

"مشروعية الهجمات السيبرانية التي لا ترتقي إلى مستوى القوة المحظرة" "The Legality of Cyber Operations Falling Below the Threshold of the Prohibited Use of Force"

إعداد الباحثة:

د. ماريا جان التولاني

Received: 12/07/2026 | Revised: 13/07/2026 | Accepted: 21/08/2026 | Published: 02/08/2026

non-intervention remains capable of adapting to the transformations brought about by the digital age.

Keywords: Cyber operations; Principle of non-intervention; Coercion; Sovereignty; Domaine réservé; Public international law.

ملخص البحث

فرض التطور المتسارع للفضاء السيبراني تحديات غير مسبوقة أمام قواعد القانون الدولي العام، لاسيما في ظل تزايد الهجمات الإلكترونية التي تستهدف الدول دون أن ترتقي إلى مستوى استخدام القوة المحظورة بموجب ميثاق الأمم المتحدة. وقد أدى هذا الواقع إلى بروز إشكالية قانونية أساسية تتمثل في التساؤل حول مدى خضوع هذه الهجمات لمبدأ عدم التدخل في الشؤون الداخلية والخارجية للدول، باعتباره أحد المبادئ الجوهرية التي يقوم عليها النظام القانوني الدولي المعاصر.

وتكتسب هذه الإشكالية أهمية خاصة بالنظر إلى أن غالبية العمليات السيبرانية التي تشهدها العلاقات الدولية لا تؤدي إلى أضرار مادية مباشرة أو إلى نتائج تماثل آثار الهجمات المسلحة، على الرغم من قدرتها على التأثير في عمل المؤسسات العامة أو ممارسة الضغوط على الدول أو المساس بحرية اتخاذها لقراراتها السيادية. الأمر الذي يطرح تساؤلات حول مدى كفاية القواعد الدولية التقليدية لمواجهة هذه الأنماط المستحدثة من التهديدات.

وتزداد صعوبة معالجة هذه المسألة بسبب جملة من العقبات القانونية والتقنية وعلى رأسها غياب تعريف دولي موحد لمفهوم التدخل السيبراني غير المشروع وعدم الاتفاق على المقصود

Abstract:

The rapid expansion of cyberspace has posed unprecedented challenges to the established rules of public international law, particularly in light of the increasing prevalence of cyber operations targeting states without reaching the threshold of the prohibited use of force under the United Nations Charter. This reality has given rise to a fundamental legal question concerning the extent to which such operations are subject to the principle of non-intervention in the internal and external affairs of states, a principle that constitutes one of the cornerstones of the contemporary international legal order.

The significance of this issue stems from the fact that most cyber operations occurring in contemporary international relations do not produce direct physical damage or consequences comparable to those resulting from armed attacks, despite their potential to disrupt the functioning of public institutions, exert pressure on states, and undermine their freedom to make sovereign decisions independently. This raises important questions regarding the adequacy of traditional rules of international law in addressing these emerging forms of threats.

The examination of this issue is further complicated by a number of legal and technical obstacles, most notably the absence of a universally accepted definition of unlawful cyber intervention, the lack of consensus regarding the meaning of coercion in the digital environment, and the absence of precise criteria for determining the scope of matters falling within the domaine réservé of states. Additional challenges arise from the difficulties associated with attributing cyber operations to a particular state, given the technical complexity of cyberspace, as well as the divergent views of states concerning the applicability of existing rules of international law to cyber activities.

Against this backdrop, addressing this issue through the lens of international legal instruments, judicial decisions, and contemporary scholarly approaches has become essential in assessing the extent to which the principle of

ومن هنا، تبرز الحاجة إلى دراسة هذه الإشكالية في ضوء النصوص الدولية والاجتهادات القضائية والاتجاهات الفقهية الحديثة، بهدف تقييم مدى قدرة مبدأ عدم التدخل على مواكبة التحولات التي فرضتها الثورة الرقمية على طبيعة العلاقات الدولية.

الكلمات المفتاحية: الهجمات السيبرانية، مبدأ عدم التدخل، الإكراه، السيادة، المجال المحفوظ للدولة، القانون الدولي العام.

بعنصر الإكراه في البيئة الرقمية، فضلاً عن عدم وجود معايير دقيقة لتحديد نطاق الشؤون التي تدخل ضمن المجال المحفوظ للدول. كما تبرز إشكالية إسناد الهجمات الإلكترونية إلى دولة معينة في ظل الطبيعة التقنية المعقدة للفضاء السيبراني، إلى جانب تباين مواقف الدول بشأن مدى انطباق قواعد القانون الدولي على الأنشطة السيبرانية.

How to Cite This Article

التولاني، م. ج. (2026). مشروعية الهجمات السيبرانية التي لا ترتق إلى مستوى القوة المُخْطَرَة. *المجلة العربية للنشر العلمي (AJSP)*، 9(94)، (393-407).



المقدمة:

تشكل الهجمات السيبرانية التي شنتها ولا تزال تشنها كل من إيران وإسرائيل في نزاعها الحالي صراعاً موازياً للنزاع التقليدي، حيث تبذل كل من الدولتين جهودها لشن ما أمكن من الهجمات التخريبية ضد البنى التحتية كتلك التي استهدفت محطات الوقود والموانئ والمنشآت النووية. إذ بالرغم من الأضرار الضخمة التي يمكن أن تسببها هذه الهجمات، إلا أنها وبسبب طبيعتها يتمكّن مرتكبها من التصل من المسؤولية المباشرة أمام المجتمع الدولي.

وقد أدّى غياب الاتفاق حول كيفية تطبيق القانون الدولي على الأنشطة السيبرانية للدول إلى وجود حالة من الضياع أو الغموض القانوني، خصوصاً وإن بعض الدول لا تزال تفضّل هذا الوضع لقناعتها بأن أي تنظيم متفق عليه للعمليات السيبرانية قد لا يخدم مصالحها. في حين تفضل دول أخرى وجود أساس قانوني واضح سواء لتنفيذ العمليات السيبرانية أو لتحديد ما إذا كانت دولة أخرى انتهكت القانون الدولي. فالدول التي تتعرض لهجمات سيبرانية تحتاج إلى تحديد القواعد القانونية التي تم خرقها لتتمكن من تحديد الإجراءات المشروعة التي يحق لها اتخاذها ردّاً على ذلك. وبالمثل، فإن الدول التي تفكر في تنفيذ عمليات سيبرانية أو تقوم بها تحتاج إلى فهم حدود القانون لضمان عدم خرقها له.

وبالرغم من أن تحديد العتبة التي يُعدّ عندها الفعل السيبراني استخداماً للقوة لا يزال محل جدل، إلا أنه يبدو أن أغلب الفقهاء والباحثين باتوا يؤكدون على أنّ الهجمات التي تُسبّب إصابة أو وفاة أشخاص أو إلحاق ضرر أو تدمير بالأعيان ترتقي إلى مستوى استخدام القوة أو الهجوم المسلح بموجب ميثاق الأمم المتحدة. لكن في الواقع، أن أغلبية العمليات السيبرانية التي تقوم بها الدول عادة تقع دون عتبة استخدام القوة، إذ تتخذ شكل تدخلات مستمرة منخفضة المستوى تُلحق ضرراً بالدولة المستهدفة وغالباً دون آثار مادية ملموسة. فعلى سبيل المثال، أكّدت الصين أنها كانت هدفاً لهجمات كبدتها في العام 2017 خسائر اقتصادية قاربت 60 مليار دولار نتيجة حوادث

الأمن السيبراني، وأن 93.5% من هجمات الفدية فيها جاءت من خارج البلاد¹. وفي تشرين الأول من العام 2019، كشف المركز الوطني للأمن السيبراني في المملكة المتحدة أن البلاد تعرّضت لما يقارب 1800 هجوم سيبراني خلال السنوات الثلاث السابقة². كل ذلك وإن دلّ على شيء فهو يدل على أنه لا يمكن إهمال هذا النوع من الهجمات أو إهمال مدى تأثيرها على الدول.

من هنا كان من الضروري التساؤل حول ما إذا كان من شأن الهجمات السيبرانية التي لا تصل إلى مستوى استخدام القوة أن تُشكّل، كما حال بعض التصرفات التقليدية، انتهاكاً لمبدأ حظر التدخل في الشؤون الداخلية أو الخارجية للدول المستهدفة.

