التحول في مفهوم القوة والصراع : دراسة في الحروب السيبرانية▽

The shift in the concept of power and conflict: A study in cyber wars

ا. م. د. شيماء معروف فرحان •
Shiemma Marouf.Frhan

الملخص

يحاول البحث تشخيص اهم مؤشرات التحول والتغيير التي طالت مفاهيم القوة والصراع ومفهوم الامن والحروب في العلاقات الدولية، وذلك عبر الوقوف على اهم الاسباب المؤدية لذلك التحول في تلك المفاهيم. ومنها الثورة التكنولوجية والمعلوماتية الهائلة، وتعدد الفاعلين من غير الدول وبالتالي تعدد انماط الهجمات السيبرانية التي شهدتها العديد من الدول الامر الذي لفت الانظار الى ضرورة اعتماد استراتيجيات جديدة لإدارة الانماط الجديدة من الحروب والصراعات.

الكلمات المفتاحية : القوة السيبرانية ، الصراع السيبراني ، الحروب السيبرانية ، الفضاء السيبراني

Abstract:

The research was attempts to diagnose the most important indicators of transformation and change which affected the concepts of power ,conflict and wars in international relations and international system in general. By identifying the most important reasons leading to that transformation in those concepts including the massive technological and information revolution. The multiplicity of non-state actors and, consequently, the multiplicity of patterns of cyber-attacks witnessed by many countries, which drew attention to the necessity of adopting new strategies to manage new patterns of wars and conflicts.

- Keywords : Cyber power , cyber conflict, cyber wars, cyber space.

المقدمة

تعد الحرب والقوة والصراع من المفاهيم التقليدية القديمة التي لازمت ظهور البشرية والتي تعتمد على توظيف العنف او الاكراه في تحقيق الاهداف والمصالح المبتغاة ومع التطور الذي شهدته النظام الدولي ووحداته الدولية ارتبطت تلك المفردات بمصالح الدول واهدافها لتتضمن اشكال وابعاد ومستويات مختلفة اختلفت باختلاف المعطيات والمتغيرات التي شهدها النظام الدولي في اواخر القرن العشرين واوائل القرن الحادي والعشرين سيما ظهور الثورة المعلوماتية التي ساهمت في خلق بيئة جديدة لنشوب

▽ تاريخ التقديم : 2023/10/8 تاريخ القبول: 2023/11/6 تاريخ النشر: 2023/12/31
• استاذ مساعد في كلية العلوم السياسية / الجامعة المستنصرية . shiemmafrhan@Gmail.com

صراعات حول ما يعرف بالنفوذ السيبراني في الفضاء الالكتروني بوصفه الساحة الجديدة للتفاعلات العالمية مما ساهم في بلورة مفاهيم جديدة منها القوة السيبرانية والحروب السيبرانية والتهديدات السيبرانية والامن السيبراني. ووفقا لذلك فلاوجود لدولة قوية واخرى ضعيفة الاوفق هذا المنظور .

اهمية البحث: تتجسد اهمية البحث في محاولة رصد وفهم التطورات التي حدثت في مفاهيم القوة والصراع والحروب وتحول تلك المفاهيم من النمط التقليدي القائم على القوة الصلبة الى انماط جديدة قائمة على توظيف الثورة الرقمية وتكنولوجيا المعلومات بالشكل الذي انعكس على توازنات القوة التقليدية بين الفواعل الدوليين وعلى مجمل التفاعلات داخل النظام الدولي .

هدف البحث: يهدف البحث التركيز على الدور الذي يلعبه العامل التكنولوجي وثورة المعلومات الرقمية في تبدل معطيات التفاعلات الدولية في النظام الدولي من التفاعلات القائمة على النماط التقليدية الى انماط جديدة بات العامل التكنولوجي فيها هو المتغير الحاسم سيما انه يشكل احد اهم مقومات القوة في النظام الدولي وتأثير ذلك على شكل النظام الدولي وموازين القوة فيه .

مشكلة البحث: تتركز مشكله البحث في تساؤل مفاده: كيف اثرت الثورة التكنولوجية والمعلوماتية على مظاهر القوة والحروب والصراعات الدولية في اطار النظام الدولي ؟ . ومن هذا التساؤل تتفرع عدة اسئلة

1. ما هو مدى تأثير الثورة التكنولوجية في تحول بيئة الصراعات والحروب والتفاعلات الدولية الاخرى من بيئة النظام الدولي التقليدية الى بيئة افتراضية جديدة .
2. ماهي التحولات التي طرأت على مفاهيم القوة والصراع والحروب في اطار البيئة الافتراضية الجديدة من حيث الابعاد والخصائص .
3. هل اثرت تلك التحولات الناجمة عن الثورة التكنولوجية والمعلوماتية على الاطراف الداخلة في اطار تلك الحروب والصراعات؟ ام لاتزال الدول هي اللاعب الوحيد فيها ؟.
4. ماهي اهم الهجمات السيبرانية التي حدثت في اطار التفاعلات الافتراضية الجديدة ؟.

فرضية البحث: يفترض البحث وجود توجه واهتمام ملحوظ من قبل الفواعل (الدول وغير الدول) نحو تطوير وتعزيز مقومات القوة السيبرانية لما تتمتع به من سمات وخصائص تجعل منها العنصر الحاسم في الصراعات والحروب القادمة .

منهجية البحث: اعتمد البحث على عدة مناهج منها المنهج التحليلي الذي اختص بتحليل اسباب التحول في مفاهيم القوة والصراع وبالتالي اسباب التحول في شكل القوة وانماط التفاعلات الجديدة ، والمنهج المقارن الذي تم اعتماده للمقارنة والتوصل الى اوجه الاختلاف بين مظاهر القوة والصراع والحروب

التقليدية والانماط الجديدة منها ، وايضا اعتمد البحث على المنهج الوصفي في دراسة نماذج من الهجمات السيبرانية التي شهدها النظام الدولي في الآونة الاخيرة .

هيكلية البحث : يتقسم البحث الى النقاط الاتية :

اولا: الفضاء السيبراني واثره في تحول مفهوم القوة في العلاقات الدولية . ثانيا : تحول الصراع من النمط التقليدي الى الصراع السيبراني. ثالثا: التهديدات السيبرانية والامن السيبراني. رابعا : الحروب السيبرانية.

اولا: الفضاء السيبراني واثره في تحول مفهوم القوة في العلاقات الدولية .

تعد التكنولوجيا اليوم من اكثر المفاهيم المؤثرة في التفاعلات الدولية في اطار النظام الدولي فهي المتغير الاكثر تأثيرا في بنية النظام السياسي وفي تفاعلاته المختلفة سيما ما يتعلق منها بمفاهيم القوة والصراع والامن التي طالها التغيير تبعا لتأثير التكنولوجيا في مجمل اتجاهات ومسارات العلاقات الدولية [1].

