Journal of Police and Legal Sciences

Volume 14 | Issue 2 Article 2

7-31-2023

Mechanisms to reduce cyber threats and risks

Saad alsuwaileh

DOI: https://doi.org/10.69672/3007-3529.1017

آليات الحد من التهديدات والمخاطر السيبرانية

عميد دكتور / سعد مفلح حمود الصويلح

أكاديمية سعد العبد الله للعلوم الأمنية، الكويت

الملخص :

تناول آليات الحد من التهديدات والمخاطر السـيبرانية البحث لأن الفضـاء الإلكتروني سـاحة هامة للتفاعلات الدولية المختلفة، خاصـةً في الآونة الأخيرة في ظل زيادة الهجمات الإلكترونية بين بعض الدول، بما يؤثر على أمنها القومي. وفي إطار ذلك تحاول العديد من الدول بذل الجهد من أجل تطوير قدراتها لاسـتخدامها في أي هجوم إلكتروني، أو اتخاذ الإجراءات الوقائية الكافية لحمايتها من أي هجمات إلكترونية محتملة، خاصةً في ظل تأثير تلك الهجمات على أماكن ومؤسـسـات حيوية مثل البنوك والوزارات أو على المرافق الهامة مثل مرافق المياه والكهرباء وغيرها من الخدمات المختلفة التي تؤثر سـلباً وبشـكل مباشر على المواطنين ...وأن الهجمات الإلكترونية تتزايد وتيرتها مؤخراً بشكل كبير، سواءً من حيث الحجم أو التطور أو شدة التأثير...والتعاون الدولي مع سـلطات إنفاذ القانون، وأن تتخذ كل دولة طرف تدابير بتبادل وتقديم معلومات مفيدة إلى السـلطات المختصـة لأغراض التحقيق والإثبات الجنائي في القضايا السيبرانية ، وفي ضوء التطور المستمر لظاهرة الجريمة السيبرانية ، يتعين على أجهزة الشرـطة الدولية تبادل المعلومات والمعارف من أجل اتخاذ إجراءات آنية مسـتندة إلى المعلومات بشـأن تجميع الأدلة الجنائية الرقمية وتأمين وحماية البنية التحتية الإلكترونية الحرجة من الاختراق الإلكتروني والحماية من الهجمات السـيبرانية للمنشـآت الهامة والحيوية وخاصـة هجمات الحرمان من الخدمة Denial of Service (DoS) وهي من أهم التوصـيات التي استخلصت من الدراسة.

الكلمات المفتاحية:

المخاطر السيبرانية- الهجمات الإلكترونية – مواجهة التهديدات السيبرانية.

Mechanisms to reduce cyber threats and risks

Dr.Saad mefleh humoud alsuwaileh
Saad Al-Abdullah Academy for Security Sciences (State of Kuwait)

Abstract :

Addressing the mechanisms of reducing cyber threats and risks Research Because cyberspace is an important arena for various international interactions, especially in recent times in light of the increase in cyber-attacks between some countries, which affects their national security. In this context, many countries are trying to make an effort to develop their capabilities to be used in any cyber-attack, or to take adequate preventive measures to protect them from any possible cyberattacks, especially in light of the impact of these attacks on vital places and institutions such as banks and ministries or on important facilities such as water and electricity utilities and other various services that negatively and directly affect citizens ... International cooperation with law enforcement authorities, and that each State Party should take measures by exchanging and providing useful information to the competent authorities for the purposes of investigation and criminal evidence in cyber cases, and in light of the continuous development of the phenomenon of cybercrime, international police agencies should exchange information and knowledge in order to take real-time, information-based action on the collection of digital forensics and the security and protection of the infrastructure. Critical electronic infrastructure from electronic penetration and protection from cyber-attacks for important and vital facilities, especially denial of service (DoS) attacks, which is one of the most important recommendations drawn from the study.

Keywords:

cyber threats - cyberspace - security.

مُقدمة:

نعيش اليوم العصر الرقمي، بفضل الثورة الهائلة في تكنولوجيا المعلومات والاتصال، فزيادة التشابك في جميع المجالات أدى إلى خلق بيئة جديدة للتفاعل بين الأفراد والمجتمعات والدول، وهو ما اصطلح عليه بالفضاء السيبراني، هذا الفضاء الذي يتميز بالتطور السريع، والغموض الشديد، وقد خلق الاستخدام السيئ لهذا الفضاء بيئة مليئة بالمخاطر والتهديدات، شكلت تهديدا خطيرا للأمن القومي للدول حيث تغيرت مفاهيم القوة والصراع والحرب، وارتبطت طبيعتها بالفضاء السيبراني.

وانطلاقًا من الأهمية التي بات ينطوي عليها المجال التكنولوجي في الحياة اليومية للمواطنين، فإن الأمن السيبراني أضحى اليوم ذا أهمية غير قابلة للتفاوض بشأنها، سواء كان ذلك للأفراد أو للشركات والحكومات، وحقيقة الأمر، فإن ما شهده عام 2022 من تزايد في الهجمات والتهديدات السيبرانية لم يكن من حيث الحجم والنطاق فقط، ولكنه من حيث التطور الحادث في آليات وأدوات تلك الهجمات وحساسية وأهمية الوحدات المُستهدفة.

الأمر الذى أدى إلى وضع الأمن السيبراني كركيزة أساسية في بناء الأمن القومي، سارعت الدول لتشكيل الهيئات والمؤسسات المدنية والعسكرية، وسن التشريعات القانونية ووضع استراتيجيات خاصة لمواجهة التهديدات والمخاطر السيبرانية الحالية والمُستقبلية، بهدف الدفاع عن أمنها، فضلاً عن العمل على المُستويين الإقليمي والدولي من أجل فضاء سيبراني آمن وسلمى.

ومع ازدياد الأخطار السيبرانية تعتمد المؤسسات يوميًا استراتيجيات لزيادة الاعتماد على تكنولوجيا المعلومات؛ منتجة حجمًا هائلاً من البيانات عن طريق خدمات الـ Cloud أو البنية التحتية الخاصة، وتدريجيًا تصبح هذه البنى التحتية عرضة للاختراقات المختلفة، لهذا ليس غريبًا أن تزداد المخاطر والتهديدات يومًا بعد يوم لا سيما مع زيادة عدد المُستخدمين مع عدم وجود برامج تدريبية أو توعوية تستهدف رفع الوعي بتلك المخاطر الناجمة عن تزايد الاعتماد على التكنولوجيا دون استعداد.

وفي مُواجهة موجات قد لا تنتهي من الهجمات والتهديدات السيبرانية التي تستهدف الأجهزة الذكية المُتصلة بالإنترنت، وفي مُقدمتها أجهزة وشبكات الحاسبات وما تحتويه من برمجيات وبيانات وما تقدمه من خدمات، جاء حرب المعلومات بين الدول لتستخدم الفضاء الإلكتروني كساتر لها[1]().

ويتضح مما سبق؛ أنَّ الفضاء السيبراني أصبح ميدان المعركة الرئيسي لهذه الجيوش السيبرانية، ولكنه ليس الميدان الوحيد، فكما تقاتل القوات المسلحة في الميادين الأربعة التقليدي "الأرض، والجو، والبحر، والفضاء الخارجي"، فإن الجيوش السيبرانية تقاتل في جميع هذه الميادين مشتركة، إلى جانب قتالها – أيضًا- في الميدان الخامس الافتراضي وهو الفضاء السيبراني.

الأمر الذى يستلزم أن يكون السلاح المُناسب لتحقيق الردع وحفظ الأمن يجب أن يكون من مُشتقات عصره؛ حتى يكون فعالاً ومُناسبًا، فالسلاح هنا يجب أن يكون سيبرانيًا وذكيًا، يختلف عن الأسلحة التقليدية الأُخرى، فمثلاً حينما كان المجتمع البشري زراعيًا كانت الْحِرَاب والرماح والسيوف، وجميعها أسلحة من موارد الأرض مباشرة وبتدخل طفيف من الإنسان عليها، وحينما فرض الإنسان مزيدًا من السيطرة على الطبيعة وأصبح المُجتمع صناعيًا استطاع تطوير الدبابات والطائرات وغيرها من الأسلحة، وحينما يصبح المجتمع "ذكيًا" فإن السلاح يجب أن يتوافق والعصر.

([1]) عمار ياسر البابلي: "الفضاء الإلكتروني التحديات الأمنية المعاصرة"، دراسات استراتيجية ومستقبلية، معهد البحوث والدراسات العربية، جامعة الدول العربية، 2020، ص11.

الجديد، وإلا فلن يكون فعالاً في حفظ أمن الدولة وأهدافها ، كشــف ذلك كله عن أهمية البحث عن التعامل مع هذا التحول على نحو مُؤسسي وقانوني وتقني.

(أولاً) . أهمية البحث:

تتوقف أهمية البحث على أهمية الظاهرة التي يتم دِرَاســتها، وعلى قِيمتها العلمية وما يمكن أنَّ تُحققه من نتائج يمكن الاستفادة منها، وما يمكن أنَّ تخرج به من حقائق يمكن الاستناد إليها، ومن ثم تتمثل أهمية هذا البحث **في الآتي**:

- تحظى دراسة موضوع آليات الحد من المخاطر والتهديدات السيبرانية بأهمية بالغة، حيث تنبع أهمية هذه الدراســة من أنها تتطرق إلى موضــوع على جانب كبير من الأهمية، وهو اســتغلال الفضاء الإلكتروني للقيام بالأعمال الإجرامية التي تهدد بدورها الأجهزة الحرجة والحساسة للدول.
- كما تكمن أهمية الدراسة في كون الفضاء السيبراني أصبح من الأهمية بمكان الوقوف على عمليات تأمينه ضد عمليات الاختراق والتجسس الأمر الذي يهدد الأمن القومي للبلاد.
- إلقاء الضوء على التحديات السيبرانية التي تواجه الدول نظرًا لأن الجرائم السيبرانية تعتبر جرائم ذات طبيعة خاصــة، والوقوف على مدى قدرة التشريعات الجزائية على مواجهة هذه الجرائم وكيفية التصدي لها.

(ثانيًا) . أهداف البحث:

هناك مجموعة من الأهداف تسعى مجموعة البحث لتحقيقها من هذه الدراسة، تتمثل في الآتي:

1) تسليط الضوء على ماهية الأمن السيبرانى والفضاء الإلكتروني.
2) الوقوف على الهجوم والأخطار السيبرانية والتسارع المحموم بين الدول.
3) بيان مضمون الحرب السيبرانية للسيبرانية.
4) إبراز مدى تأمين البنية التحتية الإلكترونية.
5) أهمية الأمن السيبراني في تأمين البنية التحتية المعلوماتية الحرجة
6) إلقاء الضوء على التطور الحادث الإرهاب والتطرف في الفضاء الرقمي

(ثالثًا) . مُشكلة البحث:

تتلخص مشكلة البحث في أن الجرائم السيبرانية المستحدثة تُمثل تحديًا أمنيًا وتشريعيًا وقضائيًا لأى مُجتمع بســبب المخاطر والتهديدات الناتجة عن هذه الجرائم، فالتهديدات لم تعد تعتمد على قوة الســلاح فقط، بل ظهرت وســائل إجرامية ســيبرانية حديثة تعتمد على التقنيات الجديدة، فالمعطيات القديمة لم تســتمر على حالها، إذ ما لبث العالم أن تحول إلى قرية صــغيرة بفعل ســهولة الاتصــالات التي قادتها ثورة التكنولوجيا المعلوماتية الحديثة، الأمر الذى يســتلزم الوقوف على كيفية المواجهة التشــريعية والأمنية لهذه الأخطار والتهديدات الســيبرانية التي تهدف الإضرار بالأمن القومي للدول وتهديد التحتية الإلكترونية للدول

(رابعاً) . تساؤلات البحث:

1. ماهية الأمن السيبراني ؟

2. ماهية الهجوم السيبراني والتسارع المحموم بين الدول؟
3. ما هي الآليات التشريعية والاتفاقيات الدولية التي تهدف إلى أمن السيبراني؟
4. ما أهمية الأمن السيبراني في تأمين البنية التحتية المعلوماتية الحرجة؟
5. ما هي أهم التحديات والأخطار السيبرانية؟
6. ما مدى أهمية آليات تحقيق الأمن السيبراني؟

(خامساً). خطة البحث:

يقسم البحث إلى مبحثين يسبقهما **مقدمة**، سنتناول في **المبحث الأول:** ماهية الأمن السيبراني والمخاطر السيبرانية وسنعرض في **المطلب الأول**: "مفهوم الأمن السيبراني"، وفي **المطلب الثاني**: "مفهوم المخاطر السيبرانية وصورها".

وسنتناول في **المبحث الثاني**: " الآليات الدولية والوطنية للحد من المخاطر والمهددات السيبرانية "؛ سنعرض في **المطلب الأول**: "الآليات الدولية لمُواجهة المخاطر السيبرانية في ظِل التشريعات المُقارنة"، وفي **المطلب الثاني**: "استراتيجيات الدول لحِماية أمنها من المخاطر والتهديدات السيبرانية".

المبحث الأول

ماهية الأمن السيبراني والمخاطر السيبرانية

تمهيد وتقسيم:

مما لاشك فيه أنه مع التقدُّم التقني الكبير المُعاصر في مجال المعلومات والاتصالات عبر الإنترنت، صار من السهل جدًّا توظيف المُجرمين والإرهابيين لهذه التقنيات المُتطوِّرة في وضع خططهم الإجرامية والإرهابية وتنفيذها والترويج لها، حتى غدت هذه الوسائل العصرية تحدِّيًا خطِرًا يُهدِّد المجتمع الدَّولي بأسره.

إن مُواجهة الأخطار والتهديدات السيبرانية تحتاج إيمانًا صادقًا وجهدًا دؤوبًا وشراكة مُجتمعية مُوسعة تشمل الجهات الحكومية والقطاع الخاص والمُؤسسات البحثية والتعليمية ومُنظمات الأعمال والمجتمع المدني لتعظيم الاستفادة من الفرص المُتميزة التي تتيحها تقنيات الاتصالات والمعلومات الحديثة في شتي مجالات التنمية الاقتصادية والاجتماعية والثقافية، مع حماية مُجتمعنا من مخاطر وأضرار الجرائم والهجمات السيبرانية، ومع الزيادة المُستمرة في جرائم الإنترنت أصبح تأمين الفضاء الإلكتروني ضد المخاطر السيبرانية عنصرًا أساسيًا في اسراتيجية إدارة المخاطر لدى الدول[1].

لذا، سوف نقسم هذا المبحث إلى مطلبين، وذلك على النحو التالي:

المطلب الأول: مفهوم الأمن السيبراني.

المطلب الثاني: مفهوم المخاطر السيبرانية وصورها.

المطلب الأول

---

(1) راجع فى ذلك؛

See website, Cyber Insurance, Retrieved on 14/3/2021, from

(2) https://www2.deloitte.com/us/en/insights/focus/humancapital-trends.htm

مفهوم الأمن السيبراني

بدايةً يود الباحث الوقوف على **تعريف الفضـاء الإلكتروني، وقد عرفته وزارة الدفاع الأمريكية "United States Department of Defense" بـأنـه:** "شـبكـة مُتوافقـة من البنى التحتيـة لتكنولوجيا المعلومات، بما في ذلك الإنترنت وشـبكات الاتصـالات وأنظمة الكمبيوتر والمعالجات ووحدات التحكم المضمنة، والمُحتوى الذي يتدفق عبر ومن خلال هذه المكونات، ويتم تقسيمها إلى ثلاث طبقات مُحددة: الشـبكة المادية، الشـبكة المنطقية، الطبقة الاجتماعية أو الشـخصـية الإلكترونية"[1].

أولاً. عناصر الأمن السيبراني :

كما **عرفت الوكالة الفرنسـية لأمن أنظمة الإعلام الفضـاء السـيبراني بأنه:** "فضـاء التواصـل المشكل من خلال الربط البيني العالمي لمُعدات المُعالجة الآلية للمعطيات الرقمية"، فهو بيئة تفاعلية حديثة، تشـمل عناصر مادية وغير مادية، مكوّن من مجموعة من الأجهزة الرقمية، وأنظمة الشـبكات والبرمجيات، والمُستخدمين سواء مُشغلين أو مُستعملين"[2].

أمَّا بالنسـبة **لتعريف الأمن السـيبراني،** عرفه البعض بأنه: "التقنيات والإجراءات التي تهدف إلى حماية أجهزة الكمبيوتر والشـبكات والبيانات من الدخول غير القانوني ونقاط الضـعف والهجمات المنقولة عبر الإنترنت من قِبل الجانحين السيبرانيين"[3].

وقد عرفه **فريق العمل المُشـترك المعني بتعليم الأمن السـيبراني في جامعة جورج واشـنطن،** أنه: "نظام قائم على الحوسـبة يشـمل التكنولوجيا والأشـخاص والمعلومات والعمليات المُؤكدة، ويشمل إنشاء وتشغيل وتحليل واختبار أنظمة الكمبيوتر الآمنة. إنها دورة دِرَاسة مُتعددة التخصصات، بما في ذلك الجوانب القانونية والسياسية والعوامل البشرية والأخلاق وإدارة المخاطر".

وعرفه **إدوارد أمورسو "Amoroso Edward"** بأنه: "وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسـوب أو الشـبكات، وتشـمل تلك الوسـائل الأدوات المُسـتخدمة في مُواجهة القرصنة وكشف الفيروسات ووقفها، وتوفير الاتصالات المُشفرة"[4].

يستخلص مما سبق من تعاريف؛ أنَّ الأمن السيبراني يتمثل في اتخاذ كافة التدابير اللازمة التقنية والقانونية لحماية كل ما هو موجود على السـايبر، وحتى لا يختلط على الباحثين في التفرقة بين الأمن السيبراني وأمن المعلومات فيجب أن يشمل تعريف الأمن السيبراني، الأمن الإلكتروني والأمن الرقمي، وبالتالي فنعرف الأمن السيبراني بأنه: "كل الإجراءات التي تتخذ لحماية الاتصالات والشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشـغيلية، ومكوناتها من برمجيات وأجهزة، وما تقدمه من خدمات، وما تحتويه من بيانات، سواء كانت حماية سابقة وقائية بواسطة وضع أنظمة حماية من المخاطر المحتملة أو حماية لاحقة من أي هجوم سيبراني أو اختراق أو تعطيل أو تعديل أو دخول أو

---

(3) Gioe, D. V., Goodman, M. S., & Wanless, A. Rebalancing cybersecurity imperatives: patching the social layer. Journal of Cyber Policy, 4(1), 2019. Pp.117-137.

(1) KEMPF Olivier, Introduction à la Cyber stratégie, Paris, 2021, p.19.

(2) K. K. Panigrahi, Information Security and Cyber Law, published by tutorials point ,2015, p.1.

(3) راجع في ذلك الموقع الإلكتروني الآتي؛ https://political-encyclopedia.org

استخدام أو استغلال غير مشروع ويشمل أيضًا المحافظة على البنى التحتية الحساسة للدولة من هجمات الروبوتات وغيرها وسواء ارتكبت الجريمة السيبرانية عن طريق الجهات الحكومية أو غير الحكومية". ويُنظم الإجراءات الخاصة بالأمن السيبراني وفقًا للقوانين واللوائح الوطنية للدولة.

