Shadow Hackers:

تصاعد دور "الجيوش الإلكترونية" في المؤسسات العسكرية

إيهاب خليفة

منسق برنامج التطورات التكنولوجية بمركز المستقبل للأبحاث والدراسات المتقدمة، أبوظبي

وجد كثير من محترفي القرصنة والبرمجة مكاناً لهم بمرتبات عالية داخل القوات المسلحة للدول، وأصبحوا يشكلون ذراعاً أساسية للمساهمة في تحقيق أهداف الدولة، وباتوا بمنزلة "جنود ظل" يعملون خلف شاشات الكمبيوتر، ولديهم من الإمكانيات والتقنيات البرمجية والإلكترونية ما يمكنهم من لعب دور فعّال في أوقات الأزمات والحروب.

وفي هذا الإطار أدركت بعض الدول أهمية إنشاء وحدات للحروب الإلكترونية (Cyber Warfare) على شبكة الإنترنت من مئات أو آلاف القراصنة المحترفين، مثل الصين والولايات المتحدة الأمريكية، واتجهت دول أخرى مثل روسيا لكي تحذو حذوهم على الرغم من قدراتها المتقدمة في مجال حروب الفضاء الإلكتروني، وقد نجحت الوحدة 8200 الإسرائيلية بالتعاون مع وكالة الأمن القومي الأمريكي في تغيير موازين القوى الإلكترونية من خلال التطور الذي أحدثته في مجال الأسلحة الإلكترونية بإنشاء فيروس (Stuxnet)، وترددت في وسائل الإعلام العربية خاصة في أعقاب الربيع العربي الأنباء عن وجود جيوش إلكترونية، مثل الجيش الإلكتروني السوري التابع لنظام بشار الأسد، وكتائب الياسياج الإلكترونية التابعة للنظام الإيراني، وأخيراً تردد في وسائل الإعلام ما تم تسميته بجيش إلكتروني مصري مهمته الدفاع عن صورة مصر على شبكة الانترنت.

وفي هذا الإطار يمكن تفهم تحذير وزير الدفاع الأمريكي الأسبق، ليون إدوارد بانيتا، من أن الولايات المتحدة الأمريكية مهددة بحرب الفضاء الإلكتروني، وأنها مسألة وقت حتى يحدث هجوم مثل بيرل هاربر إلكترونياً، ولذلك سوف تتم الإشارة إلى ظاهرة القرصنة، وأنواع الهاكرز ومستويات خبرتهم، ثم تناول الجيوش الإلكترونية باعتبارها الأشكال الأكثر مؤسسية من الهاكرز، وأخيراً بيان بعض العمليات التي يقوم بها الهاكرز.

والقرصنة ظاهرة قديمة بدأت مع نشأة الحاسب الآلي وشبكات الكمبيوتر، ويمكن تعريفها بأنها "عملية اختراق لأجهزة الحاسوب، تتم عبر شبكة الإنترنت غالباً؛ نظراً لارتباط أغلب حواسيب العالَم عبر هذه الشبكة، أو حتى عبر شبكات داخلية يرتبط فيها أكثر من جهاز حاسوب، ويقوم بهذه العملية شخص أو عدة أشخاص متمكنين في برامج الحاسوب وطرق إدارتها؛ أي أنهم مبرمجون ذوو مستوى عال، يستطيعون بواسطة برامج مساعدة اختراق حاسوب معين والتعرف على محتوياته، ومن خلالها يتم اختراق باقي الأجهزة المرتبطة معها في نفس الشبكة"[1].

وغالباً ما يلجأ بعض الأشخاص إلى القرصنة الإلكترونية، إما بغرض الشهرة وإمكانية الحصول على وظيفة ذات دخل عال في شركات التكنولوجيا العملاقة، أو بغرض السرقة، من خلال سرقة بطاقات الائتمان أو تحويل الأموال من البنوك أو غيرها، وقد وجدت بعض الشركات،

مثل شركة ميكروسوفت وسيلة من هؤلاء الهاكرز للكشف عن الثغرات الأمنية الموجودة في أنظمة مايكروسوفت ومعالجتها في مقابل مرتبات عالية، كما وجدت بعض الحكومات فيهم وسيلة للمساهمة في تحقيق أهداف الدولة الاستراتيجية، كالحكومة الصينية والروسية والأمريكية، مثل محاولة اختراق أنظمة الفضاء الإلكتروني للدول الأخرى، وسرقة البيانات والمعلومات والخطط العسكرية والاستراتيجية، والدفاع عن الشبكات الوطنية للدولة ضد أي محاولة اختراق خارجية.

