مجلة جامعة الانبار للعلوم القانونية والسياسية

اسم المقال: الإطار التنظيمي لاستخدام المرتزقة السيبرانين بموجب القانون الدولي
اسم الكاتب: م.د. مصطفى عماد محمد البياتي
رابط ثابت: https://political-encyclopedia.org/index.php/library/6367
تاريخ الاسترداد: 2026/11/03 09:29 +03

الموسوعة السياسيّة هي مبادرة أكاديمية غير هادفة للربح، تساعد الباحثين والطلاب على الوصول واستخدام وبناء مجموعات أوسع من المحتوى العلمي العربي في مجال علم السياسة واستخدامها في الأرشيف الرقمي الموثوق به لإغناء المحتوى العربي على الإنترنت.
لمزيد من المعلومات حول الموسوعة السياسيّة - Encyclopedia Political، يرجى التواصل على info@political-encyclopedia.org

استخدامكم لأرشيف مكتبة الموسوعة السياسيّة - Encyclopedia Political يعني موافقتك على شروط وأحكام الاستخدام المتاحة على الموقع https://political-encyclopedia.org/terms-of-use

تم الحصول على هذا المقال من موقع مجلة جامعة الانبار للعلوم القانونية والسياسية ورفده في مكتبة الموسوعة السياسيّة مستوفياً شروط حقوق الملكية الفكريّة ومتطلبات رخصة المشاع الإبداعي التي ينضوي المقال تحتها.

Journal of Anbar University for Law and Political Sciences
مجلة جامعة الانبار للعلوم القانونية والسياسية
P. ISSN: 2706-5804 E.ISSN: 2075-2024
Volume 14- Issue 1- March 2024 المجلد ١٤- العدد ١ – اذار ٢٠٢٤

Regulatory Framework for the Use of Cyber Mercenaries under International Law

[1] Lecturer Dr. Mustafa Emad Mohammed Al-Bayati
[1] Kufa University - College of law

1: Email: mustafai.albayati@uokufa.edu.iq
2: Email:

Abstract:

The emergence of a new type of mercenary, represented by cyber mercenaries, especially with the subject's lack of international regulation, has led many States to use and purchase their services for the range of advantages offered by such use, since attacks by cyber mercenaries pose a challenge to the concept of direct participation in hostilities provided for in the article. (47) of Additional Protocol I to the Geneva Conventions, since the port of the cyberattack may be far from confrontational, yet it does harm directly and significantly to the other party. The use of cybercrime mercenaries is a real challenge to accountability and punishment, for the difficulty of identifying the mercenary and establishing the link between him and the user.

We have adopted the analytical curriculum in our study of the research topic and have concluded a number of results, the most important of which is, International conventions dealing with mercenaries, such as Additional Protocol I to the 1977 Geneva Conventions, The 1977 OAU Convention on the Elimination of Mercenarism in Africa, The 1989 International Convention against the Recruitment, Use, Financing and Training of Mercenaries was all incomplete and inadequate in defining the concept of mercenary because it did not cover all forms of mercenarism, especially modern ones, and because it took the traditional approach established under the article. (47) of Additional Protocol I, and that it is difficult to achieve the attribution of international responsibility to the State at the present time, depending on the evolution of techniques that make it unequivocal and irrefutable to establish the State's relationship with cybercrime mercenaries.

DOI
10.37651/aujlps.2023.144035.1097

Submitted: 24/1/2024
Accepted: 10/2/2024
Published: 15/03/2024

Keywords:
Cyber mercenaries
Cyber attacks
Cyberspace
Armed Attack
Shutdown and denial of service attacks (DDOS)
Scanning Attack
Reasonable denial.

©Authors, 2024, College of Law University of Anbar. This is an open-access article under the CC BY 4.0 license (http://creativecommons.org/licenses/by/4.0/).

الإطار التنظيمي لاستخدام المرتزقة السيبرانيين بموجب القانون الدولي

م.د. مصطفى عماد محمد البياتي [١]
[١] جامعة الكوفة – كلية القانون

الملخص:

ان ظهور نوع جديد من المرتزقة متمثلا بالمرتزقة السيبرانيين ، خاصة مع افتقار الموضوع للتنظيم على الصعيد الدولي ، دفع العديد من الدول الى استخدامهم وشراء خدماتهم لمجموعة المزايا التي يوفرها ذلك الاستخدام ، حيث ان الهجمات التي يقوم بها المرتزقة السيبرانين تشكل تحديا لمفهوم المشاركة المباشرة في الاعمال العدائية الوارد النص عليه في المادة (٤٧) من البروتوكول الاضافي الاول لاتفاقيات جنيف ، اذ من الممكن ان يكون منفذ الهجوم السيبراني بعيد كل البعد عن حظ المواجهة ومع ذلك يقوم بالحاق الضرر بشكل مباشر وكبير بالطرف الاخر و يمثل استخدام المرتزقة السيبرانيين تحدياً حقيقياً للمسائلة والعقاب ، لصعوبة تحديد المرتزق واثبات الصلة بينه وبين الجهة التي استخدمته . وقد اعتمدنا المنهج التحليلي عند دراستنا لموضوع البحث وانتهينا الى عدد من النتائج يتمثل اهمها في ، ان الاتفاقيات الدولية التي تناولت موضوع المرتزقة كالبروتوكول الإضافي الأول لاتفاقيات جنيف الصادر عام ١٩٧٧ ، و اتفاقية منظمة الوحدة الافريقية للقضاء على الارتزاق في افريقيا لعام ١٩٧٧ ، والاتفاقية الدولية لمناهضة تجنيد المرتزقة واستخدامهم وتمويلهم وتدريبهم لعام ١٩٨٩ اتسمت جميعها بالنقص والقصور عند تحديدها لمفهوم المرتزق وذلك لكونها لم تشمل كل صور الارتزاق وخاصة الحديث منها ولكونها اخذت بالنهج التقليدي الذي أُسس بموجب المادة (٤٧) من البرتوكول الإضافي الأول ، و ان من الصعب تحقق اسناد المسؤولية الدولية الى الدولة في الوقت الحاضر و يتوقف تحقق ذلك على تطور التقنيات التي تجعل اثبات علاقة الدولة بالمرتزقة السيبرانيين امر لا لبس فيه و بأدلة رقمية لا يمكن دحضها .

الكلمات المفتاحية:

المرتزقة السيبرانيين ، الهجمات السيبرانية ، الفضاء السيبراني ، الهجوم المسلح ، هجمات الاغلاق والحرمان من الخدمة ، هجمات المسح ، الانكار المعقول .

المقدمة

ان استخدام المرتزقة مشكلة ليست بالجديدة على الصعيد الدولي ، الا انها ظهرت بوجه جديد من خلال ظهور وازدهار نوع من المرتزقة تعمل في الفضاء السيبراني ، خاصة مع افتقار الموضوع للتنظيم على الصعيد الدولي ، مما دفع العديد من الدول الى استخدام وشراء خدمات هذا النوع من المرتزقة لما يوفروه من مزايا تتمثل اهمها في امكانية الانكار المعقول وتجنب التدخل بشكل مباشر وقلة التكاليف ، وقد برز ذلك في النزاعات الحديثة كما في النزاع الروسي الجورجي عام ٢٠٠٧ والنزاع الروسي الاوكراني منذ العام ٢٠١٤ ولغاية الان والتي بينها في متن البحث عند الحديث عن تطبيقات استخدام المرتزقة السيبرانيين .

ان الهجمات التي يقوم بها المرتزقة السيبرانيين تشكل تحديا لمفهوم المشاركة المباشرة في الاعمال العدائية الوارد النص عليه في المادة (٤٧) من البروتوكول الاضافي الاول لاتفاقيات جنيف ، اذ من الممكن ان يكون منفذ الهجوم السيبراني بعيد كل البعد عن حظ المواجهة ومع ذلك يقوم بالحاق الضرر بشكل مباشر وكبير بالطرف الاخر ؛ وعلى الرغم مما تقدم فأن العديد من الهجمات السيبرانية صنفت على انها لم تستوف عتبة استخدام القوة او الهجوم المسلح الوارد في المادة (٤/٢) من ميثاق الأمم المتحدة ، لكنها بسبب ما افرزته النزاعات المسلحة الحالية وخاصة النزاع الروسي الاوكراني فان الامر يستوجب إعادة النظر في طبيعة هذه الهجمات اذ أصبحت تستهدف البنى التحتية الأساسية واهداف عسكرية اثناء النزاع المسلح ، وبالتالي فأنها أصبحت تمثل انتهاكا لمبادئ منع التدخل وسيادة الدولة وخطر استخدام القوة .

أولا : أهمية موضوع البحث :

وتكمن أهمية موضوع البحث في الاتي :

١- ازدياد لجوء الدول الى استخدام المرتزقة السيبرانيين في نزاعاتها المسلحة وحتى في وقت السلم لما يوفره ذلك من مزايا يتمثل أهمها في منح الدولة إمكانية الانكار عن وجود اية صلة لها مع الأفعال والهجمات التي ينفذها هؤلاء المرتزقة.

٢- اهتمام المجتمع الدولي بتطور استخدام هذه الفئة من خلال مناقشة الفريق العامل المعني باستخدام المرتزقة كوسيلة لانتهاك حقوق الانسان واعاقة ممارسة حق الشعوب في تقرير مصيرها ، في تقريره لعام ٢٠٢٠-٢٠٢١ الى الاثار السلبية التي يشكلها استخدام المرتزقة السيبرانيين على حقوق الانسان .

ثانيا : مشكلة موضوع البحث :

وتتمثل مشكلة البحث في الاتي :

١- ان ما نجده حاليا من اتفاقيات دولية تُعنى بالمرتزقة وخاصة ما ورد بموجب المادة (٤٧) من البروتوكول الإضافي الأول لاتفاقيات جنيف فهي تضع عتبة مرتفعة لانطباق وصف

المرتزق على المشاركين في النزاعات المسلحة ، وبالتالي يثار التساؤل المتمثل في هل تعد الهجمات السيبرانية اذا استوفت معايير محددة مشاركة مباشرة في الاعمال العدائية ، وهل يعد منفذيها مرتزقة ؟

٢- كما يمثل استخدام المرتزقة السيبرانيين تحدياً حقيقياً للمسائلة والعقاب ، لصعوبة تحديد المرتزق واثبات الصلة بينه وبين الجهة التي استخدمته .

ثالثا : منهج البحث:

وسنعتمد المنهج التحليلي لتحليل موضوع البحث ولمحاولة الإحاطة بكافة جوانبه ، والبحث في التطبيقات الحديثة له .

