WWW.Alharazin.com

ما هي
الحرب السيبرانية ؟

What Is Cyber Warfare?

Mahmoud J Alharazin

#الحرب_السيبراينة

تُعـرَّف الحـرب السـيبرانية عـادة علـى أنهـا هجـوم إلكترونـي أو سلسـلة مـن الهجمـات التـي تسـتهدف بلـدًا مـا. لديهـا القـدرة علـى إحـداث الخـراب فـي البنيـة التحتيـة الحكوميـة والمدنيـة وتعطيـل الأنظمـة الحيويـة , ممـا يـؤدي إلـى إلحـاق الضـرر بالدولة وحتى الخسائر في الأرواح.

أنواع الهجمات في الحروب السيبرانية

1. هجمات التجسس " Espionage "
2. هجمات التخريب " Sabotage "
3. هجمات رفض الخدمة " DoS Attacks "
4. الهجمات المفاجئة " Surprise Attacks "
5. هجمات الدعاية " Propaganda Attacks "
6. همجات الاضطراب الاقتصادي " Economic Disruption "
7. هجمات على شبكات الطاقة الكهربائية " Electrical Power Grid "

أمثلة على الحروب السيبرانية

1. Stuxnet Virus : هي عبارة عن فايروس عمل على مهاجمة البرنامج النووي الإيراني ، حيث يعتبر من بين أكثر الهجمات الإلكترونية تطوراً في التاريخ.

2. Fancy Bear : تدعي "CrowdStrike" أن مجموعة الجرائم الإلكترونية الروسية "Fancy Bear" استهدفت القوات الصاروخية والمدفعية الأوكرانية بين عامي 2014 و 2016. انتشر البرنامج الضار عبر تطبيق Android مصاب تستخدمه وحدة المدفعية D-30 هاوتزر لإدارة بيانات الاستهداف.

استخدم الضباط الأوكرانيون التطبيق على نطاق واسع ، والذي يحتوي على برنامج تجسس X-Agent.حيث يعتبر هذا هجوماً ناجحاً للغاية , حيث أدى إلى تدمير أكثر من 80% من مدافع الهاوتزر D-30 الأوكرانية.

كيفية مكافحة الحرب السيبرانية

لا يـزال الوضـع القانونـي لهـذا المجـال الجديـد غيـر واضـح حيـث لا يوجـد قانـون دولـي يحكـم اسـتخدام الأسـلحة السـيبرانية. ولكـن هذا لا يعني أن الحرب السيبرانية لا يعالجها القانون.

نشـر مركـز التميـز للدفـاع السـيبراني التعاونـي (CCDCoE) دليـل تاليـن " Tallinn "، وهـو كتـاب مدرسـي يعالـج التهديـدات السـيبرانية النـادرة والخطيـرة. حيـث يوضـح هـذا الدليـل متـى تنتهـك الهجمـات الإلكترونيـة القانـون الدولـي وكيـف يمكـن للـدول أن تسـتجيب لمثل هذه الانتهاكات.

كيفية مكافحة الحرب السيبرانية

عمل تقييمات المخاطر من خلال المناورات السيبرانية

أفضل طريقة لتقييم استعداد الدولة للحرب الإلكترونية هي إجراء تمرين أو محاكاة واقعية , تُعرف أيضاً باسم المناورات الإلكترونية.

يمكن أن تختبر المناورات كيفية استجابة الحكومات والمنظمات الخاصة لسيناريو الحرب السيبرانية , وكشف الثغرات في الدفاعات , وتحسين التعاون بين المنظمات في الدولة. و يمكن أيضاً أن تساعد المناورات المدافعين على تعلم كيفية التصرف بسرعة لحماية البنية التحتية الحيوية وإنقاذ الأرواح.

كيفية مكافحة الحرب السيبرانية

عمل تقييمات المخاطر من خلال المناورات السيبرانية

يمكن أن تساعد المناورات الإلكترونية البلدان على تحسين الاستعداد للحرب السيبرانية من خلال:

1.اختبار المواقف المختلفة/ مثل اكتشاف الهجمات في المراحل المبكرة , أو تخفيف المخاطر بعد اختراق البنية التحتية الحيوية بالفعل.

2.اختبار السيناريوهات غير العادية / وذلك من خلال إنشاء فريق خاص يعمل كمهاجم ويحاول إيجاد طرق مبتكرة لاختراق نظم الدولة , حيث يمكن المدافعين من تعلم كيفية التخفيف من التهديدات الحقيقية.

كيفية مكافحة الحرب السيبرانية

عمل تقييمات المخاطر من خلال المناورات السيبرانية

3. تقسيم العمل وآليات التعاون / تتطلب الحرب الإلكترونية العديد من الأفراد من مختلف المنظمات والوحدات الحكومية للتعاون. يمكن أن تجمع المناورات الإلكترونية هؤلاء الأشخاص , الذين قد لا يعرفون بعضهم البعض , وتساعدهم على تحديد كيفية العمل معاً في حالة حدوث أزمة.

4. تحسين السياسات / قد تضع الحكومات سياسات للحرب الإلكترونية , ولكنها تحتاج إلى اختبارها في الممارسة العملية. يمكن أن تختبر المناورات الإلكترونية فاعلية السياسات وتوفر فرصة لتحسينها.

أشـهر المواقـع لمراقبـة الهجمـات السـيبرانية بين

1. https://www.fireeye.com
2. https://talosintelligence.com
3. https://cybermap.kaspersky.com
4. https://threatmap.fortiguard.com
5. https://livethreatmap.radware.com
6. https://securitycenter.sonicwall.com