وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم

"دراسة على ضوء دليل "تالين" بشأن القانون الدولي المطبق على العمليات السيبرانية ٢٠١٣ – ٢٠١٧"

د. محمد عادل محمد عسكر

أستاذ مساعد بقسم القانون الدولي العام

كلية الحقوق– جامعة المنصورة

٢٠٢٠

قائمة المختصرات

1st	*First.*
21.th	*21century.*
3rd. edn.	*Third edition.*
AALCO	*Asian-African Legal consultative organization*
A. F. L. Rev	*Air War and the Law of War 32 Air Force Law Journal.*
AJIL	*American Journal of International Law.*
Alb. L.J. Sci. & Tech	*Albany Law Journal of Science and Technology.*
Am. Soc'Y INT'L L. Poc	*American Soc'y of Int'l Law & policy.*
AM. U. INT'L L. Rev.	*American University International Law Review*
B.C. Int'l & Comp. L. Rev.	*Boston College International and Comparative Law Review.*
BRIT. Y.B. INT'L L.	*British Year Book of International Law.*
CAL. L. REV	*California Law Review.*
CARDOZO J. Int'l & Comp. L.,	*Cardozo Journal of International and Comparative Law.*
CHINESE J. INT'L L	*Chinese Journal of International Law.*
CORNELL L. Rev.	***Cornell Law Review****.*
CNN	*Cable News Network.*
DDoS	*Distributed Denial of Service.*
Denv. J. Int'l L. & Pol'y,	*Denver Journal of International Law and Policy.*
ECR	*European Conservatives and Reformists.*
ELINT	*Electronic Intelligence.*
ESCWA	*Economic and Social Commission for Western Asia*
FAO	*Food and Agriculture Organization.*
GEO. L. J.	*Georgetown Law Journal.*
GEO. WASH. L. REV.	*The George Washington Law Review.*
GGE	*Group of Governmental Experts.*
HARV. INT'L L.J.	*Harvard International Law Journal*
HUMINT	*Human intelligence.*
ICRC	*The International Committee of the Red Cross.*
ICTR	*International Criminal Tribunal for Rwanda.*
ICTY	*The International Criminal Tribunal for the former Yugoslavia.*
IGE	*Intergovernmental Group of Experts.*
ILO	*International Labour Organization.*
ILSA	*International Law Students Association.*
Inc.	*Incorporation.*
Int'l Crim. Trib.	*The international criminal tribunals.*
Int'l J. Intelligence &	*International Journal of Intelligence and Counterintelligence.*

Counterintelligence	
Int'l L. & Pol	*International Law and policy.*
Int'l L Stud. Ser. US Naval War College	*International Law Studies Series. US Naval War College.*
Int'l Rev. Red Cross	*The International Review of the Red Cross.*
ITLOS	*International Tribunal for the Law of the Sea.*
J. Air L. & Com	*Journal of Air Law and Commerce.*
J. CONFLICT & SECURITY L.7	*Journal of Conflict and Security Law.*
J. Crim. Law & Criminology	*Journal of Criminal Law and Criminology.*
J. Nat'l Sec L & Pol'y	*Journal of National Security Law & Policy.*
J. NAT'L ASS'N ADMIN. L.	*Journal of the National Association of Administrative Law..*
JAPANESE ANN. of Int'l L.,	*Japanese Annual of International Law.*
LEIDEN J. INT'L L.	*Leiden Journal of International Law.*
MAX PLANCK Y.B. U.N. L.,	*Max Planck Yearbook of United Nations.*
MELB. J. INT'L L.	*Melbourne Journal of International Law.*
MICH. J. INT'L L.	*Michigan Journal of International Law.*
MINN. L. REV	*The Minnesota Law Review.*
MIT Tech. Rev	*MIT Technology Review.*
NATO CCD COE	*NATO Cooperative Cyber Defence Centre.*
No.	*Number.*
N.Y. TIMES	*The New York Times.*
N.Y.U. J. Int'l L. & Pol	*New York University Journal of International Law and Politics*
OEWG	*Open-Ended Working Group.*
P.	*Page.*
Office of the Sec'y of Def.	*Office of the Secretary of Defense.*
PACE Int'l L. Rev	*Pace International Law Review.*
Para.	*Paragraph.*
PENN. ST. L. REV	*Penn State Law Review.*
PCA	*Permanent Court of Arbitration.*
P. R.	*Previous Reference.*
Ph.D	*Doctor of Philosophy.*
PUB. INT'L L.	*Public International Law.*
RSIL	*Research Society of International Law.*
RUSI	*Royal United Services Institute.*
SIGINT COMINT	*Signals Communications intelligence.*
STAN. L. & POL'Y REV.	*Stanford Law and Policy Review.*

U. Chi. L. Rev	*University of Chicago Law Review*
UNEP	*United Nations Environment Programme.*
UN.Doc	*United Nations Documents.*
United Nations Conf. Int'l Org	*United Nations Conference on International Organization*
UNDESA	*United Nations Department of Economic and Social Affairs.*
UNMOVIC	*United Nations Monitoring, Verification and Inspection Commission*
UN Women	*United Nations Entity for Gender Equality and the Empowerment of Women.*
UNODC	*United Nations Office on Drugs and Crime.*
UPU	*Universal Postal Union*
US DOD	*United States Department of Defense.*
V.	*Versus*
Va. J. Int'l L.	*Virginia Journal of International Law.*
Vol.	*Volume.*
WASH. POST	***Washington Post***
WFP	*World Food Programme.*
WHO	*World Health Organization .*
WIPO	*World Intellectual Property Organization.*
WSIS	*World Summit on the Information Society.*
W.W.W	*World Wide Web.*
YALE J. INT'L L	*Yale Journal of International Law*
YJIL	*Yale Journal of International Law.*

مُقَدِّمَة

أولاً: موضوع الدراسة:

رسَّخ التطور الجامح في مجال التكنولوجيا منذ منتصف القرن العشرين، لاستغلال الإنسان لبيئة الفضاء السيبراني، وتَحَوّل المعاملات في المجتمعات إلى الاعتماد على شبكة الإنترنت، سواء في الخدمات الحكومية، أم أعمال الشركات التجارية والمهن الفردية، أم التواصل بين الأفراد، وعلى مستوى الدول، أضحى هذا النمط هو جوهر إدارة أنظمة الأمن القومي[١]، وتشغيل البني التحتية للنظم الاقتصادية، والمالية، والاجتماعية، والسياسية، والعسكرية[٢]، وقد شَكَّلت هيمنة تلك التعاملات السيبرانية على جوانب الحياة، بيئة تهديد جديدة ومتطورة لأمن الدول وسلمها[٣]، وطرحت سيلاً من الإشكاليات المتعلقة بكيفية استغلالها، كتطويعها للقيام بهجمات الكترونية، ربما ترقي الآثار الناتجة عنها إلى ما تخلفه النزاعات المسلحة التقليدية من آثار، وقد تُمثّل تدخلاً غير مشروع في شئون الدول، أو تُقوِّض استقرارها، أو تُهدّد العلاقات الودية الدولية[٤].

ويُعرّف الفضاء السيبراني، بأنه مجال الكتروني يسمح بالتواصل العالمي بين الأفراد والكيانات والدول، وتداول معلومات وبيانات وتخزينها، وهو يَتَشَكَّل نتيجة تفاعل العنصر

---

(١) **يُعدُ اصطلاح "الأمن القومي" من المصطلحات الحديثة نسبيًا**، والتي يكثر استخدامها من جانب السياسيين والصحفيين، إلا مفهومه لا يزال غامضًا بشدة، وقد ترتب على هذا الغموض، حرية كل دولة في تحديد مفهومه بالنسبة لها، وبحيث أصبح لدي كل منها فقه الأمن القومي الخاص بها، ومؤسسات وأجهزة رسمية تتخصص في هذا المجال، وقد تعدَّدت التعريفات بشأنه، واتفقت غالبيتها على أنه يعني، قدرة الدولة على اتخاذ التدابير الضرورية لحماية مصالحها الأساسية من التهديدات الخارجية والداخلية المحيقة بها، بحيث تتولَّد حالة عامة من الاستقرار، وشعور الأفراد بالطمأنينة على أرواحهم وممتلكاتهم، فالأمن القومي هو أمن المجتمع والأفراد من خلال أمن الدولة، وهو حالة شعورية لا يمكن بلوغها، إلا من خلال التأكد من قدرة الدولة على اتخاذ كافة التدابير والإجراءات، اللازمة للدفاع عن المصالح المشروعة للجماعة. **راجع: د. محمد صافي يوسف**، تدابير حماية الأمن القومي كاستثناء على تطبيق قواعد القانون الدولي العام، المجلة المصرية للقانون الدولي، الجمعية المصرية للقانون الدولي، العدد السادس والستون، ٢٠١٠، ص ١٦٧، وما بعدها.

(٢) **تعتمد غالبية الأنشطة العسكرية المعاصرة لبعض الدول، كالولايات المتحدة الأمريكية، على استخدام تقنيات الكترونية**، في كافة المجالات العسكرية، والنزاعات وتدابير مكافحة الإرهاب، وتتأثر هذه الأنشطة من حيث تعثرها، أو تحقيق الهدف منها، وفقًا للإمكانات والقدرات المتعلقة بالإنترنت. **راجع:**

H. P. FAGA, *the Implications of Transnational Cyber Threats in International Humanitarian Law: Analysing the Distinction between Cybercrime, Cyber Attack, and Cyber Warfare in the 21st Century, Baltic Journal of Law & Politics, Vol. 10, No. 1, 2017, PP. 1: 5.*

(3) ***UN Secretary-General, 'Foreword',*** *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN.Doc.A/70/174, 22 July 2015.*

(4) ***S. HAROON,*** *International Humanitarian Law on Cyberwarfare and Pakistan's Legal Framework, Research Associate, Conflict Law Centre, RSIL, 2018, PP.11:13.*

البشري من مستخدمين ومشغلين مع عدة وسائل تقنية كأجهزة الحاسب الآلي، وشبكة الانترنت، وبرامج التشغيل، ويُمكن من خلاله توجيه عمليات، مثل "التسلل السيبراني"، و"الجريمة السيبرانية"، و"الهجمات السيبرانية"، و"الحرب السيبرانية"، و"التجسس السيبراني"، والتي تشترك في كونها تُمثّل اختراقًا للأنظمة الالكترونية للدولة الضحية، مع صعوبة تمييز مكان العملية، أو التعرف بسهولة على القائم بها، كما لا تتطلب التواجد على إقليم الدولة المُستهدفة[١].

وحري بالذكر، أن من بين الآثار الناتجة عن العمليات السيبرانية، ما قد يصل إلى التَحكم في أنظمة تشغيل مؤسسات الدول الحيوية، أو البني التحتية لها، وتدميرها، أو تعطيلها، وفقًا لخصائص وأهداف كل عملية، ومن ذلك تعطيل أو إتلاف النظم الالكترونية الخاصة بتشغيل أجهزة مؤسسات صحية، مما قد ينتج عنه وفيات، وتفاقم في درجة الإصابات، أو تعطيل نظم إدارة شبكات توزيع الكهرباء، وقطع التيار الكهربائي على نطاق واسع، وكذلك التحكم في محطات تنقية مياه الشرب، مما يجعل المياه ملوثة وغير صالحة للشرب، أو عرقلة نظام المرور للتسبب في حوادث، أو التأثير على فعالية سير النقل الجوي ـ الأرضي، أو التلاعب بإحصائيات تخص الأمن القومي، أو بيانات حكومية يعتمد عليها نظام الضمان الاجتماعي، أو نظام الضرائب الوطني، بحيث تتكبَّد الدولة المستهدفة أضرارًا مالية فادحة[٢].

وقد بدأت العمليات السيبرانية تثير قلق المجتمع الدولي، مع شن هجوم سيبراني على دولة "استونيا" خلال عام ٢٠٠٧، نتج عنه السيطرة على الأنظمة الالكترونية لمؤسساتها، وجعلها خارج الخدمة، وتعطيل بعض الخدمات الضرورية كالإطفاء، والإسعاف[٣]، وكذلك إثارة أزمة عرقية داخلية، بعد اختراق حسابات التواصل الاجتماعي لمواطنين، ونشر آراء تؤجج العنصرية، وقد تم توجيه اتهامات للحكومة الروسية باعتبارها مسئولة عن هذا الهجوم. ولم تستطع "استونيا" بوصفها عضوًا في حلف الناتو أن تطلب حق "الدفاع الجماعي" بموجب المادة

---

(1) ***EASTWEST INSTITUTE,*** *RUSSIA-U.S. Bilateral on Cybersecurity Critical Terminology Foundations 2 (James B. Godwin III et al. eds., Feb. 2014),* ***available at:*** *https://perma.cc/79P7-L3SP. 29/3/2020.*

(2) ***J. CARAVELLI, N. JONES****, Cyber Security: Threats and Responses for Government and Business, ABC-CLIO, LLC, 2019, PP. 49: 56.*

(٣) **لم تكن هذه الهجمات الأولي من نوعها،** إلا أنها كانت الأولي من حيث ضلوع الدول فيها، وكذلك حجم وشدة الآثار الناتجة عنها، وقبل هذا التاريخ، لم تتوقف الدول، ولا الكيانات الخاصة ولا الأفراد، عن القيام بعمليات سيبرانية لأغراض مختلفة، ومنها الهجمات السيبرانية التي قام بها طفل كندي يبلغ من العمر (١٥) عامًا، خلال عام ٢٠٠٠، واستهدف بها وقف الخدمة عن مستخدمي مواقع انترنت رئيسة مثل، "*Yahoo*"، "*eBay*"، "*Twitter*"، "*Netflix*"، "*CNN*"، وبالفعل أُغلقت هذه المواقع مؤقتًا، وتضررت مصالح بعض الدول والأفراد، إلا أن مثل هذه العمليات لم تنل الاهتمام الكافي دوليًا، لأسباب متعددة، منها أن الفاعل لم يكن دولة. **راجع:**

S. HAROON, *International Humanitarian Law on Cyberwarfare and Pakistan's Legal Framework, P. R., P. 12;* ***M. FAHEY, N. WELLS****, Yahoo Data Breach is among the Biggest in History, CNBC (Sept. 22, 2016),* ***available at:*** *https://perma.cc/92A2-N497. 1/4/2020.*

رقم (٥) من معاهدة حلف شمال الأطلسي[١]، لعدم قدرتها على تحديد هوية أو مكان القائم بالهجوم، والتي هي من خصائص العمليات السيبرانية[٢].

وفي عام ٢٠٠٨، أُستخدمت الهجمات السيبرانية في النزاع المسلح بين "روسيا"، "وجورجيا"، وتمكنت "روسيا" من الاستيلاء على (٥٤) موقعًا إخباريًا لجورجيا، وموقعًا رسميًا لوزارة الدفاع، وموقعًا ماليًا لأحد البنوك، وتم قطع خدمة الانترنت عن "جورجيا" لمدة ست ساعات، مما أدي إلى توقف ما قُدّر بنسبة ٣٥% من مؤسسات جورجيا المعتمدة على شبكات الإنترنت، ومنها البنك الوطني، الذي اضطر إلى تعليق جميع خدماته الالكترونية في الفترة من ٨ إلى ١٩ أغسطس، وقد تم كل ذلك بالتزامن مع شن عمليات عسكرية تقليدية[٣].

وخلال عام ٢٠١٠، تم شن هجوم الكتروني على المرافق النووية الإيرانية، عُرف بـ "*Stuxnet*"، حيث أُدخلت برامج الكترونية ضارة إلى النظام الالكتروني، المختص بتشغيل أجهزة الطرد المركزي التي تعمل على تخصيب اليورانيوم، مما أدى إلى إتلاف (١٠٠٠) جهاز طرد مركزي واستبعادها من الخدمة، مع اختفاء أي أثر للفيروس المُستخدَم في الهجوم بمجرد تحقق الأضرار، وصُنّفت الآثار الناتجة عن هذا الهجوم بأنها لم تكن لتحدث قبل تطوير القدرات الالكترونية إلا نتيجة هجوم مسلح مادي[٤].

---

(١) **قضت المادة رقم (٥) من اتفاقية "*North Atlantic Treaty Organization*"**، بأن أي هجوم مسلح ضد طرف أو أكثر، يعتبر هجومًا ضد جميع الأطراف، ومن ثم، فإنه في حالة شن هجوم مسلح على أحد الأطراف، فإنه يمارس حقه في الدفاع الفردي أو الجماعي، بما في ذلك استخدام القوة المسلحة، وفقًا للمادة (٥١) من ميثاق الأمم المتحدة، وبمساعدة طرف أو أكثر، وبالتنسيق مع الأطراف الأخرى. **راجع:**

M. N. SCHMITT, *PILAC Lecture on Cyber Operations and IHL: Fault Lines and Vectors, April 2015, Lecture at Harvard Law School,* ***available at:*** *http://pilac.law.harvard.edu/events/cyber-operations-and-international humanitarian-law-fault-lines-and-vectors. 20/12020.*

(٢) **وعلى سبيل المثال، وخلال عام ٢٠١٣**، تم شن هجمات سيبرانية، بدا أنها تنطلق من مركز الدفاع السيبراني لحلف الناتو (*CCD COE*)، وأسفرت عن تخريب مواقع الكترونية للحكومة الأوكرانية، وفي الواقع، لم تنطلق الهجمات من الحلف، حيث قام نفس المُهاجم بتوجيه بعض من الهجمات ضد موقع (*NATO*)، وضد قوات الدفاع الإستونية، وجيوش دول أخرى أطراف في الحلف، وخلال هذه الهجمات الأخيرة، جعل الأمر يبدو كما لو أن الحكومة الأوكرانية هي التي قامت بها، وبالتالي تكون هناك صعوبة في التعرف على هوية المهاجم بشكل صحيح في مثل هذه الحالات. **راجع:**

M. N. SCHMITT, L. VIHUL, *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 Defence Centre of Excellence, Cambridge University Press, Cambridge, 2019, PP. 91: 92.*

(٣) **بمجرد أن نشبت حالة العداء بين روسيا وجورجيا**، قام موقع الكتروني روسي، بتحميل قائمة بأنظمة "جورجيا" الالكترونية المُستهدفة، وكذلك البرامج التي يمكنها اختراق هذه الأنظمة، وأتاح الوصول إلى هذه القائمة والبرامج، لأي شخص مهتم بالمشاركة في الهجوم، وبالفعل اشترك الآلاف من الروس في هذا الأمر. **راجع:**

S. P. WHITE*, Understanding Cyberwarfare: Lessons from the Russia-Georgia War, Modern war institute, 2018, PP. 5: 6.*

(4) ***H. LIN, A. ZEGART****, Bytes, Bombs, and Spies, the Strategic Dimensions of Offensive Cyber Operations, BROOKINGS INSTITUTION PRESS, Washington, D.C.,*

وخلال نفس العام ٢٠١٠، أدانت وزيرة الخارجية الأمريكية حينها "هيلارى كلينتون"، الهجوم السيبراني، الذي تعرَّضت له شركة "*Google*"، منذ منتصف ديسمبر عام ٢٠٠٩، والتي انتهت التحقيقات إلى أن الغرض منه، تمثَّل في سرقة معلومات من البريد الالكتروني "*Gmail*"، تخص مواطنين صينيين يعملون في مجال حقوق الإنسان، وأعلنت " كلينتون" أنه هذا الهجوم يُمثّل جريمة بموجب القانون الدولي، ويعتبر اعتداءًا على المجتمع الدولي بأكمله، وأن الدول أو الجماعات المتورطة فيه، سوف تواجه إدانات دولية وعقوبات قاسية، وطالبت المجتمع الدولي باتخاذ إجراءات صارمة ضد أي دولة، أو كيان ينفذ هجمات الكترونية(١).

وخلال عام ٢٠١٤، جلبت ممارسات التجسس السيبراني، التي جرت خلال النزاعات بين "روسيا" و"أوكرانيا"، وأخري بين "فلسطين" و"إسرائيل"(٢)، وكذلك النزاع في العراق(٣)، و"ليبيا"(٤)، وسوريا"(٥)؛ مسألة التهديدات السيبرانية إلى واجهة الاهتمام الدولي، وأظهرت حاجة المجتمع الدولي المُلِّحة، إلى نمط قانوني أو تنظيم ساري، يُبيِّن كيف يُمكن تطبيق القانون الدولي على الممارسات السيبرانية(٦).

وقد وُصف عام ٢٠١٦ في الإعلام العالمي بأنه عام العمليات السيبرانية(٧)، وكان الحدث الأبرز فيه، هو اتهام الروس بالتدخل السيبراني للتلاعب بنتائج الانتخابات الأمريكية، حيث أعلن

2020, PP. 3: 4, 152; ***M. GERVAIS,*** *Cyber Attacks and the Laws of War, Berkeley Journal of International Law, Vol. 30, Issue 2, 2012, P.46.*

(1) ***I. LACHOW:*** *Cyber Terrorism: Menace or Myth? In: Kramer, Franklin, Starr, Stuart and Wentz, Larry Cyberpower and National Security. Publisher: Potomac Books Inc, US, 2009, PP. 440:441.*

(2) ***K. GEERS****, Cyber War in Perspective: Russian Aggression against Ukraine, NATO CCD COE Publications, Tallinn 2015.*

(٣) **سعت الولايات المتحدة قبل غزو العراق،** إلى تجميد الحسابات المصرفية لقادة العراق في أوربا، حتى لا يتم تمويل المواجهة العسكرية، ولم ينل هذا الاقتراح موافقة أوربية، نظرًا لرد الفعل المُتوقع، والذي يُشكّل خطورة على البنية السيبرانية الأوربية. **راجع:**

E. J. TALBOT, *Cyber Attacks: Proportionality and Precautions in Attack, 89 International Law Studies, 2013, P. 208.*

(4) ***J. L. GOLDSMITH****, Quick Thoughts on the US Governments, Refusal to Use Cyber-attacks in Libya, (18 October 2011) Brookings Institute,* ***available at:*** *http://www.brookings.edu/blogs/up- front/posts/2011/10/18-cyberattack-libya-goldsmith. 22/11/2019.*

(5) ***Report of Kaspersky Lab Global Research and Analysis Team,*** *Syrian Malware, the Ever - Evolving Threat, August 2014,* ***available at:*** *https://securelist.com/files/2014/08/KL_report_syrian_malware.pdf. 7/2/ 2019.*

(6) ***G. SULMASY****,* ***J. YOO****, Counterintuitive: Intelligence Operations and International Law, 28 MICH. J. INT'L L., 2007, P. 625.*

(٧) **حيث تم اختراق أنظمة الأمن الالكتروني لشركة "*Yahoo*" للتكنولوجيا،** وسُرقت بيانات تخص بعض المستخدمين من الشركات والأفراد، كما وقع أيضًا الهجوم المعروف باسم (*DDoS*) الذي استهدف البنية التحتية لشبكة الانترنت العالمية، وأوقف معظم خدمات الإنترنت الرئيسية في جميع أنحاء العالم. **راجع:**

N. WOOLF, *DDoS attack that disrupted internet was largest of its kind in history, experts say, the Guardian (26 October 2016),* ***available at:***

"جيمس كلابر" مدير الاستخبارات الأمريكية، أن المخابرات الأمريكية على ثقة بأن الحكومة الروسية متورطة في هذا الاختراق، بغرض التأثير على نتائج الانتخابات لصالح "دونالد ترامب"، وأن عملاء روس قاموا باختراق أنظمة المعلومات التابعة للجنة الوطنية الديمقراطية، وحصلوا على كل تقاريرها، ورسائل البريد الالكتروني المُتبادلة بين أعضائها، وتم التلاعب بالمعلومات والبيانات الخاصة باللجنة لصالح المُرشَّح المذكور[١].

وفي مايو من عام ٢٠١٧، أثَّر هجوم "*WannaCry*" أو "الفدية"، على مئات الآلاف من أجهزة الكمبيوتر حول العالم، وكان من تصميم وتنفيذ قراصنة من كوريا الشمالية، وتأثرت به بصفة خاصة مؤسسات الخدمات الصحية الوطنية في بريطانيا، حيث استغل الفيروس ثغرة في بعض أنظمة تشغيل "*Microsoft*"، وسمح للمهاجم بالتحكم بالأجهزة المُخترقة، وتشفير الملفات المُخزَّنة عليها، ثم طلب دفع فدية كشرط لإزالة التشفير، وإعادة الملفات في حالة قابلة للاستخدام[٢].

وفي نفس العام ٢٠١٧، أرجع عدد من المختصين بشأن التسلح، نسبة الفشل العالية وغير المسبوقة في اختبارات صواريخ "باليستية" لكوريا الشمالية، بلغت سبعة اختبارات فاشلة من أصل ثمانية وبنسبة ٨٨%؛ إلى أن الولايات المتحدة الأمريكية كانت تدير عمليات سيبرانية ضد برنامج تطوير هذه الصواريخ، تنفيذًا لإستراتيجية الأمن القومي الأمريكي لعام ٢٠١٧، التي تقضي بفرض عقوبات عاجلة على الدول والجهات الأخرى التي تمارس أنشطة سيبرانية عدائية، مع تكبيدها خسائر فادحة[٣].

والمُرتجى من القانون أن يساير هذا الواقع ويُنظمه، ويؤسس لمسايرة تطوره مستقبلاً، إلا أنه بالنظر إلى أن هذه العمليات السيبرانية، واستخدامها لأغراض عدائية، وآثارها الجسيمة، لم تكن في حسبان واضعي القواعد الدولية السارية، ولم يكن بالإمكان تصورها ـ بشكل كامل ـ وقت صياغة هذه القواعد؛ فقد اقتصر مُعظمها على تنظيم الأفعال المادية الملموسة، أو بعض العمليات السيبرانية البسيطة، كأحكام اتفاقية استخدام البث في دعم السلام لعام ١٩٣٨، والتي مثَّلت أول صك دولي يُنبّه إلى خطورة بعض العمليات السيبرانية، وأوردت التزامات تُقَيِّد "بث" أي آراء قد تُشكّل تهديدًا للسلم والأمن الدوليين، وتحظر نشر أي دعاية تُحرّض على الحرب بأي وسيلة[٤]، وألزمت مادتها الأولي الأطراف بحظر وإيقاف أي بث إذاعي داخل أقاليمها، إذا كان من شأنه تحريض السكان على أفعال تتعارض مع النظام الداخلي، أو أمن أي إقليم آخر، كما

---

https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet. 3/4/2020.

(1) ***V. NARAYANAN**, Harnessing the Cloud: International Law Implications of Cloud-Computing, 12 Chicago Journal of International Law, 2012, P. 783.*

(2) ***D. TRENIN,** Information is a Potent Weapon in the New Cold War, the Guardian (Sept. 17, 2016), **available at:** https://perma.cc/QPT4-4B8T. 15/2/2020.*

(3) ***D. E. SANGER, W. J. BROAD**, White House, National Security Strategy of the United States of America, December 2017, **available at:** www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017 0905.pdf. 22/3/2020.*

(4) ***International Convention concerning the Use of Broadcasting in the Cause of Peace,** Sept. 23, 1936, 186 L.N.T.S. 301.*

حظرت مادتها الثانية، البث الذي يُحرّض على الحرب ضد أي طرف آخر متعاقد، وذلك دون تمييز بين خطاب الدول أو الأفراد.

ثم توالت الاجتهادات الفقهية بشأن التعامل مع العمليات السيبرانية، وجاءت الاستجابة الدولية الأهم والأبرز، مُتمثّلة فيما عُرف بدليل "تالين" للقانون الدولي المُطبَّق على الحرب السيبرانية "*Tallinn Manual on the International Law Applicable to Cyber Warfare*"، بإصداريه رقمي (١)، (٢) لعامي ٢٠١٣، ٢٠١٧ على التوالي، حيث أكَّدت قواعده على أن بعض أحكام القانون الدولي الساري، يمكن تطبيقها في مجال الفضاء السيبراني، أو اعتبارها نقطة انطلاق مناسبة للتعامل مع هذا التطور التقني[١]، بحيث لا يتوقف تنظيم العمليات السيبرانية على إبرام اتفاقيات جديدة، مع اعتبار أن بعض هذه العمليات قد تستوفي معيار أعمال العنف، وترقي إلى درجة استخدام القوة المسلحة، أو تكافئ الهجوم المسلَّح التقليدي، وتدخل ضمن نطاق "الأسلحة الجديدة"، المنصوص عليها في المادة رقم (٣٦) من البروتوكول الإضافي الأول لعام ١٩٧٧، إذا كانت الآثار الناتجة عنها جسيمة كوفاة أشخاص، أو إتلاف، أو تدمير أشياء[٢].

كما أكَّد الدليل على تطبيق مبادئ ومفاهيم القانون الدولي الإنساني على العمليات السيبرانية، كمبدأ التمييز، والضرورة العسكرية والتناسب، وكذلك مفهوم المشاركة المباشرة في الأعمال السيبرانية العدائية، وأجاز حق الدفاع الشرعي ضد التهديدات السيبرانية، وتوَّسع ليستوعب تقرير حق الدول في الدفاع الاستباقي ضد هذه التهديدات، إذا كان هذا الدفاع يُمثّل آخر فرصة للدولة لاتخاذ تدابير دفاعية فعالة، ضدها كتهديدات جدية وشيكة، أو أن هذا الدفاع يُمثّل آخر فرصة ممكنة للرد، وإن لم تغتنمها الدولة فلن تتمكن من درء الخطر.

ووفقًا لدليل "تالين"، يُعَد سلوك التجسس السيبراني، أحد أخطر التهديدات السيبرانية، فيما يتعلَّق بالتأثير على العلاقات الودية بين الدول[٣]، مع اعتباره يرقي إلى مستوى هجوم مُسلَّح

---

(١) **وهو دراسة غير ملزمة للدول، أتمها عشرون أكاديميًا ومتخصصًا في القانون الدولي، ويُشار إليهم باسم فريق الخبراء (*IGE*)**، وتبني الإشراف علي إعداده حلف (*NATO*)، ويبين الدليل مدى ملاءمة القانون الدولي الساري للتطبيق على العمليات السيبرانية، وبدأ إعداده خلال عام ٢٠٠٩، داخل مركز للدفاع السيبراني التابع للناتو في مدينة "تالين" عاصمة "استونيا"، وظهر أول إصدار له عام ٢٠١٣، وأُطلق عليه "تالين١"، وتضمَّن (٩٥) قاعدة توجيهية لسلوك الدول في سياق الحرب السيبرانية، مع تعليقات على كل قاعدة، وفي عام ٢٠١٧ ظهر الإصدار الثاني، وأُطلق عليه "تالين٢"، وتضمَّن (١٥٤) قاعدة، ليُشكّل مستوى أكثر اتساعاً لمعالجة العمليات السيبرانية، مع تعليقات على كل قاعدة، تبين مدى توافق الفريق عليها، والإشكاليات التي أثيرت عند صياغتها. ويرجع تسمية الدليل بهذا الاسم نسبةً إلى "تالين" عاصمة "استونيا"، التي تعرَّضت لسلسلة هجمات سيبرانية من قِبل "روسيا" عام ٢٠٠٧. **راجع:**

E. T. JENSEN, *The Tallinn Manual 2.0: Highlights and Insights, Research Paper, No. 17, Georgetown Journal of International Law, 2017, P. 1;* ***R. BUCHAN,*** *Cyber Espionage and International Law, HART PUBLISHING, Oxford, 2019, PP. 6, 19.*

(2) ***E. SHOSHAN****, Applicability of International Law on Cyber Espionage Intrusions, Faculty of Law, Stockholm University Press, 2014, PP. 31: 32.*

(3) ***C. FORCESE,*** *Spies Without Borders: International Law and Intelligence Collection, 5 J Nat'l Sec L & Pol'y, 2011, PP. 179:181.*

تقليدي، أو استخدامًا للقوة العسكرية؛ في حالة استغلال المعلومات المُتَحصَّل عليها منه، للتسبب في أضرار جسيمة لدولة، كوفاة أشخاص أو إصاباتهم، أو تدمير أعيان.

وبالرجوع إلى تاريخ التجسس بوجه عام، نجد أن المجتمعات المتعاقبة قد تقبلته كسلوك مشروع خلال الحروب، سواء بجمع معلومات سرية عن العدو، أو بنقل معلومات مُضلّلة إليه، طالما لم يتحوَّل الأمر إلى سلوك الغدر[١]، وقديمًا لم تنشب حربٌ، أو يُعقد سلام، بدون معلومات جمعها جواسيس، كما ساد مفهوم ارتباط قوة الدولة بقيمة المعلومات السرَّية التي يُحصّلها جواسيسها، باعتبار أن معرفة ما يدور داخل أو خارج حدود الدولة، لاسيما التهديدات المحتملة، يُبقيها قوية، ويُمكّنها من إحباط أي خطر قبل أن يتحقق[٢]. وقد أشار "*Hugo Grotius*" خلال القرن السابع عشر، إلى أن قانون الأمم ـ بلا شك ـ يسمح بإرسال الجواسيس، ولكن إذا قُبض عليهم، فإنهم يعاملون بمنتهي القسوة ثم يُقتلون، وفي قليل من الأحيان يعاملون بعدالة، من الخصوم الذين يتحلّون بالشرف في القتال[٣].

وقد عالج القانون الدولي التجسس أثناء النزاعات المسلحة، باعتباره سلوكًا مشروعًا، ولم يرد أي التزام دولي على الأطراف المتحاربة باحترام أراضي أو حكومات الدول المعادية، وعلى سبيل المثال، اعتبرت لوائح لاهاي لعامي ١٨٩٩، ١٩٠٧، أن التدابير التي يتخذها أطراف العداء للحصول على معلومات عن العدو وإقليمه أثناء الحرب واقع مقبول[٤]، وأن استخدام الجواسيس يُقبل كخداع مشروع في الحرب ولا يُشكّل مخالفة[٥]، وذلك في جميع مجالات العداء سواء البرية، أم البحرية، أم الجوية. كما تُقبل الاستفادة من خيانة جنود العدو، أو مواطنيه، سواء بواسطة الرشوة، أو طواعية[٦]، وعزّزت تلك الصكوك من اتجاه قبول التجسس، عندما نظَّمت معاملة الجاسوس الذي يتم القبض عليه، ولكن بعد عودته من مهمة التجسس، وانضمامه لجيشه الذي ينتمي إليه؛ باعتباره أسير حرب، ولا يتحمل أي مسئولية عن أفعال التجسس السابقة[٧].

---

(1) ***Program on humanitarian policy and conflict research****, Harvard University, commentary on the hpcrmanual on international law applicable to air and missile warfare, 2010, PP. 244:257.*

(2) ***A. LUBIN,*** *Espionage and the right to privacy, ILSA Quarterly, volume 24, issue 3, 2016, P. 22.*

(3) ***H. GROTIUS,*** *the Rights of War and Peace, Including the Law of Nature and of Nations, New York: Cosimo, Inc., 2007, P. 331.*

(٤) **نصت المادة (٢٤) من لوائح لاهاي، بشأن احترام قوانين وأعراف الحرب البرية لعام ١٩٠٧، على أنه: "** يجوز اللجوء إلى خدع الحرب والوسائل اللازمة لجمع المعلومات عن العدو والميدان". ومن ثم يجوز للدول في حالة الحرب، أن تجمع معلومات من خلال الاستطلاع والمراقبة من الجو والأرض، واعتراض رسائل العدو، والوثائق اللاسلكية وغيرها.

(٥) **المواد من (٢٩): (٣١)** من الاتفاقية الخاصة باحترام قوانين وأعراف الحرب البرية لعام ١٩٠٧.

(6) ***L. OPPENHEIM,*** *International Law: a Treatise: War and neutrality, Green & Co, H Lauterpacht, ed, 1955, P. 422.*

(٧) **المادتين (٣١)، (٣٦) من اتفاقية لاهاي الرابعة بشأن احترام قوانين وأعراف الحرب البرية لعام ١٩٠٧.**

وعلي جانب آخر، لم يتعرَّض القانون الدولي لتنظيم التجسس في وقت السلم صراحةً، ولم تُقرّر المحاكم الدولية اتجاهًا صريحًا بشأنه، من حيث مشروعيته أو حظره، بالرغم من أن محكمة العدل الدولية قد نظرت بعض الدعاوى التي تضمَّنت ممارسات تجسس، مثل قضية "نيكارجوا"، وقضية "رهائن طهران"[١]. وقبل ذلك، أوردت المحكمة الدولية الدائمة للعدل عام ١٩٢٧ في قضية "لوتس"، أنه لا يمكن افتراض حظر سلوك معين، أو فرض قيود على ممارسات الدول، إذا لم يتم النص صراحةً على ذلك بموجب قاعدة دولية[٢]، واستنبط بعض الفقه من ذلك، أن التجسس في زمن السلم ـ بحسب الأصل ـ ليس محظورًا دوليًا، إلا أن ذلك الاتجاه، لم يتم ترسيخه في الأحكام اللاحقة سواء لنفس المحكمة، أم في أحكام محكمة العدل الدولية.

ويدق الأمر بشأن التجسس السيبراني في وقت السلم، سواء عند دراسته، أو التطرق لمحاولة تنظيمه، نظرًا للافتقار إلى قواعد عامة صريحة، يمكن الاستناد إليها في هذا الشأن، وكذلك طبيعته وخصائصه، لاسيما الوسائل التكنولوجية المتطورة التي يتم بواسطتها، والتي لم يُكشف عن تفاصيلها لأغراض هذا التنظيم، وقلة الممارسات الدولية بشأنه[٣]، وصعوبة تحديد ما إذا كانت ممارسته المتزايدة، يمكن أن تمثل قاعدة تسامح، أو ترخيصًا، باعتباره عرفًا دوليًا في طور النشأة[٤]، وبوجه عام، غموض الوضع القانوني للفضاء السيبراني، من حيث مدى خضوعه لسيادة الدول، بحيث يُمثّل التجسس من خلاله تدخلاً في شئونها[٥]، وهو ما جعل جانب من الفقه، يشَبَّه محاولة سبر أغوار التجسس السيبراني أو تنظيمه، بأنه كتثبيت مسمار من الهلام في جدار[٦].

وقد استرعي شيوع وانتشار التجسس السيبراني بين الدول، وتنافسها في تطوير وسائل ممارسته كنمط يعزز قدراتها الدولية؛ نَظَرَ الفقه الدولي منذ أواخر عام ١٩٩٠، فبدأت تظهر بعض الدراسات التي تُنبّه إلى خطورته، وتُقيّم مدى الحاجة إلى استحداث قواعد تواكب تطوره وتُحْكِم تنظيمه[٧]، وسعت بعض الدول والمنظمات الدولية إلى تنظيمه، من خلال بعض المبادئ

---

(1) ***D FLECK,*** *Individual and State Responsibility for Intelligence Gathering, 28 MICH. J. Int'l L., 2007, PP. 687, 691:692.*

(2) ***The Case of the S.S.*** *Lotus' (France v Turkey) (Judgment) [1927] PCIJ Rep Series A No 10, 18.*

(3) ***D. FLECK,*** *Searching for International Rules Applicable to Cyber Warfare, A Critical First Assessment of the New Tallinn Manual, 18 J. CONFLICT & SECURITY L., 2013, P.331.*

(4) ***G. BROWN, K. POELLET****, The Customary International Law of Cyberspace, Strategic Studies Quarterly 6, 2012, P.133.*

(5) ***K. TOWNSEND****, Rise in State-Sponsored Cyber Espionage: the Tipping Point of Cyber Warfare, SECURITY WEEK (Aug. 23, 2016),* ***available at:*** *https://perma.cc/S9A9-B7XU. 5/1/2020.*

(6) ***S. P. WHITE****, Understanding Cyber warfare, P. R., P. 33;* ***M. FINNEMORE, D. B. HOLLIS,*** *Constructing Norms for Global Cybersecurity, 110 AM. J. INT'L L. 425, 2016, PP. 459: 460.*

(7) ***R. A. CLARKE, R. K. KNAKE,*** *the Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats, Penguin, Dhu'l-Q. 13, Political Science, 2019, PP. 162: 163;* ***R. BUCHAN,*** *the International Legal*

التوجيهية والمعايير، والتي يمكنها مواكبة سرعة تطور وسائل ممارسته، وتغيُرها بمرور الوقت[١]، إلا أن غالبية هذه المحاولات بَدَت غير واقعية، ومنها اقتراح حظره، وهو ما عارضته دول عدة، لأهمية هذا السلوك فيما يتعلَّق باعتبارات أمنها القومي[٢]؛ ومنها الاستناد على تحليلات تقنية غير دقيقة، كإدراجه ضمن نطاق الهجمات السيبرانية، أو اعتباره مرادفًا للتسلل السيبراني، أو الجريمة السيبرانية؛ ومنها الإقرار بمشروعيته وعدم جواز اتخاذ أي تدابير مضادة ضد ممارسته[٣].

كما حاولت الجمعية العامة للأمم المتحدة في عام ٢٠١٣، استعراض ومناقشة بعض جوانب التجسس بوسائل تكنولوجية متطورة، ولكنها لم تتخذ قرارًا بتنظيمه، أو وضع إطار له، أو توجيهات خاصة به، واقتصر القرار الصادر منها على مخاطبة الدول لمراجعة عملياتها الاستخباراتية، للتأكد من أنها لا تنتهك حقوق الإنسان لاسيما الحق في الخصوصية[٤]. وبوجه عام، يبقي التنظيم الدولي الساري لسلوك التجسس، هو نقطة الانطلاق للبحث فيما إذا كان يمكن إعمال بعض القواعد السارية بشأنه، والنظر فيما إذا كان سلوكًا مشروعًا، أو يمكن اعتباره بمثابة قاعدة عرفية قيد التطوَّر، أم أنه سلوك ينتهك واجب الحفاظ على السلامة والاستقلال السياسي للدول، ويُمثّل تدخلاً غير مشروعًا في شئون الدول.

وفيما يخص ممارسة التجسس من البحار، سواء بالوسائل العادية أو السيبرانية، فإن له خصوصية من وجهين، **الأول**: وجود نصوص صريحة في اتفاقية الأمم المتحدة لقانون البحار لعام ١٩٨٢، تحظر جمع المعلومات من قبل السفن والغواصات، التي تمر في المساحات البحرية للدول الساحلية وقت السلم، لاسيما المُتعلقة بالمرور البريء في البحار الإقليمية والمضايق، وبما

Regulation of State-Sponsored Cyber Espionage, Legal, Policy & Industry Perspectives, 2016, PP. 65: 87.

(١) **لم يبدأ السعي لتنظيم التجسس السيبراني خلال التسعينيات**، باقتراحات لإبرام صكوك دولية مُلزمة تنظمه، نظرًا لسرعة تطوره، وتغير المفاهيم الخاصة به بمرور الوقت، وبحساب أن التزامات الأطراف في الصكوك الدولية وإجراءات الامتثال لها، يتم النص عليها سلفًا وبشكل مُفصَّل، بما لا يتوافق مع سرعة تطور هذه الوسائل. **راجع:**

***K. E. EICHENSEHR**, the Cyber-Law of Nations, 103 GEO. L. J. 317, 2015, PP. 361:365.*

(2) ***C. FORCESE,** Pragmatism and Principle: Intelligence Agencies and International Law, 102 VA. L. REV. ONLINE, 2016, PP. 6768.*

(٣) **ومن ناحية ثانية، وُجدت حلول واقعية قابلة للتطبيق بشأن تنظيم التجسس السيبراني، ولكن فيما يتعلّق بالمجال الاقتصادي**، منها على سبيل المثال، تفاوض الولايات المتحدة الأمريكية والصين، على معاهدة لتنظيم التجسس الاقتصادي بينهما، والتي انخفضت نسبة ممارسة التجسس السيبراني بين الدولتين أثناء التفاوض عليها، بحوالي ٩٠% من وقائع التجسس التي كان يتم اكتشافها، إلا أن مثل هذا الاتفاق الثنائي خاص بالدولتين، ولا يتعرَّض إلا للتجسس في المجال الاقتصادي. **راجع:**

***J. E. MCGHEE**, Hack, Attack or Whack; the Politics of Imprecision in Cyber Law, 4 J. L. & CYBER WARFARE 13, 2014, P.41.*

(4) ***UN General Assembly,** Group of Governmental Experts, Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc A/68/98 (24 June 2013) Para. 19.*

يُمكن فهمه باعتبار أن الاتفاقية قد حسمت عدم مشروعية سلوك التجسس من البحار في وقت السلم. **والثاني**: يتعلَّق بفهم وتفسير الحريات المكفولة للدول في أعالي البحار، بموجب المادة (٨٧) من نفس الاتفاقية، لاسيما حرية الملاحة والتحليق، وباقي الاستخدامات المرتبطة بتشغيل السفن والطائرات؛ بأنها تشمل وتتضمَّن سلوك جمع المعلومات كأحد عناصر هذا الحق[١].

ويبقي التوجيه الأبرز دوليًا بشأن التعامل مع التجسس السيبراني، هو دليل "تالين" بإصداريه لعامي ٢٠١٣، ٢٠١٧، وبالرغم من كونه توصيات غير ملزمة، إلا أنه أورد أحكامًا مهمة يُمكن البناء عليها بشأن تنظيم العمليات السيبرانية عمومًا والتجسس خصوصًا، لاسيما مدي خضوع بيئة الفضاء السيبراني لسيادة الدول، وأحكام التجسس على معلومات مُخزَّنة، أو منقولة بواسطة البنية التحتية المادية، داخل إقليم دولة مستهدفة أو خارجها، وكذلك مدى اعتبار تلك العمليات، تدخلاً بالإكراه في شئون الدول، يكافئ استخدام القوة المسلحة، وكذلك مدى توافقها مع الوظيفة الدبلوماسية.

وأخيرًا نظَّم دليل "تالين" تقرير أحكام المسئولية الدولية عن العمليات السيبرانية، بالأخذ في الاعتبار، أنه وإن كانت بعض هذه العمليات لا تنتهك القانون الدولي في حد ذاتها، إلا أن الطريقة التي تتم بها قد تُمثِّل فعلا دوليًا غير مشروع، كانتهاك سيادة الدول، وحظر التدخل في شئونها، مع تحمل الدولة المسئولية الدولية عن العمليات السيبرانية التي تُنسب إليها، وتُشكّل خرقًا لالتزام دولي[٢]، وكذلك تقرير المسؤولية الجنائية الفردية، والمسؤولية الجنائية للقادة والرؤساء، عن إصدار أوامر بشن عمليات سيبرانية تُشكّل جرائم حرب.

---

(١) **وذلك بالأخذ في الاعتبار أن السفن والطائرات في منطقة أعالي البحار** تخضع وبشكل حصري لقوانين دولة العلم وفقًا لحكمي المادتين رقمي (٩٢، ٩٤) من اتفاقية الأمم المتحدة لقانون البحار لعام ١٩٨٢.

(٢) **القاعدة رقم (٦) من دليل "تالين ١" لعام ٢٠١٣.**

ثانيًا: إشكاليات البحث:

(١) تثير دراسة بيئة الفضاء السيبراني والعمليات التي تتم بواسطته، إشكاليتين مرتبطتين، تتعلق الأولى بماهية هذه البيئة، وطبيعتها، ومدى خضوعها لسيادة الدول، وخصوصيتها المُميّزة عن البيئة المادية، وبالتالي خصوصية الممارسات والعمليات التي تتم من خلالها، وتتعلَّق الإشكالية الثانية، بضرورة التعرف على مدي إمكان تطبيق قواعد القانون الدولي الساري عليها، أو الحاجة إلى استحداث قواعد جديدة.

(٢) تتطلَّب المفاهيم الخاصة بالعمليات السيبرانية المختلفة، كالحرب السيبرانية، والهجمات السيبرانية، والتجسس السيبراني، والتسلل السيبراني، والإرهاب السيبراني، والجريمة السيبرانية، وبما لكل منها من خصائص مميزة، وعدم الاتفاق على تعريفات محددة لها؛ ضبطًا وتدقيقًا، وتمييزًا لكل منها، لتجنب الخلط بينها، والذي قد يؤدي إلى **صعوبات أكاديمية** بشأن معالجتها أو دراستها، لاسيما عدم وضوح أو تحديد موضوع البحث، **وصعوبات عملية**، تتعلق بكيفية الرد المقبول من جانب الدول على كل منها، **وكذلك صعوبات تشريعية**، من حيث إن معظم الدول تقوم بتنظيم تلك العمليات وطنيًا، باعتبارها نوع واحد فقط، وهو الجريمة السيبرانية ذات الصبغة الجنائية، كالنصب، والسرقة، وتزوير التوقيع الالكتروني، والأفعال الإباحية، ولا تُفرد تلك التشريعات مساحة لباقي العمليات السيبرانية، التي تستهدف تعطيل أو تدمير الأنظمة الالكترونية لمؤسسات الدول، والبني التحتية الالكترونية لها، وقد تكافئ الآثار الناتجة عنها، ما قد ينتج عن هجوم مسلح تقليدي.

(٣) يعتمد تعريف النزاع المسلح الدولي على وقوع أعمال عنف، واستخدام قوة مسلحة بين الأطراف المتنازعة، وآثار جسيمة في الأرواح والممتلكات، وهي عناصر مادية ملموسة على أرض الواقع يمكن تبينها ورصده، وتثور إشكالية مدى إمكان اعتبار العمليات السيبرانية أعمال عنف، أو كونها تكافئ استخدام القوة المسلحة بين الأطراف المتنازعة، حتى يُمكن القول بإمكان تطبيق القانون الدولي الإنساني عليها؟ لاسيما مبادئ الضرورة والتمييز والتناسب، أو تحديد ماهية المشاركة المباشرة في العمليات العدائية بالرغم من كونها هجمات سيبرانية غير مادية؟ وهل يجوز للدول التي تستهدفها هذه الهجمات، أن تستخدم في مواجهتها حق الدفاع الذي تكفله المادة رقم (٥١) من ميثاق الأمم المتحدة؟

(٤) توقَّع واضعو البروتوكول الإضافي الأول لعام ١٩٧٧، في المادة رقم (٣٦)، بعنوان "الأسلحة الجديدة"، حدوث تطورات مستقبلية في وسائل وأساليب الحرب، وأن علي الأطراف التحقق مما إذا كانت هذه التطورات محظورة بمقتضى البروتوكول، أو بموجب قواعد القانون الدولي، فهل تدخل العمليات السيبرانية ضمن فئة الأسلحة الجديدة وفقًا للبرتوكول، بالرغم من عدم النص عليها بشكل مباشر؟

(٥) يُثير تورط كيانات خاصة في شن هجمات سيبرانية تكافئ الهجوم المسلح، بعض الإشكاليات، منها، هل تنطبق قواعد قانون النزاعات المسلحة علي تلك الكيانات، ومدي إمكان إلزامها بالمبادئ الأساسية له، مثل الضرورة، التمييز، التناسب، والإنسانية، بالنظر إلى كونها ليست طرفًا في اتفاقيات القانون الدولي الإنساني. وكذلك صعوبة تحديد الوضع القانوني للقائمين بالهجمات السيبرانية، من الأفراد الذين تستخدمهم تلك الكيانات، أو تصنيفهم كمدنيين أو مقاتلين، وبالتالي

صعوبة تحديد مدى مشروعية استهدافهم بالرد. وأيضًا، طرق مساءلة هذه الكيانات دوليًا، لأنها لا تتمتع بالشخصية القانونية الدولية، وليست طرفًا في اتفاقات القانون الدولي الإنساني.

(٦) نظَّم القانون الدولي التجسس أثناء الحرب، ولم يتم حظر وسائل جمع المعلومات، إلا أن القواعد ذات الصلة لم تُعَرّف أو تُحدّد الأركان المادية لسلوك التجسس، أو وسائله، وأشارت إلي ذلك بعبارات مُجْمَلَة مثل "الوسائل اللازمة لجمع المعلومات عن العدو"، كما عالجت ممارسة التجسس من قبل الأشخاص الطبيعيين "الجواسيس"، ولم تتطرق إلى وسائل أخرى، كالتجسس السيبراني، وبالتالي يتطلب الأمر تحديد ماهية هذا السلوك، وأركانه، وبيان مدى انطباق القواعد السارية على أنواع التجسس الحديثة.

(٧) لم تُنظّم القواعد الدولية السارية التجسس في وقت السلم، أو تبين مدى مشروعيته، مع انتشار هذه الممارسة، ووجود دوافع لدي الدول للاستمرار فيها، ويزداد الأمر غموضًا فيما يتعلَّق بالتجسس الالكتروني وقت السلم، ويتطلَّب الأمر بحث واستجلاء مدى مشروعية هذا السلوك، وهل توجد ضرورة قانونية وعملية لتنظيمه؟ وهل تُعد القواعد السارية نقطة انطلاق مناسبة لذلك؟ أم أن النهج الأكثر ملاءمة هو ترك الأمر للتدابير الثنائية ومتعددة الأطراف بين الدول ذات الصلة، مثل ما أقرته بعض اتفاقات التسلَّح التي سمحت بتحقق الأطراف، كلُ بوسائله التقنية من أنشطة الطرف الآخر[١]؟

(٨) تمارس معظم الدول التجسس من خلال وكالات استخباراتها، أو بواسطة ممثلين، أو كيانات خاصة تابعة لها، وفي كل الحالات، فإن أحد نتائج التجسس التقليدي هو انتهاك قاعدة السيادة والسلامة الإقليمية للدول المُستهدفة، والتدخل في شئونها، لوجود الجواسيس داخل إقليم الدول، إلا أن التكنولوجيا الحديثة تثير إشكالية، تتعلق بكيفية انتهاك التجسس السيبراني لهذه القاعدة، مع عدم وجود أي عملاء مُتسلّلين داخل أقاليم الدول المُستهدفة؟ وكيف يمكن اعتباره تدخلاً في شئون الدول، بالنظر إلى ضرورة توافر شرط الإكراه، في الأفعال المُكونة للتدخل غير المشروع؟

(٩) هل يستوفي التجسس الالكتروني متطلبات الممارسة الدولية المقبولة، ويمكن اعتباره قاعدة عرفية في طور التبلور أو النشأة؟ باعتبار أن الدول تمارسه منذ منتصف الخمسينيات، وبواسطة مؤسسات وطنية علنية، كما اعتمد مجلس أمن الأمم المتحدة، في اتخاذ قرارات بالإذن في استخدام القوة، أو فرض جزاءات دولية سواء على الدول أم الأفراد؛ على معلومات مُتحَصَّل عليها من عمليات تجسس الكتروني، ولم يُقابل هذا الأمر بالرفض أو الاستهجان، كما أن ردود الفعل الدولية علي هذا السلوك، تتباين ولا تنحصر في رفضه، أو معارضته، وكثيرًا ما يتم تبريره على أهميته في حفظ السلم والأمن الدوليين، ومكافحة الإرهاب.

(١٠) تثير الطبيعة السريَّة للتجسس السيبراني إشكالية، تتعلَّق بصعوبة تأصيل اتجاه قانوني بشأنها، فالقضايا التي عُرضت على محاكم دولية، وتضمنت في شق منها ممارسة التجسس، لم يتم التركيز على هذا ممارسة السلوك، أو إقرار اتجاه بشأنه، ويتطلَّب الأمر التوسّع في دراسة معظم الممارسات الخاصة بهذا السلوك، وردود الفعل عليها منذ بدايته في فترة الستينيات وحتى الآن، وتَتَبُع

---

(١) **الاتفاقية الثنائية المبرمة عام ١٩٧٢ بين الولايات المتحدة الأمريكية، وروسيا**، بشأن الصواريخ المضادة للقذائف الباليستية؛ واتفاق "سالت ١" (*SALT 1*)، واللذان أوردا صياغة "الوسائل التقنية الوطنية للتحقق" من نشاط الطرف الآخر.

الإحصائيات والتقارير المُتاحة في وسائل الإعلام الرقمية، ومواقع الانترنت الرسمية، لاستجلاء أركانه، ومدي قبوله دوليًا، وكذا الأطر أو التوجيهات أو نوعية القواعد التي تناسب تنظيمه.

(١١) رُصدت منذ منتصف العشرينيات حوادث تجسس، تتم بانتظام من داخل المياه الإقليمية للدول، وبمرور الزمن تطور هذا السلوك إلى الشكل السيبراني، لاسيما من قبل السفن الحربية، مما يثير إشكاليات تتعلق بالمعايير القانونية التي يُمكن أن تُطبق حال انتهاك سيادة الدول الساحلية بالتجسس السيبراني، ورد الفعل أو التدابير المضادة المقبولة، وما إذا كانت قواعد قانون البحار لعام ١٩٨١ قد تعرَّضت لتنظيم مثل هذه الأفعال، أو بيّنت التدابير التي يمكن اتخاذها في هذه الحالات وسلطة الدول الساحلية في إنفاذ هذه التدابير.

(١٢) تُضلّل التكنولوجيا الحديثة المفاهيم التقليدية لمسئولية الدولة، مثل صعوبة أو استحالة "إسناد" العمليات السيبرانية لمصدر معين، حيث إنها تتم في سرية وبسرعة فائقة، ويتم توجيهها عبر أجهزة كمبيوتر كثيرة، ومن دول مختلفة، ولا يتيسر التحقق من مصدر الهجوم أو هوية المهاجم، ويتطلَّب الأمر مزيدًا من الدراسة، لاستجلاء كيف يمكن التعامل مع العقبات التقنية والقانونية بشأن الإسناد، سواء فيما يتعلَّق بالدول، أو الفئات الأخرى التي تضطلع بتلك العمليات، من الأفراد أو الكيانات الخاصة، لاسيما في حالة وجود صلة بين الدول وهذه الفئات، وذلك على ضوء مشروع لجنة القانون الدولي بشأن مسئولية الدول لعام ٢٠٠١، وكذلك دليل تالين بإصداريه لعامي ٢٠١٣، ٢٠١٧.

ثالثًا: تحديد نطاق البحث ومصطلح الدراسة:

(١) تُركّز الدراسة على العمليات السيبرانية، التي تتم عبر الفضاء السيبراني "*Cyber Space*"، وليس الفضاء الخارجي "*Outer Space*"، وذلك من وجهة نظر قانونية دون مناقشة التفاصيل الفنية.

(٢) لا تسعى الدراسة للتفرقة بين أنواع التجسس السيبراني المختلفة، كالسياسي، أو الاقتصادي، أو العسكري، أو غيرها، لأن السلوك واحد في كل هذه الحالات، وهو الاختراق الالكتروني وممارسة التجسس، ومن ثم، تسعي الدراسة لعرض رؤية مستدامة بشأن سلوك التجسس السيبراني، دون التطرق للدافع، والذي يُعد التعرف عليه صعبًا، إن لم يكن مستحيلاً في مجال العمليات السيبرانية[(١)].

(٣) بالنسبة لتحديد مصطلح الدراسة؛ فإن العمليات التي تتم في "الفضاء السيبراني" كالهجمات أو التجسس تُوصف ـ بحسب الأصل ـ بأنها "سيبرانية"، نسبة إلى الوسط التي تتم من خلاله "*Cyber Space*"، إلا أن بعض وثائق الأمم المتحدة التي تصدر باللغة العربية، تستخدم لفظي "السيبرانية" و"الالكترونية" بالتبادل وباعتبارهما مترادفين، ولا يختص أحدهما بما يُميّزه عن الآخر، ومن ذلك، تقرير

(١) **وعلى سبيل المثال**، عندما تخترق دولة النظم الالكترونية، للبنوك الوطنية لدولة أخري، وتحصل على معلومات تمكّنها من تقويض اقتصاد الدولة المستهدفة، في حالة نشوب نزاع بين الدولتين، فإن سلوك التجسس لا يختلف، عما إذا كان الهدف من الحصول على المعلومات، هو تقويض ثقة العملاء فيه ودفع الاستثمارات إلي بنك أخر، ففي الحالتين نكون بصدد سلوك تجسس سيبراني. **راجع:**

***M. XINMIN**, Key Issues and Future Development of International Cyberspace Law, 2 China Quarterly of International Strategic Studies, 2016, PP. 119: 128.*

خبراء الأمم المتحدة المعني بإجراء دراسة شاملة عن الجريمة السيبرانية وتدابير التصدي لها[١]، ولكن الرؤية الأقرب للدراسة، أن الفضاء السيبراني يتكون من جزء مادي، وجزء افتراضي، فما يتعلَّق بالتصرفات التي ترتبط بالجزء المادي، أو ما يُطلق عليه "البنية التحتية الالكترونية"، كأجهزة الحاسبات وشبكة الانترنت، وأنظمة التشغيل، والبرمجيات، فيُمكن أن نُطلق علي "الكتروني"، وما يتعلَّق بالعمليات التي هي عبارة عن أوامر يتم نقلها وتوجيهها، من خلال الجزء الافتراضي غير المادي، لتؤثّر على أنظمة تقنية لدولة، فإن الدراسة ستعتمد لها وصف "السيبراني"[٢].

رابعًا: مبررات البحث:

(١) بعد أن اعتمدت معظم المجتمعات وبشكل متنامي، على النمط السيبراني في كافة تعاملاتها المدنية أو العسكرية وغيرها، صارت الانتهاكات السيبرانية أحد عوامل تهديد أمن وسلامة الدول، ومن ذلك، إمكان استخدام المعلومات التي يتم الحصول عليها من التجسس، لإلحاق أضرار جسيمة بالدول، قد تناظر ما قد ينتج عن استخدام القوة المسلحة التقليدية، حتى أن الدول قد عمدت إلى تخصيص مرافق خاصة، لرصد الجرائم السيبرانية، والتعامل معها باعتبارها من التهديدات الأساسية للأمن القومي.

وعلى سبيل المثال، صرَّح "*Anders Rasmussen*" الأمين العام لمنظمة "*NATO*"، أن مقر المنظمة يتعرض يوميًا لأكثر من (١٠٠٠) محاولة تجسس سيبرانية، وأن هذه الهجمات تنطلق من أكثر من (١٠٠) دولة[٣]، مما يشير إلى تطور هذه الظاهرة وانتشارها، كما قُدّرت تكلفة هذه الاقتحامات الالكترونية، على الاقتصاد العالمي بحوالي ٢.١ تريليون دولار خلال عام ٢٠١٩[٤]، ومن ثم، تتعاظم الحاجة إلى دراستها، واستجلاء جوانبها، لاقتراح ما يلائمها من معايير، أو قواعد قد تحكمها أو تُفيد في التعامل مع خطورتها.

(٢) لا يكفي للتعامل قانونًا مع العمليات السيبرانية، لاسيما التجسس السيبراني وقت السلم، الاعتماد على ما ورد في الاتفاقيات الدولية السارية، كاتفاقيات "جنيف" لعام ١٩٤٩، أو بعض نصوص اتفاقية "فيينا" للعلاقات الدبلوماسية لعام ١٩٦١، المتعلقة بمخالفة الدبلوماسي لمهام وظيفته، والتورط في التجسس، أو غيرها من القواعد السارية، التي ربما لا تأخذ في الاعتبار طبيعة العمليات السيبرانية، وخصوصيتها، ويتطلب الأمر دراسة هذه العمليات للبحث عما يناسب طبيعتها وخصوصيتها من قواعد.

---

(١) **مكتب الأمم المتحدة المعني بالمخدرات والجريمة:** تقرير الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، والتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لها،" فيينا"، ٢٠١٣، وثيقة: (*UNODC/CCPCJ/EG.4/2013/2*). كما تجدر الإشارة إلى أن الموقع الالكتروني للأمم المتحدة، يعتمد مصطلح الفضاء الالكتروني بالتبادل مع الفضاء السيبراني.

(٢) **وعلى سبيل المثال**، يمكن التعبير عن شن هجوم سيبراني لدولة على مؤسسة عسكرية لدولة أخري، بأن هجومًا "**سيبرانيًا**" تم إطلاقه لاستهداف الأنظمة "**الالكترونية**" لمؤسسة عسكرية للدولة.

(3) ***S. GORMAN, S. FIDLER****, Cyber Attacks Test Pentagon, Allies and Foes, 2010,* ***available at:*** *http://www.wsj.com/articles/SB10001424052748703793804575511961264943300. 16/5/2019.*

(4) ***Press Release, Juniper Research****, Cybercrime Will Cost Businesses Over $2 Trillion by 2019 (May 12, 2015),* ***available at:*** *https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over- 2trillion. 24/3/2019.*

(٣) فيما يتعلَّق بسلوك التجسس وقت السلم، فإنه لم يتم تنظيمه صراحةً بموجب القواعد السارية، ويتطلب الأمر إلقاء الضوء على مثل هذا السلوك، والبحث في مدى مشروعيته، ومحاولة استنباط أو تأصيل أو اقتراح ما يناسبه من قواعد أو معايير أو توجيهات أو أطر.

(٤) على المستوى الوطني، ربما تكون مثل هذه الدراسات التي تتناول الهجمات السيبرانية، والتجسس السيبراني، مفيدة بشأن توضيح عناصر وأركان هذه العمليات، وبيان الوضع القانوني الدولي لها، مما يضع أمام مشرعي الدول معايير محددة، يمكن من خلالها تناول هذه الأفعال بالتنظيم وطنيًا، مما يسهم في مواجهة هذا النوع من التحديات الأمنية الحديثة.

خامسًا: منهج البحث:

ستعتمد الدراسة على عدة مناهج؛ التحليلي، والتأصيلي، والتاريخي، والمقارن، حيث عمد البحث إلى تحليل أحكام القانون الدولي الساري، والقانون الدولي الإنساني، واتفاقية قانون البحار لعام ١٩٨١، واتفاقية "فيينا" للعلاقات الدبلوماسية لعام ١٩٦١، والاتفاقية الدولية للاتصالات لعام ١٩٧٣، واتفاقية الأمم المتحدة بشأن حصانات الدول وممتلكاتها من الولاية القضائية لعام ٢٠٠٤، وغيرها من الصكوك الدولية ذات الصلة بسلوك التجسس أو النزاعات المسلحة، بغرض فهم وتدقيق الأحكام العامة لها، وتحليل ما إذا كانت تصلح لتنظيم نفس السلوك وقت السلم، أو في حالة تطوره وممارسته من خلال وسائل الكترونية، كما تم تناول العديد من الأحكام القضائية والتحكيمية الدولية بالتحليل، لاسيما ما صدر عن محكمة العدل الدولية، ومحكمة التحكيم الدائمة، وكذا تم تناول آراء الفقه بالتحليل، من أجل استخلاص معالجة لإشكاليات البحث.

وستكون أيضًا دراسة تأصيلية حيث تُوخِي فيها أن يتم تأصيل ووضع ما تم التوصل إليه من حلول وبدائل في إطار قابل للتطبيق على أرض الواقع، لاسيما فيما يتعلق بالوضع القانوني للتجسس وقت السلم عمومًا والسيبراني خصوصًا، ومدى اعتباره بمثابة تدخل في شئون الدول، أو مدى إمكان اعتباره بمثابة عرف دولي، وتقديم اقتراحات لمعايير شكلية وموضوعية، لنصوص يمكنها تنظيم التجسس السيبراني في وقت السلم.

يضاف إلى ذلك أن الدراسة ستتبع المنهج التاريخي، من حيث رصد العديد من الحالات ووقائع التجسس الدولية منذ منتصف العشرينيات، لاسيما التي مثَّلت بؤرة اهتمام للمجتمع الدولي، ولاقت ردود أفعال من الدول ذات الصلة عليها، ثم متابعة تطور مثل هذه الحالات والممارسات على مر الزمن، إلى أن وصلت للشكل السيبراني، بغرض معرفة كيفية تطور هذا السلوك مستقبلاً، والعوامل المؤثرة في ذلك، وتحديد أي القواعد يمكن أن تلائم تنظيمه، وتحد من خطورته.

وبشأن كون الدراسة مقارنة، حيث تعرضت لتشريعات بعض الدول التي تعاملت مع تنظيم التجسس السيبراني أو أي أفعال أو إجراءات ذات صلة، ثم المقارنة بينها، بغية التعرف على أفضل ما ورد بهذه التشريعات وطرق تنفيذها، في محاولة للاستفادة من كل ذلك في الإجابة على إشكاليات البحث.

سادسًا: خطة البحث:

الفصل الأول: القانون الدولي والعمليات التي تتم من خلال الفضاء السيبراني.
الفصل الثاني: التنظيم القانوني الدولي الساري بشأن التجسس.
الفصل الثالث: الوضع القانوني للتجسس السيبراني ومسئولية الدول عن العمليات السيبرانية.

الفصل الأول

القانون الدولي والعمليات التي تتم من خلال الفضاء السيبراني

تمهيد وتقسيم:

دخل مصطلح "الفضاء السيبراني" "*Cyberspace*" إلى الثقافة العامة من خلال قصص الخيال العلمي وبعض الفنون، فكان أول من استخدمه كاتب الخيال العلمي "*William Gibson*"، وذلك في قصة نشرها عام ١٩٨٢، ووصفه بأنه: مُجمَّع للبيانات والمعلومات التي يتداولها، مليارات من مستخدمي الشبكات الالكترونية في جميع أنحاء العالم يوميًا، باستخدام أجهزة كمبيوتر متصلة بالانترنت[١].

ويُرد أصل مُصطلح "*Cyber*" إلى كلمة "سيبرنتيك" "*Cybernetic*"، المأخوذة من اللغة اللاتينية القديمة، وتعني "التَوْجِيه" أو "التَحَكُّم" أو "الرائد" أو "الدَفَّة"، وقد شاع استخدام ذلك المصطلح في التسعينيات، من قبل كثير من المختصين في التقنيات الالكترونية، وخبراء الأمن، والقادة الحكوميين، والعسكريين، وغيرهم من المهتمين بالتكنولوجيا، باعتبار أنه يعني البيئة أو الوسط أو المجال، الذي تتم فيه تبادلات ومعاملات افتراضية الكترونية بين كل المجتمعات[٢].

وبمرور الزمن شاع استخدام بيئة الفضاء السيبراني في كافة المعاملات، والتي لم تخل من ممارسة بعض الأفعال غير المشروعة والجرائم، إلا أنها ذات طبيعة مختلفة ومتميزة عن الأفعال أو الانتهاكات التقليدية التي تتم في بيئة مادية ملموسة، ونوالي بيان ماهية الفضاء السيبراني، والممارسات التي قد تتم من خلاله وتشكّل جرائم، ومدى استيعاب قواعد القانون الدولي لتنظيم هذه الممارسات، وذلك من خلال المباحث التالية:

المبحث الأول: ماهية الفضاء السيبراني وأبرز العمليات التي تتم من خلاله.

المبحث الثاني: مدي انطباق القانون الدولي الساري على العمليات السيبرانية.

المبحث الثالث: بعض جهود التعاون الدولي بشأن تنظيم العمليات السيبرانية.

المبحث الأول

ماهية الفضاء السيبراني وأبرز العمليات التي تتم من خلاله

عُرَّف الفضاء السيبراني باعتباره، مجال أو بيئة افتراضية، أي غير مادية، تتكون من تفاعل عناصر مادية وأخري غير مادية، وتتيح التواصل بين كل أجزاء العالم من خلال شبكات الكترونية مترابطة، كما تتيح تداول قدر غير محدود من المعلومات المختلفة، أو تخزينها، ويتمثل الجزء المادي في

---

(1) ***E. SHOSHAN,*** *Applicability of International Law on Cyber Espionage Intrusions, P. R., PP. 11:12.*

(2) ***M. XINMIN****, Letter to the Editors: What Kind of Internet Order Do We Need? 14 Chinese Journal of International Law, 2015, PP. 399: 402;* ***R. KISSEL****, Glossary of Key Information Security Terms, National Institute of Standards and technology, U.S Department of Commerce , Revision, 2, May, 2013, P.57.*

البنية التحتية الالكترونية، مثل الحاسبات الآلية، وشبكة الانترنت، ويتمثل العنصر غير المادي، في الوسط الافتراضي الذي يتم تداول المعلومات من خلاله[1].

وكذلك هو مجال له طبيعة خاصة، فهو مُستقّل عن أي مكان أو زمان، بحيث لا يتطلب أن تكون الأطراف المتفاعلة من خلاله، متواجدة في موقع محدد، أو لحظة محددة لكي يتم التواصل بينهم، وتخضع المكونات المادية للفضاء السيبراني لسيادة الدول التي تقع على أقاليمها، بخلاف الفضاء الخارجي، الذي لا يخضع لسيادة أي دولة، ويمكن من خلال الفضاء السيبراني إجراء عمليات متعددة، كالتسلل السيبراني، والهجمات السيبرانية، والتجسس السيبراني، وغيرها، من العمليات التي تعتمد على طبيعته وخصائصه المميزة.

ولدراسة تعريف الفضاء السيبراني وطبيعته، والتمييز بينه وبين الفضاء الخارجي، فإننا نقسم هذا المبحث إلى المطلبين التاليين:

المطلب الأول: تعريف الفضاء السيبراني، والتمييز بينه وبين الفضاء الخارجي.

المطلب الثاني: أنواع العمليات السيبرانية.

المطلب الأول

تعريف الفضاء السيبراني والتمييز بينه وبين الفضاء الخارجي

اعتمدت المجتمعات الحديثة بشكل متنامٍ على تكنولوجيات الاتصالات والمعلومات، لاسيما الشبكة العالمية (*W.W.W*)، بحيث يتم التواصل بينها من خلال أجهزة وأنظمة الكترونية متطورة، تُنشئ ما يُطلق عليه البيئة الافتراضية، التي تتم فيها هذه الاتصالات، أو الفضاء السيبراني "*Cyberspace*"، وتُوّضح الإحصائيات تزايد عدد المستخدمين لهذا الفضاء، حيث لم يتجاوز (٥١٣) مليون مستخدم، في عام ٢٠٠١، وبنسبة تُقدَّر بـ (٨%) من سكان العالم وقتها، بينما قُدّر عددهم في عام ٢٠١٦، بحوالي (٢.٧) مليار مستخدم، وبنسبة تقترب من (٣٩%) من سكان العالم، وبحلول نهاية عام ٢٠١٧، بلغ عد المستخدمين حوالي ٥٤% من سكان العالم، بزيادة ١٠٥٢% منذ عام ٢٠٠٠[2]. **ونوالي تعريف الفضاء السيبراني، والتمييز بينه وبين الفضاء الخارجي من خلال الفروع التالية.**

الفرع الأول

تعريف الفضاء السيبراني وطبيعته

أولاً: تعريف الفضاء السيبراني:

---

(1) ***Oxford English Dictionary Online,*** *Cyberspace Oxford University Press November 2010,* ***available at:***

http://www.oed.com.ezp.sub.su.se/view/Entry/240849?redirectedFrom=cyberspace&accessed

. 14/3/2018.

(2) ***Internet World Stats:*** *Usage and Population Statistics, 21 June 2018,* ***available at:*** *www.internetworldstats.com/stats.htm. 14/3/2018.*

عرَّفت الوكالة الفرنسية لأمن أنظمة الإعلام (*ANSSI*) الفضاء السيبراني، بأنه مجال غير مادي للتواصل من خلال شبكات الكترونية مترابطة، يتشَكّل نتيجة تفاعل عناصر مادية وأخري غير مادية، الأولي عبارة عن مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشغلين أو مستعملين، والثانية حاصل ما يتم نقله وتداوله أو التصرف فيه من معلومات[١].

وتم تعريفه في قاموس وزارة الدفاع الأمريكية للمصطلحات العسكرية السيبرانية بأنه: مجال افتراضي عالمي، يتم تداول المعلومات المختلفة والمتنوعة من خلاله، ويتَشكَّل من بني تحتية تكنولوجية، تتمثل في الحاسبات الآلية، ونظم الإنترنت والاتصالات، والأفراد القائمين على تشغيلها والتحكم فيها[٢].

كما وُصِف بأنه وسط الكتروني، يتواصل من خلاله المستخدمون في كل دول العالم، ويطلعون على المعلومات، ويتبادلون ما هو متاح للتبادل منها، وذلك باستخدام تقنيات حديثة، تمثل الجزء المادي الملموس في تشكيل هذا الفضاء، مثل الحواسيب الآلية، وأنظمة شبكة الانترنت، والبرمجيات المتخصصة، ومواضع نقل وتخزين البيانات، ويُطلق عليها البنية التحتية السيبرانية[٣].

وعُرف بأنه بيئة تتشَكَّل من ناتج تفاعل تكنولوجيا تخزين ومعالجة وإتاحة معلومات مختلفة، والأشخاص الذين ينفذون هذه المهام، والأجهزة التي يتم من خلالها كل ذلك كالحاسبات الآلية والشبكات الالكترونية، وهو مجال غير مادي بطبيعته، بالرغم من أن العناصر التي تُنشئه وتُشَغِلُه مادية[٤].

وكذلك هو مُجمَّع للمعلومات التي يطلّع عليها ويتداولها مستخدمون من كل أنحاء العالم، بواسطة أجهزة حاسبات آلية، تتصل مع بعضها بواسطة شبكة الانترنت، ويتم الاعتماد عليه في تعاملات الحياة المختلفة لاسيما التجارية منها، نظرًا لطبيعته التي تُيسّر التواصل، وتنقل البيانات لمسافات هائلة في ثوان معدودة[٥].

وهو بيئة أو مجال غير مادي عالمي، يمكن من خلاله تخزين وتبادل كم هائل من البيانات والمعلومات، ويَتَشَكَّل هذا المجال من شبكة مترابطة من البني التحتية لتكنولوجيا المعلومات، وبما يشمل الإنترنت، وشبكات الاتصالات، وأنظمة الكمبيوتر، ووحدات التحكم[٦].

وعرَّفه دليل "تالين ٢" لعام ٢٠١٧، بأنه بيئة الكترونية تَتَشَكّل نتيجة التفاعل بين طبقات مادية، ومنطقية، واجتماعية، تتمثّل الطبقة المادية في عناصر شبكة الاتصالات، أي الأجهزة والبنية التحتية الأخرى، كالكابلات وأجهزة التوجيه، وأجهزة الكمبيوتر، وتتمثَّل الطبقة المنطقية في الاتصالات التي تتم

---

(1) ***T. PLOUG,*** *Ethics in Cyberspace: How Cyberspace May Influence Interpersonal Interaction, 1st. edn., Springer, 2009, P. 70.*
(2) ***US Department of Defense Dictionary of Military Terms,*** *Computer Intrusion,* ***available at:*** *http://www.dtic.mil/doctrine/dod_dictionary/data/c/11171.html. 14/3/2018.*
(3) ***S. J. SHACKELFORD****, Managing Cyber Attacks in International Law, Business and Relations: In Search of Cyber Peace, 1st. edn., Cambridge University Press, UK 2014, P. 53.*
(4) ***C. INGLIS,*** *Illuminating a New Domain: the Role and Nature of Military Intelligence, Surveillance, and Reconnaissance in Cyberspace,* ***in: H. LIN, A. ZEGART,*** *Bytes, Bombs, and Spies, P. R., P. 20.*
(5) ***H. PH. FAGA****, the Implications of Transnational Cyber Threats in International Humanitarian Law, P. R., PP. 3: 5;* ***S. AVIN, D. SEAMAN****, the Space Warfare, Concepts and Trends, Berlin, 2011, P. 75.*
(6) ***R. BUCHAN,*** *Cyber Espionage and International Law, P. R., P. 15.*

بين أجهزة الشبكة، وبما يشمل التطبيقات، والبيانات، والبروتوكولات التي تسمح بتبادل البيانات عبر الطبقة المادية، وتشمل الطبقة الاجتماعية الأفراد والمجموعات المنخرطة في الأنشطة السيبرانية[١].

ومن التعريفات السالفة، يمكننا تعريف الفضاء السيبراني باعتباره، مجال إلكتروني غير مادي، يتم من خلاله التواصل بين كل أنحاء العالم، وكذلك تخزين ونقل وتداول كم غير محدود من المعلومات، التجارية أو الاقتصادية، أو الاجتماعية، أو الثقافية، أو العسكرية، أو الدبلوماسية، أو الاستخباراتية، أو الشخصية، أو غيرها مما يخص الدول، والمؤسسات والكيانات الخاصة، والأفراد، ويعتمد وجود هذا المجال على عناصر مادية وبشرية، وتتمثل العناصر المادية في أجهزة الحاسب الآلي، التي تتصل ببعضها عن طريق شبكة الانترنت وما يرتبط بها من تقنيات وبرامج، ويضطلع العنصر البشري بتشغيل وتفعيل هذه العناصر المادية.

ثانيًا: طبيعة الفضاء السيبراني:

كون الفضاء السيبراني ـ في جزء منه ـ بيئة افتراضية، يعني أنه مُستقّل عن أي مكان أو زمان، وبما عبَّر عنه جانب فقهي باصطلاح "الاستقلال الزماني المكاني" " *Specific Spatiotemporal Location*"، بحيث لا يتطلب أن تكون الأطراف المتفاعلة من خلاله، متواجدة في موقع محدد، أو لحظة محددة لكي يتم التواصل بينهم. وبعبارة أخري، فإنه يفتقر إلى المادية والواقع الظاهري، ولا يعرف الحدود الوطنية، ولا يخضع للجغرافيا، أو الحدود، أو الحيازة أو الملكية، وتتساوى في إمكانية الوصول إليه واستغلاله، الحكومات، والكيانات الخاصة، والشركات، والأفراد، بدون أي تفرقة من أي نوع[٢].

وفيما يتعلَّق بالجزء المادي الذي يُشكّل هذا الفضاء، فإنه يخضع لمبدأ السيادة الإقليمية للدول، ولذا رفض فريق الخبراء (*IGE*) الذي صاغ دليل "تالين"، وصفه بأنه مشاع عالمي مُشترك، لأن ذلك الوصف يتجاهل كونه يتشكّل في جزء منه من مكونات مادية، توجد داخل أقاليم دول، وتخضع لسيادتها، وكذلك الأفراد المنوط بهم تشغيل هذه المكونات، يخضعون لسيادة الدول التي يتواجدون على إقليمها، وحتى الأنشطة السيبرانية التي قد تعبر حدودًا، أو تقع في المياه الدولية، أو المجال الجوي الدولي، أو الفضاء الخارجي، جميعها يتم نتيجة تشغيل الأفراد أو الكيانات الخاضعين لولاية دولة أو أكثر، للأجزاء المادية للفضاء السيبراني[٣].

والفضاء السيبراني موجود ومُفَعَّل في كل مكان تصل إليه شبكة الانترنت، وهو مُصمَّم بحيث يستحيل على أي جهة أو كيان التحكم فيه، بل إنه لا يُمكن لأي دولة مهما بلغت قدراتها التكنولوجية أن تُحصي حتى حركة تداول المعلومات خلاله، أو تنسب أي إجراء تم بواسطته إلي نفسها أو إلى أي دولة أخري، أو فرد أو مؤسسة، حيث إن معظم الاتصالات التي تتم خلاله تستخدم وسائل تمويه وتشفير ولا يُمكن لأي نظام مراقبة التعرف بدقة على مصدرها[٤].

---

(1) ***M. N. SCHMITT, L. VIHUL****, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, P. R., P. 12.*
(2) ***D. AUCSMITH,*** *Disintermediation, Counterinsurgency, and Cyber Defense, in: H. LIN, A. ZEGART, Bytes, Bombs, and Spies, P. R., PP. 344: 346*
(3) ***M. N. SCHMITT, L. VIHUL,*** *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, P. R., P. 12.*
(4) ***O. A. HATHWAY, R. CROOTOF, P. LEVTIZ, A. NIX, A. NOWLAN ,W. PERDUE, J. SPIEGEL****, The Law of Cyber –Attack, California Law Review, 2012 , P. 7;*

وفيما يخص استخدامه لأغراض عدائية، فقد وُصف بأنه مجال خامس للعمليات العسكرية المرتقبة، إلى جانب البر والبحر والجو والفضاء، مع سهولة وفاعلية استخدامه[١]، وعلي سبيل المثال، يحتاج إيقاع القوة من الجو إلي طائرات مقاتلة، وصواريخ، ورادارات، في حين أن إيقاع القوة من الفضاء السيبراني، إلى أي مجال آخر كالبري، أو البحري، أو الجوي، أو الفضائي، يتطلَّب فقط الولوج إلى شبكة الانترنت، واستخدام بعض البرمجيات الضارة، وهي كافية للتسبُب في آثار جسيمة، تكافئ ما قد ينتج عن استخدام القوة التقليدية[٢].

كما تتوافر ميزات لمن يبدأ بالهجوم من السيبراني، حيث يختار هدفه بحرية، وكذلك توقيت وطريقة الهجوم، ثم يُحقّق الضرر وينسحب، أما المُدافع، فعليه أن يكون جاهزًا في أي وقت ولأي تهديد، علاوة على التكلفة المنخفضة نسبيًا للهجوم مقارنةً بالدفاع، حيث لا يحتاج المهاجم، سوى لأجهزة حاسب آلي، مُتصلة بشبكة الانترنت، ليتمكَّن من تهديد قدرات أي دولة، أو تقويض أنظمتها الالكترونية، أو تدمير أو محو معلومات سريَّة تملكها، بينما تكون تكلفة التعامل مع ذلك الهجوم، أو إصلاح الأضرار الناتجة عنه عالية جدًا[٣].

الفرع الثاني

التمييز بين الفضاء السيبراني والفضاء الخارجي

بالنظر إلى كون الفضاء السيبراني "*Cyber Space*"، حيزًا افتراضيًا وبيئة الكترونية، تتشَكَّل نتيجة تشغيل العنصر البشري لأجهزة الحاسب الآلي، المُتصلة بشبكة الانترنت ووسائط الربط بينهما؛ فليس لهذا الحيز موقع معين أو مكان محدد يوجد فيه، فهو يستقل عن أي مكان أو زمان محدد، كما يخضع في جزء منه وهو مكوناته المادية، لمبدأ السيادة الإقليمية للدول، **وذلك بخلاف "الفضاء الخارجي" "*Outer Space*"**، والذي يمكن تعريفه، بأنه حيّز لا يخضع لسيادة أي دولة، ولا توجد قاعدة قانونية يمكن أن تقرر امتداد سيادة الدول على هذا الفضاء، الذي يشبه إلى حد كبير وضع البحار العالمية، وقد نصت المادة رقم (٢)، من اتفاقية ١٩٦٧ بشأن المبادئ التي تحكم أنشطة الدول في مجال استكشاف واستخدام الفضاء الخارجي، بما في ذلك القمر والأجرام السماوية، على أنه: "لا يكون الفضاء الخارجي بما في ذلك القمر والأجرام السماوية الأخرى، محلاً للتملك الوطني بادعاء السيادة أو على أساس الاستخدام، أو وضع اليد، أو بأي وسائل أخرى[٤].

وعلى الصعيد الدولي، فقد تم تناول المجال الجوي للدول، وكذلك الفضاء الخارجي، بالتنظيم منذ نهاية الحرب العالمية الأولي[٥]، بينما لم يتم تنظيم الفضاء السيبراني إلا حديثًا، وبشكل جزئي، لمواجهة

---

(1) ***W. J. LYNN III****, Defending a New Domain: The Pentagon's Cyberstrategy, Foreign Affairs, Issue 89, No. 5, September/October, 2010, PP. 97:108.*

(2) ***B. F. HARRIS****, America, Technology and Strategic Culture: A Clausewitzian Assessment, New York, Routledge, 2009, PP. 7: 12.*

(3) ***W. J. LYNN III****, Defending a New Domain, P. R., PP. 89:90.*

(٤) **المادة (٢) من معاهدة المبادئ المنظمة لأنشطة الدول في مجال استكشاف واستخدام الفضاء الخارجي**، بما في ذلك القمر والأجرام السماوية الأخرى ١٩٦٧، (*18 U.S.T. 2410, 610 U.N.T.S. 205*).

(٥) **لا يوجد اتفاق دولي بشأن تحديد المسافة بين المجال الجوي والفضاء الخارجي**، وقد ظهرت اتجاهات أربعة في هذا الشأن، **أولاً:** نظرية امتداد سيادة الدولة إلى مالا نهاية، **ثانيًا:** النظريات العلمية: ومفادها تحديد المسافة على أساس أقصى ارتفاع يمكن أن تصله طائرة، **ثالثًا:** نظرية السيطرة الفعلية: بحيث تمتد السيادة إلى الحد الذي تمارس فيه الدولة اختصاصًا

جرائم مُحدَّدة تتعلَّق بحماية تعاملات الأفراد، وعلى سبيل المثال، تم تنظيم حماية مصالح الأشخاص في التعاملات السيبرانية ـ وبما لا يشمل العمليات السيبرانية بين الدول، أو كل أنواع هذه العمليات[١] ـ وذلك بموجب اتفاقية مجلس أوربا "بودابست"، بشأن الجرائم المرتكبة عن طريق الإنترنت وشبكات الحاسوب الأخرى لعام ٢٠٠١[٢]، وكذلك تم تنظيم تأمين وحماية البيانات الشخصية الالكترونية، بموجب اتفاقية الاتحاد الأفريقي بشأن الأمن الالكتروني وحماية البيانات الشخصية لعام ٢٠١٤[٣].

وكانت معاهدة باريس عام ١٩١٩، من أوائل المحاولات المبذولة لتنظيم المجال الجوي، والتي نصت على سيادة الدولة الكاملة على مجالها الجوي، ثم أعادت معاهدتي مدريد ١٩٢٦، وهافانا ١٩٢٨، التأكيد على هذا المبدأ، ثم أُبرمت معاهدة شيكاغو عام ١٩٤٤[٤]، وأعادت النص على قاعدة سيادة الدولة الكاملة والمطلقة على الهواء فوق إقليمها، وفي عام ١٩٥٥، وأثناء انعقاد مؤتمر قمة جنيف بين الولايات

وسيطرة فعلية، **رابعًا:** النظرية الوظيفية: وترفض فكرة فصل المجال الجوي عن الفضاء الخارجي، وتكون التفرقة على أساس طبيعة النشاط ومدى تأثيره على الدولة، فيطبق قانون الفضاء على كل نشاط يرتبط بالفضاء منذ لحظة إطلاقه، أما إذا ارتبط النشاط بإقليم معين، فيطبق عليه النظام القانوني للهواء، وتمارس الدولة اختصاص عليه، أيًا كان ارتفاعه. **راجع:**

Report of the Scientific and Technical Subcommittee on the Work of its Fifth Session, *Para. 36, UN Doc. A/AC.105/39, 6 September 1967.*

(1) ***H. ROIGAS****, Mixed Feedback on the African Union Convention on Cyber Security and Personal Data Protection, INT'L CYBER DEVELOPMENTS REVIEW (Feb. 20, 2015),* ***available at:*** *https://perma.cc/795P-X22V. 8/3/2020.*

(٢) **اتفاقية مجلس أوربا "بودابست"، بشأن الجرائم المرتكبة عن طريق الإنترنت وشبكات الحاسوب الأخرى لعام ٢٠٠١** (*Budapest Convention on Cybercrime) (BCC*)**:** تُعد أول معاهدة دولية بشأن جرائم الإنترنت، **وهي تُركّز على تنظيم الجرائم ذات الصبغة الجنائية،** مثل انتهاكات حق المؤلف، والاحتيال الالكتروني، والتصوير الإباحي للأطفال، وانتهاك أمن الشبكات، وفُتح باب التوقيع والانضمام إلى المعاهدة، للأعضاء في "مجلس أوربا" وغير الأعضاء، ودخلت حيز النفاذ في ٢٠٠٤/٧/١، من خلال (٥) تصديقات بما فيها (٣) دول أعضاء في مجلس أوروبا، وتوقيعات (٥٥) دولة حتى تاريخ ٢٠٢٠/٧/٢٩. **راجع:**

Convention on Cybercrime*, Nov. 23, 2001, 2296 U.N.T.S. 167.*

(٣) **تغطي هذه الاتفاقية نطاقًا واسعًا لأنشطة الإنترنت،** بما يشمل التجارة الالكترونية، وحماية البيانات، والعنصرية وكراهية الأجانب، واستغلال الأطفال في المواد الإباحية، والأمن السيبراني الوطني، وتتطلب الاتفاقية من كل طرف، حماية بيانات مواطنيها الشخصية، وضمان عدم استخدامها إلا لغرض مشروع، كما تطلبت الاتفاقية من كل طرف، أن تضع إطارًا قانونيا لحماية "البيانات المادية"، ومن بين (٥٤) دولة وقعت على الاتفاقية، تتطلَّب الاتفاقية تصديق (١٥) منها، لتدخل إلى حيز النفاذ، وهو ما لم يحدث حتى الآن. **راجع:**

African Union Convention on Cyber Security and Personal Data Protection, *June 27, 2014, A.U. Doc. EX.CL/846(XXV).*

(٤) **في ١٢مارس لعام ١٩١٩، أُنشئت لجنة من سبعة دول،** لصياغة مشروع معاهدة بشان الهواء وقت السلم، وفي ١٣ أكتوبر عام ١٩١٣، انتهت اللجنة من صياغة المعاهدة، وتم التوقيع والتصديق عليها من (٣٣) دولة، وأطلق عليها معاهدة "باريس"، وقرَّرت في مادتها الأولي، مبدأ سيادة الدولة المطلقة على الفضاء الجوي فوق إقليمها، باستثناء حق المرور البريء لطائرات الدول الأجنبية. **وفي أول نوفمبر من عام ١٩٢٦، تم توقيع اتفاقية "مدريد"، من قبل ممثلي (٢١) دولة،** ورغم تصديق (٧) دول عليها، إلا أنها لم تدخل حيز النفاذ، وقد تطابقت أحكامها مع أحكام معاهدة باريس ١٩١٩، حيث تبنت قاعدة سيادة الدول المطلقة على الفضاء الجوي فوق إقليمها. **ووُقّعت معاهدة "هافانا" في ٢٠ فبراير ١٩٢٨،** ودخلت حيز النفاذ بعد تصديق (١١) دولة عليها، ونصت المادة (١) منها على قاعدة سيادة الدولة الكاملة والمطلقة على الفضاء الجوي فوق إقليمها، بنفس صياغة معاهدة باريس ١٩١٩، كما نصت على حق كل دولة في منع التحليق فوق مناطق معينة من إقليمها. **وفي ٧ ديسمبر عام ١٩٤٤،** وُقعت معاهدة "شيكاغو"، وأقرت في مادتها الأولي بالسيادة الكاملة والمطلقة لكل دولة، على الفضاء الجوي فوق إقليمها، وكذلك حقها في تقييد أو حظر تحليق الطائرات الأجنبية فوق مناطق معينة من إقليمها، لأسباب الضرورة العسكرية، أو الأمن العام، بما لا يعيق الملاحة الجوية. **راجع: د. على صادق عبد الحميد صادق،** أمن الدولة في النظام القانوني للهواء وللفضاء الخارجي، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، ١٩٧٩، ص ٨١: ٩٨.

المتحدة الأمريكية والاتحاد السوفيتي السابق وانجلترا وفرنسا، قدم الرئيس الأمريكي "ايزنهاور" مشروع أطلق عليه السماوات المفتوحة، بشأن تبادل المعلومات عن المنشآت والقواعد العسكرية في الولايات المتحدة الأمريكية والاتحاد السوفيتي، بطريق الاستطلاع والتصوير الجوي، وبما يعني حرية كل من الدولتين في القيام بالاستطلاع الجوي فوق أي منطقة في الدولتين مع استخدام ما يلزم من وسائل تقنية للتصوير[1].

وفيما يتعلَّق بالفضاء الخارجي، فقد تراضت الدول في الصكوك الدولية على أن القاعدة فيه هي الحرية، ولكن بما يتوافق مع قواعد القانون الدولي، ومن ذلك، ما نصت معاهدة الفضاء لعام ١٩٦٧ في مادتها الأولي، من أن لكل الدول حرية استكشاف واستخدام الفضاء الخارجي، بما في ذلك القمر والأجرام السماوية دون تمييز وفقا للقانون الدولي، كما نصت المادة الثالثة من المعاهدة، على أن التزام الأطراف عند مباشرتها لأنشطتها الخاصة باستكشاف واستخدام الفضاء الخارجي، بمراعاة القانون الدولي بما في ذلك ميثاق الأمم المتحدة.

ومما سبق، يُمكننا القول، بأن الفضاء السيبراني "*Cyber Space*"، يستقل عن أي مكان أو زمان محدد، ويخضع في جزء منه لمبدأ السيادة الإقليمية للدول، بينما لا يخضع "الفضاء الخارجي" "*Outer Space*"، لسيادة أي دولة، وقد تناولت بعض الاتفاقيات الدولية الفضاء الخارجي بالتنظيم، بينما لم يتم تناول الفضاء السيبراني بالتنظيم، إلا بشكل جزئي، لمواجهة جرائم مُحدَّدة، وأخيرًا، يُمكن توجيه عمليات سيبرانية من الفضاء السيبراني ضد الأنظمة الالكترونية ذات الصلة بالفضاء الخارجي.

المطلب الثاني

أنواع العمليات السيبرانية

يُستخدم الفضاء السيبراني لإتمام تعاملات الكترونية متنوعة، سواء للدول أم المؤسسات والكيانات الأخرى، والأفراد، ومن هذه التعاملات ما قد يُشكّل جرائم، تمس الأفراد والكيانات الخاصة كالشركات، ومن أمثلتها الجرائم السيبرانية ذات الصبغة الجنائية، والتسلل السيبراني، ومنها كذلك ما قد ينتج عنه أضرارًا، أو ربما يرقي لتهديد أمن الدول، مثل الهجمات السيبرانية، والحرب السيبرانية، والتجسس السيبراني.

ومع تشابه هذه الممارسات باعتبارها تتم الكترونيًا ومن خلال الفضاء السيبراني، إلا أنها ليست متماثلة أو مترادفة، فلكل منها خصائص مميزة، وقد يؤدي الخلط بينها إلى صعوبة أكاديمية، تتمثل في عدم معالجته أو دراستها بشكل صحيح، وصعوبات عملية تتعلق بكيفية الرد المقبول قانونًا من جانب الدول على كل منها، وكذلك صعوبات تشريعية، حيث تقوم معظم الدول بتنظيم تلك العمليات وطنيًا، باعتبارها نوع واحد يتعلَّق بالجريمة السيبرانية ذات الصبغة الجنائية، كالنصب، والسرقة، وتزوير التوقيع الالكتروني، ولا تُفرد تلك مساحة تنظيمية لباقي العمليات السيبرانية، التي هي من الخطورة بحيث تستهدف الأنظمة الالكترونية لمؤسسات الدول، وقد تكافئ الآثار الناتجة عنها، ما ينتج عن هجوم مسلح تقليدي، ويتطلّب الأمر معالجة كل منها بنصوص تتوافق مع تعريفها وطبيعتها وخصائصها المميزة، وآثارها المُحتملة.

---

(1) ***F. J. OSSENBECK, P. C. KROECK,*** *Open Space and Peace, A Symposium on Effects of observation, 1964, P. 30.*

ولأغراض الدراسة، نبدأ بالتمييز بين هذه الممارسات، وذلك بتعريف كل منها، وتحديد خصائصها المميزة، ثم نقوم بتحليل ما قد يَميّز كل منها عن الآخر، وذلك على النحو التالي.

الفرع الأول

التسلل السيبراني والهجوم السيبراني

أولاً: التسلل السيبراني:

تبدأ العمليات السيبرانية بالوصول غير المصرح به إلى داخل شبكة الكترونية ما، حيث يتم تخزين أو تداول بيانات سرية، أو محمية، ومجرد الوصول غير المشروع إلى المعلومات، يُمثّل لب التسلل السيبراني، حيث يتواجد المُتسلّل داخل شبكة معلومات تخص دولة ما، أو كيان بخلاف الدولة، أو شركة، أو أفراد، دون متابعة اتخاذ إجراءات أخري[١].

وبالتالي يمكن القول، بأن هذا التسلل يُمثّل خطوة أولي لكافة العمليات السيبرانية الأخرى، وبعد التسلل إلى الأنظمة الالكترونية، يكون أمام المُتسلّل خيارات عدة، وفقًا للهدف الذي يريد تحقيقه؛ فإما أن يقف عند حد التسلل دون المتابعة لتحقيق هدف آخر، وإما أن يتابع القيام بعمليات أخري، كنقل المعلومات السرية التي تم الاطلاع عليها، كما هي دون تعديل، وذلك إلى دولة أو كيان أو أفراد، وهو ما يُعرف بالتجسس السيبراني؛ أو القيام بتعديل هذه المعلومات، أو محوها، أو التحكم في أنظمة الكترونية، أو بني تحتية للدولة، أو تعطيلها، وهو ما يُصنَّف كهجمات سيبرانية، والتي إذا تكررت وتتابعت فإنها تُصنَّف كحرب سيبرانية.

ثانيًا: الهجوم السيبراني "*Cyber-attack*":

أوردت القاعدة رقم (٣٠) من "دليل تالين ١"، ونظيرتها رقم (٩٢) من "تالين ٢"، تعريفًا للهجوم السيبراني باعتباره: "عملية إلكترونية هجومية أو دفاعية، يُتوقع وفقًا للمجرى العادي للأمور أن تتسبب في أضرار جسيمة كإصابة أو موت أشخاص، أو تلف أو تدمير أشياء[٢]. ونلاحظ أن الأمثلة التي أوردها التعريف لأضرار الهجوم السيبراني، منها ما لا يُمكن تداركه كموت أشخاص، أو تلف أو تدمير أشياء، وهي نفس الآثار التي يُمكن أن تحدث نتيجة استخدام القوة، أو الهجوم العسكري المسلح من دولة على أخرى[٣].

وعَرّف في إستراتيجية الأمن السيبراني الألمانية، بأنه: "هجوم يتم من خلال الفضاء السيبراني، مُوجَّه للإضرار بأنظمة تكنولوجيا المعلومات لدولة، وذلك بتعديلها ـ كلها أو بعضها ـ أو تحريفها، أو

---

(1) ***M. C. WAXMAN****, Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), Yale Journal of International Law 36, 2011, PP. 421: 422.*

(2) ***Rule No. (92) Of the Tallinn Manual 2:*** *Definition of cyber attack: A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.*

(3) ***T. HERR, P. ROSENZWEIG****, Cyber Weapons and Export Control: Incorporating Dual Use with the Prep Model, 8 J. NAT'L SEC. L. & POL'Y, 2015, P. 301.*

تدميرها[١]. وهذه الآثار تنتج عما يُطلق عليه "القنبلة الذكية" "*Logic bomb*"، وهي برنامج أو أوامر الكترونية، تتسبب في إيقاف تشغيل نظام الكتروني أو شبكة الكترونية، و/أو محو جميع البيانات أو البرامج على الشبكة[٢].

وأوردت إستراتيجية المملكة المتحدة السيبرانية، ثلاثة أشكال يُمثل كل منها هجومًا الكترونيًا، وهي: "التلاعب بآليات تبادل المعلومات إلكترونيًا"؛ "اعتراض الموجات اللاسلكية"؛ "تعطيل الاتصالات الالكترونية[٣]".

وعرَّف دليل الجيش الأمريكي للعمليات السيبرانية والإرهاب السيبراني لعام ٢٠٠٥ " *U.S. Army's Cyber Operations and Cyber Terrorism*" **الهجوم السيبراني بأنه:** القيام عمدًا بأنشطة تخريبية لأجهزة كمبيوتر و/أو شبكات، بغرض التسبب في أضرار، أو تحقيق أهداف اجتماعية، أو أيديولوجية، أو دينية، أو سياسية، أو أي أهداف مماثلة، أو ترهيب أي شخص، أو أي جهة، لتحقيق تلك الأهداف[٤]، ووفقًا للدليل، تهدف الهجمات السيبرانية إلى تحقيق أهداف أربعة رئيسة، وهي:

١) التلاعب بحقيقة المعلومات وما يتعلق بأمانتها، وذلك بتعديلها لتصبح غير صحيحة وبلا قيمة؛

٢) إخفاء المعلومات وجعلها غير متاحة للمستخدمين المصرح لهم باستخدامها؛

٣) فض سرية المعلومات وكشفها، بحيث يَطَّلِع عليها مستخدمين غير مصرح لهم بذلك؛

٤) تدمير المعلومات ماديًا بمحوها أو إتلافها.

وفي عام ٢٠١١، نشرت قيادة إدارة الأمن السيبراني بالولايات المتحدة الأمريكية دليلاً، عرَّفت فيه الهجوم السيبراني بأنه: فعل عدائي يتم باستخدام الكمبيوتر، والشبكات والأنظمة السيبرانية ذات الصلة، ويهدف إلى تعطيل و/أو تدمير أو التلاعب بأنظمة الإنترنت لدولة، أو المعلومات المُخزَّنة على الحاسبات الآلية لها، أو وظائف هذه الأجهزة، ويتم هذا الهجوم بوسائل متعددة منها المراسلات الالكترونية المزيفة، أو الرسائل المفخَّخة، ويتميز الهجوم بأن آثاره عادةً ما تكون منفصلة من الناحية

---

(1) ***German Federal Ministry of the Interior***, *Cyber Security Strategy for Germany, Berlin: Beauftragter der Bundesregierung für Informationstechnik, 2011, PP. 14:15.*

(٢) **حيث يُحقّق الهجوم السيبراني أهداف التخريبية،** من خلال برامج الكترونية ضارة "فيروسات"، قادرة على تقويض نظم تشغيل الحاسبات الآلية، والتحَكُم فيها، ويُنظر إلي الأنظمة التي تتعرض لمثل هذا الهجوم، على أنها تعمل بشكل صحيح، ولا يتم اكتشاف ما أصابها من خلل بسهولة، مع استمرارها في إعطاء نتائج مضللة. **راجع:**

D. PUN, *Rethinking Espionage in the Modern Era, Chicago Journal of International Law, Volume 18, Number 1, 2017, P. 353.*

(3) ***UK Cabinet Office,*** *the UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World (November 2011),* ***available at:*** *https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf. 22/6/2019.*

(4) ***US Army Training & Doctrine Command,*** *DCSINT Handbook No. 1.02, Critical Infrastructure Threats and Terrorism: Cyber Operations and Cyber Terrorism Handbook, 2005, at VII-2.*

الجغرافية عن نقطة إطلاقه[1]. ونلاحظ أن التعريف قد ركَّز على غرضين للهجوم، وهما إلحاق الضرر بالنظم الالكترونية، أو المعلومات ذات الصلة، وتدمير البنية المادية المرتبطة بتشغيل واستخدام هذه النظم.

وعرَّفه جانب فقهي بأنه: "أي فعل يهدف إلى تقويض وظائف شبكة حاسوب لأغراض سياسية، أو أمنية، أو اقتصادية، تصب في صالح دولة أو دول معينة"[2]. **وكذلك هو:** "أية محاولات لتغيير، أو تعطيل، أو تدمير أنظمة الكمبيوتر، أو الشبكات أو المعلومات أو البرامج المُحمَّلة عليها أو التي تعمل من خلالها"[3]، ويمتد نطاقها وأثارها إلى ما وراء ذلك، حيث يمكن أن تُستخدم لتعطيل المنشآت الحيوية للدول والتي تعتمد في تشغيلها على الذكاء الاصطناعي، مثل محطات الكهرباء والمياه، ومحطات الطاقة النووية، وإشارات المرور، وغيرها[4].

وبتحليل التعريفات السابقة، نجد أنها تناولت الهجوم السيبراني، كفعل عدائي، ينتج عنه أضرارًا مباشرة للأنظمة الالكترونية التي يستهدفها، وغير مباشرة للدول، أو المؤسسات، أو الأفراد، حيث يُدمر تلك الأنظمة أو يعطلها أو يجعل التحكم فيها للمهاجم، ومن أمثلته، تعطيل الأنظمة الالكترونية لشبكات الكهرباء، وقطعها علي نطاق واسع، أو تدمير أنظمة تشغيل أحد السدود، والتسَّبب في حدوث فيضانات، أو تعطيل أجهزة مؤسسات طبية، بما قد يؤدي إلى حدوث وفيات، وهي أضرار قد تكافئ ما ينتج عن هجوم مسلح تقليدي أو أعمال عسكرية مادية، ويغلب استخدام الهجمات السيبرانية لأغراض سياسية، أو أمنية، أو ما يتعلَّق بإدارة الحكم في الدول، ومن ذلك، الهجوم السيبراني الذي شنته الولايات المتحدة الأمريكية على العراق، قبل هجومها المسلح عليه عام ٢٠٠٣، مما نتج عنه فض سريَّة رسائل بريد الكتروني لمؤسسات سيادية عراقية ونشرها[5].

وكثيرًا ما تستغل الدول كيانات خاصة للقيام بهذه الهجمات[6]، وعلى سبيل المثال، في أبريل ٢٠١٠، ورد في اعترافات "محمد ولد صلاحي"، في قضية بشأن عضويته في تنظيم القاعدة، أن التنظيم قد نفذ هجمات سيبرانية ناجحة، لاسيما هجوم عام ٢٠٠١، الذي استهدف حاسبات مكتب رئيس الوزراء الإسرائيلي، وكذلك إغلاق عدة مواقع على الإنترنت[7]، وأوضح المتهم أن التنظيم يحرص على تعزيز قدراته في مجال الحاسبات وتكنولوجيا المعلومات، وتكنولوجيا الانترنت والفضاء السيبراني، والإفادة من

---

(1) ***US DOD,*** *Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, Dirs. of the Joint Staff Directories, Joint Terminology for Cyberspace Operations, November 2011,* ***available at:*** *http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20 Cyberspace%20Operations.pdf. 2/4/2020.*

(2) ***O. HATHAWAY, et al.,*** *the Law of Cyber-Attack, Calif. L. Rev. 100, 2012, P. 820.*

(3) ***W. A. OWENS, K.W. DAM, H. S. LIN****, eds., Technology, Policy, Law, and Ethics Regarding US Acquisition and Use of Cyber-attack, Capabilities National Research Council Report, 2009, P. 1.*

(4) ***R. A. CLARKE, R. K. KNAKE****, Cyber War, P. R., PP. 70:74.*

(5) ***M. A. VATIS****, Cyber Attacks during the War on Terrorism: A Predictive Analysis, Institute for Security Technology Studies at Dartmouth College, Report OMB No. 074-0188, September 2001, PP. 5:9.*

(6) ***S. TOMAR,*** *Proxy Warfare, Journal of Defense Studies, Vol. 8, No. 2, 2014, P.152.*

(7) ***C. D. DELUCA****, the Need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors, Pace Int'l L. Rev. Online Companion 3, 2013, PP. 291:292.*

ذلك في التخطيط للهجمات وتنفيذها، مما يجعلها أكثر فاعلية في تحقيق أهدافها، مع الصعوبة البالغة في التعرف على مصدرها[١].

وفيما يتعلق بالصلة بين الهجوم السيبراني والتسلل السيبراني، فإن جميع الهجمات السيبرانية تبدأ بتسلل سيبراني، على عكس هذا الأخير، الذي تتوقف الإجراءات الخاصة به عند حد الوصول إلى الأنظمة الالكترونية، أي أن التسلل مرحلة يمكن وصفها بأنها ساكنة، لا تؤدي إلى تغيير بيانات مستهدفة، أو تدميرها أو تعديلها، وتقتصر فقط على مجرد الدخول والوصول إلى المعلومات، بخلاف الهجوم الذي يشمل إحداث أضرار، مثل تعطيل الأنظمة الالكترونية، أو تعديل البيانات المُخزَّنة عليها، أو محوها.

الفرع الثاني

الجريمة السيبرانية والإرهاب السيبراني

أولاً: الجريمة السيبرانية:

أشارت الأمم المتحدة في المدونة الصادرة عنها بشأن الجريمة المعلوماتية، إلي عدم وجود اتفاق بين الخبراء بشأن العناصر المكونة لجرائم الكمبيوتر، وبالتالي لا يوجد تعريف دولي جامع أو متفق عليه لهذه الجرائم، حيث تتشعَّب وتكثر الأفعال التي يمكن أن ينطبق عليها هذا الوصف، وتبقي هذه الإشكالية محلاً لاجتهاد الفقهاء، الذين رغم اختلافهم، فقد اتفقوا على بعض سمات هذه الجرائم، مثل كونها:

(١) أفعال غير مشروعة قانونًا، تتم باستخدام أنظمة الحواسيب الآلية المتصلة بشبكة الانترنت، والمعدات التقنية ذات الصلة[٢]، فهي تنتهك قواعد جنائية وطنية، أو قواعد من القانون الجنائي الدولي، وتتشابه مع الجرائم العادية في عناصرها، ولكنها تختلف عنها باختلاف البيئة والوسائل المستخدمة، وهي التكنولوجيا الحديثة من وسائل اتصال وشبكات معلوماتية.

(٢) تهدف إلى الحصول على معلومات غالبًا ما تخص الأفراد والكيانات الخاصة، مثل بيانات وحسابات البنوك، وذلك بغرض الابتزاز أو التسبب في ضرر لضحية، وفي قليل من الأحوال تتم بهدف استخدام المعلومات المُتحصل عليها في أغراض سياسية أو تقويض الأمن القومي لدولة[٣].

(٣) غالبًا ما تُرتكب من قبل جهات أو كيانات فاعلة بخلاف الدول[١].

---

(١) **وعقب قتل "أسامة بن لادن"، دعا تنظيم القاعدة أعضاءه للقيام بما أطلق عليه "الجهاد السيبراني"**، من خلال شن سلسلة هجمات سيبرانية على بعض الدول، ومنها "بريطانيا"، التي أعلنت أنها تستعد بخطة تأهب قُصوى، لمواجهة تلك الهجمات. ومن المنظمات المُصنَّفة ككيانات إرهابية ذات قدرات تكنولوجية تمكنها من الانخراط في هجمات سيبرانية، أربع منظمات مقرها الولايات المتحدة الأمريكية، وهي: "*Nation*"، "*Stormfront*"، "*Hammerskin*"، "*Aryan*". **راجع:** ***D. B. HOLLIS****, Why States Need an International Law for Information Operations, Lewis & Clark Law. Review 11, 2007, PP. 1031: 1033;* ***U.K. Secretary of State for the Home Dep't, Contest:*** *the United Kingdom's Strategy for Countering Terrorism, 2011,* ***available at:*** *https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97995/strategy-contest.pdf. 19/3/2020.*

(2) ***O. HATHAWAY, et al****., the Law of Cyber-Attack, P. R., PP. 833: 834.*

(3) ***M. GERCKE****, Understanding Cybercrime: Phenomena, Challenges and Legal Response (ITU): Telecommunication Development Bureau, 2012, PP. 2:3.*

وقد عُرِّفت باعتبارها، سلوك غير مشروع، يماثل أي جريمة تقليدية، مثل السرقة، والاحتيال، والابتزاز، وسرقة الهوية، إلا أنها تتم بوسائل الكترونية مُستحدثة وعبر الإنترنت، فهي جريمة قديمة تتم بطريقة جديدة، وقد قُدّر في عام ٢٠١٥، أن حوالي ٥٩٤ مليون شخص في جميع أنحاء العالم كانوا ضحايا جرائم على الإنترنت(٢).

