السنة: العاشرة المجلد: 10 العدد: 02 ص ص: 359- 387
EISSN 2676-1645 ISSN 2543-375X

أطر عمل الاتحاد الأوروبي للحد من تهديدات الإرهاب السيبراني

The Eu Frameworks to Reduce Cyber Terrorism Threats

محمد بودرمين*، جامعة الإخوة منتوري قسنطينة1
مخبر العقود وقانون الأعمال
mohammed.boudermine@doc.umc.edu.dz

منال بوكورو، جامعة الإخوة منتوري قسنطينة1
مخبر الدستور الجزائري والدراسات القانونية الاستشرافية
Manel.boukourou@umc.edu.dz

تاريخ الاستلام: 2025/01/19 تاريخ القبول: 2025/03/18

ملخص:

تناقش هذه الدراسة التهديد المحتمل الذي يشكله الإرهاب السيبراني على أمن الاتحاد الأوروبي ومستقبله، كما تناقش وجهة نظر الأخير تجاه هذا التهديد. وتهدف إلى تحليل الأطر والسياسات التي اعتمدها الاتحاد بشكل متدرج كآليات للتعامل مع هذا الخطر الناشئ، لنصل إلى فهم كيف عزز الاتحاد الأوروبي الأمن السيبراني لدوله الأعضاء، ووفر حماية فعالة للبناء التحتية الحيوية من الهجمات السيبرانية، رغم التحديات التي واجهها. يعتمد البحث على منهجين المنهج الوصفي ومنهج تحليل المضمون. بهدف رصد مفهوم الإرهاب السيبراني في السياق الأوروبي، واستكشاف أشكال تهديداته المتعددة، إلى جانب تحليل الوثائق والسياسات المتعلقة بمكافحته وتقييم مدى فعاليتها لتخلص الدراسة إلى جملة من النتائج، أبرزها أن الاتحاد الأوروبي قد استجاب للتصاعد المستمر في التهديدات السيبرانية ذات الطابع الإرهابي من خلال إعمال مجموعة آليات على مستويات متعددة وبأبعاد مختلفة.

* المؤلف المراسل

الكلمات المفتاحية: الإرهاب السيبراني، التهديدات السيبرانية، الاتحاد الأوروبي، الاستجابة الأطر.

Abstract:

This study examines the potential threat posed by cyberterrorism to the security and future of the European Union, as well as the Union's perspective on this threat. It aims to analyse the frameworks and policies that the EU has progressively adopted as mechanisms to address this emerging risk, seeking to understand how the Union has enhanced cybersecurity for its Member States and established effective protection for critical infrastructure against cyberattacks, despite the challenges encountered.

The research relies on two methodologies: the descriptive approach and content analysis. Its objective is to examine the concept of cyberterrorism within the European context, explore its various forms of threats, analyze relevant documents and policies on combating it, and assess their effectiveness. The study concludes with a set of findings, most notably that the European Union has responded to the continuous escalation of cyber threats of a terrorist nature by activating a range of mechanisms within a comprehensive strategic vision that operates on multiple levels and across different dimensions.

Keywords: Cyber terrorism; Cyber threats; European Union; Response; Frameworks.

□

مقدمة:

تعد تقنية المعلومات والاتصالات من أهم ما توصل إليه العقل البشري في العصر الحالي؛ وتعتبر أنظمة الحاسوب أساسية في إدارة عديد الوظائف الحيوية. أحد هذه العناصر هو تشغيل البنى التحتية الأساسية، مثل محطات الطاقة، المياه، والصحة، والأنظمة المصرفية، وإدارة الأجهزة الحكومية.. الخ.

ومع الزيادة الهائلة في استخدام هذه التقنيات، برزت عديد التحديات الناجمة عن إساءة استخدامها؛ تمثلت في تهديدات أمنية ذات طابع سيبراني أخذت من هذه البنى التحتية أهدافا للقائمين بها.

وعلى غرار دول العالم، يعاني الاتحاد الأوروبي عديد التهديدات السيبرانية التي تؤثر على أمنه واستقراره؛ خاصة الصادرة عن المجموعات التي توصف أنها إرهابية، والتي تهدف إلى إلحاق الضرر بمؤسساته والمجتمع على حد سواء. وفي محاولة منه لمكافحة هذه التهديدات التهديدات عمد الاتحاد الأوروبي إلى وضع عديد الاستراتيجيات والسياسات في شكل قوانين وآليات مؤسسية كأطر عمل لتوحيد مساعيه في مواجهة هذا الخطر وجعل الإنترنت في منأى عن الاستخدام الإرهابي.

تتمثل أهمية الدراسة في تسليط الضوء على التحديات الأمنية الناجمة عن الهجمات السيبرانية الإرهابية الناشئة، التي أصبحت تشكل خطرا على البنى التحتية الحيوية للاتحاد الأوروبي؛ ومن ثم التعرف على رؤية الأخير تجاه هذه التهديدات، وكيفيات تعامله معها، من خلال الآليات التي استحدثها.

وتهدف الدراسة إلى استكشاف الجهود التي بذلها الاتحاد الأوروبي باعتباره نموذجا رائدا في مجال الأمن السيبراني، في سبيل مكافحة الإرهاب السيبراني والحد من تهديداته؛ من خلال تناول الآليات التي اعتمدها، وتقييم فاعليتها بناء على النتائج المحققة.

من أجل ذلك، جاءت هذه الدراسة لتناقش الإشكالية التالية: إلى أي مدى استجابت آليات عمل الاتحاد الأوروبي المعتمدة لتطلعاته في مكافحة الإرهاب السيبراني والتهديدات المترتبة عنه؟

يندرج تحت هذه الإشكالية أسئلة فرعية تتمثل في:

- كيف يعرف الاتحاد الأوروبي الإرهاب السيبراني ويصنفه من بين الجرائم الأخرى؟ وما تصوره لخطورة هذا التهديد؟

- كيف ساهمت التهديدات المتزايدة للإرهاب السيبراني في وضع أطر استباقية؟ وهل ساهم تطوير هذه الأطر في بلوغ تطلعات الاتحاد الأوروبي للحد من هذه التهديدات في ظل التحديات القائمة؟

لغرض الوصول إلى الهدف من الدراسة والإجابة على الإشكالية والتساؤلات الفرعية تم اعتماد منهجين: المنهج الوصفي، من أجل عرض مفهوم الإرهاب السيبراني ومختلف التهديدات المرتبطة به والناجمة عنه واستعراض الأطر المعتمدة؛ ومنهج تحليل المضمون، بهدف تحليل الوثائق الصادرة عن الاتحاد الأوروبي، وتقييم مدى فعاليتها كآليات في مواجهة التهديدات السيبرانية الإرهابية.

المحور الأول: التهديدات الإرهابية السيبرانية للاتحاد الأوروبي

يعتبر الإرهاب السيبراني والتهديدات المترتبة عن أنشطته وعملياته في منطقة الاتحاد الأوروبي من الخطورة بمكان؛ ويمكن إرجاع ذلك إلى المزايا التي تمنحها التقنية الحديثة لهذا النوع من التهديد، وكذا طبيعة تكوين الاتحاد نفسه. وسنحاول في هذا المحور التعرف على الإرهاب السيبراني والتهديدات التي يشكلها وفق تصور الاتحاد الأوروبي؛ من خلال تناول مدلوله والحالات الواقعة.

1. مدلول الإرهاب السيبراني في الاتحاد الأوروبي

يناقش هذا العنصر مضمون الإرهاب السيبراني عبر مستويين: الأول يتعلق بالمفهوم العام لهذه الظاهرة وسماتها الفريدة، والثاني يركز على التعريف الإجرائي الذي تبنته مؤسسات الاتحاد الأوروبي عند تناولها له كتهديد.

1.1 مفهوم الإرهاب السيبراني

نتناول تعريف الإرهاب السيبراني، من خلال مجموعة من التعريفات الفقهية الواردة في شأنه بشكل تدرجي؛ كما نميزه عن باقي التهديدات المشابهة.

في عام 1998، أورد باري كولن (باحث في معهد الاستخبارات والأمن في كاليفورنيا) لأول مرة مصطلح "الإرهاب السيبراني"، ورأى أنه نتاج تقارب بين العالم الافتراضي والعالم المادي وشرح العالم الافتراضي أنه مجال عمل برامج الحاسوب، حيث تخزن وتستخدم البيانات؛ في حين أن العالم المادي هو واقع

الحياة والعمل (Collin, 1996). وفي نفس العام، أضاف مارك بوليت (خبير مكتب التحقيقات الفيدرالي) إلى هذا المفهوم، واعتبر أن الإرهاب السيبراني هجوم متعمد ذو دوافع سياسية، ينصب على أنظمة الكمبيوتر، ويتضمن أنشطة عنيفة تشنها حكومات أو مجموعات منظمة سرية على أهداف حكومية (Pollitt, 1998, p. 03).

