Atlantic Council

SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

ندوة الصراع العربي الإسرائيلي:
تعزيز الثقة بين إسرائيل والأردن في التعاون الدفاعي والأمني

الأمن السيبراني

SIMON HANDLER

الموضوع

- إن اختراق المعلومات الحساسة وتسريبها من قبل الجهات الفاعلة الحكومية وغير الحكومية تنشأ عنه آثار ضارة على الأمن القومي. وعلى الرغم من أن الذكاء الاصطناعي يمكن أن يساهم في زيادة عدد التهديدات السيبرانية، إلا أنه يمكن استخدامه أيضًا للكشف عنها والتخفيف منها. وستناقش هذه الجلسة وستتناول كيف يمكن لحلول الأمن السيبراني التي تعمل بالذكاء الاصطناعي أن تساعد كلا البلدين على مواجهة هذه التهديدات وتساهم في تحقيق الاستقرار الإقليمي.

عرض اليوم

- فهم عمليات الاختراق والتسريب
  - *الدوافع والوسائل والعواقب*
  - *أمثلة بارزة*
- النظر خارج المنطقة
- التهديدات الإقليمية في الشرق الأوسط
- وصف المجال السيبراني
- تأطير جديد للاستراتيجية السيبرانية
- تطبيق الاستراتيجية

فهم عمليات الاختراق والتسريب

- التقارب بين العمليات السيبرانية والمعلوماتية
- استخدام الخصوم (وأحيانًا حتى الحلفاء) للأدوات السيبرانية للوصول إلى المواد السرية و/أو الحساسة ونشرها في وقت لاحق للجمهور.
  - *معلومات*
  - *أدوات*

- في حين أن مصطلح "تسريب" يشير إلى نوع من الحقيقة بخصوص المواد المسربة، إلا أن عمليات الاختراق والتسريب تتضمن التلاعب أيضًا.
- الإسناد المبهم، والأعلام الزائفة، وقابلية الإنكار

الدوافع والوسائل والعواقب

- **الدوافع**
  - *محاولات متعمدة لتوجيه الحكم الأخلاقي العام ضد المستهدف*
  - *كشف القدرات ونقاط الضعف وعدم اليقين*
  - *مالية*
- **الوسائل**
  - *التصيّد الاحتيالي العشوائي*
  - *التصيّد الاحتيالي المحدد الهدف*
  - *برنامج الفدية Ransomware*
  - *هجمات سلسلة التوريد*
- **العواقب والأخطار الكامنة والمخاطر**
  - *الآثار المترتبة على الأمن القومي والاقتصادي والاجتماعي.*
  - *قد يكون من الصعب قياس التأثير، ولكنها قد تتراوح بين العواقب المحلية والجيوسياسية الوخيمة إلى الآثار غير المهمة.*
  - *توفر أدوات القرصنة الوسائل للخصوم من أجل الحصول على مواد سرية ومن ثم نشرها، ولكنها تهدد بلفت الانتباه إلى العملية نفسها، بدلاً من فضيحة التسريب.*

أمثلة بارزة على عمليات الاختراق والتسريب

- 1929 – مذكرة تاناكا (مصدر غير معروف)
- 2016 – اللجنة الوطنية الديمقراطية (الاستخبارات الروسية)
- 2016 – وثائق بنما (جون دو)
- 2017 – برنامج الأزرق الأبدي (وسطاء الظل)
- 2020 – برنامج الانفجار الشمسي/ شركة الرياح الشمسية (ليس معروفًا إذا كان للاختراق والتسريب، ولكن هناك احتمالات لذلك)

النظر خارج المنطقة

- الدول الفاعلة
  - *روسيا*
  - *كوريا الشمالية*
  - *الصين*

- الجهات الفاعلة من غير الدول
  - *مجموعات رانسوماوري (Ransomware)*
  - *النشطاء المخترقون (Hacktivists)*
  - *الأفراد المستقلون*

المشهد الإقليمي

- الدول الفاعلة
  - الإمارات العربية المتحدة
  - *السعودية*
  - *إيران*

- الجهات الفاعلة من غير الدول
  - *حماس (مولراتس MoleRATS/ غزة سايبرغانغ Gaza Cybergang)*
  - *حزب الله (الأرز اللبناني)*

وصف المجال الإلكتروني

- الارتباطات غير المنتظمة
  - *تستخدمها الدول الفاعلة والجهات الفاعلة من غير الدول*
  - *منهجيات غير متماثلة متكررة*
- الصراع الدائم منخفض الشدة
  - *المنطقة الرمادية بين السلام والحرب*
- المناظر الطبيعية المترابطة
  - *غير المقاتلين الذين يتعرضون للصراع*
- مشكلة القدرة على التمييز

تأطير جديد للاستراتيجية السيبرانية

- تحول التأطير من الهجمات الكارثية لمرة واحدة
- بدلاً من ذلك، خُذ دروسًا في الصراع السيبراني من الصراع غير المنتظم. توفر استراتيجيات مكافحة الإرهاب ومكافحة التمرد دروسًا مفيدة.
  - *التنافس الاستخباري*
  - *الزمانية والتطور*
  - *التنافس بشكل أفضل*

تطبيق الاستراتيجية

- التدابير السلبية
  - *إعطاء الأولوية للمخاطر بشكل صارم*
  - *تحسين الإمكانية الدفاعية*
  - *التركيز على قدرة التكيف*
  - *القدرة على الصمود*
- التدابير النشطة
  - *تحديد الهوية وتبادل المعلومات*
  - العقوبات
  - *إجراءات إنفاذ القانون*
  - *ممارسة الضغط على الملاذات الآمنة*

Thank you

תודה

شكرا