التحالف غير المرئي: التعاون الأمريكي–الإسرائيلي في صناعة برامج التجسس

1. المقدمة

في زمنٍ تتقاطع فيه الخوارزميات مع الجغرافيا، وتُدار فيه المعارك بالبيانات بدل الدبابات، برز التحالف الأمريكي–الإسرائيلي كأحد أكثر التحالفات التقنية والاستخباراتية تأثيرًا في تشكيل ملامح النظام الدولي الجديد. لم يعد التعاون بين واشنطن وتل أبيب حكرًا على مجالات الدفاع التقليدي أو التبادل الاستخباراتي الكلاسيكي، بل تمدّد إلى فضاءات رقمية معقّدة تصوغ فيها برمجيات التجسس والأمن السيبراني حدود القوة والهيمنة. بينما توفّر الولايات المتحدة رأس المال والشرعية السياسية والهيمنة المؤسسية، تقدّم إسرائيل الكفاءة التقنية والقدرة على الابتكار في الميدان السيبراني، لتتشكل بينهما شراكة تكنولوجية–استخباراتية تُعيد تعريف مفهوم الأمن القومي في القرن الحادي والعشرين. هذه الشراكة ليست مجرد تبادل مصالح، بل هي شبكة معقدة من التداخلات الاقتصادية والاستخباراتية والقيمية، تجعل من التكنولوجيا ساحة نفوذ مشتركة ومصدرًا للتوتر في آن واحد.

من خلال تحليل ديناميات هذا التعاون وتفاعلاته، يسعى هذا البحث إلى فهم كيف أصبحت البرمجيات التجسسية جزءًا من البنية الاستراتيجية للتحالف الأمريكي–الإسرائيلي. فالتحالف الذي بدأ كحاجة أمنية متبادلة، تحوّل اليوم إلى تحالف معرفي–رقمي تتقاطع فيه المصالح التجارية مع الرهانات الجيوسياسية، وتتصارع داخله معاني الأمن والحرية في زمن لا حدود فيه للمعلومة.

2. التاريخ والتطور: جذور التعاون الاستخباراتي والتوسّع إلى الفضاء السيبراني

لدى الولايات المتحدة وإسرائيل تاريخ طويل من التعاون الاستخباراتي الوثيق سبق ظهور عصر الإنترنت. فمنذ خمسينيات القرن الماضي، عملت وكالة الاستخبارات المركزية الأميركية (CIA) وجهاز الموساد الإسرائيلي جنبًا إلى جنب في تبادل المعلومات حول التهديدات الإقليمية. ويؤكد مسؤولو الاستخبارات السابقون متانة هذه العلاقة؛ إذ أشار مدير الـCIA الأسبق جون برينان إلى أن الوكالة تتبادل "أكثر المعلومات حساسية" مع الموساد بفضل مستوى عالٍ من الثقة المتبادلة. وبدوره ذكر تامير باردو، الرئيس الأسبق للموساد، أن مستوى التعاون بين الجهازين بلغ درجة غير مسبوقة تاريخيًا رغم أي خلافات سياسية عابرة بين قيادتي البلدين. هذا الأساس المتين في الشراكة الاستخباراتية التقليدية مهّد الطريق لتوسيع نطاق التعاون إلى مجال الأمن السيبراني مع تطور التهديدات التكنولوجية (Harvard Gazette, 2021).

برز التعاون الأمريكي–الإسرائيلي في الفضاء الرقمي بشكل جلي لأول مرة مع عملية Stuxnet السيبرانية في عام 2010. فقد كُشف عن دودة حاسوبية خبيثة استهدفت أجهزة الطرد المركزي النووية الإيرانية وعطّلتها، وتبيّن أنها نتاج جهد مشترك بين الاستخبارات الأمريكية والإسرائيلية. شكّلت Stuxnet سابقة تاريخية بهجوم سيبراني دمّر بنية تحتية صناعية فعلية، مما أكد انتقال التحالف الاستخباراتي بين البلدين إلى ميدان الحرب الإلكترونية (Congress.gov, 2010).

استمرت خطوات التعاون السيبراني الرسمي في التصاعد. ففي عام 2016، أقرّ الكونغرس الأمريكي قانون الشراكة المتقدمة للبحوث بين الولايات المتحدة وإسرائيل (United States-Israel Advanced Research Partnership Act) لتعزيز التعاون

في أبحاث الأمن الإلكتروني. وبموجب هذا القانون، توسّع نطاق برنامج بحث وتطوير مشترك بين وزارة الأمن الداخلي الأمريكية ووزارة الأمن العام الإسرائيلية ليشمل تقنيات الأمن السيبراني. أتاح ذلك تمويل مشاريع مشتركة وتسريع تحويل الأبحاث السيبرانية إلى تطبيقات تجارية، ما دعم ازدهار قطاع الشركات السيبرانية الناشئة في إسرائيل (CyberScoop, 2016).

