المركز العربي للأبحاث و دراسة السياسات
Arab Center for Research & Policy Studies

دراسة

# الهجمات عبر الإنترنت:
# ساحة الصِّراع الإلكترونيِّ الجديدة

خالد وليد محمود | سبتمبر ٢٠١٣

الهجمات عبر الإنترنت: ساحة الصِّراع الإلكترونيِّ الجديدة

سلسلة: دراسات

خالد وليد محمود | سبتمبر ٢٠١٣



---

المركز العربيّ للأبحاث ودراسة السّياسات مؤسّسة بحثيّة عربيّة للعلوم الاجتماعيّة والعلوم الاجتماعيّة التطبيقيّة والتّاريخ الإقليميّ والقضايا الجيوستراتيجية. وإضافة إلى كونه مركز أبحاثٍ فهو يولي اهتمامًا لدراسة السّياسات ونقدها وتقديم البدائل، سواء كانت سياسات عربيّة أو سياسات دوليّة تجاه المنطقة العربيّة، وسواء كانت سياسات حكوميّة، أو سياسات مؤسّسات وأحزاب وهيئات.

يعالج المركز قضايا المجتمعات والدول العربيّة بأدوات العلوم الاجتماعيّة والاقتصاديّة والتاريخيّة، وبمقاربات ومنهجيّات تكامليّة عابرة للتّخصصات. وينطلق من افتراض وجود أمن قوميّ وإنسانيّ عربيّ، ومن وجود سماتٍ ومصالح مشتركة، وإمكانيّة تطوير اقتصاد عربيّ، ويعمل على صوغ هذه الخطط وتحقيقها، كما يطرحها كبرامجَ وخططٍ من خلال عمله البحثيّ ومجمل إنتاجه.

---

المركز العربيّ للأبحاث ودراسة السّياسات
شارع رقم: ٨٢٦ – منطقة ٦٦
الدفنة
ص. ب: ١٠٢٧٧
الدّوحة، قطر
هاتف: ٤٤١٩٩٧٧٧ ٩٧٤+ | فاكس: ٤٤٨٣١٦٥١ ٩٧٤+
www.dohainstitute.org

# المحتويات


مقدمة ١

أولًا: المجال الافتراضيُّ، المفهوم والدِّلالة ٤

ثانيًا: "الهاكرز" واختراق الحيِّز الافتراضيِّ ٧

ثالثًا: "الأنونيمس" جيشٌ ثكنته العالم الافتراضيُّ ١٠

رابعًا: الفضاء الإلكتروني والتَّسارع المحموم بين الدُّول ١٥

خامسًا: إسرائيل في قلب الصِّراع الإلكترونيِّ ٢٠

١. الإمكانيَّات الإسرائيليَّة في الفضاء الإلكترونيِّ ٢٦

٢. الأهميَّة الاقتصاديَّة لتكنولوجيا المعلومات الإسرائيليَّة والفضاء الافتراضيِّ ٣١

٣. ما أهميّة الهجوم على المواقع الإلكترونيَّة في إسرائيل؟ ٣٢

خلاصة ٣٤

## مقدمة

شهدت ساحة الحرب في "المجال الافتراضيِّ" Cyberspace خلال السَّنوات الأخيرة العديد من التَّطوُّرات والتَّجاذبات الميدانيَّة والنَّظريَّة، كان أبرزها ما دار مؤخَّرًا من هجمات إلكترونيَّةٍ أسهمت فيها دول ومنظَّماتٌ وأفرادٌ، وألحقت أضرارًا ماديَّةً ومعنويَّةً. وتقف عمليَّات القرصنة الإلكترونيَّة على رأس تلك الهجمات التي بدأت تثير قلق الدُّول والحكومات، بل وحتَّى الأفراد؛ بسبب تعدُّد الجهات التي تستطيع الانخراط بها، وصعوبة تتبُّع مصادرها أو تحديد مكان انطلاقها، وكلفة تداعياتها. وعلى هذا الأساس، أصبحت الشَّبكة العنكبوتيَّة ساحة نزاعاتٍ وصراعاتٍ، يدخل في سياقها التَّجسُّس والاختراق والتَّحكُّم في قواعد بياناتٍ قد تمسُّ الأمن القوميَّ والحيويَّ لبعض الدُّول. وفي ضوء سيرورات التَّطوُّر في مجال الفضاء الإلكترونيِّ، شرع معظم الحكومات بوضع هذا المجال في مكان متقدِّمٍ من قائمة أهدافها وأولويَّاتها الاستخباريَّة ونشاطاتها الوقائيَّة.

ومنذ انتقال وسائل التَّواصل الجماهيريِّ إلى الشَّبكة العنبكوتيَّة في التِّسعينيَّات، وزيادة الطَّلب على الإنترنت، سواءً في الإنتاج أو التَّوزيع أو الاتِّصال أو التَّمويل ... إلخ، بات معظم خدمات العالم الإنتاجية والخدماتيَّة والمعلوماتيَّة يعتمد بصورةٍ جوهريَّةٍ وأساسيَّةٍ على تلك الشَّبكة، وهذا ما زاد المخاطر من جرَّاء الاعتماد الكبير عليها، وزاد أيضًا من مخاطر ما يمكن أن تتسبَّب به الهجمات الإلكترونيَّة التي يتعاظم دورها ويتسع نطاقها في عالمٍ أصبحت فيه شبكة الإنترنت هشَّةً ويسهل اختراقها، نتيجة تطوُّر البرمجيَّات والحواسيب، وزيادة نشاط "قراصنة المعلومات" أو "الهاكرز" الذين باتوا يمتلكون خبرةً عميقةً في ميدان تقنيات المعلومات، ولهم القدرة على استغلال معرفتهم للولوج في الأعماق المظلمة والمحظورة في نظم شبكات الحواسيب بمختلف أشكالها، ويستهدفون المواقع الإلكترونيَّة البالغة الأهميَّة من خلال تعطيل نشاطها لساعاتٍ، وسرقة المعلومات الخاصَّة بالأفراد والمؤسَّسات – وأخطرها، بالطَّبع، تلك المتعلِّقة بالمؤسَّسات الماليَّة والعسكريَّة – ويقومون بنشاطاتٍ تخترق المؤسَّسات، ويوصِّلون من خلالها رسائل سياسيَّةً احتجاجيَّة، أو يجمعون بها الوثائق والأسرار، أو حتَّى المال. ومجال خطورة هؤلاء ليس كونهم

يقومون بتحرُّكات خطرةٍ وضارَّةٍ بقدر ما يمكن القول بوجود "جهل" بقدراتهم، بمعنى عدم التَّنبُّؤ بتحرُّكاتهم ونتائجها[1].

لقد أصبحت الهجمات الإلكترونيَّة واحدةً من السُّبل المؤثرة من دون تكاليف كبيرة، بعد أن أصبح العالم أمام قوىً تتسلَّح بالتِّكنولوجيا الحاسوبيَّة، ويمكنها بكبسة زرٍّ الاختراق وارتكاب أفعالٍ تقنيَّةٍ مضرَّةٍ بالآخرين عبر العالم الافتراضيِّ. وثمَّة العديد من التَّطوُّرات والتَّجاذبات والسِّجالات الميدانيَّة والنَّظريَّة، التي ألقت الضَّوء على هذا المجال الجديد نسبيًّا (الهجمات الإلكترونيَّة)، لا سيَّما بعد الهجمات الإلكترونيَّة التي شنَّتها مجموعة "الأنونيمس" أو "المجهولين" Anonymous[2] في العالم، وفي الشَّرق الأوسط، وتحديدًا في إسرائيل، خلال السَّنوات القليلة الماضية، وبسببها بدا وكأنَّ "الصِّراع" المستعر بين هؤلاء اللاعبين يتَّخذ شكل ما يُعتقد بأنَّه "هجماتٌ متبادلة" تعرَّضت لها منشآتٌ ومنظوماتٌ في مجالاتٍ عدَّةٍ على جبهتي هذا الصِّراع، وخلَّفت أضرارًا ماديَّةً ومعنويَّةً، تتضارب التَّقديرات بشأن حجمها وتأثيرها في نشاطات مؤسَّساتٍ وبرامج ماليَّةٍ وتكنولوجيَّةٍ، مدنيَّةٍ وعسكريَّةٍ.

---

[1] Theuns Verwoerd, *Honours Report, Active Network Security*, November 5, 1999, p. 12, Ray Hunt (Supervisor), http://www.cosc.canterbury.ac.nz/research/reports/HonsReps/1999/hons_9909.pdf

[2] تعد مجموعة "الأنونيمس" من أكثر المجموعات المؤثِّرة في تاريخ القراصنة الحديث؛ إذ تستمر فعَّاليَّات المجموعة إلى يومنا هذا في نشاطاتها. ولا توجد أيُّ معلوماتٍ حول عددهم أو مجموعاتهم الفرعيَّة. لهم عملياتٌ شهيرة، من بينها دعمهم لموقع "ويكليكس". وقد سبَّبت هذه المجموعات العديد من المشكلات السِّياسيِّة عبر العالم، إضافة إلى هجومهم على مواقع شركاتٍ عالميَّة عدَّةٍ، وتدخُّلهم في الانتخابات الإيرانيَّة عام ٢٠٠٩، مع القيام بمهاجمة مواقع حكوميَّةٍ أستراليَّةٍ من أجل المطالبة بالسماح للمستخدم بالتَّصفُّح من دون حجبٍ لأيِّ موقعٍ، ومواقع حكوميَّةٍ للعديد من الدُّول، وتسريب معلومات شخصيَّةٍ لشخصيَّاتٍ معروفةٍ في البحرين والمغرب ومصر والأردن. كما كان الرَّبيع العربيُّ ميدان عملٍ مكثَّفٍ لأعضائها؛ إذ قدَّموا دعمًا فوريًّا للثَّورات الشَّعبيَّة في تونس ومصر عبر شنِّ هجماتٍ قويَّةٍ ضدَّ المواقع الحكوميَّة للبلدين. وقد أثنى عليهم بعض المحلِّلين كمقاتلين رقميِّين، وأدانهم آخرون كونهم مقاتلون حاسوبيُّون فوضويُّون. انظر: أحمد أبو طالب، "أنونيمس: القرصنة السِّياسيَّة عبر الفضاء الإلكترونيِّ"، **الأهرام الرقمي**، ٢٠١٢/١/١:

http://digital.ahram.org.eg/Policy.aspx?Serial=780539

أفرز مفهوم الهجوم الإلكترونيِّ عبر المجال الافتراضيِّ ظهور حشدٍ كبيرٍ من المفردات والتَّحدِّيات. لذا، تحاول هذه الورقة توصيف "الجانب العمليَّاتيِّ" لموضوع الهجمات الإلكترونيَّة التي تُشنُّ عبر شبكة الإنترنت، وتطرّق إلى ماهية المجال الافتراضيِّ بصورةٍ أكثر شموليَّةً، وتحديد معالمه من خلال التَّركيز على "الهاكرز" ومجموعة "الأنونيمس"، بوصفهما من المسائل الشَّائكة التي نمت في تربته الرَّقميَّة، وكمصطلحين ضمن الدَّائرة المفاهيميَّة للفضاء الإلكترونيِّ. ولكي تتَّسع دائرة المعالجة المعرفيَّة للمسألة، تلقي الورقة الضَّوء على جهود بعض الدُّول في هذا المجال، كما يجرى التركيز في الجزء الأخير منها على حالة إسرائيل من ناحية الهجوم الذي تعرَّضت له في السَّابع من نيسان/ أبريل ٢٠١٣، وكذلك على جهودها في مجال بناء استراتيجيَّاتها الدِّفاعيَّة في الفضاء الإلكترونيِّ.

تهدف الورقة إلى تكوين صورةٍ واضحة المعالم عن البيئة الجديدة للمجال الافتراضيِّ، وهي التي أصبح مصير دولٍ ومستقبلها مرهونين بقدرتها على التَّعامل معها، والعمل على استثمارها لإعادة تشكيل مفردات المنظومات الأمنيَّة والتِّقنيَّة في عصر المعلومات. وتنبع أهميَّتها من أنَّ الهجمات عبر هذا الفضاء باتت تُعدُّ دليلًا يمكن الاسترشاد به للتَّعامل الصَّحيح مع ما تطرحه هذه الظَّاهرة على أرض الواقع من تداعياتٍ جديدةٍ، تضاف إلى قائمة التَّهديدات التَّقليديَّة التي تواجه الدُّول والجماعات والأفراد على حدٍّ سواء. وقد تتجاوز المستوى الدَّاخليَّ إلى مستوى الفواعل من الدُّول في العالم، "سيَّما في ظلِّ تنامي دور الفضاء الإلكترونيِّ في المجالات المختلفة، وتزايد الاعتماد عليه من قبل الأفراد، والجماعات السِّياسيَّة، والمؤسَّسات الحكوميَّة، مما يزيد من الأهميَّة الإستراتيجيَّة لهذه الآليَّات، ومن فاعليتها في تحقيق أهداف مستخدميها"[٣].

[٣] نوران شفيق علي، "فواعل افتراضيَّةٌ: المواجهات الإلكترونيَّة بين القوى السِّياسيَّة بعد الثَّورات العربيَّة"، مجلة **السياسة الدولية**، ١٠ حزيران/ يونيو ٢٠١٣، انظر: http://www.siyassa.org.eg/NewsContent/2/106/3137

## أولًا: المجال الافتراضيُّ، المفهوم والدِّلالة

من الممكن ماديًّا تحديد ما يُعرف بفضاء "السَّايبر" أو ما يُطلَق عليه أيضًا "الحيِّز أو الفضاء الافتراضيُّ" Cyberspace، بأنّه المجال الرَّقميّ الإلكترونيّ Digital Medium الممتدّ عبر مختلف خطوط الاتِّصالات المعدنيَّة والضَّوئيَّة والهوائيَّة وقنواتها في شبكة الشَّبكات "الإنترنت"، وهو بهذا المعنى، طريق المعلومات الفائق السُّرعة بتعبيره التِّكنولوجيّ. واقترن هذا الفضاء بمفاهيمه المختلفة؛ إذ انعدام جغرافيا المكان الطَّبيعيّ، وظهور جغرافيا الإبحار المعلوماتيّ في الاتِّجاهات شتَّى، وفي الآن ذاته. وهذا ما جعل هذه الظَّاهرة (فضاء السَّايبر) أهمَّ خصائص عصر المعلومات بلا منازعٍ. فهي تجسِّد عمليًّا، مجتمع القرية الكونيَّة، من خلال فضائها الافتراضيّ المنفتح الآفاق، الذي يضع الإنسان في عالمٍ رقميٍّ مختلفٍ: أسسه وخصائصه وقيمه الجديدة[٤]. "فالحديث هو بروز العالم الافتراضيّ كمساحةٍ مكانيَّةٍ وزمانيَّةٍ أضحت كما الأرض الجديدة؛ حيث هرعت إليها رؤوس الأموال والحركة الثَّقافيَّة والعلميَّة المعاصرة، ومظاهر التَّسلية، وكذلك الجريمة ... إلخ"[٥].

