Cyber Defence

تنامي التهديدات السيبرانية للمؤسسات العسكرية

إيهاب خليفة

رئيس وحدة التطورات التكنولوجية، المستقبل للأبحاث والدراسات المتقدمة، أبوظبي

في ضوء التطور التكنولوجي المتسارع، وتنامي دور الفاعلين من نشطاء وجيوش إلكترونية وفواعل من دون الدول في المجال السيبراني، زادت التهديدات الإلكترونية، بصورة شملت، ليس فقط المواقع والخدمات الإلكترونية المدنية، ولكن أيضاً البيانات والمنشآت العسكرية، بالإضافة إلى البنية التحتية الحرجة كالمفاعلات النووية، وهو تطور يفرض تحديات على الأمن القومي للدول.

ويسعى هذا التحليل لإلقاء الضوء على مفهوم الدفاع الإلكتروني من واقع الاستراتيجيات العسكرية المختلفة، وآليات تحقيقه، بالإضافة إلى الوقوف على أهم أهداف الدفاع الإلكتروني والمؤسسات المسؤولة عن تحقيقه في هذا المجال، وتحديد أبرز التطورات التكنولوجية التي أحدثت تقارباً بين المجالات المدنية والعسكرية، وما فرضه ذلك من تحديات أمنية تسعى الدول لمواجهتها.

أولاً: الدفاع الإلكتروني في الاستراتيجيات العسكرية

يقصد بالدفاع الإلكتروني "مجموعة القدرات النظامية التي تمتلكها القوات المسلحة للحماية من تأثيرات الهجمات الإلكترونية، والتخفيف من حدتها والتعافي منها بسرعة"[1]. وقد عرّفت العقيدة الفرنسية الدفاع الإلكتروني على أنه: "مجموعة الوسائل الفنية وغير الفنية التي تسمح للدولة بالدفاع عن نظم المعلومات الحرجة في الفضاء الإلكتروني"[2]، وفي الاستراتيجية النمساوية، فإن مصطلح الدفاع الإلكتروني يشير إلى "جميع التدابير اللازمة للدفاع عن الفضاء الإلكتروني بالوسائل المناسبة لتحقيق الأهداف العسكرية الاستراتيجية"[3]، ويعرفه البرلمان الأوروبي بأنه "عملية تطبيق الإجراءات الأمنية من أجل الحماية من الهجمات الإلكترونية، والتعامل معها. وتستهدف تأمين البنية التحتية لنظم الاتصالات والقيادة والسيطرة"[4].

وفي الاستراتيجية العسكرية البلجيكية، فإن الدفاع الإلكتروني هو "تطبيق تدابير وقائية فعّالة للحصول على مستوى مناسب من الأمن الإلكتروني، وتقليل المخاطر الأمنية إلى مستوى مقبول"[5]. وباستثناء التعريف الأخير، فإن جميع التعريفات السابقة تطرقت إلى الدفاع الإلكتروني بمفهومه السلبي، والذي يعني القدرة على استقبال الهجمة الإلكترونية، وتلافي آثارها سريعاً من دون الإضرار بالبنية التحتية والأهداف الاستراتيجية للدولة، أما التعريف البلجيكي فقد أضاف بعداً جديداً وهو الدفاع الإلكتروني الوقائي أو الإيجابي، والذي يعني منع الهجمة قبل حدوثها، سواء من خلال اتخاذ تدابير وقائية أو هجمات إلكترونية استباقية.

ومن مجمل التعريفات السابقة، يمكن تعريف الدفاع الإلكتروني الوقائي بأنه: "وسيلة لتحقيق الأمن الإلكتروني من خلال استخدام

آليات رصد الهجمات الإلكترونية وتحليلها وتحديد مصدرها والتخفيف من حدة آثارها على نظم الاتصالات والشبكات والبنية التحتية، وذلك في وقتها الحقيقي، مع توافر القدرات الهجومية لتعقب الكيانات وتدمير الشبكات، التي انطلق منها هذا التهديد"[6].

