المعهد المصري للدراسات
EGYPTIAN INSTITUTE FOR STUDIES

المجال الخامس
الفضاء الإلكتروني

عمر حامد شكر

دراسات استراتيجية

٢٨ يونيو ٢٠١٩

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

المجال الخامس ـ الفضاء الإلكتروني

د. عمر حامد شكر

لم تعد المجالات الأربعة التي عرفت في المواجهة المسلحة التقليدية بين الدول (البر والبحر والجو والفضاء) وحدها على الساحة الدولية بل دخل مجال خامس لهذه المواجهة وهو (الفضاء الإلكتروني)، حيث من المتوقع أن تكون الحرب الإلكترونية (Cyber War) السمة الغالبة إن لم تكن الرئيسية للحروب المستقبلية في القرن الواحد والعشرين.

وتكمن خطورة حروب الإنترنت والشبكات في كون العالم أصبح يعتمد أكثر فأكثر على الفضاء الإلكتروني (Cyberspace)، لا سيما في البنى التحتية المعلوماتية العسكرية والمصرفية والحكومية إضافة إلى المؤسسات والشركات العامة والخاصة. ولا شك أنّ ازدياد الهجمات الإلكترونية والتي نشهد جزءًا بسيطا منها اليوم يرتبط أيضًا بازدياد هذا الاعتماد على شبكات الكمبيوتر والإنترنت في البنية التحتية الوطنية الأساسية، وهو ما يعني إمكانية تطوّر الهجمات الإلكترونية اليوم لتصبح سلاحًا حاسمًا في النزاعات بين الدول في المستقبل، علمًا أنّ أبعاد مفهوم الحرب الإلكترونية لا تزال غير مفهومة لدى شريحة واسعة من المراقبين وحتى العامة [1].

وليس هناك من إجماع واسع على تعريف محدد ودقيق لمفهوم الحرب الإلكترونية الآن، حيث تعرف وزارة الدفاع الأمريكية الحرب الإلكترونية بأنها "استخدام أجهزة الكمبيوتر والإنترنت لإجراء الحرب في الفضاء الإلكتروني"[2].

وقد اجتهد عدد من الخبراء من ضمن اختصاصاتهم في تقديم تعريف يحيط بهذا المفهوم، فعرّف كل من (ريتشارد كلارك وروبرت كناكي) الحرب الإلكترونية على أنها "أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها"[3].

ومن المتوقع أن تصبح الحرب الإلكترونية نموذجًا تسعى إليه العديد من الجهات نظرًا للخصائص العديدة التي تنطوي عليها، ومنها:

---

(1) علي حسين باكير، المجال الخامس. الحروب الإلكترونية في القرن الـ 21، مركز الجزيرة للدراسات، 12 يناير، 2011، آخر زيارة في 2016/7/3

(2) Alex Michael, "Cyber Probing: The Politicisation of Virtual Attack", Defence Academy of the United Kingdom, September 2010, p. 1.

(3) للمزيد حول الحرب الإلكترونية انظر كتاب:

Cyber War, "The Next Threat to National Security and What to Do About It", by Richard A. Clarke and Robert Knake, Harpercollins e-books, New York, 2010.

1- إن حروب الإنترنت هي حروب لا تناظرية (Asymmetric): حيث إن التكلفة المتدنية نسبيًا للأدوات اللازمة لشن هكذا حروب يعني أنّه ليس هناك حاجة لدولة ما مثلا أن تقوم بتصنيع أسلحة مكلفة جدًا مثل حاملات الطائرات والمقاتلات المتطورة لتفرض تهديدًا خطيرًا وحقيقيًا على دولة مثل الولايات المتّحدة الأمريكية على سبيل المثال[4].

2- تمتّع المهاجم بأفضلية واضحة: في حروب الإنترنت يتمتع المهاجم بأفضلية واضحة وكبيرة عن المدافع، فهذه الحروب تتميز بالسرعة والمرونة والمراوغة. وفي بيئة مماثلة يتمتّع بها المهاجم بأفضليّة.

3- فشل نماذج "الردع" المعروفة حيث يعد مفهوم الردع الذي تمّ تطبيقه بشكل أساسي في الحرب الباردة غير ذي جدوى في حروب الإنترنت. فالردع بالانتقام أو العقاب لا ينطبق على هذه الحروب. فعلى عكس الحروب التقليدية حيث ينطلق الصاروخ من أماكن يتم رصدها والرد عليها، فإنه من الصعوبة بمكان بل ومن المستحيل في كثير من الأحيان تحديد الهجمات الإلكترونية ذات الزخم العالي. بعض الحالات قد تتطلّب أشهرًا لرصدها وهو ما يلغي مفعول الردع بالانتقام وكثير من الحالات لا يمكن تتبع مصدرها، وحتى إذا تم تتبع مصدرها وتبين أنها تعود إلى فاعلين غير حكوميين، فإنه في هذه الحالة لن يكون لديهم أصول أو قواعد حتى يتم الرد عليها.

4- المخاطر تتعدى استهداف المواقع العسكرية: لا ينحصر إطار حروب الإنترنت باستهداف المواقع العسكرية، فهناك جهود متزايدة لاستهداف البنى التحتية المدنية والحسّاسة في البلدان المستهدفة، وهو أمر أصبح واقعيًا في ظل القدرة على استهداف شبكات الكهرباء والطاقة وشبكات النقل والنظام المالي والمنشآت الحساسة النفطية أو المائية أو الصناعية بواسطة فيروس يمكنه إحداث أضرار مادّية حقيقية تؤدي إلى انفجارات أو دمار هائل.

ومن المعروف أن هذا النوع من الحروب يعتبر حديثا في العلوم العسكرية، فإنه لا يستخدم أسلحة الحرب التقليدية المعروفة بشكل مباشر، بل تكمن أهميته في قيمة المعلومات التي تأتي عن طريقه، والتي تعتبر العين التي ترى وتوجه الأسلحة في ساحة المعركة.

تطوير المجال الإلكتروني:

قامت العديد من الدول بتطوير قدراتها الهجومية والدفاعية في مجال الحرب الإلكترونية، وعلى رأس هذه الدول هي الولايات المتحدة الأمريكية والصين وروسيا.

(4) William J. Lynn III, Defending a New Domain: The Pentagon's Cyber Strategy, Foreign Affairs, September-October 2010, p. 98.

[1] الولايات المتحدة الأمريكية:

على الرغم من أنّها تبقى الدولة الأكثر امتلاكاً للقدرات والتقنيات الهجومية العالية المطلوبة في الحروب الإلكترونية، إلا أنّه من الواضح أنّ اهتمامها انصب مؤخراً على تعزيز القدرات الدفاعية في هذا المجال. ونظراً لأنها الدولة الأكثر اعتماداً في العالم على الإنترنت وعلى الشبكات في مختلف القطاعات المدنية والعسكرية تبدو الأكثر اهتماماً بالجانب الدفاعي فيما يتعلق بالحروب الإلكترونية مقارنة بالدول الأخرى.

ويمكن الإشارة إلى واقعة حدثت في عام 1983 ويعتبرها نقطة فاصلة في تطور ترسانة الولايات المتحدة للحرب الإلكترونية التي استخدمتها بشكل فاعل في حرب الخليج عام 1991 ثم في صربيا في أواسط التسعينيات وقبل ذلك ضد الاتحاد السوفيتي السابق في سنين الحرب الباردة[5].

وتتلخص الحادثة في أن الرئيس الأميركي الراحل رونالد ريجان كان يشاهد فيلم الخيال العلمي "ألعاب الحرب" عام 1983، واستعرض الفيلم قصة فتى يخترق منظومة أحد المؤسسات العسكرية الأمنية بدون أن يعلم، وكاد الفتى أن يشعل حرباً عالمية ثالثة بدون أن يدري، الأمر الذي أقلق ريجان؛ حيث استدعى ريجان في الأيام التالية كبار مساعديه وجنرالات الجيش، وسألهم بشكل مباشر "هل يمكن أن يحدث ذلك فعلا؟" في إشارة إلى قصة الفتى في فيلم "ألعاب الحرب". وبعد أيام جاء الجواب مباشراً وصاعقاً لريجان حيث قيل له "إن الأمر أخطر من ذلك بكثير". وعليه نتج عن النقاش بين ريجان وكبار مسؤولي الأمن والجيش زوبعة من ورش العمل والدراسات والتحقيقات انبثقت عنها مذكرة الأمن القومي رقم 145 في 17 سبتمبر/أيلول عام 1984 وحملت عنوان "السياسة القومية لأمن الاتصالات وأنظمة المعلومات الأوتوماتيكية".

