الحرب السيبرانية وأثرها في العلاقات الدولية: حرب الكيان الصهيوني على حزب الله أنموذجا[▽]

Cyber warfare and its impact on international relations: The Zionist entity's war on Hezbollah as a model

أ.م.د. سعود محمد الشاوش* Dr. Saoud Muhammad Al-Shawesh

الملخص:

تعد الحرب السيبرانية مفهوما حديثا للحروب، والتي ارتبط ظهورها ارتباطاً وثيقا نتيجة للتقدم الهائل الذي صاحب تطور وتقدم تكنولوجيا المعلومات والاتصالات، وهدفت هذه الدراسة الى التعرف على الحروب السيبرانية وأثرها في العلاقات الدولية، وأورد الباحث أنموذجا لها والمتمثل بحرب الكيان الصهيوني على حزب الله، مستخدما في ذلك المنهج الوصفي التحليلي، بالإضافة إلى منهج القوة في العلاقات الدولية، ومنهج النظم، وصاغ فرضية الدراسة بالقول: لا تعد الحرب السيبرانية ذات تأثير مهم في العلاقات الدولية.

وقد أثبتت الدراسة عدم صدقية هذه الفرضية، حيث أن الحرب السيبرانية ذات أهمية كبرى في التأثير على العلاقات الدولية بل ومقدمة لحروب عسكرية شاملة فيما بعد استخدامها، وقد توصلت الدراسة إلى عدد من النتائج كان من أهمها: أن معظم دول العالم تدرك مدى أهمية تطوير استراتيجيات حديثة للحروب تخضع بها الخصوم بتكاليف مادية وبشرية قليلة، كما أنه لا يمكن الاستغناء عن القوة العسكرية(الصلبة) بعد استخدام الحرب السيبرانية، فالحرب الصلبة هي تالية لها، وكان ذلك واضحا وبينا عندما قام الكيان الصهيوني بشن هجماته السيبرانية على حزب الله كمقدمة لشن الحرب العسكرية الشاملة على الحزب، كما توصلت الدراسة إلى التأكيد على أهمية الاستفادة من التقدم التكنولوجي في بناء الجيوش الحديثة ومن ضمنها القوة السيبرانية.

الكلمات المفتاحية: الحرب السيبرانية–القوة الناعمة –العلاقات الدولية– حزب الله–الكيان الصهيوني.

Abstract:

Cyber warfare is a modern concept of warfare, the emergence of which is closely linked to the tremendous progress that accompanied the development and advancement of information and communications technology. This study aimed to identify cyber warfare and its impact on international relations. The researcher provided a model for it, represented by the war of the Zionist entity on Hezbollah, using the descriptive analytical approach, in addition to the approach of power in international relations, and the approach of systems. He formulated the hypothesis of the study by saying: Cyber ??warfare does not have a significant impact on international relations. The study proved the invalidity of

▽ تاريخ التقديم : 2025/1/7 تاريخ القبول: 2025/2/10 تاريخ النشر: 2025 /3/31

* مركز الدراسات السياسية والاستراتيجية، جامعة صنعاء saoud.alshawesh@su.edu.ye

this hypothesis, as cyber warfare is of great importance in influencing international relations and even a prelude to comprehensive military wars after its use. The study reached a number of results, the most important of which were: Most countries in the world realize the importance of developing modern strategies for wars that subjugate opponents at low material and human costs. It is also impossible to dispense with military (hard) power after using cyber warfare, as hard warfare follows it. This was clear and evident when the Zionist entity launched its cyber attacks on Hezbollah as a prelude to launching a comprehensive military war on the party. The study also concluded that it is important to benefit from technological progress in building modern armies, including cyber power.

Keywords: Cyber warfare – soft power – international relations – Hezbollah – the Zionist entity.

المقدمة:

استخدام القوة في العلاقات الدولية أمر شائع ومنذ مئات السنين، والذي اختلف فقط هو في نوعية القوة المستخدمة، وبعد أن كانت القوة العسكرية المسلحة هي الشائعة في تلك الحروب بدأ الاعتماد على قوى أخرى غير تلك القوة والتي كانت تعرف بالقوة الصلبة لتحل محلها قوى أخرى أقل تكلفة وأكثر فتكا وتأثيرا والتي تسمى بالقوة الناعمة، ومن ثم لم تعد الجيوش الجرارة التي تتكون من مئات الآلاف من المقاتلين وترسانة هائلة من الصواريخ والطائرات هي القوة الوحيدة ، بل أصبحت القوة التكنلوجية تأخذ موقع الصدارة من تلك القوى لتحل محلها.

وتعد الحرب السيبرانية واحدة من أهم وسائل الحروب الحديثة والتي شهدت تطورا ملحوظا، وتم استخدامها في العديد من الأماكن عبر العالم، ويعد الهجوم السيبراني الذي قام به الكيان الصهيوني على حزب الله اللبناني في17سبتمبر 2024 بمثابة المثال الأبرز والأكثر تأثيرا على الإطلاق والأول من نوعه على مستوى العالم، وكان ذلك الهجوم بمثابة المقدمة للحرب الصلبة التي شنها الكيان الصهيوني على لبنان فيما بعد ذلك الهجوم.

مشكلة الدراسة:

مشكلة الدراسة تتمثل في السؤال الرئيس الآتي:

ما هو تأثير حرب الكيان الصهيوني على حزب الله في ضوء توظيف القوة السيبرانية: كأسلوب جديد في الحرب ضد حزب الله؟

منهجية الدراسة:

اعتمدت الدراسة على المنهج الوصفي والذي يهتم بدراسة ووصف الظواهر والأحداث التي تكون محلا للدراسة، ويتم ذلك عن طريق جمع المعلومات والبيانات والحقائق عنها ووصف الظروف الخاصة بها كما

هي في الواقع وتحليلها وتفسيرها والحصول على تقديرات دقيقة لحدوثها [1] كما اعتمدت على المنهج الواقعي (القوة والمصلحة) والذي يقوم على أساس تحليل الأحداث الجارية في المجتمع الدولي على أساس الارتكاز على فكرتي القوة والمصلحة [2] كما اعتمدت الدراسة على منهج تحليل النظم" لديفيد استون" والذي يقوم على أساس وجود مدخلات عبارة عن مطالب ورغبات يتم إدخالها الى النظام السياسي ومن ثم تخرج على شكل قرارات وسياسات وأفعال يتم تطبيقها[3] .

أهداف الدراسة:

1-التعرف على الحرب السيبرانية وما هو أثرها في العلاقات الدولية.

2-استعراض بعضا من صور الحرب السيبرانية على مستوى العالم

3-وضع مقترحات لكيفية مواجهة الحرب السيبرانية.

حدود الدراسة:

الحدود الموضوعية:

تركز الدراسة على الحرب السيبرانية التي شنها الكيان الصهيوني على حزب الله.

الحدود المكانية: الأراضي اللبنانية.

الحدود الزمانية: العام 2024.

فرضية الدراسة:

لا تعد الحرب السيبرانية ذات تأثير مهم في العلاقات الدولية.

أهمية الدراسة:

1- الأهمية النظرية:

تعد هذه الدراسة من الدراسات القليلة التي تحدثت عن تأثير الحرب السيبرانية على العلاقات الدولية ومن الدراسات النادرة التي تناولت تطبيقا لتلك الحرب والمتمثل في الحرب السيبرانية التي شنتها الكيان الصهيوني ضد حزب الله اللبناني.

2-الأهمية العملية:

تعد الدراسة مرجعا لمن يبحث عن الحروب السيبرانية وأثرها على العلاقات الدولية، كما ستكون مرجعا لصناع القرار السياسي والأمني للتعرف على أثر تلك الحروب وكيفية مواجهتها.

([1]) بلبل ابتسام، قيمة الأمن السيبراني في توجهات السياسة الخارجية الروسية تجاه المنطقة الإفريقية، رسالة ماجستير (الجزائر: جامعة أمحمد بوقرة-بومرداس-كلية الحقوق والعلوم السياسية، قسم العلوم السياسية،2019-2020) ص 7.

([2]) طه حميد حسن العنبكي، نرجس حسين زاير العقابي، أصول البحث العلمي في العلوم السياسية (بغداد: دار اوما، الرباط: دار الأمان، الجزائر: منشورات الاختلاف، بيروت: منشورات ضفاف، الطبعة الأولى 1436هـ 2015م) ص88.

([3]) محمد شلبي، المنهجية في التحليل السياسي المفاهيم المناهج الاقترابات والأدوات(الجزائر،1997) ص17.

الدراسات السابقة:

1-دراسة فواز عبدالرحمن علي دودة: "الأمن السيبراني في الجمهورية اليمنية" [1] وتمثلت مشكلة الدراسة في التعرف على أهمية الأمن السيبراني للجمهورية اليمنية على الجانبين العام والخاص، ومدى توافر التقنيات والأنظمة والسياسات التي تحد من ظاهرة الجرائم السيبرانية، واستخدم الباحث المنهج الوصفي في دراسته، وكانت النتيجة الرئيسة للدراسة تتمثل في أن الجريمة السيبرانية عمل اجرامي وغير مشروع تستدعي معاقبة كل من يقوم بها أو يسهل حدوثها.

2-دراسة نبهان زمبور السعدي :"جيوبولتيك المخاطر السيبرانية للفضاء الإلكتروني على الأمن القومي لدول المشرق العربي" [2] وهدفت الدراسة إلى الكشف عن مفهوم الأمن السيبراني كمجال للجغرافيا السياسية، وكانت مشكلة الدراسة تتمثل في السؤال البحثي ما هو مفهوم ومخاطر الأمن السيبراني من منظور الجغرافيا السياسية، وتوصلت الدراسة إلى عدد من النتائج من أهمها أن معظم دول المشرق العربي تواجه مخاطر جيوبوليتكية لأمنها السيبراني.

3- دراسة عماد خليل إبراهيم، و نجوان هاني محمود " استخدام القوة السيبرانية في سياسات الدول الكبرى"[3] وكانت المشكلة البحثية للدراسة تتمثل في السؤال: كيف توظف الدول الكبرى القوة السيبرانية في إدارة سياساتها الدولية؟ وكانت فرضية الدراسة تقول: كلما حاولت الدول الكبرى استخدام القوة السيبرانية في سياساتها الدولية بهدف توطيد أمنها الوطني انعكس ذلك على زيادة التنافس فيما بينها، وتوصلت الدراسة إلى عدد من الاستنتاجات كان أهمها أن القوة السيبرانية باتت حقيقة مساندة للقوة التقليدية لبعض الدول وداعمة لها في العمليات العسكرية المختلفة.

4- دراسة محمد حسن سعيد دراجي، و عمر صالح العكور: "الهجمات السيبرانية وفقا لأحكام القانون الدولي الإنساني [4]وتمحورت مشكلة الدراسة في مدى إمكانية إخضاع الهجمات السيبرانية إلى القانون الدولي الإنساني، واستخدمت الدراسة المنهج الوصفي التحليلي، والمنهج القانوني ،والمنهج التاريخي، وتوصلت الدراسة إلى عدد من النتائج من أهمها: أن الهجمات السيبرانية تستخدم في النزاعات المسلحة

([1]) فواز عبدالرحمن علي دودة: "الأمن السيبراني في الجمهورية اليمنية" مجلة منارات الأمن (صنعاء: أكاديمية الشرطة، المجلد(1) العدد 11 يناير –يونيو2024).

([2]) نبهان زمبور السعدي "جيوبولتيك المخاطر السيبرانية للفضاء الإلكتروني على الأمن القومي لدول المشرق العربي"، مجلة مركز بابل للدراسات الإنسانية (المجلد14 العدد 2، 2024).

