مهاب عادل *

البلقنة الإلكترونية
وأدوات التأثير الجديدة لإسرائيل

أزاحت قضايا التجسس الإلكتروني الإسرائيلية عبر برامج تكنولوجية متقدمة يتم من خلالها مراقبة المستخدمين لشبكات الاتصال ومنصات التواصل الاجتماعي، الستار عن أدوات جديدة تطورها إسرائيل للتأثير في الفضاء الإلكتروني وتوجيه الرأي العام سواء أكان ذلك تحت مظلة الأنشطة الاستخباراتية للتجسس أم مزاحمة القوى التكنولوجية المتقدمة في هذا المجال الرائج من الناحية الاقتصادية.

يبرز هذا التوجه في ظل تصاعد الحديث عن اتجاه بعض الدول نحو ما يُعرف بـ «بلقنة الإنترنت» (Cyberbalkanization) بحيث تقوم ببناء شبكتها الخاصة بها دون الاستعانة بالخارج لفرض حالة من العزلة المعلوماتية على مواطنيها بدافع تعزيز الرقابة والسيطرة المحلية على المحتوى المتداول على الشبكة المعلوماتية تحت مظلة حماية الأمن القومي للبلاد. ومن النماذج الواضحة في هذا الشأن شبكة «كوانجميونج» في كوريا الشمالية، وشبكة «حلال إنترنت» في إيران، وشبكة «رونت» الروسية.

هذا فضلًا عن توجه بعض الدول الديمقراطية لفرض قيود وضوابط على استخدامات مواطنيها للشبكة المعلوماتية، فعلى سبيل المثال تتجه بريطانيا لتطبيق الضوابط على وسائل التواصل الاجتماعي مع خطط لإدخال تشريعات «الأضرار الرقمية»،[1] كما أنها على وشك تطبيق الرقابة على المواقع الإباحية بالنسبة للبالغين. بالإضافة إلى تحكمها الهادئ في الصحافة الإلكترونية من خلال استخدام إشعارات (DSMA) المعروفة باسم إرشادات وسائط الدفاع والأمن.[2] وخلال أزمة الحرب الأوكرانية الأخيرة، اتجه عدد من الدول الأوروبية لحجب المواقع الإخبارية الروسية على شبكة الإنترنت داخل حدودها في إطار عقابي لتلك الوسائل الإعلامية الروسية.

* باحث مصري مختص في الشأن الإسرائيلي

«التكنولوجيا ركيزة أساسية للمفهوم الأمني في إسرائيل».

ومؤخـرًا كشـف تحقيـق اسـتقصائي أجـراه «اتحـاد الصحافيـين الدوليـين»، وصحيفـة «الغارديـان» البريطانية، خـلال شـباط ٢٠٢٣، عـن تـورط إسرائيـل بالتلاعـب في انتخابـات جـرت في أكثـر مـن ٣٠ دولـة حـول العالـم، باسـتخدام مجموعـة مـن الأدوات والبرامـج السريـة التـي ضللـت الـرأي العـام.[٣] ومـن قبـل ذلـك كانـت فضيحـة تجسـس برنامـج بيغاسـوس الـذي طورتـه مجموعـة «إن. إس.أو» الإسرائيليـة (NSO)، الـذي اسـتخدم للتجسـس عـلى صحافيـين وناشـطين حـول العالـم، إلى جانـب رؤسـاء دول ودبلوماسـيين وأفـراد عائـلات ملكيـة.[٤]

ومـن ثـم، تفـرض تلـك المعطيـات الحاجـة إلى فهـم التحـولات الناشـئة في الفضـاء الرقمـي، ومـا يمكـن تسـميته بــ «السـباق السـيبراني» بـين القـوى الكـبرى مـن أجـل التأثـير وتوجيـه دفـة الـرأي العـام العالمـي حـول العديـد مـن القضايـا المحليـة والدوليـة، بمـا يخـدم مصالحهـم. وذلـك بالتطبيـق عـلى الحالـة الإسرائيليـة ومحاولاتهـا توظيـف تلـك التكنولوجيـا لخلـق فـرص اخـتراق حقيقيـة تسـمح لهـا بكـسر حالـة العزلـة التـي واجهتهـا طيلـة العقـود الماضيـة، عـبر إيجـاد أرضيـات مشـتركة للتعـاون السـيبراني مـع شركاء جـدد. وكذلـك توظيفهـا في إطـار إسـتراتيجيتها الأمنيـة المرنـة لـردع الخصـوم دون اللجـوء للمواجهـة الماديـة الخشـنة التـي سـتترتب عليهـا تكلفـة تحـاول تـل أبيـب باسـتمرار تجنبهـا.

أولًا: نظريتا «التعرض الانتقائي والتنافر المعرفي» .. مدخل للفهم

اتجهـت الدراسـات المبكـرة لبحـث مسـألة التعـرض الانتقائـي لـدى مسـتخدمي وسـائل الإعـلام، حيـث ركـز البحـث الأول مـن نوعـه الـذي أجـراه «جوزيـف كلابـر»، عـلى الربـط بـين الذاتيـة والتعـرض لوسـائل الإعـلام بغـرض فهـم المواقـف الاجتماعيـة. حيـث وجـد أن المحتـوى الإعلامـي لـه تأثـيرات محـدودة فقـط عـلى الـرأي العـام. وأشـارت نتائـج دراسـته إلى أن الأفـراد لديهـم ميـل قـوي للانخـراط في التعـرض الانتقائـي للمعلومـات عندمـا يكـون لديهـم بالفعـل معتقـدات ثابتـة حـول موضـوع مـا. بالإضافـة إلى ذلـك، وجـد أن المواقـف الاجتماعيـة تميـل إلى أن تصبـح أكثـر تطرفًـا بمـرور الوقـت بسـبب التكـرار المطـول للمعلومـات السـاكنة.[٥]

ووفقًـا لازارسـفيلد وآخريـن، فـإن «التعـرض دائمًـا انتقائـي؛ حيـث توجـد علاقـة إيجابيـة بـين آراء النـاس ومـا يختـارون الاسـتماع إليـه أو قراءتـه». ويعـد «أقـوى شـكل مـن أشـكال التعـرض الانتقائـي هـو أن الأفـراد يفضلـون التعـرض للاتصـالات التـي تتفـق مـع آرائهـم الموجـودة مسـبقًا». ومـن ثـم، يُعتقـد أن الأفـراد يبحثـون بنشـاط عـن المـواد التـي تدعـم آراءهـم، ويتجنبـون بنشـاط المـواد التـي تتعـارض معهـا.[٦]

بينمـا ركـز هـذا النـوع مـن البحـث عـلى وسـائل الإعـلام وانتقائيـة المسـتخدم، ركـزت مجموعـة أخـرى كبـيرة مـن

المؤلفات على ما إذا كانت هذه النتائج ذات صلة بالفضاء السيبراني. وأصبحت إحدى النظريات الأولى التي تتعلق بالانتقائية لأنماط نشاط الإنترنت تُعرف باسم «البلقنة الإلكترونية»، ويُعرَّف مستخدم الإنترنت في «Cyber Balkan» بأنهم الأشخاص الذين يميلون إلى تعريف «مجتمعهم» بشكل أساسي من حيث أولئك الذين يشاركون قيمهم بغض النظر عن القرب المادي، يفضلون أن يكونوا محاطين بآخرين مشابهين عبر الإنترنت.[٧] وتبعًا لذلك، يعرضون أنفسهم بشكل انتقائي إلى مواقع الويب حيث يتوقعون من الآخرين تأكيد وجهات نظرهم الموجودة مسبقًا. ووفقًا لهذه النظرية، فإن الدافع وراء Cyber Balkan هو الرغبة في الحفاظ على الشعور باليقين في معتقداتهم السابقة، ومن المرجح أن يعبروا عن الغضب تجاه المعارضة السياسية.[٨]