انطلاقا من هذا الوصف، ظهرت مفاهيم أخرى مرتبطة بهذا المصطلح كالفضاء السيبراني، والجريمة السيبرانية، والحرب والهجمات السيبرانية.. الخ

وفي شهادتها أمام اللجنة الخاصة بمراقبة الإرهاب بمجلس النواب الأمريكي سنة 2000، قدمت دوروثي دونينغ تعريفا أكثر إحاطة بمضمون الإرهاب السيبراني؛ حيث بينت أنه:"..تقارب الإرهاب والفضاء الإلكتروني.."، ورأت بإمكانية اعتبار الهجمات على البنى التحتية بمثابة إرهاب عبر الإنترنت، وتحديدا الهجمات ذات الدوافع السياسية التي تلحق أضرارا جسيمة بالأنظمة المالية، أو تلويث المياه، أو انقطاع الكهرباء..الخ ومن بين الخصائص التي تبنتها لتحديد مصطلح الإرهاب السيبراني، أنها أعمال أو تهديدات غير قانونية موجهة ضد أنظمة معلومات الكمبيوتر أو شبكاته؛ والغرض من هذه الهجمات هو إحداث ضغوط اجتماعية تؤدي أو تساهم في أعمال عنف ضد الأشخاص أو الممتلكات، ما عبرت عنه "بالأضرار الجسيمة التي تنحصر في البنى التحتية" (Denning, 23 May 2000)

وبهذا المعنى، فإن الإرهاب السيبراني يعد هجوما متعمدا يتم بواسطة الشبكة أو عن طريقها؛ من أجل إحداث تدمير أو تعطيل لأنظمة معلومات البنى التحتية للدول، خاصة الحيوية منها، قصد تقويض المجتمع وتحقيق أهداف سياسية معينة.

ولسبب طبيعته المميزة، بما يتضمنه من خصائص، وتعدد الفاعلين، وتنوع أهدافه؛ من المهم الإشارة إلى أن: بعض الهجمات سيبرانية لا يرجع مصدرها إلى الإرهاب السيبراني (Crime, 1994, p. 04) إنما إلى مجرمو الإنترنت الذين يهدفون إلى الحصول على مكاسب مالية مثل القراصنة، أو من أجل إحداث التخريب والفوضى دعما لإنجاح أنشطتهم الإجرامية العابرة للحدود التي تقوم بها عصابات

الجريمة المنظمة. كذلك، هناك الهجمات ذات الطابع الجيوسياسي الصادرة من الدول ضد البنى التحتية لدول مناوئة لها (أنظر العنصر 1.2).

في حين يهدف الإرهابيون السيبرانيون من خلال عملياتهم السيبرانية إلى تحقيق غايات سياسية تتجاوز التهديدات والاحتياجات المعروفة للقراصنة والمجموعات الإجرامية؛ إلى الدعاية والعنف على نطاق واسع، ما يثير الخوف والفوضى والتمرد السياسي (Conway, 2003, p. 06).

وعليه، فإن التهديدات الجيوسياسية وتلك المنفذة من الجماعات الإجرامية والقراصنة، وإن كانت جديرة بالاهتمام أيضا، إلا أن الإرهاب السيبراني يمثل التهديد الرئيسي باعتباره خطرا ناشئا يهدد الأمن والاستقرار الوطني والإقليمي والعالمي؛ ما يجعله مصدر خطر. ومن ثم، عمدت الدول إلى سن مجموعات واسعة من القوانين تستهدف بشكل خاص تهديد الإرهاب السيبراني، وإن كان القليل منها من وضع إطارا محددا يقوض استخدام الأخير لتكنولوجيا المعلومات؛ من بينهم الاتحاد الأوروبي محل الدراسة.

2.1 تعريف الاتحاد الأوروبي للإرهاب السيبراني

أول ما تم استخدام مصطلح "الإرهاب السيبراني" في الاتحاد الأوروبي كان عام 2001، بموجب خطة عمل مجلس الاتحاد الأوروبي من أجل تعزيز التعاون بين اليابان والاتحاد (Christopher Baker-Beall, 2021, p. 1092). ورد ذكره باعتباره شكلا من أشكال الجريمة السيبرانية، وواحد من مجموع التهديدات الأمنية المحتملة المرتبطة بالجريمة العابرة للحدود الوطنية الأمر الذي تطلب إجراء تعاون ثنائي من أجل مكافحتها، بين إدارة شرطة اليابان واليوروبول.

كما أورد أول تقرير عن حالة الإرهاب واتجاهاته في الاتحاد الأوروبي لعام 2002، الصادر عن المجلس الأوروبي واليوروبول (Union C. o., 2002, p. 12) ذكر الإرهاب السيبراني، واعتبره نوعا من التهديدات الأمنية إلى جانب إرهاب اليمين المتطرف، وإرهاب اليسار الفوضوي، والإرهاب الجهادي، والإرهاب الانفصالي..الخ. وبقي يرد في التقارير اللاحقة، آخرها عام 2023، باعتباره شكلا محتملا من التهديدات.

وكجزء من خطة عمل الاتحاد لعام 2006، تم الإشارة إلى الإرهاب السيبراني في تقرير لجنة مكافحة الإرهاب الذي أوصى بالتركيز على إيجاد تعاون دولي، مبني على ثلاث أسس هي: الحد من التطرف والتجنيد، مكافحة تمويل الإرهاب، ومواجهة الإرهاب السيبراني (Coordinator, 2006, p. 04).

اعتبر عام 2010 منطلقا للاتحاد الأوروبي في وضع تعريف للإرهاب السيبراني؛ حيث أثار هجوم "ستاكسنت" حفيظة الاتحاد وخوفه من الضعف المرتبط بالأنظمة المعلوماتية للبنى التحتية الحيوية في حال وقوع هجوم مماثل. حيث جاء في ورقة المناقشة التي أعدها منسق الاتحاد لمكافحة الإرهاب (CTC) في نوفمبر 2010 "..إن حادث ستاكسنت أظهر مرة أخرى أن البنى التحتية الحيوية يمكن أن تكون عرضة للهجمات.. في جانبها الخاص بالمعلومات والاتصالات. وعلى الرغم من أن الإرهاب السيبراني لا يعتبر التهديد الرئيسي للاتحاد، يتعين اعتبار أن الهجمات السيبرانية أعمالا جاذبة للجماعات الإرهابية، على غرار المنظمات الإجرامية وغيرها من الجماعات المعادية. لذلك، من الأهمية بمكان تدارك التهديد المستقبلي قبل اكتساب الجماعات الإرهابية المعرفة وقدرات الهجوم على البنى التحتية" (Union C. o., EU Counter- Terrorism Strategy - Discussion Paper, 2010, p. 06)

في جويلية 2011، طرح فريق العمل التابع للاتحاد الأوروبي المعني بالإرهاب (WPT) مبادرة لجمع المعلومات حول التهديدات المتزايدة الناجمة عن الهجمات السيبرانية، وخاصة الإرهابية منها. وقد أبرز الفريق بشكل خاص الحاجة إلى بناء مفهوم واضح للإرهاب السيبراني، مع اقتراح قائمة بأهم المصطلحات التي قد تسهم في تحديث التشريعات (Terrorism, 2011, p. 02) وأوضح الفريق أن الاتحاد بحاجة ليس فقط إلى تعريف دقيق لهذه الظاهرة، بل أيضا إلى تطوير فهم مشترك لطبيعة التهديد.

في نوفمبر 2011، عرض فريق العمل (WPT) نتائج مبادرة قدمتها مجموعته الفنية، تضمنت قائمة بالمصطلحات المرتبطة بالعمليات السيبرانية مثل: الفضاء السيبراني، وحادث أمن المعلومات، والأمن السيبراني.. وغيرها وعرف الإرهاب السيبراني بأنه "جريمة إرهابية.."، مستندا في ذلك إلى المادة الأولى من القرار

الإطاري الصادر عن المجلس الأوروبي بشأن الفضاء السيبراني (رقم JHA 475/2002 لعام 2002)، والتي حددت ثمانية أفعال تشكل جرائم إرهابية. وتعتبر الفقرة الرابعة (د) منها الأقرب إلى عمليات الإرهاب السيبراني، حيث نصت على: ".. التسبب في تدمير واسع النطاق لمرفق حكومي عام، أو نظام نقل، أو مرفق من مرافق البنى التحتية بما في ذلك نظام المعلومات. مما قد يعرض حياة الأفراد للخطر أو يؤدي إلى خسائر اقتصادية جسيمة (Council of The Europeran Union, 2002).

على الرغم من الارتباط الأكثر للأعمال الواردة في الفقرة الرابعة (د) بالإرهاب السيبراني عن غيرها، يمكن اعتبار باقي الجرائم المذكورة في المادة إرهابا سيبرانيا إذا نفذت بوسائل رقمية. وأشار فريق العمل (WPT) خلال مراجعته لقائمة المصطلحات إلى أن تعريف الإرهاب السيبراني غير محدد بوضوح في تشريعات الدول الأعضاء، وأن مفهوم "الهجمة السيبرانية" يغطي غالبية الحالات التي تصنف كإرهاب سيبراني (Christopher Baker-Beall, p. 1093).

بناء على ذلك، يتبين أن الاتحاد الأوروبي لم يقدم تعريفا واضحا للإرهاب السيبراني، واكتفى باستخدام مصطلحات عامة مثل: الجريمة السيبرانية (IOCTA)، والهجمات، والتهديدات، دون تخصيص الإرهاب السيبراني الذي حدده الاتحاد وفق اعتبارين رئيسيين:

الأول: استخدام الإنترنت لأغراض إرهابية، مثل نشر المحتوى المتطرف.

الثاني: تعطيل البنى التحتية الرقمية لإحداث ضرر واسع النطاق.

