مخاطر منظومات الأقمار الصناعية

د. علي المشاط

2016-02-01

أصبحت منظومات الأقمار الصناعية أدوات أساسية مُمَكِّنة لمجموعة واسعة من التطبيقات التجارية، والعلمية، والعسكرية في العالم المعاصر. ولسوء الحظ، فإنّ هذه المنظومات إذا ما تعرّضت للضرر بفعل ظاهرة طبيعية أو هجمات بشرية، قد تُعرِّض المجتمعَ العالمي لمجموعة واسعة من المشكلات الحادة التي قد تضع مليارات البشر تحت الخطر. ونحن اليوم نعتمِد بشدة على الأقمار الصناعية بكافة أنواعها ومنها أقمار الاتصالات والبَثّ التلفزيوني، وتحديد المواقع العالمية، ومراقبة الأرض، والاستشعار عن بُعد، ورصد الأحوال الجوّية، ومراقبة التغيُّر المناخي، والإنذار المبكر من الكوارث. بالإضافة إلى الدعم العسكري، ومراقبة المواصلات والنقل. وباختصار، أصبحت هذه البُنية التحتيّة الفضائية أساسية في أداء المجتمعات المعاصرة. وغدَت هذه المنظومات تدعم النمو الاقتصادي، والخدمات التربوية والصحية، والنقل، وأنظمة الطاقة، والأمن العام، وإجراءات حكومية أساسية، وكذلك بوسائل شتّى أنماط الحياة المجتمعية مثل الرياضة، والترفيه، والأخبار.

إنّ الاعتماد المتزايد على بعض هذه المنظومات يجعل منها بُنيةً تحتيّة حسّاسة. وأي إخلالٍ أو تدميرٍ مستقبلي لهذه البُنية التحتية قد يُولّد ضرراً دائماً وربّما خسائر كبيرة في الأرواح والأموال. وباختصار، فقد أصبحت هذه المنظومات الحسّاسة عِماداً تكنولوجياً للبُنى التحتية الاعتيادية القائمة، مثل الطاقة، والنقل، والاتصالات، والأمن، والتشبيك المعلوماتي، ومجموعة واسعة من الأنظمة العسكرية والدفاعية الأساسية.

جوانب الضعف والمخاطر: كيف تُشكّل منظومات الأقمار الصناعية مصدرَ خطرٍ

من الضروري أن تُقيَّم جوانبُ ضعف منظومات الأقمار الصناعية للتهديدات الطبيعية والإرهابية في مجالاتٍ مثل التداخُل مع التردُّدات الراديوية والتشويش، والهجوم الليزري، والأشعة الكهرومغناطيسية من جرّاء انفجارٍ نووي أو عواصف شمسية، إضافةً إلى أنواع عديدة من الهجمات السايبرية، في الوقت الذي يمكن استخدام منظومات الأقمار الصناعية كاحتياطٍ أساسي وحمايةٍ عند فشل البُنية التحتيّة الأرضية. وفي الوقت الحاضر، هنالك اهتمامٌ دولي بمخاطر الفضاء

الخارجي من قِبَل الأمم المتحدة وجمعيات علمية تهتم بالفضاء الخارجي وذلك لاستبيان وتقييم المخاطر العالمية للمنظومات الفضائية التجارية والعسكرية. وتطرح هذه الورقة تقييماً لأهم المخاطر العالمية لجوانب الضعف وقابلية التعرُّض للضرر. وتشمل تلك جوانبَ الضعف وقابلية التعرُّض للضرر بفعل الظواهر الطبيعية مثل الانفجارات الشمسية الحادّة والتدفُّق الهائل للبلازما من الإكليل الشمسي، وسقوط النيازك. ويمكن حصر تأثيراتها على:

- خطوط الطيران (النقل الجوّي)
- الشبكات الكهربائية
- كافة شبكات تكنولوجيا المعلومات والاتصالات (ICT)
- شبكات المياه
- المدن الكبرى ومناطق التجمُّعات الحَضرية الكبيرة
- العمالة المستندة إلى البُنية التحتية الأساسية
- البُنية العسكرية

خطوط الطيران (النقل الجوّي)