أولاً: أنواع الهاكرز:

يستخدم مصطلح الهاكر (Hacker) ليشير إلى ذلك الشخص الذي يسعى إلى معرفة كل شيء عن أنظمة الكمبيوتر، ويحاول أن يجد حلولاً ليجعلها تعمل بكفاءة أعلى أو أن تقوم بمهام ليس من المفترض أن تقوم بها[2]، على عكس الأفراد التقليديين الذي يسعون فقط إلى معرفة الضروريات التي يحتاجونها، والهاكرز بصفة عامة ثلاثة أنوع يمكن تقسيمهم على النحو التالي:

• الهاكر ذو القبعة البيضاء (White hat hacker)، ويطلق على الهاكر الصالح، وهو ذلك الشخص الذي يستخدم قدراته في مجال الكمبيوتر بصورة شرعية، لا يترتب عليها الإضرار بمصالح الغير، ويحاول أن يجد الثغرات في أنظمة الكمبيوتر بهدف تأمينها من محاولات الاختراق الخارجية.

• الهاكر ذو القبعة السوداء (Black hat hacker)، يطلق على الهاكر المفسد، ويسمى بالإنجليزية (Cracker)، للتمييز بينه وبين الهاكر الصالح، وهو الشخص الذي يستغل قدراته للإضرار بمصالح الآخرين، أو لتحقيق أهداف غير شرعية، كسرقة البنوك والبطاقات الائتمانية، واختراق مواقع الإنترنت لكسب المال.

• الهاكر ذو القبعة الرمادية (Grey hat hacker)، وهو ذلك الشخص المترنح بين الإصلاح والعبث، فهو تارة يقوم بتأمين وحماية أنظمة الكمبيوتر، وتارة أخرى يقوم باختراقها لتحقيق أهداف شخصية.

ولعل تلك التسميات جاءت من الأفلام الغربية القديمة، التي كان الأفراد الصالحون يرتدون القبعات البيضاء، والمفسدون القبعات السوداء.

ثانياً: مستويات الهاكرز

يمكن تصنيف الهاكرز إلى ثلاثة مستويات وفقاً لخبراتهم، ودرجة احترافهم في عملية الاختراق، وذلك على النحو التالي:

• الهاكرز المبتدئ (Script kiddies):

يمكن أن يُطلق عليه "مشروع هكر"، فهو الشخص الذي يستخدم الأدوات المطورة بواسطة الهاكر من أجل القيام بعملية قرصنة محدودة على أنظمة كمبيوتر، وغالباً ما تكون مهاراته ضعيفة، ويمكن مواجهة محاولات اختراقه في بدايتها.

• الهاكرز المتمرن (Intermediate Hackers):

وهم الأشخاص الذين لديهم مهارات برمجية كافية في أنظمة الكمبيوتر والشبكات، ويعلمون ما يمكن أن يقوم به كود معين لتحقيق وظيفة معينة، ولكن مثل الفئة السابقة، عادة ما يستخدمون برامج وأكواد معروفة نسبياً، ويعتمدون على الثغرات الموجودة في الأنظمة لمحاولات اختراقها.

• الهاكرز المحترف (Elite Hackers):

وهم الأشخاص المهرة والموهوبون في استخدام الكمبيوتر واستطلاع شبكات الإنترنت، ويقومون بعملية تصميم برامج القرصنة الإلكترونية، ولديهم قدرة على اختراق الأنظمة المؤمنة، ومواجهة محاولات الاختراق الخارجية من قراصنة آخرين، وليس كل القراصنة يمكن أن يصلوا إلى هذا المستوى من الحرفية، وتصنف تحت هذه الطائفة "قراصنة الظل" (Shadow Hackers)، والذين يتم استقطابهم من قبل الدول للقيام بأدوار في مجال الدفاع والهجوم في الفضاء الإلكتروني.

