ISSN: (3006-8614)
E-ISSN: (3006-8622)
Journal of Alma'rifa for Humanities
available online at: https://uomosul.edu.iq/womeneducation/almarifa/

The Geopolitical Implications of Digital Warfare and Cyber Conflict on National Security and the Global Economy

Omar Riyadh Faisal **Mohammed Riyadh Faisal**
Al-Hadara Boys' School / Nineveh Education Directorate
Northern Technical University / Nineveh Technical Management Institute

***Corresponding author: E-mail:**
mfa98894@ntu.edu.iq

0000-0002-7187-638X

***Keywords*:**
Geopolitical impacts
digital warfare
cyber conflict
national security

ARTICLE INFO

Article history:
Received **29. May.2025**
Revised **21. Jul.2025**
Accepted **31. Jul.2025**
Available online 3.Jan.2026

Email:
almarefaa.ecg@uomosul.edu.iq

ABSTRACT

In recent decades, the world has witnessed a qualitative shift in the nature of international conflicts, with digital (cyber) warfare becoming one of the most prominent contemporary geopolitical threats. Wars are no longer fought solely with conventional weapons; cyberspace has become an open arena for conflict between states, groups, and non-state actors. This research focuses on studying the geopolitical impacts of digital warfare, highlighting its direct and indirect repercussions on the national security and internal stability of states, as well as its serious repercussions on the global economy, supply chains, and the financial sector. The research also discusses how cyber conflict has changed the concepts of sovereignty, deterrence, and international hegemony, and contributed to reshaping global alliances and balances of power. The research relies on an analysis of real-life models of digital attacks and draws on academic sources and specialized international research centers, with the aim of providing a comprehensive view of the risks and challenges posed.

التأثيرات الجيوسياسية للحرب الرقمية والصراع السيبراني على الأمن القومي والاقتصاد العالمي

عمر رياض فيصل محمد رياض فيصل
مدرسة الحضارة للبنين/ مديرية تربية نينوى
الجامعة التقنية الشمالية/ معهد إدارة تقني نينوى

الخلاصة:

يشهد العالم في العقود الأخيرة تحولاً نوعياً في طبيعة الصراعات الدولية، حيث باتت الحرب الرقمية السيبرانية تمثل أحد أبرز التهديدات الجيوسياسية المعاصرة. لم تعد الحروب تخُاض بالسلاح التقليدي فقط، بل أصبحت الفضاءات الإلكترونية ساحة مفتوحة للصراع بين الدول، والجماعات، والفواعل غير الدوليين. يركز هذا البحث على دراسة التأثيرات الجيوسياسية للحروب الرقمية، مع تسليط الضوء على تداعياتها المباشرة وغير المباشرة على الأمن القومي للدول واستقرارها الداخلي، بالإضافة إلى انعكاساتها الخطيرة على الاقتصاد العالمي وسلاسل الإمداد والقطاع المالي. كما يناقش البحث كيف غيرّ الصراع السيبراني من مفاهيم السيادة، والردع، والهيمنة الدولية، وساهم في إعادة تشكيل التحالفات العالمية وتوازنات القوى. يعتمد البحث على تحليل نماذج واقعية للهجمات الرقمية، ويستند إلى مصادر أكاديمية ومراكز أبحاث دولية متخصصة، بهدف تقديم رؤية شاملة للمخاطر والتحديات التي يفرضها هذا النوع من الحروب على الأمن والاستقرار الدوليين.

الكلمات المفتاحية: التأثيرات الجيوسياسية، الحرب الرقمية، الصراع السيبراني، الأمن القومي

مقدمة

في عصر العولمة والتطور الرقمي المتسارع، لم تعد الحروب والصراعات تقتصر على ميادين القتال التقليدية، بل امتدت إلى الفضاء الإلكتروني، لتشكل ما يُعرف بـ "الصراع السيبراني". هذا النوع من الصراع يتضمن استخدام التكنولوجيا الرقمية، خصوصًا عبر الإنترنت، كأداة للهجوم على بنى تحتية حيوية، أو للتجسس، أو لنشر معلومات مضللة بهدف زعزعة استقرار الدول والمؤسسات. ومع تزايد الاعتماد على الأنظمة الرقمية في جميع مجالات الحياة، من الاقتصاد إلى الأمن والدفاع، أصبحت التهديدات السيبرانية تمثل تحديًا إستراتيجيًا خطيراً. من هنا، يُعد فهم طبيعة الصراع السيبراني، أسبابه، أنواعه، وآليات مواجهته ضرورة ملحة للحفاظ على الأمن القومي والسيادة الرقمية في العصر الحديث.

مع انفجار الثورة المعلوماتية ودخول العصر الرقمي خاصة في القرن الحادي والعشرين وما نتج عنه من تداعيات عديدة بسبب ظهور تهديدات وجرائم سيبرانية أصبحت تشكّل تحدياً كبيراً

للأمن القومي وكذلك الدولي، لدرجة أن العديد من الباحثين اعتبر الفضاء السيبراني بمثابة المجال الخامس في الحروب بعد البر والبحر والجو والفضاء، وهو ما استدعى ضرورة وجود ضمانات أمنية ضمن هذه البيئة الرقمية.

ومن هنا تبرز الحاجة إلى ضرورة فهم ماهية الأمن السيبراني كمتغير جديد في العلاقات الدولية.

ومن هنا يمكن اعتبار تحدي الامن السيبراني اعلى تحديات الامن القومي في القرن الواحد والعشرين مع الاشارة الى ان مفهوم الامن لم يعد مرتبط بالجوانب العسكرية فقط بل يواكب كل التحديات والتطورات التي من الممكن ان تكون عائق امام الاقتصاد الرقمي وتدفق المعرفة.

في عالمنا المترابط بواسطة الشبكة، يستفيد الجميع من برامج الدفاع السيبراني. فمثلاً على المستوى الفردي يمكن أن يؤدي هجوم الأمن السيبراني إلى سرقة الهوية أو محاولات الابتزاز أو فقدان البيانات المهمة مثل الصور العائلية كما تعتمد المجتمعات على البنية التحتية الحيوية مثل محطات الطاقة والمستشفيات وشركات الخدمات المالية لذا فإن تأمين هذه المنظمات وغيرها أمر ضروري للحفاظ على عمل مجتمعنا بطريقة آمنة وطبيعية.

الأمن السيبراني هو عبارة عن مجموع الوسائل التقنية والتنظيمية والادارية التي يتم استخدامها لمنع الاستخدام الغير مصرح به وسوء الاستغلال واستعادة المعلومات الالكترونية ونظم الاتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني. والأمن السيبراني هو سلاح استراتيجي بيد الحكومات والأفراد لا سيما أن الحرب السيبرانية أصبحت جزءاً لا يتج أز من التكتيكات الحديثة للحروب والهجمات بين الدول.

وفي عصر التكنولوجيا أصبح لأمن المعلومات الدور الأكبر صد ومنع أي هجوم إلكتروني قد تتعرض له أنظمة الدولة المختلفة، وأيضًا حماية الأنظمة التشغيلية من أي محاولات للولوج بشكل غير مسموح به لأهداف غير سليمة، وهو السبب وراء الأمر الملكي بإنشاء الهيئة الوطنية للأمن السيبراني.

