# حيل وطرق مُبتكرة

## محاولات الحركات الإرهابية لامتلاك أسلحة غير تقليدية

د. إيهاب خليفة

باحث وكاتب مختص بالتقنيات وقضايا التطرف، مصر

ظلَّت فكرةُ حصول الجماعات الإرهابية على سلاح غير تقليدي؛ كالأسلحة النووية أو الكيميائية أو البيولوجية مستبعدةً؛ لصعوبة الأمر، ولا سيَّما السلاح النووي، نظرًا للإجراءات الأمنية الشديدة التي تمارسها الدولُ في عمليات إنتاج الموادِّ النووية ونقلها وتداولها. ولو افترضنا جدلًا أن الجماعاتِ الإرهابيةَ حصلت على سلاح نووي بالسرقة أو بأيِّ طريقة أُخرى، فإن نقل هذا السلاح واستخدامَه في عمليات إرهابية يتطلَّب من الإجراءات ميدانيًّا ما لا تقدر عليه الجماعاتُ الإرهابية؛ كالحصول على صواريخَ بالستية أو طائرات عملاقة، إلا أن ذلك لم يمنع الجماعاتِ الإرهابيةَ من المحاولة؛ كقيام بعضهم بالتغلغُل إلى إحدى المنشآت النووية في بروكسل عام 2016م؛ بُغيةَ تنفيذ تفجير داخل مفاعل نووي أو سرقة موادَّ نووية.

### التفجير بالطائرات المسيَّرة

صدر في سبتمبر 2022م كتابٌ لأبي محمد المصري أحدِ قادة تنظيم القاعدة بعنوان «عمليات 11 سبتمبر بين الحقيقة والتشكيكات»، تحدَّث فيه عن محاولات الجماعات الإرهابية تنفيذَ تفجير نووي بتوجيه طائرة مسيَّرة محمَّلة بآلافٍ من أوعية الوقود العالي الاشتعال، إلى أحد المفاعلات النووية في أمريكا. وإذا نظرنا إلى التطوُّر الكبير الذي شهدَته الأسلحة السيبرانية في العقد الماضي، وما يمكن تنفيذُه بها من اختراق المنشآت النووية، أو العبث بنظُم السلامة داخل المفاعلات، مثلما حدث في مُنشأة نطنز الإيرانية عام 2009م، فإن القلق من شنِّ الجماعات الإرهابية هجَمات سيبرانية تستهدف المفاعلات النووية يزداد.

وقد أورد أبو محمد المصري في كتابه أفكارًا غير تقليدية لتنفيذ تفجير نووي؛ كالاعتماد على أفراد من الجاليات المسلمة والأقلِّيات التي تعمل في المنشآت النووية، لتجنيدهم في تنفيذ هجَمات داخل هذه المنشآت، أو القيام بعمل تخريبي يؤدِّي إلى حدوث تسرُّب إشعاعي؛ لجعل بعض المناطق غير صالحة للحياة البشرية. وممَّا جاء في كتابه بهذا الصَّدَد:

«إذا وضعنا في الاعتبار المخزونَ الهائل من الأسلحة النووية داخل الأراضي الأميركية، وهو نقطةُ ضعف كبيرةٌ إذا استطاعت الجماعاتُ المقاتلة الوصولَ إليه، وتجريبَ جزء منه على

الأراضي الأميركية، بحيث يجعلُ من أميركا أرضًا غيرَ صالحة للعيش. وهذا أمرٌ ليس بالبعيد، لكنَّه بحاجة إلى إعمال الفكر في كيفية الوصول إلى هذا المخزون الإستراتيجي». ثم أوضحَ فكرته قائلًا: «الجيشُ الأميركي فيه عناصرُ من الجالية المسلمة، وكذلك من الأفارقة الذين يشعرون بالمهانة والذِّلَّة من تصرُّفات البِيض العنصريين التي لا تتوقَّف، وبالاستفادة من هذه النفوس المشحونة يمكننا الوصولُ إلى الهدف والاستفادةُ من ضربة نوعية في الصميم».

هذا على مستوى الأفكار النظرية، ويُضاف إليها محاولاتٌ عملية للقيام بتخريب نووي من قِبَل الجماعات المتطرفة، منها على سبيل المثال: تفجيراتُ بروكسل التي نفَّذها تنظيم داعش في مارس 2016م؛ إذ كشفت عن تخطيط منفِّذي العملية لإحداث هجوم نووي بتفجير إحدى المحطَّات النووية؛ فقتلوا حارسَ إحدى المنشآت، وحصلوا على بطاقة الدخول الخاصَّة به؛ من أجل القيام بتفجير داخل المنشأة. وعثرت الشُّرطة على مقطع مصوَّر مدَّته 12 ساعة من المراقبة، يصوِّر منزل أحد مديري البرنامج النووي البلجيكي، وكان ذلك جزءًا من خُطَّة لخطفه وإجباره على تمكينهم من دخول المنشأة النووية.

