مركز حمورابي
للبحوث و الدراسات الاستراتيجية

ترجمات

تطور العمليات السيبرانية في النزاعات المسلحة

Www.hcrsiraq.net
بغداد ـ عرصات الهندية - مجاور السفارة الصينية
+9647810234002
hcrsiraq@yahoo.cpm

مركز حمورابي
للبحوث و الدراسات الاستراتيجية

تطور العمليات السيبرانية في النزاعات المسلحة

تحليل فورن بوليسي

مركز حمورابي للبحوث و الدراسات الاستراتيجية

26 تموز 2023

العنوان: العراق ـ بغداد ـ الكرادة ـ عرصات الهندية ـ مجاور السفارة الصينية
بغداد الجادرية صندوق بريد 2405
Website: http://www.hcrsiraq.net
Mobile: 00964 - 7810234002
Baghdad - Aljadiriyah - P O. Box: 2405
E-mail: hcrsiraq@yahoo.com

أصبح المجال الرقمي بشكل متزايد ساحة معركة للجهات الفاعلة الحكومية وغير الحكومية التي تستفيد من القدرات في الفضاء السيبراني لتعزيز الأهداف الجيوسياسية الاستراتيجية.

وتعد الحرب الهجينة، واستخدام التكتيكات غير العسكرية جنبا إلى جنب مع الحرب الحركية التقليدية لتحقيق أهداف السياسة الخارجية، ليست ظاهرة جديدة. ومع ذلك، فإن استخدام روسيا لتقنيات الحرب الهجينة في أوكرانيا - وخاصة العمليات السيبرانية - لم يسبق له مثيل من حيث الحجم والنطاق. فالعمليات السيبرانية ، واستخدام التكنولوجيا الرقمية لمراقبة أو تعطيل أو إفساد أو تدمير البنية التحتية الحكومية والمدنية والمعلوماتية ، هي طريقة هجوم سريعة التطور وشائعة بشكل متزايد ، وتشكل مجالا رئيسيا للحرب الهجينة. وأكد تواتر وتنوع العمليات السيبرانية في حرب أوكرانيا المستمرة على الحاجة الملحة ليس فقط لفهم مظاهرها بشكل أفضل ولكن أيضا تحديد استراتيجيات للتخفيف من آثارها المدمرة.

الفائدة الاستراتيجية والتكتيكية للعمليات السيبرانية

التدخل في المنظمات المستهدفة والتأثير عليها لتوجيهها إلى اتخاذ قرارات طوعية تضر بأمنها ، وغالبا ما تستخدم عمليات المعلومات. وأيضا ، الحصول على وصول استراتيجي إلى البنية التحتية المدنية والحكومية ، غالبا تحسبا للمشاركة التكتيكية.

زعزعة الاستقرار

شن هجمات عدوانية وواضحة - بما في ذلك ضد البنية التحتية الحيوية - بهدف استقطاب و / أو إحباط و / أو تفتيت المنظمة المستهدفة ومكوناتها.وغالبا ما يقترن ذلك بالهجمات الحركية ، وضرب البنية التحتية الحكومية والمدنية لإجبار الاستجابة المطلوبة من المنظمة المستهدفة ومكوناتها.

Mobile: 00964 - 7810234002
Baghdad - Aljadiriyah - P O. Box: 2405
E-mail: hcrsiraq@yahoo.com
العنوان: العراق ـ بغداد ـ الكرادة ـ عرصات الهندية ـ مجاور السفارة الصينية
بغداد الجادرية صندوق بريد 2405
Website: http://www.hcrsiraq.net