بالتوازي مع التعاون الحكومي الرسمي، شهد العقد الماضي تحولًا مهمًا من التجسس الحكومي التقليدي إلى سوق خاصة مزدهرة لبرمجيات التجسس. فخريجو الوحدات السيبرانية الإسرائيلية النخبوية (مثل وحدة 8200 العسكرية) أسّسوا شركات خاصة طوّرت أدوات اختراق متقدمة تُباع تجاريًا لحكومات حول العالم. تُعد مجموعة إن إس أو ("NSO Group") التي تأسست في عام 2010 مثالًا بارزًا، إذ أنشأها ضباط سابقون في وحدة 8200 وحققت نجاحًا عالميًا من خلال بيع برنامج التجسس بيغاسوس ("Pegasus"). في البداية، تلقّت "إن إس أو" تمويلًا من مستثمرين دوليين؛ فقد استحوذت شركة الاستثمار الأمريكية فرانسيسكو بارتنرز ("Francisco Partners") في عام 2014 على 70% من أسهمها مقابل 130 مليون دولار، مما يعكس انخراط رأس المال الأمريكي مبكرًا في هذه الصناعة (TechCrunch, 2024).

وفي السنوات اللاحقة ظهرت شركات إسرائيلية أخرى كسرت احتكار "إن إس أو"، منها شركة باراغون سوليوشنز ("Paragon Solutions") التي تأسست عام 2019 بقيادة قدامى وحدة 8200 وبدعم شخصيات مثل رئيس الوزراء الأسبق إيهود باراك. وقد جذبت "باراغون" أيضًا استثمارات أمريكية كبيرة من صناديق رأس مال مخاطر مثل باتري فنتشرز ("Battery Ventures"). وهكذا يمكن القول إن البنية التحتية للصناعة السيبرانية الإسرائيلية بُنيت بدعم مالي وتقني أمريكي جزئيًا، في حين استفادت الأجهزة الأمريكية من ابتكارات نظرائها الإسرائيليين (Reuters, 2024; WIRED, 2024).

شهد التعاون الأمريكي–الإسرائيلي في هذا القطاع محطات لافتة. فعلى سبيل المثال، كشفت تقارير صحفية في عام 2022 أن مكتب التحقيقات الفيدرالي ("FBI") حصل على ترخيص لاختبار برنامج "بيغاسوس" فعليًا في عام 2019، في عهد إدارة ترامب. ورغم تأكيد الـ"إف بي آي" أنه لم يُشغّل البرنامج عمليًا في تحقيقات داخلية، إلا أنه أنفق قرابة 5 ملايين دولار على عقد العام الأول ثم 4 ملايين للتجديد، مبررًا ذلك بالحاجة إلى فهم التقنيات الحديثة ومخاطر وقوعها في الأيدي الخطأ (The Guardian, 2022). أثار هذا الكشف ضجة حيث جاء في وقت كانت إدارة بايدن تضع "إن إس أو" على القائمة السوداء، لكنه أظهر أيضًا اهتمام الأجهزة الأمنية الأمريكية بالحصول على أدوات التجسس الإسرائيلية المتقدمة ولو لغرض التجربة والتقييم.

باختصار، تطور التعاون الأمريكي–الإسرائيلي من تاريخ طويل من الثقة الاستخباراتية إلى شراكة وثيقة في ساحة الأمن السيبراني. وساهم الدعم التشريعي والمالي الأمريكي في تمكين قطاع التجسس السيبراني الإسرائيلي، في حين استفادت الولايات المتحدة من التقنيات الإسرائيلية سواء عبر الشراء المباشر أو التعاون البحثي والتدريبي. هكذا بُنيت منظومة معقّدة تجمع التكنولوجيا بالسياسة، وتمهد لفهم المشهد الحالي لصناعة برامج التجسس.

