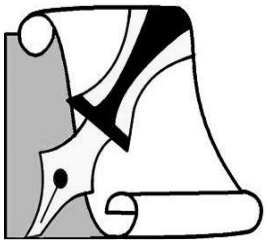
مركز باحث للدراسات الفلسطينية والاستراتيجية

التقدير نصف الشهري

تحليل للتطورات السياسية والأمنية في «إسرائيل»

www.bahethcenter.net
Email: baheth@bahethcenter.net
bahethcenter@hotmail.com



باحث للدراسات
الفلسطينية والاستراتيجية

تحليل نصف شهري للتطوّرات السياسية والأمنية في «إسرائيل»

أهداف المركز الرئيسية:

1. إعادة فلسطين إلى موقعها الحقيقي كقضية مركزية للأمة.
2. الترويج للقيم الجهادية والنضالية في إطار استراتيجية تحرير فلسطين.
3. بناء علاقة متينة مع النخب والشخصيات المعنية بالقضية الفلسطينية.
4. إصدار دراسات وأبحاث وتقارير ذات بعد استراتيجي وتحليلي.

"بيغاسوس": أكبر فضيحة تجسس إسرائيلية

1 – مدخل:

كشف تحقيق استقصائي أجرته مؤسسة "فوربيدن ستوري" و"أمنستي إنترناشنال" بالتنسيق مع 17 وسيلة إعلام دولية، عن فضيحة تجسس عالمية بواسطة برنامج "بيغاسوس" الإسرائيلي. وشملت فضيحة التجسس هذه التجسس على مسؤولي الدول والحقوقيين والصحافيين ورجال أعمال. ويتم توجيه الاتهام إلى عدد من أجهزة الاستخبارات في الدول التي حصلت على البرنامج الإسرائيلي ومنها المغرب والمكسيك والهند والإمارات والسعودية. وكان الحديث في البدء عن صحافيين ونشطاء في مجال حقوق الإنسان، لاسيما وأن اللائحة الأولى التي سربتها "واتس آب" سنة 2019 وأبلغت مئة شخص بتعرض هواتفهم للتجسس كانت تضم نشطاء حقوق الإنسان وصحافيين من المغرب والإمارات والمكسيك وإسبانيا، لكن هذه المرة تفاقم الملف حيث تم التجسس على 50 ألف هاتف، وتم اختراق البعض منها ولم يتم النجاح في التسلل إلى أخرى. والمفاجأة الكبرى هي أن لائحة الشخصيات المتجسس عليها تضم، وفق جريدة "لوموند" الفرنسية، مسؤولين كبارا على رأسهم ملك المغرب محمد السادس والرئيس الفرنسي إيمانويل ماكرون، ورئيس جنوب إفريقيا والرئيس العراقي. كما جرى الكشف عن تعرض رؤساء حكومات ما يزالون في مناصبهم للتجسس، بينهم رئيس الحكومة المغربية سعد الدين العثماني، ورئيس حكومة مصر مصطفى كمال مدبولي. كما تعرض رؤساء حكومات سابقون للتجسس بواسطة بيغاسوس، وهم اللبناني سعد الحريري واليمني أحمد بن ظاهر والبلجيكي شارل ميشيل والفرنسي إدوارد فيليب والأوغندي روكهانا روغوندا. وفي إسبانيا، ذكرت صحيفة "البايس" اليومية الوطنية أن الحكومة الإسبانية ربما استخدمت برنامج "بيغاسوس" للتجسس على 4 انفصاليين كتالونيين بارزين. ونشرت مؤسسة NSO الاسرائيلية صانعة الجهاز بيانا تنفي فيه استهداف هاتف الملك محمد السادس والرئيس الفرنسي إيمانويل ماكرون، ونفت الحكومة المغربية في بيان لها استعمال هذا البرنامج أو شراءه. ومن شأن استهداف ملوك ورؤساء الدول والحكومات أن يترتب عليه تحقيق دولي وعقوبات ضد الدول التي

استهدفت أخرى، علما أن القضاء الأوروبي بدأ التحقيق في عملية التجسس هذه، بينما يطالب نواب من البرلمان وخاصة اليسار الذين جرى استهدافهم، بضرورة توسيع التحقيق ليكون أوروبيا أو دوليا.

لقد وصفت صحيفة "الغارديان" البريطانية برنامج "بيغاسوس" بأنه "أقوى برنامج تجسّس تمّ تطويره على الإطلاق من قبل شركة خاصّة اسرائيلية. وأنه بمجرد أن يتسلّل إلى هاتفك، يتحوّل إلى جهاز مراقبة يعمل على مدار 24 ساعة. يُمكنه نسخ الرسائل التي ترسلها أو تتلقّاها، وجمع صورك وتسجيل مكالماتك. كما تكمن مخاطره في أنه يستطيع تصويرك سرًا من خلال كاميرا هاتفك، أو يُشغّل الميكروفون لتسجيل محادثاتك. كما يمكنه تحديد مكانك الحالي، والمكان الذي كنت فيه، والأشخاص الذين قابلتهم.

2 – ما هو "بيغاسوس"؟

كلمة "بيغاسوس" تعني الجواد المجنح الابيض الجميل في الميثولوجيا الإغريقية، والاسم يأتي من التقليد المتأثر بالمخلوقات الهجينة مثل القنطور الذي هو تمثال نصفه رجل ونصفه الآخر حصان والفونوس – نصف إنسان ونصف ماعز وهكذا، لكن "بيغاسوس" الذي نحن بصدده هنا هو برنامج قرصنة أو تجسّس، طوّرته شركة "إن إس أو" الإسرائيلية، وسوّقت له ومنحت رخصة استخدامه لعدد من الحكومات في جميع أنحاء العالم.

يستطيع البرنامج اختراق مليارات الهواتف التي تعمل بأنظمة تشغيل "أي أو أس" (IOS)، و"أندرويد" (Android). والجدير بالذكر أن هذا النظام ليس الوحيد من نوعه في هذا المجال. إذ توجد غابة شاسعة لسوق التجسس الإلكتروني تختفي ايضاً تحت "شجرة" بيغاسوس الكبيرة، بحيث أن تمكن برنامج بيغاسوس من التنصت على المكالمات وقراءة رسائل تطبيق واتساب أو تليغرام والتقاط الصور من الجهاز المخترق وتحديد موقع الهاتف الذكي لا تعتبر قدرات استثنائية في سنة 2021.

في هذا الصدد، يوضح الخبير باستيان بوب أن ما يميز "علية القوم" في ميدان التجسس الرقمي هذا هو "قدرتها على أن تؤمَن إدخال برنامج التجسس في أجهزة الضحايا في سرية تامة". و بيغاسوس ينتمي إلى هذه الحفنة من برامج التجسس التي يمكن تفعيلها عن بعد من دون أي تدخل من الضحية. بعبارة أخرى، لا يحتاج الأمر لنقر الشخص المستهدف على رابط ما أو الدخول إلى موقع مضلل أو الرد على رسالة لكي يخترق

برنامج التجسس جهازه. لا يتطلب الأمر أكثر من إدخال رقم هاتف الشخص المستهدف بالتعقب على منصة للمراقبة عن بعد ومن ثم يتكفل بيغاسوس بالباقي. وتعتبر هذه القدرة على الاختراق في سرية تامة الميزة الأهم التي يقدمها "نجوم" التجسس الإلكتروني الخواص لزبائنهم.

إضافة إلى شركة "إن إس أو"، توجد شركات إسرائيلية أخرى إضافة إلى "شركة واحدة على الأقل في شمال أوروبا" قادرة على توفير المستوى نفسه من الخدمات، بحسب باستيان بوب الذي رفض كشف المزيد من التفاصيل بشأن هوية مسوقي الأسلحة الإلكترونية. وإذا ما كانت شركة "إن إس أو" الأكثر شهرة بين مزودي برامج التجسس، فإن ذلك يعود بالأساس إلى "امتلاكها أكبر عدد من الزبائن حول العالم والأكثر ترويجا علنيا لقدراتها"، بحسب رأي فيليب روندال الخبير في شركة "شاك بوينت". ويؤكد باستيان بوب ايضا أن هذه الشركة تمثل "الذراع الإلكترونية للدبلوماسية الإسرائيلية. ويضيف أنه عندما توقع الدولة العبرية اتفاقا مع دولة أخرى، يمكن أن يتضمن فصولا تتعلق بتزويد شركة "إن إس أو" مخابرات تلك الدولة ببرنامج التجسس الشهير. وهي طريقة تستخدمها الحكومة الإسرائيلية لتحقيق مكاسب سياسية من قطاع التجسس الإلكتروني الذي لا يمثل برنامجا بيغاسوس وكانديرو سوى جزء منه. وقد ساعد ترويج تكنولوجيا شركة إن إس أو "بالتأكيد في التوصل إلى اتفاقات لتطبيع العلاقات مع بعض الدول العربية" على غرار المغرب أو الامارات، بحسب تصريح الباحث في المعهد الإسرائيلي للأمن القومي يوؤيل غوغاسنكي لوكالة الأنباء الفرنسية.

