

تفجيرات "البيجر" في لبنان.. تكنولوجيا قديمة ومخاطر مستقبلية

قُتل ما لا يقل عن تسعة أشخاص وأُصيب ما يقرب من 3 آلاف آخرين عندما انفجرت أجهزة النداء الشخصي "البيجر" المُستخدمة من قبل أعضاء حزب الله - بما في ذلك المقاتلين والمسعفين - بشكل متزامن في لبنان يوم 17 سبتمبر 2024. ووقعت هذه الانفجارات بعد أن رنّت أجهزة النداء الشخصي؛ مما دفع عناصر حزب الله إلى لمسها أو رفعها ليفحصوا الشاشات؛ فأدى ذلك إلى وقوع إصابات بينهم، واستمرت تلك الانفجارات قرابة الساعة، حسب شهود عيان.

وكانت الانفجارات محدودة الشدة نسبياً، تصيب فقط الشخص الذي يمسك جهاز "البيجر" أو الأقرب إليه، وأظهرت مقاطع فيديو من المستشفيات ومشاركات عبر وسائل التواصل الاجتماعي أفراداً يعانون من إصابات في الوجه وفقدان أصابع وجروح كبيرة في عظم الفخذ؛ حيث مكان وضع الجهاز داخل الجيب. لكن لم تتسبب الانفجارات في أضرار كبيرة للمباني أو في اندلاع حرائق.

وقد اختلفت الروايات حول أسباب التفجيرات، فبينما اعتبرتھا الحكومة اللبنانية هجوماً سيبرانياً على الأجهزة المتفجرة، قال آخرون إن إسرائيل ربما تسللت إلى سلسلة التوريد الخاصة بأجهزة "البيجر" وفختها بمواد متفجرة قبل أن يتم نقلها إلى حزب الله.

ما هو "البيجر"؟

البيجر" هو جهاز إلكتروني صغير يُستخدم لاستقبال الرسائل النصية أو الإشعارات دون الحاجة إلى اتصال بالإنترنت. وكان يُستخدم بشكل شائع في التسعينيات وبداية الألفية كوسيلة أساسية للتواصل قبل أن تصبح الهواتف المحمولة متاحة على نطاق واسع.

وتعتمد أجهزة "البيجر" على استقبال إشارات راديوية رقمية من شبكة الاتصالات، وهذه الإشارات تحتوي على معلومات مثل النصوص أو التنبيهات، التي يتم فك تشفيرها وعرضها على شاشة "البيجر"؛ إذ يمكن للأخير عرض الرسائل النصية أو الإشعارات القصيرة، وفي بعض النماذج يمكن للمستخدمين الرد على الرسائل أو الاتصال برقم محدد.

ويستخدم عناصر حزب الله اللبناني أجهزة "البيجر" في التواصل فيما بينهم عبر الرسائل، معتقدين أنهم سيتمكنون من تجنب تعقب إسرائيل لمواقعهم الجغرافية؛ لأن هذه الأجهزة لا تتطلب إنترنت أو شبكة لاسلكية، ولا تستخدم بيانات تحديد الموقع الجغرافي؛ مما يجعلها آمنة نسبياً مقارنة بالهواتف الذكية.

:أهم الاستخدامات

على الرغم من أن استخدام "البيجر" قد تراجع بشكل كبير مع ظهور الهواتف الذكية؛ فإنه لا يزال يُستخدم في بعض المجالات المتخصصة، مثل: المستشفيات والمرافق الصحية ومراكز التسوق وأحياناً في الجولات السياحية في الصحراء، حيث يُستخدم للحصول على إشعارات سريعة وموثوقة، وذلك كما هو موضح في التالي:

المجال الطبي والرعاية الصحية: يُستخدم "البيجر" على نطاق 1- واسع في المستشفيات؛ لأنه يوفر وسيلة موثوقة وسريعة لإرسال الإشعارات للطواقم الطبية. ويُفضل في بعض الأحيان على الهواتف المحمولة؛ لأنه لا يعتمد على شبكة الإنترنت أو إشارات الهاتف المحمول التي قد تكون غير مستقرة في بعض الأماكن داخل المستشفى. كما تُستخدم هذه الأجهزة في حالة الطوارئ لإبلاغ الأطباء والممرضين والمسعفين بالتحرك السريع؛ إذ يمكن أن تكون الإشعارات الفورية حاسمة لإنقاذ الأرواح.

خدمات الطوارئ والإنقاذ: تستخدم بعض فرق الإطفاء والشرطة أجهزة 2- "البيجر" لتنبيه فرق العمل حول الحوادث والمهام الطارئة؛ لأنها تعمل بشكل موثوق في البيئات التي قد تكون فيها إشارات الهواتف المحمولة ضعيفة أو غير متوفرة.

الصناعات الخطرة والمواقع الصناعية: تُستخدم أجهزة "البيجر" 3- في البيئات الصناعية، حيث قد يكون من غير الآمن استخدام الهواتف المحمولة أو الشبكات اللاسلكية؛ بسبب التداخل أو المخاطر الأمنية، فيما توفر "البيجر" وسيلة تواصل آمنة وفعالة في مثل هذه البيئات.

