المعهد المصري للدراسات
EGYPTIAN INSTITUTE FOR STUDIES

الجيوبوليتكس السيبرانية والاستقرار في الشرق

ترجمات

١ يناير ٢٠١٨

عادل رفيق
مترجم وصحفي مصري

TURKEY- ISTANBUL
Bahçelievler, Yenibosna Mh 29 Ekim Cad. No: 7 A2 Blok 3. Plaza D: 64
Tel/Fax: +90 212 227 2262 E-Mail: info@eis-eg.org

WWW.EIPSS-EG.ORG
Eipss.EG Eis_EG

الجيوبوليتكس السيبرانية والاستقرار في الشرق الأوسط

عادل رفيق

المصدر: كريستينا كوسش / كبير الباحثين المقيمين بـ "صندوق مارشال الألماني (جي إم إف) - الولايات المتحدة"

منذ أن تسبب اختراق الموقع الإلكتروني للحكومة القطرية في يونيو ٢٠١٧ في إثارة أشد الأزمات التي تعرض لها مجلس التعاون الخليجي منذ تأسيسه، اتجهت دول الخليج إلى تكثيف جهودها لتعزيز قدراتها الإلكترونية ومواكبة الخطوات السريعة التي حققتها القوى الإلكترونية الإقليمية: إيران وإسرائيل. و من أجل إذكاء مشاعر الفرقة والخلافات بين دول المنطقة وسط جو مشحون بالتوترات منذ فترة طويلة، فقد تم استخدام تقرير إخباري مزيف في تعميق الاستقطاب واستغلال المشاعر المعادية لإيران من أجل تعميق هوة الخلافات وتمزيق المنطقة. لم تساهم أزمة قطر فقط في تصعيد التوترات الممتدة منذ فترة طويلة في منطقة شديدة الأهمية لمصالح الولايات المتحدة والاتحاد الأوروبي، وإثارة الشكوك حول الترتيبات الأمنية في المنطقة؛ لكنها أوضحت كذلك كيف أن السعي وراء تحقيق طموحات جيوسياسية توسعية من خلال شن هجمات إلكترونية موجهة يمكن أن يولد الصراعات ويؤدي إلى انهيارات سياسية كبيرة في لمح البصر.

وتعمل الاتجاهات الجيوسياسية العالمية على أن تكون حاضرة في منطقة الشرق الأوسط منذ زمن بعيد، وبشكل مكثف. فالابتكار الرقمي يتيح للخصوم السياسيين فرصة متزايدة لإيجاد نقاط الضعف التي يمكنها تدمير قدرات القوة الاقتصادية والعسكرية للدولة المعادية. وتقف الجغرافيا السياسية في مفترق طرق شديد الخطورة عندما يصبح مجال الفضاء الإلكتروني هو خط المواجهة الرئيسي. وعلى مدى السنوات القليلة الماضية، بذلت الحكومات والمجموعات غير الحكومية في الشرق الأوسط وشمال أفريقيا جهودا كبيرة لبناء قدراتها الإلكترونية. وقد يؤدي انتشار الأسلحة

الإلكترونية في المنطقة واستخدامها كأدوات جيوسياسية إلى تصاعد الأزمات الإقليمية وتفاقمها، وإلى زيادة المصالح الغربية في المنطقة.

الوجه الرقمي للجغرافيا السياسية

وقد ركزت معظم النقاشات عبر الأطلسي عن الأمن الإلكتروني - من الزاوية الجيوسياسية - على روسيا وتدخلها في الانتخابات الغربية. وقد أوضحت العمليات الروسية في الولايات المتحدة وفرنسا وعبر أوروبا بشكل كبير إمكانية إثارة الفوضى السياسية في الخارج باستخدام الأدوات الإلكترونية. ومع دخول الرقمية إلى الصناعات المختلفة، أصبحت الجغرافيا السياسية – وهي استخدام المهارة السياسية والأصول للحصول على نفوذ في الشؤون الدولية – بعيدة بشكل كبيرعن الإطار الجغرافي الأصلي لها. ويستضيف الفضاء الإلكتروني (السيبراني) – وهو الشبكة العالمية لتكنولوجيا المعلومات المترابطة بما في ذلك الأجهزة والبرمجيات والمعلومات – يستضيف بعض أهم الأسلحة ونقاط الضعف الجيوسياسية للدول على حد سواء. وبما أنه لا يمكن التفريق بين التهديدات الإلكترونية والتهديدات الجسدية، فمن المرجح أن تكون "الجيوسياسية الإلكترونية" في طليعة المنافسة الجيوسياسية في المستقبل.

وتشمل الأدوات السيبرانية المستخدمة من أجل تحقيق الأهداف الجيوسياسية مجموعة كبيرة من الأدوات مثل تلك المتعلقة بالمراقبة، والتجسس، والتضليل، أو الهجمات المدمرة. ويمكن تقسيم الهجمات السيبرانية إلى نوعين:

١) الإختراقات التي تستهدف جمع المعلومات (التجسس الرقمي)،

٢) الهجمات على الأنظمة الأجنبية لإيقاف شبكات الأعداء أو إتلافها، مثل الهيئات الحكومية والأهداف الرمزية والبنية التحتية الحيوية.

