المركز الديمقراطي العربي؛ برلين- ألمانيا
مركز مؤشر للاستطلاع والتحليلات- ألمانيا

مجلة مؤشر للدراسات الاستطلاعية

دورية دولية محكمة
تعنى بنشر نتائج البحوث الاستطلاعية
في مجالات العلوم الاجتماعية والإنسانية

المجلد 07، العدد 20 ديسمبر 2025
Issue 3, Vol.19, September 2025
ISSN: 2701 - 9233

المركز الديمقراطي العربي
مجلة مؤشر للدراسات الاستطلاعية

DEMOCRATIC ARABIC CENTER, GERMANY

Journal (Index) of exploratory studies

International scientific periodical journal
Deals with the field of exploratory studies of social and human sciencies

مجلة مؤشر للدراسات الاستطلاعية

Germany: Berlin 10315
Gensinger- Str: 112
http://democraticac.de
http://indexpolls.de

مجلة مؤشر للدراسات الإستطلاعية

Journal Index For Exploratory Studies

مجلة مؤشر للدراسات الاستطلاعية

دورية دولية محكمة

تعنى بنشر البحوث الميدانية والتطبيقية

في مجالات العلوم الإجتماعية والإنسانية

تصدر عن

المركز الديمقراطي العربي

ومركز مؤشر للإستطلاع والتحليلات بألمانيا

Director of the Index Center
for Survey and Analytics
SAAD Elhadj

President of the Democratic
Arab Center
Ammar Sharaan

Editor-in-chief
Dr. Violla Makhzoum
Deputy Editor-in-Chief
Dr. Leila CHIBANI
Chairman of the advisory committee
Dr.Rabih Baalbaki
managing editor
Dr.sultan Nasser Eddin

Volume
07
Issue
20
Year
December 2025

ISSN: 2701-9233

Germany: Berlin 10315
http://democraticac.de http://indexpolls.de
Tel: 0049-code
030-89005468/030-89899419/030-57348845

رئيس الهيئــة العلميــة

أ.د. محمد رمال (لبنان)

د. عباس حمادة (لبنان)	د. لمى قميحة (لبنان)
د.أمين بري (لبنان)	د. بيان كمال الدين (لبنان)
د. رشدي زعيتر(لبنان)	د. اياد خلف محمد (العراق)
د. نادية طالب سلمان (العراق)	د سوزان زمّار(لبنان)
د. ايمان صالح (لبنان)	د. جمال مسلماني (لبنان)
د. كمال الزمراوي (المغرب)	أ.د. ليال عبد السلام الرفاعي (لبنان)
د. نينات كامل (لبنان)	د. غادة عزام (لبنان)
د. فاديا حسين (لبنان)	د. حسن الدمان (المغرب)
د. غسان جابر(لبنان)	د. فاطمة رحال (لبنان)
د. يحيى زلزلي (لبنان)	أ.د. حسين سالم مكاون (العراق)
د. ردينة حمادي (لبنان)	د. سماح رمضان (لبنان)
د. سميح عزالدين (لبنان)	د. رائد محسن (لبنان)
د. محمد جبرالعبودي (العراق)	د. مريم رسطوم (المغرب)
أ.د. صبري المدهون (مصر)	أ.د. حاكم موسى عبد الحسناوي (العراق)
د. ريم القريوي (تونس)	د. وفاء برتيمة (الجزائر)
د. هاجرالمفضلي (المغرب)	د. أمل هواري (لبنان)

Chair of the Scientific Committee

Prof. Mohamad Rammal (Lebanon)

Dr. Lama Koumayha (Lebanon)	Dr. Abbas Hmadeh (Lebanon)
Dr. Bayan Kamaelddine (Lebanon)	Dr. Amin Berri (Lebanon)
Dr. Iyad Khalaf Mohamad (Iraq)	Dr. Rushdi Zaiter (Lebanon)
Dr. Suzanne Zammar (Lebanon)	Dr. Nadia Taleb Salman (Iraq)
Dr. Jamal Meslmani (Lebanon)	Dr. Iman Saleh (Lebanon)
Prof. Layal Abed Salam Al-Rifaii (Lebanon)	Dr. Kmaal Al-Zemrawi (Morocco)
Dr. Ghada Azzam (Lebanon)	Dr. Ninette Kamel (Lebanon)
Dr. Hassan Damen (Morocco)	Dr. Fadia Hussein (Lebanon)
Dr. Fatima Rahal (Lebanon)	Dr. Ghassan Jaber (Lebanon)
Prof. Hussein Salem Mekkawen (Iraq)	Dr. Yehia Zalazali (Lebanon)
Dr. Samah Ramadan (Lebanon)	Dr. Roudayna Hmadeh (Lebanon)
Dr. Raed Mohsen (Lebanon)	Dr. Samih Ezzeddine (Lebanon)
Dr. Maryam Rostoum (Morocco)	Dr. Mohamad Jaber Abboudi (Iraq)
Prof. Moussa Abed Al-Hassnawi (Iraq)	Prof. Sabri Madhoun (Egypt)
Dr. Wafaa Bertima (Algeria)	Dr. Reem Al-Karyawi (Tunisia)
Dr. Amal Hawari (Lebanon)	Dr. Hajjar Al-Moufdali (Morocco)

محددات النشر

- يجب أن تندرج المقالات العلمية ضمن واحدة من المجالات التالية: السوسيولوجيا والأنثروبولوجيا؛ علوم التربية؛ علم النفس؛ علوم الاعلام والتواصل؛ علم الإدارة؛ العلوم السياسية؛ الديموغرافيا؛ الجغرافيا الاجتماعية.
- تميل المجلة بشكل خاص إلى تفضيل الدراسات الميدانية على الدراسات النظرية (هذا لا يعني بالضرورة رفض المقالات النظرية)؛ إذ من المستحسن أن يعتمد الباحثون في مقالاتهم المرسلة على إحدى هذه المناهج: المنهج الكمي ممثلا في استعمال الاستبيان وأدوات المعالجة الإحصائية. والمنهج الكيفي ممثلا في التقنيات الاثنوجرافية من قبيل توظيف المقابلات وتحليل الخطاب والملاحظة بالمشاركة...
- تقبل المجلة المقالات المحررة باللغات العربية أو الإنجليزية أو الفرنسية.
- تحث المجلة الباحثين على اتباع الشروط والمعايير الواردة في دليل النشر الخاص بالجمعية الأمريكية لعلم النفس (APA).
- تقبل المجلة المقالات بأحجام لا تزيد عن **20** صفحة.
- لا تقبل المجلة البحوث المنشورة سابقا، أو التي هي قيد الدراسة للنشر في مجلة أخرى.
- يقدم العمل في ملف وورد فقط، ويرسل إلى البريد الإلكتروني التالي: j.index@democraticac.de
- يجب الالتزام بالضوابط الشكلية للتحرير وفقاً للقالب الخاص بالمجلة (يمكن تحميل القالب من خلال الدخول على صفحة المجلة: https://cutt.us/PrMYV
- حجم الخط (**14**) ونوع الخط "ساكال مجلة" (Sakkal Majalla) بالنسبة للغة العربية، وحجم الخط 13 ونوع الخط "تايم نيو رومان" (Time New Roman) بالنسبة للغات الأجنبية؛ وأن تترك مسافة 1,15 بين الأسطر؛ وتفعل روابط الويب بوضع خط تحتها، لكي يتم فتحها.
- تزرع الصور التوضيحية والجداول والأشكال حسب ورودها في النص، ولا توضع في آخره.
- عدم استخدام الهوامش، ويمكن استخدام التوضيحات في النص، كما يجب إضافة الوصف التفصيلي في ملاحق منفصلة.
- لا يجب أن ترد أسماء المؤلفين في متن النص أو قائمة المصادر؛ وإذا كان لزاما فعل ذلك فيتم استبدالها بكلمة (المؤلف)؛ ويعتبر المؤلف مسؤولا عن إعادة تصحيح هذه التغييرات في حال قبول المقالة للنشر.
- يتم رفض أو قبول البحوث اعتمادا على تقارير المحكمين الدوليين.
- عند قبول البحث يتسلم الباحث إشعارا بالقبول، وفي حال طولب بالتعديل يمنح مهلة لإتمام جميع التصويبات والإجراءات (إن وجدت).

INSTRUCTIONS FOR AUTHORS

- Scientific articles must fall within one of the following fields: Sociology and Anthropology; Educational Sciences; Psychology; Media and Communication sciences; Management Science; Political Science; Demography; Social Geography.
- The journal in particular tends to favor field studies over theoretical studies (this does not necessarily means rejecting theoretical articles); It is recommended that researchers rely on their articles on one of these methods: the quantitative approach represented by the use of questionnaires and statistical processing tools. The qualitative approach is represented in ethnographic techniques such as the use of interviews, discourse analysis, and participatory observation…
- The journal accepts articles written in Arabic, English or French. o the journal urges researchers to follow the terms and standards of the American Psychological Association (APA) Publication Guide. o The journal accepts articles of no more than 20 pages.
- The journal does not accept previously published research, or that is under study for publication in another journal .
- The work is submitted in«Word file»only, and sent to the journal's e-mail.
- The formal controls for editing must be adhered to the template of the journal .
- Font size (14) and font type Sakkal Majalla for the Arabic language, while font size 13 and font type Time New Roman must be adhered to for foreign languages; It should also leave a space of 1.15 between lines; Web links are activated by underlining them, to be opened.
- The illustrations, tables, and figures are planted as they appear in the text, and are not placed at the end of it .
- Margins are not used, explanations can be used in the text, and detailed descriptions should be included in separate appendices.
- The authors' names should not appear in the body of the text or the list of sources; If it is necessary to do so, it shall be replaced by the word (author); The author is responsible for re-correcting these changes if the article is accepted for publication.
- Research is rejected or accepted depending on the reports of international arbitrators.
- Upon acceptance of the research, the researcher receives a notification of acceptance, and if the amendment is requested, he is given a deadline to complete all corrections and procedures (if any).

Details and information | تفاصيل ومعلومات

البريد الإلكتروني | E-mail	j.index@democraticac.de
الهاتف | Phone	00213660061297 00213778725481
العنوان | Address	Germany: Berlin 10315
الموقع الإلكتروني | Website	الصفحة الرسمية على المركز الديمقراطي العربي الموقع الخاص بالمجلة
مواقع التواصل الاجتماعي	https://www.facebook.com/MajallatIndex
Facebook Accounts	https://www.facebook.com/groups/indexpolls?_rdc=1&_rdr

المجلة مفهرسة ضمن | The following is a list of the Indexing databases

CiteFactor
Academic Scientific Journals

DOAJ

قاعدة بيانات شمعة توثق وتفهرس المقالات التربوية للمجلة

شمعة shamaa
شبكة المعلومات العربية التربوية
Arab Educational Information Network

قاعدة بيانات المكتبة الوطنية الألمانية

DEUTSCHE NATIONAL BIBLIOTHEK
GERMAN NATIONAL LIBRARY
المكتبة الوطنية الألمانية

قاعدة بيانات معرفة e-Marefa

معرفة
E-MAREFA

قائمــة المحتويــات | Contents

الباحث	عنـــوان المقـــال	الصفحـــة
ميساء سويف ا.د. هادية الشامي	الرقابة على أصحاب العمل وضرورة استفادتهم من الضمان الاجتماعي	10
د. علاء الدين بو مرعي	الشركات العسكرية والأمنية الخاصة وتأثير عملها على تطبيق مبدأ التمييز بين المدنيين والمقاتلين	23
د. محمد إبراهيم قانصو	الحرب السيبرانية: التهديدات، الاستراتيجيات، وتحديات الردع في الفضاء الرقمي	38
د. علاء الدين بو مرعي	القانون الإنساني بين الحرب السيبرانية والأسلحة المستقلة	62

كلمة العدد

بسم الله الرحمن الرحيم

عشرون عددًا... ليست مجرّد تسلسل زمني لإصدارات، بل حكايةُ التزامٍ معرفي، ومسيرةُ بحثٍ صبور، ورهانٌ واعٍ على أن المعرفة الدقيقة قادرة على إضاءة أكثر الأسئلة تعقيدًا في مجتمعاتنا. منذ العدد الأوّل، لم تكن *مجلة مؤشر للدراسات الاستطلاعية* مشروع نشرٍ تقليدي، بل رؤية علمية تؤمن بأن الأرقام حين تُنتَج بنزاهة، وتُقرأ بعقل نقدي، تتحوّل من بيانات صامتة إلى أدوات فهم وصناعة قرار.

يأتي العدد العشرون في لحظة عالمية وإقليمية بالغة الحساسية، تتسارع فيها التحوّلات الاجتماعية والاقتصادية والسياسية، وتزداد الحاجة إلى البحث الاستطلاعي الرصين الذي يميّز بين الرأي والانطباع، وبين المعطى العلمي والتأويل المتسرّع. من هنا، نرى في هذا العدد محطة نضجٍ علمي ومؤسسي، تؤكّد أن المسار الذي اخترناه لم يكن الأسهل، لكنه كان الأكثر صدقًا ومسؤولية.

لقد حرصت المجلة، عبر أعدادها المتعاقبة، على أن تكون مساحةً مفتوحة للباحثين الجادّين، ومنبرًا للدراسات التي تلتزم بالمنهجية، وتحترم أخلاقيات البحث، وتسعى إلى قراءة الواقع كما هو، لا كما نحبّ أن يكون. واليوم، ونحن نطلق العدد العشرين، نجدد عهدنا بأن يبقى *مؤشر* صوتًا علميًا مستقلًا، لا يخضع لإملاءات، ولا يساوم على الدقّة، ولا يتنازل عن حق المجتمع في معرفة مبنية على الدليل.

إن هذا العدد ليس احتفالًا بما أنجزناه فحسب، بل دعوة مفتوحة لما هو آتٍ. دعوة إلى تعميق ثقافة الاستطلاع، وتوسيع دوائر التعاون البحثي، وربط نتائج الدراسات بالسياسات العامة، وبحاجات الناس الفعلية. كما هو تذكير بأن البحث العلمي الحقيقي يبدأ بسؤال صادق، وينتهي بمسؤولية أخلاقية تجاه الإنسان والمجتمع.

في العدد العشرين، نؤكّد أن *مؤشر للدراسات الاستطلاعية* سيبقى مساحةً للفكر النقدي، وجسرًا بين الباحث وصانع القرار، ومنصّةً تؤمن بأن المعرفة ليست ترفًا، بل شرطًا أساسيًا لبناء المستقبل.

العدد 20 ليس خاتمة مرحلة، بل بداية أعمق...

بداية نكتبها معًا، بعلمٍ أكثر وعيًا، وبحثٍ أكثر التزامًا، ورؤيةٍ أكثر إنسانية.

رئيس التحرير د. فيولا مخزوم

مجلة مؤشر للدراسات الاستطلاعية
Journal index of exploratory studies
المجلد 07، العدد 20
ISSN: 2701-9233

الرقابة على أصحاب العمل وضرورة استفادتهم من الضمان الاجتماعي

Employer oversight and the necessity of their inclusion in social security benefits

ميساء سويف

الجامعة الاسلامية في لبنان

Maysaa_swaif@hotmail.com

ا.د. هادية الشامي

الجامعة الاسلامية في لبنان

hadia.alchami@iul.edu.lb

ملخص البحث

يُعَدّ الضمان الاجتماعي أداةً مهمةً لحماية أصحاب العمل وضمان استقرارهم المالي، إلا أنّ مشكلة عدم استفادتهم منه تظلّ قائمةً رغم التزامهم بالرقابة. يهدف هذا البحث إلى تسليط الضوء على أهمية استفادة أصحاب العمل من الضمان الاجتماعي وتقديم اقتراحات قانونية لتحسين الوضع القانوني.

يخضع أصحاب العمل للرقابة،إذ يُشرف التفتيش على تطبيق قوانين الضمان الاجتماعي ويضمن أن يلتزم أصحاب العمل بدفع الاشتراكات اللازمة والتصريح عن موظفيهم. الرقابة قد تكون شاملة أو حصرية وتُنفذ بشكل دوري أو طارئ، وتخضع المؤسسات للمراقبة بانتظام، لكن الرقابة لا تشمل بالضرورة أصحاب العمل أنفسهم الذين يُعتبرون المساهمين الرئيسيين في النظام من دون استفادة، هذا الوضع يشكل عبئًا على أصحاب العمل الذين يرون أن دفعهم للاشتراكات لا يعود عليهم بأي فائدة، ما يؤدي أحيانًا إلى فساد أو تجاوزات في نظام التصريح والاشتراكات.

من هنا، توصي الدراسة بضرورة تعديل النظام القانوني لضمّ أصحاب العمل إلى الضمان الاجتماعي أسوةً بالعاملين لديهم، بما يضمن لهم الحصول على رعاية صحية وتقديمات أخرى مشابهة. وقد تم اقتراح تعديل القانون لإلزام أصحاب العمل بالانتساب للضمان الاجتماعي وتحديد الاشتراكات على أساس الأجر المحدد في النظام، بحيث يتمكن هؤلاء من الحصول على تقديمات المؤسسة، وهو ما سيساهم في تحفيز أصحاب العمل على الامتثال للقوانين والوفاء بموجباتهم.

فتفعيل الضمان الاجتماعي لأصحاب العمل مع فرض رقابة فعالة يمكن أن يؤدي إلى تحسين وضعهم الاقتصادي والاجتماعي، ويساهم في تعزيز استقرار الشركات وتوفير بيئة عملٍ أكثر عدلًا لكافة الأطراف.

الكلمات المفتاحية: الضمان الاجتماعي، أصحاب العمل، خضوع أصحاب العمل، الإصلاح القانوني.

Abstract

Social security is a vital tool for protecting employers and ensuring their financial stability; however, the issue of their lack of direct benefits remains a persistent problem, despite their full compliance with regulatory obligations. This research aims to highlight the importance of extending social se

curity benefits to employers and to propose legal reforms that would enhance their legal standing within the system.

Employers are subject to strict oversight, as inspections ensure that they comply with social security laws, declare their employees, and pay the required contributions. Although institutions are regularly monitored, such oversight does not necessarily include employers themselves, who are major contributors to the system without receiving any direct benefits. This situation imposes a significant burden on employers, who often feel that their contributions yield no personal advantage, sometimes resulting in irregularities, corruption, or underreporting of wages.

Accordingly, the study recommends amending the legal framework to include employers within the scope of social security coverage, similar to their employees, thereby granting them access to healthcare and other benefits. The proposed amendment seeks to mandate employer affiliation to the social security system and determine contributions based on a standard wage, enabling them to receive the institution's benefits. Such reform would encourage greater compliance and support a healthier legal environment.

Activating social security coverage for employers, along with effective oversight mechanisms, can significantly improve their economic and social conditions, enhance business stability, and promote a fairer working environment for all parties involved.

Keywords: social security, employers, oversight of employers, employers' compliance with social security, legal reform.

المقدمة

تعد مسألة خضوع أصحاب العمل للرقابة وأهمية استفادتهم من الضمان الاجتماعي من المواضيع الهامة خصوصا في ظل الظروف الاقتصادية والاجتماعية التي يمر بها لبنان. فمن ناحية، يعتبر الضمان الاجتماعي أداة هامة لتوفير الحماية الاجتماعية لأصحاب

العمل ولضمان استقرارهم المالي في مواجهة المخاطر المختلفة. ومن ناحية أخرى، يترتب على أصحاب العمل التزام رقابي صارم وهو ما يشكل عبئًا عليهم إذا لم يتمكنوا من الاستفادة من الضمان الاجتماعي .

حيث يشهد مفهوم الحماية الاجتماعية في السنوات الأخيرة تطوّراً لافتاً، حيث لم يعد محصوراً بفئة الأجراء فقط، بل بات يشمل مختلف الفاعلين الاقتصاديين بما فيهم أصحاب العمل. إلا أنّ التشريعات اللبنانية ما زالت تعتمد مقاربة تقليدية تفصل بين الطرفين، بحيث يتمتع الأجراء بمظلّة الضمان الاجتماعي، فيما يبقى أصحاب العمل خارج أي إطار حمائي رغم دورهم الأساسي في العملية الإنتاجية. هذا التباين يخلق فجوة واضحة بين المسؤوليات المترتّبة على أصحاب العمل من جهة، والحقوق الممنوحة لهم من جهة أخرى، ما يبرز الحاجة إلى إعادة تقييم شاملة للنظام القانوني الحالي بما ينسجم مع مبادئ العدالة الاجتماعية ومتطلّبات الإصلاح المعاصر ففي الفصل الأول من هذا البحث تم التركيز على خضوع أصحاب العمل للرقابة، وهو أمرٌ حيويٌّ لضمان الامتثال للقوانين المتعلقة بالعمل والظروف التي يتعين عليهم توفيرها للعمال. كما ناقش الفصل الثاني ضرورة استفادة أصحاب العمل من الضمان الاجتماعي، باعتباره أداة أساسية لحماية مصالحهم وضمان استقرار شركاتهم، من خلال تقديم اقتراحات قانونية، يسعى هذا البحث الى تسليط الضوء على كيفية تحسين النظام القانوني لضمان التوازن بين رقابة الدولة وحقوق أصحاب العمل.

1.1.هدف الدراسة

يهدف البحث إلى دراسة خضوع أصحاب العمل للرقابة والإضاءة على أهمية استفادتهم من الضمان الاجتماعي . كما يهدف الى التأكيد على ضرورة وجود قانون يرعى هذا الضمان في لبنان نظرًا لأهميته في وقتنا الحالي مما يجعل من مسألة ضمان أصحاب العمل قضيةً بالغة الأهمية.

2.1 .إشكالية الدراسة

تتمثل إشكالية البحث في غياب إقرار قانون شامل يضمن استفادة اصحاب العمل من الضمان الاجتماعي حتى يومنا هذا على الرغم من أهميته من نواحٍ عديدة.

3.1 .أسئلة الدراسة

لضمان أصحاب العمل أهمية كبرى: فما هي هذه الأهمية؟ وما هي العوائق التي تحيل وراء عدم تطبيقه؟ وما هي الأسباب تبرر ضرورة ضمان أصحاب العمل؟

وما هي الآليات القانونية والرقابية التي تحدد خضوع أصحاب العمل للرقابة في لبنان؟

4.1 .منهج البحث

يعتمد البحث منهجية تحليلية عمادها دراسة الوقائع و تحليلها.

5.1. اصحاب العمل

صاحب العمل هو السلطة التي توظف وتدفع أجور الأفراد الموظفين لديها مقابل عملهم. قد يكون فردًا أو مؤسسةً تمثّل العديد من الأشخاص، أو أي نوع من الأعمال التجارية،أي هو كل شخص طبيعي أو اعتباري يشغِّل عاملًا أو أكثر مقابل أجر.حيث يقوم بتحديد شروط التوظيف للموظفين مثل الأجور الشهرية، وأيام الدوام والإجازة وساعات العمل، وهو المسؤول قانونًا عن ظروف العمال والمسؤول عن ضمانهم، حيث يجب عليه أن يدوّن دون بياض أو حشو أو حك أو تصحيح في صندوق خاص وفق نموذج تضعه إدارة الصندوق تحت تصرفه ويبين فيه تاريخ كل تدوين أسماء الأشخاص الخاضعين للضمان، وتاريخ ومحل ولادتهن ومقدار أجرهم والتعويضات الإضافية التي يستفيدون منها وذلك قبل مباشرتهم العمل، وكذلك تاريخ الانقطاع عن العمل أو الصرف منه خلال ثلاثة أيام على الأكثر تلي تاريخ حصوله، وصاحب العمل الذي يغفل تنظيم هذا السجل يعاقب بغرامة وبحال عدم دفعه خلال خمسة عشر يوما منتاريخ تنظيم محضر الضبط تضاعف العقوبة.

يكون صاحب العمل مسؤول عن التصريح عن التحاق الشخص الخاضع للضمان بالعمل او عن تركه العمل وذلك خلال خمسة عشر يوما من تاريخ الالتحاق أو الترك تحت طائلة عقابه بغرامة بحال اغفاله هذا التصريح، واذا تجاوز التأخر في التصريح مدة أقصاها ثلاثة أشهر من تاريخ الالتحاق بالعمل أو الترك يعاقب المخالف بغرامة إضافية.

1.5.1. أصول الرقابة على أصحاب العمل

حدد نظام التفتيش ومراقبة أصحاب المؤسسات في الفصل الثاني منه قواعد المراقبة وأصول أجرائها، مُحدداً في القسم الاول أنواع إجراء المراقبة وحالاتها ومهل إنجازها. حيث تجري مراقبة اصحاب العمل ومن هم في حكمهم المنصوص عليهم في المواد 9 إلى 12 من قانون الضمان الإجتماعي وفقاً لأحكام المادة 77 وما يليها من ذات القانون وأحكام هذا النظام على أساس مخططات عمل تصدر عن المدير العام سنويا بناء على اقتراح المدير.

وتكون المراقبة شاملة أو حصرية، وتتناول الأولى مختلف نواحي تنفيذ قانون الضمان الإجتماعي والأنظمة والمراسيم المتممة له وتجري إما بطريقة دورية للمؤسسات المسجلة او بطريقة المسح الشامل للمؤسسات المكتومة او بصورة طارئة تلقائياً من قبل المديرية أو بناءً على أي طلب حسب الاصول.

وتتم الثانية بصورة طارئة تلقائيا من قبل مديرية التفتيش والمراقبة او بناءً على أي طلب حسب الأصول.

وقد نصّ النظام على أن تخضع المؤسسات المسجلة لدى الصندوق للمراقبة الشاملة ضمن خطة منهجية مرة كل خمس سنوات بصورة دورية منتظمة وتخضع المؤسسات المكتومة لمسح شامل مرة كل عشر سنوات على الاقل وذلك للتصريح عنها وتسوية اوضاعها تجاه الصندوق. كما ويمكن للمدير أن يقرر إجراء المراقبة الدورية والمسح الشامل في دورة زمنية أقصر لبعض فئات المؤسسات والأنشطة والمناطق الجغرافية وذلك تبعاً للضرورة والإمكانات.[1]

كما حدد نظام التفتيش ومراقبة اصحاب المؤسسات في قسمه الثاني من الفصل الثاني امتداد المراقبة التي يقصد بها امتداد المراقبة زمنيًا، فتمتد المراقبة الشاملة سواء كانت دورية أم طارئة مع مراعاة أحكام مرور الزمن من بدء مفعول الخضوع لقانون الضمان الإجتماعي أو نهاية آخر مدة استحقاق توقفت عندها المراقبة السابقة حتى آخر سنة مالية أقفل حسابها لدى صاحب العمل إلا ان هذه المراقبة السابقة تمتد حتى حصول التغيير في الأوضاع الإدارية أو القانونية لصاحب العمل في الحالات التالية:

- التوقف عن النشاط وعن استخدام أجراء خاضعين للضمان الإجتماعي.
- انتقال الملكية بسبب وفاة صاحب العمل إذا كان شخصاً طبيعياً.
- حل المؤسسة وتصفيتها أو انتهاء وجودها المادي لأي سبب كان.
- الإفلاس
- إبرام أحد العقود التي تتناول الملكية التجارية المنصوص عليها في المرسوم الاشتراعي رقم 11 تاريخ 1967/7/11 وتعديلاته إلا إذا كان وُجِد ضمانًا قانونيًا في إستمرار المؤسسة واستمرار عقود الخاضعين للضمان الإجتماعي.
- يتعين في هذه الحالة الأخيرة تغطية الاوضاع الجديدة بإجراء المراقبة حسب الاصول.