في ظل التقدم التكنولوجي الهائل والاعتماد المتزايد على الشبكات الرقمية، برز نوع جديد من الصراعات يُعرف بـ "الصراع السيبراني". لم يعد التهديد اليوم يقتصر على الهجمات المسلحة أو التجسس التقليدي، بل بات الفضاء السيبراني ساحة معارك جديدة تشهد هجمات شرسة تهدد الأمن القومي، الاقتصاد، البنية التحتية، وحتى الحياة اليومية للأفراد. الصراع السيبراني بات واقعًا يفرض نفسه على الدول والمؤسسات، ويتطلب استراتيجيات جديدة لمواجهته.

أهمية البحث

تنبع أهمية هذا البحث من كونه يتناول أحد أبرز التحولات في طبيعة الصراع الدولي المعاصر، وهو الانتقال من الحروب التقليدية إلى الحروب الرقمية السيبرانية . فمع تزايد اعتماد الدول والمؤسسات على التكنولوجيا والفضاء السيبراني، أصبحت التهديدات الرقمية تشكّل خطراً مباشراً على الأمن القومي والسيادة الوطنية والاقتصاد العالمي.

يسهم هذا البحث في فهم الأبعاد الجيوسياسية لهذه الظاهرة، من خلال تسليط الضوء على كيفية توظيف القدرات السيبرانية في تعزيز القوة والنفوذ الدولي، وإعادة تشكيل توازنات القوى بين الدول. كما يُبرز البحث الفراغ القانوني والاستراتيجي الذي تعاني منه المنظومة الدولية في التعامل مع هذا النوع من الصراعات، مما يزيد من خطورتها ويستدعي معالجتها بطرق غير تقليدية.

ويكتسب البحث كذلك أهمية خاصة في ظل ازدياد عدد الهجمات السيبرانية المعقدة على مؤسسات حساسة حول العالم، مما يجعل من الضروري دراسة هذه الحروب لفهم أدواتها، وأهدافها، وتداعياتها، والمساهمة في وضع تصورات واقعية لتعزيز الأمن السيبراني الوطني والدولي.

هدف البحث

يهدف هذا البحث إلى تسليط الضوء على مفهوم الحرب السيبرانية باعتبارها شكلاً حديثا ومعقّدًا من أشكال الصراع في العصر الرقمي، من خلال استعراض طبيعتها وخصائصها، وأشكالها المختلفة مثل الهجمات على البنية التحتية، الأنظمة العسكرية، الاقتصاد، والمعلومات. كما يسعى البحث إلى توضيح خطورة هذه الحرب على الأمن القومي والسيادة الرقمية للدول، وبيان الفرق بينها وبين الحروب التقليدية، بالإضافة إلى استعراض أبرز الأمثلة الواقعية وآليات المواجهة والحماية الممكنة.

مشكلة البحث

في ظل التطور التكنولوجي الهائل، أصبح الفضاء السيبراني مجالاً مفتوحًا للصراع بين الدول، مما أدى إلى بروز الحروب الرقمية كأداة فعالة في الصراعات الجيوسياسية الحديثة. وتكمن مشكلة البحث في عدم وجود وعي كافٍ أو أطر قانونية واستراتيجية واضحة للتعامل مع التهديدات السيبرانية المتزايدة، والتي باتت تؤثر بشكل مباشر على الأمن القومي، والاقتصاد، والسيادة الوطنية للدول. كما أن هذا النمط الجديد من الحروب يتسم بالغموض واللامركزية، مما يجعل من الصعب تحديد الفاعلين، أو الرد بشكل تقليدي ، وبالتالي، تتمثل المشكلة الرئيسية في:

"كيف تؤثر الحروب الرقمية على توازن القوى الجيوسياسي العالمي، وما هي انعكاساتها على الأمن القومي والاقتصاد، في ظل غياب قواعد اشتباك واضحة في الفضاء السيبراني؟"

فرضية البحث

انطلاقًا من مشكلة البحث، يمكن صياغة الفرضية الرئيسية على النحو الآتي:

"تُعد الحروب الرقمية أداة استراتيجية جديدة تؤثر على الأمن القومي والاقتصاد العالمي، وتحدث تحولات في موازين القوى الجيوسياسية من خلال اعتمادها على تكنولوجيا متقدمة، وفاعلين غير تقليديين، وبيئة سيبرانية غير خاضعة لقواعد دولية ملزمة".

منهج البحث:

يعتمد هذا البحث على المنهج الوصفي التحليلي، باعتباره الأنسب لدراسة الظواهر السياسية والأمنية المعاصرة، خصوصًا ما يتعلق بالحروب الرقمية وتداعياتها الجيوسياسية. حيث يقوم الباحث بوصف مفهوم الحروب الرقمية وتحليل خصائصها، وتطورها، وأنواعها، ومن ثم تقييم تأتي ارتها على الأمن القومي والاقتصاد العالمي في سياق التنافس الدولي على النفوذ.

كما يستخدم البحث أدوات التحليل الجيوسياسي لفهم كيفية توظيف القدرات السيبرانية في الصراع بين الدول، وتحليل نماذج واقعية للهجمات السيبرانية التي أثرت في موازين القوى، وساهمت في إعادة تشكيل مفاهيم الردع والسيادة والتحالفات.

الدارسات السابقة في الصراع السيبراني

شهد موضوع الص ارع السيبراني اهتمامًا متزايدًا في الأوساط الأكاديمية والأمنية خلال السنوات الأخيرة، نظراً لتزايد حجم الهجمات وتعقيدها. ومن أبرز الدراسات التي تناولت هذا المجال:

1–دراسة "الحرب السيبرانية: التحديات الأمنية في العصر الرقمي جامعة أكسفورد 2018: –

تناولت مفهوم الحرب السيبرانية، وأكدت أن الفضاء الرقمي أصبح ساحة معترف بها للصراع، وركزت على ضرورة تطوير استراتيجيات دفاعية متقدمة.

2–دراسة "الهجمات السيبرانية على البنى التحتية الحيوية "– معهد بروكنغز 2019:–

ناقشت مخاطر الهجمات السيبرانية على الكهرباء والمياه والقطاع الصحي، وأوصت بتكامل الدفاع السيبراني مع الأمن القومي التقليدي.

3–دراسة "الصراع السيبراني بين الدول الكبرى (مركز الدراسات الاستراتيجية والدولية) CSIS، 2020: –

ركزت على الصراع السيبراني بين الولايات المتحدة، روسيا، والصين، واستعرضت نماذج من الهجمات وأثرها الجيوسياسي.

4–رسالة ماجستير بعنوان "الأمن السيبراني ودوره في حماية الأمن القومي " جامعة نايف العربية للعلوم الأمنية) 2021: –

أوضحت العلاقة الوثيقة بين الأمن السيبراني والأمن القومي العربي، وناقشت واقع التهديدات السيبرانية في المنطقة.

5–دراسة محلية بعنوان "الصراع السيبراني في الشرق الأوسط: التهديدات والتحديات" – مجلة العلوم السياسية العربية) 2022: –

تناولت الأبعاد الإقليمية للهجمات السيبرانية، خصوصًا بين دول مثل إيران وإسرائيل، ومدى تأثيرها على الأمن والاستقرار.

اولاً: نشأة الصراع السيبراني

تعود بدايات الصراع السيبراني إلى أواخر القرن العشرين، مع تصاعد الاعتماد العالمي على شبكات الحاسوب والإنترنت في المجالات العسكرية والاقتصادية والإدارية. ومع تطور التكنولوجيا، بدأ يظهر الفضاء الإلكتروني كساحة جديدة للصراع لا تقل أهمية عن البر والبحر والجو.