رابعا : هيكل البحث :

وسنتناول موضوع البحث في ثلاث مباحث نخصص الأول لبيان ماهية المرتزقة السيبرانيين وندرس في الثاني تطبيقات استخدام المرتزقة السيبرانيين اما المبحث الثالث فسنفرده لطبيعة العلاقة المنشئة للمسؤولية الدولية المترتبة عن استخدام المرتزقة السيبرانيين نسبقها بمقدمة ونلحقها بخاتمة نبين فيها اهم ما توصلنا اليه من استنتاجات وتوصيات .

I. المبحث الاول

ماهية المرتزقة السبرانيين

يلاقي استخدام المرتزقة السيبرانيين رواجا في الاونة الاخيرة وذلك لما يمتاز به هذا الاستخدام من خصائص ، مما يثر تحديات قانونية تتعلق بعدم وجود تعريف خاص بالمرتزقة بشكل عام والمرتزقة السيبرانيين بشكل خاص ، وضرورة تحديد الخصائص التي يتصف بها هؤلاء المرتزقة لكي يصبح من الممكن معرفة حقيقتهم وماهيتهم .

ولذلك سنتناول هذا المبحث في مطلبين نخصص الاول لتعريف المرتزقة السيبرانيين وندرس في الثاني الخصائص المميزة للمرتزقة السبرانيين .

I.أ. المطلب الأول

تعريف المرتزقة السيبرانيين

يعد من الضروري وضع تعريف للمرتزقة السيبرانيين يتصف بالوضوح وبالقابلية للتطبيق ، فاذا اريد ان يتم معاقبة هذه الفئة فلابد من وجود معايير واضحة لتحديدهم ، وكذلك اذا وضعنا على الدول التزاماً بمنع استخدام المرتزقة السيبرانيين ومحاسبتهم على أي نشاط يقومون به على اقليمها فينبغي قبل ذلك وضع تعريف او تحديد دقيق للمرتزقة السيبرانيين لكي تتمكن الدول من القيام بواجباتها [1] .

ويتنازع تعريف المرتزق بشكل عام اتجاهين نوردهما ادناه :

(1) Henry C. Burmester, "The recruitment and use of mercenaries in armed conflicts." American Journal of International Law , Vol (72), No (1) , (1978) , p, 37.

أولا / التعريف التقليدي للمرتزق :

ويمكن ان نلمس وجود هذا الاتجاه في التعريف الوارد في الاتفاقيات الدولية وكذلك في التعاريف الفقهية التي تناولت الموضوع ، لذلك سنتناول هذا الاتجاه في الفقرتين ادناه :

أ/ التعريف الاتفاقي :

لا يمكن لنا ان نسلم بوجود تعريف للمرتزق ورد في الاتفاقيات الدولية ، لكون ما ورد في هذه الاتفاقيات لا يعدو ان يكون تحديداً ووصفاً للمرتزق فقط [١]، ونجد هذا التحديد وارداً في البروتوكول الإضافي الأول لاتفاقيات جنيف الصادر عام ١٩٧٧ [٢] ، وفي اتفاقية منظمة الوحدة الافريقية للقضاء على الارتزاق في افريقيا لعام ١٩٧٧ [٣] ، والاتفاقية الدولية لمناهضة تجنيد المرتزقة واستخدامهم وتمويلهم وتدريبهم لعام ١٩٨٩ [٤]، وقد ورد في هذه

---

(1) Christopher Kinsey, "International Law and the Control of Mercenaries and Private Military Companies," Cultures & Conflits [Online], English documents, online June 26, 2008, accessed March 30, 2021. P , 4-5. URL http://journals.openedition.org/conflits/11502

(٢) تنص المادة (٤٧)، من البروتكول الاضافي الاول على ما يلي " ١- لا يجوز للمرتزق التمتع بوضع المقاتل أو أسير الحرب.

٢- المرتزق هو أي شخص :

أ) يجرى تجنيده خصيصاً، محلياً أو في الخارج، ليقاتل في نزاع مسلح،

ب) يشارك فعلاً ومباشرة في الأعمال العدائية،

ج) يحفزه أساساً إلى الاشتراك في الأعمال العدائية، الرغبة في تحقيق مغنم شخصي، ويبذل له فعلاً من قبل طرف في النزاع أو نيابة عنه وعد بتعويض مادي يتجاوز بإفراط ما يوعد به المقاتلون ذوو الرتب والوظائف المماثلة في القوات المسلحة لذلك الطرف أو ما يدفع لهم،

د) وليس من رعايا طرف في النزاع ولا متوطناً بإقليم يسيطر عليه أحد أطراف النزاع،

= هـ) ليس عضواً في القوات المسلحة لأحد أطراف النزاع، وليس موفداً في مهمة رسمية من قبل دولة ليست طرفاً في النزاع بوصفه عضواً في قواتها المسلحة.

(٣) المادة (١)، من اتفاقية منظمة الوحدة الافريقية للقضاء على الارتزاق في الوثيقة CM/817 (XXIX) Annex II Rev-1 ،حيث جائت هذه المادة ترتكز على ذات التحديد الوارد في المادة (٤٧) من البروتكول الاضافي الاول مع المحاولة لتوسعة مفهوم الوارد في المادة (٤٧) من البروتكول المذكور من خلال اضافة الفقرة (٢)، للمادة (١)، من الاتفاقية ، ينظر :

Ilaria D'Anna , I mercenari nel diritto internazionale , Dottorato di ricerca in Ordine Internazionale e Diritti Umani , Sapienza Universita DI Roma FACOLTÀ DI SCIENZE POLITICHE , Anno Accademico 2010 - 2011 , p.p. 122-124 .

(٤) وتنص الفقرة (٢)، من المادة (١)، من الاتفاقية على " ٢. والمرتزق هو أيضا أي شخص يقوم، في أي حالة أخرى، بما يلي:

(أ) تم تجنيده خصيصا محليا أو خارجيا لغرض المشاركة في عمل من أعمال العنف المتضافرة التي تهدف إلى: '١' الإطاحة بحكومة أو تقويض النظام الدستوري للدولة ؛ أو '٢' تقويض السلامة الإقليمية لدولة ما " وللمزيد من المعلومات حول الاتفاقيات اعلاه ينظر : د. كاظم عبد علي و مالك عباس جيثوم، "الأساس القانوني لتنظيم الارتزاق في القانون الدولي"، *مجلة الكلية الإسلامية الجامعة* ، العدد (٥٩) ، الجزء (١)، (٢٠٢١).

الاتفاقيات الثلاث نهجين الأول تقييدي كما هو الحال في النص الوارد في البروتوكول الإضافي الأول الذي لا يمكن ان يطبق الا في حالات نادرة جدا [١] ، والنهج الثاني بأخذ بالمفهوم الواسع لتحديد المرتزق كما نلاحظ ذلك من خلال نص المادة (١) من الاتفاقية الدولية لمناهضة تجنيد المرتزقة واستخدامهم وتمويلهم وتدريبهم لعام ١٩٨٩[٢].

وبالمحصلة يمكن لنا ان نلاحظ بان الاتفاقيات الثلاث المبينة مسبقاً اتسمت بالنقص والقصور عند تحديدها لمفهوم المرتزق وذلك لكونها لم تشمل كل صور الارتزاق وخاصة الحديث منها ولكونها اخذت بالنهج التقليدي الذي أُسس بموجب المادة (٤٧) من البرتوكول الإضافي الأول .

ب/ التعريف الفقهي:

وقد عرف الفقه التقليدي المرتزقة بأنهم (كل مدني مسلح يتقاضى اجراً للقيام بعمليات عسكرية في منطقة نزاع اجنبي)[٣] ، كما عرف بأنه (جندي على استعداد لبيع مهاراته العسكرية لمن يدفع اعلى سعر ، بغض النظر عن السبب)[٤] ، وعرف أيضا بأنه (جندي محترف يقاتل من اجل أي دولة او امة بغض النظر عن المصالح او القضايا السياسية)[٥].

ويظهر من التعاريف أعلاه انها تشترط توافر مجموعة من الخصائص لانطباق مفهوم المرتزق تتمثل في المشاركة المباشرة في نزاع مسلح ، وان يكون الشخص اجنبي (ليس من مواطني احد اطراف النزاع) ، وان يهدف لتحقيق الربح المادي ، وهذه الخصائص مأخوذة من المفهوم التقليدي الوارد في المادة (٤٧) من البرتوكول الإضافي الأول .

وخلاصة القول بأن الاتجاه التقليدي لتعريف المرتزق لم يعد كافياً ليشمل جميع النشاطات التي يمكن ممارستها اليوم من خلال شبكات الانترنت العابرة للحدود ، اذ بإمكان المرتزق ان لا يشارك بالقتال المسلح وانما يقوم بشن هجمات الكترونية تستوفِ معايير

---

(١) ذهب البعض تعبيرا عن الطابع التقييدي الوارد في المادة (٤٧)، من البروتكول الاضافي الاول الى درجة التندر بالقول (كل مرتزق لا يستطيع استبعاد نفسه من هذا التعريف يستحق اطلاق النار عليه وعلى محاميه) ، ينظر :

Geoffrey Best , Humanity in Warfare : The Modern History of the International Law of Armed Conflicts , First publishing , Little Hampton Book Services Ltd Publisher , 1980 , p, 328 .

(2) Ilaria D'Anna , op.cit, p.p, 132-137 .

(3) Sean McFate , Mercenaries and War: Understanding Private Armies Today , National Defense University Press , DU Washington, D.C. , Press First printing, December 2019 , p. 7 .

(4) Christopher Kinsey, op.cit, p, 5 .

(5) PR Kumar ,The Dogs of War Multidomain Mercenaries Operating in the Ukraine War ,Centre for Land Warfare Studies , "MANEKSHAW PAPER. No. 99, New Delhi , 2023 , p.1

الهجمات المسلحة من حيث اثارها المدمرة الناتجة عنها، لذلك ينبغي ان يكون تعريف المرتزق يساير هذه التحديات الموجودة على الساحة الدولية حاليا [١] .

ثانيا: التعريف الحديث للمرتزق :

نظرا للنقص في التعريف التقليدي للمرتزق انبرى اتجاه في الفقه الدولي لغرض وضع تعريف حديث للمرتزق و تكمن الميزة الأساسية لهذا الاتجاه بأخذه بنظر الاعتبار الأنشطة الحديثة للمرتزقة في الفضاء السيبراني، اذ يعرف المرتزقة طبقا لهذا الاتجاه بأنهم (جهات وسيطة ذات قدرات هجومية سيبرانية تقوم على نحو غير مشروع بترويج معلومات استخبارية مخترقة ، او برامج حاسوبية مستقلة ، او خبرات تقنية لاحد المستفيدين مقابل مكاسب مالية او ايدلوجية) [٢] ، كما عرفوا بأنهم (فرد او مجموعة من الخبراء يمكنهم تقديم مهاراتهم لأي شخص يدفع مبلغاً جيداً من المال) [٣] ، اما الفريق العامل المعني باستخدام المرتزقة كوسيلة لانتهاك حقوق الانسان واعاقة ممارسة حق الشعوب في تقرير المصير فعرفهم بأنهم (فئة من الجهات الفاعلة التي يمكنها ان تولد أنشطة متصلة بالمرتزقة) [٤] .