وعليه فإن الإرهاب السيبراني بهذا المفهوم يحتل درجة أقل أهمية في خطاب الاتحاد الأوروبي، نظرا لعدم تسجيل أي هجمات فعلية تستهدف البنى التحتية الحيوية ذات أغراض سياسية حتى اليوم (Weimann, 2004, p. 09), ومع ذلك، يتعامل معه بجدية كونه سيناريو محتمل قد يحدث في أي لحظة، مما يجعله موضوعا بارزا في السياسات الأمنية الأوروبية.

2. التهديدات الناشئة عن الإرهاب السيبراني الماسة بأمن الاتحاد الأوروبي

نتطرق في هذا العنصر إلى بعض العمليات والأنشطة السيبرانية كحالات مست دولا أعضاء في الاتحاد الأوروبي وأخرى ضمن أمنه الإقليمي، تمثلت في هجمات

وتهديدات ذات طابع إرهابي. نبهت الاتحاد إلى خطورتها وشكلت نقطة فارقة في تحول السياسة الأمنية الأوروبية نحو الأمن السيبراني.

1.2 حالات للهجمات السيبرانية في الاتحاد الأوروبي وأوروبا

تنامت التهديدات والهجمات السيبرانية بشكل كبير في الاتحاد الأوروبي وبعض دول أمنه الإقليمي، وذلك عبر حوادث متكررة طالت دوله، ساهمت في إيقاظ وعي الأخير بالمخاطر التي تكتنف أنظمة معلومات بناه التحتية فعلى سبيل المثال: إحدى أولى الحوادث السيبرانية التي مست دول الاتحاد كانت هجوم إستونيا في أبريل 2007، حيث شنت أربع هجمات سيبرانية من نوع "حجب الخدمة" (DDoS)، استهدفت المؤسسات الحكومية الإستونية وبواسطتها، تم تعطيل خوادم البريد الإلكتروني للبرلمان ووسائل الإعلام والبنوك.

في حين أن هذه الهجمات - التي مست البنى التحتية - لم ترتب أضرارا كبيرة بالقدر الذي شكلت إنذارا للاتحاد، لإدراك حجم الخطر، (Malthe Munkøe, 2022, p. 74) بقابلية تعرض أنظمة معلومات بناه التحتية لمثل هذه الهجمات، ليس فقط من طرف الحكومات، وإنما أيضا من طرف الجماعات الإرهابية.

ومن جانب آخر، شهدت دول تتطلع للانضمام إلى الاتحاد الأوروبي هجمات مماثلة؛ ففي عام 2015، كانت أوكرانيا ضحية لهجمات سيبرانية أرجع مصدرها إلى قراصنة مدعومين من روسيا. استهدفت هذه الهجمات مواقع حكومية، منها البرلمان ووزارتا الدفاع والخارجية، كما طالت نظام شبكة الكهرباء، وألحقت أضرارا بقطاع الطاقة؛ حيث تسببت في انقطاع التيار الكهربائي، ما أثر على الأنشطة الحيوية للبلاد. وبعدها بعامين، تم نشر برنامج "Not Petya" الذي عطل المؤسسات الأوكرانية الرئيسة، مثل الوزارات الحكومية والبنوك والشركات (Madnick, 2022).

شكلت هذه الهجمات الصدمة الكبيرة الثانية لأوروبا - وإن لم تكن الوحيدة التي استهدفت دولا تتطلع للانضمام إلى الاتحاد - إذ شهدت حالات أخرى مماثلة، مثل الهجمات على جورجيا عام 2008، ما خلق جوا من الضعف والشك بين الأعضاء وعلاقاتهم السياسية مع العالم.

وعلى غرار ما شهدته إستونيا وأوكرانيا، تعاني دول أعضاء في الاتحاد الأوروبي - مثل رومانيا وهولندا وفنلندا وألمانيا - من هجمات "حجب الخدمة" على مؤسساتها بشكل متكرر. ومن الأمثلة على ذلك: الهجوم السيبراني على البنك الفنلندي رأس سنة 2014، وهجوم عام 2016 على بنك "HSBC" في لندن، واللذان أديا إلى منع العملاء من إجراء المعاملات المصرفية (Katarina Kertysova, 2018, p. 23).

هذه الحالات وإن كانت هذه ذات طبيعة جيوسياسية في الغالب إلا أنه يمكن اعتبارها نموذجا لإمكانية استهداف دول الاتحاد بهجمات إرهابية أكثر تأثيرا خاصة مع تطور نشاط المنظمات الإرهابية العالمية وتوجهها نحو التقنيات السيبرانية.

2.2 تهديد الإرهاب السيبراني للاتحاد الأوروبي

أظهرت سجلات عن تحضيرات كانت تجرى من قبل جماعات إرهابية وأفراد في محاولة لتنفيذ هجمات سيبرانية ضد دول غربية، منها الاتحاد الأوروبي. ففي عام 2011، دعا تنظيم القاعدة - عبر بث شريط فيديو - إلى شن هجمات سيبرانية ضد أهداف غربية، ما جعل الاتحاد الأوروبي يستشعر خطر تحول اهتمام المنظمات الإرهابية نحو الجانب السيبراني. وفي عام 2014، حث تنظيم الدولة أتباعه والمتعاطفين معه على تقديم توجيهات للطامحين في الإعداد لعمليات ضد الدول الغربية، بما في ذلك الهجمات السيبرانية. كما وجدت أدلة على التخطيط لهجمات إرهابية عبر وسائل التواصل الاجتماعي، وتطبيقات المراسلة المشفرة، والويب المظلم (Jayakumar, 2021, p. 873).

وعلى المستوى الفردي، تعتبر قضية جنيد حسين - المواطن البريطاني الذي أسس فريق "Poison Team" ونفذ سلسلة هجمات اختراق سيبراني ضد حلف الشمال الأطلسي ووزارة الدفاع البريطانية - مثالا واضحا على هذا التهديد. فبعد سجنه عام 2012 وإطلاق سراحه، رجع إلى سوريا، وتطور نشاطه من مجرد "مؤثر" رئيسي لتنظيم داعش على منصة "إكس" (تويتر سابقا)، ليصبح عضوا رئيسيا في فريق العمليات السيبرانية التابع للتنظيم وهو الفريق الذي نفذ عدة محاولات هجومية ضد الحكومات الغربية (Jayakumar, p. 874).

كما أشارت تقارير عن سعي المنظمات الإرهابية - والأفراد والمجموعات المتعاطفة معها - للحصول على تقنيات تمكنهم من تنفيذ هجمات ذات تأثير مدمر. ورغم عدم تحقيقهم هذا الهدف بعد، إلا أن استمرار أنشطتهم الحالية تستدعي التعامل معها بجدية (Issah, 2021, p. 48) .

يلاحظ أن تعرض الاتحاد الأوروبي المتكرر للهجمات السيبرانية، إلى جانب التهديدات المرتبطة بها، كشف عن نقاط ضعف في بنيته الأمنية. ولا يرجع هذا الضعف إلى تنامي الجريمة السيبرانية فحسب، بل أيضا إلى تزايد الفرص التي يوفرها القراصنة ومجرمو الإنترنت لهذه المنظمات؛ الأمر الذي شكل حالة من التشتت لدى أجهزة إنفاذ القانون في دول الاتحاد، في التمييز بين الأفعال الإجرامية العادية والهجمات السيبرانية ذات الطابع الإرهابي. وهو ما مثل تحديا إضافيا ونقطة ضعف في المنظومة الأمنية السيبرانية للاتحاد الأوروبي (Sheelagh Brady, 2020, p. 123) .

ورغم أن الهجمات السيبرانية في تلك الفترة لم تحدث أضرارا جسيمة بالبنى التحتية الحيوية - نظرا للاستعدادات الأمنية التي تتمتع بها حكومات الاتحاد الأوروبي، وضعف الإمكانات التقنية المستخدمة - إلا أنها مثلت مصدر قلق جدي للاتحاد ومستقبل أمنه السيبراني.

3. رؤية الاتحاد الأوروبي لتهديدات الإرهاب السيبراني

برز مصطلح "الإرهاب السيبراني" لأول مرة في الخطاب الرسمي للاتحاد الأوروبي عام 2001، في أعقاب أحداث 11 سبتمبر، من خلال سلسلة الوثائق الصادرة عن المجلس الأوروبي والمفوضية الأوروبية، إلى جانب تقارير برلمانية ومداولات تشريعية متنوعة. وتكشف هذه المصادر عن تباين في التصورات المفاهيمية للإرهاب السيبراني؛ فبينما ذهبت معظم الوثائق الرسمية إلى اعتباره جريمة خطيرة ترتكبها جماعات إرهابية غير حكومية تستهدف الأنظمة المعلوماتية، أبدى بعض أعضاء البرلمان الأوروبي رأيا مغايرا مفاده أن الدول قد تكون طرفا فاعلا في هذا النوع من الإرهاب (Christopher Baker-Beall, p. 1091).

وعلى الرغم من بروز مفهوم الإرهاب السيبراني في الخطاب المؤسسي للاتحاد الأوروبي، ووصفه كتهديد أمني متصاعد، فإن تحديد ماهيته القانونية بقي

يعاني من غموض مفاهيمي. إذ افتقرت جميع الوثائق الأمنية الصادرة عن مؤسسات الاتحاد إلى تعريف واضح ودقيق يتوافق مع الإطار الشامل لمكافحة الإرهاب.

