القرصنة في الفضاء الإلكتروني وأثرها على أمن الدول

رحاب عبدالحي محمد عثمان

جامعة النيلين

مجلة كلية الدراسات العليا

الرقم الدولي الموحد: 1858-6228

المجلد: 15 ، 2020م
العدد: 09

كلية الدراسات العليا
جامعة النيلين

Graduate College Journal – NU
Vol.15 -2020, Issue (9)
ISSN: 1858-6228, http://www.neelain .edu.sd

مجلة الدراسات العليا - جامعة النيلين
المجلد 15 –2020، العدد (9)
الرقم الدولي الموحد للدوريات: 1858-6228

القرصنة في الفضاء الإلكتروني وأثرها على أمن الدول

رحاب عبدالحي محمد عثمان
قسم العلوم السياسية, كلية الدراسات الاقتصادية والاجتماعية، جامعة النيلين, الخرطوم، السودان

المستخلص

هذه الورقة بعنوان القرصنة في الفضاء الإلكتروني واثرها علي امن الدول, هدفت الورقة الي معرفة مدي تأثير القرصنة الإلكترونية علي أمن الدول خاصة مع تنامي استخدام الدول للفضاء الإلكتروني في إدارة شئونها، تأتي أهمية هذه الورقة من أهمية الفضاء الإلكتروني الذي أصبح ساحة لهجمات القرصنة الإلكترونية، التي تعتبر الان المهدد الأول لأمن واقتصاديات الدول. استندت الورقة علي فرضية أن الفضاء الإلكتروني اصبح له تأثير كبير علي امن الدول من خلال المحتوي المعلوماتي العسكري والامن والفكري والسياسي والاجتماعي والاقتصادي في الفضاء الإلكتروني خاصة مع توجه الدول نحو الإدارة الإلكترونية في إدارة شئونها. استخدمت هذه الورقة المنهج التاريخي والوصفي والتحليلي . وقد توصلت الورقة الي عدة نتائج، هي إن اتساع نطاق استخدام وسائل الاتصال وتكنولوجيا المعلومات وكثافة التفاعلات الدولية في الشبكة العنكبوتية افرز انتشار الأنشطة غير السلمية في الفضاء الإلكتروني، ومن اهم التوصيات ضرورة الحذر والحيطة عند استخدام البيانات والمعلومات في المجال الافتراضي، اصدار تشريعات دولية تحرم تلك الهجمات ضرورة التعاون الدولي في مجال مكافحة الجرائم الالكترونية

الكلمات المفتاحية: القرصنة, أمن الدول، الفضاء الالكتروني

.

المقدمة

أصبح العالم اليوم يشهد تطوراً في المخاطر الأمنية مع تطور مراحل النضج التكنولوجي لوسائل الاتصال من مرحلة النمو السريع إلى مرحلة الاستخدام الكثيف لهذه الوسائل، فقد أدى هذا الاستخدام إلى تهديد أمن الفضاء الإلكتروني من خلال استخدامه بصورة سلبية خاصة من قبل القراصنة (الهاكرز) حيث لم تسلم فضاءات تبادل المعلومات ومواقع التواصل الاجتماعي من هجماتهم المتمثلة في السطو على الصور والبيانات الشخصية، واستخدامها للابتزاز والمساومة والتشهير إضافة إلى استغلال بيانات الحسابات الشخصية والاعتداء على أنظمة المعلومات، فرضت تلك الاستخدامات إعادة التفكير في مفهوم الأمن الذي لم يعد مرتبطاً بالقدرات العسكرية للدولة فقط، بقدر ما هو مرتبط بالحفاظ على الأمن في الفضاء الإلكتروني1.

أهمية البحث

تأتي اهمية هذه الورقة من اهمية الفضاء الإلكتروني واهمية العمليات اليومية التي تتم استخدامها فيه سواء العسكرية أو السياسية أو الاقتصادية، إذ مع كثافة التفاعلات الدولية في هذا الفضاء الالكتروني انتشرت الانشطة غير السلمية فيه، والتي من ابرزها هجمات القرصنة الالكترونية التي جعلت الفضاء الالكتروني بيئة غير آمنة.

مشكلة البحث :

تتمثل مشكلة البحث في دراسة الفضاء الالكتروني وعمليات القرصنة التي تتم من خلاله، واثر تلك الهجمات الإلكترونية على أمن بعض الدول.

هدف البحث :

معرفة مدي تأثير القرصنة الإلكترونية علي امن الدول، وتسليط الضوء علي أهم الهجمات التي نفذها القراصنة الإلكترونيين.

فرضيات البحث:

ان اتساع نطاق استخدام وسائل الاتصال وتكنولوجيا المعلومات وكثافة التفاعلات في الشبكة العنكبوتية افرز أنشطة غير سلمية في الفضاء الإلكتروني والتي من ابرزها هجمات القرصنة الإلكترونية. ان توجه الدول إلي الإدارة الإلكترونية في إدارة شؤونها العامة جعلها هدف لهجمات القرصنة الإلكترونية التي أثرت علي امن واقتصاديات العديد من الدول.

الفضاء الإلكتروني والأمن الإلكتروني:

الفضاء الإلكتروني عبارة عن فيض رقمي من المعلومات لا يعتمد كلياً على البيئة المحسوبة التي توفرها شبكات المعلومات بل يتعامل أيضاً بكثافة مع

[1] www.siyssa.org.eg/new/2017.aspx, 22/12/2018, 9:30AM.

مفرداته مثل سرعة نقل البيانات وصلاحية الدخول إلى الشبكة، بالإضافة إلى المعالجات التي تتناول البيانات المتدفقة ضمن البيئة الإلكترونية[1].

ويتميز الفضاء الإلكتروني باستخدام الإلكترونيات والمجال الكهرومغناطيسي لتخزين البيانات عن طريق النظم المتصلة والمرتبطة بالبنية التحتية الطبيعية ويتكون من المكون الطبيعي والمادي والذي يعكس شكل المعلومات في الفضـــاء الإلكتروني "Soft Ware"، أما المكون الثالث فيتمثل في عملية التواصل بين المعلومات والبشر وحركة التفاعل ما بين البرمجيات والمعدات وارتباط ذلك بتصورات وقيم وسلوك المستخدمين من البشر.

