

مجلة العلوم القانونية والاجتماعية

Journal of legal and social studies

Issn: 2507-7333

Eissn: 2676-1742

دليل تالين والقواعد المنطبقة على الهجمات السيبرانية

The Tallinn Manual and International Legal Norms Applicable to Cyber attacks

محمد الأبيض*

طالب دكتوراة، كلية الحقوق، جامعة الجزائر 01 يوسف بن خدة

m.labiad@univ-alger.dz

تاريخ النشر: 2025/12/01

تاريخ القبول: 2025/10/01

تاريخ ارسال المقال: 2025/09/01

*المؤلف المرسل

الملخص:

شهدت العقود الأخيرة تصاعداً غير مسبوق في حجم وخطورة الهجمات السيبرانية التي باتت تشكل تهديداً حقيقياً للأمن الدولي وفي ظل الغموض القانوني المحيط بتلك الهجمات، جاء دليل تالين كمحاولة فقهية لتقنين تطبيق قواعد القانون الدولي العام على الفضاء السيبراني.

تقدم هذه الدراسة تحليلاً نقدياً للدليل، وتناقش مدى فعاليته في تفسير مبادئ السيادة، وعدم التدخل، وحظر استخدام القوة، والمسؤولية الدولية في البيئة الرقمية، كما تتناول تحديات الإثبات والإسناد، ودور الفاعلين غير الرسميين، والانقسامات الجيوسياسية في تفسير القانون.

وتخلص الدراسة إلى أن دليل تالين، رغم قيمته العلمية، يظل غير كافٍ كمرجع إلزامي لتنظيم السلوك السيبراني للدول، ويستدعي تطويراً عبر اتفاق دولي شامل يحقق التوازن بين الأمن الرقمي والسيادة القانونية.

الكلمات المفتاحية: القانون الدولي العام؛ دليل تالين؛ الهجمات السيبرانية؛ المسؤولية الدولية؛ الفضاء السيبراني.

Abstract:

In recent decades, cyberattacks have become a growing threat to international peace and security, challenging traditional legal frameworks. The Tallinn Manual emerged as a scholarly attempt to interpret how public international law applies to cyberspace.

This study offers a critical legal analysis of the Manual, evaluating its interpretation of key principles such as sovereignty, non-intervention, the prohibition on the use of force, and state responsibility. It also examines the challenges of attribution, the role of non-state actors, and geopolitical biases influencing legal interpretations.

The study concludes that while the Tallinn Manual is a valuable academic resource, it lacks the binding force and inclusivity needed to regulate state behavior in cyberspace, underscoring the need for a more balanced and comprehensive international legal instrument.

Keywords: Public International Law; Tallinn Manual; Cyber Attacks; International Responsibility; Cyberspace.

مقدمة:

شهد العقدان الأخيران تحولاً جذرياً في طبيعة التهديدات التي تواجه الدول، حيث انتقل الصراع من ميادين القتال التقليدية إلى ساحات غير مرئية، يقودها الفاعلون عبر شبكات الحواسيب وأنظمة الاتصالات، فقد أصبحت الهجمات السيبرانية أداة استراتيجية تعتمد عليها الدول والمجموعات غير الحكومية على حد سواء، لاستهداف الخصوم وتحقيق مكاسب سياسية وأمنية واقتصادية، دون خوض حروب معلنة بالمفهوم التقليدي أو صدامات مباشرة، خاصة وأنه وبالرغم من الطبيعة الافتراضية لهذا النوع من الهجمات، فإن الأضرار والمعاناة الناتجة عنها لا تقتصر على العالم الافتراضي، ففي عصر يجري فيه التحكم بكل شيء إلكترونياً، قد تستهدف بعض الهجمات الإلكترونية مؤسسات البنية التحتية، مما يسبب ضرراً للمدنيين بسبب تذبذب أو انقطاع الخدمات أو المواد الأساسية كالمياه أو الكهرباء أو الرعاية الطبية، وقد يترتب على ذلك معاناة كبيرة وربما فقدان البعض لحياتهم.