(1) Noëlle van der Waag-Cowling and others , report on the provision of military and security cyber products and services by ‘cyber mercenaries’ and its human rights impact , Submission to the Working Group on the use of mercenaries , 2021 . Available at https://www.ohchr.org/sites/default/files/Documents/Issues/Mercenaries/WG/CyberMercenaries/AccessNow.pdf

(2) Jose de Arimateia da Cruz and Pedron Stephanie , Cyber Mercenaries: A New Threat to National Security, International Social Science Review journal , Vol. 96 , Iss. 2 , Article 3 , 2020 , p.3 .

(3) Alexandra Borgeaud dit Avocat, Arta Haxhixhemajli, Michael Andruch - Editors , NEW TECHNOLOGIES, FUTURE CONFLICTS, AND ARMS CONTROL , Center for Security Analyses and Prevention, Prague , JANUARY 2021 . p. 50 .
Available at : https://cbap.cz/wp-content/uploads/CBAP_NewTechPaper2021FREN.pdf

(٤) تقرير الفريق العامل المعني بمسألة استخدام المرتزقة وسيلة لانتهاك حقوق الانسان وإعاقة ممارسة حق الشعوب في تقرير مصيرها ، آثار المرتزقة والجهات الفاعلة ذات الصلة بالمرتزقة والشركات العسكرية والامنية الخاصة التي تشارك في انشطة الكترونية على حقوق الانسان ، الوثيقة A/76/151 ، ٢٠٢١ ، ص٤ .

ونرى بأنه لا بأس باستخدام العناصر الأساسية التي يقوم عليها النهج التقليدي في تعريف المرتزق مع إضافة الخصائص المميزة للمرتزقة السيبرانيين عند وضع تعريف خاص بهم وذلك لاتحاد الفئتين بالعناصر الأساسية[١]، وعليه يمكن لنا وضع تعريف للمرتزقة السيبرانيين يتمثل في الاتي (أي شخص اجنبي طبيعي او معنوي يستخدم الفضاء السيبراني للمشاركة في نزاع مسلح او عنف موجه الى التدخل بشكل غير مشروع في الشؤون الداخلية او تقويض السلامة الإقليمية او الاستقلال السياسي لإحدى الدول بهدف تحقيق مكاسب شخصية).

ويتميز التعريف الذي اوردناه أعلاه باحتفاظه بالخصائص الأساسية للمرتزقة التقليدين التي يتمثل أهمها في كون المرتزق اجنبي ليس احد رعايا اطراف النزع ، وبكونه يهدف الى تحقيق مكسب شخصي ، واخذ التعريف أيضا بالمفهوم الواسع للمرتزق الذي يمكن ان نلمسه في نص الفقرة (٢) من المادة (٢) من الاتفاقية الدولية لمناهضة تجنيد المرتزقة واستخدامهم وتمويلهم وتدريبهم ، اذ يمكن ان يعمل المرتزقة من خلال هذا المفهوم في أوقات النزاع المسلح والسلم أيضاً ، كما ان اهم ما يميز تعريفنا هذا كونه اخذ بنظر الاعتبار الاشكال الحديثة للمرتزقة المتمثلة بمرتزقة الفضاء السيبراني فهو اذاً يتفق مع الاتجاه الحديث لتعريف المرتزق .

(١) ينظر في المعنى نفسه :
Usalama Reforms Forum , Report on The Provision of Military and Security Cyber Products and Services by 'Cyber Mercenaries' and Its Human Rights , Kenyan , Available at :
https://usalamaforum.org/wp-content/uploads/2021/09/Report-on-The-Provision-of-Military-and-Security-Cyber-Products-and-Services-by-%E2%80%98Cyber-Mercenaries-and-Its-Human-Rights-Impact.pdf

I.ب. المطلب الثاني

الخصائص المميزة للمرتزقة السيبرانيين [١]

Distinctive characteristics of cyber mercenaries

يمكن لنا ان ندرج اهم الخصائص المميزة للمرتزقة السيبرانيين في الفقرات الاتية تباعاً :

أولاً / تتمثل الخاصية الأولى من الخصائص المميزة للمرتزقة السيبرانيين في امتلاكهم للمهارة والخبرة العالية في مجال الانترنيت التي يتمكنون من خلالها من توفير البنى التحتية للاتصالات والمعلومات التي تضمن التفوق التقني والعسكري عند الدفاع او شن الهجمات السيبرانية في حالات النزاع المسلح او في وقت السلم لغرض اثارة العنف الذي يؤدي الى التدخل في الشؤون الداخلية او تهديد السلامة الإقليمية والاستقلال السياسي للدولة المستهدفة[٢].

فالحصول على معلومات مهمة يؤدي تسريبها الى الاضرار بالدولة ، او بث معلومات مضللة تهدف الى زعزعة الثقة بالحكومة والنظام السياسي ، او استهداف البنى التحتية والخدمات الضرورية للمواطنين او التدخل في التعبير عن حقهم في تقرير المصير كما في التدخل بالانتخابات ، كل ذلك يمكن ان يندرج تحت مفهوم اعمال العنف التي تؤدي الى التدخل في الشؤون الداخلية والمساس بالاستقلال السياسي والإقليمي للدولة المستهدفة [٣].

(١) ومن الجدير بالملاحظة ان المرتزقة السيبرانيين يمكن ان يقدموا خدماتهم وقت النزاعات المسلحة ووقت السلم ويمكن تميزهم عن قراصنة الانترنت من خلال كون الفئة الاخيرة غالبا ما تكون من الهواة لا يتصفون بنفس القدر من الحرفية التي يتمتع بها المرتزقة السيبرانيين وبانهم يعملون في الغالب بشكل منفرد او بمجموعات صغيرة ونادرا ما ينفذون اعمالا بالوكالة عن الدول بعكس المرتزقة السيبرانيين الذين يرتبطون دائما بدول يعملون على تنفيذ اعمال وكالة عنها ، كما ان اغلب الاعمال التي يقوم بها قراصنة الانترنت لا يمكن ان ترتقي الى مستوى الهجوم فهي لا تعدو عن اختراق لشركة او سرقة بيانات شخص او موقع الكتروني بعكس الحال مع المرتزق السبراني ، واخيرا فأن قراصنة الانترنت لا يسعون دائما الى الكسب المادي بعكس المرتزقة السيبرانيين الذين يكون هدفهم الاساس هو الكسب المادي . يراجع
Tim Maurer ,Cyber mercenaries , First published , Cambridge University Press, 2018.

(2) Ori Swed and Daniel Burland , Cyber Mercenaries: Review of the Cyber and Intelligence PMSC Market , A report for The Working Group on the use of mercenaries as a means of violating human rights and impeding the exercise of the rights of peoples to self-determination , (2021) , p.p. 6-8 .

(3) Ibid.p.p. 6-8 .

ثانياً / لا يشترك المرتزقة السيبرانيين بشكل مادي في النزاع المسلح ، وانما يباشرون القتال من خلال ما يقومون به من اعمال بواسطة الفضاء السيبراني اذا استوفت هذه الاعمال المعايير المطلوبة في الهجوم المسلح او اعمال العنف[١] .

ثالثا / ان الهدف الأساس الذي يصبو اليه المرتزق سواء كان المرتزق التقليدي ام المرتزق السيبراني يتمثل في تحقيق مكاسب خاصة غالباً ما تكون مكاسب مادية و ان استخدام الدول للمرتزقة السيبرانيين يعد خياراً اقتصادياً جيد لكون هؤلاء المرتزقة يطورون خبراتهم بشكل مستمر وبوتيرة سريعة وبتكلفة اقل تعجز المؤسسات التابعة للدولة عن القيام بها[٢].

رابعاً / صعوبة تحديد هوية المرتزق السيبراني سواء كان فرد ام مجموعة افراد وذلك بسبب عامل المهارة التقنية التي يمتلكها هؤلاء المرتزقة والتي يستطيعون من خلالها مسح جميع الاثار الناتجة عن قيامهم بأعمالهم في الفضاء السيبراني ، ما يجعل ذلك يمثل عقبه في طريق القاء القبض عليهم ومعاقبتهم قانوناً [٣].

خامساً / يوفر استخدام المرتزقة السيبرانيين قابلية للإنكار المعقول للدولة ، اذ حتى في حالة تحديد هوية المرتزق فانه يصعب ربط هؤلاء المرتزقة بالدولة المستخدمة لهم ، مما يمثل

---

(١) اللجنة الدولية للصليب الأحمر، "الحرب السيبرانية والقانون الدولي الإنساني "، مقال منشور على الموقع الالكتروني :
https://www.icrc.org/ar/document/%D8%A7%D9%84%D8%AD%D8%B1%D8%A8-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%88%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A
وللمزيد ينظر:
Russell Gilchrest , THE INVOLVEMENT OF MERCENARIES AND PRIVATE MILITARY SECURITY COMPANIES IN ARMED CONFLICTS: WHAT DOES IHL SAY? , Available at :
https://www.geneva-academy.ch/news/detail/482-the-involvement-of-mercenaries-and-private-military-security-companies-in-armed-conflicts-what-does-ihl-say
Miles Kenyon , Citizen Lab Response to the U. N. Working Group on the Use of Mercenaries , February 18, 2021 , Available at :
https://citizenlab.ca/2021/02/citizen-lab-response-to-the-u-n-working-group-on-the-use-of-mercenaries/
(2) Tim Maurer , Cyber proxies and their implications for liberal democracies , The Washington Quarterly Journal , Vol (41) , No (2) , 2018 , p. 173 .
(3) Ataa Dabour , The Rise of Cyber-mercenaries , 15 May, 2021 , p. 2 , Available at : http://www.hscentre.org/technology/the-rise-of-cyber-mercenaries/

حافزاً يشجع الدول للجوء الى استخدام هؤلاء المرتزقة وخاصة في غير حالات النزاع المسلح عندما لا ترغب الدولة بالدخول في نزاع مباشر [١] .

سادساً / اسوة بالمرتزق التقليدي ، لا يعتبر المرتزق السيبراني مقاتلاً عن احد اطراف النزاع ولا يحظى بالحماية القانونية التي يوفرها القانون الدولي الإنساني لأسير الحرب [٢] .

