كلية القانون
College of Law
QATAR UNIVERSITY جامعة قطر

دار نشر جامعة قطر
Qatar University Press

OPEN ACCESS
Submitted: 4/9/2021
Reviewed: 28/9/2021
Accepted: 4/10/2021

القانون الدولي والهجمات الإلكترونية ما دون استخدام القوة

فاطمة الظبيري

أستاذ مشارك، جامعة الكويت، الكويت

f.alzubairi@ku.edu.kw

ملخص

مع ازدياد اعتماد الدول على الفضاء الإلكتروني في حفظ ونقل البيانات والمعلومات، تظهر الهجمات الإلكترونيّة ما دون استخدام القوة كخرق لأمن هذا الفضاء، وأمن المعلومات. يتطرق البحث لصورتين من صور الهجمات الإلكترونيّة، هما؛ التجسُّسُ الإلكترونيّ، وعمليات التخريب الإلكترونيّة. يُواجه البحث إشكاليّةَ عدم تجريم القانون الدولي بشكل صريح للتجسس خلال فترة السِلْم، والذي قد يَترتب عليه قيام بعض الدول بعمليات تجسس ضد دول أخرى دون رادع قانوني. إن التجسس الإلكترونيّ قد يكون خطوة أولى في اتِّجاه المزيد من التدخل غير المشروع لدول في شؤون دول أخرى؛ إذ إن الحصول على معلومات سريّة من دون موافقة الدولة الضحيَّة قد يجعل الدولة الفاعلة في مركز قوة يسمح لها بمعرفة مواطن ضَعف الدولة الضحيّة، وبالتالي التأثير عليها؛ إمّا من خلال الضغط السياسيّ، أو من خلال شَنّ هجمات تخريب إلكترونية. يُقدّم البحث مُعالجة قانونيّة حول كيفيّة تعامُل القانون الدُّوليّ مع التجسس الإلكترونيّ وعمليات التخريب الإلكترونيّة؛ من خلال تفعيل مبدأَيْ السيادة وعدم التدخل، باعتبارهما حجر الأساس في صون الدولة لممتلكاتها من معلومات وبنية تحتيّة، وكذلك سلامتها السياسية.

الكلمات المفتاحية: التجسس الإلكتروني، التخريب الإلكتروني، السيادة، عدم التدخل

للاقتباس: الظبيري، فاطمة. «القانون الدولي والهجمات الإلكترونية ما دون استخدام القوة»، **المجلة الدولية للقانون**، المجلد الحادي عشر، العدد الأول، 2022

https://doi.org/10.29117/irl.2022.0211

دار نشر جامعة قطر
Qatar University Press

كلية القانون
College of Law
QATAR UNIVERSITY جامعة قطر

OPEN ACCESS

Submitted: 4/9/2021
Reviewed: 28/9/2021
Accepted: 4/10/2021

International law and cyber-attacks without the use of force

Fatemah Alzubairi
Assistant Professor, Kuwait University, Kuwait
f.alzubairi@ku.edu.kw

Abstract

With the increasing reliance of countries on cyberspace to store and transmit data and information, cyber attacks appear as a breach to cybersecurity and information security. The research deals with two forms of cyber attacks, namely cyber espionage and cyber sabotage. It discusses the issue that international law does not explicitly criminalize espionage during peace, which may encourage some countries to carry out espionage operations against other countries without legal deterrence. Cyber espionage may be a first step towards more illegitimate interference in other countries' affairs, as obtaining confidential information without the consent of the victim state may put the attacker in a position of power that allows it to know the weaknesses of the victim state and thus influence it either through political pressure or cyber sabotage. This research offers a legal understanding on how international law deals with cyber espionage and sabotage through activating the principles of sovereignty and non-interference as the cornerstone in protecting the sovereignty of the state, over its property including information and infrastructure, as well as its political integrity.

Keywords: Cyber espionage; Cyber sabotage; Non-intervention; Sovereignty

Cite this article as: Alzubairi F., "International law and cyber-attacks without the use of force", *International Review of Law*, Volume 11, Regular Issue 1, 2022

https://doi.org/10.29117/irl.2022.0211

المقدمة

تُعتبر تهديدات الأمن الإلكترونيّ أحد الظَّواهر المُعاصرة التي تُقلق الأمْن والسِّــلْمَ الدُّوَليّين؛ إذ إن الاستغلال غير المَشروع لشــبكة المعلومات يُهدد معه مصالح الدُّول والمجتمع الدُّولي كَكُلٍّ. ولأنّ مُعظم الحكومات المُعاصرة تعتمد على الإنترنت، فأيّ انتهاك لشــبكاتها قد يُؤدّي إلى شَل خدماتها كالمُواصلات والطَّاقة. فَفِي حال وقُوع مثل تلك الهجمات الإلكترونيّة، فإن الدولة الضحية قد تفقد ســيطرتها كُليّا، أو جُزئيّا على قطاع ما بما يُؤثِّر على سيادتها وســلامتها السياســية. من هذا المُنطلق، يُقدِّم البحث دراســة حَول كيفيَّة تعامُل القانون الدولي مع الهجمات التي تَستهدف الدُّول عن طريق الإنترنت. لقد أصبحت الحاجَة مُتزايدةً لإطارٍ قانوني دولي ذي قُيود موضوعيّة مُشتركة تســعى لِفرْضِ حِماية قانونيّة دُوليّة مُوحدَّة تخدم الدول مُنفردة ومجتمعة في تعزيز الأمن المحلي والأمن الدولي دون انتقاص لسيادات الدول وسُلُطاتها التقديريّة في تَبَنِّي قوانين تَخْتلف في جُزئياتها لتلبية احتياجاتها الداخلية.

يبدأ البحث بالمبحث الأول الذي يبين فيه ماهية الهجمات الإلكترونيّة ما دون اســتخدام القوة، ويقســمها إلى نوعين: التَّجسس الســيبراني، وعمليات التخريب الســيبراني، والتي يخصص البحث لكل منهما مطلب. ويُقصد بالتجســس الإلكتروني الحصول على المعلومات والبيانات من قواعد البيانات وأجهزة الحاسوب دون إذن الدولة المُراد التجســس عليها. أمّا عمليات التخريب الإلكترونيّة فهي تتشكَّلُ في صور عديدة، كإرسال فيروس لأجهزة الحاسوب، أو التسبُّب بتعطيل المُنشآت إلكترونيًّا، أو شَلّ الإنترنت لدولة ما. وهذه الصُّور من التخريب قد وقعت فعليًّا على أرض الواقع، لكن يَظَلُّ السؤال حَول كيفيّة تعامُل القانون الدُّولي مع الجهات الفاعِلة حينما تُعرف. يبين البحــث في هذين المطلبين خطورة كل من هاتين الصورتين من الهجــمات الإلكترونية وأهمية بذل الدول جهودها لمواجهة أخطار الاستغلال السيئ للفضاء الإلكتروني. ينتقل البحث بعدها إلى المبحث الثاني، والذي يبين فيه كيفية تعامــل القانون الدولي في صورتــه الحالية مع الهجمات الإلكترونية. يعترف البحــث بوجود قصور في الاتفاقيات الدولية والعرف الــدولي في مجال الأمن الإلكتروني، لذا يوجه أنظاره إلى المبــادئ العامة للقانون الدولي، وتحديدا إلى مبدأ الســيادة ومبدأ عدم التدخل. فيرى البحث أن في ارتكاب التجســس الإلكتروني، أو عمليات التخريب الإلكترونية اعتداء على سلطان الدولة في صون ممتلكاتها الإلكترونية والتي تشمل شبكات الإنترنت والبنية التحتية وأجهزة الحاسوب والبيانات الرقمية، فأي اعتداء على سلامة هذه الممتلكات هو اعتداء على الحق السيادي للدول في إدارة شــؤونها الداخلية دون تدخل. ينقســم هذا المبحث إلى مطلبين، الأول يتناول الحق السيادي للدول على فضائها الإلكتروني. إن مبدأ الســيادة يكفل للدولة ممارسة ســلطاتها على إقليمها بشكل تام ومانع، ولأن عمليات التجســس الإلكتروني تتم دون موافقة الدولة الضحية، فإن البحث يجــادل بأنه يجب اعتبار هذه العمليات انتهاكا لمبدأ الســيادة. ويرى البحث أنه إذا كانت عمليات التجســس الإلكتروني تنتهك سيادة الدولة، فإنه من باب أولى اعتبــار عمليات التخريب الإلكترونيــة، التي تترك آثارًا مادية ضارة، اعتداء على مبدأ الســيادة. أما المطلب الثاني فيتناول حق الدول بصون فضائها الإلكتروني من عدم التدخل. إن معنى مبدأ عدم التدخل يشــوبه الغموض؛ إذ يقصره البعض على حالات الإكراه الناتجة عن وجود تدخل عسكري. يركز البحث على انتفاء عنصر الرضا للدولة ضحيــة الهجمات الإلكترونية، لذلك يدعو البحث إلى الأخذ بمفهوم موســع للتدخل المحظور في القانون الدولي

ليشمل حظر هجمات التجسس السيبراني والتخريب السيبراني. إن البحث إلى جانب تقديمه لدراسة تفصيليّة لمبادئ القانون الدولي، يبين أهمية القانون المرن الممثل بتوصيات الأمم المتحدة، التي تتميز بإمكان إصدارها خلال مدد موجزة يجعل منها وسيلة جذابة للدول باعتبارها غير ملزمة، وأيضًا وسيلة قابلة على مواكبة التطور التكنلوجي السريع. إن أهمية القانون المرن هو أنه قد يشكل خطوة أولى في توجيه سلوك الدول إلى حين نشوء عرف دولي، أو تبني اتفاقيات دولية تنظم الفضاء السيبراني. هذا بالإضافة إلى السوابق القضائية وآراء الفقهاء اللذان يستند عليهما البحث باعتبارهما مصادر احتياطية تقدم تفسيرا للقانون الدولي حول مسائل الفضاء الإلكتروني بما يواكِب مُتطلبات العصر ويضمن احترام سيادة القانون. إن الهدف من هذا البحث هو الوقوف على العقبات القائمة في القانون الدولي واقتراح توصيات حول تطويره وتفسيره لحظر الهجمات الإلكترونية بما يكفل احترام سيادات الدول بما يعزز مناخا آمنا للفضاء الإلكتروني للمجتمع الدولي ككل.

حدود البحث:

يُعالج البحث الأفعال الإجراميّة التي تقع من خلال شبكة الإنترنت، والتي تُشكِّلُ هجمات "إلكترونيّة" أو "سيبرانيّة"؛ إذ إن هذين المصطلحين يحملان المعنى ذاته، ويستخدمهما البحث بشكل مترادف. إن الهجمات السيبرانيّة التي يُعالجها البحث هي التي ترتكبها دُول، أو جِهات مدعومة من دول، وتستهدف دُولًا أُخرى، دون أن تُشكِّل عُدوانا مُسلحًا. هذه الهجمات بحاجة إلى توفُّر ثلاثة عناصر: أولا، الجهة الفاعلة دولة، أو أفراد، أو جماعات مدعومة من دول، وهي الجهات المعنية في القانون الدولي. ثانيا، الضحيّة دَولة، أو أحد أشخاص القانون الدولي العام. فالقانون الداخلي يعنى بما يُعرَفُ بالجرائم الإلكترونيّة، مثل انتحالِ الشَّخصيّة، وسَرِقة البيانات، وقرصنة الحسابات، حتى وإن تطلَّب الأمر تعاونًا دوليًا لتفعيل مسائل كقواعِد الإسناد، وتَتَبُّع الجُناة، والتَّسليم. تجدر الإشارة إلى أن البحث يأخذ بعَين الاعتبار احتماليّة تداخُل المصالح، فالجرائِمُ الإلكترونيّة قد تَستهدف القِطاعَيْن العام والخاص في ذات الوقت، وفِي هذه الحالات فإنَّه يلزم النظر إلى الهجمات الإلكترونية بوصفها مشروعًا إجراميًا واحدًا يستهدِفُ أمْنَ واستقرار الدولة. أمَّا العُنْصر الثالث هو أن الهجمات تُرتكب من دون استخدام القوة، فالهجمات التي تَصِل إلى حدِّ العُدوان يُعالجها القانون الدُّوليّ الإنسانيّ. وتخرج هذه الفئة الأخيرة من حدود البحث، مع ذلك يشار إليها حينما تنطبق وقت السلم دون حرب معلنة، وذلك بهدف تبيان التداخل بين الحالات المختلفة ومدى إمكانية تفاقم الهجمات ما دون استخدام القوة لتصل إلى حد العدوان.