ثمَّة تعريفات عديدةٌ للمجال الافتراضيّ أو حيِّز "السَّايبر": فالاتِّحاد الدَّوليُّ للاتِّصالات International Telecommunication Union – وهو وكالة الأمم المتَّحدة المتخصِّصة في مجال تكنولوجيا المعلومات والاتِّصالات – يعرِّف الحيِّز الافتراضيَّ بأنَّه: الحيِّز الماديُّ وغير الماديِّ الذي ينشأ أو يتكوَّن من جزءٍ أو من كلِّ العناصر التَّالية: حواسيب، وأجهزةٍ ممكننةٍ، وشبكاتٍ، ومعلوماتٍ محوسبةٍ، وبرامج ومضامين، ومعطيات مرورٍ ورقابةٍ، والذين يستخدمون كلَّ ذلك[٦]. و"خلافًا للتَّعريفات التي تنظر إلى الحيِّز

---

[٤] علي محمد رحومة، **الإنترنت والمنظومة التكنو–اجتماعيَّة، بحثٌ تحليليٌّ في الآليَّة التقنيَّة للإنترنت ونمذجة منظومتها الاجتماعيَّة** (بيروت: مركز دراسات الوحدة العربيَّة، ٢٠٠٥)، ص ٣٣.

[٥] عمر بن يونس، **المجتمع المعلوماتيُّ** ( بيروت: الدَّار العربيَّة للموسوعات، ٢٠١٠)، ص ١٣.

[6] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf

الافتراضيِّ كبعدٍ أو مجالٍ خامسٍ، هناك توجُّهٌ يرى فيه واحداً من سبعة مجالاتٍ (حيِّزاتٍ)، إلى جانب الجوِّ والفضاء والبحر والبرِّ والحيِّزين الإلكترو–مغناطيسيِّ والإنسانيّ"[٧]. وهناك من يعرِّف المجال الافتراضيَّ على أنَّه "ساحة الحرب الخامسة"، بعد البرِّ والبحر والجوِّ والفضاء الخارجيِّ. وفي التعريف ذاته، يكون المجال الافتراضيُّ أوسع من الإنترنت، بل يتوسَّع من ذلك ليشمل الشَّبكات الحاسوبيَّة الأخرى التي ترتبط إلكترونيًّا بالإنترنت، وفيها أنظمة التَّحكُّم وجمع البيانات SCADA، وهي التي تتيح التَّواصل بين منظومات الحوسبة، والتي تتحكَّم في الأجهزة ذات الصِّلة بمفاصل الاقتصاد[٨].

إذًا، "فالفضاء الافتراضيُّ بات يعتبر كمجالٍ خامسٍ للحروب بين الدُّول؛ حيث عرف العالم عبر التَّاريخ الحروب البريَّة، والحروب البحريَّة، وحديثًا الحروب الجوِّيَّة، ومؤخَّرًا عرفنا حرب الفضاء، والآن ظهرت حرب الإنترنت"[٩]. كذلك فإنَّ هذا التَّوجُّه، يميِّز بين الحيِّز الافتراضيِّ وبين الحيِّز الإلكترو–مغناطيسيِّ، ويعتبر الشَّريحة الإنسانيَّة حيِّزًا أو مجالًا قائمًا بذاته[١٠].

إنَّ القاسم المشترك الواضح بين سائر التَّعريفات هو الشَّريحة العقليَّة، أمَّا الاختلاف والتَّباين فيما بينها، فيعكسان – على ما يبدو – الاهتمام الذي توليه كلُّ دولةٍ أو منظَّمةٍ في سياق مواجهتها للتَّحدِّيات في الحيِّز الافتراضيِّ. ولكن يبدو أنَّ الفوارق في التَّعريفات لا تعكس فهمًا مختلفًا للمجال الافتراضيِّ، لأنَّ

---

[٧] "الحرب في الحيّز الافتراضيِّ"، مجلة **قضايا إسرائيلية**، العدد ٤٣– ٤٤ (شتاء ٢٠١٢)، ص ٣.

[8] Fred Schreier, *On Cyberwarefare*, The Geneva Centre for the Democratic Control of Armed Forces (DCAF), at: www.dcaf.ch/content/download/67316/.../OnCyberwarfare-Schreier.pdf

[٩] عماد غنيم، "الحروب الافتراضيَّة القاتلة"، **الأهرام الرقمي**، ٢٠١٠/١٠/٢٥، انظر:

http://digital.ahram.org.eg/articles.aspx?Serial=340346&eid=601

[١٠] يوصِّف الكاتب فرد شريير بعض ملامح المجال الافتراضيِّ بأنَّه: يعتمد على الطَّيف الإلكترو–مغناطيسيِّ؛ مبنيٌّ على آليَّاتٍ مصطنعةٍ؛ يتكرَّر صنعه؛ والدَّخول إليه سهلٌ وغير مكلفٍ؛ الصفة الغالبة في المجال الافتراضيِّ هي الهجوم لا الدِّفاع. للمزيد، انظر:

Schreier, *On Cyberwarefare*

جميع أصحاب هذه التَّعريفات يقرُّون – كما أسلفنا – بوجود الشَّرائح الثَّلاث التي يتضمَّنها تعريف الأمم المتَّحدة[١١].

وفَّرت ثورة الاتِّصال والمعلومات أكثر من آلةٍ أو أداةٍ لتذليل الصِّعاب أمام العاملين في مجتمع المعلومات وشبكاته الممتدَّة على الفضاء المعلوماتيِّ العولميِّ. ويلاحَظ أنَّ ثمَّة مجموعةً متنوِّعةً من الأدوات الرَّقميَّة والفيزيائيَّة التي يُكثِر المتخصِّصون من استخدامها في اختبار أداء الشَّبكات المعلوماتيَّة أو تحديد مواطن الخلل فيها، وتتوافر لقراصنة الإنترنت أكثر من فرصةٍ لاستخدامها في عمليَّاتٍ تستهدف اختراق النِّظام. وخلال العقد الأخير، ظهر على ساحة الإنترنت وبرمجيَّات الحاسوب الكثير من الأدوات المعلوماتيَّة التي تحمل آثارًا ضارَّةً على النِّظام المعلوماتي، قام بصناعتها هواةٌ، أو جهاتٌ سخَّرت نشاطاتها وقدراتها لتوفير آلاتٍ تساهم في تخريب النُّظم المعلوماتيَّة لصالح جهاتٍ أخرى، أو لتحقيق مآرب متباينةٍ.

لقد عرف عالمنا المعاصر أوَّل عاصفةٍ إلكترونيَّةٍ جامحةٍ من خلال ما أحدثته تسريبات "ويكليكس" التي عُرفت باسم "عاصفة ويكليكس" Storm Wikileaks، وتضمَّنت استخدام موقعها على الإنترنت في نشر صورٍ ضوئيَّةٍ لآلاف الوثائق السِّرِّيَّة الرَّسميَّة المتبادلة بين وزارة الخارجيَّة الأميركيَّة وبعثاتها بدول العالم، وما أحدثته تلك التَّسريبات من توتُّرٍ حادٍّ في العلاقات الدوليَّة على جميع الصعد، ومنها توتُّر العلاقات بين كثيرٍ من القادة في العالم؛ لما نسبته إليهم من أقوالٍ وتصريحاتٍ تتعارض مع سياساتهم المعلنة تجاه شعوبهم، وهو ما أدَّى إلى حدوث اضطراباتٍ واحتجاجاتٍ عديدة بهذه الدُّول.

كان لاستخدام الإنترنت في بثِّ هذه التَّسريبات أثرٌ مهمٌّ في ترسيخ مفهوم الإنترنت وأهميتها وخطورتها، بوصفها إحدى ثمار ثورة المعلومات والاتِّصالات، وما تتيحه لمستخدميها من إمكانات تكنولوجيَّةٍ متنوِّعةٍ، قادرةٍ على إحداث نتائج غير محدودةٍ؛ إيجابيَّةً كانت أم سلبيَّةً، على كلِّ الصعد المحليَّة والإقليميَّة والدَّوليَّة[١٢].

---

[١١] "الحرب في الحيّز الافتراضيِّ".

[١٢] محمود الرَّشيديِّ، **الإنترنت والفيس بوك .. ثورة ٢٥ يناير نموذجًا** (القاهرة: الدَّار المصريَّة اللبنانيَّة، ٢٠١٢)، ص ١٦.

## ثانيًا: "الهاكرز" واختراق الحيِّز الافتراضيِّ

جاءت عمليَّات القرصنة الإلكترونيَّة كأحد تجلِّيات فصول الثَّورة المعلوماتيَّة، وظهر ما بات يُعرَف بالحرب الإلكترونيَّة القائمة أساسًا على أجهزة الحاسوب والشَّبكة العنكبوتيَّة، ونواتها "الهاكرز"[١٣] كشخصيَّةٍ محوريَّةٍ برزت على سطح البيئة الرَّقميَّة، وهم الذين يعملون عبر الاختراق البرمجيِّ لأجهزة الحاسوب. بيد أنَّ تزايد حجم المعلومات المنتشرة على الشَّبكة العنكبوتيَّة، وتصاعد قيمتها، بوصفها مصدرًا معرفيًّا واقتصاديًّا وسياسيًّا وأمنيًّا – بحسب طبيعة الموقع الذي يحتويها – قد ألقيا بظلالهما على هذا الميدان، فأحدثا تغييرًا جوهريًّا في أهداف عمليَّة الهجوم الإلكترونيِّ أو القرصنة المعلوماتيَّة التي كانت في بدايتها عبارةً عن نزعةٍ فضوليَّة للوصول إلى معرفةٍ جديدةٍ، أو تحدِّي العقبات الأمنيَّة التي تضعها الجهات الأخرى لغرض الإحساس بنشوة النَّصر، فتوجَّهت أهداف هذه العمليَّات صوب استثمار هذه القدرات، وترجمتها إلى مكاسب ماديَّةٍ أو سياسيَّةٍ موجَّهةٍ. وأصبحت إمكانيَّة إحداث تدميرٍ جزئيٍّ أو كلِّيٍّ في المواقع الرَّقمية التي تستهدفها الهجمات الإلكترونيَّة جزءًا مكمِّلًا للسُّلوك الذي يمارسه "الهاكرز" على النُّظم التي يمارس عليها آليَّة الاختراق.

يجري اختراق الحيِّز الافتراضيِّ أو الفضاء المعلوماتيِّ للدُّول عن طريق مجموعات قراصنة الحاسوب (ويقوم بهذه العمليَّة شخصٌ، أو مجموعة أشخاصٍ، وربما بضع مئاتٍ، أو بضع آلافٍ من المستخدمين) الذين يتمتَّعون بالقدرة على التَّحكُّم في برامج الحاسوب وطرق إدارتها، وهم مبرمِجون ذوو مستوىً عالٍ،

---

[١٣] يمكن تصنيف قراصنة المعلومات إلى قسمين: "الهاكرز" Hackers أو المبتدئين أو الهواة الذين يكون الهدف من وراء اختراقهم للأنظمة الإلكترونيَّة التَّعلُّم والتَّسلية على الأغلب. وهناك من يسمون "الكراكرز" Crackers وهم المخترقون المحترفون الذين يكون دخولهم إلى الحواسيب من أجل غايةٍ معيَّنةٍ.

يستطيعون اختراق أجهزة حاسوب والتعرف على محتوياته، ومعظم هؤلاء يرفضون التَّصريح عن هويَّتهم الحقيقيَّة خشية الملاحقة من أجهزة الدَّولة، ويختارون لأنفسهم صفة "مجهولٍ".

وهناك خمسة محاور رئيسةٍ يمكن أن يلجأ إليها "الهاكرز" للدُّخول إلى شبكة الحواسيب، وأن يُحْدثوا أضرارًا، وهي:

١. الحصار الافتراضيُّ Virtual Sit-Ins and Blocked: يهدف إلى إحداث خللٍ أو تمزيقٍ في آليَّات سريان العمليَّات التَّقليديَّة، مع كفِّ عمليَّات الدُّخول إلى الخدمات والمعدَّات الرَّقميَّة بمختلف أشكالها، وخلال فترةٍ زمنيَّةٍ معيَّنةٍ ينجم عنه خللٌ في الموقع، ولا يستطيع المستخدمون الدُّخول إليه[١٤].

٢. قنبلة البريد الإالكترونيِّ Email Bomb: تتمثل هذه العمليَّة بإرسال كمٍّ كبيرٍ (آلاف الرَّسائل الإلكترونيَّة) إلى صندوق البريد الإلكترونيِّ للخصم، بحيث ينشأ من هذا النَّوع من الهجمات تعطُّل قدرة البريد على تلقِّي الرَّسائل والتَّعامل معها[١٥].

٣. قرصنة مواقع الويب واختراق الحواسيب Web Hacks and Computer Break-Ins: يقوم الهاكر بهذه العمليَّة من خلال الدُّخول غير المشروع إلى إحدى مواقع الويب الموجودة على الشَّبكات المعلوماتيَّة، واستبدال معلومات جديدة بالمعلومات الموجودة عليه، تغيِّر من هويَّته[١٦].

٤. الفيروسات: يعمد الهاكرز هنا إلى زج الفيروسات وديدان الإنترنت، ونشرها في شبكات المعلومات الوطنيَّة والإنترنت؛ بقصد إحداث خللٍ مؤقَّتٍ أو دائمٍ في الملفَّات ونظم التَّشغيل المستهدَفة.