يتواصل ارتفاعُ حجم رحلات النقل الجوّي على نحو دراماتيكي. وثمة تنظيمٌ لأكثر من مائة ألف رحلة طيران مدني كلّ يوم. وهذا لا يشمل رحلات الطيران الخاصة والرحلات المتصلة بالشؤون العسكرية. وتعتمد هذه الرحلات بشدّة على المنظومات الفضائية للملاحة – لا سيّما منظومة تحديد المواقع العالمية (GPS). وهناك إطلاقٌ مُنتَظَرٌ لمجموعة أقمار "إيريديوم نكست". وأيُّ إخفاقٍ في هاتين المنظومتين الملاحيتين العاملتَين بالأقمار الصناعية يشل إلى حدٍّ كبير، قدرات عمليات الإقلاع والهبوط للطائرات. وإذا ما أخفقت هذه المنظومات العالمية لتحديد المواقع، والملاحة، والتوقيت على نحو دقيق (المنظومة الروسية "غلوناس" GLONASS، والمنظومة اليابانية "كواسي زينث" Quasi Zenith، والمنظومة الصينية "بايي داو" Bei Dou، ومنظومة أقمار الملاحة الإقليمية الهندية) إضافة إلى منظومة تحديد المواقع العالمية، فهذا من شأنه أن يشلّ قدرات توجيه رحلات الطيران المدني والعسكري أيضاً. إنّ هذه المنظومات هي عرضة للتشويش عليها أو تعطيلها بفعل الكوارث الطبيعية، إذ من شأن أي "نبضة كهرومغناطيسية" (EMP) ناجمة عن انفجارٍ نووي أو انفجارٍ شمسي حادّ أن يكون لها تأثيرٌ مُدمِّر على المعدّات الإلكترونية في الطائرات وبالتالي على جميع الأقمار الصناعية العاملة حالياً في المدار.

الشبكات الكهربائية وجوانب الضعف

إنّ أي "نبضة كهرومغناطيسية" طبيعية يُطلقها انفجارٌ شمسي حادّ على غرار الانبعاث الهائل للبلازما من الإكليل الشمسي قد تُحدِث انقطاعاً في شبكات

الكهرباء الرئيسية. فعلى سبيل المثال، فإنّ "حادثة مونتريال" في العام 1989 قطعت الخدمة الكهربائية عن مدينة شيكاغو في الولايات المتحدة وصولاً إلى مدينة مونتريال في كندا. ولو كان لهذا الحَدَث أن يتكرّر اليوم فلربّما يُعطّل تأثيره إمدادات النفط وشبكات الكهرباء في جميع أنحاء العالم. ولربّما اشتعلت آلاف المحوّلات الكهربائية واستغرقَ استبدالها أشهراً عديدة. ويتطلّب التخطيطُ للشبكات الكهربائية الذكية أيضاً أن يأخذ في عين الاعتبار المخاطرَ الطبيعية والإرهاب السايبري. فربّما تكون الهجمات على شبكات الطاقة الكهربائية الأكثر شيوعاً بين مُختَرِقِي الإنترنت.

كافة شبكات تكنولوجيا المعلومات والاتصالات

إنّ نقطة الضعف الأولى في معظم الدول تتمثّل حالياً في تكنولوجيات المعلومات والاتصالات وكذلك انقطاع الطاقة الكهربائية. ذلك أنّ معظم البُنى التحتية الأكثر أهمية (النقل، الطاقة، المياه، الصرف الصحي، وشبكات الاتصالات العسكرية والأمنية) تعتمد فعلياً بنسبة مئة بالمئة على شبكات تكنولوجيا المعلومات والاتصالات. واليوم، تتّسِم شبكات تكنولوجيا المعلومات والاتصالات وأنظمة "المراقبة والإشراف وحيازة البيانات" (SCADA) بحمايةٍ غير كافية ضد المُخترقين. فالأنظمة المستندة إلى منظومات الأقمار الصناعية لم يتم تصميمها على نحو تام لتأمين احتياطات ضرورية في حالات الطوارئ بما في ذلك الكوارث الطبيعية كالأعاصير، والزلازل والفيضانات. وبإمكان تكنولوجيات جديدة على غرار أنظمة المنصّات العالية الارتفاع أن توفّر مجالاً آخر للمناعة. ويمكن أيضاً أن تُزَوَّد الأقمار الصناعية بمستويات إضافية من الحماية.

شبكات المياه

إنّ المجتمعات المزدحمة تزدادُ تعرُّضاً لانهياراتٍ في شبكات الاتصالات، والمعلومات، والمواصلات، والشبكات المالية. وفي حالاتِ كوارثٍ كبرى مثل اضطراب شمسي عنيف، وسقوط نيزك كبير خطر، وهجمات "نبضة كهرومغناطيسية"، فإنَّ العنصرَ الأساسي لنقطة الضعف ربّما يتبدّى أولاً في ما يتعلّق بانهيار شبكات إمدادات المياه. وهذا قد ينطبق بشكلٍ خاص على الدول أو المدن الكبرى التي تضطر إلى استيراد جميع موادها الغذائية تقريباً أو استمداد مياهها عبر أنابيب ممتدة لمسافاتٍ طويلة. وهناك وسائل عديدة يمكن من خلالها لهجماتٍ إرهابية أو كوارث طبيعية أن تعوق، أو تُغلِق، أو تُحدِث اضطراباً في خطوط نقل الإمدادات، وكذلك تُلوّث أو تُسمِّم أو تُؤثّر سلباً في إمدادات المياه وشبكات إمداد الأغذية إمّا عبر هجومٍ مادي مباشر أو من خلال هجمات سايبرية. ويتعيّن أنْ تُؤخَذ في الاعتبار وبكل جديّة استراتيجياتُ التشبيك الاحتياطي المستندة إلى الفضاء فضلاً عن الاستراتيجيات الدفاعية لمواجهة الانبعاثات الهائلة من الإكليل الشمسي والهجمات السايبرية