وعلى ذلك؛ يمكن أن يتسع نطاق التعريف ليشمل: الاستراتيجيات والسياسات والمعايير المُتعلقة بأمن الفضاء الإلكتروني والعمليات فيه، ويشمل الأُطر الكفيلة بالحد من التهديدات السيبرانية، والحد من الضعف السيراني، وتطوير آليات الردع السيبراني، والمشاركة الدولية، والاستجابة للحوادث السيبرانية، والمرونة، وسياسات وأنظمة التعافي، بما في ذلك عمليات شبكة الكمبيوتر، وضمان المعلومات، وإنفاذ القانون، والدبلوماسية، والأنشطة العسكرية والاستخباراتية ذات الصلة من حيث صلتها بأمن واستقرار البنية التحتية العالمية للمعلومات والاتصالات[1].

وتجدر الإشارة إلى أنَّ الأمن السيبراني هو مُصطلح يستخدم لوصف قُدرات بلد أو مُنظمة أو شركة في الحماية من الهجمات الفيروسية؛ وبالتالي يجب أن تتضمن إدارة الهجمات السيبرانية عادةً الآتي[2]:

1- إزالة مصدر التهديدات.
2- مُعالجة نقاط الضعف في النظام.
3- تقليل التأثيرات من خِلال تخفيف الضرر واستعادة الوظائف.

يمكن تقييم وضع الأمن السيبراني للبلدان بناءً على تطورها في الركائز الخمس: (القانونية، والتقنية، والتنظيمية، وبناء القدرات، والتعاون)، بهدف حماية الأمن السيبراني[3].

ثانيًا. عناصر الأمن السيبراني[4]:

- **التقنية technology** تشكل التكنولوجيا والتقنية دورًا في غاية الأهمية في حياة الأفراد والمنظمات، حيث توفر الحماية الفائقة لهم أمام الهجمات السيبرانية، وتشتمل حماية الأجهزة بمُختلف أشكالها الذكية والحاسوبية والشبكات بالاعتماد على جدران الحماية واستخدام البرامج الضارة ومكافحة الفيروسات وغيرها.
- **الأشخاص People :** يستوجب الأمر لزومًا على الأشخاص من مستخدمي البيانات والأنظمة في منشأة ما استخدام مبادئ حماية البيانات الرئيسية كتحديد كلمة مرور قوية، وتفادى فتح الروابط الخارجية والمرفقات عبر البريد الإلكتروني، إلى جانب القيام بعمل نسخ احتياطية للبيانات.

(1) **Kaspersky. What is cybersecurity.2021. pp.1-5.** www.kaspersky.com/

(2) **Richardson, M. D., Lemoine, P. A., Stephens, W. E., & Waller, R. E. Planning for Cyber Security in Schools: The Human Factor. Educational Planning, 27(2), 2020.p.22.**

(3) **حنين جميل أبو حسين: "الإطار القانوني لخدمات الأمن السيبراني – دراسة مقارنة"، رسالة استكمالاً لمتطلبات الحصول على درجة الماجستير، كلية الحقوق، جامعة الشرق الأوسط، 2021، ص18.**

(4) **منى عبدالله السمحان: "متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود"، مجلة كلية التربية، جامعة المنصورة، العدد 111، يوليو 2020، ص ص 14، 15.**

- **الأنشـــطة والعمليات Process :** يتم توظيف الأشـــخاص والتقنيات للقيام بالعديد من العمليات والأنشطة وتسييرها بما يتماشى مع تطبيق أُسس الأمن السيبراني والتصدي لهجماته والتعامل مع التحديات الأمنية بكل كفاءة.

ثالثاً - الهدف من الأمن السيبراني:

- ضمان توافر استمرارية عمل نظم المعلومات والبيانات والأنظمة الذكية، مع تعزيز حماية وسرية وخصوصية البيانات والمعلومات الحكومية والشخصية، مع اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حدٍ سواء من المخاطر المحتملة في مجالات استخدام الإنترنت المختلفة وكذا الإنترنت العميق "Deep Web"

- تعزيز حماية أنظمة تقنية المعلومات والذكاء الاصطناعي وحماية مصالح الدولة الحيوية وأمنها الوطني، والبنية التحتية الحساسة فيها، مع تعزيز حماية أنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات، حماية الأنظمة التشغيلية من أي محاولات للولوج بشكل غير مسموح به لأهداف غير سليمة.

رابعًا. أبعاد الأمن السيبراني:

أصبح الفضاء الإلكتروني أحد العناصر الرئيسية التي تؤثر في النظام الدولي بما يحمل من أدوات تكنولوجيا تلعب دورًا مهمًا في عملية التعبئة والحشد في العالم، فسهولة استخدامها ورخص تكلفتها ساعدا على قيامها بأدوار مختلفة في الحياة البشرية، سواء اقتصادية أو معلوماتية أو سياسية، أو عسكرية أو أيدولوجية، ومن هنا قامت بعض دول العالم في السنوات الأخيرة بتطوير استخدام مهارات الإنترنت والحواسيب كأدوات هجوم ودفاع واستخبارات وحروب نفسية[1]، **ومن ثمَّ فهناك أبعاد للأمن السيبراني تتمثل في:**

(1) الأبعاد العسكرية: تنشأ أهمية الأمن السيبراني في هذا البُعد من خطورة الهجمات السيبرانية والاختراقات التي تؤدي إلى نشأة الحروب والصراعات المسلحة، واختراقات الأنظمة الحساسة، وما قد يحدث عنها من تهديدات لأمن الدول والحكومات، ومرد هذا وذاك أن جُزءً كبيرًا من الصراعات بين القوى العظمى في العالم، قد انتقلت من ميادين القتال الكلاسيكية إلى العالم السيبراني[2].

(2) الأبعاد السياسية: أصبح أمن الفضاء السيبراني من الأهمية بمكان حيث يُسهم فى تعزيز سيادة الدولة "**السيادة الرقمية**"، وبالتالي يُمثل بُعدًا سياسيًا للدول، كما نظرت مراكز فكر عالمية كمركز "بلفر" وكلية "هارفارد كيندى"، للأمن السيبراني باعتباره طاقة إلكترونية عالمية تتطلب وجود استراتيجية لتوطين الإنترنت وحماية المصالح التجارية والصناعية جنبًا إلى جنب مع حماية الأمن القومي والصحة الإلكترونية للمواطنين، ومُراجعة دور القوة الإلكترونية[3].

---

(1) أمانى عصام محمد: "استخدام روسيا للقوة السيبرانية في إدارة تفاعلاتها الدولية"، مجلة كلية التجارة وإدارة الأعمال، جامعة حلوان، المجلد الثاني والعشرون، العدد الرباع، أكتوبر 2021، ص171.

(2) عبدالغفار عفيفي الدويك: "الأزمات والحروب السيبرانية...تهديدات تتجاوز الفضاء الإلكتروني"، دراسة مركز صقر للدراسات، العراق، 15 فبراير 2019.

(3) JuliaVoo.et.al. National Cyber power index 2020–Methodology and analytical considerations. USA: HARVARD Kenedy School.2020.p.5–8.

(3) الأبعاد الاقتصادية: يرتبط الأمن السيبراني ارتباطًا وثيقًا بالحفاظ على الأنشطة الاقتصادية لكل الدول، فالترابط وثيق بين الاقتصاد والمعرفة فأغلب الدول تعتمد في تعزيز اقتصادها وازدهارها على إنتاج وتداول المعرفة والمعلومات على جميع المستويات، مما يبرر الدور الخطير للأمن السيبراني في حماية الاقتصاد[1].

(4) الأبعاد القانونية: ترتبط الأنشطة المختلفة التي يقوم بها الأفراد والمؤسسات بالقوانين، ومن ظهور المجتمع المعلوماتي ظهرت القوانين الجديدة التي تُعد البيئة التنظيمية التشريعية المنظمة لحماية هذا المُجتمع وحفظ الحقوق فيه بكافة ما يتضمن من أبعاد، ويقوم الأمن السيبراني في هذا البُعد على حماية المُجتمع المعلوماتي ويُساعده في تطبيق وتنفيذ هذه القوانين والتشريعات، ومن ثم فلابد من العمل على دعم أُطر التعاون الدولي على مُستوى التصدي للمخاطر السيبرانية[2].

خامساً - أهمية الأمن السيبراني في ظل التحول الرقمي:

يُعرف التحول الرقمي بأنه عملية انتقال القطاعات الحكومية أو الشركات إلى نموذج عمل يعتمد على التقنيات الرقمية في ابتكار المنتجات والخدمات، وتوفير قنوات جديدة من العائدات التي تزيد من قيمة منتجاتها ، و هو عملية انتقال تستخدم فيها التقنيات الرقمية في بناء العمليات التجارية الجديدة أو التعديل على نموذج الأعمال الموجود مسبقاً[3]، لتبسيط الإجراءات وتوفير سهولة الوصول تلبية للمتطلبات المتغيرة وتماشياً مع التكنولوجيا الحديثة والعالم الرقمي ، بدءً من الحضور على مواقع التواصل الاجتماعي واستخدام تطبيقات الهاتف الذكي والحوسبة السحابية، وصولاً إلى أمن المعلومات وتحليل البيانات والخوارزميات المتقدمة والواقع المعزز والذكاء الصناعي والطباعة الثلاثية الأبعاد ومنصات إنترنت الأشياء وغيرها .

وأدى التطور السريع وازدياد حجم المعلومات إلى تعقيد عملية التحكم والإفادة من التطبيقات التي انتشرت في شتى مجالات العمل وعلى جميع المستويات لتحقيق التقدم وأداء الأعمال بفعالية وكفاءة ولا يخفى ما رافق هذا التقدم من المجازفات سواء أكانت مخاطر أم فرص، وبالتزامن مع الانتشار الواسع للتقنية مفاهيم مجمعة مثل الحوكمة التقنية و حوكمة التحول الرقمي، و برزت هذه المصطلحات بصورة هامة وحيوية مترافقة مع استراتيجيات المؤسسات للتطوير و الحد من المخاطر و التلاعب.

ويري الباحث أن العلاقة بين الأمن السيبراني والأمن القومي تزداد كلما زاد نقل المحتوى المعلوماتي والعسكري والأمني والفكري والسياسي والاجتماعي والاقتصادي والخدمي والعلمي والبحثي إلى الفضاء السيبراني، خاصة مع تسارع الدول في تبني الحكومات الإلكترونية والمدن الذكية، واتساع نطاق وعدد مُستخدمي الإنترنت في العالم، مما أدى إلى أن تكون قواعد البيانات القومية في حالة انكشاف خارجي[4]، ويقدر الاتحاد الدولي للاتصالات أن حوالى 5,3 مليار شخص، (66% من سكان العالم)، يستخدمون الإنترنت في عام 2022.

---

(4) راجع في ذلك؛ سلسلة الكتل وآفاقها العالمية وفى مصر:

(5) Techopedia (2021). Blockchain Economy://www.techopedia.com/definitio

(1) تقرير صادر عن المنظمة العربية لتكنولوجيا الاتصالات والمعلومات، تونس، الجمهورية التونسية، 2021، ص30.

(2) انظر تقرير بعنوان: ماذا تعرف عن الثورة الصناعية الرابعة، المنشور بتاريخ 2018/7/1، على موقع العربية، نقلاً عن جريدة القافلة السعودية، على الرابط الإلكتروني:https://www.alarabiya.net/ar/qafilah/2018/07/01 /

(3) إيهاب خليفة: "القوة الإلكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الإنترنت"، دار العربي، 2017، ص5.

المطلب الثاني
مفهوم المخاطر السيبرانية وصورها

تتسم المخاطر والتهديدات السيبرانية بطابع سرية الهوية وألا تترك – الجرائم السيبرانية- سوى القليل من الأثر، إضافةً إلى أنها لا تقف أمام تلك المخاطر أي قيود إقليمية أو زمنية، ويمكن أن تسبب أضرارًا فورية لعدد لا يحصى- من الضحايا، وتتم عن طريق هجمات واختراقات وتسلل داخل النُظم المعلوماتية بغرض تدميرها أو الحصول على تلك المعلومات السرية عسكرية كانت أو اقتصادية[1]، والسؤال الذى يطرح نفسه أين تقف الدول من حيث النضوج السيبراني ومدى استعدادها لمُواجهة تزايدات التهديدات والمخاطر السيبرانية على الحكومات ودوائر الصناعة ومصالح الأعمال والمواطنين[2]. **ونعرض مفهوم المخاطر السيبرانية، وأهم صورها:**

(أولاً). مفهوم المخاطر السيبرانية:

هناك **تعريفات كثيرة ومُتعددة للمخاطر السيبرانية، ويمكننا أن نستخلص منها تعريفًا جامعًا بأنها**: "أي خطر لوقوع حادث إلكتروني ناشئ عن استخدام تكنولوجيا المعلومات والاتصالات الذي يضر بسرية البيانات، أو الخدمات، أو توفرها، أو سلامتها، أو إمكانية تتبعها، ويؤدي إلى ضعف التكنولوجيا التشغيلية في النهاية، وإلى اضطراب الأعمال، وانهيار البنية التحتية، وإلحاق أضرار مادية بالبشر والمُمتلكات".

كما عرفت الهيئة الوطنية السعودية للأمن السيبراني عام 2018 المخاطر السيبرانية بأنها: "المخاطر التي تمس أصول المُؤسسة وأفرادها وعملياتها والرؤية والرسالة والسمعة بسبب خلل في استخدام المعلومات أو بسبب الوصول غير المصرح لها بما يطال قيم المُجتمع ودينه وأخلاقه والبنى التحتية".[3]

ويتضح لنَّا من خلال ما سبق؛ أنَّ المخاطر السيبرانية تنشأ عن استخدام البيانات الإلكترونية ونقلها، بما في ذلك أدوات التكنولوجيا مثل: الإنترنت وشبكات الاتصالات، كما يشمل الضرر المادي الذي يمكن أن ينجم عن حوادث الأمن السيبراني، والاحتيال المُرتكب عن طريق إساءة استخدام البيانات، وأي مسؤولية تنشأ عن تخزين البيانات، وتوافر المعلومات الإلكترونية وسلامتها وسريتها – سواء كانت مُتعلقة بالأفراد، أو الجماعات، أو الحكومات.

(ثانيًا). أبرز المخاطر والتهديدات السيبرانية:

(1) الاختراقات السيبرانية:

وذلك عن طريق القرصنة والتي تقوم بدورها بنسخ البرمجيات غير المصرح به، أو إعادة إنتاجها، أو استخدامها أو تصنيع نسخ بطريقة غير مشروعة أو نشر أو توزيع المُنتج البرمجي أو استغلاله على

---

(1) وفاء لطفى: "الجهود الدولية في مجال مكافحة جرائم الإرهاب السيبرانى: التجربة الماليزية نموذجًا"، مجلة كلية الاقتصاد والإدارة، جامعة 6 أكتوبر، المجلد الثالث والعشرون، العدد الأول، يناير 2022، ص156.

(2) نظرة عامة على أدوات تقييم القدرات السيبرانية القائمة على الصعيد الوطني (GOAT)، المنتدى العالمي للخبرات السيبرانية (GFCE)، مرجع سابق.

(3) عمار ياسر البابلي، الآليات الحديثة لحماية وتأمين نظم المعلومات وأثارها على الأداء الأمني، رسالة دكتوراه، كلية الدراسات العليا، أكاديمية الشرطة، القاهرة، 2018، ص 235.

نحو مادي أو تقليدها أو مُحاكاتها والانتفاع بها على نحو يخل بحقوق الدول والمُؤسسات بدون الحصول على إذن أو تفويض[1]، ويمكن أن تتخذ الاختراقات السيبرانية إحدى الصور الآتية:

أ- اختراق المواقع والصفحات السيبرانية على الإنترنت وتدميرها، أو إلغائها، أو إتلافها، أو التعديل والعبث بالبيانات والمعلومات المُتوفرة عليها.

ب- شغل العنوان (الرابط) السيبراني للموقع أو تحويله لعنوان موقع آخر على الإنترنت.

ج- اختراق البيرد السيبراني للآخرين والاستيلاء عليه واستخدامه في انتحال شخصية الغير.

د- اختراق قواعد البيانات وحذف أو تعديل المعلومات الموجودة عليها، أو الاستيلاء على المعلومات المتوفرة عليها، كأسماء المُستخدمين وأرقامهم السرية وعناوين الاتصال الخاصة بهم واستخدامها لأغراض غير مشروعة أو بيعها إلى جهات مُستفيدة.

وتقوم القراصنة جراء الاختراقات بالتعبير عن المواقف السياسية، من خلال الهجمات على مواقع حكومية مثل جماعة "ويكيليكس، وأنونيموس"[2]، وتعد الفيروسات الخبيثة إحدى أدوات اختراقات الأمن السيبراني والتي تعتمد على ثغرات أمنية في برامج الحماية والأنظمة الأمنية، ومنها: فيروس "ستاكس نت عام 2010"، و"شمعون"[3]، و"حشرة الحب"، الفدية "Ransomware".

(2) التجسس السيبراني:

فعلى الرغم من تناول القوانين المُقارنة التجسس بصورة إلكترونية، إلا أنه لا يوجد تعريف موحد، فقد أطلق القانون الفرنسيـ لفظ كل فعل تسليم أو إتاحة الحصول إلى أي قوة أجنبية.. على مُعطيات رقمية إلكترونية..إلخ[4]، أو لفظ الدخول أو البقاء غير المشروع[5]، أو الالتقاط أو التنصت ..إلخ[6]. أمَّا النظام السعودي على التجسس لفظ التنصت أو الالتقاط أو الاعتراض أو الدخول غير المشروع للنظام المعلوماتي[7]، وبالنسبة للقانون الإماراتي أطلق لفظ الدخول دون تصريح أو بتجاوز التصريح، كذلك لفظ الاعتراض أو الالتقاط..إلخ[8].

وعلى ذلك؛ تُعد هذه الجريمة من أخطر الجرائم السيبرانية، وتهدف إلى تعطيل عمل الشبكات العنكبوتية وحواسيبها، وأنظمتها بهدف سرقة معلومات سرية سياسية، أو عسكرية أو مالية من دولة

---

(1) خالد مصطفى فهمى: "الحماية القانونية لبرامج الحاسب الآلى فى ضوء قانون حماية الملكية الفكرية طبقًا لأحدث التعديلات – دِرَاسة مُقارنة"، 2005، بدون ناشر، ص210.

(2) مجموعة دولية من نشطاء القراصنة، بدأت عام 2003 تطلق هجمات إلكترونية ضد الحكومات والمُؤسسات والأشخاص، نقلاً عن؛ خالد ظاهر عبدالله: "دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي"، مجلة البحوث الفقهية والقانونية، كلية سعد العبدالله للعلوم الأمنية، الكويت، العدد الثامن والثلاثون، إصدار يوليو 2022، ص410.

(3) راجع في ذلك الموقع الإلكتروني الآتي: http://www.masralarabia

(4) المادة (411) من قانون العقوبات الفرنسي بشأن الجرائم ضد الأمة رقم 913-93 لعام 1993.

(5) الفقرة (1 من المادة 323) من قانون العقوبات الفرنسي الجديد لعام 1992 المعدل.

(6) الفقرة (1 من المادة 226) من قانون العقوبات الفرنسي الجديد لعام 1992 المعدل.

(7) المادة (3) والمادة (7) من النظام السعودي لمكافحة الجريمة المعلوماتية.

(8) المواد (2، 4، 12، 15، 21، 22) من مرسوم رقم (5) لعام 2012 بشأن مكافحة جرائم تقنية المعلومات الإماراتى.

ونقلها إلى دولة أُخرى، وهو من الأســـاليب التي تلجأ إليها التنظيمات الإجرامية والإرهابية لجمع معلومات حول المُؤسسات والقطاعات الحكومية، والعسكرية، والسياسية، والاقتصادية[1].

(3) الإرهاب السيبراني:

عرفه "جيمس لويس "James Lewiss" بأنه: "استخدام أدوات شبكات الحاسوب في تدمير أو تعطيل البنى التحتية الوطنية المهمة، مثل: الطاقة والنقل، أو بهدف ترهيب الحكومة والمدنيين"[2].

