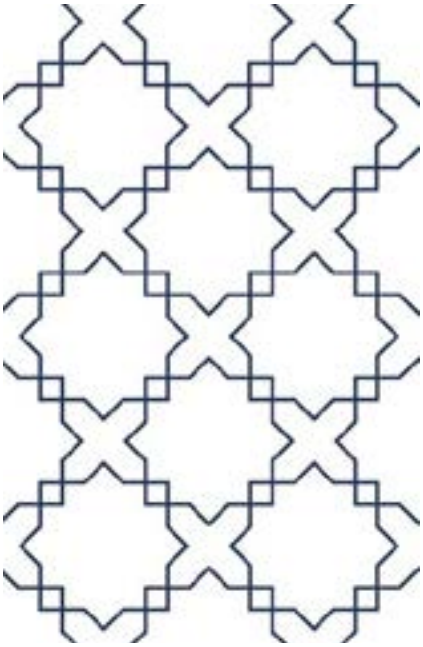
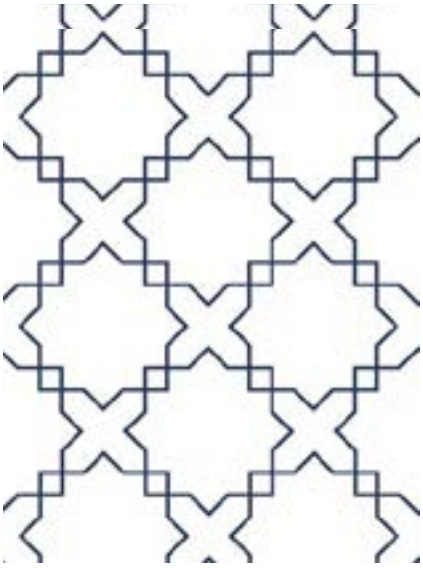


دراسات مترجمة



الدفاع، والإسناد، والمعاقبة:
ردع الحرب السيبرانية في عصر الذكاء الاصطناعي

إعداد: مجموعة التحليل التابعة لمؤسسة السياسة الخارجية
ترجمة: أ.د. رائد شهاب احمد
كلية الامام الأعظم الجامعة

تواجه قوة الردع التابعة لحلف شمال الأطلسي اختبارات تاريخية في المجالات الحركية والرقمية. فقد جلبت الحرب في أوكرانيا ما يسمى بمصطلح «الحرب الهجينة» إلى الواجهة وتزامنت مع ارتفاع مطرد في العمليات السيبرانية التي تستهدف أعضاء حلف شمال الأطلسي وحلفائهم. كما زادت الهجمات ضد المدنيين والبنية الأساسية الحيوية، على الرغم من الإجماع العالمي المتزايد على أن مثل هذه الهجمات تنتهك القانون الإنساني الدولي. وفي الوقت نفسه، يعمل الاستخدام المتزايد للذكاء الاصطناعي على تعزيز الهجمات السيبرانية والردع السيبراني على حد سواء، مع إمكانية تغيير مستقبل الحرب الهجينة. وبينما يحتفل حلف شمال الأطلسي بالذكرى الخامسة والسبعين لتأسيسه، يسلط هذا الموجز الضوء على الفرص المتاحة لتطوير وتنفيذ استراتيجيات ردع فعالة تأخذ في الاعتبار دور الذكاء الاصطناعي وتستعد له. وبالتركيز على الهجمات السيبرانية الأكثر تدميراً، يحدد هذا التحليل فجوات الردع الحرجة ويقدم توصيات عبر القطاعات لتعزيز الردع.