يؤكد خبراء أمن المعلومات أن الحلقة الأضعف في عملية الاختراق هو العنصر البشري، حيث الأخطاء البشرية هي التي تؤدي إلى عمليات الاختراق الواسعة أو حتى المستحيلة، وعلى سبيل المثال يؤكد الخبراء أن عملية اختراق شركة "RSA" والتي تعتبر من أشهر الشركات في أمن المعلومات والتي تفترض ن تتمتع بإجراءات صارمة فيما يخص الأمان، ولكن كل ذلك لم يمنع من اختراقها، حيث تسبب خطأ بشري صغير بعملية اختراق واسعة طالت أنظمة الشركة وعملائها[2].

أصبح المفهوم الجديد للأمن القومي يدور في فلك الحفاظ على أمن الدولة في ظل تطور وسائل الاتصال، ومن ثم أختلفت آليات التعامل معهاً، وأصبح الأمن انعكاساً للمرحلة التاريخية التي يمر بها وطبيعة الصراع الدولي في ظل الموجه المعلوماتية التي يشهدها العالم، وقد انعكس ذلك على تغير مفهوم الأمن حيث أثرت الثورة التكنولوجية على دور الفاعلين الدوليين، وتغير شكل الحرب وأدواتها وعمل أجهزة الجيش.

وظهرت أشكال جديدة من الهجمات والتي غلب عليها الطابع التكنولوجي، كالقرصنة الإلكترونية التي تتم داخل الشبكات متعدية حدود الدول والتي شملت دولاً وأطرافاً من غير الدول.

فرضت تلك التحديات إعادة التفكير في الأجندة الدولية خاصة مع اتساع مفهوم الأمن، والذي أصبح يرتبط بتلك الدرجة التي تمكن الدولة من أن تصبح في مأمن من خطر التعرض لهجوم إلكتروني.

وتعني كلمة الأمن في مجال الفضاء الإلكتروني إجراءات الحماية ضد التعرض للأعمال العدائية والاستخدام السيئ لتكنولوجيا الاتصال والمعلومات، ومن جهة أخرى فإن الأمن القومي يُعني بحماية وغياب التهديد لقيم المجتمع الأساسية وغياب الخوف من خطر تعرض هذه القيم للهجوم، وتشير كلمة الأمن إلى طيف واسع من المجالات ضمن وخارج حقل تقنية المعلومات.

ويتميز الأمن الإلكتروني بعدد من الخصائص أهمها السرية من خلال التأكد أن المعلومات لم تصل لأشخاص غير مخولين بالحصول عليها، والتأكد من صلاحية الاتصال والرسالة أو مصدر هذه المعلومات، ويتميز الأمن الإلكتروني بتوافر التكامل الذي يعني جودة أي نظام للمعلومات ومدى صحة وموثوقية نظام التشغيل، وإيضاً التشغيل، والتكامل المنطقي للتجهيزات والبرمجيات التي توفر آليات الحماية ومدى التناغم بين المعلومات مع البيانات المخزنة، وهناك خاصية التوافر والإتاحة من خلال الوصول الموثوق للبيانات وخدمات المعلومات عند الحاجة إليها من قبل الاشخاص المخولين بذلك، وخاصية مكافحة الأنكار من خلال التأكيد بان مرسل البيانات قد حصل على وصول البيانات إلى المرسل إليه، وبان المستقبل قد حصل على إثبات شخصية المرسل مما يمنع احتمال انكار أي من الطرفين بأنه قد عالج هذه البيانات.

القرصنة الإلكترونية: لم تعد سرقة أجهزة الحاسب الآلي بعينها تمثل أهمية لصاحبها بقدر ما تمثله المعلومات والبرامج المخزنة فيما من أهمية، وتتمثل السرقة في أختراق الشبكات أو سرقة المعلومات المخزنة، كما قد تشمل التحويلات المالية[3]، غير المشروعة وغيرها من العمليات وتتم هذه العمليات أو الهجمات من خلال ما يطلق عليهم القراصنة أو الهكرز (Hackers).

والقرصان الإلكتروني هو المبرمج القادر على اختراق النظم الأمنية في الفضاء الإلكتروني أو مكتشف الثغرات[4]، ويقوم بتنفيذ عملية الاختراق عادة شخص أصطلح على تسميته بالقرصان أو الهاكر وهو في العادة شخص له معرفة عميقة بالحواسيب وشبكاتها، ويملك مهارة عالية في لغات البرمجة وأنظمة التشغيل، ويعتبر غالباً بمثابة خبير في هذا المجال بحيث يستطيع بمهارته استغلال نقاط الضعف في أي شبكة حاسوب لاختراقها، وكانت كلمة قرصنة في الأصل تحمل معنى إيجابياً قبل أن تتحول إلى المعنى السلبي الذي تركز عليه وسائل الإعلام حالياً[5].

ويقسم المهتمون بمتابعة تكنولوجيا المعلومات وأخبارها قراصنة الانترنت عادة إلى قسمين: القراصنة الأخلاقيين (القبعات البيض) والقراصنة

[1] عادل عبد الصادق، الفضاء الإلكتروني وتهددات جديدة للأمن القومي، 2011م، على الموقع:
www.accronline.com/artical-data.com-12/12/2018, 8:10AM 11 فبراير 2013

[2] . www.alwght.con/ar/News/124178-14/12/2018,9:50AM

[3] ذياب البداينة، **الأمن اوحرب المعلومات**، ط 2، دار الشروق للنشر والتوزيع، الأردن، 2006م، ص 14.

[4] أحمد أبو طالب، **القرصنة السياسية عبر الفضاء الإلكتروني**، مجلة السياسة الدولية، العدد 87، 2012، 108.

[5] http://www.aljazeera.net/knowlegdedate/mewscoverage/2015/1/5%D8-12/12/2018,10:00AM.

المجرمين (القبعات السود)، ويضاف إليهما أحيانا قسم ثالث هم أصحاب القبعات الرمادية.

وأنشطة الاختراق التي تعرف باسم "Hackivism" تشمل اختراق مواقع الانترنت الحكومية أو المؤسسية أو الإعلامية أو الشركات الخاصة أو القطاع المصرفي أو نظم تقنية المعلومات، من أجل ايصال رسالة ذات طبيعة سياسية أو اقتصادية أو اجتماعية.

أدت علاقة الفضاء الإلكتروني بعمل عدد من المنشآت الحيوية سواء كانت مدنية أو عسكرية لإمكانية تعرضها لهجوم من خلال استهدافها لوسيط للخدمات، أو بشل عمل أنظمتها المعلوماتية مما يؤثر على أدائها، ومن ثم فإن التحكم في تنفيذ هذا الهجوم يعد أداة سيطرة ونفوذ بالغة الأهمية[1].

