أثر الجرائم الإلكترونية على أمن واستقرار الدول : قرصنة الموقع الإلكتروني لوكالة الأنباء القطرية أنموذجا

الباحثة صباح كزيز
طالبة دكتوراه علوم – علاقات دولية واستراتيجية
قسم العلوم السياسية والعلاقات الدولية
kezizsp@gmail.com

الدكتور سمير قط
أستاذ محاضر "ب"
جامعة محمد خيضر – بسكرة (الجزائر)
sgatt@yahoo.fr

الملخص:

تعتبر ظاهرة الجريمة الإلكترونية العابرة للحدود من التهديدات الأمنية الجديدة التي تواجه الدولة خصوصا في الآونة الاخيرة، لأنها تمس أو تهدد جانب أساسي من أمنها وتزعزع استقرارها، حيث تعتمد هذه الجريمة بالأساس على وسائل الاتصال المتطورة وأدوات التقنية الحديثة في خلق أشكال جديدة من الأزمات في الدولة أو الدول المستهدفة، ما يستدعي البحث في تداعيات هذه الظاهرة على الأمن الوطني للدول في ظل تنامي مخاطر التكنولوجيا الرقمية .

بحث هذه الدراسة بداية في العلاقة بين التكنولوجيا والأمن من منطلق أن أمن المعلومات الإلكترونية أصبح يصنف كجزء مهم في أي سياسة أمنية وطنية، من ناحية ثانية تبحث الدراسة في أشكال ومخاطر الجرائم الإلكترونية على أمن الدول، انطلاقا من أن البنية التحتية لأغلب المجتمعات تدار عبر أدوات التقنية الحديثة، ما جعلها تواجه تحديات جديدة عابرة للحدود تنبع من الأنشطة غير المشروعة عبر شبكة الإنترنت. من جهة ثالثة نحاول تسليط الضوء على قرصنة الموقع الإلكتروني لوكالة الأنباء القطرية كأحد أبرز الأمثلة على الجرائم الإلكترونية التي تمس الاستقرار والأمن الوطني للدول.

Abstract:

The phenomenon of transnational cyber-crime is one of the new security threats facing the state, especially in recent times, As it affects and threatens a fundamental aspect of its security and destabilization. This crime is mainly based on advanced means of communication and modern technology tools in creating new forms of crisis in the country or target countries. Hence the importance of the study in exposing the risks and implications of this phenomenon to the national security of countries in light of the growing risks of digital technology.

This study examines of the relationship between technology and security. On the grounds that the security of electronic information has been classified as an important part of any national security policy, On the other hand, the study examines the forms and risks of cybercrime on the security of States, Since the infrastructure of most societies is managed through the tools of modern technology, Making it face new cross-border challenges stemming from illegal activities over the Internet. On the third hand, we are trying to highlight the piracy of the website of the Qatar News Agency as one of the most prominent examples of cyber-crimes affecting the stability and national security of countries.

مقدمة:

بالنظر لتعدد العمليات الإلكترونية كأثر مترتب على الثورة المعلوماتية وسهولة تقديم الخدمات العامة عن طريق الوسائل الإلكترونية، والتي تدور في فلك شبكة الإنترنت، غير أن رواج العمليات الإلكترونية واكبها ظهور آثار سلبية مجسدة في الجرائم المستحدثة التي ترتكب عن طريق النظم والأدوات التقنية، وهي جرائم عابرة للحدود لا تتمركز في دولة أو مجتمع محدد بل تعبر الحدود لتهدد دول ومجتمعات عديدة، خصوصا وأن العالم اليوم يوصف بأنه " قرية عالمية" نتيجة التطور المذهل في وسائل الاتصالات وتقنية المعلومات، هذا النوع من الإجرام يطرح الكثير من الصعوبات والتحديات أمام الدولة أو الدول المستهدفة خصوصا فيما يتعلق بالقدرة على اكتشاف هذه الجرائم وإثباتها.

من هنا تبرز أهمية هذه الدراسة في كونها ترتكز على تحليل ظاهرة على درجة كبيرة من الخطورة والتي تتمثل أساسا في الجرائم الإلكترونية، تزداد خطورة هذه الظاهرة عندما ترتبط بأهداف أطراف خارجية تسعى بطريقة غير مباشرة إلى خلق أزمات للدولة المستهدفة، ولهذا الغرض تم تناول عملية القرصنة التي تعرض لها الموقع الإلكتروني لوكالة الأنباء القطرية كأنموذج لهذه الدراسة.

وتهدف الدراسة إلى تحديد ومعرفة طبيعة وصور هذه الجرائم مع بيان للصعوبات التي قد تواجه استقرار وأمن الدول أمام التنامي المتزايد للظاهرة، إضافة إلى ما يترتب من إشكالات أمنية، سياسية، قانونية، اقتصادية واجتماعية معقدة.

من هنا تُثار إشكالية أمن واستقرار الدول في ظل إنشار الجريمة الإلكترونية التي تعد من الظواهر العالمية الخطيرة التي أضحت تمثل معضلة أمنية لدى الدول، فتنوع هذه الجرائم وانتشارها يشكل تهديد كبير تواجهه الدول الساعية إلى حفظ الأمن والاستقرار الوطني والإقليمي والدولي على حد سواء، الأمر الذي يدعو إلى ضرورة البحث في التأثيرات والتداعيات التي تترتب عن الظاهرة بأشكالها وصورها المختلفة، من هنا تحدد إشكالية الدراسة في:

- كيف تؤثر الجريمة الإلكترونية على أمن واستقرار الدول؟

وتنطلق الدراسة فرضية أساسية مفادها:

- تتحدد خطورة الجريمة الإلكترونية على أمن واستقرار المجتمعات في كونها جريمة عابرة للحدود تستهدف الاختراق الأمني للمؤسسات العامة والحيوية للدولة المستهدفة.

تتهيكل الورقة البحثية في محاور ثلاثة، على النحو التالي:

المحور الأول: مقاربة مفاهمية لمتغيرات الدراسة

أولا : الجريمة الإلكترونية (المفهوم والخصائص)

ثانيا: الارتباط بين الأمن الإلكتروني والأمـن الوطني

المحور الثاني: الجريمة الالكترونية كتهديد لأمن الدول وسبل مواجهتها

أولا: إشكالية أمن واستقرار الدول على ضوء مخاطر الجرائم الإلكترونية

ثانيا: متطلبات تحقيق الأمن الإلكتروني والتصدي للجرائم المستحدثة

المحور الثالث: قرصنة الموقع الإلكتروني لوكالة الأنباء القطرية " قنا "

أولا- فبركة تصريحات ونسبها لأمير دولة قطر بعد قرصنة موقع " قنا "

ثانيا- التحقيقات والنتائج حول تفاصيل عملية القرصنة

المحور الأول: مقاربة مفاهمية لمتغيرات الدراسة

يعتبر هذا المحور القاعدة النظرية للموضوع الذي نسعى لمعالجته، لذا حاولنا من خلاله ضبط الجانب النظري والمفاهيمي لمتغيرات الدراسة، وذلك على النحو الاتي:

أولا- الجريمة الإلكترونية (المفهوم والخصائص):

1- تعريف الجريمة الإلكترونية :

طرأت تغييرات كبيرة على أسلوب عمل المجرمين في العقد الأول من القرن الحادي والعشرين[1]، حيث تعتبر الجريمة الإلكترونية من الآثار السلبية التي خلفتها التقنية العالية حيث أخذت هذه الظاهرة الإجرامية حيزا كبيرا من الدراسات من أجل تحديد مفهومها مما انجر عنه وضع عدد من المصطلحات للدلالة عليها كجرائم التقنية العالية وجرائم المعلوماتية وجرائم الإنترنت، الجرائم المستحدثة...الخ [2]، ويتكون مصطلح الجريمة الإلكترونية أو الافتراضية (*cyber-crimes*) من مقطعين هما الجريمة (*crime*) والإلكترونية(*cyber*) ويستخدم مصطلح الإلكترونية لوصف فكرة جزء من الحاسب أو عصر المعلومات، أما الجريمة فهي السلوكيات والأفعال الخارجة على القانون[3]. كما تعرف

[1]- منظمة الإنتربول، "مكافحة الجريمة في القرن الواحد والعشرين 2000- 2010"، تقرير صادر عن الإنتربول، فرنسا، 2010، ص 2.

[2]- يوسف صغير، "الجريمة المرتكبة عبر الأنترانت،" مذكرة ماجستير في تخصص القانون الدولي للأعمال، (قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، 2010)، ص 7.

[3]- ذياب موسى البدانية،"الجرائم الالكترونية: المفهوم والأسباب"، ورقة بحثية ضمن فعاليات المؤتمر العلمي حول: (الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، كلية العلوم الاستراتيجية، عمان، الأردن، أيام 2-7 سبتمبر 2013).

الجريمة أيضا بأنها أي سلوك سيء متعمد يتسبب في إلحاق الضرر بالضحية أو ينتج عنه حصول الجاني على كسب أو فائدة لا يستحقها.[1]

وقد عرف مكتب تقييم التقنية في الولايات المتحدة الأمريكية الجريمة المستحدثة (الإلكترونية) بأنها "الجرائم التي تقوم فيها بيانات الحاسب الآلي والبرامج المعلوماتية بدور رئيسي"، كما عرفت أيضا بأنها "نشاط جنائي يمثل اعتداء على برامج وبيانات الحاسب الإلكتروني"، وعرفها أيضا بأنها " كل استخدام في صورة فعل أو امتناع غير مشروع للتقنية المعلوماتية، ويهدف إلى الاعتداء على أي مصلحة مشروعة، سواء أكانت مادية أو معنوية".[2]

أما الفقيه الألماني تاديمان (*Tiedemaun*) فقد عرفها بأنها "كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب باستخدام الحاسب".

