خالد وليد محمود*

الهجمات عبر الإنترنت
ساحة الصراع الإلكتروني الجديدة

ترصد هذه الورقة بالتحليل ظاهرة الهجمات الإلكترونية عبر الإنترنت وتلقي مزيدًا من الضوء على المجال الافتراضيّ بوصفه ساحة قتالٍ جديدةٍ باتت تشكِّل تهديدًا يضاف إلى قائمة التَّهديدات التَّقليديَّة التي تواجه العالمَ، وتتجاوز في أبعادها وآثارها الحدود الجغرافيَّة والسِّياسيَّة، وتلقي بتداعياتها على مستقبل الأمن القوميِّ والحيويِّ للدُّول. وتحاول الدراسة إبراز المسائل والتداعيات المتعلقة بعمليَّات الاختراق التي يقوم بها قراصنة الإنترنت "الهاكرز" ومجموعة "المجهولين" أو "الأنونيموس"، مع ملامسة المساحة التي تمتد إليها تأثيرات المجال الافتراضي، والتي تغلبت على المسافات، وباتت تعد دليلًا يمكن الاسترشاد به للتعامل الصحيح مع ما تطرحه هذه الظاهرة على أرض الواقع من تهديدات جديدة.

* باحث في المركز العربي للأبحاث ودراسة السياسات.

شهدت ساحة الحرب في "المجال الافتراضي" Cyberspace خلال السنوات الأخيرة، عدّة تطوّرات وتجاذبات ميدانية ونظرية، كان أبرزها ما دار مؤخّرًا من هجمات إلكترونية عبر الإنترنت أسهمت بها دول ومنظّمات وأفراد، وألحقت أضرارًا مادية ومعنوية. وتقف عمليات القرصنة الإلكترونية على رأس تلك الهجمات التي بدأت تثير قلق الدول والحكومات، بل حتى الأفراد، بسبب تعدّد الجهات التي تستطيع الانخراط فيها، وصعوبة تتبّع مصادرها أو تحديد مكان انطلاقها وكلفة تداعياتها. وعلى هذا الأساس، أصبحت الشبكة العنكبوتية ساحة نزاعات وصراعات يدخل في سياقها التجسس والاختراق والتحكّم في قواعد بيانات قد تمسّ الأمن القومي والحيوي لبعض الدول. وفي ضوء سيرورات التطوّر في مجال الفضاء الإلكتروني، شرعت معظم الحكومات بوضع هذا المجال في مكانٍ متقدّم من قائمة أهدافها وأولوياتها الاستخبارية ونشاطاتها الوقائية.

لقد أصبحت الهجمات الإلكترونية أحد أسهل السبل للتأثير في "العدو" والرد عليه، ومن دون تكاليف كبيرة؛ إذ بإمكانها إلحاق أضرار بمصالح الأفراد والمؤسسات والدول عبر اختراق المواقع الإلكترونية الحيوية وتعطيلها. وثمّة تطوّرات ألقت الضوء على هذا المجال الجديد نسبيًّا، ولا سيّما بعد الهجمات الإلكترونية التي شنّتها مجموعة "الأنونيموس" أو "المجهولين" Anonymous[١]، وبخاصة في منطقة الشرق الأوسط، وتحديدًا في إسرائيل، خلال السنوات القليلة الماضية. لقد بدا أنّ هذه الهجمات سبّبت "صراعًا" بين عدة لاعبين، اتّخذ شكل ما يُعتقد أنّه "هجمات متبادلة" تعرّضت لها منشآت ومنظومات في مجالاتٍ عديدة، وخلّفت أضرارًا مادية ومعنوية، تتضارب التقديرات بشأن حجمها وتأثيرها في نشاطات مؤسّسات وبرامج مالية وتكنولوجية؛ مدنيّة وعسكريّة.

١ تعد مجموعة "الأنونيموس" من أكثر المجموعات المؤثّرة في تاريخ القراصنة الحديث؛ إذ تستمر فعّاليّات المجموعة إلى يومنا هذا في نشاطاتها. ولا توجد أيُّ معلومات حول عددهم أو مجموعاتهم الفرعيّة. لهم عملياتٌ شهيرة، من بينها دعمهم لموقع "ويكليكس". وقد سبّبت هذه المجموعات العديد من المشكلات السياسيّة عبر العالم، إضافة إلى هجومها على مواقع شركاتٍ عالميّة عدّة، وتدخّلها في الانتخابات الإيرانيّة عام ٢٠٠٩، مع القيام بمهاجمة مواقع حكوميّةٍ أستراليّة من أجل المطالبة بالسماح للمستخدم بالتّصفُّح من دون حجبٍ لأيّ موقع. كما هاجمت هذه المجموعات مواقع حكوميّةٍ للعديد من الدُّول، وسربت معلومات شخصيّةٍ لشخصيّاتٍ معروفةٍ في البحرين والمغرب ومصر والأردن. كما كان الرّبيع العربيُّ ميدان عملٍ مكثّفٍ لأعضائها؛ إذ قدّموا دعمًا فوريًّا للثّورات الشّعبيّة في تونس ومصر عبر شنّ هجماتٍ قويّةٍ ضدّ المواقع الحكوميّة للبلدين. وقد أثنى عليهم بعض المحلّلين كمقاتلين رقميّين، وأدانهم آخرون كونهم مقاتلون حاسوبيُّون فوضويُّون. انظر: أحمد أبو طالب، "أنونيمس: القرصنة السّياسيّة عبر الفضاء الإلكترونيّ"، **الأهرام الرقمي**، ٢٠١٢/١/١:
http://digital.ahram.org.eg/Policy.aspx?Serial=780539

المجال الافتراضي: المفهوم والدلالة

بإمكاننا – ماديًّا - تحديد ما يُعرف بـ "السايبر" أو ما يُطلق عليه أيضًا "الحيّز أو الفضاء الافتراضي"، بأنه المجال الرقمي الإلكتروني Digital Medium الممتدّ عبر مختلف خطوط الاتصالات المعدنية والضوئية والهوائية وقنواتها في شبكة "الإنترنت". ووفق التعبير التكنولوجي فإنه "طريق المعلومات الفائق السرعة". واقترن هذا الفضاء بمفاهيمه المختلفة، حيث انعدام جغرافيا المكان الطبيعي، وظهور جغرافيا الإبحار المعلوماتي في شتّى الاتجاهات وفي الآن نفسه. وهذا ما جعل هذه الظاهرة تعد إحدى أهمّ خصائص عصر المعلومات؛ فهي تجسّد عمليًّا مجتمع القرية الكونية، من خلال فضائها الافتراضي المنفتح الآفاق، والذي يضع الإنسان في عالمٍ رقمي مختلف من حيث أسسه وخصائصه وقيمه الجديدة[٢]؛ "فالحديث هو بروز العالم الافتراضي كمساحة مكانيّة وزمانيّة أضحت كما الأرض الجديدة، حيث هرعت إليها رؤوس الأموال والحركة الثقافيّة والعلميّة المعاصرة، ومظاهر التسلية وكذلك الجريمة"[٣].

