مقال
06

الفوز في الحدود الرقمية

تطوير الأهداف السيبرانية والجرأة العسكرية

الدكتور جريج أوستن (Dr. Greg Austin)
أستاذ مساعد، معهد العلاقات الأسترالية الصينية،
جامعة التكنولوجيا سيدني، أستراليا

ملخص

إن المتخصصين المطلوبين بشدة للفوز بالمعارك في الفضاء الإلكتروني هم المستهدفون. دورهم معقد للغاية. فهم يقومون باكتشاف واستغلال نقاط الضعف في أنظمة العدو. هدفهم هو زعزعة هذه الأنظمة أو تعطيلها، مع تحقيق تأثيرات معرفية أو جسدية على قوات العدو. ويجب أن يكون فيلق المستهدفين مدربًا تدريبًا عاليًا ويتمتع بخبرة كبيرة في العديد من المجالات المرتبطة بالاستخبارات، بما في ذلك السياسة وعلم النفس. ويجب أن يكون المستهدفون موجودين بأعداد كبيرة بما يكفي، مع تنوع كبير في التخصصات لدعم الأهداف التشغيلية. ويجب أن يتمتع قادتهم بالجرأة العسكرية والخبرة اللازمتين لتحقيق النتائج العملياتية بناء على نصائحهم. إن العلاقة بين المستهدف والقائد في الفضاء السيبراني قد تكون أكثر أهمية من أي مجال آخر من مجالات العمليات، باستثناء الأسلحة النووية. إن تطوير قوة دائمة من المستهدفين السيبرانيين ذوي القدرات العالية، بدعم من العمليات المتقدمة لربطهم بالقادة العسكريين المنتشرين في المقدمة، هو الأولوية الرئيسية للنجاح في ساحة المعركة الرقمية.

مقدمة

في تطوير الأفراد السيبرانيين لمهام الأمن القومي، بما في ذلك القوة الجوية، لا يوجد دور واحد قد يكون بنفس أهمية دور المستهدف. وقد شارك في هذا الرأي صراحة اثنان من المتخصصين العسكريين الصينيين الذين ينظرون إلى هذا الدور باعتباره "العمل الأساسي في خطة تشغيلية للفضاء السيبراني" (Zhang and Yao, 2015). كما أن القوات الجوية الأمريكية لديها مناصرون أقوياء لوجهة النظر القائلة بأن الاستهداف السيبراني يجب أن يكون في قلب استراتيجيتها وخطط تطويرها لعمليات الفضاء السيبراني الكاملة (Anderson, 2016).

ورغم أن هذه المشاعر لا نصادفها عادة في المناقشات المفتوحة المصدر حول العمليات العسكرية السيبرانية، إلا أنه من السهل تبريرها. يمكن للمستهدفين أن يتولوا مهام معقدة للغاية، وطموحات عسكرية مذهلة، ومسؤوليات ثقيلة بالنظر إلى مفاهيم الحرب المتطورة. وقد تم التعبير عن هذه المفاهيم بطرق مختلفة على مدى العقدين الماضيين. وقد كُلِّفت القوات السيبرانية الصينية بتنفيذ عمليات "لشلّ نظام العمليات الخاص بالعدو وتخريب نظام القيادة الحربية الخاص بالعدو خلال المراحل المبكرة من الأعمال العدائية (Costello and McReynolds, 2018). وتحدث القادة الأميركيون عن "ضربة عالمية في جزء من الثانية" (Cartwright, 2009) أو خيارات سيبرانية لجميع مراحل العمليات (Cyber Command, 2015). كان المفهوم الأمريكي الأكثر طموحًا هو تحقيق "الاختراق ثم تفكيك أنظمة العدو وصنع القرار، وبالتالي هزيمة قدراته الهجومية" (Pacific Command, 2020).

تتناول هذه المقالة ما هو مطلوب للجمع بين موهبة مستهدف الإنترنت وهدف اختراق النظام والتأثيرات المعوقة العميقة التي يمكنها هزيمة القدرات الحركية للخصم. وتشير المناقشة إلى أن الاعتقاد السائد منذ فترة طويلة بشأن القيمة المحدودة للعمليات السيبرانية في الحرب سوف يتم التغلب عليه، مع مرور الوقت، من خلال إدراك كيف يمكن للجرأة والطموح العسكريين أن يساعدوا في تحقيق الإمكانات الكاملة للحرب السيبرانية.