([3])عماد خليل إبراهيم، و نجوان هاني محمود "استخدام القوة السيبرانية في سياسات الدول الكبرى " المجلة العراقية للعلوم السياسية (السنة الخامسة العدد (10) آذار 2024).

([4]) محمد حسن سعيد دراجي، و عمر صالح العكور، "الهجمات السيبرانية وفقا لأحكام القانون الدولي الإنساني، دراسات: الشريعة والدراسات القانونية (المجلد51، العدد1، 2024).

ومن ثم فهي تخضع لأحكام القانون الدولي الإنساني، كما أنها تمثل اعتداء على أمن وسيادة الدول، وتعد انتهاكاً لميثاق الأمم المتحدة.

5-دراسة علاء الدين فرحات: "الحرب السيبرانية ومستقبل الأمن العالمي"[1] وتمثلت مشكلة الدراسة في السؤال: ما مدى تأثير الحروب السيبرانية على الأمن العالمي؟ ولم يستخدم الباحث منهجية للدراسة وتمثلت النتيجة الرئيسة للدراسة في أن الحروب القادمة ستكون حربا مدمرة ومعتمده بشكل كبير على الإنترنت والتكنولوجيا مستخدمة من أجل ذلك جيوشاً حديثة منظومتها القتالية سيبرانية، لتصبح بذلك ميدانا رابعا من ميادين الحرب.

5- دراسة أنعام عبد الرضا سلطان العكابي: " توظيف الحروب السيبرانية في تطوير مفهوم القوة للدول الكبرى"[2]، وكانت إشكالية الدراسة تتمثل في السؤال: ماهي العوامل المحفزة التي أسهمت في ظهور حروب الفضاء السيبراني وتوظيفها من قبل الدول الكبرى؟ واستخدمت الدراسة المنهج التحليلي الاستنباطي وتوصلت الدراسة إلى نتيجة رئيسة مفاداها أن السيبرانية أصبحت مجال آخر من مجالات استعراض القوى وممارسة النفوذ وتحقيق التفوق والتنافس الدولي.

6- دراسة أحمد محيي محمد أحمد علي: "أثر الحرب السيبرانية الإسرائيلية-الإيرانية على الأمن الإقليمي العربي" [3] وهدفت الدراسة إلى قياس وتحليل أثر الحرب السيبرانية-الإسرائيلية-الإيرانية على الأمن القومي العربي، وكانت مشكلة الدراسة تتمثل في السؤال: كيف تؤثر الحرب السيبرانية-الإسرائيلية على الأمن القومي العربي، وتوصلت الدراسة إلى عدد من النتائج كان من أهمها أنه من الممكن تكوين نظام أمني إقليمي عربي في المجال الأمني السيبراني حتى لو لم يتفق جميع أعضاء هذا النظام على التهديدات الأمنية.

تقسيم الدراسة:

تم تقسيم الدراسة على النحو الآتي:

أولاً: القوة السيبرانية: التعريف والبدايات والدوافع.

تعد القوة بكافة مكوناتها هدفا أساسياً تسعى كل الدول إلى الحصول عليها. ويعيش العالم على أعتاب ثورة نوعية جديدة يقودها الذكاء الاصطناعي وأنترنت الأشياء والطابعات ثلاثية الأبعاد والعملات الافتراضية والشرائح الذكية المغروسة في أجساد البشر، ويصبح المجتمع متآكلا لصالح الآلة على حساب الإنسان،

([1]) علاء الدين فرحات، الحرب السيبرانية ومستقبل الأمن العالمي، مجلة الناقد للدراسات السياسية، (المجلد6) العدد 2 (2022).

([2]) أنعام عبد الرضا سلطان العكابي، "توظيف الحروب السيبرانية في تطوير مفهوم القوة للدول الكبرى" مجلة قضايا سياسية، (جامعة النهرين: كلية العلوم السياسية، العدد 73، إبريل-مايو-يونيو2023).

([3]) أحمد محيي محمد أحمد علي، "أثر الحرب السيبرانية الإسرائيلية-الإيرانية على الأمن الإقليمي العربي" مجلة المعهد العالي للدراسات النوعية (مجلد 3 عدد 8 يوليو (2023).

وسيكون المجتمع الحالي هو المجتمع الخامس (مجتمع ما بعد المعلومات)، ويأتي تاليا بعد المجتمعات الأربعة السابقة عليه وهي مجتمعات الصيد، ومجتمع الزراعة، ومجتمع الصناعة، ومجتمع المعلومات [1].

1-التعريف:

تطلق كلمة "سيبراني" (cyber)على كل ما يتعلق بالشبكات الإلكترونية الحاسوبية وشبكة الأنترنت[2] أما الحرب السيبرانية فهي مصطلح واسع يصف استخدام القدرات السيبرانية في الفضاء السيبراني، من قبل دولة ضد أخرى لتحقيق أهداف محددة [3] وهناك العديد من التعريفات للحرب السيبرانية، ومن ثم ونظرا للحجم الصغير لهذه الدراسة فسيكتفي الباحث بالتعريفين الآتيين:

- الحرب السيبرانية هي" **"تلك الهجمات الدقيقة والمعقدة للغاية عبر نظم وشبكات الكمبيوتر والأجهزة الذكية، تستهدف البنية التحتية المدنية والعسكرية للدول، من محطات الطاقة والكهرباء، ونظم الاتصالات والمواصلات والأقمار الصناعية، وخدمات تحديد الموقع الجغرافي والسيارات ذاتية القيادة وإنترنت الأشياء، فضلا عن المفاعلات النووية والسدود والخزانات المائية، هي دقائق أو ساعات قليلة حتى تصبح الحياة المزدهرة بالتكنولوجيا الذكية الغناء، مصدر السعادة والرخاء للبشرية، مجرد كومة من الأجهزة الإلكترونية والأجساد البشرية الممزقة تعلو فوق بعضها"**[4] .
- **"الحرب السيبرانية والتي تسمى بالحرب الإلكترونية عبر الإنترنت وهي إجراء عسكري يتضمن استخدام الطاقة الكهرومغناطيسية للتحكم في المجال الذي يتميز باستخدام الإلكترونيات والطيف الكهرومغناطيسي لاستخدام بيانات التبادل عبر الأنظمة الشبكية والبنى التحتية المرتبطة به"** [5] و**"يعتمد هذا النمط من الجرائم الإلكترونية على فريق من المختصين في المعارك الذكية، ويقوم مشغلو الحروب السيبرانية بالتخطيط للنشاطات الهجومية والدفاعية وإدارتها وتنفيذها عبر الفضاء السيبراني"**[6]

([1]) إيهاب خليفة، مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي (المستقبل للأبحاث والدراسات المتقدمة(الإمارات)، القاهرة: العربي للنشر، الطبعة الأولى2019) ص11.

([2]) الأمن السيبراني، منشور على الرابط: تاريخ الزيارة 2025/2/27 الساعة 4:18.

https://oercommons.org/courseware/lesson/94012/student/?section=5 .

([3]) مينة بوطاطة، الحروب السيبرانية في العلاقات الدولية: المفهوم والظاهرة، رسالة ماجستير،(الجزائر: جامعة 20 أوت1955سكيكدة، كلية الحقوق والعلوم السياسة،1442-1443هـ2021-2022م) ص 23.

([4]) د. إيهاب خليفة، مرجع سابق، ص 10.

([5]) أنعام الكايد، مرجع سابق، ص 428.

([6]) مجدي الداغر، "اتجاهات النخبة نحو توظيف الإعلام الأمني لتطبيقات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية وانعكاساته على دعم وتعزيز الأمن السيبراني في مصر: دراسة ميدانية"، المجلة العربية لبحوث الإعلام والاتصال (العدد33 ابريل-يونيو2021) ص33.

ويعد عالم الرياضيات NORBERT WEINER الأول في استخدام مصطلح السيبرانية عام 1948 خلال دراسته للاتصال و السيطرة والقيادة [1] .

2-بدايات الحرب السيبرانية:

نظرا للاعتماد الكبير والمتزايد في حياة الإنسان اليومية على الأنظمة المعلوماتية وعلى الأجهزة المرتبطة بالشبكة العالمية للمعلومات(الإنترنت) وتشعب تلك الأجهزة من حيث طبيعتها(تليفونات محمولة وحواسيب وغيرها) وازدياد عدد مستخدميها زادت فرص اختراق تلك الأنظمة ومعرفة بياناتها وتسربها [2] ومع التوسع المستمر في استخدام التقنيات الحديثة أصبح تطور المجتمعات مرتبطا بتلك التقنيات، وبالرغم من تلك الأهمية ظهرت أفعال وتصرفات تهدف إلى إعاقة تلك التقنيات وتحد من الاستفادة منها[3] وتعود نقطة البداية لمجال بحوث الذكاء الاصطناعي إلى المؤتمر الذي أقيم في كلية "دارتموث" (البريطانية) في العام 1956 واصبح الحاضرون في ذلك المؤتمر هم قادة بحوث الذكاء الاصطناعي لعدة عقود، ومنهم "جون مكارثي"، و"مارفن ميسكاي، "الين نويل"،"هربرت سيمون"[4] .

وكانت فترة الحرب الباردة ما بين الاتحاد السوفيتي والولايات المتحدة هي بداية الحرب السيبرانية ،حيث قامت وكالة المخابرات السوفيتية(KGB) بسرقة معلومات وتكنلوجيا تابعة للدول الغربية في عملية سميت ب(LINEX) [5]ويحكي فيلم ألعاب الحرب (WAR Games) الذي انتج في عهد الرئيس الأمريكي" رونالد ريغان" أن شابا أمريكيا استطاع أن يخترق حاسوب عسكري للبحث عن لعبة إلكترونية، لكنه ومن غير قصد فّعل الترسانة النووية الأمريكية ضد الاتحاد السوفيتي، وعندما شاهد الرئيس الأمريكي" ريغان" ذلك الفيلم سأل مستشاريه عن إمكانية اختراق الأجهزة العسكرية الأمريكية فكانت الإجابة نعم وأسوأ مما يمكن تصوره [6] .

وفي عصرنا الحالي توجد الكثير من الدول ذات القوة السيبرانية الكبيرة، تأتي الولايات المتحدة وروسيا والصين على رأس هذه القوى. وتتمتع الولايات المتحدة بمكانة فريدة كقوة سيبرانية من الدرجة الأولى على مستوى العالم، وكانت الهيمنة على الفضاء السيبراني هدفاً استراتيجياً للولايات المتحدة منذ منتصف

([1]) حنان عباس سلمان، و ابتسام كاظم جاسم، "القوة السيبرانية وأثرها على القوة الاقتصادية-الصين أنموذجاً"، مجلة مركز دراسات الكوفة، (جامعة الكوفة، العدد (70) الجزء الأول، سبتمبر 2023) ص 623.

([2]) الأمن السيبراني (المملكة العربية السعودية: الهيئة العامة للمنشآت الصغيرة والمتوسطة(منشآت) 2022) ص3.

([3]) جميل زكريا محمود،" في الجريمة المعلوماتية وأساليب التأمين" في: المؤتمر الدولي لأمن المعلومات الإلكترونية معا نحو تفاعل رقمي آمن 18-20ديسمبر 2005(بلدية مسقط(عُمان)المنظمة العربية للتنمية الإدارية(القاهرة)(الشارقة) ص 131.

([4]) عبيد أسعد سعد الدين، الذكاء الصناعي (عمان: دار الابداية ناشرون وموزعون، الطبعة الأولى 2012-1433هـ) ص 20.