II. المبحث الثاني

تطبيقات استخدام المرتزقة السيبرانيين

تتراوح أنشطة المرتزقة السيبرانيين بين مهام الدفاع ضد الهجمات السيبرانية والحرب الالكترونية والمبادرة بشن الهجمات الالكترونية التي تتضمن الاضرار والتخريب والتجسس واستهداف البنى التحتية العسكرية والمدنية ونشر المعلومات المضللة لإضعاف قدرات العدو ، ويمكن ان نلاحظ ممارسة هذه النشاطات في وقت النزاع المسلح والسلم على السواء [٣] .

وعليه سنتناول هذا المبحث في مطلبين نخصص الأول لتطبيقات استخدام المرتزقة السيبرانيين في أوقات النزاع المسلح ، وندرس في الفرع الثاني تطبيقات استخدام المرتزقة السيبرانيين وقت السلم .

II.أ. المطلب الأول

تطبيقات استخدام المرتزقة السيبرانيين في أوقات النزاع المسلح

أصبحت الهجمات الالكترونية جزء مهم في النزاعات المسلحة الحديثة ، اذ نجد الى جانب الهجمات العسكرية التي تشن على الأرض وجود هجمات الكترونية تشن بواسطة الفضاء السيبراني ، وهذا ما يصطلح عليه حالياً (بالحرب الهجينية)[٤] ، ويتجلى ذلك في الحرب التي تدور رحاها حالياً بين روسيا وأوكرانيا .

---

(1) Syed Hamza Mannan , Projecting Power: How States Use Proxies in Cyberspace , Journal of National Security Law & Policy ,Vol (10) , (2019) , p. 448

(2) See : Michael N. Schmitt ed. , Tallinn manual 2.0 on the international law applicable to cyber operations , Cambridge University Press, 2017 , p.p . 412-413 .

(٣) تقرير الفريق العامل المعني بمسألة استخدام المرتزقة وسيلة لانتهاك حقوق الانسان وإعاقة ممارسة حق الشعوب في تقرير مصيرها ، المصدر السابق ، ص ٧ .

(٤) يعد بيل نميث ، أول من استخدم هذا المصطلح في تسعينيات القرن العشرين حيث عرفها بانها " :نموذج عصري لحرب العصابات حيث يستعمل الثوار التكنولوجيا الحديثة، والوسائل المتطورة لحشد الدعم المعنوي والشعبي" .يراجع

W. J. Nemeth, “ Future War and Chechnya: A Case for Hybrid Warfare”, Thesis, California :(Naval Postgraduate School) , June 2002, Available at http://calhoun.nps.edu/bitstream/handle/10945/5865/02Jun_Nemeth.pdf?sequence=1Accessed 17th Oct 2017.

أسماء حداد ، الحروب الهجينة، "الأزمة الأوكرانية أنموذجا" ، *مجلة مدارات سياسية* ، *الجزائر* ، عدد ديسمبر ٢٠١٧ ، ص ١١٤-١٢٩ .

فنجد بان هذا النوع من الحروب هي السائدة بين طرفي النزاع ، حيث شهد الفضاء السيبراني هجمات الكترونية شنها طرفي النزاع بواسطة الأجهزة الحكومية تارة او بواسطة المرتزقة السيبرانيين او المتطوعين كما يطلق عليهم تارة أخرى [١] .

وقبل ان ننخرط بالدخول في صلب الموضوع يتبادر الينا سؤال مهم جداً تمت مناقشته بشكل كثيف على الصعيد الفقهي والدولي ويتمثل في ، هل ان الهجمات الالكترونية التي تشن في الفضاء السيبراني يمكن ان ترقى الى ان تكون هجوما مسلح ؟ [٢] .

و تعرف المادة (٤٩) من البروتوكول الإضافي الأول الهجمات بانها " اعمال العنف الهجومية والدفاعية ضد الخصم " ، اما الهجمات الالكترونية فيعرفها دليل تالين المنطبق على العمليات الالكترونية بانها " العمليات الالكترونية سواء كانت هجومية او دفاعية ، من المتوقع بشكل معقول ان تسبب إصابة او وفاة للأشخاص او تلف او تدمير للأشياء"[٣] .

واضح مما تقدم بان أي هجوم الكتروني تنشأ عنه إصابة او موت للأشخاص او تلف او تدمير للأشياء يستوفِ معيار الهجوم المسلح ، فالعبرة اذاً بالأثار المترتبة على الهجوم لا بالوسيلة التي تم بها سواء كانت مادية او الكترونية طالما أدت الى ذات الأثر [٤] ، وقد اكد ذلك اللجنة الدولية للصليب الأحمر حيث ذهبت الى (العمليات التي تهدف الى تعطيل عين ما – حاسوب او شبكة حاسوبية – تشكل هجوماً بموجب القواعد بشأن إدارة العمليات العدائية ، سواء جرى تعطيل العين بوسائل حركية ام سيبرانية) [٥] .

---

(1) Russia-Ukraine conflict: What role do cyberattacks play? , article published on the site :
https://www.dw.com/en/russia-ukraine-conflict-what-role-do-cyberattacks-play/a-60945572

(2) Heather Harrison Dinniss , UKRAINE SYMPOSIUM – MILITARY NETWORKS AND CYBER OPERATIONS IN THE WAR IN UKRAINE , Apr 29, 2022 , Available at :
https://lieber.westpoint.edu/military-networks-cyber-operations-war-ukraine/

(٣) القاعدة (٩٢)، من دليل تالين (٢,٠)، بشأن القواعد الدولية المنطبقة على العمليات السيبرانية ، ينظر Michael N. Schmitt ed. , Op.cit, p. 417 .

(4) Ib.id , p.p. 417-418 .

(5)The Red Cross , Report International humanitarian law and the challenges of contemporary armed conflicts , 32nd International Conference of the Red Cross and Red Crescent , Geneva, 8-10 December 2015 , p. 41 .

كما ينظر الى موقف منظمة حلف شمالي الاطلسي (الناتو) الذي يعتبر بأن الهجمات الالكترونية قد تؤدي الى تطبيق المادة (٥) من النظام الاساسي للمنظمة ، والخاصة بتفعيل الدفاع المسلح الجماعي للدول الاطراف في الحلف في حالة وقوع هجوم عسكري على احدى الدول الاطراف . ينظر :
Michaela Prucková , Cyber attacks and Article 5 – a note on a blurry but consistent position of NATO , Last visited on 29/8/2023 , Available at :
https://ccdcoe.org/library/publications/cyber-attacks-and-article-5-a-note-on-a-blurry-but-consistent-position-of-nato/

واثناء فترات النزاع المسلح تأخذ هجمات المرتزقة السيبرانيين احد الاشكال الاتية :

أولا / هجمات المسح:

وقد استخدم المرتزقة السيبرانيين في العديد من الهجمات التي شنوها أدوات الكترونية ينتج عنها مسح واتلاف البيانات والمعلومات المخزنة على الأجهزة الالكترونية ، وقد يكون هذا الاستخدام سابقاً او مرافقاً هجمات العسكرية على الأرض بغية دعمها وانجاحها [١] ، ففي اليوم الأول للهجوم العسكري الروسي على أوكرانيا الموافق ٢٠٢٢/٢/٢٤ أدى هجوم الكتروني الى تعطيل القمر الاصطناعي Viasat (KA-SAT) ، الذي يزود الوحدات العسكرية الأوكرانية بخدمات الانترنت والاتصالات ، وتستفاد دول اوربية أخرى منه في التزود بالانترنت ، كما استهدف الهجوم الالكتروني أيضاً محطات السكك الحديدية التي تستخدمها أوكرانيا في نقل الامدادات والأشخاص العسكرين ونقل المدنيين في ذات الوقت ، الا ان الهجوم الأخير كان اقل ضررا بسبب تدخل الولايات المتحدة الامريكية للتصدي للهجوم[٢]، وتعرضت أيضاً كل من شركتي (Triolan) المجهزة لخدمات الانترنت وشركة (Ukrtelecom) الخاصة بالاتصالات لهجمات الكترونية في شهر اذار / مارس من عام ٢٠٢٢ ، مما أدى الى تعطيل واضعاف الخدمات التي تقدمها كلتا الشركتين [٣] .

ثانيا / هجمات الاغلاق والحرمان من الخدمة (Shut down and denial of service attacks (DDOS) :

شن مجموعة من المرتزقة السيبرانيين بالإضافة الى بعض الجهات الذين يشتبه بارتباطهم بالحكومة الروسية ، قبل الهجوم المسلح على أوكرانيا بأيام قليلة تمهيداً للهجوم العسكري هجمات الكترونية باستخدام أدوات تؤدي الى اغلاق وتعطيل الشبكات والمواقع

---

(١) و مثال هذه الادوات (HermeticWiper , AcidRain , DoubleZero , CaddyWiper) ينظر:
Pawel Knapczyk , Overview of the Cyber Weapons Used in the Ukraine - Russia War , Aug 18, 2022 , Available at :
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war/

(2) Nadiya Kostyuk and Erik Gartzke , Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine , Texas National Security Review , Vol (5) , No (3) , 2022 , p, 120 .

وينظر ايضاً :

David Cattler and Daniel Black , The Myth of the Missing Cyberwar Russia's Hacking Succeeded in Ukraine—And Poses a Threat Elsewhere Too , April 6, 2022 , Available at :
https://www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberwar?check_logged_in=1

(3) Jon Bateman , Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences and Implications , WORKING PAPER Carnegie Endowment for International Peace , 2022 , p , 10 .

الالكترونية والبنى التحتية الخاصة بالطاقة[١]، بهدف بث الاضطراب وعدم اليقين بين المواطنين لتعطيل وصولهم للمعلومات والخدمات التي تزودهم بها عادة الحكومة الأوكرانية[٢].

وقامت مجموعة من المرتزقة السيبرانيين تدعى ب(Fancy Bear) التي يشتبه بعلاقتها مع أجهزة الاستخبارات الروسية عند بداية اندلاع النزاع المسلح باختراق احد التطبيقات التي يستعين بها جنود المدفعية الاوكرانيين لتسهيل استخدامهم للمدفعية من طراز (D-30) ، وتمكنوا من تحديد مواقع مستخدمي هذا التطبيق واستهدافهم بدقة مما أدى الى وقوع خسارة كبيرة في هذا النوع من المدفعية [٣] .