ويعرف الفضاء السيبراني(cyber space) بانه المجال الافتراضي الذي يعتمد على نظم الكمبيوتر وشبكات الانترنت وما توفره من معلومات وبيانات واجهزة . وهناك من يرى ان الفضاء السيبراني هو البعد الخامس للحرب وهذا التعريف يحدد الفضاء السيبراني بالمجال العسكري فقط دون التطرق للمجالات الاخرى[2] وبذلك فقد وفر الفضاء السيبراني بيئة افتراضية جديدة تحولت في ظله العلاقات الدولية من بيئة النظام الدولي التقليدية الى بيئة اخرى دخلت فيها التكنولوجيا الرقمية في كل مجالات تلك العلاقات العسكرية والاقتصادية والامنية.

1. دور الفضاء السيبراني في تحول مفهوم القوة .من الأمور المستقرة في العلاقات ت الدولية أن مصادر قوة الدولة وأشكالها تتغير، فإلى جانب القوة الصلبة ممثلة في القدرات العسكرية والاقتصادية، تزايد الاهتمام بالأبعاد غير المادية للقوة، ومن ثم بروز القوة الناعمة التي تعتمد على جاذبية النموذج والإقناع، ومع ثورة المعلومات ظهر شكل جديد من أشكال القوة وهي القوة الالكترونية التي تركت تأثيرا مهما على المستويين المحلي والدولي فهي من جهة ادت الى انتشار توزيع القوة بين اكبر عدد من الفاعلين مما اضعف قدرة الدولة على السيطرة على تلك الانماط الجديدة من القوة وبالتالي منحت الفاعلين من غير الدول القدرة على ممارسة كل من القوة الصلبة والقوة الناعمة في آن معا وذلك عبر الفضاء

[1] . اسماعيل زروقة ، الفضاء السيبراني والتحول في مفاهيم القوة والصراع ، مجلة العلوم القانونية والسياسية ، المجلد 10 ، العدد 1 ، ابريل ، 2019 ص 19

[2] نوره شلوش ، القرصنة الالكترونية في الفضاء السيبراني : التهديد المتصاعد لأمن الدول ، مجلة مركز بابل للدراسات الانسانية ، المجلد 8 ، العدد 2، 2018، ص189. 190 .

الإلكتروني [1] وتعرف القوة السيبرانية بانها " قدرة الدولة القومية على السيطرة والتأثير داخل وعبر الفضاء السيبراني لدعم عناصر ومقومات القوة الاخرى[2] " ويعتمد تحقيق القوة السيبرانية لأي دولة على قدرة الدولة على تطوير موارد العمل في الفضاء السيبراني والتي تختلف عن المقومات التقليدية للقوة ، عموما حدد جوزيف ناي ثلاثة انواع من الفاعلين الذين يمتلكون القوة السيبرانية وهم[3]

ا. **الدول** : تعد الدولة فاعل محوري في تسيير الفضاء السيبراني انطلاقًا من إمكاناتها المادية والبنيوية والبشرية والقانونية". فقد تستخدم الدول الحرب السيبرانيّة لكي لا تلجأ إلى الحرب العسكريّة المباشرة، وبذلك تستخدمها ضمن صراعاتها وعمليّاتها. وأضحت الدول تتنافس في إطارها. فالدول التي تمتلك بنى تحتيّة سيبرانيّة قويّة قادرة أن تشن هجومات يتُسبب بخسائر للخصم[4].

ب . **المنظمات والشركات:متعددة الجنسيات** [5]: وتشمل الشركات متعدّدة الجنسيّات القادرة على اختراق أنظمة معلومات للأفراد والجماعات. كما هو الحالّ في مواقع التواصل الاجتماعي كفيسبوك وتويتر في ظل البيانات التي تجمعها، فهي قادرة أن تخترق العديد من الحسابات وتستخدمها لصالح أهداف مرتبطة بها أو بيعها لجهات معيّنة. وبذلك تستطيع ضرب اقتصاديات دول معيّنة وتتلاعب في بياناتها.

ت . الفاعلون من غير الدول : وتتضمن الجماعات الإرهابيّة التي تقوم بالحرب السيبرانيّة من أجل اختراق المواقع التابعة للدولة ونشر ما يتلاءم مع أجندتها، وذلك للترويج لأفكارها وأيديولوجيتها ونشر الأخبار التي تبث الخوف .

ث . الأفراد : يمتلك الأفراد القدرة على تهديد أمن الدول من خلال السيبرانيّة وذلك في ظل الإمكانات التي تؤهلهم للقيام بذلك مثل "المال، الإعلام، الأفكار– المعلومات وتوظيفها ضمن أهداف خاصة،

---

[1] . محمود علي عبد الرحمن ، الفضاء الالكتروني واثره على مفاهيم القوة والامن والصراع في العلاقات الدولية ، مجلة كلية السياسة والاقتصاد ، جامعه بني سويف ، المجلد 16 ، العدد 15 ، يوليو ، 2022، ص 425.

[2] . حازم محمد خايل ، استغلال الفضاء السيبراني في الحروب غير التقليدية : دراسة في الوكالة السيبرانية والارهاب السيبراني ، المجلة العلمية لكلية الدراسات الاقتصادية والعلوم السياسية بجامعه الاسكندرية ، المجلد الثامن ، العدد 15، يناير 2023، ص289.290

[3] جوزيف س. ناي، الحرب والسلام في الفضاء الإلكتروني، بحث منشور على شبكة المعلومات الدولية، 2005/2/24، الموقع :http//www.project-syndicate.org/commentary/presedent-push-gose-soft/Arabic تاريخ المشاهدة 2023/11/11 ، س800

[4] . عادل عبد الصادق ، اثر الارهاب الالكتروني على مبدا استخدام القوة في العلاقات الدولية 2001 . 2007 ، رسالة ماجستير ، كلية السياسة والاقتصاد ، القاهرة ، 2009 ، ص 69.

[5] . . محمد منذر جلال وسرى غضبان ، تكنولوجيا الحروب السيبرانية واستراتيجية المواجهة الدولية ، مصدر سبق ذكره ، ص170 .

بهدف التأثير في سلوك الوحدات الفاعلة على المستوى الدولي، بما يخدم مصالحهم , وغالبا ما يطلق على هؤلاء الافراد بالقراصنة وهم اشخاص لهم القدرة على التعامل مع انظمة الحواسيب والشبكات ولهم القدرة على اختراق اي نظام حماية لتلك الشبكات [1].

ثانيا : تحول الصراع من النمط التقليدي الى الصراع السيبراني.

مع بروز الفضاء الالكتروني كساحة ومجال جديدة للصراع بين الفاعلين المختلفين تعرضت ظاهرة الصراع الدولي للتغيير عبر التحول من الصراع التقليدي الى الصراع الالكتروني او السيبراني والذي يعبر عن حالة من التناقض والاختلاف في الاهداف والقيم بين الفاعلين سواء كانوا من الدول او غير الدول ومع انتشار الفضاء الإلكتروني وسهولة الدخول إليه، اتسعت دائرة الصراعات الالكترونية وأزداد عدد المهاجمين عبر الفضاء الالكتروني ويتميز الصراع الالكتروني عن الصراع التقليدي بسمات عدة منها .[2]

1. ساحة صراع افتراضية ، فالصراع الافتراضي ليس له ساحة جغرافية محددة بل يتميز بساحات مفتوحة تتصارع به الاطراف المتناقضة عبر الفضاء الالكتروني .