3. المنتجات والتقنيات الإسرائيلية: Pegasus وGraphite وأدوات المراقبة المتقدمة

أحدثت برمجيات التجسس الإسرائيلية طفرة في قدرات الاختراق والمراقبة الرقمية بفضل تقنياتها المتطورة. ويُعتبر برنامج Pegasus الذي تطوره مجموعة NSO، والذي ذكرناه سابقا، أبرز مثال على ذلك، إذ ذاع صيته عالميًا كأحد أقوى أدوات التجسس على الهواتف الذكية. من الناحية التقنية، يعد Pegasus برمجية خبيثة متقدمة تُمكّن مشغّلها من السيطرة شبه الكاملة على هاتف

الضحية. فبمجرد إصابة الجهاز، يستطيع المهاجم استخراج الرسائل النصية والصور ورسائل البريد الإلكتروني والمحادثات المشفرة، وتسجيل المكالمات الهاتفية، بل وحتى تشغيل الكاميرا والميكروفون للتنصت دون علم صاحب الهاتف. الأخطر من ذلك أن Pegasus يعتمد على هجمات "دون نقر" (Zero-click) لا تتطلب أي تفاعل من الضحية لبدء الاختراق. فقد استغلّ مطوّروه ثغرات "اليوم الصفري" في تطبيقات المراسلة وأنظمة التشغيل، مما يتيح حقن البرنامج في الجهاز عبر رسالة غير مرئية (كخدمة iMessage مثلًا) دون حاجة لنقر رابط. وهذا يجعل الهجوم غير قابل عمليًا للإيقاف من قبل المستخدم المستهدف أو حتى كثير من وسائل الحماية التقليدية (The Guardian, 2023; Human Rights Watch, 2023).

جرى توثيق قدرات Pegasus عبر تحقيقات تقنية رصينة. فعلى سبيل المثال، أكدت تحليلات مختبر الأمن التابع لمنظمة العفو الدولية أن Pegasus يستطيع الاختراق الخفي لأجهزة iPhone وأندرويد ومن ثم تفريغ كم هائل من البيانات الشخصية الحساسة (The Guardian, 2023). ولا يترك البرنامج أثرًا يُذكر بعد إتمام مهمته، مما يصعّب اكتشافه. وقد وصفت إحدى ضحاياه – وهي مديرة في منظمة هيومن رايتس ووتش – تجربتها بالقول إنها تعرضت لهجمات متكررة دون أن تضغط على أي رابط ولم يكن بوسعها فعل شيء لإيقاف ذلك (Human Rights Watch, 2023). هذا المستوى من التطور جعل Pegasus مرادفًا لقمة التجسس الرقمي الحديث، وبفضله باعت NSO منتجاتها لعشرات الحكومات.

في مواجهة شهرة بيغاسوس ("Pegasus")، ظهرت أدوات تجسس منافسة تبنت نهجًا تقنيًا مختلفًا. ومن أبرزها برنامج غرافيت ("Graphite") الذي تطوره شركة باراغون الإسرائيلية ("Paragon"). يوفر غرافيت قدرة اختراق مماثلة من حيث السيطرة على الجهاز، لكنه يركّز على جوانب معينة. فوفقًا لمصادر تقنية، يتميّز غرافيت بقدرته على استخراج البيانات من النسخ الاحتياطية السحابية المرتبطة بالهاتف واستهداف تطبيقات المراسلة مثل واتساب وسيغنال وفيسبوك ماسنجر والبريد الإلكتروني جيميل. أي أن غرافيت قد يتجاوز تخزين الجهاز المحلي إلى اختراق حسابات وخدمات سحابية لاستقاء المعلومات منها. وعلى غرار "بيغاسوس"، أكدت الأدلة الحديثة أن غرافيت يمتلك آلية اختراق دون تفاعل من الضحية؛ حيث كشف مختبر سيتزن لاب ("Citizen Lab") في عام 2025 عن استخدام ثغرة عبر آي مسج ("iMessage") لاختراق هاتف صحفي بشكل "غير تفاعلي" (Zero-Click) وإصابة جهازه بـغرافيت . وبعد الاختراق، يستطيع المشغّل الوصول سريًا إلى محتويات تطبيقات التواصل المشفّر على الجهاز تمامًا كما يفعل "بيغاسوس". ويعلق باحث في Citizen Lab أن الضحية لا يشعر بشيء: "خلال لحظة يكون الهاتف ملكك، وفي اللحظة التالية تبدأ بياناته بالتدفق إلى المهاجم"، في إشارة إلى مدى خفاء وسرعة سيطرة Graphite على الجهاز (Associated Press, 2025).

وبالرغم من التقارب في خطورة Pegasus وGraphite، ثمة اختلاف تقني في طريقة عملهما. فشركة NSO صممت Pegasus ليكون شاملًا في اختراق كل وظائف الهاتف (تشغيل الكاميرا، الميكروفون، تتبع الموقع، إلخ)، فيما ركزت Paragon في تسويق Graphite على أنه أكثر انتقائية وربما "أخلاقي" في جمع المعلومات – إذ تدعي أنه يقيّد نفسه باستخراج المحادثات من تطبيقات الدردشة فقط. وبالفعل صرّحت Paragon أنها تضع قيودًا أخلاقية ذاتية على أدواتها بحيث تستهدف فقط محتوى الاتصالات في التطبيقات، ولا تجمع كل بيانات الجهاز. كما تؤكد الشركة أنها تتعامل فقط مع وكالات حكومية في 39 دولة تعتبرها "ديمقراطيات مستنيرة" حسب وصفها (WIRED, 2024).