كانت أولى المؤشرات الجادة على وجود صراع سيبراني ما حدث في أواخر التسعينات، عندما بدأت دول كبرى مثل الولايات المتحدة وروسيا والصين بتطوير وحدات متخصصة في الدفاع والهجوم الإلكتروني. لكنّ التحول الفعلي نحو مفهوم "الحرب السيبرانية" بدأ بعد:

- هجوم "إستونيا" عام 2007، عندما تعرضت مؤسسات حكومية ومصرفية وعسكرية لهجمات إلكترونية منسقة، يُعتقد أن روسيا كانت وراءها، وهو ما اعتبر أول "حرب سيبرانية" معلنة ضد دولة ذات سيادة.(Thomas Rid,2013, p47)
- ثم جاء فيروس "Stuxnet" عام 2010، الذي استهدف البرنامج النووي الإيراني، ويُعتقد أنه نتيجة تعاون استخباراتي أمريكي–إسرائيلي. وقد شكّل نقطة تحول كبرى في فهم خطورة وقدرة الهجمات السيبرانية على إحداث أضرار مادية حقيقية.

منذ ذلك الحين، تطور الصراع السيبراني ليصبح جزءًا لا يتجزأ من استراتيجيات الأمن والدفاع الوطني، حيث باتت الدول تخصص موارد ضخمة لبناء "جيوش إلكترونية" .

ثانيا ا – مفهوم الحروب الرقمية:

تشير الحروب الرقمية أو"الحروب السيبرانية" الى نوع من الصراعات التي تستخدم فيها الوسائل التكنولوجية الرقمية كأدوات للهجوم والدفاع، بدلاً من الأسلحة التقليدية. وتحدث هذه الحروب في الفضاء السيبراني، أي عبر شبكات الإنترنت والأنظمة الحاسوبية.

تعرف الحروب الرقمية بأنها أنشطة هجومية تنفذها دول، أو مجموعات، أو أفراد باستخدام أدوات رقمية تهدف إلى اختراق أو تعطيل أو تدمير البنى التحتية المعلوماتية أو التكنولوجية للدولة المستهدفة، أو التلاعب بالمعلومات، أو سرقتها. (David Whetham,2016,p90).

2–1: خصائص الحروب الرقمية

أ. خفاء الفاعل (صعوبة التتبع):

غالبًا ما تتم الهجمات السيبرانية دون قدرة واضحة على تحديد هوية المهاجم، مما يجعل من

الصعب الرد أو اتخاذ إجراءات قانونية مباشرة.

ب- انخفاض التكلفة المادية:

لا يتطلب الصراع السيبراني معدات عسكرية أو تحريك جيوش، بل يتم عبر أجهزة حاسوب وخبرات تقنية ، مما يقلل التكلفة مقارنة بالحروب التقليدية.

ج. التأثير الواسع والسريع:

يمكن للهجمات الإلكترونية أن تحدث تأتي ارت كبيرة في وقت قصير، مثل تعطيل شبكات الكهرباء أو الخدمات الحكومية أو المؤسسات المالية.

د. لا حدود جغرافية له:

الصراع السيبراني يتجاوز الحدود الدولية، ويمكن تنفيذه من أي مكان في العالم ضد أي جهة، دون قيود مكانية أو زمنية. (Mary McEvoy Manjikian,2010,p384)

هـ. استمرار الصراع دون إعلان حرب:

قد تدور حروب سيب ارنية بين دول أو جهات لسنوات دون أن يُعلن عنها رسميًا، مما يضيف بُعدًا خفيًا للأمن القومي.

و. قابلية التكرار والتعديل:

يمكن تكرار الهجوم الإلكتروني عدة مرات مع تعديلات بسيطة على البرمجيات أو نقاط الضعف، مما يمنح المهاجم مرونة عالية.

ع. تداخل الفاعلين (دول، جماعات، أفراد) :

المشاركون في الصراع السيبراني قد لا يكونوا حكومات فقط، بل أيضًا جماعات إجرامية، ناشطين، أو أفراد مستقلين، ما يعقّد طبيعة الصراع.

ز. الاستخدام المزدوج للتكنولوجيا:

الكثير من أدوات وتقنيات الهجوم السيبراني تستخدم أيضًا لأغراض سلمية، مما يجعل من الصعب تنظيم

استخدامها أو حظرها(Jerry Brito and Tate Watkins,2011,p42).

2-2: أنواع الهجمات في الحروب الرقمية:

- الهجمات الإلكترونية(Cyber Attacks)
- التجسس الرقمي (Cyber Espionage)
- التشويش والتخريب السيبراني(Cyber Sabotage)
- نشر المعلومات المضللة عبر الإنترنت(Cyber Propaganda)

2-3: أهداف الحروب الرقمية :-

تهدف الحروب الرقمية) الحروب السيبرانية (إلى تحقيق مجموعة من الأهداف الاستراتيجية

والسياسية والاقتصادية والعسكرية، دون الحاجة إلى خوض مواجهة تقليدية مباشرة. فيما يلي أبرز هذه الأهداف: Clarke, Richard,2010,p22

أ. شل البنية التحتية الحيوية

استهداف شبكات الكهرباء، المياه، الاتصالات، الموانئ، المطا ارت، والقطاعات الصحية بهدف تعطيل الحياة اليومية. مثال: الهجوم السيبراني على شبكات الكهرباء في أوكرانيا عام 2015.

ب. التجسس وسرقة المعلومات

الحصول على بيانات حساسة من أنظمة حكومية أو عسكرية أو شركات كبرى) أسرار الدولة، براءة اختراع، معلومات مالية(، يُعد هذا من أبرز الأهداف الاقتصادية والاستخباراتية.

ج. إضعاف القدرات العسكرية

- اختراق أنظمة الدفاع والرادارات والتحكم بالطائرات أو السفن أو الصواريخ.
- تعطيل أنظمة القيادة والسيطرة أثناء الأزمات أو الحروب.

د. التأثير على الأري العام

استخدام وسائل التواصل الاجتماعي لنشر الشائعات، المعلومات المضللة، أو الدعاية السياسية.

تهدف هذه الاستراتيجيات إلى خلق انقسام داخلي أو تقويض الثقة بالمؤسسات الرسمية.

هـ. التأثير على الانتخابات أو السياسات الداخلية

التدخل في الأنظمة الانتخابية أو تسريب معلومات لإضعاف مرشح معين.

مثال: التدخل الروسي المزعوم في الانتخابات الأمريكية 2016.

ز. الابتزاز الرقمي والهجمات المالية

- تنفيذ هجمات فدية(Ransomware)تطلب من الضحايا دفع مبالغ مالية مقابل استعادة بياناتهم.
- استهداف البنوك أو الأسواق المالية لإحداث اضطرابات اقتصادية.

و. إرباك العدو دون تصعيد عسكري مباشر

تستخدم كوسيلة ضغط أو عقاب دون الدخول في مواجهة مسلحة، ما يسمح بتحقيق أهداف استراتيجية بهدوء وفعالية. (Singer, P. W.,2014,p34)

2-4: الحروب الرقمية بمنظور جيوسياسي

تمثل الحروب الرقمية أو السيبرانية أحد أبرز مظاهر التحول في طبيعة الصراع الجيوسياسي في القرن الحادي والعشرين. لم تعد السيطرة الجيوسياسية مقتصرة على الحدود الجغرافية والمقدرات العسكرية التقليدية، بل امتدت إلى الفضاء الرقمي، حيث تتداخل القوة السيادية، المعلومات، والقدرات التكنولوجية في تشكيل موازين القوى بين الدول.

