Deterrence by Resilience:

إمكانيات تحقيق الردع في صراعات الفضاء الإلكتروني

إيهاب خليفة

منسق برنامج التطورات التكنولوجية بمركز المستقبل للأبحاث والدراسات المتقدمة

على الرغم من صعوبة ردع الهجمات الإلكترونية نتيجة صعوبات تحديد هوية الفاعلين ومعالجة الثغرات، فضلاً عن امتلاك "أسلحة إلكترونية" نوعية تضاهي السلاح النووي، فإن الردع بالاستيعاب قد يتحقق من خلال نظم الإنذار المبكر ووسائط البيانات الاحتياطية وتشفير البيانات الرئيسية، مما يقلص من إمكانية حدوث هجمات إلكترونية تهدد مصالح الدولة.

أولاً: تحولات المفاهيم الاستراتيجية التقليدية

ساهمت الابتكارات التكنولوجية الحديثة خاصة في مجال الفضاء الإلكتروني في تغير الأفكار التقليدية للحروب، وغيرت من الأشكال التقليدية للقوة، وأدخلت مفاهيم جديدة لم تكن موجودة من قبل، وأعادت صياغة مفاهيم قديمة، وظهر نوع جديد من القوة هو القوة الإلكترونية (Cyber Power)، يعمل بجانب الأشكال التقليدية للقوة سواء كانت الصلبة أو الناعمة، وأصبحت من أهم أدوات تحقيق السياسة الخارجية للدول، بل والسياسات الداخلية أيضاً، ويقصد بها قدرة الفاعل – سواء كان دولة أو فواعل من غير الدول، مثل الحركات الإرهابية والتنظيمات الإجرامية والأفراد وغيرهم - على استخدام وسائل التكنولوجيا الحديثة والاتصالات لتحقيق أهداف معينة عبر شبكات الكمبيوتر والإنترنت، قد تشمل سرقة بيانات مهمة أو تدميرها أو تعديلها أو إغلاق نظم إلكترونية أو إعادة ضبطها، هذه النظم قد تكون مدنية أو عسكرية، شخصية أو عامة.

وأصبح الحديث عن الحروب الإلكترونية بمنزلة خبر يومي في معظم المواقع والصحف الإخبارية، فالحديث عن الفيروسات والهجمات الإلكترونية يتزايد، سواء كانت هذه الهجمات تستهدف دولاً أو شركات أو أفراداً، ولعل النموذج التقليدي في ذلك، تبادل الاتهامات بين الحكومتين الأمريكية والصينية، حول قيام الصين بشن هجمات إلكترونية ضد قطاعات صناعية ومالية أمريكية بهدف سرقة براءات اختراع أو معلومات تجارية مهمة.

واستطاعت الدول صغيرة الحجم قليلة السكان التي ليس لها وزن استراتيجي في المعارك العسكرية، أن تضع دولاً كبرى في تهديد مباشر، حيث تستطيع دولة صغيرة مثل إسرائيل لديها قدرات تكنولوجية متقدمة، وأسلحة إلكترونية معقدة، تهديد دولة كبرى لها وزن عسكري واستراتيجي، ولكن لكي يتحقق ذلك لابد من أن تدرك هذه الدول الصغيرة الأهداف الحيوية للدول الكبرى في الفضاء الإلكتروني، حتى تستطيع إصابتها إصابة مباشرة.