هنا تجدر الإشارة إلى أن وظيفة الإنترنت تعمل على جعل التعرض السلبي أكثر صعوبة، والبحث عن المعلومات الانتقائية أسهل مما كان عليه في الماضي.[٩] ووفقًا لفريدمان يميل أولئك الذين ينخرطون في السياسة عبر الإنترنت إلى الانخراط في أنماط «التعرض الانتقائي» (Selective Exposure)، التي يتم تحديدها من خلال تفضيل الأفراد للاهتمام بالمعلومات التي من المرجح أن تؤكد وجهات نظرهم الموجودة مسبقًا. كما يؤكد على دور منفعة المعلومات في قيادة اختيار المعلومات المتوافقة أو المتناقضة في المواقف.[١٠]

يشبه هذا المفهوم إلى حدّ كبير نظرية «ليون فيستنجر» عن «التنافر المعرفي» (Cognitive Dissonance)، حيث يتجنب الأفراد بنشاط عدم تأكيد المعلومات بسبب كرههم للشعور بعدم اليقين أو الغموض. تساعد هذه التفسيرات بدورها على فهم أسباب تطوير أولئك الذين يستخدمون الوسائط الجماعية والاجتماعية للمعلومات السياسية مستويات أعلى من اليقين وأقصى المواقف بمرور الوقت.[١١]

تدريجيًا، أصبحت المنصات عبر الإنترنت تتبنى عادةً نشاط المستخدم المرتبط بالتعرض الانتقائي للأخبار وتشجعه. وأصبحت أنماط التعرض للتحيز الإخباري على نحو متزايد نتيجة ثانوية للتقنيات التي صممت نفسها حول مبادئ التعرض الانتقائي. على سبيل المثال المواقع مثل Facebook، من خلال تصميم خوارزمياته، يعرض للمستخدمين عن قصد المعلومات التي يميلون إلى «الإعجاب» بها من أجل منح جمهوره تجربة ممتعة.[١٢]

تجدر الإشارة إلى أن هذه الممارسة لا تُجرى حصريًا عن طريق مواقع الأخبار على الإنترنت. وإنما تحدد أيضًا مؤسسات الإعلام الجماهيري الحزبية المحتوى بناءً على ما يعتقدون أن جمهورهم يريدون رؤيته، والذي أثبت أنه إستراتيجية عمل مربحة للغاية.[١٣] وبالتالي، تعكس هذه المداخل النظرية ملامح التحول التي أحدثتها الثورة التكنولوجية في عالم الفضاء الرقمي، وطبيعة تفاعل السلوك الإنساني مع تلك التحولات خاصة في ما يتعلق باستقاء المعلومات وتشكيل المواقف الذاتية تجاه القضايا المجتمعية والسياسية. حيث سهّل السلوك الانتقائي في التعرض للمعلومات المتوافقة مع آراء الشخص ومواقفه السابقة وفقًا لنظريتي التعرض الانتقائي والتنافر المعرفي، عملية الاختراق والتضليل المعلوماتي التي تقوم بها شركات تكنولوجيا المعلومات وشركات السوق الرقمي لتوجيه آراء الأفراد وسلوكهم الاستهلاكي تجاه السلع السياسية والاقتصادية المتوافقة مع ميولهم الشخصية ووفقاً لما يُعرف بـ «خوارزميات الفلترة».

هنا تجدر الإشارة إلى أن هذا التوجه السلوكي للأفراد، بالإضافة إلى توجه بعض الدول لتطبيق ما يسمى بـ «البلقنة الإلكترونية»، من خلال إنشاء شبكة انترنت خاصة يسهل التحكم في محتواها، لتقييد عملية الاختراق التي تقوم بها الشركات التكنولوجيا المملوكة للقوى الكبرى المسيطرة على السوق الرقمي العالمي وتطبيقاته المختلفة. فإن هذه التوجهات تساعد على تعزيز عمليات الاختراق، لكن لصالح الدول نفسها من أجل فرض مزيد من السيطرة على مواطنيها ومراقبة نشاطهم وتوجيهه بما يتوافق مع مصالح النخب الحاكمة وتوجهاتها. وهو ما تستفيد منه الشركات التكنولوجية لتطوير أدوات تحقق هذه الأهداف، لتجني من وراء ذلك مكاسب مادية وسياسية، ويبرز ذلك بشكل واضح في الحالة الإسرائيلية التي سيتم التعرض إليها تفصيلًا في المحور الآتي.

ثانيًا: التكنولوجيا الإسرائيلية.. حدود الاختراق واتجاهات التأثير

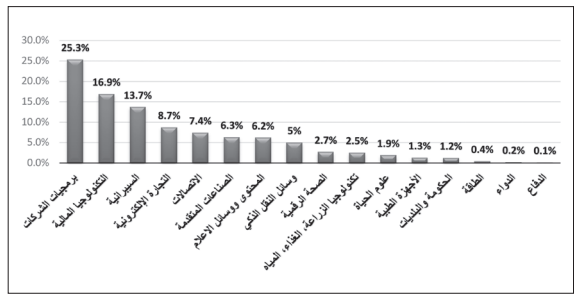
يشكل القطاع التكنولوجي في إسرائيل أحد محركات النمو الأساسية للاقتصاد، حيث ينمو هذا القطاع بشكل مطرد، وفي العام ٢٠٢١ نما ناتج قطاعات التكنولوجيا الفائقة بأكثر من ١٠٪، وبلغ ٢٣٧ مليار

يشكل القطاع التكنولوجي في إسرائيل أحد محركات النمو الأساسية للاقتصاد، حيث ينمو هذا القطاع بشكل مطرد، وفي العام ٢٠٢١ نما ناتج قطاعات التكنولوجيا الفائقة بأكثر من ١٠٪، وبلغ ٢٣٧ مليار شيكل، وتجاوزت صادرات التكنولوجيا الفائقة ٥٠٪ من الصادرات الإسرائيلية.

شيكل، وتجاوزت صادرات التكنولوجيا الفائقة ٥٠٪ من الصادرات الإسرائيلية وبلغت ٥٤٪ (مقارنة بـ ٤٣٪ في العام ٢٠٢٠)، وتشكل نحو ٦٧ مليار دولار.[١٤]

يجذب هذا القطاع النسبة الأكبر من الاستثمارات، حيث جمعت الشركات الناشئة الإسرائيلية أكثر من ٢٥ مليار دولار في العام ٢٠٢١ - ٥٦٪ من الاستثمارات كانت في برمجيات الشركات، السيبرانية، والتكنولوجيا المالية[١٥](انظر شكل رقم ١). كما تحتل إسرائيل الصدارة في ما يتعلق بالاستثمارات المحلية في مجال البحث والتطوير في القطاع المدني حيث بلغ إجمالي الاستثمارات٪ ٥,٤ (٧٦,٢ مليار شيكل) من الناتج المحلي الإجمالي – أعلى من المتوسط لجميع دول منظمة التعاون الاقتصادي والتنمية (OECD) -)مقارنةً مع ٧٢,٩ مليار شيكل، ٥,١٪ من الناتج المحلي الإجمالي، في العام ٢٠١٩).[١٦]