مركز حمورابي
للبحوث و الدراسات الاستراتيجية

تفريغ العمليات السيبرانية في النزاعات المسلحة

تقوم الدول بنشر العمليات السيبرانية بشكل انتقائي لأكثر من عقد من الزمان كجزء من استراتيجيتها الجيوسياسية ولتعزيز أهداف السياسة الخارجية - على سبيل المثال، عندما أفادت التقارير أن الولايات المتحدة وإسرائيل نشرتا برمجيات خبيثة من طراز "ستوكسنت" في عام 2010 لتدمير 20 في المائة من أجهزة الطرد المركزي النووية الإيرانية. وأحد الأسباب الرئيسية التي تدفع الحكومات إلى نشر التكتيكات السيبرانية هو إنكارها المعقول، مقارنة بالعمل العسكري التقليدي، الذي يمكنها من إجبار الخصوم دون إشعال حرب شاملة. ومع ذلك، يتم استخدام العمليات السيبرانية بشكل متزايد، بما في ذلك في أوكرانيا، كمقدمة للعمليات العسكرية أو إلى جانبها.

وفي أوكرانيا وأماكن أخرى، تطلق الجهات الفاعلة في مجال التهديد العنان للعمليات السيبرانية لشل حركة الخدمات الحكومية، وتخريب البنية التحتية الحيوية، وتعطيل الانتخابات، وتحقيق أهداف أخرى. وفي النزاعات المسلحة، تستفيد الجهات الفاعلة في مجال التهديد من التكتيكات السيبرانية لزيادة العمليات الحركية. وعلاوة على ذلك، تستخدم الجهات الفاعلة في التهديد العمليات السيبرانية - مثل تلك التي تولد المعلومات المضللة وتضخمها - لإضعاف وتقويض التماسك الاجتماعي، مما يؤدي إلى تفاقم التشرذم السياسي.

أنواع مختلفة من الجهات الفاعلة في التهديد السيبراني

جهة التهديد هي أي منظمة أو شخص أو مجموعة توجه أو تسهل هجوما في الفضاء السيبراني لإلحاق الضرر بهدف معين، بما في ذلك الكيانات الحكومية وغير الحكومية. وداخل المنظمة المستهدفة، قد يكون ممثل التهديد قادرا على تجنيد عملاء للعمل كعملاء "داخليين"، مدفوعين بالربح أو التظلم الشخصي أو متعاطفين مع قضية سياسية.

- الدول: العملاء داخل حكومة بلد ما، بما في ذلك، على سبيل المثال، الوكالات العسكرية والاستخباراتية التي تجري عمليات إلكترونية كجزء من السلوك الأوسع للسياسة الخارجية.

- مجرمو الإنترنت: الجهات الفاعلة غير الحكومية ، بما في ذلك الأفراد والجماعات ، الذين يقومون بعمليات إلكترونية بدافع الربح في المقام الأول.

- قراصنة الإنترنت: الجهات الفاعلة غير الحكومية ذات الدوافع السياسية، والتي تقصر نشاطها على المجال السيبراني. وقد يكونون أو لا يكونون متعاطفين مع دولة معينة.

- الجماعات الإرهابية: هم الجهات الفاعلة غير الحكومية ذات الدوافع الأيديولوجية وغالبا ما تسعى إلى زرع الفتنة أو نشر حملات التأثير جنبا إلى جنب مع الهجمات الجسدية.
- مرتزقة السايبر: عملاء سيبران خاصون مأجورون يتم التعاقد معهم من قبل جهة فاعلة حكومية أو غير حكومية لعملية معينة، أو لبيع تكنولوجيا معينة.

وفي العقود الأخيرة، لعبت العمليات السيبرانية دورا مركزيا في تكتيكات "المنطقة الرمادية"، حيث تحافظ الدول الأطراف في النزاع على علاقات دبلوماسية رفيعة المستوى بينما تتفاعل بشكل عدائي تحت عتبة الحرب. وقد تعمل الجهات الفاعلة في مجال التهديد من غير الدول بشكل مستقل أو تكون تابعة للحكومات ومدعومة منها.

العمليات السيبرانية ليست مجالا روسيا فقط

كما توضح هذه الأمثلة ، فإن العديد من الجهات الفاعلة في مجال التهديد تستخدم العمليات السيبرانية لحرب المعلومات، والبيانات الدبلوماسية ذات الدعاية العالية، والمراقبة، وغيرها من الأهداف.