وبمقابل الهجمات المذكورة في الفقرتين أعلاه أعلنت أوكرانيا بشكل صريح عن تشكيل جيش الكتروني تكون العضوية فيه مفتوحة لأي شخص ، وركزت في هذا الإعلان على ان الجيش سيمثل جيشاً من المتطوعين الذين يعملون دون مقابل يقدم لخدماتهم [٤] ، وبالفعل شن افراد هذا الجيش عمليات الكترونية دفاعية وهجومية ضد روسيا وحلفائها ، حيث هاجم هذا الجيش على سبيل المثال نظام سكك الحديد البيلاروسي الذي تستخدمه روسيا في نقل الامدادات والجنود بالإضافة الى وظيفته المدينة ، كما ساهم هذا الجيش بالعديد من عمليات الاختراق ومهاجمة البنى التحتية والمواقع الحكومة الروسية [٥] .

---

(١) و مثال هذه الادوات (DDOS) و (Industroyer , Industroyer2) الخاصة بأستهداف منشأت الطاقة . ينظر الموقع الالكتروني الخاص بشركة (Microsoft) الذي يحتوي على قاعدة بيانات مفصلة لهذه الادوات

https://www.microsoft.com/en-us/security/business/security-101/what-is-a-ddos-attack

(2)Cyber Peace Institute , Ukraine Conflict: Cyberattacks, Frequently Asked Questions , June 16, 2022 , Available at :
https://cyberpeaceinstitute.org/news/ukraine-conflict-cyberattacks-frequently-asked-questions/

(3) Crowdstrike Global Intelligence Team , Use of Fancy Bear Android Malware in Tracking of Ukrainian Field Artillery Units , Report Published December 22 , 2016 , p.p 1-10 .

(٤) وذلك بمحاولة واضحة لأبعاد افراد هذا الجيش الالكتروني الذي يتألف من (٣٠٠٠٠٠) شخص غالبيتهم من الاجانب ، من الوقوع تحت طائلة النصوص الدولية والوطنية الخاصة بالمرتزقة . ينظر :

Kristen E. Eichensehr , Ukraine cyberattacks and the lessons for international law , American Journal of International Law , Vol (116) , 2022 , p , 149.

(٥) وفي هذا الصدد ينظر البيان الرسمي لوزارة الخارجية الروسية الذي نص على (لاول مرة تعلن دولة عضو في الامم المتحدة بشكل علني عن عدوان الكتروني و حرب الكترونية ..) في اشارة واضحة الى ان هذه الحرب تشن بواسطة مرتزقة سيبرانيين . يراجع الموقع الرسمي لوزارة الخارجية الروسية على الرابط :
https://mid.ru/en/foreign_policy/news/1806906/

ويذهب البعض الى ان الهجمات الالكترونية أصبحت أداة لا بد منها في النزاعات المسلحة الحديثة ، سواء كانت هذه الهجمات تشن من قبل الدول ام من قبل المرتزقة السيبرانيين الذين يعملون لحسابها ، ويدللون بذلك على النجاح الكبير للهجمات الالكترونية التي رافقت الهجمات المسلحة للقوات الروسية ، اذ أدت هذه الهجمات الى ارباك وارهاق القوات الأوكرانية خاصة في الفترة الأولى من النزاع المسلح [١] .

II.ب. المطلب الثاني

تطبيقات استخدام المرتزقة السيبرانيين وقت السلم

يتبين بشكل واضح أنشطة المرتزقة السيبرانيين وقت السلم في الفقرتين ادناه:

أولا / التجسس وجمع المعلومات :

يعد التجسس من الأنشطة المهمة للدول والتي تمكنها من الحصول على معلومات اكثر عن اعدائها وتحدد أهدافها الحيوية والاستراتيجية ، وبقدر ما يمثله هذا الامر من أهمية وقت النزاع المسلح من خلال معرفة المعلومات والخطط والعلم بمواقع العدو وتحركاته الخ ، فان أهميتها لا تقل أهمية عنها في وقت السلم ، اذا اثبتت النزاعات الدولية الحديثة كالنزاع الروسي الاوكراني الذي اشتعل فتيله ابتداءً من عام ٢٠١٤ وتطور ليصل الى حد النزاع العسكري المسلح ، ان للتجسس في وقت السلم اثره الكبير حيث نجد بان اكثر الهجمات الالكترونية اثراً ونجاحاً حدثت بهدف التجسس وجمع المعلومات في وقت السلم [٢] ، ويمكن ملاحظة التجسس في وقت السلم بشكل واضح من خلال ما يقوم به المرتزقة السيبرانيين في الأمثلة الاتية :

أ / مشروع (Raven) الذي أنشئ عام ٢٠٠٩ من قبل دولة الامارات العربية المتحدة ، والذي ضم مجموعة من محترفي الانترنيت من جنسيات اجنبية متعددة يتقدمهم افراد أمريكيين كانوا يعملون سابقاً في أجهزة الاستخبارات ، والذين استخدموا أدوات متطورة لاختراق الأجهزة الالكترونية والتجسس على محتوياتها من اجل الحصول على المعلومات والبيانات الموجودة عليها وتحديد اماكن وجود مستخدميها ، و اثبت هذا المشروع نجاحه عند استخدامه ضد النشطاء في ميدان حقوق الانسان والميدان السياسي سواء كانوا افراد او دول [٣] .

---

(1) Jon Bateman , Op.cit, p. 5 .

(2) James A. Lewis , Cyber War and Ukraine , Center for Strategic & International Studies Report , Published June 16, 2022 , p.p. 1-3 . Available at : https://www.csis.org/analysis/cyber-war-and-ukraine

(٣) استطاع الافراد العاملين بهذا المشروع اختراق الأجهزة الالكترونية لعدد من الشخصيات المهمة مثل امير قطر الحالي الشيخ (تميم بن حمد ال ثاني) ورئيس تحرير صحيفة العربية (عبد الله العتبا) ورئيس قناة الجزيرة الشيخ (حمد بن ثامر بن محمد ال ثاني) . ينظر :

Jose de Arimateia da Cruz and Pedron Stephanie , op.cit , p, 14 .

وكذلك تعمل شركة (Dark Matter) التي تأسست في الامارات العربية المتحدة عام ٢٠١٤ ، على القيام بذات الخدمات التي يقدمها المشروع أعلاه ، وتتألف من افراد أجانب محترفين في المجال السيبراني ويتقاضون مقابلا عالياً للخدمات التي يقدمونها [١] .

ب/ باعت شركة (NSO Group Technologies) الإسرائيلية خدماتها المتمثلة بأداة الاختراق المعروفة بـ(Pegasus) الى عدد من الحكومات ، منها الحكومة المكسيكية التي استخدمتها في البداية بحجة تتبع المجرمين وتجار المخدرات لكن سرعان ما اتضح بان خدمات هذه الشركة كانت موجهه بالأساس لمتابعة معارضين الحكومة السياسيين والصحفيين والناشطين في مجال حقوق الانسان ، كما اشترت خدمات الشركة المذكورة حكومات اخرها منها المملكة العربية السعودية أيضاً [٢] .

ج/ القى مكتب التحقيقات الفدرالي التابع للولايات المتحدة الامريكية في عام ٢٠٢٠ على عدد من المرتزقة السيبرانيين وذلك لقيامهم بأنشطة تجسس وجمع معلومات تستهدف شركات الادوية العاملة على تصنيع لقاح فايروس (Covid-19) ، كما استهدفوا قطاعات أخرى كقطاع التكنلوجيا ، ويعد ما تقدم سابقة مهمة اذ ان هؤلاء المرتزقة السيبرانيين لم يتم تحديدهم فقط وانما اتهموا بالعمل لصالح دولة معينة وبمقابل اجر [٣] .

---

(1) WOMEN'S INTERNATIONAL LEAGUE FOR PEACE AND FREEDOM , Report SUBMISSION TO THE UN WORKING GROUP ON THE USE OF MERCENARIES REGARDING "CYBER MERCENARIES" AND THEIR HUMAN RIGHTS IMPACT , FEBRUARY 2021 , p, 11. Available at : https://www.reachingcriticalwill.org/news/latest-news/15209-wilpf-submits-views-on-cyber-mercenaries-and-human-rights

(٢) للمزيد من انشطة المرتزقة السيبرانيين التجسسية يراجع الموقع الالكتروني الخاص بمؤسسة (citizenlab) التابعة لجامعة تورنتو والمتخصصة بالكشف عن حالات التجسس الرقمي ضد المجتمع المدني وغيرها من التقنيات والممارسات التي تؤثر على حرية التعبير عبر الإنترنت ، وكشف اشخاص المرتزقة السيبرانيين القائمين بها وارتباطاتهم الدولية . ينظر :

https://citizenlab.ca/

ومما يجدر ذكره بأن إسرائيل بسجلها المعروف بانتهاكات حقوق الانسان تملك العديد من الشركات المتقدمة في ميدان المراقبة وتوفير خدمات التجسس وتحديد المواقع في الفضاء السيبراني ، لتفاصيل اكثر عن هذه الشركات ونشاطاتها ينظر :

Patrick Howell O'Neill , An internal investigation shows private-sector mass surveillance is happening on a scale never before revealed , December 16, 2021 , Available at : https://www.technologyreview.com/2021/12/16/1042652/facebook-says-50000-users-were-targeted-by-cyber-mercenary-firms-in-2021/

(3) Josephine Helen Dwan and Others , Pirates of the cyber seas: Are state-sponsored hackers modern-day privateers?, Law, Technology and Humans Journal , Vol (4) , No (1) , 2022 , p, 50 .

ويظهر مما تقدم بان أنشطة المرتزقة السيبرانيين في مجال التجسس وجمع المعلومات هي في ازدياد مضطرد ، ويدل على ذلك توجه العديد من الشركات ورؤوس الأموال التي تصرف لشراء خدمات هؤلاء المرتزقة ، وان ذلك يُنبئ بمؤشر خطير لانتهاك حقوق الانسان وخاصة الحق بالخصوصية الشخصية وحرية التعبير عن الراي في مجال الانترنيت [١] .

ثانيا / التخريب (sabotaging) :

وتتجلى أنشطة المرتزقة السيبرانيين في هذا المجال من خلال الأمثلة الاتية :

أ / شنت مجموعة من المرتزقة السيبرانيين الذين يشتبه بعلاقتها بروسيا هجمات الكترونية في عامي ٢٠١٥-٢٠١٦ على مرافق الطاقة الكهربائية في أوكرانيا ، مما أدى الى تعطيلها عن تقديم خدماتها للمواطنين لعدة أيام [٢] .

ب / في وقت سابق للهجوم العسكري المسلح لروسيا على أوكرانيا تعرض ما يقرب من ٥٠٠٠ توربينه رياح موجودة في المانيا تعمل لتوليد الطاقة الكهربائية الى التوقف التام نتيجة استهدافها بهجوم الكتروني [٣] .