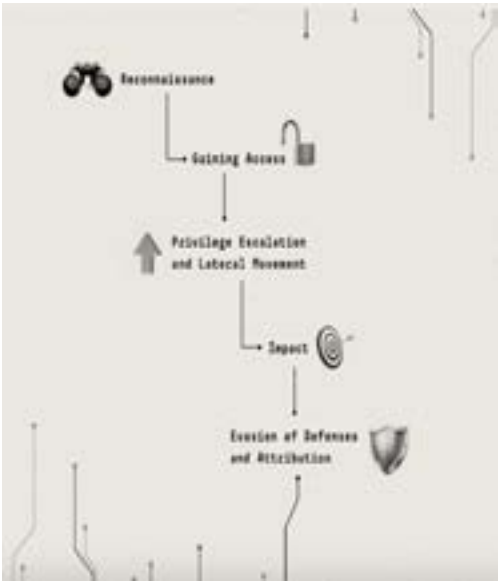
يمكن تقسيم استراتيجيات الردع السيبراني إلى نهجين رئيسيين: تلك التي تقلل من الفوائد المتصورة للهجمات، وتلك التي تزيد من تكاليفها المتصورة. وتسعى استراتيجية الإنكار إلى الحد من الحافز للهجوم من خلال جعل الأنظمة الرقمية مرنة، بحيث يمكنها الصمود في وجه الهجمات مع تحمل خسارة ضئيلة للقدرات. على سبيل المثال، يمكن لتدريبات الدفاع السيبراني وفرق الاستجابة السريعة تقليل الأضرار التي تلحقها الهجمات السيبرانية واستعادة الوصول بسرعة إلى الخدمات المستهدفة. وتسعى استراتيجية العقوبة إلى فرض عواقب على المهاجمين تفوق أي فوائد محتملة للهجوم، ومحاسبة المهاجمين على أفعالهم. أحد الشروط الأساسية للعقاب هو تحديد المهاجم بدقة، والمعروف أيضاً باسم الإسناد. تشمل أمثلة التبعات العقابية الجهود الجارية لتوضيح وإنفاذ القانون الدولي بشأن العمليات السيبرانية، فضلاً عن تحذيرات حلف شمال الأطلسي من أن الهجمات السيبرانية «التراكمية الخبيثة الكبيرة» على دولة عضو قد تؤدي إلى تفعيل المادة ٥ من معاهدة شمال الأطلسي والتي تنص على اتفاق «الاعضاء على أن الهجوم المسلح ضد واحد أو أكثر منهم (في أوروبا أو أمريكا الشمالية) يعتبر هجوماً ضدهم جميعاً.»

الذكاء الاصطناعي يقدم قدرات جديدة لكل من المهاجمين والمدافعين في الفضاء الإلكتروني

يجد المهاجمون الإلكترونيون بشكل متزايد طرقاً جديدة لتطبيق الذكاء الاصطناعي لتعزيز نطاق وتعقيد وإخفاء عملياتهم مع تقليل التكاليف المرتبطة بذلك. على سبيل المثال، يُقال إن الذكاء الاصطناعي يقود زيادة في هجمات التصيد الاحتيالي. حيث وجد تقرير عام ٢٠٢٣ أن ٧٥ في المائة من ٦٥٠ متخصصاً في الأمن السيبراني شملهم الاستطلاع شهدوا زيادة في الهجمات على مدار العام السابق، ومن بينهم ٨٥ في المائة يعزون الارتفاع إلى الذكاء الاصطناعي. حيث تشكل هذه القدرات تهديدات جديدة للبنوك وشبكات الطاقة والمستشفيات والانتخابات وأشكال أخرى من البنية التحتية الحيوية التي يستهدفها عادةً قراصنة مدعومون

من الدولة، فضلاً عن البيانات الحساسة أو الملكية الفكرية. من خلال خلق بيئة يكون فيها الهجوم أرخص وأسهل من بناء دفاعات فعالة، فإن الذكاء الاصطناعي لديه القدرة على تصعيد الصراعات الهجينة وإلحاق ضرر كبير بالمدنيين.

شكل رقم (١): دورة حياة الهجمات الإلكترونية



تقييم تأثير الذكاء الاصطناعي على مدار دورة حياة الهجوم الإلكتروني

يمكن تقسيم دورة حياة الهجمات الإلكترونية إلى مراحل. هنا، تم دمج إطار عمل MITRE ATT&CK في خمس مراحل (انظر الشكل (١)، تمثل جدولًا زمنيًا مبسطًا لكيفية تأثير الذكاء الاصطناعي على الردع الإلكتروني أثناء محاولة الهجوم.