هذه المزاعم تأتي في سياق محاولة Paragon التمايز عن سمعة NSO التي تلاحقها اتهامات واسعة بانتهاك حقوق الإنسان. ومع ذلك، أظهرت الوقائع أن Graphite يمكن استخدامه بنفس أسلوب Pegasus للتجسس التعسفي؛ فقد كُشف مثلًا عن استهداف نحو 90 مستخدمًا لتطبيق واتساب في أكثر من 20 دولة أوروبية عبر ثغرة استغلها Graphite، وفق إفادات شركة Meta في مطلع عام 2023. وأثبت Citizen Lab إصابة هواتف صحفيين أوروبيين بهذا البرنامج، بينهم صحفيان إيطاليان تلقيا تحذيرات أمنية من آبل وواتساب حول استهداف أجهزتهم (Associated Press, 2023).

إلى جانب الأدوات الموجهة ضد الأفراد، طورت إسرائيل أيضًا منظومات مراقبة جماعية واسعة النطاق تستفيد من البنية التحتية للتكنولوجيا السحابية. ففي تحقيق حديث عام 2025، كُشف أن وحدة الاستخبارات العسكرية الإسرائيلية (وحدة 8200) أقامت مشروعًا طموحًا لتخزين تسجيلات جميع المكالمات الهاتفية التي يجريها الفلسطينيون في الضفة الغربية وقطاع غزة على خوادم لشركة مايكروسوفت. تمكنت الوحدة عبر تعاون مع مايكروسوفت من الحصول على قسم خاص ومحصن ضمن منصة Azure السحابية لتخزين هذه الكمية الهائلة من الاتصالات. ووفق مصادر استخباراتية، جاء هذا القرار بعدما أدركت الوحدة أنها لا تمتلك قدرة تخزينية أو حاسوبية داخلية تستوعب "ملايين المكالمات في الساعة" التي تريد اعتراضها. وقد طُبق المشروع فعليًا منذ عام 2022، حيث تقوم أنظمة تنصت تابعة للوحدة بتسجيل ملايين المحادثات اليومية بين الفلسطينيين ثم رفعها إلى سحابة Azure للاحتفاظ بها لفترات طويلة. وأظهرت وثائق مسرّبة أن جزءًا كبيرًا من هذه البيانات الحساسة يُخزن في مراكز بيانات مايكروسوفت في أوروبا (هولندا وأيرلندا)، ما يثير إشكالات قانونية وأخلاقية جسيمة حول الخصوصية وسيادة البيانات (The Guardian, 2025).

الأخطر أن هذه المنصة السحابية لم تكن أرشيفًا خاملاً فحسب، بل دُمجت مع أدوات تحليلية متقدمة لاستخلاص معلومات استخبارية قابلة للتنفيذ. فقد استخدمت وحدة 8200 تقنيات الذكاء الاصطناعي لمسح وفهرسة الكم الهائل من المكالمات والنصوص بحثًا عن مؤشرات تهديد. على سبيل المثال، طُوّر نظام ضمن المشروع يقوم بمسح جميع الرسائل النصية بين الفلسطينيين وتصنيفها بحسب مستوى الخطورة باستخدام خوارزميات ترصد كلمات مفتاحية تتعلق بالأسلحة أو نوايا مشبوهة. وتصف مصادر في الوحدة هذا التحول بأنه "ثورة" في نهج المراقبة انتقل من تعقب أهداف محددة إلى مراقبة "الجميع طوال الوقت" بهدف التنبؤ الاستباقي بالتهديدات. علاوة على ذلك، تفيد مصادر عسكرية بأن هذه البيانات جرى استغلالها خلال الحرب على غزة (2023–2025) في تحديد أهداف لضربات جوية عبر تحليل مكالمات الأشخاص في مواقع معينة قبل القصف. هذا الاستخدام يوضح التكامل بين أدوات التجسس الرقمية والبنى العسكرية العملياتية (The Guardian, 2025).