ثمّة تعريفات عديدة للمجال الافتراضي أو حيّز "السايبر"؛ فالاتّحاد الدَّوليُّ للاتّصالات International Telecommunication Union - وهو وكالة الأمم المتَّحدة المتخصِّصة في مجال تكنولوجيا المعلومات والاتّصالات - يعرِّف الحيّز الافتراضي على النحو التالي: الحيّز المادي وغير المادي الذي ينشأ أو يتكوّن من جزءٍ أو من كلّ العناصر التالية: حواسيب، وأجهزة ممكننة، وشبكات، ومعلومات محوسبة، وبرامج ومضامين، ومعطيات مرور ورقابة، والذين يستخدمون كلّ ذلك[٤]. و"خلافًا للتعريفات التي تنظر إلى الحيّز الافتراضي كبعدٍ أو مجال خامس، هناك توجّه يرى فيه واحدًا من سبعة مجالات، إلى جانب الجوّ والفضاء والبحر والبرّ والحيّزين الإلكترو-مغناطيسي والإنساني"[٥]. وهناك من يعرّف المجال الافتراضي بأنّه "ساحة الحرب الخامسة"، بعد البرّ والبحر والجوّ والفضاء الخارجي. وفي التعريف ذاته، يكون المجال

٢ علي محمد رحومة، **الإنترنت والمنظومة التكنو-اجتماعيّة، بحثٌ تحليليٌّ في الآليّة التقنيّة للإنترنت ونمذجة منظومتها الاجتماعيّة** (بيروت: مركز دراسات الوحدة العربيّة، ٢٠٠٥)، ص ٣٣.

٣ عمر بن يونس، **المجتمع المعلوماتي** (بيروت: الدار العربية للموسوعات، ٢٠١٠)، ص ١٣.

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

٥ شموئيل إيفن ودافيد سيمنطوف، "الحرب في الحيّز الافتراضي"، **قضايا إسرائيلية**، العدد ٤٣- ٤٤ (شتاء ٢٠١٢).

الافتراضي أوسع من الإنترنت؛ إذ يتوسّع ليشمل الشبكات الحاسوبية الأخرى التي ترتبط إلكترونيًّا بالإنترنت، بما فيها أنظمة التحكّم وجمع البيانات SCADA، والتي تتيح التواصل بين منظومات الحوسبة، والتي تتحكّم في الأجهزة ذات الصلة بمفاصل الاقتصاد[٦]. إذًا، "فالفضاء الافتراضي بات يعتبر كمجال خامس للحروب بين الدول، حيث عرف العالم عبر التاريخ الحروب البرية والحروب البحرية، وحديثًا الحروب الجوّية، ومؤخّرًا عرفنا حرب الفضاء، والآن ظهرت حرب الإنترنت"[٧].

> القاسم المشترك الواضح بين سائر التعريفات هو الشريحة العقلية، أمّا الاختلاف والتباين في ما بينها، فيعكسان - على ما يبدو - الاهتمام الذي توليه كلّ دولة أو منظّمة في سياق مواجهتها التحدّيات في الحيّز الافتراضي

إنّ القاسم المشترك الواضح بين سائر التعريفات هو الشريحة العقلية، أمّا الاختلاف والتباين في ما بينها، فيعكسان - على ما يبدو - الاهتمام الذي توليه كلّ دولة أو منظّمة في سياق مواجهتها التحدّيات في الحيّز الافتراضي، ولكن يبدو أنّ الفوارق في التعريفات لا تعكس فهمًا مختلفًا للمجال الافتراضي، لأنّ جميع أصحاب هذه التعريفات يقرّون - كما أسلفنا - بوجود الشرائح الثلاث التي يتضمّنها تعريف الأمم المتحدة[٨].

لقد عرف عالمنا المعاصر أوّل عاصفة إلكترونية جامحة من خلال ما أحدثته تسريبات "ويكليكس" التي عُرفت باسم "عاصفة ويكليكس"، وتضمّنت استخدام موقعها الإلكتروني في نشر صور ضوئية لآلاف الوثائق السرّية الرسمية المتبادلة بين وزارة الخارجية الأميركية وبعثاتها في دول العالم، وما أحدثته تلك التسريبات من توتّر حادّ في العلاقات الدولية على جميع الصعد، وتسبّبت في توتّر العلاقات بين كثير من القادة والرؤساء والملوك في العالم؛ لما نسبته إليهم من أقوالٍ وتصريحات تتعارض مع سياساتهم المعلنة تجاه شعوبهم، وهو ما أدّى إلى حدوث اضطرابات واحتجاجات عديدة في هذه الدول.

"الهاكرز" واختراق الحيّز الافتراضي

جاءت عمليات القرصنة الإلكترونية كأحد تجلّيات فصول الثورة المعلوماتية. وظهر ما بات يُعرف بالحرب الإلكترونية القائمة أساسًا على أجهزة الحاسوب والشبكة العنكبوتية، ونواتها "الهاكرز"[٩] كشخصية محوريّة برزت على سطح البيئة الرقمية، وهم الذين يعملون عبر الاختراق البرمجي لأجهزة الحاسوب. بيد أنّ تزايد حجم المعلومات المنتشرة على الشبكة العنكبوتية، وتصاعد قيمتها بوصفها مصدرًا معرفيًّا واقتصاديًّا وسياسيًّا وأمنيًّا - بحسب طبيعة الموقع الذي يحتويها - قد ألقت بظلالها على هذا الميدان؛ فأحدثت تغييرًا جوهريًّا في أهداف عملية الهجوم الإلكتروني أو القرصنة المعلوماتية التي كانت في بدايتها نزعة فضولية للوصول إلى معرفة جديدة، أو تحدّي العقبات الأمنيّة التي تضعها الجهات الأخرى لغرض الإحساس بنشوة النصر. وقد توجّهت أهداف هذه العمليات صوب استثمار هذه القدرات وترجمتها إلى مكاسب مادية أو سياسية موجّهة. وأصبحت إمكانية إحداث تدمير جزئي أو كلّي في المواقع الرقمية التي تستهدفها الهجمات الإلكترونية جزءًا مكمّلًا للسلوك الذي يمارسه "الهاكرز" من خلال اختراق النظم.

يجري اختراق الحيّز الافتراضي أو الفضاء المعلوماتي للدول عن طريق مجموعات قراصنة الحاسوب (ويقوم بهذه العملية شخص أو مجموعة أشخاص وربّما بضع مئات أو بضعة آلاف من المستخدمين الذين لديهم القدرة على التحكّم في برامج الحاسوب وطرق إدارتها، وهم مبرمجون ذوو مستوى عالٍ يستطيعون اختراق أجهزة حاسوب والتعرّف إلى محتوياته). ومعظم هؤلاء يرفضون التصريح بهويّتهم الحقيقية خشية ملاحقة أجهزة الدولة، ويختارون لأنفسهم صفة "مجهول".

