الحرب الإلكترونية .. جيل جديد من الحروب لا نعرفه

"إنه عمل استفزازي يستحق عقوبة مشددة"، بهذا وصفت شبكة الأخبار الحكومية في كوريا الشمالية عزم شركة سوني بيكتشر الأمريكية الترفيهية عرض فيلم ساخر عن زعيمها الحالي كيم يونج أون، فما شكل هذه العقوبة المشددة التي تحدثت عنها كوريا الشمالية؟!

أعلنت شركة سوني بيكتشر الأمريكية صبيحة أحد الأيام التي تلت هذا التهديد عن تعطل نظام الحاسوب الخاص بالشركة ومسح بعض البيانات الخاصة بالشركة من عليه، وسرقة ما قيمته 10 سنوات من رسائل البريد الإلكتروني ونشر مقتطفات محرجة من هذه الرسائل، كما تم الإعلان عن سرقة بيانات شخصية لموظفي الشركة وكبار المسؤولين بها، كما تم تسريب مقتطفات من 5 أفلام من إنتاج الشركة من بينها 4 لم يتم عرضهم حتى الآن؛ ما سيؤدي إلى خسارة تتكبدها الشركة تصل إلى مليارات الدولارات.

بعد ساعات من هذه الوقائع التي مُنيت بها الشركة أعلنت عن إلغاء عرض فيلم "المقابلة"، الفيلم الساخر من الزعيم الكوري الشمالي بدور السينما الأمريكية، فمن وراء هذا الحادث الهوليودي بامتياز؟

نقلت شبكة "إن بي سي" الأمريكية الإخبارية عن مصدر بالحكومة تصريحاته عن هذه الحادثة بأن عملية الاختراق مصدرها من خارج كوريا الشمالية، ولكن هذه الاختراقات تمت بتحريض من الحكومة الكورية الشمالية وأن مكتب التحقيقات الفيدرالي الأمريكي "إف بي آي" لديه أدلة دامغة تشير إلى وجود علاقة بين كوريا الشمالية وعملية الاختراق، إلا أن المسؤول الأمريكي رفض الإفصاح عن مزيد من المعلومات المتعلقة بهذه الحادثة، يقرأ هذا التصريح بجوار تصريح الرئيس الأمريكي باراك أوباما لشبكة تليفزيون"سي إن إن" تعقيبًا على هذا الحادث بأنه لا يعتقد أن هذا العمل من أعمال الحرب إنما هو مجرد عمل من أعمال التخريب الإلكتروني، والولايات المتحدة تدرس الرد المناسب.

الرئيس الأمريكي لا يعد هذا نوعًا من أنواع الحرب وإنما هو مجرد تخريب إلكتروني، في هذا الصدد يجب أن نؤكد أن ما حدث هي حرب مكتملة الأركان والوقائع ولكنها من أجيال الحروب الجديدة التي ظهرت مؤخرًا وحديثًا "كحروب ردع" تستخدم الوسائل الإلكترونية الحديثة في توجيه ضرباتها الهجومية والدفاعية تجاه الدول المعادية، بل إن الجيوش النظامية اعتمدت أسلحة وفروع بها مختصة بهذا النوع من الحروب، كما أن أجهزة مختصة داخل الدول تابعة لهيئات مختلفة باتت مختصة في التحقيقات المتعلقة بالجريمة الإلكترونية، إذن ما هي الحروب الإلكترونية؟ ومتى ظهرت؟ وما هو دورها الحالي في العالم؟

لقد اخترع ماركوني أول جهاز برق لاسلكي قبل بضع سنوات من اندلاع الحرب بين روسيا والإمبراطورية اليابانية عام 1904 وكانت هذه الحرب هي أول الحروب التي استخدم فيها الراديو أو الإشارات اللاسلكية من قبل القوات البحرية في الجيشين.

