حروب الفضاء الإلكتروني

كتبه فريق التحرير | 22 فبراير ,2015

في أبريل عام 2007، وقع هجوم غير مسبوق على شبكات الإنترنت لدولة إستونيا، وقد شمل الشبكات الخاصة بالبرلمان والبنوك والوزارات والصحف والإذاعات، وأدى إلى شلل في خدمات عامة متعددة لمدة ثلاثة أسابيع، وكان الهجوم قد وقع إبان بعض الخلافات مع روسيا؛ مما دفع بأصابع الاتهام تجاهها، وهي شكوك تأكدت عام 2009 حين صرح قسطنطين جولوسكوكوف، قيادي بمجموعة ناشي الشبابية التي يدعمها الكرملين في روسيا، بأنه المسؤول عن الهجوم.

مرة أخرى، وفي عام 2008، أثناء الحرب بين روسيا وجيورجيا، تعرضت مواقع إعلامية وحكومية جيورجية متعددة لهجمات من مخترقين مجهولين، واتضح أنهم روس بطبيعة الحال، ثم تبع ذلك عام 2010 الهجمات على وحدات الطرد المركزي لتخصيب اليورانيوم في مفاعل نتانز في إيران، والتي تمت باستخدام الفيروس الإلكتروني ستاكسنِت (Stuxnet)، واحد من أكثر الأسلحة الإلكترونية تعقيدًا، ليتبع ذلك في 2012 هجوم آخر على أجهزة الكومبيوتر بوزارة النفط الإيرانية، وشركة النفط الإيرانية القومية، باستخدام فيروس فليم (Flame)، والذي يفوق ستاكسنِت في تأثيره وتعقيده، كما أفادت شركة الأمن الروسية "كاسبِرسكي لابز"، ويُعَد بمثابة "مكنسة" إلكترونية تسرق وتمسح المعلومات.

كانت هذه أبرز الهجمات الإلكترونية الخارجية التي أصابت دولًا قومية، وهو ما دفع الكثير من

صناع القرار والمخططين الإستراتيجيين إلى الاهتمام بالحروب الإلكترونية بشكل لا يقل عن نظيرتها الكلاسيكية، البرية والبحرية والجوية، لاسيما وأن العديد من الدول اليوم، خاصة الصغيرة منها، أصبحت تعتمد على شبكات الإنترنت لترسيخ قوتها وتقديم العديد من الخدمات لمواطنيها.

الولايات المتحدة

تنقسم حروب الفضاء الإلكتروني طبقًا للمؤسسة العسكرية الأمريكية إلى قسمين رئيسيَّين: الدفاع الإلكتروني (Defensive Counter Cyber DCC)، والهجوم الإلكتروني (Offensive Counter Cyber OCC)، ويشمل الأول التعرّف على أي أنشطة إلكترونية عدوانية، وكشف هوية القائمين عليها، واعتراضها بنجاح، وتدميرها أو على الأقل وقف آثارها التخريبية، في حين تشمل الثانية كافة العمليات الرامية إلى تدمير، أو تعطيل، أو تحييد، الإمكانيات الإلكترونية الخاصة لأي بلد قبل أو بعد استخدامه ضد الولايات المتحدة أو أي من حلفائها، بالإضافة إلى جمع المعلومات من أي أجهزة كومبيوتر وأنظمة وشبكات معلوماتية، وتعديلها أو تعطيلها أو تدميرها.

بدأت الولايات المتحدة في الاهتمام بمجال حروب الفضاء الإلكتروني عام 1993، حين دشنت مركز الحروب المعلوماتية التابع للقوات الجوية، وكانت عمليات الدفاع والهجوم آنذاك تتم معًا تحت قيادة وحدة الحرب المعلوماتية رقم 609، ورغم ذلك، فإن دورها ظل مقتصرًا على التنسيق مع البنتاجون وتقديم الاقتراحات له، دون القدرة على شن هجمات أو حملات دفاع في المجال الإلكتروني.