إلا انه يمكن ان تتناول المراقبة الشاملة او الحصرية في حال تناولت موضوع رقابة سابقة بموجب أمر مهمة اضافي صادر عن المدير، وذلك فيحال ظهور عناصر جديدة تبرر ذلك مع مراعاة احكام مرور الزمن المنصوص عليها قانوناً.[2]

وقد نص نظام التفتيش ومراقبة اصحاب المؤسسات أن على المفتش أن يطلب التنحي عن المهمة إذا كان بينه وبين صاحب العمل او الشاكي قرابة أو مصاهرة لغاية الدرجة الرابعة أو صداقة وثيقة أو عداوة مستحكمة يمكن أن تُعَرِّض نتائج تقريره للطعن. وفي حال عدم ورود طلب التنحي من المفتش، يحق للمدير بناءً على اقتراح رئيس المنطقة أن يتخذ قرارًا بتنحية المفتش للأسباب المبينة في الفقرة السابقة أو في حال ارتكاب المفتش خطأ مهنياً من شأنه التأثير على نتائج التفتيش. كما يحق في الاحوال المبينة في الفقرتين السابقتين لكل من صاحب العمل او الشاكي ان يطلب تنحية المفتش بتقديم طلب خطي إلى المديرية، وعلى المدير ان يبت فيه خلال خمسة ايام من

[1] النظام رقم 19، نظام التفتيش ومراقبة أصحاب العمل، الفصل الثاني، القسم الأول، المادة 11
[2] مرجع نفسه، المادة 14

تاريخ وروده. وفي كافة الأحوال، يحق لصاحب العمل او الشاكي ان يطعن بنتائج التفتيش امام المحكمة المختصة مدلياً ببطلانها عند توفر اسباب التنحي.[3]

2.5.1 مكان المراقبة وزمان المراقبة

أ. مكان المراقبة:

تجري المراقبة على المؤسسة في مركزها الرئيس أو الفرع التابع لها أو على عنوان المسؤول عنها الذي يمثلها ت7جاه الغير. وإلا يمكن إجراؤها او استكمالها شرط عدم الإخلال بمبدأ إجراء المراقبة محلياً، لدى:

- المسؤول عن المؤسسة بصورة قانونية إذا كانت شخصاً معنوياً
- مكتب المحامي وكيل صاحب العمل أو ورثته.
- مكتب المحاسبة المعتمد في حال تعذر نقل الدفاتر والسجلات إلى مكتب المفتش.
- وكيل التفليسة
- مصفي المؤسسة او الحارس القضائي.

ويحظر على المفتش القيام بمهامه لدى معقبي المعاملات الذين يمكن ان يعتمدهم صاحب العمل في علاقته مع الصندوق.[4]

ب. زمان المراقبة:

يستفاد من نص الفقرة (8) من المادة 77 ان اصحاب العمل كافة ملزمون باستقبال مفتشي الصندوق وتمكينهم من القيام بمهامهم بناءً على موعد سابق، أي يمتنع على المفتشين الدخول المفاجئ إلى المؤسسة والمباشرة بإجراء المراقبة فيها إذا تمنع صاحب العمل.

إلا انه بمقتضى المادة 18 من نظام التفتيش ومراقبة اصحاب العمل، يتوجب على المفتش القيام بالزيارة الاولى للمؤسسة من دون اعلام مسبق والاتصال مباشرة بصاحب العمل أو من يقوم مقامه بصورة قانونية، او برئيس المحاسبة المسؤول عن شؤون العمال والمستخدمين والتعريف عن نفسه بإبراز بطاقة الوظيفة.

وفي حال تعذر المباشرة بإجراء المراقبة فعلياً منذ الزيارة الأولى، يحدد المفتش موعداً لاحقاً للمباشرة بها بموجب إشعار بزيارة مفتش.

وفي حال استحالة مقابلة صاحب العمل أو المسؤول في مكان المؤسسة أو تعذر إجراء المراقبة في مكان آخر لعدم توافر الحالات المنصوص عليها في الفقرة (2) من المادة 17 من هذا النظام، توجه دعوة حضور بواسطة رئيس المنطقة إلى صاحب العمل أو المسؤول عن المؤسسة بصورة قانونية على عنوان السكن المصرح عنه إلى الصندوق

[3] النظام رقم 19، نظام التفتيش ومراقبة أصحاب العمل، الفصل الثاني، القسم الثالث، المادة:16
[4] المرجع نفسه، المادة:17

أو العنوان المعروف بأي طريقة أخرى مرتين متتاليتين للإجتماع بالمفتش وتزويده بالإيضاحات والمعلومات والمستندات اللازمة لإجراء المراقبة.[5]

إن هذا النص، برأينا، لا يولي المفتش حق اجراء المراقبة إذا عارض صاحب العمل إتمامها، انما يضع على عاتقه موجب القيام بالزيارة الاولى بشكل مفاجئ. وفي حال تعذر المباشرة بالمراقبة فعلياً، يجب على المفتش ان يحدد موعداً لاحقاً بموجب اشعار بزيارة.

أما المشترع الفرنسي، وبعد ان كان يلزم اصحاب العمل باستقبال المفتشين في كل حين من دون ارسال اشعار لهم، فرجع عن ذلك ليقرر بأن كل رقابة تجري تطبيقاً لأحكام المادة 7/243 من قانون الضمان الإجتماعي الفرنسي، يجب ان يسبقها ارسال اشعار بواسطة كتاب مضمون مع اشعار بالوصول او بالاستلام.

اما الاوقات المسموح للمفتش بممارسة رقابته فيها فتُحدد ضمن أوقات العمل العادية وطبقاً للدوام المعمول به في المؤسسة وعليه التوفيق بين المقتضيات العملية لكلا الفريقين.[6]

6.1. ضرورة استفادة أصحاب العمل من الصندوق الوطني للضمان الاجتماعي مع اقتراحات حول هذه الاستفادة:

بالرغم من المساهمات المالية الكبيرة التي يقدمها أصحاب العمل في الصندوق الوطني للضمان الاجتماعي فانهم في الغالب لا يحصلون على أي استفادة بالمقابل. فأصحاب العمل هم من أكبر المساهمين ماديا في الصندوق، بالإضافة الى أعضاء مجلس الإدارة الذين يقومون بمهام كبيرة ويتمتعون بصلاحيات ومهام أساسية لاستمرارية الصندوق إنما لا يستفيدون من خدماته التي يشاركون بشكل أساسي بوجودها.

فأصحاب العمل لا سيما أصحاب المهن الحرة يعانون الحرمان من فرصة الاستفادة من الرعاية الصحية، وكذلك يشترك في هذه المعاناة أعضاء مجالس ادارة المؤسسات العامة والخاصة والشركات من حرمانهم من تقديمات الصندوق الوطني للضمان الاجتماعي.

هذا الو اقع يخلق تفاوتا كبيرا بين الأجراء وأصحاب العمل حيث يتمتع الأجراء بالحماية الصحية والاجتماعية بينما يظل أصحاب العمل غير مستفيدين من هذه الخدمات بالرغم من تمويلهم للصندوق.

1.6.1.استفادة أصحاب العمل من الصندوق:

حددت المادة 9 من قانون الضمان الإجتماعي الأشخاص الخاضعين للضمان منذ المرحلة الأولى، إلا أنّها لم تذكر أصحاب العمل، بالرغم من قيام هؤلاء بتأمين ضمان أغلب المضمونين. إذ يخضع للضمان الأجراء اللبنانيون (عمّال ومستخدمون) الدائمون والمؤقتون والمتمرنون والموسميون والمتدربون الذين يعملون لحساب رب عمل

[5] نظام التفتيش ومراقبة أصحاب العمل، الفصل الثاني، القسم الرابع، المادة:18
[6] ناجي شوفاني، مرجع سابق، ص: 664

واحد أو أكثر لبناني أو أجنبي، أيا كانت مدة أو نوع أو طبيعة أو شكل أو صحة العقود التي تربطهم برب عملهم وأيا كان شكل أو طبيعة كسبهم وأجورهم حتى ولو كان هذا الكسب أو الأجر مدفوعاً كلياً أو جزئياً، على شكل عمولة أو حصة من الأرباح أو على الإنتاج وسواء كان مدفوعاً من قبل رب العمل أو من قبل أشخاص ثالثين.[7]

وإذا نظرنا إلى أجهزة الصندوق فإنها تتكون من مجلس إدارة ولجنة فنية وأمانة سر. وقد روعي في تأليف مجلس إدارة الصندوق تمثيل المعنيين بإدارة نظام الضمان الإجتماعي وتطبيقه، ألا وهم الدولة وأصحاب العمل والأجراء. إذ تحدد الدولة الأسس التي تقوم عليها سياستها على صعيد الضمان الإجتماعي عن طريق إصدار القوانين ووضع الأنظمة، سواء لناحية الخضوع لها أو لناحية التقديمات التي يؤمّنها. ويمكنها من خلال تمثيلها في مجلس الإدارة أنّ تتابع وأن تتدخل عند الاقتضاء لتأمين تنفيذ هذه السياسة. **أما أصحاب العمل فقد وُضعت على عاتقهم موجبات قانونية ومالية، إذ يتحملون في المرحلة الحالية القسم الأكبر من تمويل الضمان الإجتماعي. والأجراء هم المستفيدون من تقديمات هذا الضمان والمشاركون إلى حد ما في تمويله إلى جانب أصحاب العمل.**[8]

بالتالي فإن أصحاب العمل يتحملون موجبات قانونية ومالية فائقة من دون أي فائدة أو مقابل، حيث المستفيد الأول والأخير هم الأجراء الذين لولا أصحاب العمل لما كان ليتمتع بهذه النعمة.

وبالعودة للمادة 21 من قانون العمل والضمان الإجتماعي فإن الأطباء المقبولين من الصندوق المنصوص عنهم في هذه المادة الذين يؤمّنون العناية الطبية للمرضى المستفيدين منها، هم الأطباء الخاضعين لتقديمات العناية الطبية في حالات المرض والأمومة، استناداً لأحكام البند 4 من المادة 9 من قانون الضمان الإجتماعي التي نصت على أن: "يخضع الأطباء المقبولون لدى الصندوق وفقاً لأحكام قانون الضمان الإجتماعي والنظام الداخلي، وذلك بموجب مرسوم يتخذ في مجلس الوزراء بناءً على إقتراح وزير العمل والشؤون الإجتماعية وإنهاء مجلس إدارة الصندوق".

فحتى الأطباء مستفيدون من الصندوق الوطني للضمان الإجتماعي، وذلك على عكس أصحاب العمل في المؤسسات، فهم غير خاضعين للضمان الإجتماعي. فلما كان كل من الأطباء وأصحاب العمل خاضعين للرقابة، حيث تخضع الفئة الأولى للرقابة الطبية من مستشفيات وصيدليات وأطباء، والفئة الأخيرة للرقابة على أصحاب العمل، فلماذا يستفيد الأطباء من الصندوق من دون إستفادة أصحاب العمل؟

وفي ما يخص موضوع التفتيش على أصحاب العمل، فقد أخضعت المادة 77 (المعدلة وفقاً للمرسوم الإشتراعي 116-تاريخ 30-6-1977) في فقرتها الأولى أصحاب العمل لمراقبة الصندوق: "يخضع أصحاب العمل في ما يتعلق بتطبيق أحكام هذا القانون والمراسيم والأنظمة المتممة له لمراقبة الصندوق"، وحددت موجباته في نصوص فقرات المادة نفسها.

---

[7] **قانون الضمان الإجتماعي الإجتماعي، المادة 9 بند 1**

[8] **ناجي شوفاني، شرح قانون الضمان الإجتماعي، الطبعة الأولى، د.ن، 2011، ص:34**

إن صاحب العمل هو من يقوم وفقاً للأحكام القانونية والنظامية المرعية التطبيق بالتصريح عن الأشخاص الخاضعين للضمان الإجتماعي، وتحديد الكسب الذي يُتخذ أساساً لحساب الإشتراكات، كما يقوم بحسم تلك الإشتراكات المتوجبة عليهم ومن ثم يدفع المجموع في المكتب الاقليمي أو المحلي المختص خلال المهلة القانونية.

وفي ضوء ما تقدم تظهر أهمية التحقق من مدى تنفيذ أصحاب العمل لموجباتهم القانونية والمالية للتأكد من تقيدهم أو مخالفتهم للنصوص القانونية ولا سيما التصريح عن الأشخاص الخاضعين للضمان ودفع الإشتراكات المتوجبة عليهم ومقدار الكسب الحقيقي الذي تحسب على أساسه هذه الإشتراكات.

فمن المعلوم أنّ أصحاب المؤسسات التجارية ينسبون العاملين لديهم إلى مؤسسة الضمان الإجتماعي، لكن في الواقع، عندما يذهب مفتش الضمان الإجتماعي إلى هذه المؤسسات للرقابة على رواتب العاملين فيها، فإنّ بعض أصحاب هذه المؤسسات يطلبون من المفتشين التغافل عن المبلغ الحقيقي للرواتب وتسجيل مبالغ أقل، مقابل رشوة يقوم صاحب المؤسسة بدفعها للمفتش.[9] وبالمقابل، يقوم المفتش بقبول هذه الرشوة لعدة أسباب أهمها المحسوبيات الطائفية، السياسية، المناطقية وغيرها.[10]

ولعل الدافع الأساسي لقيام أصحاب المؤسسات باعتماد أسلوب الرشاوى وعدم التزامهم بما هو متوجب عليهم تجاه مؤسسة الضمان الإجتماعي هو عدم تغطيتهم من قبل صندوق الضمان الإجتماعي، إذ تقتصر التغطية على العاملين في المؤسسة التجارية من دون أصحابها. فيعتبر أصحاب المؤسسات بذلك أنهم يتكلفون من دون إستفادة لشخصهم. لذلك، نرى أنه من الصائب أنّ يقوم قانون الضمان الإجتماعي بتعديل هذه الثغرة وتغطية أصحاب المؤسسات مع العاملين في المؤسسات، حتى يشعر أصحاب المؤسسات التجارية بمسؤولية أكبر تجاه صندوق الضمان الإجتماعي وأن ما يدفعونه من رسوم سيعود عليهم بالمقابل بمنفعة ولن يكون مجرّد عبءٍ يسعون للتخلص منه أو على الأقل، تخفيفه بأي طريقة سواء اعتماد أسلوب الرشوة أو إيجاد باب آخر للإنتساب للضمان الإجتماعي، وإن كان ذلك عن طريق التحايل كشراء لوحة سيارة عمومية مثلاً. (أخضعت المادة التاسعة من قانون الضمان الإجتماعي في فقرتها الأولى (أولاً) في الصندوق الوطني للضمان الإجتماعي حيث نصت على إنّ :"تحدد بمراسيم تتخذ بمجلس الوزراء بناءً على اقتراح وزير العمل والشؤون الإجتماعية وإنهاء مجلس إدارة الصندوق وبالشروط المحددة فيها، فئات سائقي السيارات العمومية والحرفيين وسائر فئات الأشخاص اللبنانيين غير المذكورين في هذه المادة الذين تتبين ضرورة إخضاعهم منذ المرحلة الأولى، لبعض أو جميع فروع الضمان الإجتماعي". فلا يخفى أنّ الشخص الذي لا يكون له باب للضمان بالتالي ليس لديه غطاء صحي، يضطر إلى أنّ يبحث عن أي طريقة لضمان نفسه وعائلته، ومن إحدى تلك الطرق شراءه للوحة (السيارة العمومية) من دون ممارسة هذه الوظيفة فعلياً، مما يعتبر إحتيالًا على الضمان الإجتماعي. بالتالي فإن عدم إخضاع أصحاب

[9] صادق علوية، رئيس مصلحة الضمان الإجتماعي، مقابلة شخصية، الأربعاء 2019/4/10، أبدى فيها عن وجود بعض الموظفين الذين يتلقون الرشأوى، وقد تمت ملاحقة البعض منهم

[10] نبيل جواد، مسؤول الدعم التقني والفني، مقابلة شخصية، الأربعاء 2019/4/10

العمل للضمان الإجتماعي من الممكن أنّ يدفعهم لايجاد حلول بديلة غير قانونية لتفادي الأضرار الناتجة عن عدم خضوعهم للضمان.

2.6.1.اقتراح حول خضوع أصحاب العمل للضمان الاجتماعي:

قد تقدم حضرة مدير عام الصندوق الوطني للضمان الإجتماعي الدكتور محمد كركي إلى حضرة رئيس مجلس إدارة الضمان بتاريخ 8 آب 2018 بمرسوم خضوع أصحاب العمل ومن في حكمهم لأحكام قانون الضمان الإجتماعي فرع الضمان والأمومة تحت الرقم 2569، بعد النظر بالطلبات المتكررة التي تقدّم بها معالي وزير العمل وبعض أعضاء مجلس الإدارة، لذا تم إيداع مشروع المرسوم المتعلق بإخضاع أصحاب العمل ومن في حكمهم لأحكام قانون الضمان الإجتماعي مع الدراسة الإكتوارية التي أعدّها الخبير الإكتواري. وذلك بعد أنّ اقتضت الحاجة لإخضاع هذه الفئة من اللبنانيين لأحكام قانون الضمان الإجتماعي واستفادتهم من تقديماته الصحية، وقد رجا الاطلاع وعرض الموضوع على مجلس الإدارة وتقرير ما يرونه مناسباً.

وأُخضِع إلزامياً لأحكام قانون الضمان الإجتماعي - فرع ضمان المرض والأمومة أصحاب العمل ومن في حكمهم، غير الخاضعين لأحكامهم أو لأي نظام تأميني عام آخر، بأي صفة أخرى، شرط ممارسة العمل شخصيًا على الأراضي اللبنانية، وذلك بناءاً على إقتراح وزير العمل، وبعد استشارة مجلس شورى الدولة، بناء على موافقة مجلس الوزراء، وقرار مجلس إدارة الصندوق الوطني للضمان الإجتماعي المتضمن الإنهاء بمرسوم خضوع أصحاب العمل ومن في حكمهم لأحكام قانون الضمان الإجتماعي، وبناءًا على قانون الضمان الإجتماعي الموضوع موضع التنفيذ بموجب المرسوم رقم 13955 تاريخ 1963/9/26 ولا سيما المادة التاسعة منه. والمقصود بأصحاب العمل ومن في حكمهم، مثل التجار المسجلون في السجل التجاري وفقاً للمادة 24 من قانون التجارة البرية، والشركاء في شركات التضامن، والشركاء المفوضين في شركات التوصية البسيطة، والمدير المفوض بالتوقيع في الشركات المحدودة المسؤولية، ورؤساء مجلس الإدارة المدراء العامين وأعضاء مجالس الإدارة في الشركات المساهمة وشركات التوصية المساهمة، طوال فترة انتخابهم، والمدراء العامين المساعدين في الشركات المساهمة، ورؤساء وأعضاء مجالس الإدارة في المؤسسات العامة أو ذات الصفة العامة، والشركاء المتضامنون في شركات التوصية المساهمة، والمدراء المفوضين بالتوقيع في الشركات المدنية المسجلة في السجل المدني لدى الغرفة الابتدائية المدنية في بيروت، ومدراء الشركات الأجنبية التي تملك فروعًا في لبنان أو مكاتب تمثيل، وسائر أصحاب العمل المسجلين في الصندوق ويستخدمون أجراء. وأنّ هؤلاء الأشخاص يستفيدون مع أفراد عائلتهم، بمفهوم المادة 14، من قانون الضمان الإجتماعي من تقديمات العناية الطبية في فرع ضمان المرض والأمومة شرط أنّ يتقدموا من الصندوق بطلب إنتساب وفقاً للأصول مع المستندات المطلوبة، وأن يتثبت الصندوق من تسديدهم للإشتراكات المتوجبة عليهم لثلاثة أشهر سابقة لتاريخ التثبت الطبي. وتحدد الإشتراكات المتوجبة على أصحاب العمل ومن في حكمهم على أساس المعدل العادي المعمول به على أساس كسب شهري مقطوع مقداره الحد

الأقصى للكسب الخاضع للإشتراكات المعمول بها في فرع ضمان المرض والأمومة. وتحدد دقائق تطبيق هذا المرسوم في نظام الصندوق الداخلي وفقاً لأحكام المادة 76 من قانون الضمان الإجتماعي.

الأسباب الموجبة: حيث أنّ القانون رقم 16/75 الصادر بتاريخ 1975/4/11 قد عدل بعض أحكام المادة التاسعة من قانون الضمان الإجتماعي وأضاف إلى البند "أ" من الفقرة أولاً المقطع "هـ" التالي نصه: "تحدد بمراسيم تتخذ في مجلس الوزراء بناء على اقتراح وزير العمل وإنهاء مجلس إدارة الصندوق وبالشروط المحددة فيها، فئات سائقي السيارات العمومية والحرفيين وسائر فئات الأشخاص اللبنانيين غير المذكورين في هذه المادة الذين يتبين طبيعة إخضاعهم منذ المرحلة الأولى لبعض أو جميع فروع الضمان الإجتماعي".

وحيث أنّ التجار ورؤساء مجالس الإدارة والمدراء العامين والمفوضين بالتوقيع في الشركات التجارية وهم شركاء أساسيون في نظام الضمان الإجتماعي اللبناني بصفتهم أصحاب عمل يصرحون عن أجرائهم ويسددون عنهم الإشتراكات المتوجبة.

كما أنّ غالبية التجار ينتمون إلى فئتي صغار أو متوسطي التجار وبمعظمهم غير خاضعين لأي نظام حماية إجتماعية يؤمن لهم ولأفراد عائلاتهم الاستقرار الإجتماعي والتغطية الصحية.

لذلك تم وضع هذا المرسوم لإخضاع هذه الفئة لأحكام فرع ضمان المرض والأمومة في الصندوق وإفادتهم من تقديمات العناية الطبية في هذا الفرع وتحديد الكسب المتخذ لحساب الإشتراكات بالحد الأقصى المعمول به لفرع ضمان المرض والأمومة وفقًا للمعدل العادي المعمول به في الصندوق على أنّ يبدأ الخضوع إعتبارًا من بداية الشهر السادس لنشر المرسوم في الجريدة الرسمية لجهة إستحقاق الإشتراكات وبداية الشهر التاسع للنشر لجهة استحقاق التقديمات.

أمّا بالنسبة للدراسة الإكتوارية ، فإنّ أهم ما ورد فيها إلى جانب الاحصاءات من خلال الدراسة بطريقة تقريبية:

نظراً للظروف الإجتماعية الدقيقة التي تعاني منها جميع فئات المجتمع اللبناني، بما في ذلك أصحاب المؤسسات والتجار والشركات التجارية، لجهة الارتفاع الهائل في نفقات الإستشفاء بالإضافة إلى الغلاء الفاحش في أقساط شركات التأمين الخاصة، لذلك لا بد من إيجاد نظام حماية اجتماعية يؤمن لهؤلاء نوعًا من الاستقرار الإجتماعي على صعيد المرض والأمومة، وذلك عن طريق إخضاع هذه الفئات إلى الصندوق الوطني للضمان الإجتماعي.

ونظراً لعدم توافر (حاليًا) معطيات إحصائية حول أصحاب هذه المؤسسات وأفراد عائلاتهم الذين يقع على عاتقهم استخراج ما يلزم من عناصر أهمها:[11]

- متوسط الأعمار لهؤلاء الأشخاص

[11] **مكتب الدراسات الاكتوارية، الصندوق الوطني للضمان الإجتماعي، مشروع انشاء نظام الزامي خاص بأصحاب المؤسسات والرامي الى استفادتهم من تقديمات فرع ضمان المرض والأمومة.**

- التكوين العائلي (متوسط عدد أفراد العائلة)
- عدد الزوجات على عاتق الزوج (لا تعمل)
- عدد الأولاد:
  - أقل من 18 سنة.
  - من 18 سنة لغاية 25 سنة.
- عدد الأهل (الأب والأم)

لخطورة هذا النظام، ولغياب كامل المعطيات الإحصائية الضرورية حول صاحب المؤسسة أو التاجر وأفراد عائلته الذين هم على عاتقه، وتجنباً من الوقوع بنتائج سلبية، كما حصل بالنظام الخاص للاختياريين، اقترح حضرة مدير عام الصندوق الوطني للضمان الإجتماعي الدكتور محمد كركي بمشروع القانون هذا، تعديل هذا الإشتراك برفع الأجر المعتمد البالغ أربع مرات وربع الحد الأدنى الرسمي للأجور بنسبة 10% أو 15% أو 20%.

وقد تقدم حضرة وزير العمل مصطفى بيرم بكتاب لجانب مجلس إدارة الصندوق الوطني للضمان الإجتماعي موضوعه مشروع مرسوم يرمي إلى خضوع أصحاب العمل ومن في حكمهم لأحكام قانون الضمان الإجتماعي – فرع المرض والأمومة، المحال إلى جانبهم بموجب كتاب المدير العام رقم 2569 تاريخ 2018/8/8 تضمن ما يلي:

يعاني أصحاب العمل لا سيما أصحاب المهن الحرة الحرمانَ من فرصة الإستفادة من الرعاية الصحية، وكذلك يشترك في هذه المعاناة أعضاء مجالس إدارة المؤسسات العامة والخاصة والشركات من حرمانهم من تقديمات الصندوق الوطني للضمان الإجتماعي.

بالرغم من أنّ قانون الضمان الإجتماعي قد أُلزِم باتخاذ التدابير المناسبة لإخضاع كافة العاملين وأصحاب العمل لأحكامه.

الخاتمة

يتضح أن إيجاد توازن فعلي بين خضوع أصحاب العمل للرقابة وتمكينهم من الاستفادة من تقديمات الضمان الاجتماعي هو أمر ضروري لتعزيز بيئة عمل سليمة ومستدامة في لبنان. فالرقابة وحدها لا تكفي مهما بلغت فعاليتها ما لم تترافق مع حقوق موازية لصالح أصحاب العمل الذين يشكلون العمود الفقري لتمويل النظام. كما ان استمرار حرمانهم من التغطية الصحية وسائر التقديمات يفاقم شعورهم بالغبن ويدفع بعضهم الى ممارسة مخالفات، سواء من خلال التهرب أو التصريح غير الدقيق أو إيجاد بدائل غير قانونية.

فبينما تضمن الرقابة القانونية تنفيذ الالتزامات المتعلقة بالتأمينات الاجتماعية بشكل فعال، كما وتضمن حقوق العمال وتحسن شروط العمل، فإنّ استفادة أصحاب العمل من الضمان الاجتماعي توفر لهم الحماية والمرونة لمواصلة نشاطاتهم التجارية بشكل قانوني وآمن وتؤمن حمايتهم من الازمات المحتملة خاصة في ظل الظروف الاقتصادية الصعبة التي يعاني منها لبنان.

إنّ الواقع القانوني القائم يكشف بوضوح أنّ استثناء أصحاب العمل من أي تغطية عبر الضمان الاجتماعي لم يعد يتلاءم مع حاجات سوق العمل ولا مع المبادئ الحديثة للحماية الاجتماعية. فاستمرار هذا الاستثناء يكرّس فجوة بين الالتزامات الواجبة على أصحاب العمل وبين غياب أي حماية مقابلة لهم، ما يستدعي مراجعة تشريعية جديّة تعيد التوازن إلى هذا النظام. ومن هنا، يصبح توسيع نطاق الضمان ليشمل أصحاب العمل خطوة ضرورية تساهم في تعزيز الأمان الاجتماعي، وتحقيق المساواة في الحقوق، ودعم استقرار البيئة الاقتصادية بشكل أكثر شمولية وعدالة.

لذا، فإن إدراج أصحاب العمل ضمن فئات المستفيدين من الضمان الاجتماعي لا يسهم فقط في تعزيز الحماية الاجتماعية، بل يشكل حجر أساس في تحديث نظام الحماية الاجتماعية وجعله اكثر عدالة وشمولية.

وللحد من الفساد وتحسين مستوى الامتثال. وفي ظلّ الأزمة الاقتصادية التي تعصف بلبنان، تبرز الحاجة الماسّة إلى إصلاحات قانونية شاملة تعيد هيكلة العلاقة بين الدولة وأصحاب العمل بما يخدم مصلحة الاقتصاد الوطني ويؤمّن استقرارًا مهنياً وصحيًا لجميع الفئات العاملة.

قائمة المراجع

- **القوانين**

- قانون الضمان الإجتماعي الإجتماعي.
- مشروع انشاء نظام الزامي خاص بأصحاب المؤسسات والرامي إلى استفادتهم من تقديمات فرع ضمان المرض والأمومة، مكتب الدراسات الاكتوارية، الصندوق الوطني للضمان الاجتماعي.