ثالثاً: العمليات الإلكترونية للهاكرز

ويمكن تصنيف المهام التي يمكن أن تقوم بها الجيوش الإلكترونية في ثلاثة أنواع رئيسية هي مهاجمة شبكات الخصم واستطلاعها والتجسس عليها والدفاع عن شبكات الدولة، ويتضح ذلك في التالي:

1- مهاجمة شبكات الحاسب الآلي (Computer Network Attack, CNA):

وتشمل اختراق الشبكات بحقن الحاسبات بكم هائل من البيانات لتعطيلها أو وضع بيانات ومعلومات محرفةً لإرباك مستخدمي الحاسبات، ونشر الفيروسات (Viruses) وما شابهها من البرامج الصغيرة المؤذية مثل الديدان (Worms)، وتلغيمها بالقنابل المنطقية (Logic Bombs) التي يتم تنشيطها في الوقت المناسب للمهاجم لكي تتلف ما تحتويه الحاسبات من بيانات وبرمجيات، أو القيام بهجمات إلكترونية أو مادية لقطع لخدمات الإنترنت (Denial Of Service Attacks) عن الخصم، وتدمير قواعد البيانات الإلكترونية التي يمتلكها، وتعطيل قدرته على النشر السريع لقدراته وإمكانياته وقواته، أو قطع أنظمة الاتصال بين الوحدات العسكرية وبعضها وتعطيل شبكات الكمبيوتر، أو شل أنظمة الدفاع الجوي أو التوجيه الإلكتروني للخصم، أو السيطرة على وحدات القيادة والتوجيه، أو فقدان العدو قدرته على التحكم أو الاتصال بالأقمار الصناعية[3]، وقد يصل الأمر إلى التدمير الفعلي (Physical Destruction) من خلال تدمير الجانب المادي، مثل الخادمات والأسلاك والكابلات والأجهزة التي تحتوي على معلومات يصعب التأثير عليها من بعد، وتتم عملية التدمير بالأسلحة التقليدية كالجوية والبحرية والبرية أو بعمليات القوات الخاصة.

2- الدفاع عن شبكات الحاسب الآلي (Computer Network Defense CND):

وتشمل هذه العملية حماية الشبكات وأجهزة الكمبيوتر من أي عملية اختراق خارجي، ويجب أن يكون التأمين على مستوى البرمجيات (Software) والمكون المادي للشبكات (Hardware)، بحيث يتم تأمين الشبكة من أي اختراق خارجي بأي من الأسلحة الإلكترونية السابق ذكرها، وكذلك تأمين المكون المادي للشبكات، مثل الخوادم أو الشرائح الإلكترونية، والتي قد تكون مبرمجة من قبل المصمم لكي تعمل في ظروف غير عادية لصالحه[4].

3- استطلاع شبكات الحاسب الآلي (Computer Network Exploitation):

وتعني القدرة على الدخول غير المشروع والتجسس على شبكات الخصم، من دون أن يصاحب ذلك تدمير أو تخريب للبيانات والمعلومات، بهدف الحصول على هذه المعلومات، والتي قد تشمل خطط دفاع وهجوم عسكري، أو أسراراً عسكرية وحربية، أو معلومات سياسية واستخباراتية، ولا تتوقف وظيفتها على ذلك فحسب، بل يمكن من خلالها عمل خرائط لشبكات الحاسب الآلي واستخدامها مستقبلاً في عمليات الهجوم الإلكتروني، كما يمكن ترك بعض الثغرات من خلال الأبواب الخلفية (Backdoors) لحقن الشبكة بفيروسات للقيام بمهام معينة، مثل نقل البيانات إلى أجهزة المتجسس[5]، كما يمكن أيضاً استخدامها في التأثير على أفكار وسلوكيات الخصم من خلال شن حرب نفسية، وذلك بنشر مثل هذه الخطط العسكرية والبيانات أو إرسالها إليه مرة أخرى لكي يدرك إلى أي مدى هو مُخترق ولن يستطيع المواجهة.

رابعاً: أبرز نماذج الجيوش الإلكترونية للدول

هناك اتجاه متزايد للدول لإنشاء وحدات خاصة بالحروب الإلكترونية التي تتم عبر الفضاء الإلكتروني وشبكات الحاسب الآلي، ومن أبرز هذه الوحدات الخاصة بالدول:

1- الوحدة61398 – الصين:

هي وحدة سرية خاصة بجيش التحرير الشعبي الصيني، تقوم بعمليات التجسس الإلكتروني، وسرقة المعلومات الاقتصادية، خاصة من الولايات المتحدة الأمريكية، وتتسم عملياتها بالسرية التامة، ولا يتم الإعلان عنها، وفي تقرير صادر عن شركة مانديات الخاصة بالأمن الإلكتروني، أكدت أن الوحدة 61398 بدأت في شن أولى هجماتها منذ عام 2006، وقامت بسرقة مئات التيرابيتس من البيانات الخاصة بـ 141 منظمة تشمل المخططات التكنولوجية، وعمليات التصنيع والبيانات والوثائق وخطط التسعير والتسويق، ورسائل البريد الإلكتروني وقوائم الاتصال، كما لوحظ أن ما لا يقل عن 115 شركة من هذه الشركات تقع في الولايات المتحدة الأمريكية[6].