وقد أصبحت هجمات القرصنة الإلكترونية تمثل تهديداً حقيقياً لاقتصاديات وأمن الدول، فقد ظهرت أسلحة إلكترونية جديدة "Cyberweapon" ومتعددة كالفيروسات وهجمات انكار الخدمة والاختراق والتشويش، ويؤدي التعرض لهجوم مباشر إلى اتلاف كم هائل من أوامر السيطرة على أجهزة الكمبيوتر ونظم ربط الشبكات ومن ثم يحدث شلل تام أو جزئي في قدرة النظام على الرد على طلبات المستخدمين المدنيين والعسكريين، ويمكن لشخص واحد أن يحدث مثل هذا الشلل في شبكة أو مجموعة شبكات مترابطة.

وتطورت الهجمات الإلكترونية من مجرد عمليات بحث بدافع الفضول في البدء لعمليات جيدة التمويل والتنظيم من التجسس السياسي والعسكري والاقتصادي والتقني، فقد تم الكشف عن شبكة تجسس إلكترونية تعمل في الصين تمكنت من اختراق 1295 جهاز كمبيوتر في 103 دولة وتعد الحادثة الأكبر في العالم من حيث عدد الدول التي تم اختراق شبكاتها وأجهزتها ومنها وزارات الخارجية في كل من أيران وبنغلاديش ولاتفيا وأندونيسيا والفلبين وبروناي وتايلند وبوتان، وتم اكتشاف أجهزة تنصت على الكمبيوتر في سفارات كل من الهند وكوريا الجنوبية واندونسيا وقبرص ومالطا وتايوان والبرتغال والمانيا وباكستان[2].

أبرز هجمات القرصنة الإلكترونية:

أُتهمت الصين في 2009م بالوقوف وراء سرقة البيانات من برنامج مقاتلات (إف 35) التابع لشركة "لوكهيد مارتن" الأمريكية التي تعد أحدث طائرة في العالم، وفي أغسطس 2009م تمكن الأمريكي البرت غونز اليسن البالغ من العمر 28 عاماً بالتعاون مع قرصانيتين روسيتين من سرقة بيانات لـ 130 مليون بطاقة مصرفية ونقلها إلى خوادم في أوكرانيا وهولندا ولاتفيا[3]، كما أن السلطات الأمنية الأمريكية وصفت العملية بأنها أكبر عملية قرصنة إلكترونية في تاريخ الولايات المتحدة في ذلك الوقت من دون التطرق إلى الخسائر المالية المترتبة عليها وقد حكم على غونز إليس لاحقاً السجن بمدة عشرين عاماً.

وفي يناير 2010م عطلت جماعة تطلق على نفسها اسم "الجيش الإيراني السيبراني" خدمة البحث على الانترنت لمحرك البحث الصيني الشائع (بايدو) وكان يتم تحويل مستخدمي محرك البحث إلى رسالة سياسية إيرانية[4].

أفاد تقرير حكومي رسمي للجرائم الإلكتروني نشرته جامعة الأمن العام الصينية أن هجمات القرصنة كلفت الاقتصاد الصيني 46 مليار دولار أمريكي في الفترة من يونيو 2011 إلى يونيو 2012م.

في نفس العام اخترق الجيش الرقمي الباكستاني مكتب التحقيقيات المركزي الهندي، وردت الهند باختراق حواسيب الجيش وبعض الوزارات.

وفي يناير 2011م أعلنت الحكومة الكندية تعرض وكالاتها لهجوم إلكتروني ضخم من بينها وكالة البحث والتطوير الدفاعي الكندية، وأجبرت الهجمات وزارة المالية ومجلس الخزانة الكنديين على فصل اتصالهما بالانترنت، وفي يوليو 2011م أعلن وزير الدفاع الأمريكي أن قراصنة انترنت سرقوا 24 ألف ملف من وزارة الدفاع في عملية واحدة خلال شهر مارس 2011م.

كما أنه في يناير 2012م تمكن قرصان سعودي يدعي "أوكس عمر" من اختراق خوادم سلاح الجو الإسرائيلي، وذكرت وسائل الإعلام الإسرائيلية أن عمر دخل بطريقة مفاجئة بعد غياب لعدة أشهر على سيرفر تدريب الطيارين، وحصل على كمية كبيرة من البيانات والصور والهويات والشهادات[5].

تعرضت في أغسطس 2012م شركة النفط الوطني السعودية (أرامكو) لهجوم ساهم في تدمير آلاف أجهزة الحاسوب، وأدى إلى تعطيل نحو آلف حاسوب، لكنه لم يؤثر في العمليات الحيوية المتعلقة بالنفط.

وقد شن في سبتمبر 2012م ناشطون إيرانيون هجمات إلكترونية على مدى 12 شهراً أستهدفت – حسب وكالة رويترز – بنك "أوف أميركا" و"جي بي مورغان" و"سيتي غروب". وفي أكتوبر 2012م قرصان سعودي يدعي "فارس" اخترق موقع صحيفة "جيروزاليم بوست" الإسرائيلية ورفع عليه علم بلاده.

---

[1] الأمن السيبراني والأمن المعلوماتي. http://www.linkedin.com/plus/hanen-ali@saada-14/12/2018,9.30AM .

[2] عادل عبد الصادق، **كابلات الانترنت في الشرق الأوسط، ملف الإرهاب السياسة والإستراتيجية**، مجلة الإهرام، العدد 160، أبريل 2008م، ص 45-46

[3] القرصنة الإلكترونية https://www.dw.com/ar/t/119111848 2013/2/24م، 9:30AM.

[4] الجزيرة نت.

[5] http://mwdia.emaitalyoum.com/images/po;oply.inline-imeges/2012/01/ar22-1112-111.hjp92-13/12/2018,9:30AM .

وقد شنت في أبريل 2013م مجموعة "أنونيموزس" هجوماً على مواقع إسرائيلية دعماً للأسرى والقضية الفلسطينية، وشملت القائمة مواقع مالية، وسياسية، ووزارة الدفاع، وموقع جهاز الأمن الداخلي (الشاباك)، والصناعات العسكرية الإسرائيلية، إضافة إلى موقع مكتب الإحصاء الرسمي، وموقع وزارة التربية والتعليم، وعشرات المواقع الأخرى وآلاف الحسابات الإسرائيلية على موقعي فيسبوك وتوتير. وفي نفس العام صرحت خدمة الاتصال المرئي "سكايب" بأنها تعرضت لاختراق، ولكنها قالت أن بيانات المستخدمين لم تتضرر، جاء ذلك بعد يوم على إعلان الجيش السوري الإلكتروني المؤيد للرئيس بشار الأسد أنه تسلل إلى حسابات "سكايب" على مواقع للتواصل الإجتماعي.

