in the Age of Digital Insecurity », ***GEORGETOWN JOURNAL OF INTERNATIONAL AFFAIRS***, VOL. XVIII, N3, (FALL 2017), P-p: 68-69.

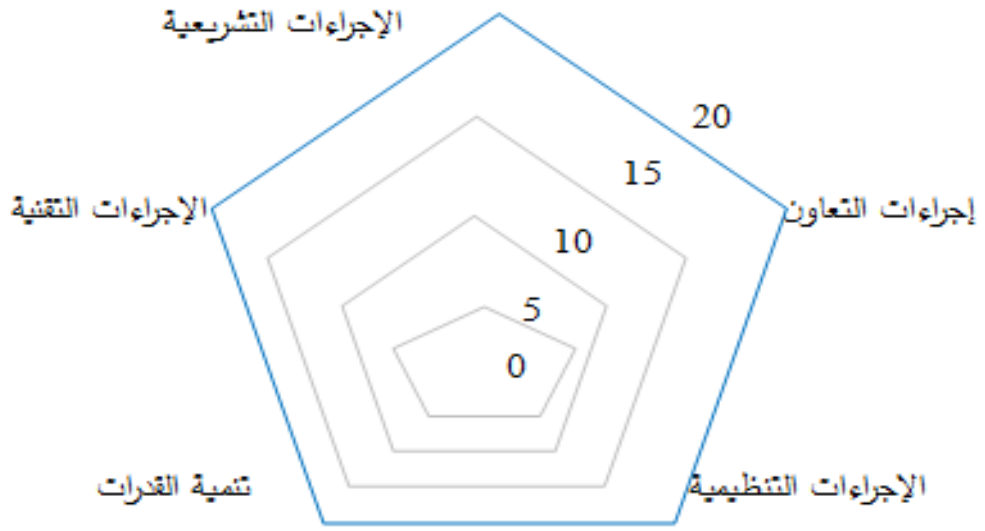
[2] Herzog, « Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses », ***Journal of Strategic Security***, vol.4, N.2 (Summer 2011), P.51.

[3] لمزيد من التفاصيل حول ترتيب دول العالم، راجع:

ITU, ***Global Cybersecurity Index, Measuring Commitment to Cyber Security (2020)***, 2021, p-p: 25-27.

بامتلاكها لسياسات وضوابط أكثر شمولا على مستوى دول البلطيق، فيما يخص الأمن والدفاع السيبراني[1]، وفي تقرير بعنوان "الحياة الرقمية في الخارج" جاءت في المرتبة الأولى من حيث الحرية على الانترنت وتقديم الخدمات الإلكترونية[2].

الشكل (13): نموذج إستونيا حسب مؤشر الأمن السيبراني العالمي لعام 2020.



النتيجة العامة	إجراءات تشريعية	إجراءات تقنية	إجراءات تنظيمية	تنمية القدرات	إجراءات التعاون
99,48	20.00	20.00	20.00	19.48	20

Source: ITU, Global Cybersecurity Index, Measuring Commitment to Cyber Security (2020), 2021, p.111.(بتصرّف)

لقد تمكنت إستونيا من تجاوز آثار الهجمات الإلكترونية التي تعرضت لها في 2007، والتي أدت إلى تعطيل عمل الحكومة الإلكترونية وخدمة المواطنين لمدة فاقت الأسبوعين، بالتالي يمكن اعتبارها نموذجا لدول الاتحاد الأوروبي في مجالي الأمن والدفاع السيبراني، والمؤشرات الظاهرة تؤكد ذلك، مع الإشارة إلى أن العناصر الخمسة المحددة في الجدول (الإجراءات التشريعية، التقنية، التنظيمية، تنمية القدرات وإجراءات التعاون) هي ركائز لتحديد مستوى الأمن السيبراني المحقق في كل دولة حسب الاتحاد الدولي للاتصالات التابع لمنظمة الأمم المتحدة.

[1] Dusco Tomic, and Others, *"Cyber Security Policies of East European Countries",in* **: *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*** (Springer International Publishing, 22 Mars 2018), p-p : 5-6.

[2] وحدة الدراسات والتقارير بالمركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات (ألمانيا–هولندا)، "الأمن السيبراني، الحكومة الإلكترونية، الخدمات الحكومية الرقمية"، https://www.europarabit.com/?p=72350 (2021/11/10)

أثرت الهجمات الإلكترونية التي عاشتها إستونيا في ابريل 2007 على البعد الدفاعي لهذه الدولة، فقد تمت مراجعة السياسة الدفاعية وأُدخل البعد الدفاعي السيبراني للتصدي لأيّ هجمات إلكترونية في المستقبل، كما أُنشئ مجلس الأمن السيبراني في 2009 وجرى استحداث قانون للطوارئ يركز على جاهزية المواجهة في حال حدوث هجمات سيبرانية، وتعد إستونيا من أوائل الدول التي امتلكت إستراتيجية وطنية للأمن السيبراني (تبنتها في 2008)، وتمكنت من تجاوز حالة الفراغ القانوني والمؤسسي بالنسبة لإدارة المجال السيبراني، وتدور أهداف سياسات الأمن والدفاع السيبراني لدولة إستونيا عموما حول خمسة أهداف مركزية هي[1]:

- حماية أنظمة المعلومات المتصلة بالخدمات الأساسية.
- تعزيز محاربة الجريمة السيبرانية.
- تطوير قدرات الدفاع السيبراني الوطنية.
- إدارة التهديدات السيبرانية.
- تطوير الأنشطة عبر القطاعات المختلفة (cross-sectoral).

وشكّل الاهتمام بالجانب الأكاديمي محطة ضرورية بالنسبة لإستونيا، فقد أنشأت جامعة تالين (تالين هي عاصمة إستونيا) للتكنولوجيا وجامعة تارتو برنامج ماستر في الأمن السيبراني، وتم قبول أول دفعة في 2009، كما أنشأت جامعة تالين للتكنولوجيا في 2014، بالتعاون مع مركز إستونيا للجريمة السيبرانية، برنامج الدراسات العليا في مجال الطب الشرعي الرقمي، إلى جانب ذلك فقد اشتمل تدريب الدروع المقفلة في 2017 على 800 خبير في الأمن السيبراني من مجموع 25 دولة مشاركة في التمرين المتعلق بمحاكاة الهجمات الإلكترونية[2].

ومن أجل إستراتيجية إستونيا للأمن السيبراني للفترة: 2019-2022 تم تخصيص 2,1 مليار يورو لكل عام، مع الارتكاز على أربعة محاور هي[3]:

- حماية حقوق الإنسان والحريات الأساسية في الفضاء السيبراني.
- الأمن السيبراني متصل بعملية التنمية على الصعيدين الاجتماعي والاقتصادي.
- حماية المعلومات وأهمية التشفير بوصف ذلك من صميم الأمن.
- تكريس الشفافية وثقة المواطن.

---

[1] Herzog, ***Op.Cit,*** P-p : 70-71.

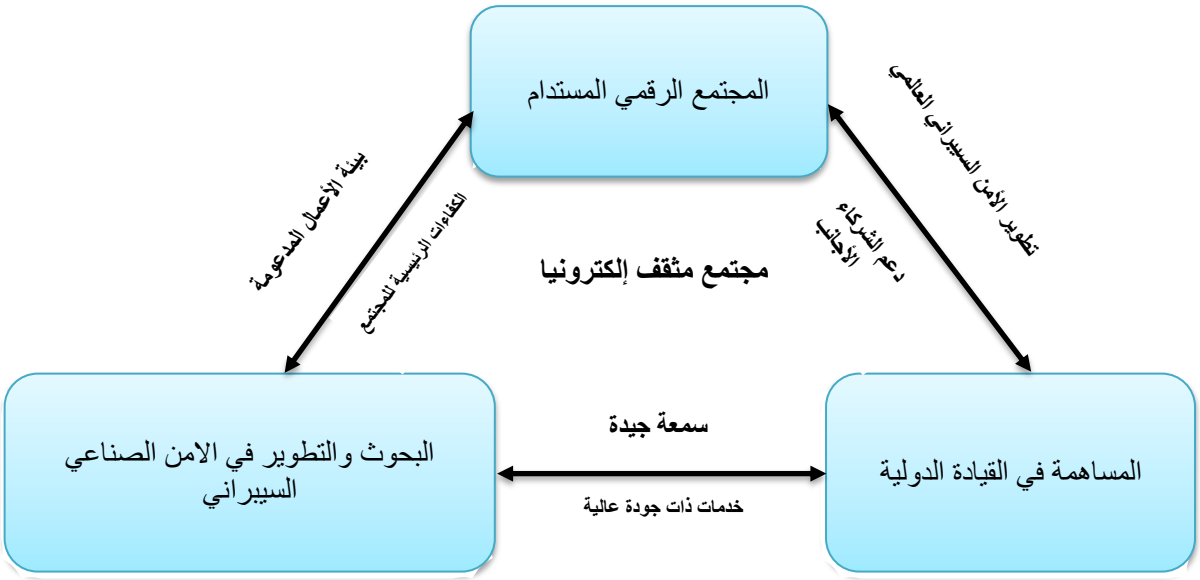
[2] ***Ibid***, P-p :72-73.

[3] Kevin Kohler, ***Estonia's National Cybersecurity and Cyberdefense Posture: Policy and Organizations*** (CYBERDEFENSE REPORT), Cyber Defense Project (CDP), Center for Security Studies (CSS), ETH Zürich (Zürich, September 2020), p.11.

انطلاقا من تلك المبادئ، تهدف إستراتيجية الأمن السيبراني الجديدة لدولة إستونيا إلى ما يلي[1]:

- بناء "مجتمع رقمي مستدام" يعتمد على المرونة التقنية في مواجهة الحوادث السيبرانية.
- دعم البحث العلمي من خلال تطوير القدرة السيبرانية، وهذا بغرض "تعزيز صناعة تنافسية عالميا".
- تعزيز مكانة إستونيا كدولة رائدة في المجال السيبراني.
- بناء مجتمع له وعي وثقافة سيبرانية كافية.

الشكل (14): مخطط توضيحي لأهم الأهداف المتوخاة من إستراتيجية الأمن السيبراني لإستونيا خلال الفترة 2019-2022.



Source: Kevin Kohler, Estonia's National Cybersecurity and Cyberdefense Posture: Policy and Organizations (CYBERDEFENSE REPORT), Cyber Defense Project (CDP), Center for Security Studies (CSS), ETH Zürich (Zürich, September 2020), p.12.

يتضح من خلال الشكل أن إستونيا تهتم ببناء مجتمع سيبراني مواكب لتطور تكنولوجيا المعلومات والاتصالات، وأكثر من ذلك فهي ترمي إلى صناعة الأمن السيبراني، خاصة مع المكانة المرموقة التي تحظى بها في الاتحاد الأوروبي كدولة تمكنت من بناء قدرات دفاعية في المجال الرقمي بعد تعرضها لحوادث وهجمات خطيرة، وهذا كله لا يمكن عزله عن اهتمامها بموقعها كشريك دولي يتمتع بدرجة عالية

[1] Shashi Jayakumar, « Cyber Attacks by Terrorists and other Malevolent Actors: Prevention and Preparedness: With Three Case Studies on Estonia, Singapore, and the United States », *in: Alex P.Shmid, **HANDBOOK OF TERRORISM PREVENTION AND PREPAREDNESS*** (The Hague : ICCT Press, 2021), p.923.

من الكفاءة والمصداقية والنضج السيبراني، إلى جانب كونها دولة رائدة في المجال ذاته على الصعيد الأوروبي وفي نطاق حلف الناتو.

أنشأت إستونيا قيادة إلكترونية مكلفة بالدفاع السيبراني والتعاون مع الناتو، مع العلم أن أهم التدريبات في المجال السيبراني تُجرى فيها، مثل تمارين "الدروع المقفلة" (Locked Shields)، كما تشجع إستونيا الشراكة بين القطاعين العام والخاص، وتدعم كذلك المؤسسات الناشئة من خلال دعوتها إلى "الانضمام إلى مسرّع الذكاء الاصطناعي الدفاعي والأمن السيبراني، وهو الأول من نوعه في أوروبا"[1].

- بريطانيا:

يرجع تاريخ اهتمام المملكة المتحدة بقوانين تأمين الفضاء السيبراني إلى سنوات سابقة، ففي 1990 مثلا سنّت قانون إساءة استخدام الحاسوب وهو يتضمن مكافحة الدخول غير المشروع للنظام، التطفل والعبث والمساس (أو التعديل) غير المشروع للنظام بهدف تعطيله[2].

تعتبر الحكومة البريطانية المساسَ بالبنية التحتية الحرجة (CNI) مساسا خطيرا بالاقتصاد الوطني وبأمن وسلامة الحكومة والمجتمع[3]. وعلى صعيد مكافحة الإرهاب السيبراني، كانت بريطانيا في مقدمة الدول التي تتصدى لاستخدام الجماعات الإرهابية للإنترنت، وذلك منذ جويلية 2006 عندما ظهرت استراتيجيتها لمكافحة الإرهاب الدولي (CONTEST)، فتصورها انطلق من أن شبكة الانترنت تحمل توجهات عديدة متطرفة وبالتالي فهي تحمل بذور الإرهاب في أية لحظة، وبالفعل تطور اعتماد الإرهابيين على هذه الشبكة مما سمح بانتشار واسع للفكر المتطرف، وفي مارس 2009 نشرت الحكومة نسخة منقّحة لاستراتيجيتها بما يتضمن تطويرا لسياسات مكافحة الإرهاب عبر الانترنت، ويجري العمل على إزالة المضمون الإرهابي وتشجيع نشر أفكار مضادة أي رافضة للتطرف في المجتمع، فقد تم إطلاق وحدة الإحالة عبر الانترنت (CTIRU) في 2010 لتكون مسؤولة عن تحديد المحتوى المتطرف والممجّد للإرهاب وبالتالي حذفه أو إزالة الموقع بالتعاون مع مزودي خدمة الإنترنت (ISPs)، وقد سُجّلت على سبيل المثال 3100 إحالة على هذه الوحدة (أي وحدة الإحالة عبر الانترنت) خلال الفترة: فبراير 2010- سبتمبر 2012، وتم حذف 410 محتوى من منصات فيسبوك وتويتر وغيرها[4].وتمتلك بريطانيا قاعدة بيانات تخص

---

[1] ***Ibid***, p.926.

[2] عبد الجليل إسماعيل حسن الشيخ زيني، ***الإرهاب الإلكتروني في القانون الدولي: الماهية والجزاء*** (بيروت: منشورات الحلبي الحقوقية، ط1، 2020)، ، ص 244

[3] Paul Cornish, and Others, ***Cyberspace and the National Security of the United Kingdom: Threats and Responses***, A Chatham House Report (Mars 2009), p.16.

[4] Ines von Behr, and Others, ***Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism*** (Brussels : Rand Europe, 2013), p.4.

عددا كبيرا من الأفراد في إطار الوقاية من التطرف، ويهدف هذا الإجراء إلى السيطرة على الفكر المتطرف بمراقبته وقمعه قبل أن يتحول إلى نشاط إرهابي فعلي[1].

أنشأت بريطانيا هيئة مستقلة "تتمتع بسلطة فرض الغرامات على شركات الانترنت، وإصدار تشريعات تجعل من حيازة المواد المتطرفة الرقمية والترويج لها جريمة، فضلا عن مطالبة شركات التواصل الاجتماعي بحذف ومنع انتشار المحتوى الارهابي في وسائل التواصل الاجتماعي"، بالإضافة إلى تطوير برامج رقمية تحظُر زيارة المحتوى الإرهابي، وتطوير وحدة خاصة بمكافحة الإرهاب عبر الانترنت حيث يتم العمل على حذف محتويات تتضمنه أو تمجّده[2].

لقد عملت بريطانيا خلال السنوات الماضية على سد العجز الموجود في جاهزيتها الدفاعية في الفضاء السيبراني وتعزيز أمنها السيبراني، وكانت إستراتيجية الأمن القومي للمملكة المتحدة في 2008 تحت عنوان: "الأمن في عالم مترابط" إستراتيجية شاملة من حيث الخطط والأهداف والقدرات، معبّرةً عن التحولات التي يشهدها العالم، ثم جرى تحديثها في 2009 تحت عنوان: "الأمن للجيل القادم" ليتم تناول الأمن السيبراني كبعد مهم للأمن، بالتالي ستبرز إستراتيجية خاصة بالأمن السيبراني (CSS)، وهو ما فرضه الواقع حيث أصبحت كل الخدمات في المملكة المتحدة وفي العالم بأسره تعتمد على الفضاء السيبراني، مما يجعل هذا الفضاء ذا أهمية "حيوية" تتطلب تأمينَه من كل أشكال التهديدات، ويتم تعريف بعض القطاعات الوطنية في المملكة المتحدة بوصفها "خدمات أساسية" تتصل بالفضاء الرقمي وهي: الحكومة، الاتصالات، خدمات الطوارئ، الطاقة، المالية، الغذاء، المياه، الصحة والنقل[3].

وتم إنشاء المركز الوطني للأمن السيبراني بتاريخ: 01 أكتوبر 2016، ويهدف إلى تعزيز الشراكة بين الحكومة والشعب ومختلف القطاعات في الدولة، وتقديم المشورة للقطاعات الهامة حول كيفية حماية الشبكات ونظم المعلومات من التهديدات السيبرانية، بالتالي عُدّ مرجعا هاما ومصدرا للمعلومة بخصوص التهديدات الجديدة التي يكون الفضاء الرقمي وسيطا لها[4].

وتعد منصة "عملية لندن" منصة لمناقشة القضايا السيبرانية، جاءت بمبادرة من وزير خارجية بريطانيا السابق "ويليام هيغ" William Hague الذي دعا القادة عبر العالم للنقاش سنويا بخصوص "إيجاد توافق في الآراء بشأن السلوك المسؤول في الفضاء الإلكتروني"[5].وتم استحداث برنامج "بلدية لندن"

---

[1] جاسم محمد واخرون، ***الإرهاب والتطرف في أوروبا من الداخل: الجماعات الجهادية، الإسلام السياسي واليمين المتطرف*** (مصر: المكتب العربي للمعارف، ط1، 2021)، ص 84-85.

[2] حسن سعد عبد الحميد، "سياسة أوروبا الإلكترونية ضد الإرهاب والتطرف"، مركز النهرين للدراسات الإستراتيجية (العراق، 10 فبراير 2019)، https://www.alnahrain.iq/post/370# (2021/11/11)

[3] Tim Stevens, « Reading Power in UK Cybersecurity », in: https://www.academia.edu/1157394/Reading_Power_in_UK_Cybersecurity (30/12/2021), p-p: 5-8.

[4] United Kingdom, ***Stratégie Nationale de Cyber Sécurité (2016-2021),***2016, p.24.

[5] Thomas Renard, EU Cyber Partnership: Assessing the EU Cyber Strategic Partnerships with Third Countries in the Cyber Domain, ***European Politics and Society***, 19(3), (January, 2018), p.13.

تحت مسمى "مكافحة التطرف العنيف" (Countering Violent Extremism) بتكلفة مليون جنيه إسترليني، ومع زيادة الهجمات الإرهابية في بريطانيا خلال الأعوام الأخيرة، باتت السلطات مخولة بتوقيف وتفتيش أي شخص وبدون شبهة معينة في إطار برامج الوقاية من التطرف والعمل الإرهابي، ولكن هذا الإجراء هو من جهة غير عادل ومثير للقلق لأنه يمس حقوق الإنسان وكرامته[1].

ويُعرف مسجد "فينسري بارك" في بريطانيا بأنه "مسجد المتطرفين"، فقد كان معقلا لأبي حمزة المصري[2] أحد قياديي تنظيم القاعدة في السابق، إضافة إلى زكريا الموسوي المتهم الأول في هجمات 11 سبتمبر 2001 بالولايات المتحدة، "وتشير التقديرات إلى أن 35 شخصا على الأقل من المحتجزين بمعتقل "غوانتانامو" مرّوا بالمسجد، وفقا ل "سكاي نيوز عربية" في 19 يونيو 2017"، وانطلاقا من ذلك طرحت بريطانيا برنامج "الأمن الوقائي لأماكن العبادة"[3].

- فرنسا:

تتبنى فرنسا عددا من السياسات والتدابير لمكافحة الإرهاب الإلكتروني، ومن ضمنها تزويد مشغّلي الانترنت ومنصات التواصل الاجتماعي بأدوات محاربة التطرف، والاتفاق مع شركات التواصل الاجتماعي على حذف المحتوى الإرهابي[4].

وأدى خطر الهجمات الإرهابية في فرنسا وانتشار خطاب العنف والتطرف عبر الانترنت إلى وضع النواب الفرنسيين (في 14 ماي 2020) قانون محاربة خطاب الكراهية عبر الانترنت، وبالتالي إلزام منصات التواصل الاجتماعي بحذف المحتوى الذي يحضّ على العنف والكراهية والعنصرية والتطرف عموما في ظرف 24 ساعة، مع فرض غرامة تقدر ب 1,25 مليون يورو، وتتم مراقبة الأفراد المتطرفين والخطرين من قبَل أجهزة المخابرات والأمن الفرنسية، كما تمتلك أجهزة الأمن الفرنسية ملفات تعريفية تحت مسمى "S" تشمل الأشخاص الخطرين والمسجلين ضمن "بلاغات الوقاية من التطرف" (FSPRT)، يضاف إلى ذلك أن الرئيس الفرنسي "ماكرون" قد أعلن بتاريخ: 02 أكتوبر 2020 عن تخصيص 10 مليون يورو لمؤسسة "إسلام فرنسا" وإنشاء "معهد علمي للدراسات الإسلامية"[5].

وأوصى "نداء كرايستشيرش"، وهو عبارة عن مؤتمر احتضنته باريس في 15 ماي 2019، بوضع خطة لقمع والوقاية من الإرهاب، ومن ذلك العمل على منع تحميل المحتوى المتطرف على الانترنت،

---

[1] جاسم محمد، واخرون، ***مرجع سابق***، ص 217-219.

[2] أبو حمزة المصري (1958-)، كنية لأحد المنتمين إلى تنظيم القاعدة، عُرف بنشر خطاب الكراهية في بريطانيا -حيث يقيم- تجاه الأجانب، وهو متهم بالإرهاب ومحكوم بالسجن مدى الحياة.

[3] ***المرجع نفسه***، ص: 34، 39.

[4] حسن سعد عبد الحميد، مرجع سابق.

[5] جاسم محمد واخرون، ***مرجع سابق***، ص: 34، 213-214.

ومحاربة أسباب التطرف، وحذف المحتوى الذي يحث على الإرهاب، وعمل اليوروبول في 2018 على تعطيل المواقع الإلكترونية التابعة لتنظيم "داعش" الإرهابي[1].

وكشفت الحكومة الفرنسية في 5 أبريل 2021، عن مشروع قانون جديد لمكافحة الإرهاب من خلال مراقبة الإنترنت عبر تطبيقات "واتساب" و "سيغنال" و "تيليغرام" باستخدام الخوارزميات، وتوسيع استخدام أجهزة الاستخبارات الفرنسية للخوارزميات لتعقب الإرهابيين المحتملين، وأثار القانون الجديد جدلا كبيرا في أوساط المدافعين عن الحريات وعن استخدامات شبكة الإنترنت[2].

ومع احتمال عودة المقاتلين الإرهابيين الأجانب، تبقى برامج الوقاية من التطرف والإرهاب في المستقبل بحاجة إلى تعزيز أكبر، فهؤلاء قد تشبعوا لسنوات بالفكر المتطرف خاصة وأنهم كانوا متواجدين في معاقل الصراع بالشرق الأوسط، وتهتم فرنسا بتدابير الوقاية من أجل احتواء التهديد الإرهابي، فهي تشمل "تأهيل الأئمة والموظفين المحليين وإشراك المراكز الإسلامية في تأهيل المتطرفين، ومواجهة الاستقطاب الذي يمارَس داخل السجون الفرنسية، وكذلك إعادة تأهيل واندماج لمن اعتنقوا الفكر المتطرف في الضواحي الفرنسية". ومع ذلك لا يمكن الجزم بالفعالية المثلى لمثل هذه التدابير، فالإرهاب يعاد تأطيره من خلال تغيير الأساليب باستمرار[3].

- ألمانيا:

وضعت ألمانيا قانون NetzDG لمحاربة المحتوى الإرهابي وغير القانوني، وقد دخل حيز التنفيذ في 01 أكتوبر 2017، وهو يتضمن إزالة المحتوى في ظرف 24 ساعة من تقديم المستخدم لشكوى ضده، كما وضعت فرنسا قانون "مكافحة المحتوى الذي يحض على الكراهية عبر الانترنت" (Loi Avia) الذي اعتُمد في جويلية 2019، ولكنه تعرض للنقد الشديد باعتباره مناقضا لحرية التعبير، فألغاه المجلس الدستوري الفرنسي، ثم أُنشئ "مرصد الكراهية على الإنترنت" الذي بدأ العمل في جويلية 2020[4].

وعبّرت ألمانيا عن كونها تتمتع بحصانة من تهديدات الإرهاب السيبراني، ولها في هذا الشأن سياسة وقائية من خلال استحداث جهاز أمني يتولى "جمع المعلومات الاتية من الخلايا الإرهابية القائمة عبر

---

[1] ***المرجع نفسه***، ص 269-270.

[2] المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات، "مكافحة الإرهاب في أوروبا . تدابير وقائية واستباقية جديدة"، 2021/10/11، https://bit.ly/3spNy1q (2021/11/22)

[3] جاسم محمد واخرون، ***مرجع سابق***، ص 215-216.

[4] جاسم محمد، "صناعة الكراهية داخل أوروبا... منصات التواصل الاجتماعي تؤجج العنف، دور الاتحاد الأوروبي محدود في إعادة تأهيل الإرهابيين"، 2021/06/17، https://bit.ly/3pjEQ2h (2021/12/15)

الحدود ووضعها تحت المراقبة المستمرة وإفشال أية عمليات إرهابية والحد من نموها وكشف مصادر تمويلها"[1].

كما طورت ألمانيا إجراءات وقائية تخص الإرهاب السيبراني، أهمها ما يلي:

- تطوير ما سمي بنظام "رادار داعش" (RADAR – ITE): صنفت الحكومة الألمانية جماعات الإرهاب الجهادي على إثر حادثة الدهس الشهيرة (19 ديسمبر 2016) بالتزامن مع الاحتفال بأعياد الميلاد في أوروبا، والتي أدت إلى مصرع 12 شخصا وأكثر من 50 جريحا، هذا التقسيم يندرج في إطار "رادار داعش" (iTE)[2]الذي طوره جهاز الأمن الألماني بالتعاون مع جامعة كونستانس بألمانيا، يستهدف الكشف المبكر عن النشاط الإرهابي معتمدًا على تحليل سلوك الفرد وأسلوب حياته، ويخضع هذا النظام للتحديث المستمر لتتبع نشاط الجماعات المتطرفة والإرهابية مثلا من خلال المراقبة الإلكترونية وتجميع البيانات، و"يعمل هذا النظام الرقمي عبر وضع مجموعة من الاجابات لـ (73) سؤالاً لتقييم المخاطر، ووفق مقاييس ثلاثة (خطر عال، خطر ملحوظ، خطر معتدل) لقياس احتمالية عنف الشخص المشتبه به"[3].

- فرض غرامات على شركات التواصل الاجتماعي إذا تأخرت في معالجة وحذف المحتوى الإرهابي عبر منصاتها، وإنشاء جيش ألماني مسؤول عن أمن فضاء الانترنت[4]. كما لجأت ألمانيا إلى إلزام تطبيقات مثل فيسبوك وتويتر وانستغرام "بإبلاغ المكتب الاتحادي للتحقيقات الجنائية عن منشورات بعينها فور نشرها، وهو ما ينطبق، على سبيل المثال، على الدعاية النازية والتحضير لجريمة إرهابية وفقا ل "DW" في 19 فبراير 2020"[5].

- برنامج مطابقة الفحوصات الجينية: يدعمه الاتحاد الأوروبي بقيمة مليون يورو، "ويقضي البرنامج بمطابقة إجراءات الفحوص الجينية اللازمة للتعرف على هوية الشخص ومطابقة النظم الإلكترونية والبنية التحتية الضرورية للتعرف على الإرهابيين"، إلى جانب برنامج موسع لمكافحة الإرهاب من خلال التشديد في مسألة الرقابة على من يُعتبرون خطرا على الأمن الألماني، برنامج مكافحة تسلل الإرهابيين، برامج إلكترونية عديدة مثل قناة فكاهية على اليوتيوب هدفها التحذير من التطرف، برنامج "فينيكس" الذي يُنتظر اكتماله في 2026 والهدف منه مراقبة الاتصالات الإلكترونية بين الأفراد المتطرفين[6].

---

[1] عبد الجليل إسماعيل حسن الشيخ زيني، ***مرجع سابق***، ص 243-244.

[2] جاسم محمد واخرون، الإرهاب والتطرف في أوروبا من الداخل، ***مرجع سابق***، ص 73-75.

[3] حسن سعد عبد الحميد، مرجع سابق.

[4] المرجع نفسه.

[5] جاسم محمد واخرون، الإرهاب والتطرف في أوروبا من الداخل، ***مرجع سابق***، ص.34.

[6] ***المرجع نفسه***، ص: 220، 222.

- أوكرانيا:

كان الهجوم الإلكتروني الذي تعرضت له أوكرانيا في 23 ديسمبر 2015، والذي مسّ محطات توزيع الكهرباء وشبكة الانترنت ونتج عنه تأثُّر الخدمة لدى أكثر من 200 ألف مستهلك[1]، ذا تأثير بالغ في سياسات الدول الأوروبية مما طرح ضرورة تفعيل الوقاية والتدخل المستعجل عند وقوع هجمات من هذا النوع. ومن الأمثلة البارزة أن أوكرانيا نفسَها خصصت نقطة اتصال تخص تبليغ الأفراد عن المضايقات وخطابات الكراهية التي يكون المجال السيبراني ميدانا لها[2]. لقد خطَت أوكرانيا خطوات قوية وفعالة في مجال الأمن والدفاع السيبراني، بعد أن تعرضت لهجمات قوية مسّت حتى بنيتها التحتية، مما جعلها تمضي قُدما نحو تنظيم وتحديث قوانينها في هذا الصدد واستحداث وتعزيز ترسانتها السياسية والتقنية والمؤسساتية، كل ذلك بما يضمن المرونة السيبرانية والوقاية والتصدي الجيدين لتهديدات الفضاء الإلكتروني[3].

ويعمل الاتحاد الأوروبي على مكافحة الإرهاب السيبراني بالاعتماد على مجموعة من التدابير المتنوعة مثل[4]:

- تطوير سياسات إلكترونية تثبّط التجنيد والانخراط في صفوف الإرهاب.
- تطوير سياسات معالجة وإزالة المحتوى الذي يحض على الكراهية والإرهاب من خلال الانترنت.
- الاستعانة بعمل الخبراء في قضايا التطرف والإرهاب في وضع خطط وسياسات لمواجهة الإرهاب السيبراني، ودراسة أسباب وظروف تحوّل الفرد العادي إلى شخص يدعم أو يمارس الإرهاب من خلال شبكة الانترنت.

بالتالي فإن الاتحاد الأوروبي يعمل على تطوير سياسة دفاع سيبراني متكاملة، تتصدى من جهة للهجمات الإلكترونية وتحارب من جهة أخرى الإرهاب السيبراني، وهو ما سيتم التطرق إليه بالتفصيل في المطلب الثالث.

[1] United Kingdom, ***Op.Cit***, p.16.

[2] Le Centre pour la Gouvernance du Secteur de Sécurité, ***Guide pour la Bonne Gouvernance de la Cyber Sécurité*** (Genève, 2019), p.14.

[3] Dusco Tomic, and Others, ***Op.Cit***, p-p : 8-9.

[4] حسن سعد عبد الحميد، مرجع سابق.

المطلب الثالث: استراتيجيات الأمن والحوكمة السيبرانية.

أصبحت الحوكمة من المواضيع التي تطرح نفسها بشدة منذ تسعينيات القرن الماضي تقريبا، وهذا بالنظر إلى ما بات يشكله هذا النمط من ضرورة للدول حتى ترقى إلى مستوى تطلعات مواطنيها، ولأنه يهدف بالأساس إلى خدمة المصلحة العامة على جميع الأصعدة (سياسيا، إداريا، اجتماعيا، اقتصاديا وأمنيا). ومفهوم الحوكمة la gouvernance أو الحكم الراشد/الجيد la bonne gouvernance من المفاهيم التي لا تحظى بإجماع، فقد قُدّم في شأنه العديد من التعريفات.

أ- مفهوم الحوكمة:

بدأ انتشار استخدام المفهوم في تسعينات القرن المنصرم من خلال المنظمات الدولية وبرنامج الأمم المتحدة الإنمائي (PNUD)، بالتزامن مع أزمات اقتصادية ومالية عرفتها دول عديدة عبر العالم كروسيا واليابان وشرق آسيا، فارتبطت نشأة الحوكمة بالبعد الاقتصادي[1]. في 1989 صدر تقرير للبنك الدولي عرّف الحكامة بأنها "أسلوب ممارسة السلطة في تدبير الموارد الاقتصادية والاجتماعية للبلاد من أجل التنمية"[2]. ثم عرّف الحكم الراشد سنة 1997 بأنه "الطريقة الخاصة بممارسة السلطة السياسية والاقتصادية والإدارية قصد تسيير أحسن للشؤون العمومية"[3]. كما عرّفته منظمة الشفافية الدولية بأنه "الغاية الحاصلة من تكاثف جهود كل من الدولة والقطاع الخاص والمجتمع المدني ومختلف المواطنين في مكافحة ظاهرة الفساد"[4]. كما تعني الحوكمة "مجموعة القوانين والنظم والقرارات التي تهدف إلى تحقيق الجودة والتميز في الأداء" انطلاقا من شروط أساسية كالضبط والرقابة والمساءلة[5].

ب- حوكمة الأمن السيبراني في السياق الأوروبي:

يمكن تعريف الحوكمة في السياق الأوروبي بأنها "حصيلة العديد من الطرق التي يدير بها الأفراد والمؤسسات، العامة والخاصة، شؤونَهم المشتركة. إنها عملية مستمرة يمكن من خلالها استيعاب المصالح

---

[1] مركز أبو ظبي للحوكمة، "أساسيات الحوكمة: مصطلحات ومفاهيم"، سلسلة التراث التثقيفية للمركز، https://loiarabe.blogspot.com/2019/07/pdf_28.html، ص05.

[2] محمد أوجار، "ملاحظات أولية في موضوع الحكم الرشيد أو الحكامة الجيدة"، في: محسن عوض وكرم خميس، ***الندوة الدولية حول التنمية والديمقراطية وتطوير النظام الإقليمي العربي***، (القاهرة: المنظمة العربية لحقوق الإنسان، ط1، 2013)، ص57

[3] محمد غربي، "الديمقراطية والحكم الراشد: رهانات المشاركة السياسية وتحقيق التنمية"، ***دفاتر السياسة والقانون***، عدد خاص (أبريل 2011)، ص371.

[4] نبيل البابلي، ***تقرير بعنوان: الحكم الرشيد، الأبعاد والمعايير والمتطلبات***، المعهد المصري للدراسات، القاهرة (18 جانفي 2018)، ص02.

[5] محمد ياسين غادر، "محددات الحوكمة ومعاييرها" (ورقة بحث قدمت في المؤتمر العلمي الدولي: عولمة الإدارة في عصر المعرفة، جامعة الجنان، طرابلس/لبنان، 15-17 ديسمبر 2012)، ص: 2، 13.

المتضاربة أو المتنوعة، ويمكن اتخاذ إجراءات تعاونية. وهي تشمل المؤسسات والأنظمة الرسمية المخوَّلة لفرض الامتثال، فضلاً عن الترتيبات غير الرسمية التي وافق عليها الأشخاص والمؤسسات أو يرون أنها في مصلحتهم"[1].

على إثر هجمات مدريد ولندن في 2004 و2005 على التوالي، وضع الاتحاد الأوروبي أول إستراتيجية شاملة لمكافحة الإرهاب، تقوم على أربع ركائز هي: المنع والحماية والمتابعة والاستجابة، وجرى التأكيد من خلالها على التعاون مع الدول غير الأعضاء في الاتحاد الأوروبي والمؤسسات الدولية[2]. وأدت الرقمنة المتواصلة في الدول الأوروبية إلى "تغذية" التهديدات السيبرانية والإرهاب الإلكتروني، وجدير بأن يُذكر في هذا الصدد نمطُ الحكومة الإلكترونية الذي أصبح شكلا متطورا للإدارة والحكم وتجسيد العلاقة الجيدة بين الإدارة والمواطن، ولكنّ ذلك يطرح في المقابل تحديات كثيرة بالنسبة لقواعد البيانات والتعاملات المالية في حال وقوع هجوم سيبراني أو عمل إرهابي إلكتروني، وهو ما جرى بالفعل مع إستونيا في 2007 عندما تم تعطيل الشبكات وتوقفت الخدمات الحكومية.

يأتي اهتمام الاتحاد الأوروبي بحوكمة قطاع الأمن والدفاع انطلاقا من رؤية مفادها أن "قصور الحوكمة الرشيدة في قطاع الدفاع سوف يفرز تحديات أمنية خطيرة"، وبالفعل جرى التأكيد على أن النزاهة والمساءلة في قطاع الدفاع أمر ضروري لاستقرار المنطقة الأورو- أطلسية، وفي المقابل يعد ضعف الحوكمة أو انتشار الفساد تهديدا لهذا الاستقرار[3]. وقد حظي عنصر الشفافية في قطاع الأمن والدفاع باهتمام واسع لدى منظمة حلف الناتو، انطلاقا من المبادئ التي يدعو إليها وترتبط بها سياساته الدفاعية، مثل قيم الحكم الديمقراطي وحقوق الإنسان وحوكمة المؤسسات[4].

تسمح الشفافية بوصفها واحدة من ركائز الحكم الجيد بتطوير فهم المجتمع للتهديدات الأمنية وأيضا تعزيز ثقافة الثقة بين الشركاء أو الفاعلين في الفضاء الإلكتروني، وكانت منظمة الأمن والتعاون في أوروبا (OSCE) قد تبنت في 2014 اتفاقية تخصّ إجراءات الثقة، حيث تتضمن مشاركةَ أعضائها معلومات حول المشاريع والبرامج والمؤسسات المخولة بالأمن السيبراني لكل دولة، وهو ما يتيح تبادل الأفكار وتثمين الحوار بخصوص المسائل الهامة التي يعنى بها قطاع الأمن السيبراني[5].

---

[1] Mario Nicolas Castellon Machado, ***Cyber Security Governance: Securing the European Union's Cyber Domain,*** Master's Dissertation in Crisis and Security Management Programme (Leiden University: Faculty of Governance and Glabal Affairs, August 2015), p.17.

[2] Sofija Voronova, ***Understanding EU Counter-Terrorism Policy***, European Parliament Research Service (EPRS), (January 2021), P.4.

[3] منظمة حلف شمال الأطلسي، ***المنهج التعليمي المرجعي: الحوكمة الرشيدة وبناء النزاهة في قطاع الدفاع والقطاعات الأمنية ذات الصلة*** (2012)، ص: 1، 3.

[4] مركز جنيف للرقابة الديمقراطية على القوات المسلحة (DCAF)، ***بناء النزاهة والحد من الفساد في قطاع الدفاع.. خلاصة وافية لأفضل الممارسات*** (جنيف، 2010)، ص-ص 26-27.

[5] Le Centre pour la Gouvernance du Secteur de Sécurité, ***Op.cit.***, p-p : 21-22.

وفي 2018، قام مركز حوكمة قطاع الأمن بجنيف ومديرية التعاون للأمن والدفاع بفرنسا بوضع دليل "الحوكمة الجيدة للأمن السيبراني"، لغرض تعزيز حوكمة الأمن في الفضاء الإلكتروني مما يعني تطبيق مبادئ الحوكمة في مجال تسيير وضبط هذا الفضاء بما يجعله آمنا من التهديدات والمخاطر، وانطلاقا من كون قطاع الأمن مُركَّبا وغيرَ محدود كما أن إصلاحه يعد عملية سياسية وتقنية بما يضمن حقوق الإنسان والأمن الإنساني عموما[1].

وبالعودة إلى الحديث عن الأمن والحوكمة في إستراتيجيات الأمن السيبراني الأوروبي، حددت استراتيجية الاتحاد الأوروبي في مجال مكافحة الإرهاب، حسب الأجندة الخاصة الصادرة في ديسمبر 2020، أربعة عناصر هي[2]:

أولا: توقُّع التهديدات الراهنة والمحتمَلة في السياق الأوروبي.

ثانيا: منع حدوث الهجمات الإرهابية، ويتضمن ذلك سياسة المنع ومحاربة إيديولوجيا التطرف ونشر ثقافة الديمقراطية.

ثالثا: حماية المواطن الأوروبي من التهديد الإرهابي وتداعياته، من خلال حماية البنى التحتية الحرجة وتقليص ثغرات الأمن داخل الاتحاد الأوروبي.

رابعا: الاستجابة، وتكون بالعمل مع وكالات الاتحاد الأوروبي المخولة بمكافحة الجرائم المستحدَثة مثل اليوروبول والمحكمة الأوروبية، وإيجاد الإطار القانوني الأنسب للتعاطي مع الجرائم وإنفاذ القانون.

انطلاقا من ذلك يتضح كيف أن مكافحة الإرهاب تحتل الصدارة في أولويات الاتحاد الأوروبي وكيف أن تحيين الاستراتيجيات أمرٌ ضروري، وينطبق هذا على مكافحة الإرهاب السيبراني حيث تولي الأجندة الخاصة اهتماما واسعا بالمنع والاستجابة للجرائم المستحدَثة عبر الفضاء السيبراني، وهذا لا ينفصل عن حوكمة الأمن السيبراني.

ج- إستراتيجيات الأمن السيبراني للاتحاد الأوروبي:

يتم التركيز في هذه النقطة على ثلاث استراتيجيات للأمن السيبراني بالنسبة للاتحاد الأوروبي، وهي التي ظهرت في الفترات الاتية: 2013، 2017 ثم نهاية 2020.

جاءت إستراتيجية الاتحاد الأوروبي الأولى حول الأمن السيبراني في عام 2013 تحت شعار: "من أجل فضاء سيبراني مفتوح، امن ومؤمَّن" Pour un Cyberspace Ouvert, Sur et Sécurisé، وهي تستهدف تكريس المرونة السيبرانية والدفاع السيبراني انطلاقا من نظرة الاتحاد الأوروبي لنفسه كفاعل في هذا الفضاء (أو كما يجب أن يكون)، فامتلاك القوة السيبرانية يعني الفعل والتأثير على السلوكيات في الفضاء السيبراني، مع أخذ بعين الاعتبار حشد مختلف الوسائل لذلك بما فيها العسكرية والدبلوماسية،

[1] ***Ibid***, pages : 6, 11-13.

[2] European Commission, ***A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond***, COMMUNICATION FROM THE COMMISSION (Brussels, 09/12/2020), p.2.

وتطوير إمكانيات الدول الأعضاء وسياساتها في مجال الأمن السيبراني، والدفع قُدُمًا بالحوار العسكري-المدني حول القضايا ذات الصلة، فضلا عن الحوار مع الشركاء الدوليين والأساسيين مثل الناتو، وقد حدد المجلس الأوروبي في 2014 الإطار الإستراتيجي للدفاع السيبراني الأوروبي بالتركيز على "رفع المرونة وتقوية الإمكانيات لمواجهة التهديدات الهجينة"[1]، خاصة وأن الاتحاد الأوروبي يعتبر أن الفضاء السيبراني مجالٌ للعمليات في إطار سياسة الدفاع السيبراني[2].وقد انطلقت استراتيجية 2013 من خمس أولويات كالآتي[3]:

- تحقيق المرونة في الفضاء السيبراني.
- التصدي للجريمة السيبرانية.
- تطوير سياسة للدفاع السيبراني في إطار الاتحاد الأوروبي.
- تطوير الموارد المتنوعة في مجال الأمن السيبراني (الصناعية والتكنولوجية).
- تطوير سياسة دولية خاصة بالفضاء السيبراني مع تعزيز القيم التي يدافع عنها الاتحاد الأوروبي.

لقد عبرت إستراتيجية الاتحاد الأوروبي لعام 2013 عن تأثير الفضاء الرقمي بأنه "شكّل منتدى لحرية التعبير وممارسة الحقوق الأساسية وأعطى للشعوب وسائل المكافحة من أجل مجتمعات ديمقراطية"، مما جعل الاتحاد الأوروبي يعمل على تطوير إستراتيجية شاملة تنطلق من الدفاع عن المعايير والمبادئ والقيم الأساسية له داخل وخارج الفضاء السيبراني، دون أن يتم إغفال احترام حقوق الإنسان كما يعبر عن ذلك[4].

في 2017 تعرض الاتحاد الأوروبي لهجمات برامج الفدية (التي تُنسب إل كوريا الشمالية) على غرار "واناكراي "WannaCry و"بيتيا"Petya، وقد كانت درجة المرونة والاستجابة جيدة على مستوى الاتحاد الأوروبي وعلى المستويات الوطنية، خاصة مع التعاون الذي أظهرته وكالات الأمن السيبراني الأوروبية، تبع ذلك طرح إستراتيجية الاتحاد الأوروبي الثانية لعام 2017 لتكون مكملة لسابقتها، مؤكدة على المرونة والدفاع السيبراني وبناء القدرات للتصدي للهجمات الإلكترونية، والتعاون الدولي الذي لا غنى عنه، ودور أصحاب المصلحة المتعددة في حماية الفضاء السيبراني[5].

---

[1] Delphine Deschaux-Dutard, ***Op.Cit***, p-p : 20-22.

[2] European Commission, The EU's Cybersecurity Strategy in the Digital Decade, ***Op.Cit***, P.18.

[3] Commission Européenne, ***Op.Cit***, p : 3,5.

[4] ***Ibid***, p.2.

[5] Gloria González Fuster and Lina Jasmontaite, «Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights », in: Markus_Christen and Others (editors), ***The Ethics of Cybersecurity*** (Switserland : The International Library of Ethics, Law and Technology, 2020), P-p : 98-100.

ثم تم الإعلان عن إستراتيجية الاتحاد الأمني في جويلية 2020، وهي تمتد من 2020 إلى 2025، وتهدف إلى ضمان الأمن في العالمين المادي وغير المادي، بما يعنيه ذلك من توفيق بين الأمن بمفهومه التقليدي والأمن داخل الفضاء السيبراني، وبما يشمله من مكافحة للإرهاب وتمويله[1].

في ديسمبر 2020، طرحت المفوضية الأوروبية وخدمة العمل الخارجي الأوروبي (EEAS) إستراتيجية جديدة للأمن السيبراني للاتحاد الأوروبي، وكان الهدف منها تعزيز المرونة السيبرانية في مواجهة تهديدات خطيرة كالإرهاب الإلكتروني، وحماية المستخدمين داخل الفضاء السيبراني، وسعيًا من القادة الأوروبيين إلى تحقيق استقلالية تدريجية على الصعيد الإستراتيجي "ويشمل ذلك تعزيز القدرة على اتخاذ خيارات مستقلة في مجال الأمن السيبراني، بهدف تعزيز القيادة الرقمية للاتحاد الأوروبي والقدرات الإستراتيجية"[2]. تستهدف إستراتيجية الأمن السيبراني الجديدة للاتحاد الأوروبي لعام 2021 تحقيق ثلاثة أهداف مركزية هي: المرونة والسيادة التكنولوجية، القدرة التشغيلية لمنع وردع والاستجابة للتهديدات، وكل هذا بغرض النهوض بفضاء رقمي عالمي ومفتوح، لذلك تقترح المفوضية الأوروبية وضع شبكة من مراكز العمليات الأمنية مع تعزيز أدوار الوكالات الأوروبية المختصة في الأمن السيبراني، وتلتزم بتخصيص أكثر من 300 مليون يورو لدعم الشراكة عام–خاص وتكريس الحوكمة الجيدة للفضاء السيبراني، كما يلتزم الاتحاد الأوروبي بتحسين أدوار مؤسساته "من خلال أحدث قدرات الذكاء الاصطناعي والتعلم الآلي واستكمالها ببنية تحتية للحوسبة الفائقة تم تطويرها في الاتحاد الأوروبي من خلال التعهد الأوروبي المشترك للحوسبة عالية الأداء"، إلى جانب الدور المعوَّل عليه بخصوص الوحدة الإلكترونية المشتركة الجديدة والتي توفر شبكة متينة من المراقبة والقدرة على اكتشاف التهديد قبل وقوعه[3].

وقد خصص الاتحاد الأوروبي مع منتصف 2020 مبلغ 49 مليون يورو، وُجّه "لتعزيز الابتكار في أنظمة الأمن السيبراني والخصوصية"، وفي إطار برنامج "أوروبا الرقمية" (2021–2027) خصص مبلغ 1,6 مليار يورو للاستثمار في قدرات الأمن السيبراني الأوروبي[4].وسيركز عمل المجلس الأوروبي في الأعوام المقبلة على عدد من الأولويات وهي[5]:

- إنشاء شبكة من مراكز العمليات الأمنية عبر الاتحاد الأوروبي، والهدف من ذلك هو الرصد والكشف عن حوادث الفضاء الإلكتروني.

---

[1] Sofija Voronova, ***Op.cit,*** p.6.

[2] European Council, Council of the European Union, « Cybersecurity: How the EU tackles cyber threats ? »,in: https://www.consilium.europa.eu/en/policies/cybersecurity/(12/09/2021)

[3] European Commission, The EU's Cybersecurity Strategy for the Digital Decade, ***Op.Cit***, P-p : 4-12.

[4] European Council, Council of the European Union, « Cybersecurity: how the EU tackles cyber threats», in: https://www.consilium.europa.eu/en/policies/cybersecurity/

[5] Council of the EU, « Cybersecurity: Council adopts conclusions on the EU's Cybersecurity Strategy », 22/03/2021,in: https://www.consilium.europa.eu/en/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy/ (12/09/2021)

- تفعيل العمل المشترك لفرض معايير أمان الإنترنت الرئيسَة ورفع معدل الأمان والانفتاح في الفضاء الرقمي.
- دعم جهود السلطات المختصة بإنفاذ القانون.
- تعزيز الدبلوماسية السيبرانية للاتحاد الأوروبي عبر توفير الأدوات المناسبة.
- إنشاء مجموعة عمل للاستخبارات الإلكترونية.
- تعزيز التعاون مع الأطراف الدولية المتنوعة، من دول ومنظمات.
- تنشيط عمل الوحدة الإلكترونية المشتركة استكمالا لبناء القدرة التشغيلية للوقاية والردع والاستجابة.

