جامعة المنوفية
كلية الحقوق

الجرائم المعلوماتية المهدِدة للأمن القومي المصري

The information Crimes that threatens Egyptian National Security

الباحث الدكتور
أسامة صلاح محمود الماحى
عميد دكتور بالمعاش – وزارة الداخلية

الجرائم المعلوماتية المهدِدة

للأمن القومي المصري

المستخلص:

هدف البحث إلى تحديد الجرائم المعلوماتية المهددة للأمن القومي المصري، واستخدم الباحث المنهج الوصفي، وتوصلت نتائج الدراسة إلى أن الإرهاب الإلكتروني من أهم الجرائم التي تهدد الأمن القومي المصري، ويجب تضافر جميع الجهود لمواجهته.

الكلمات الدالة:

الجرائم المعلوماتية– الأمن القومي المصري.

Abstract:

The information Crimes that threatens

Egyptian National Security

The study aimed to identify information crimes that threaten the Egyptian national security, and the researcher used the descriptive approach. The results of the study concluded that electronic terrorism is one of the most important crimes that threaten the Egyptian national security, and all efforts must travel to confront it.

Key Words:

The information Crimes– Egyptian National Security.

المقدمة

أولاً- موضوع البحث:

تشكل الجريمة إحدى القضايا الرئيسة في دول العالم؛ حيث تشغل بال الحكومات والمختصين والأفراد على حد سواء، ونتيجة للتطور المذهل في الاتصالات وتكنولوجيا المعلومات، وظهور الإنترنت، والانتشار الواسع والسريع للتكنولوجيا أدى ذلك إلى ظهور الجرائم المعلوماتية التي أصبحت خطراً على الأمن القومي للبلاد.

إن النشاط أو السلوك المادي في جرائم الإنترنت يتطلب وجود بيئة رقمية واتصال بالإنترنت ويتطلب ذلك معرفة بداية هذا النشاط والشروع فيه ونتيجته، وتثير مسألة النتيجة الإجرامية في الجرائم المعلوماتية مشاكل عديدة، فعلى سبيل المثال مكان وزمان تحقق الجريمة المعلوماتية.

ورغم التصاعد المستمر في أعداد المستخدمين للإنترنت وانتشار الجريمة المعلوماتية منذ بداية الألفية الثالثة، فلم تتفاعل حكومات العالم بالقدر المطلوب لحمايه الأمن السيبراني، علماً بأن كل المجتمعات حول العالم تعتمد بشكل أساسي على شبكات الحاسب الآلي في القطاع العام والخاص وعلى مستوى الأفراد؛ إلا أنه في السنين القليلة الماضية أصبحت حماية أمن المعلومات والاتصالات والشبكات ومواجهة الجريمة المعلوماتية تشكل أولوية في سياسات العديد من الدول.

وعلى الرغم من امتلاك مصر تراكم ممارساتي في التعامل مع الظواهر الإرهابية بصفتها التقليدية وكيفية مواجهتها، إلا أنه في ظل اتساع نطاق وتداعيات التغيير السياسي الذي شهدته المنطقة العربية بدءاً من عام ٢٠١١ والمعروف بثورات الربيع العربي؛ وقد شهدت تلك الأحداث تحولات نوعية؛ حيث مثلت قضية الإرهاب الإلكتروني التحدي الأخطر للأمن القومي المصري، ومن ثم ظهرت ضرورة تطوير آليات لمواجهة هذه القضية من خلال استراتيجيات حديثة وتطوير منظومة أمنية لمواجهة هذا الإرهاب.

ثانياً- أهمية البحث:

يكتسب البحث أهميته من أهمية التحديات الأمنية والتقنية والقانونية المصاحبة لاستخدامات تقنية المعلومات والحاسب الآلي والإنترنت، ومن خطورة الوضع الراهن للجريمة المعلوماتية على البنية التحتية لأنظمة تقنية المعلومات والاتصالات وتهديد الاختراقات والهجمات

المستمرة على نظام مؤسسات القطاع العام والخاص والأفراد، وتهديد الأمن القومي لمصر والدول الأخرى.

ثالثاً- مشكلة البحث:

تكمن مشكلة البحث في تفاقم الجريمة المعلوماتية وتعدد أنواعها وازدياد حجم خسائرها وأضرارها؛ بحيث أصبحت مهدداً حقيقياً لأمن المعلومات في كافة المجالات العامة والحيوية بالقطاع العام والخاص والأفراد، بل مصدر خطورة على الأمن القومي وعلى السلم والأمن الدوليين بسبب استخدام الإنترنت في الأنشطة الإرهابية التي تهدد الأمن القومي.

وتشكل العوامل التالية مشكله البحث وتجعلها أكثر تعقيداً:

١. الاستيلاء على المعلومات المحفوظة في الحاسب الآلي أو المنقولة عبر شبكة الإنترنت أو تغييرها أو حذفها.
٢. إلحاق الأذى بأشخاص أو جهات اعتبارية.
٣. تهديد الأمن القومي العسكري والاقتصادي والاجتماعي.
٤. الاستخدامات السلبية لشبكات التواصل الاجتماعي من خلال بث الأفكار الهدامة والمنحرفة وعرض المواد الإباحية والاحتيال والتزوير وانتهاك الحقوق الخاصة والاستغلال الجنسي للأطفال.
٥. صعوبة مكافحة الجرائم المعلوماتية على المستوى الوطني والدولي بسبب سهولة إخفاء معالمها وصعوبة الحصول على الدليل المادي.

رابعاً- تساؤلات البحث:

يدور البحث حول تساؤل رئيس مؤداه:

- **ما الجرائم المعلوماتية المهددة للأمن القومي المصري؟**

ويتفرع من هذا التساؤل مجموعة من التساؤلات الفرعية على النحو التالي:

١. ما الجرائم المعلوماتية وما خصائصها؟
٢. ما جرائم الإرهاب الإلكتروني؟
٣. ما الإرهاب والمواجهة الأمنية؟
٤. ما الأمن القومي المصري؟

خامساً- منهج البحث:

يستخدم الباحث المنهج الوصفي الذي يهتم بتحليل الواقع وتشخيصه وتفسيره، واستخلاص النتائج، وذلك بهدف التوصل إلى توضيح أهم الجرائم المعلوماتية المهددة للأمن القومي المصري.

سادساً- الدراسات والبحوث السابقة:

يُعد الرجوع للدراسات والبحوث السابقة خطوة مهمة في البحث العلمي، ويمكن الرجوع للدراسات والبحوث السابقة ذات الصلة بموضوع البحث حسب التسلسل الزمني من الأقدم إلى الأحدث، **كما يلي:**

١. **دراسة: ميادة بشير، ويوسف عثمان (٢٠١٨)**[١].

هدفت الدراسة إلى تعرف دور العلاقات العامة في التوعية بالجرائم الإلكترونية بالتطبيق على عدة هيئات تمثلت في: وزارة الداخلية، وزارة الاتصالات، المركز القومي للمعلومات، المركز السوداني لأمن المعلومات، وزارة العدل، والهيئة القومية للاتصالات، وتم استخدام المنهج الوصفي، واستعانت الدراسة بالاستبيان والمقابلة والملاحظة كأدوات للدراسة.

وكانت أهم نتائج الدراسة هي أن الإدارات المختلفة نجحت في عقد شراكات واتفاقيات بخصوص التوعية بمخاطر الجرائم الإلكترونية، ومن أكثر الوسائل الإعلامية كانت الصحف والتلفزيون، لكنها لم تهتم باستخدام الإعلام الرقمي في التوعية، كما توصلت نتائج الدراسة إلى أن هناك اتفاقيات بين إدارة العلاقات العامة بالجهات التشريعية والتنفيذية لتكوين هيئات للتوعية بقضايا التكنولوجيا.

---

(١) ميادة بشير، يوسف عثمان، توظيف برامج العلاقات العامة في التوعية بمخاطر الجرائم الإلكترونية، دراسة تحليلية ووصفية على الإدارات المسؤولة عن الجرائم الإلكترونية، وزاره العدل، وزاره الداخلية، وزاره الاتصالات وتكنولوجيا المعلومات في الفترة بين ٢٠١٦-٢٠١٧، مجله العلوم الإنسانية، المجلد (١٩)، العدد (٢)، ٢٠١٨، ص ص ١٥٦-١٧٥.

٢. **دراسة: علي الشهري (٢٠١٩)**[١].

هدفت الدراسة إلى وضع رؤية استراتيجية للحد من الجرائم الإلكترونية لتعزيز الأمن السيبراني من خلال التعرف على طبيعة تلك الجرائم وأسبابها، والوقوف على التهديدات والمخاطر التي تعترض الأمن السيبراني في السعودية، وتم استخدام المنهج الوصفي، واعتمد الباحث على استبانة (S.W.O.T) لجمع البيانات.

وكانت أهم نتائج الدراسة أن الجرائم الإلكترونية لا تعترف بأي حدود مكانية أو زمنية، وأن التقنيات الحديثة وفرت فرصاً غير مسبوقة لانتشارها، وأن انتهاك السياسات الأمنية الخاصة تمثل أهم التهديدات التي تواجه الفضاء السيبراني.

٣. **دراسة: Ahmed Alkalei (2020)**[٢].

هدفت الدراسة إلى وضع استراتيجيات للمساعدة في الحد من الجرائم الإلكترونية وتعزيز الأمن السيبراني، وتم استخدام استبانة كأداة لجمع البيانات.

وكانت أهم النتائج هي أن معظم الهجمات الإلكترونية تنشأ بسبب خطأ بشري يرتبط بنقص المعرفة حول اختلاف ديناميات الجرائم الإلكترونية والأمن السيبراني، وأن زيادة المعرفة والوعي من قبل موظفي تكنولوجيا المعلومات وغيرهم من الموظفين المعنيين بديناميات الأمن السيبراني يُعد ضرورياً للغاية في الحد من تلك الجرائم، كما توصلت إلى أن المراقبة والتنبيهات المناسبة هي الاستراتيجية الأكثر فاعلية لمنع الجرائم الإلكترونية وتعزيز الأمن السيبراني، يليها اكتساب المعرفة حول الأمن السيبراني، ثم تعزيز إدارة المخاطر واتخاذ القرار، ثم تطوير التقنيات والبرامج، وإنشاء فريق أمني قوي، وتطبيق قوانين الأمن السيبراني يليها التخصيص الفعال للموارد.

٤. **دراسة: Mohammed Aldhamdi (2020)**[٣].

هدفت الدراسة إلى تطوير رؤية استراتيجية لمكافحة الجرائم الإلكترونية لتعزيز الأمن السيبراني في المملكة العربية السعودية من خلال التعرف على طبيعة أنواع الجرائم الإلكترونية وأبعاد الأمن السيبراني ودور مكافحة الجرائم الإلكترونية في تعزيز الأمن السيبراني، وتم استخدام استبيان لجمع البيانات.

---

(١) علي الشهري، رؤيه استراتيجية لمكافحة الجرائم الإلكترونية تعزيزاً للأمن الإنساني، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، كليه العلوم الاستراتيجية،.٢٠١٩.

(2) Alkalei, A., A Strategic, Vision to Reduce Cyber-crime and enhance Cyber Security, International Journal of Advance Science and Technology, Vol. 29, No. 7, 2020, p. 12.

(3) Mohammed Aldhamdi, A Strategic, Vision to reduce Cyber-crime to enhance Cyber Security, Webology, Vol. 17, No. 2, December 2020, pp. 289-295.

وكانت أهم نتائج الدراسة هي أن أبعاد الرؤية الاستراتيجية التطويرية في مراقبه الشبكة وإعدادات التنبيه للكشف عن الأنشطة المشبوهة تُعد مهمة للغاية، وكذلك تقييم المخاطر وتطوير سياسة الأمن السيبراني، وتوظيف أحدث لتقنيات الأمان والمعدات اللازمة للكشف عن التهديدات والمخاطر والتصدي لها، وتعزيز سياسات التعاون والتنظيمي بين القطاعين العام والخاص، والتأكيد على الحاجة إلى القيم الأساسية مثل أمن البيانات الشخصية وحرية التعبير والتدفق الحر للمعلومات، والدعوة إلى تعاون دولي مشترك.

٥. **دراسة: أميرة محمد محمد (٢٠٢١)**[١].