> أدركت بعض الدول أهمية إنشاء وحدات للحروب الإلكترونية على شبكة الإنترنت من مئات أو آلاف القراصنة المحترفين، مثل الصين والولايات المتحدة الأمريكية، واتجهت دول أخرى مثل روسيا لكي تحذو حذوهم على الرغم من قدراتها المتقدمة في مجال حروب الفضاء الإلكتروني.

ويُعتقد أن الوحدة 61398 تخضع لإدارة المكتب الثاني التابع للإدارة الثالثة لهيئة أركان جيش التحرير الشعبي، وتقع في منطقة شنغهاي وتقوم شركة الاتصالات الصينية بإمدادها بنوع خاص من الألياف الضوئية لنقل بيانات الإنترنت، ويعتقد التقرير أن الوحدة تضم أو أنها هي نفسها تشكل ما أطلقت عليه مانديت اسم (APT1: Advanced Persistent Threat) أي التهديد المستمر المتقدم، الذي قام بالهجوم على عدد كبير من المؤسسات الصناعية والحكومية حول العالم منذ عام 2006 على الأقل.

وتعتمد الوحدة 61398 على شبكة من القراصنة الإلكترونيين الصينيين في 13 دولة، يقع معظمهم في الولايات المتحدة التي يقع فيها أكثر من 100 جهاز كمبيوتر مخصص لغرض العمليات الإلكترونية، وفي 18 فبراير 2013، أصدرت المخابرات المركزية الأمريكية تقريراً من 60 صفحة يتهم الوحدة 61398 بالوقوف وراء عمليات تجسس وتخريب تمت من خلال شبكة الإنترنت[7]، وفي 19 مايو 2014، ولأول مرة في التاريخ، وجّه المدعي العام الأمريكي إريك هولدر– باسم مكتب التحقيقات الفدرالي– تهماً جنائية بسرقة معلومات تجارية حساسة من خمس شركات أمريكية كبرى (أبرزها يو إس ستيل، ألكوا، وستنجهاوس للإلكترونيات، سولار ورلد)، إلى خمسة ضباط في الوحدة 61398 التابعة للجيش الصيني، وطلب من الحكومة الصينية تسليمهم للولايات المتحدة[8] ودائماً ما تواجه الصين الاتهامات الموجهة إليها بالقيام بهجمات إلكترونية أو سرقة معلومات سرية بالنفي، والادعاء بأنها أيضاً ضحية لعمليات قرصنة إلكترونية.

2- قيادة الفضاء الإلكتروني (Cyber Command)– الولايات المتحدة:

استحداث البنتاجون في يونيو 2009 قيادة عسكرية مهمتها الرد على هجمات قراصنة المعلومات وتنفيذ عمليات في الفضاء الإلكتروني[9]. وقد تم تعيين أول جنرال عسكري لإدارة حروب الفضاء الإلكتروني هو الجنرال الكسندر كيث، وتستهدف وزارة الدفاع الأمريكية من تلك القيادة الجديدة أن تشرف على مختلف الجهود المتعلقة بالإنترنت في كل أجهزة القوات المسلحة، سواء من حيث تأمينها أو القيام بعمليات إلكترونية عسكرية ضد أهداف خارجية، وفي كلمه له أكد وزير الدفاع الأمريكي تشاك هيجل أنه من المتوقع أن يصل عدد قوات القيادة العسكرية للفضاء الإلكتروني إلى 6000 مقاتل بحلول عام 2016[10].

وقبل استحداث هذه القيادة كانت الحكومة الأمريكية تعتمد على وكالة المخابرات المركزية (CIA) ووكالة الأمن القومي الأمريكي (NSA) للقيام بعملياتها في الفضاء الإلكتروني، بل أن معظم مشاريع التجسس الإلكتروني الكبرى للولايات المتحدة مثل بريزم (PRISM) وغيره نفذتها وكالة الأمن القومي.