هاجمت مجموعة "سايبر بيركوت" الأوكرانية في مارس 2014م المواقع الإلكترونية لحلف الناتو، والمتحدثة باسم الحلف "أونا لونغكيسكو" قالت أن "الهجوم أدى إلى تعطيل مواقع الحلف لعدة ساعات"[1].

كما أدي الهجوم علي البرلمان الألماني عام 2015 والذي يشتبه بتورط اجهزة سرية روسية بتنفيذه الي حدوث فوضي كبيرة .فقد استهدف الهجوم 20 الف جهاز حاسوب يستخدمهم السياسيون الألمان والموظفون المدنيون، وتمكن المهاجمون من سرقة بيانات حساسة طالبوا علي اثرها بعدة ملايين ليتراجعوا.

وبالرغم من تصريح مجموعة من القوميين مسؤوليتهم عن ذلك الهجوم بهدف الضغط علي الحكومة الألمانية وقتها للتوقف عن دعم أوكرانيا. فقد أفادت التقارير أن أفراد من المخابرات الروسية كانت متورطة بذلك، تكمن خطورة هذه الهجمات في أن خطورة سرقة الملفات السرية، واستغلالها من قبل القراصنة تهدد الامن الاجتماعي والسياسي للدولة[2].

وقد اتهمت إدارة الرئيس الامريكي "دونالدترامب" في 23\3\2018 مجموعة من عشرة قراصنة إلكترونيتان إيرانيين بتنفيذ واحدة من اكبر حملات القرصنة التي ترعاها الدول ضد الولايات المتحدة الامريكية فقد استهدفوا عشرات الجامعات والشركات والهيئات الحكومية الأمريكية علي نطاق العالم وسرقوا بيانات وملكيات فكرية يبلغ حجمها (31 تيرابايت).

وذكر تقرير نشرته مؤسسة كارنيغ للسلام الدولي في يناير 2017م أن الهجمات الإلكترونية أصبحت وسيلة رئيسية للنظام الايراني فهي تمنحه فرصا اقل خطورة لجمع المعلومات والرد علي الاعداء في الداخل والخارج وذكر المسؤول الأول للتكنولوجيا بشركة "ماكافي" للأمن الإلكتروني "ستيف غرويمان" أن دولة مثل ايران يمكنها الحصول عن طريق سرقة الملكيات الفكرية إلكترونيا مالا تستطيع تطويره بنفسها من خلال استثماراتها الخاصة، أن سرقة الملكية الفكرية هي سرقة مستقبل وسرقة أمن قومي قادم ومستقبل شركات واعمال تجارية وسرقة لموارد مجتمعات ووظائف عالية المردود ومستويات معيشة مستقبلية لشعوب بأكملها[3].

وفي يوم الثلاثاء الموافق 27/يونيو/2016م طال هجوم معلوماتي جديد أجهزة كمبيوتر في مختلف أنحاء العالم، الهجوم تم بواسطة فيروس يعرف باسم "بيتيا" وهو برنامج خبيث يطال أجهزة الكمبيوتر ولا يتركها إلا بعد تحويل مبلغ من المال، وقد طالب منفذو الهجوم دفع مبلغ من المال بعملة "بنتكوين" الإلكترونية لقاء تحرير كل جهاز كمبيوتر والبلدان التي طالها الهجوم المعلوماتي هي (الدنمارك، فرنسا، المانيا، هولندا، أسبانيا، أوكرانيا، روسيا، الهند وغيرها)[4].

وتزايدت الهجمات الإلإلكترونية عبر الانترنت وسط ارتفاع حدة خطورتها أيضاً وتعد هجمات ما يعرف بفيروس الفدية واحدة من أكثر أنواع الهجمات[5].

وقد أعلنت وكالة الشركة الأوربية "يوروبول" في 2016/12/1م عن تفكيك شبكة مختفية في الجريمة عبر شبكة الانترنت كانت تنشط في نحو مائة وثمانين دولة وقد ألحقت أضراراً بنصف مليون حاسوب وتسببت في خسائر قدرت بمئات الملايين من اليورهات.

كما أن هنالك شبكة تسمى "أفالانش" كانت تقوم منذ 2009م وحتى 2016م بهجمات إلكترونية بمساعدة برمجيات خبيثة كما عملت على تجنيد وسائط مكلفة بتبيض أموال لحساب منظمات إجرامية. وقد ضبط أجهزة خوادم ونطاقات مواقع إلكترونية ثم استخدامها لمواجهة عملاء مصرفيين على شبكة الانترنت[6].

وقد أعلنت جماعة قراصنة تطلق على نفسها أسم "وسطاء الظل" وتستخدم برمجية خبيثة، تطلق عليها "Wannacry" أنها اخترقت وكالة الأمن القومي في 2016م وقامت مرة أخرى في أبريل ببعث رسالة احتجاج إلى الرئيس الأمريكي

[1] خالد وليد محمود، الهجمات عبر الانترنت ساحة للصراع الإلكتروني الجديد، المركز العربي للأبحاث ودراسة السياسات، 2003م، ص 11.

[2] www.acees.gv.bh، الأربعاء 2019/5/2م، الساعة 9:30 صباحاً.

[3] Aljazeera.net، الأربعاء 2019/5/2م، الساعة 10:15 صباحاً.

[4] http://arbic.euronews.com/2012/06/27/a-ware-of-cyber-attack-strike-companies-in-several-countries-15/12/2018,8:30AM .

[5] http://www.skynewsarabia.com-14/12/2018,11:00AM .

[6] http://arabic.euronews.com/2016/12/01.eurpt.operationavalancne-strike-at-golobal-online-crim-networt. 10/12/2018,9:30AM

"ترامب" وأفصحت عن تفاصيل اسحتواذها على برمجيات استخدمتها وكالة الأمن القومي الأمريكي للتجسس[1].

وقد أطلق وسطاء الظل في أبريل 2017م مجموعة من أدوات القرصنة التابعة لوكالة الأمن القومي، وقد عطلت برمجية "الفدية الخبيثة" 300 ألف جهاز[2].