استخدم اليابانيون أجهزة مقلدة من جهاز الراديو الأصلي على سفنهم لكنها كانت رديئة للغاية، كذلك استخدم الروس محطات لاسلكية محمولة على سفنهم، لم يكن يعرف اليابانيون أية احتياطات أو حذر في استخدام إشارات الراديو والتي كانت تُستقبل عن طريق السفن اليابانية والروسية على حد سواء ولكن نظرًا لوجودة محطات الإشارة الروسية كان الروس يستقبلون التعليمات اليابانية في الحرب قبيل أن تصل إلى الأسطول الياباني بوقت قليل، لذلك عمد الروس إلى خطط دفاعية محكمة طبقًا لمعرفتهم بخطط اليابان الهجومية؛ فتم إفشال عدة هجمات بحرية يابانية طبقًا لهذه الاختراقات، وبهذا هي رحلة بداية "المخاض" للحرب الإلكترونية تاريخيًا والتي ظهرت جلية بين روسيا واليابان ولو بشكل عشوائي في هذه الحرب.

تطور الأمر في الحرب العالمية الأولى عندما نجح البريطانيون في القيام بعمليات تجسس إلكترونية فريدة من نوعها نجحوا من خلالها في حل جميع الشفيرات الحربية الألمانية التي من المفترض أنها على درجة عالية من الدقة والسرية، كذلك قام الألمان بعمليات مضادة في هذه الحرب إلى أن وصلت الحرب الإلكترونية إلى مرحلة جديدة في بدايات الحرب العالمية الثانية وذلك بإدخال تقنيات الرادار لتوجيه الضربات الإلكترونية ولا يوجد أشهر من معركة التصنت التي خاضتها بريطانيا تجاه قائد البارجة الألمانية "بسمارك" عن طريق أجهزة تصنت رُزعت في إيرلندا تمكن خلالها البريطانيون من الاستماع عن بعد لكل التقارير التي يرفعها القائد الألماني إلى القيادة الألمانية العامة؛ الأمر الذي أدى إلى تحديد موقعه بدقة كبيرة ومهاجمة بارجته حتى إغراقها.

مع ظهور ثورة تكنولوجيا المعلومات والاتصالات وتطور أدوات تكنولوجيا الاتصال ظهرت مرحلة ثالثة للحرب الإلكترونية هي أشد شراسة وأكثر تعقيدًا من سابقتها تستخدم الشبكة العنكبوتية "الإنترنت" في إرسال هجمات على الدولة المعادية تؤدي إلى خسائر اقتصادية وخسائر في البنية التحتية أيضًا مما يعد نوعًا من استنزاف الموارد باستخدام الحرب الإلكترونية بدلاً من حروب الاستنزاف العسكرية التي اعتمدتها الجيوش قديمًا كتكتيك حربي.

هذا التطور النوعي جعل مسارات الحرب الإلكترونية أكثر اتساعًا، فرغم صعوبة تصور الأمر إلا أنه وصل لدرجة كبيرة من الجدية عالميًا في استخدام هذا السلاح للدفاع والهجوم في آن واحد، فعلى سبيل المثال لا الحصر يعكف الخبراء في وزارة الدفاع الأمريكية "البنتاجون" حاليًا على تطوير قدرات الولايات المتحدة إلكترونيًا لشن هجومًا على أنظمة الحاسبات التابعة للدول الأخرى، كذلك ذكرت صحيفة لوس أنجلوس تايمز الأمريكية أن المسؤولين العسكريين بالولايات المتحدة لديهم رغبة للمضي في تطوير القدرات الهجومية الأمريكية في مجال الحرب الإلكترونية للانتقال بأمريكا من التركيز على الدفاع عن الأمن القومي الأمريكي إلى مرحلة الهجوم والمباغتة واعتماد هذا الأسلوب كأحد أساليب الحرب الجديدة التي

ستستخدم قريبًا.

أحد المسارات التي تعني بها الحرب الإلكترونية جيدًا هو مسار "المعلومة" والسطو عليها؛ فمعرفة المعلومات المشفرة أو البيانات السرية الخطرة التي تعمد كل الدول على إخفائها هو هدف رئيسي لهذه الحرب، ولا تقتصرهذه القرصنة الإلكترونية على المعلومة العسكرية وفقط بل إن تطور أشكال الحروب إلى الحرب الاقتصادية والثقافية جعل كافة المعلومات ذات أهمية وأن اختراق المجتمعات لا يتم إلا بهذه المعلومات.