وتجدر الإشارة إلى أنه في ذلك الوقت كانت الحواسيب المحمولة محدودة الانتشار للغاية، وخدمة الإنترنت لم تكن متاحة للجمهور بعد، إلا أن ذكرت المذكرة تحديداً مخاطر استخدام أجهزة الحاسوب وإمكانية اختراقها وسرقة المعلومات منها من قبل أجهزة استخبارات منافسة أو منظمات "إرهابية".

ويرى الكاتب (فريدمان كابلان) صاحب كتاب (المنطقة الخفية)، أن هذه الوثيقة هي بذرة لما بات يعرف فيما بعد باسم "الحرب الإلكترونية"، والتي كانت نقطة تحول في طبيعة مهام وكالة الأمن القومي التي ومنذ تأسيسها تركزت

---

[5] للمزيد انظر: كتاب (فريد كابلان) حول التاريخ السري للحرب الإلكترونية في نشوء وتطور البنية التحتية لهذا النوع من الحروب والجانب الخفي لاستخداماتها.

Fred kaplan,"Dark Territory: The Secret History Of Cyber War", simon and schuster publishing, New York,2016.

مهامها على اعتراض الاتصالات التي تقوم بها الدول والمنظمات غير الأميركية، إلا أن المذكرة رقم 145 أضافت لعمل الوكالة مهمة تأمين الأنظمة الإلكترونية الأميركية.

وقد أثارت المهمة الجديدة للوكالة اعتراضات داخل الأجهزة التشريعية الأميركية، حيث إن الوكالة كانت تعمل بعيداً عن الأميركيين وغير مسموح لها التجسس عليهم أو اعتراض اتصالاتهم، وأراد دعاة الحريات المدنية التركيز على أن الخط الفاصل بين عدم التجسس على الأميركيين وتأمين منظوماتهم الإلكترونية هو خط واضح للوكالة.

وأثيرت القضية بعد ذلك في عهد الرئيس الأسبق بيل كلينتون، إلا أنها لم تحتل حيزاً كبيراً حتى جاءت هجمات سبتمبر/أيلول عام 2001 والحرب الأميركية على أفغانستان ثم العراق. حيث كانت الولايات المتحدة منغمسة في حروب تقليدية تستخدم فيها كافة أنواع الأسلحة وكان الجنود الأميركيون يسقطون قتلى كل يوم.

وفي خضم تلك الظروف، كانت الحرب الإلكترونية في ذيل اهتمامات الأميركيين، ولكنها في الوقت ذاته كانت على رأس أولويات إدارة الرئيس الأميركي السابق جورج بوش الابن، حيث كان العمل على هذا النوع من الحروب يجري على قدم وساق خلف أبواب مغلقة، ودأبت المؤسسة العسكرية الأميركية على وضعه في خدمة أهداف المعارك التقليدية على الأرض.

إلا أن هذا السيناريو لم تنفرد به الولايات المتحدة، ولم يكن من الممكن أن تحتكره لنفسها، فمع انتشار الإنترنت في العالم، أصبح سيناريو تكامل الحرب الإلكترونية مع الحرب التقليدية معمولاً به في دول حول العالم، بعض منها تصنف ضمن أصدقاء الولايات المتحدة.

بدأت النقلة الكبرى في عالم الحرب الإلكترونية في عهد الرئيس الأمريكي باراك أوباما، حيث تضاعفت الميزانية المرصودة ثلاث مرات تقريباً، من 2.7 مليار دولار إلى سبعة مليارات دولار، واستحدث وزير الدفاع الأميركي السابق (روبرت غيتس) وحدة متخصصة مكرسة لقيادة الحرب الإلكترونية.

أما العاملون من قبل الجيش الأميركي في هذا المجال فقد تضاعف عددهم أيضًا من 900 إلى أربعة آلاف شخص، ومن المتوقع أن يصل عددهم إلى ستة عشر ألفا في السنوات القادمة. ومرة أخرى، ولا يقتصر هذا التوسع على الولايات المتحدة، فقد وصل عدد الدول التي حذت حذوها إلى عشرين دولة.

وفي مايو/أيار 2009، وافق الرئيس السابق بارك أوباما على توصيات لمراجعة سياسة الفضاء الافتراضي، ووجهت السلطة التنفيذية العمل بشكل وثيق مع جميع اللاعبين الرئيسيين في مجال الأمن السيبراني، بما في ذلك حكومات الولايات والحكومات المحلية والقطاع الخاص، وذلك لضمان استجابة منظمة وموحدة للحوادث السيبرانية في

المستقبل، وتعزيز الشراكات العامة والخاصة لإيجاد الحلول التقنية التي تضمن أمن الولايات المتحدة والازدهار. كذلك الاستثمار في الأبحاث المتطورة والتنمية اللازمة للابتكار والاكتشاف لمواجهة التحديات الرقمية. والبدء بحملة لتعزيز الوعي بالأمن السيبراني ومحو الأمية الرقمية[6].

وفي 26 نيسان/أبريل 2010، كشفت وكالة الاستخبارات المركزية الأمريكية (CIA) عن مبادرة جديدة لمحاربة الهجمات الإلكترونية[7]، ووضعت من خلالها العناوين العريضة للخطة المناسبة لخمس سنوات قادمة.

كما قامت الولايات المتّحدة في مايو/أيار 2010 بإنشاء قيادة الإنترنت "سايبر كوم" وعيّنت مدير وكالة الاستخبارات القوميّة الجنرال (كيث أليكساندر) قائدًا عليها، مهمته الحرص على حماية الشبكات العسكرية الأمريكية على الدوام [8]. وقد بدأت هذه القيادة العمل فعلاً في الأول من تشرين الأول/أكتوبر 2011 بعد أن كان قد تمّ الإعلان عن ضرورة إنشائها في العام 2009، وهي تضم 1000 فرد من نخبة القراصنة والجواسيس الإلكترونيين المحترفين والمميزين يعملون تحت إمرة الجنرال أليكسندر، وتشير التقديرات إلى أنّ الولايات المتّحدة بحاجة إلى قوة قوامها حوالي 20 ألفا إلى 30 ألف فرد بنفس المميزات والصفات حتى تضمن تنفيذ المهام الدفاعية الإلكترونية على أكمل وجه في حماية الولايات المتّحدة بأسرها.

وقد قامت وزارة الدفاع الأمريكية (البنتاجون) بتصنيف الإنترنت على أنه الميدان الرابع من ميادين الحروب بعد الجو والبحر والبر. حيث تقوم الولايات المتحدة الأمريكية بإجراء مناورة سنوية تحت اسم (سايبر ستورم) لاختبار جاهزيتها لمواجهة أي هجمات إلكترونية معادية ويشارك بها 112 جهازا أمنيا أمريكيا.

وهكذا برزت الحرب الإلكترونية كعامل قوة وضعف في وقت واحد، حيث إنها أداة تجسس وسلاح حرب في وقت واحد، وعامل ضغط يمكن للولايات المتحدة أن تستخدمه ضد أعدائها، ويمكن لأعدائها أن يستخدموه ضدها في الوقت ذاته.

[2] الصين:

تعتبر من أكثر الدول التي تعمل على تطوير قدراتها الهجومية في المجال الإلكتروني، وهي واحدة من الدول القليلة التي تدمج فعلاً مفهوم "الثورة في الشؤون العسكرية" (RMA) في صلب العقيدة العسكرية، وخاصة في مجال الحرب

(6) The Comprehensive National Cybersecurity Initiative.

(7) CIA Director Leon E. Panetta Unveils Blueprint for Agency's Future, April 26, 2010. link

(8) War in the fifth domain: Are the mouse and keyboard the new weapons of conflict, The Economist, July 1st 2010. link آخر زيارة في 2016/7/3

الإلكترونية. وتؤكد الورقة الصينية البيضاء حول السياسة الدفاعية الصينية للعام 2006 [9]، أنّ الهدف الرئيس من بناء جيش حديث، هو جعله قادرًا على الفوز في حروب المعلوماتية بحلول منتصف القرن الواحد والعشرين. وهو الأمر الذي أعادت تأكيده ورقة عام 2009. وقد قامت الصين بتخصيص قسمًا عسكريًا كاملاً لعمليات التجسس الإلكتروني.

ولأن الصين ليست على المستوى العسكري لأمريكا وروسيا، فهي تحاول على الأرجح استغلال البُعد الإلكتروني لتطوير قدراتها "اللاتناظرية" لتحقيق تفوق في هذا المجال وبالتالي ضمان قدرات ردعيّة تتيح لها توفير الوقت اللازم لبناء قدراتها التقليدية من جهة، وتتيح لها أيضًا اكتشاف نقاط ضعف خصومها في المجال الإلكتروني للتركيز عليها[10].