هدفت الدراسة إلى وضع رؤية استراتيجية نموذجيه متكاملة لمكافحة الجرائم الإلكترونية من زوايا مختلفة يمكن تطبيقها على كافه المستويات، والتي من شأنها حماية المجتمع من الشائعات والأخبار المضللة المثارة على مواقع التواصل الاجتماعي، وتأمين سلامة عمل قطاعات الدولة المختلفة من خلال تحقيق الأمن لها من أي اختراقات، وتعزيز الحفاظ على الأمن القومي من خلال استطلاع آراء الخبراء والمتخصصين عبر ثلاث جولات مختلفة بتطبيق أسلوب "ديلفي"، وأسلوب التخطيط الاستراتيجي.

وكانت أهم نتائج الدراسة هي تعدد أسباب وأساليب انتشار تلك الجرائم، وتنوع تهديداتها على الأصعدة الاجتماعية، والسياسية، والأمنية، والاقتصادية، كما تعددت الآليات المقترحة ما بين الآليات القانونية، والأمنية، والتقنية، والإعلامية، والتربوية، والتعليمية، والفنية، والدولية للحد من مخاطر انتشار تلك الجرائم والحفاظ على الأمن السيبراني، وسلامة المجتمع وشبكات البنية التحتية وتدعيمها بكل وسائل الأمن والحماية.

تعقيب على الدراسات والبحوث السابقة:

١. هدفت الدراسات والبحوث السابقة إلى تعرف دور جهاز العلاقات العامة ببعض الوزارات والهيئات في التوعية بمخاطر الجرائم المعلوماتية، وهدفت إلى وضع رؤية استراتيجية للحد من هذه الجرائم.
٢. توصلت نتائج الدراسات والبحوث السابقة إلى أهمية وجود اتفاقيات وشراكات لمواجهة الجرائم المعلوماتية، وأهمية مراقبة الشبكات، وكشف الأنشطة المشبوهة وتقييم المخاطر وتطوير سياسة الأمن السيبراني.

ما ينفرد به البحث الحالي:

---

(١) أمير محمد محمد، استراتيجيات مكافحة الجرائم الإلكترونية في العصر المعلوماتي تعزيزاً لرؤيه مصر ٢٠٣٠، دراسة استشراقية، مجلة البحوث الإعلامية، كليه الإعلام، جامعة الأزهر، العدد (٥٨)، الجزء (٤)، يوليو ٢٠٢١، ص ص ١٧٦٥-١٨٠٨.

اهتم البحث الحالي بالمخاطر التي تسببها الجرائم المعلوماتية للأمن القومي، وهي مخاطر تصاب بها الدولة في الداخل والخارج ويجب تكثيف الجهود لمواجهتها.

رابعاً- خطه البحث:

تم تقسيم البحث إلى أربعة مباحث وخاتمة، **وذلك على النحو التالي:**

المبحث الأول- ماهية الجرائم المعلوماتية.

المبحث الثاني- جرائم الإرهاب الإلكترونية.

المبحث الثالث- الإرهاب والمواجهة الأمنية.

المبحث الرابع- الأمن القومي المصري.

الخاتمة- تتضمن أهم نتائج البحث والتوصيات.

قائمه المراجع.

المبحث الأول

ماهية الجرائم المعلوماتية

تمهيد وتقسيم:

تعتبر الجرائم المعلوماتية من أوسع أنواع الجرائم في الوقت الحالي وأوسعها انتشاراً، وتتميز بخصائص كثيرة من أبرزها أن الذي يقوم بها مجرم له مواصفات خاصة وقدرات تقنية مرتفعة، **وسوف نتناول ذلك فيما يلي:**

المطلب الأول– تعريف الجرائم المعلوماتية.

المطلب الثاني– خصائص الجرائم المعلوماتية.

المطلب الثالث– صور الجرائم المعلوماتية.

المطلب الأول

تعريف الجرائم المعلوماتية

تعددت التعريفات الخاصة بالجريمة المعلوماتية، واختلفت الاتجاهات حول هذا الأمر بين مفهوم موسع لمفهوم الجريمة المعلوماتية، وبين مفهوم مضيق لها؛ فهناك تعريف فني عام للجريمة المعلوماتية بأنها نشاط إجرامي يستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود[١].

وهناك تعريفاً قانونياً يفصل العناصر، فمن الناحية القانونية يقضى تعدد استعمالات الحاسب الآلي، واختلاف عناصره وعملياته إيجاد تعريف لكل عنصر أو عملية، ويحدد أركان كل نشاط إجرامي[٢].

ووفقاً لتعريف منظمة التعاون الاقتصادي والتنمية والذي أوردته بلجيكا في تقريرها أن الجرائم المعلوماتية هي كل فعل أو امتناع من شأنه الاعتداء على الأمور المادية والمعنوية يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل تقنية المعلومات[٣].

---

(١) أنظر:

- **نائلة عادل محمد فريد، جرائم الحاسب الآلي الاقتصادية– دراسة نظرية وتطبيقية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، ٢٠٠٣، ص ص ١٩–٢٦.**
- **أحمد خليفة الملط، الجرائم المعلوماتية، الإسكندرية، دار الفكر الجامعي، ٢٠٠٥، ص ص ٨٩–٩٧.**

(٢) محمد الأمين البشرية، التحقيق في الجرائم المستحدثة، الطبعة الأولى، جامعه نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٤، ص٨٨.

(٣) أيمن عبد الله فكري، جرائم نظم المعلومات– دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، ٢٠٠٦، ص ٦٨.

كما تعرف بأنها أي سلوك غير مشروع يرتبط بإساءة استخدام الحاسب الآلي ويؤدي إلى تحقيق أغراض غير مشروعة[١].

وهي أيضاً أي فعل يعاقب عليه القانون تم بمساعدة أو يتطلب ارتكابه الدراية بتكنولوجيا الحاسب الآلي[٢].

المطلب الثاني

خصائص الجرائم المعلوماتية

تتميز الجرائم المعلوماتية بالعديد من الخصائص، **ومنها ما يلي:**

١. تتم في بيئة رقمية معلوماتية قوامها النظم البرامجية المعلوماتية الحاسوبية، وأجهزة ومعدات وأدوات وتجهيزات الحاسب الآلي، أي تتم في وبواسطة جناحي الحاسب الآلي: مكوناته المادية Hardwaer ومكوناته البرمجية Softwaer.

٢. يقوم بها مجرم ذو طبيعة خاصة وإمكانيات خاصة علمية معلوماتية، يستخدم في جريمته المواد المعرفية Knowledgeware، والأساليب الاحترافية.

٣. صعوبة الحصول على دليل مادي في مثل هذه الجرائم، حيث تغلب الطبيعة الإلكترونية على الدليل المتوفر[٣].

٤. تستعصى على الإثبات بالطرق التقليدية وتستلزم طرقاً خاصة مستحدثة للإثبات، قوامها التعليم والتدريب المستمر لعلوم الحاسب الآلي، لذا فإنها تقضي وجود رجل شرطة معلوماتي، ومحقق معلوماتي، وقاضي معلوماتي؛ فضلاً عن الخبير المعلوماتي، حتى يتم كشف الجريمة وتعقب الجناة فيها ومحاكمتهم، لذا فإن عملية الاستعانة بالخبرة الفنية المتخصصة المؤهلة والمدربة؛ تصبح حتمية لكشف واشتقاق وتحليل وتفسير الدليل الجنائي الذي يقدم للمحكمة لتقرير البراءة أو الإدانة، فضلاً عن تدريب رجال الضبط القضائي والمحققين والقضاة على نظم وتكنولوجيا المعلومات وكيفية ضبط وتداول وفهم الأدلة في هذه الجرائم.

٥. هذه الجرائم عابرة لحدود المكان فيمكن عن طريق الحاسب الآلي أو هاتف نقال لشخص في الصين أن يرتكب جريمة تزييف أو تزوير أو سرقه معلومات ضد شخص معنوي في الولايات المتحدة الأمريكية أو في أي دولة أخرى.

---

(١) عبد الفتاح مجازي، مبادئ الإجراءات الجنائية في جرائم الحاسب الآلي والإنترنت، دار الكتب القانونية، المحلة الكبرى، ٢٠٠٧، ص ٣٨٦.

(٢) نبيل عبد المنعم جاد، أسس التحقيق والبحث الجنائي العملي، أكاديمية الشرطة، مطبعة كلية الشرطة، القاهرة، ٢٠٠٥، ص ٣٧٢.

(٣) محمد زكي أبو عامر، الإجراءات الجنائية في التشريع المصري، الجزء الأول، دار النهضة العربية، القاهرة، ٢٠٠١، ص ٨٧.

٦. تتم الجرائم المعلوماتية في وقت ضئيل جداً لا يتعدى ثانية أو جزء من الثانية في بعض الجرائم.
٧. تدني نسبة الإبلاغ عن تلك الجرائم من المجني عليهم وخاصة في حالة الشركات ومؤسسات الأعمال، لتجنب الإساءة للسمعة، ورغبة في عدم زعزعة ثقة العملاء.
٨. غالباً ما تكون الخسائر الناجمة عن الجرائم المعلوماتية فادحة للمجني عليه[١].

المطلب الثالث

صور الجرائم المعلوماتية

إن جرائم الإنترنت أو ما يسمى Cyber Crimes هي ظواهر إجرامية تقرع أجراس الخطر لتنبه مجتمعاتنا عن حجم المخاطر والخسائر التي يمكن أن تنجم عنها وهي في تطور مستمر[٢].

وإذا كانت مجتمعاتنا العربية لم تتأثر بشكل كبير من هذه الظواهر الإجرامية، إلا أن هناك دولاً كثيرة أصبحت مهتمة بتلك الظواهر ومفهومها القانوني، وصفات المجرم المعلوماتي، وسمات هذا العالم الإلكتروني، وصور الجرائم الإلكترونية، **والتي تتمثل فيما يلي**[٣]:

أولاً- الجرائم التي تتم ضد الحواسيب الآلية ونظم المعلومات:

وتتمثل في الجرائم التالية[٤]**:**

١. جرائم الإضرار بالبيانات:

يعتبر هذا الفرع من الجرائم الإلكترونية أشدها خطورة وتأثيراً وأكثرها حدوثاً وتحقيقاً لخسائر الأفراد والمؤسسات على حد سواء، ويشمل هذا الفرع كل أنشطة تتضمن تعديل أو محو أو سرقة أو إتلاف أو تعطيل العمل للمعلومات وقواعد البيانات الموجودة بصوره إلكترونية Digital Form على الحواسب الآلية المتصلة أو غير المتصلة بشبكة المعلومات، أو مجرد محاولة الدخول بطريقه عليها.

---

(١) المرجع السابق، ص ١١٧.
(٢) السيد عاشور، الإدارة العلمية والمعلومات، الجمعية المصرية للحاسب الآلي، ٢٠٠٠، ص ٢٠.
(٣) مجدي فؤاد، الجريمة المعلوماتية وحماية حقوق الملكية الفكرية، بحث غير منشور، ٢٠٠٩، ص ٩.
(٤) دراسة شاملة عن الجريمة السيبرانية، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، ٢٠١٣، ص ٢٣.

وأبسط تلك الأنشطة هو الدخول لأنظمة المعلومات وقواعد البيانات بصورة غير مشروعة والخروج دون إحداث أي تأثير سلبي عليها، ويقوم بذلك النوع من الأنشطة ما يطلق عليها المخترقون ذوي القبعات البيضاء White Hat Hackers، الذين يقومون بالدخول بطريقة غير مشروعة على أنظمة الحاسب أو شبكات المعلومات أو مواقع الإنترنت مستغلين بعض الثغرات في تلك النظم، مخترقين بذلك كل سياسات وإجراءات أمن المعلومات التي يقوم بها مديرو تلك الأنظمة والشبكات.

وفي التقرير السنوي الثامن لمكتب التحقيقات الفيدرالية الأمريكي الصادر عام (٢٠٠٣م) بعنوان جرائم الحاسب، فإن أكثر خسائر المؤسسات بالولايات المتحدة الأمريكية تأتي من الاستيلاء على المعلومات، والتي كبدتها خلال هذا العام خسائر تتعدى السبعين مليون دولار أمريكي، ويأتي في المركز الثاني نشاط تعطيل نظم المعلومات محققا خسائر تتجاوز خمسة وستين ونصف مليون دولار في هذا العام.