- **المراسيم والأنظمة**

- النظام رقم 19، نظام التفتيش ومراقبة أصحاب العمل

- **الكتب**

- شوفاني ناجي، شرح قانون الضمان الإجتماعي، الطبعة الأولى، د.ن، 2011
- علوية صادق، شرح قانون الضمان الإجتماعي وفق أحكام وإجتهادات الفقه والقضاء، الطبعة الأولى منشورات زين الحقوقية، بيروت، 2019

- **مقابلات**

- بو ناصيف شوقي ، مدير مالي ورئيس الديوان في الضمان الإجتماعي، تاريخ: 2024/4/5
- جواد نبيل ، مسؤول الدعم التقني والفني، مقابلة شخصية، الأربعاء 2019/4/10
- علوية صادق ، رئيس مصلحة الضمان الإجتماعي، الأربعاء 2019/4/10
- مهدي لينا، موظفة في الضمان الإجتماعي، مقابلة شخصية، تاريخ: 2024/3/21

مجلة مؤشر للدراسات الاستطلاعية
Journal index of exploratory studies
المجلد 07، العدد 20
ISSN: 2701-9233

الشركات العسكرية والأمنية الخاصة

وتأثير عملها على تطبيق مبدأ التمييز بين المدنيين والمقاتلين

Private Military and Security Companies and the Impact of Their Operations on the Application of the Principle of Distinction Between Civilians and Combatants

د. علاء الدين بو مرعي

الجامعة الاسلامية في لبنان

alaadinbumeri@gmail.com

الملخص

شهدت العقود الأخيرة تزايداً ملحوظاً في اعتماد الدول على الشركات العسكرية والأمنية الخاصة للقيام بمهام عسكرية وأمنية كانت تقليدياً من اختصاص القوات المسلحة النظامية، وذلك في إطار خصخصة الوظائف العسكرية وتخفيف الأعباء البشرية والمادية عن الجيوش الوطنية. غير أن هذا التوجّه أفرز إشكاليات قانونية معقّدة، في مقدمتها صعوبة تحديد الوضع القانوني لأفراد هذه الشركات أثناء النزاعات المسلحة، وما إذا كانوا يُصنَّفون كمقاتلين أم مدنيين، الأمر الذي ينعكس مباشرة على تطبيق مبدأ التمييز بين المدنيين والمقاتلين، بوصفه أحد المبادئ الأساسية للقانون الدولي الإنساني.

يناقش هذا البحث الطبيعة القانونية لأفراد الشركات العسكرية والأمنية الخاصة في ضوء قواعد القانون الدولي الإنساني، ولا سيما اتفاقيات جنيف والبروتوكول الإضافي الأول، من خلال تحليل مدى انطباق صفة المقاتل عليهم، أو اعتبارهم مدنيين يرافقون القوات المسلحة، وفقاً لطبيعة المهام التي يؤدونها ومستوى مشاركتهم في الأعمال العدائية. كما يتناول البحث أثر مشاركة هذه الشركات في النزاعات المسلحة على فاعلية مبدأ التمييز، وما تخلقه من غموض في عملية التصنيف، بما يؤدي إلى إضعاف الحماية المقررة للمدنيين، ويُعقِّد مسألة المساءلة القانونية عن الانتهاكات المرتكبة.

ويُبرز البحث أن غياب إطار قانوني دولي ملزم ينظم عمل الشركات العسكرية والأمنية الخاصة يسهم في اتساع فجوة الإفلات من المسؤولية، سواء على مستوى الدول المتعاقدة أو على مستوى الأفراد العاملين في هذه الشركات. كما يخلص إلى أن تحديد الصفة القانونية لأفراد الشركات يجب أن يتم على أساس كل حالة على حدة، وفق طبيعة النشاط المنفّذ، مع ضرورة التمييز بين المهام ذات الطابع المدني وتلك التي تشكل مشاركة مباشرة في الأعمال العدائية.

ويخلص البحث إلى التأكيد على الحاجة الملحّة لتطوير قواعد القانون الدولي الإنساني، أو اعتماد آليات دولية أكثر فاعلية، تضمن ضبط أنشطة الشركات العسكرية والأمنية الخاصة، وتحقيق التوازن بين متطلبات الواقع العملي للنزاعات المسلحة المعاصرة، والحفاظ على جوهر مبدأ التمييز، بما يكفل حماية المدنيين، ويضمن المساءلة عن انتهاكات القانون الدولي الإنساني.

الكلمات المفتاحية: الشركات العسكرية والأمنية الخاصة، مبدأ التمييز، المدنيون والمقاتلون، النزاعات المسلحة، القانون الدولي الإنساني، المشاركة المباشرة في الأعمال العدائية، المسؤولية الدولية، وثيقة مونترو.

Abstract

In recent decades, states have increasingly relied on private military and security companies to perform military and security functions that were traditionally the exclusive responsibility of regular armed forces. This trend has emerged within the broader context of the privatization of military functions and the reduction of human and material burdens on national armies. However, this development has generated complex legal challenges, foremost among them the difficulty of determining the legal status of personnel employed by these companies during armed conflicts and whether they should be classified as combatants or civilians. This ambiguity directly affects the application of the principle of distinction between civilians and combatants, which constitutes one of the fundamental principles of international humanitarian law.

This study examines the legal status of private military and security company personnel in light of the rules of international humanitarian law, particularly the Geneva Conventions and Additional Protocol I. It does so by analyzing the extent to which combatant status may apply to such personnel, or whether they should instead be regarded as civilians accompanying the armed forces, depending on the nature of the tasks they perform and the degree of their participation in hostilities. The study also explores the impact of these companies' involvement in armed conflicts on the effectiveness of the principle of distinction, and the ambiguity it creates in classification processes, which in turn weakens the protection afforded to civilians and complicates legal accountability for violations committed.

The study highlights that the absence of a binding international legal framework regulating the activities of private military and security companies contributes significantly to the widening accountability gap, both at the level of contracting states and at the level of individual company personnel. It further concludes that the determination of the legal status of such personnel must be conducted on a case-by-case basis, in accordance with the nature of the activities carried out, with a clear distinction drawn between tasks of a civilian nature and those amounting to direct participation in hostilities.

Finally, the study emphasizes the urgent need to develop international humanitarian law rules or to adopt more effective international mechanisms capable of regulating the activities of private military and security companies. Such measures are essential to striking a balance between the practical realities of contemporary armed conflicts and

the preservation of the core of the principle of distinction, thereby ensuring the protection of civilians and guaranteeing accountability for violations of international humanitarian law.

Keywords: Private Military and Security Companies; Principle of Distinction; Civilians and Combatants; Armed Conflicts; International Humanitarian Law; Direct Participation in Hostilities; International Responsibility; Montreux Document.

المقدمة

تمتد أصول الشركات العسكرية والأمنية الخاصة عميقاً في تاريخ الأعمال العسكرية والأمنية فقد كانت في أول انطلاقتها مجموعات صغيرة يُكَوِّنها أفرادٌ مرتزقة، وكانت بعض الدول تستأجرها لخوض الحروب ضدّ أعدائها. ثمَّ تصاعد دور تلك مجموعات، وتنامى حتى ظهر على الساحة الدولية ما يُعرَف، اليوم، باسم «الشركات العسكرية والأمنية الخاصة» التي صارت تُشكِّل قوة عسكرية مكوَّنة من أفراد مقاتلين، قادرة على القتال، وفرض السيطرة العسكرية الميدانية أثناء خوض النزاعات المسلحة، وقادرة على فرض الأمن، وحماية الجهات التي تعمل لصالحها.

وبالفعل فإن مشاركة الشركات العسكرية والأمنية الخاصة في الأعمال العدائية، تُؤثِّر على تطبيق مبدأ التمييز بين المدنيين والمقاتلين، نظراً إلى أن تلك المشاركة تنعكس على تصنيف أفراد الشركات، خصوصاً أن مشاركتهم في العمل العسكري مهما كان نوعه تجعل من خصمهم غير قادر على تصنيفهم بين مقاتلين وغير مقاتلين، وغير قادر على التعامل معهم.

وبالإضافة إلى ما سبق فإن العقدة الإجرائية المتصلة بتحديد التكييف القانوني لأفعال الأفراد العاملين ضمن الشركات يحول دون تمكين الطرف المتضرر من إثبات المسؤولية القانونية عن تلك الأفعال. وعليه، تنشأ ضرورة ملحة لتحديد الأطراف المسؤولة التي تتحمل تبعات الانتهاكات المرتكبة من قبل هؤلاء الأفراد.

وفي هذا السياق، فقد أسفرت ممارسات الشركات العسكرية والأمنية الخاصة في عدد من الدول عن خرق قواعد القانون الدولي الإنساني بشكل جسيم، نجم عنه إلحاق الضرر بالمدنيين. وقد أثارت هذه الوقائع تساؤلات جوهرية بشأن النطاق القانوني لعمل هذه الشركات وشرعية وجودها، مما حفز المجتمع الدولي والدول المعنية إلى السعي نحو صياغة صكوك دولية تهدف إلى تنظيم وتقنين أنشطة هذه الشركات، ومن أبرزها المبادرة المعروفة باسم «وثيقة مونترو».

وبالنظر إلى واقع عمل الشركات هذه وأفرادها في ميادين النزاع المسلح، وانعكاس هذا العمل على مبدأ التمييز بين المدنيين والمقاتلين، فإن دراسة هذا الواقع تكتسي أهميةً كبيرة تنبع من أن عمل أفراد الشركات في

ميادين النزاع يُشكل علامة فارقة في تطبيق مبدأ التمييز تُظهرها قضية تصنيف هؤلاء الأفراد بين مقاتلين أو غير مقاتلين. وما هذه الدراسة هنا إلا محاولةً للإضاءة على تصنيف هؤلاء الأفراد بين مقاتلين أو غير مقاتلين، ومحاولةً تهدف إلى كشف تأثير عمل هذه الشركات على مبدأ التمييز، وتحديد المسؤوليات الناتجة عن انتهاك القانون الدولي الإنساني.

وانطلاقاً مِمّا تقدم، فإن الشركات العسكرية والأمنية تقوم بدور أساسي في العمل العسكري الميداني مما يُشكل إطاراً عاماً يؤدي إلى خللٍ في تطبيق مبدأ التمييز بين المدنيين والمقاتلين، وعليه يمكن **طرح الإشكالية التالية: ما تأثير عمل هذه الشركات على تطبيق مقتضيات مبدأ التمييز؟**

وللإجابة عن هذه الإشكالية لا بدّ من تحديد الطبيعة القانونية لأفراد الشركات في حال تطبيق مُقْتَضَيات مبدأ التمييز، ودراسة تأثير عمل هذه الشركات على هذا المبدأ، ومن ثُمَّ تحديد الجهة التي يُمكن أن تتحمل مسؤوليات عن انتهاك أفراد الشركات القانون الإنساني ، وذلك في المبحثين الآتيين:

المبحث الأول: الطبيعة القانونية لأفراد الشركات العسكرية والأمنية الخاصة أمام مُقْتَضَيات مبدأ التمييز.

المبحث الثاني: تأثير عمل الشركات العسكرية والأمنية الخاصة على مبدأ التمييز والمسؤولية عن انتهاكِ هذه الشركات القانونَ الدولي الإنساني.

1. الطبيعة القانونية لأفراد الشركات العسكرية والأمنية الخاصة أمام مُقْتَضَيات مبدأ التمييز.

يَفْرِض مبدأ التمييز على أطراف أيّ نزاع مسلح أن يكونوا قادرين على تمييز المقاتلين عن المدنيين، وهذا الفرض يُوْجِب أن يقوم المقاتلون بتمييز أنفسهم عن المدنيين، ويُوْجِب ألّا يُشارك المدنيون مباشرة في الأعمال العدائية.

وتحديد الطبيعة القانونية لأفراد الشركات العسكرية والأمنية الخاصة أمام مُقْتَضَيات مبدأ التمييز يستوجب تحديد ما إذا كان هؤلاء الأفراد مقاتلين كمقاتلي القوات المسلحة النظامية، أم مدنيين يرافقون القوات المسلحة، فمبدأ التمييز يَفْرِض على أطراف النزاع المسلح تصنيف الأفراد المتواجدين في هذا النزاع، بين مقاتلين، ومدنيين، كي يُستطاع توجيه العمليات العسكرية ضدّ المقاتلين، دون المدنيين، ويَفْرِض على المدنيين عدم المشاركة في الأعمال العدائية كَيْلا يكونوا عُرضةً لِفُقْدانهم الحماية التي يُقِرُّها لهم القانون الإنساني الدولي.

وبما أن الشركات العسكرية والأمنية الخاصة تُشارك أثناء النزاعات المسلحة في الأعمال العدائية، فإنّ عليها التزام مبدأ التمييز، وعلى أفرادها الذين يُشاركون في هذه الأعمال أن يُميّزوا أنفسهم عن المدنيين بناءً على ما يقتضيه

هذا المبدأ، وعليه لا بدّ من دراسة حالهم أمام مقتضيات هذا المبدأ، وذلك في المطلبين الآتيين:

المطلب الأول: أفراد الشركات العسكرية والأمنية مقاتلون .

المطلب الثاني: أفراد الشركات العسكرية والأمنية الخاصة مدنيون يرافقون القوات المسلحة.

1.1. أفراد الشركات العسكرية والأمنية مقاتلون.

إنّ تحديد كون أفراد الشركات العسكرية والأمنية الخاصة مقاتلين، أم غير مقاتلين يُوْجِبُه ثلاثة أمور: أولها تَمَكُّن القوات المُواجِهَة لهؤلاء الأفراد من معرفة ما إذا كانوا أهدافاً عسكرية شرعية يمكن مهاجمتها بشكل قانوني، أم لا. وثانيها معرفة ما إذا كانوا يشاركون في الأعمال العدائية بشكل قانوني أم لا، وثالثها معرفة ما إذا كان بالإمكان محاكمتهم نتيجة مشاركتهم في الأعمال العدائية، أم لا.

أمّا عملية تحديد وَضْع المقاتل فترتبط بعضويته في القوات المسلحة التابعة لطرف ما في النزاع، أو بعضويته في ميليشيات، أو في وحدات متطوعة تستوفي معايير محددة، وتنتمي إلى هذا الطرف. وعند تقويم حالة أفراد الشركات العسكرية والأمنية الخاصة، من الضروري تقويم اندماجهم في القوات المسلحة، أو قدرتهم على تلبية متطلبات التأهّل ليكونوا كأفراد الميليشيات المنصوص عليهم في الفقرة ألِف (2) من المادة 4 من اتفاقية جنيف الثالثة، أو تقويم ما إذا كان قد تَمَّ دمجهم في القوات المسلحة كما هو منصوص عليه في الفقرة ألِف (1) من المادة 4 من اتفاقية جنيف الثالثة. ومن الضروري، كذلك، تقويم ما إذا كان أفراد الشركات الخاصة مدمجين في القوات المسلحة التابعة لأحد أطراف النزاع، على النحو المحَدَّد في المادة 43 من البروتوكول الإضافي الأول.

وفي حقيقة الأمر يمكن التصور أنّه إذا تَمَّ دمج جميع أفراد الشركات في القوات المسلحة، فمن شأن ذلك أن يَحُلَّ جميع القضايا المتعلقة بتنظيم أفراد الشركات، ويَحُلّ مشاكل تصنيفهم وفق ما يقتضيه مبدأ التمييز والقانون الإنساني الدولي، ولكن هذا التصور يبدو غير واقعي في ظلّ لجوء الدول إلى خصخصة الأعمال العسكرية الحكومية، ولجوئها إلى الاستعانة بمصادر خارجية للقيام بالمهام العسكرية والأمنية.

وبناءً على ما تقدم يصحّ القول: إنّ أفراد الشركات العسكرية والأمنية الخاصة يُمْكِن أن يكتسبوا صفة مقاتل بإحدى طريقتين: أُولاهما، بالاستناد إلى المادة 43 من البروتوكول الإضافي الأول[12]؛ وثانيتهما،

([12]) المادة 43 من البروتوكول الإضافي الأول تعرف "القوات المسلحة" بأنها جميع القوات المسلحة المنظمة والمجموعات والوحدات التي تكون تحت قيادة مسؤولة أمام طرف في النزاع عن سلوك مرؤوسيها، حتى لو كان ذلك الطرف ممثلاً بحكومة لا يعترف بها الطرف الآخر. تضع هذه المادة تعريفاً للقوات المسلحة يشمل القوات النظامية وغير النظامية، بهدف تحديد من هم المقاتلون الذين يحق لهم وضع أسرى الحرب. راجع البروتوكول الإضافي الأول لعام 1977.

بالاستناد إلى الفقرة ألِف من المادة 4 من اتفاقية جنيف الثالثة[13].

إنّ أفراد الشركات العسكرية والأمنية الخاصة يعملون ضمن مجموعة عسكرية متكاملة، ولا يعملون منفردين كُلٌّ على حِدة، وبالتالي فإنّ عليهم احترام قواعد الحرب وعاداتها.

وعلى الرغم من أنّ الامتثال لِشَرط الالتزام بقواعد الحرب وعاداتها ليس صعباً، فإنّ الممارسات العملية التي يقوم بها أفراد الشركات ومجموعاتهم لا تُظهر أنهم مستعدون لتلبية هذا الشرط، ولا للامتثال للقانون الإنساني الدولي. فلقد أظهرت حوادث عديدة أن الشركات وأفرادها لا يلتزمون قواعد الحرب وعاداتها، ولا القانون الإنساني الدولي، فعلى سبيل المثال، تَوَرَّط العاملون في الشركات العاملة في العراق بحوادث إطلاق نار، واعتداءات ضدّ مدنيين. وفي كثير من هذه الحوادث كان هؤلاء العاملون هم مَنْ بدأوا الاعتداء، وإطلاق النار.

ومما تقدم يبدو أن أفراد الشركات العسكرية والأمنية الخاصة لا يُلَبّون الشروط الواردة في الفقرة ألِف من المادة 4 من اتفاقية جنيف الثالثة، بسبب ممارساتهم التي تَحيدُ عن القواعد القانونية السليمة، ولأنهم يُنَفِّذون أعمالهم بطريقة لا يريدون فيها أن يكونوا مسؤولين عن انتهاكات، أو حوادث يسقط فيها ضحايا مدنيون. وبالتالي فهُمْ لا يمكن أن يكونوا مقاتلين شرعيين كمقاتلي القوات المسلحة التابعة للدول ولا مقاتلين كمقاتلي الميليشيات، أو الوحدات المتطوعة المندمجة في القوات المسلحة.

2.1. أفراد الشركات العسكرية والأمنية الخاصة مدنيون يُرافقون القوات المسلحة

يَرِد في الفقرة ألِف (1و2) من المادة 4 من اتفاقية جنيف الثالثة مبدأ مفاده أن المقاتلين المؤلَّفين من أفراد القوات المسلحة، والميليشيات، ووحدات المتطوّعين، المنتمين إلى القوات المسلحة، يحق لهم، وحدهم، أن يتمتعوا بوَضْع أسرى الحرب عند وقوعهم في الأسر، ولكن الفقرة ألِف (4) من المادة نفسها يَرِد فيها استثناءٌ محدود مفاده أن هناك فئة أخرى من الأشخاص الذين يحق لهم التمتع بوَضْع أسير حرب عند وقوعهم في الأسْر هم: «الأشخاص الذين يرافقون القوات المسلحة دون أن يكونوا في الواقع جزءاً منها، كالأشخاص المدنيين الموجودين ضمن أطقم الطائرات الحربية، والمراسلين الحربيّين، ومتعهّدي التموين، وأفراد وحدات العمال أو الخدمات المختصة بالترفيه عن العسكريين، شريطة أن يكون لديهم تصريح من القوات المسلحة التي يرافقونها، والتي يجب عليها أن تزوّدهم لهذا الغرض ببطاقة هويّة»[14].

---

(13) المادة 4 من اتفاقية جنيف الثالثة تحدد الأشخاص الذين تحميهم الاتفاقية في أوقات النزاع أو الاحتلال، وهم أي شخص يجد نفسه تحت سلطة طرف في النزاع ليس من رعاياه، أو تحت سلطة دولة احتلال ليس من رعاياها. لا تشمل هذه المادة رعايا الدولة غير المرتبطة بالنزاع، ولكنها تمنح رعايا الدول المحايدة ورعايا الدول المتحاربة حماية محدودة إذا كانت دولهم ممثلة دبلوماسياً في الدولة الواقعة تحت سلطتها. راجع اتفاقية جنيف الثالثة لعام 1949.

(14) Para. (A) (4) of article 4 of *Geneva Convention III*, relative to the treatment of prisoners of war of 12 august 1949.

أمّا الأمر الذي يفتقر إلى الوضوح الكافي في هذه الفقرة فهو أنها لا تُعطي قائمة شاملة بمقدمي الخدمات الذين يمكن أن يرافقوا القوات المسلحة، لكونها قائمة إرشادية فحسب. وليس في التعليق على اتفاقية جنيف الثالثة ما يُلقي الضوء على حدود الأنشطة التي يمكن لهذه الفئة من الأشخاص القيام بها، فالتعليق يَذْكُر، فقط، أنّ «القائمة المقدمة هي للإشارة، مع ذلك يُمكن لنصّ [الفقرة ألِف (4)] أن يشمل فئات أخرى من الأشخاص الذين قد يُطلب منهم، في ظروف مماثلة، مرافقة القوات المسلحة أثناء أي نزاع»[15]. وهذا يعني أن إدراج فئة من المدنيين المرافقين للقوات المسلحة في الفقرة ألِف (4)، وإدراج أنشطتها التي يمكن أن تقوم بها على سبيل المثال لا الحصر، وإضفاء صفة «غير المقاتل» عليها، أمورٌ تُبَيّن أن المقصود من هذه الفقرة ألّا تَشْمَلَ فئةُ المدنيين هذه أشخاصاً يقومون بأنشطة تُعَدّ مشارَكة مباشرة في الأعمال العدائية. وأمّا الأمر الذي لا يفتقر إلى الوضوح في هذه الفقرة فهو أنها اشترطت لهذه الفئة من الأشخاص وجوب أن يكون لديها تصريح من القوات المسلحة التي ترافقها، وأن يحمل أفرادها بطاقات هويَّة تُعَرِّفُهم.

وفي ما يتعلق بأفراد الشركات العسكرية والأمنية الخاصة فإنّ انتماءهم إلى فئة المدنيين الذين يرافقون القوات المسلحة، ومنحهم وَضْع أسير حرب، مرهون بوجود تصريح بمرافقة القوات المسلحة، يُمْنح لهم من قِبَل هذه القوات، ويتضمَّن تحديد الوظيفة التي يؤدونها.

وفي اجتماع حول «مقاولي الشركات العسكرية الخاصة» عَقَده في العام 2005 خبراء قانونيون، جرى نقاشٌ حول أفراد الشركات، رأى فيه أحد الخبراء أن الدول لا يمكنها ببساطة منح وَضْع أسير حرب لأفراد الشركات الذين استأجرتهم بمجرد إصدار بطاقة هويَّة لهم؛ فلا بُدّ من وجود صلة بينهم وبين القوات المسلحة، ورأى، أنّه إذا ما تمّ وصف أفراد الشركات بأنهم أشخاص يرافقون القوات المسلحة، فمن غير الواضح ما إذا كان هذا يعني أن على أفراد القوات المسلحة أن يكونوا حاضرين فعلياً حيث تعمل الشركات الخاصة أم لا، ولكن على الأقل، يجب أن يُقَدِّموا نوعاً من الخدمة للقوات المسلحة لا أن يكونوا مجرد مُنَفِّذي عقد للدولة التي تَتْبَع لها هذه القوات[16]. وبالنظر إلى هذا الرأي يمكن القول: إن أفراد الشركات يمكنهم أن يكونوا مدنيين يرافقون القوات المسلحة إذا كانوا يقدِّمون لهذه القوات خدمات ذات طابع مدني، ويحملون تصريحاً بالعمل، وبالتالي يمكنهم التمتع بوَضْع أسير حرب إذا ما وقعوا في الأسْر، شرط ألّا يشاركوا في أعمال عدائية. ولا يمكن أنْ تُعَدّ العقود التي تنشأ بين الشركات والدول تصريحات بمرافقة القوات المسلحة.

---

[15] Jean De Preux, Commentary on Geneva convention III 1949, translated to English by A.P. de Heney, (Geneva: ICRC, 1960), p. 64.

[16] *Report of the Expert Meeting on Private Military Contractors: Status and State Responsibility for their Actions*, organized by the University Centre for International Humanitarian Law, Geneva, (29, 30 August 2005), p. 14_15. (https://docplayer.net/117880-Expert-meeting-on-private-military-contractors-status-and-state-responsibility-for-their-actions.html) (Last site visit november 2025).

هذه الفئة من الأشخاص المرافقين للقوات المسلحة لا تُعَدّ مؤهَّلة لتكون مقاتلة أثناء النزاعات المسلحة، ولا يمكنها المشاركة في الأعمال القتالية بصورة مباشرة، كما أنها مستثناة من أن تُعَدّ فئة من المدنيين لأن الفقرة الأولى من المادة 50[17] من البروتوكول الإضافي الأول استثنت هؤلاء الأشخاص من تعريف المدني، فهُمْ يُعامَلون على أنهم أسرى حرب في حال وقوعهم في قبضة العدوّ أثناء النزاع المسلح بمقتضى المادة 4 من اتفاقية جنيف الثالثة.

ومن الواضح أن طبيعة الأنشطة المدرجة في الفقرة ألِف (4) من المادة 4، باستثناء نشاط الأفراد المدنيين العاملين ضمن أطقم الطائرات الحربية، تتعلق جميعها بعمليات الدعم والخدمات، ولا ترتبط بالوظائف القتالية الخاصة بالقوات المسلحة، وهذا دليل على وجود شرط ضمني في هذه الفقرة مؤدّاه أن التمتع بوَضْع أسير الحرب يُوْجِب على الأفراد المعنيين ألّا يشاركوا في الأعمال القتالية مشاركةً مباشرةً[18].

وهذا الشرط الضمني لا يحظى بالموافقة على المستوى الدولي، فَوِزارة الدفاع الأمريكية، مثلاً، لديها موقف خاص مفاده أن هؤلاء الأشخاص الذين يقعون في نطاق الفقرة ألِف (4) من المادة 4، ويرافقون القوات المسلحة لا يفقدون وَضْع أسير الحرب نتيجة مشاركتهم المباشرة في الأعمال العدائية، إذا ما تَمَّ القبض عليهم[19]. أما مُبَرِّر هذا الموقف فحقيقةٌ مفادها أن الفقرة ألِف (4) من المادة 4 تشمل أشخاصاً معينين قد يُتوقّع منهم المشاركة المباشرة في الأعمال العدائية في ظروف معينة، كالأشخاص المدنيين العاملين ضمن أطقم الطائرات العسكرية[20].

وإذا ما تمّ القبول بهذا الموقف، وبأنْ ليس هناك شرط ضمنيّ في الفقرة ألِف (4) من المادة 4 يَمنع الأشخاص الذين يرافقون القوات المسلحة من المشاركة المباشرة في الأعمال العدائية، عندها يمكن للدولة في

---

(17) الفقرة 1 من المادة 50 من البروتوكول الأول: «المدني هو أي شخص لا ينتمي إلى فئة من فئات الأشخاص المشار إليها في البنود الأول والثاني والثالث والسادس من الفقرة (أ) من المادة الرابعة من الاتفاقية الثالثة والمادة 43 من هذا اللحق "البروتوكول". وإذا ثار الشك حول ما إذا كان شخص ما مدنياً أم غير مدني فإن ذلك الشخص يُعَدّ مدنياً». راجع، شريف عتلم، محمد ماهر عبد الوهاب، موسوعة اتفاقيات القانون الدولي الإنساني، النصوص الرسمية للاتفاقيات والدول المصدقة والموقعة، ط. 6، (القاهرة: إصدار بعثة اللجنة الدولية للصليب الأحمر بالقاهرة، 2002)، ص 290.

(18) Emanuela-Chiara Gillard, Business goes to war: Private/Security Companies and International Humanitarian Law, International Review of the Red Cross, Vol. 88, No. 863, (September 2006) (pp. 525_ 572). p. 538.

(19) Ibid, p. 538.

(20) *Report of the Expert Meeting on Private Military Contractors: Status and State Responsibility for their Actions, organized by the University Centre for International Humanitarian Law, Geneva, (29, 30 August 2005), p. 14_15. (https://docplayer.net/117880-Expert-meeting-on-private-military-contractors-status-and-state-responsibility-for-their-actions.html) (Last site visit november 2025)*, p. 14.