وقد جاء في "الاستراتيجية العسكرية الصينية" لعام 2012 والتي كان من أهم محاورها وضع الخطوط العريضة لاستراتيجية الأمن الإلكتروني وتعزيز موقع "موقف الدفاع النشط"، وذلك من خلال العمل على تحقيق بعض الأهداف الاستراتيجية: العمل على بناء جيش قوي، وتنفيذ المبدأ الاستراتيجي العسكري للدفاع النشط، والعمل على تسريع عملية تحديث الدفاع الوطني والقوات المسلحة، والعمل على الدفاع بحزم عن السيادة والأمن والتنمية. ومن بين الأدوات التي عكفت الصين على تطويرها في المجال الإلكتروني إنشاؤها طائرة جاسوسية أطلقت عليها اسم CSA-003 وهي مخصصة للدفاع عن نشاطها السيبراني الإلكتروني، حيث إن إحدى وظائف الطائرة جمع معلومات استخباراتية حول النشاط الإلكتروني للخصم وكذلك الكشف عن أنظمتها الإلكترونية [11].

وتتميز هذه الطائرة التي صممتها الشركة الصينية لإنتاج أجهزة إلكترونية للطائرات (China Electronic Technology Corporation's Avionis)، بوجود أجهزة (مكشفات) استشعار فيها ما يمكنها من تسجيل المؤشرات الإلكترونية التي ترسلها معدات عسكرية أو رادارات أو أي أجهزة إلكترونية أخرى يستخدمها العدو.

كما تزود طائرة الجاسوسية بمنظومة استشعار كهرضوئي تعمل بالأشعة تحت الحمراء وغيرها ما يسمح لها بتسجيل نشاط قوات العدو الإلكترونية في أي ظروف جوية.

كما من الممكن للطائرة أن يعتمد عملها على إشارات لأقمار الصناعية ومحطات الاتصالات الأرضية.

---

(9) للمزيد حول وثيقة الورقة الصينية البيضاء لعام 2006 انظر تفاصيل الوثيقة:

China's National Defense in 2006 link

(10) علي حسين باكير، المجال الخامس.. الحروب الإلكترونية في القرن الـ 21، مرجع سابق.

(11) Jeffrey Lin and P.W. Singer," Meet China's new spy plane (with an Austrian body), March 14, 2016. link آخر زيارة في 2016/6/23

إن المنافسة الأمريكية-الصينية قد ترتقي إلى مرحلة "حرب إلكترونية باردة"، وهو ما يعني دخول البلدين في مرحلة سباق تسلح سيبراني جديد قد يؤدي في النهاية إلى تعاظم الخسائر والأضرار التي قد تلحق بالبلدين. ويزيد من احتمالات نشوب هذه الحرب البادرة الانقسام الأيديولوجي بين الغرب والصين، فيما يتعلق بمسألة حق الوصول إلى المعلومات إلكترونيًّا. والحكومة الصينية تعتقد أن لديها الحق في التحكم في وصول مواطنيها إلى شبكة الإنترنت، وترى أن الجهود الغربية للسماح للمواطنين الصينيين بالالتفاف حول هذه الضوابط، تُعتبر انتهاكًا للأمن السيبراني الوطني الصيني.

وقد وصف الرئيس الأمريكي باراك أوباما في سبتمبر 2015، الهجمات الإلكترونية الصينية المزعومة بأنها "غير مقبولة" وذلك قبيل زيارة الرئيس الصيني شي جين بينغ[12].

ووجهت أصابع الاتهام إلى الصين في العديد من هجمات قرصنة استهدفت مؤسسات أمريكية، من بينها هجوم استهدف بيانات ملايين الموظفين الحكوميين.

وقال أوباما "الولايات المتحدة بحاجة إلى أن تكون أكثر سرعة في الاستجابة لمثل هذه الهجمات".

كما أعلن البيت الأبيض، أن الرئيس أوباما لن يقيم بعد الآن في فندق، والدورف استوريا، في نيويورك، الذي اشترته شركة صينية عام 2014. في إشارة إلى مخاوف بشأن تجسس محتمل من قبل الصين.

من جانبه قال الرئيس الصيني شي جين بينغ في نهاية عام 2015، "إنه يجب على جميع الدول أن تعارض بشكل مشترك عمليات التنصت على الإنترنت وهجمات الفضاء الالكتروني وسباق التسلح الالكتروني"[13].

كما يشير عدد من خبراء الأمن الإلكتروني إلى أنّ الصين قد تكون قامت باستهداف الهند من خلال فيروس ستكنست، مستندين في ذلك إلى أنّ الهند وحتى نهاية أيلول/سبتمبر 2010 تعد الدولة الأكثر تعرّضا للفيروس وفقا لإحصاءاتهم، وتأتي في المرتبة الأولى من حيث عدد الحواسيب المصابة بالفيروس متخطّية كل من إيران وإندونيسيا وبواقع 60 ألف جهاز. حيث شهدت العلاقات بين البلدين توتراً عام 2010 على خلفية نزاعات حدودية وسياسية متزايدة مؤخرا.

[12] الرابط اخر زيارة في 2016/6/22

[13] صحيفة الشعب اليومية، "الرئيس الصيني: يجب على العالم مواجهة هجمات الإنترنت وسباق التسلح الالكتروني"، 2015/12/16. الرابط آخر زيارة في 2016/6/22

[3] روسيا:

تتبنى روسيا كما الصين تطوير قدراتها في الحرب الإلكترونية لاسيما في الشق الهجومي، وقد اتهمت بأنها تقف وراء العديد من الحالات المشهورة إلى الآن من دون أن يكون هناك دليل مادي قوي على ذلك. لكن الواضح أنّ روسيا ومنذ انهيار الاتحاد السوفيتي تعتمد على وسائل أقل تكلفة وأكثر فاعلية في مواجهة الولايات المتّحدة وحلف شمال الأطلسي. إذ تعتبر القدرات اللاتناظرية ومن ضمنها الحرب الإلكترونية إحدى أهم وسائل المواجهة في ظل التفوق العسكري للناتو وواشنطن.

وقد رصد تقرير الاستخبارات الأمريكية، مجموعة "التهديدات العالمية" التي تعد أهم تحديات الأمن القومي الأمريكي، بأن الحكومة الأمريكية والقوات المسلحة، والشبكات التجارية، تتعرض بشكل يومي لمحاولات اختراق من جانب مجموعة من الفاعلين، من دول قومية تستخدم برامج متطورة للغاية مثل روسيا والصين، ودول أقل تقدمًا لكنها تستهدف إلحاق الضرر مثل إيران وكوريا الشمالية، أو عبر مجرمين يستهدفون الحصول على المال، أو من خلال قراصنة لهم دوافع أيديولوجية متطرفة.

وذكر التقرير أن وزارة الدفاع الروسية قامت، بحسب عسكريين كبار روس، بإنشاء شبكة إلكترونية خاصة مسؤولة عن القيام بالأنشطة الإلكترونية الهجومية، والتي تتضمن عمليات الدعاية وإدراج البرامج الضارة في الأنظمة المستهدفة، وأن روسيا تعمل على إنشاء فرع متخصص في عمليات الشبكات الإلكترونية [14].

كما أن هناك دولا أخرى قامت بتطوير قدراتها الهجومية والدفاعية في مجال الحرب الإلكترونية ومنها:

_ إنجلترا: قامت بإصدار استراتيجية الأمن الإلكتروني القومية في حزيران/يونيو 2009[15]، كما قامت بإنشاء وحدة الأمن الإلكتروني ومركز العمليات ومقرّه وكالة الاستخبارات القومية (GCHQ)، وبدأت وظيفتها عمليا في شهر آذار/مارس 2010.

- حلف شمال الأطلسي (ناتو): ناقش الحلف الشكل والحد الذي يمكن عنده اعتبار الهجمات الإلكترونية بمثابة إعلان حرب أو شكل من أشكال الاعتداء العسكري الذي يفرض على الدول الأعضاء الالتزام بتقديم المساعدة والدفاع عن الحليف الذي يتعرّض لذلك الهجوم[16]. وقد ذكر تقرير الناتو الصادر في أيار/مايو 2010 الذي بلور

(14) الاستخبارات الأمريكية تتوقع هجمات إلكترونية... وترى تطور روسيا "مثيرًا للقلق"، SPUTNIK عربي، 2015/3/16. الرابط آخر زيارة في 2016/6/22

15) Cyber Security Strategy of the United Kingdom, UK, June 2009. link

16) Cyberwar, the Economist, July 3rd, 2010, p: 11.