المبحث الأول: الهجمات الإلكترونيّة ما دون استخدام القوة

إن مُعظم الهجمات الإلكترونيّة التي وقعت على أرض الواقع تمَّت من دُون استخدام القوة المسلحة، فالهجمات الإلكترونيّة الأكثر شُيوعًا تأخذ شَكْل اختراق أجهزة الكمبيوتر وشبكات الويب من خلال نشر الفيروسات بهدف تعطيلها، أو من خلال تلقيحها بمعلومات خاطئة بهدف تضليل المُستخدِمين. هذا النوع من الهجمات يتناوله البحث باعتباره عمليات تخريب سيبراني. وهناك شكل آخر دارج، وهو استطلاع شبكات الحاسب الآلي، والذي تخترق فيه شبكات الخَصم بهدف الحُصولِ على البيانات والمعلومات دون تدميرها. إن مثل هذه الأفعال يتناولها البحث

باعتبارها أعمال تَجَسُّس، خاصةً حينما تستهدف معلومات تَمَس أمن الدولة، كالأسرار العسكريّة، أو الاستخباراتيّة، وفي الحالتين فإن الأمن السيبراني ينتهك دون عُنف، أو اسْتخدام القوة العسكريّة[1].

يمكــن النَّظر إلى الكثير مــن عمليات الاقتحام الإلكــترونيّ والتدخل في أنظمة الكمبيوتــر لجمع المعلومات على أنها أفعال تجســس بين الدول، والتجســس جريمة لها وجود منذ القدم. ويعتبر التجسس ضد الدولة جريمة بِمُوجــب القانون الداخليّ للكثير من الدُّول، كما يُعالج القانون الدُّوليّ الإنســانيّ طريقة التَّعامل مع الجواســيس أثناء النِّزاعات المُســلّحة. رغم هذا التَّنظيم القانونيّ، فإن الإشــكاليّة هي عَدَم مُعالجة القانون الدوليّ للجاسوسيّة التي تَقع وقْت السلم، فسُــكوت القانون الدولي عن هذا النوع من التجسس يَجعل منها أفعالًا مُباحة قانونًا، رَغْم اعتبارها مُسْــتهجَنةً أَخلاقيًّا وسياسيًّا – على الأقل من قِبَل الدولة الضحية...[2]. إن عَدم وضوح القانون الدولي في اعتبار التجســس عمل غير مشروع ضِد سيادات الدُّول أدَّى إلى غُموض في تكييف عمليات الاقتحام الإلكترونيّ بغرض التجســس. إن أمن المعلومات جُزء من الأمن الإلكترونيّ والذي قد ينتهك بصور متعددة مثل التجســس والتخريب. يرى البحث أنه حين تســتخدم دَولة ما المعلومات التي حصلت عليها من خلال التجسس السيبرانيّ من أجل شَــنّ هجمات إلكترونيّة ضد دولة أخرى خرقا لسيادَة الدولة، فحق الدولة في ممارسة سلطاتها وسيطرتها على إقليمها بشكل كامل يقتضي منع التدخلات الخارجية بكافة أشكالها، بما في ذلك عمليات التجسس والتخريب الإلكتروني. يجادل البحث أن عدم تجريم هذه الأفعال بشكل صريح في اتفاقيات دولية لا يعني خروجها من دائرة القانون، فمبادئ القانون الدولي كفيلة بفرض الحماية اللازمة للحق السيادي للدول على فضائها الإلكترونيّ. يقوم البحث بالتأكيد على أهمية تقديم تفسيرات معاصرة لمبادئ القانون الدولي تواكب التطور التكنلوجي وتكفل تعزيز الأمن والسلم الدوليين.

يقوم البحث بدراسة أعمال التَّجســس وأعمال التَّخريب باعتبارهما صورتَيْن من صُور الهجمات الإلكترونيّة ما دون استخدام القوة. فعلى الرغم من أنَّ هاتين الصُّورتَين يَشُوبهما الغُموض من حيث التَّكييف القانوني، فإن الهدف من دراســتهما هو توجِيه المَساعي المُســتقبليّة لتفســير وتطوير القانون الدوليّ لضمان أنَّ هذه الهجمات الإلكترونيّة يحكمها القانون وليس أهواء الدول.

المطلب الأول: التَّجسّسُ السيبراني

تَشوبُ العَلاقات بين الدُّولِ الكثيرُ من المُنافسة وأحيانًا العداوة، ولتعزيز معرفة الدول بمنافسيها وبنقاط القوة والضعف لديهم، يأتي دور التجســس والذي يتمثل بتجميع المعلومات الاستخباريّة. التجسس بمفهومِه التقليدي هو المُمارســة التي تُرســل الدولة بِمُوجبها عميلًا إلى أراضي دولة أُخرى مِن أَجــل الحصول على معلومات سريّة، ويُشارُ إلى استخدام الأفراد للحصول على المعلومات بالذَّكاء البشريّ (Human Intelligence)...[3]. فالتجسس

1 عادل عبد الصادق، **الاقتصاد الرقمي وتحديات السيادة السيبرانية**، المركز العربي لأبحاث الفضاء الإلكتروني، القاهرة، 2020، ص36.

2 Geoffrey B. Demarest, "Espionage in International Law", Denver Journal of International Law and Policy 24 (1996): 326.

3 Russell Buchan, "The International Legal Regulation of State-Sponsored Cyber Espionage" in Anna-Maria Osula and Henry Rõigas (eds.), International Cyber Norms: Legal, Policy and Industry Perspectives Tallinn: NATO CCD COE, 2016) 65-66.

هــو جمع غير مُصرح به للمعلومات غير المُتاحة للجمهور، فلا بُدَّ مِن التمييز بين جمع المعلومات الاســتخبارية من المصادر المُتاحة للجمهور والتي لا إشكاليّة قانونيّة عليها، وبين جمعها من مصادر خاصة غير مُصرَّح بها والتي تصل إلى حد التجسس...[4].

لقد صارت أســاليب التجســس أكثر ابتكارًا وتنوعًا مع التطور التكنولوجيّ؛ إذ تســتغل السُّفن والطائرات والأقمار الصناعية لمُراقبة الخصوم، وامتدت هذه الأســاليب لتشمل الإنترنت. وبسبب الكَم الهائِل من المعلومات المُخَزَّنة إلكترونيًّا، بالإضافة إلى إمكانيّة جمعها دون معرفة هوية الفاعل، صار التجســس الإلكترونيّ وسيلة جذابة للفاعــل[5]. ويمكن تعريف التجســس الإلكترونيّ بأنــه العمليات التي تحصل من خــلال الإنترنت، لِغرض جَمع المعلومات الاستخبارية من أجهزة الكمبيوتر، أو أنظمة المعلومات، أو الاتصالات، أو الشبكات، من دون معرِفة، أو رِضا الضَّحيّة[6].

إن دراسة التجســس الإلكترونيّ تتطلَّب مُواجَهة إشكاليتَين: الأولى هي عدم مُعالجة القانون الدوليّ للتجسس بشــكل صريح، والثانية هي عدم وجود تَقْنين وَافٍ في القانون الدُّوليّ لِممارســات الفضاء الإلكترونيّ. الإشــكاليَّة الأولى دفعت جانِبًا من الفقه بالتســليم بِأن التجسس غير محظور في القانون الدولي، وهو أمر عَزَّزته مُمارسة الدُّول. فعقود طويلة من مُمارســة بعض الدول التجســس على دول عدوة وأخرى صديقة، لم يُقابل بُمطالَبة جِدِّيَّة باعتبار الجاسوســيّة انتهاكًا لمبدأ السيادة. ومن الممارســات التي تُؤكِّد على عدم حظر الجاسوسيّة، قيام بعض الدول بتبادل الجواسيس المقبوض عليهم[7].

إن عدم مُطالَبة الضَّحايا مِن الدُّول بِتجريم هذه الأفعال قد يَرجع إلى اســتخدام ذات الدول أداة التَجَسُّس ضِد دُول أُخرى، فمن مَصلحَة الدولِ بما فيها الضحايا عدم تحريم التجسس، وذلك للاستمرار بمُمارسته دون التَّعرض للمُســاءلَة القانونيّة. لقد وضع هذا المنطِقُ الجاسوسيَّة ضِمن مِنطقة رماديّة تَحكمها مَصالِحُ الدُّول السيَّاسيَّة وليس القانون الدولي، وهكذا فإن هذه المُمارسة المبنيّة على الواقعيّة السياسية استثنت الجاسوسية من الأفعال غير المشروعة التي تَمس مبدأ الســيادة[8]. وقد امْتَدَّ القَبُول الضمنِيّ بِعدمِ مَســاسِ الجاسوســيّة بِمبدأ السيادة لِعملياتِ التجسس الإلكتروني، وبذا تعامل بوصفها أفعال ليست محظورة في القانون الدولي.

أما الإشكالية الثانية، فتتمثل بِزَعْم البعض بأن الفضاء الإلكتروني هو مِنطقة خارج القانون law-free zone[9]. يُدَعِّم مُدَّعِي هذا الزَّعم حججهم بالطبيعة الافتراضيّة للفضاء الإلكتروني ومُمارســاته العابرة للحدود والتي لا

4 المرجع السابق، 85.

5 ضرغام جابر عطوش آل مواش، **جريمة التجسس المعلوماتي**، المركز العربي للنشر، القاهرة، 2017، ص82؛ وانظر أيضًا: Buchan, *idem*, 66.

6 Presidential Policy Directive/PPD-20, U.S. Cyber Operations Policy (October 2012), http://www.fas.org/irp/offdocs/ppd/ppd-20.pdf.

7 Gary Brown and Keira Poellet, "The Customary International Law of Cyberspace", Strategic Studies Quarterly Vol. 6, No. 3, (2012), 133.

8 المرجع نفسه،

9 Sean Watts, "Low-Intensity Cyber Operations and the Principle of Non-Intervention", Baltic Yearbook of International Law 14 (2014): 142.

يمكن حَصرها في رُقْعَة جغرافيّة مُعينة، وبذا يُشَكِّك هذا الرأي بإمكانيّة تَمتع الدول بالسيادة الإقليميّة على الفضاء الإلكتروني[10]. فمفهوم السيادة الإقليمية قد يبدو للبعض غَير قابِل للتطبيق على الفضاء السيبراني، وهذا الرأيُ يتجاهل أن الفضاء الإلكتروني بحاجة إلى بِنْيَة تحتيّة والتي تَشتمل على أسلاك وأجهزة إرسال واستقبال عبر الأقمار الصناعيّة وأبراج الإنترنت، وهي بمجملها تخلق صِلة بين الفضاء الإلكتروني وأقاليم الدول كما سنرى لاحِقًا[11].