١- الاستطلاع Reconnaissance:

هنا, يقوم المهاجمون بجمع المعلومات التي تساعدهم في اختيار أهدافهم وتصميم الهجوم. ويمكن أن يشمل ذلك معلومات حول الأهداف البشرية المستخدمة في الهندسة الاجتماعية، أو المعلومات الفنية حول الشبكات المستهدفة وأنظمة البرامج.

أ- استخدام المهاجم للذكاء الاصطناعي

يمكن للمهاجمين تدريب أدوات الذكاء الاصطناعي لجمع معلومات حساسة، على سبيل المثال من خلال التعرف على الوجه عبر ملفات تعريف الوسائط الاجتماعية. ويمكن أيضاً تدريب الذكاء الاصطناعي على التهرب من مرشحات البريد العشوائي، وصياغة رسائل البريد الإلكتروني والمستندات الواقعية، وتقليد أصوات أو أنماط الكتابة للشخصيات الموثوق بها، مما قد يحسن أساليب الهندسة الاجتماعية مثل التصيد الاحتيالي.

ب- استخدام المُدافِع للذكاء الاصطناعي

تم تصميم بعض أدوات الذكاء الاصطناعي للتمييز بين النصوص والصور ومقاطع الفيديو أو المقاطع الصوتية التي ينشئها الإنسان والذكاء الاصطناعي، مما قد يساعد في مواجهة حملات التصيد الاحتيالي المعززة بالذكاء الاصطناعي. حيث تستخدم برامج الذكاء الاصطناعي الأخرى التحليلات التنبؤية لتخمين متى وأين قد تظهر التهديدات السيبرانية المستقبلية. يمكن لهذه القدرة تحذير المنظمات المستهدفة لنشر تدابير وقائية قبل أن تتحقق التهديدات.

٢- الحصول على رخصة الدخول

يمكن للمهاجم ان يضمن موطئ قدم في نظام المعلومات الذي يستهدفه. وقد يتضمن ذلك سرقة بيانات اعتماد من مستخدمين مسموح لهم الدخول أو استغلال ثغرة في البرنامج للحصول على «باب خلفي» في النظام.

أ- استخدام المهاجم للذكاء الاصطناعي

يمكن أن يؤدي تطبيق الذكاء الاصطناعي على مجموعات بيانات كلمات المرور الكبيرة إلى تمكين تخمين كلمة المرور بشكل أكثر دقة. قد تكون الروبوتات التي تعمل بالتعلم الآلي أفضل وأسرع بالفعل في حل CAPTCHA من البشر، ويمكن للذكاء الاصطناعي المساعدة في التحايل على انظمة الحماية أو أنظمة الأمان البيومترية. يمكن استخدام تقنيات الهندسة الاجتماعية التي تعمل بالذكاء الاصطناعي لسرقة بيانات اعتماد تسجيل دخول المستخدم. يمكن للذكاء الاصطناعي أيضاً إنشاء محتوى ويب قد يجذب المستخدمين غير المطلعين إلى هجمات حُفر المياه.

ب- استخدام المُدافِع للذكاء الاصطناعي

يمكن لأدوات الذكاء الاصطناعي مسح البرامج بسرعة للكشف عن أنماط الترميز غير الآمنة أو نقاط الضعف الأخرى، ثم اقتراح طرق أكثر أماناً لترميز نفس الوظائف. حيث يساعد هذا مصممي البرامج على تصحيح الثغرات الأمنية قبل إصدار المنتجات ويساعد محترفي الأمن السيبراني على القضاء على الأبواب الخلفية قبل استغلالها من قبل المهاجمين. كما يستخدم الذكاء الاصطناعي في البرامج التي تكتشف الوصول غير المصرح به إلى النظام. ومن خلال تقليل الإيجابيات الخاطئة بين الأنشطة التي تم وضع علامة عليها، يمكن للذكاء الاصطناعي مساعدة محترفي الأمن السيبراني في معالجة الحالات الأكثر خطورة.

٣- تصعيد الامتيازات والحركة الجانبية

قد تكون الخطوات التي يتخذها المهاجم بعد اختراقه الأولي للنظام للحصول على امتيازات إضافية مطلوبة لأهدافه أو للوصول إلى أنظمة أخرى أكثر حساسية أو قيمة.