وتعرفها منظمة التعاون الاقتصادي والتنمية بأنها "كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن الاستخدام غير المشروع لتقنية المعلومات.[3]

بناء على ما سبق يمكن القول أن الجريمة الإلكترونية هي كل : الأفعال أو نشاطات غير المشروعة، تكون وسيلة تقنية المعلومات محلا لها أو أداة للقيام بها.

2- خصائص الجريمة الإلكترونية:

تتميز الجرائم المرتكبة بواسطة الكمبيوتر كأداة أو كهدف للجريمة بالخصائص التالية :[4]

---

[1]- حسن طاهر داود، جرائم نظم المعلومات، الرياض: أكاديمية نايف العربية للعلوم الامنية، 2000، ص 23.

[2]- مفتاح بوبكر المطردي، "الجريمة الإلكترونية والتغلب على تحديات"، ورقة بحثية ضمن فعاليات المؤتمر العلمي الثالث (لرؤساء المحاكم العليا في الدول العربية، السودان، أيام 23- 25 سبتمبر 2012)، ص 3.

[3]- هشام محمد فريد رستم، "الجرائم المعلوماتية: أصول التحقيق الجنائي الفني"، ورقة بحثية مقدمة ضمن فعاليات المؤتمر العلمي حول: (القانون والكمبيوتر والإنترنت، مركز الإمارات للدراسات والبحوث الاستراتيجية، الإمارات العربية المتحدة، 2004)، ص ص 405-409.

[4]- عبد العال الديربى، "الجريمة المعلوماتية: تعريفها.. أسبابها.. خصائصها"، المركز العربي لأبحاث الفضاء الإلكتروني، 2016/12/11، متوفر على الرابط الإلكتروني:
http://accronline.com/article_detail.aspx?id=7509

أ- سرعة التنفيذ:

لا يتطلب تنفيذ الجريمة عبر الكمبيوتر الوقت الكبير ولكن هذا لا يعني أنها لا تتطلب الإعداد قبل التنفيذ أو استخدام معدات وبرامج معينة.

ب- التنفيذ عن بعد:

بحيث يمكن للفاعل تنفيذ جريمته وهو في دولة بعيدة كل البعد عن الفاعل سواء كان من خلال الدخول للشبكة المعنية أو اعترض عملية تحويل مالية أو سرقة معلومات هامة أو تخريب...الخ.

ج- عابرة للدول:

إن ربط العالم بشبكة من الاتصالات من خلال الأقمار الصناعية والفضائيات والإنترنت جعل الانتشار الثقافي وعولمة الثقافة والجريمة أمرا ممكنا وشائعا، لا يعترف بالحدود الإقليمية للدول ولا بالمكان، ولا بالزمان، ففي مجتمع المعلومات تلغى الحدود الجغرافية بين الدول لارتباط العالم بشبكة واحدة.

د- جرائم ناعمة:

تتطلب الجريمة التقليدية استخدام الأدوات والعنف أحيانا كما في جرائم الإرهاب والمخدرات، والسرقة والسطو المسلح، غير أن الجرائم المتصلة بالكمبيوتر تمتاز بأنها جرائم ناعمة لا تتطلب عنفا، فنقل بيانات من كمبيوتر إلى أخر أو السطو الإلكتروني على أرصدة بنك ما لا يتطلب أي عنف أو تبادل إطلاق نار مع رجال الأمن، كما أن هناك العديد من الجرائم "التقليدية" اتخذت منعطفاً جديداً مع ظهور الإنترنت، مثل الجرائم ضد الأطفال والجرائم المالية وحتى الإرهاب[1].

هـ- صعوبة متابعتها وإثباتها:

تتميز جرائم الإنترنت عن الجرائم التقليدية بأنها صعبة الإثبات، وهذا راجع إلى افتقاد وجود الآثار التقليدية للجريمة، وغياب الدليل الفيزيقي(بصمات، تخريب، شواهد مادية) وسهولة محو الدليل أو تدميره في زمن متناه القصر، وبذلك يصعب متابعة جرائم الانترنت والكشف عنها وإقامة الدليل عليه، فهي جرائم تتسم بالغموض، فعولمة هذه الجرائم يؤدي إلى تشتيت جهود التحري والتنسيق الدولي لتعقب مثل هذه الجرائم، فهذه الجرائم هي صورة صادقة من صور العولمة، فمن حيث المكان يمكن ارتكاب هذه الجرائم عن بعد وقد يتعدد هذا المكان بين أكثر من دولة ؛ ومن الناحية الزمنية تختلف

[1]- *"Cybercriminalité" , 2018/05/11, in site internet: https://www.interpol.int/Crime-areas/Cybercrime*

المواقيت بين الدول، الأمر الذي يثير التساؤل حول: (تحديد القانون الواجب التطبيق على هذه الجريمة؟). [1]

ثانيا- الارتباط بين الأمن الإلكتروني والأمن الوطني:

يتفق معظم المؤلفين والباحثين على أن مفهوم الأمن الوطني مفهوم مثير للجدل والنقاش، وهناك شبه إجماع على أن الأمن يقصد به عدم وجود تهديد للقيم الرئيسية سواء فيما يتعلق بالفرد أو المجتمع وبالتالي هناك خلاف رئيسي حول ما إذا كان التركيز ينصب على أمن الأفراد أو الدول أو العالم ككل.[2] وفي ظل ما يشهد العالم من بروز لمتغيرات جديدة وتحولات حاصلة في شتى المجالات خصوصا في مجال التكنولوجية، فكان لها أثر بالغ وانعكاس على مختلف المفاهيم وتطويرها كمفهوم الأمن ومفهوم التهديد، في هذا السياق برزت ظاهرة الجريمة الإلكترونية كتهديد خطير يمس بأمن الدول خاصة المتقدمة منها التي تعتمد بشكل كبير على الوسائل التقنية والتكنولوجيا المعلوماتية والاتصال في معظم المجالات، ومن هنا برز مفهوم الأمن الإلكتروني كهاجس للدول في سياساتها الأمنية، كأحد المتطلبات والعناصر الضرورية المتكاملة في منظومة الأمن القومي.

فقد رفعت أغلب دول العالم – بما فيها الدول العربية– شعار التحول إلى مجتمع المعلومات والمعرفة، وتنفذ خططا واسعة النطاق لتحويل هذا الشعار إلى واقع، وفي هذا السياق يتم إنشاء سلاسل من قواعد البيانات القومية الكبرى، كما يجري تطوير شبكات الاتصالات ونشر الإنترنت عبر خطوط الاتصالات العادية والسريعة، كما تنشط الدول في نشر مفاهيم وخدمات الحكومة الإلكترونية، وتصدر قوانين التوقيع الإلكتروني الذى يمهد الطريق صوب تفعيل أنشطة التجارة والأعمال الإلكترونية على نطاق واسع، مع تتبنى العديد من برامج التنمية المعلوماتية المتكاملة في مختلف الوزارات والهيئات والمؤسسات، غير أن تشييد بنية معلوماتية قومية واسعة المجال وتبني التوجه نحو مجتمع المعلومات وضع المجتمع والدولة والمؤسسات أمام تحديات ومخاطر جديدة، فالمجتمع الذي يمتلك بنية معلوماتية واسعة يواجه تهديدات في أمن المعلومات تتسم بالشمول والاتساع وعمق التأثير.[3]

---

[1] – عبد العال الديربى، "الجريمة المعلوماتية: تعريفها.. أسبابها.. خصائصها"، مرجع سابق.

[2] - *Dario Battistella, Dario Battistella, Théories des relation internationales, 2-ed, Paris press de sciences po, 2006, pp 461,462.*

[3] – جمال محمد غيطاس، "الأمن المعلوماتي والجرائم الإلكترونية.. أدوات جديدة للصراع "، مركز الجزيرة للدراسات، 10 /03/ 2012، متوفر على الرابط الإلكتروني: =

في هذا السياق أصدرت الأمم المتحدة مجموعة من القرارات عبر جمعيتها العامة أظهرت مدى تصاعد الاهتمام العالمي بظاهرة استخدام تكنولوجيا الاتصال والمعلومات والتقنيات الحديثة استخداما سلبي أو غير سلمي، حيث اتخذت بتاريخ 22 نوفمبر 2002 قرارا بشأن التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، تبعه في شهر ديسمبر من نفس السنة قرار أخر حول إرساء ثقافة عالمية لأمن الفضاء الالكتروني(الرقمي) واعتبر من أهم القرارات التي استهدفت العمل على حماية البنية التحتية الحيوية للمعلومات وحث الدول والمنظمات الدولية والإقليمية على تكثيف التعاون الدولي لمجابهة الجرائم الإلكترونية[1].

فالأمن الإلكتروني أصبح ضرورة قومية وجب على جميع دول العالم إدراجها ضمن سياساتها العامة، نظرا لترابط بين الأمن الوطني بمختلف مجالاته والأمن المعلوماتي، وذلك على النحو الاتي:[2]

1- الأمن الوطني العسكري:

تعمل غالبية الابتكارات العسكرية والتسليحية في وقتنا الحاضر من خلال ربطها بوسائل الاتصال الحديثة، وشبكات الإنترنيت، وقواعد البيانات وأنظمة المعلومات العسكرية والحربية، والتي تمكن مستخدميها من التحكم بها عن بعد، يعد ال محتوى المعلوماتي الرقمي العسكري من أخطر الأبعاد تأثيرًا على الأمن القومي لأي دولةٍ في العالم، نظرًا لحساسية ما يحتويه من معلوماتٍ رقميةٍ والكترونيةٍ عن الجوانب العسكرية والتسليحية للدول؛

2- الأمن الوطني السياسي:

يتلخص هذا المحتوى الأمني بالبيانات الرقمية، والمعلومات الإلكترونية التي تخص الأحزاب في الدولة، إضافة للمعلومات التي تتعلق بالبرلمانات، ورئاسة الدولة، وأجهزتها السيادية، وهي معلوماتٍ حساسةٍ قد تؤدي لحروبٍ أهليةٍ في حال.

=http://studies.aljazeera.net/ar/issues/2012/02/201222913222865296O.htm

[1]- نوران شفيق، أثر التهديدات الإلكترونية على العلاقات الدولية،القاهرة :المكتب العربي للمعارف، 2015، ص 108.