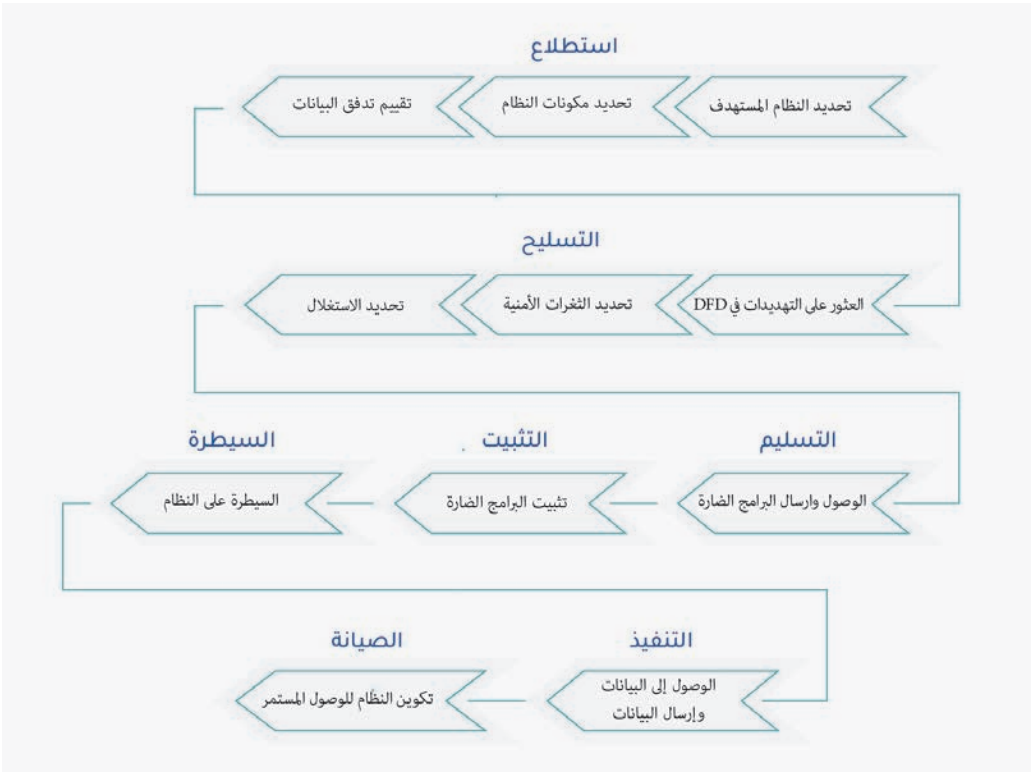
المستهدفون السيبرانيون

يلعب المستهدفون السيبرانيون دورًا رائدًا في دمج القدرات السيبرانية مع القوى الأخرى في العمليات السياسية أو العسكرية. في وكالة المخابرات المركزية والقوات الجوية الأمريكية، تعد أدوار الاستهداف شديدة الصعوبة: "الاستفادة من أكثر الأدوات السيبرانية تقدمًا ومجموعات البيانات والمنهجيات لتحليل المعلومات من جميع المصادر" (وكالة المخابرات المركزية) لدعم قرارات الاستهداف في كل من الهجوم والدفاع. تعتمد قرارات الاستهداف على المعرفة العميقة بأنظمة تكنولوجيا المعلومات الخاصة بالعدو والمحلية، وإجراءات التشغيل، والقدرات، والتخطيط العسكري أو الاستراتيجي. وعادة ما يتضمن الملف

> تعتمد قرارات الاستهداف على المعرفة العميقة بأنظمة تكنولوجيا المعلومات الخاصة بالعدو والمحلية، وإجراءات التشغيل، والقدرات، والتخطيط العسكري أو الاستراتيجي.

الشخصي لهؤلاء المحللين درجة متقدمة في العلوم التقنية ذات الصلة، وخبرة في لغة أجنبية، وخبرة سابقة في مجال الاستخبارات الأميركية. إن تعقيد مهمة الاستهداف السيبراني واضح في عقيدة القوات الجوية الأمريكية (2021) بشأن الاستهداف. وقد حددت توقعات واضحة بأن تطوير الأهداف للمفاهيم التشغيلية وأوامر المهام يجب أن "يدمج التحليل المتخصص لدعم العمليات الفضائية والفضاء السيبراني والطيف الكهرومغناطيسي والمعلوماتية".

في العمليات السيبرانية، يعد الاستهداف عملية مستمرة تشمل عدة مراحل. تبدأ بالتحقيق والتخطيط، ثم تنتقل إلى اختراق النظام وشن الهجمات. بعد ذلك، يتم تقييم الأضرار والاستغلال اللاحق. وأخيرًا، تتم إعادة تحديد الأولويات وإعادة الهجوم إذا لزم الأمر. يعتمد ذلك على المعرفة العميقة والقدرة على الوصول إلى أنظمة الخصم. وعلى النقيض من العمليات الحركية، حيث يمكن، على سبيل المثال، إنجاز الكثير باستخدام صور فوتوغرافية بعيدة المدى للهدف، فإن هذا التحليل في الفضاء السيبراني يعتمد على الحفاظ على الاشتباك والتواجد في أنظمة العدو السيبرانية. فمثلاً يوضح الشكل 6.1عملية هجوم نموذجية تجمع بين أطر Cyber Kill Chain وSTRIDE وATTACK، وقد يشتمل على مئات من التقنيات الفرعية والأدوات أثناء تنفيذ المهمة.