مفهوما ودورا جديدا للحلف عام 2020 أنّ هناك ضرورة لتكثيف الجهود وتعزيز قدرات الرد على الهجمات الإلكترونية التي تترك مخاطر متزايدة على أن تتضمن مساعدة الحلفاء على تطوير قدرات دفاعية تضمن الردع المناسب[17].

_ إسرائيل: في أواخر تسعينات القرن الماضي نجح أحد الخبراء الإسرائيلين في مجال الحواسيب، والذي كان يعمل في جهاز الأمن الداخلي الإسرائيلي (شين بيت) من خلال تقنيات القرصنة من اقتحام نظام الكمبيوتر الخاص بمستودع (بي جالوت) للوقود شمالي تل أبيب، وكان الهدف إجراء اختبار روتيني لتدابير الحماية بالموقع الاستراتيجي، حيث أدرك الإسرائيلون أنه بخلاف الاطلاع على البيانات السرية، فإنهم يستطيعون أيضا تنفيذ تفجيرات متعمدة بمجرد برمجة تغيير في مسار خطوط الأنابيب18.

ومنذ ذلك الوقت تبلورت الحرب الإلكترونية شيئاً فشيئاً لتصبح ركناً رئيسياً في التخطيط الاستراتيجي لإسرائيل. وتعتبر الوحدة (8200) في الجيش الإسرائيلي أكثر الوحدات تطوراً من الناحية التقنية والتكنولوجية ولها نشاطات واسعة في حروب الإنترنت والشبكات، وقد انضم إليها الآلاف من العقول الإسرائيلية منذ إنشائها نظراً لشهرتها الواسعة حيث تعمل على ضمان التفوق النوعي لإسرائيل من خلال عمليات دفاعية أو هجومية في الفضاء الإلكتروني19.

وعلى الرغم من أنّه قد تمّ تصنيف الوحدة 8200 من قبل بعض المؤسسات المعنيّة بأنها أكبر سادس مطلق لهجمات الإنترنت في العالم، فإن هذه الوحدة ليست الوحيدة التي تتمتع بهذه القدرات التقنية العالية في إسرائيل، فهناك العديد من الوحدات الأخرى التي تتمتع بقدرات متطورة جداً في مجال تكنولوجيا المعلومات في جميع التخصصات. حيث يتم تجنيد الأطفال الإسرائيليين من النخبة حتى قبل إنهائهم دراستهم الثانوية، عندما يبلغ هؤلاء سن الـ 25 عاماً، يكون لديهم أكثر من 7 سنوات خبرة عملية في مجال التكنولوجيا.

وتشترك الاستخبارات الإسرائيلية (الشين بيت) أيضاً للقيام بنفس المهمة، ويتم الاستفادة في هذا الإطار من العناصر المخضرمة أيضاً، ومن المؤسسات التقنية والمعلوماتية الإسرائيلية ومن العاملين فيها كرافد مهم.

---

17) NATO 2020: Assured Security, Dynamic Engagement, NATO, May 2010, p: 11. link

18) ANALYSIS-Wary of naked force, Israelis eye cyberwar on Iran, Reuters,07 Jul,2009. link

19) Israel's unit 8200: cyber warfare Telegraph Newspaper, 30 Sep 2010. link

أبرز الهجمات الإلكترونية على مستوى العالم:

1_ هجوم إستونيا: يجمع الخبراء على أنّ الهجوم الإلكتروني الذي استهدف إستونيا في العام 2007، يكاد يكون الهجوم الإلكتروني الأول الذي يتم على هذا المستوى ويستخدم لتعطيل المواقع الإلكترونية الحكومية والتجارية والمصرفية والإعلامية مسبباً خسائر بعشرات الملايين من الدولارات إضافة إلى شلل البلاد. وعلى الرغم من أنّ الشكوك كانت تحوم حول موسكو على اعتبار أن الهجوم جاء بعد فترة قصيرة من خلاف إستوني-روسي كبير، إلا أنّ أحداً لم يستطع تحديد هوية الفاعل الحقيقي أو مصدر الهجوم الذي تم، وهي من المصاعب والمشاكل التي ترتبط بحروب الإنترنت إلى الآن.

2_ فيروس "ستكسنت Stuxnet"وهو عبارة عن برنامج كمبيوتر خبيث يهاجم أنظمة التحكم الصناعية المستخدمة على نطاق واسع في مراقبة الوحدات التي تعمل آليا، وعلى الرغم من أنه تم اكتشاف هذا الفيروس لأول مرة من قبل شركة بيلاروسية تدعى VirusBlockAda، حيث قالت إنها عثرت على التطبيق الخبيث في جهاز كمبيوتر يعود لأحد عملائها الإيرانيين.

وهناك من يرى أن وكالَتَي الاستخبارات الأمريكية والإسرائيلية استطاعتا تصميم هذا الفيروس والذي عمل على اختراق وتعطيل المنشآت النووية الإيرانية. كما أن هناك من يرى أن إسرائيل قامت لوحدها بشن هذا الهجوم الإسرائيلي، حيث إن الهجوم كان دقيقًا إلى درجة تحديد عدد أجهزة الطرد المركزي، وقد احتاج تفعيل هذا الهجوم مجرد تشغيل أجهزة الكمبيوتر في المنشآت الإيرانية. وبمجرد أن تسلل الفيروس إلى الأجهزة، أخفى وجوده، واستطاع تعطيل أجهزة الطرد المركزي بمهارة فائقة، حيث عمل على تغيير الضغط داخل أجهزة الطرد المركزي، وجعل سرعة الدورات داخل الأجهزة متفاوتة، مما أدى إلى انهيارها.

ويعتبر البعض أن نجاح هذا الهجوم انتقل بالعالم إلى مرحلة توظيف الهجمات السيبرانية في تحقيق أضرار مادية متعمدة، وهو ما يفتح الباب أمام الكثير من التكهنات بأن مثل هذه الأسلحة المتطورة يمكن أن تصبح أمرًا شائعًا في المستقبل.

ففي 25 سبتمبر/أيلول 2010، أكدت إيران أن العديد من وحداتها الصناعية تعرضت لهجوم إلكتروني بعد إصابتها بفيروس "ستكسنت" ويعد هذا الفيروس وفق العديد من التقارير التي صدرت مؤخراً واحداً من أعقد الأدوات التي تم استخدامها إلى الآن.

حيث كان الخبراء يعتقدون أنّ مهمّة البرنامج هي التجسس الصناعي ونقل المعلومات التي تساعد على تقليد المنتجات[20]. لكن تبيّن لخبراء الهندسة العكسيّة فيما بعد أنّ الأمر مختلف كليّاً. فالبرنامج وعلى عكس الكثير من البرامج المعروفة إلى الآن ليس مخصصاً للتجسس وسرقة المعلومات الصناعية لمحاولة كسب المال أو لسرقة الملكية الفكرية. فبعد حوالي أربعة أشهر من العمل، ظهر أن الأمر أكثر تعقيداً مما كان متصوراً، وأننا نقف اليوم أمام نوع جديد من البرامج التي من الممكن أن تتحول إلى نموذج للأطراف التي تنوي إطلاق هجمات إلكترونية تؤدي إلى دمار حقيقي واقعي في البلد المستهدف حتى دون الحاجة إلى الإنترنت[21].

فالبرنامج لا يعمل بشكل عشوائي كما هي العادة وإنما بشكل محدد جداً؛ إذ يقوم بعد اختراق الأجهزة والحواسيب بالتفتيش عن علامة فارقة تتعلق بأنظمة صنعتها شركة "سيمنز الألمانية"، فإذا ما وجدها يقوم عندها بتفعيل نفسه ويبدأ بالعمل على تخريب وتدمير المنشأة المستهدفة من خلال العبث بأنظمة التحكم وقد تتعدد المنشآت التي يستطيع مهاجمتها من خطوط نقل النفط إلى محطات توليد الكهرباء وحتى المفاعلات النووية وغيرها من المنشآت الاستراتيجية الحسّاسة، أمّا إذا لم يجدها، فيترك الحاسوب وشأنه.

فالبرنامج كبير ومشفّر جداً ومعقد جداً ويوظّف تقنيات ذكية وجديدة، ولا يلزمه للعمل أي تدخل بشري في أي مرحلة من المراحل، ويكفي أن يكون هناك بطاقة ذاكرة تخزين إلكترونية مصابة به حتى يبدأ عمله.

ولأنه على هذه الدرجة من التعقيد والتطور ولأنّه يعمل بشكل محدد جداً، حيث يرى البعض أنه من صنع دولة، ومن البديهي أن تكون المنشأة أو المنشآت الأساسية التي يبحث عنها لتدميرها أو تخريبها قيّمة للغاية وعلى درجة عالية من الأهمية. وبناء على هذا الاستنتاج، ذهبت العديد من المصادر إلى التخمين بأنّ مفاعل بوشهر الإيراني قد يكون الهدف الأساسي الذي يبحث البرنامج عنه لتدميره.