ولمعالجة هذه الإشكالية، لا بد من الإجابة على عدد من الأسئلة الفرعية وأبرزها:

-ما مدى خضوع الهجمات السيبرانية غير التقليدية لمبدأ عدم التدخل المكرس منذ العام 1945 في ميثاق الأمم المتحدة؟

-متى تخرق الهجمات السيبرانية عتبة التدخل المشروع وتحوّل إلى انتهاك لقواعد القانون الدولي؟

-إلى أي مدى يمكن التحقق من توفر عنصر الإكراه في الهجمات السيبرانية؟

-هل من سوابق دولية تبنّت تدخلاً سيبرانياً غير مشروعاً؟

-هل يُشكّل التجسّس الإلكتروني أو الرقمي تدخلاً غير مشروعاً في شؤون الدول؟

تكمن أهمية هذا البحث في كونه استجابةً للتحوّلات الجوهرية التي أحدثها الفضاء السيبراني في طبيعة العلاقات الدولية والتي كانت إلى حد قريب خاضعة لقواعد قانونية تم الاتفاق عليها في العام 1945 أي قبل ظهور تكنولوجيا المعلومات بعقودٍ طويلة. إذ باتت الهجمات السيبرانية الدولية تُهدّد كل الدول من دون استثناء ممّا يضع سيادة الدول وحقوقها في منع التدخل في شؤونها المكرّس في ميثاق الأمم المتحدة في خطرٍ مُحدّق. من هنا كان لا بُدّ من دراسة الهجمات السيبرانية في ضوء مبدأ عدم التدخل الذي يُشكّل حجر الأساس للسيادة الوطنية.

على ضوء كل ذلك، تبرز أهمية دراسة مدى انطباق حظر التدخل على الهجمات السيبرانية (المطلب الأول) والتدخل السيبراني غير المشروع في المجال الحفوظ للدولة (المطلب الثاني).

المطلب الأول: مدى انطباق حظر التدخل على الهجمات السيبرانية

إذا كانت الكثير من التصرفات السيبرانية محدودة التأثير ولا تشكل استخداماً للقوة، إلا أنّ العديد منها تتخطى، في حالات معينة، حدود حظر التدخل وتحوّل إلى عملٍ غير مشروعٍ يُرتّب مسؤولية دولية ويُعطي الدول المُستهدفة الحقّ بالرد. لذلك ومن أجل معرفة مدى

¹ Ministry of Foreign Affairs of the People's Republic of China (2019), 'The Daily Telegraph Publishes a Signed Article by Ambassador Liu Xiaoming Entitled Dialogue and co-operation are the only way to cyber security', available at: https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zwjg_665342/zwbdtxt_665378/t1631237.shtml, accessed: 23/11/2025, 11:00 am.

² National Cyber Security Centre, 2019, Annual Review 2019, available at: <https://www.ncsc.gov.uk/news/annual-review-2019>, accessed: 23/11/2025, 11:30 am.

خضوع الهجمات الإلكترونية لمبدأ حظر التدخل في الشؤون الداخلية للدول، لا بُد من دراسة خضوع الهجمات السيبرانية لمبدأ عدم التدخل (الفرع الأول) والإكراه كعنصر أساسي من عناصر التدخل السيبراني (الفرع الثاني).

الفرع الأول: خضوع الهجمات السيبرانية لمبدأ عدم التدخل

يميل العديد من الفقهاء إلى تجريد مبدأ عدم التدخل من صفته القانونية الدولية الملزمة ويعتبرونه مبدأ عامًا. من هنا، لا بُد بدايةً من دراسة الأساس القانوني لمبدأ عدم التدخل (أولاً) للتمكّن من تحديد التدخل السيبراني غير المشروع (ثانياً).

أولاً: الأساس القانوني لمبدأ عدم التدخل

تمّ تكريس مبدأ عدم التدخل والإشارة إلى أهميته في العديد من النصوص الدولية، لاسيما في المادة الثانية من ميثاق الأمم المتحدة، التي نصّت في فقرتها السابعة على أنّه "ليس في هذا الميثاق ما يسوغ" للأمم المتحدة "أن تتدخل في الشؤون التي تكون من صميم السلطان الداخلي لدولة ما..."³، كما تمّت الإشارة إليه، بصورة ضمنية، في الفقرة الأولى من المادة عينها التي أكدت على أنّ هيئة الأمم المتحدة تقوم على مبدأ المساواة في السيادة بين جميع الدول الأعضاء في المنظمة⁴. فالمساواة لا يُمكن أن تتحقّق إلّا اذا تمّت حماية الدول ذات السيادة من التدخلات. أمّا الفقرة الرابعة من المادة الثانية فحظرت التدخل الذي يأخذ شكل استخدام القوة أو التهديد باستخدامها⁵.

كما أصدرت الجمعية العامة للأمم المتحدة جملة من القرارات حثّت بموجبها على عدم جواز التدخل في الشؤون الداخلية للدول⁶. كذلك احتلّ هذا المبدأ مكانةً مهمّةً على الصعيد الإقليمي، إذ كرّسته المادة الثامنة من ميثاق جامعة الدول العربية⁷ والمادة الثالثة من القانون التأسيسي للاتحاد الإفريقي⁸.

ولم تكن أحكام وقرارات محكمة العدل الدولية بعيدة عن هذا المنطق. فقد رفضت هذه الأخيرة في قضية مضيق كورفو التدخل في شؤون الدول⁹. ولكل من يرفض اعتبار مبدأ عدم جواز التدخل مبدأً قانونياً مُستقلاً عن باقي المبادئ الدولية، جاء رد المحكمة الدولية قاطعاً

³ ميثاق الأمم المتحدة، المادة 2، الفقرة 7، متاح على: <https://www.un.org/ar/about-us/un-charter/full-text>، تاريخ وساعة الزيارة: 2026/3/23، 11:00 ق.ظ.

⁴ المرجع السابق، المادة 2، الفقرة 1؛ للمزيد راجع: مسعد زيدان، تدخل الأمم المتحدة في النزاعات المسلحة غير ذات الطابع الدولي، دار الكتب القانونية، مصر، 2008، ص. 184.

⁵ ميثاق الأمم المتحدة، المادة 2، الفقرة 4، مرجع سابق.

⁶ الجمعية العامة، إعلان عدم جواز التدخل في الشؤون الداخلية للدول وحماية استقلالها وسيادتها، قرار رقم 2131، تاريخ 1965/12/21، متاح على: https://legal.un.org/avl/pdf/ha/ga_2131-xx/ga_2131-xx_a.pdf، تاريخ وساعة الزيارة: 2021/12/26، 09:15 ق.ظ؛ الجمعية العامة، إعلان مبادئ القانون الدولي المتعلقة بالعلاقات الودية والتعاون بين الدول وفقاً لميثاق الأمم المتحدة، قرار رقم 2625، تاريخ 1970/10/24، مرجع سابق؛ الجمعية العامة، إعلان بشأن عدم جواز التدخل بجميع أنواعه في الشؤون الداخلية للدول، التوصية رقم 36/103، تاريخ 1981/12/09، متاح على: <https://undocs.org/ar/A/RES/36/103>، تاريخ وساعة الدخول: 2021/10/14، 10:00 ق.ظ.

⁷ ميثاق جامعة الدول العربية، المادة 8، متاح على <http://www.lasportal.org/ar/aboutlas/Pages/Charter.aspx>، تاريخ وساعة الزيارة: 2021/10/21، 15:00 ب.ظ؛ للمزيد راجع: محمد الأنباري، مبدأ عدم التدخل واستثناءاته في القانون الدولي المعاصر، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2016، ص. 91.

⁸ القانون التأسيسي للاتحاد الإفريقي، 2000، متاح على: https://au.int/sites/default/files/pages/34873-file-constitutive_act_ar.pdf، تاريخ وساعة الزيارة: 2021/08/09، 10:30 ق.ظ.

⁹ وفقاً لمحكمة العدل الدولية، إنّ حق التدخل المزعوم تجسيده لسياسة القوة، سياسة غطت في الماضي أخطر التجاوزات، ولا يمكن أن تجد لها مكاناً في القانون الدولي...، "محكمة العدل الدولية، قضية قناة كورفو، تاريخ 1949/12/15، ص. 11، متاح على: <https://www.icj-cij.org/node/103096>، تاريخ وساعة الزيارة: 2026/2/2، 10:30 ق.ظ.