3 – كيف يعمل البرنامج؟

عام 2016، اكتشف باحثون نسخة مبكّرة من "بيغاسوس" بعد أن اخترقت الهواتف من خلال ما يُسمّى "التصيّد بالرمح" (Spear Phishing)، القائم على استهداف شخصٍ محدّد وإرسال الرسائل النصّية أو رسائل البريد الإلكتروني التي تُغري المستخدم للنقر على رابط ضار. ومنذ ذلك الحين، تطوّرت قدرات شركة "أن.أس.أو" على شنّ هجمات بما يُعرف باسم "النقر الصفري"، والتي لا تتطلّب أي تفاعل من مالك الهاتف من أجل تحقيق النجاح. غالبًا ما تُستغلّ هذه الثغرات الأمنية في "يوم الصفر"، وهي عيوب أو أخطاء في نظام التشغيل لا تعلم الشركة المصنّعة للهاتف المحمول بوجودها، وبالتالي لم تتمكّن من إصلاحها.

في عام 2019، كشف تطبيق "واتساب" عن استخدام برنامج "إن إس أو" لإرسال برامج ضارّة إلى أكثر من 1400 هاتف من خلال استغلال ثغرة "يوم الصفر". وبإجراء مكالمة هاتفية من "واتساب"، يُمكن تثبيت رمز "بيغاسوس" الخبيث على الهاتف، حتى لو لم يرد المستخدم مطلقًا على المكالمة. وفي الآونة الأخيرة، بدأت شركة "إن إس أو" باستغلال الثغرات الأمنية في برنامج "آي مسج" من شركة "آبل"، للوصول إلى مئات الملايين من أجهزة "آيفون"، على الرغم من أن الشركة تقول إنها تقوم باستمرار بتحديث برامجها لمنع مثل هذه الهجمات. وشرح كلاوديو غوارنييري، الذي يُدير مختبر الأمن التابع لمنظمة العفو الدولية ومقره برلين، أن "الأمور أصبحت أكثر تعقيدًا بكثير بالنسبة للأهداف"، مشيرًا إلى أن عملاء الشركة تخلّوا عن الرسائل النصيّة المشبوهة لشنّ هجمات أكثر دقة بدون نقر. وأوضح أنه بالنسبة لشركات مثل "إن إس أو"، فإن استغلال البرامج المثبّتة على الأجهزة، مثل "آي مسج"، أو المُستخدمة على نطاق واسع مثل "واتساب"، أمر جذّاب لأنه يزيد من عدد الهواتف المحمولة التي يُمكن استهدافها بنجاح.

بصفة الشريك التقني لـ"مشروع بيغاسوس" (Pegasus Project)، اكتشف مختبر منظمة العفو الدولية، في تموز 2021 آثارًا لهجمات ناجحة من قبل عملاء "بيغاسوس" على أجهزة "آيفون" التي تعمل باصدارات محدثة من "آي أو أس". وأشار تحليل الأدلة الجنائية لهواتف الضحايا أن بحث "إن إس أو" المستمر عن نقاط الضعف ربما امتد ليشمل تطبيقات أخرى شائعة. وإذا لم تنجح هجمات "التصيّد بالرمح" أو هجمات "النقر الصفري"، يُمكن أيضًا تثبيت "بيغاسوس" عبر جهاز إرسال واستقبال لاسلكي يقع بالقرب من الهدف، أو يتمّ تثبيته يدويًا ببساطة إذا تمكّن العميل من سرقة هاتف الهدف. وبمجرد تثبيته على الهاتف، يمكن لبرنامج "بيغاسوس" جمع أي معلومات، أو استخراج أي ملف، وتسريب الرسائل النصيّة، والعناوين، وسجل المكالمات، والتقويمات، ورسائل البريد الإلكتروني، وتاريخ تصفّح الإنترنت. وقال غوارنييري: "عندما يتمّ اختراق جهاز آيفون، يتمّ ذلك بطريقة تسمح للمهاجم بالحصول على ما يسمى بامتيازات الجذر، أو الامتيازات الإدارية، على الجهاز. يمكن للشركة أن تفعل أكثر مما يمكن لمالك الجهاز القيام به". واستثمرت "إن إس أو" جهودًا كبيرة في جعل برمجياتها صعبة الاكتشاف. ويشكّ باحثو الأمن في أن الإصدارات الأحدث من "بيغاسوس" تُشغّل فقط الذاكرة المؤقتة للهاتف، بدلًا من محرّك الأقراص الثابتة، ما يعني أنه بمجرد إيقاف تشغيل الهاتف، يختفي كل أثر للبرنامج تقريبًا. وأحد أهم التحديات التي يطرحها برنامج "بيغاسوس" أمام الصحافيين والمدافعين عن

حقوق الإنسان، هو أن البرنامج يستغلّ نقاط الضعف غير المكتشفة، ما يعني أنه حتى مستخدم الهاتف المحمول الأكثر وعيًا بالأمان لا يمكنه منع الهجوم.

عادة هناك طرق معينة يمكن للشخص اكتشاف استهدافه، ولكن برنامج بيغاسوس لكونه برنامجا ذكيا جدا، فيصعب على شخص غير تقني أو مهندس كشفه. ففي برامج التجسس الرخيصة والتقليدية هناك مؤشرات معينة، مثل عمل ضوء كاميرا الهاتف في أوقات غير متوقعة، أو ارتفاع حرارة الجهاز بشكل أعلى من الطبيعي، أو استهلاك البطارية بسرعة أكبر أو تغير خلفية الشاشة، أو ظهور برامج جديدة بشكل مفاجئ، أو يتم استهلاك مساحة التخزين بشكل سريع. ولكن مع بيغاسوس المؤشرات التقنية يصعب على غير الخبير كشفها، لأن الاختراق الناجح، هو الاختراق الصامت الذي لا يمكن الكشف عنه. ولذلك لا يزال من غير الواضح عدد الأشخاص الذين تم اختراق أجهزتهم، رغم أن أحدث التقارير الإعلامية تقول إن هناك أكثر من 50 ألف رقم هاتف في بنك أهداف زبائن الشركة الإسرائيلية.

4– سوق ذو ربحية عالية:

تؤكد المعلومات التي كشفها كونسورتيوم "فوربيدن ستوريز" وجود طلب كبير على هذا النوع من البرامج التجسسية. إذ كان بحوزة شركة "إن إس أو" 30 زبونا حكوميا مستعدا لإنفاق الملايين من الدولارات لمكافحة الإرهاب أو للتجسس على الصحافيين وقادة الرأي. ويقول باستيان بوب في السياق: "إنه سوق متنام. هناك تزايد في عدد الناشطين فيه وفي أساليب التجسس المقترحة". وبالتالي، فإن من لا يقدرون على الحصول على خدمات الشركات الكبرى في هذا القطاع بإمكانهم التعامل مع شركات تعرض برامج تجسس لا تتطلب سوى تفاعل بسيط من الضحية وهو ما ينطبق على برنامج كانديرو.إذ يكفي أن يقوم صاحب الهاتف الذكي المستهدف بفتح رسالة أو رابط مفخخ. ويضيف الخبير في شركة شاك بوينت "إنها تكلف أموالا أقل بكثير وهناك العشرات من الشركات التي تبيع هذا النوع من الخدمات التي يبقى مستوى سريته أقل بقليل". ويعمل مرتزقة التجسس الإلكتروني الأقل كفاءة على تطوير أساليبهم شيئا فشيئا ما يعني أنه "من المرجح أن تكون هناك عشرات الشركات القادرة على عرض المستوى نفسه من خدمات "إن إس

أو" خلال الخمسة أعوام المقبلة" بحسب تقدير باستيان بوب. وهو ما يعني أن مخاطر برامج التجسس – المتاحة لأجهزة الاستخبارات الحكومية فقط– هذه سيكون أكبر بكثير في حال حصول المجرمين الرقميين عليها. ويلاحظ فيليب روندال أنه "في معظم الأحيان، ينتهي الأمر بالأسلحة الإلكترونية التي تستخدمها الدول بعرضها للبيع في السوق السوداء للجرائم الإلكترونية".

وهو ما جعل بيير ديلشر من شركة "كاسبرسكي" يعتبر أنه من الضرورة زيادة "تقنين تجارة واستغلال هذه البرامج لضمان رقابة أكبر على القطاع". فمن يعلم حجم الأضرار التي يمكن أن يحدثها محترفو الجرائم الإلكترونية في حال استحواذهم على برنامج من حجم بيغاسوس القادر على الحصول على معطيات شخصية من أي هاتف في كنف السرية المطلقة.

لقد تعرّضت هواتف ناشطين حقوقيين وصحفيين ومحامين حول العالم للاستهداف عبر برنامج التجسس الاسرائيلي الذي باعته شركة NSO لحكومات سلطوية، بحسب ما أفادت به تقارير إعلامية. وأشارت التقارير إلى قائمة تضم قرابة 50 ألف رقم هاتف لشخصيات محلّ اهتمام من جانب عملاء لشركة "إن إس أو" الإسرائيلية. ولم تحدد التقارير مصدر القائمة ولا هويات جميع الشخصيات التي تعرضت هواتفها للاختراق. وتنكر شركة "إن إس أو" القيام بأية انتهاكات، وتقول إن البرنامج صُمم لاستهداف المجرمين والإرهابيين، وإنه لا يقدَّم لغير المؤسسات الاستخباراتية والعسكرية والمعنية بإنفاذ القانون في دول ذات سجلات جيدة في مجال حقوق الإنسان. وأضافت الشركة في بيان لها أن التحقيق الأصلي الذي استندت إليه التقارير، وقامت به منظمة "فوربيدن ستوريز" غير الحكومية من باريس، ومنظمة العفو الدولية المعنية بحقوق الإنسان، كان "مليئا بفرضيات خاطئة ونظريات غير موثقة".