انطلاقا مما سبق يتضح اهتمام الاتحاد الأوروبي بملف الأمن السيبراني، وهو ما عكسته الاستراتيجيات المنتهجة منذ 2013. يأتي ذلك في سياق تكريس الحوكمة الجيدة في الفضاء السيبراني الأوروبي، وبالموازاة مع تفعيل أدوار عدد من الهيئات والوكالات المتخصصة في حماية الأمن السيبراني ومكافحة الإرهاب الإلكتروني والهجمات السيبرانية على حد سواء، وفيما يلي أهم هذه الوكالات:

د- الوكالات المتعلقة أو المتخصصة في الأمن السيبراني:

- **وكالة الدفاع الأوروبية (EDA):**

مقرها في بروكسل، وهي وكالة حكومية دولية تابعة لمجلس أوروبا، تتمثل مهمتها في "دعم الدول الأعضاء والمجلس في جهودهم لتحسين القدرات الدفاعية الأوروبية في مجال إدارة الأزمات والحفاظ على سياسة الأمن والدفاع الأوروبية كما هي الآن وكما ستتطور في المستقبل"، بالتالي تعمل الوكالة على تعزيز التعاون العسكري والدفاعي فيما بين الدول الأعضاء، وتضم حوالي 4000 خبير وطني في ملفات الدفاع التعاوني، كما لها أربعة أهداف مركزية هي: تطوير القدرات الدفاعية، تعزيز البحوث وتكنولوجيا الدفاع، تعزيز التعاون في مجال التسلح، ثم إنشاء سوق لمعدّات الدفاع الأوروبي بما يسهم في تقوية السوق الأوروبية من حيث الصناعة والتقنية، وبالنسبة لإدارة الأمن السيبراني فقد ساهمت وكالة الدفاع الأوروبية في إستراتيجية الأمن السيبراني للاتحاد الأوروبي، لتكون بذلك واحدة من الهيئات المهمة في مجال الدفاع السيبراني الأوروبي وتنسيق جهود وقدرات الأعضاء، فضلا عن التعاون مع الوكالات الأوروبية الأخرى، مثل وكالة أمن الشبكات والمعلومات (ENISA) ومركز الجريمة الإلكترونية (EC3)، في مجال تحليل وتقييم المخاطر، والتدريب ومشاركة الممارسات الجيدة[1].

- **المكتب الأوروبي للتعاون الشُّرَطي (EUROPOL):**

[1] Mario Nicolas Castellon Machado, ***Op.Cit***, p-p : 80-81.

يجري وصفه بأنه عنصر أساسي في تكريس التعاون الشرطي وقمع الجرائم السيبرانية[1]. فقد كان الهدف منه تحسين التعاون الشرطي بين أعضاء الاتحاد الأوروبي لمكافحة التهديدات الجديدة العابرة للحدود كالإرهاب والإرهاب الإلكتروني، وبالتالي العمل على إنفاذ القانون الدولي في المسائل ذات الصلة[2]. فهو إذًا وكالة هامة في مجال جمع المعلومات والتنسيق بين الدول الأعضاء في الاتحاد الأوروبي، ويشمل ذلك معلومات حول المقاتلين الإرهابيين الأجانب (FTF) والدعاية للنشاط الإرهابي عبر الانترنت[3]. أنشأ اليوروبول في 2013 المركز الأوروبي لمكافحة الجريمة السيبرانية، ثم عمل على تطوير إستراتيجية سماها "+2020" تتعلق بالتصدي للجريمة المنظمة والجريمة السيبرانية، وتأتي في سياق تعزيز إمكانات الاتحاد الأوروبي بمؤسساته وجامعاته لمواجهة التهديدات عبر الفضاء الإلكتروني[4].

وذكر اليوروبول في وقت سابق أنه تعامل مع تسع منصات إلكترونية (من بينها غوغل، تويتر، إنستغرام، وتليغرام) في سياق محاربة دعاية تنظيم "داعش" الإرهابي عبر الانترنت، فقام بفحص "فيديوهات دعائية وإصدارات وحسابات على مواقع التواصل الاجتماعي تدعم الإرهاب والتطرف العنيف"[5].وفي 2016 أُنشئ المركز الأوروبي لمكافحة الإرهاب (ECTC)، التابع لليوروبول، ليصبح مؤسسة داعمة لسلطات الاتحاد الأوروبي في مكافحة الإرهاب تأسيسا على السهولة في تبادل المعلومات، التعاون العابر للحدود من أجل تبادل وتنسيق الخبرات، بالإضافة إلى المساعدة في عملية التحقيق بخصوص الجرائم الإرهابية[6].

على إثر هجمات 11 سبتمبر 2001، أَلزم مجلس الاتحاد الأوروبي كل دولة عضو بإرسال المعلومات الآتي ذكرها إلى اليوروبول: البيانات المحددة لهوية فرد أو مجموعة إرهابية، القضايا ذات الصلة بجرائم الإرهاب، كل ما يفيد التحقيقات، استخدام التطور التقني في الاتصالات والتهديد المقترن بامتلاك أسلحة دمار شامل، كما جرى التأكيد على تبادل المعلومات حول الإرهاب في قرار المجلس JHA671/2005 والذي دعا إلى وضع نقطة اتصال داخل كل دولة عضو لتقوم بتجميع المعلومات المتعلقة بالتحقيق الجنائي. بالتالي، يعتبر اليوروبول وكالة مهمة في مكافحة الإرهاب السيبراني لأنه يوفر

---

[1] Pierre Berthelet, « Aperçu de la lutte contre la Cybercrime dans l'Union Européenne », ***Revue de science criminelle et de droit penal comparé***, 1(N°1), (2018), in : https://www.cairn.info/revue-de-science-criminelle-et-de-droit-penal-compare-2018-1-page-59.htm (15/09/2021)

[2] Süleyman ÖZEREN, «Cyberterrorism and International Cooperation: General Overview of the Available Mechanisms to Facilitate an Overwhelming Task », ***NATO Science for Peace and Security Series*** **(SPS)**, vol.34 (2007), p-p: 82-83.

[3] المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات، "مكافحة الإرهاب داخل الاتحاد الأوروبي: إستراتيجيات وتشريعات"، 28 أكتوبر 2021، https://bit.ly/3xy8/3i (2021/11/10)

[4] « Cybercriminalité : Un Défi à Relever aux nivaux National et International », Op.cit.

[5] "كورونا يعرقل جهود أوروبا في مواجهة خلافة داعش السيبرانية. دار الإفتاء المصرية تحذّر من هجمات الدولة الإسلامية في أعياد الميلاد"، 2020/12/22، https://bit.ly/3ehEZxy (2021/01/11)

[6] Europol (2021***), European Union Terrorism Situation and Trend Report (TE-SAT)***, Publications Office of the European Union, Luxembourg P.103.

المعلومات، بالإضافة إلى إنشاء وحدة تنبيه داخله لمكافحة الإرهاب (تعمل على مدار 24 ساعة)، وتضم ضباط اتصال من الشرطة والاستخبارات، ولكن بالرغم من إيجابيات اليوروبول يظل التنسيق بين الدول الأعضاء وتبادل المعلومات المهمة في مجال مكافحة الإرهاب والإرهاب الإلكتروني صعبا إلى حد ما، وهذا بالنظر إلى اختلاف الإطار السياسي والقضائي بين أعضاء الاتحاد الأوروبي من جهة، وحساسية بعض المعلومات ورفض الدولة مشاركتَها لصلة ذلك بحماية البيانات والخصوصية، هذا من جهة ثانية[1].

- **المركز الأوروبي للجرائم السيبرانية (EC3):**

تأسس في 2013 ومقره في لاهاي (هولندا)، يندرج في إطار هيكلة اليوروبول، ويعمل على تسهيل التواصل ما بين الخدمات المتنوعة في إطار محاربة الجريمة السيبرانية ومن أجل انترنت امن ومفتوح، تعنى نشاطاته بمكافحة الإجرام الإلكتروني، يضاف إلى ذلك جملة من النشاطات كتعزيز البحث العلمي في مجال الأمن السيبراني والتهديدات السيبرانية، دعم وتعزيز عمل المؤسسات الشرطية والقضائية، إنجاز تقارير حول التهديدات الجديدة ذات الصفة السيبرانية وتحليلها واستشراف التهديدات، وكل ذلك لا ينفصل عن الدور الممارس من لدُن المركز في الإنذار أو الكشف المبكر بما يسمح بجعل الدول الأعضاء تتصدى للهجمات وتحتوي انعكاساتها[2]. فهو مركز يوفر المعلومات والتحليلات ويدعم عملية التحقيق في الجرائم الإلكترونية، يعزز المهارات ويسهم في حشد الموارد، ويعزز التعاون في إطار تبادل المعلومات بين القطاعين العام والخاص من خلال التقارير المُعدَّة بخصوص التهديدات السيبرانية وتطوراتها وتحولات الفضاء السيبراني ذاته[3].

- **وكالة الاتحاد الأوروبي المكلفة بأمن الشبكات والمعلومات (ENISA):**

تم إنشاؤها في 2004 (مقرها باليونان). هي وكالة محورية تشكل دعامة للاتحاد الأوروبي ولأعضائه وللقطاع الخاص، فهي تمدّ هؤلاء بالتوجيه والإرشاد "ولهذا الغرض تقوم بجمع وتحليل البيانات، وبدراسة تقييم المخاطر وإدارتها، وبالتوعية وتعزيز التعاون بين القطاع العام والخاص"[4].تدعم الوكالة عمل المفوضية الأوروبية الرامي إلى تعزيز إمكانيات وفرص التعاون الأوروبي في المجال السيبراني، فضلا عن دورها في الجانب الاستشاري والتوعوي– التحسيسي[5]. وتدعو المفوضية هذه الوكالة إلى تقديم العون وتعزيز عمل

---

[1] Oldrich Bures, « Informal counterterrorism arrangements in Europe: Beauty by variety or duplicity by abundance? », ***Cooperation and Conflict***, 47(4), November 2012, pp: 495-518.

[2] « EC3, Le Centre Européen de la Lutte Contre la Cyber-Crime », in :https://www.guidedetective.fr/articles/ec3-le-centre-européen-de-lutte-contre-la-cybercrime

[3] Commission Européenne, ***Op.cit,*** p.11.

[4] اللجنة الاقتصادية والاجتماعية لغربي آسيا (ESCWA)، ***الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية: توصيات سياسية*** (نيويورك: منشورات منظمة الأمم المتحدة، 2015)، ص12.

[5] Cours de Comptes Européennes, ***Défis à relever pour une Politique de l'UE Efficace dans le Domaine de la Cyber Sécurité***, Document d'Information (Mars 2019), p.11.

الدول الأعضاء من حيث تطوير المهارات وآليات المرونة السيبرانية، والمساعدة في تنفيذ تمارين المحاكاة، ففي 2012 مثلا نظمت الوكالة مع بعض الدول الأعضاء في الاتحاد الأوروبي "الشهر الأوروبي للأمن السيبراني"[1].

تعمل وكالة أمن الشبكات والمعلومات على حماية البيئات الافتراضية للدول الأعضاء في الاتحاد الأوروبي، وتقديم الخبرات والحلول بخصوص الثغرات والتحديات التي يواجهها الفضاء الرقمي في أوروبا[2]. كما أنها تنسق عمل فريق الاستجابة لطوارئ الحاسوب، على المستوى الوطني وعلى مستوى الاتحاد الأوروبي، وبالتالي فهي تعمل على المستوى التشغيلي[3]. ويجري وصفها بأنها مركز خبرة داخل الاتحاد الأوروبي، وهذا نظرا لجهودها في تطوير ثقافة الأمن السيبراني على مستوى مواطني الاتحاد وحتى القطاعين العام والخاص، بالإضافة إلى عملها بالموازاة مع مبادرتين هما: نظام تنبيه مشاركة المعلومات الأوروبي (EISAS) والنظام الأوروبي للشراكة (عام–خاص) من أجل المرونة (EP3R)[4].

- **الوكالة الأوروبية للإدارة التشغيلية لأنظمة تكنولوجيا المعلومات (EU-LISA):**

تأسست في عام 2012، مقرها في تالين (إستونيا)، ولديها مكاتب في ستراسبورغ (فرنسا)، تعمل على أن "تكرّس نفسَها لإضافة قيمة إلى الدول الأعضاء باستمرار، ودعم جهودها من خلال التكنولوجيا من أجل أوروبا أكثر أمانًا"، وعلى هذا الأساس تهدف إلى "تقديم خدمات وحلول عالية الجودة وذات فعالية"، "بناء الثقة بين جميع أصحاب المصلحة ومواءمة قدرات التكنولوجيا باستمرار مع الاحتياجات المتطورة للدول الأعضاء"، بالإضافة إلى هدفها في التميز في مجال اختصاصها الدقيق، وتجب الإشارة إلى أنه منذ إنشاء هذه الوكالة تم تكليفها بإدارة ثلاثة مجالات تخص قواعد بيانات مهمة لمواطني الاتحاد الأوروبي وهي: نظام معلومات شنغن (SISII)، نظام معلومات التأشيرة (VIS) وقاعدة بيانات Dactyloscopy الأوروبية (EURODAC)، بالإضافة إلى أن الوكالة مسؤولة عن تنفيذ التدابير الأمنية، والتدريب على استخدام الأنظمة، وإعداد الإحصائيات والتقارير والبحوث المتصلة، ولا يقتصر ذلك على حدود "شنغن" وإنما يمتد خارجها من خلال ما يُعرف بمبادرة "الحدود الذكية". بالتالي، وانطلاقا من تلك التدابير، تساهم الوكالة في إدارة الأمن السيبراني للاتحاد الأوروبي من خلال حماية وإدارة البيانات الحيوية لمواطني الاتحاد[5].

---

[1] Commission Européenne, ***Op.cit.***, p-p : 8-9.

[2] Alexandru ION, IMPLEMENTING ENISA'S CYBER SECURITY PLAN IN THE EUROPEAN UNION ", in the 12 international scientific conference strategies, Strategic changes in security a nd international relation, vol 3, Bucharest, Romania: April 14-15, 2016, in: https://cutt.us/h7IH9 (04/012/2021).

[3] Anna Kańciak, "In search of EU law in the domain of cyberspace protection- The proposal based on the cyber PDCA model", ***Journal of Cyber Security Technology,*** Vol.1, Issue 2 (April 2017), P-p: 127-143. 24/05/2017, in: https://cutt.us/mmEHV (22|05|2021).

[4] Mario Nicolas Castellon Machado, ***Op.cit***, p-p : 81-83.

[5] ***Ibid***, p-p: 74-75.

- **شبكة التوعية بالتطرف (RAN):**

أنشأها الاتحاد الأوروبي (المفوضية الأوروبية) لتكون حلقة وصل بين الأطراف المتنوعين، وهي تضم فئات أكاديمية (مدرّسون، خبراء اجتماعيون..) ومهنية (الشرطة) بالإضافة إلى منظمات غير حكومية[1]. تعمل على تسهيل تبادل المعلومات في سياق التصدي للتطرف والإرهاب بجميع أنواعهما[2].تضم أكثر من 3200 عضو من الأوساط الأكاديمية والحكومية والمجتمع المدني، و"تتمثل مهمة الشبكة في تعزيز المشاريع التجريبية وأفضل الممارسات عبر الحدود ونشر نتائج الأبحاث الجديدة، وفي عام 2019 تمّ إنشاء مجلس توجيه إضافي لتقديم المشورة للدول الأعضاء بشأن سياسات الوقاية الخاصّة"[3].

- **وحدة الإحالة عبر الانترنت في الاتحاد الأوروبي (IRU):**

كان لهجمات شارلي ايبدو في فرنسا سنة 2015 وقعٌ كبير على سياسات مكافحة الإرهاب في أوروبا، فعلى إثر ذلك استحدث الاتحاد الأوروبي في إطار اليوروبول هذه الوحدة الخاصة بمتابعة والكشف عن المحتوى المتطرف والإرهابي عبر الانترنت، لتكون نسخة مطوَّرة من وحدة "فحص الشبكة" Check The Web التي استخدمتها المملكة المتحدة (بريطانيا) منذ 2007[4]. يرتبط عمل الوحدة بالمركز الأوروبي للتعاون الشرَطي Europol، وتضم خبراء ومختصين في مجال مكافحة الإرهاب وتطوير تكنولوجيا المعلومات والاتصالات، وللإشارة فإنه خلال الفترة: 2015-2017 تم العثور على ما يعادل 46392 محتوى إرهابي عبر الانترنت[5]. ومن جويلية 2015 وحتى نهاية 2020 أشرفت وحدة الإحالة على تقييم 127168 محتوى يوصف بالإرهابي عبر 370 منصة إلكترونية، ليتم إحالة 123551[6].وفي تقرير لوحدة الإحالة صدر في جوان 2016 فقد تم تحليل أكثر من 11 ألف رسالة إلكترونية كان الهدف منها استقطاب أفراد أوروبيين للانخراط في النشاط الإرهابي العابر للحدود، وبالتعاون مع شركتي فيسبوك وتويتر تمت إزالة 92 بالمائة من المحتوى المتطرف، ويمكن تلخيص مهام وحدة الإحالة فيما يلي[7]:

---

[1] Ines von Behr, and Others, ***Op.cit,*** p.7.

[2] Mar Negreiro, ***The NIS2 Directive: A High Common Level of Cybersecurity in the EU, EU Legislation in Progress***, European Parliament Research Service (December 2021), P.68.

[3] جاسم محمد، "صناعة الكراهية داخل أوروبا.."، مرجع سابق.

[4] محمود رشدي، "اليوروبول: تهديدات متصاعدة وتحديات راهنة"، 2018/10/22، https://www.almarjie-paris.com/4596 (2021/04/08)

[5] Le Centre pour la Gouvernance du Secteur de Sécurité, ***Op.Cit***, p-p : .97-100.

[6] Europol, ***Op.Cit***, p-p : 105-106.

[7] محمود رشدي، **مرجع سابق**.

- ✓ مراقبة وكشف المحتوى المتطرف والإرهابي عبر الإنترنت، وذلك من خلال تتبع الكلمات الدلالية التي تتضمنها المنشورات المتطرفة كالتحريض على العنف مثلا.
- ✓ التحليل والتقييم من خلال إرسال المحتوى إلى قاعدة بيانات الوحدة المركزية، وهنالك يتم تأكيد ما إذا كان بالفعل محتوى إرهابيا يتطلب حذفَه.
- ✓ التعرف على هوية القائمين على هذا المحتوى.
- ✓ دعم الجهات الأمنية الشُّرَطية على مستوى الاتحاد الأوروبي فيما يخص المحتوى الإلكتروني.
- ✓ جمع المعلومات التي تسمح بفهم تكتيكات الجماعات الإرهابية وأساليبها الدعائية، وهو ما يتيح المجال لتطوير آليات محاربتها.
- ✓ العمل على إزالة المحتوى المذكور بعد إحالته (تسمى مرحلة الإحالة) إلى الشركات المعنية (مثل فيسبوك أو تويتر).

وكان البرلمان الأوروبي والمجلس الأوروبي قد ناقشا مشروع اتفاق يتعلق بالمحتوى الإرهابي على الانترنت والتصدي للأخبار الكاذبة والمضلّلة، حيث "يُلزم شركات الانترنت بإزالة المحتوى الإرهابي في مدة لا تتجاوز ساعة من نشره، وتشمل مضامين النشر في الانترنت التسجيلات الصوتية أو مقاطع الفيديو التي تحرض على ارتكاب جرائم إرهابية أو توفر تسهيلات لارتكاب جرائم إرهابية"، وعلى أساس ذلك يتعزز صدّ الدعاية الإرهابية من خلال تعطيل وإزالة المحتوى، وهنا يلاحَظ اهتمام الاتحاد الأوروبي بدور الفضاء السيبراني في النشاط الإرهابي أو كما قال النائب في البرلمان الأوروبي "باتريك جاكي": "الانترنت هو المكان الذي يقوم فيه الإرهابيون بالتجنيد وتبادل الدعاية وتنسيق الهجمات"[1].

وذكر مشغّلُو منصات التواصل الاجتماعي على غرار فيسبوك وتويتر ويوتيوب أن حوالي 90 بالمائة من المحتوى المتطرف والإرهابي يتم اكتشافُه قبل إزالته، وقامت شركة "تلغرام" بغلق حوالي 8500 حساب للمنخرطين في تنظيم "داعش" الإرهابي، وكانت الجهود الأوروبية قد تمكنت من وقف تشغيل خدمة الرسائل بالنسبة للتطبيق "الذي يُعتبر المنفذ الرئيس للمجموعة منذ 2015، وفقا ل "يورو نيوز" في 28 يناير 2020"، كما تمكّن الاتحاد الأوروبي من حذف ما يعادل 26 ألف حساب على الانترنت، كانت حسابات تابعة لتنظيم "داعش" الإرهابي، أتى ذلك بعد أن اكتشفت الحكومات الأوروبية نمو توظيف

[1] "اتفاق أوروبي بشأن مكافحة المحتوى الإرهابي في الانترنت"، 2020/12/12، https://arabic.euronews.com/2020/12/12/eu-mep-agreed-plan-fight-against-terror-content-online (2021/01/30)

الإرهابيين لشبكة الانترنت في نشر الفكر المتطرف والدعاية للعمل الإرهابي، ولم يقتصر الأمر على الإرهاب الجهادي كما يوصف، وإنما احتل أيضا نشاط اليمين المتطرف في أوروبا موقعا خطيرا من حيث استغلال المنصات الاجتماعية، وكمثال فإن الاعتماد على الدردشات الجماعية عُدّ سياسة معروفة لدى هؤلاء، خاصة وأن تطبيقات مثل تلغرام تتيح إمكانية إنشاء دردشة جماعية بمعدل 200 ألف شخص، في حين يحدد واتساب الدردشة الجماعية ب256 شخصا فقط. معنى ذلك أن فرصة نشر الفكر المتطرف تزيد انطلاقا من عدد المشاركين في المحادثة[1].

ويكمل عملَ شبكة التوعية بالتطرف ووحدة الإحالة عبر الانترنت دورُ الشبكة الأوروبية للخبراء حول التطرف (ENER)، وهي منظمة أسسها الاتحاد الأوروبي، ويستضيفها معهد التغيير في المملكة المتحدة، تضم شبكة من المنظمات والخبراء في قضايا التطرف والإرهاب، كما أنها محاولة لتعميق فهم التهديدات ذات الصلة من خلال المنشورات والندوات وورش العمل[2].

- **المحكمة الأوروبية (Eurojust):**

جهاز مهم من أجهزة الاتحاد الأوروبي، أنشئت في 2002 ومقرها في هولندا، تمثل وكالة التعاون في مسائل العدالة الجنائية، فهي تساعد الدول في مجال مكافحة الإرهاب والجرائم المنظمة العابرة للأوطان، من خلال المساعدة في التحقيقات والملاحقات القضائية على مستوى دولتين على الأقل، وإنفاذ الصكوك القانونية للاتحاد الأوروبي[3].

- **وكالة الاتحاد الأوروبي للتدريب على إنفاذ القانون (CEPOL):**

وكالة تابعة للاتحاد الأوروبي، أنشئت في 2005 ومقرها في بودابست، تشرف على تدريب عناصر الشرطة والمسؤولين في مجال إنفاذ القانون وتشجيع تبادل المعرفة والخبرات والتعاون بين المؤسسات الشرطية، بالاعتماد على تقنيات تدريب متطورة ومبتكَرة[4]. لقد تم تأسيس الوكالة الأوروبية لإنفاذ القانون

[1] جاسم محمد واخرون، الإرهاب والتطرف في أوروبا من الداخل، ***مرجع سابق***، ص: 12، 27-35.

[2] Ines von Behr, and Others, ***Op.cit***, P-p: 6-7.

[3] « Eurojust », in: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/eurojust_en (15/10/2021)

[4] « European Union Agency for Law Enforcement Training (CEPOL) », in: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/cepol_en(23/04/2021)

لغرض تسهيل التفاعل وتنسيق المهام بين مؤسسات الاتحاد الأوروبي، وهي تقوم بتدريبات متخصصة في مجال مكافحة الإرهاب، "أي أنها تشارك في بناء القدرات"[1].

- **أنظمة/وحدات الاستجابة الطارئة (CIRT/CERTS)[2]:**

تم إنشاء نظام وحدات الاستجابة لحوادث الكمبيوتر على مستوى الاتحاد الأوروبي (EU-CERT) في سبتمبر 2012، وتعد منظمة دائمة تفيد مؤسسات وهيئات الاتحاد الأوروبي من حيث تقديم معلومات حول نقاط الضعف في منتجات المؤسسات والتطبيقات والبرامج وقواعد البيانات وأنظمة التشغيل، ومعلومات أخرى حول الحوادث الرقمية التي تمس الكمبيوتر والفضاء الإلكتروني في إطار الجريمة السيبرانية بمضمونها الواسع[3].

وحدات الاستجابة لطوارئ الحاسوب (CIRT/CIRTS) تقدم المشورة وتزود المؤسسات بإشعارات بخصوص الهجمات المتوقعة[4]. لذلك فهي أساسية لحماية البنية التحتية للمعلومات، خاصة وأنها ترصد التهديدات ونقاط الضعف بسرعة فائقة[5]، وتسمح بمتابعة حوادث الكمبيوتر عبر نقطة اتصال مركزية والاستجابة لها[6]، بإمكان أي مواطن أوروبي يعاني حالة طوارئ تتعلق بالحاسوب الاتصالُ بفرق الاستجابة للطوارئ حسب حاجته، "سواء كان ذلك للاستخدام الجماعي أو الشخصي"، وفي حالة تواجد مواطن من الاتحاد الأوروبي في المملكة المتحدة مثلا يمكنه الاستفادة من 17 فريقا وطنيا أو 10 فرق دولية[7].

- **الوحدة السيبرانية المشتركة:**

تمثل منصة افتراضية ومادية للتعاون داخل الاتحاد الأوروبي في مجال الأمن السيبراني، فهي مخصصة لتنسيق وتنظيم عمل وكالات الاتحاد الأوروبي والتعاون التشغيلي وتبادل المساعدة، وتهدف إلى تحقيق الجاهزية في الفضاء السيبراني ومزيد من الوعي بتهديدات هذا الفضاء، إلى جانب تعزيز الاستجابة والتعافي، وكان النقاش داخل الاتحاد الأوروبي حول الوحدة السيبرانية المشتركة قد تناول تحديد القدرات المتوفرة على صعيد الاتحاد وعلى المستويات الوطنية، وسبل التعاون الجيد، والموارد المخصصة لهذه الوحدة بغرض تفعيلها وتعزيز قدرة الاستجابة لتهديدات الفضاء السيبراني[8].

---

[1] Mar Negreiro, ***Op.Cit***, P.68.

[2] CIRT: Computer Incident Response Teams and CERTS: Computer Emergency Response Teams

[3] Mario Nicolas Castellon Machado, ***Op.cit***, p.84.

[4] Javier Argomaniz, "EUROPEAN UNION RESPONSES TO TERRORIST USE OF THE INTERNET", ***Cooperation and Conflict,*** vol.50, N2, (2015), p.9.

[5] اللجنة الاقتصادية والاجتماعية لغربي آسيا، ***مرجع سابق***، ص21.

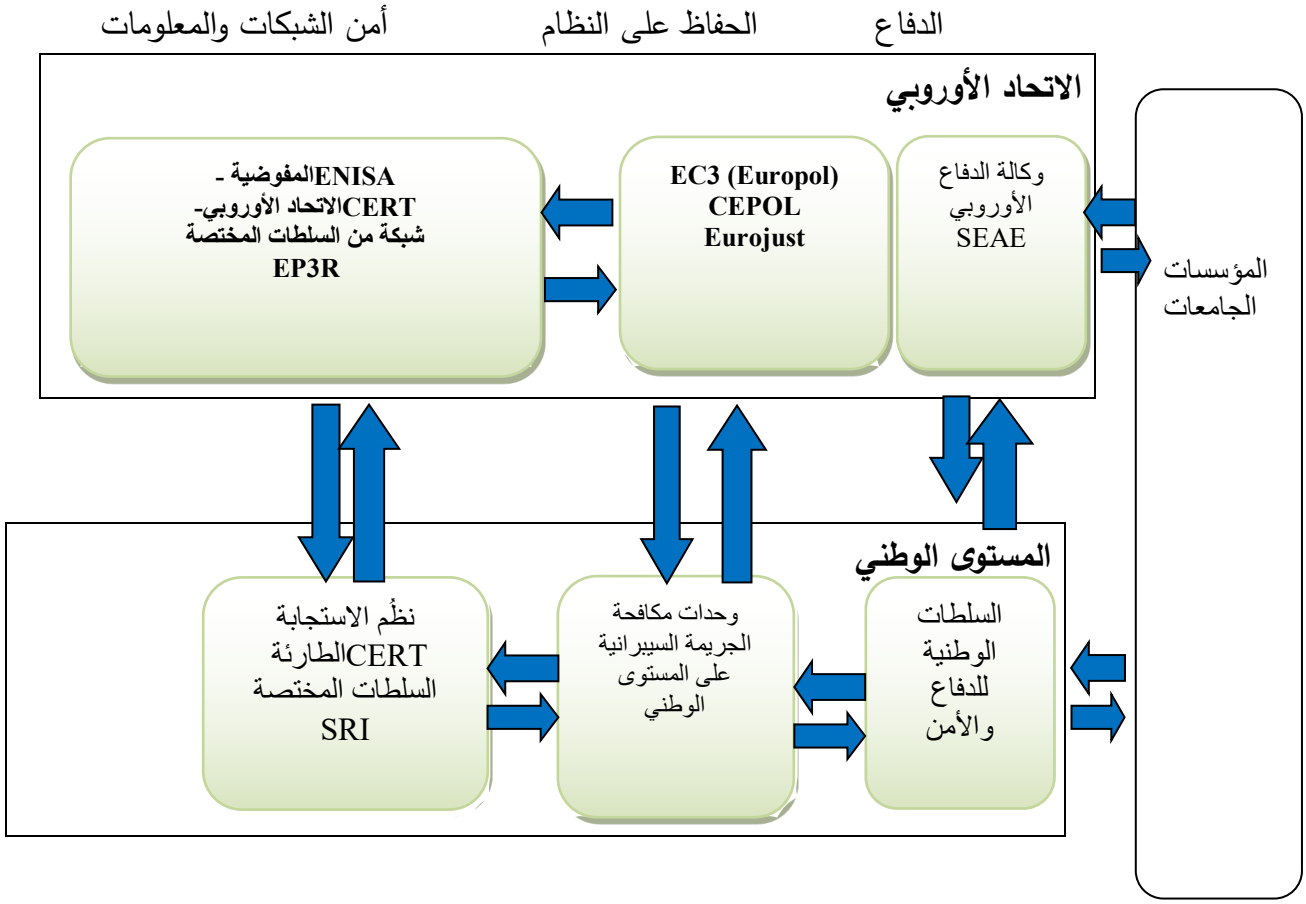
[6] ITU, ***Op.Cit,*** 2021, p.06.

[7] Mario Nicolas Castellon Machado, ***Op.cit***, p.102.

[8] European Commission, The EU's Cybersecurity Strategy for the Digital Decade, ***Op.Cit***, P-p : 13-14.

فيما يلي مخطط يلخص أهم الوكالات المختصة بحماية الأمن السيبراني الأوروبي، إلى جانب الجهات المخولة بذلك على المستوى الوطني لأعضاء الاتحاد الأوروبي:

الشكل (15): مخطط يوضح المؤسسات المخولة بحفظ الأمن السيبراني على مستوى الاتحاد الأوروبي وعلى المستوى الوطني والتفاعل فيما بينها.



Surce : Commission Européenne, La Haute Représentation de l'Union Européenne pour les Affaires Etrangeres et la Politique de Sécurité, ***Stratégie de Cyber Sécurité de l'Union Européenne : un cyberspace ouvert, sur et sécurisé***, Communication conjointe au parlement Européen, au conseil, au comité économique et sociale Européen et au comité des régions (Bruxelles, Juin 2013), p.19.

يوضح المخطط الجهات المخولة والمختصة بحماية الأمن السيبراني بأبعاده جميعها على مستوى الاتحاد الأوروبي من جهة، وعلى المستوى الوطني بالنسبة للدول الأعضاء من جهة ثانية. ثم يظهر التفاعل والتعاون الحاصل بين هذه الجهات سواء على مستوى الاتحاد الأوروبي أو على المستوى الوطني، أو حتى بين الاتحاد ككيان والوكالات الوطنية داخل أعضائه، مع إبراز الاهتمام بالجانب الأكاديمي باعتبار أن البحوث الرصينة من أساسيات إنتاج المعرفة والوعي والثقافة السيبرانية، فضلا عن تزويدها للوكالات الأوروبية بالتحاليل والرؤى الاستشرافية.

- الدبلوماسية السيبرانية:

يحتاج الاتحاد الأوروبي إلى أن يعزز مكانته ودوره في إطار حوكمة الفضاء السيبراني بشبكة من أدوات الدبلوماسية السيبرانية، وتتمثل أهميتها في الترويج للرؤية الأوروبية في المجال السيبراني وتبادل المعلومات مع أطراف دولية متنوعة[1]. ويَبرز طموح الاتحاد الأوروبي لأن تصبح قضايا الأمن السيبراني من صميم علاقاته الخارجية، باعتبار أن ذلك يسمح بتشكيل وعي وثقافة سيبرانية أكبر تجاه تهديدات الفضاء غير المادي، هذا جنبا إلى جنب مع ضرورة تعزيز الوعي السياسي بأهمية المرونة السيبرانية[2].

تنادي البنائية بضرورة تفعيل آليات الدبلوماسية الرقمية لخلق بيئة ثقة في هذا العالم الافتراضي، والتي يمكن تعريفها على أنها "وسيلة لتحقيق أهداف الدبلوماسية العامة عن طريق استخدام أنظمة الاتصال الحديثة، أو ما يعرف بالمجتمعات الافتراضية... معتمدةً في ذلك على إستراتيجية التفاعل بين المواطنين والمسؤولين لإيجاد منصات جديدة للتواصل والتفاعل وتعبئة الرأي العام مع جماهير ومستخدمين آخرين من جميع أنحاء العالم". وتعد الولايات المتحدة الأمريكية أول دولة تقوم بإنشاء دبلوماسية رقمية وذلك في 2003، بهدف الترويج للنموذج الأمريكي، كما قامت بريطانيا بإنشاء مجموعة الدبلوماسية الرقمية في 2009[3].بالتالي، يجب التنويه بدور الدبلوماسية السيبرانية في تحديد النشاط المسموح به داخل الفضاء السيبراني، وهو ما يدخل في إطار قواعد السلوك السيبراني للدولة، لهذا فإن تكريس دبلوماسية رقمية محددة الأهداف، تعنى بمواضيع الفضاء السيبراني، يُنظر إليه كعملية مهمة لحماية الأمن السيبراني الأوروبي[4].

يتضح من خلال ما سبق تناوله أن استراتيجيات الأمن السيبراني في الاتحاد الأوروبي تولي اهتماما بالغا بحوكمة الأمن، ويظهر ذلك من خلال الرؤية المتكاملة والسياسات المتبناة طوال ما يقارب عقدا كاملا من الزمن.

---

[1] European Commission, The EU's Cybersecurity Strategy for the Digital Decade, ***Op.Cit***, P.22.

[2] European Union Institute for Security Studies (EUISS***), Cyberspace and EU Action to 2030***, A report based on an expert webinar organised by the French Permanent Representation to the European Union on, with the support of the EU Institute for Security Studies (9 July 2021), p.3.

[3] سارة يحيى، "Cyber Diplomacy: بُعد غير تقليدي في العلاقات غير الرسمية بين الدول"، ***دورية اتجاهات الأحداث***، العدد 6 (يناير 2015)، ص-ص: 08-10.

[4] ميليسا هاثاواي، ***مؤشر الجاهزية الإلكترونية: خطة للجاهزية الإلكترونية- خط قاعدي ومؤشر*** (الولايات المتحدة الأمريكية: معهد بوتوماك للدراسات السياسية، نوفمبر 2015)، ص: 25-26.

خاتمة الفصل واستنتاجاته:

على الرغم أنه من الواضح أن خطاب الاتحاد الأوروبي حول تهديد الإرهاب السيبراني قد تغذى جزئيًا من خلال بعد التهديدات التي أبرزناها، والمتعلقة بتلك التي تمس أو قد تمس البنية التحتية الحرجة والقيم المجتمعية، إلا أن الخطاب حول الإرهاب السيبراني في معظمه توقع تهديدًا افتراضيًا أكبر يواجه المستقبل. خاصة مع إمكانات الجماعات الإرهابية وقدرتها على تطوير نفسها، واستغلال نقاط الضعف في البنية التحتية الحيوية الموجودة في الاتحاد الأوروبي، كما أن السلطات الحكومية والأكاديميين الأوروبيين على حدٍ سواء أقروا بإمكانات الإنترنت في تعزيز التطرف السياسي أو الديني أو الأيديولوجي، وعديد الآثار المترتبة عن استخدام الويب، على سبيل المثال لا الحصر: كوسيلة الاتصال، أو لنشر المعلومات والدعاية الأيديولوجية، كمنصة للتجنيد، أو بيئة لجمع التبرعات، أو كآلية للهجمات الإلكترونية والجسدية.

ومن بين التهديدات التي تواجه الحكومات والمجتمعات الأوروبية نذكر : التطرف ونشر خطاب الكراهية، سرقة، تعطيل أو تدمير المعلومات أو الأنظمة الحاسمة لأمن الدولة أو البنية التحتية أو الجيش، في حين أن التعريفات التقليدية للإرهاب السيبراني عالجت مثل هذه التهديدات على وجه التحديد، يجب أن تدرك المفاهيم المعاصرة أيضًا أن أكبر فائدة للإرهابيين للإنترنت كونها مُيسرا وليس دافعًا.

وما يلاحظ أن الترابط بين الإنترنت يكمل تمامًا الهيكل غير المتبلور والطبيعة المتمحورة حول وسائل الإعلام للمنظمات الإرهابية المعاصرة التي تستخدم وسيلة الدعاية والتجنيد، وجمع الأموال، ونشر المعلومات، والتبرير لعملياتها الإجرامية. وبهذه الطريقة، قد يكون من الأنسب وصف الإنترنت على أنه عامل مضاعف للقوة ومُمَكّنْ لها، كما يربط الأفراد المتفاوتين جغرافيًا من خلال التأثير على الوعي الظرفي، الأمر الذي قاد الدول الأوروبية لتعزيز طروحات بناء الأمن الجماعي في شقه السيبراني، لحماية البنية التحتية الحيوية من هجمات الإرهاب السيبراني بمختلف أطيافه الجهادي، اليميني، اليساري، والانفصالي، الجماعات التي لديها القدرة على إحداث تأثيرات كبيرة على حياة الناس وعلى الأنشطة الاقتصادية، البنى الأمنية والسياسية باستخدام شبكات الاتصالات وأنظمة المعلومات.

وانطلاقا من ذلك يمكن تقديم الاستنتاجات الآتية:

الاستنتاجات:

- من خلال تحليل استجابة الاتحاد الأوروبي لتهديد الإرهاب يمكن القول ان تهديد الإرهاب السيبراني غير محدد بشكل جيد، سواء داخل الاتحاد الأوروبي أو على الصعيد الدولي، وأن الاتحاد الأوروبي يعتمد على تهديد الإرهاب السيبراني – جنبًا إلى جنب مع مجموعة أوسع من التهديدات – لتأييد ضرورة التدابير الأمنية والتشريعية الحالية والمستقبلية للاتحاد الأوروبي.

- إن إضفاء الطابع الأمني على تهديدات الإرهاب السيبراني يتناسب مع نهج أمني وقائي أوروبي شامل لزيادة مرونة البنية التحتية الحيوية للتدخل السيبراني، هذا النهج لتوضيح مشهد التهديد السيبراني هو أيضًا رمز للنهج الوقائي لرسم الخرائط والتخفيف من المخاطر التي تواجه البنى الحرجة داخل الدول الأوربية.

- بينما ارتكز الاهتمام على أن التهديد السيبراني على أساس أنه يمثل مشكلة "ما بعد الدولة أو مابعد الدولنة" بشكل واضح، إلا أنه من الصعوبة بما كان تجاوز المفهوم الويستفالي للمشكلة أو للحلول الممكنة، يؤدي هذا إلى مفارقة مركزية حول الأمن السيبراني كما نتصوره حاليًا: فمن ناحية، تبيَّن أنها مسألة لا يمكن التعامل معها بشكل فعال من خلال أدوات الدولة مثل الجيش أو مؤسسات انفاذ القانون، ولكن على الرغم من ذلك، لا تزال هناك توقعات قوية أن تتحمل الدولة مسؤولية توفير الأمن في هذا المجال. وقد أدت هذه المفارقة إلى التركيز في وثائق سياسة الأمن السيبراني على ضرورة التعاون الدولي للوصول لبنية صلبة للأمن الجماعي.

- إن مدارسة حوكمة الأمن في الاتحاد الأوروبي كمشكلة عمل جماعي وفق تحليل المنتج المشترك تجعلنا نخلص إلى أن الدول الأعضاء الأصغر في الاتحاد الأوروبي ليست حرة في رؤية سياسات الأمن الجماعي، على عكس إحدى الفرضيات المركزية في أدبيات الاختيار العام التي توضح أن الدول الأعضاء في الاتحاد الأوروبي في الواقع تتقاسم التكاليف بالتساوي مع الأبعاد المختلفة للحوكمة الأمنية.

- الدول الأوربية ألزمت نفسها بمواصلة تطوير قدراتها الوطنية للدفاع السيبراني وتعزيز الأمن السيبراني لشبكاتها، الاستراتيجية التي تعد أولوية قصوى لضمان الدفاع عن شبكاتها الوطنية، لهذا الغرض تتعاون الدول الأوربية ضمن تحالفات (دول الاتحاد الأوروبي وحلف الناتو) مع السلطات الوطنية لضمان مستوى مناسب من الدفاع الإلكتروني.

- يطرح الفضاء السيبراني مشكلات قانونية وأخلاقية كتلك المتصلة بالحياة الخاصة (الخصوصية) وحرية التعبير، من خلال هذا حاول الاتحاد الأوروبي معالجة التهديدات السيبرانية الجديدة، لكن هذه المعالجة السوسيو–أمنية تتقاطع في مضمونها مع مبادئ الديمقراطية والحقوق الأساسية للأفراد، ومع ذلك، هذا لا يجعل هذه السياسات غير مهمة، قد تكون بعض المبادرات على المستوى الأوروبي –التي تتقاطع وخصوصية الأفراد–والمصممة لتقويض التطرف عبر الإنترنت، قد فشلت بالفعل في تحقيق التوازن بين الحاجة إلى اتخاذ إجراءات فعالة مقابل الالتزام بحماية خصوصية مستخدمي الإنترنت.

- نخلص إلى أن بناء الأمن الجماعي الأوروبي في العصر السيبراني يعد مهمة معقدة حيث توجد العديد من التحديات والعقبات التي يجب معالجتها, ومن أبرز المشكلات التي تظهر في هذا السياق ما يلي:

1- **انعدام الثقة:** أحد أكبر التحديات هو أن الدول الأوروبية لا تثق في بعضها البعض عندما يتعلق الأمر بالأمن السيبراني، حيث أن هناك نقص في الثقة والتعاون بسبب الخصومات التاريخية والمصالح الوطنية، وهذا يجعل من الصعب بناء إطار عمل للأمن الجماعي.

2- **التهديدات غير المتكافئة:** في عصر الإنترنت غالبًا ما تكون التهديدات غير متكافئة، مما يعني أن الجهات الفاعلة الصغيرة ذات الموارد القليلة يمكن أن تلحق أضرارًا كبيرة، الأمر الذي يجعل من الصعب إنشاء نظام أمان شامل يمكنه معالجة جميع التهديدات السيبرانية المحتملة.

3- **الاختلافات الثقافية:** لدى البلدان الأوروبية المختلفة مناهج مختلفة للأمن السيبراني ومواقف مختلفة تجاه الخصوصية والمراقبة، وهذا يجعل من الصعب وضع قواعد ومعايير مشتركة يمكن أن تكون بمثابة أساس لإطار الأمن الجماعي.

4- **التحديات التقنية:** نظرًا لتعقيد وتعقيد التهديدات الإلكترونية، من الصعب بناء حلول تقنية فعالة يمكن أن توفر درجة عالية من الأمان مع ضمان خصوصية المستخدم وحريته.

5- **التحديات القانونية والتنظيمية:** البيئات القانونية والتنظيمية في مختلف البلدان الأوروبية ليست موحدة، وهذا يجعل من الصعب إنشاء إطار قانوني يمكن استخدامه لمحاكمة مجرمي الإنترنت أو محاسبة الشركات على انتهاكات البيانات.

- بشكل عام، يتطلب بناء الأمن الجماعي الأوروبي في العصر السيبراني اتباع نهج شامل يعالج التحديات التقنية والقانونية والثقافية، وسيتطلب استثمارا كبيرا في التكنولوجيا وبناء القدرات، فضلا عن قدر أكبر من التعاون والتنسيق بين الدول الأوروبية.

الفصل الرابع

الفصل الرابع: إستراتيجية بناء الأمن السيبراني الأوروبي- الرهانات والتحديات

المبحث الأول: النهج الأوروبي التعاوني عبر الوطني لأمن الشبكات والمعلومات.

المبحث الثاني: الصكوك القانونية وإعادة بناء القدرات.

المبحث الثالث: نحو تطوير جدول أعمال بحث حول الإرهاب الإلكتروني- التحديات التقنية والحلول.

تمهيد الفصل:

في ظل الزخم الذي أُعطي لموضوع الإرهاب وسبل مكافحته، تنامت استراتيجيات مكافحة الإرهاب والتطرف عبر الأنترنت، وتم في هذه الفترة تشكيل إجماع عالمي غير مسبوق تجاه هذه الظاهرة، حيث تم تطوير المؤسسات والأعراف والممارسات على مستويات دولية، وأصبح إدراج البعد السيبراني في سياسات وإستراتيجيات الدفاع ضرورة أقرها عصر المخاطر العابرة للحدود، ولا تنفصل الإستراتيجية الأوروبية عن الإستراتيجية الدولية في مكافحة الإرهاب بشكل عام والإرهاب الإلكتروني بشكل خاص، بحثا عن تحقيق الأمن في الفضاء الإلكتروني (أمن الفرد والمجتمع والدول)، كما أن معالجة الظاهرة الإرهابية، بمظاهرها المتنوعة وتحولاتها وتطورات أساليبها، جعلت منها أساسا تبنى عليه استراتيجيات الدفاع في الدول الأوروبية، من خلال محاربة التنظيمات الإرهابية كتنظيم "داعش" الإرهابي، والجماعات الانفصالية في أيرلندا الشمالية، إلى جانب ألمانيا وتجربتها مع الجيش الأحمر اليساري، وإسبانيا وتجربتها مع منظمة "إيتا"[1].

ومع تطور أشكال التهديدات، والنمو في التحديات السيبرانية التقليدية The Growth in Traditional Cyber Challenges و استخدام التقنيات المتطورة للقيام بجرائم سيبرانية، خاصة بالتزامن مع ظهور الذكاء الاصطناعي والروبوتات، تم طرح إشكالية مفادُها: هل الدول الأوروبية على استعداد لمواجهة التحديات المتنامية الناجمة عن التهديدات الناشئة والهجينة المستحدَثة في الفضاء السيبراني؟[2].

قبل الخوض في تفاصيل الاستجابة الأمنية، يجب أن نفهم تصنيف سياسات مكافحة الإرهاب بشكل عام والتي يمكن تقسيمها إلى: الوقاية، الحماية، الملاحقة والرد أو الاستجابة للتهديد، ومنها بحث سبل الردع، انطلاقا من ذلك، وبعد أن تم التطرق بإسهاب في الفصلين السابقين إلى عناصر هامة كانت بمنزلة مداخل أساسية لموضوع الأطروحة، يأتي الفصل الثالث والأخير ليشكّل فهما واضحا للرؤية الأوروبية الشاملة بناءً على المنطق الاستباقي والوقائي، عبر فحص هذا التوسع في التهديدات الإرهابية السيبرانية وممارساتها، التي وجدت في أوروبا بيئة مناسبة لنشاطاتها، وذلك من حيث الأسس والآليات

[1] Miriam Allam, Damian Gadzinowski, ***Combating the Financing of Terrorism: EU Policies, Polity and Politics***, EIPASCOPE (02/2009), p.41.

[2] Udo Helmbrecht–Deutor, « Cybersecurity: Best Practices », Conference (Greece, 12/12/2018), p.2.

والثغرات وسياسات التعاون العبر– وطني، ليكون هذا الفصل تشخيصا للسياسات والمشكلات التي يطرحها تقييم المخاطر الذي تم مدارسته في الفصل السابق، بعد فحص الطبيعة الأمنية التي أوجدها الإرهاب السيبراني؛ ومنه، سيكون هذا الفصل تحليلا للمجالات المؤسسية والجهات الفاعلة التي يتم من خلالها تنفيذ السياسة الأمنية الأوروبية، بالإضافة إلى محاولة الكشف عن رؤية جديدة لتحقيق المرونة والنضج السيبراني لمواجهة أو ردع التهديد الإرهابي المحتمل في الفضاء المادي وغير المادي، وما الذي يمكن بلوغه انطلاقا من السياسات والتدابير المتناوَلة، وبحث سبل تحسينها.

المبحث الأول: النهج الأوروبي التعاوني الوطني وعبر الوطني لأمن الشبكات والمعلومات.

يتناول هذا المبحث جانبا من إستراتيجيات التعاون عبر الوطني في مجال مكافحة الإرهاب السيبراني وحماية أمن الفضاء السيبراني، حيث يتناول دور التعاون الدولي إلى جانب الدفاع الحربي للناتو في إطار سياسات الدفاع السيبراني والتعاون في مجالات عديدة أهمها تسليم المجرمين والإرهابيين الإلكترونيين، فضلا عن التعاون في مجالات التدريب على مكافحة الإرهاب بما في ذلك الإرهاب الإلكتروني.

المطلب الأول: الشراكة الأوروبية بين القطاعين العام والخاص بشأن الأمن السيبراني.

يعّرف مكتب العمل الدولي الشراكة بأنها "علاقة طوعية وتعاونية بين هيئات فاعلة مختلفة في القطاعين العام (الحكومي) والخاص (غير الحكومي)، يوافق فيها كل المشاركين على العمل جنبا إلى جنب لتحقيق هدف مشترك أو للقيام بمهام معينة"[1].

إن "المقاربات المتعددة الفواعل في مجال الفضاء السيبراني والأمن السيبراني، تسمى بالشراكة عام–خاص (PPP)، تلعب دورا هاما لضمان حوكمة الأمن السيبراني"[2]. ويكون ذلك من خلال استعانةالمؤسسات العسكرية بالقطاع الخاص لغرض تنفيذ بعض المهام، كما تفعل الولايات المتحدة الأمريكية، وأيضا لتوفير الموارد والأجهزة وبناء نُظم أمنية متكاملة[3].فحماية الفضاء السيبراني والبنية التحتية للمعلومات يشترك في مسؤوليتها القطاع الحكومي والقطاع الخاص، فهذا يضمن المرونة وقدرة الردع لتهديدات المجال السيبراني[4]. ويتضمن مفهوم الشراكة partenariat معايير الثقة والعمل الجماعي والتشاور والتفاعل وتبادل المعلومات والخبرات المتاحة، ووضع إستراتيجية أو خطة عمل مدروسة لمواجهة تهديدات الفضاء السيبراني، بالإضافة إلى عملية تحسيس المواطن بمخاطر هذه التهديدات.

---

[1] مكتب العمل الدولي، لجنة التعاون التقني، ***وثيقة رقم GB.301/TC/1*** (جنيف، مارس 2008)، ص01.

[2] Le Centre pour la Gouvernance du Secteur de Sécurité, ***Op.cit,*** p.93.

[3] إيهاب خليفة، ***مرجع سابق***، ص56.

[4] الاتحاد الدولي للاتصالات، لجنة الدراسات، المسألة 22/1، ***تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني*** (د.س.ن)، ص.10.

