سياسات مكافحة الإرهاب السيبراني: نماذج مختارة

م . د عبد الرحمن محمد عيسى
كلية العلوم السياسية/ جامعة النهرين

م . م سيف نبهان إسماعيل
كلية العلوم السياسية/ جامعة النهرين

م . د مصطفى صادق عواد
كلية العلوم السياسية/ جامعة النهرين

ركّز البحث على فهم طبيعة الإرهاب السيبراني كتهديد غير تقليدي يتجاوز الحدود الجغرافية، ويصعّب عملية التتبع والإسناد القانوني، مما يتطلب آليات استجابة معقدة ومتعددة المستويات، وفي هذا الإطار، يسلط البحث الضوء على الأنموذج الأمريكي في مكافحة الإرهاب السيبراني، الذي يعتمد على استراتيجيات استباقية وتشريعات فدرالية وأوامر تنفيذية متقدمة، إلى جانب التعاون بين القطاعين العام والخاص، كما يستعرض الأنموذج الأوروبي الذي يتبنى نهجًا جماعيًا يوازن بين الحماية الأمنية والحريات الرقمية، عبر تشريعات موحدة وهيئات تنسيقية متخصصة، و يهدف البحث إلى تحليل هذه النماذج وتقديم رؤية علمية لفهم آليات الاستجابة المختلفة، مع التأكيد على أهمية تطوير سياسات متكاملة ومرنة تواكب تطور التهديدات الرقمية، وتستند إلى التعاون الدولي والحوكمة التقنية والقانونية.

الكلمات المفتاحية: الإرهاب، الإرهاب السيبراني، الأمن السيبراني.

Policies of Combating Cyberterrorism: Selected Models

Dr. Abdulrahman Muhammed Isa
Al-Nahrain University/ College of Political Sciences

Asst. Inst. Saif Nabhan Ismael
Al-Nahrain University/ College of Political Sciences

Dr. Mustafa Sadiq Awad
Al-Nahrain University/ College of Political Sciences

The research focused on understanding the nature of cyberterrorism as a non-traditional threat that transcends geographical boundaries and complicates the processes of tracking and legal attribution. This complexity necessitates multi-level and sophisticated response mechanisms. Within this framework, the study highlights the American model in combating cyberterrorism, which relies on proactive strategies, federal legislation, advanced executive orders, and cooperation between the public and private sectors. It also reviews the European model, which adopts a collective approach that balances security protection with digital freedoms, through unified legislation and specialized coordination bodies. The research aims to analyze these models and provide a scientific insight for understanding the various response mechanisms, emphasizing the importance of developing integrated and flexible policies that keep pace with the evolving digital threats and are based on international cooperation, as well as technical and legal governance.

Keywords: Terrorism, cyberterrorism, cyber security.

الاستلام	الإرجاع	القبول
2025/5 /12	2025/ 5/ 18	2025/ 5/22

المقدمة

تصاعدت في العقود الأخيرة وتيرة التهديدات الإرهابية بفعل التقدم التكنولوجي المتسارع، إذ لم تعد الحروب تقتصر على ساحة المعركة التقليدية، بل باتت الفضاءات الرقمية تستخدم كجبهات جديدة للصراع، وقد أفرز هذا التحول مفهوما معقدا ومتعدد الأبعاد يعرف بـ"الإرهاب السيبراني"، وهو نوع من الإرهاب يوظّف تقنيات المعلومات والاتصالات بهدف زعزعة استقرار الدول، وتهديد أمن المجتمعات من خلال هجمات إلكترونية تستهدف البنى التحتية الحيوية، أو تنشر الخوف والارتباك عبر أدوات غير تقليدية كالتضليل الإعلامي، والهجمات على البيانات، ومع تطور قدرات الجماعات الإرهابية الرقمية أصبحت الدول ملزمة بإعادة صياغة سياساتها الأمنية والقانونية لمواجهة هذا النوع الجديد من التهديدات، الذي يتجاوز في طبيعته الحدود الجغرافية، ويعقّد مسألة تتبع الجناة وتحديد الجهة المسؤولة، وضمن هذا السياق تبلورت جهود متباينة على المستويين الدولي والإقليمي لمكافحة الإرهاب السيبراني تتراوح بين التشريعات، والاستراتيجيات الوقائية، والآليات التقنية، وهو ما يستدعي تحليلاً مقارنا لأبرز هذه النماذج.

يمثل الأنموذجان الأمريكي والأوروبي في مكافحة الإرهاب السيبراني تجربتين غنيتين من حيث تنوع السياسات، وتطور الأطر القانونية والمؤسسية، فالولايات المتحدة بوصفها إحدى القوى الرائدة في مجال الأمن السيبراني اعتمدت نهجا هجوميا واستباقيا يرتكز على مبادئ "الدفاع الموزع" والتعاون الاستخباراتي مع القطاع الخاص مدعوما بمنظومة تشريعية قوية مثل قانون USA PATRIOT Act وأوامر رئاسية تعنى بحماية سلسلة التوريد الرقمية، في المقابل تبنى الاتحاد الأوروبي مقاربة شاملة تمزج بين صلابة التشريع، والتنسيق المؤسساتي متعدد المستويات، والالتزام بحقوق الإنسان، وحماية الخصوصية الرقمية، من خلال توجيهات مثل NIS2 و DSA، وأجهزة متخصصة كـ ENISA و CERT-EU. ومن هنا تنبع أهمية هذه الدراسة في فهم تمايز واختلاف السياقات القانونية والسياسية بين الأنموذجين، ومدى فاعلية كل منهما في التصدي لخطر الإرهاب السيبراني وصولاً إلى استخلاص أفضل الممارسات القابلة للتطبيق على النطاقات الإقليمية الأخرى.

أولًا: إشكالية البحث

تتمثل إشكالية البحث في التساؤل عن مدى فاعلية السياسات التي تتبعها الولايات المتحدة والاتحاد الأوروبي في مكافحة الإرهاب السيبراني، وفيما إذا كانت هذه السياسات قادرة على التكيف مع تطور التهديدات الرقمية وتعقيدها التقني والقانوني، مع مراعاة التوازن بين الأمن وحقوق الإنسان.

ثانيًا: أهمية البحث

تكمن أهمية هذا البحث في كونه يتناول واحدة من أكثر الظواهر تهديدا للأمن القومي والسلم الدولي في العصر الرقمي، وهي ظاهرة الإرهاب السيبراني، كما يسلط الضوء على كيفية استجابة النظم القانونية والمؤسساتية في كل من الولايات المتحدة والاتحاد الأوروبي لهذا التهديد المتغير، مما يوفر قاعدة معرفية يمكن الإفادة منها في تصميم سياسات وطنية فاعلة في دول أخرى، لا سيما في العالم العربي.

ثالثًا: هدف البحث

يهدف هذا البحث إلى تحليل السياسات القانونية والتشغيلية التي تتبناها كل من الولايات المتحدة الأمريكية والاتحاد الأوروبي في مكافحة الإرهاب السيبراني من خلال دراسة الأطر التشريعية، والاستراتيجيات الوطنية، والآليات المؤسسية، بهدف استخلاص نماذج فعالة يمكن اعتمادها أو تكييفها في سياقات مختلفة.

رابعًا: فرضية البحث

تنطلق فرضية البحث من أن السياسات التي تعتمد على التوازن بين الإجراءات الأمنية والتشريعات الوقائية، مع دعم القدرات التقنية والاستخباراتية، تعد أكثر فاعلية في مواجهة الإرهاب السيبراني، كما إن التعاون الدولي وتكامل الأدوار المؤسسية يمثلان ركيزتين أساسين في بناء استجابة مستدامة لهذا التهديد العابر للحدود.

خامسًا: منهج البحث

يعتمد البحث على المنهج الوصفي التحليلي في دراسة مفهوم الإرهاب السيبراني وسياسات مكافحته، مع توظيف المنهج المقارن لتحليل الفروقات والتشابهات بين الأنموذجين الأمريكي والأوروبي، واستخلاص الدروس المستفادة.

سادسًا: هيكلية البحث

قُسم هذا البحث على مقدمة وخمسة محاور وخاتمة، تناول المحور الأول، الإطار المفاهيمي لمفهوم الإرهاب السيبراني من خلال تحليل طبيعته وخصائصه، وأبرز التهديدات المرتبطة به، ويليه المحور الثاني الذي يركز على السياسات الأمريكية في مكافحة الإرهاب السيبراني من حيث الأطر الاستراتيجية والتشريعية والتشغيلية، في حين يتناول المحور الثالث الأنموذج الأوروبي في التعامل مع التهديدات السيبرانية الإرهابية عبر أدوات تشريعية ومؤسساتية مشتركة، فضلاً عن الخاتمة والاستنتاجات.

المحور الأول: الإطار المفاهيمي

المطلب الأول: مفهوم الإرهاب السيبراني

يعد الإرهاب من أكثر المفاهيم إثارة للجدل في القانون الدولي والسياسات الجنائية نظرا لتعدد الأبعاد، التي يتقاطع فيها مع الدين والسياسة والأيديولوجيا والقانون، فالإرهاب ليس مجرد ظاهرة عنف بل هو ممارسة مقصودة ذات أهداف رمزية تسعى لإحداث تأثيرات نفسية تتجاوز نطاق الفعل المادي نفسه، ويجمع أغلب الفقهاء على أن الإرهاب يتسم بخصائص مميزة، أبرزها، التهديد المتعمد باستخدام العنف أو القوة ضد المدنيين أو البنى التحتية بهدف التأثير على صانعي القرار السياسي أو تغيير واقع مجتمعي معين، وغالبا ما يكون مدفوعا بدوافع أيديولوجية أو سياسية أو دينية متطرفة، ويتميز الإرهاب أيضا بأنه نشاط غير متماثل تلجأ إليه جماعات غير نظامية لا تمتلك القدرات العسكرية النظامية ما يدفعها إلى تبني تكتيكات غير تقليدية، مثل زرع العبوات الناسفة، أو الهجمات العشوائية على المدنيين[1]، كما يندرج في مفهوم الإرهاب استخدام وسائل غير عنيفة مثل التحريض والتضليل والتجنيد الإيديولوجي، إذا اقترنت بهدف خلق حالة من الخوف المنظم أو تعطيل النظام العام، كما إن هذا البعد الرمزي والنفسي للإرهاب هو ما يميزه عن الجرائم التقليدية، إذ يهدف الفاعل الإرهابي إلى بث الرعب وفرض إرادته على الجماعة أو السلطة وليس

فقط إلى تحقيق منفعة مادية مباشرة، ولهذا فإن فهم الإرهاب يتطلب تحليلاً متعدد المستويات يتناول الفاعل، والوسيلة، والهدف، إلى جانب السياق الثقافي والسياسي الذي نشأت فيه الجماعة الإرهابية أو نفذت عملياتها[2].