---

[14] J. Slobbe, "Hacktivists: Cyberterrorists or Online Activists?" 2012, http://arxiv.org/pdf/1208.4568.pdf

[١٥] حسن مظفَّر الزَّرو، **الفضاء المعلوماتيُّ** (بيروت: مركز دراسات الوحدة العربيَّة، ٢٠٠٧)، ص ٢١٦.

[16] Slobbe, "Hacktivists."

٥. هجمات الحرمان من الخدمة Denial of Service, DoS: هي هجماتٌ تتمُّ بإغراق المواقع بسيلٍ من البيانات غير اللازمة، يجري إرسالها ببرامج متخصِّصةٍ تعمل على نشر هذه الهجمات، فتسبب بطء الخدمات أو ازدحامًا مروريًّا على هذه المواقع، فيصعب وصول المستخدمين إليها. وقد تعرَّض الكثير من المواقع المهمَّة والحسَّاسة لمثل هذه الهجمات؛ ومن أبرزها: Word press و Amazon وغيرها، على الرَّغم من وجود بعض المنتجات والبرمجيَّات التي تدَّعي قدرتها على إيقاف مثل هذه الهجمات[١٧].

تجدر الإشارة إلى أنَّ العالم، وخلال العقدين الأخيرين على أقلِّ تقديرٍ، بدأ يشهد، في ظلِّ الثَّورة التِّكنولوجيَّة والرَّقميَّة، عمليَّات اختراقٍ لمنظوماتٍ معقَّدةٍ؛ ليس لأهدافٍ عسكريَّةٍ[١٨] فحسب، ولكن أيضًا لأغراضٍ اقتصاديَّةٍ[١٩] أو إعلاميَّةٍ أو سياسيَّةٍ أو حتَّى إجراميَّةٍ. ويتوقَّع الخبراء "نموًّا متواصلًا في عدد الهجمات المُوجَّهة خلال العام ٢٠١٣، وتواصل ظاهرة "القرصنة المُسيَّسة"، وظهور هجماتٍ إلكترونيَّةٍ، واستخدام أدوات مراقبةٍ "شرعيَّةٍ" في الفضاء الإلكترونيِّ برعايةٍ حكوميَّةٍ، وهجماتٍ على البنى التَّحتيَّة المعتمدة على الحوسبة، وتدهور الخصوصيَّة الرَّقميَّة، واستمرار المشكلات مع السُّلطات الرَّقميَّة

---

[17] http://compnetworking.about.com/od/networksecurityprivacy/g/denialof service.htm

[١٨] زادت خلال العقدين الماضيين، نتيجةً للتَّطوُّرات الرَّئيسة في بيئة الصِّراع الدَّولي، عمليَّة انتشار أنظمة الأسلحة والأجهزة العسكريَّة الذكيَّة التي تعتمد فاعليتها على دقة المعلومات المستخدمة لتشغيلها وحداثتها، واعتماد أنظمة الأسلحة والأجهزة المتَّصلة بها على أنظمة معلوماتٍ عالميَّةٍ تتَّصل مباشرةً بأجهزة الحواسيب التي تسيطر عليها دولٌ أخرى؛ مثل: نظام الملاحة العالميِّ GPS وأنظمة الاتِّصالات والاستطلاع بالأقمار الصِّناعيَّة، مع ضعف السَّيطرة على انتشار المعلومات، فازدادت مخاوف الدُّول المتقدِّمة تكنولوجيًّا – وهي التي تعتمد بناها التَّحتيَّة كثيرًا على أنظمة المعلومات – من تعرُّض أنظمة معلوماتها للتَّخريب والاختراق.

[١٩] ثمة هجماتٌ إلكترونيَّةٌ تستهدف ضرب اقتصاد دولةٍ ما، أو سرقة البنوك والحسابات المصرفيَّة، وهي أشهر أغراض القرصنة. وفي عام ٢٠١٢، عرضت جريدة **واشنطن بوست** تقريرًا استخباراتيًّا أميركيًّا حول عمليَّات التَّجسُّس الإلكترونيِّ والاختراق التي تستهدف العديد من الدُّول؛ ومن بينها الولايات المتَّحدة، وأكد التَّقرير أنَّ مثل هذه العمليَّات تهدّد المصالح الاقتصاديَّة للدُّول.

والائتمانيَّة في الإنترنت، والنُّموَّ المتواصل لأعداد البرمجيَّات الخبيثة التي تهدِّد نظام التَّشغيل والأجهزة المحمولة، والثَّغرات والبرامج المستغلَّة"[٢٠].

وفي أعقاب نشاطات "الهاكرز" المتزايدة والتَّسابق المحموم للحكومات في هذا المجال الذي غيَّر شكل الحرب الحديثة، أدركت الدُّول مدى فداحة ما يواجهها من تهديداتٍ، وأنَّ الأمر لا يتعلَّق بالأمور العسكريَّة فحسب، ولكنَّه يتجاوز ذلك إلى أمورٍ مدنيَّةٍ[٢١] "لإلحاق الضَّرر وإصابة دولٍ كاملةٍ بالشَّلل عن طريق لوحة المفاتيح (الكيبورد) على اعتبار أنَّ من لا يسارع باستيعاب ذلك لن يصمد في أيِّ مواجهةٍ"[٢٢].

## ثالثًا: "الأنونيمس" جيشٌ ثكنته العالم الافتراضيُّ

ثمة الكثير من العوامل التي تجعل من "الأنونيمس" سلاحًا مناسبًا يمتلك مجموعةً من المميِّزات الفريدة التي تجعل منه موضوعًا يستأثر باهتمام الكثير من المستخدمين المجهولين لشبكة الإنترنت المنتشرين على عموم رقعة البسيطة. ومن هذه المميِّزات: قابليَّة الاختراق لنظم المعلومات، وغياب الحدود المكانيَّة عن الفضاء المعلوماتيِّ، وعدم وضوح الهويَّة الرَّقميَّة للمستخدم المستوطن في بيئته المفتوحة، وتوسيع رقعة الاهتمام بما يتجاوز حدود السُّلطة أو المجتمع الذي تقيم فيه، مما يزيد قدرتها التَّأثيريَّة بشكلٍ

---

[٢٠] "التَّجسُّس والهجمات الإلكترونيَّة المُوجَّهة للبلدان: أبرز تحدِّيات ٢٠١٣"، جريدة **الاقتصادية** السعودية، ٢٠١٣/٤/٨، انظر: http://www.aleqt.com/2013/04/08/article_745515.html

[٢١] يتَّسم الحيِّز الافتراضيُّ أيضًا بكونه حيِّزًا يدمج المجالين المدنيَّ والعسكريَّ. ففي الكثير من الحالات تكون الاتِّصالات العسكريَّة مرتبطةً بشبكاتٍ مدنيَّةٍ. من هنا تغدو حماية البنى والشَّبكات المدنيَّة حيويَّةً للأغراض العسكريَّة أيضًا. في الوقت ذاته، تمتلك الجيوش قدراتٍ افتراضيَّةً يمكن أن تساعد في حماية الشَّبكات المدنيَّة.

[٢٢] عادل شهبون، "حروب السايبر ساحة المعارك الجديدة بين الدول"، **الأهرام الرَّقميُّ**، ٢٠١١/٦/٤، انظر:

http://digital.ahram.org.eg/articles.aspx?Serial=528342&eid=1103

ملموس. كذلك، فإنَّ هذه الجماعة "لا تتكوَّن حصريًّا من مجموعةٍ من محترفي القرصنة، أو ما يعرف بـ"الهاكرز"، ولكنَّها تضمُّ في صفوفها مجموعاتٍ لديها مهارات الكتابة، وأخرى قادرةً على صناعة مقاطع الفيديو، وأخرى ناشطةً في الشَّارع، وأخرى قد لا يكون لديها أيٌّ من هذه المهارات، ولكنَّها تساعد في نشر المعلومات والرَّسائل واستنساخها، خاصَّةً على شبكات التَّواصل الاجتماعيِّ"[٢٣]. ومن المميِّزات أيضًا تدنِّي الكلفة الماديَّة؛ إذ إنَّ توافر الأدوات المعلوماتيَّة على الإنترنت وقيام هذه المجموعة بفك الشَّيفرات البرمجيَّة يوفِّران عددًا ضخمًا من النُّظم البرمجيَّة والوسائل التي تمكِّن هؤلاء من استغلالها في توجيه ضرباتهم لخصومهم بسهولةٍ، ومن دون الحاجة إلى مصادر تمويلٍ ضخمةٍ. وتبدو أهم سمةٍ تتَّصف بها مجموعة "الأنونيمس" أنَّها ليست لديها عقيدةٌ جامعةٌ سوى الإصرار على النِّضال والحريَّة المطلقة في الإنترنت[٢٤].

تجدر الإشارة إلى أنَّ المنتسبين إلى مجموعة "الأنونيمس" لا يعيشون في عالمهم الخاصِّ، وفي غرفٍ مغلقةٍ ومعتمةٍ كما تُصوِّرهم هوليود، وإنَّما هم شبابٌ يعون ما يحدث في العالم، ويقدِّسون ثقافة الإنترنت، كونها تجسِّد حريَّة التَّعبير. هذه المجموعة أفرادها مجهولو الهويَّة، ولا يتبعون هرميَّةً معيَّنةً، وهم مطلوبون إلى العدالة لاختراقهم جهاز الاستخبارات الأميركيَّة، ونشرهم وثائق تابعةٍ لوكالة الاستخبارات المركزيَّة، ودعمهم المباشر لـ "ويكليكس" عبر قرصنة موقعَي "ماستر كارد" و"أمازون" ردًّا على رفض هاتين المؤسَّستين إفساح المجال أمام المواطنين لاستعمال موقعيهما في إرسال مساعداتٍ ماديَّةٍ لـ "ويكليكس".

مجموعة "الأنونيمس" هي كيانٌ عابرٌ للقارَّات، كلُّ ما تحتاجه لشنِّ هجماتها هو أعدادٌ من المبرمجين الأذكياء، وبضعة حواسيب، وتراكم الخبرة المعلوماتيَّة لدى طيفٍ واسعٍ من مستخدمي الحواسيب، مع توافر كمٍّ كبيرٍ من المعلومات التي تساهم بتطوير المهارات على مجموعةٍ كبيرةٍ من المواقع "المهمَّة" المنتشرة على الشَّبكة العنكبوتيَّة، وهذا ما بات يشكِّل عاملًا حاسمًا في زيادة الاهتمام بهذا الميدان، وبخاصَّة بعد أن "تحوَّلت هذه القرصنة إلى عمليَّاتٍ منظَّمةٍ من التَّجسُّس والتَّخريب والحرب الإلكترونيَّة

[٢٣] أبو طالب، "أنونيمس: القرصنة السِّياسيَّة".

[24] Slobbe, "Hacktivists."

القويَّة على مستوى الدُّول أو التَّنظيمات، بعد أن استهدفت هذه العمليَّات قطاعاتٍ حيويَّةً أدَّت إلى إذعان دولٍ كبرى، والاعتراف بالخطر الحقيقيِّ الذي يمكن أن تشكِّله"[٢٥].

باتت العوامل والمميِّزات التي أشرنا إليها أعلاه – وغيرها لا يتسع المقام لذكرها – تشكِّل بيئةً خصبةً لنموِّ تيَّارٍ قادرٍ على شنِّ هجماتٍ "سيبرانيَّة" رحاها الحيِّز الافتراضيُّ، قادرةٍ – إن ارتقت في وسائلها ودهائها – على اختراق مواقع البنى التَّحتيَّة للدُّول، وربَّما التَّحكُّم بحركة الملاحة الجويَّة، وإشارات المرور الضَّوئيَّة، وربما اختراق أنظمة الحرب الإلكترونيَّة. "فحجم المعلومات المنتشرة على ساحة الإنترنت وتصاعد قيمتها قد ألقت بظلالها على ميدان عمل "الهاكرز" والقرصنة المعلوماتيَّة، فأحدثت تغيُّرًا جذريًّا في أهدافها؛ من نزعةٍ فضوليَّةٍ للوصول إلى معرفةٍ جديدةٍ أو تحدِّي العقبات الأمنيَّة التي تضعها الجهات الأخرى لغرض الإحساس بنشوة النَّصر، للتَّوجُّه نحو أهدافٍ تستثمرها وتترجمها إلى مكاسب ماديَّةٍ أو سياسيَّةٍ"[٢٦].

ثمة أكثر من سببٍ لدى قراصنة الإنترنت الذين ينتمون إلى "الأنونيمس" يجعلهم يميلون إلى ممارسة أنواع الاختراق شتَّى على النِّظام الحاسوبيِّ، منها تراكم الأحقاد والضَّغائن، والرغبة في تدمير ما لدى الغير، وإحداث نوعٍ من التَّخريب. وهناك قراصنةٌ يقومون بهجماتٍ وهميَّةٍ، بهدف فحص الأمن لدى النِّظام المختبر، ويكون هذا النَّوع من الهجوم بالتَّوافق. ومنها كذلك وجود تحدٍّ تقنيٍّ وإثبات الذَّات بين مستخدمٍ وآخر، أو التَّسلية وحبِّ الاستطلاع، ووجود إغراءاتٍ ماديَّةٍ توفِّرها حكوماتٌ وجهاتٌ لـ "الهاكرز" ذوي المهارات الفنيَّة العالية في استخدام برمجة الحاسوب واختراقه للحصول على بياناتٍ مهمَّةٍ من نظامٍ معلوماتيٍّ. وقد يكون هذا الدَّافع ناتجًا من الفقر أو العوز، أو بسبب الطمع، أو بسبب الرَّغبة في إطاحة منافسٍ نتيجةً لتضارب المصالح. وكذلك الفضول والرَّغبة في اكتشاف المجهول وساحة الممنوع، أو وجود أغراضٍ ودوافع سياسيَّةٍ تجمع بين أفرادٍ أو جماعاتٍ لها عقائد وأفكارٌ سياسيَّةٌ معيَّنةٌ وتحاول استخدام أدوات ممارسة الاختراق الحاسوبيِّ لخدمة معتقداتها وتوجُّهاتها السِّياسيَّة، فتلجأ – مثلًا– إلى التَّدمير أو التَّجسس على مواقع إلكترونيَّةٍ وشبكاتٍ وقواعد بياناتٍ لدولٍ أو جماعاتٍ أو شركاتٍ تراها معاديةً لها،

---

[٢٥] "(الهاكرز)... قراصنة العصر الإلكترونيِّ"، **شبكة النبأ المعلوماتية**، ٢٠١٢/١/٣١، انظر:

http://www.annabaa.org/nbanews/2012/01/313.htm

[٢٦] الزَّرو، **الفضاء المعلوماتيُّ**، ص ٢١٨.