باختصار، تقنيات التجسس الحديثة التي طورتها إسرائيل وشركاؤها تتراوح بين أدوات فردية خارقة تمكن من اختراق أي هاتف ذكي تقريبًا، وبين منصات مراقبة شاملة للشعوب بأكملها باستخدام سحابات تخزين عملاقة وذكاء اصطناعي. لقد نقلت Pegasus وGraphite وأمثالهما التجسس الإلكتروني إلى مستويات غير مسبوقة من التوغل في الحياة الرقمية، وأصبحت التكنولوجيا بذلك أداة بيد السلطة يمكن أن تستخدم للقمع.

4. المال والتقنية بين واشنطن وتل أبيب

ازدهار صناعة برامج التجسس لم يكن مدفوعًا فقط بالطلب الأمني، بل تغذّى أيضًا من استثمارات مالية كبيرة وصفقات ملكية عابرة للحدود، لعب فيها رأس المال الأمريكي دورًا ملحوظًا. فرغم أن شركات مثل إن إس أو ("NSO") وباراغون ("Paragon")

انطلقت من إسرائيل، إلا أن الاستثمار الأمريكي أسهم بقوة في نموها، مما خلق شبكة مصالح اقتصادية معقدة بين القطاعين الأمني والتجاري في البلدين (TechCrunch, 2024).

في بدايات مجموعة إن إس أو("NSO Group") ، سارعت صناديق الاستثمار الأمريكية إلى الدخول في هذا القطاع الواعد. وكما سلف، استحوذت شركة فرانسيسكو بارتنرز ("Francisco Partners") الأميركية على حصة الأغلبية في إن إس أو عام 2014 ، لتضخ السيولة اللازمة لتوسع الشركة عالميًا. وبقيت تلك الحصة بيدها حتى 2019 حين اشتراها مجددًا مؤسسو إن إس أو الإسرائيليون ليستعيدوا السيطرة . ولكن خلال فترة الملكية الأمريكية، نما حجم أعمال إن إس أو بشكل مضطرد وأبرمت عقودًا جديدة حول العالم. وليس فرانسيسكو بارتنرز حالة منفردة؛ إذ كشفت رسائل بريد إلكتروني مسربة عام 2015 أن الشركة ذاتها كانت مهتمة أيضًا بالاستثمار في شركة إيطالية منافسة هي هاكينج تيم ("Hacking Team") قبل انهيار الأخيرة. يوضح ذلك أن المستثمرين الأمريكيين رأوا مبكرًا فرصًا ذهبية في سوق السايبر الهجومي وسعوا لبناء محافظ متنوعة فيه.

لم يقتصر الأمر على الصناديق الخاصة، بل امتد إلى شركات استثمار ضخمة ومجموعات دفاعية. ففي ديسمبر 2024، أُعلن أن شركة إيه إي إندستريال بارتنرز ("AE Industrial Partners") الأمريكية (ومقرها فلوريدا) – المختصة بالاستثمار في قطاعات الطيران والأمن – استحوذت على شركة باراغون سوليوشنز ("Paragon Solutions") الإسرائيلية بصفقة قدرها 500 مليون دولار (قد ترتفع إلى 900 مليون بحسب الأداء). هذه الصفقة حظيت بموافقة الجهات الرسمية في كل من واشنطن وتل أبيب، ما يعكس وجود ضوء أخضر سياسي على أعلى المستويات لمثل هذه الاندماجات الحساسة. ووفق التقارير، يخطط المستثمر الأمريكي لدمج "باراغون" مع شركة أمريكية أخرى هي ريد لاتيس ("Red Lattice") المتخصصة في الأمن السيبراني، بغية إنشاء كيان أقوى يخدم السوق الأمريكية والحلفاء الغربيين "بأدوات مراقبة مسؤولة" (Reuters, 2024).

ومن الجدير بالذكر أن "باراغون" منذ تأسيسها حرصت على استقطاب تمويل من صناديق أمريكية مرموقة مثل باتري فنتشرز ("Battery Ventures") وريد دوت كابيتال ("Red Dot Capital")، بل إنها استعانت بشركات استشارات وعلاقات حكومية في واشنطن مثل ويست إكزك أدفايزرز ("WestExec Advisors") – التي شارك في تأسيسها وزير الخارجية الحالي أنتوني بلينكن – لتسهيل دخولها للسوق الأمريكي وتأمين علاقات مع الزبائن الحكوميين. هذه الجهود آتت أُكلها؛ فبالإضافة لعقد وكالة الهجرة والجمارك الأمريكية ("ICE") عام 2024، نُقل عن مصادر أن وكالة مكافحة المخدرات الأمريكية ("DEA") استخدمت برنامج "باراغون" في عمليات سابقة. كما أن "باراغون" نجحت في تفادي أي عقوبات أمريكية أو إدراج على قوائم سوداء، بخلاف "إن إس أو"، وربما يعود ذلك جزئيًا إلى حملة ضغط (لوبي) نشطة في واشنطن أنفقت فيها مئات آلاف الدولارات (WIRED, 2024).