في هذا السياق. إذ بعد أن أشارت إلى أنه يُحظر على كل الدول التدخل، سواء بصورة مباشرة أو غير مباشرة، في الشؤون الداخلية والخارجية للدول الأخرى، وبعد أن أكدت على أن استخدام القوة يُعتبر مثالاً واضحاً على التدخل غير القانوني، اعتبرت أنه يجب الأخذ بالقاعدتين الدوليتين جنباً إلى جنب، ذلك أن التدخل لا يزال مفهوماً متميزاً¹⁰، وعلى حد تعبير القاضي جينينغز "لا يمكن أن يكون هناك شك في أن مبدأ عدم التدخل هو مبدأ مستقل من مبادئ القانون الدولي العرفي الأخرى"¹¹، رغم ارتباطه الوثيق بمبدأي حظر استخدام القوة ومبدأ السيادة. وأعادت محكمة العدل الدولية التأكيد على المكانة المستقلة لمبدأ عدم التدخل في العام 2005، عندما قرّرت أن أوغندا خرقت الواجبات القانونية المترتبة عليها، بموجب مبدأ عدم استخدام القوة ومبدأ عدم التدخل¹². أما تمسك الدول بمبدأ حظر التدخل في شؤونها فهو أمر واضح، ولا يترك أي مجال للشك حول مكانة هذه القاعدة القانونية وتميزها عن باقي القواعد القانونية الأخرى¹³.

ثانياً: التدخل السيبراني غير المشروع

إذا كان الأساس القانوني لمبدأ عدم التدخل لا لبس فيه، إلا أن تعريف وتحديد التصرفات التي تُشكّل تدخلاً ليس بالأمر اليسير. وقد أدى الغموض الذي يشوب مضمون هذا المبدأ، إلى فتح المجال أمام التشكيك بإمكانية خضوع الهجمات السيبرانية له. فقد تمّ اعتبار أن هذا المبدأ ينطبق فقط على العمليات التقليدية الملموسة. إذ اعتبر البعض أنه من الصعب تصنيف التدخل الذي يحصل بطريقة غير ملموسة (مثل الإشعاع) بأنه يُشكل انتهاكاً لسيادة الدول وتدخلًا غير مشروعاً¹⁴. فالفضاء الإلكتروني مجال إفتراضي، لا يمكن لأي دولة أن تُسيطر عليه أو أن تمارس صلاحياتها الإقليمية عليه. ويُؤكّد على هذه الفرضية معهد القانون الدولي الانساني الذي اعتبر أن البُنية المُميّزة للفضاء السيبراني تكمن في كونه بيئة افتراضية تخرج عن نطاق اختصاص أي دولة بمفردها¹⁵. لذلك لا يمكن اعتبار أن العمليات التي تشنّ في هذا العالم الافتراضي تدخلاً غير مشروعاً.

ولكن الحُجج المُقدّمة لم تكن كافية لإخراج العمليات السيبرانية من نطاق تطبيق مبدأ عدم التدخل. فالسيادة لا تشمل فقط الإقليم المادي للدولة وإنما هي مفهوم أوسع، وتمتد لتشمل كل شأن يحصل على الإقليم المادي وخارجه إذا ارتبط به. فهي تعني حق الدول في تنظيم شؤونها الداخلية والخارجية دون أي تدخل. مما يدلّ على أن مبدأ عدم التدخل تم تكريسه، ليس فقط لحماية إقليم الدول، وإنما لحماية حق هذه الدول في ممارسة سلطاتها وتنظيم شؤونها داخل هذا الإقليم وخارجه. والتدخل المحظور، بحسب محكمة العدل الدولية، هو التدخل الذي يتعلق بأمر يُسمح فيها لكل دولة عملاً بمبدأ السيادة أن تتخذ قراراتها بحرية "كاختيار النظام السياسي والاقتصادي

¹⁰ محكمة العدل الدولية، القضية المتعلقة بالأنشطة العسكرية وشبه العسكرية في نيكاراغوا وضدّها، (نيكاراغوا ضد الولايات المتحدة الأميركية)، ص. 171، متاح على: <https://www.icj-cjj.org/case/70>، تاريخ وساعة الزيارة: 2026/2/2، 10:00 ق.ظ.

¹¹ Russell Buchan, "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?", Journal of Conflict & Security Law, Oxford University Press, vol. 17, no. 2, 2012, p. 221.

¹² محكمة العدل الدولية، الأنشطة المسلحة في أراضي الكونغو (جمهورية الكونغو الديمقراطية ضد أوغندا)، تاريخ 2005/12/19، الجمعية العامة، تقرير محكمة العدل الدولية 1 آب 2005 - 31 تموز 2006، A/61/4، ص. 33.

¹³ Sean Watts, "Low-intensity Cyber Operations and the Principle of Non-intervention", Baltic yearbook of International Law, vol. 14, 2015, p. 140.

¹⁴ Sean Kanuck, "Recent Development: Information Warfare: New Challenges for Public International Law", Harvard International Law Journal, vol. 37, 1996, p. 288.

¹⁵ International Humanitarian Law Institute, Rules of Engagement Handbook, September 2009, p.15, in Russell Buchan, "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?", Journal of Conflict & Security Law, Oxford University Press, volume 17, number 2, 2012, p. 222.

والإجتماعي والثقافي وصياغة سياستها الخارجية¹⁶. ويكون التدخل غير مشروع، عندما يتم استخدام طرق الإكراه لإلزام الدول على القيام بتصرف خارج ارادتها حول شأن من شؤونها¹⁷. إذا لنكون أمام تدخل غير مشروع، لا بُدَّ من توافر عدة عناصر وهي: حصول التدخل من قبل دولة ضد دولة أخرى، أن يكون الهدف منه إكراه الدولة على القيام بتصرفات خارج ارادتها في شأن من شؤونها الداخلية أو الخارجية التي لها الحرية في التصرف فيها. وهذا التدخل يُمكن أن يكون مباشراً أو غير مباشر¹⁸.

على ضوء ذلك، يمكن تعريف التدخل غير المشروع، بأنه تعرّض دولة لشؤون دولة أخرى، بهدف إلزام الدولة المُتدخل في أمر من أمورها باتباع ما تُمليه عليها في شأن من شؤونها الخاصة¹⁹. ممّا يعني أنه لنكون أمام هجوم سيبراني مُخالف لحظر التدخل، لا بُدَّ من حصول تصرف سيبراني قسري يهدف إلى إكراه الدولة المُستهدفة، من أجل منعها من القيام بمهامها وصلاحياتها وأو منعها من ممارسة الأنشطة أو اتخاذ الخيارات التي يحق لها اتخاذها أو القيام بها بموجب القانون الدولي، أي التدخل في كل ما هو ضمن اختصاصها الداخلي.

إذا إنّ الوسيلة المُستخدمة لا تُشكل بحد ذاتها أساساً لتحديد ما إذا كان التصرف يُشكّل تدخلاً غير مشروعاً. فسواء حصل بالطرق التقليدية أو غير التقليدية كالهجوم السيبراني، يبقى الأساس لتصنيف أي عمل دولي على أنه تدخل غير مشروع، توافر الشروط الأساسية المذكورة أعلاه بغض النظر عن الوسيلة المُستخدمة لتحقيق الغاية. وقد أكّد خبراء دليل تالين على أنه لا يجب على الدول التدخل في الشؤون الداخلية والخارجية للدول الأخرى لاسيما بواسطة الوسائل الرقمية²⁰، واكدوا على عُنصرين من عناصر التدخل غير المشروع، الإكراه والشؤون الداخلية والخارجية. أما فريق الخبراء الحكوميين فاعتبر أنّ الهجمات السيبرانية التي لا ترقى إلى مستوى استخدام القوة تخضع لمبدأ حظر التدخل في الشؤون الداخلية للدول²¹، ويبدو أنّ الدول تتجه إلى الأخذ بوجود التقيد بمبدأ عدم التدخل عند شن الهجمات السيبرانية.

¹⁶ محكمة العدل الدولية، القضية المتعلقة بالأنشطة العسكرية وشبه العسكرية في نيكاراغوا وضدّها، (نيكاراغوا ضد الولايات المتحدة الأمريكية)، مرجع سابق، ص. 220.

¹⁷ Hugh Handeyside, "The Lotus Principle in ICJ Jurisprudence: Was the Ship Ever Afloat?", Michigan Journal of International Law, The University of Michigan, USA, vol. 29, no. 1, 2007, p. 77.

¹⁸ للمزيد راجع: Gaetano Arangio-Ruiz, Human Rights and Non-intervention in the Helsinki Final Act, Sijthoff & Noordhoff, 1977, p. 257.

¹⁹ Terry Gill, "Non-Intervention in the Cyber Context", in Katharina Ziolkowski (ed.), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy, NATO Cooperative Cyber Defence Centre of Excellence Publication, Estonia, 2013, p. 218.

²⁰ دليل تالين، القاعدة 66، للمزيد راجع: محمد عسكر، 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 2013-2017"، مجلة البحوث القانونية والاقتصادية، جامعة بنى سويف، مصر، المجلد 33، العدد 1، 2021، ص. 385.

²¹ الجمعية العامة، فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، تاريخ 2013/06/24، الفقرة 20، UN Doc A/68/98؛ الجمعية العامة، فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، تاريخ 2015/07/22، الفقرة 26، UN Doc A/70/174.