ويجري اختراقها من قبل مجموعات من متطوِّعين يناهضون تلك النُّظم. ونشير إلى هذا بوصفه فكرًا جديدًا يقوم على استخدام مجموعاتٍ من قراصنة "الهاكرز" في الإنترنت لمهاجمة المواقع الإلكترونيَّة على الشَّبكة، وذلك دعمًا لقضايا الشُّعوب وفضح الحكومات الفاسدة.

ومثال ذلك أنَّه عندما تحرَّكت شعوبٌ عربيَّةٌ ضدَّ الدِّكتاتوريِّين الذين سيطروا عليها لفتراتٍ لا تقلُّ عن نصف قرنٍ من الزمن، فيما أصبح يُعرَف بـ "الرَّبيع العربيِّ"، كانت الإنترنت أيضًا هي الحليف التِّكنولوجيَّ الذي مكَّن النَّاس من تبادل المعلومات، وتنظيم التَّظاهرات، وترويج الحركة بأسرها. ووقتها فُتح نقاشٌ واسعٌ بشأن قيم القرصنة الإلكترونيَّة، فبعدما اعتاد الخطاب العربيُّ السَّائد تصوير "الهاكرز" على أنَّهم شبابٌ مهووسون تقنيًّا، ويقضون وقتهم في محاولة خرق أمن الدُّول والمؤسَّسات الكبرى من باب التَّسلية فحسب، جاءت الانتفاضات الشَّعبيَّة العربيَّة لتبيِّن أنَّ كثيرًا من عباقرة الحاسوب هؤلاء يستعملون خبرتهم لمساعدة الثُّوَّار وفضح الحكومات؛ مثل مساعدتهم المواطنين المصريِّين في إيجاد حلٍّ مكَّنهم من استعمال مواقع التَّواصل الاجتماعيِّ عندما أمرت حكومة الرئيس السابق حسني مبارك تعطيل خدمات الإنترنت، كما ساعدت المحتجِّين الليبيِّين واليمنيِّين، وقام أعضاءٌ من "الأنونيمس" بقرصنة المواقع الرَّسميَّة التَّابعة لنظام الرَّئيس التُّونسيِّ السَّابق، زين العابدين بن علي، ردًّا على حجب الإنترنت عن الشَّعب التُّونسيِّ في إلى الحكومة ]...[بداية الثَّورة، ثم تركوا رسالةً في هذه المواقع المقرصنة، جاء فيها: "نحن مجهولون التُّونسيَّة: لن يتم التَّسامح مع الهجوم على حرِّيَّة التَّعبير وحرِّيَّة وصول مواطنيكم إلى المعلومات، وأيُّ منظَّمةٍ متورِّطةٍ في الرِّقابة سيجري استهدافها". هؤلاء يعتبرون أنَّ الحكومات تستعمل الشَّبكة العنكبوتيَّة لمراقبة المواطنين، ولذا، يحقُّ للمواطنين، وعبر الإنترنت أيضًا، كشف أسرار هذه الحكومات وعمليَّاتها[27].

وقد سبق أن قامت مجموعة "الأنونيمس" بهجمات عدَّةٍ "ضدَّ مواقع وصفحات الهيئات الحكوميَّة والوزارات يناير، ردًّا على قمع قوَّات الأمن للمتظاهرين، وانتقامًا لقطع الإنترنت ٢٥ المصريَّة في أثناء ثورة فيها مع تعاونواOperation Egyptوالاتصالات عن المصريِّين، وهو ما أطلق عليه اسم "العملية مصر"

[٢٧] تانيا الخوري، "كلنا شهود عيان: ربيع العرب بالصُّور والحروب الإلكترونيَّة"، **مجلَّة الدِّراسات الفلسطينيَّة**، العدد ٨٨ (خريف ٢٠١١)، ص ١٢٨.

غير تقليديَّةٍ تمكِّن المصريين من الاتصال بالإنترنت بعد قطع لتوفير طرقٍ"[28] تيليكوميكس "مجموعة الخدمة عنهم.[29]

تجدر الإشارة أنَّه "منذ احتماء الاحتجاجات في تونس، بدأت تنتشر فيديوهات على الإنترنت تحمل توقيع "أنونيموس"، تحت اسم "العمليَّة تونس"، وهي عمليَّةٌ انتقاميَّةٌ من السُّلطات التُّونسيَّة لما مارسته من عنفٍ ضدَّ المتظاهرين وحملات اعتقالٍ للمدوِّنين؛ إذ تمَّ تعطيل مواقعها الحسَّاسة، ولا سيَّما مواقع وزارات الدِّفاع والدَّاخليَّة والخارجيَّة. وقد تكرَّرت هذه الأفعال بالنَّمط نفسه الذي يبدأ، غالبًا، برسالة دعمٍ للشَّعب، ثم تهديدٍ ووعيدٍ للحكومة، بالنِّسبة لمصر، وليبيا، وتركيا، وإسبانيا، واليونان، وإيطاليا، والبرتغال، ودول شرق أوروبا، وزيمبابوي، والصِّين، وروسيا، وإيران، وسوريا، وغيرها، كدعمٍ للحركات الاحتجاجيَّة التي حدثت هناك، أو مؤازرةً لحركات المطالبة بالدِّيمقراطيَّة ومناهضة الفساد"[٣٠]. وهذا ما حدث كذلك في الولايات المتَّحدة لدعم حركة "احتلوا" Occupy، ولكن بشكلٍ مختلفٍ[٣١]؛ إذ قامت المدوَّنات والصَّفحات الإخباريَّة التَّابعة والمتعاطفة مع "أنونيمس" على الفيسبوك بمتابعةٍ ميدانيَّةٍ أكثر منها حشدًا أو فعلًا إلكترونيًا. وبهذا، "تكون هذه الجماعة قد أسهمت بصورةٍ أو بأخرى في إلقاء الضَّوء على تلك الاحتجاجات عن طريق شبكات الإعلام البديل، في ظلِّ تعتيم الإعلام التَّقليديِّ الذي تعمَّد غضَّ البصر عنها، على الأقلِّ في بدايتها"[٣٢].

بات اليوم من الصَّعب إلى حدٍّ ما التَّعرُّف إلى عدد أعضاء هذه المجموعة التي باتت رمزًا للمهاجمين الإلكترونيِّين، وهم أشبه بجيشٍ ثكنته العالم الافتراضيُّ الذي يلتقون فيه ويتبادلون الحديث في غرف دردشةٍ سرِّيَّةٍ، ويعملون في أنحاء العالم شتَّى، ولهم أولويَّاتهم الخاصَّة، لا يترأَّسهم أحدٌ، وشعارهم أنَّهم "مجهولون، لا يسامحون ولا ينسَوْن"، يختمون بها كلَّ بياناتهم المكتوبة أو المصوَّرة، في إشارةٍ إلى من ينتهك حرِّيَّة

---

[٢٨] التيليكوميكس Telecomix، مجموعة من القراصنة الإلكترونيين المهتمين بكشف من يحجب ويراقب الإنترنت.

[٢٩] أبو طالب، "أنونيمس: القرصنة السِّياسيَّة".

[٣٠] المرجع نفسه.

[٣١] المرجع نفسه .

[٣٢] المرجع نفسه.

التَّعبير، ويحدُّ من الاستعمال الحرِّ للإنترنت. أمَّا هدفهم فهو فضح الحكومات الفاسدة، أي جميع الحكومات كما يصرِّحون. وهذا ما يجعلنا نقف اليوم عند ظاهرةٍ عابرةٍ للقارَّات، وشكلٍ من أشكال الحركات الاحتجاجيَّة المعاصرة في القرن الحادي والعشرين، تأخذ من الفضاء الإلكترونيِّ ساحةً لنشاطاتها وردود أفعالها.

## رابعًا: الفضاء الإلكتروني والتَّسارع المحموم بين الدُّول

يعدُّ مفهوم الهجوم الإلكترونيِّ (الحرب الافتراضيَّة أو الإلكترونيَّة، أو حرب الإنترنت والسَّاحات الرقميَّة، أو الحرب السيبرانيَّة cyber warfare) بحدِّ ذاته "مفهومًا جديدًا على صعيد النِّزاعات الدَّوليَّة في القرن الحادي والعشرين، وهي تشير إلى "أساليب للحرب تعتمد على تكنولوجيا المعلومات، تستهدف الحواسب أو المواقع الإلكترونيَّة، وتشمل عمليات تسلُّلٍ إلى أنظمة الحاسب الآليِّ، وجمع بياناتٍ أو تصديرها أو إتلافها أو تغييرها أو تشفيرها، كما تشمل عمليَّات زرع برمجيَّاتٍ ضارَّةٍ للتَّجسُّس، وغير ذلك من العمليَّات السَّيبرانيَّة أو الإلكترونيَّة، أو ما يُطلق عليه عمليَّات اختراقٍ أو قرصنةٍ إلكترونيَّة"[٣٣]. وبناء عليه، فإنَّه إذا كان اكتشاف البارود قد غيَّر من ملامح الخريطة الدَّوليَّة للحروب، فإنَّ التَّحكُّم في مسارات الدَّولة الحديثة معلوماتيًّا، أضحى قادرًا على إصابة الدُّول الكبرى بالشَّلل والهزيمة من دون أن تطلَق عليها رصاصةٌ واحدةٌ[٣٤].

ويشكِّل هذا المفهوم جزءًا لا يتجزَّأ من الجيل الخامس من الحروب غير المتكافئة التي قد تشنُّها مجموعات أو أفرادٌ أو دولٌ تستخدم التِّكنولوجيا المتطوِّرة لأغراضٍ وأهدافٍ معيَّنةٍ. "وتتعدَّد أغراض

---

[٣٣] أمل خيري، "إسرائيل وقراصنة الإنترنت.. جولةٌ جديدةٌ في الحرب السَّيبرانيَّة"، ٢٠١٣/٤/١١، انظر:

http://www.alamatonline.net/l3.php?id=56608

[٣٤] أنتوني جورجي، "تجربةٌ أولى ناجحةٌ للحرب الإلكترونيَّة على إسرائيل"، جريدة **الخليج** الإماراتية، ٢٠١٣/٤/١٨، انظر:

http://www.alkhaleej.ae/portal/e0c8722a-ca8c-4255-b0c2-27695b3b3a54.aspx

القرصنة الإلكترونيَّة، وإن كانت كلُّها تشترك في تهديدها للمصالح الاقتصاديَّة للدُّول، فهناك هجماتٌ تستهدف ضرب اقتصاد دولةٍ ما، أو سرقة البنوك والحسابات المصرفيَّة، وهي أشهر أغراض القرصنة"[٣٥]. كما بات "الفضاء الإلكترونيُّ وتعقيداته التِّكنولوجيَّة المتسارعة، من أهمِّ وسائل الصِّراع المستقبليَّة القادرة على حسم جوانب كثيرةٍ. ففي مختلف الإستراتيجيَّات العسكريَّة الحديثة، باتت تسود نظريَّات الجيوش الذَّكيَّة القائمة على النَّوع لا الكمِّ، وبكلامٍ أكثر دقَّة؛ النَّوع المتخصِّص القائم على دعامات هضم التِّكنولوجيا المتقدِّمة، القادرة على تحقيق أعلى المكاسب بأدنى المتطلَّبات"[٣٦].

وخلال السَّنوات الأخيرة، بات العالم يتعرَّف على عالمٍ مغايرٍ، في ضوء امتداداتٍ للمجال العامِّ[٣٧] تمثَّلت بامتدادين رئيسيَّين: أحدهما يعبِّر عن امتداد الفضاء الإعلاميِّ لتتسابق الأفكار بصورةٍ كبيرةٍ، ومعها تتزايد درجة الاعتماد الجماهيري على الإعلام، فيما كان الامتداد الآخر في تعاظم الحيِّز الذي يشغله الفضاء الإلكترونيُّ كحيِّزٍ قتاليٍّ جديدٍ، ينضمُّ إلى مجالات البَرِّ والبحر والجوِّ والفضاء، في ساحة المعركة العصريَّة[٣٨]؛ الأمر الذي حثّ العديد من دول العالم على مواكبة التَّطوُّرات العالميَّة في هذا المجال، وتسريع وتيرة "استعدادها في مواجهة هذا التَّحدي الجديد"، وذلك بغية تحسين سبل ووسائل الدِّفاع عن حيِّزها الافتراضيِّ. وقد شرعت دولٌ عصريَّةٌ وجيوشٌ متقدِّمةٌ في العالم بزيادة نشاطها وتكثيف جهودها في الحيِّز الافتراضيِّ الذي يشكِّل مصدر قوَّةٍ لها، لكنَّه يكشف في الوقت ذاته أيضًا عن مَواطن ضعفٍ. وعلى سبيل المثال، فإنَّ البنى التَّحتيَّة الحيويَّة لعمل الدَّولة (كالكهرباء والمياه والمواصلات) وشبكات

---

[٣٥] خيري، "إسرائيل وقراصنة الإنترنت".

[٣٦] فهد سعيد، "الحرب الإلكترونيَّة"، موقع مجتمع القبَّعات البيضاء، ٢٠١٢/٥/٢٨، انظر:

http://www.whit3hats.com/?p=2775

[٣٧] هبة رؤوف عزَّت، "الذَّات والمساحة والزَّمن.. من المجال العامِّ إلى الشَّارع السِّياسيِّ"، ملحق اتجاهات نظرية، مجلَّة **السِّياسة الدَّوليَّة**، كانون الثَّاني/ يناير ٢٠١٢، ص ٣١.

[38] For more details, see: "On Cyber Warfare," at: http://www.dcaf.ch/content/download/67316/.../ OnCyberwarfare-Schreier.pdf

القيادة والسَّيطرة والتَّحكُّم العسكريَّة، وكذلك التِّقنيات المتطوِّرة لساحة القتال العصريَّة، كلُّها تعتمد على هذا الحيِّز الافتراضيِّ[٣٩].