الشكل (١): توزيع الاستثمارات في شركات التكنولوجيا الفائقة الخاصة حسب مجال النشاط خلال العام٢٠٢١ [١٧]



المصدر: تقرير حالة إسرائيل للتكنولوجيا الفائقة لعام ٢٠٢٢، هيئة الابتكار الإسرائيلية، متاح على:
https://innovationisrael.org.il/en/reportchapter/part-israeli-high-tech-2022-situation-report#footnote5_nq60t16

شكلت هذه الطفرات في المجال التكنولوجي الإسرائيلي حافزًا لإصدار الحكومة الإسرائيلية قرار رقم ٤٥٥ في تشرين الأول ٢٠٢٠، الهادف بشكل أساسي إلى زيادة عدد طلاب الدراسات العليا الباحثين في موضوعات التكنولوجيا الفائقة بنسبة ٦٠٪، ومضاعفة عدد طلاب الدكتوراه في هذه المواد مقارنة بعام ٢٠١٩. [١٨]

تسعى إسرائيل عبر المجال التكنولوجي إلى تعزيز قدرتها على «المنافسة على التفوق» الجارية في العقد الماضي بين القوى العظمى والدول في ما يتعلق بالقيادة في المجالات التكنولوجية، بما في ذلك الذكاء الاصطناعي، والحوسبة الكمومية، والسيبرانية، والروبوتات، وتقنيات الفضاء. حيث تؤثر هذه المنافسة بدورها على ميزان القوى العالمي ومكانة الدول وقدرتها على العمل في الساحة الدولية. ووفقًا للرؤية الإسرائيلية فإن تل أبيب تتأثر بهذه المنافسة في جانبين، أحدهما، الجانب العسكري «الخشن» مثل حشد القوة العسكرية، والقدرة على استخدام قوتها في ساحة المعركة، وقدرتها على محاربة ما تسميه «الإرهاب». والجانب الأخر «الناعم» مثل تصدير التقنيات المدنية والعسكرية التي تؤثر على الاقتصاد، والوظائف في الاقتصاد، والقدرة على توظيف القوة الناعمة في الساحة الدولية.[١٩]

تحتل إسرائيل في الوقت الراهن مركزًا متقدمًا في مجال النشاط السيبراني الدفاعي والهجومي. وهو ما يعزز ميزتها العسكرية، كما أنها تخلق مجال تصدير له تأثير دولي ومحلي على الاقتصاد الإسرائيلي عبر ٥٠٠ شركة سيبرانية، بمبيعات سنوية تقدر بنحو ١٠ مليارات دولار.[٢٠]

وقد تأثرت مكانة إسرائيل الدولية بشكل سلبي، نتيجة الانكشاف السلبي لاستخدام المنتجات السيبرانية الهجومية لشركة NSO الإسرائيلية خلال الفترة (٢٠١٩ – ٢٠٢١)، في أعمال التجسس وانتهاك حقوق الإنسان ضد المسؤولين الرسميين في الدول الصديقة لتل أبيب (بما في ذلك ضد الرئيس الفرنسي إيمانويل ماكرون)، وأُجبرت

وزارة الدفاع الإسرائيلية على إعادة تقييم سياستها في ما يتعلق بالرقابة على الصادرات العسكرية.[٢١]

وتوالى بعد ذلك حدوث انكشافات سلبية أخرى حول الاستخدامات غير المشروعة للتكنولوجيا السيبرانية الإسرائيلية، كان آخرها ما كشف عنه تحقيق استقصائي من تورط إسرائيل بالتلاعب في انتخابات جرت في أكثر من ٣٠ دولة حول العالم، باستخدام مجموعة من الأدوات والبرامج السرية التي ضللت الرأي العام في تلك الدول. هذا فضلاً عن ما كشف عنه تقرير مختبر "سيتيزن لاب"، بتطوير شركة تكنولوجية إسرائيلية تدعى "كوا دريم"، برنامج تجسس جديد باسم "راين"، على غرار برنامج بيجاسوس، استخدم في اختراق هواتف صحفيين ومعارضين ومنظمات حقوقية، في ١٠ دول، بقارات مختلفة، باستخدام خوادم إنترنت في عدد من الدول. وتعتمد هذه الأداة على تقنية "زيرو كليك" (هجوم بدون أي نقرات)، حيث تستغل هذه الأداة ثغرات في انظمة تشغيل الهواتف، ومنها أجهزة الأيفون حيث تقوم باختراق خدمة التقويم الرقمي التابعة لشركة "آبل" - iCloud Calendar - ما يسمح للمهاجمين بإرسال استدعاء وهمي للهاتف، ومن ثم الوصول إليه. بينما يحتاج حامل جهاز أندرويد إلى الضغط مرة واحدة على رابط يرسل إلى هاتفه.[٢٢]

ومن ثم، تفرض تلك المعطيات جملة من اتجاهات التأثير التي استهدفتها إسرائيل عبر اقتحامها لهذا المجال التكنولوجي، وتحديدًا مجال التطبيقات السيبرانية، وتحقيقها مركزًا متقدمًا بين مصاف القوى الكبرى، وهو ما يُمكن إجماله على النحو الآتي:

توجيه الرأي العام والتأثير في الحكومات

كشف التحقيق الاستقصائي الذي أجراه «اتحاد الصحافيين الدوليين»، وصحيفة «الغارديان»، ونشر في ١٥ شباط الماضي، أن فريقًا من القراصنة الإسرائيليين، يديره عنصر سابق في القوات الخاصة الإسرائيلية، يُدعى تل حنان، واسمه المستعار «خورخي»، يتخذ من مكتب غير مميز في منطقة صناعية في «موديعين»، على بعد ٢٠ ميلاً خارج تل أبيب، مقرًا له، تلاعب بأكثر من ٣٠ عملية انتخاب في جميع أنحاء إفريقيا وأميركا الجنوبية والوسطى والولايات المتحدة وأوروبا.[٢٣] باستخدام القرصنة والتخريب والمعلومات المضللة الآلية على وسائل التواصل الاجتماعي، من خلال زرع المواد في المنافذ الإخبارية الشرعية، والتي يتم تضخيمها بعد ذلك بواسطة برنامج Aims لإدارة الروبوتات. هذا فضلًا عن استغلال نقاط الضعف في نظام اتصالات الإشارات العالمي SS7، الذي أُعتبر لعقود من الزمن نقطة ضعف في شبكة الاتصالات.[٢٤]

كما كشفت وثائق مسربة لصحيفة الغارديان في إطار التحقيق أن الفريق الإسرائيلي كان يُجري بعض عمليات التضليل من خلال شركة إسرائيلية تدعى «ديمومان إنترناشيونال»، المسجلة على موقع إلكتروني تديره وزارة الدفاع الإسرائيلية لتعزيز الصادرات الدفاعية.[٢٥] وكشفت تلك الوثائق أن عمليات التضليل استهدفت عمليات انتخابية أفريقية في كينيا وكذلك السباق الرئاسي في نيجيريا عام ٢٠١٥.[٢٦]

وفي السياق نفسه، رفعت شركة WhatsApp التابعة لشركة فيسبوك دعوى قضائية ضد مجموعة «إن. إس.أو» الإسرائيلية (NSO)، في تشرين الأول ٢٠١٩، بحجة أن أدوات NSO استغلت ثغرة أمنية في خدمتها لمهاجمة نحو ١٤٠٠ هاتف حول العالم.[٢٧]

تعكس هذه الوقائع أحد اتجاهات التأثير التي ترغب تل أبيب في تحقيقها من خلال التطور التقني الذي يسمح لها بتضليل الجمهور وتوجيه الرأي العام والتأثير في العمليات الانتخابية للدول الأخرى، وهو ما سيؤثر بدوره على حكومات تلك الدول، حيث تتيح هذه التدخلات من خلال التقنيات الإسرائيلية ترجيح كفة مرشح على آخر سيصبح في ما بعد مسؤولًا رسميًا في تلك الدولة، وسيكون مدينًا برد هذه الخدمة من خلال تقديم الدعم لتل أبيب بتسهيل تواجدها بأن يكون لها موطئ قدم في تلك المنطقة، بالإضافة إلى تقديم الدعم في المحافل الدولية.