أ- استخدام المهاجم للذكاء الاصطناعي

بمجرد الدخول إلى نظام عبر الإنترنت، يمكن للمهاجمين استخدام الذكاء الاصطناعي لتحديد أنماط الترميز غير الآمنة، بما في ذلك توسيع نطاق تقنية تسمى «التشويش»، مما يجعل العثور على نقاط الضعف واستغلالها في الأنظمة المستهدفة أسرع.

ب- استخدام المُدافِع للذكاء الاصطناعي

يمكن لأدوات مراقبة الذكاء الاصطناعي مسح سجلات حركة مرور الشبكة الضخمة لتحديد الانحرافات عن السلوك العادي عبر الإنترنت ووضع علامة على النشاط الضار بسرعة الجهاز. وهذا يقصر أو يلغي فرصة المهاجمين لإلحاق الضرر قبل الكشف عن نشاطهم، مما يقلل مما يسمى «ميزة التحرك الأول» التي يمكن أن تحبط الردع في سياقات عسكرية أخرى.

٤- التأثير

يمثل التأثير الإجراءات التي يقوم بها المهاجم لتحقيق أهدافه داخل النظام، مثل تشفير الملفات أو استخراجها، أو إيقاف

تشغيل مواقع الويب، أو إتلاف البنية التحتية المستهدفة.

أ- استخدام المهاجم للذكاء الاصطناعي

عند اللجوء للهجوم، يمكن للذكاء الاصطناعي مساعدة المبرمجين في إنشاء برامج ضارة أو برامج فدية متطورة يمكن أن تزيد من التعطيل والدمار الناجم عن الهجمات الإلكترونية (على سبيل المثال، من خلال البحث بكفاءة أكبر في الأجهزة عن البيانات الهامة أو الملكية الفكري)ة.

ب- استخدام المُدافِع للذكاء الاصطناعي

يعد الذكاء الاصطناعي مكوناً أساسياً في برامج تحديد البرامج الضارة ومنع فقدان البيانات، مما يساعد المؤسسات المستهدفة على منع أو تخفيف التدمير والتعطيل الناجم عن الهجمات الإلكترونية.

٥- التهرب من الدفاعات والإسناد

يحاول المهاجمون إخفاء نشاطهم من أجل تجنب الكشف والإسناد طوال عملية الهجوم.

أ- استخدام المهاجم للذكاء الاصطناعي

يمكن أن يساعد ترميز الذكاء الاصطناعي المهاجمين على التهرب من الكشف عن طريق تغيير توقيعات البرامج الضارة باستمرار. على سبيل المثال، يتم برمجة برنامج تسجيل ضغطات المفاتيح المسمى Black Mamba للاتصال بـ ChatGPT لتوليد كود جديد ومختلف في كل مرة يتم تشغيله فيها، مما يحبط الجهود المبذولة للكشف عن الكود المستخدم في الهجمات السابقة. هناك أيضاً مخاوف من أن الذكاء الاصطناعي قد يتعلم محاكاة كيفية كتابة المستخدمين البشريين أو تصرفهم عبر الإنترنت للتهرب من أنظمة الأمان.

ب- استخدام المُدافِع للذكاء الاصطناعي

يمكن للأدوات التي تعمل بالذكاء الاصطناعي تحديد الأنماط في سلوك المتسلل، مثل توقيتهم وطرقهم وحركتهم داخل نظام عبر الإنترنت. وبالتناغم، قد تشكل هذه الأنماط توقيعًا مميزاً يمكن أن يساعد في الكشف والإسناد. يستفيد المدافعون بشكل متزايد من أدوات الطب الشرعي الرقمي التي تعمل بالذكاء الاصطناعي لإعادة بناء جداول زمنية للجرائم الإلكترونية وتحديد مرتكبي الهجمات الإلكترونية، مما يمهد الطريق للمساءلة والردع.