لاحقًا، في عام 1998، أنشأ البنتاجون قوة دفاع شبكات الكومبيوتر المشتركة (JTF-CND) لتولي مسؤولية الهجوم والدفاع الإلكتروني، قبل أن يتم الفصل بينهما، لتؤول مهمة الهجوم إلى وكالة الأمن القومي، ومهمة الدفاع إلى وكالة الدفاع عن أنظمة المعلومات، واللتين اجتمعتا لاحقًا تحت مظلة القيادة الإلكترونية الأمريكية (USCYBERCOM)، عام 2009، والتي يقودها مدير وكالة الأمن القومي نظرًا لتمتّعها بإمكانيات كبيرة في مجال تكنولوجيا المعلومات والاتصالات، كما تدل على ذلك التسريبات الأخيرة بخصوص تجسس الوكالة على دول مختلفة حول العالم.

الورقة الإستراتيجية للأمن القومي الإلكتروني الصادرة عن البيت الأبيض في واشنطن عام 2003

الصين

تستثمر الصين بقوة في مجال الدفاع الإلكتروني، لاسيما وهو المجال الذي قد يعطيها تفوقًا على الولايات المتحدة وروسيا بالنظر لتفوقهما عليها في المجالات التقليدية، ولا تعتمد الصين فقط على جيشها النظامي والوحدات الخاصة بالدفاع الإلكتروني، مثل الوحدة 61398 الشهيرة في الجيش، ولكنها تقوم أيضًا بتنظيم كتائب معلوماتية، أو ما يُعرَف بـ "ميليشيات الإنترنت"، والتي تتكون من المدنيين الذين يعملون لصالح الدولة.

طبقًا للمحللين، تستهدف الصين دولًا عدة بهجماتها الإلكترونية حول العالم، وهي تهدف بالأساس لجمع أسرار اقتصادية وتجارية وصناعية تعطي شركاتها ومؤسساتها المزيد من التفوق، أكثر منها محاولات للاختراق والتجسس للحصول على معلومات سيادية أو سياسية تقليدية، وتُعرَف

الهجمات الإلكترونية الصينية بأنها شديدة الكفاءة رغم غياب التعقيد فيها.

تُعَد الصين الخطر الأبرز على الولايات المتحدة في مجال حروب الفضاء الإلكتروني، وهذا هو ما يعتقده الكثير من المسؤولين في البنتاجون، والصين بدورها ترى في واشنطن عدوًا إلكترونيًا لا يُستهان به، لاسيما وأن التشابك الاقتصادي والتجاري بينهما يعني أن الحرب التقليدية شبه مستحيلة نظرًا لآثارها المدمّرة على اقتصاد البلدين، في حين الحرب الإلكترونية ممكنة جدًا بالنظر للدمار الذي قد يوقعه طرف على آخر من خلالها، خاصة وأن معظم الشركات والبنوك والهيئات الحكومية والمؤسسات المالية وغيرها تعتمد على الفضاء الإلكتروني في كلٍ من الصين والولايات المتحدة.

يقوم الطرفان بحوار إلكتروني، حيث تم أول اجتماع لمجموعة عمل الفضاء الإلكتروني الأمريكية الصينية في يوليو 2013، وهي مجموعة علقت الصين مشاركتها فيها في 2014 نظرًا لاتهامات الولايات المتحدة لخمس صينيين بالتجسس الاقتصادي والسرقة الإلكترونية لأسرار تجارية العام الماضي، ولا يُعرَف بعد ما إذا كانت ستشارك هذا العام.

الرؤية الصينية للحروب الإلكترونية، في ورقة لـ "لي جانغ"، مدير معهد المعلومات في بكين، وأحد رعاة الحوار الأمريكي الصيني حول الأمن الإلكتروني

روسيا

تهتم روسيا بشدة بحروب الفضاء الإلكتروني، وهو أحد أولوياتها في البحوث العسكرية، خاصة وهي تواجه دولًا كبرى كالصين والاتحاد الأوروبي لا يمكنها أن تضاهيها على المستوى الاقتصادي والديمغرافي، ولا تملك حرية العمل العسكرية تجاهها كما تفعل في مجالها المحدود بشرق أوروبا وأسيا الوسطى، وهو ما يعني أن تطوير منظومة دفاعها الإلكترونية سيعطيها قدرة على الضغط على الاتحاد الأوروبي، حيث تعتمد كافة الدول على الإنترنت في معظم ما تقوم به من عمليات اقتصادية وتجارية.