وقد صرح وسطاء الظل أنهم استغلوا متصفحات الويب، وأجهزة التوجيه، والهواتف الذكية، وبيانات شبكة تحويل الأموال الدولية "سويفت"، فضلاً عن بيانات شبكات البرامج النووية والصينية والأيرانية، أو الكورية الشمالية، والصواريخ النووية للوصول إلى أهدافهم وقد أكدت شركة مايكروسوفت[3]. في 14 أبريل 2017م أنها أصلحت الثغرات الموجودة في أصدارات متعددة من نظام التشغيل "ويندوز" التي كشفت عنها التسريبات التي نشرتها مجموعة القراصنة الإلكترونية المعرفة باسم سماسرة الظل (Shadow Broker)[4].

وقد تعرضت ما يقرب من 150 دولة والآلاف المؤسسات لقرصنة إلكترونية في يوم الجمعة 12 مايو 2017م لهجمات إلكترونية، وهو ما وصفه البعض بالهجوم الأكبر في التاريخ، وقد وصفت الخسائر على الأمن الإلكتروني بأنها لا تقل عن الخسائر الي نتجت عن أحداث الحادي عشر من سبتمبر 2011م[5].

وقد نجمت هذه الهجمات أيضاً عن ما يسمى بفيروس "الفدية الخبيثة"، ولم يقتصر هذا الفيروس على تشفير بيانات أجهزة الكمبيوتر في مؤسسات حكومية، بل طال شركات أعمال خاصة مثل مصنع سيارات "نيسان" في بريطانيا ومصنع سيارات "رينو" في سلوفينا، وشركة "تليفونيكا" العملاقة للاتصال في أسبانيا[6]. وقد ذكرت رئيسة الوزراء البريطانية "تيريزا ماي" ان هجمات إلكترونية استهدفت خدمة الصحة العامة "إن أتش أس" عشرات المستشفيات في بريطانيا[7]. كما أعلنت وزارة الداخلية الروسية في الوقت ذاته تعرض اجهزة الكمبيوتر التابعة لها لهجوم فيروسي.

وهذه الموجه من الهجمات التي تمت على مستوى عالي أثارت قلق خبراء المعلومات الذين لفتوا النظر إلى أن القراصنة قد يكونوا استفادوا من ثغرة أمنية في أنظمة "ويندوز" كشفت النقاب عنها وثائق سرية خاصة بوكالة الأمن القومي الأمريكية التي تمت قرصنتها.

وقد أكدت في ذلك الوقت وزارة الأمن الداخلي الأمريكية في بيان لها أنها على إطلاع على تقارير "الأسنوماري" المعروفة باسم "وانا كراي" التي تؤثر على كيانات عالمية متعددة، وهي نوع البرامج الضارة التي تصيب جهاز الكمبيوتر[8].

ويقوم البرامج الخبيث المستخدم بإغلاق ملفات المستخدمين ويجبرهم على دفع فديات مالية تتراوح قيمتها ما بين 300 – 600 دولار في شكل عملة "بيتكوين" الإلكترونية عن كل جهاز من أجل عودته للعمل مجدداً بشكل طبيعي[9].

وقد صرح لاحقاً الرئيس التنفيذي لشركة مايكروسوفت "برادسميت" أن "هجوم واناكري" استخدم عناصر مسروقة من عمليات الحرب السيبرانية التي تملكها وكالة الامن القومي[10].

أثار هجوم واناكري المخاوف من ان الأسلحة السيبرانية القوية لجهاز التجسس يمكن أن تتحول إلى أداة إجرامية، مما يؤكد أن تهديدات الأمن السيبراني قد وصلت إلى مستويات جديدة وخطيرة[11].

وقد شهد العالم مرة أخرى هجوم استهدف شركات كبرى ومصارف وبنى تحتية في روسيا وأوكرانيا وانتقل إلى غرب أوروبا ومنها إلى الولايات المتحدة، وذلك يوم الأربعاء 28 يوليو 2017م، ويعتبر هذا الهجوم هو الأكثر تعقيداً في سلسلة الهجمات التي تستخدم عشرات أدوات القراصنة التي سرقت كما ذكر سابقاً من وكالة الأمن القومي الأمريكية، فقد وصل معدل انشار الهجمات إلى خمسة ملايين رسالة في الساعة وفق شركة "فوسيونت سيكيوريتي" ومع نهاية اليوم الأول فقط من الهجمات أعلنت شركة "أفاست للأمن المعلوماتي" أنها رصدت أكثر من 75 ألف هجوم في 99 بلداً، وهو الذي تجاوز المائة فيما بعد وهدد أكثر من 100 دولة في العالم، ومع استناد هذه الهجمات على برمجيات خبيثة طورتها وكالة الأمن القومي لاستخدامها ضد خصومها.

ووفق هيئة الإذاعة البريطانية شملت الهجمات دولاً من ضمنها (روسيا، الهند، الصين، بريطانيا، فرنسا، إيطاليا، المانيا، البرتغال، فيتنام، تايوان

[1] فاطمة الزهراء، كيف كشفت هجمات الفدية الخبيثة، ثغرات الأمن السيبراني، الأحد 14 مايو، 2017م http://futureuae.com. 9:30AM

[2] http://www.aljazeera.net/news/scienceandtetechnology/2012/15-10:30AM .

[3] مايكروسوفت توكد إصلاح ثغرات، سماسرة الظل، 2017/4/15م

[4] أحمد الخضر، مجموعة القرصنة وسطاء الظل، تهدد بنشر أداه اختراق جديدة في يوليو القادم البوابة العربية للأخبار النصبة.

[5] http://aitnews.com/2017/05/3,8:30AM .

[6] http://futureaae.com/ar/futuerfile/tem/22,9:30AM .

[7] http://www.skynewsarabia.com,8:30AM . السبت الموافق: 13 مايو 2017م

[8] http://www.kuna.net.ku/article.prentpage-aspxid=210082&languagar-12/12/2018,8:10AM .

[9] https://www.masraway.com/news.9:30AM/13مايو 2017.

[10] وكالة الأنباء الكويتية" وسطاء الظل يشنون هجوماً على شبكة الانترنت يثير صدمة في مختلف أنحاء العالم.

[11] صموئيل جليس، مجرد الغارديات، https://www.noonpost.org.content,9:20AM 20/ مايو 2017م.

ودولاً أخرى)، وهو ما أُعتبر أكبر تفش لبرمجيات الفدية في التاريخ. ففي روسيا تضررت وزارتا الداخلية والصحة، وشركة القطارات الروسية الحكومية، وشركة للهواتف المحمولة، بالإضافة إلى بنوك محلية مختلفة[1].