الشكل 6.1: مثال على هجوم يجمع بين إطارات عمل متعددة (adapted from Straub, 2020)

وفقًا للقوات الجوية الأمريكية، فإن الاستهداف السيبراني "يستغرق وقتًا أطول في كثير من الأحيان" من العمليات الحركية بسبب طبيعة المجال (USAF, 2023). ويجب أن يتضمن التخطيط النظر في "التأثيرات الهامة من الدرجة الثانية والثالثة"، فضلاً عن تجنب الصراع مع وكالات الاستخبارات، وإدارات السياسة، والحلفاء (حسبما تملي الظروف). ويشارك المستهدفون أيضًا في الدفاع السيبراني، وتحديد نقاط الضعف في التضاريس السيبرانية المهمة التي قد تتعرض للهجوم من قبل الخصوم. ومع ذلك، في العقيدة الرسمية للقوات الجوية الأمريكية، يشير "الاستهداف" فقط إلى العمليات السيبرانية الهجومية (USAF, 2023).

يجب أن تكون وظائف الاستهداف السيبراني متاحة على مستويات الحرب الثلاثة (الاستراتيجي والتشغيلي والتكتيكي). في الولايات المتحدة، تعمل القيادة السيبرانية مع قادة المقاتلين الموحدين (على سبيل المثال، القيادة الأمريكية في أوروبا) كقائد للمهام الاستراتيجية، مثل مهاجمة القيادة والسيطرة للعدو. يساهم أفراد الأمن السيبراني التابعون للقوات الجوية الأمريكية في هذه المهام الاستراتيجية بموجب تعيينهم لقيادة الأمن السيبراني، لكن القوات الجوية تركز تخطيطها واستهدافها السيبراني على المهام التشغيلية والتكتيكية.

بدأت القوات الجوية الأمريكية هذه العملية لتطوير أجهزة الاستهداف على الأقل في تسعينيات القرن العشرين، حيث نشرت أجهزة استهداف سيبرانية في حملة قصف حلف شمال الأطلسي عام 1999 ضد يوغوسلافيا السابقة. بدأت القوات الجوية في تعزيز هذا في عام 2006 عندما بدأت في إنشاء قيادتها السيبرانية الخاصة (Air Force, 2006)، وهي الخطوة التي علقتها عندما تم إنشاء قيادة القوة السيبرانية المشتركة بعد عدة سنوات.

وتظل القدرات السيبرانية للقوات الجوية الأمريكية قيد المراجعة والتطوير المستمر. على سبيل المثال، في عام 2024، رأت ضابطة كبيرة في القوات الجوية الأمريكية، الفريق أول ليا لودرباك، نائبة رئيس الأركان لعمليات الاستخبارات والمراقبة والاستطلاع والتأثيرات السيبرانية، فرصة كبيرة لمواصلة تطوير العمليات السيبرانية التكتيكية لدعم التفوق الجوي مقارنة بحالتها الحالية المتخلفة نسبيا (Pomerlau, 2024a). ومن غير المتوقع أن تنضج العناصر التنظيمية الرئيسية لهذا (إنشاء جناح جديد للفضاء السيبراني وتطوير مفهوم تشغيلي للتفوق الجوي المدعوم بالسيبراني) قبل الفترة الزمنية 2025-2027. وسوف يشهد هذا الإطار الزمني تجنيد وتدريب مجموعات جديدة من المستهدفين السيبرانيين. يمكن العثور على رؤية مثيرة للاهتمام حول كيفية استجابة القوات الجوية الأمريكية للاحتياجات التكتيكية في استهداف الفضاء السيبراني في تحليل أجراه أحد ضباطها حول دمج القدرات السيبرانية في العمليات الخاصة للقوات الجوية الأمريكية (Kopecki, 2016).

تعلن وكالة الاستخبارات المركزية الأمريكية (CIA) بشكل علني عن دور المستهدف السيبراني وتصف مسؤولياتها الثقيلة بأنها "إنشاء فرص عملياتية، ودفع العمليات الناجحة" (CIA, undated). تتضمن القوات الجوية الأمريكية دور الاستهداف باعتباره تخصصًا محددًا في حشدها الاستخباراتي. وفي الوقت نفسه، يتم توفير أجهزة استهداف سيبرانية للوكالات والقوات الأميركية بأعداد كبيرة على ما يبدو من قبل شركات من القطاع الخاص، مثل General Dynamics، وBAE Systems، وBooz Hamilton، استناداً إلى الإعلانات على صفحات الوظائف في الولايات المتحدة.