وفي حين أنه من غير المُكلِف والسهل نسبيا على القراصنة القيام باقتحام نظام ما، فإن القيام بشن هجوم له تأثير في العالم الحقيقي يبدو أكثر تعقيدا، ويتطلب قدرات لا تمتلكها العديد من القوى، ناهيك عن الجهات الفاعلة غير الحكومية. وتُعتبر كُلفة

الهجمات الإلكترونية كأداة للإرغام المباشر محدودة للغاية نظرا للطبيعة غير المعلنة لكل من هوية المنفذ والرسالة المقصودة من وراء الهجوم. غير أن الهجمات السيبرانية تتميز كثيراً عن الأدوات التقليدية ذات التأثير الدولي في ميدان المعركة الجيوسياسية وذلك من نواح أخرى كثيرة. ولهذه الهجمات قدرة عالية على التخريب بكُلفة اقتصادية منخفضة نسبيا للمهاجمين. وكذلك تُعتبر الكُلفة السياسية – في شكل إمكانية التعرض لخطر الانتقام – منخفضة جداً، نظرا للتحديات التي تعترض إمكانية تحديد هوية من قام بالهجوم. كما أن إغفال القانون الدولي لعقوبات ونصوص واضحة وقاطعة لمواجهة العمليات السيبرانية العابرة للحدود يجعلها أكثر جذباً للبعض. وحيث أنها تجمع بين القدرة التخريبية العالية والانتشار السريع بتكلفة سياسية واقتصادية منخفضة، فإن الهجمات السيبرانية تنتشر بشكل كبير بين الجهات الفاعلة التي تتبع استراتيجية جيوسياسية موسعة ذات موارد و / أو قدرات دفاعية محدودة.

ونظرا لصعوبات إسناد الهجمات إلى مرتكبيها وما يترتب على ذلك من احتمالات الانتقام المرتبطة بها، يمثل المجال السيبراني تحديا للآليات التقليدية للردع. ففي عام ٢٠١٥، قال أحد كبار الشخصيات الأمريكية المتخصصة في الفضاء الإلكتروني لمجلس الشيوخ الأمريكي أنه نظرا لأن الردع التقليدي "يتآكل لدرجة مقلقة، فإن معالجة هذا الخطر في مجال الفضاء الإلكتروني" أمر أساسي "من أجل الحفاظ على فعالية الأدوات التقليدية للسلطة الوطنية". ويمثل الانتشار السيبراني للجهات الفاعلة ذات الأجندة الإقليمية الممتدة في منطقة الشرق الأوسط تحديا خاصا في هذا الشأن.

الصحوة الإلكترونية في الشرق الأوسط وشمال أفريقيا

للجيوسياسية السيبرانية جذورها في منطقة الشرق الأوسط. ففي يونيو ٢٠١٢، نشرت وسائل الإعلام الأمريكية معلومات مسربة عن هجوم إلكتروني أمريكي-إسرائيلي على منشآت نووية إيرانية باستخدام فيروس "ستوكسنيت" الذي تم اكتشافه لأول مرة في عام ٢٠١٠. ويُعتقد أنها كانت المرة الأولى التي يتسبب فيها سلاح سيبراني هجومي في

إحداث أضرار مادية لمنشأة صناعية، بهدف الحد من الطموحات النووية الإيرانية من خلال تدمير خُمس أجهزة الطرد المركزي لتخصيب اليورانيوم الإيراني. وفي عامي ٢٠١١ و ٢٠١٢، اكتشفت مؤسسة "كاسبرسكي لاب"، ومقرها روسيا، اثنين من أدوات التجسس الإلكترونية الأخرى (دوكو واللهب) المرتبطة بـ "ستوكسنيت". وفي أعقاب ذلك، نُقل عن مسؤول كبير في الحرس الثوري الإيراني وصفه للحرب السيبرانية بأنها "أكثر خطورة من الحرب المادية الحقيقية."

وعلى مدى أكثر من عقد، استخدمت إيران أدوات إلكترونية للتجسس على المنشقين الإيرانيين والحد من وصول المواطنين الإيرانيين إلى المعلومات. وقد برزت القدرات الإلكترونية الإيرانية مع نشأة المؤسسات التعاونية الوطنية "هاكتيفيست" في العقد الأول من القرن الحادي والعشرين والتي كانت تهاجم بشكل منهجي شبكات المنظمات الأجنبية والحكومات المعادية للجمهورية الإسلامية. ويواصل العديد من الأعضاء السابقين في هذه الجماعات أنشطتهم اليوم لحساب النظام تحت مظلة "الجيش السيبراني الإيراني". وقد أدت أحداث الثورة الخضراء لعام ٢٠٠٩ إلى قيام النظام بشكل منهجي بتعزيز القدرات الإلكترونية للحد من المعارضة الداخلية. وأنشأت إيران أيضا نظام تشغيل حاسوبي وطني في عام ٢٠١٢، وكذلك خدمة بريد الكتروني وطنية في العام التالي. وبحلول عام ٢٠١٩ تقريبا، من المتوقع أن تكون شبكة الإنترنت الوطنية، المنفصلة عن الشبكة العالمية، جاهزة للعمل. ومنذ أن بدأت عملية "ستوكسنيت" عام ٢٠١٠ التي كشفت عن تعرض إيران للتدخل الأجنبي عبر الفضاء الإلكتروني، بدأت إيران في تكريس موارد كبيرة لزيادة ترسانتها الإلكترونية. وقد تطورت الأنشطة السيبرانية للجمهورية الإسلاميةعلى مدار العقد الماضي "من وسائل منخفضة التقنية للهجوم على أعدائها إلى ركيزة من ركائز مفهوم أمنها القومي".

ويُعد المجلس الأعلى للفضاء الإلكتروني الذي أنشأه آية الله خامنئي عام ٢٠١٢ بهدف تعزيز صنع القرار الإلكتروني في هيئة واحدة تحت قيادته – هو الهيئة الحكومية التي تشرف على معظم الأنشطة الإلكترونية بالبلاد. ويتألف المجلس من أعضاء أجهزة

المخابرات والأمن الإيرانية المختلفة. وعلى الرغم من أن الطريقة التي يتم تفعيل القدرات السيبرانية من خلالها في المؤسسات المختلفة للجهاز السياسي والدفاع الإيراني لا تزال غامضة، فإن لائحة اتهام لسبعة قراصنة إيرانيين كانت قد صدرت عن وزارة العدل الأمريكية عام ٢٠١٦ ذكرت بشكل لا لبس فيه أن المتهمين "قاموا بأعمال (سيبرانية) نيابة عن الحكومة الإيرانية، بما في ذلك جهاز الحرس الثوري الإسلامي ".