وعلى الرغم من هذه المخاطر الناشئة، فإن الذكاء الاصطناعي لديه القدرة على أن يكون عاملاً حاسماً للدفاع السيبراني. حيث يمكن للذكاء الاصطناعي أن يساعد في مراقبة نشاط المستخدمين عبر الإنترنت واكتشاف نقاط الضعف في البرامج وإصلاحها قبل أن يستغلها المهاجمون، مما يعزز الردع بالإنكار. وفي الوقت نفسه، يمكن لأدوات التفحص والتعقب الرقمية المتطورة أن تتضمن الذكاء الاصطناعي للكشف عن الهجمات السيبرانية ونسبتها، مما يتيح الردع بالعقاب. لقد دمجت مجموعة واسعة من منتجات الأمن السيبراني الذكاء الاصطناعي لسنوات. وعلى عكس المراقبين البشريين، فإن الأنظمة الآلية لا تعرف الكلل ويقظة على الدوام، ويمكن أن يساعد أتمتة مهام الأمن الأساسية في معالجة نقص المهارات العالمية في مجال الأمن السيبراني. ومع تسارع قدرات الذكاء الاصطناعي، سيتطلب الردع من المدافعين السيبرانيين مواكبة

أحدث التقنيات ومواكبة التطور التكنولوجي للمهاجمين.

إن النشر الفعال لأدوات المراقبة وأدوات التفحص والتعقب القوية هذه سيتطلب تعميق التعاون بين القطاعين العام والخاص، والمدني والعسكري، والدول المتحالفة. يمتلك القطاع الخاص ويدير ٨٠٪ من البنية التحتية السيبرانية العالمية وعادة ما يكون أول من يكتشف الهجمات ويستجيب لها. ولهذا السبب، يدمج تعهد الدفاع السيبراني المعزز لحلف شمال الأطلسي المكونات السياسية والعسكرية والتقنية للردع السيبراني مع قدرات القطاع الخاص. وعلى نحو مماثل، يمكن لتبادل المعلومات بين الدول والخبراء المستقلين أن يساعد في سد فجوات الأدلة، وتحديد المسؤول، وزيادة مصداقية الاتهامات من خلال مصادر مؤكدة. وقد استخدم تحالف الاستخبارات Five Eyes (يشمل: الولايات المتحدة, المملكة المتحدة, كندا, استراليا, ونيوزيلاندا) هذه الاستراتيجية لنسب الهجمات السيبرانية الصينية والروسية بشكل جماعي، في حين يمكن للمنظمات غير الربحية المستقلة التي تقدم خدمات الإسناد الشفافة أن تزيد من مصداقية اتهامات الدولة.

رسم خرائط لاستخدام مجموعات القراصنة لنماذج اللغة الكبيرة

في عام ٢٠٢٣، دخلت شركة Microsoft في شراكة مع OpenAI لتوثيق كيفية استخدام خمس مجموعات قرصنة معروفة لنماذج اللغة الكبيرة (LLMs) لتحسين عملياتها. ووجد بحثهم أن المهاجمين استخدموا نماذج اللغة الكبيرة أثناء مرحلة الاستطلاع وللمساعدة في الترميز والترجمة. ومع ذلك، فإن نماذج اللغة الكبيرة ليست سوى شكل واحد من أشكال الذكاء الاصطناعي وتشير أبحاث أخرى إلى أن تأثيرات الذكاء الاصطناعي قد تكون أكثر وضوحاً في مرحلة الوصول والاختراق في الهجوم الإلكتروني. الا انه لا يزال فهم الأدوار والتأثيرات المحتملة للذكاء الاصطناعي في العمليات الإلكترونية والحرب الهجينة ناشئاً.

