Cyber Power:

تأثيرات "قوة الفضاء الإلكتروني" على التفاعلات الأمنية في العالم

إيهاب خليفة

منسق برنامج التطورات التكنولوجية بمركز المستقبل للأبحاث والدراسات المتقدمة- أبوظبي- الإمارات العربية المتحدة

ساهمت التطورات التكنولوجية في إضافة أدوات جديدة وقدرات غير تقليدية يمكن للدول استخدامها في إدارة العلاقات الدولية، فقد أضافت التطورات التكنولوجية أبعاداً جديدة لأدوات القوة التقليدية للدولة سواء كانت صلبة أو ناعمة، وهي قوة الفضاء الإلكتروني (Cyber Power) والتي يعرفها جوزيف ناي بأنها "القدرة على تحقيق الأهداف المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء الإلكتروني[1]".

وتستخدم العديد من الدول القدرات التي يتيحها الفضاء الإلكتروني لاعتبارات الأمن والقوة العسكرية بشكل جعلها تدخله ضمن حساباتها الاستراتيجية وأمنها القومي، وظهر بُعد جديد في الصراعات الدولية هو "صراع الفضاء الإلكتروني"، حيث يستطيع أحد أطراف الصراع أن يوقع خسائر فادحة بالطرف الآخر، وأن يتسبب في شل البنية المعلوماتية والاتصالاتية الخاصة به، وهو ما يسبب خسائر عسكرية واقتصادية فادحة، من خلال قطع أنظمة الاتصال بين الوحدات العسكرية وبعضها البعض، أو تضليل معلوماتها، أو سرقة معلومات سرية عنها، أو من خلال التلاعب بالبيانات الاقتصادية والمالية وتزييفها أو مسحها من أجهزة الحواسيب.

وبالرغم من فداحة الخسائر، فإن الأسلحة بسيطة لا تتعدى في أغلب الأحوال "الكيلو بايتس" التي تتمثل في فيروسات إلكترونية تخترق شبكة الحاسب الآلي، وتنتشر بسرعة بين الأجهزة، وتبدأ عملها في سرية تامة وبكفاءة عالية، وهي في ذلك لا تفرق بين المقاتل والمدني، وبين العام والخاص، وبين السري والمعلوم.

ويمكن تحديد الأنماط الرئيسية، القائمة أو المحتملة، للتطبيقات الأمنية لقوة الفضاء الإلكتروني كالتالي:

أولاً: نمط الهجوم في الفضاء الإلكتروني:

1- استهداف البنية التحتية المدنية المرتبطة بالفضاء الإلكتروني (Civil Cyber Infrastructure):

تتجه العديد من دول العالم إلى ميكنة أنظمتها الخدمية وبنيتها التحتية، بهدف توفير الوقت والجهد والتمويل، وبالرغم من المميزات التي تقدمها الميكنة الإلكترونية فإنها تجعل البنية التحتية عرضة للاختراق الإلكتروني. فحينما تتعرض البنية التحتية الحيوية (Critical Cyber Infrastructure) لهجمات إلكترونية، فإنّ احتمالات كارثية يمكن أن تحدث، فمثلاً اختراق نظام المواصلات كأنظمة ملاحة الطيران والسفن وأنظمة السكك الحديدية والعبث بها، قد يوقع آلاف الضحايا في دقائق معدودة، كذلك فإن استهداف بعض القطاعات الحيوية، مثل مصافي البترول ومصانع الكمياويات وأنظمة المستشفيات ومحطات توليد الكهرباء والمفاعلات النووية، قد تترتب عليه خسائر فادحة للدولة.

2- تهديد البنى التحتية العسكرية المرتبطة بالفضاء الإلكتروني (Military Cyber Infrastructure):

مثّل فيروس ستاكسنت على سبيل المثال، قفزة نوعية وكمية في القدرات المدمرة لحرب الفضاء الإلكتروني، فقد أعلنت الاستخبارات الإيرانية أن فيروس ستاكسنت أصاب ما يقدر بستة عشر ألف جهاز كمبيوتر نتيجة تعرضها لهذا الفيروس في

أكتوبر 2010[2]، وتسبب في تعطيل نحو 1000 من أجهزة الطرد المركزي في منشأة ناتانز لتخصيب اليورانيوم، ما تسبب في تعطيل البرنامج النووي الإيراني مرحلياً.