بيغاسوس باهظ الثمن، ووفقاً لأسعار 2016، فإن اختراق عشرة أجهزة يكلّف 650 ألف دولار، إضافة إلى نصف مليون دولار رسوم تثبيت البرنامج، وهي مبالغ تُدفع بسخاء من قبل الأنظمة الديكتاتورية العربية؛ من أجل ملاحقة المعارضين السياسيين والنشطاء الحقوقيين، فهي دول تملك المال ولا تملك الحق ولا المعرفة، وسبق للاحتلال أن تاجر عبر جهاز الموساد في عمليات ومهارات استخباراتية لجماعات إرهابية ودول ديكتاتورية، في حين ترفض الدول الديمقراطية أن تشتري أو تبيع مثل هذه البرامج، فكل دولة تجتهد بتصنيع مثل هذه البرامج لاستخداماتها الرسمية، ضمن بروتوكول أخلاقي وقانوني، ويُخضع للرقابة التشريعية. وتشير

كثرة العملاء المستفيدين من البرنامج، وكذلك كثرة المستهدفين وتعدد مواقعهم وصفاتهم، إلى استثمار الاحتلال لهذه الفوضى –التي هي تحت سيطرتها– لمراقبة قادة سياسيين ورجال أعمال وصحفيين ورؤساء دول، في خطوة خبيثة لاستدراجهم في شَرَك التعاون الإجباري مع السياسة الإسرائيلية، وكلٌ حسب موقعه ومستواه. وأفادت وثائق استخبارات في السابق بوقوع صحفيين ووزراء وبعض الرؤساء في وحل التخابر الأمني مع الاحتلال.

عندما يستخدم البرنامج من قبل طغاة بصفة حاكم أو مسؤول، فإن النتيجة الحتمية هي اعتقال المستهدف إن لم يكن قتله وتصفيته، وهو ما أكده خبير الاستخبارات الإسرائيلي "يوسي ميلمان" بأن "الاختراق قد ينتهي بعملية قتل كما كان الأمر بالنسبة للصحفي السعودي جمال خاشقجي"، حيث أكدت المعلومات أن هاتف صديق مقرب لـ"خاشقجي" وهاتف خطيبته التركية خديجة جنكيز اخترقا ببرنامج "بيغاسوس"، وقال إدوارد سنودن – الموظف السابق في وكالة الأمن القومي الأمريكية، والملاحق قضائيًّا في بلاده بتهمة تسريب معلومات سرية– أن شركة "NSO" الإسرائيلية ساعدت السعودية على تعقب وقتل الصحفي جمال خاشقجي.

الخلاصة هي أن كيان الاحتلال هو مصدر التجسس التجاري في العالم، وأن المال العربي –للأسف– بات مصدر للاستثمار الإسرائيلي، وأن المواطن العربي الرافض للخنوع هو المستهدف دائماً، وأصبح من الواجب على كل من يعمل في دوائر الاستنهاض للأمة، أن يحذر من استخدام الهواتف الذكية في أنشطتهم، وعدم احتفاظ تلك الهواتف لأي مادة تعرضه للابتزاز، هو أو أيٍّ من أفراد أسرته، أو جماعته. وتجدر الاشارة هنا الى ما تقوم به المقاومة الفلسطينية من عدم استخدام عناصرها لتلك الهواتف، وأنها تتواصل في أنشطتها عبر خطوط هواتف سلكية خاصة، أحيطت بالسرية والكتمان، وهي استراتيجية اعتمدتها المقاومة لإحباط التفوق التكنولوجي الإسرائيلي في المراقبة والتنصت.

5 – إسرائيل في خدمة القمع:

إن اتساع دائرة المستهدفين ببرنامج "بيغاسوس" للتجسس، من المكسيك إلى الهند، يعيد إلى الواجهة الأدوار التاريخية الدموية لتحالف الاحتلال الإسرائيلي مع المستبدين حول العالم. وبالنسبة للبعض، الأمر ليس مفاجئاً، فأدوات وأصابع تل أبيب كانت حاضرة دوماً في هذا الإطار؛ من دعم ديكتاتوريات أميركا اللاتينية

وضرب حركات التحرر، إلى التحالف الوثيق مع نظام الأبرتهايد (الفصل العنصري) السابق في جنوب أفريقيا، إلى اغتيالات "الموساد" لفلسطينيين وعرب، من أوسلو إلى اليونان ومالطا والامارات، بتغطية أمنية وسياسية في أوروبا.

الجديد في الأمر أن تطور الاتصالات يفضح أكثر الوجه الخفي للصهيونية في علاقاتها العالمية المشبوهة، المتخفي خلف مزاعم "التقدم" و"الديمقراطية الوحيدة في المنطقة"، وهو ما كشفه، في أكثر من مناسبة، الباحث الراحل المعادي للصهيونية، إسرائيل شاحاك.

إن تدفق المعلومات يضع قادة الاحتلال أمام معضلة، فيسارعون إلى تشكيل "لجان" لفحص ما جرى، والأرجح لكيفية انكشاف برنامجهم الخبيث "بيغاسوس"، وربما لإدراكهم أن "تابو" عدم المسّ بكيانهم يكاد يكسر قوالبه النمطية. ولأن الأمر تجاوز المنطقة العربية، التي تسربت منها منذ أعوام، أخبار استخدام تقنيات الاحتلال للقمع، فلعل هذه "الفضيحة" ستأخذ أبعاداً أخرى مستقبلاً. فأوروبا تجد نفسها أمام استحقاق مهم، بعد كشف صحافتها عن استخدام رئيس وزراء المجر القومي المحافظ، فيكتور أوربان، البرنامج لاستهداف 300 شخصية صحافية وحقوقية وسياسية، وربما في دول أخرى، ما يعني الدوس عملياً على كل القيم والمبادئ التي يبشر بها الاتحاد الأوروبي.

مع توسّع الفضيحة، لم يعد لسردية "معاداة السامية"، وخصوصاً بعد أن صارت أيادي تل أبيب ملطخة بدماء كثيرة تتجاوز فلسطين المحتلة، المقدرة السابقة ذاتها على تكميم الأفواه؛ لا الحقوقية ولا الأكاديمية ولا الإعلامية على الأقل، مما يشكل فرصة أخرى لإعادة تصويب الأسئلة عن إفلات المجرمين الصهاينة المنتهكين لحقوق الإنسان من العقاب. صحيح أنه سياسياً قد تتدخل المصالح لحماية مرتكبي الفظائع، لكن هذه التدخلات في المقابل ستفضح من يغطيها في الغرب، وكذلك من يهرول في المنطقة نحو التحالف مع الاحتلال بحجة "تفوقه التقني"، متناسياً قتله بنفسه لكل تفوّق عربي بالتنكيل والتهجير، وقبوله المذل لشعار "الديمقراطية الوحيدة"، وسط دعم وتفضيل الاحتلال له، لتكميم الأفواه وتوسيع الاضطهاد ولإغراق المنطقة في صراع البقاء بنشر الجوع، بعد عقود من بناء الدول الحديثة. وفي كل الأحوال، ان الكشف الجديد ربما يزيد أيضاً من قراءة الرأي العام العالمي، للاحتلال الإسرائيلي، بكثير من التشبيه بأعتى الأنظمة ظلامية وعنصرية وقمعية في العالم. وفي السياق يقول مصطفى السعيد في صحيفة "الأهرام" المصرية إن "فضيحة التجسس

الإسرائيلية تهز العالم"، وهو قارنها " بفضيحة ووترغيت التي تسببت في استقالة الرئيس الأمريكي الاسبق ريتشارد نيكسون، بعد اكتشاف ضلوعه في التجسس على الحزب الديمقراطي المنافس عام 1972". ويتابع: "الفضيحة الجديدة أكثر عمومية، وإن كانت بالتأكيد ذات مغزى سياسي، لكن الأهم أنها ستكون ظاهرة أخطر وأكثر شيوعاً، وواحدة من ثمار تطور الحروب السيبرانية، ونتاج سرعة وتعقيدات برامج التجسس التي ستجعل البشر منزوعي الخصوصية... لكن ما يثير المخاوف ألا يقتصر الأمر على حروب بين الدول، وأن يصبح عدد هائل من البشر ضحية لتلك العمليات، وأن تنتشر هذه البرامج لتصبح كابوساً شخصياً للكثيرين حول العالم".

