تحليلات وآراء

الهجوم كأفضل وسيلة للدفاع...
قراءة في التحول السيبراني الاستباقي لكوريا الجنوبية وتحالفها الاستراتيجي مع الولايات المتحدة

بقلم: نور نبيه جميل/باحثة في مركز حمورابي للبحوث والدراسات الاستراتيجية

مركز حمورابي للبحوث والدراسات الاستراتيجية

13 تموز 2025

تأسس مركز حمورابي للبحوث والدراسات الإستراتيجية عام 2008 بمدينة بابل (الحلة)، وحصل على شهادة التسجيل من دائرة المنظمات غير الحكومية المرقمة 1Z71874 بتاريخ 2012/12/25، بوصفه مركزا علميا بحثيا يهتم بدراسة الموضوعات السياسية والمجتمعية، فضلاً عن الاهتمام بالقضايا والظواهر الراهنة والمحتملة في الشأن المحلي والإقليمي والدولي، ويتعامل مع باحثين من مختلف التخصصات داخل العراق وخارجه، وتحتضن بغداد المقر الرئيسي للمركز.

- لا يجوز إعادة نشر أي من هذه الأوراق البحثية الا بموافقة المركز، وبالإمكان الاقتباس بشرط ذكر المصدر كاملا.
- لا تعبر الآراء الواردة في الورقة البحثية عن الاتجاهات التي يتبناها المركز وانما تعبر عن رأي كاتبها.
- حقوق الطبع والنشر محفوظة لمركز حمورابي للبحوث والدراسات الاستراتيجية.

للتواصل

العراق - بغداد - الكرادة

+964 7810234002

hcrsiraq@yahoo.com

www.hcrsiraq.net

مركز حمورابي للبحوث والدراسات الاستراتيجية

تحليل السياق الاستراتيجي

يشكل الفضاء السيبراني اليوم أحد أهم ساحات الصراع الاستراتيجي في النظام الدولي، حيث تحولت الهجمات السيبرانية من كونها أدوات تابعة للحروب التقليدية إلى تهديدات رئيسة تمس الأمن الوطني للدول بشكل مباشر. في هذا الإطار، أقدمت كوريا الجنوبية على إعادة تعريف إستراتيجيتها للأمن السيبراني عبر التحول من نهج تفاعلي إلى نهج استباقي للدفاع السيبراني. هذا التحول ليس منفردًا بل مترافقًا مع تعاون وثيق مع الولايات المتحدة، الدولة الرائدة في مجال الأمن السيبراني، ومنسجمًا مع مفهوم "الدفاع الأمامي" الأمريكي.

السياق الإقليمي الذي يحيط بكوريا الجنوبية معقد، إذ تواجه تهديدًا متناميًا من كوريا الشمالية التي استثمرت بكثافة في تطوير قدراتها السيبرانية للهجوم على أهداف سياسية واقتصادية وعسكرية، كما أن المنافسات الدولية الكبرى بين الولايات المتحدة والصين تضيف جانب أخر من التعقيد إلى المشهد السيبراني. لذلك، فإن التحول نحو الدفاع الاستباقي مع حليف قوي متمكن في هذا المجال يعد خطوة استراتيجية تتماهى مع متطلبات الواقع المتغير والبيئة الاستراتيجية المتسمة بالتوجس والريبة وعدم اليقين.

طبيعة الهجوم السيبراني ضمن الاستراتيجية الدفاعية الاستباقية

في ضوء التطورات التي يشهدها الفضاء السيبراني، تعيد كوريا الجنوبية صياغة مفهوم الدفاع التقليدي بدمج "الهجوم الاستباقي" كأداة دفاعية. لكن من الضروري تفكيك المفاهيم المتعلقة بهذا "الهجوم":