وقد فرض هذا الواقع الجديد تحديات قانونية عميقة على منظومة القانون الدولي العام، خاصة في ظل الغموض المحيط بكيفية تطبيق القواعد العامة التي تحكم المجتمع الدولي ومن أهمها قواعد السيادة، وحظر استخدام القوة، ومبدأ عدم التدخل على الفضاء السيبراني، وفي هذا السياق جاء دليل تالين كمحاولة فقهية طموحة لتقنين كيفية انطباق قواعد القانون الدولي على العمليات السيبرانية، من خلال جهد جماعي لمجموعة من الخبراء الدوليين تحت إشراف المركز التعاوني للدفاع السيبراني التابع لحلف الناتو.

ورغم أن الدليل لا يتمتع بقوة إلزامية، فإنه أصبح مرجعاً رئيسياً في النقاشات الفقهية والسياسية المتعلقة بالأمن السيبراني، لا سيما في ظل التصعيد العالمي المتزايد للهجمات السيبرانية التي تستهدف البنى التحتية الحيوية، والمؤسسات السيادية، والمجتمعات المدنية.

غير أن هذا الدور المتنامي للدليل يثير تساؤلات حيوية حول مدى اتساق محتواه مع مبادئ القانون الدولي الراسخة، وحول قدرته على تلبية متطلبات المشهد السيبراني المتغير بسرعة فائقة.

من هنا، تهدف هذه الدراسة إلى تحليل قانوني نقدي لمضامين دليل تالين، من خلال تقييم مدى نجاحه في تقديم إطار منهجي لتطبيق قواعد القانون الدولي العام على العمليات السيبرانية، والكشف عن أوجه القوة والقصور فيه، كما تسعى الدراسة إلى وضع الدليل ضمن سياقه السياسي والقانوني، واستكشاف ما إذا كان يشكل أساساً مناسباً لتطوير اتفاق دولي ملزم، أم أنه يكرّس اختلالات في فهم وتطبيق القانون الدولي في الفضاء الرقمي.

إشكالية الدراسة:

رغم الأهمية الفقهية المتزايدة لدليل تالين، إلا أن طابعه غير الملزم وتعدد التأويلات التي يقدمها لمبادئ القانون الدولي، يطرح إشكالية جوهرية حول مدى قدرته على ضبط النشاط السيبراني في ظل التصعيد العالمي المتسارع للهجمات.

فهل يوفر دليل تالين إطاراً قانونياً فعالاً ومتسقاً لتطبيق قواعد القانون الدولي العام على الهجمات السيبرانية؟

وإلى أي مدى يواكب هذا الدليل تطورات الفضاء السيبراني من حيث المفاهيم، والمسؤولية، والعتبات القانونية لاستخدام القوة، والرد القانوني المشروع؟

الأسئلة الفرعية:

1. ما مدى دقة ووضوح المفاهيم القانونية التي يعتمدها الدليل (مثل السيادة السيبرانية، وعدم التدخل) ؟
2. كيف يؤسس الدليل لمبدأ المسؤولية الدولية عن الهجمات السيبرانية؟
3. ما مدى واقعية التفسير الذي يقدمه الدليل لمفهوم استخدام القوة في الفضاء السيبراني؟
4. هل يمكن اعتبار الدليل أساساً لبناء اتفاق دولي ملزم أم أنه يكرّس ازدواجية المعايير؟
5. ما هي حدود الدليل القانونية والسياسية في ظل غياب توافق دولي شامل حول محتواه؟

فرضيات الدراسة:

- تفترض الدراسة أن دليل تالين، رغم أهميته لا يقدم إجابات حاسمة لكافة الإشكالات القانونية المرتبطة بالفضاء السيبراني، بل يفتح الباب لتأويلات متباينة بين الدول.
- كما تفترض أن محتوى الدليل يعكس رؤية قانونية غربية تميل إلى تبرير ممارسات بعض الدول الكبرى، دون تحقيق توازن قانوني شامل.

أهداف الدراسة:

1. تحليل المبادئ القانونية الأساسية التي اعتمدها دليل تالين في تنظيم العمليات السيبرانية.

2. تقييم مدى اتساق محتوى الدليل مع قواعد القانون الدولي العام، خاصة ما يتعلق باستخدام القوة والمسؤولية الدولية.

3. تقديم قراءة نقدية في ضوء الممارسات الدولية الحديثة في مجال الأمن السيبراني.