رغم الأهمية المتزايدة التي يحظى بها موضوع الإرهاب في العلاقات الدولية والنظم القانونية الوطنية، فإن المجتمع الدولي لم يتمكن حتى الآن من الاتفاق على تعريف قانوني موحد له، الأمر الذي يمثل إشكالية كبيرة في سبيل مكافحته على نحو فعال ومنسق، ويعود ذلك إلى تعقيدات متعددة، أبرزها التباين في وجهات النظر بين الدول الكبرى والدول النامية، واختلاف المواقف السياسية إزاء حركات المقاومة والتحرر، إذ ترى بعض الدول أن استخدام العنف لأغراض التحرر من الاحتلال لا ينبغي تصنيفه ضمن الإرهاب، بينما تعده دول أخرى تهديدا للأمن والاستقرار الدولي، وقد أسهم هذا التباين في إفشال محاولات الأمم المتحدة لتبني "اتفاقية شاملة حول الإرهاب الدولي"، التي عرضت للنقاش منذ تسعينيات القرن الماضي،[3] وبدلاً من ذلك جرى التعامل مع الإرهاب من خلال اتفاقيات قطاعية جزئية، مثل "اتفاقية قمع تمويل الإرهاب"، أو "الاتفاقية الدولية لقمع التفجيرات الإرهابية"، من دون معالجة شاملة للإرهاب كمفهوم موحد، واللافت أن معظم هذه الاتفاقيات تركز على الفعل الجرمي من دون التطرق إلى الأبعاد السياسية أو السياقية، مما يخلق فجوة في المعالجة القانونية، كما إن هذا الغموض في التعريف يسمح بإساءة استخدام قوانين مكافحة الإرهاب لتقييد الحريات الأساسية تحت ذرائع أمنية؛ لذا فإن الحاجة باتت ماسة إلى صياغة تعريف قانوني موضوعي ومتوازن للإرهاب يميز بين العنف غير المشروع وبين الأشكال المشروعة للمقاومة بموجب القانون الدولي الإنساني، ويراعي حقوق الإنسان ومبدأ التناسب في استخدام القوة[4].

لقد شهد الإرهاب في العقود الأخيرة تطورا ملحوظًا في طبيعته وأدواته واستراتيجياته بالتوازي مع التحولات التكنولوجية والاجتماعية العالمية، ففي السابق كان الإرهاب يعتمد بالأساس على العمليات المسلحة المباشرة، مثل التفجيرات أو الاغتيالات، إلا أن المتغيرات العالمية كالعولمة الرقمية، وتفكك النظم التقليدية للحرب، وانتشار وسائل الاتصال الحديثة، ساعدت الجماعات الإرهابية على تطوير نماذج جديدة من الإرهاب ذات طابع غير مادي أو رمزي، إذ لم يعد الإرهاب حكرا على التفجير أو القتل العشوائي؛ بل بات يشمل أدوات متقدمة، مثل الحرب النفسية، والتجنيد

الإلكتروني، والتضليل الإعلامي، والهجمات السيبرانية، كما إن تطور البنية المعلوماتية العالمية سهل على هذه الجماعات الوصول إلى جمهورٍ أوسع، وتخزين معلومات سرية، وتمويل عملياتها عبر قنوات خفية مثل العملات الرقمية5، فضلاً عن ذلك اتجهت بعض الجماعات إلى استهداف البنى التحتية الحيوية مثل المستشفيات، والمصارف، وأنظمة التحكم المروري، في محاولة لإحداث شلل وظيفي للدولة من دون الحاجة إلى احتلال مادي، وهذا التحول النوعي في طبيعة الإرهاب جعل منه أكثر خطرا من ذي قبل؛ لأنه بات يتسلل عبر بيئات لا يمكن حمايتها بالوسائل التقليدية، كما إن تحديد الفاعل الإرهابي صار أكثر صعوبة في ظل استخدام شبكات "الدارك ويب"، والتشفير، والهويات المزيفة، ومن هنا؛ فإن إعادة فهم الإرهاب كظاهرة متعددة الأبعاد والأشكال، تستدعي من الدول إعادة النظر في استراتيجيات المواجهة الأمنية والقانونية بما يتناسب مع التحولات التقنية والاجتماعية المعاصرة[6].

يرتبط ظهور الإرهاب السيبراني بتطور التكنولوجيا الرقمية والاعتماد المتزايد على الشبكات الإلكترونية في إدارة البنى التحتية للدول والمؤسسات، وقد بدأ الاهتمام بهذا النمطٍ من التهديدات في تسعينيات القرن العشرين، بعد أن برزت الجرائم الإلكترونية بوصفها تهديدا جديدا للخصوصية والبيانات، لتتطور لاحقا إلى جرائم أكثر تعقيدا ترتبط بالأمن القومي، إلا أن الربط بين الإرهاب والفضاء السيبراني لم يتحقق فعليا إلا بعد هجمات الحادي عشر من سبتمبر 2001، التي كشفت أن الجماعات الإرهابية لا تعتمد فقط على الوسائل التقليدية بل توظف كذلك الإنترنت في التخطيط والاتصال والتجنيد، ومع التوسع في استخدام الفضاء الرقمي في الحياة العامة والخاصة، ظهرت مخاطر أن تستغل الجماعات المتطرفة هذه البيئة المفتوحة لتنفيذ عمليات تخريبية، سواء بإسقاط مواقع حكومية، أو تعطيل شبكات حيوية، أو إثارة الفوضى المعلوماتية، وقد أثبتت حوادث لاحقة، مثل الهجوم على أنظمة التحكم الصناعية (SCADA) أو اختراق أنظمة نقل الطاقة، أن هذه الجماعات تمتلك قدرات رقمية متطورة ما دفع الدول إلى إدراك أهمية حمايةِ البنى التحتية الرقمية كجزء من أمنها الوطني؛ وبالتالي فإن نشأة الإرهاب السيبراني لا تَعد تحولاً مفاجئاً بل هي نتاج تراكمي لتحولات تكنولوجية وأمنية متداخلة فرضت على صناع القرار إعادة صياغة مفهوم "الجبهة الداخلية"، لتشمل البيئة الإلكترونية كحيز تهديد لا يقل أهمية عن الميدان العسكري التقليدي[7].

أمام تصاعد وتيرة التهديدات الإلكترونية المرتبطة بالجماعات الإرهابية سعت العديد من المنظمات الدولية والإقليمية إلى وضع تعريفات إجرائية لمفهوم الإرهاب السيبراني، رغم عدم وجود تعريف موحد وملزم على المستوى الدولي، فمثلاً تعرف وكالة الأمن القومي الأمريكية (NSA) الإرهاب السيبراني بأنه "التهديد أو الاستخدام المتعمد للأنظمة المعلوماتية ضد أهداف مدنية أو حكومية بهدف إحداث أثر نفسي أو سياسي يخدم أهدافاً إرهابية"، أما الاتحاد الأوروبي فقد اكتفى في وثائقه الاستراتيجية بالإشارة إلى "الاستخدام الإرهابي للفضاء الإلكتروني" من دون تقديم تعريف دقيق وركّز بدلاً من ذلك على تشريعات تتعلق بمكافحة المحتوى الإرهابي على الإنترنت مثل تنظيم إزالة المحتوى المتطرف خلال 24 ساعة[8].

في المقابل قدمت بعض الهيئات الإقليمية تعريفات أكثر وضوحا، كما في اتفاقية منظمة شنغهاي للتعاون، (SCO) التي عدت الإرهاب السيبراني نوعا من "النشاطات التي تهدف إلى تقويض الأمن العام أو الإضرار بالبنية التحتية الحيوية باستخدام أدوات تقنية عبر الإنترنت"، أما الأمم المتحدة وبخاصة من خلال لجنة مكافحة الإرهاب (CTC)، فقد امتنعت عن تعريف مباشر لكنها أشارت في تقارير عديدة إلى "القلق من استخدام الإنترنت كأداة لتجنيد الإرهابيين، والتخطيط للهجمات، والتحريض على العنف"، ويظهر من هذه المقاربات أن أغلب المؤسسات تميل إلى تعريف "عملي وظيفي" للإرهاب السيبراني يركّز على السياق والوسيلة والنتيجة،[9] من دون أن تدخل في الجدل النظري بشأن المفهوم، وذلك لتجنب العقبات السياسية التي تعترض التعريفات الشاملة، ومع ذلك؛ فإن هذا التعدد في التعريفات يبرز الحاجة إلى إطار قانوني دولي يضمن التماسك والفاعلية في مكافحة هذا النوع من الإرهاب، ويراعي في الوقت ذاته الحريات الرقمية، وحقوق الإنسان[10].

المطلب الثاني: خصائص الإرهاب السيبراني

يعد الإرهاب السيبراني ظاهرة حديثة نسبيا في مجال الجريمة المنظمة والإرهاب، إذ يستند إلى الاستخدام المتعمد للتقنيات الرقمية لتنفيذ هجمات تهدف إلى زعزعة استقرار المجتمعات والحكومات وزرع الخوف في نفوس الأفراد، وتنطوي هذه الظاهرة على خصائص تميزها عن أشكال الإرهاب التقليدية، وتعزز قدرة الفاعلين على التخفي والتأثير بعيدا عن الحدود والوضع

الجغرافي مما يحدد إطارا جديدا للتحديات الأمنية والقانونية والتقنية، وفيما يلي أهم الخصائص التي تميز الإرهاب السيبراني[11]:

1. الطابع غير المادي (اللاملموسية)

يعتمد الإرهاب السيبراني على التسلل إلى الشبكات والأنظمة الرقمية من دون مواجهة مادية مباشرة مع الضحية هذه الخاصية تجعل من الصعب على الأفراد والمؤسسات إدراك الهجوم في مراحله الأولى، إذ لا يظهر الدمار بصورته التقليدية، بل يمكن أن يتجلّى في تعطّل الخدمات أو سرقة البيانات أو تشفيرها، ومن ثم، يتيح هذا الطابع لفاعلي الإرهاب السيبراني إحداث تأثيرات مدمرة عبر قنوات غير مرئية، ما يخلق حالة من عدم اليقين والخوف المستمر.

2. تجاوز الحدود الجغرافية

لا تقف الهجمات السيبرانية عند حدود دولة معينة، إذ يمكن للمهاجمين إجراء اعتداءات على بنى تحتية أو مؤسسات في أي منطقة من العالم بغضون ثوانٍ، عبر شبكة الإنترنت، وهذا الأمر يعقّد من مهمة الدول في حماية أمنها القومي، ويفتح الباب أمام تصاعد التوترات الدبلوماسية بشأن مسائل السيادة، إذ قد تعد الهجمة من عمل دولة أخرى أو مجموعات لا تحمل جنسية محددة[12].