ومن أحد المميزات التي تعتمد عليها الدول في الحرب الإلكترونية هي أنها لا يلزم لها تورط مباشر من قبل الحكومات أو الجيوش، إذ تستطيع الدول الدفع بمجموعة من "القراصنة" الغير تابعين لها للقيام بهجمات إلكترونية تجاه مؤسسات أو دول بعينها للحصول على معلومات مطلوبة أو تدمير أهداف مخطط لها.

ومن هذا الحديث نستطيع إيجاد تعريف مبسط للعامة يتحدث عن عمليات الحرب الإلكترونية المركزة في مجال القرصنة حديثًا بالحديث عنها كأحد عمليات الاختراق التي تتم عبر الوسائل التكنولوجية المختلفة وأشهرها حديثًا شبكة الإنترنت، هذا الاختراق يتم لشبكات داخلية لدول أو لمؤسسات أخرى بهدف تعطيل عمل وحدات بعينها من هذه الشبكات كما يحدث في الجيوش أو اختراق حواسيب معينة للحصول على معلومات منها أو التشويش على أجهزة هجومية إلكترونية باستخدام أجهزة مضادة يتم هذا بالتحايل على أنظمة المعالجة الآلية لكشف البيانات الحساسة وتغييرها أو التأثير عليها أو حتى إتلافها تمامًا.

هناك عناصر رئيسية لهذه الحرب يجب الإشارة إليها: تتمثل في الدعم الإلكتروني والهجوم الإلكتروني والحماية الإلكترونية، هذا العناصر تمثل استخدامات الحرب الإلكترونية بشكل عام في الواقع بالنسبة للدول، لكن الأمر غير مقتصر على الدول كما ذكرنا من قبل، حيث يمكن أن يقوم بهذه الأعمال مجرد أشخاص متمكنون ذوو مستوى عال يستطعيون بواسطة بعض الأدوات المساعدة مهاجمة مواقع إلكترونية لدول كاملة وانتهاك خصوصياتها واختراق أنظمتها الإلكترونية بشكل كامل أو إحداث ذلك تجاه مؤسسات بعينها بغرض السرقة أو الإتلاف.

وإليكم بعض الحالات الفردية للقرصنة الإلكترونية عبر العقود الماضية:

في عام 1986 استطاع شاب كولمبي سرقة خط تيليكس حكومي ومراسلة مجموعة مصارف بريطانية لنقل أكثر من 13 مليون دولارًا من أرصدة الحكومة الكولومبية.

مجموعة من القراصنة الروس المحترفين نجحوا في نقل 10 ملايين دولار من سيتي بانك إلى حسابات مصرفية في فنلندا وإسرائيل، وقد تم إيقافهم في الولايات المتحدة وحُكم عليهم بثلاث سنوات سجن.

عام 2001 لم يتمكن زوار موقع شركة مايكروسوفت للبرمجيات على مدار يومين من زيارة الموقع بسبب اختراق الموقع من قبل بعض القراصنة.

في عام 2007 نجح قرصان تركي في الهجوم على موقع الأمم المتحدة وإلحاق بعض الأضرار به.

في هذه الصدد الفردي ينقسم العاملون في هذا المجال إلى فئتين:

*هاكرز "Hackers" الذين يعتمدون على برامج التجسس الجاهزة والمتاحة لاستخدامها في زرع ملفات تجسس في حواسيب الأهداف عن طريق الثغرات في أنظمة المعلومات، ومن ثم الحاق الضرر بها أو استخلاص معلومات منها وهذا النوع من العاملين يتسمون بأنهم هواة وأن أهدافهم شخصية بحتة من أجل مال أو دوافع إثبات للذات.