4. اقتراح مداخل لتطوير منظومة قانونية أكثر توازنًا وشمولًا في مجال القانون الدولي السيبراني.

المنهج المعتمد:

تعتمد الدراسة على المنهج التحليلي النقدي، القائم على تحليل الدليل من زاوية قانونية مقارنة، من خلال:

- تحليل النصوص القانونية الدولية ذات الصلة (ميثاق الأمم المتحدة، قواعد المسؤولية الدولية...)
- مراجعة فقه القانون الدولي، وآراء الخبراء المشاركين في إعداد دليل تالين.
- تقييم الفجوة بين المبادئ النظرية والممارسة الدولية الواقعية.

المبحث الأول: الإطار النظري والقانوني لدليل تالين

في ظل التوسع المتسارع للفضاء السيبراني، برزت الحاجة إلى تأطير قانوني ينظم سلوك الدول في هذا المجال. وقد جاءت وثيقة دليل تالين لتشكل مرجعًا فقهيًا مهمًا يسعى إلى إسقاط قواعد القانون الدولي العام على العمليات السيبرانية، يتناول هذا المبحث الإطار النظري والمرجعي للوثيقة، مع التركيز على طبيعتها القانونية ومبادئها الأساسية.

المطلب الأول: الطبيعة القانونية والسياسية لدليل تالين

إن تحديد الطبيعة القانونية لدليل تالين يعد خطوة أساسية لفهم موقعه ضمن منظومة القانون الدولي فهذا المطلب يحلل الخلفية السياسية التي نشأ في سياقها الدليل، ويستعرض مدى إلزاميته القانونية وانعكاس ذلك على قيمته التطبيقية في ضبط الهجمات السيبرانية.

الفرع الأول: السياق الدولي لنشأة دليل تالين

برز دليل تالين في سياق تصاعد الهجمات السيبرانية وتزايد تأثيرها على الأمن القومي للدول، خاصة بعد سلسلة من الهجمات البارزة التي استهدفت منشآت مدنية وحكومية، كهجوم "ستوكس نات" الذي سبب أضرارًا وخيمة للبرنامج النووي الإيراني، وهو برمجية خبيثة يعتقد أنها طورت من طرف الولايات المتحدة الأمريكية

وإسرائيل، وكذا الهجمات العديدة التي استهدفت أوكرانيا وأهمها الهجمات على النظام الآلي الانتخابي في جوان 2014 واختراق شبكة الكهرباء في ديسمبر 2016، وقد أدرك المجتمع الدولي هشاشة الإطار القانوني التقليدي في التعامل مع هذه التهديدات الجديدة، ما دفع مركز التميز للدفاع السيبراني التعاوني التابع لحلف شمال الأطلسي إلى إطلاق مشروع علمي لصياغة مرجعية قانونية للفضاء السيبراني، تُرجم أولاً في "دليل تالين 1.0" سنة 2013، ثم نُقح بشكل موسع في إصدار تالين 2.0 سنة 2017.¹

يمتاز هذا الإصدار الأخير بتوسيع نطاقه ليشمل حالات السلم وليس فقط النزاعات المسلحة، مما يجعله أكثر شمولاً، كما يُعد ثمرة جهد جماعي لمجموعة من الخبراء القانونيين من دول متعددة، سعت إلى تفسير كيفية تطبيق قواعد القانون الدولي العام، بما فيها قواعد ميثاق الأمم المتحدة، على العمليات السيبرانية.²

الفرع الثاني: الطبيعة القانونية غير الملزمة للدليل وتداعياتها

رغم أهمية دليل تالين كمصدر فقهي متقدم، إلا أنه يفتقر إلى الصفة الإلزامية، فهو ليس معاهدة ولا قراراً دولياً صادراً عن هيئة رسمية، بل يمثل جهداً أكاديمياً شبه جماعي، وهو ما يثير تساؤلات حول مدى إمكانية اعتباره مرجعاً معتمداً لتفسير القانون الدولي، خاصة أن محتواه يعكس إلى حد كبير الرؤية الغربية-الأطلسية لأمن الفضاء السيبراني.³

