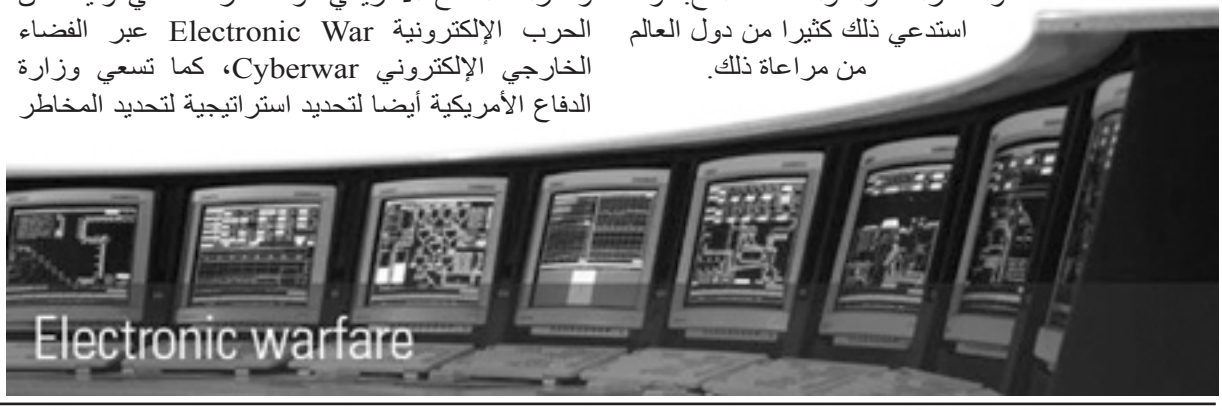
العالم الافتراضي
والحروب الإلكترونية

بعد الحروب التقليدية التي تتم علي الأرض والبحر والجو والفضاء دخلت الحروب مجالها الخامس الافتراضي المرتبط بالإنترنت، وصارت تمثل تهديدا معقدا ومتعدد الأوجه. فمن الملاحظ حاليا، أن المجتمعات الحديثة صارت تعتمد بصفة شبه كليا علي الأنظمة والتطبيقات الرقمية المحملة علي شبكة الإنترنت مما قد يمثل مجالا خصبا واسع للهجومات والتهديدات الإلكترونية الضارة علي مؤسسات الدول الحيوية كمحطات الكهرباء، ومصافي البترول، والبنوك وأنظمة التحكم في خطوط الطيران، ورادارات السيطرة والرقابة التي ترتبط بالأمن القومي، الخ. وقد أدي ذلك إلي محاولة كثير من دول العالم وحاصة الرائدة والمتقدمة منها في مجالات تكنولوجيا المعلومات والاتصالات في تطوير البرمجيات التي تخفض وتخد من تلك التهديدات الإلكترونية المتوقعة علي منشآتها المختلفة وخاصة الحيوية منها.

وتعود جذور مشكلة التعرض لهجمات التهديد لمشكلة جرثومة الألفية لعام ٢٠٠٠ عندما سادت العالم باكملة مخاوف من تعطل أنظمة الاتصالات والمؤسسات المالية وغيرها بسبب التحول من الرقم ١٩٩٩ إلي الرقم ٢٠٠٠، إلا أنـه تم حل تلك المشكلة بصورة تكنولوجية عالية المستوي. إلا أن ذلك الهاجس في تعطل المقومات الأساسية لأي دولة باستخدام فيروسات إلكترونية معينة تعطل شبكات الاتصال في أي مؤسسة أو منظمة ما بل والدولة ذاتها. وقد صار تطوير واستخدام هذه الفيروسات الإلكترونية كأسلحة يمكن توظيفها بهدف الانتقام أو الابتزاز، أو حتى الترويج للحماية من الفيروسات صار من الأمور المعروفة لدي مستخدمي الحاسبات الآلية في كل أرجاء العالم. أما استخدام تلك الفيروسات الإلكترونية كأسلحة حربية بدلا من الدبابات والطائرات والغواصات، الخ. وقد استدعي ذلك كثيرا من دول العالم من مراعاة ذلك.

وفي هذا الصدد، أعلن رئيس الولايات المتحدة الأمريكية باراك أوباما في عام ٢٠٠٩ بأن الولايات المتحدة خسرت ما يقرب من تريليون دولار بسبب جرائم الإنترنت التي تمثل عالم جريمة أضخم كثيرا من عالم مافيا المخدرات علي سبيل المثال، كما أعلن أيضا الرئيس الأمريكي في العام ٢٠١١ أن البنية الأساسية التحتية الرقمية للولايات المتحدة الأمريكية تمثل ثروة وطنية استراتيجية لذلك عين رئيس الأمن السابق في شركة مايكروسوفت مسئولا عن أمن شبكات المعلومات الهامة الأمريكية. كما أنشأت وزارة الدفاع الأمريكية قيادة لأمن الإنترنت لوضع خطة شاملة لتأمين عمليات الدفاع عبر شبكات الجيش الأمريكي بحيث تقدر علي اكتشاف أي مخاطر أو هجومات عبر الإنترنت من أي مكان في العالم تسعي لاختراق إمكانيات وقدرات الدفاع الأمريكي، وقد نشر ذلك في وثيقة عن الحرب الإلكترونية Electronic War عبر الفضاء الخارجي الإلكتروني Cyberwar، كما تسعي وزارة الدفاع الأمريكية أيضا لتحديد استراتيجية لتحديد المخاطر



الإلكترونية وتوضيح سبل الرد عليها عسكريا، أو من من خلال فرض عقوبات مالية، أو وضع معايير دولية ضد استخدام شبكات المعلومات.