مع تبدُّل نمط الحياة في عصر الازدهار الإلكترونيِّ، تغيَّرت أشكال الأشياء، ومنها أنماط الحرب الإلكترونيَّة التي أخذت منحىً حديثًا، يتماشى مع التَّطوُّر التِّقنيِّ[٤٠]، وثمَّة من يعتبر أنَّه "إذا كان البرُّ، والبحر، والجوُّ، والفضاء الخارجيُّ، هي المسارح التَّقليديَّة للحروب الغابرة، فإنَّ حيِّز الإنترنت الافتراضيَّ يُعدُّ هو المسرح الحقيقيُّ للحرب الإلكترونيَّة؛ إذ باتت الأطراف الدَّوليَّة تتنازع وتتسابق على استغلال هذا المجال لمصلحتها، وقد تمتدُّ مسارح الحروب الإلكترونيَّة من أمام شاشات الحواسيب إلى قاع المحيطات، وحتَّى الطَّبقات العليا للفضاء الخارجيِّ، وقد يُستخدَم فيها مختلف أرقى تقنيات النُّظُم الإلكترونيَّة: "المراقبة والكشف، والقيادة والسَّيطرة، والإعاقة والخداع، ورصد الأهداف، وتوجيه الضَّربات"[٤١]، فقد أصبحت إمكانيَّة إحداث تدميرٍ جزئيٍّ أو كلِّيٍّ في المواقع الرَّقميَّة التي تستهدفها الهجمات الإلكترونيَّة جزءًا مكمِّلًا للسُّلوك الذي يمارسه القرصان على النُّظم التي يمارس عليها آليَّة الاختراق، أو التَّلصُّص[٤٢].

يقدَّر الضَّرر الذي تلحقه الهجمات الإلكترونيَّة بالاقتصاد العالميِّ، بما يزيد على تريليون دولار سنويًّا[٤٣]، وقد انخرط العديد من الدُّول في المشهد الممتزج؛ حيث طُوِّرت قدراتٌ هجوميَّةٌ ودفاعيَّةٌ معًا، ضمن شكلٍ

---

[٣٩] "الحرب في الحيِّز الافتراضيِّ"، ترجمة سعيد عيَّاش، **قضايا إسرائيليَّة**، العدد ٤٣-٤٤ (شتاء ٢٠١٢).

[٤٠] يوسف أبو الحجاج، **أشهر جرائم الكمبيوتر والإنترنت** (القاهرة: دار الكتاب العربيِّ، ٢٠١٠)، ص ١٦٤.

[٤١] "الأنونيموس (Anonymous) عبثٌ إلكترونيٌّ، أم جيشٌ إلكترونيٌّ كسر نظريَّة الجيوش النِّظاميَّة التَّقليديَّة"، انظر:

http://www.shofakhbar.com/articles/4661566/

[٤٢] الزَّرو، **الفضاء المعلوماتيُّ**، ص ٢١٩.

[٤٣] روبرت كنيك، **حوكمة الإنترنت في عصر انعدام الأمن الإلكترونيِّ**، سلسلة **دراسات عالمية**، العدد ٩٥ (أبوظبي: مركز الإمارات للدِّراسات والبحوث الاستراتيجيَّة، ٢٠١١)، ص ١٣.

جديدٍ من أشكال سباقات التَّسلُّح[٤٤]. وسعت دولٌ أخرى لافتتاح معسكراتٍ لتدريب قطعات الجيوش على شنِّ هجماتٍ استباقيَّةٍ أو استراتيجيَّةٍ بأدواتٍ رقميَّةٍ عالية المستوى[٤٥]. الكلُّ يتحدَّث اليوم عن هجمات الإنترنت التي أصبحت تعادل في أضرارها المباشرة وغير المباشرة والقصيرة والطويلة الأمد تلك التي تتسبَّب بها الهجمات الصَّاروخيَّة والجوِّيَّة.

ومن أكثر المهتمِّين بهذه الأمور حاليًّا وزارة الدِّفاع الأميركيَّة؛ إذ لاحظت في الآونة الأخيرة مدى تقدُّم الصِّين عليها في هذا المجال، كما لاحظت ذلك دولٌ أخرى، ولا سيَّما كوريا الجنوبيَّة ودولٌ أوروبيَّةٌ كبيرةٌ. على هذا الأساس، قرَّرت الوزارة في أواخر عام ٢٠١٢ تمويل برنامجٍ بحثيٍّ تتولَّاه "وكالة مشاريع الأبحاث المتقدِّمة"، أطلقت عليه اسم "بلان إكس" Plan X لاختراع تقنيات إنترنت عالية المستوى وثوريَّةٍ قادرةٍ على فهم المعارك وتخطيطها وإدارتها عبر الإنترنت. والأكثر من ذلك إعلان القوَّات الجوِّيَّة الأميركيَّة في آب/ أغسطس ٢٠١٢ أنَّها تبحث عن أفكارٍ جديدةٍ حول كيفيَّة "تدمير، ومنع، وإفساد، وتعطيل، وتضليل، وإبطال أو لجم قدرة الأعداء على استخدام الإنترنت لصالحهم"[٤٦]. وقد أُطلقت قيادة الفضاء الافتراضيِّ للولايات المتَّحدة United States Cyber Command وهي التي أُسِّست عام ٢٠١٠، متأخرة جدًّا عن نظيرتها التَّابعة للاتِّحاد الأوروبِّيِّ التي أُسِّست عام ٢٠٠٤ تحت اسم "وكالة الشَّبكة الأوروبِّيَّة وأمن

---

[٤٤] "في بعض الأحيان تقف وراء عمليَّات الهجمات الإلكترونيَّة دولٌ، كجزءٍ من خططها الحربيَّة، لكن بدلًا من الهجوم العسكريِّ المباشر، تستهدف أنظمة المعلومات لدى الدَّولة المعادية، ومثال ذلك ما حدث عام ٢٠٠٨، حين أرادت روسيا صدَّ هجماتٍ إلكترونيَّةٍ ادَّعت أنَّها تعرَّضت لها من قبل جورجيا، فلم تستعن بخبراء المعلومات الحكوميِّين لصدِّ الهجمات، ولكن استعانت بالميليشيات الإلكترونيَّة التي قامت بمهاجمة نظم المعلومات الجورجيَّة من دون أن تتعرَّض روسيا للمساءلة القانونيَّة. وتمثِّل الحالة الروسيَّة مثالًا لرعاية دول كبرى لميليشيات القرصنة الإلكترونيَّة واستخدامها عند الحاجة. وترتبط عمليَّات الاختراق بغرض التَّجسُّس عادةً بمجموعات مدعومةٍ من الدَّولة نفسها، فقد قامت مجموعاتٌ من القراصنة الصِّينيِّين بهجماتٍ على شبكات وزارة الدِّفاع الهنديَّة، وتمكَّنت من الحصول على أسرار الجيش الهنديِّ، ولم تكتشف الهند الأمر إلَّا متأخرًا جدًّا، فقامت بإنشاء ما أسمته سلاح الدِّفاع ضدَّ الهجمات السَّيبرانيَّة بغرض تأمين الأسرار العسكريَّة. انظر: خيري، "إسرائيل وقراصنة الإنترنت".

[٤٥] جورجي، "تجربةٌ أولى ناجحةٌ للحرب الإلكترونيَّة على إسرائيل".

[٤٦] المرجع نفسه.

المعلومات" وإن كان دورها العسكريُّ شهد تطويرًا في عام ٢٠١٠. كما طوَّرت بريطانيا قدراتها منفردةً في عام ٢٠١٠ [٤٧].

كما تجدر الإشارة إلى أنَّ ثمَّة تسارعًا محمومًا بين الدُّول الغربيَّة على تكوين الجيوش الافتراضيَّة والتَّصدِّي لهذا التَّحدِّي، فثمَّة دولٌ عدَّةٌ طوَّرت قدراتٍ على القيام بعمليَّاتٍ إلكترونيَّةٍ هجوميَّةٍ متطوِّرةٍ، بينما شرع ما يزيد على مئة دولةٍ في تنظيم وحداتٍ للحروب الإلكترونيَّة[٤٨]. أمَّا في الدُّول العربيَّة فـ "هناك جهودٌ متعدِّدةٌ في هذا المجال، وأكثرها جهودٌ سرِّيَّةٌ، وإن كان هناك إشارةٌ لكون المغرب تملك واحدةً من أكثر هذه الجهود تقدُّمًا، وهناك العديد من دول الخليج التي تعمل في هذا السِّياق، وخاصَّةً أنَّ القدرات الإيرانيَّة المتسارعة في هذا الإطار تجعل التَّحدي أكبر، وخاصَّةً مع استعداد الإيرانيِّين لاستخدام هذه القدرات ضدَّ أيٍّ من الدُّول العربيَّة بما يخدم أجندتهم التَّوسُّعيَّة والأيديولوجيَّة، وهو أمرٌ في الغالب سيسرِّع من تطوُّر هذا الأمر عربيًّا"[٤٩].

إنَّ السِّباق بين الدُّول لم يعد مقصورًا على تصنيع أنواع الصَّواريخ أو المقاتلات، بل يشتمل على تطوير أنظمةٍ تحصِّن المواقع من عمليَّات القرصنة. و"رغم ذلك فإنَّ ما نجح فيه البعض هو اختصار زمن القرصنة، وسرعة تشغيل المواقع المخترَقة، أمَّا درء أو منع الهجمات الإلكترونيَّة فلم يتمكَّن الآن أحدٌ من اكتشافه في العالمين الافتراضيِّ والواقعيِّ"[٥٠]. ولا شكَّ أنَّ الهجوم الافتراضيَّ الذي تعرَّض له المشروع النَّوويُّ الإيرانيُّ في عام ٢٠٠٩، قد جسَّد الطَّاقة الكامنة الهائلة للسِّلاح الإلكترونيِّ عبر الفضاء

---

[٤٧] عمَّار بكَّار، "هل تكون الحرب العالميَّة الثَّالثة افتراضيَّةً؟" جريدة **الشرق** السُّعوديَّة، العدد ٣٧، ٢٠١٢/١/١٠، انظر:

https://www.alsharq.net.sa/lite-post?id=79506

[48] "Virtually Here: The Age of Cyber Warfare," McAfee Virtual Criminology Report, 2009, p.13, at: http://www.mcafee.com/us/resources/reports/rp-virtual-criminology-report-2009.pdf

[٤٩] بكَّار، "هل تكون الحرب العالميَّة الثَّالثة افتراضيَّةً؟".

[٥٠] "الهجوم الإلكترونيُّ على مواقع إسرائيليَّةٍ"، **الجزيرة نت**، ٢٠١٣/٤/٨، انظر:

http://www.aljazeera.net/programs/pages/dcf90ad4-7e85-4e4c-962e-7d6a2c063e31

الافتراضيِّ، واعتُبر حدثًا مؤسِّسًا في تطوُّره كمجالٍ قتاليٍّ. وفي هذا السِّياق، فإنَّ عددًا من حوادث الهجمات الافتراضيَّة، واستعداد بعض الدُّول في الحيِّز الافتراضيِّ، كل ذلك يدلُّ على أنَّ سباق التَّسلُّح الافتراضيِّ قد انطلق؛ إذ أقيمت في السَّنوات الأخيرة، في دولٍ مختلفةٍ، هيئاتٌ ودوائر تتناول الحيِّز الافتراضيَّ كحيِّزٍ قتاليٍّ، كما جرت بلورة إستراتيجيَّاتٍ أمنيَّةٍ للعمل في هذا الحيِّز (في الولايات المتَّحدة وبريطانيا وفرنسا وألمانيا والصِّين (التي خصَّصت أحد أذرع "جيش التَّحرير الشَّعبيِّ الصِّينيِّ" للقتال على مدار السَّاعة عبر الإنترنت، بهدف الحصول على معلوماتٍ استخباراتيَّةٍ أميركيَّةٍ)[٥١].

وفي المرحلة الرَّاهنة، هناك الكثير من الدُّول التي تشنُّ عمليَّاتٍ إلكترونيَّةً هجوميَّةً، تحت غطاءٍ منفصلٍ، ولكنَّه ذو صلةٍ، ومفاده "التَّجسُّس" و"إعداد ميدان المعركة"، وأمَّا الأفعال، من قبيل اختراق شبكات الكهرباء، بحيث يمكن تعطيلها في زمن الحرب، فتؤدي إلى زعزعة الاستقرار، وزيادة الاحتمالات بأن يتَّسع نطاق الصِّراع في الفضاء الإلكترونيِّ إلى العالم المادِّيِّ. ولم تعد هذه العمليَّات مقصورةً على دولٍ بحدِّ ذاتها، بل يمكن أن يقوم بها أفرادٌ وجماعاتٌ ومنظَّماتٌ، وتتحوَّل الهجمات الإلكترونيَّة إلى شكلٍ من أشكال الاحتجاج، وهو ما ينطبق على ظاهرة "الأنونيمس" في هذ السِّياق. وهذا ما يعكس مدى تدخُّل الفضاء الافتراضيِّ في قلب العمل الإستراتيجيِّ للدُّول، كما يكشف أنَّ الهجوم الإلكترونيَّ بات موضوعًا إستراتيجيًّا بامتيازٍ، وربما الأكثر أهميَّةً عند الحديث عن الأمن القوميِّ للدَّولة.

## خامسًا: إسرائيل في قلب الصِّراع الإلكترونيِّ

نفَّذت مجموعة "الأنونيمس" هجماتٍ متتاليةً ومنسَّقةً ضد مواقع وصفحاتٍ لهيئاتٍ حكوميَّةٍ ومؤسَّساتٍ أمنيَّةٍ وإخباريَّةٍ إسرائيليةٍ، إلَّا أنَّ هجوم يوم السَّابع من نيسان/ أبريل ٢٠١٣ كان الأوسع والأقوى، وهو

[٥١] للمزيد انظر: "حرب إنترنت غير باردةٍ بين الصِّين وأميركا وهاكرز الوحدة ٦١٣٩٨ تحدٍّ إستراتيجي للبنتاغون"، جريدة **الحياة**، ٢٠١٣/٥/١٢، انظر: http://alhayat.com/Details/512581

أشبه ما يكون بحربٍ اشتعلت على الشَّبكة العنكبوتيَّة، قادها آلافٌ من قراصنة الإنترنت العرب والأجانب، هدفوا من خلالها لـ "محو إسرائيل من على الإنترنت، والرَّد على سياساتها ضدَّ الفلسطينيِّين"[٥٢].