الفرع الثاني: الإكراه كعنصر أساسي من عناصر التدخل السيبراني

من أجل أن تُشكّل الهجمات الإلكترونية تدخلاً غير مشروعاً، لا بُدَّ من توافُّر عنصر الإكراه. من هنا، يجب إلقاء الضوء على الإكراه في القانون الدولي العام (أولاً) ودراسة تحقُّق هذا العنصر بمعزل عن آثار الهجوم (ثانياً).

أولاً: الإكراه في القانون الدولي العام

يُمثِّل الإكراه العنصر الجوهري للتدخل غير المشروع، كما يُشكّل العنصر الأساس الذي يسمح بالتمييز بينه وبين التصرفات التي تشكل خرق للسيادة²² وبينه وبين التصرفات غير الودية والتدخلات أو الضغوطات التي لا ترقى إلى مستوى التدخل غير المشروع. إلّا أن هذا التمييز ليس بالمهمة السهلة، ذلك أنّه لا يوجد تعريف دولي للمقصود بالإكراه²³، حتّى أنّ محكمة العدل الدولية التي تؤكد على أهمية هذا العنصر لم تعرّفه.

في الواقع، يقوم الإكراه على ممارسة الضغط تجاه الدولة المستهدفة. وهذا الضغط، بالنسبة للبعض، لا يُمكن أن يحصل إلّا إذا اتّخذ شكل القوة²⁴. ممّا دفع بالعديد من الفقهاء إلى اعتبار أن أي إكراه لا ينضوي على القوة لا يؤدي إلى تدخل غير مشروع، وبالتالي لا يمكن أن يُشكّل الضَّغط ذات الطابع الإلكتروني إكراهاً²⁵.

إلّا أنّ هذا الاستنتاج لا يمكن الأخذ به وذلك لأسباب متعدّدة: أولاً، من غير المُبرَّر استبعاد الضَّغوطات التي لا تنضوي على استخدام القوة من نطاق الضغوطات غير المشروعة، فذلك يؤدي إلى تجاهل القوة الحقيقية للضغوطات الإقتصادية والسيبرانية وغيرها ومقدار الضغط الذي يُمكن أن تسببه للدولة المستهدفة²⁶. ثانياً، بيّنت الممارسات الدولية أنّ الدول باتت تلجأ، بصورة خاصة، لوسائل الضغط الإقتصادية ولم تتوان مؤخراً عن استخدام الوسائل التكنولوجية للتدخل في شؤون الدول²⁷. ثالثاً، إن استبعاد كافة الضغوط غير العسكرية من نطاق الضغوطات الغير مشروعة يتعارض مع النصوص والتصرفات الدولية وحتى مع القوانين الوطنية. فالمادة 41 من ميثاق الأمم المتحدة اعتبرت أن "وقف الصلات الاقتصادية والمواصلات الحديدية والبحرية والجوية والبريدية والبرقية واللاسلكية وغيرها من وسائل

²² محمد عسكر، 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 2013-2017"، مرجع سابق، ص. 349.

²³ Antonios Tzanakopoulos, "The Right to be Free from Economic Coercion", Cambridge Journal of International and Comparative Law, vol. 4, 2015, p. 619; Todd Sechser, "A Bargaining Theory of Coercion", in Kelly Greenhill & Peter Krause (eds.), Coercion: The Power to Hurt in International Politics, Oxford University Press, UK, 2018, p. 56.

²⁴ Mitchell Berman, "The Normative Functions of Coercion Claims", Legal Theory, vol. 8, no. 1, 2002, p. 50-51.

²⁵ للمزيد راجع: Ido Kilovaty, "Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information", Harvard National Security Journal, vol. 9, Spring 2018, p. 168.

²⁶ للمزيد راجع: Alexandre George, Forceful Persuasion: Coercive Diplomacy as an Alternative to War, United States Institute of Peace Press, USA, 1992, p. 58.

²⁷ للمزيد راجع: Nozick McCloskey, Coercion: Its Nature and Significance, Southern Journal of Philosophy, Wiley-Blackwell, USA, vol. 18, no. 3, 1980, p. 341.

المواصلات وفقاً جزئياً أو كلياً وقطع العلاقات الدبلوماسية" من التدابير التي يُمكن لمجلس الأمن اللجوء إليها لممارسة الضغط على الدولة المعنية، وبالتالي لم يتم حصر وسائل الإكراه بالتدابير العسكرية فقط²⁸. وأكد عدد من الإعلانات والقرارات الصادرة عن الجمعية العامة على المفهوم الواسع للإكراه²⁹. فقد تحدّث "إعلان عدم جواز التدخل بجميع أنواعه في الشؤون الداخلية للدول" رقم 103/36 الصادر عام 1981، مُفضّلاً عن العديد من أشكال الإكراه الغير عسكرية التي تُشكّل تدخلاً غير مشروعاً كالحصار الاقتصادي والإكراه السياسي والحملات الدعائية التشهيرية³⁰. كما يمكن استخلاص النتيجة عينها من خلال مراجعة حكم محكمة العدل الدولية في قضية نيكاراغوا والولايات المتحدة، حين اعتبرت أن الإكراه يمكن أن يأخذ أشكال متعددة غير القوة العسكرية كتمويل التمرد، وإنما يكون أكثر وضوحاً في هذا النوع من العمليات³¹.

على ضوء ما تقدّم، يُمكن القول أنّ الإكراه عبارة عن كل عمل يستهدف إخضاع إرادة دولة أخرى من طرف دولة ما لحمل الأولى على التصرف بطريقة معينة ضد إرادتها لحساب الثانية، وفي مجال تتمتع فيه الأولى بمقتضى أحكام القانون الدولي بحرية التصرف³²، وبالتالي حتى لو كان هذا العمل ذات طابع سيبراني، فسيكون دون أدنى شك إكراه³³. إنّ مفهوم الإكراه واسع ويشمل التدخلات السيبرانية وغيرها سواء المباشرة وغير المباشرة. كما أنّ خبراء دليل تالين أكدوا على أن الإكراه بواسطة الوسائل السيبرانية يمكن أن يُشكّل تدخلاً غير مشروعاً³⁴. كذلك لم تتوان القوانين الوطنية عن اعتبار أنّ العديد من أشكال الضغوطات غير العسكرية أعمالاً غير مشروعة³⁵.

ولكن يبقى التساؤل حول ما اذا كان يُشترط أن يُحقّق الإكراه، الممارس بواسطة الهجمات السيبرانية، الغاية المنشودة منه، حتى يمكن القول بوجود تدخل سيبراني غير مشروع.

²⁸ صحيح أنّ هذه التدابير أو الوسائل الإكراهية حكر على مجلس الأمن الدولي دون غيره وفقاً لميثاق الأمم المتحدة، إلّا أنّها تعطي دليلاً على المقصود بالإكراه، للمزيد راجع: Eric David, "Portée et limite du principe de non-intervention", *Revue Belge de Droit International*, Bruylant, Belgique, vol. 23, 1990, p. 354.

²⁹ للمزيد راجع: الجمعية العامة، إعلان مبادئ القانون الدولي المتعلقة بالعلاقات الودية والتعاون بين الدول وفقاً لميثاق الأمم المتحدة، مرجع سابق، الديباجة، الفقرة 9؛ الجمعية العامة، إعلان عدم جواز التدخل في الشؤون الداخلية للدول وحماية استقلالها وسيادتها، قرار رقم 31/21، تاريخ 1965/12/21، مرجع سابق.

³⁰ الجمعية العامة، إعلان عدم جواز التدخل بجميع أنواعه في الشؤون الداخلية للدول، مرجع سابق، الفقرة ل، و، ي.
³¹ محكمة العدل الدولية، القضية المتعلقة بالأنشطة العسكرية وشبه العسكرية في نيكاراغوا وضدّها (نيكاراغوا ضد الولايات المتحدة الأمريكية)، مرجع سابق، ص. 212

³² للمزيد راجع: Sean Watts, "Low-Intensity Cyber Operations and the Principle of Non-Intervention", in Jean David Ohlin, Kevin Govern & al., *Cyber War: Law and Ethics for Virtual Conflicts*, Oxford University Press, UK, 2015, p. 256.

³³ كما لو قامت دولة أجنبية بتقديم الدعم المادي أو التقني لمجموعة من المتمردين لشن هجوم إلكتروني، يهدف إلى تشويه معلومات تتعلّق بالسلطات الحاكمة.

³⁴ Francois Dellerue, *Analyse du Manuel de Tallinn 2.0 sur le droit international applicable aux cyber-opérations*, Étude prospective et stratégique (EPS), 2017, p.58.