تعزيز الدبلوماسية وكسب الأصوات

استهدفت إسرائيل خلال العقود الماضية عبر جهود حثيثة كسر حالة العزلة التي فُرضت عليها خاصة في الدائرة العربية والأفريقية وأميركا اللاتينية، حيث كان لهذه العزلة تأثير سلبي على الدعم التصويتي الذي تحتاجه تل أبيب في المحافل الدولية ضد القرارات الدولية المتعلقة بإدانة انتهاكاتها ضد الفلسطينيين. وسعت إلى تحقيق ذلك من خلال مسارات عدّة ارتكزت

تحقيقًا للهدف العام الذي تعمل عليه الحكومات الإسرائيلية المتلاحقة لتعزيز دبلوماسيتها وكسب شركاء جدد، فقد ضمِنت القرارات التي اتخذتها NSO في وقت مبكر بشأن علاقتها بالمنظمين من المؤسسات الحكومية، بأنها ستعمل كحليف وثيق، إن لم يكن ذراعًا، للسياسة الخارجية الإسرائيلية.

على تعزيز قدراتها وميزاتها النوعية التي يمكن تقديمها كمحفزات لكسب شركاء جدد. فمثلما فعل جيل الآباء المؤسسين مثل ديفيد بن غوريون، الذي أقام روابط سرية مع دول ومنظمات تقع خارج حلقة الدول العربية، في جميع أنحاء الشرق الأوسط وآسيا وأفريقيا، وأطلق على هذا النهج اسم «عقيدة المحيط»، حيث كان تقديم أسلحة متطورة عاملًا أساسيًا في إقامة تلك الروابط.[٢٨] يسعى جيل الأبناء لحذو الاتجاه نفسه لكن بآليات وطرق مختلفة، فمع ترسخ مكانة إسرائيل كواحدة من أكبر مصدري الأسلحة في العالم، ظهر نوع مختلف من صناعة الأسلحة فيخت. حيث بدأ قدامى المحاربين في الوحدة ٨٢٠٠ - المعادلة الإسرائيلية لوكالة الأمن القومي – في التدفق على الشركات الناشئة السرية في القطاع الخاص، مما أدى إلى ظهور صناعة أمن إلكتروني ضخمة.[٢٩]

غيّرت هذه الأسلحة الإلكترونية بدورها العلاقات الدولية بشكل أعمق من أي تقدم منذ ظهور القنبلة الذرية. من ناحية ميزاتها النسبية فهي رخيصة، ويمكن توزيعها بسهولة وكذلك نشرها دون عواقب للمهاجم. وبالتالي يغير انتشارها بشكل جذري طبيعة علاقات الدولة، وهو ما أدركته تل أبيب منذ فترة طويلة، وبدأ بقية العالم الآن في فهمه.

وارتباطًا بما يراه الكثيرون في مجال العلاقات الدولية بأن من أدوات فن الحكم بيع الأسلحة لأغراض دبلوماسية. فقد سعت تل أبيب لتعزيز دبلوماسيتها عبر هذه الأداة، من خلال بيع أسلحتها التكنولوجية المتقدمة في المجال السيبراني، من أجل استقطاب شركاء جدد. وهو ما تحقق من خلال مجموعة «إن. إس.أو» (NSO)، التي تبيع تطبيقات تكنولوجية متطورة تُستخدم لأغراض مشروعة كمكافحة الإرهاب وتهريب المخدرات والجرائم الكبرى الأخرى، وأغراض غير مشروعة مثل مراقبة اتصالات واختراق هواتف نشطاء الرأي والمعارضين، ويأتي في مقدمة هذه التطبيقات برنامج بيغاسوس (Pegasus).[٣٠]

تجدر الإشارة إلى أن أعضاء فريق البحث في NSO هم من قدامى المحاربين في أجهزة الاستخبارات الإسرائيلية. وهم جميعًا خريجو دورات تدريبية للنخبة، بما في ذلك وحدة سرية مرموقة لبرنامج ٨٢٠٠ المسمى ARAM الذي لا يقبل سوى حفنة من أكثر المجندين ذكاءً ويدربهم على أكثر الأساليب تقدمًا لبرمجة الأسلحة السيبرانية، وتتبع هذه الوحدة مديرية المخابرات العسكرية الإسرائيلية AMAN، الوكالة الأكبر في مجتمع التجسس الإسرائيلي.[٣١]

تحقيقًا للهدف العام الذي تعمل عليه الحكومات الإسرائيلية المتلاحقة لتعزيز دبلوماسيتها وكسب شركاء جدد، فقد ضمِنت القرارات التي اتخذتها NSO في وقت مبكر بشأن علاقتها بالمنظمين من المؤسسات الحكومية، بأنها ستعمل كحليف وثيق، إن لم يكن ذراعًا، للسياسة الخارجية الإسرائيلية. حيث شرح أحد المساعدين العسكريين السابقين لبنيامين نتنياهو، رئيس الوزراء آنذاك، مزايا هذا الارتباط. قائلًا: «مع وجود وزارة دفاعنا في ضوابط كيفية تحرك هذه الأنظمة، سنكون قادرين على استغلالها وجني الأرباح الدبلوماسية».[٣٢]

وانعكاسًا لتلك السياسات كانت أولى محطات الاختبار عبر بوابة أميركا اللاتينية، حيث تواجه إسرائيل منذ سنوات تحديات دبلوماسية ضد الجماعات المعادية لها التي يدعمها خصومها في الشرق الأوسط. وقد حصلت

التجسس الإلكتروني أداة ابتزاز دبلوماسي ضاربة بيد الحكومات الإسرائيلية.