كما أنه في عام ٢٠١١ اتخذت منظمة حلف شمال الأطلسي قرارا بالقيام بإعداد دراسة لتقييم أبعاد الهجمات الإلكترونية الافتراضية وتحديد أبعاد وسبل الرد عليها وخاصة في حالة وقوع أي هجوم علي شبكة الإنترنت في أي دولة من الدول الأعضاء.

وفي عام ٢٠٠٨ الذي شهد حربا محدودة بين روسيا وجورجيا، أمكن مشاهدة حربا إلكترونية أي هجوم إلكتروني فضائي علي شبكات معلومات جورجيا المتاحة عبر شبكة الإنترنت أدي لعرقلة أجهزة جورجيا الخكومية ومؤسساتها المالية مما شل قدرة جورجيا علي التواصل. وقد تزامنت تلك الهجمات الإلكترونية التي تعرضت لها جورجيا علي تمكين الجيش الروسي في حربه عبر القوقاز.

وحتي الوقت الحالي، ما زال الغموض يحيط بفيروس «ستكسنت Stuxnet» الذي استهدف هذا الفيروس قدرات إيران النووية مما لأدي لتوقف وتخريب وإصابة ما يقرب من ألف جهاز رد مركزي في أسبوع واحد في عام ٢٠١٠، وقد اتهمت إيران كلا من الولايات المتحدة وإسرائيل بأنهما وراء نشر هذا الفيروس الذي استهدف الضرر في منشآتها النووية. وقد بدأت إيران بعد تلك الحادثة إعلان إمتلاكها جيش إلكتروني لمقاومة إي انتهاكات لإلكترونية تتعرض لها. بل إن المقاومة الفلسطينية في أعقاب الصراع بين إسرائيل وقطاع غزة في شهر نوفمبر ٢٠١٢ الذي أعاد للذاكرة الاجتياح الإسرائيلي العدواني علي القطاع في عام ٢٠٠٨، وعلي الرغم من التفاوت الظاهر في القدرات العسكرية بين المقاومة وإسرائيل، بدأت المقاومة الفلسطينية في استخدام الفضاء الخارجي الإلكتروني أولا للتعبير عن ذلك الصراع الجاري بشكل متزامن يهدف لبناء سياسة الحوار وحشد الرأي العام العالمي عبر أدوات الرأي والتعبير عبر الإنترنت، وثانيا القيام بشن هجمات التدمير والاختراق علي مواقع الشبكات الإسرائيلية تعبيرا عن المقاومة الإلكترونية أو الحرب الإلكترونية عبر الفضاء الخارجي الإلكتروني. وفي هذا التوجه، فامت مجموعة مقاومة فلسطينية تحتي مسمي «أنونيموس» بنشر قائمة بمعلومات تتضمن ٥٠٠٠ موظف إسرائيلي حكومي تبين الأسماء الكاملة باللغة العبرية لهم، مع عناوين سكنهم، وأرقام تليفوناتهم، وبريدهم الإلكتروني، الخ. كما أن مجموعة مقاومة فلسطينية أخري تتبع مجموعة «أنونيموس» السابق الإشارة إليها الحرب الإلكترونية علي المؤسسات الإسرائيلية معتمدة علي موقع نشر يخفي شخصية المرسل Anonpaste.me لنشر القائمة السابقة، إلي جانب إختراق ما يقرب من ٧٠٠ موقع أسرائيلي تتضمن مواقع بنك القدس الإسرائيلي، ووزارة الدفاع، والموقع الرسمي للرئيس الإسرائيلي، الخ من خلال أغراق تلك المواقع بسيل متدفق

من الرسائل والزيارات المزيفة. وفي الوقت الحالي، لا تخفي فيه كثير من دول العالم قدرتها علي شن حروب إلكترونية عبر شبكة الإنترنت من بينها روسيا، الولايات المتحدة، إسرائيل، كوريا الشمالية، بل وإيران وغير ذلك من الدول.

وقد أكدت شركة «مكافي» الأمريكية المتخصصة في برامج مكافحة الفيروسات أن تصفح شبكة الإنترنت أصبح في الوقت الحالي أخطر من أي وقت مضي، وأشارت إلي أن عدد البرامج الخبيثة المتوافرة علي الإنترنت وصل لأعلي معدلاته خلال الأربع سنوات ماضية وفي طريقه للزيادة لكي يصل إلي ما يقرب من ١٠٠ ألف فيروس في نهاية عام ٢٠١٣.