## الهجَمات السيبرانية النووية

من مخاطر الأسلحة السيبرانية أو (فيروسات) الحاسوب قدرتُها على استهداف المنشآت النووية، ومع أن الأمن السيبراني النووي للمنشأة يُعَدُّ أهمَّ عناصر الأمان والسلامة، بيَّنت دراسةٌ صدرت عام 2016م ضمن مبادرة التهديد النووي «The Nuclear Threat Initiative» أن نصف الدول ذات المنشآت النووية في العالم ليس لديها تشريعاتٌ أو إجراءاتٌ للأمن السيبراني؛ للحفاظ على المنشآت من الهجَمات السيبرانية! وهذا يعني أن معظم هذه المنشآت عُرضة بدرجات متفاوتة للهجَمات السيبرانية الخطِرة.

وإذا استطاعت جماعةٌ إرهابية امتلاكَ أحد هذه (الفيروسات)، أو شراءه عبر الإنترنت المظلم (Dark Web)، أو تسرَّب إليها من بعض الحكومات، أو حصلت عليه بتجنيد قراصنة إنترنت محترفين، فإن الجماعاتِ الإرهابيةَ يمكنها أن تسبِّبَ تهديدًا نوويًّا حقيقيًّا، لن يرقى بأيِّ حال من الأحوال إلى حدوث تفجير نووي؛ بسبب إجراءات السلامة والأمان داخل هذه المنشآت، لكن قد ينجُم عنه خرابٌ في الأجهزة والنُّظُم، وتسرُّب إشعاعي.

والدولُ عمومًا أعقلُ من أن تشُنَّ هجَمات سيبرانية ينتُج عنها كارثة نووية، لكنَّ الجماعات الإرهابية والمنظَّمات الإجرامية والمتطرفين لا يمتلكون ذاك التعقُّل، وقد تستطيع بعضُ الجماعات شنَّ هجَمات سيبرانية على إحدى المنشآت النووية، أو أن تخترقَ تلك المنشأة،

وتسرَّبَ معلومات مهمَّة عنها، أو تغيَّرَ في نظام إدارة المفاعل؛ ممَّا يُفضي إلى تعطُّل المفاعل ولو جزئيًّا، أو حدوث تسرُّب إشعاعي.

ولا شكَّ أن مشغِّلي المنشآت النووية والجهات التي تُديرها على علم بهذه التهديدات، لكنَّ المشكلة أن الكثير من الطرق التقليدية للدفاع السيبراني في المنشآت النووية - ومن ذلك جُدران الحماية، وتقنية مكافحة الفيروسات، والفجَوات الهوائية التي تعمل على فصل شبكات المفاعل الداخلية عن شبكة الإنترنت - لم تعُد كافيةً لمواكبة التهديدات المتصاعدة.

وتُعَدُّ «دودة ستاكسنت» أوَّلَ نموذج لاستخدام سلاح سيبراني في استهداف مفاعل نووي، وقد استُخدمت لاستهداف البرنامج النووي الإيراني عام 2009م، واعتُبرت أحدَ أخطر أنواع الأسلحة السيبرانية، ومن حينئذٍ ارتفع خطرُ الهجَمات السيبرانية التي تهدِّد المنشآت النووية.

وفي ديسمبر 2014م أعلنت شركةُ «كوريا الجنوبية للطاقة المائية والنووية» أن أنظمة الحاسوب لديها تعرَّضت لاختراق سيبراني، لكن لم تؤخَذ منها سوى بيانات غير مهمَّة، وعثرت السُّلطات على أدلَّة تشير إلى إزالة دودة إلكترونية محدودة المخاطر من أجهزة متَّصلة ببعض نظُم التحكُّم في محطَّة لتوليد الكهرباء بالطاقة النووية، واتُّهمَت كوريا الشمالية بالضُّلوع في الهجوم. وكذلك اكتُشفَت في أبريل 2016م فيروسات خبيثة داخل أجهزة الحاسوب في مفاعل جوندريمنغن في ألمانيا، واستطاع الفيروس أن يصيبَ أجهزة الحاسوب، إضافةً إلى 18 وسيطًا متحرِّكًا تُستخدَم في نقل البيانات داخل المفاعل، إلا أن الفيروس لم يؤثِّر في عمل المفاعل لأن العملياتِ الصناعيةَ مفصولةٌ عن الإنترنت.