البيئات ذات الحساسية العالية: في بعض البيئات، مثل: 4- المختبرات أو المناطق ذات الحساسية العالية للإشعاعات الكهرومغناطيسية، يمكن استخدام أجهزة "البيجر" لأنها لا تصدر إشارات قوية مثل الهواتف المحمولة.

التحكم الصناعي والتكنولوجيا: تُستخدم أجهزة "البيجر" لتنبيه 5-

المشغلين والفنيين بأي أعطال أو تحذيرات في الأنظمة الصناعية أو البنية التحتية التكنولوجية؛ إذ تعمل بشكل فعال على نقل الرسائل المهمة.

خدمات الأمن والحراسة: تعتمد بعض شركات الأمن على "البيجر" -6 لإرسال التنبيهات السريعة إلى موظفي الحراسة والمراقبة.

أشهر المصنعين:

كانت أجهزة "البيجر" تُصنع في الأساس من قِبل العديد من الشركات التكنولوجية الكبرى خلال فترة ذروتها في الثمانينيات والتسعينيات. ومن بين أبرز المصنعين لتلك الأجهزة ما يلي:

- **Motorola:** كانت شركة "موتورولا" واحدة من أكبر الشركات المصنعة لأجهزة "البيجر". وأطلقت العديد من الطرازات الشهيرة، وكان لها تأثير كبير في سوق "البيجر" العالمية.

- **NEC:** هذه الشركة اليابانية كانت أيضاً من المصنعين الرئيسيين لأجهزة "البيجر"؛ إذ قدمت منتجات متطورة خلال تلك الفترة.

- **Philips:** كانت شركة "فيليبس" جزءاً من سوق إنتاج أجهزة "البيجر".

- **Unication:** كانت من بين الشركات التي استمرت في تصنيع أجهزة "البيجر" لفترة طويلة وتخصصت في توفير حلول الاتصالات اللاسلكية.

- **Jensen:** قدمت هذه الشركة بعض الطرازات الشهيرة من أجهزة "البيجر".

- **Gold Apollo:** هي شركة تايوانية، متخصصة في إنتاج أجهزة "البيجر" وغيرها من معدات الاتصال، تأسست عام 1980، وركزت على تقديم حلول الاتصال اللاسلكية التي كانت شائعة الاستخدام قبل انتشار الهواتف المحمولة.

سيناريو هان للتفجير:

تعددت الروايات الواردة حول سبب انفجار أجهزة "البيجر" في لبنان، ومنها الآتي:

سيناريو زرع كمية صغيرة من المتفجرات أو شرائح تفجيرية محفزة -1 (Gold) في أجهزة كانت مخصصة لحزب الله قبل أشهر، وصنعتها شركة

التايوانية، والتي نفى مسؤول فيها أن تكون هي المصنع (Apollo) المباشر لتلك الأجهزة، قائلاً إن إحدى الشركات الأوروبية التي لديها الحق في استخدام العلامة التجارية "أبولو" هي من قامت بتصنيعها. ومقرها المجر (BAC) وأشارت تقارير إعلامية إلى أنها شركة

وبالنظر إلى مدى احتمالية هذا السيناريو والتهم الموجهة لإسرائيل؛ فإنها ليست المرة الأولى التي تقوم فيها إسرائيل بعمليات اغتيال عبر الهواتف المفخخة، فقد سبق أن استخدمت هاتفاً مفخخاً في اغتيال القيادي في حركة حماس يحيى عياش عام 1996؛ إذ نجحت حينها المخابرات الإسرائيلية في إيصال هاتف محمول مفخخ إلى عياش، وعند استخدامه تعرفت المخابرات الإسرائيلية على صوته وقامت بتفجير الهاتف عن بُعد أثناء استخدامه؛ مما أدى إلى مقتله.

وبالنظر إلى حجم وطبيعة الإصابات التي تعرض لها عناصر حزب الله اللبناني، والتي منها فقدان الأطراف أو جروح غائرة، وتاريخ إسرائيل في استخدام الهواتف المفخخة؛ فقد يكون هذا السيناريو وارداً بصورة كبيرة؛ مما يجعل منه أكبر عملية استهداف مباشر يتم تنفيذها عن بُعد، معروفة حتى الآن.

سيناريو تحفيز بطاريات الليثيوم الموجودة داخل أجهزة 2- "البيجر"؛ مما يؤدي إلى زيادة التحميل عليها وتفجيرها، ولكن كيف تم تحفيز هذه البطاريات حتى تصبح قابلاً موقوتة؟ في هذه الحالة: تتعدد الاحتمالات الواردة ومنها مثلاً ما يلي:

أ- أن خادم "البيجر" الذي يتم ربط معظم هذه الأجهزة عليه قد تم اختراقه عبر ثغرة، مما أدى إلى الوصول إلى جميع الأجهزة المتصلة بهذا الخادم، وتثبيت دودة خبيثة على هذه الأجهزة قامت بعمل تحميل زائد عليها تسبب في ارتفاع حرارة بطارية الليثيوم وانفجارها.