2. ادوات الصراع ادوات الكترونية توظف بها البيانات والمعلومات واجهزة الحواسيب.

3. بسبب طبيعة اسلحة الفضاء الالكتروني فان قيمة الردع لم تعد تعمل كما هو الحال في الصراعات التقليدية سواء كانت بالأسلحة التقليدية ام الاسلحة النووية بمعنى ان قيمة الردع كاستراتيجية للعمل العسكري تراجعت ولم يبقى لها تأثير واضح [3]

4. ان الصراع الالكتروني عزز من فرص الحروب اللامتماثلة ووفقا لذلك اصبحت دول اقل قوة قادرة على شن هجمات على دول اكبر واكثر قوة . [4] ومع اتساع الفضاء الالكتروني وسهولة الدخول اليه اتسعت دائرة الصراعات الالكترونية وازداد عدد المهاجمين وتحول الصراع بين الفاعلين المختلفين ينصب حول امتلاك ادوات الحماية والدفاع وتطوير القدرات الهجومية الالكترونية بهدف حيازة القوة والتفوق والهيمنة وتعزيز التنافس حول السيطرة والابتكار والتحكم بالمعلومات وبالتالي زيادة معطيات القدرة والتأثير والنفوذ

---

[1] . لبنى خميس مهدي ، تغريد صفاء مهدي ، اثر السيبرانية في تطور القوة ، مجلة حمورابي للدراسات ، مركز حمورابي للبحوث والدراسات الاستراتيجية ، العدد 33. 34 ، 2020، ص 156.

[2] . سيف نصرت الهرمزي ، وصف المقاربات لمنظورات الفاعل الرقمي والانكشاف الاستراتيجي في ظل الفضاء السيبراني ، مجلة ادأب الفراهيدي ، العدد 37، اذار ، 2019، ص237.

[3] . صلاح حيدر عبد الواحد ، حروب الفضاء الالكتروني ، دراسة في مفهومها وخصائصها وسبل مواجهتها ، رسالة ماجستير ، كلية الآداب والعلوم ، جامعة الشرق الاوسط ، تموز 2021، ص 8

[4] . دلالي جيلاني ، بنيشير يعقوب ، رهانات الامن السيبراني الوطني في ظل التحول الرقمي : قراءة في التأصيل المعرفي واستراتيجية المواجهة الشرعية ، كلية الحقوق والعلوم السياسية ، جامعة حسيبة بن بوعلي ، الجزائر ص535. 536.

على المستويين المحلي والعالمي .[1] وبما ان اطراف الصراع التقليدي يلجاون في ساحات الصراع التقليدية الى توظيف شتى انواع الاسلحة التدميرية انتقلت جبهات القتال بشكل مواز الى ساحات القتال الالكترونية وكان هذا التحول سببا في لفت الانتباه الى اعادة التفكير في حركية وديناميةالصراعات وظهر مايعرف بعصر القوة النسبية وهو ما انعكس بشكل واضح على طبيعة استراتيجيات ادارة الصراع وبالتالي على توازنات القوة في النظام الدولي .[2]

ثالثا: التهديدات السيبرانية والامن السيبراني

الأمن السيبراني (cybersecurity) وفقا للاتحاد الدولي للاتصالات هو" مجموعة الأدوات والسياسات والمفاهيم والضمانات الأمنية والمبادئ التوجيهية ونهج إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات وسبل الضمان والتكنولوجيا التي يمكن استخدامها في حماية البيئة السيبرانية والمنظمة واصول المستعملين .[3] وهو ايضا " مجموعة الاجراءات والأطر القانونية والتنظيمية التي تضعها الاجهزة الامنية للمحافظة على سرية المعلومات الالكترونية وهو تلك الجهود المشتركة بين القطاع العام والخاص والجهود المحلية والدولية الرامية الى الحفاظ على حماية الفضاء السيبراني والعمل على توفير انظمة معلومات رقمية بخصوصية عالية مقاومة للاختراقات الفيروسية[4] ويعرفه ريتشارد كمرر بانه " عبارة عن وسائل دفاعية من شانها كشف واحباط المحاولات التي يقوم بها القراصنة [5] عموما ، تقسم الهجمات والاختراقات الاليكترونية الى اربعة اصناف مهمة هي [6]:

1. اختراق اجهزة الحاسوب نفسها عن طريق فايروسات صغيرة جدا في الحجم.
2. تجنيد مجموعة من المهندسين و الخبراء ممن يعملون على هذه الحواسيب من قبل اجهزة مخابرات دولية معادية .

---

[1] . رولا حطيط ، السيبرانية ، الحرب الخفية في المنطقة المظلمة ، مركز باحث للدراسات الفلسطينية والاستراتيجية ، متاح على الرابط 9https://www.bahethcenter.net/uploaded/files/%D8%A7%D9%84%D8%B3%D%29

[2] المصدر نفسه ، ص 435

[3] اوس مجيد غالب العوادي ، الامن المعلوماتي السيبراني ، مركز البيان للدراسات والتخطيط ، بغداد ، تاريخ المشاهدة 11/ 2023/11 ، س7:30 ، متاح على الرابط ، www.bayancenter.org

[4] . محمد منذر جلال وسرى غضبان ، تكنولوجيا الحروب السيبرانية واستراتيجية المواجهة الدولية ، مصدر سبق ذكره ، ص**177**

[5] . اسماعيل زروقة ، الفضاء السيبراني والتحول في مفاهيم القوة والصراع ، ص 1021

[6] عادل عبد الصادق ، انماط الحرب السيبرانية وتداعياتها على الامن العالمي ، مجلة السياسة الدولية ، مؤسسة الاهرام متاح على الرابط :

https://www.siyassa.org.eg/News/12072.aspx

تاريخ المشاهدة 2023/10/9 س10:9 م

3-اختراق الحزم الاليكترونية المختلفة سواء السلكية واللاسلكية من التي تقوم بتوصيل اشارة الانترنيت الى اجهزة الكمبيوتر العاملة

4. زرع رقائق اليكترونية غاية في التطور و الصغر داخل مباني و اماكن عمل الحواسيب العملاقة وتقوم هذه الرقائق بسرقة معظم او اهم المعلومات المحفوظة و نقلها الى الدول المعادية.

وتتركز اغلب الهجمات و القرصنة الاليكترونية و السيبرانية حول المجالات الاتية :

1. المعلومات العسكرية الخطيرة مثل عدد الطائرات و المدرعات و الصواريخ بعيدة المدى و أمكنة حفظ واستخدام اسلحة الدمار الشامل

2. المعلومات الخاصة بحجم الاموال و نوعها و اصحابها من تلك المودعة في المصارف والبنوك الكبرى ؛ وكيفية تحريك تلك الاموال و في اي اتجاهات تصرف.

