هجمات حرجة:
الاستهداف السيبراني للأقمار الصناعية والمنشآت النووية

د. إيهاب خليفة
رئيس وحدة التطورات التكنولوجية، المستقبل للأبحاث والدراسات المتقدمة، أبوظبي

بدأت الهجمات السيبرانية تأخذ منحنى أكثر خطورة خلال السنوات القليلة الماضية، خاصة مع تنامي التوجه لدى بعض الدول للقيام باختراقات محدودة للمنشآت النووية والأقمار الصناعية التابعة للدول المناوئة لها، وهو ما ينذر بتزايد قدرة الهجمات السيبرانية على الإضرار بالمفاعلات النووية، والخدمات المدنية والعسكرية التي تقدمها الأقمار الصناعية.

مثّل استهداف الولايات المتحدة أجهزة الطرد المركزي في محطة تخصيب ناتانز النووية في إيران عبر فيروس ستاكس نت في عام 2009 أول اختراق مسجل لمحطة نووية. وفي أعقاب هذا الحدث، تصاعدت الوتيرة تدريجياً، وظهرت حالات متعددة لشن هجمات سيبرانية على منشآت نووية حول العالم، أو استهداف نظم إدارة الأقمار الصناعية المسؤولة عن الاتصالات، ونظم تحديد الموقع الجغرافي (GPS)، في تطور خطير لاستخدام الهجمات السيبرانية من شأنه أن يتسبب في كارثة نووية، أو في تصاعد الأعمال العدائية بين الدول، وفقاً لأسوأ سيناريو، خاصة إذا لم يتم تقييد إطلاق مثل هذه الهجمات.

فمنذ ابتكار الإنترنت على يد وكالة الأمن القومي الأمريكي في ستينيات القرن الماضي، واختراع شبكة الويب على يد تيم بيرنرز لي في نهاية الثمانينيات من القرن العشرين، صاحبت ذلك أيضاً ظاهرة القرصنة والاختراقات السيبرانية، وكانت غير مقلقة في بدايتها، وتتمثل في سرقة بيانات شخصية عبر البريد الإلكتروني، أو إغلاق موقع إنترنت عبر إغراقه بملايين من الطلبات حتى يتوقف عن العمل، إلا أنه مع تطور تقنيات الإنترنت وتزايد الاعتماد عليها في أشكال الحياة اليومية كافة، تطورت أيضاً الهجمات السيبرانية وأصبحت من أخطر التهديدات والتحديات اليومية التي تهدد سلامة الدول والمؤسسات والأفراد، للدرجة التي دفعت كثيراً من الدول إلى تبني استراتيجيات للأمن السيبراني، وأصبحت الهجمات السيبرانية في مقدمة تهديدات الأمن القومي التي تواجه الدول.

وعلى الرغم من خطورة الهجمات السيبرانية والتداعيات السلبية الناجمة عنها، إذا استهدفت قطاعات مثل المؤسسات المالية والاقتصادية والبيانات الشخصية للأفراد وقواعد البيانات الحكومية ونظم الاتصالات والمواصلات، فإن جميع هذه التداعيات ليست كارثية ويمكن احتواؤها، وذلك إذا قورنت بتلك الهجمات التي تستهدف المنشآت النووية والأقمار الصناعية، والتي من شأنها أن تؤدي إلى اندلاع حروب بين دولتين أو أكثر.

أولاً: بدايات استهداف المنشآت النووية

تعتبر عناصر الأمان والسلامة من أهم أركان أي منشأة نووية، وعلى الرغم من أن الأمن

السيبراني النووي (Nuclear cyber security) يعد أحد أهم عناصر الأمان والسلامة، فإنه في دراسة صدرت عام 2016 من "مبادرة التهديد النووي" (The Nuclear Threat Initiative) أشارت إلى أن نصف الدول التي لديها منشآت نووية في العالم ليست لديها إجراءات، أو تشريعات للأمن السيبراني تضمن الحفاظ على أمن المنشأة من الهجمات السيبرانية، وهو ما يعني أن معظم المنشآت النووية بهذه الدول عرضة بدرجات متفاوتة للهجمات السيبرانية[1].