ويختلف الدفاع الوقائي عن نظيره التقليدي في عنصرين رئيسيين، هما الاكتشاف المبكر للهجمات الإلكترونية، والآنية في التعامل معها حال حدوثها، فبينما يعمل الدفاع التقليدي كدرع داخلية للتخفيف من حدة الهجمات والتعافي السريع منها، يعمل الدفاع الوقائي كرمح استباقي لإعاقة الخصم عن تنفيذ الهجمة الإلكترونية. ويتحقق الدفاع الإلكتروني الوقائي من خلال ثلاثة أساليب رئيسية:

1- الكشف المبكر عن الهجمات في وقتها الحقيقي: وهو ما يتم من خلال استخدام حساسات (Sensors) على الشبكات والبرامج والتطبيقات، بالإضافة إلى توظيف المعلومات الاستخباراتية لرصد أي نشاط غير طبيعي قد يُصنف على أنه هجمة إلكترونية، وبداية مواجهتها واحتوائها قبل أن تبدأ نشاطها في الشبكة أو النظم المستهدفة.

2- الهجوم الإلكتروني الاستباقي: وذلك من خلال استخدام ونشر الديدان البيضاء (White Worms)، وهي برامج قادرة على اكتشاف التطبيقات الضارة وتدميرها قبل توظيفها في إطلاق هجمة إلكترونية محتملة، كما تقوم أيضاً بتدمير أدوات وبرمجيات القراصنة، وهو ما يساعد في إحباط مخطط الهجمة نفسها[7]، وتحديد هوية ومصدر الهجمة، بما يمكن من إطلاق هجمة إلكترونية مضادة فيما يعرف بالاختراق العكسي (Hack-back).

3- التضليل والإخفاء والخداع: وهو ما يتحقق عن طريق إخفاء هويات الأهداف الاستراتيجية للدولة على الإنترنت، وتضليل الخصم أثناء محاولة الوصول إليها أو اختراقها، من خلال أدوات التمويه والخداع وتغيير ملامح الأهداف الاستراتيجية للدولة، بما يساعد على تضليل الخصم وتشتيت الانتباه عن الهدف الرئيسي.

ثانياً: أهداف الدفاع في الفضاء السيبراني

تتمحور أهداف الدفاع الإلكتروني في الحفاظ على مقدرات الأمن القومي التكنولوجي للدولة، من خطوط اتصالات وشبكات كمبيوتر وبنية تحتية، سواء مدنية أو عسكرية، فضلاً عن تأمين البيانات الحيوية، بما يساهم في النهاية في تحقيق الأمن الإلكتروني للدولة ويمكن تحديد أهداف الدفاع الإلكتروني في التالي:

1- حماية الأهداف العسكرية: والتي تشمل تأمين نظم الإدارة والمراقبة ونظم التحكم والسيطرة ونظم توجيه الأسلحة وقطاع الاتصالات الحربية والأسلحة آلية القيادة، مثل الطائرات من دون طيار، فضلاً عن حماية المنشآت العسكرية والحيوية، مثل محطات الطاقة النووية من أي اختراق إلكتروني.

2- حماية البيانات العسكرية: والتي تشمل معلومات حول أفراد القوات المسلحة كالأسماء والرتب والمرتبات والوظائف داخل الجيش وأماكن الإقامة الشخصية، فضلاً عن خطط التسليح وتصميمات الأسلحة، وخرائط انتشار القوات وتوزيع الأسلحة.

3- حماية البنية التحتية الحرجة: مثل قطاع الاتصالات والمواصلات ومحطات الطاقة وقواعد البيانات الحكومية وخدمات الحكومات الذكية والبنوك والمؤسسات المالية.

4- دعم وحدات الحرب الإلكترونية: وهي تلك الوحدات الخاصة بإدارة الحروب السيبرانية للدولة، حيث تكون مهمة الدفاع الإلكتروني هي تأمين الخطوط خلف هذه الوحدات، بما يحمي أهداف الدولة الاستراتيجية في حالة شن هجوم إلكتروني مضاد عليها، وتوفير غطاء إلكتروني للوحدات المقاتلة بهدف التمويه والخداع وصعوبة تعقب مصدر الهجمة.

5- تحقيق الردع الإلكتروني: وذلك من خلال رفع تكلفة الهجوم الإلكتروني للدولة المعتدية، عبر إنشاء نظم دفاع إلكترونية صعبة الاختراق تحتاج إلى وقت وجهد كبيرين لاختراقها، مع تطوير قدرات تتبع الهجمات الإلكترونية واكتشاف مصدرها بما يؤدي في النهاية إلى التأثير على قرارات الخصم وردعه عن شن هجمات إلكترونية على الدولة في النهاية.