5. المعلومات الخاصة بأهم ضباط الامن و المخابرات و اماكن عملهم و من هم العملاء والوكلاء في الداخل والخارج الذين يتعاملون معهم.

6. المعلومات الخاصة باستفتاء الرأي العام و كذلك معدل اصوات الناخبين و توجهاتهم الانتخابية و السياسية سيما ما يتعلق بإجراءات الانتخابات العامة والخاصة في الدول الكبرى مثل امريكا و بريطانيا و فرنسا و روسيا و الصين و الهند و غيرها

7. المعلومات و التقارير الخاصة بنشاط و تحرك أجهزة المخابرات القوية (الاقليمية و الدولية) ممن تلك المتهمة بدعم التنظيمات و التشكيلات الارهابية المختلفة كالقاعدة و داعش و حماس و بعض التنظيمات الراديكالية المتطرفة.[1]

وللأمن السيبراني ابعادا عدة يمكن توضيحها بالاتي :

1. البعد العسكري : يتجسد هذا البعد في شقين الاول توظيف الامن السيبراني في الحفاظ على قدرة الوحدات العسكرية على التواصل عبر الشبكات العسكرية بالشكل الذي يؤمن تبادل المعلومات والأوامر وتدفقها بالشكل الذي يساعد في تحقيق الاهداف المرجوة . الا انها تشكل في الوقت ذاته نقطة ضعف خاصة ان لم تكن مؤمنة من الاختراق مما قد تؤدي الى تدمير البيانات العسكرية او قطع الاتصال بين القيادة والوحدات العسكرية فضلا عن امكانية التحكم في بعض الاسلحة او خروجها عن السيطرة .[2]ومن

[1] . حسن مظفر ، الفضاء المعلوماتي ، بيروت : مركز دراسات الوحدة العربية ،2007 ، ص216 . 217.

[2] . اسماعيل زروقة ، الفضاء السيبراني والتحول في مفاهيم القوة والصراع ، مصدر سبق ذكره ص 1022

اهم الامثلة على تلك التهديدات ، التهديدات السيبرانية التي حدثت عبر اختراق انظمة المنشأة النووية الايرانية بفايروس (ستاكنت) .[1]

2. البعد الاقتصادي : يرتبط الامن السيبراني ارتباطا وثيقا بالاقتصاد فالتلازم واضح بين اقتصاد المعرفة وتوسع استخدام تقنيات المعلومات والاتصالات [2]وتبعا لذلك اصبح الانترنت يوظف في هذا المجال كمقوم قوة عبر دعم المعاملات التجارية والمالية واستخدمت الحواسيب ايضا في تسيير وتطوير الصناعات وتحريك الاقتصاد اما في الجانب الآخر فان تلك الشبكات يمكن ان تكون سببا في اختراق الامن الاقتصادي والاضرار بأمن الدولة عبر ضرب اقتصادها وهنا يمكن الاشارة الى الاضرار المادية الجسيمة التي خلفتها الهجمات السيبرانية على استونيا عام 2007 .اذ وظف الانترنت في قطع التيار الكهربائي عن احد البنوك الرئيسة في استونيا مما تسبب في خسائر اقتصادية هائلة .[3]

3. البعد السياسي: اثر توظيف الفضاء الالكتروني في العلاقات الدولية الى خلق نوع جديد من العلاقات بين الدول تتسم بعدم الاستقرار مما اثر في الجغرافية السياسية للدول سيما عبر التجسس والتنصت وتسريب المعلومات التي اعلنت عنها وكالة الامن القومي الامريكي التي تقوم بها على الخصوم والاصدقاء ومنها التنصت على مكالمات الرئيس البرازيلي ديلما روسيف والمستشارة الالمانية انجيلا ميركل [4]

4. البعد الاجتماعي: ان التزايد الكبير في اعداد مستخدمي الانترنت حول العالم وازدياد مستخدمي مواقع التواصل الاجتماعي ساهم بشكل كبير في تسهيل عملية التفاعل البشري وتبادل الافكار والخبرات والثقافات الا انه في الوقت ذاته عرض اخلاقيات المجتمع للتهديدات والمخاطر نظرا لصعوبة مراقبة محتوى الانترنت والتعرض للاختراق الخارجي عبر المحتويات غير المشروعة او غير المرغوبة كما هو الحال بمحتوى المواقع الاباحية والترويج للإتجار بالممنوعات والدعارة والارهاب والتجنيد للقضايا التي تمس الامن والسلم الدولي .[5]

---

[1] منى الاشقر جبور ، السيبرانية هاجس العصر ، المركز العربي للبحوث القانونية والقضائية ، جامعة الدول العربية ، ص ، 28 متاح على الرابط ،
تاريخ المشاهدة 2023/10/9 https://t.me/montlq

[2] . المصدر نفسه ، ص30

[3] محمد منذر جلال وسرى غضبان ، تكنولوجيا الحروب السيبرانية ، مصدر سبق ذكره ، ص170

[4] المصدر السابق ، ص170

[5] منى الاشقر جبور ، السيبرانية هاجس العصر ، مصدر سبق ذكره ، ص30 . 34.

5. البعد القانوني : ينطوي البعد القانوني للأمن السيبراني على ضرورة مواكبة التشريعات القانونية للتهديدات السيبرانية الجديدة عبر وضع اطر وتشريعات للأعمال القانونية وغير القانونية في الفضاء السيبراني والتعاون الدولي في هذا المجال ، ومن هذا المنطلق تتمثل المخاطر القانونية في غياب الامن القانوني او حتى في تنازع وتناقض الانظمة القانونية .[1]

رابعا : الحروب السيبرانية .

الحرب السيبرانية هي حرب قائمة بالفعل بين الكثير من الدول وادوات هذه الحرب هي اجهزة الحاسوب وشبكات الانترنت ، فقد تغيرت وسائل وادوات الحرب بفعل التطور الكبير في مجال التكنولوجيا خاصة في مجال تكنولوجيا المعلومات والاتصالات التي ادت الى حدوث تغيرات نوعية في مجال ميادين القتال وانماط الحروب الحديثة[2] .