في بريطانيا تعرضت 40 منظمة محلية بريطانية تابعة لنظام الرعاية الصحية وبعض العيادات لهجمات، وهو ما اسفر عن إلغاء بعض العمليات الجراحية، وقد تعرضت عدد من الشركات الأسبانية الضخمة مثل: شركة الطاقة "أبيردرولا"، وشركة غاز "ناتورال" لهجمات، كما تعرضت شركة "تيليكوم" البرتغالية وسكك الحديد الألمانية، فضلاً عن مدارس وجامعات في الصين ومستشفيات في أندونيسيا[2].

بينما سادت حالة الطوارئ دول العالم لمعالجة تداعيات الهجمات جاءت مواجهتها من مصدر غير متوقع هو باحث شاب مجهول الهوية يبلغ من العمر 22 عاماً، وفق شبكة "سي أن أن" ينشط على الانترنت تحت أسم (Malwaretech) حيث اكتشف اعتماد القراصنة على نطاق غير مسجل قام هو بشرائه بمبلغ 10.69 دولارات فقط، ثم إعاد توجيهه إلى ما يسمى (Sinkhole) وهو خادم يوفر تقنية للتضليل تعتمد على توفير بيانات خاطئة بشان نطاق معين، ما يؤدي إلى فشل عملية الوصول إليه، الأمر الذي يجعله فعالاً في الحد من البرمجيات الخبيثة.

وقد كشفت شركة مايكروسوفت عن هجمات الكترونية مرتبطة بقراصنة ايرانيين في اكثر من مائتي شركة خلال 2018-2017م. أن هذه الهجمات اثرت في شركات النفط والغاز وصناعة الآلات الثقيلة في عدة دول وقد واجهت شركات ووكالات حكومية في الولايات المتحدة الامريكية هجمات عنيفة من قبل قراصنة ايرانيين وصينين يعتقد خبراء امنيون انه قد تم تنشيطها بسبب انسحاب الرئيس ترامب من الاتفاق النووي الايراني وصراعاته التجارية مع الصين.

وقد زعمت شركة الأمن السيبراني الأميركي "ويسيكيوريتي Rescurity" أن قراصنة يتمركزون في إيران مسئولون عن اختراق حواسيب البرلمان الاسترالي والأحزاب السياسية في البلاد. وان هذه الهجمات تشكل جزءا من حملة تجسس عالمية بدأت في 2018 واستهدفت تحالف "الأعين الخمس five Eye" الذي يضم الولايات المتحدة وكندا والمملكة المتحدة واستراليا ونيوزلندا، واعتبرتها انتقاما من قرار الرئيس الأمريكي "دونالد ترامب" نتيجة انسحابه من الاتفاق النووي الإيراني[3].

وقد أتهم قراصنة مدعمون من قبل الحكومة الصينية باختراق الموقع الالكتروني التابع لمكتب إدارة الشؤون الشخصية الولايات المتحدة الأمريكية بسرقة بيانات حوالي 22 مليون موظف حالي وسابق في الحكومة الأمريكيون اضافة الي سرقة تصاميم طائرات عسكرية امريكية .

وتأتي خطورة هذا الاختراق في أن التسلل لقواعد البيانات الحساسية بالدولة والوصول لحقائق البنية المعلوماتية لها، يُمكن رصد نقاط الضعف والمشاكل التي تواجهها علي مختلف مستوياتها إضافة الي أن اختراق والمؤسسات العسكرية يهدد الامن العسكري القومي للدولة.

اذ ان الاعتداءات المستمرة علي شبكات المعلومات واحتراق بعض البيانات والمعلومات الحساسة والمهمة الخاصة بالحكومة خاصة من دول مثل الصين وروسيا.

وقد كبدت الصناعة الأمريكية خسائر تقدر ب 400 مليار دولار امريكي في 2018.

وكانت مجموعة القراصنة "غادر-ينز أوف بيس" (جي أو ي) قد اخترقت بيانات مؤسسة "سوني" وتمكنت من الحصول علي اسرار الشركة وهددت بكشفها. حيث تفاجا العاملون بالشركة باحتراق حواسيبهم الخاصة وعلها رسالة من طرف القراصنة، تتمثل في صورة هيكل عظمي وبه رسالة موجهة إلي الشركة تفيد باحتراقها والاستيلاء علي معلومات سرية ورسائل بريدية خطيرة لمسؤولي الشركة المذكورة.

وفي هذا السياق اصدار مكتب التحقيقات الفيدرالي الامريكي بيانات يتهم فيه هذه المجموعة من القراصنة بخدمتها لصالح كوريا الشمالية، وذلك من خلاله ادلة واستنتاجات ناجمة عن عمليات سابقة لبرامج إلكترونية خبيثة تستخدم في تلك الدولة. فقد اشارت التحقيقات لتطابق هذه العملية مع العملية التي نفذتها كوريا الشمالية، في شهر مارس 2014 ضد مصارف ووسائل إعلام كورية جنوبية، ويرجع بعض المحللين عملية القراصنة علي مؤسسة "سوني" كرد علي الفيلم السينمائي الذي انتجته الشركة بعنوان المقابلة، وهو فيلم كوميدي يسخر من رئيس كوريا الشمالية. وقد بين مكتب التحقيق الفيدرالي الأميركي أن الخطر الجسيم لهذه العملية يكمن في تسريب معلومات سرية وتهديد شخصيات اميركية وازنة في صناعة السينما والتلفزيون.

ثغرات الأمن الرقمي هي معضلة الدفاع السيبراني ففي الوقت الذي شنت فيه جماعة قرصنة غامضة هذه الهجمات فقد استطاع ناشط غامض أيضاً

[1] .http://www.skynews.arabia.com.السبت 13/ مايو2017م، 9:30 صباحاً.

[2] نورة شلوس، القرصنة الإلكترونية في الفضاء السيبراني، التهديد المتصاعد على أمن الدول، مجلة مركز بابل للدراسات الأسبانية، 2018، المجلد 20، العدد 2.

[3] قراصنة إيران يستهدفون خصومها واشنطن، العربي الجديد 9 مارس 2019 الاربعاء 2019.

صدها، وقد وقفت الأجهزة الأمنية عاجزة أمام هذا الهجوم مما يكشف الفجوة الكبيرة بين أجهزة الحماية من جانب وبين قراصنة الجريمة من جانب آخر.