من جانب آخر يقول عبد الباري عطوان في "رأي اليوم" اللندنية: "ليس من قبيل الصّدفة أن تكون الحُكومات العربيّة التي وقّعت اتّفاقات سلام أبراهام في الأشهر الأخيرة، هي الأكثر تَورُّطًا في فضيحة بيغاسوس التي تَهُزّ العالم حالياً، لما تَكشِف عنه من أعمال تجسّس على أكثر من 50 ألف هاتف لصِحافيين ومُعارضين سياسيين، بل وملوك ورؤساء وِزارات وشخصيّات عربيّة وعالميّة بارزة". ويضيف: " ربّما حصلت دول انخرطت في هذه العمليّات من خِلال شرائها هذه البرامج التّجسّسيّة من الشّركة الإسرائيليّة الأُم على بعض المعلومات عن مُعارضيها مِثل المملكة العربيّة السعوديّة والمغرب والإمارات والبحرين، وتحرّكاتهم، ولكن المُشَغِّل الإسرائيلي هو المُستفيد الاول والأكبر، لأنّه وبحسب المعلومات الأوّليّة، حصَل على كَمٍّ هائلٍ من الأسرار والمعلومات". وبالتالي فإن الشركة الإسرائيلية لن تلتزم الصمت طويلاً حول عقودها ومبيعاتها، فهي باتت تحت مجهر الرصد والتعقّب والتحليل، ولم يعد ينفع كثيراً أن تضحك على العقول بالقول إنّ تطبيقها يستهدف محاربة الإرهاب والجريمة وتسهيل عمل الأجهزة المعنية بإنفاذ القانون. والدول التي اشترت التطبيق واستخدمته هي في الورطة ذاتها مع الشركة الإسرائيلية.

6 – التوظيف الأمني:

لن ندخل في تحليل نوعية الأشخاص الذين جرت مراقبتهم عبر "بيغاسوس"، ولكن سنلفت إلى فكرة أن شركة "NSO" لا تبيع هذا البرنامج إلا بعد الحصول على تصديق لجنة أمنية إسرائيلية يرأسها وزير الأمن. من ناحية أخرى لا يمكن النظر إلى واقع العلاقات الإسرائيلية مع الممالك والإمارات الخليجية بوصفها نتيجة

لمستجدات طارئة تهدد وجود تلك الكيانات، فتعليل هذه العلاقات استناداً إلى الأخطار الخارجية التي تمثلت بنظام صدام حسين سابقاً، و"الخطر الإيراني" المزعوم حاضراً، ليس مقنعاً، بل إنه دليل على سطحية النظرية الوجودية التي يجهد العقل الاستراتيجي الخليجي لتسويقها منذ عدة سنوات.

لقد قدمت تسعينيات القرن الماضي شواهد عديدة على أن جذور هذه العلاقات ترتكز على ما يشبه الأيديولوجيا النفعية المبنية على أساس عدم الاقتناع بفكرة العداء العقائدي للكيان الإسرائيلي من جهة، وبإمكانية الاستفادة من إمكانيات هذا الكيان في عملية توطيد الأمن القومي للأنظمة الخليجية وتحصينها من جهة أخرى، فكان أن استغلت دول خليجية عديدة اتفاق "أوسلو" في العام 1994، لتخرج إلى العلن واقع وجود علاقات سرية سابقة، أو بالحد الأدنى وجود نية للاعتراف بهذا الكيان وتطبيع العلاقات معه. من ناحية أخرى، تتقاطع الممالك الخليجية مع بعضها البعض في موضوع البحث عن العدو الخارجي الضروري لوجودها، بسبب قصور الوسائل الدستورية القادرة على ضمان شرعية داخلية لها، وذلك بسبب طبيعة الأنظمة الملكية المطلقة فيها. وبعد أن كانت هذه الأنظمة مستفيدة من الغطاء الأميركي في فترة الحرب الباردة، وقادرة على فرض هيمنتها وقمع أيّ معارض لها تحت حجّة المدّ الشيوعي أو البعثي، وجدت، بعد الحرب الباردة، في الجمهورية الإسلامية ضالتها، إذ استغلّت إثارة الولايات المتحدة للملف النووي الإيراني، بعد الكشف عن الموقعين السريين في نطنز وأراك، وتحوّل الملف إلى مجلس الأمن تحت عنوان تهديد السلم والأمن الدوليين، لتزرع في قلوب مواطنيها الرعب والخوف من إمكانية قيام الجمهورية الإسلامية بتهديد سيادتهم، فتثير عصبيتهم وتضمن تكاتفهم خلفها، بما يضمن استقراراً وثباتاً وقدرة على الاستمرار من دون الحاجة إلى أي تعديل ديمقراطي في مفاصلها. وإذا ربطنا بين فكرة العداء للجمهورية الإسلامية والخوف المصطنع من برنامجها النووي وبرنامجها البالستي من جهة، والأيديولوجيا النفعية المبنية على أساس عدم الإقتناع بالعداء للكيان الصهيوني وإمكانية الاستفادة من قدراته من جهة ثانية، يصبح مفهوماً ذلك التعاون الأمني والسيبراني بين الطرفين، ولا يعود مبرراً أي سبب للذهول أو المفاجأة لدينا.

منذ العام 2007، تكرّس التعاون الأمني بين الإمارات والكيان الإسرائيلي مبرَّراً بما أسموه "تهديدات عسكرية متزايدة من إيران ووكلائها"، إذ تعاقدت الإمارات مع شركة إسرائيلية أميركية لتطوير دفاعاتها الجوية حول مناطقها الحساسة، ثم ظهر إلى العلن سعي الرياض في العام 2012 للحصول على مساعدة الكيان في

عملية ملاحقة مسلحين وتعقّبهم في وسائل التواصل، إضافة إلى حاجتها إلى المساعدة في المجال السيبراني، لحماية منشآتها النفطية بعد الهجوم الكبير الذي استهدف داتا شركة "أرامكو". ولكنّ مشروع الممالك الخليجية لا يمكن حصره في الحاجة إلى التعاون من أجل الدفاع عن المنشآت الحيوية، أو تحصين داتا معلومات شركاتها النفطية، وإنما جرى العمل على استغلال هذه التكنولوجيا في عملية بناء المنظومة الأمنية التي أرادها ولي العهد السعودي محمد بن سلمان وشريكه الإماراتي محمد بن زايد أداة لتكريس الهيمنة الداخلية في بلدانهم، كوسيلة لتسهيل ارتقائهم إلى عرش دولهم ورئاستها، إضافة إلى المشروع الأكثر خطورة وجرأة، والمتمثل بمراقبة الحلفاء والخصوم، من رؤساء وسياسيين وإعلاميين وغير ذلك. وإذا كانت الدول الخليجية والمغرب قد استطاعت الوصول إلى هذا البرنامج، فإن هذا الأمر لم يكن ليتم لو كانوا يصنفون كتهديد من قبل وزارة الأمن الإسرائيلية. وعليه، يصبح لزاماً التركيز على نوعية العلاقة التي تجمع الكيان الإسرائيلي والممالك الخليجية.

بالطبع، يسوّق الخليجيون أن العلاقة الأمنية مع الكيان الإسرائيلي هي علاقة تكاملية عنوانها مصالح مشتركة وأساسها ما يسمونه "مواجهة الخطر الإيراني المشترك"، غير أن ما صرّح به وزير الأمن الإسرائيلي السابق أفيغدور ليبرمان لدى مشاركته في مؤتمر ميونخ الأخير للأمن يظهر عكس ذلك، إذ يعتقد أن "الدول العربية المعتدلة" وفق وصفه، بحاجة إلى "إسرائيل" بقدر أكبر من حاجة الأخيرة إليها. وبتحليل واقع العلاقات التي تربط الممالك الخليجية بالنظام الإقليمي والدولي، يمكننا أن نلمس حالة التنازل والانصياع الدائم إلى الراعي الدولي ووكيله الإقليمي.

إنَّ جوهر العلاقة الأمنية والسيبرانية التي تربط السعودية والإمارات بالكيان الاسرائيلي لا يقوم على أسس من التعاون والمنفعة المتبادلة بين الطرفين، فالكيان الإسرائيلي يجيد التحرك منفرداً، ويفضّل ذلك، ويتبنى سياسة خارجية تقوم على التفرد في اتخاذ القرار والتحرك بعيداً عن أي تعاون أو شراكة إقليمية. لكن فقدان الثقة بالحلفاء من جهة، وإيمانه بعدم فاعلية وقدرة الشركاء على تحقيق الأهداف المشتركة من جهة أخرى، يجعلان علاقة الكيان بالآخرين علاقة تضمن مصلحته أولاً وأخيراً. وعليه، يمكن القول إنّ كلّ ما يشاع عن روزنامة أمنية خليجية، وعن برنامج تجسس سيبراني يطال عدداً من الشخصيات السياسية من الحلفاء والخصوم، لا يمكن أن يندرج في سياق العمل الأمني الخليجي المستقل، إنما يدخل في إطار تقاطع المصالح الصهيونية