تتشابهُ الكثير من عَمليات التجسس التي تَتِم من خلال التَّسلُّل الفعليّ مع عمليات الاقتحام الإلكترونيّ، فمن النَّاحية النظريّة قد يَرى البعض أن الدخول خِفية لمكتب لِسَرقة مُستندات سريّة لا يختلف عن التَّسلل الإلكترونيّ لجهاز حاسوب وسرقة ملف إلكترونيّ. والتسليم بهذا التشابه فيه الكثير من التَّبسيط الذي يتجاهل تفصيلات مُهِمَّة مُتعلقة بعمليّات الاقتحام الإلكتروني. يُوضِّح فريقا من الباحثين في مجال الأمن السيبراني أن الخيارات المُتاحة أمام الجاسوس الذي يتسلل بنَفْسه لمكتب ما مُستهدفًا ملفًا تَظلّ محدودة إمّا بسرقته، أو إتلافه كُليًا، أو تغيير محتواه، أمّا الخيارات المُتاحة أمام من يقوم بعملية التسلل الإلكترونيّ فتكون أكثر تعددًا؛ إذ تتراوح من تغيير مجرد رقم واحد له تأثير محدود، إلى اقتحام أوْسَع لشبكات الإنترنت لأغراض استخباراتيّة، بل وإلى تعطيل أكثر تدميرًا كَشلّ المعاملات المالية وقطع الاتصالات كُليًّا لمُدَد طويلة[12]. فهناك فرق – على سبيل المثال – بين التقليل من كفاءة شبكات الاتصال وبين تعطيل كامل لها، وبين تعطيل مؤقت لمحطات طاقة في منطقة نائية، وبين إرسال إشارات مُضللة حول سلامة محطات طاقة نووية مما يؤدي إلى انفجارها وإحداث أضرار بالدولة المُستهدفة وجاراتها من الدول. رغم إمكانية تكييف عمليات الاقتحام الإلكترونيّ باعتبارها أعمال تجسس، إلا أنها ليست كلها تُرتكب لهذا الغرض؛ إذ قد تتجاوز الغاية إلى التخريب، أو حتى شَنّ عُدوان كما سنبين في موضع لاحق من هذا البحث.

إن اختلاف الغرض من التجسس يُغيّر بشكل جذري تكييف أفعال الاقتحام الإلكترونّي. ولتوضيح ذلك نطرح فَرَضيّة وهي قيام دولة ما بزرع برنامج، أو جهاز تنصت إلكتروني في جهة حساسة لدولة أخرى، ويقوم البرنامج بتسجيل المُحادثات بغرض جمع المعلومات. هنا الغرض يبدو جليا أنه تجسس، مع ذلك فإن أهداف الدولة المُتجسسة قد لا تقف عند هذا الحَدّ، وإنما تهدِف إلى استغلال هذه المعلومات لشَنّ هجمات تخريب إلكترونيّة عن طريق إرسال فيروس لأجهزة الحاسب للدولة المُستهدفة. لو اكتشف برنامج التنصُّت قبل تفعيل الفيروس، فنكون أمام مَشروع تخريب وليس مُجرَّد تَجسُّس. إن هذا المثال يُبين مَدى التَّداخُل بين أعمال التجسس الإلكترونيّة والهجمات السيبرانيّة الأُخْرى كالتخريب، فنجاحُ مثل هذه الهجمات الإلكترونيّة يعتمِد على نجاح التجسس الإلكترونيّ[13].

المطلب الثاني: عمليات التخريب السيبراني

مع اتّساع استخدام الفضاء الإلكتروني وإمكانيّة استِغلال ثَغْرة عدم التجريم الصريح للتجسس السيبراني، فإن قواعد المعلومات بما فيها السياسية والاقتصادية والأمنية قد تتعرض لخطر التخريب، أو العبث. ففي وقتنا الحالي تعتمد

10 David Johnson and David Post, "Law and Borders: The Rise of Law in Cyberspace", Stanford Law Review 48 (1996): 1367.

11 Buchan, *idem*, 71.

12 Brown and Keira Poellet, *idem*, 135–136.

13 المرجع نفسه، 135.

الدول بقطاعيها العام والخاص بشكل كبير على الإنترنت ونظم المعلومات، لذا فأي عمليات تخريب إلكترونية سيكون لها أثر سلبي على أمن الدولة الداخلي والخارجي. ونقصد بالتخريب الإلكتروني العمليات التي تُرتكب بغرض التأثير سلبًا على أنظِمة المَعلومات وشبكات التواصل الإلكترونيّة. ومن صور التخريب الإلكتروني قطع الإنترنت، الحِرمان من الخِدمة، التلاعب بالبيانات والمعلومات، وكذلك استخدام الإنترنت للتأثير على البِنْية التحتيّة[14].

إن عَمليـات التخريب الإلكترونية مختلفة وتتفاوت درجة خطورتها عـلى الدولة الضحية. ونضرب فَرَضيّات للوقـوف على مخاطر عمليات التخريب الإلكترونية؛ فحينما تتأثـر سرعة الإنترنت، أو تقطع الخدمة مؤقتًا في دولة مـا فإن الأمر قد يمتد لتعطيل أجهزة التحكم التي تعمل من خلالها المُنشـآت الماليّة كالبنوك والأسـواق الماليّة مما يُؤدّي إلى توقف المعاملات وتَضرر الشركات والأفراد، ناهيك عن زَعْزَعة المَركزين الاقتصادي والسياسي للدولة. وكذلك حينما تحجب مواقع حكومية، فإن الأمر لا يقف عند تعطيل مصالح الشـعب فحسـب، وإنما يمتد التأثير إلى خَلـق حالة من الريبة ليس فقط حول مقدرة الدولة في تأمين مواقعها الإلكترونيّة، وإنما حول قدرتها على حفظ الأمن العام.

إن أسوأ الفرضيات التي قد تسـفر عن عمليات التخريب الإلكتروني هي التي تؤدي إلى إزهاق الأرواح. فلو افترضنا قيام دولة ما بإرسال فيروس إلكتروني إلى أجهزة دولة أخرى تؤثر على أنظمة التحكم بمستشفى مما يؤدي إلى تعطيلها لمدة وقتية كبضع سـاعات، ويؤثـر هذا الفعل على حياة بعض المرضى مما يـؤدي إلى موت من هم في العناية المركزة. إن عمليات التخريب في هذه الفرضية تحدث وقت السـلم دون وجود حرب معلنة، ولكن بسبب وجـود ضحايا مدنيين، فإن القانون الواجب التطبيق يكون القانون الدولي الإنسـاني. في هذه الحالة تثور مجموعة من الأسـئلة، أهمها أنه إذا كشِـف أمر الدولة التي ارتكبت الفعل، فهل يحق للدولة الضحية اسـتخدام حقها في الدفاع الشرعي، وإن كان الأمر كذلك، فهل يكون الرد من خلال هجمة إلكترونية أم يجوز الرد باستخدام أسلحة تقليديـة. لا توجد في القانون الدولي إلى الآن إجابات قاطعة على هذه التسـاؤلات، خاصـة وأن هناك فريق من الفقهاء من يقتصر تعريف العدوان على استخدام القوة المسلحة[15]. إن مسألة العدوان في الهجمات السيبرانية تحتاج إلى بحث قائم بذاته يبين فيه تفصيلات الهجمات الإلكترونية التي تصل إلى حد العدوان في وقتي السلم والحرب.

إن عمليـات التخريب الإلكـتروني التي وقعت على أرض الواقع وأعلن عنها لم تصـل إلى حد العدوان؛ إذ لم تستهدف أي منها أرواح المدنيين. في المقابل هناك أمثلة واقعية حول عمليات تخريب استهدفت دولا ومؤسساتها، أدى البعض منها إلى شـل الحياة اليومية بما هدد معه سـيادة الدولة وقدرتها في إدارة شؤونها دون تدخل. من أبرز هـذه الأمثلة ما تعرضت له جمهورية إسـتونيا من هجمات إلكترونية عـام 2007، فتتمثل تلك الحادثة في هجمات استمرت 22 يومًا اسـتَهدفَت البنية التحتيّة الإلكترونيّة الأساسيّة لإستونيا، وعطلت خلالها المصالح بالوزارات، وإيقاف عمليات الصرف الآلي، وشَل مواقع الأخبار، وهذه الأفعال أدت إلى انقطاع الاتصالات الخارجية مما عزل

14 خليفة، 88.

15 Carsten Stahn, "'Jus ad bellum', 'jus in bello'... 'jus post bellum'? –Rethinking the Conception of the Law of Armed Force", The European Journal of International of International Law 17 (2007) 5: 923.

إســتونيا عن بقيّة دول العالم[16]. لقد حدث ذلك من خلال ما يُعرف بـ"بوت نيت"، أو شبكة الروبوت (Botnet)، والذي يســتطيع اختراق آلاف بل ملايين من أجهزة الحاســب الآلي والسيطرة عليها بالتجسس، وحجب المواقع، وإرسال البريد العشوائي، وغَمر مواقع الويب بملايين المشاهدات الوهمية، والتي بدورها تؤدي إلى تعطيل المواقع الإلكترونيّة[17]. اتهمت روسيا لكن لم يمكن الحصول على دليلٍ قاطع بتورطها[18].

منذ ذلك الحين المزيد من عمليات التخريب وقعت على دُوَل أخرى، منها الهجوم السيبرانيّ خلال قِمَّة مجموعة العشريــن في باريس عام 2011. وقد تمثل الهجوم بإرســال فيروس إلى البريد الإلكــتروني، والذي بدوره أصاب أجهزة الكمبيوتر الخاصة بكبار المســؤولين الحكوميين، بالإضافة إلى إرســال ذات الفيروس إلى البريد الإلكترونيّ لآخرين. وجهت أصابع الاتهام لدُول آسيويّة لكن دون الوصول إلى الفاعل[19].

إنّ مَخاطــر الهجمات الإلكترونية لا تقف عند وقت حدوث الهجمات ذاتها، بل قد تَسْــتمِّر لمُدَدٍ أطول بكثير، فلو اســتهدفت أجهزة التحكم الخاصة بمحطات الطاقة، وعرف الســبب – فيروس إلكترونيّ على سبيل المثال –، وتم التغلُّب على هذه الآفة وإعادة تشغيل المحطات، فهذا أمر جيد. لكن تكون المشكلة أكبر حينما تُعطل المحطات بشكل جَذري بحيث يتطلب تصليحها أسابيع، أو ربما أشهر من الصيانة. إن من يُحدِّد مَسار سلوك الدولة الضحيَّة في مثل هذه الاعتداءات هي الجهة المُعتدية بما يتوافق مع خططها ويخدم مصالحها، فقد يَستغلُّ الجُناة انشغال الدولة الضحيَّة بعمليّات الصيانة لارتكاب المزيد من الاعتداءات التي بدورها قد تُشلّ مقدرة الدولة الضحية على إصلاح الأضرار بشــكل أكبر. إن جســامة الفعل تتوقف على مقدرة الدولة التكنلوجيّة والماليّة التي تُتيح لها التصليح، أو التصنيع، أو شراء قطــع الغيار فكلما كانت الدولة متمكنة من إجراء عمليات التصليــح، كلما قل الضرر. على الرغم أن هذه الفرضيّة لم تقع عــلى أرض الواقع حتى كتابة هذا البحث، إلا أن تعزيز قدرات الدول على مواجهة الأزمات الناتجة عن الهجمات الإلكترونيّة أمر مهم، وهذه الاســتعدادات يجب ألا تقف عند الحَدِّ التكنلوجيّ، والتعاون بين الدُّول لإصلاح الضرر، وإنما لا بد من التأكيد على إدانة الفاعلين خاصَّةً إن كانوا دولًا، أو جهاتٍ مدعومةً من دُوَلٍ.

رَغم عَدَم تَقْنين القانون الدولي للتجســس السيبراني وعمليّات التخريب الإلكترونيّ كأنشطة إجرامية تتخطَّى الحــدود، إلا أن هذه الأفعال تتعارض مع المبادئ العامة للقانون الــدولي. فالقانون الدولي يرتكز على مجموعة من المبادئ التي تهــدف إلى حماية الدول والعلاقات الدولية، وأهم هذه المبادئ، مبدأ الســيَّادة الذي يَحْمي الدولة من التدخلات الخارجيّة، ومبدأ عَدم التَّدخل الذي يحمي السلامة السياسيَّة للدولة من خطر الإكراه[20].