ثالثاً: مؤسسات الدفاع الإلكتروني

أجرى مكتب الأمم المتحدة لشؤون نزع السلاح دراسة مسحية في عام 2012 على الدول الأعضاء في الأمم المتحدة البالغ عددها حوالي 193 دولة، فوجد أن من بينها 114 دولة لديها برامج وطنية للأمن الإلكتروني، وأن 74 دولة منها أولت مهمة تحقيقه للقوات المسلحة، بينما قامت 67 دولة بإناطة مهمة الأمن الإلكتروني لمؤسسات مدنية لديها[8]. وبصورة عامة، فإن مهمة تحقيق الدفاع الإلكتروني تقع على عاتق عدد من المؤسسات، وذلك على النحو التالي:

1- الجيوش الإلكترونية: حيث اتجه كثير من الدول حول العالم لإنشاء جيوش إلكترونية وفرق للعمليات عبر الفضاء الإلكتروني داخل صفوف قواتها المسلحة، تتكون من قراصنة معلومات مهمتهم اختراق شبكات الكمبيوتر الخاصة بالخصم، ونشر برامج التجسس والمراقبة، وتنفيذ المهمات العسكرية التي تطلب منها كتعطيل أحد البرامج العسكرية للخصم أو السيطرة على أحد الشبكات أو تدمير بعض الخدمات الإلكترونية، فضلاً عن الدفاع عن الشبكات القومية وحمايتها من أي محاولة اختراق.

2- فرق الاستجابة الفورية للطوارئ (Computer Emergency Response Team): وتعرف اختصاراً باسم (CERT) وهي فرق مدنية، تكون مهمتها التحقيق في الأدلة الجنائية الرقمية، ومحاولة تتبع مصدر الهجمات والمتورطين فيها[9]، وعادة ما يوجد بالدولة أكثر من فريق استجابة للطوارئ، يتبع بعضها الوزارات، مثل وزارة الاتصالات، ويتبع البعض الآخر الشركات الكبرى، سواء كانت حكومية أو غير حكومية كشركات النفط والطاقة والاتصالات.

3- كبريات شركات الاتصالات: هي أيضاً أحد خطوط الدفاع

الإلكتروني للدولة، وذلك بسبب امتلاكها قواعد بيانات خاصة بعدد كبير من المستخدمين داخل الدولة، كما تقع عليها مسؤولية تأمين جميع اتصالات الأفراد بالدولة، وضمان الحفاظ على سريتها وخصوصيتها من دون أن تتعرض للاختراق أو التسريب.

4- القوات المسلحة التقليدية: قد تشارك بعض فرق القوات المسلحة التقليدية أيضاً في عمليات الدفاع الإلكتروني، حيث تستدعى بعض العمليات الإلكترونية التدخل العسكري التقليدي من قبل القوات المسلحة، لتدمير خطوط اتصالات أو مراكز إدارة عمليات قرصنة تابع للخصم أو تدمير أسلحة خرجت عن السيطرة بسبب اختراقها.

رابعاً: قواسم مشتركة بين العسكري والمدني

بمرور الوقت حدث تقارب بين شبكة الإنترنت المفتوحة والشبكة العسكرية المغلقة، حيث أصبح بالإمكان الحصول على معلومات عسكرية من شبكة الإنترنت المفتوحة، بالإضافة إلى ظهور مجال مشترك بين الشبكة العسكرية والشبكة المفتوحة بفضل التطورات التكنولوجية، وهو ما زاد من التهديدات النابعة من الفضاء الإلكتروني، ويمكن توضيح ذلك في التالي:

1- استخدام بعض خدمات الإنترنت المدنية في الأغراض العسكرية: حيث قامت بعض الدول، مثل الولايات المتحدة الأمريكية وغيرها، بالاعتماد على تقنيات "الحوسبة السحابية" (Cloud Computing) لتسهيل عملية إدارة جنودها وقواعدها العسكرية في مناطق متفرقة حول العالم، وذلك بالتعاون مع شركة "آي بي إم" (IBM) وشركة أمازون، نظراً لما توفره هذه الخدمة من وقت وجهد وتكلفة في تقديم الخدمات والمعلومات التي تتطلبها الإدارة اللامركزية لقواتها في أماكن متفرقة حول العالم، مع الاحتفاظ بدرجة عالية من تأمين البيانات، ولم يقتصر استخدام الخدمات السحابية على جمع وتحليل وإتاحة المعلومات للجنود في الغرف المغلقة وحسب، بل أيضاً تمت إتاحته للمقاتلين العسكريين في ميدان المعركة، حيث يتم جمع المعلومات المحيطة بمكان وظروف المعركة وتحليل المعلومات العملاقة (Big Data) بصورة تساعد في تقديم أفضل سيناريو للمعركة إلى المقاتلين في الوقت الحقيقي[10].