ونظرا لأن العمليات السيبرانية أصبحت متطورة وواسعة الانتشار بشكل متزايد ، فمن الضروري لصانعي السياسات وقادة الأعمال والخبراء التقنيين ومجموعات المجتمع المدني وأصحاب المصلحة الآخرين المشاركين في معالجة الهجمات الإلكترونية والتخفيف من حدتها التعرف على هذه التكتيكات وفهمها في إطار الحرب الهجينة. وإن القيام بذلك أمر بالغ الأهمية لتجنب التخلف عن آخر التطورات السيبرانية وتعزيز التعاون لمواجهة الجهات الفاعلة التي تهدد المدنيين والبنية التحتية المدنية عمدا وبشكل عشوائي لتحقيق ميزة جيوسياسية.

اضطرابات في جميع أنحاء أوروبا من اختراق الأقمار الصناعية الروسية

كان للهجوم السيبراني على شبكة الأقمار الصناعية Viasat قبل ساعات فقط من الغزو الروسي لأوكرانيا تأثير متتالي في جميع أنحاء المنطقة. وان مصادر البيانات: منظمات المجتمع المدني ، مجلس الاتحاد الأوروبي ، معهد السلام السيبراني ، لا ديبيتشي ، وايرد ، رويترز ، يوم الصفر

التأثير على البنية التحتية العسكرية

تعطلت الاتصالات العسكرية عبر الأقمار الصناعية في أوكرانيا.

التأثير على قطاع الطاقة

أبلغت شركة الطاقة الألمانية Enercon عن فقدانها للمراقبة والتحكم عن بعد في 5,800 توربين رياح في جميع أنحاء أوروبا الوسطى.

التأثير على وصول المدنيين إلى الإنترنت

فقد عشرات الآلاف من المدنيين في أوكرانيا إشارة الإنترنت لمدة تصل إلى أسبوعين، مما أعاق الوصول إلى معلومات موثوقة.

وتأثر ما لا يقل عن 27000 مستخدم بانقطاع الإنترنت في جمهورية التشيك وفرنسا وألمانيا وبولندا والمملكة المتحدة ودول الاتحاد الأوروبي الأخرى. في فرنسا وحدها ، فقد 9000 مشترك الإنترنت.وأبلغ العملاء عن انقطاع الإنترنت في أماكن بعيدة مثل المغرب.

كيف أرست الحملة السيبرانية الروسية المستمرة الأساس للحرب الهجينة

بينما بدأ الغزو البري الروسي واسع النطاق في فبراير 2022 ، كان الكرملين يستخدم التكتيكات السيبرانية لتجهيز أوكرانيا وزعزعة استقرارها وإكراهها منذ عام 2013 على الأقل ، إن لم يكن قبل ذلك. وتشن روسيا منذ فترة طويلة حملة منسقة من الهجمات الإلكترونية على أهداف حكومية وعمليات معلوماتية واستخدمت التخريب الإلكتروني للبنية التحتية الحيوية إلى جانب عملياتها البرية والجوية في أوكرانيا. وتنبأت التكتيكات السيبرانية المتكاملة المستخدمة في شرق أوكرانيا قبل عقد من الزمان بنهج روسيا الهجين في الحرب في عام 2022.

وبدافع من ثورة الميدان عام 2013 - وهي حركة شعبية حولت أوكرانيا إلى تحالف سياسي أوثق مع الاتحاد الأوروبي وحلف شمال الأطلسي - بدأت روسيا في استخدام الهجمات الإلكترونية لشل المعارضين السياسيين وتشويه سمعتهم وتشتيت انتباههم. فعلى سبيل المثال، شنت روسيا هجمات موزعة لحجب الخدمة عن حركة الميدان في عام 2013 وتدمير شبكات الكمبيوتر والاتصالات الحكومية في عام 2014، ومن المرجح أن تصرف الانتباه عن وجود القوات الروسية في شبه جزيرة القرم قبل أيام من استفتاء مدجب دوليا حول الضم. كما اخترق عملاء روس نظام فرز الأصوات الإلكتروني في أوكرانيا، مما أدى إلى تأخير نتائج الانتخابات البرلمانية في تشرين الأول/أكتوبر 2014.