الخليجية، بما يمكن أن يبرر قبول وزارة الأمن الإسرائيلية بتصدير برنامج "بيغاسوس" إلى دول الخليج. وبالإشارة إلى مميزات هذا البرنامج، يمكن بسهولة التأكيد أن القبول الإسرائيلي بتوريد "بيغاسوس" يراعي مصالح "إسرائيل" الأمنية، وخصوصاً إذا لاحظنا مدى قدرة الشركة الأم على التحكّم في هذا البرنامج، لناحية الحصول على داتا الهواتف المستهدفة، ولو لم تكن هي المتحكّم المباشر في البرنامج، وأيضاً ما أعلنته الشركة نفسها عن عدم قدرتها على استهداف الهواتف الموجودة في الولايات المتحدة الأميركية، في إشارة إلى قدرتها على التحكّم في الساحات التي يُسمح بالعمل ضمنها. ومن خلال هذه المقاربة، نستطيع استخلاص نتيجة مفادها أنَّ "بيغاسوس" لا يشكّل أبداً باكورة التعاون الأمني بين الممالك الخليجية والكيان الإسرائيلي، إنما يمكن القول إن هذا البرنامج هو الدليل الحيّ والواقعيّ على عمق التبعية الأمنية والسيبرانية الخليجية للكيان الإسرائيلي. أما بالنسبة إلى كشف فضيحة "بيغاسوس"، فتجدر الإشارة إلى أنَّ الأمر لا يرتبط مطلقاً بصون حقوق الإنسان الأساسية التي جرى انتهاكها، والتي كان الصحافي جمال خاشقجي أول ضحاياها، وإنما يمكن ربطه بإشكالية دور محمد بن سلمان وشريكه ابن زايد الذي تكرَّس في زمن دونالد ترامب، إذ استطاعا في تلك المرحلة أن يؤثرا في السياسة العالمية أكثر من القوى التقليدية، كفرنسا وألمانيا وغيرهما. وعليه، تقاطعت المصالح الفرنسيّة والألمانيّة والإدارة الجديدة في الولايات المتحدة عند ضرورة تحجيم محمد بن سلمان وإعادة الدور والطموح السعودي خاصة، والخليجي عامة، إلى حجمه الحقيقي. وفي هذا الأمر، سنلمس صحّة ما أشرنا إليه حول طريقة الكيان الصهيوني في إدارة أموره، إذ سيتبرأ من هذه الفضيحة التجسّسية. وقد يتخذ قراراً أمنياً بتعطيل هذا البرنامج لدى الدول الخليجية وغيرها، بناءً على نصيحة أميركية أو تقدير ذاتي.

لم تكن مشاركة الإمارات في التجسّس على هواتف سياسيين وصحافيين وآخرين، في أنحاء العالم، باستخدام نظام «بيغاسوس» الإسرائيلي، سوى فصل صغير في سيرة نظامٍ ديدنه التآمر والتجسس. فقد أعاد فضح عملية التجسّس التي نحن بصددها، تظهير طبيعة هذا النظام، والتي أحسن مسؤول سابق في إدارة دونالد ترامب توصيفها، حين قال: «إنك إذا قلبْتَ حجراً في أيّ مكان من القرن الأفريقي، فستجد تحته الإمارات». لكن تطوّرَين حصلا في الاونةالاخيرة ، يهدّدان بتدفيع ابن زايد ثمناً باهظاً لسياسته هذه، مع تغيّر اتجاهات الرياح: الأوّل هو «الزعل» بينه وبين ابن سلمان، بعد اختلافهما حول الكثير من الملفّات، ومنها اليمن وقطر وإسرائيل. والثاني هو اعتقال تاجر العقارات الأميركي، «الزحلاوي» الأصل، طوم براك، بتهمة العمل لمصلحة

الإمارات كعميل غير مسجّل، في الحلقة الضيّقة حول ترامب، خاصة أن الإمارات عرضت عبر جورج نادر، اللبناني الأصل هو الآخر، المساعدة في تمويل حملة الرئيس السابق الانتخابية في عام 2016.

لربّما كانت حياكة المؤمرات أقدم حِرفة في قصور الحُكم في الخليج، إلّا أنها مع ابن زايد تجاوزت كلّ الحدود، بحيث بات الخليج والعالم العربي برمّتهما يعيشان على إيقاع الأحداث المتسارعة التي لا يفتأ ولي عهد أبو ظبي يذكي نيرانها، وصولاً إلى دخوله، بعد تطبيع العلاقات مع إسرائيل، تعاوناً علنياً وثيقاً مع «الموساد»، الذي ترأسه يوسي كوهين، أكثر مسؤول في كيان العدو تردّداً على أبو ظبي، بل إن هذا التعاون تمأسس سريعاً، وصار علاقة مباشرة بين مستشار الأمن الوطني الإماراتي، طحنون بن زايد، والجهاز الإسرائيلي، واتّسعت ملفاته، ليتحوّل إلى صداقة نادرة بين أجهزة التجسّس، التي لا تقيم عادة علاقات ودّية في ما بينها، حتى لو كانت من أقرب الحلفاء. حتى ابن سلمان يتّضح أنه كان مجرّد تلميذ عند حاكم الإمارات، الذي يقال إنه تآمر على أخيه الأكبر، رئيس الدولة، خليفة بن زايد، منذ أن أقعدت الأخيرَ جلطة دماغية في كانون الثاني من عام 2014، ثمّ نَشر له صوراً في عام 2019، بعد غياب دام كّل تلك السنوات، وهو في حال يرثى لها، في ما فسّره مناوئون لوليّ العهد على أنه محاولة لإظهار أخيه بمظهر العاجز تماماً، لإضفاء مزيد من الشرعية على حكمه.

بدأ ابن زايد مؤامراته مع جاسوس محترف هو القيادي المفصول من حركة «فتح»، محمد دحلان، الذي كان له دور في توسيع النفوذ الإماراتي، ليس في الشرق الأوسط فقط، بل أيضاً في أفريقيا وأوروبا. وللأخير تاريخ «خياني» طويل يعود إلى ثمانينيات القرن الماضي، حين جرى تجنيده من قِبَل «سي آي إي» في شمال أفريقيا، ثمّ أقام علاقات وثيقة بـ«الموساد» خلال عمله كرئيس لجهاز الأمن الوقائي في غزة. وهو مطلوب للعدالة في تركيا، مقابل 700 ألف دولار، بتهمة المساهمة في محاولة الانقلاب على رجب طيب أردوغان في 2016.

«الإنجاز» الأهمّ لابن زايد، كان اختراق الحلقة الضيقة حول دونالد ترامب، قبل فوز الأخير في انتخابات 2016، عبر طوم براك الذي أوقفته السلطات الأميركية مؤخراً لاتّهامه بأنه كان عميلاً غير مسجّل للإمارات لدى ترامب، في تطوّر يبدو أنه سيرتدّ سلباً على المشغّل، خاصة أن المواطن الإماراتي المقيم في الولايات المتحدة، راشد المالك، أُوقف معه بالتهمة نفسها. ولم تكن روسيا البلد الوحيد الذي أرسل موفديه إلى «برج

ترامب» خلال حملة الانتخابات الرئاسية عارضاً المساعدة؛ إذ يشير تقرير للجنة الاستخبارات حول التدخّل الروسي في الانتخابات إلى اجتماع في آب 2016، ضمّ جورج نادر الذي كان حينها مستشاراً لابن زايد، والذي عرض أيضاً المساعدة، فيما كان براك، بصفته رئيس لجنة تنصيب ترامب، يؤدّي دور أحد مهندسي العلاقة بين الرئيس وحكّام الخليج، ويتولّى المساهمة في تشكيل السياسة الخارجية للمرشّح وفق مصلحة ابن زايد. حتى أنه ذات مرّة دسّ في خطاب لترامب حول السياسة الخارجية، عبارات عن الخليج بطلب من الأخير، وأبلغ مسؤولاً إماراتياً كبيراً بأنه رشّح موظفين لحملة ترامب الانتخابية، من بينهم المدير السابق للحملة بول مانافورت، ثمّ سافر إلى الإمارات لإعداد استراتيجية حول ما تريده أبو ظبي من الإدارة في أوّل مئة يوم، وأوّل ستة أشهر، وأوّل سنة من الولاية، ثمّ في كامل الولاية.

إن الهدف الدائم لـ«التآمر» الإماراتي يبقى قطر، حتى بعد مصالحة «قمّة العلا» الخليجية في السعودية، والتي لم تُرضِ ابن زايد، فيما ذهب ابن سلمان فيها بعيداً، التماساً لمساعدة في الخروج من أكثر من ملفّ تَورّط فيه، في ما مثّل واحداً من أسباب «الزعل» عن نظيره في أبو ظبي. وكان لبراك دور في انحياز ترامب إلى «رباعيّ المقاطعة»، وكذلك في السعي لإقناع الإدارة بأن «الإرهاب لا يأتي فقط من إيران، وإنما أيضاً من الإخوان وحكومة تركيا»، وهو نجح بالفعل في دفعها إلى وضع الجماعة على قائمة الإرهاب. وبعد أن روّج ابن زايد لابن سلمان في البيت الأبيض، باعتباره سدّاً في وجه الإسلام السياسي من المستحيل التحرّك ضدّ الجماعات الإسلامية المعادية في العالم، من دون دعمه، عاد وصبّ تآمره عليه، فتركه غارقاً في وحول اليمن، من خلال سحب قوّاته من هناك، وخوض حرب بالوكالة ضدّ السعوديين أنفسهم، حيث تقاتل قوات «المجلس الانتقالي الجنوبي» المدعومة منه، قوات الرئيس المنتهية ولايته عبد ربه منصور هادي المدعومة من الرياض. أمّا الحلقة الأحدث في «مؤامرات» ابن زايد ضدّ ابن سلمان، فكانت الدفع باتّجاه ضرب أسعار النفط في «أوبك»، وهي التي فجّرت الخلاف بين الرجلين وأخرجته إلى العلن. فليس غريباً، والحال هذه، أن يتجسّس الرجلان على بعضهما البعض، باستخدام نظام «بيغاسوس» نفسه.