وقد **ذهب مركز حماية البنية التحتية الوطنية الأمريكية (NIPC) إلى أنه:** "فعل إجرامي يمارس بواسطة الحاسوب، أو أدواته، فيفضي إلى نشر العنف، والموت، مع إثارة الهلع"[3]، وهذا يعني أنهم يســـتخدمون تكتيكات التعدي في مجال الاحتجاج في العالم الحقيقي بالوســـائل والأدوات الحديثة[4].

ويري الباحث أنَّ الإرهاب السـيبراني لا يكاد يختلف في مضـمونه وجوهره عن الإرهاب بصـورة عامة، من حيث القصـد الإجرامي للجاني، ما خلا طريقة تنفيذ هذا الفعل أو العمل الإرهابي، فالإرهاب التقليدي يكون عن طريق استعمال العنف والقوة الفعلية ممثلة بالأسلحة النارية والمُتفجرات وغيرها من صور الأعمال الإرهابية الأُخرى، أمَّا الإرهاب السيبراني فيكون عن طريق استخدام شبكة الإنترنت للوصـول إلى الأهداف التي يسـعى إليها الإرهابي لتجنيد واسـتقطاب الأشـخاص، لا سـيما الشـباب، للالتحاق مع العناصر الإرهابية أو نشر الدعاية لتلك الجماعات المُسـلحة، أو التعرض للحكومات، أو تحريض الأشخاص على القيام بعمليات مُسلحة ضد الدولة، أو ضد جماعات مُعينة.

وفي السـياق ذاته؛ كشـف **تقرير المُنتدى الاقتصـادي العالمي**[5] عن مخاطر عميقة للهجوم الإرهابي السيبراني؛ إذ له صلة وثيقة بانهيار البِنية التحتية للمعلومات المُهمَّة، وخطر إطلاق أسلحة الدمار الشـامل، لا سـيَّما أننا نعيش اليوم في عالم مُترابط إلى حدٍ كبير ومتَّصـل الأجزاء، تجري فيه (رقمنة) المزيد من البِنى التحتية الحيوية للبيانات، ومن ثم يزداد الاعتماد عليها باطِّراد، ومن ثم أصـبح الإرهاب السـيبراني في ازدياد مطَّرد؛ نظرًا لسـهولة اسـتخدامه، وإمكانية تحمُّل كلفته، ولا يتطلب من الإرهابيين الحصول على أسلحة تقليدية باهظة الثمن، ولا نقلها إلى الموقع المراد، كما لا تثْني قيود الزمان والمكان الإرهابيين عن بطشهم؛ إذ يمكنهم شنُّ الهجمات في الواقع الافتراضي من أي مكان، وفي أي وقت، إضـافةً إلى سـهولة إمكانية الاختباء والتخفِّي عن رجال إنفاذ القانون وراء حجاب التقنية.

---

(1) ممدوح عبدالحميد عبدالمطلب: "جرائم اســـتخدام شـــبكة المعلومات – الجريمة عبر الإنترنت"، بحث مُقدم لمُؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات، 2000، ص20.

(2) انظر فى ذلك أيضًـا؛ ضـرغام جابر عطوش: "جريمة التجسـس المعلوماتى – دِرَاسـة مُقارنة"، المركز العربي للنشـر والتوزيع، مكتبة دار السلام القانونية، ط1، 2017، ص91.

(3) نقلاً عن، ريهام عبدالرحمن: "أثر الإرهاب الإلكتروني على تغير مفهوم القوة والعلاقات الدولية– دراســـة حالة: تنظيم الدولة الإسلامية"، بحث منشور على الرابط الإلكتروني الآتي: https://democraticac.de/?p=34528

(4) حسن مظفر: "الفضاء المعلوماتي"، ط1، مركز دراسات الوحدة العربية، بيروت، 2017، ص214.

(4) Keiran Hardy, George Williams, "What is Cyber Terrorism? Computer and Internet Technology in Legal Definition of Terrorism," Cyber terrorism (U.K: Springer, 2014), p.2.

(6) تقرير المنتدى الاقتصادي العالمي السنوي 2021-2022. https://www.weforum.org/reports/

(4) الهجمات الاستراتيجية والعسكرية السيبرانية:

تصمم بعض الهجمات "Attacks Integrity" لتحقيق ميزة تكتيكية أو استراتيجية عن طريق تخريب نظم معلومات الخصم المدنية أو العسكرية الهامة، فيمكن أن ينطوي التخريب على التلاعب بالبيانات داخل نظم المعلومات التي يمكن أن تشوه وعي العدو عن طريق نشر معلومات خاطئة داخل أنظمة ذكائه، أو إخفاء أنشطة محددة قد تكون تحت المراقبة[1].

كما أنَّ هناك هجمات "Attacks Availability" تسعى لإغلاق نظم المعلومات تكمن خطورة الهجمات طويلة المدى منها في ما تسببه من أضرار مدمرة على الاقتصاد، بتأثيرها على شبكة الاتصالات أو الكهرباء على سبيل المثال. أما الهجمات قصيرة المدى التي تستهدف جمع المعلومات الاستخبارية، فيمكن أن تحجب قدرة الدولة على رؤية التهديد السيبراني التقليدي أو واسع النطاق من خلال منع المدافعين العسكريين من الوصول إلى البيانات أو المصادر الاستخباراتية الحيوية وهكذا، يمكن أن تشكل تلك التهديدات خطرًا على الأمن القومي[2].

(5) الحرب السيبرانية:

ويقصد بالحرب السيبرانية: "استخدام تكنولوجيا المعلومات والاتصالات في إدارة الحرب باستخدام الإنترنت"[3]، كما تعرف بأنها: "امتداد للسياسة من خِلال الإجراءات المُتخذة في الفضاء السيبراني من قِبل جهات حكومية أو غير حكومية تُشكل تهديدًا خطيرًا لأمن الدولة أو تجرى ردًا على تهديد مُتصور ضد أمن الدولة"[4].

وعلى ذلك؛ فإن الدول أصبحت تخصص موارد مُحددة لمواجهة الحرب السيبرانية ذلك بناءً على وجهات نظر استراتيجية وتكتيكية وتشغيلية، وتشمل الحرب السيبرانية الآتي:

- قُدرات هجومية سيبرانية لبدء هجمات سيبرانية، وآليات ردع بما فى ذلك سياسات وأسلحة وقُدرات وتحالفات، واستراتيجيات وأدوات لهجوم سيبراني مضاد.
- أساليب دفاع سيبرانية وقُدرات وتدابير مضادة في النظام لتكوين قادرة على حماية المصالح والبنى التحتية للحد من آثار الحرب السيبرانية والتعافي منها.
- وحدات الإنترنت، المحاربون السيبرانيون، المنظمات والكفاءات، الهجوم والعمليات الدفاعية، إذ يمكن أن يكون الهدف الرئيسي للحرب السيبرانية هو تشوية عمليات المرافق العسكرية والصناعية والاقتصادية والإدارية الرئيسية[5].

---

(1) **Wilner, Alex S., Deterring the Undeterrable: Coercion, Denial, and Delegitimization in Counterterrorism, Journal of Strategic Studies, Vol. 34, No. 1, February 2011, pp. 3–37.**

(2) www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons-cyberstrategy-one-year-later

(3) **Dmitri Alperovitch, Towards Establishment of Cyberspace Deterrence Strategy, In: Cyber Conflict ICCC, 2011 3rd International Conference, Tallinn, Estonia, June 2011, pp. 89- 90**

(4) **Steve Winterfeld and Anderess, the Basics of Cyber Warfare, Understanding the Fundamentals of Cyber Warfare, published by Elsevier, USA, 2013, p17.**

(5) **Paulo shakariam and others, interoduction to cyber-warfare, A Multidisciplinary Approach, pubished by Elsevier, Waltham. USA, 2013, p2.**

(1) **Solange Ghernaoyti, Cyber power Crime, Conflict and security in cyberspace, pubished by Epft press, Switzerland, 2013, p156.**

- استراتيجيات وعمليات الاستغلال السيبراني من أجل أن تكون قادرة على تحديد الفرص السيبرانية والاستفادة منها لتحقيق أهداف مُحددة، وجمع المعلومات الاستخبارية وتحليلها بهدف التنبؤ ومنع الصراعات السيبرانية[1]، ولغرض الحصول على معرفة منظمة عن العدو، وأن تكون على استعداد للرد بسرعة وكفاءة على الهجمات السيبرانية، إذ يعتمد جمع المعلومات الاستخبارية على الأساليب والتقنيات المُتعلقة بأنشطة سرية وتجسس وأنشطة مراقبة من خلال الاستفادة من المصادر المفتوحة على الإنترنت على وجه التحديد عندما تستخدم بالتزامن مع عمليات استخبارات مُحددة على الإنترنت يمكن أن تُساعد على فهم بيئة التهديدات السيبرانية[2].

وبناءً على ما سبق؛ فإن استخدام تكنولوجيا المعلومات والاتصالات قد تغيرت عن طريق تحويل التركيز على تدمير إمكانية العدو للقتال، إلى تقويض عزيمة الشعب، أو شلل العدو من خلال عمليات الشبكة أو الحاسوب تتم عبر شبكات الاتصالات ونُظم المعلومات، وبشكل عام يشمل المصطلح الحرب السيبرانية "الهجمات السيبرانية" واستغلال شبكة الإنترنت، والدفاع عن الفضاء السيبراني، "الدفاع السيبراني"[3].

(6) التهديدات السيبرانية والقصف السيبراني:

تتعدد أساليب التهديد عبر الإنترنت من التهديد بالقتل لشخصيات سياسية، إلى التهديد بتفجيرات في مراكز سياسية أو تجمعات، ثم التهديد بإطلاق فيروسات لإتلاف الأنظمة المعلوماتية في العالم[4].

ويمثل القصف السيبراني هجومًا على شبكة المعلومات عن طريق توجيه مئات الآلاف من الرسائل الإلكترونية إلى مواقع هذه الشبكات الأمر الذي يؤدي إلى ضعف قدرتها على استقبال رسائل من المُتعاملين معها، وبالتالي وقف عمل الشركة، مثال: لمواقع تعرضت للقصف السيبراني "موقع شركة "أمازون" لبيع الكتب على الإنترنت، وشركة "سي أن أن" للأخبار على الإنترنت مما أدى إلى بطء تدفق المعلومات لمدة ساعتين[5].

والجدير بالذكر أنه؛ تُشير **بعض الدِرَاسات**[6] والاحصائيات إلى أنه كان هناك زيادة كبيرة في الهجمات الإلكترونية عام 2020 وما بعدها، ويتضمن مقياس مخاطر (ALLianz)، تقرير المخاطر العالمية، سنة 2020 وسنة 2021 الكثير من الدِرَاسات والاحصاءات التي تدل على الزيادة الكبيرة في الهجمات الإلكترونية، **ومنها الاحصائيات التالية:**

---

(2) محمد بكرارشوش: "استعدادات الجزائر لمقتضيات حروب الجيل الرابع بين الواقع والآفاق"، دفاتر السياسة والقانون، الجزائر، المجلد 13، العدد 3، 2021، ص426.

(3) عمر عباس خضير: "مكافحة الجرائم السيبرانية كآلية لتعزيز الأمن الإقليمي"، مركز الدراسات العربية للنشر والتوزيع، ط1، مصر، 2021، ص42.

(4) كاميران عزيز حسن: "الجهود الدولية فى مُواجهة الجرائم السيبرانية"، رسالة ماجستير، كلية القانون والعلوم السياسية، الجامعة العراقية، العراق، 2019، ص79.

(5) حسنين المحمدي بوادي: "إرهاب الإنترنت الخطر القادم"، ط1، دار الفكر الجامعي، الإسكندرية، 2006، ص86.

(6) إسراء طارق الجابري: "جريمة الإرهاب الإلكتروني – دِرَاسة مُقارنة"، رسالة ماجستير، كلية الحقوق، جامعة النهرين، العراق، 2021، ص61.

(1) "نظرة عامة على أدوات تقييم القدرات السيبرانية القائمة على الصعيد الوطني (GOAT)، مرجع سابق.

- صـــدر في الولايات المُتحدة الأمريكية في أبريل 2020؛ تقرير صـــادر عن مكتب التحقيقات الفيدرالي الأمريكي يشـير إلى زيادة بنسـبة 300% في التهديدات والمخاطر السـيبرانية والهجمات الإلكترونية.
- أصـــدرت وكالة يوروبول هي وكالة تطبيق القانون الأوروبية تقريرًا ذكرت فيه أن هجمات برامج الفدية وسرقة البيانات الشـخصـية بين يناير ويونيو سـنة 2020 بلغت 100,001 من الجرائم الإلكترونية، وبذلك فقد زادت هذه الحوادث السيبرانية بأكثر من الثلث مُنذ بداية سنة 2020.
- صـــدرت في المملكة المُتحدة تقارير تشـــير إلى زيادة بنســـبة 400% في مُحاولات الهجمات الإلكترونية في قطاع الطاقة البحرية مُنذ مايو 2020.

تتنوع التهديدات والمخاطر السيبرانية المُرتبطة بالبيانات وتكنولوجيا المعلومات، ومُؤخرًا ومع الزيادة المُستمرة في جرائم الإنترنت أصبح التأمين الإلكتروني ضد المخاطر السيبرانية عنصرًا أساسيًا في اسراتيجية إدارة المخاطر لدى أي مُنظمة[1].

(ثالثًا) . التهديدات السيبرانية المرتبطة بجائحة (COVID-19):

لقد اســـتغل المُجرمون جائحة كورونا[2] لشـــن الاعتداءات الســـيبرانية من خِلال البرمجيات الخبيثة المعروفة. كانت قد اختفت نسبيًا إلا أنه مع ظهور الجائحة اتخذت أشكالاً جديدة في الظهور، **وأبرز تلك التهديدات يتمثل فى الآتي**[3]:

(1)- الاحتيـال الإلكتروني وزيـادة مواقع التصـــيـد الاحتيـالي: حيـث قـاموا مُرتكبو الجرائم السـيبرانية بإنشـاء مواقع مزورة ذات صـلة بـــ COVID-19 تهدف إلى اسـتدراج الضـحايا لفتح ملفات مُرفقة خبيثة أو النقر على وصـــلات إلكترونية احتيالية من أجل انتحال الهوية أو النفاذ خلافًا للقانون إلى حســابات خاصــة، وهو ما أكدته شركة Trend Micro[4]، أن ما يقرب من مليون رســالة تطفلية مُوجهة مُنذ يناير 2020 كانت ذات صـــلة بكوفيد – 19، وبالتالي جمع المعلومات أو اختلاس ملايين الدولارات وتحويلها إلى حسابات غير مشروعة.

(2)- البرمجيات الخبيثة (برمجة انتزاع الفدية وهجمات تعطيل الخدمة DDoS): حيث قاموا مُرتكبو الجرائم السـيبرانية ببث برمجيات خبيثة مثل: برمجية انتزاع الفدية لتعطيل بنى تحتية ومُؤسسـات حيوية مثل المستشـفيات، بهدف منع البنى التحتية من الوصـول إلى البيانات الحساسـة أو تعطيل منظوماتها الكمبيوترية، مما يؤدي إلى تفاقم الأزمة.

(3)- البرمجيات الخبيثة بهدف جمع البيانات: وذلك مثل أحصـنة طروادة بهدف التسـلل عن بُعد، وبرمجيات سرقة المعلومات، والتجسـس، وأحصـنة طروادة المصرـفية، والتي تتغلغل بدورها في

---

(2) See website, Cyber Insurance, Retrieved on 14/3/2021, from https://www2.deloitte.com/us/en/insights/focus/humancapital-trends.htm

(3) **الجائحة هي: "أعلى درجات الخطورة في قوة انتشـار الفيروس، وذلك بانتشـاره في أكثر من منطقة جغرافية في العالم وليس في قارة أو إقليم". للمزيد انظر الموقع الإلكتروني الآتي:** https://www.droitetentreprise

(4) انظر فى ذلك؛ تقرير بعنوان: "التهديدات السـيبرانية المُرتبطة بكوفيد -19 فى العالم"، الصـادر عن منظمة الإنتربول، وذلك من خلال الموقع الرسمي الآتي: WWW.INTERPOL.INT

(5) هي؛ شركة يابانية مُتخصصة في مجال أمن تكنولوجيا المعلومات في مجالات: "الأمن السحابي، أمن المحتوى، أمن الهواتف المحمولة، أمن البيانات، أمن الخوادم، برامج مُكافحة الفيروسـات، التخزين الآمن للبيانات عبر الإنترنت"، حيث تم تأسـيسـها عام 1988 بكاليفورنيا، الولايات المُتحدة. راجع فى ذلك؛ الموقع الرسمي للشركة:

(6) https://www.trendmicro.com/en-us/business.html

المنظومة الكمبيوترية عن طريق المعلومات المُرتبطة بكوفيد -19 كطُعم لتعطيل الشـــبكات وسرقة البيانات واختلاس الأموال، وأيضًا زرع برمجيات "بوتنت" الخبيثة.

الأمر الذى دفع خُبراء الإنتربول المُختصـــين بمُكافحة الجريمة الســـيبرانية، بهدف مُكافحة التهديدات الســيبرانية التي تســتغل تفشي فيروس كورنا، وتم تعميم نشرات بنفسـجية لتنبيه البلدان الأعضاء إلى التهديدات السيبرانية الجديدة والشديدة الخطورة، فضلاً عن الإرشادات التقنية لتعظيم الحماية من تلك التهديدات السيبرانية.

المبحث الثاني
التشريعات والآليات الدولية والوطنية
للحد من المخاطر والمهددات السيبرانية

تمهيد وتقسيم:

يبذل المُجتمع الدولي جهودًا مُتزايدة لفهم أوضـاع الأمن السـيبراني من أجل الوقوف على نقاط الضـــعف واتخاذ قرارات تهدف إلى تعزيز القُدرات الســـيبرانية، وقد وضـــعت مُؤســـســـات البحوث والمُنظمات الإقليمية والشركات أُطرًا ونماذج وأرقامًا قياســـية، بهدف تطبيقها في جميع أنحاء العالم، مشـــيدةً قاعدة معرفية تبين أين تقف الدول من حيث الوعى بالأمن الســـيبراني، ومدىَ اســـتعدادها التشـــريعي والاســـتراتيجي لمُواجهة التهديدات الســـيبرانية على الحكومات، والمواطنين، ومجالات الصناعة[1] ، كما تحظى عمليات مُواجهة المخاطر السيبرانية في المُنظمات المُعاصرة بشكل عام وفي المجال الأمني بشـكلٍ خاص بأهمية كبيرة في الوقت الحاضر، وتُشـكل توجهًا إداريًا جديدًا؛ من أجل توفير الحِماية اللازمة للمُنظمات وضـمان اسـتمرارها لأداء نشـاطها بكفاءة عالية[2]، وتُعد المخاطر والتهديدات الســـيبرانية أكبر تحدٍ يواجه المُســـتخدمين الإلكترونيين، مما يســـتلزم أن يكون لكل دولة اسـتراتيجية شـاملة للتوعية بالسـلامة الإلكترونية لضـمان حصـول جميع مُسـتخدمي الإنترنت داخل بلدهم على الوعى والمعرفة والمهارات في الفضاء السيبرانية[3].

لذا، سوف نقسم هذا المبحث إلى مطلبين، وذلك على النحو التالي:

المطلب الأول: التشريعات المقارنة وآليات الحماية من المخاطر السيبرانية.

المطلـب الثـاني: اســـتراتيجيـات الـدول لحِمـايـة أمنهـا من المخـاطر والتهـديـدات السيبرانية.