وفي موازاة ذلك، أطلق الكرملين حملات إعلامية على وسائل الإعلام الرئيسية ووسائل التواصل الاجتماعي تهدف إلى تهيئة المجتمعات المحلية لدعم الضم.فقد أثارت وسائل الإعلام التي ترعاها روسيا والروبوتات ومزارع المتصيدين وتلاعبت بالمخاوف والانقسامات التاريخية من خلال ربط حركة الميدان الموالية للغرب بمتعاون نازي في القرن 20 وتصوير روسيا على أنها حامية لجميع الروس العرقيين والمتحدثين بالروسية.و سعت عمليات التضليل الدولية التي قامت بها روسيا إلى ردع وتأخير رد الحكومة الأوكرانية والمجتمع الدولي من خلال تصوير الانفصاليين المدعومين من روسيا في شرق أوكرانيا وشبه جزيرة القرم على أنهم مقاتلون محليون من أجل الحرية. وأظهرت هذه الحملات المنسقة قدرة روسيا واستعدادها لنشر الأدوات السيبرانية لاستغلال وتضخيم الانقسامات المجتمعية قبل النشاط البري وأثناءه وبعده.

وحتى بعد أن هدأت العمليات البرية الروسية في شرق أوكرانيا وشبه جزيرة القرم في عام 2014، استمرت الجهود السيبرانية الروسية لزعزعة استقرار أوكرانيا وتشويه سمعة الحكومة المنتخبة ديمقراطيا في كييف، وركزت بشكل متزايد على تخريب البنية التحتية الحيوية. ففي عامي 2015 و 2016 ، استهدف المتسللون الروس محطات التوزيع الفرعية بالقرب من كييف ، مما أدى إلى تعطيل إمدادات الطاقة لمئات الآلاف من السكان لساعات ، مما أثر على الاتصالات وخدمات الطوارئ والبنية التحتية الأخرى. واستهدفت البرامج الضارة الروسية الأنظمة المالية في أوكرانيا في عام 2017 ، مما تسبب في أضرار عالمية تبلغ حوالي 10 مليارات دولار. وقد أظهرت هذه الهجمات بعيدة المدى،

بما في ذلك أول هجوم رقمي معترف به علنا على الإطلاق تسبب في انقطاع التيار الكهربائي، إمكانية زعزعة الاستقرار لدى الجهات الفاعلة التي تشكل تهديدا لاستغلال نقاط الضعف في شبكات الإنترنت للبنية التحتية الحيوية لإلحاق الأذى بالمدنيين وتكبد تكاليف منهم.

فقد تكثفت العمليات السيبرانية من حيث التواتر والحجم في الأشهر التي سبقت الغزو الروسي واسع النطاق. فمن يوليو 2020 إلى يوليو 2021 ، وجدت Microsoft أن 19 بالمائة من تحذيرات نشاط تهديد الدولة القومية العالمية التي أصدرتها كانت للعملاء في أوكرانيا ، في المرتبة الثانية بعد الولايات المتحدة في تلك الفترة الزمنية. وفي 24 فبراير 2022، شنت روسيا غزوها العسكري واسع النطاق لأوكرانيا إلى جانب هجوم إلكتروني على أجهزة مودم الأقمار الصناعية التي عطلت الاتصالات العسكرية الأوكرانية. ومنذ ذلك الحين ، استخدمت روسيا تكتيكات قسرية - بما في ذلك DDoS ، والمساحات ، والتشويه ، والتزييف العميق ، ورسائل البريد الإلكتروني المخادعة - في محاولة لتشويه سمعة أهداف الحكومة الأوكرانية ، وتآكل ثقة الجمهور ، وإحباط معنويات المجتمع الأوكراني.