اعتماد الهجمات على برمجيات تم تطويرها من قبل وكالة الأمن القومي الأمريكي اعتماداً على ثغرات اكتشفتها في نظام تشغيل ذي انتشار عالمي أثار الجدل بشأن مشروعية مثل تلك المعلومات التي لها تبعات مدمرة على الأمن العالمي، خاصة في ظل احتمالات تعرض تلك الجهات الأمنية للاختراق ووقوع مثل تلك المعلومات في أيدي الجماعات الإجرامية كما هو الحال في تلك الهجمات.

هذا الأمر صار قضية حساسة بالنسبة للولايات المتحدة الأمريكية بعد أن أخذت مجموعة وسطاء الظل في نشر أدوات البرمجيات المسروق من مخزون حكومة الولايات المتحدة من أجهزة القرصنة الخاصة بها[1].

ورغم تقديم مايكروسوفت تحديثات لعلاج الثغرات حثت المستخدمين على تحميلها، إلا أن العاملين بمجال الأمن أكدوا من عدم إمكانية تحميل تلك التحديثات على نطاق كبير، خاصة مع استخدام نسخ أقدم مثل ويندوز (أكس بي)[2].

مخاطر الهجمات الإلكترونية:

أن المجهولية وغياب الرقابة التشريعية والتنظيمية عن تلك المعاملات المشفرة يثير المخاوف بشأنها، لا سيما بعد أن باتت وسيلة لتحصيل الفدية في حالة الهجمات الخبيثة.

استهداف المؤسسات الصحية: أشار تقرير (أي بي إم – أكس فورس للأمن الرقمي) لعام 2016م إلى أن مؤسسات الرعاية الصحية باتت هي الأعلى تعرضاً للهجمات الرقمية (مما يعرض حياة المئات من المرضى للخطر).

دوافع مالية: أشار تقرير قسم الجرائم الحاسوبية وقضايا الملكية الفكرية الأمريكي، إلى أن هناك 4000 هجوم من برمجيات الفدية الخبيثة عبرت يومياً منذ بدء عام 2016م.

كذلك تقرير "فيروزن" للابتكار الرقمي حول التحقق من اختراق البيانات لعام 2016م، والذي تضمن تحليل 100 ألف واقعة و2260 اختراقاً في 82 دولة. أوضح إن 89% من الهجمات الإلكترونية تتضمن دوافع مالية أو تجسسية – هيمنة الشركات الكبرى – إذ أن أحد أسباب الانتشار الكبير للبرنامج هو الاستخدام العالمي واسع النطاق لنظام "ويندوز" الذي أنتجته شركة "مايكروسوفت". أشار تقرير شركة ديل السنوي للتهديدات الأمنية في عام 2016م إلى أن البرمجيات الخبيثة تضاعف عددها إلى 8.19 مليار، فيما أصبحت أنظمة "أندرويد" هي الأكثر استهدافاً.

في الوقت نفسه غيرت الهجمات الإلكترونية من طبيعة التفاعلات الدولية، حيث بدأت بعض الدول تعتمد عليها لحسم الصراعات لصالحها، وتجلي ذلك على سبيل المثال، في أتهام روسيا بالتدخل في انتخابات الدول الغربية لقرصنة الحملات الانتخابية للتأثير على فرص فوز المرشحين، كما الحال في الانتخابات الأمريكية التي فاز بها الرئيس الأمريكي "دونالد ترامب" بل إن الاتهامات بالقرصنة الإلكترونية طالت روسيا من قبل الحملة الانتخابية لمرشح الوسط في الانتخابات الفرنسية "إيمانويل ماكرون" والذي فاز بمنصب الرئاسة في السابع من مايو 2017م في فرنسا.

ونجد أن هناك 120 دولة تقوم بتطوير طرق لاستخدام الانترنت كسلاح لاستهداف أسواق المال ونظم الكمبيوتر الخاصة بالخدمات الحكومية، وتقوم أجهزة الاستخبارات الدولية بالفعل باختبار شبكات الدول الأخرى بصورة روتينية بحثاً عن ثغرات لتوظيفها عند الضرورة.

وقد تم الكشف عن 1.7 مليار هجمة إلكترونية في يونيو 2018م، وقد صرح المسؤولون إلى أنه قد حان الوقت للتطلع إلى طرق جديدة لمحاربة الفوضى التي تعم فضاء الأمن الإلكتروني[3].

ونتيجة لكل تلك العمليات والهجمات وما يحدث من الفضاء الإلكتروني فإن قضية أمن الفضاء الإلكتروني أضحت قضية دولية تحظى بالمزيد من الاهتمام بشكل جعلها أحدى أوليات الأمن القومي في العديد من الدول بل ارتباطها بالأمن الدولي ككل وهذا يتطلب أهمية التعاون الدولي في مجال تأمين الفضاء الإلكتروني.

ان دعم الإمن الإلكتروني يتطلب عدد من الإجراءات من قبل مجموعة الأنشطة والإجراءات التكنولوجية وغير التكنولوجية بهدف حماية شبكات المعلومات والاتصال وما تتضمنه من برمجيات ومعدات وتطبيق إجراءات وأنشطة حماية تخدم عمليات التأمين من قبيل البحث والتطوير ورفع الوعي بالثقافة العالمية لحماية الفضاء الإلكتروني كمرفق دولي يهم المجتمع الدولي، وهذا ما يتطلب وجود إستراتيجية خاصة أهم معاييرها.

إدراك درجة العلاقة بين الفضاء الإلكتروني والأمن القومي وقضايا التنمية والاستقرار السياسي.

[1] مفاجأة "الأمن القومي" الأمريكية وراء الهجمات الإلكترونية، نيويورك تايمز. http://www.youm7.com.stor/1/7/2018,8:30AM .

[2] فاطمة الزهراء عبد الفتاح، كيف كشفت هجمات الفدية الخبيثة ثغرات الأمن السيبراني، الأحد 14 مايو 2017م، http://futureuae.com/ar/mainpage/item/2793,12/12/2018,11:00 .

[3] http://www.skynewnewarabia.com,8:30AM الثلاثاء 28 يونيو 2018.

- أهمية وجود هيكل تنظيمي أو مؤسسي يتولى مواجهة تلك المخاطر، ويعمل على الحفاظ على مراجعة سياسية الأمن واكتشاف الثغرات وتطوير الحماية وفهم الأخطار المرتطبة بالاستخدام السيء لتقنية تكنولوجيا الاتصال وكيفية التعامل معها.
- أهمية دور الأفراد في عملية الأمن بمعرفتهم بالإجراءات الأمنية التي يمكن أن تستخدم لتأمين مصادر تكنولوجيا الاتصال والمعلومات، مع ضرورة عقد اتفاقيات دولية لحماية الفضاء الإلكتروني.