16 المرجع نفسه، 21؛ انظر أيضًا:

Rain Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective" in Matthew Warren (ed), Case Studies in Information Warfare and Security for Researchers (London: Academic Conferences Limited, 2013) 121.

17 Heli Tiirmaa-Klaar and others, Botnets (New York: Springer Science & Business Media, Jun 29, 2013) 18.

18 Damien McGuinness, "How a cyber attack transformed Estonia", 27 April 2017, BBC News, online: <https://www.bbc.com/news/39655415>.

19 للمزيد حول هجمات التخريب الإلكتروني، انظر:

Fen Osler Hampson and Eric Jardine, Look Who's Watching, Revised Edition: Surveillance, Treachery and Trust Online (Watrloo: McGill-Queen's Press, 2016) 188.

20 Buchan, *idem*, 68.

المبحث الثاني: تعامل القانون الدولي مع الهجمات الإلكترونية

يُعتبر الإنترنت باستخداماته المُتنوعة مجالًا حديثًا نسبيًا وفي تطور مستمر، فالتكنولوجيّات الأساسيّة للإنترنت لها وجود منذ الستينات من القرن العشرين، لكن مع نهاية القرن الماضي وبداية القرن الحادي والعشرين، سريعًا ما تطورت استخدامات الإنترنت وصارت مُتاحَة على نِطاق واسِع. ومع ذلك، فإن تَقْنين استخدامات الفضاء الإلكترونيّ ظلّ متأخرًا بسبب ارتباطه بمسائل عمليّة لم يكن هناك وضوح حولها، أهمها فيما يتعلق برغبة الدول وقدرتها الفعليّة على تنظيم استخدامات الفضاء الإلكتروني، بل ومدى إمكانيتها في التوصل للجُناة في حال وقوع انتهاكات إلكترونيّة[21]. إن صعوبة التوصل للجناة تظهر جليا على الصعيد الدولي؛ إذ إن محاولات التَّقصّي التي تقوم بها الدَّولة الضحيّة قد تنتهي بعدم معرفة الفاعل، ناهيك عن فَرَضية رفض الدولة المُشتبَه بها التعاون بحجة السريّة والحساسيّة السياسيّة، بل إن الدولة الضحية قد تتعمد أن تتظاهر بعدم اكتشاف أن اقتحامًا إلكترونيًّا قد وقع على أجهزتها بغرض المزيد من البحث. أما على الصعيد المَحلّي فالتوصل للجناة ومحاسبتهم أسهل نسبيا. فدول متعددة استطاعت الكشف عن هويّة الفاعلين من العصابات الإجرامية والمتسللين الذين يعملون لمصلحتهم الخاصة في مناسبات عدة، وتعاملت مع هؤلاء وفق القانون الداخلي. على سبيل المثال، تَمَكَّن مكتب التحقيقات الفيدراليّ في الولايات المتحدة من كشف العديد من عمليّات احتيال رقمية وعمليات اقتحام إلكترونيّة لحسابات بنكيّة، وألقي القبض على الجُناة وحوسبوا قضائيّا[22]. تجدر الإشارة أن هذه الحالات رغم أهميتها لا تُشكل سوابق قضائيّة في القانون الدُّولي لأن الجهة الفاعلة لم تكن دولة[23]. مع ذلك، فإن استطاعة بعض الدول محاسبة الجناة قد يكون خطوة في تعزيز التعاون المشترك وتبادل الخبرات من أجل إتاحة فضاء إلكتروني آمن على الصعيدين الداخلي والإقليمي.

إن التقدم في وسائل معرفة وتتبع الجناة رغم أنها صارت متاحة أكثر – على الأقل لبعض الدول – إلا أن هذا التقدم لا يخلو من عقبات، والتي بدورها تؤثر على محاولات وضع إطار قانوني دولي للتعامل مع عمليات الاقتحام والتخريب الإلكتروني. وأبدأ بتجارب الدول المتقدمة في إحراز تقدما في الكشف عن الجناة، ثم إلى الصعوبات العملية التي تواجهها على الصعيدين الداخلي والإقليمي، والتي بطبيعة الحال تنطبق على الحالات التي تستلزم تدخل القانون الدولي في حل المنازعات بين الدول. فَعَلى الصعيد المحلي، في عام 2012 أعلنت الولايات المتحدة أنها تمتلك القدرة على تحديد موقع المخالفات والهجمات الإلكترونيّة[24]، وأنها بالفعل كشفت عن الفاعلين في مناسبات

21 Timothy S. Wu, "Cyberspace Sovereignty? The Internet and the International System", Harvard Journal of Law & Technology, Volume 10, Number 3 Summer 1997, p. 649.

22 "Nigerian National Arrested for Scheme to Conduct Cyber Intrusions to Steal Payroll Deposits" (June 2, 2021) Attorney's Office Southern District of New York, online: <https://www.justice.gov/usao-sdny/pr/nigerian-national-arrested-scheme-conduct-cyber-intrusions-steal-payroll-deposits>; "Russian Cybercriminal Convicted of Defrauding American Companies of Millions of Dollars Through Digital Advertising Scheme", U.S. Attorney's Office, Eastern District of New York (May 28, 2021) online: <https://www.justice.gov/usao-edny/pr/russian-cybercriminal-convicted-defrauding-american-companies-millions-dollars-through>.

23 Brown and Poellet, *idem*, 133.

24 James B. Comey, "Addressing the Cyber Security Threat", FBI, International Conference on Cyber Security, Fordham University, New York (January 7, 2015) online: <https://www.fbi.gov/news/speeches/addressing-the-cyber-security-threat>.

عِدّة وقامت بمحاسبتهم قضائيّا[25]. تلت الولايات المتحدة دولٌ أُخرى كبريطانيا وألمانيا في التأكيد على القُدرة على الكشف عن الجهات المسؤولة عن الهجمات الإلكترونيّة[26]. مع ذلك فإنَّهُ لا بد من التمييز بين تصريحات الدول، وبين ممارساتها الفعلية؛ إذ تكشف الممارسة الفعلية أن الدول ذاتها التي سبق ذكرها، لازالت تصدر تصريحات مختلفة تُشير إلى عَجزها – ولو جزئيًّا – في مجال الأمن الإلكتروني. على سبيل المثال، تعترف الولايات المتحدة بقصور القدرات الوطنية، وصعوبة العمل مع البلدان ذات القدرات المحدودة وذلك لملاحقة الجرائم الإلكترونية قضائيّا[27]. وقد أقرت بريطانيا بوجود نفس الصعوبة، فلاتزال الحاجة قائمة لتأهيل المزيد من الموظفين في مجال تكنولوجيا المعلومات والاتصالات، خاصة في مجال تنفيذ القوانين الوطنية[28]. والصعوبة تزيد في مُلاحقة الجرائم الإلكترونيّة في الكثير من البلدان النامِيَة التي لاتزال تفتقر إلى الهياكل الإلكترونية المتطورة والآمنة وإلى قوانين فعَّالة وفِرَق مُتخصصة لإنفاذ القوانين[29]. ورَغم العَقَبات العمليّة فإن الدُّول لم تستسلم، بل لازالت تعمل جاهِدة للتغلب عليها، ولكن جهود الدول المتطورة تكنلوجيًّا بمفردها لن تكون مجدية من دون شراكة الدول الأخرى، خاصة أن هذه الأخيرة قد يستغلها الجُناة كمعاقل لارتكاب جرائمهم والتهرب من الملاحقة. إن هذه الإشكاليات قد تخلق حالة من التردد لدى الدول للمضي في تقنين هيكل قانوني متكامل للتعامل مع الهجمات الإلكترونية التي تستوجب تدخل القانون الدولي، فإذا كانت الدول تواجه صعوبات على الصعيد المحلي، فكيف لها أن تواجه الصعوبات العالمية.

لقد أدى تردد الدول في العمل على تقنين شامل لممارسات الفضاء الإلكتروني على الصعيد الدولي، وكذلك بطء إجراءات تحضير وإبرام الاتفاقيات الدولية، إلى ضرورة إيجاد وسيلة أكثر مرونة لسد الفراغ العملي والتشريعي. لذلك نجد دخول منظمة الأمم المتحدة من خلال تشكيل فريق الخبراء الحكوميين المعني بالتطورات في مجال المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي لسد جزء من هذه الثغرة. فالمنظمات الدولية وعلى رأسها الأمم المتحدة لها دور في خلق قانون مرن كخطوة توجيهية لدول العالم. إن تدخل المنظمات الدولية هو أمر مألوف، فهذه المنظمات هي ضمن أشخاص القانون الدولي والتي تسعى من خلال التعاون مع الدول إلى تشجيع الأطراف لتنظيم المسائل العالقة وفق قنوات التفاوض في القانون الدولي.

25 "Wichita Lawyer Pleads Guilty to Being Involved in Cyberattack", U.S. Attorney's Office, District of Kansas, (October 15, 2019) online: <https://www.justice.gov/usao-ks/pr/wichita-lawyer-pleads-guiltyto-being-involved-cyberattack>; "California Telescope Enthusiast Sentenced to Prison for Cyber Attack", U.S. Attorney's Office, Western District of Oklahoma (December 4, 2018) <https://www.justice.gov/usao-wdok/pr/california-telescope-enthusiast-sentenced-prison-cyber-attack>.

26 "UK National Cyber Security Centre (NCSC) updates on the Turla Group" (21 October 2019) online: <https://www.ncsc.gov.uk/news/turla-group-behind-cyber-attack>; "Chancellor's speech to GCHQ on cyber security" GOV.UK (17 November 2015) online: <https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security>.
"Germany detects new cyberattack targeting politicians, military" Deutsche Welle (30 June 2018) online: <https://www.dw.com/en/germany-detects-new-cyberattack-targeting-politicians-military/a-46515590>.

27 تقرير الأمين العام "مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية"، 30 يوليو 2019، الأمم المتحدة، 74/ A/ 130، 106.

28 المرجع نفسه.

29 تقرير فريق الخبراء الحكوميين المعني بالتطورات في مجال المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، 24 يونيو 2013، الجمعية العامة للأمم المتحدة، 68/ A/ 98، 15.

إن أمـــن الفضاء الإلكتروني هو أحد الفروع التي لاتزال مَحـــلَّ تطوير وتقنين دولي، فلقد عملت الجمعية العامة للأمم المتحدة على إصدار توصيات حول جرائم أجهزة الحاسب وقضايا الأمن الإلكتروني منذ التسعينات من القرن العشريـــن، ومع ذلك لم يأتي اعتراف المجتمع الدولي بتطبيق القانون الدولي على الفضاء الإلكترونيّ بشـــكل صريح حتـــى عام 2013[30]. جاء ذلك في تقرير فريق الخبراء الحكوميين المَعني بالتطورات في مجال المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي الذي أنشأته الجمعية العامة للأمم المتحدة، والذي ينصُّ على أن "القانون الدولي، وخاصة ميثاق الأمم المتحدة، قابل للتطبيق، وهو ضروري للحفاظ على السلام، والاستقرار، وتعزيز بيئة تكنولوجيا المعلومات والاتصالات لأن تكون مفتوحة، آمنة، ســـلمية، ومتاحة"[31]. وصفت الولايات المتحدة هذا القرار باعتباره إجماع تاريخي حول فهم القضايا السيبرانية ذات الأهمية الوطنية والدولية الحاسمة وتأكيد على التزام الدول في التقيد بالقواعد والمبادئ الراســـخة في القانون الدولي[32]. ورغم أن القرار غير ملزم فإن له قيمة أدبية هامة لصدوره تحت مظلة الأمم المتحدة. تجدر الإشارة بأن فريق الخبراء الحكوميين الذي شكلته الأمم المتحدة تألف من ممثلين 15 دولة عضو في الأمم المتحدة، بما في ذلك قوًى سيبرانية عظمى أهمها الولايات المتحدة، روسيا، والصين[33]. إن هذه المعطيات تعكس اهتمام المجتمع الدولي في تنظيم الفضاء الســـيبراني بما يحقق الأمن والسلم الدوليين. رغم هذا الحماس فإن القيمة الفعلية لهذا القرار محل جدل، فلقد أثار التقرير أسئلة أكثر من تلك التي أجاب عليها. فليس هناك خلاف حول أهمية تطبيق القانون الدولي، لكن الســـؤال هو أي قواعد القانون الدولي قابلة للتطبيق في المجال السيبراني؟ لم يجب القرار صراحة على هذا السؤال، وهو ما يسعى البحث الإجابة عليه.