3. صعوبة التتبع والإسناد

يستفيد الإرهابيون السيبرانيون من تقنيات تشفير الاتصال مثل VPN وتقنية تور، ومن خوادم وسيطة موزعة في دول مختلفة، مما يزيد من صعوبة تعقّب مصدر الهجوم قد يستخدمون كذلك برمجيات خبيثة قادرة على محو آثارها أو تبديل مساراتها تلقائيا، فتضيع الأدلّة الرقمية في بحار الإنترنت، ويصعب على أجهزة التحقيق الجنائية تحديد الفاعل الحقيقي أو الجهة الداعمة له.

4. التكلفة المنخفضة

لا تتطلب الهجمات السيبرانية موارد بشرية أو لوجستية ضخمة، كما هو الحال في الهجمات التقليدية؛ يكفي مجموعة صغيرة من المخترقين وأدوات برمجية متاحة مجانا أو بتكلفة منخفضة ليشنوا هجمات فعالة، هذه الحقيقة تسهم في توسيع دائرة

الفاعلين المحتملين لتشمل أفرادا أو جماعات ذات قدرات مالية محدودة، ما يجعل من مكافحة الإرهاب السيبراني تحديا مستمرا أمام الأجهزة الأمنية [13].

5. السرعة والانتشار

يمكن لهجمة إلكترونية أن تنتشر بسرعة فائقة عبر الشبكات المرتبطة ببعضها، فتقض على خدمات لا حصر لها في غضون دقائق، كما إن البرمجيات الضارة (مثل الفيروسات والديدان) قادرة على إعادة إنتاج نفسها، وتوزيع نسخ متعددة تلقائيا، مما يضاعف سرعة انتشار الهجمة ويعقّد عملية احتوائها.

6. القابلية للتوسع والتكرار

تتميز الهجمات السيبرانية بالقدرة على استهداف مئات أو آلاف الأنظمة في وقت واحد، من دون الحاجة لتنسيق بشري مباشر لكل هدف، إذ يكفي نشر شفرة خبيثة يمكنها استغلال ثغرة معينة في أنظمة مختلفة لتكرار الهجمة بشكل أوتوماتيكي، ما يزيد من حجم الضرر، ويضعف من فرص الاستجابة السريعة [14].

7. الاعتماد على البنى التحتية الرقمية

ينبع تأثير الإرهاب السيبراني من اختراق البنى التحتية الحيوية، التي تدعم القطاعات الأساسية من الطاقة، والمياه، والصحة، والاتصالات، كما إن تعطّل أي من هذه الخدمات قد يؤدي إلى تعطيل كامل لمنظومة الحياة اليومية في المجتمعات، مما يظهر مدى الارتباط الوثيق بين الأمن السيبراني والأمن القومي.

8. التأثير النفسي والاجتماعي

يهدف الإرهابي السيبراني إلى زرع الخوف والشك بين أفراد المجتمع من خلال تعطيل الخدمات الحيوية أو تسريب بيانات حساسة، وهذا التأثير النفسي قد يكون أقوى من الضرر المادي نفسه، إذ يغدو المواطن في حالة قلق دائم من تعرضه للهجوم أو تسرب معلوماته الشخصية، ما يضعف الثقة في المؤسسات الحكومية والخاصة على حد سواء [15].

9. استخدام التقنيات مزدوجة الاستخدام

يستفيد المهاجمون من أدوات وتقنيات متوفرة رسميا للجهات الحكومية والخاصة، مثل برامج إدارة الشبكات، وأدوات فحص الثغرات، لتحويلها إلى أسلحة إلكترونية، وهذه الطبيعة المزدوجة للاستخدام تعقّد عملية وضع الأطر التنظيمية وتقييد التكنولوجيا، لأن الحظر الشامل قد يضر بالوظائف المشروعة للأنظمة الرقمية[16].

10. الغموض القانوني والإطار التنظيمي

لم تسبق القوانين الجنائية وقوانين مكافحة الإرهاب التطور السريع للتكنولوجيا الرقمية، مما خلق ثغرات قانونية بشأن تعريف "الإرهاب السيبراني" وعقوباته، إذ تتباين تشريعات الدول بشأن هذا الموضوع بناء على أولوياتها الأمنية والسياسية، الأمر الذي يحد من إمكانية التعاون الدولي الفعال في مواجهة هذه الظاهرة.

تجسد خصائص الإرهاب السيبراني تحديات جديدة للمجتمع الدولي تتجاوز بكثير معايير مكافحة الإرهاب التقليدي، سواء من ناحية التتبع، أو الإسناد، أو الاستجابة والتصدي لهذه التحديات، لذا يتوجب على الدول والمؤسسات الأمنية تطوير استراتيجيات شاملة تشمل تحديث الأطر القانونية، وتعزيز التعاون الدولي، وتطوير تقنيات دفاعية قادرة على الكشف المبكر واستباق الهجمات، كما إن رفع وعي الأفراد والمؤسسات بأهمية الأمن السيبراني وإجراءات الحماية الأساسية يشكّل خط الدفاع الأول والأكثر فاعلية في مواجهة هذا النوع من الإرهاب[17].

المطلب الثالث: أنواع التهديدات السيبرانية الارهابية

تعد التهديدات السيبرانية الإرهابية إحدى أبرز التحديات التي تواجه الأمن القومي والمؤسسي في العصر الرقمي، إذ تمتد آثارها من تعطيل الخدمات الحيوية إلى تهديد السلامة الفيزيائية للمواطنين، وتتنوع أساليب هذا النوع من الإرهاب باختلاف أهدافه التقنية والاستراتيجية، فتشمل هجمات تقليدية معروفة، وأخرى متطورة ناشئة تعتمد على تقنيات حديثة، مثل الحوسبة السحابية، والذكاء الاصطناعي، والحوسبة الكمية، ويسعى هذا العرض إلى دمج التصنيفين الرئيسين للتهديدات السيبرانية الإرهابية—التي تشير إلى الطرائق التقليدية والهجينة المعروفة، وتلك "الجديدة" التي برزت مؤخرا وكما يلي[18]:

أولًا: التصنيف التقليدي للتهديدات السيبرانية الإرهابية

1. **هجمات حجب الخدمة الموزعة:** تنطوي على إغراق الخوادم والأنظمة بهدف استنزاف مواردها وتعطيلها عن تقديم الخدمات، وعادة ما يتم ذلك عبر شبكات "بوتنت" تضمُّ أعدادا كبيرة من الأجهزة المخترقة، ويترتّب على هذه الهجمات توقف المواقع الحكومية والبنوك وشبكات الاتصالات، مما يخلق حالة من الذعر، ويلحق أضرارا اقتصادية كبيرة.
2. **البرمجيات الخبيثة:** تشمل الفيروسات، والديدان، والتروجانات، والبرمجيات التجسسية، التي تصمَّم لاستغلال ثغرات البرامج، أو إسقاطها عبر رسائل "التصيد" وتزداد خطورة هذه الأدوات عند تطورها إلى "هجمات متقدمة مستمرة (APT)، إذ يتمكن المهاجم من البقاء مخفيا داخل الشبكة لفترات طويلة قبل تنفيذ الهجوم[19].
3. **الاستهداف المباشر للبنى التحتية الحيوية:** يركز على التحكم في الأنظمة الصناعية، والطاقة، والمياه، والقطاع الصحي عبر اختراق أنظمة الإشراف والتحكم، ويُمكّن هذا النوع من التهديدات الإرهابيين من إلحاق أضرار فيزيائية فعلية، مثل انقطاعَ التيار الكهربائي، أو إلحاق أضرار بمنشآت صناعية حساسة.
4. **هجمات الفدية والابتزاز الإلكتروني:** تعتمد على تشفير بيانات الضحية أو تعطيل أنظمتها ثم المطالبة بفدية مقابل مفتاح فك التشفير، وقد أظهرت تجارب دولية دفع مؤسسات حكومية ومستشفيات مبالغ هائلة لاستعادة بياناتها مع تعريض معلومات حساسة للتسريب إذا ما امتنع الضحية عن الدفع.
5. **التلاعب بالمعلومات والحرب الإعلامية الإلكترونية:** يستهدف بث الأكاذيب أو تزوير المحتوى الصوتي والمرئي عبر الاختراق أو "Deepfake"، بهدف زعزعة ثقة الجمهور في المؤسسات الرسمية أو تأليب الرأي العام على حكومات وأفراد بعينهم، ويعد هذا التكتيك تهديدا مزدوجا؛ لأنه يدمر مصداقية المعلومات، ويعيد تشكيل الواقع السياسي والاجتماعي[20].
6. **هجمات سلسلة التوريد الرقمية:** تنجح عبر اختراق مزودي الخدمات أو المكتبات البرمجية التي تعتمد عليها جهات متعددة، فتنتشر الشيفرات الخبيثة إلى مئات أو آلاف

العملاء دفعة واحدة، ويتطلب التصدي لها تشديد إجراءات التحقق من أمان الطرف الثالث، ومراقبة التحديثات والتوزيعات البرمجية.

7. **استغلال ثغرات إنترنت الأشياء:** تتيح الأجهزة الذكية الضعيفة في الحماية (كاميرات المراقبة، الحساسات المنزلية، أجهزة الإنذار) مدخلاً للمهاجمين إلى الشبكات الداخلية، إذ يمكن استخدام هذه الأجهزة كجزء من "بوتنت" أو للتجسس والتخريب، مثل تعطيل أنظمة إنذار المباني الحيوية.
8. **الهجمات الفيزيائية–السيبرانية:** تجمع بين الاختراق الرقمي والتخريب الفيزيائي كتعطيل مركبات ذاتية القيادة، أو شبكات النقل الذكية، أو استهداف بنى تحتية مع الحواسيب الصناعية، ويستلزم هذا النوع تنسيقاً عالي المستوى بين الخبرات التقنية والهندسية، ويمثّل تهديدا مباشرا على الأرواح والممتلكات[21].