1. مفهوم الحروب السيبرانية

تتجسد ملامح الحروب السيبرانية في محاولة كل دولة من الدول الى اختراق شبكات الدول الاخرى واستغلال ما يوجد بها من ضعف وثغرات للنيل من الخصم دون الحاجة الى ميادين القتال التقليدية .[3] تبعا لذلك ، نتساءل ما هو مفهوم الحرب السيبرانية ؟ يعرف قاموس أوكسفورد الحرب السيبرانية بأنّها: "استخدام تكنولوجيا الكمبيوتر لمهاجمة أنظمة المعلومات التابعة لدولة أو منظمة، ومنعها من القيام بأنشطة هامّة." كما عرفها قاموس كامبردج انها " استخدام الإنترنت للهجوم على أجهزة الكمبيوتر الخاصة بالدولة من أجل الإضرار بأشياء مثل أنظمة الاتصالات والنقل أو إمدادات المياه والكهرباء".[4] وكذلك تعرف الحروب الالكترونية: "هي المشهد الصراعي المستقبلي والقادم للبشرية ولكن بصورة رقمية وتكنلوجية .[5] كما يعرف جوزيف ناي الحرب الالكترونية بأنّها "الأعمال العدائيّة في الفضاء السيبراني التي لها آثار تُعادل أو تفوق العنف الحركي التقليدي." بذلك يكون قد حدّد مدى قوّة تأثير الحرب

---

[1] منى الاشقر جبور ، السيبرانية هاجس العصر ، مصدر سبق ذكره ، ص30 . 34.

[2] . http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime legislation.pdf

[3] مرعي علي الرميحي ، ومتطلبات الامن القومي الجديدة ، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية ، المانيا / برلين ، ط1، 2022 ، ص30.

[4] مفهوم الحرب السيبرانية ، الموسوعة السياسية ، متاح على الرابط https://political-encyclopedia.org/dictionary/%D8%A7

[5] خالد الثوراني ، الجيوش الافتراضية بين الصراع الدولي والتسقيط السياسي المحلي ، شبكة النبا المعلوماتية ، تاريخ النشر 25/6/2017، متاح على الرابط https://annabaa.org/arabic/informatics/11558

السيبرانيّة وتفوّقها على كافة الحروب التقليديّة. [1]وثمة فروقات بين الحروب السيبرانية والحروب الالكترونية اذ ان الاخيرة توظف المجال الكهرومغناطسي الموجود عبر اجهزة الحاسوب وشبكات الانترنت وتعتمد على اسلحة عديدة منها [2]

ا . **الحقيبة الكهروستاتيكية** : وهو عباره عن جهاز صغير يشبه الحقيبة يقوم بتوليد نبضات كهرومغناطيسية فائقة القدرة يمكن من خلالها تدمير كافة الوحدات الالكترونية في أي مؤسسة مالية او محطة ارسال مما يتسبب في تعطيلها وافقادها فاعليتها .

ب . **القنبلة الالكتروستاتيكية** : تعمل هذه القنبلة على اطلاق اشعاع ضوئي عالي الطاقة عند اصطدامها بالاوكسجين والنيتروجين الموجود في الغلاف الجوي تطلق شحنة من الالكترونيات التي تنتشر لمئات الاميال ينتج عنها صاعقة صوتيه تعمل على تعطيل مصابيح الشوارع ومحطات الارسال واجهزة التلفاز وتتسبب في صهر خطوط الكهرباء والهواتف ، وترفع درجة حرارة الحواسيب وتدمر المعلومات المخزنة بها .

ت . **الفايروسات الذكية** : تمكنت العديد من الدول من تطوير فايروسات الكترونية يمكنها اختراق جميع الاجهزة والمعدات الالكترونية وتعطيلها وتدميرها وان استخدام هذه الفايروسات ضد اهداف مدنية او عسكرية ينذر بقيام حرب عالمية ثالثة تعتمد على اسلحة فائقة الدقة غير مرئية وغير مسيطر عليها ومن قبل عدو يصعب تمييزه او اكتشافه .

اما الحرب السيبرانية فتختلف في طبيعة أنشطتها وأهدافها [3]

فمن حيث الأنشطة تتكون الحرب السيبرانية من الهجوم الإلكتروني عبر الإنترنت (Cyber EA). وهو مهاجمة الدولة لأجهزة عدوها الالكترونية وشبكاته، بقصد تعطيلها وتدميرها، وبالتالي التسبب بأضرار مادية كبيرة له. ومن الحماية الإلكترونية عبر الإنترنت(Cyber EP) . والتي تتضمن إجراءات ووسائل حماية ودفاع سلبي للأجهزة الالكترونية من التعرض لأي هجوم سيبراني واجراءات ودعم الحرب الإلكترونية عبر الإنترنت(Cyber ES) . وهي إجراءات لتحديد مصدر الطاقة الكهرومغناطيسية من

---

https://www.siyassa.org.eg/News/18501.aspx

[1] المصدر نفسه

[2] **سبهان ابراهيم ، الحرب الالكترونية اخطر من الحرب النووية ، مجلة درع الوطن ، مديرية التوجيه المعنوي في القيادة العامه للقوات المسلحة ، الامارات ، متاح على الرابط**
https://www.nationshield.ae/index.php/home/details/research/

[3] المصدر السابق .

الأنظمة الشبكية بهدف دعم عمليات الدفاع او الهجوم المستقبلي. وتهدف عمليات الهجوم السيبراني إلى كشف أو تغيير أو تعطيل أو تدمير أو سرقة أو السيطرة على شبكات وأجهزة العدو والخصم، لا سيما في القطاعات الحيوية كالاتصالات وتوليد الكهرباء وتوزيع المياه، وحتى في إدارة قطاع النقل والمواصلات.

وهناك نوعين للهجوم: نشط أو غير نشط ، الهجوم النشط الذي يقوم بتغيير موارد النظام الالكتروني او التأثير على تشغيله. أما غير النشط فهو معرفة المعلومات والبيانات التي يحتويها هذا النظام والاستفادة منها، لكن دون وجود القدرة على إدخال تغييرات عليها. _اما عن أشكال الهجمات السيبرانية فهنالك الهجمات غير النشطة التي تتركز حول مراقبة أجهزة الكمبيوتر والشبكات، شبكات الاتصال السلكية واللاسلكية، التنصت على أنابيب الألياف الضوئية، والهجمات النشطة ، مثل هجوم رفض الخدمة، هجوم الحوت، هجوم "واناكاري" او برمجية الفدية.[1] وبالرجوع الى تاريخ هذا النوع من الحروب نجد ان عالم السياسة الامريكي مورتن كابلان كان قد اشار الى ان هذه الحروب كانت قد تطورت خلال الحرب الباردة بين الولايات المتحدة الامريكية والاتحاد السوفيتي السابق. الا ان التطبيق الفعلي لهذا النوع من الحروب كان خلال حرب الخليج الثانية عام 1991 عندما قامت القوات الامريكية باختراق وتعطيل منظومة الدفاع الجوي العراقية عبر تدمير كابلات الالياف الضوئية وشبكة الاتصالات العسكرية الممتدة بين بغداد والبصرة وكانت تلك الهجمات بمثابة الحملة الاولى لوسائل الحرب المضادة للقيادة والسيطرة والتي اشرت مجيء حرب الكترونية قادمة [2]

3. نماذج تطبيقية على الهجمات السيبرانية .