لم يقتصر الأمر على تهديد البنى التحتية المدنية فحسب، بل شمل أيضاً البنى التحتية العسكرية، وهنا يطرح البعض تصوراً مستقبلياً حول إمكانية قيام فيروسات الكمبيوتر بإصابة نظم الدفاع الجوي ونظم توجيه الصواريخ والطائرات بدون طيار، بل وإمكانية إخراج الأقمار الصناعية عن مداراتها أو السيطرة عليها.

3- سرقة المعلومات والبيانات العسكرية أو التلاعب بها (Cyber Espionage):

يتم في هذه الحالة اختراق الشبكات الخاصة بالمؤسسات الأمنية بهدف سرقة استراتيجيات عسكرية أو خرائط انتشار أنظمة تسليح، أو تصميمات لمعدات عسكرية، أو حتى قواعد بيانات عسكرية. وقد انطلقت واحدة من أخطر الهجمات ضد أنظمة حواسب الجيش الأمريكي في عام 2008، من خلال وحدة تخزين (USB) بسيطة متصلة بكمبيوتر محمول تابع للجيش في قاعدة عسكرية موجودة في الشرق الأوسط، ما شكل ما يشبه جسراً رقمياً، تم من خلاله نقل آلاف الملفات من البيانات إلى خوادم خارجية (Servers)، كما تم استهداف أكثر من 72 شركة من بينها 22 مكتباً حكومياً و13 من مقاولي وزارة الدفاع بهدف سرقة معلومات حول الخطط والمباني العسكرية[3].

وفي تقرير مقدم إلى الكونجرس الأمريكي سربت أجزاء منه إلى صحيفة الواشنطن بوست، ذُكر أن قراصنة صينيين يعملون لصالح الحكومة الصينية قاموا بسرقة معلومات عسكرية أمريكية حول منظومات مضادة للصواريخ من طراز "PAC–3" ونظام "THAAD"، بالإضافة إلى المعلومات حول الطائرات والسفن العسكرية، ما مكن الحكومة الصينية من استخدام هذه المعلومات لتطوير تقنياتها العسكرية وهو ما وفر عليها الكثير من الوقت والجهد والأموال لتطوير هذه الأسلحة[4].

وفي الوقت الذي أعلنت فيه الصين عن إنشاء وحدات حرب الفضاء الإلكتروني عام 2003 تعرضت الولايات المتحدة في العام ذاته لواحدة من أسوأ حلقات التجسس الإلكتروني، ويطلق عليها اسم "Titan Rain"[5]، وفيها تم سحب ما يتراوح بين 10 و20 تيرابايت من المعلومات من شبكة البنتاجون غير السرية[6]، كما قام قراصنة إلكترونيون صينيون بشن بضع هجمات على المواقع الإلكترونية لشركة "لوكهيد مارتين" الأمريكية وسرقوا معلومات عن تكنولوجيا تصنيع مقاتلة "أف– 35" التي استخدمتها الصين فيما بعد لدى تصميم وتصنيع مقاتلة "تي 20" الصينية. وقد أطلقت الاستخبارات الأمريكية على سلسلة من الهجمات التي شنها القراصنة الصينيون عام 2007 تسمية "الجحيم البيزنطي"، وكانت الهجمات الإلكترونية تستهدف المؤسسات الصناعية الحكومية الأمريكية[7].

4- اختراق أنظمة التحكم والسيطرة:

تكمن الميزة النسبية لقوة الفضاء الإلكتروني في قدرتها على ربط الوحدات العسكرية بعضها ببعض وبالأنظمة العسكرية، بما يسمح بسهولة تبادل المعلومات وتدفقها، وسرعة إعطاء الأوامر العسكرية، والقدرة على إصابة الأهداف وتدميرها عن بعد. وقد تتحول هذه الميزة إلى نقطة ضعف، إن لم تكن الشبكة الإلكترونية المستخدمة في ذلك مؤمنة جيداً، منعاً للتلاعب بالأنظمة العسكرية، أو إعادة توجيه أسلحة الخصم ضد أهداف وهمية أو صديقة.

وعلى سبيل المثال، استطاعت قوات الدفاع الجوي الإيرانية السيطرة إلكترونياً على طائرة بدون طيار أمريكية من طراز "RQ–170"، في ديسمبر 2011 وإرغامها على النزول في حالة شبه سليمة[8]، وذلك من خلال اختراق إلكتروني للطائرة دون التسبب في تدميرها من خلال إطلاق النار، وقد أكد الجنرال أمير علي حجي زادة، قائد القوات الجوية والفضائية في الحرس الثوري الإيراني، في أبريل 2012، أن طهران نجحت في اختراق أسرار طائرة الاستطلاع بدون طيار الأمريكية[9].