ب- أن هذه الأجهزة استقبلت ترددات عالية الشدة من طائرات من دون طيار قريبة من المنطقة، قامت بإرسال هذه الترددات إلى الأجهزة بعد كشف شفرتها؛ مما أدى إلى ارتفاع درجة حرارة البطارية بصورة كبيرة وانفجارها.

يمكن (Back Door) ج- قد تحتوي أجهزة "البيجر" على أبواب خلفية اللجوء إليها وتوظيفها بصورة تؤدي إلى انفجار بطارية الأجهزة.

د- من الوارد أيضاً أن تكون إسرائيل قد نجحت في اختراق سلسل التوريد الخاصة بتصنيع "البيجر"، وفي استبدال البطاريات الأصلية

. بأخرى تحتوي على مواد متفجرة .

لكن من التجارب السابقة، فإن انفجار بطاريات الليثيوم بقوة تؤدي إلى مثل هذه الإصابات أو قريبة منها؛ يتطلب أن تكون مشحونة بالكامل، أما البطاريات غير المشحونة كاملاً فهي لا تنفجر بقدر ما تحترق وتصدر منها غازات ودخان، وليس انفجاراً . وبالنظر إلى طبيعة الإصابات في لبنان؛ فإن سيناريو تفخيخ أجهزة "البيجر" بشرائح مُحفزة للتفجير أو بكميات من المتفجرات تعمل فيه بطاريات الليثيوم كعامل مساعد يُعد هو السيناريو المُحتمل .

وقد يكون كلا السيناريوهين؛ أي أنه تم اختراق أجهزة "البيجر" وتفخيخها معاً . فحسب الشهود، هذه الأجهزة قامت بإعطاء إشارات قبل الانفجار، حتى تخدع عناصر حزب الله ويمسكون بها في أيديهم؛ محققة أكبر قدر من الإصابات المؤثرة. أو قد يكون هذا الرنين هو أصلاً كود التفجير الذي تم إرساله إلى أجهزة "البيجر" حتى تبدأ عملية تحفيز البطارية تمهيداً لتفجير الشحنة المفخخة، مما يضع احتمالية أنه على الأقل تم اختراق الترددات التي تعمل عليها هذه الأجهزة قبل تفجيرها، أو حتى اختراق الأجهزة نفسها مسبقاً أثناء وضع الشحنة .المفجرة فيها .

وعلى الرغم من راحة هذا السيناريو؛ فإنه من الممكن أيضاً أن تكون إسرائيل طورت تقنية مشابهة لدودة "ستاكس نت" وتسببت في تفجير أجهزة "البيجر"؛ إذ إنها نجحت بالتعاون مع وكالة الأمن القومي الأمريكي في تطوير دودة خبيثة تم زرعها في شبكة الكمبيوتر الخاصة بمنشأة "نطنز" النووية في عامي 2009/2010، وتسببت هذه الدودة في تدمير ما يقرب من ألف من أجهزة الطرد المركزي المُستخدمة في تخصيب اليورانيوم، وعملت هذه الدودة على إغلاق صمامات التنفيس الخاصة بأجهزة الطرد مسببة انفجارها؛ ومن ثم يبقى السؤال؛ هل من الوارد أن إسرائيل طورت تقنية مشابهة لتقنية "ستاكس نت" التي كانت موجودة منذ أكثر من 15 عاماً واستخدمتها في تفجيرات "البيجر"؟

:مخاطر كارثية

تفتح هذه التفجيرات غير المسبوقة آفاقاً كبيرة للتفكير في سيناريوهات كارثية، ربما قد يصبح فيها كل شيء يعتمد على التكنولوجيا في حياتنا سلاحاً؛ فالهواتف الذكية والساعات الذكية وأجهزة "التابلت" وأجهزة الكمبيوتر المحمولة وألعاب الأطفال مثل

“السكوتر”، تعتمد كلها على بطاريات الليثيوم؛ مما قد يجعلها أسلحة موقوتة. كما تُعد السيارات التي تعتمد على الكهرباء بمثابة سيارات مفخخة مسبقاً، يمكن استخدامها في عمليات اغتيال أو تنفيذ هجمات إرهابية بطرق جديدة.

هذا بخلاف إمكانية اختراق أي جهاز يحتوي على كود أو برمجية رقمية مثل: مولدات الكهرباء ومحطات تحلية المياه والسدود ونظم المواصلات وغيرها من مرافق البنية التحتية، والتسبب في خسائر مادية وبشرية فادحة؛ قد تنقل أساليب الحرب بين البشر إلى مرحلة جديدة من التدمير، فلا تفرق بين المدني والعسكري وبين الكبير والصغير.

د. ايهاب خليفة - رئيس وحدة التطوير التكنولوجي

مركز المستقبل للأبحاث والدراسات