وإذا كانت الدول أكثر تعقلاً من أن تقوم بشن هجمات سيبرانية تنتج عنها كارثة نووية، فإن الحركات الإرهابية والمنظمات الإجرامية والمتطرفين لا يتمتعون بالضرورة بهذه الدرجة من التعقل، فقد تستطيع بعض الحركات الإرهابية امتلاك عناصر فنية مؤهلة تمكنها من شن هجمات سيبرانية على إحدى المنشآت النووية، وأن تتسبب في اختراق المنشآت وتسريب معلومات مهمة عنها، أو أن تتلاعب في نظام إدارة المفاعل، مما ينتج عنه تسريب إشعاعي كبير، أو ارتفاع في درجة حرارة المفاعل يؤدي، مع عوامل إهمال أخرى، إلى انصهار قلب المفاعل، وحدوث انفجار نووي.

ويمكن القول إن الهجمات على المنشآت النووية باتت تتمتع بعدد من السمات، والتي يمكن توضيحها في النقاط التالية:

1- صعوبة تأمين المفاعلات النووية: على الرغم من إدراك مشغلي المنشآت النووية والجهات الإدارية تصاعد التهديدات السيبرانية للمفاعلات النووية، فإن المشكلة تكمن في أن العديد من الطرق التقليدية للدفاع السيبراني في المنشآت النووية، بما في ذلك جدران الحماية وتكنولوجيا مكافحة الفيروسات والفجوات الهوائية (Air Gaps) التي تعمل على فصل شبكات المفاعل الداخلية عن شبكة الإنترنت لم تعد كافية لمواكبة التهديدات الديناميكية المتصاعدة.

2- إمكانية التسبب في تدمير مادي: يعتبر فيروس ستاكسنت والذي اعتبر حينها أخطر أنواع الأسلحة السيبرانية التي تم تطويرها، ومثّل نقلة نوعية في خطورة الحروب السيبرانية، والذي بفضله انتقلت الحرب من تدمير البيانات وسرقتها إلى تدمير المكونات المادية نفسها ونظم التشغيل، وتم استخدام هذا الفيروس في استهداف البرنامج النووي الإيراني.

وقد طورت وكالات الاستخبارات الأمريكية والإسرائيلية فيروس "ستاكسنت" تحت إدارة الرئيس جورج دبليو بوش، كأداة لتعطيل البرنامج الإيراني لتطوير الأسلحة النووية، حيث تم زرع الفيروس عبر جاسوس إيراني داخلي جنده عملاء المخابرات الهولندية، بناء على طلب من وكالة المخابرات الأمريكية والمخابرات الإسرائيلية[2].

وتم اكتشاف ستاكسنت عام 2009 عندما أصاب أجهزة الطرد المركزي الإيراني في منشأة ناتانز لتخصيب اليورانيوم، وتسبب في تعطيل وخروج عدد كبير منها عن العمل، حيث استهدف نظم تشغيل أجهزة الطرد المركزي، التي تعمل عبر برنامج التحكم الصناعي (SCADA) من صنع شركة سيمنز الألمانية، وقام بتسجيل مؤشرات تتعلق بعملية تخصيب اليورانيوم، ثم قام بالتلاعب بآلية عمل أجهزة الطرد وتخريبها، حيث لدى ستاكسنت القدرة على إعادة برمجة وحدات التحكم المنطقي القابلة للبرمجة وإخفاء التغييرات التي تم تنفيذها، وفي الوقت نفسه عرض المعلومات القديمة التي قام بتسجيلها على الشاشات لكي يظهر الأمر للمراقبين والفنيين أن كل شيء يسير بصورة طبيعية، حتى نجح في إنهاء مهمته.

وبصورة عامة يقوم ستاكسنت بمهاجمه أنظمة التحكم الصناعية المستخدمة على نطاق واسع في المنشآت المهمة، مثل خطوط نقل النفط ومحطات توليد الكهرباء والمفاعلات النووية وغيرها من المنشآت الاستراتيجية الحسّاسة، وتقوم بالانتقال بين الأجهزة عبر أجهزة "يو إس بي" (USB) مستغلة إحدى نقاط الضعف في برنامج التشغيل ويندوز.

وليس ذلك فحسب، فقد نقلت شبكة "سي إن إن" الإخبارية الأمريكية عن شون مكجيرك، رئيس دائرة أمن الإنترنت في وزارة الأمن الوطني الأمريكية قوله أمام الكونجرس: "هذا الفيروس يمكن أن يدخل تلقائياً إلى أي نظام، ويسرق صيغة المنتج الذي يتم صنعه، ويغير خلط المكونات في المنتج، ويخدع المشغلين وبرامج مكافحة الفيروسات عبر إيهامهم بأن كل شيء يسير بصورة طبيعية"[3].