([5]) حنان عباس سلمان، و ابتسام كاظم جاسم، "القوة السيبرانية وأثرها على القوة الاقتصادية-الصين أنموذجاً"، مجلة مركز دراسات الكوفة، (جامعة الكوفة، العدد (70) الجزء الأول، سبتمبر 2023) ص 632.

([6]) يوسف الحسيني، معارك طاحنة لكنها بلا ضجيج، هكذا يخوض العالم حروبه السيبرانية، منشور بتاريخ 2024/9/19 على الرابط: https://bit.ly/3NfecDz ،تاريخ الزيارة 2024/9/22 الساعة 5:54

التسعينيات، وقد تم تخصيص مبلغ 11.2 مليار دولار من الميزانية المخصصة للدفاع في العام 2023 للحماية السيبرانية[1] وفي مايو 2024 قامت الولايات المتحدة بإطلاق استراتيجية الولايات المتحدة الدولية الخاصة بمجال الفضاء الإلكتروني والسياسة الرقمية، و" **تركز الاستراتيجية على مفهوم التضامن الرقمي، والذي يمثل الرغبة في العمل معا لتحقيق أهداف مشتركة والوقوف معا ومساعدة الشركاء على بناء القدرات وتقديم الدعم المتبادل**" [2] .

3-دوافع الحرب السيبرانية:

ما يميز الحرب السيبرانية أنها حرب تخاض في أجهزة الحواسيب المرتبطة بالإنترنت، بعيدا عن ميدان المعركة والأسلحة التقليدية، وهي حرب منخفضة التكلفة، كما أنها تفصح عن مستقبل الحروب في العالم [3] والدافع الرئيس لاستخدام الحرب السيبرانية هو تحقيق مكاسب عسكرية أو سياسية ضد عدو ما.

ومن ثم يمكن تشبيه الحرب السيبرانية بأنها نوع من أنواع الإرهاب، ولكنه إرهاب إلكتروني والذي يقصد به استخدام شبكة الإنترنت والشبكة المعلوماتية من أجل استهداف أمن الدول وبناها التحتية، وحتى الأشخاص، من أجل تحقيق أهداف سياسية أو اقتصادية أو عقائدية أو دينية[4]. وفي العام 2020 تم الاعتراف بالهجمات الإلكترونية كواحدة من أكبر التهديدات في العالم، فعلى سبيل المثال صنف المنتدى الاقتصادي العالمي الهجمات الإلكترونية بين أكبر عشر مخاطر على مستوى العالم من حيث الاحتمالية والتأثير [5].

وتسعى غالبية دول العالم إلى تحقيق الأمن السيبراني، وهناك مؤشر الأمن السيبراني العالمي، والذي يقيس مدى التزام البلدان بالأمن السيبراني، ويعتمد على أساس خمسة ركائز – (أ) التدابير القانونية (ب) التدابير الفنية (ج) التدابير التنظيمية (د) تنمية القدرات(هـ) التعاون، ويتم تجميعها في درجة إجمالية[6]

([1]) خالد وليد محمود، "المغالبة والتنافس في القدرات السيبرانية الأمريكية –الصينية" منشور بتاريخ 7مايو 2024 على الرابط: https://mediterraneancss.uk/2024/05/07/cyber-capabilities-united-states-of-america-china/
تاريخ الزيارة 2024/10/16 الساعة 4:23.

([2]) إطلاق استراتيجية الولايات المتحدة الدولية الخاصة بمجال الفضاء الإلكتروني والسياسة الرقمية، وزارة الخارجية الأمريكية مكتب المتحدث باسم الخارجية الأمريكية، منشور بتاريخ 6مايو2024 على الرابط: https://bit.ly/48pMGwV .

([3]) تخوض حروبا سيبرانية: من هي أقوى دول العالم؟ وكيف سيكون شكل الحرب العالمية الثالثة؟ منشور على الرابط : https://bit.ly/3YoL9Uf تاريخ الزيارة2024/10/16 الساعة 5:25.

([4]) أحمد عريبي فدعم،"دور الأمم المتحدة في مكافحة الإرهاب الإلكتروني" مجلة تنسيق(مجلد(36)عدد(5) 30كانون الاول2022م1444هـ) ص 1095.

([5])جيل بارام ،كيفين ليم، عرض :مرفت زكريا، "الحرب السيبرانية ومستقبل الصراع الإيراني الإسرائيلي" آفاق سياسية (المركز العربي للبحوث والدراسات، العدد 59، يوليو 2020) ص 107.

([6]) مؤشر الأمن السيبراني العالمي "Global Cybersecurity Index" **تاريخ الزيارة 2024/10/12 الساعة 16:42.**
https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx.

وجاءت 46 دولة من مختلف أنحاء العالم في المرتبة الأولى(من درجة 95 إلى درجة 100) لهذا المؤشر ومن ضمنها الولايات المتحدة وأستراليا والمملكة المتحدة، ومن الدول العربية جاءت البحرين والإمارات ومصر وقطر والأردن والمغرب وعمان والسعودية[1] .

ومن المهام الرئيسة للحرب السيبرانية تقديم الدعم المعلوماتي واللوجستي؛ فيتم التجسس على العدو من خلال اختراق شبكاته الإلكترونية والتعرف على تصميمات أسلحته ونوع تسليح جيشه وتواجد وانتشار قواته، والأهداف التي يسعى إلى تدميرها في حالة الحرب [2] وبالإمكان إيراد الأسباب الآتية كدوافع لاستخدام هذه الحرب [3]:

1-سهولة الاستخدام وقليلة التكلفة.

1-الحاق الضرر بالخصوم والأعداء.

2-تجنب الإدانات والمساءلات القانونية.

وبالإمكان القول إن أهم الأهداف المتوخاة من شن الحرب السيبرانية ضد دولة ما هي:

1-مقدمة لشن حرب عسكرية تالية لها وهذا ما حدث عندما قام الكيان الصهيوني بشن حربه السيبرانية على حزب الله في 17سبتمبر 2024 ثم تلاها بعد ذلك شن حرب عسكرية طاحنة ضد الحزب .

2- تدمير واسع النطاق للبنى التحتية والاقتصادية بما فيها البنى الإلكترونية للدولة المستهدفة [4].

ثانيا: أدوات الحرب السيبرانية:

هناك العديد من أدوات الحرب السيبرانية من أهمها:

1-شبكة الإنترنت:

تعد من اكثر الوسائط إثارةً للجدل، باعتبارها من أبرز تطورات تكنولوجيا الاتصال التي انتشرت بشكل كبير وواسع في جميع أنحاء العالم، وكانت بمثابة عاصفة عصفت بالمبادئ التقليدية للإعلام وقلبت موازينه ونقلته إلى عالم الرقمية[5]وهي شبكة الشبكات التي تتواصل عبرها الملايين من أجهزة

([1]) Global Cybersecurity Index 2024 5th Edition منشور على الرابط
https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf
p24 تاريخ الزيارة 2025/2/25 الساعة 13:45.

([2]) د. إيهاب خليفة، مجتمع ما بعد المعلومات، مرجع سابق، ص ص 10-11.

([3]) أنعام الكايد، مرجع سابق، ص430.

([4])عماد خليل إبراهيم، و نجوان هاني محمود، مرجع سابق، ص 25.

([5])أ.بن خليفة نوفل، اتجاهات الصحفيين الرياضيين الجزائريين نحو استخدام الصحافة الإلكترونية: دراسة ميدانية على عينة من الصحفيين الرياضيين، مجلة الدراسات الإعلامية (برلين: المركز الديمقراطي العربي، العدد العاشر، فبراير 2020) ص131.

الكمبيوتر وذلك لتبادل المعلومات بشتى أنواعها الرقمية والمرئية والمسموعة أو حفظها واسترجاعها عند الطلب [1] .

وبتوفر شبكة الإنترنت أصبح للمشتركين فيها استخدامات متنوعة وتسهيلات لا حصر لها في أمور الحياة، كالبريد الإلكتروني وما يتبعه من استقبال معلومات وإرسال ملفات؛ والمشاركة في المنتديات، واستخدام برامج المحادثة بأشكالها كافة: كتابيا، وصوتيا، وكتابيا وصوتيا، ومرئيا، والاطلاع على مواقع ترفيهية وألعاب وتسلية وسفر وسياحة وتسوق وتجارة وغيرها من المواقع المختلفة [2] .

2-الميديا الإجتماعية SOCIAL MEDDIA (مواقع التواصل الإجتماعي):

الميديا الاجتماعية عبارة عن فئة واسعة من التطبيقات الإلكترونية تقوم على عدة وظائف كالتفاعل بين مستخدميها ونشر وتوزيع المضامين بالإضافة إلى بناء شبكات من العلاقات الاجتماعية ومنها ما هو مخص لبناء العلاقات الاجتماعية "كالفيس بوك" ومنها ما هو مخصص لتبادل الصور "كالانستقرام "وآخر للفيديوهات "كاليوتيوب"[3].

وبحسب الموقع العالمي Statista • والذي أجاب على سؤال ماذا يفعل الناس على وسائل التواصل الاجتماعي، أكد الموقع على أنه في العام 2022 كان ما يقرب من نصف مستخدمي وسائل التواصل الاجتماعي يستخدمونها للبقاء على اتصال مع العائلة والأصدقاء. بالإضافة إلى ملئ أوقات الفراغ، والبحث عن الإلهام، وقراءة القصص الإخبارية، ولقد زاد مقدار الوقت الذي يقضيه الأشخاص على وسائل التواصل الاجتماعي بشكل مطرد خلال العقد الماضي. وفي عام 2023، كان الناس يقضون في المتوسط 151 دقيقة يوميا على وسائل التواصل الاجتماعي[4].

الجدير بالذكر أن عدد سكان العالم يقدر بـــ 8,111,590,531 [5] واعتبارًا من أبريل 2024، كان هناك 5.44 مليار مستخدم للإنترنت في جميع أنحاء العالم، وهو ما يمثل 67.1 بالمائة من سكان العالم. ومن

([1]) د.عبدالله صالح النجار، واقع استخدام الإنترنت في البحث العلمي لدى أعضاء هيئة التدريس بجامعة الملك فيصل، مجلة مركز البحوث التربوية (جامعة قطر، السنة العاشرة، العدد التاسع عشر،يناير 2001) ص 135.

([2]) أفنان دروزه، درجة استخدام طلبة آلية العلوم التربوية في جامعة النجاح الوطنية لشبكة الإنترنت، مجلة جامعة النجاح للأبحاث (العلوم الإنسانية) (فلسطين ،المجلد23(3)2009) ص 807.

([3]) توفيق ذباح، المعالجة الإعلامية لقضايا البيئة عبر وسائل الإعلام الجديد: دراسة وصفية تحليلية لصفحة الوكالة الوطنية للنفايات على الفايسبوك أنموذجا، مجلة الدراسات الإعلامية (برلين: المركز الديمقراطي العربي، العدد العاشر، فبراير 2020) ص 319.

• شركة ألمانية متخصصة في بيانات السوق والمستهلكين.

([4]) Social media – statistics & facts منشور على الرابط:

https://www.statista.com/topics/1164/social-networks/#topicOverview

تاريخ الزيارة 2025/2/25 الساعة 15:34.

([5]) https://www.worldometers.info/ar/ تاريخ الزيارة 2024/5/25 الساعة 4:15.

هذا المجموع، كان 5.07 مليار، أو 62.6% من سكان العالم من مستخدمي وسائل التواصل الاجتماعي [1].