وقد ترتب على هذا الطابع غير الملزم عدم وجود توافق دولي حول مضمون الوثيقة المذكورة، حيث رفضت بعض الدول الكبرى، كروسيا والصين، الاعتراف بها أو اعتبارها مرجعاً ملزماً، بينما تبنتها دول غربية عديدة ضمن سياساتها الدفاعية السيبرانية.⁴

كما أن هذه الوثيقة، وعلى الرغم من قيمتها التحليلية، ما زالت تفتقر إلى الشرعية التمثيلية الشاملة التي تؤهلها لتكون قاعدة عالمية لتنظيم الفضاء السيبراني.⁵

المطلب الثاني: المبادئ الأساسية لدليل تالين في ضوء القانون الدولي العام

يعتمد الدليل في تأصيله القانوني على تفسير عدد من المبادئ العامة للقانون الدولي، ومحاولة تطبيقها على الفضاء السيبراني، يهدف هذا المطلب إلى تحليل مدى اتساق هذه التفسيرات مع الإطار التقليدي للقانون الدولي، لاسيما فيما يتعلق بمبدأ السيادة، وعدم التدخل، واستخدام القوة، والدفاع المشروع.

الفرع الأول: مبدأ السيادة وعدم التدخل في الفضاء السيبراني

يقرّ دليل تالين بأن مبدأ السيادة ينطبق على الفضاء السيبراني، على غرار المجالات البرية والبحرية والجوية وبموجب هذا التصور، فإن أي تدخل خارجي في أنظمة الدولة السيبرانية يمكن أن يُعد انتهاكاً للسيادة، إلا أن الدليل يفرّق بين الانتهاك "الفعلي" الذي يؤدي إلى أضرار مادية ملموسة (كالتسبب في شلل شبكة الكهرباء وشبكة التزود بالمياه) والانتهاك "البسيط" (كالتجسس الإلكتروني)، ويعتبر أن الانتهاك الأول فقط هو الذي يشكل خرقاً حقيقياً للسيادة.⁶

أما بالنسبة لمبدأ عدم التدخل، فإن الدليل يعتمد تفسيراً قريباً من اجتهاد محكمة العدل الدولية في قضية نيكاراغوا، حيث يعتبر التدخل محظوراً إذا مسّ بنظام الدولة في مجالات تُعدّ من صميم اختصاصها، كالنظام السياسي أو الاقتصادي، غير أن هذا المعيار يظل غامضاً في البيئة السيبرانية، حيث يصعب التمييز بين التدخل المشروع (مثل حرية التعبير الرقمية) والتدخل غير المشروع (مثل التأثير على الانتخابات).⁷

الفرع الثاني: استخدام القوة والحق في الدفاع المشروع

عالج دليل تالين إشكالية حساسة تتمثل في متى يمكن اعتبار الهجوم السيبراني "استخداماً للقوة" وفقاً للمادة 02 فقرة 04 من ميثاق الأمم المتحدة، ويقر الدليل أن الهجمات السيبرانية يمكن أن ترقى إلى مستوى استخدام القوة إذا ترتب عليها أثر مادي جسيم، كإحداث دمار في البنى التحتية أو إزهاق الأرواح.⁸

وتبعاً لذلك، يرى الدليل أنه يجوز للدولة المتضررة ممارسة حقها في الدفاع الشرعي وفق المادة 51 من الميثاق، بشرط أن يُشكّل الهجوم السيبراني عدواناً مسلحاً بمفهومه التقليدي، إلا أن هذا الطرح يواجه صعوبة في تحديد "عتبة الضرر" التي تبرر تفعيل الحق في الدفاع المشروع، خاصة في ظل طبيعة الهجمات السيبرانية التي غالباً ما تكون خفية وتدرجية.⁹

وعليه، فإن الدليل رغم سعيه لتأصيل تطبيق قواعد القانون الدولي العام على الواقع السيبراني، يظل قاصرًا عن تقديم معيار دقيق لتحديد متى يبلغ الفعل السيبراني مستوى "التهديد" أو "استخدام القوة"، فهو يعتمد مقارنة قائمة على الآثار المترتبة على الهجوم، كمعيار رئيسي في التكيف، دون أن يبلور مؤشرات واضحة لهذا الأثر، ما يجعل مسألة التوصيف القانوني عرضة لتقديرات متباينة، فعلى سبيل المثال قد تعتبر بعض الدول اختراقا الكترونيا تهديدًا مباشرًا لأمنها القومي، في حين لا ترى فيه دول أخرى ما يرقى إلى هذا الوصف.