يحاول "الهاكرز" جذب انتباه الخصم ومناصريه عن طريق إحداث خللٍ أو تمزيق في آليات سريان العمليات التقليدية، مع كفّ عمليات الدخول إلى الخدمات والمعدّات الرقمية بمختلف أشكالها. ومن خلال توظيف هذه الآلية المعلوماتية تستطيع مجموعات من الناشطين - من ذوي المهارة العالية في استخدام برمجة الحاسوب قد تتألّف من مجموعة صغيرة أو كبيرة من المستخدمين - تحقيق عملية "غزو" معلوماتي لموقعٍ إلكتروني محدّد على شبكة الإنترنت، وخلال بعد زمني

6 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

٧ عماد غنيم، "الحروب الافتراضية القاتلة"، **الأهرام الرقمي**، ٢٠١٠/١٠/٢٥، انظر: http://digital.ahram.org.eg/articles.aspx?Serial=340346&eid=601

٨ إيفن وسيمنطوف.

٩ يمكن تصنيف قراصنة المعلومات إلى قسمين: "الهاكرز" Hackers أو المبتدئين أو الهواة الذين يكون الهدف من وراء اختراقهم الأنظمة الإلكترونية التعلم والتسلية على الأغلب. وهناك من يسمّون "الكراكرز" Crackers؛ وهم المخترقون المحترفون الذين يكون دخولهم إلى الحواسيب من أجل غاية معيّنة تحقّق لهم ما يهدفون إليه.

محدّد بحيث تورث هذا الموقع آفة الفيضان المعلوماتي فتحول دون الوصول إلى هذا الموقع أو الدخول إليه، سواء كان هؤلاء المستخدمون أصحاب المواقع أو زوّارًا[١٠].

هناك خمسة محاور رئيسة يمكن أن يلجأ إليها "الهاكرز" للدخول إلى شبكة الحواسيب وإحداث أضرار، وهي:

- الحصار الافتراضي Virtual Sit-Ins and Blocked : يهدف إلى إحداث خلل أو تمزيق في آليّات سريان العمليات التقليدية، مع كفّ عمليات الدخول إلى الخدمات والمعدّات الرقمية بمختلف أشكالها. وخلال فترة زمنية معيّنة، ينجم عن هذا الحصار خلل في الموقع، ولا يستطيع المستخدمون الدخول إليه[١١].
- قنبلة البريد الإلكتروني Email Bomb: تتمثّل هذه العملية في إرسال كمٍّ كبير (آلاف الرسائل الإلكترونية) إلى صندوق البريد الإلكتروني للخصم؛ بحيث ينشأ عن هذا النوع من الهجمات تعطّل قدرة البريد عن تلقّي الرسائل والتعامل معها[١٢].
- قرصنة مواقع الويب واختراق الحواسيب Web Hacks and Computer Break-Ins: يقوم "الهاكرز" بهذه العملية من خلال الدخول غير المشروع إلى أحد مواقع الويب الموجودة على الشبكات المعلوماتية، واستبدال معلومات جديدة بأخرى موجودة عليه، تغيِّر من هويّته[١٣].
- الفيروسات، يعمد "الهاكرز" هنا إلى نشر الفيروسات وديدان الإنترنت في شبكات المعلومات الوطنية وشبكة الإنترنت؛ بقصد إحداث خللٍ موقّت أو دائم في الملفات ونظم التشغيل المستهدفة.
- هجمات الحرمان من الخدمة Denial of Service, DoS: وهي هجمات تجري عن طريق إغراق المواقع بسيلٍ من البيانات غير اللازمة تُرسل من خلال برامجَ متخصّصة تعمل على نشر هذه الهجمات؛ ما يسبّب بطء الخدمات أو ازدحامًا مروريًّا على هذه المواقع، ويسبّب صعوبة وصول المستخدمين إليها نظرًا لهذا الاكتظاظ. وقد تعرّضت الكثير من المواقع المهمّة والحسّاسة لمثل هذه الهجمات؛ ومن أبرزها: Word press وAmazon وغيرها، على الرغم من وجود بعض المنتجات والبرمجيات التي تدّعي قدرتها على إيقاف مثل هذه الهجمات[١٤].

تجدر الإشارة إلى أنّ العالم، وخلال العقدين الأخيرين على أقلّ تقدير، بدأ يشهد في ظلّ الثورة التكنولوجيّة والرقميّة عمليات اختراق منظومات معقّدة ليس لأهـدافٍ عسكريّة[١٥] فحسب، ولكن أيضًا لأغراضٍ اقتصاديّة[١٦] أو إعلاميّة أو سياسيّة أو حتّى إجراميّة. ويتوقع الخبراء "نموًّا متواصلًا في عدد الهجمات المُوجَّهة خلال عام ٢٠١٣، وتواصل ظاهرة "القرصنة المُسيَّسة"، وظهور هجمات إلكترونية واستخدام أدوات مراقبة "شرعية" في الفضاء الإلكتروني برعاية حكومية، وهجمات على البنى التحتية المعتمدة على الحوسبة، وتدهور الخصوصية الرقمية، واستمرار المشاكل مع السلطات الرقمية والائتمانية في الإنترنت، والنموّ المتواصل لأعداد البرمجيات الخبيثة التي تهدّد نظام التشغيل والأجهزة المحمولة، والثغرات والبرامج المستغلّة"[١٧].

وفي أعقاب نشاطات "الهاكرز" المتزايدة والتسابق المحموم للحكومات في هذا المجال الذي غيّر شكل الحرب الحديثة، أدركت الدول مدى فداحة ما يواجهها من تهديدات. إنّ الأمر لا يتعلّق بالأمور العسكرية فحسب، ولكنه يتجاوز ذلك إلى أمورٍ مدنية أيضًا[١٨] "لإلحاق الضرر وإصابة دول كاملة بالشلل عن طريق لوحة المفاتيح (الكيبورد) على اعتبار أنّ من لا يسارع باستيعاب ذلك لن يصمد في أيّ مواجهة"[١٩].

---

١٠ حسن مظفر الزرو، **الفضاء المعلوماتي** (بيروت: مركز دراسات الوحدة العربية، ٢٠٠٧)، ص ٢١٦.

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

١٢ الزرو، ص ٢١٧.

13 Slobbe.

14 http://compnetworking.about.com/od/networksecurityprivacy/g/denialof service.htm

١٥ 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 العالميّ 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.

١٦ 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.

١٧ "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

١٨ يتّسم الحيّز الافتراضي أيضًا بكونه حيّزًا يدمج المجالين المدني والعسكري؛ ففي الكثير من الحالات تكون الاتصالات العسكرية مرتبطة بشبكات مدنيّة. من هنا تغدو حماية البنى والشبكات المدنية حيوية للأغراض العسكرية أيضًا. في الوقت ذاته، تمتلك الجيوش قدرات افتراضية يمكن أن تساعد في حماية الشبكات المدنيّة.

