المستقبل
للأبحاث والدراسات المتقدمة

اسم الموضوع : :السيناريو الكارثي

عنوان الموضوع : متى تتحول الحرب السيبرانية إلى حرب شاملة؟

تاريخ النشر : 03/01/2022

اسم الكاتب : د. شادي عبدالوهاب

الموضوع :

حذر الرئيس الأمريكي، جو بايدن، في أواخر يوليو 2021، من أن الهجمات السيبرانية يمكن أن تتصاعد إلى حرب شاملة مع تصاعد التوتر بين واشنطن من جانب، وكل من روسيا والصين من جانب آخر، بسبب سلسلة من حوادث القرصنة السيبرانية التي استهدفت الوكالات الحكومية والشركات والبنية التحتية الأمريكية. وفي عام 2011، أعلنت وزارة الدفاع الأمريكي أن الهجمات السيبرانية تعتبر "عملاً من أعمال الحرب" وتستوجب "الرد العسكري"، غير أن هذا التهديد لم ير تطبيقاً عملياً حتى الآن.تصاعد استهداف البنية التحتية الحيوية: أضحت التفاعلات السيبرانية العدائية تفرض تهديداً متزايداً على البنية التحتية الحيوية للدول، وهو ما يثير المخاوف بأن تتسبب في اندلاع صراع شامل بين دولتين، خاصة مع تصاعد وتيرة تلك الهجمات واتساع تأثيرها، ومن أهم الأمثلة على ذلك ما يلي: 1- الهجوم على خط أنابيب كولونيال الأمريكي: تعرضت الولايات المتحدة، في مايو 2021، لهجوم سيبراني استهدف "خط أنابيب كولونيال" الذي يحمل البنزين ووقود الطائرات المكرر، ويعمل على تلبية احتياجات الطاقة للمستهلكين في المنطقة الشرقية من الولايات المتحدة، من هيوستن في تكساس إلى ميناء نيويورك، وهو ما أجبرها على إغلاق شبكتها، والتي تخدم حوالي 50 مليون مستهلك في جنوب وشرق الولايات المتحدة . وكانت الولايات المتحدة قد تعرضت لهجمات مماثلة سابقة، وحملت إدارة بايدن روسيا مسؤولية الهجمات وفرضت على موسكو عقوبات مالية وطردت دبلوماسيين ، ومن المحتمل أن تكون موسكو متورطة في هذه الهجمات، خاصة أن الرئيس الأمريكي، جو بادين، على الرغم من نفيه تورط روسيا في الهجمات، فإنه أكد أنه يقع على عاتقها مسؤولية لمواجهة الهجمات السيبرانية التي تنبع من أراضيها . 2- الهجمات الإيرانية – الإسرائيلية المتبادلة: ففي 26 أكتوبر من عام 2021، أدى هجوم إلكتروني على نظام توزيع الوقود في إيران إلى شلل محطات الوقود في البلاد البالغ عددها 4300 محطة، والتي استغرقت 12 يوماً لاستعادة الخدمة بالكامل، وهو ما ردت عليه إيران بشن هجوم على منشأة طبية إسرائيلية كبرى. كما اتهمت إيران بمحاولة شن هجوم على نظام المياه الإسرائيلي في 2020، ما تسبب في عطل محدود، وهو ما ردت عليه تل أبيب عبر شن هجوم على البنية التحتية لميناء بندر عباس، ما تسبب في توقف أجهزة الكمبيوتر في الميناء عن العمل، وترتب عليه اصطفاف السفن أمام ميناء الشهيد رجائي لأميال.ومن الملحوظ أن هدف الهجمات الإسرائيلية ضد إيران هو خلق حالة من الفوضى والغضب الشعبي وإثارة الاضطرابات والاحتجاجات المجتمعية على نطاق واسع. فقد توقفت محطات الوقود فجأة عن العمل ووجهت رسالة رقمية للعملاء تطالبهم بتقديم شكوى إلى المرشد الأعلى لإيران، آية الله علي خامنئي، مع عرض رقم هاتف مكتبه. كما سيطر المتسللون على اللوحات الإعلانية في مدن مثل طهران وأصفهان، واستبدلوا الإعلانات بالرسالة "خامنئي، أين البنزين الخاص بي؟" .وفي المقابل، قامت طهران بشن عمليات انتقامية ضد الضربات الإسرائيلية السيبرانية المتكررة في محاولة لتأكيد قدرتها على تهديد الأمن الإسرائيلي، ومحاولة وقف الهجمات الإسرائيلية السيبرانية ضدها.