ومن هنا ظهرت الحاجة إلى تطوير استراتيجيات جديدة، تتلاءم مع العصر السيبري (Cyber Age) الذي اختلفت فيه حسابات القوة والردع والحرب، ذلك العصر الذي يعتبر الإنترنت هو الإطار العام الحاكم لتفاعلاته كافة، سواء كانت شخصية أو عامة، عسكرية أو سياسية، اقتصادية أو اجتماعية، فتمت إعادة تعريف مفهوم الحرب ليظهر شقها الإلكتروني، وظهر شكل جديد من أشكال القوة هو القوة الإلكترونية، وتمت إعادة صياغة مفهوم الردع ليشمل الردع الإلكتروني (Cyber Deterrence) باعتباره من الأدوات الرئيسية في منظومة التوازن الاستراتيجي، والتي قد تمنع قيام حرب إلكترونية عالمية، يكون الضحايا فيها من المدنيين قبل العسكريين، وتصيب البنى التحتية المدنية قبل العسكرية، وتتسبب في انهيار دول بأكملها، ولكن هناك صعوبات حقيقية في تحقيقه.

ثانياً: إعادة تعريف مفهوم الردع

الردع بصفة عامة هو منع الخصم من القيام بفعل عدائي، إما بسبب تخوفه من هجوم مضاد يفوق قدراته الدفاعية، أو ارتفاع تكلفة الهجوم مقارنة بالمكاسب التي يمكن أن يحققها ، فيما يُعرف بردع الخطر برفع تكلفة الهجوم وتقليل فوائده، تحقيق الردع يتطلب مكونين رئيسيين، نوايا معبر عنها من الطرف الأول برغبته في الدفاع عن مصلحة ما من ناحية، وإدراك الطرف الثاني أن التعارض مع الطرف الأول حول هذه المصلحة سوف يكون مكلفاً له من ناحية أخرى، بصورة تمنعه من اتخاذ أي موقف عدائي نحوه، وهنا يتحقق الهدف الرئيسي من الردع هو جعل الطرف الثاني سلبياً تجاه الطرف الأول، أي لا يقوم بأخذ أي موقف هجومي نحوه، فهو سعي نحو البقاء على الحالة (status quo).

والردع نوعان هما ردع بالمنع أو الردع السلبي والردع بالانتقام أو الردع الإيجابي، ويحدث الردع بالمنع من خلال تقوية النظم الدفاعية بصورة ترفع تكلفة هجمات الخصم عن مكاسبه، وغالباً لا يكون الهدف الرئيسي هنا هو الردع بقدر ما يكون هو الدفاع والتأمين ضد أي عدو محتمل وليس عدواً محدداً بعينه، وهنا تكون حسابات الخصم بالسالب، أي أن يدرك ارتفاع تكلفة الهجوم عن المكاسب التي يمكن أن تتحقق، أما الردع بالانتقام فهو ردع إيجابي يقوم على فكرة العقاب، وفيه يدرك الخصم أن أي هجوم سيتبعه هجوم آخر انتقامي لا يستطيع تفاديه أو تحمله، ويشمل ذلك الإعلان عن المصالح الحيوية واستعراض القوة والتهديد باستخدامها في حالة المساس بها .

ويقصد بالردع الإلكتروني قدرة الدولة على تطوير قدرات عسكرية موثوقة ومتبادلة ومتماثلة على الفضاء الإلكتروني تكون قادرة على التأثير على قرارات الخصم وتمنعه من شن هجمات عسكرية عبر الفضاء الإلكتروني عليها .

يتشابه الردع بصفة عامة مع الردع الإلكتروني في عدة نقاط، منها صعوبة تطبيق القانون في العلاقات العابرة للحدود، حيث يتميز الفضاء الإلكتروني بعدم وجود حدود جغرافية له توضح سيادة الدول عليها، ولما كانت الأسلحة المستخدمة في الفضاء الإلكتروني غير محددة سلفاً وتخضع للتطور التكنولوجي، وغالباً ما تظهر الهجمات نتيجة ثغرات تم اكتشافها، ومن ثم فإنه يصعب حصر هذه الأسلحة لمنع أو تقنين استخدامها .