في عام 2022، عدلت وزارة الدفاع الأمريكية عقيدتها بشأن العمليات المشتركة في الفضاء السيبراني لإعطاء المزيد من الاهتمام للعمليات الاستكشافية (العمليات التي تنطوي على "نشر قوات الفضاء السيبراني داخل المجالات المادية"

(Pomerlau, 2023). وسيكون لهذا آثار مهمة على المستهدفين، وخاصة فرض أعباء جديدة محتملة تتعلق بالتعرف بسرعة على الأنظمة التي لم يتم تحليلها من قبل أو العلاقات بين هذه الأنظمة والأشياء التشغيلية الأخرى. في أغسطس/آب 2024، كشفت القوات الجوية الأمريكية عن خطتها لرفع مستوى المشورة السيبرانية لرئيس القوات الجوية من خلال تقسيم وظائف نائب رئيس الأركان الحالي للاستخبارات والسيبراني إلى تعيينين مختلفين، نظراً للأهمية الناشئة لعمليات الفضاء السيبراني والحاجة إلى المشورة المتخصصة في هذا المجال (Pomerlau, 2024b).

الأرثوذكسية السيبرانية

هناك اعتقاد راسخ بأن العمليات السيبرانية الهجومية لا يمكن أن يكون لها سوى تأثير محدود في الصراع العسكري. في عام 2009، خلص مارتن ليبيكي، أحد أبرز الباحثين في مجال الحرب السيبرانية، في تقرير كتبه لصالح القوات الجوية الأمريكية إلى أن "الحرب السيبرانية الاستراتيجية من غير المرجح أن تكون حاسمة" وأن "الحرب السيبرانية العملياتية تلعب دوراً متخصصاً مهماً ولكن هذا الدور فقط" (Libicki, 2009). في عام 2012، أجرى توماس ريد وبيتر ماكبيرني من كينجز كوليدج لندن تمييزًا مهمًا بين الأسلحة السيبرانية الموجهة إلى هدف محدد والتي قد تكون ذات قيمة عالية من حيث التأثير وتلك ذات التطبيق الأكثر عمومية والتي تكون ذات قيمة أقل من حيث التأثير (Rid and McBurney, 2012). وقالوا إن هناك عقوبة واضحة مرتبطة بتطوير الأسلحة عالية القيمة التي "تزيد الموارد والاستخبارات والوقت اللازم للتطوير والنشر" والتي "من المرجح أن تقلل من عدد الأهداف" و"الفائدة السياسية للأسلحة السيبرانية".

> هناك اعتقاد راسخ بأن العمليات السيبرانية الهجومية لا يمكن أن يكون لها سوى تأثير محدود في الصراع العسكري.

وكانت هذه التقييمات سليمة في ذلك الوقت، ولكن لا بد من تفسيرها في ضوء التعريفات التي استخدمها المؤلفون لمصطلح "الحرب السيبرانية" أو "السلاح السيبراني". وفي قضية ليبيكي، كان تعريفه للحرب السيبرانية ضيقاً (لا يتضمن حرباً "حقيقية"، أي حرباً مادية) (Libicki, 2009). يعرف ريد وماكبيرني السلاح السيبراني بشكل ضيق إلى حد ما بأنه "رمز كمبيوتري يستخدم، أو مصمم للاستخدام، بهدف التهديد أو التسبب في ضرر جسدي أو وظيفي أو عقلي للهياكل أو الأنظمة أو الكائنات الحية". وفي الوقت نفسه، يقترحان أن هناك حاجة إلى مزيد من البحث في التأثيرات على مستوى النظام وأن مفهوم الحرب السيبرانية ذاته إشكالي.

في عام 2018، حددت دراسة أمريكية ثلاث تيارات فكرية (أشبه بمراحل التطور) في المؤسسة الدفاعية الأمريكية (Paul et al., 2018). كانت هذه المحاور هي: "الرش" (بمعنى أن أجزاء صغيرة من عمليات المعلومات مقبولة وعادة ما تكون مجرد فكرة لاحقة)، والالتزام الكامل بإمكانيات عمليات المعلومات من خلال الهيكل والموارد والتكامل، وتحول نموذجي إلى القبول الكامل والتخطيط للنتائج حيث تكون بيئة المعلومات هي "المحدد الأساسي لتلك الإجراءات". ولم يترك التقرير مجالا للشك في وجهة نظره التي مفادها أن وزارة الدفاع كانت في ذلك الوقت عالقة في مكان ما بين "الرش" والالتزام الكامل بعمليات المعلومات، وكانت بعيدة كل البعد عن التحول النموذجي الذي يبدو أن هذه القدرات السيبرانية توفره.