ومما هو جدير بالذكر أن ثاني أكثر مواقع الإنترنت شعبية وعدد زائرين "ياهو" Yahoo قد تعرض لهجوم من ذلك النوع في فبراير من عام (٢٠٠٠م)، الأمر الذي أدى إلى انقطاع خدمة الاتصال بالموقع لمدة تجاوزت الثلاث ساعات حتى استطاع المهندسون بالشركة تحديد المناطق التي بدأ منها الهجوم، وتعاملوا معها بوضع فلاتر على جهاز الاتصال Router الموجود بالشركة لحجب تلك المناطق عن الاتصال بالخوادم الموجودة بالشركة وتعطيلها عن العمل[١].

٢. جرائم الاعتداء على الأشخاص:

والمقصود بالاعتداء هو السب والقذف والتشهير وبث أفكار وأخبار من شأنها الإضرار الأدبي أو المعنوي بالشخص، أو الجهة المقصودة من خلال الحاسب الآلي، وتتنوع طرق الاعتداء بداية من الدخول على الموقع الشخصي للشخص المشهر به، وتغيير محتوياته، والذي يندرج تحت الجرائم التي تتم ضد الحواسيب أو الشبكات، أو عمل موقع آخر يتم من خلاله نشر أخبار ومعلومات غير صحيحة، والذي يندرج تحت الجرائم باستخدام الحواسب الآلية والشبكات، والذي غالباً ما يتم من خلال إحدى مواقع الاستضافة المجانية لصفحات الإنترنت، والتي أصبح

---

(١) محمد علي قطب، الجرائم المعلوماتية وطرق مواجهتها، ج (٢)، مملكة البحرين، وزارة الداخلية، الأكاديمية الملكية للشرطة،٢٠١٠، ص ص ١-١٠.

عددها بالألاف في كافة الدول المتصلة بالإنترنت والتي تسمى Free Web Hosting Services.

ومن أشهر تلك الوقائع ما حدث لموقع البنك المركزي المصري على شبكة الإنترنت؛ منذ عدة سنوات؛ حيث قام المهاجم بالدخول بصورة غير مشروعة على جهاز الخادم الذي يتم بث الموقع منه، مستغلاً إحدى نقاط الضعف فيه، وقام بتغيير الصفحة الرئيسية للموقع، الأمر الذي أحدث فزعاً في أوساط المتعاملين مع البنك خوفاً من أن يكون الاعتداء قد امتد إلى المعاملات البنكية الأخرى[١].

٣. جرائم نشر وتطوير الفيروسات:

كانت بداية تطوير فيروسات الحاسب الآلي في منتصف الثمانينات من القرن الماضي في باكستان على أيدي أثنين من العاملين في مجال الحواسيب الآلية، واستمرت الفيروسات في التطور والانتشار حتى بات يظهر ما يقارب المائتي فيروس الحديث شهرياً، والتي تعددت خصائصها وأضرارها[٢].

ثانياً- الجرائم التي تتم باستخدام الحواسيب الآلية ونظم المعلومات:

ومن هذه الجرائم ما يلي:

١. جرائم الاعتداء والتشهير والإضرار بالمصالح الخاصة والعامة:

مثل الاعتداء والتشهير بالأنظمة السياسية والدينية، ولعل أشهر تلك الوقائع قيام بعض الهواة بوضع بعض البيانات في شكل صور من القرآن الكريم وبدأوا في الإعلان عنها من خلال أحد مواقع البث المجاني الشهيرة وهو موقع "ياهو"، الأمر الذي استدعى الأزهر الشريف والمجلس الأعلى للشئون الإسلامية إلى مخاطبة المسئولين عن الموقع، وتم بالفعل إزالة تلك الصفحات، ووضع اعتذار رقيق بدلاً منها[٣].

---

(١) المرجع السابق، ص ٥.

(٢) المرجع السابق، ص ٨.

(٣) محمد علي قطب، الجرائم المستحدثة وطرق مواجهتها، قراءه في المشهد القانوني والأمني وعلاقته بالشريعة الإسلامية، دار الفجر للنشر والتوزيع، ٢٠٠٩، ص ١٩٦.

٢. جرائم الاعتداء على الأموال:

مع زياده درجه اعتماد المؤسسات المصرفية على تكنولوجيا المعلومات والاتصالات، والتحول التدريجي في كافة أنحاء العالم نحو ما يطلق عليه البنوك والمصارف والمؤسسات المالية الإلكترونية، فقد شهد هذا التطور ظهور عدد كبير من الجرائم الإلكترونية[١].

(١) محمد عبد اللطيف فرج، التكنولوجيا الحديثة وجرائم غسل الأموال، بحث غير منشور، ٢٠٠٩، ص ١٩.

المبحث الثاني

جرائم الإرهاب الإلكتروني

تمهيد وتقسيم:

يُعد الإرهاب مشكلة كبيرة تهدد الأمن قومي لدول العالم كما يهدد المؤسسات العامة والأفراد، وعلى ذلك سوف نتناول هذا الموضوع في المطالب التالية:

المطلب الأول– مفهوم الإرهاب.

المطلب الثاني– الإرهاب الإلكتروني.

المطلب الأول

مفهوم الإرهاب

إذا كان الإرهاب وليد التطرف، فإن الاختلاف في تعريفه وخصوصاً على المستوى الدولي لا يزال مستمراً؛ والسبب في ذلك يعود إلى اختلاف مصالح الدول والجهات والقوى الدولية، وفي كثير من الأحيان يتم خلط الإرهاب بالمقاومة لأغراض سياسية، وهو ما تعتمده إسرائيل في سياستها التوسعية الاستيطانية؛ حيث تُعد كل مقاومة لإرهابها الدولي إرهاباً، علماً بأن المقاومة عمل مشروع حسب القانون الدولي من أجل التحرر الوطني، مثل حق الدفاع عن النفس طبقاً للمادة (٥١) من ميثاق الأمم المتحدة والتي تنص على: "الحق الطبيعي للدول، فرادى أو جماعات في الدفاع عن نفسها إذا اعتدت قوة مسلحة على أحد أعضاء الأمم المتحدة، وذلك إلى أن يتخذ مجلس الأمن التدابير اللازمة لحفظ السلام والأمن الدوليين"[١].

وقد رصد الباحث "أليكس شميد" Alex Schmid[٢] في كتابه Political Terrrorism وجود نحو (١٥٩) تعريفات لمصطلح الإرهاب، وهي تنطلق من خلفيات ومصالح سياسية مختلفة.

ويذهب الباحث والمفكر الأمريكي "تشومسكي" إلى تحديد مضمون الإرهاب الذي يعني حسب وجهه نظره "كل محاولة لإخضاع أو قسر السكان المدنيين أو حكومة ما عن طريق

---

(١) المادة (٥١) من ميثاق الأمم، المتحدة الفصل السابع، نيويورك، للأمم المتحدة، ٢٠١٢.

(2) Alex, P., Schmid & Albert, J., Jongman, Political Terrrorism: a Research to Concepts, Theories, Data Bases and Literature, COMT-Publication 12, New Brunswick, NJ: Transaction Books, 1984, 1083.

الاغتيال والخطف أو أعمال العنف، بهدف تحقيق أهداف سياسية، سواء كان الإرهاب فردياً أو تقوم به مجموعات أو تمارسه دولة، وهو الإرهاب الأكثر خطورة[١].

ويشير "باتريك سيل" Patrick Seale[٢] إلى أن المنظمات الصهيونية هي أول من أدخل الإرهاب عبر القنابل التي توضع في الحافلات والأسواق العربية، وذلك أثناء الثورة الفلسطينية بين عامين ١٩٣٦-١٩٣٩، وكانت منظمة "فيلاديمير جابوتنسكي" هي من بادر بذلك، وهو ما سارت عليه قيادات إسرائيلية مثل: بن جوريون، وجولدا مائير، وموشي ديان، وإسحاق شامير، ومناحم بيجن، ونيتنياهو، وغيرهم، وصولاً إلى العدوان المتكرر على غزة.

وبناء على ما سبق فإن معظم الاتفاقيات التي صدرت عن الأمم المتحدة لم تعالج موضوع الإرهاب بصورة شاملة، بل عالجت الإرهاب الفردي وإرهاب الجماعات، واستبعدت معالجة ظاهرة الإرهاب الدولي الذي تمارسه الدولة وحكومتها.

- **التطرف والإرهاب:**

التطرف Extremism ظاهرة تكاد تشغل الناس في جميع المجتمعات بما فيها المجتمعات المتقدمة، لأنها أصبحت لا تهدد السلم المجتمعي والحياة العامة والعلاقات بين الناس فحسب، بل السلم والأمن الدوليين خصوصاً إذا ما تحولت من الفكر والتنظير إلى الفعل والتنفيذ، فما بالك إذا ما استخدم الدين ذريعة للتطرف، وذلك من خلال التكفير Expiation للآخر، وذلك بتأثيمه ومن ثم تحريمه، وبالتالي تجريمه، وسيكون الأمر من الخطورة بمكان إذا ما استخدم العنف أو الإرهاب وسيلة لفرض ذلك خارج نطاق القانون والقضاء، والجدير بالذكر أن ظاهرتي التطرف والإرهاب استفحلتا لدرجه مريعة، بعد موجة ما أطلق عليه "ثورات الربيع العربي" التي بدأت في مطلع (٢٠١١م)، والتي كان من مظاهرها تفشي الفوضى وانفلات الأمن وضعف هيبة الدولة الوطنية، بل تآكلها أحياناً، كما حدث في ليبيا واليمن، إضافة إلى محاولات التفتيت والتقسيم كما هو بالعراق وسوريا، وارتفاع منسوب الشغب والإرهاب ليشمل خريطة واسعة وتضاريس مختلفة حتى في ظل استمرار الدولة وانهيار الشرعية القديمة، وعدم استكمال بناء

---

(١) نعوم تشومسكي، القوة والإرهاب: جذورهما في عمق الثقافة الأمريكية: ترجمة: يحيى الشهابي، دمشق، دار الفكر، ٢٠٠٣، ص ١٧١.

(٢) باتريك سيل، أبو نضال، بندقية للإيجار، المناضلون في خدمات الموساد، مراجعة: أحمد رائف، القاهرة، دار الزهراء للإعلام العربي، ١٩٩٣، ص ١٣٠.

ورسوخ الشرعيات الجديدة، والذي ساعد في بعض الاختراقات الأمنية والأعمال الإرهابية وذلك كما حدث في مصر وتونس، على الرغم من أن الجيش في كلا البلدين كان له دور كبير في حمايه الدولة والمجتمع ومنع الانزلاق نحو الحرب الأهلية[١].

المطلب الثاني

الإرهاب الإلكتروني

يعرف الإرهاب الإلكتروني بأنه هو العدوان أو التخويف أو التهديد مادياً أو معنوياً باستخدام الوسائل الإلكترونية الصادر من الدول أو الجماعات أو الأفراد على الإنسان في دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق، بشتى طرق وصور الإفساد في الأرض[٢]، وتكمن خطورة الإرهاب الإلكتروني في سهولة استخدام هذا السلاح مع شدة أثره وضرره، ويقوم مستخدمه بعمله الإرهابي وهو في منزله أو مكتبه، أو في أي مكان آخر يستطيع من خلاله تنفيذ فعله الإجرامي، ومما يسهل من ذلك أن هذا النوع من الإرهاب يعتمد على البرمجيات كسلاح له، وتلك البرمجيات يسهل الحصول عليها عبر الإنترنت من خلال إعداد لبرمجية إرهابية، وقد اهتم المشرع الفرنسي بالإرهاب في المجال المعلوماتي، فقد جاءت المادة (١/٤٢١) من قانون العقوبات الفرنسي الجديد بأنه من الأعمال الإرهابية الأعمال الأتية: السرقة، والابتزاز، التدمير، والتجريد، الإتلاف، وكذلك الجرائم في مجال المعلوماتية حسبما يعرفه في الكتاب الثالث من هذا القانون؛ تُعد تلك الأعمال إرهابية، حيث تكون ذات علاقة بمشروع فردي أو جماعي يهدف إلى الإخلال بشكل خطير بالنظام العام بالترويع أو بالرعب.