اهتم الاتحاد الأوروبي بدفع عجلة الشراكة بين القطاعين العام والخاص في مجال مرونة الفضاء السيبراني[1]، فقد تم إنشاء الشراكة الأوروبية بينهما منأجلالمرونة (EP3R) في مارس 2009، واستمر العمل بها إلى غاية 2013، بهدف تفعيل التعاون في مجال الاتصالات، وأتى ذلك بعد أن كشف مسح أوّلي لحماية بنية المعلومات الحرجة (CIIP) في الاتحاد الأوروبي أن البنية التحتية للمعلومات الحيوية كانت مجزأة جغرافيًا نظرا للمنافسة بين شركات الاتصالات، وخاصة لأن التهديدات السيبرانية باتت تُطرح بقوة على أجندة الأمن الأوروبي في ظل انتشار هجمات سيبرانية وهواجس تخص الإرهاب الإلكتروني، وتَمثل الهدف من هذه الشراكة في[2]:

- تبادل المعلومات بين القطاع العام والقطاع الخاص، والعمل على تثمين الممارسات الجيدة.
- مناقشة كل ما يخص أولويات السياسة العامة والأهداف المتوخّاة.
- تحديد متطلبات المرونة والحوكمة في المجال السيبراني الأوروبي.

يحظى القطاع العام في الاتحاد الأوروبي، من حيث تدخله في مجال حماية الأمن السيبراني، بأهمية كبيرة، ولكن هذا لا يعني أن القطاع الحكومي خال من السلبيات في مجال إدارة الأمن السيبراني الأوروبي، ويكفي أن تكون البيروقراطية واحدة من أهم عيوبه، إلى جانب نقص الخبرة التقنية في المجال السيبراني.

ولأن جميع التقنيات المتعلقة بالمجال السيبراني يتم إنتاجها من قبل شركات خاصة، أصبح القطاع الخاص في أوروبا أكثر أهمية من أي وقت مضى بوصفه فاعلًا أساسيا في حوكمةا لأمن السيبراني، حيث يعد أيضا مصدر إلهام للممارسات الجيدة والخبرة التقنية والابتكار، ولهذا تم إنشاء أربع فئات من الشركات الخاصة: شركات البرمجيات، شركات الأجهزة، مُوفّرو خدمات الإنترنت، وأصحاب ومُصنّع والبنية التحتية الحيوية[3].

[1] Tin Hojsgaard Munk, ***Op.cit***, p.156.
[2] Mario Nicolas Castellon Machado, ***Op.cit***, p-p: 83-84.
[3] ***Ibid***, p.92.

يتميز القطاع الخاص بانفتاحه في حين يكون القطاع العمومي أكثر صرامة وهرمية في العادة، لهذا يُنظر إلى العلاقة بين القطاعين في سياق حوكمة الأمن الأوروبي من منطلَق تجاوُز "أشكال التعاون التقليدية" والانخراط بصورة أكبر في "حوكمة الشبكة"[1].

ويتوقف نجاح الشركة بين القطاعين العام والخاص على ثلاثة عناصر هي[2]:

- وضوح القيمة التي ستتحقق من خلال الشراكة بالنسبة لأصحاب المصلحة جميعهم.
- وضوح الأدوار والمسؤوليات لدى أطراف الشراكة.
- عنصر الثقة، وهو ما ينعكس بشكل جيد على تبادل المعلومات في إطار الشراكة.

ومن أكثر المجالات التي يمكن للقطاعين الحكومي والخاص التعاون في إطارها الاستجابةُ لحوادث الكمبيوتر، تبادل المعلومات وتنسيق أُطر التعاون فيما بينهما[3].فضلا عن ذاك فإن الشراكة عامّ–خاص تثبت أهميتها في السياق الأوروبي في مجال تشجيع قدرة التنافس والابتكار في مجال الأمن السيبرانيوضمان الإمداد المستمر لمنتجات وخدمات الأمن السيبراني المبتكرة بدول الاتحاد الأوروبي[4]. ومع استمرار القطاعين العام والخاص في تقديم السلع والخدمات عبر الفضاء الرقمي، سيستمر المجال السيبراني في التوسع ليصبح أكثر ارتباطًا بضرورات الحوكمة[5].

وفي تقرير يتعلق بالشفافية صدر في 2017 عن وحدة التبليغ عن المحتوى في الانترنت (IRU) بالاتحاد الأوروبي، جاء أن "التعاون مع القطاع الخاص يلعب دورا أساسيا في مجال الوقاية"[6].

---

[1] Grzegorz Abgarowicz and Others, ***Critical Infrastructure Security– the ICT Dimension*** (Joanna Świątkowska Editor), (Poland: The Kosciuszko Institute, 2014), P.54.

[2] George Christou, ***Op.Cit***, p.49.

[3] Zurich Insurance Groupe LTD &Foundation ESADE-Center for Global Economy and Geopolitics, ***Risk Nexus: Global Cyber Governance, Preparing for New Business Risks*** (Switzerland, 2015), p.27.

[4] Nina Olesen (B), « European Public-Private Partnerships on Cybersecurity - An Instrument to Support the Fight Against Cybercrime and Cyberterrorism », B. Akhgar and B. Brewster (eds.), ***Combatting Cybercrime and Cyberterrorism, Advanced Sciences and Technologies for Security Applications***, (Switzerland : Springer International Publishing, 2016), P-p: 259- 278

[5] Mario Nicolas Castellon Machado, ***Op.cit.***, p.4.

[6] Le Centre pour la Gouvernance du Secteur de Sécurité, ***Op.cit.***, p.97.

لقد أفرزت الشراكة بين القطاعين العمومي والخاص، في ظل الرؤية الأوروبية لتهديدات الفضاء السيبراني وباسم الشراكة من أجل المرونة (EP3R)، منصة قابلة للتطبيق وبحاجة إلى تحديث دائم، فضلا عن تمارين المحاكاة للتهديدات السيبرانية، والتي تعد ذات أهمية واسعة في إطار هذه الشراكة من أجل اختبار فاعلية التعاون بين الدول الأعضاء والقطاع الخاص داخل الاتحاد الأوروبي، وهنا يجب التذكير ببعض التمارين مثل: التمرين الأول الذي كان في 2010 وحمل عنوان: « Cyber Europe 2010 »، والتمرين الثاني في أكتوبر 2012 بعنوان: « Cyber Europe 2012 »، بالإضافة إلى التمرين المشترك بين الولايات المتحدة الأمريكية والاتحاد الأوروبي في نوفمبر 2011 بعنوان[1]: « Cyber Atlantic 2011 ».

ويحدد دليل الحكامة الجيدة للأمن السيبراني، الصادر في 2019 عن مركز حوكمة قطاع الأمن بجنيف (سويسرا)، أربعة أنماط للشراكة بين القطاعين العمومي والخاص في مجال الأمن السيبراني وهي[2]:

- **أولا:** شراكة مؤسساتية يحددها القانون، تعنى بالاستجابة لمتطلبات حماية البنى التحتية الحرجة.
- **ثانيا:** شراكة تتعلق بتحقيق أهداف محددة، تعنى بالتأسيس لثقافة سيبرانية عبر منصة رقمية أو مركز خاص لهذا الغرض، مع تعزيز العمل الجيد.
- **ثالثا:** شراكة تحددها الاستعانة بخدمات خارجية في حال عجز الدولة عن تلبية حاجات القطاع الخاص، وهذا له دور أيضا في وضع سياسات دقيقة تخص الأمن السيبراني.
- **رابعا:** الشراكة الهجينة (Les PPP Hybrides): تتولى حشد فرق التدخل في حالة الطوارئ، المتصلة بأمن المعلومات، وتعتمد عليها الدولة في تزويد الإدارات أو البلد كله بخدمات هذه الفرق.

وعموما، يمكن تلخيص أهمية ودور الشراكة بين القطاعين العمومي والخاص في تعزيز الأمن السيبراني من خلال النقاط الآتي ذكرها[3]:

- رفع مستوى التحسيس بتحديات وتهديدات الأمن السيبراني بالنسبة لدول الاتحاد الأوروبي.

---

[1] Commission Européenne, ***Op.cit.***, p.7

[2] Le Centre pour la Gouvernance du Secteur de Sécurité***, Op.cit.***, p-p : 94-95.

[3] Le Centre pour la Gouvernance du Secteur de Sécurité***, Op.cit***, p.94.

- تعزيز المهارات السيبرانية على الصعيد الوطني بتحفيز روح المبادرة.
- توفير الموارد المالية والتقنية للمتخصصين في ميدان الأمن الإلكتروني.
- دعم البحث العلمي في مجال الأمن السيبراني.
- تدعيم الوقاية من الجريمة وتحديدا ذات الصفة السيبرانية.

المطلب الثاني: التعاون الدولي وثقافة الأمن السيبراني المتعدد المستويات.

أصبح التعاون في المسائل الجنائية والتحقيقات أمرا يفوق الضرورة، وهذا لأن نوعية التهديدات والجرائم قد تغيرت بشكل كبير، فهي اليوم لادولاتية وعابرة للحدود الوطنية التقليدية، مما يجعل مسألة التعاون ملحة[1].

وقد كان فريق عمل الخبراء الحكوميين بمنظمة الأمم المتحدة قد أصدر تقريرا في 2015 يحدد في ثناياه معايير (هي توصيات أيضا) لجعل الفضاء الإلكتروني مفتوحا، آمنا ومستقرا، وتتمثل هذه المعايير فيما يأتي[2]:

- ضرورة التعاون بين الدول لتعزيز أمن واستقرار استخدام تكنولوجيا المعلومات والاتصالات.
- ضرورة مراجعة المعلومات ذات الصلة بتكنولوجيا المعلومات والاتصالات.
- اتخاذ الإجراءات اللازمة لحماية البنى التحتية الحرجة من التهديدات السيبرانية.
- اتخاذ تدابير الوقاية من التقنيات والبرامج الضارة.
- تشجيع آليات التبليغ ومشاركة المعلومات الهامة ذات الصلة.
- التزام الدول بعدم دعم أو التورط في أنشطة عدوانية تتخذ من تكنولوجيا المعلومات والاتصالات وسيلة وهدفا لها.

---

[1] مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC)، ***دليل التعاون الدولي في المسائل الجنائية لمكافحة الإرهاب*** (فيينا، 2009)، ص.02.

[2] Le Centre pour la Gouvernance du Secteur de Sécurité, ***Op.cit.,*** p.46.

يتعاون الاتحاد الأوروبي مع المنظمات والهيئات الدولية بما في ذلك الأمم المتحدة، والمنتدى العالمي لمكافحة الإرهاب، ومجلسأوروبا (CoE)، ويعمل بنشاط في إطار إستراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب (2006) وقرارات مجلس الأمن الدولي ذات الصلة بمكافحة الإرهاب والإرهاب الإلكتروني.وكمثال، ففي عام 2018 صدّق الاتحاد الأوروبي على اتفاقية مجلس أوروبا وبروتوكولها الإضافييبشأن منع الإرهاب، وتهدف الاتفاقية إلى تعزيز مكافحة الإرهاب في إطار احترام حقوق الإنسان[1].

وقد أصدرت منظمة الأمم المتحدة جملة من القرارات مثل: القرار 63/55 الصادر بتاريخ: 4 ديسمبر 2000، القرار 121/56 الصادر بتاريخ: 19 ديسمبر 2001، والمتعلق بمكافحة الجريمة السيبرانية والاستخدام السيء وغير المشروع لتكنولوجيا المعلومات والاتصالات، القرار 60/177 لعام 2005 والذي يخص التعاون في هذا السياق، القرار 64/211 لعام 2010 والذي يدعو الدول لتحديث تشريعاتها المتعلقة بالجريمة الإلكترونية، بالإضافة إلى منتدى القمة العالمية لمجتمع المعلومات حيث يتم التأكيد على بناء الثقة والأمن في الفضاء السيبراني[2]. يضاف إلى ذلك القرار 1624 (2005) والقرار 1822 (2008) الذي يشجع التعاون الدولي لصد الإرهاب عن استغلال تكنولوجيا المعلومات والاتصالات، والقرار 1963 (2010) الذي تناول زيادة توظيف الانترنت في النشاط الإرهابي بغرض التجنيد والتحريض، والقرار 2255 (2015) الذي تناول أيضا توظيف الانترنت في النشاط الإرهابي بغرض التجنيد والدعم والتحريض والتمويل[3].

لقد عملت الأمم المتحدة على تحديث القوانين وتعزيز تدابير الأمن بصورة لا تمس حقوق الإنسان الأساسية، والتكريس للتعاون الدولي والتعاون بين المنظمات المعنية بالأمن السيبراني، وأتى القرار رقم 2255 لعام 2015 شاملا لأساليب استخدام الانترنت لأغراض إرهابية، ومن ضمنها التسهيل والتحريض والتجنيد والتمويل[4]. وفي 2010 أشار مجلس الأمن الدولي إلى الاستخدام المتنامي للانترنت من قبَل

---

[1] Sofija Voronova, ***Op.cit***, p.8.

[2] اللجنة الاقتصادية والاجتماعية لغربي آسيا، ***مرجع سابق***، ص.09.

[3] خالد حسن أحمد لطفي، ***مرجع سابق***، ص.171.

[4] عبد الجليل إسماعيل حسن الشيخ زيني، ***مرجع سابق***، ص: 248، 251.

الإرهابيين "لأغراض التوظيف والتحريض والتمويل والتخطيط والتحضير" لأعمالهم[1].وفي الوقت الحالي، يجب أن يركز مجلس الأمن أيضا على تهديد الإرهاب السيبراني، كما يمكن للدول إنشاء "تجمع استخباراتي" ضد الإرهاب السيبراني تحت رعاية منظمة الأمم المتحدة، وذلك بالتوازي مع اتباع نهج شامل لردع الهجمات السيبرانية استنادا إلى القانون الدولي والأعراف الدولية لأن الدول "تشترك في المصلحة في تبني أو تقنين معايير مشتركة لتسيير المعاملات الدولية ... أو في تعزيز أو حظر أنواع معينة من السلوك من قبل الدول"، وبالتالي ضرورة توحيد الإطار المحدد لاستخدام الدول لقدراتها السيبرانية[2].

وتكون حماية البيانات من خلال تشفيرها وإنشاء نظام متكامل لتأمينها من خلال إتاحة برامج محاربة الفيروسات والبرامج الضارة، وعدم السماح بجعل المعلومات الأمنية الحساسة ذات مصدر مفتوح، فمن المفروض أن يتم تقييد مشاركتها بين الجهات المختصة حمايةً لها ولمنع استغلالها من قبَل جماعات الإرهاب الإلكتروني، وكانت اتفاقية مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، الصادرة عن الأمم المتحدة، قد تطرقت إلى أنه "ينبغي للنظم القانونية أن تحمي سرية البيانات ونظم الحواسيب وسلامتها وتوافرها، من أي عرقلة غير مأذون بها، وأن تضمن معاقبة من يقوم بإساءة استعمالها لأغراض إجرامية"[3].

وتظل اتفاقية بودابست مبادرة رائدة لتنسيق الجهود ودعم إمكانيات الدول، والتعاون المثمر في مجال التصدي للجرائم السيبرانية، وقد احتوت على ثلاثة أقسام كما يلي: القواعد الموضوعية للجرائم، إجراءات التحقيق وآليات التعاون الدولي[4]. ولا ينفصل تطبيق اتفاقية مجلس أوروبا بشأن الجريمة الإلكترونية عن تطبيق الصكوك القانونية المتصلة بمكافحة الإرهاب، وهذا يندرج ضمن "توفير الأساس القانوني للتعاون

---

[1]United Nations Office on Drugs and Crime (UNDOC), United Nations Counter-Terrorism Implementation Task Force, ***The Use of The Internet for Terrorist Purposes*** (UNO: New York, September 2012), P-p: 17, 74.

[2] Murat Dogrul, and Others, « Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism », in: ***3rd International Conference on Cyber Conflict***, C. Czosseck, E. Tyugu, T. Wingfield (Eds.), (Tallinn, Estonia, 2011).

[3] عبد الجليل إسماعيل حسن الشيخ زيني، ***مرجع سابق***، ص: 234، 238.

[4] اللجنة الاقتصادية والاجتماعية لغربي آسيا، ***مرجع سابق***، ص11.

ضد استخدام الإنترنت لأغراض إرهابية"[1]. كما تعنى منظمة الأمن والتعاون في أوروبا (OSCE) بتحديات الأمن السيبراني ومن ضمنها الإرهاب الإلكتروني. ففي 2004 أقرّ المجلس الوزاري الأوروبي التصدي لاستخدام الإنترنت من قبل الإرهابيين في أغراض الدعاية والتجنيد، ومراقبة تحركات الجماعات الإرهابية، وتبادل المعلومات بين حكومات منظمة الأمن والتعاون الأوروبية[2].

- **الحوار الاستراتيجي في مجال الأمن السيبراني:**

يهتم الاتحاد الأوروبي بإجراء حوارات إستراتيجية تخص قضايا الأمن السيبراني والإرهاب الإلكتروني، وهو ما يظهره الجدول الاتي.

الشكل (16): نماذج من الحوار السيبراني للاتحاد الأوروبي مع شركائه الاستراتيجيين.

البلد	مضمون الحوار الاستراتيجي
البرازيل	السياسة السيبرانية الدولية، حوار مجتمع المعلومات
كندا	لقاء خبراء من الاتحاد الأوروبي وكندا والولايات المتحدة حول حماية البنية التحتية
الصين	فريق العمل السيبراني، حوار حول تكنولوجيا المعلومات والاتصالات
الهند	حوار سياسي حول الأمن السيبراني، حوار مجتمع المعلومات
اليابان	حوار سيبراني، حوار حول تكنولوجيا المعلومات والاتصالات
المكسيك	فريق يعنى بالاتصالات، حوار حول الأمن العام وإنفاذ القانون
روسيا	حوار مجتمع المعلومات
جنوب إفريقيا	حوار مجتمع المعلومات
كوريا الجنوبية	حوار سيبراني، حوار مجتمع المعلومات
الولايات المتحدة الأمريكية	مجموعة العمل المعنية بالأمن السيبراني والجريمة السيبرانية (WGCC)، حوار سيبراني، حوار مجتمع المعلومات، لقاء خبراء من الاتحاد الأوروبي وكندا والولايات المتحدة بشأن حماية البنية التحتية الحرجة

المصدر: Thomas Renard, EU Cyber Partnership: Assessing the EU Cyber Strategic Partnerships with Third Countries in the Cyber Domain, ***European Politics and Society***, 19(3), (January 2018), P-p: 1-19.

[1] UNDOC, ***Op.cit***, p.21.

[2] Mitko Bogdanoski, Drage Petreski, ***Op.cit,*** p.68.

يتضمن الشكل أهم الشركاء الاستراتيجيين بالنسبة للاتحاد الأوروبي على الصعيد السيبراني، بمعنى أن الاتحاد الأوروبي يهتم بتحقيق قيمة مضافة مع هؤلاء على صعيد التعاون في مجال الأمن السيبراني ومحاربة الإرهاب الإلكتروني، مع أن الاثار تظل متفاوتة بالاعتماد أولا على عامل الثقة بين الطرفين، ففي حالة الحوار الاستراتيجي مع روسيا والصين تبقى الأمور غير واضحة خاصة وأن الاتحاد الأوروبي ينظر إلى هاذين البلدين كطرف يهدد أمن الفضاء السيبراني في أوروبا، والدليل اتهام روسيا مع كل هجوم سيبراني تتعرض له دولة أوروبية من داخل أو خارج الاتحاد.

بالإضافة إلى أن التعاون مع روسيا (وهي عضو في مجلس أوروبا) ركز في البداية على "استخدام الانترنت من قبَل الجماعات الإرهابية وتوسع تدريجيا ليشمل الجرام الإلكترونية"، وقد حظي ملف الإرهاب السيبراني باهتمام واسع خاصة مع مشاركة روسيا في مبادرة "التحقق من الشبكة" (Check the Web) التي أطلقها اليوروبول، ولكن تبقى مسألة عدم الثقة عاملا مؤثرا يُضعف هذا السياق التعاوني، دون نسيان تأثير الأزمة الأوكرانية في طبيعة العلاقات بين الاتحاد الأوروبي وروسيا[1].

- **التعاون مع الولايات المتحدة وحلف الناتو:**

أدرج الاتحاد الأوروبي منذ 2001 فقرات مكافحة الإرهاب في الاتفاقيات الثنائية والمتعددة الأطراف التي تخص الشراكة والتعاون، كما أبرم اتفاقيات قطاعية مع أطراف دولية خارج الاتحاد الأوروبي تخص التعاون الشرَطي والقضائي (اتفاقيات المساعدة القانونية المتبادلة وتسليم المجرمين، اتفاقيات تسجيل أسماء الركاب (PNR) ، اتفاقيات التعاون بين اليوروبول والمحكمة الأوروبية)، وفي عام 2010 أبرم الاتحاد الأوروبي اتفاقية برنامج تتبُّع تمويل الإرهاب (TFTP) مع الولايات المتحدة، من أجل تبادل المعلومات ودعم عمل أجهزة إنفاذ القانون،كما يزود الاتحاد الأوروبي بعض الدول بمساعداتفنية وتدريبية تمس دعم بناء القدرات في مجال مكافحة الإرهاب التقليدي والإرهاب السيبراني[2].

[1] Thomas Renard***, Op.Cit.,*** p.10.
[2] Sofija Voronova, ***Op. Cit,*** P.8.

وكانت قمة لشبونة (نوفمبر 2010) بين الاتحاد الأوروبي والولايات المتحدة الأمريكية لغرض "تعزيز أنشطة الأمن السيبراني والجريمة السيبرانية والمساهمة في مواجهة تهديدات الأمن السيبراني العالمية"، وتضمن التعاون بين الطرفين أربعة مجالات هي: إدارة الحوادث السيبرانية، الشراكة عام–خاص، التوعية، الجريمة الإلكترونية، وفي إطار التعاون جرى تمرين Cyber Atlantic في نوفمبر 2011 بهدف اختبار القيمة المحققة من وراء هذا التعاون، ثم نُظم الحوار السيبراني بين الاتحاد الأوروبي والولايات المتحدة في 2014 لتعزيز تبادل المعلومات والخبرات والتصدي الجيد للتهديدات السيبرانية وبناء القدرات[1]. خلال قمة الناتو في وارسو بتاريخ: 8 جويلية 2016، جرى التأكيد على أهمية تمتين أواصر التعاون بين الاتحاد الأوروبي والناتو في مجالات الدفاع وتبادل المعلومات الاستخباراتية وحماية الأمن السيبراني، وقد جرى دعم تبادل المعلومات بين فرق الاستجابة لطوارئ الكمبيوتر على مستوى المنظمتين (CIRT من الجانب الأوروبي وNCIRC بالنسبة للناتو)[2].وتتمثل أهمية تفعيل التعاون بين الاتحاد الأوروبي وحلف الناتو في كون ذلك يعزز تكامل الأدوار والمسؤوليات ومرونة الأمن، وبالتالي مرونة الأمن والدفاع في الفضاء السيبراني، خاصة مع تداخل عضوية الدول على مستوى الطرفين (أي الاتحاد الأوروبي والناتو)[3].

- **برامج الاتحاد الدولي للاتصالات (ITU):**

تم إنشاء الاتحاد الدولي للاتصالات في 1865 تحت اسم اتحاد التلغراف الدولي، قبل أن يتم تغيير الاسم في 1947 وينضم إلى الأمم المتحدة، وهو يضم إلى جانب الدول أكثر من 700 مؤسسة من القطاع الخاص والجهات الأكاديمية، ويعمل على تنسيق الاستراتيجيات الوطنية للدول في مجال الأمن السيبراني وتشجيع التعاون الدولي وبين القطاعات المختلفة، ويهدف إلى حماية البنية التحتية للمعلومات ودعم بناء القدرات بالنسبة للدول النامية، ويهتم الاتحاد الدولي للاتصالات بعنصر الثقة في استخدام تكنولوجيا

[1] George Christou, ***Op.Cit,*** p-p : 163-167.
[2] European Union Institute for Security Studies, ***EUISS Yearbook of European Security*** (Y.E.S 2017), P-p: 27-28.
[3] George Christou, ***Op.cit.,*** p.54.

المعلومات والاتصالات، كما يتعاون مع الوكالة الأوروبية لأمن الشبكات والمعلومات (ENISA) "بنشر خريطة الطريق المتعلقة بمعايير الأمن في مجال التكنولوجيا المعلوماتية والاتصالات[1].

أطلق رئيس الاتحاد الدولي للاتصالات "حمدون إ.توريه" البرنامج العالمي للأمن السيبراني في مايو 2007، ليكون بمثابة "إطار للتعاون الدولي لتعزيز الثقة والأمن في مجتمع المعلومات"، وتشمل ركائزه: تدابير قانونية، تقنية/إجرائية، تدابير تنظيمية، بناء القدرات والتعاون الدولي[2]. ثم ظهر بعد هذه الأجندة الدليل الوطني للأمن السيبراني الذي وضعه الاتحاد الدولي للاتصالات في 2011، حيث " يركز على القيم والثقافة والاهتمامات الوطنية بكونها الركيزة الأساسية لإعداد إستراتيجية وطنية فعالة"، وفي 2015 وُضع مؤشر الأمن السيبراني العالمي (GCI) ومن خلاله يجري قياس مستوى الأمن السيبراني لدول العالم انطلاقا من الركائز الخمس المذكورة[3].

ويهتم برنامج الأمن السيبراني العالمي الذي وضعه الاتحاد الدولي للاتصالات بالتعاطي مع الرهانات المتنوعة التي تواجه الأمن السيبراني، بما فيها التقني– السياسي والرهان القانوني– التشريعي، فمن الناحية القانونية يتم استهداف احتواء الثغرات في التشريعات الوطنية والعمل على وضع نموذج تشريعي صالح للتطبيق على الصعيد العالمي، وتنظيميا يسعى البرنامج إلى إقامة هياكل تصد الهجمات السيبرانية على غرار CERT/CIRT والشراكة الدولية المتعددة الأطراف لمواجهة التهديدات السيبرانية(IMPACT)، أما من الناحية التقنية والإجرائية فيتم استهداف "معالجة مواطن الضعف في المنتجات البرمجية التي ترمي إلى استحداث خطط الاعتماد والبروتوكولات والمعايير المقبولة عالميا"، وبالنسبة لبناء القدرات يهدف البرنامج

---

[1] عبد الجليل إسماعيل حسن الشيخ زيني، ***مرجع سابق***، ص : 255–259.

[2] حمدون إ.توريه، ***البحث عن السلام السيبراني*** (الاتحاد الدولي للاتصالات، يناير 2011)، ص: 39.

[3] ميليسا هاثاواي، "إدارة الخطر السيبراني الوطني"، https://potomacinstitute.org/images/CRI/Managing-National-Cyber-Risks_FINAL-Arabic.pdf (2021.12.11)، ص: 5-6.

إلى تطوير الخبرة والمعرفة والثقافة السيبرانية، للوصول في النهاية إلى ثقافة سيبرانية مستدامة واستباقية[1]. يمكن شرح ذلك فيما يأتي[2]:

- إجراءات تقنية:

تتمثل في فرق تدخل وطنية خاصة بحالة وقوع هجمات سيبرانية، فهي وحدات منظمة تتدخل في حدود مهامها، بالإضافة إلى وحدات تدخل قطاعية Sectorielles تتعلق بحالة وقوع حوادث سيبرانية تمس أمن المعلومات في قطاع ما، وخاصة القطاعات الهامة كالصحة والخدمات العمومية والمالية وغيرها.

- إجراءات تخص الجانب القانوني والبنية التنظيمية:

تكون في إطار الإستراتيجية الوطنية للأمن السيبراني التي تعد ضرورة تقع ضمن أولويات الحكومات في الوقت الراهن، لأن وجودَإستراتيجية وطنية ذكية كفيلٌ بحماية أمن الدولة والمجتمع والتصدي لكل تهديد من شأنه إلحاق الضرر بالمصلحة الوطنية والعامة والبنى التحتية كما هو شأن الإرهاب الإلكتروني. ويعد تجميع المؤشرات ذات الصلة بالأمن السيبراني مهما لتحليل وتقييم المخاطر الراهنة والمحتملة.

- إجراءات ذات صلة بتعزيز القدرات:

وتشمل تحسيس المواطنين بالخطر السيبراني، تقديم برامج بحثية والاستفادة من الخبراء في مجال الأمن السيبراني.

- الإجراءات ذات الصلة بالتعاون الدولي:

تتمثل في الاتفاقيات الثنائية الأطراف، المشاركة في المنتديات الدولية، الاتفاقيات المتعددة الأطراف، وأيضا الشراكة بين القطاعين العمومي والخاص لما تحظى به من أهمية في تعزيز حماية الفضاء الإلكتروني

[1] حمدون إ.توريه، ص: 97–100.

[2] ITU, ***Programme de Cyber Sécurité, Groupe d'experts chargé de la pondération de l'indice GCI*** (Aout 2020), P-p : 9-12.

ومواجهة التهديدات على غرار الإرهاب السيبراني. يضاف إلى ذلك الشراكة الداخلية بين المنظمات لغرض تعزيز الموارد وتبادل المعلومات.

- **الاتحاد الأوروبي والانتربول:**

تم إنشاء المنظمة الدولية للشرطة الجنائية (الانتربول) في 1923، وهي تهدف إلى التعاون بين الدول في مكافحة الجرائم والإرهاب الإلكتروني، وذلك من خلال تجميع وتبادل المعلومات[1]. وهي منظمة تعمل على "تأمين وتنمية التعاون المتبادل على أوسع نطاق بين كل سلطات الشرطة الجنائية، في إطار القوانين القائمة في مختلف البلدان وبروح الإعلان العالمي لحقوق الإنسان"، وكان قرار مجلس الأمن 1617 لعام 2005 قد دعا الدول إلى العمل في إطار الانتربول فيما يتعلق ببيانات الأشخاص ووثائق السفر، فتبادل المعلومات بين المكاتب الشرطية يكون عبر الأنتربول لأنها منظمة يؤطرها القانون الدولي العام لتقوم على مبدأ تعاون الأعضاء، فضلا عن الإطار القانوني لذلك . يشكل الانتربول إذًا شريكا أساسيا بالنسبة للاتحاد الأوروبي في مجال مكافحة الإرهاب، ويستفيد الاتحاد الأوروبي من بيانات الانتربول ومن برامجه في مجال التدريب وبناء القدرات[2]. ونتيجة مسح أجراه على 194 دولة، رصد الانتربول خلال الفترة: يناير– ابريل 2020 ما يعادل 907 الاف رسالة إلكترونية غير مرغوبه بها، و737 حادث سيبراني[3].

ويظل تبادل المعلومات بخصوص الإرهابيين محطة مهمة، ويتضمن ذلك "تقديم المعلومات والبيانات والوثائق والمواد الاستدلالية التي تطلبها سلطة قضائية أجنبية، وهي بشأن النظر في جريمة ما عن الاتهامات التي وجهت إلى رعاياها في الخارج والإجراءات التي اتخذت ضدهم، وقد يشمل التبادل في المعلومات السوابق القضائية للجناة"[4].

---

[1] عبد الجليل إسماعيل حسن الشيخ زيني، ***مرجع سابق***، ص216.

[2] "الانتربول والاتحاد الأوروبي"، https://interpol.int/ar/5/3/2 (2021/10/15)

[3] جاسم محمد واخرون، الإرهاب والتطرف في أوروبا من الداخل، ***مرجع سابق***، ص 564.

[4] عبد الجليل إسماعيل حسن الشيخ زيني، ***مرجع سابق***، ص220.

وبالعودة إلى مرتكزات مدرسة باريس، يمكن تنظيم عملية المراقبة الشرَطية لتتبع الجماعات المتطرفة والإرهابية واحتواء الخطر الإرهابي الناشئ –انطلاقا من الانترنت– داخل المجتمعات المحلية أولا، وحسب "جانزوسكي" Janczewski فإن أساليب الدفاع قد لا تكون كفيلة دوما بصد التهديدات، لذا يبقى التعاون ضروريا، ويشمل التعاون الدولي ما يلي[1]:

– الأطراف التي لها أنظمة متشابه وتواجه التهديدات نفسها، فالتعاون بين مزودي خدمة الإنترنت (ISP) للتصدي لهجمات توزيع الخدمة يكون أكثر فاعلية لإيجاد الحلول.

– التنسيق في القوانين الوطنية بشكل يتكامل مع القوانين الدولية، حيث إن حظر عمليات القرصنة مثلا في كل دولة سيؤدي حتما إلى تراجع التهديد المرتبط بهذا النوع من الهجمات الإلكترونية.

ويندرج في سياق ما تناولته مدرسة باريس تنسيق الدول الأوروبية فيما يتعلق بالسجلات الجنائية للمواطنين من خارج الاتحاد الأوروبي، وهو ما يمكن اعتباره مكملاً لنظام معلومات السجلات الجنائية الأوروبية اللامركزية (ECRIS) لمواطني الاتحاد الأوروبي. بالإضافة إلى توفير نقطة اتصال خاصة بتتبع المقاتلين الإرهابيين الأجانب، بمعنى مراقبة تحركاتهم وتنقلاتهم داخل الاتحاد في حال عودتهم إلى بلدانهم الأصلية، وهي عملية تحتاج إلى تنسيق وتعاون أكبر بين أعضاء الاتحاد الأوروبي.

وترى النظرية الليبرالية أن التعاون الدولي مهم جدا لمواجهة الهجمات السيبرانية، فالحكومات بمفردها لا تكون قادرة على ذلك، كما تؤكد الليبرالية الجديدة على إنشاء مؤسسات دولية لمواجهة هذا التهديد. "من الناحية النظرية، سيكشف كل عضو عن قدراته، ويقدم أساليب للأعضاء لتحديد نشاطهم السيبراني، وتبادل التقنيات الدفاعية المتقدمة، وتعزيز الثقة وخلق الشفافية"، ولكن هذا يصطدم واقعيا بضرورة مشاركة المعلومات فيما بين الدول، وهو الأمر الذي يثير حفيظة البعض ويرفضه البعض الاخر باعتبار أن المعلومات المراد مشاركتُها قد تكون حساسة وخطيرة[2].

---

[1] Murat Dogrul, and Others, ***Op.cit.***

[2] إبراهيم بولمكاحل، ***مرجع سابق***، ص155.

لقد شكّلت الهجمات الإرهابية في باريس (نوفمبر 2015) نقطة تحوُّل في السياسات الأوروبية لمكافحة الإرهاب، مما كثّف التعاون بين أجهزة الشرطة والاستخبارات داخل الاتحاد الأوروبي، كما عمل الاتحاد الأوروبي على تعزيز تدابير مراقبة الحدود عبر 'قواعد البيانات البيومترية".

- **التعاون الدولي في مجال تسليم المجرمين والإرهابيين الإلكترونيين:**

تُعرّف عملية تسليم المجرمين كما يلي: "تسليم المجرمين هو أن تسلم دولة (الدولة المطلوب منها التسليم) شخصا يوجد في إقليمها إلى دولة أخرى (الدولة الطالبة) تبحث عن ذلك الشخص إما بهدف ملاحقته أو بهدف تسليط العقوبة التي حكَمت بها عليه محاكمُها"[1].

ولم يكن تسليم المجرمين بين الدول ملزما، وذلك قبل أن تظهر اتفاقات تنظم هذه العملية على الصعيد الدولي وتلزم الدول بالتعاون في مجال تسليم المجرمين، مثال ذلك اتفاقية البلدان الأمريكية لتسليم المجرمين (1981)، والاتفاقية الأوروبية لسنة 1957 ثم بروتوكولها الإضافي (1958 و1975)، إضافة إلى اتفاقية "تبسيط" إجراءات التسليم بين أعضاء الاتحاد الأوروبي، ويعد التعاون بخصوص ملاحقة وتسليم الإرهابيين الإلكترونيين ضروريا جدا لأنه يشكل حصانة من الإرهاب السيبراني، وقد تم إقرار الاعتراف المتبادل في إطار التعاون القضائي في المسائل الجنائية داخل الاتحاد الأوروبي، معنى ذلك أن "ينفذ مبدأ الاعتراف المتبادل بالقرارات القضائية التي تصدرها أجهزة العدالة الجنائية لدى الدول الأعضاء في الاتحاد"[2].

وفي مجال تسليم المجرمين بما فيهم الإرهابيون، يؤطّر القانون الدولي إجراءات التحقيق والتسليم والعدالة الجنائية، ويرتبط تجريم العمل الإرهابي بأربعة أُطُر هي: قرارات مجلس الأمن الدولي ذات الصلة، الصكوك العالمية، الصكوك الإقليمية والقوانين الوطنية[3]. تلتزم الدول بعدد من التدابير مثل ملاحقة وتسليم الجرمين، بسط الولاية القضائية لملاحقة مرتكبي الفعل الإرهابي، تسليم الإرهابي إلى العدالة، احترام سيادة

---

[1] مكتب الأمم المتحدة المعني بالمخدرات والجريمة، ***مرجع سابق***، ص: 201

[2] عبد الجليل إسماعيل حسن الشيخ زيني، ***مرجع سابق***، ص : 222-223.

[3] مكتب الأمم المتحدة المعني بالمخدرات والجريمة، ***مرجع سابق***، ص : 3-6.

القانون والتجريم المزدوج للوقائع، وعدم استخدام المعلومات المتاحة في إطار التعاون الدولي لغرض مختلف أو غير مشروع[1].

لقد كانت أحداث 11 سبتمبر 2001، ثم هجمات مدريد ولندن (2004 و2005 على التوالي) حدثا فاصلا في تعزيز الاتحاد الأوروبي لسياساته المتعلقة بمكافحة الظاهرة الإرهابية، من خلال تعزيز "التعاون القضائي، التعاون بين أجهزة الشرطة، سلامة وسائل النقل، مراقبة الحدود وتأمين الوثائق، مكافحة التمويل، الحوار السياسي والعلاقات الخارجية، والدفاع ضد هجمات الأسلحة البيولوجية والكيميائية والمشعّة والنووية"[2].

وجاء في الفقرة 2 من القرار 1373 أنه على جميع الدول "تزويد كل منها الأخرى بأقصى قدر من المساعدة فيما يتصل بالتحقيقات أو الإجراءات الجنائية المتعلقة بتمويل أو دعم الأعمال الإرهابية، ويشمل ذلك المساعدة على حصول كل منها على ما لدى الأخرى من أدلة لازمة للإجراءات القانونية"[3]. بالتالي ينص هذا القرار على ضرورة تبادل المساعدات في مجال التحقيقات والإجراءات الجنائية المتصلة بدعم وتمويل الإرهاب، من خلال توفير الأدلة والمعلومات المتاحة، وبحسب القرار ذاته لا يجب التراخي في تسليم المجرمين والإرهابيين للعدالة، بحيث "تسهر الدول على... كفالة تقديم أي شخص يشارك في تمويل أعمال إرهابية أو تدبيرها أو الإعداد لها أو ارتكابها أو دعمها إلى العدالة"، كما يعد قرار مجلس الأمن رقم 1373 لعام 2001 مهما في إطار تدابير مكافحة الإرهاب الدولي، فهو يحدد إطارا للتعامل مع جريمة الإرهاب وتمويل الأعمال الإرهابية ويوصي بالتعاون في مجال مكافحة الإرهاب، كما يحظر القرار 1624 لعام 2005 التحريض على الإرهاب[4].

---

[1] ***المرجع نفسه***، ص 35-36.

[2] خالد حسن أحمد لطفي، ***الإرهاب الإلكتروني: آفة العصر الحديث، والاليات القانونية للمواجهة، ط1*** (الإسكندرية: دار الفكر الجامعي، 2018)،ص.160.

[3] مكتب الأمم المتحدة المعني بالمخدرات والجريمة، ***مرجع سابق***، ص104.

[4] ***المرجع نفسه***، ص 14-21.

وبنص المادة 24 من اتفاقية بودابست بعنوان: "تسليم المجرمين"، تُلزم الاتفاقية الدول الأطراف بالنسبة للجرائم الواردة في المواد: 2←11 "شريطة أن يعاقَب على هذه الجرائم بموجب قوانين كلا الطرفين المعنيين، بعقوبة سالبة للحرية لمدة سنة على الأقل أو بعقوبة أشد"، ولا يقتصر التسليم على الأطراف، بحيث يمكن لدولة أخرى غير طرف أن تقدم طلبا بالتسليم فتكون المعاهدة هي المرجع الذي يتم الاستناد إليه[1]. وتوصي المادة 25 بالتعاون بين الأطراف في مجال التحقيق والمتابعة، بما يتضمنه ذلك من اعتماد على الوسائط المتطورة كالفاكس والبريد الإلكتروني بحيث وصفتها الاتفاقية بـ "وسائل الاتصال العاجلة"[2]. و"فيما يتعلق بتسليم المجرمين، تتيح الصكوك الدولية ذات الصلة بمكافحة الإرهاب للدول الأطراف أن تستعم لها أسسا قانونية كافية للقبول بتسليم المجرمين"[3].

- **<u>التعاون الدولي في مجال التدريب على محاربة الإرهاب الإلكتروني:</u>**

تستلزم مكافحة الإرهاب السيبراني تدريبا معمقا في الجانب الفني والتقني، وهنا يجب أن يبرز دور التعاون بين القطاعين الحكومي والخاص، ودور وكالات إقليمية ودولية، مثل اليوروبول والانتربول، في إتاحة الفرصة لتنظيم دورات تدريبية في مجال التحقيقات الإلكترونية على سبيل المثال، ويمكن للجهات الأكاديمية أن توفر تدريبات متخصصة أيضا، كما هو الحال مع جامعة دبلن التي أنشأت مركز الأمن السيبراني في 2006، كما كانت المفوضية الأوروبية قد أشرفت في 2010 وموّلت مشروع "شبكة مراكز التميز للجرائم الإلكترونية للتدريب والبحث والتعليم"، ويتوفر مكتب الأمم المتحدة المعني بالجريمة والمخدرات منذ 2011 على منصة رقمية مختصة في التدريب على مكافحة الإرهاب، حيث تقدّم تدريبات في مجال العدالة الجنائية، كما يتم الاعتماد في العصر الحالي على مقاربة متعددة التخصصات في مكافحة الإرهاب والإرهاب السيبراني، ومثال ذلك تكامُل عمل وكالات إنفاذ القانون، جهاز الاستخبارات، ممارسي العدالة الجنائية، وغيرها [4].

---

[1] مجلس أوروبا، مجموعة المعاهدات الأوروبية (رقم 185)، ***الاتفاقية المتعلقة بالجريمة الإلكترونية- بودابست***، ص13.

[2] ***المرجع نفسه***، ص14.

[3] مكتب الأمم المتحدة المعني بالمخدرات والجريمة، ***مرجع سابق***، ص22.

[4] UNDOC, ***Op.cit.***, p : 72, 104.

ومن الضروري تطوير ادوات التدريب بما يواكب خصوصية جريم الإرهاب الإلكتروني، فلا يكفي الاستناد إلى التدبير القانونية دون خبرة تقنية تواكب هذا النوع من الجرائم وتجعل المتدرب متحكما في البرمجيات والشبكة وتحليل البيانات، لذا يجب أن يكون التدريب من مهام المتخصصين القادرين على تقديم إضافة حقيقية[1].

تبعا لذلك، يتضح أن التعاون الدولي يحتل موقعا مهما جدا من أجل تجسيد فكرة ثقافة الأمن العالمي والأمن السيبراني، ويسعى الاتحاد الأوروبي باستمرار إلى نشر هذه الثقافة إلى جانب ثقافة التعاون لمكافحة الإرهاب والإرهاب الإلكتروني.

المطلب الثالث: الدفاع الحربي لحلف شمال الأطلسي وسياسات الدفاع السيبراني.

يعمل حلف الناتو على مواكبة تحولات البيئة الإستراتيجية الأوروبية والعالمية، محافظا على مبدأ الدفاع الجماعي كركيزة له، وبالرغم من رؤية البعض القائمة على أساس أنه لا داعي لاستمرار الحلف بعد نهاية الحرب الباردة ونهاية الخطر السوفييتي، استمر الناتو بحجة عدم الاستقرار الإقليمي في أوروبا وظهور صراعات عرقية كما كان الحال في كوسوفو، مما فرض عليه التكيف مع الظرف الدولي والإقليمي الجديد ومع التهديدات الجديدة، وهو ما برز مع مفهومه الاستراتيجي نهاية القرن الماضي خلال قمة واشنطن (1999)، حيث رأى أن التهديدات المستقبلية "متعددة الاتجاهات وغالبا يصعب التنبؤ بها"، وقد نال موضوع الإرهاب اهتماما كبيرا وواضحا في سياق ذلك[2].

فالناتو كترتيب أمني موجود مسبقًا يعمل على التكيف مع عصر المعلومات، لكن للمواد التي أسس لها ميثاق الناتو (المادة الخامسة) ليست مجهزة بشكل جيد للتصدي للهجمات الإرهابية السيبرانية ودفعت إلى بذل جهود متضافرة لاستكشاف تداعيات الأمن السيبراني على التعاون المستقبلي بين الدول الأعضاء[3].

---

[1] عبد الجليل إسماعيل حسن الشيخ زيني، ***مرجع سابق***، ص: 225-228.

[2] قسم الدبلوماسية العامة (بروكسل)، وثيقة بعنوان: ***معًا من أجل الأمن.. مدخل لفهم منظمة حلف شمال الأطلسي*** (د.س.ن)، ص 5-10.

[3] Madeline Carr, ***Op.cit***.

يوفر النظر إلى الناتو بعض الأفكار حول تحديات دمج مفاهيم "الهجمات الارهابية الإلكترونية" في الترتيبات الأمنية العسكرية التقليدية عبر عدة آليات وميكانيزمات أبرزها:

أ– إدراج الدفاع السيبراني في إستراتيجية حلف شمال الأطلسي:

أصبح الدفاع السيبراني اليوم جزءا من مهمة الناتو الأساسية للدفاع الجماعي، ويركز الناتو في مجال الدفاع السيبراني على حماية شبكاته (بما في ذلك العمليات والمهام) وتعزيز المرونة السيبرانية[1]، التي يعرفها الموقع الرسمي للحلف على أنها" قدرة المجتمع على المقاومة والتعافي من مثل هذه الصدمات وتجمع بين كل من الاستعداد المدني والقدرة العسكرية، حيث يعد الاستعداد المدني ركيزة أساسية لمرونة الحلفاء وعامل تمكين حاسم للدفاع الجماعي للحلف[2].

بالنسبة للناتو أصبح الفضاء السيبراني غير منفصل عن المجال العسكري، فقد تحول إلى فضاء معسكر نظرا لأهميته المتزايدة استراتيجيا وحيويا[3]، لهذا عمل الحلف على إدراج الدفاع السيبراني في أجندة أعماله، الأمر الذي تجسد بداية من قمة براغ (2002)، ثم عمل على تطوير سياسة للدفاع السيبراني في 2008 بعد الهجمات الإلكترونية التي شُنّت ضد إستونيا[4]. وخلال قمة وارسو لعام 2016، اعتبر الناتو أن المجال السيبراني هو مجال للعمليات من واجبه الدفاع عنه[5].انطلاقا من ذلك أصبح الدفاع السيبراني جزءا لا يتجزأ من السياسة الدفاعية العامة للناتو، بل إنه واحدة من أولوياته في عالم شديد التحول وكثير الاضطراب، وكانت قمة بروكسل لعام 2018 قد تناولت إنشاء مركز للعمليات السيبرانية،كما تم التأكيد في

---

[1] « Cyber Defense », 02/07/2021, in: https://www.nato.int/cps/en/natohq/topics_78170.htm (15/09/2021)

[2] « Resilience and Article 3 », 11/06/2021, in: https://www.nato.int/cps/en/natohq/topics_132722.htm (15/09/2021)

[3] Cours de Comptes Européennes, ***Op.cit***, p.14.

[4] Tughral Yamin, « Combating Cyber Terrorism through an Effective System of Cyber Security Cooperation », (Terrorism Experts Conference, Ankara, Oct.2015), p.13.

[5]Raquel Vazquez Llorente, A Digital Geneva Convention? The Role of the Private Sector in Cybersecurity, LES Ideas***, Strategic Update*** (May 2018), p.5.

قمة بروكسل لعام 2021 على أهمية تشكيل سياسة دفاعية سيبرانية شاملة بحيث لا ينفصل ذلك عن المرونة والتكيف اللتين يجب أن يتحلى بهماالحلف على الصعيد الدفاعي[1].

وأثناء قمة لشبونة في 2010 تم إدراج الدفاع السيبراني ضمن المفهوم الإستراتيجي للحلف، ليتم إقرار سياسة الدفاع السيبراني لحلف شمال الأطلسي في 2011، وفي قمة المجر جرى التأكيد على أن "الهجوم الرقمي ضد دولة عضو يعالَج في إطار البند الخامس" (أي من اتفاقية الحلف)، أما في قمة فرصوفيا عام 2016 فقد قام الحلف بإدراج الفضاء السيبراني ضمن نطاق عملياته بالموازاة مع سعي مستمر لتعزيز التعاون مع الاتحاد الأوروبي في مجال الدفاع السيبراني، وفي 2018 اتفق وزراء دفاع الدول الأعضاء على إنشاء مركز جديد للعمليات السيبرانية (Snape)، وتجب الإشارة إلى أن لجنة الدفاع السيبراني التابعة لحلف الناتو لها دور استشاري وتوجيهي للدول الأعضاء، كما أن اللجنة الثلاثية "C3" (consultation, commandement, contrôle) لها دور محوري في الدفاع السيبراني[2].

تنص المواد 4 و5 من ميثاق حلف شمال الأطلسي على الدفاع الجماعي، كما يتم الاستناد إلى المادة 51 من ميثاق الأمم المتحدة، وعلى هذا الأساس تم تكييف الدفاع السيبراني ليتماشى مع رؤية الحلف وهدف الدفاع المشترك في حال تعرُّض عضو من أعضائه إلى هجوم سيبراني مهما كان نوعه، بالتالي فإن الدفاع السيبراني عنصر مهم في الإستراتيجية الشاملة للحلف، وقد تم إنشاء بُنى مؤسساتية لهذا الغرض، كما أن الردع الإلكتروني أساسي أيضا، ويهدف الحلف إلى "تطوير نظام دفاع قوي مع معايير أمنية محسَّنة، والتركيز على الوقاية والمرونة وعدم التكرار"، بالرغم مما يكتنف ذلك من تحديات وثغرات بدايةً بصعوبة التعرف على العدو في الفضاء السيبراني، وصولا إلى الثغرات القانونية[3].

---

[1] « Cyber Defense », publié le : 08/07/2021, in : https://www.nato.int/cps/fr/natohq/topics_78170.htm (15/10/2021)

[2] Le Centre pour la Gouvernance du Secteur de Sécurité, ***Op.cit***, p.56.

[3] « L'OTAN dans la cyber guerre : Stratégie globale et capacités opérationnelles », Publié le : 17/04/2017, in : http://www.diploweb.com/L-OTAN-dans-la-cyberguerre-stratégie-globale-et-capacités-opérationnelles.html (10/11/2021)

ويمارس الحلف أدوارا جادة في مجال مكافحة الإرهاب الإلكتروني والحوادث السيبرانية، ففي قمة براغ شهر نوفمبر 2002 عزم الحلف على زيادة قدراته لمواجهة الهجمات السيبرانية، وتم تحضير عدد من الأجهزة المتخصصة مثل: وكالة خدمات أنظمة المعلومات والاتصال (NCSA)، والمركز التقني المكلف بأمن الحواسيب والاتصال[1]. بالتالي أصبح دمج القدرات السيبرانية ضمن منظومة الدفاع الحربي أمرا ضروريا، بحيث تعد الأسلحة السيبرانية "مضاعفات للقوة" وتعزيزا للقدرات الحربية التقليدية، كما أكد ذلك البحث الصادر عن الاتحاد الدولي للاتصالات بعنوان: "البحث عن السلام السيبراني" (يناير 2011)[2].