١٩ عادل شهبون، "حروب السايبر ساحة المعارك الجديدة بين الدول"، **الأهرام الرَّقمي**، ٢٠١١/٦/٤، انظر:
http://digital.ahram.org.eg/articles.aspx?Serial=528342&eid=1103

"الأنونيموس": جيشٌ ثكنته العالم الافتراضي

ثمة الكثير من العوامل التي تجعل من مجموعة "الأنونيموس" سلاحًا ملائمًا يمتلك ميزات فريدة، منها: قابلية الاختراق لنظم المعلومات، وغياب الحدود المكانيّة عن الفضاء المعلوماتي، وعدم وضوح الهويّة الرقمية للمستخدم المستوطن في بيئته المفتوحة، وتوسيع رقعة الاهتمام بتجاوز حدود السلطة أو المجتمع الذي تقيم فيه المجموعة ما يزيد قدرتها التأثيرية بصورة ملموسة. وهذه المجموعة لا تتكوّن حصريًّا "من محترفي القرصنة ولكنها تضمّ في صفوفها مجموعات لديها مهارات الكتابة، وأخرى قادرة على صناعة مقاطع الفيديو، وأخرى ناشطة في الشارع، وأخرى قد لا يكون لديها أيّ من هذه المهارات، ولكنها تساعد في نشر المعلومات والرسائل واستنساخها، خاصّةً على شبكات التواصل الاجتماعي"[٢٠]. ومن المميزات أيضًا تدنّي الكلفة المادية؛ إذ إنّ توافر الأدوات المعلوماتية على شبكة الإنترنت، وقيام هذه المجموعة بفكّ الشفرات البرمجية يوفّران عددًا ضخمًا من النظم البرمجية والوسائل التي تمكّن هؤلاء من استغلالها في توجيه ضرباتهم لخصومهم بسهولة، ومن دون الحاجة إلى مصادر تمويل ضخمة. وتبدو أهمّ سمة تتّسم بها مجموعة "الأنونيموس" أنّها ليست لديها عقيدة جامعة سوى الإصرار على النضال والحرية المطلقة في الإنترنت[٢١].

تجدر الإشارة إلى أنّ المنتسبين إلى مجموعة "الأنونيموس" لا يعيشون في عالمهم الخاصّ وفي غرفٍ مغلقة ومعتمة كما تصوّرهم هوليود، وإنما هم شبّان يعون ما يحدث في العالم ويقدّسون ثقافة الإنترنت كونها تجسّد حرية التعبير. هذه المجموعة أفرادها مجهولو الهويّة، ولا يتبعون هرميّة معيّنة، وهم مطلوبون إلى العدالة؛ لاختراقهم وكالة الاستخبارات المركزية الأميركية ونشرهم وثائقها، ودعمهم المباشر لـ "ويكليكس" عبر قرصنة موقعَي "ماستر كارد" و"أمازون"؛ ردًّا على رفض هاتين المؤسستين فسح المجال أمام المواطنين لاستعمال موقعيهما في إرسال مساعدات مادية لـ "ويكليكس".

وثمّة أكثر من سبب لدى قراصنة الإنترنت الذين ينتمون إلى "الأنونيموس" يجعلهم يميلون إلى ممارسة شتّى أنواع الاختراق على النظام الحاسوبي، مثل: تراكم الأحقاد والضغائن، ورغبة في تدمير ما لدى الآخرين، وإحداث نوع من التخريب، والقيام بهجمات وهمية بهدف فحص الأمن لدى النظام المخترَق وتكون هذه الهجمات بالتوافق، وإثبات الذات بين مستخدمٍ وآخر، والتسلية وحبّ الاستطلاع. كما قد تكون هناك إغراءات ماديةٍ توفرها حكومات وجِهات لـ "الهاكرز"؛ للحصول على بيانات مهمّة من نظام معلوماتي. وقد يكون هذا الدافع ناتجًا من الفقر أو الطمع أو الرغبة في إطاحة منافس نتيجة لتضارب المصالح، وكذلك من الفضول والرغبة في اكتشاف المجهول وساحة الممنوع، أو من وجود أغراض ودوافع سياسية تجمع بين أفراد أو جماعات لها عقائد وأفكار سياسية معينة، وتحاول استخدام أدوات الاختراق الحاسوبي لخدمة معتقداتها وتوجّهاتها السياسية، فتلجأ مثلًا إلى تدمير مواقع إلكترونية وشبكات وقواعد بيانات لدول أو جماعات أو شركات تراها معادية لها. وهذا ما نشير إليه هنا بوصفه فكرًا جديدًا يقوم على استخدام مجموعات من "الهاكرز" في الإنترنت لمهاجمة المواقع الإلكترونية على الشبكة؛ دعمًا لقضايا الشعوب وفضح الحكومات الفاسدة.

ومثال ذلك أنّه عندما تحرّكت شعوب عربية ضدّ الحكام الدكتاتوريين الذين سيطروا عليها لعقود من الزمن، في ما أصبح يُعرف بـ "الربيع العربي"، كانت الإنترنت الحليف التكنولوجي الذي مكّن الناس من تبادل المعلومات وتنظيم التظاهرات وترويج الحركة بأسرها. وحينئذ، فُتح نقاش واسع بشأن قيم القرصنة الإلكترونية؛ فبعدما اعتاد الخطاب العربي السائد تصوير "الهاكرز" على أنّهم شباب مهووسون تقنيًّا، ويقضون وقتهم في محاولة خرق أمن الدول والمؤسسات الكبرى من باب التسلية فحسب؛ جاءت الانتفاضات الشعبية العربية التي اندلعت في المنطقة العربية لتبيّن أنّ كثيرًا من عباقرة الحاسوب هؤلاء يستعملون خبرتهم لمساعدة الثوّار وفضح الحكومات، مثل مساعدتهم المواطنين المصريّين في إيجاد حلّ مكّنهم من استعمال مواقع التواصل الاجتماعي، عندما أمرت حكومة الرئيس السابق حسني مبارك بتعطيل خدمات الإنترنت، كما ساعدت المحتجّين الليبيين واليمنيين. وقام أعضاء من "الأنونيموس" بقرصنة المواقع الرسمية التابعة لنظام الرئيس التونسي السابق بن علي ردًّا على حجب الإنترنت عن الشعب التونسي في بداية الثورة، ثمّ تركوا رسالة في هذه المواقع المقرصنة جاء فيها: "نحن مجهولون ... إلى الحكومة التونسية: لن يتمّ التسامح مع الهجوم على حرية التعبير وحرية وصول مواطنيكم إلى المعلومات، وأيّ منظّمة متورّطة في الرقابة سيجري استهدافها". يرى هؤلاء أنّ الحكومات تستعمل الإنترنت لمراقبة المواطنين؛ ولذا يحقّ للمواطنين، وعبر الإنترنت أيضًا، كشف أسرار هذه الحكومات وعملياتها[٢٢]. وقد سبق أن قامت مجموعة "الأنونيموس"

٢٠ أبو طالب.