ثانيًا: التهديدات السيبرانية الإرهابية الجديدة والمتطورة

1. **الهجمات المدعومة بالذكاء الاصطناعي:** يستغل المهاجمون تقنيات تعلّم الآلة لاكتشاف الثغرات، وصياغة رسائل تصيد شخصية للغاية، اعتمادا على تحليل سلوك الضحية، أو لتوليد شيفرات خبيثة قادرة على التحايل على أنظمة الكشف التقليدية، وتفرض هذه الهجمات على الدفاعات السيبرانية استخدام أساليب "الذكاء الاصطناعي المضاد"، وتقنيات كشف الهجمات العدائية.
2. **هجمات التزييف العميق:** توظّف تقنيات توليد الفيديو والصوت المزيف لتعزيز قدرات التضليل، والابتزاز، والتشهير، عبر إنتاج تسجيلات تدعي تصريحات زائفة لمسؤولين أو قادة؛ مما يمس بمصداقية المؤسسات، ويثير بلبلة سياسية واجتماعية[22].
3. **استغلال بنى الجيل الخامس:** أتاح التوسع في شبكات الجيل الخامس فتح ساحات هجومية جديدة، إذ ازدادت الأجهزة الطرفية المتصلة بشكل كثيف، وارتفعت معدلات نقل البيانات مع انخفاض الكمون*، مما يجعلها هدفاً جاذبا لاعتراض المعلومات وتحليلها في الزمن الحقيقي، كما أصبحت خاصية (تقطيع الشبكة)* التي تمكّن من تخصيص شرائح مستقلة لخدمات محددة، عرضة للاستغلال لتعطيل وظائف حيوية عبر استهداف شرائح معينة، وهنا في هذا التصارع بين الكثافة العالية والتجزئة المتعددة،

يبرز دور بنية، صفر ثقة (Zero Trust) قائمة على التحقق المستمر من هوية كل كيان وصلاحياته قبل منحه حق الوصول، وبهذه الآلية يمكن تأسيس مستوى أمني مرن وشامل يتوافق مع تعقيدات شبكات الجيل الخامس المتسارعة[23].

4. **البرمجيات الخبيثة القائمة على الذاكرة فقط:** تعمل ضمن ذاكرة النظام من دون ترك أثر على الأقراص الصلبة مما يجعلها صعبة الاكتشاف التقليدي، وينشط هذا النوع في الهجمات المتقدمة المستمرة، ما يحتم استخدام تحليل السلوك في الذاكرة، وتقنيات المراقبة المستمرة.
5. **الهجمات العدائية على نماذج التعلم الآلي:** تستهدف تشويه بيانات التدريب أو استغلالها لإغراء الأنموذج بإخراج نتائج خاطئة، مما يضعف أنظمة كشف التسلل ذات الأساس الذكي، أو أنظمة تحليل الصور في كاميرات المراقبة، ويستلزم مواجهتها تصميم نماذج مقاومة للسموم الهجومية، وآليات تحقق من سلامة البيانات[24].
6. **تهديدات سلسلة التوريد لمنصات الذكاء الاصطناعي:** يختبئ الخطر في تضمين شيفرات خبيثة ضمن مكتبات أو أطر عمل مفتوحة المصدر، يستخدمها مطورو الذكاء الاصطناعي، فتصل تلقائيا إلى المؤسسات عند تحميل النماذج، وتجبر هذه التهديدات على إجراء تدقيق أمني دوري والاعتماد على التواقيع الرقمية، وعزل بيئات التدريب والتشغيل.
7. **التهديدات الكمومية المستقبلية:** مع بلوغ الحوسبة الكمومية مراحل متقدمة، ستعرض خوارزميات التشفير التقليدية للخطر، مما يستدعي الانتقال إلى خوارزميات "تشفير مقاوم للكم"، وإعادة هيكلة بروتوكولات الأمان لضمان سرية البيانات المخزنة والمنقولة.

المحور الثاني: الأنموذج الأمريكي في مكافحة الإرهاب السيبراني

تعتمد الولايات المتحدة الأمريكية في مكافحة الإرهاب السيبراني على منظومة متكاملة تجمع بين أطر قانونية وتشريعات رئاسية، واستراتيجيات وطنية واضحة، وهيئات مؤسسية متخصصة إلى جانب آليات تشغيلية وتقنية متطورة يهدف هذا المحور إلى تقديم عرض علمي لأبرز سياسات الولايات المتحدة الأمريكية في هذا المجال، مبينا كيفية ترابط هذه الجوانب لتحقيق أعلى مستويات الفاعلية في مواجهة التهديدات الإرهابية عبر الفضاء الإلكتروني، ومقسم حسب الآتي[25].

المطلب الأول: الإطار الاستراتيجي الوطني

أصدرت إدارة بايدن–هاريس في 2 مارس 2023 "الاستراتيجية الوطنية للأمن السيبراني" المرتكزة على أربعة أركان متكاملة، تهدف إلى بناء منظومة دفاعية استباقية وقادرة على الابتكار مبنية على أربعة محاور رئيسة[26]:

أولًا: الاستباق والتعاون

يقيم هذا الركن على مبدأ الدفاع الموزّع (Defend Forward)، الذي يمكّن الوكالات الفيدرالية والشركاء الدوليين من رصد وتحليل التهديدات على شبكات الخصوم قبل تفجرها في الفضاء الداخلي، يشمل ذلك:

1. نشر وحدات استخبارات سيبرانية متنقلة تعمل بالتنسيق مع تحالف Five Eyes وحلف الناتو.
2. استخدام منصات مشتركة قائمة على الذكاء الاصطناعي لتحليل حركة المرور والتعرف الآني على أنماط الهجوم.
3. تبادل المستجدات الاستخباراتية والتكتيكات مع القطاع الخاص لتوحيد جهود الرد وتقليل الفجوات الزمنية.

ثانيًا: تعزيز الصمود المؤسسي

يركّز هذا الركن على بناء قدرات المؤسسات لاستكشاف الهجمات والتعافي السريع منها[27]:

1. **المرونة السيبرانية:** قياس جاهزية القطاعات الحيوية عبر مؤشرات محددة مثل متوسط زمن الكشف (MTTD)، ومتوسط زمن الاسترداد (MTTR)، وتنظيم تمارين محاكاة دورية لهجمات على مرافق الطاقة والاتصالات.
2. **ورش العمل والتدريب:** عقد سيناريوهات حوادث رقمية معقدة لاختبار خطط الطوارئ وتحديثها باستمرار بناء على الدروس المستفادة.
3. **مؤشرات الأداء الرئيسة**(KPIs) : تقييم نسب الاكتشاف الداخلي مقابل الاكتشاف الخارجي، وتحليل سرعة الاستجابة لتحديد نقاط القوة والضعف المؤسسية.

ثالثًا: رفع تكلفة الهجوم

يهدف إلى جعل أي محاولة اختراق أكثر كلفة على المهاجم من حصيلتها المتوقعة[28].

1. **مشاركة مؤشرات التهديد:** تبادل مستمر ومؤتمت لـ "Threat Indicators" بين الجهات الحكومية والقطاع الخاص، مما يحد من فاعلية الأدوات الخبيثة.
2. **الدفاع المدعوم بالذكاء الاصطناعي:** تطوير خوارزميات تصفية ذكية تعترض التدفقات المشبوهة وتحللها في الوقت الحقيقي.
3. **عقوبات فورية:** تنسيق مع وزارتي العدل والخزانة لتجميد أصول الجهات الإرهابية فور تحديدها، ورفع تكلفة أي هجوم رقمي عبر إجراءات قانونية رادعة.

رابعًا: تمكين الابتكار والبحث

يكرس هذا الركن الموارد لتطوير خطوط الدفاع المستقبلية[29].

1. **صناديق البحث الموجه:** تخصيص 10 ملايين دولار سنويا لصناديق الأمن الكمومي وشبكات الجيل الخامس، تشرف عليها مختبرات وطنية بالتعاون مع جامعات وشركات ناشئة.
2. **الشراكات الأكاديمية–الصناعية:** برامج "الأمن السيبراني التكاملي" التي تجمع طلبة الدراسات العليا مع خبراء الصناعة لنقل نتائج الأبحاث إلى تطبيقات عملية.
3. **حاضنات الابتكار في CISA:** توفر حاضنات الابتكار التابعة لوكالة CISA مسرعات تقنية متكاملة تدعم الشركات الناشئة في مجالات الذكاء الاصطناعي والمحاكاة الكمومية، مصحوبة بإشراف فني وقانوني متنوع التخصصات.

المطلب الثاني: الأُطر التشريعية والقانونية الأساسية

تشكّل الأُطر التشريعية والقانونية العمود الفقري لاستراتيجية الولايات المتحدة في مكافحة الإرهاب السيبراني، إذ توفر الأساس القانوني لصلاحيات الأجهزة الأمنية وتوازنها مع حماية الحقوق المدنية، ومنذ هجمات الحادي عشر من سبتمبر سخرت واشنطن التشريعات لتعزيز قدرات المراقبة والكشف المبكر، فشهدت العقود الماضية صدور قوانين رئيسة تحدد صلاحيات وتقييدات الأجهزة الاتحادية، وتضمن مشاركة فعالة بين القطاعين العام والخاص في تبادل المعلومات بشأن التهديدات الرقمية ومن هذه القوانين الآتي[30]:

أولًا: قانون USA PATRIOT Act (2001)

جاء هذا القانون استجابةً لحاجة ملحة لتعطيل مخططات الإرهاب قبل وقوعها، فوسع صلاحيات الجهات الأمنية بما في ذلك[31]:

1. إصدار أوامر "الاستماع الخفي" (Pen Register and Trap and Trace) لمتابعة مسارات الاتصالات الرقمية.
2. استخراج سجلات تصفح الإنترنت وبيانات المواقع الجغرافية.
3. تنسيق العمليات الاستخباراتية بين أجهزة وزارة العدل ووكالة الأمن القومي (NSA) لضمان استهداف شبكات دعم الإرهاب.

ثانيًا: قانون تبادل المعلومات السيبرانية (CISA 2015)

صاغه الكونغرس لتمكين تبادل "مؤشرات التهديد" (Threat Indicators) بين الحكومة والشركات التقنية، مع مراعاة حماية الخصوصية[32]:

1. حمايات قانونية (indemnification) تمنع رفع دعاوى ضد الجهة المبلغة ما لم تثبت سوء نية.
2. إنشاء نظام موحد لتلقي وتحليل المعلومات بشأن الثغرات والهجمات في الوقت الحقيقي.
3. تشجيع التعاون الطوعي بين الصناعات الحيوية (الطاقة، المال، الاتصالات) والوكالات الفيدرالية.

ثالثًا: قانون الإبلاغ عن الحوادث للبنى الحيوية (CIRCIA 2022)

يمثل أحدث شروحات التشريع الفيدرالي، إذ يفرض التزامات صارمة على الكيانات المغطاة:

1. إبلاغ CISA خلال 72 ساعة من اكتشاف أي اختراق يؤثر في الخدمات الحيوية.
2. إخطار خلال 24 ساعة عن أي عملية دفع فدية مقابل البيانات المشفرة.
3. بناء قاعدة بيانات مركزية للهجمات الإلكترونية الإرهابية، ما يمكّن الوكالة من تتبع شبكات الاتصال الخفية وردع الجهات الممولة.