ابتداءً من عام 2018، أصبحت القوات المسلحة الأميركية أكثر استباقية في تعاملها مع العمليات السيبرانية بطريقة قد تفتح إمكانات جديدة للعمل الهجومي، ولكنها كانت في جوهرها دفاعية. اعتمدت القيادة السيبرانية (2018) رؤية مفادها أن الولايات المتحدة قادرة على اكتساب والاحتفاظ بالتفوق في الفضاء السيبراني. وانتقل البنتاغون بشكل منفصل إلى استراتيجية المشاركة المستمرة في عمليات الفضاء السيبراني، حيث كان أحد المكونات الرئيسية هو مفهوم "الدفاع إلى الأمام" (Department of Defense, 2018). وسوف يتطلب ذلك مستويات جديدة من العمل الدفاعي، سواء في الشبكات الصديقة أو المعادية، ضد العمليات المعادية. ولكن هذه الإجراءات سوف تظل دون عتبة النزاع المسلح، ولكنها سوف تنطوي على مستويات جديدة من الوصول المنتظم من جانب المشغلين الأميركيين إلى شبكات الخصم. ومن شأن هذا الوصول بدوره أن يوفر للقوات الأميركية وضعا أفضل للانتقال السريع إلى عمليات سيبرانية هجومية أكثر شمولا.

وقد ساعدت هذه التحولات في إرساء الأساس لتصريحات أكثر طموحا حول نية الولايات المتحدة شل حركة خصومها في الفضاء السيبراني، مثل بيان عام 2020 المذكور أعلاه والذي يهدف إلى "تفكيك أنظمة صنع القرار لدى الخصم".

والآن، في عام 2024، تؤكد دراسة أكاديمية تعتمد إلى حد كبير على تحليل الحرب بين روسيا وأوكرانيا هذه العقيدة التقليدية. وخلصت الدراسة إلى أن هناك فائدة محدودة للعمليات السيبرانية في الحرب "بسبب عدم ملاءمتها للتدمير المادي، والمخاطر العالية للفشل، والتكاليف المرتفعة للعمليات [السيبرانية] المعقدة التي من المرجح أن تحقق تأثيرات ناجحة ومدمرة، والتناقض بين وتيرة العمليات التقليدية والسيبرانية مما يؤدي إلى صعوبات في التكامل بين المجالات" (Pedersen and Jacobsen, 2024).

ومن ناحية أخرى، يزعمون أنه قد تكون هناك "نافذتان ضيقتان" لتحقيق المنفعة العسكرية. وهذه هي احتمالات "الفائدة الاستراتيجية التراكمية من استهداف البنية التحتية الحيوية والحكومات في سلسلة متواصلة من العمليات السيبرانية الأقل تعقيداً؛ والتركيز على العمليات في بداية القتال حيث يمكن التخطيط للتكامل عبر المجالات قبل بدء الحرب". حددت المقالة القرارات التنظيمية والتحديات الفنية كأسباب رئيسية لعدم وجود عمليات سيبرانية عبر المجالات بدلاً من الخوف من التصعيد أو القيود القانونية.

وكما أشرت في مكان آخر (Austin, 2016)، هناك على الأقل ثلاثة أبعاد حاسمة للمشكلة السياسية التي يفرضها القتال السيبراني، والتي لم تأخذها التقييمات الداعمة للأرثوذكسية الراسخة في الاعتبار:

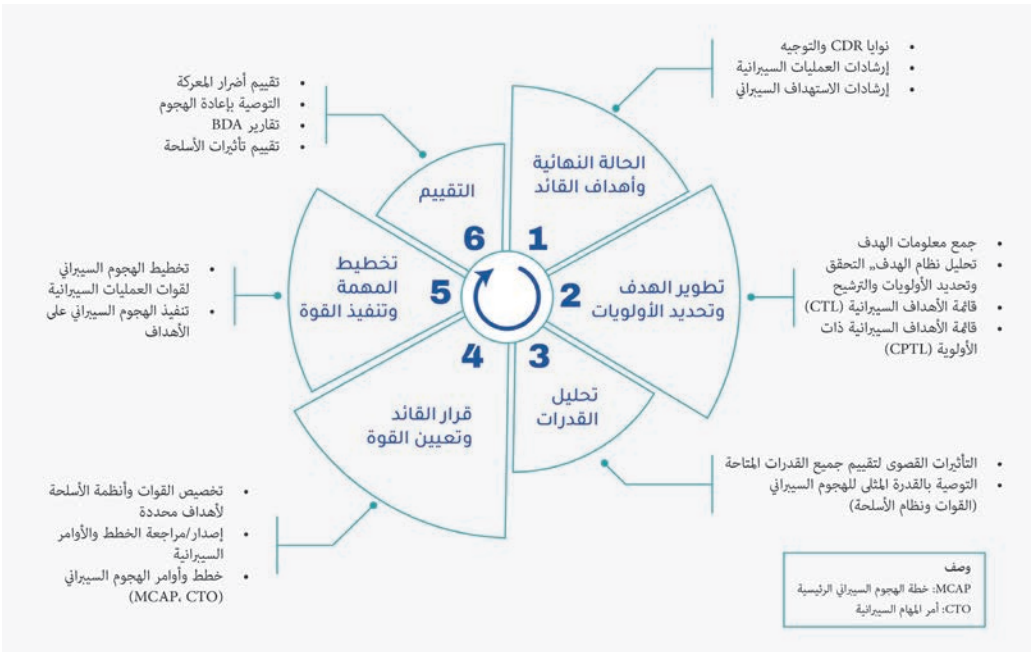
- تطورات تقنية جذرية في مجال الأسلحة السيبرانية
- تغيرات في الطابع السياسي للأسلحة السيبرانية مع تراكم ترسانات سيبرانية كاملة من قبل الدول بدلاً من مجموعة غير مكتملة من الأسلحة السيبرانية الفريدة (حزم الهجوم)
- تغيرات في الاستراتيجية مع ابتعاد البلدان عن الممارسات العسكرية التقليدية إلى استراتيجيات العصر السيبراني حيث تعتبر الهيمنة على المعلومات والتفوق في الفضاء السيبراني أمراً ممكناً.