لكن دخول المستثمرين الأمريكيين بهذا الزخم أثار تساؤلات حول مدى استمرار السيطرة الإسرائيلية على شركاتها السيبرانية. فعلى سبيل المثال، حين ظهرت أنباء اهتمام شركة الدفاع الأمريكية إل ثري هاريس ("L3Harris") بشراء تقنية بيغاسوس ("Pegasus") عام 2022، تخوّف مسؤولو الأمن الإسرائيلي من فقدان التحكم وتقييد زبائن "إن إس أو" المستقبليين. وبالفعل، تضمنت خطة "إل ثري هاريس" (التي أُحبطت لاحقًا) تحويل "إن إس أو" لخدمة مجموعة صغيرة من الدول الحليفة (خمس عيون والناتو) تحت إشراف أمريكي. وقيل إن هذه المباحثات لاقت دعمًا ضمنيًا من بعض أوساط الاستخبارات الأمريكية التي رأت مصلحة في امتلاك واشنطن لتقنية "بيغاسوس"، لكن البيت الأبيض عارضها بشدة لأسباب تتعلق بالأمن القومي ومخاوف التفاف إسرائيل على العقوبات. انتهت الصفقة المقترحة بالتوقف التام بعد إعلان البيت الأبيض رفضه الصارم لها (The Guardian, 2022).

وبشكل عام، يمكن القول إن الولايات المتحدة أصبحت من أكبر المستثمرين والعملاء في قطاع التجسس السيبراني الإسرائيلي. هذا الواقع أوجد شبكة مصالح اقتصادية–أمنية بين البلدين: فشركات إسرائيلية كـ"إن إس أو" و"باراغون" تجد في السوق الأمريكي مصدرًا للأموال والخبرة وفرصة للنمو "الشرعي"، مقابل حصول مؤسسات الأمن الأمريكية على تقنيات متقدمة ربما تفتقر لها محليًا. ومع ذلك، ترافق هذا مع توترات داخلية، فبعض دوائر صنع القرار الأمريكي قلقة من توسيع هذه السوق لما قد تسببه من انتشار غير مضبوط لتقنيات خطرة. أما إسرائيل، فتحاول الموازنة بين دعم قطاع تقني يعتبر مصدر دخل ونفوذ دبلوماسي، وبين ضبطه تحت إشراف وزارة الدفاع كي لا يخرج عن السيطرة أو يورطها دوليًا (TechCrunch, 2024; WIRED, 2024).

بالنتيجة، أدت تدفقات التمويل والاستحواذات عبر الأطلسي إلى إعادة تشكيل القطاع: فمن جهة وفرت للشركات الإسرائيلية سيولة وحواضن كبرى للنمو (كما في حالة "باراغون" مع "إيه إي بارتنرز")، ومن جهة أخرى أعطت الولايات المتحدة موطئ قدم مباشر للتحكم في دفة هذه التقنيات – أو على الأقل منع خصومها من الوصول إليها. بيد أن هذا التغلغل المالي يحمل مخاطر أيضًا، إذ يطمس الخط الفاصل بين القطاعين العام والخاص في مسائل التجسس، وقد يفتح بابًا خلفيًا لنفوذ متبادل بين الأجهزة الاستخباراتية والشركات الاستثمارية.

5. الاعتبارات القانونية وحقوق الإنسان: صراع بين مقتضيات الأمن والمساءلة

أثار الانتشار الواسع لبرمجيات التجسس الإسرائيلية وتبعات إساءة استخدامها موجة من التحديات القانونية والنقاشات الحقوقية على المستوى الدولي. فمن جهة، تؤكد الشركات المنتجة وحكومات الزبائن على أهمية هذه الأدوات لأمن المواطنين، ومن جهة مقابلة تشير منظمات حقوق الإنسان إلى الانتهاكات الجسيمة للخصوصية والحريات الناتجة عنها، داعية إلى محاسبة المستخدمين والمطورين على حد سواء. وفي خضم ذلك، تصاعدت الجهود القضائية والتنظيمية لمحاولة ضبط هذه الصناعة ومساءلة الأطراف الضالعة في التجاوزات.