ووفقاً للمادة (٣/٤٢٢) من قانون العقوبات الفرنسي الجديد، يكون العمل الإرهابي مرتكباً من فعل أفراد طبيعيين كما يكون الشخص المعنوي مرتكباً لجريمة إرهابية، وتناولت أحكام هذا

---

(١) عبد الحسين شعبان، والتطرف والإرهاب، إشكاليات نظرية وتحديات عملية (مع إشارة خاصة إلى العراق)، كراسات علمية محكمة، وحدة الدراسات المستقبلية، برنامج الدراسات الاستراتيجية مكتبة الإسكندرية، ٢٠١٦، ص ١٦.

(٢) عبد الرحمن عبد الله، وسائل الإرهاب الإلكتروني، حكمها في الإسلام وطرق مكافحتها، اللجنة العلمية للمؤتمر التالي من مواقف الإسلام من الإرهاب، ٢٠٠٤، ص ٤.

القانون تجريم العدوان على نظم المعالجة الآلية للمعلومات التي تُعد أفعالاً إرهابية، إذا حدث وارتكب ثم ترتب على ارتكابها إحلالاً خطيراً بالنظام العام[١].

وقد ظهر مصطلح الإرهاب الإلكتروني عقب الطفرة الكبيرة التي حققتها تكنولوجيا المعلومات واستخدامات الحواسب الألية والإنترنت تحديداً في إدارة معظم الأنشطة الحياتية، ويرجع ظهور هذا المفهوم إلى بداية التسعينيات نتيجة للزيادة الإلكترونية في معدلات استخدام الإنترنت والاعتماد عليه في إدارة شئون الدول، ولذا أصبح مكافحة الإرهاب الإلكتروني على قمة أجندات الدول، حيث تخصص دولاً كثيرة نسباً كبيرة من ميزانيتها في مكافحة الإرهاب الإلكتروني[٢].

وهذا ما دعى (٣٠) دولة إلى توقيع الاتفاقية الدولية الأولى لمكافحة الجريمة عبر الإنترنت عام (٢٠٠١) في بودابست[٣].

أولاً- تعريف الإرهاب الإلكتروني:

عرفت الموسوعة السياسية الإرهاب الإلكتروني بأنه استخدام العنف غير القانوني أو التهديد به بأشكاله المختلفة كالاغتيال، والتشوية، والتعذيب، والتخريب، والنسف، بغاية تحقيق هدف سياسي معين مثل كسر روح المقاومة والالتزام عند الأفراد وهدم المعنويات عند الهيئات والمؤسسات، أو كوسيلة من وسائل الحصول على معلومات أو مال، وبشكل عام استخدام الإكراه لإخضاع طرف مناوئ لمشيئة الجهة الإرهابية[٤].

كما عرفت الاتفاقية العربية لمكافحة الإرهاب في الفقرة الثانية من المادة الأولى الإرهاب بأنه: "كل فعل من أفعال العنف أو التهديد به أياً كانت بواعثه أو أغراضه يقع تنفيذاً لمشروع إجرامي فردي أو جماعي ويهدف إلى إلقاء الرعب بين الناس، أو حريتهم، أو أمنهم للخطر، أو

---

(١) محمد أبو الفتوح الغانم، الإرهاب وتشريعات المكافحة في الدول الديمقراطية، القاهرة، دار النهضة العربية، ١٩٩١، ص ٢١٤.

(٢) فرانك بولتر، الإرهاب.... ما بين المفهوم التقليدي والحروب الإلكترونية، ترجمة: هشام الحناوي، المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات، ب.ت، تاريخ الدخول: http://www . europarabct.com

(٣) عبد الوهاب الكيالي، موسوعة السياسة، المؤسسة العربية للدراسات والنشر، دار الهدى للنشر والتوزيع، بيروت، ج (١)، ٢٠٠٧، ص ١٥.

(٤) ولد الصديق ميلود، مكافحه الإرهاب بين مشكلة المفهوم واختلاف المعايير، ج (١)، مركز الكتاب الأكاديمي، عمان، ٢٠١٧، ص ١١٢.

إلحاق الضرر بالبيئة، أو بإحدى المرافق، أو الأملاك العامة أو الخاصة، أو احتلالها، أو الاستيلاء عليها، أو تعرض أحد الموارد الوطنية للخطر[١].

كما يعرف الإرهاب الإلكتروني بأنه العدوان، أو التخويف، أو التهديد المادي أو المعنوي الصادر من الدول، أو الجماعات، أو الأفراد على الإنسان في دينه، أو نفسه، أو عرضه، أو عقله، أو ماله بغير حق باستخدام الموارد المعلوماتية والوسائل الإلكترونية بشتى صنوف العدوان وصور الفساد[٢].

كما يعرف بأنه هجوم غير شرعي يستهدف أجهزة الحاسوب والشبكات والمعلومات المخزنة فيها، بحيث يؤدي القيام بذلك إلى ترويع حكومة ما أو إجبار مواطنيها لتأييد أهداف سياسية أو اجتماعية[٣].

١. أهداف الإرهاب الإلكتروني:

يمكن إجمال أهداف الإرهاب فيما يلي[٤]:

أ. أهداف إرهابية تنطوي على عنف يستهدف حياة الأفراد وسلامتهم وإثارة الفوضى ونشر الخوف والرعب بين الأشخاص والدول.

ب. إلحاق الضرر بالبنى المعلوماتية وتدميرها والإضرار بوسائل الاتصالات وتقنية المعلومات.

ج. تعطيل الأداء الطبيعي لنظم السيطرة والرقابة الإلكترونية وتعطيل عمل الأجهزة والهيئات الحكومية والمرافق الاستراتيجية في الدولة.

د. تهديد السلطات العامة والمنظمات الدولية وابتزازها.

هـ. نشر الأخبار والأحداث المفبركة والتي تؤدي إلى نشر الفزع والذعر لدى الأفراد.

---

(١) هشام بشير، الإرهاب الإلكتروني في ظل الثورة التكنولوجية وتطبيقاته في العالم العربي، آفاق سياسية، العدد (٤)، القاهرة، المركز العربي للبحوث والدراسات، ٢٠١٤، ص ص ٧٦-٩٥.

(2) Also, M. N., Ogun, P., Terrorism Schmid of Cyberspace and Cyber Terrorism: New Challenges and Responses, IOS Press, 2015, p. 15.

(٣) بيتر غرابوسكي، جرائم الحاسب الآلي، الأبعاد العالمية في القيادة العامة لشرطة أبو ظبي، شبكات الإنترنت وتأثيراتها الاجتماعية والأمنية، مركز البحوث والدراسات الأمنية، القيادة العامة لشرطه أبو ظبي، ٢٠٠٦، ص ٣٣٨.

(٤) عبد الله عبد العزيز العجلان، الإرهاب الإلكتروني في عصر المعلومات، المؤتمر الدولي لحماية أمن المعلومات، القاهرة، من ٢-٣ يونيو، ٢٠٠٨، ص ١٤.

ومما سبق يمكن الإشارة إلى أن أهداف الإرهاب الإلكتروني يهدد الأمن القومي في الداخل والخارج، وذلك من خلال نشر الأكاذيب في الداخل التي تنتشر بين الناس والتي تؤدي إلى توجيه أعمال تخريبية، ومظاهرات ضد الدولة، وكذلك يهدد الأمن القومي في الخارج من خلال رسم صورة سيئة عن الدولة يظهرها بمظهر الدولة الديكتاتورية التي لا تراعي حقوق الإنسان، وهذا بالطبع يؤدي إلى اعتراض الهيئات العالمية والدول الكبرى على هذه الدولة، وحرمانها من المساعدات الاقتصادية واللوجستية التي تحقق للدولة التطور والتقدم في مختلف المجالات.

٢. خصائص الإرهاب الإلكتروني:

يمكن تحديد أبرز خصائص الإرهاب الإلكتروني فيما يلي:

أ. الإرهاب الإلكتروني عابر للدول:

حيث أنه في الغالب يكون الجاني من بلد والجريمة الإرهابية الواقعة في بلد آخر[١].

ب. الإرهاب الإلكتروني صوره ناعمة من صور الإرهاب:

والسبب في ذلك هو مدى السهولة التي يتم بها ارتكاب جريمة الإرهاب الإلكتروني، حيث أنها لا تحتاج إلى مجهود عضلي كالجرائم الإرهابية التقليدية، فالجريمة الإلكترونية ومنها جرائم الإرهاب الإلكتروني ترتكز على الدراية الذهنية والتفكير العملي المدروس القائم على المعرفة بتقنيات التكنولوجيا والمعلومات[٢].

ج. سهولة ارتكاب جرائم الإرهاب الإلكتروني:

والسبب في ذلك هو غياب الرقابة والسيطرة على الشبكات المعلوماتية، لأنه في ظل ما تتمتع به شبكة المعلومات العالمية من كونها شبكة افتراضية لا يمكن التحكم فيما يعرض عليها، حيث يمكن لأي شخص الدخول ووضع ما يريده على الشبكة، وتقتصر إمكانية الجهات الرقابية على مجال الشبكات الافتراضية في منع الوصول إلى بعض المواقع من خلال حجبها أو إغلاقها أو تدميرها بعد نشر المجرم ما يريد[٣].

٣. الأثار السلبية للرقمية:

لا يمكن إنكار المخاطر والتهديدات المرتبطة بالرقمية، وتشير عبارة "البيانات الضخمة" إلى الحجم المتزايد دائماً للمعلومات الرقمية التي يمكن أن تستخدمها المنظمات لإجراء تنبؤات

---

(١) محمد محيي عوض، مشكلات السياسة الجنائية المعاصرة، جرائم نظم المعلومات، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، ١٩٩٤، ص ٦٠.

(٢) هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط، ١٩٩٤، ص ٨٢.

(٣) عبد الله عبد العزيز العجلان، الإرهاب الإلكتروني في عصر المعلومات، المؤتمر الدولي لحماية أمن المعلومات، القاهرة، من ٢-٣ يونيو، ٢٠٠٨، ٤٨.

حول عادات الناس اليومية وسلوكياتهم بطريقة لم تكن ممكنة من قبل وتشير استطلاعات الرأي بأن بياناتهم آمنة عبر الإنترنت.

ويُعد استخدام التشفير وآليات الأمان الأخرى ضرورية لضمان أمن الإنترنت، والتجسس الإلكتروني له تهديد كبير ليس فقط على الاقتصاد ولكن على المواطنين والدولة أيضاً، ويمكن للتكنولوجيات الرقمية المتزايدة والمترابطة أن تؤدي إلى أشكال جديدة من الهجمات الإلكترونية التي تهدد الصالح العام، وفي مواجهة هذه التحديات يجب العمل مع جميع أصحاب المصالح لصياغة حلول لمواجهة هذه المخاطر[١].

(١) Die, Bundesregiering, Digital Agenda 2014-2017, 2014, pp. 1-40.

المبحث الثالث

الإرهاب والمواجهة الأمنية

تمهيد تقسيم:

يتم استخدام الإنترنت لتحقيق أهداف إرهابية من خلال الدعاية الإرهابية والتمويل للتنظيمات الإرهابية، وهذا ما يتطلب مواجهة أمنية مع تطوير أساليب المواجهة، **وعلى ذلك سوف نتناول هذه الأوجه في المطالب التالية:**

المطلب الأول– طرق استخدام الإنترنت في أغراض إرهابية.

المطلب الثاني– المواجهة الأمنية للجرائم المعلوماتية.

المطلب الأول

طرق استخدام الإنترنت في أغراض إرهابية.

يتم استخدام الإنترنت في أعمال الإرهاب من خلال ما يلي:

أولاً– الدعاية:

يستخدم الإرهابيون الإنترنت لرصد دعاياتهم، وعادة ما تتخذ الدعاية شكل اتصالات عبر وسائط متعددة تحمل تعاليم أيدولوجية أو إرشادات عملية، أو تقدم مشروعاً للأنشطة الإرهابية، أو تسوق المبررات لها، أو تشجع على القيام بها، وقد تشمل الاتصالات التي تضر ضرراً واضحاً بحماية الأمن القومي وهي الاتصالات التي يجتمع فيها عنصرا: التحريض عن قصد على ارتكاب بأعمال عنف ضد أفراد بعينهم، أو مجموعات معينة من الأفراد، واحتمال نجاح هذا التحريض[1].