[2]- جمال غيطاس، أمن المعلومات والأمن القومي، القاهرة: شركة نهضة مصر للطباعة والنشر والتوزيع، 2007، ص 27.

3-الأمن الوطني للجهاز الإداري الحكومي:

يتلخص هذا الجانب الأمني والقومي بالخدمات الإلكترونية المقدمة للجماهير، والمتعلقة بأعمال الحكومة الإلكترونية، تقوم هذه الخدمات على عنصر الثقة المتبادلة بين الحكومة ومواطنيها، ذلك يعني أنه في حال تعرض هذه الأعمال للقرصنة، فإن الحكومة تفقد مصداقيتها من قبل مواطنيها، خصوصًا في الدول المتقدمة تقنيا؛ العبث بها؛

4- الأمن الوطني الاقتصادي:

يعد أكثر القطاعات الأمنية والقومية عرضة للهجمات الإلكتروني، نظرا لتحول اقتصاديات العالم إلى كيانات اقتصادية معرفية معتمدة على المعلومات الرقمية، كالبنوك، والبورصات، وغيرها، والتي تشكل في حال التعرض لها خسائر اقتصادية وقومية هائلة؛

5- الأمن الوطني الاجتماعي:

يشكل هذا البعد وجها تعريفيا عن البيانات ونظم المعلومات المخصصة للتعامل مع الحالة الاجتماعية للدولة ككل، كالدراسات الإحصائية والسكانية وغيرها، بحيث تشكل وفي حال الاطلاع عليها بشكلٍ غير قانوني، تهديدا لسلامة المجتمع بأسره؛

6- الأمن الوطني الفكري والثقافي الإعلامي:

يمثل هذا البعد ذروة الإنتاج الفكري لأي دولة في العالم، وهي معلوماتٍ ذات طابعٍ جماعي وفرد ي على حد سواء، كونها تعتمد على وسائل الإعلام الحديثة، والتي قد تساهم في رفع أو خفض مظاهر الأمن القومي لأي دولة، كالمظهر المادي المتعلق باستقرار المواطنين، والذي له علاقة مباشرًة في خفض أو رفع الهواجس الأمنية للدولة؛

7- الأمن الوطني العلمي والبحثي:

يتعلق هذا المحتوى الأمني والوطني بالبيانات والمعلومات الخاصة بالمؤسسات البحثية والعلمية والجامعات، وهي تشكل ثروًة قومية مستقبلية تحوي العديد من الاكتشافات وبراءات الاختراع المعرضة للسرقة أو القرصنة الإلكترونية.

انطلاقا من أن الأمن الإلكتروني يشكل عنصرا مهما في السياسة الأمنية الوطنية للدول، بات معلوما أن صناع القرار خصوصا في الولايات المتحدة الأمريكية، دول الاتحاد الأوروبي، روسيا، الصين وغيرها من الدول، يصنفون مسائل الدفاع الإلكتروني أو الأمن الإلكتروني كأولوية في سياساتهم الدفاعية الوطنية، هذا وقد أعلنت أكثر من 130 دولة حول العالم عن تخصيص أقساما وسيناريوهات خاصة بالحرب الإلكترونية ضمن فرق

الأمن الوطني، تضاف جميع هذه الجهود إلى الجهود الأمنية التقليدية لمحاربة الجرائم الإلكترونية والاحتيال الإلكتروني والأوجه الأخرى للمخاطر السيبرانية. [1]

إذ يشكل الأمن السيبراني مجموع الأطر القانونية والهياكل التنظيمية، وإجراءات سير العمل بالإضافة إلى الوسائل التقنية والتكنولوجية والتي تمثل الجهود المشتركة للقطاعين الخاص والعام، المحلية والدولية والتي تهدف إلى حماية الفضاء الإلكتروني الوطني، مع التركيز على ضمان توافر أنظمة المعلومات وتمتين الخصوصية وحماية سرية المعلومات الشخصية واتخاذ جميع الإجراءات الضرورية لحماية المواطنين والمستهلكين من مخاطر الفضاء الإلكتروني[2].

المحور الثاني: الجرائم الإلكترونية كتهديد لأمن الدول وسبل مواجهاتها

نحاول من خلال هذا المحور البحث في طبيعة الجرائم الإلكترونية ومظاهرها الأساسية، ثم التركيز على معالجة نقطتين أساسيتين: معرفية كيف تؤثر هذه الجرائم على أمن واستقرار الدول؟ وماهي سبل مواجهتها؟

وهذا كالاتي:

أولا- إشكالية أمن واستقرار الدول على ضوء مخاطر الجرائم الإلكترونية :

1- طبيعة الجرائم الإلكترونية وكيف تنعكس على أمن الدول:

أ- جرائم ذات طابع (سياسي – أمني):

يبرز هذا الصنف من خلال التجسس على شخصيات السياسية أو تهديدهم بالقتل أو اختراق مؤسسات عمومية وحيوية للدولة، وفي هذا السياق وقعت عدة حوادث تبين تعرض بعض المراكز العسكرية لجرائم قرصنة معلوماتية بهدف الوصول والحصول على معلومات مخزنة في ذاكرة الحاسبات الآلية المستعملة فيها، وأكبر مثال على ذلك، سرقة معلومات عسكرية تتعلق بالسفن الحربية الخاصة بالدول الأعضاء في حلف شمال الأطلنطي *NATO* وذلك من خلال أنظمة الحاسبات الآلية الخاصة بسلاح البحرية الفرنسية في صيف 1994م.[3]

---

[1]- " الأمن السيبراني "، موقع الهيئة المنظمة للاتصالات، الجمهورية اللبنانية، 2017/12/11، متوفر على الرابط الإلكتروني: *http://www.tra.gov.lb/Cybersecurity-AR*

[2] – المرجع نفسه.

[3] – حسين بن سعيد الغافري، " الجرائم المتعلقة بشبكة الإنترنت مفاهيم وأساليب وخصائص"،2017/11/12، متوفر على الرابط الإلكتروني: *http://www.mouwazaf-dz.com/t30021-topic*

وقد حدث، أيضا، أن تمكن قرصان أمريكي يبلغ من العمر ثمانية عشر عاماً، من اختراق واحدا من أكثر النظم التقنية العسكرية أمانا، وهو الخاص بوزارة الدفاع الأمريكية "البنتاجون" وتسلل عبر ما يسمى "الجدران النارية" (*Fire Wals*) التي وضعت لحماية هذه الشبكة وكان بإمكانه أن يعرض البشرية كلها لخطر الإبادة لو تمكن من مواصلة عمله للنفاذ المخزون النووي الاستراتيجي ومعرفة شفرته، وضبطها نحو اتجاه معين لإطلاق آلاف القنابل النووية. [1]

وفي عام 2010 تم استغلال شبكة الإنترنت العالمية في تسريب وثائق تحوي معلومات وثائق سرية كشفها موقع "ويكليكس"(*WikiLeaks*) حيث كان لهذه الوثائق والموقع نفسه دور فاعل بما حدث في العالم العربي بكشف هذه الوثائق أمور سرية عديدة حول الحكام وحاشيتهم وعن حجم الفساد الموجود في هذه الدول.[2]

وفي شهر ماي 2017 تم اختراق الموقع الرسمي لوكالة الأنباء القطرية، وبث تصريحات (مفبركة) على لسان أمير قطر الشيخ تميم بن حمد آل ثاني، تسبب الأمر في توتر بين دول مجلس التعاون الخليجي وبين قطر والمملكة العربية السعودية بالذات (الأزمة الخليجية).[3]

ب- جرائم ذات طابع اقتصادي:

هذا الصنف من الجرائم يكمن في اختراق النظام المصرفي وإلحاق الضرر بأعمال البنوك وأسواق المال العالمية، والتعرض لعمليات التحويل المالي. ومن اشهر جرائم سرقة الأموال والتي جرت إحداثها في إمارة دبي بدولة الإمارات العربية المتحدة في أواخر عام 2001 ما قام به مهندس حاسبات أسيوي يبلغ من العمر 31 عاما وتم نشر وقائع الجريمة في ابريل من عام 2003 حيث قام بعمل العديد من السرقات المالية لحسابات عملاء في 13 بنكاً محلياً وعالمياً حيث قام باختلاس الأموال من الحسابات الشخصية وتحويل تلك الأموال إلى حسابات وهمية قام هو بتخليقها كما قام أيضا بشراء العديد من السلع

---

[1]- جميل الصغير،مرجع سابق، ص 24.

[2] - منذر أحمد زكي شراب، "السياسة الخارجية القطرية في ظل التحولات السياسية العربية 2003-2012"، مذكرة ماجستير في تخصص دراسات الشرق الأوسط، (قسم التاريخ كلية الآداب والعلوم الإنسانية جامعة الأزهر، 2014)، ص 134.

[3]- سليمان نمر، "أزمة مفتعلة مع قطر"، 2017/12/11، متوفر على الرابط الإلكتروني:
https://www.alaraby.co.uk/opinion

والخدمات عبر شبكة الانترنت مستخدماً بيانات بطاقات الائتمان والحسابات الشخصية لعدد كبير من الضحايا. [1]

ج- جرائم ذات طابع اجتماعي:

الجرائم الإلكترونية تؤثر على حياة المدنيين ورفاهيتهم وحتى ثقافتهم وتستهدف عبر رسائلها للإعلام والجمهور الخاص بالمجتمعات التي تقوم بترويعها وإرهابها، وهذا من خلال:

- الجرائم التي يتم الوصول فيها إلى الهويّة الإلكترونية للأفراد بطرق غير مشروعة؛ كحسابات البريد الإلكتروني وكلمات السر التي تخصهم، وقد تصل إلى انتحالِ شخصياتهم وأخذ الملفات والصور المهمة من أجهزتهم، بهدفِ تهديدهم بها ليمتثلوا لأوامرهم.
- تخريب منظومة العلاقات الاجتماعية وتخريب النسيج الأخلاقي من خلال المساس بالعلاقات الأسرية وذلك بسبب الكثير من النتائج التي تُسبّبها بعض أنواع الجرائم الإلكترونية كالتشهير ببعض الأفراد ونشر الأخبار الكاذبة والإشاعات.
- ظهور حالات الاختطاف والاغتيالات حتى بعد دفع المبالغ المالية[2]،إضافة إلى ظاهرة إدمان الشبان على الألعاب الإلكترونية خصوصا فئة المراهقين بين 12 و16 عام.