مفهوم الحروب الرقمية جيوسياسياً هي أداة تستخدمها الدول أو الفواعل غير الدوليين للتأثير في مصالح الدول الأخرى، وزعزعة استقرارها السياسي أو الاقتصادي أو الأمني، باستخدام الفضاء السيبراني كأرض معركة افتراضية وهي ليست فقط صراعاً تقنياً، بل تعبير عن تنافس نفوذ وهيمنة واستراتيجية.

2–5: كيف غيّرت الحروب الرقمية الجغرافيا السياسية؟

أ. تلاشي الحدود الجغرافية التقليدية

في الحروب التقليدية، يُحدد العدو بموقع جغرافي. أما في الحروب الرقمية، فإن العدو قد يكون في أي مكان في العالم ويضرب عن بعد دون الحاجة إلى جيوش أو أسلحة ميدانية.

ب. صعود "السيادة السيبرانية"

. أصبحت حماية الفضاء الرقمي(البيانات، الشبكات، المعلومات الوطنية) مكونًا أساسياً من السيادة الوطنية.

. الدول باتت تعتبر أي اختراق رقمي انتهاكًا مباشراً لسيادتها.

ت. إعادة تشكيل موازين القوى

. القوى الصاعدة رقميًا) مثل الصين، روسيا، إيران، وكوريا الشمالية (أصبحت تمتلك أدوات تأثير وتهديد تنافس بها القوى الكبر ى.

. أدّى هذا إلى نقل ميدان الص ارع من الميدان العسكري إلى الفضاء الرقمي.

2–6: أهداف الدول من توظيف الحروب الرقمية جيوسياسياً :

التفسير الجيوسياسي	الهدف
تعطيل البنية التحتية أو التأثير على الاقتصاد الوطني أو النسيج الاجتماعي	إضعاف الخصوم
استخدام الهجمات الرقمية كوسيلة ضغط دون التورط في حرب شاملة	تعزيز الردع دون التصعيد
التدخل في الانتخابات، أو دعم حملات رقمية داخل دول أخرى للتأثير على سياساتها	فرض النفوذ الإقليمي/الدولي
لتجسس وسرقة الأسرار العسكرية والتجارية والسياسية	تحقيق مكاسب استراتيجية خفية

يمكن أن يأخذ الصراع السيبراني أشكالاً متعددة مثل:

. الهجمات التخريبية :(Cyber Attacks) تعطيل الخدمات أو تدمير أنظمة حيوية.

. القرصنة والتجسس الإلكتروني :(Cyber Espionage) اختراق البيانات لأغراض استخباراتية.

. الحروب النفسية والمعلوماتية :(Information Warfare) نشر الشائعات والمعلومات المضللة.

ويُعد الصراع السيبراني من أخطر أنواع الصراعات الحديثة، نظراً لعدم وضوح حدود الفاعلين فيه، وصعوبة تتبع مصدر الهجوم، وسرعة تأثيره، وارتباطه بالأمن القومي للدول. (Adam P. ,2012,p35)

2-7: التأثيرات الجيوسياسية للحرب الرقمية على الأمن القومي

أ -تهديد البنية التحتية الحيوية

. الهجمات السيبرانية يمكن أن تستهدف أنظمة الكهرباء، المياه، النقل، الاتصالات، والمستشفيات.

. هذا النوع من الهجمات لا يُسبب أضراراً اقتصادية فحسب، بل يشلّ قدرة الدولة على حماية مواطنيها.

مثال :هجوم "Stuxnet" على البرنامج النووي الإيراني)2010(عطّل أجهزة الطرد المركزي دون أي قصف فعلي.

ب- **زعزعة الاستقرار الداخلي**

. يمكن للهجمات الرقمية أن تنشر معلومات مضللة، أو تفتعل أزمات سياسية داخلية، مما يُضعف شرعية الحكومات.

. تدخلات سيبرانية في الحملات الانتخابية تقوض الثقة الديمقراطية.

مثال: التدخل الروسي في الانتخابات الأمريكية(2016) أثار أزمة ثقة واسعة في النظام السياسي الأمريكي.

ج- **خلق جبهات غير تقليدية للصراع**

. الحرب الرقمية لا تقتصر على المجال العسكري، بل تضاف إلى أدوات الردع والسيطرة السياسية.

. تهديد دائم ومفتوح على مدار الساعة، يصعب التنبؤ به أو ربطه بدولة معينة.

الدول اليوم تعيد صياغة عقيدتها الأمنية لتشمل "الردع السيبراني" كجزء من دفاعها القومي.

2-8: التأثيرات الجيوسياسية للحروب الرقمية على الاقتصاد العالمي

أ- تكلفة اقتصادية ضخمة للهجمات السيب ارنية

. خسائر الهجمات الرقمية على الشركات والحكومات تقدّر بمئات المليارات سنويًا.

. تؤدي إلى توقف الإنتاج، تسريب بيانات العملاء، فقدان الثقة، وانهيار أسهم الشركات.

مثال: هجوم (2017) "WannaCry" ألحق أضرارًا بأكثر من 200,000, مؤسسة في 150 دولة، وشلّ مستشفيات وشركات نقل ومصانع.

ب- سباق التسلح الرقمي وتأثيره على السوق

. الدول تنفق مبالغ ضخمة على تطوير الدفاعات الرقمية، بما في ذلك الذكاء الاصطناعي، وتكنولوجيا الحوسبة الكمية.

. هذا يؤدي إلى إعادة توزيع الاستثمارات العالمية، ويمنح الأفضلية للدول ذات التقدم التكنولوجي.

ج– زعزعة سلاسل الإمداد العالمية

. الهجمات على أنظمة الموانئ، الشحن، والطيران يمكن أن تعطل التجارة الدولية.

. التوتر السيبراني بين القوى الكبرى) مثل أمريكا والصين (أدى إلى تسيس التكنولوجيا وفصل الأسواق الرقمية.

مثال: العقوبات الأمريكية على شركة "Huawei" الصينية أثرت في البنية الرقمية العالمية وخلقت انقسامًا تقنيًا بين الشرق والغرب (Singer, P. W,2014,69) .

خلاصة التحليل الجيوسياسي

التأثير الجيوسياسي	المجال
على المعلومات، ضعف الردع، تهديد مباشر للسيادة الوطنية	الأمن القومي
تعطيل التجارة، خسائر فادحة، خلل في سلاسل الإمداد، تسابق استثماري في الأمن السيبراني	الاقتصاد العالمي

ثالث: طبيعة الهجوم السيبراني

1– **الهجمات السيبرانية على البنى التحتية،** يقوم المهاجمون باختراق أنظمة التحكم الصناعية مثل (SCADAأو ICS) المستخدمة لإدارة وتشغيل هذه المنشآت. الهدف قد يكو ن:(59justin ,2018,p
.(Joque

. تعطيل الخدمة مؤقتا أو لفترة طويلة

. تدمير الأنظمة للتحقيق في الأضرار الجسيمة

. الابتزاز أو الضغط السياسي

. إثارة الفوضى وبث الذعر بين السكان أمثلة واقعية:

أ .هجوم أوكرانيا(2015):

هجوم سيبراني تسبب في انقطاع الكهرباء عن مئات الآلاف من المنازل، ويُعد من أوائل الهجمات الناجحة على شبكة كهرباء.

ب .هجوم على منشآت المياه في إسرائيل(2020):

محاولة اختراق أنظمة المياه بهدف تغيير كميات الكلور، مما كان سيهدد سلامة السكان.

ج .هجوم على خط أنابيب "كولونيال" في الولايات المتحدة(2021):

أدى إلى شلل مؤقت في إمدادات الوقود على الساحل الشرقي، وخسائر اقتصادية ضخمة.

