بعد تفجيرات البيجر: كم من الشركات في الغرب يحركها الموساد في مجال آليات وبرامج التشفير للتواصل؟

قامت إسرائيل بتفجير أجهزة المناداة «البيجر» يوم الثلاثاء ثم ووكي توكي يوم الأربعاء من الأسبوع الجاري وتسببت في جرح الآلاف ومقتل العشرات، ما يطرح علامات استفهام وشكوك كبيرة على الأجهزة والبرامج الرقمية المستعملة في الاتصال، ثم كم من شركة تجسس إسرائيلية تختبئ وراء شركات في دول ثالثة. في الوقت نفسه، هل ستؤدي هذه التطورات إلى الرهان على برامج بديلة مثلما يحدث في السلاح؟ وفي كل الحروب ومنذ القدم، تعمد الجيوش إلى ضرب أدوات التواصل بين مختلف مكونات جيش العدو بهدف ضرب التنسيق بين الوحدات، ما يعجّل بهزيمة العدو. ويدخل تنفيذ عمليتي إسرائيل يومي الثلاثاء والأربعاء في هذه الخانة، أي تصفية استباقية لما أمكن من القادة السياسيين والعسكريين لإضعاف حزب الله وزرع الرعب وغياب الثقة في القواعد، غير أنها أخطأت التقدير بسبب عدم سقوط قيادات كبرى في حزب الله خلال العمليتين بل غالبية الضحايا من المدنيين خاصة المنتمين إلى حزب الله.

وتعتبر عملية تفجير أجهزة الاتصال مثل «البيجر» معقدة، وتنقل جريدة «يديعوت أحرونوت» استنادا إلى مصادر استخبارية أمريكية أن إسرائيل خططت على مدى 15 عاما لعملية تفجير أجهزة المناداة «البيجر» السريعة. من جهة أخرى، تنفي تايوان أن تكون مصدر البيجر، والأمر نفسه مع بلغاريا بعدما أشيع استيراد هذه الأجهزة من هذا البلد الأوروبي. كما تنفي اليابان تصدير ووكي توكي المستعمل يوم الأربعاء في التفجير. ولا يمكن استبعاد عدم علم اليابان وبلغاريا باستعمال أراضيهما لعمليات مثل هذه بحكم مناورات الموساد في العالم في إنشاء شركات كثيرة كواجهة للعمليات الاستخباراتية المعقدة. ورغم كل هذا، يبقى غياب الحذر في شراء هذه الأجهزة والبرامج المستعملة فيها من مسؤولية خبراء حزب الله الذين لم يكونوا أذكياء في هذا الشأن، وهم العارفون بمدى مناورات الموساد في ملف أجهزة الاتصالات وبرامج التواصل عالميا.
ومنذ تأسيسه ومثل باقي الاستخبارات وخاصة التابعة للدول الكبرى،

يسعى الموساد إلى محاولة السيطرة والتلاعب بأجهزة الاتصال لأنها طريقة فعالة للحصول على المعلومات وأشد المعلومات سرية. لهذا تستثمر الاستخبارات في الشركات الواجهة الخاصة بالتشفير وبيع معدات الاتصال وبرامج التواصل المجانية في محاولة لخداع المنافس والعدو في حالة استعمالها. ولعل من أكبر عملية تجسس في القرن العشرين بعد الحرب العالمية الثانية هي التي تتعلق باختراق المخابرات الألمانية والأمريكية ودور للموساد لشركة «كريبتو» السويسرية، التي كانت تبيع برامج وآلات التشفير لـ120 حكومة في العالم على مدى عقود، ومن ضمن الدول التي استخدمت آلات كريبتو إيران وباكستان وجميع الدول العربية. اعتقدت الدول أن مراسلاتها آمنة ومشفرة، لتنفجر الفضيحة سنة 2020 بأن كريبتو كانت تعمل بتنسيق مع المخابرات الأمريكية التي كانت تطلع على مضامين الرسائل المشفرة وتزود الموساد بكل ما يتعلق بالشرق الأوسط.