2- مظاهر تهديد الجرائم الإلكترونية لأمن الدول واستقرارها:

تتعدد وتختلف صور حدوث الجريمة الالكترونية، باختلاف الوسائل المستخدمة في ارتكابها وكذلك الجهات المسؤولة عن ارتكابها، لذا سنحاول في العنصر التركيز على أهم مظاهر الجرائم الإلكترونية التي تأثر على أمن واستقرار الدول، وذلك على النحو الاتي:

أ- التجسس الإلكتروني:

يقصد بالتجسس في هذا الموضع " الاطلاع المعلومات خاصة بالغير، ومؤمنة في جهاز أخر، وليس مسموح لغير المخولين بالاطلاع عليها،[3] حيث أثر الفضاء الإلكتروني على الأدوات الاستخباراتية وسهل القدرة على جمع المعلومات والتصنت والتجسس، إضافة

---

[1]- فؤاد جمال،" الجرائم المعلوماتية"،2017/11/28، متوفر على الرابط الإلكتروني:
http://almohakmoonalarab.ahlamontada.com/t91-topic

[2]- بلاسم جميل خلف،" أبعاد جريمة غسيل الاموال وانعكاساتها على الاقتصاد العراقي"،2017/11/12، متوفر على الرابط الإلكتروني: *www.nazaha.iq/search_web/eqtsade/3.doc*

[3]- محمد عبد الرحيم سلطان العلماء، "جرائم الانترنت والاحتساب عليها"، ورقة بحثية مقدمة ضمن فعاليات المؤتمر العلمي حول: (القانون والكمبيوتر والانترنت أيام 1- 3 ماي 2000، جامعة الامارات العربية المتحدة، كلية الشريعة والقانون، م 3، ط3، 2004)، ص 880.

لتسهيل النشاطات السرية في العلاقات الدولية كعملية الاغتيالات نتيجة تزايد العلاقة بين التكنولوجيا والأمن،[1] إذ تقوم مؤسسات استخباراتية خاصة باجتذاب القراصنة للاستفادة من خدماتهم في التعاقد مع شركات كبرى تسعى للحصول على معلومات مهمة عن منافسيها، وتقوم شركات أخرى بتوظيفهم وتوجيههم لإلحاق الضرر المادي والمعنوي بالمنافسين من خلال تدمير ثقة عملائهم بهم، كما أصبحوا هؤلاء القراصنة سلاحا مؤثرا في أوساط الجماعات الإرهابية، حيث يتم استغلالهم للتجسس ولنشر رسائلهم السياسية عبر الإنترنت.[2]

أيضا يمكن توظيفهم من قبل الدول من أجل التخطيط أو القيام بهجمات إلكترونية أو لجمع المعلومات عن الجهات والدول المعادية، وعلى ضوء هذه الحقائق مجتمعة ينبغي التعامل مع هؤلاء على أنهم يشكلون تهديدًا لأمن الدول، وفي الوقت الذي يؤكد الخبراء فيه صعوبة خوض معركة حاسمة مع هذه الفئات، لذا يجب على جميع الدول توظيف عدد كبير من الخبراء الذي لهم الخبرة الفنية والتقنية[3] لمواجهة الجوسسة الإلكترونية، وبذلك يمكن القول شبكة الأنترنت سهلت الأعمال التجسوسية بشكل كبير، حيث يقوم المجرمون بالتجسس على الأشخاص أو الدول أو المنظمات أو الهيئات أو المؤسسات الدولية أو الوطنية، وتستهدف عمليات التجسس في عصر المعلومات ثلاث أهداف رئيسية : (التجسس العسكري، التجسس السياسي، التجسس الاقتصادي).[4]

ب- الحرب الإلكترونية:

يشير مصطلح الحرب الإلكترونيّة والذي يطلق عليه بالإنجليزية (*Cyber warfare*) إلى استخدام جملة من الممارسات والإجراءات التي تسعى لإلحاق الخلل والعطل بالأنظمة والوسائل الإلكترونية الخاصة بالعدو، بالإضافة إلى تحقيق الحماية للذات من الاستطلاع الإلكتروني المعادي ومقاومته، وتحقيق الاستقرار للنظم الإلكترونية الصديقة، ويعتبر استخدام الطاقة الكهرومغناطيسيّة في نطاق الحرب الإلكترونيّة ضروريا؛ وذلك لغايات

---

[1] – ريهام عبد الرحمن رشاد العباسي، "أثر الارهاب الإلكتروني على تغير مفهوم القوة في العلاقات الدولية دراسة حالة: تنظيم الدولة الاسلامية"، مركز الديمقراطي العربي، 2017/01/10، متوفر على الرابط الإلكتروني : *http://democraticac.de/?p=345*

[2] – خالد محمد غازي،" الإرهاب الإلكتروني"، 2017/10/11، متوفر على الرابط الإلكتروني: *http://baladnews.com/save.php?cat=2&article=8841*

[3] – المرجع نفسه.

[4] – علي عدنان الفيل، الإجرام الإلكتروني، دمشق: منشورات زين الحقوقية، 2011، ص ص 96- 97

تعطيل حركة العدو، ومنعها من استغلال المجال الكهرومغناطيسي الصديق. إن الحرب الإلكترونية تتخذ من شبكة الإنترنت حلبَة صراع لها، وتأتي الهجمات التي تشن فيها بسبب دوافع سياسية، وتوجه الضربات الإلكترونية على مواقع الإنترنت الرسمية للعدو، وكل ما يتعلق بشبكاته وخدماته الأساسية، وتكون الضربات بقرصنة وتعطيل المواقع، وسرقة البيانات السريّة وتخريبها، واختراق الأنظمة المالية.[1]

ج- السرقة والاحتيال والقرصنة عبر الإنترنت:

من الأخطار الناجمة عن استخدام شبكة الإنترنت والحاسب الآلي على السواء هو خطر القرصنة عبر الإنترنت ذلك أن نمط القرصنة التقليدية قد تغير إلى قرصنة عبر الإنترنت وهذا ما أعلنته أحدث دراسات اتحاد البرمجيات (*B.s.a*) وهي اختصار لـ (*Business Soft ware Alliance*) وهي منظمة تمولها كبرى شركات البرمجيات في العالم مثل مايكروسوفت ولوتس لمراجعة وتحليل سوق البرمجيات،[2] ويتم هذا من خلال:

- **سرقة المعلومات وتزويرها:** يقوم كثير من الأفراد والمنظمات الإجرامية والتي ترغب في الكسب المادي السريع باستنساخ المطبوعات والمواد الصوتية والبرامج المستخدمة في الحاسب الآلي وذلك باستخدام التقنية الرقمية البالغة الإتقان، بعد ذلك يقومون بتوزيعها وبيعها بثمن أقل بكثير من السعر الأساسي ملغين بذلك حقوق المؤلف أو الشركة المنتجة بل ومعتدين بالسرقة عليه، والتي تسبب خسائر مالية كبيرة.[3] وملخص هذه الجريمة الاعتداء على المعلومات المخزنة في ذاكرة الحاسب الآلي بسرقتها أو تحريفها أو التلاعب بها، وكذلك اعتراض المعلومات المرسلة من خلال شبكة الانترنت وتغيير محتواها، وأشار تقرير نشره ميرر وأندروود 1994 أن خسائر رابطة ناشري البرمجيات وبسبب السرقة والقرصنة والتزوير قدرت بـ 7.4 مليار دولار منها 2 مليار دولار خسائر ما سرق

[1] – إيمان الحياري،" مفهوم الحرب الإلكترونية"،2016/12/22، متوفر على الرابط الإلكتروني: *http://mawdoo3.com*

[2] – عثمان الصديق أحمد محمد، الجرائم الإلكترونية في القانون السوداني (دراسة مقارنة علي ضوء الاتفاقية الدولية لمكافحة الجريمة المنظمة عبر الحدود الوطنية لسنة 2002م)، مذكرة ماجستير في تخصص القانون، كلية القانون، جامعة الخرطوم، ص 50، متوفر على الرابط الالكتروني: *http://khartoumspace.uofk.edu/bitstream/handle*

[3] – تركي محمد العطيان،" جرائم الحاسب الآلي: دراسة نفسية تحليلية"،2017/01/10، متوفر على الرابط الإلكتروني: *http://www.minshawi.com/other/oteyan.pdf*

من خلال شبكة الانترنت، وخسرت السوق الامريكية لصناعة البرامج الحاسوبية 3.8 مليار دولار و690 مليون دولار في مجال نشر الكتب.[1]

- **سرقة وابتزاز الأموال:** يقصد بها استخدام شبكة الإنترنت بهدف الحصول على المال، كالدخول إلى شبكات البنوك والتحويل غير المشروع للأموال من حساباتها، أو التلاعب في الحسابات المودعة لدى البنوك بتحويلها من حساب إلى آخر، أو الحصول على الرقم السري الذي يمكن المجرم من الدخول إلى هذه الحسابات والتلاعب بها. ومن صورها كذلك سرقة الأموال باستخدام البطاقات البنكية المسروقة والقيام بتصنيع البطاقات المزورة بعد الحصول على أسماء وأرقام البطاقات الأصلية، ويمكنهم الحصول على هذه المعلومات من خلال شبكة الإنترنت ممن قاموا بالشراء عن طريقها، أو من خلال الفنادق ومحطات البنزين، والمحلات الكبرى أو سرقتها وغير ذلك من الصور.[2]

- **التخريب والإتلاف:** معظم الدول خصوصا المتقدمة، تعتمد اليوم على نظم معلومات وبيانات يتم الاستفادة منها بعد معالجتها مثل عمل المصارف، المستشفيات والتعليم وملفات الموظفين والوزارات... إلخ، إذ تعتمد أنظمتها على تقنية الاتصال عن بعد للتشغيل والتحكم والتحليل لأي موضوع والربط بينها بواسطة الحاسب الآلي، وإذا تم اختراقها أو الدخول إليها وإتلافها سيؤدي ذلك إلى نتائج سلبية على الفرد والشركات والدولة معا.[3]

- **الغش التجاري:** لقد تصاعد دور الاقتصاد الرقمي، ونمت التجارة الإلكترونية، وأصبح على كل دولة ترغب في بناء اقتصاد قوى أن تهتم بالاستثمار في التكنولوجيا، ورفع مستوى التعليم التقني داخل الدولة.[4] غير أن انتشار البيع والاستثمار عبر تقنية الحاسوب أو ما يسمى بالتجارة الإلكترونية حيث يقوم أشخاص أو مجموعات إجرامية باستخدام شبكة الإنترنت لعرض السلع للبيع والشراء لعقد صفقات مغشوشة أو طلب التبرعات المزيفة وطرح استثمارات تجارية وهمية عن طريق الإنترنت.