يبرز هذا بوضوح وجهة نظر الحلف حيث يمكن للهجمات الإرهابية الإلكترونية أن تتجاوز عتبة الهجوم المسلح، مما يسمح بالدفاع الفردي أو الجماعي عن النفس بموجب المادة 51 من ميثاق الأمم المتحدة والمادة الخامسة من معاهدة شمال الأطلسي. علاوة على ذلك ، ولأول مرة منذ أن تناول حلف الناتو موضوع الدفاع الإلكتروني في عام 2006 ، تم التأكيد صراحةً على أن الدفاع الإلكتروني أصبح جزءًا من مهام وجهود الدفاع الجماعي للحلف

تبعا لذلك تبنت الدول الأعضاء سياسة الدفاع السيبراني المحسّنة (ECDP)* التي تؤكد على أن جملة مبادئ أهمها: عدم قابلية أمن الحلفاء للتجزئة، والوقاية، الكشف، المرونة، التعافي، والدفاع.

وتنص بوضوح على أن "(...) مسؤولية الدفاع الإلكتروني الأساسية لحلف الناتو للدفاع عن شبكاتها الخاصة، وأن المساعدة المقدمة للحلفاء يجب أن تتم وفقًا لروح التضامن، مع التأكيد على مسؤولية الحلفاء في تطوير القدرات ذات الصلة لحماية الشبكات الوطنية ".[3]

---

[1] Mitko Bogdanoski, Drage Petreski. ***Op.cit***, p-p :65-66.

[2] حمدون إ.توريه، ***مرجع سابق***،ص79.

* حاول برنامج ECDP تكييف القانون الدولي ليخلص لقابلية تطبيقه على العمليات الإلكترونية، بما في ذلك القانون الإنساني الدولي (IHL) أو قانون النزاعات المسلحة (LOAC).

[3] Wiesław Goździewicz, and others, ***Op.cit.***

ب–مركز التميز للدفاع السيبراني (CCDCOE) التابع لحلف الناتو:

تم الاتفاق في 2008 على إنشاء مركز دفاع سيبراني تعاوني (مركز التميز للدفاع السيبراني) في "تالين" عاصمة إستونيا، وذلك بمساهمة سبع دول هي: إستونيا، ألمانيا، إسبانيا، إيطاليا، لاتيفيا، ليتوانيا وسلوفاكيا[1]. تبرز أهمية هذا المركز في التدريب وتنمية السلوك السيبراني في بعده الدفاعي وبحث المسائل القانونية والأمنية المتصلة بالفضاء السيبراني[2]. بالإضافة إلى منح قدرات عملياتية أكبر في مجال الدفاع السيبراني[3]. بالتالي، يهدف مركز التميز بإستونيا إلى تطوير عقيدة الحلف الدفاعية السيبرانية على المدى البعيد، بالاعتماد على[4]:

- تقديم المبادئ والمفاهيم المتصلة بالفضاءالسيبراني.
- تنظيم ورش عمل تدريبيةوتمارين لصالح الدول الأعضاء.
- المساهمة في البحث والتطوير.
- تقديم المشورة للحلف بخصوص الهجمات السيبرانية.

في 2009 دعا مركز التميز للدفاع السيبراني مجموعة خبراء مستقلين في مجال قانون النزاعات المسلحة (أي المجموعة الدولية للخبراء IGE) لوضع دليل خاص بالحرب السيبرانية، سمّي بدليل "تالين"، وهو يتضمن رؤية دقيقة تخص القانون الدولي المطبق على الحرب السيبرانية بما يشمله ذلك من قوانين ما قبل (jus addbellum) وأثناء الحرب (jus inbello)، ليشكل بذلك خلاصة خبرة أكاديمية، عملية وتقنية،

---

[1] « L'OTAN ouvre un nouveau centre d'excellence sur la Cyber Défense », publié le : 14/05/2008, in : https://www.nato.int/cps/fr/natohq/news_7266.htm?selectedLocale=fr (15/10/2021).

[2] George Christou, ***Op.cit,*** p.51.

[3] Emmanuel Dupuy, « Quels enjeux politiques en matière de cyber défense ? ***», Revue Militaire***, N°1 (Janv.-Fév. 2013), p.20.

[4] Marion KOKEL, ***The Engagement of NATO in Cybersecurity: Securing the 5th Battlefield***, Mémoire présenté en vue de l'obtention du grade de Master en Sciences Politiques, Orientation Relations Internationales-Finalité Sécurité, Paix, Conflits (UNIVERSITE LIBRE DE BRUXELLES, UNIVERSITE D'EUROPE, FACULTE DES SCIENCES SOCIALES ET POLITIQUES, 2013-2014), P.72.

فيصبح بالتالي مرجعا مهما لصناع القرار، وليفنّد الفكرة السائدة أو المتداولة بأن "القانون الدولي صامت في المجال السيبراني"[1].

وفي مجال دراسة الإرهاب السيبراني، يحدد مركز الدفاع السيبراني للتعاون (CCDCOE) ثلاثَ مقاربات يراها أساسية وهي[2]:

- سيبرانية الهدف: أي "استهداف البنى التقنية للدولة من أجهزة، وخوادم، وشبكات، وقواعد بيانات بغرض الإضرار بمصالحها، أو إثارة الفزع بين المواطنين". هذه المقاربة تتبناها منظمة الأمن والتعاون في أوروبا على سبيل المثال.
- سيبرانية الأداة: بمعنى الأداة المستخدمة في تحقيق الغرض من الإرهاب السيبراني، مثل البرامج الخبيثة والضارة (فيروسات، أحصنة طروادة..).
- سيبرانية المجال: أي أن الأهداف الإرهابية متصلة بالفضاء السيبراني مهما اختلفت الأدوات. هذه المقاربة تتبناها الدول الكبرى كالولايات المتحدة وروسيا، إلى جانب دول أوروبية مثل بولندا وإيطاليا.

وتحرص قوات الحلف منذ 2010 على إجراء تمرين دولي يعرف باسم "الدروع المقفلة" Locked Shields، وهو يستهدف تعزيز القدرات السيبرانية للدول قبل وأثناء الفترات الحرجة حيث تكون أنظمة المعلومات والبنى التحتية مهددة، كما يستهدف تعزيز التعاون الدولي وتبادل الخبرات، ويعتمد هذا التمرين على نمط المحاكاة الافتراضية لخطر حاصل يتمثل في وقوع هجوم إلكتروني واسع وخطير، فيتم بناء سيناريوهات وتحديد إجراءات التعامل مع هذا الوضع[3]. وتجدر الإشارة هنا إلى وحدة الاستجابة لحوادث الكمبيوتر (NCIRC) التابع للحلف، والتي تعمل على الكشف والاستجابة للتهديد السيبراني والتعافي من آثاره[4].

---

[1] Kristen E.Eichensehr, « The Tallinn Guide », ***The American Journal of International Law***, vol.108 (July 2014), p.585.

[2] بولمكاحل، ***مرجع سابق***، ص145.

[3] CCDCOE, « LockedShields », in : https://ccdcoe.org/exercises/Locked-Shields (20/10/2021)

[4] David P. Fidler, &Others, « NATO, Cyber Defence and International Law », ***Journal of International and Comparative Law***, vol.4, Issue 1 (Fall 2013), p.9.

الشكل (17): الناتو ومقاربة الدفاع السيبراني في إطار سياساته للدفاع الحربي.

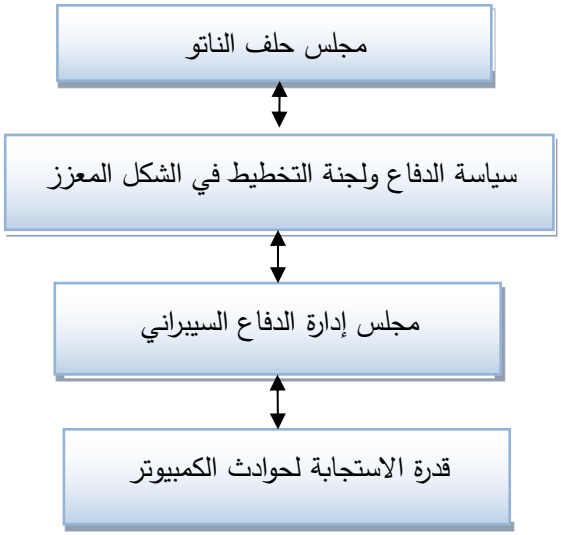
إستراتيجية الدفاع السيبراني	جهود الدفاع السيبراني لحلف الناتو
الدفاع ضد أي شكل من الهجوم السيبراني	تعزيز الدفاع السيبراني لأنظمة الناتو ضد أي شكل من الهجمات السيبرانية (مثال: وحدة التدخل الطارئ لحوادث الكمبيوتر NCIRC)
جمع المعلومات، الحفظ، المشاركة والتحليل	– تحسين عملية جمع المعلومات، تحليلها ومشاركتها – المشورة الجيدة، الإنذار المبكر والتوعية الظرفية – الاستخدام المتزايد للمعلومات الاستخباراتية ذات "المصدر المفتوح"
توسيع نطاق أنشطة الدفاع السيبراني	– الجناح العسكري للناتو والوكالات المدنية التابعة – تحسين الدفاع السيبراني لأعضاء الناتو – العمل مع القطاع الخاص في إطار أعضاء الناتو – التعاون مع الدول غير الأعضاء في الناتو في مجال الدفاع السيبراني – تحديد متطلبات المشاركين من خارج الناتو في مهمة إدارة الأزمات
الانتقال من التدابير السلبية إلى التدابير النشطة	– فرق الاستجابة السريعة للناتو – اختبار اختراق أنظمة الناتو – وعي الناتو بالنقاشات التقنية، السياسية والتشريعية المتعلقة بدفاع أكثر نشاطا
دمج الدفاع السيبراني مع مخططات دفاع أخرى	إدماج الدفاع السيبراني في عملية التخطيط الدفاعي للناتو

Source: David P. Fidler, &Others, « NATO, Cyber Defence and International Law », ***Journal of International and Comparative Law***, vol.4, Issue 1 (Fall 2013), p.20.

يوضح الجدول جهود حلف الناتو في إطار إستراتيجية الدفاع السيبراني، فقد عمل خلال ما يقارب عقدين من الزمن على تطوير سياسات الدفاع الحربي بما يواكب تحولات البيئة الأمنية والإستراتيجية إقليميا وعالميا، ليقوم بدمج الدفاع السيبراني في نطاق عملياته الحربية بالاعتماد على أساليب الوقاية والمواجهة والتعافي. إن الدفاع السيبراني يتطلب جهدا حثيثا بدايةً من جمع المعلومات وتحليلها (إدراك طبيعة التهديد وهوية العدو)، وصولا إلى المواجهة الفعلية عند التعرض إلى هجوم أو حالة إرهاب إلكتروني.

كما تم إنشاء هيئة إدارة الدفاع الإلكتروني، ومركز الامتياز للدفاع السيبراني التعاوني، وقدرة الاستجابة لحوادث الكمبيوتر، ومع ذلك لا تزال هناك ثغرات خطيرة في قدرات الدفاع الإلكتروني للحلف[1].

الشكل (18): هياكل حوكمة الدفاع السيبراني لدى حلف الناتو.

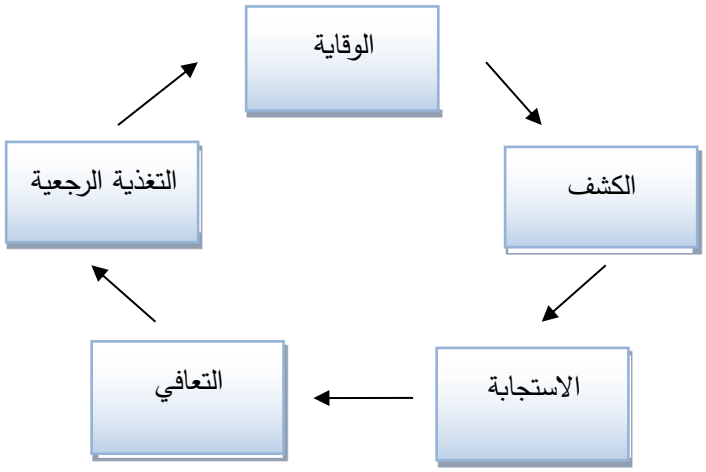


Source: David P. Fidler, and Others, « NATO, Cyber Defence and International Law », ***Journal of International and Comparative Law***, vol.4, Issue 1 (Fall 2013), p.10.

يوضح الشكل هياكل حلف الناتو المسؤولة عن حوكمة الدفاع السيبراني، وهذا يعكس اهتمام الحلف وتركيزه على الدفاع في الفضاء السيبراني في ظل انتشار التهديدات ذات الطابع غير التقليدي ونمو التهديد المحتمَل الناجم عن الإرهاب السيبراني في الأعوام الأخيرة.

[1] Murat Dogrul, and Others, ***Op.cit.***

الشكل (19): منهج عمل وحدة الاستجابة لحوادث الكمبيوتر التابعة للناتو.



Source: David P. Fidler, and Others, « NATO, Cyber Defence and International Law **»,** ***Journal of International and Comparative Law***, vol.4, Issue 1 (Fall 2013), p.10.

يوضح الشكل عناصرعمل وحدة الاستجابة لحوادث الكمبيوتر التابعة لحلف الناتو، وهي: الوقاية، الكشف، الاستجابة، التعافي والتغذية الرجعية، حيث يتم العمل بصورة وقائية استباقية بهدف السرعة في الكشف عن التهديد المحتمَل وقوعه، وبالتالي الاستجابة له لحظة وقوعه حتى يتمكن القائمون على هذه الوحدة من تحقيق هدف التعافي من آثاره.

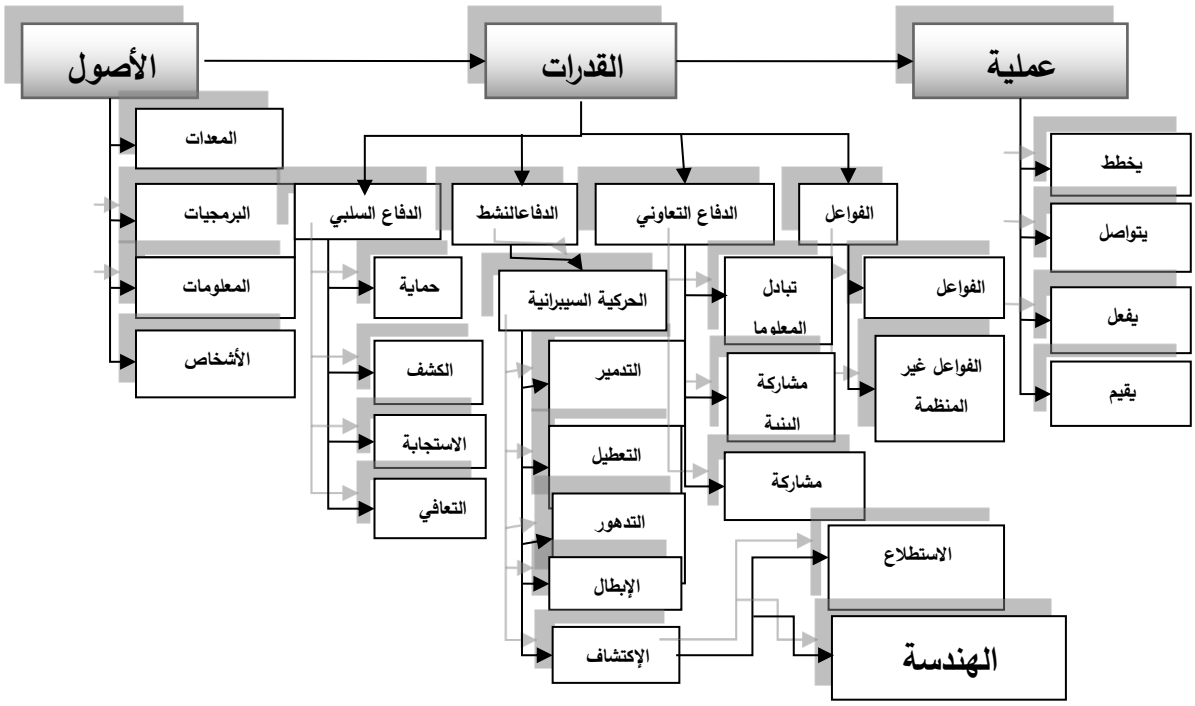
- سياسة الدفاع الذكي لحلف الناتو:

قام حلف الناتو بدمج الدفاع الإلكتروني في برنامجين مهمين من برامجه وهُما: عملية التخطيط الدفاعي لحلف الناتو (NDPP) ومبادرة الدفاع الذكية، وحيث يخدم البرنامج الأول تكامل الدفاع السيبراني في الإطار الوطني فيأخذ الناتو بعين الاعتبار الحد الأدنى من المتطلبات لمساعدة الحلفاء (ضحايا هجوم إلكتروني مثلا) في حماية الأنظمة والشبكات الوطنية إذا تم اختراق الناتو أو معلوماته من خلال هذه الحادثة، يهدف البرنامج الثاني إلى الاستفادة من الموارد لإمكانيات أكبر في هذا المجال[1].يُنظر إلى الدفاع الذكي في إطار الدفاع السيبراني كطريقة تعاونية لتوليد القدرات الدفاعية الحديثة للحلف، أي "بطريقة أكثر

[1] Marion Kokel, ***Op.Cit***, p.72.

كفاءة من حيث التكلفة وفعالة ومتماسكة" كما جاء في الموقع الرسمي للناتو، وفي قمة شيكاغو في ماي 2012 وافق قادة الناتو على تبني نظام الدفاع الذكي لتمكينه من تطوير واكتساب والحفاظ على القدرات المطلوبة لتحقيق أهدافه لعام 2020 وهي: "قوات حديثة ومترابطة بإحكام ومجهزة بشكل مناسب، تدريب وممارسة وقيادة"، وانطلاقا من ذلك تطورت سياسات الدفاع الذكي في إطار الدفاع الحربي والدفاع السيبراني للناتو، لتتكرّس فكرة العمل المشترك والمتناسق مع تنسيق التخفيضات المخطط لها في ميزانية الدفاع[1].

الشكل (20): نموذج الدفاع عن القدرة السيبرانية.



Source: Farzan Kolini, L. Janczewski, « Cyber Defense Capability Model: A Foundation Taxonomy », (submitted to: International Conference on Information Resources Management (CONF-IRM), 2015), in: https://cutt.us/B83tg

[1] « Smart Defence », in: https://www.nato.int/cps/en/natohq/topics_84268.htm (13/09/2021)

يوضح الشكل[1] العناصر المتدخّلة في الدفاع عن القدرة السيبرانية، وهو نموذج قابل للإسقاط على سياسات الدفاع السيبراني للناتو وحتى الاتحاد الأوروبي، حيث تمثل الأصول Assets الموارد ذات القيمة لدى الحكومات والمنظمات والأفراد، قد تكون ملموسة أو غير ملموسة، والحكومات مطالَبة بحمايتها من التهديدات الإلكترونية، ويتم تعريف أصل الأجهزة بأيّ معدّات Hardware تكنولوجية تسهّل خدمةً أو قيمة للمستخدمين النهائيين، فيتم استخدام الأجهزة لنقل المعلومات أو الخدمات أو تخزينها أو معالجتها أو التحكم فيها أو تقديمها إلى المستخدمين، وتعد أجهزة الكمبيوتر ومعدات الشبكات والبنية التحتية لتكنولوجيا المعلومات وأنظمة SCADA وكابلات الألياف أمثلة على أصول الأجهزة، أما البرمجيات Software فتشير إلى أصل البرنامج وتطبيقات تكنولوجيا المعلومات أو البرامج أو قاعدة البيانات المستخدَمة على نطاق واسع، من قبل الأفراد أو المنظمات أو الحكومات، في حين تعرّف القدرات Capabilities من خلال قدرة المدافع السيبراني على الاستعداد والوقاية والكشف والرد على هجوم إلكتروني، مما يتطلب تطوير أدوات إستراتيجية للدفاع النشط والسلبي والتعاون مع جهات مختلفة.

يشير مفهوم الدفاع السلبي Passive Defense إلى جميع التدابير والضوابط التي يمكن استخدامها بشكل سلبي لحماية واكتشاف والاستجابة والتعافي من التهديد السيبراني، مما يوفر وسيلة للتركيز على جعل الأصول الإلكترونية أكثر مقاومة أو مرونة تجاه الهجمات الإلكترونية، ويشمل الدفاع السلبي العناصر التالية:

- **الحماية (Protection):** تشير الحماية إلى إعداد وتنفيذ الضمانات المناسبة لضمان تقديم أصول الخدمة، ويمكن تحقيق حماية الأمن السيبراني باستخدام تقنيات القائمة البيضاء أو آليات الدفاع المعمَّق أو عمليات التصحيح، برامج مكافحة الفيروسات، جدران الحماية، ضوابط الوصول، اختبار الاختراق، عمليات التدقيق، وهي أمثلة على حماية النظام.

[1]Farzan Kolini, L. Janczewski, « Cyber Defense Capability Model: A Foundation Taxonomy », (submitted to : International Conference on Information Resources Management (CONF-IRM, 2015), in : https://cutt.us/B83tg

- **الكشف (Detect):** يشير الكشف إلى تطوير وتنفيذ العمليات والأنشطة لاكتشاف وقوع الأحداث السيبرانية، ويمكن تحقيق الكشف من خلال آليات أو تقنيات المراقبة، وتعد أنظمة كشف التسلل (IDS) وإدارة الحوادث والمعلومات الأمنية (SIEM)، وكذا المراقبة الصوتية كتقنيات يمكن تطبيقها لهذا الغرض.
- **الرد (Response):** يشير إلى تطوير وتنفيذ الأنشطة للاستجابة لحدَث إلكتروني تَمّ اكتشافه، من خلال –على سبيل المثال– الفصل بين الشبكات ومفتاح القفل عبر الإنترنت (حل تقني)، وهو ما تستخدمه الأنظمة الاستبدادية عادةً.
- **التعافي (Recovery):** بمعنى تطوير وتنفيذ الأنشطة أو العمليات التي تعيد الخدمات المخترَقة إلى مسارها الطبيعي، مع تقليل التأثير التخريبي للحوادث السيبرانية.

أما الدفاع السيبراني النشط Active cyber defence فيعرفه "روزنزوايغ" Rosenzweig بأنه "القدرة المتزامنة في الوقت الحقيقي على الاكتشاف، الكشف، التحليل وتخفيف التهديدات. يعمل الدفاع السيبراني النشط باستخدام أجهزة الاستشعار والبرامج والذكاء للكشف وإيقاف النشاط الضار بشكل مثالي قبل أن يؤثر في الشبكات والأنظمة"، ويشمل الدفاع النشط العناصر التالية:

- **التدمير (Destruction):** يحدث التدمير عندما يتم إتلاف أجهزة أو معدات تكنولوجيا المعلومات، ومن ثم تكون الأجهزة التالفة معطلة أو لا تعمل بشكل صحيح.
- **التعطيل (Disruption):** يشير التعطيل إلى نوع من رفض الخدمة أو الاستخدام غير المصرح به.
- **التدهور(Degradation):** يحدث تدهور الخدمة عندما تقع الخدمات المطلوبة خارج مستوى الخدمة المحدد مسبقًا، وبالتالي فإن المستخدم الشرعي سيواجه انخفاض جودة الخدمة (QOS).
- **الإبطال (Nullification):** أي قدرة الكيان على إبطال هجوم إلكتروني باستخدام القدرة الإلكترونية.

- **الاكتشاف (Discovery):** بمعنى قدرة الكيان على اكتشاف معلومات قيمة حول الهدف من مصادر مختلفة من بينها الهندسة الاجتماعية والاستطلاع، وتعتبر عمليات التصيد والعمليات النفسية وذكاء المصدر المفتوح OSINT (Open Source Intelligence) من الأنواع الشائعة لعمليات الاكتشاف.

بين سياسات الدفاع السيبراني للاتحاد الأوروبي والناتو:

التعاون بين الاتحاد الأوروبي والناتو ليس جديدا، بل يمتد لما يقارب 15 سنة، وخاصة فيما يتعلق بالدفاع وبناء القدرات وتوحيد الرؤية تجاه التهديدات الأمنية الهجينة والمشتركة التي تتعلق بالإرهاب وتمس الأمن السيبراني[1]. ولكن الحديث عن استراتيجية دفاع سيبراني مستقل في الفضاء الأوروبي (الاتحاد الأوروبي تحديدا) يجعلنا نذكر بعض المعوّقات مثل: رفض أو تخوف بعض الدول الأعضاء من مشاركة معلومات حساسة يُعد المساسُ بها وتسريبُها مساسا بالسيادة الوطنية، بالإضافة إلى الارتباط الدائم وغير المشروط بين الاتحاد الأوروبي وحلف الناتو في مجال الدفاع، وفي هذا السياق يلاحظ أن بولونيا مثلا بقيت تحت مظلة الحلف دون أن تغفل تطوير قدراتها الدفاعية الخاصة، كما أن إستونيا بعد تعرضها لهجمات سيبرانية طورت منظومتها الخاصة للدفاع السيبراني، كما دعت فرنسا في 2018 إلى أهمية تشكيل قوة أوروبية سيبرانية مستقلة[2]. من هنا تَبرز أهمية تطوير الاتحاد الأوروبي لسياساته الدفاعية في المجال السيبراني وفي مكافحة الإرهاب الإلكتروني، بالموازاة مع مسؤولية كل دولة عضو داخله عن تطوير منظومتها الدفاعية الخاصة، وحتى يتجاوز وصفَه بالطرف المسهّل والمحرّك للاتصال بين الأعضاء المشترَكة بين الطرفين (أي بين الاتحاد الأوروبي والناتو)[3].

انطلاقا مما تم تناوله في مطلب الدفاع الحربي للناتو، يتضح أن لهذا الحلف دورا ملموسا في التصدي للهجمات الإرهابية والإرهاب السيبراني من خلال التأسيس لمنظومة دفاع سيبراني مجهزة بكل الأدوات المتطورة.

---

[1] « EU-NATO Cooperation », in: https://www.consilium.europa.eu/en/policies/defence-security/ (11/12/2021)

[2] Rémy Ravel, ***Op.Cit***, p-p : 5-10.

[3] Dusco Deschaux-Dutard, ***Op.Cit***., p-p : 27-28.

المبحث الثاني: الصكوك القانونية في أوروبا وإعادة بناء القدرات.

يتم التطرق في هذا المبحث إلى الجانب القانوني لمحاولة تنظيم الفضاء السيبراني الأوروبي في إطار تطوير وتفعيل القوة السيبرانية الأوروبية. في هذا الإطار، عملت مختلف المؤسسات الأوروبية النافذة على ملء الفراغ القانوني فيما يتعلق بالفضاء غير المادي، مع محاولة –في الوقت نفسه–لبلوغ ثقافة سيبرانية شاملة وحالة من الوعي المجتمعي بالمخاطر الراهنة المتصلة بالإرهاب السيبراني.

المطلب الأول: رؤية أوروبية جديدة لملء الفراغ القانوني في الفضاء السيبراني.

تناوُل الصكوك القانونية الأوروبية التي تخص مكافحة الإرهاب عموما يدفعنا إلى الحديث عن ثلاث مؤسسات لها أدوار بارزة في مجال مكافحة الإرهاب في أوروبا، وهي: مجلس أوروبا (CoE)، المجلس الأوروبي (EC) ومنظمة الأمن والتعاون في أوروبا (OSCE).

أ– مجلس أوروبا (CoE):

يعد الاتحاد الأوروبي منظمة منفصلة عن مجلس أوروبا، ولكنه في الوقت ذاته مرتبطٌ به بشدة نظرا لتداخُل العضوية (الدول الأعضاء في الاتحاد الأوروبي هي أيضا أعضاء في مجلس أوروبا)[1]، فمجلس أوروبا مؤسسة دولية حكومية غير تابعة للاتحاد الأوروبي، تأسست في 1949 وهي تُعنى بحماية حقوق الإنسان وقيم الديمقراطية وسيادة القانون، وكان لمجلس أوروبا دور في تأسيس المحكمة الأوروبية لحقوق الإنسان لاحقًا، وهو يتكون من 47 دولة ويتخذ من ستراسبورغ في فرنسا مقرا له[2].

يركز مجلس أوروبا على نهج ثلاثي الأبعاد في مكافحة الإرهاب والإرهاب السيبراني باعتباره نمطا مستجَدا، بدايةً بتعزيز الإطار القانوني، ومعالجة أسباب الإرهاب، وهذان البعدان لا ينفصلان عن حماية القيم الأساسية للمجتمعات الأوروبية، وعلى الصعيد التشريعي اعتمد مجلس أوروبا عددا من الصكوك

---

[1] UNODC, « Regional Counter-Terrorism Approaches », https://www.unodc.org/e4j/en/terrorism/module-5/key-issues/european-region.html

[2] The European Union, ***How the European Union works ? Your Guide to the EU Institutions*** (Brussels : Publications Office, 2012), P.13.

القانونية لمكافحة الإرهاب، أهمها المعاهدة الإطار الرئيسَة لمكافحة الإرهاب والمتمثلة في "اتفاقية مجلس أوروبا لمنع الإرهاب" (اعتُمدت في 16 مايو 2005، ودخلت حيز النفاد في 1 جوان 2007)، وقد جاءت الاتفاقية لزيادة فعالية الصكوك الدولية المتصلة بمكافحة الإرهاب وتعزيز الجهود الدولية في ذات الشأن، حيث يشمل "منع" الإرهاب مثلا: تجريم الأفعال التي قد تؤدي إلى الإرهاب مثل الاستفزاز العام، التجنيد والتدريب، تعزيز سياسات المنع الوطنية والدولية وما تتطلبه من تعاون من خلال "تعديل الترتيبات القائمة لتسليم المجرمين والمساعدة المتبادلة والوسائل الإضافية"، كما تم اعتماد بروتوكول إضافي لاتفاقية مجلس أوروبا بشأن منع الإرهاب، استجابةً لقرار مجلس الأمن رقم 2178 (2014)، وذلك بتاريخ: 22 أكتوبر 2015 (رقم 217 في سلسلة معاهدات مجلس أوروبا)، ليدخل حيز التنفيذ في 1 جويلية 2017، ويشمل تلقّي تدريب إرهابي، والسفر (أيضا تمويله وتنظيمه) إلى الخارج بهدف الإرهاب، أتى ذلك بعد الارتفاع الملحوظ لأعداد المقاتلين الإرهابيين الأجانب الأوروبيين في صفوف الجماعات والتنظيمات الإرهابية في الشرق الأوسط، حيث تم تسجيل ما يقارب 25 ألف شخص انخرطوا وقتها في صفوف تنظيمات إرهابية على غرار تنظيم "داعش" الإرهابي، وبالتالي بات العمل الإرهابي بحاجة ملحة إلى تطوير جهود التصدي له وللعوامل التي تسبقه مثل التجنيد والتدريب والتمويل، فهي من الخطر بمكان مما يجعلهاجريمة جنائية، وهو ما جعل مجلس أوروبا يطلق بالمقابل خطة عمل لثلاث سنوات تخصّ "مكافحة التطرف العنيف والراديكالية" على مستوى المدارس والسجون والانترنت، وتوجد أيضا "اتفاقية مجلس أوروبا المتعلقة بغسل عائدات الجريمة والبحث عنها وضبطها ومصادرتها وبتمويل الإرهاب" (رقم 198 في سلسلة معاهدات مجلس أوروبا)، والتي اعتُمدت في 16 مايو2005 ودخلت حيز التنفيذ في 1 ماي 2008، لتكون أول معاهدة دولية تُعنى بمنع ومكافحة غسل الأموال وتمويل الإرهاب، إلى جانب ذلك يهتم مجلس أوروبا بالتعاون الدولي في مجال تسليم المجرمين الإرهابيين، وقد أنشأ لجنة من الخبراء تعرف باسم: CODEXTER، وهي تساعد في تنفيذ صكوك المجلس القانونية لمكافحة الإرهاب ومعالجة الثغرات الموجودة[1].

[1] UNODC, Op.cit.

يتضح من خلال ذلك أن مجلس أوروبا يمارس دورا بارزا في مكافحة الإرهاب، من خلال لجنة الخبراء (CODEXTER) واعتماده الاتفاقية الأوروبية لقمع الإرهاب (1977) والبروتوكول المعدل في 2003، إضافة إلى الاتفاقية الأوروبية للوقاية من الإرهاب (لمنظمة الأمن والتعاون أيضا وحدة خاصة بمكافحة الإرهاب منذ 2003)[1].

ب–المجلس الأوروبي (EC):

يعد المجلس الأوروبي من بين المؤسسات الهامة التابعة للاتحاد الأوروبي، يتمثل دوره في وضع التوجهات العامة والأولويات، لهذا يوصف بأنه "صانع القرار الأساسي في الاتحاد الأوروبي"، وتتمثل مهام المجلس في[2]:

- التشريع بالاشتراك مع البرلمان الأوروبي، فهو بذلك يدعم عمل البرلمان باللوائح والتوجيهات المنظمة في الجانب القانوني.
- تنسيق سياسات الدول الأعضاء (مثال: السياسة الاقتصادية).
- تحسينالعلاقات الخارجية والأمنية المشتركة في الاتحاد الأوروبي.
- إبرام الاتفاقيات الدولية.
- اعتماد ميزانية الاتحاد الأوروبي بالاشتراك معالبرلمان الأوروبي.

حدد المجلس الأوروبي أهم أهداف الاتحاد الأوروبي في مجال مكافحة الإرهاب والإرهاب السيبراني، فالتعاون الدولي يبقى ذا قيمة قصوى وأولوية لا تقل أهمية عن باقي السياسات، إلى جانب قطع سبل التمويل على الجماعات والتنظيمات الإرهابية، وزيادة قدرات وكفاءة مؤسسات الاتحاد الأوروبي في مكافحة ومنع العمل الإرهابي على اختلافه، يشمل ذلك أيضا تعزيز مراقبة الحدود، بالإضافة إلى تعزيز أساليب التعاطي مع آثار الهجمات الإرهابية، والتصدي جيدا لسياسات التجنيد والاستقطاب التي تتبعها الجماعات الإرهابية من

[1] عبد الجليل إسماعيل حسن الشيخ زيني، ***مرجع سابق***، ص 262.

[2] The European Union, ***Op.cit,*** P-p : 12-15.

خلال الانترنت[1]. وتعد مراقبة البيانات البيومترية للأفراد عملا أساسيا في التعرف على الأفراد، وفي هذا السياق يندرج مشروع FIRST الذي يفّعل خاصية المتابعة والتعرف على الوجه عبر الأدوات الرقمية، مما يسهل مهمة جمع البيانات البيومترية المتعلقة بالمقاتلين الإرهابيين الأجانب أو غيرهم من الأفراد الإرهابيين، بالإضافة إلى "الية التعرف التلقائي على هوية القادمين" والتي تقع ضمن إجراءات الاتحاد الأوروبي لمراقبة الحدود والوافدين عليه[2].

وتُلزم إستراتيجية الاتحاد الأوروبي لعام 2005، المعتمدة من قبَل المجلس الأوروبي، بالانخراط العالمي في مكافحة هذه الظاهرة المتطورة باستمرار، دون إخلال بحقوق الإنسان وحرياته، مع التأكيد على أربعة عناصر محورية هي[3]:

- منع الإرهاب، ويتضمن ذلك منع أسبابه وظروفه، أي منع ظهور جيل جديد من الإرهابيين.
- حماية المواطن والبنية التحتية الحيوية الأوروبية من الهجمات الإرهابية.
- ملاحقة الإرهابيين وتقديمهم إلى العدالة، والعمل على تثبيط مساعي التخطيط والاتصال والتمويل.
- معالجة آثار العمل الإرهابي والتكفل بالضحايا.

وقد اعتمد المجلس الأوروبي في 2008 "إستراتيجية الاتحاد الأوروبي لمكافحة التطرف والتجنيد للإرهاب"، وجرت مراجعتها في 2014 في ظل التحدي المتمثل في تجنيد الأفراد للعمل الإرهابي بالشرق الأوسط، وتعززها أدوات قانونية أخرى مثل: القرار الإطار JHA / 475/2002 (عُدّل في 2008)، وهو يقدم تعريفا مشتركا للإرهاب والجرائم المتصلة به، وفي 7 مارس 2017 اعتمد المجلس الأوروبي توجيهابشأن مكافحة الإرهاب، يجرم السفر داخل الاتحاد الأوروبي أو خارجه أو إليه لأغراض إرهابية، مثل الانضمام

---

[1] *Sarah Leonard and Christian Kaunert, «* Introduction – Beyond EU Counter-terrorism Cooperation: European Security, Terrorism and Intelligence », in: Christian Kaunert and Sarah Leonard (Editors), ***European Security, Terrorism and Intelligence : Tackling New Security Challenges in Europe*** *(Palgrave Macmillan, 2013), p.5.*

[2] جاسم محمد واخرون، الإرهاب والتطرف في أوروبا من الداخل، ***مرجع سابق***، ص: 291، 514.

[3] UNODC, *Op.cit.*

إلى أنشطة جماعة إرهابية أو بغرض ارتكاب هجوم إرهابي، إضافة إلى توجيه البرلمان الأوروبي والمجلس الأوروبي لعام 2015 بشأن مكافحة الإرهاب (قمع التمويل لأغراض إرهابية)[1].

يضاف إلى ذلك تحيين تعريف الجريمة الإرهابية على مستوى الاتحاد الأوروبي والتشريع لملاحقة جريمة الإرهاب الإلكتروني،مع التأكيد دوما على أن تبادُل المعلومات بين سلطات إنفاذ القانون محطة ضرورية لمواجهة تهديد الإرهاب الإلكتروني[2]. ويعد جمع البيانات الدقيقة من مهام أجهزة الاستخبارات، وقد أكد تقرير لمعهد واشنطن لسياسات الشرق الأدنى (12 نوفمبر 2019) أن "جمع المعلومات الاستخباراتية الشاملة يشكل أمرا ضروريا لرصد التهديدات المحلية التي قد تتحول إلى تهديدات ضد الوطن، وهذا يعني التركيز على كل شيء بدءًا من الجماعات المتطرفة الهامشية غير المنتسبة"[3].

ج– منظمة الأمن والتعاون في أوروبا (OSCE):

توصف بأنها "أكبر منظمة أمنية إقليمية بعضوية 57 دولة مشاركة من جميع أنحاء أمريكا الشمالية وأوروبا وآسيا"، لتشكّل منتدى للحوار السياسي والأمني حول المسائل والقضايا المشتركة، وفرصة للتعاون وإدارة الأزمات، مع العلم أن قراراتها غير ملزمة من الناحية القانونية، وفي مجال مكافحة الإرهاب تعمل المنظمة على تكريس تعاون منسق على جميع المستويات وعبر جميع القطاعات والفاعلين (من الدولة إلى المجتمع المدني)، وقد تبنّت عددا من القرارات المتعلقة بمكافحة الإرهاب على مستوى الاتحاد الأوروبي مثل: القرار رقم 1 بشأن مكافحة الإرهاب الصادر في 2001،وخطة عمل بوخارست لمكافحة الإرهاب، وتحثّ المنظمة الدول الأعضاء على التصديق على الصكوك الدولية لمكافحة الإرهاب وجعلها تتوافق والقوانين الوطنية وحقوق الإنسان، كما تهتم بتعزيز التعاون الدولي في إطار العدالة الجنائية ومنع الإرهاب وتمويله ومنع تدفّق المقاتلين الإرهابيين الأجانب من أوروبا، مع الإشارة إلى الإعلان الوزاري بشأن منع ومكافحة التطرف العنيف والراديكالية اللذين يؤديان إلى الإرهاب (4 ديسمبر 2015)[4].

---

[1] ***Idem***.

[2] Sofija Voronova, ***Op.Cit,*** P-p : 5-6.

[3] جاسم محمد، واخرون، الإرهاب والتطرف في أوروبا من الداخل، ***مرجع سابق***، ص.27.

[4] UNODC, ***Op.cit.***

وقدرت ميزانية الاتحاد الأوروبي لمكافحة الإرهاب ب 168,7 مليار يورو في نهاية 2020[1]. ويعد إنشاء مركز "الحالة الراهنة" (STTCEN) محطة أساسية في التعاطي مع التهديد الإرهابي على مستوى الاتحاد الأوروبي، وذلك من خلال تشكيل ثلاث مجموعات: تعنى الأولى (Coter) بمتابعة الإرهاب خارج حدود الاتحاد الأوروبي، وتختص الثانية (TWG) في الأمن الداخلي، أما المجموعة الثالثة فتُعنى "بمهمة متابعة اللائحة الأوروبية المعادية للإرهاب"[2].

وإلى جانب رغبة الاتحاد الأوروبي في تأمين بُناه التحتية ومصالحه ومواطنيه في الفضاء السيبراني، يلاحَظ من خلال الجهود المبذولة لفرض منظومة تشريعية صارمة في وجه تهديدات الإرهاب الإلكتروني والهجمات السيبرانية أنه يسعى كذلك لأن يكون فاعلا مؤثرا في الفضاء السيبراني من خلال تثبيت وضعه كمنظم للسلوك ومطبق للقانون الدولي داخل هذا الفضاء، وهذا يُذكّر بما جاء في وثيقة المفوضية الأوروبية الخاصة بإستراتيجية الاتحاد الأوروبي في مجال الأمن السيبراني لعام 2020، حيث إن الاتحاد الأوروبي يفكر عالميا ويتحرك أوروبيا.

ويسعى الاتحاد الأوروبي إلى تسريع وتيرة تنفيذ الصكوك القانونية الحالية، وسد الفراغ في الفضاء السيبراني، وتحديث التشريعات الحالية ذات الصلة بمحاربة الإرهاب الإلكتروني، وتفعيل تعاون أكبر في مجال إنفاذ القانون. وأتى إعلان أجندة الاتحاد الأوروبي لمكافحة الإرهاب لعام 2021 بعد أن عرفت أوروبا هجمات إرهابية عنيفة خريف 2020، مما أدى إلى اعتماد جدول أعمال الاتحاد الأوروبي الجديد لمكافحة الإرهاب في ديسمبر 2020، وتقوم الأجندة الجديدة على أربع ركائز هي:التوقع، المنع، الحماية والاستجابة، وقد تعرضت إلى ضرورة محاربة الفكر المتطرف الذي يتخذ من الانترنت وسيلة له لينتشر وليكرس العمل الإرهابي، وضرورة تحديث آليات الاتحاد الأوروبي في مجال مكافحة الظاهرة الإرهابية المتطورة باستمرار[3].

---

[1] جاسم محمد واخرون، ***مرجع سابق***، ص.513.

[2] عبد الجليل إسماعيل حسن الشيخ زيني، ***مرجع سابق***، ص262.

[3] Sofija Voronova, ***Op.Cit***., P.11.

- **اتفاقية بودابست الخاصة بمكافحة جرائم الكمبيوتر:**

تحدد اتفاقية بودابست (التابعة لمجلس أوروبا) التي دخلت حيز التنفيذ في جويلية 2004، الإطار القانوني للتعاطي مع الجرائم السيبرانية، ولكنها تظل قاصرة في معالجة بعض أنواع الهجمات السيبرانية مثل التجسس وأعمال التخريب[1]. تلزم معاهدة بودابست الموقعين عليها (على الصعيد الوطني وعبر الوطني)بدعم الجهود الدولية، وأنه "على الدول تحديد ومقاضاة لمجرمين الإلكترونيين... والتأكيد على أن القوانين والممارسات تحجب الملاذات الآمنة عن المجرمين، والتعاون مع التحقيقات الجنائية الدولية دون تأخير"، وبالإضافة إلى ذلك "على الدول إدراك وتحمل مسئوليتها لحماية البنى التحتية المعلوماتية وتأمين الأنظمة المحلية ضد الدمار أو سوء الاستخدام"[2]. تشجع اتفاقية بودابست التعاون بين الدول في مجال إنفاذ القانون وتوفر إطارا لتنسيق الجهود الوطنية على مستوى التشريع، ولكنها في المقابل غير ملزمة للدول إذ كانت ترى ما "يمس بسيادتها، أو بأمنها، أو النظام العام فيها أو مصالح أساسية أخرى"[3].

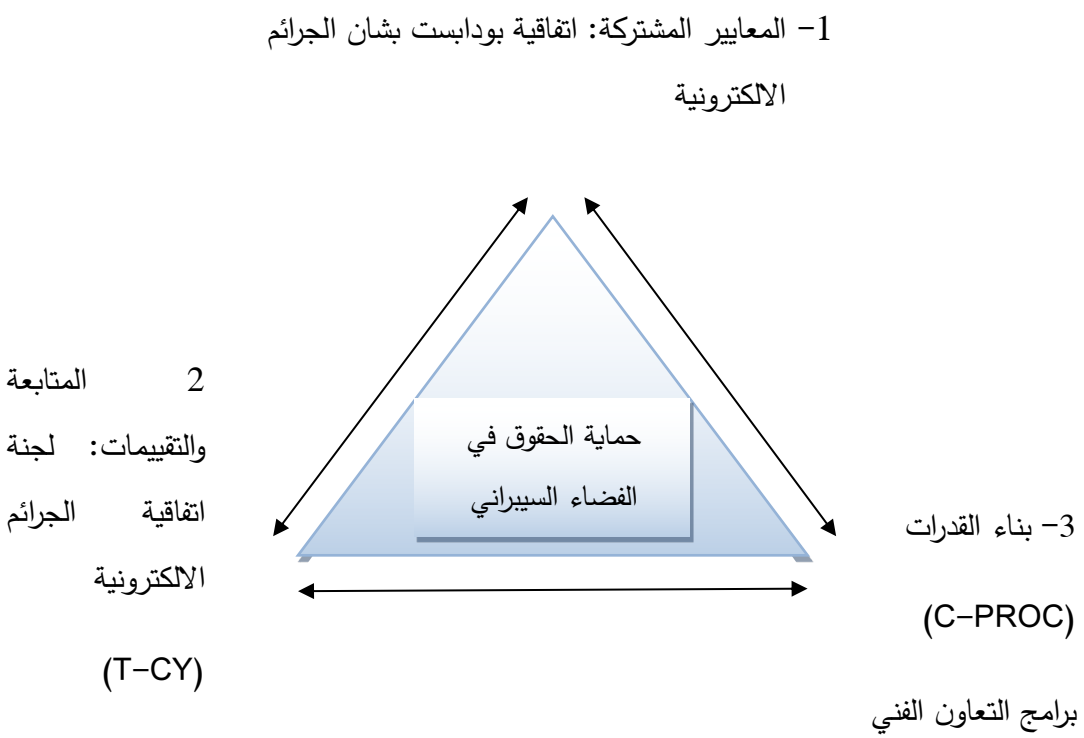
---

[1] حمدون إ.توريه، ***مرجع سابق***، ص87.

[2] سكوت وارن هارولد وآخرون، ***التوصل إلى اتفاق مع الصين بشأن الفضاء الإلكتروني*** (كاليفورنيا: منشورات مؤسسة راند، 2016)، ص 42-43.

[3] ميليسا هاثاواي، مؤشر الجاهزية الإلكترونية، ***مرجع سابق***، ص14.

الشكل (21): مقاربة مجلس أوروبا لحماية الفضاء السيبراني.



Source: Panagiotis Trimintzios and Others, ***Cybersecurity in the EU common Security and Defence Policy (CSDP): Challenges and Risks for the EU***, European Parliament- Think Thank (16 May 2017), p. 30.

يوضح الشكل المعايير الثلاثة التي تقوم عليها مقاربة مجلس أوروبا في حماية الفضاء الإلكتروني، حيث تبرز أهمية المعايير المشتركة في قمة المثلث، المتابعة والتقييم ثم بناء القدرات من خلال برنامج التعاون التقني الذي يشرف عليه مكتب المجلس المكلف بحماية الفضاء الإلكتروني (C-PROC)، وهو يساعد الدول في تعزيز أنظمتها القانونية وتكريس التعاون عام–خاص فضلا عن تحسين فرص التدريب والتعاون الدولي والعمل على إنفاذ القانون في مجال مكافحة الجرائم الإلكترونية[1].

[1] Panagiotis Trimintzios and Others, ***Cybersecurity in the EU common Security and Defence Policy (CSDP) : Challenges and Risks for the EU***, European Parliament- Think Thank (16 May 2017), P.30.

وتجب الإشارة إلى أن الانضمام إلى اتفاقية بودابست متاحٌ لجميع الدول، أعضاءً كانوا في الاتحاد الأوروبي أو غير أعضاء، وقد عرفت مصادقة 61 دولة حتى عام 2019، ويعد عمل مجلس أوروبا مكملا لمهام المنظمة الأوروبية للأمن والتعاون، والتي تهتم بمعالجة المسائل ذات الصلة بالفضاء الإلكتروني، وخاصة الأمن والإرهاب السيبراني[1]. تهدف اتفاقية بودابست المتعلقة بالجريمة الإلكترونية (23 نوفمبر 2001) إلى بلورة "سياسة جنائية مشتركة" كما جاء في الديباجة، وتؤكد على التعاون الدولي في المسائل الجنائية، كما تعد تكملةً وتعزيزا لاتفاقيات مجلس أوروبا بخصوص التعاون في المجال الجنائي[2]. بالتالي، تبقى اتفاقية بودابست الصك القانوني الأشهر ضمن السياسات الأوروبية لمكافحة الجرائم الإلكترونية، ولكنها في مقابل ذلك إطار قانوني قاصر عن مواكبة التطورات السريعة في تكنولوجيا المعلومات وفي الجرائم والتهديدات على غرار الإرهاب الإلكتروني[3]. فمن الانتقادات الموجهة إليها أنها لم تتناول جريمة الإرهاب الإلكتروني، وهي تركز على الحكومات كأطراف محورية للتصدي للتهديدات السيبرانية دون أن تعمل على حشد اهتمام دولي معتبَر للانضمام إليها[4].

يستلزم التطور التكنولوجي رؤية وإطارا تشريعيا يتناسب معه، أما في الفضاء السيبراني فلا يوجد تطور كبير في مجال التشريع، خاصة وأن الجهود المبذولة ترتبط أكثر بالجانب الفني، ورغم الجهود المعتبرة التي قام بها الاتحاد الأوروبي لتنظيم الفضاء الرقمي وحمايته، يمكن القول إنه مازال يواجه ثغرات عديدة ومعقدة خاصة من الناحية القانونية ومن حيث ضبط المفاهيم الأساسية ومن بينها الإرهاب السيبراني، بالتالي فإن المشرّع الأوروبي يواجه تحديا مهما في هذا الصدد، وقد ذكر البرلمان الأوروبي في 2012 عددا من التحديات القانونية والسياسية في الفضاء السيبراني، حيث مازال الاتحاد الأوروبي يعاني عدم الضبط والتنسيق التام في سياساته ومؤسساته بهذا الشأن، بما يتطلب "نهجا متعدد التخصصات وعالميا ومنسقا لهذه التحديات على مستوى الاتحاد الأوروبي"، وقد ركز في أجندات عمله على حماية الأمن السيبراني والبنية التحتية وأمن المستخدمين انطلاقا من حماية أمن الشبكات والمعلومات وضمان تحقيق

---

[1] Le Centre pour la Gouvernance du Secteur de Sécurité, ***Op.Cit.,***p.52.