³⁵ للمزيد راجع: Kathleen Sullivan, "Unconstitutional Conditions", *Harvard Law Review*, Harvard Law School, vol. 102, 1989, p. 1443.

ثانيًا: تحقّق الإكراه بمغزل عن آثار الهجوم

بحسب عدد من الفقهاء، لا يكفي فعل الإكراه لوحده لنكون أمام تدخل غير مشروع، بل لا بُدَّ من الأخذ بعين الاعتبار مدى تأثيره على الطرف المستهدف وليس الوسيلة المستخدمة أو نوع الفعل³⁶. إذ لا قيمة للإكراه السيبراني الذي لا يُنتج آثار فعلية على الطرف المعني.

في الواقع، إنّ اعتماد معيار الآثار المترتبة على الإكراه حصراً، لنفي أو لتأكيد مشروعية الفعل المرتكب يُؤدّي أولاً إلى إضفاء المشروعية على مجموعة من التصرفات المستخدمة للضغط على الدولة المستهدفة، رغم أنّها مخالفة للقواعد القانونية الدولية. فلو افترضنا أنّ الهجوم الإلكتروني على استونيا لم يُؤدّل أي آثار اقتصادية ومالية ولم ترسخ له السلطات، ألا يكفي الإكراه الذي تمت ممارسته بواسطة هذه الهجمات لاعتباره تدخلاً غير مشروعاً. ثانياً، يُؤدّي الأخذ بمعيار الآثار إلى اعتبار الفعل عينه مشروعاً في حالاتٍ مُعيّنة وغير مشروعاً في حالاتٍ أخرى. ويُشكّل التدخل الروسي المُفترض، في كلتا الانتخابات الأميركية والفرنسية، مثلاً واضحاً على ذلك. فقد تم اعتبار أنّ التدخل السيبراني الروسي في العام 2016 في الانتخابات الرئاسية الأميركية ساهم في فوز دونالد ترامب³⁷، في حين أنّ نفس طريقة الإكراه قد فشلت في تحقيق الفوز للمرشحة للانتخابات الرئاسية الفرنسية ماريان لو بان في العام 2017. فالأخذ بمعيار آثار الإكراه يُؤدّي إلى اعتبار أنّ التصرف الروسي في الحالة الأميركية تدخل غير مشروع وفي الحالة الفرنسية تصرف مشروع، كون التأثير على نتيجة الانتخابات لم يتحقّق. وما يدعم هذا الرأي، الإجراءات التي اتخذتها الدولة الأميركية كرد على الهجوم الإلكتروني الروسي الذي تعرّضت له إبان الانتخابات الرئاسية لعام 2020. فعلى الرغم من فشل الهجوم المزعوم في إيصال ترامب إلى الرئاسة لولاية ثانية، إلا أنّ الولايات المتحدة فرضت عقوبات بحق روسيا لاعتبارها أنّ هذه الهجمات تُشكّل عملاً غير مشروعاً³⁸ بالرغم من عدم تحقق النتيجة³⁹.

في الواقع، تبرز أهمية آثار الهجوم السيبراني في أنّها قد تُوفّر دليلاً حاسماً على حصول التدخل وقد تُساعد في تقييم مدى تناسب أي رد يُتخذ من قبل الدولة المُستهدفة بموجب القانون الدولي. إذ من دون تأثير فعلي واضح، سيكون من الصعب إثبات تأثير الهجوم على

Romana Sadurska, "Threats of Force, The American Journal of International Law", vol. 82, no.2, 36 1988, p. 244, (pp. 239-268); Sean Watts, "Low-Intensity Cyber Operations and the Principle of Non-Intervention", Baltic yearbook of International Law, volume 14, 2015, p. 256.

³⁷ التدخل الروسي في الانتخابات الأميركية: مولر يؤكد مُجدداً أمام الكونغرس أنّ تقريره لم يُبرّئ دونالد ترامب، 2019/07/24، متاح على: <https://www.france24.com/ar/20190724>، تاريخ وساعة الدخول: 2021/10/23، 9:30 ق.ظ.

³⁸ توصّلت وكالات الإستخبارات الأميركية، في تقرير أذار 2021، إلى أنّ الرئيس الروسي وجه، على الأرجح، جهوداً عبر الإنترنت، لمساعدة دونالد ترامب في الفوز بولاية ثانية...، للمزيد راجع: "الولايات المتحدة تفرض عقوبات على روسيا بسبب هجمات إلكترونية شملت" انتخابات الرئاسة 2020"، 2021/04/15، متاح على: <https://www.bbc.com/arabic/world-56745451>، تاريخ وساعة الزيارة: 2021/05/06، 15:15 ب.ظ؛ فارس العمارات، الأمن السيبراني المفهوم وتحديات العصر، الطبعة الأولى، دار الخليج للنشر والتوزيع، الأردن، 2022، ص. 189.

³⁹ كما لم تول ألمانيا أهمية لآثار الهجمات، عندما تحدّثت عن التدخل السيبراني الغير مشروع. إذ اعتبرت أنّ نشر المعلومات الخاطئة وخرق المواقع ذات العلاقة بالعملية الانتخابية من شأنها أن تولّد نزاعات داخلية وتمرد وعصيان مدني، للمزيد راجع: The Federal Government (Germany), On the Application of International Law in Cyberspace, Position Paper, 03/2021, available at : <https://www.auswaertiges-amt.de/blob/2446304/2ae17233b62966a4b7f16d50ca3c6802/on-the-application-of-international-law-in-cyberspace-data.pdf>, accessed: 28/04/2021, 11:00 am.

وذهبت أستراليا في الإتجاه عينه، للمزيد راجع: International Law Supplement to Australia's International Cyber Engagement Strategy, 2019, p.2, available at: https://www.internationalcybertech.gov.au/sites/default/files/2020-11/2019%20Legal%20Supplment_0.PDF, accessed: 28/04/2021, 11:10 am.

قدرة الدولة المُستهدفة على تنفيذ وظائفها السيادية. إلا أنّ عدم حصول آثار لا يجب أن ينفي عن الفعل صفته غير المشروعة⁴⁰. ففي حُكمها الصادر في قضية نيكاراغوا والولايات المتحدة الأميركية، اعتبرت محكمة العدل الدولية أنّ توفير الأموال للمُتمردين الذين يقومون بأنشطة عسكرية وشبه عسكرية ضد نيكاراغوا هو "بلا شك تدخّل في الشؤون الداخلية لنيكاراغوا"⁴¹. فسواء أدّى هذا التمويل إلى النتيجة المرجوة، أي سقوط السلطة الحاكمة أو لم يؤدّ إلى ذلك، لا يُمكن إنكار الضغط الذي تمّت ممارسته على السلطات النيكاراغوانية في شؤونها الداخلية.

أدّا، إنّ تحديد مدى مشروعية الطريقة المستخدمة لممارسة الضغوط على الدولة المستهدفة، لا يجب أن يرتبط بالآثار التي أحدثتها الوسيلة المستخدمة وإنّما بالسلوك الذي تم اعتماده. هل هذا السلوك مُطابق للقانون الدولي أو مُخالف له؟ فحدوث الإكراه مع باقي عناصر التدخل كافٍ لاعتبار الفعل غير مشروع وخرق لمبدأ عدم التدخل، بغض النظر عن مدى انصياع الدولة المُستهدفة للضغط.

المطلب الثاني: التدخل السيبراني في المجال المحفوظ للدولة

تمتلك الدول ذات السيادة الحق في التصرف في شؤونها الداخلية والخارجية بحرية وهو حق مكمل لحق السيادة الذي مُنح لهذه الدول، بموجب القانون الدولي. مما يعني أنّ أي عملية سيبرانية تستهدف التدخل في هذه الشؤون من شأنها أن تتحوّل إلى عملٍ غير مشروع. لذلك يُعالج هذا الفرع عدم جواز التدخل في الشؤون الداخلية والخارجية للدول (الفرع الأول) والحالات الأخرى للتدخل السيبراني غير المشروع (الفرع الثاني).

الفرع الأول: عدم جواز التدخل في الشؤون الداخلية والخارجية للدول

لا يكتمل التدخل غير المشروع إلا إذا تعرّض لشأن من شؤون الدول الداخلية والخارجية، لذلك لا بد من القاء الضوء على مضمون الشؤون الداخلية والخارجية (أولاً) والتدخل السيبراني في شؤون الدول (ثانياً).