كوابح الحرب الشاملة: يتمثل القاسم المشترك في الهجمات الأخيرة في أنها باتت أكثر عدوانية، وتركز على البنية التحتية الحيوية التي تخدم قطاعاً واسعاً من المدنيين. وعلى الرغم من ذلك، فإن هناك عدداً من العوامل التي تتسبب في منع تحول الحرب السيبرانية، في مستواها الحالي، إلى حرب شاملة بين الدول، وهو ما يمكن توضيحه على النحو التالي: 1- القابلية للإنكار: لا شك أن القابلية للإنكار تساعد على ضبط التفاعلات الصراعية في الفضاء السيبراني وتريث الدول قبل أن تقوم بشن هجمات سيبرانية انتقامية يترتب عليها تصاعد التفاعلات العدائية إلى مستوى الحرب بين الدول. ويقصد بالقابلية للإنكار هو صعوبة تيقن الدول من هوية الطرف المهاجم، إذ تتسم الحروب السيبرانية بأنها ذات طبيعة خاصة، حيث يتم شن الهجمات بشكل عام دون أن يعلن أي طرف مسؤوليته عنها، لذا، فإنه في الغالبية العظمى من الحالات، يصعب تحديد مصدر الهجوم .ويلاحظ أن إنكار أو إخفاء هوية المجموعة التي تقف وراء الهجوم السيبراني يتم أحياناً تضمينها في البرامج التي يتم استخدامها في الهجوم السيبراني. فعلى سبيل المثال، قد تمت برمجة برنامج ستاكس نت، والذي تم توظيفه في مهاجمة أجهزة الطرد المركزي الإيرانية، بحيث يمتلك القدرة على محو آثاره بشكل ذاتي، وهو ما حال دون تحديد ومعرفة هوية الطرف المهاجم حتى بعد رصد إيران لما يعرف بفيروس ستاكس نت وتحليلها .كما أنه بات يصعب على الدولة التمييز بين الهجمات التي تشنّها الدول والجماعات الإجرامية بالاستناد إلى طبيعة الهجوم. ففي الماضي، كانت العصابات السيبرانية توظف برامج الفدية، وذلك للحصول على أموال بصورة غير مشروعة، بدلاً من جمع المعلومات الاستخباراتية أو التسبب في ضرر عبر السيطرة على أنظمة التحكم الصناعية، والتي عادة ما يتورط في هذه النوعية من الهجمات الجماعات السيبرانية المرتبطة بالدول. ومع ذلك، فإنه منذ عام 2019، توسعت هجمات برامج الفدية لتشمل الهجمات التي وفي أوائل عام 2020، حذرت وكالة الأمن السيبراني وأمن .(Ekans) "تركز بشكل أقل على تشفير البيانات، وأكثر على تعطيل أنظمة التحكم الصناعية مع تطور برنامج الفدية "إيكانز من شن مثل هذه الهجمات على خط أنابيب الغاز الطبيعي . ومن ناحية أخرى، فإنه على الرغم من أن جماعات الفدية السيبرانية تقوم بشن هجماتها لأغراض (CISA) البنية التحتية المتورطة في الهجوم على خط أنابيب ،(DarkSide) "إجرامية، أو تحقيق الربح المادي، فإن أهدافها في النهاية تصب في صالح دول بعينها. فعلى الرغم من تأكيد جماعة "دارك سايد كولونيل، بأنها "جماعة غير سياسية، وليس لها صلة بالاعتبارات الجيوسياسية، وأنه ليست هناك حاجة إلى ربطها بحكومة محددة"، فإن أهدافها تتسق مع الأهداف الروسية الرامية إلى إظهار عجز الحكومة الأمريكية عن مواجهة هجوم سيبراني، والذي تسبب في ارتفاع أسعار الجازولين في المناطق المتضررة لأعلى مستوى في ست سنوات ونصف . وعلى الجانب الآخر، فإن بعض الهجمات السيبرانية التي تتورط فيها بعض الدول يكون الهدف منها، بالإضافة إلى إثارة الفوضى، هو توليد أرباح. ومن ذلك "مجموعة لازاروس"، والتي تتهمها وهي وحدة استخبارات عسكرية تابعة لكوريا الشمالية. فقد قامت المجموعة بلعب دور في هجوم الفدية المدمر الذي شنّته كوريا ،(Lab 110) "واشنطن بأنها تعمل لصالح "المخترب 110 والذي تسبب في شلل 300 ألف جهاز كمبيوتر في 150 