وكذلك هي أنشطة غير مشروعة تستهدف المعلومات السرية، وتؤثر على وجودها وسلامتها، من حيث الاطلاع عليها، أو تعديلها، أو تخريبها، أو حذفها، وذلك باستخدام تقنيات الكترونية، كالكمبيوتر وشبكة الانترنت، والبرامج المعلوماتية، وينتج عنها ضرر جسيم للدول، والمؤسسات، والكيانات الخاصة، والأفراد(٣).

وتعني كذلك، أي سلوك الكتروني يستهدف فرد، أو فئة من الأفراد، بغرض الحصول على معلومات عن الحسابات البنكية، أو أرقام بطاقات الائتمان السرية، بغرض سرقتها أو التحويل بين الحسابات المالية، أو سرقة حسابات الإنترنت، لاستخدامها في انتحال الشخصية، أو التهديد، أو التشهير، أو التحريض على أعمال غير مشروعة، أو انتهاك حقوق الملكية الفكرية والأدبية، بحيث يحقق الجاني فوائد مادية أو معنوية، مع تحميل الضحية خسارة مقابلة(٤).

ومن تعريفات الجرائم الالكترونية المعروضة، نلاحظ أنها قد اتصفت باتساع النطاق، بحيث تشمل أي نشاط إجرامي يتم في الفضاء السيبراني، وربما يؤدي هذا النطاق الواسع، إلى الخلط بين أنواع "العمليات السيبرانية"، وهو ما حدث واقعًا، في حادثة اختراق الأنظمة الالكترونية لفرع شركة "*Sony*" اليابانية، بالولايات المتحدة الأمريكية في ٢٤ نوفمبر عام ٢٠١٤، وأعلنت الشركة أنها تعرَّضت لإرهاب سيبراني، على غرار هجمات ٩/١١(٥)، ولاحقًا، صنَّف مكتب التحقيقات الفيدرالي الأمريكي، العملية بأنها هجوم سيبراني، ثم أشار "أوباما"، إلى أن العملية جريمة سيبرانية.

---

(1) ***S. GORDON***, ***R. FORD,*** *On the Definition and Classification of Cybercrime, J. Computer Virology, 1, 2006, P. 13.*

(2) ***D. LITTLE, J. SHINDER***, *Scene of the Cybercrime: Computer Forensics Handbook, MA: Syngress Publishing, Inc. Rockland, 2002, P. 16.*

(3) ***S. W. BRENNER***, *At Light Speed: Attribution and Response to Cyber crime/Terrorism/Warfare, the Journal of Criminal Law and Criminology, No.97, Issue 2, 2007, PP. 382: 386.*

(4) ***T. PARKER***, *6 Ways to Protect Yourself against Cybercrime,* ***available at:*** *www.investopedia.com. 1/2/2019.*

(٥) **قرَّرت الشركة أن الهجوم استهدف إتلاف "فيلم" سينمائي باسم "المقابلة"**، يتعلق موضوعه باغتيال رئيس كوريا الشمالية، وقد نفت الأخيرة أي صلة لها بالواقعة، لكنها أشادت بجماعة "حراس السلام" التي أعلنت مسئوليتها عن الهجوم، باعتبارها قد قامت بعمل صالح"، وقد تعهَّد "أوباما" بالرد الذي يتناسب مع الهجوم، وفي الوقت والمكان وبالطريقة التي ستراها الإدارة الأمريكية مناسبة، **راجع:**

G. REYNOLDS, *Ethics in Information Technology, Cengage Learning, Rab. II 14, 2018, PP. 126: 129;* ***D. ROBERTS***, *"OBAMA" Imposes New Sanctions against North Korea in Response to Sony Hack, the Guardian January 2, 2015,* ***available at:*** *http://www.theguardian.com/us-news/2015/jan/02/obama-imposes-sanctions-north-korea-sony-hack-the-interview. 21/3/2020.*

ومن العرض السابق، وبشأن التمييز بين الجريمة الالكترونية والهجوم السيبراني، يمكن القول بأن:

(١) تشير الجريمة الالكترونية إلى كل فعل غير مشروع يتم من خلال الفضاء السيبراني، سواء تسبب في حدوث أضرار أم لم يُسبّب، وفي حالة حدوث ضرر، فلا يُشترط فيه درجة معينة من الخطورة، وذلك بخلاف الهجوم السيبراني.

(٢) تستهدف الجريمة الالكترونية الدول، والمؤسسات، والكيانات الخاصة، والأفراد، بينما يكثر وقوع الهجوم السيبراني على الدول ومؤسساتها، وتميل بعض التعريفات لأخذ الجريمة الالكترونية في اتجاه جرائم الأموال، كالسرقة والنصب وغيرها، مع كونها تتم من خلال بيئة الكترونية، وذلك بخلاف الهجمات السيبرانية التي يغلب عليها طابع استهداف الدول، ولغرض التخريب أو الإضرار السياسي أو الأمني أو الاقتصادي لها.

(٣) تبدأ الهجمات السيبرانية عادةً بأفعال تعتبر جرائم الكترونية، وبالتالي يمكن القول بأن كل هجمة الكترونية تبدأ بجريمة الكترونية، ولكن ليست كل جريمة الكترونية يمكن أن تتطور لتصير هجومًا الكترونيًا.

ثانيًا: الإرهاب السيبراني:

دعا مجلس الأمن الدولي في قراره رقم (١٥٦٦) لعام ٢٠٠٤، جميع الدول إلى حظر عدة أفعال، وعدم تبريرها أو القيام بها لاعتبارات سياسية، أو أيديولوجية، أو عرقية، أو دينية أو فلسفية، ومنها: "... الأعمال الإجرامية، بما فيها الموجهة ضد المدنيين، والتي ينتج عنها أو يُقصد من ورائها التسبب في الوفاة، أو الإصابة البدنية الجسيمة، أو تدمير الممتلكات، أو إلحاق أضرار جسيمة بها، أو أخذ الرهائن، أو الترهيب وإثارة حالة من الرعب بين عامة الناس، أو بين مجموعة من الأشخاص، أو بين أشخاص معينين، أو لإجبار حكومة دولة أو منظمة دولية للقيام أو الامتناع عن أي فعل والتصرف بطريقة معينة...[1]".

وعادةً ما تهدف الجرائم الإرهابية إلى تحقيق الأفعال التي حظرها قرار مجلس الأمن السابق، لاسيما الإضرار بالمدنيين، ونشر الرعب بين مواطني الدول، إلى جانب تهديد أمن وسلامة واستقرار الدول، أو محاولة تقويض أنظمة الحكم الوطنية، وقد تطورت وسائل ارتكاب هذه الجرائم، بحيث صارت تتم من خلال الفضاء السيبراني، مما يُيّسر ارتكابها عن بعد، مع سهولة جمع المعلومات التخطيط والإعداد لها، وتبادل وتنسيق الخبرات بشأنها، وصعوبة معرفة المهاجم، أي أن الفضاء السيبراني قد وفّر لهذه الكيانات الإرهابية مساحات افتراضية للتدريب، والعمل بعيدًا عن مخاطر مواجهة الجيوش النظامية[2].

ومن الأمثلة على ذلك، أنه بعد وقوع أحداث الحادي عشر من سبتمبر عام ٢٠٠١، فَقَد تنظيم القاعدة معظم مقراته الآمنة في أفغانستان، فاتجه إلى استخدام التكنولوجيا لتبادل المعلومات، ونقل رسائل

(1) ***UNSC Resolution (1566) (2004),*** *8 October 2004, UN Doc S/RES/1566(2004).*
(2) ***C. WILSON****, CRS Report for Congress, Computer Attack and Terrorism: Vulnerabilities and Policy Issues for Congress, 1 April, 2005,* ***available at:*** *http://www.iwar.org.uk/cyberterror/resources/crs/45184.pdf. 12/1/2019.*

"بن لادن" وقادة القاعدة حول العالم، واستغل التنظيم من خلال الفضاء السيبراني بدون أي مخاطر، ومن ذلك، استمرار حركة "طالبان" ولأكثر من سنة، في نشر وإذاعة عملياتها العسكرية في أفغانستان عبر موقع الكتروني، استأجرته من شركة أمريكية في ولاية "تكساس"، بمبلغ (٧٠) دولارًا في الشهر، تُدفع بواسطة بطاقة ائتمان، ويتفاعل مع هذا الموقع نحو (١٥) مليون مستخدم. وكذلك، في عام ٢٠٠٧، قام مجموعةٌ من الجنود الأمريكيين بالتقاط صور تذكارية في قاعدة عسكرية بالعراق، وظهر في خلفيتها مجموعة من طائرات الهليكوبتر، وبعد قيام الجنود بتحميل الصور على الإنترنت، استطاعت جماعة إرهابية استغلال "العلامات الجغرافية" "*Geotags*" التي أفصحت عنها الصور، وحدَّدت موقع القاعدة، ودمرت أربع طائرات باستخدام قذائف الهاون[١].

وفي حين تستهدف معظم الجرائم الالكترونية جني مكاسب شخصية غير مشروعة، يتم توجيه الإرهاب السيبراني بشكل أكبر لتحقيق أهداف سياسية، أو طائفية، أو تقويض نظم داخلية، وزعزعة ثقة المواطنين في قدرة الدول على حمايتهم، ولذا يمكن القول بأن الجريمة الالكترونية، تستهدف الأفراد أو المؤسسات الخاصة، ويهدف القائم بها في الغالب إلى تحقيق مغنم ما، وتختلف عن الإرهاب السيبراني في الغرض والنتيجة.

الفرع الثالث

الحرب السيبرانية والتجسس السيبراني

أولاً: الحرب السيبرانية:

يصف مصطلح "الحرب السيبرانية"، كل الأفعال التي تستهدف تخريب أو تعطيل الأنظمة التكنولوجية المتصلة بالإنترنت، والتي تعتمد عليها الدول في إدارة مؤسساتها، بحيث يؤدي ذلك إلى وقوع أضرار ربما تُكافئ ما قد ينتج عن استخدام دولة للقوة العسكرية المسلحة، وتُعد الولايات المتحدة الأمريكية من بين أول الدول التي أوردت تعريفًا للحرب السيبرانية، **حيث قسمت وزارة الدفاع الأمريكية العمليات التي يُمكن وصفها بأنها كذلك إلى فئات ثلاث؛** الحرب السيبرانية الهجومية، ونظيرتها الدفاعية، والثالثة استخباراتية.

واعتبرت الوزارة أن **الحرب السيبرانية الهجومية تعني:** "عمليات وإجراءات معادية باستخدام الكمبيوتر، أو الشبكات أو الأنظمة ذات الصلة، وتهدف إلى تعطيل، و/أو السيطرة على، و/أو تدمير الأنظمة السيبرانية الحيوية، و/أو المعلومات المُخزَّنة على أجهزة الكمبيوتر المتصلة بتلك الشبكات. **ووفقًا للمفهوم الدفاعي تعني:** "الإجراءات المُتخذة للحماية من الأنشطة غير المصرح بها، داخل أنظمة معلومات وزارة الدفاع وشبكات الكمبيوتر، وبما يشمل رصد هذه الأنشطة، وكشفها، وتحليلها، والرد عليها". **وفي مجال الاستخبارات، عُرفت بأنها**: "اختراق أنظمة الشبكات الالكترونية لدولة، بغرض الحصول على معلومات سرية، واستغلالها لصالح الدولة القائمة بالتجسس وفقًا للهدف من العملية، والذي يغلب عليه طابع تقييم قدرات الدولة الضحية[٢].

---

(1) ***S. W. BRENNER**, At Light Speed, P. R., P. 386; **S. VENTKATESH**, Cyber Terrorism, Authors Press, Delhi, 2003, P. 24.*

(2) ***DOD Joint Terminology for Cyberspace Operation,** Washington, D.C. 20318-9999, 2018, P. 6.*

كما عرَّف جانب فقهي الحرب السيبرانية بأنها: استخدام حاسبات وأنظمة ووسائل إلكترونية، للقيام بعمليات هجومية تمس سلامة الحاسبات والشبكات والأنظمة الالكترونية لدول أخرى، بغرض تحصيل ميزة نسبية على هذه الدول، والتي قد تتمثل في التلاعب بسرية البيانات والمعلومات الالكتروني لها، أو محوها وتدميرها، أو التحكم بنظم تشغيل مؤسساتها[١].

ونلاحظ أن التعريفات المعروضة للحرب السيبرانية، قد ابتعدت عن مفهوم الحرب الوارد في الصكوك الدولية باختلاف مراحل تطورها، كما أنها قصرت مفهوم تلك الحرب، على مهاجمة الأنظمة الالكترونية لدولة، والقيام بأفعال تمس نزاهة وسرية المعلومات المُحَمّلة عليها، أو التحكم فيها، أو تدميرها، دون التعرض للآثار الأخرى، مثل تدمير بني تحتية حكومية، أو تعطيل الاتصالات المدنية، أو التلاعب بالأسواق المالية، والتسبب في أضرار اقتصادية، أو وفاة أشخاص[٢]، **ووفقًا لهذا النظر، ظهرت بعض التعريفات التي اتسمت بتوسعها في تعريف الحرب السيبرانية،** لاسيما فيما يخص الآثار التي قد تنتج عنها، ومنها ما يلي:

عرَّفت منظمة شنغهاي للتعاون، "النزاعات السيبرانية"، و"حروب المعلومات السيبرانية"، باعتبارهما نزاعًا مسلحًا بالمعنى المقصود في القانون الدولي الإنساني، ويعني مواجهة بين دولتين أو أكثر، من خلال الفضاء السيبراني، وباستخدام تكنولوجيا المعلومات والشبكات، وتهدف فيه كل منهما إلى الإضرار بالأنظمة الالكترونية للأخرى، وزعزعة استقرار المجتمع، أو تقويض النظم السياسية، أو الاقتصادية، أو الاجتماعية، أو إكراه الدولة الخصم على اتخاذ قرارات تحقق مصلحة طرف أو أطراف معادية[٣].

كما بيَّنت اللجنة الدولية للصليب الأحمر أن "الحرب السيبرانية"، تشير إلى وسائل وأساليب حديثة للنزاعات المسلحة، تتمثل في شن عمليات سيبرانية، قد تكافئ آثارها ما ينتج عن النزاع المسلح، أو إجراء هذه العمليات في سياق نزاع مسلح بالمعنى المقصود في القانون الإنساني الدولي[٤].

وعرّفها جانب فقهي بأنها: "سلسلة هجمات تقوم بها دولة ضد أخرى بواسطة الفضاء السيبراني، وقد تُعادل آثارها ـ في بعض الحالات ـ ما ينتج عن الهجوم المسلح التقليدي، أو استخدام القوة العسكرية، ويكون استخدام القوة هو الرد المُتناسب معها، عندما تؤدي إلى وقوع وفيات أو إصابات، أو تدمير للممتلكات[٥].

وتعني كذلك هجمات الكترونية تتم في دقائق معدودة، ضد البني التحتية الالكترونية لدولة، بغرض تدميرها، أو السيطرة عليها والتحكم فيها، والتسبب في أضرار مادية، تكافئ ما قد ينتج عن

---

(1) ***S. W. BRENNER, L. L. CLARKE***, *Civilians in Cyber Warfare: Conscripts, Vanderbilt Journal of Transnational Law, 43, 2010, PP. 1028: 1031.*

(2) ***A. J. SCHAAP***, *Cyber Warfare Operations: Development and Use under International Law, A. F. L. Rev. 64, 2009, P.133.*

(3) ***Annexure to the Agreement between the Government of the Member States of the Shanghai Cooperation***, *in the Field of International Information Security (16 June 2009) Shanghai Cooperation Organization (SCO).*

(4) ***ICR,*** *What Limits Does the Law of War Impose on Cyber Attacks? (June 2013),* ***available at:*** *https://www.icrc.org/eng/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm.15/11/2019.*

(5) ***J. W. ROLLINS***, ***C. A. THEOHARY***, *Cyber warfare and Cyber terrorism: In Brief, Congressional Research Service (CRS) Report, R43955, March 27, 2015, P. 11.*

الهجمات المسلَّحة التقليدية، كإصابة أفراد، أو وفيات، أو تدمير ممتلكات، ومن أمثلتها، التحكم في نظم إطلاق الصواريخ، وتوجيهها لتدمير بعض مؤسسات للدولة، أو تخريب أنظمة مراقبة الحركة الجوية والأرضية، مما ينتج عنه حوادث تتضمن إصابات ووفيات، أو فض سرية البريد الالكتروني لمؤسسات عسكرية وسيادية، أو تعطيل أنظمة الأمن الغذائي، أو تعطيل شبكات الكهرباء، أو القيام بكل ذلك، مع بقاء هوية المهاجم غير معروفةً[١].

ثانيًا: التجسس السيبراني:

عّرِّف المُؤلَّف الخاص بحلف "الناتو"، بعنوان "*Peacetime Regime for State Activities in Cyberspace*" التجسس السيبراني بأنه: قيام دولة، أو جهاز تابع لها، أو وكيل عنها، بالاطلاع على، أو نسخ البيانات السرية غير المتاحة للجمهور، والمحفوظة على أنظمة تكنولوجيا المعلومات، أو شبكات الكمبيوتر الموجودة في إقليم أو منطقة خاضعة لولاية دولة أخرى، بواسطة عمليات سرية وبذرائع مزيفة، أو كاذبة، وبدون ترخيص أو موافقة من مالكي أو مشغلي هذه الأنظمة، أو شبكات الحاسوب المستهدفة، أو الدولة الإقليمية[٢].

وعُرِّف كذلك بأنه الوصول غير المصرح به إلى معلومات سرية مخزنة في حاسبات الكترونية، أو على شبكات تكنولوجيا المعلومات، كتلك المتعلقة بالملكية الفكرية، أو مشاريع البحث والتطوير، أو أي معلومات أخرى محمية من قبل مالكها، أو أسرار تخص كيان ما، كالدول، أو المؤسسات العسكرية، أو الشركات، أو حتى الأفراد، ونسخها وسرقتها ونقلها لجهة أو جهات أخرى[٣].

وكذلك هو استغلال شبكة الحاسوب الالكترونية "*CNE*" "*Computer Network Exploitation*"، أو التسلل إليها، والحصول على معلومات سرية، باستخدام مظهر خادع أو مُموّه، وربما يتطور إلى هجوم إلكتروني إذا تم تطوير استغلال المعلومات في عمل هجوم على الشبكة أو تخريبها[٤].

---

(1) ***M. ROSCINI***, *World Wide Warfare: Jus ad bellum and the Use of Cyber Force, 14 Max Planck Y.B. United Nations Law, 2010, P. 96;* ***F. DELERUE***, *State Responses to Cyber Operations, European University Institute, Ph.D. in Law, Global Relations Forum Young Academics Program, Policy Paper Series No.5, 2016, P. 11.*

(2) ***K ZIOLKOWSKI***, *Peacetime Cyber Espionage, New Tendencies in Public International Law, in K. ZIOLKOWSKI (ed), Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy, 1st edn., NATO CCD COE Publication, Tallinn 1, 2013, P. 429.*

(3) ***C.f. The MI5,*** *Cyber Threats,* ***available at:*** *https://www.mi5.gov.uk/home/the-threats/cyber.htmlviewed. 12/3/2019.*

(4) ***The Vice Chairman of the Joint Chiefs of Staff***, *Joint Terminology for Cyberspace Operations, 2010,* ***available at:*** *http://www.nsciva.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace %20Operations.pdf. 12/3/ 2019.*

ويشير كذلك إلى أي فعل يتم القيام به سرًا، أو تحت ذرائع كاذبة باستخدام القدرات السيبرانية لجمع المعلومات أو محاولة جمعها، ومن أمثلة هذه القدرات، مراقبة الاتصالات أو البيانات أو المعلومات الأخرى، أو نسخها، أو التقاطها، أو نقلها أو تخزينها إلكترونيًا[١].

ويعني كذلك عملية الكترونية لنسخ، والحصول على بيانات سرية مُخزَّنة في الفضاء السيبراني، أو عابرة له، فهو ينصَّب على نسخ البيانات، ولا يؤثر على سلامتها أو وجودها، أو سلامة الشبكات والأنظمة التي تُخزنها أو تقوم بتداولها، وإذا نتج عن تلك العملية تدمير البيانات أو إتلافها، أو التأثير على وظائف شبكات وأنظمة الكمبيوتر، فإنها تُصنف كهجوم سيبراني، باعتبار أن التجسس السيبراني له طبيعة استغلالية ولا يهدف إلى التأثير على البيانات أو المعلومات، بخلاف الهجمات السيبرانية التي ربما ينتج عنها آثارًا جسيمة، نتيجة التحكم بالبيانات والمعلومات، أو محوها[٢].

وفي الوثيقة التي أعدها معهد "الشرق والغرب" "*East West Institute*"، خلال عام ٢٠١٤، والتي تمثل جهدًا مشتركًا بين خبراء "روس"، وأمريكيين، تم تعريف التجسس السيبراني بأنه: "عملية إلكترونية تهدف إلى الحصول على معلومات سريَّة، غير مصرح بالاطلاع عليها، وذلك باستخدام وسائل سرية[٣].

وعرَّف دليل "تالين ١" التجسس السيبراني وقت النزاعات المسلحة بأنه: أي عمل يتم تنفيذه سرًا، أو تحت ادعاءات كاذبة، بواسطة قدرات الكترونية، بغرض جمع معلومات، أو محاولة جمعها بقصد إبلاغها إلى طرف مُعادٍ، وأوردت القاعدة رقم (٦٦/أ) منه أن التجسس السيبراني وغيره من أشكال جمع المعلومات، المُوجَّهة ضد العدو أثناء النزاع المسلح، لا تنتهك قانون النزاعات المسلحة، **وبشأن تمييز التجسس السيبراني عن الحرب السيبرانية، يمكن القول بالآتي:**

(١) ينطوي التجسس السيبراني على ممارسة جمع معلومات سرًا، من خلال وسائل الكترونية، ولا يهدف إلى إلحاق أضرار مادية فورية، أو تعطيل الأنظمة الالكترونية للدول المُستهدفة، في حين أن الحرب السيبرانية غالبًا ما ينتج عنها أضرارًا، مباشرة للأنظمة الالكترونية، وغير مباشرة كآثار لتدمير تلك الأنظمة أو تعطيلها، ومن أمثلة هذا التجسس، البرنامج الذي أُطلق عليه "*Flame*"، وأُكتشف عام ٢٠١٢، وكان قد استمر لمدة عامين في التجسس على حاسبات، وأفراد، وشركات، ومؤسسات حكومية في الشرق الأوسط، وتمكن واضعوه من جمع قدر هائل من المعلومات، ونقل كل ما عُرض على شاشات الأجهزة المُستهدفة، وتسجيل الاتصالات التي تمت على برامج المحادثات مثل "*Skype*"، دون تغيير أي بيانات، أو إتلافها، أو التسبب بأية أضرار مادية[٤].

---

(1) ***M. N. SCHMITT, L. VIHUL****, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, P. R., P. 168.*

(2) ***I. KILOVATY****, World Wide Web of Exploitations – the Case of Peacetime Cyber Espionage Operations under International Law: Towards a Contextual Approach, 18 Columbia Science and Technology Law Review, 2016, PP. 42: 48.*

(3) ***EASTWEST INSTITUTE,*** *RUSSIA-U.S. Bilateral on Cybersecurity Critical Terminology Foundations 2, P. R., Websit.*

(٤) **وقد رجَّح المختصون أن هذا البرنامج المتطور، من إنتاج دولة أو على الأقل كيان تدعمه دولة، كما تم الكشف في أكتوبر من عام ٢٠١٢**، عن حالة أخرى من التجسس السيبراني تمت على نطاق واسع، حيث اكتشفت شركة أمن

(٢) يتوافق تعريف التجسس السيبراني وقت النزاعات المسلحة، مع نظيره الوارد في الاتفاقيات الخاصة بالحرب والنزاعات المسلحة، مع افتقار المصدرين سواء الدليل، أم اتفاقيات الحرب، إلى حسم إشكالية التجسس في زمن السلم، وقد يرجع ذلك ولو جزئيًا إلى أن قواعد القانون الدولي عمومًا لم تحسم هذه الإشكالية صراحة.

(٣) يمكن وصف التجسس السيبراني، باعتباره جريمة حالة وأخري مؤجلة، وتتمثَّل الأولي في الولوج غير المُصرّح به للأنظمة الالكترونية لدولة، والاطلاع على بيانات ومعلومات سريّة، وتتحقّق الجريمة المؤجلة، عند استخدام هذه المعلومات لاحقًا للإضرار بالدولة المُستهدفة، بينما يمكن وصف الحرب السيبرانية بالجريمة الفورية التي تحدث آثارها بمجرد وقوعها.

(٤) الحرب السيبرانية تشمل عدة هجمات الكترونية، سواء تمت في مرة واحدة أم على دفعات، أما التجسس السيبراني فإنه في حد ذاته لا يُمثّل هجومًا الكترونيًا، حيث يهدف للحصول على معلومات ويتم إنهاء حالة التجسس بعد تمام هدفه، ولكن عند استخدام المعلومات المُتحصل عليها في شن هذه هجمات الكترونية فإن ذلك يعتبر مرحلة منفصلة عن التجسس، ولها تعريفها وخصائصها التي تميزها.

ونلاحظ وجود علاقة بين المفاهيم المختلفة للانتهاكات السيبرانية، سواء التسلل، أم الحرب، أم الهجوم، أم الجرائم السيبرانية؛ من حيث إن كل منها يتم باستخدام وسائل تقنية خاصة بالشبكات والحاسبات، وأن أي انتهاك منها يبدأ بفعل التسلل إلى الموقع المُستهدف، ثم يتنوع قصد المُتسلل بعد ذلك، إما أن يتبع التسلل بمجرد الاطلاع على معلومات سرية من الموقع أو ننسخها ونقلها، دون تغيير شيء في هذا الموقع وما يتضمنه من معلومات، ودون محاولة للسيطرة عليه أو التحكم فيه، وهنا نكون بصدد تجسس الكتروني.

أما إذا تلي التسلل السيبراني توافر قصد جنائي للحصول على مغنم ما، باستغلال الوجود على الموقع المُستهدف، كالسرقة أو النصب أو الاستيلاء على بيانات مالية، نكون بصدد جرائم الكترونية.

وإذا أعقب المهاجم التسلل السيبراني بالتحكم في البيانات الموجودة على الموقع المستهدف، والسيطرة عليها واستغلال ذلك في تعطيل المرافق الأساسية، أو تخريبها أو تعطيلها، فإننا نكون بصدد هجمات الكترونية.

أما الحرب السيبرانية فإنها تتمثل في شن عدة هجمات الكترونية، سواء كانت دفعة واحدة أو على عدة مراحل، ولذا فإنها أوسع نطاقًا من الهجمات السيبرانية، وقد يتم شن الحرب السيبرانية ضمن نزاع مسلح مادي بين دولتين، وربما ترقي الآثار الناتجة عنها لتُكافئ ما ينتج عن استخدام القوة العسكرية المادية.

وقد تتداخل الانتهاكات السابقة في بعض مراحلها، فمثلاً وفي ظروف معينة قد تشكل الحرب السيبرانية أيضًا جريمة إنترنت، عندما تتم هذه الحرب وفقًا لعدة مراحل، تمثل إحداها جريمة الكترونية،

البرمجيات "*Kaspersky*"، حملة تجسس إلكتروني أُطلق عليها اسم "*Red October*"، كانت نشطة منذ عام ٢٠٠٧، وتهدف إلى جمع معلومات استخباراتية من بعثات دبلوماسية، ومؤسسات البحوث العلمية والحكومية لعدة دول. **راجع:**
***Kaspersky Labs and ITU Research**, New Advanced Cyber Threat, (Kaspersky Lab 29 May 2012, **available at:** http://usa.kaspersky.com/about-us/presscenter/ press-releases/kaspersky-lab-and-itu-research-reveals-new-advanced-cyberthrea. 25/3/2019.*

كتنفيذ الحرب بعد تقويض وظائف شبكة كمبيوتر تابعة لمؤسسة عسكرية وحكومية لعدو، مع تصنيف هذا التقويض في القانون الوطني للدولة المُستهدفة كجريمة جنائية، أو اعتباره جريمة بموجب قواعد القانون الجنائي الدولي.

المبحث الثاني

مدي انطباق القانون الدولي الساري على العمليات السيبرانية

يتضمن القانون الدولي العام نوعين من القواعد التي تُنظّم استخدام الدول للقوة؛ **يتعلَّق الأول** بمشروعية استخدامها قبل نشوب الأعمال العدائية "*jus ad bellum*"[1]، **وينظم النوع الثاني** استخدامها أثناء النزاعات المسلحة "قانون الحرب" "*jus in bello*"، حيث تُعني بتطبيق مبادئ الإنسانية، والاستخدام المشروع للأسلحة، والأهداف المشروعة، وحماية بعض الفئات والأماكن والأشياء[2]. ولم يتعرَّض أي من النوعين صراحةً للعمليات السيبرانية، بالنظر إلى أن هذه القواعد قد أُبرمت في وقت لم تكن فيه هذه العمليات شائعة أو ربما حتى مُتصورة، فتم التركيز على تنظيم وسائل وأساليب استخدام القوة المادية أو "الحركية"، والتي تختلف في طبيعتها وخصائصها عما قد يتم في مجال الفضاء السيبراني من عمليات[3].

وإذا كانت قواعد القانون الدولي الإنساني لم تتطرق مباشرةً، إلى تنظيم أو ضبط العمليات السيبرانية؛ إلا أن بعض النصوص الدولية، والاتجاهات الفقهية، والأحكام القضائية الدولية، تدعم رؤية مفادها إمكان تطبيق تلك القواعد، وكذلك مبادئ القانون الإنساني على العمليات السيبرانية، ولدراسة هذه الاتجاهات فإننا نقسم هذا المبحث إلى المطالب التالية.

المطلب الأول: الأساس المنطقي لتطبيق قواعد القانون الدولي الساري على العمليات السيبرانية.

المطلب الثاني: تطبيق ومفاهيم مبادئ القانون الدولي الإنساني على العمليات السيبرانية.

المطلب الثالث: حق الدفاع عن النفس في مواجهة العمليات السيبرانية.

المطلب الأول

الأساس المنطقي لتطبيق قواعد القانون الدولي الساري على العمليات السيبرانية

حدّد البروتوكول الإضافي الأول لعام ١٩٧٧، والملحق باتفاقات جنيف لعام ١٩٤٩ في مادته رقم (١/٤٩) معنى "الهجمات"، باعتبارها أعمال عنف ضد الخصم، سواء كانت هجومية أم دفاعية، تتم خلال نزاع مسلح، والذي إما أن يكون دوليًا، وينصرف معناه إلى النزاع بين دولتين أو أكثر باستخدام قوات

---

(١) **قضت المادة رقم (٤/٢) من ميثاق الأمم المتحدة بأنه:** "يمتنع جميع الأعضاء في علاقاتهم الدولية، عن التهديد أو استخدام القوة، ضد السلامة الإقليمية أو الاستقلال السياسي لأية دولة، أو بأي طريقة أخرى تتعارض مع مقاصد الأمم المتحدة". وتضمن الميثاق استثناءين لهذا الحظر، وهما استخدامها بإذن من مجلس الأمن وفقًا للمادة رقم (٤٢) منه، والدفاع عن النفس وفقًا للمادة رقم (٥١) منه.

(2) ***N. MELZER,*** *International Humanitarian Law: A Comprehensive Introduction, ICRC, Geneva, 2016, P. 17.*

(3) ***T. RID****, Cyber War Will Not Take Place, 35 Journal of Strategic Studies 5, 2012, P. 15.*

مسلحة، وبغض النظر عن طول مدة النزاع، أو عدد العمليات العدائية فيه[1]، وإما أن يكون غير دولي، عندما ينشب بين مجموعة مسلحة منظمة غير نظامية ودولة، أو بين جماعتين مسلحتين منظمتين أو أكثر، وتُرتكب فيه أعمالاً عدائية جسيمة، ويستثني من هذا الوصف حالات الاضطرابات والتوترات الداخلية، مثل أعمال الشغب، وأعمال العنف المنفصلة والمتفرقة، وغيرها من الأعمال ذات الطبيعة المماثلة"[2].

ونلاحظ أن تعريف النزاع المسلح الدولي يعتمد على وجود أعمال عنف، واستخدام قوة مسلحة بين الأطراف المتنازعة، وهي عناصر مادية ملموسة على أرض الواقع يمكن تبينها ورصدها، ومتابعة أثارها. كما يتطلب النزاع المسلح غير الدولي درجة معينة من الجسامة في استخدام القوة بحيث تُشكّل ما يمكن وصفه بالأعمال العدائية الجسيمة، وتُستثني الأعمال التي لا تكافئ هذا القدر من القوة المادية من نطاق تطبيق أحكامه، كأعمال الشغب، وأعمال العنف المنفصلة والمتفرقة.

ويثور التساؤل حول إمكان استيفاء العمليات السيبرانية لمعيار وجود أعمال عنف، أو كونها ترقي إلى درجة استخدام القوة المسلحة، وذلك حتى يُمكن القول بإمكان تطبيق القانون الدولي الساري عيها، وقد نوقشت هذه الإشكالية عند إعداد دليل "تالين"، وكان الاتجاه السائد بين أعضاء (*IGE*)، أن القانون الدولي الساري متماسك إلى حد بعيد، وينطوي على قيم منطقية وواقعية يمكن تطبيقها على العمليات السيبرانية، وتمت الإشارة إلى مصطلح الأسلحة الجديدة، الوارد في المادة (٣٦) من البروتوكول الإضافي الأول لعام ١٩٧٧، باعتبار أنه يمكن تطبيقه على العمليات السيبرانية.

ولدراسة هذه الإشكالية، فإن نقطة البداية تتمثل في تحليل أمرين؛ **الأول:** مدى انطباق مفهوم الأسلحة الجديدة الوارد في المادة (٣٦) من البروتوكول الإضافي الأول لعام ١٩٧٧، على العمليات السيبرانية، **ويتعلق الأمر الثاني** بتحديد ماهية القوة كعنصر أساسي في النزاعات المسلحة، ومدي توافرها في العمليات السيبرانية. **ونفرد الفرعين التاليين لبحث هذين الأمرين.**

الفرع الأول

مدى انطباق مفهوم "الأسلحة الجديدة" الوارد في المادة (٣٦)

من البروتوكول الإضافي الأول لعام ١٩٧٧، على العمليات السيبرانية

أوضحت المادة رقم (٣٦) من البروتوكول الإضافي الأول لعام ١٩٧٧ بعنوان "الأسلحة الجديدة"، أن واضعي هذه المعاهدة يتصورون تغييرات مستقبلية في وسائل وأساليب الحرب، وعليهم أن يتحققوا مما إذا كانت تلك التغييرات محظورة بمقتضى البروتوكول، أو بموجب قواعد القانون الدولي،

---

(١) **وفقًا لتعليقات اللجنة الدولية للصليب الأحمر،** فإنه يعني أي نزاع ينشأ بين دولتين وتتدخل فيه القوات المسلحة، بغض النظر عن طول مدة النزاع، أو عدد العمليات العدائية فيه، كما يشمل مفهومه أيضًا استخدام القوة المسلحة من قبل مجموعة مسلحة منظمة، من غير الدول ضد دولة، ما دامت تلك المجموعة تتصرف تحت السيطرة الشاملة والفعلية دولة أخرى. **راجع:**

Application of the Convention on the Prevention and Punishment of the Crime of Genocide *(Bosn. & Herz. v. Serb. & Montenegro.), 2007 I.C.J. 108, Para. 404 (Feb. 26);* ***Prosecutor v. Tadić, Case No. IT-94-1-I,*** *Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, Para. 70, Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995.*

(2) ***R. GEISS****, Cyber Warfare: Implications for Non-International Armed Conflicts, 89 INT'L L. STUD., 2013, P. 627.*

حيث نصت المادة على أنه: **"يلتزم أي طرف سام متعاقد، عند دراسة، أو تطوير، أو اقتناء سلاح جديد، أو أداة للحرب، أو إتباع أسلوب للحرب، بأن يتحقق مما إذا كان ذلك محظوراً في جميع الأحوال أو في بعضها بمقتضى هذا الملحق "البروتوكول"، أو أية قاعدة أخرى من قواعد القانون الدولي التي يلتزم بها الطرف السامي المتعاقد".**

ويمكن فهم نص المادة (٣٦) باعتبار أن التكنولوجيا المُستحدثة حالاً أو لاحقًا، تدخل ضمن نطاق تطبيق القانون الإنساني الساري، وإن لم يتم النص عليها بشكل مباشر، ولا مجال القول بأن هذا القانون لم يتناول مسألة استخدام تكنولوجيات حديثة في الحرب، أو أن تصميمه لا يغطي الوسائل المُتطورة للنزاعات المُسلَّحة، فهو مؤهل للتعامل مع إدراج أسلحة جديدة، مثل العمليات السيبرانية، والتي يُمكن تصنيفها كأسلحة جديدة، بغض النظر عن عدم وجودها وقت صياغة البرتوكول[١].

ويدعم الفهم السابق، أن "شرط مارتنز" الذي كُرِّس لأول مرة في ديباجة اتفاقية لاهاي لعام ١٨٩٩، ثم ورد في الفقرة السابعة من ديباجة اتفاقية لاهاي الرابعة لعام ١٩٠٧، وفي وقت لاحق تضمنته اتفاقيات جنيف لعام ١٩٤٩، بالإضافة إلى البروتوكولات الإضافية لعام ١٩٧٧، واتفاقية حظر أسلحة تقليدية معينة لعام ١٩٨٠؛ **قد نص على أنه:** "وإلى أن يحين استصدار مدونة كاملة لقوانين الحرب، ترى الأطراف السامية المتعاقدة من المناسب أن تعلن أنه في الحالات غير المشمولة بالأحكام التي اعتمدتها، يظل السكان المتحاربون تحت حماية وسلطان مبادئ قانون الأمم، كما وردت في التقاليد التي استقر عليها الحال بين الشعوب المتمدنة وقوانين الإنسانية ومقتضيات الضمير العام". ووفقاً لتعليقات اللجنة الدولية للصليب الأحمر؛ فإن شرط "مارتنز" ديناميكي بطبيعته، وقابل للتطبيق بغض النظر عن أنواع الأسلحة الحالية، أو ما قد يطرأ عليها من تطورات لاحقة أو تكنولوجية مُستحدثة[٢].

كما قرَّرت محكمة العدل الدولية، في رأيها الاستشاري بشأن الأسلحة النووية عام ١٩٩٦، أن المبادئ والقواعد الراسخة للقانون الإنساني تنطبق على جميع أشكال الحرب، وعلى جميع أنواع الأسلحة، سواء الموجودة في الماضي، أم التي في الحاضر أو ستوجد في المستقبل[٣]. أي أن قانون النزاع المسلح ينطبق على أي استخدام للقوة بغض النظر عن السلاح.

كما أكَّد فريق الخبراء الحكوميين الذي تم تشكيله برعاية الجمعية العامة للأمم المتحدة عام ٢٠١٥، لدراسة مدى قابلية المبادئ القانونية للتطبيق على ممارسات تكنولوجيا المعلومات؛ على أن المبادئ القانونية بما في ذلك الإنسانية، والضرورة، والتناسب، والتمييز، قابلة للتطبيق على تكنولوجيا المعلومات، وبالتالي، فإن القانون الدولي الإنساني يمكن أن يسري على الحرب السيبرانية، مع مراعاة الخصائص المميزة لهذا المجال[٤].

---

(١) **البروتوكول الإضافي لعام ١٩٧٧**، والملحق باتفاقيات جنيف لعام ١٩٤٩، والمتعلق بحماية ضحايا المنازعات المسلحة الدولية، دخل حيز التنفيذ ٧ ديسمبر ١٩٧٨.

(2) ***Y. SANDOZ, C. SWINARSKI, B. ZIMMERMANN (eds.),*** *ICRC Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, ICRC AP Commentary, Para. 39.*

(٣) **الرأي الاستشاري لمحكمة العدل الدولية بشأن مشروعية استخدام الأسلحة النووية عام ١٩٩٦**، الفقرة رقم (٨٦).

(4) ***Group of Government Experts Report,*** *Developments in the Field of Information and Telecommunications in the Context of International Security, 22 July 2015, UN General Assembly Doc. A/70/174.*

ونلاحظ أن الفهم السابق لشرط "مارتنز"، وما أقرته محكمة العدل الدولية بشأن تطبيقه، وتعليق اللجنة الدولية للصليب الأحمر عليه؛ يعكس اتجاهًا مرنًا، ربما يهدم الرؤية الخاصة بعدم تناول أنواع النزاعات الحديثة كالعمليات السيبرانية في القانون الدولي الإنساني، باعتبار أن هذا الشرط يُقدّم مبادئ عامة للسلوك في مجال النزاعات المسلحة، ويترك الحكم على أي مُستجدات قد تدخل ضمن إطار هذه المبادئ لوقت تحققها، وبمراعاة الظروف المتغيرة والتطورات، وبما يشمل ظهور وسائل وأساليب حديثة للحرب.

فالمبادئ تبقى ثابتة، ولكن تطبيقها العملي يختلف من وقت لآخر ووفقًا للأحوال التي يتم التطبيق فيها، حتى أن مفهوم القوة المسلحة كعنصر أساسي في النزاعات المسلحة قد تتغير طبيعتها، وربما لا تظل قاصرة على الشكل التقليدي أو الأعمال العسكرية المسلحة، وقد تنطبق على العمليات السيبرانية، وهو ما نقوم بدراسته من خلال الفرع التالي.

الفرع الثاني

مدى انطباق وصف القوة المسلحة على العمليات السيبرانية

أولاً: الموقف في إطار القانون الدولي الساري:

لما كان النزاع المسلح وضعًا يستوجب تطبيق القانون الدولي الإنساني، فإن فهم الفلسفة التي تأسَّس عليها هذا القانون، يقتضي ألا يقتصر ذلك النزاع على الحالات التي تُستخدم فيها القوة المادية، ويجب أن يتضمَّن أي هجوم يُشكّل عنفًا ضد الخصم، سواء كان ذلك في حالة الدفاع أو الهجوم، ولعل ذلك الفهم هو نفس المنطق، الذي جعل القانون الدولي يحظر الأسلحة البيولوجية والكيميائية، على الرغم من أنها ليست وسائل مادية للهجمات، بالمعنى الوارد في المادة (٤٩) من البرتوكول الإضافي الأول لعام ١٩٧٧[(١)]، علاوة على أن قواعد القانون الإنساني تهدف إلى حماية أشخاص وأماكن وأشياء، وغيرها مما هو محل للحماية، وقد يترتب على استبعاد الهجمات غير المادية بطبيعتها من نطاق تطبيقه إلى إحباط أو تقويض أهدافه.

كما سمح البروتوكولان الإضافيان لعام ١٩٧٧، والتعليقات عليهما ـ ضمنًا ـ بإمكان تفسير مفهوم النزاع المسلح بشكل موسّع، يتوافق مع الفلسفة التي تأسس عليها القانون الدولي الإنساني، وهي تحقق مقومات هذا النزاع بناءً على تقدير مدى توافر درجة معينة من جسامة **"الآثار الناتجة عنه"، لا الطبيعة المادية أو الحركية للهجمات**، وهو ما يمكن استنباطه من حُكم المادة رقم (٢/٥٢) من البرتوكول الإضافي الأول لعام ١٩٧٧[(٢)]، والتي اعتّدت بالآثار الناتجة أو درجة التدمير التي تسببها بعض الهجمات، باعتبارها تحقق ميزة عسكرية أكيدة، كالتدمير التام أو الجزئي أو الاستيلاء على الأعيان أو تعطيلها.

---

(١) **المادة (٤٩) تعريف الهجمات ومجال التطبيق: ١-** تعني "الهجمات" أعمال العنف الهجومية والدفاعية ضد الخصم. **٢-** ....، . **٣-** تسري أحكام هذا القسم على كل عملية حربية في البر كانت، أم في الجو أم في البحر قد تصيب السكان المدنيين أو الأفراد المدنيين أو الأعيان المدنية على البر. **وقد تم إبرام اتفاقية حظر استحداث وإنتاج وتكديس الأسلحة البكتريولوجية (البيولوجية)، والأسلحة السامة وتدميرها،** في ١٦ ديسمبر ١٩٧١، ودخلت حيز النفاذ في ٢٦ مارس ١٩٧٥؛ **وكذلك اتفاقية حظر استحداث، وإنتاج، وتخزين، واستعمال الأسلحة الكيميائية وتدمير تلك الأسلحة،** في ١٣ يناير ١٩٩٣، ودخلت حيز النفاذ في ٢٩ أبريل ١٩٩٧.

(٢) **نصت الفقرة (٢) من المادة (٥٢) على أنه:** "تُقصر الهجمات على الأهداف العسكرية فحسب، وتنحصر الأهداف العسكرية فيما يتعلق بالأعيان على تلك التي تسهم مساهمة فعالة في العمل العسكري، سواء كان ذلك بطبيعتها أم بموقعها أم

وحري بالذكر، أنه لا يوجد اتفاق فقهي بشأن تحديد مصطلح "العمليات العسكرية"، فاعتبرها البعض مرادفًا لمفهوم "الهجمات" المنصوص عليه في المادة (٤٩) من البروتوكول الإضافي الأول وبما يعني "أعمال العنف"[١]، وهو مفهوم يصعب تصور تطبيقه على العمليات السيبرانية، التي تبتعد في حد ذاتها وبطبيعتها عن كونها أعمال عنف، إلا أن محكمة العدل الدول الدولية، قد أرست مفهومًا مهمًا في قضية "نيكاراجوا" عام ١٩٨٦، وهو ضرورة التمييز بين أخطر أشكال استخدام القوة، وهي التي تشكل هجومًا مسلحًا، وبين الأشكال الأخرى الأقل خطورة"[٢]، بحيث يكون العامل الحاسم في تحديد كون الفعل يمثل استخدامًا للقوة، أو يكافئ الهجوم المسلّح هو نطاق العمليات وآثارها.

ويمكن فهم المعيار السابق، باعتبار أن "نطاق" و"شدة" و"جسامة الآثار" الناتجة عن استخدام القوة، هي المُحدّد لوصف الهجوم المُسلَّح، فإذا أُستخدمت "قوة" بدرجة معينة من الجسامة، وتمت على نطاق واسع، وخلَّفت خسائر في الأرواح، أو تدميرًا للممتلكات؛ فإننا نكون أمام هجوم مسلح، يدخل ضمن نطاق حكم المادة رقم (٢) المشتركة لاتفاقيات جنيف الأربع لعام ١٩٤٩، حتى وإن كانت تلك الآثار ناتجة عن عمليات الكترونية[٣]، كما لا يمكن تصنيف العمليات السيبرانية، التي لا ينتج عنها آثارًا جسيمة باعتبارها استخدامًا للقوة، كالعمليات التي تهدف إلى مجرد تقويض ثقة مواطنين في حكومتهم، وبالقياس على حُكم محكمة العدل الدولية في قضية "نيكاراجوا"، فيما تضمّنه من أن تمويل مقاتلين، وإن كان سلوكًا غير قانوني، إلا أنه لا يرقي إلى مستوى استخدام القوة؛ فإن "تمويل" شن هجمات إلكترونية، أو "إمداد" مجموعة متمردة ببرامج إلكترونية ضارة، وتدريب أعضائها على استخدامها، لا يمكن اعتباره بمثابة استخدامًا للقوة.

ويدعم الفهم السابق، ما ورد بقرار الجمعية العامة للأمم المتحدة رقم (٣٣١٤) بتاريخ ١٩٧٤/١٢/١٤ بشأن "تعريف العدوان"، حيث لم يقدِّم القرار تعريفًا محددًا للهجوم المسلح أو القوة المسلحة، ولكنه أورد في مادته رقم (٣/أ/ز) أمثلة على أعمال أو مواقف قد تصل إلى حد الهجوم المسلح، وكان من بينها المشاركة الكبيرة لدولة ما، في أنشطة غير النظاميين، والمرتزقة ضد دولة أخرى، وهذه المُشاركة ربما لا تعني أي عمل فعلي من أعمال الهجوم المسلح، ولكنها قد تتمثل في تقديم الدعم والمعونة والمساندة[٤].

بغايتها أم باستخدامها، والتي يحقق تدميرها التام أو الجزئي أو الاستيلاء عليها أو تعطيلها في الظروف السائدة حينذاك ميزة عسكرية أكيدة". **راجع كذلك:**

***M. N. SCHMITT**, Rewired Warfare: Rethinking the Law of Cyber Attack, 96 IRRC (893), 2014, P. 201.*

(1) ***D. TURNS,** Cyber War and the Concept of 'Attack' in International Humanitarian Law' in Dan Saxon (ed.) International Humanitarian Law and the Changing Technology of War, Brill, 2013, P. 217.*

(2) ***Military and Paramilitary Activities in and Against Nicaragua** (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, Para. 191, 195.*

(٣) **نصت المادة رقم (٢) المشتركة على أنه:** "علاوة على الأحكام التي تسري في وقت السلم، تنطبق هذه الاتفاقية في حالة الحرب المعلنة أو أي اشتباك مسلح آخر ينشب بين طرفين أو أكثر من الأطراف السامية المتعاقدة، حتى لو لم يعترف أحدها بحالة الحرب".

(٤) **ووفقًا للفقرة، تشمل أعمال العدوان: الغزو**، والقصف، والهجمات على القوات المسلحة لدولة ضحية أو الأساطيل البحرية، أو الجوية، والمشاركة الكبيرة من دولة في أنشطة غير نظاميين ومرتزقة ضد دولة أخرى. **راجع:**

***UN General Assembly,** Definition of Aggression, G.A. Res. 3314, U.N. GAOR, 29th Sess., U.N. Doc. A/RES/3314 (Dec. 14, 1974); **R. HEINSCH**, the Crime of Aggression after*

وتاريخيًا رفض واضعو ميثاق الأمم المتحدة عام ١٩٤٥ مُقترحًا بتضمين الإكراه الاقتصادي في معنى "الإكراه"[١]، كما رفضت الجمعية العامة للأمم المتحدة إدراج مفهوم الإكراه الاقتصادي في الإجراءات التي أدت إلى اعتماد إعلان مبادئ القانون الدولي المتعلقة بالعلاقات الودية بين الدول لعام ١٩٧٠[٢]، ونحت كثير من الدول في سياساتها الوطنية نهج الجمعية العامة للأمم المتحدة[٣]، وبالتالي فإن العمليات السيبرانية التي تهدف إلى إكراه دولة اقتصاديًا لن تعتبر استخدامًا للقوة.

ويُقرّر جانب أن الهجوم السيبراني يرقي لدرجة هجوم مسلح وفقًا لنتيجته الإجمالية، ومدي تأثيره على رفاهية الدولة الضحية، وبنيتها التحتية السياسية والاقتصادية والاجتماعية، وعندما يكون تأثير هذا الهجوم جسيمًا، فإنه يُعتبر هجومًا مسلحًا، وينشأ للدولة الضحية حق الرد عليه عسكريًا[٤].

كما تبنَّت بعض التشريعات والسياسات الوطنية، نهج "المسئولية الصارمة" لتقييم الهجمات السيبرانية، مثل "قانون حماية البنية التحتية الحيوية للولايات المتحدة الأمريكية" لعام ٢٠٠١، الذي قرّر أن أي عملية سيبرانية تُوجَّه ضد بنية تحتية أساسية للدولة[٥]، تُعتبر هجومًا مسلحًا، بحساب أن بعض هذه العمليات لها آثار يتعذر تداركها، كالوفيات أو الإصابات الخطيرة، أو إتلاف الممتلكات. كما اعتمدت الحكومة الهولندية عام ٢٠١١، تقريرًا بشأن العمليات السيبرانية، اعتبرت بموجبه أن ما يؤدي منها إلى تدمير، أو إلحاق ضرر جسيم، أو دائم، بالبنية التحتية الحيوية العسكرية أو المدنية، أو إعاقة الدولة عن أداء مهامها الأساسية، أو التسبب في ضرر اقتصادي جسيم ودائم، يُمكن اعتباره هجومًا مسلحًا، بالمعنى الوارد في القانون الدولي الإنساني[٦].

وترتيبًا على ما سبق، يمكن أن ترقى العمليات السيبرانية إلى كونها هجومًا مسلحًا ينظمه القانون الدولي الإنساني؛ إذا أمكن تقدير الأضرار الناتجة عنها، ووُجد أنها تكافئ وتماثل ما قد ينتج عن هجوم مسلَّح مادي، وعلى سبيل المثال؛ عندما يتسبب هجوم سيبراني في إغلاق شبكة وطنية لتوليد

Kampala: Success or Burden for the Future? Goettingen Journal of International Law 2 (2010), PP. 733-740.

(1) ***United Nations Conf.*** *Int'l Org., Docs. 2, 334, 609, 617(e)(4) (1945).*

(2) ***U.N. Special Comm. on Friendly Relations,*** *U.N. Doc. A/AC.125/SR.110-14 (1970).*

(٣) **وعلى سبيل المثال،** أورد تقرير صادر عن الحكومة الهولندية في ديسمبر ٢٠١١، أنه لا يمكن تعريف الضغط أو الإكراه الاقتصادي،على أنه استخدام للقوة بموجب الفقرة (٤) من المادة (٢) من ميثاق الأمم المتحدة. **راجع:**

December 2011 report endorsed by the Dutch government, *Advisory Council on Int'l Affairs and the Advisory Comm. on Issues of Pub. Int'l Law, Cyber Warfare 20 (No. 77, AIV/No.22, CAVV) (Dec. 2011).*

(4) ***M. HALBERSTAM****, Hacking Back: Re-evaluating the Legality of Retaliatory Cyber-attacks, the Geo. Wash. Int'l L. Rev. 46, 2013, PP. 212:216, 221:223;****G. KERSCHISCHNIG****, Cyber Threats and International Law, Eleven International Publishing, 2012, P. 294.*

(٥) **عرَّف القانون "البنية التحتية الحيوية" بأنها**: "النظم والأصول الحيوية الأمريكية، سواء كانت مادية أو افتراضية"، واعتبر أن تعطيلها أو تدميرها، سيكون له تأثير ضار على الأمن والمواطنين، والاقتصاد، والصحة العامة، والسلامة. وتم تعديل القانون عام ٢٠٠٩، فيما تضمنّه من تعريف البنية التحتية الحيوية، حيث فصَّل أنها تشمل، الأصول العامة والخاصة، بما في ذلك الخدمات المصرفية والمالية، وشبكات الكهرباء، ومصافي النفط والغاز، وخطوط الأنابيب، والمياه، والمرافق الصحية، والاتصالات. **راجع:**

S. R. STEVENS*, Internet War Crimes Tribunals and Security in an Interconnected World, Transnat'l L. & Contemp. Probs. 18, 2009, P. 676.*

(6) ***December 2011 report endorsed by the Dutch government,*** *P. R., P. 29.*

الطاقة، فإن هذا الفعل يكافئ الهجوم المسلح، لأنه قبل تطوير القدرات الالكترونية، لم يكن من الممكن إغلاق مثل هذه الشبكة إلا من خلال قصف عسكري، أو غيره من أشكال الهجوم المسلَّح المادي؛ وكذلك ما يتعلَّق باحتفاظ الحكومات بنسخ رقمية، لبيانات الدولة الأساسية، كتعداد السكان، والخدمات الاجتماعية، والتصويت في الانتخابات، والضرائب، وغيرها، ويُشكّل نسخ هذه البيانات، أو محوها، أو تعديلها، عائقًا أمام استمرار ممارسة الوظائف الحكومية، بصورة قد تفوق تدمير أجزاء أو بني تحتية مادية للحكومة.

ثانيًا: الموقف على ضوء دليل "تالين":

أوردت القاعدة رقم (٣٠) من "تالين ١"، أن الهجمات السيبرانية الوقائية أو الدفاعية، التي من المتوقع على نحو معقول، أن تتسبب في إصابة أو موت أشخاص، أو إتلاف أو تدمير أشياء، تُعد بمثابة هجوم مسلح. وهو تطبيق صريح لما قرَّرته محكمة العدل الدولية في قضية "نيكاراجوا" عام ١٩٨٦، من حيث الاعتداد بمعيار جسامة الآثار الناتجة عن العمليات السيبرانية عند إرادة تصنيفها، وقرَّرت غالبية أعضاء (*IGE*)، أن الأضرار الجسيمة التي حاقت بالمرافق النووية الإيرانية عام ٢٠١٠، نتيجة هجوم "*Stuxnet*"، تكافئ استخدام القوة المسلَّحة، ولم تكن لتحدث قبل تطوير القدرات السيبرانية، إلا نتيجة هجوم مسلح مادي، حيث أدت إلى تدمير "ألف" جهاز طرد مركزي، وجعلها غير صالحة للخدمة، مع اختفاء الفيروس المُستخدَم بمجرد تحقق الأضرار[١].

ثم ذهبت التعليقات على المادة (٣٠) من دليل "تالين ١" إلى ما هو أبعد مما سبق، حيث قرَّرت أن القاعدة لم تتطلَّب أي شروط بشأن درجة الإصابة، أو مقدار التلف، أو حجم الضرر، وكونه دائمًا أو مؤقتًا، ولذا يمكن اعتبار أن بعض العمليات السيبرانية تكافئ الهجوم المسلح، على الرغم من أن الأضرار الناتجة عنها لا تشمل الإصابات أو الوفاة، إلا أنها تؤثر على وظيفة مرافق حيوية وأساسية للدول أو تُعطلها، بحيث يصير المرفق غير قابل للاستخدام، أو على الأقل يلزمه إصلاحات جذرية ليعمل مرة أخرى، كتعطيل نظم إدارة شبكات توزيع الكهرباء، أو التلاعب بإحصائيات تخص الأمن القومي للدولة، أو التأثير على فعالية سير النقل الجوي الأرضي، أو التلاعب بتقديرات مُحصَلة نظام الضرائب الوطني[٢].

كما أوردت تلك التعليقات عدة عوامل إذا توافرت، تدعم اعتبار العمليات السيبرانية مكافئة لاستخدام القوة، وأبرزها "الخطورة"، و"طبيعة الهدف"، أو كونها تمهيدًا لاستخدام قوة عسكرية مادية، مع الإشارة إلى الثقل النسبي لعامل "الخطورة"، فكلما اتصفت العملية بالخطورة الجسيمة، كلما اقتربت من كونها استخدامًا للقوة، مثل العمليات التي تستهدف تُقوِّيض الوظائف الحكومية، أو المجتمعية، أو الاقتصادية[٣].

ومن العرض السابق يمكن القول بأن، القانون الدولي العام ينطوي على قيم واقعية، وبعض القواعد والمبادئ التي يمكن تطبيقها على تهديد العمليات السيبرانية، إذا أُعتبرت داخلة ضمن نطلق حكم المادة رقم (٣٦) من البرتوكول الإضافي الأول لعام ١٩٧٧، أو إذا كانت الآثار الناتجة عنها تكافئ الآثار

---

(1) ***Y. DINSTEIN***, *Cyber War and International Law, 89 INT'L L. STUD. 276, 2013, PP. 279:280.*

(2) ***W. H. BOOTHBY***, *Weapons and the Law of Armed Conflict, OUP, 2nd edn., 2016, P.238.*

(٣) **التعليق على المادة رقم (٣٨) من دليل تالين،** الفقرات (١٠٧: ١١٣).

الناتجة عن استخدام قوة مسلحة مادية، كالإصابات الجسيمة، والوفاة، ودمار الممتلكات، كما يمكن تطبيق تلك القواعد كذلك في حالات النزاع المسلح التي تعتمد في جزء منها على الهجمات السيبرانية جنبًا إلى جنب مع الأسلحة المادية، وقد طبَّق دليل "تالين" بإصداريه، منطق البروتوكولين الإضافيين لعام ١٩٧٧، وتعامل مع العمليات السيبرانية باعتبارها فئة جديدة من "السلاح"، تخضع لشروط القانون الإنساني الدولي والقيود الواردة به.

المطلب الثاني

تطبيق مبادئ ومفاهيم القانون الدولي الإنساني على العمليات السيبرانية

يُعد مبدأ التمييز أحد المبادئ الأساسية للقانون الدولي الإنساني[١]، ويقتضي أن تُميّز الأطراف المتحاربة في كل الأوقات بين المدنيين والعسكريين، وبين الأعيان المدنية والأهداف العسكرية، وأن تتجنب شن هجمات عشوائية، أو توجيه القوة إلا ضد الأهداف العسكرية، وكذلك مبادئ الضرورة العسكرية والتناسب، والتي تتطلب تحقيق توازن دقيق بين حافزين متناقضين، هما الضرورة العسكرية والاعتبارات الإنسانية، وكذلك مفهوم المشاركة المباشرة في الأعمال العدائية، بحيث يعتبر مقاتلاً كل من يشارك في الأعمال العدائية بشكل مباشر. ونوالي بحث مدى انطباق هذه المبادئ على العمليات السيبرانية، وذلك من خلال الفروع التالية.

الفرع الأول

إعمال مبدأ التمييز في مجال العمليات السيبرانية

نصت المادة (٤٨) من البروتوكول الإضافي الأول لعام ١٩٧٧ على مبدأ التمييز، وطالبت أطراف النزاع بالتمييز بين المدنيين والعسكريين في جميع الأوقات، وكذلك بين الأهداف المدنية والأهداف العسكرية[٢]، وحظرت مادتي البروتوكول الأول رقمي (٥١)، (٥٧) الهجوم الذي يُتوقع أن ينتج عنه خسائر عرضية أو إصابات في أرواح المدنيين، أو إلحاق أضرار بالأعيان المدنية، أو الجمع بينهما. وأكدت المادة رقم (٥٢) منه، على أن الأعيان المدنية لا تكون محلاً للهجوم، وتقتصر الهجمات على الأهداف العسكرية فحسب، وإذا ثار الشك حول تكريس عين مدنية، مثل دور العبادة، أو المنازل، أو المدارس، في تقديم مساهمة فعالة للعمل العسكري، فيُغلّب افتراض أنها لا تستخدم كذلك[٣].

وفي مجال العمليات السيبرانية، قرَّرت القاعدة رقم (٣١) من "تالين ١"، والقاعدة رقم (٩٣) من "تالين ٢"؛ تطبيق مبدأ التمييز على الهجمات السيبرانية خلال أي نزاع مسلح[٤]، كما حظرت القاعدة (٤٩) من "تالين ١"، والقاعدة (١٠٥) من "تالين ٢"، الهجمات العشوائية، ووسائل أو أساليب الحرب

---

(١) **الرأي الاستشاري لمحكمة العدل الدولية بشأن مشروعية استخدام الأسلحة النووية عام ١٩٩٦**، الفقرة ٧٨.

(٢) **نصت المادة (٤٨) من البرتوكول الإضافي الأول على أن:** "تعمل أطراف النزاع على التمييز بين السكان المدنيين والمقاتلين وبين الأعيان المدنية والأهداف العسكرية، ومن ثم توجه عملياتها ضد الأهداف العسكرية دون غيرها، وذلك من أجل تأمين احترام وحماية السكان المدنيين والأعيان المدنية".

(٣) **وأوردت الفقرة رقم (٢) من المادة (٥٢) من البرتوكول الإضافي الأول لعام ١٩٧٧**، معايير للتحقق من مدى توافر الطبيعة العسكرية لهدف ما، وهي: مساهمته الفعالة بطبيعته أو موقعه أو غرضه أو استخدامه في القوة العسكرية للخصم؛ وأن يكون تدميره أو الاستيلاء عليه أو تحييده يوفر أفضلية عسكرية محددة للمعتدي.

(4) ***Rule No. (93) Of the Tallinn Manual 2****: Distinction: The principle of distinction applies to cyber attacks.*

السيبرانية العشوائية بطبيعتها، والتي تكون كذلك إذا لم تكن: (أ) موجهة إلى هدف عسكري محدد، أو (ب) محدودة فيما يتعلَّق بآثارها على النحو الذي يقتضيه قانون النزاعات المسلحة[١]، ومن ذلك، عندما تستخدم دولة برامج ضارة، لاستهداف شبكة أنظمة عسكرية أجنبية محددة، إلا أنه وفقًا لطبيعة تلك البرامج، فإنه بمجرد إدخالها إلى الشبكة المُستهدفة، تنتقل وتنتشر في الشبكات المدنية بشكل عشوائي، وتتسبب في أضرار لأنظمة الكترونية مدنية، وفي هذه الحالة، لا يتوافق استخدام هذه البرامج مع مبدأ التمييز المنصوص عليه في القاعدتين السالفتين.

والمُلاحظ، أن الدليل لم يُوضّح، في التعليقات على القواعد المذكورة، كيفية تطبيق مبدأ التمييز، بالرغم من أن طبيعة العمليات السيبرانية قد لا تسمح بذلك، حيث يتم إطلاق الهجمات السيبرانية من خلال بنية تحتية الكترونية، لها طبيعة الاستخدام المزدوج، لأغراض عسكرية ومدنية على حد سواء، ولا يمكن فصل أحد الاستخدامين عن الآخر[٢]، وهو نفس الحال أيضًا بالنسبة للأهداف التي تُوجَّه إليها هذه الهجمات، حيث تتصل ببنية تحتية إلكترونية تستخدم لأغراض عسكرية ومدنية.

وعلي سبيل المثال، تتم الاتصالات العسكرية عبر كابلات ووسائط أخرى، تُستخدم أيضًا لتسيير حركة المرور المدنية، كما يعتمد توجيه الأسلحة، على البيانات التي يوفرها نظام تحديد المواقع عبر الأقمار الصناعية "*GPS*"، والذي يخدم أغراضًا مدنية مثل الملاحة، بل إن وسائل التواصل الاجتماعي مثل "*Facebook*"، "*Twitter*" قد تُستخدم على نطاق واسع لنقل معلومات عسكرية[٣]، وبالتالي يكون من الصعب التمييز بين ما هو مدني وما هو عسكري، عند شن هجمات أو حروب الكترونية، ومن المقبول في القانون الإنساني الدولي، أنه عندما يبدأ استخدام شيء مدني لأغراض عسكرية، فإنه يصير عرضة للهجوم كهدف عسكري بالتخصيص.

واستحدث "دليل تالين ١" في قاعدته رقم (٣٩)، و"تالين ٢" في القاعدة (١٠١) منه، حُكمًا ربما لا يتوافق مع ما ورد بالقاعدة (٣١) من "تالين ١"، بشأن تطبيق مبدأ التمييز على العمليات السيبرانية، حيث قرّرت القاعدتان، بأن جميع الأغراض والمرافق ذات الاستخدام المزدوج هي أهداف عسكرية دون شروط[٤]، وهنا تثور إشكالية التوفيق بين إعمال مبدأ التمييز بشأن الهجمات السيبرانية، وبين اعتبار كل المرافق المزدوجة أهدافًا عسكرية، مع الأخذ في الاعتبار، أن المرافق العسكرية للدول تعتمد على بني تحتية الكترونية تُستخدم لأغراض مدنية، لأنه من الصعب تمويل إنشاء وصيانة شبكات انترنت منفصلة للأغراض العسكرية فقط، لاسيما مع اتجاه الدول للحفاظ على قدراتها العسكرية مع خفض ميزانياتها[٥]،

---

(1) ***Rule No. (105) of the Tallinn Manual 2****: Indiscriminate means or methods it is prohibited to employ means or methods of cyber warfare that are indiscriminate by nature. Means or methods of cyber warfare are indiscriminate by nature when they cannot be: (a) directed at a specific military objective, or (b) limited in their effects as required by the law of armed conflict and consequently are of a nature to strike military objectives and civilians or civilian objects without distinction.*

(2) ***R. GEIB, H. LAHMANN,*** *Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space, 45 ISR. L. REV., 2012, P. 381.*

(3) ***N. LUBELL,*** *Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply? 89 INT'L L. STUD., 2013, P. 252.*

(4) ***Rule No. (101) of Tallinn Manual 2****: "Objects used for civilian and military purposes Cyber infrastructure used for both civilian and military purposes is a military objective*".

(٥) **التعليق على القاعدة رقم (٣١) من دليل تالين،** الفقرة رقم (٢).

وبالتالي، فإذا كان تطبيق مبدأ التمييز في النزاعات التقليدية ليس يسيرًا، فإنه في مجال العمليات السيبرانية معقدًا للغاية، باعتبار أن شبكة الإنترنت مترابطة، ويتم توجيه هذه العمليات من خلال بني تحتية تخدم أغراضًا مدنية أيضًا.

الفرع الثاني

مبدأي الضرورة العسكرية والتناسب في مجال العمليات السيبرانية

من أهم الأسس التي يستند عليها القانون الدولي الإنساني، تحقيق التوازن بين حافزين متناقضين، هما الضرورة العسكرية، والاعتبارات الإنسانية، وهذا هو جوهر مبدأ التناسب، الذي يسمح بشن هجمات على أهداف مشروعة تقتضيها الضرورة العسكرية، ولكن إلى الحد الذي تفوق فيها الأضرار الجانبية للهجوم، ما قد يتحقق من ميزات عسكرية متوقعة، فلا يجوز القيام بمثل هذه الهجمات العشوائية، وينبغي إلغائها أو تعليقها، وقد قرَّر البرتوكول الإضافي الأول لعام ١٩٧٧، هذا المبدأ في مادتيه رقمي (٥١/٥/ب)، (٥٧/٢/ب)[١].

وفي مجال الهجمات والحروب السيبرانية، حظرت القاعدة رقم (١١٣) من "تالين ٢"، الهجوم السيبراني الذي يُتوقع أن يتسبب في خسائر عرضية في أرواح المدنيين، أو إصابتهم، أو إلحاق أضرار بأعيان مدنية أو مزيج من تلك الأضرار، مما لا يتناسب مع الميزة العسكرية المتوقعة[٢]، **ويتطلب تطبيق هذا المبدأ من القادة العسكريين أن يتوخوا توجيه العداء، ضد أهداف عسكرية دون غيرها**، وأن يراعوا حكم المادتين (٥١/٥/ب)، (٥٧/٢/أ) من البرتوكول الإضافي الأول لعام ١٩٧٧، وفي نفس الوقت يُطلب من القادة كذلك ـ مع تقييم النتائج المباشرة للهجوم السيبراني ـ تقييم أي نتائج غير مباشرة قد تحدث، لاتخاذ قرار بشأن تنفيذ العملية أو إلغائها[٣].

وعلى سبيل المثال، من المرجح عند مهاجمة نظام التحكم في حركة النقل الجوي الحربي، أن يؤثر ذلك أيضًا على الطائرات المدنية، وبالتالي يجب إعمال مبدأ التناسب، من حيث مراعاة إمكان انتقال البرامج الضارة الموجهة ضد أهداف عسكرية، وبشكل غير مباشر إلى بنية تحتية إلكترونية مدنية لا علاقة لها بالهجمات[٤].

---

(١) **نصت المادة (٥١/٥/ب) من البرتوكول على أنه:** "تعتبر الأنواع التالية من الهجمات، من بين هجمات أخرى، بمثابة هجمات عشوائية: والهجوم الذي يمكن أن يتوقع منه أن يسبب خسارة في أرواح المدنيين أو إصابة بهم أو أضراراً بالأعيان المدنية، أو أن يحدث خلطاً من هذه الخسائر والأضرار، يفرط في تجاوز ما ينتظر أن يسفر عنه ذلك الهجوم من ميزة عسكرية ملموسة ومباشرة. **ونصت المادة (٥٧/٢/ب) على أنه:** "يلغى أو يعلق أي هجوم إذا تبين أن الهدف ليس هدفًا عسكريًا أو أنه مشمول بحماية خاصة أو أن الهجوم قد يتوقع منه أن يحدث خسائر في أرواح المدنيين أو إلحاق الإصابة بهم، أو الأضرار بالأعيان المدنية، أو أن يحدث خلطًا من هذه الخسائر والأضرار، وذلك بصفة عرضية، تفرط في تجاوز ما ينتظر أن يسفر عنه ذلك الهجوم من ميزة عسكرية ملموسة ومباشرة".

(2) ***Rule No. (113) of Tallinn Manual 2:*** *Proportionality: A cyber attack that may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated is prohibited.*

(3) ***Y. DINSTEIN****, the Conduct of Hostilities under the Law of International Armed Conflict, CUP, 3rd, edn., 2016, P. 9.*

(٤) **التعليقات على القاعدة (٣٩) من دليل "تالين"**، الفقرتين (٢، ٦)؛ **التعليقات على القاعدة (٥١) من دليل "تالين"**، الفقرة (٤).

ويتطلب إعمال مبدأ التناسب مراعاة الحيطة بشأن تقييم جدوى الهجمات السيبرانية، ومن ذلك، إنشاء القادة نظام للمعلومات عن الأهداف المحتملة وتقييمها، من حيث مساهمتها في تحقيق ميزة عسكرية من عدمه، واستخدام وسائل متطورة لتحديد هذه الأهداف بدقة أثناء العمليات، وربما يصعب إعمال المتطلبات السابقة أو الرقابة عليها، وذلك على الرغم من أن دليل "تالين ١" قد قرَّر في قواعد من (٥٣): (٥٥)، ونظيراتها من "تالين ٢"، من (٩٣): (١١٣)، تجنيب المدنيين الهجمات، وضرورة التحقق من الأهداف، والتأكيد على توجيه تحذيرات عند الهجوم، وإلغاء الهجوم أو تعليقه في حالة عدم استيفاء معايير التناسب؛ إلا أنه لم يُوضّح كيفية تفعيل ذلك، مع كون البنية التحتية الالكترونية ذات استخدام مشترك، إضافة إلي أن الالتزام بتوجيه تحذيرات عند الهجوم، يتنافي مع ما تعتمد عليه هذه العمليات من عنصر المفاجئة والسرعة، وكذلك الصعوبة البالغة أو استحالة تقييم الأخطار الجانبية، التي قد تحدث على إقليم دولة أخري نتيجة تخريب نظم الكترونية لها.

كما حظر "تالين ٢" في قاعدته رقم (١٠٤)، استخدام وسائل أو أساليب الحرب السيبرانية، التي وفقًا لطبيعتها قد تُسبّب إصابة أو معاناة غير لازمة لتحقيق الهدف من العملية[١]، وأوردت تعليقات فريق (*IEG*) أن هذه القاعدة لن تُنتهك إلا في حالات نادرة، **على سبيل المثال،** عند وجود مقاتل يعتمد في تنظيم ضربات قلبه، على جهاز يعمل بواسطة الإنترنت، وأثناء النزاع المسلح السيبراني، يكون من المشروع السيطرة على جهاز تنظيم ضربات قلبه، وإيقافه بغرض قتله أو جعله عاجزًا عن القتال، إلا أنه من غير المشروع، القيام بذلك بطريقة تُسبّب لهذا المقاتل ألمًا ومعاناة مفرطة، لا تخدم تحقيق الهدف العسكري للعملية، كأن يتم إيقاف قلبه، ثم إعادته عدة مرات قبل قتله، وهو سلوك من شأنه أن يدخل ضمن نطاق المعاملة القاسية أو اللاإنسانية[٢].

وقد استوحت المادة رقم (٥٩) من "تالين ١"، حكم المادة رقم (٥٨/أ، ب) من البرتوكول الإضافي الأول لعام ١٩٧٧، بشأن فرض التزامات سلبية على أطراف النزاع، باتخاذ الاحتياطات اللازمة لحماية المدنيين والأعيان المدنية[٣]، إلا أن القاعدة (٥٩)، لم تُفَصّل هذه الحماية، وإنما صاغتها بشكلٍ ضمنيٍ، فقضت بأن يلتزم أطراف النزاع باتخاذ جميع التدابير الممكنة، وحماية المدنيين الخاضعين لسيطرتهم من "الأخطار" التي يمكن أن تنشأ عن هجوم الكتروني[٤]، وفسَّرت أغلبية فريق الخبراء الدولي في تعليقاتهم على المادة، أن "الأخطار" التي قد تحيق بالمدنيين تعني الوفاة، أو الإصابة، أو إلحاق الأضرار بالأعيان المدنية، بينما أكدت أقلية من الفريق، على أن هذه الأخطار يجب أن تشمل ما قد يُسبب اضطرابًا كبيرًا في الحياة اليومية أيضًا[٥].

---

(1) ***Rule No. (104) of Tallinn Manual 2:*** *Superfluous injury or unnecessary suffering: It is prohibited to employ means or methods of cyber warfare that are of a nature to cause superfluous injury or unnecessary suffering.*

(٢) **مضمون حكم المادة (١) من اتفاقية مناهضة التعذيب، وغيره من ضروب المعاملة أو العقوبة القاسية أو اللاإنسانية أو المهينة لعام ١٩٨٤.**

(٣) **قضت المادة رقم (٥٨/أ، ب) من البرتوكول الإضافي الأول بعنوان "الاحتياطات ضد أثار الهجوم"** بأن تقوم أطراف النزاع، قدر المستطاع، بما يلي: (أ) السعي جاهدة إلى نقل ما تحت سيطرتها من السكان المدنيين والأفراد المدنيين والأعيان المدنية بعيدًا عن المناطق المجاورة للأهداف العسكرية، (ب) تجنب إقامة أهداف عسكرية داخل المناطق المكتظة بالسكان أو بالقرب منها.

(٤) **التعليق على القاعدة رقم (٥٩)** من دليل تالين، الفقرات (٤، ٨، ١٠).

(٥) **التعليق على القاعدة رقم (٥٩)** من دليل تالين، الفقرة (٩).

ومما سبق، نَتَبَيَّن أهمية اعتماد قواعد تفصيلية وصريحة، بشأن تفعيل مبادئ القانون الدولي الإنساني في مجال الهجمات السيبرانية، لأن القواعد السارية، لا تواكب طبيعة هذا التطور بكل تفاصيله، مع مراعاة توضيح كيفية تطبيق تلك المبادئ، لاسيما تخدم البنية التحتية السيبرانية المُستهدفة، أغراضًا مدنية وعسكرية على حد سواء، **ونوضح مدي الحاجة إلى ذلك من خلال المثالين التاليين:**

في عام ١٩٩٩، قام حلف (*NATO*) بقصف محطة تلفزيون مملوكة للدولة الصربية في "بلجراد"، مما أسفر عن وفاة ستة عشر مدنيًا، وقطع البث التلفزيوني لمدة ست ساعات، وبرر الحلف ذلك القصف، بأن المحطة جزء من شبكة عسكرية للقيادة والاتصالات، ومن ثم تُعد هدفًا عسكريًا مشروعًا[١]، وفي تقرير قدمته اللجنة المُشكَّلة من قبل المحكمة الجنائية الدولية ليوغوسلافيا السابقة (*ICTY*)، لمراجعة ذلك القصف، أُثيرت الشكوك حول التبرير الذي ساقه الحلف، إلا أن التقرير انتهي إلى التوصية بعدم جدوى التحقيق في الحادث[٢]، وأيًا ما كان الأمر، ومن منظور الإنسانية، فإن عدد القتلى المدنيين في ذلك القصف، يثير تساؤلات لا يمكن تجاهلها ويتطلب ضمانات جدية لعدم استهداف المدنيين.

وكذلك في عام ٢٠١٥، تعرَّضت شبكة التلفزيون الفرنسية "*TV5 Monde*"، إلى هجوم سيبراني، أدي إلى وقف البث في (١٢) قناة تابعة للشبكة لمدة عشر ساعات[٣]، ولم يُصنَّف أحد هذه العملية باعتبارها استخدامًا للقوة أو هجومًا مسلحًا، يستوجب تطبيق قواعد القانون الدولي الإنساني ومبادئ التمييز والتناسب، بالرغم من استهدافها لأنظمة مدنية، وربما ينتج عنها قتلي وإصابات وتدمير أعيان.

الفرع الثالث

العمليات السيبرانية ومفهوم المشاركة المباشرة في الأعمال العدائية

حظرت المادة رقم (٣/٥١) من البروتوكول الإضافي الأول لعام ١٩٧٧، تعريض المدنيين لهجمات، إلا إذا شاركوا مباشرة في الأعمال العدائية[٤]، فالأصل أنهم يتمتعون بحماية ما لم يشاركوا مباشرةً في القتال، وقد ظل تفسير ماهية "المشاركة المباشرة" محلاً للنقاش والاختلاف، مع كل الإسهامات التي قُدمت لتوضيحه، لاسيما "الدليل التفسيري" الذي أصدرته اللجنة الدولية للصليب الأحمر، في مايو من عام ٢٠٠٨، مُتضمنًا عشر توصيات مع التعليق عليها، تُوضّح مفهوم المشاركة المباشرة في النزاعات المسلحة الدولية وغير الدولية[٥].

---

(1) ***NATO***, ***Press Conference by NATO Spokesman***, *Jamie Shea and Colonel Konrad Freytag, SHAPE, 23 April 1999,* ***available at:*** *http://www.nato.int/kosovo/press/p990423l.htm. 2/9/2019.*

(2) ***ICTY***, *Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia, 14 June 2000,* ***available at:*** *http://www.icty.org/en/press/final- report-prosecutor committee-established-review-nato-bombing-campaign-against-federal. 7/5/2018.*

(3) ***G. CLULEY***, *TV5Monde Attack Proves Hacking Attribution Is Very Difficult, 10 June 2015, available at: https://www.grahamcluley.com/tv5monde-attack-hacking-attribution. 5/4/2018.*

(٤) **نصت المادة رقم (٣/٥١) على أنه:** "يتمتع الأشخاص المدنيون بالحماية التي يوفرها هذا القسم ما لم يقوموا بدور مباشر في الأعمال العدائية وعلى مدى الوقت الذي يقومون خلاله بهذا الدور".

(5) ***ICRC***, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law, Intl Rev Red Cross 90, 2009, Paras. 991, 995:996.*

وتحوز مناقشة المشاركة المباشرة للمدنيين في الأعمال العدائية أهمية في سياق العمليات السيبرانية؛ لأن منها ما يتم من قبل كيانات خاصة تستخدم أفرادًا مدنيين لإجرائها، وعند تصنيف تلك العمليات باعتبارها تكافئ الهجوم المسلح، يكون وضع هؤلاء الأفراد وبحسب الأصل أنهم مدنيون، وفقًا لنص المادة (٥٠) من البروتوكول الإضافي الأول لعام ١٩٧٧، وليسوا مقاتلين وفقًا للمادة (٤٣) من البرتوكول[١].

ويتطلب الأمر استيفاء تلك الكيانات الخاصة معايير مُحدَّدة ليتحقق وضع المقاتل للأفراد العاملين فيها، تشمل أن يكون لها هيكل تنظيمي، وأن تعمل تحت قيادة مسئولة، وتتميز بعلامة يمكن التعرف عليها عن بعد، وأن تحمل السلاح علانية، وتلتزم بقوانين الحرب وأعرافها، وفي حالة عدم استيفاء هذه الكيانات لتلك المعايير مع كونهم يشاركون مباشرةً في أعمال عدائية، فإنهم يفقدون الحماية المقررة لهم كمدنيين بموجب القانون الدولي، ويجوز استهدافهم واحتجازهم[٢].

وقد حدَّد الدليل التفسيري للجنة الدولية للصليب الأحمر لعام ٢٠٠٩، معايير ثلاثة، لاعتبار المدنيين مشاركين مباشرةً في نزاع مسلح، وكونهم عرضة لاستهدافهم بوصفهم مقاتلين، وهي:

المعيار الأول: عتبة أو حد الضرر: بمعني القيام بفعل يشكل جزءًا من سير العمليات العسكرية العدائية، بين الأطراف في نزاع مسلح، ولا يمكن فصله عن هذه العمليات، ويُتوقع وفقًا للمنطق المقبول أن يؤثر فيها، أو على القدرة العسكرية لأحد أطراف النزاع أو، بدلاً من ذلك، ينتج عنه درجة معينة من الضرر، كالموت أو الإصابة، أو تدمير الأشياء؛ **ويخص المعيار الثاني: السببية المباشرة:** وجود علاقة سببية مباشرة بين الفعل والضرر الناتج عنه. وقد بيَن التعليق على هذه التوصية، أنه يجب فهم علاقة السببية هذه، باعتبارها تعني وجوب أن يكون الضرر مباشرًا ويمكن إثباته في خطوة واحدة؛ **والمعيار الثالث هو: ترجيح العلاقة الحربية لصالح أحد أطراف النزاع:** ويتطلب أن يكون الهدف من الفعل، دعم أحد طرفي النزاع على حساب الآخر، كأن يؤدي إلى ضرر لطرف، ويكون من شأنه ترجيح موقفه على الطرف الآخر[٣].

ونلاحظ مدى صعوبة إثبات تحقّق المعايير المذكورة سلفًا، في مجال الهجوم السيبراني أو الحرب السيبرانية، **وعلي سبيل المثال، بالنسبة للمعيار الأول:** نجد أن الأنشطة التي يتكون منها هذا الهجوم ربما لا تلبي في كثير من الأحيان "حد الضرر"، الذي يؤثر سلبًا على العمليات أو القدرات العسكرية لطرف

---

(١) **قضت المادة رقم (٥٠) من البرتوكول الإضافي الأول بأنه** المدني هو أي شخص لا ينتمي إلى فئة المقاتلين، وإذا ثار الشك حول ما إذا كان الشخص مدنياً أم لا فإنه يعد مدنيًا، ولا يجرد المدنيون من صفتهم وجود أفراد بينهم لا يسري عليهم تعريف المدنيين. **وقضت المادة (٤٣) منه بأن،** القوات المسلحة لطرف النزاع "المقاتلين"، تتكون من كافة القوات المسلحة والمجموعات والوحدات النظامية التي تكون تحت قيادة مسئولة عن سلوك مرؤوسيها، والتي تخضع لنظام داخلي يكفل إتباع قواعد القانون الدولي على النزاع المسلح، ويعد أفراد القوات المسلحة لطرف النزاع عدا أفراد الخدمات الطبية والوعاظ مقاتلين.

(2) ***N. MELZER**, Keeping the Balance between Military Necessity and Humanity: A Response to Four Critiques of the ICRC's Interpretive Guidance on the Notion of Direct Participation in Hostilities, Int'l L. & Pol. 42, 2010, P. 831.*

(٣) **يُعد من قبيل المشاركة المباشرة في العداء،** حراسة منشأة عسكرية، ونقل الأسلحة، وجمع المعلومات الاستخبارية، والإمداد بالمعدات العسكرية، وتحديد مواقع الأسلحة والمعدات للطرف الأخر. **راجع:**

***A. FAITE,** Involvement of Private Contractors in Armed Conflict: Implications under International Humanitarian Law, Defense Studies 166, vol. 4, Issue: 2, 2004, P.170.*

في النزاع، **وفي حالة تسبب الهجوم السيبراني** في وفيات أو إصابات، أو تدمير، أو الإضرار بالأمن العام، أو الصحة العامة، أو الاقتصاد، مع كونها لا تؤثر سلبًا على القدرات العسكرية لأحد أطراف النزاع، فإنها لا تستوفي درجة الضرر المطلوب لتأهل المدنيين كمشاركين بشكل مباشر في العمليات العدائية.

ويتطلب معيار "السببية المباشرة"، أن يكون التأثير أو الضرر قد نتج مباشرة عن الفعل، فلا يُعتَّد بالأفعال التي ينقطع فيها التسلسل السببي(١)، وفي سياق الهجمات السيبرانية لا يمكن التحقق من هذا الأمر، بسبب سلسلة الخطوات التي تتم من خلالها الهجمات، حتى تُحدث أثرها المباشر، أو درجة الضرر المُتطلبة بموجب المعيار الأول، علاوة على أن الحرب السيبرانية نشاط متخصص، تحرص جيوش العالم على دمجه في عملياتها وتشكيلاتها العسكرية الشاملة، وربما يزيد ذلك من صعوبة تحديد وضع الأفراد القائمين عليه(٢).

وكانت "السويد" من الدول التي تعاملت، مع صعوبات تحديد وضع أفراد الكيانات الخاصة في العمليات السيبرانية، التي قد ترقي إلى نزاعات مُسلَّحة، حيث قرَّرت أنه عند الاستعانة بمصادر خاصة خارجية للتجسس السيبراني، فإنها تخضع للإشراف من قبل جهاز مخابرات الإشارات، ويُحظر على هذه المصادر جمع أي معلومات استخباراتية يمنع القانون السويدي، جهاز المخابرات نفسه من جمعها، ووفقًا للمتحدث الرسمي باسم المؤسسة، لا توجد لائحة محددة لهذا الحظر، ولكن المؤسسة تضع معاييرًا داخلية لمتطلبات وحدود جمع المعلومات الاستخبارية، إضافة إلى الرقابة الصارمة على امتثالها من جانب جهاز الاستخبارات السويدي(٣).

ومن العرض السابق يمكننا استنباط ما يلي:

أولاً: على الرغم من أهمية التوجيه الذي أصدرته اللجنة الدولية للصليب الأحمر عام ٢٠٠٩، إلا أن المعايير التي أوردها لا يمكن إعمالها كقاعدة عامة، وإنما وفقًا لتقييم كل حالة على حدة، ومع ذلك لم يوضح التوجيه من الذي له سلطة الحكم على هذه الحالات، علاوة على أن تلك المعايير تحتمل التأويل والتباين في التفسير، وليست قاطعة في شأن تحديد ماهية المشاركة المباشرة في القتال، وبالتالي يصعب إعمالها في مجال الهجمات والحروب السيبرانية.

ثانيًا: على خلاف العسكريين المشاركين في عمليات العداء المسلح، ضمن نزاع مسلح مادي، وتحددهم بدقة لوائح لاهاي لعام ١٩٠٧ في مادتها الأولي، وكذلك اتفاقية جنيف الثالثة لعام ١٩٤٩، كجزء من القوات المسلحة لأحد أطراف النزاع؛ توجد صعوبة بالغة في تحديد مدى الانخراط والمشاركة المباشرة للأفراد عند شن عمليات سيبرانية، لاسيما المنتمين منهم إلى كيانات بخلاف الدول، ومن ذلك، صعوبة التعرف على هوياتهم، وأدوارهم في الهجوم، فمنهم من يشارك في تصميم البرامج الضارة، التي تُستخدم في الحرب السيبرانية الهجومية أو الدفاعية، ومنهم من يُثَّبت هذه البرامج على أجهزة الحاسب،

---

(1) ***ICRC,*** *Direct Participation in Hostilities, Interpretive Guidance, New York University Journal of International Law and Politics, vol. 42, 2010, PP. 641: 686.*

(2) ***M. N. SCHMITT****, Rewired Warfare, P. R., P. 190.*

(3) ***F. WALLIN, Spokesperson****, Swedish National Defence Radio Establishment, Försvarets radioanstalt, 23 October 2014 and Stockholm, Sweden 24 October 2014.*

ومنهم من يعمل على إدارة المواقع الالكترونية ذات الصلة، ومنهم من يوفر خدمات الصيانة الفنية، أو يتولي تشغيل البرامج التي تُفعِّل العمليات السيبرانية.

المطلب الثالث

حق الدفاع عن النفس في مواجهة العمليات السيبرانية

أقرَّت المادة رقم (٥١) من ميثاق الأمم المتحدة، استخدام الدول للقوة بغرض الدفاع عن نفسها ضد أي هجوم مسلح، ووفقًا لدليل "تالين" بإصداريه، فإن العمليات السيبرانية التي ينتج عنها أضرارًا أو إصابات جسيمة؛ تكافئ الهجوم المسلح، ويحق للدول استخدام حق الدفاع عن النفس في مواجهتها، وفيما يتعلَّق بالمبادرة بالدفاع الاستباقي أو الوقائي، في مواجهة الهجوم المسلح الذي يوصف بكونه "وشيكًا"، فقد اعتمد دليل "تالين" معيارًا لنشأة هذا الحق في مواجهة الهجوم السيبراني المرتقب، وأُطلق عليه معيار "الفرصة الأخيرة". **ونوالي دراسة هذا الموضوع من خلال الفروع التالية.**

الفرع الأول

حق الدفاع عن النفس ضد العمليات السيبرانية المُحقَّقَة

حظر ميثاق الأمم المتحدة في مادته رقم (٤/٢)، على جميع أعضاء المنظمة، استخدام القوة أو التهديد باستخدامها في العلاقات الدولية، ثم أورد الميثاق بعض الاستثناءات على هذا المبدأ، منها ما ورد بالمادة رقم (٥١) منه، بشأن حق الدول في الدفاع عن نفسها عند التعرض لهجوم مسلَّح، وتبنت محكمة العدل الدولية تفسيرا ضيقًا للمادة (٥١)، بالتأكيد على جواز حق الدفاع فقط في حالة الهجوم المسلح، من قبل دولة ضد دولة أخرى، وأوردت المحكمة في قضية "منصات النفط" عام ٢٠٠٣ أمثلة لهذا الهجوم، حيث اعتبرت أن استهداف منصة عسكرية، أو منشأة عسكرية قد يرقى إلى مستوى الهجوم المسلح[١].

وكانت محكمة العدل الدولية قد قرّرت في قضية "نيكاراجوا" عام ١٩٨٦، استبعاد ما وصفته بمجرد حادثة حدودية من نطاق الهجوم المسلح[٢]، كما أوضحت القاضية "*Rosalyn Higgins*"، في رأيها الانفرادي في قضية "الجدار العازل" التي نظرتها المحكمة عام ٢٠٠٤، أنها غير مقتنعة بأن عدم استخدام القوة، أو التدابير غير القسرية، كبناء جدار، يُمكن أن تقع ضمن نطاق الدفاع عن النفس بموجب المادة (٥١) من ميثاق الأمم المتحدة، حيث يجب لإعمال مضمون الحكم أن تواجه الدولة قوة مسلَّحة[٣].

وقد اعتمد دليل "تالين" بإصداريه (١، ٢) ما قررَّته محكمة العدل الدولية، بشأن اشتراط وجود قوة مسلَّحة، لنشوء الحق في الدفاع ضد العمليات السيبرانية، حيث تطلَّب الدليل أن ينتج عن هذه العمليات إصابات أو وفاة، أو أضرار جسيمة للممتلكات والأعيان، أما العمليات التي لا ينتج عنها مثل هذه الآثار، فلا يُمكن تصنيفها كهجوم مسلح، وبالتالي، لا يجوز استخدام حق الدفاع في مواجهتها، وذلك مثل عمليات نسخ معلومات، أو سرقتها، أو الحرمان من خدمات الكترونية غير أساسية.

---

(١) **حكم محكمة العدل الدولية في قضية (*Oil Platforms*)**، ٢٠٠٣، الفقرات (٥٧: ٦١).

(٢) **حكم محكمة العدل الدولية في قضية (*Nicaragua v. USA*)**، ٢٧ يونيو ١٩٨٦، الفقرة ١٩٥.

(3) ***Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory***, *Advisory Opinion, 2004, ICJ Rep 136, para. 35, Separate Opinion of Judge Higgins.*

ولعل الاستناد إلى معيار درجة الخطورة، لتصنيف العمليات السيبرانية كهجوم مسلح، يثير إشكالية تتعلق بكيفية تقدير أو تقييم هذه الخطورة، إلا أنه يُمكن الاعتماد على تقييم مدى تأثير العملية على الدولة المضرورة، وعلى سبيل المثال، عند تعطيل أو إعاقة مؤسسات الدولة عن أداء وظائفها، وحدوث أضرار يتعذر تداركها، كتخريب الأجهزة التي تعتمد عليها مُنشآت طبية، مما ينتج عنه وفيات، فإن مثل هذه العمليات تكافئ استخدام للقوة، ويكون للدول حق الرد عليها بموجب المادة (٥١) من الميثاق[١].

وعلى المستوى الوطني، تبنت بعض الدول معيار درجة الخطورة، لتصنيف العمليات السيبرانية، وما إذا كانت تكافئ الهجوم المسلَّح، وتتأهل للرد عليها وفقًا للمادة (٥١) من ميثاق الأم المتحدة، ومنها الولايات المتحدة الأمريكية، التي أكدت في تقرير قدمته إلى الأمم المتحدة عام ٢٠١١، أنه في بعض الظروف تُشكِّل الأنشطة التخريبية في الفضاء السيبراني هجومًا مسلحًا، ويكون من الملائم ألا يقتصر الرد عليها بشن هجوم إلكتروني مضاد فحسب، وإنما يتطلب أيضًا هجومًا بالوسائل العسكرية التقليدية[٢]، إلا أن التقرير لم يُحدّد ماهية الأنشطة التخريبية أو أنواعها، وفي عام ٢٠١٢، ضمَّنت الولايات المتحدة الأمريكية في إستراتيجيتها بشأن الفضاء السيبراني، أنها ستقوم بالرد على أي أعمال عدائية تتم في الفضاء السيبراني، بموجب حقها في الدفاع عن النفس، دون النظر لممارسات الدول الأخرى بهذا الشأن[٣].

كما اعتمدت الولايات المتحدة الأمريكية عام ٢٠١٧، تفسيرًا مُوسّعًا لحق الدفاع عن النفس في مواجهة التهديدات السيبرانية، وذلك بموجب الأمر الرئاسي الصادر في الحادي عشر من مايو لنفس العام، بعنوان "تعزيز الأمن السيبراني للشبكات الفيدرالية والبنية التحتية الحيوية " *"Strengthening the Cyber security of Federal Networks and Critical Infrastructure*"، والذي سمح بالقيام بعمليات عبر الحدود، في حالة وجود دولة غير راغبة، أو غير قادرة على تنفيذ التزاماتها الدولية، المتعلقة بعدم استخدام أراضيها للإضرار بالدول الأخرى بطرق سيبرانية، وبما يشمل شن هجمات سيبرانية، ضد الدول التي قد يتم استخدام أقاليمها كمصدر للهجمات، مع افتقارها إلى التقنيات اللازمة للكشف عن هذه الهجمات و/أو اتخاذ تدابير لوقفها، أو عدم وجود فرصة للتشاور بشأنها، نظرًا لسرعتها الفائقة[٤].

وتُبرّر الولايات المتحدة الأمريكية سياستها السيبرانية، بأنها رد فعل للهجمات التي استهدفتها، ومن أخطرها، هجمات "*Moonlight Maze*"، في أواخر التسعينيات، التي وصفتها الإدارة الأمريكية بأنها تُماثل عمليات الاستطلاع التي تسبق الحرب، حيث نتج عنها سرقة معلومات تخص وزارة الطاقة،

---

(1) ***N. TSAGOURIAS***, *Cyber Attacks, Self-defence and the Problem of Attribution, J. Conflict & Sec L. Vol. 17, No 2, 2012, PP. 229:244.*

(2)***United Nation,*** *General Assembly, Developments in the field of information and telecommunications in the context of international security, Report, Sixty-sixth session, 15 July 2011, (UN Doc. A/66/152).*

(3) ***U.S., The White House***, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, 2011, P. 9.*

(4) ***The White House, Fact Sheet: U.S.*** *Policy Standards and Procedures for the Use of Force in Counterterrorism Operations Outside the United States,* ***available at****: http://www.whitehouse.gov/the-press-office/2013/05/23/fact-sheet-uspolicystandards-and-procedures-use-force-counterterrorism. 5/12/2019.*

ووكالة "*NASA*"، ومتعاقدين مع الجيش الأمريكي، وبعض المشروعات البحثية للجامعات[١]. وفي عام ٢٠١٥، تمكّن مهاجمين "روس"، من اختراق البريد الالكتروني للبيت الأبيض، والإطلاع على المراسلات مع الدبلوماسيين ومسئولي وزارة الخارجية، وكذلك اختراق شبكة للبنتاجون، وهيئة الأركان المشتركة[٢].

وفي فبراير من عام ٢٠١٧، قدَّم القطاع الخاص الأمريكي، مُمثَّلاً في شركة "مايكروسوفت"، اقتراحًا لإبرام ما أطلق عليه "اتفاقية جنيف الرقمية"، حيث أعلن "براد سميث" رئيس الشركة، أن اتفاقية جنيف الرابعة لعام ١٩٤٩، قد نظَّمت حماية المدنيين في أوقات الحرب، ويحتاج العالم اليوم إلى صياغة "اتفاقية جنيف الرقمية"، التي تضطلع بحماية الحكومات والمدنيين، من العمليات السيبرانية في أوقات السلم، ومثلما اعترفت اتفاقية جنيف الرابعة، بأن حماية المدنيين تتطلب مشاركة فعالة من الهيئة الدولية للصليب الأحمر، فإن الحماية من العمليات السيبرانية تتطلب مساهمة فاعلة من شركات التكنولوجيا، التي تمثل قطاعًا كبيرًا، ينبغي أن يلتزم بالعمل الجماعي، لجعل الإنترنت بيئة أكثر أمانًا[٣].

وفي "هولندا"، أصدر المجلس الاستشاري للشئون الدولية، بالتعاون مع اللجنة الاستشارية المعنية بقضايا القانون الدولي، تقريرًا عام ٢٠١١، بأن الأفعال التي تؤدي إلى الوفاة، أو الإصابة الجسيمة، أو تدمير أشياء، تكافئ الهجوم المسلح، ويُمكن تصور العمليات السيبرانية باعتبارها هجومًا مسلحًا، وإعمال حكم المادة (٥١) من ميثاق الأمم المتحدة في مواجهتها؛ إذا كان يمكن، أو أدت بالفعل، إلى تعطيل في أداء الدولة، أو نتج عنها آثار تهدد استقرار الدولة[٤]. ويتطلَّب ذلك النهج وقوع اضطراب في الدولة نتيجة عملية سيبرانية، أو محاولة ذلك ، كأن يتم منع حكومة من أداء مهامها، أو تعطيل شبكة اتصالات عسكرية، أو الحيلولة دون تنظيم أو نشر قوات مسلحة؛ في حين لا يُمثَّل تعطيل بعض الخدمات الالكترونية، كالمعاملات المصرفية، هجومًا مسلحًا.

وحري بالذكر، أنه عند شن كيانات بخلاف الدول، عمليات سيبرانية تستهدف تقويض بني تحتية رئيسة للدول، فإنه وفقًا للقواعد الدولية، لا يُمكن إعمال تدابير الدفاع وفقًا للمادة (٥١) من الميثاق في مواجهتها، حتى عندما تكافئ آثارها درجة الهجوم المسلح، لأن هذه الكيانات ليست من أشخاص القانون الدولي، وليست طرفًا في الاتفاقيات الدولية[٥]، وقد أكدت محكمة العدل الدولية على هذا المعني، في قضية الجدار العازل عام ٢٠٠٤، ردًا على ما قرّرته "إسرائيل"، من أن بناء هذا الجدار الأمني، يحميها من الهجمات الإرهابية، وأنه عمل قانوني وفقًا لحقها في الدفاع عن النفس بموجب المادة (٥١) من ميثاق

---

(1) ***A. J. SCHAAP***, *Cyber Warfare Operations, P. R., P. 141.*

(2) ***J. FISHEL, L. FERRAN***, *State Dept. Shuts Down Email After Cyber Attack, ABC NEWS (Mar. 13, 2015),* ***available at:*** *http://abcnews.go.com/US/state-dept-shutsemail-cyber attack/story?id=29624866. 25/1/2020.*

(3) ***B. SMITH***, *President of Microsoft: the need for a Digital Geneva Convention, RCA Conference, San Francisco, February 2017, https://blogs.microsoft.com. 11/10/2019.*

(4) ***AIV/CAVV Report,*** *Government's response to the AIV's advisory report, the internet, a global free space with limited state control, and the WRR's advisory report, the public core of the internet: an international agenda for internet governance, AVT16/BZ119746, 2011, P. 21.*

(5) ***A. S. DEEKS***, *Unwilling or Unable: Toward a Normative Framework for Extraterritorial Self-Defense, 52 VA. J. INT'L L., 2012, P. 483.*

الأمم المتحدة، حيث لم تتعرَّض المحكمة لما إذا كانت المادة تنطبق على الأفعال غير القسرية كبناء جدار، ولكنها رفضت تطبيقها في هذه الحالة، على أساس أن أعمال العنف التي تدعي "اسرائيل" بتعرضها لها، لا تُعزى إلى دولة، وإنما إلى جهات فاعلة، متواجدة داخل أراضي خاضعة لسيطرتها[1].

ومن العرض السابق يمكننا ملاحظة الآتي:

أولاً: يكون معيار درجة الخطورة وجسامة الآثار منطقيًا، عند تقدير توافر حالة الدفاع عن النفس ضد العمليات السيبرانية، ولكن بالنسبة للدول التي تمتلك إمكانات الكترونية متقدمة، بحيث تكون قادرة على تقييم تلك العمليات، وتقدير مدى خطورتها وجسامة أثارها، والرد في مواجهتها، بقوة سيبرانية مضادة، وهو أفضل خيار قانوني لمواجهة تلك العمليات، أما الدول التي لا تملك مؤهلات سيبرانية على نفس القدر من التطور، فإنه يصعب عليها إعمال هذا المعيار

ثانيًا: اللجوء إلى استخدام أسلحة مادية كرد على عملية سيبرانية، ربما لا يتوافق مع مبدأ التناسب، ولا يكون فاعلاً بشأن إنهاء العملية وتلافي أثارها.

ثالثًا: تواجه التدابير الخاصة بالدفاع عن النفس ضد العمليات السيبرانية صعوبات، بشأن تطبيق قواعد القانون الدولي الإنساني، حيث يصعب فنيًا تتبع مصدر هذه العمليات، لأنها تتم من خلال عدة مراحل، قد تقع كل منها في دولة مختلفة، مع طول الفترة الزمنية المُتطلبة لهذا التتبع، وفي النهاية، قد ينطوي تحديد ذلك المصدر أو هوية المهاجم على قدر من الخطأ، ومن المؤكد أن أي إجراء دفاعي خاطئ يتم اتخاذه ضد نظام وسيط، يمثل مخالفة لمبدأ التمييز، في حين أنه إذا كان التتبع ناجحًا، ينبغي تحديد الأنظمة المهاجمة بشكل دقيق، وتمييز المدني منها والعسكري، ثم البدء في اتخاذ إجراءات دفاعية مستنيرة ومحددة للتعامل مع العملية.

ثالثًا: ربما يكون من الأفضل عند توافر شروط الدفاع وفقًا للمادة (٥١) من الميثاق، في مواجهة العمليات السيبرانية، عدم التفرقة بين جهات شن هذه العمليات، وسواء كان المهاجم دولة، أو جهة فاعلة تابعة، أو غير تابعة لدولة[2]، لأن طبيعة تلك العمليات تستوجب الرد إلكترونيًا وبسرعة متناهية، ولا تحتمل الانتظار لتمييز الجهة المُهاجمة، وإلا فإن الأضرار تتفاقم، وقد تؤدي لتقويض بعض أنظمة الدولة، مع فقد الدولة ميزة الاستجابة والرد الفاعل في الوقت المناسب.

الفرع الثاني

الدفاع الوقائي عن النفس في مجال العمليات السيبرانية المُحتَمَلة

على الرغم من عدم الاتفاق على امتداد حق الدفاع، الوارد في المادة رقم (٥١) من ميثاق الأمم المتحدة ليشمل الهجمات المحتملة، إلا أن هناك جانب فقهي يدعم هذا المفهوم، كحق للدول في مواجهة الهجوم المسلح الذي يوصف بكونه "وشيكًا" أو "فوريًا"، على الرغم من أن آثاره الجسيمة لم تظهر

(1) ***Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory***, *Advisory Opinion, 2004, ICJ Rep 136, para. 95.*
(2) ***D. BETHLEHEM****, Self-Defense against an Imminent or Actual Armed Attack by Nonstate Actors, 106 AJIL, 2012, P. 770.*

بعد[١]، كما أوضح تقرير للأمين العام للأمم المتحدة، بعنوان "الحرية الأكبر" " *In Larger Freedom*"، أن التهديدات الوشيكة مشمولة بموجب المادة (٥١) من الميثاق، والتي صيغت لحماية الحق الأصيل للدول ذات السيادة، في الدفاع عن نفسها ضد هجوم مسلح، وبما يشمل الهجمات الوشيكة بالإضافة إلى الهجمات التي تقع بالفعل[٢].

وقد تم تداول وصف الهجوم بكونه "وشيكًا" أو "فوريًا" لأول مرة، في المذكرات الدبلوماسية المتبادلة بين "الولايات المتحدة الأمريكية" و"بريطانيا العظمى"، أثناء حادث "كارولين" في القرن التاسع عشر، عندما أعلن وزير الخارجية الأمريكي "دانيال ويبستر"، أن حق الدفاع عن النفس لا ينطبق، إلا عندما تكون هناك ضرورة فورية له، لا تترك أي خيار لوسائل أخري، ولا تترك لحظات للتداول[٣].

ودام بعد ذلك اشتراط هذا الوصف في الهجوم، كمُتطلّب لتقدير إجراءات الدفاع الوقائي في مواجهته[٤]، وهو وصف زمني، يُشير إلى عدم قدرة الدولة على تفادي خطر محدق ووشيك، إلا من خلال المبادرة بالهجوم على مصدر التهديد، وأن هذا الاستباق هو السبيل الوحيد لدرء الخطر، وكانت الولايات المتحدة الأمريكية من أوائل الدول، التي أشارت إلى هذا المضمون، في إستراتيجيتها للأمن القومي عقب هجمات سبتمبر ٢٠٠٢، حيث أوردت أن الدول المارقة والإرهابيين، يسعون إلى مهاجمتنا باستخدام وسائل غير تقليدية، وأسلحة دمار شامل، ويتطلَّب الحفاظ على قيمة ومضمون حق الدفاع عن النفس، أن يتكيف مع تلك البيئة الأمنية المتغيرة[٥].

وبشأن الهجمات الاستباقية في مجال الفضاء السيبراني، فقد قرّرت القاعدة رقم (٢٦) من "تالين ٢" بعنوان "الضرورة"، أنه يجوز للدولة أن تتصرف بناءً على متطلبات الضرورة، للرد على تهديدات تنطوي على خطر وشيك، سواء كانت ذات طبيعة إلكترونية أم لا، وذلك لغرض حماية مصلحة أساسية، وباعتبار أن هذا التصرف هي الوسيلة الوحيدة لحماية هذه المصلحة، أو أن استباق الهجوم يمثل آخر فرصة للدولة لاتخاذ تدابير دفاعية فعالة[٦]، الأمر الذي يتطلَّب شروط ثلاثة: **أولاً؛** وجود مؤشرات جدية على أن عملية سيبرانية محتملة وشيكة ستنطلق ضد الدولة؛ **وثانيًا:** مكافئة الآثار المُحتملة للعملية لآثار

---

(1) ***T. D. GILL, P. A. DUCHEINE****, Anticipatory Self-Defense in the Cyber Context, 89 INT'L L. STUD., 2013, P. 438;* ***C. FOCARELLI****, Self-Defence in Cyberspace, in: N. Tsagourias, R. Buchan (eds), Research Handbook on International Law and Cyberspace, Cheltenham, Edward Elgar, 2015, P. 271.*

(2) ***Report of the Secretary-General****, In Larger Freedom: Towards Development, Security and Human Rights for All, UN Doc A/59/2005, 21 March 2005, para. 124.*

(3) ***Letter from Daniel Webster to Lord Ash Burton (Aug. 6, 1842)****, in 2 International Law Digest, 412, John Bassett Moore ed., 1906.*

(4) ***Y. DINSTEIN****, War, Aggression and Self-Defence, 5th. edn., Cambridge University Press, Cambridge, 2011, P. 88.*

(5) ***The White House,*** *National Security Strategy of the United States, 15 (Sept. 2002).*

(6) ***Rule (26) of Tallinn Manual: Necessity:*** *A State may act pursuant to the plea of necessity in response to acts that present a grave and imminent peril, whether cyber in nature or not, to an essential interest when doing so is the sole means of safeguarding it.*

الهجوم المسلح؛ **وثالثًا:** أن تكون المبادرة بالهجوم تُمثّل آخر فرصة لدي الدولة للدفاع، وإذا لم تغتنمها فلن تتمكن من درء الخطر[1].

وبالأخذ في الاعتبار أن سرعة العمليات السيبرانية الموجهة ضد دولة، قد تُجبرها على المبادرة بالرد، عند مجرد ترجيح احتمال وقوع الهجوم، وعدم الانتظار حتى يقع فعليًا؛ فقد اعتمد الدليل معيارًا لنشأة حق المبادرة في الدفاع ضد العمليات السيبرانية، أُطلق عليه "نافذة الفرصة الأخيرة"، أو "*Last Window of Opportunity*"، وباعتبار أن الخطر يكون وشيكًا، عندما تكون نافذة الفرصة لاتخاذ إجراء منعه على وشك الإغلاق، كأن يتوافر لدولة معلومات مُوَّثقة، بأن بعض الكيانات الخاصة سوف تستهدف بنيتها التحتية بعمليات سيبرانية في تاريخ مُحدّد، بغرض تدميرها أو تعطيلها، فإنه وفقًا للمعيار المذكور، يجوز للدولة أن تتخذ إجراءًا استباقيًا ضد هذه الكيانات، لأن عدم القيام بذلك يُمثّل مخاطرة فقدان فرصة منع تلك العمليات بشكل فعال[2].