إنّ قواعد القانون الدولي ذات طابع متطور؛ إذ إنها قابلة لمواكبة المســـتجد من الأمور على الســـاحة الدولية[34]، فمســـائل كثيرة لم تكن معالجة في الماضي، صارت لها قواعد تنظيميّة مفصلة، كمسائل الفضاء الخارجي التي لم تكن موجودة وقت إنشـــاء ميثـــاق الأمم المتحدة[35]. فوفقًا لرأي الفقيه جي أل بريرلي فـــإن الهدف من القانون الدولي في التعامل مع المشـــكلات المتجددة، هو ليس تقديم حلول جامدة ذات تطبيقات حَرفِيَّة، بل الهدف هو إنشاء هياكل عامة لفهم المشـــكلات التي تواجه الدول، وتوفير إطار قانونيّ للاستجابة لسلوك وأفعال الدول. هذا الاستخدام للقانون الدولي يتيح للدول فهم الإشـــكاليات الموجودة، وكذلك معرفة الخيارات المتاحة، والمقبولة دوليًّا للتعامل مع المشـــكلة[36]، وهذا الفَهم للقانون الدولي يســـمح بتبني حلولًا مرنة، تُتيح للدول التعامل مع المشـــكلات التي تواجهها بما يتناســـب مع نُظمها القانونيـــة، وفي ذات الوقت هذه الحلول مبنيّة على مبـــادئ ثابتة، ومتفق عليها في القانون الدولي، والتي بدورها تؤمن مناخًا قائمًا على التعاون، وحسن النية.

30 تقرير فريق الخبراء الحكوميين المعني بالتطورات في مجال المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، مرجع سابق، 8.

31 المرجع نفسه، 9.

32 US Department of State, "Statement on Consensus Achieved by the UN Group of Governmental Experts on Cyber Issues" (7 June 2013) <https://2009-2017.state.gov/r/pa/prs/ps/2013/06/210418.htm>.

33 Kubo Mačák, From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers (2017) 30 Leiden Journal of International Law 877, 4-5.

34 عيسى عبيد، **محكمة العدل الدولية ودورها في تطوير قواعد القانون الدولي الجنائي**، دار أمجد، عمان، 2017، ص105.

35 Mačák, *idem*, 13.

36 J. L. Brierly, The Law of Nations: An Introduction to the International Law of Peace (Oxford: Oxford University Press, 1963) 76.

لو افترضنا أنه طورت القُــدرات المخابراتيّة والتكنولوجيّة، وبالفعل عرفت هوية الفاعل من الدول الأخرى، فإن تحديد أي قواعد القانون الدولي قابلة للتطبيق هي مسألة جوهرية. يرى البحث أنه في ظل غياب قواعد قانونية دوليــة عرفية واتفاقية كافية حــول العمليَّات المُرتكَبة في الفضاء الإلكتروني، فــإن الأمر يقتضي البحث في مبادئ القانون الدولي، وتحديدًا مبدأ السيادة ومبدأ عدم التدخل.

المطلب الأول: الحق السيادي للدول على فضائها الإلكتروني

عندما تكون شبكات الإنترنت مدعومة بالبنية التحتية في دولة ما، وتخترق، أو تخترق أجهزة الحاسوب ويحصل على المعلومات المُخزَّنة فيها، فإنّ الدولة الضحية تَعتَبر أنّ ســيادتها الإقليميّة مُنتهكة؛ إذ يرى البحث أن التجسس الإلكتروني هو سلوك ينتهك مبدأ السيادة. ويقصد بمبدأ السيَادة مُمارسة الدولة لسلطاتها العليا السياسية والقانونية على إقليمها بشــكل مُطلق دون انتقاص، أو تجزئة، فلكُلّ دولة سلطان على أراضيها، مما يعني أنه لا يجوز لأي دولة أن تقوم بتجريد دولة أخرى من ســلطاتها[37]. وقد أوضح المُحكِّم ماكــس هوبر في قرار التحكيم في جزيرة بالماس بأن: "السيادة في العلاقات بين الدول مفادُها الاستقلال، الاستقلال فيما يتعلق بجزء من الكرة الأرضية، هو الحق الخاص فيه، "وبممارســة وظائف الدولة على ذلك الجزء"[38]. وفق هذا المعنى، فإن الســيادة والاســتقلال لا ينفك أحدهما عن الآخر، فالدول المستقلة هي من لها الحق المطلق والانفرادي بممارسة سلطاتها السيادية على أرضها. وقد تطرَّقت محكمة العدل الدُّوليّة للســيَّادة والاســتقلال في قضية "قناة كورفو" مُشيرة إلى أن "بين الدول المستقلة، يُعَدّ احترام الســيادة الإقليمية أساسًا جوهريا للعلاقات الدولية"[39]. فمبدأ السيادة هو من المبادئ المُسلَّمُ بها في القانون الدولي والتي من شأنها تعزيز السِّلم والعلاقات الدولية.

رغم رُسوخ مبدأ السيادة في القانون الدولي، فإن المُمارسة العمليّة لا تخلو من خروقات، وهذه الخروقات شملت المجال الســيبراني؛ حيث انتهك هذا المبدأ من قبل دول عدة وفي مناســبات مختلفة. على ســبيل المثال، عام 2013 اكتشف تجســس الولايات المتحدة بشكل مستمر على البرازيل، مما دفع رئيسة البرازيل آنذاك (ديلما روسيلف) إلى إلغاء رحلتها المقررة إلى واشــنطن للقاء رئيس الولايات المتحدة آنذاك باراك أوباما احتجاجا على الأمر، بل قامت بأكثــر من ذلك؛ إذ توجهت إلى مقر الأمــم المتحدة، واصِفةً الأمر بالاعتداء على القانون الدُّولي والســيادة. تقول روسيلف: "إن التَّطفل على هذا النحو في حياة وشــؤون البُلدان الأخرى هو انتهاك للقانون الدولي وهو بِحدِّ ذاته إهانة للمبادئ التي يجب أن تنســق العلاقات فيما بين الدول، لا ســيّما الصديقة، ولا يمكن لدولة ما أن تعلو على حســاب سيادة دولة أخرى."[40] إن المُفردات التي استخدمتها رئيســة البرازيل تُمثِّل تبيانا لمَنطق القوة الذي تستغله

37 Simona Ţuţuianu, Towards Global Justice: Sovereignty in an Interdependent World (The Hague: Springer Science & Business Media, 2012) 18.

38 Island of Palmas Case (Netherlands v. USA) Reports of International Arbitral Awards, 4 April 1928, 838.

39 Corfu Channel Case (United Kingdom of Great Britain and Northern Ireland v. Albania) ICJ Reports of judgments, 9 April 1949, 35.

40 المرجع نفسه؛ وانظر أيضًا: Julian Borger, 'Brazilian President: US Surveillance a 'Breach of International Law,' The Guardian, September 24, 2013, online: <http://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance>.

بعض الدول للاعتداء على القانون الدولي وعلى سيادات دول أخرى والتي قد تمر دون محاسبة. إن عدم وجود سوابق قضائية حول انتهاك مبدأ السيادة في المجال السيبراني يضعف من شأن الحماية القانونية للضحايا من الدول من خطر التجسس. لكن لا بد من الالتفات إلى حقيقة أن المجال السيبراني حديث نسبيا، لذلك فإن عدم وجود سوابق قضائية قد يكون نتيجة منطقية لذلك. المشكلة هي أن التجسس موجود منذ القدم، لكن لم تُحاسب أي دولة على أفعال التجسس التقليدية – كما بينا في موضع سابق من البحث. إن هذا البحث يرفض التسليم بالاستمرار بعدم حظر التجسس، خاصة التجسس السيبراني، لما لهذا الفعل من خطر على مستقبل الأمن والسلم الدوليين، ناهيك عن مساسه بمبدأ السيادة. لذا ينظر البحث بالسوابق القضائية التي تمحورت حول مبدأ السيادة، ومن ثم قياس هذه الأحكام على حالات التجسس السيبراني.

إن القضاء الدولي لا يخلو من السوابق التي تؤكد على أهمية احترام مبدأ السيادة. ومن الأحكام القضائية التي تؤكد على حظر الاعتداء على السيادة ما جاء في قضية "لوتس"، فقد أوضحت المحكمة الدائمة للعدل الدولي أنّ "القيد الأول والأهم الذي يَفرِضُه القانون الدولي على دولة ما هو أنه – في حالة عدم وجود قاعدة تسمح بعكس ذلك – لا يجوز لها مُمارسة سلطتها بأي شكل في أراضي دولة أخرى"[41]. بمعنى أنه يحق للدول ممارسة سيادتها كما تشاء، طالما لم تتعارض ممارستها مع حَظر صريح. ويُعتبر من المحظورات مُمارسة دولة لسيادتها على إقليم دولة أخرى دون رضا الأخيرة.

ومثال آخَر على تطبيقات مبدأ السيادة ما جاء في قضية قناة "كورفو"، حيث قامت المملكة المتحدة بإرسال سُفُن حربيّة إلى المياه الإقليمية لألبانيا لجمع أدلَّة على التعدين غير القانوني، وقد استنكرت محكمة العدل الدُّوليّة تصرف المملكة المتحدة بتصريحها أنه "لا يُمكن للمحكمة أن تعتبر الحقَّ المزعوم في التدخل إلا تجسيدًا لسياسة القوة، حيث أدَّى إلى حدوث انتهاكات جسيمة في الماضي، ولا يمكن لمثل هذه الانتهاكات أن تجد مكانًا في القانون الدولي"[42]. واستطردت المحكمة بالقول إنه "بين الدُّول المُستقلة، يُعتبر احترام السيادة الإقليمية، ركيزة أساسية للعلاقات الدولية... لكن لضمان احترام القانون الدولي... يجب على المحكمة أن تُعلن أن تصرفات فِرقة البَحريَّة البريطانيَّة تُشكّل انتهاكًا للسيادة الألبانية"[43]. إنّ أساس عدم مَشروعيّة سلوك المملكة المتحدة في المياه الإقليمية الألبانية هو اقتحام سُفُنها العسكريّة للمياه دون تصريح[44]؛ أي أن مبدأ السيادة يشترط احترام أقاليم الدُّول الأخرى، بغض النظر عن وقوع ضرر مادي من عدمه.

إن مجرد دخول دولة ما إقليم دولة أخرى دون اشتراط وقوع ضرر مادي يعتبر انتهاكا لمبدأ السيادة. قياسًا على ذلك، يُمكن اعتبار استخدام طائرات الاستطلاع فوق الإقليم الجوي لدولة أخرى انتهاك لسيادتها. ويبقى السؤال حول مَدى إمكانيّة قياس عمليات استخدام طائرات الاستطلاع للتجسس على عمليات التجسس الإلكترونيّة التي تقع – على سبيل المثال – على قاعدة البيانات لدولة ما، فعمليات الاقتحام الإلكتروني بغرض جمع المعلومات بحد ذاتها لا تترك آثارًا ماديّة تخريبيّة ضارة على قاعدة البيانات، أو البنية التحتية للدولة الضحيّة.

41 The Case of S.S. 'Lotus', (France v. Turkey), PCIJ Reports of Judgments. Series A No. 10, 7 September 1927, paras. 19–20.