21 Slobbe.

٢٢ تانيا الخوري، "كلنا شهود عيان: ربيع العرب بالصور والحروب الإلكترونية"، مجلة **الدراسات الفلسطينية**، العدد ٨٨ (خريف ٢٠١١)، ص ١٢٨، انظر:
http://www.palestine-studies.org/files/pdf/mdf/11116.pdf

بعدّة هجمات ضدّ مواقع وصفحات الهيئات الحكومية والوزارات المصرية في أثناء ثورة يناير، ردًّا على قمع قوّات الأمن للمتظاهرين،٢٥ وانتقامًا لقطع الإنترنت والاتصالات عن المصريّين، وهو ما أُطلق عليه اسم "العملية مصر"، والتي تعاونت فيها مع مجموعة "تيليكوميكس"[٢٣] لتوفير طرق غير تقليدية تمكّن المصريين من الاتصال بالإنترنت بعد قطع الخدمة عنهم[٢٤].

تجدر الإشارة إلى أنّه "منذ احتماء الاحتجاجات في تونس، بدأت تنتشر فيديوهات على الإنترنت تحمل توقيع "أنونيموس" تحت اسم "العملية تونس"، وهي عملية انتقامية من السلطات التونسية لما مارسته من عنف ضدّ المتظاهرين وحملات اعتقال للمدوّنين؛ إذ جرى تعطيل مواقعها الحسّاسة، ولا سيّما مواقع وزارات الدفاع والداخلية والخارجية"[٢٥]. وقد تكرّرت هذه الأفعال بالنمط نفسه في دول أخرى؛ إذ يجري غالبًا البدء بتوجيه رسالة دعم للشعوب، ثمّ تهديد ووعيد للحكومات، مثل حالات مصر وليبيا وتركيا وإسبانيا واليونان وإيطاليا والبرتغال ودول شرق أوروبا وزيمبابوي والصين وروسيا وإيران وسورية وغيرها، كدعم للحركات الاحتجاجية التي حدثت هناك، أو مؤازرة لحركات المطالبة بالديمقراطية ومناهضة الفساد[٢٦]. وهو ما حدث كذلك في الولايات المتحدة لدعم حركة "احتلّوا" Occupy، ولكن بطريقة مختلفة[٢٧]؛ إذ قامت المدوّنات والصفحات الإخبارية التابعة لمجموعة "أنونيموس" على الفيسبوك والمتعاطفة معها بمتابعة ميدانية أكثر منها حشدًا أو فعلًا إلكترونيًّا. وبهذا، "تكون هذه الجماعة قد أسهمت بصورة أو بأخرى في إلقاء الضوء على تلك الاحتجاجات عن طريق شبكات الإعلام البديل، في ظلّ تعتيم الإعلام التقليدي الذي تعمّد غضّ البصر عنها على الأقلّ في بدايتها"[٢٨].

بات من الصعب اليوم إلى حدٍّ ما التعرّف إلى عدد أعضاء هذه المجموعة التي باتت رمزًا للمهاجمين الإلكترونيين؛ وهم أشبه بجيش ثكنته العالم الافتراضي الذي يلتقون فيه ويتبادلون الحديث في غرف دردشة سرّية ويعملون في شتّى أنحاء العالم ولهم أولوياتهم الخاصّة، ولا يترأسهم أحد، وشعارهم أنّهم "مجهولون، لا يسامحون ولا ينسون"؛ وهي العبارة التي يختمون بها كلّ بياناتهم المكتوبة أو المصوّرة، في إشارة إلى من ينتهك حرية التعبير ويحدّ من الاستعمال الحرّ للإنترنت. أمّا هدفهم، فهو فضح الحكومات الفاسدة؛ أي جميع الحكومات كما يصرحون. وهذا ما يجعلنا نقف اليوم عند ظاهرة عابرة للقارّات وشكل من أشكال الحركات الاحتجاجية المعاصرة في القرن الحادي والعشرين تأخذ من الفضاء الإلكتروني ساحة لنشاطاتها وردود أفعالها.

> إنّ التحدّي القائم في مجال عمليات اختراق منظومات إلكترونية لا يقتصر على دولة بعينها وحسب، وإنّما يشمل دولًا كثيرة من بينها إسرائيل التي وجدت نفسها في الشهور القليلة الماضية أمام ضربات إلكترونية شنّتها مجموعة "الأنونيموس"، كبّدتها خسائرَ معنوية ومادية.

إسرائيل في قلب الصراع الإلكتروني

إنّ التحدّي القائم في مجال عمليات اختراق منظومات إلكترونية لا يقتصر على دولة بعينها وحسب، وإنّما يشمل دولًا كثيرة من بينها إسرائيل التي وجدت نفسها في الشهور القليلة الماضية أمام ضربات إلكترونية شنّتها مجموعة "الأنونيموس"، كبّدتها خسائرَ معنوية ومادية، ما دعاها إلى حشد جيش من الخبراء والتقنيّين لمواجهتها. وتكمن حساسية إسرائيل ومخاوفها من خطر مجموعات القرصنة الإلكترونية، في إدراكها الطاقة الكامنة لمثل هذه الهجمات على حيّزها الافتراضي، وعلى اعتبار أنّها تمارس على نطاقٍ واسع هذا النوع من الحرب في محاولتها تحقيق أهداف تكتيكية وإستراتيجية؛ وهذا ما أفضى إلى ظهور قراءات مختلفة لوسائل الصراع العربي الإسرائيلي في المنطقة، انطلاقًا من إمكانية استعمال التكنولوجيا والفضاء الإلكتروني بصورةٍ فعّالة، في حروب بات فيها العقل سيّد الموقف[٢٩].

يوم السابع من نيسان / أبريل ٢٠١٣، شنّت مجموعات قرصنة إلكترونية ثاني أكبر هجماتها ضدّ المواقع الرسمية والتجارية والاجتماعية في إسرائيل. وقد وجّهت تلك المجموعات بالتعاون والتنسيق مع مجموعة "أنونيموس" - أحد حلفاء "ويكليكس" التي صنّفتها مجلّة

٢٣ التيليكوميكس Telecomix، مجموعة من القراصنة الإلكترونيين المهتمين بكشف من يحجب الإنترنت ويراقبه.
٢٤ أبو طالب.
٢٥ المرجع نفسه.
٢٦ المرجع نفسه.
٢٧ المرجع نفسه
٢٨ المرجع نفسه.
٢٩ علي بدوان، "إسرائيل وحرب السّايبر"، جريدة **البيان** الإماراتية، ٢٠١٢/٧/١٧، انظر: http://www.albayan.ae/opinions/articles/2012-07-17-1.1689715

تايم الأميركية واحدة من أكثر المجموعات تأثيرًا في العالم[٣٠]- رسالةً إلى العالم من خلال مقطع فيديو نُشر على موقع يوتيوب جاء فيها أنّ "أقوى المخترقين من مختلف أنحاء العالم قد قرّروا أن يتوحّدوا في كيانٍ واحد تضامُنًا مع الشعب الفلسطيني ومحو إسرائيل من على الإنترنت"[٣١]. وفي ذلك المقطع، ظهر شخص يلبس قناع المجموعة ويتحدّث عن خطوات الهجوم التي حدّدها بمسح إسرائيل من شبكة الإنترنت، وفضح الخطط المستقبلية والجرائم. ولم يجْر الإفصاح عن الخطوة الثالثة، وقال "أمّا الخطوة الثالثة والأخيرة، فسنقدّمها لكم هديّة نحن الأنونيموس"[٣٢].