على الصعيد القانوني، تواجه شركة إن إس أو غروب ("NSO Group") الإسرائيلية سيلًا من الدعاوى القضائية في محاكم متعددة. إحدى أبرز هذه القضايا هي دعوى شركة ميتا ("Meta") المالكة لتطبيق واتساب ("WhatsApp") ضد "إن إس أو"، حيث اتهمت "واتساب" الشركةَ الإسرائيلية باختراق خوادمها عام 2019 لاستغلالها في إصابة نحو 1400 هاتف مستخدم ببرنامج بيغاسوس ("Pegasus"). وبعد معركة قانونية مطولة في المحاكم الأمريكية، مُنيت "إن إس أو" بنكسة كبيرة حين رفضت المحكمة العليا الأمريكية في أوائل 2023 طعنها بطلب الحصانة السيادية، مما مهد الطريق لإدانتها وتعويض شركة "ميتا" بـ168 مليون دولار. كما رفعت شركة آبل ("Apple") دعوى مماثلة تسعى فيها لمنع "إن إس أو" من استخدام برمجياتها، وأطلقت تحديثات أمنية تضمنت "وضع القفل" ("Lockdown Mode") لحماية المستخدمين (Associated Press, 2023).

إضافةً للدعاوى المدنية، وجدت "إن إس أو" نفسها في مواجهة عقوبات حكومية مباشرة أثرت بعمق على أعمالها. فقد أدرجت وزارة التجارة الأمريكية في نوفمبر 2021 شركتي "إن إس أو" وكانديرو ("Candiru") على "قائمة الكيانات" السوداء ("Entity List")، وهو ما حظر أي تعامل تجاري معها دون ترخيص خاص. واستندت الوزارة في قرارها إلى أدلة على أن تقنيات "إن إس أو" استُخدمت لاستهداف صحفيين ونشطاء، في خرقٍ للسياسة الخارجية الأمريكية. كما فرضت وزارة الخزانة الأمريكية عام 2023 عقوبات على مجموعة إنتيليكسا ("Intellexa")، في حين أعلنت وزارة الخارجية عن سياسة جديدة تقضي بفرض قيود تأشيرات

على مطوري أو مستخدمي برامج التجسس لأغراض غير مشروعة (Reuters, 2021; The Washington Post, 2023; WIRED, 2023).

دوليًا، تنامت الدعوات إلى وضع إطار تنظيمي عالمي يحد من الانتشار غير المنضبط لبرمجيات المراقبة. ففي يناير 2025، عقد مجلس الأمن بالأمم المتحدة جلسة خاصة حول برمجيات التجسس بدعوة من الولايات المتحدة ودول أوروبية، لبحث سبل تعزيز ضوابط التصدير عبر اتفاقات دولية. كما شاركت دول عدة في عملية بال مول ("Pall Mall Process") بقيادة بريطانيا لإرساء مبادئ تنظّم التجارة في هذه الأدوات. وفي السياق ذاته، أطلقت إدارة بايدن خلال قمة الديمقراطية لعام 2023 مبادرة دولية ضمت 11 دولة في بدايتها، ارتفع عددها لاحقًا إلى 23، بهدف تبادل المعلومات حول صادرات برامج التجسس وضمان استخدامها ضمن المعايير الحقوقية (American University, 2025; The Washington Post, 2023).

أحد أبرز التحديات في مسألة المساءلة القانونية هو الطبيعة العابرة للحدود لهذه الصناعة المحاطة بالسرية. فغالبًا ما تُبرم العقود بين شركات التجسس والحكومات ضمن تصنيفات أمنية سرية تعيق المحاكم من الوصول إلى المعلومات. وقد واجهت لجان برلمانية في المجر وبولندا وإسبانيا صعوبات في التحقيق في فضائح بيغاسوس ("Pegasus") بسبب رفض الحكومات الكشف عن الوثائق بحجة الأمن القومي، فيما منحت وزارة الدفاع الإسرائيلية تراخيص تصدير سرية لتلك الشركات، مما عقد الجهود المحلية والدولية لمحاسبتها (The Washington Post, 2023).

لكن رغم هذه العقبات، شهدنا مؤشرات على تقدم جزئي في محاسبة بعض الشركات. فبالإضافة إلى حكم التعويضات لصالح "ميتا"، واجهت "إن إس أو" أوامر قضائية في إسرائيل بشأن ديونها، وأُجبرت شركة كوادريم ("Quadream") الإسرائيلية – التي أسسها مدير سابق في "إن إس أو" – على الإغلاق في عام 2023 بعد فضح استخدامها في عمليات اختراق. ووفق مسؤولين أمريكيين، بدأت الاستراتيجية الأمريكية المعروفة بـ"قطع الإمدادات" تؤتي ثمارها، إذ تراجعت قدرة الشركات المعاقبة على التحرك المالي عالميًا وأصبح مدراؤها يخشون القيود على السفر (The Washington Post, 2023; Associated Press, 2023).