ثالثاً: صعوبات تحقيق الردع في الفضاء الإلكتروني

يعتبر الردع النووي النموذج التقليدي لفهم ودراسة الردع، فالقاعدة الرئيسية تقول إنه كلما زادت القوة التدميرية للسلاح، قل الميل إلى استخدامه، فالدول التي تمتلك سلاحاً نووياً لا تميل إلى استخدامه أو التلويح باستخدامه لتسويه الصراعات بينها، نظراً للقدرة التدميرية العالية للسلاح، وسهولة تتبع الخصم وإلحاق نفس مقدار الأذى به، ومن ثم ترتدع الدول عن استخدامه، ولكن هذا لا ينطبق على الردع في الفضاء الإلكتروني، وذلك لأن البيئة التي يعمل فيها الإنترنت مختلفة تماماً، ويتضح ذلك في الآتي:

1- صعوبة معرفة الطرف المعتدي: لكي يكون الردع ناجحاً لابد من توافر ثلاثة عناصر رئيسية هي التتبع (attribution)، والتواصل (signaling)، والمصداقية(credibility) ، ويقصد بالتتبع القدرة على معرفة مصدر الهجمة، من أين تأتي؟، سواء كان دولة محددة أو فاعل محدد، وفي نفس الوقت القدرة على إرسال رسالة إلى الجمهور المستهدف، بأن هناك مصلحة معينة لا يجب التعارض عليها، والمصداقية، أي في حالة الإعلان عن مصدر الهجمة لابد من أن يكون هناك رصيد كاف لدى الجمهور لتصديق هذا الإعلان ، وبالتطبيق على الفضاء الإلكتروني نجد صعوبة تحقيق العناصر الثلاثة السابقة وذلك كالتالي:

أ- التتبع: على الرغم مما وصلت إليه التكنولوجيا من تقدم في عملية التتبع، فإنها تتقدم أيضاً في عمليات التمويه والإخفاء، بصورة تجعل معرفة مصدر الهجمة شبه مستحيل، إلا في حالة الهجمات الصغيرة البسيطة التي يرتكب أصحابها أخطاء، وليس في حالة الهجمات المعقدة التي تقوم بها دول، فمثلاً الهجمات الروسية على استونيا عام 2007، والهجمات الأمريكية الإسرائيلية على المفاعل النووي الإيراني عام 2010، والهجمات الكورية على شركة سوني عام 2015،

والرد الأمريكي بقطع الإنترنت عن كوريا لمدة 10 ساعات، جميع هذه الهجمات لم يتم تبني الهجوم صراحة من قبل الدول المعتدية، بل إن بعضها أنكر القيام بذلك من الأساس، على الرغم من توفر أدلة مرتبطة بالظروف السياسية وليس الفنية أو القانونية.

ب- المصداقية: فمعظم حالات الاختراق لا يتم الإعلان عنها من ناحية، ومعظم الدول تنكر الاتهامات الموجهة إليها بشن هجمات إلكترونية من ناحية أخرى، فالجميع يتهم والجميع ينكر، فمن أين تأتي المصداقية في الفضاء الإلكتروني الذي صمم على إخفاء هوية الطرف الآخر؟

ج- التواصل، فالفاعل غير معروف من الأساس لكي يتم التواصل معه، فالمصالح في الفضاء الإلكتروني متشابكة، فقد يكون دولة أو فرداً أو جماعة إرهابية أو تنظيماً إجرامياً أو غيره، ومن ثم يصعب إرسال الرسالة إلى الجمهور أو الفاعل المستهدف.

2- صعوبة وضع الخصم في تهديد حقيقي: الدول التي تتعرض لهجمات إلكترونية هي التي تستطيع أن تقدر مدى فداحة هذه الهجمات والخسائر المترتبة عليها، ومن ثم فقد تقوم دولة بشن هجوم إلكتروني انتقامي على دولة أخرى بهدف تحقيق الردع بالانتقام، وإمكانية إصابة أهداف معينة داخل الدولة.