شُنّت الهجمات الإلكترونية باسم "OpIsrael #" من خلال أسلوب "الهجمات الموزّعة" واستطاعت من خلاله توجيه ضربة رقميّة إلى إسرائيل. ويعدّ هذا الأسلوب من التقنيات المتقدّمة التي باتت تستخدمها مجموعة "الأنونيموس" وتثير قلق المهتمّين بالشبكات الرقميّة. نفّذ الهجوم على المواقع الإسرائيلية مجموعة قراصنة الإنترنت من عدّة دول منها: فلسطين ولبنان والجزائر وإيران وجنوب أفريقيا وفرنسا وأميركا وألبانيا وكوسوفا والمغرب وتركيا وإندونيسيا وتونس ومصر والسعودية والأردن. ونجح الهجوم في التشويش على العشرات من المواقع الإلكترونية الإسرائيلية وتعطيلها، والتي أضحت غير متاحة على شبكة الإنترنت. كما تزامن موعد الهجوم في ٧ نيسان / أبريل مع يوم ذكرى الهولوكوست "ذكرى المحرقة"؛ التي قالت المجموعة المهاجمة في رسالتها للإسرائيليّين: إنها فكرةٌ "ابتدعتموها وأولياؤكم وجعلتم العالم يؤمن بالمحرقة اليهودية". واستهدف الهجوم مواقع إلكترونية مهمّة، ونجح في اختراق مواقع[٣٣] الحكومة والجيش والصناعات العسكرية، ومنها موقع رئيس الوزراء ووزارة الدفاع وموقع الاستخبارات وموقع مجلس الوزراء وسوق الأوراق الماليّة والمحاكم الإسرائيلية وشرطة تل أبيب وحزب كاديما ووزارة التعليم وبنك القدس، ونحو عشرين ألف حساب على الفيسبوك، وخمسة آلاف حساب بنكي، وغيرها. وتمكّن "الهاكرز" أيضًا من عرض قضيّة الأسرى الفلسطينيين من خلال وضع صورٍ لبعضهم؛ مثل صورة الأسير الفلسطيني الذي كان مضربًا عن الطعام سامر العيساوي، والتي احتلّت شاشات الحاسوب المخترقة[٣٤].

بعد الهجوم الإلكتروني، سادت حالة من الجدل السياسي والاقتصادي والعسكري والإعلامي لدى جمهورٍ واسع من المجتمع الإسرائيلي عبّرت عنه وسائل الإعلام المختلفة بخصوص الجاهزية الأمنيّة والتحصين الإلكتروني لمثل هذا الهجوم والخسائر المادية المتوقّعة.

لقد سرّبت مجموعة "أنونيموس" في ٢٨ حزيران/ يونيو ٢٠١١ وفي عدّة مواقع، رسالة تتضمّن هجومًا إلكترونيًّا على الموقع الرسمي للكنيست الإسرائيلي، وعطّلت أعماله لساعات؛ ردًا على قمع الفلسطينيّين واحتلال أراضيهم. ولأنّ الحكومة الإسرائيليّة كانت قد شنّت حربًا إلكترونيّة على إيران ولبنان (بعثت بفيروس "ستاكس نت" Stuxnet للهجوم على المنشآت النووية الإيرانيّة، وقامت بقرصنة شركات الاتّصالات اللبنانيّة عبر عملاء لها)[٣٥]، فإنّ هذا الأمر في نظر مجموعة "الأنونيموس" يحلّ الهجوم عليها. وقد بعثت المجموعة رسالة مصوّرة استعملت فيها برنامجًا آليًّا يقرأ إنسان آليّ من خلاله العبارات التالية: "إلى الشعب الفلسطيني النبيل: خلال الأعوام الخمسة والستّين الماضية فُرض عليكم العيش في أوضاع لا إنسانية من طرف نظام صهيوني عنصري غير قانوني ... أنونيموس هي إخوانكم وأخواتكم، أبناؤكم وبناتكم، أهاليكم وأصدقاؤكم، بغضّ النظر عن السنّ والجنس والعرق والدين والإثنية، أو مكان الولادة. أنونيموس هي أنتم متّحدون أقوياء ... انضمّوا إلينا في معركة حرية المعلومات حول العالم ... نحن لا نسامح، ولا ننسى"[٣٦].

وفي عام ٢٠١١، قامت مجموعة من مجموعة "الأنونيموس المصريين" بتنفيذ "العملية نتنياهو"، بالهجوم على موقع رئيس الوزراء الإسرائيلي بنيامين نتنياهو؛ انتقامًا لمقتل جنود مصريّين على الحدود. وجرى بالفعل تعطيل الموقع، إضافةً إلى مواقعَ إلكترونية إسرائيلية أخرى[٣٧].

---

٣٠ بسام القنطار، "أنونيموس: خلّي الكيبورد صاحي"، جريدة **الأخبار**، ٢٠١٣/٤/٨، انظر:
http://www.al-akhbar.com/node/180791

٣١ "رسالة من الأنونيموس إلى الكيان الصهيوني"، ٢٠١٣/٤/٧، انظر:
https://www.youtube.com/watch?v=FPbjIS-GDHU&feature=player_embedded

٣٢ حسب ما جاء في الرسالة التي وجّهتها المجموعة المهاجمة للإسرائيليّين: "أنتم لم تتوقّفوا قطّ عن انتهاكاتكم التي لا تنتهي لحقوق الإنسان، لم تتوقّفوا قطّ عن المستوطنات غير الشرعية، لم تحترموا وقف إطلاق النار، بل لا تحترمون حتّى القانون الدولي"، انظر:
http://www.youtube.com/watch?v=0_rEQKUpsUc

٣٣ للمزيد 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

٣٤ "أنونيموس تشنّ أعنف هجوم إلكتروني ضدّ إسرائيل"، ٢٠١٣/٤/٧، انظر:
http://www.tech-wd.com/wd/2013/04/07/opisrael

للمزيد عن حجم الخسائر، انظر:
http://www.aleqt.com/2013/04/08/article_745515.html

٣٥ في نيسان/ أبريل ٢٠١٢ اتّهمت إيران كلًّا من إسرائيل والولايات المتّحدة باختراق أجهزة الكمبيوتر في مفاعل بوشهر النووي، وزرع فيروس "ستاكس نت" الذي أثّر في مفاعلاتها النووية.

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

٣٧ أبو طالب.