5- الحرب النفسية الإلكترونية (Cyber Psychological Warfare):

يقصد بها استخدام وسائل الإعلام الحديثة وخدمات الإنترنت في بث رسائل وأفكار وتوجهات معينة، بهدف التأثير على الجماهير والجيوش وصناع القرار، ومن أبرز الأمثلة التي تم فيها استخدام أساليب تكنولوجية لممارسة الحرب النفسية قيام القوات الأمريكية إبان حرب الخليج الثانية 2003، باختراق الشبكة العسكرية ذات الدوائر المغلقة الخاصة بالجيش العراقي، وأرسلت رسائل من القيادة الأمريكية الوسطى إلى الضباط والجنود العراقيين عبر البريد الإلكتروني تعلن فيها غزو العراق في المستقبل القريب، وتؤكد أن الهدف هو إزاحة الرئيس العراقي صدام حسين وابنيه دون إصابة الجنود العراقيين، وطالبت القادة بأن يضعوا المدرعات والدبابات التي تحت إمرتهم في صورة تشكيل ثم يتركونها ويذهبون إلى بيوتهم، مما يسهل على القوات الأمريكية إصابة الأهداف، وقد وجدت القوات الأمريكية عند ضرب العراق بعض الوحدات، وقد اصطفت ودباباتها بانتظام أمام قواعدها، مما سمح للطائرات الأمريكية بقصفها قصفاً محكماً [10].

وفي عام 2011، أعلنت وكالة مشروعات البحوث الدفاعية المتطورة (DARPA) عام 2011 عن برنامج لاستخدام مواقع التواصل الاجتماعي في تحقيق التواصل الاستراتيجي من خلال تحسين فهم وزارة الدفاع لما يجري على مواقع التواصل الاجتماعي في الوقت الحقيقي له (Real Time)، خاصة في المناطق التي تنتشر فيها قوات أمريكية، فضلاً عن قيام وزارة الدفاع الأمريكية باستخدام مواقع التواصل في بث رسائل إعلامية

تخدم مصالحها الاستراتيجية[11].

6- استخبارات الفضاء الإلكتروني (Cyber Intelligence):

ساهمت الثورة التي أحدثتها التكنولوجيا في تطوير أدوات التجسس، فأصبح بالإمكان التجسس على ملايين الأفراد في نفس الوقت، وتسجيل مكالماتهم الهاتفية، وصورهم الشخصية، ومراسلاتهم البريدية، بل وتصوير حياتهم الشخصية لحظة بلحظة، ويزداد الأمر خطورة في حال كان الهدف أحد صناع القرار في الدولة، وهو ما حدث عندما قامت الولايات المتحدة بالتجسس على محادثات هاتفية لـ 35 من زعماء العالم[12]، فقد شهدت العلاقات بين الولايات المتحدة الأمريكية وألمانيا أزمة دبلوماسية على خلفية قيام وكالة الأمن القومي الأمريكي بالتجسس على هاتف إنجيلا ميركيل[13]، وبالمثل استدعي وزير الخارجية الفرنسي لوران فابيوس السفير الأمريكي في باريس لمناقشة تقرير نشرته صحيفة فرنسية يفيد بأن الولايات المتحدة تجسست على ملايين المكالمات الهاتفية الخاصة بالمواطنين في فرنسا[14].

ثانياً: نمط الدفاع الإلكتروني:

1- تعظيم معايير الأمان بالشبكات الحيوية:

هناك معركة مشتعلة دائماً بين صنّاع الفيروسات من جهة وشركات البرمجيات من جهة أخرى، فحينما ظهرت فيروسات الكمبيوتر واتضحت خطورتها، وبدأت شركات البرمجة في إنتاج برامج مضادة لها، تعمل على إزالتها ووقف نشاطها، وهو ما استثار صانعي الفيروسات، فقاموا بإنتاج فيروسات أكثر ضراوة وأخطر انتشاراً، إلى الحد الذي أصبح الفيروس قادراً ليس فقط على تدمير برنامج التشغيل، بل على إصابة المكون المادي للأجهزة الإلكترونية وإصابتها بالشلل. كما أن تطوير أساليب وأنظمة أمن المعلومات يكون غالباً كرد فعل على هجمات إلكترونية ناجحة، ومن ثم تظهر الثغرات التي تمت منها عملية الاختراق، وتبدأ مرحلة تأمينها، ولذلك كان من الضروري على الدول فصل شبكاتها الحرجة عن الإنترنت، ووضع نظام صارم لنقل البيانات والمعلومات خلالها، والتأكد من ولاء العناصر البشرية التي تعمل عليها، والقيام بأساليب محاكاة لشن هجمات إلكترونية لمعرفة مواطن الضعف وتلافيها.