وفي تقرير أصدرته مؤسسة "وي آر سوشيال"،والذي يقدم إحصاءات وتحليلات لأثر الرقمنة على حياة الناس وجاء في ذلك التقرير للربع الأول من عام 2023 المعلومات الآتية[2]:

1- عدد مشتركي الهاتف المحمول حول العالم 5.48 مليار، أي ما يعادل 68.3 بالمائة من إجمالي سكان العالم وهناك 6.9 مليار هاتف ذكي قيد الاستخدام حول العالم.

2- تشير أحدث البيانات إلى أن هناك الآن أكثر من 18مليار شخص يستخدمون الإنترنت، أي ما يعادل 64.6% من سكان العالم.

3- بلغ العدد العالمي "لهويات المستخدمين" النشطة لوسائل التواصل الاجتماعي 4.80مليار في أبريل/نيسان 2023.

أما مواقع التواصل الاجتماعي المختلفة فقد بلغ عدد المشتركين فيها في العام 2023 ما يقارب خمسة مليارات شخص حول العالم، واحتل موقع "الفيس بوك" المرتبة الأولى بعدد مشتركين بلغ2.19 مليار مشترك وجاء بعده تطبيق "انستقرام" ب1.65 مليار مشترك ثم تطبيق" تيك توك" ب1.56 مليار مشترك[3]، أما مستخدمي تطبيق "الواتس آب" فقد بلغ عدد المشتركين فيه 2 مليار مستخدم[4] .

3-الهندسة الاجتماعية:

يختلف تعريف مفهوم الهندسة الاجتماعيةً وفقا للتخصصات العلمية وطبيعة السياق المستخدم، وفي العلوم السياسية يرتبط المفهوم بقضايا التأثير على مواقف الأفراد والجماعات فمصطلح الهندسة الاجتماعية في العلوم السياسية مرتبط بقضايا التأثري على مواقف الأفراد والجماعات أو استخدام

---

(1) Number of internet and social media users worldwide as of February 2025 (in billions) منشور على الرابط:
https://www.statista.com/statistics/617136/digital-population-worldwide/
تاريخ الزيارة 2025/2/25 الساعة 15:40.

(2) الوضع الرقمي العالمي منشور بتاريخ 27 أبريل 2023 على الرابط:
https://wearesocial.com/uk/blog/2023/04/the-global-state-of-digital-in-april-2023/?u[%E2%80%A6]swearesocialcomukblog202304theglobalstateofdigitalinapril2023 تاريخ الزيارة 2024/5/25 الساعة 4:11.

(3) ارتفاع عدد مستخدمي وسائل التواصل الاجتماعي في العالم إلى أكثر من 5 مليارات شخص، فديو منشور على الرابط:
https://www.youtube.com/watch?v=-E4kE-tg46U تاريخ المشاهدة 2024/7/22 الساعة 5:10

(4) 2 مليار مستخدم يتواصلون حول العالم، وبخصوصية تامة، منشور على الرابط:
https://blog.whatsapp.com/two-billion-users-connecting-the-world-privately?lang=ar_AR تاريخ الزيارة 2024/7/22 الساعة 5:31.

مختلف الأساليب للتأثير على مواقف معينة وسلوكيات اجتماعية على نطاق واسع [1] **و"الهندسة الاجتماعية تقنية تلاعب تستغل الخطأ البشري للحصول على معلومات خاصة أو حق الوصول أو الأشياء الثمينة"**[2] **وتعني الهندسة الاجتماعية استخدام أساليب ملتوية للخداع للحصول على معلومات أو امتيازات بطرق غير مشروعة**[3] .

و"لا مفرّ من العيون التي تراقبنا حتى وإن ابتعدنا عن الجميع واعتكفنا في غرفتنا.. فحواسيبنا، وهواتفنا الذكية، ومتصفحات الإنترنت، يعلمون الكثير عنّا وعن حياتنا وأسرارنا بأدق تفاصيلها، هذا فضلاً عن أناس امتهنوا مهمّة رصد ومراقبة الآخرين وجمع معلوماتهم وبياناتهم الشخصية للاستيلاء عليها، وهو ما يعود عليهم بالكثير من الأموال"[4].

"إن هندسة العقل وبرمجة تفكيره عن طريق التحكم بالرأي العام هو من أخطر الأساليب التي تواجه العقل البشري وأعقدها إذ تسعى أساليب الهندسة تلك على اختلاف أشكالها إلى عمليات السيطرة على التفكير عند الإنسان والأليات الذهنية الخاصة به سواء كان من العامة كمثقف، عسكري، فنان، شخص عادي...الخ " [5] .

والهندسة الاجتماعية هي فن اختراق عقول البشر وخداعهم، بهدف الحصول على معلومات أو بيانات أو أموال كانت ستظل خاصة وآمنة ولا يمكن الوصول إليها. ولقد أصبحت الهندسة الاجتماعية، ذات شعبية كبيرة في السنوات الأخيرة نظرا للنمو الهائل والمتسارع لشبكات التواصل الاجتماعي والبريد الإلكتروني والأشكال الأخرى للاتصالات الإلكترونية [6].

([1]) سالم سعيد الكندي حليمة سليمان البلوشي،" الوعي بثقافة الهندسة الاجتماعية لدى طلبة كليات التعليم التقني بسلطنة عمان: دراسة حالة لطلبة الكلية التقنية بالمصنعة"، جامعة السلطان قابوس مجلة الآداب والعلوم الاجتماعية ص 74.

[2] ماهي الهندسة الاجتماعية؟ منشور على الرابط:
https://me.kaspersky.com/resource-center/definitions/what-is-social-engineering
تاريخ الزيارة 2025/2/25 الساعة 6.

([3]) عبدالله البريدي، أسرار الهندسة الاجتماعية: نحو ابتكار أدوات جديدة لزيادة ذكاءنا الجمعي(الرياض: كتاب العربية11، الطبعة الأولى 1432هـ2011م) ص 28.

([4]) الهندسة الاجتماعية.. انتبه بياناتك في خطر! "نحن مخترقون ومراقبون طالما أننا متصلون بالإنترنت" منشور بتاريخ27نوفمبر 2018 على الرابط: https://stj-sy.org/ar/1013/
تاريخ الزيارة 2024/5/27 الساعة 15:19.

([5]) حسن سعد عبد الحميد، هندسة العقل: دراسة في أساليب خداع الراي العام (العراق: مجلس الأمن الوطني، مركز النهرين للدراسات الاستراتيجية، كراس النهرين العدد(20)1441هـ2020) ص7.

([6]) الهندسة الاجتماعية، نشرة توعوية يصدرها معهد الدراسات المصرفية بدولة الكويت العدد(4) 2019 منشور على الرابط:
https://kibs.edu.kw/wp-content/uploads/2021/10/Edaat-Mar-2019.pdf
تاريخ الزيارة 2024/5/27 الساعة 15:20.

ويعتمد موضوع الهندسة الاجتماعية على استهداف الناحية النفسية للإنسان، حيث يقوم المخترقون باستخدام المحفزات الأساسية للسلوك البشري مثل زرع الخوف والفضول والإلهاء والحماسة وغيرها، فعلى سبيل المثال قد ثير صورة معينة عواطف البعض للتبرع لجهة خيرية معينة بشكل مخادع، أو من خلال إثارة الخوف الداخلي للبعض الآخر عبر إعلامهم باختراق إحدى حساباتهم، وأن عليهم إعادة تعيين كلمات المرور الخاصة بهم، أو قد يكون الفضول والاستطلاع دافعان لمشاهدة صور أو مقاطع معينة [1].

4-الذكاء الاصطناعي (AI) Artificial Intelligence:

كانت سنة 2018 بمثابة النقلة الكبرى للذكاء الاصطناعي، فقد نمت هذه التكنولوجيا بشكل كبير على أرض الواقع حتى أصبحت أداة رئيسة تدخل في صلب جميع القطاعات [2] " **ويسمح الذكاء الاصطناعي لجهاز الحاسوب أن يفكر، ويتصرف، ويستجيب كما لو أنه إنسان، ويمكن تزويد أجهزة الحاسوب بكميات هائلة من المعلومات والبيانات، ليتم تدريبها على تحديد الأنماط الموجودة فيها؛ فتصبح قادرة بعد ذلك على إنتاج تنبؤات، وحل المشكلات، وحتى التعلم من أخطائها**" [3].

ويجمع الكثير من الخبراء على أن تكنلوجيا الذكاء الاصطناعي سوف تغير من شكل الحروب المستقبلية في عديد من جوانبها، لأنها أحدثت تغييرا في مفهوم الردع التقليدي، كالصواريخ الجديدة العابرة للقارات Hypersonic ، وطائرات الدرونز القادرة على تدمير العديد من الأهداف من بعد ودون تكلفة مادية أو بشرية كبيرة [4] . والذكاء الاصطناعي له دور مزدوج في الحرب السيبرانية، فمن ناحية أولى يستخدم في تعزيز الحماية للبيانات والتصدي لأي هجمات محتملة بشأنها والكشف عن أية محاولات لتلك الهجمات، كما يستخدم في نفس الوقت في اختراق الأنظمة والتجسس عليها وشن هجوم سيبراني تجاهها[5].

ويتم استخدام الذكاء الاصطناعي في حرب المعلومات وجمعها وفي ساحات المعارك أيضا وذلك من خلال [6] :

([1]) الاختراق بالهندسة الاجتماعية ماذا تعرف عنه؟ منشور بتاريخ 2017/15 على الرابط:
https://bit.ly/3UVBVvH تاريخ الزيارة 2024/5/27 الساعة 15:23.

([2]) الذكاء الاصطناعي لخدمة الإنسانية والعالم، منشور على الرابط:
https://bit.ly/4f10UWQ تاريخ الزيارة 2024/6/14 الساعة 14:46.

([3]) الذكاء الاصطناعي: هل هو خطير، وما هي الوظائف التي يهددها؟ منشور بتاريخ14يونيو/حزيران 2023 على الرابط:
https://www.bbc.com/arabic/science-and-tech-65905663
تاريخ الزيارة 2024/6/14 الساعة 14:52.

([4]) سالم نسرين، أثر توظيف تقنيات الذكاء الاصطناعي عسكريا: دراسة في متغيري الحروب والنزاعات دراسة مجلة القانون والعلوم البينية (الجزائر: جامعة زيان عاشور-الجلفة-(العدد(1)2024) ص872.

([5]) حسام عبد الأمير خلف، و وهج علي حمزة، "مفهوم الأمن السيبراني وعلاقته بالذكاء الاصطناعي"، مجلة جامعة الأنبار للعلوم القانونية والسياسية، العدد(2) المجلد(13) كانون الأول (2023) ص 639.

([6]) سالم نسرين، مرجع سابق، ص871.

– العمليات الجوية لتدمير مراكز أنظمة القيادة والسيطرة.

– العمليات الخاصة لقطع خطوط الاتصالات.

– التشويش الإلكتروني على اتصالات الخصم.

– إدخال أهداف وهمية في رادارات الخصم بواسطة الخداع الإلكتروني.

– اخّتراق شبكات الحاسب الآلي التابعة للخصم وحقنها بمعلومات غير دقيقة.

وهناك مخاطر من الذكاء الاصطناعي فقد يصبح الذكاء الاصطناعي متقدما لدرجة أنه قد يتفوق على البشر ويتخذ قرارات تشكل تهديدا وجوديا للبشرية سواء عن قصد أو عن غير قصد، في حال ما عجز الإنسان عن التحكم فيه بالشكل المطلوب ومن ضمن هذه المخاطر [1]:

1–على سبيل المثال لو قام الذكاء الاصطناعي المصمم لتحسين تدفق حركة المرور إعادة توجيه جميع المركبات إلى مكان واحد، مما يتسبب في حدوث ازدحام وفوضى هائلة.