---

(1) للمزيد انظر في ذلك؛ وثيقة المُنتدى العالمي للخبرات السيبرانية (GFCE)، ص4. من خلال الموقع الإلكتروني:

(2) https://globalcybersecurityforum.com/ar

(3) انظر أيضًا؛ محمد سـعيد إسـماعيل: "التأمين الإلكتروني ضـد المخاطر السـيبرانية: المشـكلات القانونية والحلول المُقترحة– دِرَاســـة في القانون القطري والمُقارن"، كلية القانون، جامعة قطر، المجلة الدولية للقانون، المجلد العاشـــر، العدد الثالث، 2021، ص206.

(4) تركي المخلفي: "درجـة تطبيق إدارة المخـاطر"، مجلـة القراءة والمعرفـة، كليـة التربيـة، جـامعـة عين شـــمس، العدد (207) يناير 2019، ص20.

(1) Kritzinger, E. Improving Cybersafety Maturity of South African Schools. Information, 11(10),2020, p4.

المطلب الأول

التشريعات المقارنة وآليات الحماية من المخاطر السيبرانية

(أولاً) . التشريع الدولية لحماية الأمن السيبراني:

(1) بالنسبة للتشريع الإماراتي:

يبدأ تنفيذ قانون مكافحة الشائعات والجرائم الإلكترونية، أول يناير (2022)، الذي يتماشى مع التطور الإلكتروني المتسارع في وسائل الاتصالات وما نجم عنها من اتساع نطاق استخدام الشبكة المعلوماتية، سواء في وسائل التواصل الاجتماعي أو تطبيقات برامج الأجهزة الذكية، بعد إساءة استخدام البعض تلك الوسائل نجم عنها انتشار ظاهرة الجرائم الإلكترونية، سواء ما يمس الوحدة الوطنية، أو الجرائم الماسة بالأشخاص، مثل جريمة الابتزاز والجرائم الواقعة تحت طائلة الأموال كجرائم الاحتيال الإلكتروني، الأمر الذي كشف عن الحاجة لتجريم بعض الأفعال غير المجرمة في السابق.. الحاجة لتشديد العقوبات على الأفعال المجرمة لتحقيق الردع.

بناءً على قانون ترويج الاشاعات المادة 197 مكرر 2، فإن كل من استعمل أي وسيلة من وسائل الاتصال وتقنية المعلومات في نشر معلومات وأخبار تعرّض أمن الدولة للخطر وتهدّد أو تمس النظام العام فيها، سيعاقب بالسجن المؤقت على جريمته.

وتكون العقوبة الحبس مدة لا تقل عن سنتين والغرامة التي لا تقل عن 200 ألف درهم إذا ترتب على أي من الأفعال المذكورة تأليب الرأي العام أو إثارته ضد إحدى سلطات الدولة أو مؤسساتها أو إذا ارتبط بزمن الأوبئة والأزمات والطوارئ أو الكوارث [1].

فإن هذا القانون يحقق خمسة أهداف مجتمعية وقانونية، تشمل الحد من العبث المنتشر على وسائل الاتصال الإلكتروني، وحماية المجتمع والمواقع والبيانات الحكومية من جرائم تقنية المعلومات، وحماية خصوصية الأشخاص وحياتهم الأسرية والخاصة، ومكافحة الشائعات وجرائم النصب والاحتيال عن طريق التواصل الإلكتروني، والحد من نطاق الاعتداء على الخصوصية باستخدام تقنية المعلومات سواء على الأشخاص أو الكيانات أو العائلات بدون رضاء وفي غير الأحوال المصرح بها وأن نشر الشائعات جريمة يعاقب عليها القانون بالحبس مدة لا تقل عن سنة، وفقاً للمادة 198 مكرر من قانون العقوبات الاتحادي[2].

(2) بالنسبة للتشريع الأمريكي:

في أكتوبر 2001، أصدرت الولايات المُتحدة الأمريكية قانون مُكافحة الجريمة المعلوماتية، كما أصدرت اتفاقية أمريكا لمُكافحة الجرائم الإلكترونية، عام 1999[3]، والتي توسعت من خلال سُلطات التحقيق والمراقبة الإلكترونية، كما أصدرت لجنة الكونغرس "على المُستوى الفيدرالي"، عام 1984 قانون الاحتيال وسوء استخدام الحاسوب "computer fraud and abase act"، وبموجب هذا القانون اعتبر الوصول إلى المعلومات الحكومية بدون رخصة من قِبل الجنايات، والوصول إلى القيود

---

(2) يوسف الشريف ، شرح قانون 34 لسنة 2021 ، جريدة الامارات اليوم ، نشر بتاريخ 25 يناير 2022 ومتاح علي https://www.emaratalyoum.com/local-section/other/2022-01-25-1.1590341

(1) تقرير صحيفة البيان الإماراتية بشأن جريمة عقوبة نشر الشائعات والأخبار الكاذبة ، نشر بتاريخ 11 فبراير 2022 https://www.albayan.ae/uae/news/1.4337512-02-01-2022

(2)

(3) عبدالحق باسو: "الإرهاب المعلوماتي في القانون المغربي والقانون الدولي"، أبحاث الدورة التدريبية "مُكافحة الجرائم الإرهابية المعلوماتية"، كلية التدريب، جامعة نايف العربية للعلوم الأمنية، الرياض، 2006، ص22.

المالية أو بيانات الائتمان في المُؤسسات المالية أو الوصول إلى الحاسبات الآلية الحكومية من قِبل الجنح، ويُمثل قانون الولايات المُتحدة، التشريع الرئيسي- لجرائم الكمبيوتر، ويشمل قانون الولايات المُتحدة الأمريكية في فصله (18)[1]، التشريع الرئيسي- لجرائم تقنية المعلومات الحديثة، فقد استجاب الكونغرس لمشكلة جرائم تقنية المعلومات من خلال سنّ العديد من القوانين الفيدرالية، كان أولها قانون الاحتيال وإساءة استخدام الكمبيوتر عام 1986، ومن ثم عُدل عام 1994 من أجل التعامل مع مشكلة الشيفرة الخبيثة وغيرها من البرامج التي تهدف إلى تغيير أو إتلاف أو تدمير البيانات على نظام الحاسوب[2]. وأورد بالقسم (1030)[3] من الفصل (18) أن هناك أفعال تعد من قبيل الجرائم:

- الدخول غير المصرح به إلى أي كمبيوتر.
- التوصل غير المصرح به "الدخول" إلى أحد أنظمة الحاسوب للحصول على معلومات أمنية وطنية مع وجود نية لضرر الولايات المُتحدة الأمريكية أو لمنفعة دولة أجنبية.
- التوصل غير المصرح به "الدخول" إلى نظام حاسوب خاص بالحكومة الفيدرالية الأمريكية.
- التوصل غير المصرح به "الدخول" إلى أحد أنظمة الحاسوب للحصول على معلومات خاصة بأموال محمية.
- بث أو تهديد بارتكاب ضرر لأي نظام حاسوب محمي عبر الولايات المُتحدة أو للتجارة الأجنبية بغرض ابتزاز أموال أو نافع من أي شخص طبيعي أو معنوي[4].

إن معظم الولايات المتحدة تتوفر لديها تشريعات تُحَظْر هجمات التدمير "الجرائم السيبرانية"، وتعتبرها أكثر خطورة من أنشطة الدخول غير المصرح به، فضلاً عن تجريم استخدام الحاسوب لتعطيل أو قطع أي خدمة أساسية ذات النفع العام، والتي تشمل كافة الخدمات الحكومية[5] وتعتبرها أنماطًا مُستجدة للظاهرة السيبرانية، وتحاول تقنين استخدام محرك البحث في مجموعة من شركات الاتصالات كـ (MSN) و (YAHOO) و (GOOGL)، وبالفعل فقد تسنى لها إلزام هذه الشركات بناءً على أوامر قضائية، بتحصين البيانات المتعلقة ببعض مُستخدمي هذه الشبكات، وذلك للاستعانة بها في الأبحاث التي تباشرها القطاعات الأمنية والقضائية في بعض الجرائم السيبرانية.

(3) بالنسبة للتشريع الفرنسي:

---

(4) **Susan. W. Brenner-state cybercrime legislation in the United States of America- Available at:** www.richmond.edu. **Hossein Bidgoli – the internet encyclopedia – volume –joun Wiley and sons 2004-p.326.**

(5) **Debra. Little jhon Shinder, Michal cross-scene of the cybercrime- published by syngress-seconded itiou 2008-p.663.**

(6) **Title 18 cection 1343 of the united states Federal code.**

(7) **Title 18 cection 1030 of the united states Federal code.**

(1) بخصوص الأنظمة الجرمية الواردة في القسم (1030) من الفصل (18) من قانون الولايات المتحدة.

(2) **Susan. W. Brenner-state cybercrime legislation in the United States of America- the Richmond Journal of Law and technology – volume6, issue3, winter 2001. P.6. Available:** www.Richmond.Edu.

ففي فرنسا، صدر المرسوم رقم (1012) لسنة 2011 في شأن الاتصالات الإلكترونية[1]، وجاء الباب الثالث منه بعنوان: "مكافحة التعدي على الخصوصية وأمن نُظم المعلومات في مجال الاتصالات الإلكترونية"؛ حيث تضمنت أحكامه جرائم انتهاك المواقع التي تقع بواسطة شبكات الاتصالات والمعلومات والعقوبات المقررة لها، والتي تصل إلى حد السجن لمدة خمس سنوات، والغرامة التي لا تجاوز فى مقدارها (300 ألف يورو). كما أضاف المشرع الفرنسي- إلى تقنين العقوبات أحكامًا تجرم سرية المراسلات، وتجرم انتحال شخصية الغير باستخدام بياناته، واستخدام المراسلات لأعمال إجرامية.

وقد عزز المشرع الفرنسي- قانون 23 كانون الثاني 2006 بشأن مُكافحة الإرهاب الاستجابة لمتطلبات الوقاية **وفق المتغيرات السريعة فى وسائل النقل وتقنيات الاتصالات**، وقد أسفرت هذه الجهود عن وضع استراتيجية طويلة الأجل[2]، كما تضمن تعديلات على قانون الإجراءات الجنائية نصت على مركزية محاكم تطبيق العقوبات بباريس – التي تشرف على تنفيذها- بشأن المحكوم عليهم في جرائم إرهابية، وإنشاء محاكم جنايات متخصصة للأحداث الإرهابية، (المادة 706-25)، كما استحدث هذا القانون نظامًا لتحسين تعويض ضحايا الأعمال الإرهابية[3].

(ثانياً)- استراتيجيات الدول لحماية أمنها من المخاطر والتهديدات السيبرانية :

فرضت بعض الدول استراتيجيات وفق آليات مُحددة لحماية أمن المعلومات والبيانات لديها، ومن أهمها دول الاتحاد الأُوروبي وفقًا لتعليمات اللائحة رقم 2016/679 للبرلمان الأوروبي والمجلس الأوروبي بتاريخ 27 أبريل 2016، بشأن حماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية وحرية نقل هذه البيانات[4]، حيث تضمن القسم الثاني التزامات أمن البيانات

Ordonnance no 2011-1012 eu 24 août 2011 relative aux communications électroniques.

(3) **La France face au terrorisme: Livre blanc du Gouvernement sur la sécurité intérieure face au terrorisme**

(4) **(texte imprimé) / France. Premier Ministre; France, Secrétaire. – Paris: La Documentation française, 2006. – 1**

(5) **vol. (141 p.); 24 cm.**

(6) **ISBN: 978 – 2 – 11 – 006101 – 0, Langues: Français (fre)**

(7) **(3)La loi no 2006 – 64 du 23 janvier 2006 relative a la lutte contre le terrorism, rev. sc crim 2006, no 2, p 366.**

(1) **REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.**

الشـخصـية، وألزم كل من المراقب[1]، والمُعالج[2]، ومن ثم ينبغي مُراعاة أحدث التطورات وتكاليف التنفيذ وطبيعة المُعالجة ونطاقها وسـياقها وأغراضـها، فضـلاً عن مخاطر تنوع الاحتمالات وشـدتها فيما يتعلق بحقوق وحريات الأشخاص الطبيعيين والمراقب والمعالج[3]،**ومن تلك الاستراتيجيات:**

(1)- استراتيجية دولة الإمارات العربية المتحدة:

تعزيز بيئة رقمية آمنة وموثوقة في دولة الإمارات، في ظل التطور التكنولوجي وتزايد التهديدات السيبرانية المواكبة له، بما في ذلك تهديدات نشطاء القرصنة الإلكترونية، ومجموعات الجرائم الإلكترونية المنظمة التي تمثل تهديداً على الأمن القومي، وأصول أمن المعلومات وبنيتها التحتية، أطلقت هيئة تنظيم الاتصالات والحكومة الرقمية، الدليل الإرشادي "نظام ضمان أمن المعلومات في دولة الإمارات" وذلك لتوفير مرجعية لمتطلبات رفع الحد الأدنى من مستوى حماية أصول أمن المعلومات، وأنظمة الدعم في جميع الجهات المعنية في الدولة.

تتخذ دولة الإمارات العديد من الإجراءات والتدابير والمبادرات لتعزيز أمنها السيبراني وتتضمن هذه الجهود التالي[4]:

- تنفيذ شبكة إلكترونية اتحادية (**FEDNET**) : نفذت دولة الإمارات ممثلة بهيئة تنظيم الاتصالات والحكومة الرقمية شبكة اتحادية معززة ببنية تحتية مشتركة (**FedNet**) تسمح بالتوصيل البيني، وتبادل البيانات بين جميع الجهات المحلية والاتحادية في الدولة، وتعزز قنوات التواصل فيما بينها باستخدام بنية تكنولوجية موحدة وآمنة .
- توفر الشبكة بيئة أمن متعددة الطبقات تضمن أعلى مستويات الأمان في البنية التحتية اعتماداً على الترميز متعدد البروتوكولات (**MPLS**)، وتتيح ربطاً آمناً بالإنترنت لكافة الجهات الحكومية الاتحادية عبر مزود مزدوج لخدمة الإنترنت، ما يسمح بتحقيق إنتاجية أعلى، كما توفر هذه الخدمة اتصالاً موحداً بالإنترنت في الجهات الاتحادية، مما يقلل إمكانية التعرض لهجمات الدخلاء عن طريق الحد من الثغرات.
- كرست دولة الإمارات فريق الاستجابة الوطني لطوارئ الحاسب الآلي (**aeCERT**)، الذي يهدف إلى تحسين معايير وممارسات أمن المعلومات، وحماية البنى التحتية لقطاع الاتصالات وتقنية المعلومات من مخاطر واختراقات الإنترنت.

---

(2) **(EU) 2016/679, controller: means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.**

(3) **–المراقب: يعني الشخص الطبيعي، أو الاعتباري، أو السلطة العامة، أو الوكالة، أو أي هيئة أخرى تحدد، بمفردها، أو بالاشتراك مع آخرين، أغراض ووسائل معالجة البيانات الشخصية؛ عندما يتم تحديد أغراض ووسائل مثل هذه المعالجة بموجب قانون الاتحاد، أو قانون الدول الأعضاء، يجوز توفير المراقب، أو المعايير المحددة لترشيحه بموجب قانون الاتحاد، أو قانون الدول الأعضاء.**

(4) **(EU) 2016/679, processor: means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.**

(5) **See, (EU) 2016/679, Article 32 Security of processing, General Data Protection Regulation (GDPR).**

(6) **السلامة السيبرانية والأمن الرقمي ، موقع حكومة دبي الذكية ، على الانترنت : https://u.ae/ar-ae/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security**

- **مبادرة سالم التوعوية** : لغرض توفير بيئة إلكترونية آمنة، لجميع مستخدمي الإنترنت، والجيل الصاعد على وجه الخصوص، أطلق مركز الاستجابة لطوارئ الحاسب الآلي (**aeCERT**) بالتنسيق مع برنامج خليفة لتمكين الطلاب (أقدر) موقع سالم للتوعية الإلكترونية ، يشكل الموقع المنصة الرسمية الوطنية الموحدة للتوعية الإلكترونية في دولة الإمارات الذي تجتمع عليه جميع الجهات المعنية على مستوى الدولة، لتحقيق أهدافها التوعوية الموجهة إلى الطلبة ، ويقوم "سالم" بإرشاد وتوجيه جميع مستخدمي الشبكة نحو ثقافة معلوماتية آمنة في دولة الإمارات، ويدعم الموقع الوعي الأمني من خلال الفيديوهات التثقيفية، والمواد، والرسائل التوعوية، والألعاب الهادفة ، ويهدف المركز إلى تعزيز قانون مكافحة جرائم تقنية المعلومات والمساعدة في استحداث قوانين جديدة حول أمن المعلومات، وبناء خبرات وطنية في مجال أمن المعلومات، وإدارة الطوارئ وتحري الأدلة في الحاسبات، وإنشاء مركز اتصال موثوق للإبلاغ عن جرائم تقنية المعلومات في الدولة، ومركز وطني لجمع المعلومات عن التهديدات والمخاطر وجرائم تقنية المعلومات[1]..
- مبادرة سايبر سي 3 (**3Cyber C**) : تهدف مبادرة سايبر سي 3 إلى تطوير المواطن الرقمي القادر على الحصول على فوائد المشاركة على شبكات الإنترنت، وامتلاك مهارة القراءة والكتابة الرقمية، والتفكير النقدي في قراءة وتحليل مصادر المعلومات وفهم العواقب الأخلاقية، واتخاذ القرار الأخلاقي الجيد لسلوكه على الإنترنت. تهدف المبادرة إلى حماية المستخدم من مخاطر الشبكة العنكبوتية، وتعزيز الثقافة الإلكترونية، والتوعية بالاستخدام الإيجابي للتكنولوجيا والإنترنت، وأساسيات أمن المعلومات.
- تطبيق الهوية الرقمية**UAE Pass app-** :تعد الهوية الرقيمة أول هوية وطنية رقمية لجميع المواطنين والمقيمين والزوار، وتسمح بوصول المستخدمين إلى خدمات الهيئات الحكومية المحلية والاتحادية، ومزودي الخدمات الآخرين. تقدم الهوية الرقمية أيضاً حلولاً سهلة للدخول إلى الخدمات عبر الهواتف الذكية دون الحاجة إلى كلمة سر أو اسم مستخدم، فضلاً عن إمكانية التوقيع على المستندات رقمياً، والتحقق من صحتها دون الحاجة لزيارة مراكز الخدمة.
- **مؤشر دبي للأمن الإلكتروني :** أطلق سمو الشيخ حمدان بن محمد بن راشد آل مكتوم، ولي عهد دبي رئيس المجلس التنفيذي مؤشر دبي للأمن الإلكتروني الأول من نوعه على مستوى العالم، والذي يدعم الأداء العام للأمن الإلكتروني في مختلف الجهات الحكومية على مستوى الإمارة، بما يرسخ مكانتها بوصفها المدينة الأكثر أمانا في الفضاء الإلكتروني[2].

يأتي إطلاق المؤشر في إطار مستهدفات استراتيجية دبي للأمن الإلكتروني لحماية إمارة دبي من مخاطر الفضاء الإلكتروني، ودعم الابتكار والنمو الاقتصادي للإمارة في ظل التقدم التكنولوجي والتحول الذكي الذي تشهده ، حيث يتيح المؤشر تعزيز المنافسة بين الجهات الحكومية في مجال الأمن الإلكتروني وتطوير مقدراتها وتقدمها في هذا المجال ،عمل على تطوير المؤشر، مركز دبي للأمن الإلكتروني في إطار مهامه المحددة بموجب قانون تأسيسه، والتي تشمل وضع وتنفيذ سياسة أمن المعلومات الحكومية في إمارة دبي والإشراف على تنفيذ المعايير لضمان تحقيق الأمن الإلكتروني في الإمارة، إلى جانب التأكد من فاعلية أنظمة أمن شبكة الاتصالات وأنظمة المعلومات لدى الجهات الحكومية، والإشراف على مدى التزام الجهات الحكومية بتنفيذ متطلبات أمن المعلومات الصادرة عن المركز ومتابعة تنفيذها.