كما أن التشجيع على العنف أمر شائع في الدعاية للإرهاب، ويزيد نطاق الانتشار الواسع للمواد التي توزع عبر الإنترنت من أعداد المتأثرين بمحتوى هذه المواد بأضعاف مضاعفة، على ذلك فإن القدرة على توزيع المواد عبر الإنترنت تقلل من الاعتماد على قنوات الاتصال التقليدية مثل دوائر الإعلام التي قد تتخذ خطوات للتحقق من مصداقية المعلومات الواردة إليها على نحو مستقل، أو تقوم بتعديل أو حذف الجوانب التي تعتبرها استفزازية إلى حد الإفراط.

([1]) العهد الدولي الخاص بالحقوق المدنية والسياسية، قرار الجمعية العامة ٢٢٠٠ ألف (د–٢١)، الفقرة ٢ من المادة ١٩، ص ٣.

كما أن الترويج للخطاب المتطرف الذي يشجع على أعمال العنف توجه شائع لدى مجموعة متزايدة من منصات الإنترنت التي تنشر محتويات يعدها المستخدمون أنفسهم، وقد توزع هذه المحتويات باستخدام بعض غرف الدردشة ومنصات التواصل الاجتماعي والمواقع ذات الشعبية لعرض الصور وتبادل الملفات[١].

إن أكبر خطر تشكله الدعاية الإرهابية يتعلق بالطريقة التي تستخدم بها والقصد الذي تبث من أجله، فالدعاية الإرهابية التي توزع عبر الإنترنت تشمل مجموعة واسعة من الأهداف وتوجه إلى مختلف أنواع الجماهير، وقد تستخدم الدعاية من أجل تحقيق هدف متطرف، ولإثبات النجاح في تنفيذ هجمات إرهابية لمن قدم دعماً مالياً لمنفذي هذه الأعمال، وقد تشمل الأهداف الأخرى للدعاية الإرهابية التأثير على نفسية الفرد لإضعاف إيمانه ببعض القيم الاجتماعية الجماعية[٢].

كما يمكن استخدام شبكة الإنترنت لإقامة علاقات بمن يتجاوبون مع الدعاية والتماس الدعم منهم، وتقبل المنظمات الإرهابية إقبالاً متزايداً على استخدام مواد الدعاية التي توزع عبر منصات مثل: الموقع المحمية بكلمات سر وروابط مجموعات الدردشة التي يخضع الدخول إليها لقيود باعتبارها وسيلة للتجنيد السري[٣]، ويتيح انتشار شبكة الإنترنت الواسع للتنظيمات الإرهابية والمتعاطفين معها إمكانية التجنيد على نطاق عالمي[٤].

وقد تكون شبكة الإنترنت وسيله فعالة للغاية في تجنيد القُصر الذين يمثلون نسبة كبيرة من مستخدميها، وقد تتخذ الدعاية المنشورة عبر الإنترنت بغرض تجنيد القُصر شكل رسوم متحركة، أو مقاطع فيديو لموسيقى ذات شعبية، أو ألعاب كمبيوتر[٥].

---

(١) UNODC، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، استخدام الإنترنت في أغراض إرهابية، الأمم المتحدة، نيويورك، ٢٠١٣، ص ٤.

(2) Gabriel Weimann, Terror on the internet: the new Arena, the new challenges, washing, D.C, United State Institute of Peace Press, 2006, pp. 37-38.

(3) The McGraw-Hill Homeland, Scott Gerwehr Daly, Al Qaida: Terrorist Selection and Recuitment, Security Handbook, David Kamien, ed., New York, McGraw-Hill, 2006, p. 83.

(4) Handbook of Internet Crime, Dorothy E denning, terror's web: how the Internet is Transforming terrorism, Y nonne Jewhes and majidyar, eds, cullompton, United Kingdom, Willan Publishing, 2010, pp. 194-217.

(5) Gabriel Weimann, Online Terrorists Prey on the Vulnerable, yale Global on line, 5 March 2008. http://yaleglobalyale.edu/content/online-terrorists-prey-vulnerable.

ثانياً- التمويل:

يمكن للتنظيمات الإرهابية وأنصارها استخدام الإنترنت أيضاً لتمويل الأعمال الإرهابية، ويمكن أن تصنف الطرائق التي يستخدمها الإرهابيون لطلب الموارد والأموال وجمعها عبر الإنترنت إلى أربعة فئات عامة هي: الطلب المباشر، والتجارة الإلكترونية، واستغلال أدوات الدفع عبر الإنترنت، واستغلال المنظمات الخيرية، ويشير الطلب المباشر إلى استخدام المواقع الشبكية، ومجموعات الدردشة ورسائل البريد الإلكتروني الجماعية، والاتصالات الموجهة للأنصار لطلب التبرعات بينهم، كما يمكن أن تستخدم المواقع الشبكية باعتبارها متاجر إلكترونية تبيع الكتب وتسجيلات صوتية ومرئية وغيرها من المواد للأنصار، وتسهل خدمات الدفع عبر الإنترنت المتاحة عبر المواقع الشبكية المخصصة أو عبر منصات الاتصالات تحويل الأموال إلكترونياً بين الأطراف المعنية، وكثيراً ما تحول الأموال عن طريق التحويلات البرقية الإلكترونية أو بطاقات الائتمان، أو خدمات الدفع البديلة مثل "باي بال" أو "سكايب"[١].

كذلك من الممكن استغلال خدمات الدفع عبر الإنترنت بأساليب احتيالية مثل انتحال الشخصية وسرقة بطاقات الائتمان والاحتيال من التحويلات البرقية الإلكترونية، والاحتيال في معاملات الأوراق المالية، وجرائم الملكية الفكرية، والاحتيال في المزادات.

كما يمكن تحويل وجهة الدعم المالي الموجه إلى المنظمات المشروعة ظاهرياً مثل المؤسسات الخيرية إلى أغراض غير مشروعة، ومن المعروف أن بعض التنظيمات الإرهابية تنشئ شركات صورية تحت غطاء مشاريع خيرية لطلب التبرعات عبر الإنترنت، وقد تدعي هذه المنظمات أنها تقوم بدعم أهداف إنسانية في حين تستخدم التبرعات في الواقع لتمويل أعمال إرهابية[٢].

ثالثاً- التدريب:

في السنوات الأخيرة أصبحت التنظيمات الإرهابية تستخدم الإنترنت استخداماً متزايداً بوصفه ساحة تدريب بديلة للإرهابيين، وهناك مجموعة متزايدة من الوسائط التي توفر منصات لنشر أدلة عملية في صور كتيبات إلكترونية، ومقاطع صوت وفيديو، ومعلومات، ونصائح.

رابعاً- التخطيط:

أشار العديد من الممارسين في مجال العدالة الجنائية إلى أن جميع قضايا الإرهاب التي خضعت للملاحقة القضائية تقريباً قد استخدمت فيها تكنولوجيا الإنترنت، ويذكر أن التخطيط

---

(١) UNODC، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، مرجع سابق، ص ٤.

(2) Maura Conway, Terrorist, use of Internet and fighting back, information & Security, Vol. 19, 2006, pp. 12-14.

لعمل إرهابي عادة ما ينطوي على اتصال عن بعد ما بين عدة أطراف، كما يمكن أن تستخدم مختلف أشكال تكنولوجيا الإنترنت لتسهيل التحضير لأعمال إرهابية[1].

المطلب الثاني

المواجهة الأمنية للجرائم المعلوماتية

إن المواجهة الأمنية للجرائم المعلوماتية لا تختلف كثيراً عن المواجهة الأمنية للجرائم التقليدية، ويبدو الاختلاف فيما تثيره تقنية المعلومات من مشكلات في مجال جمع الأدلة والإثبات ومشروعية الإجراءات التي تقوم بها أجهزة الأمن في مواجهة تلك الجرائم مع أهمية تطوير أساليب البحث عن الأدلة لتواكب التطورات الحاصلة في مجال الجريمة المعلوماتية، **ويمكن تناول هذا الموضوع بالتفصيل الاتي:**

أولاً- مشروعية الإجراءات الأمنية في مكافحه جرائم الإنترنت:

يقصد بالمشروعية الإجرائية التقيد بأحكام القانون والعمل في إطاره بهدف تقرير ضمانة أساسية للأفراد لحماية حرياتهم وحقوقهم الشخصية ضد تعسف السلطة بالتعدي عليها في غير الحالات المنصوص عليها قانوناً[2]، ولسنا هنا بصدد تناول الإجراءات الشرطية في مرحلة جمع الاستدلالات أو في مرحلة التحقيق، فتلك الإجراءات منصوص عليها قانوناً، إنما نتناول تلك الإجراءات في مجال جرائم الإنترنت، ففي خصوص جمع الاستدلالات فإنه إذا كانت الجرائم محلها أجهزة الحاسب الآلي ذاتها أو أحد ملحقاته، فإن أجهزة الأمن تقوم بمباشره عملها دون أي خروج على حدود المشروعية، إذ أن أجهزة الحاسب الآلي شأنها شأن أي جهاز آخر، وبالتالي لا يتطرق ذلك إلى الدخول إلى حرمة الحياة الخاصة لأياً من الأشخاص، وإذا كان محل الجريمة هو الملفات والبيانات الموجودة داخل أجهزة الحاسب الآلي، وكان الجهاز خاصاً بشخص ما، أي أن الجهاز مستقل وغير موجود ضمن شبكة للحاسبات الآلية، فإن هذا الغرض أيضاً لا يثير أي مشكلة من ناحية حدود المشروعية لأن البحث وجمع التحريات لا يترتب عليه أيضاً انتهاك لحرمة الحياة الخاصة لأي شخص.

([1]) الحكم الصادر بتاريخ ٤ مايو ٢٠١٢ عن محكمة باريس الابتدائية في القضية رقم ٠٩٢٦٦٣٩٠٣٦ (الفرقة الرابعة عشر/٢)، باريس.

([2]) أحمد ضياء، مشروعيه الدليل في المواد الجنائية، رساله دكتوراه، كلية الحقوق، جامعة عين شمس، ١٩٨٣، ص ١٠٢.

ثانياً- إثبات جرائم الإنترنت:

المشكلة الرئيسة في مجال إثبات جرائم الكمبيوتر والإنترنت أنه يصعب اكتشافها، وإذا اكتشفت يصعب ملاحقتها وضبطها ومرتكبوها يتسمون بالدهاء والذكاء والسرعة الفائقة في ارتكاب هذه النوعية من الجرائم، كما أن الأدلة التقليدية غير ملائمة لإثبات تلك الجرائم، وفي هذه الجرائم تصطدم أجهزة الأمن بتكتيك معلوماتي غير مسبوق -سواء كمحل للجريمة أو كوسيلة مستحدثة لارتكبها- وهو قدرة المجرمين على استحداث وسائل مبتكرة على الدوام مثل برامج الاختراق والفيروسات؛ إذ يستطيع الجاني أن يرتكب جريمة دون أن يترك وراءه أي أثر خارجي ملموس، وإذا كان ثمة دليل على الإدانة فيستطيع الجاني تدميره في ثوان معدودة، خاصة وأن المجرم المعلوماتي يتميز بذكاء وبمهارة تقنية عالية ومعارف فنية في مجال المعلوماتية وأنظمة وبرامج الحاسبات الآلية، وهو على دراية بالأسلوب المستخدم في التشغيل، واللغة المستخدمة في تخزين المعلومات وكيفية استدعائها، بل قد يكون من المتخصصين في مجال تقنية المعلومات[١].

ومما يزيد من صعوبة إثبات الجريمة واكتشافها؛ فإن الرغبة في استقرار حركة التعامل ومحاولة إخفاء أسلوب ارتكاب الجريمة حتى لا يتم تقليدها من جانب الأخرين يدفع المجني عليه إلى الإحجام عن مساعدة السلطات المختصة في إثبات الجريمة أو في الكشف عنها، وحتى في حالة الإبلاغ فإن المجني عليه لا يتعاون مع جهات التحقيق خوفاً مما يترتب على ذلك من دعاية مضادة وضياع ثقة المساهمين[٢].

---

(١) محمد يحيى الدين عوضين، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات، القاهرة، دار النهضة العربية، ١٩٩٣، ص ٤٧٦.

(٢) ذكي أمين حسونه، جرائم الكمبيوتر والجرائم الأخرى في مجال التكنولوجيا المعلوماتية، القاهرة، دار النهضة العربية، ١٩٩٤، ص ٤٧٧.