1. الهجوم كجزء من الدفاع الاستباقي: لا يعني "الهجوم" بالضرورة شن هجمات تقليدية عدائية عشوائية، بل يمكن أن يكون استباقيًا في صورته، مثل تعطيل بنية تحتية إلكترونية معادية قبل أن تستخدم ضد الدولة، أو تتبع مصادر الهجوم وتعطيلها.
2. التركيز على خصوم محددين: معظم العمليات الاستباقية تركز على كوريا الشمالية، التي تستثمر في هجمات إلكترونية معقدة لاستهداف البنية التحتية لكوريا الجنوبية. وهذا يتطلب قدرة على تنفيذ عمليات مضادة فعالة قد تُصنّف هجومية تقنيًا.
3. الفرق بين الهجوم الاستباقي والهجوم العدواني: الهجوم الاستباقي هنا يشكل رد فعل وقائي يهدف إلى الحماية، وليس توسيع نطاق السيطرة أو تنفيذ أجندة توسعية، مما يجعل منه جزءًا من الاستراتيجية الدفاعية وليس العدوانية.
4. البُعد القانوني والأخلاقي: تبقى هذه العمليات مقيدة بإطارات قانونية ودولية تسعى للحد من التدخلات العابرة للسيادة، مما يحتم على الدولتين وضع ضوابط واضحة لضمان احترام المعايير القانونية والأخلاقية.

أهداف التعاون السيبراني بين كوريا الجنوبية والولايات المتحدة

يرتكز التعاون الاستراتيجي بين كوريا الجنوبية والولايات المتحدة على عدة أهداف واضحة ومتكاملة منها؛ تعزيز القدرات التقنية والاستخباراتية أي تبادل المعلومات الاستخبارية المتعلقة بالتهديدات السيبرانية في الوقت الحقيقي، وتطوير أنظمة إنذار مبكر تسمح بالاستجابة السريعة للهجمات المحتملة. تشمل هذه الأنظمة أدوات متقدمة لتحليل البيانات الضخمة والذكاء الاصطناعي لرصد الأنماط غير الاعتيادية.

إضافة الى تنسيق السياسات والاستراتيجيات بمعنى إقامة إطار مشترك لوضع السياسات الأمنية وإدارة الأزمات السيبرانية بشكل موحد، بحيث تضمن الدولتان سرعة التفاعل وفعالية التنسيق في حال وقوع أي هجوم. وتطوير القدرات العملياتية عبر إجراء تدريبات وتمارين مشتركة لتعزيز الكفاءة في التصدي للهجمات المعقدة والمتعددة الأوجه، بما في ذلك الهجمات التي تستهدف البنية التحتية الحيوية مثل الشبكات الكهربائية والاتصالات والمؤسسات المالية. واخيراً بناء منظومة دفاعية مشتركة تعمل على تنسيق القدرات التقنية والاستخباراتية بين الدولتين لتوفير تغطية أمنية شاملة من خلال شبكات موحدة أو مترابطة تسمح بمراقبة وتحليل الهجمات بشكل مشترك.

الدوافع الاستراتيجية وراء التحول الاستباقي والتعاون الدولي

تتعدد الدوافع التي حثت كوريا الجنوبية على تبني هذا التحول الاستراتيجي في الأمن السيبراني، منها، تصاعد التهديدات من كوريا الشمالية؛ حيث أصبحت الهجمات السيبرانية جزءًا لا يتجزأ من الحرب الهجينة التي تخوضها بيونغ يانغ، مستهدفة الأنظمة الحكومية، البنية التحتية الاقتصادية، والمؤسسات الحيوية. هذه التهديدات باتت تستهدف أيضًا المؤسسات الخاصة التي تعتبر جزءًا من الاقتصاد الوطني.

إضافة الى تغير طبيعة الحروب الدولية، فالاعتماد المتزايد على الفضاء السيبراني في الحروب الحديثة يفرض ضرورة تبني استراتيجيات قادرة على المواجهة في هذا الفضاء سريع التغير، حيث تتسم الهجمات بالتعقيد والسرعة والانتشار.

في ضوء ذلك تعزيز الردع من خلال التعاون مع الولايات المتحدة: يشكل التحالف مع الولايات المتحدة عنصر قوة واعتبارًا استراتيجيًا لكوريا الجنوبية، إذ تمتلك الولايات المتحدة قدرات استخباراتية وتقنية متقدمة تسهم في تعزيز القدرة الدفاعية لكوريا الجنوبية، وتزيد من قدرة الردع الاستراتيجي في مواجهة التهديدات.