2–يمكن استخدام الذكاء الاصطناعي لتشغيل أسلحة فتاكة ذاتية التشغيل مثل الطائرات بدون طيار، وقد يتم اختراقها واستخدامها استخداما ضارا بأصحابها أنفسهم، ووقع أوضح مثال على خطورة الأسلحة ذاتية التشغيل في تجربة لسلاح الجو الأميركي بتاريخ 2 يونيو/حزيران 2023، حيث قررت طائرة مسيرة (درون) تعمل بالذكاء الاصطناعي، خلال اختبار محاكاة قتل مشغلها (الافتراضي) الذي كان يُفترض أن يقول "نعم" للموافقة على الهجوم على الأهداف المحددة (الوهمية) لأنها رأت أن مشغلها يمنعها من تحقيق هدفها ويتدخل في جهودها لإكمال مهمتها.

3–يمكن استخدام الذكاء الاصطناعي للمراقبة الجماعية (أنظمة التعرف على الوجوه على سبيل المثال) وتمكين الحكومات أو الكيانات الأخرى من مراقبة مواطنيها والسيطرة عليهم على نطاق غير مسبوق. وقد يؤدي ذلك إلى فقدان الخصوصية، فضلا عن إساءة استخدام السلطة من قبل أولئك الذين يتحكمون في تقنيات المراقبة هذه وربما استخدامها لانتهاك حقوق الإنسان وغيرها من أشكال القمع.

4–يتمتع الذكاء الاصطناعي بالقدرة على أتمتة العديد من الوظائف، مما قد يؤدي إلى اضطراب أسواق العمل وإلغاء العديد من الوظائف بشكل كبير.

وتحتل الولايات المتحدة الأمريكية مرتبة الصدارة فيما يتعلق بالذكاء الاصطناعي• وتهيمن حاليا هي والصين على البحث والتطوير في مجال الذكاء الاصطناعي [2].

([1]) رماح الدلقموني، "مستقبل الذكاء الاصطناعي ما هي أسوأ مخاطره المحتملة؟ وكيف نتصدى لها؟" منشور بتاريخ2023/6/11 على الرابط: https://bit.ly/4c1l14e تاريخ الزيارة 2024/6/14 الساعة 15.

• للمزيد من المعلومات التفصيلية عن ترتيب الدول في مؤشر الذكاء الاصطناعي للعام 2024 AI Index Report الذي صدر عن جامعة ستانفورد الأمريكية أنظر موقع الجامعة: https://aiindex.stanford.edu/report/

([2]) خالد وليد محمود، عن مؤشر الذكاء الاصطناعي 2023،منشور بتاريخ2023/7/23 على الرابط: https://bit.ly/3xmHN9E تاريخ الزيارة2024/6/17 الساعة 7:52.

5-التزييف العميق Deepfakes :

تقنية التزييف العميق عبارة عن إنشاء محتوى فيديو وصوت يتم من خلاله انتحال شخصيات أخرى وتقديم معلومات مزيفة عن سلوكهم و أنشطتهم و البيئة المحيطة بهم[1].ومن خلال التزييف العميق يتم توليد صور أو مقاطع فيديو أو صوت أو نصوص مزيفة باستخدام أدوات التعلم الآلي المتقدمة، مما يؤدي إلى انتشار المعلومات المضللة على نطاقات ضخمة عبر الإنترنت، وهذا يمكن أن يقوض سلامة المعلومات ويقوض الثقة في مصادر الأخبار وقد يؤدي -في سيناريو مرعب- إلى قيام صناع القرار في مجال الأمن القومي في يوم من الأيام إلى اتخاذ إجراءات فعلية بناء على معلومات خاطئة، مما قد يؤدي إلى أزمة كبيرة، أو أسوأ من ذلك الحرب[2] .

ومن أبرز صور استخدام هذه التقنية التي تقوم على أساس الخداع والتضليل [3] :

1-فبركة مشاهد مزيفة لقوات أو أسلحة عسكرية امتلكتها الدولة لتحقيق حالة من الردع لدى الأعداء .

خلق مشاهد كاذبة لأحداث عنف أو اعتداء، كمشاهد اعتداء الشرطة على المواطنين، وهو ما قد يستفز مشاعر الجماهير وجعلها تخرج في تظاهرات حقيقية ضد أجهزة الدولة.

-فبركة تصريحات مسيئة لسياسيي قد تؤدي إلى اندلاع أعمال عنف أو تظاهرات أو حتى توتر في العلاقات مع دول أخرى.

وفي مايو 2023انتشرت صور تُظهر انفجاراً بالقرب من مبنى وزارة الدفاع الأمريكية "البنتاجون "مما تسبب في حدوث ارتباك وانخفاض مُؤقت في سوق الأسهم الأمريكية، وقد أوضح" البنتاجون" أن الصور زائفة وتم تزييفها بواسطة الذكاء الاصطناعي بدقة وحرفية عالية [4] .

ثالثاً: نماذج للحرب السيبرانية

تعرضت العديد من الدول إلى عدة هجمات سيبرانية، وتتنوع ما بين تدمير أنظمة إلكترونية لمنشآت عسكرية أو مدنية حيوية، وتعطيل وإتلاف الشبكات العسكرية، وتعطيل أو اختراق أو تدمير شبكات القطاع العام وتعطيل البنى التحتية للدول [5] ونظرًا للطبيعة السرية للعمليات الحربية السيبرانية فهناك

([1]) دليل التزييف العميق يوليو 2021(دولة الإمارات: البرنامج الوطني للذكاء الاصطناعي) ص 7.

([2]) مستقبل الذكاء الاصطناعي ما هي أسوأ مخاطره المحتملة؟ وكيف نتصدى لها؟ منشور بتاريخ2023/6/11 على الرابط: https://bit.ly/4c1I14e تاريخ الزيارة 2024/7/23 الساعة 21:40.

([3]) نسرين سالم، مرجع سابق،ص873..

([4]) مؤيد الزعبي، عندما يلتقي التزييف العميق والذكاء الاصطناعي كذِّب ما تراه عينك، منشور بتاريخ 23مايو 2023 على الرابط: https://bit.ly/3LytTVk تاريخ الزيارة 2024/6/14 الساعة 11:49.

([5]) حامد محمد علي البلداوي، مواجهة الحرب السيبرانية في قواعد القانون الدولي الإنساني، مجلة الجامعة العراقية (العدد57ج2، 2022م،1444هـ) ص 372.

العديد من تلك العمليات التي لم يكشف النقاب عنها[1] وهناك أمثلة عديدة لهجمات سيبرانية قامت بها دول عديدة كروسيا والصين وايران وإسرائيل وكوريا الشمالية، وفيما يلي عدد من الأمثلة لتلك الهجمات:

- الهجوم السيبراني الروسي على إستونيا وأوكرانيا:

تعد الحرب السيبرانية من أدوات القوة الناعمة الروسية المستخدمة إلى جانب الآليات الاقتصادية والسياسية من أجل تحقيق أهداف السياسة الخارجية الروسية [2] ففي العام 2007 شنت روسيا هجوما سيبرانيا كبيرا على إستونيا• مما عرضها لمخاطر غير مسبوقة، ويعود السبب في ذلك الهجوم إلى قيام إستونيا بنقل تمثال عبارة عن نصب تذكاري من الحرب السوفياتية، وقد أدى ذلك الهجوم الى تعطل الكثير من مواقع الأجهزة الحكومية واستمر ذلك الهجوم لمدة ثلاثة أسابيع [3].

وكانت هذه الحرب السيبرانية الروسية بمثابة جرس إنذار لحلف الناتو حيث وافق في العام 2008 على أن تكون هناك سياسة للناتو تقوم على الاهتمام بالدفاع السيبراني [4] كما قامت روسيا في يونيو من العام 2017 بشن هجوم سيبراني على أوكرانيا على خلفية أزمة القرم بين البلدين وشُن الهجوم على مؤسسات ووزارات وبنوك وصحف وشركات كهرباء واستخدم المهاجمون الروس برمجيات خبيثة من نوع "بيتا" وأدى الهجوم إلى تعطيل أنظمة المعلومات وتوقف أجهزة الحاسوب، مع مطالبة بدفع فدية بالعملة الإلكترونية (بيتكوين) التي لا يمكن تعقبها [5] .

وبعد الغزو الروسي لأوكرانيا في العام 2022، شنت روسيا العديد من الهجمات السيبرانية مستهدفة من ذلك البنى التحتية لأوكرانيا مثل الطاقة والاتصالات والنقل، ولا تهدف هذه الهجمات إلى شل القدرة التشغيلية للبلاد فحسب، بل وأيضاً إلى بث الفوضى بين السكان كما حدث في العام 2015 حيث شنت روسيا الهجوم الإلكتروني على شبكة الطاقة الأوكرانية مما أدى إلى انقطاع الكهرباء عن مئات الآلاف من الناس [6] .

([1]) إيهاب عنان،" معارك طاحنة لكنها بلا ضجيج، هكذا يخوض العالم حروبه السيبرانية" منشور بتاريخ32يوليو 2024 على رابط المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات:
https://bit.ly/3B6tLdF تاريخ الزيارة 2024/9/22 الساعة 6:52.

([2]) بلبل ابتسام، مرجع سابق، ص 43.

• إحدى جمهوريات دول البلطيق.

([3]) الياس حرفوش، القرصنة الروسية ليست جديدة... الحرب الإلكترونية الأولى في استوينا، منشور بتاريخ 22مارس 2107 على الرابط: https://bit.ly/4dNGsYJ تاريخ الزيارة 2024/10/219 الساعة 7:05.

([4]) أحمد محيي محمد أحمد علي، مرجع سابق، ص 1223.

([5]) صالح حيدر عبد الواحد، حروب الفضاء الإلكتروني؛ دراسة في مفهومها وخصائصها وسبل مواجهتها، رسالة ماجستير، (عمان: جامعة الشرق الأوسط، كلية الآداب والعلوم، قسم العلوم السياسية تموز/يوليو2021) ص29.

([6]) أمن سيبراني التجسس السيبراني الروسي، الاستراتيجيات والأهداف، منشور بتاريخ23سبتمبر 2024 على رابط المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات: https://bit.ly/4dO95oE تاريخ الزيارة 2024/10/17 الساعة 5:25..

- الهجوم السيبراني الروسي للتأثير على الانتخابات الأمريكية:

في يناير من العام 2017، أصدر مكتب مدير الاستخبارات الوطنية الأمريكي تقريرا اتهم فيه روسيا بإطلاق حملة سيبرانية استهدفت التأثير على الانتخابات الرئاسية الأمريكية، وتعتقد وكالات الاستخبارات الأميركية أن الرئيس الروسي" فلاديمير بوتين" قد أصدر أوامره بالسعي إلى التأثير على الانتخابات الرئاسية الأمريكية لعام2016 [1] وقد أيدت لجنة الاستخبارات في مجلس الشيوخ الأمريكي وبالإجماع، استنتاج مجتمع الاستخبارات الأمريكي بأن موسكو "تدخلت في انتخابات عام 2016 من أجل دعم المرشح الجمهوري "دونالد ترامب"، كما أن هناك اتهامات استخباراتية أمريكية مماثلة بالتدخل الروسي في انتخابات 2024 من أجل دعم المشرح نفسه، وأن موسكو تستخدم الذكاء الاصطناعي لإنشاء محتوى مزيف مقنع من أجل مساعدة "دونالد ترامب "وهو ما ينفيه المرشح الجمهوري" دونالد ترامب" [2] .