ثالثاً: أهمية التدريب في مجال البحث عن أدلة جرائم الإنترنت:من المعلوم أن الجهات المنعقد بها التحري والاستدلال تتبع طرق تقليدية لجمع عناصر الإثبات عن طريق التفتيش والضبط، أي تجميع الاستدلالات المادية تمهيداً لتحقيق واستخلاص الأدلة أو البراهين المادية ولكن في محيط المعلومات وشبكة الإنترنت لا تستطيع سلطة الاستدلال تطبيق إجراءات الإثبات التقليدية على غالبية جرائم تقنية المعلومات خاصة ما يتعلق بالأشياء المعنوية كمحل للجريمة.

وإزاء ذلك يجب تدريب وتأهيل مأموري الضبط بجرائم تقنية المعلومات فيما يتعلق بالأساليب الفنية المستخدمة في ارتكاب الجريمة، وفيما يتعلق بطرق الكشف عنها، والقرائن والدلائل المستحدثة في مجال إثباتها وكيفية معاينتها والتحفظ عليها، وكيفية فحصها فنياً، وهذا يتطلب تنمية استعدادهم الخاص وتكون مهارات فنية خاصة حتى يتكون لديهم درجة من المعرفة الفنية تتناسب مع حجم المتغيرات والتطورات المتلاحقة في مجال تقنية المعلومات، مع تطوير أساليب البحث عن الأدلة وتقديمها وتقديرها لتواكب هذه التطورات ولا تتخلف عنها[١].

رابعاً: دور الأمم المتحدة في تفشي ظاهرتي التطرف والإرهاب:إن تفشي ظاهرة التطرف والإرهاب باتب قضية مطروحة على طاولة البحث والتشريع في الأمم المتحدة وعلى صعيد المجتمع الدولي كله، فلم يَعد كافياً منذ أحداث ١١ سبتمبر عام ٢٠٠١ الإرهابية التي حدثت في الولايات المتحدة الأمريكية، وجود قرارات تصالح قطعياً وجزئياً لبعض مظاهر التطرف والإرهاب، وإنما استجدت الحاجة الملحة والماسة إلى بحث شامل للظاهرتين بأبعادهما ودلالتهما المختلفة، وقد أصدرت الأمم المتحدة نحو (١٩) اتفاقية وإعلاناً دولياً حول الإرهاب، لكنها لم تتوصل إلى تعريف ماهيته، بسبب اختلاف المصالح الدولية، والتفسيرات والتأويلات الخاصة بذلك، خصوصاً من جانب القوى المتحكمة في العلاقات الدولية، وعلى الرغم من أن مجلس الأمن الدولي أصدر ثلاثة قرارات بعد أحداث ١١ سبتمبر ٢٠٠١، وفيما بعد أربعة قرارات بعد احتلال "داعش" للموصل في عام ٢٠١٤، لكن الأمر لم يتغير وظل تعريف الإرهاب عائماً، بل ازداد أكثر التباساً بحكم التفسيرات المختلفة بشأنه، باختلاف مصالح القوى الدولية[٢].

---

(١) سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، القاهرة، دار النهضة العربية، القاهرة، ١٩٩٩، ص ١٢٩.

(٢) قارن نصوص القرارات الدولية التي أصدرت بعد أحداث ١١ سبتمبر ٢٠٠١، عبد الحسين شعبان، الإسلام والإرهاب الدولي، ثلاثية الثلاثاء الدامي: الدين، القانون، السياسة، لندن، دار الحكمة، ٢٠٠٢.

المبحث الرابع

الأمن القومي المصري

تمهيد وتقسيم:

يشار إلى مفهوم الأمن القومي على أنه تأمين كيان الدولة من الأخطار التي تهددها وتهدد أمنها على المستوى الداخلي والخارجي، ويُعد الإرهاب الإلكتروني من أهم القضايا التي تهدد الأمن القومي المصري والدولي، **وعلى ذلك سوف نتناول ذلك في ما يلي:**

المطلب الأول– مفهوم الأمن القومي.

المطلب الثاني– بعض الجرائم المعلوماتية التي تهدد الأمن القومي المصري.

المطلب الثالث– الإرهاب الإلكتروني وتهديد الأمن القومي المصري.

المطلب الأول

مفهوم الأمن القومي

لا يوجد تعريف واحد متفق عليه للأمن القومي، ولا يوجد اتفاق حول المستهدفين من تحقيق الأمن القومي ولا مهدديه، ولا حتى كيفية تحقيقه، وحيث تتعدد تعريفاته بتعدد الزوايا التي يتناولها الباحثين، ومن هنا يمكن القول بأن هناك ثلاثة اتجاهات أساسيه في تعريف الأمن القومي، حيث يعرفها كل اتجاه من منظور يختلف عن الأخر، فهناك من يعرفها من منظور القوة العسكرية، وهناك من يعرفها من منظور الإجراءات التي يجب اتباعها لحماية كيان الدولة، أما الاتجاه الثالث فيعرفها من منظور القدرات التي يجب توفرها لمواجهة المخاطر التي تهدد الدولة[1].

ووفقاً للاتجاهات الثلاثة، فقد تم وضع عدد من التعريفات، فيعرفه الدكتور/ حامد ربيع، من منظور القوه العسكرية على أنه: الحماية العضوية والمادية لكل مواطن ينتمي إلى الجماعة أولاً وللجماعة ثانياً كحقيقة بشرية، بحيث لا يتعرض كيانها لأية مخاطر بأي معنى من معانيها، أو أنه تلك المجموعة من القواعد الحركية التي يجب على الدولة أن تحافظ على احترامها، وأن

([1]) إيمان بكر أبو الهوى، التهديدات الإسرائيلية الأمن القومي والمائي العربي: دراسة حالة إسرائيل ونهر الأردن في الفترة من ١٩٩٤-٢٠١٠، رساله ماجستير غير منشورة، كليه الحقوق، جامعه القاهرة ،٢٠١١، ص ١٧.

تفرض على الدول المتعاملة معها مراعاتها لتستطيع أن تضمن لنفسها نوعاً من الحماية الذاتية الوقائية الإقليمية[١].

وقد عرف الدكتور/ أمين هويدي، وهو من مؤيدي اتجاه الإجراءات الصارمة لحماية الكيانات الدولية، الأمن القومي بأنه الإجراءات التي تتخذها الدولة في حدود طاقتها للحفاظ على كيانها ومصالحها في الحاضر والمستقبل مع مراعاه المتغيرات الدولية، وبهذا فإن الأمن القومي يشمل الأمن العسكري[٢].

وبالنسبة للاتجاه الثالث، فقد عرف الدكتور/ علي الدين هلال، الأمن القومي بأنه تأمين كيان الدولة ضد الأخطار التي تهددها داخلياً وخارجياً، وتهيئة مصالحها، وتهيئة الظروف المناسبة لتحقيق أهدافها وغاياتها القومية[٣].

كما يُعرف الأمن القومي بأنه قدرة الدولة على تأمين استمرار أساس قوتها الداخلية والخارجية، والعسكرية، والاقتصادية في مختلف مناحي الحياه لمواجهة الأخطار التي تهددها من الداخل والخارج، وفي حاله الحرب والسلم على حد سواء[٤].

ويعرف أيضاً بأنه قدرة الأمة العربية على حفظ إنجازاتها وأسسها ومبادئها من الأخطار والتهديدات التي تواجهها سواء كان تهديداً يخص قطراً عربياً معيناً أو يخص الأمة العربية كلها[٥].

كما يمكن القول بأن الأمن القومي له ثلاثة مستويات هي: المستوى الداخلي وهو مستوى يتعلق بحفظ المجتمع وحمايته من أي اختراق أو تهديد، وإقرار مفهوم الاستقرار في كافة المجالات، والمستوى الإقليمي وهو يتعلق بالصِلات الإقليمية للدولة مع الدول الأخرى، والمستوى

---

(١) حامد ربيع، نظرية الأمن القومي العربي، القاهرة، دار الموقف العربي، ١٩٨٤، ص ص ٣٠-٣٦.

(٢) أمين هويدي، الأمن العربي في مواجهة الأمن الإسرائيلي، دار الطباعة، بيروت، ١٩٧٥، ص ٧.

(٣) علي الدين هلال، الأمن القومي العربي: دراسة في الأصول، مجلة شئون عربية، العدد (٣٥)، يناير ١٩٨٤، ص ٦.

(٤) زكريا حسين، مذكرات في الأمن القومي، كلية التجارة، جامعة الإسكندرية، ٢٠٠١، ص ص ١٢-١٥.

(٥) رائد حسنين، السياسة الإسرائيلية في أفريقيا، دار ابن رشد للنشر، مؤسسة مدارك، بيروت، ٢٠١٨، ص ١٤٣.

الدولي وهو مستوى أعلى مما سبقه، إذ يتعلق بحراك الدولة ضمن المحيط العالمي، وهذه المستويات لا يمكن تحقيقها إلا إذا تم دمجها جميعاً مع بعضها البعض[١].

وبناء على ما سبق يعرف الباحث الأمن القومي المصري بأنه تلك الإجراءات التي تتخذها الحكومة المصرية لتأمين حدودها الداخلية والخارجية من خطر أي تهديد قد يعتري سيادة الدولة سواء من الداخل أو من الخارج من الدول المعادية الحكومة المصرية.

المطلب الثاني

بعض الجرائم المعلوماتية

التي تهدد الأمن القومي المصري

حدد القانون رقم ١٧٥ لسنة ٢٠١٨ بعض الجرائم المعلوماتية الخاصة بالدولة، **فيما يلي**[٢]:

١. جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة:

نصت المادة ٢٠ من القانون على ما يلي: "يعاقب بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز، مائتي ألف جنية، أو بإحدى هاتين العقوبتين، كل من دخل عمداً أو دخل بخطأ غير عمدي وبقي بدون وجه حق أو تجاوز حدود الحق المخول له من حيث الزمان أو مستوى الدخول أو اختراق موقعاً خاصاً أو بريداً إلكترونياً أو حساباً خاصاً أو نظاماً معلوماتياً يُدار بمعرفة أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة أو مملوكاً لها أو يخصها...".

---

(١) العين عبد الله آل العيون، الأمن الوطني الأردني، جريدة الرأي، بتاريخ ٢٠١٦/٥/٢٥، تاريخ الدخول ٢٢/٠٩/١٠ على الرابط التالي: http://alrai.com/article/789414.html

(٢) قانون رقم ١٧٥ لسنة ٢٠١٨، الجريدة الرسمية، العدد (٣٢) مكرر، في ١٤ أغسطس، سنة ٢٠١٨، ص ٣.

٢. جريمة الاعتداء على سلامة الشبكة المعلوماتية:

نصت المادة ٢١ على ما يلي: "يعاقب بالحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن مائة ألف جنية ولا تجاوز خمسمائة ألف جنية أو بإحدى هاتين العقوبتين كل من تسبب متعمداً في إيقاف شبكة معلوماتية عن العمل أو تعطيلها أو الحد من كفاءة عملها أو التشويش عليها أو إعاقتها أو اعتراض عملها أو أجرى بدون وجه حق معالجة إلكترونية للبيانات الخاصة بها ويعاقب كل من تسبب بخطئه في ذلك بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن خمسين ألف جنية بدون وجه حق معالجة إلكترونية للبيانات الخاصة بها ويعاقب كل من تسببه بخطئه في ذلك بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن خمسين ألف جنية ولا تجاوز مائتي ألف جنية أو بإحدى العقوبتين.

فإذا وقعت الجريمة على شبكة معلوماتية تخص الدولة أو أحد الأشخاص الاعتبارية العامة أو تمتلكها أو تدار بمعرفتها تكون العقوبة السجن المشدد، والغرامة لا تقل عن خمسمائة ألف جنية ولا تجاوز مليون جنية.

المطلب الثالث

لظروف المشددة

في الجرائم المعلوماتية التي تهدد الأمن القومي[١]:

حددت المادة ٣٤ من نفس القانون أنه: "إذا وقعت أي جريمة من الجرائم المنصوص عليها في هذا القانون بغرض الإخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر أو الإضرار بالأمن القومي للبلاد أو بمركزها الاقتصادي أو منع أو عرقلة ممارسة السلطات العامة لأعمالها أو تعطيل أحكام الدستور أو القوانين أو اللوائح أو الإضرار بالوحدة الوطنية والسلام الاجتماعي تكون العقوبة على السجن المشدد".