- **التحويل الإلكتروني الغير شرعي للمال:** تحويل الأموال إلكترونيا منتشر في العالم عبر المصارف العالمية، ويتم تداول الآلاف لمثل هذه العمليات يوميا وعلى مدار الساعة، كل ذلك

---

[1]- عارف خليل أبو عيد، "جرائم الانترنت: دراسة مقارنة"، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، الإمارات العربية المتحدة، العدد 3، أكتوبر 2007، ص 84.

[2]- المرجع نفسه، ص 88.

[3]- تركي محمد العطيان،" جرائم الحاسب الآلي: دراسة نفسية تحليلية"، مرجع سابق.

[4]- ريهام عبدالرحمن رشاد العباسي، "أثر الارهاب الإلكتروني على تغير مفهوم القوة في العلاقات الدولية دراسة حالة: تنظيم الدولة الاسلامية"، مرجع سابق.

يتم باستخدام الحاسب الآلي يستخدم فيها بطاقات ائتمان مصرفية قابلة للاختراق والتزييف لذلك من السهل اعتراض هذه العمليات وبسهولة من المزيفين.[1] وصورة هذه الجرائم أن يستخدم الشخص الحاسب الآلي للدخول إلى شبكة الإنترنت، والوصول غير المشروع إلى البنوك والمصارف والمؤسسات المالية، وتحويل الأموال من تلك الحسابات الخاصة بالعملاء إلى حسابات أخرى، وذلك بإدخال بيانات غير حقيقية أو تعديل أو مسح البيانات الموجودة بقصد اختلاس الأموال أو نقلها أو إتلافها.[2]

د- الجرائم المنظمة عبر الإنترنت:

الجريمة المنظمة ليست وليدة التقدم التكنولوجي وإنما استفادت منه، فبسبب وسائل الاتصال والتكنولوجيا أصبحت غير محددة لا بقيود الزمان ولا قيود المكان، وأضحى انتشارها على نطاق واسع وكبير، حيث استغلت عصابات الجريمة المنظمة الإمكانات المتاحة في وسائل الإنترنت في التخطيط والتمرير وتوجيه المخططات الإجرامية وتنفيذ عملياتها بسهولة[3]، فالجرائم الإلكترونية ذات نشاط إجرامي معقد تنفذها جماعات على درجة كبيرة من التنظيم تستهدف الثراء والسكب غير المشروع بصورة مستمرة.

- **غسيل الأموال عبر الإنترنت:** تعدّ جرائم غسيل الأموال (*MONEY LAUNDERING*) أخطر جرائم عصر الاقتصاد الرقمي، إذ تشكل تحدي حقيقي أمام مؤسسات المال والأعمال،[4] فالأساليب التكنولوجية الحديثة تستخدم كإحدى الوسائل السريعة لعمليات غسيل الأموال الأمر الذي صعب معها إمكانية الرقابة على مصدر تلك الأموال يتم استخدام الوسائل الحديثة كالبطاقات الذكية وأجهزة الكمبيوتر ومن خلال الأنترنت عبر منظومة حماية وتشفير لضمان سرية عمليات الإيداع، وبذلك تتم عبر سلسلة من العمليات المعقدة والسريعة والمتعاقبة التي لا يمكن فصلها عن مصادرها غير المشروعة.

- **تجارة المخدرات عبر الإنترنت:** بعد انتشار استخدام الشبكة العالمية للإنترنت، ساعدت على الترويج للمخدرات وأصبحت تستعملها كسوق مغرية وأضحى في الإمكان لأي شخص أن يكتشف كيفية الحصول على المخدرات من خلال هذه الشبكة، بل وأن يتعلم كيفية استعمالها. وفي هذا السياق يشير التقرير الصادر عن منظمة الشرطة الدولية(إنتربول) أن 890 مليون

[1] – ريهام عبدالرحمن رشاد العباسي، مرجع سابق.

[2] – عارف خليل أبو عيد، مرجع سابق، ص 84.

[3] – سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الإنترنت، الإسكندرية: دار الفكر الجامعي، 2007، ص 83

[4] – بلاسم جميل خلف،" أبعاد جريمة غسيل الأموال وانعكاساتها على الاقتصاد العراقي"، مرجع سابق.

شخص في آسيا وأوربا وأمريكا الشمالية ممن يتعاطون المخدرات يحصلون عليها عن طريق الشبكة.[1]

هـ- المنظمات الإرهابية واستخدام الإرهاب الإلكتروني:

تعتبر شبكة الإنترنت وسيلة للاتصال بالغة الأهمية بالنسبية للمنظمات الإرهابية، حيث أدى الفضاء الإلكتروني إلى تحول الإرهاب إلى تهديد عالمي، وأصبح الإرهاب جريمة عابرة للحدود القومية من حيث النشاط والخطط والتمويل والأعضاء، وتصاعد نشاط الجماعات الإرهابية عبر الفضاء الإلكتروني وتعزيز بعدها العالمي، وتم استخدام المنجزات التكنولوجية في ممارسة الارهاب، والتي استطاع الإرهابيون من خلالها تحقيق أضرار غير متوقعة وهائلة تتجاوز التهديدات التي تمثلها الدول لبعضها البعض. حيث استغلت الجماعات الارهابية بكافة أشكالها وأنماطها الفكرية المزايا الالكترونية كعنصر حيوي لدعم وتحقيق أهدافها، وتحولت بعد أن كانت مجموعات قلائل من الأفراد متوزعة جغرافياً الى مجتمع افتراضي غير محدد الأبعاد الكمية وكان ذلك له دور كبير في تضخيم الصورة الذهنية لقوة وحجم تلك المجموعات، ولقد ظهر التزاوج بين الإرهاب والإنترنت بشكل أكثر وضوحاً بعد أحداث 11 سبتمبر، ولكنه منذ عام 1999 كانت كل الجماعات الإرهابية حاضرة على الإنترنت بشكل كبير وبعد عام 2001 كان هناك أكثر من 5 الاف موقع إلكتروني وغرف محادثة إلكترونية تابعة للجماعات الارهابية وتستخدمها للتأثير على الرأي العام من خلال معركتها الفكرية، أو استخدامها للقيام بأعمال إرهابية مادية عن طريق جمع المعلومات والتنسيق والتنظيم.[2]

ثانيا- متطلبات تحقيق الأمن الإلكتروني والتصدي للجرائم المستحدثة:

إن نقطة انطلاق الأمن الإلكتروني الوطني تبدأ بتطوير سياسة وطنية لرفع الوعي حول قضايا الأمن السيبراني والحاجة لإجراءات وطنية وإلى التعاون الدولي، أما الخطوة الثانية فتتمثل بتطوير المخطط الوطني لتحفيز الأمن السيبراني بهدف تقليص مخاطر وأثار التهديدات السيبرانية وتتضمن المشاركة في الجهود الدولية والإقليمية لتحفيز مكافحة الجرائم السيبرانية، وهذا من خلال:

---

[1] – أخام بن عودة زواوي مليكة، "تحديات ظاهرة الجريمة العابرة للأوطان والثورة المعلوماتية"، ورقة بحثية مقدمة ضمن فعاليات المؤتمر المغاربي الأول حول: (المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، ليبيا، أيام 27– 30 أكتوبر 2009).

[2] – ريهام عبدالرحمن رشاد العباسي، "أثر الارهاب الإلكتروني على تغير مفهوم القوة في العلاقات الدولية دراسة حالة: تنظيم الدولة الاسلامية"، مرجع سابق.