- الهجمات السيبرانية الإيرانية:

استخدمت إيران تكتيكات الهندسة الاجتماعية في العديد من الهجمات السيبرانية البارزة، بما في ذلك هجوم 2012 على شركة أرامكو السعودية، وكان من تداعيات هذا الهجوم أن هرعت الدول الخليجية نحو إسرائيل لتشكل فيما بينها جبهة لتبادل الخبرات السيبرانية لمواجهة إيران [3].

- هجمات الكيان الصهيوني ضد إيران:

شن الكيان الصهيوني بواسطة فيروس الكمبيوتر ستكسنت"Stuxnet " هجوما سيبرانيا لمهاجمة وتدمير برنامج إيران النووي في العام 2010، بالتعاون مع الولايات المتحدة [4] و إنتاج الفيروس المدمر مشروع أمريكي إسرائيلي بمساعدة بريطانيا وألمانيا، وزعم وزير الاستراتيجية للكيان الصهيوني "موشي يعالون" في ذلك الوقت أن البرنامج النووي الإيراني واجه "صعوبات" أخرت –عدة سنوات– احتمال حيازة إيران السلاح النووي[5] .

([1]) الياس حرفوش، مرجع إلكتروني سابق.

([2]) ترامب "يرفض" تحذيرات جديدة بشأن التدخل الروسي في الانتخابات الأميركية" منشور بتاريخ 8سبتمبر 2024 على الرابط: https://bit.ly/4f9FOpl تاريخ الزيارة 2024/10/19 الساعة 7:14.

([3]) أحمد محيي محمد أحمد علي، مرجع سابق، ص 1236.

([4]) أحمد علو،" الحروب السيبرانية والعنف الرقمي واقع عالمي جديد" منشور على موقع الجيش اللبناني: https://bit.ly/4gwEePU تاريخ الزيارة 2024/9/22 الساعة 7.

([5]) فيروس ستاكسنت: الولايات المتحدة وإسرائيل "تعاونتا" لاستهداف برنامج إيران النووي، منشور بتاريخ 16يناير 2011 على الرابط: https://www.bbc.com/arabic/worldnews/2011/01/110116_us_iran_israel_stuxnet_nuke تاريخ الزيارة 2024/10/10 الساعة 5:17.

وفي تصنيف لدراسة أجريت عام 2024 عن أعلى الدول التي تصدر منها جرائم سيبرانية كانت على النحو الآتي [1]:

1-روسيا 2-أوكرانيا 3-الصين4-الولايات المتحدة 5-نيجيريا6-رومانيا 7-كوريا الشمالية8-المملكة المتحدة9-البرازيل10-الهند.

رابعا: حرب الكيان الصهيوني السيبرانية تجاه حزب الله2024

قبل الحديث عن حرب الكيان الصهيوني السيبرانية تجاه حزب الله يجب أن نشير في البداية إلى بعض النقاط المهمة وذلك على النحو الآتي:

1-رؤية حزب الله تجاه الكيان الصهيوني:

كانت العلاقة ما بين حزب الله والدولة اللبنانية في اطار ما يعرف بالدولة الضعيفة التي يسيطر عليها المجتمع القوي، ويعد العام 1989 وهو العام الذي وقع فيه ما يعرف باتفاق الطائف بين الفصائل اللبنانية المتقاتلة، العام الذي بدأ يشهد وضوحا لنفوذ حزب الله في الدولة اللبنانية، خاصة وأن الحزب قد قبل باتفاق الطائف[2] وأصبح الحزب فاعلا سياسيا بعد مشاركته في الانتخابات البرلمانية والبلدية في أعوام 1992، 1994 ، 1996، وقد تمكن الحزب من امتلاك قوة مسلحة خاصة به مؤكدا على خيار أنه حزب إسلامي مقاوم يعمل في خدمة الدولة اللبنانية، وأنه يسعى إلى إخراج قوات الكيان الصهيوني من داخل لبنان [3] و "**في عام 1985 أعلن حزب الله عن تشكيله الرسمي في بيان تلي آنذاك، عرف باسم "الرسالة المفتوحة للمستضعفين"، وكانت الرسالة بمثابة الوثيقة الرسمية التي تعبر عن نهج حزب الله ومشروعه السياسي بوصفه حركة جهادية هدفها الأساس دحر الاحتلال الإسرائيلي**" [4] وجاء في الوثيقة التأسيسية لحزب الله 2009 :

" **تمثّل "إسرائيل" تهديداً دائماً للبنان – الدولة والكيان – وخطراً داهماً عليه، لجهة أطماعها التاريخية في أرضه ومياهه، وبما هو أنموذج لتعايش أتباع الرسالات السماوية، في صيغة فريدة، ووطن نقيض**

---

(1) Cyber news, Threat Actor, Threat Intelligence December 27, 2024 منشور على الرابط: https://cyble.com/blog/top-countries-facing-cybercrime-threats/

تاريخ الزيارة 2025/2/27 الساعة 6:10

(2) مروة حامد البدري العلاقة بين إيران وسورية وحزب الله وآثارها في الدولة اللبنانية، مجلة سياسات عربية (الدوحة: المركز العربي للدراسات العدد5،تشرين الثاني 2019) ص40.

(3) فهم صعود حزب الله اللبناني صراع المنطقة الأمنية في جنوب لبنان (1985 - 2000م)،مجلة مسارات(السعودية، العدد23،جمادى الأولى 1437هفبراير2016) ص 10.

(4) محمد محمود مرتضى، برنامج حزب الله الانتخابي.. الرسالة المفتوحة الثالثة، منشور على الموقع الرسمي لحركة المقاومة الإسلامية بلبنان على الرابط:

https://moqawama.news/essaydetails.php?eid=34839&cid=330 تاريخ الزيارة 2024/9/29 الساعة 15:53.

لفكرة الدولة العنصرية التي تتمظهر في الكيان الصهيوني. فضلاً عن ذلك، فإنّ وجود لبنان على حدود فلسطين المحتلة، وفي منطقة مضطربة جراء الصراع مع العدو الإسرائيلي، حتّم عليه تحمّل مسؤوليات وطنيةً وقوميةً" [1] . وكان حزب الله يرى أن الحرب مع الكيان الصهيوني لم تنته بعد فهناك أراض لبنانية محتلة من قبل إسرائيل في مزارع "شبعا" وتلال" كفرشوبا" ولابد من استعادتها[2].

2-خبرة الكيان الصهيوني في الحرب السيبرانية:

في 12 مايو من العام 2011 أعلن رئيس حكومة الكيان الصهيوني آنذاك " بنيامين نتنياهو" عن إنشاء "هيئة السايبر الوطنية" في الكيان وأن الهدف الأساس لهذه الهيئة هو تعزيز قدرات إسرائيل الدفاعية عن البنى التحتية الحيوية من الهجمات القادمة من الفضاء الإلكتروني [3].

ويمتلك الكيان الصهيوني العديد من القدرات السيبرانية متفوق بذلك على العديد من دول العالم وقد طالبت وثيقة استراتيجية الجيش الإسرائيلي والتي نشرت في العام 2015 بتوفير قدرات دفاعية متوازنة في جميع الظروف وجميع المجالات القتالية بما فيها السايبر، وتم تأسيس ما يعرف ب"سلطة الدفاع السيبراني الوطني القومي" في العام 2016 وتتبع مكتب رئيس الوزراء مباشرة [4] .

وقد تعرض الكيان الصهيوني للعديد من الهجمات السيبرانية، مما جعله يدرك أن الحروب القادمة لها هي حرب الفضاء الإلكتروني ، ولذلك أصبحت القوة السيبرانية من الأدوات الرئيسة المستخدمة من قبل جيش الكيان الصهيوني لتحقيق أهدافه الاستراتيجية [5] فعلى سبيل المثال في أواخر شهر إبريل من العام 2020 وقعت الكثير من الهجمات السيبرانية على العديد من مرافق الصرف الصحي والمياه في جميع أنحاء البلاد واتهم الكيان الصهيوني إيران بالوقوف وراء تلك الهجمات [6] وقد كشف قائد وحدة الأمن السيبراني في الجيش الإسرائيلي، العقيد "راحيلي دمبينسكي" أن عدد الهجمات التي تعرض لها الكيان

([1]) الوثيقة السياسية لحزب الله 2009، منشوره على رابط المقاومة الإسلامية-لبنان-:
https://moqawama.news/essaydetailsf.php?eid=16245&fid=47
تاريخ الزيارة 2024/9/29 الساعة 16:20.

([2]) أمل سعد غريب، حزب الله: الدين والسياسة، (بيروت: مركز الحضارة لتنمية الفكر الإسلامي، الطبعة الثانية 2009) ص 14.

([3]) محمود محارب، مراجعة كتاب إسرائيل والحرب الإلكترونية قراءة في كتاب: حرب في الفضاء الإلكتروني: اتجاهات وتأثيرات على إسرائيل (المركز العربي للأبحاث ودراسة السياسات (معهد الدوحة) أغسطس 2011) ص6.

([4]) أحمد بن علي الميموني، الجبهة النِشطة :تداعيات المواجهة السيبرانية بين إيران وإسرائيل، مجلة الدراسات الإيرانية (المعهد الدولي للدراسات الإيرانية(رصانة)السنة الرابعة العدد الثاني عشر، أكتوبر 2020) ص 73.

([5]) مريم محمد سيد حسن على علام، "القوة السيبرانية في السياسة الخارجية الإسرائيلية تجاه إيران 2010- 2020 "منشور بتاريخ15نوفمبر 2023 على الرابط:
https://democraticac.de/?p=93046 تاريخ الزيارة2024/10/10 الساعة 4:29.

([6])جيل بارام ، كيفين ليم، مرجع سابق،ص107.

سواء كان الجيش أو الدوائر الحكومية أو الشركات الكبرى والمؤسسات الاقتصادية والأمنية والصحية والتعليمية في إسرائيل، قد بلغت 3 مليارات هجوم منذ بداية الحرب على غزة في اكتوبر 2023[1] .

ويعد الكيان الصهيوني متقدما في مجال الحروب السيبرانية وله تجارب عديدة في هذا الشأن. وتعد الوحدة 8200 متخصصة في شن تلك الهجمات السيبرانية، وهذه الوحدة والتي اسمها "اشموني ماتايم" وتوازي وكالة الأمن القومي الأمريكية أو مكاتب الاتصالات الحكومية البريطانية، وهي أكبر وحدة عسكرية مفردة في جيش الكيان الصهيوني [2] وقد شنت العديد من الهجمات السيبرانية على عدد من الأهداف العسكرية والمفاعلات النووية الإيرانية.

ويلاحظ على الهجوم السيبراني للكيان الصهيوني على إيران أنه يهدف إلى [3]:

- ✓ التجسس وجمع معلومات استخبارية عن إيران بشكل عام وبرنامجها النووي بشكل خاص.
- ✓ الهجوم وإحداث أضرار بالمشروع النووي الإيراني.
- ✓ الردع وبحيث تمنع إسرائيل إيران من شن هجوم سيبراني عليها.

3-الهجوم السيبراني للكيان الصهيوني على حزب الله:

في 17سبتمبر 2024 شن الكيان الصهيوني هجوما سيبرانيا هو الأول من نوعه على مستوى العالم، سواء من حيث الأدوات المستخدمة أو من حيث الآثار المترتبة على ذلك الهجوم.