كما حددت المادة ١٣٥ المسئولية الجنائية للشخص الاعتباري في ما يلي: "يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن ثلاثين ألف جنية ولا تزيد على مائة ألف جنيه أو بإحدى هاتين العقوبتين كل مسئول عن الإدارة الفعلية لأي شخص اعتباري إذا تعرض الموقع والحساب الخاص أو البريد الإلكتروني أو النظام المعلوماتي المخصص للكيان الذي يديره لأي جريمة من الجرائم المنصوص عليها في هذا القانون ولم يبلغ بذلك الجهات الرسمية المختصة وقت علمه بالجريمة.

---

(١) القانون رقم ١٧٥ لسنة ٢٠١٨، ص ٣١.

المطلب الرابع

الإرهاب الإلكتروني وتهديد الأمن قومي المصري

تمكنت الحكومة المصرية من القضاء على عدد كبير من الكتائب الإلكترونية في مصر والتابعة لجماعة الإخوان المسلمين، والتي تعمل من داخل شركات حقيقتها ذات طابع تجاري، ومن الباطن تعمل (IT) للجان إلكترونية لإحداث الفوضى في مصر تحت مسمى اللجان التنظيمية الإعلامية، وأبرز تلك الكتائب الإلكترونية "خلية المعلومة السوداء" والتي يديرها أيمن عبد الغني زوج بنت خيرت الشاطر والمقيم حالياً في تركيا، كما يتبين من التحريات أن تلك الشركات قامت بتجنيد شباب تتراوح أعمارهم بين ٢٥-٥٠ سنة مقابل ٥٠ دولار في اليوم، وتبين أن هؤلاء الشباب منهم من ليست له توجهات سياسية ويعمل كأجير باليومية، ومنهم من يرتبط بعلاقة مباشرة بالإخوان[١].

كما تمكنت الأجهزة الأمنية مؤخراً من القضاء على إحدى اللجان الإلكترونية التركية الإعلامية والتي اتخذت إحدى الشقق بمنطقة باب اللوق كمركز لنشاطها المناوئ للدولة تحت غطاء شركه "استيا" للدراسات والتي أسستها جماعة الإخوان بدعم من تركيا[٢].

فضلاً عن ذلك فهناك أمثلة للإرهاب إلكتروني تتمثل في تنفيذ هجمات إرهابية افتراضية على المواقع الإلكترونية المهمة، وذلك لسرقة أرقام بطاقات الائتمان أو استهداف البنية التحتية للدولة التي تعتمد على الخدمات الرقمية بهدف تعطيلها، أو مهاجمة أهداف اقتصادية لإيقافها عن العمل[٣].

ومما سبق يتبين أن الإرهاب الإلكتروني له أثر كبير على الأمن القومي لدول الربيع العربي، ومنها مصر، وذلك من خلال استغلاله للأوضاع الاقتصادية والسياسية فيها، حيث أنه مع التطور المعرفي والتكنولوجي لدى الجماعات الإرهابية، ظهر قصور الأمن القومي عن حماية كافة المجالات للدولة، كما أن الفضاء الإلكتروني قد تجاوز الحدود التقليدية للدولة وأصبح هناك وفرة في المعلومات والأفكار، وبذلك لم يعد مفهوم الأمن قومي متعلق بالكيان المادي بل أصبح مفهوم جديد يدور في فُلك الحفاظ على سلامة الدولة في ظل التطورات التكنولوجية والمعلوماتية.

---

(١) عمر النقيب، تفاصيل سقوط أكبر خلية إرهابية إلكترونية في مصر، موقع (٢٤)، منشور في ٢٠١٩/٤/٨، تاريخ الدخول ٢٢/١٠/١ متاح على: https://24-ac/articlo/4999.

(٢) أشرف عبد الحميد، مصر تكشف تفاصيل القبض على خلية إلكترونية مدعومة تركياً، منشوره في ٢٠٢٠/١/١٥، تاريخ الدخول ٢٠١٢/١٠/٢ على الرابط: https://ara.tv/543pdf.

(٣) يوسف ابن أحمد الرميح، الإرهاب والإعلام الجديد، الإرهاب الرقمي، موقع جريدة الجزيرة، منشور في ٢٠١٥/٣/٧، تاريخ الدخول ٢٠٢٢/١٠/٣ على الرابط: http://www.al-jazirah.com/ 20150307/arlhhm.

الخاتمة:

تناول الباحث في هذا البحث موضوع "الجرائم المعلوماتية المهددة للأمن القومي المصري"؛ حيث قَسم الباحث البحث إلى أربعة مباحث، تناول: المبحث الأول- ماهية الجرائم المعلوماتية وذلك من خلال تقسيمه إلى ثلاثة مطالب، تناول المطلب الأول- تعريف الجرائم المعلوماتية، والمطلب الثاني- خصائص الجرائم المعلوماتية، المطلب الثالث- صور الجرائم المعلومات المعلوماتية، وقد جاء المبحث الثاني- متناولاً جرائم الإرهاب الإلكتروني، وذلك من خلال تقسيمه إلى مطلبين، المطلب الأول- مفهوم الإرهاب، والمطلب الثاني- الإرهاب الإلكتروني، أما المبحث الثالث- فتناول الإرهاب والمواجهة الأمنية، وتم تقسيمه إلى مطلبين، المطلب الأول- طرق استخدام الإنترنت في أغراض إرهابية، المطلب الثاني- المواجهة الأمنية للجرائم المعلوماتية.

وقد جاء المبحث الرابع- فتناول الأمن القومي المصري، وتم تقسيمه إلى ثلاثة مطالب، المطلب الأول- مفهوم الأمن القومي، المطلب الثاني- بعض الجرائم المعلوماتية التي تهدد الأمن القومي المصري، المطلب الثالث- الإرهاب الإلكتروني وتهديد الأمن القومي المصري، وقد اختتم البحث بعدد من النتائج والتوصيات.

أولاً- النتائج:

توصل البحث إلى مجموعة من النتائج، من أهمها:

١. إن الجرائم المعلوماتية وما يعتريها من إشكاليات ومعوقات تمثل خطراً يهدد الاستقرار الدولي والأمن الداخلي للدول، وللجرائم المعلوماتية صوراً مختلفة وتعتبر جرائم الإضرار بالبيانات أشدها خطورة وتأثيراً وأكثرها تحقيقاً للخسائر للأفراد والمؤسسات على حد سواء.

٢. يعتبر الإرهاب الإلكتروني من أهم الجرائم المعلوماتية التي تهدد الأمن القومي للدول وبخاصة الدول المستهدفة مثل مصر، وهو عابر للحدود، لأنه يقع بين أكثر من دولة وهذا يؤدي إلى صعوبة إثبات هذا النوع من الجرائم المعلوماتية.

٣. تعتبر أهم أهداف الإرهاب الإلكتروني هي تدمير الأمن القومي للدول في الداخل والخارج.

٤. ضرورة المواجهة الأمنية للجرائم المعلوماتية مع مراعاة الاختلاف فيما تثيره تقنية المعلومات من مشكلات في مجال جمع الأدلة والإثبات ومشروعية الإجراءات التي تقوم بها أجهزة الأمن.

٥. تمثل جريمة الاعتداء على الأنظمة المعلوماتية للدولة المصرية من أهم الجرائم التي تهدد الأمن القومي المصري، ولذا حدد القانون المصري رقم ١٧٥ لسنة ٢٠١٨ العقوبات المناسبة لها.

٦. أهمية مواجهة الإرهاب الإلكتروني، وخاصة أن المجتمع المصري يواجه مشكلات حقيقية ومتعددة في قضية الإرهاب بصفة عامة والإرهاب الإلكتروني بصفة خاصة.

٧. ضرورة بذل الجهود لمواجهة تحديات التطرف والعنف الإلكتروني من خلال الحد من سوء استغلال شبكة المعلومات والخدمات الإلكترونية المصاحبة لهذه الجهود، **ومن هذه التحديات:**

أ. **التحديات الأمنية:** وتتمثل في نقص الخبرات الفنية في مجالات تحديد أركان الجريمة المعلوماتية وتقديمها كقضية مكتملة أمام مؤسسات الدولة، بالإضافة إلى صعوبة الرصد والتحقق من هذه القضايا.

ب. **التحديات الفكرية والثقافية:** لأن الثقافات والمعلومات الفكرية أصبح الوصول إليها يتم بسهولة عبر شبكة الإنترنت، وأن ما يُعد جريمة في تشريع معين قد لا يكون بالضرورة جريمة في تشريع أخر، وهذا جعل من الصعوبة المعالجة الفكرية الشرعية لاختلاف التفسيرات للجريمة من ثقافة لأخرى.

ج. **التحديات القانونية والتشريعية:** تتمثل هذه التحديات في عدم استيعاب التشريعات والأنظمة للجرائم الفكرية المستحدثة عبر شبكة المعلومات، بالإضافة إلى تنازع القوانين وعدم وضوح الاختصاص القضائي في هذه الجرائم، وصعوبة وضع معايير واضحة لتحديد الموقع المتطرف أو المحرض على العنف أو اختراق الأمن القومي المصري.

٨. زيادة التطور التكنولوجي الهائل تم توظيفه من بعض الدول في أعمال مهددة للأمن القومي المصري على الرغم من بذل الأمن جهوداً كثيرة لمواجهة هذا التهديد.
٩. هناك تحدي للتنظيم القانوني للهجمات الإلكترونية بسبب عدم وجود إرادة دولية خاصة من قِبل الدول المهيمنة في هذا المجال، لأن مثل هذه الجرائم المعلوماتية تمثل مصالح استراتيجية لهذه الدول.

ثانياً- التوصيات:

١. ضرورة وضع مفهوم دولي موحد للإرهاب بصفة عامة، والإرهاب الإلكتروني بصفة خاصة لمنع الاستغلال السيء للمفهوم الحالي الذي يكيل بمكيالين.
٢. تشكيل فريق من المتخصصين من رجال الأمن لرصد ومتابعة المواقع التكفيرية المتطرفة ومواجهتها، ونشر مواقع إلكترونية ذات استقلال فكري عن تجاذبات التيارات الفكرية والمصالح السياسية.
٣. تفعيل قوانين مكافحة الجرائم المعلوماتية من أجل تجفيف منابع الأفكار المتطرفة والإرهابية التي تهدد الأمن القومي للدولة المصرية.
٤. ضرورة التنسيق العربي والدولي في مكافحة الإرهاب، وتشجيع قيام اتحادات عربية تسعى للتصدي لجرائم الإرهاب الإلكتروني.
٥. تفعيل المكافحة الوقائية للحماية من الإرهاب الإلكتروني، وذلك من خلال تفعيل دور المؤسسات التوعوية بالمجتمع المصري.
٦. إنشاء مراكز بحثية بالمدارس والجامعات تهتم وتحافظ على الأمن المعلوماتي، وتواجه أي محاولات للنيل من الأمن القومي المصري.
٧. تفعيل دور المجتمع المدني للقيام بدوره في وقاية الشباب من الوقوع في الجرائم المعلوماتية اللاأخلاقية عبر شبكة الإنترنت.
٨. تعديل بعض أحكام القانون رقم (١٧٥) لسنة ٢٠١٨ في شأن مكافحة تقنية المعلومات، وذلك بهدف التزام الدقة في تحديد الأفعال المعاقب عليها، وتجنب غموض الصياغة التشريعية، ووضع تعاريف دقيقة لها، وتغليظ العقوبات فيما يرتبط بجرائم تقنية المعلومات.
٩. استحداث بعض نصوص القانون لسد الثغرات ومواكبة سرعة التطور التكنولوجي وأدواته.
١٠. فهم وإدراك طبيعة القضاء الإلكتروني واعتباره عنصر رئيس في الأمن القومي المصري، إذ أن له علاقة وطيدة بقضايا التنمية السياسية والاقتصادية والاجتماعية، وضرورة إدماجه في العقيدة الأمنية للدولة المصرية.

قائمة المراجع

أولاً- المراجع العربية:

١. UNODC، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، استخدام الإنترنت في أغراض إرهابية، الأمم المتحدة، نيويورك، ٢٠١٣.