مجموعة «إن.إس.أو» الإسرائيلية (NSO) على ترخيص من وزارة الدفاع الإسرائيلية ببيع تكنولوجيتها وتحديدًا برنامج بيغاسوس (Pegasus) للمكسيك،[٣٣] التي كانت تخوض معركة ضد عصابات المخدرات، وتبحث عن طرق لاختراق خدمة رسائل BlackBerry المشفرة التي يفضلها عملاء الكارتل، وبفضل التكنولوجيا الإسرائيلية (Pegasus) تمكنوا من القبض على زعيم كارتل سينالوا إل تشابو «خواكين غوزمان».[٣٤]

هنا تجدر الإشارة إلى أنه على الرغم من عدم وجود دليل مباشر على أن عقود المكسيك مع NSO قد أحدثت تغييرًا في سياستها الخارجية تجاه إسرائيل، فإن هناك نمط ارتباط يمكن الاسترشاد به على نمط جديد مغاير في السلوك التصويتي للمكسيك تجاه تل أبيب، فبعد تقليد طويل من التصويت ضد إسرائيل في مؤتمرات الأمم المتحدة، بدأت المكسيك ببطء في تحويل التصويت بـ «لا» إلى الامتناع عن التصويت.[٣٥] بعد ذلك، في العام ٢٠١٦، ذهب الرئيس المكسيكي إنريكي بينيا نييتو، الذي خلف كالديرون في العام ٢٠١٢، إلى إسرائيل، التي لم تشهد زيارة رسمية من رئيس مكسيكي منذ العام ٢٠٠٠.[٣٦] ليتبادل بعد ذلك نتنياهو هذه الزيارة في العام التالي ويزور مكسيكو سيتي، وهي أول زيارة لرئيس وزراء إسرائيلي على الإطلاق.[٣٧] وبعد فترة وجيزة، أعلنت المكسيك أنها ستمتنع عن التصويت على العديد من القرارات المؤيدة للفلسطينيين التي كانت تنظر فيها الأمم المتحدة.[٣٨]

أيضًا تمكنت إسرائيل من كسب أصوات كل من الهند والمجر وبنما في المحافل الدولية، فبعد تثبيت أنظمة NSO في مدينة بنما في العام ٢٠١٢، صوتت حكومة الرئيس البنمي ريكاردو مارتينيلي لصالح إسرائيل في مناسبات عديدة، بما في ذلك التصويت ضد قرار الأمم المتحدة منح فلسطين صفة دولة مراقب غير عضو في الأمم المتحدة، حيث عارضت إسرائيل وبنما وسبع دول أخرى فقط القرار، بينما صوتت لصالحه ١٣٨ دولة.[٣٩] وقد ساهمت صفقة الأسلحة المتطورة ومعدات المخابرات بقيمة ٢ مليار دولار تقريبًا – بما فيها نظام (Pegasus)، التي أُبرمت على هامش زيارة رئيس الوزراء الهندي ناريندرا مودي، لأول مرة منذ عقود في تموز ٢٠١٧،[٤٠] في تجاوز الخط التقليدي لسياسة الهند من ناحية «الالتزام بالقضية الفلسطينية».[٤١] وأعقب ذلك زيارة نتنياهو إلى نيودلهي في كانون الثاني ٢٠١٨. وفي ٦ حزيران ٢٠١٩، صوتت الهند لصالح إسرائيل في أحد مجالس الأمم المتحدة، حيث أيدت الموقف الإسرائيلي داخل المجلس الاقتصادي والاجتماعي الرافض لطلب «المؤسسة الفلسطينية

لحقوق الإنسان» (شاهد) الحصول على العضوية الاستشارية للمجلس.[٤٢]

بالنسبة لرئيس الوزراء المجري فيكتور أوربان، الذي رخصت في عهده وزارة الدفاع الإسرائيلية ببيع Pegasus إلى المجر، فقد كان الداعم المخلص لإسرائيل في الاتحاد الأوروبي. وفي العام ٢٠٢٠، كانت المجر واحدة من الدول القليلة التي لم تتحدث علنًا ضد خطة إسرائيل في ذلك الوقت لضم مساحات من الضفة الغربية من جانب واحد.[٤٣]

بينما جاءت درة التاج التي توجت هذه الاتفاقات ومثّلت اختراقًا تاريخيًا للعزلة الإسرائيلية في الدائرة الأكثر أهمية لتل أبيب (الدائرة العربية) من خلال الاتفاقات الإبراهيمية مع بعض الدول العربية التي اقتنت بدورها التكنولوجيا الإسرائيلية، ونشرت العديد من الصحف العالمية ومنها مجلة التايمز تقارير عن الدور الذي لعبته مبيعات Pegasus في تأمين دعم الدول العربية في الحملة الإسرائيلية ضد إيران وحتى في التفاوض على اتفاقيات أبراهام.[٤٤]

بالنسبة للدائرة الأفريقية، تمكنت تل أبيب من إيجاد موطئ قدم عزز حضورها في مؤسساتها القارية (صفة مراقب في الاتحاد الأفريقي) وهو ما يُثير بدوره أزمة في الوقت الراهن، نظرًا لرفض بعض الدول الأفريقية هذه العضوية (جنوب أفريقيا، الجزائر، نيجيريا). وبالنظر لقائمة الدول التي كشفت التحقيقات الاستقصائية مؤخرًا عن اقتنائها التكنولوجيا الإسرائيلية لمراقبة مواطنيها والمعارضين في دولهم، نجد أنها لا تتضمن هذا التيار الرافض للحضور الإسرائيلي. بينما تعززت وسط أعضاء وجهة النظر الداعمة للحضور الإسرائيلي من خلال تيار مؤيد شمل كلًا من: إثيوبيا وتوغو وغانا والمغرب. وهو ما دفع الكاتب الإسرائيلي المتخصص في الشأن الأفريقي يوتام جيدرون، بوصف نهج إسرائيل بـ «الوسيط» للدبلوماسية في إفريقيا،[٤٥] وذلك على خلفية التحقيق الذي أجرته مجموعة الصحافيين الاستقصائيين (Forbidden Stories)، بأن هواتف المواطنين الغانيين تخضع بالفعل للمراقبة بشكل غير قانوني من خلال برامج التجسس الإسرائيلية (Pegasus). والذي اقتنته غانا في كانون الأول ٢٠١٥، عبر شركة Infralocks Development Limited (IDL) التي توسطت عملية الشراء بعقد بقيمة ٥,٥ مليون دولار مع مجموعة NSO لشراء Pegasus. ثم أعادت بعد ذلك بيع البرنامج إلى هيئة تنظيم الاتصالات في غانا، وهي الهيئة الوطنية للاتصالات (NCA)، مقابل ٨ ملايين دولار.[٤٦]

تعزيز الرقابة والسيطرة المحلية

استهدفت تل أبيب من تطويرها هذه التكنولوجيات السيبرانية أن يكون لها نصيب من استخدامها على المستوى المحلي، من أجل فرض السيطرة وتعزيز الرقابة على حركة المعارضة التي تعززت مؤخرًا نتيجة السياسات المتطرفة التي ينتهجها رئيس الوزراء نتنياهو في إطار مناورته السياسية مع شركائه المتطرفين من الأحزاب الدينية لتحصينه من الملاحقة القضائية. وانعكس ذلك في تقرير لموقع كلكاليست الإخباري، الذي أكد استخدام الشرطة الإسرائيلية برنامج Pegasus (الذي اقتنته الشرطة الإسرائيلية في العام ٢٠١٣، تحت قيادة المفوض آنذاك روني الشيخ، المعين من قبل نتنياهو) للتجسس على النشطاء السياسيين، بمن فيهم معارضو رئيس الوزراء نتنياهو.[٤٧]

تقليص الآثار الاقتصادية لجائحة (Covid - 19)

على الرغم من حالة التراجع الاقتصادي التي شهدتها إسرائيل نتيجة تداعيات الجائحة، فقد أدى النمو السريع لمبيعات خدمات التكنولوجيا وارتفاع الطلب على المنتجات الرقمية وأمن البيانات -مع نقل العالم للأنشطة عبر الإنترنت بسبب الوباء- إلى تحسن في نمو الصادرات وارتفاعها بنسبة ١,٩٪. وهو ما كان له تأثيره الإيجابي على تقليص الآثار الاقتصادية للجائحة على الاقتصاد الإسرائيلي.[٤٨] حيث أكد التقرير السنوي لبنك إسرائيل لعام ٢٠٢٠ بأن «الصادرات لعبت دورًا رئيسًا في كبح تأثير الأزمة على الاقتصاد». خاصة صادرات الخدمات المتقدمة للصادرات التكنولوجية، التي «شهدت طلبًا عالميًا مرتفعًا، ظل قويًا، لا سيما في المجالات التي تتخصص فيها إسرائيل».[٤٩]