2- إنشاء أحلاف عسكرية إلكترونية (Cyber Alliance):

أطلق حلف الناتو بقيادة الولايات المتحدة الأمريكية عام 2002 دعوة لتحسين قدراته الدفاعية ضد هجمات الفضاء الإلكتروني، وركز الحلف في السنوات التالية بشكل أساسي على تنفيذ تدابير الحماية السلمية المطلوبة للجانب العسكري، حيث دفعت هجمات الفضاء الإلكتروني– التي وقعت في إستونيا عام 2007– الحلف لإعادة التفكير في حاجته لسياسة دفاع إلكتروني، ومن ثم وضع الحلف للمرة الأولى في تاريخه سياسة رسمية "للدفاع الإلكتروني" تم اعتمادها في يناير عام 2008، لتضع ثلاث دعائم أساسية: أولها التضامن: بمعنى تقديم المساعدة عند الطلب، وخلاف ذلك يتم احترام مبدأ سيادة الدولة، وثانيها عدم التكرار: بمعنى تفادي الازدواجية غير الضرورية في الهياكل والقدرات على المستوى الدولي والإقليمي والوطني، وثالثها التأمين: من خلال التعاون القائم على الثقة مع الأخذ في الاعتبار حساسية المعلومات ذات الصلة التي لابد أن تكون متاحة، وأماكن الانكشاف الممكنة التي يمكن أن تتعرض للاختراق بصورة أسهل[15].

ثالثاً: صعوبة الردع الإلكتروني:

إن هدف الردع هو إيجاد مجموعة من المحفزات المانعة لقيام أحد أطراف الصراع باعتداء أو هجوم مستقبلاً، وإذا كان ذلك هو هدف الردع في التفاعلات الدولية على أرض الواقع، فإنه مختلف جزئياً في حالة الردع في الفضاء الإلكتروني، لأن أحد الفاعلين غير قادر على إزالة أو تدمير الطرف الآخر كلياً، كما في حالة الردع النووي مثلاً، كما أنه ليس من السهولة تحقيق الردع في الفضاء الإلكتروني، بسبب خاصية التخفي، والتي تجعل من الصعوبة على متخصصي الأمن الإلكتروني أن يتعرفوا على خصومهم أو أن يتوقعوا من أين سوف تأتيهم الهجمة الإلكترونية القادمة، وهو ما يطرح سؤالاً حول إمكانية أن تقوم الهجمات الإلكترونية بتهديد السلم والأمن العالمي؟[16].

ولتحقيق الردع الإلكتروني يجب أن تعمل الدول على زيادة قدراتها الدفاعية من خلال حائط صد للهجمات الإلكترونية، ووضع أجهزة استشعار (Sensors) على بنيتها التحتية للكشف المبكر عن الأخطار الإلكترونية، وتطوير قدراتها في مجال التتبع العكسي للهجمات الإلكترونية لمعرفة مكان إطلاقها.

خلاصة:

أدخلت التطورات التكنولوجية العديد من المفاهيم السياسية والعسكرية غير التقليدية، مثل حرب الفضاء الإلكتروني، والبنية التحتية للفضاء الإلكتروني، وتجسس الفضاء الإلكتروني، وغيرها من المفاهيم المرتبطة بالأمن القومي للدول. ومكنت هذه التطورات الفاعلين الدوليين من غير الدول سواء كانوا أفراداً هواة أو جيوشاً نظامية أن تخترق الأجهزة العسكرية والأمنية وتسيطر عليها وتعبث بمحتوياتها، وباتت الدول التي أنتجت هذه التكنولوجيا هي الأكثر تعرضاً للتهديدات الإلكترونية، فضلاً عن صعوبة التزامها بمتطلبات الحفاظ على أمنها القومي الناجم عن التطورات التكنولوجية.

ونتيجة للتطور التكنولوجي أصبحت الدول في حاجه إلى استراتيجيات جديدة لإدارة أمن الفضاء الإلكتروني، تنطلق من مبدأ رئيسي هو القابلية للاختراق (Vulnerability)، ومن خلال تتبع بعض النماذج السابقة نجد أن القوة الإلكترونية أصبحت تستخدم إلى جانب القوة العسكرية، فالفضاء الإلكتروني مجال

عام لا يعترف بالحدود، وفي حالة حدوث حرب إلكترونية، فإن احتمالية وجود خسائر قائمة، حتى لو لم تكن الدولة مشتركة في هذه الحرب.