لم يكتفِ وليّ العهد السعودي، المسكون بهاجس العرش، بحملة التطهير التي أطلقها تحت عنوان «مكافحة الفساد»، ولقيت، للمفارقة، رواجاً في الغرب الذي بدا معجباً بحزم الأمير «الإصلاحي». بل إن تلك الحملة جرّت وراءها أخرى، وقادت المملكة إلى سلوك طريق الجاسوسيّة كسبيل لردع المخالِفين وتكميم الأفواه، ولو

بالقتل تقطيعاً إذا اضطرّ الأمر. وفي نهاية عام 2016، أي بعد نحو عامين على بدء حُكم سلمان بن عبد العزيز، دخلت شركة «إن إس أو» الإسرائيلية في مفاوضات مع مسؤولين في الاستخبارات السعودية، لبيع نظام التجسُّس، «بيغاسوس»، إلى الرياض. وهي شراكة لم تكن لتحصل من دون حصول الشركة – وهي واحدة من مجموعة شركات تعاونت مع المملكة – على ضوء أخضر من وزارة الأمن الإسرائيلية التي أصدرت، وفق أكثر من تحقيق صحافي نُشر أخيراً في هذا السياق، تصاريح تصدير رسمية لشركات تعمل في مجال البرمجة و»الهاي تك»، لبيع برمجيّاتها الخاصة بالتجسُّس والقرصنة، إلى السلطات السعودية، وكل مَن يرغب في مراقبة مواطنيه. استمرّت الشراكة الإسرائيلية – السعودية حتى بعد استخدام هذه الأخيرة برمجيات التجسّس لملاحقة المعارضين والناشطين الحقوقين، واغتيال خاشقجي. ويفيد تحقيق نشرته صحيفة «نيويورك تايمز»، السبت، أعدّه محلّل الشؤون الاستخبارية في صحيفة «يديعوت أحرونوت» رونين بيرغمان، بمشاركة الصحافيَّين مارك مازيتي وبن هابرد، بأن «السبب الحقيقي وراء الصمت الرسمي الإسرائيلي على هذه النشاطات، هو أن ممثّلي الشركات الضالعة في أنشطة التجسُّس والقرصنة، ذهبوا إلى السعودية بتصريح خاص صادر عن المؤسسة الأمنية الإسرائيلية التي منحتهم موافقتها الكاملة»، بل و»شجعتهم» على العمل مع المملكة، مشترطةً أن تبقى المداولات في إطارٍ سرّي. مع بداية عام 2017، باعت «إن إس أو» برنامج القرصنة الرئيس الذي طوّرته، «بيغاسوس»، للاستخبارات السعودية، ليتم استخدامه من قِبَل فريق سعود القحطاني، المستشار المُقال في الديوان الملكي، والذي اتُّهم، في نهاية عام 2018، بإصدار أوامر قتل خاشقجي، فيما كشفت المعلومات التي جمعتها الاستخبارات الأميركية أن القحطاني حافظ، خلال عام 2017، على اتصالات مكثّفة مع كبار مسؤولي الشركة الإسرائيلية. الصمت الطويل الذي استغرقته تل أبيب للتعليق على جريمة اغتيال خاشقجي، كان شاهداً على «حرجها» حيال القضيّة التي وإن كان رئيس الحكومة الإسرائيلية، بنيامين نتنياهو، وصفها بـ»المروّعة» في بيان أصدره يوم الثاني من تشرين الثاني 2018، أي بعد شهر كامل من ارتكابها داخل القنصلية السعودية في إسطنبول، إلّا أنه شدّد، في الوقت ذاته، على ضرورة التعامل معها بالشكل الصحيح: «من المهمّ للغاية أن تبقى السعودية مستقرّة، لأن إيران هي المشكلة الكبرى في المنطقة». على هذا، تفيد التقارير المنشورة في الإعلام الغربي، بدخول الرياض وتل أبيب، منذ

عام 2014، في اتصالات غير رسمية، توّجها ابن سلمان بلقاء جمعه إلى نتنياهو نهاية العام الماضي، من دون أن يُنتِج اتفاقاً رسمياً لتطبيع العلاقات على الطريقة الإماراتية.

تفرّعت ماكينة التجسّس السعودية لتغطي نشاطاتها أكبر مساحة ممكنة، وتطاول أكبر عدد من المخالفين الذين «يهدّدون» مستقبل العرش. ففي آب 2020، كشفت وكالة «بلومبرغ» عن ارتباط قضية التجسّس الضالع فيها موظفون في شركة «تويتر» (2015) لمصلحة السعودية، باعتقال معارضين سعوديين واختفاء آخرين، من مثل الناشط عبد الرحمن السدحان الذي اعتُقل على يد الشرطة السرية في الرياض في آذار 2018، علماً أنه عمل موظّفاً في الهلال الأحمر، فضلاً عن نشاطه «السرّي» على «تويتر». كذلك، حدّدت وكالات حقوقية هوية ستة سعوديين كانوا يديرون حسابات مجهولة أو بأسماء مستعارة تنتقد الحكومة وتم اعتقالهم، بفضل عملاء المملكة في الشركة، وهم الموظفان أحمد أبو عمو، وهو لبناني يحمل الجنسية الأميركية، وعلي آل زباره، السعودي الجنسية، بالإضافة إلى أحمد المطيري، وهو اختصاصي تسويق سعودي له علاقات مع سلطات بلاده. وقبل ذلك، وتحديداً في آذار 2020، كشفت صحيفة «غارديان» البريطانية، عن استغلال المملكة ثغرة في شبكة الهواتف المحمولة الدولية، لتتبُّع مواطنيها المسافرين إلى الولايات المتحدة، ورصْد تحركاتهم والتجسّس عليهم. وذكرت أن أحد المبلّغين أطلعها على ملايين طلبات التتبُّع السرية المرسلة من السعودية، منذ تشرين الثاني 2019، والتي هدفت إلى تحديد مواقع المواطنين السعوديين في أميركا، عبر رصد مواقع هواتفهم المحمولة المسجّلة في المملكة. وهي طلباتٌ جاءت من جانب «أكبر ثلاث شركات للهواتف المحمولة في السعودية: «سعودي تيليكوم»، و»موبايلي»، والتي أرسلت إلى مشغّل الهاتف المحمول الأميركي في المتوسط، 2.3 مليون طلب تتبُّع شهرياً في المدّة ما بين تشرين الثاني 2019 وآذار 2020.

بالنسبة إلى شركة «إن إس أو» تحديداً، فإن علاقتها بالسعودية بدأت في نهاية عام 2016، حيث كانت الشركة الأولى التي بدأت مفاوضات مع مسؤولين استخباريين سعوديين من أجل بيع برامجها لهم، بعد حصولها على ترخيص من وزارة الأمن الاسرائيلية. وفي بداية عام 2017، باعت الشركة منظومتها المركزية للولوج إلى الهواتف، والمعروفة باسم «بيغاسوس»، للإستخبارات السعودية. كذلك، حصلت ثلاث شركات إسرائيلية عاملة في المجال نفسه هي: «كفادريم»، «كيندرو»، و«فرينت» على تراخيص من وزارة الأمن

الإسرائيلية لبيع منتَجاتها الهجومية للسعودية، بحسب صحيفة «هآرتس». أمّا الشركة الخامسة فتُدعى «سيليبريت»، وهي تنتج منظومات ولوج فيزيائي إلى الهواتف المحمولة، وقد باعت هي الأخرى خدماتها للسعودية، ولكن «من دون الحصول على رخصة من وزارة الأمن». وبالعودة إلى «كينديرو»، فهي متخصّصة في الولوج إلى منظومة «ويندوز»، التي كشفت منتِجتها، شركة «مايكروسوفت»، في وقت سابق، أن زبائن «كينديرو» اقتحموا الحواسيب، مُتّهمة الشركة الإسرائيلية ببيع بعض الحكومات برنامجها من أجل التجسّس على صحافيين، وسياسيين، ومعارضين، وناشطين حول العالم، علماً أن «كينديرو» باعت على الأقلّ منظومة واحدة للسعودية، فيما بدأت شركة «كفادريم» مفاوضات مع المملكة في أيار من العام 2018.