وكشف تقرير صادر عن مركز أبحاث IVC-Meitar، بأن شركات التكنولوجيا الإسرائيلية حققت مكاسب قدرها ٩,٣ مليار دولار من المستثمرين في العام ٢٠٢٠، وسجل الربع الأول من العام ٢٠٢١ رقمًا قياسيًا بلغ ٥,٥ مليار دولار، أي أكثر من

وفقًا لإستراتيجية إسرائيل الأمنية، تعتبر التكنولوجيا ركيزة أساسية للمفهوم الأمني للدولة، وأحد مقومات التفوق النوعي الذي تسعى تل أبيب لتحقيقه في إطار المنافسة المستمرة على التفوق بين القوى العظمى في ما يتعلق بالقيادة في المجالات التكنولوجية، بما في ذلك الذكاء الاصطناعي، والحوسبة الكمومية، والسيبرانية، والروبوتات، وتقنيات الفضاء.

ضعف المبالغ التي تم جمعها في الفترة نفسها من العام ٢٠٢٠، وأعلى بنسبة ٨٩٪ من الأموال التي تم جمعها في Q4 2020,[٥٠]

ردع الخصوم وتحجيم تكلفة الخيار العسكري

وفقًا لإستراتيجية إسرائيل الأمنية، تعتبر التكنولوجيا ركيزة أساسية للمفهوم الأمني للدولة، وأحد مقومات التفوق النوعي الذي تسعى تل أبيب لتحقيقه في إطار المنافسة المستمرة على التفوق بين القوى العظمى في ما يتعلق بالقيادة في المجالات التكنولوجية، بما في ذلك الذكاء الاصطناعي، والحوسبة الكمومية، والسيبرانية، والروبوتات، وتقنيات الفضاء.

ونظرًا للاتجاهات الحديثة في النطاق العملياتي العسكري نحو التوظيف الفعّال للأنظمة العسكرية غير المأهولة في ضوء محدودية الموارد وارتفاع كلفة الأسلحة التقليدية، فقد حذت إسرائيل هذا الحذو في اتجاهات صراعها مع الداخل الفلسطيني. وأظهرت عملية «حارس الأسوار» في أيار ٢٠٢١ التفوق التكنولوجي العسكري باستخدام التقنيات المتقدمة، بقيادة الذكاء الاصطناعي من خلال الضربات السريعة والدقيقة على الأهداف، والاستخدام المتقدم للقوة الجوية. حيث سلطت العملية الضوء على أهمية تقنيات الدفاع الجوي الإسرائيلية المتقدمة، مع التركيز على تحسين قدرات القبة الحديدية، مثل اعتراض الطائرات بدون طيار (وإن لم يكن ذلك فعّالًا ضد أنواع مختلفة من الطائرات بدون طيار).[٥١] فضلًا عن الاستخدام التشغيلي لـ «سرب» (مجموعة من الطائرات بدون طيار) لغرض تحديد مواقع الأهداف الأرضية وضربها.[٥٢]

أيضًا تلجأ إسرائيل إلى الأسلحة السيبرانية لإيصال رسائل الردع وفي الوقت نفسه خفض تكلفة الخيار العسكري، وانعكس ذلك خلال مهاجمة الأهداف النووية الإيرانية، وكان آخرها الهجوم السيبراني الذي استهدف شبكة توزيع الكهرباء لمنشأة نطنز النووية في نيسان ٢٠٢١.[٥٣] وبالتالي، تسعى إسرائيل من خلال تطويرها المستمر لقدراتها التكنولوجية في المجال العسكري، إلى تعزيز تفوقها في إطار منافسة القوى العظمى، وخفض كلفة عملياتها العسكرية التي تقوم بها سواء تجاه قطاع غزة أو الجبهة الشمالية، إلى جانب ردع إيران وموازنة التطور النوعي الذي أحدثته في تكنولوجيا الطائرات بدون طيار عبر تطوير تكنولوجيا دفاعية متقدمة تمكنها من ردع أي هجمات محتملة من وكلاء إيران المحليين المنتشرين في جوارها الجغرافي. هذا فضلًا عن فتح أسواق جديدة لمنتجاتها العسكرية التكنولوجية وكسب شركاء جدد.

خاتمة

على الرغم مما عكسته اتجاهات التأثير السابقة من فرص لتعزيز الحضور الإسرائيلي في محيطها الإقليمي والدولي -عبر بوابة «التفوق النوعي» في المجال التكنولوجي والسيبراني، وتمكينها من تجاوز تراكمات الماضي المرتبطة بحالة العزلة المفروضة عليها، عبر الترويج لقدراتها وإتاحة نقلها لشركائها الجدد مقابل تطبيع العلاقات- فإن ذلك لم يلغ مكامن التهديد لهذه المكانة المكتسبة بوتيرة متسارعة، لاعتبارات عدّة من أبرزها: (١) الانكشافات السلبية

الأخيرة لاستخدامات التكنولوجيا الإسرائيلية وتحديدًا برنامج (Pegasus) في أعمال التجسس والمراقبة، التي أدت إلى التأثير السلبي على هذه المكانة المكتسبة لدى المجتمع الغربي. ومن تبعيات ذلك إدراج وزارة التجارة الأميركية لكل من مجموعة (NSO) وشركة (Candiru) الإسرائيليتين في القائمة السوداء الأميركية للكيانات في ٣ تشرين الثاني ٢٠٢١، نتيجة تعارضهما مع مصالح الأمن القومي أو السياسة الخارجية للولايات المتحدة، بناءً على أدلة «أن هذه الكيانات طورت وقدمت برامج تجسس إلى الحكومات الأجنبية التي استخدمتها لاستهداف المسؤولين الحكوميين والصحافيين ورجال الأعمال والنشطاء والأكاديميين والعاملين في السفارات بشكل ضار».[٥٤]

(٢) تقييد الوصول للتكنولوجيا الأميركية والإضرار بسمعة الشركات الإسرائيلية، فمن شأن هذا الإدراج للشركات الإسرائيلية ضمن القائمة السوداء الأميركية، التي أعقبها إدراج فيسبوك في القائمة السوداء مزيدًا من شركات الأسلحة الإلكترونية والاستخبارات الإسرائيلية، أن يخيف العملاء المحتملين والموظفين. هذا فضلًا عن تقييد الوصول إلى التكنولوجيا الأميركية التي تحتاجها هذه الشركات لتشغيل عملياتها - بما في ذلك أجهزة كمبيوتر Dell وخوادم Amazon السحابية – وهو ما سيكون له تداعياته على قدرة هذه الشركات على العمل. وعبّر عن ذلك الرئيس السابق لمديرية الإنترنت الوطنية الإسرائيلية، إيغال غونا، بإنه يعتقد أن الخطوة ضد الشركات الإسرائيلية، هي جزء من شيء أكبر يستهدف تحييد تفوق إسرائيل في مجال الأسلحة السيبرانية. قائلًا: «علينا الاستعداد لمعركة الدفاع عن السمعة الطيبة التي كسبناها بصدق».[٥٥]