في البدء لم يكن للهجمات السيبرانية صدى على المستوى الدولي، واقتصر الموضوع على الجرائم السيبرانية التي تتعرض لها المؤسسات المالية والمصرفية فضلا عن الشركات المتخصصة ببرمجة نظم الاتصالات وقد دأبت الدول على اتخاذ التدابير اللازمة لتجريم تلك الافعال وفرض العقوبات . اما فيما يتعلق بموضوع الهجمات السيبرانية، فقدر اشار اليه الخبير الروسي ديمتري كريجوروف بانه يتجسد في التهديد على المستوى العسكري والسياسي فضلا عن التهديدات الاجرامية والارهابية التي يمكن

---

[1] الحرب الالكترونية والسيبرانية : تنوع اشكال والهدف واحد ، متاح على الرابط
https://alkhanadeq.com/post.php?id=1682
ايضا ، العوفي دليلة ، الحرب السيبرانية في عصر الذكاء الاصطناعي ورهاناتها على الامن الدولي ، مجلة الحكمة للدراسات الفلسفية ، مؤسسه كنوز الحكمة للنشر والتوزيع ، 2021، ص36

[2] . صلاح حيدر عبد الواحد ، مصدر سبق ذكره ، ص 25

لمجموعات من غير الدول تبنيها من اجل الحصول على مكاسب سياسية او اقتصادية . [1] واعلن المنتدى الاقتصادي العالمي أن الهجمات السيبرانية تشكل خامس أكبر الأخطار العالمية إلى جانب أسلحة الدمار الشامل والتغير المناخي، مرجحاً ارتفاع كلفة الهجمات إلى 10.5 تريليون دولار بحلول العام 2025، وبذلك ترتفع تلك الخسائر بمعدل 15 في المئة سنوياً إذ سجلت عام 2015 ثلاثة تريليونات دولار[2].

وهنالك العديد من النماذج على الهجمات السيبرانية منها الهجمات التي نفذتها الولايات المتحدة الامريكية عام 1982 ضد منظومة التحكم العالية صناعيا في انبوب نفط **(Chelyabinsk)** التابع للاتحاد السوفيتي السابق [3] وفي عام 1999تعرضت المانيا لهجوم سيبرأني استهدف الشركات الاقتصادية وتسبب في تعطيل المراكز المالية احتجاجا على اجتماع قمة مجموعة الثمان (G8) . [4]

وتعد الحرب السيبرانيّة الروسيّة الأوكرانيّة هي من اهم النماذج التطبيقية في مجال الحروب السيبرانية اذ سُجِّلَت أولى الهجمات السيبرانيّة على أنظمة المعلومات الخاصة بالشركات ومؤسسات الدولة في أوكرانيا خلال الاحتجاجات الجماهيريّة في عام 2013. [5] وتصاعدت الحرب السيبرانيّة الروسية مع اختراق شبكة الكهرباء الأوكرانية عام 2015 ومرة أخرى عام 2016 والهجوم على مواقع حكوميّة في أوكرانيا في ديسمبر 2016، فضلًا عن الهجمات الروسيّة في يونيو2017، والهجمات على مواقع الحكومة الأوكرانية في يناير 2022. [6] وجاءت هذه الهجمات في ظل توتر العلاقات بين روسيا واوكرانيا بعد ان ضمت روسيا شبه جزيرة القرم الاوكرانية الى اراضيها عام 2014 .[7] اما النموذج الأخر لتلك الهجمات هو ما تعرضت له انظمة الاتصال الالكترونية التابعة لوزارة الدفاع الامريكية ووكالة

---

[1] صلاح حيدر عبد الواحد ، مصدر سبق ذكره ، ص 26.25 .

[2] خليل موسى ، الهجمات السيبرانية ذراع العصر للصراع العالمي ، اندبندنت عربي متاح على الرابط، https://www.independentarabia.com/node/329781

[3] . محمد منذر جلال ، مصدر سبق ذكره ، ص 143. 144

[4] المصدر السابق ، ص 144 ص153.

[5] . وزارة الخارجية الأمريكية بيان للوزير أنتوني ج. بلينكن 10أيار/مايو، 2023. متاح على الرابط

https://www.state.gov/translations/arabic/%D9%86%D8%A8

[6] المصدر نفسه .

[7] . المصدر نفسه . كذلك ينظر ، عز الدين ابو عيشة ، الهاكرز : كتائب الاقتحام الالكتروني في الحرب الروسية . الاوكرانية ، اندبندنت عربي 25/شباط/ 2023 متاح على الرابط https://www.independentarabia.com/node/424096

الفضاء الامريكية ووكالة الطاقة الامريكية خلال المدة بين عامي 1998.2000 والتي ادت الى الاستحواذ على الألاف من الملفات التي تصنف بانها عالية السرية واتهمت الولايات المتحدة الامريكية روسيا الاتحادية في شن تلك الهجمات الا ان الاخيرة انكرت ذلك واعلنت انها غير مسؤولة عن تلك الهجمات . ويرى اخرون ان اول الهجمات السيبرانية هي تلك الهجمات التي شنت خلال حرب كوسوفو عام 1999 من خلال استهداف سلاح الجو التابع لحلف شمال الاطلسي شبكات الهاتف في يوغسلافيا (سابقا) [1] ومن الامثلة الاخرى على تلك الهجمات ، الهجوم الالكتروني الذي استهدف منظومة المعلومات التابعة لوزارة الصحة البريطانية عام 2017 مما ادى الى تخريب في السجلات الطبية في مجموعة من المستشفيات ، وتوقف بعض المنشأة الصحية عن العمل بسبب تلك الهجمات التي طالت اجهزة الحاسوب المتعلقة بالنظام الصحي .[2]

وعلى صعيد منطقة الشرق الاوسط ، تعرضت (اسرائيل) لهجمات سيبرانية نفذتها مجموعة "الانونميس" مما كبدها الكثير من الخسائر المادية والمعنوية وهو ما يشير الى حدوث تحول في وسائل الصراع العربي . الاسرائيلي بالاعتماد على وسائل التكنولوجيا والفضاء السيبراني في الحروب القادمة ، وفي ابريل عام 2013 تعرضت المواقع الاسرائيلية لا كبر الهجمات السيبرانية ونجحت في اختراق مواقع الحكومة والجيش والصناعات العسكرية ومنها موقع رئيس الوزراء ، ووزارة الدفاع والاستخبارات ، ومجلس الوزراء وسوق الاوراق المالية والمحاكم الاسرائيلية وشرطة تل ابيب ووزارة التعليم وبنك القدس ، بالإضافة الى قيام تلك المجموعة بنشر بيانات شخصية لأكثر من (5000) مسؤول اسرائيلي تضمنت اسماؤهم وارقامهم والعناوين الشخصية لبريدهم الالكتروني .[3]_كلما نفذت إيران عمليات سيبرانية ردا على نزاعات، أو توترات، أو تحركات اعتبرتها هجومية. سابقا، كانت تصمم تلك العمليات بشكل يُلحق تكاليف ملموسة ويُظهر قدرة استهداف استراتيجية مع الحفاظ على إمكانية الإنكار بشكل معقول وتجنب التصعيد.