---

(1) «العين السيبرانية».. مبادرة لتعزيز قدرات الأمن السيبراني لحكومة أبوظبي ، جريدة الخليج الرسمية ، على موقعها الرسمي على الانترنت ، بتاريخ 22 يناير 2022.

(1) الاستراتيجية الوطنية للأمن السيبراني ، هيئة تنظيم الاتصالات والحكومة الرقمية ، متاح على الموقع الإلكتروني

https://tdra.gov.ae/ar/national-cybersecurity-strategy

(2)- استراتيجية الولايات المتحدة الأمريكية السيبرانية والتكنولوجية:

- **حماية البنية التحتية الحرجة:** حيث تعتمد البنية التحتية الحرجة في الولايات المتحدة الأمريكية على النظم التكنولوجية والسيبرانية بصورة رئيسية بما في ذلك النظم الصحية، ونظم الاتصالات، والمواصلات، ومحطات الطاقة، والسدود، والمفاعلات النووية، والأقمار الصناعية.
- **الحفاظ على البيانات والمعلومات الاستراتيجية:** فقد أصبح العالم على وشك الانتقال نحو الجيل الخامس من الاتصالات اللاسلكية، فتلك الشبكات أصبحت الصين منافسًا قويًا فيها عبر شركاتها، مثل هواوي، ومن يقوم ببناء وتطوير هذه الشبكات يستطيع بطريقة أو بأخرى أن يسيطر على شريان المعلوماتي العالمي. الأمر الذي دفع الإدارة الأمريكية لإصدار تشريعات تمنع تعاون الشركات الأمريكية مع الشركات الصينية.
- **مواجهة مخاطر هجمات طلب الفدية:** ارتفعت هجمات برامج الفدية؛ والتي تستهدف تشفير البيانات في شبكات الأنظمة الصناعية للشركات وتطالب بدفع مبالغ مالية لإعادتها بنسبة 5%، بين عامي 2018 و 2020، ومن بين هذه الهجمات، شكلت الجهات المصنعة أكثر من ثلث الهجمات المؤكدة على المنشآت الصناعية، تليها المرافق الخدمية، والتي شكلت 10%، كما ارتفعت التكاليف المقدرة للهجمات إلى حدٍ كبير - حيث قفزت من 8 مليارات دولار أمريكي في عام 2018 إلى 11.5 مليار دولار أمريكي في عام 2019، ووصلت إلى 20 مليار دولار أمريكي في عام 2020؛ وقد أدى الاضطراب التشغيلي الناتج عن برامج الفديات في بيئات التقنيات التشغيلية إلى زيادة قدرها 23 ضعفًا، وفي عام 2020، كانت هناك زيادة بنسبة 32 بالمائة في هجمات برامج الفدية على مؤسسات الطاقة والمرافق[1].
- **صعوبة منع الهجمات السيبرانية:** تشير العديد من الدراسات إلى أنَّ قادة الأعمال والحكومات يدركون التهديدات السيبرانية في القطاع الصناعي، ولكنهم ليسوا مستعدين بعد لمواجهتها. غالبًا ما تكون الهجمات السيبرانية عابرة للقارات ويتعرض الجميع لها دون استثناء ويعد التهديد للشركات الصناعية قائمًا على مستوى العالم، ومع ذلك، بسبب
- العوامل الجيوسياسية وتركّز النشاط الصناعي في بعض البلدان؛ فإنَّ التهديدات تكون أكثر حدة فيها دونًا عن غيرها[2].

<u>وشملت الاستراتيجية التكنولوجية السيبرانية الأمريكية العناصر الآتية:</u>

1- **الحد من مخاطر الأمن القومي التي تسببها التهديدات السيبرانية:** وذلك لما تسببه من أضرار جسيمة للأمن القومي.

2- ضمان الريادة الأمريكية في ظل المنافسة التكنولوجية الشرسة: هو ما يضمن بقاء الولايات المتحدة على قمة هرم الابتكار التكنولوجي.

---

(1) Cybersecurity Magazine, Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031 (2021); 2021 Ransomware Statistics, Data & Trends, PurpleSec (2021)p1.

(2) حسين الشدوخي: "الدفاع السيبراني في القطاع الصناعي"، تقرير بشأن تقييم ثغرات الأمن السيبراني والاستعداد لمواجهتها في قطاع الطاقة والموارد الطبيعية، أكتوبر 2021، ص4.

3- **إنترنت مفتوح وآمن وموثوق به وقابل للتشـغيل المتبادل:** حيث يعد الإنترنت موردًا اسـتثنائيًا للتعلم، والتواصل، والنمو الاقتصادي، الأمر الذى يدعو إلى وضع آليات لضمان إنترنت آمن.

4- **وضـع معايير فنية أخلاقية:** وذلك بوضـع معايير فنية أخلاقية تنظم عمل التقنيات الناشـئة، وتساعد في ضمان جودة المنتج، وحماية صحة المستهلك وسلامته، وتسهيل التشغيل البيني العالمي.

5- **تكنولوجيا تعمل من أجل الديمقراطية:** وذلك من أجل الرد على التهديدات التكنولوجية التي تهدد القيم الديمقراطية، كمحاربة المعلومات المضـللة، والدفاع عن حرية الإنترنت والحد من إساءة الاستخدام.

6- **تعزيز التعاون:** وذلك بين حلفاء الولايات المتحدة الأمريكية[1].

شكل يوضح الضوابط الأساسية للأمن السيبرانى

(3) . استراتيجية الحكومة المصرية في مواجهة جرائم السيبرانية:

أ- . الاستراتيجية المصرية للأمن السيبراني (2017 - 2021):

أُطلق المجلس الأعلى للأمن السـيبراني التابع لرئاسـة مجلس الوزراء برئاسـة وزير الاتصـالات وتكنولوجيا المعلومات الاسـتراتيجية الوطنية للأمن السـيبراني (2017-2021) وتهدف إلى تأمين البنى التحتية للاتصـالات والمعلومات بشـكل متكامل وذلك لتوفير البيئة الآمنة لمختلف القطاعات وذلك في إطار جهود الدولة لدعم الأمن القومي وتنمية المجتمع المصري في ظل تزايد التهديدات والتحديات المستقبلية في المجال السيبراني.

وتقدم الاسـتراتيجية خطة عمل تمتد على مدار الأعوام 2017-2021[2] وتم وضـع خطة مرتبة وفقًا للأهداف، بما يدعم التحول نحو اقتصـاد رقمي متكامل يحقق طموحات المواطنين ويحمى

(3) عبـدالغفار عفيفي:"اسـتراتيجية الـردع السـيبراني للولايـات المتحـدة الأمريكيـة", الريـاض، كليـة العلـوم الاسـتراتيجية والأمنية, جامعة نايف العربية للعلوم الأمنية, 2018 , ص ص 196-200.

(1) الاسـتراتيجية الوطنيـة للأمـن السـيبراني 2017-2021 الصـادرة عـن المجلـس الأعلـى للأمـن السـيبراني، رئاسة مجلس الوزراء، من خلال الرابط https://sis.gov.eg/storg/181171

مصـالحهم ويحافظ على مصـالح الدولة العليا ويسـم في نهضـتها وازدهارها. ويمكن تحديد أهم ركائز الاستعداد لمواجهة الأخطار المعلوماتية التي تتضمنها الاستراتيجية **فيما يلى:**

ـــ **الإطار التشريعي:** من خلال وضع الإطار التشريعي الملائم لأمن الفضاء السيبراني ومكافحة الجرائم السيبرانية وحماية الخصوصية وذلك بمشاركة من الأطراف المعنيين وذوى الخبرة في القطاع الحكومي والخاص مع الاســترشــاد بالخبرات والتجارب والبرامج الدولية ذات الصــلة، حيث إن فراغ تشريعات بشأن تلك الجرائم قد يعد ضررًا بالغًا بمنظومة المعلومات الإلكترونية والخدمات الإلكترونية ومن قثم يجب على الدول ملاحقة هذا التطور بصياغة قواعد تشريعية جديدة وملائمة لمواجهة تلك الجرائم التي تكتسب أهمية كبرى يومًا بعد يوم.

ـ **المواطنة الرقمية:** برنامج لحماية الهوية الرقمية وتفعيل البنى التحتية اللازمة لدعم الثقة في التعاملات الإلكترونية بوجه عام وفى الخدمات الحكومية الإلكترونية بوجه خاص مثل بنية المفتاح المعلن PKI infrastructure key public التي يعتمد عليها التوقيع الإلكتروني وتنظمها وتشــرف عليها هيئة تنمية صناعة تكنولوجيا المعلومات.

ويعتمد البرنامج على تشــكيل لجنة عليا للمواطنة الرقمية تقوم بإعداد رؤية اســتراتيجية على المســتوى القومي للمواطنة الرقمية وخطة عمل لتحويل مفهوم المواطنة الرقمية إلى واقع ملموس وإخلاق مشروعات قومية تستهدف تطبيقات موسعة تسهم في تيسير وتأمين التعاملات الإلكترونية اعتمادًا على البنية التحتية التي تم إنشاؤها.

ـــــ **إعداد الكوادر البشــرية:** تنمية الكوادر البشــرية والخبرات اللازمة لتفعيل منظومة الأمن السيبراني في مختلف القطاعات بالتعاون والشراكة بين الجهات الحكومية والقطاع الخاص والجامعات ومؤسسات المجتمع المدني.

. **دعم البحث العلمي:** من خلال دعم برامج ومشروعات التعاون بين الجهات البحثية والشركات الوطنية وخاصة في مجال تحليل البرمجيات الخبيثة المتقدمة ومجال تحليل الأدلة الرقمية وفى مجال حماية وتأمين نظم التحكم الصــناعية ومجال تطوير أجهزة وأنظمة تأمين النظم والشــبكات ومجال التشــفير والتوقيع الإلكتروني ومجال حماية البنى التحتية للاتصــالات وتكنولوجيا المعلومات ومجال تأمين الحواسب السحابية وحماية قواعد البيانات الكبرى ومجال تقنيات الذكاء الاصطناعي كما يلزم كأولوية قصــوى إنشــاء مراكز أو معامل وطنية لاعتماد الأنظمة والأجهزة والبرمجيات والتطبيقات المستخدمة في الجهات الحيوية وفي البنى التحتية الهامة.

ـــــ **التوعية المجتمعية:** برنامج للتوعية المجتمعية بالفرص والمزايا التي تقدمها الخدمات الإلكترونية للأفراد والمؤسسات والجهات الحكومية التي قد تواجهها على أن تشمل حملات سنوية موســعة على مســتوى الجمهورية والمؤتمرات والندوات وورش العمل النوعية في مختلف القطاعات وأن تخاطب مختلف المســتويات بدءًا من المســتوى القيادي وحتى الأطفال وطلاب المدارس والجامعات والمواطن البســيط، ويلزم إصــدار ونشر تقارير دورية للتوعية بأهم الأخطار الســيبرانية وآليات مواجهتها والجهود التي تبذل والأنشطة ذات الصلة بمجال الأمن السيبراني.

ب- . المركز المصري للاستجابة للطوارئ المعلوماتية (سيرت)[1]:

(1) **الموقع الرسمي لوزارة الاتصالات وتكنولوجيا المعلومات:**
https://www.mcit.gov.eg/Ar/Mediq-Center/Latest-News/News/7566

يقوم المركز المصري للاستجابة للطوارئ المعلوماتية (سيرت) الذي تأسس في أبريل 2009 بمبادرة من الجهاز القومي لتنظيم الاتصالات، الدعم على مدار 24 ساعة لحماية البنية المعلوماتية الهامة ويعمل بالمركز فريق مؤلف من 16 متخصصًا. ويعمل المركز في رصد الهجمات وصدها معتمدًا على مصادر المعلومات والتقارير المختلفة التي يتلقاها من مراكز الأمن السيبراني على مستوى العالم، كما قام المجلس بوضع استراتيجية خاصة بالأمن السيبراني تمتد من العام 2017 حتى عام 2021، من خلال التعاون المشترك، يمكن تلقي إشعارات احتمال الهجمات محتملة وبالتالي البحث عن مصدر تلك الهجمات وسد الثغرات التي يمكن من خلالها النفاذ إلى البنية الأساسية الحرجة، وبالتالي تعطيل تلك الخدمات.

وتجدر الإشارة إلى أن المركز المصري للاستجابة للطوارئ المعلوماتية "سيرت" لديه العديد من اتفاقيات التعاون مع فريق الطوارئ للحاسوب بالولايات المتحدة "us-CeRt" ووكالة أمن الإنترنت الكورية "KISA" في مدينة سيول والهيئة الماليزية للأمن السيبراني كما أن "سيرت" عضو في فريق الاستجابة لطوارئ الحاسوب التابع لمنظمة المؤتمر الإسلامي.

ج- .اللجنة الوطنية المعنية بالاستخدام الآمن للإنترنت للأطفال:

بدأت اللجنة الوطنية المعنية بالاستخدام الآمن للإنترنت للأطفال عملها في يونيو 2013 وهى تعتبر استكمالاً لجهود فريق العمل الوطني المعنى بالاستخدام الآمن للإنترنت الذى كان مشكلاً من ذي قبل في الفترة من أكتوبر 2009 إلى يناير 2012، بهدف وضع وتفعيل استراتيجية إيمانًا منها بأن تمكين الأطفال من استخدام الإنترنت هو السبيل الأمثل لحمايتهم من المخاطر المتصلة بالإنترنت[1].

.أهداف اللجنة: تهدف اللجنة إلى ما يأتي:

1- توحيد وتنسيق الجهود المبذولة وذلك من منطلق أن مسؤولية عالم الإنترنت تقع على عاتق المجتمع والذي يجب أن يضع على رأس قائمة أولوياته واهتماماته السعي لتوفير أفضل السُبل لحماية الأُسرة ورقابة الطفل من مختلف المخاطر وخاصة تلك التي تمس الخصوصية.

2- تعزيز عنصر الأمان لكل من الأطفال وأسرهم بخلق بيئة آمنة لاستخدام الإنترنت.

3- وقايتهم من المخاطر المرتبطة بعالم الإنترنت من خلال تحديد وتطوير الأدوات والأساليب المتبعة التي من شأنها تحقيق الأمن والسلامة في العالم الافتراضي.

4- تتبنى اللجنة منهجية العمل متعدد الأطراف التي تقوم على جذب جميع الأطراف المعنية بقضايا الاستخدام الآمن للإنترنت للأطفال .

انعقاد اليوم العالمي للإنترنت الآمن:

ينعقد اليوم العالمي للإنترنت الآمن يوم 11 فبراير من كل عام في جميع أنحاء العالم تحت شعار "معًا من أجل إنترنت أفضل" وذلك لتعزيز الاستخدام الآمن للتكنولوجيا الرقمية للأطفال والشباب، ويدعوا الحدث الشباب والآباء ومقدمي الرعاية والمعلمين والأخصائيين الاجتماعيين ومسؤولي الاتحاد جميعًا من أجل المساعدة في خلق إنترنت أفضل.

---

(1) وزارة الاتصالات وتكنولوجيا المعلومات المصرية ، مرجع سابق.

ويري الباحث أن اللجنة الوطنية المعنية بالاستخدام الآمن للإنترنت للأطفال تضم في عضويتها ممثلي عدد من الوزرات والجهات الحكومية منها "الداخلية، العدل، التربية والتعليم، التعليم العالي، الشباب والرياضة، الاتصالات وتكنولوجيا المعلومات، غرفة صناعة تكنولوجيا المعلومات والاتصالات، المجلس القومي للطفولة والأمومة".

اليوم العالمي للإنترنت بدأ منذ أحد عشر عامًا كمبادرة من الاتحاد الأوروبي وشبكة Insafe في الدول الأوروبية، وبمرور الوقت تخطى الاحتفال حدود أوروبا وأصبح الاحتفال الذي بدأ بعدد 14 دولة عام 2004 ينظم اليوم فيما يقرب من 100 دولة في جميع أنحاء العالم.

ويري الباحث أن التطور السريع في تكنولوجيا الكمبيوتر، دفع المجتمع الدولي للدخول في مرحلة جديدة أصبح فيها للأمن السيبراني دور أساسي سواء في الاستحواذ على عناصره الأساسية أو في تعظيم القوة، لظهور محددات جديدة لهذه القوة سواء من حيث طبيعتها أو أنماط استخدامها أو طبيعة الفاعلين فيها، وانعكاس ذلك على قدرات الدول وعلاقاتها الخارجية مما جعل هذه البيئة السيبرانية حقيقة غير مسبوقة، واتجهت الدول إلى الحفاظ على أمنها القومي لمواجهة ما يعرف بصراع "عصر المعلومات.

المطلب الثاني

الآليات الدولية لمُواجهة المخاطر السيبرانية

تبرز أهمية التعاون الدولي في المسائل الجنائية ذات الصلة بالجرائم السيبرانية، بالنظر إلى الطابع عبر الوطني الذي تتسم به هذه الجرائم والتي تستخدم في ارتكابها في أغلب الأحوال شبكة الإنترنت، ومن ثم تتحقق عناصر الركن المادي للجريمة وآثارها في الغالب في دولة أو أكثر، وهو ما يتطلب ضرورة وجود قواعد قانونية تنظم مسائل التعاون بين جهات إنفاذ القانون بين الدول، علاوة على أن الأدلة الرقمية المتخلفة عن هذه الجرائم قد توجد في أكثر من دولة، وهو ما يتطلب تفعيل أحكام التعاون الدولي القضائي في هذا الشأن.

كما أصبحت جرائم الإنترنت مُشكلة عالمية تؤثر على كل الدول تقريبًا[1]، ولا تخضع الجرائم السيبرانية في الوقت الحالي للسيطرة القوية كما يتضح من تفحص للإحصائيات السنوية التي ينتجها معهد أمن الحاسوب (CSI) أو الفريق المعني بطوارئ الحاسوب والاستجابة لها (CERT)[2]، ووفقًا لمكتب الأُمم المُتحدة لمكافحة الجرائم والمُخدرات(UNODC) فإن تهديدات سلامة الإنترنيت قد ارتفعت بشكل كبير في السنوات الأخيرة، وأنَّ عدد ضحايا الجريمة الإلكترونية على الصعيد العالمي بلغ 431 مليون[3]، وأمام هذا الرقم من ضحايا التجاوزات غير المشروعة ومع عدم وجود مُواكبة قانونية للمُستجدات لهذه الجرائم، أيقنت الدول إلى ضرورة سن القوانين الصارمة للتصدي لتلك المخاطر السيبرانية، وتبني برامج وخطط لمُكافحتها، الأمر الذى جعل العديد من الدول

---

(1) Petter Gottschalk,datakriminalitet i Norge,2011,fylkesbiblioteket i Akershus, p.241.