وكان لبنان قد شهد انفجار آلاف أجهزة النداء الآلي "البيجر" والاتصالات اللاسلكية "ووكي توكي" التي كانت لدى عناصر "حزب الله" على مدار يومين ما أدى إلى مقتل 37شخصا وإصابة 3000 آخرين[4]. وقد أشارت بعض التكهنات المبكرة إلى أن أجهزة البيجر قد تكون تعرضت لهجوم قرصنة معقد تسبب في انفجارها، ولكن الخبراء استبعدوا هذه النظرية بسرعة، ولإحداث هذا الحجم من الأضرار، من المحتمل أن تكون الأجهزة قد تم تجهيزها بالمتفجرات قبل أن تصل إلى حيازة حزب الله[5] .

([1]) إسرائيل تعرضت لـ3 مليارات هجوم سيبراني منذ حرب 7 أكتوبر، منشور على الرابط:
https://bit.ly/400UnHs تاريخ الزيارة2024/9/22

([2]) ماهي "الوحدة 8200" الإسرائيلية المختصة بالحرب الإلكترونية المشتبه بوقوفها وراء تفجيرات لبنان؟ منشور بتاريخ 2024/9/18 على الرابط: https://bit.ly/3MTyH8p تاريخ الزيارة 2024/9/22 الساعة 7:46

([3]) مهند مصطفى، "تصعيد الحرب السيبرانية بين إسرائيل وإيران" منشور بتاريخ26يوليو 2022 على الرابط:
https://www.epc.ae/ar/details/featured/taseid-alharb-alsaybiraniat-bayn-iisrayiyl-wa-iiran
تاريخ الزيارة 2024/10/11 الساعة 5:49.

([4]) جلسة عاصفة في مجلس الأمن بشأن تفجيرات أجهزة اتصالات حزب الله "،منشور بتاريخ 21 سبتمبر 2024 على الرابط:
https://arabic.cnn.com/middle-east/article/2024/09/21/lebanon-and-israel-clash-in-un-security-council-over-device-explosions تاريخ الزيارة 2024/9/22 الساعة 8:27..

([5]) توم بينيت، "تفجيرات أجهزة حزب الله: الأسئلة التي لم يتم الإجابة عليها، منشور بتاريخ20سبتمبر 2024 على الرابط:
https://www.bbc.com/arabic/articles/c4g5wd8g9z5o تاريخ الزيارة 2024/9/22 الساعة 8:07.

أما المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات فإنه يعيد السبب في تلك التفجيرات إلى قيام أجهزة الاستخبارات الإسرائيلية بإخفاء متفجرات في (5000) جهاز اتصال قبل أشهر من تفجير أجهزة حزب الله، كما تم الكشف عن رسالة نصية مشفرة تسببت في الانفجارات، وكان الموساد قد قام بحقن لوحة داخل أجهزة اتصالات تحتوي على مادة متفجرة تتلقى شفرات من الصعب جدا اكتشافها حتى باستخدام أي جهاز أو ماسح ضوئي [1].

وكانت تلك التفجيرات قد وصفها الأمين العام لحزب الله، حسن نصر الله بأنها ضربة كبيرة و قاسية أمنياً وإنسانيا وغير مسبوقة في تاريخ المقاومة في لبنان وغير مسبوقة في تاريخ الصراع العربي الإسرائيلي وعلى مستوى العالم [2].

الجدير بالذكر أن مشاركة عناصر حزب الله في القتال في سوريا، منذ عام 2011، كانت سببا آخر سّهل من عملية رصد تحركات حزب الله؛ فالمشاركين في ذلك القتال أصبحوا مكشوفين، بسبب استخدامهم أنظمة اتصال تقليدية قابلة للرصد مثل أجهزة الهواتف المحمولة واللاسلكي[3]. وأيا كانت الوسائل التي استخدمت في تنفيذ تلك الهجمات السيبرانية فلا يمكن القول بعدم وجود اختراق أمنى داخلي لحزب الله ساعد على تنفيذ تلك الهجمات وبتلك الدقة وبذلك النجاح الكبير.

ومنذ إعلان حزب الله في 8 أكتوبر 2024 دعمه ومساندته لما يعرف بمعركة طوفان الأقصى حدثت العديد من المواجهات العسكرية بين إسرائيل وحزب الله مما أدى إلى نزوح ما يقارب 60 الف مواطن لبناني وما يقارب من 110 الف مستوطن إسرائيلي، وخلال هذه الفترة التزم الطرفان بقواعد اشتباك محددة[4].

وفي يوم الجمعة 27سبتمبر 2024 شن الكيان الصهيوني غارات عنيفة جدا على الضاحية الجنوبية ببيروت مستهدفة القيادة المركزية لحزب الله مستخدمة ثمانين قنبلة خارقة للتحصينات مما أدى إلى اغتيال أمين عام الحزب حسن نصر الله وعدد آخر من ممن كانوا معه حينذاك [5].

([1]) ملف أمن دولي . تحول قواعد الاشتباك ما بين حزب الله وإسرائيل إلى الحرب الهجينة، منشور بتاريخ22سبتمبر 2024 على الرابط: https://bit.ly/408HZFt تاريخ الزيارة 2024/10/17 الساعة 5:45.

([2]) الكلمة الكاملة للأمين العام لحزب الله حسن نصر الله بعد تفجيرات البيجر، منشور على الرابط:
https://www.youtube.com/watch?v=jtd9oOHBkWw
تاريخ المشاهدة(فديو)2024/9/29 الساعة 14:54.

([3]) جواسيس أم اختراق تكنولوجي: كيف قتلت إسرائيل نصر الله؟ منشور بتاريخ 29سبتمبر 2024 على الرابط: https://bit.ly/3ZMjg9J تاريخ الزيارة 2024/9/29 الساعة 6:58.

([4]) "العدوان الإسرائيلي على لبنان بعد استهداف مقر القيادة المركزية لحزب الله واغتيال أمينه العام" سلسلة تقدير موقف (الدوحة: المركز العربي للأبحاث ودراسة السياسات، وحدة الدراسات السياسية، تقدير موقف 29أيلول/سبتمبر 2024) ص 4.

([5])المرجع السابق، ص 4.

وكان لذلك الهجوم السيبراني والذي تبعه هجوم عسكري أدى إلى اغتيال الأمين العام لحزب الله حسن نصر الله وقعا كبيرا على المواقف الدولية المختلفة فعلي سبيل المثال [1]:

رأى الرئيس الأميركي "جو بايدن" أنّ اغتيال نصرالله "إجراء يحقق العدالة لضحاياه الكثيرين، من بينهم الآلاف من المدنيين الأميركيين والإسرائيليين واللبنانيين"، أما روسيا فقد أدانت بشدة اغتيال حسن نصر الله ،وأن إسرائيل تتحمل المسؤولية الكاملة" عن العواقب "المأسوية" التي يمكن أن يؤدي إليها في المنطقة، ورأى النائب الأول للرئيس الإيراني" محمد رضا عارف" أنّ اغتيال حسن نصرالله سيؤدي إلى زوال إسرائيل، فيما وجه الرئيس التركي اتهامه لإسرائيل بأنها ترتكب إبادة جامعية ووصف هجومها على حزب الله واغتيال أمينه العام بالوحشي.

وواصل الكيان الصهيوني هجومه العسكري على لبنان وعلى مقدرات حزب الله بالتحديد واغتال العشرات من قياداته الكبيرة وأحدثت دمارا كبيرا لبناه التحتية، ومن ثم يمكننا القول أن الحرب السيبرانية التي شنها الكيان الصهيوني على حزب الله كان لها تداعياتها الكبيرة على العلاقات الدولية، ويبدو من استقراء الواقع الحالي أن ذلك الهجوم سيغير الكثير من الواقع الدولي ومن المواقف الدولية، ولن نكون مبالغين لو قلنا أن ما قبل تلك الهجمات السيبرانية على حزب الله ليس كما بعده.

الخاتمة:

من خلال العرض السابق في هذه الدراسة اتضح أن الحرب السيبرانية أصبحت واقعا لا يمكن الفرار منه، وأن هذه الحرب هي انعكاس واضح للتطور العلمي الهائل في المجالات المختلفة وخاصة في مجال تكنلوجيا المعلومات والاتصالات، وأن الحروب المستقبلية الحديثة ستكون الحرب السيبرانية هي الحرب الأكثر بروزا فيها، وهذا لا يعني التقليل من أهمية الحروب العسكرية التقليدية، حيث لا يمكن الاستغناء عنها بالمطلق، ولكن ستكون رديفة للحرب السيبرانية والعكس صحيح كذلك.

وقد نفت الدراسة الفرضية التي انطلقت منها الدراسة والتي نصت على ألا تأثير مهم للحرب السيبرانية على العلاقات الدولية،وأن العكس من ذلك هو الصحيح؛ فالحرب السيبرانية ذات تأثير مهم في العلاقات الدولية خاصة في مجالها العسكري، وقد استخدمت تلك الحرب في العديد من الأمثلة على مستوى العالم، وجاء هجوم الكيان الصهيوني السيبراني على حزب الله ليكون نموذجا واضحا لذلك التأثير، حيث أن ذلك الهجوم السيبراني كان بمثابة المقدمة لشن هجوم عسكري كبير على حزب الله، والذي أدى الى خسائر بشرية ومادية فادحة للحزب.

([1]) ردود فعل عربية ودولية على اغتيال نصر الله، منشور بتاريخ 2024/9/29 على الرابط:
https://bit.ly/3N4ZM8F تاريخ الزيارة 2024/9/29 الساعة 7:08.

نتائج الدراسة:

1-تدرك معظم دول العالم أهمية تطوير استراتيجيات حديثة للحروب تمكنها من إخضاع الخصوم بتكاليف مادية وبشرية قليلة ومن ثم ستكون الحروب العالمية القادمة حروبا سيبرانية [1] كما باتت العديد من الدول تلجأ بشكل متصاعد لشن هجمات سيبرانية تلحق الأذى بالخصوم وترغمهم على الخضوع والإذعان لمطالب الدولة المهاجمة [2].

2-أصبحت الحرب السيبرانية جزءا مهما في سياسات الدول وعلاقاتها الدولية وأداة مهمة من أدوات سياستها الخارجية.

3-تعد الحرب السيبرانية بمثابة اعتداء على أمن وسيادة الدول وانتهاكا لميثاق الأمم المتحدة [3]

ومن حق أي دولة تتعرض إلى هجوم سيبراني اعتبار ذلك الهجوم بمثابة حرب معلنة عليها ومن حقها استخدام القوة في الدفاع عن نفسها ضد ذلك الهجوم.

4-كان من نتائج الحرب السيبرانية الإسرائيلية على حزب الله أن تبوأت إسرائيل مكانة دولية مهمة في مجال استخدام الحروب السيبرانية.

5-بالرغم من أهمية الرحب السيبرانية إلا أنه لا يمكن الاستغناء عن الحرب العسكرية التقليدية وكان الهجوم السيبراني الإسرائيلي على حزب الله وما تلاه من هجوم عسكري تقليدي دليل واضح على ذلك.

التوصيات

اولاً:(لصناع القرار):

1-بذل الجهود الدولية لاعتبار الحرب السيبرانية واحدة من صور الاعتداء المسلح التي تستوجب العقوبات الدولية كونها خرقا واضحا لميثاق الأمم المتحدة.

2-الاستفادة من التقنيات التكنلوجية الحديثة كوسائل دفاعية ضد أي هجوم سيبراني.

3-أنشاء تكتل سيبراني عربي لتبادل المعلومات والخبرات وتبني استراتيجيات موحدة للدفاع السيبراني.