وهكذا، فمن المتوقع مع مرور الوقت أن تصبح الاستنتاجات التي توصل إليها ليبيكي، وريد، وماكبيرني أقل أهمية. في الواقع، قدم ليبيكي (2017) مقالاً رائداً حول التقارب بين حرب المعلومات والعمليات السيبرانية حيث أجاب على السؤال الأخير بشكل واضح بالإيجاب، على الرغم من أنه لم يضعه بهذه الطريقة تمامًا.

الجرأة العسكرية

هناك زاوية حاسمة أخرى. إذا كانت أكبر نقاط الضعف العسكرية لدى الخصم تكمن في أنظمته السيبرانية للقيادة والسيطرة الاستراتيجية أو في سيطرته السيبرانية على أنظمة ومنصات الأسلحة، فلماذا لا يسعى القائد العسكري للخصم إلى مهاجمة مثل هذه الثغرات؟ هل ينبغي للقائد العسكري أن يقبل العقيدة التقليدية القائمة منذ زمن طويل أو أن يسعى إلى اختبار الحدود؟ هل يريد القائد مستهدفين إلكترونيين يقولون إن بعض المهام لا يمكن تنفيذها وليست فعالة من حيث التكلفة أو مستهدفين يمكنهم على الأقل تطوير خيارات الهجوم، بغض النظر عن مدى صعوبتها؟ هل العقبات تنظيمية أكثر (قضايا اختيارية) أم أنها متأصلة في التكنولوجيا؟

إن الاستهداف في الفضاء السيبراني قد يكون معقدًا للغاية، وخاصة عندما يتعلق الأمر بمتابعة التأثيرات على النظام. إن أي عملية استهداف سيبراني معينة، مثل تلك الموضحة في الشكل 6.2، فإنها سوف تعتمد في كثير من الأحيان على جمع معلومات استخباراتية متعددة الاتجاهات في الفضاء السيبراني على مدى فترة زمنية ممتدة. وسيكون معظم التحليل خارج نطاق فهم القادة العسكريين الذين ليسوا متخصصين في الأمن السيبراني. وقد تم توضيح التعقيد على المستوى الفني بشكل جيد في دراسة كورية (Kim and Eom, 2016). ووفقا للدراسة نفسها، هناك جوانب سياسية واجتماعية وإدراكية ومؤسسية إضافية للقدرة السيبرانية تحتاج إلى التحليل واستهدافها.



الشكل 6.2: عملية الاستهداف السيبران (Kim et al., 2022)

لـذا، فـإن القائـد القتـالي الـذي يعتـزم استكشـاف خيـارات الهجـوم السـيبراني مـن المرجـح أن يحتـاج إلى فريـق كـبير مـن المسـتهدفين ذوي التخصصـات المتنوعـة والذيـن يعملـون بنشـاط على خيـارات المهمـة على مـدى فترة طويلـة. وقـد قـدرت إحـدى الدراسـات التـي أجريـت على دودة ستوكسـنت أن فرقـاً مختلفـة مـن المتخصـصين (مـا يصـل إلى 45 شـخصاً) كانـوا يعملـون على مـدار عـامين أو نحـو ذلـك لإنشـاء الـدودة (de Falco, 2012). وقـد اسـتخدم ستوكسـنت في هجـوم على محطـة للوقـود النـووي الإيـراني، والـذي ربمـا أدى إلى تـدمير مـا يصـل إلى 1000 جهـاز طـرد مركـزي (de Falco, 2012). وخلـص هـذا التحليـل إلى أن "ستوكسـنت يختلـف عـن أي دودة سـابقة أخـرى بسـبب تعقيـده ومرونتـه وإمكاناتـه ومجموعـة ميزاتـه وأدائـه متعـدد الأدوار وهدفـه" (de Falco, 2012). وأظهـرت الدراسـة أن التفـكير الإبداعـي يمكـن أن يخلـق تـأثيرات سـيبرانية غير متوقعـة مـن قبـل على نطاق واسع.