ويمكننا القول بأن طبيعة العمليات السيبرانية، قد تُحفّز الدول وتزيد من دوافعها بشأن قبول نهج "الفرصة الأخيرة"، بشأن تلك العمليات، بالنظر إلى طبيعتها السرية، والمفاجئة، والفورية، والتي يصعب تحديد مصدرها، أو نسبتها إلى جهة معينة بشكل مؤكد في وقت مناسب، علاوة على أنها يمكن أن تؤدي إلى عواقب يتعذر تدارك آثارها، وعلى ضوء ذلك، يكون الالتزام الصارم بالمعيار الزمني غير منطقي، لأنه الوقت بين اتخاذ قرار إجراء هجوم عبر الإنترنت، وتنفيذه، وتحقق عواقبه يمكن قياسه "بالملي ثانية"، فإذا كان للحق في الدفاع عن النفس أي مضمون، فيجب أن تكون الدولة قادرة على التصرف لتفادي مثل هذا الهجوم، بمجرد علمها بأنه على وشك التنفيذ، وأنها إذا ترددت في الاستجابة، فإنها تخاطر بفقدان فرصة الدفاع عن نفسها بفعالية.

الفرع الثالث

الدفاع عن النفس في مواجهة العمليات السيبرانية المُوجَّهة من الكيانات الخاصة

وفقًا لما أوردته محكمة العدل الدولية في قضية "نيكاراجوا"، فإن الهجوم المسلح لا يشمل فقط عمل القوات النظامية عبر الحدود، ويشمل كذلك أن تُرسل دولة أو تنيب عنها؛ عصابات، أو جماعات مسلحة، أو غير نظامية، أو مرتزقة؛ للقيام بأعمال قوة مسلحة ضد دولة أخرى، بدرجة من الجسامة تصل إلى ـ ضمن جملة أمور ـ هجوم مسلح فعلي تقوم به القوات النظامية" أو تتدخل وتشارك فيه بدور أساسي.

وعندما تتورط كيانات خاصة في شن هجمات سيبرانية تكافئ الهجوم المسلح، يثور التساؤل حول إمكان تطبيق قواعد النزاعات المسلحة عليها، بالنظر إلى كونها ليست طرفًا في اتفاقيات القانون الدولي الإنساني، علاوة على عدم تطرق القانون بشكل كافٍ، لبيان كيفية إلزام هذه الكيانات بالامتثال لأحكامه أثناء النزاعات المسلحة، لاسيما تطبيق المبادئ الأساسية له مثل الضرورة، التمييز، التناسب، والإنسانية.

وتجدر الإشارة، إلى أن دليل "تالين" لم يتعرَّض لهذه الإشكالية تحديدًا، وإنما تناول كيفية إسناد العمليات السيبرانية التي تقوم بها هذه الكيانات إلى الدول، وذلك في سياق تقرير المسئولية الدولية عن تلك

---

(1) ***M. N. SCHMITT,*** *21st. Century Conflict: Can the Law Survive? 8 MELB. J. INT'L L., 2007, PP. 443, 454.*

(2) ***M. N. SCHMITT, L. VIHUL,*** *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, P. R., P. 139.*

العمليات، وبالرجوع إلى القواعد العامة، لاستنباط اتجاه بشأن تلك الإشكالية، نجد أن مسألة تطبيق اتفاقات القانون الدولي الإنساني على الكيانات الخاصة، قد طُرحت من جانب الوفد الأمريكي خلال جلسات صياغة اتفاقيات جنيف لعام ١٩٤٩، ولكن اللجنة التي شُكلت لبحث هذا الاقتراح، انتهت إلى أن الدول المتعاقدة ليست ملتزمة بتطبيق الاتفاقيات، مع كيانات لا تعتبر نفسها ملتزمة بأحكامها قانونًا أو واقعًا[١].

وفيما يتعلق بالنزاعات المسلحة غير الدولية، والتي يكون أحد أطرافها كيان بخلاف الدول، فقد أفردت المادة رقم (٣) المشتركة بين اتفاقيات جنيف الأربع لعام ١٩٤٩، حدًا أدنى من الحماية لجميع أطراف هذه النزاعات، ووردت صياغة المادة بالنص على التزام "كل طرف في "**النزاع**"[٢]، وليس "كل طرف في "**الاتفاقية**"، وبما يُفهم منه إمكان أن يكون هذا الطرف، كيانًا مسلحًا بخلاف الدولة، وليس طرفًا في اتفاقيات جنيف، ويؤيد هذا الفهم ما قررته محكمة العدل الدولية، من أن المادة (٣) المشتركة في اتفاقات جنيف، تمثل معيارًا للحد الأدنى للقواعد التي تعكس "اعتبارات وثوابت إنسانية أساسية"، ينبغي أن تحكم أي نزاع، وبغض النظر عما إذا كانت حربًا داخلية، أو نزاعًا دوليًا[٣].

ومن ثم، ووفقًا لما قررته المحكمة الخاصة لسيراليون، يُمكن إعمال هذه المادة، باعتبارها قانونًا دوليًا عرفيًا، واستنتاج أن حكمها ملزم للكيانات المسلحة كطرف في النزاع[٤]، سواء أعلنت عن نيتها الالتزام بالمعاهدة أم لا[٥]، وبخلاف ذلك نكون أمام نتيجة غير منطقية، تتمثل في أن هذه المادة تتعامل مع النزاعات المسلحة غير الدولية، وفيها أطراف من غير الدول، ثم لا تكون هذه الأطراف ملزمة بنصها، مما قد يؤدي للقضاء على الطابع الإنساني لهذه المعاهدات.

ويؤيد المعنى السابق، ما ورد في نص المادة (٣/٤/ج) من البروتوكول الإضافي الثاني لعام ١٩٧٧، الذي قرر أنه لا يجوز تجنيد الأطفال دون الخامسة عشر، في القوات أو "الجماعات المسلحة"، ولا يجوز السماح باشتراكهم في الأعمال العدائية، والذي يُفهم باعتباره يُنشئ التزامات على أي "مجموعة مسلحة"، بالامتناع عن توظيف الأطفال، أو السماح لهم بالمشاركة في الأعمال العدائية.

ويدعم ذلك أيضًا، ما أوردته اتفاقية تنظيم استخدام الأسلحة التقليدية لعام ١٩٨٠، في مادتها (٤/٧) من أن: "الأطراف المتعاقدة، والأطراف الذين يملكون السلطة، قد يوافقون على قبول وتطبيق التزامات البروتوكول الإضافي الأول لاتفاقيات جنيف، على أساس المعاملة بالمثل، وبموجب التعديل الذي أُدخل على الاتفاقية في عام ٢٠٠١، ألزمت المادة (٣/١) منها، كل طرف من أطراف النزاع،

---

(١) **وجاءت صياغة المادة رقم (١) المشتركة بين اتفاقات جنيف لعام ١٩٤٩**، لتؤكد على أن الالتزامات التي يفرضها القانون الدولي الإنساني غير متبادلة بوجه عام، وإنما تُلزم أطراف هذه الاتفاقات، الذين تعهدوا باحترامها وضمان احترامها في جميع الأحوال. **راجع:**

***Federal Political Dept**., Final Record of the Diplomatic Conference of Geneva of 1949 Vol. II-A, Berne ed., 1963, PP. 813: 814.*

(2) ***C. EWUMBUE**, Respect for international humanitarian law by armed non-state actors in Africa, International Journal of the Red Cross, vol. 88, 2006, PP. 905: 920.*

(3) ***Nicaragua v United States** of America International Court of Justice (1986) at paras. 218.*

(4) ***Appeals Chamber Decision on Challenge to Jurisdiction**: Lomé Accord Amnesty, Case No. SCSL-2004-15-AR72(E) and SCSL-2004-16-AR72(E) at para. 47, 13 March 2004.*

(5) ***G. BRITAIN, Ministry of Defence**, the Manual of the Law of Armed Conflict, Oxford University Press, 2005, P. 385.*

بتطبيق القيود الواردة في هذه الاتفاقية والبروتوكولات الملحقة بها، في حالة نشوب نزاعات مسلحة غير دولية في أراضي أحد الأطراف[١].

كما قرر مجلس حقوق الإنسان بشأن النزاع المسلح في "سري لانكا"، أنه على طرفي النزاع الالتزام بقواعد القانون الإنساني الدولي، فالدولة تمتثل حتى في غياب مبدأ المعاملة بالمثل، وتلتزم حركة "*Tigers of Tamil Eelam*، بغض النظر عن سلوك الطرف الآخر[٢].

وأشارت محكمة العدل الدولية في قضية "نيكاراجوا" لعام ١٩٨٦، إلى أن مجموعة "*Contras*" كانت مُلزمة بأحكام المادة (٣) المشتركة لاتفاقيات جنيف، كما كانت الولايات المتحدة ملزمة بعدم تشجيع أو دعم أو تقديم المساعدة للأشخاص أو الجماعات الضالعة في النزاع في نيكاراجوا، بالمخالفة وفقًا للمادة (٣) المشتركة بين اتفاقيات جنيف الأربع لعام ١٩٤٩[٣].

كما قررت دائرة الاستئناف في المحكمة الخاصة لسيراليون عام ٢٠٠٤، أن جميع الأطراف في أي نزاع مسلح، سواء الدول أو الجهات الفاعلة من غير الدول، تلتزم بموجب قواعد القانون الدولي الإنساني، على الرغم من أن الدول فقط هي التي تكون أطرافًا في المعاهدات الدولية، وقد صار ذلك مُستقرًا عليه[٤]، وبينت المحكمة أن التزام هذه الكيانات من غير الدول، ينبع من أن الالتزام الوارد في المادة (٣) المشتركة بين اتفاقيات جنيف لعام ١٩٤٩، والذي يعكس اعتبارات إنسانية أساسية، أصبح قاعدة عرفية ملزمة[٥].

وفي دعوى "*Prosecutor v Thomas Lubanga Dyilo*"، والتي نظرتها المحكمة الجنائية الدولية، ركَّزت الدائرة التمهيدية للمحكمة، على النتيجة التي كانت دائرة الاستئناف في محكمة الخاصة لسيراليون قد انتهت إليها، والمتعلقة بأن الحظر المفروض على تجنيد الأطفال قد تبلور "كقاعدة عرفية"[٦].

---

(١) **وفي مجال حقوق الإنسان، نجد ثلاث معاهدات تُخاطب أحكامها جهات مسلحة غير حكومية، الأولي:** البروتوكول الاختياري لاتفاقية حقوق الطفل لعام ٢٠٠٠، المعني بتجنيد الأطفال، في المادة رقم (٤) منه، **والثانية**، بشأن حماية الأشخاص من الاختفاء القسري لعام ٢٠٠٦، في مادتها رقم (٢)، و**الثالثة:** اتفاقية الاتحاد الأفريقي لحماية ومساعدة المشردين داخليًا في أفريقيا لعام ٢٠٠٩ " كمبالا ٢٠٠٩"، التي أفردت التزامات خاصة بالجماعات المسلحة، ومجموعة من الأفعال التي يُحظر على أفرادها إتيانها. **راجع**:

A. CLAPHAM, *Human Rights Obligations of Non-State Actors, Oxford University Press, 2006, P. 75.*

(2) ***U.N. Human Rights Council****, 11th Special Session, the Human Rights Situation in Sri Lanka (May 27, 2009),* ***available at:*** *http:// www2.ohchr.org/english/bodies/hrcouncil/specialsession/11/index.htm. 1/9/2019.*

(3) ***Nicaragua v United States*** *of America International Court of Justice (1986), Paras: 218: 220.*

(4) ***Prosecutor v. Sam Hinga Norman*** (*Case No. SCSL-2004-14-AR72(E)) Decision on Preliminary Motion Based on Lack of Jurisdiction (Child Recruitment), Decision of 31 May 2004, at para. 22.*

(5) ***Appeals Chamber Decision on Challenge to Jurisdiction***: *Lomé Accord Amnesty, Case No. SCSL-2004-15-AR72(E) and SCSL-2004-16-AR72(E) at para. 47, 13 March 2004.*

(6) ***Prosecutor v Thomas Lubanga Dyilo****, Decision on the confirmation of charges, paras. 311, 312.*

وبوجه عام، نلاحظ أن الممارسات الدولية، لاسيما في أعقاب هجمات الحادي عشر من سبتمبر عام ٢٠٠٢، قد اتجهت نحو إمكان تطبيق مضمون حكم المادة رقم (٥١) من ميثاق الأمم المتحدة، وما يناظرها من العرف الدولي، على هجمات الكيانات بخلاف الدول التي تتم دون تبعية لأي دولة[1]، مع إمكان تحمل هذه الكيانات ببعض الالتزامات أثناء النزاعات المسلحة، وفقًا لحكم المادة (٣) المشتركة بين اتفاقيات جنيف لعام ١٩٤٩، والملاحظ، أنه مع وجود هذا الاتجاه.

ونلاحظ عدم وجود **آليات دولية محددة** لبيان كيف يمكن إلزام هذه الكيانات بالامتثال، أو تقرير مسئوليتها عند المخالفة، بحساب أنها لم تتفق أو توافق علي أي التزامات، بل إنها ربما تكون في حالة نزاع مسلح مع الدولة نفسها، ولا تعترف بسلطتها السياسية. وفي الواقع العملي يستعصي ذلك الأمر على التنفيذ، لاسيما في مجال الهجمات السيبرانية، لكونه يمثّل بيئة خصبة لنشاط تلك الكيانات، التي يتهيأ لها القيام بعمليات عدائية بسهولة ودون أي مسئولية.

المبحث الثالث

بعض جهود التعاون الدولي بشأن تنظيم العمليات السيبرانية

حاولت الدول حماية مصالحها من التضرر، بسبب استهدافها بعمليات سيبرانية مختلفة، أو استهداف الشركات الخاصة بها ومواطنيها، فسعت من خلال عضويتها في منظمات دولية، أو من خلال تشريعاتها الوطنية، إلى محاولة تنظيم هذه العمليات، كما شاركت في بعض المؤتمرات لنفس الغرض، ونعرض لبعض هذه الممارسات من خلال المطالب التالية.

المطلب الأول: جهود منظمة الأمم المتحدة.

المطلب الثاني: جهود بعض المنظمات الإقليمية والتحالفات الدولية .

المطلب الثالث: بعض التشريعات العربية بشأن العمليات السيبرانية.

المطلب الأول

منظمة الأمم المتحدة

أصدرت منظمة الأمم المتحدة عدة قرارات وتوصيات، بشأن العمليات السيبرانية، كما أنشأت فرقًا من الخبراء الحكوميين المعنيين بهذه العمليات، وناقشت بعض هيئاتها أمن الفضاء السيبراني، كما تم اقتراح اتفاقيات دولية ومدونات سلوك بشأن الفضاء السيبراني، ونعرض لذلك من خلال الفروع الآتية:

الفرع الأول

قرارات ووثائق للأمم المتحدة بشأن العمليات السيبرانية

أصدرت الأمم المتحدة عدة قرارات بشأن الجرائم السيبرانية والمعلوماتية، منها القرار رقم ٦٣/٥٥ بتاريخ ٢٠٠٠/١٢/٤، والقرار رقم ١٢١/٥٦ بتاريخ ٢٠٠١/١٢/١٩، بشأن مكافحة سوء استخدام تكنولوجيا المعلومات، وقد أوصى الأول بأن تُضمّن الدول في قوانينها وممارساتها، عدم توفير ملاذات

(1) ***S.C. Res 1368****, U.N. Doc. S/RES/1368 (Sept. 12, 2001);* ***S.C. Res****. 1373, U.N. Doc. S/RES/1373 (Sept. 28, 2001).*

آمنة لكل من يسيء استخدام تكنولوجيا المعلومات، وضمان حماية سرية المعلومات وسلامة أنظمة الحاسوب، ضد أي اعتداء غير مشروع، مع تقرير عقوبة على ذلك الفعل. ودعا القرار ١٢١/٥٦، الدول عند صياغة قوانين وطنية، أو سياسات، أو ممارسات تخص مكافحة سوء استخدام تكنولوجيا المعلومات، أن تأخذ في الحسبان أعمال وإنجازات لجنة الوقاية من الجرائم والعدالة الجزائية. وفي عام ٢٠٠٥ أصدرت الأمم المتحدة القرار ٦٠/١٧٧، بشأن تشجيع التعاون الدولي لمكافحة الجرائم السيبرانية، وتقديم المساعدة للدول الأعضاء في هذا المجال، كما أصدرت في عام ٢٠١٠، القرار رقم ٦٤/٢١١، الذي يدعو الدول إلي تحديث قوانينها في مجال الجرائم السيبرانية، والخصوصية، والبيانات الشخصية، والتجارة والتوقيع الإلكترونيين، وكذلك اعتماد اتفاقيات إقليمية بهذا الشأن[١].

الفرع الثاني

إنشاء فرق من الخبراء الحكوميين المعنيين بالعمليات السيبرانية

في عام ٢٠٠٤، أنشأت الجمعية العامة للأمم المتحدة مجموعة للخبراء الحكوميين (*GGE*)، لدراسة تأثير تطورات تكنولوجيا المعلومات والاتصالات على الأمن القومي والشئون العسكرية للدول، وقد تابع الفريق اجتماعاته سنويًا[٢]، وخلال عام ٢٠١٠ قدَّم الفريق تقريرًا، سلَّط من خلاله الضوء على التهديدات التي تثيرها العمليات السيبرانية للسلم والاستقرار الدوليين، وأن الافتقار إلى توجيه دولي بشأنها قد يتسبّب في أضرار جسيمة، وأورد التقرير التوصيات التالية[٣]:

(١) مواصلة الحوار بين الدول، لمناقشة المعايير المتعلقة باستخدام تكنولوجيا المعلومات والاتصالات، للحد من مخاطرها، وحماية البني التحتي الالكترونية للدول.

(٢) السعي لتحقيق تدابير بناء الثقة، في مجال الحد من مخاطر استخدام الدول لتكنولوجيا المعلومات والاتصالات، بما في ذلك تبادل الآراء الوطنية بشأن استخدامها.

(٣) تبادل المعلومات بشأن التشريعات الوطنية والمعلومات الوطنية، واستراتيجيات وتقنيات وسياسات أمن الاتصالات وأفضل الممارسات.

(٤) تحديد تدابير لدعم بناء القدرات في أقل البلدان نموًا.

وقدمت مجموعة (*GGE*) تقريرًا عام ٢٠١٥، تضمَّن (١١) توصية، منها ضرورة تطبيق القانون الدولي على الفضاء السيبراني، وعدم استهداف البني التحتية الالكترونية للدول، أو دعم الأنشطة ذات الصلة، واعتبار أي دولة مسئولة عن الهجمات السيبرانية التي تنطلق من أراضيها، وأشار التقرير

---

(1) ***S. SCHJOLBERG,*** *The History of Global Harmonization on Cybercrime Legislation, 2008,* ***available at:*** *http://www.cybercrimelaw.net/documents/cybercrime_history.pdf, P. 9. 1/7/2020.*

(2) ***(A/RES/2004/2005),*** *(A/RES/73/266/2006/2007), (A/RES/58/32/٢٠٠٩/٢٠١٠), (A/RES/66/24/2012/2013), (A/RES/68/243/2014/2015), (A/RES/ 70/237/2016/2017), (A / RES / 73/27/2019/2020).*

(3) ***J. A. LEWIS,*** *Confidence-building and international agreement in cybersecurity, disarmament forum confronting cyberconflict, United Nations Institute for Disarmament Research UNIDIR Printed at United Nations, Geneva GE.12-00703—May 2012—4,270 UNIDIR/2012/1 ISSN 1020-7287, PP. 37: 43.*

صراحة إلى أن التوصيات المقترحة كلها طوعية وغير ملزمة، ولكنها خطوة مهمة بشأن تطوير إطار معياري متفق عليه.

وفي ديسمبر من عام ٢٠١٨، أنشأت الجمعية العامة للأمم المتحدة، فريق عمل مفتوح العضوية، معني بتطورات تكنولوجيا المعلومات والاتصالات والفضاء السيبراني (*OEWG*)[١]، للعمل بالتوازي مع مجموعة (*GGE*)، وتكليفه وفقًا للفقرة رقم (٥) من قرار إنشائه، بمواصلة دراسة التهديدات السيبرانية الحالية والمحتملة، والقواعد والمعايير والمبادئ الدولية التي يمكن أن تدعم تنظيمه، وكذلك دراسة إمكان إقامة حوار مؤسسي منتظم، تحت مظلة الأمم المتحدة وبمشاركة واسعة، وتم تفويض (*OEWG*) لعقد اجتماعات للتشاور مع الأطراف ذات الصلة، كالمنظمات غير الحكومية، والأوساط الأكاديمية، وأصحاب المصالح[٢].

وقد بدأ (*OEWG*) عمله في ٣ يونيو من عام ٢٠١٩، باجتماع تنظيمي، ضمَّ ممثلين عن (١٠٠) دولة، كما عقد جلسته الموضوعية الأولى في الفترة من ٩: ١٣ سبتمبر ٢٠١٩، وتلاها الاجتماع التشاوري، في الفترة من ٢: ٤ ديسمبر ٢٠١٩، وعُقدت الدورة الموضوعية الثانية، في الفترة من ١٠: ١٤ فبراير ٢٠٢٠، والدورة الموضوعية النهائية، في الفترة من ٦: ١٠ يوليو ٢٠٢٠، على أن يقدم تقريرًا إلى الدورة رقم (٧٥)، للجمعية العامة للأمم المتحدة، في الفترة من ١٥: ٣٠ سبتمبر ٢٠٢٠[٣].

الفرع الثالث

مناقشة المجلس الاقتصادي والاجتماعي لأمن الفضاء السيبراني عام ٢٠١١

عقد المجلس الاقتصادي والاجتماعي للأمم المتحدة، في التاسع من سبتمبر عام ٢٠١١، اجتماعًا لمناقشة أمن الفضاء السيبراني والتنمية، والقضايا والتحديات ذات الصلة، واشترك في المناقشات إدارة الشئون الاقتصادية والاجتماعية، والإتحاد الدولي للاتصالات، ورئيس لجنة الأمم المتحدة المعنية بتسخير العلم والتكنولوجيا لأغراض التنمية، ومنظومة الأمم المتحدة، والقطاعين العام والخاص، بالإضافة إلى منظمات المجتمع المدني المهتمة بمجالات الفضاء السيبراني والجرائم السيبرانية، وحُدّدت أهداف الاجتماع بأنها:

(١) بناء وعي على مستوى السياسات الدولية، عبر تزويد أعضاء المجلس الاقتصادي والاجتماعي، بصورة عن الوضع الحالي والتحديات المتعلقة بأمن الفضاء السيبراني، وارتباطاته بالتنمية.

(٢) تحديد أفضل السياسات المتعلقة بهذا المجال، والمبادرات المطبقة في مختلف أنحاء العالم، لبناء ثقافة أمن الفضاء الإلكتروني.

(٣) استكشاف خيارات للاستجابة العالمية، بشأن تزايد معدلات الجريمة الإلكترونية.

---

(١) **قرار الجمعية العامة (*A/RES/73/27/2018*).**

(٢) **تطلَّب القرار** موافقة حكومات الدول على حضور هذه الفئات، وتم اختيار "يورج لوبر" ممثل "سويسرا" رئيساً للفريق، **راجع:**

https://www.un.org/disarmament/open-ended-working-group/.*20/7/2020.*

(3) ***Protecting People in Cyberspace:*** *The Vital Role of the United Nations in 2020, protectcyberspace@microsoft.com. 20/7/2020; https://dig.watch/processes/un-gge. 20/7/2020.*

كما ناقش الاجتماع الفوارق الاقتصادية بين الدول، وعدم قدرة النامية منها على مكافحة الجرائم السيبرانية، وكذلك افتقاد الشراكة بينها وبين الدول والصناعية، مما يؤدي إلى خلق ملاذ آمن، لمهاجمي الفضاء السيبراني لارتكاب جرائمهم. كما تم مناقشة الحاجة إلى إبرام اتفاقية دولية بشان الفضاء السيبراني، بما يشمل احتمال البناء على اتفاقية "بودابست"، باعتبارها تُنسق بين الدول بشأن بعض الجرائم الالكترونية، كالتعدّي على حق المؤلف، والغش، واستغلال الأطفال في المواد الإباحية، وجرائم الكراهية، وانتهاكات أمن الشبكات. وقرَّر "الازاروس كابامبي" رئيس المجلس الاقتصادي والاجتماعي، أن أعضاء الاجتماع، قد اتفقوا على أن الأمن السيبراني قضية عالمية، لا يمكن حلها إلا عبر شراكة عالمية، لاسيما من خلال الأمم المتحدة، التي يمكنها استخدام قدراتها الإستراتيجية والتحليلية لمعالجة مثل هذه القضايا(١).

الفرع الرابع

مقترحات باتفاقيات دولية ومدونات سلوك بشأن الفضاء السيبراني

في الحادي عشر من سبتمبر عام ٢٠١١، تلقي أمين عام الأمم المتحدة، من ممثلي "الصين"، و"روسيا الاتحادية"، و"طاجكستان"، و"أوزبكستان"، مسودة لمدونة قواعد سلوك دولية، بشأن المعايير المقبولة للتعامل في الفضاء السيبراني، وتنظيم اعتراض المعلومات الالكترونية، وأمن المعلومات، مع دعوة الدول للمشاركة فيها، باعتبار أن سلامة التواصل عبر الانترنت، تمثّل عنصرًا أساسيًا للأمن القومي للدول، وتألفت المدونة من ثلاثة أجزاء؛ ديباجة، وهدف، ونطاق، بحيث تضمن حماية السلامة الإقليمية للدول، وتدعم حقها في السيادة على معلوماتها السرية، كما تتعهد كل دولة ببذل الجهد والتعاون، بشأن عدم استخدام تكنولوجيا المعلومات والاتصالات، للقيام بأعمال عدائية قد تشكل تهديدًا للسلم والأمن الدوليين(٢).

وخلال عام ٢٠١٢، اقترحت بعض الدول ضرورة إبرام اتفاقية دولية لتنظيم الانترنت، من خلال منظمة الأمم المتحدة، تحظر صراحةً سلوك التجسس السيبراني، وخاصة في المجال الاقتصادي، إلا أن المشاورات التي جرت بهذا الشأن قد تراجعت؛ لاختلاف وجهات النظر بين الولايات المتحدة ودول أوروبا من جهة، والائتلاف الذي تقوده روسيا والصين من جهة أخري، وذلك بشأن طبيعة وحجم دور الدول في إدارة الإنترنت دوليًا، وكذلك المعايير الدولية المقترحة بخصوص أمن المعلومات(٣).

وفي أكتوبر من عام ٢٠١٣، قدمت دولتي "البرازيل" و"ألمانيا" اقتراحًا إلى منظمة الأمم المتحدة، للمطالبة بإضافة مادة إلى العهد الدولي للحقوق المدنية والسياسية "*ICCPR*"، تنظم خصوصية المعلومات وحرية التعبير والأنشطة عبر الانترنت، وتعتبر أنه من ضمن انتهاكات حقوق الإنسان،

---

(1) ***https://www.un.org/development/desa/ar/news/intergovernmental-coordination/cybersecurity-demands-global-approach.html****. 24/7/2020.*

(٢) **اعترضت الولايات المتحدة على هذا الاقتراح**، علي سند من أنه لا يدعم تطبيق قواعد القانون الدولي، ومثل هذه العملية ينبغي أن تتم من خلال اتفاقيات دولية ثنائية أو متعددة الأطراف، وتدعم كل أصحاب المصلحة في مجال الفضاء السيبراني، ولا تقتصر على الحكومات باعتبارها صاحبة الدور الرئيسي. **راجع:**

Ministry of Foreign Affairs of the People's Republic of China, *China, Russia and Other Countries Submit the Document of International Code of Conduct for Information Security to the United Nations,* ***available at****: http://www.fmprc.gov.cn/eng/zxxx/t858978.htm. 19/4/2020.*

(3) ***L. G. CROVITZ****, Information Age: America's First Big Digital Defeat, Wall St. J., Dec. 17, 2012, at A15.*

المراقبة خارج الحدود الإقليمية والاعتراض الجماعي للمعلومات والاتصالات، والمعلومات الشخصية والبيانات[١]. وفي بداية عام ٢٠١٤ جدَّدت "الصين" دعوتها للدول، بضرورة وضع مدونة بشأن تنظيم المعاملات من خلال الفضاء السيبراني، والتفاوض على اتفاقية دولية تنظم التجسس السيبراني، تحت مظلة الأمم المتحدة[٢].

وبنهاية عام ٢٠١٩، ناقشت الجمعية العامة للأمم المتحدة، مشروعًا يتضمن إطار صك دولي بشأن الفضاء السيبراني، وإنشاء لجنة خبراء على أساس التمثيل الجغرافي العادل، يُناط بها صياغة مشروع هذا الصك، لاسيما مكافحة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إجرامية، أو إرهابية، أو تحض على العنف والكراهية، وتم إقرار المشروع بالموافقة، بأغلبية (٧٩) صوتًا، مقابل رفض (٦٠)، وامتناع (٣٣) عن التصويت، وسوف تجتمع اللجنة لأول مرة، ولمدة ٣ أيام في أغسطس ٢٠٢٠، في "نيويورك" للاتفاق على سياسة وخطة عملها[٣].

الفرع الخامس

مؤتمر القمة العالمية لمجتمع المعلومات (*WSIS*) ٢٠١٦

تعقد الأمم المتحدة مؤتمر القمة العالمية لمجتمع المعلومات " *World Summit on the Information Society*) (*WSIS*)، ليكون بمثابة منصة، لعرض تطور احتياجات أصحاب المصالح الخاصة المتعلقة بتكنولوجيا المعلومات والاتصالات، وإقرار مناهج عمل مُنظمة وشاملة على المستويات الوطنية، والإقليمية، والدولية، والسعي لإيجاد رؤية مشتركة، تدعم بناء مجتمع معلومات مُوجه نحو التنمية، مع تحقيق الأمن بشأن إتاحة الوصول إلى المعلومات، واستخدامها، والتشارك فيها[٤].

وتُجري سنويًا منذ عام ٢٠٠٥ في جنيف مجموعة من الفعاليات المتصلة بأهداف المؤتمر، يستضيفها الاتحاد الدولي للاتصالات، ويشارك في تنظيمها كل من "اليونسكو" "*UNSCO*"، و"مؤتمر الأمم المتحدة للتجارة والتنمية" "*UNCTAD*" وبرنامج الأمم المتحدة الإنمائي "*UNEDO*"، بالتعاون

---

(1) ***W. BRADFORD,*** *International Legal Compliance: Surveying the Field, 36 GEO. J. INT'L L. 495, 2005, PP. 495: 519.*

(٢) **وأشارت الدعوة إلى اتفاقية مجلس أوروبا "بودابست"، لعام ٢٠٠١**، باعتبارها تُركّز على حماية الأشخاص من الجرائم الالكترونية، ولم يوقع عليها كثير من الدول، ويُنظر إليها كصك يحتاج إلى تحسين، حيث لم تنظم كثير من العمليات السيبرانية. **راجع:**

M. M. WATNEY, *the Use of Electronic Surveillance in Conducting Criminal Investigations on the Internet, Handbook of Electronic Security and Digital Forensics, 2010, PP. 525: 535.*

(3) ***http://www.un.org/arabic/news/fullstorynews.asp?newsID=5690.*** *25/7/2020.*

(٤) **أيَّد قرار الجمعية العامة (*56/183*) في ٢١ ديسمبر ٢٠٠١**، عقد القمة على مرحلتين، الأولى، في جنيف في الفترة من ١٠ : ١٢ ديسمبر عام ٢٠٠٣، والثانية، في تونس من ١٦ : ١٨ نوفمبر من عام ٢٠٠٥، وبالفعل انعقدت القمة بمرحلتيها، وبلغ عدد المشاركين في المرحلة الأولي (١١٠٠٠) ممثل عن (١٧٥) دولة، وفي ٢٠٠٥، بلغ عددهم أكثر من (١٩٠٠٠) يمثلون ١٧٤ دولة. **راجع:**

WSIS Forum 2016*, WSIS Action Lines: Supporting the Implementation of SDGs,* ***available at:***

https://sustainabledevelopment.un.org/content/documents/10186World%20Summit%20on%20Information%20Society%202016%20Outcomes%202016-May-16.pdf.25/8/2019.

مع منسقي العمل التابعين للقمة العالمية لمجتمع المعلومات (*UNDESA*، *FAO*، *UNEP*، *WHO*، *UN Women*، *WIPO*، *WFP*، *ILO*، *WMO*، *UN*، *ITC*، *UPU*، *UNODC*)[1].

وقد استعرضت الجمعية العامة للأمم المتحدة في عام ٢٠١٥، تنفيذ نتائج تلك القمة العالمية، واعتمدت اعتماد القرار (*A/70/125*)، الذي دعا إلى المواءمة بين عمل القمة وخطة التنمية المستدامة لعام ٢٠٣٠، بالإضافة إلى عقد منتدى القمة العالمية لمجتمع المعلومات على أساس سنوي حتى عام ٢٠٢٥[2].

وفي الفترة من ٢: ٦ مايو من عام ٢٠١٦ انعقد مؤتمر (*WSIS*) في مقر الاتحاد الدولي للاتصالات بجنيف، وركّز على خطط عمل القمة، لاسيما دعم تنفيذ أهداف التنمية المستدامة، تنفيذًا لقرار الجمعية العامة "*A/70/125*"، وإيلاء الاعتبار لآليات متابعة واستعراض تنفيذ خطة التنمية المستدامة لعام ٢٠٣٠، مع استكمال موضوعات الفعاليات السابقة، وتميز منتدى عام ٢٠١٦ بكثافة الحضور لأصحاب المصلحة من مختلف الدول، وكذلك ممثلي الدول، والقطاع الخاص، والمد المدني والأكاديمي، والمنظمات الدولية، مما وفَّر مُناخًا مثالياً لتبادل الرؤى، وقد عُقدت ضمن فعاليات المنتدى (١٥) جلسة تناولت (١٤) موضوعًا[3].

الفرع السادس

الدورة التاسعة عشرة للجنة المعنية بتسخير العلم والتكنولوجيا لأغراض التنمية

منذ عام ٢٠٠٦، تم تفويض لجنة الأمم المتحدة المعنية بتسخير العلم والتكنولوجيا لأغراض التنمية (*CSTD*) (*United Nations Commission on Science and Technology for Development*)، وهي هيئة فرعية تابعة للمجلس الاقتصادي والاجتماعي (*ECOSOC*)، ويدعم "الأونكتاد" عملها على نطاق واسع؛ لتكون بمثابة مركز التنسيق والمتابعة في إطار منظومة نتائج القمة العالمية لمجتمع المعلومات (*WSIS*) وإسداء المشورة للمجلس الاقتصادي والاجتماعي في هذا الشأن، وفي دورتها التاسعة عشرة التي انعقدت في الفترة من ٩ إلى ١٣ مايو ٢٠١٦، بجنيف في سويسرا، كان

---

(1) ***Asian-african Legal consultative organization international law in cyberspace****, the AALCO Secretariat 29 C, Rizal Marg, Diplomatic Enclave, Chanakyapuri, New Delhi – 110 021 India, 2016.*

(2) ***WSIS Forum 2016 "WSIS Action Lines:*** *Supporting the Implementation of SDGs, P. R., Website.*

(٣) **تمحورت هذه الموضوعات حول خطوط عمل القمة وخطة عام ٢٠٣٠**، وسد الفجوة الرقمية، وبناء القدرات، والتعلم الالكتروني، والتمويل من أجل التنمية، وبناء الثقة والأمن بشأن استخدام تكنولوجيا المعلومات، وإتاحة الوصول إلى المعلومات، وتطبيقات وخدمات تكنولوجيا المعلومات والاتصالات، والاقتصاد والتجارة الرقمية، والإعلام، والأبعاد الأخلاقية لمجتمع المعلومات والمعرفة. **راجع:**

WSIS Forum 2016: *High Level Track Outcomes and Executive Brief", 2-6 May, 2016, Geneva, Switzerland,* ***available at:*** *https://www.itu.int/net4/wsis/forum/2016/Outcomes/#ft>. 12/6/2019.*

على رأس أولويات اللجنة موضوع "التبصر بالتنمية الرقمية"، واستعرضت فيه التقدم المحرز في تنفيذ نتائج القمة العالمية لمجتمع المعلومات (*WSIS*)[١].

وفي عملية الاستعراض، سلط المشاركون الضوء على الجوانب الإيجابية والسلبية للتنفيذ، من ناحيتين: الأولي، ضرورة مواكبة النمو السريع لتكنولوجيا الاتصالات منذ عام ٢٠٠٥، باستهداف إتاحة هذه التكنولوجيا لأكثر من نصف سكان العالم بنهاية عام ٢٠١٦، وأبدى كثير من المشاركين قلقهم، من أن معظم الدول النامية تفتقر إلى الوصول إلى تكنولوجيا المعلومات والاتصالات، ولا تفي بوعود إتاحتها لمواطنيها، وبوجه عام، تم إقرار سياسات تدعم التحول الرقمي للدول، وتراعي السياق الاجتماعي والاقتصادي والسياسي لها، وذلك ضمن خطة التنمية لعام ٢٠٣٠، وفي النهاية، أكَّد المشاركون على أهمية تعزيز مجتمعات المعلومات، ومواكبة سرعة التطور في التعاملات الرقمية، ومراعاة احتياجات الدول النامية، والاهتمام بإجراء البحوث لاستجلاء الاتجاهات الحديثة في مجال تكنولوجيا المعلومات والاتصالات[٢].

وفي ١٥ مايو ٢٠٠٦، صرَّح الأمين العام للأمم المتحدة، بأنه "في عالم يتزايد فيه الترابط وإقامة الشبكات، أضحى من المهم ضمان سلامة النظم والهياكل التحتية من هجمات الفضاء السيبراني، والعمل في الوقت نفسه على بثِّ الثقة في التعاملات الإلكترونية، وغيرها من الخدمات والتطبيقات الإلكترونية، حيث إن هذا الخطر له طابع دولي، ويتطلب إرساء ثقافة عالمية لأمن الفضاء الإلكتروني، والعمل على تحييد الفضاء الإلكتروني، ووضع القواعد المتعلقة به وتطبيقها[٣].

الفرع السابع

جهود الاتحاد الدولي للاتصالات

أعلن الأمين العام للاتحاد الدولي للاتصالات عام ٢٠٠٧، إطلاق مبادرة أجندة شاملة بشأن الأمن السيبراني، تتضمَّن التوصل إلى إطار أو بروتوكول لتنسيق جهود مكافحة الجرائم السيبرانية، وبما يشمل تدابير قانونية، وتقنية، وإجرائية، وتنظيمية، وتعاون دولي. وفي عام ٢٠٠٨، نشر الاتحاد تقريرًا نهائيًا أعدَّه أكثر من (١٠٠) خبير بشأن آليات تنفيذ الأجندة[٤]، كما سعى الاتحاد لوضع إطار مشترك بشأن التعامل مع الأمن السيبراني، على المستويات الوطنية والإقليمية والعالمية، وعلى الصعيد العربي، تستضيف سلطنة "عمان"، المركز الإقليمي للأمن الإلكتروني للمنطقة العربية، التابع للاتحاد الدولي للاتصالات، والذي يهدف إلى تقديم الخدمات والمبادرات للمنطقة العربية، بشأن تحسين قدرات الأمن الإلكتروني[٥].

---

(1) ***Commission on Science and Technology for Development:*** *Report on the Nineteenth Session (9-13 May 2016), Economic and Social Council, Official Records, 2016, Supplement no. 11 (E/2016/31-E/CN.16/2016/4).*

(2) ***Asian-African Legal consultative organization international law in cyberspace****, P. R., Website.*

(3) ***http://www.un.org/arabic/news/fullstorynews.asp?newsID=5690.*** *25/7/2020.*

(4) ***S. SCHJOLBERG****, The History of Global Harmonization on Cybercrime, P. R., Website.*

(٥) **اللجنة الاقتصادية والاجتماعية لغربي آسيا**، الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية: توصيات سياساتية، الأمم المتحدة، نيويورك، ٢٠١٥، (*E/ESCWA/TDD/2015/1*)، ص ١٠.

المطلب الثاني

جهود بعض المنظمات الإقليمية والتحالفات الدولية

كان للمنظمات الإقليمية دور مهم، بشأن التعامل مع العمليات السيبرانية بأنواعها المختلفة، وتحقيق قدر من الأمن في مجال المعاملات السيبرانية، ومن أبرز هذه المنظمات، الاتحاد الأوربي، والمنظمة الاستشارية الآسيوية الإفريقية، ومنظمة حلف شمال الأطلسي، ونعرض لجهود كل منظمة منها من خلال الفروع التالية.

الفرع الأول

الاتحاد الأوربي

اعتمدت دول الاتحاد الأوربي وثيقة "إستراتيجية الأمن السيبراني" " *Cybersecurity Strategy of the European Union*"، والتي تمثل رؤية الاتحاد بشأن فضاء سيبراني آمن، من الاضطرابات أو الهجمات الالكترونية، وإقرار تدابير مضادة ضد أي هجمات محتملة، وتضمنت الوثيقة مجموعة ضمانات وإجراءات، لحماية سريَّة وأمان المعاملات المدنية والعسكرية من أي تهديد، وحماية شبكات دول الاتحاد وبنيتها التحتية الالكترونية، وبما يشمل عدم إعاقتها عن العمل، أو الإضرار بالهيكل المادي لها[١].

وتفعيلاً لهذه الوثيقة، صدَّق المجلس الأوروبي في نوفمبر من عام ٢٠١٤، على "سياسة الدفاع السيبراني الإطارية للاتحاد" "*EU Cyber Defence Policy Framework*"، وذلك في اجتماع لوزراء الدفاع، تم خلاله التأكيد على أن أمن الفضاء السيبراني أحد الأولويات الرئيسة للاتحاد، وتمثلت أبرز أهداف هذه السياسة، في العمل على تطوير الدفاع السيبراني للدول الأعضاء، في إطار سياسة الدفاع والأمن المشتركة، وتعزيز الأبحاث والعلوم المختلفة ذات الصلة، وتكثيف أوجه التآزر والتعاون في هذا المجال، مع الجهات الفاعلة من خارج الاتحاد الأوروبي لاسيما حلف شمال الأطلسي[٢].

واستكمالاً لسعي الاتحاد الحثيث نحو تحقيق الأمن السيبراني لأعضائه؛ أصدر البرلمان الأوربي التوجيه (١١٤٨/٢٠١٦) في ٦ يوليو ٢٠١٦، بشأن التدابير المشتركة الخاصة بمستوى عالٍ لأمن الشبكات ونظم المعلومات في جميع دول الاتحاد، والتي هي جزء أساسي من الإستراتيجية العامة للأمن السيبراني للاتحاد، وقد تطلب التوجيه، أن تتبنى كل دولة عضو إستراتيجية وطنية لأمن الشبكات والمعلومات، وأن تنشئ سلطة وطنية تكون مسئولة عن ذلك، وكذلك إنشاء مجموعة فنية متخصصة للرد على التهديدات السيبرانية، وأُطلق عليها "فريق الاستجابة لطوارئ الكمبيوتر" " *Computer Emergency Response Team*" "*CERT*"[٣].

---

(1) ***Cybersecurity Strategy of the European Union:*** *an Open, Safe and Secure Cyberspace, JOIN (2013) 1 final, Brussels, 2013.*

(2) ***An outline for European Cyber Diplomacy Engagement****, 9967/4/14 REV 4, DG D 1C, Brussels, September 2014.*

(3) ***Directive (EU) 2016/1148 of the European Parliament and of the Council,*** *of 6 July 2016, concerning measures for a high common level of security of network and information*

الفرع الثاني

المنظمة الاستشارية القانونية الآسيوية الإفريقية

حققت محاولات تنظيم الفضاء السيبراني من خلال المنظمة الاستشارية القانونية الآسيوية الإفريقية، "*Asian-African Legal Consultative Organization*" "*AALCO*"، تقدمًا خلال فترة زمنية قصيرة، حيث بدأت باقتراح من "الصين" لتنظيم هذا الموضوع، وإدراجه كبند في جدول أعمال الدورة السنوية الثالثة والخمسين للمنظمة، والتي عُقدت في "طهران" عام ٢٠١٤، وقد قُبل ذلك الاقتراح بأغلبية الآراء، ثم نوقش الموضوع بعد ذلك في جميع دورات انعقاد المنظمة اللاحقة، ومع الدورة الخامسة والخمسين، تم تشكيل فريق عامل مفتوح العضوية لدراسة تفاصيل الموضوع وفروعه، وبدأ هذا الفريق اجتماعاته في عام ٢٠١٦ بمقر الأمانة العامة للمنظمة، لبحث الموضوعات التالية[١]:

أ) مدى سيادة الدولة على الفضاء السيبراني؛

ب) الاستخدام السلمي للفضاء السيبراني؛

ج) قواعد التعاون الدولي في مجال مكافحة الجرائم السيبرانية؛

د) القواعد الدولية لاسيما ميثاق الأمم المتحدة ذات الصلة بالفضاء السيبراني.

وتم تكليف أمانة المنظمة بموجب قرار معتمد في الدورة السنوية الرابعة والخمسين بإعداد دراسة حول الموضوعات السابقة ليتم إقرارها خلال الدورة السنوية لعام ٢٠١٧.

وناقش الفريق العامل مفتوح العضوية في اجتماعه الثاني عام ٢٠١٧ موضوعات أربعة:
الأول: سيادة الدولة في الفضاء السيبراني، وأُثيرت إشكالية عدم قدرة كثير من الدول، على ممارسة كامل السيادة على الكيانات بخلاف الدول في هذا المجال، وبالتالي عدم قدرتها بشأن مكافحة العمليات السيبرانية، وغيرها من العمليات السيبرانية التي تنطلق من داخل أراضيها، وتم الاتفاق على التزام عام بممارسة حقوق السيادة على الفضاء السيبراني، مع احترام حقوق الدول الأخرى عليه، ووضع قواعد لحل الإشكالية المعروضة[٢].

وتمثل الموضوع الثاني في حوكمة الفضاء السيبراني: لاسيما برتوكولات الاتصال (*DNS*)، واتفق الفريق على أن التوافق السياسي مطلوب لإدارة الموارد الحيوية للإنترنت، وعلى الأمم المتحدة أن يكون لها دور في ذلك. **وتعلَّق الموضوع الثالث بالحرب السيبرانية:** حيث تمت مناقشة جوانبها، وكيفية تطبيق قواعد القانون الإنساني الدولي عليها. **وتمثل الموضوع الرابع في مكافحة الجرائم السيبرانية وفقًا لقواعد القانون الدولي:** حيث نوقشت بعض جوانب اتفاقية مجلس أوربا "بودابست"[٣]، وبعض المثالب

---

systems, across the Union, Official Journal of the European Union, ***available at:*** *https://eur-lex.europa.eu/legal content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN. 14/8/2020.*

(1) ***Asian-african Legal consultative organization,*** *P. R., Website.*

(٢) **المنظمة الاستشارية القانونية الآسيوية - الإفريقية (آلكو)**، المذكرة التوضيحية للدورة السنوية الثامنة والخمسين لمنظمة (آلكو)، مركز "جيوليوس نيريري" الدولي للمؤتمرات، دار السلام، جمهورية تنزانيا المتحدة، أكتوبر، ٢٠١٩، ص ١٦: ١٧.

(٣) **ألزمت المادة رقم (٢) من الاتفاقية**، الأطراف بسن تشريعات لتجريم الوصول إلى كامل أو أي جزء من نظام الحاسبات السيبرانية دون حق، كما وصفت المادة السلوك المجرَّم بأنه انتهاك التدابير الأمنية، كما قضت المادة (٣) منها

التي تتضمنها وتحتاج إلى معالجة، وكذلك تمت الإشارة إلى أن دراسة مكتب الأمم المتحدة المعني بالمخدرات والجريمة، بشأن الجريمة السيبرانية، يمكن أن تكون نقطة محورية كأفضل المساعي لإنشاء قواعد إقليمية أو عالمية نموذجية، لاسيما إبرام اتفاقية عالمية في إطار الأمم المتحدة لمكافحة جرائم الإنترنت[١].

وفي دورتها السادسة والخمسين، نظرت المنظمة في وثيقة الأمانة العامة (*AALCO/56/NAIROBI/ 2017/SD/S17*)، التي أشارت إلى إدراك الأعضاء لأهمية الفضاء السيبراني، وتأثيره على الدول ومواطنيها، والحاجة إلى منع استخدام تكنولوجيا المعلومات والاتصالات، في أغراض تتعارض مع الاستقرار والأمن الدوليين، مع كالجرائم السيبرانية، والحرب السيبرانية، والإرهاب السيبراني، سواء من جانب الدول، أو الكيانات بخلاف الدول، وبما يُعَظّم الحاجة إلى إنشاء آلية عالمية شفافة ومتوازنة، لإدارة شبكة الإنترنت وسد "الفجوة الرقمية" بين الدول، وتعزيز التنسيق والتعاون القضائي بين الدول الأعضاء، لمكافحة إساءة استخدام تلك التكنولوجيا لأغراض إجرامية، ووفقًا لمبادئ وقواعد القانون الدولي، بما في ذلك ميثاق الأمم المتحدة، ومواصلة تطوير هذه القواعد لتلائم الفضاء السيبراني[٢].

الفرع الثالث

منظمة حلف شمال الأطلسي

تبنّي (*NATO*) إعداد دليل "تالين"، بشأن القانون الدولي المُطبق على الحرب السيبرانية، بإصداريه لعامي ٢٠١٣، ٢٠١٧، وهو توجيه غير ملزم، بشأن القواعد الدولية التي تحكم العمليات السيبرانية، حيث استضاف المركز التعاوني للدفاع السيبراني (*Cooperative Cyber Defence Centre of Excellence*)، التابع للحلف، بمقره في مدينة "تالين" عاصمة "استونيا"، صياغة هذا الدليل في الفترة من عام ٢٠٠٩ وحتى ٢٠١٧، بجهود فريق خبراء قانونيين دوليين (*IGE*) برئاسة البروفيسور "*Michael N. Schmitt*"[٣].

بأن الاعتراض دون حق، الذي يتم بواسطة الوسائل التقنية لنقل بيانات غير عامة من الحاسوب، ينبغي أن يشكّل أيضًا جريمة جنائية في تشريعات أطراف الاتفاقية. **راجع:**

B. RABOIN, *Corresponding Evolution: International Law and the Emergence of Cyber Warfare, 31 J. NAT'L ASS'N ADMIN. L. JUDICIARY, 2011, PP. 632: 640.*

(1) ***Asian-african Legal consultative organization international*** *law in cyberspace, P. R., PP. 6:7.*

(2) ***Asian-african Legal consultative organization international*** *law in cyberspace, P. R., P. 8.*

(٣) **(*NATO*): منظمة عسكرية أو تحالف عسكري دولي**، تأسس عام ١٩٤٩، بناءً على معاهدة شمال الأطلسي، التي وُقّعت في واشنطن عام ١٩٤٩، ويتشكّل من (٣٠) دولة، من أمريكا الشمالية وأوروبا، ومن بين أبرز أهدافه، الدفاع المشترك لأطرافه ضد أي هجوم من قبل أطراف خارجية، ويقع مقره الرئيسي في "هارين"، ببروكسل، بلجيكا. وقد **تشكّل فريق (*IGE*) من (١٦) مُتخصّصًا من البارزين في مجال القانون الدولي**، واستعان الفريق بهيئة مكونة من (٤) مستشارين تقنيين، تحت إشراف خبراء من الحلف، وممثلين عن اللجنة الدولية للصليب الأحمر، وتمت مراجعة الدليل من قبل أساتذة قانون دولي، منهم "البروفيسور مايكل شميت بالكلية البحرية الأمريكية"؛ "لي كومودور بالكلية الجوية الأمريكية"؛ "ويليام بوثبي - نائب مدير خدمات القانون للقوات الجوية الملكية بالمملكة المتحدة؛ "برونو ديميير - الجامعة الكاثوليكية في لوفين". **راجع:**

وقد ظهر الإصدار الأول من الدليل عام ٢٠١٣، وتضمَّن (٩٥) قاعدة لسلوك الدول في سياق الحرب السيبرانية، مع تعليقات على كل قاعدة، وفي عام ٢٠١٧ ظهر الإصدار الثاني، وتضمَّن (١٥٤) قاعدة، تُشكّل مستوى أكثر عُمقًا بشأن معالجة العمليات السيبرانية، مع تعليقات على كل قاعدة، تبين النقاش الذي دار بشأنها، وأي وجهة نظر قُبلت بالأغلبية، وموقف الأقلية إن وُجد، وكذلك حالات الإجماع. وانتهي الدليل إلى أن القواعد الدولية السارية فاعلة إلى حد كبير، ويمكن تطبيقها على العمليات السيبرانية، وتعرَّض الدليل لبعض الإشكاليات القانونية في المجال السيبراني، كسيادة الدول، وقواعد ممارسة الاختصاص، وقانون مسئولية الدول، إضافة إلى قانون حقوق الإنسان، وقانون البحار، والقانون الدبلوماسي والقنصلي[١].

وتجدر الإشارة إلى أن هذا الدليل ليس صكًا دوليًا رسميًا أو مُلزمًا، ولا يمثل وجهة نظر (*NATO*)، أو الدول التي شارك خبراء من جنسيتها في وضع الدليل، وإنما هو رؤية الخبراء المستقلين الذين صاغوه بصفاتهم الشخصية، ومع ذلك، فإن أهميته كبيرة، كوثيقة رائدة في مجال العمليات السيبرانية، وخطوة مهمة لتنظيم الفضاء السيبراني، وإن كانت غير كافية، ويلزم أن تتبعها خطوات أخري[٢].

وقد أثار الدليل مخاوف جانب من الفقه، باعتبار أنه ربما يتسبَّب في تنافس بين الدول، لتعزيز التَسَلُح بوسائل الهجوم السيبرانية، أو ما أُطلق عليه "عسكرة الفضاء السيبراني، والتي وثَّقتها بعض الدراسة القانونية، وفرَّرت أن مثل هذا التنظيم قد يساهم في خلق جو من انعدام الأمن والتوتر في المجتمع الدولي[٣]. وفي عام ٢٠١٠، شكَّلت منظمة الأمم المتحدة، مجموعة خبراء حكوميين لدراسة هذا الأمر، والتي قدَّمت ثلاثة تقارير، مفادها، وجود قبول عام لدى الدول لتنظيم هذه العمليات وقت السلم ولأغراض السلمية وفقًا للقانون الدولي[٤].

وفي تقريرها المُقدَّم في دورتها رقم (٣٢) عام ٢٠١٥، أكدت اللجنة الدولية للصليب الأحمر على أن تنظيم القانون الدولي للعمليات السيبرانية، لا يُمكن اعتباره تشجيعًا على عسكرة الفضاء السيبراني، ولا ينبغي أن يفهم بأنه يُضفي الشرعية على الحرب السيبرانية، مثلما أنه من الخطأ الادعاء بأن اتفاقيات "جنيف" تضفي الشرعية على الحرب بشكل عام[٥].

***NATO Cooperative Cyber Defense Centre of Excellence**, TALLINN MANUAL on the International Law Applicable to Cyber Warfare 45 (Michael N. Schmitt et al. eds., 2013), **available at:** https://perma.cc/DHK8-7WFG. 20/4/2020;*

(1) ***M. J. ADAMS**, a Warning about Tallinn 2.0, Whatever It Says' Law fare, (4 January 2017), **available at:** https://www.lawfareblog.com/warning-about-tallinn-20-%E2%80%A6-whatever-it-says. 15/7/2019.*

(2) ***M. N. SCHMITT, S. WATTS,** The Decline of International Humanitarian Law Opinion Juries and the Law of Cyber Warfare, 50(2) Texas International Law Journals, 2015, P. 189.*

(3) ***M. D. CAVELTY**, The Militarisation of Cyberspace: Why Less May Be Better' in C. CZOSSECK, R. OTTIS, K. ZIOLKOWSKI (eds.), 4th International Conference on Cyber Conflict, NATO CCD COE, 2012, P. 141.*

(4) ***UN Doc A/65/201 (2010); UN Doc A/68/98 (2013); UN Doc A/70/174 (2015)**.*

(5) ***ICRC**, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts' (October 2015), **available at:** https://www.icrc.org/en/download/file/15061/32ic-report-on-ihl-and-challenges-of armed-conflicts.pdf.13/3/2020.*

الفرع الرابع

الاتفاقيات والمبادرات الإقليمية بشأن العمليات السيبرانية

تُعد اتفاقية مجلس أوروبا "بودابست"، والتي دخلت حيز النفاذ عام ٢٠٠٤، أبرز الاتفاقيات الإقليمية في مجال الجريمة السيبرانية ذات الصبغة الجنائية، وتهدف إلى تنسيق تشريعات الأعضاء في هذا المجال، وتعزيز قدراتها بشأن التحقيق والمقاضاة في هذه الجرائم، وتتضمن الاتفاقية ثلاثة أجزاء، الأول بشأن القواعد الموضوعية للجرائم، والثاني حول إجراءات التحقيق، والجزء الثالث حول آليات التعاون الدولي، وقد استوحت عدة دول، لاسيما في المنطقة العربية أحكام الاتفاقية عند إعداد قوانينها الوطنية بشأن الجرائم السيبرانية[١].

وعلى الصعيد العربي، تم إبرام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، في ٢٠١٠/١٢/٢١، وتضمنت خمسة فصول، أحدها خاص بتحديد أنواع الجرائم السيبرانية، وآخر يخص الجانب الإجرائي، وفصل خاص بالتعاون القانوني والقضائي بين الأعضاء. وقد وقَّعت (١٨) دولة عربية عليها، وصدَّقت (٧) دول[٢].

كما أعدت "*ESCWA*"، في إطار مشروع "تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية"[٣]، والذي أقَّر في الفترة من عام ٢٠٠٩، وحتى ٢٠١٢، إرشادات بشأن التشريعات السيبرانية[٤]، والتي تعتبر كنموذج تشريعي لدول المنطقة، وتشمل بالإضافة إلى الجرائم السيبرانية، الاتصالات الإلكترونية وحرية التعبير، والتوقيع الإلكتروني، والمعاملات الإلكترونية، والتجارة الإلكترونية وحماية المستهلك، ومعالجة البيانات ذات الطابع الشخصي، وحقوق الملكية الفكرية في المجال المعلوماتي والسيبراني.

وفي دول الكومنولث، أعّدت مجموعة خبراء قانونًا نموذجيًا عام ٢٠٠٢، مُستوحى من اتفاقية بودابست، تحت مُسمّي "قانون الجرائم المتعلقة بالحاسوب". كما اعتمدت منظمة التعاون والتنمية الاقتصادية (*OECD*) (*Organization for Economic Cooperation and Development*)، في عام ٢٠١٤ اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني[٥].

وأقر الاتحاد الأوروبي عام ٢٠٠٣، إطارًا تنظيميًا بشأن الاعتداء على الأنظمة المعلوماتية، ودخل حيز النفاذ عام ٢٠٠٥، كما أنشأت وكالة الاتحاد الأوروبي لأمن الشبكات والمعلومات "*ENISA*" "*European Union Agency for Network and Information Security*"،

---

(١) **اللجنة الاقتصادية والاجتماعية لغربي آسيا**، الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية: توصيات سياساتية، الأمم المتحدة، نيويورك، ٢٠١٥، (*E/ESCWA/TDD/2015/1*)، ص ٢٣.

(2)***http://www.lasportal.org/wps/wcm/connect/LAS/las/las_ar_aln/arab_legal_network_agreements/?WCM_Page.ResetAll=TRUE.*** *1/7/2020.*

(3)***http://isper.escwa.un.org/FocusAreas/CyberLegislation/Projects/tabid/161/language/arLB/Default.aspx2.*** *1/7/2020.*

(4)***http://isper.escwa.un.org/Portals/0/Cyber%20Legislation/Regional%20Harmonisation%20Project/Directives/Directives-Full.pdf****. 5/7/2020.*

(5)***http://opennetafrica.org/wpcontent/uploads/researchandpubs/African%20Union%20Convention%20on%20Cyber 02Security%20&%20Personal%20Data%20Protection.pdf.*** *5/7/2020*

مؤسسات متخصصة، لتعزيز التعاون بين دول الاتحاد في مجال الأمن السيبراني، وتقديم توصيات بشأن السلامة المعلوماتية، وتحصين البنية الالكترونية الأساسية، وتعزيز قدرات الدول على تفادي المخاطر السيبرانية والتصدي لها[١].

المطلب الثالث

بعض التشريعات العربية بشأن العمليات السيبرانية

قامت بعض الدول بإصدار تشريعات متخصصة بشأن العمليات السيبرانية، في حين ضمَّنت بعض الدول نصوصًا ذات صلة بالجريمة السيبرانية في تشريعاتها المختلفة، كتلك الخاصة بالمعاملات الإلكترونية، أو التجارة الإلكترونية، أو حماية حقوق الملكية الفكرية، أو قانون العقوبات. وفيما يلي نورد ملخصًا لوضع تشريعات العمليات السيبرانية في بعض الدول العربية[٢]، وذلك من خلال الفروع التالية:

الفرع الأول

أورد الدستور المصري لعام ٢٠١٤، بعض النصوص بشأن أمن المعلومات، حيث نص في مادته رقم (٣١) بأن: "أمن الفضاء المعلوماتي، جزء أساسي من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه، على النحو الذي ينظمه القانون"؛ كما نصت المادة (٥٧) منه على أن: "للحياة الخاصة حرمة، وهي مصونة لا تُمس، وللمراسلات البريدية والبرقية والإلكترونية والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، ولا تجوز مصادرتها، أو الاطلاع عليها، أو رقابتها إلا بأمر قضائي مُسبَّب، ولمدة محددة، وفى الأحوال التي يبينها القانون؛ كما تلتزم الدولة بحماية حق المواطنين في استخدام وسائل الاتصال العامة بكافة أشكالها، ولا يجوز تعطيلها أو، أو حرمان المواطنين منها بشكل تعسفي[٣].

وتم سن التشريع رقم (١٥) لسنة ٢٠٠٤، بشأن التوقيع الإلكتروني، والذي قضي في مادته رقم (٢٣) على تجريم فعل التزوير الإلكتروني، للمحررات الإلكتروني، وكذلك تضمَّن القانون أحكام بشان التوقيع الإلكتروني، واستعمال المزور الإلكتروني، وإتلاف محرر إلكتروني أو تعديله، وكذلك تم تعديل المادة رقم (١١٦) من قانون الطفل رقم (١٢٩) لسنة ٢٠٠٨، بشأن الاستغلال الجنسي للأطفال عبر الإنترنت، إضافة إلى بعض النصوص المتفرقة، في عدة قوانين مثل قانون العقوبات، كحماية الحق في الحياة الخاصة، والمادة (١٧١) المتعلقة بوسائل العلانية، وقانون الأحوال المدنية رقم ١٤٣ لسنة ١٩٩٤، بشأن حماية الحق في الخصوصية والحياة الخاصة، وقانون تنظيم الاتصالات رقم (١٠) لسنة ٢٠٠٣، الذي يهدف إلي تحقيق سلامة وأمن نظم وشبكات الاتصالات، ويجرم الأفعال التي تلحق الضرر بشبكات الاتصالات، أو تعطيلها، أو التنصت على الاتصالات، والقانون رقم (٨٢) لسنة ٢٠٠٢، بإصدار قانون حماية الملكية الفكرية.

---

(1) ***ENISA,*** *Roadmap to provide more proactive and efficient Computer Emergency Response Team training,* ***available at:***
http://www.enisa.europa.eu/activities/cert/support/exercise/roadmap-to-provide-more-proactive-andefficient-cert-training. 5/7/2020.

(٢) **اللجنة الاقتصادية والاجتماعية لغربي آسيا**، الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية: توصيات سياساتية، الأمم المتحدة، نيويورك، ٢٠١٥، (*E/ESCWA/TDD/2015/1*)، ص ٣٣: ٣٤.

(٣) **اللجنة الاقتصادية والاجتماعية لغربي آسيا**، الأمان في الفضاء السيبراني، المرجع السابق، ص ٣٥.

الفرع الثاني

الإمارات العربية المتحدة

كانت دولة الإمارات العربية المتحدة سّباقة بشأن إقرار قانون لمكافحة جرائم تقنية المعلومات رقم (٢) لعام ٢٠٠٦، كما أوصى مجلس التعاون الخليجي، في مؤتمر انعقد في يونيو ٢٠٠٧، بصياغة اتفاقية بشأن الجرائم السيبرانية تكون دول المجلس من أعضائها، وقد حدَّثت الإمارات العربية المتحدة قانونها، بإلغاء القانون المذكور رقم (٢) لسنة ٢٠٠٦، واستبداله بالقانون الاتحادي رقم (٥) لسنة ٢٠١٢، والذي بدا أكثر تفصيلاً، ومراعاة للأنماط المستجدة في ارتكاب الجرائم السيبرانية، إلا إن هذا القانون لم يتضمن قواعد إجرائية مفصلة خاصة بالتحقيقات الجزائية المتعلقة بالجرائم السيبرانية[١].

الفرع الثالث

الأردن

أقر "الأردن" قانون جريمة أنظمة المعلومات رقم (٣٠) لعام ٢٠١٠، ويحدد عناصر جرائم نظم المعلومات، ويُعالج الثغرات في التشريعات القائمة من حيث التعامل مع نظم المعلومات وجرائم الإنترنت، وقد تعامل القانون مع نمطين من الجرائم، الجرائم المُستحدثة، وبما يشمل الولوج إلى نظم المعلومات والشبكات بدون إذن، ومحو أو نسخ، وإضافة أو تغيير المعلومات، ونشر الفيروسات، وسرقة البيانات المستعملة في المداولات المالية الإلكترونية. والنمط الثاني، يتمثل في استعمال نظم المعلومات والشبكات، في الجرائم الخاصة بالتأثير على القصر أو المُعاقين عقليًا، أو الترويج للدعارة[٢].

الفرع الرابع

تونس

أصدرت "تونس" مجموعة من التشريعات المتعلقة بشكل مباشر أو غير مباشر بالأمان السيبراني، وهي: أو القانون رقم (٥) لسنة ٢٠٠٤، المتعلق بتنظيم مجال السلامة المعلوماتية، وضبط القواعد العامة لحماية النظم المعلوماتية والشبكات، والقانون رقم (٨٩) لسنة ١٩٩٩، المتعلق بتنقيح وإتمام بعض الأحكام الجنائية وإضافة فصل خاص بالجرائم المعلوماتية، وكذلك القانون التوجيهي رقم (١٣) لسنة ٢٠٠٧، لسنة ٥١١٢ المتعلق بإرساء قواعد خاصة بالاقتصاد الرقمي، والقانون الأساسي رقم (٦٣) لسنة ٢٠٠٤، المتعلق بحماية المعلومات الشخصية، والقانون رقم (٨٣) لسنة ٢٠٠٠، المتعلق بالمبادلات والتجارة الإلكترونية، والقانون رقم (٥٧) لسنة ٢٠٠٠، المتعلق بتنقيح وإتمام بعض فصول الالتزامات والعقود، للاعتراف بالسندات والتوقيع الإلكتروني، والقانون رقم (٧٥) لسنة ٢٠٠٣، المتعلق بدعم الجهود الدولية لمكافحة الإرهاب ومنع غسل الأموال، وقانون الاتصالات لعام ٢٠٠١، وتعديلاته[٣].

الفرع الخامس

---

(١) **اللجنة الاقتصادية والاجتماعية لغربي آسيا**، الأمان في الفضاء السيبراني، المرجع السابق، ص ٣٤.

(٢) **اللجنة الاقتصادية والاجتماعية لغربي آسيا**، الأمان في الفضاء السيبراني، المرجع السابق، ص ٣٤.

(٣) **الوكالة الوطنية للسلامة المعلوماتية**، وزارة التعليم العالي والبحث العلمي وتكنولوجيا، المعلومات والاتصال على الاستبيان المرسل لها في إطار هذه الدراسة، تونس، أيلول/سبتمبر ٢٠١٤، **اللجنة الاقتصادية والاجتماعية لغربي آسيا**، الأمان في الفضاء السيبراني، المرجع السابق، ص ٣٤.

لبنان

في عام ٢٠١٢، انتهت لجنة مشكلة من قبل رئاسة مجلس الوزراء اللبناني، وضمت ممثلين عن الوزارات المعنية والقطاع الخاص، من إعداد مشروع قانون متكامل حول المعاملات الإلكترونية والتوقيعات الإلكترونية، وحماية البيانات ذات الطابع الشخصي، غير أن المشروع لم يُعتمد بعد، وكان قد سبق إقرار القانون رقم (٧٥) في ١٩٩٩/٤/٣، بشأن حماية الملكية الأدبية والفنية، وكذلك القانون رقم (١٤٠) في ١٩٩٩/١٠/٢٧، المتعلق بصون الحق بسرية المكالمات الهاتفية، إضافة إلى بعض النصوص التقليدية في قانون العقوبات، والتي يمكن تطبيقها في مجال الجرائم السيبرانية، مثل الاحتيال والسب والتخريب[١].

الفرع السادس

الجمهورية العربية السورية

صدر في الجمهورية العربية السورية، المرسوم التشريعي رقم (١٧) في ٢٠١٢/٢/٨، بشأن تنظيم التواصل على شبكة الانترنت، ومكافحة الجريمة المعلوماتية، ومسؤوليات مزودي خدمات الشبكة وواجباتهم، وحجب المواقع الإلكترونية، كما يُحدّد أصناف الجرائم السيبرانية وعقوباتها وحالات تشديدها، وقبل هذا المرسوم، كان القانون رقم (٤) في ٢٠٠٩/٢/٢٥، قد صدر لتنظيم التوقيع الإلكتروني وخدمات الشبكة، وتضمن بوجه خاص تنظيم التوقيع الإلكتروني، وشروطه والتصديق عليه، كما تضمن النص على المخالفات الخاصة بتزوير التوقيع الإلكتروني واستعماله. كما صدر بتاريخ ٢٠١٠/٦/٩، القانون رقم (١٨) الخاص بتنظيم قطاع الاتصالات، وكذلك قانون الإعلام بمرسوم رقم (١٠٨) لسنة ٢٠١١، الذي تضمن تنظيم وسائل التواصل على الشبكة، والمخالفات والجرائم المرتبطة بها. والمرسوم التشريعي رقم (٦٢) في ٢٠١٣/٩/١٦، الخاص بتنظيم والملكية الفكرية، وحماية المصنفات المعلوماتية[٢].

الفرع السابع

بعض الدول العربية الأخرى

أقرت المملكة العربية السعودية نظام مكافحة جرائم المعلوماتية عام ٢٠٠٧، كما أصدرت البحرين القانون رقم (٦٠) لسنة ٢٠١٤، بشأن جرائم تقنية المعلومات، كما أعدَّت الكويت مسودة مشروع قانون حول الجرائم السيبرانية. ويتوافر لدى "إسكوا" العديد من الدراسات حول وضع التشريعات السيبرانية ومنها الجرائم السيبرانية في المنطقة العربية حتى عام ٢٠١٣[٣].

والملاحظ على التشريعات السابقة، أن جميعها يتناول تنظيم العمليات السيبرانية ذات الصبغة الجنائية، والتي من أمثلتها، النصب، والسرقة، وتزوير التوقيع الالكتروني، والأفعال الإباحية لاسيما ما يتعلَّق بالأطفال، وغيرها من الجرائم السيبرانية، ولم تُفرد تلك التشريعات مساحة لتعريف كافة العمليات السيبرانية، والتمييز بينها، ومعالجة كل منها بنصوص تتوافق مع طبيعتها وآثارها المُحتملة، خاصةً

---

(١) **اللجنة الاقتصادية والاجتماعية لغربي آسيا**، الأمان في الفضاء السيبراني، المرجع السابق، ص ٣٥.

(٢) **اللجنة الاقتصادية والاجتماعية لغرب آسيا**، الأمان في الفضاء السيبراني، المرجع السابق، ص ٣٦.

(3) ***Regional Profile of Information Society in the Arab region**, 2013, **available at:** http://www.escwa.un.org/information/publications/edit/upload/E_ESCWA_ICTD_13_6_E.pdf , chapter 5 and 6. 5/7/2020.*

العمليات التي تستهدف مؤسسات الدول، والبني التحتية الالكترونية لها، كالهجمات السيبرانية، والتجسس السيبراني، والإرهاب السيبراني، والحرب السيبرانية.

ونوالي من خلال الفصل الثاني دراسة أحد تطبيقات التهديدات السيبرانية، وهو التجسس السيبراني، حيث نبدأ بدراسة سلوك التجسس عمومًا، لاسيما ماهيته، وأنواعه ودوافع القيام به، والوضع القانوني الدولي الساري بشأنه سواء خلال النزاعات المسلّحة، أو في أوقات السلم، لنتقدم بعد ذلك لندرس الوضع القانوني الدولي للتجسس السيبراني.

الفصل الثاني

التنظيم القانوني الدولي الساري بشأن التجسس

تمهيد وتقسيم:

تلجأ الدول إلى ممارسة التجسس في أوقات النزاعات المسلَّحة، لتُحقّق ميزات عسكرية وإستراتيجية تساعدها في الانتصار على الخصم، وفي أوقات السلم، تدعم المعلومات السرية المُتحصَّل عليها تحقيق الكفاءة السياسية لحكومات الدول، لاسيما فيما يخص اتخاذ قرارات ملاءمة على الصعيد الوطني أو الدولي، وكذلك تعزيز قدرة الدول على استخدام حق الدفاع عن النفس، ودعم رصد الامتثال للالتزامات الدولية، وأيضًا دعم أغراض الملاحقة الجنائية الدولية.

وقد نظَّمت قواعد القانون الدولي سلوك التجسس أثناء النزاعات المسلحة، ولكنها لم تتطرق صراحةً إلى تنظيمه في وقت السلم، سواء بالحظر أو الإباحة، بالرغم من حرص الدول على سن تشريعات وطنية تنظم هذا السلوك في وقت السلم ، والذي أُعتبر بموجب معظمها ـ إن لم يكن كلها ـ جريمة خطيرة يُعاقب عليها بأشد العقوبات، والمُلاحظ أن القواعد الدولية الخاصة بالتجسس أثناء الحروب، أو الوطنية بشأنه في زمن السلم، قد ركَّزت على ممارسته بواسطة مصادر بشرية أو فئة الجواسيس، ولم تتطرق بشكل صريح إلى الوسائل الحديثة في جمع المعلومات، والتي يُطلق عليها الاستخبارات التقنية، وتتم من خلال الفضاء السيبراني.

وقد اجتهد كثير من الفقه في تفسير القواعد الدولية، وتحليل الأحكام القضائية، والممارسات الدولية ذات الصلة بالتجسس، في محاولة لاستجلاء مدى مشروعيته في زمن السلم، وقرر البعض أنه فعل مشروع، نظرًا لعدم وجود قاعدة دولية تحظره صراحةً، بينما قرَّر جانب فقهي آخر عدم مشروعية التجسس وقت السلم، لأنه ينتهك مبادئ قانونية أساسية وراسخة في القانون الدولي، مثل السيادة والسلامة الإقليمية للدول، وعدم التدخل في شئون الدول، وكذلك يتعارض مع إنماء العلاقات الودية بين الدول، وجاء الاتجاه الفقهي الثالث ليقرر بأن التجسس لا هو قانوني ولا هو غير قانوني، وأن وضعه لا يزال غامضًا، فلا توجد أي اتفاقية دولية تحظره أو تجيزه، وتدل الممارسات الدولية على أن الدول تعتبره غير مقبول ولكنه ليس محظورًا.

وتُثار خصوصية التجسس من البحار، بمناسبة النص في اتفاقية الأمم المتحدة لقانون البحار لعام ١٩٨٢، على حظر جمع المعلومات من قبل السفن والغواصات، التي تمر في البحار الإقليمية والمضايق للدول الساحلية وقت السلم، وكذلك اعتراف المادة (٨٧) من الاتفاقية، بحق الأطراف في حرية الملاحة والتحليق، وغيرها من الاستخدامات المشروعة، المرتبطة بتشغيل السفن والطائرات في أعالي البحار،

والتـي يُمكـن فهمهـا باعتبـار أن سلوك جمـع المعلومـات يُمثّـل أحـد عناصـر هذا الحـق، لاسـيما أن السـفن والطائرات في منطقة أعالي البحار تخضع وبشكل حصري لقوانين دولة العلم.

وترتيبًا على ما سبق، فإننـا نـوالي دراسـة سلوك التجسس فـي القـانون الـدول من خـلال المباحث التالية:

المبحث الأول: ماهية التجسس وأنواعه ودوافع ممارسته.

المبحث الثاني: الوضع القانوني للتجسس في القانون الدولي.

المبحث الثالث: خصوصية تنظيم سلوك التجسس من البحار وقت السلم.

المبحث الأول

ماهية التجسس وأنواعه ودوافع ممارسته

تنوعت تعريفات "التجسس" وتعدَّدت سواء في اللغة، أم الاصطلاح، أم الفقه، أم القواعد الدولية، وتمحور معظمها حول إتيان هذا السلوك وقت النزاعات المسلحة، مع التركيز على القائم بالنشاط، وهو الجاسوس الذي يتم إرساله في سرية من قبل دولة، وباستخدام مظاهر كاذبة أو تحت تَخَفٍ، لجمع معلومات سريّة غير مُصرَّح بجمعها، ثم نقلها إلى طرف آخر، وهي الطريقة التي يُطلق عليها "الذكاء البشري"[1]. كما نلمح من خلال الواقع العملي، وجود تشابه بين ممارسة التجسس وبعض المصطلحات، مثل العمل السري، والاستخبارات، مما يتطلب وفقًا لأغراض الدراسة، تعريف كل منها والتمييز بينها. **ونوالي دراسة ذلك من خلال المطالب التالية:**

المطلب الأول: تعريف التجسس والتمييز بينه وبعض المصطلحات التي قد تتشابه معه.

المطلب الثاني: أبرز وسائل التجسس.

المطلب الثالث: أهم دوافع ممارسة التجسس دوليًا.

المطلب الأول

تعريف التجسس والتمييز بينه وبعض المصطلحات التي قد تتشابه معه

تنوَّعت تعريفات التجسس والجواسيس، وتأثرَّت بالجهة التي أوردتها، وعندما نستعرض تلك التعريفات، نلاحظ أنها قد تتشابه مع بعض المصطلحات الأخرى كالاستخبارات والعمل السري، والتي ربما يتم الخلط بينها وبين سلوك التجسس، ونوالي دراسة تعريف التجسس والجواسيس، ونميز بين ما قد يشتبه بسلوك التجسس من مصطلحات، وذلك من خلال الفروع التالية.

الفرع الأول

تعريف التجسس

أولاً: التجسس في اللغة:

---

(1) ***N. SOLCE**, the Battlefield of Cyber Space: The Inevitable New Military Branch – The Cyber Force, Alb. L.J. Sci. & Tech. 18, 2008, PP. 296:297.*

يُرَدّ "مصطلح التجسس" إلى الفعل "جَسّ"، والاسم منه: التَجَسُّس، والمصدر تَجَسَّسَ، والمفعول مُتجسَّس، و"جَسُّ الخبر": بحث عنه واستطلعه وفحصه، وتجسَّس الشَّخصَ على الشَّخصِ: قام بجمع المعلومات عنه، وتَجَسَّسْتُ فلانًا: بحثت عنه، والتَّجَسُّسُ: التفتيش عن بواطن الأمور، والجاسُوسُ: العين يَتَجَسَّسُ الأخبار ثم يأتي بها"، وَتَجَسَّسَ عَلَيْهِمْ فِي عَمَلِهِمْ: جَاءَ يَسْتَطْلِعُ أَخْبَارَهُمْ وَأَسْرَارَهُمْ وَتَعَرُّفُها لِيَنْقُلَهَا إِلَى مَنْ يَهُمُّهُ الأَمْرُ. كما يُعبّر فعل جَسُّ عن: المَسُّ باليَدِ، وقَامَ بِجَسِّ نَبْضِهِ: لَمْسِهِ وَتَحَسُّسِهِ، وجَسَّ الطَبِيبُ نَبْضَ الْمَرِيضِ: لَمَسَهُ لِيَتَعَرَّفَ دَقَّاتِهِ، وجَسَّ الأَرْضَ: وَطِئَهَا، وفَحْصِهِ، وجَسَّ نَبْضَ الحَالَةِ الرَّاهِنَةِ بَعْدَ الأَحْدَاثِ: اِخْتَبَرَهَا وامْتِحَنَهَا عَنْ قُرْبٍ، سَبَرَ غَوْرَهَا، وجَسَّ الشخصَ بعينه: أَحَدَّ النظر إليه ليَسْتَبِينَه[١].

ثانيًا: التجسس في الاصطلاح:

التجسس: البحث عن العورات والعيوب، وكشف ما ستره الناس، قال ابن الأثير: التجسس هو التفتيش عن بواطن الأمور، وكذلك هو تتبع أحوال الآخرين للاطلاع على أسرارهم، وقيل: هو تتبع الإنسان أخاه ليطلع على عوراته، سواء كان ذلك عن طريق مباشر بأن يتجسس الإنسان بنفسه، أو بوسائل أخري. وقال القرطبي: التجسس هو البحث، ومنه قيل: رجل جاسوس، إذا كان يبحث عن الأمور[٢].

وقد عرَّف قاموس أكسفورد الإنجليزي "*Oxford English Dictionary*"، مصطلح "التجسس" "*Spying*" بأنه: مصطلح يستخدمه العامة أكثر من كونه مصطلح قانوني، ويعني إطلاع شخص أو غيره بطريقة سرية على معلومات ليست متاحة للجميع، أو مراقبة شيء، مع توافر دوافع أو نوايا عدائية بشأن استغلال هذه المعلومات، وغالبًا ما يرتبط التجسس بتوظيف أشخاص للقيام بهذا السلوك، ويُطلق عليهم "جواسيس"، وهم العملاء السريون الذين يراقبون أشخاص أو أماكن أو أحداث، بغرض الحصول على معلومات سرية عندما تسنح لهم الفرصة[٣].

وتجدر الإشارة إلى أن الشريعة الإسلامية قد ذمَّت التجسس، ومن ذلك قول الله تعالى: **"يَا أَيُّهَا الَّذِينَ آمَنُوا اجْتَنِبُوا كَثِيرًا مِّنَ الظَّنِّ إِنَّ بَعْضَ الظَّنِّ إِثْمٌ وَلَا تَجَسَّسُوا وَلَا يَغْتَب بَّعْضُكُم بَعْضًا أَيُحِبُّ أَحَدُكُمْ أَن يَأْكُلَ لَحْمَ أَخِيهِ مَيْتًا فَكَرِهْتُمُوهُ وَاتَّقُوا اللَّهَ إِنَّ اللَّهَ تَوَّابٌ رَّحِيمٌ"**[٤]. وقال عز وجل: **"وَالَّذِينَ يُؤْذُونَ الْمُؤْمِنِينَ وَالْمُؤْمِنَاتِ بِغَيْرِ مَا اكْتَسَبُوا فَقَدِ احْتَمَلُوا بُهْتَانًا وَإِثْمًا مُّبِينًا"**[٥]. وتدل الآيات على حُرمة أذي المؤمنين والمؤمنات، ومن هذا الأذى تتبع عوراتهم والتجسس عليهم.

كما ثبت في الصحيحين، أن أبا هريرة رضي الله عنه قال: قال رسول الله صلى الله عليه وسلم: «إياكم والظن، فإن الظن أكذب الحديث، ولا تَحَسَّسُوا ولا تجَسَّسُوا ولا تنافسوا ولا تحاسدوا ولا تباغضوا، ولا تدابروا وكونوا عباد الله إخوانًا». قال ابن جرير: وَلَا تَجَسَّسُوا: أي ولا يتتبع بعضكم عورة بعض، ولا يبحث عن سرائره، يبتغي بذلك الظهور على عيوبه، ولكن اقنعوا بما ظهر لكم من أمره وبه فاحمدوا أو ذموا، لا على ما لا تعلمونه من سرائره، وذكر أثر ابن عباس: نهى الله المؤمن من أن يتتبع عورات

---

(١) **معجم لسان العرب، ابن منظور (٣٨/٦)**؛ معجم تاج العروس، الزبيدي (٤٩٩/١٥)؛ معجم تهذيب اللغة، الأزهري، (٢٤٢/١٠).
(٢) **التفسير المنير، الزحيلي، (٢٤٧/٢٦).**
(3) ***Oxford English Dictionary,*** *Oxford University Press, 2010, Definition of espionage.*
(٤) **سورة الحجرات، الآية رقم (١٢).**
(٥) **سورة الأحزاب، الآية رقم (٥٨).**

المؤمن. وقال قتادة: هل تدرون ما التجسس، أو التجسس؟ هو أن تتبع، أو تبتغي عيب أخيك لتطلع على سره[١].

وعن أبي برزة الأسلمي رضي الله عنه: قال رسول الله صلى الله عليه وسلم: «يا معشر من آمن بلسانه ولم يدخل الإيمان قلبه، لا تغتابوا المسلمين، ولا تتبعوا عوراتهم، فإنه من اتبع عوراتهم يتَّبّع الله عورته، ومن يتبع الله عورته يفضحه في بيته»[٢].

وقال عبد الله بن مسعود رضي الله عنه: "إنا قد نُهينا عن التجسس ولكن إن يظهر لنا شيء نأخذ به[٣]، قال أبو حاتم البستي: "التجسس من شعب النفاق، كما أن حسن الظن من شعب الإيمان، والعاقل يحسن الظن بإخوانه وينفرد بهمومه وأحزانه، كما أن الجاهل يسيء الظن بإخوانه، ولا يفكر في جناياته وأشجانه"[٤].

ومما سبق نلاحظ أن التجسس في اللغة والاصطلاح، يشير إلى سلوك البحث والتحري عن أمور غير مُتاحة للعيان، والاطلاع على ما يُعد سرًا عند أصحابه، عن طريق وسائل الاستطلاع والاستكشاف، مع توافر دوافع أو نوايا عدائية بشأن استغلال هذه المعلومات، **كما نلاحظ أن التعريفات** قد قصرت ـ إلى حد ما ـ نطاق اقتراف هذا العمل من خلال العنصر البشري، أو تبادل التجسس من قبل الأفراد، بحيث يرتبط بتوظيف أشخاص للقيام بهذا السلوك، ويُطلق عليهم "جواسيس".

ثالثًا: التجسس في الاتفاقيات الدولية:

(١) اتفاقية لاهاي بشأن احترام قوانين وأعراف الحرب البرية لعام ١٩٠٧[٥]:

قرَّرت المادة (٢٤) من اتفاقية لاهاي بشأن احترام قوانين وأعراف الحرب البرية لعام ١٩٠٧، مشروعية أفعال التجسس وقت الحرب، حيث قضت بجواز اللجوء إلى الخدع والوسائل اللازمة لجمع المعلومات عن العدو والميدان[٦]، مثل معرفة الخطط الحربية، وأنواع الأسلحة المستخدمة وعددها، ونظام تعبئة الجيش، وعدد المقاتلين، ومستوى تدريبهم ومعنوياتهم. كما اعتبرت المادة رقم (١/٢٩) من الاتفاقية الشخص جاسوسًا؛ إذا قام أثناء نزاع مسلح، بجمع معلومات أو حاول جمعها، سرًا وتحت إدعاء كاذب، أو تعمد التخفي للحصول عليها، في منطقة عمليات لأحد الأطراف، بنية إبلاغها إلى العدو[٧]. وأخرجت الفقرة الثانية للمادة (٢٩)، من نطاق وصف الجواسيس، أفراد القوات المسلحة الذين يخترقون منطقة عمليات جيش العدو، لجمع المعلومات "علنًا".

(٢) اتفاقية جنيف الرابعة بشأن حماية المدنيين وقت الحرب لعام ١٩٤٩:

---

(١) **صحيح مسلم بشرح النووي.**
(٢) **رواه أحمد وأبو داود وابن حبّان، وصحّحه ابن حبّان والألباني.**
(٣) **أبو معاوية عن الأعمش عن زيد عن عبد الله ابن مسعود، الصحيح المسند، ص ٨٤٥.**
(٤) **روضة العقلاء ونزهة الفضلاء**، محمد بن حبان أبو حاتم البُستي، تحقيق: محمد محي الدين عبد الحميد، دار الكتب العلمية، بيروت، جزء ١، ١٩٧٧، ص ١٢١.
(٥) **دخلت الاتفاقية حيز النفاذ في ٢٦ يناير ١٩١٠**، وتشتمل على ملحق يتضمَّن اللائحة المتعلقة بقوانين وأعراف الحرب البرية.
(٦) **نصَّت المادة (٢٤) من الاتفاقية على أنه:** "يجوز اللجوء إلى خدع الحرب والوسائل اللازمة لجمع المعلومات عن العدو والميدان".
(٧) **نصَّت المادة (١/٢٩) من الاتفاقية على أنه:** "لا يعد الشخص جاسوسًا إلا إذا قام بجمع معلومات، أو حاول ذلك في منطقة العمليات التابعة لطرف في النزاع، عن طريق عمل من أعمال الزيف أو تعمد التخفي بنية تبليغها للعدو".

قرّرت المادة رقم (٦٨) من اتفاقية جنيف الرابعة لعام ١٩٤٩، بأنه يُمكن للدولة المضرورة أن تُعاقب على سلوك التجسس بالإعدام، وبشأن فرض هذه العقوبة على شخص محمي، فإنها لا تكون إلا في حالات إدانته بالتجسس، أو اقترافه لأعمال تخريب خطيرة ضد المنشآت العسكرية التابعة لقوة الاحتلال، أو الجرائم المُتعمَدة التي تتسبب في وفاة شخص أو أكثر[١].

(٣) البرتوكول الإضافي الأول لعام ١٩٧٧، والملحق باتفاقات جنيف لعام ١٩٤٩:

تضمنَّت المادة رقم (٤٦) من البروتوكول بعنوان "الجواسيس"، فقرات أربع[٢]، بيَّنت بعبارات قاطعة أن حُكمها ينطبق فقط على أفراد القوات المسلَّحة الذين يمارسون التجسس[٣]، واعتبرت أن القبض على أي منهم مُتلبسًا بهذا السلوك، يمنعه من التمتع بوضع أسير الحرب، ويجوز أن يعامل كجاسوس، ولا يُعتبر الشخص الذي يقوم بجمع المعلومات أو يحاول ذلك، وهو يرتدي زى قواته المسلحة جاسوسًا، حيث يُشترط أن يُقارف هذا السلوك عن طريق عمل من أعمال الخداع أو التخفي، وكذلك إذا مارس التجسس فرد من القوات المسلحة لطرف في النزاع، ثم عاد إلى الجيش الذي ينتمي إليه، ثم قُبض عليه بعد العودة، فلا يُسأل عن أعمال التجسس التي اقترفها سلفًا، ولا يُعامل كجاسوس، ما لم يتم هذا القبض عليه قبل لحاقه بالقوات المسلحة التي ينتمي إليها.

ونلاحظ على النصوص الدولية المعروضة أنها:

(١) لم تحظر اللجوء لوسائل جمع المعلومات أثناء النزاعات المسلحة، إلا أنها قررت إمكان فرض عقوبة الإعدام عند إدانة أحد باقتراف هذا السلوك، وهو موقف غامض إلى حد ما، حيث لم تحظر السلوك، ثم قرَّرت العقاب على التلبس باقترافه، وربما يُعزى ذلك ولو جزئيًا، إلى وجود اتجاه لحظر التجسس، وقت صياغة تلك الصكوك، إلا أنه لم يكن من الممكن فعل ذلك بشكل فوري، فاتجه الأطراف إلى تحقيق ذلك تدريجيًا، من خلال تقرير هذه العقوبة الجسيمة على ممارسته.

(٢) لم تُعَرّف فعل التجسس صراحةً أو تحديدًا، وإنما أشارت إليه بعبارات غير مُفصَّلة مثل "الوسائل اللازمة لجمع المعلومات عن العدو"، وبالتالي تبقي ماهية هذا السلوك، وأركانه غير محددة في تلك النصوص. كما قصرت جواز ارتكابه على أوقات النزاعات المسلحة، ولم تتطرق إطلاقًا لإمكان

---

(١) **مما نصت عليه المادة (٦٨) من اتفاقية جنيف الرابعة لعام ١٩٤٩ أنه:** "ولا يجوز أن تقضي القوانين الجزائية بعقوبة الإعدام على أشخاص محميين إلا في الحالات التي يدانون فيها بالجاسوسية، أو أعمال التخريب الخطيرة للمنشآت العسكرية التابعة لدولة الاحتلال، أو بمخالفات متعمدة سببت وفاة شخص أو أكثر، .....، ولا يجوز إصدار حكم بإعدام شخص محمي إلا بعد توجيه نظر المحكمة بصفة خاصة إلى أن المتهم ليس من رعايا دولة الاحتلال، وغير ملزم بأي واجب للولاء نحوها. لا يجوز بأي حال إصدار حكم بإعدام شخص محمي تقل سنه عن ثمانية عشر عامًا وقت اقتراف المخالفة".

(٢) **مما نصت المادة رقم (٤٦) من البرتوكول الإضافي الأول لعام ١٩٧٧، أنه:** "١- إذا وقع أي فرد من القوات المسلحة لطرف في النزاع، في قبضة الخصم أثناء مقارفته للتجسس فلا يكون له الحق في التمتع بوضع أسير الحرب ويجوز أن يعامل كجاسوس..، ٢- لا يعد مقارفًا للتجسس فرد القوات المسلحة لطرف في النزاع الذي يقوم بجمع أو يحاول جمع معلومات لصالح ذلك الطرف في إقليم يسيطر عليه الخصم إذا ارتدى زى قواته المسلحة أثناء أدائه لهذا العمل.٣- لا يعد مقارفًا للتجسس فرد القوات المسلحة لطرف في النزاع، ...، ما لم يرتكب ذلك عن طريق عمل من أعمال الزيف أو تعمد التخفي. ٤- لا يفقد فرد القوات المسلحة لطرف في النزاع، ....، حقه في التمتع بوضع أسير الحرب ولا يجوز أن يعامل كجاسوس ما لم يقبض عليه قبل لحاقه بالقوات المسلحة التي ينتمي إليها".

(٣) **بخلاف ما كانت عليه نصوص المواد من (٢٩: ٣١) من اتفاقية لاهاي ١٩٠٧،** التي جاءت صياغتها مطلقة دون قصر على العسكريين، ومن ذلك نص المادة رقم (٢٩) "يمكن أن يعتبر الشخص جاسوسا...."، وكذلك المادة رقم (٣١) "الجاسوس الذي يقبض عليه بواسطة العدو..." وهي نصوص يمكن أن تفسر على أنها تعنى الجاسوس العسكري أو الجاسوس المدني.

ارتكابه في أحوال أخري، وعالجت ممارسته من قبل الأشخاص الطبيعيين "الجواسيس"، ولم تتطرق إلى أي وسائل أخرى له، كالتجسس من خلال الفضاء السيبراني أو بوسائل تقنية حديثة.

(٣) اشترطت في طريقة جمع المعلومات أن تكون سرَّية وباستخدام مظاهر كاذبة وزائفة، ولم تنص على أن تكون المعلومات في حد ذاتها سرَّية، وبالتالي فإن السلوك السري لجمع المعلومات هو أحد عناصر التجسس، أما المعلومات فإنها قد تكون غير سرية، كعدد جنود معسكر ما، ومستوى تدريبهم، ودرجة معنوياتهم، وقد تكون سرَّية، مثل التخطيط العسكري، وأنواع الأسلحة، ونظام تعبئة الجيش. ودعمًا لهذا الفهم، قرّرت تلك الصكوك منح وضع أسير الحرب، للجندي الذي يُقبض عليه مُتلبسًا بالتجسس، أو يحاول ذلك، وهو يرتدي زيه العسكري، ولا يُعتبر جاسوسًا، حيث إنه يُشترط أن يقترف التجسس عن طريق أعمال الخداع أو تعمد التخفي.

(٤) قرَّرت صفة الجاسوس للشخص الذي يتم القبض عليه مُتلبسًا، حال ارتكابه أعمال التجسس في منطقة تحت سيطرة الدولة المُعادية، مع قصده جمع المعلومات بغرض إبلاغها إلى العدو، ولم تتطرق لكون هذا الشخص يفعل ذلك لغايات أخري، مثل محاولة تدوين الواقعة، أو نشر مقال علمي، أو تأليف كتاب أكاديمي، وبالتالي فإنه إذا أمكن إثبات القصد من الفعل في هذه الحالات، لا يُمكن وصف القائم بها بأنه جاسوس.

رابعًا: التجسس في الفقه:

يُمكن تقسيم آراء الفقه الدولي بشأن التجسس إلى فئتين، الأولي: تقصر هذا السلوك على وقت النزاعات المسلحة، والثانية، تُعرِّفه بوجه عام، دون قصره على وقت معين، ونعرض لذلك على النحو التالي:

(١) تعريف التجسس بالاقتصار على وقت النزاعات المُسلَّحة:

قرر جانب فقهي أن القانون الدولي قد تناول سلوك التجسس من خلال بيان وضع الجواسيس، باعتبارهم وكلاء غير رسميين لدولة، يتم إرسالهم في أوقات النزاعات المسلحة، للحصول سرًا على معلومات عن مسائل عسكرية أو سياسية أو صناعية، أو غيرها، ولأغراض العلاقات الدولية، لا يمكن الاعتراف بهؤلاء الجواسيس كوكلاء للدول، ولا يتقرر لهم أي حصانة أو حماية من قبل الدولة المُرسِلة[١].

وبيَّن جانب فقهي أن التجسس يُعبّر عن السعي أثناء نزاع مسلح باستخدام السريّة، والتمويه، والادعاءات الكاذبة، للحصول على معلومات بقصد إبلاغها للعدو، ويعاقب الجاسوس بالقتل، سواء نجح أو لم ينجح في الحصول على المعلومات، أو نقلها إلى العدو أو لم يتمكن[٢].

وميَّز جانب من الفقه بين نوعين من التجسس، الأول الذي يتم بواسطة "جاسوس محارب"، والثاني، يقترفه جاسوس غير محارب، فالأول ضابط أو جندي من جيش معادي يحصل سرًا، أو يسعى للحصول على معلومات، داخل منطقة عمليات عسكرية لصالح جيشه، و"الجاسوس غير المحارب"؛ إما مدني في دولة محاربة يعمل سرًا في أي مكان، أو جاسوس عسكري يعمل متخفيًا داخل المناطق الداخلية

(1) ***A. J. RADSAN****, the Unresolved Equation of Espionage and International Law, 28 MICH. J. INT'L L. 595, 2007, P. 610.*
(2) ***D. B. HOLLIS****, An e-SOS for Cyberspace 52 (2), Harvard International Law Journal, 2011, P. 370.*

للدولة المتحاربة[١].

وعُرَف كذلك بأنه، جمع معلومات في أوقات الحروب، بواسطة أشخاص مدنيين أو عسكريين، بوسائل خفية وغير مُصرَّح بها، داخل أراضي دولة أجنبية دون علمها أو موافقتها، ثم يُرسلونها سرًا إلى حكوماتهم، أو إلى أشخاص، أو كيانات معادية للدولة التي أُرسلوا إليها، مع وعيهم التام بطبيعة ما يمارسونه من خداع[٢].

واعتبر جانب فقهي أنه ينطوي على حصول عملاء لدولة عمدًا، على معلومات سرية ذات أهمية للأمن الوطني لدولة أخرى معادية، بمناسبة عمليات عدائية بين الدولتين، وقد يتم ذلك من خلال مواطنين خونة يتم تجنيدهم وتطوير إمكاناتهم، من خلال عملاء للدولة المعادية أو جواسيس لها[٣].

(٢) تعريف التجسس بوجه عام دون قصره على وقت النزاعات المُسلَّحة:

قرَّر جانب فقهي أن التجسس نشاط يتم بوسائل سريَّة وخادعة، تُشكّل في حد ذاتها مخالفة للقانون الدولي، ويمارسه بعض الأفراد نيابة عن الدول، بغرض جمع معلومات سرية تتعلق بالدولة الضحية، وإذا أمكن إسناد أفعال هؤلاء الوكلاء إلى دولة، فإن ما قد يرتكبونه بمناسبة ممارستهم للتجسس يُسند إليها، حتى وإن كان قد تم بالتجاوز لما كُلّفوا به[٤]. كما أنه يعني قيام دولة بإرسال وكلاء إلى دولة أخرى سرًا، لجمع معلومات تتعلق بقدراتها وأنشطتها، باستخدام الخداع، مع كون هؤلاء الوكلاء غير مصرح به لهم بذلك[٥].

وعُرف كذلك، بأنه عمليات تستهدف جمع معلومات سرية، مع اتجاه إرادة المخططين لها والقائمين بها بتوقي اكتشاف أمرهم، ثم القيام بتحليل هذه المعلومات وتقييمها ومعالجتها، بحيث يمكن اتخاذ قرارات بناءً عليها، لاسيما في مجالات صنع السياسات الحكومية[٦].

وهو إدارة وسائل وآليات تنطوي على انتهاك قوانين دولة أخرى وسيادتها، لجمع معلومات عنها[٧]، وهذه الآليات "دورية" و"متصلة"، حيث تتألف من مراحل مختلفة كالتخطيط، والحصول على المعلومات، ونقلها، ثم تحليلها ومعالجتها، ثم الاستفادة منها، ويشير مصطلح "دورية" إلى استمرارية

---

(1) ***L. S. EDMONDSON**, Espionage in Transnational Law, 5 Vanderbilt Journal of Transnational, 1972, P. 415.*
(2) ***M. BURN,** the Debatable Land: a Study of the Motives of Spies in Two Ages, Hamilton Publisher, 1970, PP. 2: 4.*
(3) ***L. T. COL, G. B. DEMAREST**, Espionage in International Law, DENV. J. INT'L L. & POLY, VOL. 24, Issue: 2, 3, 1996, P. 323.*
(4) ***A. J. RADSAN**, the Unresolved Equation of Espionage and International Law, P. R., PP. 613: 615.*
(5) ***L. K. JOHNSON**, Preface to Strategic Intelligence: Understanding the Hidden Side of Government, Loch K. Johnson ed., 2007, P. 70.*
(6) ***L. TRUST, M. ROSCINI**, Cyber Operations and the Use of Force in International Law, OUP, 2014, PP. 12,240: 241.*
(7) ***R. BUCHAN**, the International Legal Regulation of State-Sponsored Cyber Espionage, P. R., PP. 68.*

الأفعال المكونة للتجسس وتأثير كل خطوة على الأخرى، مع إمكان إطلاق "التجسس" على أي جزء من الدورة، سواء التخطيط، أو الجمع، أو التحليل، أو تحديد المعلومات التي تمثل أولوية[١].

وعُرِّف بأنه نشاط تقرر حكومة دولة القيام به، لجمع معلومات غير مُعلنة، وغير مُصرَّح بالاطلاع عليها، من خلال إرسال فرد أو مجموعة أفراد لإقليم دولة أخرى للحصول على هذه المعلومات، واستخدامها لاحقًا للتأثير على الأوضاع السياسية والاقتصادية والعسكرية للدولة الضحية، مع حرص الدولة القائمة بالتجسس ألا يكون دورها ظاهرًا أو علنيًا[٢].

ويعني كذلك إرسال الدول عملاء لها لجمع معلومات سريَّة ونقلها، باستخدام الخداع والتمويه، ويكون هؤلاء العملاء مسئولين جنائيًا وبشكل شخصي أمام الدولة المُستهدفة، وعندما تكافح دولة مضرورة تجسس دولة أخرى، فإن هذا الوضع يُطلق عليه "التجسس المضاد"، ونتيجة للتطور التكنولوجي، صار يتم باستخدام وسائل تقنية، بحيث لم يعد الوجود المادي للجواسيس في الإقليم المستهدف ضروري مُتطلبًا[٣].

ويبيّن جانب فقهي أن التجسس يتأسس على أركان ثلاثة: "العنصر المادي أو "السلوك"، و"القصد"، و"العنصر الموضوعي"؛ ويتحقّق العنصر المادي بانتقال شخص من دولته إلى خارجها لاقتراف التجسس، مع اتجاه إرادته وتعمده القيام بهذا النشاط، وهذا هو عنصر "القصد"؛ ويتحقَّق العنصر الموضوعي بأن تستفيد دولة في سياساتها ومصالحها بالمعلومات المُتحصل عليها، في مقابل ضرر للدولة التي نُفذ فيها التجسس[٤].

وبتحليل العرض السابق يمكننا ملاحظة ما يأتي:

(١) تمحورت التعريفات الخاصة بالتجسس وقت النزاعات المسلحة على القائم بالنشاط، وهو الجاسوس الذي يتم إرساله لجمع معلومات غير مُصرَّح بجمعها، ونقلها إلى طرف آخر، وهو نفس نهج القواعد الدولية المُنَظِمة للتجسس وقت الحرب، حيث ركَّزت على الجواسيس ووضعهم القانوني، ولم توضّح ماهية السلوك نفسه. أما للتعريفات الخاصة بالتجسس بوجه عام، فهي لم تُضف جديدًا على نظيراتها الخاصة بالتجسس وقت النزاعات المسلحة، وإنما قرّرت نفس النهج والمعاني، مع عدم تحديد وقت معين لاقتراف التجسس.

(٢) تناولت التعريفات المظاهر التي تُثبت صفة الجاسوس، وهي ممارسة التجسس باستخدام أساليب تمويه وخداع وإدعاء كاذب، بحيث لا يمكن تمييزه كعدو، وبما يعني أن الخداع والادعاء الكاذب هو جوهر سلوك التجسس وقت الحرب، ويؤكد ذلك، أنه إذا اقترف أحد أفراد القوات المسلحة التجسس وهو يرتدي زيه العسكري، فإنه لا يُعد "جاسوسًا"، ويُعتبر فرد استطلاع، وفي حالة احتجازه يتمتع بوضع أسير الحرب.

---

(1) ***T. LANSFORD****, Multinational Intelligence Cooperation, in: Countering Terrorism and Insurgency in the 21st Century, International Perspectives, James J.F. Forest ed., 2007, P. 419.*

(2) ***J. E. PRETZ, R. J. STERNBERG,*** *Cognition and Intelligence: Identifying the Mechanisms of the Mind, Cambridge University Press, 2005, PP. 12:15.*

(3) ***O. A. HATHAWAY, et al****., the Law of Cyber-Attack, P. R., PP. 855: 356.*

(4) ***R. D. WILLIAMS****, (Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action, 79 GEO. WASH. L. REV., 2011, PP. 1162: 1164*

(٣) ركَّزت التعريفات جميعها على وسيلة واحدة من وسائل التجسس وهي المصادر البشرية، أو الذكاء البشري، ولم تأخذ في الاعتبار وسائل جمع المعلومات بطرق تقنية حديثة، لاسيما التجسس الذي يتم من خلال تكنولوجيا الاتصالات والمعلومات، وبالتالي لا يدخل سلوك التجسس من خلال الفضاء السيبراني ضمن تنظيم تلك القواعد، حيث إنه لا يعتمد على العنصر البشري المُتسلّل إلى الدولة المضرورة، لممارسة نشاطه السري، وإنما يتم بواسطة أجهزة تقنية متطورة[١].

(٤) اعتبرت بعض التعريفات أن التجسس يشمل مرحلة جمع المعلومات، ثم نقلها، ثم تحليلها والاستفادة منها، بينما من الناحية الفنية، يقتصر نشاط التجسس على جمع المعلومات فقط، أما الأنشطة الخاصة بتحليل المعلومات المُتحصل عليها، أو معالجتها فلا تدخل ضمن إطار عملية التجسس، وتندرج ضمن مرحلة أخري يُطلق عليها الاستخبارات، وهو ما يقودنا إلى التفرقة بين سلوك التجسس وما قد يشتبه به من مصطلحات أخري كالاستخبارات، وذلك من خلال الفرع التالي.

الفرع الثاني

التمييز بين التجسس وبعض المصطلحات التي قد تتشابه معه

أولاً: التجسس "*Spying*" والعمل السري "*Covert Action*":

قد يتم الخلط بين سلوكي التجسس والعمل السري، وقد يعتبرهم البعض مترادفين، وهي نظرة غير صحيحة، حيث إن بينهما اختلاف جوهري، يتمثل في أن "العمل السري"، لا يهدف إلى جمع معلومات، أو تحليلها والاستفادة منها، وإنما هو فعل يتم القيام به لإحداث تأثير فعلي على أرض الواقع، لتحقيق مصلحة وطنية من وجهة نظر الدولة الفاعلة، وعلى سبيل المثال يُعد من قبيل العمل السري؛ تدمير محطات الطاقة لدولة ما، كما حدث في "نيكاراجوا" بغرض تقويض نظام "ساندينيستا"، وكذلك اغتيال قادة أجانب، ونشر أخبار ودعاية مناهضة للشيوعية في دول تحت سلطة الاتحاد السوفيتي السابق أثناء الحرب الباردة[٢].

وقد أُثيرت إشكاليات تتعلَّق بالعمل السري لأجهزة المخابرات الوطنية، بعد الكشف في منتصف الثمانينيات، عن ممارسة وكالة المخابرات المركزية الأمريكية "*CIA*"، لهذا النوع من النشاط منذ الحرب العالمية الثانية، والذي اتخذ أشكالاً متعدّدة، منها توفير المال والدعم السياسي لأحزاب سياسية، في انتخابات بعض الدول الأجنبية مثل "إيطاليا"؛ وإنشاء منصات دعاية ونشر لأفكار معينة في دول أخري، مثل إذاعة أوروبا الحرة، والقيام بمحاولات اغتيال قادة دول أجنبية، مثل "فيدل كاسترو"، والقيام ببيع أسلحة إلي دول يُشتبه بصلتها بأنشطة إرهابية مثل "إيران"، مقابل إطلاق سراح رهائن أمريكيين، وتدريب متمردين مثل "كونترا" في "نيكارجوا"[٣].

ويمكننا ملاحظة أن مرحلة جمع الجواسيس لمعلومات سرية ونقلها إلى دولهم، لا تتضمن مثل هذه الأعمال السرية، إلا أن العمل السري قد يحتاج إلى معلومات التجسس حتى يتم بنجاح، كأن يتم

---

(1) ***R. A. FALK, R. J. STANGER,*** *Essays on Espionage and International Law, Columbus, OH: Ohio State University Press, 1962, P. 51.*
(2) ***L. K JOHNSON****, On Drawing a Bright Line for Covert Operations, 86 AM. J. INT'L L., 1992, P. 784.*
(3) ***R. A. FALK,*** *CIA Covert Actions and International Law, 12 Soc'Y, 1975, PP. 39:44.*

اعتراض مراسلات واتصالات مؤسسة معينة، أو نظام معين، أو أفراد محددين، أو معرفة عَدَد المعدات في منشأة عسكرية، بغرض استهدافها بأعمال سريَّة.

(٢) "التجسس" "*Spying*" و"الاستخبارات" "*Intelligence*":

قرّر بعض الفقه أن مصطلح "الاستخبارات"، يُعبّر عما هو أوسع من سلوك جمع معلومات سرية، حيث يشير إلى أكثر من مرحلة من مراحل عمل أجهزة المخابرات، فهو يشمل جمع المعلومات، إضافة إلى تحليلها، ثم تقييمها، لمعرفة سبل الاستفادة منها، ولهذا تَفْصِل معظم أجهزة الاستخبارات بين عمليات جمع المعلومات، ومرحلة معالجتها؛ بحيث يختص الجواسيس بجمع المعلومات، ثم يتولى فنيون مُتخصّصون تحليلها[١]، ومن ثم، يشمل مُصطلح الاستخبارات مرحلتي جمع المعلومات، والنتائج التي تم استخلاصها من هذه المعلومات[٢].

وينتقد جانب فقهي استخدام الاستخبارات كمرادف للتجسس، باعتبار أن الاستخبارات أعم وأشمل، حيث **تتضمن شقين: الأول؛** المعلومات السرية التي يتم الحصول عليها بطرق متنوعة، كالتنصت على الاتصالات، وفك الشفرات وقراءتها، والذكاء البشري، وغيرها من وسائل جمع المعلومات، **ويتمثل الشق الثاني** في ناتج عملية تحليل هذه المعلومات، وفهمها بغرض توجيه عمل ما[٣]، فالاستخبارات هي الناتج النهائي المرجو من أجهزة المخابرات الوطنية، وبما يشمل جمع وتفسير ومعالجة وتقييم وتحليل المعلومات المتاحة، بشأن الدول الأجنبية والقوى المعادية، أو التي من المُحتمل أن تكون معادية، أو التهديدات الفعلية أو المحتملة، ودعم وتعزيز عملية صنع القرارات الملاءمة للرد علي تلك التهديدات[٤].

ومن العرض السابق نستنبط أنه:

(أ) لا يقتصر مصطلح "الاستخبارات" على المعلومات التي جُمعت فقط، وإنما يصف الناتج النهائي من جمعها ومعالجتها وتقييمها وتحليلها، حتى تصير صالحة للاستخدام في مجال معين، لاسيما أغراض حفظ الأمن القومي للدول، وينبغي التمييز في هذا الشأن بين نشاط الدول الخاص بجمع المعلومات السرية، غير المُصرَّح بالاطلاع عليها، وغيرها من المعلومات المُتاحة للكافة، ويُمكن جمعها من البحث عبر الإنترنت، ومراسلي الأخبار، ووسائل الإعلام، والكتب والأبحاث، وغيرها من وسائل المعرفة.

(ب) يُمثّل التجسس جزء من دورة استخبارات تُنتج معلومات نهائية، لازمة لصانعي القرارات، وواضعي السياسات، وغالبًا ما تنصَّب المناقشات القانونية بشأن الاستخبارات عمومًا على مرحلة جمع المعلومات، لا تحليلها، باعتبار أن عملية الجمع هي التي قد تُمثّل تدخلاً في شئون الدول، أما مرحلة "التحليل"، فلا يبدو أنها تثير في حد ذاتها قضايا مهمة في العلاقات بين الدول.