وعلى ضوء هذا، كم من الشركات التي أنشأها الموساد في عدد من مناطق العالم أوهمت دولا وهيئات وخبراء بأنها توفر السرية في الاتصالات؟ في هذا الصدد، وعلاوة على الخداع في الأجهزة، تعتبر إسرائيل من الدول الرئيسية التي تتلاعب ببرامج الاتصال وبرامج التي أصبحت ضرورية لحماية البيانات في شبكة VPN التشفير مثل الإنترنت، وكذلك الشركات التي تقدم خدمات البريد الإلكتروني الآمن. وعادة ما يتجنب الكثير من الخبراء استعمال خدمات البريد المشفر لشركات في سويسرا وإيسلندا لأن الدولتين توفران الأمن السيبراني وتحترمان الخصوصية ولا يوجد تخوف من وجود استخبارات وراءها مثل حالة كريبتو. وفي المقابل، يراهنون على خدمات البريد الإلكتروني العادي مثل جيميل وياهو وهوتميل مع تطبيق برامج مشفرة خاصة بهم. في الوقت ذاته، تدرك بعض الدول مدى تورط إسرائيل في هذه الممارسات، لهذا أنشأت ما يسمى قاموس لغة خاصة بها يستعمل القنوات العادية في التواصل ولكن تكون عملية فك معاني الكلمات صعبة للغاية، ويبقى الأسلوب الأنجع رغم أنه الأقدم في التجسس.

وفي الوقت الذاته، تحاول إسرائيل السيطرة على برامج التواصل، وكان تالمون ماركو الذي عمل في وحدة الاستخبارات العسكرية الإسرائيلية هو الذي أنشأ برنامج «فيبر» الذي كان الأكثر استعمالا في العالم قبل واتسآب وتلغرام. وساور الكثير من الدول القلق من خطورة البرنامج بسبب ارتباطه بإسرائيل. وكانت أصوات كثيرة قد طالبت بعدم استعمال فيبر. وعندما تخلت أغلبية العالم عن استعمال فيبر لصالح واتسآب ثم تلغرام، لجأت إسرائيل إلى اختراع برامج التجسس المتطورة على شاكلة بيغاسوس لاختراق هواتف رؤساء دول وحكومات وصحافيين وحقوقيين وقادة عسكريين بحكم عدم تحكمها في

برامج مثل واتسآب وسينيال وتلغرام.
ونظرا للخطورة التي بدأت تشكلها هذه البرامج في الحروب السيبرانية خاصة في رصد واغتيال السياسيين والمقاومين مثل حالة فلسطين ولبنان، بدأ الرهان المحتشم على أجهزة وبرامج تواصل من إنتاج الصين وروسيا. ومن أبرز هذه البرامج تلغرام وهو الوحيد الذي يعتقد أنه لا تستطيع المخابرات الغربية الوصول إلى مضمونه، عكس الأخرى الأمريكية مثل سينيال وواتسآب، حيث توجد اتفاقيات سرية بين هذه الشركات والاستخبارات الغربية، للتعاون تحت مسميات شتى ومنها «حماية الأمن القومي الأمريكي». كما أن تلغرام عكس باقي البرامج، يتميز بخاصيات منها التشفير القوي للدردشات السرية، وحجم التخزين وقنوات التواصل الجماعية. وعلى ضوء هذا، يجب فهم اعتقال ثم الإفراج في فرنسا عن مخترع تلغرام بافيل دوروف نهاية شهر آب/أغسطس الماضي.
ومن باب المقارنة، وعت الكثير من الدول ومنها العربية مدى تحكم الغرب في الأسلحة التي تشتريها، وكيف لا يمكن استعمالها مثلا في مهاجمة إسرائيل. ولهذا، بدأت دول مثل السعودية ومصر تفكر في السلاح الروسي. وما يحدث في مجال الأسلحة يحدث في مجال التواصل والاتصالات، لأن جيوشا واستخبارات بدون أجهزة تواصل وبرامج اتصالات آمنة تخسر المعارك قبل بدايتها.

حسين مجدوبي

صحيفة القدس العربي