3- تعدد أساليب الاستهداف: يتوقف تأثير الهجمة السيبرانية على المنشأة النووية على الهدف من الهجمة نفسها، وتتراوح من تأثير ضعيف إلى تأثير كارثي، ويمكن تصنيف الهجمات السيبرانية على المنشآت النووية إلى ثلاثة أنواع رئيسية هي[4]:

أ- الهجمات على شبكات الأعمال: تستهدف هذه الهجمات سرقة البيانات الحيوية، سواء الخاصة بالعاملين في المنشأة النووية، أو إجراءات السلامة بداخلها، والتي قد تستخدم للابتزاز، أو المكاسب المالية، كما يمكن أن تستخدم كوسيلة لسرقة معلومات تساعد في الوصول إلى أنظمة الوصول وأنظمة التحكم الصناعي.

ب- الهجمات على أنظمة صلاحيات الدخول: تهدف إلى اختراق نظام أذونات الموظفين بالمنشأة، بما في ذلك أنظمة الحماية المادية، أو التحكم والسيطرة، وذلك بهدف دخول المنشأة، أو حتى الوصول إلى مناطق مقيدة (Restricted Areas) من المنشأة، والتي قد تحتوي على بعض المواد النووية التي يخطط المهاجمون إلى سرقتها واستخدامها في أعمال إرهابية.

ج- الهجمات على أنظمة التحكم الصناعية: تعد أخطر أنواع الهجمات، التي يمكن أن تتعرض لها المنشأة النووية، حيث تستهدف الأنظمة الرقمية التي تتحكم في المنشأة، مثل أجهزة الاستشعار والصمامات وأنظمة التبريد وأجهزة الطرد المركزي، بما في ذلك أنظمة الأمن والسلامة، بما قد يؤدي إلى تعطيل المفاعل بصورة جزئية، أو كلية أو إطلاق مواد مشعة، مثلما حدث مع أجهزة الطرد المركزي الإيرانية.

4- تنامي وتيرة استهداف المفاعلات: تصاعد في الآونة الأخيرة

معدل استهداف المفاعلات النووية بهجمات سيبرانية، فقد أعلنت شركة كوريا الجنوبية للطاقة المائية والنووية أن أنظمة الكمبيوتر لديها تعرضت لاختراق سيبراني في ديسمبر 2014، لكن لم تؤخذ منها سوى بيانات غير حساسة، حيث عثرت السلطات الكورية الجنوبية على أدلة تشير إلى وجود "دودة" إلكترونية محدودة المخاطر في أجهزة متصلة ببعض نظم التحكم في محطة لتوليد الكهرباء من الطاقة النووية، غير أنه لم يعثر على أي فيروس ضار في وحدات التحكم بالمفاعلات.

وقررت وزارة الطاقة والمؤسسة المنظمة للطاقة النووية في كوريا الجنوبية إبقاء فرق الطوارئ في حالة تأهب، تحسباً لأي هجمات إلكترونية على محطات الطاقة النووية، مشيرة إلى ضلوع كوريا الشمالية في الهجوم، لكن ليس هناك ما يؤكد ذلك[5].

ومن ناحية أخرى نشرت صحيفة نيويورك تايمز تقريراً صادراً من الحكومة الأمريكية يدعي أن روسيا قامت بشن هجمات سيبرانية ضد منشآت نووية ومحطات كهرباء ومياه في كل من الولايات المتحدة وأوروبا خلال الفترة من 2015 وحتى 2017، من دون أن يشير التقرير إلى ما إذا كان الهدف من هذه الهجمات هو التدمير، أو التجسس وجمع المعلومات[6].

> **حذر مركز تشاتم هاوس دول حلف الناتو، في تقرير صادر في يوليو 2019، من أن الحرب السيبرانية من جانب روسيا والصين ضد أوروبا أصبحت تمثل أحد أبعاد الحرب "الهجينة" ضد أنظمة الناتو والدول الأعضاء الرئيسية، خاصة محاولات استهداف الأقمار الصناعية.**

وفي أبريل 2016 تم اكتشاف فيروسات خبيثة داخل أجهزة كمبيوتر في مفاعل جوندريمنجن (Gundremmingen) في ألمانيا، حيث استطاع الفيروس أن يصيب أجهزة الكمبيوتر، فضلاً عن 18 وسيطاً متحركاً آخر يستخدم في نقل البيانات داخل المفاعل، إلا أن الفيروس لم يؤثر على عمل المفاعل، نظراً لأن العمليات الصناعية نفسها مفصولة عن الإنترنت[7].