خطورة هذا النوع من الهجمات:

قد يؤدي إلى شلل في الحياة اليومية.

- يُعرض حياة الناس للخطر، خاصة في المشافي أو أنظمة النقل.
- يُضعف ثقة المواطنين في الدولة ومؤسساتها.
- يُعد عملًا عدائيًا يقترب من إعلان الحرب الفعلية.

كيف يتم الحماية منها؟

- تحديث الأنظمة الأمنية باستمرار.
- فصل أنظمة التحكم الحساسة عن الإنترنت قدر الإمكان.
- تدريب الطواقم الفنية على كشف ومحاكاة الهجمات.
- مراقبة النشاطات الشبكية وتحليل السلوك الشاذ.

2-**الهجمات على الأنظمة العسكرية: للتجسس أو تعطيل قدرات الردع والدفاع**

تعد الأنظمة العسكرية من أكثر الأهداف حساسية في الصراع السيبراني، حيث يؤدي اختراقها إلى تهديد مباشر للأمن القومي والسيادة الوطنية. وتشمل هذه الأنظمة شبكات الاتصالات العسكرية، أنظمة التحكم بالأسلحة، الأقمار الصناعية، نظم الرادار، ومراكز القيادة والتحكم.

Nazario (160Jose ,2009,p)

أهداف الهجمات السيبرانية على الأنظمة العسكرية:

أ- تعطيل قدارت الردع والدفاع:

مثل تعطيل أنظمة الدفاع الجوي أو التشويش على أنظمة الاتصالات خلال فترات التوتر أو الصراع.

ب- التلاعب أو زرع برمجيات خبيثة:(Malware)

لاستخدامها لاحقًا في تعطيل أو تدمير المعدات العسكرية في لحظة حرجة.

ت- التشويش على الأقمار الصناعية العسكرية:

مما قد يؤدي إلى فقدان السيطرة على الطائرات بدون طيار أو الصواريخ الموجهة.

ث- التجسس الإلكتروني (Cyber Espionage) :

لاختراق قواعد البيانات السرية وسرقة معلومات استخباراتية، خطط عسكرية، مواقع قواعد أو تحركات القوات.

أمثلة واقعية:

- هجوم الصين على قاعدة بيانات مكتب شؤون الموظفين الأمريكي (OPM) عام 2015: تم خلاله تسريب معلومات حساسة تخص موظفين في الجيش والاستخبارات.
- محاولات اختراق أنظمة الدفاع الأمريكية والNATO :

تشمل هجمات معقدة تنفذها دول أو مجموعات مدعومة من حكومات بهدف جمع معلومات

أو)Julie E. Mehan,2008,p41(. اختبار الدفاعات

فيروس:(2010) Stuxnet

يُعتقد أنه استخدم لتعطيل برنامج إيران النووي، وهو مثال على هجوم سيبراني يُصنف تحت نطاق الهجمات العسكرية غير التقليدية.

خطورة هذا النوع من الهجمات:

- يُضعف الجاهزية العسكرية للدولة.
- قد يؤدي إلى شلل في أنظمة الدفاع في لحظة هجوم فعلي.
- يفتح المجال لأعمال عدوانية تقليدية في ظل غياب الرد الرقمي.
- يشكل خرقًا خطيراً للسيادة والردع الاستراتيجي.

الحماية والاستجابة:

- تطوير وحدات "الجيش السيبراني" في العديد من الدول.
- استخدام الذكاء الاصطناعي لرصد الهجمات المتقدمة.
- بناء أنظمة عسكرية مغلقة غير متصلة بالإنترنت. (Air-Gapped Networks)
- تعزيز التعاون الأمني والاستخباراتي بين الحلفاء.

3- **الهجمات الاقتصادية: كاختراق البنوك وسرقة البيانات المالية أو ضرب الثقة في الأسواق**

تعد الهجمات الاقتصادية من أخطر أشكال الصراع السيبراني نظراً لتأثيرها المباشر على الاستقرار المالي للدول والشركات والأفراد. وتركّز هذه الهجمات على ضرب المؤسسات الاقتصادية الحساسة مثل البنوك، البورصات، الشركات الكبرى، أو حتى سلاسل الإمداد. (Lillian ,2017,p78

.(Ablon and Andy Bogart

أهداف الهجمات الاقتصادية:

أ- اخت ارق الأنظمة المصرفية:

بهدف سرقة أموال أو بيانات عملاء حساسة تستخدم لاحقًا في الابتزاز أو في عمليات غسيل أموال.

ب- ضرب الثقة في الأسواق المالية:

من خلال تعطيل البورصات أو نشر أخبار كاذبة تؤدي إلى انهيارات في الأسهم أو تغير سلوك المستثمرين.

ت- شل الشركات الكبر ى:

عبر هجمات الفدية (Ransomware) أو حجب الخدمة (DDoS) ، مما يوقف الإنتاج أو يعطّل الخدمات لفترة طويلة(Marie Baezner,2019,p61).

ث- استهداف سلاسل التوريد العالمية:

مثل الهجوم على أنظمة الشحن أو النقل، مما يؤثر على التجارة الدولية والإمدادات الأساسية.

أمثلة واقعية:

هجوم:(2017) "WannaCry" .

تسبب في شلل الآلاف من الأنظمة حول العالم، بما في ذلك أنظمة مصرفية وشركات مالية.

الهجوم على بنك بنغلاديش(2016):

تم خلاله تحويل 81 مليون دولار من البنك المركزي عن طريق أوامر مزورة عبر نظام.SWIFT هجمات الفدية على شركات الطاقة واللوجستيات: (Peter Pascucci,2017,p416)أدت إلى توقفات مكلفة وتراجع في ثقة المستثمرين في بعض الأسواق.

خطورة هذا النوع من الهجمات:

- خسائر مالية مباشرة ضخمة.
- فقدان ثقة المستثمرين والعملاء في المؤسسات المالية.
- اضطراب الأسواق وزعزعة الاستقرار الاقتصادي للدول.
- ارتفاع التكاليف الأمنية وزيادة أسعار الخدمات بسبب الإنفاق على الحماية.

آليات الحماية:

- تشفير المعاملات والبيانات المالية.
- مراقبة الأنظمة المالية باستخدام الذكاء الاصطناعي لرصد الأنماط المشبوهة.
- تدريب العاملين في القطاع الاقتصادي على الأمن السيبراني.
- التعاون بين القطاعين العام والخاص لرصد الهجمات والرد عليها سريعًا.

4- حروب المعلومات: نشر الشائعات والمعلومات المضللة للتأثير على الأري العام أو الانتخابات

حروب المعلومات هي أحد أكثر أشكال الص ارع السيبراني تأثيراً وخطورة، حيث تستهدف عقول الناس ووعيهم بدلاً من الأنظمة أو البنى التحتية. تعتمد هذه الحروب على نشر الشائعات، المعلومات المضللة، والتلاعب بالمحتوى الرقمي لتوجيه ال أري العام، التأثير في السلوك الاجتماعي، أو تقويض الثقة بالمؤسسات. (Michael Robinson,2015,p79) .

أهداف حروب المعلومات:

أ- التأثير على الانتخابات وصنع القرار السياسي.

عبر التلاعب بالرأي العام ونشر حملات تضليل تستهدف مرشحين أو أحزابًا معينة.

ب- نشر الفوضى وزرع الشكوك داخل المجتمع.

مثل نشر معلومات كاذبة حول أزمات صحية، كوارث وهمية، أو أخبار مزيفة تمس الأمن.

ت– تقويض الثقة بالمؤسسات الحكومية والإعلامية.