وعلى سبيل المثال، يتضح ضعف القدرة على الردع في إطار الهجمات التي قامت بها كوريا الشمالية ضد شركة سوني للإنتاج السينمائي في الولايات المتحدة الأمريكية، وذلك على خلفية فيلم سينمائي أنتجته شركة سوني يسيء لرئيس كوريا الشمالية، وترتب عليها تسريب العديد من الإيميلات والأفلام الجديدة على الإنترنت، فكان رد الولايات المتحدة الأمريكية أنها شنت هجمات إلكترونية على كوريا الشمالية ترتب عليها قطع الإنترنت لمدة 10 ساعات تقريباً، إلا أن كوريا الشمالية لم تتأثر بسبب تدني اعتمادها على الإنترنت.

ولكي يمكن أن ينجح الردع بالانتقام من خلال شن هجمات إلكترونية، يجب معرفة الأهداف الحرجة للخصم المراد ردعه، ومصالحه الحقيقية داخل الفضاء الإلكتروني، حتى يكون الهجوم فعالاً، وحتى يحقق الردع هدفه، ولذلك فهناك علاقة طردية بين تعدد الأهداف الإلكترونية التي يمكن إصابتها وبين الردع، فكلما تعددت الخدمات والنظم الإلكترونية الحرجة المتصلة عبر الإنترنت، كان الردع ناجزاً فعالاً، وكلما قلت هذه الخدمات والنظم، قلت فاعلية الردع الإلكتروني.

3- صعوبة منع الهجمات الصفرية: يتميز الفضاء الإلكتروني بالتحديث التكنولوجي المستمر، فبصورة يومية يتم اختراع وتطوير فيروسات في معامل خاصة، لم يتم الكشف عنها ولم ترصدها شركات الأمن الإلكتروني، فبعضها يصيب المكون المادي (Physical)، وبعضها وهو كثير يهتم بالجانب البرامجي (Software)، وبعضها وهو أيضاً غير محدود يركز على المعلومات (Information) سواء بهدف السرقة أو التضليل أو التدمير.

كما أن هذه الفيروسات تستغل الثغرات الحديثة التي تظهر في الأنظمة قبل أن يتم تحديثها ومعالجتها، فيما يعرف بالهجمات الصفرية (Zero-day Attack) ومن ثم قد تظهر الثغرة اليوم وتستغلها بعض الفواعل لشن هجمة إلكترونية قبل أن يتم اكتشافها ومعالجتها من قبل الأجهزة المختصة، ومن ثم يفشل تحقيق الردع بالمنع، بسبب ثغرات أمنية في أنظمة الدفاع أو فيرس جديد تم تطويره.

> يمكن تطبيق مفهوم الردع بالاستيعاب من خلال إنشاء نظم إلكترونية حمائية، مثل الدروع الإلكترونية والشبكات المغلقة والقيام بعمليات اختبار دائمة للشبكات بهدف معرفة مواطن الضعف فيها والعمل على علاجها، بالإضافة إلى تدعيم مرونة أنظمة الدولة في التعامل مع الهجمات الإلكترونية، وتبني خطط بديلة دائماً، وأنظمة أخرى يمكنها أن تحل محل الأنظمة التي تتعرض لهجمات إلكترونية أو تخرج من الخدمة، واتباع مبدأ المصارحة والشفافية في المعلومات.

4- القيود القانونية الدولية: هناك جانب آخر قد يجعل عملية الردع عبر الفضاء الإلكتروني غير فعّالة، هذا الجانب قد يهم القانونيين والسياسيين أكثر من العسكريين، ألا وهو القيود القانونية الخاصة بمبدأ استخدام القوة في العلاقات الدولية وفقاً لميثاق الأمم المتحدة، حيث تنص المادة 2/ 4 من ميثاق الأمم المتحدة على منع استخدام القوة في العلاقات الدولية أو التهديد باستخدامها، إلا بما يتوافق ومقاصد الأمم المتحدة ، كما اشترطت المادة 51 من الميثاق ضرورة إبلاغ مجلس الأمن بأي تدابير هجومية سوف تتخذها الدولة في حالة الدفاع عن النفس، ولما كانت الهجمات الإلكترونية أحد أشكال استخدام القوة في العلاقات الدولية، أو التهديد باستخدامها، فإنه ينطبق عليها أحكام ميثاق الأمم المتحدة والقيود التي يفرضها، وهو ما قد يكون عائقاً أمام نجاح الردع الإلكتروني وفاعليته.