أولاً: مضمون الشؤون الداخلية والخارجية

لا يمكن التدرّج بوجود تدخل غير مشروع إلا إذا تناول شؤوناً يعود للدولة صاحبة السيادة الحق بتنظيمها بحرية. أي لا يكفي حصول إكراه بل لا بُدّ من أن يكون قد مُرس بهدف التدخل في شأنٍ من شؤون الدولة سواء الخارجية أو الداخلية. وقد أكّدت محكمة العدل الدولية في قضية نيكاراغوا على ضرورة توافر الصلة بين غُصُرِي التدخل⁴². ولكن كما هي الحال في ما يتعلّق بمفهوم الإكراه، لا يتضمّن أي مصدر من مصادر القانون الدولي تحديد المقصود بهذه الشؤون التي تُعرّف أيضًا بالمجال المحفوظ للدول، كما لا تُوجد أي لائحة أو معيار يُمكن الإستناد إليه لتأكيد أو لنفي ما إذا كان شأن ما يدخل ضمن فئة الشؤون التي لا يحق لأي جهة خارجية بمن فيهم الأمم المتحدة التدخل فيها⁴³. وهو ما يقف عائقاً من جديد أمام محاولة تحديد متى تُشكل الهجمات السيبرانية انتهاكاً لعدم التدخل. حتّى أنّ دليل تالين الذي أكّد على وجوب عدم تدخل الدول سيبرانياً في الشؤون الداخلية أو الخارجية لدولة أخرى، لم يُقدّم توضيحاً كافياً

⁴⁰ للمزيد راجع: محمد عسكر، 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 2013-2017"، مرجع سابق، ص. 386.

⁴¹ محكمة العدل الدولية، القضية المتعلقة بالأنشطة العسكرية وشبه العسكرية في نيكاراغوا وضدّها (نيكاراغوا ضد الولايات المتحدة الأميركية)، تاريخ 27/06/1986، مرجع سابق، ص. 216-217.

⁴² محكمة العدل الدولية، القضية المتعلقة بالأنشطة العسكرية وشبه العسكرية في نيكاراغوا وضدّها (نيكاراغوا ضد الولايات المتحدة الأميركية)، مرجع سابق، ص. 218.

⁴³ للمزيد راجع: علي إبراهيم، الحقوق والواجبات الدولية في عالم متغيّر (المبادئ الكبرى والنظام الدولي الجديد)، دار النهضة العربية، مصر، 1995، ص. 403.

للمقصود بالشؤون الداخلية والخارجية إنما اكتفى بالإشارة إلى مبدأ عدم التدخل الذي أشارت إليه محكمة العدل الدولية في قضية نيكاراغوا في العديد من الإعلانات والمعاهدات الدولية وفي عددٍ من قرارات الجمعية العامة للأمم المتحدة⁴⁴.

وفي محاولة لتحديد نطاق المجال المحفوظ، يُمكن القول بأنّ هذا المجال يتضمّن الشؤون الغير مُنظمة، من حيث المبدأ، من قبل القانون الدولي⁴⁵. ولكنّ هذا التحديد الذي جاء في الرأي الإستشاري للمحكمة الدائمة للعدل الدولية في قضية "مراسيم الجنسية في تونس والمغرب" للعام 1923، وإن كان قد ساعد في وضع معيار لتصنيف الشؤون التي تُعتبر من الاختصاص الداخلي للدول وتلك التي لا تُقرّر فيها الدول بحرية، إلا أنّه لا يُساعد في وضع لائحة مُفصلة ودقيقة بهذه الشؤون. فالقانون الدولي في تطوّر مستمرٍ والشؤون التي كانت في السابق جكرًا على الدولة مُنفردة باتت شأنًا دوليًا⁴⁶. وقد أكدت محكمة العدل الدولية أنّ نطاق تطبيق حظر التدخل يُمكن أن يتطوّر مع تطوّر الممارسات والمواقف الدولية⁴⁷. كما أنّ نطاق المجال المحفوظ يختلف بين دولةٍ وأخرى بحسب الإلتزامات الدولية التي ترتبط بها كل دولة لاسيما من خلال المعاهدات الدولية والإقليمية والثنائية وسواها، إذ لا تُوجد دولتان خاضعتان لإلتزامات قانونية دولية مُطابقة⁴⁸. ممّا يعني أنّ ما يُعتبر شأنًا داخليًا لدولةٍ ما قد يكون خارجيًا لدولةٍ أخرى.

ورغم عدم وجود لائحة بالشؤون التي يُعتبر المساس بها من قبل دولة ما تدخلًا غير مشروعًا، إلا أن عدد من القرارات والإعلانات الدولية والإجتهادات ساهم في تبيان البعض منها⁴⁹. فقد بات من المُتفق عليه على سبيل المثال أنّ اختيار النظام السياسي والاقتصادي والثقافي وصياغة السياسة الخارجية تدخل ضمن إطار المجال المحفوظ للدولة وهو حق غير قابل للتصرف⁵⁰. لذلك، إنّ تشجيع الجماعات الإرهابية أو المعارضة للحكم ودعمها والتدخل في نزاعاتٍ داخليةٍ تدخلًا غير مشروعًا⁵¹، كونه يمسّ بالشؤون الداخلية للدولة المستهدفة. وأكّد خبراء دليل تالين بأن التدخلات في شؤون الدول السياسية والتي تكون مصحوبة بدرجة معينة من الإكراه تعتبر انتهاكًا لمجالها المحفوظ⁵².

⁴⁴ دليل تالين، القاعدة رقم 66، للمزيد راجع: Francois Dellerue, Analyse du Manuel de Tallinn 2.0 sur le droit international applicable aux cyber-opérations, op. cit., p.57

⁴⁵ محكمة العدل الدولية الدائمة، مراسيم الجنسية في تونس والمغرب، تاريخ 1923/02/07، Summaries of Judgments, Advisory opinions and orders of the Permanent Court of international Justice, 2012, Series B, n.4, P.7

⁴⁶ Terry Gill, Non-Intervention in the Cyber Context, in Katharina Ziolkowski, Peacetime Regime for State Activities in Cyberspace, op. cit., p.220.

⁴⁷ محكمة العدل الدولية، القضية المتعلقة بالأنشطة العسكرية وشبه العسكرية في نيكاراغوا وضدّها (نيكاراغوا ضد الولايات المتحدة الأمريكية)، مرجع سابق، ص. 17.

⁴⁸ للمزيد راجع: Russel Buchan, "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?", op. cit., p.224.

⁴⁹ الجمعية العامة، إعلان مبادئ القانون الدولي المتعلقة بالعلاقات الودية والتعاون بين الدول وفقًا لميثاق الأمم المتحدة، قرار رقم 2625، مرجع سابق.

⁵⁰ للمزيد راجع: Marcelo Kohen, "The Principle of Non-Intervention 25 Years After the Nicaragua Judgment", Leiden Journal of International Law, vol. 25, no.1, 2012, p. 159.

⁵¹ محكمة العدل الدولية، القضية المتعلقة بالأنشطة العسكرية وشبه العسكرية في نيكاراغوا وضدّها (نيكاراغوا ضد الولايات المتحدة الأمريكية)، مرجع سابق، ص. 17.

⁵² Francois Dellerue, Analyse du Manuel de Tallinn 2.0 sur le droit international applicable aux cyber-opérations, op. cit., p.57

كل ذلك يسمح بالقول، أنه بالرغم من عدم وجود لائحة بالشؤون الداخلية للدول، إلا أن الخطوط العريضة مرسومة، وما يُشكل تدخلاً غير مشروعاً هو كل عمل يمنع أو يُعيق الدولة صاحبة السيادة من ممارسة سلطاتها واتخاذ قراراتها، بغض النظر عن شكل التدخل سواء أكان مُسلحاً أو غير مُسلحاً حتى لو اتخذ شكل التهديد .