ج / تعمل المجموعة التي يطلق عليها (Atlas Intelligence Group) او (Atlas Cyber-Army) كمرتزقة سيبراني ، حيث تم رصدها من خلال ما تقوم به من أنشطة يتمثل أهمها بهجمات الكترونية تخريبية باستخدام تقنية الـ(DDOS) التي تهدف من خلالها الى اغلاق المواقف وشبكات الاتصالات نظير مقابل مادي لهذه الخدمات [٤] .

ونخلص مما تقدم الى انه بالرغم من الاتفاق على انطباق قواعد القانون الدولي الإنساني على أنشطة المرتزقة السيبرانيين المرتكبة اثناء النزاع المسلح ، الا ان ذلك لا يعني بأن انشطتهم وقت السلم تبقى دون الخضوع لقواعد قانونية تحضرها اذ تظل هذه الانشطة خاضعة لقواعد القانون الدولي لحقوق الانسان والتشريعات المحلية التي تجرم هذه الأنشطة [٥].

---

(١) قرار الجمعية العامة للامم المتحدة ، الحق بالخصوصية بالعصر الرقمي ، ٢٠١٣ ، الوثيقة A/C.3/68/L.45/Rev.1 .

(٢) نيري زيلبر ، ظهور المرتزقة في المجال السيبراني ، ١ سبتمبر ٢٠١٨ ، مقال منشور على الموقع الرسمي لمعهد واشنطن لسياسة الشرق الأدنى ، متاح على الرابط :
https://www.washingtoninstitute.org/ar/policy-analysis/zhwr-almrtzqt-fy-almjal-alsybrany

(3) KENNETH R. ROSEN , The Man at the Center of the New Cyber World War , article published Politico Magazine , 2022 , Available at :
https://www.politico.com/news/magazine/2022/07/14/russia-cyberattacks-ukraine-cybersecurity-00045486

(4) Elizabeth Montalbano , Hackers for Hire: Adversaries Employ 'Cyber Mercenaries' , Article published in July 21/ 2022 , Available at :
https://threatpost.com/hackers-cyber-mercenaries/180263/

(٥) ينظر في ذات المعنى :

Ataa Dabour , op.cit .

III. المبحث الثالث

طبيعة العلاقة المنشئة للمسؤولية الدولية المترتبة عن استخدام المرتزقة السيبرانيين

يشكل استخدام المرتزقة السيبرانيين تحدياً كبيراً في مجال تحديد المسؤولية الدولية ، وذلك لكون استخدام هذه الفئة من المرتزقة يزيد من إمكانية الاستفادة من الانكار المعقول ويؤدي ذلك الى تعقيد مضاف لما هو عليه الحال في ميدان اسناد المسؤولية الدولية في الفضاء السيبراني ، لذلك سنتناول هذا المبحث في مطلبين نخصص الأول لطبيعة العلاقة التي تربط المرتزقة السيبرانيين مع الدول التي يعملون لصالحها ، وندرس في المطلب الثاني المسؤولية الدولية المترتبة عن استخدام المرتزقة للسيبرانيين .

III.أ. المطلب الأول

طبيعة العلاقة بين المرتزقة السيبرانيين والدولة التي يعملون لصالحها

لا تظهر بوضوح طبيعة العلاقة التي تربط المرتزقة السيبرانيين بالدولة ، اذ نجدها متباينة بحسب طبيعة الدولة و أيدولوجيتها السياسية والاقتصادية ، حيث يمكن ان نجدها بصورة عقد او تفويض تام يمنح للمرتزقة السيبرانيين يتمتعون بموجبه بمساحة واسعة من الحرية عند القيام بأنشطتهم فهم لا يخضعون لأشراف الدولة ولكن يعملون لتحقيق هدف محدد لهم مسبقا من قبلها [١] .

اما الصورة الثانية للعلاقة فتكون بعكس الصورة الأولى اذ يرتبط المرتزقة السيبرانيين بأجهزة الدولة ويخضعون لسيطرتها ومراقبتها الفعليين [٢] ، وتشكل الصورة الأخيرة للعلاقة في اغفال وغض طرف الدولة عن نشاط المرتزقة السيبرانيين الذي يتم على

---

(١) يمكن لهذه الصورة من صور العلاقة ان تتسم بالخطورة العالية في ميدان التطبيق على ارض الواقع فيمكن ان يتحول هؤلاء المرتزقة ضد الدولة التي يعملون لصالحها فحذر ميكيافيللي منذ وقت طور من خطورة الاعتماد على المرتزقة بالقول (ان المرتزقة عديموا الفائدة وخطرون في آن واحد ، ومن يمسك بدولته بواسطة قوات المرتزقة لا يمكن ابدا ان يجلس بصلابة او امان) . ينظر :
ميكيافيللي ،*كتاب الامير* ، ترجمة اكرم مؤمن ، (القاهرة: مكتبة ابن سينا للطبع والنشر ، ٢٠٠٤)، ص٦٦.
ويؤكد وجهة النظر هذه ما قام به مرتزقة فاغنر (Wagner) من محاولة فاشلة للتمرد على الحكومة الروسية بتأريخ ٢٠٢٣/٦/٢٣ . ينظر بيان وزارة الدفاع الروسية على الموقع الالكتروني الرسمي للوزارة على الرابط الاتي :
https://eng.mil.ru/en/news_page/country/more.htm?id=12471264@egNews

(٢) ان هذه الصورة من صور العلاقة بالرغم من تجاوزها لمساوئ الصورة الاولى الا انها تجعل المرتزقة السيبرانيين يصبحون اشبه بجهاز تابع للدولة مما يؤدي الى تضييع الدولة لاهم ميزة تستفيد منها عند استخدامها لهؤلاء المرتزقة والمتمثلة بالانكار المعقول ، اضافة الى ان الاشراف على هؤلاء المرتزقة ومتابعتهم يحتاج الى تقنيات وامكانيات لا تمتلكها الى القليل من الدول المتطورة في مجال التكنولوجيا . ينظر:
Tim Maurer, Proxies and Cyberspace , Journal of conflict and security law , Vol (21) , No (3) , 2016 , p.p.393-396.

أراضيها او بواسطة بنيتها التحتية للاتصالات والانترنت وعدم ايقافها للنشاط المذكور بعد علمها به مع امتلاكها القدرة على ذلك [١] .

ومن خلال دراستنا لموضوع البحث وما اوردناه من صور لاستخدام المرتزقة السيبرانيين نجد تبايناً واضحاً في صور العلاقة التي يرتبط بها هؤلاء المرتزقة فالدولة تقيم علاقتها مع هؤلاء المرتزقة وفقاً للصورة التي تلائمها ، لكن غالباً ما تسعى الدول الى الاستفادة من ميزة الانكار المعقول في علاقتها مع هؤلاء المرتزقة اذ انها دوماً تسعى الى استغلال هؤلاء المرتزقة كستار يحجب هوية وصورة تدخلها في الاعمال الصادرة من المرتزقة والموجهة الى دول أخرى او الى الغير في الفضاء السيبراني ، و بالرغم من الاستفادة من هذه الميزة الا انه لا يمكن التعويل عليها في كل الأحوال اذ ان التطور التكنولوجي السريع قد مكن في بعض الحالات من تحديد هوية هؤلاء المرتزقة والدول التي يعملون لحسابها [٢] .

ان ميزة الانكار المعقول يمكن ان تكون غير ذات جدوى اذا كان الهجوم الالكتروني موجه الى احدى الدول المتطورة تكنولوجيا ، الا انها تبقى تمثل ميزة ذات قيمه عالية حاليا خاصة اذا كانت الدولة القائمة بالهجوم السيبراني او المرتزقة السيبرانيين الذين يعملون لحسابها من المحترفين في هذا المجال مما يمكنهم من إخفاء اثار هجماتهم وبالتالي تحديد هويتهم واسناد أعمالهم للدولة التي يعملون لحسابها .

III.ب. المطلب الثاني

المسؤولية الدولية المترتبة على استخدام المرتزقة السيبرانيين

لتحقق المسؤولية الدولية للدولة ينبغي توافر شروطها ، ويعد الاسناد احد اعقد هذه الشروط وأكثرها اثارة للجدل في ما يتعلق بالأنشطة السيبرانية فهل تُنسب الأنشطة التي يقوم بها المرتزقة السيبرانيين والمتمثلة بالهجمات الالكترونية والعنف المرتكب في الفضاء السيبراني وغيرها من الأفعال غير المشروعة الى الدولة ام انه يصعب اثبات العلاقة بين هؤلاء المرتزقة والدولة وبالتالي يسقط احد الاركان المهمة لتحقيق المسؤولية الدولية ؟

يتطلب القانون الدولي في وضعه الحالي عتبة عالية لتحقيق مسؤولية الدولة عن العاملين بالوكالة عنها ، وتتمثل هذه العتبة بمعيار (السيطرة الفعلية)[٣] ، المتضمن ضرورة

(1) Tim Maurer ,Cyber mercenaries , First published , Cambridge University Press, 2018 , p.p. 47-48 .

(2) Samantha V. Feuer , From the Shadows to the Front Page: State Use of Proxies for Cyber Operations , A Thesis Submitted To The Freeman Spogli Institute for International Studies , Stanford University , 2020 , p, 83 .

(3) Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, I.C.J. Reports 1986, , par. 115 , p, 54 .

ان تكون الدولة مسيطرة فعلياً على نشاط وكلائها (في حالتنا هذه المرتزقة السيبرانيين) لكي تتحقق مسؤوليتها عن ما يصدر عنهم من أفعال ، ويعد ذلك بحق عتبة عالية على صعيد الهجمات الالكترونية [١] .

كما تظهر في حالة اخر عند قيام المرتزقة السيبرانيين بأنشطتهم على أراضي الدولة ويستخدمون بنيتها التحتية للاتصالات والانترنيت ، فهل تنعقد مسؤولية الدولة عن الانشطة المذكورة ؟ [٢] .

يذهب اتجاه تؤيده السوابق القضائية الدولية يتمثل في ان الدولة ينبغي عليها بذل العناية الواجبة في الفضاء السيبراني من خلال عدم السماح باستخدام بنيتها التحتية للاتصالات والانترنت للإضرار بغيرها من الدول وإيقاف ذلك حال علمها به [٣] .

وهنا من الضروري ان نميز بين الاسناد كركن قانوني رئيسي لتحقق مسؤولية الدولة وبين نسبة الفعل الى دولة معينة كمسالة ذات طابع سياسي (الاسناد السياسي) ، اذ ان اغلب الهجمات الالكترونية تم نسبتها الى دول معينة بذاتها ، لكن لم يتم اسناد هذه الهجمات بشكل قانوني اليها ، والامثلة هنا كثيرة ننتخب منها حالة الهجمات الالكترونية التي استهدفت التدخل في الانتخابات الرئاسة في الولايات المتحدة الامريكية لعام ٢٠١٦ ، حيث نسبت هذه الهجمات الى روسيا ولكن لم يتم اسناد ما تقدم بشكل قانوني للدولة المذكورة ، واكتفت الولايات المتحدة بتوجيه اتهامات جنائية بحق عدد من الأشخاص [٤].