2- الحصول على معلومات عسكرية باستخدام خدمات الإنترنت المدنية: فمثلاً يمكن الحصول على صور لمواقع عسكرية من خلال "خرائط جوجل" و"خدمات جوجل إيرث" (Google Earth)، والتي تتيح للمدنيين الحصول على صور فورية للقواعد العسكرية بكل سهولة ويسر، كما يقوم بعض الجنود بوضع بياناتهم الشخصية على صفحات الإنترنت ومواقع التواصل الاجتماعي، وهي التي من خلال تحليلها يمكن الوصول إلى معلومات عسكرية مهمة، مثل رتب الجنود وأماكن إقامتهم وشبكة علاقاتهم الشخصية وزملائهم من أفراد القوات المسلحة.

3- دمج تقنيات عسكرية في بعض الأجهزة المدنية: ومن الأمثلة على ذلك نظم تحديد المواقع الجغرافي (GPS)، حيث كانت قاصرة في بدايتها على الاستخدامات العسكرية فقط، لكن بمرور الوقت، ومع الحاجة إليها في الاستخدامات المدنية، أصبح كل شخص معه هاتف ذكي تتوافر فيه هذه الخاصية، بصورة تقترب كثيراً من تلك المستخدمة في العمليات العسكرية، مما يعني قدرة الحركات المتطرفة على استخدام بعض التقنيات المدنية، مثل الدرونز التجارية وتحميلها بمواد متفجرة وتوجيهها عبر نظام (GPS) لاستهداف شخصيات عامة أو قواعد عسكرية.

4- الاعتماد على القطاع الخاص في القيام ببعض المهام العسكرية: حيث تلجأ وكالة الأمن القومي الأمريكي وبعض المؤسسات العسكرية في دول مختلفة إلى التعاقد مع مقاولين من الخارج والتعامل مع كثير من الشركات الخاصة للقيام ببعض المهام، مثل توريد أجهزة أو تأسيس شبكات أو بناء نظم أمنية ونظم اتصالات أو غيرها من الأعمال، وقد يؤدي ذلك إلى حدوث بعض الثغرات الأمنية داخل المؤسسات العسكرية.

> تلجأ وكالة الأمن القومي الأمريكي وبعض المؤسسات العسكرية في دول مختلفة إلى التعاقد مع مقاولين من الخارج والتعامل مع كثير من الشركات الخاصة للقيام ببعض المهام، مثل توريد أجهزة أو تأسيس شبكات أو بناء نظم أمنية ونظم اتصالات أو غيرها من الأعمال، وقد يؤدي ذلك إلى حدوث بعض الثغرات الأمنية داخل المؤسسات العسكرية.

ولذلك أصبح هناك مجال مشترك على الإنترنت يجمع بين الاستخدام المدني والعسكري، وقد شكل هذا المجال نقطة ضعف داخل صفوف القوات المسلحة، تزامنت مع نقطة ضعف أخرى، هي تطور تقنيات الهجوم الإلكتروني على الشبكات العسكرية المغلقة، فتزايدت التهديدات الإلكترونية للقوات المسلحة، وأصبح من الضروري الاهتمام بالدفاع الإلكتروني كأحد أبعاد الدفاع بصورة عامة.

خامساً: التحديات الأمنية الرئيسية

نتيجة لاقتراب الخطوط الفاصلة بين شبكة الإنترنت العادية والشبكات العسكرية من ناحية، مع تطوير القدرات الهجومية في مجال الحروب الإلكترونية، يتعرض الدفاع الإلكتروني لعدد من التحديات الرئيسية، والتي يمكن تحديدها في التالي:

1- استهداف البنية التحتية الحرجة للدولة: إذ يتم استهداف البنية التحتية للدولة، سواء كانت مدنية أو عسكرية بهجمات إلكترونية، مثل استهداف محطات الطاقة والوقود والخدمات المالية والمصرفية ونظم الاتصالات والمواصلات. ومن أبرز الأمثلة على ذلك تعرض أوكرانيا خلال شهر يونيو 2017 لهجمة إلكترونية شملت محطات الطاقة، بالإضافة إلى المؤسسات المالية، وأحد أكبر مطاراتها[11].