ويجب أن تعمل الاستراتيجيات الجديدة على محوري الدفاع والهجوم بهدف تحقيق الردع الإلكتروني، وذلك من خلال تعظيم معايير الأمان لشبكة الإنترنت الداخلية، وكشف أماكن الاختراق والتعرف على مصادرها والتعامل الفوري معها، فضلاً عن تطوير قدرات هجومية إلكترونية، فقد ظهر جلياً أن القوة الإلكترونية حققت الكثير من الأهداف العسكرية والأمنية، مما يجعلها سلاحاً إضافياً إلى جانب القوى التقليدية.

---

1) Joseph S. Nye, **Cyber Power**, (Cambridge, Harvard Kennedy School, May 2010). p4.

2) "Iran says Stuxnet virus infected 16,000 computers", (Fox news, February 18, 2012), http://www.foxnews.com/world/2012/02/18/iran–says–stuxnet–virus–infected–16000–computers/

3) اولاف تايلر، "التهديدات الجديدة: الأبعاد الإلكترونية"، (**مجلة حلف الناتو**، سبتمبر 2011)، يمكن المطالعة على الرابط التالي

http://www.nato.int/docu/review/2011/11–september/Cyber–Threads/AR/index.htm

4) Ellen Nakashima, Confidential Report Lists U.S. Weapons System Designs Compromised By Chinese Cyberspies, (**Washington Post**, 27 May, 2013)

http://www.washingtonpost.com/world/national–security/confidential–report–lists–us–weapons–system–designs–compromised–by–chinese–cyberspies/2013/05/27/a42c3e1c–c2dd–11e2–8c3b–0b5e9247e8ca_story.html

5) James A.Lewis, "Computer Espionage, Titan Rain and China", (**CSIS**, Cyber security Program, Dec. 14, 2005) http://csis.org/files/media/csis/pubs/051214_china_titan_rain.pdf

6) ريتشارد كلارك وروبرت نيك، **حرب الفضاء الإلكتروني: التهديد التالي للأمن القومي وكيفية التعامل معه**، (أبوظبي: مركز الإمارات للدراسات والبحوث الاستراتيجية، 2012)، ص ص 69–71.

7) "أمريكا تتهم الصين بسرقة تكنولوجيا صنع مقاتلة أف – 35"، (**موقع روسيا اليوم**، 14 مارس 2014)

/http://arabic.rt.com/news/668023

8) "إيران تسقط طائرة استطلاع امريكية بدون طيار"، (**موقع روسيا اليوم**، 4 ديسمبر 2011)، على الرابط التالي:

/http://arabic.rt.com/news/573311

9) "إيران تؤكد اختراق أسرار الطائرة الاميركية (آر كيو– 170)، (**موقع إيلاف الإخباري**، 22 أبريل 2012)

http://www.elaph.com/Web/news/2012/4/731015.html#sthash.eQfwfoLU.dpuf

10) ريتشارد كلارك وروبرت نيك، **مرجع سبق ذكره**، ص ص 22–24

11) "Pentagon Seeks to Manipulate Social Media for Propaganda Purposes", (Global Research, 21 July 2011), http://www.globalresearch.ca/pentagon–seeks–to–manipulate–social–media–for–propaganda–purposes/25719

12) –NSA monitored calls of 35 world leaders after US official handed over contacts, On April 18, 2014

http://www.theguardian.com/world/2013/oct/24/nsa–surveillance–world–leaders–calls

13) – تقرير: الولايات المتحدة تجسست على هاتف ميركل منذ 2002، خبر منشور على موقع **بي بي سي**، 26 أكتوبر 2013، يمكن المطالعة على:

http://www.bbc.co.uk/arabic/worldnews/2013/10/131026_us_bugged_merkel.shtml

14) – فرنسا تستدعي السفير الأمريكي في باريس لمناقشة تهم بالتجسس على ملايين الفرنسيين، خبر منشور على موقع بي بي سي 21 أكتوبر 2013، يمكن المطالعة على:

http://www.bbc.co.uk/arabic/worldnews/2013/10/131021_france_us_spying_crisis.shtml

15) د. اولاف تايلر، **مرجع سبق ذكره**

16) Martin C. Libicki, **Cyber deterrence and Cyber war**, (Santa Monica: RAND, 2009), P 28–31