يتمحور التصور الأوروبي لتهديد الإرهاب السيبراني حول إمكانية استهداف البنى التحتية الحيوية - التي تتسم بالضعف في ظل اعتمادها المتزايد على التقنية السيبرانية – خاصة وأن تقارير اللجنة الأوروبية تؤكد تزايد الترابط في المجالات الاقتصادية والاجتماعية. .(Christopher Baker-Beall, p. 1096)

ومن هذا المنظور بنى الاتحاد الأوروبي تصوره لتهديد الإرهاب السيبراني حيث اعتبر احتمال الهجمات السيبرانية الإرهابية مبررا كافيا لحث الدول الأعضاء على تعزيز آليات الحماية الوقائية تحسبا لهجمات محتملة.

وتجلى هذا التوجه بوضوح في " تقرير حالة الإرهاب " لعام 2022 الصادر عن الاتحاد الأوروبي، والذي أشار إلى أن جائحة كوفيد-19 قد زادت من مخاطر تنفيذ هجمات ضد أنظمة المعلومات الحيوية في دول الاتحاد من جماعات إرهابية. (Commission, Communication From the Commission on the EU Security Union Strategy, 2020). الأمر الذي دفع المفوضية الأوروبية إلى التأكيد على ضرورة منع الاستخدام الإجرامي للأدوات الرقمية في وثائق سياسية لاحقة، مثل "استراتيجية العقد الرقمي 2020" و"أجندة مكافحة الإرهاب".

في تحول لافت، جاءت وثيقة المجلس الأوروبي الصادرة عام 2011 بعنوان "ملخص المبادرة بشأن مكافحة الهجمات السيبرانية الإرهابية" لتقلل من شأن التهديد، معتبرة أن هذه الهجمات لا تشكل خطرا جسيما على المدى القريب، وأن الغرض من المبادرة يقتصر على تقييم مستوى استعداد الدول الأعضاء. كما عكست الوثيقة رؤية المجلس التي تنظر إلى الإرهاب السيبراني بوصفه "جريمة إلكترونية" في المقام الأول .(Christopher Baker-Beall, p. 1095) مما يؤشر على استمرار الغموض المفاهيمي في التعامل مع هذه الظاهرة.

وعليه، يتبين من خلال وثائق الاتحاد الأوروبي المذكورة أن الأخير يعطي تفسيرات مختلفة للإرهاب السيبراني؛ أهمها: أنه يمثل جريمة إرهابية خطيرة صادرة عن جماعات مختلفة، بما فيها الجهات المدعومة من الدول وأن التهديد

الناجم عنه، وإن كان محتملا فإنه في تزايد مستمر وذو تأثير منهجي، ينصب بشكل أساسي على البنى التحتية الحيوية.

إن تهديد الإرهاب السيبراني - وإن كان صعب التحديد بدقة، واقتصار خطره على الهجمات الصادرة من جهات مدعومة من دول (مثل حالة إستونيا وأوكرانيا) - فإنه يبرز حاجة ملحة لتعزيز الأمن السيبراني؛ ليس للتخفيف من الهجمات الإرهابية فحسب، بل أيضا للتصدي للهجمات غير الإرهابية كما أن تحسين الاستجابة الأوروبية المشتركة تبقى ضرورية لاحتواء هذه التهديدات أو تجاوزها.

المحور الثاني: استجابة الاتحاد الأوروبي لتهديدات الإرهاب السيبراني

استجابة للتهديدات السيبرانية ذات المصدر الإرهابي وغيرها من العمليات ذات الصلة، اتجه الاتحاد الأوروبي نحو بناء أمنه السيبراني الداخلي وتعزيزه، عن طريق التعاون المشترك بين دوله الأعضاء. ثم وسع نطاق هذا التعاون تدريجيا ليشمل أطرافا ثالثة، ليأخذ في نهاية المطاف بعدين: داخلي بين الدول الأعضاء، وخارجي مع الشركاء الدوليين.

1. تبلور عمل الاتحاد لمكافحة الإرهاب السيبراني

بسبب تزايد المحاولات لمهاجمة أنظمة الحاسوب والمعلومات، والوعي بحقيقة أن خدمات الاتصال وتداول المعلومات بين المستخدمين قد تنشئ تهديدات جديدة ذات طبيعة خطيرة، والخوف من تحول هذه التهديدات من طابعها الإجرامي إلى هجمات إرهاب سيبراني؛ توصل الاتحاد الأوروبي إلى استنتاجٍ مفاده أن الحماية القانونية التي توفرها الآليات التقليدية غير كافية ويرجع ذلك إلى أن الظواهر الإجرامية السيبرانية لم تكن مدرجة ضمن القواعد الجنائية القائمة، التي كانت مقيدة بمبدأ سيادة الدول، مع شيئ من التداخل في الولاية القضائية.

وعليه، تم إبرام اتفاقية بودابست عام 2001 (Europe, 2001)، كإطار قانوني ملزم للتعامل مع التهديدات السيبرانية العابرة للحدود، بعد أربع سنوات من التعاون بين مجلس أوروبا ودول غير أعضاء مثل الولايات المتحدة وكندا واليابان. حددت الاتفاقية نقاطا رئيسية للتعاون، هدفت من خلالها إلى توفير آليات كافية للحد من هذه الجرائم أو على الأقل منع تطورها، ومواءمة القوانين الوطنية، لكنها واجهت تحديات تمثلت في تباين التشريعات الوطنية للدول الأعضاء. الأمر

الذي استدعى وضع حد أدنى ملزم من التشريعات يحظى بالإجماع، كمعيار لتنظيم هذا المجال، ومواءمة القوانين الداخلية بشكل تدريجي. كما أضيف إليها "بروتوكول إضافي" عام 2003، يهدف إلى تجريم الأفعال العنصرية المعادية للأجانب عبر استخدام الوسائل الالكترونية (Sheelagh Brady, p. 60).

وضعت الاتفاقية أهدافا محورية لتعزيز التعاون متعدد الأبعاد في مواجهة التهديدات السيبرانية، وشملت تصنيفا واسعا للجرائم الإلكترونية. ورغم ذلك لم تتناول صراحة الإرهاب السيبراني كمفهوم مستقل، وإن كانت قد أشارت إلى الهجمات السيبرانية باعتبارها عنصرا مرتبطا بالتهديدات الإرهابية.

2. استجابة الاتحاد الأوروبي لتهديدات الإرهاب السيبراني على المستوى الداخلي

من أجل جعل المنطقة الأوروبية في منأى عن العمليات الإرهابية السيبرانية، وتزامنا مع تزايد الهجمات السيبرانية، استجاب الاتحاد الأوروبي لهذه التهديدات بإحداث تعاون داخلي متناسق بين دوله، مدعوم بمنظومة متنوعة من السياسات والاستراتيجيات المتعاقبة؛ لتعزيز صمود أعضائه ومواجهة التحديات المستجدة.

1.2 استراتيجية الاتحاد الأوروبي للأمن السيبراني لسنة 2013

أعلن عن هذه الاستراتيجية بعد سنوات من الهجمات السيبرانية التي استهدفت إستونيا وليتوانيا ودولا أخرى تطمح للانضمام إلى الاتحاد. ركزت الوثيقة على الحاجة الملحة لتطوير إطار قانوني وسياسي شامل لتعزيز الأمن السيبراني، حيث تضمنت خمسة أهداف رئيسية، منها: تعزيز التعاون بين الدول الأعضاء، وإنشاء فرق الاستجابة للطوارئ السيبرانية (CERTs) وتبني معايير أمنية موحدة لحماية البنية التحتية الرقمية الحيوية. كما عززت الاستراتيجية التنسيق مع اليوروبول عبر مركز مكافحة الجرائم السيبرانية (EC3)، مما ساهم في تحسين القدرات الأوروبية لتتبع الأنشطة الإجرامية والإرهابية عبر الفضاء السيبراني (European Parliament t. C., 2013).

مع ذلك، تخلل الاستراتيجية عدة تحديات، أهمها أنها لم تكن ذات طابع ملزم، ما أدى إلى إختلاف وتفاوت في تنفيذها بين الدول الأعضاء. كما افتقرت إلى آليات إنفاذ صارمة وحلول كافية لمواجهة التهديدات الخارجية وأغفلت قضايا حاسمة مثل التطرف والتجنيد السيبراني. إضافة إلى ذلك شكل غياب فرق

الاستجابة للطوارئ الحاسوبية في أحد عشر دولة عضوا تحديا آخر أثر على فعالية الاستراتيجية إقليميا ووطنيا (Mortera-Martinez, 2018, p. 05)

ورغم هذه التحديات، تعتبر الاستراتيجية بمثابة حجر الأساس لسياسات الأمن السيبراني في الاتحاد الأوروبي، حيث استمدت وسارت على نهجها عديد السياسات والأطر اللاحقة.

2.2 إطار سياسة الدفاع السيبراني 2014

جاء هذا الإطار كردة فعل على القصور الذي شاب الاستراتيجيات الوطنية للأمن السيبراني للدول الأعضاء، من حيث التباين بينها، وصعوبات تنفيذ استراتيجية 2013. حيث هدفت السياسة إلى تعزيز التعاون بين وكالات الدفاع الوطنية عبر تطوير برامج تدريبية وأبحاث في مجال الأمن السيبراني وتحسين التنسيق بين الدول الأعضاء والمؤسسات الأمنية مثل اليوروبول والوكالة الأوروبية للأمن السيبراني (ENISA). كما عززت تبادل المعلومات بين الجهات الفاعلة في الأمن والدفاع، مما رفع قدرة الاتحاد على التصدي للتهديدات السيبرانية، بما فيها الهجمات الإرهابية (Issah, p. 55).