الخاتمة:

نخلص إلى أن الاستخدامات غير السلمية للفضاء الإلكتروني أدت إلى تهديد أمن الدول، خاصة مع عدم وجود اتفاقية دولية تنظم الفضاء الإلكتروني واستخداماته وتحدد الواجبات والمسؤليات في العمل على حفظ أمنه.

وأصبح التفوق في مجال الفضاء الإلكتروني عنصراً حيوياً في تنفيذ عمليات ذات فاعلية، وتعتمد قدرة الهجوم في الفضاء الإلكتروني على نظم التحكم والسيطرة، وقد أوجدت ملايين أجهزة الكمبيوتر المنتشرة في كل مكان عالماً أفتراضياً نشا نتيجة عملية الاتصال والتفاعل في الفضاء الإلكتروني، ومثل وسيطاً جديداً للقوة حيث يمكن للقراصنة دخول الفضاء الإلكتروني والسيطرة على الأجهزة وسرقة المعلومات وإفسادها أو تعطيلها، ومع زيادة اعتماد الدول والمؤسسات والأفراد على أجهزة الكمبيوتر أصبح الانترنت مرادف لاستخدام الذكاء الاصطناعي، وأصبح الفضاء الإلكتروني بقعة غير امنة.

ومن أهم النتائج التي تم التوصل إليها:

- أن اتساع نطاق استخدام وسائل الاتصال وتكنولوجيا المعلومات مع كثافة التفاعلات الدولية في الشبكة العنكبوتية، نتيجة لسهولة استخدامها ورخص تكلفتها والسرعة في وصول المعلومات جعل كل ذلك الفضاء الإلكتروني بيئة غير آمنة من خلال الاستخدامات غير السلمية التي تتم فيه.
- أن الاستخدام غير السلمي للفضاء الإلكتروني من خلال هجمات القرصنة التي تحدث فيه جعله غير آمن خاصة مع توجه الدول إلى تبني الإدارة الإلكترونية في إدارة شئونها العامة.
- أثرت هجمات القرصنة التي تمت في الفترة الماضية على أمن واقتصاديات العديد من الدول.

ومن أهم التوصيات:

- ضرورة الحذر والحيطة من قبل الأفراد والحكومات عند استخدام البيانات والمعلومات في المجال الافتراضي.
- ضرورة عقد اتفاقيات دولية للفضاء الإلكتروني.
- تعزيز التعاون الدولي في مجال مكافحة القرصنة الإلكترونية.
- ضرورة وجود قوانين دولية وإقليمية لمحاربة القرصنة الإلكترونية.

قائمة المراجع:

1. أبو طالب، أحمد، القرصنة السياسية عبر الفضاء الإلكتروني، مجلة السياسة الدولية، العدد 87، 2012م.
2. الخضر، أحمد، مجموعة القرصنة وسطاء الظل، تهدد بنشر أداه اختراق جديدة في يوليو القادم البوابة العربية للأخبار النصبة.
3. محمود، خالد وليد، الهجمات عبر الانترنت ساحة للصراع الإلكتروني الجديد، المركز العربي للأبحاث ودراسة السياسات، 2003م.
4. البداينة، ذياب، الأمن اوحرب المعلومات، ط 2، دار الشروق للنشر والتوزيع، الأردن، 2006م.
5. عبد الصادق، عادل، كابلات الانترنت في الشرق الأوسط، ملف الإرهاب السياسة والإستراتيجية، مجلة الإهرام، العدد 160، أبريل 2008م
6. شلوس، نورة، القرصنة الإلكترونية في الفضاء السيبراني، التهديد المتصاعد على أمن الدول، مجلة مركز بابل للدراسات الأسبانية، 2018م، المجلد 20، العدد 2.
7. وكالة الأنباء الكويتية، وسطاء الظل يشنون هجوماً على شبكة الانترنت يثير صدمة في مختلف أنحاء العالم.

المواقع الإلكترونية:

8. http://futureaae.com/ar/futuerfile/tem/22.
9. http://www.aljazeera.net/news/scienceandtetechnology/2012/15.
10. http://www.kuna.net.ku/article.prentpage-aspxid=210082&languagar.
11. http://www.skynewsarabia.com.
12. www.alwght.con/ar/News/124178.

13. www.siyssa.org.eg/new/2017,aspx.
14. الأمن السيبراني والأمن المعلوماتي.
. http://www.linkedin.com/plus/hanen-ali@saada
15. الجزيرة نت.
http://mwdia.emaitalyoum.com/images/po;oply.inline-imeges/2012/01/ar22-1112-111.hjp92.
16. صموئيل جليس، مجرد الغارديات،
https://www.noonpost.org.content 20/ مايو 2017م.
17. عادل عبد الصادق، الفضاء الإلكتروني وتهددات جديدة للأمن القومي، 2011م، متاح على الموقع: www.accronline.com/artical-data.com 11 فبراير 2013م.
18. فاطمة الزهراء عبد الفتاح، كيف كشفت هجمات الفدية الخبيثة ثغرات الأمن السبيراني، الأحد 14 مايو 2017م،
http://futureuae.com/ar/mainpage/item/2793.
19. فاطمة الزهراء، كيف كشفت هجمات الفدية الخبيثة، ثغرات الأمن السبيراني، الأحد 14 مايو، 2017م، http://futureuae.com.
20. مفاجأة "الأمن القومي" الأمريكية وراء الهجمات الإلكترونية، نيويورك تايمز. http://www.youm7.com.stor/1/7/2018.
21. http://arbic.euronews.com/2012/06/27/a-ware-of-cyber-attack-strike-companies-in-several-countries.
22. القرصنة الإلكترونية https://www.dw.com/ar/t/119111848 2013/2/24م.
23. http://www.aljazeera.net/knowlegdedate/mewscoverage/2015/1/5%D8
24. http://arabic.euronews.com/2016/12/01.eurpt.operationavalancne-strike-at-golobal-online-crim-networt.
25. http://aitnews.com/2017/05/3.
26. http://www.skynews.arabia.com.com. السبت 13/ مايو2017م.
27. http://www.skynewsarabia.com. السبت الموافق: 13 مايو 2017م
28. https://www.masraway.com/news. 2017مايو/13.
29. http://www.skynewnewarabia.com الثلاثاء 28 يونيو 2018م.
30. www.acees.gv.bh الأربعاء 2019/5/2م، الساعة 9:30 صباحاً.
31. Aljazeera.net الأربعاء 2019/5/2م، الساعة 10:15 صباحاً.