هذه الحال أن تسمح لشركة خاصة بمرافقة قواتها المسلحة، وبإصدار بطاقات هوية لأفراد هذه الشركة، وبالتالي يصبح هؤلاء جميعاً ضمن الفقرة ألِف (4) من المادة 4، سواء أشاركوا مباشرة في الأعمال العدائية أم لم يشاركوا[21] . وهذا يعني أنه يمكن منح أفراد الشركات صفة المدنيين المرافقين للقوات المسلحة، ولكن هذا الأمر غير مقبول لأن منحهم هذه الصفة يجعل أفراد الشركات الذين يشاركون في الأعمال العدائية أشخاصاً محميّين، ولهم حق التمتع بوَضْع أسير حرب، وهذا مخالف للمنطق القانوني الذي يرفع الحماية عن الأشخاص المدنيين الذين يشاركون في الأعمال العدائية بشكل غير قانوني، طوال مدة مشاركتهم تلك.

وانطلاقاً من التحليل السابق، يمكن القول: إن أفراد الشركات العسكرية والأمنية الخاصة الذين يقدمون خدمات غير قتالية (كالتموين) هم مدنيون مرافقون للقوات المسلحة، بشرط حصولهم على ترخيص رسمي. أما الذين يؤدون مهاماتٍ قتالية (كصيانة الأسلحة)، فلا ينطبق عليهم هذا التصنيف. لذلك، يجب تحديد صفة كل فرد بناءً على طبيعة عمله.

2. **تأثير عمل الشركات العسكرية والأمنية الخاصة على مبدأ التمييز، والمسؤولية عن انتهاكِ هذه الشركات القانونَ الدولي الإنساني.**

إن مشاركة الشركات العسكرية والأمنية الخاصة في الأعمال العدائية يطرح عدداً من القضايا القانونية تتعلق بمبدأ التمييز، ويفرض تحدّياتٍ تتعلق بتطبيق هذا المبدأ، وبتطبيق الحماية الخاصة بالمدنيين، والأعيان المدنية، وتحدّياتٍ أُخَرَ تتعلق بتحديد المسؤوليات عن انتهاك القانون الإنساني.

فتواجد الشركات العسكرية والأمنية الخاصة في مناطق النزاعات المسلحة، ومشاركتُها في الأعمال العدائية، يطرح قضايا قانونية تتعلق بحالها إزاء مبدأ التمييز، ولا سيّما ما يتصل من هذه القضايا بتصنيف أفراد هذه الشركات بين مقاتلين ومدنيين، وما يتصل باعتماد مفهوم المشاركة المباشرة في الأعمال العدائية من أجل تحديد حقوق الشركات، ومسؤولياتها، وتُثير مشاركتُها في الأعمال العدائية، فوق ذلك، قضية المسؤولية عن انتهاكها هي وأفرادُها القانون الإنساني الدولي.

ومن هذا المنطلق لا بدّ من بحث هذه القضايا القانونية التي يطرحها عمل الشركات العسكرية والأمنية، وذلك في مطلبين:

1.2. تأثير عمل الشركات العسكرية والأمنية الخاصة على مبدأ التمييز.

تُشارك الشركات العسكرية والأمنية الخاصة أثناء النزاعات المسلحة في الأعمال العدائية، مشاركةً تُؤثِّر على

---

[21] Ibid, p. 14.

تطبيق مبدأ التمييز، بسبب انعكاسها على قضية تصنيف أفراد الشركات، فاشتراك هؤلاء في الأعمال العدائية، يُصَعِّب على خصمهم عملية تصنيفهم، وكيفية التعامل معهم، لأنه من غير المعروف لديه قَبْل دخول المعركة ما صفة أفراد هذه الشركات، أَمُقاتلون هم أم مدنيون؟ وصعوبة عملية التصنيف هذه تُفْقِدُ المتضرّر من عمل أفراد الشركات القدرة على تحميلهم مسؤوليات أفعالهم، لذلك تظهر الحاجة إلى معرفة الجهات التي تتحمل مسؤولية الانتهاكات التي يرتكبها هؤلاء الأفراد. فالشركات العسكرية والأمنية الخاصة التي عملت في بعض الدول، ارتكبت انتهاكات للقانون نتج عنها إضرار بالمدنيين، ساهم في ظهور علامات استفهام حول دور هذه الشركات وحول قانونية عملها، الأمر الذي دفع بعض الدول إلى محاولات وَضْع وثائق دولية تُقَنِّن عمل هذه الشركات، على شاكلة المحاولة التي سُمِّيَت «وثيقة مونترو»[22].

ومن خلال دراسة القواعد التي تتصل بتحديد الصفة القانونية للمقاتل النظامي يبدو أنّه بالإمكان دمج أفراد الشركات العسكرية والأمنية الخاصة ضمن القوات المسلحة التابعة للدول، وبالإمكان معاملتهم على أنهم مقاتلون شرعيون كأفراد القوات المسلحة، إلا أن الممارسات الدولية تدل على أن الدول التي تَستخدِم أفراد الشركات لا تَعُدُّهم أعضاء في قواتها المسلحة النظامية، فهي تستأجر خدماتهم لتنفيذ مهمات معينة، ثمَّ تتركهم يُغادرون بعد تنفيذ تلك المهمات، ولا مجال لدمجهم في القوات المسلحة. هذا الواقع، يُرتّب أن أفراد الشركات غير مؤهلين ليكونوا مقاتلين كمقاتلي القوات المسلحة، بل يبقون أفراداً يُنَفِّذون عقوداً تُبرمها شركاتهم مع الدول.

إنّ أفراد الشركات العسكرية والأمنية الخاصة الذين يقدِّمون للقوات المسلحة خدمات لا تصل إلى مستوى المشاركة المباشرة في الأعمال العدائية، كخدمات التموين، والمطبخ، وغسل الملابس، وغيرها من الخدمات التي لا ترتبط بالقتال، يمكن أن يندرجوا ضمن فئة الأشخاص الذين يرافقون القوات المسلحة شرط أن يحصلوا على الترخيص اللازم من القوات المسلحة والدولة المعنية، لا أن يكون عملهم مقتصراً، فقط، على تنفيذ عقد مُبْرَم مع الدولة. أما أفراد الشركات الذين يقدِّمون خدمات تقترب من صميم العمليات العسكرية، كتحميل الأسلحة، وصيانة الدبابات، وتشغيل الطائرات الحربية، وأنظمة الدفاع الجوي، فلا يمكن إدراجهم ضمن فئة المدنيين المرافقين للقوات المسلحة، لأن هؤلاء يشاركون في الأعمال العدائية[23]. وبالتالي لا بدّ من الفصل في أمر تحديد صفة أفراد الشركات على أساس كل حالة على حدة، أيْ بناءً على طبيعة الأنشطة التي تقوم بها الشركات العسكرية والأمنية الخاصة وأفرادها.

([22]) راجع، **وثيقة مونترو بشأن الالتزامات القانونية الدولية والممارسات السليمة للدول ذات الصلة بعمليات الشركات العسكرية والأمنية الخاصة أثناء النزاع المسلح**، مونترو، 17 أيلول 2008، واردة ضمن رسالة موجهة إلى الأمين العام من الممثل الدائم لسويسرا لدى الأمم المتحدة، الجمعية العامة مجلس الأمن، الدورة 63، السنة 63، وثيقة رقم (A/63/467–S/2008/636).

([23]) *Report of the Expert Meeting on Private Military Contractors, op. cit* p. 14_15.

وبناءً على ما تقدم، يبدو أنه من المهم تحديد إذا ما كانت فرضية أن أفراد الشركات العسكرية والأمنية الخاصة مدنيون أمراً مقبولاً بموجب مبدأ التمييز.

إن المدني شخص لا ينتمي إلى القوات المسلحة، ولا يشارك مباشرة في الأعمال العدائية[24]، هذا التعريف يَحُلّ، من الناحية النظرية، المشكلة المتعلقة بوَضْع أفراد الشركات العسكرية والأمنية الخاصة، أيْ أنه يمكن الاستنتاج أنّ أيَّ فردٍ من أفراد الشركات لا ينتمي إلى القوات المسلحة، ولا يشارك مباشرة في الأعمال العدائية، يُعَدّ مدنياً، وهذا يعني أن الأفراد الذين لا يتأهّلون ليكونوا مقاتلين هم مدنيون، وبالتالي هم أشخاص مَحْمِيّون، بموجب القانون الدولي الإنساني، من الاستهداف، وليس لهم الحق في المشاركة المباشرة في الأعمال العدائية.

ولكن القول: إنّ أفراد الشركات العسكرية والأمنية الخاصة هم مدنيون سيكون له عواقب تُؤثِّر على فاعليَّة مبدأ التمييز. لأن هؤلاء الأفراد لن يكونوا قادرين على تمييز أنفسهم عن المقاتلين في ميادين النزاعات المسلحة، فمعظمهم يقوم بأدوار قتالية، ويشارك مباشرة في الأعمال العدائية، وبالتالي لن يكون الطرف خَصْمُ هؤلاء الأفراد قادراً على معرفة كيفية التعامل معهم سواء في أثناء القتال، أم في أثناء وقوعهم أسرى لديه، ولن يكون المتضرّرون من أفعالهم قادرين على مقاضاتهم أمام المحاكم. لذلك لا بدّ من أن تعمل الشركات على تصنيف أفرادها وتحديد وظائفهم، وعلى التفريق بين مَنْ يعمل في وظيفة مدنية، وبين مَنْ يعمل في وظيفة عسكرية، لأن اشتراك أفراد الشركات في الأعمال العدائية يجب أن يُوْضَع له حدّ بشكل يمنع عملهم غير القانوني، فتنفيذ العقود التي تُبرمها شركاتهم مع دولة ما قد لا يتضمن أيّ إشارة تدلّ على إمكانية مشاركتهم في النزاعات المسلحة.

ويبدو أن تزايد الاعتماد على الأفراد المدنيين التابعين للشركات العسكرية والأمنية الخاصة في هذه الأدوار التي تُعَدّ، فعلاً، تصرفات يُمكن تفسيرها على أنها مشاركة مباشرة في الأعمال العدائية يكون ذا تأثير بالغ سلبيّ على تطبيق مبدأ التمييز، وعلى القانون الدولي الإنساني.

ويبدو أن اعتماد مفهوم المشاركة المباشرة في الأعمال العدائية لا يُساهم في تحديد حقوق الشركات العسكرية والأمنية الخاصة، ولا في تحديد مسؤولياتها، ولا يُساهم في تصنيف أفرادها، نظراً إلى صعوبة تحديد معنى مفهوم المشاركة المباشرة في الأعمال العدائية، وصعوبة تحديد الأنشطة التي ترقى إلى حدّ المشاركة المباشرة في الأعمال العدائية[25]. ونظراً إلى أن الدول لا تُوَفِّر توجيهات واضحة تساعد في تحديد الأنشطة التي تُشكّل

([24]) راجع، شريف عتلم ومحمد ماهر عبد الوهاب، موسوعة اتفاقيات القانون الدولي الإنساني، مرجع سابق، ص 354.

([25]) نيلس ميلزر، **دليل تفسيري لمفهوم المشاركة المباشرة في العمليات العدائية بموجب القانون الدولي الإنساني**، اللجنة الدولية للصليب الأحمر، الطبعة العربية الأولى، (القاهرة: المركز الإقليمي للإعلام، مارس/آذار 2010، ص 52).

مشاركة مباشرة في الأعمال العدائية، وإنّ هذا الأمر يؤدي إلى استحالة معرفة متى يمكن أن يكون أفراد الشركات المدنيون عُرضةً للهجوم، لأن كل طرف في النزاع قد يَستخدِم فَهْمَه الشخصي لمفهوم المشاركة المباشرة في الأعمال العدائية، ويعمل على تطبيقه على أفراد الشركات.

إنّ تصنيف أفراد الشركات العسكرية والأمنية الخاصة مقاتلين ومدنيين، والفصلَ بين هذين الصنفين، لا يؤدّيان إلى الوضوح التّام، لأن هؤلاء الأفراد لا يحكم عملَهم قانونٌ واضح، وهم لا يلتزمون مبادئ القانون الدولي الإنساني، فهُمْ لا يصَنِّفون أنفسهم على أنهم صِنفان: مقاتلون نظاميون، ومدنيون عاديون، بل يحاولون دائماً الإفلات من هذا التصنيف، ويَعُدّون أنفسهم مدنيين، وهذا ما لا يُمكن القبول به قانوناً. لذلك لا بُدّ من أنْ يُصَنّف أفراد الشركات، وأن يُعَدّ بعضُهم مقاتلين بناءً على طبيعة عملهم العسكري، وبعضُهم الآخر مدنيين بناءً على طبيعة عملهم المدني، ولا بُدّ من تأكيد هذا التصنيف في مواثيق دولية تتفق الدول عليها، وتَتَّبِعها الشركات العسكرية والأمنية الخاصة، فتلتزم بقواعد القانون الدولي الإنساني، وتتحمل المسؤولية عن أفعالها.

2.2. المسؤولية عن انتهاك الشركات العسكرية والأمنية الخاصة القانون الدولي الإنساني.

وفي إطار الحديث حول المسؤولية عن انتهاك الشركات العسكرية والأمنية الخاصة القانون الدولي الإنساني يمكن القول: إنّ الدول تتحمل المسؤولية عن ارتكاب الشركات العسكرية والأمنية الخاصة انتهاكاتٍ للقانون الإنساني الدولي، وذلك بموجب نصوص البروتوكول الإضافي الأول، ونصوص القانون الدولي العرفي، وقواعد مسؤولية الدول[26]. إلا أن هذه النصوص والقواعد الحالية ضَيِّقة حيناً، وغامضة حيناً آخر، ويَتَعذّر تطبيقها على جميع حالات استعانةِ الدول بخدمات الشركات العسكرية والأمنية الخاصة. وفي هذه النصوص والقواعد ثغرات يمكن للدول أنْ تَنْفُذ منها كي تتهرَّب من المسؤولية عن انتهاك الشركات القانون الإنساني، ومبادئه. والدول تميل، عادةً، إلى عدم تحمّل المسؤولية عن أي انتهاكات، وما استعانتها بالشركات العسكرية والأمنية إلّا تهرّب من تحمّل هذه المسؤولية، وقد أظهرت ممارسات الدول أنها، في كثير من الأحيان، تلجأ إلى التنصّل من الأعمال غير القانونية، ومن الانتهاكات التي قد تقوم بها الشركات وأفرادها، وهذا ما يُعيق عملية ملاحقة الدول قانونياً أمام المحاكم الجنائية الدولية، ويمنع المتضررين من أفعال الشركات من أن يحصلوا على العدالة.

وما يزيد الأمر صعوبةً، أن الدول التي يتورَّط مواطنوها في انتهاكات وعمليات عسكرية في دول أجنبية، قد لا يكون لديها المعلومات اللازمة لمحاكمتهم، أو التحقيق في الانتهاكات والجرائم التي ارتكبوها، أو قد لا يكون لديها القدرة على جلب الشهود اللازمين لإجراء المحاكمة.

([26]) راجع **مشاريع المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً**، تقرير لجنة القانون الدولي إلى الجمعية العامة عن أعمال دورتها الثالثة والخمسين، حولية لجنة القانون الدولي، م. 2، ج. 2، (الأمم المتحدة: 2001، ص 32).

وبالتالي، فإنّ مقاضاة أفراد الشركات أمر شديد الصعوبة لأسباب، أولها عدم قدرة الدول على تأمين نظام قانوني يساعد في تَتَبُّع أفراد الشركات، وفي التحقيق في جميع الانتهاكات والجرائم التي يرتكبونها. وثانيها الطريقة الخاصة التي تعمل بها الشركات، والتي لا تسمح بتحديد الأفراد الذين يقومون بانتهاكات إذْ إنّ هؤلاء قد يُغادرون مكان عملهم فَوْر انتهاء عقودهم مع الشركة، ويصبح من المستحيل ملاحقتهم. وثالثها عدم اتّباع الشركات في عملها نظاماً قانونياً خاصاً تستند إليه، ويسمح لها بملاحقة أفرادها المتورطين في المخالفات والانتهاكات.

وبالإضافة إلى ما سبق يمكن القول: إنّ القواعد القانونية التي تلحظ مسؤولية الدولة، ومسؤوليتَي الفرد والقيادة، ليست مناسبة للتطبيق على أنشطة الشركات العسكرية والأمنية الخاصة أثناء النزاعات المسلحة، والسبب في ذلك يرجع إلى العلاقة غير الواضحة بين الدول وهذه الشركات، وإلى الطريقة الغامضة التي تعمل بها هذه الشركات. وبالتالي، ينشأ عن ذلك حاجة إلى نظام قانوني يرعى شؤون التعامل بين الدول والشركات العسكرية والأمنية الخاصة، ويُمَكِّنُ من الاستعانة به لتحديد الأطراف المسؤولة عن انتهاك القانون الدولي الإنساني أثناء النزاعات المسلحة.

الخاتمة

بعد دراسة تأثير عمل الشركات العسكرية والأمنية الخاصة على تطبيق مبدأ التمييز فإنه يمكن الاستنتاج أنه في السنوات الأخيرة تزايد اعتماد الدول على متعاقدين مدنيين لأداء مهام عسكرية كانت حكراً على قواتها المسلحة، ويُعزى ذلك إلى عوامل عدة، منها: الرغبة في تقليص حجم الجيوش النظامية وخفض نفقاتها، والحاجة إلى خبرات فنية متخصصة لتشغيل التقنيات الحربية الحديثة، مثل أنظمة الذكاء الاصطناعي والفضاء السيبراني.

وقد أدى هذا التوجه إلى ظهور تحديات أمام تطبيق مبدأ التمييز بسبب ظهور فئة من الأفراد يصعب تحديد وضعهم القانوني بدقة. فغموض صفتهم القانونية يحول دون معرفة ما إذا كانوا مقاتلين أم مدنيين، مما يثير إشكاليات حول مدى أهليتهم للمشاركة المباشرة في الأعمال العدائية، وحول نطاق الحقوق والواجبات المترتبة عليهم بموجب القانون الدولي الإنساني.

هؤلاء المقاولون المدنيون الذين تَعْتَمِد عليهم الدول أثناء النزاعات المسلحة لا يجوز لهم المشاركة في الأعمال العدائية، لأن مبدأ التمييز يقضي بأن يشارك المقاتلون في الأعمال العدائية، وبأن يمتنع المدنيون عن هذه المشاركة. وبما أنّ الدول لا تتخلى عن ممارسة استخدام مقاولين مدنيين كأفراد الشركات العسكرية والأمنية الخاصة، في حالات النزاع، وبما أنّها تميل إلى الاعتراف بهذه الممارسة بدلاً من الامتناع عنها، فإنّ هذا الحال يستوجب أن يُراعى تطبيق مبدأ التمييز عَبْر استيعاب هذه الممارسة، كي تبقى لهذا المبدأ فاعليّته أثناء النزاعات

المسلحة.

وفي الختام لا بدّ من القول: إن مبدأ التمييز بين المدنيين والمقاتلين، الذي أقرته المادة 48 من البروتوكول الإضافي الأول، يمثل قاعدة جوهرية قابلة للتطبيق على أشكال النزاعات المسلحة المعاصرة كافة، فهذا المبدأ شأنه شأن مجمل قواعد القانون الدولي الإنساني، يتمتع بالمرونة الكافية لاستيعاب التطورات المتسارعة في طبيعة هذه النزاعات.

وبالتالي، فإن الدول مدعوة ليس فقط إلى الامتثال لهذه القواعد، بل، وأيضاً، إلى الإسهام الفعّال في تطوير القانون الإنساني لضمان توفير الحماية الكاملة، لكلِّ مَنْ يَستحقُّها بموجب القانون.

قائمة المراجع

- شريف عتلم، ومحمد ماهر عبد الوهاب، موسوعة اتفاقيات القانون الدولي الإنساني، النصوص الرسمية للاتفاقيات والدول المصدقة والموقعة، ط. 6، (القاهرة: إصدار بعثة اللجنة الدولية للصليب الأحمر بالقاهرة، 2002).

- مشاريع المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً، تقرير لجنة القانون الدولي إلى الجمعية العامة عن أعمال دورتها الثالثة والخمسين، حولية لجنة القانون الدولي، م. 2، ج. 2، (الأمم المتحدة: 2001، ص 32).

- نيلس ميلزر، دليل تفسيري لمفهوم المشاركة المباشرة في العمليات العدائية بموجب القانون الدولي الإنساني، اللجنة الدولية للصليب الأحمر، الطبعة العربية الأولى، (القاهرة: المركز الإقليمي للإعلام، مارس/آذار 2010).

- وثيقة مونترو بشأن الالتزامات القانونية الدولية والممارسات السليمة للدول ذات الصلة بعمليات الشركات العسكرية والأمنية الخاصة أثناء النزاع المسلح، مونترو، 17 أيلول 2008، واردة ضمن رسالة موجهة إلى الأمين العام من الممثل الدائم لسويسرا لدى الأمم المتحدة، الجمعية العامة مجلس الأمن، الدورة 63، السنة 63، وثيقة رقم (A/63/467–S/2008/636).

- Emanuela-Chiara Gillard, Business goes to war: Private/Security Companies and International Humanitarian Law, International Review of the Red Cross, Vol. 88, No. 863, (September 2006) (pp. 525_ 572).

- Geneva Convention III, relative to the treatment of prisoners of war of 12 august 1949. (English edition).

- Jean De Preux, Commentary on Geneva convention III 1949, translated to English by A.P. de Heney, (Geneva: ICRC, 1960).

- Report of the Expert Meeting on Private Military Contractors: Status and State Responsibility for their Actions, organized by the University Centre for International Humanitarian Law, Geneva, (29, 30 August 2005), p. 14_15. (https://docplayer.net/117880-Expert-meeting-on-private-military-contractors-status-and-state-responsibility-for-their-actions.html) (Last site visit november 2025).

مجلة مؤشر للدراسات الاستطلاعية
Journal index of exploratory studies
المجلد 07، العدد 20
ISSN: 2701-9233

الحرب السيبرانية: التهديدات، الاستراتيجيات، وتحديات الردع في الفضاء الرقمي

Cyber Warfare: Threats, Strategies, and Deterrence Challenges in Cyberspace

د. محمد إبراهيم قانصو

الجامعة الاسلامية في لبنان

m-kanso@hotmail.com

الملخص

يهدف هذا البحث إلى مقاربة ظاهرة "الحرب السيبرانية"، وتحليل طبيعتها المهددة للأمن القومي والدولي في العصر الرقمي، واستكشاف الاستراتيجيات المتبعة للردع. يتناول البحث نشأة وتطور مفهوم الحرب السيبرانية، ويحدد طرائق الهجمات وأنماطها التي تتجاوز الحدود الجغرافية، مع إبراز المميزات التي تجعلها سلاحًا ذا كلفة منخفضة وتأثير فاعل ومخفي. اعتمد البحث على المنهج الوصفي التحليلي، مستعرضاً أبرز نماذج الصراع السيبراني الدولي (كالهجمات بين الولايات المتحدة وإيران). خلص البحث إلى أن الطبيعة غير الملموسة والمجهولة المصدر لهذه الهجمات تقوض من فعالية الردع السيبراني التقليدي، مما يفرض تحديات قانونية وموثوقية. ويوصي البحث بضرورة تطوير استراتيجيات ردع مرنة تشمل الأنظمة البديلة وإعادة التأسيس السريع للأنظمة المُخترقة، وتنمية الوعي الفردي والمؤسساتي لمواجهة هذه التهديدات التي باتت تمثل الجيل الخامس من الحروب.

الكلمات المفتاحية : الكلمات المفتاحية :الحرب السيبرانية؛ الأمن السيبراني؛ الردع السيبراني؛ الهجمات السيبرانية؛ الفضاء الرقمي؛ حرب الأصفار والأحاد.

Abstract

This research aims to contextualize and critically analyze the phenomenon of "Cyber Warfare" and its inherent threat landscape to national and international security in the digital age, while exploring emergent deterrence strategies. The study traces the genesis

and evolution of the cyber warfare paradigm, meticulously cataloging the vectors and topologies of attacks that transcend geopolitical boundaries. A key focus is placed on the characteristic features that position cyber operations as low-cost, high-impact, and covert asymmetrical capabilities. Utilizing a descriptive-analytical methodology, the research examines salient models of international cyber conflict (e.g., between the United States and Iran). The findings conclusively demonstrate that the intangible and ambiguous attribution inherent in these attacks significantly degrades the efficacy of conventional cyber deterrence frameworks, thereby introducing critical legal and credibility challenges. Consequently, the study recommends the architecting of resilient deterrence strategies that incorporate redundant systems, rapid system reconstitution capabilities following compromise, and the cultivation of heightened individual and institutional cyber vigilance to effectively counter these threats, which represent the fifth generation of conflict.

Keywords: Cyber Warfare; Cybersecurity; Cyber Deterrence; Cyber Attacks; Digital Cyberspace; Binary Warfare (Zero–One Warfare).

المقدمة

مَثَّلَ بزوغُ الثورة الرقمية وانتشار الإنترنت منعطفاً حاسماً، نقل الفضاء الإلكتروني من مجرد أداة اتصال إلى نسيج حيوي مُعقَّد تُمارس عليه كافة أنشطة البشرية، من الاقتصاد إلى السياسة إلى الأمن القومي. هذا التحول الجوهري أوجد بيئة خصبة لنشوء شكل جديد من الصراعات، تُعرف بالحرب السيبرانية، التي لم تعد مجرد تهديد نظري، بل أصبحت واقعاً ملموساً يُشكِّل الجيل الخامس من الحروب.

لم تعد هذه الحرب مقصورة على دوائر المخابرات التقليدية، بل أصبحت ساحة معقدة تتداخل فيها أدوار الفواعل، وغيرها فإلى جانب الوحدات المتخصصة في الجيوش النظامية، وبرزت مجموعات قرصنة إلكترونية مدعومة أو متسامح معها من قبل بعض الدول، تعمل في منطقة رمادية بين الحرب والسلم. هذا التشابك يجعل من "حرب البتات والبايتات "ساحة صراع غير تقليدية بالغة الغموض.

تتميز هذه المواجهات السيبرانية بطابعها اللامتماثل، حيث يمكن لفاعل صغير نسبياً أن يلحق أضراراً جسيمة بدولة عظمى. وهي حرب مبهمة المعالم :يصعب تحديد هوية المهاجم بدقة) مشكلة نسب الهجوم، وتكون الأهداف غالباً استباقية ومدروسة لتعطير البنى التحتية الحيوية أو سرقة الملكية الفكرية أو تقويض الاستقرار السياسي. وغالباً ما تكتشف الدولة أو المؤسسة المستهدفة الهجوم بعد فوات الأوان، بعد أن تكون الخسائر قد وقعت، ما يجعل الردع والاحتواء تحدياً استراتيجياً شائكاً.

وهكذا، لم يعد الفضاء السيبراني مجرد تقنية، بل تحول إلى مجال جيوسياسي حاسم، تُعيد فيه هذه الحروب الخفية تعريف مفاهيم القوة والسيطرة والهيمنة في النظام العالمي المعاصر.

1.1. إشكالية البحث

تتمحور إشكالية هذا البحث حول التساؤل الرئيسي التالي: إلى أي مدى أدت الطبيعة الخاصة للهجمات السيبرانية (المجهولة المصدر وغير المتماثلة) إلى إعادة تعريف مفهومي القوة والصراع في العلاقات الدولية، وإلى أي مدى يمكن تحقيق الردع الفاعل في ظل هذه الطبيعة الاستثنائية والتحديات المصاحبة لها؟

ويتفرع عن هذا التساؤل أسئلة فرعية يسعى هذا البحث للإجابة عنها:

- كيف أعادت الهجمات السيبرانية تعريف مفهومي القوة والصراع في العلاقات الدولية؟
- ما مدى فعالية استراتيجيات الردع السيبراني في مواجهة إشكالية إخفاء هوية المهاجم؟
- ما مدى قدرة الأطر القانونية الدولية الحالية على تنظيم الفضاء السيبراني ومواجهة تحدياته؟

أهداف البحث

يسعى هذا البحث إلى تحليل الآثار الناجمة عن الحرب السيبرانية على مفاهيم القوة والصراع في العلاقات الدولية، وتقييم إمكانية تحقيق الردع الفاعل في هذا المجال. ولتحقيق ذلك، يهدف البحث إلى:

تحليل المرتكزات المفاهيمية للحرب السيبرانية وسماتها التي أعادت بها تعريف طبيعة الصراع الدولي.