1. تطوير استراتيجية وطنية للأمن الإلكتروني وحماية البنية التحتية للمعلومات الحساسة.
2. إنشاء تعاون وطني بين الحكومة ومجتمع صناعة الاتصالات والمعلومات.
3. خلق قدرات وطنية لإدارة ومواجهة جرائم الحاسب الآلي.
4. تحفيز ثقافة وطنية للأمن الإلكتروني.
5. سد الفراغ التشريعي في مجال مكافحة الجريمة الإلكترونية، على أن يكون شاملا للقواعد الموضوعية والإجرائية، وعلى وجه الخصوص النص صراحة على تجريم الدخول غير المصرح به إلى الحاسب الآلي وشبكات الاتصال (الإنترنت) والبريد الإلكتروني، وكذلك اعتبار البرامج والمعلومات من الأموال المنقولة ذات القيمة، أي تحديد الطبيعة القانونية للأنشطة الإجرامية التي تمارس على الحاسب الآلي والإنترنت، وأيضا الاعتراف بحجية للأدلة الرقمية وإعطاؤها حكم المحررات التي يقبل بها القانون كدليل إثبات .
6. منح سلطات الضبط والتحقيق الحق في إجراء تفتيش وضبط أي تقنية خاصة بالجريمة الإلكترونية تفيد في إثباتها، على أن تمتد هذه الإجراءات إلى أية نظم حاسب آلي آخر له صلة بمحل الجريمة.
7. تفعيل التعاون الدولي على مستوى المنظمات الدولية ودور المعاهدات الدولية ومبدأ المساعدة القانونية والقضائية المتبادلة.
8. تفعيل دور المجتمع المدني والمؤسسات للقيام بدور التوعية والوقائية من الوقوع في الممارسات الخاطئة للإنترانت.
9. العمل على تطور مجال الأمن الإلكتروني من خلال إعداد أنظمة ضبطية وقضائية مؤهلة في التعامل مع الجرائم الإلكترونية.[1]

يرى الأستاذ (باري بوزان–*Barry Buzan*) أن الأمن يعني العمل على التحرر من التهديد، والأمن الوطني مرتبط بقدرة الدول على الحفاظ على هويتها المستقلة ووحدتها الوطنية[2]. وبما أن مخاطر أمن المعلومات باتت ترقى إلى مستوى تهديد الأمن القومي ككل، فإن وسائل المواجهة والحماية لابد وأن تكون تحت منظومة أمن قومي، لأنه من الخطأ أن تكون الأخطار والتهديدات شاملة وربما منسقة ومخططة أحيانا ثم تأتي سبل ووسائل

[1] – مفتاح بوبكر المطردي، مرجع سابق، ص 54.

[2] – *Barry Buzan, People States and fear ;an agenda for dites national security studies in the post cold war era, 2 ed, boulter Lynne rienner publishers,1991, p 116.*

مواجهتها جزئية وعفوية وخالية من التخطيط وتفتقر للتنسيق، وقد قدمت اليابان نموذجا لهذا المستوى من التعامل مع أمن المعلومات حينما أعلنت منذ أكتوبر/تشرين 2005 البدء في تنفيذ برنامج شامل على مستوي مؤسسات وهيئات الدولة والشركات الخاصة يستهدف التدريب على صد الهجمات الإلكترونية الشاملة سواء بالفيروسات أو عمليات القرصنة والتلصص والتجسس الاقتصادي أو التخريب الإلكتروني أو هجمات تعطيل شبكات الاتصالات والمعلومات، وجاء هذا البرنامج التدريبي المستمر حتى في إطار استراتيجية وسياسة متكاملة لأمن المعلومات باليابان تنفذها الدولة حماية لاقتصادها، وقد تزامنت مع المخطط الياباني مخططات مماثلة في عدة الدول من العالم.

لذا لابد من الإشارة إلى أن إدارة المعلومات المتداولة داخل البنية المعلوماتية القومية بما يدعم الأمن القومي أمر يتطلب فهما ورؤية جديدة لأساليب ومناهج وأدوات تداول المعلومات بين أطراف المجتمع وبعضها البعض داخليا، وكذلك مناهج وأدوات وأساليب إدارة وتداول المعلومات بينها وبين الجهات الخارجية، كشركاء السياسة والتجارة والأعمال والتعليم والبحث العلمي والتصنيع...إلخ، وهذه قضية مهمة ومعقدة في آن واحد، وهي تحتاج جهدا مؤسسيا لن يتحقق على النحو المطلوب إلا عندما تتبوأ قضية أمن المعلومات مكانها الصحيح كركيزة أساسية للأمن القومي.[1]

المحور الثالث: قرصنة الموقع الإلكتروني لوكالة الأنباء القطرية "قنا"

خصص هذا المحور للبحث في عملية القرصنة التي تعرض لها الموقع الإلكتروني لوكالة الأنباء القطرية " قنا " كأنموذج لأثر الجرائم الإلكترونية على أمن واستقرار الدول، إذ تعد قضية اختراق الموقع الإلكتروني لوكالة الأنباء القطرية أحد أبرز الأمثلة على جرائم القرصنة الالكترونية والتي كانت من بين أسباب توتر العلاقات بين(قطر) و(المملكة السعودية، الامارات العربية، البحرين)، على إثر ذلك أكدت وكالة الأنباء القطرية (قنا) أن التصريحات التي نسبت إلى أمير دولة قطر والتي نشرت على موقعها هي تصريحات ملفقة ومفبركة، وأن موقعها الإلكتروني تعرض للاختراق من جهة غير معروفة، وبعد النتائج الأولية للتحقيقات في جريمة قرصنة موقع وكالة الأنباء

[1] – جمال محمد غيطاس، "الأمن المعلوماتي والجرائم الإلكترونية.. أدوات جديدة للصراع "، مرجع سابق.

وحساباتها على وسائل التواصل الاجتماعية، [1] أن هذا الاختراق تم بالاعتماد تقنيات عالية جدا وأساليب مبتكرة.

أولا – فبركة تصريحات ونسبها لأمير دولة قطر بعد قرصنة موقع "قنا":

جاء في التصريحات المنسوبة للأمير تميم بن حمد آل ثاني ما يلي: [2]

- أن ما تتعرض له قطر من حملة ظالمة، تزامنت مع زيارة الرئيس الأميركي إلى المنطقة، وتستهدف ربطها بالإرهاب، وتشويه جهودها في تحقيق الاستقرار معروفة الأسباب والدوافع.
- إننا نستنكر اتهامنا بدعم الإرهاب رغم جهودنا المتواصلة مع أشقائنا ومشاركتنا في التحالف الدولي ضد داعش"، مضيفاً: "إن الخطر الحقيقي هو سلوك بعض الحكومات التي سببت الإرهاب بتبنيها لنسخة متطرفة من الإسلام لا تمثل حقيقته السمحة، ولم تستطع مواجهته سوى بإصدار تصنيفات تجرم كل نشاط عادل."
- لا يحق لأحد أن يتهمنا بالإرهاب لأنه صنف الإخوان المسلمين جماعة إرهابية، أو رفض دور المقاومة عند حماس وحزب الله. وطالب مصر ودولة الإمارات العربية المتحدة، ومملكة البحرين بـ "مراجعة موقفهم المناهض لقطر، ووقف سيل الحملات والاتهامات المتكررة التي لا تخدم العلاقات والمصالح المشتركة، مؤكداً أن قطر لا تتدخل بشؤون أي دولة، مهما حرمت شعبها من حريته وحقوقه.

وأشار إلى أن "قاعدة العديد مع أنها تمثل حصانة لقطر من أطماع بعض الدول المجاورة، إلا أنها هي الفرصة الوحيدة لأميركا لامتلاك النفوذ العسكري بالمنطقة، في تشابك للمصالح يفوق قدرة أي إدارة على تغييره."

- وعن القمة العربية – الإسلامية- الأميركية التي شاركت فيها قطر بالرياض، دعا إلى العمل الجاد المتوازن بعيداً عن العواطف، وسوء تقدير الأمور، مما ينذر بمخاطر قد تعصف بالمنطقة مجدداً نتيجة ذلك، وبين أن قطر لا تعرف الإرهاب والتطرف، وأنها تود المساهمة في تحقيق السلام العادل بين حماس الممثل الشرعي للشعب الفلسطيني وإسرائيل، بحكم التواصل المستمر مع الطرفين، فليس لقطر أعداء بحكم سياستها المرنة.

---

[1]- إسلام الراجحي، "العربية جهزت ضيوف الهجوم على قطر قبل ساعتين من اختراق الوكالة"، 24-05-2017، متوفر على الرابط الإلكتروني: *http://www.thenewkhalij.org/ar/node/69114*

[2]- ريهام مازن، تصريحات تميم، الاهرام اليومي، 26 مايو 2017 السنة 141 العدد 47653، متوفر على الرابط الإلكتروني: *http://www.ahram.org.eg/News/202276/59/596027*

وشدد الأمير تميم على أن قطر نجحت في بناء علاقات قوية مع أميركا وإيران في وقت واحد، نظراً لما تمثله إيران من ثقل إقليمي وإسلامي لا يمكن تجاهله، وليس من الحكمة التصعيد معها، خاصة أنها قوة كبرى تضمن الاستقرار في المنطقة عند التعاون معها، وهو ما تحرص عليه قطر من أجل استقرار الدول المجاور.

ثانيا- التحقيقات والنتائج حول تفاصيل عملية القرصنة:

كشفت التحقيقات والنتائج التي أعلن عنها الجهاز الوطني لمكافحة الجريمة السيبرانية في بريطانيا "كوارتز أن:[1]

- المحاولة بدأت قبل نحو شهر من القرصنة الحقيقية، وبالتحديد في 19 أبريل، حينما نجح قراصنة من الوصول إلى موقع الويب على شبكة الإنترنت التابع لوكالة الأنباء القطرية "قنا."

- عناوين بروتوكولات هؤلاء القراصنة كانت روسية (لكن تقنياً فإن ذلك لا يثبت أن الاختراق قد تم من داخل روسيا).

- بعد ثلاثة أيام من محاولات القراصنة البحث عن ثغرات موقع "قنا"، وجدوا أخيرا ضعفاً في ترميز الشبكة الداخلية لوكالة الأنباء واستطاعوا الدخول، وفي غضون بضعة أيام أخرى، كان المتسلل يسيطر على الشبكة بالكامل، وبدأ في جمع عناوين البريد الإلكتروني وكلمات السر والرسائل.

- بعد أسابيع، وفي مساء يوم 23 مايو، دخل الهاكر نظام وكالة الأنباء القطرية، وقام بتحميل قصة إخبارية ملفقة وتصريحات مغلوطة منسوبة إلى أمير قطر تميم بن حمد آل ثاني.