وفي عام ٢٠١٢، نجح مواطن سعودي في التاسعة عشرة من عمره يسمّي نفسه OXOMAR في اختراق مواقع إلكترونية تخصّ أفرادًا ومصارفَ، والحصول على معلومات تتعلّق بعشرات آلاف بطاقات الائتمان العائدة لإسرائيليين، وقام بنشرها على الملأ، ما يمكّن أيّ شخص من شراء ما يريد على الإنترنت باستخدام تلك البطاقات[٣٨]. كشفت جريدة **يديعوت أحرنوت** (٢٠١٢/١/١٧) أنّ الشابّ السعودي المذكور حاول اختراق مواقع إلكترونية إسرائيلية حسّاسة، بما في ذلك مواقع عدّة لبنى تحتية ووزارات وإدارات حكومية. أضافت الصحيفة أنّ الشابّ أكّد أنّه قام بذلك انتقامًا من إسرائيل على أعمال القتل والاعتداء على الفلسطينيين، وأنّ حرب غزّة ٢٠٠٨-٢٠٠٩ كانت محفّزة له ليقوم بذلك[٣٩].

بعد حادث "أسطول الحرية" التركي في نهاية أيار/ مايو ٢٠١٠، تعرّض نحو ألف موقع إسرائيلي للاختراق من جانب هاكرز أتراك[٤٠]. وفي ٢٩ تشرين الثاني/ نوفمبر ٢٠١٠ جرى اغتيال عالم نووي إيراني في طهران، وإصابة عالم آخر. بعد ذلك بيومين، توقّفت شبكة الاتصالات الإسرائيلية "سيلكوم" عن العمل لعدّة ساعات بعد هجوم إلكتروني[٤١]. وفي ٢٥ كانون الثاني/ يناير ٢٠١١، سقطت أيضًا شبكة "بيزيك" للاتصالات الإسرائيلية، وانقطعت الخدمة عن العملاء لعدّة ساعات. تحدّث البعض في إسرائيل عن عطلٍ فنّي، وعدّه آخرون اختراقًا من جانب قراصنة لتلك الشبكة[٤٢].

الإمكانيات الإسرائيلية في الفضاء الإلكتروني

أصبحت مسألة الحرب الإلكترونية من الأدوات الرئيسة التي يستخدمها الجيش الإسرائيلي لتحقيق أهدافه الإستراتيجية انطلاقًا من إدراك إسرائيل حقيقة أنّ الحرب القادمة هي حرب الفضاء الإلكتروني، والتي رأى المراسل العسكري الإسرائيلي البارز إليكس فيشمان أنّها حرب تستعدّ لها تل أبيب جيّدًا، خشية أن تدخل في أنظمتها الحسّاسة فيروسات تشلّ عملها في أحرج الأوقات، خاصّةً أنّ "أعداءها" نجحوا في السيطرة على عدّة أنظمة في السنوات الأخيرة، وقفزوا إلى مراتب تقنية ذات صلة بحرب "السايبر" الجارية بين الجيوش في عمق قلب معلومات العدوّ، وهي جبهة دينامية يستعملون فيها سلاحًا ثقيلًا، وتشبه الحديث عن "رقعة شطرنج" ضخمة عالمية تتحارب فيها أفضل العقول[٤٣].

لذا ظهرت دعوات من داخل المؤسسة الأمنيّة ولجنة الخارجية والأمن في الكنيست تنادي بضرورة إعادة صوغ النظرية الأمنيّة الإسرائيلية التي تمت بلورتها مطلع خمسينيات القرن الماضي بما يتوافق مع تلك الحرب التي باتت تمثّل هاجسًا يلفّ إسرائيل، ما دعاها إلى إجراء العديد من التجارب في هذا المجال وخرجت بنتائج تؤكّد الخطورة المتولّدة من إمكانية اختراق المواقع الحسّاسة في إسرائيل. ولهذا حاولت أن تسخّر إمكانياتٍ بشرية ومادية لدعم هذه المشاريع.

ومع ذلك، تبقى الأدبيات المتاحة للبحث في هذا الموضوع قليلة؛ إذ لا تتناول بوضوح إستراتيجية إسرائيل وعقيدتها إزاء الأمن الإلكتروني سوى بصورة طفيفة. وعند الحديث عن الاستعدادات التي قامت بها إسرائيل لحماية مجالها الافتراضي، فمن الممكن الإشارة إلى عددٍ من النقاط البارزة في هذا السياق:

١. تركّز الوحدة ٨٢٠٠ للجيش الإسرائيليّ، المكوّنة من المجنّدين والضُّبّاط، أعمالها على ثلاث نَواحٍ من الحرب الإلكترونية؛ هي: جمع المعلومات الاستخباراتيّة، والدِّفاع والهجوم الإلكترونيَّان.

٢. يتولّى جهاز الأمن الدّاخليّ (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[٤٤].

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[٤٥].

---

٣٨ غازي حمد، "الجهاد الإلكتروني ... والحرب الجديدة ضدّ إسرائيل"، جريدة **فلسطين**، ٢٠١٣/٤/٨.

٣٩ شهبون.

٤٠ المرجع نفسه.

٤١ المرجع نفسه.

٤٢ المرجع نفسه.

٤٣ عدنان أبو عامر، "إسرائيل وحرب الإنترنت"، **الجزيرة نت**، ٢٠١٢/٢/٧، انظر:
http://www.aljazeera.net/opinions/pages/910f8b7d-b7d0-4ac1-b875-78cca8d77c8e

٤٤ 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

٤٥ يوسف بوغنيمي، "الأنونيموس Anonymous عبث بالإنترنت، أم جيش إلكتروني 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 الدفاع عن المجال الافتراضيِّ[٤٦]. 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 الشيفرة و"جدران" الدِّفاع الافتراضيِّ الإسرائيليِّ[٤٧].

٥. في عام ٢٠١٢ خصَّص معهد الأمن القوميِّ الإسرائيليُّ برنامجًا تدريبيًا حول "الأمن السيبراني" أو أمن المعلومات، وأصدر المعهد في أيار/ مايو ٢٠١٢ تقريرًا مفصَّلًا عن "الحرب السيبرانية"، 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[٤٨].

٦. في آذار/ مارس ٢٠١١ أجازت الحكومة إقامة وحدة "منمار" (مديريَّة منظومات المعلومات) الحكوميَّة، وهي هيئة وزارية مشتركة، مهمتها 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[٤٩].

٧. أجازت الحكومة الإسرائيليَّة في ٢٧ آذار/ مارس ٢٠١١ إقامة "وحدة إدارة المعلومات"، وهي تتبع مدير عامِّ وزارة الماليَّة الإسرائيليَّة، ومسؤولةٌ مسؤوليةً مباشرةً عن جميع أنظمة الاتِّصالات المحوسبة الحكوميَّة، ومنها مشروع "بنية الحكومة التَّحتيَّة لعصر الإنترنت"[٥٠].

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[٥١].

٩. في عام ٢٠٠٢ أقيمت السُّلطة الرَّسميَّة لحماية المعلومات في جهاز الأمن العامِّ "الشَّاباك"، وهي مسؤولةٌ عن التَّوجيه المهنيِّ للهيئات ذات الصِّلة في مجال حماية شبكات حاسوبٍ حيويَّةٍ من التَّهديدات الإرهابيَّة والتَّخريب في مجال حماية المعلومات المصنَّفة (السِّريَّة) وتهديدات التَّجسُّس[٥٢].