42 The Corfu Channel Case, *idem*, 35.

43 Ibid.

44 Buchan, *idem*, 70.

إنّ السيادة الإقليميَّة للدولة على فضائها الإلكتروني يقتضي إخضاع عمليّات الاقتحام والتجسس الإلكتروني لمتطلبات مبدأ السيادة، إلا أن هذا الأمر لم يعالجه القانون الدُّولي بشكل صريح إلى الآن. رغم ذلك فإن جانبًا من الفقه ينظر إلى عمليات التجسس وقت السِّلم بأنها تشكل انتهاكًا ليس فقط للقانون الداخليّ، وإنما للقانون الدُّوليّ أيضًا، والذي يقضي بأنه "على الدول احترام وحدة الأراضي والاستقلال السياسيّ للدول الأخرى"[45]. فمن خلال هذا الفهم لعمليات التجسس التي تتعارض مع مبدأ السيادة يمكن قياس التجسس الإلكتروني عليها، فالفضاء الإلكتروني بما فيه من بنية تحتية، وأجهزة إرسال واستقبال، وحاسوب، كل منها يخضع لإقليم دولة ما. ولأن عمليّات الاقتحام الإلكترونيّة تكون دون موافقة الدولة الضحية، فإنه يمكن – بل يجب – اعتبار أي اطلاع، أو تجميع لمعلومات غير متاحة للجمهور انتهاكا لمبدأ السيادة.

وتثور إشكالية أُخرى حول التجسس الإلكتروني ومبدأ السيادة حينما تكون المعلومات الإلكترونية التي تملكها دولة ما غير موجودة على إقليم نفس الدولة، فالمعلومات تمر في الفضاء الإلكتروني لدول أخرى، بل وعلى مساحاتٍ لا تخضع لإقليم مُعيّن كأعالي البحار. فالفضاء السيبرانيّ مجال مفتوح للاتصالات والمعلومات التي تملكها دولة ما، وتخزنها، أو تنقلها من خلال البنية التحتية الإلكترونيّة الموجودة على أراضي دولة أخرى. حينما تستخدم الدُّول هذا الفضاء السيبراني، فإنها ترغب في حماية ليس فقط ملكيتها للمعلومات، وإنما أيضًا حقها في الحفاظ على خصوصيّتها وسريّتها بعدم التعرض لها بالكشف، أو السرقة، أو النشر. قد يبدو للبعض أن حق الدولة على معلوماتها في الفضاء السيبراني أمر بَديهيّ، لكن ما هو الأساس القانوني لحمايتها حينما تكون خارج إقليم الدولة؟ إن موضوع سيادة البيانات الوطنية نظمته اتفاقية الأمم المتحدة لحصانة الدول وممتلكاتها من الولاية القضائية لعام 2004، فوفقا للاتفاقيّة تكون للدولة وممتلكاتها – ذات الطبيعة غير التجارية – حصانة من ولاية المحاكم الأجنبية حتى عندما تكون الممتلكات موجودة في أراضي دولة أخرى[46]. في ضوء هذا المعنى يمكن قياس الحصانة القضائيّة لممتلكات الدولة، على حقها بالاحتفاظ بسيادة تامة مانعة على معلوماتها الإلكترونيّة، التي تملكها خارج أراضيها[47].

إنَّ توجُّه المجتمع الدولي ينصب نحو التأكيد على وجود علاقة سيادية بين الفضاء الإلكتروني والدول. على سبيل المثال، ينص تقرير فريق الخبراء الحكوميين المَعْني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي على أن "تنطبق سيادة الدولة، والقواعد، والمبادئ الدولية المنبثقة عنها، على سلوك الدُّول فيما يتعلَّق بالأنشطة المتصلة بموضوع تكنولوجيا المعلومات والاتصالات، وعلى ولاياتها القضائية، بشأن هياكلها الأساسية لتكنولوجيا المعلومات والاتصالات داخل أراضيها."[48] إن هذه التوصية تؤكد على أنه في الفضاء الإلكتروني ينطبق مبدأ السيادة وكذلك المبادئ الدولية الأخرى المتصلة والمكملة لمبدأ السيادة، والتي يرى البحث أن من أهمها مبدأ عدم التدخل ومبدأ حسن النية. إن توصية فريق الخبراء الحكوميين تؤكد بأن الفضاء

45 Quincy Wright, 'Espionage and the Doctrine of Non-Intervention in Internal Affairs,' in *Essays on Espionage and International Law*, ed. Richard Falk (Ohio: Ohio State University Press, 1962) 12.

46 المادتان 5 و10 من اتفاقية الأمم المتحدة لحصانات الدول وممتلكاتها من الولاية القضائية لعام 2004، قرار الجمعية العامة للأمم المتحدة رقم 59/ 38، 2 ديسمبر 2004.

47 Buchan, *idem*, 76.

48 تقرير فريق الخبراء الحكوميين المعني بالتطورات في مجال المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، 10.

الإلكتروني منطقة خاضعة للقانون، وأن حجة فشـــل القانون الدولي في مواكبة تحديات التطور السريع لتكنولوجيا المعلومات والاتصالات لم تعد مقبولة. بناء على التوصية أعلاه يمكن الاستنتاج بأنه لا يمكن الأخذ بحجة إخراج الفضاء الإلكترونيّ من مظلة القانون الدولي، فمبدأ السيادة يحكم النشاط السيبراني.

إن مبدأ الســـيادة يحمي الدولة بما في ذلك بنيتها التحتيّة وكذلك المعلومات التي تملكها خارج إقليمها كَجُزء من ســـيادة البيانات الوطنية من خطر التدخل المادي. كذلك فإن مبدأ الســـيادة يعالج عمليّات التخريب الإلكتروني بشكل لا شك فيه؛ إذ إن الإضرار بالبنية التحتيّة، أو بقواعد البيانات يُعد انتهاكا لسيادة الدولة وسلامتها الإقليمية. ولا بد من التأكيد أن الحماية القانونية تتوفر، سواء أدى نشاط الدولة المُعتدية إلى إحداث ضرر مادي، أو لا كما بينا في موضع سابق من هذا المطلب. ويُمكن أن نستنتج من ذلك أن عمليات التجسس السيبراني سواء قادت إلى عمليات تخريب مادية، أو وقفت عند حد الاطلاع وأخذ المعلومات دون إذن، فإنها تُشكِّل انتهاكًا لمبدأ السيادة.

المطلب الثاني: حق الدول بصون فضائها الإلكتروني من عدم التدخل

إن حق الدولة بالانفراد بالتصرف بملكيتها التي تشـــمل البيانات والمعلومات الرقمية والبنية التحتية للإنترنت يقتضي منع الدول الأخرى من التدخل، فكما بينا في المطلب السابق أن القانون الدولي يضفي حماية سيادية للبيانات الوطنية. إن احترام الســـيادة والسلامة السياســـية للدول يسري بشكل موازٍ لمبدأ عدم التدخل، والذي يحمي الحقَّ الســـياديّ للدولة في تحديد شـــؤونها الداخلية والخارجية دون تدخل خارجي. ويمكن النظر إلى مبدأ عدم التدخل باعتباره مُكمِّلًا لمبدأ السيادة، فحماية الســـيادة تقتضي مَنْع التدخلات الخارجيّة. وكما أشرنا سابقًا، فإن التدخلات المعنيّة هي تدخلات أشخاص القانون الدولي العام من دول ومنظمات، ولا يُقصد به تدخّل الأفراد، أو الجماعات، مـــا لم يكونوا مدعومين من دول أخرى. وقد أكد ميثاق الأمم المتحدة على هذا المعنى بنصه: "ليس في هذا الميثاق ما يُســـوّغ للأمم المتحدة أن تتدخل في الشؤون التي تكون من صميم السلطان الداخلي لدولة ما، وليس فيه ما يقتضي الأعضاءَ أن يَعْرضوا مثل هذه المسائل لأن تحل بحكم هذا الميثاق"[49].

وقـــد أكدت محكمة العدل الدوليّة على هذا المعنى بِنصِّها عـــلى أنَّ "يَنْطوي مبدأ عَدم التدخل على حق كل دولة ذات سيادة في إدارة شـــؤونها دون تدخُّل خارجيّ"[50]. وتُقِرُّ المحكمة بأنّه "على الرَّغم من أنَّ أمثلة التعدي على هذا المبدأ ليســـت نادرة" إلا أنّ المحكمة تعتبر مبدأ عدم التدخل "جزءً لا يتجزأ مـــن القانون الدولي العرفي"[51]. وتؤكد المحكمة على أن القانون الدولي يتطلب احترام "الســـلامة السياسية" للدولة، كما تُقر المحكمة بأن وجود مبدأ عدم التدخل هو بمثابة "نتيجة طبيعية لمبدأ المساواة في السيادة بين الدول"[52]. إذا فمبدأ عدم التدخل يعمل جنبا إلى جنب مع مبدأي السيادة والمساواة، ومجموع هذه المبادئ يعزز من احترام السلامة السياسية للدول ويحافظ على العلاقات الودية فيما بينها.

49 الفقرة الثانية من المادة 7 من ميثاق الأمم المتحدة، 26 يونيو 1945.

50 Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), ICJ 14 Reports of Judgments, 27 June 1986, para 202.

51 المرجع نفسه، فقرة 263.

52 المرجع نفسه، فقرة 202.

لقد جاء إعلان مبـــادئ القانون الدولي المتصلة بالعلاقات الودية والتعاون بين الدول وفقا لميثاق الأمم المتحدة ليحدد الســـلوك المقبول في التعاملات بين الدول، ويشـــمل هذا الســـلوك المقبول عدم التدخل في شؤون الدول الأخرى. ينص الإعلان على أهمية "مُراعاة الدول الصديقة للالتزام الذي يقتضي عدم التدخل في شـــؤون أية دولة أخرى، هو شرط أساسي لضمان عيش الأمم معا في سلام، لأن ممارسة أي شكل من أشكال التدخل أمر لا يقتصر على خرق الميثاق معنى ونصا، بل يؤدي كذلك إلى خلق حالات تهديد السلم والأمن الدوليين"[53].

واســـتطرد الإعلان بالنـــص على أنه "ليس لأيّة دولـــة، أو مجموعة من الدول أن تتدخـــل، بصورة مباشرة، أو غير مباشرة ولأي ســـبب كان، في الشـــؤون الداخلية والخارجية لأية دولة أخرى، وبالتالي فإن التدخل المُســـلَّح، وكافة أشـــكال التدخل، أو محاولات التهديد الأخرى، التي تستهدف شـــخصية الدولة، أو عناصرها السياسية، والاقتصادية، والثقافية، تُمثل انتهاكًا للقانون الدولي.

ولا يجوز لأيّة دولة اســـتخدام التدابير الاقتصادية، والسياســـية، وأي نوع آخر منها، أو تشـــجيع استخدامها، لإكراه دولة أخرى على النزول عن مُمارسة حقوقها السيادية، والحصول منها على أية مزايا.

كما أنه لا يجوز لأية دولة تنظيم النشـــاطات الهادمة، أو الارهابية، أو المسلحة، التي ترمي إلى قلب نظام الحكم في دولة أخرى بالعنف، أو مساعدة هذه النشاطات، أو التحريض عليها، أو تمويلها، أو تشجيعها، أو التغاضي عنها"[54].