المبحث الثاني: التقييم النقدي والحدود القانونية لدليل تالين

رغم القيمة النظرية لدليل تالين، إلا أن فعاليته التطبيقية تظل محل جدل واسع، خاصة في ظل التحديات المرتبطة بالإثبات، والإسناد، وتعدد الفاعلين غير الرسميين، يهدف هذا المبحث إلى تقديم قراءة نقدية لمضمون الدليل، وتحديد حدوده القانونية والعملية في تنظيم الهجمات السيبرانية.

المطلب الأول: المسؤولية الدولية للدولة عن الهجمات السيبرانية

تُعد المسؤولية الدولية من الركائز الأساسية لضبط سلوك الدول، لكن تطبيقها على الهجمات السيبرانية يواجه عقبات جوهرية، يناقش هذا المطلب موقف دليل تالين من إسناد الأفعال السيبرانية إلى الدول، ومدى إمكانية مساءلتها وفقًا للقواعد التقليدية للمسؤولية الدولية.

الفرع الأول: قواعد الإسناد في دليل تالين ومدى واقعيته

تُعد مسألة الإسناد من أعقد الإشكاليات التي تواجه القانون الدولي السيبراني، نظرًا لما تتسم به الهجمات الإلكترونية من طابع سري، واعتمادها على تقنيات التخفي، والتمويه، وتعدد الأطراف الوسيطة¹⁰، يحاول دليل تالين معالجة هذه الإشكالية من خلال تبني المعايير التقليدية للإسناد في المسؤولية الدولية كما وردت في مشروع لجنة القانون الدولي حول مسؤولية الدولة عن الأفعال غير المشروعة دوليًا¹¹.

وينص الدليل على أن الهجوم السيبراني يُنسب إلى دولة ما إذا نفذه أحد أجهزتها الرسمية أو ارتكب تحت توجيهها أو سيطرتها الفعلية، إلا أن هذا الشرط - المستمد من معيار "السيطرة الفعلية" في قضية نيكاراغوا - يصعب إثباته تقنيًا في الفضاء السيبراني، حيث لا تترك الهجمات بصمات مادية مباشرة، وغالبًا ما يتم تنفيذها عبر أجهزة مخترقة في دول ثالثة.¹²

وقد انتُقد الدليل على هذا الأساس، لأنه يعتمد معايير تقليدية دون مراعاة خصوصيات الفضاء السيبراني، مما يجعل إثبات الإسناد شبه مستحيل في أغلب الحالات، ويفتح الباب أمام "الإنكار المعقول" من طرف الدول المعتدية.¹³

الفرع الثاني: مسؤولية الدولة عن أفعال الفاعلين غير الرسميين

يناقش دليل تالين أيضاً إمكانية تحميل الدولة المسؤولية عن أفعال فاعلين غير رسميين، كمجموعات القراصنة المدعومة أو المتواطئة مع الدولة، ويقر الدليل بأنه يمكن تحميل الدولة المسؤولية عن أفعال هؤلاء إذا ثبت أنها وجهتهم، أو كانت تمارس سيطرة فعلية على عملياتهم، أو تبنت أفعالهم لاحقاً بشكل صريح.¹⁴

غير أن هذا الشرط يُعتبر من الناحية العملية معقداً جداً، إذ غالباً ما تكون العلاقة بين الدولة وهذه الكيانات مبنية على الإنكار، أو الدعم غير المباشر، أو غض الطرف عن نشاطاتها.

كما أن غياب آليات تحقيق دولية أو تقنية مستقلة للتحقق من علاقة الدولة بالفاعل السيبراني يعرقل عملية الإسناد القانوني، ما يجعل من تطبيق المسؤولية الدولية أمراً نظرياً أكثر منه عملياً، ويضعف من فعالية قواعد الردع القانوني في الفضاء السيبراني.