ولأسباب تتعلق بالحاجة إلى مواجهة التهديدات المتصاعدة، تم تحديث الإطار عام 2018، ليضفي تركيزا أكثرعلى تعزيز التعاون بين الدفاع المدني والعسكري، من خلال إنشاء فرق استجابة للأزمات السيبرانية عبر الحدود وحماية شبكة اتصالات (Pernik, 2017, p. 05).

على الرغم من هذا التحديث، واجه الإطار تحديات جوهرية، منها افتقاره إلى آليات إنفاذ ملزمة لضمان التزام الدول الأعضاء بمضامينه، وعدم معالجته الكافية للهجمات القادمة من خارج الاتحاد، كذلك إغفاله رسم استراتيجيات واضحة لمكافحة الأنشطة الإرهابية السيبرانية، حيث إقتصر تركيزه على الجوانب العسكرية.

3.2 الأجندة الأوروبية للأمن 2015-2020

تم اعتمادها من طرف المفوضية الأوروبية في أبريل 2015، تحت مسمى "الأجندة الأوروبية للأمن" (Commission, EU cybersecurity initiatives: working towards

(a more secure online environment, 2016, p. 02) بهدف خلق مجال للأمن الداخلي في الاتحاد الأوروبي حتى عام 2020. حددت مواجهة الجرائم والهجمات السيبرانية - خاصة الإرهابية منها - باعتبارها إحدى المحاور الرئيسية، حيث تضمنت تدابير عملية مثل إنشاء مركز أوروبي لمكافحة الإرهاب، وتطوير استراتيجيات تفصيلية للتعامل معه، وتعزيز التعاون مع القطاع الخاص (Vogl, 2015, p. 02).

وعلى عكس السياسات السابقة، لم تشجع الأجندة على إيجاد تشريعات جديدة، بل دعت إلى التنفيذ الكامل والفعال للقوانين والآليات القائمة. بالإضافة إلى ذلك، ركزت على تعزيز التعاون القضائي بين الدول الأعضاء من خلال تشجيع الاعتراف المتبادل بالقرارات القضائية وتشكيل فرق تحقيق مشتركة كما عملت الأجندة على بناء القدرات من خلال تنفيذ التشريعات القائمة وإيجاد مجال أكبر للتعاون الأمني والقضائي بين أصحاب المصلحة الأعضاء. (Vogl, p. 03)

رغم هذه الجهود، يؤخذ على هذه الأجندة أن عدم تشجيعها على إيجاد تشريعات جديدة يعتبر قصورا منها في مواجهة التهديدات الأمنية المتطورة خاصة في ظل التغيرات السريعة في طبيعة الجرائم السيبرانية والإرهابية.

4.2 توجيه أمن الشبكات وأنظمة المعلومات (NIS)

تم إعتماد هذا التشريع بموجب اتفاق سياسي اعتمد في ديسمبر 2015 تحت رقم 2016/1148. ودخل حيز النفاذ في أغسطس 2016. تضمن وضع حد أدنى لمتطلبات الأمن السيبراني المشتركة بين دول الاتحاد الأوروبي. ومنح مدة واحد وعشرين شهرا لتضمين متطلباته في تشريعاتهم الوطنية، وستة أشهر إضافية لتحديد مشغلي الخدمات الأساسية المعتمدين من قبلهم. (Malthe Munkøe, p. 78)

هدف التوجيه إلى تحسين القدرات الوطنية والإقليمية للدول الأعضاء في مواجهة الطوارئ السيبرانية، من خلال إلزام الأعضاء بوضع استراتيجية وإيجاد هيئات للأمن السيبراني، وفريق استجابة لطوارئ أمن الكمبيوتر على مستوى وطني. كما سعى إلى تحسين أطر عمل الوكالات الوطنية عبر وضع معايير تحقق المرونة السيبرانية. تتضمن إلزام مشغلي الخدمات الأساسية (مثل الرعاية الصحية، والطاقة، والمياه، والنقل، والخدمات المصرفية) ومقدمي الخدمات الرقمية (محركات البحث، وخدمات الأسواق عبر الإنترنت، وخدمات الحوسبة

السحابية) باعتماد تدابير أمنية صارمة، وإبلاغ الجهات المختصة عن الهجمات السيبرانية (Commission, EU cybersecurity initiatives: working towards a more secure online environment, p. 04)

اعتبر هذا التوجيه خطوة متقدمة في استجابة التشريعات الجنائية للجرائم السيبرانية، حيث ساهم في تقارب التشريعات الوطنية لتجريم الهجمات السيبرانية، ما سهل التعاون عبر الحدود بين سلطات إنفاذ القانون.

مع ذلك، سجلت نقائص عديدة في تنفيذه، مما أبرز الحاجة إلى تحديثه بانتهاء مدته عام 2020.، بموجب التوجيه رقم 2022/2555 (NIS 2) الذي دخل حيز النفاذ في يناير 2023، تضمنت توجيهاته نطاقا أكثر شمولا, كإلزام الكيانات بتطوير ملفات مخاطر أمنية عالية، وتغطية حوادث السيبرانية واسعة النطاق، وإخضاع قطاعات جديدة مثل الاتصالات والبريد والصناعة الكيميائية والنووية وقطاع البيئة. كما حدد شهر أكتوبر 2024 موعدا نهائيا للامتثال لمتطلباته (Parliament, Supporting the implementation of Union policy and law regarding cybersecurity/ NIS 2 Network and Information Systems Directive, 2022 2023)

اشترط التوجيه على الدول الأعضاء تحديد الكيانات التي تعتبرها بنى تحتية حيوية، كما وضع التزامات على هذه الكيانات بضمان قدرتها على الصمود من خلال إجراء تقييم دوري للمخاطر التي تؤثر على عملها ووجودها. كما يتعين عليها أيضا التعهد بالرفع المستمر من القدرة على الصمود في وجه الهجمات السيبرانية ومختلف التهديدات ذات الصلة.

من المتوقع أن يحقق هذا التوجيه تنسيقا أكبر بين التشريعات الوطنية خاصة بعد مراجعته بموجب اقتراح تشريعي قدم إلى اللجنة البرلمانية عام 2021، دعا إلى تشديد التزامات الأمن السيبراني في مجالات إدارة المخاطر والإبلاغ، وتبادل المعلومات (European Parliament E. U., 2022, p. 11).

5.2 استراتيجية 2017 للأمن السيبراني وقانون الأمن السيبراني

في عام 2017، أصدرت المفوضية الأوروبية استراتيجية جديدة للأمن السيبراني (RTE, 2017) كتحديث لاستراتيجية 2013، ردا على الهجمات السيبرانية المتزايدة التي أصبحت أكثر خطورة على البنى التحتية الحيوية وقيم الاتحاد.

تضمنت إنشاء آليات جديدة مثل الوكالة الأوروبية للأمن السيبراني، بهدف المساعدة في الدفاع ضد الهجمات السيبرانية واسعة النطاق (Speech, 2017).

ومن أجل تنفيذ هذه الاستراتيجية، قدمت المفوضية في العام ذاته قانون الأمن السيبراني (CERT-EU) بعنوان"إطار عمل للرد الدبلوماسي المشترك للاتحاد الأوروبي على الهجمات الضارة"، عرف أيضا باسم "مجموعة أدوات الدبلوماسية السيبرانية" (European Parliament E. U., p. 03).

سعى هذا القانون إلى تحقيق هدفين رئيسيتين: الأول تمثل في التصدي للهجمات المتزايدة على البنى التحتية الحيوية التي تمس مقومات الحياة اليومية مثل الماء والكهرباء والصحة، والثانية الحد من حالات الاختراق التي تمس بيانات المستخدمين الخاصة. (EU Cybersecurity Regulatory Landscape, 2024, p. 08) ولتحقيق ذلك تم وضع مخطط للاستجابة المنسقة لحالات وأزمات الأمن السيبراني الواسعة النطاق.

اعتبرت هذه الآليات خطوة مهمة في تطوير سياسة الأمن السيبراني للاتحاد، من حيث تعزيز القدرات الدفاعية وتحسين التعاون في مواجهة التهديدات السيبرانية.

على الرغم من ذلك، واجهت هذه الاستراتيجية والقانون عدة تحديات أبرزها صعوبة التنسيق الناجم عن الاختلاف في التشريعات الوطنية وتفاوت القدرات التقنية بين الدول، إلى جانب محدودية الموارد المالية والتكنولوجية لدى بعضها (Sadoian, 2025). وقد أدى ذلك إلى ظهور إشكاليات قانونية مرتبطة بتفسير وتطبيق "مجموعة أدوات الدبلوماسية السيبرانية"، خاصة في سياق الهجمات العابرة للحدود (Revised Implementing Guidelines, Cyber Diplomacy Toolbox، 2023). إضافة إلى ذلك، برزت مخاوف بشأن تحقيق التوازن بين تعزيز الأمن السيبراني وحماية خصوصية البيانات، فضلا عن ضرورة التصدي للتهديدات السيبرانية المتطورة التي تعتمد على تقنيات حديثة مثل الذكاء الاصطناعي (The Cyber Diplomacy Toolbox، 2017).

رغم هذه التحديات، تعتبر استراتيجية 2017 وقانون الأمن السيبراني خطوتين مهمتين نحو تعزيز الأمن السيبراني في دول الاتحاد، من خلال توفير إطار شامل للتعاون والرد على التهديدات السيبرانية.