كما نشرت الصحيفة تقريراً آخر صادراً من البنتاجون خاصاً باستخدام أدوات غير حركية (Non-kinetic options) لمهاجمة الصواريخ النووية، بما يعني ذلك استخدام الهجمات السيبرانية، أو أي أدوات أخرى غير عسكرية[8]، ولعله جدير بالذكر أن مهاجمة صاروخ نووي عبر هجمات سيبرانية قد ينجم عنه انفجار الصاروخ وحدوث كارثة نووية، وهو ما يثير التساؤل حول الحاجة إلى صلاحيات الرئيس الأمريكي أولاً للموافقة على شن الهجمة السيبرانية باعتبار أن استخدام إطلاق أو مواجهة سلاح نووي يتطلب الحصول على إذن الرئيس أولاً.

وفي يونيو 2017 تعرضت أيضاً محطة "تشيرنوبل" النووية لهجوم سيبراني حسبما ذكرت الوكالة الأوكرانية الفيدرالية للتحكم بمنطقة عزل "تشيرنوبل"، وقالت الوكالة إن الانقطاع المؤقت بأنظمة تشغيل "ويندوز" أوقف العمل على المراقبة الآلية للإشعاعات المتسربة في المنطقة الصناعية، وإن المشرفين اضطروا إلى تنفيذ هذه العمليات يدوياً[9].

ثانياً: الهجمات على الأقمار الصناعية

تعتمد الأقمار الصناعية بصورة رئيسية على بنية تحتية سيبرانية، سواء تمثلت في البرمجيات المستخدمة (Software)، أو الأجهزة (Hardware)، وتزداد خطورة الأمن السيبراني للأقمار الصناعية تدريجياً مع تزايد الاعتماد عليها، سواء في الأغراض المدنية أو العسكرية، فإذا تمت السيطرة مثلاً على نظم تحديد الموقع الجغرافي والتلاعب ببيانات الأقمار الصناعية، فإن ذلك سيؤدي لنتائج كارثية، مثل التلاعب بمسارات المركبات ذاتية القيادة الآلية، مثل السيارات والقطارات وخروجها عن مسارها مسببة كوارث بشرية، أو تغيير مسار صاروخ، أو طائرة مسيّرة عسكرية، إلى وجهة أخرى، أو مناطق مدنية مسببة خسائر كبيرة، فضلاً عن ذلك يمكن اختراق عملية الاتصال بالقمر الصناعي والتلاعب بها لإخراج القمر الصناعي عن مداره أو التجسس وسرقة المعلومات المرسلة منه.

وهناك طريقة شائعة أخرى للهجوم على الأقمار الصناعية، وذلك عن طريق "أجهزة التشويش"، حيث يمكن للتشويش أن يتداخل مع الإشارات التي تنتقل من الأقمار الصناعية إلى المحطات الأرضية، أو تمنع وصولها من الأساس، حيث ذكر تقرير حديث صادر عن وكالة الاستخبارات الدفاعية الأمريكية (DIA) أن الصين تعمل الآن على تطوير أجهزة تشويش يمكن أن تستهدف مجموعة واسعة من الترددات، بما في ذلك نطاقات الاتصالات العسكرية. ويُعتقد كذلك أن كوريا الشمالية اشترت أجهزة تشويش من روسيا. ومن المعروف أن التنظيمات المسلحة في العراق وأفغانستان تستخدمها أيضا[10].

ويلاحظ أن الهجمات على الأقمار الصناعية تتصف بعدد من السمات، والتي يمكن بيانها على النحو التالي:

1- صعوبة التأمين السيبراني: يعتبر الأمن السيبراني أحد أهم مكونات هذه الصناعة العملاقة، لكن المشكلة أن نقاط الضعف التي يمكن استغلالها في شن هجمات سيبرانية على الأقمار الصناعية متعددة، بعكس المنشآت النووية التي يمكن فصل بعض أقسامها عن شبكة الاتصالات والإنترنت، وهو أمر صعب الحدوث بالنسبة للأقمار الصناعية، فهي صنعت لكي تحقق التواصل والاتصال، ولا يمكن أن تكون فعّالة من دون هذه الوظيفة، وهو ما يجعل من اختراقها ليس بالأمر الشاق. فمثلاً يمكن اختراق القمر الصناعي أثناء عملية الاتصال مع المحطة الأرضية، ويمكن اختراق المحطة الأرضية نفسها عبر اختراق أجهزة الكمبيوتر الموجودة بها، ومن ثم السيطرة على القمر الصناعي من الأرض[11].