4-تطبيق ما يعرف بالتحكم بالمعلومات بالنسبة للأفراد عند محاولاتهم الوصول إلى المعلومات وذلك عن طريق [4]:

- ✓ شيء فريد خاص بالمستخدم نفسه.
- ✓ شي يملكه المستخدم (البطاقة الشخصية)
- ✓ شيء يعرفه المستخدم (كلمة المرور).

([1])علاء الدين فرحات، مرجع سابق، ص 692.

([2]) صالح حيدر عبد الواحد، مرجع سابق، ص 73.

([3]) محمد حسن سعيد دراجي، و عمر صالح العكور، مرجع سابق، ص9.

([4]) الأمن السيبراني، مرجع سابق، ص5.

كما يجب اتخاذ الاحتياطات الواجبة للحماية ومنها [1]:

- ✓ التوعية والتعريف بأساليب وطرق الاختراق والحرب السيبرانية.
- ✓ وضع نسخ احتياطية بشكل دائم وحفظها في أماكن سرية وآمنة.
- ✓ التحديث المستمر لبرامج التشغيل وأنظمتها.
- ✓ فحص الأجهزة والبرامج قبل استخدامها.

4-إن شيوع وانتشار المبدأ القانوني الذي يقول لا عقوبة إلا بنص يعد بمثابة عائق أمام اتخاذ العقوبات المناسبة ضد الجرائم التي تعتمد على الوسائل التكنلوجية الحديثة في الاتصالات مما يؤدي إلى الإفلات من العقوبة لمن يقوم بارتكابها [2]ومن ثم لابد من إصدار التشريعات المحلية والدولية الخاصة بجرائم الحروب السيبرانية.

5-تاهيل وتدريب الكوادر الفنية والقانونية لمواجهة الحرب السيبرانية خاصة وأن هذه الحرب من الصعب إثبات حدوثها وتحتاج إلى أدلة رقمية من اجل ذلك، وتحتاج كذلك إلى خبراء مؤهلين وأجهزة تكنلوجية متطورة [3].

6-العمل على نشر ثقافة وطنية تستهدف التوعية بأهمية الأمن السيبراني[4] .

7- وضع تصورات لكيفية استخدام وسائل اتصالات حديثة تكون غير قابلة للاختراق والاستفادة من تجربة حزب الله فيما يتعلق بتفجير البيجرات وأجهزة اللاسلكي.

ثانيا: توصيات للباحثين:

1-التصدي بالدراسة البحثية لموضوع الذكاء الاصطناعي ودوره في صنع القرار السياسي.

2-دور الذكاء الاصطناعي في التنشأة السياسية.

3-كيفية مجابهة مخاطر الذكاء الاصطناعي.

References:

•Amal Saad Gharib, Hezbollah: Religion and Politics, (Beirut: Center of Civilization for the Development of Islamic Thought), second edition 2009.(

•Cybersecurity (Kingdom of Saudi Arabia: General Authority for Small and Medium Enterprises (Monsha'at) 2022).

•Ihab Khalifa, Post-Information Society: The Impact of the Fourth Industrial Revolution on National Security (Al-Mustaqbal for Advanced Research and Studies (UAE), Cairo: Al-Arabi Publishing, first edition 2019).

([1]) الأمن السيبراني، المرجع السابق، ص7.

([2]) منار محسن عبدالغني، و معمر خالد عبدالحميد "المواجهة القانونية لجرائم الإنترنت بين مبدأ المشروعية وقصور التشريع ودور القضاء في معالجته، مجلة الجامعة العراقية العدد 39/ 2 ، 31 ديسمبر 2017) ص 426.

([3]) حسون عبود هجيج، و صفاء كاظم غازي، "آثار جريمة القرصنة الإلكترونية"، مجلة القادسية للقانون والعلوم السياسية (جامعة القادسية(العراق) العدد الثاني، المجلد السابع كانون الاول2016) ص 204.

([4]) فواز عبد الرحمن علي دودة، مرجع سابق، ص 34.

•Taha Hamid Hassan Al-Anbaky, Narjis Hussein Zayer Al-Aqabi, Principles of Scientific Research in Political Science (Baghdad: Dar Oma, Rabat: Dar Al-Aman, Algeria: Ikhtilaf Publications, Beirut: Dafaf Publications, first edition 1436 AH 2015 AD).

•Abdullah Al-Baridi, Secrets of Social Engineering: Towards Inventing New Tools to Increase Our Collective Intelligence (Riyadh: Kitab Al-Arabiya 11, first edition 1432 AH 2011 AD).

•Obaid Asaad Saad Al-Din, Artificial Intelligence (Amman: Dar Al-Ibdaya Publishers and Distributors, first edition 2012-1433 AH).

•Balbal Ibtisam, The Value of Cybersecurity in Russian Foreign Policy Orientations Towards the African Region, Master's Thesis (Algeria: University of Mohamed Bouguerra-Boumerdes-Faculty of Law and Political Science, Department of Political Science, 2019-2020).

•Saleh Haider Abdel Wahid, Cyber Wars; A Study of Their Concept, Characteristics and Ways to Confront Them, Master's Thesis, (Amman: Middle East University, Faculty of Arts and Sciences, Department of Political Science, July 2021).

•Mina Boutata, Cyber Wars in International Relations: Concept and Phenomenon, Master's Thesis, (Algeria: University of August 20, 1955 Skikda, Faculty of Law and Political Science, 1442-1443 AH 2021-2022 AD)

" •The Israeli Aggression on Lebanon after Targeting the Central Command Headquarters of Hezbollah and Assassinating its Secretary-General" Situation Assessment Series (Doha: Arab Center for Research and Policy Studies, Political Studies Unit, Situation Assessment September 29, 2024).

•A. Ben Khalifa Noufel, Algerian Sports Journalists' Attitudes towards the Use of Electronic Journalism: A Field Study on a Sample of Sports Journalists, Journal of Media Studies (Berlin: Arab Democratic Center, Issue Ten, February 2020).

•Ahmed bin Ali Al-Maimouni, The Active Front: Implications of the Cyber Confrontation between Iran and Israel, Journal of Iranian Studies (International Institute for Iranian Studies (Rasanah), Fourth Year, Twelfth Issue, October 2020). • Ahmed Arabi Faddam, "The Role of the United Nations in Combating Cyber Terrorism" Coordination Magazine (Volume (36) Issue (5) on 30 December 2022 AD 1444 AH.

•Ahmed Mohie Mohammed Ahmed Ali, "The Impact of the Israeli-Iranian Cyber War on Arab Regional Security" Journal of the Higher Institute for Qualitative Studies (Volume 3 Issue 8 July (2023.(

•Political Horizons (Arab Center for Research and Studies, Issue 59, July 2020).

•Afnan Darwazeh, The Degree of Use of the Internet by Students of Educational Sciences Mechanism at An-Najah National University, An-Najah University Journal for Research (Humanities) (Palestine, Volume 23 (3) 2009).

•Enaam Abdul-Ridha Sultan Al-Akabi, "Employing Cyber Wars in Developing the Concept of Power for Major Powers" Political Issues Magazine, (University of Nahrain: College of Political Science, Issue 73, April-May-June 2023).

• Tawfiq Dhabah, Media Treatment of Environmental Issues Through the Media New: A descriptive and analytical study of the National Waste Agency's Facebook page as a model, Journal of Media Studies (Berlin: Arab Democratic Center, Issue 10, February 2020). • Gil Baram, Kevin Lim, Presentation: Mervat Zakaria, "Cyberwar and the Future of the Iranian-Israeli Conflict"

•Hamed Mohammed Ali Al-Baldawi, Confronting Cyber Warfare in the Rules of International Humanitarian Law, Journal of the Iraqi University (Issue 57, Vol. 2, 2022 AD, 1444 AH).

•Hussam Abdul Amir Khalaf, and Wahj Ali Hamza, "The Concept of Cyber Security and Its Relationship to Artificial Intelligence", Journal of Anbar University for Legal and Political Sciences, Issue (2) Volume (13) December.(2023)

•Hassan Saad Abdul Hamid, Engineering the Mind: A Study of Methods of Deceiving Public Opinion (Iraq: National Security Council, Al-Nahrain Center for Strategic Studies, Karas Al-Nahrain Issue (20) 1441 AH 2020).

•Hassoun Aboud Hajij, and Safaa Kazim Ghazi, "The Effects of the Crime of Electronic Piracy", Al-Qadisiyah Journal of Law and Political Science (University of Al-Qadisiyah (Iraq) Issue Two, Volume Seven December 2016).

•Hanan Abbas Salman, and Ibtisam Kazem Jassim, “Cyber Power and Its Impact on Economic Power - China as a Model,” Journal of the Kufa Studies Center, (University of Kufa, Issue (70), Part One, September 2023). • Salem Nasreen, The Impact of Employing Artificial Intelligence Technologies in the Military: A Study of the Variables of Wars and Conflicts, A Study of the Journal of Law and Interdisciplinary Sciences (Algeria: University of Ziane Achour-Djelfa-(Issue (1) 2024.(

•Salem Saeed Al-Kindi Halima Suleiman Al-Balushi, "Awareness of the Culture of Social Engineering among Students of Technical Education Colleges in the Sultanate of Oman: A Case Study of Students of the Technical College in Al-Musannah", Sultan Qaboos University Journal of Arts and Social Sciences

•Abdullah Saleh Al-Najjar, The Reality of Using the Internet in Scientific Research among Faculty Members at King Faisal University, Journal of the Center for Educational Research (Qatar University, Tenth Year, Nineteenth Issue, January 2001).

•Alaa El-Din Farhat, Cyber Warfare and the Future of Global Security, Al-Naqid Journal of Political Studies, (Volume 6) Issue 2.(2022)

•Imad Khalil Ibrahim, and Najwan Hani Mahmoud, "The Use of Cyber Power in the Policies of Major Powers" The Iraqi Journal of Political Science (Fifth Year, Issue (10) March 2024).

•Understanding the Rise of the Party God, the Lebanese, the conflict of the security zone in southern Lebanon (1985-2000 AD), Masarat Magazine (Saudi Arabia, Issue 23, Jumada al-Ula 1437 AH, February 2016).

•Fawaz Abdulrahman Ali Doda: “Cybersecurity in the Republic of Yemen,” Manarat al-Amn Magazine (Sana’a: Police Academy, Volume (1), Issue 11, January-June 2024).

•Majdi al-Dagher, “Elite trends towards employing security media for artificial intelligence applications in combating cybercrimes and its implications for supporting and enhancing cybersecurity in Egypt: A field study,” Arab Journal of Media and Communication Research (Issue 33, April-June 2021). • Muhammad Hassan Saeed Daraji, and Omar Saleh Al-Akkour, “Cyberattacks according to the provisions of international humanitarian law,” Studies: Sharia and Legal Studies (Volume 51, Issue 1, 2024).

•Marwa Hamed Al-Badri, The Struggle between Iran, Syria and Hezbollah and its Effects on the Lebanese State, Arab Policies Magazine (Doha: Arab Center for Studies, Issue 5, November 2019).

•Manar Mohsen Abdul-Ghani, and Muammar Khaled Abdul-Hamid, “Legal Confrontation of Internet Crimes between the Principle of Legitimacy and the Shortcomings of Legislation and the Role of the Judiciary in Addressing It,” Journal of the Iraqi University, Issue 39/2, December 31, 2017.(

•Nabhan Zambour Al-Saadi, “Geopolitics of Cyber Risks of Cyberspace on the National Security of the Arab Mashreq Countries,” Journal of the Babylon Center for Human Studies (Volume 14, Issue 2, 2024).