وعلاوة على ذلـك، فقـد دخلـت التكنولوجيـات التـي تعـزز إمكانيـة تنفيـذ العمليـات السـيبرانية الهجوميـة على المسـتوى الاستراتيجـي حيـز التنفيـذ على مـدى السـنوات الخمـس عشرة الماضيـة. لقـد أدت الحوسـبة عاليـة الأداء، والعمـل الجماعـي بين الإنسـان والآلـة، والـذكاء الاصطناعـي إلى إحـداث تغـيير جـذري في المعتقـدات التقليديـة السـائدة حـول القيمـة المحـدودة للعمليـات السـيبرانية. وكما تـشير إحـدى الدراسـات، "لقـد تـم بالفعـل اسـتخدام الـذكاء الاصطناعـي والتعلـم الآلي لتحـسين محتـوى رسـائل التصيـد الاحتيـالي عبر البريـد السـيبراني، وتجنـب مرشـحات البريـد العشـوائي، ورسـم خرائـط وتنظيـم جمـع البيانـات حـول أهـداف محـددة بشـكل أفضـل، وهـو مـا يظـل الأسـاس لمعظـم الهـجمات السـيبرانية" (Jacobsen and Liebetrau, 2023). أصبـح المسـتهدفون الآن قادريـن على إكمال المهـام المعقـدة اللازمـة لشـن هـجمات سـيبرانية فعالـة على المسـتوى الاستراتيجـي بسرعـة أكبر بكـثير مما كانت عليه قبل خمسـة عشر عامًا.

الخاتمة

ويبـدو أن مفاتيـح التـأثيرات الاستراتيجيـة في العمليـات السـيبرانية الهجوميـة تكمـن في الطمـوح العسـكري والتنظيـم والتخطيـط المسـبق أكثر مـن القيـود التكنولوجيـة. في زمـن الحـرب، سـيكون التطـرف هـو شـل أو قطـع رأس عمليـة اتخـاذ القـرار لـدى الخصـم مـع تعطيـل الاتصـالات والقيـادة والسـيطرة بشـكل كـبير. وفي تحديـد هـذه الطموحـات، سـوف يعتمـد القـادة العسـكريون بشـكل كامـل على الإبـداع والمعرفـة التـي يتمتـع بهـا مسـتهدفوهم السـيبرانيون. ليـس هنـاك مـا يضمـن أنهـم سـيكونون قادريـن على تحقيـق التـأثيرات المرجـوة. ومـع ذلـك، مـع وجـود المسـتوى المناسـب مـن المسـتهدفين، والتنظيـم والقيـادة لتحقيـق أقصى قـدر مـن التـأثير، ومكافأتهـم وفقـا لذلـك، فمـن المؤكـد تقريبـا أن العمليـات السـيبرانية الهجوميـة سـوف تخلـف تـأثيرات استراتيجيـة ملحوظـة. وفي الوقـت الحـالي، سـيكون هنـاك احـتمال أقـل أن تكـون مثـل هـذه التـأثيرات حاسـمة في نتائـج المعـارك أو الحـرب، ولكـن مـن المحتمـل أن تكـون عدة بلدان في متناول مثل هذه القدرات.

المراجع

Anderson, S. (2016) Airpower Lessons for an Air Force Cyber-Power Targeting Theory. School of Advanced Air and Space Studies. Available from: https://media.defense.gov/2017/Nov/21/2001847267/-1/-1/0/DP_0023_ANDERSON_AIRPOWER_LESSONS.PDF

Austin, G. (2016) AUSTRALIA REARMED! Future Needs for Cyber-Enabled Warfare. ACCS Discussion, Paper 1. Available from: https://www.socialcyber.co/_files/ugd/15144d_6a1eb662e90e4c96beb5ccfa655cbc6a.pdf

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B. and Anderson, H. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. New York: Cornell University Press. Available from: https://arxiv.org/pdf/1802.07228

Cartwright, J. (2009). Presentation at the Center for International and Strategic Studies, June 4, 2009. The text is no longer available on the world wide web.