غير أن الواقع لا يزال يشير إلى قدرة هذه الشركات على المراوغة. فقد أظهرت دراسة مشتركة عام 2024 صادرة عن المجلس الأطلسي ("Atlantic Council") والجامعة الأمريكية ("American University") أن العديد من الشركات المعاقبة تعيد تسمية نفسها وتؤسس كيانات جديدة في دول أخرى لتجنب الرقابة والعقوبات. فعلى سبيل المثال، بعد إدراج "إنتيليكسا" على قائمة العقوبات الأمريكية، أغلقت موقعها الإلكتروني، لكن فروعها استمرت بالعمل تحت أسماء مختلفة في دول لم تُدرج ضمن العقوبات. ويؤكد الخبراء أن هذا التلاعب الهيكلي يبرهن على قصور المساءلة الحالية والحاجة لتنسيق دولي أقوى لسد الثغرات القانونية (The Washington Post, 2024; American University, 2025).

6. الخاتمة

يكشف هذا البحث، عبر محاوره المتعددة، عن أن التعاون الأمريكي–الإسرائيلي في صناعة وبرمجة التجسس لم يعد مجرد علاقة تقنية أو استخباراتية، بل تحوّل إلى بنية استراتيجية متكاملة تجمع بين الاقتصاد والأمن والسياسة والقانون. فمنذ بدايات التعاون في الأمن السيبراني، تطورت الشراكة لتصبح منظومة مؤسسية متشابكة تشمل التشريعات، وتمويل الشركات، وتبادل الخبرات، وتنسيق السياسات الدولية في فضاء المراقبة الرقمية.

تُظهر النتائج أن إسرائيل مثّلت المختبر التطبيقي للتقنيات الهجومية الرقمية، بينما وفّرت الولايات المتحدة رأس المال والغطاء القانوني والسياسي لتوسيع هذه الصناعة عالميًا. هذا التفاعل خلق حالة تبادل نفوذ فريدة: فإسرائيل صدّرت التكنولوجيا واحتفظت بالخبرة العملياتية، في حين استثمرت واشنطن في الشركات الإسرائيلية ووجهت بوصلتها نحو الاستخدامات المتوافقة مع مصالحها الأمنية. وهكذا أصبح الفضاء السيبراني ساحة تعاون مشترك ولكن أيضًا مجال تنافس مضمر، حيث يسعى كل طرف للحفاظ على تفوقه الاستخباراتي دون المساس بشفافية التحالف. اقتصاديًا، رسّخ التمويل الأمريكي والاستحواذات المتبادلة مكانة إسرائيل كمركز عالمي لتطوير أدوات التجسس، وحوّل التعاون الثنائي إلى تحالف صناعي–استخباراتي متكامل يمتد من المختبرات إلى الأسواق العالمية.

المراجع:

Al Jazeera. (2023). Israeli police accused of using Pegasus spyware without court order. https://www.aljazeera.com

Associated Press. (2023). Meta says Graphite spyware targeted 90 WhatsApp users across Europe. https://apnews.com

Associated Press. (2025). Citizen Lab confirms Graphite zero-click exploit on journalist iPhone. https://apnews.com

Congress.gov. (2010). Stuxnet cyber operation report. https://www.congress.gov

CyberScoop. (2016). One of two U.S.-Israel cybersecurity cooperation bills signed. https://www.cyberscoop.com

Harvard Gazette. (2021). Intel agencies in an age of ‘nuclear’ cyberattacks. https://news.harvard.edu

Human Rights Watch. (2023). Spyware and human rights violations linked to Pegasus use. https://www.hrw.org

Reuters. (2024). Israeli spyware firm Paragon acquired by U.S. investment group. https://www.reuters.com

TechCrunch. (2024). Israeli spyware maker NSO and the rise of Pegasus. https://techcrunch.com

TechCrunch. (2024). Paragon’s Graphite spyware and U.S. contracts. https://techcrunch.com

The Guardian. (2022). FBI confirms it obtained NSO's Pegasus spyware. https://www.theguardian.com

The Guardian. (2023). Pegasus spyware and the rise of Israeli cyberpower. https://www.theguardian.com

The Guardian. (2025). Israel's Unit 8200 uses Microsoft Azure to store Palestinian call data. https://www.theguardian.com

WIRED. (2024). ICE signs $2 million contract with spyware maker Paragon Solutions. https://www.wired.com

WIRED. (2024). Inside Paragon: The 'ethical' spyware company competing with NSO. https://www.wired.com