---

[1] ـــ ـــــ ، الهجمات السيبرانية مفهومها والمسئولية الدولية الناشئة عنها في ضوء القانون الدولي المعاصر ، مجلة المحقق العلمي ، للعلوم القانونية والسياسية ، العدد الرابع ، السنة الثامنة ، 2016 ، ص 624.

[2] . صلاح عبد الواحد ، حروب الفضاء الالكتروني ، دراسة في مفهومها وخصائصها وسبل مواجهتها ، مصدر سبق ذكره ، ص30.

[3] . خالد وليد محمود ، الهجمات عبر الانترنت :ساحة الصراع الالكتروني الجديدة ، المركز العربي للابحاث ودراسة السياسات ، 2013 ، ص21. 22 .

ومن أبرز هذه الهجمات السيبرانية "عملية أبابيل" التي استهدفت المؤسسات المالية الأميركية بين عامَي (2012. 2013) و"هجوم شامون" عام 2012 ضد شركة النفط السعودية العملاقة "أرامكو". [1]

وبالمقابل، تعرضت ايران للعديد من الهجمات السيبرانية التي شنتها الولايات المتحدة الامريكية ضدها عبر استخدام فايروس (stuxnet)الذي تم تطويره لاستهداف المنشآت الصناعية الايرانية وخاصة النووية منها والذي ادى الى تدمير اكثر من (1000) جهاز طرد مركزي فضلا عن الهجمات التي تعرضت لها محطات النفط الايرانية . [2] اما على صعيد تطوير استراتيجيات مواجهة الهجمات السيبرانية تعد الولايات المتحدة الامريكية ، وكوريا الجنوبية ودول اوربية كبرى من اكثر المهتمين في هذا المجال . ففي عام 2012 قررت وزارة الدفاع الامريكية تمويل برنامج بحثي تتولاه وكالة مشاريع الابحاث المتقدمة اطلق عليه تسمية (Plan X) الغرض منه التوصل الى تقنيات انترنت عالية الدقة قادرة على فهم وتخطيط وتنفيذ المعارك عبر الانترنت ، والاكثر من ذلك البحث عن تقنيات جديدة في مجال تحجيم قدرة الاعداء على استخدام الانترنت لصالحهم [3]. _وقد طرح الرئيس الامريكي السابق دونالد ترامب خلال عام 2018 استراتيجية جديدة عرفت ب "الاستراتيجية القومية السيبرانية" التي جعلت من الفضاء السيبراني جزءا مهما لايتجزا عن جوانب الحياة الامريكية واعطت هذه الاستراتيجية للولايات المتحدة الامريكية الحق في الدفاع عن امنها السيبراني والامن القومي بشكل عام عبر تركيزها على حماية الشبكات والانظمة والبيانات ، وتعزيز اقتصاد رقمي امن ومزدهر والحفاظ على الامن والسلم الامريكي من خلال تعزيز التعاون مع الحلفاء لمعاقبة الجهات التي تستخدم الادوات السيبرانية لتهديد الامن القومي الامريكي _وفي مارس 2021 طرحت استراتيجية الرئيس الامريكي جو بايدن لمواجهة التهديدات السيبرانية وتحسين الدفاعات السيبرانية[4] .وثمة تنافس محموم بين الدول الاوربية لتطوير جيوشها الافتراضية وتطوير قدراتها على شن الهجمات الالكترونية ._اما على صعيد المنطقة العربية ، فقد تعرضت العديد من المواقع الخاصة بجهات امنية ووزارات مهمة الى اعتداءات واختراقات وتعطيل العمل فيها لعدة ساعات ومنها

---

[1] . المصدر نفسه ، ص 208. كذلك ينظر ، الازمة الايرانية تنتقل الى الفضاء السيبراني ، 12/ حزيران /2019 متاح على الرابط https://www.alhurra.com/different- .

[2] . الهجمات السيبرانية على ايران ، الابعاد والتداعيات ، 4 /مارس / 2020 ، ملتقى ابو ظبي ، مركز الامارات للسياسات متاح على الرابط https://epc.ae/ar/brief/cyber-attack-on-iran-dimensions-and-implications ، تاريخ الدخول 2023/11/11 س 10:27

[3] . عباس متعب فرج ، مصدر سبق ذكره ، ص 207

[4] . المصدر نفسه ، ص 208 .

دولة الامارات العربية المتحدة ففي هذا الاطار صرح القائد السابق لسلاح الجو في الاماراتي بحدوث اختراق للبنى التحتية الاماراتية من قبل المتسللين عبر الانترنت سيما بالتزامن مع تصاعد التوتر بين الفلسطينيين واسرائيل وهو ما جعل الكثير من الدول العربية تبحث عن تطوير قدراتها في هذا المجال ولكنها تتسم بالسرية وتعد دول الخليج العربي ودولة المغرب الاكثر تقدما في هذا المجال .[1]

- **الخاتمة والاستنتاجات**

شكل الفضاء السيبراني ميداناً جديدا لممارسة النفوذ العالمي والتنافس الدولي وذلك عبر توظيف السيبرانية وهو ماحول الصراع في النظام الدولي من الصراعات والحروب التقليدية الى نوع أخر من الصراعات والحروب الا وهي الصراعات والحروب السيبرانية فقد ادى تزايد الاعتماد على الحواسيب في ظل الثورة المعلوماتية الى التأثير في كافة جوانب ومجالات العلاقات بين الدول سياسيا، واقتصاديا ، وعسكريا وامنيا وهو ما لفت انظار الوحدات الدولية الى ضرورة تعزيز قدراتها الهجومية السيبرانية وتقوية استراتيجياتها الدفاعية عبر تطوير برامج لتحصين برامجها الإلكترونية وتزداد خطورة هذه الهجمات في الحالات التي يتوقع ان يقوم بها اطراف من الفاعلين من غير الدول ، دون القدرة على تحديد هوياتهم وهو ما يشكل تحديا كبيرا امام الهجمات السيبرانية كتلك التي تتصل بصعوبة إسنادها إلى مرتكبيها، وتراجع تكلفتها مقارنة بأدوات القوة الصلبة، وقدرتها على استهداف الخصوم على نحوٍ دقيق دون المساس بالمدنيين.

ومن المتوقع ان يصبح الصراع من أجل السيطرة على الفضاء السيبراني في المستقبل المنظور الشكل المهيمن للمنافسة الاستراتيجية في عصر المعلومات. بعد ان اصبحت المعلومات موردًا استراتيجيًّا مهما بين الدول لتعظيم الاستفادة من مزاياه العسكرية والاقتصادية. وفي ذلك الإطار، لا يتطلب الأمر استراتيجية مختلفة لاستخدام الفضاء السيبراني، ولكن منظارًا أوسع للاستراتيجية السيبرانية وقد توصل البحث الى مجموعة من الاستنتاجات منها :

1. ان التطور الذي يشهده النظام الدولي في مجال ثورة التكنولوجيا والمعلومات وظهور ما يعرف بالفضاء السيبراني يعد من المؤشرات الواضحة والمهمة على تغير ميادين الصراعات والحروب من الميادين التقليدية الى الميادين او الفضاءات السيبرانية وهي فضاءات افتراضية تتصف بطبيعة وخصائص تختلف عن الميادين المادية .