2- استهداف الأقمار العسكرية: يزداد اعتماد المؤسسات العسكرية على الأقمار الصناعية لإرسال البيانات وتلقي المعلومات، مثل الطقس والملاحة والصور، وأي هجوم سيبراني يستهدف سلامة البيانات المتدفقة عبر الأقمار الصناعية يؤثر على النطاق الترددي المتاح للاستخدام العسكري، مع الأقمار الصناعية ذات الاستخدام المزدوج المدني والعسكري، فهناك "حاجة متزايدة لتطبيق مواصفات عسكرية عالية الجودة في حماية البيانات[12].

وفي تقرير صادر من شركة سيمنانتيك للأمن السيبراني في يونيو 2018 أشار إلى وجود هجمة سيبرانية من أجهزة صينية ضد أهداف في أمريكا وجنوب آسيا شملت أقمار صناعية إلى جانب أهداف أخرى، وذلك بهدف التجسس[13]، وليس الصين وحدها، بل أن الفاعلين من دون الدول مثل الحركات الإرهابية والمرتزقة من القراصنة يمكن لهم اختراق الأقمار الصناعية، وإلحاق ضرر كبير بها، أو التجسس على المعلومات المتدفقة منها بهدف استغلالها، أو بيعها لأطراف أخرى بمقابل مادي.

ففي عام 2008، نجحت إحدى الهجمات الإلكترونية على محطة أرضية في النرويج في التدخل في عمل أقمار "لاندسات" التابعة لوكالة ناسا، وذلك لمدة 12 دقيقة، وفي وقت سابق من عام 2019، تمكّن بعض المتسللين من الوصول إلى القمر الصناعي "تيرا إرث" (Terra Earth) التابع للوكالة ذاتها، وقاموا بالوصول إلى البيانات ومراكز التحكم من دون إصدار الأوامر، ومن غير الواضح من يقف وراء الهجوم، على الرغم من أن بعض المحللين في ذلك الوقت وجّهوا أصابع الاتهام للصين[14].

3- توظيفها ضمن الحرب الهجينة: حذر مركز تشاتم هاوس دول حلف الناتو، في تقرير صادر في يوليو 2019، من أن الحرب السيبرانية من جانب روسيا والصين ضد أوروبا أصبحت تمثل أحد أبعاد الحرب "الهجينة" ضد أنظمة الناتو والدول الأعضاء الرئيسية، خاصة محاولات استهداف الأقمار الصناعية، حيث تقوم معظم العمليات العسكرية المشتركة على اتصالات وتنسيق بين الدول قائم عبر الأقمار الصناعية[15].

4- تطوير أقمار كمومية: بدأ الجيش الأمريكي، في محاولة لتحقيق أمن الأقمار الصناعية، يسعى إلى تطوير أقماره الصناعية بصورة يجعلها أكثر مناعة في مواجهة الهجمات السيبرانية وعمليات التشويش، وكذلك أكثر صعوبة في تحديد مكانها. فعلى سبيل المثال، من المُقرر أن تُطلق واشنطن عام 2022 قمراً صناعياً تجريبياً جديداً، هو "إن تي أس - 3" (NTS-3) الذي سيكون بهوائيات قابلة للبرمجة والتوجيه، ويمكن أن يبث إشاراته بقوة أكبر لمواجهة التشويش، وتم تصميمه ليبقى موجهاً للنقطة التي يركز عليها على الأرض، حتى لو فقد اتصاله بوحدات التحكم الأرضية، كما تمت برمجته على كشف محاولات التشويش على إشاراته[16].

كما دفع ذلك بعض الدول، مثل الصين والولايات المتحدة الأمريكية وروسيا وكذلك الاتحاد الأوروبي إلى تصميم أقمار صناعية كمومية (Quantum Communications Sat-ellite) بهدف تشفير البيانات المتدفقة من القمر الصناعي إلى المحطة الأرضية والعكس، حتى تحمي عملية الاتصال بالقمر من القرصنة والاختراق، وكان أول قمر صناعي كمومي أطلقته الصين عام 2016، كما وقع الاتحاد الأوروبي اتفاقية لتصميم أقمار صناعية تقدم خدمة اتصالات كمومية مع شركة (SES S.A.) في لوكسمبرج التي توفر خدمة الاتصال بالأقمار الصناعية إلى العديد من الجهات الحكومية والخاصة حول العالم[17].