الشكل ٢: خارطة القرصنة

لا يزال تحقيق المرونة السيبرانية الشاملة يعتمد على الأساسيات

في حين أن الأمن السيبراني المدعوم بالذكاء الاصطناعي يمكن أن يساعد في تسوية الملعب التكنولوجي، فإن الذكاء الاصطناعي وحده غير كافٍ لضمان بقاء الأنظمة الرقمية مرنة في مواجهة الهجمات السيبرانية. حيث يستغل المهاجمون السيبرانيون الخطأ البشري، والذي يساهم في حوالي ٨٨ في المائة من خروقات البيانات. يمكن أن ينمو هذا الخطر مع انتشار تقنيات التصيد بالذكاء الاصطناعي. سيتطلب الردع الفعال من مطوري التكنولوجيا تصميم ونشر أجهزة وبرامج جديدة مع وضع الأمان في الاعتبار، ووضع أقل قدر ممكن من العبء على المستخدمين النهائيين. حث تقرير صادر عن وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية (CISA) في نيسان/أبريل ٢٠٢٣ مصنعي التكنولوجيا على منع «العملاء من الاضطرار إلى إجراء مراقبة مستمرة وتحديثات روتينية والسيطرة على الأضرار» من خلال جعل المنتجات آمنة «جاهزة للاستخدام، مع القليل من تغييرات التكوين الضرورية أو بدونها وميزات الأمان المتاحة دون تكلفة إضافية".

فقبل وقوع الهجمات، يمكن للدول والحلفاء الاستفادة من التدريبات، وحلقات العمل البرمجي، وتمارين الفريق الأحمر، والمبادرات الأخرى لتطوير استراتيجيات الاستجابة المنسقة. كما يمكنهم الاستثمار في فرق الاستجابة السريعة لاستعادة القدرات المتضررة بسرعة وتقليل الاضطراب. لقد أثبت فريق الاستجابة لحالات الطوارئ الحاسوبية في أوكرانيا فعاليته العالية ضد الهجمات الإلكترونية الروسية كجزء من استجابة أوسع عبر القطاعات. ومع ذلك، لم تتمكن الفرق المكافئة او الموازية التي يديرها مركز الأمن السيبراني التابع لحلف شمال الأطلسي من معالجة الهجمات الإلكترونية التي عانت منها ألبانيا في عام ٢٠٢٢، وقد تحتاج إلى الإصلاح لتصبح أكثر مرونة وتبسيطًا واستباقية.

قد تكون استراتيجيات الدفاع السيبراني الجماعية الحالية بطيئة للغاية في منع الهجمات أو ردعها بشكل فعال. على سبيل المثال، تتطلب القرارات الخاصة بنشر فريق استجابة سيبرانية تابع لحلف شمال الأطلسي حالياً عملية طلب رسمية يتبعها إجماع بين جميع الدول الأعضاء البالغ عددها ٣٢ دولة، وهو ما قد يستغرق وقتاً طويلاً لمنع الضرر الذي قد يلحقه المهاجمون. ففي قمة فيلنيوس لعام ٢٠٢٣، التزم حلف شمال الأطلسي بقدرة دعم الحوادث السيبرانية الافتراضية (VCISC) لتمكين التخفيف الدولي عن بُعد من الأنشطة السيبرانية الضارة. ولتحقيق النجاح، ستحتاج قدرة دعم الحوادث السيبرانية الافتراضية إلى هيكل مبسط قادر على نشر المستجيبين بسرعة، بالإضافة إلى الثقة بين أصحاب المصلحة المشاركين لمشاركة المعلومات الحساسة اللازمة لتشخيص الهجمات وإعادة الشبكات السيبرانية إلى العمل. في بعض الأحيان، قد يكون تفعيل فرق الاستجابة من بلد واحد موثوق به أسرع وأكثر فعالية من تعبئة تحالفات متعددة الجنسيات، مثلما حدث عندما قدمت فرق من الولايات المتحدة المساعدة لألبانيا في عام ٢٠٢٢.

يتطلب فرض عواقب ذات مغزى على المهاجمين السيبرانيين تطوير خيارات انتقام متناسبة

يتطلب الردع السيبراني الفعّال الجمع بين المرونة والإسناد والعقوبات المعقولة للمهاجمين السيبرانيين. إن أحد السبل للمساءلة هو القانون الدولي، ولكن الجهود الجارية لتوضيح تطبيق القانون الدولي على عالم الإنترنت تواجه أسئلة مهمة لم تتم الإجابة عليها. إن المشاركة المتزايدة للمدنيين في العمليات السيبرانية تطمس التمييز القانوني بين المقاتلين وغير المقاتلين وقد تعرض المدنيين للانتقام العسكري. بالإضافة إلى ذلك، فإن الاستخدام المتزايد للمرتزقة السيبرانيين قد يتطلب تحديث التعريف القانوني للمرتزقة لمحاسبة الدول ووكلائها.