إنَّ التَّحدي القائم في مجال عمليَّات اختراق المنظومات الإلكترونيَّة، لا يقتصر على دولةٍ بعينها، ولكنه طال دولًا كثيرةً؛ من بينها إسرائيل التي وجدت نفسها في الشُّهور القليلة الماضية أمام ضرباتٍ إلكترونيَّةٍ شنَّتها مجموعة "الأنونميس"، كبَّدتها خسائر معنويَّةً وماديَّةً، مما دعاها إلى حشد جيشٍ من الخبراء والتِّقنيِّين لمواجهتها. وتكمن حساسية إسرائيل ومخاوفها من خطر مجموعات القرصنة الإلكترونيَّة في إدراكها للطَّاقة الكامنة لمثل هذه الهجمات على حيِّزها الافتراضيِّ، وعلى اعتبار أنَّها تمارس على نطاقٍ واسعٍ هذا النَّوع من الحرب في محاولتها تحقيق أهدافٍ تكتيكيَّةٍ وإستراتيجيَّةٍ؛ وهذا ما أفضى إلى ظهور قراءاتٍ مختلفةٍ لوسائل الصِّراع العربيِّ – الإسرائيليِّ في المنطقة، انطلاقًا من إمكانيَّة استعمال التِّكنولوجيا والفضاء الإلكترونيِّ بشكلٍ فعَّالٍ، في حروبٍ بات فيها العقل سيِّد الموقف[٥٣].

يوم السَّابع من نيسان/ أبريل ٢٠١٣، شنَّت مجموعات قرصنةٍ إلكترونيَّة ثاني أكبر هجماتها ضدَّ المواقع الرَّسميَّة والتِّجاريَّة والاجتماعيَّة في إسرائيل، وقد وجَّهت تلك المجموعات – بالتَّعاون والتَّنسيق مع مجموعة "الأنونيمس" التي تعتبر أحد حلفاء "ويكليكس"، والمصنَّفة من قبل مجلَّة **تايم** الأميركيَّة كواحدةٍ من أكثر المجموعات تأثيرًا في العالم[٥٤] – رسالةً إلى العالم من خلال مقطع فيديو، نُشِر على موقع يوتيوب، جاء فيها أنَّ "أقوى المخترقين من مختلف أنحاء العالم قد قرَّروا أن يتوحَّدوا في كيانٍ واحدٍ؛ تضامُنًا مع الشَّعب

---

[٥٢] "رسالة من الأنونيموس إلى الكيان الصهيوني"، ٢٠١٣/٤/٧، انظر:

https://www.youtube.com/watch?v=FPbjIS-GDHU&feature=player_embedded

[٥٣] علي بدوان، "إسرائيل وحرب السَّايبر"، جريدة **البيان** الإماراتية، ٢٠١٢/٧/١٧، انظر:

http://www.albayan.ae/opinions/articles/2012-07-17-1.1689715

[٥٤] بسام القنطار، "أنونيموس: خلّي الكيبورد صاحي"، جريدة **الأخبار**، ٢٠١٣/٤/٨، انظر:

http://www.al-akhbar.com/node/180791

الفلسطينيِّ، ومحو إسرائيل من على الإنترنت"[٥٥]. وفي ذلك المقطع ظهر شخصٌ يلبس قناع المجموعة، ويتحدَّث عن خطوات الهجوم التي حدَّدها بمسح إسرائيل من الشَّبكة العنكبوتيَّة، وفضح الخطط المستقبليَّة والجرائم، بينما لم يتمَّ الإفصاح عن الخطوة الثَّالثة، وقال: "أمَّا الخطوة الثَّالثة والأخيرة سنقدِّمها لكم هديَّةً نحن الأنونيموس"[٥٦].

شُنَّت الهجمات الإلكترونيَّة باسم # OpIsrael من خلال "تكنيك الهجمات الموزَّعة"، واستطاعت من خلاله توجيه ضربةٍ رقميَّةٍ إلى إسرائيل، ويُعدُّ هذا "التكنيك" من التِّقنيات المتقدِّمة التي باتت تستخدمها جماعة "الأنونيمس" وتثير قلق المهتمِّين بالشَّبكة العنكبوتيَّة والشَّبكات الرَّقميَّة. وقد نفَّذ الهجومَ على المواقع الإسرائيليَّة مجموعة قراصنة الإنترنت من دولٍ عدَّةٍ؛ بينها: فلسطين ولبنان والجزائر وإيران وجنوب أفريقيا وفرنسا والولايات المتَّحدة وألبانيا وكوسوفا والمغرب وتركيا وإندونيسيا وتونس ومصر والسُّعوديَّة والأردنُّ وغيرها. ونجح الهجوم في التَّشويش، وإسقاط العشرات من المواقع الإلكترونيَّة الإسرائيليَّة التي أضحت غير متاحةٍ على الإنترنت. كما تزامن موعد الهجوم في ٧ نيسان/ أبريل مع يوم ذكرى الهولوكوست – ذكرى المحرقة – التي قالت المجموعة المهاجمة في رسالتها للإسرائيليِّين: إنها فكرةٌ "ابتدعتموها وأولياؤكم وجعلتم العالم يؤمن بالمحرقة اليهوديَّة".

واستهدف الهجوم مواقع إلكترونيَّةً مهمَّةً في إسرائيل، ونجح في اختراق مواقع[٥٧] الحكومة والجيش والصِّناعات العسكريَّة، ومن ذلك مواقع: رئيس الوزراء، ووزارة الدِّفاع، والاستخبارات، ومجلس الوزراء،

---

[٥٥] "رسالة من الأنونيموس إلى الكيان الصهيوني".

[٥٦] حسب ما جاء في الرِّسالة التي وجَّهتها المجموعة المهاجِمة للإسرائيليِّين: "أنتم لم تتوقَّفوا قطُّ عن انتهاكاتكم التي لا تنتهي لحقوق الإنسان، لم تتوقَّفوا قطُّ عن المستوطنات غير الشَّرعيَّة، لم تحترموا وقف إطلاق النَّار، بل حتَّى لا تحترمون القانون الدَّوليَّ" انظر: http://www.youtube.com/watch?v=0_rEQKUpsUc

[٥٧] للمزيد حول المواقع التي اختُرقت، انظر:

http://www.israj.net/arabic/index.php/2011-05-14-07-15-55/2011-05-14-07-16-17/2011-05-14-23-52-51/7087-7-2013

وسوق الأوراق الماليَّة، والمحاكم الإسرائيليَّة، وشرطة تل أبيب، وحزب كاديما، ووزارة التَّعليم، وبنك القدس، ونحو ٢٠٠٠٠ حسابٍ على الفيسبوك و٥٠٠٠ حسابٍ بنكيٍّ، وغيرها. وقامت "أنونيمس" بنشر بياناتٍ شخصيَّةٍ لأكثر من ٥٠٠٠ مسؤولٍ إسرائيليٍّ؛ منها أسماؤهم وأرقام هويَّاتهم والعناوين الشَّخصيَّة لبريدهم الإلكترونيِّ، كما كشفت المجموعة عن بياناتٍ لأكثر من ٦٠٠٠٠٠ مستخدمٍ إسرائيليٍّ. ووضع "الهاكرز" في هذه المواقع رسائل مؤيِّدةً وداعمةً للفلسطينيِّين، وأغاني، وتنديدًا بالسِّياسات الحربيَّة الإسرائيليَّة، وجرى كذلك وضع سورٍ من القرآن الكريم في بعضها. وتمكَّن "الهاكرز" أيضًا من عرض قضيَّة الأسرى الفلسطينيِّين من خلال وضع صورٍ لبعضهم – مثل صورة الأسير الفلسطينيِّ الذي كان مضربًا عن الطَّعام، سامر العيساويِّ، التي احتلَّت شاشات الحاسوب المخترَقة – وعرض جرائم الاحتلال الإسرائيليِّ على مائدة الرَّأي العامِّ العالميِّ[٥٨].

سادت بعد الهجوم الإلكترونيِّ حالةٌ من الجدل السِّياسيِّ والاقتصاديِّ والعسكريِّ والإعلاميِّ لدى جمهورٍ واسعٍ من المجتمع الإسرائيليِّ، عبَّرت عنه وسائل الإعلام المختلفة حول الجاهزيَّة الأمنيَّة والتَّحصين الإلكترونيِّ لمثل هذا الهجوم والخسائر الماديَّة المتوقَّعة.

وعلى الرَّغم من الاستعدادات الإسرائيليَّة لمثل ذلك الهجوم، فإن الهجوم الإلكترونيَّ كان الأشدَّ من نوعه، أي أقوى بعشرة أضعافٍ من هجومٍ مشابهٍ تعرَّضت له إسرائيل خلال عمليَّة "عمود السَّحاب" العسكريَّة الإسرائيليَّة ضدَّ قطاع غزَّة في تشرين الثَّاني/ نوفمبر ٢٠١٢، وثمَّة "أقلُّ من ١٠٠ موقعٍ إلكترونيٍّ صغيرٍ وحوالي ١٥ موقعًا إلكترونيًّا لمنظَّماتٍ كبيرةٍ تضرَّرت لفتراتٍ تراوحت ما بين دقائق معدودةٍ وساعاتٍ عدَّةٍ،

---

[٥٨] "أنونيموس تشنُّ أعنف هجومٍ إلكترونيٍّ ضدَّ إسرائيل"، ٢٠١٣/٤/٧، انظر:

http://www.tech-wd.com/wd/2013/04/07/opisrael

وللمزيد عن حجم الخسائر، انظر: "أنونيموس تعطِّل إنترنت إسرائيل بـ ٤٤ مليون هجمةٍ"، جريدة **الاقتصادية** السعودية، ٢٠١٣/٤/٨، انظر:

http://www.aleqt.com/2013/04/08/article_745515.html

وبينها موقعان أو ثلاثةٌ تضرَّرت لفترات طويلةٍ"[٥٩]. كما أنَّ عدد مواقع المصالح التِّجاريَّة الصَّغيرة في إسرائيل التي اخترقها الهاكرز يصل إلى مئاتٍ، وربَّما أكثر من ذلك[٦٠].

سرَّبت مجموعة "أنونيمس" في ٢٨ حزيران/ يونيو ٢٠١١، وفي مواقع عدَّةٍ، رسالةً تتضمَّن هجومًا إلكترونيًّا على الموقع الرَّسميِّ للكنيست الإسرائيليَّة، وعطَّلت أعمالها لساعاتٍ، ردًّا على قمع الفلسطينيِّين واحتلال أراضيهم. ولأنَّ الحكومة الإسرائيليَّة كانت قد شنَّت حربًا إلكترونيَّةً على إيران ولبنان (بعثت بفيروس "ستاكس نت" Stuxnet للهجوم على المنشآت النَّوويَّة الإيرانيَّة، وقامت بقرصنة شركات الاتِّصالات اللبنانية عبر عملاء لها)[٦١]، فإن هذا الأمر في نظر "أنونيمس" يحلُّ الهجوم عليها. وقد بعثت المجموعة برسالةٍ مصوَّرةٍ، استعملت فيها برنامجًا آليًّا يقرأ من خلاله إنسانٌ آليٌّ العبارات التَّالية: "إلى الشَّعب الفلسطينيِّ النَّبيل: خلال الأعوام الخمسة والسِّتين الماضية فُرض عليكم العيش في أوضاعٍ لاإنسانيَّةٍ من طرف نظامٍ صهيونيٍّ عنصريٍّ غير قانونيٍّ ... أنونيمس هي إخوانكم وأخَواتكم، أبناؤكم وبناتكم، أهاليكم وأصدقاؤكم، بغضِّ النَّظر عن السِّنِّ والجنس والعرق والدِّين والإثنيَّة، أو مكان الولادة. أنونيمس هي أنتم متَّحدين أقوياء... انضمُّوا إلينا في معركة حرِّيَّة المعلومات حول العالم ... نحن لا نسامح، ولا ننسى"[٦٢].

---

[٥٩] "أنونيموس تعطِّل إنترنت إسرائيل".

[٦٠] "على الرَّغم من تأكيد صدِّ الهجوم، إسرائيل تقرُّ: هجوم السَّايبر الأخير الذي تعرضنا له كان الأشدَّ حتَّى الآن"!، **المشهد الإسرائيليُّ**، تقرير خاص، ٢٠١٣/٤/٩، انظر:

http://www.madarcenter.org/pub-details.php?id=441

[٦١] في نيسان/ أبريل ٢٠١٢ اتَّهمت إيران كلًّا من إسرائيل والولايات المتحدة باختراق أجهزة الكمبيوتر في مفاعل بوشهر النَّوويِّ، وزرع فيروس "ستاكس نت" الذى أثَّر في مفاعلات إيران النَّوويَّة.

[62] Anonymous- Operation Palestine- Short Press Release, 1/3/2011, at: http://www.youtube.com/watch?v=2-zXF1DVNDY

وفي عام ٢٠١١ قامت مجموعةٌ من "جماعة الأنونيمس المصريِّين" بتنفيذ "العمليَّة نتنياهو"، بالهجوم على موقع رئيس الوزراء الإسرائيليِّ، بنيامين نتنياهو، انتقامًا لمقتل جنودٍ مصريِّين على الحدود، وجرى بالفعل تعطيل الموقع، بالإضافة لمواقع إلكترونيَّةٍ إسرائيليَّةٍ أخرى[٦٣].

وفي عام ٢٠١٢ نجح مواطنٌ سعوديٌّ في التَّاسعة عشرة من عمره، سمى نفسه OXOMAR، في اختراق مواقع إلكترونيَّةٍ تخصُّ أفرادًا ومصارف، والحصول على معلوماتٍ تتعلَّق بعشرات آلاف بطاقات الائتمان العائدة لإسرائيليِّين، وقام بنشرها على الملأ، وهذا ما يمكِّن أيَّ شخصٍ من شراء ما يريد على الإنترنت باستخدام تلك البطاقات[٦٤]. وكشفت جريدة **يديعوت أحرنوت** في ١٧ كانون الثَّاني/ يناير ٢٠١٢ أنَّ الشَّابَّ السُّعوديَّ المذكور حاول اختراق مواقع إلكترونيَّةٍ إسرائيليَّةٍ حسَّاسةٍ؛ منها مواقع بنى تحتيَّةٍ ووزاراتٍ وإداراتٍ حكوميَّةٍ. وأضافت الجريدة أنَّ الشَّابَّ أكَّد أنَّه قام بذلك انتقامًا من إسرائيل على أعمال القتل والاعتداء على الفلسطينيِّين، وأنَّ حرب غزَّة ٢٠٠٨-٢٠٠٩ كانت محفِّزةً له ليقوم بما قام به[٦٥].