[2] مجلس أوروبا، ***مرجع سابق***، ص02.

[3] George Christou, ***Op.Cit.***, p.57.

[4] Tin Hojsgaard Munk, ***Op.Cit.,***p-p : 146-147.

المرونة السيبرانية، وهذا بحاجة إلى ربطه بالتعاون الدولي من أجل مواجهة فعالة لتهديدات الإرهاب الإلكتروني،ويعد عامل التكامل والتنسيق المستمر بين وكالات الاتحاد الأوروبي المختصة بحماية الأمن السيبراني ضرورة قصوى، حيث يجري ربط عمل مؤسسات إنفاذ القانون والمؤسسات القضائية بنشاط القطاعين العام والخاص داخل الاتحاد في المجال ذاته وبالمؤسسات الدولية المختصة في إطار التعاون الدولي خارج نطاق الاتحاد الأوروبي، مع الاستفادة من خبرات الدول الأعضاء المتطورة من الناحية القانونية والمؤسسية، ولأن الفضاء السيبراني متطور باستمرار فهذا يجعل من الصعب تبسيط التدابير المتخذة على الصعيد الأوروبي[1].

- **التوجيه الخاص بأمن الشبكات والمعلومات داخل الاتحاد الأوروبي:**

يعد التوجيه الخاص بأمن الشبكات وأنظمة المعلومات (NIS) لعام 2016 أول إجراء تشريعي على مستوى الاتحاد الأوروبي، يرمي إلى تنمية التعاون داخل الاتحاد بشأن الأمن السيبراني، فقد "حدد الالتزامات الأمنية لمشغلي الخدمات الأساسية (في القطاعات الحيوية مثل الطاقة والنقل والصحة والتمويل) ولمقدمي الخدمات الرقمية (الأسواق عبر الإنترنت ومحركات البحث والخدمات السحابية)"، ثم أتى اقتراح من المفوضية الأوروبية لتعديل هذا التوجيه بما يستجيب للتطور التقني وتحول التهديد الأمني في المقابل[2]. يتضمن توجيه أمن الشبكات والمعلومات ثلاثة أقسام هي[3]:

- القدرات الوطنية: فمن الضروري أن تتوفر دول الاتحاد الأوروبي على قدرات سيبرانية، سواء من خلال وحدات الاستجابة لطوارئ الحاسوب أو عبر إجراء تمارين سيبرانية.
- التعاون العابر للحدود بين دول الاتحاد الأوروبي.
- الإشراف الوطني على القطاعات الحيوية: حيث تشرف الدول الأعضاء على الأمن السيبراني لمشغلي السوق المهمين بالنسبة للقطاعات الحيوية، كما تشرف على مزودي الخدمات الرقمية المهمين (الأسواق عبر الإنترنت، محركات البحث السحابية..).

---

[1] Anna Kańciak, ***Op.cit.***
[2] European Council, ***Op.Cit.***
[3] "NIS Directive", https://www.enisa.europa.eu/topics/nis-directive (15/11/2021)

يوفر التوجيه الخاص بأمن الشبكات وأنظمة المعلومات للاتحاد الأوروبي تدابير تشريعية لتعزيز الأمن السيبراني الأوروبي وتكريس ثقافة أمنية واسعة، وتتم مراجعته بشكل دوري كما حدث في 2018، وفي ديسمبر 2020 تم اقتراح توجيه أمن الشبكات والمعلومات NIS2 لتحسين مستوى الأمن السيبراني الأوروبي عبر السياسات والأدوات والقدرات المتاحة لمواجهة الهجمات السيبرانية، حيث "يقوم بتحديث الإطار القانوني الحالي مع الأخذ في الاعتبار الرقمنة المتزايدة للسوق الداخلية في السنوات الأخيرة وتطور مشهد تهديدات الأمن السيبراني"[1].

- **قانون الأمن السيبراني للاتحاد الأوروبي لعام 2019:**

تم اقتراح قانون الاتحاد الأوروبي للأمن السيبراني في 2017، ثم دخل حيز التنفيذ في 2019، وبذلك تم منح امتيازات أكبر للوكالة الأوروبية لأمن الشبكات والمعلومات (ENISA) لتصبح الوكالة الأوروبية للأمن السيبراني، مما يسمح لها بممارسة دور أكبر في تطوير استراتيجيات الأمن السيبراني وتنسيق الاستجابة والمرونة فيما يخص الهجمات الإلكترونية والإرهاب السيبراني[2].ويشمل قانون الأمن السيبراني لعام 2019 دعم التعاون وتبادل المعرفة بخصوص قضايا الأمن السيبراني، وبناء القدرات من خلال تمارين المحاكاة التي تتم على مستوى الاتحاد الأوروبي[3]. بالإضافة إلى خطة لإصدار شهادات الامتثال لمعايير الأمن السيبراني في الاتحاد الأوروبي، مما يحفز الثقة على مستوى المؤسسة والمستهلك[4].

يسعى الاتحاد الأوروبي إلى ضمان الأمن السيبراني لأعضائه وتقوية سياساتهم في مواجهة الإرهاب الإلكتروني، فحتى وإن كان ضمان وتحقيق الأمن من وظائف الدولة ومسؤولياتها الأولى يظل الاتحاد

---

[1]European Commission, « Shaping Europe's Digital Future », in: https://digital-strategy.ec.europa.eu/en/policies/nis-directiven (15/11/2021)

[2] Erik Lindvall, ***More dangerous than guns and tanks: How Cybersecurity is Framed by the EU and Sweden ?***, Master's thesis (Uppsala University : Department of Government, Spring 2020), p-p : 33-34.

[3] Martina Urbinati, Sonia Lucarelli, "The Securitization of Cyberspace : Building the Cyber Resilient European Union of Tomorrow", p.8. in: https://www.academia.edu/41650573/The_Securitization_of_Cyberspace_Building_the_Cyber_Resilient_European_Union_of_Tomorrow (11/01/2022).

[4] جوشوا ميلتزر، كاميرون كيري، "علاقات متشابكة: كيف تدعم التجارة الرقمية سياسات الأمن السيبراني؟"، عرض: رغدة البهي، 2019/10/02، https://bit.ly/3sZqYfS (2021/12/11)

الأوروبي منظمة مسؤولة بالموازاة في توفير الدعم والتنسيق وتكريس التعاون ووضع الإطار القانوني والسياسي والاستراتيجي لمكافحة الإرهاب السيبراني، وأيضا تقييم الثغرات والفراغ الموجود[1]. وفي هذا السياق سعت المفوضية الأوروبية إلى دعم عمل سلطات إنفاذ القانون في الاتحاد الأوروبي من خلال تعزيز قدراتهم الرقمية وتزويدهم بمهارات وأدوات أكثر، حتى يتسنى للقانون أن يتدارك ثغراته في الفضاء السيبراني وتكون هناك مواجهة أمثل للجرائم السيبرانية[2]. ومع أن دول الاتحاد الأوروبي قد سدّت بعض الثغرات التنظيمية التي يمكن أن يستغلها الإرهابيون الناشطون إلكترونيا، على سبيل المثال في مجال التمويل، يظل الاتحاد يواجه تهديدات معقدة باستمرار "تجعل نجاحاته النسبية في الحرب ضد الإرهاب موضع تساؤل"[3].

ولا تتوقف النصوص القانونية للاتحاد الأوروبي عند تجريمالتحريض على الفعل الإرهابي، وإنما تمس أيضا "الاستفزاز العلني لارتكاب جريمة إرهابية" بالإضافة إلى التجنيدوالتدريب[4].كان تركيز استراتيجية الاتحاد الأوروبي على منع وصول الإرهابيين إلى أوروبا، وهو ما وضحته الركائزُ الأربعُ التي قامت عليها وتمت الإشارة إليها سابق (منع، حماية، متابعة واستجابة)، وظل الأمر على حاله لأكثر من عقد من الزمن، حتى تم التفطُّن إلى أهمية مراجعة السياسات الأوروبية في مجال مكافحة الإرهاب بما يواكب التحول في أشكاله وأساليبه، وتحديدا مع بروز وانتشار الإرهاب الإلكتروني[5].

- تحديات التشريع في الفضاء السيبراني:

يُظهر الواقع أنه لا سبيل إلى تنظيم الفضاء السيبراني دون إطار تشريعي، ولا سبيل إلى مكافحة الإرهاب الإلكتروني عبر تدابير وسياسات لا تقترن بأُطُر قانونية، "ذلك أن القانون قوة اجتماعية، ويساهم بشكل فعلي في فرض معايير السلوك الاجتماعي على الأفراد، وفي تحقيق التنسيق والتوافق الاجتماعي

---

[1] Sofija Voronova, ***Op.Cit,*** P.1.

[2] Commission Européenne, The EU's Cybersecurity Strategy in the Digital Decade, ***Op.Cit***., P.15.

[3] رافاييل بوسونج، "الخطوات التالية لسياسة الاتحاد الأوروبي لمكافحة الإرهاب.. التهديدات المتطورة للجهادية والتطرف اليميني والتعاون عبر الأطلسي"، ترجمة: يوسف سامي، https://asbarme.com/5716/ (2021/09/12)

[4] Sylvia BODIN, and Others, « International Cooperation in the face of Cyber-Terrorism: Current Responses and Future Issues », in: https://www.ejtn.eu/Documents/THEMIS%202015/Written_Paper_France_1.pdf (10/11/2021)

[5] جاسم محمد واخرون، الإرهاب والتطرف في أوروبا من الداخل، ***مرجع سابق***، ص26.

عبر صياغة سلوك الأفراد"[1]. ومع ذلك، لا يمكن القياس على القواعد القانونية العامة في جميع الحالات، فالفضاء السيبراني يتّسم بتركيبته المعقدة من حيث المحتوى والجانب التقني، كما يرتبط قصور التشريع في الفضاء السيبراني بعاملين هما[2]:

- ديناميكية الفضاء السيبراني مقابل "الطابع السكوني نسبيا للقانون": يعني ذلك أن الفضاء الرقمي لا يتوقف عن التطور والتجدد، بالتالي تكون التهديدات الحاصلة داخله متطورة باستمرار، ومن المفترض أن تكون القوانين الوطنية والدولية مواكبةً لخصوصية هذا الفضاء، ولكن الملاحَظ هو الطابع "السكوني نسبيا" للقوانين، ومع ذلك تسعى دول الاتحاد الأوروبي إلى جعل قوانينها مواكبة للتهديدات السيبرانية ومن ضمنها الإرهاب السيبراني.
- إمكانية التحايل على القانون في المجال السيبراني:معناه أن المجرم في الفضاء السيبراني يمكنه التحايل من خلال أساليب التخفي وتزييف الهوية، عن طريق تغيير وغلق الحسابات الشخصية أو غير ذلك مما تتيحه تكنولوجيا المعلومات والاتصالات، وهذا يجعل المشرّع يواجه صعوبة في كشف جريمة الإرهاب الإلكتروني خاصة وأن العنصر المادي هو أحد العناصر الواجب توفرها في الجريمة.

ويرى الدكتور عادل عبد الصادق أنه "لا يوجد موقف دولي واضح من هجمات الفضاء الإلكتروني ولا توجد سوابق قانونية يمكن الاستناد إليها، وهذا ما يدفع إلى ضرورة الوصول إلى نُظم قانونية يمكن أن تنشئ قواعد خاصة بتنظيم استخدام الفضاء الإلكتروني وتجريم استخدامه في الأغراض العسكرية، أو تلك الأنشطة التي تضر بأهميته ودوره في المجتمع الدولي"[3]. يتناول دليل تالين للقانون الدولي المطبق على الحرب الإلكترونية (الناتو 2013) توسيع نطاق القانون الدولي الإنساني ليشمل الفضاء الافتراضي، وهو ما يؤكد هاجس الدول المتعلق بالآثار الاقتصادية والسياسية والاجتماعية للتهديدات السيبرانية، ويؤكد أيضا مصلحة المجتمع الدولي المتصلة بتكنولوجيا المعلومات والاتصالات والضرورة القصوى لضمان الأمن

---

[1] إسماعيل أوقادي، مرجع سابق.

[2] المرجع نفسه.

[3] عادل عبد الصادق، "أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني"، ***سلسلة أوراق***، العدد 23 (الإسكندرية: وحدة الدراسات المستقبلية، 2016)، ص145.

السيبراني[1]. ولكن، إذا كان القانون الدولي ينطبق على الفضاء السيبراني فما هي آليات تطبيقه؟ وما هو الإطار الذي يشرّع الدفاع عن النفس في حال وقوع إرهاب إلكتروني؟

من هنا سعى المجتمع الدولي إلى استحداث "اتفاقية جنيف الرقمية" والتي ترمي إلى "حماية المدنيين من خطر الحروب الإلكترونية لتُحاكي اتفاقية جنيف الخاصة بحماية المدنيين في الحروب، الصادرة عام 1949"[2].وكانت شركة "مايكروسوفت" Microsoft قد عبّرت عن الحاجة الملحة لاتفاقية رقمية في الفضاء السيبراني، تكون كفيلة بحماية الأفراد من الحروب الإلكترونية والهجمات السيبرانية في زمن السلم[3]. وهي مبادرة ورؤية تستحق التطوير، وبالأخص مع الاستخدام المتزايد للوسائط الإلكترونية واندماج الانترنت في مختلف مجالات الحياة.

وتبقى التدابير التشريعية غير كافية لمكافحة الإرهاب السيبراني، ويجب تنظيم إجراءات ردع عسكرية لصد الإرهابيين عن استغلال الإنترنت، جنبا إلى جنب مع تدابير استباقية تردع هذا الاستغلال، وهو ما يقوم بها الناتو والاتحاد الأوروبي من خلال اليات الكشف المبكر والتبليغ عن التهديد ليسهل احتواؤه قبل حدوثه فعليا، ويشير مصطلح "الردع السيبراني" إلى التدابير الاستباقية التي يتم اتخاذها لمواجهة أنشطة الإرهاب السيبراني، تتمثل مهمته في "منع العدو من شن هجمات في المستقبل عن طريق تغيير رأيه أو مهاجمة تقنيته أو بوسائل أكثر وضوحا (مثل المصادرة أو إنهاء الخدمة أو الحبس أو الإصابة أو التدمير)"، ردًا على هجوم إلكتروني، ويسعى حلف الناتو إلى تشكيل منظومة ردع قوية ومساعدة أعضائه في تعزيز قدراتهم الردعية بالتنسيق مع الحلف[4].

---

[1] Luisa Cruiz Lobato and Kai MichailKenkel, “Discourses of Cyberspace Securitization in Brazil and in the United States », Artigos, ***Politica Internacional***, Vol.58, Issue: 2, P-p: 23-43, (Jul-Dec 2015).

[2] "الخطر السيبراني واستحقاق التشريع الدولي.. اتفاقية جنيف الرقمية مثالا"، 2017/08/28، (2021/11/11) https://www.alriyadh.com/1619757

[3] Brad Smith & Vice Chair, "The need for a Digital Geneva Convention", 14/02/2017, in: https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/ (21/06/2020)

[4] Murat Dogrul, and Others, ***Op.cit.***

المطلب الثاني: الثقافة الوطنية للسلامة السيبرانية.

أ- مفهوم الثقافة السيبرانية:

يمكن تعريف الثقافة السيبرانية بأنها "مجموعة من الثقافات والمنتجات الثقافية الموجودة على الانترنت و/أو التي أصبحت ممكنة من خلال الانترنت، إلى جانب القصص التي تُروى عن هذه الثقافات والمنتجات الثقافية"، أو هي الثقافة التي أفرزها الاستخدام البشري لتكنولوجيا المعلومات والاتصالات حيث يعد الكمبيوتر والانترنت طرفا أساسيا فيها، وبذلك يجري التفاعل بين الإنسان والآلة، ويتم تصنيف الثقافة السيبرانية إلى تلك الموجودة قبل ظهور الانترنت، وتلك التي تشكلت مع ظهور الانترنت[1]. كما تعرّف بأنها "مزيج من الأنشطة والقيم والذهنية والإدراك الذي يشكّله الناس في إطار الدراسة، العمل، التواصل، الترفيه والحياة اليومية على خلفية عصر الشبكة"[2].وقد حدد الباحث "ماسيك" Jakub Macek في عام 2004 أربعَ فترات زمنية للثقافة السيبرانية هي[3]:

- الأولى تمتد إلى فترة سبعينيات القرن العشرين، وقد اقتصرت الثقافة السيبرانية حينها على بعض الطلاب والباحثين في مجال السيبرنتيك، وأصحاب برمجيات الكمبيوتر.
- الثانية يمكن حصرُها في السبعينيات والثمانينيات، عندما خرجت الثقافة السيبرانية من نطاق الجامعات والمعاهد لتعرف توسعا وانتشارا تدريجيا.
- المرحلة الثالثة تزامنت مع انتشار الحواسيب الصغيرة في العالم الغربي بدايةً.

---

[1] Chai Lee Goi, « Cyberculture: Impacts on Netizen », ***Asian Culture and History***, Vol.1, No.2 (July 2009), P-p: 140-141.

[2] Wenjing You, « The Influence of Cyberculture on Life Style under the Background of new Media », ***Frontiers in Educational Research***, Vol.3, Issue 5, P.90.

[3] Lee Goi, ***Op.cit***, P-p: 141-142.

"جاكوب ماسيك" أستاذ وباحث من دولة التشيك، مهتم بوسائل الإعلام وأثر العامل التكنولوجي في بعده الاجتماعي والسياسي.

– الفترة الرابعة تمتد من نهاية الثمانينات إلى نهايات القرن العشرين، وخلالها تشكلت فلسفة جديدة بخصوص الثقافة السيبرانية حيث أصبحت الانترنت والكمبيوتر أكثر شعبية.

ب–مفهوم ثقافة الأمن السيبراني:

تشير ثقافة الأمن السيبراني (CSC) إلى "المعرفة والمعتقدات والتصورات والمواقف، وافتراضات ومعايير وقيم الأشخاص فيما يتعلق بالأمن السيبراني وكيف تظهر علىالسلوك"، يعني ذلك بلوغ مرحلة يصبح فيها الأمن السيبراني لصيقا بالعادات والسلوكيات، مما يعكس مرحلة متقدمة من الوعي والمعرفة بالتهديد على مستوى الفرد، الجماعة والمؤسسة، وهو ما يحفز في المقابل المرونة السيبرانية[1]. فثقافة الأمن السيبراني تكون حصيلة العمل الجماعي وتنسيق الأدوار بين الوكالات المتخصصة في الأمن السيبراني، مع إعطاء اهتمام واسع للشراكة الفعالة بين القطاعين الحكومي والخاص، خاصة وأنه لا يخفى على أحد أن الدولة قد انسحبت من بعض القطاعات الهامةوالإستراتيجية لصالح القطاع الخاص، فالبنية التحتية الأوروبية اليوم تُدار أيضا بواسطة القطاع الخاص، وكمثال على ذلك تُذكر قطاعات النقل والصحة والبنوك وحتى الطاقة[2].

تعمل منظمة الأمم المتحدة على تطوير ثقافة سيبرانية عالمية، مع ضرورة التأكيد على أن هذه الثقافة عبارة عن "صناعة" يجب أن تتحمل مسؤوليتَها منظماتٌ وطنية وجهات رسمية وغير رسمية، بالإضافة إلى أهمية التدريب في مجال الأمن السيبراني.

وتناول منتدى القمة العالمية لمجتمع المعلومات في ابريل 2021 مواضيع عديدة تتعلق بالأمن السيبراني من بينها دور الفرد من خلال وعيه وإدراكه للمخاطر الواقعة وكيفية الوقاية منها[3]. إن الوعي والمسؤولية متغيران أساسيان في مواجهة التهديدات السيبرانية، فذلك يقطع الطريق على بعض الأنشطة

---

[1] ENISA, ***Cyber Security Culture in organizations*** (NOVEMBER 2017), P.7.

[2] The Software Alliance (BSA), EU Cybersecurity Dashboard: A Path to a Secure European Cyberspace?, P.6. in: https://cybersecurity.bsa.org/ (21/10/2021).

[3] الاتحاد الدولي للاتصالات، "لماذا نحتاج إلى أمن سيبراني أكثر شمولا؟"،
(2021/09/12) https://www.itu/netw/wsis/forum/2021/ar/Agenda/Session/328

الإجرامية داخل فضاء يتمتع بمرونته وغياب الرقابة فيه، ومثالُ ذلك محتوى الخطاب والكراهية والتجنيد الإلكتروني في صفوف الجماعات الإرهابية.

إن دور التوعية بقضايا الأمن السيبراني لا يمكن الاستغناء عنه، فهو السبيل إلى تكوين ثقافة سيبرانية وثقافة للأمن السيبراني في المجتمعات، مما يشكل حصنا منيعا في وجه التطرف والإرهاب السيبراني.

المبحث الثالث: نحو تطوير جدول أعمال بحثي حول الإرهاب السيبراني– التحديات التقنية والحلول.

يُخصص هذا المبحث لتقديم قراءة في مستلزمات تطوير جدول أعمال بحثي في الاتحاد الأوروبي يخص الإرهاب السيبراني، معنى ذلك استخلاص التحديات بما فيها التقنية واقتراح الحلول الملائمة، وهو ما سيتضح في نهاية المبحث تحديدا (المطلب الثالث) المتعلق بالنضج السيبراني، حيث يسعى الاتحاد الأوروبي إلى بلوغ مرحلة النضج، كفاعل دولي في الفضاء السيبراني من جهة، إلى جانب دعم وتحفيز دوله على تحقيق هذا الهدف انطلاقا من عوامل القوة الذاتية.

المطلب الأول: تطوير السياسات وخرائط الطريق لأبحاث الجريمة الإلكترونية والإرهاب الإلكتروني.

عمل الاتحاد الأوروبي من خلال هياكله وسياساته على تطوير سياسات تخص أبحاث الجريمة الإلكترونية والإرهاب السيبراني، هو ما برز من خلال وكالة يوروبول التي تصدر تقارير دورية حول حالة التهديد والجريمة السيبرانية في الاتحاد الأوروبي، والوكالة الأوروبية للأمن السيبراني (ENISA) التي تعد تقارير متنوعة تشكّل مرجعا لرسم السياسات وخرائط الطريق لمكافحة الإرهاب السيبراني.

ويجب التأكيد على أن الدور الأكبر في مكافحة التطرف والإرهاب يجري على المستوى المحلي، أي المجتمعات المحلية، حيث قد تتوفر ثغرات معينة تشكل عاملا مهما لإنتاج جيل من المتطرفين، ولهذا يهتم الاتحاد الأوروبي من خلال رؤية هياكله ومؤسساته ومسؤوليه بعنصر التوعية بمخاطر التطرف وفي المقابل نشر ثقافة السلم الاجتماعي والحوار والتعايش، مع أن هذا الجانب يظل قاصرا عن احتواء تهديد الإرهاب عبر الانترنت خاصة مع صعود اليمين المتطرف في أوروبا خلال الأعوام الأخيرة وانتشار خطاب الكراهية تجاه الأجانب، مما بات يؤثر بشكل كبير في مستويات الاستقرار المجتمعي على المستوى المحلي، الوطني وعبر الوطني، وهو ما أكده انتشار هجمات اليمين المتطرف الإرهابية التي يمكن اعتبارُها ردة فعل على خطاب الكراهية داخل المجتمعات الأوروبية.

في هذا السياق، تعد جهود شبكة التوعية بالتطرف (RAN) معتبرَة في التكريس للممارسات الجيدة، فخلال اجتماع في مايو 2013 تم تناول دور الإنترنت في التطرف، وكان المؤتمر رفيع المستوى لشهر

ديسمبر 2012 قد أكد على تبادل المعرفة وأفضل الممارسات بين المنظمات على مستوى الاتحاد الأوروبي والقطاع الخاص، واقترح أمثلة على الممارسات الجيدة في تنفيذ "الخطابات المضادة" (أي المضادة للتطرف) على الإنترنت واستكشاف سُبل التعاون مع القطاع الخاص في التصدي للتطرف عبر الشبكة العنكبوتية.

كما تعقد الشبكة الأوروبية للخبراء حول التطرف (ENER) ورشات عمل وندوات مفيدة في إطار رسم السياسات الأوروبية لمكافحة التطرف والإرهاب في صورته التقليدية والسيبرانية، وهو ما يُظهر الاهتمام بدمج الجانب الأكاديمي في عملية رسم السياسات وخرائط الطريق، حيث عملت شبكة الخبراء الأوروبية حول التطرف (ENER) كمنصة للمناقشة وتقديم الخبرة منذ عام 2008، وقد أعدت سلسلة من أوراق السياسات واستضافت حلقات دراسية حول دور الإنترنت في عملية التطرف[1].

ويصدر يوروبول تقارير دورية مهمة بالنسبة لصانعي السياسات في الاتحاد الأوروبي، وهي أربعة أنواع: تقرير اتجاه وحالة الإرهاب في الاتحاد الأوروبي (TE-SAT)، تقييم الجريمة المنظمة والخطيرة في الاتحاد الأوروبي (SOCTA)، تقييم تهديد الجريمة المنظمة عبر الانترنت (IOCTA) ومراجعة يوروبول السنوية[2]. تتمثل أهمية هذه التقارير في أنها تعطي تقييما للحالة الراهنة، وتزود صانعي القرار برؤية استشرافية، بخصوص التدابير والسياسات الواجب اتخاذها في مواجهة تهديدات متجددة وأخرى مستحدثة على غرار الجريمة الإلكترونية والإرهاب السيبراني.

وفي سياق الحديث عن تطوير السياسات وخرائط الطريق لأبحاث الجريمة الإلكترونية والإرهاب السيبراني، يمكن التطرق إلى عدد من النقاط من ضمنها:

- مقاربة إعادة التوازن المجتمعي ومعالجة التطرف العنيف المؤدي للإرهاب السيبراني في أوروبا:

تركيز المجتمع الأكاديمي على المحتوى يعني أن الجهود قد تركزت على تدقيق مجموعة واسعة من مواقع الاحتجاج الجهادية واليمينية المتطرفة والتي ظهرت على الإنترنت. مما لا شك فيه أن هذا يوفر

[1] Argomaniz, ***Op.Cit.***

[2] « Main Reports », 06/12/2021, in: https://www.europol.europa.eu/publications-events/main-reports (30/12/2021)

لواضعي السياسات والممارسين رؤى ثاقبة حول روايات الإرهابيين واستراتيجيات التسويق والمعتقدات والتنظيم، وهي عوامل مهمة، ولكن هذا يمثل جانبا واحدا للتطرف عبر الإنترنت (أو ما يمكن تسميته "سوق التطرف عبر الانترنت")، أي جانب العرض للمحتوى، فلا يزال جانب الطلب (كيفية تفاعل الفرد مع المواد المتطرفة المعروضة عبر الانترنت) يشكل فجوة في صنع السياسات والفهم الأكاديمي، وانطلاقا من ذلك ظل دور الإنترنت في عملية التطرف صعب المعالجة، على الرغم من الاهتمام الكبير بالسياسة والعمل الأكاديمي، إذ لا يُعرف الكثير عن تجارب الأفراد على الإنترنت وتفاعلهم عند تطرفهم[1].

- إدارة الجودة في الفضاء السيبراني:

تذكر الأدبيات أن مناقشة نموذج إدارة الجودة (PDCA) * تعود إلى النصف الأول من القرن العشرين، وتحديدا 1939 في كتاب: "الطريقة الإحصائية من وجهة نظر إدارة الجودة" لصاحبه "والتر شيوارت" (Walter Shewhart)، ثم قام "إدواردز دمينغ" (W. Edwards Deming) ** بتعديل الدورة لتُعرف باسمه وتصبح PDSA، ويشمل التخطيط وضع جدول زمني وحشد الموارد وتحديد الأهداف والمسؤوليات في إطار منهجية عمل ونطاق زمني محدد، في حين تتعلق الدراسة بدراسة النتائج المحققة، وغير المحققة، ومدى التوافق بين ما تم التوصل إليه والأهداف التي حُددت سلَفا، لتتضمن المرحلة الأخيرة مواصلة تنفيذ السياسات عبر تحديثها وتطويرها لتواكب التحول المستمر في الفضاء الرقمي، أو مراجعة وإعادة التخطيط من أجل تحسين إدارة الجودة (عملية التحسين تبقى مستمرة). هذا النموذج يمكن إدراجه في سياق حوكمة الأمن السيبراني، فالعناصر المذكورة تعبر عن أهم المراحل التي يجب أن تمر بها إدارة الجودة في الفضاء السيبراني، بالتالي فإن النموذج يستهدف ضمان التحسين المستمر للأمن السيبراني[2].

---

[1] ***Ibid***, p 11.

[*] PDCA اختصارا لـ : خطّط (plan)، افعل (do)، تحقّق (check)، نفّذ (act).

[**] "ويليام إدواردز دمينغ" (1900-1993)، مهندس أمريكي وعالم إحصائيات وكاتب وباحث، تأثر بأعمال سابقه "والتر شيوارت" (1891-1967) وهو فيزيائي أمريكي وعالم إحصائيات أيضا.

[2] للمزيد راجع ما يلي:

Anna Kańciak, ***Op.cit.***

– مركز الكفاءة في الصناعة والتكنولوجيا والبحوث الأوروبي للأمن السيبراني:

تمخّض عن قرار جمع المجلس الأوروبي والبرلمان الأوروبي في ديسمبر 2020، ومقره الان في بوخاريست (عاصمة رومانيا)، يهدف إلى زيادة المرونة السيبرانية وتطوير الأمن السيبراني، دون أن يتم إغفال دعم المؤسسات الناشئة ودعم البحث والابتكار في هذا المجال[1].

ويبقى عنصر البحث الأكاديمي في قضايا الأمن السيبراني والجريمة والإرهاب الإلكترونيين ضروريا حسب تصور الاتحاد الأوروبي، فهو الذي يسمح بتطوير السياسات وخرائط الطريق ورسم المستقبل، وتوفر مؤسسات الاتحاد الأوروبية ميزانيات معتبرة للبحث الأكاديمي في هذا الجانب لاقتناعها التام بضرورته القصوى.

المطلب الثاني: الطريق السيبراني إلى المستقبل– منهجية تطوير السياسات وخرائط الطريق للأمن السيبراني الأوربي.

لقد بات من الأهمية الوصول إلى تفاهم مشترك حول حدود حرية التعبير والمسؤوليات القانونية لمنصات الإنترنت ومقدمي الخدمات، وأن تستمر الدول الأعضاء في الاتحاد الأوروبي في العمل على المدى الطويل على تكييف قوانينها مع نبذ خطاب الكراهية[2]. ولهذا، يسعى الاتحاد الأوروبي إلى بذل مزيد من الجهود وهو في صدد وضع وتحديث منهجية لتطوير السياسات وخرائط الطريق لحماية الأمن السيبراني الأوروبي ومكافحة الإرهاب الإلكتروني، يتجلى ذلك من خلال:

أولا: في مجال التعاون.

يمكن تقسيم النهج الأمني التعاوني للاتحاد الأوروبي إلى فئتين عريضتين:

---

[1] European Council, Council of the European Union, « Cybersecurity: how the EU tackles cyber threats», in: https://www.consilium.europa.eu/en/policies/cybersecurity/ (10/12/2021)

[2] سكاي نيوز، "إرهاب عبر الإنترنت.. تحذيرات من تطبيقات إخوانية تنشر التطرف"، 2022/01/12، متاح على (2022/01/20) https://cutt.us/hSmk3

1) التعاون المؤسسي، و 2) الفهم المشترك للأمن. عندما يتعلق الأمر بالتعاون يتم التركيز بشكل خطابي كبير على تطوير نهج مشترك للأمن السيبراني قائم على تعزيز التعاون بين الجهات الفاعلة والأدوات والسياسات[1].

تؤكد الاستراتيجية الأمنية الأوربية على ضرورة التعاون مع الجهات الفاعلة على المستويين الداخلي والدولي، من أجل تحسين القدرات الدفاعية والأمنية للاتحاد الأوروبي[2]. بيد أن محاولات بناء القدرات لحماية البنية التحتية والاستجابة للحوادث على الصعيدين الإقليمي والدولي تتعلق بشكل أكثر بأي هجوم إرهابي إلكتروني "محتمل". وتعد مبادرة IMPACT، أي "الشراكة الدولية المتعددة الأطراف ضد التهديدات السيبرانية"والتي تستضيفها ماليزيا، واحدة من الأمثلة حول أهمية التعاون لرسم المستقبل السيبراني،وتهدف هذه المبادرة إلى توفير منتدى عالمي للحكومة والصناعة؛ قدرة دولية على الاستجابة للحوادث السيبرانية؛ التدريب في مجال الأمن السيبراني، وغيرها من المسائل المتصلة بحماية الأمن السيبراني، كما يوصف مركز التميز للدفاع السيبراني التابع لمنظمة حلف شمال الأطلسي (الناتو)، ومقره تالين عاصمة إستونيا، بأنه نموذج متطور ومركز أبحاث يهدف إلى توفير الخبرة الأمنية للأعضاء داخل الحلف، ومع ذلك، تبدو هذه المبادرات جنينية نسبيًا، فلم يمض أكثرُ من عَقدين على ظهورها،وبالإضافة إليها فقد عززت المنظمات الأخرى عنصر التعاون بين أعضائها، مثل رابطة دول جنوب شرق آسيا (آسيانASIAN) ، ومنظمة الدول الأمريكية (OAS) ومنظمة شنغهاي للتعاون (SCO)[3]. ويتضح من خلال هذه المبادرات (وغيرها مما تم التعرض إليه في عنصر سابق حول التعاون) صدقية الأبحاث التي تؤكد أن الأمن الأوروبي يُبنى على المستوى فوق الوطني على حساب المستوى الوطني، خاصة ما تعلق بمكافحة اللإرهاب[4].

ويشمل التعاون أيضا الجانب التشريعي، مثلا من خلال وضع تشريع يخصّ المحتوى المتاح على الانترنت، مثل اتفاقية مجلس أوروبا لمنع الإرهاب، والتي تحتوي على أحكام ضد "الاستفزاز العام لارتكاب

1 Helena Carrapico, André Barrinha, ***Op.cit.***

2 Jukka Ruohonen, ***Op.cit.***

3 Report of the Working Group on: ***Countering the Use of the Internet for Terrorist Purposes***, Counter-Terrorism Implementation Task Force (CTITF) - February 2009, p.12.

4 Jukka Ruohonen***, Op.cit.***

جريمة إرهابية" ونشر المواد المتعلقة بتدريب الإرهابيين، وقد تم تبني هذا النهج على مستوى الاتفاقية "الإطار" الجديدة للاتحاد الأوروبي بشأن مكافحة الإرهاب[1].

ولا جري الاهتمام بالتعاون في قضايا الأمن السيبراني ومكافحة الإرهاب بمعزل عن الجانب الأكاديمي، بالنظر إلى دوره المعلوم في رسم مستقبل الأمن السيبراني الأوروبي، وفي ظل ذلك تسعى المفوضية الأوروبية إلى دعم برنامج ماجستير مخصص للأمن السيبراني، والمساهمة في خارطة طريق لبحوث الأمن السيبراني في الاتحاد الأوروبي لما بعد 2020[2].

ثانيا: أتمتة(Automation) آليات الرصد والمكافحة لجرائم الإرهاب الإلكتروني.

يشير مصطلح الأتمتة إلى "دمج الآلات في نظام التحكم الذاتي"، وبالتالي"تطبيق الآلات للمهام التي يتم تنفيذها مرة واحدة أو على نحو متزايد من قبَل البشر، والمهام التي كانت مستحيلة لولا ظهورها (أي ظهور الأتمتة)"[3].ومع ظهور أجهزة الكمبيوتر والتطور في تقنيات المعلومات والاتصالات، أصبح للذكاء الاصطناعي مكانة هامة انطلاقا من الاعتماد على خوارزميات متطورة لتحليل المعلومات ورصد الأخبار المزيفة بشكل فوري وأوتوماتيكي وأكثر سرعة من مجموعات الرصد التقليدية.

وقد قامت شركة "جوجل" (Google) خلال عام 2016 بتمويل 20 مشروعا أوروبيا يعمل على التحقق من المعلومات، وتضمّن ذلك مشروعين في بريطانيا استخدما تقنيات الذكاء الاصطناعي لمكافحة الأخبار الزائفة أثناء الانتخابات النيابية في المملكة المتحدة.

ولا يتم الاكتفاء برصد الشائعات والأخبار الزائفة فحسب، ولكن يتم العمل على التعقب الرقمي للمحتوى بمعنى تتبع انتشار الأخبار المغلوطة، وتعقب مصدرها، والتحقق من عناصرها بشكل فوري ومنظم.

---

[1] European Commission, The EU's Cybersecurity Strategy in the Digital Decade, ***Op.Cit***. P-p: 4-12.

[2] Countering the Use of the Internet for Terrorist Purposes, ***Op.cit***, p.17

[3] عاصم محمد، "ما هي الأتمتة؟ وكيف تطورت تاريخيا حتى عصرنا الحديث؟"، 2018/06/23، (2021/12/20) https://www.ida2at.com/what-is-automation-and-how-has-it-evolved/

وتلعب مراكز أو وحدات التحكم في الشائعات دورا معتبرا في الرصد والمتابعة، فهي مراصد مزودة بالتقنيات والتطبيقات اللازمة لمراقبة الفضاء السيبراني ورصد الشائعات، خاصة في فترات الأزمات والطوارئ، وقد أشار الباحث "أونوك من جامعة "ورك" البريطانية في دراسته حول انتشار الشائعات على وسائل التواصل الاجتماعي إلى أهمية مثل هذه المراكز، مع الحرص على تزويد المواطنين في الوقت المناسب بالمعلومات الصحيحة.

نظم إدارة السمعة الرقمية:

هي نظم ارتبطت بالعلاقات العامة وبيئة الشركات والأعمال، ولكن يمكن الاستفادة منها بشكل عام في رصد الموضوعات المتداولة، وجمع ردود الفعل بشأنها، وصياغة الردود أو محتوى مضاد ونشرها[1].

الذكاء الاصطناعي:

تمكّنت وسائل الذكاء الاصطناعي من لعب دور إيجابي مهم من خلال توفير قدر كبير من الوقت والجهد في إجراءات البحث والتتبع أخذاً في الاعتبار ضخامة حجم المعلومات التي تتم معالجتها ومدى التعقيد والتشابك والتشابه فيها بينها، ومن التطبيقات المهمة في هذا السياق تطبيق برمجيات الذكاء الاصطناعي على أجهزة التصوير والمراقبة وعلى قواعد البيانات المصورة للأفراد حيث صارت تقنية التعرف على الوجه باستخدام الذكاء الاصطناعي أداة أساسية في تحديد هوية مرتكبي أعمال العنف والحوادث الإرهابية، وقد استُخدم الذكاء الاصطناعي ونجح بالفعل في تقليص احتمالات الخطأ في مراحل البحث والتحري وتحييد المتورطين وكذلك في مراحل الملاحقة والسعي لإنفاذ القانون حيث يتم تضييق دوائر الاشتباه وتسهيل عمليات الحصر والفرز للمعلومات والأشخاص والمعطيات كلها ذات الصلة. كل ذلك ساعد في رفع مستوى الدقة والكفاءة في الجانب الأمني المباشر لمواجهة الإرهاب، كما وفر مناخاً من الثقة بأجهزة

[1] فاطمة الزهراء عبد الفتاح، "التشارك الإلكتروني:آليات مكافحة الشائعات في الفضاء السيبراني"، موقع المستقبل للأبحاث والدراسات المستقبلية، 29 ماي2017، https://futureuae.com/ar-/Mainpage/Item/2841 (2022/02/27)

الأمن، وخلق طمأنينة لدى الرأي العام تجاه المؤسسات والآليات المنخرطة في تلك المواجهة وذلك بفضل الأدوار التي لعبها في العمليات التالية[1]:

- **التنبؤ:**

يساعد الذكاء الاصطناعي بهذا الدور في معرفة وتحديد نوعية الأشخاص القابلين للتأثر بأفكار متطرفة أي المستهدفين المحتملين سواء للجماعات المتطرفة فكرياً أو التنظيمات الإرهابية الحركية وبالتالي يمكن حصر أفراد معينين يمكن تصنيفهم كمتطرفين إرهابيين محتملين[*].

- **التعرف على الإرهابيين:**

عبر استخدام خوارزمية معتمدة على الذكاء الاصطناعي لتحليل البيانات الوصفية لمستخدمي الحواسيب والهاتف المحمولة للتنبؤ بالإرهابيون المحتملين. وبرغم أن النماذج المستخدمة لم تكن فعالة بحد ذاتها، لكنها توضح القيمة التنبؤية للبيانات عند تحديد الروابط الوثيقة مع الظاهرة الإرهابية.

- **الهشاشة والقابلية للتطرف:**

طوَّرت بعض شركات التكنولوجيا أدوات لتقييم قابلية التعرض للأيديولوجيات المتطرفة العنيفة؛ مثل شركة (Jigsaw) التابعة لشركة (Alphabet Inc) "المعروفة سابقاً باسم Google Ideas" التي أعلنت

---

[1] وجدان فهد، "الذكاء الاصطناعي بين التكتيكات الإرهابية والاستراتيجيات الوطنية"، 1 مارس 2022، في:
https://trendsresearch.org/ar/insight/ai-between-terrorist-actics-and-national-strategies/(08|03|2022)

[*] تم تطوير نماذج تتنبأ بموقع الهجمات الإرهابية وتوقيتها. ففي عام 2015 على سبيل المثال ادّعت شركة تكنولوجية ناشئة (PredictifyMe) أن نموذجها، الذي يحتوي على أكثر من 170 نقطة بيانات، كان قادراً على التنبؤ بالهجمات الانتحارية بدقة 72%. كذلك اعتمدت بعض النماذج الأخرى على بيانات المصادر المفتوحة للأفراد الذين يستخدمون الوسائط الاجتماعية والتطبيقات على هواتفهم المحمولة، ومن بينها نظام التعرف على الأحداث في وقت مبكر (EMBERS)، الذي يدمج نتائج مختلف النماذج التنبؤية المنفصلة من أجل التنبؤ بأحداث مثل تفشي الأمراض وأحداث الاضطرابات المدنية. ومن التجارب الملهمة في هذا المجال كانت في عام 2013؛ فقد تم تطبيق نماذج التنبؤ السلوكية لجماعة "عسكر طيبة"، التي كانت مسؤولة عن العديد من الهجمات في باكستان والهند، ووصلت إلى شهرة عالمية مع هجمات بومباي في عام 2008. فبناء على المعلومات المتوافرة وتاريخ هذه الجماعة والحقائق الأخرى عنها، طبق الباحثون قواعد تسمى "الاحتمالية الزمنية" وكان أساس البحث هو النماذج السلوكية، وقد نتج عن البحث بعد ذلك توصيات عدة سياسية للحد من هجمات تلك الجماعة انظر: وجدان فهد، **المرجع نفسه**.

مشروعها باسم "إعادة التوجيه"، الذي يستهدف مستخدمي مواقع مشاركة الفيديو الذين قد يكونون عُرضة للدعاية من الجماعات الإرهابية مثل تنظيم "داعش"، إذ يُعيد المشروع توجيههم إلى مقاطع الفيديو التي تتبنّى رواية موثوق بها ومضادة لرواية التنظيم.

- **التحصين:**

تطوير مساهمة الذكاء الاصطناعي في هذا الاتجاه باستحداث برامج موجهة تقوم بإعادة توجيه أولئك المستهدفين المحتملين إلى مصادر تأثير ومحتوى معلوماتي معين يعمل على ترشيد الأفكار وتقليل احتمالات انتقال الأفراد إلى مصاف الإرهابيين.

- **الملاحقة:**

تسهم تطبيقات الذكاء الاصطناعي في تحديد الجماعة أو الطرف أو الشخص المتورط في العمل الإرهابي سواء بالتنفيذ أو التخطيط وذلك بتحليل المعطيات الخاصة بالعمليات محل التحري، مثل: نوع العملية، والمكان، ونوع السلاح، والهدف، ومطابقة المعلومات مع التاريخ السابق للجماعات أو الأفراد المشتبه بهم، وذلك باستخدام معايير محددة للتصفية والترتيب وتوجد نماذج محددة حققت نسب دقة عالية تجاوزت 80%.

ثالثا: مشروع "سايبر رود" (CyberROAD).

يقوم هذا المشروع على سد الفجوة من خلال جمع شبكة واسعة من الخبرات والتجارب، لمعالجة الجرائم الإلكترونية والإرهاب السيبراني من منظور واسع، ويهدف إلى تحديد الثغرات البحثية اللازمة لتعزيز أمن الأفراد والمجتمع ككل ضد أشكال الجريمة والإرهاب التي تتم عبر الفضاء الإلكتروني وداخله، ويتناول هذا البحث التقنيات الراهنة، مع أخذ بالاعتبار التحدي الرئيس المتصل بالمستقبل، وخاصة ما يتعلق بالتحديات الناشئة عن المزيد من دمج العالم الرقمي في جوانب الحياة التي لا تتصل بالإنترنت، وقد تم تنفيذ المشروع من قبَل عشرين (20) شريكا دوليا في مجال مكافحة الجريمة السيبرانية والإرهاب السيبراني، وهم يمثلون خبرات أكاديمية، صناعية، حكومية وغير حكومية مرموقة من جميع أنحاء أوروبا، ويتمثل

الهدف المحوري من ذلك في تنسيق الجهود الأوروبية لزيادة المرونة السيبرانية وضمان أمثل للأمن السيبراني الأوروبي، والتأسيس لخارطة طريق في هذا الصدد[1].

وتشمل خارطة الطريق التي تم تطويرها داخل مشروع "سايبر رود" جميع الجوانب التي قد تساهم فيتطوير تقنيات أفضل وأكثر قوة لمنع الهجمات السيبرانية واكتشافها والتعافي منها أو احتواء امتداد اثارها (جانب المرونة السيبرانية)، بالإضافة إلى الجوانب القانونية والطب الشرعي فيما يخص مكافحة الجريمة الإلكترونية والإرهاب السيبراني، وصولاً إلى تطوير أساليب أفضل لقياس ولتحليل التهديد وتوعية المواطن بقضايا الأمن السيبراني عموما، وتُعَد خارطة الطريق النتيجة النهائية لعملية جمع المعلومات وتحليلها، من أجل فهم التحديات المستقبلية[2].

رابعا: سوق رقمية واحدة.."أوربة" (Europeanization) مشتريات الأمن السيبراني العامة.

ورثت سوق الأمن السيبراني الأوروبي بعض المشاكل التي تواجه سوق الأمن الأوروبي العام، حيث يعاني سوق الأمن السيبراني في الوقت الحالي من تفتت كبير يرجع جزئياً إلى حقيقة أن الأمن بشكل عام والأمن السيبراني على وجه الخصوص (خاصة كعنصر أساسي في البنية التحتية الحيوية وحماية الأصول الوطنية) يظل من الامتيازات الوطنية. لدى الدول الأعضاء في الاتحاد الأوروبي البالغ عددها 28 دولة لوائح وأساليب مختلفة تجاه الأمن السيبراني بالإضافة إلى مخاوف تتعلق بخصوصية البيانات[3]، غير أن الاتحاد الأوروبي يعمل على دفع عجلة مشروع السوق الرقمية الموحدة الذي أُطلق في 2015 بناءً على ثلاث ركائز هي: الوصول (Access)، البيئة (Envirnment) والاقتصاد والمجتمع (Economy and Society)، وبذلك يهدف إلى تسهيل إجراءات التجارة الإلكترونية، تشجيع المنافسة بين الشركات انطلاقا من معيار الثقة، إلى جانب "تعزيز وصول مواطني الاتحاد الأوروبي إلى السلع والخدمات الرقمية" دون إخلال بمعايير الخصوصية والأمان الشخصي، ليشكل كل ما سبق ذكره بيئة ملائمة للمعاملات الرقمية

[1] Commission Européenne (191804), "Final Report Summary - CYBERROAD (Development of the CYBER crime and CYBER terrorism reseach ROAD map)", 15 Novembre 2016, in: https://cordis.europa.eu/project/id/607642/reporting/fr

[2] ***Idem***.

[3] Nina Olesen, ***Op.cit,*** p 259- 278

داخل الاتحاد الأوروبي مما ينمّي الاقتصاد الرقمي للاتحاد، مع الإشارة إلى فرض نمط جديد من تحرير المعاملات في هذه السوق المستحدثة ألا وهو تحرير البيانات عبر كسر منطق الحدود الجغرافية[1].

يعد بناء سوق رقمية واحدة جزءا أساسيا ولا يقل أهمية ضمن استراتيجية الاتحاد الأوروبي لضمان أمنه السيبراني وتحقيق النضج السيبراني في المستقبل،وهذا المشروع يتطلب إرادة سياسية وأدوات تنفيذ مثل: تعبئة الأموال والموارد، وإنشاء هيكل حوكمة بين الجهات الفاعلة الرئيسَة لضمان التنفيذ الفعال من قبل المؤسسات والدول الأعضاء وأصحاب المصلحة داخل الاتحاد الأوروبي، وستقدم المفوضية الأوروبية مقترحات تشريعية ومبادرات لوضع مقياس السوق الموحدة في خدمة المستهلك، كما يدعو جدول الأعمالالمفوضية والبرلمان والدول الأعضاء إلى العمل معًا واتخاذ خطوات طموحة ترقى بمستوى الأمن السيبراني المرغوب فيه مستقبلا[2].

ولتحقيق ذلك يجب على الاتحاد الأوروبي مواجهة تحديات بناء سوق رقمية واحدة جديرة بالثقة ومرنة عبر الإنترنت، ويأتي على رأس التحديات ما يلي:

- نقص التمويل لشركات الأمن السيبراني الأوروبية مما يعطّل إمكانية توسيع مجالها.
- تجزئة صناعة الأمن السيبراني في أوروبا.
- الاعتماد على مقدمي الخدمات من خارج الاتحاد الأوروبي.
- عدم التوافق بين برامج البحث والتطوير العامة ومتطلبات السوق.
- التجزئة على الصعيد التنظيمي.
- الافتقار إلى متطلبات التقييس والمشتريات المشتركة بالنسبة الدول الأعضاء[3].

---

[1] Raphaël Moncada ,"The European Digital Single Market ", 16/10/2017, in: https://www.eyes-on-europe.eu/the-european-digital-single-market (01/06/2020)

[2] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: ***A Digital Single Market Strategy for Europe***, COM (2015) 192 final. P.17, in: https://cutt.us/EOtjD

[3] Rafael Rivera Pastor & others, Achieving a sovereign and trustworthy ICT industry in the EU, EPRS | European Parliamentary Research Service Scientific Foresight Unit December 2017PE 6 (STOA) 14 .531,in:

تلك الاستراتيجيات مهمة لتأطير مشتريات الأمن السيبراني، بمعنى ما يتعلق بتكنولوجيا المعلومات والاتصالات، مع ضرورة التذكير بأن القطاع العام يظل تقليديا ومستهلَكا في هذا الجانب، وأن الأمن السيبراني يظل مسألة مدنية في المقام الأول، بالرغم من إدراج سياسات الدفاعا السيبراني في الأعوام الأخيرة نظرا لطبيعة وحتمية التهديد، وتؤكد العديد من وثائق السياسة الحديثة في الاتحاد الأوروبي أنه يجب تحسين برامج البحث والتطوير التي لها بُعد مزدوج الاستخدام، والتي تغطي الأمن السيبراني بشكل واضح، ومن المهم أيضا التأكيد على أن برامج الأمن السيبراني التي يمولها الاتحاد الأوروبي تُدار بشكل أساسي من خلال الشراكة بين القطاعين العام والخاص من أجل تحقيق فعالية أكبر[1].