من ناحية أخرى، إن قيام إسرائيل ببيع برنامج «بيغاسوس» للمغرب لكي يستخدمه الأخير للتجسّس على المسؤولين الفرنسيين، يُعدّ تطوّراً يستحقّ التأمّل فيه، لأنه يكشف تحوّلاً في طبيعة التحالفات التي تنسجها تل أبيب وفي نظرتها الفعلية لِمَن تعتبرهم حلفاء من «الدرجة الثانية». محاولات إسرائيل للتجسّس حتى على أهمّ حلفائها، ليس بالأمر الجديد. جميعنا يذكر قضيّة الأميركي جوناثان بولارد الذي اعتُقل سنة 1985 بتهمة التجسّس على بلاده لحسابها. الجديد هو بيعها برامج تجسّس لدول أخرى تعمل على تطوير علاقاتها معها، كالمغرب مثلاً، دون التأكُّد من عدم استخدامها ضدّ حلفاء آخرين، كفرنسا مثلاً. يعزو فردريك مورو، الخبير الفرنسي في شؤون الدفاع، في مقابلة مع «لوموند»، عدم اكتراث إسرائيل لردّ الفعل الفرنسي أو الأوروبي تجاهها، إلى قناعتها بأنه سيكون في غاية الضعف. ولا شكّ في أن هذا الرأي يتضمّن الكثير من الوجاهة لأن التحوّلات البنيوية، السياسية والاجتماعية، التي شهدها الكيان الصهيوني في العقود الماضية، وطغيان التيارات الفاشية القومية والدينية على المشهد السياسي فيه، كان لها أيضاً أثر كبير على الفهم السائد للوضع الدولي وللتحالفات. العالم من منظور هذه القوى، بات غائباً أكثر من أيّ حقبة سابقة، وموازين القوى الفجّة هي التي تحكم تعامل أطرافه بعضها مع بعض، صراعاً وتقاطعاً وتحالفاً. إن إسرائيل لا تحترم إلّا الأقوياء، وهم في حالتنا الولايات المتحدة وروسيا والصين، وتتجنّب استفزازهم. أمّا الآخرون، فهي تتعاطى معهم، وكما أظهرت «الفضيحة»، وفقاً لأولوياتها الظرفيّة. وما فعلته اسرائيل مع فرنسا، لن تتردّد في تكراره في المستقبل مع دول كالمغرب والإمارات والسعودية إذا اقتضت مصالحها المتغيّرة ذلك. لا تحالفات ثابتة، أو على الأقلّ تجنّباً للتأزيم، إلّا مع الأقوياء. هي لم تراعِ الاندفاعة الفرنسية غير المسبوقة حيالها في السنوات الماضية، والتي

فصّلها الباحث والصحافي الفرنسي، جان ستيرن، في سلسلة مقالات على موقع «شرق 21» عن اللوبي الإسرائيلي في بلاده. فشركة «إلبيت» الإسرائيلية تساهم في إنتاج نظام «العقرب»، وهو في قلب استراتيجية القوات البرية الفرنسية في العقود القادمة، و»يسمح بتطوير قيادة رقمية واحدة تعتمد على وصلة مشتركة تسمح للجنود المنتشرين في الميدان وكذلك للأدوات العسكرية الجديدة، مثل الطائرات من دون طيار والروبوتات، بأن تكون متّصلة في وقت واحد لتستبق بالتالي ردود فعل العدو». أمّا الشركات الفرنسية العاملة في حقل التكنولوجيا الرقمية، ف»جميعها تريد الموساد عندها»، بحسب العنوان الحرفي لإحدى مقالاته في السلسلة المشار إليها آنفاً، والتي يتحدّث فيها عن مدى إعجاب الشركات الخاصّة وصناعات الدفاع الفرنسية، بإنجازاته في المجالات التكنولوجية، خاصّة برنامج «بيغاسوس». وهذه المقالة نُشرت في 26 نيسان الماضي، أي قبل «الفضيحة»، ما يضعنا أمام هُيام من طرف واحد يقابله عدم اكتراث، إن لم يكن ازدراء من الطرف الآخر.

7 – الجهات المستهدفة بالبرنامج:

لأن بيغاسوس من برامج التجسس الموجهة والمكلفة جدا فإن الجهات الفاعلة تستخدمه لمهاجمة أفراد "ذوي قيمة عالية" من الناشطين السياسيين أو غيرهم ممن بإمكانهم الوصول إلى معلومات مهمة وحساسة وسرية. ولكن من المحتمل أيضا استخدامه للهجوم على أهداف محددة لأغراض متعددة، بما في ذلك التجسس على الشركات الكبرى، وكثيرا ما يكون الرؤساء التنفيذيون والمديرون الماليون والمسؤولون التنفيذيون والفرق المالية في مرمى الهجوم، لأنهم عادة يملكون وصولا إلى البيانات السرية، خاصة عبر أجهزتهم المحمولة. وما يزال دوي فضيحة التجسس الاسرائيلي على هواتف أكثر من 50 ألف صحفي وسياسي وناشط حقوقي من مختلف دول العالم يتردد في كل القارات. وفيما يلي نظرة على آخر مستجدات الفضيحة وأبرز الدول التي تم التجسس على هواتف فيها.

لقد تحول الحصان المجنح في الميثولوجيا الإغريقية، "بيغاسوس"، إلى أحد البرمجيات الخبيثة المسماة حصان طروادة. وكشف تحقيق استقصائي نشر في عدة وسائل إعلام عالمية فضيحة برنامج التجسس "بيغاسوس"، الذي طورته شركة NSO Group الإسرائيلية، وطاول العالم بأسره. وتم التجسس على أكثر من 50 ألف هاتف تعود معظمها لصحفيين، ولكن بعضها يعود أيضاً لساسة ونشطاء حقوقيين ومدراء شركات وآخرين.

ومن بين المستهدفين بالبرنامج ساسة أوروبيون بارزون كرئيس وزراء بلجيكا السابق ورئيس المجلس الأوروبي الحالي، شارل ميشيل. كما تم استهداف رقم والده، لويس ميشيل، الذي كان عضواً في البرلمان الأوروبي حتى عام 2019. والاسم الآخر البارز هو الرئيس الفرنسي إيمانويل ماكرون. إذ عثر على رقم هاتف يستخدمه منذ عام 2017 من بين الأرقام المستهدفة، بحسب صحيفة "لوموند" الفرنسية. كما عثر على أرقام تعود لأحد حراسه الشخصين السابقين ورقم وزير الخارجية، جان إيف لودريان، ورئيس الوزراء الأسبق، إدوار فيليب. وقد نددت الحكومة الفرنسية بما وصفته بـ"وقائع صادمة للغاية". وقال الناطق باسم الحكومة غابريال أتال لإذاعة "فرانس إنفو"، "إنها وقائع صادمة للغاية، وإذا ما ثبتت صحتها، فهي خطيرة للغاية". وأضاف "نحن ملتزمون بشدة بحريّة الصحافة، لذا فمن الخطير جداً أن يكون هناك تلاعب وأساليب تهدف إلى تقويض حرية الصحافيين وحريتهم في الاستقصاء والإعلام". ويتهم المغرب بالوقوف خلف استهداف أرقام الساسة الفرنسيين والبلجيك. بيد أن الرباط تنفي مسؤوليتها. وقرر المغرب رفع دعوى قضائية أمام المحكمة الجنائية في باريس ضد منظمتي "فوربيدن ستوريز" والعفو الدولية بتهمة التشهير على خلفية اتهامهما الرباط بالتجسس باستخدام برنامج "بيغاسوس". من ناحية اخرى تبين حوالي 15 ألف رقم من اللائحة المنشورة لهواتف كانت عرضة للتجسس تعود لأشخاص من المكسيك، من بينهم الرئيس، أندريس مانويل لوبيس أوبرادور، وبعض أفراد أسرته وآخرين من معارفه. ويحمل زعيم المعارضة السابق الحكومة السابقة المسؤولية. ووصل أندريس مانويل لوبيس أوبرادور إلى سدة الرئاسة عام 2018. وكانت المكسيك أول دولة تمتلك برنامج "بيغاسوس" عام 2011. يمكن كذلك أن يكون لقتل صحفي مكسيكي علاقة بالتجسس عليه بواسطة البرنامج. فقد اغتيل سيسيليو بينيدا بيرتو بالرصاص عام 2017 بعد نشره تقارير لسنوات عن الفساد ومافيا المخدرات في البلاد. وتضم القائمة أرقام 26 صحفياً مكسيكياً، من بينهم رئيس مكتب صحفية "نيويورك تايمز" في العاصمة المكسيكية ورقم أحد معدات التقارير في العاصمة لصالح قناة "سي إن إن" الأمريكية. ويتم الحديث عن استهداف أكثر من 180 صحفياً حول العالم، كالمجريين سزابولكس باني وأندراس زابو، اللذين يعملان في Direk36 الاستقصائية والتي ليست قريبة من الحكومة. ومن بين من تعرض للتجسس إحدى أشهر الصحفيات الاستقصائيين في أذربيجان، خديجة إسماعيلوفا، هذا بالإضافة لعديد كبير من الصحفيين والنشطاء الحقوقيين في البلاد. وعُثر في هاتفها على آثار لبرنامج التجسس "بيغاسوس".

يظهر أن لبرنامج التجسس علاقة ما ايضاً بمقتل الصحفي السعودي جمال خاشقجي في القنصلية السعودية في إسطنبول عام 2018، بحسب منظمة العفو الدولية، التي تقول إن الهاتف النقال لخطيبة خاشقجي التركية خديجة جنكيز تم اختراقه بعد أربعة أيام فقط من مقتله. ويعتقد أن السياسي التركي ياسين أكتاي قد تمت مراقبته أيضاً. كان أكتاي صديقاً لخاشقجي ومستشاراً للرئيس التركي رجب طيب أردوغان.