وتتمثل المهمة الرئيسية لهذه القيادة في حماية شبكات وزارة الدفاع وأنظمتها، والاستعداد لخوض حروب الفضاء الإلكتروني، والدفاع عن شبكات الدولة الأمريكية، من خلال إدارة عمليات شبكات المعلومات التابعة لوزارة الدفاع الأمريكي، لتحقيق هدفين رئيسيين هما، حماية حرية عمل الولايات المتحدة وحرية عمل حلفائها في الفضاء الإلكتروني، وحرمان أعداء الولايات المتحدة – عند الحاجة – من حرية العمل في الفضاء الإلكتروني.

وقد أوضح الكسندر كيث في مقال نشره استراتيجية عمل هذه القيادة الجديدة، والتي تتركز في[11]:

- التعامل مع الفضاء الإلكتروني كمجال يمكن أن تستفيد منه وزارة الدفاع الأمريكية للقيام بعمليات عسكرية واستخباراتية وتجارية.
- تبني مفاهيم جديدة للعمل الدفاعي، مثل مفهوم "الدفاع الإلكتروني النشط"، والذي يهدف لمراقبة حركات الإنترنت في الفضاء

الإلكتروني من أجل حماية شبكات وزارة الدفاع وأنظمتها.

• قيام الوزارات والوكالات الحكومية الأمريكية بالتعاون مع القطاع الخاص من أجل وضع استراتيجية تشمل الحكومة وأجهزتها كافة، للتوصل لاستراتيجية وطنية شاملة لأمن الفضاء الإلكتروني.

• الاستفادة من مؤهلات المواطنين ذوي الخبرات العالية، وذلك عن طريق توظيف قوى عاملة إلكترونية ماهرة والحفاظ عليها وتشجيع الابتكار التقني السريع.

3- قراصنة الظل التابعون للحكومة الروسية:

صرح المتحدث باسم وزارة الدفاع الروسية "إيجور يجوروف" في أكتوبر 2014 أن روسيا تخطط لبناء نظام إلكتروني شامل على مراحل يتم الانتهاء منها عام 2017 لحماية البنية الأساسية للقوات المسلحة من الهجمات الإلكترونية، كما أمر وزير الدفاع "سيرجي شويجو" في صيف 2014 بإدراج 500 من الطلبة المتميزين في استخدام الحاسب الآلي في "وحدات علمية" خاصة، وسيعتبر عملهم مثل الخدمة العسكرية[12].

ولكن هذا لا يعني أن روسيا لا تمتلك عناصر بشرية مؤهلة للقيام بالعمليات الإلكترونية، حيث إنها تعتمد على عدد كبير من القراصنة، سواء المتطوعون أو الذين يتم توظيفهم لخدمة أغراض عسكرية، حيث قامت روسيا في 2007 بشن حرب إلكترونية شاملة على إستونيا بسبب نقل تمثال يخلد تضحيات جنود روس في الحرب العالمية الثانية[13]، ونتج عنها شل قطاعات البنوك والوزارات وشبكات الاتصالات من خلال هجمات اختراقية سريعة ومدروسة أدت إلى دمار لوجستي كبير، ولم يعد المواطنون قادرون على إجراء معاملاتهم البنكية الإلكترونية التي تتم 97% منها عبر الإنترنت[14] أو التواصل مع بعضهم بالبريد الإلكتروني لأيام عديدة، وتم تعطيل البنية التحتية للاقتصاد الرقمي الإستوني[15]، وهو ما تكرر أيضاً في أعقاب الحرب الروسية الجورجية عام 2008، حيث شنت روسيا هجمات إلكترونية لتعطيل شبكة البنية التحتية الجورجية.

4- الوحدة 8200 – إسرائيل

وقد تم إنشاؤها عام 1952، وتولت في مرحلة لاحقة من إنشائها مهام قيادة الحرب الإلكترونية في الجيش الإسرائيلي، وتتمتع بعلاقات تعاون وثيقة مع وكالة الأمن القومي الأمريكي (NSA) وقيادة الفضاء الإلكتروني (US Cyber Command)، وتمتلك أهم وأكبر قاعدة تجسس إلكترونية إسرائيلية بالنقب للتنصت على البث الإذاعي والمكالمات الهاتفية والفاكس والبريد الإلكتروني في قارات آسيا وأفريقيا وأوروبا.