إن نشاط إيران السيبراني الدولي لا يقتصر على التجسس والآليات الدفاعية، بل إنه أصبح يستهدف بشكل متزايد الاضطرابات السياسية بهدف تحقيق أهداف جيوسياسية. وقد برزت هذه القدرات في أغسطس ٢٠١٢، عندما هاجمت مجموعة قراصنة إيرانية تدعى "شمعون" شركة أرامكو السعودية، أكبر شركة نفط في العالم، وأساس الثروة السعودية وذلك ردا على فيروس مجهول تم اكتشافه في شبكة وزارة النفط الإيرانية قبل ذلك بأربعة أشهر. وقد قام الفيروس الخبيث المدمر الذي أطلقته مجموعة "شمعون" بإزالة البيانات على ثلاثة أرباع أجهزة الكمبيوتر التابعة لشركة أرامكو، وبثت على شاشاتها صورة لعلم أمريكي يحترق. واضطرت أرامكو حينئذ إلى إغلاق شبكتها وتدمير حوالي ٣٥،٠٠٠ جهاز كمبيوتر. وفي وقت لاحق من ذلك العام، أطلقت جماعة "هاكتيفيست" نفس الفيروس المختص بإزالة المعلومات على "هيئة الغاز الطبيعي" في قطر، 'جاس راس'.

في فبراير ٢٠١٤، أظهرت إيران أيضا أنها على أتم استعداد لاستخدام الفضاء الإلكتروني في الاستهداف المباشر لمن يعارضون سياساتها في الخارج وتخويفهم. فهاجمت شبكة مؤسسة "لاس فيجاس ساندز"، والتي كان الرئيس التنفيذي لها، وهو مؤيد قوي لإسرائيل، قد اقترح علنا إطلاق قنبلة نووية على طهران. وأجرت إيران أيضا أنشطة لـ 'منع الخدمة' وذلك بإيقاف إمكانية الوصول إلى النظم مؤقتا. وفي عامي ٢٠١٣ و ٢٠١٤، استهدف القراصنة الإيرانيون المؤسسات المالية الأمريكية. ولعل الأهم من ذلك أن إيران أثبتت قدرتها ونواياها للدخول على شبكات وأنظمة البنية التحتية الحيوية لمنافسيها، مثلما حدث عندما اخترقت أنظمة التحكم في سد صغير يعمل بالحاسوب في راي بروك

بنيويورك. وفي حين تم الكشف عن أن الجمهورية الإسلامية كانت من وراء ١٩ عملية هجوم إلكتروني برعاية الدولة منذ عام ٢٠١٠، فقد كانت أيضاً هدفاً لـ ١٨ من مثل هذه العمليات من قبل آخرين.

وتمتلك إسرائيل، قبل إيران، أهم القدرات الإلكترونية في منطقة الشرق الأوسط وشمال أفريقيا، على نفس مستوى القوى الإلكترونية الأولى في العالم: الولايات المتحدة وروسيا والصين. ومع أنها من أكثر اللاعبين السيبرانيين حنكة على مستوى المنطقة، فقد كانت إسرائيل هدفاً لـ ١١ من العمليات السيبرانية الهجومية المعروفة منذ عام ٢٠١٠ وكانت وراء شن خمس عمليات من هذا القبيل خلال نفس الفترة. وفي سياق سعي إسرائيل للدفاع عن نفسها ضد هجمات القراصنة الصغيرة، تزعم إسرائيل أنها قامت بصد ضربة واسعة النطاق من إيران خلال حرب الأولى مع حماس. كما نسبت شركات الأمن السيبراني الأمريكية أنشطة "وقف الخدمة" ضد إسرائيل للقراصنة الإيرانيين (وربما تحت رعاية الدولة) خلال وبعد حرب غزة عام ٢٠١٤. وفي العام التالي، اكتشفت شركة أمن إلكترونية إسرائيلية حملة واسعة النطاق للهجوم السيبراني تستهدف الموردين العسكريين وشركات الاتصالات ووسائل الإعلام والجامعات في إسرائيل وعشرات البلدان الأخرى باستخدام برامج ضارة تهدف إلى سرقة البيانات الحساسة. وتشتبه الشركة في أن حزب الله الذي يدين بالولاء لإيران كان من وراء الهجوم، مما يمثل تحولا في نطاق المعركة الرقمية لإسرائيل مع خصومها الإقليميين.

وفي عام ٢٠١٢، أنشأت الحكومة الإسرائيلية مكتبا وطنيا للفضاء الإلكتروني؛ ثم في عام ٢٠١٥، أسست الهيئة السيبرانية الوطنية كجهاز تنسيق بميزانية قدرها ٥٠٠ مليون دولار لاستكمال إعداد كفاءات صنع السياسات. وتماشيا مع نهج إسرائيل في مجال تنظيم المشاريع في مجال الفضاء الإلكتروني، أنشأت الحكومة الإسرائيلية مجموعة مراكز أبحاث للتهديدات السيبرانية في مدينة بئر السبع الصحراوية - وذلك على غرارعمالقة التقنية الأمريكية الرئيسيين مثل جوجل - وهي تضم فريقاً من الخبراء السيبرانيين الحكوميين، والقطاع الخاص.

وتُعتبر وحدة إسـرائيل ٨٢٠٠، المسـؤولة عن العمليات الإلكترونية، هي أكبر وحدة في قوات الدفاع الإسرائيلية. وقد اعتمد نتنياهو الأمن السيبراني كأولوية شخصية، وترتبط الهيئات الإلكترونية المذكورة آنفا مؤسسيا بمكتب رئيس الوزراء الإسرائيلي. في أوائل عام ٢٠١١، تعهد نتنياهو علنا بتحويل إسـرائيل إلى "قوة إلكترونية عالمية". وفي أوائل عام ٢٠١٦، كان لدى إسرائيل أكثر من ٣٠٠ شركة من شركات الأمن السيبراني ، وحققت صـادرات بقيمة ٦ مليارات دولار، و ٢٠ في المائة من الاسـتثمارات الخاصـة في المجال السـيبراني في العالم. وبينما تعزز بلدان مثل إيران وإسـرائيل مكاسـبها كقوى إلكترونية كبيرة، تحاول قوى أخرى في المنطقة اللحاق بالركب.