CIA. Undated. Cyber Targeter. Available from: https://www.cia.gov/careers/jobs/cyber-targeter/

Costello, J. and McReynolds, J. (2018). China's Strategic Support Force: A Force for a New Era. Washington, DC: National Defense University Press. Available from: https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf

Cyber Command. (2015). Beyond the Build: Delivering Outcomes through Cyberspace. Washington, DC: U.S. Department of Defence. Available from: https://nsarchive.gwu.edu/sites/default/files/documents/2692135/Document-27.pdf

Cyber Command. (2019). Achieve and Maintain Cyberspace Superiority. Washington, DC: U.S. Department of Defence. Available from: https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf

De Falco, M. (2012). Stuxnet Facts Report. A Technical and Strategic Analysis. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. Available from: https://ccdcoe.org/uploads/2018/10/Falco2012_StuxnetFactsReport.pdf

Department of Defense. (2018). Summary. 2018 Department of Defense Cyber Strategy. Washington, DC: Department of Defense. Available from: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/cyber_strategy_summary_final.pdf

Jacobsen, J.T. and Liebetrau, T. (2023) Artificial intelligence and military superiority: How the 'cyber-AI offensive-defensive arms race' affects the U.S. vision of the fully integrated battlefield. In F. Cristiano, Broeders, D., Delerue, F., Douzet, F. and Géry, A., (2023) Artificial Intelligence and International Conflict in Cyberspace, Issue 1, pp. 135-156

Kim, K.H. and Eom, J. (2016) Modeling of cyber target selection for effective acquisition of cyber weapon systems. International Journal of Security and Its Applications, 10(11), pp. 293-302. Available from: https://article.nadiapub.com/IJSIA/vol10_no11/24.pdf

Kim, K., Oh, S., Lee, D., Kang, J., Lee, J., & Shin, D. (2022). A Study on Cyber Target Importance Quantification and Ranking Algorithm. Applied Sciences, 12(4), 1833. https://doi.org/10.3390/app12041833

Kopecki, T. (2016). New Tools for a New Terrain: Air Force Support to Special Operations in the Cyber Environment. Maxwell Air Force Base: USAF Air Command and Staff College. Available from: https://apps.dtic.mil/sti/tr/pdf/AD1040710.pdf

Libicki, M. (2009). Cyber deterrence and Cyberwar, Santa Monica CA: Rand Corporation. Available from: https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

Libicki, M. (2017) The convergence of information warfare. Strategic Studies Quarterly 11.1, pp. 49-65

Lopez, C. (2006), Air Force leaders to discuss new 'Cyber Command' [Online] Air Force Print News. Available from: https://www.af.mil/News/Article-Display/Article/129517/air-force-leaders-to-discuss-new-cyber-command/

Pacific Command. (2020), Transforming the Joint Force: A Warfighting Concept for Great Power Competition [Online]. Available from: https://www.pacom.mil/Media/Speeches-Testimony/Article/2101115/transforming-the-joint-force-a-warfighting-concept-for-great-power-competition/

Paul. C., Clarke, C., Triezenberg, B., Manheim, D., and Wilson, B. (2018) Improving C2 and Situational Awareness for Operations in and Through the Information Environment. RAND. Available from: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2400/RR2489/RAND_RR2489.pdf

Pedersen, F. and Jacobsen, J. (2024) Narrow windows of opportunity: the limited utility of cyber operations in war. Journal of Cybersecurity. Volume 10, Issue 1. Available from: https://academic.oup.com/cybersecurity/article/10/1/tyae014/7727352?login=false

Pomerlau, M. (2023), New DOD doctrine officially outlines and defines 'expeditionary cyberspace operations' [Online]. Available from: https://defensescoop.com/2023/05/12/new-dod-doctrine-officially-outlines-and-defines-expeditionary-cyberspace-operations/

Pomerlau, M. (2024a), 'This is overdue'– Air Force creating tactical cyber capabilities to ensure air superiority [Online]. Available from: https://defensescoop.com/2024/05/23/air-force-creating-tactical-cyber-capabilities-ensure-air-superiority/

Pomerlau, M. (2024b), Air Force splitting up intelligence and cyber effects organization [Online]. Available from: https://defensescoop.com/2024/08/28/air-force-splitting-up-intelligence-cyber-effects-organization/

Rid, T. and McBurney, P. (2012). Cyber Weapons. RUSI Journal. February/March vol. 157 (1), pp.6–13 Available from: https://www.tandfonline.com/doi/epdf/10.1080/03071847.2012.664354

USAF. (2021). Air Force Doctrine Publication 3-60, Targeting. Washington, DC: U.S. Air Force. Available from: https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-60/3-60-AFDP-TARGETING.pdf

USAF. (2023). Air Force Doctrine Publication 3-12, Cyberspace Operations. Available from: https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-12/3-12-AFDP-CYBERSPACE-OPS.pdf

Zhang, C. and Yao, Z., (2015). A game theoretic model of targeting in cyberspace [Online] IEEE. Available from: https://ieeexplore.ieee.org/document/7280218