ثانياً: التدخل السيبراني في شؤون الدول

بما أن مبدأ حظر التدخل يهدف إلى حماية حقوق الدولة، لاسيما لجهة ممارسة صلاحياتها وسياساتها في شتى المجالات والحفاظ على سيادتها وسلامتها وحرمتها الإقليمية، فذلك يعني أن الهجمات السيبرانية التي تمسّ بهذه الحقوق والتي تُعتبر تدخلاً غير مشروعاً يُمكن أن تتخذ أشكالاً مُتعددة. فكل هجوم سيبراني مهما كان نوعه، يهدف إلى ممارسة الإكراه على دولة ما بقصد إعاقة قيام السلطات بعملها أو منعها من ممارسة صلاحياتها وحقوقها بحرية أو عرقلة سير أعمالها، سواء لفترة محدودة أو طويلة، يُشكل تدخلاً غير مشروعاً. ويُقدّم لنا الهجوم الذي تعرّضت له استونيا مثلاً واضحاً على التدخل في شؤون الدول من خلال الهجمات الإلكترونية. فقد تمّ استهداف شبكات الإنترنت لدولة إستونيا في 26 نيسان 2007 في هجمات معقدة طالت الشبكات الخاصة بالبرلمان والبنوك والوزارات والصحف والإذاعات، مما أدى إلى شلل في خدمات عامة متعددة لمدة ثلاثة أسابيع وكبدت السلطات خسائر مادية فادحة ومعنوية كبيرة⁵³. هذا الهجوم، الذي حصل بهدف إلزام استونيا بالرجوع عن قرارها المُتعلق بنقل نصب تذكاري لجندي سوفياتي من وسط مدينة تالين⁵⁴، انتهك حق السلطات الإستونية بالتصرف داخل إقليمها في شأن من شؤونها الخاصة، ذلك أن إزاحة تمثال شأن داخلي بحت، وقد تمّ استخدام الهجوم كوسيلة للضغط على السلطات الإستونية. فلو افترضنا أن روسيا هي المسؤولة عن الهجوم نكون أمام تدخل غير مشروع يُعطي السلطات الإستونية الحق بالردّ على الهجوم. في المُقابل، لا يُمكن تصنيف الهجوم السيبراني الذي تعرّضت له شركة سوني الأمريكية⁵⁵ على أنه انتهاك لمبدأ عدم التدخل لافتقاره لعنصر الإكراه. إذ من الصعب تصوّر أن هذا الهجوم شكّل ضغطاً مباشراً أو غير مباشراً على السلطات الأمريكية. صحيح أن هذا العمل يبقى غير مشروع إلا أنه لا يُشكل خرقاً لمبدأ عدم التدخل.

الفرع الثاني: الحالات الأخرى للتدخل السيبراني غير المشروع

قد لا تُشكل العديد من الهجمات السيبرانية بحد ذاتها تدخلاً غير مشروعاً إنما قد تؤدي إلى خرق حظر التدخل، فالهجمات قد تشكل عملاً تحضيرياً أو جزءاً من عمل مُركّب (أولاً)، كما قد تؤدي إلى انتهاك التجسس السيبراني لمبدأ عدم التدخل (ثانياً).

أولاً: الهجمات الإلكترونية كعمل تحضيري أو جزء من عمل مركب

ارتبطت الانتخابات الرئاسية الأمريكية لعام 2016 بأربع هجمات سيبرانية رئيسية⁵⁶، وكانت الأهم بينها سلسلة الهجمات التي استهدفت اللجنة الوطنية الديمقراطية التابعة للحزب الديمقراطي. إذ تم استهداف قاعدة البيانات العائدة للحزب لاسيما الملف المُتعلق بالمُرشح

⁵³ للمزيد حول الهجوم الذي تعرّضت له استونيا راجع: Eneken Tikk & Liis Vihul & al., International Cyber Incidents: Legal Considerations, NATO Cooperative Cyber Defence Centre of Excellence, Estonia, 2010, p.14 -34

⁵⁴ Terry Gill, Non-intervention in the Cyber Context, op. cit., p.234.

⁵⁵ Cyber Attack on Sony Pictures Entertainment, US Homeland Security Statement by Secretary Johnson on 19/12/2014, available at: www.dhs.gov/news/2014/12/19/statement-secretary-johnson-cyber-attack-sony-pictures-entertainment, accessed: 23/09/2021, 9:30 am.

⁵⁶ الهجوم الأول استهدف بريد المرشحة الديمقراطية هيلاري كلينتون، الذي تضمّن معلومات جوهرية تتعلّق بحملتها الإنتخابية. الهجوم الثاني انصبّ على خرق قاعدة بيانات الناخبين وأنظمة البرمجيات الخاصة بها في 39 ولاية، الثالث الهجوم على أجهزة التصويت المستخدمة بصورة واسعة في الولايات المتحدة؛ للمزيد راجع: وثيقة أمريكية مسربة: قراصنة تابعون للاستخبارات الروسية حاولوا

المنافس لدونالد ترامب، في حين أن هجمات أخرى خرقت البريد الإلكتروني للعديد من أعضاء الحزب وغيرها من الوثائق، وقد تمت سرقة المعلومات المتعلقة بها ومن ثم نشرها على موقع ويكيليكس. تم اعتبار أن السلطات الروسية هي المسؤولة عن هذه الهجمات⁵⁷. واعتبر البعض أن الهدف الأساسي لهذه العمليات هو تسهيل وصول ترامب إلى سدة الرئاسة، أي بعبارة أخرى الهدف هو التأثير والتلاعب في الانتخابات الرئاسية الأمريكية لعام 2016. فهل يمكن اعتبار ما حصل تدخلاً في الشؤون الداخلية الأمريكية وبالتالي تدخلاً غير مشروعاً؟

من حيث المبدأ، إن التدخل في الانتخابات الرئاسية لأي دولة يُعتبر شكل من أشكال الإكراه، إذ إن هذا التصرف يؤثر على حق الدولة المستهدفة في اتخاذ قراراتها بحرية في ما يتعلق بشؤونها الداخلية. ولكن لا يمكن اعتبار أن أي تدخل في الانتخابات المتعلقة بدولة من الدول عملاً غير مشروعاً. فتعبير الرئيس الروسي عن رغبته في وصول ترامب إلى سدة الرئاسة لا يُعتبر تدخلاً في حين أن خرق أجهزة التصويت وتغيير النتائج يشكل، دون أدنى شك، انتهاكاً لحظر التدخل. وفي حالة الهجمات التي تعرض لها الحزب الديمقراطي، يجب التمييز بين الهجوم الإلكتروني الذي أدى إلى سرقة المعلومات وبين عملية نشر المعلومات المخترقة على ويكيليكس. ذلك أن عملية خرق البريد الإلكتروني ومختلف الوثائق لا تُشكل بحد ذاتها تدخلاً غير مشروعاً، كونها تشكل عملاً تحضيرياً وليس جزءاً من عمل مُركَّب. فلو توقفت العملية على خرق المواقع وجمع المعلومات دون أن تستتبعها عملية النشر، لكان هذا الهجوم خرقاً للسيادة الأمريكية وليس تدخلاً، في حين أن عملية نشر المعلومات المسروقة يُشكل حُكماً تدخلاً غير مشروعاً يهدف إلى ممارسة الإكراه في العملية الانتخابية التي تُعتبر شأنًا داخلياً بحثاً كونه جزءاً من فعل مُركَّب. من هنا تبرز أهمية التمييز بين العمل التحضيري والفعل الذي يُشكل جزءاً من عمل مُركَّب، ذلك أن وسائل الرد التي تمتلكها الدولة المستهدفة تختلف بحسب ما إذا كان الهجوم الإلكتروني يُشكل انتهاكاً للسيادة أو يرقى إلى مستوى التدخل غير المشروع⁵⁸. رغم هذا الاستنتاج، اعتبر بريان ايغان (المستشار القانوني الأميركي) أن الهجمات السيبرانية لا تُشكل انتهاكاً للقانون الدولي إلا إذا أدت إلى أضرار مادية جسيمة⁵⁹.

الأمر عينه ينطبق في حالة الانتخابات الرئاسية الفرنسية لعام 2017، إذ حصلت العديد من الهجمات الإلكترونية التي استهدفت حملة المرشح ايمانويل ماكرون "En Marche"، وتم نشر المعلومات التي تمت سرقتها عبر عدة مواقع إلكترونية⁶⁰. وكما في الحالة الأمريكية، يجب التمييز بين عملية سرقة المعلومات وعملية نشرها. فعملية الخرق التي استهدفت موقع الحملة الانتخابية تُشكل عملاً

اختراق الأنظمة الانتخابية، 2017/06/08، متاح على: <https://www.france24.com/ar/20170606>، تاريخ وساعة الزيارة: 2021/09/23، 9:45 ق.ظ.

Suzan Henenessey, "What Does the US Government Know about Russia and the DNC Hack?",⁵⁷ 25/07/2016, available at: www.lawfareblog.com/what-does-us-government-know-about-russia-and-dnc-hack, accessed: 23/09/2021, 10:00 am.

Ido Kilovaty, "Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information", Harvard National Security Journal, volume 9, Spring 2018, p. 152.

Jens David Ohlin, "Did Russian Cyber-Interference in the 2016 Election Violate International Law?",⁵⁹ Texas Law Review, vol. 95, 2017, p.1579.

Jean-Baptiste Vilmer, Alexandre Escorcia & al., Information Manipulation: A Challenge for Our Democracies, report by the Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, Fondation Descartes, Paris, 2018.