وفي بعض الأحيان، تزامنت الهجمات الإلكترونية مع العمل الحركي، على سبيل المثال، عندما استهدفت الضربات العسكرية الروسية والهجمات الإلكترونية الوكالات الحكومية في دنيبرو في وقت واحد في 11 مارس 2022. ومع ذلك، فإن الطرق والمدى الذي تعمل به روسيا باستمرار على مواءمة استراتيجياتها السيبرانية والحركية لم يتم تحديدها بالكامل بعد.

واستهدفت العمليات السيبرانية في الوقت نفسه البنية التحتية الحيوية المدنية. ووفقا لبيانات Microsoft ، من فبراير 2022 إلى أكتوبر 2022 ، كانت 55 بالمائة من الأهداف الأوكرانية التي ضربتها البرامج الضارة للمساحات الروسية عبارة عن مؤسسات بنية تحتية حيوية ، بما في ذلك الطاقة والمياه وخدمات الطوارئ والرعاية الصحية. وفي أبريل 2022، أحبطت أوكرانيا محاولة روسية للاستيلاء على أنظمة التحكم الصناعية الكهربائية مع إمكانية قطع التيار الكهربائي عن مليوني نسمة. وقد حدث كل هذا على خلفية حملة تضليل مستمرة معادية للغرب وموالية لروسيا داخل أوكرانيا وروسيا، مثل منشورات وسائل التواصل الاجتماعي التي تدعي أن أوكرانيا كانت على وشك الاستسلام من جانب واحد. وبالتوازي مع ذلك، عمل الكرملين على تقويض الدعم الدولي لأوكرانيا والتضامن معها، على سبيل المثال، من خلال اتهام

أوكرانيا باستخدام الجنود الأطفال والادعاء بأن الناطقين بالروسية في شرق أوكرانيا تعرضوا للإبادة الجماعية.

كيف يمكن لتحديات إسناد الهجمات الإلكترونية أن تقوض الإجماع الدبلوماسي والاستجابة الحاسمة

أظهرت عمليات روسيا في أوكرانيا ، هناك العديد من التحديات التي تحول دون إسناد العمليات السيبرانية بدقة وبشكل يمكن التحقق منه. وان بعض الهجمات - تلك الخاصة بالمراقبة ، على سبيل المثال - يمكن أن تمر دون أن يتم اكتشافها أو الإبلاغ عنها لفترات طويلة من الزمن ، مما يعقد استراتيجية تحديد الهوية والتصدي في الوقت المناسب. وعلاوة على ذلك، قد تختار الحكومات الاعتماد على وكلاء مثل المرتزقة السيبرانيين لصرف الانتباه والحفاظ على إمكانية إنكار معقولة. وقد تكون مقيدة أيضا ببروتوكولات تبادل المعلومات الاستخباراتية، في حين قد يتم تثبيط المنظمات الخاصة عن مشاركة الإخفاقات المتصورة في قدراتها الدفاعية السيبرانية. وإن الحواجز التي تحول دون تحديد نسب يمكن إثباتها وجمع الأدلة على الهجمات التي تشنها الجهات الفاعلة في القطاعين العام والخاص يمكن أن تقوض سرعة وتناسب الردود الدبلوماسية أو العسكرية.

وبما أن القانون الدولي الإنساني بشأن السلوك في النزاعات المسلحة يسبق انتشار العمليات السيبرانية، حتى عندما يتم تحديد الهجمات ونسبها، فإن الافتقار إلى المعايير والأطر القانونية الدولية المتفق عليها والراسخة للتصدي للحرب السيبرانية يشكل تحديا. ويمثل دليل تالين محاولة ملحوظة من قبل الأكاديميين والممارسين لتوضيح المخاوف وتدوين النهج لمعايير الفضاء السيبراني. وبالإضافة إلى ذلك، تم إنشاء حوارات أصحاب المصلحة المتعددين ومجموعات العمل على المستويات الإقليمية والوطنية وفوق الوطنية، بما في ذلك فريق الخبراء الحكوميين التابع للأمم المتحدة منذ فترة طويلة وفريقه العامل المفتوح العضوية الذي تم إنشاؤه مؤخرا (وبدعم من روسيا)، وكلاهما يسعى إلى وضع معايير السلوك وتطبيق القانون الإنساني في الفضاء السيبراني، ومنتدى حوكمة الإنترنت التابع لإدارة الشؤون الاقتصادية والاجتماعية التابعة للأمم المتحدة .