(2) انظر في ذلك؛ دليل الأمن السيبراني للدول النامية، الإتحاد الدولي للاتصالات، ص17. متاح على الرابط https://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-a.pdf

(3)UN conference weighs efforts to combat cybercrime, create safer digital world- UN newscentre-2017.1.18-available at http://www.un.org/apps/news/story.asp?NewsID=50610#.WH7PThvhC03

تصدر التشريعات والقوانين الوطنية لُمكافحة هذه الجريمة، فضلاً عن الاتفاقيات والمُؤتمرات الدولية من أجل ضـمان توفير الحماية القانونية الفاعلة للأفراد وللمؤسـسـات الحكومية والخاصـة من هذه الجرائم، وفي بحثنا هذا حرصـنا على تناول واقع التشـريعات المُقارنة، ودور الاتفاقيات والمؤتمرات في مُكافحة الجريمة السيبرانية، **وذلك من خلال النقاط التالية:**

(أولاً) . أهمية التعاون الدولي في مجال الجرائم السيبرانية:

نظراً للطابع عبر الوطني لجرائم تقنية المعلومات، اسـتلزمت إجراءات مُكافحتها ضرورة تضـافر الجهود الدولية وتعزيز التعاون الدولي بين دول العالم في مجال مواجهة هذه الجرائم، ولاشـــك في أن المواجهة الفعالة لهذه الجرائم تتحقق من خلال تفعيل التعاون الدولي في المسائل الجنائية[1]، وترجع أهمية التعاون الدولي في مكافحة الجرائم السيبرانية إلى الطبيعة الخاصة لجريمة سيبرانية كجريمة عبر وطنية، تتطلب تحقيقات سريعة تتسـم بالخبرة والتعاون غير المسـبوق، وهو ما يتطلب ضرورة تعاون أجهزة إنفاذ القانون بصورة سريعة وفعالة عبر الحدود الوطنية[2].

(ثانياً) . التعاون الدولي فى مُكافحة المخاطر والتهديدات السيبرانية:

(1) التعاون الأمني على المُستوى الدولي:

يلعب الإنتربول دورًا رائدًا فيما يتعلق بتحقيق أهداف التعاون الشرطي الدولي على صعيد العالم، ويتركز نشاط الإنتربول حاليًا على ستة مجالات: "الفساد، ملاحقة الفارين من وجه العدالة، المخدرات والجريمة المنظمة، السـلامة العامة والإرهاب، والاتجار بالبشـر، والإجرام المالي المرتكب بواسـطة التكنولوجية المتقدمة"[3]. ويقوم الإنتربول بدور نشـط وخلاق في اسـتغلال التكنولوجيا الحديثة، التي تتيح تبادل البيانات الدولية على نطاق واسـع بشـأن الإرهاب بشـكل عام وفى عدد من المشـكلات المتعلقة بالجريمة[4].

وقد حظي الدور الحيوي الذي يضـطلع به الإنتربول بصـفته مركزًا عالميًا للبيانات المتصـلة بالإرهاب باعتراف دولي، فالقرار رقم (2178) الصـادر عن مجلس الأمن التابع للأُمم المُتحدة عام 2015 أوكل إلى الإنتربول ولاية واضـحة، تتمثل في عمل المركز عالميًا لتبادل المعلومات الشـرطية الرامية إلى مكافحة التهديد الإرهابي[5]، وانضـم الإنتربول في عام 2016 إلى التحالف العالمي لمكافحة تنظيم الدولة الإسلامية، حيث أضاف الإنتربول إلى التحالف الذى يضم 73 بلدًا ومنظمة دولية عنصرًا حاسـمًا من عناصر العمل الشـرطي الدولي، إذ يعمل بمثابة قناة لتبادل المعلومات بين مناطق النزاع والشرطة في جميع أنحاء العالم[6].

يضـطلع الإنتربول بدور كبير في مواجهة وردع الهجمات الإرهابية عبر الوطنية التي تبدأ في بلد واحد وتنتهى في بلد آخر، إذ أنشـأ الإنتربول في أول أكتوبر 2001 "الإدارة الفرعية للسـلامة العامة

---

(1) أنظر: ديباجة الاتفاقية الأوروبية المتعلقة بالجريمة الإلكترونية، بودابست، 2001/11/23.

(2) كريسـتوفر بينتر: التهديد الذي تفرضـه الجريمة المعلوماتية والحاجة إلى التعاون الدولي، المؤتمر الدولي السـادس للجرائم المعلوماتية الذي نظمته المنظمة الدولية للشرطة الجنائية، القاهرة، 13-2005/4/15، ترجمة مركز بحوث الشرطة، ص66.

(3) Sandler, T., Arce, D. G., Enders, W. An Evaluation of Interpol's CooperativeBased Counterterrorism Linkages, The Journal of Law & Economics, 54 (1), 2011, PP.79-110, The University of Chicago Press for The Booth of Business,p.79.

(4) Jacobs J. B, D Sharing Criminal Records: The United States, the European Union and Interpol Compared, 30 Loy. L.A. Int'l & Comp. L. Rev. 125. 2008. P.127.

(5) انظر تقرير الإنتربول السنوي لعام 2015، ص34. https://www.interpol.int/ar/4/5

(6) انظر تقرير الإنتربول السنوي لعام 2014، ص13. https://www.interpol.int/ar/4/5

والإرهاب"، بعد أحداث 11 سبتمبر 2001 في الولايات المتحدة، كما أنشأ مركز "العمليات والتنسيق"، للرد على طلبات البلدان الأعضاء أثناء الأزمات، وتنسيق تقديم المساعدة الخاصة باللغات الرسمية الأربع "الإنجليزية، والفرنسية، والإسبانية، والعربية" للإنتربول، ويسهل المركز أيضًا تبادل المعلومات الاستخبارية ونقل جميع إشعارات الإنتربرول[1].

ويتم التعاون من خلال: منظومة اتصالات (1/7-24)، ومنظومة (MIND وFIND)[2]، فضلاً عن تعزيز منظومة (24/7-1) نظام الإنتربول السابق، وترفع من قدرته على التعاون السريع والفعال لمكافحة الإرهاب وكافة أشكال الجرائم الدولية الخطرة[3]، أمَّا منظومة (MIND وFIND) فتمكّن موظفي الشرطة في خط المواجهة من الاتصال مباشرةً بمنظومات الإنتربول، وتتزايد قيمة (النشرة الحمراء)، التي تكتسب القيمة القانونية لمذكرة التوقيف الاحتياطي[4].

وعلى غرار منظمة الإنتربول أنشأ المجلس الأوروبي في لوكسمبورج عام 1991 شرطة أوروبية هي اليوروبول (Europol)، لتكون همزة وصل بين أجهزة الشرطة الوطنية في دول المنظمة ولملاحقة الجناة في الجرائم العابرة للحدود ومنها بطبيعة الحال الجرائم المتعلقة بالإنترنت، وإلى جانب ذلك صممت وكالات خصيصًا لتيسير هذا التنسيق، بين كل من اليوروبول، ووحدة التعاون القضائي (Eurojust)، التي أنشأتها الاتفاقية، الموقعة في 26 يولية 1995، وهى وحدة التعاون القضائي لتحقيق الأمن الداخلي للاتحاد الأوروبي، وتضطلع اليوروچست بدور نشط ومهم بصفة خاصة في دعم وتعزيز التنسيق والتعاون بين سلطات التحقيق والادعاء الوطنية، وهى جهة فاعلة رئيسية ومركز خبرة قضائية لأنشطة مكافحة الجريمة المنظمة والجريمة العابرة للحدود والإرهاب داخل الاتحاد.

كما تطور التعاون في أوروبا ضد الاستخدام الإرهابي للإنترنت كثيرًا، إذ تم إنشاء فرق تحقيق مشتركة، وهى آلية أنشأها المجلس الأوروبي وفق القرار (JHA.13/465/2002)، كما اعتمد المجلس توصية في عام 2002 بإنشاء فرق مخصصة متعددة الجنسيات للقيام بذلك وجمع وتبادل المعلومات عن الإرهاب، ويجوز لليوروبول واليوروچست أن يشاركا معًا في إنشاء هذه الفرق بناءً على طلب دولة عضو، ويمكن أيضًا إنشاء مثل هذه الفرق مع دولة ثالثة على أساس قضائي مثل البروتوكول الإضافي الثاني لعام 2001 الملحق بالاتفاقية الأوروبية بشأن المساعدة المتبادلة في المسائل الجنائية بمجلس أوروبا، أو اتفاق عام 2009 بشأن تبادل المساعدة القانونية بين الاتحاد الأوروبي والولايات المتحدة[5].

وبما أن الطابع الحِمائي يسيطر على المفهوم الأوروبي للتعامل مع البيانات عبر الإنترنت، فقد تلاحظ – في الآونة الأخيرة- سعى المفوضية الأوروبية إلى بلوغ إنترنت آمن وحماية للبيانات

---

(1) Sandler, and other, supra note 3, at 84. P80.

(2) للمزيد انظر الموقع الرسمي للإنتربول الدولي: https://www.interpol.int/ar/4/5

(3) عبدالكريم حيمر: "منظمة الإنتربول، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2014، ص30 https://www.interpol.int/ar/4/5

(4) للمزيد انظر الموقع الرسمي للإنتربول الدولي: https://www.interpol.int/ar/4/5

(1) Bodin, S., Echilley, M. & Quinard-Thibault, O., International cooperation in the face of cyber-terrorism: current responses and future issues, Themis competiton Semi- Final A- International Cooperation in Criminal Matters, 2015. P.13.

وللخصوصية، من خِلال مشروع حِماية الأفراد من مُعالجة واختراق بياناتهم في بيئة الإنترنت؛ بحيث يهدف التوجيه الأوروبي إلى **تنظيم مسألة التعامل مع البيانات الشخصية لمُستخدمي الإنترنت**[1].

(2) التعاون القضائي الدولي:

يُقصد بالتعاون القضائي: تعاون السلطات القضائية في مختلف الدول لمكافحة الجريمة[2]، بهدف التقريب في الإجراءات الجنائية من حيث إجراءات التحقيق والمحاكمة إلى حين صدور الحكم على المتهم وضمان عدم إفلاته من العقاب نتيجة لارتكابه جريمة في عِدة دول، والتنسيق بين السلطات القضائية في هذا الشأن يجرى للاتفاق على معايير موحدة[3]. كما أن منع الهجمات السيبرانية والحماية منها والتصدي لها، هي من محاور سياسة مكافحة الإرهاب، وينطبق الشيء نفسه على الاستخدام الإرهابي المحتمل لتكنولوجيا المعلومات والاتصالات لمهاجمة البنية التحتية أو المرافق أو الخدمات التي تتيح إمكانية استخدام الإنترنت[4].

أن تنقل المجرمين وأثر الجريمة التي تتم عبر الفضاء الإلكتروني، يتطلب تعاون السلطات في البلدان المعنية، ويتمثل أحد المطالب الرئيسية للمحققين في التحقيقات عبر الوطنية، وفيما يتعلق بهذه المسألة فإن الصكوك التقليدية للتعاون القضائي الدولي في مسائل القانون الجنائي كثيرًا ما لا تفي بالمتطلبات من حيث سرعة التحقيقات في جرائم الإنترنت[5]، وتلعب هذه الصكوك دورًا فعالاً في مكافحة استخدام الإنترنت لأغراض إرهابية لأنها تسمح بالتعاون الدولي السريع[6]، وعلى الرغم من التسليم بأهمية أساليب التعاون القضائي، إلا أن استقراء الواقع يطالعنا بخضوعها لكثير من الشروط والاستثناءات التي تضعف من فعاليتها[7]، ومن بينها مسألة الاختصاص القضائي.

ومن ذلك، يقوم التعاون في الاتحاد الأوروبي على أساس الاعتراف المتبادل بأهميته وضرورته، وهو يستند إلى أمر الاعتقال الأوروبي الذى أقر في عام 2002، ومذكرة الأدلة الأوروبية التي أُنشئت في عام 2008، وهذه الأدوات تجعل التعاون أسهل بين الدول الأعضاء فى الاتحاد الأوروبي من خلال استبعاد متطلبات التجريم المزدوج في قائمة الجرائم، فإن إجراءات استخدامها بسيطة وتضطلع بها السلطات القضائية مباشرة، ومع ذلك، غالبًا ما كان الحكم الأُوروبي على الأدلة غير مجدٍ لأنه يتطلب

---

(2) "**Le projet de directive et de règlement sur l'utilisation des données personnelles– la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données**". **La Commission européenne, Bruxelles, le mercredi, 25 janvier, 2012.**

(3) **أحمد عزت أنور: "دور الوسائل الإلكترونية في الإثبات أمام القضاء – دراسة مقارنة"، رسالة دكتوراه، كلية الحقوق جامعة عين شمس، 2022، ص33.**

(4) **(3) حسين فنور: "المنظمة الدولية للشرطة الجنائية والجريمة المنظمة"، رسالة ماجستير، كلية الحقوق بن عنكون، جامعة الجزائر، 2016، ص ص 133، 134.**

(5) **Fidler, D. P., Cyberspace, Terrorism and International Law, Journal of Conflict & Security Law, 21 (3), Oxford University Press, 2016.p478.**

(1) **Gercke, M. understanding cybercrime: phenomena, challenges and legal response, Telecommunication Development Sector, ITU publication, Switzerland, 2012, p.267.**

(2) **Bodin and other, supra note 1, at 27, p12.**

(3) **محمود شريف بسيوني: "الجريمة المنظمة عبر الوطنية– ماهيتها ووسائل مُكافحتها دوليًا وعربيًا"، ط1، دار الشروق، القاهرة، 2004، ص192.**

اليقين بشـــأن وجود الأدلة المطلوبة، ونتيجة لذلك، تم إنشـــاء صـــك عام 2014 وهو أمر التحقيق الأوروبي الذى يغطي جميع إجراءات التحقيق تقريبًا.

ويري الباحث أن التعاون الأمني الرقمي بين الدول، يسـاهم مسـاهمة كبيرة في انحسـار الجريمة المنظمة والقضـــاء عليها وخاصـــة الجرائم الإرهابية ، وهو ما يتطلب ضرورة تفاعل الدول فيما بينها وزيادة الجهود في ســـبيل تشـــجيع وتفعيل هذا التعاون، بإيجاد وســـائل تعاونية في المســـائل الأمنية الكفيلة بالوقاية من الجريمة وتتبع مرتكبيها في حالة وقوعها.

(ثالثًا) . دور الاتفاقيات والمؤتمرات الدولية في مُكافحة الجرائم السيبرانية:

(1) اتفـاقيـة مُكـافحـة إسـاءة اسـتعمـال تكنولوجيـا المعلومـات لأغراض إجراميـة رقم 63/55 لسنة 2000: تهدف إلى مُكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، صـــادرة عن الجمعية العامة لمُنظمة الأُمم المُتحدة، وتكثف الجمعية جهودها لمُكافحة الجريمة العابرة للحدود الوطنية بجميع أبعادها، ومنها الجرائم السيبرانية.

(2) اتفاقية بودابسـت لمكافحة الجرائم المعلوماتية لسـنة 2001 والبروتوكول المُلحق بها: شـــهدت العاصـــمة المجرية بودابســـت في 2001/11/23 ميلاد أولى المعاهدات الدولية التي تكافح جرائم الإنترنت بعد أن وصلت إلى حد خطير أصبح يهدد الأشخاص والممتلكات، وقد وقعت على تلك المعاهدة (26) دولة أوروبية بالإضـــافة إلى كندا واليابان وجنوب أفريقيا والولايات المتحدة الأمريكية وللمعاهدة أهمية قصوى في توفير أُسس الأمن العام وتتضمن 48 مادة موزعة على أربعة فصول، وقد نصـت هذه الاتفاقية على تسـمية مجموعة الأعمال عبر الوسـائل الإلكترونية غير المشـروعة، وحثَّ الدول الأعضاء فيها على تجريمها في تشريعات داخلية، كما تضَّمنتْ الاتفاقية عِدة طوائف من الجرائم الإلكترونية[1]:

أ- الجرائم التي تستهدف عناصر أمن المعلومات الإلكترونية.
ب- الجرائم المرتبطة بالحاسوب الإلكتروني.
ج- الجرائم المرتبطة بالمحتوى الإلكتروني.
د- الجرائم السيبرانية.

ولقد ألزمت هذه الاتفاقية الدول الأوروبية أو أي دولة توقع أو تنضـم إليها من خارج المجموعة الأوروبية إقرار العقوبات الملائمة واتخاذ التدابير الفعالة لهذه الجرائم وســـواءً أكانت ســـالبة لحرية الأشخاص الطبيعية أو حرية الأشخاص المعنوية.

(3) الاتفاقية الأمريكية لعام 1999 واتفاقية الاتحاد الأفريقي لعام 2014:

بالنسـبة للاتفاقية الأمريكية بشـأن جرائم الحاسـوب والإنترنت، حيث تهدف إلى تعزيز حماية أمن الحاسوب الآلي من الجرائم السيبرانية، وبينت المادة (3) منها الجرائم الإرهابية السيبرانية، وذلك عن طريق الدخول غير المصرـح به إلى نظام الحاسـوب الآلي، وتعديل وحذف البيانات بهدف الإضرار بالمؤســـســـات التي تملك هذه الخدمات أو حذف البيانات في تغييرها لإعطاء معلومات كاذبة بهدف إيقاع أضرار مادية.

(1) خالـد حسـن أحمـد لطفـى: "جـرائم الإنترنـت بـين القرصـنة الإلكترونيـة والابتـزاز الإلكترونـي"، ط1، دار الفكـر الجامعي، الإسكندرية، 2018، ص54.

وبمطالعة مواد هذه الاتفاقية يتضح أنها جاءت لتعزيز مكافحة الجرائم السيبرانية وصيانة الحقوق والحريات الشخصية، ولحماية أمن الدولة ومؤسساتها من الأضرار التي تخلفها تلك الجرائم السيبرانية.

أما **اتفاقية الاتحاد الإفريقي** فيما يتعلق بالأمن السيبراني وحماية البيانات الشخصية لعام 2014، فإنها جاءت لتشمل أوسع نطاق من الأنشطة عبر الإنترنت، والتجارة الإلكترونية، وحماية البيانات، والجرائم الإرهابية السيبرانية، والأمن السيبراني، حيث جاءت أقسام الأمن السيبراني - في هذه الاتفاقية- لتحمي حقوق الإنسان، كما تُتيحُ للدول الأعضاء سن قوانين وطنية لمكافحة الجرائم السيبرانية.

(4) الاتفاقيات العربية لمُكافحة الجرائم الإلكترونية:

القانون العربي الاسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها، واعتمدته جامعة الدول العربية من خلال الأمانة العامة لمجلس وزار العدل العرب[1]، ويتكون من (27) مادة تجرم الأنشطة المتعلقة بالحاسوب والإنترنت وجميعها تعد ضمن الجرائم السيبرانية.

(5) دور المُؤتمرات الدولية في مُكافحة الجرائم السيبرانية:

تعمل المنظمات الدولية باستمرار لمواكبة التطورات في شأن الجرائم السيبرانية، وقد أسست مجموعات عمل لوضع استراتيجيات لمكافحة هذه الجرائم، **ومن أهم هذه المؤتمرات**:

1- مؤتمر الأمن السيبراني الدولي الخامس لإنفاذ القانون والصناعة والخبراء الأكاديميين – نيويورك (5-8 كنون الثاني 2015): حيث تم عقده باستضافة وكالة التحقيقات الفيدرالية الأمريكية، وبمشاركة جامعة فرود هام، الأمريكية.

2- المؤتمر الإقليمي السابع للطب الشرعي الرقمي والجرائم السيبرانية سيؤول كوريا الجنوبية (6-8/تشرين الثاني 2015): حيث تضمن محاور الطب الشرعي الرقمي والتحقيق في الجرائم السيبرانية، وذلك نظرًا لأهميته لإنفاذ القانون والأمن القومي.

3- المؤتمر الإقليمي الثالث في الأمن السيبراني (2014/21-20)، بسلطنة عُمان، بالتعاون مع الاتحاد الدولي للاتصالات (ITU)، متحدثًا في مجالات تكنولوجيا المعلومات والاتصالات والأمن السيبرانى.