دولة. كما تورطت المجموعة نفسها في هجوم سيبراني ،(WannaCry) "الشمالية في عام 2017، والمعروف باسم "واناكراي في عام 2016 على بنك بنجلاديش وسرقة ما قيمته 81 مليون دولار . وتوضح الأمثلة السابقة أنه يصعب التمييز بين الهجمات التي تتورط فيها دول، وتلك التي تشنها جماعات إجرامية لغرض توليد أرباح مادية بشكل غير مشروع.2- الردع النشط في الفضاء السيبراني: يلاحظ أن هناك صعوبة حقيقة في تطبيق الردع في الفضاء السيبراني، بسبب صعوبة تحديد هوية الطرف المهاجم، حيث باتت الدول تواجه معضلة أساسية في مجال ردع الهجمات السيبرانية، إذ إن توجيه دولة ضربة سيبرانية انتقامية رداً على هجوم تعرضت له قد يترتب عليها استهداف دولة بالخطأ لم تكن تورطت في مهاجمتها سيبرانياً من الأساس، وهو ما يفتح الباب أمام التصعيد بالخطأ، في حين أن عدم رد الدولة المستهدفة سوف يجعل هناك اعتقاداً سائداً بأن هذه الدولة ضعيفة، بما يغري بزيادة الهجمات السيبرانية ضدها ، كما في حالة الولايات المتحدة وروسيا.وفي حالات أخرى، تتجه الدول إلى الرد، حال تأكدها بتورط دولة معينة، عبر تنفيذ هجمات سيبرانية تستهدفها، وتكون عادة بالقوة نفسها، أو مكافئة لقوة الهجوم السيبراني الذي تعرضت له بهدف التأكيد على قدرتها على إحداث أضرار سيبرانية، ومن ثم ردع خصمها عن مواصلة التصعيد ضدها، كما في حالة الهجمات السيبرانية المتبادلة بين إسرائيل وإيران، والتي أخفقت، حتى الآن، في وقف الهجمات السيبرانية بينهما. ويساعد على تنفيذ الهجمات السيبرانية المتبادلة حقيقة أنه يستحيل على أي دولة من الدول التعرف على الثغرات الموجودة في أنظمتها، وهو ما يتيح للطرف المهاجم استغلال هذه الثغرات في شن الهجمات. (Titan) "وعلى سبيل المثال، فإنه في عام 2007، اكتشفت الحكومتان الأمريكية والبريطانية عن عملية اختراق واسعة لأجهزتهم منذ العام 2002، وكانت تعرف باسم "تيتان راين وهي الهجمات التي يعتقد أن الصين كانت متورطة فيها. 3- محاولة ضبط التفاعلات العدائية: تتجه الدول، في بعض الأحيان، إلى محاولة وقف الهجمات السيبرانية عبر محاولة ، (Rain التوصل إلى تفاهمات ثنائية مع خصومها. ففي قمة يونيو في جنيف، حذر بايدن شخصياً بوتين من أن الولايات المتحدة "سترد عبر السيبر" إذا استهدفت الدولة الروسية أو المتسللون المقيمون في روسيا البنية التحتية الأمريكية الحيوية. وتمثلت القطاعات التي حذر بايدن بوتين من استهدافها في الطاقة والرعاية الصحية وتكنولوجيا المعلومات والمرافق التجارية، والنقل والخدمات المالية والمواد الكيميائية.واتهمت إدارة بايدن روسيا والصين، أو المتسللين الموجودين داخل البلدين، بتنفيذ بعض الهجمات. وحذر المسؤولون الأمريكيون من أن واشنطن سترد بـ "مزيج من الأدوات المرئية وغير المرئية"، لكن الهجمات السيبرانية استمرت من دون توقف ، وإن على مستوى أقل حدة، وهو ما يفتح الباب أمام إمكانية توصل الدول لتفاهمات