في سياق متصل، تمت الدعوة إلى فرض حظر أوروبي على أجهزة التوجيه الصينية المزيفة بسبب الوجود المفترض "للأبواب الخلفية" وأدوات التجسس التي يستخدمها الإرهابيون عادة كميزة للتخفي. وقد دعت إلى استبدالها بمعدات أوروبية الصنع [2].

ولأجل "أَوربة" المشتريات لتحقيق "أمننة" القطاعات السيبرانية، من الضروري مواصلة العمل بشأن المشتريات الدفاعية، والتي يجب أن تكون متطابقة مع مشتريات الأمن السيبراني، كما هو الحال مع الدفاع والأمن التقليدي، مما يزيد احتمال المنافسة ويحسّنها، وفيما يتعلق بالشراكات بين القطاعين العام والخاص في مجال الأمن العام فهي عنصر محوري ضمن الخطط المستقبلية للاتحاد الأوروبي، وقد وُجدت أدلة على أن مقاولي الدفاع الأوروبيين الكبار (مثل: Thales Group،Selex،Airbus،Indra) قد تلقوا تمويلات البحث والتطوير الممنوحة للقطاع الخاص في المجال السيبراني[3].

وكانت المفوضية الأوروبية قد أعلنت عن إستراتيجية معززة للأمن السيبراني في أوروبا، وهي تقوم على "وضع تدابير وقائية ترمي إلى تعزيز عمل الوكالة الأوروبية للأمن السيبراني من خلال تخصيص

---

https://www.europarl.europa.eu/RegData/etudes/STUD/2017/614531/EPRS_STU(2017)614531_EN.pdf

[1] Jukka Ruohonen, ***Op.cit.*** P-p: 376-377.

[2] Memphis Krickeberg, ***Op.cit .***

[3] Jukka Ruohonen, ***Op.cit.*** p.371

ميزانيات لتشغيل اليات أوروبية منسقة وواضحة المعالم لمكافحة التهديدات المرتبطة بهجوم إلكتروني مستقبلي"، فضلا عن رفع معدل الأمان في الانترنت بالنسبة للمؤسسات الخاصة والصغيرة[1].

المطلب الثالث: إمكانية الوصول إلى النضج السيبراني.

قبل الحديث عن النضج السيبراني تجب الإشارة إلى الجاهزية الإلكترونية التي تعد عاملا أساسيا لقياس القوة السيبرانية للدولة، وهي تعبّر عن مدى استعداد الدولة من حيث مستوى التطور التقني والمعلوماتي وتجسيد الحكومة الإلكترونية، فضلا عن توفّر أُسس وآليات مواجهة الهجمات الإلكترونية ومحاربة التطرف والإرهاب عبر الانترنت، ويتم قياس الجاهزية السيبرانية من خلال العناصر الآتية[2]:

- توفُّر إستراتيجية وطنية تعبّر عن جدية الدولة في التعاطي مع اقتصادها وأمنها، حيث يتم حشد الوسائل والموارد الضرورية لتدعيم الجاهزية الإلكترونية وضمان الأمن السيبراني.
- توافر آليات التصدي والاستجابة للحوادث الإلكترونية، ويكون ذلك عبر فرق الاستجابة لطوارئ الكمبيوتر والتعاون الدولي لاختبار القدرات التشغيلية، وغيرها من الآليات.
- إطار تشريعي قوي ومتناسق يتعلق بالوقاية ومكافحة الجريمة السيبرانية، بما يتماشى والحوكمة وتحولات الجرائم المستحدَثة.
- مشاركة المعلومات بين القطاعات المختلفة وبين أصحاب المصلحة (قطاع حكومي، قطاع خاص، الوكالات المتخصصة، الخ)، ويشمل ذلك المعلومات التي يمكنها الإفادة في مجال تأمين الفضاء السيبراني.
- دور البحث في مجال الأمن السيبراني في تعزيز هذا الأمن، وكمثال ملموس فقد خصّص برنامج Horizon 2020 التابع للاتحاد الأوروبي 80 مليار أورو للبحث والتطوير وتشجيع الابتكار في مجالات متنوعة.

---

[1] "المفوضية الأوروبية تكشف عن اليات حماية الأنظمة الرقمية من تهديدات الهجمات الإلكترونية، 2020/12/17، https://cutt.us/UwOhQ (22|09|2021)

[2] لمزيد من التفصيل في عنصر الجاهزية السيبرانية راجع: ميليسا هاثاواي، مؤشر الجاهزية الإلكترونية، ***مرجع سابق***، ص: 06-31.

- الدبلوماسية السيبرانية عنصر مركزي لا يجب إهمالُه، فهي كفيلة أيضا بإيجاد الحلول لمشكلات الأمن في الفضاء السيبراني.
- الدفاع السيبراني بصورة فعالة، حيث تكون الدولة مستعدة للدفاع عن مصالحها في الفضاء السيبراني وحماية بُناها التحتية الحساسة.

وبالرغم من الدور الكبير الذي تمارسه وكالات الاتحاد الأوروبي للأمن السيبراني في تفعيل جانب الجاهزية السيبرانية، يبقى هنالك تفاوت من حيث النضج على صعيد المرونة السيبرانية واكتشاف والاستجابة للتهديدات، ولهذا توصي المفوضية الأوروبية برفع معدل الاستثمار في الأمن السيبراني داخل الاتحاد الأوروبي لبلوغ مرحلة النضج السيبراني، وهذا بالموازاة مع دعم برنامج "التوعية عبر الانترنت" لتعزيز الثقافة السيبرانية[1]. فالجاهزية السيبرانية لا تتحقق بالصدفة، وإنما بامتلاك مقوماتها وعناصرها، ومن عناصر القوة السيبرانية توفُّر البنية التحتية، وهي بمنزلة الأرضية التي يُعتمد عليها في ممارسة القوة وتشمل: أجهزة الكمبيوتر، شبكات الاتصال، البرمجيات، قاعدة بيانات، يضاف إليها المؤسسات والتشريعات الخاصة بضمان الأمن السيبراني والمتصلة بإستراتيجية مدروسة[2].

وفي إطار سياساته لضمان الأمن السيبراني الأوروبي، يهتم الاتحاد الأوروبي بمستوى أو درجات النضج السيبراني في دوله، وذلك من خلال السعي الدائم إلى رفع المرونة السيبرانية وتنمية قدرات وكالات الأمن السيبراني على مستوى الاتحاد من جهة وعلى مستوى أعضائه (المستوى الوطني) من جهة أخرى.

في هذا السياق، تعد وكالة أمن الشبكات والمعلومات (ENISA) من وكالات الاتحاد الأوروبي الناشطة والمؤثرة والتي تعمل باستمرار على تحسين كفاءتها في إفادة الدول الأعضاء وتبادل المعرفة مع الوكالات الأوروبية في الشأن ذاته، وهي تُصدر بشكل متواصل دراسات رصينة وتقارير تتعلق بالأمن

---

[1] European Commission, The EU's Cybersecurity Strategy in the Digital Decade***, Op.cit***., P.24.

[2] إيهاب خليفة، "Cyber Power: نمط جديد لممارسة التأثيرات غير التقليدية في العلاقات الدولية"، ***دورية اتجاهات الأحداث***، العدد 6 (يناير 2015)، ص4.

السيبراني ومن بينها دراسة مفصلة صدرت في 2015 تتناول موضوع النضج السيبراني في الاتحاد الأوروبي، مع تناول نماذج من المستويات الوطنية (أي بعض الدول من الاتحاد الأوروبي).

يُعرف نموذج تقييم نضج الأمن السيبراني اختصارا بـ: ICS-SCADA، وهو يخص تحديد مستوى هذا النضج في القطاعات الحساسة على مستوى الاتحاد الأوروبي (البنى التحتية الحرجة)، وينقسم إلى ثلاثة أبعاد أساسية كما يلي[1]:

- **البعد التشريعي:** يركز على التقدم الذي تحرزه الدول الأعضاء في الجانب القانوني لتحسين الأمن السيبرانيICS-SCADA.
- **البعد التشغيلي:** يتناول مستوى كفاءة الدول الأعضاء في دعم مقدمي الخدمات المهمة، وكذلك التدابير التي تنمي الوعي وتسهم في مشاركة المعلومات حول الممارسات الجيدة.
- **البعد المحلي:** يركز على فرص وتحديات في مجال تحسين الأمن السيبرانيICS-SCADA ويحدد مجالات التركيز مستقبلا.

يتضح من خلال الأبعاد المحددة أنها تشمل الجانب النظري والعملي، حيث لا يمكن للرؤية الأوروبية أن تتجسد عبر اللوائح والقوانين فحسب وإنما يلاحَظ توفُّر جهد ملموس لضمان الأمن السيبراني ومكافحة الإرهاب الإلكتروني في الوقت نفسه، حيث تعرف السياسات والتدابير الأوروبية تحيينا مستمرا بما يواكب طبيعة التهديد والتحول الذي يطالُه، ولهذا تعد دراسة وتقييم مستوى النضج السيبراني ذات أهمية بالغة سواء بالنسبة للوقت الراهن أو من أجل مستقبل أفضل.

خلال الفترة: 2014–2020 قامت المفوضية الأوروبية بتمويل 47,5 مليون يورو من قدرات الأمن السيبراني في الاتحاد الأوروبي، ومع منتصف 2021 خصصت المفوضية ما يقارب 11 مليون يورو

[1] Rossella Mattioli, Konstantinos Moulinos*, **Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors*** (Greece : ENISA, 2015), P.14.

لتمويل 22 مشروعا يسهم في تعزيز الأمن السيبراني ومحاربة الإرهاب الإلكتروني والهجمات السيبرانية وتدعيم جهود 18 دولة في الاتحاد الأوروبي[1].

كما تم العمل على نموذج أوكسفورد للنضج والمتعلق بقدرات الأمن السيبراني (CMM) المطور في 2016، وهو يتناول تفاوُت المستويات بين الدول من حيث النضج السيبراني بغرض التقييم ورسم السياسات في المستقبل، ذلك من خلال خمسة عناصر (أبعاد القدرات) وعبر خمسة مستويات (ابتدائي، تكويني، قائم، إستراتيجي وديناميكي)، وتتمثل العناصر في[2]:

- إستراتيجية الأمن السيبراني، الثقافة السيبرانية والمجتمع، المهارات السيبرانية (من خلال التعليم والتدريب)، الإطار القانوني– التنظيمي، المعايير، المنظمات والتقنيات.

ويتم تصنيف مستويات النضج السيبراني حسب ما تناولته وكالة الاتحاد الأوروبي لأمن الشبكات والمعلومات إلى[3]:

- **المستوى الأساسي:** حيث لا توجد أنشطة تتصل بقضايا الأمن السيبراني، بما يشير إلى أن الدولة مازالت في طور مبتدئ على صعيد الجاهزية السيبرانية.
- **مستوى التطوير:** تكون الأنشطة قيد التطوير، وهنا تبدأ جهود الدولة في البروز شيئا فشيئا.
- **المستوى الراسخ:** حيث تجرى الأنشطة بانتظام على المستوى الأساسي.
- **المستوى المتقدم:** تُنفّذ الأنشطة "بفهم عميق لمتطلبات ICS-SCADA المحددة".
- **المستوى الرائد:** حيث تُنفّذ الأنشطة في مستوى يتجاوز الحاجات الأساسية الحالية، بمعنى ما هو مرغوب فيه أو كما يجب أن يكون. وتعد إستونيا دولة رائدة ونموذجا متطورا على الصعيد السيبراني، ليس فقط على مستوى الاتحاد الأوروبي وإنما على الصعيد الدولي.

---

[1] "المفوضية الأوروبية تخصص 11 مليون يورو لتعزيز قدرات الأمن السيبراني"، 2021/05/10، (2021/11/15)https://gate.ahram.org.eg/News/2714163.aspx

[2] ميليسا هاثاواي، "مخطط وطني للأمن السيبراني"، مرجع سابق، ص07.

[3] Rosella Mattioli, Konstantinos Moulinos, ***Op.cit.*** p.15.

ويُصنف الملف التعريفي للقائمين والمؤثرين في مستويات نضج الأمن السيبراني الأوروبي (حسب تقرير وكالة الأمن السيبراني الأوروبي) إلى أربعة ملفات مركزية وهي[1]:

- **القادة:**

تتمتع الدول الأعضاء التي تشهد مستويات متقدمة جدا من الأمن السيبراني على صعيد النضج بتواجد نظام قانوني متطور ورؤية إستراتيجية متكاملة وقوية، ويلاحَظ هنا دور القادة الواعي في عملية تحسين النضج السيبراني، هذا في ظل توفر مستوى متقدم من التعاون بين القطاعين عامّ–خاص ومن التدريب والمهارة السيبرانية (خبرات الأفراد العاملين والوكالات المتخصصة)، وأيضا دور البحث الأكاديمي وانفتاح القادة أنفسهم على تبادل المعرفة والمعلومة ومشاركة الخبرات الذاتية الناجحة، بالتالي يمكن القول إن الدول الأعضاء تتمتع –انطلاقا من هذا الملف التعريفي– بمستوى متقدم جدا من الأتمتة والرقمنة وبالتالي مستوى عال من النضج السيبراني.

- **الفئات المؤيدة:**

تشمل الدول الأعضاء التي تزوّد مشغّلي البنية التحتية الحرجة بالأدوات الضرورية لتحسين مستوى الأمن السيبرانيICS-SCADA، ويبرز هنا الدعم الحكومي والشراكة عام– خاص، بالإضافة إلى دور مراكز البحث، فانطلاقا من منصات لتبادل المعلومات "يتم تطوير تدابير استباقية بالتعاون الوثيق للغاية مع أصحاب المصلحة الداخليين (الحكومة ومشغلي CI) والخارجيين (الأكاديميين والوكالات الخاصة)"، بالتالي تركز الدول الأعضاء على "بناء الوعي الأمني"ICS-SCADA عبر المعرفة والتدريب.

- **المؤيدون التفاعليون:**

يشير هذا الملف التعريفي إلى عملية التفاعل في إطار تحسين نضج الأمن السيبراني الأوروبي، فيتم بذلك العمل على تجاوز عوامل الضعف، وتلعب عناصر التوعية والثقة ومشاركة الممارسات الجيدة دورا هاما في هذا الصدد.

---

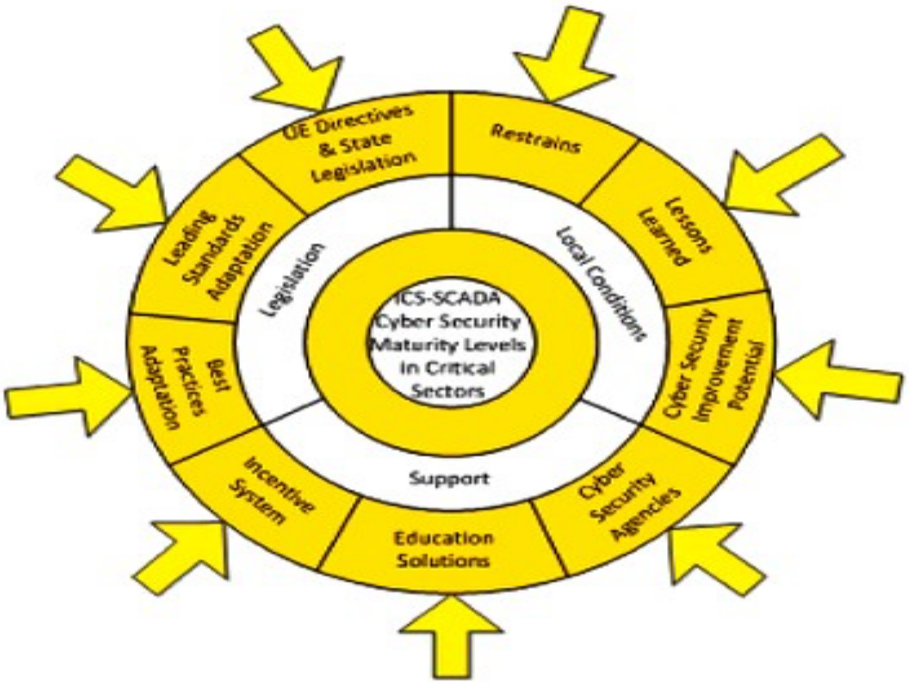
[1] ***Ibid***, P-p: 17-23.

- **المطورون الأوائل:**

ويضم هذا الملف التعريفي الدول الأعضاء التي تعرف مستوى نضج ابتدائي أو منخفض مقارنة بغيرها، حيث تتراوح مدة إطلاق التشريعات المتعلقة بالأمن السيبراني من سنتين إلى ثلاث سنوات، وهو مستوى متأخر كما يلاحَظ، ويميزه أن الشراكة بين القطاعين العام والخاص مثلا في مراحلها الأولى، كما أن الخبرة ضئيلة وبالتالي فإن هذه الدول بحاجة إلى وعي أكبر وتكريس للممارسات الجيدة.

ويسمح تقييم مستوى النضج السيبراني في الاتحاد الأوروبي وعلى مستوى أعضائه بالوقوف على نقاط القوة ونواحي الضعف المختلفة، سواءٌ تعلّق الأمر بالجانب التشريعي (القوانين) أو الممارسات والتدابير التي تلتزم بها وكالات الاتحاد الأوروبي بالتنسيق والتعاون فيما بينها.

الشكل (22): أبعاد نموذج نضج الأمن السيبرانيICS-SCADA



Source: Rossella Mattioli, Konstantinos Moulinos, ***Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors*** *(Greece : ENISA, 2015),* P.14.

وتقدم وكالة الاتحاد الأوروبي للشبكات والمعلومات (ENISA) توصيات أساسية لتحسين حالة النضج السيبراني في الدول الأعضاء، يمكن اختصارُها في الأفكار الآتية[1]:

– العمل على تطوير السياسات الرامية إلى ضمان أمن البنى التحتية الحرجة، حيث يبقى الهدف المحوري للاتحاد الأوروبي هو رفع مستوى الأمن والأمان السيبراني وبلوغ مرحلة متقدمة جدا من النضج السيبراني.

– العمل على تطوير ممارسات جيدة خاصة بالأمن السيبراني، ويمسّ ذلك أدوارا متعددة للشراكة عام– خاص وللوكالات الأوروبية المتخصصة.

– توصي الوكالة ب "توحيد تبادل المعلومات بين القطاعات الحيوية والدول الأعضاء"، ويجب التذكير هنا بأن تبادل المعلومة ومشاركة الممارسات الجيدة والعمل على تطويرها من الأمور الضرورية لضمان أمن البنية التحتية الحرجة المتصلة بالفضاء السيبراني، يضاف إلى ذلك "تعزيز نهج مشترك للإبلاغ عن حوادث الأمن السيبراني والممارسات الجيدة".

– تسمى هذه التوصية ب "بناء الوعي الأمني السيبراني"، حيث يجب التأكيد على سلطات الدول الأعضاء (دور صانعي القرار وواضعي السياسة).

– تعزيز الخبرة عبر التدريب وبرامج التعليم، وهو أمر ضروري لتعزيز الأمن السيبراني الأوروبي.

– الحاجة إلى مزيد من الأنشطة المتعلقة بالبحث والتطوير والتقييم، ويشمل ذات تطوير الجانب الفني أو التقني.

من كل ما سبق، يتضح أن الوصية النضج السيبراني عملية مرحلية طويلة تحتاج إلى تدابير وسياسات عديدة ومتناسقة، بغرض الوصول إلى هدف النضج. ويعد التأسيس لوعي أمني سيبراني بالنسبة للفرد وللسلطات على حد سواء نقطة محورية في سبيل بلوغ مرحلة النضج السيبراني، وتلعب عملية التوعية والتثقيف عبر القنوات المتنوعة دورها في هذا الجانب.

[1] ***Ibid***, p-p: 36-37.

خاتمة الفصل واستنتاجاته:

على إثر هجمات 11 سبتمبر 2001 في الولايات المتحدة الأمريكية، أصبح الإرهاب في مقدمة التهديدات الأمنية التي تواجه الدول الأوروبية، فعمل الاتحاد الأوروبي على تطوير إستراتيجية مدروسة من جميع النواحي، فعلى صعيد الرؤية، هناك إستراتيجية وإدراك أمني لطبيعة التهديد في الفضاء السيبراني، ويشمل ذلك جانب التشريع (الإطار القانوني) والتنفيذ (سياسات الحوكمة والتعاون الدولي والدفاع السيبراني)، بالإضافة إلى وجود تصور على المدى المتوسط والبعيد لما يجب أن تكون عليه حالة الأمن السيبراني في الاتحاد الأوروبي، وصولا إلى مستويات متقدمة من النضج السيبراني ترسيجا لثقافة سيبرانية شاملة للمجتمعات والحكومات الأوروبية.

تنطلق رؤية الاتحاد الأوروبي للأمن السيبراني من الاهتمام بتنظيم أربعة مجالات أو موضوعات، يشمل ذلك السوق الداخلية للأمن السيبراني حيث يتم العمل على تنظيمها بغرض الوصول إلى مرحلة الأمان في القدرات التشغيلية ونشاطات التجارة الإلكترونية والمعاملات الرقمية، بالإضافة إلى إنفاذ القانون حيث عمل الاتحاد الأوروبي على إنشاء منظومة قانونية تخص المجال السيبراني، يتم تحديثها باستمرار لتواكب وتعزز قدرات الأمن والدفاع السيبراني للاتحاد، كما تحظى الدبلوماسية الرقمية باهتمام واسع باعتبارها الوجه المقابل للدفاع السيبراني (وهو المجال الرابع). وعليه، تمتزج المجالات أو الأبعاد الأربعة المذكورة لتحقيق السيادة والمرونة في الفضاء اللامادي، والنهوض بفضاء إلكتروني عالمي ومفتوح من خلال التكريس لتعاون دولي (داخل الاتحاد الأوروبي وخارجه) يحقق قدرا من الأمن والأمان للجميع في الفضاء السيبراني.

استنادا إلى ذلك، تنطلق أولويات الاستراتيجية الأوروبية لمكافحة الإرهاب السيبراني من[1]:

- تعزيز أداء المؤسسات الرسمية وغير الرسمية لحماية الفضاءين المادي والسيبراني.
- حماية البنية التحتية المادية والرقمية لضمان النفاد إلى الخدمات الأساسية.

[1] جاسم محمد، "استراتيجيات مكافحة الإرهاب والتطرف في الاتحاد الأوروبي– الوقاية والمقاضاة والحماية"، 2021/10/22، https://bit.ly/3nZU/a4 (2022/11/10)

- دعم منظومة الدفاع السيبراني وتعزيز المرونة.

وانطلاقا من ذلك يمكن تقديم الاستنتاجات الآتية:

- قطع الاتحاد الأوروبي أشواطا كبيرة في وضع إستراتيجية للأمن السيبراني ترتكز على أدوات الحوكمة والشراكة بين القطاعين العام والخاص، وتنسيق سياسات الدول الأعضاء وتدعيم الجاهزية السيبرانية، وكانت إستراتيجيات الأمن السيبراني للاتحاد الأوروبي منذ 2013 (إستراتيجية 2013، 2017 ثم 2020) معبّرة عن تحولات البيئة الأمنية في الفضاء السيبراني وضرورات التكيف ووضع الأولويات من أجل حماية هذا الفضاء بشكل يحقق أمنا أكبر، وفي الوقت ذاته لا يمسّ بالحقوق والحريات الأساسية للمواطن. ويهتم الاتحاد الأوروبي بالمرونة السيبرانية بوصفها نقطة الوصل بين حشد القدرات والموارد ومكافحة الهجمات السيبرانية والإرهاب الإلكتروني بصورة فعالة.

- ركزت استجابة الاتحاد الأوروبي على رفع معايير مرونة البنية التحتية للاتصالات الحساسة لمنع الهجمات الإلكترونية المحتملة، استجابة كانت مدفوعة بالمخاوف الأمنية المتعلقة بالهجمات الافتراضية ذات الأصل الإرهابي والتي يغذيها التطرف.

- يهتم الاتحاد الأوروبي بالتعاون الدولي في مجال تأمين الفضاء السيبراني ومكافحة الإرهاب الإلكتروني، ويتفق في ذلك مع رؤية وأهداف الاتحاد الدولي للاتصالات والرؤية الأممية القائمة على دعم مناخ التعاون الدولي في مجال تسليم المجرمين والإرهابيين والتدريب على مكافحة الإرهاب السيبراني. فالتعاون الدولي لا يمكن الاستغناء عنه في عصر العولمة وفي ظل ضرورة تقاسُم أعباء التهديدات الأمنية التي تحدث عبر الفضاء الرقمي، ومع ذلك تظل مسألة عدم الاتفاق على تعريف واحد وشامل للإرهاب الإلكتروني من بين المعوّقات التي تقف في وجه الدول والحكومات في سياق الجهود المتواصلة لمحاربة هذا النمط من الإرهاب الجديد.

- سعى الاتحاد الأوروبي إلى تشكيل منظومة دفاع سيبراني متميزة، عبر حشد كل ما توفَّر له من موارد ووسائل، وعبر وضع سياسات وتوجيهات وتعزيز المنظومة القانونية في مجال الأمن السيبراني الأوروبي، ولا ينفصل ذلك عن التعاون مع حلف شمال الأطلسي. وبالرغم من التحليلات التي ذهبت إلى أنه لا وجود لمنظومة دفاعية حقيقية وفعالة لأوروبا خارج إطار حلف الناتو، يمكن القول إن منظومة الأمن

والدفاع السيبراني للاتحاد الأوروبي تتعزز وتكتمل جنبا إلى جنب مع الدفاع الحربي للناتو وسياساته للدفاع السيبراني، وهذا انطلاقا من أهمية التعاون بين المنظمتين (الاتحاد الأوروبي والناتو) وتبادل الخبرات وتنسيق السياسات من أجل "**أوروبا آمنة ومستقرة سيبرانيا**".

– يتميز الاتحاد الأوروبي والمؤسسات التابعة له بوجود رؤية تخص ملء الفراغ القانوني في الفضاء الرقمي، ولكن تبقى التدابير التقنية والإجرائية التي يتوخى الاتحاد الأوروبي الالتزام بها في إطار سياسات حماية المجال السيبراني ومكافحة التهديدات السيبرانية، بما فيها الإرهاب الإلكتروني، تواجه تحديات عديدة مثل:

– لا يوجد اتفاق بين أعضاء الاتحاد الأوروبي حول تعريف موحد للدفاع السيبراني، وهي مشكلة قد تجعل هذا الدفاع محدودا. كما لا يوجد اتفاق فعلي حول تعريف الإرهاب الإلكتروني حيث هنالك صنفان تم التطرق إليهما في الفصل الأول من الدراسة: إرهاب إلكتروني محض، وآخر هجين يرتبط بأساليب نشر التطرف والكراهية عبر الانترنت والفضاء السيبراني عموما.

– طبيعة أو خصوصية الفضاء الإلكتروني في حد ذاته، حيث تعد طبيعة هذا المجال ميزة وفي نفس الوقت تحدّ للحكومات الراغبة في حماية الأمن السيبراني، دون الإخلال بحرية الفرد واختراق خصوصيته، بالإضافة إلى أن الإرهابيين يجدون ملاذا آمنا أو شبه امن داخل هذا الفضاء، يجعلهم يتحركون وينشطون ويخططون، مع سهولة التخفي وحذف الأثر، مما يصعّب المهمة أمام الحكومات الأوروبية للتحكم في ظاهرة الإرهاب الإلكتروني.

– إلى جانب التكامل والتفاعل ما بين وكالات ومؤسسات الاتحاد الأوروبي المختصة في الأمن السيبراني (إضفاء الطابع المؤسسي على الأمن الأوروبي)، وما يتخلل ذلك من تبادل الأدوار وتفعيل الشراكة والتعاون بين القطاعين العام والخاص، يمكن تسجيل تحدّ يتعلق بالضعف المسجل على مستوى بعض دول الاتحاد الأوروبي من حيث الإطار القانوني والإجرائي والقوة السيبرانية عموما، حيث مازالت تعاني ضعفا أو هشاشة سيبرانية.

– أهمية الردع السيبراني تظل محدودة، بالرغم من الحضور البارز لإستراتيجية الردع في تحقيق الاستقرار والأمن الجماعي لدول الاتحاد الأوروبي، ويرجع ذلك إلى عدم توفر شروط الردع بصورة كلية –

إلا نادرا– وهي: معرفة المهاجم (العدو) ومصدر أو موقع الهجوم، وهذا شرط أساس لتحديد متطلبات الاستجابة وبناء الإستراتيجية والقدرات انطلاقا من طبيعة العدو وخصائصه، بالإضافة إلى عنصر الشفافية بمعنى إدراك الخصم لقدراتك السيبرانية أو العكس، وهو ما يسمح بردع الهجوم واحتوائه بناءً على قراءة أولية لهذه القدرات[1].

– يؤكد المختصين في الشأن السيبراني الأوروبي أن الإرهاب السيبراني "المحض" لم يتحقق بعد، في أوروبا أو خارجها، ولذلك يتم التركيز على مواجهة التطرف من خلال الانترنت وشبكات التواصل الاجتماعي، والذي يراد من ورائه تحفيز الفعل الإرهابي على أرض الواقع[2]. بالإضافة إلى أن سياسات الأمن السيبراني في الاتحاد الأوروبي عموما تتعلق بمواجهة الهجمات السيبرانية وحماية البنية التحتية الحرجة بصورة أساسية، في حين تظل سياسات مكافحة الإرهاب الإلكتروني بحاجة إلى جهود أكبر خاصة على صعيد المَأسسة والتشريع.

ويبقى رسم خرائط طريق للمستقبل السيبراني في أوروبا متوقفا على عدد من العوامل من ضمنها مستوى الشراكة بين القطاعين العام والخاص، ومستوى النضج الذي بلغه الاتحاد الأوروبي في مكافحة الإرهاب الإلكتروني وأشكال التهديدات السيبرانية الأخرى، ومن جهة أخرى، التحديات التقنية والفنية والتشريعية التي مازالت تواجهه والتي يجري العمل على التقليل منها وفق منهجية مدروسة انطلاقا من عدة مشاريع تم التطرق إليها في هذا الفصل.

---

[1] حمدون إ.توريه، ***مرجع سابق***، ص: 89–90.

[2] Dennis Broeders, and Others, « Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy », 02/06/2021, https://www.tandfonline.com/doi/full/10.1080/1057610X.2021.1928887 (15/11/2021)

خـــاتمـــة

الخاتمة:

لقد كان خلق السلام والأمن في أوروبا والحفاظ عليهما طموحًا ثابتًا وأساسيًا للمشروع الأوروبي خاصة مع بروز تهديدات جديدة كالإرهاب السيبراني، التهديد الذي تبين في النهاية أنه أكثر تعقيدًا من الفكرة التي لدينا عنه في البداية، نظرًا لأبعاده المتعددة.

ومع ذلك، ومن وجهة النظر هذه، يبقى الإرهاب السيبراني أحد أعراض البيئة الإستراتيجية الجديدة، بكل ما تحمله من تحولات اجتماعية وسياسية وتقنية وأمنية أفرزها عالم ما بعد هوبز، حيث يتضاعف الفاعلون ويتحدون لوضع إستراتيجيات عالمية وأخرى محلية. فهو عالم تتعارض جغرافيته مع المناطق ومع الشبكات، وتتقاطع فيه تمثيلات بعض "الدول" وآخرين (الأفراد) على طول خطوط مجزأة، بعيدة كل البعد عن النطاق الموحد لإيديولوجيات الماضي والتي عملت على بناء شخصية "الإرهابي". فهو إذًا عالم تكون فيه التهديدات في نهاية المطاف منخفضة، ولكن نقاط الضعف كبيرة، مما يجدد الجدل التقليدي حول الأمن.

اعتبارا من ذلك، أصبح الإرهاب السيبراني مصدر قلق متزايد للمجتمع الدولي برُمّته، خاصة وأنه يربط الإرهاب كظاهرة بالتطور التقني والمعلوماتي ليفرز نمطا جديدا من التهديد قد يكون أكثر خطرا، خاصة مع الاستخدام المتزايد لأجهزة الحاسوب والهواتف الذكية ولشبكة الإنترنت. وهناك حتماً جانب إقليمي ودولي في هذا الموضوع، فالأنشطة الارهابية الإلكترونية في تزايد مستمر، وهي تؤثر سلبًا في تطور المجتمع والاقتصاد الأوروبيين، وتؤثر بشكل كبير في البنية السوسيو–اقتصادية والأمنية الأوروبية، بالرغم من زيادة مستوى الوعي بالتهديدات السيبرانية، وأعمال إنفاذ القانون على مستوى أوربا والعالم لمكافحتها. والنظام الحالي للقوانين والمعايير والتعريفات الدولية للإرهاب السيبراني لا يفي بالغرض بخصوص تشكيل إطار جادّ لمكافحة الإرهاب السيبراني وحماية الأمن السيبراني للدول، بل إنه في الواقع يزيد من مخاطر التهديد من خلال تشكيل منطقة رمادية أو فجوة يمكن أن يستغلها الإرهابيون السيبرانيون.

إن مصطلح "الإرهاب السيبراني" مصطلح جدلي، لا يحظى لحد الآن باتفاق حول تعريفه وتحديد مؤشراته النظرية والإجرائية، مما يعكس الحاجة إلى تعريف مشترك بين الدول وإن كان المجتمع الدولي حتى الآن غير قادر على الوصول إلى تعريف مشترك، شامل ودقيق لمصطلح "الإرهاب" بحد ذاته.

ويمكن حصر استخدامات الإنترنت لأغراض إرهابية فيما يلي[1]:

- تنفيذ هجمات إرهابية عن طريق تغيير المعلومات على أنظمة الكمبيوتر (عن بُعد).
- تعطيل تدفق البيانات بين أنظمة الكمبيوتر.
- استخدام الإنترنت كمصدر للمعلومات، أو كوسيلة لنشر المعلومات المتصلة بالنشاط الإرهابي.
- كوسيلة لدعم المجتمعات والشبكات المخصصة إما لملاحقة أو دعم أعمال الإرهاب.

وقد زادت هجمات الحادي عشر سبتمبر 2001 من شدة الجدل حول قضية "الإرهاب الإلكتروني" بين الباحثين الأكاديميين وصانعي السياسات والصحافة أيضا. ومع ذلك، فإن عدد الهجمات التي يمكن وصفها بأنها "إرهاب إلكتروني" لا يزال قليلا مقارنة بالهجمات السيبرانية الأخرى على غرار القرصنة والتخريب، وهذا وفقًا للعديد من الخبراء، يقودنا هذا إلى أن الإرهاب السيبراني كظاهرة قد تم تضخيم دورها وتأثيرها تبعا لتأثيراتها لحد الآن، والإرهاب الالكتروني كمفهوم أمني أخذ أهميته في الاهتمام به وتضخيمه أيضا. ولكن، وبالرغم من أن هجومًا إلكترونيًا إرهابيا واسع النطاق لم يحدث بعد، الا أنه لا يمكن تقليص الاهتمام بهذا التهديد الأمني الخطير، لسببين أولهما أن تضخيم هذا التهديد هو بمثابة آلية لمواجهته وجزء من الاستجابة عبر ما يسمى بتفعيل آليات الإنذار المبكر، وثانيهما لأن التطور في تكنولوجيا المعلومات والاتصالات مستمر ومتسارع، وبالتالي فإن احتمال وقوع وانتشار هجمات الإرهاب السيبراني يبقى وارد جدًا، ولهذا يعكف الاتحاد الأوروبي من خلال سياساته ومؤسساته ووكالاته المختصة في الأمن السيبراني والتحديث الدائم لقوانينه ولوائحه التنظيمية، على مواكبة التطور التقني من جهة والتطور في نمط ومستوى التهديدات السيبرانية من جهة أخرى، وفي مقدمة تلك التهديدات يَبرز الاهتمام بمكافحة الإرهاب السيبراني.

فعلى مستوى الدول والحكومات الأوربية، بات يُنظر إلى الأنترنت بشكل متزايد كأحد الأصول الإستراتيجية التي يجب استغلالها لأغراض الأمن القومي، وربما ساحة معركة أيضا حيث يمكن أن يكون الصراع الاستراتيجي في أعلى مستوياته من خلال شنّ حرب إلكترونية واسعة، والملاحظة المركزية التي وَجَب التنبيه إليها هي أن الاعتماد المتزايد على البنية التحتية لتكنولوجيا المعلومات والاتصالات يخلق نقاطَ ضعف وفرصًا لاستغلالها من قبل الإرهابيين، وتحتفظ تكنولوجيا المعلومات والاتصالات بوظيفة

[1] Report of the Working Group on Countering the Use of the Internet for Terrorist Purposes, ***Op. Cit.*** p.8.

تمكينية متزايدة الأهمية بالنسبة للجرائم الخطيرة والمنظمة والتطرف الأيديولوجي والسياسي، وربما حتى العدوان الذي ترعاه الدولة.

انطلاقا من كل ذلك، يمكن القول إن الاتحاد الأوروبي يواجه مجموعة من التحديات المتصلة بالاستخدام غير المشروع لتكنولوجيا المعلومات والاتصالات، وفي مقدمتها الأنشطة الإرهابية المتصلة بالتكنولوجيا والانترنت، مما يفرض نمطا معينا من التنسيق بين الدول الأعضاء وبذل مزيد من الجهود (في إطار الاتحاد وخارجه) لمكافحة الإرهاب السيبراني.

وبالتاني، ساهمت الفصول الثلاثة من هذه الأطروحة في تمحيص واختبار فرضيات الأطروحة في مشكلة البحث، ويمكن التأكيد على أن الاستجابة الأمنية الأوربية السيبرانية مرتبطة بوجود تأثير استراتيجي للإرهاب السيبراني والذي فرض تغيرات إستراتيجية على منظومة الأمن والفكر الأمني الأوروبي. وتأسيسا على ذلك تخلُص الدراسة إلى عدد من الاستنتاجات المحورية وهي كالآتي:

- لقد أتاحت الهندسة الأصلية للإنترنت للإرهابيين استخدامها لتفادي المطاردة الأمنية، ولأغراض التواصل والتجنيد والتنظيم، ويمكن وصف الإنترنت بأنها "معسكر تدريب افتراضي" للأفراد ليصبحوا متطرفين فكريا ثم إرهابيين عمليا، كما يمكن الاستفادة من "عُقد الشبكات" وبالتالي تعطيل الحياة الاقتصادية والاجتماعية وتحقيق أضرار جسيمة للبنية التحتية الأوروبية الحرجة، إلى جانب الاستفادة من الطبيعة "الشبكية" و"المفتوحة" لمجتمع المعلومات المعاصر مما يشكل نقاط ضعف جديدة و"أهدافاً سهلة" للإرهابيين.
- الهجمات الإرهابية الالكترونية قد تكون آلية من آليات التستر عن حرب الكترونية، فالدول قد تدعم الجماعات الإرهابية جهادية كانت أم انفصالية راديكالية لخوض حرب بالوكالة لتحقيق أهدافها السياسية.
- نظرًا لأن الإرهاب السيبراني يستخدم وسائل التواصل الاجتماعي لاستهداف الأفراد الذين لديهم إمكانية الوصول إلى الإنترنت، فمن الضروري أن يتم تدريب المواطنين على التعرف على المخاطر المحتملة ومعرفة أفضل السبل للإبلاغ عن أعمال الإرهاب السيبراني. وتعد برامج وحملات توعية المواطنين بقضايا الأمن السيبراني مهمة في تشكيل ثقافة سيبرانية شاملة، ويجب على المنصات الشهيرة مثل فيسبوك وتويتر ويوتيوب التفكير في تعزيز قدرتها على تحديد وإزالة المحتوى المتطرف والإرهابي، بناءً على طلب الوكالات الأوروبية المختصة في الأمن السيبراني، وبناءً على روح المسؤولية.

- بما أنه من المرجح أن يزداد الإرهاب في الفضاء السيبراني تماشيا مع درجة التقدم التكنولوجي، يجب بذل جهود بحثية مستقبلية لتوثيق وتحليل أنشطة الإرهاب السيبراني المختلفة بلغات عديدة، تفاديا لقصور المعلومة، وتعزيزا لمخاطبة جمهور واسع على المستوى العابر للأوطان، وأيضا تكريسا لمستقبل سيبراني آمن يشارك فيه جميع الباحثين من جميع الأوساط الأكاديمية.
- إن الحدود الجغرافية للإرهاب السيبراني تتجاوز حدود الدول القومية، وبالتالي ينبغي النظر في بذل جهد شامل وجماعي بشأن التدابير المقيدة لأنشطة الإرهاب السيبراني. هنا تبرز أهمية التعاون الدولي التي يؤكدها الاتحاد الأوروبي، باعتباره عنصرا أساسيا لا غنى عنه في مكافحة التهديدات السيبرانية والإرهاب الإلكتروني. ويسعى الاتحاد الأوروبي إلى توسيع دائرة التعاون في مجال الأمن السيبراني، بهدف تبادل المعلومات المهمة والخبرات وتوسيع نطاق التدريب في مكافحة الإرهاب الإلكتروني والجريمة السيبرانية. وتعد الشراكة مع حلف شمال الأطلسي (الناتو) في المجال السيبراني مفيدة جدا، خاصة وأن الحلف قد أدرج منذ سنوات الدفاع السيبراني ضمن منظومته الدفاعية الحربية، هذا إلى جانب الاتحاد الأوروبي الذي عمل هو الآخر على تكريس سياسة دفاع سيبراني أوروبية عبّر عنها في إستراتيجيته للأمن السيبراني لعام 2013.
- تتمثل طبيعة الأنترنت في كونه "نظام غير ويستفالي"، غير أن الدول الأوروبية قطعت شوطًا كبيراً في مواجهة الإرهاب عبر الإنترنت من خلال مكافحة المحتوى المتطرف، والتصدي للهجمات المحتملة، لكن على الرغم من الجهد الأوروبي المبذول في مكافحة الإرهاب السيبراني يظل الأمر صعبا بالنظر إلى محدودية المواجهة والاستجابة، كما أن تتبع الجماعات المتطرفة والتنظيمات الإرهابية عبر الأدوات الإلكترونية المتطورة تظل بحاجة إلى جهد أكبر خاصةً مع تطور أساليب العمل الإرهابي المعتمد على الفضاء السيبراني والدعاية عبر الانترنت[2]، هذا من ناحية، ومن ناحية أخرى نظرا لعدم وجود نهج واحد متكامل لمعالجة مسألة "استخدام الإنترنت لأغراض إرهابية".
- أثبتت الدراسات والتقارير الأوروبية أن الإرهابيين في أوروبا يهتمون باستخدام الإنترنت لأغراض إرهابية، وذلك سواء بالنسبة لجماعات الإرهاب الجهادي كما تسمى أو بالنسبة لجماعات اليمين المتطرفة، وقد أثبتت حالات كثيرة حدوث هجمات إرهابية أياما قليلة بعد نشر هذه الجماعات لخطاب الكراهية والتحريض عبر وسائط التواصل الاجتماعي مثل فيسبوك وتويتر.

[2] حسن سعد عبد الحميد، مرجع سابق.

- شكلت بعض الشواهد التاريخية لحالات استخدام الإرهابيين للأنترنت كوسيلة او كهدف تصورا مفاده أن تبلور الخطاب الأمني المتعلق بالإرهاب السيبراني تدريجيا في قاموس الاتحاد الأوروبي، وهي الصلة بين خطاب التهديد والممارسات المترابطة التي شرعها أو سُنَّت ردًا عليه.
- بدأ الإبلاغ عن تهديدات الإرهاب السيبراني للدول الاوربية بالظهور في تقارير اليوروبول بوتيرة أكبر، كانت اخطرها التهديدات الإرهابية الجهادية، الا ان هناك صور اخرى مثل "الإرهاب الانفصالي" و"الإرهاب اليساري" و "الإرهاب اليميني".
- ان الأمننة الجماعية للاتحاد الأوروبي للفضاء السيبراني مدعومة مثلها مثل استجابات الاتحاد الأوروبي للإرهاب، من خلال ثلاث مبادئ منفصلة، ولكنها مترابطة على مستوى الاتحاد الأوروبي: الحرية والعدالة والأمن؛ السوق الداخلية؛ وسياسة الأمن والدفاع المشتركة.
- على الرغم من استمرار المشكلات المتعلقة بتنفيذ السياسة في هذا المجال السيبراني، الا أنه لا يزال من الممكن وصف الاتحاد الأوروبي بأنه جهة فاعلة إقليمية استثنائية في القضايا السيبرانية.
- لم يثبت لحد الان وجود تهديد للهجمات السيبرانية على أي بنية طاقوية أو عسكرية أوربية، لكن يشير بعض الباحثين إلى أنه تم التذرع بتهديد الإرهاب السيبراني لهذه البى عبر مؤسسات الاتحاد الأوروبي وهياكله الاقتصادية والأمنية كجزء من عملية إعادة إضفاء الشرعية على الحاجة إلى مشاركة عموم أوروبا في تأمين البنية التحتية الحيوية.
- بالرغم من أن الاتفاقيات الأوروبية تؤسس لحماية حقوق الإنسان والحريات، وأنها من صميم المجتمع الديمقراطي الأوربي، لكن الممارسات الأمنية الحكومية تعكس ازدواجية المعايير بمخالفتها لذلك في كثير من الأحيان، حيث لا تزال هناك فجوة كبيرة بين الخطاب والقيم الأوروبية وبين الممارسات الفعلية لمؤسسات انفاذ القانون في أوروبا، بين الدور المنشود للاتحاد الأوروبي كفاعل أمني موحد وبين التطورات المنفذة لحماية هذا الغرض.
- يهتم الاتحاد الأوروبي بتعزيز الشراكة مع القطاع الخاص، حيث يلعب أصحاب المصلحة غير التقليديين دورًا مهمًا في حماية البيانات وتقديم الضمانات لإجراءات الحماية السيبرانية، وفي وضع معايير المحتوى المقبول.
- تعتبر الإجراءات الوقائية بشأن الهجمات الإرهابية الإلكترونية مهمة جدا في سياق تأمين الفضاء السيبراني الأوروبي، ولهذا سعى الاتحاد الأوروبي، مجتمِعًا وعلى مستوى دوله الأعضاء، إلى تعزيز السياسات الواقية من التطرف عبر الانترنت وأنشطة الإرهاب السيبراني، وتعد بريطانيا مثلا دولة

رائدة في استحداث أنظمة الكشف المبكر والتحقق من المحتوى الإرهابي عبر المنصات الرقمية، وفي الجهة المقابلة تعد استونيا رائدة ومتقدمة على صعيد التأسيس لمنظومة دفاع سيبراني شاملة.

- إن مدارسة حوكمة الأمن في الاتحاد الأوروبي كمشكلة عمل جماعي وفق تحليل المنتج المشترك تجعلنا نخلص إلى أن الدول الأعضاء الأصغر في الاتحاد الأوروبي ليست حرة في رؤية سياسات الأمن الجماعي، على عكس إحدى الفرضيات المركزية في أدبيات الاختيار العام التي توضح أن الدول الأعضاء في الاتحاد الأوروبي في الواقع تتقاسم التكاليف بالتساوي مع الأبعاد المختلفة للحوكمة الأمنية.
- لا يزال الجانب التشريعي فيما يتعلق بقضايا الأمن السيبراني ومكافحة الإرهاب الإلكتروني قاصرا، تواجهه التحولات المستمرة في أساليب العمل الإرهابي والاستفادة من تقنيات الذكاء الاصطناعي، ولكن لا يمكن إنكار أهمية الجهود الحثيثة المبذولة على مستوى الاتحاد الأوروبي من أجل تكييف المنظومة القانونية داخله مع تطور نمط التهديد الأمني، وتكييف التشريعات الوطنية في المقابل.
- ركزت سياسة الاتحاد الأوروبي لمكافحة الإرهاب السيبراني على التدابير الأمنية الداخلية والخارجية التي تم الاتفاق عليها بين الدول الأعضاء للاتحاد ومع الشركاء والفاعليين الدوليين، البعد الداخلي لاستجابة الاتحاد الأوروبي ارتكز على القدرات المؤسسية للاتحاد الأوروبي من حيث نهجها في "إدارة التهديد الإرهابي"، حيث سلطت الضوء على العديد من مجالات العدالة وسياسة الشؤون الداخلية حيث زادت كفاءات الاتحاد الأوروبي في مكافحة الإرهاب، بما في ذلك التعاون بين الشرطة والقضاء، وتبادل المعلومات، والهجرة ومراقبة الحدود.
- تبقى مسألة النضج السيبراني متوقفة على عدد من العوامل والتحديات، فدول الاتحاد الأوروبي متفاوتة مثلا من حيث الجاهزية السيبرانية ودرجة المرونة السيبرانية، ولكن هذا لا ينفي مساعي التنسيق وجهود الوقاية والدفاع السيبراني داخل الاتحاد.
- لن يكون من المعقول توقع القضاء على جميع التهديدات الإلكترونية بشكل دائم: فالتهديدات متنوعة ومتطورة باستمرار، وسيكون من المستحيل تصفية الاستخدام الإجرامي أو العدائي (الفعلي أو المحتمل) للبنية التحتية الأوربية لتكنولوجيا المعلومات والاتصالات. ويعزى هذا الوضع جزئياً إلى الاعتماد الواسع النطاق على تكنولوجيا المعلومات والاتصالات.

خلاصة القول، تبقى الجهود الأوروبية في سياق تنظيم الفضاء السيبراني وبناء منظومة مؤسساتية وقانونية رادعة، معتبرة، خاصة بالنظر للتحول السريع في نمط التهديدات السيبرانية، فضلا عن عدم توفُّر تعريف دقيق لمفاهيم ومصطلحات مثل الإرهاب السيبراني، وغيرها مما يتصل بالفضاء الرقمي وتكنولوجيا المعلومات والاتصالات.

واستنادا إلى النتائج التي نوقشت أعلاه، وجب تطوير خطة طريق أوروبية من أجل مكافحة فعالة لمخاطر الإرهاب السيبراني، وهو ما يفرض علينا تقديم بعض التوصيات القائمة على مقاربة بحثية كُلّانيّة، والتي نُبرزها كالتالي:

- ضرورة الوصول إلى تعريف مشترك للإرهاب والإرهاب السيبراني كنقطة بداية؛ لأن ضبط المصطلحات والمفاهيم أساسي في المواجهة والاستجابة.
- تطوير الدعم المنهجي العلمي لردع الهجمات الإرهابية باستخدام شبكات المعلومات العالمية، وتطوير جهاز مفاهيمي واحد، ومقياس لتقييم التهديدات السيبرانية وعواقبها.
- تطوير آليات للمعلومات المتبادلة حول هجمات الكمبيوتر واسعة النطاق والحوادث الكبرى في الفضاء السيبراني.
- تحديد الأنشطة على الإنترنت (مثل القرصنة والدعاية والهجوم على البنى التحتية، وما إلى ذلك) على أنها إرهاب إلكتروني، فهي تتضمن عنصر الإرهاب بشكل أو بآخر.
- اتخاذ تدابير قانونية وطنية أساسية أكثر مواءمة والترتيبات القانونية الدولية، مع الحرص الدوري على مواءمة التشريعات الوطنية مع التشريعات الدولية.
- الانتقال النشط لتشكيل مجتمع المعلومات عبر بناء قاعدة بيانات أوربية للبحوث حول استخدام الإنترنت لأغراض إرهابية، وهو ما سيسمح بوضع منهجية علمية وخارطة طريق دقيقة لمكافحة الإرهاب السيبراني.
- تكثيف العمل الجماعي لمكافحة الإيديولوجيات المتطرفة المنتشرة عبر الإنترنت، ويشمل ذلك كل الخلفيات الأيديولوجية التي تروج للتطرف وتحرض على الإرهاب.
- تعزيز دور الاتحاد الأوروبي والهيئات الوطنية في قضايا الأمن السيبراني، فمن الضروري توحيد جهود الدول المختلفة، ووكالات إنفاذ القانون والخدمات الخاصة، مثل هذا التفاعل ممكن بشرط أن تتوافق مصالح الدول المختلفة في هذا المجال، مع مراعاة الخصائص الإقليمية والوطنية للتشريعات.