سباق التسلح السيبراني في الخليج؟

منذ هجوم أرامكو السـعودية عام ٢٠١٢، كانت إيران والسـعودية تطلقان نيران المدفعية الرقمية على بعضـهما البعض في صـراع متجدد في الفضـاء الإلكتروني ، وبلغ ذروته مع تداعيات أزمة قطر على دول مجلس التعاون الخليجي في يونيو ٢٠١٧. ووفقا لقطر، فقد قام قراصنة بخرق موقع وكالة الأنباء القطرية على شبكة الإنترنت وذلك باستخدام أجهزة من داخل الإمارات العربية المتحدة لوضـع تصـريحات زائفة تحتوي على ملاحظات مثيرة للجدل حول إيران وغيرها من القضـايا الإقليمية الحسـاسـة على المسـتوى الدبلوماسـي، ونسـبتها إلى أمير قطر. وسـرعان ما تحول هذا الاختراق، الذي نفت حكومة الإمارات العربية المتحدة المشاركة فيه، إلى المقاطعة المستمرة لدولة قطر من قبل دول أعضـاء في مجلس التعاون الخليجي: السـعودية والإمارات والبحرين، بالإضافة إلى مصـر. ثم تسـربت رسـائل محرجة من البريد الإلكتروني للسـفير الإماراتي في الولايات المتحدة بعد فترة وجيزة، مما يشـير إلى محاولة الانتقام من جانب قطر، على الرغم من أن قطر نفت أي تورط في هذا الأمر. وتشـير الأرقام الواردة أدناه – عن العمليات الإلكترونية التي ترعاها الدولة، والتي قام بجمعها مجلس العلاقات الخارجية –

أن سباق التسلح السيبراني يجري على قدم وساق بين إيران وإسرائيل ودول مجلس التعاون الخليجي، وتُظهر فيه المملكة العربية السعودية ضعفا واضحا.

وأدى التحدي الأمني الرقمي في الخليج العربي الذي تتزايد فيه العدائية بشكل كبير إلى تحفيز دول خليجية صغيرة مثل الإمارات العربية المتحدة - التي تفتخر بشبكات المدن الذكية ولكنها تخشى من تزايد نقاط الضعف السيبراني – للاتجاه نحو بناء صناعات دفاع إلكترونية كبيرة. ووفقا لمنظمة التعاون الإسلامي، فإن "الخطوات الكبيرة التي تتخذها المنطقة نحو الرقمنة - التي من المتوقع أن تضيف أكثر من ٨٠٠ مليار دولار إلى الناتج المحلي الإجمالي وأكثر من ٤ ملايين وظيفة بحلول عام ٢٠٢٠ - تجعل الخليج هدفا رئيسيا للتهديدات الإلكترونية التي تتطور بشكل سريع. وبالإضافة إلى ذلك، فإن الاعتماد الشديد على النفط والغاز، بما في ذلك في توفير المياه العذبة، يجعل دول الخليج والشرق الأوسط وشمال أفريقيا على وجه الخصوص أهدافا ضعيفة للهجمات الإلكترونية ذات التأثير الإنساني الكبير. وبينما يكافح الخليج ومناطق أخرى في العالم من أجل بناء ردع فعال ضد الانتهاكات الرقمية الإجرامية، فإن منظومة القوانين الخاصة بذلك ليست فعالة ضد القرصنة التي تتم تحت رعاية دول وليس فقط أفراد.

وقد أدت الهجمات التي وقعت خلال السنوات القليلة الماضية إلى قيام نشاط ملحوظ بين دول مجلس التعاون الخليجي لبناء قدرات الأمن السيبراني وانشاء المؤسسات ووضع الاستراتيجيات. وبصرف النظر عن بناء قدراتها الخاصة، فإن لدى المملكة العربية السعودية ودول مجلس التعاون الخليجي الأخرى الموارد اللازمة للاستعانة بمصادر خارجية وتوظيف قراصنة من الطراز العالمي في عملياتها الإلكترونية. في عام ٢٠١٣، وهو العام الذي أعقب هجوم "شمعون" على أرامكو، اعتمدت المملكة العربية السعودية أول استراتيجية وطنية لأمن المعلومات. وفي فبراير ٢٠١٧، افتتحت الرياض مركزها الوطني للأمن السيبراني التابع لوزارة الداخلية كمركز تنسيق فني وطني للدفاع الإلكتروني. ومن المتوقع أن ينمو سوق الأمن السيبراني السعودي بنحو ٦٠٪ إلى ٣,٤٨ مليار دولار بحلول عام ٢٠١٩. وبالمثل، أنشأت دولة الإمارات العربية المتحدة الهيئة

الوطنية للأمن الإلكتروني ومقرها أبو ظبي في أغسطس ٢٠١٢، واعتمدت في عام ٢٠١٧ استراتيجية دبي للأمن السيبراني. هيئة التنسيق السيبراني المشتركة بين الوزارات في قطر، وضعت اللجنة الوطنية للأمن السيبراني الاستراتيجية الوطنية للأمن السيبراني في البلاد في عام ٢٠١٣.

وتُشير استثمارات طهران الكبيرة في تطوير قاعدتها التكنولوجية والقوى العاملة إلى أنها لن تبقى خلف إسرائيل لفترة طويلة. وتستخدم إيران الفضاء الإلكتروني لتطوير ونشر أدوات غير متماثلة ضد الولايات المتحدة والمنافسين الإقليميين في إسرائيل والخليج. وقد اتسعت ساحة الهجمات السيبرانية كثيراً بالنسبة لطهران تزامناً مع توسعها الإقليمي عبر الحرب بالوكالة.وتستهلك الحرب التقليدية بالوكالة في ساحات القتال في سوريا واليمن تكاليف مالية وبشرية كبيرة في تلك المواجهات.