وبالتالي نرى في الوقت الحاضر من الصعب تحقق اسناد المسؤولية الدولية الى الدولة و يتوقف تحقق ذلك على تطور التقنيات التي تجعل اثبات علاقة الدولة بالمرتزقة السيبرانيين امر لا لبس فيه و بأدلة رقمية لا يمكن دحضها [٥] ، و يبقى من الممكن في حالة

---

(١) ينظر نص المادة (٨)، من مشروع المواد المتعلقة بمسؤولية الدول عن الافعال غير المشروعة دوليا لعام ٢٠٠١ التي تنص على (يعتبر فعلا صادرا عن الدولة بمقتضى القانون الدولي تصرف شخص او مجموعة اشخاص اذا كان الشخص او مجموعة الاشخاص يتصرفون في الواقع بناء على تعليمات تلك الدولة او بتوجيهات منها او تحت رقابتها لدى القيام بذلك التصرف) .

(2) Kosmas Pipyros et al , Cyberoperations and international humanitarian law: A review of obstacles in applying international law rules in cyber warfare , Information & Computer Security Journal ,Vol (24) ,No (1) , 2016 , p, 48 .

(٣) ينظر تقرير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية و اللاسلكية في سياق الامن الدولي ، الوثيقة (A/70/174) ، ٢٠١٥ ، الفقرة (ج) ، ص١١ .

كما ينظر: Corfu Channel case, Judgment of April gth, 1949 : I.C.J. Reports 1949, p.22

(4) Kristen Eichensehr , Cyberattack Attribution and International Law , Article published in July 24, 2020 , Available at : https://www.justsecurity.org/71640/cyberattack-attribution-and-international-law/

(5) Charles Clore House , State Responsibility for Cyber Operations: International Law Issues , British Institute of International and Comparative Law , Event Report , London , 9 October 2014 , p, 8 .

تحديد هوية هؤلاء المرتزقة محاسبتهم سواء كانوا افرادا ام جماعات [١] ، وتقديمهم الى المحاكمات [٢] ، ورفع الحصانة الممنوحة للمقاتلين اثناء النزاع المسلح عنهم [٣] ، ولا يتضمن ذلك من الناحية القانونية اسناد انشطتهم غير المشروعة الى دولة معينة [٤] .

الخاتمة

وفي ختام البحث نورد اهم الاستنتاجات والمقترحات التي توصلنا اليها ادناه :

أولاً : الاستنتاجات :

١ - ان الاتفاقيات الدولية التي تناولت موضوع المرتزقة كالبروتوكول الإضافي الأول لاتفاقيات جنيف الصادر عام ١٩٧٧ ، و اتفاقية منظمة الوحدة الافريقية للقضاء على الارتزاق في افريقيا لعام ١٩٧٧ ، والاتفاقية الدولية لمناهضة تجنيد المرتزقة واستخدامهم وتمويلهم وتدريبهم لعام ١٩٨٩ اتسمت جميعها بالنقص والقصور عند تحديدها لمفهوم المرتزق وذلك لكونها لم تشمل كل صور الارتزاق وخاصة الحديث منها ولكونها اخذت بالنهج التقليدي الذي أُسس بموجب المادة (٤٧) من البرتوكول الإضافي الأول .

٢- ان أي هجوم الكتروني تنشأ عنه إصابة او موت للأشخاص او تلف او تدمير للأشياء يستوفِ معيار الهجوم المسلح ، فالعبرة اذاً بالأثار المترتبة على الهجوم لا بالوسيلة التي تم بها سواء كانت مادية او الكترونية طالما أدت الى ذات الأثر .

٣- ان الهجمات الالكترونية أصبحت أداة لا بد منها في النزاعات المسلحة الحديثة ، سواء كانت هذه الهجمات تشن من قبل الدول ام من قبل المرتزقة السيبرانيين الذين يعملون لحسابها ، ويدل على ذلك النجاح الكبير للهجمات الالكترونية التي رافقت الهجمات المسلحة للقوات الروسية .

---

(١) ينظر الأمرين التنفيذيين الذين اصدرهما رئيس الولايات المتحدة الامريكية بالرقم ١٣٦٩٤، في ١ نيسان/أبريل ٢٠١٥ وبالرقم ١٣٦٩٤ في ٢٨ كانون الاول/ديسمبر ٢٠١٦ ، والخاصين بفرض جزاءات على الأفراد والكيانات المسؤولين عن بعض الأنشطة الخبيثة القائمة على الإنترنت أو المتواطئين معها. كما ينظر لائحة (الاتحاد الأوروبي) ٧٩٧/٢٠١٩ بشأن التدابير التقييدية ضد الهجمات السيبرانية التي تهدد الاتحاد أو الدول الأعضاء فيه .

(٢) ينظر الدعوى التي اقامتها شركة واتس اب (WhatsApp) ضد شركة (NSO) الاسرائيلية امام المحكمة العليا في الولايات المتحدة الامريكية .

Jonathon W. Penney and Bruce Schneier , Platforms, Encryption, and the CFAA: The Case of WhatsApp v. NSO Group , berkeley technology law journal , Vol (36) , 2021 , 101-142.

(٣) المادة (١/٤٧)، من البروتكول الاضافي الاول .

(4)The Federal German Government , On the Application of International Law in Cyberspace , Position Paper , March 2021 , Available at : https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf

٤- بالرغم من الاتفاق على انطباق قواعد القانون الدولي الإنساني على أنشطة المرتزقة السيبرانيين المرتكبة اثناء النزاع المسلح ، الا ان ذلك لا يعني بأن انشطتهم وقت السلم تبقى دون الخضوع لقواعد قانونية تحضرها اذ تظل هذه الانشطة خاضعة لقواعد القانون الدولي لحقوق الانسان والتشريعات المحلية التي تجرم هذه الأنشطة .

٥- من الصعب تحقق اسناد المسؤولية الدولية الى الدولة و يتوقف تحقق ذلك على تطور التقنيات التي تجعل اثبات علاقة الدولة بالمرتزقة السيبرانيين امر لا لبس فيه و بأدلة رقمية لا يمكن دحضها .

ثانياً : التوصيات :

وسنورد اهمها ادناه :

١- تعديل الاتفاقية الدولية لمناهضة تجنيد المرتزقة واستخدامهم وتمويلهم وتدريبهم لعام ١٩٨٩ ، لكي تأخذ بنظر الاعتبار الصور الجديدة للارتزاق التي يتقدمها المرتزقة السيبرانيين.

٢- ابرام اتفاقية دولية او وضع انظمة للتعاون الدولي الثنائي او الجماعي في ميدان التكنولوجيا والتقنيات التي تقود الى الكشف عن هؤلاء المرتزقة واسناد المسؤولية الى الدول التي يعملون لصالحها .

٣- تجريم استخدام المرتزقة السبرانيين وتجريم الانشطة التي يقومون بها في النظم القانونية الوطنية ، والقاء القبض عليهم ومحاسبتهم ، وذلك لسد الفراغ الحاصل على المستوى الدولي حالياً الذي لم يجرم هذه الصورة من صور الارتزاق الحديث .

٤- بذل الدول للعناية الواجبة المتمثلة بمراقبة بنيتها التحتية للاتصالات والانترنت ومنع استخدامها او استخدام اراضيها من قبل هؤلاء المرتزقة السيبرانيين او من قبل دول اخرى تسعى للأضرار بشخص او طرف اخر وايقاف هذه الافعال ومعاقبة مرتكبيها .

المصادر

أولاً : الكتب

١- ميكيافيللي، *كتاب الامير*، ترجمة اكرم مؤمن، مكتبة ابن سينا للطبع والنشر ، القاهرة ، ٢٠٠٤ .

ثانيا : البحوث والدوريات

١- د. حيدر كاظم عبد علي و مالك عباس جيثوم، "الأساس القانوني لتنظيم الارتزاق في القانون الدولي"، *مجلة الكلية الاسلامية الجامعة* ، العدد (٥٩) ، الجزء (١) ، (٢٠٢١).

٢- أسماء حداد، "الحروب الهجينة، الأزمة الأوكرانية أنموذجا"، *مجلة مدارات سياسية*، الجزائر عدد ديسمبر، (٢٠١٧).

ثالثا : الاطاريح والرسائل .

1- Ilaria D’Anna , I mercenari nel diritto internazionale , Dottorato di ricerca in Ordine Internazionale e Diritti Umani , Sapienza Universita

DI Roma FACOLTÀ DI SCIENZE POLITICHE , Anno Accademico 2010 - 2011.
3- Samantha V. Feuer , From the Shadows to the Front Page: State Use of Proxies for Cyber Operations , A Thesis Submitted To The Freeman Spogli Institute for International Studies , Stanford University , 2020 .
4- W. J. Nemeth, " Future War and Chechnya: A Case for Hybrid Warfare", Thesis, California :(Naval Postgraduate School) , June 2002 .

رابعا : المعاهدات والمواثيق الدولية.

١- البروتوكول الاضافي الاول لعام ١٩٧٧، والملحق باتفاقيات جنيف لعام ١٩٤٩ .
٢- اتفاقية منظمة الوحدة الافريقية للقضاء على الارتزاق لعام ١٩٧٧ .
٣- النظام الاساسي لمنظمة حلف شمالي الاطلسي لعام ١٩٤٧ .

خامسا : القرارات والتقارير والوثائق الدولية .

١- تقرير الفريق العامل المعني بمسألة استخدام المرتزقة وسيلة لانتهاك حقوق الانسان وإعاقة ممارسة حق الشعوب في تقرير مصيرها ، آثار المرتزقة والجهات الفاعلة ذات الصلة بالمرتزقة والشركات العسكرية والامنية الخاصة التي تشارك في انشطة الكترونية على حقوق الانسان ، الوثيقة A/76/151 ، ٢٠٢١ .
٢- - قرار الجمعية العامة للامم المتحدة ، الحق بالخصوصية بالعصر الرقمي ، ٢٠١٣ ، الوثيقة A/C.3/68/L.45/Rev.1 .
٣- مشروع المواد المتعلقة بمسؤولية الدول عن الافعال غير المشروعة دوليا لعام ٢٠٠١ .
٤- تقرير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية و اللاسلكية في سياق الامن الدولي ، الوثيقة (A/70/174) ، ٢٠١٥ .
5- Ori Swed and Daniel Burland , Cyber Mercenaries: Review of the Cyber and Intelligence PMSC Market , A report for The Working Group on the use of mercenaries as a means of violating human rights and impeding the exercise of the rights of peoples to self-determination , (2021) .
6- The Red Cross , Report International humanitarian law and the challenges of contemporary armed conflicts , 32nd International Conference of the Red Cross and Red Crescent , Geneva, 8-10 December 2015 .