كما ينص "دليل تالين (Tallinn Manual) الخاص بالقواعد المنظمة للحروب الإلكترونية وتنظيم قواعد الاشتباك عبر الإنترنت أن العمليات الإلكترونية (Cyber Operations) والتي من شأنها استخدام أو التهديد باستخدام الهجمات الإلكترونية ضد إقليم دولة ما أو استقلالية نظام سياسي معين بما يتعارض مع ميثاق الأمم المتحدة، هي غير قانونية .

ولما كانت هناك صعوبة فنية في الأساس لتحديد الطرف المعتدي، فإن محاسبته قانونياً غير واردة، كما أن اتخاذ إجراءات حفظ الأمن والسلم الدولي من قبل مجلس الأمن والأمم المتحدة ضده غير واردة، ومن ثم فالهجمات

الإلكترونية سوف تستمر بصورة تجعل القول إن الردع الإلكتروني صعب في أفضل حالته وربما مستحيل.

رابعاً: آليات تحقيق "الردع بالاستيعاب"

يتضمن الردع بالاستيعاب تبني خطط واستراتيجيات للتعامل مع الهجمات الإلكترونية في حالة حدوثها، تشمل التخفيف من حدتها، وعدم تأثير البنى التحتية الحرجة والخدمات الرئيسية والمعلومات المهمة التي تشكل ركيزة للأمن القومي للدولة، ويتحقق ذلك من خلال الآتي:

1- إنشاء نظم إنذار مسبق ومجسات إلكترونية: بحيث تركز على حماية المرافق والبنية التحتية الحرجة التي يمكن أن تكون عرضة للهجمات الإلكترونية، وتساعد في اكتشاف الهجمة الإلكترونية فور وقوعها مباشرة، مما يسهل من عملية تفادي المخاطر التي يمكن أن تنجم عنها.

2- تعدد مصادر الطاقة داخل الدولة: فلا يجب أن تعتمد الطاقة داخل الدولة على عنصر واحد فقط، فمثلاً إذا تم استهداف شبكات الكهرباء، يجب أن تكون هناك مصادر بديلة ولو تقليدية لمنع انقطاع الكهرباء، خاصة عن المؤسسات المهمة والحيوية، كالمستشفيات والمحال التجارية الكبرى والمصانع وغيرها، بحيث تكون لديها نظم توليد كهرباء بديلة يمكن أن تعمل عليها.

3- إيجاد نظم إلكترونية بديلة للخدمات: فلا يجب الاعتماد على نظام إلكتروني واحد، في حالة تعرضه لهجمة إلكترونية تتوقف الخدمة عنه تماماً، مثل أنظمة البنوك والأنظمة المالية والخدمات المدنية الحكومية، هذه الأنظمة يجب أن تتعدد طرق الدخول إليها في حالة استهدافها من خلال أنظمة بديلة تعمل أوقات الطوارئ.

4- إنشاء Back up للبيانات المهمة: سواء كانت هذه البيانات تخص القطاع الحكومي أو القطاع الخاص، وذلك من خلال تبني استراتيجية شاملة لإنشاء نسخ احتياطية من بيانات مواطني الدولة، هذه النسخة يتم تحديثها بصورة يومية، من خلال مزامنة (Synchronizing) البيانات الموجودة بالأنظمة الإلكترونية في مختلفة المؤسسات، مع نظام أرشفة وحفظ البيانات الرئيسي، ومن ثم في حالة تدمير بعض البيانات جراء هجمات إلكترونية، تظل هناك نسخ احتياطية يمكن الرجوع إليها.