---

(1) ***K. J. WHEATON, M. T. BEERBOWER***, *Toward a New Definition of Intelligence, 17 STAN. L. & POL'Y REV., 2006, P. 319.*

(٢) **وهو نفس المعنى الذي أوردته محكمة أمن الدولة العليا الخاصة المصرية**، في حكمها في القضية رقم (٢٠٢) عليا، لسنة ١٩٦٠، ص ١٢، من أن مهمة المخابرات تتضمن جمع المعلومات وتقديرها جزءًا جزءًا، وتجميعها، حتى تتكون منها صورة أكثر وضوحًا، يمكن من خلالها رؤية الأشياء الواقعة أو المتوقعة.

(3) ***S. CHESTERMAN***, *We Can't Spy If We Can't Buy! the Privatization of Intelligence and the Limits of Outsourcing Inherently Governmental Functions, The European Journal of International Law, Vol. 19, No. 5, 2008, P. 1057.*

(4) ***D. PUN***, *Rethinking Espionage in the Modern Era, P. R., P. 353.*

المطلب الثاني

أبرز وسائل التجسس

إذا كان الهدف من التجسس هو الحصول على معلومات سرية، فإن وسائل القيام بذلك تتنوع وتختلف، ما بين الاعتماد على العنصر البشري، أو على التكنولوجيا الحديثة، ونبيّن ذلك من خلال الفروع التالية:

الفرع الأول

التجسس البشري أو الذكاء البشري

يُستخدم مصطلح الاستخبارات البشرية، أو الذكاء البشري "*Human intelligence* " "*HUMINT*"، للتعبير عن جهود الحصول على معلومات سرية للدول، بالاعتماد على أشخاص مُدربين على الانخراط في ذلك سرًا، سواء في زمن السلم أم الحرب[١]، وسواء كانوا ممن يحملون جنسية الدولة المُستهدفة أم لا، من مدنيين وعسكريين، ومتطوعين لديهم استعداد للانخراط في التجسس لصالح الغير[٢]، كما يندرج تحت هذه الفئة أيضًا، أولئك الذين يدلون بمعلومات لها صفة السرية دون تبصر أو قصد، أو عند استجوابهم، أو المعلومات التي تحصل عليها سلطات دولة من اللاجئين إليها، أو من خلال مقابلات مع رجال أعمال أو سائحين، أو العائدين من دول أجنبية، أو مقالات صحفيين ومقابلاتهم[٣].

الفرع الثاني

التجسس التقني

يُجسّد هذا النوع من التجسّس أحد حالات تسخير التكنولوجيا للقيام بجمع معلومات سرية، ويندرج تحته أنواع عدة، لعل أبرزها:

أولاً: تجسس الاتصالات والإشارات " *Signal- Communication intelligence* **" "** *SIGINT COMINT* **":**

برز هذا النوع من التجسس مع ظهور تكنولوجيا الاتصالات، التي تُتيح إرسال رسائل صوتية ومرئية، سواء بحالتها العادية، أم في صورة مُشَفّرة، فوجَّهت الدول قدراتها الالكترونية، لمراقبة ورصد هذه الإشارات، ثم اعتراضها وفك شفرتها، والحصول على ما تتضمنه من معلومات، وبما يشمل إشارات الراديو، والاتصالات السلكية، أو اللاسلكية، وإشارات الأقمار الصناعية، أو التنصت على الهواتف الخاصة بالأفراد والكيانات[٤]. ويُرجع جانب من الفقه تفوق الولايات المتحدة الأمريكية، على الاتحاد

---

(1) ***R. BUCHAN,*** *Cyber Espionage and International Law, P. R., P. 3.*

(2) ***U.S. Dep't of the Army,*** *Human Intelligence Collector Operations, FM 2-22.3, 2006, PP. 1: 4.*

(3) ***L. T. COL, G. B. DEMAREST****, Espionage in International Law, P. R., PP. 323: 326.*

(٤) **قدَّم سكرتير عام الأمم المتحدة عام ١٩٧٣، تقريرًا إلى المجلس الاقتصادي والاجتماعي،** يشرح فيه تطور وسائل المراقبة، ومجال الالكترونيات، وتأثير ذلك على الأنماط الاجتماعية، وأوضح أنه صار من السهل نسبيًا سماع الشخص ورؤيته، وتسجيل صوته وتصويره دون علمه، سواء في الأماكن العامة أو في الأماكن التي يعتقد أنها مأمونة. **راجع:**
Report of the Secretary General, *Human Rights and Scientific and Technological Development, U.N. Economic and Social Council, E/Cn. 41116, 23 January, 1973, Part I, P. 9.*

السوفيتي السابق في مجال الاستخبارات، إلى سبق الأولي في الاعتماد على وسائل التجسس التقنية، لاسيما بواسطة الطائرات والأقمار الصناعية[١].

وتمارس بعض أجهزة المخابرات الوطنية، هذا النوع من التنصت بشكل روتيني، ووفقًا للتشريعات الوطنية، ومن ذلك، جهاز خدمات الاستخبارات الكندية " *Canadian Security Intelligence Service*" "*CSIS*"، الذي قدَّم مسئولوه طلبًا عام ٢٠٠٨ إلى المحكمة الكندية العليا، بموجب القسم رقم (١٢) من قانون خدمات الاستخبارات الكندي لعام ١٩٨٤، للحصول على تصريح باعتراض الاتصالات الخاصة بأفراد متواجدين داخل أراضي دول أخرى، وبما يشمل تركيب أجهزة ومعدات للوصول إلي هذه الاتصالات والتنصت عليها[٢].

وفي يونيو من عام ٢٠١٣، كشف "*Edward Snowden*" المتعاقد السابق مع (*NSA*) الأمريكية، أن الوكالة وعلى مر سنوات، قامت بعمليات تجسس الكتروني مُمنهَج ومستمر، على دول، وجهات حكومية، وغير حكومية أجنبية، من خلال اعتراض الإشارات، والمراسلات الإلكترونية، والاتصالات الهاتفية، ومن أبرز الجهات التي أُستهدفت؛ مقرات اتصال الحكومة البريطانية، ومسئولين في منظمات دولية كالاتحاد الأوروبي، وممثلي دول كالمستشار الألمانية "أنجيلا ميركل"، وزعماء دينيين "البابا"، وشركات نفط برازيلية "بيتروباس"، ومنظمات غير حكومية كاليونيسيف، وأطباء حول العالم، وبعض الأفراد المُشتبه بتورطهم في عمليات إرهابية[٣].

ثانيًا: التجسّس السيبراني "*Electronic Intelligence* " "*ELINT*"[٤]:

ويعني جمع معلومات من خلال الفضاء السيبراني، باستخدام حاسبات آلية متصلة بشبكات الانترنت، ومن أي مكان في العالم، دون تَطَلُّب تواجد أفراد أو مجموعات في مكان توافر المعلومات أو على إقليم الدول المُستهدفة، ومن ثم، فإن كل ما يتطلبه هذا النوع من التجسس، هو بنية تحتية الكترونية، عبارة عن حاسبات آلية مُتصلة بشبكة الانترنت، وبرامج تشغيلها[٥].

ثالثًا: الاستخبارات الفوتوغرافية أو من خلال التصوير "*Imagery intelligence*" "*IMINT*":

وهو جمع المعلومات بواسطة التصوير الفوتوغرافي سواء الأرضي أم الجوي، وغالبًا ما يرتبط هذا النوع من التجسس بالأماكن والمنشآت والمناطق أو الأشياء التي تحتاج إلى استطلاع واستكشاف[٦].

---

(1) ***Hearings on Missiles,*** *Space and other Major defense Matters, before the subcommittee on the Armed Forcos of the U.S. Senate, 86th Cong. 1960, P. 70.*

(2) ***Re Canadian Security Intelligence Service Act*** *[2008] FC 301, [2008] 4 FCR 230, paras 50:52.*

(٣) **استخدمت (*NSA*) برنامج "*PRISM*"، لمراقبة (٣٥) دولة**، وتذرَّعت بأنه نشاط إعلامي وليس تجسسًا، وأنه أمر قانوني ومصرَّح به وفقًا للتشريعات الأمريكية، ولا يتم إلا بعد استيفاء إجراءات قانونية، ورقابة "الكونجرس"، والقضاء الأمريكي. **راجع:**

D. PUN, *Rethinking Espionage in the Modern Era, P. R., P. 353;* ***SCHMIDT, ERIC,*** *Jared: The New Digital Age. Publisher: John Muray Publishers, UK, 2013, PP. 7, 254: 256.*

(٤) **بشأن تعريف التجسس الالكتروني، راجع:** الفصل الأول، المبحث الأول، المطلب الثاني، الفرع الثالث، ثانيًا.

(5) ***S. TOMAR****, Proxy Warfare, P. R., PP. 15: 20.*

(6) ***H. H. DINNISS,*** *Cyber Warfare and the Laws of War, CUP, 2012, P. 262.*

ووفقًا لما سبق، يمكننا القول، بأن سلوك التجسس قد تطوَّر بظهور الوسائل الالكترونية المختلفة، التي تتيح جمع كم هائل وغير محدود من المعلومات بسرعة ويسر، ودونما تطلب تواجد الجواسيس في مكان وجود المعلومات، على عكس الوسائل التقليدية، التي كانت تعتمد على قدرة ومهارة العنصر البشري والسمات الشخصية للجواسيس، مع تطلب تواجدهم في إقليم الدولة المُستهدفة، وتكون أبرز خصائص التجسس السيبراني، هو تخطيه للحدود المادية والجغرافية، بحيث يتم القيام به من أي مكان في العالم.

المطلب الثالث

أهم دوافع ممارسة التجسس دوليًا

صارت ممارسة التجسس أمر واقع وحقيقة لا يمكن إنكارها بين الدول، بغض النظر عن مشروعية السلوك، حيث تسعى تلك الدول للحصول على معلومات سريَّة تُمكّنها من الدفاع عن مصالحها، العسكرية، أو الأمنية، أو الاقتصادية، وغيرها[1]، وعلي سبيل المثال، أشار تقرير صادر عن المكتب الأمريكي لبراءات الاختراع، والعلامات التجارية، أن المشروعات الصناعية المُسْتَحدَثة، والمُسجَّلة وفقًا لقواعد الملكية الفكرية، تساهم بأكثر من (٦) تريليون دولار في الناتج المحلي الإجمالي الأمريكي، ويؤدي التجسس عليها وسرقتها إلى خسائر مادية فادحة، علاوة على التكلفة التي يتحملها المستثمرون لمواجهة وتوقي هذا التجسس، والتي تُشير التقديرات إلى أنها تبلغ نحو (٤) أربعة ملايين دولار سنويًا، وبزيادة تقارب ٣٠% كل عام[2]. **وبوجه عام، يكون للدول دوافع متعددة للانخراط في التجسس، ومن أبرزها نورد ما يلي.**

الفرع الأول

تعزيز كفاءة اتخاذ القرارات السياسية والاقتصادية

تسعى الدول للحصول على معلومات تُمكّنها من تقييم ما يجري على الصعيد الدولي، أو ما يُحتمل أن يحدث، والمفاضلة بين خيارات التعامل معه والرد عليه، سواء بالوسائل السلمية أم العدائية، كحالات وقوع اضطرابات أو نزاعات، أو أي تهديدات قد تتأثر بها الدولة، مثل حيازة بعض الدول المعادية لأسلحة دمار شامل، كما تدعم معلومات التجسس قدرة الدول في تحقيق توازن مع باقي القوي الدولية، وتسهم في تحقيق منافع اقتصادية وأمنية، ووفقًا لما قرَّره جانب فقهي، فإن الدول تجمع المعلومات السرية، لتتمكن من اتخاذ قرارات بشأن ردع احتمال شن هجوم مفاجئ عليها؛ أو لتيسير العمل الدبلوماسي، والاقتصادي، والعسكري، والقرارات المتعلقة بحالة العداء عند نشوب نزاع مسلح، وكذلك ردع الأفراد أو الجماعات أو الدول التي تمارس أعمال الإرهاب ضد الدولة، أو لتحقيق المصالح التي تُقدّر الدولة أنها متوافقة مع أمنها القومي[3].

---

(1) ***S. CHESTERMAN**, the Spy Who Came in From the Cold War: Intelligence and International Law, 27 Mich. J. Int'l L.2006, PP. 1071, 1099:1100.*

(2) ***J. FINKLE**, Hacking Is Such a Problem that the Cost of Cyber Insurance is Skyrocketing, VENTUREBEAT (Oct. 11, 2015), **available at:** https://perma.cc/8UFD-Z6MQ. 6/4/2020.*

(3) ***M. WATNEY,** Challenges Pertaining to Cyber War under International Law. Cyber Warfare and Digital Forensics (Cybersec2014), 2014, PP. 1: 5.*

وفي الحالات التي تحتاج فيها الدول إلى اتخاذ قرارات للمفاضلة بين الانخراط في نزاع مسلَّح، أو الاستمرار في المفاوضات بشأن مسألة معينة، كتعيين حدود أو حقوق تجارية؛ تكون معلومات التجسس حاسمة في الحد من حالة عدم اليقين لدى الأطراف، من حيث تكاليف الحرب المتوقعة، والقوة العسكرية للطرف الآخر، والفوائد التي قد تتحقق من الاستمرار في التفاوض، وإذا توافر فهم أفضل للوضع الفعلي، تستطيع الدول حسم أمرها فيما يتعلق بالدخول في نزاع مسلح، أو التمسك بالتوصل إلى تسوية تفاوضية بدلاً من ذلك[١].

ومن الممارسات الدولية بشأن استخدام التجسس لتحقيق مصالح الدول، ما قررته وكالة الاستخبارات الأمريكية، من أن "روسيا" تدخلت للتأثير على نتائج الانتخابات الأمريكية لعام ٢٠١٦، بواسطة أعمال تجسس الكتروني وفقًا لما رأته متوافقًا مع مصالحها[٢]. وكذلك ما عرضه "هنري كيسنجر" وزير خارجية الولايات المتحدة الأمريكية عقب حرب ١٩٧٣، من استعداد بلاده لاستخدام معلومات استخبارية تم الحصول عليها من تجسس للطائرة (*U-2*)، لتهدئة الوضع بين "مصر"، و"إسرائيل"، باعتبار أن هذه المعلومات ذات صلة بحماية الطرفين من أي هجوم مفاجئ بعد الحرب، وبالمثل، ساعدت المعلومات الاستخباراتية لكل من الهند وباكستان على تجنب الحرب في كشمير في عام ١٩٩٠[٣].

الفرع الثاني

المراقبة المتبادلة للامتثال لاتفاقيات الحد من التسلح

ظهر هذا المفهوم في أواخر الستينيات، ومثَّل عاملاً حاسمًا آنذاك في نجاح المفاوضات بين الولايات المتحدة الأمريكية والاتحاد السوفيتي السابق، بشأن إبرام اتفاقيات لضبط القدرات النووية لكل منهما، ويُجسّد هذا المفهوم حق كل دولة طرف في اتفاقية للحد من التسلح، أن تتحقّق بوسائلها الوطنية الخاصة، من المعلومات التي يقدمها الطرف الآخر، بشأن امتثاله للالتزامات المقررة عليه في هذا المجال، بغرض تفادي خطر انعدام الثقة بشأن المعلومات المتبادلة بين الأطراف.

وقد وثَّقت عدة اتفاقات دولية هذا الاتجاه، ومن أبرزها الاتفاقين المُبرمين في "موسكو" من عام ١٩٧٢ بين الولايات المتحدة والاتحاد السوفيتي السابق، وهما معاهدة الصواريخ المضادة للقذائف الباليستية "*Anti-Ballistic Missile Treaty* (*ABM*)"، واتفاق "سالت ١" (*SALT 1*)، وتم النص فيهما على حرية كل طرف في التأكد من امتثال الطرف الآخر لالتزاماته المقررة بموجب الاتفاقين، من خلال ما أُطلق عليه "وسائل التحقق التقنية الوطنية" "*National Technical Means of Verification*"، المتاحة له، بطريقة تتسق مع مبادئ القانون الدولي، مع تعهد كل طرف بعدم التدخل في وسائل الطرف الآخر، وألا يتعمد أي طرف استخدام تدابير إخفاء أو تمويه تعوق تحقق الطرف الآخر

(1) ***J. NZELIBE, J. YOO****, Rational War and Constitutional Design, 115 YALE L.J. 25, 2006, P. 112.*
(2) ***M. A. LUSTED, D. HARRIS,*** *Russian Hacking in American Elections, ABDO, 2019, PP. 43: 45.*
(3) ***A. JAMES,*** *Peacekeeping in International Politics, Springer, 2017, PP. 112, 158: 161*

بواسطة هذه الوسائل[١]، وفي عام ١٩٨٢، أُدرجت أحكام مماثلة في قرار للجمعية العامة بشأن أحكام أساسية لمعاهدة تحظر تجارب الأسلحة النووية[٢].

وبالتالي تُقرّر مثل هذه الاتفاقيات لأطرافها، حق استخدام وسائل التحقق التقنية الوطنية في جمع معلومات خاصة بالتسلح، لغرض التأكد من امتثال الطرف الآخر، وعلى الرغم من عدم صياغة هذا الحق بصورة صريحة، إلا أن النص ينطوي على إمكان تكييف هذا السلوك بشكل أو بآخر، ليكون متسقًا مع مبادئ القانون الدولي، لاسيما على ضوء عدم وجود أي قاعدة دولية تقضي بحظر التجسس صراحةً[٣].

وقد رسَّخت المعاهدات التي أُبرمت لاحقًا، بين الولايات المتحدة والاتحاد السوفيتي السابق، في مجال الحد من الأسلحة، لإتباع أو توسيع نهج معاهدة (*ABM*)، واستخدام وسائل وطنية للتحقق من الامتثال، ومن ذلك معاهدة الأسلحة النووية المتوسطة المدى لعام ١٩٨٧، التي أكدت على نفس صياغة اتفاقية (*ABM*)، وأضافت حقًا للأطراف بتقديم (٦) طلبات سنويًا لتنفيذ "تدابير تعاونية"، بشأن تفتيش قواعد بعض أنواع الصواريخ، والسماح بكشف أسطح جميع الهياكل والمباني الثابتة ذات الصلة، وذلك في غضون (٦) ساعات من قبول الطلب ولمدة (١٢) ساعة، كما أكَّدت المعاهدة على أهمية الوسائل التقنية الوطنية للتحقق، مثل الأقمار الصناعية المُخصّصة للاستطلاع، وموافقة كل طرف على عدم التدخل فيما يتعلق بهذه الوسائل[٤].

كما تضمنت أحكام معاهدة تخفيض الأسلحة الإستراتيجية لعام ١٩٩١، التزامًا على الأطراف بالحد من استخدام التشفير أو التشويش، أثناء عمليات اختبار الصواريخ، لضمان مراقبة الأطراف للامتثال لأحكام الاتفاقية[٥]. واتبعت اتفاقية "السماوات المفتوحة" "*Open Skies Agreement*" لعام ١٩٩٢ في مادتيها (١/١)، (٤/١١) نهجًا أكثر تنظيمًا، حيث نصت على نظام لرحلات مراقبة جوية ـ غير مسلحة ـ على كامل أراضي أطرافها، وحددت عدد الرحلات وأنواع الطائرات المسموح باستخدامها، والتكنولوجيا الفوتوغرافية المُستخدمة، كما وضعت التزامًا بتوفير الصور التي يتم جمعها لأي دولة طرف أخرى[٦].

ويُعلّق جانب فقهي على نهج تلك الاتفاقات، بأن له أثر إيجابي على السلم والأمن الدوليين، حيث يؤدي لزيادة الثقة المتبادلة بين أطراف المعاهدات، عندما تؤكد عمليات التجسس المُتبادلة، أن التعهدات والضمانات المُقدمة من كل طرف دقيقة، وسوف تكون الدول أكثر استعدادًا للتعاون مُستقبلاً، لأن لديها آلية للتأكد من مدى صدق تعهدات الأطراف الأخرى[٧].

---

(1) ***Treaty on the Limitation of Anti-Ballistic Missile Systems,*** *U. S.-U.S.S.R, art. XH, May 26, 1972, 23 U.S.T. 3435, in force Oct. 3, 1972, the United States announced its withdrawal on Dec. 14, 2001).*
(2) ***G.A. Res. 37/85,*** *U.N. GAOR, 37th Sess., Annex, arts. 6-8, U.N. Doc. A/RES?37/85 (Dec. 9, 1982).*
(3) ***C. D. BAKER****, Tolerance of International Espionage: P. R., P. 1105.*
(4) ***Treaty on the Elimination of Intermediate-Range and Shorter-Range Missiles,*** *U.S. - U.S.S.R., art. XII, Dec. 8, 1987 (in force June 1, 1988).*
(5) ***Strategic Arms Reduction Treaty,*** *U.S.-U.S.S.R., art. X, July 31, 1991.*
(6) ***Treaty on Open Skies,*** *Mar. 24, 1992,* ***arts.*** *I(1), 11(4),*
(7) ***N. JUPILLAT****, From the Cuckoo's Egg to Global Surveillance: Cyber Espionage that Becomes Prohibited Intervention, 42 North Carolina Journal of International Law and Commercial Regulation, 2017, PP. 933: 935.*

الفرع الثالث

استخدام الاستخبارات لأغراض الملاحقة الجنائية الدولية

سعي المجتمع الدولي إلي تحقيق العدالة، عند انتهاك أحكام القانون الدولي، من خلال إنشاء المحاكم الدولية، وبالرغم من أن المعلومات السرية لا ينبغي أن تكون أساسًا للإجراءات أمام أي محكمة دولية، إلا أنها مثَّلت إفادة في بعض الحالات، التي يصعب توافر أدلة بشأنها، كالانتهاكات التي تقع أثناء النزاعات المسلحة، وربما يحوز أطراف النزاع معلومات استخباراتية بشأنها، يقبلوا عرضها أمام محكمة دولية، أو التشارك في جزء منها مع المحققين، وقد تُفيد في مجال معرفة شهود لم تكن المحكمة على علم بهم؛ أو حماية شهود تؤثر شهادتهم على سير القضية، أو توفير فهم أفضل للقضية، أو ربما التيقن من نزاهة وشفافية المحكمة نفسها[١].

ويمكن رد استخدام معلومات استخبارات في الملاحقة الجنائية الدولية، إلى تاريخ إنشاء المحكمة الجنائية الدولية ليوغوسلافيا السابقة (*ICTY*)، **حيث تضمنَّت القاعدة رقم (٧٠/ ب) من قواعد المحكمة الإجرائية وقواعد الإثبات فيها أنه:** "إذا قُدمت إلى المدعي العام معلومات على أساس سري، لاستخدامها فقط في الحصول على أدلة جديدة، فإن هذه المعلومات ومصدرها لا يكونا محلاً للكشف، إلا بموافقة من الشخص أو الكيان الذي قدمها، ولا يجوز بأي حال من الأحوال تقديمها كأدلة دون إفصاح مسبق عنها للمتهم"[٢]. وتجدر الإشارة إلي أن المحكمة الجنائية الدولية "لرواندا"، قد اعتمدت حكمًا مماثلاً ضمن قواعدها الإجرائية[٣].

وقد أوضح القاضي "*Richard Goldstone*"، أول مدع عام لمحكمة (*ICTY*)، أهمية هذه المعلومات، بشرط عدم الإخلال بالحماية الإجرائية لحقوق المتهمين، ومراعاة رغبة الدول التي تقدمها في تجنب الكشف عن مصادرها وطرق جمعها[٤]. كما أورد القاضي "*Louise Arbour*" الذي خَلَفَ "*Goldstone*"، كمدع عام، أن القاعدة (٧٠) مهمة ومفيدة للغاية، باعتبار أن الاستخبارات من أي مصدر تُمثّل آلية فاعلة للتوصل إلى أدلة مفيدة، وواقعًا تم تعيين فنيين في وظيفة "محلل معلومات استخباراتية" في (*ICTY*)[٥].

وخلال مرحلة التفاوض على إنشاء المحكمة الجنائية الدولية، أكّد عدد من ممثلي الدول على أهمية إدراج أحكام تتعلق بحماية معلومات الأمن القومي للدول، والتي قد تُعرض علي المحكمة عند نظر قضايا معينة[٦]، ومثلما كان الحال في محكمة (*ICTY*) السابقة، سمح نظام روما الأساسي، للمدعي العام

---

(1) ***P. NICHOLSON****, Int'l Criminal Tribunal for the Former Yugoslavia, The Function of Analysis and the Role of the Analyst within the Prosecutor's Office of an International Criminal Court 6 Feb., 2003).*

(2) ***Int'l Crim. Trib. for the Former Yugo.,*** *Rules of Procedure and Evidence rule 70 (B), 33 I.L.M. 484, U.N.Doc.IT/32/Rev.37 (2006).*

(3) ***Prosecutor v. tIie Ndayambaje and Sylvain Nsabimana,*** *Case Nos. ICTR-96-8-T and ICTR-97-29A-T, (Nov. 15, 2001).*

(4) ***R. GOLDSTONE****, Remarks: Intelligence and the Use of Force in the War on Terrorism, 98 Am. Soc'Y INT'L L. Poc., 2004, PP. 147:148.*

(5) ***L. ARBOUR****, Presentation, History and Future of the International Criminal Tribunals for the Former Yugoslavia and Rwanda, 13 AM. U. INT'L L. REV., 1998, PP. 1495: 1508.*

(6) ***M. A. NEWTON****, the International Criminal Court Preparatory Commission: The Way It Is & the Way Ahead, 41 VA. J. INT'L L., 2000, PP. 204:212.*

للمحكمة، بإبرام اتفاقات تتعلَّق بعدم الكشف عن الوثائق أو المعلومات التي قد يحصل عليها، وأن يستخدمها فقط لأغراض التوصل إلى أدلة جديدة[١]، وواقعًا تزايد قبول المحكمة للقضايا التي تتضمن معلومات استخباراتية، كما أُنشئت وظائف داخل مكتب المدعي العام، لمعالجة وتحليل المعلومات الناتجة عن استخبارات عسكرية[٢].

ويتم التعامل مع المعلومات الاستخباراتية في المحكمة الدولية، من خلال حق المدعي العام أو دوائر المحكمة، في طلب الحصول على معلومات أو المساعدة، مع الالتزام بعدم الإفصاح إلى أقصى حد ممكن عن مصادرها وطرق جمعها. وإذا رفضت دولة الإفصاح عن المعلومات، فعليها أن تخطر المدعي العام أو المحكمة بأسباب قرارها، وتُثبت أن هذه المعلومات تتعلق بأمنها القومي[٣]، لما يستتبع ذلك من الانتقاص من قدرة المحكمة على المضي قُدمًا في القضية، وبالرغم من ذلك، إذا قررت المحكمة أن الأدلة ضرورية لإثبات إدانة المتهم أو براءته، فيجوز لها أن تحيل المسألة إلى جمعية الدول الأطراف، أو إلى مجلس الأمن، إذا كانت الإحالة إلى المحكمة من خلاله، لاتخاذ قرار بشأن الإفصاح عن هذه المعلومات[٤].

وتجدر الإشارة إلى أنه في الواقع العملي، وخلال المحاكمات الجنائية الدولية، تُبدي بعض الدول عدم رغبتها في تقديم معلومات تجسس، أو ربما تواجه صعوبة مواءمة تقديمها أمام المحكمة، ومن ذلك أنه خلال فترة الإبادة الجماعية في "رواندا"، تم إبلاغ "*Romeo Dallaire*"، قائد قوات الأمم المتحدة المتبقية في "كيجالي" بأن الولايات المتحدة الأمريكية لديها معلومات استخباراتية تفيد بوجود مُخطط لاغتياله شخصيًا، وقد علق "*Dallaire*" بأنه ينبغي أن أكون ممتنًا لهذه المعلومات، ولكن إذا أمكن جمع استخبارات بهذه الدقة، فكيف لم تُسجل الولايات المتحدة أو أي دولة أخري، أدلة على الإبادة الجماعية التي تحدث هنا في "رواندا"، لتقديمها إلى المحاكم الدولية لتحقيق العدالة[٥]؟

---

(١) **المادة رقم (٥٤/ ٣/ هـ) من النظام الأساسي للمحكمة الجنائية الدولية.**

(2) ***Public Hearing of the Office of the Prosecutor,*** *Int'l Crim. Court (June 17-18, 2003) (testimony of Peter Nicholson),* ***available at:*** *http://www.icc-cpi.int/library/organs/otp/ph/030714_otpphI s5_PeterNicholson.pdf. 15/7/2019.*

(3) ***Prosecutor v. Tihomir Blaskic,*** *Case No. IT-95-14-T, Judgment on the Request of the Republic of Croatia for Review of the Decision of Trial Chamber II of 18 July 1997, 68 (Oct. 29, 1997).*

(٤) **المادتين رقمي (٧٢/ ٧، ٦، ٥)، (٨٧/ ٧) من النظام الأساسي للمحكمة الجنائية الدولية**، حيث تتضمنان استخدام وسائل تعاونية للتوصل إلى حل، إما بالتفاوض على تعديل الطلب أو الموافقة علي شروط حماية المصلحة المُهددة. **وتجدر الإشارة إلى أنه وفقًا لقواعد (*ICTY*) كانت الدول ملتزمة بالإفصاح عن المعلومات**، بينما وفقًا لنظام روما الأساسي، يحق للدول رفض طلب المحكمة، وتظهر قضية "*Blaskic*" أهمية الاستخبارات في تقديم أدلة تبرئة، وكذلك أهميتها فيما يتعلق بتسبيب الاستئناف الذي انتهي إلى تخفيض العقوبة بالنسبة للمدعى عليه، ومنحه إفراجًا مبكرًا. **راجع:**

R. WEDGWOOD*, International Criminal Tribunals and State Sources of Proof: The Case of Tihomir Blaskic, 11 LEIDEN J. INT'L L., 1998, P. 635;* ***Prosecutor v. Tihomir Blaskic,*** *Case No. IT-95-14-A, Judgment (July 29, 2004).*

(٥) **وكان "*Dallaire*" قد أدلى بشهادته بشأن الإبادة الجماعية في "رونـدا"، أمام لجنة من منظمة الوحدة الأفريقية وأورد** فيها: في الحقيقة هناك أمانة للأمم المتحدة، وهناك أمين عام، وهناك مجلس الأمن، ولكن أعتقد أن هناك شيء فوق كل هذا، كاتفاق دائم بين القوى ذات المصالح الواحدة، بحيث تعمل على اتخاذ قرار قبل وصول أي موضوع إلى مجلس الأمن، وهذه الدول لديها معلومات استخباراتية أكثر من أي وقت مضى، وكانوا يعرفون بالضبط ما يجري في "رواندا"، ولكنهم لم يقدموا أي دليل مما في حوزتهم. **راجع:**

R. DALLAIRE*, Shake Hands with the Devil: the Failure of Humanity in Rwanda, 2003, P.339;* ***Int'l Panel of Eminent Personalities to Investigate the 1994 Genocide in Rwanda and the Surrounding Events****, Rwanda: The Preventable Genocide,* ***15.33*** *(2000),* ***available at:*** *http://www.aegistrust.org/images/stories/oaureport.pdf.16/6/2020.*

ومن ناحية أخري، قد تواجه المحاكم الجنائية الدولية، مشكلة وجود قدر كبير من هذه المعلومات، بصورة قد تُشكك في نزاهة الإجراءات، وذلك على النحو الذي تم الادعاء به في المحكمة الخاصة لسيراليون عام ٢٠٠٤، ودفعت لجنة الدفاع بأنها تُشكّك في نزاهة الإجراءات؛ نظرًا للعلاقة الوثيقة بين رئيس التحقيقات في المحكمة، ومكتب التحقيقات الفيدرالي الأمريكي "*FBI*"[١]، وقد ردَّ مكتب المدعي العام مؤكدًا علي ضرورة إدراك التزاماته في مرحلة التحقيق، والتي منها الحصول على المساعدة الخارجية، ولكنه يلتزم بخط فاصل لا يمكن تجاوزه بين هذه المساعدة وبين تلقي تعليمات من أي كيان، واستشهد مكتب المدعي بنص المادة (٣٩) من القواعد الإجرائية وقواعد الإثبات للمحكمة، من حيث إنه يجوز للمدعي العام أثناء التحقيق، أن يلتمس مساعدة أي سلطة حكومية معنية، أو أي هيئة دولية ذات صلة، بما في ذلك المنظمة الدولية للشرطة الجنائية "الإنتربول"[٢]، **وبالفعل رفضت المحكمة الادعاء بالتشكيك في استقلالية الإجراءات، على أساس أنه لم يثبت وجود علاقة بين مكتب التحقيقات الفيدرالي ومكتب المدعي العام**[٣].

ويمكن القول بأن فاعلية آليات الملاحقة الجنائية الدولية، تعتمد في جزء منها على المعلومات الاستخباراتية، لاسيما خلال مرحلة التحقيق، وهو الأمر الذي تم تقنينه ضمن قواعد وإجراءات عمل كثير من المحاكم الجنائية الدولية، إلا أن ذلك يتطلب الالتفات إلى محاذير بشأن استخدام تلك المعلومات، **لعل أولها**: تحرّي كيفية الحصول عليها ومدي مشروعيتها، **وثانيها:** التدقيق في مدى صحة تقييم هذه المعلومات، لاسيما أن الأجهزة المعنية بتلقيها في المحاكم قد تفسرها وتقيّمها، دون الرجوع إلى المصادر التي استخرجتها، **وثالثها:** تمييز المعلومات مفتوحة المصدر، والتي ربما لا تكون بنفس دقة نظيرتها السرية.

الفرع الرابع

تحقيق مصالح مشتركة للدول

يُمكن رد تاريخ التبادل والتَشَارُك في الاستخبارات، بغرض تحقيق مصالح مشتركة، إلى ما شَهِدَتهُ الحرب العالمية الثانية من تعاون واسع بين وكالة المخابرات البريطانية ونظيرتها الأمريكية، بهدف مراقبة أوروبا والشرق الأقصى، حيث وقَّعت الولايات المتحدة الأمريكية"، و"المملكة المتحدة"، عام ١٩٤٧، اتفاقية بشأن تبادل المعلومات التي تحصل عليها كل دولة من اعتراض إشارات واتصالات دول العالم، وفي عام ١٩٤٨، وقعت الدولتان مع "أستراليا"، و"كندا"، "ونيوزيلندا" بروتوكولات مماثلة، وبموجبها تم الربط بين فرع استخبارات الإشارة لوكالة الأمن القومي الأمريكي، ومقر الاتصالات الحكومي البريطاني، وإدارة الاتصالات والإشارات الأسترالية، والمؤسسة الكندية لأمن الاتصالات، ومكتب أمن الاتصالات الحكومية النيوزيلندي، وتم تقسيم الأدوار والأعباء بين هذه الأجهزة، بحيث يتم مراقبة وجمع معلومات من أجزاء مختلفة من العالم، ثم التشارك فيها كما هي، أو بعد تحليلها، وقد أُطلق

---

(١) **واستند هذا الدفاع إلى أن المدعي العام عمل** و/ أو بناء على طلب و/ أو بالاشتراك مع مكتب التحقيقات الفدرالي، بالمخالفة للمادة (١/١٥) من النظام الأساسي، التي تحظر على المدعي العام تلقي تعليمات من أي حكومة أو من أي مصدر آخر. **راجع:**

Prosecutor v. Sesay, Kallon, & Gbao, *Case No. SCSL-04-15-T, 4 (Nov. 1, 2004).*

(٢)**المواد (٨ /ج، د، هـ)، المادة (٣٩)، (٤٠)** من القواعد الإجرائية وقواعد الإثبات، وتتعلق بالمساعدة المقدمة من دول أخرى.

(3) ***Prosecutor v. Sesay, Kallon, & Gbao, Case No. SCSL-04-15-T,*** *43 (May 2, 2005).*

علـي هذا التحـالف اسم "*Anglo-Sphere*"، والـذي امتـد بعـد ذلـك ليُشـكَّل أساسًـا لعلاقـة طويلـة الأمـد، وروابط ممتدة بين أجهزة مخابرات الدول المُنشأة له[١].

وواقعًا، تُنشأ هذه التحالفات بين دول تجمعها علاقات تاريخية، أو ثقة متبادلة، أو بروتوكولات مشتركة، ودائمًا ما تكون الولايات المتحدة الأمريكية هي الشريك الأبرز في معظم تلك التحالفات، حيث تُخصّص ميزانية ضخمة للتجسس بالمقارنة بباقي الدول، وبما يقارب الأربعة والأربعين مليار دولار سنويًا[٢]، ولعل أهم أهداف هذه التحالفات، هو دعم أطرافها لدى التعامل مع بعض المشاكل العالمية، كالنزاعات المُسلَّحة، والإرهاب، والهجرة غير المشروعة، وانتشار الأمراض الخطيرة "كالإيدز"، و"سارس"[٣].

وتختلف صور التشارك في هذه المعلومات، فمنها ما يقتصر على التبادل فقط، ومنها ما يشمل فك الشفرات أو المساعدة في التحليل، ومنها ما يتمثّل في الانتفاع بنتيجة تم التوصل إليها[٤]، وتجدر الإشارة إلى أن أطراف تلك التحالفات، ينظرون إلي إقصائهم منها، أو الحد من تبادل الاستخبارات معهم كنوع من العقاب، وعلى سبيل المثال، في عام ١٩٨٥، أعلنت حكومة العمال المنتخبة حديثًا في "نيوزيلندا"، أنها لن تسمح للسفن الأمريكية المسلحة نوويًا، أو التي تعمل بالطاقة النووية بالدخول إلى موانئها، وردًا على ذلك، هددت الولايات المتحدة، من بين جملة أمور، بأنها ستحد من تبادل معلومات الاستخبارات مع "نيوزيلندا"[٥].

وقد امتَّد أمر تبادل معلومات التجسس إلى منظمة الأمم المتحدة، حيث تعاملت بعض أجهزتها بناءً على استخبارات وردت إليها من بعض الدول، وعلى سند من أن هذا السلوك يدعم أغراض التعاون الدولي، لاسيما في مجال مكافحة الإرهاب، ومنع نشوب النزاعات المُسلَّحة، وضمان فاعلية عمليات حفظ السلام، ومن ذلك اعتماد مجلس الأمن صراحةً، على معلومات تجسس من شانها تبرير غزو العراق عام ٢٠٠٣، وتنظيمه لجزاءات تجميد أصول لقائمة أشخاص تم إعدادها بناءً على هذه المعلومات[٦].

ومن التطبيقات القضائية الوطنية، التي تناولت تقاسم المعلومات، قضية "حرية المعلومات" التي نظرتها المحكمة العليا "لكندا"، بشأن مطالبة مؤسسات تنفيذية في الدولة بتعديل قوانين أمن المعلومات، وتشديد الرقابة عليها، وجعل الوصول إليها أصعب، وذلك نظرًا لاعتماد "كندا" وبشكل أساسي، على

---

(1) ***N. BOOTH,*** *Lucifer Rising: British Intelligence and the Occult in the Second World War, History Press, 2016, PP. 308: 311.*

(2) ***Central Intelligence Agency,*** *Statement by the Director of Central Intelligence Regarding the Disclosure of the Aggregate Intelligence Budget for Fiscal Year 1998 (Mar. 20, 1998),* ***available at:*** *https://www.cia.gov/cia/public affairs/pressrelease/1998/psO32098.htm. 5/7/2019.*

(3) ***R. A. POSNER,*** *Preventing Surprise Attacks: Intelligence Reform in the Wake of 9/11, Lanham, MD: Rowman and Littlefield, 2005, PP. 175: 177.*

(4) ***A. J. RADSAN****, the Unresolved Equation of Espionage and International Law, P. R., P. 606.*

(٥) **وقد استعادت الدولتان العلاقة بعد ذلك بوقت قصير**، ولاحقًا عانت "كندا" من استبعاد مماثل بعد موقفها من حرب العراق. **راجع:**

M. RUDNER*, Hunters and Gatherers: The Intelligence Coalition Against Islamic Terrorism, 17 INT'L J. Intelligence & Counterintelligence, Issue: 193, 2004, P. 201.*

(6) ***S. CHESTERMAN****, One Nation under Surveillance: A New Social Contract to Defend Freedom without Sacrificing Liberty, Oxford University Press, 2011, PP. 70, 105, 157.*

معلومات تجسس ترد إليها من الولايات المتحدة الأمريكية، ومن ثم ينبغي أن تُراعي "كندا" توقعات حلفائها، فيما يخص قدرة التشريعات الكندية على الحفاظ على سرية المعلومات الحساسة التي تحصل عليها[١].

الفرع الخامس

دعم حق الدول في الدفاع عن النفس

أوردت المادة رقم (٥١) من ميثاق الأمم المتحدة، حقًا أصيلاً للدول في الدفاع عن نفسها ضد أي هجوم مسّلح، وربما تُمثّل المعلومات الاستخباراتية عنصرًا من عناصر هذا الحق، لأن توافرها يدعم اتخاذ قرار بشأنه، ويعزز فعالية اللجوء إليه[٢]، وتحرص الدول على ربط سياساتها الخاصة بجمع معلومات الاستخبارات، بتطورات التحديات الأمنية التي تواجهها، لاسيما في مجال مكافحة الإرهاب، والتنظيمات المسلحة المناوئة لها، كتنظيم القاعدة الذي أعلن أنه لن يلتزم بأي مبادئ صاغتها كيانات فوق وطنية، أو صكوك قانونية دولية[٣]، ويتطلب مثل هذا الوضع ضرورة توافر معلومات دقيقة بأحوال وتحركات وتخطيط مثل هذه التنظيمات، وأنواع الأسلحة التي تحوزها، أو الدول التي تدعمها أو توفر لها الإيواء، بما يُحقق الفعالية فيما يتعلق بدفاع الدول ضدها.

وقد اعتمدت إستراتيجية الأمن القومي الأمريكية الاتجاه السابق، وأقرّت استخدام الإجراءات الوقائية والاستباقية، كوسيلة لتوقي الهجمات من قبل منظمات إرهابية دولية، وذلك بالاعتماد على معلومات استخبارات، يمكن من خلالها تقييم التهديدات والمخاطر المحدقة بالأمن القومي، وإحباط أي هجمات عدائية محتملة[٤].

المبحث الثاني

الوضع القانوني للتجسس في القانون الدولي

مارست المجتمعات البشرية التجسس منذ بداية التاريخ، وكانت القواعد الدولية الخاصة بتنظيمه أكثر حداثة، وتعلّقت باقترافه أثناء الحرب، مثل اتفاقيات لاهاي لعام ١٩٠٧، ثم اتفاقيات جنيف لعام ١٩٤٩، والبروتوكول الإضافي الأول الملحق بها لعام ١٩٧٧، إلا أن القانون الدولي لم يُفرغ لنفس السلوك في زمن السلم أي أحكام[٥]، وتوَّلت التشريعات الوطنية ذلك، فنظمَّت قواعدها سلوك التجسس في وقت السلم، وأُعتبر بموجب معظمها ـ إن لن يكن كلها ـ جريمة على درجة عالية من الخطورة، ويُعاقب عليها بأشد العقوبات[٦]، ومن ثم، تحكم القواعد الدولية سلوك التجسس بين المتحاربين، وتُحدّد الوضع

---

(1) ***C. FORCESE,*** *Spies Without Borders, P. R., PP. 179: 181;* ***M C. WAXMAN,*** *Cyber-Attacks and the Use of Force, P. R., PP. 431: 432.*

(2) ***J. YOO,*** *Force Rules: U.N. Reform and Intervention, 6 CHI. J. INT'L L., 2006, PP. 640: 641.*

(3) ***G. SULMASY****, the Law of Armed Conflict in the Global War on Terror, 19 NOTRE DAME J.L. ETHICS & PUB. POL'Y, 2005, P. 309.*

(4) ***D. COLE,*** *Just War and the Ethics of Espionage, Routledge, 1 edition, 2014, PP. 53:54.*

(5) ***S. CHESTERMAN****, the Spy Who Came in from the Cold War, P. R., PP. 1071: 1072.*

(٦) **على سبيل المثال، قرَّرت بعض الدول العربية، عقوبة الإعدام لمن يقترف التجسس وقت الحرب،** كقانون العقوبات المصري رقم (١١٢) لسنة ١٩٥٧، وقضت مادته رقم (٨٠)، بأن يعاقب بالإعدام كل من سلَّم لدولة أجنبية أو لأحد ممن يعملون لمصلحتها أو أفشى إليها أو إليه بأية صورة، وعلى أي وجه، سرًا من أسرار الدفاع عن البلاد، أو توصل بأية

القانوني للجواسيس، بينما تظل مشروعيته والوضع القانوني لمقترفيه في وقت السلم أمر غير مُحدَّد وغير محسوم دوليًا.

ولدراسة الوضع القانوني لسلوك التجسس سواء أثناء النزاعات المسلحة أم في وقت السلم، فإننا نقسم هذا المبحث إلى المطلبين التاليين:

المطلب الأول: التنظيم الدولي للتجسس أثناء النزاعات المسلحة.

المطلب الثاني: الوضع القانوني الدولي للتجسس في وقت السلم.

المطلب الأول

التنظيم الدولي للتجسس أثناء النزاعات المسلحة

نعرض من خلال هذا الجزء، للوضع القانوني الدولي له في أوقات النزاعات المسلحة، لاسيما في اتفاقيات لاهاي لعام ١٨٩٩، ١٩٠٧، واتفاقيات جنيف لعام ١٩٤٩، والبرتوكول الأول الملحق بها لعام ١٩٧٧، وكذلك أحكام القضاء، وآراء الفقه، وذلك من خلال الفروع التالية.

الفرع الأول

التجسس في وقت الحرب وفقًا لقواعد لاهاي

أجازت قواعد لاهاي لعام ١٨٩٩ استخدام خداع الحرب، والوسائل اللازمة للحصول على معلومات عن الدولة المعادية، وهو حُكم يماثل ما نصت المادة رقم (٢٤) من اللائحة التنفيذية لقوانين وأعراف الحرب البرية لعام ١٩٠٧[1]، من حيث إن: "خداع الحرب واستخدام التدابير اللازمة للحصول على معلومات عن العدو والبلاد تعتبر جائزة"، ونلاحظ أن النصوص السابقة لم تُورد أي استثناء على قاعدة جواز استخدام "خداع الحرب" للحصول على المعلومات، وبالتالي لم تفرض أي قيد على سلوك التجسس في وقت الحرب.

طريقة إلي الحصول على سر من هذه الأسرار بقصد تسليمه أو إفشائه لدولة أجنبية، أو لأحد ممن يعملون لمصلحتها، وكذلك كل من أتلف لمصلحة دولة أجنبية شيئاً يعتبر سرًا من أسرار الدفاع، أو جعله غير صالح لأن ينتفع به. **كما قضت المادة (١٥٩) من قانون العقوبات العراقي** رقم (١١١) لسنة ١٩٦٩ بأن: يعاقب بالإعدام كل من سعى لدى دولة أجنبية معادية أو تخابر مع أحد ممن يعملون لمصلحتها لمعاونتها في عملياتها الحربية ضد العراق أو للإضرار بالعمليات لحربية للجمهورية العراقية وكل من دبر لها الوسائل المؤدية إلى ذلك أو عاونها بأي وجه على نجاح عملياتها الحربية. **وكذلك التشريع الجزائري** في مادته رقم (٦٤) من قانون العقوبات لعام ١٩٦٦، والمادة رقم (١١/ف)، (١١٣) من **قانون العقوبات الأردني** المؤقت رقم (٣٣) لعام ٢٠٠٠، والمادة رقم (١٤٧) من **قانون العقوبات العُماني** رقم (٧) لعام ١٩٧٤، والمادة (١١) من **القانون الكويتي** الخاص بجرائم أمن الدولة الخارجي والداخلي رقم (٣١) لعام ١٩٧٠. **وفيما يتعلَّق ببعض الدول الأجنبية**، فقد نصَّ بعضها على عقوبة الإعدام كالمادة رقم (٦٥) من المدونة العقابية الروسية لعام ١٩٦٠، والمعدلة بالمرسوم الصادر في ٥ مايو ١٩٦١، وكذلك المادة (٧٩٤/ب) من **التشريع الجنائي الفيدرالي للولايات المتحدة الأمريكية** لعام ١٩١٧، والمادة (١١٦) من المدونة العقابية البلجيكية لعام ١٩٣٧، في حين عاقبت دول أخرى عليه بالسجن المشدّد **كالتشريع الفرنسي**، الذي كان يعاقب بعقوبة الإعدام بموجب المادة رقم (٧٦/ أ) من التشريع الصادرة في ٢٩ يوليو ١٩٣٩، ثم صدر المرسوم الخاص بجرائم أمن الدولة لعام ١٩٦٤، والذي أبقى على العقوبة نفسها وأضاف أن يكون تنفيذها رميًا بالرصاص، إلا أنه تم إلغاء هذه العقوبة، واُستبدلت بعقوبة الأشغال الشاقة المؤبدة بموجب القانون الصادر رقم (٨١-٩٠٨) في ١٩٨١/١٠/٩. **وكذلك المادة رقم (٢٥٨) من قانون العقوبات الإيطالي** لعام ١٩٣٠، إلا أن بعض الدول قد اتجهت حديثًا إلى إلغاء عقوبة الإعدام عمومًا في تشريعاتها مثل بريطانيا، والصين، وأسبانيا، واليونان.

(١) **المادة رقم (٢٤) من اللائحة التنفيذية لقوانين وأعراف الحرب**، القسم الثاني بعُنوان "الأعمال القتالية"، من الفصل الأول بعنوان "وسائل إيذاء العدو والحصار والقصف".

وأوردت اتفاقية لاهاي لعام ١٩٠٧، في المادة رقم (٢٩) من الفصل الثاني منها بعنوان "الجواسيس"، تعريفًا للجواسيس باعتبارهم، "الذين يقومون بجمع معلومات أو محاولة ذلك، في منطقة عمليات تابعة لطرف في النزاع، عن طريق عمل من أعمال الزيف أو تعمد التخفي، وذلك لإبلاغها للعدو"، وبيَّنت المادتان رقمي (٣٠، ٣١) من الاتفاقية الوضع القانوني للجواسيس، لاسيما حالة القبض على الجاسوس بعد عودته إلى القوات المسلحة التي ينتمي إليها، حيث يتمتع بوضع أسير الحرب ـ بما له من حقوق وامتيازات ـ ولا يتحمل المسئولية عن أي عمل من أعمال التجسس التي اقترفها، كما لا يجوز معاقبة الجاسوس دون محاكمة[١].

ونلاحظ أن المواد المعروضة من اتفاقيتي لاهاي لعامي ١٨٩٩، ١٩٠٧ قد استنسخت ـ إلى حد كبير ـ أحكام مدونة "ليبر" لعام ١٨٦٣، وإعلان "بروكسل" لعام ١٨٧٤[٢]، من حيث إجازة استخدام خدع الحرب وجمع المعلومات، والوضع القانوني للجواسيس عند القبض عليهم، أو عند فرارهم والتحاقهم بالجيش الذي ينتمون إليه.

الفرع الثاني

التجسس في وقت الحرب في اتفاقات جنيف لعام ١٩٤٩

بموجب اتفاقية جنيف الرابعة بشأن حماية المدنيين وقت الحرب لعام ١٩٤٩، تم إضافة بعض الأحكام الخاصة بالتجسس، والضمانات الإجرائية بشأن معاملة الجواسيس، ومنها المادة (٥) التي قضت بأن الأشخاص الخاضعين للحماية بموجب الاتفاقية، والذين توجد شبهات قاطعة أو ثبت قيامهم بالتجسس في الأراضي المحتلة، يفقدون الحقوق المُقرّرة بموجب الاتفاقية، والتي قد تضر بأمن الدولة لو استمرت في منحها لهم، مثل حرية الاتصال، وفي كل الأحوال يعاملون بإنسانية، وفي حالة ملاحقتهم قضائيًا، لا يُحرمون من حقهم في محاكمة عادلة علي النحو الذي نصت عليه هذه الاتفاقية[٣].

---

(١) **وهو نفس الحكم الوارد في اتفاقية ١٨٩٩**، بشأن عدم توقيع عقاب على الجاسوس الذي يُضبط متلبسًا إلا بعد محاكمته. **راجع: الاتفاقية الثانية بشأن قوانين وأعراف الحرب البرية وملحقها:** اللوائح المتعلقة بقوانين وأعراف الحرب البرية، المواد من (٢٩: ٣١)، اعتمد ٢٩ يوليو ١٨٩٩.

(٢) **طُبِّق قانون "ليبر" رقم (١٠٠) لعام ١٨٦٣، خلال الحرب الأهلية الأمريكية**، وعَرَّف الجاسوس بأنه، شخص يسعى سرًا تحت مظهر كاذب أو تمويه، لجمع معلومات بقصد نقلها إلى العدو، ويعاقب بالقتل شنقًا، سواء نجح في الحصول على المعلومات أم لا، وسواء نقلها إلى العدو أم لا. **كما يُعد إعلان "بروكسل" لعام ١٨٧٤**، من أوائل جهود دوين قوانين الحرب دوليًا، واعتبر أن خدع الحرب غير محظورة، ويعتبر الشخص جاسوسًا، إذا تصرف سرًا أو تحت ادعاء كاذب، لجمع أو محاولة الحصول على معلومات، في إقليم مُحتل بنية إرسالها إلى قوة معادية، وإذا قُبض عليه مُتلبسًا يُحاكم وفقًا للقوانين السارية في دولة الجيش الذي قبض عليه، أما الجاسوس الذي يتمكن من العودة إلى جيشه، ثم يُقبض عليه من قبل العدو، فإنه يعامل كأسير حرب ولا يتحمل أي مسئولية عن أعماله السابقة. **راجع:**
Project of an International Declaration concerning the Laws and Customs of War. Brussels, *27 August 1874,* ***available at:*** *https://ihl-databases.icrc.org/ihl/INTRO/135.10/4/2020.*

(٣) نصت **المادة (٥) من اتفاقية جنيف الرابعة لعام ١٩٤٩، على أنه:** "١- إذا اقتنع أحد أطراف النزاع بوجود شبهات قاطعة بشأن قيام شخص تحميه الاتفاقية في أراضي هذا الطرف بنشاط يضر بأمن الدولة، أو إذا ثبت أنه يقوم بهذا النشاط، فإن مثل هذا الشخص يحرم من الانتفاع بالحقوق والمزايا التي تمنحها هذه الاتفاقية، والتي قد تضر بأمن الدولة لو منحت له. ٢- إذا اعتقل شخص تحميه الاتفاقية في أراض محتلة بتهمة الجاسوسية أو التخريب أو لوجود شبهات قاطعة بشأن قيامه بنشاط يضر بأمن دولة الاحتلال، أمكن حرمان هذا الشخص في الحالات التي يقتضيها الأمن الحربي حتما من حقوق الاتصال المنصوص عليها في هذه الاتفاقية. وفي كل من هاتين الحالتين، يعامل الأشخاص المشار إليهم في الفقرتين السابقتين، مع ذلك، بإنسانية، وفي حالة ملاحقتهم قضائيا، لا يحرمون من حقهم في محاكمة عادلة قانونية على النحو الذي نصت عليه هذه الاتفاقية".

وتناولت المادة رقم (٦٨) من الاتفاقية سلوك التجسس، باعتباره الجريمة الوحيدة التي يمكن لسلطة الاحتلال أن تنفذ حكم الإعدام عند ثبوتها على شخص محمي بموجب الاتفاقية، حيث قرَّرت أنه لا يجوز للأحكام الجزائية التي تصدرها هذه السلطة وفقًا للمادتين (٦٤)، (٦٥)[1]، أن تفرض عقوبة الإعدام على شخص محمي، إلا في الحالات التي يُدان فيها بالتجسس، أو اقتراف أعمال تخريب خطيرة ضد منشآت عسكرية تابعة لقوة الاحتلال، أو جرائم متعمدة ينتج عنها وفاة شخص أو أكثر، شريطة أن يعاقب على هذه الجرائم بالإعدام، بموجب قانون الأرض المحتلة الساري قبل بدء الاحتلال. ومن ثم، فإن الشخص المحمي الذي يرتكب جريمة تستهدف الإضرار بسلطة الاحتلال، ولكنها لا تشكل محاولة لاستهداف حياة أفراد قوات الاحتلال أو إدارته، ولا تشكل خطرًا جماعيًا جسيمًا، ولا تلحق ضررًا بالغًا بممتلكات أو قوات الاحتلال، أو الإدارة أو المنشآت التي يستخدمونها، يعاقب بالاعتقال أو السجن البسيط، مع مراعاة أن تتناسب مدة الاعتقال، أو السجن مع الجريمة.

كما قررت الفقرة الثالثة من المادة (٦٨) من الاتفاقية، أنه لا يجوز إصدار حكم الإعدام على شخص محمي، إلا بعد توجيه نظر المحكمة بصفة خاصة، إلى حقيقة أن المتهم ليس من رعايا دولة الاحتلال، وغير ملزم به بأي واجب للولاء نحوها، وبأي حال لا يجوز إصدار حكم الإعدام على شخص محمي تقل سنه عن ثمانية عشر عامًا وقت ارتكاب المخالفة.

وقضت الاتفاقية في مادتيها رقمي (٧٢، ٧٣) بإجراء المحاكمات الخاصة بالتجسس في وجود مساعدة قانونية، ومنح المُدان حق الاستئناف، وأعطت المادة رقم (٧٥) المحكوم عليه بالإعدام، حق تقديم التماس بالعفو أو إرجاء تنفيذ العقوبة، كما قررت عدم تنفيذ الحكم الصادر بالإعدام، إلا بعد مضي ستة شهور من تاريخ استلام الدولة الحامية للإخطار، المتعلق بالحكم النهائي الذي يؤيد هذه العقوبة، أو قرار رفض طلب التماس العفو أو إرجاء العقوبة، ويجوز خفض مهلة الستة شهور في حالات الطوارئ الخطيرة، أو عدم تناسب الانتظار مع الظروف السائدة، وتمثيله تهديدًا لأمن دولة الاحتلال أو قواتها المسلحة.

الفرع الثالث

التجسس في وقت الحرب في البروتوكول الإضافي الأول ١٩٧٧

أكدت المادة رقم (٤٦) من البروتوكول الإضافي الأول لعام ١٩٧٧، على تعريف ومعاملة الجواسيس على النحو المنصوص عليه في المادة (٢٩) من اتفاقية لاهاي لعام ١٩٠٧، وقررت لهم نفس الوضع القانوني، والإجراءات المُتبعة عند القبض عليهم، والتي قبلها القانون الدولي كعرف لأكثر من ١٠٠ عام، ومن ذلك عدم أحقيتهم في الحصول على وضع أسير الحرب، إلا بعودتهم إلى قواتهم المسلحة قبل القبض عليهم، مع التأكيد على معاملتهم إنسانيًا، وحصولهم على محاكمات عادلة بإجراءات منصفة،

---

(١) **نصت المادة (٦٤) من اتفاقية جنيف الرابعة لعام ١٩٤٩على أنه:** "تبقي التشريعات الجزائية الخاصة بالأراضي المحتلة نافذة، ما لم تلغها دولة الاحتلال أو تعطلها إذا كان فيها ما يهدد أمنها أو يمثل عقبة في تطبيق هذه الاتفاقية. ومع مراعاة الاعتبار الأخير، ولضرورة ضمان تطبيق العدالة على نحو فعال، تواصل محاكم الأراضي المحتلة عملها فيما يتعلق بجميع المخالفات المنصوص عنها في هذه التشريعات. على أنه يجوز لدولة الاحتلال إخضاع سكان الأراضي المحتلة للقوانين التي تراها لازمة لتمكينها من الوفاء بالتزاماتها بمقتضى هذه الاتفاقية، وتأمين الإدارة المنتظمة للإقليم وضمان أمن دولة الاحتلال وأمن أفراد وممتلكات قوات أو إدارة الاحتلال وكذلك المنشآت وخطوط المواصلات التي تستخدمها". و**نصت المادة (٦٥) من الاتفاقية على أنه:** "لا تصبح القوانين الجزائية التي تفرضها دولة الاحتلال نافذة إلا بعد نشرها وإبلاغها للسكان بلغتهم، ولا يكون لهذه الأحكام أثر رجعي".

وحظرت المادة (٣٩) من البروتوكول، استخدام وسائل خداع، تتعلّق بدول محايدة أو ليست طرفاً في النزاع، كالأعلام الخاصة بها، أو شاراتها أو زيها العسكري، بغرض الإضرار بالفئات المحمية أو للحصول على معلومات[١].

وبالرغم من تأكيد المادة (٤٦) على أن القاعدة في معاملة الجواسيس، أنهم لا يُعدون أسرى حرب، إلا أن الصياغة تركت مساحة للسلطة التقديرية للدولة التي تقبض عليهم، وقضت في الفقرة الأولي من المادة، أن أي فرد في القوات المسلحة يقع تحت سلطة طرف معاد أثناء اقترافه للتجسس، لا يكون له الحق في مركز أسير حرب و"يجوز" معاملته كجاسوس، وبالتالي فإن الأمر مبني على الجواز، ويترك الأمر للدولة صاحبة المصلحة، والتي لها الحق في اعتباره أسير حرب أو جاسوس، رغم انطباق شروط الجاسوس عليه.

واشترطت المادة (٤٦) ثلاثة شروط لتمام فعل التجسس وهي؛ جمع المعلومات؛ وعدم ارتداء الزى العسكري، والعمل في إقليم يسيطر عليه طرف معاد، **وبالنسبة لجمع المعلومات؛** يجب أن تتعلّق الممارسة بجمع معلومات أو محاولة جمعها، بقصد إرسالها إلي طرف مُعادٍ، ويخرج من نطاق ذلك، الذي يقوم بعمليات تخريب، أو يمارس التجارة مع العدو، فلا يعد جاسوسًا، **ولم تتطلب المادة وسيلة معينة لجمع المعلومات،** فيستوي أن يحصل عليها بالرؤية، أو باستخدام تقنيات، كما لا تُشكّل طرق إرسالها أهمية، **ولم تُحدد المادة طبيعة المعلومات أو نوعها،** ولعل المنطق يُشير إلى أن المقصود بها، كل ما تُسبغ عليه الدولة وصف السرية، وقد تكون اقتصادية، أو عسكرية، أو غيرها، مع ضرورة توافر قصد إرسال المعلومات إلى طرف معادٍ، فلا يعتبر جاسوسًا من حصل على تلك المعلومات، دون توافر هذا القصد لديه، **وأخيرًا فقد ساوت المادة بين إتمام الفعل وبين الشروع فيه،** فكل سعي للحصول على معلومات، سواء نجح أم لا يعد تجسسًا.

وفيما يتعلَّق بشرط عدم ارتداء الزى العسكري، فإن فرد القوات المسلحة الذي يجمع المعلومات وهو يرتدي الزى العسكري لجيشه، لا يعتبر جاسوسًا، ويعد قائمًا بعملية استطلاع، ويتمتع بوضع أسير الحرب، وهذا الحكم لا يجوز التوسع في مفهومه أو قياسه على وقت السلم، فلا يوجد استطلاع في وقت السلم. **وفيما يتعلَّق بشرط العمل في إقليم يسيطر عليه طرف معاد،** فقد كانت اتفاقية لاهاي ١٩٠٧، تنص على شرط مختلف، وهو جمع المعلومات في "منطقة عمليات أحد المتحاربين"، إلا أنه بعد التطور الهائل في أساليب الحرب، اتسع مفهوم منطقة العمليات، لدرجة تشمل كل إقليم الطرف المحارب المحتل وغير المحتل، وأصبح اصطلاح منطقة العمليات لا يتناسب مع تلك التطورات.

ومن العرض السابق للقواعد الدولية السارية بشأن التجسس وقت الحرب، يمكننا استنباط ما يلي:

---

(١) **نصت المادة (٣٩) من البرتوكول على أنه:** ١- يحظر في أي نزاع مسلح استخدام الأعلام أو استخدام العلامات أو الشارات أو الأزياء العسكرية الخاصة بالدول المحايدة أو غيرها من الدول التي ليست طرفا في النزاع. ٢- يحظر استخدام الأعلام أو استخدام العلامات أو الشارات أو الأزياء العسكرية المتعلقة بالخصم أثناء الهجمات أو لتغطية أو تسهيل أو حماية أو عرقلة العمليات العسكرية. ٣- لا يخل أي من أحكام هذه المادة أو الفقرة الأولي (د) من المادة ٢٠ بقواعد القانون الدولي السارية والمعترف بها بصفة عامة والتي تطبق علي التجسس أو علي استخدام الأعلام أثناء إدارة النزاع المسلح في البحر.

أولاً: ركزت هذه القواعد على معاملة فئة الجواسيس ولم تورد تنظيمًا شاملاً لسلوك لتجسس، بل إنها لم تتعرض لتعريف التجسس في حد ذاته، وإنما فصَّلت كل ما يتعلَّق بالوضع القانوني للقائمين به والمقارفين له وهي فئة الجواسيس.

ثانيًا: عدّدت شروط اعتبار الشخص جاسوسًا، وهي التخفي وراء ادعاءات كاذبة، أو استخدام وسائل خداع أو تمويه، بنية نقل معلومات إلى طرف معادي، وبخلاف ذلك لا يتوافر في حق الشخص صفة الجاسوس، وذلك على الرغم من أن بعض وسائل جمع المعلومات، لا تتطلب استخدام مثل هذه المظاهر أو الادعاءات المتطلبة كأركان لجريمة التجسس.

ثالثًا: بالرغم من عدم حظر القواعد الدولية لسلوك التجسس صراحةً، وعدم وجود التزام عام من جانب المتحاربين لاحترام أراضي أو حكومة الدولة المعادية؛ إلا أن الدلالة السلبية المقترنة بهذا السلوك، كانت هي القاسم المشترك بين القواعد المنظمة لوضع الجواسيس أثناء الحرب، في كل المراحل الزمنية، وبدليل تقرير عقوبة الإعدام عند القبض على الجاسوس مُتلبسًا، وبالتالي يمكن القول بأن التعامل الدولي مع التجسس يُمثّل تناقضًا، من حيث تنظيمه كجزء من أعمال الحرب، مع فرض عقوبة على مقترفه تصل إلى الإعدام، ولم تتضمن القواعد ذات الصلة أحكامًا تدعم فهم هذا التناقض.

رابعًا: نظمت قوانين الحرب معاقبة الجواسيس بشكل رادع، وعدم أحقيتهم في التمتع بوضع أسرى الحرب، وتحملهم المسئولية الشخصية عن أفعالهم، إلا أن هذه القواعد لم تُصنِّف التجسس كجريمة حرب، ولا يُحاكم الجواسيس كمجرمي حرب، كما لم تتعرَّض تلك القواعد لمدي انتهاك الحكومة المرسلة لهم للقانون الدولي، أو مدي إمكان تقرير المسئولية الدولية عن هذا السلوك.

خامسًا: منحت قواعد التجسس الجاسوس نوعًا من التقادم الخاص بسلوكه، إذا نجح في الانضمام إلى القوات المسلحة النظامية التي يعمل لحسابها، حتى ولو قبض عليه بعد ذلك، فلا يُحاكم بتهمة التجسس، وربما يرجع ذلك، إلى صعوبة إثبات سلوك التجسس مع طبيعته السرّية، لاسيما في حالة نجاح الجاسوس في العودة إلى جيشه، أو ربما لاعتبار التجسس أحد خدع الحرب المسموح بها، أو ربما أُدرج هذا الحُكم باعتباره قاعدة من قواعد الحرب العرفية المعمول بها منذ أكثر من مائة عام.

المطلب الثاني

الوضع القانون الدولي للتجسس في وقت السلم

لم تتطرق قواعد القانون الدولي لتنظيم ممارسة التجسس في وقت السلم صراحةً، بالرغم من صيرورة أنشطة التجسس ممارسة روتينية للدول في الأوقات العادية[1]، وذلك باستثناء بعض القواعد التي يمكن تكييفها للتعامل مع هذا السلوك، كواجب احترام السيادة الإقليمية للدول وسلامتها واستقلالها السياسي، وباعتبار أن إرسال وكلاء لها إلى إقليم دولة أخرى دون موافقة الأخيرة ينتهك هذا الواجب، ووفقًا لذلك، تكون ممارسة التجسس في وقت السلم مخالفة لالتزام دولي مُستقر[2].

وربما يرجع عدم تنظيم سلوك التجسس دوليًا ـ ولو جزئيًا ـ إلى أن فوائد ممارسة غالبية الدول له، تجعلها غير راغبة في توجيه أي انتباه إليه، أو إنشاء أي نوع من الرقابة عليه، بحيث تستمر في ممارسته

(1) ***C. D. BAKER**, Tolerance of International Espionage, P. R., P. 1091.*
(2) ***C. FORCESE**, Spies Without Borders, P. R., PP. 186:193.*

بدواعي الأمن القومي، مع تأكيدها على أنها لا تتدخل في شئون الدول الأخرى. وعندما نتتبع غالبية الآراء الفقهية التي تناولت التجسس وقت السلم، يمكننا تقسيمها إلى اتجاهات ثلاثة، يري الأول منها أن القانون الدولي لم يحظر هذا السلوك صراحةً وبالتالي يمكن القول بمشروعيته، ويري اتجاه آخر أن التجسس في وقت السلم غير مشروع لكونه ينتهك بعض أحكام القانون الدولي، ويذهب اتجاه ثالث، إلى أن لهذا السلوك موقعًا وسطًا بين المشروعية وعدم المشروعية، فلا هو مشروع ولا هو غير مشروع.

ولمعالجة الوضع القانوني للتجسس وقت السلم، فإننا نتناول الاتجاهات الفقهية السابقة بالدراسة، وذلك من خلال الفروع التالية.

الفرع الأول

الاتجاه الخاص بمشروعية التجسس وقت السلم وفقًا للقانون الدولي

يري أصحاب هذا الاتجاه، أن التجسس في وقت السلم مشروع، ولا يمكن دحض ذلك، للأسباب الآتية:

أولاً: عدم وجود حظر صريح لسلوك التجسس وقت السلم بموجب قواعد القانون الدولي:

اعتمدت المحكمة الدولية الدائمة للعدل، في حكمها الصادر في قضية "لوتس" عام ١٩٢٧، معيارًا لتحديد عدم مشروعية أي سلوك دولي، وهو "ضرورة النص صراحةً على حظره"، وأوردت المحكمة أن: "القانون الدولي يحكم العلاقات بين الدول المستقلة، وقواعده الملزمة تنبثق من إرادة الدول الحرة، التي يتم التعبير عنها في الاتفاقيات، أو الأعراف المقبولة كمبادئ قانونية تنظم العلاقات بين هذه الدول؛ ومن ثم، لا يمكن افتراض وجود قيد على استقلال الدول، ولكنَّ القيد الأساسي والأهم الذي يفرضه القانون الدولي على الدولة، هو أنه في حالة عدم وجود قاعدة تُرخّص بخلاف ذلك، لا يجوز لها ممارسة سلطتها بأي شكل من الأشكال في إقليم دولة أخرى"[(١)]. أي أنه للقول بعدم مشروعية سلوك معين أو حظره دوليًا، ينبغي النص علي ذلك صراحةً بموجب قاعدة محددة، وإذا غاب مثل هذا الحظر الصريح، تبقى كل دولة حرة في ممارسة ما يحقق مصالحها.

وبإسقاط المعيار السابق للمحكمة على سلوك التجسس في وقت السلم، فإنه لم يُحظر بموجب أي معاهدة ثنائية أو جماعية، بشكل مباشر أو غير مباشر، ولا يمكن استنباط ذلك من نصوص عامة يرد ذكرها في معاهدات الصداقة، وحسن الجوار، كالنص الخاص بعدم التدخل في الشئون الداخلية للدول مثلاً، حيث لا يُمكن الاعتماد على الطابع شديد العمومية لهذه النصوص، باعتبارها حظرًا للتجسس في العلاقات الدولية[(٢)].

ويُثبت الواقع أن الدول تحتاج إلى الحصول على معلومات لتعزيز استقرارها، وتحقيق الكفاءة السياسية، والاحتراز من أي تهديد قد يكون مُحدقًا بها؛ وإذا كان التجسس هو أحد السُبل التي تحقق ذلك،

---

(1) ***The Case of the S.S. 'Lotus' (France v Turkey)*** *(Judgment), [1927] PCIJ Rep. Series A No. 9, 10, Paras. 18, 19.*

(2) ***A. S. DEEKS****, Confronting and Adapting Intelligence Agencies and International Law, 102 VA. L. REV. 599, 2016, P. 600.*

فهو أمر مشروع لعدم وجود قاعدة دولية صريحة تحظره في وقت السلم[١]، ولا يمكن تطبيق القواعد المُنظمة للتجسس في زمن الحرب على نفس السلوك وقت السلم، أو تقرير نفس العقوبة المُشدَّدة وهي الإعدام للجواسيس، لأن أحوال الحرب هي التي تؤدي إلي تقرير هذه العقوبة، على عكس التجسس وقت السلم، الذي لم تحظره قاعدة دولية، أو تعتبره خطأً أخلاقيًا، أو سياسيًا، أو قانونيًا، أو تُقرّر عقوبة على ممارسته[٢].

ويؤكّد جانب من الفقه، على المعنى السابق بقوله، أنه ومنذ نشأة القانون الدولي، لا يوجد حظر بشأن ممارسة التجسس في زمن السلم، وهو ما يعني نشوء قاعدة عرفية بجواز هذا السلوك، ويكون للدول وفقًا لمبدأ المساواة في السيادة أن تتصرف كما تشاء، طالما لا توجد قواعد تحظر سلوكها، وهذه القاعدة مُؤيدة بما ورد في حكم المحكمة الدولية الدائمة للعدل في قضية "الوتس" عام ١٩٢٧، من حيث إن الأصل هو إباحة أي سلوك أو إجراء ما لم يتم حظره صراحةً بموجب قاعدة دولية[٣].

ويقرر جانب فقهي، أن تنظيم التجسس دوليًا وقت السلم لم ينل اهتمامًا كافيًا، وبالرغم من أنه فعلٌ غير ودي، ومُجرَّم في معظم القوانين الوطنية، إلا أنه لا يمثل جريمة دولية ولا ينتهك القانون الدولي، ولا أدلّ على ذلك، من أن عدد الاحتجاجات الرسمية التي قدمتها دول، بسبب تعرضها للتجسس وقت السلم كانت قليلة نسبيًا، مما يطرح احتمال القبول الدولي ـ ولو بشكل متردد ـ لشرعية هذا السلوك، أو ربما ملامسته لعتبة العرفية[٤].

ويبيَّن جانب فقهي آخر، أن التجسس عنصرًا أساسيًا في الشئون الدولية، ومن الإنصاف القول بأن ممارسات الدول وعلى مر التاريخ تعترف بالتجسس كوظيفة حكومية وبالتالي تدعم شرعيته، مع إمكان اعتباره نوع من القواعد العرفية التي ما زالت في مرحلة التشكيل، ونلاحظ أنه حتى في القوانين الوطنية، لا يُعاقب الجواسيس لأنهم ينتهكون قواعد دولية تحظر سلوكهم، ولكن لأنهم ينفذون عمليات ضد المصالح الوطنية[٥].

ويري جانب فقهي، أنه على الرغم من مخاوف انتهاك التجسس وقت السلم لواجب السلامة الإقليمية والاستقلال السياسي للدول، إلاَّ أنه لا يزال حقًا سياديًا للدول القومية، ولا توجد قاعدة دولية تحظره، وعلى من يعارض ذلك عبء الإثبات، كما لا يوجد ما يفيد أن الدول الموقعة على ميثاق الأمم المتحدة، تعتقد أن المادة (٢) أو المادة (٥١) منه تحظران جمع المعلومات الاستخباراتية، والواقع أن ممارسة الدول في السنوات التالية لاعتماد الميثاق تشير إلى عكس ذلك[٦].

---

(1) ***G. BROWN**, Spying and Fighting in Cyberspace: What is Which?, 8 J. NAT'L SEC. L. & POL'Y., 2016, PP. 621:622*

(2) ***L. PELICAN**, Peacetime Cyberespionage: A Dangerous, but Necessary Game, 20 CommLaw Conspectus, 2012, P. 363.*

(3) ***A. E. ROBERTS**, Traditional and Modern Approaches to Customary International Law: A Reconciliation, 95 AM. J. INT'L L. & n. 199, 2001, PP. 757: 776.*

(4) ***H. HANDEYSIDE**, the Lotus Principle in ICJ Jurisprudence: Was the Ship Ever Afloat? 29 MICH. J. INT'L L., 2007, PP. 71: 72.*

(5) ***G. SULMASY, J. YOO**, Counterintuitive: Intelligence Operations and International Law, P. R., P. 628.*

(6) ***Q. WRIGHT**, Espionage and the Doctrine of Non-Intervention in Internal Affairs, P. R., P. 12.*

ومن الممارسات الدولية التي تؤيد هذا الاتجاه، واقعة "جوزينكو" عام ١٩٤٥، حيث توجه "إيجور جوزينكو" الموظف المُختص بفك الشفرات بسفارة الاتحاد السوفيتي السابق في "أوتاوا"، إلى السلطات الكندية، طالبًا اللجوء السياسي، وكاشفًا عن تلقيه أوامر من الحكومة السوفيتية بالتجسس على "كندا"[١]، وتجنيد مدنيين، وعسكريين، وموظفين، وباحثين، وبرلمانيين، بغرض الحصول على معلومات تخص التسلّح النووي "لكندا"، وقرَّر أنه نجح في الحصول على تفاصيل خاصة بالقنبلة الذرية، التي كانت الولايات المتحدة الأمريكية تحتكر أسرارها مع "بريطانيا" و"كندا"[٢]. وعلى الرغم من عدم إنكار الحكومة السوفيتية لتلك الوقائع، فقد اكتفت "كندا" بسحب رئيس بعثتها في الاتحاد السابق، وإعلان بعض موظفي سفارته في "أوتاوا" غير مرغوب فيهم[٣]، ولم تطالب بجبر ما أصابها من أضرار، أو تُصرّح بوجود أساس قانوني يُمكن الاستناد إليه في مثل هذه المطالبة.

وكذلك، في سابقة هي الأولي من نوعها، منح القانون الأمريكي للأمن القومي "*National Security Act*" لعام ١٩٤٧، الحكومة سلطة إجراء عمليات استخبارات خارج إقليمها، استنادًا إلى أنه عدم وجود قاعدة دولية تحظر التجسس وقت السلم[٤].

ثانيًا: ضرورة التجسس لدعم سيادة الدول وحماية الأمن القومي لها:

يرتكز هذا التبرير على أن ممارسة التجسس وسيلة ضرورية لترسيخ سيادة الدول، وحماية أمنها القومي من أي تدخل أجنبي أو أعمال إرهاب ، لاسيما بعد إقرار نظام دولي يتأسس على أحكام ميثاق الأمم المتحدة، وصيرورة سيادة الدول غير مطلقة، بالنظر إلى الالتزامات التي يتم الاتفاق عليها لصالح المجتمع الدولي[٥]، وبالتالي يُمثّل التجسس عنصرًا رئيسًا لتحقيق الكفاءة السياسية وإدارة الدولة، بما يوفره من معلومات لازمة لتلبية حاجة صانعي القرار الآنية والمستقبلية في كافة المجالات، كدعم فاعلية حق الدول في الدفاع عن النفس وفقًا للمادة (٥١) من الميثاق؛ بتمكينها من معرفة متى يمكن أن تتعرّض لهجوم مسلح، وما هي قدرات الدول المعادية، ثم اتخاذ الإجراءات الدفاعية اللازمة لمواجهة أي تهديدات فورية أو محتملة[٦].

---

(1) ***J. E. TUNNELL**, Latest Intelligence: An International Directory of Codes Used by Government, Law Enforcement, Military and Surveillance Agencies, 1990, P. 101.*

(2) ***Canadian Security Intelligence Service,** Commentary No. 76: the Canadian Government Security Screening Program, **available at:** http://www.csis-scrs.gc.ca/eng/comment/com76e.html.24/11/2019.*

(٣) **وتم تقديم عشرين شخصًا إلى المحاكمة في "كندا" عن هذه الواقعة**، ولم يكن من بينهم أحد من أعضاء السفارة السوفيتية في "كندا"، حيث لم يرفع الاتحاد السوفيتي السابق الحصانة عن أحد منهم. **راجع:**

***R. D. SCOTT**, Territorial Intrusive Intelligence Collection and International Law, 46 Air Force Law Review, 1999, P. 217.*

(4) ***National Security Act of 1947,** Pub. L. No. 80-253, 61 Stat. 495, codified as amended in scattered sections of 50 U.S.C. ch. 15.*

(5) ***P. WU**, Impossible to Regulate? Social Media, Terrorists, and the Role for the U.N., 16 CHI. J. INT'L L. 281, 2015, PP. 310:311.*

(٦) **أكَّد الرئيس الأمريكي الأسبق "جورج واشنطن"** في أول خطاب له، على أن الاستعداد للحرب هو أكثر السبل فعالية للحفاظ على السلام، وإذا توافر لدى مُتخذي القرارات معلومات دقيقة بشأن التهديدات المحتملة، وقدرات الخصوم ونواياهم، فإنهم سيتمكنون من الرد بشكل رادع على أي هجمات أو تهديدات إستراتيجية. **راجع:**

***D. WEISSBRODT**, Cyber-conflict, Cyber-crime, and Cyber-espionage, 22 Minnesota Journal of International Law, 2013, P. 347.*

ويُقرَّر جانب فقهي أن التجسس وقت السلم غير محظور دوليًا "بصورة جوهرية" بل إنه يدعم حق الدول في الدفاع المكفول بموجب ميثاق الأمم المتحدة، لاسيما الوقائي، بحيث يُمكنها توقي التهديدات المُحتملة، كما يؤدي رصد الدول المتبادل لبعضها البعض، إلى استقرار المجتمع الدولي، لأنه يُحقق وظيفتين؛ **الأولى**: "كضوء أحمر"، يحذر الدول من أي هجمات مفاجئة قد تهدد مصالحها المشتركة، **والثانية: "**كضوء أخضر**"** في حالة استقرار الأوضاع الدولية، بحيث يوجّه الدول للعمل على تعزيز وإنماء علاقاتها[١].

ثالثًا: اعتماد منظمة الأمم المتحدة على معلومات استخبارات عند اتخاذ بعض القرارات:

دعمت منظمة الأمم المتحدة جمع وتبادل المعلومات السرية، في مجال التعاون الدولي لمكافحة الإرهاب والتفتيش على الأسلحة، ومن ذلك قرار مجلس الأمن رقم (١١٧٣) المُتخذ وفقًا للفصل السابع من الميثاق، والذي دعا الدول إلي توفير المعلومات المتعلقة بعمليات أو شبكات أو تحركات الإرهابيين، وبالفعل دعمت المعلومات الاستخباراتية التي توافرت في هذا المجال، استخدام تدابير بديلة للمواجهات العسكرية، كاستباق فرض جزاءات مالية واقتصادية، من شأنها تقويض الأنشطة الإرهابية، وصون السلم والأمن الدوليين أو استعادتهما، وكذلك إعداد قوائم أُدرج فيها أفراد وكيانات متورطين وضالعين في الأنشطة الإرهابية، أو مُمولين لتنظيمات إرهابية يستهدفها مجلس الأمن، وتجميد أصولهم إلى أجل غير مسمى، وبما يُجنب الدول أخطار الإرهاب، ويُجنب المواطنين تحمل آثار الجزاءات التي قد تُفرض دون تمييز[٢].

وبموجب قرار مجلس الأمن رقم (١٢٦٧) تم إنشاء لجنة للإشراف على تنفيذ الجزاءات، وتصنيف الأموال التي يتعين تجميدها، والتي أصدرت قرارها رقم (١٣٩٠) في ديسمبر من عام ٢٠٠٠، بتجميد أموال "بن لادن"، وكل من ينتمي إلى تنظيم القاعدة[٣]. وفي يناير من عام ٢٠٠٤، وبموجب القرار رقم (١٥٢٦)، اقترح بعض أعضاء المجلس، دعوة الأفراد المدرجين في القوائم، لتقديم معلومات تنفي وجود أي رابطة لهم مع تنظيم القاعدة[٤]، وفي يوليو من عام ٢٠٠٥، تطلَّب قرار اللجنة رقم (١٦١٧) من الدول، عند اقتراح إدراج أسماء إضافية للقائمة، أن يكون ذلك مُسبَّبًا، وأن تقوم بإبلاغ ـ قدر الإمكان ـ وكتابةً كلما أمكن، الأفراد والكيانات المدرجة في القائمة بالتدابير المفروضة عليهم، والمبادئ والإجراءات التي تحكم عملية الإدراج والرفع من القائمة، وخلال عام ٢٠٠٥، تم تجميد أصول (٣٤٧) فردًا، (١١٩) كيانًا[٥].

ويمكن القول بأن الركيزة الرئيسة لتنفيذ القرارات السابقة، تمثَّلت في الاعتماد على نظام متكامل وموثوق به من المعلومات المُعلنة والسريّة، يتم على أساسه الإدراج في القوائم، ومنح إعفاءات إنسانية، والتقليل إلى أقصى حد من الأضرار التي ربما تلحق بالدول، نتيجة توقيع جزاءات على أفراد أو كيانات

---

(1) ***N. TSAGOURIAS**, the Legal Status of Cyberspace, in Research Handbook on International Law and Cyberspace, ed. Nicholas Tsagourias and Russell Buchan, Edward Elgar, 2015, P. 17.*

(2) ***S.C. Res.** 1173 11, U.N. Doc. S/RES/1173 (June 12, 1998**); S.C. Res.** 1333, 7 8(c), U.N. Doc. S/RES/1333 (Dec. 19, 2000); **S.C. Res**. 917 3, U.N. Doc. S/RES/ 917 (May 6, 1994).*

(3) ***S.C. Res. 1390, U.N. Doc.** S/RES/1390 (Jan. 16, 2002).*

(4) ***S.C. Res. 1526, 17, U.N. Doc.** S/RES/1526 (Jan. 30, 2004).*

(5) ***S.C. Res. 1617, 4, U.N. Doc**. S/RES/1617 (July 29, 2005).*

ينتمون إليها[١]، بل إن سياسة رفع الأسماء من القائمة، والتي تم الإعلان عنها في أغسطس من عام ٢٠٠٢، اقتضت أن يُقدّم الشخص المُدرج إلى دولته التماسًا لإعادة النظر في وضعه، وتحمّله عبء تقديم معلومات تُبرّر رفع اسمه، ثم مراجعة هذه المعلومات والتحقق من صحتها، وطلب معلومات إضافية عند الاقتضاء، وتتوقف القدرة على اتخاذ قرار مستنير بشأن الإدراج أو الرفع من القائمة، على مدى صحة وجدية المعلومات المُقدَمة[٢].

الفرع الثاني

الاتجاه الخاص بعدم مشروعية التجسس وقت السلم وفقًا للقانون الدولي

قرَّرت المحكمة الجنائية الخاصة في "هولندا"، أن التجسس وقت السلم عمل مخالف للقانون الدولي، وعندما يتم بناء على أوامر من الدولة، فإنه يُشكّل انتهاكًا دوليًا، قد تتقرَّر على أساسه مسئوليتها في مواجهة الدول المُستهدفة[٣]، وهو اتجاه أيده جانب من الفقه، باعتبار أن التجسس وقت السلم غير مشروع، لأنه يتعارض مع طبيعة العلاقات الودية بين الدول، وينتهك مبادئ قانونية أساسية وراسخة في القانون الدولي، لاسيما واجب احترام السيادة والسلامة الإقليمية للدول، وعدم التدخل في شئونها، حيث يُعد مبدأ السيادة من أخص خصائص الدولة، وينبثق عنه حقها في عدم التدخل في شئونها، واحترام ولايتها وسلطتها السيادية على إقليمها[٤]، ومن القواعد التي رسَّخت لهذا الواجب، المادة رقم (٤/٢) من ميثاق الأمم المتحدة، بشأن امتناع الدول في علاقاتها عن استعمال القوة أو التهديد باستعمالها، ضد السلامة الإقليمية أو الاستقلال السياسي لأي دولة، أو بأي طريقة أخرى لا تتفق مع مقاصد الأمم المتحدة، ونبيّن ذلك كما يلي.

أولاً: مضمون مبدأ عدم التدخل:

يُعد مبدأ عدم التدخل في شئون الدول الداخلية والخارجية، جزءًا لا يتجزأ من القانون الدولي العرفي، وقد أكَّدت عليه صراحةً عدة إعلانات دولية، منها، إعلان الجمعية العامة للأمم المتحدة عام ١٩٦٥، بشأن عدم جواز التدخل في الشئون الداخلية للدول، وحماية استقلالها وسيادتها، وإعلان مبادئ القانون الدولي المتعلقة بالعلاقات الودية بين الدول لعام ١٩٧٠[٥]، وأُعلن بموجبهما أن: "لكل دولة حق غير قابل للتصرف، في اختيار نظامها السياسي، والاقتصادي، والاجتماعي، والثقافي، دون تدخل بأي شكل من الأشكال من دولة أخرى"، و"لا يحق لأي دولة أو مجموعة من الدول أن تتدخل بصورة مباشرة أو غير مباشرة، ولأي سبب، في الشئون الداخلية أو الخارجية لأي دولة أخرى".

---

(1) ***S.C. Res****. 1452, para. 1(a), U.N. Doc. S/RES/1452 (Dec. 20, 2002).*

(2) ***Bin Laden's Ex-Bodyguard Is Taken Off Lists of Terrorists****, L.A. TIMES, Jan. 5, 2005, PP. 7: 10;* ***U.N. Doc. S/2005/83,*** *(Feb. 15, 2005).*

(3) ***Lauterpacht, Annual Digest,*** *1949, vol. 16, case No. 87, In Re Flesohe, Holland, special Crimnal Court, Amsterdam, P. 272.*

(4) ***M. N. SCHMITT, ed.,*** *Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, Cambridge, 2013, P. 16.*

(٥) **إعلان عدم جواز التدخل في الشؤون الداخلية للدول** وحماية استقلالها وسيادتها، ٢١ ديسمبر ١٩٦٥ *(UN Doc. A/RES/20/2131)*؛ **إعلان مبادئ القانون الدولي المتعلقة بالعلاقات الودية** والتعاون بين الدول وفقاً لميثاق الأمم المتحدة ٢٤ أكتوبر ١٩٧٠، (*UN Doc. A/RES/25/2625*)؛ **إعلان عدم جواز التدخل والتدخل في الشؤون الداخلية للدول**، ٩ ديسمبر ١٩٨١، (*UN Doc. A/RES 36/103*).

ووفقًا لمضمون تلك الإعلانات، والتي تُمثّل انعكاسًا للقانون العرفي علي نطاق واسع[١]، تُحظر كافة أشكال التدخل في شئون الدول، أو محاولات تهديد سيادتها أو شخصيتها القانونية، أو عناصرها السياسية، أو الاقتصادية، أو الثقافية، وأي فعل يُخالف ذلك يُعد انتهاكًا للقانون الدولي.

كما تم تكريس مبدأ عدم التدخل في العديد من المعاهدات الدولية الإقليمية والثنائية، والنص عليه بشكل مباشر أو ضمني، ومن ذلك المادة رقم (٨) من اتفاقية "مونتيفيديو" بشأن حقوق وواجبات الدول لعام ١٩٣٣، والمادة رقم (١/٢) من ميثاق الأمم المتحدة بشأن المساواة في السيادة بين الدول، وبما يشمل امتناع أي دولة عن ممارسة سلطاتها على أراضي دولة أخرى، أو التدخل في شئونها، أو اتخاذ أي إجراءات تحرم أو تعوق الدول الأخرى من استخدام حقوقها السيادية، الخاصة بتسيير شئونها الداخلية والخارجية، واستقلالها في الحكم.

ويشمل حظر التدخل في شئون الدول، كافة عناصر إقليم الدول، البري، والبحري، والجوي، وعلى سبيل المثال، قررت اتفاقية الأمم المتحدة لقانون البحار لعام ١٩٨٢، حق المرور البريء في البحر الإقليمي للدول الساحلية، والذي يتطَلَّب الامتناع عن أي أعمال قد تمثل تهديدًا لأمن الدولة الساحلية أو نظامها[٢]، وكذلك حظر استخدام المجال الجوي للدول، في أي عمليات نقل غير مشروعة، أو جمع معلومات، وقد تُقرّر الدول استخدام القوة دون سابق إنذار، في مواجهة التعدي المتعمد، أو المُخطط له، لمجالها الجوي من قبل طائرات عسكرية، في غير حالات المِحَنْ أو الضرورة[٣].

وباستعراض حكم محكمة العدل الدولية في قضية قناة "كورفو" لعام ١٩٤٩، نجد أن المحكمة قد رسّخت لمبدأ عدم التدخل، حيث قررت أن احترام السيادة الإقليمية بين الدول المستقلة، هو أساس جوهري للعلاقات الدولية، وأن قرار "المملكة المتحدة" بإرسال سفن حربية إلى المياه الإقليمية "لألبانيا" لجمع أدلة على إمكانية التعدين، يمثل توغلاً غير مُصرّح به في أراضي "ألبانيا"، وبالتالي انتهاكًا لسيادتها[٤].

كما أوضح حكم المحكمة في قضية نيكاراجوا عام ١٩٨٦، معنى أفعال التدخل غير المشروع في شئون الدول، باعتبارها كل ما يؤثر على المسائل التي من حق كل دولة وفقًا لمبدأ سيادة الدول أن تقررها بحرية، فيما يخص نظامها السياسي، أو الاقتصادي، أو الاجتماعي، أو الثقافي، أو إدارة السياسة الخارجية، حيث يتم إكراه الدولة فيما يتعلق بهذه المسائل التي يجب أن تظل حرة[٥]. كما أكدّت المحكمة حكمها في قضية "*Timor-Leste v. Australia*"، عام ٢٠١٤ على نفس المبدأ، وقررت أن تدخل دولة في الاتصالات التي تتم على إقليم دولة أخري، يُمثل حجة مقبولة لإثارة مبدأ حظر التدخل وانتهاك السيادة[٦].

---

(١) **حكم محكمة العدل الدولية في قضية "نيكاراجوا" ١٩٨٦،"***Nicaragua v. United States***"**، ٢٧ يونيو ١٩٨٦، الفقرة ٢٠٢.

(٢) **المادة رقم (١٩/ ٢/ ج) من اتفاقية الأمم المتحدة لقانون البحار عام ١٩٨٢،**

(3) ***R. M. CHESNEY****, Leaving Guantdnamo: The Law of International Detainee Transfers, 40 U. RICH. L. REV., 2006, P. 657.*

(٤) **مجموعة أحكام محكمة العدل الدولية ١٩٤٩-١٩٩٢، الحكم في قضية "قناة كورفو"** عام ١٩٤٩، الفقرات ١: ٣، ٩:٦، ١١.

(٥) **حكم محكمة العدل الدولية في قضية "نيكاراجوا" ١٩٨٦، "***Nicaragua v. U.S.A***"**، ٣٠ أبريل ١٩٨٦، الفقرة ٢٠٥.

(6) ***Timor-Leste v. Australia,*** *Provisional Measures Order, 2014 I.C.J. 147, 148 (Mar. 3).*

كما أوضح قرار التحكيم الصادر في قضية "جزيرة بالماس" لعام ١٩٢٨، أن السيادة في العلاقات بين الدول تعني الاستقلال بجزء من الكرة الأرضية، دون أي دولة أخرى، واكتساب حقوق عليه لممارسة مهام الدولة[١]، التي تتم داخل هذا الإقليم ويترتب عليها آثار خارجه، وكذلك الإجراءات التي تتخذ في الخارج ولها آثار داخل ذلك الإقليم، ومن الأمثلة على ذلك، أنه في تفجير "لوكربي"، انعقدت الولاية القضائية للمملكة المتحدة، على الرغم من أن القنبلة التي فجرت الطائرة، كانت قد وُضعت على متنها في "مالطا"[٢].

ومن الممارسات الدولية بشأن تعامل الدول بموجب مبدأ حظر التدخل، واقعة إسقاط الاتحاد السوفيتي السابق، لطائرة التجسس الأمريكية (*U-2*) عام ١٩٦٠، والتي كانت تحلق فوق الإقليم السوفيتي، وهي تتمتع بحصانة سيادية، وكان قائدها وكيلاً عن الحكومة الأمريكية، إلا أن نشاط الطائرة المتمثل في جمع المعلومات، جعل الاتحاد السابق يُقرَّر بأنه تعرَّض لتدخل غير مشروع في شئونه وانتهاك لسيادته، وبالفعل قام بإسقاط الطائرة، وقبض علي قائدها، دون النظر للحصانة المقررة بموجب القانون الدولي[٣].

وفي ابريل عام ٢٠٠١، اصطدمت طائرة مراقبة تابعة للبحرية الأمريكية بطائرة مقاتلة صينية فوق بحر الصين الجنوبي، مما أدى إلى تحطم المقاتلة الصينية ومقتل قائدها وسقوطها في البحر، فأجبرت القوات الصينية الطائرة الأمريكية على الهبوط، واحتجزت طاقمها لمدة (١١) يومًا، مع قيامها بتفكيك أجزاء من الطائرة، وتمسكت الصين بأن هذه المراقبة تدخلاً غير مشروع وانتهاكًا لمجالها الجوي، وخرقًا لاتفاقية الأمم المتحدة لقانون البحار، التي تطلَّبت احترام حقوق الدول الساحلية عند التحليق فوق منطقتها الاقتصادية الخالصة[٤].

ثانيًا: شروط إعمال مبدأ عدم التدخل:

بالنظر إلى عدم وجود قاعدة دولية تُحدّد معايير أو شروط، لمضمون حظر التدخل، فقد مثَّل تكييف الفعل الذي يُمكن اعتباره انتهاكًا للمبدأ، وتدخلاً في شئون الدول موضع جدل، إلا أن محكمة العدل الدولية وفي حكمها الصادر في قضية "نيكاراجو" عام ١٩٨٦، أوردت ضبطًا لهذه الإشكالية، باعتبار أن الفعل يُعد تدخلاً غير مشروع عندما يُشكّل إكراهًا للدولة، في المسائل التي يحق لها أن تقررها بإرادة حرة، وقررت المحكمة أنه وفقًا لمبدأ السيادة، يُحظر على جميع الدول فرادي أو مجموعات، التدخل بشكل مباشر أو غير مباشر، في الشئون الداخلية والخارجية للدول الأخرى، وذلك في المسائل التي رخَّص فيها

---

(1) ***Island of Palmas Case (Netherlands v. USA),*** *2 RIAA 829, 838 (Perm. Ct. Arb. 1928).*

(٢) **حيث تم تفجير طائرة أميركية** أثناء تحليقها فوق قرية" لوكربي" الاسكتلندية عام ١٩٨٨، وتم القبض على (٢) ليبيين عام ١٩٩١، وفي عام ٢٠٠١، تمت إدانة ضابط الاستخبارات "عبد الباسط المقرحي" بالتفجير وحُكم عليه بالسجن مدى الحياة، وفي أغسطس عام ٢٠٠٩، أفرجت عنه الحكومة الاسكتلندية لإصابته بالسرطان، وتوفي في مايو ٢٠١٢، وفي عام ٢٠٠٣، أقرَّت الإدارة الليبية بالمسئولية عن تفجير "لوكربي"، ودفعت تعويضات لأسر الضحايا. **راجع: محكمة العدل الدولية،** الجماهيرية العربية الليبية ضد الولايات المتحدة الأمريكية، حكم عام ١٩٩٨.

(3) ***A. LIPTAK****, Experts Doubt Accused C.IA. Operatives Will Stand Trial in Italy, N.Y. TIMES, June 27, 2005 at A8.*

(4) ***E. DONNELLY,*** *The United States-China EP-3 Incident: Legality And Realpolitik, 9 J. CONFLICT & SECURITY L., 2004, P. 25.*

القانون لكل دولة أن تقررها بحرية مطلقة، ويكون التدخل غير مشروع عندما تُستخدم أساليب الإكراه للتأثير على شيء من هذه الخيارات[١].

ومن ثم، فإنه وفقًا لصياغة الحُكم، يُمثّل عُنصر "الإكراه" جوهر التدخل المحظور، وبحيث ينفي الفعل إرادة الدولة، ويعدم قدرتها على السيطرة عليه، كأن يتم باستخدام القوة، بشكل مباشر كالعمل العسكري، أم بشكل غير مباشر من خلال دعم أعمال تخريب، أو أنشطة إرهابية مسلحة داخل دولة أخرى، وذلك بغرض تحقيق أهداف معينة، كالحفاظ على بعض الأوضاع القائمة أو تغييرها، أو التأثير على قرارات الدولة الضحية داخليًا أو خارجيًا[٢]، أما الأفعال التي لا تتضمن قسرًا وإكراهًا للدولة فلا يُمكن أن تُمثّل تدخلاً.

ويؤكد جانب فقهي على ضابط الإكراه الوارد في حكم محكمة العدل الدولية، فيُقرر أن التدخل يُشير إلى الأفعال التي يُقصد بها إجبار دولة للحصول منها على تبعية وخضوع، عند ممارسة حقوقها السيادية، أو الحصول منها على أي مغنم من أي نوع، ولا يقتصر ذلك على البعد الإقليمي المادي، ولكن يشمل سلطتها فيما وراء إقليمها، كحماية استقلالها وحريتها السياسية[٣].

ويقرر جانب فقهي آخر، أن التدخل غير المشروع هو الذي يتضمن إكراهًا، ويُجبر دولة على التصرف بطريقة لم تكن لتختارها طوعًا، وفقًا للمجري العادي للأمور، وبما يشمل إجبارها على اتخاذ إجراءات لتأمين سيادتها، حيث يُعد الإكراه بمثابة الخط الفاصل لتحديد التدخل غير المشروع[٤].

ويري جانب فقهي ثالث، أن التدخل غير المشروع في شئون دولة، لغرض تغيير حالة فعلية موجودة أو الحفاظ عليها كما هي، يجب أن يكون "ديكتاتوريًا"، بحيث يُكره الدولة المُستهدفة ويُعدم إرادتها، مما يدفعها إلى اتخاذ قرارات فيما يتعلق بسياساتها أو ممارساتها، لم تكن لتتخذها كدولة حرة وذات سيادة[٥].

ثالثًا: مدي إمكان اعتبار ممارسة التجسس وقت السلم تدخلاً غير مشروع في شئون الدول:

قرَّر جانب فقهي أن سلوك التجسس وقت السلم ينتهك القانون الدولي، لاسيما واجب احترام مبدأ السلامة الإقليمية والاستقلال السياسي للدول الأخرى، حيث يتطلب تواجد عملاء دولة، داخل إقليم دولة أخرى دون تصريح، والقيام بجمع معلومات سريَّة غير مرخص بجمعها من الدولة المُستهدفة، علاوة على أنه إذا كان سن التشريعات الوطنية من صميم اختصاص كل دولة، وعلي الدول الأخرى احترام هذا الاختصاص الوطني؛ فإن معظم التشريعات الوطنية تحظر ممارسة التجسس وقت السلم، وتقرَّر له أشد

---

(١) **محكمة العدل الدولية، قضية "نيكاراجوا" ١٩٨٦، "*Nicaragua v. U.S.A.*"**، ٢٧ يونيو ١٩٨٦، الفقرتين ٢٠٢، ٢٠٥.

(2) ***R. HIGGINS, P. WEBB, D. AKANDE, S. SIVAKUMARAN, J. SLOAN,*** *Oppenheim's International Law: United Nations, Oxford University Press, 2019, P. 432.*

(3) ***M. S. MCDOUGAL, H. D. LASSWELL, W. M. REISMAN****, The Intelligence Function and World Public Order, P. R., PP. 365: 367.*

(4) ***S. WATTS****, Low-Intensity Cyber Operations and the Principle of Non-Intervention, Baltic Yearbook of International Law 14, 2014, P. 142.*

(5) ***C. LOTRIONTE****, Countering State-Sponsored Cyber Economic Espionage under International Law, 40 North Carolina Journal of International Law and Commercial Regulation, 2015, PP. 456:461.*

العقوبات، وتُجرّم تسلّل الجواسيس داخل أقاليمها، ومن ثم، ينتهك هذا السلوك حكم المادة رقم (٧/٢) من ميثاق الأمم المتحدة، التي قرَّرت قيدًا على الدول، بعدم التدخل في المسائل التي هي من صميم السلطان الداخلي للدول الأخرى[١].

وأورد جانب فقهي آخر أن ممارسة التجسس وقت السلم، تنتهك الواجب المقرر على الدول بموجب القانون الدولي، باحترام السيادة والسلامة الإقليمية، والاستقلال السياسي لبعضها البعض، وأن التواجد غير المصرح به، في أي جزء من إقليم دولة ذات سيادة، وبأي صورة، أو من خلال وكيل يعمل بصفته الرسمية، يشكل انتهاكًا لذلك الواجب[٢]، بل إنه لا يمكن السماح لدولة بإرسال قواتها، أو عسكرييها، أو قوات الشرطة التابعة لها، إلى أراضي أجنبية أو المرور خلالها بدون إذن[٣].

وشدّد جانب فقهي ثالث في مقال له عام ١٩٨٤، عن التجسس بالطائرات، على عدم مشروعية هذا السلوك دوليًا في وقت السلم، لانتهاكه مبدأ السيادة الإقليمية للدول، وتنافي طبيعته السرية مع ودية العلاقات بين الدول، حيث تُرسل دولة وكلاء لها سرًا إلى إقليم دولة أخري، دون علم الأخيرة أو موافقتها، للقيام بنشاط لم يُرخَّص لهم به[٤]، ووضع الفقيه تمييزًا بين السلوك الذي يتنافي مع القواعد الدولية، ويُعد غير مشروع، وبين السلوك الذي يُشكّل جريمة دولية، ورسَّخ لكون التجسس لا يشكل في حد ذاته جريمة دولية، يُمكن المحاسبة عليها في المحاكم الدولية، مثل الإبادة الجماعية، أو التعذيب، أو غيرها من جرائم الحرب أو الجرائم ضد الإنسانية، وتاريخيًا لم توجه أي محكمة دولية سواء في " نورمبرج" أو "لاهاي" أو في أي مكان أخر، اتهامًا، أو تقضي بإدانة أي شخص بسلوك التجسس.

وقرّر فقيه آخر أن التجسس وقت السلم غير مشروع، وينبغي اعتباره جريمة بموجب القانون الدولي، واقترح أن يتم إدراجه ضمن ما أُطلَق عليه الجرائم ضد الأمن "*Crimes against security*"، التي انعقدت من أجلها محاكم "نورمبرج"، و"طوكيو"، وبما يشمل جميع التصرفات التي تقوم بها دولة، بالمخالفة للمادة (٧/٢) من ميثاق الأمم المتحدة، من حيث التدخل في الشئون الداخلية لدولة أخري، وانتهاك تشريعاتها الوطنية، التي تُقرر عدم مشروعية التجسس[٥].

ومن ممارسات التجسس وقت السلم، التي أثارت انتهاك مبدأ حظر التدخل، واقعة اقتراب الغواصة السوفيتية النووية (*U-137*) عام ١٩٨١، من القاعدة البحرية السويدية "*Karlskrona*"، ثم محاصرة القوات السويدية لها، واستجواب رُبَّانها "بيوتر جوشين"، الذي قرَّر أن الغواصة ضلَّت الطريق، بسبب عطل في معدات التوجيه الملاحي[٦]. وقد أدي الحادث إلى مواجهة دبلوماسية بين السويد والاتحاد

---

(1) ***A. L. KOZIK****, the Concept of Sovereignty as a Foundation for Determining the Legality of the Conduct of States in Cyberspace,14 Baltic Yearbook of International Law, 2014, PP. 93:99.*

(2) ***Q. WRIGHT,*** *Espionage and the Doctrine of Non-Intervention in Internal Affairs, P. R., P.12.*

(3) ***L. OPPENHEIM,*** *International Law: A Treatise, P. R., P. 288.*

(4) ***I. DELUPIS****, Foreign Warships and Immunity for Espionage, 78 Am. J. INT'L L. 53, 67 (1984).*

(5) ***J. MORENOFF****, World peace Through Space Law, Michie Co., 1976, PP. 212: 215.*

(٦) **كان الاتحاد السوفييتي السابق دائم الانتهاك لهذه المساحة البحرية لمدة تُقارب ثلاثة أرباع قرن،** حيث تواجدت الغواصات الروسية في المياه الإقليمية للسويد بغرض التجسس منذ منتصف عام ١٩٥٠، ومنذ بداية عام ١٩٦٢ وحتى عام ١٩٨٨، أُشتبه في ضلوعها في أكثر من (٢٠٠) عملية تجسس داخل نفس المساحة البحرية. **راجع:**

السوفيتي السابق، حيث قدَّمت الخارجية السويدية في ٢٧ أكتوبر من عام ١٩٨١، مذكرة احتجاج للاعتراض على انتهاك إقليمها، وخرق المبادئ الأساسية للقانون الدولي، وادعاءات بوقوع أضرار نتيجة تسرب إشعاع من جسم الغواصة، **والملاحظ أن** هذه المذكرة لم تستند أو تُشر صراحةً إلى أن سبب الاحتجاج هو سلوك التجسس، ولكنها استندت إلى كونها "أنشطة غير مشروعة" تمثل تدخلاً في إقليم دولة ذات سيادة[١].

وفي عام ١٩٨٣ أسقط الاتحاد السوفييتي السابق، طائرة تابعة للخطوط الجوية الكورية، كانت تحلق فوق شبه جزيرة "*Kamchatka*"، مما أدي إلى مقتل مائتان وستون شخصًا، من بينهم عضو في الكونجرس الأمريكي، وتمسك السوفيت بمشروعية موقفهم، باعتبار أن الطائرة كانت تتجسس على منشآت عسكرية سوفيتية في جزيرة "*Sakhalin*"، وبما يُعد انتهاكًا لسيادتهم وتدخلاً في شئونهم الداخلية[٢].

وفي عام ٢٠١٣، وبعد كشف "*Snowden*" عن المراقبة التي قامت بها وكالة الأمن القومي الأمريكي لكثير الدول، والمنظمات الدولية، والأفراد، تم التعامل مع هذه الواقعة من جانب دول مثل "البرازيل"، و"جزر البهاما"، و"إندونيسيا"، باعتبارها تخالف القانون الدولي، الذي رسَّخ لحق كل دولة في السيطرة الكاملة والمتفردة على أراضيها، ومواطنيها، وشئونها، وحظر عليها التدخل علنًا أو سرًا في الشئون الداخلية أو اختصاصات الدول الأخرى. وبالتالي، لم تقبل تلك الدول سلوك التجسس في وقت السلم بوجه عام، واعتبرته فعلاً غير مشروع، ويُمثّل انتهاكًا لسيادتهم وتدخلاً في أقاليمهم، بالمخالفة للحقوق والواجبات المقرر دوليًا في هذا الشأن[٣].

ووفقًا لما سبق، يمكننا القول بالآتي:

(١) يتحقق انتهاك السيادة والسلامة الإقليمية، عندما تقوم دولة بالتدخل وبأي شكل في إقليم دولة أخرى، بغض النظر عن تحقق أضرار نتيجة هذا التدخل من عدمه[٤]، وقد رسّخت محكمة العدل الدولية لمبدأ حظر التدخل، وأوردت معيارًا لتحقق هذا التدخل، وهو أن يُشكّل إكراهًا للدولة، ويؤثر على قراراتها بشأن اختيار النظام السياسي، أو الاقتصادي، أو الاجتماعي، أو الثقافي، أو على صياغة سياستها الخارجية، أو أي مسألة مما يحق للدول أن تقررها بإرادتها الحرة، أما الأفعال التي لا تتضمن قسرًا فلا يُمكن أن تُمثّل تدخلاً.

***B. J. THEUTENBERG**, U 137 – Folkrätt och neutralitetspolitik i tillämpning, 2 Kungliga Krigsvetenskapsakademins handlingar och tidskrift, 1982, PP. 12: 13.*

(1) ***R. OLIPHANT**, Why Would a Russian Submarine Enter Swedish Waters?, TELEGRAPH (Oct. 20, 2014), **available at:** http://www.telegraph.co.uk/ news/worldnews/europe/sweden/11174289/Why-would-a-Russian-submarine-enter-Swedish-waters.html. 15/3/2020.*

(2) ***W. RICHEY,** Theories Persist on KAL 007 Shootdown, CHRISTIAN SCI. MONITOR, May 28, 1986, P. 3.*

(3) ***J. F. MURPHY**, Cyber War and International Law: Does the International Legal Process Constitute a Threat to U.S. Vital Interests? 89 International Law Studies, 2013, P. 309.*

(4) ***W. H. V. HEINEGG**, Territorial Sovereignty and Neutrality in Cyberspace, International Law Studies 89, 2013, P. 129.*

(٢) يتفق الباحث مع الاتجاه الخاص بأن التجسس وقت السلم، ينتهك واجب احترام مبدأ السيادة والسلامة الإقليمية، والاستقلال السياسي للدول الأخرى، ويُمثّل تدخلاً في شئون الدول، بدايةً من تواجد عملاء دولة على إقليم دولة أخرى دون إذن أو تصريح، ثم جمعهم لمعلومات غير مرخص بجمعها، وصولاً إلى مخالفة هذا السلوك للتشريعات الوطنية التي تحظر ممارسة التجسس وقت السلم، وتقرر له أشد العقوبات، ووصولاً إلى إمكان استخدام تلك المعلومات في التأثير على إرادة الدولة، أو في القيام بعمل عسكري ضدها، أو القيام بأي فعل يحرم أو يعوق استخدام الدول لحقوقها السيادية في تسيير شئونها الداخلية والخارجية، واستقلالها في الحكم.