تؤكّد هذه القوانين مجتمعة على أهمية وجود هيكل قانوني رصين يكفل فاعلية مكافحة الهجمات الرقمية، مع الحفاظ على المعايير الدستورية للخصوصية وحقوق الأفراد، بما يعزز ثقة المجتمع في قدرة الحكومة على حماية أمنه من دون المساس بحرياته الأساس.

المطلب الثالث: الأوامر التنفيذية لتعزيز أمن سلاسل التوريد البرمجية

في إطار تعزيز أمان البرمجيات الحكومية، وحماية سلسلة التوريد الرقمية من الثغرات والاختراقات، أطلقت إدارة بايدن–هاريس مجموعة من الأوامر التنفيذية، التي تفرض معايير صارمة على دورة حياة تطوير ونشر البرمجيات، تهدف هذه المبادرات إلى تحويل الحكومة الفيدرالية إلى "عميل مبتكر" يرفع سقف الأمان في السوق بأكمله، ويجعل من توزيع المنتجات الرقمية آمنا منذ بدايته وهذه الأوامر هي كالآتي[33]:

أولًا: الأمر التنفيذي 14028 (12 مايو 2021)

بني هذا التوجيه الرئاسي على مفهوم "الأمن حسب التصميم"(Security by Design) ، مؤكّدا أن الأمان ليس إضافة ثانوية بل يمثل جزءا لا يتجزأ من هندسة البرمجيات، وقد اشتمل على:

1. قوائم مكونات البرمجيات(SBOMs): اشتراط تقديم وثيقة تفصيلية توضح المكونات المفتوحة والمملوكة المضمنة في المنتج الرقمي، ما يسهل تتبع الثغرات واستبدالها سريعا عند اكتشافها.
2. إطار عمل تطوير البرمجيات الآمنة: يلزم إطار عمل تطوير البرمجيات الآمنة (SSDF) الصادر عن NIST جهات العقد الفيدرالية باعتماد منهجية شاملة تتضمن تحليل الشيفرة الثابتة، واختبارها ديناميكيا، وإدارة الثغرات الأمنية طوال دورة حياة البرمجيات من مرحلة التصميم والبرمجة إلى الاختبار والإنتاج.
3. آليات الإفصاح عن الثغرات: تدعم هذه الآليات اعتماد البائعين لسياسات إفصاح آمن عن الثغرات الأمنية، وتعزز التعاون مع الباحثين الأمنيين لضمان معالجة نقاط الضعف وتصحيحها قبل أن يتم استغلالها.

ثانيًا: الأمر التنفيذي 14144 (16 يناير 2025)

أصدر الرئيس الأمر التنفيذي 14144 في 16 يناير 2025 كإضافة مكملة لأمر 14028، معنيا بترسيخ جاهزية الحكومة الفيدرالية لمجابهة التحديات الأمنية الناشئة، ويركّز هذا التوجيه على ثلاثة محاور أساس[34]:

1. **تقييم مخاطر الذكاء الاصطناعي وإنترنت الأشياء:** تلزم الوكالات الفيدرالية بإجراء دراسات أثر منهجية (Impact Assessments) لكشف مواطن الضعف في نماذج التعلم الآلي والأجهزة المتصلة، تمهيدا لوضع استراتيجيات تخفيف مناسبة.
2. **التحول إلى تشفير ما بعد الكم:** توجه الجهات الحكومية لاستبدال خوارزميات التشفير التقليدية بأخرى مقاومة للحوسبة الكمومية، وفق معايير "البحث الوطني لأمن المعلومات الكمومية"، لضمان المحافظة على سرية البيانات على المدى الطويل.
3. **توسيع متطلبات SBOM و SSDF:** تضاف إلى قوائم مكونات البرمجيات (SBOM)، وإطار تطوير البرمجيات الآمنة (SSDF)، فئات جديدة تشمل النماذج الذكية، وحاويات الذكاء الاصطناعي، مع اشتراط خضوع هذه المكونات لفحوص أمنية صارمة قبل اعتمادها في عقود الحكومة الفيدرالية.

من خلال هذا، نجحت الإدارة التنفيذية في[35]:

أ. ربط العقود الفيدرالية بمعايير أمان متقدمة تجعل كل مورد رقمي يتحمل مسؤولية صيانته واستقراره الأمني.

ب. تحفيز السوق على تبنّي ممارسات الأمان في منتجاته لتعزيز فرصه في الفوز بعقود حكومية، مما يرفع جودة الأمان السيبراني على مستوى القطاع الخاص.

ج. بناء منظومة مستدامة وقابلة للتطوير تواكب التقنيات الجديدة وتضمن سرعة الاستجابة للتهديدات قبل أن تتحول إلى أزمات أمنية.

4. **بنية الحوكمة والجهات المسؤولة**

تشكل بنية الحوكمة في الولايات المتحدة إطارا متكاملاً لتنفيذ الاستراتيجية الوطنية للأمن السيبراني، إذ تتعاون جهات متعددة على مستويات فنية واستراتيجية

لضمان استجابة مرنة ومتوازنة، ويمكن تلخيص الأدوار والمسؤوليات الرئيسة كما يلي[36]:

أ. **وكالة الأمن السيبراني وأمن البنى التحتية:** تُعدّ المحور المركزي لتنسيق جهود الدفاع وحماية القطاعات الحيوية عبر مركز التنسيق الوطني للأمن السيبراني (NCCIC) تشرف CISA على إطلاق أنموذج نضج الثقة الصفرية (Zero Trust Maturity Model)، الذي يوصي بالتدرج في تطبيق مبادئ عدم الثقة الافتراضية، ويتضمن:

- تعزيز إدارة الهوية والمصادقة المتعددة العوامل (IAM & MFA).
- تطبيق سياسات حد أدنى من الامتيازات (Least Privilege) على الموارد جميعا.
- المراقبة المستمرة للأنشطة الشبكية والكشف الفوري عن السلوكيات الشاذة، كما تقدم الوكالة استشارات تقنية وورش عمل عملية لدوائر الولاية والبلديات، بهدف رفع مستوى الصمود السيبراني في مرافق الطاقة والمياه والاتصالات.

ب. **مكتب التحقيقات الفيدرالي – قسم الجرائم الإلكترونية**

يقود الجانب الجنائي في مكافحة الجرائم السيبرانية الإرهابية ضمن مهمة مشتركة (NCIJTF) تضم أكثر من 30 جهة إنفاذ قانون اتحادية ومحلية، وتشمل مهمات القسم[37]:

- جمع وتحليل الأدلة الرقمية وفق معايير قضائية صارمة.
- تنسيق الملاحقات الجنائية عابرة الحدود عبر التعاون مع شركاء دوليين.
- تبادل المعلومات الاستخباراتية مع CISA لتحويل النتائج الفنية إلى إجراءات قانونية رادعة.

ج. **مجلس مراجعة السلامة السيبرانية**

- أنشئ بمرسوم رئاسي في فبراير 2022 ليكون هيئة مستقلة لمراجعة الحوادث الكبرى—كثغرة—(Log4j)، وتقديم توصيات تقنية واستراتيجية، ويركّز عمل المجلس على:

- تحليل جذور الاختراقات وتقويم نقاط الضعف التصميمية.
- اقتراح تعديلات للأوامر التنفيذية والتشريعات لتعزيز "الأمن حسب التصميم".
- وضع معايير لفرض اختبارات اختراق دورية قبل نشر الأنظمة.
- تتلاقى هذه الجهات ضمن هيكلية حوكمة متعددة الطبقات، تبدأ من مستشاري الأمن السيبراني الرئاسيين، مرورا بلجان الخبراء التقنية، ووصولًا إلى الإدارات التنفيذية، لضمان توافق القرارات مع المتطلبات الفنية والسياسات الوطنية.

5. الآليات التشغيلية ومشاركة المعلومات

تشكل الآليات التشغيلية ومشاركة المعلومات العمود الفقري لاستراتيجية الولايات المتحدة في مكافحة الإرهاب السيبراني، إذ تضمن سرعة الكشف والاستجابة، وتقليص الفجوات بين الاكتشاف والمعالجة، ويمكن تلخيص أبرز هذه الآليات كما يلي[38]:

أ. مراكز مشاركة وتحليل المعلومات

تضم هذه المراكز قطاعات حيوية مثل الطاقة والمالية والاتصالات والصحة، وتعمل على:

- تبادل مؤشرات الاختراق: (Threat Indicators) تلقّي وإرسال بيانات عن البرمجيات الخبيثة وأساليب الهجوم إلى الأعضاء بشكل مستمر.
- تنسيق إجراءات التخفيف: (Mitigation Playbooks) توفير دليل موحد للاستجابة السريعة عند رصد هجوم، مع نصائح تقنية وعملية تناسب كل قطاع.
- ورش العمل والتدريب المشترك: عقد جلسات دورية تجمع خبراء القطاعين العام والخاص لتحليل هجمات سابقة، وتحديث خطط الاستجابة.

ب. منصة US-CERT / NCCIC

تعمل هذه المنصة التابعة لـ CISA على مدار الساعة، وتقدم خدمات رئيسة تشمل[39]:

- إصدار تحذيرات تقنية آنية: نشر تقارير فنية عن ثغرات خطيرة أو هجمات جارية، مع توصيات فورية للحد من الضرر.

- دعم الوكالات المحلية والولائية: تخصيص فرق استجابة ميدانية لمساعدة الحكومات الإقليمية على احتواء الحوادث.
- التنسيق الدولي: مشاركة التنبيهات مع الشركاء الأجانب لضمان ترابط الجهود وتبادل أفضل الممارسات.

ج. تمارينRed/Blue/Purple Team

تجري هذه التمارين بانتظام لمحاكاة بيئات الهجوم والدفاع، وتشمل[40]:

- الفرق الحمراء: (Red Teams) تحاكي تقنيات وسيناريوهات الجماعات الإرهابية الرقمية لاكتشاف الثغرات.
- الفرق الزرقاء: (Blue Teams) تختبر القدرة الدفاعية على صد الهجمات ورَدِها في الزمن الحقيقي.
- الفرق البنفسجية: (Purple Teams) توحد تحليلات الهجوم والدفاع لإنتاج خطط تصحيحية وتحسينات منهجية.

أسهم تطبيق هذه الآليات في خفض زمن الاستجابة للهجمات السيبرانية بنحو 40% في بعض القطاعات الحيوية خلال العامين الماضيين، مما يعكس فاعلية الدمج بين تبادل المعلومات والتدريب العملي والمحاكاة المستمرة.

6. الأُطر المرجعية والتوجيهات التقنية

تشكل الأُطر المرجعية والتوجيهات التقنية الدليل التنفيذي للمؤسسات الحكومية والخاصة لاتباع أفضل الممارسات في إدارة المخاطر السيبرانية، وضمان الابتكار المستدام، ومن أبرز هذه الأُطر[41]:

أ. إطار العمل السيبراني لـ(NIST (CSF

يبني هذا الإطار هيكله على خمس وظائف رئيسة، مع إضافة وظيفة سادسة في الإصدار 20 لتعميق البعد الحوكمي عبر[42]:

- التعرف: تحديد الأصول الحيوية ونقاط الضعف، ووضع خريطة شاملة للمخاطر المحتملة.