وعلى الرغم من مختلف أدوات الدفاع التي تحت تصرفها، فإن هناك شكوكاً - على الأقل – في أن يستطيع الجيش التقليدي الإيراني المنافسة مع أعداء إيران الإقليميين والدوليين في ساحة المعركة. وعلى النقيض من ذلك، فإن كفة قدراتها في مجال الفضاء الإلكتروني ترجح لصالحها عند المقارنة مع دول المنطقة. فالهجمات السيبرانية تسمح لإيران "بالهجوم على خصومها بشكل مستمر على الصعيد العالمي، ، ولتحقيق تأثيرات استراتيجية بطرق لا يمكن أن تكون متاحة في المجال المادي"، كما يقول خبير الإنترنت مايكل آيزنشتات.

إذا كان اعتماد إيران على وكلاء للقيام بعمليات عسكرية نيابة عنها جعل نسبه مباشرة إلى القيادة الإيرانية أمراً صعبا، فإن الأمر بنفس الصعوبة كذلك في حالة الفضاء السيبراني، حيث أن درجة السيطرة على مجموعة من القراصنة أمر غامض ويمكن أن يتغير بسرعة مع مرور الوقت. ويُعتقد أن إيران قد قدمت الدعم إلى المجموعات الإلكترونية لحزب الله، والجيش الإلكتروني السوري، والجيش السيبراني اليمني، وكذلك حماس. وعلى الرغم من درجة السيطرة التي تمارسها القيادة السياسية الإيرانية على وكالات الاستخبارات، فإن أمر استئجار قراصنة يكون في غاية الغموض؛ ومع ذلك فإن

الخبراء يرون بأن الهجمات الإلكترونية على الأعداء السياسيين لإيران تعتمد على الأقل على موافقة ضمنية من النظام. وكما يقول مايكل سولمبير، فإنه رغم أن اعتماد إيران بشدة على الوكلاء يجنبها نسبة ما يقومون به إلى الجمهورية الإسلامية، فإنه يحمل كذلك عددا من المخاطر. فقد تختلف مصالح الوكلاء، أو قد تتعارض مع مصالح الدول الراعية لها، وقد تكون أكثر ميلا لاحتواء مخاطر الأضرار الجانبية. وقد تكون درجة حرصهم على إخفاء انتماءاتهم أقل من رعاياهم، مما يزيد من خطر تعرض الدولة الراعية للتتبع والانتقام والتصعيد. وأخيرا، فعلى عكس أن نقل البنادق أو المتفجرات إلى الوكلاء تتطلب إمدادات جديدة منتظمة باستمرار، فإنه بمجرد نقل الموارد والأدوات الإلكترونية إلى الوكلاء، تصبح إزالة هذه الأدوات بشكل فعال خارجاً عن سيطرة الدولة الراعية. وهذا بدوره قد يحفز الوكلاء على الاستمرار في نفس المسار وعدم التوقف، وقد يصبحوا مستقلين عن الدول الراعية، و قد يصل الأمر حتى إلى استخدام الأدوات التي حصلوا عليها ضد الدولة الراعية. وبعبارة أخرى، فإذا كان التحكم في الوكلاء يمثل تحديا في الحرب المادية، فإن ممارسة هذه السيطرة ستكون أكثر صعوبة بالنسبة للدول الراعية في عالم الفضاء الإلكتروني.

ومما يزيد من تعقيد إمكانية تصعيد العداوات في منطقة الشرق الأوسط وشمال أفريقيا عن طريق الهجمات السيبرانية أن الدول ليست وحدها من يقوم - مباشرة أو عن طريق جيوش القراصنة التي قد تستخدمها – بهذه الهجمات، ولكن هناك أيضاً جهات فاعلة مستقلة وغير حكومية تستخدم الهجمات السيبرانية والحرب الرقمية على نطاق أوسع من أجل تحقيق أهدافها. وقد أتاح انتشار الأيديولوجية الجهادية والدعاية لها، والأدوات اللازمة من أجل التجنيد والتدريب، وكذلك الاتصالات المشفرة عبر الإنترنت – أتاح للجماعات المتطرفة العنيفة العابرة للحدود الوصول إلى جمهور عالمي . وعلى الرغم من أن تنظيم الدولة الإسلامية قد فقد قبضته الإقليمية، فإن "إمبراطوريته على وسائل التواصل الاجتماعي" لا تزال قائمة. في الواقع، مع تراجع تنظيم داعش على ساحة المعركة المادية، فمن المرجح أن يشهد الامتداد الجيوسياسي للتنظيم انطلاقة جديدة

عبر قنوات الفضـــاء الإلكتروني. وقـد أدى الاختراق الـذي فـام بـه الجيش السـوري الإلكتروني - وهو مجموعة من القراصـنة الذين يدعمون بشـار الأسـد - في أبريل ٢٠١٣ ، إلى إرســال تغريدات مزورة من حســاب "أســوشــييتد برس" على تويتر حول هجوم محتمل بالقنابل على الرئيس أوباما ، مما أدى إلى تراجع كبير في البورصــة الأمريكية. كما هاجم الجيش السوري الإلكتروني أيضاً وسائل الإعلام الغربية الرئيسية الأخرى بما في ذلك ســي بي إس، وبي بي ســي، وواشــنطن بوســت، وأونيون، ردا على ما أســمته التغطية أحادية الجانب للحرب الأهلية الســورية. وبُعد هجوم عام ٢٠١٥ على قناة "تي في ٥ موند" الفرنســية والذي تبنته داعش دليل آخر للقدرة المتزايدة للمهاجمين السيبرانيين من غير الدول في منطقة الشرق الأوسط. وعلى الرغم من السعي الحثيث لمجموعات مثل داعش إلى بناء قدرات إلكترونية هجومية، يرى الخبراء أنها بعيدة كل البعد عن القدرات والتهديدات الكبيرة التي تُشــكلها القرصــنة التي ترعاها الدول. وعلى نفس المنوال، قال نائب مدير الدفاع الأمريكي روبرت وورك في أواخر عام ٢٠١٥، "تقوم الجماعات الإرهابية، بما في ذلك تنظيم الدولة الإســلامية في العراق والشــام، بإجراء تجارب للقرصــنة يمكن أن تُشــكل أســاســا لتطوير قدرات إلكترونية أكثر تقدما. ويقوم بعض المتعاطفين مع الإرهابيين بشــن هجمات إرهابية منخفضــة المســتوى نيابة عن الجماعات الإرهابية وبذلك يجذبون انتباه وســائل الإعلام التي قد تبالغ في القدرات والتهديدات التي تشكلها هذه الجهات الفاعلة.