5- تشفير البيانات الرئيسية: وذلك من خلال تشفير البيانات الحرجة والمهمة، مثل البيانات العسكرية والمراسلات السرية، حتى إذا ما تعرضت لإحدى الهجمات الإلكترونية وتمت سرقتها، يصبح من الصعب على الطرف المعتدي فهم ما بداخلها، وحتى يكتسب الطرف المعتدى عليه بعض الوقت من أجل المناورة، إما باكتشاف هذا الطرف ومفاوضته، أو الإعلان المسبق عنها.

ومن ثم يجب على الدولة أن تعمل وفق استراتيجية شاملة للفضاء الإلكتروني، تشمل المؤسسات الحكومية والعسكرية إلى جانب القطاع الخاص والمجتمع المدني والأفراد، وتقوم على التوعية الكاملة بالتهديدات المحتملة القادمة من الفضاء الإلكتروني وكيفية التعامل معها، وإنشاء جهات مختصة قادرة على التعامل مع هذه التهديدات واكتشافها في وقت ومبكر.

وفي المجمل يمكن تطبيق مفهوم الردع بالمنع من خلال إنشاء نظم إلكترونية حمائية، مثل الدروع الإلكترونية (Cyber Shield) والشبكات المغلقة (Intranet)، والقيام بعمليات اختبار دائمة للشبكات (Cyber Drill) بهدف معرفة مواطن الضعف فيها والعمل على علاجها.

ويضاف لذلك إمكانية تطبيق مفهوم الردع بالانتقام من خلال تبني الموهوبين من الطلاب في مجال الكمبيوتر، وإنشاء قسم خاص في المؤسسات العسكرية للقراصنة الإلكترونيين، وشن هجمات إلكترونية ضارية على المشكوك في قيامهم بمهاجمة أنظمة ومؤسسات الدولة.

بالإضافة إلى ذلك يجب تطبيق مفهوم الردع بالاستيعاب من خلال زيادة مرونة أنظمة الدولة في التعامل مع الهجمات الإلكترونية، وتبني خطط بديلة دائما، وأنظمة أخرى يمكنها أن تحل محل الأنظمة التي تتعرض لهجمات إلكترونية أو تخرج من الخدمة، واتباع مبدأ المصارحة والشفافية في المعلومات، حتى وإن تمت سرقة معلومات وتسريبها، فإنها في النهاية تعكس توجه الدولة الحقيقي، ولا تمثل قيمة مضافة في عالم السياسية.

1- Clorinda Trujillo, The Limits of Cyberspace Deterrence, the Air War College, Air University, 2014. P 45

2- Martin C. Libicki, Cyberdeterrence andCyberwar, Santa Monica, CA: RAND, 2009. P7

3- Jason Rivera, Achieving cyberdetterence and the ability of small states to hold large states at risk, Architectures in Cyberspace, Cycon 2015, NATO Cooperative Cyber Defence Centre Of Excellence, May 2015, p7.

4- Tobias Metzger, Deterrence theory in the cyber-century, Research Division EU/Europe, 02, May 2015

5- Clorinda Trujillo, The Limits of Cyberspace Deterrence, the Air War College, Air University, 2014. P 45

6- انظر ميثاق الأمم المتحدة المادة الثانية الفقرة الرابعة.

7- دليل "تالين" هو وثيقة استرشادية غير ملزمة للدول، تم إعداده من قبل لجنة بحلف شمال الأطلسي عام 2013.

8- دليل تالين حول القانون الدولي المنطبق على الحرب السيبرانية – من إعداد اللجنة الدولية للخبراء بدعوة من مركز التميز للدفاع السيبراني التعاوني التابع لحلف شمال الأطلسي (الناتو)، مطابع جامعة كمبريدج، 2013، ص 45.