يقدم الإعلان فهما شـــاملا لصور التدخل المحظور التي تهدد الأمن والســـلم الدوليـــين، والتي لا تقتصر على استخدام القوة المسلحة، وإنما تشمل وسائل الإكراه الاقتصادي والسياسي، والأنشطة الإرهابية، بل وأي تحريض، أو تمويل لها. إن هذه الصور رغم أهميتها فإنها تظل توصية غير ملزمة، ناهيك أن معنى عدم التدخل لا يزال يشوبه الغموض، فليس من الواضح ما إذا كان حظر التدخل المقصود يســـتلزم عناصر كالإكراه، أو القسر، أو استخدام القوة المســـلحة، والتي بدورها تتســـبب بأضرار ماديّة للدولة، أم أن التدخل المحظور يَشـــمل أعمالًا لا تؤدِّي إلى إحداث أضرار مَلْمُوســـة، كالاطلاع على المعلومات، أو أخذهـــا دون إذن. فَفِي قضية "نيكاراغوا"، قدمت محكمة العدل الدوليّة مفهوما حول عدم التدخل، اشـــترطت فيه توافر عنـــصران: الأول هو الإكراه والقسر، والثاني هو التأثير على الدولة المُستهدَفة بطريقة تحرمها من ممارسة ســـيادتها بشكل معتاد وحر[55]. فالتدخل المحظور الوارد في قضية نيكارغوا يُقصد به استخدام الإكراه، أو القسر للتأثير على إرادة الدولة في ممارسة خياراتها بحرية على نظامها. في المُقابل فإنّ التدخل الذي يحدث خارج سياق استخدام القوة، لايزال من دون تقنين واضح.

إنّ محكمة العدل الدولية لم تبين المقصود بالإكراه والقسر خارج ســـياق استخدام القوة، وتَرْك هذه المسألة دون تقنين قانونيّ واضح دفع البعض إلى تفســـير الإكراه وفق معيار ضيق. فعلى ســـبيل المثال، يرى الفقيه لاسا أوبنهام بأن التدخل غير المشروع هو: "تدخل ديكتاتوري... في شـــؤون دولة أخرى بغـــرض الحفاظ على، أو تغيير الحالة

53 إعلان مبادئ القانون الدولي المتصلة بالعلاقات الودية والتعاون بين الدول، قرار الجمعية العامة للأمم المتحدة 2625 (د25–)، 24 أكتوبر 1970.

54 المرجع نفسه.

55 Case Concerning Military and Paramilitary Activities in and against Nicaragua, *idem*, para. 205

الفعليّة للأشياء"[56]. وَوِفق هذا المعنى فإن الخَطَّ الفاصل بين ما هو مسموح وغير مسموح، بشأن التدخل، أو التأثير على دولة أخرى، هو حينما يُراد من الفعل إجبار الدولة على التصرف، أو الامتناع عن التصرف، خارج إرادتها في الظروف العاديّة[57]. ولكنّ تدخل دولة ما بشكل استبدادي لفرض تغييرات في السياسة الداخلية، أو الخارجية لدولة أخرى يمثل تفسيرًا ضيقًا للتدخل غير المشروع، لذلك يُسلِّم البعض بصعوبة تطبيق مبدأ عدم التدخل في السياق السيبراني، لأن التجسس الإلكتروني قد يتوقف على الإلمام بأسرار الدولة الضحية دون استلزام عنصر القسر، أو الاجبار والذي ينتفي معه التأثير على سلوك الدولة.

من المعلوم أن أحكام محكمة العدل الدولية، ذات حجية نسبية تنطبق على أطراف النزاع فقط، مع ذلك يبقى لهذه الأحكام قيمة أدبية هامة في تقديم التفسير القانوني. لكن للأخذ بالتفسير القانوني المُقدم في قضية ما، لا بد من وجود تقارب بين القضيّة الحاليّة محل النزاع، والقضيّة التي تمَّ الفصل فيها، فنجد في قضية نيكاراغوا أنّ محكمة العدل الدولية نظرت إلى الحالة المعروضة أمامها حينما يكون التدخل "خصوصا واضحًا في حالة التدخل الذي يستخدم القوة"، واستطردت المحكمة بأنها ستحدد فقط جوانب المبدأ التي يبدو أنها ذات صلة بحل النزاع[58]. ويمكن الاستنتاج من هذا النص بأن المحكمة قدمت مفهوما حَوْل مبدأ عدم التدخل بناءً على أمرين، الأول خاص في حالة التدخل الذي يستخدم القوة، والثاني خاص في النزاع المعروض، أي أنها لم تقدم تفسيرًا عامًّا لمبدأ عدم التدخل، وإنّما اقتصر حكمها على الجوانب المتعلقة بالمنازعة المعروضة على وجه التحديد.

يقول الفقيه القانوني راسل بوكان: إنه يجب قراءة حكم محكمة العدل الدولية باعتباره يقدم تفسيرًا جزئيًا وغير مكتمل لمبدأ عدم التدخل، وبالتالي لا يمكن قياس حكمها في قضية نيكارغوا على السلوك الذي لا يتضمن استخدام القوة مثل التجسس الإلكتروني[59]. ويجادل بوكان بأنه في حين أن مبدأ السيادة يحمي البُعد الماديّ المتمثل بأراضي الدولة وممتلكاتها، فإن مبدأ عدم التدخل أيضًا مُصمَّم لحماية السيادة، لكن بجانبها الميتافيزيقي المُتمَثل في السَّلامة السياسيّة للدولة[60]. وهذه السلامة لا تتحقق دون حماية قانونية دولية للبيانات والمعلومات، التي تملكها الدولة إلكترونيا، والتي ترغب في الحفاظ على خصوصيتها، وسريتها من الاطلاع غير المأذون به. هذه الحُجَج تدفعنا إلى الدعوة إلى التوسع في تفسير مبدأ عدم التدخل، بحيث يشمل المُمارسات الحاصلة دون رضا الدولة الضحيّة، سواء توفّر، أو انتفى عنصر استخدام القوة، أو الإكراه، أو القسر.

نَجِد أن مفهوم عدم التدخل ليس جامدًا ومقصورًا على استخدام القوة، فهُنالِك مُمارسات قانونيّة أَخذت بالفعل مفهومًا أكثر توسُعا حول مبدأ عدم التدخل. من هذه الممارسات الدعوى المُقامة أمام محكمة العدل الدوليّة من قِبَل تيمور الشرقية ضد أستراليا، والتي ادعت فيها تيمور الشرقية أن أستراليا تواصلت مع مَكتب مُحامٍ في أستراليا يعمل لصالح تيمور الشرقية، وذلك لجمع معلومات سِرِّيّة تتعلق بالتقاضي القائم بين الدولتين، وقد طالبت تيمور

56 Lassa Oppenheim and Hersch Lauterpacht, International Law: A Treatise. Vol. I, Peace, 8th edn (London: Longman, 1955) 305.

57 Buchan, *idem*, 77.

58 Case Concerning Military and Paramilitary Activities in and against Nicaragua, *idem*, para 205.

59 Buchan, *idem*, 79.

60 المرجع نفسه، 78.

الشرقية الحصول على أمر مؤقت لإيقاف نشاط أستراليا، وتدمير المُستندات والبيانات التي حصلت عليها أستراليا. وقد جاء حكم محكمة العدل الدولية بأنه "في هذه المرحلة من الإجراءات... تحتاج [المحكمة] أن تُقرِّر ما إذا كانت الحُقوق التي تُطالِب بها تيمور الشرقية بِشأن الأُسُس الموضوعيّة، والتي تَسعى إلى الحِماية من أجلِها، معقولة"[61]. اعتبرت محكمة العدل الدولية أن مطالبة تيمور الشرقية معقولة، وعلى أساسه أصدرت أمرًا مؤقتًا بأنه يجب على أستراليا "عدم التدخل بأي شكل من الأشكال في الاتصالات بين تيمور الشرقية ومستشاريها القانونيين"[62]. إن هذا الحُكم يُقدِّم مفهومًا مُوَسَّعًا لمبدأ عدم التدخل؛ إذ يشترط أن يكون أساس المطالبة بعدم التدخل معقولًا، دون اشتراط وقوع إكراه فعلي أثَّر على سلوك الدولة الضحية. إن التفسير المتوسع لمبدأ عدم التدخل يتوافق مع المنطق ومقتضيات العصر حيث المعرفة قوة، فتجميع المعلومات بشكل غير مشروع هو شكل من أشكال التدخل الذي تتوافر معه احتمالية استخدام الإكراه ضد الدولة الضحية والتأثير على سلوكها مُستقبلًا.

إن تفسير محكمة العدل الدوليّة لمبدأ عدم التدخل في قضية تيمور الشرقية ضد أستراليا أعلاه، تزيد فاعليته حينما يطبق جنبًا إلى جنبٍ مع مبدأ السيادة – الذي تناولناه بالتفصيل في المطلب السابق – وأيضًا مع مبدأ المساواة في السيادة، ولقد أكدَّ ميثاق الأمم المتحدة على مبدأ المُساواة في السيادة؛ حيث تنصُّ المادة الثانية من ميثاق الأمم المتحدة على أن "تقوم الهيئة على مبدأ المساواة في السيادة بين جميع أعضائها." وهذا المبدأ يؤكد على أن جميع الدول متساوية في السيادة، بغض النظر عن الحجم، أو الكثافة السكانية، أو الثقل السياسي؛ لذا ليس من حق أي دولة أن تتدخل في شؤون دولة أخرى، بما فيها المُمارسات التي تقع خارج إرادة، أو رغبة الدولة الضحية.

إن هذه المبادئ مُجتمعة تُنشئ حماية للدولة على سيادتها من التدخلات الخارجية، بما في ذلك التدخلات الناشئة عن الأنشطة السيبرانية. في هذا السياق أكَّد فريق الخبراء الحكوميين حول التطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي التابع للأمم المتحدة بأنه على الدول الامتناع عن التدخل في شؤون الدول الأخرى؛ إذ "يجب أن تفي الدُّول بالتزاماتها الدولية فيما يتعلق بالأفعال غير المشروعة دوليًا المنسوبة إليها، ويجب ألا تستخدم الدول وكلاءً لارتكاب أفعال غير مشروعة دوليًا، كما ينبغي أن تسعى الدول إلى ضمان عدم استخدام أراضيها من قِبَل جهات فاعلة دون الدُّول الأخرى للاستخدام غير القانوني لتكنولوجيا المعلومات والاتصالات."[63] إن صياغة هذه التوصية جاءت بلغة عامة بعيدة عن التفصيل، مع ذلك فهي تؤكد على التزامات معينة. فعلى الدول عدم الانخراط بأفعال غير مشروعة دوليا في مجال المعلومات والاتصالات بما يؤثر سلبا على الأمن الدولي، وكجزء من هذا الالتزام فإن على الدول عدم استخدام وكلاء عنها لتنفيذ عمليات غير مشروعة ضد دول أخرى. فالدولة تكون مسئولة عن أنشطة الجهات التي توظفها، أو تمولها لتعمل لصالحها، وهو التزام سلبي بامتناع الدولة عن الانخراط بعمليات غير مشروعة بنفسها، أو عن طريق وكلاء. كذلك على الدول ضمان عدم استخدام أراضيها لأغراض غير مشروعة من قبل جهات مستقلة، وهو التزام ببذل عناية بصون الأراضي ومراقبتها فعليا لمنع جهات أخرى من استغلالها

61 Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia) ICJ Reports of Judgments, 3 March 2014, para 26.

62 المرجع نفسه، فقرة 55.

63 تقرير فريق الخبراء الحكوميين المعني بالتطورات في مجال المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، مرجع سابق، ص10.

لأغراض غير مشروعة. إنَّ الإشـــارة إلى مســـئولية الدولة على الوفاء بالتزاماتها عن الأفعال غير المشروعة – بما في ذلك اســـتخدام الوكلاء في المجال الســـيبراني – فيه تأكيد على حظر التدخل غير المشروع، والذي أرى أنه لا بد من إدخال التجسس السيبراني كأحد صوره. في المجال السيبراني، يعد الوصول إلى المعلومات والاستيلاء عليها خرق للسلطة الســـيادية للدولة بغض النظر عن وجود ضرر مادي. فالضرر المعنوي يتحقق حينما يُتوصل إلى معلومات غير متاحة للعامة والتي تعد سريتها وخصوصيتها جزء من الحقوق السيادية التامة المانعة للدولة.