(٣) على الرغم من عدم تصنيف التجسس وقت السلم في حد ذاته كجريمة دولية، إلا أن طبيعته السرية تتنافي مع ودية العلاقات بين الدول، وهو ما كشفت عنه الممارسات الدولية الخاصة بهذا السلوك، حيث قرَّرت الدول التي استهدفها التجسس وقت السلم، عن احتجاجها عليه، كونه نشاطًا غير مشروع، ويُمثل تدخلاً في أقاليم دول ذات سيادة، ولا يمكن قبوله في العلاقات الدولية.

(٤) **إلى جانب اتفاق الباحث مع انتهاك التجسس وقت السلم لواجب احترام مبدأ السيادة والسلامة الإقليمية للدول**، فإنه يطرح فكرة تأسيس عدم مشروعية هذه الممارسة، على مخالفتها للمبادئ العامة للقانون، المنصوص عليها في المادة (١/٣٨/ج) من النظام الأساسي لمحكمة العدل الدولية، كأحد مصادر القانون الدولي، حيث إنه إذا أمكن جمع ومقارنة جميع تشريعات التجسس الموجودة في دول العالم، ربما يمكن القول بأن هناك حظر دولي للتجسس، باعتبار أن غالبية القوانين الوطنية ـ إن لم يكن كلها ـ تُجرّم هذا السلوك وتعاقب عليه، وبالتالي يمكن اعتبار أن هذه العمومية في التجريم، تدخل في نطاق مخالفة ممارسة التجسس لهذا المصدر من مصادر القانون الدولي.

الفرع الثالث

الاتجاه الخاص بأن التجسس لا هو مشروع ولا هو غير مشروع

أورد الفقيه "*Scott*" عام ١٩٩٩، أن حالة التجسس وقت السلم وفقًا للقانون الدولي لا تزال غامضة، ولا توجد أي اتفاقية دولية تحظر هذا السلوك أو تجيزه، وفي الممارسات الدولية، دائمًا ما تعلن الدول أن التجسس وقت السلم غير مقبول، ولكنه ليس محظورًا، بل إن معظم الدول لها مصلحة للقيام بهذا النشاط، مع حظره وتجريمه على الغير بموجب التشريعات الوطنية[1]. ومن ثم فإن الفقيه يعتقد بأن التجسس ليس قانونيًا، ولا غير قانوني، لعدم وجود تنظيم ساري ينظمه، ولازدواج معايير الدول بشأنه، حيث تمارسه، ولا تستبعد أن يتم ممارسته ضدها، ولكنها تحظره في تشريعاتها الوطنية، وتعترض وتحتج عندما يستهدفها.

ويذهب الفقيه "*Demarest*" إلى أن مسألة مشروعية التجسس وقت السلم، أو عدم مشروعيته، لا يمكن الجزم بها، ولكن على الدول إعمال مبدأ الحيطة بشأن هذا السلوك، مع حق كل دولة في ملاحقة من يقومون به. ونلاحظ أن الفقيه لا يُقر هذا السلوك ولا يدافع عنه، ولكنه أيضًا لا يُقرّر عدم

(1) ***R. D. SCOTT***, *Territorially Intrusive Intelligence Collection and International Law, P. R., PP. 220: 223.*

مشروعيته[١].

وهي نفس رؤية الفقيه "*Christopher Baker*"، بشأن غموض الوضع القانوني للتجسس وقت السلم، حيث أشار في مقال له عام ٢٠٠٤، إلى عدم وجود أي ترخيص أو حظر صريح بشأن التجسس وقت السلم في المعاهدات الدولية، وانتهي إلى أن وضع هذا السلوك وفقًا للقانون الدولي يتصف بعدم التحديد[٢]".

من جانبه يرى "*Daniel Silver*" أن الوضع القانوني الدولي للتجسس يكاد تكون "متناقضًا"، حيث تتجه الدول للتجسس على بعضها، وتُدين التجسس الموجه ضدها، ويُبيّن الفقيه أن القَدْر المتيقن بشأن هذه المسألة، أن سلوك التجسس لم يُحظر صراحةً بموجب معاهدة، أو غيرها من قواعد القانون الدولي، وكذلك لم يُسمح به إلا في زمن الحرب، حيث اعتبر ممارسة مقبولة تحكمها قوانين الحرب[٣].

ويؤكد جانب فقهي آخر على غموض الوضع القانوني الدولي للتجسس في وقت السلم، من حيث عدم حظره أو إباحته، فلا هو مشروع ولا هو غير مشروع، وفى ضوء غياب أي قواعد صريحة، باستثناء بعض القواعد التي توضح تعارض هذا السلوك مع الوظيفة الدبلوماسية، لا يزال التجسس وقت السلم يخضع للقوانين الوطنية، ويخرج عن نطاق القواعد الخاصة بقانون الحرب[٤].

وفيما يتعلَّق بمدى شرعية أنشطة التجسس التي تتم من البحار وقت السلم، فإن لها خصوصية مميزة، وفقًا لاتفاقية الأمم المتحدة لقانون البحار لعام ١٩٨٢، وقواعد القانون الدولي الأخرى ذات الصلة، **ونوالي دراسة هذه الخصوصية والأحكام ذات الصلة بها، من خلال المبحث التالي.**

(1) ***L. T. COL, G. B. DEMAREST,*** *Espionage in International Law, P. R., PP. 321: 321.*
(2) ***C. D. BAKER****, Tolerance of International Espionage, P. R., P. 10091: 1093.*
(3) ***D. B SILVER****, Intelligence and Counterintelligence, in John Norton Moore and Robert F Turner (eds), National Security Law, Durham, NC: Carolina Academic Press, 2nd edn., 2005, P. 965.*
(4) ***K. ZIOLKOWSKI****, Peacetime Cyber Espionage, P. R., P. 430.*

المبحث الثالث

خصوصية تنظيم سلوك التجسس من البحار وقت السلم

تتسابق بعض الدول للتمركز في بعض أجزاء من البحار كمنطقة المحيط الهادئ، وتسعى لوضع أكبر عدد ممكن من القطع البحرية فيها، لأغراض متعددة لاسيما جمع المعلومات[١]، نظرًا لوجود حالة من العداء والتوتر، والنزاعات التاريخية بشأن جزر في تلك المنطقة بين بعض الدول، والتي تحرص على تجهيز قطعها البحرية بإمكانات متطورة، تمكنها من التخفي والاقتراب من شواطئ الدول الأخرى دون اكتشافها، والقيام بالمراقبة ونقل المعلومات، من خلال إشارات وترددات سرية مشفرة، مع التذرع بأن ذلك لا يُخالف القانون الدولي، ويتوافق مع مبدأ حرية الملاحة الوارد في المادة (٨٧) من اتفاقية الأمم المتحدة لقانون البحار[٢].

وكان من أكثر الدول مُداومةً على ممارسة التجسس من البحار، الولايات المتحدة الأمريكية، والاتحاد السوفيتي السابق، والصين، وكوريا الشمالية، ويرجع تاريخ أول الوقائع التي أثارت ممارسة هذا السلوك، إلى منتصف العشرينيات، عندما قامت غواصات روسية في عام ١٩٢٥، بدوريات قبالة ساحل الولايات المتحدة، على بعد أربعين ميلًا من شاطئ كاليفورنيا الشمالية، بغرض جمع معلومات عن القطع البحرية الحربية الأمريكية، ولدى مطاردة القوات الأمريكية للغواصات سارعت بالهروب[٣].

وتُثار خصوصية التجسس من البحار من وجهين، **أولهما:** وجود نصوص صريحة تحظر جمع المعلومات، من قبل السفن والغواصات التي تمر في المساحات البحرية للدول الساحلية في أوقات السلم، لاسيما الأحكام المُتعلقة بالمرور البريء في البحار الإقليمية والمضايق، وبما يمكن فهمه بأن اتفاقية قانون البحار لعام ١٩٨٢، قد قرّرت عدم مشروعية سلوك التجسس من البحار وقت السلم. **وثانيهما**: ما قرَّرته

---

(١) **تتمركز في هذه المنطقة قطع بحرية لحوالي (٤٠) دولة، منها ما يقرب من (٥٥٠) غواصة تعمل بالطاقة النووية،** حيث إنها أكثر أنواع الغواصات قدرة على التحمل، والتخفي، وسلاسة الحركة، وعلى سبيل المثال، تنشر "الولايات المتحدة الأمريكية" فيها (٧٢) غواصة، منها (٥٨) تعمل بالطاقة النووية، وتنشر "روسيا" (٦٤) غواصة، منها (١١) نووية. وتُشغل "المملكة المتحدة" و"فرنسا" (٦) غواصات نووية. ولكل من "تركيا"، و"إسرائيل" (١٤) غواصة. وتُشغِّل "إيران" (٣١) غواصة. والصين (٦٦) غواصة، وتنشر "الهند" (١٥) غواصة منها واحدة نووية. وتُشغل عشر دول أخري في تلك المنطقة نحو (١٧٣) غواصة، مثل "أستراليا"، "إندونيسيا"، "اليابان"، "ماليزيا"، "باكستان"، "سنغافورة"، كوريا الجنوبية"، "تايوان"، "فيتنام". **راجع:**

S. PERLO-FREEMAN, C. SOLMIRANO, *Stockholm Int'l Peace Research Inst., SIPRI Fact Sheet: Trends in World Military Expenditure, 2013, 2014, PP. 4: 5;* ***S. SAUNDERS****, United States, in IHS JANE'S FIGHTING SHIPS 2014–2015, 2014, PP. 927, 934:940;* ***Total Submarine Strength by Country,*** *GLOBAL FIREPOWER,* ***available at:*** *http://www.globalfirepower.com/ navy-submarines.asp.13/3/2020.*

(٢) **نصت المادة (٨٧) من اتفاقية الأمم المتحدة لقانون البحار لعام ١٩٨٢، بعنوان "حرية البحار" على أنه:** "١- أعالي البحار مفتوحة لجميع الدول، ساحلية كانت أو غير ساحلية. وتمارس حرية أعالي البحار بموجب الشروط التي تبينها هذه الاتفاقية وقواعد القانون الدولي الأخرى، وتشتمل فيما تشتمل، بالنسبة إلى كل من الدول الساحلية وغير الساحلية، على: أ- حرية الملاحة؛ ب- حرية التحليق؛ ج- حرية وضع الكابلات وخطوط الأنابيب المغمورة؛ د- حرية إقامة الجزر الاصطناعية وغيرها من المنشآت؛ هـ- حرية صيد الأسماك؛ و- حرية البحث العلمي. ٢- تمارس هذه الحريات من قبل جميع الدول مع إيلاء المراعاة الواجبة لمصالح الدول الأخرى في ممارستها لحرية أعالي البحار، وكذلك الاعتبار الواجب لما تنص عليه هذه الاتفاقية من حقوق فيما يتعلق بالأنشطة في المنطقة".

(3) ***D. F. WINKLER****, Cold War at Sea: High Seas Confrontation between the United States and the Soviet Union, 2000, PP. 33: 34.*

المادة (٨٧) من الاتفاقية، بشأن حق الأطراف في حرية الملاحة والتحليق، وغيرها من الاستخدامات المشروعة المرتبطة بتشغيل السفن والطائرات في أعالي البحار، والذي ربما يُفهم باعتبار أن جمع المعلومات يدخل ضمن نطاق هذه الحريات، لاسيما أن السفن والطائرات في منطقة أعالي البحار تخضع وبشكل حصري لقوانين دولة العلم وفقًا للمادتين رقمي (٩٢، ٩٤) من الاتفاقية. **ونوالي عرض خصوصية سلوك جمع المعلومات من البحار، من خلال المطلبين التاليين.**

المطلب الأول: بعض وقائع لتجسس الدول في البحار.

المطلب الثاني: القواعد الدولية بشأن التجسس من البحار.

المطلب الأول

بعض وقائع لتجسس الدول من البحار

تعددت وقائع التجسس في المساحات البحرية للدول، وكان من أبرز الممارسين لهذا السلوك هي الولايات المتحدة الأمريكية، والاتحاد السوفيتي السابق، وكذلك الصين وكوريا الشمالية، ونعرض لنماذج من وقائع التجسس التي مارستها هذه الدول، ورد الفعل عليها سواء من الدول المتضررة أو المجتمع الدولي، وذلك من خلال الفروع التالية.

الفرع الأول

بعض وقائع التجسس الروسي من البحار

خلال عام ١٩٤٧، رصدت الولايات المتحدة الأمريكية، خمس غواصات روسية تقبع بالقرب من قواعد عسكرية بحرية أمريكية، أمام جزر "الأكيونين" في المحيط الهادي، وصرَّح قائد الأسطول الأمريكي وقتها "جون سيلفان" أن الغواصات كانت تجمع معلومات عن تسليح القطع البحرية الأمريكية. وخلال نفس العام رُصدت غواصة روسية حاملة للصواريخ "الباليستية"، قرب الساحل الشرقي للولايات المتحدة وعلى بعد (١٢) ميل من "كيب هنري" - "فرجينيا"، ووفقًا لضابط الاستخبارات الأمريكي "*Charles C. Kirkpatrick*"، أن الغواصة كانت تمارس التجسس، بواسطة إحدى عشر جهازًا هوائيًا لالتقاط الإشارات، إلا أن البحرية الأمريكية لم تتعامل معها أو تُبعدها، لأنها ظلت في المياه الدولية ولم تغادرها، ونحن شعب يحترم القانون الدولي ويلتزم به[1].

وخلال عام ١٩٥٥ تم رصد (٥) حالات لسفن وغواصات روسية، وهي تمارس التجسس في البحار السويدية، وبدايةً من عام ١٩٦٢ وحتى عام ١٩٨٨، أُشتبه في وقوع أكثر من (٢٠٠) عملية تجسس داخل الحدود البحرية السويدية. وفي فبراير من عام ١٩٦٠، اتهم وزير الدفاع البريطاني "هارلود واتكنسون" السوفييت، بنشر دوريات بحرية من الغواصات، بغرض التجسس على الأسلحة النووية التي

(1) ***J. RAYMOND**, Soviet Trawler Called Spy Ship, P. R., P. 8.*

كان يجري اختبارها على الساحل البريطاني، وكذلك على القاعدة الصاروخية البالستية في "رولي لوك"، و"اسكتلندا"[١].

وفي الفترة ما بين عام ١٩٦٩، وحتى ١٩٨٣، أرسل الاتحاد السوفيتي (٢٢) سفينة حربية إلى "كوبا"، تمركزت قبالة الساحل الشرقي للولايات المتحدة الأمريكية، وتجسّست على قواعد الأسطول الأمريكي[٢].

وفي عام ١٩٨١، رُصدت الغواصة السوفيتية النووية (*U-137*)، وهي تتجسس على القاعدة البحرية السويدية "*Karlskrona*"، مما أدي إلى مواجهة دبلوماسية بين السويد والاتحاد السوفيتي السابق، وقدَّمت الخارجية السويدية في ٢٧ أكتوبر عام ١٩٨١، مذكرة احتجاج اعترضت فيها على انتهاك إقليمها، وخرق المبادئ الأساسية للقانون الدولي، وادعاءات بأضرار نتيجة تسرب إشعاع من جسم الغواصة[٣].

وخلال عام ١٩٨٣، نشرت البحرية الروسية في البحر الكاريبي، قُبالة ساحل "فلوريدا"، سفينتين سطحيتين ـ حاملة صواريخ موجهة وفرقاطة بحرية ـ بالإضافة إلى غواصة، وسفينة الإمداد " *Genrik Gasanov*"، وذلك لمراقبة تجارب صاروخية أمريكية كانت تُجري في ميناء "كيب كانافيرال"، وكانت الولايات المتحدة تحتج بأن هذه الوقائع غير مشروعة[٤].

وخلال يومي ٢٨، ٢٩ من شهر إبريل عام ٢٠١٥، رصد الأسطول البحري الفنلندي غواصة روسية، تقبع بالقرب من المياه الإقليمية للعاصمة "هلسنكي"، وعلي بعد حوالي (١٧٥) ميل من قاعدة بحرية روسية في "بطرسبرج"، وقامت القوات الفنلندية بإنزال معدات كي تُوقف الغواصة، إلا أن الأخيرة سارعت بالهروب[٥].

الفرع الثاني

بعض وقائع تجسس الولايات المتحدة الأمريكية من البحار

كانت الولايات المتحدة الأمريكية من أكثر الدول التي وُجِّه إليها اتهامات بالتجسس من البحار، لاسيما من "الصين" و"كوبا" و"الاتحاد السوفيتي السابق"، وترجع تاريخ الممارسات الامريكية ذات الصلة، إلى وقت نشوب الحرب العالمية الثانية، حيث بدأت القطع البحرية تنتشر على طول ساحل جزر

---

(1) ***P. WALKER***, *Sweden Searches for Suspected Russian Submarine Off Stockholm, P. R., Website.*

(2) ***R. HALLORAN***, *Soviet Ships Came Close, Navy Says, N.Y. TIMES (Feb. 14, 1983),* ***available at:*** *http://www.nytimes.com/1983/02/15/world/soviet-ships-came-close-navy-says.html.2/4/2020.*

(٣) **ولم تستند المذكرة أو تُشر صراحةً إلى أن سبب الاحتجاج هو التجسس**، ولكنها استندت إلى كونها "أنشطة غير مشروعة". **راجع:**

B. J. THEUTENBERG, *U 137 – Folkrätt och neutralitetspolitik i tillämpning, P. R., Website.*

(4) ***R. HALLORAN***, *Soviet Ships Came Close, Navy Says, N.Y. TIMES (Feb. 14, P. R., Website.*

(5) ***A. MARSZAL***, *Finland Fires Warning Shots at "Foreign Submarine" Near Helsinki, (Apr. 28, 2015),* ***available at:*** *http://www.telegraph.co.uk/news/worldnews/europe/finland/11568042/Finland-fires-warning-shots-at-foreignsubmarine- near-Helsinki.html. 5/3/2020.*

"الباسيفيك"، التي كانت اليابان تحتلها، بغرض الاستطلاع وجمع المعلومات، وخلال ديسمبر عام ١٩٤٩، تم نشر دوريات من الغواصات على طول مضيق "تايوان"، وفي المياه الإقليمية الصينية، بغرض جمع معلومات عسكرية، وبالفعل تمكنت من ذلك، بعد اقترابها من موانئ "آموي"، و"فوكو" لما يُقارب ستة أميال بحرية[١].

وفى يونيو من عام ١٩٥٠، توسعت الولايات المتحدة في نشر غواصاتها لتشمل مياه "بتروبا فسلوفسك" في بحر اليابان، لمراقبة عمليات الشحن المختلفة للأسطول الروسي البحري، والميناء التجاري للشرق الأقصى، وأثناء الحرب الكورية رَصدت هذه الغواصات كميات وأنواع التحويلات والبضائع، وغيرها مما تم إرساله بالسفن بواسطة الاتحاد السوفييتي من "فالدي فوستوك" في كوريا الشمالية، وامتدت رقابة هذه الغواصات داخل المياه الإقليمية لجزر روسيا حيث تتركز أكبر القواعد النووية السوفييتية في "ماستوتش"[٢].

وفي أغسطس من عام ١٩٦١، احتجَّت "كوبا" على وجود غواصات أمريكية داخل مياهها الإقليمية، وقيامها بعمليات تجسس تحت اسم عملية "هولي ستون"، والتي استمرت حوالي تسعين يومًا، وهدفت لجمع معلومات عن الأسطول البحري الكوبي[٣].

وفي عام ١٩٦٤، قامت المدمرة الأمريكية "مادوكس" بالتجسس في خليج "تونكين" قُبالة ساحل فيتنام الشمالية، ورصدتها القوات البحرية الفيتنامية وهاجمتها[٤]، مما دفع الكونجرس الأمريكي للاجتماع في السابع من أغسطس من نفس العام، وإصدار ما عُرف بقرار خليج "تونكين"، الذي أعطى للرئيس الأمريكي حينها "جونسون" تفويضًا واسعًا، لاتخاذ الإجراءات اللازمة، وبما يشمل استخدام القوة، تجاه تأمين قُبالة فيتنام الجنوبية[٥]، وكان ذلك القرار مؤشرًا على دخول الولايات المتحدة في حرب مع فيتنام.

وفي عام ١٩٦٧، قامت وكالة الأمن القومي الأمريكية، بنشر مجموعة من سفن التجسس بوسائل إلكترونية، ومنها السفينة "*USS Liberty*"، والمُصنَّفة كسفينة أبحاث تقنية، لجمع معلومات استخباراتية خلال الحرب بين جمهورية مصر العربية وإسرائيل، وذلك في المياه الدولية قبالة ساحل سيناء، وقد تعرضت السفينة لهجوم خاطئ، من قبل بعض القطع الحربية الإسرائيلية والطائرات الحليفة لها[٦].

وفي ٢٣ يناير من عام ١٩٦٨، احتجزت دورية بحرية لكوريا الشمالية السفينة الأمريكية "*Pueblo*"، داخل المياه الإقليمية الكورية، باعتبارها كانت تقوم بإبلاغ معلومات استخباراتية[٧]، وردت

---

(1) ***B. WOODWARD,*** *VEIL: the Secret Wars of the CIA, 1981– 1987, 2005, PP. 455:463.*
(2) ***S. KAYE,*** *Freedom of Navigation, Surveillance and Security: Legal Issues Surrounding the Collection of Intelligence from Beyond the Littoral, 24 AUSTRALIAN Y.B. INT'L L., 2005, P. 93.*
(3) ***B. WOODWARD****, VEIL: THE SECRET WARS OF THE CIA, 1981– 1987, 2005, PP. 455–460.*
(4) ***E. E. MOISE****, Tonkin Gulf and the Escalation of the Vietnam War 50–66 (1996).*
(5) ***L. B. JOHNSON****, U.S. Reaction to Events in the Gulf of Tonkin, August 1–10, 1 VIETNAM 1963– 1968, 1964, 1992, P. 589.*
(6) ***A. J. CRISTOL,*** *the Liberty Incident Revealed: the Definitive Account of the 1967 ISRAELI ATTACK ON THE U.S. NAVY SPY SHIP 172 (2013).*
(7) ***G. H. ALDRICH,*** *Questions of International Law Raised by the Seizure of the U.S.S. Pueblo, 63 AM. SOC'Y INT'L L. PROC. 2 (1969).*

السلطات الأمريكية بأن السفينة كانت في أعالي البحار، ولها الحق في حرية الملاحة، وبما يشمل الاستماع إلى الإشارات الإلكترونية من أي مكان، وأنها سفينة حربية تتمتع بحصانة سيادية، حتى مع كونها قد دخلت بالخطأ إلى البحر الإقليمي لكوريا الشمالية[١].

وفي عام ١٩٩٢، وجَّه الاتحاد السوفييتي السابق تحذيرًا للولايات المتحدة الأمريكية، بسبب نشر الأخيرة لغواصات في المياه الإقليمية السوفيتية، وصرَّح وزير الدفاع السوفيتي السابق "ريتشارد سفيني" باختراق الولايات المتحدة للمياه الإقليمية لبلاده، وتعامل الأسطول السوفييتي معها بالقوة[٢].

وفي أبريل من عام ٢٠٠١، اعترضت طائرتان مقاتلتان صينيتان، مروحية أمريكية من طراز (*EP-3*)، وهي تقوم بمهمة استطلاع في بحر الصين الجنوبي، وأثناء الاعتراض حدث تصادم بين إحدى المقاتلتين والمروحية، نتج عنه سقوط المقاتلة في البحر وفقد قائدها، وكذلك هبوط المروحية اضطراريًا في جزيرة "*Hainan*"، وقامت السلطات الصينية باحتجاز طاقم المروحية الأمريكي لأكثر من أسبوع، وذلك بعد تفكيك الطائرة من معداتها الالكترونية المتطورة، وقد سارعت الولايات المتحدة الأمريكية بالاحتجاج على معاملة الصين للطائرة وطاقمها، واعتبار أن ذلك يمثل انتهاكًا لسيادتها، مع التأكيد على حقها في ممارسة حرية التحليق في المنطقة الاقتصادية الخالصة للصين[٣].

وفي عام ٢٠٠٩، وأثناء قيام السفينة الأمريكية "*USNS*" بإجراء عمليات استطلاع وجمع معلومات استخباراتية في المنطقة الاقتصادية الخالصة للصين، قامت سفن بحرية صينية بمطاردتها ومحاصرتها، والقبض عليها، وإجراء تحقيقات مع طاقمها، ثم أعلنت "الصين" أن السفينة كانت تقوم بمهام تجسس[٤].

الفرع الثالث

بعض وقائع لتجسس الصين وكوريا الشمالية من البحار

مارست "الصين"، و"كوريا الشمالية" عمليات تجسس بحري لاسيما ضد "اليابان"، و"كوريا الجنوبية"، ومن ذلك، أنه خلال سبتمبر عام ١٩٩٦، رُصدت غواصة لكوريا الشمالية بالقرب من المياه الإقليمية لنظيرتها الجنوبية، وعلى متنها إحدى عشر قتيلاً في ملابس مدنية، وتبين أنهم كانوا يحاولون التسلل لكوريا الجنوبية، ثم اشتبكت معهم قوات حرس الحدود وقتلتهم، مقابل قُتل ثلاثة من القوات، وقرَّرت "كوريا" الشمالية، أن الغواصة قد انحرفت تجاه "كوريا" الجنوبية نتيجة عطل في محركها، وطالبت بتسليم جثث البحارة، إلا أن "كوريا" الجنوبية رفضت، على سند من أن هذه المجموعة، كانت

---

(١) **احتجزت السلطات الكورية طاقم السفينة لمدة (١١) شهرًا**، وطلبت منهم التوقيع على "اعترافات" بالدخول إلى مياهها الإقليمية للتجسس، ثم وقَّعت الدولتان وثيقة، ورد فيها أن الولايات المتحدة تعترف بارتكاب مخالفة وتعتذر عنها، وفور الإفراج عن البحارة، أصدر ممثل الولايات المتحدة الأمريكية بيانًا، نفي فيه صحة الوثيقة، وقرَّر أنه أُكره على التوقيع عليها كشرط لتحرير الطاقم. **راجع:**

***Pueblo**, Seizure: Facts, Law, Policy, 63 AM. SOC'Y INT'L L.PROC. 1, 1–2 (1969).*

(2) ***A. H. DEAN,** the Second Geneva Conference on the Law of the Sea: The Fight for Freedom of the Seas, 54 AM. J. INT'L L. 751, 751 (1960).*

(3) ***R. PEDROZO**, Military Activities in and over the Exclusive Economic Zone, in Freedom of Seas, Passage Rights and the 1982 Law of the Sea Convention Myron H. Nordquist, Tommy T.B. Koh & John Norton Moore eds., 2009, PP. 235, 239:48.*

(4) ***United States Protests Chinese Interference with U.S. Naval Vessel**, Vows Continued Operations, 103 AM. J. INT'L L., 2009, P. 349.*

تتجسس بغرض التخطيط لقتل الرئيس "بارك شانج" . وعلى أثر ذلك، أصدر رئيس مجلس الأمن بيانًا، ناشد فيه الطرفين التزام التهدئة، ووقف أي أعمال عدائية، إلى حين التوصل إلى اتفاق سلام، وقد أشادت كوريا الشمالية بالبيان، واعتبرته انتصارًا لها، لأنه لم يلق باللوم عليها[١].

وفي عام ١٩٩٨ تم القبض على غواصة تابعة لكوريا الشمالية في المياه الإقليمية لكوريا الجنوبية، وبادر (٩) أفراد من على متن السفينة بالانتحار، خوفًا من القبض عليهم، وأوضحت وكالة استخبارات "كوريا" الشمالية، أن القارب أصابه عطل، جعله ينحرف عن طريقه ويدخل المياه الإقليمية لكوريا الجنوبية، بينما قرَّرت كوريا الجنوبية أن القارب كان يقوم بالتجسس عليها[٢].

وفي ١٠ نوفمبر من عام ٢٠٠٤، تواجدت إحدى الغواصات الصينية في المياه الإقليمية لليابان، فوجَّهت لها السلطات اليابانية أمرًا بالطفو على السطح، وإلا فإنها ستُعامل كغواصة معادية، وبعد الواقعة، قدَّم وزير الخارجية الياباني احتجاجًا رسميًا ضد الصين، على سند من أن تواجد هذه الغواصة في المياه اليابانية يُعد انتهاكًا للقانون الدولي، وطالب "الصين" باعتذار رسمي، وتوضيح وافٍ لما حدث، وردت "الصين" بأن دخول غواصتها إلى المياه اليابانية كان بطريق الخطأ نتيجة عطل فني. إلا أنه بعد الواقعة، استمرت الغواصات الصينية بالتواجد قرب بعض الجزر اليابانية[٣]، وفي مارس من عام ٢٠١٤، أعلن وزير الدفاع الياباني تشكّكه في الدور الذي تقوم به الغواصات الصينية في المحيطين، الهندي والهادي، حيث يعتقد بأنها تعمل على تأجيج الصراعات بين دول مثل "تايوان"، و"فيتنام"، و"الفلبين"، و"ماليزيا"، و"بيروني"، و"إندونيسيا"، والجزر الأخرى في "أمريكا"، و"الهند"، و"استراليا"، مما يعرِّض السلم والأمن في هذه المناطق للخطر[٤].

وخلال عام ٢٠١٠، قامت إحدى غواصات كوريا الجنوبية بإغراق قارب تابع لكوريا الشمالية في البحر الأصفر، بادعاء أنه كان يقوم بمهمة تجسس، مما أدي لوفاة (٦٤) شخصًا كانوا على متن القارب، وبعرض الأمر على مجلس الأمن، لم يستطع التوصل إلى قرار كما لم يقم بإدانة الحادثة[٥].

المطلب الثاني

القواعد الدولية بشأن التجسس من البحار

نتطرق لدراسة الوضع القانوني للتجسس والحصول معلومات من المساحات البحرية للدول، وذلك على ضوء خصوصية الأحكام الواردة في اتفاقية الأمم المتحدة لقانون البحار لعام ١٩٨٢، لاسيما النظام القانوني الخاص بالمساحات البحرية، وذلك من خلال الفروع التالية.

---

(1) ***S. BAGDASAROVA,*** *Brave New World: Challenges in International Cybersecurity Strategy and the Need for Centralized Governance, 119 PENN. ST. L. REV., 2015, PP. 1030:1033.*

(2) ***R. PEDROZO****, Close Encounters at Sea: The USNS Impeccable Incident, 63 NAVAL WAR C. REV., 2009, P. 101.*

(3) ***K. E. CALDER****, China and Japan's Simmering Rivalry, 85 FOREIGN AFF., 2006, PP. 129: 133.*

(4) ***K. TAKAHASHI, J. HARDY****, Japan Tracks Suspected Chinese Sub near Okinawa Island, JANE'S DEFENCE WKLY., Mar. 20, 2014.*

(5) ***J. ASHLEY ROACH, ROBERT W. SMITH,*** *Excessive Maritime Claims, Vaughan Lowe & Robin Churchill eds., 3d ed. 2012, PP. 379: 385.*

الفرع الأول

التجسس في البحر الإقليمي

للدولة الساحلية سيادة على بحرها الإقليمي، باستثناء القيد المتمثل في حق المرور البريء للسفن والغواصات[١]، والذي نصت عليه المادة (١٧) من اتفاقية قانون البحار لعام ١٩٨٢، بحيث يُرَخَّص لسفن جميع الدول بالعبور السريع والمتواصل في البحر الإقليمي لدولة ساحلية بغرض اجتيازه، ويكون هذا المرور بريئًا عند استيفاء مُتطلَّبات المادة (١/١٩) من الاتفاقية، والامتناع عن القيام بأنشطة تضر بسلم الدولة الساحلية أو بحسن نظامها أو بأمنها، مما يُغيّر طبيعة المرور ويصبح "غير بريء"، وأوردت المادة اثني عشر نشاطًا، **منها: أي عمل يكون بغرض جمع معلومات للإضرار بأمن الدولة الساحلية؛** وأي عمل يهدف إلى التدخل في نظم اتصالات مرافق أو منشآت أخرى تابعة للدولة الساحلية؛ وأي نشاط آخر لا يتعلق مباشرة بالمرور[٢].

وحري بالذكر، أنه ينبغي التمييز بين سلوك جمع معلومات عن الدول الساحلية، وبين معرفة المعلومات الضرورية بشأن التنقل بأمان في البحار، أو ما يُعرف بعلم المحيطات "*Oceanography*"، ويشمل التعرَّف على خصائص الطقس، وتيارات المد والجزر، وعمق المياه، وأنماط حركة الملاحة البحرية[٣]، والتي لم تحدد القواعد الدولية قدرًا معيّنًا لها، إلا أن تخطي الحد المُتعارف عليه وفقًا للأصول البحرية، يجعل مرور السفينة غير برئ بموجب حكم المادة (١٩) من الاتفاقية[٤]. وعلى سبيل المثال، اعتادت السفن الحربية الأمريكية عند مرورها بالبحار الإقليمية للدول، مسح البيئة البحرية لأغراض غير

---

(١) **ابدأ اعتماد هذا الحق من قبل معهد القانون الدولي عام ١٨٩٤**، ولكن ثار الجدل بشأن امتداده إلى السفن الحربية، قياسًا على عدم أحقية جيوش الدولة في عبور أقاليم الدول الأخرى، وفي الفترة من عام ١٩٢٧، وحتى عام ١٩٣٠، وافقت اللجنة التحضيرية لمؤتمر عصبة الأمم بشأن التدوين التدريجي للقانون الدولي، على انطباق المرور البريء على السفن الحربية. وفي عام ١٩٥٨، أكَّدت الاتفاقية المتعلقة بالبحر الإقليمي والمنطقة المتاخمة أن جميع الدول تتمتع بحق المرور البريء، بما في ذلك السفن الحربية. **راجع:**

***J. S. REEVES**, the Codification of the Laws of Territorial Waters, 24 AM. J. INT'L L. 486, 1930, PP. 490:493.*

(٢) **نصت المادة رقم (١٩) من اتفاقية قانون البحار لعام ١٩٨٢ على أنه:** "١- يكون المرور بريئا مادام لا يضر بسلم الدولة الساحلية أو بحسن نظامها أو بأمنها. ويتم هذا المرور طبقا لهذه الاتفاقية ولقواعد القانون الدولي الأخرى. ٢- يعتبر مرور سفينة أجنبية ضارًا بسلم الدولة الساحلية أو بحسن نظامها أو بأمنها إذا قامت السفينة أثناء وجودها في البحر الإقليمي بأي من الأنشطة التالية: أ- أي تهديد بالقوة أو أي استعمال لها ضد سيادة الدولة الساحلية أو سلامتها الإقليمية أو استقلالها السياسي، أو بأية صورة أخرى انتهاكا لمبادئ القانون الدولي المجسدة في ميثاق الأمم المتحدة، ب- أي مناورة أو تدريب بأسلحة من أي نوع، ج- أي عمل يهدف إلى جمع معلومات تضر بدفاع الدولة الساحلية أو أمنها، د- أي عمل دعائي يهدف إلى المساس بدفاع الدولة الساحلية أو أمنها، هـ- إطلاق أي طائرة أو إنزالها أو تحميلها، و- إطلاق أي جهاز عسكري أو إنزاله أو تحميله، ز- تحميل أو إنزال أي سلعة أو عملة أو شخص خلافا لقوانين وأنظمة الدولة الساحلية الجمركية أو الضريبية أو المتعلقة بالهجرة أو الصحة. ح- أي عمل من أعمال التلويث المقصود والخطير يخالف هذه الاتفاقية. ط- أي من أنشطة صيد السمك. ى- القيام بأنشطة بحث أو مسح. ك- أي فعل يهدف إلى التدخل في عمل أي من شبكات المواصلات أو من المرافق أو المنشآت الأخرى للدولة الساحلية. ل- أي نشاط آخر ليست له علاقة مباشرة بالمرور".

(3) ***H. ZHANG**, Is It Safeguarding the Freedom of Navigation or Maritime Hegemony of the United States? Comments on Raul (Pete) Pedrozo's Article on Military Activities in the EEZ, 9 CHINESE J. INT'L L., 2010, P. 31.*

(4) ***M. MASAHIRO**, the Submerged Passage of a Submarine through the Territorial Sea, the Incident of a Chinese Atomic-Powered Submarine, 10 SING. Y.B. INT'L L., 2006, PP. 243: 249.*

ملاحية، والتقاط أي محادثات وإشارات صادرة من الدول الساحلية، سواء كانت تخصها أم لا، وهو سلوك يتنافى مع شروط المرور البريء[١].

وقبل سريان اتفاقية الأمم المتحدة لقانون البحار لعام ١٩٨٢، كانت اتفاقية عام ١٩٥٨ بشأن البحر الإقليمي والمنطقة المتاخمة، قد أقرّت في مادتها (٤/١٤) حق المرور للسفن في البحار الإقليمية للدول الساحلية، بشرط عدم المساس بسلمها، أو نظامها، أو أمنها، أو الانخراط في أنشطة ليس لها علاقة بالمرور، وإلا تحوَّل إلى مرور غير برئ، يحق للدول الساحلية أن تمنع السفن منه[٢]، ويدخل ضمن نطاق هذه الأنشطة التي يُمكن أن تضر بسلم الدول الساحلية وأمنها، جمع المعلومات غير المُصرَّح بجمعها.

وقبل سريان هذه الاتفاقات، كانت معظم النظم الملاحية للدول تلتزم تُجسّد العرف الدولي[٣]، الذي يحظر على السفن المارة في البحار الإقليمي، أن تقوم بأي نشاط "غير عادي"، لتتمكَّن من جمع معلومات سريّة، وهو وضع يختلف عما ورد باتفاقية ١٩٨٢، التي حظرت في مادتها (٢/١٩)، القيام بأي عمل يهدف إلى جمع معلومات قد تُضر بأمن الدولة الساحلية، ويتجسّد الفرق في أنه وفقًا للعرف، كان يُعتقد أن جمع معلومات سرية أثناء المرور البريء يتوافق مع القانون الدولي، طالما لم يتم بناءً على نشاط "غير عادي"، أو مخالفة للنمط المعتاد في الإبحار، إلا أن اتفاقية قانون البحار لعام ١٩٨٢، قد اعتبرت أن أي ممارسة لجمع المعلومات، تتعارض مع متطلبات حق المرور البريء[٤].

وتجدر الإشارة إلى أن دليل "تالين ٢" لعام ٢٠١٧، قد قرّر انطباق اتفاقية الأمم المتحدة لقانون البحار لعام ١٩٨٢، على العمليات السيبرانية، التي تتم من خلال بنية تحتية سيبرانية موجودة في البحار، وقضت القاعدة رقم (٤٥) منه، بأنه وفقًا للمادة رقم (٨٨) من الاتفاقية، لا يجوز إجراء عمليات سيبرانية في أعالي البحار إلا لأغراض سلمية[٥]، وأن الأنشطة السيبرانية لا تُستبعد من نطاق مفهوم الحريات في

---

(1) ***ODOM,*** *the True "Lies" of the Impeccable Incident: What Really Happened, Who Disregarded International Law, and Why Every Nation (Outside of China) should be Concerned, 18 MICH. ST. J. INT'L L., 2010, P. 411.*

(٢) **نصت المادة (١٤) من الاتفاقية عام ١٩٥٨، بعنوان: "حق المرور البريء"**، على أنه: ١- مع مراعاة احكام هذه المواد، فإن سفن جميع الدول الساحلية او غيرها تتمتع بحق المرور البريء في البحر الإقليمي. ٢- المرور معناه الملاحة في البحر الاقليمي، إما بقصد عبوره دون الدخول في المياه الداخلية، أو الدخول فيها أو الخروج منها إلى أعالي البحار. ٣- المرور يشمل حق الوقوف والرسو وإنما بقدر ما يكون ذلك متصلاً بالملاحة العادية أو كنتيجة محتومة لظروف قاهرة بسبب وقوع السفينة في محنة. ٤- يكون المرور بريئًا طالما أنه غير ضار بالسلام وحسن النظام أو سلامة الدولة الساحلية. وهذا المرور يجب أن يتم طبقا لهذه المواد وقواعد القانون الدولي الأخرى. ٥- لا يعتبر مرور سفن الصيد الأجنبية بريئًا إذا لم تراع القوانين والأنظمة، التي تضعها الدولة الساحلية وتعلنها لمنع الصيد في البحر الإقليمي. ٦- على الغواصات أن تسير فوق سطح الماء وأن ترفع علمها".

(3) ***Statement on United States Oceans Policy,*** *Office of Ocean and Polar Affairs, Law of the Sea Convention, 1973,* ***available at:*** *https://www.state.gov/law-of-the-sea-convention.20/4/2020.*

(4) ***K. E. EICHENSEHR****, the Cyber-Law of Nations, 103 GEO. L. J. 317, 2015, PP. 336:340.*

(٥) **ويُعرَّف مصطلح "الأغراض السلمية" في هذه القاعدة** بالإشارة إلى المادة ٣٠١ من الاتفاقية، التي تؤكد على حظر التهديد باستخدام القوة أو استخدامها. **راجع كذلك:**

Rule (45) of Tallinn Manual 2: *Cyber operations on the high seas: Cyber operations on the high seas may be conducted only for peaceful purposes, except as otherwise provided for under international law.*

أعالي البحار، والاستخدامات القانونية الأخرى للبحار، مع التقيد بعدم انتهاك هذه العمليات للقانون الدولي الساري، ومراعاة الحرية المقررة للدول الأخرى[١].

كما تطرَّق الدليل في القاعدة رقم (٤٨) منه إلى التجسس السيبراني في البحر الإقليمي، من خلال التأكيد على واجبات السفن التي تتمتع بحق المرور البريء عبر هذه المساحة البحرية لدولة ساحلية، ومنها ضرورة الامتثال في أي عمليات إلكترونية تقوم بها، للشروط المُتطلبة لهذا الحق، لاسيما الأنشطة المتعلّقة بجمع المعلومات التي قد تضر بأمن الدولة الساحلية[٢]، والتزامها بألا تمس أنشطتها الالكترونية خلال المرور، بأمن الدولة الساحلية أو نظامها.

ومن ثم، يُمكن القول، بأنه وفقًا للعرف الملاحي الدولي، وكذلك اتفاقية عام ١٩٥٨ بشأن البحر الإقليمي والمنطقة المتاخمة، واتفاقية قانون البحار لعام ١٩٨٢، نجد حكم دولي بشأن جمع معلومات بشأن الدول الساحلية من البحار وقت السلم، باعتبار أن ذلك ينفي وصف البراءة عن المرور خلال البحار الإقليمية، وينتهك أحد حقوق الدول الساحلية، التي يكون لها الحق منع مرور السفن الأجنبية في هذه المساحة البحرية، إذا اعتبرت أن هذا المرور يشكل إخلالاً بمقتضيات أمنها[٣].

الفرع الثاني

التجسس في المضايق الدولية

قرّرت محكمة العدل الدولية بمناسبة نظرها لقضية قناة "كورفو" عام ١٩٤٦، أن الدول تتمتع بحق العبور بين جزأين من أعالي البحار "المضايق"، دون إذن سابق من الدول الساحلية، شريطة أن يكون هذا المرور بريئًا، ولا يحق لتلك الدول أن تحظر هذا المرور عبر المضيق وقت السلم[٤]، وبعد مد

---

(1) ***Rule (46) of Tallinn Manual 2****: The right of visit and cyber operations A warship or other duly authorised vessel may exercise the right of visit to board a vessel without flag State consent on the high seas or within an exclusive economic zone if it has reasonable grounds for suspecting the vessel is utilizing cyber means to engage in piracy, slave trading, or unauthorised broadcasting; appears to be without nationality; or is of the nationality of the visiting vessel.*

(٢) **عدَّدت القاعدة أنشطة الكترونية تنتهك المرور البريء، وهي** (١) التهديد أو استخدام القوة بالوسائل السيبرانية ضد الدولة الساحلية، (٢) الأنشطة السيبرانية لجمع المعلومات الضارة بأمن الدولة الساحلية؛ (٣) الدعاية التي تتم بوسائل الإنترنت وتؤثر على الدفاع أو أمن الدولة الساحلية؛ (٤) الإطلاق أو الهبوط أو الصعود على متن طائرة أو غيرها من المعدات العسكرية، بما في ذلك تلك التي تشارك أو قادرة على إجراء العمليات السيبرانية، (٥) أنشطة البحث أو المسح، بما في ذلك تلك التي أجريت من خلال الوسائل السيبرانية، (٦) العمليات السيبرانية التي تستهدف التدخل في أنظمة الاتصالات أو مرافق أو منشآت أخرى للدولة الساحلية، (٨) أي نشاط إلكتروني آخر لا يتعلَّق بالمرور. **راجع نص القاعدة:**
Rule No. (48) of Tallinn Manual 2: *Cyber operations in the territorial sea: In order for a vessel to claim the right of innocent passage through a coastal State's territorial sea, any cyber operations conducted by the vessel must comply with the conditions imposed on that right.*

(٣) **أسهمت اتفاقية قانون البحار لعام ١٩٨٢**، في تحديد مفهوم الأمن القومي من خلال الإشارة إلى بعض الحالات التي يشكل فيها مرور السفن الأجنبية في البحر الإقليمي تهديدًا لأمن الدولة، ويتحوَّل من ثم إلى مرور غير بريء، يحق للدولة الساحلية منعه. **راجع: د. محمد صافي يوسف**، تدابير حماية الأمن القومي كاستثناء على تطبيق قواعد القانون الدولي العام، المرجع السابق، ص ٢١٣: ٢١٤.

(٤) **اصطدمت مدمرتان بحريتان بريطانيتان بألغام مزروعة في مضيق "كورفو"**، وعرضت "ألبانيا" النزاع على محكمة العدل الدولية، التي اعتبرت أن السفن الحربية البريطانية كانت تمر مرورًا بريئًا، حيث لم تكن في تشكيل قتالي أو تنخرط في مناورات، وتم تفريغ أسلحتها وتخزينها في الوضع الطبيعي وقت السلم، ولم يكن هناك جنود إضافيين على متنها، وليس

مساحة البحر الإقليمي من (٣) أميال، إلى (١٢) ميلاً بحريًا بموجب اتفاقية قانون البحار لعام ١٩٨٢، أُستخدم أكثر من مائة مضيق لغرض الملاحة الدولية، مع كونها متداخلة مع بحار إقليمية للدول، وحري بالذكر، أنه كانت لدى بعض الدول قناعة بأن نظام المرور البريء لا يكفي لضمان حرية الملاحة، لاسيما بالنسبة للغواصات الحربية والنووية، ولذا تفاوضت هذه الدول على تطبيق نظام "المرور العابر" "*Transit passage*" في عدد من مضايق العالم الاستراتيجية، مثل "جبل طارق"، و"باب المندب"، و"هرمز"[١].

وتُعرِف المادة رقم (٢/٣٨) من اتفاقية قانون البحار لعام ١٩٨٢، المرور العابر بأنه، ممارسة حرية الملاحة والتحليق لغرض وحيد، وهو العبور المتواصل والسريع في المضيق، وفقًا لأنماط التشغيل العادية التي تعتمدها السفن والطائرات في مرورها[٢]، ولا يتطلب المرور العابر من الغواصات الطفو وإظهار العلم، وإنما يعترف بمرورها المغمور عبر المضيق، باعتبارها الطريقة المعتادة للغواصات في الملاحة البحرية، كما يتيح للسفن الحربية والغواصات والطائرات العسكرية أن تعبر بنفس تشكيلها بما يحافظ على سريتها وأمنها[٣]، ويتيح استخدام أجهزة الرادار والسونار ومعدات سبر الأعماق، وإطلاق واستعادة الطائرات بعد استئذان الدولة الساحلية[٤]، ولا يمكن للدول الساحلية المتاخمة عرقلة نشاط المرور العابر خلال فترة السلم[٥]، ويُحظر على السفن أو الطائرات الحربية القيام بأنشطة تُمثّل تهديدًا أو استخدامًا للقوة ضد السيادة أو السلامة الإقليمية، أو الاستقلال السياسي للدول الواقعة على حدود المضيق[٦].

وبالرغم من أن قواعد المرور العابر في المضايق لا تُبيح اقتراف سلوك التجسس، وتحظر على السفن والطائرات التهديد بالقوة أو باستخدامها ضد السيادة أو السلامة الإقليمية أو الاستقلال السياسي للدولة المتاخمة للمضيق؛ وأن تمتنع كذلك عن القيام بأي أنشطة لا تتعلق بالمرور؛ إلا أنه من الناحية الواقعية لا يُمكن التحكم في منع ممارسة التجسس، الذي يبدو غير متعارض مع المرور العابر، ما دام لا يرقى إلى مستوى التهديد باستخدام القوة أو استخدامها، أو تهديد سيادة الدولة الساحلية أو سلامتها الإقليمية

هناك أي دليل على أن السفن كانت تتجسس على "ألبانيا". **راجع: محكمة العدل الدولية**، قضية (المملكة المتحدة ضد ألبانيا)، ١٩٤٩، الفقرات ٣٠: ٣٢.

(١) **وكذلك مضيق "ملقا"، و"سنغافورة"، و"سوندا"، ولومبوك"، وممر "ويندوارد" بين "كوبا" و"هيسبانيولا". راجع:**

***J. N. MOORE**, the Regime of Straits and the Third United Nations Conference on the Law of the Sea, 74 AM. J. INT'L L. 1980, PP. 77, 80: 81, 95:110 (1980)*

(٢) **المادة (٢/٣٨) من اتفاقية الأمم المتحدة لقانون البحار ١٩٨٢، ونصت على أنه:** ٢- المرور العابر هو أن تمارس وفقا لهذا الجزء حرية الملاحة والتحليق لغرض وحيد وهو العبور المتواصل السريع في المضيق بين جزء من أعلي البحار أو منطقة اقتصادية خالصة وجزء آخر من أعالي البحار أو منطقة اقتصادية خالصة. غير أن تطلب تواصل العبور وسرعته لا يمنع المرور خلال المضيق لغرض الدخول إلى دولة مشاطئة للمضيق أو مغادرتها أو العودة منها، مع مراعاة شروط الدخول إلى تلك الدولة.

(٣) **المادة رقم (٣٩/١/ج) من اتفاقية الأمم المتحدة لقانون البحار لعام ١٩٨٢.**

(٤) **المادة رقم (٤٠) من اتفاقية الأمم المتحدة لقانون البحار لعام ١٩٨٢.**

(٥) **المادة رقم (٤٤) من اتفاقية الأمم المتحدة لقانون البحار لعام ١٩٨٢.**

(٦) **المادة رقم (٣٩/١/ب) من اتفاقية الأمم المتحدة لقانون البحار لعام ١٩٨٢.**

أو استقلالها السياسي، وعلى سبيل المثال يمكن التذرع بوقوع حوادث أثناء العبور وإتيان أنشطة سرية ربما لا تتفق مع الغرض منه[1].

ومن العرض السابق يمكن القول، بأن جمع المعلومات من البحر الإقليمي للدول وقت السلم، يخالف نص المادة (١٩) من اتفاقية الأمم المتحدة لقانون البحار لعام ١٩٨٢، التي اعتبرت أن هذا السلوك يُغَيّر طبيعة المرور ويجعله غير بريء، وتكون أحد التفسيرات المطروحة، أن الاتفاقية قد حظرت صراحةً هذا السلوك، وقرَّرت عدم مشروعيته، إلا أن ما يصم هذا التفسير بالضعف، أن الاتفاقية لم تتعرَّض للحالة التي يستهدف فيها التجسس أثناء المرور، دولاً أخري بخلاف الساحلية، فالسفينة التي تمر في البحر الإقليمي لدولة ساحلية، تلتزم بالامتثال لمتطلبات النظام والأمن تجاه هذه الدولة، ولا تتحمَّل بواجب مماثل تجاه الدول الأخرى، وعند ممارسة التجسس ضد دولة ثالثة من البحر الإقليمي لدولة ساحلية، فإن ذلك لا ينتهك الامتثال لشروط المرور البريء المُستحق للدولة الساحلية، ولا ينتهك نصوص اتفاقية الأمم المتحدة لقانون البحار لعام ١٩٨٢، ومن ثم، فقد حظرت الاتفاقية سلوك جمع المعلومات كشرط أو مُتطلَّب للمرور البريء، وليس تقريرًا لعدم مشروعيته.

أي أن أحكام المرور البريء الواردة في اتفاقيتي عام ١٩٥٨، وعام ١٩٨٢، تتعلَّق بشروط التمتع بهذا الحق، ولا علاقة لها بتنظيم مشروعية الأنشطة التي تتنافي معه، كجمع المعلومات، وعلى سبيل المثال، يُتطلب من الغواصات أن تطفو على السطح وتُظهر علمها للتمتع بحق المرور البريء، وعند عدم الاستجابة لذلك، ومرور إحدى الغواصات وهي مغمورة، لانخراطها في جمع معلومات عن الدولة الساحلية، فإن عدم مشروعية سلوكها تتجسّد في مخالفة شروط المرور البريء، وبالتالي تُمنع من التمتع بهذا الحق، وليس للأمر أي علاقة بمدي مشروعية سلوك جمع المعلومات.

الفرع الثالث

خيارات الدول الساحلية عند الاشتباه في حالات تجسس بحري

قرَّرت المادة (٩٥) من اتفاقية قانون البحار لعام ١٩٨٢، حصانة كاملة للسفن الحربية في أعالي البحار من ولاية أي دولة ما عدا دولة العلم، **وبموجب المادة (٢/٥٨) من الاتفاقية،** تمتد هذه الحصانة لتشمل المساحات الخاضعة لولاية الدول الساحلية، بما فيها البحر الإقليمي، وتكون السيادة على السفن الحكومية، ومنها الحربية والغواصات الطافية، لدولة العلم الذي ترفعه السفينة، وليس للدول الساحلية ولاية عليها، سواء قضائية أم إجرائية مثل القبض، أو الاحتجاز، أو فرض تدابير تنفيذ جبرية[2]، **كما قضت المادة (٣٢) من الاتفاقية بشأن** البحر الإقليمي والمنطقة المتاخمة، بأنه: "ليس في هذه الاتفاقية ما يؤثر على حصانات السفن الحربية".

---

(١) **وفقًا للمادة رقم (١/٣٩/ج) من اتفاقية الأمم المتحدة لقانون البحار ١٩٨٢،** والتي قضت بأن الدول تمتنع عن أية أنشطة غير تلك الملازمة للأشكال المعتادة لعبورها المتواصل السريع، إلا إذا أصبح ذلك ضروريا بسبب قوة قاهرة أو حالة شدة.

(٢) **نصت المادة رقم (٢/٥٨) من اتفاقية ١٩٨٢، على أنه:** "تنطبق المواد من (٨٨) إلى (١١٥) وغيرها من قواعد القانون الدولي المتصلة بالأمر، على المنطقة الاقتصادية الخالصة بالقدر الذي لا تتنافى به مع هذا الجزء"؛ فإن المادة رقم (٩٥) من الاتفاقية تنطبق كذلك في المنطقة الاقتصادية الخالصة وبما يُقدر بـ (٢٠٠) ميل بحري من الدول الساحلية.

وعندما يتعلق الأمر باشتباه الدول الساحلية في حالات تجسس، تقوم بها السفن أو الغواصات الأجنبية من البحر الإقليمي للدولة، فإنه وفقًا لاتفاقية قانون البحار لعام ١٩٨٢، تكون قدرتها على الرد محدودة، ولا يتاح لها سوى خيارات المطالبة بمغادرة البحر الإقليمي فورًا، أو استخدام القوة.

أولاً: طلب المغادرة فورًا:

أوردت المادة (٢٣) من اتفاقية البحر الإقليمي لعام ١٩٥٨ أنه: إذا لم تمتثل أي سفينة حربية لأنظمة الدولة الساحلية، المُتعلقة بالمرور عبر البحر الإقليمي وتجاهلت طلب الامتثال، فإن الدولة الساحلية قد تطلب من السفينة أن تغادر البحر الإقليمي. وأوردت المادة (٣٠) من اتفاقية قانون البحار لعام ١٩٨٢، نفس الحكم بالنص على أنه، إذا لم تمتثل أي سفينة حربية لقوانين ولوائح الدولة الساحلية فيما يتعلق بالمرور عبر البحر الإقليمي، وتجاهلت أي طلب بذلك، فإنه يجوز للدولة الساحلية أن تطلب منها مغادرة البحر الإقليمي فورًا.

وعلي سبيل المثال، في عام ١٩٦٨، صرَّحت الولايات المتحدة الأمريكية، أنه حتى لو كانت سفينة "*USS Pueblo*" قد تواجدت داخل البحر الإقليمي لكوريا الشمالية حين تم الاستيلاء عليها، فإن مصادرتها غير مقبولة، وتُعد انتهاكًا للحصانة السيادية الأمريكية، وفي حالة عدم وجود تهديد مباشر وفوري بهجوم مسلح، فإن أقصى إجراء يمكن أن تتخذه الدولة الساحلية، هو مرافقة السفينة الحربية حتى تخرج من مياهها الإقليمية"[١].

وقد اعتمدت مدونة المُستجدات المفاجئة في البحر "*Code for Unplanned Encounters at Sea*" لعام ٢٠٠٣، نفس النهج السابق في مادتها (٦/٢)، من حيث أن "الجزاء الوحيد الذي يمكن أن تفرضه دولة ساحلية على سفينة حربية أو سفينة حكومية، هي طلب مغادرة المياه الداخلية أو البحر الإقليمي[٢].

وبالتالي فإنه وفقًا للقواعد الدولية المتعلقة بتنظيم البحار، عند تورط سفينة حربية في التجسس على دولة ساحلية، يكون الخيار القانوني الأول للدولة، أن طلب مغادرة السفينة فورًا، دون القبض عليها أو احتجازها، أو اتخاذ أي إجراءات من شانها المساس بحصانة السفينة السيادية[٣]، وهو ما استندت إليه الولايات المتحدة الأمريكية في حادثة السفينة "*Pueblo*".

ثانيًا: استخدام القوة:

وفيما يتعلق باستخدام دولة ساحلية القوة ضد سفن أو غواصات أجنبية، لعدم استيفائها لشروط المرور البريء، نصَّت المادة رقم (١/٢٥) من اتفاقية قانون البحار لعام ١٩٨٢، على أنه: "للدولة الساحلية أن تتخذ في بحرها الإقليمي الخطوات اللازمة لمنع أي مرور لا يكون بريئًا". بيد أن صياغة

---

(1) ***C. PINTO**, Maritime Security and the 1982 United Nations Convention on the Law of the Sea, in UN INST. for Disarmament Research, Maritime Security: the Building of Confidence, Jozef Goldblat ed., 1992, PP. 9: 18.*

(2) ***Western Pacific Naval Symposium,** Code for Unalerted Encounters at Sea (CUES), para. 2.6, reprinted in 4(4) Australian J. of Maritime and Ocean Affairs, 2003, PP. 126: 127.*

(3) ***J. KRASKA**, Military Operations, in the Oxford Handbook of the Law of the Sea, Donald R. Rothwell et al. eds., 2015, PP. 866, 871:872*

المادة وردت غامضة فيما يخص تفسير ماهية "الخطوات الضرورية" المُتطلبة لإجبار السفن على الامتثال، أو ما هو المستوى المناسب لاستخدام القوة أو حدودها أو توقيت اللجوء إليها[١].

وقد استخدمت بعض الدول القوة، أو أبدت استعدادها لاستخدامها، في مهاجمة غواصات مجهولة دخلت إلى مياها الإقليمية دون إذن ـ حتى ولو كانت حربية ـ باعتبار أن ذلك مُبَرَر بموجب حق الدفاع ضد أي متسلل ينتهك إقليم الدولة[٢]، وأيَّد جانب فقهي هذا الاتجاه، باعتبار أنه يحق للدول الساحلية أن تستولي ـ يُفترض بالقوة ـ على السفن العسكرية التي تمارس أنشطة التجسس قُبالة شواطئها[٣]، على سند من أن دخول قطع بحرية حربية إلى البحر الإقليمي لدولة ساحلية، يمكن تقييمه بشكل أولي كهجوم مسلح، مما يعطي الدولة حق اتخاذ تدابير مسلحة مضادة، بينما على جانب آخر، تقرر بعض الدول أنه لا يحق للدولة الساحلية استخدام القوة، ضد غواصة في بحرها الإقليمي لمجرد وجودها، ويحتاج الأمر إلي توافر مؤشرات أو أدلة على عدوانية السفينة[٤].

وفيما يخص بعض الاتجاهات التشريعية الوطنية للتعامل مع الاشتباه في التجسس البحري، نجد بعض الدول مثل "السويد"، قد قامت في عام ١٩٨٢، بتعديل تشريعاتها الخاصة بالمرور البريء للسفن الحربية والغواصات الحكومية الأجنبية[٥]، وتم اشتراط عبورها وفقًا لشروط اتفاقية قانون البحار لعام ١٩٨٢[٦]، وإذا لم تمتثل يتم إعلامها بالتنظيمات ذات الصلة، وإبعادها عن الإقليم"، ويجوز عند الضرورة استخدام القوة المسلحة[٧]، وبالنسبة للغواصات المتسللة، يتم اتخاذ إجراءات طردها، وعند الضرورة تُستخدم القوة المسلحة دون سابق إنذار، إذا توافرت مؤشرات بشأن خطورة تواجدها[٨]، أو ما يشير إلى نية عدائية؛ كقصد توجيه أعمال عدائية ضد أهداف سويدية داخل أو خارج الإقليم السويدي؛ أو ضد سفن أو طائرات سويدية في أعالي البحار[٩].

وبالنسبة للقانون الأمريكي، فقد تضمن أحكامًا تتعلّق باستخدام القوة، ردًا على الأعمال العدائية، أو عند إظهار نية العداء من جانب قطع بحرية لدول أخرى، كالقيام بمناورات تمنع أو تعرقل السفن أو الطائرات الحربية الأمريكية، أو الاقتراب من قوات أمريكية في وضع هجوم، كأن تتباطأ الطائرة أو

---

(١) **اعتمدت بعض السوابق القضائية، معيار استخدام القوة "الضرورية والمعقولة"**، في حالات التعامل خارج البحر الإقليمي، للقيام بالزيارات، والبحث والتفتيش، وسحب السفن غير الممتثلة إلى أقرب ميناء، ومن المتوقع أن تلجأ سلطات الدول الساحلية إلى كل وسيلة دون استخدام القوة، قبل اتخاذ قرار باتخاذها، كالتضييق على تلك السفن بالوسائل الملاحية.
راجع:
R. CRUSADER, (U.K. v. Den.), *Comm'n of Enquiry, Mar. 23, 1962, 35 I.L.R. 485 (E. Lauterpacht ed. 1967).*

(2) ***Laws and Regulations on the Regime of the Territorial Sea,*** *United Nations LEGIS. SERIES, December 1956, U.N. Leg. Ser. ST/LEG/SER/B/6 81, 241.*

(3) ***L. OPPENHEIM****, Oppenheim's International Law, P. R., P.750:751;* ***H. A. SMITH,*** *the Law and Custom of the Sea 47–48, (3d ed. 1959, PP. 164:165.*

(4) ***Y. DINSTEIN****, War, Aggression and Self-Defense, P. R., P. 213.*

(٥) في عام ١٩٦٦عدَّلت السويد تشريعاتها، ثم أعادت تعديلها في عام ١٩٨٢ تحت مسمى "*IKFN-Ordinance*".

(6) ***IKFN-Ordinance, § 3, 7, 8.***

(7) ***IKFN-Ordinance, § 18.***

(8) ***IKFN-Ordinance, § 15/2, 17.***

(9) ***IKFN-Ordinance, § 13, 14.***

السفينة الأجنبية بعد سرعتها الثابتة لدى اقترابها من القوات، أو استخدام الرادارات لتحديد مواقع القوات الأمريكية[١].

أما "اليابان" فقد اعتمدت في عام ٢٠٠٤، نهجًا للتعامل مع الغواصات الأجنبية في مياهها الإقليمية، ويستند إلى المادة رقم (٨٢) من قانون الدفاع الذاتي رقم (١٦٥) لعام ١٩٥٤[٢]، الذي قضي بأنه يجوز للقائد العام بموافقة رئيس الوزراء، أن يأمر بفرض الإجراءات اللازمة في البحر لحماية الأرواح أو الممتلكات، أو الحفاظ على السلام والنظام العام. ومن ذلك، مطالبة الغواصات المغمورة داخل المياه الإقليمية بالطفو على السطح أو مغادرة المياه الإقليمية؛ وتتولي قيادة عمليات الأمن البحري مراقبتها وتحديد جنسيتها، وما إلى ذلك، واتخاذ أي إجراء خاص تقتضيه الضرورة؛ وبعد مغادرتها تستمر عمليات الأمن البحري للتأكد من عدم عودتها مرة أخرى للبحر الإقليمي؛ وتُتخذ التدابير اللازمة بالتواصل مع الدول المعنية، ويتم توضيح وجهة نظر الدولة من خلال نشر تفسير مناسب وفي الوقت المناسب للمواطنين ودون تأخير[٣].

ويُثير خيار استخدام القوة ضد القطع البحرية المُشتبه بضلوعها في التجسس، إشكالية مدى إمكان اعتبار هذا سلوك التجسس مكافئًا لاستخدام القوة المسلحة، وبالتالي منح الدولة الساحلية حق الدفاع ضده؟

وباستعراض حكم محكمة العدل الدولية في قضية "نيكاراجوا" عام ١٩٨٦، دفعت الأخيرة بأن رحلات المراقبة الجوية والبحرية الأمريكية على أراضيها خلال عام ١٩٨٤، تتعارض مع سيادتها، ورد الدفاع الأمريكي بأن البعثات الاستطلاعية الأمريكية تمت وفقًا للحق في الدفاع الفردي والجماعي، ضد العدوان المسلح لدولة "نيكاراجوا" على جيرانها في أمريكا الوسطى، ووفقًا لإستراتيجية دفاع مشترك مع دول من أمريكا الوسطى. وقد قررت المحكمة أنه: "من غير المحتمل أن تنظر المحكمة في تورط غواصة وقت السلم في أعمال تجسس باعتباره هجومًا مسلحًا، أو أن تُجيز المحكمة استخدام القوة بموجب حق الدفاع عن النفس في هذه الحالات بوجه عام، وإنما يجب بحث كل حالة على حدة"[٤].

ورفضت المحكمة ادعاء "الولايات المتحدة الأمريكية" و"السلفادور" باستحقاق حالة الدفاع الشرعي ضد هجوم مسلح من "نيكاراجوا"، وقررت أن المراقبة الجوية الأمريكية هي انتهاك للقانون الدولي، بينما قررت أن المناورات البحرية الأمريكية التي جرت في الفترة من عام ١٩٨٢ وحتى عام ١٩٨٥ قُبالة ساحل "نيكاراجوا"، لا تُشكّل تهديدًا أو استخدامًا للقوة ضد "نيكاراجوا"، باعتبار أنه وإن مثَّل تدريب وتسليح وتجهيز المتمردين انتهاكًا للقانون الدولي، إلا أن سيادة "نيكاراجوا" لم تتعرض للخطر جراء تلك الأنشطة الأمريكية شبه العسكرية[٥].

وذلك على الرغم من أن المادة رقم (٣٠١) من اتفاقية الأمم المتحدة لقانون البحار لعام ١٩٨٢، قد فرضت التزامًا قانونيًا منفصلاً يعزز ويدعم الامتناع عن التهديد باستعمال القوة أو استخدامها في الأنشطة

---

(1) ***P. DOMBROWSKI, C. DEMCHAK,*** *Cyber War, Cybered Conflict, and the Maritime Domain, Naval War College Review, No. 67, Vol. 2, 2014, P. 75.*

(2) ***Cabinet Secretariat****, Ryousui-nai Senbotsu-Sensuikan e no Taisho nit suite (On Coping with Submarines Navigating within Territorial Waters) 19 January 2005.*

(3) ***Japan Protests New Incursion,*** *INVESTOR'S BUS. DAILY, Dec. 9, 2004, at A2.*

(٤) **حكم محكمة العدل الدولية في قضية (*Nicar. v. U.S.*)، ٢٧ يونيو ١٩٨٦، الفقرات: ١١، ١٢، ١٩٠: ١٩٢.**

(٥) **حكم محكمة العدل الدولية في قضية (*Nicar. v. U.S.*)، ٢٧ يونيو ١٩٨٦، الفقرات: ٢٩٢: ٢٩٣.**

البحرية، حيث نصت على أنه: "تمتنع الدول الأطراف، في ممارستها لحقوقها وأدائها لواجباتها بموجب هذه الاتفاقية، عن أي تهديد باستعمال القوة أو استعمالها ضد السلامة الإقليمية أو الاستقلال السياسي لأية دولة، أو بأي صورة أخرى تتنافى ومبادئ القانون الدولي المتضمنة في ميثاق الأمم المتحدة".

وقررت المحكمة أن التدخل بمستوى متدن، كإرسال عصابات مسلحة أو مجموعات غير نظامية مسلحة أو مرتزقة" إلى دولة أخرى؛ يُشكل هجومًا مسلحًا فقط إذا بلغ حجم وآثار هذا التدخل أو كانت خطورته تعادل غزو نظامي[١]، ونلاحظ أن التجسس البحري في حد ذاته لا يكافئ الهجوم المسلح، ووفقًا للحكم، لم يكن هناك ما يبرر لجوء الدولة الساحلية للدفاع عن النفس، ضد هجوم متدني الخطورة من حيث حجمه وآثاره، من قبل مجموعات غير نظامية أو متمردين[٢]، ولا يمكن قبول استخدام القوة ضد تدخل الغواصات خلال زمن السلم ردًا قانونيًا مناسبًا من قبل الدولة الساحلية، حيث إن الأمر لا يرقي إلى درجة الهجوم المسلح وفقًا لحجمه أو آثاره.

وبالنظر إلى حكم المادة (٣١) من اتفاقية قانون البحار لعام ١٩٨٢، بتحمل دولة العلم المسئولية عن أي خسارة أو ضرر يلحق بالدولة الساحلية، نتيجة لعدم امتثال سفنها الحربية مع قوانين وأنظمة الدولة الساحلية الخاصة بالمرور البريء[٣]، يمكن القول بمساءلة الدول الأجنبية التي تُشغّل قطع بحرية عن قيامه بالتجسس، إلا أنه بالرجوع إلى الأعمال التحضيرية للاتفاقية، نجد أن هذا الحكم قد تمت صياغته لينظم مسئولية السفن الحكومية الأجنبية والحربية، عن الأضرار التي تلحق بالبيئة البحرية[٤]، ومن ثم فإن فلسفة الحكم تجعل من غير المحتمل الاستناد إليه لتقرير مسئولية دولة العلم عن التجسس البحري[٥].

ووفقًا للمادتين (٢٨٢)، (٢٨٦) من اتفاقية قانون البحار، تخضع منازعات الأطراف المتعلقة بالاتفاقية للتحكيم الملزم أو الفصل القضائي[٦]، إلا أنه في حالة نشأة نزاع يتعلّق بتورط سفينة أو غواصة حربية في جمع معلومات استخبارية، فإن لدولة العلم التي تتبعها السفينة أو الغواصة، أن تُعلن عدم قبولها لحل النزاع بموجب نظام تسوية المنازعات الإجباري للاتفاقية، إعمالاً لنص المادة رقم (١/٢٩٨/ب) منها، والتي تُجيز لأي دولة أن تعلن عن عدم قبولها لحل منازعاتها بموجب هذا النظام، في واحد من ثلاث فئات، وهي: المنازعات المتعلقة بالأنشطة العسكرية[٧]؛ منازعات أنشطة إنفاذ القانون فيما يتعلق

---

(١) **حكم محكمة العدل الدولية في قضية (*Nicar. v. U.S.*)، ٢٧ يونيو ١٩٨٦، الفقرات (١٩٥، ٢٤٧، ٢٤٩)**

(٢) **الفقرة رقم (١٩٥) من حكم محكمة العدل الدولية لعام ١٩٨٦.**

(3) ***G.A. Res. 56/83, annex,*** *Responsibility of States for Internationally Wrongful Acts, at 2 (Jan. 28, 2002).*

(4) ***United Nations Convention on the Law of the Sea 1982:*** *a Commentary 263 (Satya N. Nandan & Shabtai Rosenne eds., 1993).*

(5) ***C. L. SRIRAM****, Revolutions in Accountability: New Approaches to Past Abuses, 19 AM. U. INT'L L. REV., 2003, PP. 301.*

(٦) **نصت المادة رقم (٢٨٦) من الاتفاقية على أنه:** تُطبق الإجراءات المنصوص عليها في هذا الفرع رهنا بمراعاة الفرع (٣) يحال أي نزاع يتعلق بتفسير هذه الاتفاقية أو تطبيقها عند عدم التوصل إلى تسوية وفقا للفرع (١)، بناءً على طلب أي طرف في النزاع، إلى المحكمة ذات الاختصاص بموجب هذا الفرع". **كما نصت المادة رقم (٢٨٢) منها على أنه:** "إذا كانت الدول الأطراف التي هي أطراف في نزاع يتعلق بتفسير هذه الاتفاقية أو تطبيقها قد وافقت، عن طريق اتفاق عام أو إقليمي أو ثنائي أو بأية طريقة أخرى، على أن يخضع هذا النزاع بناء على طلب أي طرف في النزاع، لإجراء يؤدي إلى قرار ملزم، ينطبق ذلك الإجراء بدلا من الإجراءات المنصوص عليها في هذا الجزء، ما لم تتفق الأطراف على غير ذلك".

(٧) **نصت المادة (١/٢٩٨/ب) من الاتفاقية على أنه**: **١-** لأي دولة عند توقيعها أو تصديقها على هذه الاتفاقية أو انضمامها إليها، أو في أي وقت بعد ذلك، ودون الإخلال بالالتزامات الناشئة بمقتضى الفرع (١)، أن تعلم كتابيًا أنها لا تقبل واحدًا أو أكثر من الإجراءات المنصوص عليها في الفرع (٢) فيما يتعلق بواحدة أو أكثر من فئات المنازعات التالية: .. **ب-**

بمصـايد الأسـماك والبحـوث العلميـة البحريـة[1]، والنزاعـات التـي تُعـرض علـى مجلـس الأمـن ويتـولي معالجتها[2].

وعلي سبيل المثال، تُصنّف الولايات المتحدة الأمريكية نشاط التجسس ضمن الأنشطة العسكرية، وبالتالي يمكنها استبعاد الحوادث ذات الصلة من آلية تسوية منازعات الاتفاقية[3]، وقد بدا ذلك جليًا من خلال جلسات الاستماع التي عقدها الكونجرس الأمريكي عام ٢٠٠٤، بشأن انضمام الولايات المتحدة إلى اتفاقية قانون البحار لعام ١٩٨٢، حيث قرّر المستشار القانوني لوزارة الخارجية الأمريكية، أن الاتفاقية لا تحظر أنشطة الاستخبارات ولم تُنظمها، وأن المنازعات المتعلقة بالأنشطة العسكرية، بما في ذلك أنشطة الاستخبارات لن تخضع لآلية تسوية المنازعات بموجب الاتفاقية، باعتبارها مسألة قانونية وسياسة أمريكية، ولذا لن يؤثر انضمام الولايات المتحدة إلى الاتفاقية على سلوك أنشطة الاستخبارات بأي شكل من الأشكال[4].

بينما اعترض على هذا التفسير عضوي الكونجرس "دافيد فيتر"، و"جيم ديمينت"، المعارضين لانضمام الولايات المتحدة إلى الاتفاقية، وأوضحا إعفاء خضوع الأنشطة العسكرية من الخضوع لآلية تسوية المنازعات، لا يشمل أنشطة الاستخبارات، لأن موازنة الولايات المتحدة نفسها، تعتبر أن الأنشطة العسكرية موضوع منفصل ومستقل عن أنشطة التجسس، حيث ترد الأولي في الباب رقم (١٠) من الموازنة، بينما ترد أنشطة الاستخبارات في الباب رقم (٥٠)، وهذه الموازنة يُقرها الكونجرس، ولن تتمكن الدولة من إثبات أن الاستخبارات البحرية ضمن الأنشطة العسكرية، ولن يكون هناك مجال لتطبيق نص المادة (٢٩٨) من الاتفاقية على التجسس[5].

ومن مجمل العرض السابق، يمكن أن نورد التحليل التالي:

(١) تتعلَّق اتفاقية قانون البحار لعام ١٩٨٢ بتنظيم البيئة البحرية، وقد وردت أحكامها الخاصة بحظر نشاط جمع المعلومات، في إطار استيفاء شروط التمتع بحق المرور البريء، وليس لعدم مشروعية هذا النشاط، أو لأنه ينتهك قاعدة دولية، فالاتفاقية لم تتطرَّق لتنظيمه أو حسم مدي مشروعيته، وإنما اعتبرت أن القطع البحرية التي تمارسه، لن تتمتع بحق المرور البريء في المساحات البحرية ذات الصلة، وبالتالي، لا يمكن القول بأن هناك قاعدة صريحة في القانون الدولي تحظر التجسس في وقت السلم.

(٢) لا يُمكن فهم حكم المادة (١/٨٧) من اتفاقية عام ١٩٨٢، باعتبار أن سلوك التجسس هو أحد عناصر الحق في حرية الملاحة والتحليق، لتناقض هذا الفهم مع نص المادة، ومع فلسفة أحكام الاتفاقية، والتي تشترط إيلاء المراعاة الواجبة لمصالح الدول الأخرى، ولا شك في أن سلوك التجسس لا يراعي

المنازعات المتعلقة بالأنشطة العسكرية، بما فيها الأنشطة العسكرية للسفن والطائرات الحكومية القائمة بخدمة غير تجارية، ...."

(١) **المادة (٢،٣/٢٩٧) من اتفاقية الأمم المتحدة لقانون البحار لعام ١٩٨٢.**

(٢) **المادة (١/٢٩٨، ج) من اتفاقية الأمم المتحدة لقانون البحار لعام ١٩٨٢.**

(3) ***S. REP. NO. 110-9, 2007, PP. 32:34, 36.***

(4) ***statement of William H. Taft IV, Legal Advisor, Department of State,*** *The United Nations Convention on the Law of the Sea, (Treaty Doc. 103-39): Hearing Before the Sen. Comm. on Foreign Relations, 110th Cong. 51, 52 (2007).*

(5) ***M. N. SCHMITT****, Below the Threshold, Cyber Operations, P. R., PP. 698, 701:707.*

مصالح الدول الأخرى، بل إن الاتفاقية تُقرّر عدم استيفاء القطع البحرية لشروط المرور البريء إذا قامت به، في المساحات البحرية للدول الساحلية، ضمانًا لأمن هذه الدول وسلمها، وليس من المنطقي أن تحظره الاتفاقية في بعض المساحات، وتبيحه في مساحات أخري، لأنه في الحالتين يُمثّل تهديدًا لدولة.

(٣) يقيَّد نص المادة رقم (٣٠١) من اتفاقية قانون البحار لعام ١٩٨٢، من رد فعل الدولة الساحلية، عند مخالفة السفن الأجنبية لشروط المرور البريء، وذلك في حالة عدم استخدام هذه السفن للقوة أو التهديد بها، حيث لا يمكن اعتبار مجرد تواجد غواصة مغمورة، أو سفينة مجهولة مُكافئًا للهجوم المسلح، وبالتالي لا يُمكن استخدام حق الدفاع ضد هذه الحالات، إلا إذا وُجدت مؤشرات على كون هذه القطع البحرية تُشكّل تهديدًا فعليًا للدولة الساحلية، أما مجرد وجودها ـ حتى مع الاشتباه في قيامها بالتجسس ـ ليس مبررًا كافيًا لتدمير الغواصة المتطفلة أو توجيه القوة المسلحة إليها.

وتؤيد الممارسات الدولية بشأن رد فعل الدول، على تحليق طائرات في مجالها الجوي دون تصريح، التحليل السابق، ومن ذلك، عندما أسقطت القوات السوفيتية، طائرة تابعة لشركة كورية، في الأول من سبتمبر لعام ١٩٨٣، حيث كانت تُحلِّق فوق جزيرة "ساخالين" في المجال الجوي للاتحاد السوفيتي السابق دون تصريح[١]؛ برر "الكرملين" ذلك، بأنه إجراء ضروري لحماية الدولة من التجسس[٢]، إلا أن الواقعة تم استنكارها من العديد من الدول[٣]، كما اعتمد مجلس منظمة الطيران المدني قرارًا، أدان فيه الرد السوفيتى[٤]، ولاحقًا، استخدم الاتحاد السوفيتي السابق، حق "الفيتو" ضد صدور قرار بإدانة الواقعة في مجلس الأمن[٥].

وبعد إسقاط الاتحاد السوفيتي السابق للطائرة (*U-2*) عام ١٩٦٠، أوضح في مجلس الأمن أن التحليق الأمريكي مثَّل انتهاكًا لسيادته، واقترح التصويت على مشروع القرار (*S / 4321*)، بإدانة تحليق طائرات المراقبة الأمريكية في أجواء الدول الأخرى واعتبارها أعمالاً عدوانية"[٦]؛ إلا أن معظم ردود أفعال الدول لم تتفق مع وجهة نظر السوفييت، فاعترض الممثل الأمريكي على وصف تلك المهام بالعدوانية، وقرّر أن المراقبة ضمانة أساسية لسلام دولته ضد أي هجوم مُحتمل. وقرّرت "فرنسا" أن التواجد الأمريكي في المجال الجوي السوفيتي كان "مؤسفا"، ويُعد انتهاكًا لحدوده، وتدخلاً ضمنيًا في

---

(1) ***Soviet Attack on Korean Civilian Airliner:*** *Statement by the Principal Deputy Press Secretary to the President (Sept. 16, 1983), in WKLY. PRESIDENTIAL COMP. DOC. (Off. Fed. Reg.), Sept. 19, 1983, at 1225, 1266.*

(2) ***Aviation Council Faults Soviet,*** *N.Y. TIMES, March 7, 1984, at A4.*

(٣) **مثل الولايات المتحدة، جمهورية كوريا، اليابان، الصين، أستراليا، كندا، المملكة المتحدة، نيوزيلندا، زائير، ليبيريا، هولندا، فرنسا، السويد، بلجيكا، إيطاليا، جمهورية ألمانيا الاتحادية، سنغافورة، فيجي، كولومبيا، الإكوادور، وباراغواي. راجع:**

Nations Halt Moscow Air Service to Protest Downing*, AVIATION WK. SPACE TECH., Sept. 19, 1983, at 26.*

(4) ***Attachment B: Resolution Adopted by the Council on 6 March 1984****, International Civil Aviation Organization: Action with Regard to the Downing of the Korean Air Lines Aircraft, reprinted in 23 AM. SOC'Y INT'L L. 864 (1984).*

(5) ***S.C. Res. Drft. S/15966/Rev.1,*** *Sept. 12, 1983, 22 I.L.M. 1148 (1983).*

(6) ***Cable Dated 18 May 1960*** *from the Minister of Foreign Affairs of the Union of Soviet Socialist Republics Addressed to the President of the Security Council, Rep. of the S.C. on Its Fifteenth Session (July 16, 1959–July 15, 1960), at 12, U.N. Doc. A/4494 (1960).*

شئونه، إلا أن المراقبة سلوك مقبول كممارسة بين الدول ولا تُمثل عدوانًا[١]، وقرَّر ممثل المملكة المتحدة، أن هناك مبالغة في وصف آثار تحليق الطائرة، بأنها عدوان"[٢]، ورفضت "إكوادور" و"الأرجنتين" تكييف الواقعة بأنها عدوان، كما وصفتها "الصين" بأنها حالة بسيطة، وليست ظاهرة جديدة أو نادرة بين الدول، وفي النهاية، رُفض مشروع القرار السوفيتي بنسبة تصويت (٧) إلى (٢) هما "الاتحاد السوفيتي السابق"، "وبولندا"، وامتنعت "تونس" و"سِيلَان" عن التصويت[٣].

(٤) لا يمكن الاستناد إلى حكم المادة رقم (٣١) من اتفاقية قانون البحار ١٩٨٢، الخاصة بتحمل دولة العلم المسئولية عن مخالفة قوانين المرور البريء؛ وذلك لتقرير مسئولية دولة العلم عن التجسس البحري، حيث يتعلَّق حكم المادة بالمسئولية عن الأضرار البيئية البحرية، أما ما يخص التجسس في المساحات البحرية المختلفة، ووفقًا للمادتين (٢٨٢)، (٢٨٦) من اتفاقية ١٩٨٢، فتستطيع الدول أن تتحلّل من الخضوع الإلزامي لنظام تسوية المنازعات الإجباري للاتفاقية، إذا أعلنت أنها تُصنّف التجسس ضمن الأنشطة العسكرية.

وفيما يتعلّق بممارسة التجسس من خلال الفضاء السيبراني، ومدي مشروعيته وانطباق قواعد القانون الساري عليه، أو ضرورة استحداث قواعد أخري بشأنه، فإننا نعالجه من خلال الفصل التالي.

الفصل الثالث

الوضع القانوني للتجسس السيبراني

ومسئولية الدول عن العمليات السيبرانية

تمهيد وتقسيم:

تطورت وسائل التجسس وواكبت تحوّل الدول إلى الاعتماد على شبكة الإنترنت، وتحوَّلت إلى الشكل الالكتروني، وغالبًا ما يكون هذا النوع من التجسس خيارًا جاذبًا للدول، لأسباب عدة؛ **منها القانوني**، حيث لا توجد صكوك دولية تُنظّمه، أو تُقرّر عدم مشروعيته، **ومنها الواقعي**، حيث تنخفض المخاطر المرتبطة بممارسته إلى أقصي درجة، مقارنة بالفوائد الجَمَّة المُتحصلة منه، بحساب أن الدول كانت تتعرض لمخاطر كشف الجواسيس، وربما القبض عليهم ومحاكمتهم وإعدامهم، فصار التجسس يتم بأمان من خارج حدود الدولة المستهدفة، مع صعوبة الكشف عن هوية الجاسوس أو التعرف على مكان تواجده[٤]؛ **ومنها الاقتصادي**، حيث تنخفض تكلفة وسائل التجسس السيبراني بالنسبة لنظيرتها التقليدية[٥].

وفي كثير من الأحيان، تمارس الدول التجسس السيبراني بواسطة كيانات خاصة، أو منظمات إجرامية مُتخصّصة في هذا المجال، حتى إن هذه المنظمات صارت الأكثر ربحية، بين أشكال الإجرام

---

(1) ***Cable Dated 18 May 1960****, P. R., P. 13.*
(2) ***Cable Dated 18 May 1960****,, P. R., P. 14.*
(3) ***Cable Dated 18 May 1960*** *from the Minister of Foreign Affairs of the Union of Soviet Socialist Republics Addressed to the President of the Security Council, P. R., PP. 15: 16.*
(4) ***A. MELNITZKY****, Defending America against Chinese Cyber Espionage, through the Use of Active Defenses, 20 CARDOZO J. INT'L & COMP. L., 2012, PP. 537: 570.*
(٥) **حيث لا يتعدى الأمر تجهيز بعض البرامج الالكترونية**، والحاسبات التي تُشغلها، وغيرها من الآليات المشابهة، ثم يُمكن جمع كم هائل من المعلومات السرية بسرعة فائقة. **راجع:**
M. SMEETS*, How Much Does a Cyber Weapon Cost? Nobody Knows, DEF. ONE (Nov. 21, 2016),* ***available at:*** *https://perma.cc/DNV5-7ZLX. 17/2/2020.*

المنظم في العالم، وربما يرجع تفضيل الدول لممارسة التجسس السيبراني من خلال تلك الكيانات، في جزء كبير منه، إلى تجنب تقرير مسئوليتها الدولية، أو وقوعها في حرج على مستوى الدولي، في حالة الكشف عن اقترافها لهذا السلوك، حيث تضطلع به تلك الكيانات، من خلال حاسبات آلية داخل أقاليم عدة دول، ويكون من الصعب تتبع مصدرها الأصلي أو تحديده، فإذا ما تم تحديده، فإن رد الفعل عليه يواجه إشكاليات قانونية وعملية، لاسيما ما يتعلَّق بدور كل دولة استخدمت حاسبات على أقاليمها لإتمام السلوك[1].

وقد عرضنا لإشكالية عدم تطرق القواعد الدولية لمعالجة التجسس في وقت السلم، وهو نفس الحال بالنسبة للتجسس السيبراني، من حيث عدم وجود أي صك دولي ساري يُنظمه، أو يُعرّفه أو يُبيّن ماهيته، أو يصف المصطلحات ذات الصلة به، علاوة على أن غالبية الاتفاقات التي تتناول تنظيم التعامل بواسطة الفضاء السيبراني ـ حتى الآن ـ تُركّز على حماية مصالح الأشخاص في التعاملات السيبرانية، ولا تعالج التجسس، ومن أبرزها، اتفاقية مجلس أوربا "بودابست" بشأن الجرائم المرتكبة بطريق الإنترنت وشبكات الحاسوب الأخرى لعام ٢٠٠١، وكذلك اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية لعام ٢٠١٤.

ولعل من أبرز الصعوبات التي تواجه وجود مثل ذلك التنظيم، ما أوضحه بعض الفقه من غموض الوضع القانوني لبيئة الفضاء السيبراني، لاسيما مدى خضوعها لسيادة الدول من عدمه، وما يستتبعه ذلك، من صعوبة تحديد هل تُمثل العمليات السيرانية ومنها التجسس، انتهاكًا لسيادة الدول وتدخلاً في شئونها أم لا. وكذلك الصعوبة المُتمثلة في نظر بعض الدول إلى التجسس عمومًا، باعتباره وظيفة حكومية مشروعة، وربَّما يُشكّل عُرفًا دوليًا في مرحلة النشأة[2].

ولتحليل الوضع القانوني للتجسس السيبراني، فإننا نناقش مدى خضوع الفضاء السيبراني لسيادة الدول، وما يستتبع ذلك من أن العمليات ذات الصلة به، تُعد تدخلاً غير مشروع في شئون الدول، كما نتطرق لدراسة مدى إمكان إسباغ صفة العرف الدولي على هذا السلوك، وذلك على ضوء التوجيهات التي أورها "دليل تالين" بشأن التجسس السيبراني، وأخيرًا نتناول قواعد المسئولية الدولية التي تحكم تقرير المسئولية في حالة العمليات السيبرانية، **ونعرض لذلك من خلال المباحث الآتية:**

المبحث الأول: مدي اعتبار التجسس السيبراني تدخلاً غير مشروع في شئون الدول.

المبحث الثاني: مدى إمكان تأهل ممارسة التجسس السيبراني وقت السلم كعرف دولي.

المبحث الثالث: المسئولية الدولية الناشئة عن العمليات السيبرانية.

---

(1) ***S. DARCY***, *Assistance, Direction and Control: Untangling International Judicial Opinion on Individual and State Responsibility for War Crimes by Non-state Actors, International Review of the Red Cross, 96(893), 2014.*

(2) ***G. BROWN, K. POELLET***, *the Customary International Law of Cyberspace, P. R., P.133.*

المبحث الأول

مدي اعتبار التجسس السيبراني تدخلاً غير مشروع في شئون الدول

قرَّر جانب من الفقه، أنه خلال عام ١٩٨٦، حدَّدت الجمعية العامة للأمم المتحدة، خمسة عشر مبدءًا، لضبط عمليات استشعار الأرض عن بُعد، من خلال الأقمار الصناعية والوسائل الأخرى في الفضاء الخارجي، مع التأكيد على ألا تخرج هذه العمليات، عن نطاق الاستكشاف لأغراض تحسين إدارة الموارد الطبيعية، والاستخدام المُستدام للأراضي، وحماية البيئة، وأن تتم على أساس احترام سيادة الدول التي تخضع أقاليمها للبحث، وحظر القيام بما قد يمس هذه السيادة، كمراقبة الأنشطة العسكرية من خلال الأقمار الصناعية[١]، وهو ما يعني أن الممارسات التي تتم من خلال أجهزة إلكترونية كالأقمار الصناعية تؤثر على سيادة الدول[٢].

ومن ثم، يكون من الضروري مناقشة مدى خضوع حيز الفضاء السيبراني لسيادة الدول، لأنه في حالة خضوعه، فإن العمليات التي تتم من خلاله كالمراقبة والتجسس، تُعد تدخلاً غير مشروع في سيادة الدول، أما إذا لم يكن خاضعًا لسيادة الدول فإنه لا محل للقول بانتهاك التجسس السيبراني لسيادة الدول، أو اعتباره تدخلاً في شئونها. **ونوالي دراسة هذه الإشكالية من خلال المطالب التالية:**

المطلب الأول: الاتجاه الخاص بخضوع الفضاء السيبراني لسيادة الدول وعدم مشروعية التجسس السيبراني.

المطلب الثاني: مدي اعتبار التجسس السيبراني مُكافئًا للتدخل باستخدام القوة المسلحة.

المطلب الثالث: الاتجاه الخاص بعدم خضوع الفضاء السيبراني لسيادة الدول ومشروعية التجسس السيبراني.

المطلب الأول

الاتجاه الخاص بخضوع الفضاء السيبراني لسيادة الدول

وعدم مشروعية التجسس السيبراني

بالرغم من أن الفضاء السيبراني بيئة افتراضية بلا حدود، إلا أنه غير مُنبت الصلة بسيادة الدول الإقليمية، وذلك بتقدير أن هذا الحيّز يعتمد في وجوده على عناصر مادية، هي التي تُنشئه وتُشكّله وتُفعّلُه، ولا وجود له بدونها، ويُطلق عليها "البنية التحتية السيبرانية"، ومنها أجهزة الحاسب الآلي، ومكونات شبكات الانترنت، ووسائط اتصالهما، كالكابلات، والأسلاك، وأبراج متابعة الاتصالات، وأجهزة التحكم في بث الأقمار الصناعية، وكذلك الأفراد القائمين على تشغيل وتفعيل تلك العناصر المادية، التي توجد أو تمر داخل أقاليم دول، وتخضع لسيادتها وولايتها، ورقابتها القانونية والتنظيمية[٣].

---

(1) ***G.A. Res. 41/65, Annex****, U.N. Doc. A/RES/41/65 (Dec. 3 1986).*

(2) ***G. BROWN, K. POELLET****, the Customary International Law of Cyberspace, P. R., P.133.*

(3) ***P. W. FRANZESE****, Sovereignty in Cyberspace: Can it exist? Air Force Law Review 64, 2009, P. 33.*

ولما كان هذا الفضاء مادي في جزء منه، وتوجد عناصره داخل أقاليم دول وتخضع لسيادتها، فلكي نُحدَّد مدى إمكان انتهاك التجسس السيبراني لمبدأ السيادة والسلامة الإقليمية للدول، واعتباره تدخلاً في شئون الدول، **فإننا نُفرّق بين حالتين؛ الأولي:** وجود البنية التحتية المادية للفضاء السيبراني داخل إقليم دولة مستهدفة، **والحالة الثانية،** وجود هذه البنية داخل إقليم دولة ثالثة، بخلاف الدولة المُهاجمة والدولة المُستهدفة، **ونوالي دراسة ذلك من خلال الفرعين التالين.**

الفرع الأول

وجود البنية التحتية المادية للفضاء السيبراني داخل إقليم دولة مستهدفة

في عام ٢٠١٣، أوضح فريق الخبراء الحكوميين التابع للأمم المتحدة، والمعني بالتطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي، أن مبدأ سيادة الدولة ينطبق على أنشطة الدولة الخاصة بتكنولوجيا المعلومات والاتصالات، كما تخضع البنية التحتية السيبرانية، داخل أراضي الدول لولاياتها القضائية[١]، وفي تقريره عام ٢٠١٥، كرّر الفريق هذه الفقرة، وأكَّد على انطباق مبدأ سيادة الدول على استخدام تلك التكنولوجيا، وضرورة مراعاة عدم التدخل في شئون الدول الأخرى عند الاستفادة منها[٢].

وتتعلَّق هذه الحالة بقيام دولة، بتخزين بيانات ومعلومات أو نقلها، من خلال أجهزة ووسائط موجودة داخل إقليمها، ثم التجسس عليها ونسخها والحصول عليها، وبغض النظر عما إذا كانت تلك البنية التحتية الإلكترونية حكومية، أو تملكها شركات خاصة أو أفراد، فإن تلك المعلومات والبيانات تخضع لسيادة الدولة وولايتها القضائية[٣]، ويمثّل التجسس أو التطفل عليها بأي طريقة، انتهاكًا لهذه السيادة وتدخلاً غير مشروع في شئون الدولة، وتحديدًا حقها في أن تقرر بحرية ودون إكراه، من يُرخَّص له للوصول إلى هذه البيانات أو يُمنع من ذلك، ويحق للدولة في هذه الحالة أن تُمارس ولايتها القضائية على سلوك التجسس السيبراني، كفعل نشأ خارج إقليمها، ولكنه اكتمل ولو جزئيًا داخل إقليمها، باختراق أجهزة داخل إقليمها[٤].

ومن الممارسات الدولية التي تُجسَّد هذا الاتجاه، قيام الولايات المُتحدّة الأمريكية، منذ بداية الستينيات بنشر أقمار صناعية في الفضاء الخارجي، لجمع معلومات عن أنشطة دول أخرى، لاسيما الاتحاد السوفيتي السابق، وحينها لم تقم أي دولة بإثارة مسألة انتهاك سيادتها الإقليمية، بحساب أن القانون الدولي لا يفرض حظرًا على مراقبة الأرض من الفضاء، مع كونها سلمية، ولا تُشكّل تدخلاً ماديًا في أقاليمها، إلى أن أعلن الاتحاد السوفييتي السابق، أن هذه الأقمار قد أُستخدمت لجمع معلومات عن أنشطته

---

(1) ***Group of Governmental Experts on Developments in the Field of Information*** *and Telecommunications in the Context of International Security, UN Doc A/68/98, 24 June 2013, para. 20.*

(2) ***Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security****, UN Doc A/70/174, 22 July 2015, para 27, 28/b.*

(3) ***A. AUST****, Handbook of International Law, 1st. edn. Cambridge University Press, 2005, PP; 43:44.*

(4) ***E. SHOSHAN****, Applicability of International Law on Cyber Espionage Intrusions, P. R., PP. 32: 36.*

العسكرية، وبما يعني أن سيادته قد أُنتهكت، وتم التدخل في إقليمه، وقرّر ممثل الاتحاد أمام الجمعية العامة للأمم المتحدة، أن التجسس أيًا كانت طريقته غير مشروع، وقد استهدفت المراقبة الأمريكية، جمع معلومات سرَّية تحرسها دولة ذات سيادة، وبغض النظر عن الوسيلة، فقد تم دون ترخيص، وبالمخالفة للقانون الدولي، وبما يُعد انتهاكًا لسيادة الاتحاد[١].

وفي عام ٢٠١٣، عندما تم الكشف عن قيام (*NSA*)، بالتجسس "إلكترونيًا" وبشكل دوري وروتيني على بعض الدول؛ رفضت "الأرجنتين"، و"بوليفيا"، و"البرازيل"، و"أوروجواي"، و"فنزويلا"، هذا السلوك وأدانته كونه يُمثّل انتهاكًا لسيادتها الإقليمية، وعرض ممثلو هذه الدول رفضهم وإدانتهم شفويًا على الأمين العام للأمم المتحدة، وأوضح وزير خارجية "فنزويلا" أمام مجلس الأمن رفض بلاده لأفعال التجسس العالمي التي تقوم بها الحكومة الأمريكية، والتي تنتهك سيادة الدول، ودعا الأمم المتحدة إلى إدانة هذا الانتهاك وفرض جزاء عليه[٢].

كما ألغت "ديلما روسيف" رئيسة "البرازيل"، زيارة كانت مقررة لها إلى واشنطن للقاء "أوباما"، ومع انعقاد الجمعية العامة للأمم المتحدة في نفس العام، ندَّدت "روسيف" في كلمتها بهذه الواقعة، واعتبرتها انتهاك لسيادة دولتها، وتَدَخُل في شئونها بالمخالفة للقانون الدولي، وقرَّرت أنه لا يمكن لأي دولة أن تدعم سيادتها على حساب الإضرار بسيادة دولة أخرى، وأشارت إلي أنها أبلغت الولايات المتحدة رسميًا، اعتراض بلادها علي هذه الأعمال غير القانونية، وطالبتها بالتفسير، والاعتذار، وتقديم ضمانات لعدم التكرار[٣]".

وأعلنت بعض الدول الأخرى موقفها من هذه الواقعة، ومنها "ألمانيا"، التي قرّرت أن هذا السلوك غير مقبول إطلاقًا، من كافة الوجوه، سواء القانونية، أم السياسية، أم الأخلاقية[٤]، وصرَّحت "فرنسا" أنها لا تقبل هذا السلوك من الشركاء والحلفاء[٥]، وأعلنت الصين أن (*NSA*) تنتهك القانون الدولي بشكل صارخ، وتهدد الأمن السيبراني العالمي، ويجب أن يُرفض سلوكها ويُدان من كل دول العالم[٦].

ونلاحظ أن رد فعل بعض الدول على الواقعة، بدا واضحًا ومُحدَّدًا، كالبرازيل، التي رفضت هذا السلوك باعتباره مخالفة للقانون الدولي، وكذلك "المانيا"، التي قرّرت عدم قبول هذا الفعل، وأدانت

---

(1) ***T. BAEV**, USSR Representative to the Legal Subcommittee of the UN Space Committee, Summary Record of the Twentieth Meeting, UN Doc No A/AC.105/C.2/SR.28/13, 3 May 1963.*
(2) ***Note Verbale**, from the Permanent Mission of the Bolivarian Republic of Venezuela to the United Nations Addressed to the Secretary-General, UN Doc A/67/946, 29 July 2013, 2.*
(3) ***Quoted in Julian Borger,** Brazilian President: US Surveillance a 'Breach of International Law, the Guardian September 24, 2013, **available at:** http://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance. 18/1/2020.*
(4) ***Quoted in Merkel Calls Obama about "US Spying on Her Phone",** BBC News, October 23, 2013, **available at:** http://www.bbc.co.uk/news/world-us-canada-24647268.22/2/2020.*
(5) ***Quoted in Hollande: Bugging Allegations Threaten EU-US Trade Pact,'** BBC News, July 1, 2013, **available at:** http://www.bbc.co.uk/news/world-us-canada-23125451.22/2/2020.*
(6) ***Quoted in China Demands Halt to 'Unscrupulous' US Cyber-Spying**,' The Guardian, May 27, 2014, **available at:** http://www.theguardian.com/world/2014/may/27/china-demands-halt unscrupulous-us-cyber-spying. 22/2/2020.*

الواقعة بكافة جوانبها، بينما بدت مواقف بعض الدول غامضة، ولا تُقدّم إفادة بشأن رؤيتها للتجسس السيبراني، ومنها "فرنسا"، التي قرَّرت عدم قبول هذا السلوك من "الشركاء والحلفاء"، وبما يحتمل التفسير بأنها قد تقبله من دول غير حليفة، ولا تعتبره انتهاكًا في هذه الحالة، وكذلك "الصين"، التي جاءت إدانتها، بعد عدة أشهر من صدور التقرير الأمريكي "*Mandiant*"، الذي أورد أن "الصين" متورطة وبشكل مستمر في التجسس السيبراني علي الدول[١]. إلا انه في المجمل، وبغض النظر عن طريقة التعبير، أو مدى قوة رد الفعل، فقد أشارت كل ردود الأفعال، إلى عدم قبول التجسس السيبراني، واعتباره انتهاكًا لسيادة الدول الإقليمية ولو بشكل جزئي.

وقد عالج دليل "تالين" مبدأ سيادة الدول على أنشطة البني التحتية السيبرانية داخل أقاليمها، وواجبها بعدم السماح باستخدام أراضيها، للقيام بأنشطة سيبرانية تتعارض مع حقوق الدول الأخرى، حيث قرّرت القاعدة رقم (١) من "تالين ١"، والقاعدة رقم (٢) من "تالين ٢" بعنوان "السيادة"، حق الدولة في ممارسة السيطرة على البنية التحتية السيبرانية، والأنشطة ذات الصلة بها، التي تتم داخل إقليمها السيادي[٢]، كحقها في التحكُم في الاتصال بالإنترنت، وأن تقطعه كليًا أو جزئيًا عن أي بنية تحتية إلكترونية داخلية، وذلك رهنًا بأي قيود اتفاقية أو عرفية دولية، ولها أن تُخضع هذه البنية والأنشطة المرتبطة بها، للرقابة القانونية والتنظيمية، سواء كانت تلك البنية حكومية، أو خاصة، أو ما إذا كانت الأنشطة تتم من قبل الدولة، أو أفراد عاديين أو كيانات أخري[٣].

وانتهي الدليل إلى إقرار أمرين؛ الأول: أن العمليات السيبرانية التي تستهدف البني التحتية الالكترونية داخل الدول، وينتج عنها أضرارًا مادية، تُمثّل انتهاكًا لسيادة هذه الدول. **والثاني،** لا يُمكن تصنيف العمليات التي لا تتسبب في أضرار مادية، كتدخل أو انتهاك لسيادة الدول المُستهدَفة، إلا إذا كان الهدف من العملية هو استخدام المعلومات أو البيانات لاحقًا لإكراه الدولة، على اتخاذ قرارات في الأمور التي يحق لها أن تُقرّرها بحريَّة، كالتلاعب بنتائج الاقتراع في انتخابات رئاسية[٤]، ومن ذلك، لم تُصنَّف الهجمات السيبرانية التي وُجهت ضد "استونيا" عام ٢٠٠٧، كانتهاك لسيادتها أو تدخلاً في شئونها، بالرغم من أنها قد تسبّبت في إعاقة بعض المهام الحكومية، وذلك علي سند من أنها قد استهدفت سرقة معلومات، دون توافر قصد استخدامها لإكراه حكومة "استونيا" على اتخاذ قرارات مُعينة[٥].

ومن العرض السابق لهذه الحالة يُمكن القول بأنه:

أولاً: تخضع البيانات المُخزَّنة على أجهزة تقع داخل إقليم الدولة، لسيادتها وولايتها القضائية، ويمثّل التجسس عليها أو التطفل عليها بأي طريقة، انتهاكًا لهذه السيادة وتدخلاً غير مشروع في شئون

---

(1) ***B. RABOIN****, Corresponding Evolution: International Law and the Emergence of Cyber Warfare, 31 J. NAT'L ASS'N ADMIN. L. JUDICIARY, 2011, PP. 625: 630.*

(2) ***Rule No. 2 of the Tallinn Manual 2: Sovereignty:*** *A State enjoys sovereign authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations.*

(3) ***M. N. SCHMITT****, the law of cyber warfare: quo vadis? stanford law & policy review, Vol. 25:269, 2014.*

(4) ***P. WRANGE****, Intervention in National and Private Cyberspace and International Law, Leiden, Brill, Nijhoff, 2014, P. 322.*

(5) ***R. BUCHAN****, Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? Journal of Conflict and Security Law 17, 2012, P. 211.*

الدولة، وتحديدًا انتهاك حقها في أن تقرر بحرية ودون إكراه، من يُرخَّص له للوصول إلى هذه البيانات أو يُمنع من ذلك.

ثانيًا: على الرغم من اتجاه دليل "تالين"، لنفي انتهاك سيادة الدول المضرورة، في حالة العمليات السيبرانية التي لا تنطوي على إكراه، إلا أن هذه العمليات تبقي غير مقبولة من جانب المجتمع الدولي، لأنها تنطوي على شبهة تدخل في شئون الدول، وهو ما اتضح من خلال عدم تَقَبُّل المجتمع الدولي لأنشطة المراقبة السيبرانية، التي أجرتها وكالة الأمن القومي الأمريكي على بعض الدول، بالرغم من عدم تسببها في أية أضرار، حيث لا يُتطلَّب أن تكون الأنشطة مدمرة ماديًا أو ضارة، ولكن يكفي أن تكون غير قانونية.

ثالثًا: وفقًا لدليل "تالين"، تم اعتماد عنصر "القصد" من العملية لتصنيف ما إذا كانت تُمثّل انتهاكًا لسيادة الدول، حيث قرّرت القاعدة (٣٠) من "تالين ١"، أن تصنيف هذه العمليات يتوقف على "الهدف منها"، وهو أمر نفسي، ربما يُمكن استجلائه بشأن تعاملات الأفراد، إلا أنه أمر لا مجال له في سياق الحديث عن أنشطة الدول، علاوة على أنه، في حالة استخدام المعلومات لاحقًا للتأثير على الدولة وإكراهها على فعل معين، فمن المنطقي أن تُصنف العمليات السيبرانية التي أدت إلى ذلك، باعتبارها تدخلاً في شئون الدول.

رابعًا: قد تفتقر بعض الدول إلى تقنيات تُمكنها من الإحاطة بالعمليات السيبرانية، التي تنطلق من إقليمها وتستهدف دولاً أخري، أو تفتقر إلى القدرة على وقف هذه العمليات، أو التعامل معها في وقت مناسب، وهنا ينشأ واجب قانوني على تلك الدول ببذل العناية الواجبة لمنع مثل هذه العمليات، سواء قبل بدايتها، أو عند انطلاقها، أو إنهائها بعد إطلاقها، ونظرًا لأن معيار بذل العناية نسبي، فإن القدر المتيقن للإخفاق في بذل العناية، هو ألا يصدر عن الدولة أي رد فعل، عند علمها بالتخطيط، أو الشروع في هذه العمليات، وفي كل الأحوال، على الدول أن تتخذ تدابير الحيطة، لمنع انطلاق هذه العمليات من أراضيها[1].

الفرع الثاني

وجود البنية المادية السيبرانية على إقليم دولة أخرى بخلاف المُستهدفة بالتجسس

قد تُخزِّن دولة أو تنقل معلومات سرية تملكها، من خلال أجهزة أو ناقلات موجودة داخل أقاليم دول أخرى، مع احتفاظها بملكية المعلومات، وفي حالة التجسس على هذه المعلومات، فإنه وبحسب الأصل، **يحق للدولة التي توجد البنية التحتية الالكترونية على إقليمها**، أن تحتج بانتهاك سيادتها الإقليمية، **أما بالنسبة للدولة صاحبة المعلومات**، فإن الأمر محل نظر، حيث لا يوجد أساس قانوني يُمكنها الاستناد إليه، للادعاء بأن سيادتها قد أُنتهكت، أو أنه قد تم التدخل في شئونها الداخلي.

إلا أن هناك بعض الاتفاقات الدولية، والأحكام القضائية الدولية والوطنية، وبعض الممارسات الدولية، يُمكن أن تُشكّل أساسًا قانونيًا، بشأن سيادة الدولة علي معلوماتها المُخزنة أو المنقولة الكترونيًا، من خلال وسائل داخل دول أخري، وبالتالي انتهاك سيادتها إذا تم التجسس على هذه المعلومات. **ونوالي بيان ذلك كما يلي:**

---

(1) ***K. E. EICHENSEHR**, the Cyber-Law of Nations, P. R., PP. 336:340.*

أولاً: اتفاقية الأمم المتحدة بشأن حصانات الدول وممتلكاتها من الولاية القضائية لعام ٢٠٠٤:

قضت المادة رقم (٥) من اتفاقية الأمم المتحدة بشأن حصانات الدول وممتلكاتها من الولاية القضائية لعام ٢٠٠٤، بتمتع الدولة في ما يتعلق بذاتها وممتلكاتها، بالحصانة من ولاية محاكم الدول الأخرى[١]، كما بيّنت المادة رقم (١٠) من الاتفاقية، أنه في بعض الحالات، لا يُمكن للدولة الاحتجاج بحصانتها فيما يخص الإجراءات الناشئة عن "معاملاتها التجارية"[٢]، وبما يعني أن ما تملكه الدولة أو تستخدمه لأغراض "غير تجارية"، يدخل ضمن سيادتها ويخضع لولايتها القضائية الخالصة، حتى إذا وُجد على إقليم دولة أخرى.

وبتطبيق حكم المادتين المذكورتين بشأن التجسس على معلومات تملكها الدولة، وتُخزنها أو تنقلها عبر بنية الكترونية داخل إقليم دولة أخري، فإننا نُفرّق بين المعلومات "التجارية"، و"غير التجارية"، وتظل الثانية خاضعة لسيادة الدولة المالكة لها، ويُعد التجسس عليها ـ حتى داخل إقليم دولة أخري ـ تدخلاً في سيادة الدولة المالكة، بخلاف المعلومات المتعلقة بمعاملات تجارية، فلا يمكن للدولة الاحتجاج بآثار مبدأ السيادة بشأنها[٣].

ثانيًا: اتفاقية "فيينا" للعلاقات الدبلوماسية لعام ١٩٦١:

منحت المادة (٣/٤٠) من اتفاقية "فيينا" للعلاقات الدبلوماسية لعام ١٩٦١، حصانة لاتصالات الدول ومراسلاتها، التي تتم عبر دول أخرى، وأوردت التزامًا على الدول الثالثة ـ بخلاف الدولة الموفدة والموفد لديها ـ بمنح جميع المراسلات الرسمية المنقولة عبر إقليمها، بما فيها الرسائل المرسلة بالرموز أو الشفرة أو الحقائب الدبلوماسية، نفس الحرية والحماية الممنوحتين لها في الدولة المعتمد لديها[٤]، ويمكن فهم هذا الالتزام، باعتبار أن هذه المراسلات والاتصالات، وما يتم تداوله فيها من بيانات أو معلومات، والحقائب الدبلوماسية والأشياء المنقولة فيها، تتعَلَّق بسيادة دولة، ويُمثّل اعتراضها أو التجسس عليها، انتهاك لسيادة الدول صاحبة المعلومات.