في عام 2019 حاولت الشيخة لطيفة ابنة حاكم دبي، الشيخ محمد بن راشد آل مكتوم، الفرار، بيد أن محاولتها باءت بالفشل. لكن زوجة أبيها، الأميرة الأردنية هيا بنت الحسين، نجحت في الفرار عام 2019. اليوم كشف أن رقمي هاتفي لطيفة وهيا خضعا للتجسس بالبرنامج أيضاً. وكان رقم لطيفة خاضعاً للتجسس سنة على الأقل قبل محاولة هروبها الفاشلة.

في الهند كان هناك أكثر من 1000 رقم تحت المراقبة. واتهم حزب المؤتمر الهندي المعارض رئيس الوزراء، نارياندا موري، بالخيانة، لأنه عرض الأمن الوطني للخطر بالتجسس على أرقام مواطنين هنود، حسب المؤتمر الوطني. وقد يكون الزعيم المنفي المقيم في الهند، دالي لاما، قد تعرض هو الآخر للتجسس. الزعيم الروحي للتيبت، البالغ من العمر 86 عاماً، ليس لديه هاتف جوال، بيد أن أرقام هواتف مقربين منه وجدت في القائمة. وعلى الأرجح تجسست راوندا على المعارضة وعلى هاتف رئيس جنوب أفريقيا سيريل رامافوزا. وبشكل عام يعتقد أن راوندا تجسست على ما يقارب 3500 هاتف جول.

فرع رئيس منظمة "مراسلون بلا حدود" في ألمانيا، كريستيان مير، طالب وبشكل عاجل بتشريعات دولية صارمة ضد انتشار البرمجيات الخبيثة: "يجب منع تصدير تلك التقنيات للدول الاستبدادية ومعاقبة المخالفين. تلك البرمجيات التجسسية تعرض حرية الصحافة للخطر وفي أسوء الأحوال حياة الناس أيضاً". وبالمثل طالبت المستشارة الألمانية، أنغيلا ميركل، بتشريعات دولية أكثر صرامة للمتاجرين ببرامج التجسس، مؤكدة على ضرورة ألا تقع تلك البرمجيات في "الأيدي الخطأ". في المقابل أعلنت إسرائيل عن تشكسل لجنة للتحقيق في فضيحة التجسس. وسيترأس اللجنة مجلس الأمن القومي المرتبط مباشرة برئيس الوزراء نفتالي بينت.

اخيراً ان عملية التسريب الجماعي تؤكد واحدا من احتمالين، الأول يتعلق بتقنية تسريب متعمدة سواء من طرف موظف سابق في الشركة، أي على شاكلة إدوارد سنودن الذي سرّب طرق تجسس وكالة الأمن القومي الأمريكي منذ سنوات وأحدث ضجة عالمية. وهذه الطريقة هي المتعارف عليها، إذ أن تسريبات ويكليكس

والحسابات السرية في سويسرا ثم أوراق بنما كانت عملا فرديا. ويتجلى الاحتمال الثاني في قيام جهاز استخبارات دولة كبرى في اختراق الشركة وتسريب ملفات التجسس، وقد تكون هذه الدولة قد تضررت من "بيغاسوس" وأرادت "تأديب" إسرائيل، وهذا مرجح. ويبقى الأخطر في عملية التجسس هو تحكم شركة "NSO" أو بالأحرى إسرائيل في تشغيل البرنامج، ونظرا للمشاكل التي عانت منها الدولة العبرية في عمليات التجسس خاصة مع الأوروبيين، قد تكون استعملت بعض الدول الزبائن بدون وعي منها في التجسس على شخصيات دولية. وهذا يعني أنها استعملت هذه الدول مثل حالة VPN في الإنترنت، أي إخفاء هويتها. وهذا يؤكد كيف خدعت إسرائيل أجهزة الاستخبارات هذه.

8 – خاتمة:

ضجّت وسائل الإعلام العالمية، في الاونة الاخيرة ، بالحديث عن برنامج "بيغاسوس" (Pegasus) الذي طوّرته مجموعة "إن إس أو" (NSO) الإسرائيلية، واستخدامه في التجسّس على نشطاء وصحافيين وسياسيين حول العالم. ما زاد المخاوف من انتهاكات واسعة النطاق للخصوصية الشخصية والحقوق المدنية. و"إن إس أو" ليست الشركة الإسرائيليّة الوحيدة التي يُشتبه في أنّها تزوّد حكومات أجنبيّة ببرامج تجسّس، بعد حصولها على ضوء أخضر من وزارة الدفاع الإسرائيليّة. فبرنامج "لسان الشيطان" (ديفيلز تانغ) التابع لشركة "سايتو تِك ليميتد"، المعروفة في الغالب باسم "كانديرو"، قد استُخدم هو أيضًا ضدّ مئات السياسيّين والمعارضين والصحافيّين والنشطاء.

من ناحية أخرى وصفت صحيفة "الغارديان" البريطانية برنامج "بيغاسوس" بأنه "أقوى برنامج تجسّس تمّ تطويره على الإطلاق من قبل شركة خاصّة. وأنه بمجرد أن يتسلّل إلى هاتفك، يتحوّل إلى جهاز مراقبة يعمل على مدار 24 ساعة. يُمكنه نسخ الرسائل التي ترسلها أو تتلقّاها، وجمع صورك وتسجيل مكالماتك. كما تكمن مخاطره في أنه يستطيع تصويرك سرًا من خلال كاميرا هاتفك، أو يُشغّل الميكروفون لتسجيل محادثاتك. كما يمكنه تحديد مكانك الحالي، والمكان الذي كنت فيه، والأشخاص الذين قابلتهم.

"بيغاسوس" اذن هو برنامج قرصنة أو تجسّس، طوّرته شركة "إن إس أو" الإسرائيلية، وسوّقت له ومنحت رخصة استخدامه لعدد من الحكومات في جميع أنحاء العالم. ويستطيع البرنامج اختراق مليارات الهواتف التي

تعمل بأنظمة تشغيل "أي أو أس" (IOS)، و"أندرويد" (Android). وفي عام 2016، اكتشف باحثون نسخة مبكّرة من "بيغاسوس" بعد أن اخترقت الهواتف من خلال ما يُسمّى "التصيّد بالرمح" (Spear Phishing)، القائم على استهداف شخصٍ محدّد وإرسال الرسائل النصّية أو رسائل البريد الإلكتروني التي تُغري المستخدم للنقر على رابط ضارّ. ومنذ ذلك الحين، تطوّرت قدرات شركة "أن.أس.أو" على شنّ هجمات بما يُعرف باسم "النقر الصفري"، والتي لا تتطلّب أي تفاعل من مالك الهاتف من أجل تحقيق النجاح. غالبًا ما تُستغل هذه الثغرات الأمنية في "يوم الصفر"، وهي عيوب أو أخطاء في نظام التشغيل لا تعلم الشركة المصنّعة للهاتف المحمول بوجودها، وبالتالي لم تتمكّن من إصلاحها. في عام 2019، كشف تطبيق "واتساب" عن استخدام برنامج "إن إس أو" لإرسال برامج ضارّة إلى أكثر من 1400 هاتف من خلال استغلال ثغرة "يوم الصفر". وبإجراء مكالمة هاتفية من "واتساب"، يُمكن تثبيت رمز "بيغاسوس" الخبيث على الهاتف، حتى لو لم يرد المستخدم مطلقًا على المكالمة. وفي الآونة الأخيرة، بدأت شركة "إن إس أو" باستغلال الثغرات الأمنية في برنامج "آي مسج" من شركة "آبل"، للوصول إلى مئات الملايين من أجهزة "آيفون"، على الرغم من أن الشركة تقول إنها تقوم باستمرار بتحديث برامجها لمنع مثل هذه الهجمات.

الجدير بالذكر أنه بمجرد تثبيت هذا البرنامج على الهاتف، يمكنه جمع أي معلومات، أو استخراج أي ملف، وتسريب الرسائل النصيّة، والعناوين، وسجل المكالمات، والتقويمات، ورسائل البريد الإلكتروني، وتاريخ تصفّح الإنترنت. وعندما يتمّ اختراق جهاز آيفون، يتمّ ذلك بطريقة تسمح للمهاجم بالحصول على ما يسمى بامتيازات الجذر، أو الامتيازات الإدارية، على الجهاز. وقد استثمرت "إن إس أو" جهودًا كبيرة في جعل برمجياتها صعبة الاكتشاف. ويشكّ باحثو الأمن في أن الإصدارات الأحدث من "بيغاسوس" تُشغّل فقط الذاكرة المؤقتة للهاتف، بدلًا من محرّك الأقراص الثابتة، ما يعني أنه بمجرد إيقاف تشغيل الهاتف، يختفي كل أثر للبرنامج تقريبًا. وحالياً نجد أن أحد أهم التحديات التي يطرحها برنامج "بيغاسوس" أمام الصحافيين والمدافعين عن حقوق الإنسان، هو أن البرنامج يستغلّ نقاط الضعف غير المكتشفة، ما يعني أنه حتى مستخدم الهاتف المحمول الأكثر وعيًا بالأمان لا يمكنه منع الهجوم.