- تطوير طرق للرد المشترك على تهديد الإرهاب السيبراني؛ وتوحيد التشريعات الوطنية في مجال حماية البنية التحتية للمعلومات والاتصالات من الإرهاب السيبراني، عبر العمل على جعل الاتفاقيات الثنائية متعددةَ الأطراف بين الدول الأوربية فيما يخص التعاون في مجال الأمن السيبراني، وتطوير وتوسيع قوانين معقولة وقابلة للتشغيل المتبادل بشأن الهجمات الإلكترونية بشكل عام.

- بما أن التهديد عالمي فهو بحاجة إلى حلول عالمية، ومن الضرورة إنشاء تجمع استخباراتي دولي تحت إشراف منظمة الأمم المتحدة من أجل جمع وتبادل المعلومات الاستخباراتية في وقت واحدم، كما يجب ألا يقتصر جمع المعلومات الاستخبارية على مراقبة مواقع الويب فحسب، بل يشمل أيضا جمع الأدلة الإلكترونية حول الهجمات السيبرانية المحتملة.

- تكثيف الأنشطة الشرطية فيما يتعلق بتتبع المتطرفين والإرهابيين، إضافة إلى المقاتلين الإرهابيين الأجانب العائدين أو الذين تُحتمل عودتهم من مناطق الصراع إلى بلدان المنشأ، وهذا يكون من خلال ربط النشاط الشرطي على أرض الواقع بالنشاط الرقابي عبر الانترنت من خلال نقطة اتصال دائمة التفعيل.

- الرصد المستمر للأنشطة السيبرانية والعمل على تحديد المخاطر المحتملة واتخاذ التدابير اللازمة للحد من هذه المخاط، بما يمكن من زيادة عدد فرق الاستجابة السريعة التي تمتلكها البلدان الأوروبية بمساعدة مركز القدرة على الاستجابة لحوادث الكمبيوتر التابع لحلف الناتو وأيضا مركز التميز للدفاع السيبراني التعاوني التابع للحلف.

- تحسين برامج الدفاع الإلكتروني الخاصة بالدول الأوربية من خلال التدريب وتطوير قدرات الإنذار المبكر، وتشكيل عملية صنع قرار دولية جيدة التنظيم، تمتد من اكتشاف الهجوم السيبراني إلى تدميره أو تعطيله.

- علاوة على ذلك، يجب على الدول الأعضاء في الاتحاد الأوروبي الاهتمام بمسألة إدارة المخاطر السيبرانية عن طريق وضع خطط لإدارة الأزمات الإلكترونية، وتحسين القدرات الفنية والإدارية للحد من التأثيرات السلبية للهجمات السيبرانية المختلفة.

- يجب على المسؤولين التنفيذيين المعتمدين دوليًا الرد على أي هجوم يتعلق بالأمن الدولي، وفق قواعد الاشتباك في اتفاقية جنيف الرقمية، ووفق القانون الدولي.

- بما أن التدابير التشريعية ليست كافية لمكافحة الإرهاب السيبراني، يجب وضع إجراءات عسكرية قائمة على مبادئ إستراتيجية وتشغيلية رادعة لجعل الإرهابيين يترددون في استغلال الإنترنت لأغراضهم

التدميرية، عبر تحقيق التفوق المعلوماتي على العدو. في هذا الصدد، على الحكومات الأوروبية أن تقوم بتسريع شامل لتطوير جميع مكونات المواجهة المعلوماتية.

- فيما يتعلق بالتحقيقات، تحتاج منظمات إنفاذ القانون في أوربا إلى تجهيز نفسها تكنولوجيًّا بشكل أفضل، مع مراعاة التعاون الدولي بين الوكالات على مختلف المستويات داخل وخارج حدودها الوطنية.

- لا يتطلب تهديد الإرهاب السيبراني تعاونًا تشريعيًا فحسب، بل يتطلب أيضًا تعاونًا عسكريًا بما في ذلك استراتيجيات الردع. ويمكن مناقشة الخطوات المتعلقة بالردع العسكري الدولي في ظل حلف شمال الأطلسي وصياغتها عبر تطوير استراتيجيات استباقية أخرى للأمم المتحدة والمنظمات الدولية الأخرى.

- إن استخدام البنية التحتية لتكنولوجيا المعلومات على مستوى الدولة وصولا لـ "الدولة الإلكترونية" على أساس فضاء وطني واحد لعناصر تحديد الهوية الإلكترونية، سيضمن أمانًا عاليًا ضد تهديدات الإرهاب السيبراني، وهذا سيتحقق عبر تحويل الفضاء السيبراني من مشاع غير خاضع للحكم إلى شبكة ذاتية الحكم وتطوير آليات تقييد الوصول.

- نظرًا للبيئة المعلوماتية سريعة التغير، يتعين على الدول الأوربية تطوير إجراء تنسيق ديناميكي على مدار الساعة طوال أيام الأسبوع للحملات الإعلامية لرفع مستوى التوعية بمواضيع الأمن السيبراني وبمخاطر الإرهاب السيبراني، وهي مهمة تقع على عاتق الوكالات الأوروبية المختصة في الأمن السيبراني والتي بذلت جهودا معتبرة في تحسيس المواطن الأوروبي، ويبقى دور الإعلام وشبكات التواصل الاجتماعي في هذا الصدد مهما. لتشجيع فهم شامل وشامل للأمن السيبراني عبر المجتمع.

قائمة المصادر و المراجع

المراجع باللغة العربية:

أولا: القرآن الكريم

- سورة الأنفال، الآية (60).
- سورة البقرة، الآية (40).

ثانيا: الوثائق الرسمية.

- مجلس أوروبا، مجموعة المعاهدات الأوروبية (رقم 185)، ***الاتفاقية المتعلقة بالجريمة الإلكترونية- بودابست.***
- كتب العمل الدولي، لجنة التعاون التقني، ***وثيقة رقم GB.301/TC/1***، جنيف، (مارس 2008).
- الاتحاد الدولي للاتصالات، لجنة الدراسات، المسألة 22/1، تأمين ***شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني*** (د.س.ن).

ثالثا: الكتب.

- إ.توريه، حمدون. ***البحث عن السلام السيبراني.*** الاتحاد الدولي للاتصالات، يناير 2011.
- إسماعيل حسن الشيخ زيني، عبد الجليل. ***الإرهاب الإلكتروني في القانون الدولي (الماهية والجزاء.*** ط1. بيروت: منشورات الحلبي الحقوقية، 2020.
- بري، محمد. ***السيبرنيطيقا (السيبرانية): علم القدرة على التواصل والتحكم والسيطرة.*** ط1، بيروت: المركز الإسلامي للدراسات الإستراتيجية، 2019.
- البلتاجي، سارة. ***الأمن الاجتماعي- الاقتصادي والمواطنة الناشطة في المجتمع المصري.*** ط1. قطر: المركز العربي للأبحاث ودراسة السياسات، 2016.
- بن عيسى، محسن بن العجمي، ***الأمن والتنمية.*** ط1، الرياض: منشورات جامعة نايف العربية للعلوم الأمنية، 2011.
- بي سيل، بيتر. ***الكون الرقمي الثورة العالمية في الاتصالات.*** تر.ضياء وزّاد، المملكة المتحدة: مؤسسة هنداوي سي آي سي، 2017.
- بيك، أولريش. ***مجتمع المخاطر العالمي بحثا عن الأمان المفقود.*** تر علا عادل وآخرون، ط 1، القاهرة: المركز القومي للترجمة، 2013.

- جون إس، ديفيس. واخرون. ***تهديدات مجهولة المصدر: نحو مساءلة دولية في الفضاء الإلكتروني.*** كاليفورنيا: منشورات مؤسسة راند، 2017.

- حسن أحمد لطفى، خالد. ***الإرهاب الالكتروني آفة العصر الحديث والآليات القانونية للمواجهة.*** الإسكندرية: دار الفكر الجامعي، 2019.

- حسن أحمد لطفي، خالد. ***الإرهاب الإلكتروني: افة العصر الحديث، والاليات القانونية للمواجهة.*** الإسكندرية: دار الفكر الجامعي. ط1. 2018.

- حسن جاسم، جعفر. ***حرب المعلومات بين ارث الماضي وديناميكية المستقبل.*** ط1، عمان: دار البداية للنشر والتوزيع، 2010.

- حقي توفيق، سعد. ***مبادئ العلاقات الدولية.*** عمّان: دار وائل للنشر، 2000.

- خليفة، إيهاب. ***مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي.*** المستقبل للأبحاث والدراسات المتقدمة، سلسلة كتب المستقبل، القاهرة: العربي للنشر والتوزيع، 2018.

- دندن، عبد القادر.(محررا). ***العلاقات الدولية في عصر التكنولوجيا الرقمية: تحولات عميقة، مسارات جديدة.*** ط1، عمّان: مركز الكتاب الأكاديمي، 2021.

- ستون، جون. ***الإستراتيجية العسكرية سياسة وأسلوب الحرب.*** ط1، الإمارات العربية المتحدة: مركز الإمارات للدراسات والبحوث الإستراتيجية 2014.

- سميث، ستيف. جون، بيليس. ***عولمة السياسة العالمية***، ترجمة: مركز الخليج للأبحاث، ط1، الامارات العربية المتحدة، مركز الخليج للأبحاث، 2004.

- شعبان، عبد الحسين، ***التطرف والإرهاب: إشكاليات نظرية وتحديات عملية (مع إشارة خاصة إلى العراق).*** مكتبة الإسكندرية، مصر، 2017.

- شفيق، منير. ***الإستراتيجية والتكتيك في فن علم الحرب.*** ط1، بيروت: الدار العربية للعلوم ناشرون، 2008.

- صالح، أحمد محمد. ***أنفوغرافيا الأنترنت وتداعياتها الاجتماعية والثقافية والسياسية.*** القاهرة، دار كتب عربية، 2007.

- عبد الصادق، عادل. ***الإرهاب الالكتروني القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة.*** ط 2، القاهرة: المركز العربي لأبحاث الفضاء الالكتروني، 2013.

- عبد الله بركة المطيري، عادل. ***التهديدات غير التقليدية على أمن دول مجلس التعاون الخليجي (2003-2016)***، ملخص رسالة ماجستير في العلوم السياسية، الكويت: مركز دراسات الخليج والجزيرة العربية، 2020.

- عبد المولى طشطوش، هايل. ***الإرهاب حقيقته ومعناه، دراسة تحليلية للإرهاب من حيث المعنى، الخلفية التاريخية، الدوافع والأسباب، الأشكال والأنواع.*** ط1، الأردن: دار الكندي للنشر والتوزيع، 2008.

- عبد الوهاب منصور، شادي. ***حروب الجيل الخامس: أساليب التفجير من الداخل على الساحة الدولية.*** ط1، القاهرة: العربي للنشر والتوزيع، 2019.

- عبد الصادق، عادل. ***استخدام الإرهاب الالكتروني في الصراع الدولي.*** ط 1، القاهرة: دار الكتاب الحديث، 2015.

- عبد الله المالكي، عبد الحفيظ. ***نحو مجتمع آمن فكرياً: دراسة تأصيلية واستراتيجية وطنية مقترحة لتحقيق الأمن الفكري.*** ط 1، الرياض: مطابع الحميضي. 2010.

- العبيدي، علي. ***الإرهاب واستعصاء المفهوم.*** ط1، تونس: دار المنتدى، 2018.

- العبيدي، علي. ***في الحرب على الإرهاب: من إرهاب المفهوم إلى إرهاب المقاربة.*** ط1. تونس: دار المنتدى، 2018.

- عطا صديق، رامي. شعبان أبو الحسن، فاطمة. ***الإعلام والتنمية في مواجهة الإرهاب.*** ط1، مصر: دار أطلس للنشر والإنتاج الإعلامي، 2016.

- عطية، إدريس. ***التهديدات الإرهابية الجديدة في إفريقيا: دراسة في توظيف الظاهرة وتموضعها الجيوبوليتيكي.*** ط1، الأردن: دار الإعصار العلمي، 2018.

- عوض، محسن. وكرم، خميس. ***الندوة الدولية حول التنمية والديمقراطية وتطوير النظام الإقليمي العربي.*** ط1. القاهرة: المنظمة العربية لحقوق الإنسان، 2013.

- فرج يوسف، أمير. ***مكافحة الإرهاب الالكتروني: الإرهاب الرقمي في ظل اتفاقية دول مجلس التعاون الخليجي لمكافحة الإرهاب.*** الإسكندرية: دار الكتب والدراسات العربية، 2015.

- فلاح العموش، أحمد. ***مستقبل الإرهاب في هذا القرن.*** ط1، الرياض: جامعة نايف العربية للعلوم الأمنية، 2006.

- قوجيلي، سيد احمد. ***الدراسات الأمنية النقدية: مقاربات جديدة لإعادة تعريف الأمن***. ط1، الأردن: المركز العلمي للدراسات السياسية، 2014.

- قوجيلي، سيد احمد. ***تطور الدراسات الأمنية ومعضلة التطبيق في العالم العربي***. ط1، الإمارات: مركز الإمارات للدراسات والبحوث الإستراتيجية، 2012.

- كين، ديفيد. ***حرب بلا نهاية: وظائف خفية للحرب على الإرهاب***. تر. معين الإمام، ط1، المملكة العربية السعودية: العبيكان للنشر، 2008.

- م.يانكوف، ل.يوتوف. ***السيبرنتيك والإعلام***. تر.برهان القلق، ط1، بيروت: دار الطليعة للطباعة والنشر، 1979.

- محمد البصيلي، جاسم. ***الحرب الإلكترونية: أسسها وأثرها في الحروب***. ط2، بيروت: المؤسسة العربية للدراسات والنشر، 1989.

- محمد عبد الغفار، فيصل. ***الحرب الإلكترونية***. ط1، الأردن: الجنادرية للنشر والتوزيع، 2016.

- محمد موسى، مصطفى. ***الإرهاب الالكتروني دراسة قانونية-أمنية - نفسية اجتماعية***. ط1، مصر: دار الكتب والوثائق القومية المصرية، 2009.

- محمد وهبان، أحمد. ***ظاهرة الإرهاب بين صورها التقليدية وأنماطها المستحدثة***. المملكة السعودية: إصدارات الجمعية السعودية للعلوم السياسية، 2015.

- محمد. جاسم، واخرون. ***الإرهاب والتطرف في أوروبا من الداخل: الجماعات الجهادية، الإسلام السياسي واليمين المتطرف***. مصر: المكتب العربي للمعارف. ط1. 2021.

- هاثاواي.، ميليسا. ***مؤشر الجاهزية الإلكترونية: خطة للجاهزية الإلكترونية- خط قاعدي ومؤشر***. الولايات المتحدة الأمريكية: معهد بوتوماك للدراسات السياسية، نوفمبر 2015.

- يوسف كافي، مصطفى. ***الإعلام والإرهاب الإلكتروني***. الأردن: دار الإعصار العلمي للنشر والتوزيع، 2015.

<u>ثالثا: المجلات والدوريات.</u>

- إبراهيم محمد، سمير. "دور الإرهاب الالكتروني في تقويض الأمن القومي دراسة حالة دول ثورات الربيع العربي". ***مجلة كلية السياسة والاقتصاد***. العدد الرابع أكتوبر 2019، الصفحات: 89-114

- إبراهيم مشجعل المعموري، علي. طارش عبد الرضا، أسعد. "الأمن السيبراني ودوره في انتشار ظاهرة الإرهاب الإلكتروني في العراق بعد العام 2003". ***مجلة دراسات دولية***. العدد 80، د.س.ن.

- بلعيد، نهى. "تطور استخدامات مواقع التواصل الاجتماعي في العالم العربي". ***مجلة الإذاعات العربية***. (ابريل 2016).

- بلفرد. لطفي لمين. "الفضاء السيبراني: هندسة وفواعل". ***المجلة الجزائرية للدراسات السياسية***. المجلد 3، العدد 5 (جوان 2016).

- بن سيدهم، حورية. عواشرية، رقية. "الأمن الفضائي السيبراني: التحديات والحلول". ***المجلة الجزائرية للأمن الإنساني***. المجلد 5، العدد 2 (2020).

- بن عمرة، بلقاسم أمين. "مقترب ايتيقي للفضاء السيبراني. نظرية العدالة عند "جون رولز" أنموذجا". ***مجلة الناصرية للدراسات الاجتماعية والتاريخية***. مجلد 10، عدد 2 (ديسمبر 2019).

- بن عنتر، عبد النور. تطور مفهوم الأمن في العلاقات الدولية، **السياسة الدولية**، عدد 160، المجلد 40، (2005).

- بن مرزوق، عنترة. "جريمة الإرهاب الإلكتروني: الأسباب وآليات العلاج". ***مجلة الحقوق والعلوم الإنسانية***. العدد 2 (جوان 2018).

- البهي، رغدة. "كيف تفرض الدول سيادتها على الفاعلين في المجال الافتراضي؟". ***سلسلة دراسات خاصة***. العدد 24، مركز المستقبل للأبحاث والدراسات المتقدمة (24 يونيو 2021).

- جعيجع، عبد القادر. تيغزة، زهرة. "تطور الإرهاب وانعكاسه على استقرار المجتمعات: قراءة في ظاهرة الإرهاب الإلكتروني وإستراتيجيات المواجهة". ***مجلة دفاتر السياسة والقانون***. المجلد 13، عدد1 (جانفي 2021).

- جلود. رشيد. "مقاربات سوسيولوجية معاصرة: مجتمع المخاطرة عند "أولريش بيك" أنموذجا". ***مجلة العلوم الانسانية لجامعة أم البواقي***. المجلد 8، العدد1(مارس 2022).

- جندلي، عبد الناصر. "إشكالية تكييف المنظور الواقعي للعلاقات الدولية مع التحولات الدولية لما بعد الحرب الباردة". ***مجلة المستقبل العربي***. العدد 376، (2010).

- حارك، فاتح. حمدوش، رياض. "الدولة بين الهيمنة وتحقيق الأمن في الفضاء السيبراني". ***المجلة الجزائرية للأمن الإنساني***. المجلد 07، العدد الأول (يناير 2022).

- حسين الزهراني، شيخة. "الطبيعة القانونية للهجوم السيبراني وخصائصه". ***مجلة جامعة الشارقة للعلوم القانونية***. المجلد 17، العدد 1 (جوان 2020).

- حمشي، محمد. "مدخل إلى المدارس الأوروبية في الدراسات الأمنية النقدية". ***المجلة الجزائرية للأمن الإنساني***. العدد6 (جويلية 2018).

- حمشي، محمد. "مدرسة باريس للدراسات لأمنية وإشكالية مستوى التحليل في العلاقات الدولية". ***مجلة السياسة الدولية***. م53، العدد 212 (ابريل 2018).

- حمشي، محمد. الدراسات النقدية للإرهاب بوصفه حقلا معرفيا ناشئا، مراجعة "دليل راوتليج" إلى الدراسات النقدية للإرهاب". ***سياسات عربية***. العدد 31 (مارس 2018).

- خليفة. إيهاب. "تنامي التهديدات السيبرانية للمؤسسات العسكرية". ***دورية اتجاهات الأحداث***. العدد 22 (جويلية- اوت 2017).

- خليفة. إيهاب. « Cyber Power" نط جديد لممارسة التأثيرات غير التقليدية في العلاقات الدولية". ***دورية اتجاهات الأحداث***. العدد 6 (يناير 2015).

- راجح كردي، عبد الحميد. "إشكالية مصطلح الإرهاب بين الحقيقة اللغوية والشرعية والواقع المعاصر". ***مجلة البلقاء للبحوث والدراسات***. المجلد 22، العدد 1(2019).

- روربرت غير، تيد. ***لماذا يتمرد البشر؟***. تر: مركز الخليج للأبحاث، ط1، الإمارات العربية المتحدة: مركز الخليج للأبحاث، (2004).

- زروقة، إسماعيل. "الفضاء السيبراني والتحول في مفاهيم القوة والصراع". ***مجلة العلوم القانونية والسياسية***. المجلد 10، العدد 1 (ابريل 2019).

- زقاغ، عادل. "المعضلة الأمنية المجتمعية، خطاب الأمننة وصناعة السياسة العامة". ***المجلة الجزائرية للسياسة العامة***، المجلد 1، العدد1 (سبتمبر 2011).

- زقاغ، عادل. منصوري، سفيان. الجريمة المنظمة بمنطقة الساحل الإفريقي: بانوراما سوسيو- أمنية، ***مجلة العلوم الإنسانية والاجتماعية***، العدد 23(مارس 2016).

- سليمان الموسى، عصام. "الثورة الرقمية تصنع الإعلام العربي على مفترق الطرق". ***مجلة المستقبل العربي***. العدد 376(2010).

- شافي جبر، كريمة. "الإرهاب المعلوماتي". ***مجلة كلية الآداب***. العدد 96،(2011) .

- الصحفي، روان بنت عطية الله. "الجرائم السيبرانية". ***المجلة الإلكترونية الشاملة متعددة التخصصات.*** العدد 24 (مايو 2020).

- عبد الصادق. عادل. "أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني". ***سلسلة أوراق.*** العدد 23. الإسكندرية: وحدة الدراسات المستقبلية، 2016.

- عبد الكريم العبودي، علي. "هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين". ***مجلة قضايا سياسية.*** العدد 57، (2018).

- عبد الله الحربي، سليمان. "مفهوم الأمن، مستوياته، وصيغه، وتهديداته (دراسة نظرية في المفاهيم والأطر)". ***المجلة العربية للعلوم السياسية***، العدد 19 (صيف 2008).

- عبد الوهاب منصور، شادي. "الإرهاب عن بعد: نمط تنظيمي جديد لاستهداف الدول الغربية والآسيوية". ***دورية اتجاهات الأحداث.*** العدد 24، (نوفمبر 2017).

- عزيز، نوري. "الخطاب الأمني الأورو-متوسطي تجاه ظاهرة الإرهاب بين: الأمننة/اللاأمننة". ***مجلة الحقوق والعلوم السياسية.*** مجلد 5، عدد2، (جوان 2018).

- عطية، إدريس. "تهديدات الإرهاب الدولي في منطقة شمال إفريقيا". ***المجلة الجزائرية للدراسات السياسية.*** العدد 4 (ديسمبر 2015).

- غربي. محمد. "الديمقراطية والحكم الراشد: رهانات المشاركة السياسية وتحقيق التنمية". ***دفاتر السياسة والقانون.*** عدد خاص (أبريل 2011).

- لفتة العيساوي، علي. "الفيسبوك- الوطن البديل للشباب وأثره السلبي على الشباب العراقي (دراسة وصفية تحليلية)". ***سلسلة الاختراق الثقافي.*** المركز الإسلامي للدراسات الإستراتيجية بالنجف-دولة العراق، (2021).

- مؤيد عبد اللطيف، سامر. "الحرب في الفضاء الرقمي: رؤية مستقبلية". ***مجلة رسالة الحقوق.*** العدد 2 (2015).

- محمد يحي، ربيع. "إسرائيل وخطوات الهيمنة على ساحة الفضاء السيبراني في الشرق الأوسط: دراسة حول استعدادات ومحاور عمل الدولة العبرية في عصر الإنترنت (2002 – 2013)". ***مجلة رؤى إستراتيجية*** (يونيو 2013).

- المرواني، نايف بن محمد. "تمويل الإرهاب الكترونيا: التحديات وطرق المواجهة "التجربة السعودية". ***المجلة العربية للدراسات الأمنية والتدريب***. المجلد 29، العدد 58، (ديسمبر 2013)

- مصطفى. مهند. "حول مفهوم وحدود المجال العمومي". ***مجلة مدى الكرمل***. العدد 29 (يناير 2016).

- هوفمان، بروس. "شكل من أشكال الحرب النفسية". ***مجلة اي جورنال*** (ماي 2007).

- وليد محمود، خالد. "الهجمات عبر الانترنت: ساحة الصراع الإلكتروني الجديدة". ***دورية سياسات عربية***. العدد 5 (نوفمبر 2013).

- لطفي، وفاء. "الجهود الدولية في مجال مكافحة جرائم الارهاب السيبراني: التجربة الماليزية نموذجا"، ***مجلة كلية الاقتصاد والعلوم السياسية***، المجلد 23، العدد 1، (يناير 2022) .

- يحيى. سارة. « Cyber Diplomacy » بُعد غير تقليدي في العلاقات غير الرسمية بين الدول". ***دورية اتجاهات الأحداث***. العدد 6 (يناير 2015).

رابعا: الاطروحات:

- سعيد آل عياش الشهراني، محمد. ***أثر العولمة على مفهوم الأمن الوطني "دراسة مسحية على مجموعة من الأكاديميين في الرياض"***. رسالة لنيل درجة الماجستير في القيادة الأمنية، قسم العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية. (2006).

- شفيق. نوران. ***الفضاء الإلكتروني وأنماط التفاعلات الدولية***. رسالة ماجستير (جامعة القاهرة: كلية الاقتصاد والعلوم السياسية، 2014).

- عراجي، أنديرا. ***القوة في الفضاء السيبراني: فصل عصري من التحدي والاستجابة***. رسالة لنيل دبلوم الدراسات العليا في العلوم السياسية والإدارية بكلية الحقوق والعلوم السياسية والإدارية بالجامعة اللبنانية، 2015-2016.

- فخر الدين قاسم أحمد، مجاهد. ***ترجمة الصفحات: 1-66 من كتاب الأمن الإلكتروني والحرب الإلكترونية، ما ينبغي أن يعرفه كل شخص، لبيتر وارن سينغر والن أ. فريدمان***، بحث تكميلي لنيل درجة الماجستير في الترجمة، (السودان: جامعة السودان للعلوم والتكنولوجيا، كلية الدراسات العليا، د.س.ن).

خامسا: التقارير:

- بارون، جوشوا. أوماهوني، انجيلا وآخرون. ***تداعيات العملة الافتراضية على الأمن القومي، البحث في إمكانية النشر من جهة فاعلة غير حكومية***، مؤسسة راند (2015).

- سكوت وارن، هارولد. وآخرون، ***التوصل إلى اتفاق مع الصين بشأن الفضاء الإلكتروني***. كاليفورنيا: منشورات مؤسسة راند (2016).

- شبيب، نبيل. ***التقرير الارتيادي السنوي: أثر صعود اليمين المتطرف على مسلمي أوروبا، وكيف يتعامل المسلمون مع التطرف اليميني***، المركز العربي للدراسات الإنسانية (2017).

- ***القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة***، ورقة موقف اللجنة الدولية للصليب الأحمر، مقدمة إلى فريق العمل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وإلى فريق الخبراء الحكوميين المعني بالارتقاء بسلوك الدول المسؤول في ميدان الفضاء السيبراني في سياق الأمن الدولي (نوفمبر 2019).

- اللجنة الاقتصادية والاجتماعية لغربي آسيا (ESCWA)، ***الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية: توصيات سياسية***. منشورات منظمة الأمم المتحدة، (2015).

- مركز جنيف للرقابة الديمقراطية على القوات المسلحة (DCAF)، ***بناء النزاهة والحد من الفساد في قطاع الدفاع.. خلاصة وافية لأفضل الممارسات*** (جنيف، 2010).

- مكتب الأمم المتحدة المعني بالمخدرات والجريمة. ***دليل التعاون الدولي في المسائل الجنائية لمكافحة الإرهاب*** (فيينا، 2009).

- مكتب الأمم المتحدة المعني بالمخدرات والجريمة، بالتعاون مع: فرقة العمل التابعة للأمم المتحدة المعنية بتنفيذ تدابير مكافحة الإرهاب، تقرير ***بعنوان: استخدام الإنترنت في أغراض إرهابية*** (نيويورك 2012).

- مكتب الأمم المتحدة المعني بالمخدرات والجريمة، ***دراسة شاملة عن الجريمة*** (نيويورك، فبراير 2013).

- مكتب الأمم المتحدة المعني بالمخدرات والجريمة، ***دليل بشأن الأطفال الذين تجندهم وتستغلهم الجماعات الإرهابية والجماعات المتطرفة العنيفة.. دور نظام العدالة*** (فيينا، 2018).

- منظمة حلف شمال الأطلسي، ***المنهج التعليمي المرجعي: الحوكمة الرشيدة وبناء النزاهة في قطاع الدفاع والقطاعات الأمنية ذات الصلة*** (2012).

سادسا: المداخلات العلمية

- حجاج، قاسم. "مدخل إلى تحليل نسقي للأسباب الهيكلية للهزات الأمنية الشاملة في المنطقة المغاربية–الساحلية"، ورقة مقدمة إلى المؤتمر المغاربي الدولي حول التهديدات الأمنية للدول المغاربية في ضوء التطورات الراهنة: الرهانات والتحديات، 28/27 ماي 2013.

- الحمش، منير. "مجتمع المخاطر في ظل التحولات الاقتصادية والاجتماعية" ،مداخلة في ندوة الاقتصاد الرابعة والعشرون حول التنمية الاقتصادية والاجتماعية في سورية، جمعية العلوم الاقتصادية السورية، دمشق : 2011.

- سينجر، بيتر، ا"لإرهاب الإلكتروني: خرافات، وحقائق، وفيروس ستوكسنت، وتنظيم داعش، ووسائل الإعلام الاجتماعي، ومسرح المواجهة"، سلسلة محاضرات مركز الإمارات للدراسات والبحوث الإستراتيجية، أوت 2018.

- عطوة الزنط، سعد. "الإرهاب الإلكتروني وإعادة صياغة إستراتيجيات الأمن القومي"، ورقة مقدمة إلى مؤتمر: الجرائم المستحدثة– كيفية إثباتها ومواجهتها، 15–16 ديسمبر 2010.

- عمروس، عمّارة. "اللجوء الإنساني في الفضاء الأورو–متوسطي ومشكل الاندماج في المجتمعات الأوروبية – حالة اللاجئين السوريين في ظل صعود اليمين المتطرف"، دراسة قدمت للمشاركة بورشة عمل دولية بعنوان: "الهجرة القسرية في الدول العربية: الإشكاليات والقضايا"، بيروت– تشرين الثاني/ نوفمبر 2019.

- غادر. محمد ياسين. "محددات الحوكمة ومعاييرها". ورقة بحث قدمت في المؤتمر العلمي الدولي: عولمة الإدارة في عصر المعرفة. جامعة الجنان. طرابلس/لبنان، 15–17 ديسمبر 2012.

- مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية، البند 5 من جدول الأعمال المؤقت، "النهج الشاملة المتوزانة لمنع ظهور أشكال جديدة ومستجدة للجريمة العابرة للحدود الوطنية والتصدي لها على نحو ملائم"، الدوحة: 12–19 ابريل 2015.

- يوسف الشوبكي، محمود. "مفهوم الإرهاب بين الإسلام والغرب"، ورقة مقدمة إلى مؤتمر: الإسلام والتحديات المعاصرة، الجامعة الإسلامية: كلية أصول الدين، ابريل 2007.

سابعا: الروابط الإلكترونية.

- "الانتربول والاتحاد الأوروبي"، https://interpol.int/ar/5/3/2 (15/10/2021)

- الاتحاد الدولي للاتصالات، "لماذا نحتاج إلى أمن سيبراني أكثر شمولا؟"، https://www.itu/netw/wsis/forum/2021/ar/Agenda/Session/328 (12/09/2021)

- "اتفاق أوروبي بشأن مكافحة المحتوى الإرهابي في الانترنت"، 2020/12/12، https://arabic.euronews.com/2020/12/12/eu-mep-agreed-plan-fight-against-terror-content-online (2021/01/30)

- أمين، إميل، "الأمن السيبراني العالمي: حروب خلفية ومساحات إرهابية.. خمسُ قوى تهدد استقرار المجتمعات عبر شبكات الإنترنت وبتقنيات عالية الدقة"، 2020/02/12، https://bit.ly/3hVxIGy (2022/02/22)

- أوقادي، إسماعيل، "الفضاء الرقمي والحاجة إلى باراديغم قانوني جديد"، مركز تكامل للدراسات والأبحاث (المغرب)، 2021/01/15، https://www.takamoul.org/author/author02/، (16/10/2021)

- إبراهيم الجهماني، ثامر، "مفهوم الإرهاب، كتاب في القانون الدولي"، مركز الدراسات والأبحاث العلمانية في العالم العربي، 14-07-2014، https://cutt.us/djYU (2021/09/16)

- البابلي، نبيل، "تقرير بعنوان: الحكم الرشيد، الأبعاد والمعايير والمتطلبات"، المعهد المصري للدراسات، 2018/01/18، https://bit.ly/37WkeHJ (2021/11/25)

- برو، إليزابيث، "الحرب الإلكترونية لا تقل خطورة عن الهجمات المسلحة"، مركز الجزيرة للدراسات، https://goo.gl/NnYnbb (2021/01/10)

- بشير، هشام، "الإرهاب الإلكتروني في ظل ثورة المعلومات"، 1 مايو 2012، https://araa.sa/index.php?option=com_contentview=articleid=244:2014-06-13-16-21-31catid=132:articlesltemid=294، (25 ابريل 2021).

- بوسونج، رافاييل، "الخطوات التالية لسياسة الاتحاد الأوروبي لمكافحة الإرهاب.. التهديدات المتطورة للجهادية والتطرف اليميني والتعاون عبر الأطلسي"، ترجمة: يوسف سامي، https://asbarme.com/5716 (2021/09/12)

- بوسونج، رافاييل، "الخطوات التالية لسياسة الاتحاد الأوروبي لمكافحة الإرهاب.. التهديدات المتطورة للجهادية والتطرف اليميني والتعاون عبر الأطلسي"، ترجمة: يوسف سامي، https://asbarme.com/5716/ (2021/09/12)
- حسن الباجوري، سمر، "الأسباب الاقتصادية لتنامي ظاهرة الإرهاب في إفريقيا جنوب الصحراء"، 31 ماي 2016، https://mpra.ub.uni-muenchen.de/74740 (2021/05/03)
- "الخطر السيبراني واستحقاق التشريع الدولي.. اتفاقية جنيف الرقمية مثالا"، 2017/08/28، https://www.alriyadh.com/1619757 (11/11/2021)
- د.ذ.ك، "أسرار أكبر هجوم إلكتروني في التاريخ استهدف 100 دولة"، 2017/05/13، https://bit.ly/3H0kQb6 (2021/11/24)
- الديواني، عبد الغفار، "القرن السيبراني: الدفاع الإلكتروني بين المنع والانتقام"، عرض لتقرير صادر عن المعهد الألماني للشؤون الأمنية والدولية، مركز المستقبل للأبحاث والدراسات المتقدمة، 4 جوان 2015، https://bit.ly/3iKVchF (12 جويلية 2021).
- رشدي، محمود، "اليوروبول: تهديدات متصاعدة وتحديات راهنة"، 2018/10/22، https://www.almarjie-paris.com/4596 (2021/04/08)
- راشد، سامح. "الذكاء الاصطناعي في مواجهة الإرهاب، فرص وتحديات"، مجلة درع الوطن، 1\02\2022، في: https://cutt.us/EMG8d (2022/04/04)
- الرفاعي، محسن، "الاتحاد الأوروبي يطلق وحدة الأمن السيبراني للاستجابة السريعة"، موقع أورو-نيوز، نُشر في: 2021/06/21،

https://arabic.euronews.com/2021/06/24/european-union-lanches-the-cybersecurity-rapid-response-unit (2021/09/12)

- زاركاداكيس، جورج، "الجمهورية السيبرانية.. إعادة صياغة الديمقراطيات في عصر الآلات الذكية. كيف تواجه الأنظمة السياسية والاقتصادية تحديات الأتمتة؟"، عرض: هند سمير طه، نُشر في: 22 سبتمبر 2021، https://bit.ly/3ERlcPW (2021/10/15).

- سعد عبد الحميد، حسن، "سياسة أوروبا الإلكترونية ضد الإرهاب والتطرف"، مركز النهرين للدراسات الإستراتيجية (العراق، 10 فبراير 2019)، https://www.alnahrain.iq/post/370# (2021/11/11)

- سعد عبد الحميد، حسن، "سياسة أوروبا الإلكترونية ضد الإرهاب والتطرف"، مركز النهرين للدراسات الاستراتيجية، العراق، 10 فبراير 2019 https://www.alnahrain.iq/post/370# (11/11/2021)

- سعيد، خالد وصلاح، بثينة، "التهميش والحرمان أقوى دوافع التطرف"، 9 نوفمبر 2017، https://cutt.us/ACclh (2021/05/03)

- سكاي نيوز، "إرهاب عبر الإنترنت.. تحذيرات من تطبيقات إخوانية تنشر التطرف"، 2022/01/12، https://cutt.us/hSmk3 (20/01/2022)

- سوق مكافحة الإرهاب السيبراني – النمو والاتجاهات وتأثير COVID-19 والتنبؤات (2023 – 2028)، أنظر: https://cutt.us/tBDIX

- الشامخ، إيمان، "بلا قنابل أو أسلحة.. هكذا يمكن لروسيا تدمير البنية التحتية في أوكرانيا"، موقع الجزيرة، https://bit.ly/36u9Y8S (2022/02/22)

- طرشي، ياسين، وحكيمي، توفيق، "المعضلة الأمنية الدولية"، https://qawaneen.blogpost.com/2010/06/blog-post_7365.html?m=1 (2021/09/16)

- فهد، وجدان. "الذكاء الاصطناعي بين التكتيكات الإرهابية والاستراتيجيات الوطنية"، 1 مارس 2022، https://cutt.us/1XzoV (08|03|2022)

- عبد الرحمن، عبد الستار، "الإرهاب السيبراني.. خطر يهدد العالم"، https://www.imctc.org/ar/eLibrary/Articles/Pages/Articles2322020.aspx (12 جويلية 2021)

- عبد الصادق، عادل، "الفضاء الإلكتروني وأسلحة الانتشار الشامل: بين الردع وسباق التسلح"، 2015/05/15، https://bit.ly/3fiTkuT (2021/11/24)

- عبد الفتاح، فاطمة الزهراء، "التشارك الإلكتروني: آليات مكافحة الشائعات في الفضاء السيبراني"، موقع المستقبل للأبحاث والدراسات المستقبلية، 29 ماي 2017، https://futureuae.com/ar-/Mainpage/Item/2841 (27/02/2022)

- عبد الصبور، سماح، "الإرهاب الرقمي: أنماط استخدام الإرهاب الشبكي"، شوهد في: 2019/01/18، https://futureuae.com/ar/Mainpage/Item/227(2021/09/10)

- عبد العليم، أحمد، "تهديدات غير تقليدية: مستقبل العنف في ظل التطورات التكنولوجية"، المستقبل للدراسات والابحاث المتقدمة، 24 نوفمبر 2015، https://bit.ly/3o0aOip (2021/05/28)

- "العنف الرقمي... أحدث صيحات الحروب الجديدة"، مجلة الإنساني، عدد 59، 2015، https://goo.gl/YRTBHQ(17/03/2019)

- عبد الوهاب، شادي، أبعاد توظيف إدراك التهديدات في السياسة الخارجية، المستقبل للأبحاد والدراسات المتقدمة، 20 جويلية 2017، https://cutt.us/c2i8g (2022/12/23)

- كاي أليكساندر، شوتس، "كيف يعزز الإنترنت التطرف اليميني؟"، مقال من موقع Deutsche Welle . 3-05-2020، https://p.dw.com/p/3YU0z(2022/01/27)

- كوريرا، غوردون، "التهديد المتنامي لليمين المتطرف عبر الانترنت"، موقع قناة BBC، 15 جويلية 2019، https://cutt.us/zAufh(2022/02/22)

- "كورونا يعرقل جهود أوروبا في مواجهة خلافة داعش السيبرانية. دار الإفتاء المصرية تحذّر من هجمات الدولة الإسلامية في أعياد الميلاد"، 2020/12/22، https://bit.ly/3ehEZxy

- لامباش، دانيال، "السيادة الإلكترونية: اتجاهات تشكيل مناطق سيبرانية تحت سيطرة الدول والشركات"، مركز الإمارات للدراسات والبحوث المتقدمة، 2020/09/23، https://bit.ly/3GjlbWx (2021/07/23)

- لصلج، عائشة، "العنف الرمزي عبر الشبكات الاجتماعية الافتراضية: قراءة في بعض صور العنف عبر الفيسبوك"، شوهد في: 2018/07/23، https://mominoun.com/articles/..B1-4065 (2021/09/10)

- محارب، محمد، "إسرائيل والحرب الإلكترونية: قراءة في كتاب: حرب في الفضاء الإلكتروني (اتجاهات وتأثيرات على إسرائيل) للباحثين: شامويل ايفن ودافيد بن سيمان-طوف"، 10 اوت 2011،

https://www.dohainstitute.org/ar/ResearchAndStudies/Pages/Israel_and_Cyb
(2021/11/03) er_Warfare.aspx

- محمد، جاسم، "استراتيجيات مكافحة الإرهاب والتطرف في الاتحاد الأوروبي- الوقاية والمقاضاة والحماية"، 2021/10/22، https://bit.ly/3nZU/a4 (2021/11/10)

- محمد، جاسم، "صناعة الكراهية داخل أوروبا... منصات التواصل الاجتماعي تؤجج العنف، دور الاتحاد الأوروبي محدود في إعادة تأهيل الإرهابيين"، 2021/06/17 https://bit.ly/3pjEQ2h (15/12/2021)

- محمد، عاصم، "ما هي الأتمتة؟ وكيف تطورت تاريخيا حتى عصرنا الحديث؟"، 2018/06/23، https://www.ida2at.com/what-is-automation-and-how-has-it-evolved/ (2021/12/20)

- مركز أبو ظبي للحوكمة، "أساسيات الحوكمة: مصطلحات ومفاهيم"، سلسلة التراث التثقيفية للمركز، https://loiarabe.blogspot.com/2019/07/pdf_28.html(2021/11/22)

- "المفوضية الأوروبية تكشف عن اليات حماية الأنظمة الرقمية من تهديدات الهجمات الإلكترونية"، 2020/12/17، https://cutt.us/UwOhQ (22|09|2021)

- - "المفوضية الأوروبية تخصص 11 مليون يورو لتعزيز قدرات الأمن السيبراني"، 2021/05/10، https://gate.ahram.org.eg/News/2714163.aspx (2021/11/15)

- المركز الأوروبي لدراسات مكافحة الإرهاب والإستخبارات، "مكافحة الإرهاب في أوروبا . تدابير وقائية وإستباقية جديدة"، 2021/10/11، https://bit.ly/3spNy1q (2021/11/22)

- المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات، "مكافحة الإرهاب داخل الاتحاد الأوروبي: إستراتيجيات وتشريعات"، 28 أكتوبر 2021https://bit.ly/3xy8/3i (10/11/2021)

- ميلتزر، جوشوا وكيري، كاميرون، "علاقات متشابكة: كيف تدعم التجارة الرقمية سياسات الأمن السيبراني؟"، عرض: رغدة البهي، 2019/10/02، https://bit.ly/3sZqYfS (2021/12/11)

- ناجي إدريس، مسعود، "تأثير السياسة السيبرانية على السياسة العملية ونظريات العلاقات الدولية (الجزء الأول)"، 2021/03/27، http://burathanews.com/arabic/studies/389167 (2021/09/25)

- هاثاواي، ميليسا، "إدارة الخطر السيبراني الوطني"، https://cutt.us/rb3WF (11.12.2021)
- هروس، حفيظ، "سلطة الافتراضي؟"، 15 يناير 2021، ص4، https://www.takamoul.org/?p=553 (10/03/2021)
- وحدة الدراسات والتقارير بالمركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات (ألمانيا-هولندا)، "الأمن السيبراني، الحكومة الإلكترونية، الخدمات الحكومية الرقمية"، https://www.europarabit.com/?p=72350 (2021/11/10)

ياسين، السيد، "مجتمع الخطر ودورة الخوف"، موقع جريدة الاتحاد، 10 اوت 2005، https://cutt.us/FtvM9(2021/11/24) (22/09/2021)

المراجع باللغات الأجنبية:

باللغة الإنجليزية:

أولا: الوثائق الرسمية.

- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: ***A Digital Single Market Strategy for Europe***, COM (2015) 192 final.
- European Commission, ***A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond***, COMMUNICATION FROM THE COMMISSION (Brussels, 09/12/2020).
- European Commission, ***COMMUNICATION FROM THE COMMISSION: A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond***, COM (2020) 795 final (Brussels, 9.12.2020), p.1.
- European Union Institute for Security Studies (EUISS), ***Cyberspace and EU Action to 2030***, A report based on an expert webinar Organised by the French Permanent Representation to the European Union on, with the support of the EU Institute for Security Studies (9 July 2021).
- The White House, ***The National Strategy to Secure Cyberspace,*** Washington, February 2003.

ثانيا: الكتب.

- A. Yannakogeorgos, Panayotis. ***Rethinking the Threat of Cyberterrorism, in Thomas M. Chen • Lee Jarvis Stuart Macdonald Editors, Cyberterrorism Understanding, Assessment, and Response***, New York: Springer,2014.
- A.Lewis, James. Assessing the Risk of Cyberterrorism, Cyber War and Other Cyber Threats, Center for Strategic and International Studies (CSIS), (Washington, December 2002.
- Akhgar, B. and Brewster, B. (eds.). ***Combatting Cybercrime and Cyberterrorism, Advanced Sciences and Technologies for Security Applications***. Switzerland: Springer International Publishing, 2016.
- Buzan ,Barry. Hansen, Lene. **The Evolution of International Security Studies.** Cambridge: Cambridge University Press, 2009.
- Buzan ,Barry. Wæver, Ole. Jaap De Wilde, ***Security: A New Framework for Analysis***. Boulder: Lynne Rienner, Library of Congress Cataloging-in-Publication Data, USA, 1998.
- Christen, Markus. and Others (editors). ***The Ethics of Cybersecurity***. Switserland : The International Library of Ethics, Law and Technology, 2020.
- Christian, Kaunert. and Leonard, Sarah. (Editors). ***European Security, Terrorism and Intelligence: Tackling New Security Challenges in Europe***. Palgrave Macmillan, 2013.
- Christou, George. ***Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy***. 1st edition. UK: Palgrave Macmillan, 2016.
- Czosseck, C. and others, ***3rd International Conference on Cyber Conflict***. Tallinn, Estonia, 2011.
- *Murat Dogrul, and others, "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism", in:* ***3rd International Conference on Cyber Conflict****. C. Czosseck, E. Tyugu, T. Wingfield (Eds.), Tallinn, Estonia: 2011.*
- D. Simon, Jeffrey. Technological and Lone Operator Terrorism: Prospects for a Fifth Wave of Global Terrorism, in **Terrorism, Identity and Legitimacy**, ed. Jean E. Rosenfeld. New York: Routledge, 2011.

- Douai, Aziz. Technology and terrorism: Media symbiosis and the “dark side” of the web, in: Lorenzo Cantoni and James A. Danowski, ***Communication and Technology,*** Switzerland: De Gruyter Mouton, 2015.
- E. Mehan, Julie. ***Cyberwar, Cyberterror, Cybercrime and Cyberactivism An in-depth guide to the role of security standards in the cybersecurity environment***, 2ed. Cambridgeshire. United Kingdom: IT Governance Publishing, 2014.
- Fox, Jonathan. "The Future of Religion and Domestic Conflict,” in ***Religion, International Relations and Development Cooperation***, (ed.) Berma klein Goldwijk, Wageningen Academic Publishers,2007.
- Gripsrud, Jostein. Moe, Hallvard. ***The Dogital Public Sphere: Challenges for Media Policy.*** Sweden: Nordicom, 2010.
- J. Moyano, Maria. ***Argentina’s Lost Patrol Armed Struggle 1969-1979***. New Haven and London: Yale University Press, 1995.
- Olesen, Nina. *European Public-Private Partnerships on Cybersecurity - An Instrument to Support the Fight Against Cybercrime and Cyberterrorism*, B. Akhgar and B. Brewster (eds.), ***Combatting Cybercrime and Cyberterrorism, Advanced Sciences and Technologies for Security Applications***, Springer International Publishing Switzerland 2016.
- P.Shmid ,Alex. and Others. ***HANDBOOK OF TERRORISM PREVENTION AND PREPAREDNESS.*** The Hague: ICCT Press, 2021.
- R. Bunt, Gary. ***Islam in the Digital Age E-Jihad,Online Fatwas and Cyber Islamic Environments***, London: Pluto Press, 2003.
- Ronald J, Deibert. "Circuits of Power: Security in the Internet Environment " ,In: ***Information Technologies and Global Politics, the Changing Scope of Power and Governance***, Rosenau, James N., and J.P Singh, eds. Albany, New York: State University of NY Press, 2002.
- Świątkowska, Joanna (Editor). Poland: The Kosciuszko Institute, 2014.
- Tomic, Dusco. and Others. ***Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense***. Springer International Publishing, 22 Mars 2018.
- Wilson, Clay. "Cyber Threats to Critical Information Infrastructure", in: Thomas M. Chen · Lee Jarvis Stuart Macdonald, ***Cyberterrorism Understanding, Assessment, and Response***. UK :springer, 2014.

- von Behr, Ines. and Others, ***Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism.*** Brussels: Rand Europe, 2013.

ثالثا: المجلات والدوريات.

- Shmid, Alex. "Terrorism: Definitional Problem" , ***Journal of International Law,*** Vol.36, Issue 02 (2004)
- Pauli Medeiros, Breno. And others, "The Fundamental Conceptual Trinity of Cyberspace", ***Contexto Internacional,*** 42, 1. (Jan/Apr 2020.)
- Lee Goi ,Chai. " Cyberculture: Impacts on Netizen". ***Asian Culture and History***. Vol.1, No.2 (July 2009).
- Fidler, David P. and Others. "NATO, Cyber Defence and International Law ". ***Journal of International and Comparative Law***. vol.4, Issue 1 (Fall 2013).
- Jensen, Eric Talbot. "The Tallinn Manuel 2.0: Highlights and Insights". ***Georgetown Journal of International Law***, vol.48 (2013).
- Perritt, Henry. "The Internet as a Threat to Sovereignty ? Thoughts on the Internet's Role in Strenthening National and Global Governance", ***Indiana Journal of Global Legal Studies***, Vol.05, Issue 02 (1998).
- Herzog. "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses ". ***Journal of Strategic Security***. vol.4, N.2 (Summer 2011).
- Kermer, Jan Erick. A.Nijmeijer, Rolf. "Identity and European Public Sphere in the Context of Social Media and Information Disorder". ***Media and Communication***. vol.8, Issue 4 (08/10/2020).
- Argomaniz, Javier. "EUROPEAN UNION RESPONSES TO TERRORIST USE OF THE INTERNET". ***Cooperation and Conflict***. vol.50 ,N 2,(2015).
- E.Eichensehr, Kristen. ""The Tallinn Guide". ***The American Journal of International Law.*** vol.108 (July 2014).
- Hansen, Lene and Nissenbaum, Helen. "Digital disaster, cyber security, and the Copenhagen School", ***International studies quarterly***, 53, N4, (2009).
- Tabansky, Lion. "Basic Concepts in Cyber Warfare", ***Military and Strategic Affairs,*** Vol.03, N.01 ,(2011).