خاتمة

تَطرَّق البحثُ لصورتَين للهجمات الإلكترونيّة ما دون اســـتخدام القوة، هُما التجســـس السيبراني، وعمليات التخريب الســـيبرانية، ولا بد من الإشـــارة أولًا إلى أنّ مســـألة الإثبات، ومعرفة الفاعل، وبالتالي الإسناد، لاتزال تُشكِّل صُعوبة عمليّةً في مجال الكشف عن الجُناة للجرائم السيبرانيّة. إنَّ مُستقبل الأمن والسِّلم الدوليين في المجال الســـيبرانيّ، يتوقف على تطوير وســـائل تكنولوجيّة أكثر قُدرةً على كشـــف الفاعل، وعلى حســـم مسائل الإسناد، ومسئولية الدول، بما يخدم المجتمع الدولي كَكُلٍ، كما أن هنالك حاجة لإيجاد آلية تنظيميّة تحكم الأنشطة الإلكترونيّة بحيث تُوفِّر حماية دولية لسيادات الدول، وحقوق الضحايا.

فيما يخص التجســـس السيبرانيّ، هناك إشـــكاليتان، الأولى ذات بعد قانوني تتمثل في عدم تجريم القانون الدولي للتجســـس بشكل عام، والثانية ذات بعد تكنولوجيّ تتمثل في سهولة الاعتماد على الذكاء الاصطناعي في عمليات التجسس السيبراني دون الخوض في مخاطر التجسس التقليدي الذي يعتمد على العنصر البشري ومخاطر كشفه.

في ظِلِّ التَّطوّر التكنولوجي الذي يُعزِّزُ من عمليات التجسُّس السيبرانيّ، وفي ظل انعدام تجريم واضح وصريح للتجســـس على الصعيد الدولي، فإن خيارات الدولة الضحيّة تبدو محدودة في التصعيد السياسي والاستنكار. يرى البحثُ أنَّه من الخطورة اقتصار تكييف الأنشـــطة السيبرانيّة لجمع المعلومات باعتبارها مُجَرَّد تجسس لا تأثير لها على مبدأ الســـيادة وعلى مســـتقبل الأمن والســـلم الدوليين. لذلك، هناك حاجة إلى تطوير قواعد القانون الدولي لكي تتناســـب مع حجم الهجمات الإلكترونيّة التي تبدأ بتجميع المعلومات السرية من أجل التأثير على ســـلوك الدولة عن طريق الضغط عليها سياســـيًا، أو عن طريق شن هجمات تخريب إلكترونية تشل من مقدرة الدولة على ممارسة سيادتها بشكل كامل وحر على إقليمها.

أمَّا بشـــأن هجمات التخريب السيبراني، فإن موقف القانون الدولي أكثر وضوحًا في مَنح الدولة الضحية حقا في تفعيل قنوات الحماية القانونية. فوجود أثر مادي مثل تعطيل الإنترنت، أو المســـاس بالبنية التحتية للأسلاك يُشكّل مَساسًا بســـيادة الممتلكات والبيانات الوطنية، سواء الواقعة على أراضيها، أو خارج إقليمها. وكما بيّن البحث فإن مبدأ السيادة يحمي الســـلامة المادية لأراضي الدولة وممتلكاتها، في حين يحمي مبدأ عدم التدخل السلامة السياسيّة – غير الملموسة – للدولة.

بسبب الطبيعة الافتراضية للفضاء الإلكتروني والعمليات الحاصلة من خلاله، فإنه لا بد من النظر إلى مبدأ عدم التدخل باعتباره بالغ الأهمية في حماية الســـلامة السياسية للدولة، ليس فقط على البيانات والمعلومات التي تملكها،

بــل أيضًا على حقّها في حماية سريّتها، وحقها في الاحتفاظ بخصوصيتها، لأن حماية هذا الحق في الخصوصية يضمن النزاهة السياسيّة للدولة وعدم التأثير على قراراتها.

تظهر إشــكاليّة أخرى حول مدى إمكانية تطبيق مبدأ عدم التدخل على التجســس والتخريب السيبرانيّ؛ إذ لا يُقــدّم القانون الدوليّ تفســيرًا واضحًا لمعنى وأبعاد التدخل المحظور، خاصة الذي يقع أثناء السِّــلم ودون وجود تدخل عســكري، أو دون استخدام للقسر والقوة. في هذا الشأن، يدعو البحث إلى التوسع بشكل معقول في تفسير مبدأ عدم التدخل، ليشمل ليس فقط التخريب السيبراني، بل أيضًا الاطلاع غير المُصرّح به للمعلومات، فالتجسس يكون دون رضا الدولة الضحية، وانعدام الرضا – حتى وإن حدث دون اســتخدام الإكراه، أو القوة – هو خطوة أولى في اتجاه اســتغلال الدولة الضحية، وتقويض ســلطتها وإضعاف مركزها الســياسي، وهذا الاستغلال الذي يحصل، ليس فقط من خلال عمليات التخريب الســيبراني، بل أيضًا من خلال التجسس السيبراني يُعرِّض السُّلطة السياديّة للخطر، مما يجب أن يُفسّر باعتباره شكلًا من أشكال الإكراه غير المشروع.

إن التطور التكنولوجي السريع أدى إلى تســابق الدول في تعزيز معرفتها التكنولوجية والقدرة على استعمالها بما يضعها في مركز القوة. إن تعزيز القوة السياسية والاقتصادية بل والتكنولوجية يمكن استخدامه للنهوض بالدولة وبعلاقاتها مع الدول الأخرى من خلال التعاون، لكنّ المشــكلة تظهر حين تستغل عناصر القوّة من أجل السيطرة والتأثير على ســلوك دولة، أو دول أخرى. لذلك لا بد من توجيه مُمارســات الدول نحو احترام السيادة الإقليميّة للدول الأخرى، وهو أمر لا يتحقق من دون الالتزام بمبدأ عدم التدخل وفق مفهوم معقول يشــمل حماية المجال السيبراني للدول.

المراجع

أولًا: العربية

آل مواش، ضرغام جابر عطوش. **جريمة التجسس المعلوماتي**. المركز العربي للنشر، القاهرة، 2017.

خليفة، إيهاب. **القوة الإلكترونية – كيف يمكن أن تدير الدولة شؤونها في عصر الإنترنت؟** العربي للنشر والتوزيع، القاهرة، 2017.

———. **حروب مواقع التواصل الاجتماعي**. العربي للنشر والتوزيع، القاهرة، 2016.

عبد الصادق، عادل. **الاقتصاد الرقمي وتحديات السيادة السيبرانية**. المركز العربي لأبحاث الفضاء الإلكتروني، القاهرة، 2020.

عبيد، عيسى. **محكمة العدل الدولية ودورها في تطوير قواعد القانون الدولي الجنائي**. دار أمجد، عمان، 2017.

نصار، غادة. **الإرهاب والجريمة الإلكترونية**، العربي للنشر والتوزيع، القاهرة، 2017.

ثانيًا: الأجنبية

References:

ʿAabd alṣadq, ʿadil. *al iqthṣad al raqmī wa taḥadyat al siyāda shm sibrāniya* (in Arabic), alqahīrah: al markaz alʿarabī liabḥāth alfaḍāʾ al -iliktrūnī, 2020.

ʿAabīd, ʿīsā. *Maḥkamat Al ʿadl Al duwaliya wa dawrihā fi taṭwīr qawāʿid al qānwn al duwali aljwnāʾī* (in Arabic), ʿamān dār Amjad, 2017.

Al mawāsh-ḍarghām jābir ʿaṭūsh, *jarīmat altajasus al maʿlūmatī* (in Arabic), alqaaīrah: almarkaz alʿarabī linashr, 2017.

Brierly, J. L., *The Law of Nations: An Introduction to the International Law of Peace*. Oxford: Oxford University Press, 1963.

Brown, Gary and Poellet, Keira, "The Customary International Law of Cyberspace", *Strategic Studies Quarterly*, vol. 6, No. 3, Cyber Special Edition (2012), pp. 126-145.

Buchan, Russell, "The International Legal Regulation of State-Sponsored Cyber Espionage", in Anna-Maria Osula and Henry Rõigas (eds.), *International Cyber Norms: Legal, Policy and Industry Perspectives*. Tallinn: NATO CCD COE, 2016.

Demarest, Geoffrey B, "Espionage in International Law", *Denver Journal of International Law and Policy* 24 (1996).

Hampson, Fen Osler and Jardine, Eric, *Look Who's Watching, Revised Edition: Surveillance, Treachery and Trust Online*. Watrloo: McGill-Queen's Press, 2016.

Johnson, David and Post, David, 'Law and Borders: The Rise of Law in Cyberspace,' *Stanford Law Review* 48 (1996).

Khalīfah, Aīhāb. *Alquwa Al iliktrwniya kayfa yumkinu An tudīra Al dawla shuūnahā fī ʿaṣr Al ʿintarnit* (in Arabic), Al qāhira Alʿarabī linashr wa Al tawzīʿ 2017.

_____. *ḥurūb mawāqiʿ Al tawāṣul al ʿijtimāʿī* (in Arabic), Al qāhira Alʿarabī linashr wa Al tawzīʿ 2016.

Mačák, Kubo, From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers (2017) 30 *Leiden Journal of International Law* 877.

Naṣār, ghādah. *al ʿirhāb wa Al jarīmai Alʿiliktrūniya* (in Arabic), Al qāhira Alʿarabī linashr wa Al tawzīʿ 2017.

Oppenheim, *Lassa and Lauterpacht, Hersch, International Law: A Treatise. vol. I, Peace*, 8th edn. London: Longman, 1955.

Ottis, Rain, “Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective” in Matthew Warren (ed), *Case Studies in Information Warfare and Security for -Researchers*. London: Academic Conferences Limited, 2013.

Perry, Jake, “Viewpoint: Invisible Threats” in Sean S. Costigan and Jake Perry (eds.) *Cyberspaces and Global Affairs*. New York: Routledge, 2016.

Scharre, Paul, *Army of None: Autonomous Weapons and the Future of War*. W. W. Norton & Company, 2018.

Singer, Peter W, Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know.* Oxford: Oxford University Press, 2014.

Stahn, Carsten, “‘Jus ad bellum’, ‘jus in bello’... ‘jus post bellum’? -Rethinking theStahn, Carsten, “‘Jus ad bellum’, ‘jus in bello’... ‘jus post bellum’? -Rethinking the Conception of the Law of Armed Force”, *The European Journal of International of International Law* 17 (2007) 5: 921-943.

Tiirmaa-Klaar, Heli and others, *Botnets*. New York: Springer Science & Business Media, Jun 29, 2013.

Ţuţuianu, Simona, *Towards Global Justice: Sovereignty in an Interdependent World*. The Hague: Springer Science & Business Media, 2012.

Watts, Sean, ‘Low-Intensity Cyber Operations and the Principle of Non-Intervention’, *Baltic Yearbook of International Law* 14 (2014(.

Wright, Quincy, ‘Espionage and the Doctrine of Non-Intervention in Internal Affairs’, in *Essays on Espionage and International Law*, ed. Richard Falk, Ohio: Ohio State University Press, 1962.

Wu, Timothy S, “Cyberspace Sovereignty? The Internet and the International System”, *Harvard Journal of Law & Technology*, vol. 10, no. 3, 1997.

Online Sources:

Borger, Julian. ‘Brazilian President: US Surveillance a ‘Breach of International Law’, *The Guardian*, September 24, 2013. <http://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance>.

“Germany detects new cyberattack targeting politicians, military”, Deutsche Welle (30 June 2018). <https://www.dw.com/en/germany-detects-new-cyberattack-targeting-politicians-military/a-46515590>.

McGuinness, Damien, “How a cyber attack transformed Estonia”, 27 April 2017, BBC News. <https://www.bbc.com/news/39655415>.

US Department of State, “Statement on Consensus Achieved by the UN Group of Governmental Experts on Cyber Issues” (7 June 2013) <https://2009-2017.state.gov/r/pa/prs/ps/2013/06/210418.htm>.