تحضيرياً وليس جزءاً من عملٍ مُركَّب وبالتالي لا ترقى إلى مستوى التدخل غير المشروع، ولكن يُمكن أن تُشكِّل خرقاً للسيادة الفرنسية. في المُقابل، تُشكِّل عملية نشر المعلومات عملاً مُركَّباً يرقى إلى مستوى التدخل غير المشروع، فيما لو تمَّ إثبات أنَّ السلطات الروسية هي المسؤولة عن الهجمات.

ثانياً: انتهاك التجسس السببراني لمبدأ عدم التدخل

يفتقر القانون الدولي لتعريف موحد للعمل التجسسي. فقد عرّفه دليل تالين بأنه أي عمل يتم القيام به سرّاً أو تحت ادّعاءات كاذبة بواسطة وسائل إلكترونية بهدف جمع معلومات أو محاولة جمعها⁶¹. كما تمَّ تعريفه بأنّه عملية إلكترونية تهدف الى الوصول إلى معلومات سرية غير مُصرّح بالإطّلاع عليها وتتمّ بواسطة وسائل سرية⁶². ورغم خطورة هذا التصرف السري إلا أن القانون الدولي يفترق لأي نصٍ يُحظّر التجسس الدولي أو ينظمه خارج إطار النزاعات المسلّحة⁶³. فالتجسس، الذي يقتصر على جمع المعلومات المتعلقة بالدولة المُستهدفة، لا يُعتبر عملاً مخالفاً للقانون الدولي كما لا يُشكِّل اكرهاً ولا يُقيّد حقوق وحرية الدولة ذات السيادة، أي لا يرتقي مبدئياً إلى مُستوى التدخل غير المشروع في الشؤون الداخلية. وهذا الأمر يسري بغض النظر عن طريقة التجسس المُستخدمة، سواء بواسطة عناصر تابعة للدولة المُتجسّسة وموجودة على أرض الدولة المُستهدفة أو سواء عن بعد بواسطة الوسائل الإلكترونية. وقد اعتمد خبراء دليل تالين نهجاً مُشابهاً حين اعتبروا أن التجسس السببراني لا يُشكِّل خرقاً للقانون الدولي، ولكنهم لم يستبعدوا امكانية أن تؤدي إلى خرق قواعد القانون الدولي على رأسها السيادة وقاعدة حظر التدخل وعدم استخدام القوة⁶⁴.

ورغم عدم وجود نص يحظره، إلا أن التجسس قد يُشكِّل انتهاكاً للقواعد الأساسية التي يقوم عليها القانون الدولي، لاسيما مبدأي السيادة وحظر التدخل⁶⁵. إذ قد تُستخدم المعلومات المسروقة بهدف الضغط على الدولة المعنية وإلزامها على القيام بأعمالٍ أو اتّخاذ قرارات أو الإمتناع عن ذلك في شأن من شؤونها الداخلية أو الخارجية عندها يفقد التجسس، سواء التقليدي أو السببراني، مشروعيتها ليتحوّل إلى عملٍ تحضيريّ لفعلٍ غير مشروع أو ليكون جزء من عملٍ مُركَّب يهدف إلى التدخل في شؤون الدولة. فمشروعية التجسس السببراني أو غيره تعتمد على الهدف المرجو من جمع المعلومات والطريقة التي استُخدمت فيها.

الخاتمة

في ضوء ما تقدّم، يتّضح أنّ التطور التكنولوجي المُتسارع وما رافقه من توسّع في استخدام الفضاء السببراني كأداة لتحقيق أهدافٍ سياسيةٍ واستراتيجيةٍ، قد فرض تحدّيات قانونية غير مسبوقة على قواعد القانون الدولي التقليدية. وإذا كان ميثاق الأمم المتحدة قد وُضع في مرحلةٍ

⁶¹ دليل تالين 1، القاعدة رقم 66، مايكل شميث، دليل تالين بشأن القانون الدولي المطبق على الحروب السببرانية، مرجع سابق.

⁶² هذا التعريف ورد في الوثيقة الصادرة عن معهد "East West Institute" والتي أعدها خبراء روس وأميركيين، للمزيد راجع: محمد عسكر، وضع العمليات السببرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم "دراسة على ضوء دليل تالين" بشأن القانون الدولي المطبق على العمليات السببرانية 2013-2017"، مرجع سابق، ص. 278.

⁶³ صلاح نصر، الحرب الخفية تاريخ المخابرات، الطبعة الأولى، الجزء الثاني، دار الخيال، مصر، 2002، ص. 179.

⁶⁴ محمد عسكر، وضع العمليات السببرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم "دراسة على ضوء دليل تالين" بشأن القانون الدولي المطبق على العمليات السببرانية 2013-2017"، مرجع سابق، ص. 386.

⁶⁵ للمزيد راجع: Fabien Lafouasse, "L'espionnage en droit international", Annuaire francais de droit international, vol. 47, 2001, p.63.

تاريخية لم يكن فيها الفضاء الإلكتروني قد ظهر بوصفه ميداناً للصراع بين الدول، فإن ذلك لا يعني وجود فراغ قانوني يسمح للدول بممارسة أنشطة سيبرانية تمس بسيادة غيرها من الدول وحققها في إدارة شؤونها بحرية.

إذ تبين أن مبدأ عدم التدخل، بوصفه أحد المبادئ الأساسية التي يقوم عليها النظام القانوني الدولي المعاصر، يتمتع بالمرونة الكافية التي تسمح بتطبيقه على التصرفات السيبرانية حتى وإن لم ترق هذه الأفعال إلى مستوى استخدام القوة المحظورة بموجب المادة الثانية الفقرة الرابعة من ميثاق الأمم المتحدة. فالمعيار لا يكمن في الوسيلة المستخدمة بل في طبيعة السلوك ذاته والغاية المرجوة منه. وعليه، فإن الهجمات السيبرانية التي تستهدف التأثير في الإرادة الحرة للدولة أو إكراهها على اتخاذ موقف أو الإمتناع عن اتخاذه في شأن يدخل ضمن نطاق اختصاصها المحفوظ، تشكل تدخلاً غير مشروع يُرتب المسؤولية الدولية للدولة القائمة به.

كما بات واضحاً أن عنصر الإكراه يُشكل حجر الزاوية في تصنيف التدخل السيبراني غير المشروع، وأن تحقق هذا العنصر لا ينبغي أن يُربط حصراً بآثار الهجوم أو بمدى نجاحه في تحقيق أهدافه، بل يجب أن يستند إلى طبيعة السلوك المُرتكب بحد ذاته وما ينطوي عليه من محاولة لإخضاع إرادة الدولة المستهدفة. كذلك تبين أن بعض العمليات السيبرانية كالتجسس الإلكتروني قد لا تكون غير مشروعة في ذاتها لكنها قد تتحول إلى أعمال مخالفة للقانون الدولي متى استخدمت كوسائل للإكراه أو كجزء من فعل مركب يهدف إلى التدخل في الشؤون الداخلية أو الخارجية للدول.

من هنا يتوجب على المجتمع الدولي اتخاذ عدد من التدابير وأبرزها:

1. تعزيز الجهود الدولية الرامية إلى تقنين قواعد السلوك السيبراني للدول من خلال العمل في إطار الأمم المتحدة للوصول إلى اتفاق دولي يحدد بصورة أكثر وضوحاً حدود التدخل السيبراني غير المشروع وآثاره القانونية .
2. تطوير مفهوم الإكراه في القانون الدولي العام بما يتلاءم مع طبيعة الوسائل السيبرانية الحديثة وعدم حصره بالأشكال التقليدية المرتبطة باستخدام القوة العسكرية .
3. اعتماد معايير دولية موحدة لتحديد نطاق المجال المحفوظ للدول في البيئة الرقمية بما يساهم في الحد من التفسيرات المختلفة التي قد تؤدي إلى توسيع أو تضيق نطاق مبدأ عدم التدخل .
4. تعزيز التعاون الدولي في مجال الإسناد التقني والقانوني للهجمات السيبرانية من خلال إنشاء آليات مستقلة لتحديد المسؤولية عن الهجمات العابرة للحدود، بما يحد من ظاهرة الإفلات من المسؤولية الناجمة عن صعوبة تحديد مصدر الهجوم .
5. تطوير التشريعات الوطنية المتعلقة بالأمن السيبراني بما ينسجم مع الالتزامات الدولية للدول مع ضمان احترام قواعد القانون الدولي وحقوق الإنسان في أثناء مواجهة التهديدات الإلكترونية .

وفي الخلاصة، إن مبدأ عدم التدخل يبقى الإطار القانوني لمواجهة التدخلات السيبرانية غير المشروعة، إلا أن فعاليته ستبقى رهناً بمدى قدرة المجتمع الدولي على تطوير قواعد أكثر وضوحاً واستجابةً للتحويلات المتسارعة التي يشهدها الفضاء الإلكتروني.