المنسَّقة إلخ.. فضلاً عن تقييم أفضل الخيارات. وهذا يُشكّل جزءاً أساسياً من عملية تقييم المخاطر العالمية.

المدن الكبرى ومناطق التجمُّعات الحضرية الكبيرة

إنّ معظم المدن الكبرى لم تتم هندستها وتصميمها على نحو وافٍ لتحمُّل كارثة كبيرة مثل الإعصار، أو الزلزال، أو سقوط نيزك، أو نبضة كهرومغناطيسية ناجمة إمّا عن انفجارٍ شمسي طبيعي أو هجوم إرهابي، أو هجوم سايبري ضد شبكات النقل، والمعلومات، والاتصالات إلخ.. ويشي ازدياد التمدُّن والتحضُّر، ووظائف الخدمات المعتمدة على تكنولوجيات الاتصالات والمعلومات، وكثافة السُّكّان الأكبر والاعتماد على المصاعد المرتفعة جداً في المباني العالية، بأنّ المدن الكبرى هي الأماكن الأقل مناعة ضد الهجمات أو الكوارث الطبيعية. والحلُّ يكمنُ في التشديد على أنّ المدن الصغرى يمكنها أن تُخفّف الضغط عن المدن الكبرى المُتخَمة بالسُّكّان. ويمكن لشبكات المعلومات والاتصالات في المدن الصغيرة المتّسِمة بالمناعة والاستجابة أن تساعد أيضاً من ناحية التعليم، والرعاية الصحية، والاستجابات المدنيّة الأكبر.

العمالة المستندة إلى البُنية التحتية الأساسية

يعتمد سُكّانُ المدن أكثر فأكثر على وظائف الخدمات التي يمكن أن "تتبدّد" في حال وقوع كارثة طبيعية كبرى أو هجوم إرهابي. وتكون وظائف الخدمات أكثر عرضة في حال تعرّضت البُنية التحتية الحسّاسة للتدمير أو للتعطيل لفترةٍ مستديمة. وهنا يمكن لقدرات التربية عن بُعد، والرعاية الصحية عن بُعد، وتشبيك المعلومات، والعمل عن بُعد المستندة إلى الفضاء أن تساعد في تأمين الاستقرار الاقتصادي وقدرات الاحتياط في حال وقوع كارثة طبيعية أو هجوم سايبري.

البُنية العسكرية

تعتمد الأنظمة العسكرية اليوم بازدياد على منظومات الأقمار الصناعية من أجل الاتصالات، والملاحة وتحديد الأهداف، والاستشعار والمراقبة عن بُعد، وعمليات التحكُّم بالطائرات عن بُعد. كما أنّ هناك اعتماداً على المنظومات الفضائية التجارية ذات الاستخدام المزدوج كشأن الاعتماد على المنظومات الدفاعية العسكرية المخصّصة لذلك. وفيما يتنامى هذا الاعتماد، يمكن أن تصبح الأنظمة العسكرية عرضةً لهجماتٍ سايبرية مباشرة، ونبضات كهرومغناطيسية بفعل أسبابٍ طبيعية أو أخرى من صنع البشر. لذا فإنّ أنظمة الاحتياط التي يمكن أن تؤمّن استرداداً طارئاً لأنظمة تكنولوجيا المعلومات والاتصالات الدفاعية تغدو على قدرٍ من الأهمية يزداد يوماً بعد يوم.