---

(١) **نصت المادة رقم (٥) من الاتفاقية على أنه: "**تتمتع الدولة، فيما يتعلق بنفسها وبممتلكاتها، بالحصانة من ولاية محاكم دولة أخرى، رهنا بأحكام هذه الاتفاقية". **راجع:**
United Nations Convention on Jurisdictional Immunities of States and Their Property, *A/RES/59/38 (2 December 2004).*

(٢) **نصت المادة (١٠) من الاتفاقية على أنه:** "١- إذا دخلت دولة في معاملة تجارية مع شخص أجنبي طبيعي أو اعتباري، وكانت المنازعات المتعلقة بالمعاملة التجارية تقع، بمقتضى قواعد القانون الدولي الخاص الواجبة التطبيق، ضمن ولاية محكمة دولة أخرى، لا يجوز للدولة أن تحتج بالحصانة من تلك الولاية في دعوى تنشأ عن تلك المعاملة التجارية. ٢- لا تسري الفقرة (١): (أ) في حالة معاملة تجارية بين الدول؛ (ب) أو إذا اتفق طرفا المعاملة التجارية على غير ذلك صراحة. ٣- عندما تكون إحدى المؤسسات الحكومية أو الكيانات الأخرى التي أنشأتها الدولة والتي لها شخصية قانونية مستقلة وأهلية. (أ) التقاضي؛ (ب) واكتساب الأموال أو امتلاكها أو حيازتها والتصرف فيها، بما في ذلك الأموال التي رخصت لها الدولة بتشغيلها أو بإدارتها؛ طرفًا في دعوى تتصل بمعاملة تجارية لذلك الكيان، فإنه لا تتأثر الحصانة من الولاية القضائية التي تتمتع بها تلك الدولة".

(3) ***K. IRION,*** *Government Cloud Computing and National Data Sovereignty, Policy and Internet, 2013, P. 52: 55.*

(4) ***Article (40/3) of Vienna Convention on Diplomatic Relations 1961: 3.*** *Third States shall accord to official correspondence and other official communications in transit, including messages in code or cipher, the same freedom and protection as is accorded by the receiving State. They shall accord to diplomatic couriers, who have been granted a passport visa if such visa was necessary and diplomatic bags in transit, the same inviolability and protection as the receiving State is bound to accord.*

ثالثًا: الاتفاقية الدولية للاتصالات لعام ١٩٧٣[١]:

ألزمت المادة رقم (٢٢) من الاتفاقية الدولية للاتصالات، الأطراف باتخاذ كل التدابير الممكنة لضمان سرية المراسلات الدولية، إلا أنها أوردت استثناءًا على هذا الالتزام، حيث أعطت الحق في إبلاغ هذه المراسلات إلى السلطات المختصة للدول، لغرض ضمان تطبيق قوانينها الداخلية، أو الامتثال للالتزامات المقررة عليها بموجب أي اتفاقيات دولية أخري[٢]، ونلاحظ أن هذا الاستثناء يجعل قانونًا وطنيًا يوجه الاتصالات الدولية، لغرض ضمان استقرار الأمن القومي للدول، وهو اعتداد بالولاية القضائية لهذه الدول، واعتبار أن أي أضرار قد تصيبها نتيجة هذه الاتصالات تُعتبر تدخلاً في سيادتها[٣].

رابعًا: اتفاقية مناهضة التعذيب وحظر المعاملة القاسية واللاإنسانية والمهينة ١٩٨٤، والعهد الدولي للحقوق المدنية والسياسية لعام ١٩٦٦:

انشغلت المادة رقم (٢) من الاتفاقية، بفكرة الولاية القضائية للدولة على مواطنيها المتواجدين داخل أقاليم دول أخري، حيث قضت بضرورة اتخاذ الدول جميع الإجراءات القانونية لوقف التعذيب، **"في أي إقليم يخضع لولايتها"**، وقد صيغت هذه المادة بعد تطويرها في المشروع الأصلي للاتفاقية، والذي لم ترد به عبارة "في أي إقليم"، وقد أعربت فرنسا حينها عن قلقها، من أن صياغة المادة النهائية موسعة جدًا، وسوف تُلزم الدول بتنظيم سلوك مواطنيها المقيمين في دول آخر، حيث يعني إدراج تلك العبارة، ألا يقتصر التزام الدول بهذا الواجب داخل حدودها الإقليمية، وإنما يمتد ليشمل السفن والطائرات المسجلة في دول أخرى، وفي أي إقليم وإن كان محتلاً[٤].

وحري بالذكر أن المادة رقم (٢) من العهد الدولي للحقوق المدنية والسياسية لعام ١٩٦٦، قد وسَّعت من النطاق الجغرافي لسيادة الدول على مواطنيها، أكثر مما ورد باتفاقية مناهضة التعذيب، حيث قضت بتعهد كل دولة طرف باحترام الحقوق المعترف بها في العهد، وكفالة هذه الحقوق لجميع الأفراد الموجودين في إقليمها وكذلك "الخاضعين لولايتها"، وبما يمكن تفسيره باعتبار أن **الدولة تلتزم ناحية فئتين، الأولي:** الأفراد الموجودين على إقليمها، **والثانية** الخاضعين لولايتها، وهو ما يعني أنه يجوز للدول ممارسة الاختصاص القضائي فيما يتعلق بمواطنيها بصرف النظر عن موقعهم ومكان تواجدهم[٥].

---

(١) **تم التوقيع عليها في ١٤ سبتمبر عام ١٩٧٣، خلال مؤتمر "مالقة باسبانيا" (*Málaga-Torremolinos*)**، وبموجبها تم دمج الاتفاقية الدولية للبرق، والاتفاقية الدولية للبرق بالراديو، وبحيث تغطي مجالات التلغراف والاتصالات الهاتفية والإذاعية، **راجع:**

International Telecommunication Convention, *Nov. 6, 1982, art. 22, 1531 U.N.T.S. 319 (entered into force Jan. 1, 1984).*

(2) ***Article (22):*** *1- Members agree to take all possible measures, compatible with the system of telecommunication used, with a view to ensuring the secrecy of international correspondence.* ***2-*** *Nevertheless, they reserve the right to communicate such correspondence to the competent authorities in order to ensure the application of their internal laws or the execution of international conventions to which they are parties.*

(3) ***C. FORCESE****, International law and intelligence gathering, Journal of National Security Law & Policy, Vol. 5:179, 2011, PP. 131: 133.*

(4) ***C. FORCESE****, International law and intelligence gathering, P. R., PP. 139: 149.*

(5) ***Restatement (Third)*** *the Foreign Relations Law of the United States, §402 (1987).*

وفي رأيها الإفتائي بشأن بناء جدار في الأرض الفلسطينية المحتلة عام ٢٠٠٤، أشارت محكمة العدل الدولية، إلى أن التزامات الدولة بموجب العهد الدولي الخاص بالحقوق المدنية والسياسية، تمتد إلى خارج حدود ولايتها القضائية، وتنطبق على الأفعال التي تقوم بها الدولة في ممارستها لولايتها خارج إقليمها[١].

خامسًا: حكم محكمة العدل الدولية في قضية "*East Timor v Australia*" عام ٢٠١٤:

في عام ٢٠١٣، داهمت وكالة الاستخبارات الأسترالية مكتب محاماة داخل "استراليا"، لمحام أسترالي يعمل كمستشار قانوني لدولة "تيمور الشرقية"، بغرض الحصول على وثائق تخص نزاع قائم بين الدولتين، ومعروض على محكمة تحكيم دولية، بشأن بطلان معاهدة "بحر تيمور" لعام ٢٠٠٢، وبالفعل تمكنت "استراليا" من الاستيلاء بالإكراه على وثائق سريّة "لتيمور"، والتي بدورها تقدَّمت في ١٧ ديسمبر ٢٠١٣، إلى محكمة العدل الدولية، بطلب لإصدار أمر مؤقت يُعلن بموجبه أن استيلاء "أستراليا" على تلك الوثائق، ينتهك من بين جملة أمور: ... (ط) سيادة دولة "تيمور"، مع إلزام "استراليا" بردها فورًا، وإتلاف أي نسخ في حوزتها[٢].

وفي الثالث من مارس لعام ٢٠١٤، اعتبرت المحكمة أن ادعاء "تيمور الشرقية" مقبول[٣]، وأصدرت أمرًا مؤقتًا بوجوب عدم تدخل استراليا بأي شكل في اتصالات "تيمور" ومستشاريها القانونيين، إعمالاً لمبدأ المساواة في السيادة بين الدول المنصوص عليه في المادة (١/٢) من ميثاق الأمم المتحدة. **وكان مما ورد بهذا الأمر[٤]:**

١) "تكفل "أستراليا" ألا يُستخدم مضمون المواد المُصادرة، بأي حال من الأحوال، أو في أي وقت من الأوقات، من جانب أي شخص أو أشخاص للإضرار بمصلحة "تيمور" إلى أن يتم البت في القضية؛

٢) تحتفظ أستراليا بالوثائق والبيانات الالكترونية المُصادرة وأي نسخ منها إلى أن تصدر المحكمة قرارًا آخر في هذا الشأن؛

٣) عدم تدخل "أستراليا" بأي شكل في الاتصالات بين "تيمور" ومستشاريها القانونيين، في التحكيم قيد النظر، بشأن معاهدة "بحر تيمور" لعام ٢٠٠٢، وفي أي مفاوضات ثنائية بشأن تعين الحدود البحرية مستقبلاً، أو في أي من الإجراءات الأخرى ذات الصلة بين الدولتين، بما في ذلك هذه القضية المعروضة على المحكمة.

ونلاحظ أن المحكمة لم تُشر في الأمر إلى مدى شرعية سلوك أستراليا، وإنما أشارت إلى وجوب احترامها لاتصالات "تيمور" مع مستشاريها، وفقًا لمقتضيات مبدأ سيادة الدول، ويمكن فهم منطق

(1) ***ICJ,*** *Advisory Opinion, 2004 I.C.J. 136, Para. 111, (July 9).*
(2) ***Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia),*** (*Provisional Orders), 2014, International Court of Justice, Reports of Judgments 147, paras. 1, 2, 26, 27, 55* ***available at****: https://www.icj-cij.org/en/case/156. 6/5/2020.*
(3) ***Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia),*** *P. R., Paras. 27, 28.*
(4) ***Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia),*** *P. R., Para. 55.*

المحكمة باعتبار أنه من المعقول أن تكون الوثائق التي احتفظ بها مستشار "تيمور الشرقية"، بمكتبه داخل إقليم "أستراليا"، مرتبطة ومصطبغة بسيادة "تيمور"، وأن التدخل للاستيلاء عليها يحظره القانون الدولي، **ومما يؤيّد هذا الفهم**، أنه بعد مضي عدة أشهر، وتحديدًا في ٢٥ مارس ٢٠١٥، صرَّحت "أستراليا" أنها تعتزم إعادة الوثائق إلى "تيمور"، وفي ٢٢ أبريل ٢٠١٥، أذنت المحكمة بإعادة المستندات المعنية وأي نسخ منها إلى "تيمور"، **وهو منحي يمكن إدراكه كاعتراف ضمني، من جانب أستراليا بأن أفعالها انتهكت الحقوق السيادية لدولة "تيمور".**

ومن ثم، يُمكن القول بأنه عندما تُخزِّن دولة معلوماتها السرية أو تنقلها على بنية تحتية إلكترونية داخل دولة أخرى، فإن هذه المعلومات تمثل بُعدًا للسيادة الوطنية للدولة التي تملكها، ويُمثِّل اقتحامها أو فض سريتها انتهاكًا لسيادة هذه الدولة[١].

سادسًا: قرار لجنة حقوق الإنسان في قضية *(Lopez v. Uru.)* عام ١٩٧٩:

تتلّخص وقائع القضية في اختطاف شخص وترحيله بالإكراه من "الأرجنتين"، وذلك بواسطة وكلاء لدولة "أوروجواي"، مع معاملته بشكل لا إنساني وحاط بالكرامة، وقد خلصت اللجنة إلى أن الأفراد قد يخضعوا للولاية القضائية للدولة، وإن لم يكونوا فعليًا على إقليمها، وأن المواطن "*Lopez*" كان يخضع للولاية القضائية لدولة "أوروجواي"، لكونه في نطاق سلطتها وسيطرتها الفعلية حتى وإن لم يكن على إقليمها[٢].

سابعًا: إدانة بعض أعضاء مجلس الأمن للتجسس الأمريكي عليهم:

قامت الولايات المتحدة الأمريكية وبريطانيا بالتجسس السيبراني على العراق، في الفترة التي سبقت غزوها له عام ٢٠٠٣، وامتد هذا التجسس ليشمل أعضاء في مجلس الأمن، سواء داخل دولهم أو خارجها، بهدف تقييم مدى دعمهم لصدور قرار يُجيز الغزو، وبما يشمل التحالفات التي يعتزمون الدخول فيها، والدول التي سيكون موقفها تابعًا لدول أخرى، وكل ما يمكن أن يُعطِي لصانعي السياسات الأمريكيين ميزة لتحقيق هدفهم، أو تفادى المفاجآت، وبعد كشف تفاصيل هذا التجسس[٣]؛ أعرب ممثلي الدول عن صدمتهم، باعتبار أن هذه الممارسة تُمثّل تدخلاً واضحًا في شئون دولهم، وانتهاكًا للسياسة الخارجية للدول الأعضاء في المجلس[٤].

ثامنًا: حكم المحكمة العليا الكندية في قضية (*R. v. Hape*) عام ٢٠٠٧:

أكدت المحكمة العليا الكندية في قضية "*R. v. Hape*"، على عدم جواز القيام بأي إجراءات تنفيذ جبري على أراضي دولة أخرى دون موافقتها، باعتبار أن هذه الإجراءات تُعد عملاً سياديًا خالصًا

(1) ***K. IRION***, *Government Cloud Computing and National Data Sovereignty, P. R., P. 42.*
(2) ***Human Rights Comm.,*** *Commc'n No. 52/1979 (Lopez v. Uru.), U. N. Doc. CCPR/C/13/D/52/1979 (1984),* ***available at****: http://www1.umn.edu/humanrts/undocs/html/52_1979.htm. 7/6/2020.*
(3) ***M. BRIGHT, E. VULLIAMY, P. BEAUMONT****, Revealed: U.S. Dirty Tricks to Win Vote on Iraq War, OBSERVER (UK), Mar. 2, 2003,* ***available at:*** *https://archive.commondreams.org/scriptfiles/headlines03/0302-01.htm. 1/5/2020.*
(4) ***S. CHESTERMAN****, Shared Secrets: Intelligence and Collective Security (2006),* ***available at****: http://www.lowyinstitute.org/Publication.asppid=360.5/4/2020.*

للسلطات الوطنية، ولا يُمكن لدولة أن تمارس سلطة عامة على أراضي دولة أخرى[١]، ولا تسمح القوانين الوطنية عادةً لدولة بتفتيش أماكن داخل إقليم دولة أخرى، **وبالقياس على التجسس السيبراني**، فيمكننا اعتبار أن اعتراض دولة، أو فضها لسرية بيانات مملوكة لدولة أخري، وموجودة أو مُخزَّنة داخل إقليم دولة ثالثة؛ بمثابة تفتيش تجريه دولة داخل إقليم دولة أخرى دون موافقة، وهو عمل محظور قانونًا، وعلي سبيل المثال، فسَّرت المحكمة العليا للمملكة المتحدة، الالتزامات المتكافئة بموجب الاتفاقية الأوروبية لحقوق الإنسان، باعتبار أن الأحداث التي تقع داخل مركز احتجاز بريطاني، في العراق تقع ضمن اختصاص المملكة المتحدة[٢].

تاسعًا: بعض قرارات المحاكم الوطنية:

خلصت بعض قرارات المحاكم الوطنية، إلى أن التجسس ينتهك قاعدة السيادة الإقليمية للدول، ومن ذلك، الحكم الذي أصدرته المحكمة العليا الكندية عام ٢٠٠٨، بشأن رفض طلب جهاز المخابرات الكندية، الخاص بالتصريح بمراقبة أفراد متواجدين داخل أراضي دول أخرى، وتأسَّس الحكم على أن مثل هذا النشاط، لا يتوافق مع القانون الدولي، وينتهك مبدأ السيادة الإقليمية، ومبدأ عدم التدخل في شئون الدول[٣].

ووفقًا لما سبق، يُمكننا القول بأن التجسس السيبراني، يُمثّل انتهاكًا لسيادة الدول، وخرقًا لمبدأ عدم التدخل في شئونها، بغض النظر عن الهدف منه، أو مكانه، وسواء تم من خلال بنية إلكترونية داخل إقليم الدولة المُستهدفة، أو بنية إلكترونية داخل إقليم دولة أخري، تستخدمها الدولة لتخزين أو نقل معلوماتها، وقد تأكَّد هذا الاتجاه من خلال بعض المعاهدات الدولية، وأحكام محكمة العدل الدولية، وقرارات الأمم المتحدة، والممارسات الدولية، وبعض الأحكام الوطنية المعروضة سلفًا.

الفرع الثالث

التجسس السيبراني ومدي توافر عنصر الإكراه المُتطلب لإثبات التدخل

بينت الدراسة ضرورة توافر الإكراه، لإثبات أن سلوك دولة تجاه أخري يُعد تدخلاً غير مشروعًا في شئونها، ونناقش من خلال هذا الفرع، مدي توافر عنصر الإكراه في سلوك التجسس السيبراني، وذلك من خلال منظورين أحدهما يُمكن أن نطلق عليه الاتجاه الضيّق، والآخر هو الاتجاه المُوسع، وذلك على النحو التالي.

أولاً: الاتجاه المُضيِّق بشأن مبدأ عدم التدخل:

وفقًا لحكم محكمة العدل الدولية في قضية "نيكاراجو" عام ١٩٨٦، فإن التدخل غير المشروع في شئون الدول، يتحقق بوقوع الإكراه على دولة، ونفي إرادتها، لتتخذ قرارات في المسائل التي يحق لها أن تقررها بحرية[٤]، وبالتالي فإن إثبات ما إذا كان فعلاً معينًا يُمثّل تدخلاً في شئون الدول، يتوقف على

---

(1) ***R v Hape SCC (CanLII) (2007) 2 SCR 292**, para 104-105*

(2) ***P. WRANGE**, Intervention in National and Private Cyberspace and International Law, P. R., PP. 307: 314.*

(3) ***Re Canadian Security Intelligence Service Act** [2008] FC 301, [2008] 4 FCR 230, paras 50–52.; **R v Hape [2007] 2 SCC 26** (CanLII) [2007] 2 SCR 292, para. 87.*

(٤) **حكم محكمة العدل الدولية، قضية نيكاراجوا ١٩٨٦، المرجع السابق، فقرة (**٢٠٥).

أمرين: **الأول؛** أن يكون "القصد" منه إكراه دولة لتُغيِّر سياسة ما لها، وهو أمر يتعلق بنية ومقصد الفاعل. **والثاني،** أن يؤثر هذا الفعل على إرادة الدولة، عند اتخاذ قرار في أي من المسائل أو السياسات التي يحق لها أن تقررها بحرية.

وعند تطبيق هذا النظر على عمليات التجسس السيبراني، لإثبات ما إذا كانت تُمثّل تدخلاً غير مشروعًا، فإننا نلاحظ أنه:

(١) تم اشتراط التعرف على القصد من الفعل، لتقيم ما إذا كان يعتبر تدخلاً، فإذا كان قد تم بقصد التأثير علي سياسة الدولة، فإنه يعد كذلك، وهو أمر يبتعد عن المنطق، لاستحالة استجلاء أو معرفة القصد من سلوك الدول، وبفرض وقوع التجسس السيبراني من قبل أحد الأشخاص كوكيل عن دولة، فإنه إذا لم يتم القبض عليه واستجوابه وإقراره بقصده من التجسس، يكون من المستحيل تلبية هذا الشرط، أو تمييز ما إذا كان قد أراد جمع معلومات سرية لإكراه الدولة، أم أنها مجرد عملية الكترونية تتعلَّق بمنافسة تجارية أو اقتصادية مثلاً.

(٢) يتم نفي وصف التدخل غير المشروع، عن العمليات السيبرانية التي تتعرَّض لها الدول، إذا تمت بدوافع أخرى، بخلاف قصد التأثير على قراراتها أو سياساتها، **وعلي سبيل المثال،** العملية السيبرانية "*Night Dragon*"، التي انطلقت من الصين في فبراير عام ٢٠١١، واستهدف سرقة معلومات تخص شركات أوربية عاملة في مجال النفط والطاقة، مثل صفقاتها، وطرق تمويل مشروعاتها، وعملياتها الميدانية[(١)]، وبالفعل تمت سرقة معلومات من شأنها أن تُمَكِّن أي دولة، أو كيان، أو شركة تحصل عليها، من تحقيق فوائد اقتصادية، وهنا نجد أن الهدف من العملية يتجه إلى الناحية الاقتصادية والتجارية، ووفقًا لنظر محكمة العدل السابق، لا تُمثّل هذه العملية تدخلاً غير قانوني، حيث لم يُقصد منها تغيير السياسة داخل الدولة الضحية.

وكذلك إذا فرضنا أن الدولة (أ) تعتزم التسلل الكترونيًا إلي محطة للطاقة النووية للدولة (ب)، بقصد إجبار (ب) علي تغيير موقف سياسي لها، والتي بدورها قرَّرت عدم تغيير موقفها، فتزداد عمليات الاختراق السيبراني من جانب (أ) وتمتد لتشمل سرقة أو تدمير بيانات المحطة؛ فإن هذه الحالة تُصنف كتدخل محظور. أما إذا كانت الدولة **(أ)** تخترق النظام الالكتروني للمحطة، بقصد سرقة نماذج تشغيلها، أو الاطلاع على تصميمها، ولا تنوي استخدام ذلك لأي غرض آخر، فإنه لا يمكن تصنيف هذه الحالة ـ وفقًا لصياغة محكمة العدل الدولية ـ باعتبارها من قبيل التدخل غير مشروع في شئون الدولة (ب)[(٢)].

(٣) تؤدي مسايرة صياغة محكمة العدل الدولية بشأن ضبط معيار أفعال التدخل، إلى الخلط بين مفهوم التدخل غير المشروع في شئون الدول، وبين مفهوم سيادة الدول المُستهدفة، حيث يشمل مبدأ السيادة حق الدولة في تنظيم الاتصالات السلكية واللاسلكية على إقليمها، ومراقبة مزودي خدمات الانترنت، وسن العقوبات على اختراق البيانات، ولاشك أن تنظيم الدولة لتلك الحقوق، لا علاقة له بنية

(1) ***Office of the Nat'l Counterintelligence Exec.,*** *Foreign Spies Stealing us Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2011, P. 5.*

(2) ***R. A. CLARKE, R. K. KNAKE,*** *Cyber War, P. R., P. 287.*

الطرف الأخر المخالف، أما مضمون التدخل في شئون الدول فهو يتعلَّق باتخاذ قرارات تتعلَّق بمهام ووظائف الدولة بشكل معيب نتيجة تدخل خارجي.

ولذا يمكننا القول بأن صياغة قرار محكمة العدل الدولية في قضية "نيكاراجوا"، يُوفّر توصيفًا غير مكتمل لمبدأ عدم التدخل[1]، وهو ما أقرّت به المحكمة ذاتها، عندما أوردت في بداية نظرها للقضية، أنها سوف تُحدّد فقط جوانب المبدأ التي تبدو وثيقة الصلة بالنزاع المطروح، والذي كان يتمثَّل في القيام بأنشطة شبه عسكرية، وبالتالي اكتفت ببحث جوانب المبدأ ذات الصلة باستخدام القوة، **وفي مجال التجسس السيبراني**، يؤدي تطبيق هذه الصياغة، إلى اختلاف تكييف السلوك الواحد، وهو اقتحام الأنظمة الالكترونية لدولة، تبعًا للقصد منه، وتكييف الواقعة بالاعتماد على قصد المهاجم، وهو أمر يصعب أو يستحيل ضبطه أو استجلائه أو تقييمه.

وعلى ضوء الزخم الفقهي المؤيد لفكرة أن بعض العمليات السيبرانية كالتجسس، يجب أن تدخل ضمن نطاق الحظر الوارد في المادة (٤/٢) من الميثاق، باعتبار أن المعلومات المُتحصل عليها قد تُمهد وتدعم استخدام القوة العسكرية التقليدية ضد دولة[2]؛ **فإنه من المناسب تناول مفهوم التدخل غير المشروع من منظور موسّع، يمكن أن نتلمسه من خلال بعض ممارسات الدول، والمنظمات الدولية، لاسيما الجمعية العامة للأمم المتحدة، وكذلك آراء الفقه الدولي، وذلك على النحو التالي:**

ثانيًا: الاتجاه المُوسَّع لمضمون مبدأ التدخل في شئون الدول:

(١) اتجاه محكمة العدل الدولية في حكمها المؤقت في قضية تيمور" ضد "أستراليا" عام ٢٠١٣:

في عام ٢٠١٣ وفي قضية "تيمور الشرقية" ضد "أستراليا"، أصدرت محكمة العدل الدولية أمرًا مؤقتًا، أشارت فيه إلى أن حصول "استراليا" بالإكراه، من مكتب محاماة يقع داخل الإقليم الاسترالي، على وثائق ومعلومات سرية تخص "تيمور الشرقية"، يؤثر على سيادة "تيمور"، وذلك بشكل مستقل، وبغض النظر عما إذا كانت "استراليا" ستستخدم تلك الوثائق المعلومات أم لا، لإجبار تيمور الشرقية على التصرف بطريقة معينة[3].

ويَشير هذا الأمر المؤقت للمحكمة إلى اتجاه مُوسَّع جدًا بشأن مضمون مبدأ عدم التدخل، حيث اعتبر أن سيادة دولة "تيمور" قد تأثرت، وتم التدخل في شئونها، وذلك "فقط" بقيام "استراليا" باقتحام مكتب مستشارها القانوني، والحصول قسرًا على وثائق ومعلومات تملكها "تيمور"، أي أن التدخل والانتهاك قد وقعا، بغض النظر عما إذا كانت "استراليا" ستستخدم تلك المعلومات أم لا، أو ستقوم بإكراه "تيمور" على التصرف بطريقة معينة، عند اتخاذ قرارات سيادية، أو إقرار سياسات وطنية، من عدمه.

(٢) بعض إعلانات الجمعية العامة للأمم المتحدة:

---

(1) ***D. FLECK**, Individual and State Responsibility for Intelligence Gathering, P. R., PP. 691:692.*

(2) ***M. C. WAXMAN**, Cyber-Attacks and the Use of Force, P. R., P. P. 421.*

(3) ***Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia),** P. R., Paras. 27, 55.*

باستعراض الفقرة الأولي من إعلان الأمم المتحدة لعام ١٩٦٥، بشأن عدم جواز التدخل في شئون الدول[١]، وكذلك المبدأ الأول من إعلان مبادئ القانون الدولي المتعلقة بالعلاقات الودية بين الدول وفقًا لميثاق الأمم المتحدة لعام ١٩٧٠[٢]، نجد أنهما قد اعتمدا صياغة متطابقة بشأن توضيح نطاق مبدأ عدم التدخل، تبيّن أنه **"لا يحق لدولة التدخل بشكل مباشر أو غير مباشر "لأي سبب"، في سيادة أي دولة أخرى أو استخدام "أي تدابير" ... لإكراه دولة أخرى، للحصول منها علي تبعية في ممارسة حقوقها السيادية". ونلاحظ أن صياغة الإعلانين قد اتصفت بالاتساع والمرونة**، بحيث يُحظر التدخل لأي سبب، وباستخدام أي تدابير، لإكراه دولة للحصول على تبعيتها في ممارسة حقوقها السيادية، وتدعم هذه الصياغة فهم حظر التدخل بشكل موسع، لا يتوقف على معرفة نية المُتدخل، أو اشتراط أن تتجه فقط للتأثير على سياسات الدولة.

(٣) أراء بعض الفقه الدولي:

قرَّر جانب فقهي، أنه يمكن إثبات الإكراه وتحقُق التدخل غير المشروع في مجال التجسس السيبراني، بإعمال الحكمة اللاتينية "*de minimis non curat lex*" أو "عدم الاكتراث للأفعال الأصغر"، بمعنى أن تقوم الدولة بتقييم أهمية المعلومات التي تم اختراقها، ومدي تأثر سيادة الدولة بذلك، فإذا كانت الواقعة لا تُمثّل خطورة، ولا تؤثر على مؤسسات الدولة، فإن الدولة لا تكترث لها، ولا تعتبرها تدخلاً في شئونها يتطلَّب تطبيق القانون الدولي، بل تضعها خارج نطاق الاستجابة القانونية، وتقبلها كنتيجة طبيعية للوجود داخل مجتمع، وذلك بخلاف المعلومات المهمة، التي تخص كبار المسئولين في الدولة مثل رئيسها، أو تتعلَّق بالأمن القومي للدولة، هنا تتجاوز هذه الحالة عتبة الإكراه، وتُمثّل تدخلاً غير مشروع[٣].

وذهب جانب فقهي آخر، إلى أن الدول لا تختلف على كون التجسس من الأعمال غير الودية، وقد يكافئ استخدام القوة، إذا كانت الآثار الناتجة عنه جسيمة كالآثار التي قد تنتج عن استخدام القوة التقليدية، وذلك في بعض الحالات، كاستخدام المعلومات المُتحصلة منه للتمهيد أو دعم استخدام القوة، وفي هذه الحالة يعتبر تدخلاً صريحًا في شئون الدول[٤].

(٤) دليل تالين:

قرّرت القاعدة رقم (٦٦) من دليل "تالين ٢"، بعنوان "تدخل الدول"، بأنه لا يجوز للدولة التدخل بالوسائل السيبرانية، في الشئون الداخلية أو الخارجية لدولة أخرى[٥]، كأن تُستخدم العمليات السيبرانية للتلاعب بنتائج اقتراع الكتروني، وتوجيهها نحو فوز مرشح معين، أو أن تفرض دولة حظرًا على

---

(1) ***Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty,*** *G.A. Res. 2131 (XX), U.N. Doc. A/RES/2131(XX) (Dec. 21, 1965).*

(2) ***U.N. Special Comm. on Friendly Relations,*** *U.N. Doc. A/AC.125/SR.110-14 (1970).*

(3) ***S. WATTS****, Low-Intensity Cyber Operations and the Principle of Non-Intervention, Brill, Nijhoff, 2015, PP. 138, 146.*

(4) ***H. S. LIN****, Offensive Cyber Operations and the Use of Force, J Nat'l Sec L & Pol'y 63, Vol. 4:63, 2010, PP. 71: 74.*

(5) ***Rule No. (66) Of Tallinn Manual 2: Intervention by States:*** *A State may not intervene, including by cyber means, in the internal or external affairs of another State".*

التصدير إلى دولة أخرى، فتُطلق الأخيرة عمليات سيبرانية تخريبية، ضد الدولة الأولي لإجبارها على إلغاء الحظر، وبغض النظر عن نتائج هذه العمليات، وسواء نجحت في إكراه الدولة على التصرف المطلوب أم لا، فإنها تُشكّل تدخلًا محظورًا[١].

وحري بالذكر، أن الدول تُصنّف بعض المعلومات التي تملكها، باعتبارها جزءًا من أمنها القومي، كتلك المتعلقة برموز إطلاق الأسلحة النووية، وحيثما يتم فض سريَّة هذه المعلومات، فإن مصالح الدولة السيادية تتأثر سلبًا. وتوافقًا مع هذا النهج، قرَّر بعض أعضاء (*IGE*) أن التجسس السيبراني يُمثّل تدخلاً بالإكراه في شئون الدولة الضحية، إذا انتهك حقها السيادي في الحفاظ على سرية معلوماتها المتعلقة بإدارة شئون الحكم، مما يؤدي إلى إجبارها على اتخاذ قرارات لم تكن لتتخذها لولا فض سريَّة تلك المعلومات، ومن ذلك، الاطلاع على مداولات سرية لحكومة ما، بشأن أهدافها وسياساتها الخارجية، وفض سريتها ونشرها، مما يُجبر الحكومة على اتخاذ قرارات، لم تكن لتتخذها لولا فض سرية هذه المداولات[٢].

وتجدر الإشارة إلى أنه ينبغي التمييز بين أفعال التدخل، وبين بعض الممارسات مثل الإقناع، والنقد، والدبلوماسية، والتي هي أنشطة تنطوي فقط على محاولة التأثير دون إكراه، كقيام دولة بحملة إعلامية عبر الإنترنت لإقناع دولة أخرى للتصديق على معاهدة، أو نشر وزارة خارجية دولة ما، محتوى على وسائل التواصل الاجتماعي ينتقد سياسات دولة أخرى، فلا يُمكن اعتبار ذلك قسرًا، أو تدخلًا محظورًا، يُجبر الدولة المستهدفة على اتخاذ إجراء، أو الامتناع عنه[٣].

وقد اتفق أعضاء (*IGE*) على ضرورة توافر علاقة سببية بين فعل الإكراه، وانتهاك الشئون الداخلية أو الخارجية للدولة المستهدفة، كالحالة التي تتسلّل فيها دولة إلى النظم الالكترونية لسجلات استخبارات دولة أخرى، ثم تنشرها على موقع عام ومفتوح، لتُظهر عدم قدرة الحكومة على حماية أنظمتها الالكترونية، وبالتالي تخلق أزمة سياسية، على أمل أن تؤدي هذه الأزمة، إلى فرض قيود صارمة على الاستخبارات الوطنية، مما يُيسّر للدولة الأولي اقتراف التجسس[٤]. وكذلك في حالة حصول دولة على معلومات عسكرية سريَّة لدولة أخري، وعندما تتدهور العلاقات بين الدولتين، تقوم الأولى باستخدام هذه المعلومات، في دعم هجوم مادي مُسلَّح.

كما أورد دليل "تالين ١"، في القاعدة (١١) منه، و"تالين ٢" في القاعدة (٦٩) منه، أن العمليات السيبرانية التي يكون حجمها وأضرارها قابلة للمقارنة، مع عمليات استخدام القوة التقليدية، من حيث تَسَبُّبها في أضرار، لم يكن من الممكن أن تحدث في السابق، إلا باستخدام قوة عسكرية تقليدية؛ تُمثّل

(1) ***M. N. SCHMITT, L. VIHUL****, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, P. R., P. 321, 323.*
(2) ***W. C. BANKS****, Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage, 66 Emory Law Journal, 2017, PP. 513:520.*
(3) ***M. N. SCHMITT, L. VIHUL****, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, P. R., P. 319.*
(4) ***M. N. SCHMITT, L. VIHUL****, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, P. R., P. 320.*

استخدامًا للقوة، وتنتهك المادة (٤/٢) من ميثاق الأمم المتحدة، وبالتالي يُؤيّد الدليل اعتبار التجسس السيبراني تدخلاً غير مشروع في شئون الدول، على غرار عمليات استخدام القوة لإكراه دولة ما[١].

ومما سبق يمكننا القول بأنه:

(١) يواجه تطبيق مضمون مبدأ عدم التدخل، في سياق التجسس السيبراني، إشكاليات تتعلَّق بمدى توافر الإكراه، وقصد التأثير على قرارات وسياسات الدولة، وجميعها تصب في جانب عدم اعتباره تدخلاً، ونظرًا لخطورة هذا السلوك، فإن الأمر يتطلب إعادة النظر في مضمون المبدأ وفقًا لمنظور أوسع، بحيث يتم الربط بين فعل التدخل ومدى تأثر سيادة الدولة؛ فإذا كان من شأن الفعل أن ينتهك أو يؤثر على السيادة، فإنه يمثل تدخلاً غير مشروع، وعلى سبيل المثال، وبالتطبيق على التجسس السيبراني، فإنه في حالة الاطلاع على معلومات وطنية تتعلّق بالأمن القومي للدولة، يكون مجرد الوصول إلى هذا الحد انتهاكًا لسيادة الدولة وتدخلاً في شئونها.

(٢) يكون من الأفضل في مجال حماية الدول من العمليات السيبرانية، الابتعاد عن التركيز على قصد الطرف المهاجم، واعتبار أن أي إضرار بالمصالح الأساسية للدول، أو أي تأثير على سيادتها، بمثابة تدخل غير مشروع، دون النظر إلى القصد أو النية من العملية.

المطلب الثاني

مدي اعتبار التجسس السيبراني مُكافئًا للتدخل باستخدام القوة المسلحة

أوردت المادة (٤/٢) من ميثاق الأمم المتحدة حظرًا على استخدام القوة في العلاقات بين الدول أو التهديد باستخدامها، ولكنها لم تحصر، أو تُحدّد، أو تُعرّف الأفعال التي تُشكّل استخدامًا للقوة، وقد وجَّهت بعض أحكام الميثاق إلى نوع من السلوك يدخل بصفة أساسية ضمن نطاق هذا الحظر، وهو القيام بعمليات عسكرية مسلحة في دولة أخرى[٢]، وتكشف الأعمال التحضيرية الخاصة بصياغة المادة (٤/٢)، عن رفض اقتراح بإدخال الإكراه الاقتصادي ضمن نطاق استخدام القوة[٣]، كما رفضت لجنة الأمم المتحدة للعلاقات الودية اقتراحًا، باعتبار كافة أشكال الضغوط السياسية والاقتصادية ضمن نطاق المادة (٤/٢)[٤].

ووفقًا للمادة (١/٣١) من اتفاقية "فيينا" لقانون المعاهدات[٥]، تُفسّر نصوص الاتفاقيات وفقًا لمعنى صياغتها، وعلى ضوء السياق الخاص بموضوعها والغرض منها، وإذا كان الهدف الرئيس للأمم المتحدة، هو حفظ السلم والأمن الدوليين، ومنع استخدام القوة المسلحة أو التهديد باستخدامها، فإنه ينبغي

---

(1) ***Rule No. 69 of the Tallinn Manual 2: Definition of use of force:*** *A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force.*

(٢) **أوردت المادة (٤١) من الميثاق أمثلة للتدابير التي قد يتخذها مجلس الأمن، التي وُصفت بانها "لا تنطوي على استخدام القوة المسلحة"**، كوقف الصلات الاقتصادية، والمواصلات الحديدية، والبحرية، والجوية، والبريدية، والبرقية، واللاسلكية وغيرها من وسائل المواصلات، وقفًا جزئيًا أو كليًا، وقطع العلاقات الدبلوماسية".

(3) ***Doc. 2, 617 (e) (4),*** *3 UN CIO Docs. 251, 253–4 (1945).*

(4) ***UN GAOR Special Comm. on Friendly Relations****, UN Doc. A/AC.125/SR.110 to 114 (1970).*

(٥) **نصت المادة (١/٣١) على أنه:** "تفسر المعاهدة بحسن نية ووفقاً للمعنى الذي يعطى لألفاظها ضمن السياق الخاص بموضوعها والغرض منها".

أن يُفسّر مصطلح "القوة" الوارد في المادة (٤/٢) من ميثاق الأمم المتحدة، باعتباره لا يشمل سوى القوة المسلحة التي ينتج عن استخدامها أضرارًا مادية[١].

ويتوافق التفسير السابق مع ما قررته محكمة العدل الدولية في قضية "نيكاراجوا"، من رفض اعتبار التمويل الأمريكي لمقاتلي "*Contras*" استخدامًا غير مشروع للقوة بموجب المادة (٤/٢) من الميثاق، في حين يُمثّل تنظيم أو تشجيع تنظيم إرسال قوات غير نظامية، أو عصابات مسلحة، بغرض التوغل في أراضي دولة أخرى، أو المشاركة في حروبها الأهلية استخدامًا غير مشروع للقوة[٢].

وبالتطبيق على التجسس السيبراني، فإنه وبحسب الأصل لا يعتبر استخدامًا للقوة، حيث يقتصر على الحصول على معلومات سرية، دون التسبب في أضرار "مادية"، وحتى في حالة استخدام تلك المعلومات للتأثير سلبًا على معنويات مواطني دولة، كأن يتم دمج معلومات صحيحة مع أخري مغلوطة، لبث أخبار كاذبة بشأن تفشي مرض شديد العدوى، أو زعزعة ثقة المواطنين في أداء الحكومة، أو في تصنيف اقتصاد الدولة، فلا يمكن أن يكافئ هذا التجسس استخدام القوة، قياسًا على استبعاد الأعمال التحضيرية لميثاق الأمم المتحدة، للضغوط الاقتصادية والسياسية من نطاق استخدام القوة[٣].

ومن الممارسات الدولية التي تدعم هذا الفهم، أنه بعد نشر وثائق "*Snowden*"، وكشف تجسس الولايات المتحدة الأمريكية على بعض الدول والمنظمات الدولية كالاتحاد الأوربي، تم التعامل مع الأمر باعتباره قد يُؤثّر على الطبيعة الودية للعلاقات بين الدول، أو يُضعف الثقة في بعض الأنظمة الأمنية الوطنية، ولم تتطرَّق ردود أفعال الدول، لاعتباره قد يؤدي إلى أضرار تماثل ما قد ينتج عن استخدام القوة المادية، ومن ذلك، أنه يحق لدول الاتحاد الأوربي وفقًا للمادة (٢٢٢) من معاهدة إنشائه، التضامن عند وقوع هجوم خطير على دولة طرف، وهو ما لم يحدث في حالة التجسس المعروضة، مما يشير إلى أن الأمر لم يكن ـ بالنسبة للاتحاد ـ على درجة عالية من الخطورة لإعمال خيار التضامن[٤].

إلا أن هناك اتجاهًا أقرته محكمة العدل الدولية في قضية "نيكاراجوا" لعام ١٩٨٦، ويتعلَّق بإعمال معيار حجم العملية، أو نطاقها وآثارها، لتقييم ما إذا كانت تُكافئ استخدام القوة المُسلحة، حيث ميَّزت المحكمة بين نوعين من استخدام القوة؛ **الأول:** ما أطلقت عليه أشد أشكال استخدام القوة جسامة، ويُشكّل هجومًا مسلحًا، **والثاني:** تدابير استخدام القوة بصورة أقل خطورة، ولا تُشكَل هجومًا مسلحًا[٥]، ومن أمثلة الأفعال التي تكافئ الهجوم المُسلَّح؛ إرسال جماعات مسلحة غير نظامية أو مرتزقة، للقيام ضد دول أخرى بأعمال مسلحة، تصل درجة خطورتها إلى ـ من بين جملة أمور ـ حد الهجوم المسلح الذي قد تقوم به قوات مسلحة نظامية أو تشارك فيه، ومن أمثلة الأفعال التي لا تكافئ الهجوم المسلح، إرسال عصابات مسلحة إلى إقليم دولة، مع كون درجة خطورتها والآثار المُحتمل حدوثها ليست جسيمة[٦].

---

(1) ***R. BUCHAN**, Cyber Attacks, P. R., PP. 211: 212.*

(٢) **حكم محكمة العدل الدولية، قضية نيكاراجوا ١٩٨٦، المرجع السابق، الفقرات** (٢٠٥، ٢٢٨، ٢٤٢، ٢٤٥).

(3) ***M. N. SCHMITT,** The Tallinn Manual on the International Law Applicable to Cyber Warfare, New York, Cambridge University Press, 2013, PP. 47:49.*

(4) ***C. S. YOO**, Cyber Espionage or Cyberwar? International Law, Domestic Law, and Self-Protective Measures, in: J. D. OHLIN, K. GOVERN, C. FINKELSTEIN (eds), Cyberwar: Law and Ethics for Virtual Conflicts, Oxford University Press, Oxford, 2015, P. 179.*

(٥) **حكم محكمة العدل الدولية، قضية نيكاراجوا ١٩٨٦،** المرجع السابق، الفقرات (٥١، ٦٤)

(٦) **حكم محكمة العدل الدولية، قضية نيكاراجوا ١٩٨٦،** المرجع السابق، الفقرات (١٧٦، ١٩٤).

ويعني ذلك أن الهجوم المسلح يُعتبر فئة فرعية من استخدام القوة، وبينما تشكل جميع أشكال الهجوم المسلح استخدامًا للقوة، لا يُعتبر كل استخدام للقوة هجومًا مسلحًا، يُبرر للدولة الدفاع عن نفسها وفقًا للمادة (٥١) من الميثاق، وقد تُستهدف الدول بعمليات خطيرة تكافئ الاستخدام غير المشروع للقوة وفقًا للمادة (٤/٢) من الميثاق، ولكنها ليست جسيمة بما يكفي لأن ترقي إلى درجة الهجوم المسلح.

وإذا كان مفهوم القوة المسلحة ينصرف إلى استخدام سلاح لإلحاق أضرار مادية بدولة، وبما يشمل القتل أو تدمير الأشياء[١]، فيُمكن القول، بأن أي سلوك ينتج عنه ضررًا ماديًا كالقتل أو التدمير، يُشكّل استخدامًا للقوة بالمعنى المقصود في المادة (٤/٢) من الميثاق، حتى إذا كان هذا السلوك متمثلاً في وسائل الإنترنت[٢]، وبالنسبة للتجسس السيبراني، فإنه يتم تقدير الأضرار الناتجة عنه، وما إذا كانت قد أدت لوقوع وفيات، أو إصابات، أو تلف ممتلكات، وفي حالة تحقق ذلك، يُصنّف باعتباره يكافئ استخدام القوة.

وقد استند دليل "تالين" بإصداريه، على معيار النطاق والآثار، لتحديد العمليات السيبرانية التي تكافئ استخدام القوة المسلحة، وحدَّدت القاعدة رقم (١١) من "تالين ١"، والقاعدة رقم (٦٩) من "تالين ٢"، أن أي عملية سيبرانية تُشكّل استخدامًا للقوة، بالمعنى المقصود في المادة (٤/٢) من الميثاق، إذا كان حجمها وآثارها، قابلة للمقارنة مع الآثار الناتجة عن عمليات غير سيبرانية تستخدم القوة[٣]، وأكَّدت تعليقات (*IGE*) على هاتين القاعدتين، أن مُصطلح القوة المُسلَّحة، لا يتطلب بالضرورة استخدام "أسلحة"، وإنما العامل الحاسم في ذلك، أن تتم العملية على نطاق واسع، وأن يترتّب عليها أثارًا خطيرة تُماثل ما قد ينتج عن هجوم مسلَّح تقليدي[٤].

وترتيبًا على ما سبق، يُمكن أن يُشكّل التجسس السيبراني هجومًا مُسلَّحًا، إذا استهدف الحصول على معلومات، تُمهّد لغرض عسكري، ينتج عنه قتل أشخاص، أو إتلاف أو تدمير أشياء، أو اُستخدمت المعلومات التي وفَّرها، في تدمير أنظمة تشغيل محطات تنقية مياه الشُرب، وترتّب عليها حدوث أمراض خطيرة، أو وفيات نتيجة شرب المياه ملوثة. وذلك بخلاف معلومات التجسس التي قد تُستخدم في تعطيل مؤقت لبعض الخدمات أو الأنظمة الالكترونية لدولة، ولا تكافئ استخدام القوة، وربما تُماثل التدابير التي يتخذها مجلس الأمن بموجب المادة رقم (٤١) من ميثاق الأمم المتحدة، والموصوفة بأنها لا تنطوي على استخدام القوة المسلحة[٥].

كما قرَّرت القاعدة رقم (٦٨) من دليل "تالين ٢" أن العملية السيبرانية التي تشكل تهديدًا أو استخدامًا للقوة، ضد السلامة الإقليمية أو الاستقلال السياسي لأية دولة، أو التي تتعارض بأي طريقة

(1) ***Y. DINSTEIN**, War, Aggression and Self-Defence, P. R., P. 90.*
(2) ***M. ROSCINI**, Cyber Operations and the Use of Force in International Law, P. R., PP. 52:55.*
(3) ***Rule No. (69) of Tallinn Manual 2:** Definition of use of force: A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force.*
(4) ***M. N. SCHMITT, L. VIHUL**, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, P. R., PP. 334: 341.*
(5) ***C. S. YOO**, Cyber Espionage or Cyber War, P. R., PP. 8: 10.*

أخرى مع مقاصد الأمم المتحدة، تُعد غير مشروعة[١]، وأوضحت التعليقات على هذه القاعدة، أنه لا يلزم أن تقوم القوات المسلحة للدولة بالعملية، حتى تُعد مكافئة لاستخدام القوة، ولكن ينطبق هذا الوصف في حالة قيام وكالة استخبارات الدولة بها، أو حتى كيانات خاصة تابعة للدولة[٢].

وتطرق دليل "تالين ٢" إلى حق الدول في الدفاع عن نفسها، ضد العمليات السيبرانية المُكافئة للهجوم المسلح، وذلك في القاعدة رقم (٧١) منه، التي قضت بأنه يجوز للدولة التي تكون هدفًا لعملية إلكترونية تكافئ الهجوم المسلح، أن تمارس حقها الطبيعي في الدفاع عن النفس[٣]، واشترطت القاعدتين (٧٢، ٧٣) منه، لنشأة هذا الحق، توافر عناصر الضرورة والتناسب[٤]، وكون الهجوم وشيكًا أو فوريًا[٥].

وفي التعليقات الواردة على القاعدتين، اتفق أعضاء (*IGE*) بالنسبة لحالة الضرورة، أنه إذا كانت الدفاعات الالكترونية للدولة، كافية لإحباط العملية السيبرانية، فلا يجوز اللجوء إلى أي تدابير أخرى، إلكترونية أو مادية. أما معيار التناسب فإنه يتعلَّق بمقدار القوة المسموح باستخدامها، بحيث يُنظّم نطاق وشدة الاستجابة الدفاعية المُتطلبة للتعامل مع الهجوم، ويعتمد على وضع كل عملية، فقد تكون هناك حالات تستدعي استخدام مزيدًا من القوة، أو قد تكون القوة الأقل كافية للرد، كما لا يُشترط أن تكون القوة الدفاعية من نفس طبيعة القوة الهجومية، لذا، يمكن اللجوء إلى استخدام القوة السيبرانية رداً على هجوم مسلح حركي والعكس[٦].

واختلف أعضاء (*IGE*) حول ماهية كون الهجوم السيبراني "وشيكًا"، حيث فسرته الأغلبية بأحقية الدول في الدفاع الوقائي أو الاستباقي[٧]، على سند من أن المادة (٥١) من ميثاق الأمم المتحدة، وأن لم تكن قد نصت صراحةً على الدفاع تحسبًا لهجوم وشيك، إلا أن المنطق يقتضي ألا تظل الدولة مكتوفة الأيدي في هذه الحالة، وعليها أن تدافع عن نفسها، لاسيما مع طبيعة العمليات السيبرانية التي تتصف بالسرعة الفائقة، ولا يمكن أن تنتظر الدولة حتى تتم فعليًا وتتحقق أضرارها، في حين رأي بعض أعضاء (*IEG*) أن هذا التحليل الزمني الصارم لا يمكن ضبطه، وربما يُتخذ كذريعة لانتهاك القانون الدولي،

---

(1) ***Rule No. (68) Of Tallinn Manual 2:*** *Prohibition of threat or use of force: A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful.*

(2) ***M. N. SCHMITT, L. VIHUL****, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, P. R., P. 329.*

(3) ***Rule No. (71) of Tallinn Manual 2:*** *Self-defence against armed attack: A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence. Whether a cyber operation constitutes an armed attack depends on its scale and effects.*

(4) ***Rule No. (72) of Tallinn Manual 2:*** *Necessity and proportionality: A use of force involving cyber operations undertaken by a State in the exercise of its right of self-defence must be necessary and proportionate.*

(5) ***Rule No. (73) of Tallinn Manual 2:*** *Imminence and immediacy: the right to use force in self-defence arises if a cyber armed attack occurs or is imminent. It is further subject to a requirement of immediacy.*

(6) ***M. N. SCHMITT, L. VIHUL,*** *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, P. R., PP. 334: 349.*

(7) ***C. S. YOO****, Cyber Espionage or Cyberwar, P. R., PP. 188:194, 278: 288.*

ويمكن إعمال معيار آخر، هو أن يُمثّل الرد على هذا الهجوم "آخر فرصة ممكنة" لذلك، فيُسمح للدولة المُستهدفة بالدفاع عن نفسها، إذا كان عدم الرد يجعلها غير قادرة على الدفاع بفعالية بعد بدء الهجوم[١].

وقرر الدليل أن قيام كيانات بخلاف الدول، بعمليات أو هجمات الكترونية لصالح دولة أو بدعم منها، يمكن اعتباره هجومًا مسلحًا، وللدول حق الدفاع عن النفس ضد هذه الجهات، سواء داخل أقاليمها، أو داخل الدولة التي تنطلق منها الهجمات "الدولة الإقليمية"، إذا كانت الأخيرة غير قادرة، أو غير راغبة في وقف الهجمات التي تنطلق من إقليمها، وللدولة المُستهدفة أن تطلب من الدولة الإقليمية معالجة الوضع، وذلك بموجب الالتزام العرفي الخاص بعدم سماح الدول باستخدام أقاليمها للإضرار بدول أخرى، وبما يشمل بذل العناية الواجبة للسيطرة على الكيانات الخاصة ضمن ولايتها القضائية[٢]، ولا مجال لاعترض الدولة الإقليمية على الإجراءات الدفاعية التي قد تتخذها دولة ضحية، لأن هذه الإجراءات مشروعة وفقًا للالتزام المذكور.

ومن الممارسات الدولية الخاصة بالتجسس، والتي تم تبريرها على أساس حق الدفاع الاستباقي، واقعة إسقاط الطائرة "*U-2*" عام ١٩٦٠، حيث صرَّح الرئيس الأمريكي حينها "*Eisenhower*"، بأنه كانت هناك ضرورة مُلحة ـ حتى مع كونها غير مُستحبة ـ للانخراط في التجسس، الذي كان دفاعيًا دون أي نوايا عدوانية، ولضمان سلامة الولايات المتحدة و"العالم الحر" ضد أي هجمات مفاجئة[٣]. ونلاحظ منطق الرئيس الأمريكي في تبرير التجسس بأنه تم كدفاع عن مصالح دولته، دون أي نية عدوانية، وبما يُمكن فهمه، بأن عدم المشروعية تتعلَّق فقط بالتجسس العدائي، وهو منطق يوّفر ذريعة لاقتراف السلوك بادعاء حق الدفاع الوقائي.

ونستنبط من العرض السابق؛ أن التجسس السيبراني لا يمثل بطبيعته استخدامًا للقوة، ولكن وفقًا لمعيار محكمة العدل الدولية في قضية "نيكاراجوا"، إذا اتصف نطاق هذا السلوك بالاتساع، وكانت آثاره جسيمة، وتكافئ ما قد ينتج عن نزاع مسلح مادي، كإصابة أشخاص أو وفاتهم، أو تدمير ممتلكات، فيمكن أن يرقي لدرجة استخدام للقوة، ويكون للدول حق الدفاع عن نفسها في مواجهته.

المطلب الثالث

الاتجاه الخاص بعدم خضوع الفضاء السيبراني لسيادة الدول ومشروعية التجسس السيبراني

خلال مناقشة الجمعية العامة للأمم المتحدة، تقريرًا لفريق خبراء المعلومات والاتصالات بشأن أمن الدول، طُرحت إشكالية عدم إمكان تطبيق مبدأ السيادة على الفضاء السيبراني، وصعوبات تناوله

---

(1) ***Rule (26) of Tallinn Manual 2: Necessity:*** *A State may act pursuant to the plea of necessity in response to acts that present a grave and imminent peril, whether cyber in nature or not, to an essential interest when doing so is the sole means of safeguarding it.*

(2) ***O. A. HATHAWAY, R. CROOTOF, P. LEVITZ, H. NIX, A. NOWLAN, W. PERDUE, J. SPIEGEL****, The Law of Cyber-Attack, P. R., PP. 817, 829:830.*

(3) ***The United States, The Office of Public Services,*** *Bureau of Public Affairs, President's Statement of May 16, The Department of State Bulletin, XLII, No. 109 (Washington D.C. 6 June 1960), P. 905.*

بالتنظيم دوليًا[١]، مع الإشارة إلى عدم وجود حظر على جمع المعلومات أو المراقبة بالأقمار الصناعية، وفقًا لحكم المادة (٢) من معاهدة المبادئ المنظمة لأنشطة الدول في مجال استكشاف واستخدام الفضاء الخارجي لعام ١٩٦٧[٢].

ويقرّر جانب فقهي أن طبيعة الفضاء السيبراني تختلف عن المساحات التقليدية لأقاليم الدول، كالأرض والبحر والجو، والتي تخضع لمبدأ السيادة، من حيث إنه لا محل لسيادة أي جهة علي ذلك الفضاء، حتى إن الشركات الخاصة قد شاع استغلالها له، في تقديم خدمات الكترونية متنوعة، كالاهتداء للطرق والمسارات، وتوفير خرائط للطرق والأماكن "*Google Maps*"، وكذلك توفير صور حيَّة لأقاليم دول العالم، دون أن تعترض أي دولة بأن ذلك يمس سيادتها[٣].

وتاريخيًا، لم يسبق لأي دولة، أن ادَّعت بسط سيادتها على بيئة لا تُسيطر عليها، أو تمارس عليها وظائف حكومية بطبيعتها، وعلى سبيل المثال، لم تدَّع أي دولة أن الفضاء الخارجي يُمثّل جزءًا من إقليمها، أو تحاول تنظيمه بموجب تشريع وطني[٤]، وكذلك الحال بالنسبة للفضاء السيبراني، حيث لا يُتصور انتهاك سيادة دولة عندما تسعي دولة أخري، للحصول على معلومات منقولة أو متداولة خلاله، ووفقًا للقاضي "*Max Huber*" في قضية التحكيم "جزيرة بالماس"، فإن السيادة تتضمن الاستقلال بجزء من الكرة الأرضية، دون أي دولة أخري لممارسة وظائف الدولة[٥]، وبما يشمل حماية هذا الإقليم، من أي فعل قد يؤثر على ممارسة صلاحيات الدولة السيادية، كالتسلّل المادي إليه لغرض التجسس، وهذا التسلّل هو مناط الحُكم بانتهاك سيادة الدولة، ولا تتوافر مقوماته في حالة جمع معلومات من بيئة لا تخضع لسيادة الدولة[٦].

ويؤكد جانب فقهي على المعني السابق، من حيث إن التجسس السيبراني، لا يتطلب تواجدًا ماديًا على إقليم الدولة المُستهدفة، سواء على الأرض، أو في البحر، أو الجو، وإنما يتم من خلال بيئة افتراضية، لا يمكن أن تُطبق عليها أحكام وسائل التجسس التقليدية، لعدم وجود أي تسلّل مادي أو أفراد

---

(1) ***United Nations, General Assembly,*** *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: note by the Secretary-General, A/68/98 (24 June 2013), paras.19:20.*

(٢) **معاهدة المبادئ المنظمة لأنشطة الدول في مجال استكشاف واستخدام الفضاء الخارجي**، المرجع السابق، **المادة (٢).**

(3) ***S. KANUCK,*** *Sovereign Discourse on Cyber Conflict under International Law, Texas Law Review, No. 88, 2010, P. 1571.*

(4) ***M. N. SCHMITT****, Reaction: Cyberspace and International Law: the Penumberal Mist of Uncertainty, 126 HLR F., 2013, PP. 176: 176.*

(5) ***Islands of Palmas (Netherlands v US)*** *(1928) 2 RIAA 829, 838,* ***the provision is:*** *"Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State".*

(6) ***C. FORCESE****, Pragmatism and Principle: P. R., PP. 67, 80.*

غير مُرخص لهم على إقليم الدولة، أو في نطاق المناطق السيادية لها، أو علي متن سفن أو غواصات أو طائرات حكومية، وبالتالي لا يوجد ثمة انتهاك أو تعدٍ على إقليم الدولة[١].

وقد أقرَّت القاعدة رقم (١) من دليل "تالين ١"، بعنوان "السيادة"، حق الدولة في ممارسة السيطرة على بنيتها التحتية السيبرانية داخل إقليمها، والأنشطة ذات الصلة بها، وبذلك يكون الدليل قد اكتفي، بتقرير سيادة الدولة على ما هو موجود داخل إقليمها من بنية تحتية سيبرانية، ولم يتطرق إلى إشكالية السيادة على الفضاء السيبراني بوجه عام، ويؤيد ذلك، أن أعضاء (*IGE*) قد رفضوا بالإجماع وصف هذا الفضاء بأنه مشاع عالمي مُشترك، باعتبار أن جزءًا منه عبارة عن مكونات مادية، توجد داخل أقاليم دول، وتمارس الدول صلاحياتها السيادية عليها، وحتى الأنشطة السيبرانية التي قد تعبر حدوداً، أو تنطلق من المياه الدولية، أو المجال الجوي الدولي، أو الفضاء الخارجي، يعتمد تشغيلها على أفراد خاضعين لولاية الدول[٢].

ومن ثم، فقد اتجه أعضاء (*IEG*)، إلى ترجيح الاتجاه الخاص بعدم سيادة الدول على الجزء غير المادي أو الافتراضي لهذا الحيّز، مع خضوع الجزء المادي منه، والخاص بالبنية التحتية الالكترونية داخل أقاليم الدول لسيادة هذه الدول، واعتبار الاعتداء على هذه البينية بمثابة تدخل في شئون الدول التي توجد على أقاليمها، أما الجزء الافتراضي، فلم يتم التطرق إلى علاقته بالسيادة، أو اعتباره يخضع لسيادة دولة معينة، وهو ما يتوافق مع طبيعة الفضاء السيبراني وخصائصه المُميِزة.

المبحث الثاني

مدى إمكان تأهل ممارسة التجسس السيبراني وقت السلم كعرف دولي

على ضوء عدم وجود اتفاقية دولية تنظم التجسس السيبراني، فقد أثار البعض إشكالية مدى استيفاء هذا السلوك لركني العُرف الدولي، بالنظر إلى أنه قد ظهر منذ منتصف الخمسينيات، وممارسته كثير من الدول من خلال مؤسسات رسمية، أو بواسطة وكلاء عنها، مع اعتقادها بأهميته، لاعتبارات أمنها القومي ومبررات الدفاع عن نفسها، وهي مُتطلبات قبول القواعد العرفية، التي يُستخلص وجودها، عند التيقن من سير الدول على مقتضي سلوك معين باعتباره قاعدة ملزمة[٣]. كما كانت هناك بعض ممارسات التجسس السيبراني ذات صلة بالأمم المتحدة، كمُقترح إنشاء أمانة للتحليل الاستراتيجي للمنظمة، في عام ٢٠٠٠، واتخاذ مجلس الأمن قرارات بناءً على معلومات تم توفيرها من عمليات تجسس سيبراني.

ونظرًا لتكرار هذا السلوك في المجتمع الدولي، وكذلك إقرار الدول بأهميته، فإن التساؤل يثور عن مدى استيفائه لشرط الممارسة الدولية المقبولة، أو مدى اعتباره بمثابة عُرف دولي، ونحاول فيما يلي عرض بعض الممارسات الدولية الخاصة بالتجسس السيبراني وقت السلم، ثم التركيز على تحليلها،

---

(1) ***A. SCHWABACH****, Internet and the Law: Technology, Society, and Compromises, ABCCLIO, California, 2nd., edn., 2014, P. 57.*

(2) ***M. N. SCHMITT, L. VIHUL,*** *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, P. R., P. 12.*

(٣) **د/ على صادق أبو هيف**، القانون الدولي العام، الجزء الأول، منشأة المعارف، الإسكندرية، الطبعة الحادية عشر، ١٩٧٠، ص٢١، ٢٢.

للوقوف على مدى صلاحيتها لتكوين عُرف دولي، وذلك وفقًا لما ورد في المادة رقم (٣٨) من النظام الأساسي لمحكمة العدل الدولية، ونبدأ بدراسة ذلك من خلال المطلبين التاليين:

المطلب الأول: بعض ممارسات التجسس السيبراني وقت السلم على المستوى الدولي.

المطلب الثاني: تحليل مدى إمكان تأهل سلوك التجسس السيبراني وقت السلم كعرف دولي.

المطلب الأول

بعض ممارسات التجسس السيبراني على المستوى الدولي

تعددت ممارسات الدول للتجسس باستخدام تقنيات الكترونية، واختلفت وتباينت ردود فعل المجتمع الدولي عليها، وعلى الآثار التي ترتبت عليها، كما شهدت منظمة الأمم المتحدة سابقة تخص اتخاذ مجلس الأمن قرارات، بناءً على معلومات مُتَحصَّل عليها من التجسس، وعلى المستوى القضائي الدولي، تعلَّقت بعض أحكام التحكيم الدولية، بمنازعات ذات صلة بالتجسس السيبراني. ونوالي دراسة ذلك من خلال الفروع التالية.

الفرع الأول

ممارسة الدول للتجسس السيبراني

نبين من خلال هذا الفرع بعض ممارسات التجسس السيبراني التي قامت بها بعض الدول، ورد فعل المجتمع الدولي عليها، ثم نقوم بتحليها، وذلك على النحو التالي:

أولاً: وقائع التجسس بواسطة الطائرتين الأمريكيتين (*U-2*)، (*RB-47*) عام ١٩٦٠:

استرعت حادثة الطائرة الأمريكية (*U-2*) عام ١٩٦٠، الانتباه إلى وسائل التجسس التقنية المتطورة، حيث طوَّرت وكالة المخابرات الأمريكية، هذا الطراز من الطائرات، بحيث تكون له القدرة على الاضطلاع بمهام تجسس من خلال التصوير، وفي الفترة من عام ١٩٥٦ وحتى عام ١٩٦٠، وبقيادة الطيار "*Francis Gary Powers*"، حلَّقت هذه الطائرة فوق الأراضي السوفيتية بانتظام، وقامت بالتصوير وجمع معلومات عسكرية، وفي الأول من مايو عام ١٩٦٠، قام السوفييت بإسقاطها بينما كانت تُحلّق فوق إقليمهم، وأعلنوا مقتل قائدها[١].

وخلال فترة ممارسة (*U-2*) للتجسس، لم تنفك الحكومة الأمريكية ترفض وتدين عمليات التجسس، وتُندّد بمن يتورط فيها[٢]، وبعد إسقاط الطائرة، استمرت في إنكار طبيعة مهامها، وظلَّت متمسكة بأنها كانت تقوم بأعمال استطلاع مشروعة وفقًا للقانون الدولي، كرصد الطقس والتغيرات الجوية، وإذا كان هناك ثمة انتهاك للقواعد الدولية فإن الطيار ـ الذي أُذيع نبأ موته ـ يُسأل عنه بشكل

---

(1) ***Office of the Dir. of the Cent. Intelligence Agency***, *Memorandum for Brigadier Gen. Andrew J. Goodpaster, U-2 Overflight of the Soviet Bloc (Aug. 18, 1960) (declassified Aug. 17, 1999),* ***available at:*** *http://www.eisenhower.archives.gov/research/online_documents/u2_incident.html. 15/3/2020.*
(2) ***C. FORCESE***, *Spies Without Borders, P. R., P. 203.*

شخصي[١]، وهنا أفصح الروس عن أن الطيار على قيد الحياة، وأنه اعترف تفصيلاً بالغرض من رحلات الطائرة، وأرشد عن أماكن تخزين المعلومات فيها[٢]؛ فاضطرت الإدارة الأمريكية للاعتراف بأن رحلات الطائرة كانت ترصد الوضع العسكري السوفيتي[٣].

وحري بالذكر، أنه يُشار إلى هذه الحادثة، ورد الفعل الأمريكي عليها، كبداية لتطور مفاهيم الاستخبارات في العالم، باعتبارها السابقة الأولي في تاريخ العلاقات الدولية، التي يدافع فيها رئيس دولة عن ممارسة التجسس وقت السلم، ويقرر مسئوليته المطلقة عنها، حيث برَّر الرئيس الأمريكي "آيزنهاور" واقعة التجسس، بأنها ضرورة للدفاع عن أمن بلاده، وهي أمر شائع في المجتمع الدولي، وأنها لم تكن لغرض عدائي، وإنما للحفاظ على توازن القوى، ودعم السلم والأمن في دول العالم[٤]، ولاحقًا، صرَّح "آيزنهاور" بموافقته على مطالب السوفيت بوقف مثل هذه المهام الجوية، التي اعتبروها مُعادية ولا يمكن قبولها.

وعلى الجانب الآخر، احتَّج رئيس الاتحاد السوفيتي السابق آنذاك "*Khrushchev*" رسميًا على هذه الواقعة، باعتبارها انتهاك للمجال الجوي لدولته، بالمخالفة للالتزامات الدولية[٥]، وتقدَّم إلى مجلس الأمن الدولي بمشروع قرار، طالبًا إدانة ما وصفه بالأعمال العدوانية للقوات الجوية الأمريكية ضد بلاده، إلا أن مناقشات المجلس انتهت برفض المشروع السوفيتي[٦]، والموافقة على مشروع آخر، تقدمت به كل

---

(١) **يرجع إنكار الحكومة الأمريكية لطبيعة مهام الطائرة، إلي عدة أسباب،** منها أن المخابرات الأمريكية لم تكن على يقين بمدى معرفة السوفييت ببرنامج (*U-2*) السري، وفي حالة جهلهم به، ينبغي الإبقاء عليه سريًا، لأنه كان يُنفذ على دول أخري كالصين، وإذا تم كشفه، فإن ذلك سيستتبع اتهامات من دول أخرى لم تكن على علم به، ولا تدرك طبيعة الرحلات المماثلة فوق أراضيها. **راجع:**

***R. M. BISSEL**, Jr., Origins of the U-2, 36 AIR POWER HIST 16, 1989, P. 21.*

(٢) **قُدِّم الطيار "باورز" إلى المحاكمة العسكرية في المحكمة العليا للاتحاد السوفيتي السابق عام ١٩٦٠،** واعترف بأنه مذنب بالتجسس، وأدلي باعترافات تفصيلية عن مهام الطائرة، وأن هذا المشروع خاص بالمخابرات الأمريكية، وأن الطائرة مزودة بوسائل تدمير ذاتي في حالة كشفها، مع تلقيه تعليمات بالانتحار بإبرة سامة في حالة سقوطه داخل الإقليم السوفيتي، ولكنه فضل الاستسلام. وقد طالب المدعي العام بتخفيف العقوبة على "باورز"، لتعاونه مع السلطات السوفيتية واعترافاته التفصيلية، وتم الحكم عليه بالسجن عشر سنوات، وفي ١٠ فبراير من عام ١٩٦٢، أعيد "باورز" إلى الولايات المتحدة الأمريكية، في عملية تبادل مع الجاسوس السوفيتي "رودلف ايفانوفتش أبل"، الذي كان محكومًا عليه بالسجن لمدة ثلاثين عامًا، بتهمة التجسس على الولايات المتحدة . **راجع:**

***D. WISE, T. ROSS,** The U-2 affair, Random House Publisher, 1962, PP. 196: 217.*

(3) ***R. M. BISSEL**, Origins of the U-2, 36 AIR POWER HIST 16, 1989, P. 22.*

(٤) **عُقدت جلسات استماع في مجلس الشيوخ الأمريكي عام ١٩٦٠، لمناقشة اعتراف الرئيس الأمريكي بمسئوليته عن واقعة التجسس،** وتم استدعاء وزيرة الخارجية الأمريكية حينها " كريستيان هيرتر"، ووجَّه لها رئيس المجلس "ويليام فولبرايت" حديثه قائلاً: مع درايتك بالعلاقات الدولية والسوابق ذات الصلة بها، هل إعلان رئيس دولة لمسئوليته عن التجسس هو ممارسة معتادة وعرفية بين الدول؟ وردت الوزيرة: لا، فالممارسة العامة، هي إنكار أي مسئولية بهذا الشأن، وعقّب "فولبرايت": هل توجد أي سابقة في تاريخنا أو في تاريخ أي أمة متقدمة أعلن فيها رئيس دولة، مسئوليته الشخصية عن أنشطة تجسس؟ وردت الوزيرة: لا، لم أعلم أي واقعة بهذا الشأن، ثم سألها: هل تعتقدين أنه من الحكمة أن يتحمل رئيس دولة المسئولية أنشطة التجسس؟ وأجابت: لا أعتقد أن ذلك يحدث فرقًا كبيرًا، وأعتقد أنه في هذه الحالة، كان قول الحقيقة هو المسار الأفضل من التعمق في اختلاق الأعذار أو التنصل من المسئولية **راجع:**

***Hearings Before the Senate Committee on Foreign Relations, 86th Cong.,** 2d Sess. 26 (1960).*

(5) ***Q. WRIGHT**, Espionage and the Doctrine of Non-Intervention in Internal Affairs, P. R., P. 19.*

(٦) تم رفض المشروع من (٧) دول، وموافقة (٢)، وامتناع (٢) عن التصويت هما "تونس"، و"سيلان". **راجع:**

من "الأرجنتين"، و"أكوادور"، و"سيلان"، و"تونس"، يعتبر أن هذه الواقعة، قد تُعرِّض السلم والأمن الدوليين للخطر، ويدعو الحكومات المعنية إلى حلها بالوسائل السلمية، ويناشدها الامتناع عن استعمال القوة أو التهديد باستعمالها، وأن تحترم كل منها سيادة الأخرى ووحدة أراضيها واستقلالها السياسي[١].

وحري بالذكر، أن أعمال التجسس الأمريكية بالطائرات على الإقليم السوفيتي لم تتوقف، ففي الأول من يوليو لنفس العام ١٩٦٠، أعلن الاتحاد السوفيتي السابق أن طائرة أمريكية من طراز (*RB-47*)، انتهكت مجاله الجوي بغرض التجسس، وقامت مقاتلات سوفيتية باعتراضها، وطلبت منها الهبوط، إلا أنها رفضت وحاولت الهرب خارج الحدود السوفيتية، فتم إطلاق النيران عليها وإسقاطها في المياه الإقليمية السوفيتية، وقُبض على اثنين من ملاحيها، واعترافا بتبعيتهما لوحدات الجو الخاصة بالمخابرات العسكرية الأمريكية، وأن الطائرة كانت في مهمة تجسس. وقدَّم الاتحاد السوفيتي احتجاجًا إلى الولايات المتحدة الأمريكية، حذر فيه من استمرار هذه العمليات، التي ربما تؤدي إلى اندلاع حرب جديدة، تقع مسئوليتها علي الجانب الأمريكي وحده[٢].

وقد نفت الولايات المتحدة الأمريكية الواقعة كما أعلنها السوفييت، وقررت أن الطائرة كانت تبعد بما لا يقل عن (٣٠) ميل من السواحل السوفيتية، حين قامت طائرات سوفيتية باعتراضها، لإجبارها على دخول المجال الجوي السوفيتي، ولما فشلت أطلقت عليها النيران وأسقطتها في المياه الدولية، وكانت الطائرة تقوم بمهام ملاحظة كهرومغناطيسية فوق بحر "بارنت"، وقدَّمت الحكومة الأمريكية احتجاجًا للسوفييت بشأن إسقاط الطائرة وقتل أحد ملاحيها، وإلقاء القبض على اثنين آخرين، وطالبت بإطلاق سراحهما على الفور[٣].

وفي ١٣ يوليو ١٩٦٠ أرسل وزير الخارجية السوفيتي، برقية إلى السكرتير العام للأمم المتحدة، يطلب فيها انعقاد مجلس الأمن، لبحث الأعمال العدوانية الأمريكية ضد بلاده، والتي تشكل تهديدًا للسلام العالمي، رغم تعهد الرئيس "ايزنهاور" بوقف مثل هذه الأعمال[٤]، وتقدم السوفييت بمشروع قرار لإدانة الواقعة، وتقدمت الولايات المتحدة بمشروع قرار مضاد، طلبت بمقتضاه إحالة الواقعة إلى التحقيق، من خلال لجنة تتشكَّل من أمريكيين وسوفييت ودولة ثالثة يقبلها الطرفان، أو من خلال العرض على محكمة العدل الدولية، ولم يحصل أي من القرارين على الأغلبية اللازمة لإقراره، وفي ٢٥ يناير ١٩٦١، أعلن "جون كيندي" رئيس الولايات المتحدة الأمريكية، أن الاتحاد السابق قام بإطلاق سراح ملاحي الطائرة،

***U.N. Security Council**, Official Records, 15th year, (UN Doc S/4314, 19 May 1960, 157); **Union of Soviet Socialist Republics**, Draft Resolution Concerning Alleged Aggressive Acts by the United States Air Force Against the Soviet Union, UNSC Doc S/4321(23 May 1960, not adopted).*

(1) ***U.N. Security Council,** Official Records, 15th Year, 1960, Document S/4328.*

(2) ***Soviet Notes of July 11, 15,** Department of state Bulletin, Volume XL III, July 4-December 26, 1960, PP. 164, 210, 211.*

(3) ***U.S. Note of 18th July 1960**, Department of State Bulletin, August 8, 1960, pp. 209, 210; N**.Y. Times, July 13, 1960,** P.I, C. 8; January 26, 1961, p. 1, C. 3; March 4, 1961, P.1, C. 3.*

(4) ***U.N. Security Council**, Official Record, 15th year, 880th to 883rd Meetings (July 22-26, 1960), Docs. S/P. V 880-883 and Docs. S/4384; S/4385; **S/4406; S/4409/Rev.1.***

وأعاد "كيندي" التأكيد على تعهدات "ايزنهاور" بمنع تحليق طائرات تجسس أمريكية فوق الإقليم السوفيتي[١].

وكانت جمهورية مصر العربية قد تعرَّضت قرب نهاية عام ١٩٧٠، لعمليات تجسس من قبل طائرات (*U-2*) الأمريكية، حيث رصدتها أجهزة الرادار المصرية فوق "سيناء"، وتم استدعاء المشرف على شئون الرعايا الأمريكيين بالقاهرة، وطُلب منه إبلاغ الحكومة الأمريكية باعتراض القاهرة على هذه العمليات، وفي يوم ٢٥ نوفمبر ١٩٧٠، رد المُشرف بأن هذه الطائرات كانت تستطلع الأراضي المصرية، وقد توقفت منذ ١٠ نوفمبر ١٩٧٠، ولا توجد خطط لاستئناف مهامها مرة أخري. وفي ٤ ديسمبر ١٩٧٠، استدعت السلطات المصرية السفير الأمريكي، وسلَّمته مذكرة احتجاج رسمية على الرد الأمريكي، وأن الحكومة المصرية تعارض القيام بهذه العمليات، حتى فوق الأراضي المصرية المحتلة، وتعتبرها أعمالاً عدائية[٢].

ثانيًا: برنامج "*U.S. Corona*" لعام ١٩٦٠:

مع بدايةً عام ١٩٦٠، أطلقت الولايات المتحدة الأمريكية أول برنامج للأقمار الصناعية المُخصصة للتجسس، وعُرف باسم "كورونا" "*U.S. Corona*"، أو "نظام كيول" "*Keyhole system*"، وصُنِّف هذا المشروع رسمياً بأنه "سري"، ونُفّذ تحت غطاء كونه أحد برامج حماية القوات الجوية، وقُدرت مهام التجسس التي تمت بواسطته منذ عام ١٩٦٠، وحتى عام ١٩٧٢، بأكثر من خمسين مهمة، كانت جميعها ضد الاتحاد السوفيتي السابق، وبالفعل تم جمع كم هائل وقيِّم من المعلومات السرية بشأن القدرات النووية السوفيتية[٣].

وكان من بين أبرز ثمار تجسس "*Corona*"، أنه في سبتمبر عام ١٩٦١، وبعد خمس مهمات ناجحة، خفَّضت وكالة المخابرات المركزية الأمريكية، تقديرها لعدد الصواريخ النووية السوفيتية طويلة المدى، باعتبارها تتراوح بين (١٠) إلى (٢٥) صاروخ، بعد أن كان التقدير السابق لها بأنها تتراوح بين (١٤٠) إلى (٢٠٠)، وتبدّدت المخاوف الأمريكية بشأن وجود فجوة في التسلح بهذه الصواريخ بينها وبين السوفيت، الأمر الذي أدي لتجنب زيادة الإنفاق الأمريكي على التسلح النووي. كما مكَّن برنامج "*Corona*" الولايات المتحدة الأمريكية، من معرفة موعد إجراء أول تفجير نووي للصين عام ١٩٦٤، وذلك قبل شهرين من هذا الموعد، وساعد كذلك البرنامج الكيان الصهيوني في حربه ضد الدول العربية عام ١٩٦٧[٤].

---

(1) ***U.S.I.S, Off. Text**, January 26, 1961, P. 2.*

(٢) **ومما ورد في الاحتجاج**، أن مصر لم تمنح الولايات المتحدة الأمريكية موافقة على الاستطلاع الجوي، ومن المخالف للقانون الدولي أن تُعطي لنفسها الحق في ذلك، حيث تنطوي هذه العمليات على استطلاع وتجسس على مواقع عسكرية مصرية، وإبلاغ المعلومات إلى العدو الذي يحتل أراضيناً، ولا يمكننا تفهم قيام الولايات المتحدة بهذا الأمر، إلا كعمل عدائي يخدم أهداف العدو المُحتل. **راجع: د. على صادق عبد الحميد صادق**، أمن الدولة في النظام القانوني للهواء وللفضاء الخارجي، المرجع السابق، ص ١٣٦: ١٣٧.

(٣) **وفي الثاني والعشرين من شهر فبراير لعام ١٩٩٥**، تم رفع صفة السرية عن الصور التي التقطها هذا البرنامج، بموجب قرار من الرئيس السابق "بيل كلينتون". **راجع:**

***I. FISHER**, Reports of Secret U.S. Prisons in Europe Draw Ire and Otherwise Red Faces, N.Y. TIMES, Dec. 1, 2005, at A14.*

(4) ***United States Army,** Establishment of the US Army Cyber Command, (US Army Cyber Command), **available at:** http://www.arcyber.army.mil/history.html. 25/2/2020.*

وقد علَّق الرئيس الأمريكي حينها "*Lyndon Johnson*"، على ما حققه برنامج "*Corona*" بقوله، لقد أنفقنا ما يُقارب (٤٠) مليار دولار على برامج الاستطلاع من الفضاء، وإذا لم نحصل منها على شيء سوى المعلومات التي جمعناها، فإنها تستحق أكثر من (١٠) أضعاف هذه التكلفة، لأننا الآن نعلم عدد الصواريخ والقذائف التي يمتلكها العدو، وبالتالي حوَّلنا جهودنا إلى موضوعات أهم، بدلاً من الاستمرار في القيام بأشياء لا نحتاجها، والأهم أن مخاوفنا قد تبدَّدت بشأن تهديدات تبيَّن أنها لا تستحق[١].

وكرد فعل للاتحاد السوفييتي السابق على مهام هذا البرنامج، فقد أعلن رسميًا في ٢٤ أبريل ١٩٦٣، أمام اللجنة الفرعية القانونية للفضاء بالأمم المتحدة، أن هذه الأقمار قد أُستخدمت لجمع معلومات عن أنشطته، وبما يعني أن سيادته قد أُنتهكت وتم التدخل في إقليمه، وقرّر ممثل الاتحاد السابق لدى الأمم المتحدة: "أن المعلومات التي استهدفتها المراقبة غير المشروعة، تمثل أسرارًا تحت حراسة دولة ذات سيادة، وبغض النظر عن وسيلة الحصول عليها، فقد تم دون ترخيص، وبما يُشكّل انتهاكًا لسيادة الدولة[٢].

وردّت الولايات المتحدة الأمريكية، بأن الفضاء الخارجي لا يخضع لسيادة أي دولة أو سيطرتها، ولا يمكن أن تدعي دولة ذلك عليه، وأن من حق كل الدول أن تستغله باعتباره مشاعًا عالميًا[٣]، وتطورت المناقشات لتشمل مدى خضوع الفضاء الخارجي لسيادة الدول، إلا أنها لم تتطرق لمدي مشروعية سلوك التجسس في وقت السلم، بالرغم من أن رد فعل الاتحاد السوفيتي السابق كان واضحًا، من حيث اعتراضه على جمع معلومات سريّة في حيازته وعلى إقليمه وتخضع لحراسته.

ثالثًا: عملية التجسس السيبراني "*Titan Rain*" على الولايات المتحدة الأمريكية عام ٢٠٠٣:

خلال عام ٢٠٠٣، وجَّهت الولايات المتحدة الأمريكية اتهامًا للصين، بشن حملات تجسس سيبراني واسعة النطاق ضدها، عُرفت باسم "*Titan Rain*"، واستهدفت اختراق الأنظمة الالكترونية لبعض مؤسساتها، من بينها وكالة الأمن الوطني، ووزارة الدفاع، وبعض الشركات الخاصة الكبرى[٤]، وعلى الرغم من إنكار "الصين" لهذا الاتهام، إلا أن الولايات المتحدة أصرَّت على موقفها، وأكّدت على سرقة معلومات أمنية، وبراءات اختراع، وحقوق ملكية فكرية، لاسيما من شركات التكنولوجيا الفائقة،

---

(1) ***J. T. RICHELSON,*** *America's Secret Eyes in Space: the U.S. Keyhole Spy Satellite Program, New York, Harper & Row, 1975, P. 93.*

(2) ***U.N. Doc. No.*** *A/AC.105/C.2/SR.22/5 (1963);* ***Soviet statement in the United Nations First Committee,*** *quoted in Cooper, Current Developments in Space Law, IV SPACEFLIGHT, July 1963, PP. 134:136.*

(3) ***Summary Record of the Twentieth Meeting,*** *May 3, 1963, U.N. Doc. No. A/AC. 105/C.2/SR.28/13 (1963).*

(٤) **في تقرير للكونجرس بشأن الصين عام ٢٠١٣**، أكَّد تعرض عدد هائل من أنظمة الكمبيوتر في جميع أنحاء العالم للاختراق، من قبل وكلاء للحكومة الصينية، وذلك في إشارة إلى تورط الصين في هجوم "*Titan Rain*"، كما اطَّلع الكونجرس على تقارير لوزارة الدفاع الأميركية، تفيد أنها قد تعرَّضت لتجسس سيبراني، والتطفل على ما يقرب من ٢٤.٠٠٠ ملف الكتروني. **راجع:**

Cf. Office of the Secretary of Defense*, Military and Security Developments Involving the People's Republic of China, Annual Report to Congress, (US Department of Defense 2011),* ***available at:*** *http://www.defense.gov/pubs/pdfs/2011_cmpr_final.pdf. 18/3/2020.*

وذلك بواسطة قراصنة وطنيين تستخدمهم الصين، ثم تمنح تلك المعلومات لشركات صينية مملوكة للدولة، أو لها علاقة وثيقة بها[١].

ونلاحظ أن الولايات المتحدة قد أعلنت عن هجمات "*Titan Rain*" السيبرانية، في صورة اتهام للحكومة الصينية، ولم تتعرض لتفاصيل أكثر من ذلك، بشأن سلوك التجسس نفسه، أو مدى توافقه مع القانون الدولي، وعلى الجانب الآخر لم تُصدر "الصين" أي تصريحات أخري بخلاف إنكار الاتهام.

رابعًا: التجسس السيبراني "*Ghost Net*" على كندا خلال عام ٢٠٠٩:

خلال عام ٢٠٠٩، اشتبهت السلطات الكندية، في تعرض بعض أجهزة الحاسبات لدى كبريات شركاتها الوطنية، لتجسس سيبراني، وأُطلق على هذه العملية "*Ghost Net*"، حيث كشفت التحقيقات التي أُجرتها "دائرة مراقبة حروب المعلومات" "*Information Warfare Monitor*"، عن تعرض عدد كبير من تلك الحاسبات للتجسس، بواسطة برنامج الكتروني أُطلق عليه "*Trojan*" "طروادة"، كانت له القدرة على التحكم الكامل في النظم التي يخترقها، وأن بعض القرائن تشير إلى تورط عناصر من الحكومة الصينية، ولكن لا توجد أدلة كافية على ذلك، وصرَّحت وزارة الخارجية الكندية في بيان رسمي، أنها تستنكر هذا السلوك[٢].

خامسًا: عملية التجسس "أوروا" "*Aurora*" على شركة "*Google*" الأمريكية عام ٢٠١٠:

في الثاني عشر من يناير عام ٢٠١٠، أعلن "*David Drummond*" نائب رئيس شركة "جوجل" الأمريكية، أن الشركة قد تعرضت لاختراق سيبراني مصدره "الصين، واستهدف بنية الشركة الالكترونية، وأسفر عن سرقة كم هائل من بيانات الملكية الفكرية لمشروعات الشركة، واخترق أنظمة معلومات ما يزيد عن عشرين شركة تعمل مع "جوجل"، وذلك في مجالات، الانترنت، والتمويل، والتكنولوجيا، والإعلام، والقطاعات الكيمائية[٣]. وأشار "*Drummond*" إلى وجود أدلة تُشير إلى أن هدف المُهاجمين، هو الوصول إلى حسابات بريد إلكتروني لناشطين صينيين في مجال حقوق الإنسان، وذلك على موقع "*Gmail*" التابع للشركة[٤].

---

(1) ***S. ELEGANT***, *Cyberwarfare: The Issue China Won't Touch, Time Magazine, (New York City 18 Nov 2009),* ***available at:*** *http://content.time.com/time/world/article/0,8599,1940009,00.html. 4/4/2019.*

(2) ***G. KERSCHISCHNIG***, *Cyberthreats and International Law, 1st. edn., Eleven International Publishing, The Netherlands, 2012, P. 68.*

(3) ***D. DRUMMOND***, *a new approach to China, Google: Official Blog (Jan. 12, 2010),* ***available at:*** *http://googleblog.blogspot.com/2010/01/new-approach-to-china.html. 11/5/2020.*

(٤) **لم يقم دليل قاطع على اتهام الحكومة الصينية**، وذكر تقرير قُدّمته شركة (*Northrop Grumman Corp*) إلى لجنة المراجعة الاقتصادية والأمنية الأمريكية الصينية، أن: "الأدلة التي تربط بين الصين والواقعة مقنعة، لكنها غير مباشرة، وقد ردَّ تحليل الفيروسات المستخدمة في الاختراق، عنصرًا واحدًا منها إلى الصين، إلا أن ما دعم الاتهام، هو استهداف العملية لحسابات بريد الكتروني لصينيين، مما يوحي بوجود دافع سياسي، كما نسبت عناوين الانترنت (*IP*)، التي انطلقت منها الهجمات إلي جامعة حكومية صينية. **راجع:**

Mcafee Labs and Mcafee Foundstone Professional Services, *Protecting Your Critical Assets: Lessons Learned From "Operation Aurora",* ***available at:***

وقد اتسم رد الفعل الأمريكي على الواقعة بعدم التحديد، حيث بدأ باحتجاج وزارة الخارجية، في ١٢ يناير عام ٢٠١٠ على سلوك "الصين"، باعتباره يثير تساؤلات خطيرة، تتطلع الحكومة الأمريكية للحصول على تفسير بشأنها، وفي اليوم التالي، تراجع مساعد وزيرة الخارجية وقتها " *Phillip Crowley*"، عما سبق وأبدته الوزارة من احتجاج، وصرَّح بأن الحكومة تتشاور مع "الصين" بشأن هذه الواقعة وغيرها من مجموعة قضايا أخري[١].

وفي ١٤ يناير ٢٠١٠، تغيرت صيغة التعبير عن الحادثة مرة أخري، حينما صرَّح "*Crowley*" بأن هذا الاختراق مسألة خطيرة، وأن الحكومة الأمريكية تلتزم بمعايير دولية، وتتوقع من شركائها أن يرتقوا إليها، وقد تم الدخول في محادثات واسعة مع "الصين" لمناقشة المخاوف الجدية بشأن الواقعة والتداعيات المرتبطة بها. وفي ١٥ يناير ٢٠١٠، وخلال مؤتمر صحفي، صرَّح "كراولي" أن الحكومة الأمريكية ستُصدر خلال أيام، مذكرة احتجاج بشأن الواقعة، تُعرب فيها عن قلقها، وتطلب من الحكومة الصينية تفسيرًا بشأنها[٢].

وفي ١٩ يناير ٢٠١٠، سُئل "*Crowley*" عما إذا كانت الوزارة قد أصدرت مذكرة الاحتجاج[٣]، فرد بأننا تأخذ الموضوع على محمل الجد، وقد عقدنا عدة اجتماعات مع ممثلين صينين للاستفسار. وهو تغير آخر في موقف الوزارة، من حيث الاستعاضة عن الاحتجاج بطلب تفسير. **وفي ٢١ يناير ٢٠١٠**، وفي معرِض حديثها عن موضوع حرية الإنترنت، علَّقت وزيرة الخارجية الأمريكية حينها "كلينتون" على الواقعة، بأنها تتطلع لأن تُجري السلطات الصينية تحقيقًا شاملاً بشأنها، وتأمل أن تتصف نتائجه بالشفافية[٤].

وفي ٢٢ يناير ٢٠١٠، صرَّح "*Crowley*" بأن مذكرة الاحتجاج لم تُقدَّم بعد، وفي ١٩ فبراير ٢٠١٠، وردًا على سؤال بشأن الواقعة، صرَّح بأن الوزارة أجرت محادثات مع الصين، منها لقاءات مباشرة في "لندن" بين وزيري خارجية الدولتين، وبدا أن الصينيين يدركون أهمية تلك المسألة لنا، وقد دعوناهم لإجراء تحقيق شامل بشأن الواقعة، فعقَّب صاحب السؤال، بأنه كان يعني التصريح السابق بالاحتجاج رسميًا، وهل هناك تغيير في تقييم الوضع؟ ورد "*Crowley*" بأن مذكرة الاحتجاج يمكن أن تكون بيانًا مكتوبًا، أو بيانًا شفهيًا، وقد ناقشت وزيرة الخارجية نظيرها الصيني في هذه المسألة، فإذا كنت

---

http://www.mcafee.com/us/resources/whitepapers/wp-protecting-critical-assets.pdf.27/3/2020.

(1) ***P. J. CROWLEY,*** *Assistant Secretary of State, Daily Press Briefing, Washington, DC (Jan. 13, 2010),* ***available at:*** *http://www.state.gov/r/pa/prs/dpb/2010/01/135142.htm. 29/3/2019.*

(2) ***P. J. CROWLEY****, Assistant Secretary of State, Special Briefing, Washington, DC (Jan. 15, 2010),* ***available at:*** *http://www.state.gov/r/pa/prs/ps/2010/01/135249.htm. 29/3/2019.*

(3) ***K. M. CAMPBELL****, Assistant Secretary of State, Bureau of East Asian and Pacific Affairs, Special Briefing: Briefing on the 50th Anniversary of U.S.-Japan Alliance, Washington, DC (Jan. 19, 2010),* ***available at:*** *http://www.state.gov/p/eap/rls/rm/2010/01/135400.htm. 29/3/2019.*

(4) ***H. R. CLINTON****, Secretary of State, Remarks at the Newseum, Washington, DC: Remarks on Internet Freedom (Jan. 21, 2010), http://www.state.gov/secretary/rm/2010/01/135519.htm. 2/4/2019.*

ترغب في أن تسمي ذلك احتجاجًا، فأعتقد أننا فعلنا ما يتوجب علينا فعله، وهو التعبير عن قلقنا من الهجوم علي أعلي مستوى، وطلب التحقيق فيه بشفافية[١].

وفي ١٩ مارس ٢٠١٠، سُئلت "كلينتون"، ما هي نتيجة تحقيق الصين بشأن واقعة "جوجل"؟ وأي نوع من الضغوط تمارسونه للحصول على تفسيرات؟ فأجابت، نحن نعتقد أن الأمر كله يتعلق بشركة "جوجل" و"الصين"[٢]. وعلي المستوي النيابي الأمريكي، كان للكونجرس رد فعل صريح على هذا الهجوم، حيث أصدر بالإجماع، قراره رقم (٤٠٥) في ٢ فبراير ٢٠١٠، وأدان فيه العمليات السيبرانية غير المشروعة التي يُدَّعي أنها أُطلقت من الصين ضد شركة "جوجل" وغيرها من الشركات، ودعا حكومة الصين إلي التحقيق فيها[٣].

أما فيما يتعلق برد الفعل الرسمي لحكومة الصين على الاتهامات الموجهة إليها؛ فقد أوضح المتحدث باسم وزارة خارجيتها، أن سياسة الصين إزاء احترام الدول الأخرى ثابتة، سواء على أرض الواقع، أم بشأن المعاملات على شبكة الانترنت، وتُراعي الصين الأعراف والتقاليد الثقافية الوطنية لها، والتي منها تنظيم شبكة الانترنت بتشريعات تتوافق تمامًا مع الممارسات الدولية، وتُجرّم القرصنة بكل أشكالها وتَعُدَّها انتهاكًا للقانون، ونظرًا لاستهداف الصين باقتحامات وقرصنة الكترونية بشكل مستمر، فإنها تدعو المجتمع الدولي لأن يُكثف جهوده للتعاون في مجال مكافحة قرصنة الانترنت، وأمن الانترنت وحماية خصوصية الأفراد والدول[٤].

ونلاحظ أن رد حكومة "الصين" يتمحور حول نفي مسئوليتها عن واقعة التجسس السيبراني، أو ضلوعها بأي دور فيها، بل وإدانتها لهذا السلوك، ولم تتذرَّع بأن هذا الفعل مشروع دوليًا أو أن التجسس السيبراني ممارسة مُستقر عليها في المجتمع الدولي، بل إنها طالبت بتكثيف التعاون الدولي لمكافحة مثل هذه الممارسات، وبعبارة أخري، نستطيع أن نري رفض صريح لسلوك التجسس السيبراني بشأن الواقعة المعروضة.

سادسًا: التجسس الأمريكي على هاتف المستشار الألمانية "*Merkel*" عام ٢٠١٣:

تضمَّن كشف "*Edward Snowden*" بشأن التجسس السيبراني لوكالة "*NSA*" في يونيو من عام ٢٠١٣، أن عمليات الوكالة قد شملت اتصالات المستشارة الألمانية "أنجيلا ميركل"، ولم يكن الأمر مقبولاً من جانب السلطات الألمانية، التي فتحت تحقيقًا بهذا الشأن، كما قرَّرت "ميركل" أنها ترى مثل

---

(1) ***P. J. CROWLEY****, Assistant Secretary of State, Daily Press Briefing, Washington, DC (Feb. 19, 2010),* ***available at:*** *http://www.state.gov/r/pa/prs/dpb/2010/02/136983.htm. 2/4/2019.*

(2) ***H. R. CLINTON****, Secretary of State, Interview With Indira Lakshmanan of Bloomberg TV, Moscow, Russia, (March 19, 2010),* ***available at:*** *http://www.state.gov/secretary/rm/2010/03/138677.htm. 2/4/2019.*

(3) ***S. Res. 405, 111th Cong. 2Feb. 2010; Congressional Record Volume 156,*** *Number 17 (Thursday, February 4, 2010), Pages S472-S473.* ***available at:*** *http://www.gpo.gov/fdsys/pkg/CREC-2010-02-04/html/CREC-2010-02-04-pt1-PgS472-2.htm. 2/4/2019.*

(4) ***M. ZHAOXU,*** *Foreign Ministry Spokesperson, Remarks on China-related Speech by US Secretary of State on "Internet Freedom" (Jan. 1, 2010),* ***available at:*** *http://www.fmprc.gov.cn/eng/xwfw/s2510/2535/t653351.shtml. 6/4/2019.*

هذه الممارسات غير مقبولة، وتطالب الإدارة الأمريكية بتوضيح، ثم أوضح المتحدث باسم البيت الأبيض، أن الرئيس "أوباما" قد أبلغ "ميركل" بأن بلاده لم ولن يحدث أن تجسست على اتصالاتها[١].

سابعًا: تجسس "استراليا" على "تيمور الشرقية عام ٢٠١٣:

بعد تاريخ طويل من النزاع على الحدود البحرية بين دولتي "استراليا"، و"تيمور الشرقية"[٢]، قام الطرفان عام ٢٠٠٢، بإبرام معاهدة لتنظيم ترتيبات بحرية في بحر تيمور (*Treaty with the Government of the Democratic Republic of Timor-Leste on Certain Maritime Arrangements in the Timor Sea* (*CMATS*)، وفي عام ٢٠١٣، لجأت دولة "تيمور" إلى محكمة التحكيم الدائمة (*PCA*)، مطالبة ببطلان تلك الاتفاقية، نظرًا لحصول "استراليا" على معلومات سرية بطريق التجسس، أدت لتعزيز موقفها في التفاوض، وحصولها على ميزات غير عادلة، حيث قام عملاء من الاستخبارات الأسترالية ـ بعد تنكرهم كموظفين في شركة إنشاءات استرالية تعمل في "تيمور" ـ بتركيب أجهزة تنصت في غرفة اجتماعات مجلس وزراء "تيمور"، وكذلك في مكتب رئيس الوزراء في "ديلي"، وتم رصد مناقشات تتعلق بموقف "تيمور" من المفاوضات، وبناء على هذه المعلومات، حقَّقت "استراليا" ميزات غير عادلة فيما يخص حقوقها المقررة في المعاهدة[٣].

وإذا كانت الممارسة الدولية قد جرت على أن الدول، عادةً ما تُسارع الدول إلى إنكار التجسس والتبرؤ منه، إلا أن "استراليا" دفعت في أحد مراحل التحكيم بأن الدول تتجسس على بعضها، وهو أمر جائز وفقًا للعرف الدولي، ثم توقف هذا الدفع عند حد القول به، ولم تُقدّم "استراليا" أي إثبات له، وهو بالفعل أمر صعب الإثبات، فالدول لا تقبل هذا السلوك أو تتسامح بشأنه عند التعرض له، بل إنها تحتج بقوة وبشكل فوري بمجرد علمها بحدوثه ضدها، وإذا كان الجاسوس دبلوماسيًا فيكون الطرد هو الجزاء[٤]، كما تُجَرّم غالبية تشريعات الدول التجسس وسرقة أسرار الدول، والقول بمشروعية التجسس يعني أن هذه القوانين الوطنية، تعتبر انتهاكًا لقاعدة دولية تسمح بالتجسس وهو أمر غير منطقي[٥].

---

(1) ***J. APPELBAUM, H STARK, M ROSENBACH, J. SCHINDLER***, *Berlin Complains: Did US Tap Chancellor Merkel's Mobile Phone?' Der Spiegel International (23 October 2013),* ***available at:*** *http://www.spiegel.de/international/world/merkel-calls-obama-over-suspicions-us-tapped-hermobile- phone-a-929642.html. 18/4/2019.*

(٢) **بعد احتلال إندونيسيا لتيمور عام ١٩٧٥**، أصرت على إعادة تعيين حدود الجرف القاري "لأستراليا"، والذي يتداخل مع حدود "تيمور"، وفي عام ١٩٨٩ وقعت"أستراليا" و"إندونيسيا" معاهدة "ثغرة تيمور"، بشأن تقسيم موارد المنطقة، إلا أن المعاهدة وُصمت بعدم المشروعية، لأن "إندونيسيا" كانت مُحتلة لتيمور، وفي عام ٢٠٠٢، وبعد حصول "تيمور" على استقلالها، أبرمت الدولتان معاهدة "بحر تيمور"، وتم تخصيص احتياطات نفطية بنحو ٧٩.٩% لاستراليا و٢٠.١%.
راجع:
G. TRIGGS, *Creative Conflict Resolution: The Timor Sea Treaty Between Australia and East Timor, in M. Langton, M. Tehan, L. Palmer & K. Shain, eds., Honour Among Nations? Treaties and Agreements with Indigenous People (2004), chap. 19.*

(3) ***C. SCHOFIELD***, *Minding the Gap: The Australia–East Timor Treaty on Certain Maritime Arrangements in the Timor Sea (CMATS), 22 Int'l J. Marine & Coastal L., 2007, PP. 189:190.*

(4) ***G. L. WHITE, P. SONNE, S. GORMAN***, *Russia Expels American on Spy Allegations, Wall Street Journal, May 14, 2013.*

(5) ***Q. WRIGHT***, *Espionage and the Doctrine of Non-Intervention in Internal Affairs, P. R., PP. 12:13.*

ونلاحظ أنه، بالرغم من أن "استراليا قد أثارت مسألة اعتبارها أن التجسس يُعتبر من قبيل العرف الدولي، فإنها لم تُقدَّم أي دليل علي ذلك، كما أن المحكمة لم تتعرض لمناقشة جوانب هذه الإشكالية، وتجنبت الخوض في أي من تفصيلات بشأن الحكم على هذا السلوك.

ثامنًا: الكشف عن وثائق "إدوارد سنودن" عام ٢٠١٣:

كشفت الوثائق التي أظهرها "*Snowden*" عام ٢٠١٣، من أن وكالة (*NSA*) قد استمرت في القيام التجسس السيبراني، على بعض الدول والمنظمات الدولية، لاسيما الأمم المتحدة، والاتحاد الأوروبي، والوكالة الدولية للطاقة الذرية، كما شملت رصد والاطلاع على الرسائل الالكترونية للأمين العام للأمم المتحدة، وتم تحديد (٣٨) بعثة دبلوماسية ومركزًا قنصليًا، داخل الإقليم الأمريكي باعتبارها أهدافًا للتجسس، باعتبارها ـ وفقًا للوثائق ـ أماكن تُنذر بالخطر، ومنها بينها دول في الشرق الأوسط، ودول أوربية مثل "فرنسا"، و"اليونان"، و"إيطاليا"، وعلى الجانب الآخر، استخدمت الولايات المتحدة الأمريكية بعثاتها الدبلوماسية، ومراكزها القنصلية للحصول على معلومات سرية تخص الدول الموفدين لديها[1].

وبالإضافة إلى الدول والمنظمات الدولية، استهدف التجسس جمع معلومات تخص أفرادًا في جميع أنحاء العالم، من المُشتبه في تورطهم في أنشطة ذات صلة بالإرهاب، أو مؤسسات إجرامية تعمل في مجال الاتجار بالمخدرات والبشر، وكانت طرق المراقبة السيبرانية التي تستخدمها الوكالة واسعة الانتشار، لدرجة أنها جمعت معلومات سرية تخص غير المشتبه بهم[2].

وتجدر الإشارة، إلى أن كثير من الدول قد صرَّحت بعدم قبولها لهذا التجسس، مثل "ألمانيا"، و"البرازيل"، و"الصين"، و"فرنسا"، واعتبرته يتنافي مع العلاقات الودية بين الدول، ويُمثّل تدخلاً في شئون الدول، كما أعلنت بعض المنظمات الدولية لاسيما الإنسانية، إدانتها لهذه العمليات. وعلى الجانب الآخر حاولت الإدارة الأمريكية إبان فترة رئاسة "أوباما" الدفاع عن سلوك الوكالة، فقامت بتبريره على سند من أنه كان ضروريًا للحفاظ على الأمن القومي للدولة، ولم تتطرَّق إلى تبريره باعتباره مسموحًا به أو مشروعًا بموجب القانون الدولي.

تاسعًا: اختراق الأنظمة الالكترونية لشركة "*Sony*" اليابانية بالولايات المتحدة عام ٢٠١٤:

في ٢٤ نوفمبر من عام ٢٠١٤، تم اختراق الأنظمة الالكترونية لفرع شركة "*Sony*" بالولايات المتحدة، وذلك قبل أيام من استعداد الشركة لتسويق فيلم بعنوان "المقابلة" "*The Interview*"، والذي يُجسّد قصة تتعلق باغتيال زعيم كوريا الشمالية، حيث أدخلت برمجيات خبيثة على أجهزة الشركة، لنسخ المعلومات المُحَمّلة عليها، ولاحقًا قام المهاجم بنشر بعضًا منها على شبكة الإنترنت، بما في ذلك أجزاء

(1) ***Embassy Espionage:*** *The NSA's Secret Spy Hub in Berlin, 27 October 2013, Spiegel,* ***available at:*** *www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy- a-930205.html.15/3/2020.*
(2) ***J. S. GRANICK****, American Spies: Modern Surveillance, Why Should You Care, and What To Do About It, Cambridge University Press, Cambridge, 2017, P. 24.*

من الفيلم، ورسائل بريد الكتروني متبادلة بين الشركة وموظفيها، كما تم سرقة مشروعات الأفلام القادمة[١].

وقد أُجريت تحقيقات فيدرالية أمريكية في الواقعة، وانتهت إلى أن الشركة قد تعرضت لهجوم سيبراني مصدره كوريا الشمالية، كما صرَّح الرئيس الأمريكي بأن بلاده سترد بشكل يتناسب مع الهجوم، ولكن في الوقت وبالطريقة التي تختارها، وفي الثاني من يناير عام ٢٠١٥ تم فرض عقوبات اقتصادية على كوريا الشمالية، منها تجميد أصولها المالية على الإقليم الأمريكي. وعلى الجانب الآخر، نفت "كوريا الشمالية" صلتها بالواقعة، لكنها أشادت بجماعة "حراس السلام" التي أعلنت مسئوليتها عن الهجوم، باعتبار أنهم قد "قاموا بعمل صالح"[٢].

الفرع الثاني

ممارسات تجسس سيبراني ذات صلة بمنظمة الأمم المتحدة

أولاً: مُقترح إنشاء أمانة للتحليل الاستراتيجي للأمم المتحدة في عام ٢٠٠٠:

طُرحت في عام ٢٠٠٠ مقترحات لتطوير القدرات التحليلية للأمم المتحدة، وذلك بإنشاء أمانة للتحليل الاستراتيجي "*Analysis Secretariat Strategic*"، على أن تُشكَّل من أعضاء مركز إدارة عمليات حفظ السلام، ووحدات تخطيط سياسات المنظمة، ومُحَلِّلين عسكريين[٣]، ومنذ أن بدأ تداول هذا المقترح، أبدت عدة دول تخوفها، لأنه بدا وكأن الأمم المتحدة بصدد إنشاء وكالة مخابرات خاصة بها، أو أنها ستبدأ في ممارسة التجسس، ولغرض توضيح الأمر، صرَّح الأمين العام للمنظمة بأن المجتمع الدولي يحتاج إلى وجود إنذار مبكر بشأن التهديدات، ولا ينبغي الخلط بين مقترح إنشاء أمانة للتحليل، وبين عمليات التجسس، فالمقترح لا يعدو كونه وسيلة لضمان استخدام المعلومات الموجودة بالفعل بصورة أكثر فعالية، وبالرغم من هذه الإيضاحات إلا أنه تم قد تم طرح هذا الاقتراح جانبًا في نفس العام[٤].

ثانيًا: اتخاذ مجلس الأمن قرارات بناءً على معلومات من عمليات تجسس سيبراني:

في سابقة ليست مُعتادة بالنسبة لمنظمة الأمم المتحدة، اعتمد مجلس الأمن على معلومات استخباراتية، عند "مناقشة"، أو "اتخاذ" قرارات في مجالين مهمين، **الأول:** مكافحة الإرهاب، **والثاني؛** عند مناقشة القيام بأعمال قمع وفقًا للفصل السابع من الميثاق. ويرجع تاريخ السابقة الأولي إلى عام ١٩٩٧، عندما أصدر المجلس بعض القرارات الخاصة بضرورة تعاون الدول، بشأن توفير معلومات عن عمليات وتحركات الإرهابيين والكيانات الإرهابية، وإعداد قوائم للمُشتبه بتورطهم في هذه الأعمال، أو

---

(1) ***The Interview:*** *A Guide to the Cyber Attack on Hollywood,' BBC News, December 29, 2014,* ***available at****: http://www.bbc.co.uk/news/entertainment-arts-30512032. 21/3/2020.*

(2) ***D. ROBERTS****, "OBAMA" Imposes New Sanctions against North Korea in Response to Sony Hack, the Guardian, January 2, 2015,* ***available at:*** *http://www.theguardian.com/us-news/2015/jan/02/obama-imposes-sanctions-north-korea-sony-hack-the-interview.21/3/2020.*

(٣) **طُرح هذا الاقتراح من قبل اللجنة التنفيذية للسلام والأمن بالأمم المتحدة،** التي تأسست في عام ١٩٩٧، باعتبارها أعلى أداة لتطوير وإدارة السياسات في الأمانة العامة للأمم المتحدة. **راجع:**

U.N. Doc. AIC.5/55/46/Add.1 *(Aug. 8, 2001);* ***U.N. Doc. A/55/305, S/2000/809*** *(Aug. 21, 2000).*

(4) ***U.N. Doc. A/55/502*** *(Oct. 20, 2000).*

المُمولين لها، وبناءً علي هذه المعلومات تم اعتماد وتنفيذ قرارات ذات صلة، ومنها؛ القرار رقم (١١٧٣) لسنة ١٩٩٨، (١٣٩٠) لسنة ٢٠٠٠، (١٥٢٦) لسنة ٢٠٠٤، (١٦١٧) لسنة ٢٠٠٥[١].

وتكرّر الأمر عام ٢٠٠٣، عندما شرع المجلس في مناقشة اتخاذ تدابير قمع ضد العراق، وعرضت الولايات المتحدة الأمريكية أمام الأعضاء معلومات تجسس سيبراني، وحينها لم تكن لجنة التفتيش عن الأسلحة المحظورة في العراق ـ ولمدة ثلاثة أشهر ـ قد عثرت على ما يفيد وجود مثل هذه الأسلحة، في حين واصلت إدارة "بوش" التأكيد على "تيقنها"، من أن العراق يُصنِّع ويُخزّن أسلحة دمار شامل، بالمخالفة لقرارات الأمم المتحدة، ولتوضيح مبررات هذا اليقين، عرض وزير الخارجية الأمريكي حينها "كولن باول" أمام المجلس، معلومات تم جمعها من التجسس السيبراني، وتمثَّلت في صور التقطتها الأقمار الصناعية، وإشارات لاسلكية تم اعتراضها، وقال "باول": "كل بيان أُدلي به اليوم، مدعوم بأدلة راسخة وصلبة، وليس مجرد تكهنات، وإنما حقائق بناءً على استخبارات في غاية الدقة والقوة، وكان "جورج تينيت"، مدير وكالة الاستخبارات المركزية وقتها ـ والذي ظلَّ صامتًا ـ يجلس خلف "باول" طوال كلمته التي استمرت لمدة ثمانين دقيقة[٢].