4- المؤتمر الإقليمي الأول حول مكافحة جرائم الإنترنت خلال (2-29/ شباط 2015) بالرياض، حيث شملت أجندة هذا المُؤتمر الخصائص والآثار والاتجاهات الحديثة للجريمة السيبرانية، والوعى العام بالإنترنت، وجرائم الإرهاب الإلكتروني ومفاهيم وتحديات مكافحة الجرائم السيبرانية[2].

---

(2) تم اعتماده من قبل مجلس وزراء العدل العرب في دورته التاسعة عشر بالقرار رقم (19-2003/10/8 /495)، كما تم اعتماده من مجلس وزراء الداخلية العرب في دورته الحادية والعشرين بالقرار رقم (2004-12/417)

(1) مؤتمر الرياض الإقليمي الأول حول مكافحة الإنترنت منشور على: www.wikcfp.com/cfp/servlet/even

ويري الباحث أهمية التعاون الدولي بين الدول العربية وشركات تقنيات المعلومات والاتصالات وكذلك شركات التواصل المجتمعي وإيجاد مفوضية دولية تتولى المهام مع هذه الشركات لحل الأزمات السيبرانية وخاصة في مجال الإرهاب والتطرف والمخالفات.

. الخاتمة:

تم تناول آليات الحد من التهديدات والمخاطر السيبرانية من خلال **الأول:** ماهية الأمن السيبراني والمخاطر السيبرانية وتناول أطر الأمن السيبراني وتعريفة وأهدافه وأهم المخاطر السيبرانية التي تعرضت لها الدول خلال الفترة الماضية وخاصة فترة covid-19 وكيفية اختراق البنية التحتية الإلكترونية وأن هناك تزايد التحديَّات والمخاطر المرتبطة بالفضاء الإلكتروني ، وجاء المبحث الثاني بالتشريعات والقوانين والآليات التي تتخذها الدولة لحماية الدول والمجتمعات والأفراد من جرائم تقنيات المعلومات وكذا استراتيجيات بعض الدول لمواجهة تلك المخاطر مع التطرق لأهمية التعاون الدولي الأمني لمواجهة الجرائم السيبرانية وذلك في ضوء المواثيق والاتفاقيات الدولية والعربية.

وبعد هذا العرض المُوجز للمُوضوعات التي حَوتها الدِراسة يمكن الإشارة إلى أهم النتائج والتوصيات التي توصلت إليها مجموعة البحث، وذلك على النحو التالي:

. النتائج:

1. الفضاء الإلكتروني أصبح ساحة جديدة للصراع بشكله التقليدي ولكنه ذا طابع إلكتروني يعكس النزاعات التي تخوضها الدول أو الفاعلين من غير الدول على خلفيات دينية أو عرقية أو أيديولوجية أو اقتصادية أو سياسية، ويتمدد الصراع الإلكتروني بداخل شبكات الاتصال والمعلومات متجاوزاً الحدود التقليدية وسيادة الدول، ويؤثر ذلك في امتداد مجاله وتداعياته أو آثاره، وأضافت عملية تعدد الاستخدام والفاعلين والمصالح لتنوع أشكال الصراع وأهدافه.
2. يقصد بالحرب السيبرانية هي عمليات في الفضاء الإلكتروني تستخدم وسائل وأساليب قتال تُرقى إلى مستوى النزاع المسلح ويثور القلق بشأنها بسبب ضعف الشبكات الألكترونية والتكلفة الإنسانية المحتملة من جراء الهجمات السيبرانية
3. تزداد التهديدات الناتجة من الفضاء الإلكتروني، كلما كان هناك مجال بين الشبكات سواء (العسكرية / الأمنية / الحكومية) والشبكة المفتوحة بفضل التطورات التكنولوجية
4. تتميز الجرائم السيبرانية بوقوعها في بيئة المعالجة الآلية للبينات.
5. عدم الاتفاق على تعريف موحد للأمن السيبراني.
6. يمثل أمن المعلومات التحدي الأعظم الذي يتطلب صياغة الخطط الاستراتيجية ذات المحاور التقنية في إطار تشريعي للتعامل مع المخاطر، مع مراعاة تدريب الكوادر البشرية في هذا المجال.
7. إنشاء العديد من مواقع الإنترنت لمكافحة الإرهاب السيبراني والأمن الرقمي، حيث أصبحت بمثابة مؤسسات فكرية وفنية تدعم الأمن الرقمي.
8. الوقوف على التشريعات والاتفاقيات الدولية التي تهدف إلى مواجهة التهديدات السيبرانية.

9. الوقوف على استراتيجيات بعض الدول للاستفادة منها.

التوصيات:

1- تأمين التجهيزات الإلكترونية المتطورة سواء أكانت أجهزة أو برامج، أو منصات، أو تطبيقات لا سيما منها تلك التي تضمن حماية الأنظمة والمعلومات، مع تدريب مُحققين وضباط لجمع الأدلة الرقمية وتحليلها، ومواكبة المستجدات، والتعاون مع الأجهزة المماثلة، التي تنشط على المستوى الدولي.

2- يجب الاستعداد لمرحلة جديدة من الحرب البشرية، التي باتت قادمة لا محالة، هي الحرب السيبرانية، من خلال تطوير القدرات الوطنية السيبرانية وإنشاء وحدات سيبرانية عسكرية داخل صفوف القوات المسلحة والاهتمام بتطوير ترسانة من الأسلحة السيبرانية، بالإضافة إلى صياغة اسراتيجية وطنية تعمل في إطار استراتيجية أخرى قومية تضمن الحفاظ على الأمن الإقليمي والأمن الوطني.

3- التعزيز الدائم لأمن المعلومات داخل كافة مؤسسات الدولة باعتبار الأمن السيبراني كجزء من منظومة **تحقيق الأمن القومي العربي**، جيث إن الأمن السيبراني هو العمود الفقري للحفاظ على الاقتصاد وضمان استقراره وعدم التلاعب به.

4- عقد ورش عمل لمدارسة التجارب في تدابير الأمن السيبراني للخروج بعِدة توصيات قابلة للتنفيذ وذات آليات واضحة.

5- عمل مُحاكاة حرب سيبرانية بين الدول الإقليمية؛ لضمان جاهزية جميع الوحدات السيبرانية القتالية، والتعاون الفني والتقني لتطوير قُدرات سيبرانية هجومية مشتركة، ولضمان الارتقاء بالمستوى المهاري والفكري للكوادر البشرية للكوادر الحكومية والأمنية.

6- تشجيع بناء القدرات لاستحداث ثقافة مستدامة واستباقية بشأن الأمن السيبراني، وإدراك المخاطر المحتملة في الفضاء السيبراني وفهمها من الأمور الحاسمة لاستفادة المستعمل النهائي من تكنولوجيا المعلومات والاتصالات بصورة آمنة.

7- إنشاء بنك معلومات أمنية؛ لرصد جميع البيانات المتعلّقة بالتنظيمات الإرهابية الخطِرة ذات السِّمة الدَّولية، ودعم الثقة باستدعاء المعلومة، وسرعة معرفة كل ما يتعلَّق بالأنشطة الإرهابية ، اعتماد بنك معلومات خاص للمقاتلين الأجانب حيث نتطلع إلى توسيع دائرة التعاون الرقمي ليصل إلى دول الاتحاد الأوروبي وخاصة الشرطة الأوروبية "اليوروبول" ، وما زال العديد من الشباب الأوروبي متأثرين بالفكر المتطرف وربّما يتحوّلون إلى ذئاب منفردة تنفذ هجمات إرهابية في أي وقت لا يمكن التكهن بها ولا يمكن منعها.

8- وضع آلية للمراقبة والإنذار والرد المبكر، مع ضمان قيام التنسيق بين الجهات المعنية بذلك، مع إضافة تقنيات حديثة التشفير في حفظ الملفات الحرجة والحساسة، مع تطبيق ضمانات أمن الشبكات واتصالاتها وبنيتها التحتية، واعتماد المعايير والمقاييس الدولية الخاصة بأمن المعلومات (Information security management - ISO 27001ISO/IEC)، بالحماية والأمن.

المراجع

أولا - الكتب العلمية والمؤلفات :

- حسن مظفر: "الفضاء المعلوماتي"، ط1، مركز دراسات الوحدة العربية، بيروت، 2017.
- حسنين المحمدي بوادي: "إرهاب الإنترنت الخطر القادم"، ط1، دار الفكر الجامعي، الإسكندرية، 2006.
- خالد حسن أحمد لطفى: "جرائم الإنترنت بين القرصنة الإلكترونية والابتزاز الإلكتروني"، ط1، دار الفكر الجامعي، الإسكندرية، 2018.
- خالد مصطفى فهمى: "الحماية القانونية لبرامج الحاسب الآلي في ضوء قانون حماية الملكية الفكرية طبقًا لأحدث التعديلات – دِرَاسة مُقارنة"، 2005، بدون ناشر.
- محمود شريف بسيوني: "الجريمة المنظمة عبر الوطنية- ماهيتها ووسائل مُكافحتها دوليًا وعربيًا"، ط1، دار الشروق، القاهرة، 2004.
- عبدالغفار عفيفي:"استراتيجية الردع السيبراني للولايات المتحدة الأمريكية", الرياض، كلية العلوم الاستراتيجية والأمنية, جامعة نايف العربية للعلوم الأمنية, 2018 .
- عمار ياسر البابلي: "الفضاء الإلكتروني التحديات الأمنية المعاصرة"، دراسات استراتيجية ومستقبلية، معهد البحوث والدراسات العربية، جامعة الدول العربية، 2020.
- عمر عباس خضير: "مكافحة الجرائم السيبرانية كآلية لتعزيز الأمن الإقليمي"، مركز الدراسات العربية للنشر والتوزيع، ط1، مصر، 2021.
- ممدوح عبدالحميد عبدالمطلب: "جرائم استخدام شبكة المعلومات – الجريمة عبر الإنترنت"، بحث مُقدم لمُؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات، 2000.
- إيهاب خليفة: "القوة الإلكترونية: كيف يمكن أن تدير الدول شؤونها فى عصر الإنترنت"، دار العربي، 2017.
- انظر فى ذلك أيضًا؛ ضرغام جابر عطوش: "جريمة التجسس المعلوماتي – دِرَاسة مُقارنة"، المركز العربي للنشر والتوزيع، مكتبة دار السلام القانونية، ط1، 2017.

ثانياً – رسائل الدكتوراه والماجستير

- أحمد عزت أنور: "دور الوسائل الإلكترونية في الإثبات أمام القضاء- دراسة مقارنة"، رسالة دكتوراه، كلية الحقوق جامعة عين شمس، 2022.
- إسراء طارق الجابري: "جريمة الإرهاب الإلكتروني – دِرَاسة مُقارنة"، رسالة ماجستير، كلية الحقوق، جامعة النهرين، العراق، 2021.
- كاميران عزيز حسن: "الجهود الدولية فى مُواجهة الجرائم السيبرانية"، رسالة ماجستير، كلية القانون والعلوم السياسية، الجامعة العراقية، العراق، 2019.
- حسين فنور: "المنظمة الدولية للشرطة الجنائية والجريمة المنظمة"، رسالة ماجستير، كلية الحقوق بن عنكون، جامعة الجزائر، 2016.
- حنين جميل أبو حسين: "الإطار القانوني لخدمات الأمن السيبراني – دراسة مقارنة"، رسالة استكمالاً لمتطلبات الحصول على درجة الماجستير، كلية الحقوق، جامعة الشرق الأوسط، 2021.
- عمار ياسر البابلي، الآليات الحديثة لحماية وتأمين نظم المعلومات وأثارها على الأداء الأمني، رسالة دكتوراه، كلية الدراسات العليا، أكاديمية الشرطة، القاهرة، 2018.
- عبدالكريم حيمر: "منظمة الإنتربول، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2014، ص30 https://www.interpol.int/ar/4/5
- محمد بكرارشوش: "استعدادات الجزائر لمقتضيات حروب الجيل الرابع بين الواقع والآفاق"، دفاتر السياسة والقانون، الجزائر، المجلد 13، العدد 3، 2021.

ثالثاً - الأبحاث العلمية والدراسات والمراكز البحثية:

- أمانى عصام محمد: "استخدام روسيا للقوة السيبرانية فى إدارة تفاعلاتها الدولية"، مجلة كلية التجارة وإدارة الأعمال، جامعة حلوان، المجلد الثاني والعشرون، العدد الرباع، أكتوبر 2021.
- انظر أيضًا؛ محمد سعيد إسماعيل: "التأمين الإلكتروني ضد المخاطر السيبرانية: المشكلات القانونية والحلول المُقترحة- دِرَاسة في القانون القطري والمُقارن"، كلية القانون، جامعة قطر، المجلة الدولية للقانون، المجلد العاشر، العدد الثالث، 2021.

- **عبدالغفار عفيفي الدويك: "الأزمات والحروب السيبرانية...تهديدات تتجاوز الفضاء الإلكتروني"، دراسة مركز صقر للدراسات، العراق، 15 فبراير 2019.**
- **نقلاً عن، ريهام عبدالرحمن: "أثر الإرهاب الإلكتروني على تغير مفهوم القوة والعلاقات الدولية- دراسة حالة: تنظيم الدولة الإسلامية"، بحث منشور على الرابط الإلكتروني الآتي:** https://democraticac.de/?p=34528
- **منى عبدالله السمحان: "متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود"، مجلة كلية التربية، جامعة المنصورة، العدد 111، يوليو 2020.**
- **مجموعة دولية من نشطاء القراصنة، بدأت عام 2003 تطلق هجمات إلكترونية ضد الحكومات والمُؤسسات والأشخاص، نقلاً عن؛ خالد ظاهر عبدالله: "دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي"، مجلة البحوث الفقهية والقانونية، كلية سعد العبدالله للعلوم الأمنية، الكويت، العدد الثامن والثلاثون، إصدار يوليو 2022.**
- **وفاء لطفي: "الجهود الدولية في مجال مكافحة جرائم الإرهاب السبراني: التجربة الماليزية نموذجًا"، مجلة كلية الاقتصاد والإدارة، جامعة 6 أكتوبر، المجلد الثالث والعشرون، العدد الأول، يناير 2022.**
- **تركي المخلفي: "درجة تطبيق إدارة المخاطر"، مجلة القراءة والمعرفة، كلية التربية، جامعة عين شمس، العدد (207) يناير 2019.**

<u>رابعاً : المقالات والتقارير والمواقع الرسمية والحكومية</u>

- **انظر تقرير بعنوان: ماذا تعرف عن الثورة الصناعية الرابعة، المنشور بتاريخ 2018/7/1، على موقع العربية، نقلاً عن جريدة القافلة السعودية، على الرابط الإلكتروني:**https://www.alarabiya.net/ar/qafilah/2018/07/01 /
- **انظر فى ذلك؛ تقرير بعنوان: "التهديدات السيبرانية المُرتبطة بكوفيد -19 فى العالم"، الصادر عن منظمة الإنتربول، وذلك من خلال الموقع الرسمي الآتي:** WWW.INTERPOL.INT
- **انظر فى ذلك؛ دليل الأمن السيبراني للدول النامية، الإتحاد الدولي للاتصالات، ص17. متاح على الرابط https://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-a.pdf**
- **ديباجة الاتفاقية الأوروبية المتعلقة بالجريمة الالكترونية، بودابست، 2001/11/23.**
- **تقرير المنتدى الاقتصادي العالمي السنوي 2021-2022.** https://www.weforum.org/reports/
- **تقرير صادر عن المنظمة العربية لتكنولوجيا الاتصالات والمعلومات، تونس، الجمهورية التونسية، 2021.**
- **تقرير صحيفة البيان الإماراتية بشأن جريمة عقوبة نشر الشائعات والأخبار الكاذبة ، نشر بتاريخ 11 فبراير 2022**
- **حسين الشدوخي: "الدفاع السيبراني في القطاع الصناعي"، تقرير بشأن تقييم ثغرات الأمن السيبراني والاستعداد لمواجهتها في قطاع الطاقة والموارد الطبيعية، أكتوبر 2021.**
- **راجع فى ذلك؛ وثيقة بعنوان: "نظرة عامة على أدوات تقييم القدرات السيبرانية القائمة على الصعيد الوطنى (GOAT)، المنتدى العالمي للخبرات السيبرانية (GFCE)، 2020.**
- **عبدالحق باسو: "الإرهاب المعلوماتي في القانون المغربي والقانون الدولى"، أبحاث الدورة التدريبية "مُكافحة الجرائم الإرهابية المعلوماتية"، كلية التدريب، جامعة نايف العربية للعلوم الأمنية، الرياض، 2006.**
- **كريستوفر بينتر: التهديد الذي تفرضه الجريمة المعلوماتية والحاجة إلى التعاون الدولي، المؤتمر الدولي السادس للجرائم المعلوماتية الذي نظمته المنظمة الدولية للشرطة الجنائية، القاهرة، 13-2005/4/15، ترجمة مركز بحوث الشرطة.**
- **يوسف الشريف ، شرح قانون 34 لسنة 2021 ، جريدة الامارات اليوم ، نشر بتاريخ 25 يناير 2022 ومتاح على <u>https://www.emaratalyoum.com/local-section/other/2022-01-25-1.1590341</u>**
- **الاستراتيجية الوطنية للأمن السيبراني 2017-2021 الصادرة عن المجلس الأعلى للأمن السيبراني، رئاسة مجلس الوزراء، من خلال الرابط** https://sis.gov.eg/storg/181171
- **راجع في ذلك الموقع الإلكتروني الآتي:** http://www.masralarabia
- **راجع فى ذلك الموقع الإلكتروني الآتي؛** https://political-encyclopedia.org
- **للمزيد انظر الموقع الرسمي للإنتربول الدولي: https://www.interpol.int/ar/4/5**
- **انظر تقرير الإنتربول السنوي لعام 2014، ص13. https://www.interpol.int/ar/4/5**
- **انظر تقرير الإنتربول السنوي لعام 2015، ص34. https://www.interpol.int/ar/4/5**
- **<u>ثانياً – المواد والقوانين واللوائح :</u>**
- **الفقرة (1 من المادة 226) من قانون العقوبات الفرنسي الجديد لعام 1992 المعدل.**
- **الفقرة (1 من المادة 323) من قانون العقوبات الفرنسي الجديد لعام 1992 المعدل.**
- **المواد (2، 4، 12، 15، 21، 22) من مرسوم رقم (5) لعام 2012 بشأن مكافحة جرائم تقنية المعلومات الإماراتي.**

- **المادة (3) والمادة (7) من النظام السعودي لمكافحة الجريمة المعلوماتية.**
- **المادة (411) من قانون العقوبات الفرنسي بشأن الجرائم ضد الأمة رقم 913-93 لعام 1993.**
- **بخصوص الأنظمة الجرمية الواردة في القسم (1030) من الفصل (18) من قانون الولايات المتحدة.**