مستقبلاً يحكم الهجمات السيبرانية بين الدول. 4- تجنب الهجمات السيبرانية حافة الحرب: يلاحظ أن معظم الهجمات السيبرانية يتم شنّها بحيث تبقى دون مستوى التخريب أو الدمار، الذي يمكن أن يتسبب في اندلاع الصراع المسلح، وذلك لتجنب تصعيد الحرب إلى صراع تقليدي شامل. ولذلك يمكن القول إن الحروب السيبرانية، شديدة التدمير، لم تشن، حتى الآن ، وهو ما يعرف أحياناً كذلك باسم "الحروب السيبرانية الاستراتيجية". ومع ذلك، فقد خططت القيادة السيبرانية الأمريكية إلى شن هجوم سيبراني استراتيجي على إيران. وتم كشف هذه الخطة في ووضعت الولايات المتحدة خطة مفصلة لشن هجوم سيبراني على إيران في حالة فشل الجهود الدبلوماسية للحد .(Nitro Zeus) "عام 2016. وعرفت هذه العملية باسم "نيترو زيوس من برنامجها النووي وأدى إلى اندلاع صراع عسكري. وكانت العملية "نيترو زيوس" مصممة لتعطيل شبكة الدفاع الجوي الإيرانية، ونظم الاتصالات، والأجزاء الحساسة من شبكة الطاقة. وقد تم التراجع عن التجربة في يوليو 2015، بعد إبرام الاتفاق النووي بين إيران والدول الست الكبرى. ومثل ستاكسنت، يعتقد أن التخطيط لعملية "نيترو زيوس" قد استغرق سنوات من الإعداد والاستطلاع والمحاكاة واختبار البرامج الضارة. ومن المرجح أن يُنظر إلى مثل هذا الهجوم السيبراني الاستراتيجي الواسع النطاق على أنه استخدام للقوة في العلاقات الدولية، وبالتالي من المحتمل أن يتصاعد إلى صراع تقليدي في المنطقة . وكانت التقارير الصحفية عن العملية غير واضحة حول طبيعتها، وما إذا كانت تمثل عملية استراتيجية قائمة بذاتها من شأنها إغلاق كل النظم الإيرانية "دون إطلاق رصاصة واحدة"، أو أنها بمنزلة ضربة أولى استباقية لحرب تالية، إذ إن كلا السيناريوهين يتمتعان بقدر من المعقولية . ولذلك، فإنه تحسباً للاحتمال الثاني، فإن شن مثل هذا الهجوم كان سوف يستتبعه استعداد من جانب الجيش الأمريكي للدخول في حرب تقليدية ضد إيران، خاصة إذا ما اتجهت الأخيرة لاستهداف القواعد الأمريكية والبنية التحتية الحيوية بعد تعرضها للهجوم السيبراني.5- محدودية الحروب السيبرانية حتى الآن: يجادل المنظرون العسكريون المشككون في محورية الدور الذي تلعبه الحروب السيبرانية أن فائدتها الاستراتيجية محدودة، إذ لا يمكن توظيف الحروب السيبرانية بشكل فعال لتحقيق عنصرين أساسيين من عناصر الحرب، وهما نزع سلاح القوات التقليدية للعدو أو إضعافها بشكل دائم، أو احتلال إقليم والسيطرة عليه .ومن جهة أخرى، فإنها تعاني مشكلة أخرى، وهي أن البرامج الضارة تكون معدة للاستخدام ضد دولة معينة، فهي لا يمكن استخدامها ضد جميع الدول بالضرورة، كما أن فترة استخدامها تكون محدودة كذلك، وذلك بخلاف الأسلحة التقليدية، إذ إن الصواريخ يتم تصنيعها، وتكون قابلة للاستخدام خلال فترة زمنية تمتد إلى ثلاثين عاماً، في حين أن الثغرات الأمنية في النظم التي يتم استهدافها يكون عمرها قصيراً، وبالتالي قد لا تكون صالحة للتخزين، حتى موعد شن الحروب التقليدية في مجال التفاعلات السيبرانية هو وقوع هجوم سيبراني هائل على البنية التحتية الحيوية (Doomsday scenario) بالضرورة . سيناريوهات "يوم القيامة": يقصد بسيناريو يوم القيامة في دولة معينة، مما يجعله يتسبب في مقتل عدد كبير من الأفراد، الذين تعتمد حياتهم على هذه البنية التحتية. وعلى الرغم من أن القسم السابق أوضح وجود كوابح على شن مثل هذه النوعية من الهجمات، فإنها لا تمنعها تماماً. وكما سبقت الإشارة، كانت الولايات المتحدة تستعد لشن هجوم سيبراني استراتيجي على إيران في السابق، وهو ما يعني أن الدول باتت تضمن مثل هذه الهجمات السيبرانية في حساباتها للتفاعلات العدائية. ولذلك، فإنه مع استمرار تطور القدرات السيبرانية لعدد كبير من الفاعلين، سواء من الدول أو من الجماعات الإجرامية، وامتلاكهم للقدرة على التلاعب بالبنية التحتية الحيوية، فإن