ولم تكن هذه هي المرة الأولي التي تَعرض فيها الولايات المتحدة الأمريكية، ثمار تجسسها أمام مجلس الأمن؛ فقد كان هناك ما يُعرف في تاريخ الأمم المتحدة بلحظة "*Adlai Stevenson*"، وتشير إلى جو التوتر الذي ساد جلسة مجلس الأمن في أكتوبر من عام ١٩٦٢، عندما وجَّه الممثل الأمريكي "*Stevenson*"، إلى نظيره السوفيتي "*Zorin*"، سؤلاً بشأن نشر صواريخ سوفيتية في "كوبا"، قائلاً، هل تُنكر أيها السفير أنكم قد نشرتم ومازلتم، صواريخ متوسطة وقصيرة المدى في "كوبا"؟ وأَكْمَل متسائلاً، أنت لا تنتظر ترجمة لما أقول، وتفهمه! نعم، أم لا؟ وأجاب "***Zorin***": أنا لست في قاعة محكمة أمريكية، ولا أرغب في الإجابة على سؤال طُرح عليَّ بطريقة المدعي العام، فقاطعه "*Stevenson*"، أنت الآن في قاعة محكمة للرأي العام العالمي، ويمكنك الإجابة بنعم أو لا، هل تُنكر وجودها، وأنا على استعداد لانتظار جوابك حتى يتجمد الجحيم، وعلى استعداد أيضًا لتقديم الأدلة على ما قلته فورًا، ولم يرد "*Zorin*" أو يُبدي أي استجابة، فقام "*Stevenson*"، على الفور بعرض صور بحجم كبير، لمواقع الصواريخ التي التقطتها طائرات التجسس الأمريكية[٣].

ويمكن القول، أن وقائع جلسة ٢٠٠٣، تُمثَل السابقة الأولي لاعتماد المجلس على معلومات تجسس، عند مناقشة قرار بالتدخل العسكري وفقًا للفصل السابع من الميثاق، وهو أمر يستحق النظر، حيت لم يُثر أي من أعضاء المجلس إشكالية مدى مشروعية التجسس الأمريكي على العراق، وحيازة معلومات سريَّة مُفَصَّلة عنه، وإنما تم التركيز على مدى دقة ورسوخ هذه المعلومات، والتي ثبت واقعًا خطأ المخابرات الأمريكية والبريطانية بشأنها، وكذلك عدم جدية ما كان يبديه "هانز بليكس"، الرئيس

---

(١) **تم دراسة هذا الموضوع من خلال الفصل الثاني**، المطلب الثاني بعنوان الوضع القانون الدولي للتجسس في وقت السلم، الفرع الأول، مشروعية التجسس وقت السلم وفقًا للقانون الدولي، البند ثالثًا.

(2) ***K. GROUP**, Intelligence and Analysis on Iraq: Issues for the Intelligence Community 2-3 (Central Intelligence Agency, 2004), **available at:** http://www.gwu.edu/-nsarchiv/news/20051013/keff-report.pdf. 26/4/2019.*

(3) ***R. F. KENNEDY,** Thirteen Days: a Memoir of the Cuban Missile Crisis, 53-54 (2d ed. 1971) (1969).*

التنفيذي للجنة الأمم المتحدة للمراقبة والتحقق والتفتيش (*UNMOVIC*) من قناعات تتعلق باشتباهه في احتفاظ العراق بأسلحة محظورة[١].

المطلب الثاني

تحليل مدى تأهل سلوك التجسس السيبراني وقت السلم كعرف دولي

تمهيد وتقسيم:

أوردت المادة رقم (١/٣٨/ ب) من النظام الأساسي لمحكمة العدل الدولية، شرطين أو ركنين يتحقق بوجودهما العُرف الدولي، **وهما؛ أولاً:** اتصاف السلوك بكونه ممارسة عامة موحدة ومتسقة للدول؛ **وثانيًا:** الاعتقاد بأن السلوك مُتطلب أو مسموح به بموجب القانون الدولي، أي أن يُصاحب ممارسة السلوك اعتقاد بأنه ملزم بموجب القانون الدولي.

وفيما يتعلق بالتجسس السيبراني، فإن أن كثيرًا من الدول تُمارسه، ولا تعكس ردود الأفعال الدولية بشأنه اتجاهًا أو نمطًا مُوَّحدًا أو متواترًا[٢]، عدا بعض النصوص الدولية التي تشير إلى عدم قبوله، وتحديدًا في مجال الوظيفة الدبلوماسية، ووفقًا لاتفاقية "فيينا" للعلاقات الدبلوماسية لعام ١٩٦١، كما جري العرف على إعلان الدبلوماسي المُتورط في هذا السلوك، غير مرغوب فيه، وقد يصل الأمر إلى طرده من الدولة الموفد لديها.

ولتكوين رأي قانوني منضبط بشأن هذه الإشكالية، وعلى ضوء ما تم عرضه من ممارسات للتجسس السيبراني في المطلب السابق، نبدأ بتحليل مدى صلاحية هذا السلوك للتأهل كعرف دولي، وذلك بالتطبيق على الشرطين أو الركنين الواردين في المادة (١/٣٨/ ب) من النظام الأساسي لمحكمة العدل الدولية، بشأن العرف الدولي كدليل على ممارسة عامة مقبولة كقانون بين الدول، وذلك من خلال الفروع الثلاثة التالية.

الفرع الأول

مدى توافر شرط الممارسة العامة المقبولة دوليًا

بشأن سلوك التجسس السيبراني

أوضحت محكمة العدل الدولية في قضايا الجرف القاري في بحر الشمال، أنه لنشوء قاعدة عرفية يجب أن تكون هناك ممارسة "واسعة ومتكاملة تقريبًا" لصالح تلك القاعدة، **ولا تعني الممارسة الواسعة لتلك القاعدة أن تُقبل من كل دول العالم،** ولا تتطلب من الدول التي تمارسها أن تفعل ذلك بامتثال صارم، حيث إن ذلك يُعد عتبة مرتفعة للغاية[٣].

---

(1) ***S. CHESTERMAN**, Just War or Just Peace After September 11: Axes of Evil and Wars Against Terror in Iraq and Beyond, 37 N.Y.U. J. INT'L L. & POL., 2005, P. 281.*

(2) ***E. SHOSHAN**, Applicability of International Law on Cyber Espionage Intrusions, P. R., PP. 29.*

(3) ***North Sea Continental Shelf Cases**, (Federal Republic of Germany/Denmark v. Federal Republic of Germany/Netherlands), 4 Reports of Judgments (International Court of Justice 1969), Para. 74.*

كما قرّرت المحكمة في قضية "خليج ماين" "*Gulf of Maine*" عام ١٩٨٤، أن قبول الدولة لسلوك ما، يمكن أن يتم التعبير عنه ضمنيًا، من خلال عدم الاعتراض عليه، ويجوز للطرف الآخر أن يفسر ذلك، باعتباره موافقة على السلوك[١].

وأوضح جانب فقهي، أنه عند انتشار ممارسة ما على نطاق واسع داخل المجتمع الدولي، مع عدم اعتراض الدول على شرعيتها، فإنه يُمكن اعتبار ذلك بمثابة قاعدة تسامح أو قبول لها، وكونها ترقى إلى القبول كقانون بالمعنى المقصود في المادة (١/٣٨/ب) من النظام الأساسي لمحكمة العدل الدولية[٢].

وترتيبًا على ذلك، قدَّم جانب فقهي رؤيته بشأن فهم ومقاربة ما سبق، باعتبار أن شرط الممارسة العامة المقبولة تتحقّق في التجسس السيبراني، حيث صار أحد الوظائف الأساسية لغالبية الدول، إن لم يكن جميعها، وبالتالي، فإن ممارسته تتم على نطاق واسع، ومن خلال أجهزة وطنية رسمية، ولم تُصرّح الدول أو تُعلن رسميًا، اعتراضها علي مشروعيته، ومن ثم، يمكن قبوله كممارسة عرفية دولية[٣].

ونلاحظ أن الفهم السابق مُنتقد بشدة، بالنظر إلى سرَّية نشاط التجسس السيبراني، حيث تمارسه الدول "سـرًا"، وتبذل جهودًا مُكثَّفة للحفاظ على هذه السرية، فتبالغ في تمويه مكان إطلاق عملياتها ومصدرها، وإذا تم كشفها، فإنها تُنكر صلتها به وتتنصل منه، وبالتالي، فإن هذا السلوك يبتعد تمامًا عن مضمون الممارسة العامة، ويبقي في إطار الممارسات السرية، التي لا صلة لها بتأسيس القانون الدولي العرفي، من حيث عدم وجود مجال لأن تتبادل الدول الرؤى بشأنها، بحيث تقبلها أو ترفضها.

ولعل غياب المعارضة لسلوك ما على الصعيد الدولي، تنطوي في بعض الأحيان، على موافقة من جانب الدول المعنية، إلا أن القول بذلك يتطلب البحث في سبب غياب تلك المعارضة، فإذا كانت الممارسة علنية، ووفقًا للمجري العادي للأمور، تتطلب الرد بالرفض أو القبول، والدول المعنية في وضع يمكنها من الرد، فإن افتقاد المعارضة يعني قبول الممارسة، أما إذا كانت الممارسة سريَّة، فلا مجال للاعتراض عليها أصلاً، ولا يُمكن اعتبار عدم معارضتها بمثابة قبول لها[٤].

وقد أورد التقرير الثاني للجنة القانون الدولي، بشأن تحديد القانون الدولي العرفي، استنكارًا بشأن علاقة هذه الممارسات بالعرف الدولي، وقرَّر أنه: "من الصعب فهم، كيف يمكن أن تسهم الممارسات السرية في تشكيل أو تحديد القانون الدولي العرفي[٥]؟ فشرط عمومية وعلانية ممارسات الدول أمر مهم، بحيث يتيح للدول فرصة "الرد عليها والتجاوب معها إيجابًا أو سلبًا"، ومن ثم اتخاذ قرار باعتماد القاعدة

---

(1) ***Delimitation of the Maritime Boundary in the Gulf of Maine Area****, Judgment [1984] ICJ Rep 246, para. 130.*

(2) ***K. WOLFKE****, Custom in Present International Law, Works of the Wroclaw Scientific Society, Wroclaw, 1964, P. 48.*

(3) ***A. DEEKS****, an International Legal Framework for Surveillance, 55 VA. J. INT'L L. 291, 328, 2015, P. 608;* ***N. GAOUETTE****, Ex-CIA Chief: Russian Hackers Trying to 'Mess with Our Heads', CNN (Oct. 18, 2016),* ***available at:*** *https://perma.cc/YXM4-96QL. 27/4/2020.*

(4) ***S. J. SCHACKELFORD****, Managing Cyber Attacks in International Law, Business, and relations: in Search of Cyber Peace, 1st. edn., Cambridge University Press, United States, 2014, P. 237.*

(5) ***International Law Commissions,*** *Second Report on the Identification of Customary International Law, A/CN.4/672, para. 47 (22 May 2014).*

وبدء نشوئها، أو رفضها والسعي لإجهاض بلورتها، ولا يمكن أن يحدث ذلك عندما تكون تلك الممارسة سرية[١].

إضافة إلى أن مفهوم سيادة القانون يعني، أن القواعد القانونية تكون ذات طابع عام ومُعلن، ولهذا قرَّر ميثاق الأمم المتحدة في مادته رقم (١٠٢)، أن كل معاهدة أو اتفاق دولي يعقده الأعضاء، يجب أن يسجل في أمانة الهيئة، مع نشره بأسرع ما يمكن، وهو بمثابة حظر للمعاهدات السرية، وينطبق نفس المنطق علي الممارسات في إطار العلاقات الدولية، فلا يُمكن أن يتبلور العنصر الموضوعي للعرف من ممارسة سرية، كالتنصت على مقر بعثة دبلوماسية مثلاً[٢].

ويؤكد جانب فقهي على المعنى السابق بقوله، إنه لا يمكن التذرع بشيوع سلوك التجسس للقول بمشروعيته دوليًا، لأنه يتم سرًا، ولا تُرحّب أي دولة بنسبته إليها، بل تُدينه وتنفي صلتها به عند كشف الجواسيس؛ ويعبر ذلك عن شعور بخطأ الممارسة، لا إلزاميتها أو الحق فيها[٣].

ويوضح جانب فقهي آخر، أن نظرة المجتمع الدولي للتجسس، تتسم بالتردد والغموض، ولا يوجد اتجاه موحد وثابت بشأن قبوله أو رفضه، إلا أن هذه الممارسة لها طبيعة غير ودية، وتثير القلق بشأن انتهاك الأخلاق الدولية[٤]، وعلى سبيل المثال، في عام ١٩٢٩ أغلق "*Henry L. Stimson*" - وزير خارجية أمريكي سابق - قسم التشفير والمعلومات بمكتبه، مُعلّلاً ذلك بأن "السادة لا يقرأ بعضهم بريد بعض، ثم ألغي هذا الأمر وقرر فتح القسم مرة أخري، عند ظهور أدلة بشأن تهديدات محتملة من دول في قارتي "آسيا"، و"أوروبا""[٥].

وفيما يتعلق بتبادل معلومات التجسس بين الدول، لاسيما في مجال مكافحة الإرهاب؛ فإنها لا تتم على نطاق واسع، أو بشكل روتيني ومستمر، وتحتاج إلى تفاهمات وبروتوكولات تعاون بين الدول المعنية، وبالتالي، لا يمكن القول بأنها ممارسة عامة، ومن ذلك، عندما أعلنت "*CIA*"، أنها ستشارك في عمليات سرية لجمع معلومات، بغرض استباق التهديدات، والحفاظ على الأمن القومي الأمريكي[٦]؛ فإن

---

(1) ***Y. DINSTEIN***, *The Interaction between Customary Law and Treaties, Recueil des Cours Recueil des cours, 322, 2006, P. 275.*

(2) ***United Nations, General Assembly,*** *International Law Commissions, Final Report of the Committee: Statement of Principles Applicable to the Formation of General Customary International Law, International Law Association, London conference, 2000, Para.15.*

(3) ***S. CHESTERMAN***, *the Spy Who Came in from the Cold War, P. R., PP. 1071: 1072;* ***Q. WRIGHT***, *Espionage and the Doctrine of Non-Intervention in Internal Affairs, P. R., P. 12.*

(4) ***M. G. MORA***, *Treason, Sedition and Espionage as Political Offenses Under the Law of Extradition, 26 U. PITT. L. REv. 65, 1964, PP. 79:80.*

(5) ***D. M. CRANE***, *Counterintelligence Coordination within the Intelligence Community of the United States: Divided We Stand, 12 ARMY LAW, 1995, PP. 26: 31.*

(6) ***Central Intelligence Agency,*** *CIA Vision, Mission, Ethos & Challenges,* ***available at:*** *https://www.cia.gov/about-cia/cia-vision-mission-values. 2/1/2020.*

هذا السلوك يُمثّل ممارسة من جانب دولة واحدة، ربما تهدف إلى حث الدول على تكوين قاعدة عرفية، إلا أن مثل تلك القاعدة لا تتكوَّن إلا على أساس شبكة من السوابق بين الدول[1]، وهو أمر مفتقد في هذه الحالة.

وبالتطبيق على مدي توافر ركن الممارسة العامة المقبولة دوليًا، في حالات التجسس السيبراني التي عرضنا لها سلفًا، فإننا نجد الآتي:

أولاً: بالنسبة للتجسس بالطائرة "*U-2*" عام ١٩٦٠:

استمرت الطائرة في التجسس سرًا، على عدة دول منذ عام ١٩٥٥، ولمدة تزيد عن خمس سنوات، وذلك بموجب برنامج سري لوكالة المخابرات الأمريكية، وبعد إسقاط الطائرة عام ١٩٦٠، أنكرت الحكومة الأمريكية قيامها بالتجسس، وتمسَّكت بأنها تقوم بأعمال مراقبة مشروعة كرصد الطقس والتغيرات الجوية، وإذا كان الطائرة قد انتهكت القانون الدولي، فيُسأل قائد الطائرة عن ذلك بشكل شخصي.

وعندما اضطرت الإدارة الأمريكية للاعتراف بقيامها بالتجسس، استدعي الأمر خطاب من رئيس الدولة وقتها " آيزنهاور" لشرح أسباب التورط في التجسس، وهي، أن جميع الدول تمارس هذا السلوك؛ وأنه ضرورة للدفاع عن النفس؛ وأن الروس أنفسهم يمارسون التجسس، وأنه يدعم السلم والأمن في دول العالم. ولاحقًا، وافق "آيزنهاور" على مطالب السوفيت بوقف هذه المهام الجوية.

ونلاحظ أن هذه الواقعة واضحة بشأن طبيعتها السرية، وعدم علانيتها أو عموميتها، وبما يُخالف صراحةً نص المادة رقم (١/٣٨/ ب) من النظام الأساسي لمحكمة العدل الدولية، بشأن كون الممارسة عامة ومقبولة، وقد حاولت الإدارة الأمريكية جاهدة أن تُبقي على هذه السريّة حتى بعد إسقاط الطائرة، تحُسبًا لرد فعل الدول الأخرى التي تم التجسس عليها أيضًا كالصين، وبما يعني أن تلك الإدارة لم تكن مستعدة لأن يتم الإعلان عن هذه الممارسة، أو نسبتها إليها، لأنها تُدرك أن رد الفعل عليها سيكون سلبيًا باعتبارها غير مقبولة دوليًا.

كما نلمح أنه بعد إسقاط الطائرة، تمسَّكت الإدارة الأمريكية بأن الطائرة كانت تقوم بأعمال مشروعة، ولا تنتهك القانون الدولي، وبمفهوم المخالفة فإن الأمريكيين يعتقدون أن سلوك التجسس ممارسة غير مشروعة دوليًا، وهو ما جعل رئيس الاتحاد السوفيتي السابق يحتَّج رسميًا على هذه الواقعة، ويتقدم إلى مجلس الأمن الدولي، بمشروع قرار لإدانة هذه الممارسة باعتبارها عمل عدائي.

ثانيًا: بالنسبة لبرنامج "*U.S. Corona*" لعام ١٩٦٠:

أُطلق هذا البرنامج لغرض التجسس بالأقمار الصناعية، ضمن عدة برامج لوكالة (*NSA*)، وصُنّف رسميًا بأنه "سري، ونُفّذ تحت غطاء برنامج لحماية القوات الجوية الأمريكية، وأُستخدم لجمع معلومات عن عدة دول، لاسيما الاتحاد السوفيتي السابق، وبعد أكثر من (٢٣) عامًا، وفي الثاني والعشرين من شهر فبراير عام ١٩٩٥، تم رفع صفة السرية عن الصور التي أُلتقطت بواسطته، بموجب قرار من الرئيس الأسبق "بيل كلينتون".

---

(١) **حكم محكمة العدل الدولية في قضية "نيكاراجوا" ١٩٨٦**، المرجع السابق، الفقرة ١٨٤؛ **حكم محكمة العدل الدولية في قضية برشلونة للقوى المحركة "*Belgium v. Spain*"**، ١٩٧٠، الفقرة ٣٩، الرأي المنفصل للقاضي "*Ammoun*".

وبالتالي فإن هذه الممارسة نشأت سرية، ونُفذّت في سريّة، وعندما تم كشفها، بادر الاتحاد السوفييتي السابق بالاحتجاج رسميًا عليها، وذلك أمام لجنة الفضاء بالأمم المتحدة باعتبارها تنتهك سيادته، وبالتالي لم تكن الممارسة عامة، كما لم تكن هناك ثمة موافقة أو قبول لتلك الممارسة، وإنما تم الاعتراض والاحتجاج عليها بمجرد العلم بها، ولذا فلا شك أنها تُخالف شروط تكوين العرف الدولي الواردة في المادة رقم (١/٣٨/ب) من النظام الأساسي لمحكمة العدل الدولية.

ثالثًا: بالنسبة الهجوم السيبراني "*Titan Rain*" على الولايات المتحدة الأمريكية عام ٢٠٠٣:

تمثَّل رد فعل الولايات المتحدة الأمريكية بعد علمها بهجمات"*Titan Rain*" السريَّة، في توجيه اتهام لحكومة الصين، والتي بدورها أنكرت صلتها بهذه الممارسة بشكل قاطع، ونلاحظ أن الأولي رأت أنه من ضمن حقوقها السيادية ألا يتجسس عليها أحد، وبالتالي يُجسَّد رد فعلها عدم قبول هذا الفعل دوليًا، ثم رسَّخت الصين لهذا الفهم عندما سارعت وأصرت على نفي هذا الاتهام، باعتبار أنه اتهام لا ينبغي أن يُلصق بها، وبالتالي، لا يمكن القول بأن هذه الواقعة تُمثل ممارسة عامة مقبولة دوليًا.

رابعًا: بالنسبة للكشف عن وثائق "سنودن" عام ٢٠٠٧:

بعد ممارسة وكالة الأمن القومي الأمريكية، للتجسس السيبراني على بعض الدول والمنظمات الدولية، كان الإعلان عن هذا الأمر عام ٢٠٠٧، باعتباره "كشفًا"، حيث تمت الممارسة بشكل سري، ولو لم يتم الكشف عنها ما كانت قد ظهرت، ونلاحظ كذلك أن عدم قبول هذا الفعل واستنكاره، كان هو الطابع الغالب على ردود الفعل الدولية، باعتباره يتنافي مع العلاقات الودية بين الدول، وحتى تبرير الإدارة الأمريكية نفسها له، تمثَّل في القول بأنه كان ضروريًا للحفاظ على "الأمن القومي الأمريكي"، ولم يجرؤ أحد على التطرق إلى كونه مشروعًا أو مقبولاً كممارسة عامة في القانون الدولي.

خامسًا: بالنسبة للتجسس السيبراني على كندا خلال عام ٢٠٠٩:

لم تقبل السلطات الكندية هذا السلوك، وسارعت بإجراء تحقيقات بشأنه، وعلى الرغم من إشارة بعض الأدلة إلى تورط الحكومة الصينية في الهجوم، إلا أن هذه الأدلة لم تكن كافية لإسناد الفعل لها، وتجسّد الواقعة برمتها حالة من الغموض والسرَّية، لاسيما بشأن الهدف منها، وحرص الطرف المُهاجم على عدم الإعلان أو الإفصاح عن نفسه، وحتى بعد إجراء تحقيقات وتدقيق، لم يكن بالإمكان نسبة الممارسة إلى كيان معين، مما يُبقيها ضمن نطاق الممارسات السرية، وينفي عنها صفة الممارسة العامة المقبولة وفقًا للمادة (١/٣٨/ب) من النظام الأساسي لمحكمة العدل الدولية.

سادسًا: بالنسبة لهجوم "أوروا" "*Aurora*" على شركة "*Google*" الأمريكية عام ٢٠١٠:

بعد أن أعلنت شركة "جوجل" تعرضها لهجوم سيبراني مصدره "الصين"، بدأ رد الفعل الأمريكي باحتجاج وزارة خارجيتها على هذا السلوك، ومطالبتها للحكومة الصينية بتفسير، باعتبار أن هذا الاختراق مسألة خطيرة، ثم صرَّحت وزارة الخارجية الأمريكية بأنها ستُصدر مذكرة احتجاج عن الواقعة، وأنها تتطلع لأن تُجري السلطات الصينية تحقيقًا شاملاً بشأن هذا الهجوم، كما أصدر الكونجرس الأمريكي قرارًا بإدانة مثل هذه الاختراقات غير المشروعة، مع دعوة حكومة الصين إلي التحقيق فيها.

ونلاحظ أنه بالرغم من أن الولايات المتحدة الأمريكية، لم تتعامل مع هذا الهجوم كانتهاك صريح للقانون الدولي، ودار موقفها ما بين الاحتجاج، أو الإعراب عن القلق الشديد، إلا أنه وفي المُجمل، يُمثّل هذا الموقف، عدم موافقة على هذه الممارسة أو قبولها. وعلي الجانب الآخر، بادرت الصين بنفي الاتهامات الموجهة إليها، وأدانت هذا السلوك، ولم تتذرَّع بأنه مشروع دوليًا، أو أنه ممارسة مُستقر عليها دوليًا، بل إنها طالبت بتكثيف التعاون الدولي لمكافحة مثل هذه الممارسات، ومن ثم، نجد عدم موافقة على سلوك التجسس السيبراني.

سابعًا: التجسس الأمريكي على هاتف المستشار الألمانية "*Merkel*" عام ٢٠١٣:

بعد كشف "*Edward Snowden*" في يونيو من عام ٢٠١٣، ما قامت به "*NSA*"، من تنصت على اتصالات المستشارة الألمانية "أنجيلا ميركل"، لم يكن الأمر مقبولاً من جانب السلطات الألمانية، التي فتحت تحقيقًا بهذا الشأن، كما أوضحت "ميركل" أن هذه الممارسات غير مقبولة، وطالبت الإدارة الأمريكية بتوضيح لهذا الأمر، وأوضح المتحدث باسم البيت الأبيض، أن الرئيس "أوباما" قد أبلغ "ميركل" بأن بلاده لم ولن يحدث أن تجسست على اتصالاتها. وهو ما يعكس حالة من عدم القبول للتجسس كممارسة بين الدول.

ثامنًا: بالنسبة لتجسس "استراليا" على "تيمور الشرقية" عام ٢٠١٣:

طلبت دولة "تيمور" الحكم ببطلان معاهدة الترتيبات البحرية في بحر تيمور لعام ٢٠٠٢، واستندت في طلبها، إلى حصول "استراليا" على معلومات بطريق التجسس، مما عزَّز موقفها في التفاوض، وحصولها على ميزات غير عادلة، بالمقارنة بدولة "تيمور"، وباعتبار أن طريقة الحصول على هذه المعلومات تخالف مبدأ حسن النية في العلاقات الدولية، وتُعد تدخلاً في الشئون الداخلية لدولة "تيمور" وانتهاكًا لسيادتها.

وبالتالي فإن موقف دولة "تيمور" من ممارسة التجسس، يتمثّل في كونه مخالفًا لحسن النية في العلاقات الدولية، وتدخلاً في شئون الدول وانتهاكًا لسيادتها، وهو ما يجافي توافر شرط الممارسة العامة بالنسبة لسلوك التجسس. وفيما يتعلَّق بموقف "استراليا"، فقد حاولت الدفاع عن موقفها، بأن الدول تتجسس على بعضها، وهو أمر جائز وفقًا للعرف الدولي، إلا أنها لم تُقدّم أي إثبات لهذا الدفع، والواقع أن الدول ترفض هذا السلوك، وتبادر بالاحتجاج عليه بمجرد علمها بحدوثه، وإذا كان الجاسوس دبلوماسيًا فيكون الطرد هو الجزاء.

تاسعًا: بالنسبة لمُقترح إنشاء أمانة للتحليل الاستراتيجي للأمم المتحدة:

سعى الأمين للأمم المتحدة لإيضاح أن مسألة تطوير القدرات التحليلية للأمم المتحدة، بإنشاء أمانة للتحليل الاستراتيجي، لا علاقة له بالتجسس السيبراني أو غيره من أنواع التجسس، وذلك على خلفية المخاوف التي أبدتها عدة دول، من أن تكون هذه الأمانة بمثابة وكالة مخابرات للمنظمة، وصرَّح "*Anan*" بأنه لا ينبغي الخلط بين إنشاء الأمانة وبين عمليات التجسس، فالأولي وسيلة لضمان استخدام المعلومات الموجودة والمُتاحة بالفعل بصورة فاعلة. **ونلاحظ أمرين، الأول:** هو اعتراض الدول على سلوك التجسس، واستنكار احتمالية أن تمارسه الأمم المتحدة من خلال تلك الأمانة، **والأمر الثاني،** هو محاولات الأمين العام للمنظمة، لتوضيح أن المقترح منبت الصلة بالتجسس، وبالتالي فإن هناك رفض

عام وصريح لممارسة التجسس على الصعيد الدولي، وتكون الممارسة العامة المقبولة بشأن سلوك التجسس هو رفضه على المستوى الدولي.

عاشرًا: بالنسبة لاتخاذ مجلس الأمن قرارات بناءً على عمليات تجسس سيبراني:

اعتمد مجلس الأمن على معلومات استخباراتية في مجالين مهمين: الأول؛ مكافحة الإرهاب، وهو مجال يثير مسألة سرية أنشطته، واستحالة التعرّف عليها لغرض مكافحته، إلا بتوافر معلومات عنها وعن مموليها، ومع ذلك، لم يُصرَّح المجلس بأنه يستخدم معلومات استخباراتية، ولا يعدو الأمر كونه، تلقي المجلس معلومات من الدول عن هذه الكيانات وأنشطتها، دون استجلاء مصدرها، أو الاستفسار عن كيفية الحصول عليها، وكانت قرارات المجلس ذات الصلة، تتضمن ديباجة "ضرورة تعاون الدول بشأن توفير معلومات عن عمليات وتحركات الكيانات الإرهابية والإرهابيين، وإعداد قوائم للأفراد المُشتبه بتورطهم في هذه العمال، أو المُمولين لها"، دون تَطَلُّب أن تكون معلومات استخباراتية، ولذا لا تُرسّخ هذه القرارات لوجود ممارسة عامة بشأن التجسس.

أما المجال الثاني، فهو مناقشة المجلس قرارات خاصة بتدابير قمع، بناءً على معلومات استخباراتية عُرضت أمامه وتحديدًا بشأن العراق، ويُمكن تعليل ذلك بأن الولايات المتحدة كانت تتبني إصدار قرار للموافقة على الغزو، وتسعي لتجنب استخدام "الفيتو"، وفي سبيل ذلك، سعت لتكوين اتجاه داخل المجلس يُؤّيد فكرة الحفاظ على السلم والأمن الدوليين، بأي طريقة كانت، ومنها المعلومات الاستخباراتية التي تُظهر وجود أسلحة محظورة لدي العراق، وكذلك ادعاءات "هانز بليكس"، الرئيس التنفيذي للجنة الأمم المتحدة للمراقبة والتحقق والتفتيش، بشأن احتفاظ العراق بتلك الأسلحة، وإجمالاً يُمكن القول، بأنها واقعة استثنائية أو ممارسة محدودة وليست عامة، لم تتكرر أو تتم على نطاق واسع، وإنما كانت خاصة باتخاذ هذا القرار.

وترتيبًا على ما سبق يمكننا القول بأنه:

(١) على الرغم من ممارسة كثير من الدول للتجسس السيبراني، فإنه وفقًا للمادة رقم (٣٨/١/ب) من النظام الأساسي لمحكمة العدل الدولية، لا يُمكن اعتماد هذه الممارسات كركن مادي للعرف الدولي، أو اعتبارها ممارسة عامة مقبولة، حيث إنها عادةً ما تُوصف من المجتمع الدولي، بكونها أعمال غير ودية، وتؤدي إلى توتر العلاقات بين الدول[1]، كما أنها ذات طبيعة سريَّة، وليس للممارسات السرية أي دور في تكوين العُرف، بل إنها غير مقبولة بشأن إنشاء قاعدة قانونية أو تغيير مضمونها، ولعل إخفاء الدول القيام بممارسة ما، يُعزّز الاعتقاد بأن هذه الممارسة غير مشروعة، وبغض النظر عن اتساع حجمها، حيث يصعب مع الطبيعة السرية إثبات شرط الممارسة العامة.

(1) ***H. Farrell, M. FINNEMORE****, the End of Hypocrisy: American Foreign Policy in the Age of Leaks' Foreign Affairs, November/December 2013, PP. 22: 24.*

الفرع الثاني

مدى توافر شرط الاعتقاد بالإلزام في ممارسة سلوك التجسس

يتعلق الشرط الثاني لنشوء قاعدة عرفية وفقًا للمادة رقم (١/٣٨/ب)، بوجود اعتقاد عند الدول بالإلزام القانوني للممارسة ذات الصلة، والدفاع عنها إذا طُعن عليها، ويُمثل هذا الشرط عقبة كبيرة بالنسبة للتجسس السيبراني، لأن ممارسته لا تقترن مُطلقًا بالاعتقاد بمشروعيته، بل على العكس يصاحبها اعتقاد بالإثم القانوني، وعندما تواجه أي دولة اتهامًا باحتمال ضلوعها فيه، فإنها ترفض هذا الاتهام بصرامة، وتجتهد في نفي مسئوليتها عنه[١]، ويمكن القول بأن ممارسة الدول للتجسس واعتقادها بمشروعيته، يسيران في اتجاهين متضادين[٢].

ويقرّر جانب فقهي أن التجسس السيبراني يُثير الجدل بشأن مدي تأهله كعرف دولي، إلا أن الواقع يثبت قلة الممارسات بشأنه، والافتقار إلى اعتقاد الدول بإلزاميته، حيث أعلنت دول كثيرة احتجاجها عليه وإدانتها له، باعتباره لا يتوافق مع العلاقات الدولية الودية، وحري بالذكر، أن رفض بعض أعضاء المجتمع الدولي لممارسة، بسبب مخالفتها للقانون الدولي، يحول دون تشكلها وبلورتها كعرف دولي[٣]، وهذا هو الواقع المتعلق بالتجسس السيبراني، حيث يؤيّد رد فعل الدول بشأنه ابتعاده تمامًا عن كونه عرفًا دوليًا.

وبالتطبيق على مدي توافر ركن الاعتقاد بمشروعية السلوك، وذلك في حالات التجسس السيبراني التي عرضنا لها سلفًا، فإننا نجد الآتي:

أولاً: بالنسبة لواقعة الطائرة (*U-2*) ١٩٦٠، فقد احتَّج رئيس الاتحاد السوفيتي السابق رسميًا عليها؛ باعتبارها انتهاكًا للمجال الجوي لدولته، وتقدَّم إلى مجلس الأمن بمشروع قرار، لإدانة ومنع ما اعتبره أعمالاً عدوانية من القوات الأمريكية ضد دولته، تُخلّ بمبدأ المساواة في السيادة وحرمة المجال الجوي، وبالتالي فإننا نلاحظ، أن الاعتقاد بشأن ممارسة التجسس السيبراني، هو أنها غير مشروعة ويتم الاحتجاج على ممارستها.

ثانيًا: بشأن لبرنامج "*U.S. Corona*" لعام ١٩٦٠، أعلن الاتحاد السوفييتي السابق رسميًا في ٢٤ أبريل ١٩٦٣، أمام اللجنة الفرعية القانونية للفضاء بالأمم المتحدة، أن سيادته قد أُنتهكت وتم التدخل في إقليمه، بالمخالفة للقانون الدولي، عندما أُستخدمت هذه الأقمار الصناعية لجمع معلومات عن أنشطته.

ثالثًا: واقعة الكشف عن محطة أرضية أمريكية، للتجسس بالوسائل التقنية عام ١٩٧٩، كانت تقوم باعتراض الاتصالات الصادرة من إيران تحديدًا، مما أدى بالفعل إلى توتر العلاقة بين الدول ذات الصلة،

---

(1) ***Q. WRIGHT***, *Espionage and the Doctrine of Non-Intervention in Internal Affairs, P. R., P. 17.*

(2) ***S. CHESTERMAN***, *the Spy Who Came in from the Cold, P. R., P. 1072.*

(3) ***F. L. KIRGIS***, *Custom on a Sliding Scale, American Journal of International Law 81, 1987, P. 146.*

واضطرت السلطات الأمريكية إلى تفكيكها سريعًا، للاعتقاد بوجود أدلة تشير إلى احتمال محاكمة القائمين عليها بتهمة التجسس، مما قد يضر بالوضع السياسي الأمريكي دوليًا[1].

رابعًا: إصدار الحكومة السويدية مذكرة احتجاج دبلوماسية، في أكتوبر عام ١٩٨١، على قيام غواصة سوفيتية مُزودة بوسائل متطورة لالتقاط الاتصالات اللاسلكية، بالتواجد داخل المياه الداخلية للسويد، بالقرب من قاعدة "*Karlskrona*" البحرية، باعتبار أن هذا السلوك غير مشروع، وينتهك مبدأ عدم التدخل، وهو أحد المبادئ الأساسية للقانون الدولي[2].

خامسًا: في واقعة التجسس السيبراني "*Titan Rain*" على الولايات المتحدة الأمريكية عام ٢٠٠٣، وجَّهت الحكومة الأمريكية اتهامًا صريحًا لحكومة الصين بممارسة التجسس السيبراني، وواجهت الصين هذا الاتهام بالإنكار، ونفيه بشكل قاطع، وبما يشير إلى اعتقاد الولايات المتحدة الأمريكية، أن التجسس السيبراني عمل غير مشروع، كما يُشير نفي الصين للاتهام بشكل قاطع، إلى اعتقادها بأن هذا السلوك غير مشروع دوليًا.

سادسًا: عندما كشفت وثائق "*Snowden*" عن تجسس وكالة الأمن القومي الأمريكي، على عدة دول ومنظمات دولية وأفراد، صرَّحت دول عدة، بأن هذه الممارسة لا تتفق مع القانون الدولي، ومنها "البرازيل"، التي أعلنت أمام الجمعية العامة للأمم المتحدة أن هذا السلوك يتنافي مع القواعد الدولية، والعلاقات الودية بين الدول، وعندما حاولت الإدارة الأمريكية الدفاع عن سلوك الوكالة، بررته بأنه كان ضروريًا للحفاظ على الأمن القومي للدولة، لكنها لم تُصرّح مثلاً بأنها تعتقد بمشروعيته دوليًا.

سابعًا: بعد اختراق "أورورا" "*Aurora*" لأنظمة شركة "*Google*" عام ٢٠١٠، سارعت وزارة الخارجية الأمريكية بالاحتجاج على هذه الممارسة، وطالبت الحكومة الصينية بتفسير، مما يتضح معه اعتقاد الولايات المتحدة بعدم مشروعية هذا السلوك، كما جاء رد الصين، بأن تشريعاتها الوطنية الخاصة بشبكة الانترنت تتوافق مع الممارسات الدولية، وتُجرّم القرصنة بكل أشكالها وتَعُدَّها انتهاكًا للقانون، وهو ما يعني أنها تعتقد أن التجسس السيبراني، يُعد عدم احترام للدول الأخرى، ومخالفة للممارسات الدولية المشروعة، ونوع من أنواع القرصنة.

ثامنًا: عقب الكشف عن واقعة التجسس الأمريكي، على هاتف المستشار الألمانية "ميركل"، صرَّحت وزارة الخارجية الألمانية رسميًا بأن مثل هذه الأنشطة غير مقبولة دوليًا.

تاسعًا: بعد التجسس السيبراني على فرع شركة "*Sony*"، في الولايات المتحدة الأمريكية عام ٢٠١٤، صرَّحت الإدارة الأمريكية بأن هذا السلوك ينتهك القانون الدولي، وردَّت على ذلك، بفرض عقوبات اقتصادية على "كوريا الشمالية" عام ٢٠١٥، ومن ثم، فالولايات المتحدة الأمريكية تعتقد في عدم مشروعية التجسس السيبراني دوليًا، وهو ما يعني مزيدًا من الدعم بعدم عرفية هذا السلوك.

عاشرًا: بشأن الحكم المؤقت لمحكمة العدل الدولية في قضية "*East Timor v Australia*" عام ٢٠١٤، بشأن تضرَّر "تيمور الشرقية" من استيلاء "أستراليا" على معلومات سرية ووثائق تخصها،

---

(1) ***H. SCOVILLE***, *SALT Verification and Iran: Hearings on Military, Hearings on Military Posture and H.R. 1872 (H.R. 4040), H.R. 2575 (S. 429), Part 3, Book 2, P. 2720.*

(2) ***K. ZETTER***, *US and China Reach Historic Agreement on Economic Espionage, WIRED (Sept. 25, 2015),* ***available at:*** *https://perma.cc/VUH7-VU25. 19/3/2020.*

اعتبرت المحكمة أن ادعاء "تيمور" معقولاً، وأصدرت أمرًا مؤقتًا بعدم تدخل استراليا في تعاملات دولة "تيمور" ومستشاريها القانونيين، وفي ٢٥ مارس ٢٠١٥، قرَّرت أستراليا إعادة الوثائق إلى "تيمور"، وفي ٢٢ أبريل من عام ٢٠١٥، أذنت المحكمة بإعادة المستندات إلى "تيمور"، وبما يُفهم منه تأييد ما اعتقدته "تيمور"، بشأن عدم مشروعية سلوك "استراليا" تجاهها، كما يُفهم قرار "استراليا" بشأن إعادة المستندات "لتيمور"، باعتباره اعترافًا من تلك الدولة بالاعتقاد بعدم صحة سلوكها الخاص بالتجسس.

حادي عشر: فيما يتعلّق باعتماد مجلس الأمن عام ٢٠٠٣، عند مناقشة بعض الموضوعات بموجب الفصل السابع من الميثاق، على معلومات تجسس سيبراني، فقد قرّر بعض الفقه أنه أمر مُبرَّر في حالات تهديد السلم والأمن الدوليين، أو الدفاع الشرعي وفقًا للمادة (٥١) من ميثاق الأمم المتحدة، لأن أحكام الميثاق لم تشر أو تُوجّه، إلى نوع أو طبيعة الأدلة اللازمة، لإثبات توافر حالة تهديد السلم أو تبرير الدفاع الشرعي[١]، بل إن للأمين العام دور في تنبيه مجلس الأمن، إلى أي مسألة يرى أنها تهدد السلم والأمن الدوليين، ودون اشتراط معايير معينة في رؤيته، ومن ناحية أخري، عندما عُرضت معلومات التجسس الأمريكية عام ٢٠٠٣، بشأن انتهاك العراق لقرارات المجلس، لم يكن المجلس مطالبًا بتحري اشتراطات معينة بشأن طبيعة هذه المعلومات، إلا أن هذه الحالة تبقي استثنائية، لندرتها وعدم تواترها، ولا تساهم في تكوين العرف الدولي[٢].

ووفقًا لما سبق، يمكننا استنباط عدم وجود أي دليل، يدعم فرضية أن الدول تنظر إلي ممارسة التجسس السيبراني باعتبارها مشروعة دوليًا، بل إن الاعتقاد السائد يتجه لكونها غير مشروعة، ومن ثم، فإن واقع الممارسات الدولية ليس في صالح إثبات عرفية هذا السلوك، وإنما على العكس، حيث إن الممارسة الشائعة التي تتم علنًا وعلى نطاق واسع، هي إدانته والتنصل منه، ومطالبة حظره بموجب اتفاقية دولية.

الفرع الثالث

تعارض سلوك التجسس وقت السلم مع الوظيفة الدبلوماسية

يعد التمثيل الدبلوماسي أحد أهم مظاهر العلاقات الودية بين الدول، وقد حدَّدت المادة (١/٣) من اتفاقية العلاقات الدبلوماسية لعام ١٩٦١، أنه من بين المهام الرئيسة للمبعوث الدبلوماسي في الدولة الموفد لديها، استمراره في إعلام دولته بالظروف والتطورات فيها، وقد أقرت الاتفاقية القيام بهذه المهمة بمراعاة معايير، تبتعد به عن شُبهة التجسس، فأوردت المادة (١/٣/د) من الاتفاقية، أن المبعوث الدبلوماسي يتقصّي الظروف والتطورات في الدولة المُستَقبِلة، وذلك بكل الوسائل القانونية المشروعة، ويُبلغ حكومة دولته بها، كما تطلبت المادة (٧) من الاتفاقية، الحصول على موافقة الدولة المُستقبِلة بشأن الإرساليات العسكرية.

ومن ثم، تتوقف مشروعية سلوك تقصّي التطورات وجمع المعلومات من قبل الدبلوماسيين، على طبيعة الوسائل المُستخدمة في ذلك، فيجوز لهم تحصيلها من المصادر الرسمية، والمفتوحة، والعامة، أو

---

(1) ***T. M. FRANCK**, Recourse to Force: State Action Against Threats and ARMED Attacks, 2002, PP. 97:108; **S. CHESTERMAN**, Just War or Just Peace after September 11, P. R., PP. 281: 282.*

(2) ***Y. DINSTEIN**, Computer Network Attacks and Self-Defense, P. R., PP. 99: 101.*

مما يتم تداوله في المجتمع الدبلوماسي، مع مراعاة ما أوردته المادة (٢/٤١، ٣) من اتفاقية "فيينا" لعام ١٩٦١، من عدم التدخل في الشئون الداخلية للدولة المُستقبِلة، أو استخدام منشآت البعثات بصورة تتنافى مع مهامها، أو مع قواعد القانون الدولي العام، أو أي اتفاقات خاصة سارية بين الدولة المُرسلة والدولة المُستقبلة.

وفي بداية التسعينيات، تداول جانب فقهي مصطلح "ضد الدبلوماسية" "*Anti-diplomacy*"، كتعبير عن قيام بعض الدبلوماسيين بممارسات تكنولوجية، من شأنها تهديد العلاقات الودية بين الدول، كالتجسس السيبراني[١]، حيث تحولَّت الوظائف الدبلوماسية والقنصلية، إلى الاعتماد علي النمط الالكترونية لاسيما نقل المعلومات عبر الفضاء السيبراني[٢]، ووفقًا لدليل "تالين، فإن الحرمة الممنوحة بموجب المادة رقم (٢٤) من اتفاقية "فيينا" للعلاقات الدبلوماسية لعام ١٩٦١، بشأن عدم جواز انتهاك حرمة ووثائق البعثة في أي وقت وأي مكان، تشمل الوسائط الالكترونية التي يتم تخزين أو نقل أي مستندات أو وثائق إلكترونية عليها[٣].

ومع ممارسة الدبلوماسي لمهمة إعلام دولته بأحوال الدولة المُستقبِلة، وتمتع مراسلاته ووثائقه الالكترونية بحصانة، فقد يتورط في ممارسة جمع معلومات بوسائل غير مشروعة، سواء من مصادر سريَّة، أو غير رسمية، كأن يتواصل مع عناصر في قطاع أمني للحصول على معلومات سرية، أو يستخدم مقر البعثة كمركز للتنصت الالكتروني على اتصالات في الدولة المُستقبِلة، أو يقوم بالتسلل إلى مؤسسة أو مَسْكَن لزرع أجهزة تنصت، وفي مثل هذه الحالات يكون قد تجاوز حدود وظيفته الدبلوماسية[٤]، وانتهك حكم المادة (٤١) من اتفاقية "فيينا" للعلاقات الدبلوماسية ١٩٦١، بشأن التزام الدبلوماسيين باحترام قوانين الدولة المُستَقبِلة، وحيثما يوجد تجريم للتجسس بموجب القوانين الوطنية للدول، فإن الدبلوماسي المُتورط في ممارسة التجسس ينتهك هذه القاعدة.

ونظرًا لتمتع الدبلوماسيين بحصانة جنائية وفقًا للمادة (٣١) من اتفاقية "فيينا" للعلاقات الدبلوماسية[٥]، فلا يكون أمام الدولة المستقبلة، وفقًا للمادة (٩) من الاتفاقية إلا التصرف التقليدي، بإخطار الدولة المُوفدة بأن هذا الدبلوماسي شخصًا غير مرغوب فيه، واتخاذ إجراءات تحفظية كتحديد مكان تواجده، أو تعيين حراسة عليه، مما يدفع دولته إلى استدعائه سريعًا، وبالرغم من أن اتفاقية "فيينا" لا تتطلب مبررات عند تقدير أن أحد الدبلوماسيين غير مرغوب فيه[٦]، إلا أن الصيغة التي تستخدمها الدولة

---

(1) ***J. D. DERIAN***, *Anti-Diplomacy: Spies, Terror, Speed and War, Wiley-Blackwell; 1 edition, 1992, PP. 43: 46.*

(2) ***W. M. CHOI***, *Diplomatic and Consular Law in the Internet Age, 10 Singapore Year Book of International Law, 2006, PP. 117: 118.*

(3) ***Rule (41) of Tallinn Manual 2 : Inviolability of electronic archives:*** *"documents and correspondence Archives, documents, and official correspondence of a diplomatic mission or consular post that are in electronic form are inviolable".*

(4) ***R. HIGGINS***, *UK Foreign Affairs Committee Report on the Abuse of Diplomatic Immunities and Privileges: Government Response and Report, 80 AM. J. INT'L L. 135, 1986, PP. 138:139.*

(٥) **قضت المادة (١/٣١) من الاتفاقية بأن:** يتمتع الوكيل الدبلوماسي بالحصانة من الولاية القضائية الجنائية للدولة المستقبلة. كما يتمتع بالحصانة من اختصاصه المدني والإداري.....".

(٦) **قضت المادة رقم (٩) من اتفاقية "فيينا" بأنه:** ١- يجوز للدولة المُستقبلة في أي وقت ودون الحاجة إلى توضيح قرارها، إخطار الدولة المُرسلة بأن رئيس البعثة أو أي عضو من أعضاء السلك الدبلوماسي للبعثة هو شخص غير مرغوب فيه أو أن أي عضو آخر في موظفي البعثة غير مقبول...".

عادةً، هي أن الشخص قد شارك في أنشطة لا تتفق مع مركزه الدبلوماسي[١]، وربما تلجأ الدول إلى طرد المبعوثين المتورطين، دون أن تطلب محاكمتهم من قبل دولهم، ضمانًا لمعاملة دبلوماسييها بنفس الطريقة في الحالات المماثلة.

وتُظهر الممارسة الدولية أن حالات التجسس الدبلوماسي، التي قد ترقي إلى إدانة أحد المبعوثين، وإخطار دولته بأنه غير مرغوب فيه نادرة جدًا، كما لم يتم تسجيل حالات استندت فيها الدول إلى البروتوكول الاختياري المُلحق بالاتفاقية، والمتعلق بالتسوية الإلزامية للمنازعات التي قد تثور بشأنها[٢]، والذي قضي في مادته الأولي، بأن المنازعات المتعلقة بتفسير أو تطبيق أحكام الاتفاقية ـ والتي يمكن أن يدخل التجسس ضمنها ـ يمكن أن تعرض على محكمة العدل الدولية[٣]، والتي كانت قد أشارت في قضية "رهائن طهران"، إلى صعوبة تحديد متى تمثل وظيفة الدبلوماسي بشأن تقصي أحوال الدولة المستقبلة تجسسًا، أو تدخلاً في شئونها[٤].

وفيما يتعلَّق بالتجسس الدبلوماسي بوسائل الكترونية، فقد قضت القاعدة رقم (٣٩) من "تالين٢"، والمتعلقة بحرمة المباني، المُتضمنة للبنية التحتية الالكترونية للبعثات الدبلوماسية والمراكز القنصلية، بأن هذه البنية محمية بالحصانة المقررة للبعثة أو المركز، وأن العمليات السيبرانية التي تستهدف تلك البنية، ترقى لأن تعتبر دخول غير مرخص به إلى المبنى[٥]، وعلي الدولة المستقبلة واجب اتخاذ جميع الخطوات اللازمة لحماية مباني البعثة الدبلوماسية من أي اقتحام أو ضرر، والالتزام بتيسير أداء البعثة[٦].

وأوجبت القاعدة رقم (٤٠) من "تالين ٢"، على الدولة المُستقبلة، أن تتخذ جميع الخطوات المناسبة لحماية البنية التحتية الالكترونية، لمباني البعثة الدبلوماسية، أو المركز القنصلي للدولة المرسلة، ضد التطفل أو أي ضرر[٧]، وفي المقابل لا يجوز للدولة المرسلة، أن تستخدم مباني بعثتها الدبلوماسية،

---

(١) **يختلف هذا الإجراء عما يُعرف بالطرد "الانتقامي"**، الذي يكون غير مبرر، حيث تطرد دولة دبلوماسيين من أراضيها، لظروف المعاملة بالمثل، **ومن ذلك**، أنه في مارس من عام ٢٠٠١، وبعد كشف تجسس " *Robert P. Hanssen*"، على الولايات المتحدة الأمريكية، طلبت الأخيرة من (٤) دبلوماسيين روس مغادرة إقليمها في غضون عشرة أيام، كما أمرت (٤٦) آخرين ممن وصفتهم بضبّاط المخابرات، بالمغادرة بحلول الأول من يوليو ٢٠٠١، فقامت الحكومة الروسية بالرد، وطلبت من (٤) دبلوماسيين أمريكيين المغادرة في غضون عشرة أيام، وأمرت (٤٦) آخرين بالمغادرة بحلول الأول من يوليو ٢٠٠١. ونلاحظ "التكافؤ العددي" بشأن الطرد، ولا يدخل الطرد الانتقامي ضمن نطاق الامتثال لاتفاقية "فيينا" لعام ١٩٦١، ولا يمكن اعتباره انتهاكًا لها. **راجع:**

***M. HERMAN**, Intelligence Services in the Information Age: Theory and Practice, Routledge, Rab., 2013, PP. 41:43.*

(2) ***Optional Protocol Concerning the Compulsory Settlement of Disputes**, Vienna, Italy, Apr. 18, 1961, 500 U.N.T.S. 241.*

(3) ***Article No. (1) of the protocol:** "Disputes arising out of the interpretation or application of the Convention shall lie within the compulsory jurisdiction of the International Court of Justice and may accordingly be brought before the Court by an application made by any party to the dispute being a Party to the present Protocol".*

(4) ***Case Concerning United States Diplomatic and Consular Staff in Tehran** (U.S. v. Iran), 1980 I.C.J. 3, 40 (May 24).*

(5) ***Rule (39) of Tallinn Manual 2: Inviolability of premises in which cyber infrastructure is located:** Cyber infrastructure on the premises of a diplomatic mission or consular post is protected by the inviolability of that mission or post.*

(٦) المادتان (٢/٢٢، ٢٥) من اتفاقية "فيينا" للعلاقات الدبلوماسية لعام ١٩٦١.

(7) ***Rule (41) of Tallinn Manual 2:** Inviolability of electronic archives: documents, and correspondence Archives, documents, and official correspondence of a diplomatic mission or consular post that are in electronic form are inviolable.*

للمشاركة في التجسس السيبراني ضد الدولة المستقبلة، أو استخدام البنية التحتية الالكترونية للبعثة، في الانخراط في نشاط تجاري مثلاً، أو أيًا مما يتنافي مع الوظيفة الدبلوماسية[١].

وأضافت القاعدة رقم (٤٢) على الدولة المستقبلة التزامًا، بأن تسمح وتحمي الاتصال السيبراني الحر للبعثة الدبلوماسية، أو المركز القنصلي للأغراض الرسمية[٢]، مع عدم جواز استخدام مبعوثي الدول لمباني البعثة الدبلوماسية أو المركز القنصلي، للانخراط في التجسس السيبراني ضد دولة ثالثة، حيث يتعارض ذلك مع الوظيفة الدبلوماسية، ومع واجب المبعوثين ن باحترام قوانين وأنظمة الدولة المستقبلة.

كما قرّرت القاعدة (٤٣) أنه لا يجوز استخدام مباني البعثة الدبلوماسية، أو المركز القنصلي، للمشاركة في أنشطة إلكترونية تتعارض مع الوظائف الدبلوماسية أو القنصلية، ولا يجوز للمبعوثين المشاركة في الأنشطة السيبرانية التي تتدخل في الشئون الداخلية للدولة المستقبلة، أو التي تتعارض مع قوانين وأنظمة تلك الدولة[٣]، كأن يستخدموا وسائل التواصل الاجتماعي، بغرض إقالة حكومة الدولة المستقبلة، أو المشاركة في حملات سياسية لأفراد أو مجموعات في الدولة المستقبلة.

ومن الممارسات الدولية ذات الصلة بالتجسس الدبلوماسي، أنه في عام ٢٠١٣ حركت "تيمور الشرقية"، أمام هيئة التحكيم الدائمة (*PCA*)، دعوى ضد "استراليا"، لإلغاء معاهدة (بحر تيمور)، والتي تم إبرامها بين الدولتين عام ٢٠٠٢، وذلك لقيام عملاء من الاستخبارات الأسترالية ـ بعد تنكرهم كموظفين في شركة إنشاءات تعمل في "تيمور" ـ بتركيب أجهزة تنصت في غرفة اجتماعات مجلس وزراء "تيمور"، وفي مكتب رئيس الوزراء في "ديلي"، ورصدت هذه الأجهزة مداولات تتعلق بموقف "تيمور" من المفاوضات، ومن ثم، حصلت "استراليا" علي معلومات دقيقة عن الاستراتيجيات التي ستنتهجها "تيمور" في التفاوض، ونقاط القوة والضعف المحتملة، وبناء على هذه المعلومات حقَّقت "استراليا" مميزات غير عادلة بشأن حقوقها بموجب المعاهدة[٤].

إلا أن المدير السابق للعلميات الفنية في المخابرات الاسترالية والمعروف بالضابط (*X-AL*) والذي كان مسئولاً عن قيادة عملية التنصت، كشف الواقعة ووثّقَها بأدلة، قدمها إلى "تيمور الشرقية". وعقب ذلك، ألقت الحكومة الأسترالية القبض علي الضابط، وألغت جواز سفره حتى لا يستطيع السفر إلي لاهاي للإدلاء بشهادته، كما داهمت مكتب المحامي "برنارد كولوري" في "سيدني"، وهو الذي يُمثل تيمور الشرقية أمام المحكمة، وعقب هذا الاقتحام، وفي ١٧ ديسمبر من عام ٢٠١٣ حرَّكت دولة "تيمور"

---

(1) ***M. N. SCHMITT, L. VIHUL****, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, P. R., P. 230.*

(2) ***Rule (42) of Tallinn Manual 2:*** *Free communication: A receiving State must permit and protect the free cyber communication of a diplomatic mission or consular post for all official purposes.*

(3) ***Rule (43) of Tallinn Manual 2:*** *Use of premises and activities of officials: (a) the premises of a diplomatic mission or consular post may not be used to engage in cyber activities that are incompatible with diplomatic or consular functions. (b) Diplomatic agents and consular officials may not engage in cyber activities that interfere in the internal affairs of the receiving State or are incompatible with the laws and regulations of that State.*

(4) ***G. DYER****, Australia's Surveillance of East Timor too Shameful to Share, the Telegram (12.12.2013),* ***available at****: http://goo.gl/Chng5Q. 20/3/2020.*

دعوي أخري أمام محكمة العدل الدولية، تتعلَّق باقتحام مكتب المحامي الخاص بها والاستيلاء على مستندات سريَّة تخصها[١].

وخلال مراحل تداول الدعوى، لم تُركّز هيئة التحكيم على إشكالية استخدام معلومات التجسس، في تفاوض دبلوماسي لإبرام اتفاقية دولية، والذي هو لب القضية، ولكنها التزمت ببحث ما طُلب منها فقط، حيث تركَّزت طلبات "تيمور" على تحقيق "استراليا" لمنافع غير عادلة نتيجة إدخال "الغش" في التفاوض، ولم تتضمن هذه الطلبات البت في مشروعية سلوك التجسس الذي مارسته "استراليا" أثناء التفاوض[٢]، كما لم تتضمَّن طلب وقف هذا السلوك، أو التعويض عنه كفعل غير مشروع، وما زالت الدعوى مُعلَّقة حتى بداية عام ٢٠٢٠.

ووفقًا لما سبق، يُمكننا القول بأنه:

أولاً: على الرغم من عدم حظر سلوك التجسس في مجال التبادل الدبلوماسي صراحةً، إلا أن ممارسته لا تتفق ومهام الوظيفة الدبلوماسية، وتُعد تعديًا لحدودها، وتؤثر سلبًا علي العلاقات الودية الدولية، ولم يفرض القانون الدولي عقوبات صريحة على الدبلوماسيين المتورطين في أعمال تتنافى وطبيعة وظيفتهم، إلا أن رد فعل الدول المضرورة يتمثل، وفقًا لاتفاقية "فيينا" للعلاقات الدبلوماسية ١٩٦١، في إخطار الدولة المُستقبلة، لنظيرتها الموفدة بأن هؤلاء الأشخاص "غير مرغوب فيهم"، مع تصريح الأولي بأن أنشطتهم لا تتفق وطبيعة مركزهم الدبلوماسي، ولكن من النادر عملاً أن تُعلن دولة أن نشاط مثل هؤلاء الدبلوماسيين ينتهك القانون الدولي.

ثانيًا: عدم صحة الرؤية الخاصة بأن التجسس يستوفي شرط الاعتقاد القانوني، المتطلب لتكوين العرف الدولي، باعتبار أن هذا السلوك يؤدي إلى توتر العلاقات بين الدول، ولا يتوافق مع القواعد الدولية، لاسيما اتفاقية "فيينا" للعلاقات الدبلوماسية لعام ١٩٦١، التي اعتبرت ممارسته لا تتفق مع المركز الدبلوماسي، وأن من حق الدولة المستقبلة المضرورة، أن تُخطر الدولة الموفدة بأن الدبلوماسي الذي يمارس التجسس شخصًا غير مرغوب فيه، وعادةً ما تُسارع دولته لاستدعائه، حفاظًا على علاقاتها الودية مع الدولة التي وقع فيها الانتهاك.

المبحث الثالث

المسئولية الدولية الناشئة عن العمليات السيبرانية

تُعرف المسئولية الدولية، بأنها الجزاء القانوني الذي يرتبه القانون الدولي العام، على عدم احترام أحد أشخاصه لالتزاماته الدولية[٣]، وعُرِّفت كذلك بأنها: مجموعة القواعد القانونية التي تحكم أي عمل أو

---

(1) ***G. DYER****, Australia's Surveillance of East Timor too Shameful to Share, P. R., Website.*

(2) ***Oral Proceedings,*** *Verbatim Record 2014/1, Case Concerning Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v Australia), CR 2014/1 (2014) 15–16.*

(٣) **د/ عبد العزيز محمد سرحان**، القانون الدولي العام، المجتمع الدولي، المصادر، نظرية الدولة، دار النهضة العربية، القاهرة، ١٩٨٦، ص ٣٨٥.

واقعة تُنسب إلى أحد أشخاص القانون الدولي، وينجم عنها ضرر لشخص آخر من أشخاص القانون الدولي، وما يترتب على ذلك من التزام الأول بالتعويض[١]؟

وتقتصر المسئولية الدولية وبشكل تقليدي، على النوع الذي يمكن تسميته بالعلاجي لا العقابي، والذي يتماثل ـ إلى حد كبير ـ مع نوع المسئولية المدنية للأفراد في الأنظمة الداخلية، حال ارتكابهم أفعال ضارة في حق الغير، حيث يُنشئ هذا النوع من المسئولية التزامًا على الطرف المُخل، بأن يُصلح ما يترتب على إخلاله من أضرار، مع اشتراط حدوث ضرر لشخص دولي، حتى يمكن تحريك دعوى المسئولية المدنية الدولية، أما مع عدم حدوث الضرر فإنه لا يُتصور قيام هذه المسئولية[٢].

وقد صاغت لجنة القانون الدولي مشروعًا تضَّمن (٥٩) مادة، بشأن مسئولية الدول عن الأفعال غير المشروعة دوليًا، واعتمدت عدة مواد منها عام ٢٠٠١، وفي عام ٢٠٠٦، أنجزت مجموعة من مشاريع المبادئ المتعلقة بتوزيع الخسارة، في حالة غياب نشاط خطر يُسبب الضرر العابر للحدود. وفي عام ٢٠١١، اعتمدت مجموعة من مشاريع المواد بشأن مسؤولية المنظمات الدولية، بنفس اتجاه ومبادئ مواد مسئولية الدول[٣].

وفي مجال النزاعات المسلحة، قضت المادة (٣) من اتفاقية "لاهاي" الرابعة، والخاصة بقواعد الحرب البرية لعام ١٩٠٧، بأن: "الدولة التي تُخل بأحكام هذه الاتفاقية تلتزم بالتعويض إن كان لذلك محل، وتكون مسئولة عن الأعمال التي تقع من أي فرد من أفراد قُواتها المسلحة". وقرَّرت المادة (٩١) من البرتوكول الإضافي الأول لعام ١٩٧٧، مسئولية طرف النزاع الذي ينتهك أحكام اتفاقيات جنيف لعام ١٩٤٩، أو برتوكوليها، وكذلك مسئوليته كذلك عن الأعمال التي يقترفها الأشخاص الذين يشكلون جزءًا من قواته المسلحة.

وفيما يتعلق بالمسئولية الجنائية للأفراد، فقد بزغ هذا المبدأ من خلال المحاكمات الدولية الجنائية للأفراد، عن الجرائم المرتكبة خلال الحربين العالميتين، وبدأت معالمه تتضح مع دخول نظام المحكمة الجنائية الدولية حيز النفاذ عام ٢٠٠٢، حيث أصبح من الممكن إثارة المسئولية الجنائية الدولية لممثلي ووكلاء أشخاص القانون الدولي، أو من يتصرفون لحسابهم.

ولتحريك دعوى المسئولية الدولية بين أشخاص القانون الدولي، **يلزم توافر شروط ثلاثة**، أولها ارتكاب فعل غير مشروع دوليًا؛ وتحقق ضرر نتيجة هذا الفعل؛ وأن يُسند هذا الضرر أو يُنسب لشخص دولي، ومن ثم يتم تحريك هذه الدعوى في مواجهة الشخص الدولي الذي أتى هذا الفعل الضار.

وفي مجال العمليات السيبرانية، يدق أمر تقرير المسئولية الدولية، نظرًا لطبيعة هذه العمليات، وخصائصها المُميزة، وتضمنها لبعض الممارسات التي لم يتم تحديد الوضع القانوني الدولي لها، كالتجسس السيبراني، وكذلك ارتكابها بواسطة أفراد أو كيانات بخلاف الدول، باسم الدول ولحسابها، مما

---

(١) **د/ صلاح الدين عامر**، مقدمة لدراسة القانون الدولي العام، دار النهضة العربية، القاهرة، الطبعة الثانية، ١٩٩٥، ص ٧٢٦: ٧٢٧.

(٢) **د/ وائل أحمد علام**، مركز الفرد في النظام القانوني للمسئولية الدولية، دار النهضة العربية، ٢٠٠١، ص٢٢.

(٣) **مشروع مواد لجنة القانون الدولي بشأن مسئولية الدول عن الأفعال غير المشروعة دوليًا لعام ٢٠٠١، وثيقة: (*GA Res 56/83 annex, UN Doc. A/RES/56/83, December 12, 2001*)**

يتطلَّب بحث ما إذا كان يمكن إسناد أفعال هؤلاء الأفراد أو الكيانات إلى الدول، أو المنظمات الدولية[١]، وكذلك بحث إمكانية تقرير مسئولية الأفراد سواء كانوا مرؤوسين أم قادة، من خلال الاختصاص الجنائي الدولي.

ونوالي دراسة المسئولية الدولية عن العمليات السيبرانية، على ضوء مواد لجنة القانون الدولي بشأن مسئولية الدول لعام ٢٠٠١، وكذلك قواعد دليل "تالين"، وذلك على النحو التالي.

المطلب الأول: مسئولية أشخاص القانون الدولي عن العمليات السيبرانية.

المطلب الثاني: المسئولية الفردية ومسئولية القيادة العليا عن العمليات السيبرانية.

المطلب الأول

مسئولية أشخاص القانون الدولي عن العمليات السيبرانية

أوضح دليل تالين، أن مُصطلح الدولة المسئولة، ينصرف إلى التي تنتهك التزامًا دوليًا تجاه دولة أخرى، ويُشار إلى الأخيرة بالدولة المضرورة، وتتحمَّل الدولة المسئولية الدولية عن العمليات السيبرانية التي تُنسب إليها، وتُشكّل خرقًا لالتزام دولي[٢]، ويُعد نسبة أو إسناد الفعل غير المشروع إلى الدول، هو لب تقرير المسئولية، وهو ما أوضحته المادة (١) من مشروع لجنة القانون الدولي بشأن مسئولية الدول، بشأن تحمُل الدولة المسئولية عن أفعالها غير المشروعة دوليًا، التي تُشكّل خرقًا لالتزام قانوني دولي ساري، مع نسبته إليها وفقًا للقانون الدولي[٣].

ونوالي دراسة الفعل غير المشروع دوليًا في مجال العمليات السيبرانية، وكذلك إسناد هذا الفعل إلى الدولة، وذلك من خلال الفروع التالية.

الفرع الأول

الفعل غير المشروع دوليًا في مجال العمليات السيبرانية

يُقصد بارتكاب الدولة فعلاً غير مشروع دوليًا، أن تُخالف التزامًا دوليًا مُقرّرًا عليها، والذي قد يتمثّل وفقًا للمادة (٣٨) من النظام الأساسي لمحكمة العدل الدولية، في التزام تعاهدي كاتفاقية دولية، أو قاعدة عرفية دولية، أو أحد المبادئ العامة للقانون، ولا يُشكّل مصدر الالتزام الذي تم انتهاكه، أي فارق بشأن تقرير مسئولية الدولة[٤]، مع اشتراط أن يكون الالتزام ساريًا بالنسبة لها، في الوقت الذي أتت فيه

---

(١) **امتَّد مفهوم المسؤولية الدولية ليشمل المنظمات الدولية**، وبالفعل انتهت اللجنة حتى عام ٢٠٠٨، من اعتماد (٥٣) مشروع مادة من هذه المواد. **راجع:** تقرير لجنة القانون الدولي، الدورة الثالثة والخمسون ٢٠٠٢، ملحق رقم ١٠، وثيقة (*A/56/10*).

(٢) **القاعدة رقم (٦) من "تالين ١"، والقاعدة رقم (١٤) من "تالين ٢"**، بعنوان المسئولية القانونية للدول.

Rule No. (14) of the Tallinn Manual 2*: Internationally wrongful cyber acts A State bears international responsibility for a cyber-related act that is attributable to the State and that constitutes a breach of an international legal obligation.*

(٣) **المادة رقم (١) من مشروع مواد لجنة القانون الدولي بشأن مسئولية الدول، ٢٠٠١، المرجع السابق.**

(٤) **المادة (١٢) من مشروع لجنة القانون الدولي الخاص بمسئولية الدول. راجع كذلك: د/ أحمد أبو الوفا**، المسئولية الدولية للدول واضعة الألغام في الأراضي المصرية، دراسة في إطار القواعد المُنظمة للمسئولية الدولية وللألغام البرية، دار النهضة العربية، القاهرة، ٢٠٠٣، ص ٢١: ٢٢.

الفعل[١]، ودون حاجة للبحث عن قصدها أو دوافعها، فمعيار عدم المشروعية أمر موضوعي، يتحقَّق بمجرد انتهاك الالتزام.

وقد صدرت عدة أحكام دولية لتقرير المسئولية الدولية، بالتأسيس على نظرية الفعل غير المشروع، ومنها حكم المحكمة الدائمة للعدل عام ١٩٢٨، في النزاع بين "ألمانيا" و"بولونيا" بشأن مصنع "شورزو"، وقررت المحكمة أن مجرد مخالفة التزام دولي، يستتبع الالتزام بالتعويض الكافي. وفي عام ١٩٤٩ قرَّرت محكمة العدل الدولية في قضية "قناة كورفو"، أن "ألبانيا" أخفقت في الوفاء بالتزام دولي، يقضي بإخطار الدول التي تستخدم قناة "كورفو" بوجود ألغام بها. كما أيد الرأي الاستشاري لمحكمة العدل الدولية عام ١٩٤٩، بشأن أهلية الأمم المتحدة في التقاضي ذلك الاتجاه، حيث قضى بأن أي انتهاك لتعهد دولي يرتب المسئولية الدولية[٢]".

وحري بالذكر، أن لجنة القانون الدولي قد اتجهت بشأن المسئولية الدولية، إلى عدم اشتراط الضرر لتقريرها[٣]، حيث تتقرَّر بمجرد مخالفة القانون الدولي، ولا يعني ذلك أن الضرر ليس له دور في إطار المسئولية الدولية، فهو في أغلب الأحوال الضابط الأساسي لتحديد آثار هذه المسئولية، ولكن مجرد وقوعه لا يكفي كقاعدة لتقرير المسئولية ابتداءً، ولابد من تحقق انتهاك التزام[٤].

وفي مجال العمليات السيبرانية، قد يتمثَّل الفعل غير المشروع في؛ قيام سفينة بعمليات سيبرانية ضد دولة ساحلية من داخل بحرها الإقليمي، وبالمخالفة لنظام المرور البريء؛ أو شن هجمات سيبرانية على أهداف مدنية أثناء نزاع مسلح؛ أو إتاحة دولة بنيتها التحتية الالكترونية لدول أو كيانات خاصة، أو أفراد، مما يتسبب في الإضرار بدول أخري، مع فشل الدولة صاحبة البنية التحتية في بذل العناية اللازمة لإنهاء هذه العمليات[٥].

وقد تكون العملية السيبرانية غير محظورة دوليًا، إلا أن وسائل تنفيذها تنتهك التزامات دولية، وعلى سبيل المثال، عند قيام تبادل تجاري الكتروني بين دولتين، ولكي تُعظّم إحداها منافعها، تستغل معلومات مُتحصّل عليها من التنصت على المُستخدمين، وبما ينتهك حق الإنسان في الخصوصية[٦]، أو أن تحصل دولة من التجسس السيبراني ـ غير المحظور صراحةً ـ على بيانات تشغيل أنظمة محطة طاقة نووية، ثم تُهدّد بشن عمليات سيبرانية لتدميرها، ما لم تُنْه الدولة صاحبة المحطة، عمليات عسكرية لها في الخارج، أو أن تقوم دولة بعملية سيبرانية ضد أخري، ولكن من داخل إقليم دولة ثالثة دون موافقتها بما يمثل انتهاكًا لسيادة الأخيرة[٧].

---

(١) المادة رقم (١٣) **من مشروع مواد لجنة القانون الدولي بشأن مسئولية الدول، ٢٠٠١، المرجع السابق.**
(٢) **مجموعة أحكام محكمة العدل الدولية في الفترة من ١٩٤٩: ١٩٩٢.**
(٣) **ما لم يكن شرطًا مسبقًا لوصف الفعل بأنه غير مشروع دوليًا**، أو يُمثّل أحد عناصر انتهاك قاعدة قانونية أساسية. راجع: المادة (٢) من مواد مسئولية الدول.
(٤) **د/ أحمد أبو الوفا**، المسئولية الدولية للدول واضعة الألغام في الأراضي المصرية، المرجع السابق، ص ١٨.
(5) ***M. J. SKLEROV**, Solving the Dilemma of State Responses to Cyber-attacks: A Justification for the Use of Active Defenses against States Which Neglect Their Duty to Prevent, Mil. L. Rev. 201, 2009, PP. 38:39.*
(6) ***M. N. SCHMITT, L. VIHUL,** Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, P. R., P. 170.*
(7) ***A. DEEKS,** an International Legal Framework for Surveillance, P. R., P. 302.*

كما قد تكون بعض العمليات السيبرانية ضارة أو غير ودية بشكل أو بآخر، ولكنها لا تشكل انتهاكًا لالتزم دولي، فلا تتحمل الدول المسئولية عنها بالمعنى المقصود في قواعد المسئولية الدولية، ومن ذلك، عندما تُعلّق دولة تجارتها الالكترونية مع دولة أخرى، بأن تحجب بعض مواقع التداول التجارية المشتركة، فإن الفعل يُمكن وصفه بأنه غير ودي، وربما يتسبَّب في أضرار اقتصادية، ولكنه بشكل عام لا يُمثّل خرقًا لالتزام دولي[١].

ولا يُعد الضرر المادي كالإصابات أو الوفيات، شرطًا مسبقًا لوصف الفعل السيبراني بأنه غير مشروع دوليًا، وعلى سبيل المثال، أوردت اتفاقية مجلس أوروبا "بودابست" بشأن الجرائم السيبرانية لعام ٢٠٠١، في عدة نصوص منها، بعض الأفعال باعتبارها غير مشروعة دون تطلب وجود الضرر، ومن ذلك ما ورد بالمادتين (٥)، (١/٢٠)، منها، بشأن إعاقة الدول الأطراف لعمل أنظمة الكمبيوتر، أو التدابير الأخرى، المتعلقة بجمع بيانات حركة تداول البيانات والمعلومات في أوقات معينة.

كما لا يُعد قصد التسبب بالضرر متطلبًا عامًا للفعل غير المشروع دوليًا[٢]، إلا أنه يجب الرجوع إلى الالتزام الأساسي الذي تم خرقه، ولكل حالة على حدة، لتحديد ما إذا كان هذا الالتزام يلزمه عنصر القصد، كما هو الحال مع حظر جريمة الإبادة الجماعية، حيث تتطلب توافر "قصد" تدمير مجموعة معينة، كليًا أو جزئيًا"[٣].

ولا يُشترط الموقع الجغرافي في الفعل السيبراني غير المشروع دوليًا، فقد ينطلق من إقليم الدولة المضرورة، أو إقليم دولة أخرى، أو أعالي البحار، أو المجال الجوي الدولي، أو الفضاء الخارجي، إلا في حالة المرور البريء، حيث يُتطلّب أن تقوم السفينة المعنية، بالعملية السيبرانية في البحر الإقليمي للدولة الساحلية.

وبشأن اعتماد "دليل تالين" للفعل غير المشروع دوليًا، كأساس لتقرير المسئولية الدولية عن العمليات السيبرانية، فإنه ربما يؤدي إلى خروج بعض العمليات غير المحظورة دوليًا، مثل التجسس السيبراني، من نطاق تقرير المسئولية الدولية، بالرغم من أنه من الخطورة بحيث تحتاج الدول إلى آلية دولية للمساءلة بشأنه، وجبر ما قد ينتج عنه من أضرار.

الفرع الثاني

إسناد الفعل إلى أشخاص القانون الدولي

خلصت لجنة القانون الدولي في مشروعها بشأن مسئولية الدول عام ٢٠٠١، إلى أن العنصر الثاني لتقرير المسئولية الدولية، بعد تحقق الفعل غير المشروع دوليًا، هو إسناد أو نسبة هذا الفعل إلى الدولة، ووفقًا للمواد من (٤: ١٩) من المشروع، يتحقّق ذلك، بصدور الفعل من السلطة التشريعية، أو القضائية، أو التنفيذية، أو من أفراد عاديين، أو أفعال ثوار، وحركات العصيان، باعتبار أن هذه الفئات

---

(1) ***M. N. SCHMITT, L. VIHUL,*** *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, P. R., P. 86.*

(٢) **المادة رقم (٢) من مشروع مواد لجنة القانون الدولي بشان مسئولية الدولة عن الأفعال غير المشروعة دوليًا..**

(٣) **مما نصت عليه المادة الثانية من اتفاقية منع الإبادة الجماعية** لعام ١٩٤٨، أنه: "في هذه الاتفاقية، تعني الإبادة الجماعية أياً من الأفعال التالية، المرتكبة بقصد التدمير الكلي أو الجزئي لجماعة قومية أو إثنية أو عنصرية أو دينية، بصفتها هذه.....".

تمثل أجهزة الدولة، أو تتصرف نيابة عنها، حتى لو تجاوزت تصرفاتها حدود ما رسمه القانون الداخلي أو خالفته[١].

وبالنظر إلى أن كثير من العمليات السيبرانية، تُنفذ من قبل كيانات خاصة أو أفراد، تستخدمهم الدول أو المنظمات الدولية لهذا الغرض، فإن إسناد هذه العمليات يواجه إشكاليات، تتعلَّق بصعوبة تطبيق المعايير التقليدية لإثبات الصلة بين تلك الفئات وشخص القانون الدولي، وكذلك مدى انطباق مفهوم "أجهزة الدولة" أو "وكلاء الدولة" عليهم، أو كونهم مخولين بموجب القانون الوطني، بممارسة سلطة حكومية بطبيعتها، وبالتالي اعتبارهم كأجهزة الدولة[٢]، أو كونهم قاموا بالعمل غير المشروع تحت سيطرة الدولة أو رقابتها[٣].

ولدراسة هذه الإشكاليات، واحتمالات إسناد العمليات السيبرانية إلى أشخاص القانون الدولي، والقواعد التي تحكم كل حالة، نُفرد النقاط التالية:

أولاً: المسئولية في حالة وجود علاقة قانونية بين القائم بالعملية السيبرانية وشخص القانون الدولي:

(١) مسئولية الدول عن اضطلاع أجهزة تابعة لها بعمليات سيبرانية غير مشروعة:

قضت المادة (١/٤) من مشروع لجنة القانون الدولي بشأن مسئولية الدول، بإسناد أي تصرف قام به أي جهاز من أجهزة الدولة بصفته هذه إلى الدولة، سواء كان الجهاز يمارس وظائف تشريعية، أو تنفيذية، أو قضائية، أو أية وظائف أخرى، وأيًا ما كان مكانه في الهيكل التنظيمي للدولة، وسواء كانت أحد أجهزة الحكومة المركزية، أو من أجهزة وحدة إقليمية من وحدات الدولة.

ونلاحظ أن مفهوم "أجهزة الدولة" وفقًا للمادة (١/٤) مُوسَّع، بحيث ينطبق على كل الأشخاص، أو الكيانات، التي تتمتع بهذا الوضع بموجب قوانين الدولة الداخلية، بغض النظر عن وظيفتها، أو مكانها في التسلسل الهرمي الحكومي[٤]، وهو نفس الاتجاه الذي اعتمده دليل "تالين ٢"، في قاعدته رقم (١٥) بعنوان: إسناد العمليات السيبرانية من قبل أجهزة الدولة، بأن" "العمليات السيبرانية التي تجريها أجهزة الدولة، .....، تُعزى إلى الدول". مع اتفاق أعضاء فريق (*IGE*) مع ما أقرَّته لجنة القانون الدولي، من أنه لا يمكن لدولة، أن تتجنب المسئولية عن تصرف جهاز تابع لها، بحرمانه من هذا الوضع بموجب تشريع خاص[٥].

---

(١) **حيث تُسأل الدولة عن الخطأ الذي يرتكبه موظفوها خلال ممارستهم لأعمالهم،** إذا كانوا مخولين سلطة تنفيذ أوامرها، كما تُفترض مسئوليتها إذا كانت مذنبة في اختيارهم، وفي الرقابة عليهم، وفي التعليمات الصادرة إليهم. **راجع: د/ أحمد أبو الوفا،** القانون الدولي والعلاقات الدولية، القانون الدولي والعلاقات الدولية، دار النهضة العربية، القاهرة، ٢٠٠٦، ص ٥٠٨: ٥٠٩.

(٢) **المادة رقم (٥) من مشروع مواد لجنة القانون الدولي بشأن مسئولية الدول، ٢٠٠١، المرجع السابق.**

(3) ***ICJ Genocide judgment,*** *paras 399:401;* ***ICTY Tadić decision****, paras 131, 145.*

(٤) **وذلك وفقًا لنص المادة (٢/٤) من مشروع مواد لجنة القانون الدولي بشأن مسئولية الدول،** ٢٠٠١، المرجع السابق.

(5) ***Rule No. (15) Tallinn Manual: Attribution of cyber operations by State organs****: Cyber operations conducted by organs of a State, or by persons or entities empowered by domestic law to exercise elements of governmental authority, are attributable to the State.*

وعلى الرغم من أن العمليات السيبرانية لها طبيعة سريَّة، وبما يشمل الأجهزة القائمة بها، إلا أنه في بعض الحالات يكون من الواضح، أن جهازًا معينًا يضطلع بعمليات سيبرانية حكومية، كوحدات الحرب الالكترونية للدول، أو المؤسسات التقنية المعنية بالإشراف على العمليات السيبرانية للدول[١]، وفي هذه الحالة، فإن ما يصدر عن ذلك الجهاز من أفعال، يعتبر صادرًا عن الدولة ويُنسب إليها، وإذا شكَّلت هذه الأفعال محلاً للمسئولية الدولية، فإن الدولة هي التي تتحمل عبء هذه المسئولية[٢].

وبشكل تقليدي، يُمثِّل استخدام أصول حكومية لاسيما العسكرية منها، مؤشرًا لا يمكن دحضه بشأن الإسناد، نظرًا لعدم إمكان استخدامها إلا من قبل الدولة، وفي سياق العمليات السيبرانية، لا يُمكن تطبيق هذا الافتراض بسهولة[٣]، فقد تسيطر دولة أو فرد، أو كيان بخلاف الدولة، على بنية الكترونية حكومية، ويتم استغلالها للقيام بعمليات سيبرانية، وهنا فرَّقت القاعدة رقم (٧) من "تالين ١"، بين العمليات التي تنطلق من بنية الكترونية حكومية، والتي تنطلق من بنية الكترونية بخلاف الحكومية، بحيث لا يكفي انطلاق العملية، من البنية السيبرانية "الحكومية" لدولة، كدليل لإسناد هذه العملية إليها، وإنما يُمكن اعتبار ذلك بمثابة إشارة أو قرينة، بأن الدولة المعنية قد تكون مرتبطة بالعملية[٤].

وعلى سبيل المثال، قام بعض الطلاب الأمريكيين عام ١٩٩٨، بهجوم سيبراني عُرف باسم "*Solar Sunrise*"، حيث اقتحموا الأنظمة الالكترونية لوزارة الدفاع الأمريكية، بواسطة أجهزة كمبيوتر مقرها دولة الإمارات العربية المتحدة[٥]. وكذلك خلال عام ٢٠١٣، تم شن عمليات إلكترونية عدائية، أسفرت عن تخريب مواقع الكترونية للحكومة الأوكرانية، ود بدا أنها تنطلق من مركز الدفاع السيبراني لحلف الناتو، ثم قام المهاجم بتوجيه جزء من نفس العمليات ضد موقع حلف "الناتو"، وجعل الأمر يبدو، كما لو أن الحكومة الأوكرانية هي التي قامت به، وبالتالي يواجه الإسناد ـ بشكل صحيح ـ في مثل هذه الحالات صعوبة كبيرة[٦].

وفيما يتعلَّق بوضع جهاز تابع لدولة تحت تصرف دولة أخري، فقد نصت المادة رقم (٦) من مشروع مواد مسئولية الدول، بعنوان تصرفات الأجهزة التي توضع تحت تصرف الدولة من قبل دولة أخري: "يُعتبر فعلاً صادرًا عن الدولة بمقتضى القانون الدولي، تصرف جهاز يوضع تحت تصرف هذه الدولة من قبل دولة أخرى، إذا كان هذا الجهاز يمارس اختصاصات السلطة الحكومية، للدولة التي يوضع تحت تصرفها". كما قضت القاعدة (١٦) من "تالين ٢"، بأن العمليات السيبرانية التي يضطلع بها جهاز تابع لدولة، وُضع تحت تصرف دولة أخري لممارسة مهام حكومية بطبيعتها، تُعزي إلى الدولة الأخيرة[٧]،

---

(١) **المادتين (٤)، (٥) من مشروع لجنة القانون الدولي بشأن مسؤولية الدول. راجع كذلك:** الحاشية ١٧٨، التعليق على المادة ٥.

(٢) **د/ وائل أحمد علام**، مركز الفرد في النظام القانوني للمسئولية الدولية، المرجع السابق، ص٢٢.

(٣) **تقرير فريق الخبراء الحكوميين للأمم المتحدة لعام ٢٠١٥، الفقرة (٢٨/و)**، الذي اعتمد على نص دليل تالين ١، القاعدة (٧).

(٤) **قضت القاعدة رقم (٧) من الدليل بعنوان، العمليات السيبرانية التي انطلقت من البنية التحتية السيبرانية الحكومية بأن:** "مجرد انطلاق عملية سيبرانية من البنية الالكترونية لدولة، لا يكون دليلاً كافيًا لإسناد تلك العملية إلى الدولة، وإنما يُمكن اعتبارها إشارة إلى وجود ثمة ارتباط بين العملية والدولة المعنية.

(5) ***S. J. SHACKELFORD, R. B. ANDRES****, State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem, GJIL, 2001, P. 982.*

(6) ***M. N. SCHMITT, L. VIHUL,*** *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, P. R., PP. 91: 92.*

(7) ***Rule No. (16) Tallinn Manual:*** *Attribution of cyber operations by organs of other States Cyber operations conducted by an organ of a State that has been placed at the disposal of*

ولكن باستيفاء شرطين وهما، سيطرتها الحصرية على الجهاز، وأن يتعلَّق الانتهاك بالأعمال التي كلَّفت الدولة الجهاز بها نيابة عنها[١].

ولا يقدح في ذلك، استمرار الدولة المرسلة، في تمويل أو توفير موارد لذلك الجهاز، طالما كانت الدولة المتلقية تمارس سلطة حصرية عليه، ولم تحتفظ الدولة المرسلة بسلطة استدعاء جهازها، أو توجيهه، بشأن الأنشطة التي يمارسها في الدولة المستقبلة، وبمفهوم المخالفة، إذا استمر الجهاز في تلقي تعليمات من دولته فلا تنطبق هذه القاعدة، ومن ذلك، قيام دولة بإرسال فريق دعم فني إلى دولة أخرى، للتعامل مع حادثة إلكترونية، مع تمسك الدولة المرسلة بحصول الفريق على موافقتها، قبل الانخراط في أي مهام تطلبها الدولة المتلقية، وتنفيذها تحت إشرافها، وبالتالي فإن الدولة المُرسلة تحتفظ بالسيطرة على فريقها، وتُسند أعماله إليها.

(٢) مسئولية الدول عن اضطلاع كيانات أو أشخاص بخلاف أجهزتها بعمليات سيبرانية غير مشروعة:

بالنسبة لإسناد الأفعال غير المشروعة دوليًا، التي يقترفها أشخاص أو كيانات نيابة عن الدولة، مع كونهم لا يُعتبرون ضمن الأجهزة التابعة لها، فقد أورد مشروع لجنة القانون الدولي لعام ٢٠٠١، بشأنهم حالتين:

الحالة الأولى: قرَّرتها المادة رقم (٥) من المشروع بحيث: "يعتبر فعلاً صادرًا عن الدولة بمقتضى القانون الدولي تصرف أي كيان لا يُعد من أجهزة الدولة بمقتضى المادة (٤)، ولكن يخوله قانون تلك الدولة صلاحية ممارسة بعض اختصاصات السلطة الحكومية، بشرط أن يكون الكيان قد تصرف بهذه الصفة في الحالة المعينة"، كما قرّرت القاعدة رقم (١٥) من" تالين ٢"، أن العمليات السيبرانية التي يضطلع بها أشخاص أو كيانات مخولة بموجب القانون المحلي لممارسة عناصر السلطة الحكومية، تُعزى إلى الدولة.

وبالتالي، فإنه عند تعاقد الدولة، مع أي شخص أو كيان خاص، وفقًا لتشريعاتها الداخلية، للقيام بمهام حكومية بطبيعتها، تُسند أفعال هذا الشخص أو الكيان إلى الدولة[٢]، باعتبار أنه مُخول بموجب عقد قانوني، بممارسة اختصاصات سلطة حكومية، ومن ذلك، تعاقد دولة مع شخص، أو عدة أشخاص، أو شركة خاصة وفقًا لقواعد القانون الإداري، للقيام بعمليات سيبرانية عسكرية، فتُسند الأفعال غير المشروعة دوليًا التي قد تقع جراء هذه العمليات إلى الدولة، وفي حالة تجاوز هؤلاء الأشخاص أو الكيانات، حدود ما كُلّفوا به، فإن الدولة تتحمل المسئولية أيضًا عن أفعالهم[٣]، كأن تُسند إحدى الدول مهمة الدفاع عن بنيها الالكترونية إلى شركة خاصة، مع اشتراط أن تلتزم الشركة بتنفيذ هذه المهمة وفقًا لتدابير دفاعية لا هجومية، فإذا انخرطت الشركة في الدفاع باستخدام القرصنة، أو المبادرة بالهجوم على شبكات دول أخري، فإن هذه الأفعال تُنسب إلى الدولة.

---

another State are attributable to the latter when the organ is acting in the exercise of elements of governmental authority of the State at the disposal of which it is placed.

(١) **المادة رقم (٦) من مشروع مواد لجنة القانون الدولي بشأن مسئولية الدول**، ٢٠٠١، المرجع السابق.

(٢) **المادة رقم (٥) من مشروع مواد لجنة القانون الدولي بشأن مسئولية الدول**، ٢٠٠١، المرجع السابق.

(٣) **المادة رقم (٧) من مشروع مواد لجنة القانون الدولي بشأن مسئولية الدول**، ٢٠٠١، المرجع السابق.

ومن الأمثلة على الحالة المعروضة، أنه بعد إسقاط السوفييت للطائرة الأمريكية (*U-2*) عام ١٩٦٠، والقبض على قائدها "*Francis Powers*"، اعترف بأن السلطات الأمريكية قد تعاقدت معه لقيادة الطائرة، والتحليق بها فوق الأراضي السوفيتية للتجسس وجمع معلومات عسكرية، واضطر الرئيس الأمريكي وقتها "آيزنهاور"، للاعتراف بالواقعة والتصريح بأنه مسئول عنها مسئولية كاملة، وتعهد بوقف مثل هذه الأعمال باعتبارها مُعادية وغير مقبولة[١].

أما الحالة الثانية: فقد أوردتها المادة رقم (٩) من مشروع لجنة القانون الدولي، وباعتبار صدور الفعل غير المشروع عن الدولة، إذا مارس شخص أو مجموعة أشخاص، بعض اختصاصات السلطة الحكومية في غياب السلطات الرسمية، أو في حالة عدم قيامها بمهامها، وفي ظروف تستدعي ممارسة تلك الاختصاصات". وعلى سبيل المثال، إذا استهدفت برمجيات خبيثة، وسائط اتصال أنظمة الكترونية لدولة بالانترنت، وبحيث يتم تخريبها عند استخدام تلك الوسائط، مما يستوجب أن تقطع الدولة اتصالاتها من خلال الوسائط المُصابة، لتُقلّل حجم الضرر، وتتعامل مع الموقف باستخدام وسائط بديلة، ومع عدم قدرة الدولة على ذلك، فإنها تطلب من كيان خاص أو أفراد التطوع بتوفير وسائط اتصال بديلة غير مصابة، إلى أن تتمكن من معالجة الموقف، وهنا تُسأل الدولة عن أفعالهم، إذا كانت تمثل إخلالاً بالتزام تجاه دولة أخرى[٢].

وتختلف هذه الحالة عن الخاصة بتفويض كيانات قانونًا لممارسة مهام حكومية بطبيعتها[٣]، من حيث إن هذا الحُكم يُشير إلى الحالات التي يقوم فيها الشخص أو الكيان الخاص بمساعدة الدولة مُتطوعًا، لمواجهة العمليات السيبرانية الخطيرة وغير المتوقعة، والتي عجزت الدولة عن التعامل معها، لذلك تقبل تطوع الأفراد أو الكيانات للمساعدة في تجاوز الأزمة، مع اعتبارهم يعملون نيابة عنها.

(٣) بالنسبة للمنظمات الدولية:

أشارت محكمة العدل الدولية، في فتواها الصادرة بشأن "تفسير الاتفاق المبرم في ٢٥ مارس ١٩٥١، بين منظمة الصحة العالمية و"مصر"، فإن المنظمات الدولية ملزَمة بأي التزامات تُفرض عليها بموجب القواعد العامة للقانون الدولي، أو بموجب دساتيرها، أو الاتفاقات الدولية التي تكون طرفاً فيها، وتنتهك المنظمة القانون الدولي عندما تخرق أي من هذه الالتزامات الدولية[٤].

كما أكدت لجنة القانون الدولي، في مشروعها المتعلق بمسئولية المنظمات الدولية لعام ٢٠٠٩، على التزام المنظمات بقواعد القانون الدولي[٥]، ومسئوليتها عن أفعالها التي تمثل انتهاكًا لهذه القواعد، أو من يمثلها أو يُنفذ مهام تحت سيطرتها ورقابتها[٦]. وقد نظم هذا المشروع تقرير مسئولية المنظمات الدولية

---

(١) **تفاصيل الحادث والموقف الرسمي للدولتين**، الفصل الثالث، المبحث الأول، المطلب الثاني.
(٢) **المادة رقم (٩) من مشروع مواد لجنة القانون الدولي بشأن مسئولية الدول**، ٢٠٠١، المرجع السابق.
(٣) **المادة رقم (٨) من مشروع مواد لجنة القانون الدولي بشأن مسئولية الدول**، ٢٠٠١، المرجع السابق.
(٤) **تقرير لجنة القانون الدولي، وثيقة (*A/64/10*)**، الدورة الرابعة والستون للجمعية العامة، ٢٠٠٩، المواد التي اعتمدتها اللجنة بصفة مؤقتة في القراءة الأولى، التعليق على المادة (٤)، ص ٤٨.
(٥) **تقرير لجنة القانون الدولي بشأن مسئولية المنظمات الدولية، وثيقة (*A/64/10*)**، المرجع السابق، ص ٩١.
(٦) **قرَّرت اللجنة في دورتها (٥٤) لعام ٢٠٠٢**، إدراج موضوع "مسؤولية المنظمات الدولية" ضمن أعمالها، وأنشأت فريقاً عاملاً لإعداد تقرير موجز عن نطاق هذه المسئولية، ومضمونها، وكيفية تقريرها، وغيرها من المسائل ذات الصلة، ثم اعتمدت اللجنة في نهاية دورتها (٥٤) تقرير الفريق، وفي الفترة بين عام ٢٠٠٣، وحتى عام ٢٠٠٨، اعتمدت اللجنة مؤقتاً مشاريع المواد من (١ إلى ٥٣).

بحسب الأصل، أو في حالة الوكالة عنها، حيث قررت المادة رقم (٣) منه، مسئولية المنظمات الدولية عن أي فعل غير مشروع دولياً ترتكبه[١]، بشرط توافر العناصر المتطلبة في المادة (٤) من نفس المشروع، وهي إسناد عمل أو امتناع عن عمل إلى المنظمة، وأن يُشكل هذا خرقًا لالتزام دولي مقرر عليها[٢].

وبينت المادة رقم (١/٥) من المشروع، والمتعلقة بالقاعدة العامة لإسناد التصرف إلى المنظمة الدولية، أن أي تصرف يصدر من جهاز، أو وكيل تابع للمنظمة، عند تنفيذ مهامه يعتبر صادراً عن تلك المنظمة بمقتضى القانون الدولي، بغض النظر عن مركز الجهاز أو الوكيل بالنسبة للمنظمة. وقد ذهب جانب فقهي إلى أن مشروع مواد مسئولية المنظمات الدولية بوجه عام، والمادة (١/٥) بوجه خاص، يبتعدان بشأن إسناد انتهاكات القانون الدولي التي تقع من الكيانات الخاصة، والأفراد إلى المنظمات الدولية، حيث لا يوجد نص صريح بذلك، وهو أمر ضروري، عند عملهم بناءً على تعليمات المنظمة أو تحت سيطرتها[٣].

ويُوسّع استخدام المشروع لمصطلح "الوكيل"، من نطاق مسئولية المنظمة، لأنه يشير إلى التمثيل نفسه، بغض النظر عن وضع الممثل، ويتضح هذا المعنى من فتوى محكمة العدل الدولية بشأن نطاق تطبيق المادة (٢٢/٦)، من اتفاقية امتيازات وحصانات الأمم المتحدة، حيث قررت أنه: طبقاً للمعلومات المقدمة من الأمين العام، فقد اضطرت الأمم المتحدة في عدة مناسبات، إلى أن توكل مهمات إلى أشخاص لا يتمتعون بمركز موظفي الأمم المتحدة الرسميين، وأن جوهر المسألة لا يكمن في مركزهم الإداري، وإنما في طبيعة مهامهم[٤].

وهو نفس المعنى الذي أوردته محكمة العدل الدولية، في فتواها بشأن قضية التعويضات عن الأضرار المتكبدة في خدمة الأمم المتحدة، حيث قرّرت أنه: تفهم المحكمة كلمة "وكيل" بأوسع معنى مُطلق، وباعتباره أي شخص، سواء كان موظفًا رسميًا يعمل لقاء أجر أو غير ذلك، وسواء كان مستخدمًا بصفة دائمة، أو غير دائمة، أوكل إليه جهاز من أجهزة المنظمة أداء إحدى وظائفه أو المساعدة في أدائها، وباختصار هو أي شخص يعمل الجهاز من خلاله[٥].

وترتيبًا على ما سبق، ووفقًا لما أورده مقرر لجنة القانون الدولي "جورجيو جيا"، في تقريره الثاني بشأن مشروع مسئولية المنظمات الدولية، تُسأل المنظمة عن أفعال أي أشخاص طبيعيين، أو كيانات تستخدمهم لأداء وظائف معينة لها، أو لجهاز من أجهزتها، وبما يشمل على سبيل المثال، الأفراد أو الكيانات، الذين قد تتعاقد معهم المنظمة للقيام بعمليات سيبرانية، حيث تكون المنظمة مسئولة عما يصدر منهم من أفعال، باعتبار أنهم يعملون كوكلاء تابعين لها.

---

(١) **نصت المادة (٣) من المشروع على أن:** "كل فعل غير مشروع دولياً ترتكبه منظمة دولية تترتب عليه المسئولية الدولية للمنظمة".

(٢) **نصت المادة (٤) من المشروع على أنه:** "ترتكب المنظمة الدولية فعلاً غير مشروع دولياً إذا كان التصرف المتمثل في عمل أو امتناع عن عمل: (أ) يسند إلى المنظمة الدولية بمقتضى القانون الدولي؛ (ب) يشكل خرقاً لالتزام دولي واقع على المنظمة الدولية".

(3) ***N. D. WHITE, S. MACLEOD****, EU Operations and Private Military Contractors: Issues of Corporate and Institutional Responsibility, the European Journal of International Law (EJIL) Vol. 19 No. 5, 2008, P. 976.*

(٤) **تقرير محكمة العدل الدولية عام ١٩٨٩**، ص ١٩٤، الفقرتين ٤٧، ٤٨.

(5) ***ILC Report on the Work of its Fifty-Sixth Session****, UN Doc. A/59/10 (2004), P. 99.*

ثانيًا: المسئولية في حالة خضوع القائم بالعملية السيرانية للسيطرة الفعلية لشخص القانون الدولي:

(١) بالنسبة للدول:

قرَّرت المادة (٨) من مشروع مواد لجنة القانون الدولي لعام ٢٠٠١، أنه: "يعتبر فعلاً صادرًا عن الدولة بمقتضى القانون الدولي، تصرف أي شخص، أو أية جماعة من الأشخاص، إذا كانوا قد تصرفوا في الواقع بناءً على تعليمات تلك الدولة، أو بتوجيه منها، أو تحت رقابتها لدى القيام بذلك التصرف"[١]. أي أن الدولة مسئولة عن فعل أي شخص، أو مجموعة من الأشخاص، إذا ثبت فعليًا أنه هذا الفعل قد نُفذ بناءً على أوامر صادرة منها، أو وفقًا لتوجيهاتها، أو تحت رقابتها، أو ما يمكن أن نطلق عليه، تحت سيطرتها الفعلية.

وبشأن مفهوم السيطرة الفعلية، فقد أشارت غرفة المحكمة الخاصة لسيراليون، إلى أن المقصود بها، "سلطة عليا تصدر أوامر ذات أهمية مصيرية في سير أي عملية، ولهذه السلطة القدرة على اتخاذ إجراءات تأديبية"[٢]. كما أقرت محكمة العدل الدولية في قضية نيكاراجوا عام ١٩٨٦، هذا المعيار كأساس للإسناد، عندما يتعلق الأمر بأفعال أفراد مرتبطين بالدول، وأشارت إلى أن الولايات المتحدة الأمريكية تعتبر مسئولة، عن بعض الأفعال التي قام بها مقاتلو "الكونترا"، حيث تولَّت التخطيط، والتوجيه، ودعم هذه الأفعال، ومارست من الناحية الفعلية درجة من الرقابة، تكفي لتبرير اعتبار هؤلاء المقاتلين قد تصرفوا بالنيابة عنها[٣].

وفي قضية الإبادة الجماعية عام ٢٠٠٧، قررت محكمة العدل الدولية، أنه لأغراض المسئولية الدولية، يُمكن مساواة أي شخص أو مجموعة أشخاص، أو كيانات، بأجهزة الدولة، حتى لو لم يتقرَّر هذا الوضع بموجب القانون الداخلي للدولة، شريطة أن يتصرف هؤلاء وهم يخضعون لدرجة عالية من سيطرة الدولة، وبما يشمل طريقة تنفيذ أفعالهم، وتحديد مسارها، وإدخال عوامل إليها، أو استبعادها منها، والقدرة على الأمر بوقفها، وأوردت المحكمة أن "السيطرة الفعالة"، تفوق "السيطرة العامة"، حيث تُعتبر الأخيرة بمثابة الحد الأدنى للأولي[٤].

وقد اعتمد دليل "تالين ٢"، معيار السيطرة الفعلية بشأن الإسناد، وعلى النحو الوارد في أحكام محكمة العدل الدولية في قضايا "نيكاراجوا"، و"الإبادة الجماعية"، وذلك في القاعدة رقم (١٧) منه[٥]، والتي قضت بأنه: تعزى العمليات السيبرانية التي يقوم بها فاعل من غير الدول، إلى الدولة في حالتين:

---

(١) **المادة رقم (٨) من مشروع مواد لجنة القانون الدولي بشأن مسئولية الدول، ٢٠٠١، المرجع السابق.**

(2) ***Prosecutor v Brima et al****, SCSL-04-16-T, 20 June 2007, para. 789.*

(٣) **حكم محكمة العدل الدولية في قضية "نيكاراجوا" ١٩٨٦،** *(Nicaragua v. United States)*، الفقرات ٦٢: ٦٤.

(4) ***Application of the Convention on the Prevention and Punishment of the Crime of Genocide*** *(Bosnia and Herzegovina v. Serbia and Montenegro), Judgment of 11 July 1996, Paras. 404: 406.*

(5) ***Rule No. (17) Of the Tallinn Manual 2****: Attribution of cyber operations by non-State actors Cyber operations conducted by a non-State actor are attributable to a State when: (a)*

(أ) المشاركة بموجب تعليماتها أو تحت توجيهها أو سيطرتها؛

(ب) أن تعترف الدولة بالعمليات وتعتمدها بصفتها هي.

وترتيبًا على ذلك، فإنه في حالة السيطرة الفعلية لدولة على عمليات سيبرانية، يضطلع بها فاعل من غير الدول، فإن الدولة تكون مسئولة عما قد ينتج عن تلك العمليات من أفعال غير مشروعة دوليًا، حتى مع عدم وجود علاقة قانونية مباشرة تربطها بالفاعل، على اعتبار أنه يتصرف بناءً على تعليمات الدولة، وبإشرافها وتحت قيادتها، ويُعد هذا المعيار ضمانة لتلافي الحالات، التي قد تلجأ فيها بعض الدول للتعاقد مع كيانات خاصة أو أفراد، لتجنب تقرير مسئوليتها الدولية.

وتشمل هذه القاعدة أي جهات بخلاف الدول، سواء الأفراد، أم الكيانات، ولا تتطلَّب شروطًا معينة في هاتين الفئتين، كأن تكون الكيانات قد تم تأسيسها وفقًا لقانون وطني، ولها شخصية قانونية وطنية، ولها تسلسل قيادة واضح، أو على درجة من التنظيم، أو أن يعمل الأفراد منفردين، أو في مجموعات، أو ضمن منظمات إجرامية في مجال تكنولوجيا المعلومات، أو إرهابيين إلكترونيين، وكل ما هو مُتطلَّب أن تمارس الدولة سيطرة فعلية على تلك الفئات، ومن ثم، تتحمل المسئولية عن أفعالهم غير المشروعة دوليًا[١].

ومن الأمثلة على السيطرة الفعالة في مجال العمليات السيبرانية، الحالة التي تخطط فيها دولة وتشرف، من خلال شركة وطنية، على إنتاج تحديثات ضارة لبرامج الكترونية، تتسبَّب في إتلاف البرامج المُحمَّلة على أجهزة الكمبيوتر الحكومية لدولة أخري، أو عند تعاقد الدولة مع شركة خاصة لدعم قواتها المسلحة، ثم إصدار أوامر لهذه الشركة للقيام بعمليات سيبرانية، تُمثِّل انتهاكًا للالتزامات الدولية للدولة تجاه دولة أخرى، وذلك بتوجيه برامج ضارة لتدمير بعض النظم الالكترونية للأخيرة، وفي الحالتين تُعزى أفعال الشركة إلى الدولة المُسيطرة.

وكذلك عندما تأمر الدولة شركة ببدء عمليات الكترونية ضد دولة أخرى، بغرض الدفاع عن نفسها، كإجراء قانوني مُضاد ومشروع دوليًا، إلا أن البرامج الضارة التي تستخدمها الشركة في الدفاع، تنتشر وتصيب أنظمة الكترونية لدولة ثالثة، وتتلفها أو تدمرها، وهنا يُعزى تضرر أنظمة الدولة الثالثة إلى الدولة المُستخدمة للشركة، على الرغم من أن تجاوز الضرر لدولة ثالثة لم يكن يمثِّل جزءًا من التعليمات الصادرة للشركة، إلا أنه يرتبط بالعملية التي كُلّفت بتنفيذها.

ومن ناحية أخري، فإن مشاركة الدولة ودعمها لتمويل، وتنظيم، وتدريب، وإمداد، وتجهيز كيان خاص للقيام بعملية سيبرانية، وفقًا لطريقته الخاصة، وباختيار أهدافه، وتخطيط عملياته، لا يصل بالعلاقة مع الدولة إلى درجة السيطرة الفعلية، كما لا تكفي ملكية الدولة لشركة تكنولوجيا معلومات، ليتم إسناد أفعالها إلى الدولة، وإنما يجب أن يتحقق شرط تنفيذ العمليات السيبرانية تحت سيطرتها الفعلية[٢]، وكذلك

---

engaged in pursuant to its instructions or under its direction or control; or (b) the State acknowledges and adopts the operations as its own.

(١) **التعليق على لمادة رقم (٨) من مشروع مواد لجنة القانون الدولي بشأن مسئولية الدول**، ٢٠٠١، المرجع السابق.

(٢) **المادة رقم (٨) من مشروع مواد لجنة القانون الدولي بشأن مسئولية الدول**، ٢٠٠١، المرجع السابق.

عندما تأمر الدولة شركة بإدخال برامج ضارة، إلى الشبكات الحكومية لدولة أخري، ثم يختلس أحد موظفي الشركة البرمجيات الضارة لاستهداف دولة ثالثة، فلا تُنسب العملية إلى الدولة[١].

وفيما يتعلَّق بإسناد العمليات السيبرانية للدولة، في حالة اعترافها بالعمليات واعتمادها بصفتها، وفقًا للقاعدة (١٧) من "تالين ٢"، فهو تأكيد لما أوردته المادة رقم (١١) من مشروع مواد لجنة القانون الدولي لعام ٢٠٠١، باعتبار أن الفعل صادر من الدولة إذا اعترفت بالسلوك المعني واعتمدته، كما اعترفت محكمة العدل الدولية بهذا الأساس كقانون دولي عرفي في قضية رهائن طهران، حيث قرّرت أن "إيران" تتحمل المسئولية عن احتجاز رهائن أمريكيين خلال عامي ١٩٧٩، ١٩٨١، بالأخذ في الاعتبار موافقة أجهزة الدولة الإيرانية وسلطاتها المختلفة على هذا الفعل[٢].

(٢) بالنسبة للمنظمات الدولية:

قضت المادة رقم (٦) من مشروع لجنة القانون الدولي بشأن مسئولية المنظمات، بأن أي فعل لجهاز تابع لإحدى الدول، أو وكيل تابع لمنظمة دولية، يوضع تحت تصرف منظمة دولية أخرى، يعتبر بموجب القانون الدولي، صادر عن هذه الأخيرة، إذا كانت تمارس السيطرة الفعلية على ذلك الجهاز أو الوكيل[٣].

ومن ثم، فإنه في الحالة التي تمارس فيها المنظمة الدولية السيطرة الفعلية، على شخص أو كيان خاص، لدي اضطلاعه بعمليات سيبرانية، فإن أفعاله تُسند إلى المنظمة، حتى لو كانت قد تمت من خلال مستويات قيادية متعددة ومتدرجة، طالما ظلت المنظمة الدولية هي السلطة العليا لهذه المستويات القيادية[٤].

وقد أشار الأمين العام للأمم المتحدة إلى معيار السيطرة الفعلية في مجال عمل الأمم المتحدة، بأنه حاسم فيما يتعلق بالعمليات المشتركة، حيث تتحمَّل المنظمة مسئولية الأنشطة الحربية التي تقوم بها قوات تابعة لها، إذا كانت العمليات تتم حصرًا تحت قيادتها وسيطرتها، وفي العمليات المشتركة، تُسأل الجهة التي تتولي القيادة والسيطرة التشغيلية، وفي حال عدم وجود ترتيبات بهذا الشأن، يتم الحكم على كل حالة وفقًا لدرجة السيطرة الفعلية التي يمارسها أي من الأطراف[٥].

كما أشارت المحكمة الأوروبية لحقوق الإنسان عام ٢٠٠٧، في قضية "*Behrami and Saramati v France, Germany and Norway*"، إلى مفهوم المادة رقم (٤) من مشروع لجنة القانون الدولي بشأن مسئولية المنظمات الدولية، بحيث يتم إسناد المسئولية إلى منظمة الأم المتحدة، عن

---

(1) ***M. N. SCHMITT, L. VIHUL****, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, P. R., P. 98.*

(٢) **المادة رقم (١١) من مشروع مواد لجنة القانون الدولي بشأن مسئولية الدول**، ٢٠٠١، المرجع السابق.

(٣) **وثيقة الأمم المتحدة (*A/51/389*)**، الفقرتان ١٧، ١٨، ص ٥، ٦.

(4) ***J. V. ARBUCKLE,*** *Military Forces in 21st Century Peace Operations, No Job for a Soldier? Routledge, 2006, PP. 121: 123.*

(5) ***G. GAJA,*** *Fifth Report on Responsibility of International Organizations, UN Doc. A/CN.4/583, 2 May 2007, P. 15.*

عدم إزالة القنابل العنقودية في كوسوفو، في فترة ما بعد الانسحاب الصربي في يونيو عام ١٩٩٩، وليس إلى فرنسا، التي لا تعدو كونها دولة مساهمة كانت تنشر قواتها في المنطقة المعنية[١].