هذه النماذجُ السابقة تؤكِّد الحاجة الماسَّة إلى إعادة النظر في إجراءات السلامة السيبرانية في المنشآت النووية، وإن لم يحدُث ذلك فإنها ستصبح عُرضةً للتهديدات، فإذا توافرَ لدى جماعة إرهابية تنظيمٌ قوي وقيادةٌ ذات إصرار على تحقيق الأهداف، فقد تسبِّب عمليةَ تخريب لبعض المنشآت النووية تؤدِّي إلى تسرُّب إشعاعي خطِر.

## المركَّبات الكيميائية والبيولوجية

الأسلحةُ الكيميائية والبيولوجية أقلُّ إضرارًا مقارنةً بالسلاح النووي، إلا أن استخدامها قد يترتَّب عليه خسائرُ كبيرة في الأرواح؛ لسهولة حملها وإصابة عدد كبير جدًّا من الأفراد بها، مثل: إطلاق فيروس في أحد الأنهار الجارية، أو إطلاق مركَّبات وغازات كيميائية مميتة في أحد الميادين الرئيسة، أو في الحافلات والقطارات.

ولذلك صارت الأسلحةُ الكيميائية والبيولوجية بديلًا عن الأسلحة النووية لدى الحركات الإرهابية؛ لسهولة الحصول عليها أو تركيبها، وحملها ونشرها، وقد رصدت «منظَّمة حظر الأسلحة الكيميائية» استخدامَ عامل الخردل في هجوم شنَّه تنظيمُ داعش الإرهابي عام 2015م في شمال سوريا، أدَّى إلى إصابة 20 شخصًا على الأقل، وتعرَّضَت بلدة مارع الواقعة قرب الحدود التركية في محافظة حلب، وهي آنذاك تحت سيطرة المعارضة، لقصف بذخائرَ مملوءة بموادَّ كيميائية يُعتقَد أنها كبريت الخردل، وصدر تقريرٌ عن صحيفة نيويورك تايمز يؤكِّد أن داعش استخدمت الأسلحةَ الكيميائية في سوريا والعراق أكثر من 52 مرَّة بين عامي 2014 و2016م.

وأوقفت الشرطةُ الجنائية الألمانية اثنين من المتطرِّفين المنتمين إلى تنظيم داعش، كانا يخطِّطان لشنِّ اعتداء بقنبلة بيولوجية في البلاد في يونيو 2018م، وأفاد محضرُ الاتهام الذي أعدَّته نيابةُ مكافحة الإرهاب، أنهما قرَّرا في خريف 2017م شنَّ هجوم في ألمانيا، وتفجيرَ عُبُوَّة ناسفة في حشد كبير من الناس؛ لقتل وإصابة أكبر عدد ممكن من الأشخاص.

وأعلنت المغربُ العثورَ على موادَّ سامَّةٍ بيولوجية فتَّاكة، بحَوزة خلية إرهابية داعشية اعتُقلَت في 18 فبراير 2016م بمدينة الجديدة وسَط المغرب، وقالت وِزارةُ الداخلية المغربية: «إن عناصر داعش في مدينة الجديدة المغربية، قاموا بتحضير هذه الموادِّ القاتلة؛ تمهيدًا لاستعمالها في مشروعهم الإرهابي داخل المغرب».

وفي الختام نؤكِّد أن الثورة التقنية الحديثة ووسائلها الذكية أسهمت في تغيُّر مصادر القوَّة وأساليب توظيفها، فأصبحت المعلومةُ التي هي العنصرُ الرئيس من عناصر القوَّة، متوافرةً في مواقع الإنترنت، ويشمل ذلك معلومات عن المنشآت الحيوية التي قد تصبح هدفًا لهجوم إرهابي، مثل: المنشآت النووية، ومحطَّات الطاقة، والمطارات، ومعامل البحوث، وكذلك معلومات عن كيفية صنع عُبُوَّات ناسفة، أو شراء موادَّ متفجِّرة أو أسلحة تقليدية، أو إعداد فيروسات حاسوبية لشنِّ هجَمات سيبرانية، تستهدف محطَّات الطاقة النووية، والوَقود الحيوي، والبُنى التحتية المهمَّة للدول.

هذا التغيُّر الكبير في مصادر القوَّة مكَّن الحركات المتطرفة الإرهابية من تحقيق أهداف كانت في الماضي القريب مستحيلةً عليهم، وهذا التطوُّر التقني مثلما ساعد الحركات الإرهابية في تغيير خُططها العسكرية في السنوات القليلة الماضية، قد يساعدها أكثرَ في السنوات القادمة، إن لم تُجفَّف منابعها وتكافَح أدواتُها.