ففي دراسة لها، أشارت شركة "سيمناتيك" التي تعمل في مجال برامج الأمن الإلكتروني والبرامج المضادة للفيروسات أنّ إيران تأتي في طليعة الدول المستهدفة من ناحية الإصابات التي حققها برنامج "ستكسنت" وأنّ ما يقارب 60% من أجهزة الكمبيوتر التي تعرضت لهجوم من هذا التطبيق الخبيث كانت في إيران[22].

---

[20]) Robert McMillan, Was Stuxnet Built to Attack Iran's Nuclear Program PCWorld, September 21, 2010.: link nuclear_program.html

[21]) Mark Clayton, Stuxnet malware is 'weapon' out to destroy ... Iran's Bushehr nuclear plant? The Christian Science Monitor, September 21, 2010. link Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant

[22]) Factbox: What is Stuxnet, Reuters, Fri Sep 24, 2010. link

وعلى الرغم من أنّ إيران نفت عبر مدير مشروع بوشهر محمود جعفري أن يكون الفيروس قد أصاب المفاعل أو تسبب في أي ضرر في أنظمة التحكم فيه، إلا أنها كانت قد أقرت إصابة بعض الحواسيب الشخصية المحمولة لموظفي المحطة بهذا الفيروس إضافة إلى إصابته أكثر من 30 ألف نظام حاسوبي لمنشآت صناعية متعددة داخل إيران.

وهناك عدد من الخبراء يعتقد بالفعل أنّ هدف الفيروس الأساسي قد يكون مفاعل بوشهر، وأنّ الفيروس قد حقق هدفه من التخريب بدليل أنّ إيران أعلنت أنها ستؤجّل العمل في المفاعل عدّة أشهر حتى بداية عام 2011، ويرى فيه آخرون أنّ الهدف هو منشأة ناتانز لتخصيب اليورانيوم بدليل أنّ المنشأة عانت مشكلة ظلّت طي الكتمان وأدت إلى انخفاض أجهزة الطرد المركزية القادرة على العمل بنسبة 15% فجأة وذلك في نفس الفترة التي ظهر فيها الفيروس لأول مرّة.

والسؤال الذي يطرح من هو المسؤول عن هذا الهجوم، فبحسب ما أشرنا أعلاه هناك عدة روايات ومنها:

اولاً: لا تستبعد جهات أن تكون الولايات المتّحدة الدولة المصنّعة للفيروس نظرا لتعقيده وتطوره ولما يحتاجه من خبرات وموارد هائلة. ويربط البعض بين هذا الفيروس وبين النزاع الأمريكي-الإيراني حول الملف النووي، وأنّ الهدف منه هو تخريب المجهود النووي الإيراني خاصّة أنّ الرئيس الأسبق جورج بوش الابن كان قد سمح وفقا لتقارير صحفية نقلاً عن مسؤولين حكوميين، بإطلاق جهود تتضمن العديد من الخطوات التي تهدف إلى تخريب البرنامج النووي الإيراني من خلال استهداف أنظمة الحواسيب والكهرباء والشبكات وكل ما يخدم البرنامج النووي الإيراني. ووفقا لأصحاب هذه الرواية، فقد استكمل الرئيس السابق أوباما هذا المجهود فيما بعد، خاصّة أنّ عملية تخصيب اليورانيوم كانت قد عانت مصاعب تقنية كبيرة عام 2010 وما زال من غير المعروف إذا ما كان السبب هو العقوبات الاقتصادية أم التصنيع الرديء أم عمليات التخريب الأمريكية.

ثانيا: تتجه أصابع الاتهام إلى إسرائيل دون الولايات المتحدة، فيما يتعلق بفيروس "ستكسنت" اعتمادا على عدد من المؤشرات منها:

_ توافر القدرات التقنية اللازمة للقيام بمثل ذلك العمل.

_ تعقيدات العمل العسكري التقليدي والتردد الأمريكي في الدخول بحرب جديدة أو السماح لإسرائيل بفعل ذلك.

_ توافر سوابق لإسرائيل في هذا المجال، لعلّ أبرزها أن قصف إسرائيل العام 2007 لمفاعل نووي مزعوم في سوريا، كان مسبوقاً بهجوم إلكتروني عطّل الرادارات الأرضية والراجمات المضادة للطيران[23].

كما يرى البعض وجود مؤشرات قوية تدلل على أن إسرائيل من قامت بهذا الهجوم وهي:

1- في عام 2010 كشف رئيس شعبة المخابرات العسكرية الإسرائيلية الميجر جنرال "عاموس يادلين" في خطوة نادرة أنّ مجال الحرب الإلكترونية يناسب تماماً عقيدة الدفاع في إسرائيل، وأنّ القوات الإسرائيلية أصبح لديها الوسائل الكافية لإطلاق هجمات إلكترونية استباقية من دون أي مساعدات خارجية، وهي تدرس بهدوء استخدام هذه التقنيات ضدّ الآخرين بهدف التسلل إلى معلومات أو القيام بتخريب من خلال زرع برامج في أنظمة السيطرة والتحكم في المنشآت الحساسة للأعداء في المنطقة مثل إيران24.

2- كذلك في عام 2010 توصلت إسرائيل إلى أنّ نقطة ضعف إيران الكبرى إنما تكمن في معلوماتها المحملة إلكترونياً، وهو ما يتيح استهدافها. وعندما سئل (سكوت بورج) مدير الوحدة الأمريكية لتبعات الإنترنت "وهي وحدة استشارية تقدم خدماتها في مجال الأمن الإلكتروني لمختلف الوكالات الأمنية الوطنية الأمريكية" عن السيناريو الذي يمكن أن تلجأ إليه إسرائيل لاستهداف إيران، أجاب أنه "من الممكن استخدام "البرامج الخبيثة" لإفساد أو إعطاب أو السيطرة على أجهزة التحكم في المواقع الحساسة مثل محطات تخصيب اليورانيوم، وبما أن الأصول النووية لإيران ستكون في الغالب غير متّصلة بالإنترنت، فلن يتسنى للإسرائيليين زرع الفيروس عبر الإنترنت وسيكون عليهم دسه في البرامج التي يستخدمها الإيرانيون أو في أجهزة محمولة يدخلها فنيون دون علم الإيرانيين. ويكفي توافر أي وحدة تخزين بيانات متنقلة ملوثة لإتمام هذه المهمة". وهو سيناريو شبيه بما حصل في إيران.

3- أشار (ليام أو مورشو) وهو من الذين عملوا على تفكيك "ستكسنت" ودراسة وظيفته وقدّم شرحاً عملياً لقدرته التدميرية الماديّة من خلال تجربته على مضخّة إلى وجود كلمة مفتاحية في شفرة التعليمات الخاصة بالبرنامج تحمل كلمة(Myrtus)، وهي كلمة مرادفة باللغة العبرية لكلمة "ايستر" في إشارة إلى ملكة اليهود بفارس واسمها الحقيقي (هاداسا) التي أقنعت زوجها الملك الفارسي احشورش بالقضاء على كل من يعادي اليهود ومن بينهم أخلص وزرائه "هامان". كما يقوم "ستكسنت" عندما يجد هدفه بعرض رقم من ثماني

---

[23]) Wary of naked force, Israelis eye cyber war on Iran, Reuters, Jul 7, 2009. link

[24]) Spymaster sees Israel as world cyberwar leader, 15 December 2009. link

خانات (19790509)، وهو على الأرجح تاريخ 9 مايو/أيار 1979. وفقا للأرشيف، فان هذا التاريخ شهد موت حبيب الغانيان، وهو أول إيراني يهودي تم إعدامه في إيران بعد الثورة الإسلامية بتهمة التجسس.

ويمكن القول إن إسرائيل هي المسؤول المباشر عن هذا الهجوم وبمساعدة الولايات المتحدة الأمريكية نظراً للإمكانية التقنية والتكنلوجية للبلدين والى حرصهما على إفشال المشروع النووي الإيراني لما يمثله من خطر محتمل لإسرائيل ولحرصها على أن تبقى البلد الوحيد الذي يملك السلاح النووي في المنطقة، إضافة إلى حرص الولايات المتحدة لكيلا تكون إيران دولة نووية.

ومن خلال عرض أبرز الهجمات الإلكترونية نلاحظ أن الأطراف المهاجمة لا تعلن عن مسؤوليتها عن الهجوم، ما يجعل الحرب الإلكترونية أكثر تعقيداً وما يدفع الدول إلى تطوير دفاعتها الإلكترونية لحماية أمنها وسلامة ممتلكاتها من أي هجوم مفترض.