6.2 استراتيجية العقد الرقمي وتوجيه NIS 2 لعام 2020

في سياق التصدي المتطور للتهديدات السيبرانية، أطلقت المفوضية الأوروبية أواخر عام 2020، استراتيجية جديدة للأمن السيبراني بعنوان "من أجل العقد الرقمي" (European Parliament E. c., 2020) تمتد لعشر سنوات (2020-2030). سعت إلى تحقيق هدفين رئيسيين: تعزيز البنية التحتية الرقمية الآمنة وضمان السيادة الرقمية للاتحاد الأوروبي. وتم التوصل إليها من خلال مجموعة من المبادرات الشاملة التي تضمنت تطوير أنظمة أسماء النطاقات (DNS) وإنشاء شبكة مراكز العمليات الأمنية (Cyber Shield) لرصد التهديدات السيبرانية بشكل استباقي. كما دعت الاستراتيجية لتحديث توجيه أمن الشبكات وأنظمة المعلومات (NIS) من أجل معالجة الإختلافات المسجلة في تطبيق المعايير الأمنية بين الدول الأعضاء.

دخل التوجيه المحدث NIS 2، حيز النفاد في يناير 2023، وجاء بمعايير أكثر شمولا من سابقه. حيث وسع نطاقه ليشمل قطاعات حيوية جديدة وفرض تقييمات دورية للمخاطر وإجراءات أمنية مشددة، مع تحسين آليات الإبلاغ عن الحوادث الأمنية بين الدول الأعضاء. (The NIS 2 Directive | Updates, Compliance, 2024).

اتسمت هذه الاستراتيجية بتبنيها تدابير متقدمة، حيث فرضت على الشركات الكبرى التزامات صارمة فيما يخص تطبيق المعايير الأمنية وشجعت الاستثمار في التقنيات الحديثة مثل الذكاء الاصطناعي وأنظمة التشفير. كما عززت بشكل ملحوظ التعاون بين دول الاتحاد الأوروبي وشركائه الدوليين سيما حلف الشمال الأطلسي والولايات المتحدة الأمريكية بهدف تكثيف الجهود لمواجهة التهديدات السيبرانية بشكل أكثر فعالية وتكامل.

ورغم هذا، تواجه استراتيجية 2020 وتوجيه NIS 2 تحديات مشتركة أثرت على فعاليتهما. حيث لوحظ تركيز مفرط على الجوانب التقنية على حساب تطوير سياسات متكاملة لمواجهة بعض القضايا مثل التطرف والتجنيد عبر الفضاء السيبراني. كما أن التوجيه الجديد لم يورد حلولا كافية للتعامل مع التهديدات الخارجية المعقدة. أيضا أدى عدم وجود إطار قانوني موحد إلى تفاوت كبير في تطبيق السياسات الأمنية بين الدول الأعضاء، مما أثر سلبا على التنسيق

الإقليمي (Kettemann, 2021, p. 05) كما برزت تحديات تنظيمية مثل غموض تعريف الكيانات الأساسية، وعدم وضوح معايير تقييم المخاطر وزيادة الأعباء المالية والإدارية، خاصة على الشركات الصغيرة والمتوسطة (Wilczynska-Baraniak, 2023, pp. 19-25).

رغم هذه التحديات، تعتبر استراتيجية 2020 وتوجيه NIS، خطوات مهمة نحو تعزيز الأمن السيبراني في الاتحاد الأوروبي. إلا أنه، لا تزال هناك حاجة إلى سياسات أكثر شمولية لمعالجة جميع أبعاد الإرهاب السيبراني، بما في ذلك تطوير آليات إنفاذ قانونية موحدة وضمان التوازن بين الأمن وحماية الخصوصية.

3.استجابة الاتحاد الأوروبي لتهديدات الإرهاب السيبراني على المستوى الخارجي

يرجع أصل سياسة الاتحاد الخارجية للأمن السيبراني إلى عام 2013 عندما تم اعتبار الأمن السيبراني قضية دولية بالغة الأهمية. وجاء ذلك في إطار "استراتيجية الاتحاد الأوروبي للأمن السيبراني 2013" التي أكدت على الحكومات ضرورة اعتبار الأمن السيبراني أولوية ضمن أولوياتها الخمس ودعت إلى تبني سياسات دولية متماسكة للفضاء السيبراني تتماشى مع قيم الاتحاد الأوروبي. (European Parliament t. C., 2013) وقد سبق هذا تقرير الصادر عام 2008 حول تنفيذ استراتيجية الأمن الأوروبية، والذي صنف الأمن السيبراني كأحد التحديات الرئيسية المهددة للأمن الأوروبي، مشددا على ضرورة تعزيز التعاون في هذا المجال (Union C. o., Report on the Implementation of the European Security Strategy - Providing Security in a Changing World -, 2008, p. 05)

من جانب آخر، أكدت المفوضية الأوروبية في إطار "حوارنا وتعاوننا الاستراتيجيين" مع الجهات الدولية عام 2019، على أهمية إشراك المجتمع الدولي في تطوير معايير الأمن السيبراني (Cmmunities, 2009, p. 07). وذلك انطلاقا من قناعة مفادها أن النهج الأوروبي المنفرد غير كاف لمواجهة التحديات المستقبلية، كما أشارت المفوضية عام 2011 إلى حماية البنى التحتية الحيوية وتكنولوجيا المعلومات. الأمر الذي استدعى دمج السياسة الأوروبية المتماسكة ضمن استراتيجية عالمية تشمل شركاء أساسيين من الدول والمنظمات الدولية. (Parliament, Critical Information Infrastructure Protection – Achievements and Next steps: Towards Global Cyber-Security, 2012, p. 04)

1.3 سياسة الاتحاد الخارجية في ظل استراتيجية الأمن السيبراني 2013

ساهمت استراتيجية 2013، بشكل كبير في تعزيز الجهود اللاحقة لتحقيق تقدم ملموس في مجال الأمن السيبراني، حيث دعت إلى تطبيق المبادئ والقيم والمعايير الأوروبية المقبولة، بالحفاظ على قيم الديمقراطية وحماية الحقوق الأساسية وسيادة القانون في الفضاء السيبراني (European Parliament t. C., 2013) وأكدت الاستراتيجية على أن الأمن السيبراني متعدد الأبعاد من شأنه أن يؤثر على سياسات الاتحاد المختلفة، سيما الاقتصادية (مثل السوق الرقمية الموحدة) والأمنية (مثل سياسة الأمن والدفاع المشتركة) والتي تشكل مجتمعة الأنشطة الخارجية للاتحاد. ومن أجل ضمان فعالية مواجهة التحديات السيبرانية، أكدت الاستراتيجية على ضرورة الجمع بين البعدين الداخلي والخارجي في السياسة الأمنية للاتحاد.

تركز عمل الاتحاد الأوروبي على تحقيق الأولويات الخمس التي حددتها الاستراتيجية، والتي اعتبرت أن تحديات الأمن السيبرانية ذات طابع عالمي. وبناء على ذلك، عمل الاتحاد على دمج قضايا الفضاء السيبراني في سياسته الخارجية والأمنية المشتركة، من خلال التعاون مع المنظمات الدولية الفاعلة في هذا المجال. مثل مجلس أوروبا، والأمم المتحدة، ومنظمة التعاون الاقتصادي والتنمية (OECD)، ومنظمة الأمن والتعاون في أوروبا (OSCE) وحلف شمال الأطلسي (NATO)، والاتحاد الأفريقي، ورابطة أمم جنوب شرق آسيا (ASEAN)، ومنظمة الدول الأمريكية (OAS). كما شمل التعاون دولا منفردة، على رأسها الولايات المتحدة الأمريكية التي تمثل الشريك الرئيسي للاتحاد في هذا المجال، حيث شكلا فريق عمل مشترك خاص بالأمن السيبراني والجرائم الإلكترونية منذ عام 2010 (European Parliament t. C., 2013)

2.3 بروز الدبلوماسية السيبرانية وتطورها

تمثل الدبلوماسية السيبرانية أحد الركائز الأساسية في مواجهة التحديات المعاصرة للفضاء السيبراني، بما في ذلك قضايا الأمن السيبراني وحوكمة الإنترنت وحماية الحقوق الرقمية. وعلى الرغم من عدم ذكر هذا المفهوم صراحة في استراتيجية الاتحاد الأوروبي للأمن السيبراني لعام 2013، إلا أن الوثائق اللاحقة

مثل استنتاجات المجلس الأوروبي لعام 2015 (Council G. S., Council Conclusions on Cyber Diplomacy, 2015) وخطة عمل الاتحاد لحقوق الانسان والديمقراطية (Union C. o., EU Strategic Framework and Action Plan on Human Rights and Democracy, 2012)، أشارتا إلى مفهومها. حيث تم وصف المحتوى الأساسي للدبلوماسية السيبرانية على أنه يشمل أربعة محاور رئيسية: تعزيز الأمن السيبراني، وتطبيق القانون الدولي، وتطوير حوكمة الإنترنت، وبناء القدرات السيبرانية (Union C. o., EU Strategic Framework and Action Plan on Human Rights and Democracy, p. 02) كما بينت الاستنتاجات حاجة الاتحاد إلى تحديد أولوياته المتعلقة بالمسائل السيبرانية الأمر الذي استدعى اتخاذ إجراءات مشتركة وحاسمة للحد من الجرائم السيبرانية، وخلق جو من الاستقرار والتماسك في العلاقات بين أعضاء الاتحاد ودول أخرى. (Helena Carrapico, 2017, p. 1255)