- الحماية: تطبيق الضوابط التقنية والتنظيمية لإبقاء تلك الأصول بعيدة عن متناول المهاجمين.
- الكشف: نشر آليات مراقبة مستمرة تهدف إلى اكتشاف الأنشطة المشبوهة فور حدوثها.
- الاستجابة: وضع خطط طوارئ واضحة تتضمن إجراءات إعلامية وتقنية لمعالجة الحوادث بسرعة وكفاءة.
- التعافي: استعادة القدرات التشغيلية بأقل خسائر زمنية ومادية، مع توثيق الدروس المستفادة.
- (الحوكمة) – الإصدار 20: ضيف هذا البعد آليات لإدارة مخاطر سلسلة التوريد، وتحديد الأدوار والمسؤوليات عبر المستويات الإدارية والفنية، مع مقاييس قياس الأداء المتعلقة بالامتثال والتنظيم من خلال مرونته وقابليته للتخصيص، يمكّن CSF المؤسسات من تبني مستويات نضج تتناسب مع حجمها وطبيعة عملياتها، وينشئ لغة مشتركة بين فرق الأمن السيبراني والإدارة العليا.

ب. خطة CISA الاستراتيجية (2025–2023)

تمثل هذه الخطة أول خريطة طريق شاملة لوكالة الأمن السيبراني وأمن البنى التحتية منذ تأسيسها، وتركز على أربعة أهداف متكاملة[43]:

- قيادة الدفاعِ السيبراني الوطني: تعزيز قدرات CISA في التنسيق الفيدرالي والدولي للرد على الهجمات ذات الأثر الكبير.
- خفض المخاطر: تطوير معايير تقييم المخاطر القطاعية، وتطبيق مبادرات لخفض احتمالية استهداف القطاعات الحيوية.
- تعزيز الشراكات التشغيلية: توسيع شبكة التعاون مع القطاع الخاص والباحثين والأوساط الأكاديمية لضمان تدفق مستمر للمعلومات وأفضل الممارسات.
- توحيد عمل الوكالة: "One CISA" دمج جميع وحدات CISA تحت هيكل إداري وتقني موحد يسهل اتخاذ القرارات وتبادل الموارد.

تضفي هذه الخطة الطابع المؤسساتي على جهود الدفاع السيبراني عبر تحديد مؤشرات أداء رئيسة وجداول زمنية للتنفيذ، ما يضمن قابلية القياس والتطوير المستمر، باعتماد هذين الإطارين المرجعيين، تجد المؤسسات نفسها مسلحة بمنهجيات واضحة لابتكار حلول أمنية متقدمة، وإدارة المخاطر بفاعلية، والارتقاء بقدراتها الدفاعية لتواكب الاحتياجات المتجددة في مواجهة الإرهاب السيبراني.

7. الشراكات الدولية وتبادل المعلومات متعدد الأطراف

تلعب الشراكات الدولية متعددة الأطراف دورا حاسما في تكامل جهود الولايات المتحدة لدحر الإرهاب السيبراني، إذ تتيح تبادلاً فعالاً للاستخبارات وتقنيات الدفاع المشترك عبر تحالفات رسمية ومنصات متخصصة، وفيما يلي أبرز هذه الشراكات وآليات التعاون[44]:

أ. تحالف Five Eyes

نشأ هذا التحالف في الخمسينيات، ويضم الولايات المتحدة، والمملكة المتحدة، وكندا، وأستراليا، ونيوزيلندا، وقد تطور ليصبح من أقوى آليات تبادل الاستخبارات السيبرانية، إذ يتشارك الأعضاء منصات تقنية خاصة لتحليل الأحداث العابرة للحدود، ومؤشرات التهديد (Threat Indicators) بشكل فوري، ويعقدون اجتماعات دورية لمواءمة استراتيجيات مكافحة البرمجيات الخبيثة وبرامج التجسس التي تستخدمها جماعات إرهابية ورعاة دولة، ويعد أنموذجا في "الدفاع الموزع" الذي يسمح برد فعل سريع عبر شبكة استخبارات موحدة.

ب. حلف شمال الأطلسي (الناتو)

يدعم حلف شمال الأطلسي (الناتو) "سياسة الدفاع السيبراني الشاملة 2021" عبر إشرافه على مركز Cooperative Cyber Defence Centre of Excellence في تالين بإستونيا، إذ ينفّذ المركز تدريبات مشتركة وأبحاثاً تطبيقية تركز على أربعة محاور أساسية، ومنها، التكنولوجيا، والاستراتيجية، والعمليات، والقانون، كما ينظم تمارين مشتركة تجمع قوات من الدول الأعضاء لمحاكاة هجمات رقمية واسعة النطاق، وتقييم جاهزية الدفاع المشترك، ويعزز الحلف مبدأ تفعيل المادة

الخامسة من المعاهدة في حال تعرض دولة عضو لهجوم سيبراني كبير، ما يكفل تفعيل الدعم الجماعي وتنسيق الاستجابة في مواجهة التهديدات الرقمية[45].

ج. مبادرات الأمم المتحدة والاتحاد الأوروبي

تبرز الولايات المتحدة كطرف فاعل في صياغة مبادرات دولية، تهدف إلى وقف تمويل الإرهاب السيبراني، وملاحقة مصادره، فضلاً عن تنسيق جهود إزالة المحتوى المتطرف من الإنترنت، وعلى مستوى الأمم المتحدة، تدعم واشنطن عمل لجنة مكافحة الإرهاب (CTC) لتعزيز آليات تتبع الأموال الرقمية، ومنع استخدام العملات المشفّرة في تمويل العمليات الإرهابية، أما داخل الاتحاد الأوروبي، فقد أُبرم مؤخرا اتفاق سياسي يلزم منصات التواصل بحذف المواد الإرهابية خلال 24 ساعة من نشرها، مع تبني تشريعات جديدة لمواجهة التضليل الرقمي، وقطع سبل تجنيد التطرف الإلكتروني، ومن خلال هذه الشراكات متعددة الأطراف –التي تجمع بين تبادل المعلومات الاستخباراتية، والتدريب الفني، والتحويات القانونية– تعزز الولايات المتحدة من فاعلية تعطيل الشبكات الإرهابية الرقمية، وترسخ تطبيق معايير أمنية عالمية موحدة للفضاء السيبراني[46].

8. بناء القدرات والبحث والتطوير

يرتكز نجاح أي استراتيجية للأمن السيبراني على توفر طواقم مؤهلة، وأدوات تقنية متقدمة، قادرة على مواكبة تطور التهديدات، ومن هذا المنطلق؛ تبنت الولايات المتحدة أنموذجا متكاملاً يضم ثلاثة محاور رئيسة[47].

أ. التمويل الأكاديمي والصناعي

خصصت الحكومة الأمريكية ميزانيات سنوية بمئات الملايين من الدولارات لدعم الأبحاث في:

- الذكاء الاصطناعي الأمني: تمويل مشاريع جامعية لصقل خوارزميات الكشف عن الهجمات المتقدمة (APT) والبرمجيات الخبيثة القائمة على الذاكرة.
- التشفير بعد الكمّ: (Post-Quantum Cryptography) منح بحثية لتطوير خوارزميات قادرة على الصمود أمام قدرات الحوسبة الكمومية الناشئة.

- برنامج CyberCorps منحة مشتركة بين NSF و NSA لتدريب خريجين مخصصين للعمل في وكالات فيدرالية مثل CISA و FBI وUSCYBERCOM، مع التزام بالعمل الحكومي مدة لا تقل عن ثلاث سنوات.

ب. الأكاديمية الوطنية للأمن السيبراني (NCAE)

تشرف على الأكاديمية كلٌّ من NSA و CISA و FBI وNIST/NICE بالتنسيق معUSCYBERCOM ، وتركز على[48]:

- مناهج معتمدة تشمل إدارة الحوادث والتحليل الجنائي الرقمي، وأمن البنى التحتية.
- مختبرات محاكاة متطورة تتيح للمتدرب تجربة سيناريوهات حقيقية مثل هجمات على شبكات الطاقة وأنظمة SCADA*.
- شهادات تخصصية معترف بها في القطاعين العام والخاص، ما يعزز توظيف الخريجين في مناصب متقدمة.

د. مبادرات تدريبية مشتركة

انطلقت هذه المبادرات بدعم CISA و Secret Service وعدد من الهيئات الصناعية، وتركز على[49].

- ورش عمل للإدارة العليا: تدريب أعضاء مجالس إدارة المؤسسات الحيوية على آليات الرقابة والإشراف على السياسات الأمنية.
- حلقات تنسيق تقنية تجمع خبراء من القطاعين الحكومي والخاص لتحليل الهجمات وتبادل الخطط التصحيحية.
- برامج تبادل خبرات دولية مع حلفاء مثل Five Eyes تنظم دوريات وفترات تدريب خارجية لتعزيز تبني أفضل الممارسات.

من خلال هذه المحاور المترابطة، تؤسس الولايات المتحدة لقاعدة بشرية وتقنية صلبة تضمن استدامة الابتكار وتعزيز جاهزية المؤسسات في مواجهة التحديات المستقبلية للإرهاب السيبراني.

المحور الثالث: أنموذج الاتحاد الأوروبي في مكافحة الإرهاب السيبراني

في ظل التنامي المستمر لتوظيف الجماعات الإرهابية للفضاء السيبراني، باتت دول الاتحاد الأوروبي تدرك أن مكافحة الإرهاب الرقمي لم تعد تقتصر على إجراءات انفرادية للدول الأعضاء، بل تتطلّب أنموذجا متكاملاً يشمل تشريعات موحدة، وهيئات تنفيذية متخصصة، وتنسيقاً تشغيليا وتقنيا عابرا للحدود، ويهدف هذا المحور إلى استعراض الدعائم التشريعية والمؤسسية والاستراتيجية، التي بني عليها إطار سياسات الاتحاد الأوروبي في مواجهة الإرهاب السيبراني، مع التركيز على إبراز آليات العمل وتوزيع المسؤوليات، التي سنبينها كالآتي:

أولًا: الإطار التشريعي والتنظيمي

يستند الاتحاد الأوروبي في تكوين منظومته القانونية إلى دمج أهداف الأمن والخصوصية، وتهيئة بيئة قانونية قادرة على ردع ومعاقبة الفاعلين السيبرانيين الإرهابيين، وذلك من خلال[50]:

1. توجيه أمن الشبكات ونظم المعلومات

أُقر هذا التوجيه عام 2016 كأول نص قانوني أوروبي يلزم مزودي الخدمات الأساسية (الطاقة، النقل، الصحة...) والمنصات الرقمية الكبرى باتخاذ إجراءات أمنية إلزامية، والتبليغ عن الحوادث الكبرى خلال 24 ساعة وميز التوجيه فرضية "مدرج المخاطر" التي تحدد متطلبات أمنية متفاوتة بناء على حساسية القطاع.