سادساً : المراجع الأجنبية

- **"Le projet de directive et de règlement sur l'utilisation des données personnelles-la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données". La Commission européenne, Bruxelles, le mercredi, 25 janvier, 2012.**
- **(EU) 2016/679, controller: means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.**
- **(EU) 2016/679, processor: means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.**
- **(texte imprimé) / France. Premier Ministre; France, Secrétaire. – Paris: La Documentation française, 2006. – 1**
- **Bodin, S., Echilley, M. & Quinard-Thibault, O., International cooperation in the face of cyber-terrorism: current responses and future issues, Themis competiton Semi- Final A- International Cooperation in Criminal Matters, 2015. P.13.**
- **Cybersecurity Magazine, Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031 (2021); 2021 Ransomware Statistics, Data & Trends, PurpleSec (2021)p1.**
- **Debra. Little jhon Shinder, Michal cross-scene of the cybercrime- published by syngress-seconded itiou 2008-p.663.**
- **Dmitri Alperovitch, Towards Establishment of Cyberspace Deterrence Strategy, In: Cyber Conflict ICCC, 2011 3rd International Conference, Tallinn, Estonia, June 2011, pp. 89- 90**
- **Fidler, D. P., Cyberspace, Terrorism and International Law, Journal of Conflict & Security Law, 21 (3), Oxford University Press, 2016.p478.**
- **Gercke, M. understanding cybercrime: phenomena, challenges and legal response, Telecommunication Development Sector, ITU publication, Switzerland, 2012, p.267.**
- **Gioe, D. V., Goodman, M. S., & Wanless, A. Rebalancing cybersecurity imperatives: patching the social layer. Journal of Cyber Policy, 4(1), 2019. Pp.117-137.**
- **http://www.un.org/apps/news/story.asp?NewsID=50610#.WH7PThvhC03**
- https://globalcybersecurityforum.com/ar
- **https://tdra.gov.ae/ar/national-cybersecurity-strategy**
- **https://u.ae/ar-ae/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security**
- **https://www.albayan.ae/uae/news/1.4337512-02-01-2022**
- **https://www.mcit.gov.eg/Ar/Mediq-Center/Latest-News/News/7566**
- https://www.trendmicro.com/en-us/business.html
- https://www2.deloitte.com/us/en/insights/focus/humancapital-trends.htm
- **ISBN: 978 – 2 – 11 – 006101 – 0, Langues: Français (fre)**
- **Jacobs J. B, D Sharing Criminal Records: The United States, the European Union and Interpol Compared, 30 Loy. L.A. Int'l & Comp. L. Rev. 125. 2008. P.127.**
- **JuliaVoo.et.al. National Cyber power index 2020-Methodology and analytical considerations. USA: HARVARD Kenedy School.2020.p.5-8.**
- **K. K. Panigrahi, Information Security and Cyber Law, published by tutorials point ,2015, p.1.**
- **Kaspersky. What is cybersecurity.2021. pp.1-5.** www.kaspersky.com/
- **Keiran Hardy, George Williams, "What is Cyber Terrorism? Computer and Internet Technology in Legal Definition of Terrorism," Cyber terrorism (U.K: Springer, 2014), p.2.**
- **KEMPF Olivier, Introduction à la Cyber stratégie, Paris, 2021, p.19.**
- **Kritzinger, E. Improving Cybersafety Maturity of South African Schools. Information, 11(10),2020, p4.**
- **La France face au terrorisme: Livre blanc du Gouvernement sur la sécurité intérieure face au terrorisme**
- **La loi no 2006 – 64 du 23 janvier 2006 relative a la lutte contre le terrorism, rev. sc crim 2006, no 2, p 366.**
- **Ordonnance no 2011-1012 eu 24 août 2011 relative aux communications électroniques.**
- **Paulo shakariam and others, interoduction to cyber-warfare, A Multidisciplinary Approach, pubished by Elsevier, Waltham. USA, 2013, p2.**
- **Petter Gottschalk,datakriminalitet i Norge,2011,fylkesbiblioteket i Akershus, p.241.**
- **REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.**
- **Richardson, M. D., Lemoine, P. A., Stephens, W. E., & Waller, R. E. Planning for Cyber Security in Schools: The Human Factor. Educational Planning, 27(2), 2020.p.22.**

- **Sandler, and other, supra note 3, at 84. P80.**
- **Sandler, T., Arce, D. G., Enders, W. An Evaluation of Interpol's CooperativeBased Counterterrorism Linkages, The Journal of Law & Economics, 54 (1), 2011, PP.79-110, The University of Chicago Press for The Booth of Business,p.79.**
- **See website, Cyber Insurance, Retrieved on 14/3/2021, from** https://www2.deloitte.com/us/en/insights/focus/humancapital-trends.htm
- **See, (EU) 2016/679, Article 32 Security of processing, General Data Protection Regulation (GDPR).**
- **Solange Ghernaoyti, Cyber power Crime, Conflict and security in cyberspace, pubished by Epft press, Switzerland, 2013, p156.**
- **Steve Winterfeld and Anderess, the Basics of Cyber Warfare, Understanding the Fundamentals of Cyber Warfare, published by Elsevier, USA, 2013, p17.**
- **Susan. W. Brenner-state cybercrime legislation in the United States of America-Available at:** www.richmond.edu**. Hossein Bidgoli – the internet encyclopedia – volume –joun Wiley and sons 2004-p.326.**
- **Susan. W. Brenner-state cybercrime legislation in the United States of America- the Richmond Journal of Law and technology – volume6, issue3, winter 2001. P.6. Available:** www.Richmond.Edu**.**
- **Techopedia (2021). Blockchain Economy://www.techopedia.com/definitio**

- **Title 18 cection 1030 of the united states Federal code.**
- **UN conference weighs efforts to combat cybercrime, create safer digital world- UN newscentre-2017.1.18-available at**
- **Wilner, Alex S., Deterring the Undeterrable: Coercion, Denial, and Delegitimization in Counterterrorism, Journal of Strategic Studies, Vol. 34, No. 1, February 2011, pp. 3–37.**
- www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons-cyberstrategy-one-year-later

References

First: Scientific books and literature:

- **Hassan Muzaffar: "The Information Space", 1st Edition, Center for Arab Unity Studies, Beirut, 2017.**
- **Hassanein Al-Mohammadi Bawadi: "Internet Terrorism, the Next Danger", 1st Edition, Dar Al-Fikr Al-Jamia, Alexandria, 2006.**
- **Khaled Hassan Ahmed Lotfy: "Cybercrime between Electronic Piracy and Electronic Racketeering", 1st Edition, Dar Al-Fikr Al-Jamia, Alexandria, 2018.**
- **Khaled Mostafa Fahmy: "Legal Protection of Computer Programs in the Light of the Intellectual Property Protection Law According to the Latest Amendments - A Comparative Study", 2005, without publisher.**
- **Mahmoud Sherif Bassiouni: "Transnational Organized Crime - What it is and the means of combating it internationally and Arably", 1st Edition, Dar Al-Shorouk, Cairo 2004.**
  Abdul Ghaffar Afifi: "The Cyber Deterrence Strategy of the United States of America", Riyadh, College of Strategic and Security Sciences, Naif Arab University for Security Sciences, 2018.
- **Ammar Yasser Al-Babli: "Cyberspace: Contemporary Security Challenges", Strategic and Future Studies, Institute of Arab Research and Studies, League of Arab States, 2020.**
- **Omar Abbas Khudair: "Combating Cybercrime as a Mechanism to Enhance Regional Security", Center for Arab Studies for Publishing and Distribution, 1st Edition, Egypt, 2021.**
- **Mamdouh Abdul Hamid Abdul Muttalib: "Crimes of Using the Information Network - Crime over the Internet", research presented to the Conference on Law, Computer and the Internet, College of Sharia and Law, United Arab Emirates University, 2000.**
- **Ihab Khalifa: "Electronic Power: How States Can Manage Their Own Affairs in the Internet Age", Dar Al-Arabi, 2017.**

- **See also Dergham Jaber Attoush: "The Crime of Information Espionage - A Comparative Study", Arab Center for Publishing and Distribution, Dar Al-Salam Law Library, 1st Edition, 2017.**

Second: Doctoral and master's Theses

- **Ahmed Ezzat Anwar: "The Role of Electronic Means in Evidence before the Judiciary - A Comparative Study", PhD Thesis, Faculty of Law, Ain Shams University, 2022.**
- **Esraa Tariq Al-Jabri: "The Crime of Electronic Terrorism - A Comparative Study", master's Thesis, College of Law, Al-Nahrain University, Iraq, 2021.**
- **Kamira Aziz Hassan: "International Efforts in Confronting Cybercrime", master's Thesis, College of Law and Political Science, Iraqi University, Iraq, 2019.**
- **Hocine Fanour: "International Criminal Police and Organized Crime Organization", master's thesis, Faculty of Law Ben Ankoun, University of Algiers, 2016.**
- **Haneen Jamil Abu Hussein: "The Legal Framework for Cybersecurity Services – A Comparative Study", Thesis to Complete the Requirements for Obtaining a master's degree, Faculty of Law, Middle East University, 2021.**
- **Ammar Yasser Al-Babli, Modern Mechanisms for Protecting and Securing Information Systems and Their Effects on Security Performance, PhD Thesis, Faculty of Graduate Studies, Police Academy, Cairo, 2018.**
- **Abdul Karim Haimer: "Interpol, master's Thesis, Faculty of Law and Political Science, Mohamed Khider University, Biskra, 2014, p. 30 https://www.interpol.int/ar/4/5**
- **Mohamed Bakrarouche: "Algeria's preparations for the requirements of fourth-generation wars between reality and prospects", Notebooks of Politics and Law, Algeria, Volume 13, Issue 3, 2021.**

Third: Scientific research, studies and research centers:

- **Amany Essam Mohamed: "Russia's Use of Cyber Force in Managing Its International Interactions", Journal of the Faculty of Commerce and Business Administration, Helwan University, Volume Twenty-Two, Issue Four, October 2021.**
- **See also; Mohammed Saeed Ismail: "Electronic Insurance Against Cyber Risks: Legal Problems and Proposed Solutions - Dr. Rasain Qatari Law and Comparative Law", College of Law, Qatar University, International Journal of Law, Volume X, Issue III, 2021.**
- **Abdul Ghaffar Afifi Dweik: "Cyber crises and wars... Threats beyond cyberspace", Saqr Center for Studies, Iraq, 15 February 2019.**
- **Quoted in: Reham Abdel Rahman: "The Impact of Cyber Terrorism on Changing the Concept of Power and International Relations - A Case Study: The Islamic State", research published on the following link:** https://democraticac.de/?p=34528
- **Mona Abdullah Al-Samhan: "Requirements for Achieving Cybersecurity for Management Information Systems at King Saud University", Journal of the Faculty of Education, Mansoura University, Issue 111, July 2020.**
- **An international group of hacker activists, which began in 2003 launching cyberattacks against governments, institutions and individuals, quoted Khalid Zahir Abdullah: "The Role of Penal Legislation in Protecting Cybersecurity in the Gulf Cooperation Council Countries", Journal of Jurisprudence and Legal Research, Saad Al-Abdullah College for Security Sciences, Kuwait, Issue Thirty-Eight, July 2022 Edition.**
- **Wafaa Lotfy: "International Efforts in the Field of Combating Cyber Terrorism Crimes: The Malaysian Experience as a Model", Journal of the Faculty of Economics and Administration, October 6 University, Volume Twenty-Three, First Issue, January 2022.**

- **Turki Al-Mukhlify: "The Degree of Application of Risk Management", Journal of Reading and Knowledge, Faculty of Education, Ain Shams University, Issue (207), January 2019.**

Fourth: Articles, reports, and official and governmental websites

- **See a report entitled: What do you know about the Fourth Industrial Revolution, published on 1/7/2018, on the Al-Arabiya website, quoting the Saudi Al-Qafila newspaper, at the electronic link:** https://www.alarabiya.net/ar/qafilah/2018/07/01/
- **See a report entitled: "Cyber Threats Associated with COVID-19 in the World", issued by Interpol, through the following official website:** WWW.INTERPOL.INT
- **See Cyber Guide for Developing Countries, ITU, p. 17. Available at the link https://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-a.pdf**
- **Preamble to the European Convention on Cybercrime, Budapest, 23/11/2001.**
- **World Economic Forum Annual Report 2021-2022.** https://www.weforum.org/reports/
- **Report issued by the Arab ICT Organization, Tunisia, Republic of Tunisia, 2021.**
- **Report of the UAE newspaper Al Bayan regarding the crime of spreading rumors and false news, published on 11 February 2022**
- **Hussein Al-Shadoukhi: "Cyber Defense in the Industrial Sector", Report on Cybersecurity Gap Assessment and Preparedness in the Energy and Natural Resources Sector, October 2021.**
- **See document entitled: "Overview of Nationally Based Cyber Capability Assessment (GOAT) Tools", Global Cyber Expertise Forum (GFCE), 2020.**
- **Abdelhak Baso: "Information Terrorism in Moroccan Law and International Law", Research Course "Combating Cyber Terrorist Crimes", Training College, Naif Arab University for Security Sciences, Riyadh, 2006.**
- **Christopher Painter: The threat posed by cybercrime and the need for international cooperation, Sixth International Conference on Cybercrime, organized by the International Criminal Police Organization, Cairo, 13-15/4/2005, translated by the Police Research Center.**
- **Youssef Al-Sharif, Explanation of Law 34 of 2021, Emarat Al-Youm newspaper, published on January 25, 2022 and available on https://www.emaratalyoum.com/local-section/other/2022-01-25-1.1590341**
- **The National Cybersecurity Strategy 2017-2021 issued by the Supreme Council for Cybersecurity, Presidency of the Council of Ministers, through the https://sis.gov.eg/storg/181171 link.**
- **See on that website the following: http://www.masralarabia**
- **See on that website the following: https://political-encyclopedia.org**
- **For more information, see the official INTERPOL website: https://www.interpol.int/ar/4/5.**
- **See INTERPOL Annual Report 2014, p. 13. https://www.interpol.int/ar/4/5**
- **See INTERPOL Annual Report 2015, p. 34. https://www.interpol.int/ar/4/5**

Fifth: Articles, Laws and Regulations:

- **Article 226, paragraph 1, of the new French Penal Code of 1992, as amended.**
- **Article 323, paragraph 1, of the new French Penal Code of 1992, as amended.**
- **Article (3) and Article (7) of the Saudi Anti-Cybercrime Law.**
- **Article 411 of the French Penal Code on crimes against the nation No. 913-93 of 1993.**
- **With respect to the criminal regulations listed in Section 1030 of Chapter 18 of the United States Code.**

Sixth: Foreign References

- **"The draft Directive and Regulation on the use of personal data - the protection of individuals with regard to the processing of personal data and the free movement of such data". The European Commission, Brussels, Wednesday, January 25, 2012.**

- **(EU) 2016/679, controller: means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.**
- **(EU) 2016/679, processor: means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.**
- **(Printed text) / France. Prime minister; France, Secretary. – Paris: La Documentation française, 2006. – 1**
- **Bodin, S., Echilley, M. & Quinard-Thibault, O., International cooperation in the face of cyber-terrorism: current responses and future issues, Themis competiton Semi-Final A- International Cooperation in Criminal Matters, 2015. P.13.**
- **Cybersecurity Magazine, Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031 (2021); 2021 Ransomware Statistics, Data & Trends, PurpleSec (2021)p1.**
- **Debra. Little jhon Shinder, Michal cross-scene of the cybercrime- published by syngress-seconded itiou 2008-p.663.**
- **Dmitri Alperovitch, Towards Establishment of Cyberspace Deterrence Strategy, In: Cyber Conflict ICCC, 2011 3rd International Conference, Tallinn, Estonia, June 2011, pp. 89- 90**
- **Fidler, D. P., Cyberspace, Terrorism and International Law, Journal of Conflict & Security Law, 21 (3), Oxford University Press, 2016.p478.**
- **Gercke, M. understanding cybercrime: phenomena, challenges and legal response, Telecommunication Development Sector, ITU publication, Switzerland, 2012, p.267.**
- **Gioe, D. V., Goodman, M. S., & Wanless, A. Rebalancing cybersecurity imperatives: patching the social layer. Journal of Cyber Policy, 4(1), 2019. Pp.117-137.**
- **http://www.un.org/apps/news/story.asp?NewsID=50610#.WH7PThvhC03**
- **https://globalcybersecurityforum.com/ar**
- **https://tdra.gov.ae/ar/national-cybersecurity-strategy**
- **https://u.ae/ar-ae/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security**
- **https://www.albayan.ae/uae/news/2022-01-02-1.4337512**
- **https://www.mcit.gov.eg/Ar/Mediq-Center/Latest-News/News/7566**
- **https://www.trendmicro.com/en-us/business.html**
- **https://www2.deloitte.com/us/en/insights/focus/humancapital-trends.htm**
- **ISBN: 978 – 2 – 11 – 006101 – 0, Languages: French (fre)**
- **Jacobs J. B, D Sharing Criminal Records: The United States, the European Union and Interpol Compared, 30 Loy. L.A. Int'l & Comp. L. Rev. 125. 2008. P.127.**
- **JuliaVoo.et.al. National Cyber power index 2020-Methodology and analytical considerations. USA: HARVARD Kenedy School.2020. p.5-8.**
- **K. K. Panigrahi, Information Security and Cyber Law, published by tutorials point ,2015, p.1.**
- **Kaspersky. What is cybersecurity.2021. pp.1-5. www.kaspersky.com/**
- **Keiran Hardy, George Williams, "What is Cyber Terrorism? Computer and Internet Technology in Legal Definition of Terrorism," Cyber terrorism (U.K: Springer, 2014), p.2.**
- **KEMPF Olivier, Introduction to Cyber Strategy, Paris, 2021, p.19.**
- **Kritzinger, E. Improving Cybersafe Maturity of South African Schools. Information, 11(10),2020, p4.**
- **The France and Terrorism: Government White Paper on Internal Security and Terrorism**

- **Act No. 2006-64 of 23 January 2006 on combating terrorism, rev. sc crim 2006, No. 2, p 366.**
- **Ordinance No. 2011-1012 eu 24 August 2011 relating to electronic communications.**
- **Paulo shakariam and others, interoduction to cyber-warfare, A Multidisciplinary Approach, pubished by Elsevier, Waltham. USA, 2013, p2.**
- **Petter Gottschalk, Cybercrime in Norway,2011, Akershus County Library, p.241.**
- **REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.**
- **Richardson, M. D., Lemoine, P. A., Stephens, W. E., & Waller, R. E. Planning for Cyber Security in Schools: The Human Factor. Educational Planning, 27(2), 2020.p.22.**
- **Sandler, and other, supra note 3, at 84. P80.**
- **Sandler, T., Arce, D. G., Enders, W. An Evaluation of Interpol's CooperativeBased Counterterrorism Linkages, The Journal of Law & Economics, 54 (1), 2011, PP.79-110, The University of Chicago Press for The Booth of Business, p.79.**
- **See website, Cyber Insurance, Retrieved on 14/3/2021, from https://www2.deloitte.com/us/en/insights/focus/humancapital-trends.htm**
- **See, (EU) 2016/679, Article 32 Security of processing, General Data Protection Regulation (GDPR).**
- **Solange Ghernaoyti, Cyber power Crime, Conflict, and security in cyberspace, pubished by Epft press, Switzerland, 2013, p156.**
- **Steve Winterfeld and Anderess, The Basics of Cyber Warfare, Understanding the Fundamentals of Cyber Warfare, published by Elsevier, USA, 2013, p17.**
- **Susan. W. Brenner-state cybercrime legislation in the United States of America-Available at: www.richmond.edu. Hossein Bidgoli – the internet encyclopedia – volume –joun Wiley and sons 2004-p.326.**
- **Susan. W. Brenner-state cybercrime legislation in the United States of America- the Richmond Journal of Law and technology – volume6, issue3, winter 2001. P.6. Available: www.Richmond.Edu.**
- **Techopedia (2021). Blockchain Economy://www.techopedia.com/definitio**
- **Title 18 cection 1030 of the United States Federal code.**
- **UN conference weighs efforts to combat cybercrime, create safer digital world- UN newscentre-2017.1.18-available at**
- **Wilner, Alex S., Deterring the Undeterrable: Coercion, Denial, and Delegitimization in Counterterrorism, Journal of Strategic Studies, Vol. 34, No. 1, February 2011, pp. 3–37.**
- **www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons-cyberstrategy-one-year-later**