كل هذا إلى دفع إلى تامين ما بات يعرف بالأمن السيبراني. حيث إن الأمن السيبراني"Cyber security"، هو عبارة عن مجموع الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني. إذاً فالسلاح السيبراني هو سلاح استراتيجي بيد الحكومات والأفراد لا سيما أن الحرب السيبرانية أصبحت جزءاً لا يتجزأ من التكتيكات الحديثة للحروب والهجمات بين الدول[25].

ويعد مفهوم الأمن السيبراني أحد أهم مفاهيم الحقبة القادمة، التي ربما تشهد "حروبًا إلكترونية" تحل محل الحروب التقليدية، لتصل إلى نفس مداها في الخسائر المادية، وربما تتعداه.

أثر الهجمات الإلكترونية:

دفعت الهجمات الإلكترونية الكثير من الدول لاتخاذ إجراءات وقائية للحد من الأضرار الناجمة من تلك الهجمات التي تستهدف مؤسسات الدولة والبنوك ووسائل الإعلام والمؤسسات الخدمية كمحطات المياه والكهرباء

[25] الرابط آخر زيارة في 2016/6/22

وسوف نركز على ثلاث دول في هذه النقطة قامت بإجراءات وقائية وهي كل من اليابان وكوريا الجنوبية وماليزيا وفيما يلي نشرح أبرز الهجمات الإلكترونية التي تعرضت لها هذه الدول وماهي أبرز الإجراءات وكيف أثرت هذه الهجمات على سياسات الدول الثلاث.

يرى البعض أن اليابان لم تسارع في اتخاذ تدابير مضادة تتناسب مع حجمها الاقتصادي والتكنولوجي لمواجهة الهجمات الإلكترونية[26]، حيث تعرضت اليابان لعدد من الهجمات الإلكترونية، فعلى سبيل المثال تعرضت لهجوم إلكتروني في عام 2009، يعتقد أن مصدره من الصين، وخلال هذا الهجوم تم الاستيلاء على معلومات من نحو 1000 جهاز كمبيوتر تابعة لشخصيات سياسية ودبلوماسية وعسكرية وصحفية أيضًا. وكذلك حدثت هجمات سابقة في عام 2005، حيث أصيبت الآلاف من أجهزة الكمبيوتر بالفيروسات.

وفي عام 2011، استطاع القراصنة الصينيون من التسلل إلى موقع شركة ميتسوبيشي للصناعات الثقيلة، وهي أكبر شركة يابانية، والحصول على بيانات منها تخص محطة للطاقة النووية وبيانات مهمة أخرى.

وبحسب الإحصائيات فإن اليابان تعرضت في العام 2015 لأكثر من خمسين مليون هجوم إلكتروني، وكانت 30% من مجموع هذه الهجمات قادمة من الصين و20% قادمة من الولايات المتحدة الأمريكية[27]، حيث تمكن المهاجمون في إحدى الهجمات من تعطيل الموقع الخاص برئيس الوزراء الياباني وعددٍ من المواقع الحكومية الحساسة. ويقول خبراء يابانيون في مجال الدفاع الإلكتروني إنه يتم الكشف عن هجمات على المواقع الحكومية كل بضع ثوان[28].

إن هذه الهجمات المختلفة تظهر ضعف الأمن الإلكتروني الياباني على جميع المستويات من المواطنين العاديين إلى الجيش والمؤسسات إلى الحكومة. ولذلك أصبحت قضية حماية الإنترنت أولوية بالنسبة للحكومة اليابانية.

وفي كوريا الجنوبية التي كان لها نصيب من الهجمات الإلكترونية، حيث تشير الإحصاءات إلى أن عدد الهجمات الإلكترونية التي تعرضت لها كوريا الجنوبية ارتفعت بنسب عالية ما بين عامي 2008 و2011 بنسب تصل إلى 37%. ففي ديسمبر/كانون الأول من عام 2009، أوردت الحكومة الكورية الجنوبية تقريرًا عن تعرضها لهجوم نفّذه قراصنة من كوريا الشمالية، بهدف سرقة خطط دفاعية سريّة تتضمن معلومات عن شكل التحرّك الكوري الجنوبي والأمريكي في حالة حصول حرب في شبه الجزيرة الكورية.

---

(26) Jeff Kingston," Japan's cyber security upgrade — too little, too late?" The Japan Times, MAY 21, 2016. link. آخر زيارة للموقع في 2016/8/2م.

(27) Record 54.5 billion cyber-attacks detected in Japan last year, The Japan Times, FEB 21, 2016. link. آخر زيارة للموقع في 2016/8/2م.

(28) اليابان تحت مظلة الأمن الإلكتروني الأميركي، موقع قناة سكاي نيوز عربية، أبوظبي، الإمارات، السبت 30 مايو، 2015م. الرابط آخر زيارة للموقع 2016/8/2م.

وتعرضت كوريا الجنوبية لعدة هجمات إلكترونية، حيث وقع هجوم في مارس/ آذار 2013[29]، على عددٍ من البنوك الكورية ووسائل الإعلام، وأسفر عن اضطراب في عددٍ من أجهزة الكمبيوتر وتعطل الخدمات البنكية.

وقد شكلت الهجمات تعطل شبكات الحاسوب المشغلة لثلاثة بنوك كورية جنوبية كبرى واثنين من أكبر محطات البث في البلاد، وقد تسبب الهجوم في الشلل التام لشبكات بنوك مثل بنك "شينهان" و"نوجهيوب" ومحطات إعلامية مثل "إم بي سي" و"واي تي إن" في البلاد.

وقد أفاد تقرير صادر عن مكتب الأمن الوطني الكوري الجنوبي، أنه لا يستبعد تورط كوريا الشمالية بالهجوم. وأضاف التقرير أن وزارة الدفاع الكورية الجنوبية قامت برفع مستوى الاستعداد الأمني في البلاد، وخصصت فرقًا للتعامل مع الوضع، كما دعا وزير الدفاع (كيم كوان جين) إلى اجتماع أمني طارئ [30].

ويشار إلى أن هذا الهجوم، جاء في أعقاب التجربة النووية الثالثة لكوريا الشمالية في فبراير/شباط من عام 2013، حيث تصاعدت فيه حدة التوتر في شبه الجزيرة الكورية.

وعلى إثر هذا الهجوم رفعت كوريا الجنوبية منذ ذلك الحين درجة الاستعداد في برنامج "انفو كون" للدفاع الرقمي، وهو آلية لإصدار تنبيه في حال وقوع أي هجوم إلكتروني يضر بأمن البلاد.

وتشير المصادر الكورية الجنوبية إلى ارتفاع نسبة الهجمات الإلكترونية التي تستهدف مؤسساتها، حيث وصل عدد حالات الهجمات الإلكترونية في 2012 فقط إلى 40 ألف حالة.

وفي يونيو/ حزيران 2013 تعرضت مواقع رسمية كورية جنوبية لهجمات إلكترونية، ومن بين المواقع الرسمية التي تعرضت للهجوم، الموقع الإلكتروني لمكتب رئيس الجمهورية، إضافة إلى مواقع إعلامية. وعلى إثر هذه الهجمات أعلنت كوريا الجنوبية حالة التأهب الإلكتروني في هذا الهجوم[31].

ويأتي هذا الهجوم، وهو ليس الأول من نوعه، في الذكرى السنوية لبداية الحرب الكورية (1950-1953) التي قسمت شبه الجزيرة الكورية.

وذكر بيان لوزارة العلوم الكورية الجنوبية، "أن الحكومة تستطيع تأكيد وقوع هجوم إلكتروني بواسطة قراصنة مجهولين، حيث أدى إلى إغلاق العديد من المواقع بما في ذلك موقع المكتب الرئاسي المعروف "البيت الأزرق".

---

(29) تاريخ الهجمات الإلكترونية -مخطط زمني، مجلة الناتو، 2013. الرابط آخر زيار للموقع في 2016/8/2م.

(30) CHOE SANG-HUN," Computer Networks in South Korea Are Paralyzed in Cyber-attacks", The New York Times, MARCH 20, 2013. link آخر زيارة للموقع في 2016/8/3م.

(31) هجوم على المواقع الإلكترونية في كوريا الجنوبية، BBC عربي، 25 يونيو/ حزيران 2013. الرابط آخر زيارة للموقع في 2016/8/2م.

وقد رفع الجيش الكوري الجنوبي حالة التأهب خشية من وقوع هجمات إلكترونية على مواقعه وأمرت رئيسة كوريا الجنوبية السابقة، (بارك جيون هاي)، بفتح تحقيق حول الهجمات الإلكترونية، وطلبت من لجنة الاتصالات الكورية والوكالات الحكومية والشركات إلى مضاعفة عدد المراقبين لهجمات القرصنة الإلكترونية المحتملة إلى ثلاثة أضعاف.