بعد حادث "أسطول الحرِّيَّة" التُّركيِّ، في نهاية أيَّار/ مايو ٢٠١٠، تعرَّض نحو ألف موقعٍ إسرائيليٍّ للاختراق من جانب "هاكرز" أتراكٍ[٦٦]. وفي التَّاسع والعشرين من تشرين الثَّاني/ نوفمبر ٢٠١٠ اغتيل عالمٌ نوويٌّ إيرانيٌّ في طهران وأصيب عالمٌ آخر. بعد ذلك بيومين توقَّفت شبكة الاتِّصالات الإسرائيليَّة "سيلكوم" عن العمل ساعاتٍ بعد هجوم إلكترونيٍّ[٦٧]. وفي الخامس والعشرين من كانون الثَّاني/ يناير ٢٠١١،

---

[٦٣] أبو طالب، "أنونيمس".

[٦٤] غازي حمد، "الجهاد الإلكترونيُّ.. والحرب الجديدة ضدَّ إسرائيل"، جريدة **فلسطين**، ٨ نيسان/ أبريل ٢٠١٣.

[٦٥] شهبون، "حروب السَّايبر".

[٦٦] المرجع نفسه.

[٦٧] المرجع نفسه.

سقطت أيضًا شبكة "بيزيك" للاتّصالات الإسرائيليَّة، وانقطعت الخدمة عن العملاء ساعاتٍ عدَّةً، وعلى إثر ذلك تحدَّث البعض في إسرائيل عن عطلٍ فنّيٍّ، وآخرون اعتبروه اختراقًا من قبل قراصنةٍ لتلك الشَّبكة[٦٨].

### ١. الإمكانيَّات الإسرائيليَّة في الفضاء الإلكترونيّ

أصبحت الحرب الإلكترونيَّة من الأدوات الرَّئيسة المستخدمة من قبل الجيش الإسرائيليّ لتحقيق أهدافه الإستراتيجيَّة؛ انطلاقًا من إدراك إسرائيل لحقيقة أنَّ الحرب القادمة هي حرب الفضاء الإلكترونيّ. وقد اعتبرها المراسل العسكريُّ الإسرائيليُّ أليكس فيشمان أنَّها حربٌ تستعد لها تل أبيب جيِّدًا، خشية أن تدخل في أنظمتها الحسَّاسة فيروسات تشلُّ عملها في أحرج الأوقات، خاصَّةً أنَّ "أعداءها" نجحوا في السَّيطرة على عدَّة أنظمةٍ في السَّنوات الأخيرة، وقفزوا إلى مراتب تقنيَّةٍ ذات صلة بحرب "السَّايبر"، التي يسمِّيها "حرب الظِّلال" الجارية بين الجيوش في عمق قلب معلومات العدوّ، وهي جبهةٌ ديناميَّةٌ يستعملون فيها سلاحًا ثقيلًا، وتشبه الحديث عن "رقعة شطرنجٍ" ضخمةٍ عالميَّةٍ تتحارب فيها أفضل العقول"[٦٩].

لذا ظهرت دعواتٌ من داخل المؤسَّسة الأمنيَّة ولجنة الخارجيَّة والأمن في الكنيست، تنادي بضرورة إعادة صوغ النَّظرية الأمنيَّة الإسرائيليَّة التي بُلوِرت مطلع خمسينيَّات القرن الماضي بما يتوافق مع تلك الحرب التي باتت تشكِّل هاجسًا يلفُّ إسرائيل، مما دعاها إلى إجراء العديد من التَّجارب في هذا المجال، وخرجت بنتائج تؤكِّد الخطورة المتولِّدة من إمكانيَّة اختراق المواقع الحسَّاسة في إسرائيل. ولهذا، حاولت أن تسخِّر إمكانياتٍ بشريَّةً ومادِّيَّةً لدعم هذه المشاريع.

كما تطرَّق الجنرال عاموس يادلين، رئيس شعبة الاستخبارات العسكريَّة (سابقًا)، إلى هذا الموضوع في محاضرةٍ ألقاها في معهد دراسات الأمن القوميّ بجامعة تل أبيب في كانون الأوَّل/ ديسمبر ٢٠٠٩،

---

[٦٨] المرجع نفسه .

[٦٩] عدنان أبو عامر، "إسرائيل وحرب الإنترنت"، **الجزيرة نت**، انظر:

http://www.aljazeera.net/opinions/pages/910f8b7d-b7d0-4ac1-b875-78cca8d77c8e

بقوله: إنَّ "الجيش الإسرائيليَّ يعتزم توفير حمايةٍ جيِّدةٍ للشَّبكات، والقيام أيضًا بشنِّ هجماتٍ افتراضيَّةٍ". إنَّ بإمكان الهيئة الافتراضيَّة التَّابعة للجيش الإسرائيليِّ المشاركة في حماية الحيِّز الافتراضيِّ لإسرائيل، على غرار القيادة الافتراضيَّة في الولايات المتَّحدة، لكنَّها ليست الهيئة المخصَّصة لتوفير الحماية القوميَّة الشَّاملة للحيِّز الافتراضيِّ القوميِّ للدَّولة[٧٠].

ومع ذلك، تبقى الأدبيَّات المتاحة للبحث في هذا الموضوع قليلةً؛ إذ لا تتناول بوضوحٍ إستراتيجيَّة إسرائيل وعقيدتها إزاء الأمن الإلكترونيِّ سوى بشكلٍ طفيفٍ. وعند الحديث عن الاستعدادات التي قامت بها إسرائيل لحماية مجالها الافتراضيِّ، فمن الممكن الإشارة إلى عددٍ من النِّقاط البارزة في هذا السِّياق:

١. تركِّز الوحدة ٨٢٠٠ للجيش الإسرائيليِّ، المكوَّنة من المجنَّدين والضُّبَّاط، أعمالها على ثلاث نَواحٍ من الحرب الإلكترونية؛ هي: جمع المعلومات الاستخباراتيَّة، والدِّفاع والهجوم الإلكترونيَّان.
٢. يتولَّى جهاز الأمن الدَّاخليَّ (شن–بيت) الدِّفاع عن الأنظمة الحاسوبيَّة للحكومة الإسرائيليَّة، والبنية التَّحتيَّة الإلكترونيَّة للدَّولة، والمعلومات المتعلِّقة بالقطاع المصرفيِّ، وذلك منذ نهاية التِّسعينيَّات، وله نشاطات واسعةٌ في حروب الإنترنت والشَّبكات، وهو يعدُّ وحدةً جاذبةً لأفضل العقول التِّكنولوجيَّة الإسرائيليَّة، وقد اعتُبِر أكبر وأخطر سادس وحدةٍ تقوم بإطلاق هجمات الإنترنت حول العالم[٧١].
٣. أصبح للجيش الإسرائيلي ما يقرب من ٣٠٠ خبير كمبيوتر شابٍّ يعملون خبراء على الشَّبكة العنكبوتيَّة، وأجرى توزيع ٣٠ عاملًا على الإنترنت في فروعٍ مختلفةٍ، للإشراف على شبكات الكمبيوتر، ويُعتقَد أنَّ الوحدة ٨٢٠٠ التي انبثقت من هيكليَّة جهاز الإشارة هي في صميم هذه القوَّة[٧٢].

---

[70] "CYBER WARFARE: CONCEPTS AND STRATEGIC TRENDS", *AT:* http://dno8g1zsiv2fs.cloudfront.net/upload/(FILE)1337837176.pdf

[٧١] جورجي، "تجربةٌ أولى ناجحةٌ".

[٧٢] يوسف بوغنيمي، "الأنونيموس Anonymous عبثٌ بالأنترنيت، أم جيشٌ إلكترونيٌّ كسر نظريَّة الجيوش النِّظاميَّة التَّقليديَّة"، **مراكش برس**، ٢٠١٣/٤/١٠، انظر: http://www.marrakechpress.com/?p=6279

٤. يتولَّى جهاز C4I مسؤوليَّة الاتصال وتنظيم القدرات الإسرائيليَّة وتنسيقها في الدِّفاع عن المجال الافتراضيِّ[٧٣]. وقد جرى تعيين ضابط ذي رتبةٍ عاليةٍ من جهاز الاستخبارات الإسرائيليِّ في مركز الشيفرة والأمن المعلوماتيِّ (المعروف باسمه المختصر بالعبريَّة "ماتزوب")، وكانت لديه المسؤوليَّة لجمع المعلومات حول قدرات "خصوم" إسرائيل في مجال القرصنة الإلكترونيَّة. ويقوم "ماتزوب" بشيفرة الاتِّصالات المنقولة من شبكات الشن–بيت والموساد والجيش الإسرائيلي. ولدى الجهاز نفسه فرق عملٍ تقوم بفحص الشَّيفرة و"جدران" الدِّفاع الافتراضيِّ الإسرائيليِّ[٧٤].

٥. في عام ٢٠١٢ خصَّص معهد الأمن القوميِّ الإسرائيليُّ برنامجًا تدريبيًا حول "الأمن السَّيبرانيِّ" أو أمن المعلومات، وأصدر المعهد في أيار/ مايو ٢٠١٢ تقريرًا مفصَّلًا عن "الحرب السَّيبرانيَّة"، أوصى فيه الإدارة الإسرائيليَّة بالعمل على تطوير القدرات الهجوميَّة والدِّفاعيَّة، وإجراء تدريباتٍ وطنيَّةٍ ودوليَّةٍ، ورفع حالة التَّأهب القصوى، مع إدراج الأمن المعلوماتيِّ في إستراتيجيَّات الدِّفاع الإسرائيليَّة[٧٥].

٦. في آذار/ مارس ٢٠١١ أجازت الحكومة إقامة وحدة "منمار" (مديريَّة منظومات المعلومات الحكوميَّة، وهي هيئةٌ بين–وزاريَّةٍ، مهمَّتها تركيز مجال الاتِّصالات الإلكترونيَّة في الحكومة وتنسيقه. ويُفترَض بهذه الهيئة التي تخضع لمسؤولية المدير العامِّ في وزارة الماليَّة أن تقوم بتوجيه وحدات الاتِّصال الإلكترونيِّ في وزارات الحكومة، وأن تتحمَّل المسؤوليَّة المباشرة عن جميع مشاريع الحوسبة الحكوميَّة[٧٦].

---

[73] James A. Lewis and Katrina Timlin, *Cyber Security and Cyber Warfare, Preliminary Assessment of National Doctrine and Organization*, Center for Strategic and International Studies (CSIS), 2011, at: http://www.unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf

[74] Ibid.

[٧٥] خيري، "إسرائيل وقراصنة الإنترنت".

[٧٦] "مقاطع من مذكِّرةٍ بشأن استعدادات إسرائيل لمواجهة عصر الحرب الافتراضيَّة"، **المشهد الإسرائيليُّ**، العدد ٢٩٢، ٢٣ تشرين الأوَّل/ أكتوبر ٢٠١٢، ص٧، انظر:

HTTP://WWW.MADARCENTER.ORG/MASH_HAD_PDF/AL-MASHHAD%2023-10-2012.PDF

٧. أجازت الحكومة الإسرائيليَّة في ٢٧ آذار/ مارس ٢٠١١ إقامة "وحدة إدارة المعلومات"، وهي تتبع مدير عامَّ وزارة الماليَّة الإسرائيليَّة، ومسؤولةٌ مسؤوليةً مباشرةً عن جميع أنظمة الاتِّصالات المحوسبة الحكوميَّة، ومنها مشروع "بنية الحكومة التَّحتيَّة لعصر الإنترنت"[٧٧].

٨. استحدثت الدَّولة الإسرائيليَّة جهازًا آخر في ١٨ أيَّار/ مايو ٢٠١١، وهو "الفريق القوميُّ المخصَّص للمجال الافتراضيِّ". يقوم هذا الفريق بتحصين الشَّبكات المفصليَّة للدَّولة الإسرائيليَّة ضدَّ القرصنة، وحماية القطاع الخاصِّ في هذا المجال. ويتكوَّن الفريق من ٨٠ شخصًا يقومون بمهمَّاتٍ دفاعيَّةٍ. وسيقوم الفريق بتخصيص موارد لتحسين البحث الجامعيِّ المتعلِّق بالدِّفاع عن المجال الافتراضيِّ ورفع عدد الطُّلَّاب المهتمِّين بهذا الموضوع[٧٨].

٩. في عام ٢٠٠٢ أقيمت السُّلطة الرَّسميَّة لحماية المعلومات في جهاز الأمن العامِّ "(الشَّاباك)، وهي مسؤولةُ عن التَّوجيه المهنيِّ للهيئات ذات الصِّلة بنطاق مسؤوليتها، في مجال حماية شبكات حاسوبٍ حيويَّةٍ من التَّهديدات الإرهابيَّة والتَّخريب في مجال حماية المعلومات المصنَّفة (السِّريَّة) وتهديدات التَّجسُّس والكشف[٧٩].

١٠. في عام ٢٠٠٩ أطلقت إسرائيل برنامجًا جديدًا بمنزلة "قبَّةٍ حديديَّةٍ رقميَّةٍ" تابعًا لـ "مكتب إسرائيل للحرب الافتراضيَّة"، وحسب تصريحات رئيس الوزراء الإسرائيليِّ، بينامين نتنياهو، فإنّ هذا المشروع "يقوم على تدعيم قدرات إسرائيل التِّكنولوجيَّة، من أجل التَّعامل مع الهجمات الإلكترونيَّة، ويستهدف الطلاب المتميِّزين الذين تتراوح أعمارهم ما بين ١٦ و١٨ سنةً، وتوكل إليهم مهمَّة اعتراض الهجمات الإلكترونيَّة التي تُشنُّ على إسرائيل[٨٠].

---

[٧٧] المرجع نفسه.

[78] Lewis and Timlin, *Cyber Security and Cyber Warfare*.

[79] Ibid.