وقد شهدت السنوات القليلة الماضية العديد من الهجمات الإلكترونية على بعض البنى التحتية الحرجة والمؤسسات العسكرية، مثل محطات الطاقة النووية، كما في قيام فيروس

ستاكسنت بتعطيل حوالي ألف من أجهزة الطرد المركزي في منشأة لتخصيب اليورانيوم في ناتانز في وسط إيران في عام 2010[12]، فضلاً عن تعرض أنظمة الكمبيوتر لشركة كوريا الجنوبية للطاقة المائية والنووية التي تديرها الدولة لهجمات إلكترونية في ديسمبر 2014[13]، واتهمت الولايات المتحدة روسيا بالتورط في شن هجمات إلكترونية على شبكات كمبيوتر في عدة محطات طاقة نووية[14].

2- السيطرة على الأنظمة العسكرية: ويقصد بها قيام قراصنة محترفين أو جيوش نظامية إلكترونية بشن هجمات إلكترونية بغرض السيطرة على نظم القيادة والسيطرة عن بعد، الأمر الذي يؤدي إلى إخراج بعض منظومات الأسلحة عن سيطرة القيادة المركزية، وإعادة توجيهها نحو أهداف داخلية أو ضد دول صديقة، كما يمكن أيضاً السيطرة على الطائرات من دون طيار، أو الغواصات النووية في أعماق البحار، أو السيطرة على الأقمار الصناعية العسكرية في الفضاء الخارجي وإخراجها عن سيطرة الدولة التابعة لها هذه الأسلحة والمعدات. وتزداد خطورة مثل هذه الهجمات، في ضوء التطور التكنولوجي، واعتماد اللوجستيات ونظم القيادة والتحكم وتحديد الأهداف وإصابتها على برامج كمبيوتر وشبكات الاتصالات.

3- سرقة المعلومات والبيانات العسكرية أو التلاعب بها: من خلال اختراق قواعد البيانات العسكرية وسرقتها أو تزييفها أو تدميرها إلكترونياً، حيث تسعى الهجمات الإلكترونية في هذه الحالة إلى اختراق الشبكات الخاصة بالمؤسسات العسكرية بهدف سرقة خرائط نشر أنظمة التسليح أو التصميمات الخاصة بالمعدات العسكرية، وقد انطلقت واحدة من أخطر الهجمات ضد أنظمة حواسب الجيش الأمريكي في عام 2008، من خلال وصلة "يو إس بي" (USB) متصلة بكمبيوتر محمول تابع للجيش في قاعدة عسكرية موجودة في الشرق الأوسط، ولم يتم اكتشاف انتشار برامج التجسس في كل من الأنظمة السرية وغير السرية في الوقت المناسب، مما شكل ما يشبه جسراً رقمياً، تم من خلاله نقل آلاف الملفات من البيانات إلى خوادم خارجية (Servers). وبالمثل تم استهداف أكثر من 72 شركة من بينها 22 مكتباً حكومياً و13 من مقاولي قوات الدفاع بهدف سرقة معلومات حول الخطط والمباني العسكرية[15].

4- جمع معلومات اقتصادية استخباراتية: وهو ما يتحقق عن طريق اختراق قواعد البيانات المالية والمصرفية وقواعد بيانات الشركات والبنوك وجمع المعلومات التي قد تؤثر على الأمن القومي للدولة، وكذلك من خلال التجسس على المسؤولين الماليين ووزراء المالية ورؤساء الشركات الكبرى، حيث أصدر الرئيس الأمريكي باراك أوباما أثناء فترته الثانية أوامره بوقف التنصت على مقري صندوق النقد الدولي والبنك الدولي، وذلك في إطار مراجعة أنشطة جمع المعلومات الاستخباراتية، وذلك في أعقاب التسريبات، التي كشف عنها المتعاقد السابق مع وكالة الأمن القومي إدوارد سنودن بشأن برامج لجمع كميات هائلة من البيانات عن حلفاء وأعداء الولايات المتحدة والمواطنين الأمريكيين[16].