المطلب الثاني: نقد شامل للدليل وآفاق تطوير القانون الدولي السيبراني

تبرز الحاجة إلى نقد منهجي للدليل تالين من أجل تبيان أوجه قصوره، واقتراح السبل الممكنة لتطوير إطار قانوني أكثر شمولاً وفعالية، يهدف هذا المطلب إلى تقييم مدى حيادية الدليل، وطرح رؤية مستقبلية لتطوير قانون دولي سيبراني قادر على مواجهة التحديات المتسارعة.

الفرع الأول: أوجه القصور في محتوى الدليل وتحيزه الجيوسياسي

رغم الطابع التقني والفقهي العالي للدليل تالين، إلا أنه لا يخلو من ثغرات قانونية ومحددات سياسية، أبرزها غلبة الرؤية الغربية/الأطلسية على محتواه، فالمشاركون في إعداد الوثيقة ينتمون في غالبيتهم إلى دول الناتو أو دول متحالفة معه، وهو ما أدى إلى بروز تأويلات تتماهى مع مواقف هذه الدول¹⁵، لا سيما فيما يتعلق بتوسيع مفهوم الاستخدام المشروع للقوة، أو التفسير الفضفاض لمبدأ السيادة السيبرانية.

كما أن الدليل لم يشرك خبراء من دول أخرى تمثل تيارات قانونية مغايرة (كالصين، روسيا، أو دول الجنوب)، ما يطرح تساؤلات حول مدى تمثيله للنظام القانوني الدولي بصورته الشاملة.

يُضاف إلى ذلك أن الدليل لا يقدم حلولاً عملية لغياب آليات الإسناد التقنية، أو لطبيعة الهجمات المجهولة المصدر، مما يُضعف من قيمته كمرجع تطبيقي فعال.

الفرع الثاني: إمكانية تطوير الدليل إلى اتفاق دولي ملزم

يشير دليل تالين جداراً قانونياً حول ما إذا كان يصلح كأساس لصياغة اتفاق دولي شامل ينظم الفضاء السيبراني، من جهة، يعد الدليل خطوة متقدمة من حيث التنظيم المنهجي للمبادئ الدولية، وتوفير إطار أولي للتعامل مع العمليات السيبرانية في السلم والنزاع، ومن جهة أخرى، فإن اعتماده على تفسيرات غير توافقية، وتجاهله للمواقف المختلفة للدول، يجعل من الصعب تحويله إلى اتفاقية جامعة.¹⁶

لكن رغم هذه التحديات، يمكن النظر إلى الدليل كأساس "تفاوضي" يمهد الطريق نحو بلورة معاهدة دولية ملزمة، شريطة:

- إشراك كافة الأطراف الدولية في صياغتها.
- تجاوز التحيزات الجيوسياسية.
- تضمين آليات تقنية وقانونية أكثر دقة في الإسناد والمساءلة.

إن تطوير إطار قانوني سيبراني جامع لم يعد ترفاً قانونياً، بل أصبح ضرورة تفرضها وتيرة التصعيد العالمي للهجمات السيبرانية، وتوسع أثرها على السلم والأمن الدوليين.

يُظهر تحليل دليل تالين أنه يمثل خطوة مهمة في مسار تقنين الفضاء السيبراني، لكنه يعاني من قصور قانوني وواقعي في مواكبة طبيعة هذا المجال شديد التعقيد، فبينما يوفر الدليل إطاراً فقهيًا قيمًا، إلا أن غياب التوافق الدولي، وضعف آليات الإثبات، وغلبة الرؤية الأحادية، تحدّ من قدرته على التأثير الحقيقي في ضبط سلوك الدول السيبراني.

لذلك، فإن الحاجة إلى تطوير هذا الدليل أو تجاوزه نحو اتفاقية دولية أكثر شمولاً وتوازناً، تُمثّل أولوية قصوى في زمن باتت فيه الهجمات السيبرانية تُهدد قواعد القانون الدولي والسلم العالمي على حد سواء.

الخاتمة

أفضى التحليل القانوني والنقدي لدليل تالين إلى إبراز مكانته كمرجع فقهي مهم في مجال القانون الدولي السيبراني، حيث مثّل محاولة طموحة لسد فراغ تنظيمي في مواجهة تصاعد الهجمات السيبرانية عالميًا، فقد تناول الدليل جملة من المبادئ القانونية الأساسية كالسيادة، وعدم التدخّل، وحظر استخدام القوة، والمسؤولية الدولية، في محاولة لإسقاطها على البيئة الرقمية، التي تتميز بتعقيداتها التقنية وغموض أطرافها وتعدد مصادرها.