Mobile: 00964 - 7810234002
Baghdad - Aljadiriyah - P O. Box: 2405
E-mail: hcrsiraq@yahoo.com
العنوان: العراق ـ بغداد ـ الكرادة ـ عرصات الهندية ـ مجاور السفارة الصينية
بغداد الجادرية صندوق بريد 2405
Website: http://www.hcrsiraq.net

وتوفر هذه المبادرات الأساس لمزيد من المشاركة الدولية والتعاون عبر القطاعات لتطوير مناهج عملية للتخفيف من العمليات السيبرانية والحرب الهجينة ومكافحتها.

استشراف المستقبل

أثبتت العمليات السيبرانية أنها أسلحة قابلة للتطبيق وفعالة في ترسانة الجهات الفاعلة الحكومية وغير الحكومية في جميع أنحاء العالم. وبالإضافة إلى مزاياها الاستراتيجية - لا سيما الغموض حول الإسناد وتناسب الاستجابة - يمكن أن تكون الهجمات الإلكترونية مزعزعة للاستقرار إلى حد كبير وتضخم آثار الحرب الحركية. وعلى هذا النحو ، تعد العلاقات المفتوحة والتواصلية والتعاونية بين القطاعين الخاص والعام ضرورية لتوقع العمليات السيبرانية وتحديدها وردعها والاستجابة لها ، خاصة وأن الشبكات الاجتماعية والأجهزة والإنترنت عريض النطاق تعمل كناقلات للعديد من الهجمات.

وتستدعي تأثيرات العمليات السيبرانية على المجتمع بأسره اتباع نهج الردع يشمل المجتمع بأكمله. وتحقيقا لهذه الغاية، سيكون التنسيق بين الحكومة والصناعة وأصحاب المصلحة في المجتمع المدني أمرا بالغ الأهمية في أوكرانيا وخارجها. وعلاوة على ذلك، سيكون تطوير السياسات والمبادئ التوجيهية العالمية بشأن الإسناد والاستجابة والردع والمساءلة بشأن العمليات السيبرانية أمرا بالغ الأهمية لإنهاء الإفلات من العقاب، وحماية الأمن القومي، وخلق الاستقرار الدولي في مواجهة الحرب الهجينة في المستقبل.

تم كتابة هذا التحليل من قبل كل من بارسونز غرايسون (محلل أول للسياسات والمخاطر)، وإيزابيل شميدت (محلل أبحاث وسياسات أول)، والدكتورة مايشا علام (نائب رئيس الأبحاث).

مركز حمورابي
للبحوث و الدراسات الاستراتيجية

مركز حمورابي للبحوث و الدراسات الاستراتيجية

أسس مركز حمورابي للبحوث والدراسات الاستراتيجية في،18-11-2006 بمدينة بابل(الحلة)، كمركز علمي بحثي يمتد الى دراسة الموضوعات السياسية و المجتمعية بصورة علمية و استراتيجية، فضلاً عن التركيز على القضايا والظواهر الحادثة والمحتملة قي الشأن المحلي والأقليمي والدولي ، ويتعامل مع باحثين من مختلف التخصصات داخل العراق وخارجه، وتحتضن بغداد المقر الرئيسي للمركز.

www.hcrsiraq.net

07810234002

hcrsiraq@yahoo.com

2405

hcrsiraq

hcrsiraq

العراق - بغداد- الكرادة - العرصات الهندية-قربالسفارةالصينية