وقد اعتبر وزير الخارجية القطري (محمد بن عبد الرحمن آل ثاني وزير) بأن اختراق وكالة الأنباء القطرية (قنا) هو ليس اختراقاً فقط، بل جريمة إلكترونية، وفق كافة القوانين، ويحاسب عليها القانون، وهجوم إلكتروني استهدف الوكالة، وبث تصريحات كاذبة على لسان الأمير تميم بن حمد آل ثاني. وأشار إلى تشكيل فرق تحقيق ستتولى

[1]- محطات جريمة القرصنة الإلكترونية لوكالة الأنباء القطرية، تقرير صادر عن مجلة الطلائع، العدد الرابع، 2018/02/11، متوفر على الرابط الإلكتروني:
https://altalaya.qa/%D9%85%D8%AD%D8%B7%D8%A7%D8%AA

القيام بتحقيق جنائي للتوصل إلى كشف هوية مرتكبي الجريمة، وتقديم مرتكبيها للقضاء.[1]

في هذا الإطار نفسه كشف الدكتور علي بن فطيس المري النائب العام القطري أنه وفي إطار التعاون بين قطر وتركيا في مجال مكافحة الهجمات والجرائم الإلكترونية، فقد قامت السلطات التركية بإيقاف 5 أشخاص متورطين في جريمة اختراق موقع وكالة "قنا".

كما بدأ محققون من مكتب التحقيقات الفيدرالي الأمريكي "إف بي آي" في تحديد مصدر القرصنة التي تعرضت لها "قنا"، وعقب التحقيقات المشتركة بين قطر والإف بي آي، أعلنت وزارة الداخلية النتائج المبدئية للتحقيقات بشأن جريمة القرصنة، حيث أكد فريق التحقيق أن عملية القرصنة استخدمت فيها تقنيات عالية وأساليب مبتكرة من خلال استغلال ثغرة إلكترونية على الموقع الإلكتروني لوكالة الأنباء القطرية، وتمكن فريق التحقيق من تحديد المصادر التي تم من خلالها القيام بجريمة القرصنة، كما أكد الفريق بأنه قد تمت عملية تثبيت ملف الاختراق بشهر إبريل، والذي تم استغلاله لاحقاً في نشر الأخبار المفبركة.

وكشفت وزارة الداخلية القطرية عن تفاصيل جريمة قرصنة مواقع وكالة الأنباء القطرية التي تضمنت الإعلان عن أن موقعين من الإمارات استخدما في اختراق الوكالة، وأكدت أنه تم التصفح 45 مرة من خلال شخصين من الإمارات خلال ربع ساعة بداية من الساعة 23:45 يوم 23 مايو2017 قبل الاختراق، ثم التصفح 41 مرة في الربع الساعة التالية من إحدى دول الحصار على قطر.

كما تم استخدام هاتف آيفون برقم أوروبي لاستغلال الثغرة للدخول إلى موقع وكالة "قنا" وتنفيذ عملية الاختراق، حيث تم اختراق الجهاز الرئيسي لشبكة الوكالة وتمكن من الحصول على البيانات، وقام أحد المشاركين بعملية القرصنة بمشاركتها مع شخص آخر عن طريق برنامج "*SKYPE* "

وفي 29 أبريل2017 تمكن المخترقون من الدخول إلى الثغرة عن طريق عنوان (*IP*) من إحدى دول الحصار في الازمة الخليجية[2].

[1] – إسماعيل طاي،محمد بن عبدالرحمن: كشف سير التحقيقات في "الجريمة الإلكترونية" بشفافية تامة، جريدة العرب، قطر: دار العرب، العدد 10575، 26 مايو 2017، ص 6.

[2] – محطات جريمة القرصنة الإلكترونية لوكالة الأنباء القطرية، تقرير صادر عن مجلة الطلائع، مرجع سابق.

في هذا السياق وبالنظر لعدة أسباب منها التصريحات المفبركة التي نشرت لفترة وجيزة على موقع وكالة الأنباء القطري، وكخطوة تهدف إلى الضغط على قطر، أغلقت دول الخليج المجاورة (السعودية والإمارات والبحرين)، فضلا عن مصر، حدودها البرية والبحرية والجوية وقامت بقطع العلاقات الدبلوماسية مع قطر. هذه الإجراءات أدت إلى أزمة إقليمية بعد اتخاذ إجراءات المقاطعة الدبلوماسية والحصار الاقتصادي على الدولة القطرية، تضمنت هذه الاجراءات ما يأتي:[1]

1. غلق المنفذ الحدودي البري الوحيد لقطر مع السعودية، مما أدى إلى منع وصول الغذاء والأدوية وغيرها من المواد التي تستوردها قطر براً.
2. غلق المجال الجوي والحدود البحرية أمام الطائرات والسفن القطرية، وتعليق الرحلات الجوية والبحرية مع الدوحة في ظرف 24 ساعة.
3. منعت الدول الخليجية الثلاث مواطنيها من السفر إلى قطر، ودعت أولئك الموجودين في قطر إلى المغادرة خلال 14 يوما، كما طالبت كافة المواطنين القطريين بمغادرة هذه الدول الثلاث.
4. شرّعت الدول الخليجية الثلاث قانوناً خاصاً يعاقب أي فعل عبر شبكة الإنترنت يقصد منه تأييد دولة قطر بغرامة مالية والسجن لفترة تتراوح بين 3-15 سنة.
5. منع كافة وسائل الإعلام القطرية من ممارسة نشاطها في هذه الدول (تلفزيون قطر، الجزيرة، بي إن سبورت)، كما أغلقت المواقع الإلكترونية الخاصة بها ومواقع الصحف القطرية

جدول: يوضح أهم محطات الزمنية لأهم الأحداث بعد قرصنة موقع وكالة الأنباء القطري.

20 ماي2017	▪ نشر تصريح منسوب للأمير القطري: قطر تعلن أنها تتعرض لحملة "ممنهجة ومغرضة" تتهمها بـ "التعاطف" مع الإرهاب قبل زيارة الرئيس الأمريكي دونالد ترامب الى السعودية.
24 ماي2017	▪ قطر تعلن أن موقع وكالة الأنباء الرسمية لديها تعرض" لعملية اختراق من قبل جهة غير معروفة". وأضافت أنه تم "الإدلاء بتصريح مغلوط" منسوب لأمير قطر مشددة على أن "ما تم نشره ليس له أي أساس من الصحة."
05 جوان 2017	▪ السعودية والإمارات والبحرين ومصر واليمن تقطع علاقاتها الدبلوماسية مع قطر لاتهامها صراحة بدعم "الإرهاب."

[1]- بيان سفارة دولة قطر في كندا بمناسبة مرور ثمانية أشهر على حصار دولة قطر من قبل السعودية والإمارات والبحرين ومصر، بيان على موقع سفارة دولة قطرأوتاوا، كندا، 05/ 02/2018، متوفر على الرابط الإلكتروني: *http://ottawa.embassy.qa*

08 جوان 2017	▪ شبكة "الجزيرة" القطرية تعلن أن مواقعها ومنصاتها الرقمية تتعرض لمحاولات اختراق ممنهجة ومتزايدة، وأن الموقع الإلكتروني لتليفزيون قطر تعرض لمحاولات مماثلة قبل أن تتصدى لها أنظمة الحماية.
30 أكتوبر2017	▪ الجهاز الوطني لمكافحة الجريمة السيبرانية في بريطانيا "كوارتز"، يؤكد عملية القرصنة لموقع وكالة الانباء القطرية.

المصدر: إعداد الباحثة بالاعتماد على: زهية رافع، كرونولوجيا الأزمة الدبلوماسية مع قطر، – 06 – 2017، متوفر على الرابط الالكتروني: https://www.djazairess.com/elbilad/271334 وعمرو عبدالعاطي، تطورات الأزمة القطرية، مجلة السياسة الدولية: تحليلات – شئون دولية، القاهرة: مؤسسة الاهرام، 10-8-2017، متوفر على الرابط الالكتروني: http://www.siyassa.org.eg/News/15199.aspx

بناء على ما سبق يمكن القول أن ظاهرة الجرائم الالكترونية وعمليات القرصنة التي تتعرض لها الدول على درجة كبيرة من الخطورة، تزداد خطورتها عندما ترتبط بالأبعاد السياسية والأمنية وبأهداف أطراف خارجية تسعى بطريقة غير مباشرة لزعزعة الاستقرار وخلق حالة من التوتر أو الأزمات للدولة المستهدفة.

خاتمة:

بعد تحليلنا للموضوع، يمكن القول أن الجرائم الإلكترونية تشكل تهديدا أمنيا خطيرا على استقرار الدول، وذلك بالنظر للاستخدامات السلبية للوسائل التكنولوجية خصوصا عند استغلالها من طرف الجماعات الإرهابية وقيامها بهجومات واعتداءات إلكترونية على مختلف القطاعات الحيوية للدولة، مما يطرح تحدي أساسي أمام وحدات المجتمع الدولي ويتطلب منها اتخاذ كافة التدابير الدفاعية والوقائية اللازمة لمجابهة هذه الأخطار أو الحد منها، وبالتالي تم التوصل للنتائج الآتية:

- **أفرزت ظاهرة الجرائم المعلوماتية جملة من التحديات على صعيد حماية الأمن القومي للدولة، نظرا طبيعة الجريمة المستحدثة، فهناك صعوبة في إثبات هذه الجرائم وقبول الدليل بشأنها باعتبارها لا تترك أثراً مادياً ملموسا، كما هو الحال في الجرائم التقليدية. كما أنها تعد جريمة عابرة الحدود لذا تتطلب المحاربة الفعلية لها تعاونا دوليا سريعا وفعّالا خصوصا في المسائل الجنائية والأمنية بما يسمح بدعم الجهود المحلية.**
- **بالنظر للترابط بين أمن المعلومات والأمن القومي باعتبار أن المعلومة هي ركيزة من ركائز الأمن القومي بمختلف مجالاته العسكرية والأمنية والاجتماعية والسياسية والفكرية والاقتصادية التي يجب حمايتها.**
- **بعد دراستنا لـ: قرصنة الموقع الإلكتروني لوكالة الأنباء القطرية كأنموذج لموضوع البحث، يمكن تصنيف هذا الانموذج ضمن الجرائم الالكترونية ذات الطابع**

(السياسي) ويبرز هذا الصنف من من خلال فبركة تصريحات ونسبها لشخصية سياسية (أمير دولة قطر) بغرض افتعال أزمة سياسية والضغط على الدولة.