[1] . منى الاشقر جبور ، السيبرانية هاجس العصر ، مصدر سبق ذكره ، ص 69

2. ان الحروب الالكترونية عززت من فرص وجود الحروب اللامتماثلة من حيث مستوى القوة او طبيعة اطرافها ، اذا اصبح من الممكن ان تقوم دول صغرى بشن هجمات ضد دول اقوى منها ، بل اصبح من الممكن قيام الافراد او اطراف غير دوليين بشن هجمات ضد الفواعل الدولية .

3. ادت حروب الفضاء الالكتروني الى تراجع مفاهيم الردع التقليدية لصالح ظهور اساليب ردع جديدة قائمة على وضع استراتيجيات دولية جديدة لردع محاولات الاختراق الالكتروني سيما للمؤسسات الحيوية للدولة وزيادة التركيز على حماية الامن السيبراني .

List of sources

First/Books

1- Aws Majeed Ghaleb Al-Awadi, Cyber Information Security, Al-Bayan Center for Studies and Planning, Baghdad, August, 2016 2- Hassan Muzaffar, Information Space, Beirut: Center for Arab Unity Studies, 2007.

3- Khaled Walid Mahmoud, Online attacks: The new arena of electronic conflict, Doha, Qatar, Arab Center for Research and Policy Studies, 2013

4- Muhammad Munther Jalal and Sira Ghadhban, Cyber War Technology and International Confrontation Strategy, Baghdad, Adnan Publishing House, 1st edition, 2021.

5- Marai Ali Al-Rumaihi, and the new national security requirements, Arab Democratic Center for Strategic, Political and Economic Studies, Germany / Berlin, 1st edition, 2022

6- Mona Al-Ashqar Jabour, Cyber Obsession of the Age, Arab Center for Legal and Judicial Research, League of Arab States, available at the link, https://t.me/montlq

Second: Arab magazines and periodicals.

1- Ismail Zarrouqa, Cyberspace and the Transformation in the Concepts of Power and Conflict, Journal of Legal and Political Sciences, Volume 10, Issue 1, April, 2019.

2- Al-Awfi Dalila, Cyber warfare in the age of artificial intelligence and its stakes on international security, Al-Hikma Journal for Philosophical Studies, Kunuz Al-Hikma Foundation for Publishing and Distribution, 2021.

3- Hazem Muhammad Khayel, Exploiting Cyberspace in Unconventional Wars: A Study of Cyber Agency and Cyber Terrorism, Scientific Journal of the Faculty of Economic Studies and Political Science at Alexandria University, Volume Eight, Issue 15, January 2023.

4- Saif Nusrat Al-Harmuzi, Description of Approaches to the Digital Actor's Perspectives and Strategic Exposure in Light of Cyberspace, Al-Farahidi Arts Magazine, Issue 37, March, 2019.
5-Abbas Miteb Faraj, Cyber War: A Study of Cyber Attacks between the United States and Iran, Hammurabi Journal of Studies, Issue 40, 2021.
6- Lubna Khamis Mahdi, Safaa Mahdi's tweet, The impact of cyberspace on the development of power, Hammurabi Journal of Studies, Hammurabi Center for Research and Strategic Studies, Issue 33-34, 2020.
7- Mahmoud Ali Abdel Rahman, Cyberspace and its impact on the concepts of power, security, and conflict in international relations, Journal of the Faculty of Politics and Economics, Beni Suef University, Volume 16, Issue 15, July, 2022.
8- Noura Shaloush, Electronic piracy in cyberspace: The rising threat to the security of countries, Journal of the Babel Center for Humanitarian Studies, Volume 8, Issue 2, 2018.
9- cyber attacks, their concept and the international responsibility arising from them in light of contemporary international law, Al-Muhaqqiq Al-Ilmi Journal, for Legal and Political Sciences, fourth issue, eighth year, 2016.

Third: University theses and dissertations

:

1- Adel Abdel-Sadiq, The impact of electronic terrorism on the principle of the use of force in international relations 2001-2007, Master's thesis, Faculty of Politics and Economics, Cairo, 2009.
2- Salah Haider Abdel Wahed, Cyber Wars, a study of their concept, characteristics, and ways to confront them, Master's thesis, College of Arts and Sciences, Middle East University, July 2021

Third: Internet research and articles.

1- Imogen Foulkes, Cyber Peace in the Light of the War in Ukraine, January 30, 2023, available at the link: https://www.swissinfo.ch/ara/business/%D9%85%D8%A7-
2-Joseph S. Nye, War and Peace in Cyberspace, research published on the International Information Network, 2/24/2005, website: http://www.project-syndicate.org/commentary/president-push-gose-soft/Arabic
3-Khaled Al-Thawrani, Virtual Armies between International Conflict and Local Political Destruction, Annabaa Information Network, available at the link https://annabaa.org/arabic/informatics/11558
4-Khalil Musa, Cyberattacks, the era's arm of global conflict, Independent Arabic, available at the link: https://www.independentarabia.com/node/329781

5-Rula Hoteit, Cyber, The Hidden War in the Dark Zone, Researcher Center for Palestinian and Strategic Studies, available at the link https://www.bahethcenter.net/uploaded/files/%D8%A7%D9%84%D8%B3%D%29

6-Sobhan Ibrahim, Electronic warfare is more dangerous than nuclear war, Nation Shield Magazine, Directorate of Moral Guidance at the General Command of the Armed Forces, UAE, available at the link https://www.nationshield.ae/index.php/home/details/research/

7-Adel Abdel-Sadiq, Patterns of cyber warfare and its repercussions on global security, International Politics Journal, Al-Ahram Foundation, available at the link:
https://www.siyassa.org.eg/News/12072.aspx

8-Izz al-Din Abu Aisha, Hackers: Electronic Intrusion Brigades in the Russian-Ukrainian War, Independent Arabic, February 25, 2023, available at the link https://www.independentarabia.com/node/424096

9-Ali Ferjani, Technological Transformations of Cyber Wars... NATO as a Model, International Politics, Al-Ahram Foundation, 2/7/2023, available at the link https://www.siyassa.org.eg/News/18501.aspx

10-The concept of cyber warfare, the political encyclopedia, available at the link1https://political-encyclopedia.org/dictionary/%D8%A7

11-US Department of State, Statement by Secretary Anthony J. Blinken May 10, 2023. Available at the link
https://www.state.gov/translations/arabic/%D9%86%D8%A8

12-Cyber attacks on Iran, dimensions and repercussions, March 4, 2020, Abu Dhabi Forum, Emirates Policy Center, available at the link https://epc.ae/ar/brief/cyber-attack-on-iran-dimensions-and-implications.