وقد لعبت هذه الوحدة دوراً رئيسياً في ضرب البرنامج النووي الإيراني من خلال تصميم فيروس ستاكسنت (Stuxnet) الذي أصاب 1000 من أجهزة الطرد المركزي الإيراني، وتسبب في تعطيل البرنامج النووي، وقد أكد المعلق العسكري الإسرائيلي عمير رايبوبورت أن الدور الذي تقوم به "وحدة 8200"، التابعة لشعبة الاستخبارات العسكرية الإسرائيلية (أمان)، قد جعل إسرائيل ثاني أكبر دولة في مجال التنصت في العالم، بعد الولايات المتحدة، وأشار رايبوبورت إلى أن الحواسيب المتطورة التابعة لوحدة 8200 قادرة على رصد الرسائل ذات القيمة الاستخباراتية من خلال معالجة ملايين الاتصالات ومليارات الكلمات[16].

وفي الختام يمكن القول إن الدول سوف تستمر في استقطاب قراصنة الظل، وتنمية مهاراتهم، لكي تصبح مهمتهم تحقيق الأهداف الرئيسية للدولة، سواء من خلال الدفاع أو الهجوم الإلكتروني، كما أنهم أصبحوا محل اهتمام شركات التكنولوجيا العملاقة، خاصة المتسربين منهم من القوات المسلحة، بما يمتلكون من مهارات متقدمة وخبرات عالية.

1- القرصنة الإلكترونية، **تقرير منشور على موقع الحوار نت**، تاريخ الدخول 11 نوفمبر 2014، يمكن المطالعة على http://goo.gl/8c0fwU

2- David melnichuk, **The Hacker's Underground Handbook**, p6 On http://goo.gl/6BOqQ7 on November 18, 2018

3- Colonel Jayson M. Spade, China's Cyber Power And America's National Security, Jeffrey L. Caton Editor, (U.S. Army War College, May2012) p 7

4- Ibid, 9

5- Dennis M. Murphy, ed., **Information Operations Primer**, (Carlisle, Pennsylvania: U.S. Army War College, 2010), p 169

6- APT1, Exposing One of China's Cyber Espionage Units، **Mandiat Report,** 2013، http://goo.gl/8BdszN

7- Chinese Army Unit Is Seen as Tied to Hacking Against U.S, **New York times,** Accessed Nov 15, 2014 http://goo.gl/juYV7X

8- 5 in China Army Face U.S. Charges of Cyberattacks, **New York times**, Accessed Nov 15, 2014 http://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html?hp

9- عادل عبد الصادق، أمريكا وتشكيل قيادة عسكرية في الفضاء الالكتروني ..هل بدأ الاستعداد لحروب المستقبل ؟، **مجلة تعليقات مصرية**، عدد 130، (مركز الأهرام للدراسات السياسية والاستراتيجية، يوليو 2009)، يمكن المطالعة على http://goo.gl/QEFQBW

10- U.S. cyberwarfare force to grow significantly, defense secretary says, **Washington Post**, Accessed Nov 15, 2014 http://goo.gl/uIqR7N

11- Gen Keith B. Alexander, Building a New Command in Cyberspace, **Strategic Studies Quarterly**, Vol. 5, No 2, summer 2011, p. 8.

12- روسيا تنشئ وحدات إلكترونية في قوات الصواريخ الاستراتيجية، خبر منشور على **وكالة أنباء شينخوا الصينية**، بتاريخ مطالعة 11 نوفمبر 2014. http://goo.gl/gD3373

13- عادل عبدالصادق، الإرهاب الإلكتروني القوة في العلاقات الدولية: نمط جديد وتحديات مختلفة، **مركز الأهرام للدراسات السياسية والاستراتيجية**، القاهرة، 2009، ص 216

14- Rebecca Grant, Victory in cyber space, **The Air Force Association**, October 2007,p 7, http://goo.gl/UmnT6O

15- عباس بدران، الحرب الإلكترونية .. الاشتباك في عالم المعلومات، **مركز دراسات الحكومة الإلكترونية**، لبنان، 2010، ص 5.

16- صالح النعامي، "وحدة 8200".. ذراع التنصت الإلكتروني بإسرائيل، **موقع الجزيرة نت**، تاريخ مطالعة 11 نوفمبر 2014