وإلي جانب فيروس «ستكسنت Stuxnet» السابق الإشارة إليه، يمكن الإشارة أيضا لفيروس آخر أعلنت عنه شركة «كاسبريسكي لاب» الروسية الذي يطلق عليه فيروس «جاوس» للمراقبة الإلكترونية في الشرق الأوسط يمكنه التجسس علي المعاملات المالية والبريد الإلكتروني وأنشطة التواصل الاجتماعي، ويستطيع أيضا مهاجمة البنية الأساسية ذات الطبيعة الحيوية للدول والمؤسسات، وقد تم تطوير هذا الفيروس من نفس المعامل التي أنتجت فيروس «ستكسنت Stuxnet» الذي يعتقد إنتاجه من قبل كل من الولايات المتحدة وأسرائيل. وقد أصاب فيروس «جاوس» بالفعل أجهزة الكمبيوتر الشخصية في كل من لبنان، وفلسطين بل إسرائيل أيضا، حيث أصاب في لبنان ثلاث بنوك وخاصة نظام الدفع الإلكتروني علي سبيل المثال. كما يمكن اكتشاف فيروس خبيث لبرامج الكمبيوتر يطلق عليه فيروس «فلام» أي الشعلة الذي تم إطلاقه عام ٢٠١٠ ويمثل برنامجا للتجسس الإلكتروني أيضا أكثر تعقيدا من فيروس «جاوس» يستهدف المكاتب الحكومية ومكاتب صناعة الطاقة في كل من إيران وإسرائيل والأراضي الفلسطينية المحتلة والسودان، ويمكن لهذا الفيروس سرقة الوثائق الإلكترونية أو تغييرها، إلي جانب قدرته في التصنت علي المكالمات التي تتم علي الحاسبات الآلية.

وقد أشارت دراسة قامت بها شركة « كاسبريسكي لاب»» بواسطة نظام رصد المخاطر عبر شبكة «كاسبرسكي» للأمان السحابية أن مُتصفحي الانترنت يواجهون نحو ١٠٨٠٣٥ هجمة الكترونية في الساعة أو نحو ١٨٠٠ في الدقيقة. إجمالا اعتمد المجرمون الالكترونيون ٤٠٧٣٦٤٦ نطاق لإطلاق الهجمات الالكترونية في عام ٢٠١١.

وقد قامت شركة كاسبريسكي لاب» أيضا بتحليل المواقع التي استضافت أكبر عدد من الروابط الخبيثة ووجدت أن المواقع الالكترونية الترفيهية التي تحوي مقاطع فيديو هي الأكثر خطراً، وجاءت محركات البحث في المركز الثاني، وتتبعها مواقع التواصل الاجتماعي، وتأتي المواقع بمحتوى خاص للكبار والشبكات الإعلانية في المركزين الرابع والخامس على التوالي، حسب البوابة العربية للأخبار التقنية.

وقال يوري ناميستنيكوف، كبير مُحللي البرمجيات الخبيثة في شركة «كاسبريسكي لاب» إن المُجرمين الالكترونيين يستخدمون مُختلف الأنواع من المواقع القانونية لتوزيع «ابتكاراتهم»، ولهذا الغرض يقومون بفتح صفحات في مواقع التواصل الاجتماعي ليستقطبوا ضحاياهم، يوزعون البريد المزعج من خلال الرسائل الشخصية وينشرون تعليقاتهم بنشاط على مقاطع الفيديو المشهورة ومنشورات شبيهة إضافة إلى روابط مؤدية إلى البرمجيات الخبيثة في رسائلهم.

وبالنتيجة وُجد أن ٣٨٪ من مستخدمي الانترنت في الإمارات العربية المتحدة تحتوي أجهزتهم برمجيات خبيثة، إلا أنه بالإمكان التقليل من خطر البرمجيات الخبيثة بشكل الملموس إذا اتبع المستخدم القواعد الأساسية للسلامة في الانترنت، مقل عدم النقر على الروابط في الرسائل المستلمة من مرسلين غير معروفين، وتفقد باستمرار صحة عنوان الويب في شريط أدوات المتصفح قبل إدخال البيانات الشخصية.

كما سبق، يمكن استنتاج أن الحروب الإلكترونية القادمة سوف تمثل حروب المستقبل القريب التي يلجأ إليها بدلا من الحروب التقليدية، لا بسبب تقليل أعباء التكاليف البشرية والمادية التي تتكبدها الدول من الحروب التقليدية فقط، ولكن أيضا لأن الحرب الإلكترونية لا تحتاج لاتخاذ قرارات دولية أو مبررات قانونية لشنها، فهي تمثل الخيار الأكثر تحضرا للتصدي للهجمات المحتملة، كما تمثل نوعا من الحروب المتاحة وغير المقصورة علي دول أو منظمات عسكرية تتبع دولة معينة، وإنما يمكن أن يقوم بها الأفراد أو الجمعات أو الشركات الخاصة مما يصعب السيطرة علي تلك الحروب الإلكترونية القادمة.