وفي الختام، يمكن القول إن هناك حاجة ملحة لتقييد عملية شن الهجمات السيبرانية على المنشآت النووية والأقمار الصناعية، سواء من الدول أو الفاعلين من غير الدول، نظراً لجسامة الخسائر المترتبة على ذلك، والتي قد تتمثل، وفقاً لأسوأ سيناريو في التسبب في نشوب حرب دولية، ولعل التوجه الحالي يتمثل في محاولة زيادة درجة تأمين المفاعلات النووية، والأقمار الصناعية من الهجمات السيبرانية، كما قد يكون من المفيد في هذا الإطار تبني اتفاقية دولية تهدف إلى تحجيم استهداف الدول للمفاعلات النووية والأقمار الصناعية.

1- Page Stoutland, Cyberattacks on Nuclear Power Plants: How Worried Should We Be?, **The Nuclear Threat Initiative**, March 19, 2018, accessible at: https://bit.ly/2kp6EEh (Last accessed: accessed August 19, 2019).

2- هولندا جندت جاسوساً إيرانياً... كيف تم الهجوم على منشأة "نطنز" النووية؟، **الشرق الأوسط**، 3 سبتمبر 2019، موجود على الرابط التالي: https://bit.ly/2kt0kLR

3- مسؤول: فيروس "ستكسنيت" سيغير قواعد اللعبة، **سي إن إن**، 18 ديسمبر 2010، موجود على الرابط التالي: https://cnn.it/2kpkB55 (تاريخ المطالعة: 20 أغسطس 2019)

4- The Cyber Threat to Nuclear Facilities: Frequently-Asked-Questions, **The Nuclear Threat Initiative**, accessible at: https://bit.ly/2lBzkde (Last accessed: August 20, 2019)

5- طوارئ بكوريا الجنوبية لحماية محطاتها النووية، **سكاي نيوز عربية**، 26 ديسمبر 2014، موجود على الرابط التالي: https://bit.ly/2ks0aV1

6- Page Stoutland, **op.cit.**

7- Christoph Steitz, Eric Auchard, German nuclear plant infected with computer viruses, operator says, **Reuters**, APRIL 27, 2016, accessed August 20, 2019, accessible at: https://reut.rs/2ls5gqq

8- David E. Sanger, Pentagon Puts Cyberwarriors on the Offensive, Increasing the Risk of Conflict, **The New York Times**, June 17, 2018, accessible at: https://nyti.ms/2K0XMQ0 (Last accessed: August 20, 2019)

9- محطة "تشيرنوبل" النووية تتعرض لهجوم إلكتروني، **سي إن إن**، 27 يونيو 2017، موجود على الرابط التالي: https://cnn.it/2jXtL8G (تاريخ المطالعة: 23 أغسطس 2019)

10- Niall Firth, How to fight a war in space (and get away with it), **MIT Technology Review**, June 26, 2019, accessible at: https://bit.ly/2jXtRx4 (Last accessed: August 22, 2019)

11- Meghan Bartels, Why Satellites Need Cybersecurity Just Like You, **Space**, December 10, 2018, accessible at: https://bit.ly/2E93ZWR (Last accessed: August 23, 2019)

12- Zak Doffman, U.S. Military Satellites Likely Cyber Attacked By China Or Russia Or Both: Report, **Forbes**, July 5, 2019, accessible at: https://bit.ly/2kddnRL (Last accessed August 23, 2019)

13- Joseph Menn, China-based campaign breached satellite, defense companies: Symantec, **Reuters**, June 20, 2018, accessible at: https://reut.rs/2M431vO (Last accessed: August 23, 2019)

14- نيال فيرث، عرض محمد محمود السيد، حرب الفضاء: مستقبل صراعات القوى الكبرى حول " الأقمار الصناعية"، **مركز المستقبل للأبحاث والدراسات المتقدمة**، 18 أغسطس 2019، موجود علي الرابط التالي: https://bit.ly/2lzkVyA (تاريخ المطالعة: 21 أغسطس 2019)

15- Beyza Unal, Cybersecurity of NATO's Space-based Strategic Assets, **Chatham house**, July 2019, accessible at: https://bit.ly/2XNNmtM (Last accessed August, 24, 2019)

16- Sandra Erwin, Air Force experiment NTS-3 could point the way to the next generation of GPS, **Space News**, March 16, 2019, accessible at: https://bit.ly/2Uk6UEt (Last accessed: August 24, 2019)

17- Beyza Unal, **op.cit.**