وإلى أن يتم تطبيق القانون الدولي بشكل أكثر اتساقاً في عالم الإنترنت، فإن إرساء المساءلة سيتطلب من الدول تطوير وفرض عواقب متناسبة على المعتدين السيبرانيين. ولكن الدول الفردية قد تفضل تحديد عتبات مختلفة للمخاطر والانتقام، مما يمثل تحديات للتحالفات المتعددة الجنسيات مثل حلف شمال الأطلسي، الذي ظل غامضاً بشأن ما يمكن أن تؤدي إليه الهجمات الإلكترونية من تداعيات المادة الخامسة. ورغم وجود أسباب يمكن الدفاع عنها لمثل هذا الغموض الاستراتيجي، فإن معاقبة الهجمات الإلكترونية بشكل فعال تتطلب الإجماع على ما يعتبر هجوماً. إحدى الطرق لتحديد الهجمات هي حسب الهدف، كما حدث عندما أعطى الرئيس بايدن للرئيس الروسي فلاديمير بوتن قائمة بـ ١٦ قطاعاً محظوراً من البنية التحتية الحيوية. ومع ذلك، لا تأخذ القوائم في الاعتبار شدة الهجوم النسبية، مما يجعل من الصعب التهديد بالعقاب المتناسب. يمثل التعريف «القائم على التأثيرات» بديلاً موثوقاً به، حيث يحدد الخطوط الحمراء ويحدد تدابير الانتقام بناءً على شدة التأثيرات الاقتصادية أو الاستراتيجية أو الإنسانية التي يلحقها الهجوم الإلكتروني.

كما يتطلب تعريف الهجمات الإلكترونية أيضاً تصنيف عمليات «التمركز المسبق» التي تنشئ وتحافظ على موطئ قدم في نظام رقمي للاستخدام في المستقبل، مثل الجهود الصينية الموثقة للتضمين داخل شبكات البنية التحتية الحيوية في الولايات المتحدة. وقد تكون هذه العمليات ذات نية غامضة، حيث قد تستخدم تقنيات مماثلة إما للتجسس أو لشن هجمات إلكترونية أكثر تدميراً، مما يثير تساؤلات حول ما إذا كانت هذه العمليات مؤهلة لتكون تهديدات بالعدوان بموجب القانون الدولي. وسوف يتطلب الردع الجدير بالثقة من المدافعين ليس فقط التهديد بالعواقب بشكل مجرد، بل وأيضاً معايرة وتوصيل العقوبات ــ التي تتراوح بين الإدانات الدبلوماسية، إلى العقوبات، إلى الضربات العسكرية الحركية، إلى الانتقام في عالم الإنترنت ــ التي يمكن اتخاذها رداً على أشكال معينة من العدوان الإلكتروني.

إن أي استراتيجية عقابية لابد وأن تتغلب على مخاطر وعقبات جسيمة. فرسم الخطوط الحمراء قد يقلل من المرونة في الأزمات؛ وفي حالة فشل الردع، فقد يشعر القادة بالضغط لتصعيد الصراعات إلى ما هو أبعد من مصالحهم أو تفويضهم الديمقراطي. وقد يؤدي معاقبة حادثة معينة ضمناً إلى التغاضي عن الهجمات

التي تم تجاهلها أو عدم اكتشافها من قبل، وهو ما يخاطر بالكشف عن فجوات استخباراتية أو تطبيع العمليات السيبرانية منخفضة المستوى القادرة على إلحاق ضرر كبير في المجموع. كما يمكن للانتقام الأحادي الجانب أن يشكل سوابق تقوض قدرة المجتمع العالمي على إرساء معايير سيبرانية مفيدة. على سبيل المثال، عندما دمرت إسرائيل أجهزة الطرد المركزي النووية الإيرانية أثناء هجوم ستوكسنت، بررت هذا العمل باعتباره إجراء دفاعياً يخدم الأمن الوطني والدولي. ومع ذلك، فإن الهجوم سبق معياراً محتملاً ضد الهجمات السيبرانية على المنشآت النووية، والتي قد تكون خطيرة أو مزعزعة للاستقرار بشكل خاص.