2. توجيه NIS 2 (2022)

جاء لتوسيع نطاق NIS الأصلي وإدراج قطاعات أوسع (كالأسواق المالية والفضاء الإلكتروني)، مع رفع سقف العقوبات إلى 2٪ من حجم إيرادات الشركة العالمية في حال التقصير في تبليغ الحوادث أو تطبيق معايير الحماية.

3. اللائحة العامة لحماية البيانات

رغم تركيزها على الخصوصية، فإن GDPR تفرض إخطار الجهات الرقابية والمستخدمين بتسريبات البيانات خلال 72 ساعة من الاكتشاف، الأمر الذي يسهل تنسيق الاستجابة في حال تورط حادث إرهابي سيبراني في تسريب معلومات حساسة.

4. توجيه مكافحة الإرهاب

عرف الإرهاب السيبراني ضمن نصه بوصفه استخدام الفضاء الرقمي للتخطيط أو تنفيذ أعمال تهدف إلى إضعاف الأمن العام أو التأثير في بنية الدولة، وأدرج بنودا لمعاقبة التحريض والتجنيد عبر الإنترنت، ونشر الدعاية المتطرفة.

5. التشريعات الجديدة (DSA) و (DORA) وتتضمن[51]:

أ. قانون الخدمات الرقمية (DSA 2022): يفرض على المنصات الكبرى إزالة المحتوى الإرهابي خلال ساعات من التبليغ، ويعزز إجراءات الشفافية في خوارزميات التوصية.

ب. قانون الصمود التشغيلي الرقمي: (DORA 2023) يفرض معايير استمرارية الأعمال والأمن في بيئات الخدمات المالية التي قد يستهدفها الإرهاب السيبراني لتعطيل الاقتصاد.

ثانيًا: الهيئات والمؤسسات المركزية

تنفيذ هذه التشريعات يتطلب بنية مؤسسية تضمن التطبيق المتسق بين الدول الأعضاء، وتقدم الدعم الفني والقضائي عند الاقتضاء، أبرزها[52]:

1. وكالة الاتحاد للأمن السيبراني

تعمل على وضع المعايير الفنية لأمن الفضاء السيبراني، وتطوير إطار العمل الأوروبي للأمن السيبراني، فضلاً عن تقديم المساعدة التقنية للدول الأعضاء في التدقيق والتقييم محلّيا.

2. المركز الأوروبي لمكافحة الجريمة السيبرانية

ينسق التحقيقات متعددة الجنسيات بشأن الجرائم الإرهابية الرقمية، ويدير وحدات متخصصة في تحليل الأدلة الرقمية واسترجاع البيانات من شبكات التشفير.

3. فريق الاستجابة لحوادث أمن الحاسوب الخاص بالاتحاد الأوروبي (CERT-EU)

فريق الاستجابة لطوارئ الحواسيب التابع للمؤسسات الأوروبية (المفوضية والبرلمان والمجلس) يعمل بالتنسيق المستمر مع فرق الاستجابة الوطنية (CERTs) لتبادل التحذيرات الفورية ونماذج الشفرات الخبيثة، مما يعزز القدرة الجماعية على مواجهة الهجمات السيبرانية بسرعة وفاعلية.

4. المفوضية الأوروبية–شؤون الداخلية والعدل

تشرف على تنسيق السياسات بين دوائر المفوضية والدول الأعضاء، وتضع لوائح تطبيقية وتنظيمية، وتقدم الدعم التشريعي لتعديل التوجيهات متى استجد خطر جديد.

5. وكالة الاتحاد الاوربي للتعاون في مجال العدالة الجنائية (Euro just)

يدعم التعاون القضائي عبر تنسيق طلبات التسليم والملاحقات الجنائية للأشخاص المتهمين بتنفيذ جرائم إرهابية رقمية، ويسهل التبادل القانوني واللوجستي بين الدول.

ثالثًا: الاستراتيجية الأوروبية للأمن السيبراني

لإضفاء طابع استراتيجي طويل الأمد على الجهود، أطلقت المفوضية الأوروبية استراتيجية أمن سيبراني لعام 2020 ثم حدثتها عام 2023، ترتكز على ثلاثة محاور[53]:

1. **تعزيز صمود البنى التحتية**
   - أ. نشر بنية "الاستخبارات السيبرانية المشتركة" التي تسهم في رصد التهديدات المتطورة عبر تحليل جماعي للتجزئة العميقة (Deep Packet Inspection) والذكاء الاصطناعي.
   - ب. تشجيع اعتماد مبادئ "صفر ثقة" (Zero Trust) ضمن الشبكات الحكومية والبنى التحتية الحيوية.
2. **التعاون والتنسيق العملياتي**
   - أ. إنشاء "الفرقة الأوروبية الموحدة للتصدي للحوادث السيبرانية" (J–CU) للعمل كخلية تنسيق في الأزمات الكبرى، تجمع عناصر من ENISA و Europolو–CERT EU والدول الأعضاء.
   - ب. عقد تمارين مشتركة سنوية لمحاكاة هجمات متزامنة على قطاعات متعددة، وزيادة جاهزية أجهزة الاستجابة والدفاع.
3. **تعزيز السيادة الرقمية والابتكار**
   - أ. تدعم برامج Horizon Europe وDigital Europe Program مشروعات بحثية متقدمة تستهدف ابتكار خوارزميات تشفير قادرة على الصمود أمام قدرات الحوسبة الكمومية، وتطوير أدوات لتحليل الهجمات المعتمدة على الذكاء الاصطناعي العدائي.

ب. تأسيس "مركز التميز لأمن الذكاء الاصطناعي الأوروبي" لتعزيز التعاون الأكاديمي–الصناعي وتوحيد منهجيات تقييم المخاطر في تقنيات المستقبل.

يتضح من استعراض الدعائم التشريعية والتنظيمية، والبنى المؤسسية، والاستراتيجية العامة للأمن السيبراني في الاتحاد الأوروبي، أن الأنموذج الأوروبي يعتمد على التوازن بين الحوكمة القانونية والتنسيق الفعال بين الدول الأعضاء والمؤسسات التقنية، يضمن هذا الإطار استجابة سريعة ومنسقة أمام الإرهاب السيبراني مع استعداد مستمر لمواجهة التحديات التقنية المستقبلية.

الخاتمة

في ختام هذا البحث يتضح أن الإرهاب السيبراني لم يعد تهديدا افتراضيا محدودا بل أصبح واقعا معقدا يفرض تحديات استراتيجية وتشريعية على الدول والمنظمات الدولية على حد سواء، إذ تتطلب طبيعته اللامركزية وسرعته وتعقيد تقنياته تطوير استجابات متعددة الأبعاد تتجاوز النماذج التقليدية للأمن القومي، وقد أظهرت الدراسة من خلال تحليل الأنموذجين الأمريكي والأوروبي أن فاعلية مكافحة هذا النوع من الإرهاب ترتبط بوجود منظومة قانونية مرنة، ومؤسسات أمنية متخصصة، وآليات تنسيق دولي فعالة، إلى جانب احترام حقوق الإنسان والحريات الرقمية، وعلى الرغم من التباين في المقاربات بين الأنموذجين، إلا أن هناك توافقا متزايدا على ضرورة تعزيز التعاون العابر للحدود، وتوحيد المعايير التقنية والقانونية كمدخل رئيس لتحقيق أمن سيبراني عالمي مستدام، وهو ما يستدعي من الدول النامية، ومنها الدول العربية أن تستلهم هذه النماذج، وتعمل على تكييفها ضمن بيئاتها القانونية والسياسية المحلية لمواجهة هذا التهديد المتصاعد بكفاءة واستباقية.

المصادر والهوامش

(1) محمد، منتصر أحمد، "الإرهاب كجريمة دولية في إطار القانون الدولي العام"، مجلة مصر المعاصرة، العدد (487)، السنة (2015)، ص165–168.

(2) محمد حميد عبد، "الاتفاقيات الدولية القطاعية لمكافحة الإرهاب: جدل التعريف وأزمة التكييف القانوني"، مجلة دراسات قانونية، جامعة الكوفة، العدد (30)، السنة (2022)، ص77–84.

(3) ناصر مهنا، "الإرهاب: إشكالية التعريف في القانون الدولي"، مجلة دراسات قانونية وسياسية، جامعة الجزائر 1، العدد (19)، السنة (2013)، ص45–50.

(4) محمد حميد عبد، مصدر سبق ذكره، ص86.

(5) عبد الله طارق الشامي، "تحولات الإرهاب المعاصر في البيئة الرقمية: من العمليات المسلحة إلى الهجمات السيبرانية"، مجلة الدراسات الأمنية، جامعة نايف العربية للعلوم الأمنية، العدد (66)، السنة (2023)، ص91–99.

(6) وائل فؤاد عبد الجليل، "الهجمات السيبرانية على البنى التحتية الحيوية: التحديات والاستجابات"، مجلة الأمن والحياة، وزارة الداخلية العراقية، العدد (48)، السنة (2021)، ص115–123.

(7) قاسم حسين الزبيدي، "الإرهاب السيبراني وتحديات الأمن الوطني: مقاربة في المفهوم والتهديدات"، مجلة الدراسات الدولية، جامعة بغداد، العدد (73)، السنة (2020)، ص113–118.

(8) عبد الله طارق الشامي، مصدر سبق ذكره، ص103.

(9) مروة سعد الدليمي، "الإرهاب السيبراني في المنظمات الدولية: جدلية التعريف والتقنين"، مجلة القانون والسياسة، جامعة كركوك، العدد (32)، السنة (2021)، ص201–208.

(10) المصدر نفسه، ص209.

(11) Conway, Maura. “Cyberterrorism: Academic Perspectives,” in The Routledge Handbook of International Crime and Justice Studies, Routledge, 2013, pp. 218–234.

(12) سارة عبد القادر الزيدي، "الفضاء السيبراني والسيادة الرقمية: إشكاليات الاختراق وحدود الرد القانوني"، مجلة العلوم القانونية، جامعة بغداد، العدد (80)، السنة (2022)، ص131–136.

(13) المصدر نفسه، ص137.

(14) مروة سعد الدليمي، مصدر سبق ذكره، ص211.

(15) قاسم حسين الزبيدي، مصدر سبق ذكره، ص119.