تحديد وتصنيف آليات الهجمات السيبرانية وتحليل تأثيرها على هيكل وتوزيع القوة بين الفواعل الدوليين.

دراسة السياقات التطبيقية للصراع السيبراني من خلال تحليل نماذج حالات لمواجهات بين قوى دولية.

تقييم مدى جدوى وفعالية استراتيجيات الردع السيبراني الحالية في ظل التحديات العملية والقانونية التي تفرضها طبيعة هذه الحرب.

2.1. فرضيات البحث

لإرشاد عملية التحليل، يفترض البحث ما يلي:

- أدت الهجمات السيبرانية إلى بروز "قوة السايبر "كشكل جديد من أشكال القوة، مما أحدث تغييراً في علاقات القوى الدولية.
- صعوبة الإسناد وعدم توفر المصداقية يشكلان التحدي الأبرز الذي يُقوض فعالية الردع السيبراني التقليدي.
- الاستراتيجيات الكلاسيكية غير كافية لمواجهة التهديدات السيبرانية، وتفعيل الردع يتطلب الاعتماد على خيارات مرنة مثل الأنظمة البديلة وإعادة التأسيس السريع.

3.1. أهمية البحث

تتحدد أهمية هذا البحث من خلال مساهمته المتعددة المستويات، والتي تجمع بين القيمة الأكاديمية والتطبيق العملي على النحو التالي:

1.3.1. الأهمية العلمية والنظرية

- يقدم البحث إطاراً تحليلياً متكاملاً لظاهرة الحرب السيبرانية في الأدبيات العربية، التي لا تزال تعاني من ندرة في الدراسات الاستراتيجية العميقة في هذا المجال.

- يسهم في تطوير الفهم النظري لتحولات مفاهيم القوة والسيادة والصراع في العلاقات الدولية في عصر الرقمنة.

2.3.1. الأهمية التطبيقية والعملية

- يقدم تحليلاً استراتيجياً يمكن أن يكون مرتكزاً لصياغة سياسات أمنية وطنية فاعلة وبناء استراتيجيات شاملة للدفاع السيبراني.
- يساعد في تحديد متطلبات تحقيق الردع السيبراني وتصميم أنظمة أكثر فاعلية للإنذار المبكر والاستجابة للحوادث.
- يرفع مستوى الوعي الاستباقي لدى الأفراد والمؤسسات بأهمية الأمن السيبراني، ويقدم إطاراً لبناء القدرات في مجال الحماية من التهديدات الإلكترونية.

2. المنهج المعتمد

اعتمد البحث على المنهج الوصفي التحليلي، حيث تم استخدام الجانب الوصفي لتعريف الظاهرة وتحديد طرائقها ونماذجها التاريخية، واستخدام الجانب التحليلي في تفكيك الإشكالية المعقدة للردع السيبراني وتقييم التحديات التي تعترض تطبيقه.

1.2. السيبرانية (لغة واصطلاحا)

من أجل الوقوف على مفهوم السيبرانية، سنبحث في نطاق تعريفها لغةً واصطلاحاً في ضوء المعاجم اللغوية، وما أدرج عليها المختصون في القانون الدولي العام، وخبراء تكنولوجيا المعلومات.

أ- <u>في اللغة</u>

كلمة سايبر(Cyber) يونانية الأصل وترجع إلى مصطلح (kybernetes)، الذي ورد بداية في مؤلفات الخيال العلمي، ويعني القيادة أو التحكُّم عن بعد (Cresswell , 2010)

والسيبرانية في قاموس (المورد) هي علم الضبط، ومصدرها (Cybernetics)، (البعلبكي،٢٠٠٤) وهو مصدر يتطابق مع مفهوم الهجمات السيبرانية، أي ضبط الأشياء عن بعد والسيطرة عليها.

وأول من استخدم مصطلح السيبرانية عالم الرياضيات نوربرت وينر (Norbert wiener) وذلك في عام ١٩٤٨، في أثناء دراسته لموضوع القيادة والسيطرة والاتصال في عالم الحيوان، فضلاً عن حقل الهندسة الميكانيكية (Wiener, 1948)

وبالرجوع إلى المختصين في اللغة العربية نجد أن تحدياً يواجهونه في اختيار مصطلح مقارب لمصطلح (Cyber) في اللغة الانكليزية، لعدم وجود مصطلح مناظر في اللغة العربية. إلا ان الترجمة العربية لعنوان اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية كانت ترجمة صائبة، إذ تُرجِم العنوان (Cybercrime on Conven) إلى اللغة العربية (الاتفاقية المتعلقة بالجريمة الالكترونية) (مجلس أوروبا حول اتفاقية مجلس أوروبا المتعلق بالجريمة الالكترونية، 2001).

فيما عرف قاموس مصطلحات الأمن ألمعلوماتي، مصطلح السيبرانية بالقول: "هجوم عبر الفضاء الالكتروني يهدف إلى السيطرة على مواقع الكترونية أو بنى محمية الكترونياً لتعطيلها أو تدميرها أو الأضرار بها (Kissel, 2013).

أما سبب اختيار هذا البحث لمصطلح السيبرانية ، فيعود إلى المصطلح الذي استخدمه نوربرت وينر في كتابه الذي ذكرناه سابقا (Cybernetic) ، لعدم وجود مصطلح متفق عليه في اللغة العربية من جهة، ولأن الوثائق الصادرة عن الأمم المتحدة باللغة العربية، استخدمت مصطلح السيبرانية نفسه من جهة أخرى (مكتب الأمم المتحدة المعني بالمخدرات والجريمة، 2013).

ب- اصطلاحا

تبرز عدة مصطلحات حول موضوع البحث فنجد مصطلح الهجمات السيبرانية(Cyber Attack) ومنهم من تبنى مصطلح الفضاء السيبرانيلسيج، (Cyber Space)لورنس. (2006)، بالاستناد إلى المحيط الذي تجري فيه العمليات السيبرانية الناشئة عن أداء أنظمة الكترونية مهمتها متابعة وجمع المعلومات التي تعمل الكترونياً

وتحليلها ومن ثم اتخاذ إجراءات محددة لمهاجمتها عن طريق أنظمة الكترونية أخرى مخصصة لهذا الغرض (Lewis, 2010)وتبنى آخرون مصطلح الحرب السيبرانية (Cyber Warfare) بالاستناد إلى أيدلوجية أمنية أو عسكرية، تضع منهاجاً لتحقيق أهداف على الصعيد الأمني أو العسكري تجاه (العدو المفترض) (Shin, 2011). وفي هذا البحث سوف نعتمد مصطلح الهجمات السيبرانية كونها أقرب للواقع الحالي المعاش على مستوى الدول. فالمقصود بالهجمات السيبرانية وأشهر تعريف لها " إنها الأفعال الصادرة من أجهزة الحاسوب وشبكات المعلومات التابعة لدولة ما بشكل منظم ومدروس على أجهزة حاسوب وشبكات معلومات لدولة أخرى بغرض التجسس Espionage أو التخريب **Sabotage او** التوجيه". (Saalbach, 2014).

ومن الممكن أن تكون الهجمات السيبرانية وسيلة وطريقة في الوقت نفسه، وبعبارة أخرى يعتمد ذلك على الهدف من استخدامها ، فقد تسهم في توجيه العمليات العسكرية الأخرى كالصواريخ بعيدة المدى أو الطائرات بدون طيار (Drawn) لتحديد أهداف عسكرية منتخبة وتدميرها أو لتعطيل أجهزة الكشف المبكر للهجمات التي يقوم بها سلاح جو معادي أو وقف عمليات الاتصال في المطارات العسكرية أو المدنية (الهجوم الذي قامت به إسرائيل عام 2007 ضد سوريا، إذ توقفت أجهزة الرادار وباقي منظومات الاتصال في المطارات العسكرية والمدنية عن العمل ، في أثناء الهجوم الذي نفذه سلاح الجو التابع لها على مواقع سورية زعمت إسرائيل أنها منشآت ، و في هذه الحالة يعد الهجوم السيبراني طريقة قتالية، إذ يدخل ضمن الخطط العسكرية لمفاعل نووي وبالتالي هو طريقة قتالية.) (Rid & Mcburney, p. 6).

وعلى العكس قد تكون الهجمات السيبرانية وسيلة قتالية ، من خلال استخدامها بذاتها، للتسلل إلى أنظمة الكترونية معدة لحماية أو لتنظيم سير عمل منشآت حيوية، كمحطات توليد الطاقة النووية أو السدود أو وسائل النقل كالمطارات، بهدف تطويعها والسيطرة عليها، لتدمير ذاتها بذاتها من خلال تغذيتها بمعلومات خاطئة لأجهزة التحكم والحماية الالكترونية (ما تعرضت إليه محطة (نطانز) النووية الإيرانية من هجوم سيبرآني عام 2009، وأعلنت عنه الولايات المتحدة في عام 2011، إذ استخدمت برنامجاً ويدعى (Stuxnet) عطل بعضاً من العمليات الحساسة والحق أضراراً جزئية في عمليات تخصيب اليورانيوم، وهو ما يمكن معه عد هذا الهجوم سابقة في حقل الهجمات السيبرانية) (Gervais, 2012, p. 46).

إن التمييز بين وسائل وطرائق القتال، إنما يعتمد على الهدف من استخدامها والنتيجة التي ستؤديها، فكلما كانت تتسبب بطريق مباشر أو غير مباشر بقتل أو جرح أو تدمير أو تعطيل كلي أو جزئي، فتعد وسيلة قتالية، أما إذا استخدمت كجزء من مخطط عسكري فتعد طريقة قتالية تخضع للنظام القانوني الدولي (الجمعية العامة للأمم المتحدة، 1977). وهو ما تتصف به الهجمات السيبرانية في الاثنين معاً.

2.2. **طرائق الهجمات السايبرانية** ومميزاتها

1-تعتمد الهجمات السيبرانية أساسا على الوحدات السيبرانية التي تضم الجنود السيبرانيين وهم بالأصل قراصنة رقميون يتم استخدامهم على شكل فرق متخصصة واعطائهم إمكانات لوجستية وسيرفرات على شبكات المعلومات وتوجيههم لأغراض محددة مثل مراقبة كل شبكات المعلومات الحساسة (شبكات الطاقة، المياه، الكهرباء، الاتصالات، الأمور المالية في البنوك..) او الرد على أي هجمات او التجسس او توجيه راي العام لدول معادية. وكانت معظم الهجمات الالكترونية سابقا تُشن بواسطة أشخاص أو مبرمجين لأهداف شخصية أما في العقدين الأخيرين دخلت المنظمات الأمنية والحكومات إلى هذه الساحة وأخذت تنفق الملايين لتطوير قدراتها وبناء جيوش إلكترونية للدفاع عن منشآتها وشن الهجمات المضادة. وبرزت إسرائيل وأميركا والصين وروسيا وإيران والمملكة المتحدة وكوريا الشمالية وفرنسا في مقدمة الدول المتقدمة في تقنيات الحرب الإلكترونية.

تنقسم الهجمات السيبرانية الى نوعين رئيسين:

- هجمات تعطيل جهاز الكمبيوتر المستهدف.
- هجمات يكون الغرض منها الوصول الى بيانات جهاز الكمبيوتر المستهدف وربما الحصول على امتيازات المسؤول عنه.

ومن طرائق الهجمات السيبرانية نذكر:

- الطريقة الأولى

إرسال روابط بشكل واسع عن طريق برامج التراسل لعدة مستخدمين وتعزز هذه الرسائل بخاصية تتيح التحكم بحساب كل من يفتحها حيث تمكن القراصنة الالكترونيين من الوصول الى بيانات وحسابات للمستخدمين المصرفية حتى او كلمات سر تابعة لهيئات حكومية رسمية.

- الطريقة الثانية

أن يقوم الهاكر بتجهيز عدة سيرفرات سريعة تقوم بإرسال ملايين الطلبات بوقت واحد الى موقع او عدة مواقع الكترونية مما يؤدي الى توقف عملها وهذا يكلف خسائر مالية خصوصا اذا كانت هذه الخدمات المقدمة حكومية او تابعة لهيئات مالية حيوية، فيجري استهداف البنوك أو المواقع الحكومية التي تحتوي على بيانات مهمة، أو حتى استهداف منشآت صناعية.

- الطريقة الثالثة

أن يقوم الهاكر بإنشاء مواقع بأسماء تكون قريبة جدا من أسماء مواقع عالمية موثوقة مثل apple او google ويرسل emails يطلب فيها فحص كلمة السر أو تغييرها ، فيظن المستخدم أنها الشركة العالمية ذاتها وبمجرد وضعه لكلمة السر يتحكم الهاكر ببيناته الخاصة وهذا له تأثير كبير إذا تم على مستوى الدول.

تُشكل الهجمات السيبرانية تحديًا استراتيجيًا غير مسبوق في العلاقات الدولية، حيث تجمع بين خصائص فريدة أعادت تعريف مفهوم الصراع المعاصر. فمن ناحية، تتميز هذه الهجمات بطبيعة غامضة تسمح للدول والفواعل من غير الدول.

بممارسة أعمال عدائية تحت عتبة الحرب التقليدية، مما يخلق منطقة رمادية تتحدى الأطر القانونية والسياسية القائمة. وتتعمق هذه الإشكالية مع صعوبة نسب الهجمات لمصادرها الأصلية، حيث تتداخل التقنيات المتطورة وآليات التمويه والتغطية، مما يخلق بيئة خصبة لإنكار المسؤولية ويضعف آليات الردع التقليدية.

وتمثل هذه الهجمات تحديًا للسيادة التقليدية، حيث تذوب الحدود الجغرافية وتصبح البنى التحتية الحيوية - سواء أكانت أرضية أم فضائية - عرضة للاستهداف. وهذا يوسع بشكل غير مسبوق من نطاق الصراع، حيث تتحول الشبكات الرقمية إلى ساحة معركة مفتوحة على مدار الساعة. وتتفاقم هذه التحديات مع الميزة النسبية لهذه الهجمات من حيث التكلفة، حيث تتيح للدول الصغيرة والفواعل من غير الدول منافسة القوى العظمى بتكاليف محدودة، مما يعيد رسم خريطة توازنات القوى الدولية.

وتتميز هذه الهجمات بطبيعة ازدواجية معقدة، حيث يمكن لنفس الأدوات والتقنيات أن تستخدم لأغراض دفاعية وهجومية، وأن تنتقل بسرعة بين أغراض التجسس والإعاقة والتدمير. وهذا الازدواجية تخلق تحديات كبيرة في التمييز بين الأنشطة العدائية والعمليات الروتينية، وتجعل من الصعب وضع ضوابط واضحة للاستخدام المشروع. كما تبرز الآثار الجيوسياسية العميقة لهذه الهجمات، حيث تصبح الشركات التقنية العالمية فواعل رئيسية في المشهد الجيوسياسي، وتتحول البيانات إلى سلعة استراتيجية، وتتأثر سيادة الدول بقدرتها على حماية فضاءها السيبراني.

ولا يمكن إغفال القدرة التدميرية المتصاعدة لهذه الهجمات، حيث تطورت من مجرد أعمال تخريبية محدودة إلى تهديد وجودي يمكن أن يعطل البنى التحتية الحيوية ويؤدي إلى خسائر بشرية واقتصادية كارثية. وأخيرًا، تتفرد هذه الهجمات بعنصري التوقيت والسرعة، حيث تتميز بغياب المؤشرات التحذيرية التقليدية، وتنفذ بسرعة البرق، مما يحول دون الاستباق ويحد من فرص التصدي الفعال. وهذه الخصائص مجتمعة تجعل من الهجمات السيبرانية تحديًا استراتيجيًا يستدعي تطوير أطر تحليلية جديدة وأدوات استجابة مبتكرة.

3.2. المبحث الثالث: الصراع الدولي السيبراني بين النشأة والنماذج

بات الفضاء السيبراني أحد الركائز الأساسية التي تُشكّل هيكل النظام الدولي المعاصر، حيث يمثل منصة استراتيجية توفر أدوات تكنولوجية متطورة لدعم عمليات الحشد والتعبئة على المستوى العالمي. كما يمارس تأثيراً عميقاً في تشكيل القيم السياسية السائدة، وقد ازداد نطاق هذا التأثير مع سهولة الاستخدام وانخفاض التكلفة، مما وسّع من قدرته على اختراق مختلف المجالات الحياتية.

فلم يعد التأثير مقتصراً على الجوانب السياسية والعسكرية التقليدية، بل امتد ليشمل القطاعات الاقتصادية والأنسجة الاجتماعية وحتى البنى الأيديولوجية. وأصبح من الواضح أن القدرة على توظيف هذا الفضاء بكفاءة تشكل عاملاً حاسماً في تحقيق الأهداف الاستراتيجية للدول والجهات الفاعلة، كما تزيد من قدرتها على توجيه سلوكيات المستخدمين داخل هذه البيئة الرقمية.

ومن الأمور المتعارف عليها في العلاقات 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 هو قوة السايبر (power Cyber)، ويعد جوزيف ناي (Nye. Joseph) من أبرز المهتمين بالقوة السيبرانية، حيث يعرفها بأنها: "القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني، أي أنها القدرة على استخدام الفضاء السيبراني لإيجاد مزايا للدولة، والتأثير على الأحداث المتعلقة بالبيئات التشغيلية الأخرى وذلك عبر أدوات سيبرانية " (Nye, 2010, p. 3).كما يوضح ناي أن مفهوم القوة السيبرانية يشير إلى "مجموعة الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات والشبكات الالكترونية والبنية التحتية المعلوماتية والمهارات البشرية المدربة للتعامل مع هذه الوسائل ، والتي لها تأثير كبير على المستوى الدولي والمحلي، فمن ناحية أدت إلى توزيع وانتشار القوة بين عدد أكبر من الفاعلين مما جعل قدرة الدولة على السيطرة موضع شك، ومن ناحية أخرى منحت الفاعلين الأصغر قدرة أكبر على ممارسة كل من القوة الصلبة والقوة الناعمة عبر الفضاء السيبراني، وهو ما يعني تغيرا في علاقات القوى في السياسة الدولية .

والجدير ذكرنه أن التسللات ليست بالأمر الجديد، فبقدر قَدم العصور الرومانية، كانت الجيوش تعترض اتصالات العدو. في الحرب الأهلية الأمريكية (Glantz, 2011, p. 57). استخدم جنرالات الاتحاديين والكونفدراليين (الانفصاليين) أجهزة التلغراف الجديدة لإرسال أوامر مزيفة إلى العدو. أثناء الحرب العالمية الثانية، Kahn, (1996) كسر خبراء التشفير البريطانيون والأمريكيون رموز الشفرة الألمانية واليابانية، وكان هذا عنصرا أساسيا في انتصار الحلفاء (ظل بعد ذلك سرا طوال أعوام كثيرة). وفي العقود القليلة الأولى من الحرب الباردة أيضا كان الجواسيس الأمريكيون والروس يعترضون على نحو دوري ومنتظم اتصالات بعضهم ببعض من إشارات راديوية

(لاسلكية)، وبث للموجات الميكروية (الميكروويف)، واتصالات هاتفية. ولم يقتصر الهدف على جمع معلومات استخباراتية بشأن نوايا وقدرات الطرف الآخر، بل إضافة إلى ذلك، الحصول على أفضلية في الحرب الجسيمة المخيفة المقبلة.

أ- النشأة:

هناك من يجد أنّ أفكار الهجمات السيبرانية بدأت في أمريكا منذ الثمانينات خلال عهد الرئيس رونالد ريغان، الذي رأى أنه من الممكن أن تتعرّض بلاده لخطر مثل هذه الهجمات، فأفرز فكرة مميزة وسابقة لأوانها، أنتجت "وحدة السياسة القومية بشأن الاتصالات وأمن نظم المعلومات" التي تطوّرت خلال التسعينيات، واستخدمها الجيش في عمليات الاستشعار عن بعد، وظهرت الحاجة إليها وإلى تقنياتها خلال "الحرب على العراق في 2003" (كابلان، 2019) أن استراتيجية الهجمات السيبرانية الأمريكية كانت ولا تزال، متأثرة بالأولويات الجديدة للصناعة العسكرية الإسرائيلية، المصنفة بالبالغة السرية، والتي تستهدف تباعاً الصناعة النووية الإيرانية (المركز الاستشاري للدراسات والتوثيق، 2014، ص. 17) والصناعات الدفاعية الأوروبية المفترض أنها تعود لبلدان حليفة. وفي الجهة الأخرى من العالم كانت هنالك توجهات للخصم التقليدي، ونقصد به روسيا الاتحادية (Giles, 2011, p. 47)، فقد كانت الأسبق في نطاق الاستعداد للهجمات السيبرانية. ولقد قامت بعض دول العالم بالفعل نفسه في السنوات الأخيرة وعملت على تطوير استخدام مهارات الإنترنت والحواسيب كأدوات هجوم ودفاع واستخبارات وحروب نفسية. فقد أنشأت كل من بريطانيا وفرنسا وكوريا الجنوبية وحدات خاصة في قوّاتها المسلحة مسؤولة عن الحرب الإلكترونية أو حرب المعلومات. وفي مايو 2009، أدخلت شركة American Security اسم إيران بين الدول الخمسة التي تتمتع بأقوى قدرات إنترنت في العالم، وتجمع هذه الوحدات الخاصة ما بين العقل العسكري والمهارات التقنية التي تمكّنها من الدفاع وصدّ الهجمات أو إحداث خسائر. من ناحية أخرى، يتزايد استخدام الإنترنت بشكلٍ عام، ووسائل التواصل الاجتماعي بشكلٍ خاص، كأداة فعالة في الحرب التي تشنها التنظيمات المسلحة لا سيما في الشرق الأوسط. فقد وجدت هذه المجموعات في الفضاء الإلكتروني وسيلة مفيدة في صراعها، فاستخدمت وسائل التواصل الاجتماعي لتجنيد المقاتلين. كما استفادت هذه

التنظيمات من الفضاء الإلكتروني كمنصّة لإطلاق الحرب النفسية ضد الخصوم بتصوير مشاهد العنف ونشرها على نطاق واسع لبثّ الرعب والذعر.

وعليه نجد أن العديد من الدول، اليوم، تصرف المليارات على الأنشطة السيبرانية استعداداً لحروب المستقبل، حيث تبني استراتيجيات حرب المعلومات، والتي يتمّ خوضها بهدف التشتيت، وإثارة الاضطرابات في عملية صناعة القرار لدى الخصوم، عبر اختراق أنظمتهم، واستخدام ونقل معلوماتهم حتى لا تذهب الحروب لمصلحة من يملك القوة فقط، وإنما القادر على شلّ القوة، والتشويش على المعلومة، بل وربما تغيير البيئة الثقافية والفكرية للخصوم والتأثير بها قدر الممكن.

ب- نماذج عن الهجمات السيبرانية

يسجل لنا التاريخ المعاصر، نماذج للهجمات السيبرانية، سوف نأتي على ذكر بعضها فقط، وأولها الهجوم السيبراني الذي نفذته الولايات المتحدة الأمريكية وصرحت به عام 1982 ضد منظومة التحكم العالية صناعياً في أنبوب نفط (Chelyabinsk) التابع للاتحاد السوفياتي السابق، وهو ما نفاه الاتحاد السوفياتي السابق آنذاك (Canabarro & Borne, 2013, p. 10).

أما النموذج الآخر، فهو ما تعرضت له أنظمة الاتصال الالكترونية التابعة لوزارة الدفاع الأمريكي (Pentagon)ووكالة الفضاء الأمريكية(NASA) ووكالة الطاقة الأمريكية (Department -Energy) لهجمات سيبرانية بين الأعوام 1998 -2000، والذي أدى إلى الاستحواذ على الآلاف من الملفات المصنفة بأنها عالية السرية، وقد وجهت الولايات المتحدة التهمة رسمياً إلى روسيا الاتحادية، في حين أنكرت الأخيرة -آنذاك- مسؤوليتها عن هذا الهجوم.

وفي كانون الثاني من العام 2017، كشف تقرير لوكالة الاستخبارات الأميركية عملية قرصنة على الانتخابات الرئاسية الأميركية الأخيرة حيث افاد التقرير «أنّ الرئيس الروسي فلاديمير بوتين أمر بحملة تأييد لمصلحة الرئيس ترامب، خلال الانتخابات» وأوضح «أن الروس حاولوا تقويض إيمان المواطنين بالعملية الديمقراطية الأميركية، وتشويه سمعة الوزيرة هيلاري كلينتون، والتأثير في حظوظها الانتخابية». وذلك، حسب التقرير، بسبب رغبة

روسيا في تقويض النظام الديمقراطي الحر الذي تقوده الولايات المتحدة الأميركية، وهذه العمليات الروسية باتت أكثر تصعيدًا في مباشرتها ومستوى نشاطها وسِعَة جهودها، إذا ما قورنت بعملياتها السابقة.

وقد تكون أكثر الهجمات حداثةً، ما تقوم به الولايات المتحدة وإسرائيل بشأن البرامج النووية الإيرانية، لقد شنّت الولايات المتحدة الأميركية قبيل أعوام من توصل المجتمع الدولي إلى الاتفاق النووي مع طهران (2015)، حربًا سيبرانية على مشروع إيران النووي بهدف إضعاف قدراتها النووية، وإجبارها على التنازل على طاولة المفاوضات. لكنّ الولايات المتحدة نفسها لم تكن بمأمن من الحرب السيبرانية، ففي عام 2018 وجّهت وزارة العدل الأميركية اتهامات جنائية وفرضت عقوبات على شركة إيرانية و9 إيرانيين ناشطين في معهد «مبنا» الإيراني، لاختراقهم أنظمة مئات الجامعات والشركات، بهدف سرقة البحوث والبيانات الأكاديمية والملكية الفكرية. وكانت إيران قد استهدفت الأنظمة الإلكترونية لشركة نفط أرامكو عام 2017، حيث أجبرت قوة الهجوم السلطات على استبدال مجمل الشبكة الالكترونية التي تعمل عليها الشركة، وتبع ذلك تغيير كثير من الأجهزة العاملة (Jawal Max, 2018). فهل الحرب السيبرانية هي أكثر ميدان مرشح للتصاعد خلال الفترة القادمة بين الولايات المتحدة وإيران؟ سيما وأن هناك تعامل متبادل بين إيران وروسيا من جهة وإيران والصين من جهة أخرى ، وروسيا والصين تعتبران من "الطبقة الأولى" في امتلاك القدرات الالكترونية والهجمات السيبرانية، كما وأن القدرات الفنية للقوات السايبرانية الإيرانية أصبحت واضحة جدًا، حيث تمكنت من التسلل مرارًا إلى الحكومات الغربية وشبكات الاستخبارات الإقليمية، فعلى الرغم من كل الإجراءات الأمنية التي تم اتخاذها في ديسمبر 2011، أشار المدير التنفيذي لشركة Google إريك شميدت، في مقابلة مع شبكة CNN الأمريكية، إلى أن الإيرانيين موهوبين على نحو غير معتاد في الحروب السيبرانية الحديثة، وذلك لأسباب لا تفهمها الولايات المتحدة.

و في الآونة الأخيرة وتحديدا في نيسان من العام 2020 أعلنت إسرائيل عن هجوم سيبراني استهدف شبكات المياه الخاصة بها واتهم الإسرائيليون إيران بالمسؤولية عن الهجوم في حين ان إسرائيل والولايات المتحدة الأميركية قد اطلقتا اكثر من فيروس لاستهداف المنشآت النووية الإيرانية وآخرها ما وقع في شباط وايار وتموز من العام 2020 بحيث اقر وزير الأمن الإيراني " محمود علوي" بان هناك اكثر من مليوني هجوم سيبراني وقع بين عامي 2019

و2020 وبحسب وزير الأمن ان إسرائيل وأميركا والسعودية مصدرها علما ان الأخيرة تعمل على تدريب 5000 عنصر في البانيا لهذا الغرض.