التسريع بإثارة الفوضى

كان الانتشار السيبراني في الشرق الأوسط في بعض الحالات جزءا من مجاراة التوترات والنزاعات المتمددة بين دول المنطقة. وقد كان لعزل إيران عن دول المنطقة، والحروب بالوكالة في سوريا واليمن وليبيا، والعداوة المستمرة بين إسرائيل وجيرانها – كان لذلك دور كبير في تكريس اهتمام دول المنطقة بزيادة قدراتها الســيبرانية، والتصــميم على استخدامها ضد المنافسين السياسيين للدولة (سواء داخل البلاد أو خارجها).

وفي الوقت نفسه، فإن الاستخدام السياسي للأدوات السيبرانية يُسَرع بشكل كبير إمكانية حدوث مواجهة جيوسياسية في الشرق الأوسط، قد تؤدي إلى زعزعة الاستقرار الإقليمي بشكل كبير. وتؤدي التوترات والصراعات السياسية في الشرق الأوسط وشمال أفريقيا إلى توفير أسباب إضافية للتصعيد بشكل أكبر تجاه تلك المواجهة، وهو ما حدث بالفعل بأشكال عديدة. وقد أظهرت حكاية قطر مدى هشاشة السياسية الخليجية وكيف يمكن استهدافها بسهولة من خلال العمليات الإلكترونية. إن مجرد توجيه هجوم واحد في منطقة تعج بالتوترات قد يُعَرض للخطر نظام الأمن الخليجي الذي تعتمد عليه سياسة الولايات المتحدة في الشرق الأوسط، وكذلك استمرارية الائتلاف العالمي بقيادة الولايات المتحدة لهزيمة داعش. ومع تصلب الجبهات بعد خمسة أشهر من المواجهة، يبدو أن الحفاظ على مواجهة دائمة بمستوى منخفض هو الأكثر احتمالا بين جميع الخيارات. وبدون وجود مجلس تعاون خليجي موحد، سيكون من الصعب مواجهة النفوذ الإيراني في المنطقة. ويخشى المراقبون الغربيون من أن تمهد الأزمة الطريق لدخول إيران وغيرها إلى ما كان يُعتبر حتى الآن واحداً من أكبر الترتيبات السياسية والأمنية المؤيدة للغرب (في منطقة الخليج العربي). وقد أدى ارتفاع القدرات وإدراك الإمكانات الجيوسياسية للهجمات الإلكترونية إلى تعميق الصدع العربي الداخلي، وهو ما يظهر بالفعل في ساحات المعارك التقليدية في اليمن وسوريا وليبيا، وعلى المستوى الرقمي كذلك.

ويُعد الأثر الذي يمكن أن تحدثه براعة القدرات الإلكترونية الإيرانية (الحقيقية أو المشتبه بها) على خطة العمل الشاملة المشتركة وعلاقات طهران مع القوى العالمية من بين الآسباب المباشرة لزعزعة الاستقرار على نطاق أوسع بالمنطقة. ومن المرجح أن تؤثر هجمات إيران السيبرانية المستمرة على الأهداف السياسية والمؤسسية الأمريكية – من المرجح أن تُؤثر على دوائر السياسة الأمريكية في تقييمها السنوي للعلاقة مع طهران، ولا سيما في دعم الكونجرس لبرنامج العمل المشترك أو الصفقة معها بخصوص البرنامج النووي. وإذا قللت إيران من نطاق الهجمات على الأهداف الأمريكية، وركزت

بدلا من ذلك على عمليات عدوانية غير معلنة ضـد خصـومها في المنطقة، فإن الأخيرة (دول المنطقة) سوف تتطلع إلى الولايات المتحدة للحصول على دعمها في ذلك.

وفي الوقت ذاته، قد يحاول الخصـوم الإقليميون الاسـتفادة من صـعوبات تحديد هوية مرتكب الهجوم على وجه التأكيد في تبرير العمل العدواني الموجّه ضد بعضهم البعض و / أو طلب الدعم من الحلفاء في الخارج. وعلى سـبيل المثال، فمع وصـف إيران بأنها الدولة العدوانية المارقة في المنطقة، تبدو العمليات السـيبرانية المجهولة فرصـة ذهبية لمنافسـي إيران للحصـول على ميزة جيوسـياسـية في علاقاتهم مع إدارة ترامب. وقد هاجمت نسـخة من فيروس شـمعون الذي ضـرب أرامكو السـعودية في عام ٢٠١٢ أجهزة الكمبيوتر الحكومية السـعودية في نوفمبر ٢٠١٦، وفي هي المرة تم عرض صـورة للطفل السـوري الغريق أيلان كردي على شـاشـات الأجهزة هناك. وقد اقترح بعض الخبراء أن هذا الهجوم - وهو عملية مجهولة الفاعل – كان يسـتهدف عرقلة خطة العمل الشـاملة أو ما يُعرف بالاتفاق النووي مع إيران.