وفي الختام، يمكن القول إنه في ضوء تنامي التوتر والصراعات في العلاقات بين الدول، على المستويين الإقليمي أو الدولي، فإنه يتوقع أن تلجأ الدول إلى توظيف الحروب الإلكترونية كأدوات إضافية في إدارة صراعها مع خصومها، خاصة مع تنامي أدوار الفواعل المسلحة من دون الدول، وهو ما يؤشر إلى زيادة التهديدات النابعة من الفضاء السيبراني مستقبلاً، مما يتطلب من الدول كافة اتخاذ إجراءات لضبط سلوكها في الفضاء الإلكتروني، فضلاً عن تطوير قدرات دفاعية لتأمين نفسها في مواجهة تلك التهديدات.

1- Habes B. Godwin III (et al.) (eds.), Critical Terminology Foundations 2: Russia – US Bilateral on Cybersecurity, **East-West Institute**, Policy Report no. 2, 2014, accessible at: https://dl.dropboxusercontent.com/u/164629289/terminology2.pdf

2- France's Strategy 2011, Information Systems and Defence, **Agence nationale de la sécurité des systèmes d'information (ANSSI),** accessible at: https://goo.gl/MXfmXx (Last accessed: July 26, 2017).

3- Austrian Cyber Security Strategy 2013, **Federal Chancellery of the Republic of Austria**, 2013, accessible at: https://www.bka.gv.at/DocView.axd?CobId=50999 (Last accessed: July 26, 2017).

4- Carmen- Cristina, Cyber defence in the EU Preparing for cyber warfare?, **European Parliamentary Research Service**, October 2014, accessible at: https://goo.gl/ceKME2 (Last accessed: July 27, 2017).

5- Cyber Definitions, **NATO Cooperative Cyber Defence Centre of Excellence**, accessible at: https://ccdcoe.org/cyber-definitions.html (Last accessed: July 28, 2017).

6- Robert S. Dewar, The "Triptych of Cyber Security": A Classification of Active Cyber Defence, NATO Cooperative Cyber Defence Centre of Excellence, 2014, (p. 10), accessible at: https://ccdcoe.org/cycon/2014/proceedings/d1r1s9_dewar.pdf (Last accessed: July 29, 2017).

7- Ibid., p. 10.

8- Carmen- Cristina, Cyber defence in the EU Preparing for cyber warfare?, **European Parliamentary Research Service,** October 2014, accessible at: https://goo.gl/bMPDWK (Last accessed: July 27, 2017).

9- Margaret Rouse, CERT (Computer Emergency Readiness Team), **TechTarget**, accessible at: https://goo.gl/bsTV8f (Last accessed: 10 August 2017).

10- Rick Delgado, How the U.S. Military Is Using the Cloud, **DZone**, May 19, 2015, accessible at: https://dzone.com/articles/how-us-military-using-cloud (Last accessed: July25, 2017)

11- Lizzie Dearden, Ukraine cyber-attack: Chaos as national bank, state power provider and airport hit by hackers, Independent, June 27, 2017, accessible at: https://goo.gl/NGVkND (Last accessed: August 1, 2017).

12- Iran says Stuxnet virus infected 16,000 computers, **Fox news**, February 18, 2012, accessible at: https://goo.gl/6vU2My (Last accessed: April 17, 2014).

13- طوارئ بكوريا الجنوبية لحماية محطاتها النووية، **سكاي نيوز عربية**، 26 ديسمبر 2014، موجود على الرابط التالي: https://goo.gl/7Z9s9X (تاريخ الدخول: 1 أغسطس 2017).

14- Russia is the Chief Suspect In U.S. Nuclear Power Plants Hack, **NEWSWEEK**, July 7, 2017, accessible at: http://www.newsweek.com/russia-russian-hackers-nuclear-power-633160 (Last accessed: August 1, 2017).

15- د. اولاف تايلر، **التهديدات الجديدة: الأبعاد الإلكترونية، موقع مجلة حلف الناتو**، موجود على الرابط التالي: https://goo.gl/ZLkBQ5 (تاريخ الدخول: 16 أبريل 2014).

16- أوباما أمر بوقف تجسس وكالة الأمن القومي على مقري صندوق النقد الدولي والبنك الدولي، **رويترز**، 1 نوفمبر 2013، موجود على الرابط التالي: http://ara.reuters.com/article/worldNews/idARACAE9B2C3S20131101 (تاريخ الدخول: 1 أغسطس 2017).