التطلع إلى المستقبل: المرونة السيبرانية الفعّالة في عصر الذكاء الاصطناعي

مع تطور القدرات، يمتلك الذكاء الاصطناعي القدرة على خفض التكاليف وزيادة فعالية الهجمات السيبرانية، ولكن أيضاً خفض تكلفة وجهد تدابير الأمن السيبراني. ولمواكبة هذه الديناميكيات المتغيرة، يمكن لحلف شمال الأطلسي تعزيز الردع السيبراني بالطرق التالية:

١- تقييم والاتفاق على الهجمات السيبرانية التي يمكن ردعها. ستتطلب إمكانية الذكاء الاصطناعي لتوسيع نطاق الهجمات إعطاء الأولوية للردع في مشهد تهديد مزدحم بشكل متزايد. ستكون العقوبات الأكثر مصداقية وفعالية إذا كانت متناسبة ومخصصة للسلوك الأكثر تدميراً في الفضاء الإلكتروني.

٢- إشراك الحلفاء والقطاع الخاص وأصحاب المصلحة الآخرين لحشد تحالف واسع من الخبرة الفنية والسياسية. يتطلب تسخير أحدث قدرات الذكاء الاصطناعي وأكثرها صلة التعاون المستمر بين الحكومات والمؤسسات المتعددة الجنسيات وشركات التكنولوجيا ومستخدمي الإنترنت. وعلى نحو مماثل، سيكون إسناد الهجمات السيبرانية أسهل وأكثر مصداقية إذا قامت وكالات الاستخبارات المتحالفة بتبادل المعلومات وتجميع الموارد.

٣- الاستثمار بشكل استباقي في مراقبة الذكاء الاصطناعي وتقنيات الطب الشرعي الرقمي، وتدريب وإعداد فرق الاستجابة السريعة. إن مواكبة النمو المتوقع للهجمات التي تعمل بالذكاء الاصطناعي سوف تتطلب مواكبة تطورها التكنولوجي، والثقة في المستجيبين الذين يتعاملون مع البيانات الحساسة، ونشر فرق الاستجابة بسرعة بعد الهجوم.

٤- نشر الأجهزة والبرامج الآمنة من حيث التصميم والافتراضي، وخاصة في الأنظمة الحكومية الحساسة. إن تعزيز الدفاعات السيبرانية ضد الهجمات المتقدمة بشكل متزايد يتطلب تقليل الاعتماد على المستخدمين النهائيين المعرضين للخطأ وتصميم التكنولوجيا بميزات أمان مدمجة. إن أدوات الذكاء الاصطناعي التي تفحص البرامج بحثاً عن ممارسات الترميز غير الآمنة يمكن أن تساعد المطورين في تصحيح نقاط الضعف قبل طرح المنتجات للجمهور.

٥- إنشاء آليات متعددة الجنسيات ومتناسبة وموثوقة وتوصيلها لمحاسبة المهاجمين السيبرانيين. وإلى أن يتم الالتزام بالقانون الدولي وإنفاذه بشكل أكثر اتساقاً، ستحتاج الدول إلى التهديد وفرض أشكال أخرى من الانتقام المتناسب للهجمات السيبرانية. وهذا يتطلب معايرة خيارات الاستجابة لشدة كل هجوم والظروف الجيوسياسية.

تشكل قمة حلف شمال الأطلسي في واشنطن فرصة لتأكيد وتعزيز الالتزامات بالردع السيبراني، بما في ذلك من خلال مراجعة التقدم والعقبات التي تعترض تنفيذ تعهد الدفاع السيبراني المعزز لحلف شمال الأطلسي المتفق عليه في فيلنيوس. ومن خلال الارتقاء لمواجهة تحدي التهديدات التكنولوجية الناشئة، قد يستمر التحالف لمدة ٧٥ عاماً أخرى ويعزز الدفاع السيبراني إلى ما هو أبعد من شمال الأطلسي.