وفي حكم أصدرته محكمة لاهاي الابتدائية، بشأن إسناد تصرف وحدة عسكرية هولندية ضمن قوات الأمم المتحدة، وتضمن الحكم إشارة إلى مشروع مواد لجنة القانون الدولي، ثم خلص إلى أنه ينبغي تقييم تصرفات الوحدة، باعتبارها ضمن قوات الأمم المتحدة، وأن قيامها بفعل أو امتناعها عنه، ينبغي أن يُسند من حيث المبدأ إلى الأمم المتحدة، أما إذا كانت السلطات الهولندية قد أصدرت تعليمات إلى وحدتها، بتجاهل أوامر المنظمة أو عصيانها، وانصاعت الوحدة لهذه التعليمات، فإن ذلك يهدم أساس إسناد الفعل إلى الأمم المتحدة، إلا أن المحكمة لم تر ما يكفي من الأدلة لإثبات هذا الاستنتاج"[٢].

وترتيبًا على ما سبق، تكون المنظمة الدولية مسئولة عن الأفعال أو الامتناع عنها، التي تشكل خرقًا لالتزام دولي، والتي قد تصدر مما قد يوضع تحت تصرفها وسيطرتها الفعلية من أجهزة أو كيانات[٣]، أي أن سيطرة المنظمة الفعلية على من هم تحت سيطرتها، هي المعيار في تحديد المسئولية عن الأفعال غير المشروعة، وإذا لم تمارس المنظمة الدولية السيطرة فلا تتحمل المسئولية عن أي انتهاك قد يقع من هذه الفئات.

وبوجه عام، وفيما يتعلَّق بالإسناد في مجال العمليات السيبرانية، يمكن القول بأنه:

(١) في الممارسة العملية، لا يمكن أن يتوافر إسناد قاطع بشأن العمليات السيبرانية، أو أدلة دامغة على تورط دولة ما، ولا يتبقي أمام الدول المضرورة، في كثير من الأحيان، إلا اللجوء إلى اعتماد تدابير أمنية مُحكَمة للنظم الالكترونية، ومطالبة الدولة التي انطلق منها الهجوم بإجراء تحقيقات ومقاضاة المهاجمين.

(٢) يكون من المفيد إعمال قواعد "المسئولية المفترضة"، التي أقرتها اتفاقية مجلس أوروبا "بودابست" عام ٢٠٠١، بشأن الجرائم الحاسوبية، حيث قضت بإسناد العمليات السيبرانية إلى الدولة التي تنطلق منها، بغض النظر عما إذا كان هناك تمويه أو خداع بشأن هذا المكان، استنادًا إلى إخفاق الدولة في الالتزام بواجب منع استخدام أراضيها لمهاجمة الدول الأخرى، وعدم اكتراثها، أو فشلها في التحقق من ذلك، أو ملاحقة المهاجمين، وتكون هناك قرينة مُفترضة بوجود تعاون بين الدولة والمهاجمين[٤].

وبخلاف مسئولية الدولة أو المنظمة الدولية، أوردت المادة رقم (٦٥) من مشروع لجنة القانون الدولي بشأن مسئولية المنظمات الدولية، حكمًا يتضمن عدم إخلال مواد المشروع، بأي مسألة تتصل بمسئولية أي فرد يتصرف نيابةً عن منظمة دولية أو دولة من الدول، وهو ما نتناوله بالدراسة من خلال المطلب الآتي.

---

(1) ***App. Nos. 71412/01 and 78166/01****, Behrami and Saramati v France, Germany and Norway , ECHR Grand Chamber Decision, 2 May 2007 (Admissibility)., Para 133.*

(2) ***Judgment of 10 September 2008****, case no. 265615/HA ZA 06-1671, paras. 4, 8, 14,* ***available at:*** *http://zoeken.rechtspraak.nl.19/5/2013.*

(٣) **مشروع المواد بشأن مسؤولية المنظمات الدولية**، المادة ٦، الحاشية ١٧٩.

(4) ***V. J. PROULX****, Babysitting Terrorists: Should States Be Strictly Liable for Failing To Prevent Transborder Attacks? Berkeley J. Int'l L. 23, 2005, P. 635.*

المطلب الثاني

المسئولية الفردية ومسئولية القيادة العليا عن العمليات السيبرانية

تنطبق قواعد القانون الإنساني الدولي على كل الجهات الفاعلة فيه، ويمتثل لها جميع الأفراد ذوي الصلة بالنزاع، بغض النظر عن وضعهم، وسواء كانوا يمثلون أنفسهم أو يمثلون دولة، أو منظمة دولية، وقد قررت اتفاقات جنيف لعام ١٩٤٩، مسئولية الأشخاص الذين يقترفون أو يأمرون باقتراف انتهاكات جسيمة لنصوصها أثناء النزاع المسلح الدولي[١].

ويتجسد مفهوم هذه المسئولية، في مُساءلة أي فرد، عما قد يرتكبه من أفعال مجرمَّة أو انتهاكات جسيمة للقانون الدولي، سواء اقترفها بنفسه، أو اشترك فيها، ويُعاقب إذا أُدين، بغض النظر عن توصيف هذا الفعل في القانون الداخلي، ودون اعتبار لوضع الشخص كرئيس أو مرؤوس. ونوالي دراسة مسئولية الأفراد، وكذلك القادة والرؤساء من خلال الفرعين التاليين.

الفرع الأول

المسئولية الفردية للقائمين بعمليات سيبرانية

برز مبدأ المسئولية الجنائية الفردية الدولية، مع محاكمة العسكريين الألمان لارتكابهم جرائم في الحرب العالمية الأولى، ثم ترسَّخ من خلال المحاكمات عن جرائم الحرب العالمية الثانية في "نورمبرج"، و"طوكيو"، ومن ذلك، قضى المبدأ الأول من لائحة محكمة "نورمبرج" بأن: أي شخص يقترف فعلاً يعد جريمة بموجب القانون الدولي، يكون مسئولاً، ومن ثم يكون عرضه للعقوبة، كما أشارت المحكمة إلى أن جرائم القانون الدولي ترتبط بأشخاص، لا كيانات مجردة، وينبغي إنفاذ الأحكام الدولية، تحقيقًا للردع، وضمانًا للامتثال للقانون الدولي[٢].

وقد قررت المواد (٤٩، ٥٠، ١٢٩، ١٤٦) من اتفاقيات جنيف لعام ١٩٤٩، الأولى والثانية والثالثة والرابعة، على التوالي، بتعهد الأطراف المتعاقدة باتخاذ أي إجراء تشريعي يلزم لفرض عقوبات جزائية فعالة على الأشخاص الذين يقترفون أو يأمرون باقتراف إحدى المخالفات الجسيمة لهذه الاتفاقيات، مع التزام كل طرف بملاحقة المتهمين باقتراف هذه المخالفات، أو من أمر باقترافها، وتقديمهم إلى المحاكمة أيًا كانت جنسيتهم، أو أن يسلمهم إلى طرف متعاقد معني آخر لمحاكمتهم، طالما توافرت لدى هذا الطرف أدلة اتهام كافية ضدهم.

وأقرّت المادة رقم (٢٥) من النظام الأساسي للمحكمة الجنائية الدولية، بعنوان "المسئولية الجنائية الفردية"، مسئولية الأفراد عن الجرائم التي تدخل في اختصاص المحكمة، وقرَّرت في فقراتها (١)، (٢)، (٣)، اختصاص المحكمة بشأن الأشخاص الطبيعيين، وبالتالي، فإن كل من يرتكب جريمة تدخل في اختصاص المحكمة، يكون مسئولاً عنها بصفته الفردية وعرضه للعقاب، سواء ارتكبها منفردًا، أو

---

(١) **المواد (٤٩، ٥٠، ١٢٩، ١٤٦)** من اتفاقات جنيف الأولى والثانية والثالثة والرابعة، على التوالي.

(2) ***Trial of the Major War Criminal before the International Military Tribunal**, Nuremberg, 14 November 1945-1October 1946, published in Nuremberg, Germany, 1947, P. 223.*

بالاشتراك، أو عن طريق شخص آخر، أو أمر بارتكابها، أو حث على ارتكابها، أو قدّم العون أو التحريض أو المساعدة بأي شكل آخر، لغرض تيسير ارتكاب الجريمة أو الشروع في ارتكابها.

وقد أكدت دائرة استئناف المحكمة الجنائية الدولية لرواندا "*ICTR*" في قرارها الخاص بقضية "*Akayesu*، أن مصداقية القانون الدولي الإنساني ستتراجع، وتصبح قواعده عرضة للتشكيك، إذا تم تبرئة بعض الأشخاص من المسئولية الجنائية الفردية، عن انتهاك المادة (٣) المشتركة في اتفاقات جنيف ١٩٤٩، بذريعة أنهم لا ينتمون إلى فئة معينة، فعلاقة الانتماء الخاصة هذه لا تعد شرطًا لتطبيق المادة (٣) المذكورة[١].

وكررت دائرة الاستئناف للمحكمة الجنائية الدولية ليوغوسلافيا السابقة "*ICTY*" نفس المبدأ، عندما أقرّت مسئولية الفرد الجنائية عن التعذيب، مع عدم اشتراط كونه موظفًا عامًا[٢]، كما توسعت غرفة الاستئناف لنفس المحكمة في حكمها الصادر في قضية "دوشكو تاديش"، في فهم متطلبات قيام جريمة الفرد، لتشمل المساعدة والتحريض بأي فعل، يعد دعمًا أو تشجيعًا، ماديًا أو معنويًا، لارتكاب جريمة معينة، وأن يؤدي هذا لارتكاب الفاعل الأصلي للجريمة، وقررت المحكمة أنه: "بالرغم من أن المتهم لم يضطلع بطريق مباشر في الأفعال المدعى بها، إلا أنه يظل مسئولاً إذا استطاع ممثل الادعاء أن يثبت انه: (١) شارك عن وعي في التخطيط أو التحريض أو الأمر أو ارتكاب أو بشكل آخر في المساعدة أو الدعم ارتكاب الجريمة. (٢) أن هذه المشاركة قد أدت بطريقة مباشرة وبصفة أساسية إلى ارتكاب الجريمة[٣].

وقد أقرَّت القاعدة رقم (٨٤) من "تالين ٢"، المسئولية الجنائية الفردية، عن العمليات السيبرانية التي قد تُشكّل جرائم حرب[٤]، أو انتهاكات جسيمة لقانون النزاعات المسلحة، واتفق فريق (*IGE*) على أن هذه الجرائم تُجسّد الانتهاكات الجسيمة، التي وردت في المواد (٥٠)، (٥١)، (١٣٠)، (١٤٧) من اتفاقيات جنيف لعام ١٩٤٩، من الأولي إلى الرابعة على التوالي، وكذلك المادة رقم (٨٥) من البروتوكول الإضافي الأول لعام ١٩٧٧، بشأن جرائم الحرب، كما اتفق (*IGE*) على أن الجرائم المنصوص عليها في المادة رقم (٨) من نظام روما الأساسي، بشأن النزاعات المسلحة الدولية وغير الدولية، تُشكّل أيضًا جرائم حرب، وأن الأفعال التي تُرتكب بوسائل إلكترونية يمكن اعتبارها جرائم حرب، لأن قانون النزاعات المسلحة ينطبق على وسائل وأساليب الحرب الجديدة، حتى التي لم تكن قد ظهرت وقت صياغة هذا القانون.

---

(1) ***ICTR, Prosecutor v. Jean-Paul Akayesu****, Case No. ICTR-96-4-T, Judgment, 2 September 1998, paras. 443 – 631.*
(2) ***ICTY, Prosecutor v. Kunarac, Kovac and Vukovic****, Case IT-96-23 & IT-96-23/1-A, Judgment (Appeals Chamber), 12 June 2002, para. 148.*
(3) ***ICTY Appeal Chamber,*** *Prosecutor v. Tadic, s upra note 18, at para. 229;* ***ICTY Trial Chamber,*** *Prosecutor v Krnojelac , IT-97-25, judgment, 15 Mar. 2002, at para. 88.*
(4) ***Rule No. (84) of Tallinn Manual 2:*** *Individual criminal responsibility for war crimes Cyber operations may amount to war crimes and thus give rise to individual criminal responsibility under international law.*

الفرع الثاني

مسئولية القيادة العليا في سياق العمليات السيبرانية

بموجب المادة (٢/٨٦) من البروتوكول الإضافي الأول لاتفاقيات جنيف لعام ١٩٤٩، يمكن للدول تقرير المسئولية الجنائية الفردية للرؤساء، عن أي خرق لأحكام هذه الاتفاقيات من قبل مرؤوسيهم، إذا كان هؤلاء الرؤساء يعلمون، أو توافرت لديهم معلومات في ذلك الوقت، وفشلوا في اتخاذ التدابير الممكنة وفي وسعهم عمليًا لمنع هذا الانتهاك، كما وسَّعت المادة (١/٨٧) من البرتوكول، من مسئولية الرؤساء لتشمل الأشخاص الآخرين الخاضعين لسيطرتهم[١].

كما قررت المادة رقم (٢٧) من النظام الأساسي للمحكمة الجنائية الدولية، مبدأ عدم جواز الاعتداد بالصفة الرسمية لدفع المسئولية، وتطبيق هذا النظام على جميع الأشخاص، دون تمييز بسبب صفة الشخص الرسمية، وسواء كان رئيسًا لدولة، أو حكومة، أو عضوًا في حكومة أو برلمان أو ممثلاً منتخبًا أو موظفًا حكوميًا، لا تعفيه بأي حال من الأحوال من المسئولية الجنائية بموجب هذا النظام الأساسي، كما أنها لا تشكل في حد ذاتها سببًا لتخفيف العقوبة".

وأكَّدت المادة رقم (٢٨) من النظام الأساسي للمحكمة، بعنوان "مسئولية القادة والرؤساء الآخرين"، على مسئولية القادة والرؤساء عن الجرائم التي يقترفها من هم تحت إمرتهم أو رئاستهم، ودخولها ضمن اختصاص المحكمة؛ إذا علم ذلك القائد، أو تجاهل عن وعي، أن قواته ترتكب، أو أنها على وشك ارتكاب إحدى هذه الجرائم، ولم يستخدم سلطته لمنع هذه الجرائم أو عرض المسالة علي السلطات المختصة للتحقيق والمقاضاة[٢].

وفيما يتعلق بالعمليات السيبرانية، فقد تناولت القاعدة (٢٤) من "تالين ١"، والقاعدة (٨٥) من "تالين ٢"، المسئولية الجنائية للقادة والرؤساء، من حيث تَحمُلهم المسئولية، عن إصدار أوامر بشن عمليات سيبرانية تُشكّل جرائم حرب، وذلك في حالة علمهم، أو وجوب علمهم، بسبب الظروف السائدة في ذلك الوقت، بأن مرؤوسيهم كانوا يرتكبون، أو على وشك ارتكاب، أو ارتكبوا جرائم حرب، وفشل القيادة في اتخاذ التدابير المعقولة والمتاحة، لمنع هذه الجرائم، أو معاقبة المسئولين عنها[٣].

وغني عن البيان، أن تقرير المسئولية الدولية لا يُعد غايةً في حد ذاته، وإنما يكون الهدف منه هو تطبيق آثار هذا التقرير، والتي تتعلق بجبر كامل الأضرار التي لحقت بالمضرور، وذلك بطرق مختلفة،

---

(1) ***Prosecutor v Enver Hadzihasanovic**, Mehmed Alagic and Amir Kubura, Decision on Interlocutory Appeal Challenging Jurisdiction in Relation to Command Responsibility, Case IT-01-47-AR72, Decision of 16 July 2003.*

(٢) **قررت المادة (٢/٢٨) من النظام الأساسي للمحكمة الجنائية الدولية، مسؤولية الرئيس عن جرائم مرؤوسيه** الخاضعين لسلطته وسيطرته الفعليين، في الحالات التالية: أ- إذا كان قد علم أو تجاهل عن وعي أية معلومات تبين بوضوح أن مرؤوسيه يرتكبون أو علي وشك أن يرتكبوا هذه الجرائم. ب- إذا تعلقت الجرائم بأنشطة تندرج في إطار المسئولية والسيطرة الفعليتين للرئيس. ج- إذا لم يتخذ جميع التدابير اللازمة والمعقولة في حدود سلطته لمنع أو قمع ارتكاب هذه الجرائم أو لعرض المسألة على السلطات المختصة للتحقيق والمقاضاة.

(٣) **قضت القاعدة رقم (٢٤) من الدليل بعنوان المسؤولية الجنائية للقادة والرؤساء، بأنه**: أ- يتحمل القادة والرؤساء المسئولية الجنائية، لإصدار أوامر بالعمليات السيبرانية التي تُشكّل جرائم حرب. ب- يكون القادة مسئولين جنائيًا إذا كانوا يعلمون، أو كانوا عليهم أن يعلموا بسبب الظروف السائدة في ذلك الوقت، بأن مرؤوسيهم يرتكبون أو على وشك ارتكاب، أو ارتكبوا جرائم حرب، وأخفقوا في اتخاذ التدابير المعقولة والمتاحة، لمنع ارتكاب هذه الجرائم أو معاقبة المسئولين عنها.

كالرد العيني، أو التعويض، أو الترضية، أو الجمع بينها جميعًا، وكذلك متابعة الدولة لواجبها بالوفاء بالالتزام الذي تم خرقه، ووقف الفعل غير المشروع[١].

ويعني الرد: التزام الدولة المسئولة عن فعل غير مشروع دوليًا، بإعادة الحال إلى ما كان عليه قبل ارتكاب الفعل غير المشروع دوليًا، بشرط أن يكون هذا الرد غير مستحيل ماديًا، ولا يستتبع عبئًا لا يتناسب مع المنفعة المترتبة على الرد[٢]. **أما التعويض؛** فيتحقَّق بدفع مبلغ مالي عِوضًا عما أصاب المضرور من أضرار مادية ومعنوية[٣]، وذلك حيث لا يكون الرد مُتاحًا، مع إمكان تقييم الضرر ماليًا، بما يشمل ما فات المضرور من كسب مؤكد، وما لحق به من خسارة[٤]. **ويتم اللجوء إلى الترضية،** غالبًا في حالات وقوع ضرر معنوي أو أدبي، والتي ربما لا يمكن للتعويض المالي أو الرد جبرها، ومن أمثلة ذلك، قيام الدولة المسئولة بتقديم اعتذار رسمي، أو الإقرار بالانتهاك، أو التعبير عن الأسف لوقوع الفعل، بل إن إعلان القضاء الدولي عدم مشروعية فعل دولة معينة يُعد في حد ذاته نوعًا من الترضية للدولة المُنتصفة[٥].

كما تستمر الدولة المسئولة في الوفاء بالالتزام الذي انتهكته، والكف عن الفعل غير المشروع، مع تقديم الضمانات الكافية لعدم تكرار هذا الفعل، كالتعهد بعدم التكرار، أو الإدلاء بتصريح دبلوماسي بهذا المعنى، وأهمية هذه الضمانات أنها تشكل التزامًا جديدًا على عاتق الشخص الدولي بالإضافة للتعهد الذي تم انتهاكه[٦].

---

(١) **المواد (٢٩)، (٣٠)، (٣١) من مشروع لجنة القانون الدولي لعام ٢٠٠١**، المرجع السابق.
(٢) **المادة (٣٦) من مشروع لجنة القانون الدولي لعام ٢٠٠١**، المرجع السابق.
(٣) **د/ صلاح الدين عامر**، مقدمة لدراسة القانون الدولي العام، المرجع السابق، ص ٧٦٣.
(٤) **د/ أحمد أبو الوفا**، المسئولية الدولية للدول واضعة الألغام في الأراضي المصرية، المرجع السابق، ص ٢٤.
(٥) **د/ صلاح الدين عامر**، مقدمة لدراسة القانون الدولي العام، المرجع السابق، ص ٧٦٤. **ومن الأمثلة على ذلك**: ما أوردته محكمة العدل الدولية في قضية مضيق كورفو عام ١٩٤٩، حينما ذهبت إلى أن تدخل بريطانيا في مضيق ألبانيا لإزالة الألغام، دون موافقة هذه الأخيرة يعتبر مخالفة أو انتهاكًا لسيادة ألبانيا، وأضافت المحكمة أن هذه الملاحظة تُشكل في حد ذاتها ترضية ملائمة لحكومة ألبانيا، أي أن هذه الترضية تتم لمجرد أن أعلى هيئة قضائية دولية أكدت على وجود انتهاك للسيادة الألبانية. **راجع: د/ أحمد أبو الوفا**، المسئولية الدولية للدول واضعة الألغام في الأراضي المصرية، المرجع السابق، ص ٢٥.
(٦) **د/ وائل أحمد علام**، مركز الفرد في النظام القانوني للمسئولية الدولية، المرجع السابق، ص ٣٧.

الخـــاتمـة

عرضنا في هذا البحث لموضوع العمليات السيبرانية، مع التطبيق على سلوك التجسس وقت السلم، وذلك علي ضوء القواعد الدولية السارية، وقواعد دليل "تالين" بإصداريه عامي ٢٠١٣، ٢٠١٧، وتمت الدراسة من خلال فصول ثلاثة، درسنا في الأول منها، القانون الدولي والعمليات التي تتم من خلال الفضاء السيبراني، وبيَّنا ماهية هذا الفضاء، وأنواع الانتهاكات التي تتم من خلاله، ومدي انطباق القانون الدولي الساري على تلك الانتهاكات، ثم عرضنا لبعض جهود التعاون الدولي بشأن تنظيم العمليات الرقمية والسيبرانية.

وانتقلنا في الفصل الثاني لدراسة التنظيم القانوني الدولي الساري بشأن التجسس، من خلال التطرق إلي عرض وتحليل ماهية التجسس، وأنواعه، ودوافع ممارسته، والوضع القانوني للتجسس في القانون الدولي، ثم انتقلنا لتحليل خصوصية تنظيم سلوك التجسس من البحار وقت السلم، حيث أوردت اتفاقية قانون البحار ١٩٨٢، بعض النصوص الخاصة بحظر جمع المعلومات في وقت السلم، وتعرضنا لإشكالية مدى إمكان اعتبار ذلك حسمًا لمشروعية التجسس دوليًا.

وعرضنا في الفصل الثالث للوضع القانوني الدولي للتجسس السيبراني، ومسئولية الدول عن العمليات السيبرانية، من خلال التعرض لمدي اعتبار التجسس السيبراني تدخلاً غير مشروع في شئون الدول، أو مدى إمكان تأهله كعرف دولي. وانتقلنا لبيان جوانب وأحكام المسئولية الدولية الناشئة عن العمليات السيبرانية، والآثار المترتبة على تقرير هذه المسئولية.

وقد بينت الدراسة الجوانب المختلفة لهذا الموضوع، بدايةً من التعرف على الفضاء السيبراني، والعمليات التي قد تتم من خلاله، ومدي اعتبارها مُكافئة للهجمات المسلحة التقليدية، ومرورًا بالقواعد الدولية المتعلقة بممارسة التجسس، وانتهاءً بدراسة قواعد المسئولية الدولية ذات الصلة، ويُمكن أن نجمل أهم النتائج التي توصلت الدراسة لها، على النحو التالي:

أولاً: النتائج:

(١) يُعرف الفضاء السيبراني بأنه بيئة رقمية غير مادية، تتشكّل عند تشغيل العنصر البشري لعناصر الكترونية مادية، كأجهزة الحاسب الآلي المُتصلة بشبكة الانترنت، والتقنيات والبرامج الخاصة بالتشغيل والاتصال، بحيث يمكن التواصل بين الأفراد، والكيانات، والدول، وكذلك تداول، وتخزين قدر هائل من المعلومات، التجارية أو الاقتصادية، أو الاجتماعية، أو الثقافية، أو العسكرية، أو الدبلوماسية، أو الاستخباراتية، أو الشخصية، أو غيرها. ومن طبيعة الفضاء السيبراني، عدم وجود أي حدود جغرافية له، أو مكان مُعيّن، أو زمان مُحدّد، فهو موجود حيثما وُجدت شبكة الانترنت، ولا تملكه أو تتحكم فيه أي جهة أو كيان، وتُعد المعلومات المُدخلة إليه، والمُخزَّنة عليه، والمتداولة من خلاله، هي لغة التعامل فيه، والمبدأ الذي يحكم تعاملاته، هو حرية تداول المعلومات ونقلها.

(٢) بالرغم من كون الفضاء السيبراني بيئة افتراضية، إلا أنه يخضع في جزء منه، والمتعلّق بمكوناته المادية التي تُنشئه وتُشكّله، ويُطلق عليها "البنية التحتية السيبرانية"، لمبدأ السيادة الإقليمية للدول، **وقد قرَّر دليل "تالين"** حق الدول في ممارسة السيطرة على هذه البنية، والأنشطة المتصلة بها، والتي تتم داخل إقليم الدولة، **ومن ذلك**، حقها في التحكُم في الاتصال بالإنترنت، وأن تقطعه كليًا أو جزئيًا،

وذلك رهنًا بأي قيود اتفاقية أو عرفية دولية، لاسيما في مجال حقوق الإنسان، ولها أن تُخضع هذه البنية، والأنشطة المرتبطة بها، للرقابة القانونية والتنظيمية، وحمايتها، وسواء كانت تلك البنية حكومية، أو خاصة، أو ما إذا كانت الأنشطة تتم من قبل أجهزة الدولة، أو من أفراد عاديين أو كيانات أخري.

(٣) قد يُستخدم الفضاء السيبراني لأغراض عدائية أو عسكرية، وذلك بتوجيه عمليات مثل التسلل السيبراني، أو الجرائم السيبرانية، أو الهجمات السيبرانية، أو الحرب السيبرانية، أو التجسس السيبراني، إلى إي مجال آخر، بري، أو بحري، أو جوي، أو حتى في الفضاء الخارجي، وذلك بواسطة دولة، أو مؤسسة، أو كيان، أو فرد، ومن خلال إرسال برامج ضارة لأي جهاز حاسب آلي، وتخريب المعلومات المُخزَّنة عليه، أو التجسس عليها، أو سرقتها، وقد ينتج عن هذه العمليات آثارًا جسيمة، تكافئ ما قد ينتج عن استخدام القوة التقليدية، مثل التَحكم في أنظمة تشغيل مؤسسات الدول الحيوية، أو تدميرها، أو تعطيلها، مما قد ينتج عنه وفيات،أو إصابات أو أضرار واسعة الانتشار، بحيث تتكبَّد الدولة المستهدفة أضرارًا مالية فادحة.

(٤) يُمثِّل التسلل السيبراني خطوة أولي لكافة العمليات السيبرانية، وهو مجرد الدخول إلى الأنظمة الالكترونية لدولة أو كيان أو فرد، وقد يكتفي المُتسلّل بهذا الفعل، أو يُطوّر منه لمتابعة القيام بعمليات أخري، كنقل المعلومات السرية إلى دولة أو كيان أو أفراد، وبما يُطلق عليه التجسس السيبراني، أو ربما تعديل هذه المعلومات، أو تخريبها، أو محوها، أو تخريب أنظمة الكترونية للدولة المُستهدفة، أو تعطيلها، أو التحكم فيها، مما يتسبب في وقوع أضرار ربما تكافئ أو ترقي إلى درجة استخدام القوة المسلحة التقليدية، كما هو الحال في الهجمات السيبرانية، والتي إذا تكررت وتتابعت، سواء كانت دفعة واحدة، أو على عدة مراحل، فإنها تُشكّل حربًا سيبرانية، والتي ربما يتم شنها ضمن نزاع مسلح مادي بين دولتين.

(٥) بدأت محاولات تنظيم الفضاء السيبراني بشكل جزئي، لمواجهة جرائم مُحدَّدة، تتعلَّق بحماية مصالح الأشخاص، وتجسَّدت في اتفاقية مجلس أوربا "بودابست"، بشأن الجرائم المرتكبة عن طريق الإنترنت وشبكات الحاسوب الأخرى عام ٢٠٠١، واتفاقية الاتحاد الأفريقي بشأن الأمن الالكتروني وحماية البيانات الشخصية لعام ٢٠١٤، وقد ركزتا على التصدي للجريمة السيبرانية ذات الصبغة الجنائية، وتجسَّدت الاستجابة الدولية الأهم والأبرز بشأن تنظيم العمليات السيبرانية، في دليل "تالين" للقانون الدولي المنطبق على الحرب السيبرانية، بإصداريه (١)، (٢) لعامي ٢٠١٣، ٢٠١٧ على التوالي، والذي تبني اتجاه إمكان تطبيق بعض أحكام القانون الدولي الساري علي تلك العمليات، أو اعتبار هذه الأحكام نقطة انطلاق مناسبة لتنظيمها، بحيث لا يتوقف الأمر على إبرام اتفاقيات جديدة.

(٦) سعت بعض المنظمات الدولية لتنظيم العمليات السيبرانية، ومنها، منظمة الأمم المتحدة، التي كان يُعد من أبرز جهودها، تشكيل لجنة خبراء عام ٢٠١٩، لصياغة مشروع اتفاقية تنظم العمليات السيبرانية، وكذلك الاتحاد الأوربي، الذي صدَّق على سياسة للدفاع السيبراني عام ٢٠١٤، لدعم الدول الأعضاء في هذا المجال، وتعزيز الأبحاث والعمليات والعلوم المختلفة بشأنه، كما أصدر التوجيه (١١٤٨/٢٠١٦) في ٦ يوليو ٢٠١٦، بشأن تدابير مشتركة تحقق مستوى عالٍ، لأمن الشبكات لجميع دول الاتحاد. وكذلك تبنّي حلف (*NATO*)، إعداد دليل "تالين ١، ٢" لعامي ٢٠١٣، ٢٠١٧، بشأن القواعد المُطبقة على الحرب السيبرانية.

(٧) أوضحت المادة رقم (٣٦) من البروتوكول الإضافي الأول لعام ١٩٧٧ بعنوان "الأسلحة الجديدة"، أن واضعي هذه المعاهدة، يتصورون تغييرات مستقبلية في وسائل وأساليب الحرب، وعليهم أن يتحققوا مما إذا كانت تلك التغييرات محظورة بمقتضى البروتوكول، أو بموجب قواعد القانون الدولي، ويمكن فهم هذا الحكم، باعتبار أن التكنولوجيا المُستحدثة حالاً أو لاحقًا، تدخل ضمن نطاق تطبيق القانون الإنساني، وإن لم يتم النص عليها بشكل مباشر، مع اعتبار قواعده مؤهلة للتعامل مع إدراج أسلحة جديدة، كالعمليات السيبرانية، إذا كانت تستوفي معيار أعمال العنف، وترقي إلى درجة استخدام القوة المسلحة، أو تكافئ الهجوم المسلَّح التقليدي.

(٨) اعتَّد دليل "تالين" بمعيار "نطاق" و"جسامة الآثار"، كمُحدّد لوصف الهجوم المُسلَّح، فإذا أُستخدمت "قوة" بدرجة معينة من الجسامة، وتمت على نطاق واسع، وخلَّفت خسائر في الأرواح، أو تدميرًا للممتلكات؛ فإنها تكافئ الهجوم المسلح، كالهجوم السيبراني الذي يتسبب في إغلاق شبكة لتوليد الطاقة، لأنه قبل تطوير القدرات الالكترونية، لم يكن من الممكن إغلاق مثل هذه الشبكة، إلا من خلال قصف عسكري، أو أيٍ من أشكال الهجوم المسلَّح المادي، ولم يورد الدليل شروطًا لدرجة الإصابة، أو حجم الضرر، أو كونه دائمًا أو مؤقتًا، وبالتالي يمكن أن تكافئ بعض العمليات السيبرانية الهجوم المسلح، حتى ولو لم تشمل أضرارها الوفاة، أو التدمير، ولكنها تؤثر على مرافق حيوية وأساسية للدول أو تُعطلها، بحيث يصير المرفق غير قابل للاستخدام، أو على الأقل يلزمه إصلاحات جذرية ليعمل مرة أخرى.

(٩) أكَّد دليل "تالين" على تطبيق مبادئ القانون الدولي الإنساني على العمليات السيبرانية، خلال أي نزاع سيبراني مسلح، كمبدأ التمييز، والضرورة العسكرية والتناسب، فحظر الهجمات السيبرانية العشوائية، ووسائل أو أساليب الحرب السيبرانية العشوائية بطبيعتها، كأن تستخدم دولة برامج ضارة لاستهداف شبكة أنظمة عسكرية محددة، إلا أن هذه البرامج تنتقل وتنتشر بشكل عشوائي في الشبكات المدنية، وتتسبب في الإضرار بها. كما حظر الهجوم السيبراني الذي يُتوقع أن يتسبب في خسائر عرضية في أرواح المدنيين، أو إصابتهم، أو إلحاق أضرار بأعيان مدنية أو مزيج من تلك الأضرار، مما لا يتناسب مع الميزة العسكرية المتوقعة، أو استخدام وسائل أو أساليب الحرب السيبرانية، التي قد تُسبّب إصابة أو معاناة غير لازمة لتحقيق الهدف من العملية.

(١٠) يكون من الصعب تحديد مدى المشاركة المباشرة في الأعمال السيبرانية العدائية، وذلك على خلاف المشاركين في العداء المسلح ضمن نزاع مسلح مادي، والذين تحددهم لوائح لاهاي لعام ١٩٠٧، واتفاقية جنيف الثالثة لعام ١٩٤٩، كجزء من القوات المسلحة لأحد هذه الأطراف، حيث توجد صعوبة بالغة بشأن تحديد مدى الانخراط والمشاركة المباشرة للأفراد في العمليات السيبرانية، لاسيما ما يتعلَّق بالتعرف على هوياتهم، أو أدوارهم، وبالتالي غموض وضعهم القانوني، وقد قدَّم الفقه اقتراحات تتضمن اعتبار المشاركين في تصميم برامج ضارة، أو تشغيل أنظمة الكمبيوتر الخاصة بالعمليات، ضمن فئة المدنيين المرافقين للقوات المسلحة، وفي بعض الأحوال يمكن تصنيفهم كعلماء أو خبراء في الأسلحة، وبالتالي يُصنَّفوا كمقاتلين، ويُمكن استهدافهم بالعداء، بالنظر إلي أن أدوارهم تساهم بشكل أو بآخر، في تحقيق ميزة عسكرية لأحد أطراف النزاع.

(١١) أجاز دليل "تالين" بإصداريه (١، ٢)، حق الدفاع الشرعي المُقرر في المادة (٥١) من ميثاق الأمم المتحدة، ضد التهديدات السيبرانية، ولكنه اشترط لنشوء هذا الحق، أن يكون في مواجهة تهديد يكافئ القوة المسلَّحة، ومن المتوقع أن ينتج عنه وفيات، أو إصابات، أو أضرار جسيمة للممتلكات

والأعيان، أما العمليات التي لا ينتج عنها مثل هذه الآثار، فلا يُمكن تصنيفها كهجوم مسلح، وبالتالي، لا يجوز استخدام حق الدفاع في مواجهتها، وذلك كعمليات نسخ معلومات، أو سرقتها، أو الحرمان من خدمات الكترونية غير أساسية.

(١٢) توَّسع دليل "تالين" ليستوعب تقرير حق الدول في الدفاع الاستباقي ضد التهديدات السيبرانية، التي تُملي مُتطلبات الضرورة على الدول أن تتصرف للرد عليها، باعتبارها تنطوي على خطر وشيك، وباعتبار أن هذا التصرف هي الوسيلة الوحيدة لحماية مصلحة للدولة، أو أن استباق الهجوم، يمثل آخر فرصة للدولة لاتخاذ تدابير دفاعية فعالة، مع ضرورة توافر شروط ثلاثة: الأول؛ وجود مؤشرات جدية على أن هجومًا محتملاً وشيكًا سينطلق ضد الدولة؛ والثاني: غَلَبَة صفة النزاع المسلح على هذا الهجوم من حيث الآثار المُحتملة؛ والثالث: أن تكون المبادرة بالهجوم تُمثّل آخر فرصة لدي الدولة للدفاع، وإذا لم تغتنمها فلن تتمكن من درء الخطر.

(١٣) يشير مُصطلح التجسس إلى سلوك البحث والتحري عن أمور غير مُتاحة للعيان، والاطلاع على ما يُعد سرًا عند أصحابه، باستخدام أساليب تمويه وخداع، وإدعاء كاذب، مع توافر دوافع أو نوايا عدائية بشأن استغلال هذه المعلومات، ويختلف هذا السلوك عما يُعرف بالاستخبارات أو العمل السري، وتلجأ الدول لممارسة التجسس في أوقات النزاعات المسلَّحة، لتُحقّق ميزات عسكرية وإستراتيجية تساعدها في الانتصار على الخصم، وفي أوقات السلم، تدعم المعلومات المُتحصَّل عليها كفاءة اتخاذ القرارات السياسية والاقتصادية للحكومات، وكذلك دعم قدرة الدول على استخدام حق الدفاع عن النفس، ورصد الامتثال للالتزامات الدولية، وأيضًا دعم أغراض الملاحقة الجنائية الدولية.

(١٤) عالج القانون الدولي اللجوء لوسائل جمع المعلومات أثناء النزاعات المسلحة باعتباره مشروعًا، ولم يرد أي التزام دولي على الأطراف المتحاربة باحترام أراضي أو حكومات الدول المعادية، وأن استخدام الجواسيس يُقبل كخداع مشروع في الحرب ولا يُشكّل مخالفة، مع إمكان فرض عقوبة الإعدام عند إدانة أحد باقتراف التجسس، وعلي الجانب الآخر، لم تتعرَّض القواعد الدولية لتنظيم التجسس وقت السلم صراحةً، ولم تُقرّ المحاكم الدولية، بشأن مشروعيته اتجاهًا صريحًا، باستثناء بعض القواعد التي يمكن إعمالها في هذا المجال، كواجب احترام السيادة والسلامة الإقليمية للدول واستقلالها السياسي، وعلى المستوى الوطني، حرصت الدول على سن تشريعات وطنية تنظم هذا السلوك وقت السلم، وأُعتبر بموجب معظمها ـ إن لم يكن كلها ـ جريمة يُعاقب عليها بأشد العقوبات.

(١٥) تناولت الآراء الفقهية الوضع القانوني للتجسس وقت السلم، من خلال اتجاهات ثلاثة، يري الأول منها أن القانون الدولي لم يحظر هذا السلوك صراحةً وبالتالي يمكن القول بمشروعيته، ويري اتجاه آخر أن التجسس في وقت السلم غير مشروع لكونه ينتهك بعض أحكام القانون الدولي، ويذهب اتجاه ثالث إلى أن لهذا السلوك موقعًا وسطًا بين المشروعية وعدم المشروعية، فلا هو مشروع ولا هو غير مشروع.

(١٦) تتعلَّق اتفاقية قانون البحار لعام ١٩٨٢ بتنظيم البيئة البحرية، وقد وردت أحكامها الخاصة بحظر نشاط جمع المعلومات، في إطار استيفاء شروط التمتع بحق المرور البريء، وليس لعدم مشروعية هذا النشاط، أو لأنه ينتهك قاعدة دولية، فالاتفاقية لم تتطرَّق لتنظيمه أو حسم مدي مشروعيته، وإنما اعتبرت أن القطع البحرية التي تمارسه، لن تتمتع بحق المرور البريء في المساحات البحرية ذات

الصلة، وبالتالي، لا يمكن القول بأن هناك قاعدة صريحة في القانون الدولي تحظر التجسس في وقت السلم.

(١٧) لا يُمكن فهم حكم المادة (١/٨٧) من اتفاقية عام ١٩٨٢، باعتبار أن سلوك التجسس هو أحد عناصر الحق في حرية الملاحة والتحليق، لتناقض هذا الفهم مع نص المادة، ومع فلسفة أحكام الاتفاقية، والتي تشترط إيلاء المراعاة الواجبة لمصالح الدول الأخرى، ولا شك في أن سلوك التجسس لا يراعي مصالح الدول الأخرى، بل إن الاتفاقية تُقرّر عدم استيفاء القطع البحرية لشروط المرور البريء إذا قامت به، في المساحات البحرية للدول الساحلية، ضمانًا لأمن هذه الدول وسلمها، وليس من المنطقي أن تحظره الاتفاقية في بعض المساحات، وتبيحه في مساحات أخري، لأنه في الحالتين يُمثّل تهديدًا لدولة.

(١٨) ركَّزت الصكوك الدولية ذات الصلة بالتجسس، على وسيلة واحدة من وسائل التجسس وهي المصادر البشرية، أو الذكاء البشري، ولم تأخذ في الاعتبار وسائل جمع المعلومات بطرق تقنية حديثة، لاسيما التجسس الذي يتم من خلال تكنولوجيا الاتصالات والمعلومات، كتجسس الاتصالات والإشارات، والتجسس السيبراني، والفوتوغرافي أو من خلال التصوير، وبالتالي لا يدخل سلوك التجسس من خلال الفضاء السيبراني ضمن تنظيم تلك القواعد، حيث إنه لا يعتمد على العنصر البشري المُتسلّل إلى الدولة المضرورة، لممارسة نشاطه السري، وإنما يتم بواسطة أجهزة تقنية متطورة.

(١٩) مثَّل التجسس السيبراني خيارًا جاذبًا للدول، لأسباب عدة؛ منها القانوني، حيث لا توجد صكوك دولية تُنظّمه، أو تُقرّر عدم مشروعيته، ومنها الواقعي، حيث تنخفض المخاطر المرتبطة بممارسته إلى أقصي درجة، مقارنة بالفوائد الجَمَّة المُتحصلة منه، بحساب أن الدول كانت تتعرض لمخاطر كشف الجواسيس، وربما القبض عليهم ومحاكمتهم وإعدامهم، فصار التجسس يتم بأمان من خارج حدود الدولة المستهدفة، مع صعوبة الكشف عن هوية الجاسوس أو التعرف على مكان تواجده؛ ومنها الاقتصادي، حيث تنخفض تكلفة وسائل التجسس السيبراني بالنسبة لنظيرتها التقليدية.

(٢٠) ينطوي التجسس السيبراني على جمع معلومات سريَّة من الدول المُستهدفة، ولا يتمثَّل هدفه الرئيس في إلحاق أضرار مادية فورية أو محددة، أو تعطيل أنظمة الكترونية لتلك الدول، وإنما يتم بنسخ والحصول على معلومات سرية، ويتوافق هذا التعريف مع نظيره الوارد في اتفاقيات القانون الدولي الإنساني، مع افتقار المفهومين إلى حسم إشكالية التجسس في زمن السلم، ويُمثّل التجسس السيبراني جريمة حالة، وأخري مؤجلة، تتمثل الأولي، في الولوج غير المُصرّح به للأنظمة الالكترونية لدولة، والاطلاع على معلومات سريّة، وتتحقّق المؤجلة، عند استخدام هذه المعلومات لاحقًا للإضرار بالدولة المُستهدفة.

(٢١) وفقًا لطبيعة التجسس السيبراني، فإنه وبحسب الأصل لا يُمثّل استخدامًا للقوة، حيث يقتصر على الحصول على معلومات سرية، دون التسبب في أية أضرار "مادية"، وقد استند دليل "تالين" بإصداريه، على معيار النطاق والآثار، لتحديد العمليات السيبرانية التي تكافئ استخدام القوة المسلحة، وقرَّر أن أي عملية سيبرانية تُشكّل استخدامًا للقوة، بالمعنى المقصود في المادة (٤/٢) من ميثاق الأمم المتحدة، إذا كان حجمها وآثارها، قابلة للمقارنة مع الآثار الناتجة عن عمليات غير سيبرانية تستخدم القوة، وبالتالي قد يُكافئ التجسس السيبراني الهجوم المُسلَّح التقليدي، أو يعتبر بمثابة استخدام للقوة العسكرية؛ في

حالة استغلال المعلومات المُتَحصَّل عليها منه، للتسبب في أضرار جسيمة لدولة، كوفاة أشخاص أو إصاباتهم، أو تدمير أعيان.

(٢٢) تخضع المعلومات المُخزَّنة على أجهزة ووسائط، داخل إقليم الدولة نفسها، لسيادة الدولة وولايتها، ويمثّل التجسس عليها انتهاكًا لمبدأ السيادة الإقليمية للدولة، وتدخلاً غير مشروع في شئونها، وتحديدًا انتهاك حقها في أن تقرر بحرية ودون إكراه، من يُرخَّص له للوصول إلى هذه المعلومات، كما قد تُخزِّن الدولة أو تنقل معلوماتها السرية، من خلال أجهزة داخل أقاليم دول أخرى، وفي حالة التجسس على هذه المعلومات، يحق للدولة صاحبة البنية التحتية السيبرانية، أن تحتج بانتهاك سيادتها، أما بالنسبة للدولة صاحبة المعلومات، فلا يوجد أساس قانوني قد تستند إليه، للادعاء بأن سيادتها قد أُنتهكت، إلا أن هناك اتجاهًا يُقرّر أحقيتها في ذلك، بالاستناد إلى اتفاقية الأمم المتحدة بشأن حصانات الدول وممتلكاتها من الولاية القضائية لعام ٢٠٠٤، واتفاقية "فيينا" للعلاقات الدبلوماسية لعام ١٩٦١، والاتفاقية الدولية للاتصالات لعام ١٩٧٣، واتفاقية مناهضة التعذيب وحظر المعاملة القاسية واللاإنسانية والمهينة ١٩٨٤، وحكم محكمة العدل الدولية في قضية "*East Timor v Australia*" عام ٢٠١٤، وقرار لجنة حقوق الإنسان في قضية *(Lopez v. Uru.)* عام ١٩٧٩.

(٢٣) تمارس الدول في كثير من الأحيان، التجسس السيبراني بواسطة كيانات خاصة، أو منظمات إجرامية مُتخصّصة في هذا المجال، لأسباب عدة، منها تجنب تقرير مسئولية الدولة، وكذلك تجنب وقوعها في حرج على مستوى الدولي، عند الكشف عن واقعة التجسس، باعتبارها قد وقعت بمنأى عنها، وبحساب أنه يكون من الصعب تتبع مصدر العملية، أو تحديده، وإذا تم تحديده، أو معرفة تبني الدولة له، يكون الرد صعبًا من الناحية العملية والقانونية، لقيام تلك الكيانات باستخدام أجهزة موجودة على أقاليم عدة دول.

(٢٤) نظَّم دليل "تالين" أحكام المسئولية الدولية عن العمليات السيبرانية عمومًا، والتجسس خصوصًا، وباعتبار أنه وأن كانت بعض العمليات السيبرانية، في حد ذاتها لا تنتهك القانون الدولي، فإن الطريقة التي تتم بها قد تُمثَّل فعلا دوليًا غير مشروع، كانتهاك مبدأ السيادة، وحظر التدخل في حالة التجسس السيبراني، مع تحمل الدولة المسئولية الدولية عن العمليات السيبرانية التي تُنسب إليها، وتُشكّل خرقًا لالتزام دولي، وكذلك تقرير المسئولية الجنائية الفردية، والمسئولية الجنائية للقادة والرؤساء، عن العمليات السيبرانية التي تُشكّل جرائم حرب.

(٢٥) تفتقر بعض الدول إلى تقنيات، تجعلها على علم بالعمليات السيبرانية العدائية، التي تنطلق من إقليمها وتستهدف دولاً أخري، أو تفتقر إلى القدرة على وقف هذه العمليات، أو التعامل معها في وقت مناسب، وذلك بالنظر لسرعة هذه العمليات، والتي قد لا تدوم إلا لأجزاء من الثانية، وهنا ينشأ واجب قانوني على تلك الدول ببذل العناية الواجبة لمنع هذه العمليات، سواء قبل بدايتها، أو عند انطلاقها، أو إنهائها بعد إطلاقها، ونظرًا لأن معيار بذل العناية نسبي، فإن القدر المتيقن للإخفاق في بذل العناية، هو ألا يصدر عن الدولة أي رد فعل، عند علمها بالتخطيط، أو الشروع في هذه العمليات، وفي كل الأحوال، علي الدول أن تتخذ تدابير الحيطة، لمنع انطلاق هذه الهجمات من أراضيها.

(٢٦) تنطبق اتفاقية الأمم المتحدة لقانون البحار لعام ١٩٨٢، على العمليات السيبرانية التي تتم من البحار، أو من خلال بنية تحتية سيبرانية موجودة في البحار، ولا يجوز إجراء عمليات سيبرانية في

أعالي البحار إلا لأغراض سلمية، ولا تُستبعد الأنشطة السيبرانية من نطاق مفهوم الحريات في أعالي البحار، والاستخدامات القانونية الأخرى للبحار، مع التقيد بعدم انتهاك القانون الدولي الساري، ومراعاة الحرية المقررة للدول الأخرى، وضمان ألا تمس أي عمليات سيبرانية بأمن الدولة الساحلية، أو نظامها.

(٢٧) لا يستوفي التجسس السيبراني ركني العُرف الدولي، بالنظر إلى كونه ممارسة سريَّة، لا يُمكن أن يتبلور من خلالها العنصر الموضوعي للعرف، وتوصم على الأرجح بأنها غير مبررة قانونًا، علاوة على أن اعتقاد الدول بشان سلوك التجسس، لا يصب في مصلحة اعتباره عرفًا دوليًا، حيث لا تقبل أي دولة نسبته إليها، وتَّدينه، وتنفي أي صلة به عند كشف واقعة التجسس، ويعبر ذلك عن اعتقاد بخطأ الممارسة لا إلزاميتها. وفيما يتعلق بتبادل معلومات التجسس السيبراني بين الدول، ومنظمة الأمم المتحدة، لاسيما في مجال مكافحة الإرهاب؛ فإنها لا تتم على نطاق واسع، أو بشكل روتيني ومستمر، ولا تُفصح الدول عن وسيلة الحصول عليها.

(٢٨) لا تُقر اتفاقية "فيينا" للعلاقات الدبلوماسية لعام ١٩٦١، ممارسة التجسس في مجال التبادل الدبلوماسي، وعلى الرغم من عدم حظر هذا السلوك صراحةً، إلا أن ممارساته تتنافى مع طبيعة الوظيفة الدبلوماسية وتُعد تعديًا لحدودها، وتؤثر سلبًا علي العلاقات الودية الدولية، **و**لا يفرض القانون الدولي عقوبات صريحة على الدبلوماسيين المتورطين في أعمال تتنافى وطبيعة وظيفتهم، وإنما يتمثل رد فعل الدول المضرورة في هذه الحالة، وفقًا لاتفاقية "فيينا" للعلاقات الدبلوماسية ١٩٦١، في إخطار الدولة المُستقبلة للدولة الموفدة بأن هؤلاء الأشخاص "غير مرغوب فيهم"، مع تصريح الأولي بأن أنشطتهم لا تتفق وطبيعة مركزهم الدبلوماسي، ولكن من النادر عملاً أن تُعلن دولة أن نشاط مثل هؤلاء الدبلوماسيين ينتهك القانون الدولي.

(٢٩) لا يجوز استخدام مباني البعثة الدبلوماسية، أو المركز القنصلي، للمشاركة في أنشطة إلكترونية تتعارض مع الوظائف الدبلوماسية أو القنصلية، ولا يجوز للموظفين الدبلوماسيين والمسئولين القنصليين المشاركة في الأنشطة السيبرانية، التي تتدخل في الشئون الداخلية للدولة المستقبلة، أو التي تتعارض مع قوانين وأنظمة تلك الدولة، كأن يستخدم الدبلوماسيون وسائل التواصل الاجتماعي، بغرض إقالة حكومة الدولة المستقبلة، أو المشاركة في حملات سياسية لأفراد أو مجموعات في الدولة المستقبلة.

(٣٠) للمباني التي توجد فيها بنية تحتية الكترونية للبعثات الدبلوماسية والمراكز القنصلية حُرمة، وترقي العمليات السيبرانية التي تستهدف هذه البنية، لأن تعتبر دخولاً غير مرخص به، وعلي الدولة المُستقبِلة واجب اتخاذ جميع الخطوات اللازمة لحماية المباني والبنية التحتية الالكترونية بداخلها، من أي اقتحام أو تطفل أو ضرر، وفي المقابل لا يجوز للدولة المُرسلة، أن تستخدم تلك المباني، للمشاركة في التجسس السيبراني ضد الدولة المستقبلة، أو أيًا من الممارسات التي تتنافي مع طبيعة الوظيفة الدبلوماسية.

(٣١) تتحمل الدولة المسئولية الدولية عن العمليات السيبرانية، التي تُنسب إليها، وتُشّكّل خرقًا لالتزام دولي، ويُعد إسناد الفعل غير المشروع إلى الدول، هو لب تحمل المسئولية الدولية عن العمليات السيبرانية، بالنظر إلى أن القائمين بها يحرصون على إخفاء هوياتهم ومكان هجومهم، ويستخدمون مظاهر خادعة، لإلصاق الفعل بجهة أو دولة ما، أو يشنون هجماتهم من أجهزة حاسبات داخل أقاليم دول أخرى، وبالتالي يصعب الكشف عن هوياتهم، أو تتبع مصدر الهجمات.

(٣٢) على الرغم من أن بعض العمليات السيبرانية قد تكون ضارة، أو غير ودية بشكل أو بآخر، ولكنها إذا لم تشكل انتهاكًا للقانون الدولي، فإن الدول لا تتحمل أي مسئولية قانونية عنها، بالمعنى الوارد في قواعد المسئولية الدولية، وعلى سبيل المثال، عندما تُعلّق دولة تجارتها الالكترونية مع دولة أخرى، بأن تحجب بعض مواقع التداول التجارية المشتركة، فإن الفعل يُمكن وصفه بأنه غير ودي، وربما يتسبَّب في أضرار اقتصادية، إلا أنه وبشكل عام لا يُمثّل خرقًا لالتزام دولي.

(٣٣) لا يُمثّل الضرر المادي كالإصابات أو الوفيات، شرطًا مسبقًا لوصف الفعل السيبراني بأنه غير مشروع دوليًا، كما لا يُعد قصد التسبب بالضرر متطلبًا عامًا لذلك الفعل، وفقًا لقواعد مسئولية الدولة، مثل إعاقة الدول الأطراف لعمل أنظمة الكمبيوتر، أو التدابير الأخرى، المتعلقة بجمع بيانات حركة تداول البيانات والمعلومات في أوقات معينة.

(٣٤) على الرغم من الطبيعة السرية للعمليات السيبرانية، وبما يشمل الأجهزة أو الوحدات القائمة بها، إلا أنه في بعض الحالات يكون من الواضح، أن جهازًا معينًا يمارس بعض المهام السيبرانية الحكومية، كوحدات الحرب الالكترونية للدول، أو المؤسسات الحكومية المعنية بالإشراف على تلك العمليات لدولة، وفي هذه الحالة فإن ما يصدر عن هذا الجهاز من أفعال، يعتبر صادرًا عن الدولة ويُنسب إليها، وإذا شكَّلت هذه الأفعال محلاً للمسئولية الدولية، فإن الدولة هي التي تتحمل عبء هذه المسئولية. وفي حالة وضع جهاز تابع لدولة، تحت تصرف دولة أخري، لممارسة مهام حكومية، فإن أفعاله تُعزي إلى الدولة الأخيرة، باستيفاء شرطين، وهما، السيطرة الحصرية للدولة على الجهاز، وأن تتعلَّق أفعال الانتهاك بما كُلّف به الجهاز نيابة عن الدولة.

(٣٥) يعتبر الفعل السيبراني الصادر من أي شخص أو كيان ليس من أجهزة الدولة، صادرًا عن الدولة، إذا تم تخويل هذا الكيان صلاحية ممارسة بعض الوظائف الحكومية، وأن يكون قد تصرف بهذه الصفة في الحالة المعينة، وإذا تجاوز هؤلاء الأشخاص أو الكيانات، حدود أو نطاق ما كُلّفوا به، تتحمل الدولة المسئولية عن أفعالهم، وذلك بخلاف ما يتم ممارسته من أعمال خارج نطاق هذا التكليف، كالقيام بجرائم سيبرانية لا علاقة لها بالالتزام مع الدولة، فلا تتحمل الدولة المسئولية عن تلك الأنشطة. كما تعزى العمليات السيبرانية التي يقوم بها فاعل من غير الدول إلى الدولة، بالرغم مع عدم وجود علاقة قانونية مباشرة تربطه بالدولة، وذلك عندما تتم وفقًا لتعليماتها أو تحت توجيهها أو سيطرتها؛ أو اعترافها بالعمليات واعتمادها بصفتها.

(٣٦) أقرَّ دليل "تالين ٢" المسئولية الجنائية الفردية، عن العمليات السيبرانية التي قد تُشكّل جرائم حرب، أو انتهاكات جسيمة لقانون النزاعات المسلحة، كما اتفق فريق (*IGE*) على أن الجرائم المنصوص عليها في المادة رقم (٨) من نظام روما الأساسي، لكل من النزاعات المسلحة الدولية وغير الدولية، تُشكّل أيضًا جرائم حرب، وأن الأفعال التي تُرتكب بوسائل سيبرانية يمكن اعتبارها جرائم حرب، لأن قانون النزاعات المسلحة ينطبق على وسائل وأساليب الحرب الجديدة، حتى التي لم تكن قد ظهرت وقت صياغة هذا القانون.

(٣٧) يتحمل القادة والرؤساء المسئولية الجنائية عن إصدار أوامر بشن عمليات سيبرانية، تُشكّل جرائم حرب، وذلك في حالة علمهم، أو وجوب علمهم، بسبب الظروف السائدة في ذلك الوقت، بأن

مرؤوسيهم كانوا يرتكبون، أو على وشك ارتكاب، أو ارتكبوا جرائم حرب، وفشلهم في اتخاذ التدابير المعقولة والمتاحة، لمنعها، أو معاقبة المسئولين عنها.

وقد بينت الدراسة الجوانب المختلفة لهذا الموضوع، بدايةً من التعرف على ماهية الفضاء السيبراني، والعمليات التي تتم من خلاله، والتمييز بينها وفقًا لخصائصها المُميزة، والأضرار المحتملة لها، وهل تكافئ الهجمات المسلحة التقليدية، ومرورًا بتعريف التجسس، والقواعد الحاكمة له وقت النزاعات المسلحة، واجتهاد الفقه بشأن مشروعيته وقت السلم، ثم دراسة التجسس السيبراني ومدي اعتباره عرفًا دوليًا، وأخيرًا المسئولية الدولية عن العمليات السيبرانية، ونظرًا لما أظهرته الدراسة من خطورة تلك العمليات، فإننا نورد بعض الاقتراحات والتوصيات التي ربما تحقق فاعلية وجدية بشأن التعامل معها دوليًا، وذلك على النحو التالي:

ثانيًا: التوصيات:

(١) تتمثّل الخطوة الأولي المقترحة بشأن التعامل مع العمليات السيبرانية، في التعجيل بالتفاوض على صك دولي بشأنها في إطار الأمم المتحدة، يستند إلى القواعد الدولية السارية لاسيما القانون الدولي الإنساني، وقواعد دليل تالين بإصداريه ٢٠١٣، ٢٠١٧، والتي تعتبر أكثر ملائمة لهذا المجال، وبشكل جزئي على اتفاقيتي مجلس أوربا "بودابست" لعام ٢٠٠١، والاتحاد الأفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات الشخصية لعام ٢٠١٤، مع ضرورة مراعاة ما يلي:

(أ) أن أحكام اتفاقية مجلس أوربا لعام ٢٠٠١، وكذلك الاتحاد الإفريقي لعام ٢٠١٤، تُركّز على الجرائم ذات الصبغة الجنائية، كالانتهاكات الالكترونية لحق المؤلف، والاحتيال الالكتروني، والأفعال الإباحية، وتمثَّل هدفهما الرئيس في إتباع سياسة جنائية لحماية المجتمع من "الجريمة السيبرانية"، ولم تتضمن نصوصهما تمييزًا أو تفرقة بين الجرائم السيبرانية ذات الصبغة الجنائية، وبين ما يستهدف الدول، كالهجمات والحروب السبرانية، والإرهاب السيبراني، والتجسس السيبراني، والتي تختلف طبيعتها وخصائصها عن الجرائم السيبرانية المتعلَّقة بشكل كبير بحماية مصالح الأفراد، وبالتالي ينبغي أن يكون الاعتماد على الاتفاقيتين جزئيًا، فيما يخص الأحكام المشتركة الخاصة بالفضاء السيبراني، أما ما يجب أن يتم التأسيس عليه بشكل كلي، فهو القواعد الدولية السارية، وقواعد دليل تالين بإصداريه ٢٠١٣، ٢٠١٧.

(ب) أهمية تعريف العمليات السيبرانية المختلفة بدقة، والتمييز بينها، وإفراد نصوص خاصة تتناسب مع تعريف وخصائص كل عملية، لاسيما التمييز في المعالجة القانونية بين العمليات ذات الصبغة الجنائية، والتي تتعلَّق باستهداف المعلومات والبيانات الخاصة بالأفراد والشركات والكيانات الخاصة، كالجرائم السيبرانية، وبين العمليات التي تستهدف الدول، وتُمثّل تدخلاً في شئونها وانتهاكًا لسيادتها، كالهجمات السيبرانية، والحرب السيبرانية، والإرهاب السيبراني، والتجسس السيبراني.

(ج) اعتبار العمليات السيبرانية العدائية التي تستهدف الدول، داخلة ضمن نطاق مفهوم الأسلحة الجديدة، وفقًا للمادة رقم من البروتوكول الإضافي الأول لعام ١٩٧٧، وتنظيم حق الدفاع عن النفس في مواجهتها، وفقًا للمادة (٥١) من ميثاق الأمم المتحدة، بشكل تفصيلي، وبحيث يتلاءم مع طبيعة هذه العمليات، من حيث إنها تقع في أجزاء من الثانية، وتكون آثارها وأضرارها قد تحقَّقت.

(د) النص على واجب قانوني على الدول التي تنطلق من أقاليمها عمليات سيبرانية عدائية، ببذل العناية الواجبة لمنعها، سواء قبل بدايتها، أو عند انطلاقها، أو إنهائها بعد إطلاقها، ونظرًا لأن معيار بذل

العناية نسبي، فيكون القدر المتيقن للإخفاق في بذل العناية، هو ألا يصدر عن الدولة أي رد فعل، عند علمها بالتخطيط، أو الشروع في هذه العمليات، وفي كل الأحوال، اتخاذ الدول لتدابير الحيطة، لمنع انطلاق هذه الهجمات من أراضيها.

(ه) تحديد معيار لتقييم متى تكافئ العملية السيبراني، استخدام القوة المسلَّحة، أو تعادل النزاع المسلح التقليدي، ومن المناسب أن يتمثَّل هذا المعيار في جسامة الآثار واتساع النطاق، فإذا تمت العملية السيبرانية على نطاق واسع، وخلَّفت أضرارًا جسيمة كخسائر في الأرواح، أو تدميرًا للممتلكات؛ فإنها تكافئ الهجوم المُسلح، ويكون للدول حق الرد عليها وفقًا لهذا التقييم.

(و) اعتماد قواعد تفصيلية وصريحة، بشأن تفعيل مبادئ القانون الدولي الإنساني في مجال العمليات السيبرانية، لأن القواعد السارية، لا تواكب طبيعة هذا التطور بكل تفاصيله، لاسيما توضيح كيفية تطبيق تلك المبادئ في الحالات التي تكون البنية التحتية السيبرانية المُستهدفة، في خدمة أغراض مدنية وعسكرية على حد سواء، والحالات التي تتطلَّب إعمال حكم المادة (٥١) من الميثاق، والتعامل مع إشكاليات تتبع مصدر العملية السيبرانية، والرد عليه دون غيره، لتجنب وقوع معاناة غير ضرورية، وحالة ما إذا انطوي تحديد هوية المهاجم على قدر من الخطأ، وتم مهاجمة مصدر آخر بالمخالفة لهذا المبدأ، وكذلك ما إذا كان استخدام أسلحة مادية للرد على الهجوم السيبراني، يتوافق مع مبدأ التناسب.

(ز)عند توافر شروط الدفاع وفقًا لحكم المادة (٥١) من الميثاق، في مواجهة العمليات السيبرانية، ينبغي عدم التفرقة في التنظيم القانوني بين الجهات القائمة بها، وسواء كان المهاجم دولة، أو جهة فاعلة تابعة، أو غير تابعة لدولة، لأن طبيعة هذه العمليات تستوجب الرد إلكترونيًا وبسرعة متناهية، ولا تحتمل الانتظار لتمييز الجهة المُهاجمة، وإلا فإن الأضرار تتفاقم، وقد تؤدي لتقويض بعض أنظمة الدولة، مع فقد الدولة ميزة الاستجابة والرد الفاعل في الوقت المناسب.

(ح) تفاديًا لصعوبات إسناد العمليات السيبرانية، التي تستهدف الدول، ويضطلع بها أفراد أو كيانات خاصة، يكون من المناسب، النص على التقييد ـ قدر الإمكان ـ من تفويض المهام السيبرانية التي هي بطبيعتها حكومية، أو الأعمال السيبرانية التي تُمثّل سلطة حكومية، إلى أفراد أو كيانات خاصة.

(ط) إعطاء أهمية قصوى للالتزام بالمراجعة والتقييم المستمر، لكل التطورات التكنولوجية المُستحدثة بشأن العمليات السيبرانية، مع تقييم مدى ملائمة النصوص لتطورات هذا المجال، والعمل على تلافي مواطن الضعف، مع النص على آليات بديلة مناسبة، حتى لا يُنتقص من فاعلية التزامات أو آليات الامتثال للصك الدولي، أو يواجه طعنًا في مشروعيته.

(ي) النص على نماذج من الثغرات الفنية التي يستغلها القائم بالعملية السيبرانية، ضمانًا لمستوى ملائم من الحماية والأمان في هذا المجال، وباعتبار أن هدف هذا الصك هو توقي مخاطر تلك العمليات قبل حدوثها، ويمكن أن يُناط بمؤتمر أطراف الاتفاق، تحديث كل ما يتعلق بهذه المخاطر، وإتاحة المعلومات ذات الصلة بها، والالتزام بالإعلان عن ذلك، وبما يضمن تطوير الامتثال لذلك الصك من جانب أطرافه.

(ك) نظرًا لعدم توافر إسناد قاطع بشأن العمليات السيبرانية، أو أدلة دامغة على تورط دولة ما؛ يكون من الملائم بشأن هذه العمليات، أن يتم العمل بقواعد "المسئولية المفترضة" " *Imputed Responsibility*"، التي أقرتها اتفاقية مجلس أوروبا "بودابست" لعام ٢٠٠١، بحيث يتم إسناد العملية

السيبرانية إلى الدولة التي انطلقت من إقليمها، بغض النظر عما إذا كان هناك تمويه أو خداع بشأن مكان العملية، استنادًا إلى مسئولية تلك الدولة عن الفشل، في تنفيذ واجب منع استخدام أراضيها لمهاجمة الدول الأخرى، وكذلك فشلها في التحقق من وجود عملية عدائية على إقليمها، وفشلها في ملاحقة المهاجمين.

(ل) يكون من المفيد، أن يتضمن هذا الصك جزاءات رادعة، تتصدي بشكل مناسب لحالات عدم الامتثال المتعمد، أو غير المتعمدة على حد سواء، حيث يمكن النص بموجبه على إنشاء سلطة دولية مركزية، تتكون من عدد كبير من الدول الأطراف، مهمتها تلقي حالات خرق الاتفاق، والتهديد بشكل جماعي بالرد على هذا السلوك، بطرق اقتصادية، أو سياسية، أو تجارية، أو غيرها ووفقًا لمبدأ المعاملة بالمثل، لأن تنظيم التجسس يمثل مصلحة عامة دولية، ولا يمكن أن يتجزأ، نتيجة وجود أفعال فردية، أو ثنائية، أو حتى متعددة الأطراف تخرق الامتثال لعدم مشروعيته.

(م) يكون من المناسب، النص على استمرار جهود التعاون بين الدول الأطراف، فيما يتعلَّق بالتحقيق وجمع الاستدلالات، أو تسليم المتهمين باقتراف عمليات سيبرانية عدائية إذا لزم الأمر، للدول المعنية لمحاكمتهم، لتفادي العقبات الإجرائية المُتعلقة باقتراف هذه العمليات، من داخل أقاليم دول مختلفة.

(ن) التشجيع على زيادة البحوث العلمية المتعلقة بتقليل المخاطر الناشئة عن العمليات السيبرانية، ونشرها دوريًا في مؤتمرات أطراف الاتفاقية، لتدريب الخبراء الفنيين لكل دولة عليها، حيث إن ذلك يُعزز من قوة النصوص القانونية التي تنظم هذا المجال.

(٢) تتعاظم الحاجة إلى تكثيف التعاون الدولي في مجال مكافحة العمليات السيبرانية، لاسيما تبادل تقديم الدعم بشأن أمن الشبكات، وتطوير خبرات المختصين في التحقيق في هذه العمليات، وتدريبهم وتعزيز قدراتهم بشأن التعامل معها، لاسيما ما يتعلَّق بوسائل جمع الأدلة الإلكترونية، وكذلك تطوير الوحدات والأجهزة الوطنية، والهياكل المتخصصة بالتعامل مع العمليات السيبرانية داخل هيئات إنفاذ القانون، وأجهزة النيابة العامة، والجهاز القضائي، بحيث تحصل على الخبرات والمعدات اللازمة للتصدي للتحديات التي تفرضها الجريمة السيبرانية، والتي تحتاج إلى درجة عالية من الإبداع والحنكة للتعامل معها.

(٣) بالنظر إلى احتمال عدم فاعلية الحلول القانونية، بشأن المشاكل والأخطار التي تفرضها العمليات السيبرانية؛ فعلى الدول أن تتخذ تدابير حماية ذاتية، من شانها الحفاظ على البني التحتية الالكترونية لمؤسساتها وأنظمتها، ومنها، فكرة أن يكون لدى السلطات الوطنية القدرة على قطع اتصالاتها عن الإنترنت العالمي، لوقف أي عمليات عدائية من خلال شبكة الانترنت، مع وجود آليات مراقبة تُمَكّن هذه السلطة من اتخاذ قرار القطع في وقت مناسب، وتحسين هندسة البرمجيات، بما يشمل استخدام برمجيات ولغات برمجة، يمكنها مواجهة الهجمات السيبرانية وتقييد إمكانات المهاجم.

(٤) يمكن اقتراح إنشاء وكالة خاصة بالرقابة على ممارسة العمليات السيبرانية العدائية، لاسيما التجسس السيبراني وقت السلم، ويكون عملها وفقًا لمقاصد ومبادئ الأمم المتحدة وتحت رقابتها، وتضطلع بالمتابعة المستمرة للعمليات السيبرانية العدائية أو ممارسات التجسس، وتُمنح صلاحيات رصد أي منطقة دون معوقات أو اعتراضات، بالوسائل المناسبة التي تراها، والتأكد من حقيقة المعلومات التي ترد إليها، بما في ذلك القيام بعمليات التفتيش الأرضي داخل الدول المعنية، ويكون لها كذلك صلاحيات الاتصال المباشر بالدول للحصول على استفسارات، أو للإخطار بشأن أي شكوك أو استعدادات قد يقوم بها طرف

ضد آخر، وتُحفظ جميع المعلومات التي تحصل عليها الوكالة بطريقة لا تسمح بالاطلاع عليها لغير المعنيين، وتُعامل وفقًا لأعلى درجات السريَّة والأمانة.

(٥) يكون من المفيد إعادة النظر في مضمون مبدأ عدم التدخل في مجال العمليات السيبرانية، والذي ورد في دليل "تالين، حيث اعتمد عند تصنيف هذه العمليات على "الهدف منها"، أو وقصد التأثير على قرارات وسياسات الدولة، وهو أمر نفسي، ربما يُمكن استجلائه بشأن تعاملات الأفراد، ولكنه صعب التصور في سياق الحديث عن أنشطة الدول، ونظرًا لخطورة تلك العمليات على الدول، يلزم أن يكون مضمون المبدأ مُوسَّعًا، من حيث النظر فيما إذا كانت العملية السيبرانية تنتهك سيادة الدولة؛ فإذا كان من شأنها أن تُقوض أو تعتدي على قيمة سيادة الدولة، فإنها يمثل تدخلاً غير مشروع وإكراهًا للدولة المُستهدفة.

(٦) ضرورة مواصلة الدول لسن تشريعات وطنية، تواكب التطورات المستمرة للعمليات السيبرانية، وتراعي صياغتها المفاهيم التقنية محل التنظيم، وتفي بمتطلبات عمليات التحقيق والإحالة والمحاكمة، وتتسق مع ضمانات الأصول القانونية الواجبة، مع عدم إغفال الشواغل المتعلقة بالخصوصية، وضمان الحريات المدنية، وحقوق الإنسان.

(٧) النص على حظر صريح لسلوك التجسس وقت السلم، بكافة أشكاله ووسائله، واعتباره انتهاكًا للقانون الدولي، مع اقتراح تأسيس عدم مشروعية هذه الممارسة، على مخالفته للمبادئ العامة للقانون، المنصوص عليها في المادة (١/٣٨/ج) من النظام الأساسي لمحكمة العدل الدولية، كأحد مصادر القانون الدولي، حيث إنه إذا أمكن جمع ومقارنة جميع تشريعات التجسس الموجودة في دول العالم، ربما يمكن القول بأن هناك حظر دولي للتجسس، باعتبار أن غالبية القوانين الوطنية ـ إن لم يكن كلها ـ تُجرّم هذا السلوك وتعاقب عليه، وبالتالي يمكن اعتبار أن هذه العمومية في التجريم، تدخل في نطاق مخالفة ممارسة التجسس لهذا المصدر من مصادر القانون الدولي.

(٨) يتمثَّل أحد الجوانب الأساسية للتعامل مع العمليات السيبرانية، في تنمية مستويات الوعي ونشره لدى المواطنين والمؤسسات الوطنية، بشأن المخاطر والتهديدات ذات الصلة باستخدام تكنولوجيات المعلومات والاتصالات، حيث يكون من الضروري وضع خطط توعية وطنية، تتضمن التعريف بماهية هذه العمليات ومدى مشروعيتها، وكيفية التعامل معها على المستوى الفردي، أو الشركات، والكيانات الخاصة، ويمكن أن يتم إدراج موضوع الفضاء السيبراني والعمليات ذات الصلة به، والأمن السيبراني ضمن المناهج التعليمية.

(٩) إنشاء أجهزة تحقيق متخصصة في تطبيق التشريعات السيبرانية، لها خبرات فنية فيما يخص جمع الأدلة وحفظها، والقدرة على تحليلها وتكييفها وتقديمها إلى القضاء، على أن تشمل هذه الأجهزة إلى جانب القانونيين، فنيين متخصصين في مختلف فروع تكنولوجيا المعلومات، كالشبكات المعلوماتية والتجهيزات المعلوماتية وقواعد المعلومات وبرامج الحماية والأمن السيبراني وغيرها من البرامج.

قائمة المراجع

المراجع العربية

أولاً: مراجع عامة:

- **د/ أحمد أبو الوفا**، المسئولية الدولية للدول واضعة الألغام في الأراضي المصرية، دراسة في إطار القواعد المُنظمة للمسئولية الدولية وللألغام البرية، دار النهضة العربية، القاهرة، ٢٠٠٣.
- **د/ صلاح الدين عامر**، مقدمة لدراسة القانون الدولي العام، دار النهضة العربية، القاهرة، الطبعة الثانية، ١٩٩٥.
- **د/ عبد العزيز محمد سرحان**، القانون الدولي العام، المجتمع الدولي، المصادر، نظرية الدولة، دار النهضة العربية، القاهرة، ١٩٨٦.
- **د/ على صادق أبو هيف**، القانون الدولي العام، الجزء الأول، منشأة المعارف، الإسكندرية، الطبعة الحادية عشر، ١٩٧٠.
- **د/ وائل أحمد علام**، مركز الفرد في النظام القانوني للمسئولية الدولية، دار النهضة العربية، ٢٠٠١.

ثانياً: اتفاقات دولية:

- اتفاقية لاهاي الرابعة لعام ١٩٠٧.
- الاتفاقية الدولية بشأن استخدام البث في سبيل السلام ١٩٣٦.
- اتفاقية منع الإبادة الجماعية لعام ١٩٤٨.
- العهد الدولي للحقوق المدنية والسياسية لعام ١٩٦٦.
- الاتفاقية الدولية للاتصالات لعام ١٩٧٣.
- اتفاقيات جنيف الأربع لعام ١٩٤٩.
- اتفاقية منظمة حلف شمال الأطلسي ١٩٤٩.
- معاهدة المبادئ المنظمة لأنشطة الدول في استكشاف واستخدام الفضاء الخارجي لعام ١٩٦٧.
- معاهدة الصواريخ المضادة للقذائف الباليستية، الولايات المتحدة الأمريكية والاتحاد السوفيتي لعام ١٩٧٢.
- البروتوكولين الملحقين باتفاقيات جنيف لعام ١٩٧٧.
- معاهدة الحد من الأسلحة الهجومية الإستراتيجية، الولايات المتحدة والاتحاد السوفيتي، لعام ١٩٧٩.
- اتفاقية الأمم المتحدة لقانون البحار لعام ١٩٨٢.
- اتفاقية الأمم لمتحدة لمناهضة التعذيب وحظر المعاملة القاسية واللاإنسانية والمهينة ١٩٨٤.
- معاهدة السماوات المفتوحة لعام ١٩٩٢.
- النظام الأساسي للمحكمة الجنائية الدولية لعام ١٩٩٨.
- اتفاقية مجلس أوربا "بودابست"، بشأن جرائم الإنترنت، وشبكات الحاسوب الأخرى لعام ٢٠٠١.
- معاهدة الترتيبات البحرية في بحر تيمور، "تيمور – ليشتي، واستراليا لعام ٢٠٠٢.
- اتفاقية الأمم المتحدة بشأن حصانات الدول وممتلكاتها من الولاية القضائية لعام ٢٠٠٤.

- اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية لعام ٢٠١٤.

ثالثاً: رسائل دكتوراه:

- **د. على صادق عبد الحميد صادق،** أمن الدولة في النظام القانوني للهواء وللفضاء الخارجي، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، ١٩٧٩.

رابعاً: المقالات:

- **د. محمد صافي يوسف،** تدابير حماية الأمن القومي كاستثناء على تطبيق قواعد القانون الدولي العام، المجلة المصرية للقانون الدولي، الجمعية المصرية للقانون الدولي، العدد السادس والستون، ٢٠١٠.

خامساً: منشورات للأمم المتحدة:

- **اللجنة الاقتصادية والاجتماعية لغربي آسيا،** الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية: توصيات سياساتية، الأمم المتحدة، نيويورك، ٢٠١٥.

سادساً: أحكام قضائية وتحكيمية دولية:

- المحكمة الدائمة للعدل:

- قضية "لوتس" "فرنسا ضد تركيا" عام ١٩٢٧.

- محكمة العدل الدولية:

- قضية قناة "كورفو" "المملكة المتحدة ضد ألبانيا" لعام ١٩٤٩.
- قضية برشلونة للقوى المحركة "بلجيكا ضد أسبانيا" لعام١٩٧٠.
- قضية التجارب النووية "أستراليا ضد فرنسا" لعام ١٩٧٤.
- قضية الدبلوماسيين الأمريكيين في طهران "الولايات المتحدة ضد إيران"، لعام ١٩٨٠.
- قضية ترسيم الحدود البحرية في خليج "Maine"، لعام ١٩٨٤.
- قضية "نيكاراجوا ضد الولايات المتحدة الأمريكية" لعام ١٩٨٦.
- قضية تطبيق اتفاقية منع الإبادة الجماعية، "البوسنة والهرسك ضد صربيا والجبل الأسود"، لعام ١٩٩٦.
- الرأي الاستشاري بشأن مشروعية استخدام الأسلحة النووية لعام ١٩٩٦.
- قضية الجماهيرية العربية الليبية ضد الولايات المتحدة الأمريكية، لعام ١٩٩٨.
- الرأي الاستشاري بشأن بناء جدار عازل في الأراضي الفلسطينية المحتلة لعام ٢٠٠٤.
- قضية "تيمور- ليشتي" ضد "أستراليا" لعام ٢٠١٤.

- محكمة يوغوسلافيا السابقة:

- ***ICTY, Prosecutor v. Tihomir Blaskic,*** *Case No. IT-95-14-T, 1997.*
- ***ICTY, Prosecutor v. Tadić*** *(Appeal), (IT-94-1), 2001.*
- ***ICTY, Prosecutor v. Kunarac, Kovac and Vukovic****, Case IT-96-23 & IT-96-23/1-A, Judgment (Appeals Chamber), 12 June 2002.*

- ***ICTY Trial Chamber, Prosecutor v Krnojelac*** *, IT-97-25, judgment, 15 Mar. 2002,*
- ***ICTY Prosecutor v. Sesay, Kallon, & Gbao,*** *Case No. SCSL-04-15-T, 43, 2005.*

- محكمة سيراليون:

- ***Appeals Chamber Decision on Challenge to Jurisdiction****: Lomé Accord Amnesty, Case No. SCSL-2004-15-AR72(E) and SCSL-2004-16-AR72(E) at para. 47, 13 March 2004.*
- ***Prosecutor v. Sam Hinga Norman*** (*Case No. SCSL-2004-14-AR72(E)) Decision on Preliminary Motion Based on Lack of Jurisdiction (Child Recruitment), Decision of 31 May 2004.*

- محكمة رواندا:

- ***ICTR, Prosecutor v. Jean-Paul Akayesu****, Case No. ICTR-96-4-T, Judgment, 2 September 1998, paras. 443 – 631.*
- ***ICTR , Prosecutor v. tIie Ndayambaje and Sylvain Nsabimana,*** *Case Nos. ICTR-96-8-T and ICTR-97-29A-T (Nov. 15, 2001).*

- مجلس حقوق الإنسان:

- ***Human Rights Comm.,*** *Commc'n No. 52/1979 (Lopez v. Uru.), U. N. Doc. CCPR/C/13/D/52/1979 (1984),*
- ***App. Nos. 71412/01 and 78166/01****, Behrami and Saramati v France, Germany and Norway, ECHR Grand Chamber Decision, 2 May 2007 (Admissibility).*
- ***U.N. Human Rights Council****, 11th Special Session, the Human Rights Situation in Sri Lanka (May 27, 2009),*

- أحكام تحكيمية دولية:

- قضية المملكة المتحدة ضد الولايات المتحدة الأمريكية لعام ١٨٧٢.
- قضية جزيرة بالماس "هولندا ضد الولايات المتحدة الأمريكية" لعام ١٩٢٨.

المراجع الأجنبية

1- General References:

- ***A. AUST****, Handbook of International Law, 1st. edn. Cambridge University Press, 2005.*

A. CLAPHAM, *Human Rights Obligations of Non-State Actors, Oxford University Press, 2006.*

- ***A. JAMES,*** *Peacekeeping in International Politics, Springer, 2017.*
- ***B. F. HARRIS****, America, Technology and Strategic Culture: A Clausewitzian Assessment, New York, Routledge, 2009.*

- ***D. BETHLEHEM***, *Self-Defense against an Imminent or Actual Armed Attack by Nonstate Actors, 106 AJIL, 2012.*
- ***G. BRITAIN, Ministry of Defence***, *the Manual of the Law of Armed Conflict, Oxford University Press, 2005.*
- ***H. GROTIUS,*** *the Rights of War and Peace, Including the Law of Nature and of Nations, New York: Cosimo, Inc., 2007.*
- ***J. ASHLEY ROACH, ROBERT W. SMITH,*** *Excessive Maritime Claims, Vaughan Lowe & Robin Churchill eds., 3d ed. 2012.*
- ***J. KRASKA***, *Military Operations, in the Oxford Handbook of the Law of the Sea, Donald R. Rothwell et al. eds., 2015.*
- ***J. SCOTT,*** *the Attack on the Liberty: the Untold Story of Israel's Deadly 1967 Assault on A U.S. SPY SHIP (2009).*
- ***J. V. ARBUCKLE,*** *Military Forces in 21st Century Peace Operations, No Job for a Soldier? Routledge, 2006.*
- ***K. IRION,*** *Government Cloud Computing and National Data Sovereignty, Policy and Internet, 2013.*
- ***K. TAKAHASHI, J. HARDY***, *Japan Tracks Suspected Chinese Sub near Okinawa Island, JANE'S DEFENCE WKLY., 2014.*
- ***K. WOLFKE***, *Custom in Present International Law, Works of the Wroclaw Scientific Society, Wroclaw, 1964.*
- ***L. OPPENHEIM,*** *International Law: a Treatise: War and neutrality, Green & Co, H Lauterpacht, ed, 1955.*
- ***R. HIGGINS, P. WEBB, D. AKANDE, S. SIVAKUMARAN, J. SLOAN,*** *Oppenheim's International Law: United Nations, Oxford University Press, 2019.*
- ***S. CHESTERMAN***, *One Nation under Surveillance: A New Social Contract to Defend Freedom without Sacrificing Liberty, Oxford University Press, 2011.*
- ***W. H. BOOTHBY***, *Weapons and the Law of Armed Conflict, OUP, 2nd edn., 2016.*
- ***Y. DINSTEIN***, *the Conduct of Hostilities under the Law of International Armed Conflict, CUP, 3rd, edn., 2016.*
- ***Y. DINSTEIN***, *War, Aggression and Self-Defence, 5th. edn., Cambridge University Press, Cambridge, 2011.*

2- Specialized References:

A. SCHWABACH, *Internet and the Law: Technology, Society, and Compromises, ABCCLIO, California, 2nd., edn., 2014.*

***- C. FOCARELLI**, Self-Defence in Cyberspace, in: N. Tsagourias, R. Buchan (eds), Research Handbook on International Law and Cyberspace, Cheltenham, Edward Elgar, 2015.*

***- C. S. YOO**, Cyber Espionage or Cyberwar? International Law, Domestic Law, and Self-Protective Measures, in: J. D. OHLIN, K. GOVERN, C. FINKELSTEIN (eds), Cyberwar: Law and Ethics for Virtual Conflicts, Oxford University Press, Oxford, 2015.*

***- D. COLE,** Just War and the Ethics of Espionage, Routledge, 1 edition, 2014*

***- D. TURNS,** Cyber War and the Concept of 'Attack' in International Humanitarian Law' in Dan Saxon (ed.) International Humanitarian Law and the Changing Technology of War, Brill, 2013.*

***E. SHOSHAN**, Applicability of International Law on Cyber Espionage Intrusions, Faculty of Law, Stockholm University Press, 2014.*

***- J. E. PRETZ, R. J. STERNBERG,** Cognition and Intelligence: Identifying the Mechanisms of the Mind, Cambridge University Press, 2005.*

***- J. S. GRANICK**, American Spies: Modern Surveillance, Why Should You Care, and What To Do About It, Cambridge University Press, Cambridge, 2017.*

***- G. KERSCHISCHNIG**, Cyber Threats and International Law, Eleven International Publishing, 2012.*

***- G. REYNOLDS,** Ethics in Information Technology, Cengage Learning, Rab. II 14, 2018.*

***- H. H. DINNISS,** Cyber Warfare and the Laws of War, CUP, 2012.*

***- H. LIN, A. ZEGART**, Bytes, Bombs, and Spies, the Strategic Dimensions of Offensive Cyber Operations, BROOKINGS INSTITUTION PRESS, Washington, D.C., 2020.*

***- I. LACHOW,** Cyber Terrorism: Menace or Myth? In: Kramer, Franklin, Starr, Stuart and Wentz, Larry Cyberpower and National Security. Publisher: Potomac Books Inc, US, 2009.*

***- J. CARAVELLI, N. JONES**, Cyber Security: Threats and Responses for Government and Business, ABC-CLIO, LLC, 2019.*

***- K. GEERS**, Cyber War in Perspective: Russian Aggression against Ukraine, NATO CCD COE Publications, Tallinn, 2015.*

***- K. ZIOLKOWSKI**, Peacetime Cyber Espionage, New Tendencies in Public International Law, in K. ZIOLKOWSKI (ed), Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy, 1st edn., NATO CCD COE Publication, Tallinn 1, 2013,*

*- **M. GERCKE**, Understanding Cybercrime: Phenomena, Challenges and Legal Response (ITU): Telecommunication Development Bureau, 2012*
*- **L. K. JOHNSON**, Preface to Strategic Intelligence: Understanding the Hidden Side of Government, Loch K. Johnson ed., 2007.*
*- **M. A. LUSTED, D. HARRIS,** Russian Hacking in American Elections, ABDO, 2019.*
*- **M. HERMAN**, Intelligence Services in the Information Age: Theory and Practice, Routledge, Rab., 2013.*
*- **M. N. SCHMITT**, Rewired Warfare: Rethinking the Law of Cyber Attack, 96 IRRC (893), 2014.*
*- **M. N. SCHMITT, ed.,** Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, Cambridge, 2013.*
*- **M. N. SCHMITT, L. VIHUL,** 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 Defence Centre of Excellence, Cambridge University Press, Cambridge, 2019**.***
*- **M. N. SCHMITT**, Reaction: Cyberspace and International Law: the Penumberal Mist of Uncertainty, 126 HLR F., 2013.*
*- **N. BOOTH,** Lucifer Rising: British Intelligence and the Occult in the Second World War, History Press, 2016.*
*- **N. TSAGOURIAS**, the Legal Status of Cyberspace, in Research Handbook on International Law and Cyberspace, ed. Nicholas Tsagourias and Russell Buchan, Edward Elgar, 2015.*
*- **P. WRANGE**, Intervention in National and Private Cyberspace and International Law, Leiden, Brill, Nijhoff, 2014.*
*- **R. A. FALK, R. J. STANGER,** Essays on Espionage and International Law, Columbus, OH: Ohio State University Press, 1962.*
*- **R. BUCHAN,** Cyber Espionage and International Law, HART PUBLISHING, Oxford, 2019.*
*- **R. BUCHAN,** the International Legal Regulation of State-Sponsored Cyber Espionage, Legal, Policy & Industry Perspectives, 2016.*
*- **S. AVIN, D. SEAMAN**, the Space Warfare, Concepts and Trends, Berlin, 2011.*
*- **S. HAROON,** International Humanitarian Law on Cyberwarfare and Pakistan's Legal Framework, Research Associate, Conflict Law Centre, RSIL, 2018.*

- ***S. J. SHACKELFORD***, *Managing Cyber Attacks in International Law, Business and Relations: In Search of Cyber Peace, 1st. edn., Cambridge University Press, UK 2014,*
- ***S. P. WHITE***, *Understanding Cyberwarfare: Lessons from the Russia-Georgia War, Modern war institute, 2018.*
- ***S. WATTS***, *Low-Intensity Cyber Operations and the Principle of Non-Intervention, Brill, Nijhoff, 2015***.**
- ***T. LANSFORD***, *Multinational Intelligence Cooperation, in: Countering Terrorism and Insurgency in the 21st Century, International Perspectives, James J.F. Forest ed., 2007.*
- ***T. PLOUG,*** *Ethics in Cyberspace: How Cyberspace May Influence Interpersonal Interaction, 1st. edn., Springer, 2009*
- ***W. M. CHOI***, *Diplomatic and Consular Law in the Internet Age, 10 Singapore Year Book of International Law, 2006.*

4- Articles and Researches:

- ***A. DEEKS***, *an International Legal Framework for Surveillance, 55 VA. J. INT'L L. 291, 328, 2015.*
- ***A. J. RADSAN,*** *the Unresolved Equation of Espionage and International Law, 28 MICH. J. INT'L L. 595, 2007.*
- ***A. J. SCHAAP***, *Cyber Warfare Operations: Development and Use under International Law, A. F. L. Rev. 64, 2009.*
- ***A. LUBIN,*** *Espionage and the right to privacy, ILSA Quarterly, volume 24, issue 3, 2016.*
- ***A. MELNITZKY***, *Defending America against Chinese Cyber Espionage, through the Use of Active Defenses, 20 CARDOZO J. INT'L & COMP. L., 2012.*
- ***A. S. DEEKS***, *Confronting and Adapting Intelligence Agencies and International Law, 102 VA. L. REV. 599, 2016.*
- ***A. S. DEEKS***, *Unwilling or Unable: Toward a Normative Framework for Extraterritorial Self-Defense, 52 VA. J. INT'L L., 2012.*
- ***A. WARTHAM***, *Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Charter Provisions Prohibiting the Threat or Use of Force? 64 Federal Communications Law Journal, 2012.*
- ***C. D. DELUCA***, *the Need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors, Pace Int'l L. Rev. Online Companion 3, 2013,*

- ***C. EWUMBUE***, *Respect for international humanitarian law by armed non-state actors in Africa, International Journal of the Red Cross, vol. 88, 2006.*
- ***C. FORCESE***, *International law and intelligence gathering, Journal of National Security Law & Policy, Vol. 5:179, 2011.*
- ***C. FORCESE,*** *Pragmatism and Principle: Intelligence Agencies and International Law, 102 VA. L. REV. ONLINE, 2016.*
- ***C. FORCESE,*** *Spies Without Borders: International Law and Intelligence Collection, 5 J Nat'l Sec L & Pol'y, 2011.*
- ***C. LOTRIONTE***, *Countering State-Sponsored Cyber Economic Espionage under International Law, 40 North Carolina Journal of International Law and Commercial Regulation, 2015***.**
- ***D. B. HOLLIS***, *an e-SOS for Cyberspace 52 (2), Harvard International Law Journal, 2011.*
- ***D FLECK,*** *Individual and State Responsibility for Intelligence Gathering, 28 MICH. J. Int'l L., 2007.*
- ***D. FLECK, Searching for International Rules Applicable to Cyber Warfare, A Critical First Assessment of the New Tallinn Manual, 18 J. CONFLICT & SECURITY L., 2013.***
- ***D. M. CRANE***, *Counterintelligence Coordination within the Intelligence Community of the United States: Divided We Stand, 12 ARMY LAW, 1995.*
- ***D. PUN,*** *Rethinking Espionage in the Modern Era, Chicago Journal of International Law, Volume 18, Number 1, 2017.*
- ***D. WEISSBRODT***, *Cyber-conflict, Cyber-crime, and Cyber-espionage, 22 Minnesota Journal of International Law, 2013.*
- ***E. J. TALBOT,*** *Cyber Attacks: Proportionality and Precautions in Attack, 89 International Law Studies, 2013.*
- ***E. T. JENSEN,*** *The Tallinn Manual 2.0: Highlights and Insights, Research Paper, No. 17, Georgetown Journal of International Law, 2017,*
- ***F. L. KIRGIS***, *Custom on a Sliding Scale, American Journal of International Law 81, 1987.*
- ***G. BROWN***, *Spying and Fighting in Cyberspace: What is Which?, 8 J. NAT'L SEC. L. & POL'Y., 2016.*
- ***G. BROWN, K. POELLET***, *the Customary International Law of Cyberspace, Strategic Studies Quarterly 6, 2012.*
- ***G. SULMASY***, ***J. YOO***, *Counterintuitive: Intelligence Operations and International Law, 28 MICH. J. INT'L L., 2007*

- ***H. KOH,*** *Address at the USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, Maryland: International Law in Cyberspace (Sept. 18, 2012), 54 HARV. INT'L L.J. ONLINE, 2012.*
- ***H. P. FAGA,*** *the Implications of Transnational Cyber Threats in International Humanitarian Law: Analysing the Distinction between Cybercrime, Cyber Attack, and Cyber Warfare in the 21st Century, Baltic Journal of Law & Politics, Vol. 10, No. 1, 2017.*
- ***H. S. LIN****, Offensive Cyber Operations and the Use of Force, J Nat'l Sec L & Pol'y 63, Vol. 4:63, 2010.*
- ***H. ZHANG****, Is It Safeguarding the Freedom of Navigation or Maritime Hegemony of the United States? Comments on Raul (Pete) Pedrozo's Article on Military Activities in the EEZ, 9 CHINESE J. INT'L L., 2010.*
- ***I. KILOVATY****, World Wide Web of Exploitations – the Case of Peacetime Cyber Espionage Operations under International Law: Towards a Contextual Approach, 18 Columbia Science and Technology Law Review, 2016.*
- ***J. E. MCGHEE****, Hack, Attack or Whack; the Politics of Imprecision in Cyber Law, 4 J. L. & CYBER WARFARE 13, 2014,*
- ***J. F. MURPHY****, Cyber War and International Law: Does the International Legal Process Constitute a Threat to U.S. Vital Interests? 89 International Law Studies, 2013.*
- ***J. W. ROLPH****, Freedom of Navigation and the Black Sea Bumping Incident: How "Innocent" Must Innocent Passage Be? 135 MIL. L. REV., 1992.*
- ***K. E. EICHENSEHR****, the Cyber-Law of Nations, 103 GEO. L. J. 317, 2015*
- ***K. J. WHEATON, M. T. BEERBOWER****, Toward a New Definition of Intelligence, 17 STAN. L. & POL'Y REV., 2006.*
- ***M. A. VATIS****, Cyber Attacks during the War on Terrorism: A Predictive Analysis, Institute for Security Technology Studies at Dartmouth College, Report OMB No. 074-0188, September 2001.*
- ***M. C. WAXMAN****, Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), Yale Journal of International Law 36, 2011.*
- ***M. FINNEMORE, D. B. HOLLIS,*** *Constructing Norms for Global Cybersecurity, 110 AM. J. INT'L L. 425, 2016.*
- ***M. GERVAIS,*** *Cyber Attacks and the Laws of War, Berkeley Journal of International Law, Vol. 30, Issue .2, 2012.*
- ***M. HALBERSTAM****, Hacking Back: Re-evaluating the Legality of Retaliatory Cyber-attacks, the Geo. Wash. Int'l L. Rev. 46, 2013.*

- M. WATNEY, Challenges Pertaining to Cyber War under International Law. In: The Third International Conference on Cyber Security, Cyber Warfare and Digital Forensics (Cybersec2014), 2014.

***- L. PELICAN**, Peacetime Cyberespionage: A Dangerous, but Necessary Game, 20 CommLaw Conspectus, 2012.*

***- M. J. SKLEROV**, Solving the Dilemma of State Responses to Cyber-attacks: A Justification for the Use of Active Defenses against States Which Neglect Their Duty to Prevent, Mil. L. Rev., 2009.*

***- M. N. SCHMITT,** the Law of Cyber Warfare: quo vadis? stanford law & policy review, Vol. 25, 2014.*

***-M. N. SCHMITT, S. WATTS,** The Decline of International Humanitarian Law Opinion Juries and the Law of Cyber Warfare, 50(2) Texas International Law Journals, 2015.*

***- M. ROSCINI**, World Wide Warfare: Jus ad bellum and the Use of Cyber Force, 14 Max Planck Y.B. United Nations Law, 2010.*

***- M. XINMIN**, Key Issues and Future Development of International Cyberspace Law, 2 China Quarterly of International Strategic Studies, 2016.*

***- M. XINMIN**, Letter to the Editors: What Kind of Internet Order Do We Need? 14 Chinese Journal of International Law, 2015.*

***- N. D. WHITE**, **S. MACLEOD**, EU Operations and Private Military Contractors: Issues of Corporate and Institutional Responsibility, the European Journal of International Law (EJIL) Vol. 19 no. 5, 2008.*

***- N. JUPILLAT**, From the Cuckoo's Egg to Global Surveillance: Cyber Espionage that Becomes Prohibited Intervention, 42 North Carolina Journal of International Law and Commercial Regulation, 2017.*

***- N. LUBELL,** Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply? 89 INT'L L. STUD., 2013.*

*- **N. TSAGOURIAS,** Cyber Attacks, Self-defence and the Problem of Attribution, J. Conflict & Sec L. Vol. 17, No 2, 2012.*

***- N. SOLCE**, the Battlefield of Cyber Space: The Inevitable New Military Branch – The Cyber Force, Alb. L.J. Sci. & Tech. 18, 2008.*

***- O. A. HATHAWAY et al**., the Law of Cyber-Attack, 100 CAL. L. REV. 817, 2012*

***- P. DOMBROWSKI, C. DEMCHAK,** Cyber War, Cybered Conflict, and the Maritime Domain, Naval War College Review, No. 67, Vol. 2, 2014.*

- ***P. W. FRANZESE****, Sovereignty in Cyberspace: Can it exist? Air Force Law Review 64, 2009.*
- ***P. WU****, Impossible to Regulate? Social Media, Terrorists, and the Role for the U.N., 16 CHI. J. INT'L L. 281, 2015.*
- ***B. RABOIN****, Corresponding Evolution: International Law and the Emergence of Cyber Warfare, 31 J. NAT'L ASS'N ADMIN. L. JUDICIARY, 2011.*
- ***R. A. FALK,*** *CIA Covert Actions and International Law, 12 Soc'Y, 1975.*
- ***R. A. CLARKE, R. K. KNAKE,*** *the Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats, Penguin, Dhu'l-Q. 13, Political Science, 2019.*
- ***R. BUCHAN****, Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? Journal of Conflict and Security Law 17, 2012.*
- ***R. D. SCOTT****, Territorial Intrusive Intelligence Collection and International Law, 46 Air Force Law Review, 1999.*
- ***R. D. WILLIAMS****, (Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action, 79 GEO. WASH. L. REV., 2011.*
- ***R. GEISS****, Cyber Warfare: Implications for Non-International Armed Conflicts, 89 INT'L L. STUD., 2013.*
- ***R. GEIB, H. LAHMANN,*** *Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space, 45 ISR. L. REV., 2012.*
- ***R. HIGGINS****, UK Foreign Affairs Committee Report on the Abuse of Diplomatic Immunities and Privileges: Government Response and Report, 80 AM. J. INT'L L. 135, 1986.*
- ***S. BAGDASAROVA,*** *Brave New World: Challenges in International Cybersecurity Strategy and the Need for Centralized Governance, 119 PENN. ST. L. REV., 2015.*
- ***S. CHESTERMAN****, We Can't Spy If We Can't Buy! the Privatization of Intelligence and the Limits of Outsourcing Inherently Governmental Functions, The European Journal of International Law, Vol. 19, No. 5, 2008.*
- ***S. CHESTERMAN****, Just War or Just Peace After September 11: Axes of Evil and Wars Against Terror in Iraq and Beyond, 37 N.Y.U. J. INT'L L. & POL., 2005.*
- ***S. GORDON****,* ***R. FORD,*** *On the Definition and Classification of Cybercrime, J. Computer Virology, 1, 2006.*
- ***S. R. STEVENS****, Internet War Crimes Tribunals and Security in an Interconnected World, Transnat'l L. & Contemp. Probs. 18, 2009.*

- ***S. W. BRENNER****, At Light Speed: Attribution and Response to Cyber crime/Terrorism/Warfare, the Journal of Criminal Law and Criminology, No.97, Issue 2, 2007.*
- ***S. W. BRENNER, L. L. CLARKE****, Civilians in Cyber Warfare: Conscripts, Vanderbilt Journal of Transnational Law, 43, 2010.*
- ***S. TOMAR,*** *Proxy Warfare, Journal of Defense Studies, Vol. 8, No. 2, 2014.*
- ***T. D. GILL, P. A. DUCHEINE****, Anticipatory Self-Defense in the Cyber Context, 89 INT'L L. STUD., 2013.*
- ***T. HERR, P. ROSENZWEIG****, Cyber Weapons and Export Control: Incorporating Dual Use with the Prep Model, 8 J. NAT'L SEC. L. & POL'Y, 2015.*
- ***T. RID****, Cyber War Will Not Take Place, 35 Journal of Strategic Studies 5, 2012.*
- ***V. NARAYANAN****, Harnessing the Cloud: International Law Implications of Cloud-Computing, 12 Chicago Journal of International Law, 2012*.
- ***W. A. OWENS, K.W. DAM, H. S. LIN****, eds., Technology, Policy, Law, and Ethics Regarding US Acquisition and Use of Cyber-attack, Capabilities National Research Council Report, 2009.*
- ***W. C. BANKS****, Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage, 66 Emory Law Journal, 2017.*
- ***W. H. V. HEINEGG****, Territorial Sovereignty and Neutrality in Cyberspace, International Law Studies 89, 2013*.
- ***W. J. LYNN III****, Defending a New Domain: The Pentagon's Cyberstrategy, Foreign Affairs, Issue 89, No. 5, September/October, 2010.*
- ***Y. DINSTEIN****, Cyber War and International Law, 89 INT'L L. STUD. 276, 2013.*
- ***Y. DINSTEIN****, the Interaction between Customary Law and Treaties, Recueil des Cours Recueil des cours, 2006.*

5- Theses:

- ***F. DELERUE****, State Responses to Cyber Operations, European University Institute, Ph.D. in Law, Global Relations Forum Young Academics Program, Policy Paper Series No.5, 2016.*

سابعاً: وثائق الأمم المتحدة:

(A/RES/73/27/2019/2020); (A/RES/70/237/2016/2017); (UN.Doc.A/70/174, 2015); (UN Doc A/70/174(2015); (A/RES/68/243/2014/2015); (UN Doc A/68/98

(2013); (UN Doc A/67/946, 29 July 2013); (UN Doc A/68/98, 24 June 2013); (A/RES/66/24/2012/2013); (A/RES/58/322009/2010); (UN Doc. A/65/201 (2010); (UN Doc. S/AC.51/2008/5,2008); (A/RES/73/266/2006/2007); (UN Doc. E/CN.4/2006/53/Add.5, 2006); (U.N. Doc. S/RES/1617 (2005); (A/RES/2004/2005); (UN Doc S/RES/1566(2004); (U.N. Doc. S/RES/1526 (2004); (U.N. Doc. S/RES/1390 (2002); (U.N. Doc. S/RES/1373 2001); (U.N. Doc. S/RES/1368 (2001); (U.N. Doc. A/55/305, S/2000/809 (2000); (U.N. Doc. A/55/502 (Oct. 20, 2000); (U.N. Doc. S/RES/1333 2000); (U.N. Doc. S/RES/1173 1998); (U.N. Doc. S/RES/ 917 (1994); (U.N. Doc. A/RES/41/65 (1986); (U.N. Doc. A/RES?37/85. 1982); (U.N. Doc. A/RES/3314 1974); (UN Doc. A/AC.125/SR.110 to 114 (1970); (UN. Doc. No. A/AC.105/C.2/SR.22/5 (1963); (UN Doc No A/AC.105/C.2/SR.28/13, 1963); (UN Doc No A/AC.105/C.2/SR.7, 1962); (UN Doc S/4314, 19 May 1960)

ثامناً: تقارير دولية:

***- Congressional Research Service Report**, Cyber warfare and Cyber terrorism: In Brief, R43955, March 27, 2015.*

***- Group of Government Experts Report,** Developments in the Field of Information and Telecommunications in the Context of International Security, 22 July 2015.*

***- International Law Commissions,** Second Report on the Identification of Customary International Law, A/CN.4/672, para. 47 (22 May 2014).*

***- Report of Kaspersky Lab Global Research and Analysis Team,** Syrian Malware, the Ever - Evolving Threat, August 2014.*

***- United Nation,** General Assembly, Developments in the field of information and telecommunications in the context of international security, Report, Sixty-sixth session, 15 July 2011.*

***- Office of the Nat'l Counterintelligence Exec.,** Foreign Spies Stealing us Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2011.*

***- Report of the Secretary-General**, In Larger Freedom: Towards Development, Security and Human Rights for All, UN Doc A/59/2005, 21 March 2005.*

***- United Nations, General Assembly,** International Law Commissions, Final Report of the Committee: Statement of Principles Applicable to the Formation of General Customary International Law, International Law Association, London conference, 2000.*

- ***ICTY***, *Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia, 14 June 2000.*
- ***Report on the Intermediate-Range Nuclear Forces Treaty to President Ronald Reagan)*** *from George P. Schultz, U.S. Secretary of State (Jan. 25, 1988).*
- ***Report of the Secretary General,*** *Human Rights and Scientific and Technological Development, U.N. Economic and Social Council, E/Cn. 41116, 23 January, 1973.*

تاسعاً: مقالات أكاديمية على مواقع انترنت رسمية:

- ***C. WILSON***, *CRS Report for Congress, Computer Attack and Terrorism: Vulnerabilities and Policy Issues for Congress, 1 April, 2005,* ***available at:*** *http://www.iwar.org.uk/cyberterror/resources/crs/45184.pdf.*
- ***Canadian Security Intelligence Service,*** *Commentary No. 76: The Canadian Government Security Screening Program,* ***available at:*** *http://www.csis-scrs.gc.ca/eng/comment/com76e.html.*
- ***D. ROBERTS***, *"OBAMA" Imposes New Sanctions against North Korea in Response to Sony Hack, the Guardian January 2, 2015,* ***available at:*** *http://www.theguardian.com/us-news/2015/jan/02/obama-imposes-sanctions-north-korea-sony-hack-the-interview.*
- ***D. TRENIN,*** *Information is a Potent Weapon in the New Cold War, the Guardian (Sept. 17, 2016),* ***available at:*** *https://perma.cc/QPT4-4B8T.*
- ***E. ALBERT,*** *Council on Foreign Relations: the Shanghai Cooperation Organization (Oct. 14, 2015), https://perma.cc/5KWF-JYYT.*
- ***EASTWEST INSTITUTE,*** *RUSSIA-U.S. Bilateral on Cybersecurity Critical Terminology Foundations 2 (James B. Godwin III et al. eds., Feb. 2014),* ***available at:*** *https://perma.cc/79P7-L3SP.*
- ***Embassy Espionage:*** *The NSA's Secret Spy Hub in Berlin, 27 October 2013, Spiegel,* ***available at:*** *www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy- a-930205.html.*
- ***H. R. CLINTON***, *Secretary of State, Remarks at the Newseum, Washington, DC: Remarks on Internet Freedom (Jan. 21, 2010), http://www.state.gov/secretary/rm/2010/01/135519.htm. 2/4/2019.*

***H. ROIGAS**, Mixed Feedback on the African Union Convention on Cyber Security and Personal Data Protection, INT'L CYBER DEVELOPMENTS REVIEW (Feb. 20, 2015), **available at:** https://perma.cc/795P-X22V.*

***- ICRC**, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts' (October 2015), **available at:** https://www.icrc.org/en/download/file/15061/32ic-report-on-ihl-and-challenges-of armed-conflicts.pdf.*

***- J. FINKLE**, Hacking Is Such a Problem that the Cost of Cyber Insurance is Skyrocketing, VENTUREBEAT (Oct. 11, 2015), **available at:** https://perma.cc/8UFD-Z6MQ.*

***- J. L. GOLDSMITH**, Quick Thoughts on the US Governments, Refusal to Use Cyber-attacks in Libya, (18 October 2011) Brookings Institute, **available at:** http://www.brookings.edu/blogs/up- front/posts/2011/10/18-cyberattack-libya-goldsmith.*

***- K. GROUP**, Intelligence and Analysis on Iraq: Issues for the Intelligence Community 2-3 (Central Intelligence Agency, 2004), **available at:** http://www.gwu.edu/-nsarchiv/news/20051013/keff-report.pdf*

***- L. POITRAS, M. ROSENBACH, H. STARK**, Codename 'Apalachee': How America Spies on Europe and the UN' Der Spiegel International (Hamburg 26 August 2013), **available at:** http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-oneurope-and-the-un-a-918625.html.*

***- M. FAHEY, N. WELLS**, Yahoo Data Breach is among the Biggest in History, CNBC (Sept. 22, 2016), **available at:** https://perma.cc/92A2-N497.*

***- M. WARNER**, Wanted: a Definition of Intelligence, 46(3) STUD. In Intelligence (Unclassified Edition) (2002), **available at**: https://www.cia.gov/csi/studies/vol46no3/article02.html.*

***- N. WOOLF,** DDoS attack that disrupted internet was largest of its kind in history, experts say, the Guardian (26 October 2016), **available at:** https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.*

***- NATO Cooperative Cyber Defense Centre of Excellence**, TALLINN MANUAL on the International Law Applicable to Cyber Warfare 45 (Michael N. Schmitt et al. eds., 2013)*

***- P. J. CROWLEY,** Assistant Secretary of State, Daily Press Briefing, Washington, DC (Jan. 13, 2010), **available at:** http://www.state.gov/r/pa/prs/dpb/2010/01/135142.htm.*

- ***S. ELEGANT****, Cyberwarfare: The Issue China Won't Touch, Time Magazine, (New York City 18 Nov 2009),* ***available at:*** *http://content.time.com/time/world/article/0,8599,1940009,00.html.*

. *SCHJOLBERG,* *The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva, December 2008.*

- ***WSIS Forum 2016****, WSIS Action Lines: Supporting the Implementation of SDGs: Outcomes,* ***available at:*** *https://sustainabledevelopment.un.org/content/documents/10186World%20Summit%20on%20Information%20Society%202016%20Outcomes%202016-May-16.pdf.*

عاشراً: تشريعات وسياسات وطنية:

- ***DOD Joint Terminology for Cyberspace Operation,*** *Washington, D.C. 20318-9999, 2018.*

December 2011 report endorsed by the Dutch government, *Advisory Council on Int'l Affairs and the Advisory Comm. on Issues of Pub. Int'l Law, Cyber Warfare 20 (No. 77, AIV/No.22, CAVV) (Dec. 2011).*

- ***German Federal Ministry of the Interior****, Cyber Security Strategy for Germany, Berlin: Beauftragter der Bundesregierung für Informationstechnik, 2011,*

- ***H. Farrell, M. FINNEMORE****, the End of Hypocrisy: American Foreign Policy in the Age of Leaks' Foreign Affairs, November/December 2013*

National Security Act of 1947, *Pub. L. No. 80-253, 61 Stat. 495, codified as amended in scattered sections of 50 U.S.C.*

- ***The White House, Fact Sheet: U.S.*** *Policy Standards and Procedures for the Use of Force in Counterterrorism Operations Outside the United States and Areas of Active Hostilities, 2013.*

The White House, *Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communications Infrastructure (2009),*

- ***UK Cabinet Office,*** *the UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World (November 2011.*

- ***U.K. Secretary of State for the Home Dep't, Contest:*** *the United Kingdom's Strategy for Countering Terrorism (Her Majesty's Stationary Office, July 2011).*

- ***US Army Training & Doctrine Command,*** *DCSINT Handbook No. 1.02, Critical Infrastructure Threats and Terrorism: Cyber Operations and Cyber Terrorism Handbook, 2005.*

- US DOD, *Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, Dirs. of the Joint Staff Directories, Joint Terminology for Cyberspace Operations, November 2011*.