وفي استجابة للتصاعد الملحوظ في الهجمات السيبرانية، الذي تخلل فترة ما بين 2016-2017 تم ادخال تحديثات مهمة في هذا المجال. حيث قدمت الرئاسة الهولندية في 2016 وثيقة غير رسمية حول تطوير الدبلوماسية السيبرانية المشتركة (Council P. o., 2016) وإطار عمل "مجموعة أدوات الدبلوماسية السيبرانية" لعام 2017 (Council G. S., Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") - Adoption, 2017) تلاها ادخال تحديث على استنتاجات المجلس الأوروبي عام 2017. وأقر الاتحاد في أكتوبر 2017 "مجموعة أدوات الدبلوماسية السيبرانية" تضمنت إجراءات وقائية وتقييدية للتصدي للأنشطة السيبرانية الخبيثة (Council G. S., Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities approval of the final text, 2017)

لقد حققت الدبلوماسية السيبرانية في ظل هذه الاستراتيجية إنجازات بارزة يمكن إجمالها في أربعة محاورأساسية: ففي مجال التعاون الدولي، قام الاتحاد الأوروبي بتعزيز آليات الحوار وبناء الثقة عبر إنشاء فريق متخصص للدبلوماسية السيبرانية (EEAS) تحت مظلة المفوضية الأوروبية والخدمة الخارجية. مكن هذا الفريق الاتحاد من تعزيز التواصل مع الدول والمنظمات الدولية ذات الرؤى المماثلة، كما نجح الاتحاد في دفع أربعة وعشرون دولة غير أوروبية للتصديق على الاتفاقية بحلول 2024، مما عزز الإطار القانوني العالمي لمكافحة الجرائم الإلكترونية. ومن جانب آخر منحت الاتحاد دورا قياديا في دعم الدول النامية

لبناء قدراتها السيبرانية، من خلال تقديم المساعدات الفنية وبرامج بناء القدرات، خاصة تلك التي تعاني من ضعف البنية التحتية والقوانين السيبرانية (European Parliament t. C., 2013, pp. 07-08).

وبالرغم من هذه المكتسبات، تواجه هذه الدبلوماسية عوائق قانونية وعملية جسيمة أهمها غياب إطار قانوني دولي موحد للجرائم السيبرانية قادر على مجابهة الطبيعة العابرة للحدود، والنقص المسجل في آليات تبادل المعلومات الأمنية بين الدول بموجب اتفاقات ملزمة، أيضا، تباين المواقف السياسية والقانونية بين القوى الكبرى حول مبادئ حوكمة الفضاء السيبراني كذلك التفاوت التقني والتنظيمي بين الدول، بالإضافة إلى الصعوبات الإجرائية في إثبات المسؤولية وتتبع الجرائم الإلكترونية بسبب تقنيات إخفاء الهوية والبنى التحتية الموزعة. (Dragomir، 2021).

وبنظرة استشرافية، يمكن القول أن الدبلوماسية السيبرانية ورغم ما تواجهه من تحديات، تبقى أداة حيوية لمواجهة التهديدات السيبرانية المتزايدة شرط تطوير سياسات أكثر شمولية وتوفير الموارد الكافية لضمان فعالية تنفيذها كون نجاحها يظل مرهونا بالقدرة على معالجة التحديات القائمة وتعزيز التعاون الدولي في هذا المجال الحيوي.

3.3 سياسة الاتحاد الخارجية في إطار استراتيجية العقد الرقمي 2020

ركزت استراتيجية العقد الرقمي 2020 للاتحاد الأوروبي على تعزيز السياسة الخارجية في مجال الأمن السيبراني من خلال ثلاث ركائز أساسية: الحماية من التهديدات السيبرانية، وتعزيز التعاون الدولي، وضمان إنترنت عالمية مفتوحة وآمنة (European Parliament E. c., p. 04). وقد تضمنت الاستراتيجية عدة مبادرات عملية إقترحت من خلالها إنشاء وحدة استخبارات سيبرانية ضمن مركز الاستخبارات الأوروبي (Eu INTCEN) من أجل تعزيز التنسيق الاستراتيجي في مواجهة التهديدات. كما طور الاتحاد نظام عقوبات ضد الجهات المسؤولة عن الهجمات السيبرانية، بالتعاون مع حلف الشمال الأطلسي (López, 2022, p. 726) كذلك دعمت الاستراتيجية تحديث اتفاقية بودابست 2001، وسعت لإنشاء إطار قانوني دولي جديد برعاية الأمم المتحدة لتوحيد الجهود العالمية في مكافحة

الجرائم السيبرانية. (López, p. 727) إضافة إلى ذلك، وفي إطار"بوصلة الأمن والدفاع"، وضعت الاستراتيجية برنامجا لبناء القدرات السيبرانية لدول الاتحاد ودول الجوار مع التركيز على تعزيز قدرات التحقيق في الجرائم السيبرانية ومحاكمة مرتكبيها (Annual Progress Report on the Implementation of the Strategic Compass for Security and Defence, 2024, p. 46)

وتواجه سياسة الاتحاد الخارجية في ظل هذه الاستراتيجية تحديات معقدة فمن جانب قانوني، أدى تضارب التشريعات الجنائية واختلاف التعريفات القانونية إلى صعوبات كبيرة في توحيد المفاهيم القانونية للجرائم السيبرانية ما أبرز إشكاليات عملية في تبادل الأدلة الإلكترونية عبر الحدود بسبب اختلاف المعايير والإجراءات القانونية بين الدول (Stürzer, 2022, pp. 06-08).

ومن جانب التعاون الدولي، وبسبب اختلاف وجهات النظر بين الشركاء الدوليين خاصة الولايات المتحدة حول بعض القضايا الهامة منها تحديد الشركات العملاقة (Gatekeepers) وفيما إذا كانت القوانين الأوروبية تستهدف الشركات الأمريكية بشكل تمييزي. كما تواجه استراتيجية الاتحاد الجديدة مقاومة من قبل الشركات التكنولوجية الكبرى، التي ترفض تغيير نماذج أعمالها القائمة على استغلال بيانات المستخدمين (Stürzer, 2022, pp. 03-06).

كما تواجه هذه السياسة معضلة الموازنة بين الأمن السيبراني والانفتاح الاقتصادي حيث تحاول السياسة الأوروبية إيجاد توازن دقيق بين المتطلبات الأمنية والمصالح الاقتصادية. إلا أنه تكتنفها مخاوف أمنية من استخدام معدات تكنولوجية أجنبية، ومن جهة أخرى، الحتمية اقتصادية التي تفرض عدم استبعاد هذه المعدات (Stürzer, 2022, pp. 04-05).

رغم هذه التحديات تمثل سياسة الاتحاد في ظل هذه الاستراتيجية اطارا شاملا وطموحا يعكس رؤية استباقية منه لتعزيز أمن جماعي في مواجهة التهديدات السيبرانية المتزايدة خاصة الإرهابية منها، من خلال الحفاظ على التوازن بين الأمن الرقمي والمتطلبات الأساسية.

خاتمة:

وإن كان الاتحاد الأوروبي حاليا يعتبر الفاعل الرئيسي من حيث إنشاء تدابير الأمن السيبراني بقطعه أشواطا طويلة في عملية مكافحة الإرهاب السيبراني والتهديدات ذات الصلة، بوضعه أطرا أمنية موحدة وفعالة، تم التأسيس لها مند عام 2001، تاريخ ابرام اتفاقية بودابست، كآلية مشتركة مثلت المنطلق في عملية وضع آليات العمل اللاحقة لمكافحة هذا التهديد على مستوى إقليمي، لتتطور فيما بعد من خلال التجربة وتأخذ طابعا خارجيا. إلا أنه يمكن القول أن عملية الحد من تهديد الإرهاب السيبراني وفق الأطر الحالية مازالت في حاجة إلى تطوير، لسبب يرجع إلى الطبيعة المعقدة التي تميز كلا من:

- التهديد المتطور والعابر للحدود، حيث مازال غير متفق في تحديده بوضوح، وإن تركز تهديده حسب رؤية الاتحاد على الهجمات السيبرانية على البنى التحتية، والتي بدورها أنتجت غموضا في شكل تحدي آخر حول الجهات القائمة عليها وتقارب الحدود بين أنشطة الإرهاب السيبراني والعمليات الإجرامية ذات الصلة.
- والثانية هي تركيبة الاتحاد ذاته وآلية عمله المعقدة، حيث بدا واضحا تباين رؤى أعضاء الاتحاد حول التهديد من خلال تنفيذ لتوجيهاته بطرق مختلفة الأمر الذي أوجد نقاط ضعف بكل آلية يتم ايجادها أو تحيينها.

وتداركا لهذه التحديات خلص الاتحاد إلى الاستعانة باستجابة على مستوى خارجي، بإشراك أطراف ثالثة خارجية في عملية المكافحة، كتدعيم للعملية الداخلية من خلال مجموعة أدوات وسياسات تعاون. ومن ثم نخلص إلى مجموعة من النتائج تتمثل في:

أولا: يفتقر الاتحاد إلى تعريف واضح للإرهاب السيبراني، حيث يعالجه كتهديد محتمل ضمن إطار الجرائم الإرهابية، رغم الاعتراف بتصاعد خطورته تدريجيا.