غير أن الوثيقة محل الدراسة، على الرغم من اتساع نطاقها وجودة منهجها التحليلي، لم تنج من عدد من الإشكاليات الجوهرية، أهمها طابعها غير الملزم، وغياب الإجماع الدولي حول تفسيراتها، فضلًا عن صعوبة تطبيق قواعد المسؤولية الدولية التقليدية على العمليات السيبرانية، خاصة في ظل غموض هوية الفاعل، وتعقيد الإسناد، واعتماد بعض الدول على فاعلين غير رسميين، كما أن التأويلات التي تقدمها الوثيقة لمفاهيم مركزية - كالاستخدام المشروع للقوة - ظلت أقرب إلى الرؤية الغربية منها إلى منظور جامع متعدد الاتجاهات.

وقد أظهرت هذه الدراسة أن دليل تالين، وإن كان مفيدًا كأساس للنقاش القانوني، إلا أنه غير كاف ليكون إطارًا عمليًا لضبط سلوك الدول في الفضاء السيبراني، بل إنه قد يؤدي - إذا اعتمد دون تطوير أو توافق - إلى تعميق الانقسامات القانونية والسياسية، بدلًا من توحيد الممارسات الدولية.

وبناءً عليه، فإن مستقبل القانون الدولي في المجال السيبراني يظل مرهونًا بمدى قدرة المجتمع الدولي على تجاوز المقاربات الفقهية المحدودة، والانتقال نحو تنظيم تعاوني ملزم يُحقق التوازن بين الأمن السيبراني وحقوق السيادة، ويضمن حماية البنى التحتية الحيوية والسلم الدولي في بيئة باتت أكثر هشاشة وتهديدًا من أي وقت مضى.

الهوامش

- ¹ Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017, p. 12.
- ² Marco Roscini, Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, p. 89.
- ³ محمد عبد الحكيم، القانون الدولي والنزاعات السيبرانية، دار الفكر الجامعي، الإسكندرية، 2020، ص. 66.
- ⁴ Duncan B. Hollis, "Why States Need an International Law for Information Operations," Lewis & Clark Law Review, Vol. 21, No. 4, 2017, p. 1035.
- ⁵ لجنة القانون الدولي، مشروع مواد حول مسؤولية الدول عن الأفعال غير المشروعة دوليًا، الأمم المتحدة، 2001، ص 40.
- ⁶ Nicholas Tsagourias & Russell Buchan, Research Handbook on International Law and Cyberspace, Edward Elgar, 2015, p. 121.
- ⁷ أحمد رفعت، مبادئ القانون الدولي العام، دار الجامعة الجديدة، الإسكندرية، 2018، ص 311.
- ⁸ François Delerue, Cyber Operations and International Law, Cambridge University Press, 2020, p. 176.
- ⁹ United Nations, Charter of the United Nations, 1945, <https://www.un.org/en/about-us/un-charter>.
- ¹⁰ Michael N. Schmitt, Tallinn Manual 2.0, Cambridge University Press, 2017, p. 32.
- ¹¹ لجنة القانون الدولي، مرجع سابق، ص 36.
- ¹² أحمد حسن الشريف، القانون الدولي ومسؤولية الدولة عن الأفعال السيبرانية، دار النهضة العربية، القاهرة، 2020، ص 81.
- ¹³ Russell Buchan, Cyber Espionage and International Law, Hart Publishing, 2018, p. 67.
- ¹⁴ Michael N. Schmitt, Tallinn Manual 2.0, Cambridge University Press, 2017, p. 55.
- ¹⁵ Schmitt Michael & Liis Vihul, "The Nature of International Law Norms in Cyberspace", in Proceedings of the International Law Association, 2016, p. 214.
- ¹⁶ Qing Lu, "A Chinese Perspective on the Tallinn Manual: Sovereignty and State Responsibility", Journal of East Asia & International Law, Vol. 10, No. 1, 2017, p. 61.