وقد تؤدي الهجمات العدوانية الصـريحة التي تتخطى الخطوط الحمراء في منطقة متوترة بالفعل - مثل نشـر إيران لسـلاح إلكتروني قوي يمكن أن تصـل آثاره إلى العالم المادي - إلى تفكيك كامل للعلاقات الإقليمية. وقد لا يقتصـر أثر هذا التصـعيد على الجبهات السـيبرانية فقط، بل يمكن أن يمتد أثر ذلك إلى النزاع النووي مع إيران، وجميع جبهات القتال في الشـرق الأوسـط في سـوريا واليمن وليبيا، وقد يؤدي ذلك إلى فتح خطوط مواجهة حقيقية جديدة. ويشـير الخبراء السـيبرانيون إلى أن الهجمات المدمرة من نوع فيروس شـمعون سـوف تتزايد في عددها وقوتها المدمرة في ظل اسـتمرارية الهجمات منخفضة المستوى وكذلك انتشار الأسلحة الإلكترونية الكبيرة، وذلك في ظل سعي المزيد من الدول لاكتساب قدرات سيبرانية هجومية. ولكن حتى في غياب حدوث هجمات واسعة النطاق، فقد يساهم استمرار أو زيادة "المدفعية الإلكترونية" الحالية في المنطقة في زيادة تصلب الجبهات: إيران من جهة والمملكة العربية السعودية وإسرائيل من جهة أخرى. وقد يصـل شـعور الرياض بالحصـار إلى آفاق جديدة، قد تصـل إلى

مواجهات أكثر على أرض الواقع. وبطريقة أو بأخرى، فإن الوضع الحالي لإيران كقوة صاعدة في الفضاء الإلكتروني يعني أن التنافس السياسي والتوترات السائدة منذ زمن في منطقة الخليج والشرق الأوسط بشكل عام ستتفاقم لا محالة.

وبالإضافة إلى خطر زيادة التصعيد الإقليمي، فإن ما يُعتبر الآن في معظمه مواجهات داخلية خليجية يمكن أن يتطور إلى مواجهة أكبر بين كتل مختلفة، حيث يحاول الخصوم في الجانبين ضم جهات فاعلة أخرى لدعمها. ويبدو أن الجهود التي تقوم بها بعض القوى الإقليمية مثل: السعودية ومصر وقطر وإيران - لبناء علاقات مع الصين واليابان والهند وروسيا تخوفاً مما قد يحدث في حال رفعت الولايات المتحدة وأوروبا يدها عن المنطقة، قد تسارعت كثيراً بسبب أزمة قطر، مما سيُؤدي إلى تحولات مهمة في لغز العلاقات في الشرق الأوسط. وقد أصبح هذا بالفعل حقيقة واقعة مع تحول الدوحة الواقعة تحت الحصار إلى إيران وتركيا وروسيا، واستمرار بقية دول مجلس التعاون الخليجي في كنف الولايات المتحدة وإسرائيل. وقد تمكنت قطر من تعويض الأضرار الاقتصادية الناجمة عن حصار دول مجلس التعاون الخليجي من خلال تغيير شريكها التجاري الرئيسي بحيث يصبح سلطنة عمان بدلاً من الإمارات العربية المتحدة والوصول إلى إيران وتركيا. ومن نتائج الحصار على قطر استمرار الانقسام في الخليج مما يقوي إيران ويدعم مجموعة من القوى قد تكون لها طموحات في المنطقة - إيران وروسيا وتركيا – على حساب الباقين. في الحقيقة، ظل الانقسام الخليجي في مرحلة سكون لسنوات وكانت له أسبابه الخاصة التي أدت إلى تفاقمه قبل انتشار استغلال امكانات الفضاء الإلكتروني بهدف القرصنة في منطقة الشرق الأوسط وشمال أفريقيا بسنوات.

ومع ذلك، فقد لوحظ بوضوح شديد، سواء في منطقة الخليج أوخارجها أن هجوماً الكترونياً عبر الإنترنت قد وفر الأسباب الكافية لتحويل المشاعر العدائية إلى تصعيد دبلوماسي كامل. (وهو ما حدث في أزمة حصار قطر).

وقد يؤدي صعود الفضاء الإلكتروني كساحة إضافية للجيوسياسية في منطقة الشرق الأوسط وشمال أفريقيا إلى توفير بعض الإمكانات التي تساعد على تفادي النزاعات أو تخفيف حدتها. فعلى سبيل المثال، قد تختار بعض الدول إطلاق العمليات الإلكترونية من أجل تجنب شن الهجمات العسكرية التقليدية على الأرض. يُذكر ان الهجوم الإلكتروني الإسرائيلي-الأمريكي "ستوكسنيت" قد ساهم في تجنب الضربة الوقائية التي كانت إسرائيل تخطط لها ضد إيران. ومع ذلك، فإن فاعلية هذه الآثار البديلة تنتفي تماماً عندما تقرر الدول المستهدفة أن تنتقم لتلك الهجمات السيبرانية ليس فقط بالمثل، ولكن بكل الوسائل المتاحة لها. وقد قال بنيامين نتنياهو إن إسرائيل لن تخجل من استخدام القوة العسكرية للانتقام عند تعرضها لهجوم سيبراني واسع النطاق، وذلك من أجل "الرد على الهجوم والرد على المهاجم" في آن واحد. ويُعطي الأمر التنفيذي رقم: ١٣٦٩٤ الذي وقعه الرئيس الأمريكي باراك أوباما في أبريل ٢٠١٥ حكومة الولايات المتحدة الأمريكية صلاحية الرد على الأنشطة الإلكترونية الخبيثة، خارج نطاق الفضاء الإلكتروني.

ومن المحتمل أن يكون هناك توجه إيجابي من وراء تصاعد المواجهة بين دول مجلس التعاون الخليجي من ناحية وإيران من ناحية أخرى، بما في ذلك المجال الإلكتروني، وهو ظهور نوع من التقارب البراجماتي من بعض دول مجلس التعاون الخليجي مع إسرائيل - العدو الإقليمي لإيران والقوة الأولى في المنطقة على مستوى القدرات الإلكترونية و العسكرية التقليدية . وقد لوحظ في الفترة الأخيرة تبني البحرين، وهي دولة خليجية صغيرة ذات أغلبية شيعية ، خطاباً وديًا مُعلناً تجاه إسرائيل. ويؤكد دبلوماسيون إسرائيليون أن موقف التحول تجاه إسرائيل من مملكة البحرين لا يمكن أن تتم دون موافقة المملكة العربية السعودية، وهناك العديد من التقارير غير المؤكدة أن هناك تقارب رسمي بين السعودية وإسرائيل يلوح في الأفق. وهناك تخوف من أن فك الارتباط المحتمل للولايات المتحدة في سوريا بعد الهزيمة الإقليمية لداعش سيترك المجال خالياً لإيران هناك وقد تُسهم روسيا بشكل أكبر في هذا التقارب غير الرسمي.