ثانيا: بسبب عدم تسجيل هجوم إرهاب سيبراني فعلي حتى اليوم، يرى الاتحاد الأوروبي أن التهديد المتوقع عنه ينحصر في استهداف البنى التحتية الحيوية المتسمة بالضعف، وأنه بعيد الوقوع داخل الاتحاد.

ثالثا: أن دافع استجابة الاتحاد لتهديد الإرهاب السيبراني ليست نابعة من هجمات سيبرانية واقعة، إنما باعتبارها عملية استباقية بنيت على احتمال مفترض من الحوادث الجيوسياسية لمثل حالات استونيا، إيران وأكرانيا.. الخ.

رابعا: استجاب الاتحاد للتزايد المستمر للهجمات السيبرانية بتوسيع تصوره الاستراتيجي، أين كشف عام 2013 عن أول استراتيجية له للأمن السيبراني استمرت في التطور وبلغت ذروتها باستراتيجية جديدة أكثر طموحا أطلقها في ديسمبر 2020. صاحب ذلك إنشاء وتطوير عديد الآليات القانونية، السياسية والمؤسسية بأبعاد مختلفة، إقليمية وعلى مستوى خارجي.

وفي ضوء ما توصل إليه البحث من نتائج، نورد بعض التوصيات:

. استئناف الاتحاد الأوروبي مناقشات تحديده لمعايير تعريف الإرهاب السيبراني التي بدأها عام 2011، من أجل ضمان تطبيق متسق لسياساته.

. إيجاد جهاز مستقل داخل الدول الأعضاء يتبع مؤسسة الاتحاد، يسهر على متابعة التطبيق الصحيح والموحد لمضمون توجيهاته على الأرض من أجل ضمان استجابة أكثر تناسبا.

. إيجاد بروتوكول ملحق باتفاقية بودابست خاص بالإرهاب السيبراني وتعزيز التنسيق بين الأدوات الداخلية والخارجية.

. معالجة الفجوة بين التقييمات الاستباقية والتهديدات الواقعية عبر تحديث مستمر للاستراتيجيات.

. الدعم الفعلي والغير مشروط للدول النامية والضعيفة المنظمة إلى اتفاقية بودابست وجعلها جهة إسناد للاتحاد في مكافحة الإرهاب السيبراني ومختلف التهديدات ذات الصلة.

قائمة المراجع:

Amor, N. S. (2022, Novembre 18). *Why the EU need access to first-hand intelligence information.* Retrieved 10, 11, 2024. from agence europe: https://bit.ly/4hjqTu1

Andreea Dragomir .(2021) .Cyber Diplomacy .*Lucian Blaga University of Sibiu*.10-05 ،

Annegret Bendiek Matthias C. Kettemann .(2021) .*Revisiting the EU Cybersecurity Strategy ..*germany: Stiftung Wissenschaft und Politik (SWP) – German Institute for International and Security Affairs.

Annual Progress Report on the Implementation of the Strategic Compass for Security and Defence. (2024).European Union.

Ansaria, A. (2024). Analysis of Ukraine power grid cyber-attack 2015. *World Jurnal of Advenced Engineering Technology and Sciences*, 02.

Barry C. Collin .(1996) .*The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge* .US: Institute for Security and Intelligence.

Christopher Baker-Beall, G. M. (2021). Understanding the European Union's Perception of the Threat of Cyberterrorism: A Discursive Analysis. *Journal of Common Market Stadies*, 1092.

Cmmunities, C. o. (2009, March 30). *Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience.*

Commission, E. (2016, July 05). *EU cybersecurity initiatives: working towards a more secure online environment.*

Commission, E. (2020, July 24). Communication From the Commission on the EU Security Union Strategy. Brussels, European Union: European Commission.

Council of The European Union .(2002) .*Terrorist Activity in the European Union: Situation and Trend Report 2001 - 2002 (TE-SAT)* .Brussels: European Union.

Council of the European Union .(2010) .*EU Counter- Terrorism Strategy - Discussion Paper* .Brussels: European Union.

Council of The Europeran Union. (2002, June 13). Council Framework Decision. Brussels, Europeran Union: Europeran Union.

Council, G. S. (2015, February 11). *Council Conclusions on Cyber Diplomacy.*

Council, G. S. (2017, June 07). *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") - Adoption.*

Council, G. S. (2017, Octobre 09). *Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities approval of the final text.*

Council, P. o. (2016, May 19). *Non-paper: Developing a joint EU diplomatic response against coercive cyber operations - final revised text.*

Counter- Terrorism Coordinator .(2006) .*Implementation of the Action Plan to Combat Terrorism* .Brussels: Council of the European Union.

.(2013)*Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace .*

Dorothy E. Denning 23) .May 2000 .(*Testimony before the Special Oversight Panel on Terrorism* .Washington: Georgetown University. retrieved 05.12.2024. from: https://bit.ly/3PAuV5l

EU Cybersecurity Regulatory Landscape. (2024, May).

Europe, C. o. (2001, November 23). Convention on Cybercrime. Budapest, European Union.

European Parliament, E. c. (2020, December 16). Join Communication The EU's Cybersecurity Strategy for the Digital Decade. Brussels, Belgium.

European Parliament, E. U. (2022, December 14). DIRECTIVE (EU) 2022/2555 (NIS2) on measures for a high common level of cybersecurity across the Union. Brussels, belgium.

European Parliament, t. C. (2013). JOIN 2013 Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Brussels, Belgium.

Gabriel Weimann .(2004) .Cyberterrorism How Real Is The Threat? ،Special Report .*United States Institute of Peace*.09 ،

Helena Carrapico, A. B. (2017). The EU as a Coherent (Cyber)Security Actor? *JCMS: Journal of Common Market Studies*, 1255.

Issah, A. (2021). *Achieving Cyber Peace Through an Efective Cybersecurity Governance: Analysis of the European Union Cybersecurity Strategy.* Finland: Tampere University.

Jayakumar, S. (2021). Cyber Attacks by Terrorists and other Malevolent Actors: Prevention and Preparedness. In A. P. Schmid, *Handbook of Terrorism Prevention* (p. 873). Netherlands: International Centre for Counter-Terrorism – The Hague (ICCT).

Justyna Wilczynska-Baraniak .(2023) .*The future of cybersecurity in Europ Challenges related to the NIS2 Directive* .Poland: EY .

Katarina Kertysova, E. F. (2018). *Cybersecurity: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks.* European Union: European Economic and Social Committee.

Leah Sadoian 09) .Jan, 2025 .(The EU Cyber Diplomacy Toolbox: Shaping Global Cybersecurity Standards .

López, J. J. (2022). The european union as an international actor in cybersecurity. *Cuadernos de Derecho Transnacional*, 715.

Madnick, S. (2022, March 07). *What Russia's Ongoing Cyberattacks in Ukraine Suggest About the Future of Cyber Warfare*. Retrieved from HBR Insight Centers: https://bit.ly/3C0qUEa

Malthe Munkøe, H. M. (2022). Cybersecurity in the era of hyper competitiveness: can the EU meet the new challenges? La ciberseguridad en la era de. *Revista CIDOB d'Afers Internacionals*, 74.

Mark M. Pollitt .(1998) .Cyberterrorism — fact or fancy ?*Computer Fraud &Security*, 03.

Matthias Vogl .(2015) .*Center for European Integration Studies -University of Bonn Germany*, 02.

Maura Conway .(2003) .*Cyberterrorism: The Story So Far* DORAS | DCU

Mortera-Martinez, C. (2018, July 09). *Game over? Europe's cyber problem.* Retrieved from Centre For European, 05.

Parliament, E. (2012). *Critical Information Infrastructure Protection – Achievements and Next steps: Towards Global Cyber-Security.* Brussels: European Parliament.

Parliament, E. (2022 2023, January 16). *Supporting the implementation of Union policy and law regarding cybersecurity/ NIS 2 Network and Information Systems Directive.* Retrieved 20, 12, 2024. from: https://bit.ly/3WnEEjfPernik,

B. L. (2017, December). *EU–NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions.*

Revised Implementing Guidelines, (2023). Cyber Diplomacy Toolbox .Union, Council of the European Retrieved 01, 01, 2025. from . https://bit.ly/4iQsRmI

Sheelagh Brady, C. H. (2020). *Cybercrime: Current Threats and Responses. A review of the research literature.* Irland: Research and Data Analysis Unit.

Speech, E. C. (2017, September 13). *President JEAN-Claude Juncker's State of the Union Address 2017.* Retrieved 10, 12, 2024. from: https://bit.ly/3DWWC5L

Stürzer, A. B. (2022). *Advancing European Internal and.* Berlin: Stiftung Wissenschaft und Politik (SWP).

team, E. (2019). *Challenges to effective EU cybersecurity policy.* ECA, European Court of Auditors .

Council of the European Union. (2017). The Cyber Diplomacy Toolbox. Retrieved 02, 01, 2025. from: https://bit.ly/41Q4EH3

The NIS 2 Directive | Updates, Compliance. (2024). Switzerland: GmbH, Cyber Risk.

Union, C. o. (2008). *Report on the Implementation of the European Security Strategy - Providing Security in a Changing World -.* Brussels: Council of the European Union.

Union, C. o. (2012, June 25). *EU Strategic Framework and Action Plan on Human Rights and Democracy.*

United Nations Manual on the Prevention and Control of Computer-Related Crime) .May, 1994 .(*International review of criminal policy* .

Working Party on Terrorism .(2011) .*Summary of Discussions* .Brussels: Council of the European Union.