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، فإنَّ 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[٥٣].

١١. هيئة الـ "سايبر" التَّابعة للجيش الإسرائيليِّ: في عام ٢٠٠٩ وصف الجنرال غابي أشكنازي، رئيس هيئة الأركان العامَّة آنذاك، الحيِّز الافتراضيَّ بأنه حيِّزٌ قتاليٌّ إستراتيجيٌّ[٥٤]. وبناءً على ذلك، أقيمت هيئة الـ "سايبر" في الجيش الإسرائيليِّ، لكي تستخدمها هيئة الأركان العامَّة في تنسيق نشاطات الجيش في الحيز الافتراضيِّ وتوجيهها[٥٥].

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

46 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

47 Ibid.

٤٨ أمـل خيري، "إسرائيل وقراصنة الإنترنت.. جولةٌ جديدةٌ في الحرب السيبرانية"، ٢٠١٣/٤/١١، انظر:
http://www.alamatonline.net/l3.php?id=56608

٤٩ "مقاطع من مذكِّرةٍ بشأن استعدادات إسرائيل لمواجهة عصر الحرب الافتراضيَّة"، **المشهد الإسرائيلي**، العدد ٢٩٢ (٢٣ تشرين الأوَّل/ أكتوبر ٢٠١٢)، ص٧، انظر:
http://www.madarcenter.org/mash_had_pdf/Al-Mashhad%2023-10-2012.pdf

٥٠ **المرجع نفسه.**

51 Lewis and Timlin.

52 Ibid.

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

٥٤ محمود محارب، عرض لكتاب **إسرائيل والحرب الإلكترونيَّة**، موقع المركز العربيِّ للأبحاث ودراسة السياسات، ١٠ آب/ أغسطس ٢٠١١، انظر:
http://www.dohainstitute.org/release/14e23aac-b76f-48f8-ba00-c94efe48fa36#a1

٥٥ المرجع نفسه.

الحكومة ومؤسَّساتها ودوائرها. ويستخدم المشروع وسائل وتدابير لحماية أمن شبكة الإنترنت الحكوميَّة، ابتداءً من طاقم خبراء حماية معلوماتٍ واتِّصالاتٍ، وانتهاءً بمنتجاتٍ وتقنياتٍ لشركاتٍ عالميَّةٍ رائدةٍ. كما أقيم في إطاره 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 مشروع "تهيلاه"، أو لجهاتٍ حكوميَّة غير مصنَّفة[٥٦].

على الصعيد الاقتصادي، يلاحظ أنّ ثمّة أهمية لتكنولوجيا المعلومات والفضاء الافتراضي بالنسبة إلى إسرائيل التي تُعدّ من الدول المتقدمة في العالم في مضمار تطوير التقنيات المعلوماتية والتكنولوجية. وقد حاولت إسرائيل توظيف الهجوم الإلكتروني الأخير عليها "للاستثمار بالشركات لتعزيز الصناعات الدقيقة وتطوير منظومات حماية المعلومات وجذب المستثمرين الأجانب لافتتاح المزيد من الشركات لصناعة وابتكار أنظمة المعلومات وتسويقها بالعالم بما يساهم في تعزيز وتدعيم الاقتصاد الإسرائيلي الذي يغرق بالركود"[٥٧].

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[٥٨]. 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 المحلي[٥٩]. هذا المعطى يضع إسرائيل في مصافِّ اقتصادات الإنترنت المتصدِّرة عالميًّا[٦٠].

56 "Cyber Warfare: Concepts and Strategic Trends."

٥٧ "الحرب الإلكترونيَّة تعزِّز صناعة المعلومات الإسرائيليَّة"، **وكالة فلسطين اليوم**، ٢٠١٣/٤/١٥، انظر:
http://paltoday.ps/ar/post/165435

58 "Cyber Warfare: Concepts and Strategic Trends."

59 Ibid.

60 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[٦١]. والهدف منه تحقيق غاياتٍ عدَّة مثل: كسر عزلتها الجغرافيَّة في الشَّرق الأوسط، وإقامة علاقاتٍ وثيقةٍ ومنتظمةٍ مع العالم، وتقوية 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[٦٢].

ما أهميّة الهجوم على المواقع الإلكترونية في إسرائيل؟

على الرَّغم من أنَّ مجموعة "الأنونيموس" نفَّذت تهديدها في السَّابع من نيسان/ أبريل ٢٠١٣، وعلى الرَّغم من محدوديَّة الضَّربة وآثارها التي هوَّنت إسرائيل من تداعياتها[٦٣]، 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:

الرسالة الأولى سياسيَّة، 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 في المقاومة، وأنَّ هذه القضيَّة ما زالت باقيةً في قلوبهم وعقولهم افتراضيًّا كما هي على أرض الواقع.

والرِّسالة الثَّانية تكنولوجيَّة، كونها استطاعت إيذاء إسرائيل افتراضيًّا، وأظهرت مدى قدرة الأخيرة في هذه الحرب، وأنَّ "قبَّتها الحديديَّة

٦١ تجدر الإشارة إلى قيام إسرائيل عام ٢٠٠٩ - بالتَّعاون مع الولايات المتَّحدة - بتعطيل أجهزة الطَّرد المركزيِّ التي تعتمد عليها إيران في تخصيب اليورانيوم، وذلك عبر استخدام فيروس "ستاكس نت". كما قامت بهجوم إلكترونيٍّ تعرَّضت له منظومات حواسيب إيرانيَّةٌ حسَّاسة في حزيران/ يونيو ٢٠١٢، وذلك عبر استخدام فيروس "فليم" Flame. ومن جهة أخرى، أقدمت 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.

٦٢ إيفن وسيمنطوف.

٦٣ قدَّرت مجموعة "أنونيموس" الخسائر التي سبَّبها الهجوم الإلكترونيِّ الذي بدأته مساء السَّبت على مؤسَّساتٍ ومواقع إسرائيليَّةٍ بنحو ثلاثة مليارات دولارٍ أميركيٍّ، لكنَّ إسرائيل قالت: إنَّ آثار الهجوم كانت محدودةً. "أنونيموس: كبَّدنا إسرائيل ٣ مليارات دولار في الهجمة الإلكترونية الأخيرة"، جريدة **المصريُّ اليوم**، ٢٠١٣/٤/٨، انظر:
http://www.almasryalyoum.com/node/1628706

الرَّقميَّة" يشوبها قصورٌ، وأنَّ ثمَّة جهاتٍ أخرى - سواءٌ أكانت دولاً أم أفرادًا - قادرةً على إلحاق الأذى بها.

والرِّسالة الثَّالثة عسكريَّة، وهي أنَّ إسرائيل 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 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 من الرَّسائل على خوادم الحواسيب الإسرائيليَّة، ويغرقون أنظمتها بشكلٍ تتوقَّف معه الشَّبكة عن العمل، ومعها أيضًا نظم الإنتاج والخدمات؟

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) كلَّها 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!