- Cruiz Lobato, Luisa. and Michail Kenkel, Kai. "Discourses of Cyberspace Securitization in Brazil and in the United States". Artigos, ***Politica Internacional***. Vol.58, Issue: 2, (Jul-Dec 2015).
- Bogdanoski, Mitko. Petreski, Drage. "Cyber-Terrorism: Global Security Threat ", International Scientific Defense, ***Security and Peace Journal***.(2013).
- Zubair Khan, Muhammad. And others. "From Habermas Model to New Public Sphere: A Paradigm Shift". ***Global Journal of Human Social Science***. vol.12, Issue 5 (2012).
- Khaeriah Kadir, Nadiah. and others, "Terrorism and Cyberspace: A Phenomenon of Cyber-Terrorism as Transnational Crimes"*,* ***FIAT JUSTISIA***,V 13. N 4, (December 2019).
- Bures, Oldrich. "Informal counterterrorism arrangements in Europe: Beauty by variety or duplicity by abundance? ". ***Cooperation and Conflict***. 47(4), (December 2012). 495-518.
- Bányász, Péter. "Social Media and Terrorism", ***AARMS*** , V 17, N. 3 (2018) 47–62.
- Ahmad, Rabiah. Yunos, Zahri " A Dynamic Cyber-Terrorism Framework ", ***International Journal of Computer Sciences and Information Security***, Vol.30, No.30 (2012).
- Herzog, Stephen. "Country in Focus: Ten Years after the Estonian Cyberattacks, Defense and Adaptation in the Age of Digital Insecurity é. ***GEORGETOWN JOURNAL OF INTERNATIONAL AFFAIRS***. VOL.18 N3, (FALL 2017).
- ÖZEREN, Süleyman. "Cyberterrorism and International Cooperation: General Overview of the Available Mechanisms to Facilitate an Overwhelming Task". ***NATO Science for Peace and Security Series*** (SPS). vol.34 (2007).
- Renard, Thomas. "EU Cyber Partnership: Assessing the EU Cyber Strategic Partnerships with Third Countries in the Cyber Domain". ***European Politics and Society***. 19(3), (January, 2018), P-p. 1-17
- Sieber, Ulrich. "international cooperation against terrorist use of the internet"**,** ***Revue internationale de droit pénal,*** Vol. 77, N3. (4-2006)
- V.T.Tsakanyan, " The Role of Cybersecurity in World Politics ", ***Vestnik RUDN***, vol.17, N02,(December 2017), P-p. 339-348
- You ,Wenjing. " The Influence of Cyberculture on Life Style under the Background of new Media ". ***Frontiers in Educational Research***. Vol.3, Issue 5. (2020), P-p. 90-93

رابعا: التقارير.

- S.Nye, Joseph .***Cyber Power***, Belfer Center for Science and International Affairs, Harvard Kennedy School (May 2010).
- European Union Institute for Security Studies, ***EUISS Year book of European Security*** (Y.E.S 2017).
- Europol, ***European Union Terrorism Situation and Trend Report (TE-SAT)***, Publications Office of the European Union, Luxembourg. (2021).
- Zerzri, Mayssa. ***The Threat of Cyber Terrorism and Recommendations for Countermeasures,*** Policy Advice and Strategy Development, Center for Applied Policy Research (04.2017).
- Commission on Science and Technology for Development (CSTD), ***Mapping of international Internet public policy issues***, Eighteenth session, Geneva, 4-(8 May 2015).
- F.Krepinevich, Andrew. ***Cyber Warfare : A Neclear Option ?***, Center for Strategic and Budgetary assessments, 2012.
- Ventre, Daniel. ***A Constructivist Approach of Cyber Security/Cyber Defence Concepts: Lessons of Security Studies Theories and Discursive Analysis*** , Maribor University (23.09.2013).
- Giantas, Dominika. ***Cybersecurity in the UE: Threats, Frameworks and Future Perspectives, Laboratory of Intelligence and Cybersecurity***, Working paper series N.1 (September 2019).
- ENISA, ***Cyber Security Culture in organisations*** (NOVEMBER 2017).
- Weiman, Gabriel. ***Cyber Terrorism: How Real is the Threat?*** Special Report, n119, U.S Institute of Peace (December 2004).
- Papangnou, Georgios. ***Digital Public Transnational Spaces: European Blogs and the European Public Sphere,*** UNU-Cris Working Papers (2013).
- Home Office, Secretary of State for the Home Department, ***Cybercrime Strategy*** (UK, 2010).
- ITU***, Global Cybersecurity Index, Measuring Commitment to Cyber Security (2020)***, 2021.
- ITU, ***Understanding Cybercrime: Phenomena, Challenges and Legal Response*** (September, 2012).

- Kohler, Kevin. ***Estonia's National Cybersecurity and Cyberdefense Posture: Policy and Organizations*** (CYBERDEFENSE REPORT), Cyber Defense Project (CDP), Center for Security Studies (CSS), ETH Zürich (Zürich, September 2020).
- Negreiro, Mar. ***The NIS2 Directive: A High Common Level of Cybersecurity in the EU***, EU Legislation in Progress, European Parliament Research Service (December 2021).
- K. Griffith, Melissa. and Others, Strengthening the EU's Cyber Defence Capabilities, ***Report of a CEPS Task Force, Centre for European Policy Studies*** (CEPS) Brussels (November 2018).
- Allam, Miriam. Damian Gadzinowski***, Combating the Financing of Terrorism: EU Policies, Polity and Politics***, EIPASCOPE (02/2009).
- Trimintzios, Panagiotis. and Others, ***Cybersecurity in the EU common Security and Defence Policy (CSDP): Challenges and Risks for the EU***, European Parliament- Think Thank (16 May 2017).
- Cornish, Paul. and Others, ***Cyberspace and the National Security of the United Kingdom: Threats and Responses***, A Chatham House Report (Mars 2009).
- Llorente, Raquel Vazquez***. A Digital Geneva Convention? The Role of the Private Sector in Cybersecurity***, LES Ideas, Strategic Update (May 2018).
- ***Report of the Working Group on Countering the Use of the Internet for Terrorist Purposes***, Counter-Terrorism Implementation Task Force (CTITF),(February 2009).
- Mattioli, Rossella. Moulinos, Konstantinos. ***Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors*** (Greece : ENISA, 2015).
- SANS Institute, Global Information Assurance Certification Paper (GIAC), ***Information Warfare : Cyber warfare is the Future Warfare*** (2004).
- Voronova, Sofija. ***Understanding EU Counter-Terrorism Policy***, European Parliamentary Research Service (EPRS), (January 2021).
- Tammikko, Teemu. & Tuomas Iso-Markku, ***THE EU'S EXTERNAL ACTION ON COUNTER-TERRORISM: DEVELOPMENT, STRUCTURES AND ACTIONS***, FIIA Report (June 2020), P.24.
- The European Union, ***How the European Union works ? Your Guide to the EU Institutions*** (Brussels: Publications Office, 2012).
- M.LcKenzie, Timothy. ***Is Cyber Deterrence Possible?***, Air Force Research Institute Papers , Alabama : Air University Press, 2017, p.1.

- United Nations Office on Drugs and Crime (UNDOC), United Nations Counter-Terrorism Implementation Task Force, ***The Use of The Internet for Terrorist Purposes*** (UNO: New York, September 2012).
- Zurich Insurance Groupe LTD Foundation ESADE-Center for Global Economy and Geopolitics, ***Risk Nexus: Global Cyber Governance, Preparing for New Business Risks*** (Switzerland, 2015).

خامسا: الرسائل العلمية

- Biller, Jeffrey Thomas. ***Cyber-Terrorism: Finding a Common Starting Point***, Master Thesis of Laws, George Washington University Law School, United States, 2012.
- Castellon Machado, Mario Nicolas. ***Cyber Security Governance: Securing the European Union's Cyber Domain.*** Master's Dissertation in Crisis and Security Management Programme. LeidenUniversity : Faculty of Governance and GlabalAffairs, August 2015.
- Jorgensen, Rick Frank. ***Internet and Freedom of Expression***. European Master Degree in Human Rights and Democratisation. Raoul Wallenberg Institute, 2000-2001.
- Lindvall, Erik. ***More dangerous than guns and tanks: How Cybersecurity is Framed by the EU and Sweden?.*** Master's thesis. Uppsala University: Department of Government, Spring 2020.
- Munk, Tin Hojsgaard. ***Cyber Security in the European Region: Anticipatory Governance and Practices***, A thesis submitted for the degree of Doctor of Philosophy. University of Manchester: Faculty of Humanities, School of Law, 2015.
- Muriuki, Lloyd. ***Terrorism and the Internet: How Weblogs are used to propagandise in the American led war on terrorism***, thesis submitted to the School of Arts and Sciences in partial fulfillment of the requirements for the degree of Master of Arts in International Relations, United States International University Africa Nairobi, July 2006.
- Vodouche, Carolle. ***La Contribution des Dynamiques Internationales Formelles au Renforcement de la Cybersécurité Canadienne***, Mémoire présenté à la faculté des études supérieures, Université de Montréal, en vue

de l'obtention du garde de maitrise en droit (LL.M.), Option : Droit des technologies de l'information, Mai 2015.

سادسا: المداخلات العلمية

- Bilaz, Annamaria, & Others, " Cybersecurity Strategy and Leadership Management Issues ", International May Conference on Strategic Management, Serbia, 25-27 September 2020.
- Helmbrecht–Deutor, Udo. "Cybersecurity: Best Practices", Conference Greece, 12/12/2018.
- Kolini, Farzan. L. Janczewski, "Cyber DefenseCapability Model: A FoundationTaxonomy," submitted to: International Conference on Information Resources Management (CONF-IRM), 2015.
- von Heinegg, Wolff Heintschel. Legal Implications of Territorial Sovereignty in Cyberspace, 4th International Conference on Cyber Conflict, Faculty of Law Europa-Universität, Frankfurt (Oder), Germany, 2012,
- Yamin, Tughral. " Combating Cyber Terrorism through an Effective System of Cyber Security Cooperation ", Terrorism Experts Conference, Ankara, Oct.2015.
- Wæver, Ole. "Aberystwyth, Paris, Copenhagen New 'Schools' in Security Theory and their Origins between Core and Peripherym", Paper presented at the annual meeting of the International Studies Association, Montreal, March 17-20, 2004.
- Reardon, Robert. Choucri, Nazli. " The Role of Cyberspace in International Relations: A View of the Literature ", Paper Prepared for the 2012 ISA Annual Convention, San Diego, April 2012.

سابعا: الروابط الإلكترونية.

- Ablon, Lillian. "The Motivations of Cyber Threat Actors and their use and Monetization of Stolen Data", RAND Corporation, Testimony Presented before the House Financial Services Committee, Subcommittee on Terrorism and Illicit Finance (March15th, 2018), www.rand.org/pubs/testimonies/CT490.html

- Achkoski, Jugoslav. Dojchinovski, Metodjia. "Cyberterrorism and Cybercrime: Threats for Cybersecurity", https://bit.ly/3xi4ec3 (16/03/2022)
- Aftergood, Steven. "Cybersecurity: The cold war online", nature international journal of science, 06 July 2017, https://cutt.us/SLef1 (05/12/2021)
- Alberto Gomez, Miguel. "Bias and Misperception in Cyberspace", CIBER elcano No. 53 - March 2020, https://cutt.us/c7loF (05/12/2021)
- Alexandru, ION. "IMPLEMENTING ENISA'S CYBER SECURITY PLAN IN THE EUROPEAN UNION ", in the 12 international scintific conference trategies, Strategic changes in security a nd international relation, vol 3, April 14-15, 2016, Bucharest, Romania: https://cutt.us/h7IH9 (04/012/2021).

- Alt, Casey. Load, Viral. "The Fantastic Rhetorical Power of the Computer Virus in the Post-9/11 Political Landscape". Österreichische Zeitschrift für Geschichtswissenschaften, https://doi.org/10.25365/oezg-2005-16-3-9 (04/12/2021).
- Baker Beall, Christopher. Mott, Gareth. "Understanding the European Union's Perception of the Threat of Cyberterrorism: A Discursive Analysis", https://onlinelibrary.wiley.com/doi/10.1111/jcms.13300 (10/12/2021)

- Bantman, Constance. "For Jihadist, read Anarchist? The Anarchist Stereotype then and now", Institutt for kriminologi og rettssosiologi, oslo, mars 2011, https://cutt.us/frxyB (10/11/2021).
- Bodid, Sylvia. and Others, " International Cooperation in the face of Cyber-Terrorism: Current Responses and Future Issues", https://www.ejtn.eu/Documents/THEMIS%202015/Written_Paper_France_1.pdf (10/11/2021).
- Broeders, Dennis. and Others," Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy ", 02/06/2021, https://www.tandfonline.com/doi/full/10.1080/1057610X.2021.1928887 (15/11/2021)

- C. Collin, Barry. "The Future of Cyberterrorism," paper presented at the 11th Annual International Symposium on Criminal Justice Issues, University of Illinois at Chicago, 1996, http://afgen.com/terrorism1.html. (21/09/2021)

- C. Rapoport, David. "Terrorism as a Global Wave Phenomenon: Religious Wave", Oxford University Press 26 October 2017, https://cutt.us/tOX5Y (08/12/2021)
- C. Rapoport, David. "Terrorrism and Weapons of the Apocalypse", January 1999, https://cutt.us/2fAMK (09/12/2021)

- Çam , Ömer Tuğrul. "EU official on rising ties between European extreme left", YPG/PKK, Anadolu Agency website, https://cutt.us/bbtDf (14|07|2021)

- Carr, Madeline. "Crossed Wires: International Cooperation on Cyber Security", INTERSTATE - JOURNAL OF INTERNATIONAL AFFAIRS, 2016, issue 2, https://cutt.us/IIqA3 (20/10/2021).
- Carrapico, Helena. Barrinha, André. "The EU as a Coherent (Cyber)Security Actor? ", JCMS 2017 Volume 55. Number 6, 10 May 2017, https://doi.org/10.1111/jcms.12575 (20/10/2021)
- CCDCOE, " LockedShields ", https://ccdcoe.org/exercises/Locked-Shields (20/10/2021).
- Chaudhary, Sanju. "Linkages between cyber terrorism and national security", International Peer Reviewed & Referred Scholarly Research Journal for Interdisciplinary Studies, 2016 Volume 3, Issue 22. Released on 04/3/2015, http://www.srjis.com/pages/pdfFiles/14671953634.%20SANJU%20CHAUDHARY.pdf

- Choi, Kyung-shick. And others, "Spreading Propaganda in Cyberspace: Comparing Cyber-Resource Usage of Al Qaeda and ISIS", International Journal of Cybersecurity Intelligence & Cybercrime, https://www.doi.org/10.52306/01010418ZDCD5438 (06/07/2021).
- Cohen-Almagor , Raphael. In Internet's Way: Radical, Terrorist Islamists on the Free Highway , September 2013, https://cutt.us/uVMol

- Congressional Research Service, "Terrorism Risk Insurance. Overview and Issue Analysis", December 27, 2019, Terrorism Risk Insurance: Overview and Issue Analysis for the 116th Congress (07|05|2021)
- Conway, Maura. "Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet", First Monday, November 2002, Vol. 7, No. 11-4, Reality Bytes (firstmonday.org) (07|05|2021)

- Cornish, Paul. and others, "Cyberspace and the National Security of the United Kingdom Threats and Responses", A Chatham House Report, the Royal

Institute of International Affairs, March 2009, https://www.academia.edu/1242679/Cyberspace_and_the_National_Security_of_the_United_Kingdom (12/02/2022)

- Council of the EU, «Cybersecurity: Council adopts conclusions on the EU's Cybersecurity Strategy», 22/03/2021, https://www.consilium.europa.eu/en/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy/ (12/09/2021)

- Daniel, Dobrygowski. "What would a cyberwar look like?", World Economic Forum, 25 Avril 2018 , https://cutt.us/qLMXI (05/12/2021)

- Denning, Dorothy. "Cyberterrorism", Global Dialogue (Autumn), 24 August 2000, https://cutt.us/pI6ZS (07|05|2021)

- Dharfizi, Awang Dzul-Hashriq. "Non- Conventional Security Risks of the 21st Century", International Security, 15 DECEMBER 2011, https://www.academia.edu/5451801/Non_Conventional_Security_Risks_of_the_21st_Century?email_work_card=title (28/03/2021).

- EU action to counter left-wing and anarchist violent extremism and terrorism: Discussion paper (Council doc. 10101/21, LIMITE, 28 June 2021, pdf) https://cutt.us/hrTEt (11|04|2022)

- EU action to Violent left-wing extremism and anarchism - discussion paper (Council doc. 10180/21, LIMITE, 28 June 2021, pdf) https://cutt.us/NaZnI (11|04|2022)

- EU, "Growing online censorship of presumed violent extremism of all ideological varieties", 04 June 2021, https://cutt.us/krorn (12|01|2022)

- European Commission, "Shaping Europe's Digital Future", https://digital-strategy.ec.europa.eu/en/policies/nis-directiven (15/11/2021)

- European Commission, (191804), "Final Report Summary - CYBERROAD (Development of the CYBER crime and CYBER terrorism research ROADmap)", 15 November 2016, https://cordis.europa.eu/project/id/607642/reporting/fr

- European Commission. (2001c). "Communication on creating a safer information society by improving the security of information infrastructures and combating computer-related crime" (eEurope 2002) COM(2000) 890 final, 26.01.2001. Brussels, Belgium, https://eur-

lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0890:FIN:EN:PDF (21/12/2021)
- European Council of the European Union, " 20 years after 9/11: Achievements and Challenges of EU Counter-Terrorism Efforts ", https://www.consilium.europa.eu/en/events-gsc/live-show-counter-terrorism/ (21/12/2021)
- European Council, Council of the European Union, " Cybersecurity: how the EU tackles cyber threats?", https://www.consilium.europa.eu/en/policies/cybersecurity/ (10/12/2021)
- Europol, "The Internet Organised Crime Threat Assessment 2016". Hague: Europol, 2017 ,www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assess-ment-iocta-2016
- Federal Chancellery, "Austria Cyber Security Strategy 2013", Austrian Cyber Security Strategy (bmi.gv.at)
- Gaub, Florence. "HOW THE ISLAMIC STATE SEES THE FUTURE: Why the end of times does not mean the end", 21 April 2021, How the Islamic State sees the future | European Union Institute for Security Studies (europa.eu) (09/02/2022)
- Ghasemi, Hakem. "Globalization and International Relations : Actors Move from Non- Cooperative to Cooperative Games", https://bit.ly/3MqnABe (15/08/2021)
- Ghasemi, Hakem. "Globalization and International Relations: Actors Move from Non- Cooperative to Cooperative Games", in: https://bit.ly/3MqnABe (15/08/2021)
- Goździewicz, Wiesław. and others, "NATO Road to Cybersecurity", Joanna Świątkowska(Edit), the kosciuszko institute, 2016, https://www.coursehero.com/file/70676850/NATO-Road-to-Cybersecuritypdf/ (7/07/2021).
- Grieve, Lorraine Bowman. "Cyber-terrorism and Moral Panics: A Reflection on the Discourse of Cyber-terrorism". In L. Jarvis, S. MacDonald & T. Chen (Eds), Terrorism Online: Politics, Law and Technology. Oxon: Routledge. (2015), https://cutt.us/pIYML
- H. Kirchner, Dorussen. & Sperling, J. "Sharing the Burden of Collective Security in the European Union". International Organization, https://www.researchgate.net/publication/46545054 (04|11|2021)

- Hua, Jian . Bapna, Sanjay. The economic impact of cyber terrorism Journal of Strategic Information Systems 22 (2013), http://dx.doi.org/10.1016/j.jsis.2012.10.004 (7/07/2021).
- J. Petallides, Constantine. "Cyber Terrorism and IR Theory: Realism, Liberalism, and Constructivism in the New Security Threat", 2012, VOL. 4 NO. 03, HTTPS://CUTT.US/O8GFG
- K. ILVES, LUUKAS. and Others, " European Union and NATO Global Cybersecurity Challenges: A WayForward ", PRISM, Vol. 6, No. 2 (2016) , https://www.jstor.org/stable/10.2307/26470452 (04|11|2021)
- Kańciak, Anna. "In search of EU law in the domain of cyberspace protection – the proposal based on the Cyber-PDCA model", Journal of Cyber Security Technology , Volume 1, Issue 2 (April 2017), P-p : 127-143, 24 May 2017, https://cutt.us/mmEHV (22|05|2021).
- Kaplan, Jeffrey. "Waves of Political Terrorism", Oxford Research Encyclopedias, Politics, 29 October 2021, https://cutt.us/ZfHzc (08/12/2021)
- Karimov, Nurlan. « The European Union Cyber Security and Protection of Human Rights », 01/12/2019, https://www.academia.edu/41452957/The_European_Union_Cyber_Security_and_Protection_of_Human_Rights (11/08/2021)
- Krickeberg, Memphis. "The Internet as a Slippery Object of State Security: The Problem of Physical Border Insensitivity, Anonymity and Global Interconnectedness", JOURNAL OF INTERNATIONAL AFFAIRS, 2016, VOL. 2015/2016 Issue. 2, https://issuu.com/interstate1965/docs/20152016__issue_2_-_the_cyber_issue
- L. Tafoya, William. "Cyber Terror. The Federal Bureau of Investigation". November 1, 2011, https://leb.fbi. gov/2011/november/cyber-terror. (08/09/2022).
- Lee, Choi. and Cardigan, "Spreading Propaganda in Cyberspace: Comparing Cyber Resource Usage of Al Qaeda and ISIS", International Journal of Cybersecurity Intelligence and Cybercrime, https://cutt.us/nS5cd
- Lobato, Luiza Cruz Kenkel, & Kai Michael. "Discourses of cyberspace securitization in Brazil and in the United States", Revista Brasileira de Política Internacional, 58(2), https://cutt.us/YjRuu (04|04\2022)
- Malec, Mieczyslaw. "Security perception within and beyond the traditional approach", Monterey, California. Naval Postgraduate School, Master of Arts in National Security Affairs, Naval Postgraduate School, juin 2003, http://hdl.handle.net/10945/951 (23|02|2022)

- Maxey, Levi. "Terror Finance in the Age of Bitcoin", Indian Strategic Studies, 16 JUNE 2017, https://www.strategicstudyindia.com/2017/06/terror-finance-in-age-of-bitcoin.html?m=1

- Pawlak, Patryk .and Van Raemdonck, Nathalie. "What if…the Sun led to a Cyberwar?", in: Florence Gaub (Editor), What If…? Scanning The Horizon: 12 Scenarios For 2021. Paris: European Union Institute for Security Studies (EUISS), January 2019, https://cutt.us/iVc4i

- Prime Minister's Office, "Special Action Plan for Cyber Terrorism Countermeasures for Critical Infrastructure", December 15, 2000 , https://cutt.us/OTgKv (01/06/2020)

- Raphaël Moncada ,"The European Digital Single Market », 16/10/2017, https://www.eyes-on-europe.eu/the-european-digital-single-market (01/06/2020)

- Rivera Pastor, Rafael. & others, "Achieving a sovereign and trustworthy ICT industry in the EU", EPRS | European Parliamentary Research Service Scientific Foresight Unit December 2017PE 6 (STOA) 14 . 531, https://cutt.us/YE0dl (01/06/2020).

- Ruohonen, Jukka. "An Acid Test for Europeanization: Public Cyber Security Procurement in the European Union", European Journal for Security Research (2020), https://doi.org/10.1007/s41125-019-00053-w (21/09/2021)

- Sartori, Giovanni. "Concept Misformation in Comparative Politics", The American Political Science Review, Vol. 64, No. 4 (Dec., 1970), http://www.jstor.org/stable/1958356 (21/06/2020)

- Smith, Brad. & Chair, Vice. "The need for a Digital Geneva Convention ", 14/02/2017, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/ (21/06/2020)

- Soesanto, Stefan. " Cyber Terrorism : Why it exists ? Why it doesn't ? and Why i twill ? ", real instituto elcano, https://cutt.us/PfXHT (17/04/2020)

- Stevens, Tim. " Reading Power in UK Cybersecurity", https://www.academia.edu/1157394/Reading_Power_in_UK_Cybersecurity (30/12/2021).

- Tafoya, W. L. "Cyber Terror. The Federal Bureau of Investigation," November 1, 2011, https://leb.fbi.gov/articles/featured-articles/cyber-terror (10/11/2021).

- Tidy, Joe. "Ukraine cyber-attack: Russia to blame for hack, saysKyiv ",BBC,14 January, https://www.bbc.com/news/world-europe-59992531(22/02/2022)

- Tomic, Dusko and others, " Cybersecurity Policies of East European Countries ", Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense, https://cutt.us/gWA8R (09|05|2021).

- Ulusoy H. "Collective Security in Europe Perceptions", *Journal* of *International Affairs*. 2002; 7(4) https://dergipark.org.tr/en/pub/perception/issue/49013/625259 (04/12/2021).

- UNODC, " Regional Counter-Terrorism Approaches", https://www.unodc.org/e4j/en/terrorism/module-5/key-issues/european-region.html (3/01/2022).

- Urbinati, Martina Lucarelli, Sonia. "The Securitization of Cyberspace : Building the Cyber Resilient European Union of Tomorrow", https://www.academia.edu/41650573/The_Securitization_of_Cyberspace_Building_the_Cyber_Resilient_European_Union_of_Tomorrow (11/01/2022).

- Valeriano, Brandon. C. Maness, Ryan. "International Relations Theory and Cyber Security: Threat, Conflict, and Ethics in an Emergent Domain", April 2018, https://www.researchgate.net/publication/326845990_International_relations_theory_and_cyber_security_Threats_conflicts_and_ethics_in_an_emergent_domain (04/012/2021).

- Valeriano, Brandon. C. Maness, Ryan. “International Relations Theory and Cyber Security : Threat, Conflict, and Ethics in an Emergent Domain”, April 2018, in: https://www.researchgate.net/publication/326845990_International_relations_theory_and_cyber_security_Threats_conflicts_and_ethics_in_an_emergent_domain (04/012/2021).

- W.Brenner,Susan. " Cybercrime, Cyberterrorism and Cyberwarfare ", Revue Internationale de Droit Pénal, vol.77, n.3-4 (2006), http://www.cairn.info/revue-internationale-de-droit-penal-2006-3-page-453.htm (07/08/2020).

- Williamson, Graham. "OT, ICS, SCADA – What's the difference?", kuppingercole Analysts, Jul 07, 2015, https://cutt.us/yXPP7 (24-12-2021)
- Yamin, Tughral. "Combating Cyber Terrorism through an Effective System of Cyber Security Cooperation", Terrorism Expert Conference, Ankara; October 2015, https://cutt.us/oKGxX (05/12/2021).
- "The Software Alliance (BSA), EU Cybersecurity Dashboard : A Path to a Secure European Cyberspace?", https://cybersecurity.bsa.org/ (21/10/2021).
- "Cyber Defense », 02/07/2021, https://www.nato.int/cps/en/natohq/topics_78170.htm (15/09/2021)
- "NIS Directive", https://www.enisa.europa.eu/topics/nis-directive (15/11/2021)
- "Opening Statement of Chairman Lieberman, Joseph. Securing 's Future: The American Cybersecurity Act of 2012": Before the Sen. Homeland Security and Governmental Affairs Committee, 112th Cong. (2012) (statement of Sen. Lieberman, Chairman, http://www.fdsys.gov/
- "The EU Code of conduct on countering illegal hate speech online, The robust response provided by the European Union", https://cutt.us/JKv1I (10/10/2021).
- « Eurojust », https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/eurojust_en (15/10/2021)
- « Cyber Defense », publié le : 08/07/2021, https://www.nato.int/cps/fr/natohq/topics_78170.htm (15/10/2021)

- « Definitions of Cybernetics in the Course of the Century », Department of Cybernetics, http://www.kky.zcu.cz/en/definitions-of-cybernetics
- « EU-NATO Cooperation », https://www.consilium.europa.eu/en/policies/defence-security/ (11/12/2021)
- « European Union Agency for Law Enforcement Training (CEPOL) », https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/cepol_en (23/04/2021)
- « Main Reports », 06/12/2021, https://www.europol.europa.eu/publications-events/main-reports (30/12/2021)

- « Module 14 : Hacktivism, Terrorism, Espionage, Disinformation Campaigns and Warfare in Cyberspace », https://www.unodc.org/e4i/en/cybercrime/module-14/key-issues/cyberterrorism.html
- « Resilience and Article 3 », 11/06/2021, https://www.nato.int/cps/en/natohq/topics_132722.htm (15/09/2021)
- « Smart Defence », https://www.nato.int/cps/en/natohq/topics_84268.htm (13/09/202)
- (U//FOUO), "Leftwing Extremists Likely to Increase Use of Cyber Attacks over the Coming Decade", U.S. Department of Homeland Security :The Strategic Analysis Group, Homeland Environment and Threat Analysis Division, 09/01/2019, in: https://irp.fas.org _ (08\07\2021)

باللغة الفرنسية:

أولا: الوثائق الرسمية.

- Commission Européenne, La Haute Représentation de l'Union Européenne pour les Affaires Etrangeres et la Politique de Sécurité, ***Stratégie de Cyber Sécurité de l'Union Européenne : un cyberspace ouvert, sur et sécurisé***, Communication conjointe au parlement Européen, au conseil, au comité économique et sociale Européen et au comité des régions, (Bruxelles, Juin 2013).
- Richardson, Janice et autres, "Manuel de Maitrise de l'Internet : Accompagner les utilisateurs dans le Monde en Ligne", ***Conseil de l'Europe*** (Décembre 2017).
- United Kingdom, ***Stratégie Nationale de Cyber Sécurité*** : 2016-2021, (2016).

ثانيا: الكتب

- Chitour, Chems Eddine. ***Mondialisation : l'Espérance ou le Chaos?***, Alger : ANEP, 2002.

- Denis, Jeffrey. "La Radicalisation des Jeunes Djihadistes" , in : Denis Jeffrey, et autres, ***Jeunes et Djihadisme : Les Conversions Interdites.*** Canada : Presses de l'Université Laval, 2016.

- Von Clausewitz, Carl. ***De la guerre***, Trad. Nicolas Waquet, Paris: Rivages poche, 2006.

ثالثا: المجلات والدوريات

- Dupuy, Emmanuel. " Quels enjeux politiques en matière de cyber défense ? ". ***Revue Militaire***. N1 (Janv.-Fév. 2013).
- Deschaux-Dutard, Delphine. " L'Union Européenne : Une cyberpuissance en devenir ? Réflexion sur la cyberdéfence Européenne ", ***Revue Internationale et Stratégique***. N°117 (1/2020).
- J. Klein, John." La Rétribution et la Dissuasion du Cyber Terrorisme ", ***Afrique et Francophonie*** (2018).
- Leman-Langlois, Stéphan, "Questions au Sujet de le Cybercriminalité, le Crime Comme moyen de Contrôle du Cyberspace Commercial ". ***Criminologie***, Vol. 39. N1, (Jun 2006), p. 63–81
- M. Knopf, Christina. J. Ziegelmayer, Eric. " La Guerre de Quatrième Génération et la Stratégie des Médias Sociaux des Forces Armées Américaines ", ***Afrique et Francophonie***, 2012.

ثالثا: التقارير.

- Centre de Recherches Internationales, Centre d'Etudes Européenne et de Politique Comparée, ***Compte-rendu de la 45ème séance, Djihad : Une Définition Scientifique est-elle Possible ? Les Sciences Sociales en Question : Grandes Contreverses Epistémologiques et Méthodologiques***.
- Cours de Comptes Européennes, ***Défis à relever pour une Politique de l'UE Efficace dans le Domaine de la Cyber Sécurité***, Document d'Information (Mars 2019).
- Le Centre pour la Gouvernance du Secteur de Sécurité, ***Guide pour la Bonne Gouvernance de la Cyber Sécurité*** (Genève, 2019).
- Ravel, Rémi. ***La Cyber-Coopération Européenne***, Les publications des jeunes IHEDN (Rapport, 2018).
- ITU, ***Programme de Cyber Sécurité***, Groupe d'experts chargé de la pondération de l'indice GCI (Aout 2020).
- Gendron, Angela. Martin Rudner, ***Evaluation des Cybermenaces Pesant Contre les Infrastructures du Canada,*** Rapport Préparé pour le Service Canadien du Renseignement de Sécurité (Mars 2012).

- Délégation Ministérielle aux Industries de Sécurité et à la Lutte contre les Cybermenaces, ***État de la Menace Liée au Numérique en 2017***, Rapport n1 (Janvier 2017).
- Sénat de Canada, ***Liberté, Sécurité et la Menace Complexe du Terrorisme : Des Défits pour l'Avenir,*** Rapport Intérimaire du Comité Sénatorial Spécial sur l'Anti-terrorisme (Mars 2011).
- Tremblay, Monica. ***Analyse des Impacts de la Mondialisation sur la Sécurité au Québec, Rapport 5 : De la Cybercriminalité au Déploiement de la Cybersécurité***, Canada : École Nationale d'Administration Publique, Laboratoire d'Etude sur les Politiques Publiques et la Mondialisation (Décembre 2007).
- Wolf, Philippe. Valée, Luc. ***Cyber-Conflits, Quelques Clés de Compréhension, Cybercriminalité***, INHESJ/ONDRP Rapport (2011).

رابعا: الرسائل العلمية

- Kokel, Marion. ***The Engagement of NATO in Cybersecurity: Securing the 5th Battlefield.*** Mémoire présenté en vue de l'obtention du grade de Master en Sciences Politiques, Orientation Relations Internationales-Finalité Sécurité, Paix, Conflits. UNIVERSITE LIBRE DE BRUXELLES, UNIVERSITE D'EUROPE, FACULTE DES SCIENCES SOCIALES ET POLITIQUES, 2013-2014.
- Labrie, Mathieu. ***La Sécurisation du Cyberterrorisme aux Etats-Unis***, Mémoire présenté comme exigence partielle de la maitrise en Science Politique, Canada : Université du Québec à Montréal, 2011.

خامسا: الروابط الإلكترونية.

- Ben Boubaker, Khobeib. "SCADA et cybersécurité industrielle : de l'importance de maîtriser le jargon", https://cutt.us/zGH0t (18| 11| 2021)
- « Cybercriminalité : Un Défi à Relever aux niveau National et International », www.senat.fr/rap/119-613/r19-6138.html (02.11.2021).
- « L'OTAN dans la cyber guerre : Stratégie globale et capacités opérationnelles », Publié le : 17/04/2017, http://www.diploweb.com/L-OTAN-

dans-la-cyberguerre-stratégie-globale-et-capacités-opérationnelles.html (10/11/2021).
- EC3, « Le Centre Européen de la Lutte Contre la Cyber-Crime », https://www.guidedetective.fr/articles/ec3-le-centre-européen-de-lutte-contre-la-cybercrime (15/09/2021).
- « L'OTAN ouvre un nouveau centre d'excellence sur la Cyber Défense », publié le : 14/05/2008, https://www.nato.int/cps/fr/natohq/news_7266.htm?selectedLocale=fr

(15/10/2021).

- Berthelet, Pierre. "Aperçu de la lutte contre la Cybercrime dans l'Union Européenne ", Revue de science criminelle et de droit pénal comparé, 1(N1) , (2018), https://www.cairn.info/revue-de-science-criminelle-et-de-droit-penal-compare-2018-1-page-59.htm (15/09/2021).
- *Tristan Gaudiaut, Les pays les plus touchés par des cyberattaques massives, Specops Software, 14 janv. 2022, Available on : https://cutt.us/vM7S7* (15/01/2022).

باللغة الروسية:

أولا: المجلات

- Халимат Алиевна, Аккаева. МЕЖДУНАРОДНЫЙ КИБЕРТЕРРОРИЗМ КАК ПОЛИТИЧЕСКИЙ ФЕНОМЕН, Социально-политические науки 1, (2018).

ثانيا: الاطروحات

- Николаевна, Екатерина. Молодчая. ПОЛИТИКА ПРОТИВОДЕЙСТВИЯ КИБЕРТЕРРОРИЗМУ В СОВРЕМЕННОЙ РОССИИ: ПОЛИТОЛОГИЧЕСКИЙ АСПЕКТ, диссертации на соискание ученой степени кандидата политических наук Москва,

РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ СОЦИАЛЬНЫЙ УНИВЕРСИТЕТ, 2011.

ثالثا: المواقع الالكترونية

- Константин Петрович, Курылев. ПОНЯТИЕ "МЕЖДУНАРОДНЫЙ ТЕРРОРИЗМ" СОГЛАСНО КОНСТРУКТИВИСТСКОЙ ШКОЛЕ МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ, ЖУРНАЛ ПОЛИТИЧЕСКИХ ИССЛЕДОВАНИЙ Том 3 N 1, 2019, доступны на: https://naukaru.ru/ru/nauka/article/28091/view

قائمة الأشكال والجداول والخرائط

قائمة الأشكال والجداول والخرائط:

الخرائط:

قائمة المختصرات

قائمة المختصرات:

الاختصار	باللغة الإنجليزية	باللغة العربية
C-PROC	Cyber Programme Office-Council of Europe	مكتب البرنامج السيبراني التابع لمجلس أوروبا
C3	Consultation, Commandement, Control	اللجنة الثلاثية (استشارة، قيادة، تحكم)
CCD-COE	The NATO Cooperative Cyber Defence Center of Excellence	مركز التميز للدفاع السيبراني التعاوني (حلف الناتو)
CEPOL	European Union Agency for Law Enforcement Training	وكالة الاتحاد الأوروبي للتدريب على إنفاد القانون
CI	Critical Infrastructure	البنية التحتية الحرجة
CII	Critical Information Infrastructure	البنية التحتية المعلوماتية الحرجة
CIIP	Critical Information Infrastructure Protection	حماية البنية التحتية المعلوماتية الحرجة
CIRTS	Computer Emergency Response Teams	نُظم الاستجابة لطوارئ الكمبيوتر
CMM	The Cybersecurity Capacity Maturity Model for Nations	نموذج نضج قدرات الأمن السيبراني للدول (نموذج أوكسفورد)
CODEXTER	Committee of Experts on Terrorism	لجنة الخبراء حول الإرهاب التابعة لمجلس أوروبا
CoE	Council of Europe	مجلس أوروبا
CONTEST	Couner-Terrorism Strategy	إستراتيجية مكافحة الإرهاب (المملكة المتحدة)
CSC	Cyber Security Culture	ثقافة الأمن السيبراني
CSDP	The Common Security and Defence Policy	سياسة الأمن والدفاع المشتركة
CSS	Cyber Security Strategy	استراتيجية الأمن السيبراني
CTIRU	Counter-Terrorism Internet Referral Unit	وحدة الإحالة عبر الانترنت لمكافحة الإرهاب (المملكة المتحدة)
CTW	Check The Web	تحقق من الشبكة
CVE	Counter Violent Extremism	مكافحة التطرف العنيف
EC	European Commission	المفوضية الأوروبية
EC3	European Cyber Crime Center	المركز الأوروبي لمكافحة الجريمة السيبرانية
ECDP	the Enhanced Cyber Defence Policy	سياسة الدفاع السيبراني المحسّنة
ECI	European Critical Infrastructure	البنية التحتية الحرجة الأوروبية

نظام شهادات السجلات الجنائية الأوروبية (اللامركزية)	European Union Criminal Record Certificates System	**ECRIS**
المنظمة الأوروبية للأمن السيبراني	European Cyber Security Organisation	**ECSO**
وكالة الدفاع الأوروبية	European Defence Agency	**EDA**
نظام الإنذار ومشاركة المعلومات الأوروبي	European Information Sharing and Alerting System	**EISAS**
الشبكة الأوروبية للخبراء حول التطرف	The European Network of Experts on Radicalisation	**ENER**
الوكالة الأوروبية لأمن الشبكات والمعلومات	European Union Networks and Informations Security Agency	**ENISA**
الشراكة الأوروبية عام–خاص من أجل المرونة	European Public-Private Partnership for Resilience	**EP3R**
البرنامج الأوروبي لحماية البنية التحتية الحرجة	European Programm of Critical Infrastructure Protection	**EPCIP**
سياسة الفضاء الإلكتروني الدولية للاتحاد الأوروبي	European Union-International Cyberspace Policy	**EU-ICP**
الوكالة الأوروبية للإدارة التشغيلية لأنظمة تكنولوجيا المعلومات واسعة النطاق في مجال الحرية، الأمن والعدالة	European Union Agency for Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice	**EU-LISA**
قاعدة بيانات فحص طلب اللجوء الأوروبي	European Asylum Dactyloscopy Database	**EURODAC**
وكالة الاتحاد الأوروبي للتعاون في العدالة الجنائية	The European Union Agency for Criminal Justice Cooperation	**EUROJUST**
مكتب الشرطة الأوروبية	European Police Office	**EUROPOL**
تكنولوجيا أنظمة التعرف على الوجه	Facial Recognition Systems Technology	**FIRST**
ملف التبليغات للوقاية من الراديكالية الإرهابية	Reports File for the Prevention of Terrorist Radicalizatio	**FSPRT**
المقاتلون الإرهابيون الأجانب	Foreign Terrorist Fighters	**FTF**
مؤشر الأمن السيبراني العالمي	Global Cybersecurity Index	**GCI**
أنظمة التحكم الصناعي	Industrial Control Systems	**ICS**
أنظمة التحكم الصناعي– نظام التحكم الإشرافي واكتساب البيانات (نموذج تقييم نضج الأمن السيبراني)	Industrial Control Systems-Supervisory Control and Data Acquisition	**ICS-SCADA**

تكنولوجيا المعلومات والاتصالات	Information and Communications Technologies	**ICTs**
مؤسسة البيانات الدولية	International Data Corporation	**IDC**
أنظمة كشف التسلل	Intrusion Detection System	**IDS**
المجموعة الدولية للخبراء	International Groupe of Experts	**IGE**
القانون الدولي الإنساني	International Humanitarian Law	**IHL**
الشراكة الدولية المتعددة الأطراف لمواجهة التهديدات السيبرانية	The Internation Multilateral Partnership Against Cyber Threats	**IMPACT**
منظمة الشرطة الجنائية الدولية	The International Criminal Police Organisation	**Interpol**
تقييم تهديد الجريمة المنظمة عبر الانترنت	Internet Organised Crime Threat Assessement	**IOCTA**
وحدة الإحالة عبر الانترنت في الاتحاد الأوروبي	Internet Referral Unit	**IRU**
مزودو خدمة الانترنت	Internet Service Providers	**ISP**
قانون النزاعات المسلحة	Law of Armed Conflict	**LOAC**
وكالة الاتصالات والمعلومات التابعة للناتو	NATO Communications and Informations Agency	**NCIA**
وكالة خدمات أنظمة المعلومات والاتصال	The NATO Communication and Information Systems Services Agency	**NCSA**
عملية التخطيط الدفاعي لحلف الناتو	NATO Defence Planning Process	**NDPP**
القانون الألماني لإنفاذ الشبكات	Germany's Network Enforcement Act	**NetzDG**
أمن الشبكات والمعلومات	Networks and Informations Security	**NIS**
منظمة الدول الأمريكية	Organisation of American States	**OAS**
منظمة الأمن والتعاون في أوروبا	Organisation of Security and Cooperation in Europe	**OSCE**
ذكاء المصدر المفتوح	Open Source Intelligence	**OSI**
التكنولوجيا التشغيلية	Operational Technology	**OT**
نموذج دمينغ: خطّط، افعل، أُدرس، نفّذ	Plan-Do-Study-Act	**PDSA**
تسجيل أسماء الركاب	Passenger Name Record	**PNR**
الشراكة الأوروبية بين القطاعين العام والخاص	The European Public-Private Partnership	**PPP**
جودة الخدمة	Quality of Service	**QoS**

رادار التطرف الإسلاموي	The Radar of Islamistic Extremism	**RADAR Ite**
شبكة التوعية بالتطرف	The Radicalisation Awareness Network	**RAN**
أنظمة التحكم الإشرافي واكتساب البيانات	Supervisory Control and Data Acquisition	**SCADA**
منظمة شنغهاي للتعاون	Shanghai Cooperation Organisation	**SCO**
الإعلان العالمي لحقوق الإنسان	The Universal Declaration of Human Rights	**UDHR**

ملخص الدراسة

ملخص:

تعالج الأطروحة إشكالية التأثير الاستراتيجي للإرهاب الإلكتروني على الأمن الأوربي، وذلك انطلاقا من كون تكنولوجيا المعلومات أصبحت في صلب الاهتمامات الأمنية للمجتمعات الأوروبية وقضايا الأمن العليا من ناحية، وبالنظر إلى القلق والهاجس الأمني الذي بات يشكله هذا التهديد بالنسبة للحكومات الأوروبية من ناحية أخرى.

وبين تكتيكات الإرهابيين واستراتيجيات الدول مثلت هذه الدراسة محاولة لتقديم فهم معمق للتصور الأمني الأوروبي للإرهاب السيبراني، وبالتالي لإستراتيجيات مواجهته، بما فيه من فواعل متباينة الإدراك والتصور ضمن حيز جغرافي يميزه اختلاف المدركات والتصورات. وهنا يستهدف الموضوع بالأساس البحث في تراتب منهجي، أمكن من خلاله اختبار فرضيات الدراسة، وقد جرى هذا الاختبار وفق نظريات الأمن الموسع قصد فهم وضع وتأثير ومنه أمننة قضية الإرهاب السيبراني في الأجندة الأوربية، وما أفرزته من مخرجات في صورة استراتيجيات الأمن والحوكمة السيبرانية، وذلك عبر النهج المتعدد التخصصات الذي تبنّته الدول الأوروبية والاتحاد الأوروبي تحديدا في مواجهة هذه الظاهرة الخطيرة وتأثيرها في البنى التحتية الحرجة واستقرار المجتمعات الأوروبية، وما رافق ذلك من رهان تقني-سياسي وقانوني- تشريعي، فضلا عن مكانة الاتحاد الأوروبي وتوقعاته باعتباره جهة أمنية فاعلة عبر المنصات الخطابية لمؤسساته.

وختاما، خلصت الدراسة إل أن الإرهاب السيبراني يمثل تهديدًا واضحًا للمجتمعات والحكومات الأوروبية، نتيجة وجود فجوات استغلها الإرهابيون السيبرانيون. وبالرغم من أنه يحمل في طياته تركيزا سياقيا يسيطر عليه الطابع الأوروبي، إلا أنه كنهج تجريبي يسعى الى التقاط عمليات التعاون التنظيمي والنظامي بين الفواعل الأمنية. وعليه، فإن الجهود الأوروبية في سياق تنظيم الفضاء السيبراني وبناء منظومة مؤسساتية وقانونية رادعة تبقى معتبرة، في مكافحة الارهاب السيبراني، خاصة في مجال التنسيق داخل الاتحاد الأوربي وخارجه. وهكذا فإن الدراسة كانت بمثابة اقتراح خارطة طريق سيبرانية، للمضي قُدمًا نحو تحيين المنظومة الأمنية لمواجهة مثل هذه التهديدات في المستقبل.

الكلمات المفتاحية: الإرهاب السيبراني، الأمن الأوروبي ، التهديدات السيبرانية، الأمن السيبراني، البنية التحتية الحرجة.

Résumé:

La thèse aborde la problématique de l'impact stratégique du Le cyber-terrorisme sur la sécurité européenne Partant du fait que les technologies de l'information sont devenues au cœur des préoccupations sécuritaires des sociétés européennes et des enjeux sécuritaires supérieurs d'une part, et compte tenu de la préoccupation sécuritaire et l'inquiétude que cette menace présente pour les gouvernements européens d'autre part.

Et entre les tactiques des terroristes et les stratégies des pays, cette étude à tenter de fournir une compréhension approfondie de la perception sécuritaire européenne du cyber-terrorisme, et donc des stratégies pour y faire face, et ça devant une panoplie d'acteur asymétrique et qui diverge catégoriquement, soit sur le plan des perceptions ou des visions. L'étude a été menée selon un ordre méthodologique à travers laquelle il a été possible de tester les hypothèses selon le concept élargie de la sécurité, afin de comprendre l'état et l'impact, et notamment la sécurisation, de la question du cyber-terrorisme dans L'agenda européen, et ses résultats sous forme de stratégies de cyber-sécurité et de gouvernance cybernétique. Une approche multidisciplinaire adoptée par les pays européens et l'Union européenne en particulier face à ce phénomène dangereux par son impact, soit sur les infrastructures sensibles, soit sur la stabilité des sociétés européennes ; et part l'enjeu technico-politique et juridico-législatif qui l'accompagne. Ainsi que la position et les attentes de l'Union européenne en tant qu'Actorness de sécurité à travers les plates-formes rhétoriques de ses institutions.

En fin, l'étude c'est conclu que le cyber-terrorisme constitue une menace claire pour les sociétés et les gouvernements européens, en raison de l'existence de failles exploitées par les terroristes. Et bien qu'il comporte une orientation contextuelle dominée par le caractère européen. Cependant, en tant qu'approche expérimentale, elle cherche à saisir les processus de coopération organisationnelle et réglementaire entre les acteurs de la sécurité. Ainsi, les efforts européens dans le cadre de la régulation du cyberespace et la construction d'un système institutionnel et juridique dissuasif restent importants dans la lutte contre le cyber terrorisme, notamment dans le domaine de la coordination à l'intérieur et à l'extérieur de l'Union européenne. Ainsi, l'étude était une suggestion de feuilles de route cybernétique, pour aller de l'avant vers la modernisation du système de sécurité et faire face à de telles menaces à l'avenir.

Mots-clés: Cyber terrorisme, Sécurité européenne, Cyber menaces, Cyber sécurité, Infrastructures critiques.

Abstract:

The thesis addresses the issue of the strategic impact of cyber-terrorism on European security, starting from the fact that information technologies have become at the heart of the security concerns of European societies and higher security issues on the one hand, and given the security concern and anxiety that this threat presents to European governments on the other hand.

And between the tactics of terrorists and the strategies of countries, this study attempts to provide an in-depth understanding of the European security perception of cyber-terrorism, and therefore of the strategies to deal with it, and that in front of a panoply of asymmetric actors and which diverges categorically, either in terms of perceptions or visions. The study was carried out according to a methodological order through which it was possible to test the hypotheses according to the extended concept of security, in order to understand the state and the impact, and in particular the security of the cyber-terrorism in the European agenda, and its results in the form of cybersecurity and cyber governance strategies. A multidisciplinary approach adopted by European countries and the European Union in particular in the face of this dangerous phenomenon due to its impact, either on sensitive infrastructures or on the stability of European societies; besides of the technical-political and legal-legislative bet that accompanies it. As well as the position and expectations of the European Union as a Security Actor through the rhetorical platforms of its institutions.

In the end, the study concluded that cyber-terrorism poses a clear threat to European societies and governments, due to the existence of loopholes exploited by terrorists. And although it has a contextual orientation dominated by the European character. However, as an experimental approach, it seeks to capture the processes of organizational and regulatory cooperation between security actors. Thus, European efforts within the framework of the regulation of cyberspace and the construction of a dissuasive institutional and legal system remain important in the fight against cyber terrorism, particularly in the field of internal and external coordination of the European Union. Thus, the study was a suggestion of cyber roadmaps, to move forward towards modernizing the security system and dealing with such threats in the future.

Keywords: Cyber terrorism, European security, Cyber threats, Cyber security, Critical infrastructures.

فهـــرس المحـــتويات

الفهرس