(16) عبد الله سمير عطية، "الجريمة السيبرانية والإرهاب الرقمي: دراسة تحليلية قانونية"، دار النهضة العربية، القاهرة، 2021، ص154–161.

(17) كامل حميد الجبوري، "التكنولوجيا مزدوجة الاستخدام وتداعياتها الأمنية: الإرهاب السيبراني أنموذجًا"، مجلة آفاق استراتيجية، المركز العراقي للدراسات، العدد (11)، السنة (2020)، ص79–83.

(18) Kott, Alexander, and Linkov, Igor. “Cyber Resilience: The Next Frontier in Threat Categorization.” IEEE Security & Privacy, Vol. 17، No. 4، 2019، pp. 12–21.

(19) محمود خليل الشمري، "الحوسبة الكمّية والذكاء الاصطناعي في خدمة الإرهاب الرقمي: منظور مستقبلي"، مجلة الرأي الاستراتيجي، المركز العربي للبحوث، العدد (18)، السنة (2023)، ص77–81.

(20) رغد فاضل العبيدي، "الذكاء الاصطناعي والتزييف العميق: تحديات أمن المعلومات والوعي المجتمعي"، مجلة الفكر القانوني المعاصر، جامعة تكريت، العدد (12)، السنة (2023)، ص143–148.

(21) علاء الدين فخري عبد الكريم، "سلسلة التوريد الرقمية كمدخل للهجمات السيبرانية: التهديدات وسبل المواجهة"، مجلة الدراسات الأمنية، جامعة نايف، العدد (51)، السنة (2022)، ص92–100.

(22) رغد فاضل العبيدي، مصدر سبق ذكره، ص150.

* يشير مفهوم **انخفاض الكمون** (Low Latency) إلى قصر الزمن الفاصل بين إرسال البيانات من المرسل ووصولها إلى المستقبل، ويقاس عادةً بالملّي ثانية (ms).

* يشيرُ مصطلح **تقطيع الشبكة** (Network Slicing) إلى تقنيةٍ تتيحُ إنشاء عدة شبكات افتراضية مستقلة فوق البنية التحتية الفيزيائية نفسها، إذ تُخصص كلُّ "شريحة" (Slice) لمجموعة من الخدمات أو التطبيقات ذات متطلبات معيّنة (مثل الكمون المنخفض، عرض النطاق العالي، أو مستويات الأمان المرتفعة)، وتقوم هذه التقنية بالاعتماد على مبادئ **الشبكات المعرفة برمجيًا** (SDN) **ووظائف الشبكة الافتراضية** (NFV) لتجريد الموارد—كالطيف الترددي ومعالجات الحوسبة والتخزين—وتوزيعها ديناميكيًا على الشرائح المختلفة.

(23) سامي عبد العزيز الجبوري، "أمن شبكات الجيل الخامس: التحديات والحلول"، دار الإبداع الرقمي، بيروت، 2022، ص85–91.

(24) سعدون شاكر العزاوي، "البرمجيات الخبيثة القائمة على الذاكرة في الهجمات المستمرة المتقدمة: دراسة تحليلية"، مجلة الأمن الرقمي، جامعة المستنصرية، العدد (7)، السنة (2022)، ص61–68.

(25) أحمد عبد العزيز الغنام، "السياسات الأمريكية للأمن السيبراني: قراءة في الأطر القانونية والمؤسسية"، دار الروافد الثقافية، بيروت، 2021، ص57–65.

(26) سعد محمود الفرج، "المنظومة الأمريكية لمكافحة الإرهاب السيبراني: الأبعاد القانونية والمؤسساتية"، مجلة السياسة الدولية، مركز الأهرام، العدد (222)، السنة (2023)، ص99–106.

(27) ليلى عارف العبد، "الاستراتيجية السيبرانية الوطنية للولايات المتحدة: تحليل مضمون وتقييم أداء"، مجلة الرأي العام الرقمي، العدد (10)، السنة (2022)، ص41–46.

(28) إيهاب خالد العمري، "الردع السيبراني في السياسة الأمريكية: أدوات جديدة لمواجهة التهديدات الرقمية"، مجلة الدراسات الاستراتيجية، جامعة النهرين، العدد (65)، السنة (2022)، ص117–124.

(29) صفاء محمود الزيدي، "مشاركة مؤشرات التهديد وتوظيف الذكاء الاصطناعي في الدفاع السيبراني الأمريكي"، مجلة الأمن الرقمي، المركز العربي للأبحاث، العدد (8)، السنة (2023)، ص52–57.

(30) يوسف عادل الموصلي، "التشريعات الأمريكية في الفضاء السيبراني بعد 11 سبتمبر: الأمن مقابل الحريات"، دار الساقي الأكاديمية، بيروت، 2022، ص73–81.

(31) المصدر نفسه، ص82.

(32) رندة عبد الباقي الرفاعي، "البنية القانونية لمكافحة الإرهاب الإلكتروني في السياسة الأمريكية: قراءة في قوانين ما بعد 2001"، مجلة القانون والسياسة، جامعة كركوك، العدد (36)، السنة (2023)، ص89–96.

(33) حسام فاضل النعيمي، "من قانون الوطنية إلى CLOUD Act: تطور الإطار القانوني لمكافحة الإرهاب الرقمي في أمريكا"، مجلة القانون الرقمي، العدد (10)، السنة (2022)، ص61–66.

(34) The White House, "Executive Order 14144 – Strengthening Federal Cybersecurity Readiness," Washington D.C.، 16 January 2025. Available at: www.whitehouse.gov.

(35) هيثم نبيل الدليمي، "قراءة تحليلية في الأمر التنفيذي 14144: التحول السيبراني في إدارة الأمن القومي الأمريكي"، مجلة الأمن القومي الرقمي، العدد (7)، السنة (2025)، ص33–38.

(36) محمود عبد الفتاح علي، "حوكمة الأمن السيبراني في الولايات المتحدة: الهيكل، التنسيق، والتحديات"، دار النهضة العربية، القاهرة، 2021، ص133–140.

(37) إيمان عبد الرزاق الحيدري، "البنية المؤسسية للأمن السيبراني في الولايات المتحدة: توازن بين الفاعلية والمساءلة"، مجلة الإدارة العامة، جامعة الملك سعود، العدد (88)، السنة (2022)، ص59–66.

(38) أحمد يوسف علوان، "الآليات التشغيلية الأمريكية في مكافحة الإرهاب السيبراني: دراسة في التكامل بين الاستخبارات والتقنية"، مجلة العلوم السياسية، جامعة بغداد، العدد (70)، السنة (2023)، ص97–104.

(39) المصدر نفسه، ص105.

(40) غسان عبد المنعم داود، "الاستجابة للهجمات السيبرانية: النماذج الأمريكية في المحاكاة والتمارين القتالية"، دار الأفق الرقمي، بغداد، 2022، ص77–84.

(41) ليلى عبد الهادي طاهر، "فرق المحاكاة الحمراء والزرقاء في التدريب الأمني السيبراني: بين النظرية والتطبيق"، مجلة العلوم الأمنية، جامعة نايف، العدد (49)، السنة (2023)، ص113–120.

(42) هيثم يوسف الراوي، "الفرق البنفسجية في الأمن السيبراني: أداة لدمج الرصد الهجومي والدفاعي في بيئة واحدة"، مجلة الأمن الرقمي، العدد (9)، السنة (2023)، ص33–37.

(43) CISA (Cybersecurity and Infrastructure Security Agency), "CISA Strategic Plan 2023–2025،" U.S. Department of Homeland Security, September 2022، https://www.cisa.gov/sites/default/files/2022-09/cisa-strategic-plan_2023-2025_508.pdf

(44) وزارة الأمن الداخلي الأمريكية، "التعاون الدولي في الأمن السيبراني: الاستراتيجية والمشاركة الأمريكية"، مكتب الأمن السيبراني والبنية التحتية والمخاطر، تموز 2023، ص1–18، متاح على: https://www.dhs.gov/sites/default/files/2023-07/dhs-international-cybersecurity-cooperation-strategy-2023.pdf

(45) إيهاب خليفة، "الميدان الخامس: الفضاء السيبراني في العقيدة العسكرية لحلف الناتو"، المركز العربي للأبحاث ودراسة السياسات، 9 فبراير 2020، متاح على: https://www.dohainstitute.org/ar/PoliticalStudies/Pages/The-Fifth-Domain.aspx

(46) خالد وليد محمود، "الفضاء السيبراني وتحولات القوة في العلاقات الدولية"، المركز العربي للأبحاث ودراسة السياسات، الدوحة، الطبعة الأولى، 2025، ص101–110.

(47) المصدر نفسه، ص111.

(48) CAE Community ،*NCAE-C Program Book* ،CAE-C Program Management Office ، 2025

* تشير أنظمة **SCADA** (Supervisory Control and Data Acquisition) إلى فئة من أنظمة التحكم والإشراف الصناعي المصمَّمة لمراقبة وإدارة العمليات التشغيلية في البنى التحتية الحيوية مثل شبكات الكهرباء ومحطات توليد الطاقة، محطات معالجة المياه، خطوط الأنابيب، والمصانع الكبيرة. وتقوم هذه الأنظمة بجمع البيانات الحية من الموقع (الضغط، التدفق، درجة الحرارة، مستوى الخزان...) عبر وحدات الاستطلاع البعيدة (RTUs) أو متحكمات المنطق القابلة للبرمجة (PLCs)، ثم تنقلها إلى مركز مراقبة مركزي.

(49) إيهاب خليفة، مصدر سبق ذكره.

(50) المفوضية الأوروبية، "الاستراتيجية الأوروبية للأمن السيبراني لعصر الرقمية (Cybersecurity Strategy for the Digital Decade)"، الاتحاد الأوروبي، ديسمبر 2020، متاح على: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

(51) البرلمان الأوروبي والمجلس الأوروبي، "قانون الصمود التشغيلي الرقمي للقطاع المالي (Digital Operational Resilience Act – DORA)"، اللائحة رقم2022/2554 (EU) ، اعتمدت في 14 ديسمبر 2022، نُشرت في الجريدة الرسمية، وتدخل حيز التنفيذ في 17 يناير 2025، متاح على: https://eur-lex.europa.eu/eli/reg/2022/2554/oj

(52) أندريا كالديرارو وباتريك باولاك، "الأمن السيبراني في الاتحاد الأوروبي: المرونة والقدرة على التكيّف في السياسات والحَوْكمة"، سلسلة روتليدج في سياسات المعلومات، دار روتليدج للنشر، لندن، الطبعة الأولى، 2020، ص75.

(53) الاتحاد الأوروبي والمفوضية الأوروبية، الاستراتيجية الأوروبية للأمن السيبراني لعصر الرقمية 2020 (Cybersecurity Strategy for the Digital Decade)، ديسمبر 2020، متاحة على: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy