الانترنت : ساحة سلم ام ساحة حرب ؟

الأنترنت كما عرفناه هو العمود الفقري للتجارة العالمية واشهر وسيلة تواصل واسرعها والأكثر توفرا ولكن هنالك مشكلة ظهرت مع ازدياد الاعتماد على الفضاء السبراني (Cyberspace) , ماهي حدوده ؟ ومن صاحب الحق فيه هل هو ملك للدولة ام ملك للشركات ؟ بالنسبة للحدود فلا حدود معروفة ولم يتم التفاهم على ذلك لحد الان كما هو الحال بالنسبة للبحار فحدود الدول البحرية معروفة وكدلك البرية وحتى الجوية والدولة هي من لها سلطة على الحدود ولكن الفضاء السبراني شيئ اخر ولكننا هنا دخلنا في اشكال فالكل يدعي الملكية فالشركات الخاصة تدعي انها صاحبة الأجهزة والكابلات وهي صاحبة المواد التي تمر عبر الأجهزة والدولة تقول انها وضعت القوانين وهي التي أعطت السماح باستعمال الأرض البحار والحدود و الاثنان ساهموا في بنائه والاثنان مسؤولين عن صيانته وكل جهة توثر على الأخرى فنستطيع القول انه قطاع مختلط متداخل يحتاج الى توضيح.

الفضاء السبراني وسيلة تنافس منذ نشأته على الأقل تجاريا ولكنه اليوم اصبح هاجسا قويا لكثير من الدول تخوفا من هجوم سبراني كاسح يشل مفاصل الدولة برمتها خاصة البنى التحتية التي تعتمد اعتمادا كليا على الانترنت ويتسبب بسقوط الدولة بدون اطلاق قذيفة واحدة. لقد حذرت المؤسسات العسكرية والمدنية في عدة دول غربية من هكذا احتمال وأشار رؤساء عدة أجهزة مخابراتية بان الاضوية الحمراء بدأت تضيئ.

هل يمكن القول بان سيناريو هجوم كاسح محتمل؟. يمكن الإجابة بنعم لكن الدول الكبرى الزمت نفسها بعدم القدوم على خطوة كهذه ضد أي دولة أخرى كما هو الحال بالنسبة للأسلحة النووية وبدلا من ذلك تقوم الدول بهجومات صغيرة ومحدودة وهذه الدول بأعمالها هذه التي بدأت بالتزايد خلال السنين القليلة الماضية مما أدى الى فقدان اهم خاصية تمتع بها الانترنت عبر سنينه الأولى وهذه الخاصية هي <u>الثقة.</u>

أصبح الهجوم على مؤسسات دولة معينة او على بنوكها او سرقة معلومات تجارية الصناعية او حتى التدخل في الانتخابات حتى وصل الامر الى شل شركات عملاقة وهذا يقودنا الى الاستنتاج أن نفس الساحة التي نستعملها للتواصل والتبادل التجاري والعلمي غدت ساحة معركة مدمرة.

من المتهم بما بيناه أعلاه؟, هنالك جهتان, الأولى هي الدول و الحكومات التي تقوم بهكذا قرصنة لأهداف متباينة والجهة الثانية هي الافراد والشركات الخاصة و لأغراض مادية او انتقامية. في الجهة الاولى لا يغركم انه فقط الدول الكبرى والمتقدمة هي التي لديها القدرة فقط على اعمال قرصنة كبرى والمستغرب ان دولا من العالم الثالث لها قدرات كبيرة مثل ايران او كوريا الشمالية وبدات هذه الدول بالاستثمار لتطوير مهاراتها في هذا المجال ومن الدول الكبرى الأخرى أمريكا والصين وروسيا ويجب ان لا ننسى الكيان الصهيوني واعماله القذرة بهذا المجال .

اذا ما هو الحل لوقف هذه الحرب او على الأقل تحجيمها حتى لا تكبر؟
الحل أولا ان تعمل جميع الدول صادقة لوقف اعمال القرصنة الحكومية وان تشرع قوانين رادعة للقرصنة الخاصة وثانيا على المؤسسات الدولية كالأمم المتحدة ان تأخذ دورها وتنشئ قوة بوليسية دولية لتعقب المجرمين وجلبهم للعدالة.

هنالك مصطلح جديد ظهر قبل سنين قليلة لوصف هكذا عمليات وهو "" العمليات السبرانية Cyber Operations " ويرمز هذا المصطلح الى التنافس الجديد بين القوى الدولية المختلفة وأول ما يتراءى للمتابع الحقيقي للحرب السبرانية بين جميع الأطراف انه لا توجد قوة عظمى تمسك زمام الأمور كما هو الحال في وصف العالم اعتمادا على القوى التقليدية ولكن في هذا العالم يمكن لدولة صغيرة او ضعيفة ان تكون قوة كبيرة فيه والجميل في هذا العالم وفي هذه العمليات انها سرية جدا وغير معترف بها وليس من السهل ان تعرف الفاعل الحقيقي والخاصية الأخرى انها مختلفة الاحجام والاهداف وكذلك الاتجاهات ولهذه الأسباب بدأت دول كثيرة بالتسلح سبرانيا.

هنالك امثلة كثيرة عن " العمليات السبرانية " الكبرى ويمكن ان تكون اشهرها هو اتهام روسيا في التدخل في الانتخابات الامريكية الأخيرة فالاتهام هو قرصنة موسكو لايميلات المرشحة الرئاسية هيلاري كلينتون وسرقة وثائق وايميلات سرية مثيرة للجدل وتسريب هذه الوثائق والايميلات الى موقع Wikileakes لنشرها مما تسبب في خسارتها لكثير من الأصوات المؤيدة.

كذلك هنالك المثال المشهور عندما هاجمت كوريا الشمالية شركة Sony لإنتاجها فلمها المشهور The Interview الذي يتحدث عن محاولة اغتيال الرئيس الكوري الجنوبي بطريق كوميدية وتسبب ذلك الهجوم الكبير بشل الشركة كليا حتى

انهم عادوا لاستعمال الأقلام والدفاتر لفترة طويلة حتى انتهوا من بناء نظام جديد ومتطور .

هنالك اعتراف وزارة الفاع الامريكية باختراقهم مراسلات عصابة داعش المجرمة لإعطاء معلومات خاطئة او ما يسمى بالقنابل السبرانية.

الأمثلة كثيرة وكثير من الدول تضررت بهذه القرصنة والغريب انه لم يجلب أحد للعدالة للعمليات الكبرى هنالك بعض الصغار تم مسكهم فقط.

تتهم أمريكا الصين بانها اكبر جهة تقوم بالقرصنة ضدها لسرقة معلومات وابحاث تجارية وصناعية وتدعي أمريكا ان خسارتها السنوية تتراوح بين 226$ بليون الى حد 600$ بليون سنويا , كل هذا يحدث في زمن السلم ولكن هذا يتجاوز السلام بدرجات ولكنه لا يرقى الى حد الحرب فنحن مازلنا بين بين وكل هذه مناوشات وكل طرف يعمل على زيادتها ليرى اين هو الخط الأحمر الذي لن ترضى عنه الأطراف الباقية ان يتجاوزه لذا اصبح واجبا على جميع الدول ان تعمل بجد بوقف او التقليل من القرصنة قبل ان تخرج الأمور عن السيطرة.

أن أي هجوم سبراني سيسبب خسائر فادحة خاصة أن كل شيء اصبح يعتمد على الانترنت بطريقة او أخرى فلو أخذنا أي جيش في العالم فاعتماده على الانترنت في المراقبة والتحرك ونقل المعلومات سيجعله عرضة للتوقف عن العمل عند أي هجوم سبراني يشل حركته حتى ولو كان على شبكة الكهرباء التي تغذيه وهذا ما يحذر منه قادة الجيوش الكبرى حول العالم وضغطهم على حكوماتهم للاهتمام بهذا الموضوع. أن أي قرصنة لقطع شبكة الكهرباء قرب أي قاعدة عسكرية ستكون له عواقب وخيمة ليس على المنظومة العسكرية فقط وانما حتى المواطنين العاديين الساكنين قرب القاعدة وعلى الشركات والمؤسسات والمستشفيات القريبة خاصة بعد التوسع في استعمال الIoT (Internet Of Things) ان هجوما كهذا ستكون له عواقب وخيمة , أن الخوف من هجوم كهذا حدا ببعض الحكومات التفكير الجدي في عزل المؤسسات المهمة كليا ومن هنا ظهر مفهوم " الجدار السبراني " او " Air- Gapping " الذي يمل للعزل الكلي عن الخارج ليعمل باستقلالية عن الشبكة السبرانية العالمية المفتوحة ولكن حتى هذا غير محصن 100% فالشبكات المعزولة تحتاج الى الخارج فمثلا تحتاج الى تطوير او تحديث البرامج Software وغيره بالإضافة الى ان كثيرا من الخبراء استطاعوا عبور الجدار عبر الاثير مثل WIFI او Microwave . هنالك دول تعمل جزئيا بمبدأ الجدار مثل China

Great Firewallفي الصين واهم أهدافها عزل الصين عن الخارج وتحقيق السيطرة على الداخل وما يمكن الولوج اليه ومثال اخر هو أيران وجدارها المسمى Halal Net لنفس الهدف.

ألغريب في الموضوع هو قصر نظر الحكومات والشركات في معالجة او التحصن ضد القرصنة فالمعلن هو اقل بكثير من الرقم الحقيقي اذ ان هنالك حالة غريبة وهي ان معظم الشركات الخاصة الكبرى لا تعلن عن أي قرصنة ضدها على كثرتها ومعظمها لسرقة أبحاث ومعلومات والمعلن للمتتبعين هو في معظمه قرصنة ضد مؤسسات الدولة كالصحة في بريطانيا , دائرة الضرائب في أوكرانيا الدفاع في أمريكا وغيره الكثير.

الموضوع الغريب الاخر هو الاستهانة وقلة الاستثمار الحقيقي في الدفاعات خاصة من الشركات الكبرى وطبقا لوجهة نظرهم أذ يؤمنون أن تصحيح الوضع وتغيير المعلومات بعد كل هجوم هو أرخص بكثير من الاستثمار في الدفاعات الحقيقية ولكن الكثير منهم بدأ يعي الحقيقة المؤلمة ان القرصنة تكلفه الكثير الكثير.

بدأت حكومات الدول الكبرى بالعمل لإيجاد حلول للحد من هذه الظاهرة وأول ما بدأت به هو محاولة التفاهم فيما بينها واهم المحاولات كانت خلال مؤتمر ال G7 للدول الصناعية السبع الكبرى وبعده خلال مؤتمر ال G20 للعشرين دول صناعية كبرى وتم الاتفاق للحد من ظاهرة القرصنة الممولة من الحكومات ولكن هكذا اتفاقات لا تمنع القرصنة ولم تثبت جديتها لحد الان , من باب أخر حاولت أمريكا أن تكون رائدة في هذا الموضوع عبر اقتراحها التحالف مع شركات الانترنت الكبرى للعمل على الحد من هذه الظاهرة عبر التعقب وجمع المعلومات ولكن هذا أيضا اصطدم بممانعة الشركات للتعاون مع الحكومة لأسباب مختلفة منها سياسات الشركة فيما يخص المعلومات الموجودة على شبكتها ومشاركة المعلومات مع الحكومة وحتى موقف الشركات السياسي من الإدارة الامريكية هذا بالإضافة الى المنافسة الشديدة التي بينهم.

أذا ما ألحل؟
يعتقد كثير من الخبراء أن أحسن طريقة للدفاع هي الهجوم وكذلك القوانين الصارمة والرادعة ويمكن اختصار هذه الحلول كما يلي:

أولا: المبادرة بعمل هجوم سبراني على القراصنة سوآءا دول او افراد لشل قابلياتهم.

ثانيا: تشريع قوانين صارمة للقرصنة المحلية تمتد الى فترات سجن طويلة.

ثالثا: تشريع قوانين صارمة ضد الدول او الشخاص الأجانب تتضمن اعتبار أي هجوم سبراني معادل الى هجوم فيزيائي حقيقي فأن تسبب أي هجوم بضرر سوآءا للشركات او الافراد فيجب معاقبة الجهة المعتدية حسب الضرر ويتضمن ذلك العمل لجلبهم للعدالة والمقاطعة الاقتصادية والسياسية وحتى مهاجمتهم بالأسلحة التقليدية.

رابعا: العمل على تثقيف الحكومة والشركات والافراد على أهمية الحماية وكيفية الاستثمار الصحيح في الحماية التكنولوجية وعلى انسب الطرق لخزن المعلومات او مشاركتها وكذلك كيفية التعرف على حدوث أي قرصنة وكيفية التعامل معها .

خامسا: بادرت المملكة المتحدة قبل سنتين بتأسيس مركز معني بالحماية التكنولوجية اسمته " National Cyber Security Centre " يعمل على دراسة وتطبيق افضل الطرق لحماية مؤسسات الدولة والافراد من أي هجوم سبراني مع العلم أن هذا المركز مستقل كليا وتابع لجهة عليا واحدة وبإمكانيات وصلاحيات كبيرة وعلى الدول التي تخاف على مصالحها التفكير جديا بهكذا مراكز.

سادسا: العمل مع الجامعات والمعاهد والمنظمات للاستثمار في الشباب المتفوقين تكنولوجيا لبناء جيش من العلماء يحمون البلد من أي هجوم ويقومون بتطوير منظومة الحماية للمجتمع كله.

يجب أن لا يخفى عن انظارنا ان هنالك اشخاص ومنظمات تعمل وتخطط لأعمال اكبر مما سمعناه لحد ألان فمثلا عند التحقيق مع عدة افراد متهمين بالقرصنة في أمريكا صرح احد المتهمين بانه لديهم الامكانية والقدرة ان يدفعوا بمنظومة الانترنت الى توقف كامل في أي دولة في اقل من ساعة وهنا ومن امثال هؤلاء تكمن الخطورة.

متى نستيقظ لحماية بلدنا وشعبه ومؤسساته؟؟. سؤال الى المسؤولين .....

مصعب الشيخ علي