المخاطر الناجمة عن إشعاعات كونيّة على شبكات تكنولوجيا المعلومات والاتصالات

ثمة تأكيدٌ متزايد في السنوات الأخيرة على التهديد المتنامي للإرهاب السايبري، والحرب السايبرية والمخاطر الاجتماعية الأخرى المتأتّية من الاعتماد المفرط على تكنولوجيات المعلومات والاتصالات. لكن لم يكن ثمة اعترافٌ مماثل بطبيعة العديد من المخاطر الكونيّة والمخاطر المتصلة بالحطام المداري التي قد تؤثّر سلباً في الاتصالات الفضائية، وقدرات الملاحة، والاستشعار والمراقبة عن بُعد. وثمة دراسةٌ حديثة أجرتها وكالة الفضاء الأميركية "الناسا" (NASA) قد رجّحت حدوث انفجارٍ شمسي كبير (أي تدفق كُتلي هائل للبلازما من الإكليل الشمسي) في العقد المقبل يمكن أن يُعطّل كلّياً شبكات الكهرباء وشبكات تكنولوجيا المعلومات والاتصالات بنحو 50%. وتوقّعت دراسة أجرتها مؤسّسة التأمين العالمية "لويدز" في لندن حول تداعيات حَدَث تدفُّق كُتلي هائل من الإكليل الشمسي يشلّ الشبكة الكهربائية، وخطوط نقل النفط، وأقمار تحديد المواقع العالمية، وشبكات تكنولوجيا المعلومات والاتصالات، أن يُسبِّب مثلُ هذا الحَدَث ضرراً تُقدَّر قيمته بمئات مليارات الدولارات. أمّا معظم الضحايا البشرية لمثل هذا الحَدَث فربّما تكون لأشخاصٍ قضوا نحبهم بسبب نقص الغذاء والمياه. ومن بين الحقائق التي يتم التغافل عنها، أنّه إذا ما خسرنا منظومة تحديد المواقع العالمية فإنّنا سنخسر في عضون فترةٍ قصيرة من الوقت عمليةَ تزامن شبكة الإنترنت العالمية. وهذا لا يحدّ من الضرر الشديد الناتج عن هجمات على الإنترنت، وشبكات "الإنترانت" (Intranet) بين المرافق المحلية، وشبكات الربط بين الشركات، وشبكات "المراقبة والإشراف وحيازة البيانات" (SCADA) التي تتحكّم بأنابيب النفط، وأنظمة الطاقة الكهربائية، وأنظمة الصرف الصحي، وأنظمة إشارات الحركة الجوّية والنقل، وكذلك أنظمة تبريد المفاعل النووية، وغيرها.

التقييم العالمي للبُنية التحتية الفضائية

يتعيّن إجراء مراجعة جدّية شاملة لجميع جوانب الضعف هذه وكذلك البرامج التي من شأنها أن تحُدّ من التأثيرات السيئة للمخاطر الكونية، أو إصلاح تداعياتها أو حتى تجنُّبها. وفيما تغدو المجتمعات أكثر تمدُّناً وتحضُّراً وأكثر اعتماداً على تكنولوجيا المعلومات والاتصالات، في ظل استناد الوظائف أكثر فأكثر إلى البُنية التحتية الحديثة، فإنّها تغدو أكثر عرضةً لأحداثٍ يمكن أن تُهدِّد أرواح ملايين من البشر. وهناك عددٌ كبير من نقاط الضعف التي تُراوِح بين شبكات تكنولوجيا المعلومات والاتصالات وشبكات إمداد المدن بالمياه.

الخُلاصة

ثمة حاجةٌ إلى تصنيفٍ منهجي لمختلف أنواع جوانب الضعف القائمة في ما يتعلّق بشتّى أنواع البُنى التحتية المستندة إلى الفضاء، فضلاً عن استراتيجيات حماية لمنع تلك المخاطر أو الحدّ منها، ووضع استراتيجية استرداد وتعافي بعد وقوع حَدَثٍ مماثل. وينبغي تقسيم تقييم المخاطر إلى الفئات التالية:

- أحداث كبيرة طبيعية و/أو من صنع الإنسان يمكن أن تؤثّر سلباً على شريحة كبيرة من سُكّان العالم.
- البدء بتقييمٍ خاص لمختلف أحداث الهجمات البشرية أو المخاطر الطبيعية التي يمكن أن تُضعِف أو تُدمِّر بُنية تحتية فضائية حسّاسة مخصّصة لـ:

- شبكات اتصالات ومعلومات مدنيّة أو عسكرية، بما في ذلك أنظمة أرضية، وفضائية وأخرى للمراقبة والإشراف وحيازة البيانات SCADA؛
- أقمار تحديد مواقع وملاحة (بما في ذلك جوانب الضعف في شبكة الإنترنت).
- أقمار الاستشعار والمراقبة عن بُعد ورصد الأحوال الجوّية.

إنّ إجراء هذا التقييم للبُنية التحتية الفضائية والتهديدات الكونية، إلى جانب تطوير منظومات فضاء قادرة على الاستجابة، يمكن أن يؤدّي بالفعل إلى تعاونٍ إقليمي بل وحتى عالمي في الفضاء من شأنه أن يحُدّ من النزاعات وأن يستحدث وسائلَ جديدة لاستخدام منظومات الفضاء.

بريد الكاتب الالكتروني: ali.almashat@gmail.com