▪ انطلاقا من أن الأمن الإلكتروني يشكل عنصرا هاما في السياسة الأمنية الوطنية للدول، بات إلزاميا على صانع القرار التعامل مع مسائل الدفاع الإلكتروني أو الأمن الإلكتروني كأولوية في سياساته الأمنية الوطنية، كون هذه الجريمة تمثل تهديدا مباشرا للأمن والاستقرار على المستوى الوطني والعالمي، وعائقا يحول دون إتمام عمليات التطوير والتنمية.

على هذا الأساس يمكن تقديم جملة من التوصيات المقترحة لمواجهة الجرائم المعلوماتية على الصعيد المحلي والدولي تتمثل في التالي:

- تطوير وسائل وتقنيات مراقبة شبكة الأنترنت وتعزيز إجراءات الأمن الإلكتروني والحراسة للمواقع الرسمية.
- إرساء قواعد التعاون الإقليمي والدولي في مجال الأمن الإلكتروني ومكافحة الجرائم المستحدثة التي تتم باستخدام الكمبيوتر أو عبر شبكة الإنترنت.
- التأكيد على أهمية الإجراءات الوقائية والسعي لإيجاد إطار قانوني للتعاون التعاون الدولي لمحاربة الجرائم المتصلة بالكمبيوتر، ووضع برنامج شامل يستهدف التدريب على التصدي للجرائم والهجمات الإلكترونية.

قائمة المراجع:

1- المراجع باللغة العربية

أولا: الكتب

1. داود، حسن طاهر، جرائم نظم المعلومات، الرياض: أكاديمية نايف العربية للعلوم الامنية، 2000.
2. شفيق، نوران، أثر التهديدات الإلكترونية على العلاقات الدولية، القاهرة: المكتب العربي للمعارف، 2015.
3. عياد، سامي علي حامد، الجريمة المعلوماتية وإجرام الإنترنت، الإسكندرية: دار الفكر الجامعي، 2007.
4. غيطاس، جمال، أمن المعلومات والأمن القومي، القاهرة: شركة نهضة مصر للطباعة والنشر
5. الفيل، علي عدنان، الإجرام الإلكتروني، دمشق: منشورات زين الحقوقية، 2011.

والتوزيع، 2007.

ثانيا: الدوريات والمنشورات

1. أبو عيد، عارف خليل، "جرائم الانترنت: دراسة مقارنة"، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، الإمارات العربية المتحدة، العدد 3، أكتوبر 2007.
2. طاي، إسماعيل، "محمد بن عبدالرحمن: كشف سير التحقيقات في لجريمة الإلكترونية بشفافية تامة"، جريدة العرب، قطر: دار العرب، العدد :10575، 26 ماي 2017.

ثالثا: المذكرات والأطروحات

1. شراب، منذر أحمد زكي، "السياسة الخارجية القطرية في ظل التحولات السياسية العربية 2003-2012"، مذكرة ماجستير في تخصص دراسات الشرق الأوسط، (قسم التاريخ كلية الآداب والعلوم الإنسانية جامعة الأزهر، 2014).
2. صغير، يوسف، "الجريمة المرتكبة عبر الأنترانت،" مذكرة ماجستير في تخصص القانون الدولي للأعمال، (قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، 2010).

رابعا: الملتقيات العلمية

1. رستم، هشام محمد فريد،"الجرائم المعلوماتية: أصول التحقيق الجنائي الفني"، ورقة بحثية مقدمة ضمن فعاليات المؤتمر العلمي حول: (القانون والكمبيوتر والإنترنت، مركز الإمارات للدراسات والبحوث الاستراتيجية، الإمارات العربية المتحدة، 2004).
2. زواوي مليكة، أخام بن عودة، "تحديات ظاهرة الجريمة العابرة للأوطان والثورة المعلوماتية"، ورقة بحثية مقدمة ضمن فعاليات المؤتمر المغاربي الأول حول: (المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، ليبيا، أيام 27- 30 أكتوبر 2009).
3. سلطان العلماء، محمد عبد الرحيم، "جرائم الانترنت والاحتساب عليها"، ورقة بحثية مقدمة ضمن فعاليات المؤتمر العلمي حول: (القانون والكمبيوتر والانترنت أيام 1- 3 ماي 2000، جامعة الامارات العربية المتحدة، كلية الشريعة والقانون، م 3، ط3، 2004).
4. المطردي، مفتاح بوبكر،"الجريمة الإلكترونية والتغلب على تحديات"، ورقة بحثية ضمن فعاليات المؤتمر العلمي الثالث (لرؤساء المحاكم العليا في الدول العربية، السودان، أيام 23- 25 سبتمبر 2012).
5. موسى البدانية، ذياب،"الجرائم الالكترونية: المفهوم والأسباب"، ورقة بحثية ضمن فعاليات المؤتمر العلمي حول: (الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، كلية العلوم الاستراتيجية، عمان، الأردن، أيام 2-7 سبتمبر 2013).

خامسا: التقارير

1. منظمة الإنتربول، "مكافحة الجريمة في القرن الواحد والعشرين 2000- 2010"، تقرير صادر عن الإنتربول، فرنسا، 2010.

سادسا: مقالات الانترنت

1. أحمد محمد، عثمان الصديق، الجرائم الإلكترونية في القانون السوداني (دراسة مقارنة علي ضوء الاتفاقية الدولية لمكافحة الجريمة المنظمة عبر الحدود الوطنية لسنة 2002م)، مذكرة ماجستير في تخصص القانون، كلية القانون، جامعة الخرطوم، ص 50، متوفر على الرابط الالكتروني:
http://khartoumspace.uofk.edu/bitstream/handle
2. الأمن السيبراني "، موقع الهيئة المنظمة للاتصالات، الجمهورية اللبنانية، 2017/12/11، متوفر على الرابط الإلكتروني: *http://www.tra.gov.lb/Cybersecurity-AR*
3. بيان سفارة دولة قطر في كندا بمناسبة مرور ثمانية أشهر على حصار دولة قطر من قبل السعودية والإمارات والبحرين ومصر، بيان على موقع سفارة دولة قطر- أوتاوا، كندا، 05/ 02/ 2018، متوفر على الرابط الإلكتروني: *http://ottawa.embassy.qa*
4. جمال، فؤاد،" الجرائم المعلوماتية"،2017/11/28، متوفر على الرابط الإلكتروني:

http://almohakmoonalarab.ahlamontada.com/t91-topic

5. الحياري،إيمان، مفهوم الحرب الإلكترونية"،22/12/2016، متوفر على الرابط الإلكتروني: *http://mawdoo3.com*
6. خلف، بلاسم جميل،" أبعاد جريمة غسيل الاموال وانعكاساتها على الاقتصاد العراقي"، 12/11/2017، متوفر على الرابط الإلكتروني: *www.nazaha.iq/search_web/eqtsade/3.doc*
7. الديربى، عبد العال،"الجريمة المعلوماتية: تعريفها.. أسبابها.. خصائصها"، المركز العربي لأبحاث الفضاء الإلكتروني، 11/12/2016، متوفر على الرابط الإلكتروني: *http://accronline.com/article_detail.aspx?id=7509*
8. الراجحي، إسلام، "العربية جهزت ضيوف الهجوم على قطر قبل ساعتين من اختراق الوكالة"، 24/05/2017، متوفر على الرابط الإلكتروني: *http://www.thenewkhalij.org/ar/node/69114*
9. رشاد العباس، ريهام عبد الرحمن، "أثر الارهاب الإلكتروني على تغير مفهوم القوة في العلاقات الدولية دراسة حالة: تنظيم الدولة الاسلامية"، مركز الديمقراطي العربي، 10/01/2017، متوفر على الرابط الإلكتروني : *http://democraticac.de/?p=345*
10. العطيان، تركي محمد،" جرائم الحاسب الآلي: دراسة نفسية تحليلية"،10/01/2017، متوفر على الرابط الإلكتروني: *http://www.minshawi.com/other/oteyan.pdf*
11. غازي، خالد محمد،" الإرهاب الإلكتروني"، 11/10/2017، متوفر على الرابط الإلكتروني: *http://baladnews.com/save.php?cat=2&article=8841*
12. الغافري، حسين بن سعيد، "الجرائم المتعلقة بشبكة الإنترنت مفاهيم وأساليب وخصائص"،12/11/2017، متوفر على الرابط الإلكتروني: *http://www.mouwazaf-dz.com/t30021-topic*
13. غيطاس، جمال محمد، "الأمن المعلوماتي والجرائم الإلكترونية.. أدوات جديدة للصراع "، مركز الجزيرة للدراسات، 10 /03/ 2012،متوفر على الرابط الإلكتروني: *http://studies.aljazeera.net/ar/issues/2012/02/201222913222865296O.htm*
14. مازن، ريهام، تصريحات تميم، الاهرام اليومي، 26 مايو 2017 السنة 141 العدد 47653، متوفر على الرابط الإلكتروني: *http://www.ahram.org.eg/News/202276/59/596027*
15. محطات جريمة القرصنة الإلكترونية لوكالة الأنباء القطرية، تقرير صادر عن مجلة الطلائع، العدد الرابع، 11/02/2018، متوفر على الرابط الإلكتروني: *https://altalaya.qa/%D9%85%D8%AD%D8%B7%D8%A7%D8%AA*
16. نمر، سليمان، "أزمة مفتعلة مع قطر"، 11/12/2017، متوفر على الرابط الإلكتروني: *https://www.alaraby.co.uk/opinion*

2- المراجع باللغة الاجنبية

1. *Battistella, Dario, Théories des relation internationales, 2-ed, Paris: press de sciences po, 2006.*
2. *Barry Buzan, People States and fear ;an agenda for dites national security studies in the post cold war era, 2 ed, boulter Lynne rienner publishers,1991.*
3. *Cybercriminalité" , 2018/05/11, in site internet: https://www.interpol.int/Crime-areas/Cybercrime*