[80] "Netanyahu: We're Building a Digital Iron Dome," *The Jerusalem Post*, 1/1/2013, at: http://www.jpost.com/DiplomacyAndPolitics/Article.aspx?id=298023

١١. هيئة الـ "سايبر" التَّابعة للجيش الإسرائيليِّ: في عام ٢٠٠٩ وصف الجنرال غابي أشكنازي، رئيس هيئة الأركان العامَّة، الحيِّز الافتراضيَّ بأنه حيِّزٌ قتاليٌّ إستراتيجيٌّ[٨١]. وبناءً على ذلك، أقيمت هيئة الـ "سايبر" في الجيش الإسرائيليِّ، لكي تستخدمها هيئة الأركان العامَّة في تنسيق نشاطات الجيش في الحيز الافتراضيِّ وتوجيهها[٨٢].

١٢. في عام ١٩٩٧ أقيم مشروع البنية التَّحتيَّة الحكوميَّة لعصر الإنترنت (مشروع "تهيلاه"). والهدف من المشروع، الذي أقيم في قسم المحاسب العامِّ في وزارة الماليَّة، هو تزويد خدمات تصفُّحٍ محميَّةٍ لوزارات الحكومة ومؤسَّساتها ودوائرها. ويستخدم "تهيلاه" وسائل وتدابير لحماية أمن شبكة الإنترنت الحكوميَّة، ابتداءً من طاقم خبراء حماية معلوماتٍ واتِّصالاتٍ، وانتهاءً بمنتجاتٍ وتقنياتٍ لشركاتٍ عالميَّةٍ رائدةٍ. كما أقيم في إطار "تهيلاه" مركز حماية معلومات حكومة إسرائيل الذي تشمل مهمَّاته المتابعة والرَّصد لحوادث حماية المعلومات على مستوى العالم، مع إيلاء اهتمامٍ لهجماتٍ داخل الشَّبكة تتعلَّق بإسرائيل؛ والتَّنسيق بين هيئاتٍ حكوميَّةٍ من أجل حلِّ مشكلات الحماية وتنسيق العلاقة بين هذه الهيئات وبين جهاتٍ خارجيَّةٍ، إضافةً لإجراء أبحاثٍ ودراساتٍ في هذا المجال. كما يُصدر المركز إنذارات حماية معلوماتٍ للمنظَّمات العاملة في مجال تكنولوجيا المعلومات، التي تقيم علاقاتٍ مع "تهيلاه"، أو لجهاتٍ حكوميَّة غير مصنَّفةٍ[٨٣].

---

[٨١] محمود محارب، عرضٌ لكتاب **إسرائيل والحرب الإلكترونيَّة**، موقع المركز العربيِّ للأبحاث ودراسة السِّياسات، ١٠ آب/ أغسطس ٢٠١١، انظر:

http://www.dohainstitute.org/release/14e23aac-b76f-48f8-ba00-c94efe48fa36#a1

[٨٢] المرجع نفسه.

[83] "CYBER WARFARE: CONCEPTS AND STRATEGIC TRENDS."

### ٢. الأهميَّة الاقتصاديَّة لتكنولوجيا المعلومات الإسرائيليَّة والفضاء الافتراضيِّ

تُعتبَر إسرائيل من الدُّول المتقدِّمة في العالم في مضمار تطوير التِّقنيات المعلوماتيَّة والتِّكنولوجيَّة. وقد حاولت إسرائيل توظيف الهجوم الإلكترونيِّ الأخير عليها "للاستثمار بالشَّركات لتعزيز الصِّناعات الدَّقيقة، وتطوير منظومات حماية المعلومات، وجذب المستثمرين الأجانب لافتتاح المزيد من الشَّركات لصناعة وابتكار أنظمة المعلومات وتسويقها بالعالم، بما يساهم في تعزيز وتدعيم الاقتصاد الإسرائيليِّ الذي يغرق بالركود"[٨٤].

ووفقًا لدراسةٍ أجرتها شركة الاستشارات الدَّولية "ماكينزي"، فإنَّ "اقتصاد الإنترنت" في إسرائيل ينقسم إلى قسمين أو مجالين: ويتركَّز الجزء الأعظم منه في مجال صناعة تقنيات المعلومات والاتِّصالات، ويشمل ذلك إنتاج معدَّاتٍ وبرمجيَّاتٍ وخدماتٍ وبيعها، أمَّا الجزء الأصغر، وهو الذي يشهد نموًّا سريعًا، فيتمثَّل بمجال التِّجارة الإلكترونيَّة، ويُعنَى بشراء بضائع وخدماتٍ عن طريق الإنترنت[٨٥]. وبحسب الدِّراسة، فقد بلغت قيمة المساهمة المباشرة (في الإنتاج) لاقتصاد الإنترنت في إسرائيل نحو ٥٠ مليار شيكل في عام ٢٠٠٩، أي ما يشكِّل قرابة ٦,٥% من النَّاتج المحلِّيِّ الخام[٨٦]. هذا المعطى يضع إسرائيل في مصافِّ اقتصادات الإنترنت المتصدِّرة عالميًّا[٨٧].

---

[٨٤] "الحرب الإلكترونيَّة تعزِّز صناعة المعلومات الإسرائيليَّة"، **وكالة فلسطين اليوم**، ٢٠١٣/٤/١٥، انظر:

http://paltoday.ps/ar/post/165435

[85] "CYBER WARFARE: CONCEPTS AND STRATEGIC TRENDS."

[86] Ibid.

[87] Ibid.

تشير المعطيات السَّابقة إلى أنَّ الفضاء الإلكترونيَّ يشكِّل أهميَّةً كبرى وجزءًا لا يتجزَّأ من إستراتيجيَّة إسرائيل الأمنيَّة؛ إذ يجري دمج هذا الفضاء في الجهد الأمني والعسكري العملياتي[٨٨]. والهدف منه تحقيق غاياتٍ عدَّةٍ؛ بدءًا من كسر عزلتها الجغرافيَّة في الشَّرق الأوسط، مرورًا بإقامة علاقاتٍ وثيقةٍ ومنتظمةٍ مع العالم، وليس انتهاءً بتقوية الصِّلة وتعزيز التَّرابط بين الهامش والمركز في إسرائيل، وهو ما يشكِّل عنصرًا مركزيًّا في النَّشاط الاجتماعيِّ وعاملًا مهمًّا في تمتين أواصر العلاقة بين سلطات الحكم والمواطن[٨٩].

### ٣. ما أهميّة الهجوم على المواقع الإلكترونيَّة في إسرائيل؟

على الرَّغم من أنَّ مجموعة "أنونيمس" نفَّذت تهديدها في السَّابع من نيسان/ أبريل ٢٠١٣، وعلى الرَّغم من محدوديَّة الضَّربة وآثارها التي هوَّنت إسرائيل من تداعياتها[٩٠]، فإنَّها استطاعت أن تنال معنويًّا من هيبة دولةٍ متطوِّرةٍ تكنولوجيًّا ومعلوماتيًّا، وهي من أكثر الدُّول تقدُّماً في الاتِّصالات المتطوِّرة. فالهجمات الإلكترونيَّة – على الرغم من محدوديَّتها – تعطي أكثر من رسالةٍ:

---

[٨٨] تجدر الإشارة إلى قيام إسرائيل عام ٢٠٠٩ – بالتَّعاون مع الولايات المتَّحدة – بإعطاب أجهزة الطَّرد المركزيِّ التي تعتمد عليها إيران في تخصيب اليورانيوم، وذلك عبر استخدام فيروس "ستاكس نت". وقامت بهجوم إلكترونيٍّ تعرَّضت له منظومات حواسيب إيرانيَّةٌ حسَّاسة في حزيران/ يونيو ٢٠١٢، وذلك عبر استخدام فيروس "فليم" Flame. وأقدمت إسرائيل على التَّسلُّل إلكترونيًّا إلى منظومات التَّحكُّم المسؤولة عن توجيه الدِّفاعات الجويَّة السُّوريَّة عشيَّة الغارة التي نفَّذتها الطَّائرات الإسرائيليَّة على المنشأة النوويَّة السُّوريَّة قرب دير الزُّور شمال شرق سورية في أيلول/ سبتمبر ٢٠٠٦، وأبطلت عمل هذه المنظومات، حتَّى تقلَّصت فرص تعرُّض الطَّائرات المغيرة لنيران الدِّفاعات الجويَّة السُّوريَّة.

[٨٩] "الحرب في الحيِّز الافتراضيِّ".

[٩٠] قدَّرت مجموعة القراصنة العالميِّين "أنونيمس" الخسائر التي سبَّبها الهجوم الإلكترونيِّ الذي بدأته مساء السَّبت على مؤسَّساتٍ ومواقع إسرائيليَّةٍ بنحو ٣ مليارات دولارٍ أميركيٍّ، لكنَّ إسرائيل قالت: إنَّ آثار الهجوم كانت محدودةً. "أنونيموس: كبّدنا إسرائيل ٣ مليارات دولار في الهجمة الإلكترونية الأخيرة"، جريدة **المصريُّ اليوم**، ٢٠١٣/٤/٨، انظر:

http://www.almasryalyoum.com/node/1628706

الرسالة الأولى سياسيَّةٌ، تنطلق من أنَّ قضيَّة فلسطين ما زالت تعيش في وجدان الشَّباب العرب الذين استطاعوا أن يضيفوا شكلًا آخر من أشكال المقاومة في مسار الصِّراع العربيِّ–الإسرائيليِّ بتطويعهم الإنترنت بهدف المقاومة، وأنَّ هذه القضيَّة ما زالت باقيةً في قلوبهم وعقولهم افتراضيًّا كما هي على أرض الواقع.

والرِّسالة الثَّانية تكنولوجيَّةٌ، كونها استطاعت إيذاء إسرائيل افتراضيًّا، وأظهرت مدى قدرة الأخيرة في هذه الحرب، وأنَّ "قبَّتها الحديديَّة الرَّقميَّة" يشوبها قصورٌ، وأنَّ ثمَّة جهاتٍ أخرى – سواءٌ أكانت دولاً أم أفرادًا – قادرةً على إلحاق الأذى بها.

والرِّسالة الثَّالثة عسكريَّةٌ، وهي أنَّ اسرائيل وجيشها "الذي لا يُقهَر"، ليس هو القادر والمبادر فقط بتنفيذ هجماتٍ إلكترونيَّةٍ من هذا النَّوع على بلدان العالم العربيِّ–الإسلاميِّ، فتزايد الهجمات الإلكترونيَّة واتساع رقعتها عبر الشَّبكة العنكبوتيَّة من أنحاء المعمورة، واستهداف بنىً تحتيَّةٍ لإسرائيل بشكلٍ منظَّمٍ؛ مثل شبكات المياه والكهرباء وإشارات المرور والطَّاقة والبنوك، وسرقة معلوماتٍ أمنية حساسةٍ، كلُّ ذلك يعني، من جملة ما يعنيه، تهديدًا يُضاف إلى قائمة التَّهديدات النَّظريَّة الأمنيَّة لإسرائيل التي قد تستطيع الدِّفاع عن حدودها الجغرافيَّة، ولكن المسألة تصبح مختلفةً في حال هجومٍ إلكترونيٍّ يتجاوز الجغرافيا ويختصر الزَّمان، ولا يمرُّ بالحدود. وهكذا فإنها ستحضِّر نفسها بأيِّ لحظةٍ لصدِّ هجوم مثل هذا غير متوقع النَّتائج، وربما يتكرَّر بشكلٍ مستمرٍّ في ظلِّ التَّنامي العالميِّ لحجم الهجمات الإلكترونيَّة في المرحلة المقبلة.

والسُّؤال المطروح في إسرائيل اليوم هو: ماذا ستفعل لو جرى تنسيق الهجمات الإلكترونيَّة وتوسيع نطاقها بإشراك عددٍ كبيرٍ جدًّا من "الهاكرز" من جميع أرجاء المعمورة، يرسلون كمِّيَّاتٍ لا نهائيَّة[٩١] من الرَّسائل على خوادم الحواسيب الإسرائيليَّة، ويغرقون أنظمتها بشكلٍ تتوقَّف معه الشَّبكة عن العمل، ومعها أيضًا نظم الإنتاج والخدمات؟

[٩١] ذكرت وزارة الماليَّة الإسرائيليَّة أنَّ المواقع الحكوميَّة قد تعرَّضت لما يقارب ٤٤ مليونًا من الهجمات الفريدة من نوعها.

## خلاصة

أصبح المجال الافتراضيُّ بمنزلة ساحة قتالٍ جديدةٍ تشكِّل تهديدًا يضاف إلى قائمة التَّهديدات التَّقليديَّة التي تواجه العالم، وتتجاوز في أبعادها وآثارها الحدود الجغرافيَّة والسِّياسيَّة، وتلقي بتداعياتها على مستقبل الأمن القوميِّ والحيويِّ للدُّول. وأصبحت عمليَّات الاختراق التي يقوم بها "الهاكرز" قادرةً على إغراق أجهزة خوادم الحواسيب برسائل من أنظمةٍ متعدِّدةٍ تشلُّ سير عملها وتوقف نظم الإنتاج.

وثمَّة العديد من جيوش العالم المتقدِّمة التي شرعت بزيادة نشاطها وتكثيف جهودها في هذا المجال الذي يشكِّل مصدر قوَّةٍ لها، ويكشف عن مواطن ضعفها في الوقت ذاته. وعلى سبيل المثال، فإنَّ البنى الَّتحتيَّة الحيويَّة لعمل الدَّولة (كالكهرباء والمياه والمواصلات وشبكات القيادة والسَّيطرة والتحكُّم العسكريَّة، وكذلك التِّقنيات المتطوِّرة لساحة القتال العصريَّة) كلُّها باتت تعتمد على المجال الافتراضيِّ. ففي عالم الإنترنت اليوم، تُسقط أنظمة، وتُخترَق مؤسَّسات، ويُخلَع رؤساء! كيف لا وهي حربٌ خارجةٌ عن سيطرة الدُّول وأجهزتها الأمنيَّة، لا تعترف باتِّفاقيَّاتٍ ولا معاهداتٍ ولا مواثيق، وأبطالها الافتراضيُّون – بالإضافة للدول – هم أفرادٌ وجماعاتٌ أقرب إلى "الخلايا النَّائمة" التي تصحو وقتما تشاء، وتعود لسباتها متى أرادت ذلك!