ويطلق على الفيروس الذي ضرب بعض المؤسسات الكورية الجنوبية "Dark Seoul"، حيث تم التعرف لأول مرة على هذا الفيروس في عام 2012. ويعمل هذا الفيروس على جعل أجهزة الكمبيوتر غير صالحة للاستعمال في كوريا الجنوبية. ويرى البعض أن الهدف من هذه الهجمات هو إيصال رسالة إلى كوريا الجنوبية، أن كوريا الشمالية قادرة على الوصول إلى القلب الاقتصادي لسيول دون تفجير سفينة حربية كورية جنوبية أو قصف جزيرة كورية جنوبية. وقد تم توجيه الاتهام إلى كوريا الشمالية باستخدام هذا الفيروس من خلال هجمات على مدى السنوات الثلاث (2011،2012،2013). وقال (كيم مين سيوك) المتحدث باسم وزارة الدفاع "إنه لا يمكن استبعاد احتمال تورط كوريا الشمالية بهذه الهجمات".

أما بالنسبة لماليزيا، فإن التقارير الصادرة عن المركز القومي المتخصص للأمان الإلكتروني والمعروف بـ Cyber security التابع لوزارة العلوم والتكنولوجيا والابتكار الماليزية، حيث يشير إلى أن المركز قد تلقى في الربع الثالث من عام 2011 حوالي 4526 حالة لجرائم إلكترونية متنوعة بنسبة زيادة وصلت إلى 18% عن عدد الحالات التي شهدها الربع الثاني من نفس العام [32].

وإن أكثر تلك الجرائم كانت جرائم الرسائل الإلكترونية أو الروابط التي تحمل فيروسات إلكترونية أو ما يعرف ب (Spam) فقد بلغت 1646 حالة، ثم حالات الاحتيال الإلكتروني، حيث بلغت 1355 حالة ثم حالات التلصص والتي بلغت 978، وأخيرًا حالات التحرش الإلكتروني التي بلغت 80 حالة. وقد شهدت حالات الـ(Spam)، والتلصص زيادة في الربع الثالث عن الربع الثاني من عام 2011 أما حالات الاحتيال والتحرش الإلكتروني قد شهدتا انخفاضًا عن الربع الثاني من عام 2011. الجدير بالذكر أن أغلب حالات التلصص اشتملت على تهديدات لمواقع فاعلة أو الاستيلاء على معلومات والتلاعب بها، أو سرقة حسابات إلكترونية أو كلمات السر لحسابات مواقع التواصل الاجتماعي. أما أغلب حالات الاحتيال فتمثلت في حالات النصب أو حالات النصب المتعلقة بمواقع اليانصيب، أو

(32) يسرا محمد طه، ماليزيا والتحديات الأمنية في القرن الحادي والعشرين. دراسة تطبيقية في مفهوم أمن الإنسان، في هدى ميتكيس وخليل رسلان، (محرران)، ماليزيا وتحديات القرن الحادي والعشرين، مرجع سابق، ص 135.

انتحال الشخصيات أو بيع المنتجات الوهمية. وأخيرًا بالنسبة لحالات التحرش الإلكتروني فإن أغلبها تمثل في التهديدات والمطاردات الإلكترونية الشخصية.

الجدير بالذكر أن تزايد أعداد تلك الحالات يرجع إلى تزايد أعداد مستخدمي الكمبيوتر والإنترنت، وإلى جهل المستخدمين بمصادر التهديد الإلكتروني وأشكاله، بالإضافة إلى الولع العام بكل ما هو إلكتروني واستهلاكي. ولكن على الرغم من التزايد في حالات القرصنة الإلكترونية بماليزيا إلا أن أغلبها يدخل في نطاق الجرائم المحدودة والصغيرة، حيث إن أغلب تلك الجرائم يدخل في الإطار المالي أو القرصنة الإلكترونية أي المستويين الأول من الجرائم الإلكترونية ولم تصل إلى اقتحام الأنظمة أو الإرهاب الإلكتروني، وذلك بحسب البيانات الرسمية الصادرة عن الحكومة الماليزية [33].

الإجراءات التي اتخذتها كل من اليابان وكوريا الجنوبية وماليزيا تجاه مخاطر الهجمات الإلكترونية:

أولاً- الإجراءات القانونية:

للحفاظ على بياناتها ومعلوماتها الحساسة ومؤسساتها من الهجمات، أقر البرلمان الياباني قانونًا في عام 2014 يهدف لتعزيز الأمن السيبراني، حيث منح صلاحية واسعة للمركز الوطني لمجلس الوزراء من حيث الجاهزية واستراتيجية الأمن السيبراني[34].

أما بالنسبة للجهود الماليزية في هذا الصدد فنجد أن الهيئة القومية للأمان الإلكتروني قد قامت بإصدار عدد من البيانات والتحذيرات للمستخدمين حول نقاط الضعف المختلفة في أنظمتهم والتي تجعلهم عرضة لمثل هذه التهديدات كما أنها قامت بعدد من التدريبات وألقت عددًا من المحاضرات حول الموضوع في مناسبات مختلفة للتوعية من تلك المخاطر.

ثانيًا- الإجراءات التعاونية:

في إطار سعي اليابان لحماية مؤسساتها الحيوية من الهجمات الإلكترونية، قامت بالاتفاق مع الولايات المتحدة الأمريكية على مد ما بات يعرف بـ (مظلة الدفاع الإلكتروني)[35]، حيث تعهدت واشنطن أن تمد مظلتها للدفاع

(33) يسرا محمد طه، ماليزيا والتحديات الأمنية في القرن الحادي والعشرين. دراسة تطبيقية في مفهوم أمن الإنسان، مرجع سابق، ص135.

(34) Jeff Kingston," Japan's cyber security upgrade — too little, too late?", Japan Times, MAY 21, 2016.

[35]) أمريكا تمد مظلتها للأمن الإلكتروني لحماية اليابان، صحيفة العرب القطرية، 30 مايو، 2015.

الإلكتروني لحماية اليابان، ومساعدتها في التصدي للتهديدات المتزايدة من الهجمات الإلكترونية على القواعد العسكرية، والبنية التحتية، مثل محطات الكهرباء.

وجاء في بيان مشترك بين البلدين، "نلاحظ تزايدًا في مستوى التطور بين الجهات الإلكترونية الخبيثة، بما في ذلك الجهات غير الحكومية وتلك التي ترعاها دول".

وتعهدت وزارة الدفاع اليابانية بالإسهام في الجهود المبذولة من أجل التصدي لمختلف التهديدات الإلكترونية، بما في ذلك التهديدات ضد البنية الأساسية اليابانية والخدمات التي تستخدمها قوات الدفاع الذاتي اليابانية والقوات الأميركية.

وكشف وزير الدفاع الأميركي السابق أشتون كارتر الذي التقى بنظيره الياباني (جين ناكاتاني) في سنغافورة في مايو 2015، النقاب عن استراتيجية عسكرية إلكترونية أكثر قوة، تؤكد على القدرة على الانتقام، باستخدام أسلحة إلكترونية[36].

ويشار إلى أن الأمن الإلكتروني أصبح مجالاً رئيسيًا تعمق فيه اليابان والولايات المتحدة شراكتهما العسكرية، في إطار مجموعة من المبادئ التوجيهية الأمنية الجديدة، ومن شأنها أيضًا أن تدمج أنظمة الدفاع الصاروخية، وتعطي طوكيو دورًا أمنيًا أكبر في آسيا، حيث تتنامى القوة العسكرية للصين.

وتأتي المظلة الدفاعية الإلكترونية في ظل شعور كل من الولايات المتحدة واليابان بالقلق من التهديدات الإلكترونية، بما في ذلك الهجمات المحتملة من قبل الصين وكوريا الشمالية.

كما تأتي هذه المظلة في ظل وجود ثاني أكبر قاعدة عسكرية أمريكية في آسيا، حيث تتواجد في اليابان، وعليه فإن الولايات المتحدة تستثمر لبناء قوة للتصدي والرد على الهجمات الإلكترونية.

وتأتي جهود اليابان في بناء دفاعاتها الإلكترونية والتعاون في هذا المجال مع حليفتها الولايات المتحدة، من أجل مواكبة ما قامت به الدول الأخرى في هذا المجال، خاصة الدول التي تعتبرها اليابان مصدر تهديد وهي كوريا الشمالية والصين وروسيا، كما أن اليابان تستعد لاستضافة دورة الألعاب الأولمبية في طوكيو عام 2020، وعليه تخشى من تزايد الهجمات الإلكترونية التي ربما تشن لعرقلة هذا الحدث الرياضي العالمي.