٢. أحمد خليفة الملط، الجرائم المعلوماتية، الإسكندرية، دار الفكر الجامعي، ٢٠٠٥.

٣. أحمد ضياء، مشروعيه الدليل في المواد الجنائية، رساله دكتوراه، كلية الحقوق، جامعة عين شمس، ١٩٨٣.

٤. أشرف عبد الحميد، مصر تكشف تفاصيل القبض على خلية إلكترونية مدعومة تركياً، منشوره في ٢٠٢٠/١/١٥، تاريخ الدخول ٢٠١٢/١٠/٢ على الرابط:
https://ara.tv/543pdf.

٥. أمير محمد محمد، استراتيجيات مكافحة الجرائم الإلكترونية في العصر المعلوماتي تعزيزاً لرؤيه مصر ٢٠٣٠، دراسة استشراقية، مجلة البحوث الإعلامية، كليه الإعلام، جامعة الأزهر، العدد (٥٨)، الجزء (٤)، يوليو ٢٠٢١.

٦. أمين هويدي، الأمن العربي في مواجهة الأمن الإسرائيلي، دار الطباعة، بيروت، ١٩٧٥.

٧. إيمان بكر أبو الهوى، التهديدات الإسرائيلية الأمن القومي والمائي العربي: دراسة حالة إسرائيل ونهر الأردن في الفترة من ١٩٩٤-٢٠١٠، رساله ماجستير غير منشورة، كليه الحقوق، جامعه القاهرة ،٢٠١١.

٨. أيمن عبد الحفيظ، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، القاهرة، دار النهضة العربية، ٢٠٠٥.

٩. أيمن عبد الله فكري، جرائم نظم المعلومات- دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، ٢٠٠٦.

١٠. باتريك سيل، أبو نضال، بندقية للإيجار، المناضلون في خدمات الموساد، مراجعة: أحمد رائف، القاهرة، دار الزهراء للإعلام العربي، ١٩٩٣.

١١. بيتر غرابوسكي، جرائم الحاسب الآلي، الأبعاد العالمية في القيادة العامة لشرطة أبو ظبي، شبكات الإنترنت وتأثيراتها الاجتماعية والأمنية، مركز البحوث والدراسات الأمنية، القيادة العامة لشرطه أبو ظبي، ٢٠٠٦.

١٢. حامد ربيع، نظرية الأمن القومي العربي، القاهرة، دار الموقف العربي، ١٩٨٤.

١٣. الحكم الصادر بتاريخ ٤ مايو ٢٠١٢ عن محكمة باريس الابتدائية في القضية رقم ٠٩٢٦٦٣٩٠٣٦ (الفرقة الرابعة عشر/٢)، باريس.
١٤. ذكي أمين حسونه، جرائم الكمبيوتر والجرائم الأخرى في مجال التكنولوجيا المعلوماتية، القاهرة، دار النهضة العربية، ١٩٩٤.
١٥. رائد حسنين، السياسة الإسرائيلية في أفريقيا، دار ابن رشد للنشر، مؤسسة مدارك، بيروت، ٢٠١٨.
١٦. زكريا حسين، مذكرات في الأمن القومي، كلية التجارة، جامعة الإسكندرية، ٢٠٠١.
١٧. سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، القاهرة، دار النهضة العربية، القاهرة، ١٩٩٩.
١٨. السيد عاشور، الإدارة العلمية والمعلومات، الجمعية المصرية للحاسب الآلي، ٢٠٠٠.
١٩. عبد الحسين شعبان، والتطرف والإرهاب، إشكاليات نظرية وتحديات عملية (مع إشارة خاصة إلى العراق)، كراسات علمية محكمة، وحدة الدراسات المستقبلية، برنامج الدراسات الاستراتيجية مكتبة الإسكندرية، ٢٠١٦.
٢٠. عبد الرحمن عبد الله، وسائل الإرهاب الإلكتروني، حكمها في الإسلام وطرق مكافحتها، اللجنة العلمية للمؤتمر التالي من مواقف الإسلام من الإرهاب، ٢٠٠٤.
٢١. عبد الفتاح مجازي، مبادئ الإجراءات الجنائية في جرائم الحاسب الآلي والإنترنت، دار الكتب القانونية، المحلة الكبرى، ٢٠٠٧.
٢٢. عبد الله عبد العزيز العجلان، الإرهاب الإلكتروني في عصر المعلومات، المؤتمر الدولي لحماية أمن المعلومات، القاهرة، من ٢-٣ يونيو، ٢٠٠٨.
٢٣. عبد الله عبد العزيز العجلان، الإرهاب الإلكتروني في عصر المعلومات، المؤتمر الدولي لحماية أمن المعلومات، القاهرة، من ٢-٣ يونيو، ٢٠٠٨.
٢٤. عبد الوهاب الكيالي، موسوعة السياسة، المؤسسة العربية للدراسات والنشر، دار الهدى للنشر والتوزيع، بيروت، ج (١)، ٢٠٠٧.
٢٥. علي الدين هلال، الأمن القوم العربي: دراسة في الأصول، مجلة شئون عربية، العدد (٣٥)، يناير ١٩٨٤.
٢٦. علي الشهري، رؤيه استراتيجية لمكافحة الجرائم الإلكترونية تعزيزاً للأمن الإنساني، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، كليه العلوم الاستراتيجية، ٢٠١٩.
٢٧. عمر النقيب، تفاصيل سقوط أكبر خلية إرهابية إلكترونية في مصر، موقع (٢٤)، منشور في ٢٠١٩/٤/٨، تاريخ الدخول ٢٢/١٠/١ متاح على: https://24-ac/articlo/4999.

٢٨. العهد الدولي الخاص بالحقوق المدنية والسياسية، قرار الجمعية العامة ٢٢٠٠ ألف (د-٢١)، الفقرة ٢ من المادة ١٩.
٢٩. العين عبد الله آل العيون، الأمن الوطني الأردني، جريدة الرأي، بتاريخ ٢٠١٦/٥/٢٥، تاريخ الدخول ٢٢/٠٩/١٠ على الرابط التالي:
http://alrai.com/article/789414.html
٣٠. فرانك بولتر، الإرهاب.... ما بين المفهوم التقليدي والحروب الإلكترونية، ترجمة: هشام الحناوي، المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات، ب.ت، تاريخ الدخول: http://www europarabct.com .
٣١. قارن نصوص القرارات الدولية التي أصدرت بعد أحداث ١١ سبتمبر ٢٠٠١، عبد الحسين شعبان، الإسلام والإرهاب الدولي، ثلاثية الثلاثاء الدامي: الدين، القانون، السياسة، لندن، دار الحكمة، ٢٠٠٢.
٣٢. قانون رقم ١٧٥ لسنة ٢٠١٨، الجريدة الرسمية، العدد (٣٢) مكرر، في ١٤ أغسطس، سنة ٢٠١٨، ص ٣.
٣٣. القانون رقم ١٧٥ لسنة ٢٠١٨، ص ٣١.
٣٤. المادة (٥١) من ميثاق الأمم، المتحدة الفصل السابع، نيويورك، للأمم المتحدة، ٢٠١٢.
٣٥. مجدي فؤاد، الجريمة المعلوماتية وحماية حقوق الملكية الفكرية، بحث غير منشور، ٢٠٠٩.
٣٦. محمد أبو الفتوح الغانم، الإرهاب وتشريعات المكافحة في الدول الديمقراطية، القاهرة، دار النهضة العربية، ١٩٩١.
٣٧. محمد الأمين البشرية، التحقيق في الجرائم المستحدثة، الطبعة الأولى، جامعه نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٤.
٣٨. محمد زكي أبو عامر، الإجراءات الجنائية في التشريع المصري، الجزء الأول، دار النهضة العربية، القاهرة، ٢٠٠١.
٣٩. محمد عبد اللطيف فرج، التكنولوجيا الحديثة وجرائم غسل الأموال، بحث غير منشور، ٢٠٠٩.
٤٠. محمد علي قطب، الجرائم المعلوماتية وطرق مواجهتها، ج (٢)، مملكة البحرين، وزارة الداخلية، الأكاديمية الملكية للشرطة،٢٠١٠.
٤١. محمد قطب، الجرائم المستحدثة وطرق مواجهتها، قراءه في المشهد القانوني والأمني وعلاقته بالشريعة الإسلامية، دار الفجر للنشر والتوزيع، ٢٠٠٩.

٤٢. محمد محيي عوض، مشكلات السياسة الجنائية المعاصرة، جرائم نظم المعلومات، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، ١٩٩٤.
٤٣. محمد يحيى الدين عوضين، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات، القاهرة، دار النهضة العربية، ١٩٩٣.
٤٤. ميادة بشير، يوسف عثمان، توظيف برامج العلاقات العامة في التوعية بمخاطر الجرائم الإلكترونية، دراسة تحليلية ووصفية على الإدارات المسؤولة عن الجرائم الإلكترونية، وزاره العدل، وزاره الداخلية، وزاره الاتصالات وتكنولوجيا المعلومات في الفترة بين ٢٠١٦-٢٠١٧، مجله العلوم الإنسانية، المجلد (١٩)، العدد (٢)، ٢٠١٨.
٤٥. نائلة عادل محمد فريد، جرائم الحاسب الآلي الاقتصادية- دراسة نظرية وتطبيقية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، ٢٠٠٣.
٤٦. نبيل عبد المنعم جاد، أسس التحقيق والبحث الجنائي العملي، أكاديمية الشرطة، مطبعة كلية الشرطة، القاهرة، ٢٠٠٥.
٤٧. نعوم تشومسكي، القوة والإرهاب: جذورهما في عمق الثقافة الأمريكية: ترجمة: يحيى الشهابي، دمشق، دار الفكر، ٢٠٠٣.
٤٨. هشام بشير، الإرهاب الإلكتروني في ظل الثورة التكنولوجية وتطبيقاته في العالم العربي، آفاق سياسية، العدد (٤)، القاهرة، المركز العربي للبحوث والدراسات، ٢٠١٤.
٤٩. هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط، ١٩٩٤.
٥٠. ولد الصديق ميلود، مكافحه الإرهاب بين مشكلة المفهوم واختلاف المعايير، ج (١)، مركز الكتاب الأكاديمي، عمان، ٢٠١٧.
٥١. يوسف ابن أحمد الرميح، الإرهاب والإعلام الجديد، الإرهاب الرقمي، موقع جريدة الجزيرة، منشور في ٢٠١٥/٣/٧، تاريخ الدخول ٢٠٢٢/١٠/٣ على الرابط: http://www.al-jazirah.com/ 20150307/arlhhm.

ثانياً- المراجع الأجنبية:

1. Alex, P., Schmid & Albert, J., Jongman, Political Terrrorism: a Research to Concepts, Theories, Data Bases and Literature, COMT-Publication 12, New Brunswick, NJ: Transaction Books, 1984.
2. Alkalei, A., A Strategic, Vision to Reduce Cyber-crime and enhance Cyber Security, International Journal of Advance Science and Technology, Vol. 29, No. 7, 2020, pp. 12-30.
3. Also, M. N., Ogun, P., Terrorism Schmid of Cyberspace and Cyber Terrorism: New Challenges and Responses, IOS Press, 2015.
4. Die, Bundesregiering, Digital Agenda 2014-2017, 2014, pp. 1-40.
5. Gabriel Weimann, Online Terrorists Prey on the Vulnerable, yale Global on line, 5 March 2008. http://yaleglobalyale.edu/content/online-terrorists-prey-vulnerable.
6. Gabriel Weimann, Terror on the internet: the new Arena, the new challenges, washing, D.C, United State Institute of Peace Press, 2006, pp. 37-38.
7. Handbook of Internet Crime, Dorothy E denning, terror's web: how the Internet is Transforming terrorism, Y nonne Jewhes and majidyar, eds, cullompton, United Kingdom, Willan Publishing, 2010.
8. Maura Conway, Terrorist, use of Internet and fighting back, information & Security, Vol. 19, 2006, pp. 12-14.
9. Mohammed Aldhamdi, A Strategic, Vision to reduce Cyber-crime to enhance Cyber Security, Webology, Vol. 17, No. 2, December 2020, pp. 289-295.

10. The McGraw-Hill Homeland, Scott Gerwehr Daly, Al Qaida: Terrorist Selection and Recuitment, Security Handbook, David Kamien, ed., New York, McGraw-Hill, 2006.