*الكراكرز"Crackers" هم النوع الأخطر في هذه العملية لأنهم يعملون من أجل أهداف عليا، قد يتلقون الدعم من خلال حكومات أو أنظمة استخبارات ويتميز هؤلاء المحترفون ببحثهم عن كيفية عمل أنظمة التشغيل والبيانات لا كيف يستخدمونها، فالتركيز كله منصب على الاختراق لا عن كيفية التشغيل، حيث يتم تحليل الأنظمة واكتشاف ثغراتها وبرمجة فيروسات تنجح في الدخول عن طريق تلك الثغرات لتحقيق الأهداف المطلوبة سواء بالسيطرة أو الحصول على البيانات أو سرقة الأموال.

أما على صعيد الدول فالأمر لا يقل خطورة، بل إنه أمر أصبح يهدد جميع الدول التي ليس لديها خبرة في هذا المجال وهذا يفسر اهتمام القوى العالمية بهذا النوع من الحروب اتقاءً لشره، إذ إنه لا يحتاج إلى إمكانيات عملاقة لصناعة فريق يدير حربًا إلكترونية أو قرصنة على دولة ما.

فخلال عام 1995 تعرضت حواسيب وزارة الدفاع الأمريكية إلى 250.000 هجمة، كذلك تعرضت المواقع الفيدرالية للتشوية والاختراق.

كما كشف اختصاصيون في الأمن المعلوماتي أن إيران تقف وراء هجمات إلكترونية تتعرض لها مؤسسات مالية أميركية، وذلك ردًا على العقوبات الدولية التي تستهدف الحكومة الإيرانية.

وأعلن للمرة الأولى عن هذه الاعتداءات في سبتمبر 2012، حسب شركة "رادوير" المتخصصة بالأمن المعلوماتي.

كما قال رئيس لجنة الاستخبارات بمجلس النواب الأمريكي إن الولايات المتحدة معرضة لهجمات إلكترونية قد تؤدي إلى إغلاق تام لخدمات مالية أو تدمير معلومات تحتاجها الشركات في عملياتها اليومية.

في حين أن إسرائيل في العام 2012 فرضت حظرًا إلكترونيًا على كبار ضباط أجهزتها الأمنية، ومنعت المسؤولين الأمنيين من استخدام حواسيبهم وحساباتهم على المواقع الإلكترونية، جاء هذا القرار على وقع تحذيرات من هجوم إلكتروني تخطط له إيران في إطار ما أصبح يُعرف بـ "الحرب الإلكترونية" بين الطرفين.

هذا وتجند إسرائيل أكثر من 3500 جندي افتراضي في الحرب الإلكترونية، وقد صرح وزير الاستخبارات الإسرئيلي دان ميريدور بقوله: "في هذا العالم من الحواسيب يجب علينا أن نكون في المقدمة، وذلك لنكون قادرين على مواجهة من يخطط لمهاجمتنا"، والمعني الأساسي الحاضر الغائب في تصريح المسؤول الإسرائيلي يعني أن إسرائيل تخوض حربًا إلكترونية وإن لم تكن معلنة.

وفي يوليو من العام 2010 أعلنت ألمانيا أنّها واجهت عمليات تجسس شديدة التعقيد لكل من الصين وروسيا كانت تستهدف القطاعات الصناعية والبنى التحتية الحساسة في البلاد ومن بينها شبكة الكهرباء التي تغذي الدولة.

كذلك أوردت الحكومة الكورية الجنوبية تقريرًا عن تعرضها لهجوم نفذه قراصنة كوريون شماليون بهدف سرقة خطط دفاعية سريّة تتضمن معلومات عن شكل التحرّك الكوري الجنوبي والأمريكي في حالة حصول حرب في شبه الجزيرة الكورية؛ ما أشعل الصراع عالميًا للسعي للريادة في هذا المجال.