---

[36]) نفس المصدر.

ويأتي تعزيز وسائل الردع الإلكتروني في أعقاب هجمات مؤثرة ضد شركات، بما في ذلك أعمال القرصنة على شركة (سوني بيكتشرز إنترتينمنت)، عام 2014، التي ألقت الولايات المتحدة باللائمة فيها على كوريا الشمالية.

أما في ماليزيا فعلى الرغم من أن معدلات التهديد التي تمثلها القرصنة والجرائم الإلكترونية بماليزيا مقارنة بغيرها من الدول ليست بالمرتفعة إلا أن السلطات تقوم بالتعاون مع كبرى الشركات الإلكترونية لتطوير أنظمة الحماية من تلك التهديدات، وأن تزيد من حملات التوعية لمستخدمي الكمبيوتر والانترنت وأن تعمل على توفير التحديثات المختلفة بشكل سريع لهؤلاء المستخدمين.

ويرى البعض أن جهود ماليزيا في هذا الصدد متواضعة، وأن عليها أن تبذل المزيد في هذا الاتجاه من خلال التعاون مع الدول الأخرى لحماية أمنها الإلكتروني.

ثالثًا - الإجراءات الداخلية:

في إطار تطوير اليابان قدراتها الدفاعية الإلكترونية، نظمت اليابان مسابقة دولية لمن يُعرفون بقراصنة القبعات البيض، وهم أشخاص ذوو مهارات عالية في برمجة الحاسوب.

حيث إن هؤلاء لا يستخدمون مهاراتهم في القيام بعمليات قرصنة إلكترونية غير قانونية، بل يُسخّرونها لمساعدة السلطات في مواجهة الهجمات الإلكترونية، وكشف الثغرات في البرامج والمواقع الإلكترونية.

وبعد تصفيات تم اختيار 20 فريقًا من القراصنة الشباب إلى المرحلة النهائية من مسابقة أمن الإنترنت "سيككون" الدولية. وتقول الهيئة المنظمة للمسابقة، "إن الهدف هو الاستفادة من المهارات الاستثنائية للشبان في مجال الإنترنت، وبدلاً من أن يستخدموا مهاراتهم في القرصنة الإلكترونية فإنهم يقومون تسخيرها لخدمة المجتمع"[37].

وتأتي هذه الخطوة اليابانية لأن القراصنة ذوو القبعات البيض يساهمون من خلال هجماتهم القانونية في التعرف على نقاط الضعف في أنظمة حماية الإنترنت، والثغرات في خوادم أجهزة الحاسوب الخاصة بالمؤسسات الحكومية والخاصة. وتأمل اليابان في أن تساعدها هذه المسابقات على تنشئة جيل من محترفي الإنترنت كي يساهموا في حماية فضائها الإلكتروني، في ظل تزايد كبير في عدد الهجمات التي تتعرض لها[38].

(37) القراصنة القانونيون. أمل اليابان لحماية أمنها الإلكتروني، الجزيرة نت، 2016/2/7. الرابط آخر زيارة للموقع 2016/8/2م.

(38) Jeff Kingston," Japan's cyber security upgrade — too little, too late?", Japan Times, MAY 21, 2016.

ويستخدم المعهد الوطني لتكنولوجيا المعلومات والاتصالات في اليابان(NICT) [39]، حوالي 280.000 ألف جهاز استشعار للكشف عن الهجمات الإلكترونية حول اليابان. وتهدف هذه الأجهزة للتحكم عن بعد بأنظمة المتصلة بشبكة الإنترنت والتحقق من ضعف برنامج الخادم [40].

أما كوريا الجنوبية فتعمل وزارة الدفاع على تطوير أسلحة تشبه "ستكسنيت"، وهو البرنامج الإلكتروني الذي طور لمهاجمة منشآت تخصيب اليورانيوم الإيرانية. حيث قالت وزارة الدفاع "إن الجيش الكوري الجنوبي سيقوم بعمليات من خلال استخدام هذا البرنامج". وقالت وكالة يونهاب الكورية الجنوبية، إن تطوير سلاح قادر على إحداث أضرار مادية بمنشآت كوريا الشمالية النووية هو المرحلة الثانية من الاستراتيجية التي بدأت في 2010.

ويشير المختصون أن استخدام الحرب الإلكترونية لإحداث أضرار مادية في المفاعلات النووية قد يكون له عواقب وخيمة[41]. وأن نشر برنامج "ستكسنيت"، أصبح من المستحيل التنبؤ به أو السيطرة عليه.

وقد قامت السلطات في كوريا الجنوبية بتقديم دورة تدريبية متقدمة لأبرز قراصنة الشبكة العنكبوتية في البلاد، بهدف تأهيل أفراد على مستوى عالٍ من الخبرة لمواجهة الهجمات الإلكترونية على عدد من المنشآت الحساسة.

وبحسب المعهد الكوري لبحوث تكنولوجيا المعلومات، فإن هذه الدورة التدريبية يطلق عليها اسم " Best Of The Best"، حيث يقوم العاملون عليها بتدريب مجموعة مختارة من أبرز محللي أنظمة الترميز في البرامج والأنظمة الحاسوبية[42].

وأشار المعهد إلى أن هذه الخطوة تأتي على خلفية العديد من الهجمات التي تعرضت لها البلاد خلال الأعوام الماضية، كانت أبرزها الهجوم الإلكتروني الذي وقع في العام 2011 والذي استهدف أحد أكبر البنوك وتسبب بخسائر فادحة، بالإضافة إلى الاعتداء الذي وقع بالعام 2009 على عدد من المواقع الإلكترونية التابعة للحكومة، الأمر الذي أدى إلى إلحاق خسائر وصلت قيمتها إلى 50.5 مليون دولار بحسب بعض التقديرات.

وعليه يمكن القول إن أكثر الهجمات الإلكترونية استهدفت كل من اليابان وكوريا الجنوبية ما ترتب عليهما اتخاذ إجراءات احترازية لتفادي المزيد من الهجمات والخسائر المترتبة، وأن الهجمات الإلكترونية جاءت أقل في ماليزيا ما ترتب على ذلك إجراءات أقل من نظيرتها في اليابان وكوريا الجنوبية.

---

(39) للمزيد حول المعهد الوطني لتكنولوجيا المعلومات والاتصالات في اليابان (NICT) انظر الموقع الرسمي: http://www.nict.go.jp/en

(40) Record 54.5 billion cyber attacks detected in Japan last year, The Japan Times, FEB 21, 2016.

(41) كوريا الجنوبية تطور سلاحًا إلكترونيًا في مواجهة الشمال، BBC عربي، 21 فبراير/شباط 2014. الرابط آخر زيارة للموقع في 2016/7/25م.

(42) كوريا الجنوبية تقدم دورة متقدمة لقراصنة الإنترنت، سي إن إن عربي، الاثنين، 14 كانون الثاني/يناير 2013. الرابط آخر زيارة للموقع في 2016/8/2م.

خاتمة:

إن اهتمام الدول خاصة المتقدمة بالمجال الخامس وهو الفضاء الإلكتروني خاصة في جزيئة إنشاء جيوش قادرة على الهجوم وهي جالسة في مكانها ويدافع عن مؤسسات الدولة الحيوية يجعل المجال الخامس يأخذ حيزاً كبيراً في سياسات الدول وفي استراتيجياتها المستقبلية.

ومن خلال الشرح السابق يمكن القول إن الهجمات الإلكترونية باتت أكثر خطراً من السابق خاصة مع التطور التكنولوجي الذي يحدث كل يوم وشهر وعام، وعليه فإن السلاح الإلكتروني بات بالفعل المجال الخامس إلى جانب المجالات الأربعة (البر والبحر والجو والفضاء) التي تتنافس عليها الدول خاصة المتقدمة وعلى رأسها الولايات المتحدة الأمريكية والصين وروسيا ودول أخرى.

إن التركيز على المجال الإلكتروني في الدراسات الأكاديمية مهم جداً خاصة في عالمنا العربي والذي يعتبر حقلاً دراسياً جديداً في مجال الدراسات الأمنية والذي يطغى عليه الدراسات التقليدية في العلاقات الدولية، وعليه فإن التركيز على هذا المجال مهم جداً خاصة أنه ربما يؤدي إلى ضرب العلاقات بين دولتين وأكثر في حال هاجمت دولة ما دولة أخرى عن طريق إرسال فيروسات إلكترونية تؤدي إلى تعطيل مؤسسات الدولة بكافة أشكالها [43].

([43]) الآراء الواردة تعبر عن كتابها، ولا تعبر بالضرورة عن وجهة نظر المعهد المصري للدراسات