رُغم ذلك، لم تُنشئ روسيا بعد قيادة واضحة داخل مؤسستها العسكرية لحروب الفضاء الإلكتروني كما فعلت الصين والولايات المتحدة، وهي تعتمد في ذلك ربما على مجموعات موالية لها، كما جرى أثناء هجوم 2007 على إستونيا، وتقوم بشراء المبرمجين ليعملوا لصالحها نظرًا لغياب البنية التحتية التكنولوجية الكفء التي قد توفر لها باستمرار ما تحتاجه من خبرة في هذا المجال، وهو توضحه طبيعة الهجمات التي يقوم به هؤلاء، إذ تتسم بالتعقيد، على العكس من الهجمات الصينية.

على غرار ما فعلت واشنطن وموسكو حيال المجال النووي في الحرب الباردة، قام الطرفان بتدشين خط ساخن بينهما عام 2013 لتفادي وقوع كارثة في الفضاء الإلكتروني.

الهند

تتمتع الهند ببنية تحتية تكنولوجية قوية ومعروفة، وقد تكون أبرز المرشحين للتفوق في مجال حروب الفضاء الإلكتروني، ومع ذلك فلاتزال وزارة الدفاع الهندية مترددة حيال تأسيس قيادة دفاع للفضاء

الإلكتروني، حيث لايزال الاقتراح بتأسيس قيادة إلكترونية من ثلاثة مستويات في انتظار تبنيه وتطبيقه منذ أكثر من عام.

بدأت الاقتراحات بتأسيس قيادة كهذه بعد أن قام مخترقون صينيون بالدخول على أجهزة الكمبيوتر الخاصة في مقر القيادة العسكرية الشرقية في مدينة فيشاكابَتنَم عام 2012، حيث كانت تجرى الغواصة النووية الهندية أريهانت تجارب بحرية، كما تكررت نفس الحادثة عام 2013 حين اخترق صينيون شبكات منظمة البحوث والتنمية التابعة لوزارة الدفاع.

بعد فتح تحقيق في هذه الهجمات، توصلت الهند إلى وقوع حوالي 12.000 هجوم صيني على وزارات ومؤسسات مختلفة، وعلى شبكات تخص قوات الشرطة الحدودية بين الهند والتبت؛ وهو ما دفع مسؤولين في وزارة الدفاع للاهتمام بمسألة الحروب الإلكترونية، وتقديم اقتراحات بشأنها.

من المنتظر أن تقوم حكومة رئيس الوزراء مودي باتخاذ خطوات قوية في هذا المجال، لاسيما وقد ركزت في برنامجها على المجال الإلكتروني في الاقتصاد والتجارة، على العكس من الحكومة السابقة، والتي اتُهِمَت كثيرًا بالتهاون في تعزيز قوة الهند العسكرية بوجه الصين، وبالتغاضي عن تنفيذ مقترح القيادة الإلكترونية الهندية.

أول ورقة هندية عن سياسة للأمن القومي الإلكتروني صادرة عن قسم تكنولوجيا المعلومات والإلكترونيات بوزارة الاتصالات والتكنولوجيا الهندية عام 2013

الورقة الإستراتيجية التي أصدرتها وكالة أمن الشبكات والمعلومات الفرنسية

الورقة الإستراتيجية للأمن الإلكتروني التي أصدرتها بريطانيا عام 2011

الأوراق الإستراتيجية الخاصة بدول الاتحاد الأوروبي

هذا المقال هو الأول ضمن ملف "مستقبل القوة" على نون بوست

رابط المقال : https://www.noonpost.com/5548/