مما يفتح الباب أمام اضطرابات داخلية وانقسامات مجتمعية.

ث– دعم أجندات خارجية.

حيث تستخدم المعلومات كأداة ناعمة في الحروب الباردة الحديثة.

أمثلة واقعية:

. التدخل الروسي في الانتخابات الأمريكية(2016):

عبر حملات إعلامية مزيفة على وسائل التواصل الاجتماعي للتأثير على الناخبين الأمريكيين.

نشر شائعات خلال جائحة كورونا:

مثل نظريات المؤامرة حول اللقاحات أو وجود الفيروس، والتي أربكت جهود الاستجابة الصحية في العديد من الدول.

. استخدام الذكاء الاصطناعي لإنشاء "الديب فيك:(Deepfake) " لتزوير مقاطع فيديو تظهر شخصيات عامة تقول أو تفعل أشياء لم تحدث.

وسائل حروب المعلومات:

- وسائل التواصل الاجتماعي(فيسبوك، تويتر، تيك توك).
- مواقع إلكترونية مُصمَّمة لنشر التضليل.
- حسابات مزيفة أو "روبوتات" آلية.(Bots)
- مقاطع فيديو وصور مزيفة يصعب التحقق من صحتها.

آليات المواجهة:

. رفع الوعي الرقمي لدى الجمهور وتطوير مهارات التحقق من المعلومات.

. مراقبة منصات التواصل الاجتماعي واستخدام الذكاء الاصطناعي لرصد الحملات المنظمة.

. تعزيز الشفافية الإعلامية ودعم الصحافة المهنية.

. سن قوانين تجرّم التضليل الإلكتروني والتحريض عبر الشبكات.

5–التجسس الإلكتروني: لاختراق مؤسسات حكومية أو صناعية بهدف سرقة معلومات حساسة

يُعد التجسس الإلكتروني (Cyber Espionage) أحد أبرز أدوات الصراع السيبراني، ويستهدف بشكل أساسي اختراق المؤسسات الحكومية، العسكرية، أو الصناعية بغرض سرقة معلومات حساسة أو سرية. وهو شكل من أشكال التجسس الحديث الذي يتم عبر الإنترنت، دون الحاجة إلى وجود فيزيائي للجاسوس (Michael Joseph Gross,2011,p34).

أهداف التجسس الإلكتروني:

أ- سرقة البيانات الحكومية والعسكرية الحساسة، مثل الخطط الأمنية، خرائط البنية التحتية، أو الملفات الدبلوماسية.

ب- التجسس الصناعي والتجاري، للحصول على أسرار براءات الاختراع أو تقنيات متقدمة تستخدم في المنافسة الاقتصادية.

ت- اختراق البريد الإلكتروني للمسؤولين، للحصول على معلومات داخلية أو نشرها لاحقًا بغرض الابتزاز أو الإحراج السياسي.

ث- زرع برمجيات تجسسية، لجمع معلومات على المدى الطويل دون أن يشعر بها الهدف.

أمثلة واقعية:

- "Titan Rain" عملية سلسلة من الهجمات السيبرانية استهدفت أنظمة أمريكية عسكرية وصناعية في أوائل الألفينات ، نُسبت إلى جهات صينية.

اختراق شركة:(2020) "SolarWinds"

تم استغلال برمجيات الشركة للوصول إلى شبكات حكومية أمريكية حساسة، بما في ذلك وزارات الدفاع والخزانة والطاقة.

- هجمات على شركات التكنولوجيا:

مثل محاولات مستمرة لاختراق شركات متخصصة في الذكاء الاصطناعي أوالصناعات العسكرية بهدف سرقة الأبحاث. (Rose McDermott,2019,p307)

خطورة هذا النوع من الهجمات:

- تهديد مباشر للأمن القومي.
- فقدان ميزة تكنولوجية أو معلوماتية استراتيجية.
- التأثير على الاقتصاد في حال تسرب أسرار صناعية.
- زعزعة الثقة في أمن المؤسسات المستهدفة.

طرق الحماية:

- تشفير الاتصالات والبيانات الحساسة.
- تقليل عدد الأجهزة المتصلة بالإنترنت في المؤسسات الحساسة.
- مراقبة الشبكات وتحليل الأنشطة المشبوهة.
- تعزيز وعي الموظفين بمخاطر الهندسة الاجتماعية والاختراقات.

أمثلة واقعية للصراع السيبراني

هجوم (Stuxnet 2010): فيروس سيبراني يُعتقد أن الولايات المتحدة وإسرائيل استخدمتاه لتعطيل البرنامج النووي الإيراني.

هجمات روسيا الإلكترونية: تورطت روسيا في العديد من الهجمات على أوكرانيا ودول أوروبية

وأمريكا، خصوصًا خلال الانتخابات.

هجمات على البنية التحتية في الشرق الأوسط: مثل الهجمات على منشآت النفط، والتي نُسبت إلى جماعات مدعومة من دول. (Rid,2013,p69)

رابعاً: دوافع الصراع السيبراني

- تحقيق التفوق الاستراتيجي دون تكلفة الحروب التقليدية
- التجسس وجمع المعلومات الاستخباراتية
- إضعاف الخصوم اقتصاديًا أو سياسيًا
- نشر الأيديولوجيات أو زعزعة الاستقرار
- **خامساً: آثار الصراع السيبراني**

أ- انهيار الثقة في الأنظمة الإلكترونية

ب- خسائر اقتصادية ضخمة

ت- تهديد الأمن القومي

ث- التأثير على الحياة اليومية للأفراد ج- نشر الفوضى والمعلومات الكاذبة

طرق المواجهة والحماية

- تعزيز الأمن السيبراني الوطني وتطوير قدرات الدفاع الرقمي.
- التعاون الدولي وتبادل المعلومات بين الدول.
- سن تشريعات إلكترونية تنظم الفضاء السيبراني وتعاقب المعتدين.
- تدريب الكوادر البشرية لمواجهة التهديدات الحديثة.
- التوعية العامة بمخاطر الهجمات الإلكترونية وأساليب الوقاية.

سادساً: اشهر الهجمات السيبرانية الهجمات الالكترونية

الهجمات الالكترونية الأسوأ، والمثيرة للجدل، والشائكة إلى حد ما. ويرجع سبب إدراجنا لتلك الهجمات في قائمتنا إلى أنها نالت الحظ الأكبر من الاهتمام لأسباب عدة؛ حيث كانت منتشرة على نطاق واسع، ربما، أو لأنها كانت تمثل إشارات لاتجاهات كبيرة ومخيفة. (Omry Haizler ,2017,p37)، فيما يلي الهجمات الالكترونية الهجمات السيبرانية في التاريخ المعاصر :

- هجومWannaCry

هجوم WannaCry هو هجوم باستخدام ب ارمج الفدية الضارة وانتشر سريعًا في مايو 2017. ومثل كل برامج الفدية الضارة، استولى على أجهزة الكمبيوتر المخترقة وقام بتشفير المحتويات الموجودة على الأقراص الصلبة، وطلب بعد ذلك دفع فدية بعملة البيتكوين المُشفرة لفك

تشفيرها. وتم تثبيت البرنامج الضار بشكل خاص في أجهزة الكمبيوتر بالمستشفيات التي تديرها هيئة الخدمات الصحية الوطنية البريطانية.(NHS)