ويمكن القول في ضوء تلك النماذج، إنه رغم اختلاف غرض وهدف كل حالة من الحالات السابقة، إلا أنه من الواضح أن حجم الهجمات السيبرانية يتزايد بشكل حاد، ولذا يصعب تحديد حجمها الحقيقي وبخاصة أن عديد منها لا يتم التبليغ عنه .وتتمثل القواسم المشتركة بين تلك الحالات في صعوبة تحديد مرتكبي تلك الهجمات على وجه الدقة، وغياب الرد المضاد، كنتيجة لها. والأهم أنها ليست حكرًا على الدول المتقدمة ذات أنظمة المعلومات الهائلة والمتطورة فحسب. وعليه نرجح بأن حروب المستقبل حتما ستكون حروبا سيبرانية، وعلى الأقل في جزء منها؛ حيث ان الفضاء السيبراني قد وِسم رسميا على أنه «ميدان» للحرب، مثل الجو، والبر، والبحر، والفضاء الخارجي. ونظرا إلى سلاسة وانسيابية الشبكة الحاسوبية العالمية، وبسبب حزم البيانات، وإنترنت الأشياء، فإن الحرب السيبرانية لن تشتمل على الجنود، والبحارة، والطيارين فقط؛ ولكنها، حتما ستتضمن البقية منا. حينما يكون الفضاء السيبراني في كل مكان، فإن الحرب السيبرانية يمكن أن تتسرب وتنضح عبر كل المسام الرقمية.

4.2. العمليات السيبرانية بين الأمن والردع

الأمن السيبراني (cybersecurity) مصطلح حديث، ويطلق عليه أيضا " امن المعلومات" وأمن الحاسوب" وهو فرع من فروع التكنولوجيا يعنى بممارسة حماية الأنظمة والممتلكات والشبكات والبرامج من الهجمات الرقمية، التي تهدف عادة الوصول الى المعلومات الحساسة او تغييرها او اتلافها او ابتزاز المال من المستخدمين أو تعطيل العمليات. ويعرفه "ادوارد اموروسو (Edward Amoroso) " بانه مجموع الوسائل التي من شأنها الحد من خطر الهجوم على البرمجيات او أجهزة الحاسوب او الشبكات. وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات الرقمية ووقفها، وتوفير الاتصالات المشفرة " (هارفارد بزنس ريفيو العربية، تاريخ غير متوفر).

تؤدي الطبيعة الخاصة للهجمات السيبرانية، التي تتسم بالمجهولية وعدم التماثل، إلى إعادة تعريف مفهومي القوة والصراع في العلاقات الدولية بشكل جذري. في السابق، كانت القوة تُقاس غالبًا من خلال العوامل

العسكرية والاقتصادية، ولكن مع ظهور الهجمات السيبرانية، أصبح الفضاء الرقمي يمثل ساحة جديدة للصراع. يمكن للدول أو الجماعات الصغيرة أن تستهدف القوى الكبرى بطرق غير تقليدية، مما يغير من ديناميكيات القوة التقليدية. هذا التحول يسلط الضوء على أهمية المعلومات والقدرة على الوصول إليها، حيث يمكن لمهاجم مجهول أن يؤثر على بنى تحتية حيوية أو ينشر معلومات مضللة، مما يعيد تشكيل موازين القوى.

في سياق استراتيجيات الردع، تواجه الدول تحديات كبيرة. فالهجمات السيبرانية غالبًا ما تُنفذ من قبل جهات غير معروفة، مما يجعل من الصعب تحديد هوية المهاجمين وتطبيق الردود المناسبة. هذا الإخفاء يعقد من قدرة الدول على الرد الفعال، حيث يمكن أن يؤدي إلى ردود فعل مبالغ فيها أو غير متناسبة، مما يزيد من حدة الصراع. بالتالي، تصبح استراتيجيات الردع السيبراني أكثر تعقيدًا، حيث تحتاج الدول إلى تطوير أدوات جديدة للتعامل مع هذه التهديدات، بما في ذلك تعزيز القدرات الاستخباراتية والقدرات الدفاعية في الفضاء السيبراني.

أما بالنسبة للأطر القانونية الدولية، فهي تواجه تحديات كبيرة في تنظيم الفضاء السيبراني ومواجهة تحدياته. القوانين الحالية غالبًا ما تكون غير كافية للتعامل مع الطبيعة المتغيرة للهجمات السيبرانية. تفتقر العديد من الدول إلى القوانين الملائمة التي تعالج قضايا مثل المسؤولية الدولية عن الهجمات السيبرانية، وحقوق الأفراد والدول في الفضاء الرقمي. لذلك، يتطلب الأمر تطوير آليات قانونية جديدة تتناسب مع طبيعة الهجمات السيبرانية وتسمح بتحقيق العدالة ومحاسبة المتورطين.

علاوة على ذلك، تتطلب هذه الديناميكيات الجديدة تعاونًا دوليًا موسعًا، حيث يجب على الدول العمل معًا لتحديد معايير مشتركة وتطوير استراتيجيات فعالة لمواجهة التهديدات السيبرانية. يشير البحث إلى أن الفهم التقليدي للقوة والصراع بحاجة إلى إعادة نظر، ويجب على المجتمع الدولي تعزيز التعاون وتطوير استراتيجيات جديدة لمواجهة هذه التحديات المعقدة. إن معالجة هذه الإشكاليات تتطلب أيضًا زيادة الوعي بين الأفراد والمؤسسات حول أهمية الأمن السيبراني ودوره في حماية المصالح الوطنية.

بالمجمل، يبرز هذا التحليل الحاجة إلى إعادة تقييم شاملة لمفاهيم القوة والصراع، مع التركيز على أهمية تكامل الجهود الأمنية والتشريعية لمواجهة التحديات المتزايدة في الفضاء السيبراني.

ومن هنا نجد أن ظهور الأمن السيبراني ارتبط بظهور الهجمات السيبرانية كونها باتت تشكل خرقا للأمن القومي، وهذا بسبب تأثير التكنولوجيا على المفاهيم ذات الصلة كالقوة powerوالسيادة ,sovereignty الحوكمة العالمية global governanceوالأمنية . securitization ، ونظرا لطبيعة الفضاء السيبراني، حيث انه ساحة عالمية عابرة لحدود الدول، تمتد قضية الأمن السيبراني من داخل الدولة إلى مجموعة النظام الدولي، ومع وجود مخاطر تهدّد الفاعلين جميعًا في مجتمع المعلومات العالمي تصبح القضية مرتبطة بالأمن العالمي. ومن هنا كانت اول محاولة لوضع معاهدة دولية لمراقبة الفضاء السيبراني وما يتصل به في العام 2001، وأسهمت اللجنة الدولية للصليب الأحمر بصفتها مراقبًا، في نشر ما يُعرف بـ«دليل تالين للقانون الدولي المُطبَّق على الحرب الإلكترونية". هذ بالإضافة إلى بروز اتجاهات متعدّدة لتحقيق هذا الأمن، وذلك عبر التنسيق بين أصحاب المصلحة من الحكومات، والمجتمع الأهلي، والشركات التكنولوجية، ووسائل الإعلام، وغيرها للحفاظ على خصوصية وحرية وتفكير وحق الفرد في حفظ بياناته دون اختراق .و قد بات الأمن السيبراني يشكل جزءاً أساسياً من أي سياسة أمنية وطنية، حيث بات معلوماً أن صناع القرار في الولايات المتحدة الأمريكية، الاتحاد الأوروبي، روسيا، الصين، إيران وغيرها من الدول، أصبحوا يصنفون مسائل الدفاع السيبراني/الأمن السيبراني كأولوية في سياساتهم الدفاعية الوطنية، هذا بالإضافة الى تشييد قوة سيبرانية تقوم بالهجوم من خلال برمجيات خاصة . فنجد بأن أغلب الجيوش في العالم يمتلك وحدة امن الكتروني ووحدة امن الدفاع عن الهجمات السيبرانية، لذا نجد بأن الأمن المعلوماتي لم يعد حكراً على الشركات أو المؤسسات صاحبة العلاقة، بغية حفظ البنوك ومعطياتها من أي استهداف، بل أضحى أيضاً يشكّل رهاناً قوياً وتحدياً كبيراً بوجه الدول والحكومات، بحيث تحولت وحدة الأمن الالكتروني الى قيادة قتالية منفصلة عند الدول الكبرى. وهنا تتجلى استراتيجيات المواجهة لتطرح إشكالية مدى إمكانية تحقيق الردع السيبراني لمنع الأعمال الضارة ضد الأصول الوطنية في الفضاء، والذي يرتكز على ثلاثة ركائز هي: مصداقية الدفاع، والقدرة على الانتقام، والرغبة فيه (بوفر، 1970، ص. 31). ولعل ما شهده الواقع المعاصر من حالات متباينة تطال الدول المتقدمة والنامية على حد

سواء، يؤكد ويعزز تلك الحاجة، ولكن إلى أي مدى يمكن ردع تلك الهجمات، وما هي طبيعة التحديات التي تعترض ذلك المدى؟

5.2. تحديات الردع السيبراني

إن عملية الردع تواجه تحديات أبرزها:

- أولا: الإسناد (تحديد مرتكب الهجمات بدقة)، من شأن الردع السيبراني أن يفشل طالما لم يعلن الجاني رسميًا عن مسؤوليته عن الهجوم؛ اذ يمكن لأي شخص أن يكون هو الجاني في الهجمات السيبرانية، وبخاصة أن المعدات اللازمة لشن هجوم سيبراني يمكن الوصول لها، وليست مكلفة، ويمكن شنها من أي مكان تتوافر فيه خدمة الإنترنت. فلكي يعمل الردع لابد من أن يقلق المهاجم من كشف هويته، ومن ثم تعرضه للعقاب أو الانتقام، بيد أن صعوبة تحديد مرتكب الهجمات بدقة، قد يسفر عن استهداف طرف ثالث لا علاقة له بالهجوم الاولي، وهو الأمر الذي لا يُضعف فقط من منطق الردع وفلسفته، لكنه يخلق عدوًا جديدًا أيضًا. فعدم التغلب على تلك الإشكالية يعني تكرار الهجمات مرة أخرى دون تعرض المهاجم للعقاب، أو بعبارة أخرى، تحسين سبل الإسناد ضرورة لفعالية الردع.
- ثانيا: العقبات القانونية، التي لا يمكن تطبيقها حاليا على الهجمات السيبرانية إلا بشكل غير مباشر، لان جرم القانون الدولي منسوب الى العدوان العسكري، ولكن ماذا عن الهجوم السيبراني الذي أسفر عن انفجار قاعدة عسكرية؟ وهل يحق للدولة – إعمالًا لحقها الأصيل في الدفاع عن النفس – استهداف أهداف عسكرية ضد تلك الدولة أو حتى شن هجوم سيبراني مضاد؟! لا يزال النقاش دائرًا حول المسائل القانونية المتعلقة بالهجمات السيبرانية. وعليه، قد يبدو الرد الانتقامي عملًا عدوانيًا غير مبرر أو مخالفًا لقواعد القانون الدولي (Wei, 2015).
- ثالثا: الفاعلون من غير الدول، الذين يمكن لهم إحداث أضرار بدرجات مختلفة، مما يضفي مزيدًا من التعقيد على الردع السيبراني نظرًا لصعوبة استهداف هؤلاء الفاعلين، وهنا المقصود المنظمات الإجرامية، والجماعات الإرهابية، والنشطاء السياسيين، وغيرهم، مما يدعو للتساؤل عن جدوى الرد

الانتقامي، ماذا إذا وُجد هذا الفاعل داخل دولة ما، ووفرت له دولة أخرى الحماية، أيهما يتحمل المسؤولية؟

- رابعا: المصداقية، فهي غير متوفرة في الفضاء السيبراني لكلا الجهتين، بسبب عدم توفر اسناد الهجوم الى مرتكبيه من جهة، ولان الأسلحة السيبرانية خفية وغير مرئية إلى أن يُقدم طرف ما على استخدامها. ولذلك، لا يمكن للمهاجم أن يعرف إذا امتلك الخصم القدرة على الرد أو الانتقام هذا من جهة ثانية (Cohen, 2005).

ولا يمكن تجاهل ثغرة اتساع مفهوم الردع السيبراني حيث انه يطال مجالات عدة مثل: الاتصالات، والتجارة، والأعمال التجارية، والتعليم، والتدريب، وأكثر من ذلك. لذا، بناء استراتيجية فاعلة للردع في الفضاء السيبراني يتطلب تجاوز الحديث عن المجال ككل إلى الحالات التي يمكن للردع أن يكون فاعلًا فيها، الا ان الحديث اليوم عن الردع السيبراني بات أكثر مرونة، وذلك من خلال مقاربات مختلفة، ويمكن تداولها بخيارين مختلفين:

الخيار الأول:

استخدام الأنظمة البديلة: ذلك يكون من خلال اعتماد الدولة أنظمة بديلة وليس الاعتماد على نظام واحد، يتم اختراقه بسهولة، ما يؤدي الى نتائج وخيمة؛ وبخاصة إذا تعلق هذا النظام بالبنية التحتية الرئيسية للدولة، وهذا يمكن الدولة من استخدام خيارات أخرى في حال تعرضها الى هجوم سيبراني، بحيث تلجأ الى الاستعانة بتلك الأنظمة البديلة أو الاحتياطية.

الخيار الثاني:

إعادة التأسيس: **وهذا يعتمد على التوقيت**، فإذا تمكنت الدولة التغلب على الهجوم الذي تتعرض له بسرعة، وإعادة تشغيل النظام، ستكون الآثار هامشية. ولكن الطريقة الوحيدة لتجنب الهجوم هي الاحتجاب عن الجميع، ورغم كونه السبيل الأفضل للردع، إلا أنه يكتنفه مسائل قانونية عدة.

وبناء على ما تقدم سعى هذا البحث إلى تحليل الآثار الناجمة عن الحرب السيبرانية على مفاهيم القوة والصراع في العلاقات الدولية، وتقييم إمكانية تحقيق الردع الفاعل في هذا المجال. إذ تناول المرتكزات المفاهيمية

للحرب السيبرانية وسماتها الفريدة التي تعيد تعريف طبيعة الصراع الدولي، لا سيما من خلال عدم التماثل الذي يتيح للفاعلين الضعفاء استهداف القوى الكبرى بطرق غير تقليدية. كما هدف إلى تحديد وتصنيف آليات الهجمات السيبرانية، مثل الهجمات على البنية التحتية الحيوية والهجمات المعلوماتية، وتحليل تأثيرها على هيكل وتوزيع القوة بين الفواعل الدوليين. بالإضافة إلى ذلك، وتناول السياقات التطبيقية للصراع السيبراني من خلال نماذج حالات لمواجهات بين قوى دولية، مما يتيح فهماً أعمق لاستراتيجيات الردع المتبعة ومدى فعاليتها في مواجهة التهديدات السيبرانية. من خلال هذه الأهداف، يسعى البحث إلى تقديم توصيات لتحسين الردع السيبراني وتعزيز الأمن في الفضاء الرقمي، ما يعكس ضرورة إعادة التفكير في استراتيجيات القوة والصراع في عصر المعلومات.

الخاتمة

في ختام هذ البحث، يتضح أن الواقع العالمي اليوم يتميز بتعقيدات متزايدة، حيث أصبح الفضاء السيبراني ساحة للنزاع ووسيلة لتعزيز المصالح مع تقليل المخاطر. تشكل الخصائص الجديدة لهذا الوسط التقني محفزًا قويًا للأطراف لتسوية نزاعاتها بطريقة تصادمية، في ظل صعوبة تحديد المسؤوليات عند وقوع الهجمات السيبرانية. فمع انطلاق النزاعات في الفضاء الرقمي، تبرز تحديات جديدة تتعلق بالسيادة والأمن، مما يتطلب من الدول إعادة التفكير في استراتيجياتها الدفاعية.

إن بروز عدد كبير من الفاعلين في هذا المجال، من دول وجماعات غير حكومية، أدى إلى تعقيد المشهد السيبراني وجعل من الصعب التحكم في النزاعات. فقد أصبحت المصطلحات الحربية التقليدية تتداخل مع مفاهيم جديدة مثل الإرهاب السيبراني، مما يستدعي تطوير استراتيجيات جديدة لمواجهتها. لذا، فإن المطالبة بعقد اتفاقيات دولية للحد من التسلح في الفضاء الإلكتروني، على غرار الاتفاقيات التي أُبرمت في مجالات الانتشار النووي والكيماوي، أصبحت ضرورة ملحة. يمكن أن تسهم هذه الاتفاقيات في وضع قيود على الحروب الإلكترونية واستخدامها وتوزيعها وتطويرها.

إن الاعتماد المتزايد على تقنيات المعلومات والاتصالات من قبل الدول والأفراد يفرض على الحكومات اتخاذ تدابير فعالة لإدارة المخاطر المرتبطة بالهجمات السيبرانية. ويتطلب ذلك فهمًا عميقًا لطبيعة هذه التقنيات وقدرتها على تجاوز الحدود بين الدول والمجتمعات. لا بد من تعزيز التدابير الأمنية لحماية مجتمعات المعلومات، حيث تُقوض طبيعة العمليات السيبرانية من دور الردع التقليدي. فتعرض دولة ما لهجوم يؤثر على اقتصادها أو بنيتها التحتية أو على أرواح مواطنيها، دون معرفة مصدره أو دوافعه، يقلل من فاعلية الردع.

تظل أهمية الردع قائمة، خاصة في ظل هشاشة الدول في مواجهة الهجمات السيبرانية. وبالتالي، يتطلب الأمر وعيًا متزايدًا بأساليب الوقاية وتعزيز البنية التحتية الدفاعية. كما ينبغي على الدول الاستثمار في تطوير قدرات الاستخبارات السيبرانية، لتكون قادرة على اكتشاف هوية المهاجمين وتحليل دوافعهم، مما يسهل وضع استراتيجيات ردع فعالة.

ويبقى التحدي الأكبر هو تحقيق توازن بين تعزيز القدرات السيبرانية وحماية الأمن الوطني في عالم متغير. يتطلب ذلك تعاونًا دوليًا شاملاً، حيث يمكن أن تسهم الشراكات بين الدول في تبادل المعلومات والخبرات لتعزيز الأمن السيبراني. كما يجب أن تكون هناك جهود متواصلة لتوعية الأفراد والمؤسسات حول أهمية الأمن السيبراني وطرق الوقاية، ما يؤدي إلى خلق بيئة أكثر أمانًا في الفضاء الرقمي.

النتائج

استنادًا إلى ما تقدم حول "الحرب السيبرانية: التهديدات، الاستراتيجيات، وتحديات الردع في الفضاء الرقمي"، يمكن تلخيص النتائج الرئيسة بالتالي:

- :انتقل مفهوم الحرب السيبرانية من نظرية إلى واقع ملموس يهدد الأمن القومي والدولي، ما يستدعي فهمًا شاملًا لطبيعته وآلياته.
- تعتبر الهجمات السيبرانية المتنوعة سلاحًا ذا كلفة منخفضة مع تأثيرات كبيرة، ما يشجع الفاعلين على اعتمادها كوسيلة غير تقليدية للصراع.

- تثير الحرب السيبرانية بتحدياتها قضايا قانونية تتعلق بالمسؤولية، ما يستدعي تطوير أطر قانونية جديدة.
- **ضرورة** تطوير استراتيجيات ردع تشمل تعزيز الأنظمة البديلة وإعادة التأسيس السريع للأنظمة المُخترقة وتعزيز الوعي الفردي والمؤسساتي حول التهديدات السيبرانية لتعزيز القدرة على التصدي لها.

التوصيات

استنادًا إلى النتائج الرئيسة حول "الحرب السيبرانية: التهديدات، الاستراتيجيات، وتحديات الردع في الفضاء الرقمي"، يمكن تقديم التوصيات التالية:

- يتعين على الدول والمنظمات الدولية العمل على وضع أطر قانونية جديدة تعالج القضايا المتعلقة بالمسؤولية في الهجمات السيبرانية. ويجب أن تشمل هذه الأطر معايير واضحة للتصدي للهجمات وتحديد المسؤوليات القانونية تجاه الفاعلين.
- **تعزيز التعاون الدولي** وضرورة بناء شراكات دولية قوية لمواجهة التهديدات السيبرانية، وتنسيق الجهود لمواجهة الهجمات المشتركة، وتطوير استراتيجيات ردع فعالة تعزز الأمن السيبراني على مستوى عالمي.
- تعزيز برامج التوعية والتدريب للأفراد والمؤسسات حول التهديدات السيبرانية وأساليب التصدي لها وتوفير الموارد التعليمية والدورات التدريبية لتعزيز القدرة على التعرف إلى الهجمات والرد عليها بشكل فعال.

قائمة المراجع

- البعلبكي، منير .(2004) .المورد: قاموس إنكليزي –عربي .دار العلم للملايين.
- بوفر، أندريه .(1970) .الردع والاستراتيجية)ترجمة أكرم ديري). دار الطليعة للطباعة والنشر.
- الجزيرة نت .(تاريخ غير متوفر) https://www.aljazeera.net/midan/reality/politics

- الجمعية العامة للأمم المتحدة .(2013) .دراسة شاملة عن مشكلة الجريمة السيبرانية والتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لها الوثيقة فيينا(UNODC/CCPCJ/EG.4/2013/2).
- كابلان، ف .(2019) .المنطقة المعتمة: التاريخ السري للحرب السيبرانية (ترجمة لؤي عبد المجيد). المجلس الوطني للثقافة والفنون والآداب (سلسلة عالم المعرفة) .
- لسيج، لورنس .(2006) .الكود المنظم للفضاء الإلكتروني (ترجمة: محمد سعد طنطاوي). (ط. 2). مؤسسة هنداوي للتعليم والثقافة.
- المركز الاستشاري للدراسات والتوثيق .(2014) .التحولات في العقيدة العسكرية الأمريكية: دعائم الضعف السبع (أوراق استراتيجية، العدد 2). بيروت: المركز الاستشاري للدراسات والتوثيق.
- هارفارد بزنس ريفيو العربية .(تاريخ غير متوفر). https://hbrarabic.com

- Canabarro, D. R., & Borne, T. (2013). Reflection on the fog of Cyber War (Policy working Paper). National Center for Digital Government.
- Cohen, H. (2005). The Approaches and Limitations of Cyber Deterrence. Retrieved from http://www.cs.tufts.edu/comp/116/archive/fall2015/hcohen.pdf
- Cresswell, J. (2010). Cybernetics. In Oxford Dictionary of word Origins. Oxford University Press.
- Gervais, M. (2012). Cyber Attacks and the Laws of War. Berkeley Journal of International Law, 30(2), Article 6.
- Giles, K. (2011). Information Troops a Russia Cyber Command? In legal paper third international conference on Cyber Conflicts. Tallinn Estonia.
- Glantz, E. J. (2011). Guide to Civil War Intelligence. The Intelligencer: Journal of U.S. Intelligence Studies.
- Jawal Max. (تاريخ غير متوفر). Learn about the highlights of 2018 and 2019 cyber attacks. Retrieved from https://jawalmax.com/learn-about-the-highlights-of-2018-and-2019-cyber-attacks/
- Kahn, D. (1996). The Codebreakers (Rev. ed.). Scribner.
- Kissel, R. (2013). Glassory of Key Information Security Terms. National Institute of Standards and technology, U.S Department of Commerce.
- Lewis, J. A. (2010). Sovereignty and the role of Government in Cyberspace. Center for Strategic and International Studies Journal, 16(2).
- Nye, J. S., Jr. (2010). Cyber Power. Harvard Kennedy School.
- Saalbach, K. (2014). Cyber War, Methods and Practice (Version 9.0). University of Osnabruck.
- Shin, B. (2011). The Cyber Warfare and the Right of Self–Defense: Legal Perspectives and the Case of the United States. IFANS, 19.

- Wei, M. L. H. (2015). The Challenges of Cyber Deterrence. Journal of the Singapore Armed Forces, 41(1), 13-22.
- Wiener, N. (1948). Cybernetic or control communication in the animal and the machine (2nd ed.). M.I.T. Press.

مجلة مؤشر للدراسات الاستطلاعية
Journal index of exploratory studies
المجلد 07، العدد 20
ISSN: 2701-9233

القانون الإنساني

بين الحرب السيبرانية والأسلحة المستقلة

Humanitarian Law: Between Cyber Warfare and Autonomous Weapons

د. علاء الدين بو مرعي

الجامعة الاسلامية في لبنان

alaadinbumeri@gmail.com

الملخص

يتناول هذا البحث إشكالية انطباق قواعد القانون الدولي الإنساني على أنماط النزاعات المسلحة المعاصرة، ولا سيما الحرب السيبرانية وأنظمة الأسلحة المستقلة، في ظل التطور التكنولوجي المتسارع الذي غيّر طبيعة وسائل وأساليب القتال. فقد أصبحت الدول تعتمد بشكل متزايد على الهجمات السيبرانية لاستهداف البنى التحتية الحيوية والأهداف العسكرية، وعلى أنظمة أسلحة مستقلة تعمل دون تدخل بشري مباشر، بهدف تقليل الخسائر البشرية وتحقيق تفوق عسكري أكبر. غير أن هذا التحول يثير تحديات قانونية عميقة تتعلق بمدى قدرة هذه الوسائل الحديثة على الامتثال لمبادئ القانون الإنساني الدولي، وفي مقدمتها مبادئ التمييز، والتناسب، والضرورة العسكرية، واتخاذ الاحتياطات اللازمة أثناء الهجوم.

يركّز البحث، في شقّه الأول، على الحرب السيبرانية بوصفها شكلاً جديداً من أشكال النزاع المسلح، ويحلل مدى خضوع العمليات السيبرانية لقواعد القانون الدولي الإنساني، ولا سيما مبدأ التمييز بين المدنيين والمقاتلين، في ظل الطبيعة المزدوجة للفضاء السيبراني وصعوبة تصنيف الأهداف السيبرانية، فضلاً عن الإشكاليات المرتبطة بإسناد المسؤولية القانونية عن الانتهاكات الناتجة عن الهجمات السيبرانية، نتيجة صعوبة تحديد الفاعلين الحقيقيين ومصادر الهجمات.

أما في الشق الثاني، فيتناول البحث انطباق القانون الإنساني الدولي على أنظمة الأسلحة المستقلة، ويبيّن التحديات التي تفرضها هذه الأنظمة على إمكانية احترام المبادئ الإنسانية الأساسية، نظراً لغياب الإدراك الإنساني والضمير الأخلاقي في عمليات اتخاذ القرار الآلي. كما يناقش البحث إشكالية "فجوة المسؤولية" التي قد تنشأ عند ارتكاب انتهاكات للقانون الإنساني باستخدام هذه الأنظمة، ويحلل أوجه المسؤولية المحتملة، سواء على عاتق الدول، أو القادة العسكريين، أو المبرمجين، أو الجهات المصنّعة.

ويخلص البحث إلى أن قواعد القانون الدولي الإنساني، رغم أنها وُضعت في سياق الحروب التقليدية، لا تزال قابلة للتطبيق على النزاعات الحديثة، بما فيها الحرب السيبرانية واستخدام الأسلحة المستقلة، غير أن ذلك

يستلزم تفسيراً مرناً لهذه القواعد وتطويرها بما ينسجم مع مستجدات النزاعات المعاصرة. كما يؤكد البحث على ضرورة تعزيز الأطر القانونية الدولية، ووضع آليات تنظيمية أكثر وضوحاً وفاعلية، لضمان حماية المدنيين، ومنع الإفلات من العقاب، والحفاظ على الطابع الإنساني للنزاعات المسلحة.

الكلمات المفتاحية: القانون الدولي الإنساني، الحرب السيبرانية، الأسلحة المستقلة، مبدأ التمييز، حماية المدنيين، المسؤولية الدولية، النزاعات المسلحة المعاصرة، الهجمات السيبرانية.

Abstract

This study examines the applicability of international humanitarian law (IHL) rules to contemporary forms of armed conflict, particularly cyber warfare and autonomous weapon systems, in light of the rapid technological developments that have fundamentally transformed the means and methods of warfare. States have increasingly resorted to cyber operations to target critical infrastructure and military objectives, as well as to autonomous weapon systems that operate without direct human intervention, with the aim of reducing human casualties and achieving greater military superiority. However, this shift raises profound legal challenges concerning the ability of these modern means of warfare to comply with the core principles of international humanitarian law, foremost among them the principles of distinction, proportionality, military necessity, and the obligation to take precautions in attack.