سادسا : القوانين والتشريعات .

١- الأمر التنفيذي الصادر من رئيس الولايات المتحدة الامريكية بالرقم ١٣٦٩٤، في ١ نيسان/أبريل ٢٠١٥ .

٢- الأمر التنفيذي الصادر من رئيس الولايات المتحدة الامريكية بالرقم ١٣٧٥٧ في ٢٨ كانون الاول/ديسمبر ٢٠١٦ .
٣- لائحة (الاتحاد الأوروبي) ٧٩٧/٢٠١٩ .

سابعا : مصادر الانترنت .

١- اللجنة الدولية للصليب الأحمر ،الحرب السيبرانية والقانون الدولي الإنساني ، مقال منشور على الموقع الالكتروني :
https://www.icrc.org/ar/document/%D8%A7%D9%84%D8%AD%D8%B1%D8%A8-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%A9-%D9%88%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A-%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86%D9%8A

٢- قاعدة بيانات شركة (Microsoft)
https://www.microsoft.com/en-us/security/business/security-101/what-is-a-ddos-attack

٣- الموقع الرسمي لوزارة الخارجية الروسية :
https://mid.ru/en/foreign_policy/news/1806906/

٤- الموقع الالكتروني الخاص بمؤسسة (citizenlab) :
https://citizenlab.ca/

٥- نيري زيلبر ، ظهور المرتزقة في المجال السيبراني ، مقال منشور على الموقع الرسمي لمعهد واشنطن لسياسة الشرق الأدنى ، متاح على الرابط :
https://www.washingtoninstitute.org/ar/policy-analysis/zhwr-almrtzqt-fy-almjal-alsybrany

٦- الموقع الالكتروني الرسمي لوزارة الدفاع الروسية :
https://eng.mil.ru/en/news_page/country/more.htm?id=12471264@egNews

ثامنا : المصادر الاجنبية .

Eighth : Foreign sources :

A/Books

1- Geoffrey Best , Humanity in Warfare : The Modern History of the International Law of Armed Conflicts , First publishing , Littlehampton Book Services Ltd Publisher .

2- Michael N. Schmitt ed. , Tallinn manual 2.0 on the international law applicable to cyber operations , Cambridge University Press, 2017 .
3- Sean McFate , Mercenaries and War: Understanding Private Armies Today , National Defense University Press , DU Washington, D.C. , Press First printing, December 2019 .
4- Tim Maurer ,Cyber mercenaries , First published , Cambridge University Press , 2018.

B/Research and periodicals

1- Crowdstrike Global Intelligence Team , Use of Fancy Bear Android Malware in Tracking of Ukrainian Field Artillery Units , Report Published December 22 , 2016.
2- Charles Clore House , State Responsibility for Cyber Operations: International Law Issues , British Institute of International and Comparative Law , Event Report , London , 9 October 2014 .
3- Henry C. Burmester, "The recruitment and use of mercenaries in armed conflicts." American Journal of International Law , Vol (72), No (1) , (1978).
4- Jose de Arimateia da Cruz and Pedron Stephanie , Cyber Mercenaries: A New Threat to National Security, International Social Science Review journal , Vol. 96 , Iss. 2 , Article 3 , 2020 .
5- Jon Bateman , Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences and Implications , WORKING PAPER Carnegie Endowment for International Peace , 2022 .
6- Josephine Helen Dwan and Others , Pirates of the cyber seas: Are state-sponsored hackers modern-day privateers?, Law, Technology and Humans Journal , Vol (4) , No (1) , 2022 .
7- Jonathon W. Penney and Bruce Schneier , Platforms, Encryption, and the CFAA: The Case of WhatsApp v. NSO Group , berkeley technology law journal , Vol (36) , 2021 .
8- Kristen E. Eichensehr , Ukraine cyberattacks and the lessons for international law , American Journal of International Law , Vol (116) , 2022 .
9- Kosmas Pipyros et al , Cyberoperations and international humanitarian law: A review of obstacles in applying international law rules in cyber warfare , Information & Computer Security Journal ,Vol (24) ,No (1) , 2016 .

10- Nadiya Kostyuk and Erik Gartzke , Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine , Texas National Security Review , Vol (5) , No (3) , 2022 .
11- PR Kumar ,The Dogs of War Multidomain Mercenaries Operating in the Ukraine War ,Centre for Land Warfare Studies , "MANEKSHAW PAPER. No. 99, New Delhi , 2023 .
12- Syed Hamza Mannan , Projecting Power: How States Use Proxies in Cyberspace , Journal of National Security Law & Policy ,Vol (10) , 2019 .
13- Tim Maurer , Cyber proxies and their implications for liberal democracies , The Washington Quarterly Journal , Vol (41) , No (2) , 2018 .
14- Tim Maurer, Proxies and Cyberspace , Journal of conflict and security law , Vol (21) , No (3) , 2016 .
15- Tim Maurer ,Cyber mercenaries , First published , Cambridge University Press, 2018 .

C/ Judicial decisions

1- Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, I.C.J. Reports 1986 .
2- Corfu Channel case, Judgment of April gth, 1949 : I.C.J. Reports 1949 .

D/Internet sources

1- Alexandra Borgeaud dit Avocat, Arta Haxhixhemajli, Michael Andruch - Editors , NEW TECHNOLOGIES, FUTURE CONFLICTS, AND ARMS CONTROL , Center for Security Analyses and Prevention, Prague , JANUARY 2021 . Available at : https://cbap.cz/wp-content/uploads/CBAP_NewTechPaper2021FREN.pdf
2- Ataa Dabour , The Rise of Cyber-mercenaries , 15 May, 2021 , p. 2 , Available at : http://www.hscentre.org/technology/the-rise-of-cyber-mercenaries/
3- Christopher Kinsey, "International Law and the Control of Mercenaries and Private Military Companies," Cultures & Conflits

[Online], English documents, online June 26, 2008, accessed March 30, 2021. ، URL http://journals.openedition.org/conflits/11502.
4- Cyber Peace Institute , Ukraine Conflict: Cyberattacks, Frequently Asked Questions , June 16, 2022 , Available at : https://cyberpeaceinstitute.org/news/ukraine-conflict-cyberattacks-frequently-asked-questions/
5- David Cattler and Daniel Black , The Myth of the Missing Cyberwar Russia's Hacking Succeeded in Ukraine—And Poses a Threat Elsewhere Too , April 6, 2022 , Available at : https://www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberwar?check_logged_in=1
6- Elizabeth Montalbano , Hackers for Hire: Adversaries Employ 'Cyber Mercenaries' , Article published in July 21/ 2022 , Available at : https://threatpost.com/hackers-cyber-mercenaries/180263/
7- Heather Harrison Dinniss , UKRAINE SYMPOSIUM – MILITARY NETWORKS AND CYBER OPERATIONS IN THE WAR IN UKRAINE , Apr 29, 2022 , Available at : https://lieber.westpoint.edu/military-networks-cyber-operations-war-ukraine/
8- James A. Lewis , Cyber War and Ukraine , Center for Strategic & International Studies Report , Published June 16, 2022 . Available at : https://www.csis.org/analysis/cyber-war-and-ukraine
9- KENNETH R. ROSEN , The Man at the Center of the New Cyber World War , article published Politico Magazine , 2022 , Available at : https://www.politico.com/news/magazine/2022/07/14/russia-cyberattacks-ukraine-cybersecurity-00045486
10- Kristen Eichensehr , Cyberattack Attribution and International Law , Article published in July 24, 2020 , Available at : https://www.justsecurity.org/71640/cyberattack-attribution-and-international-law/
11- Miles Kenyon , Citizen Lab Response to the U. N. Working Group on the Use of Mercenaries , February 18, 2021 , Available at : https://citizenlab.ca/2021/02/citizen-lab-response-to-the-u-n-working-group-on-the-use-of-mercenaries/

12- Michaela Prucková , Cyber attacks and Article 5 – a note on a blurry but consistent position of NATO , Last visited on 29/8/2023 , Available at :
https://ccdcoe.org/library/publications/cyber-attacks-and-article-5-a-note-on-a-blurry-but-consistent-position-of-nato/
13- Noëlle van der Waag-Cowling and others , report on the provision of military and security cyber products and services by 'cyber mercenaries' and its human rights impact , Submission to the Working Group on the use of mercenaries , 2021 . Available at
https://www.ohchr.org/sites/default/files/Documents/Issues/Mercenaries/WG/CyberMercenaries/AccessNow.pdf
14- Pawel Knapczyk , Overview of the Cyber Weapons Used in the Ukraine - Russia War , Aug 18, 2022 , Available at :
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war/
15- Patrick Howell O'Neill , An internal investigation shows private-sector mass surveillance is happening on a scale never before revealed , December 16, 2021 , Available at :
https://www.technologyreview.com/2021/12/16/1042652/facebook-says-50000-users-were-targeted-by-cyber-mercenary-firms-in-2021/
16- Russell Gilchrest , THE INVOLVEMENT OF MERCENARIES AND PRIVATE MILITARY SECURITY COMPANIES IN ARMED CONFLICTS: WHAT DOES IHL SAY? , Available at :
https://www.geneva-academy.ch/news/detail/482-the-involvement-of-mercenaries-and-private-military-security-companies-in-armed-conflicts-what-does-ihl-say
17- Russia-Ukraine conflict: What role do cyberattacks play? , article published on the site :
https://www.dw.com/en/russia-ukraine-conflict-what-role-do-cyberattacks-play/a-60945572
18 - The Federal German Government , On the Application of International Law in Cyberspace , Position Paper , March 2021 , Available at :
https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf

19- Usalama Reforms Forum , Report on The Provision of Military and Security Cyber Products and Services by 'Cyber Mercenaries' and Its Human Rights , Kenyan , Available at : https://usalamaforum.org/wp-content/uploads/2021/09/Report-on-The-Provision-of-Military-and-Security-Cyber-Products-and-Services-by-%E2%80%98Cyber-Mercenaries-and-Its-Human-Rights-Impact.pdf

20- WOMEN'S INTERNATIONAL LEAGUE FOR PEACE AND FREEDOM , Report SUBMISSION TO THE UN WORKING GROUP ON THE USE OF MERCENARIES REGARDING "CYBER MERCENARIES" AND THEIR HUMAN RIGHTS IMPACT , FEBRUARY 2021 . Available at : https://www.reachingcriticalwill.org/news/latest-news/15209-wilpf-submits-views-on-cyber-mercenaries-and-human-rights