إلا أن هذا البرنامج الضار ليس شيئًا جديدًا. ما جعل هجوم WannaCry كبي ارً ومخيفا، الوسائل التي استخدمها للنشر؛ فقد استغل إحدى الثغرات في Microsoft Windows واستخدم إحدى التعليمات البرمجية التي طورتها وكالة الأمن القومي الأمريكية وبشكل سري. يُطلق على أداة استغلال الثغرات هذه اسمEternalBlue ، وقد تمت سرقتها واختراقها من إحدى المجموعات المخترقة التي تُطلق على نفسها اسم .Shadow Brokers وقامت شركة Microsoft بالفعل بتصحيح الثغرة قبلها بأسابيع قليلة، لكن لم يتم تحديث العديد من الأنظمة. كانت شركة Microsoft غاضبة لأن الحكومة الأمريكية قد طورت سلاحًا لاستغلال الثغرات بدلاً من مشاركة المعلومات بخصوص الفجوة مع مجتمع أمن المعلومات ، ومن اشهر هذه الهجمات:-

- NotPetya

كان هجوم Petya مجرد جزء من أجزاء البرامج الضارة عندما بدأ تداوله عبر البريد العشوائي المتصيد في 2016، وكان من بين اهم اسباب شهرته انه قام بتشفير سجل التشغيل الرئيسي في الأجهزة المخترقة ، وهو ما ساعد على منع المستخدمين من الوصول الى الملفات الخاصة بهم بعد ذلك، وبشكل مفاجئ في يونيو 2017 ، بدأ انتشار نسخة اكثر خبثا من البرنامج الضار. كان مختلفا عن البرنامج الأصلي الذي تم تجاهله;NotPetya ظهر في الاساس عبر احد برامج المحاسبة الاوكرانية المخترقة ،وانتشر عبر أداة استغلال الثغرات EternalBlue ذاتها والتي استخدمها هجوم .WannaCry ويغُلب الظن أن NotPetya هو هجوم إلكتروني شنته روسيا ضد أوكرانيا، رغم أن روسيا قد أنكرت ذلك، وهو ما يفتح الباب أمام عصر محتمل من البلدان التي تستخدم البرامج الضارة كسلاح لها.(Rosenfield,2015,p25)

- Ethereum

قد لا يُمثل هذا النوع أهمية كبيرةً مثل بعض الأنواع الأخرى بالقائمة، لكن يستحق إلقاء نظرةً عليه هنا نظراً للكم الهائل من مبالغ الأموال المتكبدة Ether .عملة مشفرة مثل عملة البيتكوين، وفي شهر يوليو تمت سرقة مبلغ قدره 4.7 ملايين دولارات أمريكية بعملة Ether وذلك في غضون بضع دقائق. وبعد ذلك، وبعد بضعة أسابيع فقط تمت سرقة 32 مليون دولا ارً أمريكيًا. وقد أثارت الحادثة بكاملها الأسئلة بخصوص أمن العملات القائمة على تكنولوجيا البلوك تشين.(blockchain)

- Equifax

إحدى وكالات التصنيف الائتماني الكبيرة أعلنت في يوليو 2017 أن مجرمون قد استغلوا ثغرةً بأحد مواقع الويب الأمريكية الخاصة بتقديم الطلبات للحصول على بعض الملفات،" وتمكنوا

من الحصول على معلومات شخصية لحوالي 150 مليون شخصًا. وقد ازدت النتائج المترتبة على ذلك من غضب الأشخاص، ولاسيما عندما كان موقع الويب Equifax الذي يرجع إليه الأشخاص للتحقق من حالة اختراق المعلومات، يبدو مصممًا بصورة رئيسية لبيع خدمات.Equifax إيد سزوفير، الرئيس التنفيذي لشركةSenecaGlobal ، أوضح أن اخت ارق Equifax كان سيئًا بصفة خاصة "لأن الموقع قد تم إخطاره بالحل وكان الحل يتطلب تنفيذه في أداة يُطلق عليها Apache Struts والتي كانوا يستخدمونها جيدًا قبل حتى حدوث الاختراق. ولكنهم فشلوا في القيام بذلك في الوقت المناسب. ومن أجل منع حدوث مثل تلك الاختراقات، يتطلب الأمر إجراء تغيير في الثقافة والمصادر؛ لم تكن هناك مشكلة تقنية، حيث كان الحل التقني معروفًا بالفعل. من المؤكد أن موقع Equifax كانت لديه المصادر، لكن لم تكن لديه الثقافة المناسبة للتأكد من تطبيق الإجراءات الصحيحة".

- Yahoo

نال هذا الاختراق الكبير لنظام البريد الإلكتروني الخاص بشركة Yahoo اهتمامًا كبيراً لأنه ورغم حدوثه منذ وقت طويل في عام 2013، لكن تداعياته، فيما يتعلق بعناوين البريد الإلكتروني الخاص بشركة Yahoo البالغ عددها 3 مليار عنوان بريد إلكتروني والتي تم اختراقها، ظهرت فقط في أكتوبر 2017. وشملت المعلومات المسروقة كلمات المرور وعناوين البريد الإلكتروني المنسوخة، والمُشفرة باستخدام تقنيات غير محدثة، وسهلة الفك من حيث التشفير، وهو نوع من المعلومات يمكن أن يستخدمه المهاجمون لاختراق حسابات أخرى. وبالإضافة إلى الأضرار التي لحقت بأصحاب الحسابات، تسبب الاختراق في إعادة النظر في صفقة شراء Verizon لشركةYahoo ، حتى على الرغم أن الصفقة قد تمت بالفعل. (Evgeny Morozov,2010,p27) .

الشيء المخيف حقًا في هذا الاختراق أن ثقافة السرية التي ظلت طي الكتمان تعني أن هناك الكثير بالخارج. "لا يوجد أحد متحمس لمشاركة الاختراق، لأسباب واضحة تتعلق بالعلاقات العامة "حسبما ورد على لسان ميتش ليبرمان، مدير الأبحاث في" .G2 Crowd لكن تظهر الحقيقة في نهاية المطاف. ما الأشياء الأخرى التي لا نعرفها؟"

- GitHub

في 28 فبراير ،2018، تم اختراق الإصدار المتحكم في خدمة المضيف GitHub بهجوم حجب الخدمات، حيث تم إرسال بيانات بلغت 35.1 تيرابايت في الثانية إلى الموقع المشهور. ورغم أن GitHubقد تعرض فقط لعملية قطع اتصاله بالإنترنت بصورة متقطعة ورغم نجاحه في صد الهجوم كلياً بعد أقل من 20 دقيقةً، كانت الآثار الهائلة المترتبة على الاعتداء مثيرة للقلق؛ وتجاوز الهجوم الضخم على Dyn في أواخر 2016حيث بلغ الحد الأقصى للبيانات المرسلة 2.1

تيرابايت في الثانية.

وكانت المشكلة الأكبر تتمثل في البيئة الأساسية التي ساعدت على الهجوم. كان هجوم Dyn ناجمًا عنMirai botnet، والذي تطلب وجود برنامج ضار لاختراق الآلاف من الأجهزة، لكن هجوم GitHubاستغل أجهزة السيرفر التي تشغل نظام التخزين المؤقت للذاكرة، والتي يمكنها إعادة مجموعات ضخمة للغاية من البيانات استجابةً للطلبات البسيطة.

تم تصميم Memcached لاستخدامه فقط مع أجهزة السيرفر المحمية التي تعمل على الشبكات الداخلية، وكوسيلة أمان بعض الشيء لمنع المهاجمين الضارين من تزييف عناوين IP وإرسال كميات كبيرة من البيانات إلى الضحايا الغافلين. ولسوء الحظ، تعتمد الآلاف من أجهزة السيرفر Memcached على الإنترنت المفتوح، وكانت هناك زيادة كبيرة في استخدامه أثناء هجمات .DDoS إن القول بأن أجهزة السيرفر "مخترقة" بالكاد يكون أمراً معقولاً، لأنها سترسل الحزم بكل أريحية إلى أي مكان يتم مطالبتها به دون توجيه الأسئلة.