In its first part, the study focuses on cyber warfare as a novel form of armed conflict and analyzes the extent to which cyber operations are subject to the rules of international humanitarian law, particularly the principle of distinction between civilians and combatants. This analysis is conducted in light of the dual-use nature of cyberspace and the difficulty of classifying cyber targets, in addition to the challenges related to the attribution of legal responsibility for violations resulting from cyber attacks, given the difficulty of identifying the actual perpetrators and the sources of such attacks.

In its second part, the study addresses the application of international humanitarian law to autonomous weapon systems and highlights the challenges these systems pose to compliance with fundamental humanitarian principles, due to the absence of human judgment and moral agency in automated decision-making processes. The study further discusses the issue of the “responsibility gap” that may arise when violations of international humanitarian law are committed through the use of such systems, and analyzes the potential forms of responsibility, whether borne by states, military commanders, programmers, or manufacturers.

The study concludes that, although the rules of international humanitarian law were originally developed in the context of traditional warfare, they remain applicable to modern conflicts, including cyber warfare and the use of autonomous weapons. Nevertheless, this applicability requires a flexible interpretation and further development of these rules in order to align them with the realities of contemporary armed conflicts. The study also emphasizes the need to strengthen international legal frameworks and to establish clearer and more effective regulatory mechanisms to ensure the protection of civilians, prevent impunity, and preserve the humanitarian character of armed conflicts.

Keywords: International Humanitarian Law; Cyber Warfare; Autonomous Weapons; Principle of Distinction; Civilian Protection; International Responsibility; Contemporary Armed Conflicts; Cyber Attacks.

المقدمة

يَشْهَده العالم، اليوم، نزاعات تَسْتَعْمِل فيها الدول أساليب حربيّة حديثة، ووسائل قتالية هائلة التَّعقيد، باتَ المدنيون عُرْضَةً للقَتْل، أو الجَرْح، والأعيان المدنية لا تُمَيِّزها الهجمات القتالية عن الأهداف العسكرية، وأصبح القانون الإنساني الدولي وأحكامه، بِسَببها، وَجْهاً لِوَجْه مع تحدِّيات جِسام، وعلى مِحَكّ الصلاح لهذه المُواجهة، وفي نَظَر مُعظم أطرافها قيداً يُرجى التخلّص منه، ومن أعبائه.

ولا شكّ في أن الحرب السيبرانية تلك النوع من الحروب المستجِدة على مستوى أنواع النزاعات المسلحة وأساليبها ووسائلها، باتت اليوم تشكل هاجساً لدى الدول، وباتت واقعاً يُقلق أمن واستقرار أي دولة مهما كانت حصانتها كبيرة أمام أية هجمات سيبرانية، ومهما كان تقدمها العلمي والتقني هائلاً. فالمهاجمون مهما كانت صفاتهم أصبحوا قادرين على خرق الاحتياطات الأمنية لأية دولة بفضل القدرات المتوافرة لديهم والتطور المستمر في الفضاء السيبراني ومجال الذكاء الاصطناعي.

ويضاف، اليوم، إلى الحرب السيبرانية والأسلحة التقليدية، أنواع أسلحة جديدة هي الأسلحة المستقلة عن البشر في تشغيلها، والقادرة على القتال بمفردها في ساحة المعركة مزودةً بوسائل القتال كالمقاتلين البشريين. هذا النوع الجديد من الأسلحة بات اليوم، هاجساً للدول، أيضاً.

ويبدو أن تعاظم القدرات القتالية للدول وتنوعها، وتطورها، أصبح يُشكل تحدياً أمام ما يقتضيه القانون الإنساني الدولي من تلك الدول أثناء النزاع المسلح، فتطبيق هذا القانون وفرض مبادئه على أطراف النزاع لم يعد كما كان الحال سابقاً مع الأسلحة التقليدية، وعندما كان البشر هم مَنْ يخضون القتال ويشاركون في الأعمال العدائية. وأمام هذا الواقع بات لزاماً بحث تلك التحديات أمام تطبيق القانون الإنساني، فالحرب السيبرانية والأسلحة المستقلة باتت تشكل عائقاً أمام فرض القانون، ولذلك كانت هذه الدراسة محاولةً لكشف الواقع الذي فرضه استخدام الهجمات السيبرانية بين الدول، واستعمال الأسلحة المستقلة أو «الروبوتية»، ومحاولةً لدراسة مدى انطباق القانون الإنساني أثناء استخدام هذا النوع الجديد من الأساليب والوسائل القتالية، بالإضافة إلى تحديد الجهات التي تكون مسؤولةً عن انتهاك القانون الإنساني أثناء استخدام هذه الوسائل والأساليب الحربية الحديثة.

وتحت وطأة استخدام الحرب السيبرانية والأسلحة المستقلة أثناء النزاع المسلح، وما قد تسببه من

انتهاكات للقانون الإنساني الدولي، وما شكلته من تحديات أمام تطبيق هذا القانون فإنه يمكن طرح **الإشكالية التالية: ما مدى انطباق القانون الإنساني على الحرب السيبرانية والأسلحة المستقلة؟**

وللإجابة عن هذه الإشكالية، لا بدّ من رسم إطار قانوني واضح ركيزته الأساسية القانون الإنساني الدولي بما فيه من مبادئ أساسية يجب على الدول مراعاتها والعمل بها، ومحاسبة الأشخاص الذين ينتهكون هذه المبادئ أثناء النزاع المسلح.

وانطلاقاً مما تقدم، تم تقسيم هذه الدراسة إلى قسمين وفق ما يلي:

1. تطبيق القانون الإنساني أثناء الحرب السيبرانية والمسؤولية عن انتهاكه.
2. انطباق القانون الإنساني على أنظمة أسلحة المستقلة وتحديات فرض المسؤوليات القانونية.

1. تطبيق القانون الإنساني أثناء الحرب السيبرانية والمسؤولية عن انتهاكه.

الحرب السيبرانية مجموعة من الهجمات الإلكترونية المتبادلة تُشنّ في الفضاء السيبراني من قِبل أطراف متنازعة، سواء كانت دولًا أو جهات حكومية أو غير حكومية، وتستهدف أنظمة المعلومات وشبكات الحاسوب الخاصة بالطرف المستهدف، وتتخذ هذه الهجمات شكل برامج إلكترونية ضارة أو فيروسات حاسوبية، وتهدف إلى تعطيل أو تدمير هذه الأنظمة، أو سرقة البيانات السرية، أو شلّ الأنظمة الحيوية التي تُشغّل المرافق العامة للدولة المستهدفة أو قواتها المسلحة، كالأنظمة المالية والملاحية، مما يُشكل تهديداً مباشراً للأمن القومي وحياة المواطنين.

هذه الحرب تُحْدِث تأثيراً كبيراً على تطبيق القانون الإنساني، لِما لها من قُدرة على استهداف المدنيين والأعيان المدنية، والمقاتلين والأهداف العسكرية، على حدٍّ سواء، دون تمييزٍ بين هؤلاء وأولئك، وهي تُشَكِّل تحدّياً على مستوى إسناد المسؤولية عن الانتهاكات التي قد تَنتج عن تنفيذ هجمات سيبرانية تطال بنى تحتية حيوية، ومرافق يَستخدِمها المدنيون، كمحطات الطاقة، أو المطارات، أو غيرها.

ومن المسلم به أنه لا يجوز لأطراف أيّة حرب أنْ يخوضوها دون أنْ يلتزموا بتطبيق مبادئ القانون الإنساني أثناء تنفيذ هجماتهم على العدوّ، والحرب السيبرانية واحدة من هذه الحروب، وهي تستلزم تطبيق هذه المبادئ بشكل صارم لأن تأثيرها واسع على حياة الناس. وهنا يمكن طرح السؤال التالي: هل تنطبق مبادئ القانون الدولي الإنساني، ولا سيما مبدأ التمييز، فعلاً، على الحرب السيبرانية؟ وهل الالتزام به سهل، في حال كان تطبيقه ممكناً؟ وما التحديات التي تَرْتَسِم أمام تطبيقه أثناء شنّ هجمات سيبرانية؟ هذه الأسئلة تجعل قضية تطبيق مبدأ التمييز أثناء الحرب السيبرانية تحتاج بحثاً.

أما القضية الأخرى التي تحتاج بحثاً، أيضاً، فهي مشكلة إسناد المسؤولية عن انتهاكاتٍ للقانون الإنساني الدولي قد تُرتَكَب بسبب شَنّ هجمات سيبرانية. وهذه المشكلة تَظْهَر بسبب عدم القدرة على تحديد الأشخاص الذين يُنَفِّذون هذه الهجمات، لأنهم غير معروفين عند عدوِّهم، وهُمْ لا يُعْلِنون عن أنفسهم. ولأن الدول لا تكشف هويَّة الأشخاص الذين تتعاقد معهم في مجال الفضاء السيبراني، وشَنّ الهجمات السيبرانية؛ فهويَّة هؤلاء الأشخاص تبقى مخفيّة إلّا عن القادة المسؤولين عنهم.

وفي هذا المبحث لا بدّ من البحث في قضية تطبيق مبدأ التمييز في الحرب السيبرانية، وفي مشكلة إسناد المسؤولية، وذلك في المطلبين الآتيين:

1.1. التمييز بين المدنيين والمقاتلين أثناء الحرب السيبرانية.

2.1. إسناد المسؤولية عن انتهاك القانون الإنساني جراء الحرب السيبرانية.

1.1. التمييز بين المدنيين والمقاتلين أثناء الحرب السيبرانية.

الحرب السيبرانية حرب ذات دافع سياسي[27]، ترتكز على هجمات سيبرانية ميدانها الفضاء السيبراني، وتأخذ شكل برامج إلكترونية ضارة، أو فيروسات، وتهدف إلى تعطيل أنظمة المعلومات، والشبكات الانترنت، أو سرقة البيانات السرِّيَّة، أو شلّ الأنظمة المشغِّلة للعديد من المرافق الحيوية التابعة للدولة، أو لقواتها المسلحة، وتُشَكِّل تهديداً للأمن القومي في الدولة[28].

ولقد حَظِيَت الحرب السيبرانية بتغطية إعلامية واسعةٍ نتيجةً للهجمات السيبرانية ضدّ دولٍ عديدة، منها أستونيا وإيران، وعلى الرغم من كون هذا النوع من الحروب ليس شائعاً بين الدول، إلا أنّ بعض الهجمات التي حصلت مؤخَّراً أتت في سياق نزاعات سياسية بين دول متعادية. وإنّ دولاً كثيرة تعمل على تقوية نفسها في الفضاء السيبراني، وتعمل على امتلاك أدوات الحرب السيبرانية، وتقنياتها، تحسّباً لنشوب هكذا حرب في المستقبل.

وإنّ نطاق هذه الحرب واسع جدّاً، وهي تُتيح للمخططين العسكريين مجموعة واسعة من الإجراءات التي قد تُنَفَّذ ضدّ أطراف معادية. وإنّ الفضاء السيبراني، بمكوناته من أجهزة الكمبيوتر والإنترنت وغيرها، يَخْدِم مجالين هما: المجال المدني، والمجال العسكري، وهذا يَحْتِم أن يَتِمّ استخدام هذا الفضاء بشكل مُتناسق من قِبَل المدنيين والعسكريين، وإنّ أيّ محاولة لعرقلة استخدام هذا الفضاء نتيجة الحروب السيبرانية التي قد تنشأ بين

(27) Paulo Shakarian and others, *Introduction to Cyber-warfare A Multidisciplinary Approach*, (USA: Syngress, Elsevier, 2013, p. 2).

(28) Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, (New York: Harper Collins, 2010), p. 6.

الدول، أو التي قد تنشأ نتيجة هجمات إرهابية، سوف تكون انعكاساتها على المدنيين رهيبة، وسوف تطال حياتهم المعيشية، وتؤثّر على حقوقهم الإنسانية[29]. وهذا ما يُثير المخاوف بشأن ما إذا كان من الممكن للحرب السيبرانية عملياً أن تَمْتَثِل لمبادئ القانون الدولي الإنساني، ولا سيما مبدأ التمييز.

ومن الثابت عملياً، أنه لا يمكن خوض حروب دون تطبيق القانون الإنساني الدولي، ودون أنْ يلتزموا بتطبيق مبدأ التمييز أثناء تنفيذ هجماتهم على العدوّ، فالقانون الدولي الإنساني، الذي يُعرف بـ«قانون النزاعات المسلحة»، أو بـ«قانون الحرب»، يتكوّن من قواعد قانونية تُنظِّم سَيْر الحروب، وأهمّ هذه القواعد، ما ورد منها في اتفاقيات جنيف الأربع، وفي بروتوكوليها الإضافيين.

هذه القواعد، على الرغم من أهميتها، لا يَذْكُر أيّ منها الحرب السيبرانية، لأنها وُضِعَت في زمانٍ لم يكن فيه حروبٌ تُخاض في الفضاء السيبراني بواسطة أجهزة الكمبيوتر، والإنترنت، من خَلْف مكاتب مريحة في أماكن بعيدة عن ساحات القتال.

وبما أنّ الحرب السيبرانية باتت واقعاً جديداً يَهْتَمّ به المجتمع الدولي، والمخططون العسكريون باتوا يُدركون تهديدها، وفُرَصَ وقوعها، فلا بدّ من وجود قانون يُنظِّم سَيْرها، وشؤونها. هذا القانون يمكن أنْ يكون القانون الدولي الإنساني، الذي يرعى سَيْر النزاعات المسلحة، وشؤونها، عامةً، والذي يُعَدّ جزءاً من القواعد القانونية الدولية التي تحظى بتوافق دولي حولها.

ولكن ما يعترض هذه الإمكانية هو أنَّ المجتمع الدولي لم يَتَوَصَّل، بعد، إلى توافق في الآراء بشأن تطبيق القانون الدولي الإنساني على هذا النوع من الحرب. فقد حذَّرت بعض الدول، مثلاً، من أنّ العمليات السيبرانية قد تؤدي إلى تصعيد سباق التسلح، ورأت: إنّ القانون الدولي المعاصر لا يمتلك أية وسيلة تساهم في تنظيم شؤون استخدام هذا السلاح، وشؤون تطوّره، ورأى آخرون أنّ إطار القانون الدولي الإنساني الحالي غير مناسب للتعامل مع نموذج الحرب السيبرانية الجديد، ودعوا إلى وَضْع اتفاقية دولية جديدة تُنظّم استخدامها. أما البعض الآخر فقد رأى أنّ الإطار القانوني للقانون الدولي الإنساني الحالي يمكن أن ينطبق على الحرب السيبرانية عن طريق القياس، أيْ أنه لا حاجة إلى تطوير قواعد سلوك الدول في الفضاء السيبراني، أو إلى إعادة ابتكار القانون الدولي العرفي، كما أن القواعد الدولية الحالية ليست بالية، والمعايير الدولية الطويلة الأمد التي تُوَجِّه سلوك الدولة، في أوقات السلم والنزاع، تنطبق على الفضاء السيبراني[30].

([29]) أنظر هربرت لين، النزاع السيبراني والقانون الدولي الإنساني، مختارات من المجلة الدولية للصليب الأحمر، عدد 886، المجلد 94، (صيف 2012)، ص 517 وما بعدها.

([30]) *International Strategy for Cyberspace*, Prosperity, Security, and Opennessin a Networked World the White House Washington, USA, May, 2011, p. 9.

وينطبق قانون الحرب على أيّ نزاع مسلح دولي أو غير دولي؛ والنزاع المسلح الدولي يقع عندما تكون هناك أعمال عدائية، تشمل، أو تقتصر على العمليات السيبرانية، التي تحدث بين دولتين أو أكثر[31]. أما النزاع المسلح غير الدولي فيقع عندما يكون هناك عنف مسلح مطوَّل، يشتمل، أو يقتصر على العمليات السيبرانية، التي تحدث بين القوات المسلحة الحكومية، وقوات جماعة مسلحة واحدة أو أكثر، أو بين هذه الجماعات. وهذا يعني أنّ النزاع السيبراني يقع عندما تجري أعمال عدائية متبادلة في الفضاء السيبراني، بين جهات دولية أو غير دولية. ولكنّ أنشطة الأفراد، والكيانات غير المرتبطة بالنزاع المسلح، لا ينطبق عليها قانون الحرب (القانون الدولي الإنساني)[32]. وبالتالي، عندما يَشُنُّ فردٌ، أو مجموعةٌ من الأفراد، هجمة سيبرانية على هدف معين، ولا يكون لهذه الهجمة صلة بنزاع مسلح، فإنّ مِثْل هذا الموقف لا يُنَظِّمه القانون الدولي الإنساني.

ويجدر الانتباه إلى أن تطبيق القانون الدولي الإنساني على الهجمات السيبرانية يمكن أن ينطوي على معضلة، سَبَبُها وجود صعوبات تتعلق بتحديد حدوث عملية سيبرانية، وبتحديد مَنْشَئِها، وبالغرض المقصود منها، وبتأثيراتها الدقيقة، ولكنّ هذه المعضلة لا تمنع تطبيق القانون الدولي الإنساني[33].

وبما أنّ مبدأ التمييز ينطبق على العمليات التي تُعَدّ هجمات عسكرية فقط، فإنّه في غياب معايير واضحة تُحَدِّد ما إذا كانت العمليات السيبرانية هجمات أم لا، سيظلّ من الصعب على أطراف النزاع التي تَسْتَخْدِم العمليات السيبرانية تحديد الظروف التي ينطبق فيها مبدأ التمييز أثناء تنفيذ هذه العمليات. وبما أنّ القانون الدولي الإنساني يحتاج إلى إيجاد توازن بين حماية المدنيين والأعيان المدنية من جهة، وضمان عدم تقييد العمليات السيبرانية العسكرية بشكل غير معقول من جهة ثانية؛ فإنّ الحاجة إلى توضيح تصنيف العمليات بين هجمات، وغير هجمات، تبقى مُلِحَّةً لكي تعرف الدول ما العمليات التي يُسْمَح بها، بموجب القانون الدولي الإنساني، وما تلك التي لا يُسْمَح بها، لأن غياب هذا الوضوح يُصَعِّب تطبيق مبدأ التمييز، وهنا لا بدّ من التمييز بين أشكال العمليات السيبرانية، فلا يمكن أنْ تُعَدَّ عمليات تُسبِّب إزعاجاً للمدنيين هجمات، وبالمقابل يجب أنْ تُعَدَّ العمليات التي تؤدي إلى آثار تَمَسّ حياة المدنيين وتُسَبِّب لهم المعاناة هجمات، ويجب أن يُطَبَّق عليها مبدأ التمييز بين المدنيين والمقاتلين.

أمّا كثرة المرافق ذات الاستخدام المزدوج فتجعل تطبيق مبدأ التمييز بين الأهداف العسكرية والأعيان المدنية، أثناء الهجمات السيبرانية، عملاً صعباً جداً، فالعديد من المرافق التي تُعَدّ، تقليدياً، مدنيةً من المرجح أن

---

(31) *TALLINN MANUAL on the international law applicable to cyber warfare*, Prepared by the International Group of Experts at the Invitation of The NATO Cooperative Cyber Defense Centre of Excellence, General editor: Michael N. Schmitt, (New York: Cambridge University Press, 2013, rule 30, p. 91_92).

(32) Ibid, para 7, p. 69.

(33) Ibid, para 9, p. 70.

تصبح أهدافاً دائمة أثناء الحرب السيبرانية، نظراً لاعتماد العالم الحديث على شبكات الكمبيوتر، والإنترنت، لتشغيل المرافق العامة، والاتصالات، والعمليات الاقتصادية، والتجارية، وهذا ما يزيد احتمال أن يصبح المدنيون والأعيان المدنية عُرْضَة للهجمات السيبرانية أكثر من ذي قَبْل. وإذا لم يكن هناك وسيلة للفصل بين المرافق ذات الاستخدام المدني والاستخدام العسكري تصبح كلّ المرافق المدنية عُرْضَة للهجوم السيبراني المُعادي. لذلك يجب أن يَستجيب القانون الدولي الإنساني لِمِثْل هذه التحديات عن طريق تكييف مبدأ التمييز معها.

2.1. إسناد المسؤولية عن انتهاك القانون الإنساني جراء الحرب السيبرانية.

عندما يتعلق الأمر بالنشاط السيبراني، فإنّ العالَم يعيش في ما يُسمى «حالة من عدم السلام»، أيْ حالةً من التنافس بين الدول وسطَ طيفٍ يقع أسفل عتبة العنف المدمِّر مادياً، لكن آثاره الضارة تتجاوز مستوى المنافسة المسموح به في زمن السلم[34].

والكثير من الدول، اليوم، قادر على استخدام الأدوات السيبرانية بشكل فاعِل، نظراً إلى أن الأجهزة، والتقنيات السيبرانية، أصبحت أكثر تقدماً، وأكثر انتشاراً، وبعض هذه الدول قادرٌ على شنّ هجمات سيبرانية يَصْعُب معها تحديد الحدّ الفاصل بين آثار بعضها الذي لا يصل إلى مستوى القوة المسلحة، وبعضها الآخر الذي يصل إلى مستوى القوة المسلحة. ويبدو أنّ كثيراً من الدول، والجهات الفاعلة غير الحكومية يَستخدِم الهجمات السيبرانية للإفلات من العقاب، ولِعِلْمه أنّ هجماته السيبرانية، على الأرجح، لن تؤدي إلى أن يَرُدّ الخصم عليها، ردّاً حركياً مسلحاً.

وإنّ التقلبات في عملية تحديد المسؤولية عن الهجمات السيبرانية داخل المجتمع الدولي، وإمكانية الوصول إلى قواعد إسناد صارمة تُشكِّل كلّها تحدّياً قانونياً كبيراً. والتحدّي القانوني المتعلق بإسناد الهجمات السيبرانية غير الشرعية يُعَدّ مشكلة يجب حلّها، لأنّ عملية الإسناد تهدف إلى تحديد الأفعال غير الشرعية، وإلى تحديد المسؤولية عنها.

وبالاعتماد على قواعد لجنة القانون الدولي، تتمثل نقطة الانطلاق، في السياق السيبراني، في كَوْن الدولة تتحمّل مسؤولية دولية عن الفعل الذي يُعزى إليها المتعلق بالفضاء السيبراني[35].

وتتحمل الدول المسؤولية عن أيّ فعل غير شرعي متعلقٍ بالسايبر يقوم به بعض مسؤوليها، أو بعض التابعين لها من وكلاء، أو مقاولين، أو جهات فاعلة غير حكومية، ما دامت تُسيطر على أفعال هؤلاء سيطرةً

---

(34) Lucas Kello, The *Virtual Weapon and International Order*, (Great Britain: Yale University press New Haven and London, 2017, p. 78).

(35) *Tallinn Manual 2.0* On the International law applicable to Cyber Operations, Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence, General editor Michael N. Schmitt, (USA: Cambridge University Press, 2017, Rule 14, p. 84).

فعلية[36] . ولا يمكن للدول أن تتهرب من المسؤولية القانونية عن الأفعال غير الشرعية التي ترتكبها عَبْر وكلاء[37].

وفي نطاق الهجمات السيبرانية التي تأتي في سياق نزاع دولي مسلح، وهي قد تطوي أفعالاً غير شرعية، وانتهاكات للقانون الإنساني الدولي، فإن الجهة التي تتحمل المسؤولية هي الدولة. وإنّ أحد الشروط الأساسية لتحميل المسؤولية الدولية لدولة ما، هو أن يُعْزَى السلوك غير الشرعي إلى هذه الدولة بموجب القانون الدولي[38].

ومع مرور الوقت، تتطور الآليات التقنية، والقانونية التي تسمح بتحديد مستوى مشاركة دولة ما في عمليات سيبرانية للإعلان عن أنّ هذه الدولة مسؤولة قانوناً عن عمل سيبراني. فالدول، اليوم، أكثر قدرة على إسناد الهجمات السيبرانية مما كانت عليه قَبْلَ سنوات خَلَت. ومع ذلك، فإنّ البيئة التقنية تَتَّسِم بالديناميكية، وبالتحسّن المستمر، إذْ إنّ الأدوات التقنية الجديدة تعمل باستمرار إمّا على تحسين قدرات الإسناد، وإمّا على إعاقتها. فالغشّ، والقدرة على التخفي، وعلى تطوير العمليات السيبرانية يؤديان إلى تعقيد عمليةِ الإسناد، وعمليةِ الاستجابة، خصوصاً عندما يكون هناك حاجة إلى استجابة فورية، ضدّ دولة تُعَدّ الجاني المشتبه فيه الذي قام بالعملية السيبرانية[39].

ومع استمرار العلاقات الدولية السيبرانية، تستفيد بعض الدول المتقدِّمة، التي لديها القدرات السيبرانية الهجومية عالية المستوى، من عدم وجود قواعد صريحة تساهم في إسناد مسؤولية إليها إذا ما قامت بعمليات سيبرانية ضدّ دول ضعيفة. وفي الوقت نفسه، إنّ الخلَلَ في عملية الإسناد الحاصلَ بين الدول القوية، والدول الضعيفة، يُعادل سِباق التسلح الذي يأخذ شكل سِباق بين التقدّم في الكشف عن المسؤول، والتهرّب من الكشف عن هذا المسؤول. وهذا التهرّب أصبح، اليوم، سهلاً، لذلك يمكن للدول التي ليس لديها قدراتُ إسناد متقدِّمة أن تَسْتَمِرّ في إخفاء نفسها، بشكل موثوق به[40].

ونظراً إلى أنّ معظم الدول المتقدِّمة سيبرانياً تُدْرِك مخاطر التصعيد السيبراني، فإن لدى هذه الدول

---

[36] *Tallinn Manual 2.0*, op. cit, Rule 15, p. 87.

[37] Ibid, Rule 17, p. 92_95.

[38] يُراجع المواد 1 حتى 11، من **مشاريع المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً**، تقرير لجنة القانون الدولي إلى الجمعية العامة عن أعمال دورتها الثالثة والخمسين، حولية لجنة القانون الدولي، م. 2، ج. 2، (الأمم المتحدة: 2001، ص 32).

[39] Brian J. Egan, *Remarks on International Law and Stability in Cyberspace*, Berkeley Journal of International Law, vol. 35, Issue 1, (2017), p. 177.

[40] *Cyber Strategy,* Summary, U.S. Department of Defense, (USA, 2018), p. 1. (https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF) (last site visit november 2025).

سبباً وجيهاً لتكون أكثر شفافية بشأن عملية الإسناد، وأكثر مَيْلاً إلى تبادل المعلومات المتاحة لديها حول العمليات السيبرانية مع الدول غير المتقدمة سيبرانياً. ولكنّ مخاوف الدول حول الكشف عن مصادر استخباراتها، وعن الأساليب التقنية المتَّبَعة في عمليات الإسناد، ما زالت تُعَدّ عائقاً أمام القيام بعمليات إسناد المسؤولية بشكل شفّاف. وأخيراً، يبدو أنّ هناك حاجة إلى وَضْع معايير دولية تُوضّح طرق الإسناد، وتُنظّمها، بشكل يُساعد الدول في الكشف عن مصادر الهجمات، وفي تحديد المسؤول عن الانتهاكات، والأفعال غير الشرعية.

2. **انطباق القانون الإنساني على أنظمة أسلحة المستقلة وتحديات فرض المسؤوليات القانونية.**

الاستقلال في أنظمة الأسلحة، يعني قدرة هذه الأنظمة على اختيار الأهداف، والتعامل معها، بشكلٍ مستقل عن أيّ مشغِّل بشري، وذلك بناءً على الاستنتاجات التي تستخلصها من المعلومات المُجَمَّعة فيها، ومن قيودها المبرمجة مُسَبَّقاً. وأنظمة الأسلحة المستقلة ليست أسلحة المستقبل فحسب، بل أسلحة الحاضر أيضاً، لأنها موجودة اليوم، ومُسْتَخْدَمَة. هذه الحقيقة لها آثار عميقة على النقاش حول قانونية استخدام هذه الأسلحة. والسؤال الحاسم ليس حول ما إذا كان ينبغي حَظْر بعض هذه الأسلحة، أم لا، بل كيف يمكن استخدام القانون على أفضل وجه من أجل تنظيمها؟

وقد رأى بعض الباحثين أنه من المستحيل تطوير أنظمة أسلحة يمكنها الامتثال لقواعد القانون الإنساني الدولي، لأن مصطلحات القانون الإنساني الدولي كالمدنيين، والمقاتلين، والمشاركة المباشرة في الأعمال العدائية، وما إلى ذلك، لا تَخْضَع لتعريفات دقيقة، يمكن برمجتها، وترجمتها إلى شيفرات، وتضمينها في آلة[41]. وأمام هذا الواقع يَرْتَسِم سؤالان: هل يمكن أن ينطبق القانون الإنساني الدولي الحالي على هذه الأنظمة؟ وهل يمكن تحديد المسؤولين عن الهجمات التي تؤدي إلى انتهاك القانون الإنساني؟ وللإجابة عن هذين السؤالين تم تقسيم هذا المبحث إلى المطلبين الآتيين:

1.2. انطباق القانون الإنساني على أنظمة الأسلحة المستقلة.