فرص تحول الحرب السيبرانية الاستراتيجية إلى حرب شاملة يظل قائماً. ويمكن تحديد الحالات التي يمكن فيها تحوّل الحرب السيبرانية إلى حرب شاملة: 1- استهداف البنية التحتية الحيوية: يلاحظ أن أحد الأمور التي سوف تحوّل المواجهات السيبرانية العدائية إلى حرب شاملة بين دولتين هو في حالة استهداف البنية التحتية الحيوية للدولة، وتسببها في خسائر فادحة، أو دمار كبير. ومن الأمثلة على ذلك الهجمات على الشبكة الكهربائية التي تؤدي إلى انقطاع التيار الكهربائي بشكل كامل عن دولة معينة، أو الهجمات على النظام المالي التي تؤدي إلى خسائر اقتصادية أو انهيار اقتصادي كامل، أو الهجمات على نظام النقل مما يؤدي إلى اصطدام الطائرات والقطارات، أو الهجمات على السدود التي تؤدي إلى فتح بوابات السدود، أو الهجمات ضد محطات الطاقة النووية، والتي تؤدي إلى انصهارها . وعلى الرغم من أنه ليست هناك مؤشرات على حدوث مثل هذه النوعية من الهجمات بعد، فإن مثل هذا السيناريو قريب الحدوث. ففي ديسمبر 2014، أعلنت شركة كوريا الجنوبية للطاقة المائية والنووية أن أنظمة الكمبيوتر لديها تعرضت لاختراق سيبراني، لكن لم تؤخذ منها سوى بيانات غير حساسة، غير أنه لم يعثر على أي فيروس ضار في وحدات التحكم بالمفاعلات ، وهو ما يعني أن الهجوم لم يصل بعد إلى مرحلة التحكم في المفاعلات، أو التأثير على عملها، بصورة قد تتسبب في حدوث تسرب، أو انفجار نووي. ولكن في حالة استمرار وتنامي الهجمات السيبرانية، ونجاحها في التحكم في عمل المفاعلات، فإن مثل هذا التهديد سوف يفتح الباب أمام اندلاع حرب شاملة بين دولتين. 2- شن هجمات تقليدية وسيبرانية متزامنة: يلاحظ أن مثل هذا السيناريو لا يعد مستبعداً، إذ إنه يتوقع في أي معارك مستقبلية أن تتم المزامنة بين شن الهجوم السيبراني والهجمات العسكرية التقليدية، وهو السيناريو الأسوأ الذي تستعد له أغلب الدول حول العالم. 3- تعطيل مرافق البنية التحتية الحيوية كافة: يقوم هذا السيناريو على قيام دولة أو عدة دول بشن هجمات سيبرانية منسقة ومتزامنة تتسبب في انهيار الشبكة الكهربائية وفشل خطير في إمدادات الطاقة، مما يؤدي إلى توقف المستشفيات والقطارات والطائرات والنظام المالي عن العمل في غضون فترة زمنية قصيرة لا تزيد على خمس عشرة دقيقة، من دون أن يقوم إرهابي واحد أو جندي واحد بشن هجوم يستهدف هذا البلد" .ويلاحظ أن مثل هذا السيناريو يحتاج إلى قدرات سيبرانية متطورة، بالإضافة إلى القدرة على مراقبة النظم الحيوية للخصم في مختلف القطاعات لشن هجمات متزامنة تستهدفها جميعاً في الوقت نفسه، وهو أمر صعب الحدوث. ومع ذلك، فإن مثل هذا السيناريو سيكون تطبيقاً عملية لمقولة صن تزو، المنظر العسكري الصيني، والذي أكد أن "تحقيق مائة انتصار في مائة معركة ليس أبرع ما يقوم به القائد، ولكن السيطرة على العدو من دون قتال هو الأبرع على الإطلاق". وفي الختام، يمكن القول إن امتلاك مزيد من الفواعل، سواء من الدول، أو جماعات الجريمة المنظمة للقدرات السيبرانية المتطورة التي تؤهلها لشن هجمات سيبرانية تخترق نظم التحكم الصناعي سوف يعمل كعامل محفز للصراعات في عام 2022، وصولاً إلى إمكانية شن هجمات لتهديد وشل البنية التحتية الحيوية، التي تعتمد عليها القطاعات المدنية والجيوش على حد سواء، وذلك ما لم تقم الدول بالاتفاق فيما بينها على .وضع اتفاقية تنظم التفاعلات في الفضاء السيبراني