(٣) إيجاد بدائل محلية أميركية، تخضع للقواعد والقيود الأميركية المنظمة لاستخدامات تلك التكنولوجيا، وهو ما سيجعل الميزة الاحتكارية لشركات التكنولوجيا الإسرائيلية تتراجع. وبرز ذلك من خلال العرض الذي تقدمت به شركة أسلحة إلكترونية أميركية تدعى Boldend في كانون الثاني ٢٠٢١ لشركة Raytheon، عملاق الصناعة الدفاعية. ووفقًا للعرض الذي نشرته صحيفة The Times، طورت تلك الشركة ترسانة أسلحة خاصة بها لمختلف الوكالات الحكومية الأميركية لمهاجمة الهواتف المحمولة والأجهزة الأخرى.[٥٦]

(٤) المحدودية التكنولوجية للأسلحة السيبرانية الإسرائيلية، في ما يتعلق بالجوانب العسكرية، والتهديدات الرقمية (الهجمات الإلكترونية مثل برامج الفدية)، حيث لا تزال التكنولوجيا الإسرائيلية تواجه تحديًا في استخداماتها العسكرية يرتبط بـ «التهديد الجوي المتغير لإسرائيل»، فقد برز في السنوات الأخيرة استخدام الفصائل الفلسطينية لوسائل بدائية بشكل أساسي (مثل الطائرات الورقية والبالونات الحارقة)، وهو ما عجزت تل أبيب عن توفير حل تكنولوجي لمواجهته. هذا فضلًا عن تضاعف التهديدات المؤكدة بالهجوم الإحصائي بالصواريخ، والتهديد بضربات دقيقة عبر مشروع الصواريخ الدقيقة لحزب الله، وعن طريق الطائرات بدون طيار المتفجرة الإيرانية التي يتم تشغيلها في جميع أنحاء الشرق الأوسط ضد أهداف مختلفة.[٥٧]

(٥) الإضرار بسمعة النموذج الديمقراطي الغربي، حيث من شأن الانتهاكات التي تتسبب فيها التكنولوجيا الإسرائيلية الخاصة ببرامج التجسس والمراقبة (Pegasus)، التي ثبت استخدامها من جانب عدد من أنظمة الحكم في البلدان المختلفة ضد مواطنيها والنشطاء والمعارضين أن يضر بسمعة النموذج الديمقراطي الغربي بحكم كون إسرائيل مصنفة ضمن تلك الديمقراطيات، ويبدو أن المجتمع الغربي بقيادة الولايات المتحدة ارتأوا في تقييد عمل تلك الشركات خيارًا أفضل من تصنيف النظام السياسي في إسرائيل باعتباره نظامًا مقيدًا للديمقراطيات.

على الرغم من تلك التحديات فإن تل أبيب لا تزال تناور في مواجهة تلك الضغوط الغربية ضد شركاتها التكنولوجية بزعم أن تقييد عمل شركاتها من شأنه أن يسمح لروسيا والصين بملء هذا الفراغ، وتعزيز نفوذهما، من خلال بيع أدوات القرصنة الخاصة بهما إلى الدول التي لم يعد بإمكانها الشراء من إسرائيل. وهو ما برز خلال محادثات المسؤولين الإسرائيليين مع مستشار الأمن القومي للبيت الأبيض، أثناء زيارته لتل أبيب في كانون الأول ٢٠٢١. ومن المتوقع أن تستمر تل أبيب في مواجهة تلك الضغوط إلا أن فرص تحقيق اختراق في هذا الملف تتضاءل في الوقت الراهن مع تصاعد الاحتجاجات الشعبية في الداخل الإسرائيلي ضد سياسات الائتلاف الحكومي المتطرفة خاصة في ما يتعلق بملف إصلاح السلطة القضائية. وهو ما يتزامن مع ضغوط دولية ضد هذه السياسات.

الهوامش

1 Kevin Townsend, UK Government Proposes Digital Harms Legislation to Regulate Online Content, security week, April 12, 2019. Access Date: February 20, 2023. Retrieved From: https://www.securityweek.com/uk-government-proposes-digital-harms-legislation-regulate-online-content/

2 Kevin Townsend, Cyberbalkanization and the Future of the Internet, security week, November 1, 2019. Access Date: February 20, 2023. Retrieved From: https://www.securityweek.com/cyberbalkanization-and-future-internet/

3 Revealed: the hacking and disinformation team meddling in elections, The Guardian, February 15, 2023. Retrieved From: https://www.theguardian.com/world/2023/feb/15/revealed-disinformation-team-jorge-claim-meddling-elections-tal-hanan

4 Pegasus: What you need to know about Israeli spyware, Aljazeera, February 8, 2022. Access Date: February 20, 2023. Retrieved From: https://www.aljazeera.com/news/20228/2//what-you-need-to-know-about-israeli-spyware-pegasus

5 Gross, Benjamin. "MORE CHOICE, LESS UNCERTAINTY: THE PARADOXICAL RELATIONSHIP OF POLITICAL IDENTITY AND NEWS EXPOSURE IN THE AMERICAN PUBLIC SPHERE." Cross Currents, vol. 67, no. 4, 2017, pp. 705–25. JSTOR, Access Date: February 24, 2023. Retrieved From: https://www.jstor.org/stable/26605861

6 Ibid.

7 Chan, C. H., & Fu, K. W, The "mutual ignoring" mechanism of cyberbalkanization: triangulating observational data analysis and agent-based modeling. Journal of Information Technology & Politics, 12018) 10-). Access Date: February 25, 2023. Retrieved From: https://doi.org/10.108019331681.2018.1519480/

8 Ibid.

9 Valentino, Nicholas A., et al. "Selective Exposure in the Internet Age: The Interaction between Anxiety and Information Utility." Political Psychology, vol. 30, no. 4, 2009, pp. 591–613. JSTOR, Access Date: February 25, 2023. Retrieved From: http://www.jstor.org/stable/25655419

10 Sears, David O., and Jonathan L. Freedman. "Selective Exposure to Information: A Critical Review." The Public Opinion Quarterly, vol. 31, no. 2, 1967, pp. 194–213. JSTOR, Accessed February 23, 2023. Retrieved From: http://www.jstor.org/stable/2747198

11 "MORE CHOICE, LESS UNCERTAINTY: THE PARADOXICAL RELATIONSHIP OF POLITICAL IDENTITY AND NEWS EXPOSURE IN THE AMERICAN PUBLIC SPHERE", Op.Cit.

12 Ibid.

13 Ibid.

14 Part A: Israeli High-Tech 2022 Situation Report in Israel Innovation Authority's 2022- Innovation Report, Israel Innovation Authority, Access Date: February 26, 2023. Retrieved From: https://innovationisrael.org.il/en/reportchapter/part-israeli-high-tech-2022-situation-report#footnote5_nq60t16

15 Part A: Israeli High-Tech 2022 Situation Report in Israel Innovation Authority's 2022- Innovation Report, Op.Cit.

16 Israel in Figures: Selected Data From the Statistical Abstract of Israel 2021, Central Bureau of Statistics, Access Date: February 28, 2023. Retrieved From: https://www.cbs.gov.il/he/publications/DocLib/isr_in_n/sr_in_n21e.pdf

17 تقرير حالة إسرائيل للتكنولوجيا الفائقة لعام 2022، هيئة الابتكار الإسرائيلية، متاح على: https://innovationisrael.org.il/en/reportchapter/part-israeli-high-tech-2022-situation-report#footnote5_nq60t16

18 Ibid.

19 Liran Antebi, The Technology Arena: Maintaining the Regional Qualitative Edge in STRATEGIC SURVEY FOR ISRAEL 2022, The Institute For National Security Studies (INSS), Access Date: February 28, 2023. Retrieved From: https://www.inss.org.il/publication/technology-2022/

20 Ibid.

21 Defense Ministry said to freeze export licenses for Israeli 'cyberattack' tech, Times of Israel, February 5, 2022. Access Date: February 26, 2023. Retrieved From: https://www.timesofisrael.com/defense-ministry-said-to-freeze-export-licenses-for-israeli-cyberattack-tech/

22 Bill Marczak, John Scott-Railton, and others, Sweet QuaDreams: A First Look at Spyware Vendor QuaDream's Exploits, Victims, and Customers, The Citizen Lab, April 11, 2023. Retrieved From: https://citizenlab.ca/202304//spyware-vendor-quadream-exploits-victims-customers/.