بعد أيام فقط على هجوم GitHub، تم شن هجوم آخر بواسطة DDoS القائم على Memecached، في أحد الشركات الأمريكية المُقدمة للخدمات ولم يتم ذكر اسمها وتم إرسال بيانات بلغت 7.1 تيرابايت في الثانية (Robert Kaiser,2015,p13) .

النتائج والتوصيات :

أولاً : النتائج

1.تحول الفضاء السيبراني إلى ساحة صراع مركزية: أصبح الفضاء الإلكتروني مجالاً رئيسيًا للصراع، لا يقل أهمية عن البر والبحر والجو، حيث تستخدمه الدول والجماعات لتحقيق أهداف سياسية، اقتصادية، وعسكرية دون الحاجة لاستخدام القوة التقليدية.

2.تعقيد الصراع السيبراني وصعوبة رصده: يتميز الصراع السيبراني بعدم وضوح الفاعلين وسرعة التنفيذ، مما يصعّب من عملية التتبع والمحاسبة، ويجعل الاستجابة للتهديد أكثر تعقيدًا.

3.تزايد استهداف البنية التحتية الحيوية: عد الهجمات على قطاعات مثل الكهرباء، المياه، الصحة، والنقل من أخطر أشكال الهجمات السيبرانية، لما لها من تأثير مباشر على الحياة اليومية والأمن القومي.

4.الخطر على الأنظمة العسكرية والأمنية: يهدد الصراع السيبراني قدرات الردع والدفاع للدول، ويزيد من احتمالات الحرب الهجينة أو المواجهة غير المعلنة.

5.أثر اقتصادي بالغ الخطورة: الهجمات على المؤسسات الاقتصادية تؤدي إلى خسائر مالية ضخمة، وتعطل الثقة في الأسواق والأنظمة البنكية، كما تؤثر على سلاسل التوريد الدولية.

6.انتشار حروب المعلومات والتضليل الإعلامي: تؤدي حروب المعلومات إلى تشويه الحقائق، التأثير في الانتخابات، وزعزعة استقرار المجتمعات، ما يجعلها من الأدوات الأكثر فاعلية وخطورة.

7.قصور في التشريعات الدولية المنظمة للصراع السيبراني: لا يوجد حتى الآن إطار قانوني دولي شامل ينظم الحروب السيبرانية، مما يخلق فراغًا قانونيًا يسمح بوقوع الانتهاكات دون مساءلة.

8.تفاوت قدرات الدول في الحماية السيبرانية: تختلف إمكانيات الدول بشكل كبير في مجال الأمن السيبراني، مما يجعل الدول النامية أكثر عرضة للهجمات مقارنة بالدول المتقدمة.

ثانيا: التوصيات

1.تعزيز الأمن السيبراني الوطني: تطوير استراتيجيات وطنية متكاملة تشمل الحماية، الكشف ،الاستجابة، والتعافي من الهجمات السيبرانية، وتأسيس وحدات سيب ارنية متخصصة.

2.بناء تحالفات دولية سيبرانية: تعزيز التعاون الدولي بين الدول في مجال تبادل المعلومات، التدريب، والاستجابة الجماعية للهجمات السيبرانية.

3.سن تشريعات وطنية ودولية واضحة: ضرورة وضع قوانين تنظم قواعد الصراع السيبراني، وتحديد مسؤوليات الدول في الفضاء الإلكتروني، بما يضمن الردع والمساءلة.

4.رفع الوعي المجتمعي: تنظيم حملات تثقيفية حول الأمن السيبراني للمواطنين، وتدريب العاملين في القطاعات الحساسة على أفضل ممارسات الحماية الرقمية.

5.حماية البنية التحتية الحساسة: تحديث أنظمة التحكم الصناعية، فصل الشبكات الحرجة عن الإنترنت، وتطبيق معايير أمن صارمة في مرافق الطاقة، الصحة، والمصارف.

6.الاستثمار في البحث والتطوير السيبراني: دعم مراكز البحث الوطنية المتخصصة في الأمن السيبراني، وتشجيع الابتكار في التقنيات الدفاعية والهجومية الأخلاقية.

7.تعزيز الشفافية والمساءلة: تطوير آليات لرصد الهجمات والإعلان عنها بشفافية لتعزيز الثقة، وتحسين سُبل الوقاية والاستجابة.

8.الاهتمام بالذكاء الاصطناعي وتحليل البيانات:توظيف أدوات الذكاء الاصطناعي لرصد الأنماط الغريبة في الشبكات، والتنبؤ بالتهديدات قبل وقوعها.

المصادر

1. Ablon, L., & Bogart, A. (2017). *Zero days, thousands of nights: The life and times of zero-day vulnerabilities and their exploits*. RAND Corporation.
2. Baezner, M. (2019). *Iranian cyber-activities in the context of regional rivalries and international tensions*. ETH Zurich.
3. Brito, J., & Watkins, T. (2011). Loving the cyber bomb: The dangers of threat inflation in cybersecurity policy. *Harvard National Security Journal*, *3*(1).
4. Clarke, R. A., & Knake, R. K. (2010). *Cyber war: The next threat to national security and what to do about it*. HarperCollins.

5. Delbert, R. (2013). *Black code: Surveillance, privacy, and the dark side of the Internet*. Signal.
6. Gross, M. J. (2011). A declaration of cyber-war. *Vanity Fair, 53*.
7. Haizler, O. (2017). The United States' cyber warfare history: Implications on modern cyber operational structures and policymaking. *Cyber, Intelligence, and Security, 1*(1), 31–54.
8. Joque, J. (2018). *Deconstruction machines: Writing in the age of cyberwar*. University of Minnesota Press.
9. Kaiser, R. (2015). The birth of cyberwar. *Political Geography, 46*, 11–20.
10. Liff, A. P. (2012). Cyberwar: A new "absolute weapon"? The proliferation of cyberwarfare capabilities and interstate war. *Journal of Strategic Studies, 35*(3), 401–428.
11. Manjikian, M. M. (2010). From global village to virtual battlespace: The colonizing of the Internet and the extension of realpolitik. *International Studies Quarterly, 54*(2), 381–401.
12. McDermott, R. (2019). Some emotional considerations in cyber conflict. *Journal of Cyber Policy, 4*(3), 299–315.
13. Mehan, J. E. (2008). *Cyberwar, cyberterror, cybercrime*. IT Governance Publishing.
14. Morozov, E. (2010). Battling the cyber warmongers. *The Wall Street Journal*.
15. Nazario, J. (2009). Politically motivated denial of service attacks. In *The virtual battlefield: Perspectives on cyber warfare* (pp. 163–181).
16. Pascucci, P. (2017). Distinction and proportionality in cyberwar: Virtual problems with a real solution. *Minnesota Journal of International Law, 26*.
17. Rid, T. (2012). Cyber war will not take place. *Journal of Strategic Studies, 35*(1), 5–32.
18. Rid, T. (2013). *Cyber war will not take place*. Oxford University Press.
19. Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies, 38*(1–2), 4–37.
20. Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: Issues and challenges. *Computers & Security, 49*, 70–94.
21. Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.
22. Whetham, D. (2016). Cyber chevauchées: Cyber war can happen. In *Binary bullets: The ethics of cyberwarfare*.