2.2. المسؤولية عن انتهاك مبادئ القانون الإنساني أثناء استعمال الأسلحة المستقلة.

1.2. انطباق القانون الإنساني على أنظمة الأسلحة المستقلة.

إنّ أنظمة الأسلحة المستقلة التي يُطْلَقُ عليها اسم «الروبوتات القاتلة»، أو «الروبوتات المستقلة القاتلة»، أو «أنظمة الأسلحة الذاتية التشغيل»، تَتَّصِف بأنها:

– أنظمة أسلحة تتمتع بالاستقلالية في عملها، وتعمل دون مُشغِّل بشري، أو بإشراف مُشغِّل بشري يُتَخَلّى

(41) Thompson Chengeta, *Measuring autonomous weapon systems against international humanitarian law rules*, Journal of law and cyber warfare, Editor-in-Chief, Daniel B. Garrie, Partner, Law & Forensics, Vol. 5, Issue 1, (Summer 2016), p. 63.

عن إشرافه بَعْد تنشيط نظام السلاح[42].

- تمتلك استقلالية الخيار في اختيار الأهداف أثناء النزاع المسلح، وفي استخدام القوة المميتة ضدّها.
- تمتلك مواصفات تقنية وفنية، وذكاءً صناعياً يُمَكِّنها من تَعَلُّم كيفية التصرف في ميدان النزاع، ومن تكييف عملها مع المُتغيرات التي تطرأ على أرض النزاع.
- قادرة على اتخاذ الإجراءات اللازمة أثناء النزاع، وتحديد طريقة التصرف دون الاعتماد على مُشَغِّل بشري. وقادرة على تحديد الأهداف، والاشتباك معها، ثمّ مُهاجمتها[43].

وفي أيّ حال من الأحوال، قد تكون المزايا والمواصفات التي تتمتع بها أنظمة الأسلحة المستقلة، دوافع إلى استخدام هذه الأنظمة، ولكن على الرغم من ذلك تبقى هذه الأنظمة خاضعة لمبادئ القانون الدولي الإنساني، ويجب أن تكون قادرة على الالتزام بمبادئه.

ومن الجلي أن اتفاقيات جنيف، وبروتوكوليها الإضافيين لا تتحدث عن أنظمة الأسلحة المستقلة، لأنه لم يكن لهذه الأنظمة وجود عند وَضْع هذه الاتفاقيات، ولم يكن يَخْطُر ببال واضعيها أنّ حروباً سوف تُخاض بواسطة وسائل حربية غير بشرية تستطيع الواحدة منها المحاربة كأنّها مقاتل بشري بحدّ ذاته، ومَنْ يستعملها من البشر يُراقب عملها من بعيد، ويتدخّل فيه حينما يريد.

ولكن ليس هناك شكّ في أن تطوير الأسلحة، واستخدامها في النزاعات المسلحة، والالتزام بإجراء مراجعات قانونية أثناء دراسة سلاح جديد، أو تطويره، أو حيازته، أو اقتنائه، أعمال تخضع للقانون الإنساني الدولي، وفقاً لما تقتضيه المادة 36 من البروتوكول الإضافي الأول[44]. وهذا ينطبق على أنظمة الأسلحة المستقلة التي يجب أن تكون قادرة على التكيّف مع مبادئ: أخذ الاحتياطات اللازمة، والتناسب، والتمييز، المعنيّة بالتخفيف من آثار الحرب على المدنيين.

ومبادئ القانون الإنساني، لا يمكن أن تلتزم بها أنظمة الأسلحة المستقلة، لأن هذه المبادئ تَحتاج إلى

---

(42) كريستوف هاينز، تقرير المقرر الخاص المعني بحالات الإعدام خارج نطاق القضاء أو بإجراءات موجزة أو تعسفاً، مجلس حقوق الإنسان، الدورة 23، 9 نيسان 2013، الأمم المتحدة، A/HRC/23/47، الفقرة 37، ص 10.

(43) SEE. *MIND THE GAP,* The Lack of Accountability for Killer Robots, The International Human Rights Clinic (IHRC), Harvard Law School, Human Rights Watch, USA, (2015), p. 6.

(44) المادة 36 من البروتوكول الأول، شريف عتلم، محمد ماهر عبد الوهاب، موسوعة اتفاقيات القانون الدولي الإنساني، النصوص الرسمية للاتفاقيات والدول المصدقة والموقعة، ط. 6، (القاهرة: إصدار بعثة اللجنة الدولية للصليب الأحمر بالقاهرة، 2002)، ص 283.

قُدرة الإنسان على جمع المعلومات، وتحليلها، والتعامل مع واقع النزاع بناءً على ما يستوجبه الضمير الإنساني القويم، ولأنها تتضمن تعقيدات لا يمكن أن تُضَمّن في برامج هذه الأنظمة، ومن هذه التعقيدات: تعريف المدنيين، والمقاتلين، ومفهوم المشاركة المباشرة في الأعمال العدائية.

لذلك فإنّ نشر أنظمة أسلحة مستقلة لا تقدر على التمييز بين المدنيين والمقاتلين يُعَدّ انتهاكاً للقانون الإنساني الدولي، وأمراً لا يُمكن قَبوله في بيئات النزاعات المسلحة الفوضوية التي يُمكن أن يكون فيها المدنيون جزءاً من ساحة النزاع، لأن قرارات استهداف المقاتلين، أو المدنيين تحتاج إلى الضمير الإنساني القويم، ولا يمكن تفويض هذه القرارات إلى أنظمة أسلحة لا يُعْرَف مدى قُدرتها على التعامل مع واقع النزاعات المُتغيّر.

وتَصْعُب ترجمة بعض جوانب القانون الدولي الإنساني، كي تُضَمَّن في برنامج كمبيوتر، ومن هذه الجوانب التوجيه التفسيري الذي وَضَعته اللجنة الدولية للصليب الأحمر بشأن مفهوم المشاركة المباشرة في الأعمال العدائية، أو التفسيرات المختلفة التي وَضَعتها بعض الدول لهذا المفهوم؛ ففي سياقات النزاعات اليوم، يُشارك المدنيون بشكل مباشر في الأعمال العدائية، مما يجعل تطبيق مبدأ التمييز صعباً على الجنود العاديين، فما حال الأسلحة المستقلة[45]؟

وإذا كان لا بدّ من برمجة روبوت، فإنه لا يمكن، في أي حال من الأحوال، أن يُبَرمَج على أنّ «هذا يعتمد على كذا»، أو على أنْ «يَسْتَخْدِم حكماً منطقياً»، وبعبارة أخرى، لا يمكن أن تَتِمّ برمجته على أنّ الإجراء المناسب يعتمد على موقف محدد دون توضيح الإجراء الذي يجب أي يُتَّخذ في هذا الموقف؛ وتبقى الحاجة إلى وضوح كيف يتصرف هذا الروبوت أولويةً عند وَضْع برنامج كمبيوتر عن العوامل التي يعتمد عليها قرار الاستهداف، وكيفية تحديد تلك العوامل[46].

وتَرْتَسِم أمام استخدام أنظمة الأسلحة المستقلة مشكلةٌ تتعلق بالقدرة على تصنيف العمل الذي يقوم به المشارك في الأعمال العدائية بأنه مشاركةٌ مباشرة، وليس مشاركةً غير مباشرة.

وفي كثير من الحالات، يمكن أن يشارك شخص ما بشكل غير مباشر في المجهود الحربي الذي يقوم به أفراد القوات المسلحة، لكنّ هذه المشاركة لا تؤدي إلى فقدانه الحماية من الاستهداف. ومن الأمثلة على هذه المشاركة، المشاركة في إنتاج الأسلحة، وبيعها، ونقلها، وتوفير الأموال، والإدارة، والدعم السياسي، وصيانة البنية التحتية العسكرية، وفي هذه الحالة تحتاج أنظمة الأسلحة المستقلة، ولا سيما تلك التي لا تخضع لتحكُّمٍ بشريّ ذي معنى بعد تنشيطها، إلى ذكاء اصطناعي مكافئ للذكاء البشري كي تتمكن من التمييز بين المشاركة المباشرة في

(45) Marco Sassóli, Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to be Clarified, International Law Studies, U.S Naval College, vol. 90, (2014), p. 313.

(46) Marco Sassóli, op. cit, p. 329.

الأعمال العدائية، والمشاركة غير المباشرة، وهذا التمييز يُعَدّ تمييزاً نوعياً[47].

أمّا القيود الزمنية المتعلقة بموعد استهداف المدني المشارك مباشرة في الأعمال العدائية فَتُمثّل فكرة يَصْعُب تضمينها في نظام سلاح مستقل، لأن المدني ليس سوى هدف مشروع في الوقت الذي يُشارك فيه في القتال، ولكن هذا القيد الزمني يُعَدّ عند بعض الباحثين شرطاً غير عادل لأنه يُتيح لبعض المدنيين أن يكونوا مُزارعين في النهار، ومقاتلين في الليل، من أجل أن يَفِرّوا من استخدام القوة غير الشرعي. وفي هذه الحالة ليس بإمكان نظام سلاح مستقل أن يتمكّن من فَهْم واقع المدنيين الذين يشاركون في العمليات العدائية ليلاً ويَكُفّون عنها نهاراً، وليس بإمكانه تحديد أيّ خيار سيتخذه عند استهداف هؤلاء المدنيين.

ويَطْرَح شرطُ مُهاجَمة المدنيين أثناء مُدَّة مشاركتهم في الأعمال العدائية، فقط، تحدّيات خاصة في مجال مكافحة الإرهاب. لأنه في بعض الحالات يُعَدّ الإرهابيون مدنيين، وبسبب سِرِّيّة عملياتهم، فإنه من الصعب، إنْ لم يكن من المستحيل، تحديد النقطة التي يمكن للمرء أن يقول فيها: إنهم يشاركون مباشرة في الأعمال العدائية. ففي العمليات التي قامت بها بعض الدول ضدّ الإرهاب، بواسطة طائرات بلا طيار (Drones)، مثلاً، لم يكن استهداف الإرهابيين على أساس المشاركة المباشرة في الأعمال العدائية فحسب، بل على أساس عضويتهم في منظمة إرهابية، أيضاً، أو على أساس الاشتباه في عضويتهم. فقد تمَّ تنفيذ هجمات، من قبل بعض الدول، ضدّ الإرهابيين المُشْتَبَه بهم، خارج ساحة المعركة، حيث تَمّ توجيه هذه الهجمات في سلسلة من المناطق المضطَرِبة، أو الخارجة على القانون، في عدد من البلدان في جميع أنحاء الشرق الأوسط[48].

واستهداف الأفراد على أساس أنهم أعضاء في منظمة إرهابية معيّنة، أو أعضاء مُشْتَبَهٍ بهم، يتعارض مع مبدأ التمييز[49]. وقد يكون لهكذا استهداف تداعيات على أَمْن المدنيين؛ ولهذا السبب، يجب الاعتراض على استخدام أنظمة أسلحة مستقلة من أجل القيام بعمليات الاستهداف، ويجب التحذير من هذه الأنظمة المستقلة التي يمكن أن تكون أشدّ خطراً على المدنيين من الطائرات بلا طيّار(Drones).

2.2. المسؤولية عن انتهاك القانون الدولي الإنساني أثناء استخدام أنظمة الأسلحة المستقلة.

إن استخدام أنظمة أسلحة مستقلة لا يُسيطر عليها البشر أثناء النزاعات المسلحة، بدلاً من أسلحة يُسيطر عليها البشر، وعدم القدرة على تحديد الجهة المسؤولة عن أيّ انتهاك يحصل أثناء استخدام هذه

(47) Autonomous weapon systems: technical, military, legal and humanitarian aspects, expert meeting, International Committee of the Red Cross, Geneva, Switzerland, (26 to 28 March 2014). p. 7_8.

(48) Anthony Dworkin, *Drones and targeted killing: defining a european position*, European council of foreign relations, Policy brief, (July 2013), p. 1.

(49) Genevieve Lennon and Clive Walker, Routledge Handbook of Law and Terrorism, first edition (United Kingdom, London: Taylor & Francis Ltd, 2015, p. 58).

الأنظمة، أمران قد يؤديان إلى ما يمكن أن يُسمى فجوة المسؤولية.

وقد لَخَّص بعض الخبراء العقبات التي تَحُول دون قُدرة أنظمة الأسلحة المستقلة على الامتثال لقواعد القانون الدولي الإنساني، بما يأتي: الموثوقية، وعدم اليقين بمآلات التشغيل في غياب الإشراف البشري، ومخاطر التداخل، وقابلية الكشف (أي إمكانية اختراق البرنامج بناءً على هجوم سيبراني)، والتأخّر في معالجة الخوارزميات في الحالات المُعقَّدة، والتأخّر في البحث في مفاهيم التعلّم الذاتي، والتقويم الذاتي والتدريب، وتطوير الذكاء الاصطناعي، سواء بَعْد التصنيع، أم عَبْر الفضاء السيبراني. هذه العقبات التي تَفْرِض نفسها على عمل الأنظمة المستقلة تُعَدّ عائقاً كبيراً في طريق إمكانية تحديد المسؤولية عن الانتهاكات التي قد تحصل أثناء استخدام هذه الأنظمة في النزاعات المسلحة، وهذا ما يستدعي وجود اتجاه إلى حَظْر هذه الأنظمة.

وفي مقابل ذلك ظهرت آراء تتصور أنه في سياق الحرب ليس هناك واقع مثالي، ولا يُعَدّ وجود ثغرات في المسؤولية، حُجةً لِحَظْر استخدام هذه الأنظمة. وبدلاً من هذا الحظر، يجب القبول بحتمية فجوات المسؤولية في سياق الحرب، بنفس الطريقة التي يُقْبَلُ فيها مِثْل هذه الفجوات في المواقف الأخرى، ومثال هذه المواقف: انهيار جسر تسبب بحادث مميت، فقد نجد أنفسنا في موقف لا يمكن فيه مُساءلة أحد، وبالتالي، إذا تَمّ بناء الجسر وفقاً للتشريعات والقواعد والمعايير، وإذا لم يكن من الممكن تَوَقُّع الظروف التي أَدّت إلى انهياره، على الرغم من الحسابات الدقيقة، فإننا نقبل أن هناك فجوة طبيعية في المسؤولية قد تأتي على شكل تسامح هندسي (Engineering Tolerance)[50].

وبالانتقال إلى واقع تنظيم أنظمة الأسلحة المستقلة، فإن هناك مشكلة تتعلق بالقدرة على تحديد مسؤولية المُستخدِم (المسؤولية الجنائية)، ومسؤولية الجهة التي صنعت هذه الأنظمة (مسؤولية المُنْتِج)[51]. فنَشْر أنظمة أسلحة مستقلة لا يعني أن الجهة الرئيسية التي نشرتها يمكن أن تَتَجَنَّب المسؤولية، ويُقاس هذا على قضية، استخدام الأطفال على أنهم جنود، هذا الأمر الذي لا يخلق فجوة في المسؤولية، حيث يَتِمّ إسناد المسؤولية إلى القائد المسؤول عن استخدامهم[52].

وهنا يمكن أن تكون المسؤولية مخصصة لمستوى الجنرال أو الرئيس، الذي يُقَرِّر نَشْر نظام سلاح مستقل مُميت أو عدم نَشْرِه، وبعد ذلك، يَتِمّ تحميله المسؤولية إذا حدث خطأ ما. وكذلك، يمكن القول: إنّ أيّ

([50]) Vincent C. Müller and Thomas W. Simpson, Autonomous Killer Robots Are Probably Good News, Sociable Robots and the Future of Social Relations, Frontiers in Artificial Intelligence and Applications, vol. 273, Ios press, (2014), p. 304.

([51]) Vincent C. Müller and Thomas W. Simpson, Killer Robots: Regulate, Don't Ban, BSG Policy Memo, (November 2014). (https://philpapers.org/archive/MLLKRR.pdf) (last site visit november 2025).

([52]) Müller and Simpson, Killer Robots, op. cit.

نموذج يُحَدِّد سلسلة مسؤوليات بمعزلٍ عن الأطراف المعنية بانتهاكات قد تحصل أثناء نزاع مسلح لا ينبغي أنْ يُوْضَع مُسَبَّقاً، بل ينبغي أن تُراعى، عند وَضْعه، إمكانية أن تتحمّل تلك الأطراف المسؤولية عن تلك الانتهاكات. وليس غريباً عن الواقع أنّ يُحمِّل مبدأ مسؤولية القيادة عن الإهمال قائداً ما المسؤوليةَ عن عدم منعه ارتكاب انتهاك ما، أو عن عدم معاقبته المُرْتَكِب. والمواقف التي يَعجز فيها القائد عن منع أيّ عمل غير شرعي يقوم به مرؤوسوه، يتحمل المسؤولية نيابةً عنهم لأنّ من المفترض أن يكون للقائد سيطرة فعّالة، وأن يكون له قُدرة على منع المخالفات المحتملة. وبالتالي، فإنّ مسؤولية القيادة تستوجب، عندما يتعلق الأمر بأنظمة الأسلحة المستقلة، منظوراً إنسانياً، وتساؤلاً عمّا إذا كان القادة العسكريون في وَضْعٍ يسمح لهم بفَهْم برمجة هذه الأنظمة المُعقَّدة فهماً يُبَرِّر مسؤوليتهم الجنائية.

وإذا لم يكن بالإمكان، عملياً، العثور على قائد، أو مُبرمِج، أو صانع، ليكون مسؤولاً عن الانتهاكات، فإنّه يُخشى أن تكون هناك فجوة في تَحَمّل المسؤولية من شأنها أن تُتيح الإفلات من العقاب بسبب استخدام أنظمة الأسلحة المستقلة.

وهنا يمكن وَضْعِ إعلانٍ سياسيٍّ دولي يُؤكد أمراً أساسياً مفاده أنّ مِنْ مسؤولية البَشَر: (أ) اتخاذُ القرارات النهائية في ما يتعلق باستخدام القوة، و(ب) التحَكُّمُ في منظومات الأسلحة الذاتية التشغيل[53]. ويمكن أن يَعْقُب ذلك وَضْع مدوّناتٍ لقواعد السلوك، ومزيدٍ من تدابير بناءِ الثقة. وتضمين هذه المدوَّنات وظيفةَ استعراضٍ للتكنولوجيا الحربية المتطورة. ولكن هذا الإعلان السياسي ينبغي أن يكون خطوة مرحلية تَسْبِق إبرام صكّ مُلزم قانوناً يمكن أن يَتَّخِذ شَكْل بروتوكول جديد يُضاف إلى اتفاقية الأسلحة التقليدية.

الخاتمة

تناولت هذه الدراسة موضوع الحرب السيبرانية والأسلحة المستقلة في إطار القانون الإنساني الدولي، وقد ركزت على مدى انطباق هذا القانون على استخدام هذا النوع الجديد من الحروب والوسائل القتالية الحديثة، وركزت على تحديد المسؤوليات عن انتهاك هذا القانون جراء استخدام هذه الأسلحة وأساليب القتال التي لم تلحظها اتفاقيات جنيف والبروتوكولات الإضافية أثناء وضع نصوصها في عام 1949 وما بعده.

وانطلاقاً مما تناولته هذه الدراسة، يمكن القول في إطار ما وصلت إليه من نتائج: إنه في سياق الحرب السيبرانية يجب أن يَتِمّ تصنيف العمليات السيبرانية بين هجمات، وغير هجمات، لكي تَعْرِف الدول ما العمليات

([53]) تقرير اجتماع 2018 لفريق الخبراء الحكوميين المعني بالتكنولوجيات الناشئة في مجال منظومات الأسلحة الفتاكة الذاتية التشغيل، جنيف، 9_13 نيسان/أبريل ٢٠١٨ و ٢٧ – ٣١ آب/أغسطس 2018، (CCW/GGE.1/2018/3)، الفقرة 48، ص 27_28.

التي يُسْمَح بتوجيهها ضدّ العدوّ، بموجب مبادئ القانون الإنساني الدولي عامة، وما تلك التي لا يُسْمَح بها.

أما في ما يتعلق بمبادئ القانون الإنساني الدولي ولا سيما: التمييز، والتناسب، والضرورة العسكرية، وأَخْذ الاحتياطات اللازمة أثناء الهجوم، فإن هذه المبادئ تتضمن تعقيدات كثيرة كتعريف المقاتلين، وتعريف الأهداف العسكرية، ومفهوم مشاركة المدنيين المباشرة في الأعمال العدائية، ومفهوم أَخْذ الاحتياطات اللازمة أثناء الهجوم، وغيرها من المفاهيم المعقَّدة. هذه التعقيدات تحتاج إلى قدرات الإنسان على جمع المعلومات، وتحليلها، والتعامل مع واقع النزاع المسلح بناءً على ما يستوجبه الضمير الإنساني القويم، وهذه القدرات الإنسانية ليست مُتَوَفِّرة لأنظمة الأسلحة المستقلة، لذلك، فإنّ هذه الأنظمة لا يُمكن أن تَلْتَزم مبادئ القانون الإنساني، وما تتضمّنه من مفاهيم مُعَقَّدة.

وأمّا في ما يتعلق بالمسؤولية عن انتهاك القانون الإنساني الدولي، فإنّ الدول تُعَدُّ الجهةَ التي يمكن أنْ تتحمّل المسؤولية عن الهجمات السيبرانية التي تأتي في سياق نزاع دولي مسلح، والتي تنطوي على أفعال غير شرعية، وعلى انتهاكات للقانون الإنساني. أمّا المسؤولية عن الانتهاكات التي قد تَنتج عن استخدام أنظمة الأسلحة المستقلة، فالجهات التي يمكن أنْ تتحمّلها كثيرة، أبرزُها: الأشخاص الذين يقومون ببرمجة هذه الأنظمة، والقادة والجنود الذين يَنْشُرونها، والدول التي تُجيز استخدامها.

وفي الختام، لا بدّ من القول: إن استخدام أسلحة جديدة واستعمال أساليب قتالية حديثة لم يتمّ ذكرها ضمن قواعد القانون الإنساني الدولي العرفي، واتفاقيات جنيف، يجب أن يكون يتوافق مع هذه القواعد المعمول بها، فهي كافية للدول لتسترشد بها في حروبها، ولكي تتجنب استهداف المدنيين وتخفيف آلام الحرب عنهم. ولا بدّ، أيضاً، من تطوير قواعد القانون الإنساني بما يتناسب مع مستجدات الحروب ووسائلها.

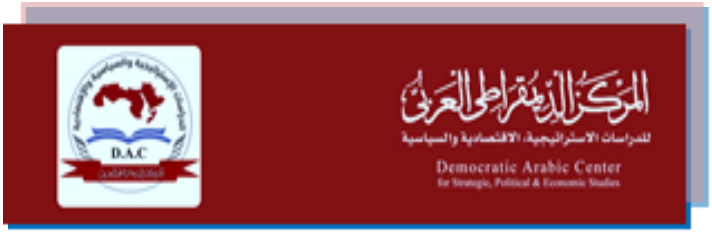
قائمة المراجع

- تقرير اجتماع 2018 لفريق الخبراء الحكوميين المعني بالتكنولوجيات الناشئة في مجال منظومات الأسلحة الفتاكة الذاتية التشغيل، جنيف، 9_13 نيسان/أبريل ٢٠١٨ و ٢٧ - ٣١ آب/أغسطس 2018، (CCW/GGE.1/2018/3).
- شريف عتلم، ومحمد ماهر عبد الوهاب، موسوعة اتفاقيات القانون الدولي الإنساني، النصوص الرسمية للاتفاقيات والدول المصدقة والموقعة، ط. 6، (القاهرة: إصدار بعثة اللجنة الدولية للصليب الأحمر بالقاهرة، 2002).
- كريستوف هاينز، تقرير المقرر الخاص المعني بحالات الإعدام خارج نطاق القضاء أو بإجراءات موجزة أو تعسفاً، مجلس حقوق الإنسان، الدورة 23، 9 نيسان 2013، الأمم المتحدة، A/HRC/23/47.

- مشاريع المواد المتعلقة بمسؤولية الدول عن الأفعال غير المشروعة دولياً، تقرير لجنة القانون الدولي إلى الجمعية العامة عن أعمال دورتها الثالثة والخمسين، حولية لجنة القانون الدولي، م. 2، ج. 2، (الأمم المتحدة: 2001).
- هربرت لين، النزاع السيبراني والقانون الدولي الإنساني، مختارات من المجلة الدولية للصليب الأحمر، عدد 886، المجلد 94، (صيف 2012).

- Anthony Dworkin, *Drones and targeted killing: defining a european position*, European council of foreign relations, Policy brief, (July 2013).
- Autonomous weapon systems: technical, military, legal and humanitarian aspects, expert meeting, International Committee of the Red Cross, Geneva, Switzerland, (26 to 28 March 2014).
- Brian J. Egan, *Remarks on International Law and Stability in Cyberspace*, Berkeley Journal of International Law, vol. 35, Issue 1, (2017).
- *Cyber Strategy*, Summary, U.S. Department of Defense, (USA, 2018) (https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF) (last site visit november 2025).
- Genevieve Lennon and Clive Walker, Routledge Handbook of Law and Terrorism, first edition (United Kingdom, London: Taylor & Francis Ltd, 2015).
- *International Strategy for Cyberspace*, Prosperity, Security, and Opennessin a Networked World the White House Washington, USA, May, 2011.
- Lucas Kello, The *Virtual Weapon and International Order*, (Great Britain: Yale University press New Haven and London, 2017).
- Marco Sassóli, Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to be Clarified, International Law Studies, U.S Naval College, vol. 90, (2014).
- *MIND THE GAP*, The Lack of Accountability for Killer Robots, The International Human Rights Clinic (IHRC), Harvard Law School, Human Rights Watch, USA, (2015).
- Paulo Shakarian and others, *Introduction to Cyber-warfare A Multidisciplinary Approach*, (USA: Syngress, Elsevier, 2013).
- Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, (New York: Harper Collins, 2010).
- *Tallinn Manual 2.0* On the International law applicable to Cyber Operations, Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence, General editor Michael N. Schmitt, (USA: Cambridge University Press, 2017).
- *TALLINN MANUAL on the international law applicable to cyber warfare*, Prepared by the International Group of Experts at the Invitation of The NATO Cooperative Cyber Defense Centre of Excellence, General editor: Michael N. Schmitt, (New York: Cambridge University Press, 2013).

- Thompson Chengeta, *Measuring autonomous weapon systems against international humanitarian law rules*, Journal of law and cyber warfare, Editor-in-Chief, Daniel B. Garrie, Partner, Law & Forensics, Vol. 5, Issue 1, (Summer 2016).
- Vincent C. Müller and Thomas W. Simpson, Autonomous Killer Robots Are Probably Good News, Sociable Robots and the Future of Social Relations, Frontiers in Artificial Intelligence and Applications, vol. 273, Ios press, (2014).
- Vincent C. Müller and Thomas W. Simpson, Killer Robots: Regulate, Don't Ban, BSG Policy Memo, (November 2014). (https://philpapers.org/archive/MLLKRR.pdf) (last site visit november 2025).


المركز الديمقراطي العربي
للدراسات الاستراتيجية الاقتصادية والسياسية
Democratic Arabic Center
D.A.C

للدراسات الإستراتيجية والسياسية والاقتصادية
المركز الديمقراطي العربي
D.A.C
Democratic Arabic Center GmbH