الجاهزية الدائمة لمواجهة الخطر السيبراني

إن الاستخدام المتزايد للهجمات السيبرانية من أجل تحقيق أهداف جيوسياسية قد يؤدي إلى تسريع تفكيك منطقة الشرق الأوسط غير المستقرة أصلا، والتي مزقتها الحروب. وسوف تُشكل الجيوسياسية السيبرانية العلاقة بين إيران وجيرانها؛ ويُنتظر من حلفاء الجانبين، وخاصة الولايات المتحدة، القيام بدور محوري في هذه المواجهة حتى ولو كان بشكل غير معلن. ومع أن الولايات المتحدة الأمريكية تُعتبر القوة الإلكترونية الرائدة في العالم، إلا أنها قد لا تستمر بنفس القوة في مجال الفضاء السيبراني كما هي الآن. وحيث أن معظم العمليات السيبرانية تتعلق بالانتقام وما قد تُحدثه من تأثير على تحالفات الهدف من هجومها، فإن من الأهمية بمكان وضع حدود واضحة لذلك وضمان حدوث الردع الفعال في الوقت الذي تظل فيه قدرات إيران محدودة إلى حد ما.

وعلى الرغم من أنه من غير الواضح ما إذا كانت إيران سترد على الهجمات السيبرانية بالوسائل العسكرية، فإن ما تعودنا عليه حتى الآن هو قيامها بالرد إلكترونياً بنفس الطريقة التي هوجمت بها؛ كما أن الاعتماد الكبير للاقتصاد الأمريكي على شبكات الحاسوب الضعيفة نسبيا قد أتاح لإيران فرصا كثيرة لإمكانية القيام بذلك. ووفقا لبعض الخبراء، فإنه نظرا للضعف السيبراني في الولايات المتحدة، فإن أفضل وسيلة لردع إيران في المجال السيبراني هو تهديدها بالقيام بعمل عسكري. ومع ذلك، وكما هو الحال مع جميع أنواع الردع، فإن قيمة وأثر مثل هذه التهديدات يعتمد على مصداقيتها. وقد كتب آيزنشتات يقول: "إن قبول وتبني واشنطن لهجوم فيروس "ستوكسنيت" لتفادي ضربة عسكرية إسرائيلية على البرنامج النووي الإيراني ربما يكون قد عزز التصور بأن الإدارة الأمريكية كانت مترددة في تحدي طهران في المجال المادي (العسكري). ومن المفارقات أن هذا الاستخدام البارز للهجوم السيبراني ضد إيران ربما كان سبباً في تقويض الردع السيبراني عن غير قصد". وتدرك إيران جيدا الآثار الضارة على الاقتصاد العالمي التي قد تسببها أي هجمات مباشرة تشنها على أهداف للولايات المتحدة ، وتُدرك

إيران جيداً قدرة الولايات المتحدة على الرد عليها، مما يجعلها أقرب إلى ممارسة ضبط النفس في هذا الخصوص. ومع ذلك، فإنه يمكن لإيران أن تضع رهاناتها بدلا من ذلك على احتمالية أن الولايات المتحدة قد تتجنب التورط في القيام بتدابير انتقامية نيابة عن حلفائها الخليجيين. إن الرد الأمريكي المتردد كثيراً على العدوان السيبراني في الخارج من شأنه أن يعطي طهران الوقت والمساحة لمواصلة المناورة والنجاح، مما يعيق قدرة الولايات المتحدة وحلفائها على الدفاع عن مصالحهم.

ويعمل عامل الردع في الأساس على إقناع الخصم بأن تكاليف القيام بأي هجوم سيفوق الفوائد المحتملة من ورائه. ولردع الهجمات السيبرانية الإيرانية، ستحتاج الولايات المتحدة وحلفاؤها في الشرق الأوسط إلى إدراك الحساسيات والأولويات السياسية لطهران جيداً لضمان أن يكون للردع والانتقام الذي تقوم به التأثير المنشود. ويُعتبر الخطر الأكبر على القوى الغربية أن يكون عند أعدائها أدنى شك حول استعدادها للانتقام أو دعم حلفائها ضد الاعتداءات السيبرانية لمن يقوم بذلك كائناً من كان. فإذا رأت إيران، على سبيل المثال، أن هجماتها السيبرانية ليس لها أي عواقب تُذكر، فإن تصعيدها للهجمات سيكون أمراً بدهياً. ومن الأمور الأساسية في مواجهة القدرة الإلكترونية لإيران أن يتم تكوين جبهة موحدة ضد البراعة المدمرة لإيران في مجال القدرة الإلكترونية، بما في ذلك الاستعداد المنهجي لفضح تلك الأعمال وتعريف الناس بمن قام بها. عدما تتوجه الجهات الفاعلة في جميع أنحاء العالم بوتيرة مثيرة للقلق إلى استغلال الفرص التي تتيحها العمليات الجيوسياسية في الفضاء الإلكتروني، فإن الفرص المتاحة لإظهار الجاهزية والردع ستكون محدودة للغاية.

***

ملحوظة: يعمل صندوق مارشال الألماني (جي إم إف) - الولايات المتحدة على تعزيز التعاون عبر الأطلسي وذلك للتعامل مع التحديات والفرص الإقليمية والوطنية والعالمية انطلاقاً من روح مشروع مارشال (خطة اقتصادية أُطلقت بمبادرة من وزير الخارجية الأميركي الأسبق جورج مارشال عام ١٩٤٧، من أجل مساعدة البلدان الأوروبية على

إعادة إعمار ما دمرته الحرب العالمية الثانية وبناء اقتصـــاداتها من جديد، وذلك عبر تقديم هبات عينية ونقدية بالإضافة إلى حزمة من القروض الطويلة الأمد).[1].

(1) الآراء الواردة تعبر عن كتابها، ولا تعبر بالضرورة عن وجهة نظر المعهد المصري للدراسات