كما أن جميع المعطيات تشير إلى بداية حرب باردة إلكترونية بين العديد من دول العالم أبرزهم بالتأكيد الولايات المتحدة، وعلى خلفية هذا أعلنت الصين عن إنشاء "الجيش الأزرق" وهي إدارة خاصة بجيش التحرير الصيني من أجل حماية الفضاء الإلكتروني الخاص بالجيش على شبكة الإنترنت والعمل على زيارة مستوى أمن شبكة القوات المسلحة الصينية، كما تشير تقارير دولية إلى أن العالم بحاجة إلى مليون خبير أمني حول العالم، للحد من الهجمات الإلكترونية الشرسة، وقد جاءت تصريحات الرئيس الأمريكي باراك أوباما مؤكدة للمعاناة هذه التي تعانيها الدول الكبرى جراء هذه الحرب في الفضاء المفتوح، حيث

أكد أن العالم يحتاج لقوانين جديدة لوقف القرصنة الإلكترونية.

تشكيل رادع في منظومة هذه الحرب هو من الصعوبة بمكان لأن ليس بها ثوابت أو قوى تقليدية كالحروب العادية التي تصنع فيها الطائرة والصاروخ المضاد لها في آن واحد، فالأمر غير متحكم به بالمرة وإمكانية إيجاد الثغرات متاحة للجميع؛ لذلك تلجأ الدول قدر المستطاع لأنظمة أمن المعلومات للتصدي لقضايا التجسس والاختراقات المختلفة، لكن الأمر به صعوبة إيجاد التأمين الكامل 100%، فما زال هناك هامش خطر غير مؤمن لذا تدفع الدول والمؤسسات العالمية مليارات الدولارات سنويًا لتحديث أنظمة الأمن المعلوماتي بها لتفادي خطر العابثين به من الدول المعادية والأفراد ولتقليل نسبة الخطر وليس لمنعها تمامًا إذ إنه أمر شبه مستحيل حتى الآن.

هذا الأمر بالتأكيد ذو أبعاد سياسية وأهمية كبرى، فانتقال الشباب إلى ميدان الفضاء الإلكتروني في مواجهة قمع الحكومات خاصة في دول العالم النامي جعل هذا الأمر سلاحًا في يد الشباب داخل عملية التغيير، وجعل الحكومات الديكتاتورية تولي له اهتمامًا خاصًا لمحاربته ومراقبته وفرض محظورات عليه، فلا يخفي على أحد دور وسائل الإعلام الإلكترونية في ثورات الربيع العربي وكيف نقلت الصورة كاملة إلى العالم أجمع عن طريق أدوات بسيطة على مواقع التواصل الاجتماعي، كما لا يخفى على أحد محاربة الأنظمة لهذه الأدوات الإلكترونية حيث دخلت ضدها حربًا إلكترونية تستهدف النشطاء على هذه المواقع كما هو الحال في مصر على سبيل المثال، حيث تم إلقاء القبض على نشطاء يديرون صفحات معارضة للنظام، كما تستهدف المواقع نفسها بحجبها كما هو الحال في المملكة العربية السعودية على سبيل المثال، أو بالمواجهة كما هو الحال في سوريا التي تستخدم ما يُعرف بالجيش السوري الإلكتروني وهو مجموعة افتراضية على شبكة الإنترنت تقوم بدعم الجيش السوري التابع لنظام بشار الأسد في قمع التظاهرات التي انطلقت ضده في عام 2011 يستهدف هذا الجيش بعملياته مواقع تابعة للمعارضة السورية كما يستخدم أساليب الدعايا والترويج تجاه الثورة السورية ببث الشائعات على الفضاء الإلكتروني.

يتضح من السابق أن العالم مقبل على حرب إلكترونية يشترك فيها الأفراد ليس فقط حصرًا على الدول والحكومات فهذه الحروب أعلت من شأن الأفراد في استخدام أدوات وتكنولوجيا الاتصال الحديثة على كافة الأصعدة وتبين للدول والحكومات أن شرًا مستطيرًا يأتي تجاههم عن طريق تلك الأدوات التي قاموا بتطويرها وتعهدوها بالرعاية، إلى أن دخلوا في مرحلة مواجهة لن تنتهي بأي حال على المدى القريب.

هذا المقال يأتيكم ضمن ملف سباق التسلح على نون بوست