مما يعني الضغط الدولي والإقليمي اذ تؤدي الديناميات الإقليمية في شرق آسيا إلى تعزيز التعاون الأمني، خاصة مع تصاعد التوترات بين الولايات المتحدة والصين، ما يدفع كوريا الجنوبية لزيادة تأمين نفسها عبر شراكات عميقة مع حلفائها.

تقييم للفوائد والمخاطر من هذا التعاون

تتلخص الفوائد في رفع مستوى القدرة الدفاعية: يمكن لكوريا الجنوبية أن تنتقل من موقف الدفاع التفاعلي إلى موقف متقدم يمكنها من منع أو تقليل تأثير الهجمات السيبرانية، وهذا يعزز من أمنها الوطني بشكل ملموس. إضافة إلى الردع الاستراتيجي أي قدرة كوريا الجنوبية على تنفيذ عمليات دفاعية هجومية استباقية تخلق حالة ردع، تحجم الخصوم عن استخدام الفضاء السيبراني كورقة ضغط أو تهديد. وتعزيز التكامل الأمني بين الحلفاء عبر يرسخ التعاون بين الولايات المتحدة وكوريا الجنوبية أطرًا مشتركة لإدارة الأزمات والتصدي للهجمات، مما يزيد من فعالية الاستجابة ويوحد الجهود في مواجهة التهديدات المشتركة.

المخاطر والتحديات:

تتبلور المخاطر عبر احتمال تصعيد التوترات الإقليمية؛ قد تفسر كوريا الشمالية، وأحيانًا أطراف أخرى، هذه الإجراءات على أنها تهديد مباشر يستوجب الرد، مما قد يؤدي إلى سباق تصعيد خطير في الفضاء السيبراني. فضلاً عن أهمية التعقيدات القانونية والأخلاقية، اذ يتطلب توظيف أدوات الهجوم الاستباقي إطارًا قانونيًا واضحًا يوازن بين ضرورة الأمن واحترام سيادة الدول وحقوق الإنسان في الفضاء السيبراني ليكون ناجحاً، كما يعد الاعتماد التقني المفرط أحد المخاطر الأساسية فقد يؤدي الاعتماد الكبير على التكنولوجيا المتقدمة إلى خلق نقاط ضعف جديدة، مثل الهجمات المضادة التي تستهدف أنظمة الدفاع نفسها. واخيرها؛ احتمالية وقوع أخطاء أو سوء تقدير: العمليات السيبرانية الاستباقية قد تتسبب في أخطاء تقنية أو معلومات خاطئة تؤدي إلى استهداف خاطئ أو تصعيد غير محسوب.

خاتمة وتوصيات

يشكل التحول نحو الدفاع السيبراني الاستباقي، وتكثيف التعاون الاستراتيجي بين كوريا الجنوبية والولايات المتحدة، خطوة جوهرية وحتمية لمواجهة التحديات السيبرانية المعاصرة التي لم تعد تقتصر على الهجمات الفردية بل تشكل تهديدات ذات أبعاد جيوسياسية واستراتيجية. رغم التحديات والمخاطر المحتملة، فإن بناء قدرات دفاعية متقدمة تعزز من الردع الوطني الكوري وتقلل من هشاشة البنى التحتية الحيوية.

لضمان نجاح هذا التحول، من الضروري:

1. تطوير أطر قانونية وسياسية مشتركة تحكم استخدام أدوات الدفاع الاستباقي بما يضمن احترام السيادة والحد من التصعيد غير المقصود.
2. تعزيز الشفافية والتنسيق الدولي لتجنب سوء الفهم وضمان استقرار البيئة السيبرانية الإقليمية والدولية.
3. الاستثمار في بناء قدرات بشرية وتقنية متطورة قادرة على التعامل مع التهديدات المتغيرة بسرعة.

4. مواصلة الحوار الاستراتيجي مع الحلفاء والشركاء الإقليميين لتعزيز الأمن السيبراني الجماعي.

بهذا، يمكن لكوريا الجنوبية أن تؤسس نموذجًا متقدمًا في الأمن السيبراني يعكس التوازن الدقيق بين الدفاع والهجوم في العصر الرقمي، ويعزز موقعها الاستراتيجي في منطقة شرق آسيا والعالم.