23 Revealed: the hacking and disinformation team meddling in elections, Op.cit.

24 Ibid.

25 Ibid.

26 Ibid.

27 WhatsApp sues Israeli firm over phone hacking claims, BBC, October 30, 2019. Access Date: February 28, 2023. Retrieved From: https://www.bbc.com/news/business-50230431

28 The officer who saw behind the top-secret curtain, Ynetnews, June 21, 2015. Access Date: February 28, 2023. Retrieved From: https://www.ynetnews.com/articles/0,7340,L-4671127,00.html

29 Swed, Ori, and John Sibley Butler. "Military Capital in the Israeli Hi-Tech Industry", Armed Forces & Society, vol. 41, no. 1, 2015, pp. 123–41. JSTOR, Access Date: February 28, 2023. Retrieved From: https://www.jstor.org/stable/48609201. Accessed 7 Mar. 2023.

30 Pegasus Spyware and Citizen Surveillance: Here›s What You Should Know, CNET, July 19, 2022. Access Date: February 28, 2023. Retrieved From: https://www.cnet.com/tech/mobile/pegasus-spyware-and-citizen-surveillance-what-you-need-to-know/

31 Ronen Bergman and Mark Mazzetti, The Battle for the World's Most Powerful Cyberweapon, The New York Times, January 28, 2022. Access Date: February 28, 2023. Retrieved From: https://www.nytimes.com/202228/01//magazine/nso-group-israel-spyware.html
32 Ibid.
33 Israel›s NSO Group Pegasus probed by Mexico if spyware purchases were legal, The Jerusalem Post, October 17, 2022. Access Date: February 28, 2023. Retrieved From: https://www.jpost.com/international/article-719847
34 Exclusive: How Mexican drug baron El Chapo was brought down by technology made in Israel, Ynetnews, January 10, 2019. Access Date: February 28, 2023. Retrieved From: https://www.ynetnews.com/articles/0,7340,L-5444330,00.html
35 The Battle for the World's Most Powerful Cyberweapon, Op.cit.
36 At the invitation of the Israeli government, President Enrique Peña Nieto will attend the State Funeral of Shimon Peres, Gobierno de México, Access Date: February 28, 2023. Retrieved From: https://www.gob.mx/epn/prensa/at-the-invitation-of-the-israeli-government-president-enrique-pena-nieto-will-attend-the-state-funeral-of-shimon-peres?idiom=en
37 PM Netanyahu Meets with Mexican President Enrique Peña Nieto, Israel›s government services and information website, September 14, 2017. Access Date: February 28, 2023. Retrieved From: https://www.gov.il/en/departments/news/eventmexicanpre140917
38 Mexico says it will henceforth vote with Israel in international bodies, Times of Israel, November 19, 2017. Access Date: February 26, 2023. Retrieved From: https://www.timesofisrael.com/mexico-says-it-will-henceforth-vote-with-israel-in-international-bodies/
39 General Assembly Votes Overwhelmingly to Accord Palestine 'Non-Member Observer State' Status in United Nations, United Nations Website, November 29, 2012. Access Date: February 28, 2023. Retrieved From: https://press.un.org/en/2012/ga11317.doc.htm
40 India bought Pegasus as part of defence deal with Israel in 2017: NYT, The Indian Express, January 30, 2022. Access Date: February 28, 2023. Retrieved From: https://indianexpress.com/article/india/india-bought-pegasus-defence-deal-israel-2017-nyt-7746655/
٤١ د. محمد فايز فرحات، العلاقات الهندية – الإسرائيلية: الموجة الثالثة، مركز الأبحاث بمنظمة التحرير الفلسطينية، تاريخ الدخول: ٢٨ شباط ٢٠٢٣. انظر:
https://www.prc.ps/92732-/#_ednref6
42 India votes in favour of Israel against Palestinian NGO in UN, India Today, June 11, 2019. Accessed February 27, 2023. Retrieved From: https://www.indiatoday.in/world/story/india-votes-in-favour-of-israel-against-palestinian-ngo-in-un-154699911-06-2019-
43 The Battle for the World's Most Powerful Cyberweapon, Op.cit.
44 Ibid.
45 YOTAM GIDRON, ISRAEL IN AFRICA SECURITY, MIGRATION, INTERSTATE POLITICS, International African Institute Royal African Society World Peace Foundation, London (2020). Access Date: February 26, 2023. Retrieved From: https://ebin.pub/israel-in-africa-security-migration-interstate-politics-178699503497813502209O4-9781786995032-.html
46 SURAYA DADOO, Israel's Spyware Diplomacy in Africa, Orient XXI, Access Date: February 28, 2023. Retrieved From: https://orientxxi.info/magazine/israel-s-spyware-diplomacy-in-africa,5859
47 Report: Israeli police used NSO surveillance to spy on political activists, i24NEWS, January 18, 2022. Access Date: February 27, 2023. Retrieved From: https://www.i24news.tv/en/news/israel/politics/1642504557-report-israeli-police-used-nso-surveillance-to-spy-on-political-activists
48 Israel at 73: How the tech sector saved the economy from the worst of COVID, Times of Israel, April 14, 2021. Access Date: February 26, 2023. Retrieved From: https://www.timesofisrael.com/israel-at-73-how-the-tech-sector-saved-the-economy-from-the-worst-of-covid/
49 Ibid.
50 Israeli tech firms raise record $5.4 billion in first quarter of year, Times of Israel, April 12, 2021. Access Date: February 26, 2023. Retrieved From: https://www.timesofisrael.com/israeli-tech-firms-raise-record-54--billion-in-first-quarter-of-year/
51 Pacholska, M. Military Artificial Intelligence and the Principle of Distinction: A State Responsibility Perspective, Israel Law Review, 12022) ,21-). Access Date: March 3, 2023. Retrieved From: https://www.cambridge.org/core/journals/israel-law-review/article/military-artificial-intelligence-and-the-principle-of-distinction-a-state-responsibility-perspective/972D0662B1207C14656D5128B7B139FA
52 Ibid.
53 Iran vows revenge for ‹Israeli› attack on Natanz nuclear site, BBC, April 21, 2021. Access Date: March 3, 2023. Retrieved From: https://www.bbc.com/news/world-middle-east-56715520
54 Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities, U.S. Department of Commerce, November 3, 2021. Access Date: March 8, 2023. Retrieved From: https://www.commerce.gov/news/press-releases/202111//commerce-adds-nso-group-and-other-foreign-companies-entity-list
55 The Battle for the World's Most Powerful Cyberweapon, Op.cit.
56 Ibid.
57 The Technology Arena: Maintaining the Regional Qualitative Edge in STRATEGIC SURVEY FOR ISRAEL 2022, Op.cit.