الالتزام الدولي ببذل العناية الواجبة في الفضاء السيبراني
بين التدابير الرادعة ومنع الأضرار السيبرانية العابرة

دكتور / أسامة حمزة محمود عبد الفتاح
مدرس القانون الدولي العام كلية الحقوق

.

Abstract:

There are divergent views about the existence of a rule or principle of "due diligence in cyberspace", As some jurisprudence claiming the absence of an obligation to act seriously in cyberspace. In this study, we try to analyze these points of view, in an attempt to fill the gap between the two point of view.

The objective of highlighting the exercise of due diligence in this context, is to consolidate the international commitment to take reasonable steps to prevent and / or stop and / or deter acts of cyber aggression issued or cross the territory of the state.

The renewed interest in the concept can be explained by the continuing challenges from a realistic and legal point of view, such as the ratio of these malicious cyber operations

(ISSN: 2356 - 9492)

to a person in international law, in light of the growing reliance on techniques of concealment and redirection.

In light of the escalation of military operations in Ukraine 2022, As cyber-attacks have increased remarkably. These dangerous threatening practices do not appear as temporary operations that can be eliminated. On the contrary, they gradually turn into a consistent pattern in international conflicts, and the fact that they do not rise to the level of armed attack necessarily sheds light on the Due diligence in cyberspace.

قائمة الاختصارات:

CC	Cyber Crime
DRM	Digital Rights Management
ECJ	European Court of Justice
ECOWAS	Economic Community of West African States
FBI	Federal Bureau of Investigation
GDPR	General Data Protection Regulation
ICCPR	International Covenant on Civil and Political Rights
IPR	Intellectual Property Rights
LEA	Law Enforcement Agency
ICSPA	International Cyber Security Protection Alliance
MLA	Mutual Legal Assistance
MOU	Memorandum Of Understanding

NCSD	National Cyber Security Division
NCFTA	National Cyber-Forensics & Training Alliance
NCIJTF	National Cyber Investigative Joint Task Force
NCSA	National Cyber Security Alliance
NCSC	National Cyber Security Centrum
FAR	Federal Acquisition Regulation
GPL	General Public License
IRS	Internal Revenue Service
MLAT	Mutual Legal Assistance Treaty
MO	Modus Operandi
URL	Uniform Resource Locator
ACHR	American Convention on Human Rights

أولاً: إشكالية البحث

نناقش في تلك الدراسة الجدل المثار حول الالتزام ببذل العناية الواجبة في الفضاء السيبراني من منظور القانون الدولى. فوفقًا للصياغة التقليدية لمحكمة العدل الدولية في قضية قناة كورفو ، فإن كل دولة "ملزمة بعدم السماح عن علم باستخدام أراضيها في أعمال تتعارض مع حقوق الدول الأخرى "في السياق السيبراني ، حثت الجمعية العامة للأمم المتحدة الدول بالفعل في عام 2000 على "ضمان أن قوانينها وممارساتها تقضي على الملاذات الآمنة لأولئك الذين يسيئون استخدام تكنولوجيا المعلومات بشكل إجرامي ."

هناك بعض الجدل حول ما إذا كان مبدأ العناية الواجبة يعكس التزامًا قابل للتطبيق على العمليات السيبرانية .كما تم اقتراح أنه في السياق السيبراني ، من الأفضل تفسير العناية الواجبة كمعيار للإسناد بدلاً من اعتبارها قاعدة أساسية قائمة بذاتها في القانون الدولي .ومع ذلك ، يستمر التحليل الحالي على أساس أنه من باب *القانون النافذ* ، فإن العناية الواجبة تشكل التزامًا دوليًا عامًا على كل دولة بعدم السماح عن عمد باستخدام أراضيها لارتكاب أعمال غير مشروعة دوليًا باستخدام الوسائل الإلكترونية .

لا تستلزم العناية الواجبة واجب المنع ، بل تستلزم التزامًا بسلوك . فالدولة تخل بالتزامها ببذل العناية الواجبة في وجود العناصر التراكمية التالية:

(ISSN: 2356 - 9492)

1. وجود أفعال (من قبل جهة فاعلة من غير الدول أو دولة من الغير) تتعارض مع حقوق الدولة الضحية ،
2. التي يتم إجراؤها من أو عبر أراضي الدولة التي يُحتمل أن تكون مسؤولة (أو من أو عبر الإقليم أو البنية التحتية الإلكترونية الخاضعة لسيطرتها) ،
3. التي كان من الممكن أن تكون غير قانونية إذا قامت بها الدولة التي يحتمل أن تكون مسؤولة .
4. التي لها عواقب وخيمة على الدولة الضحية.
5. فيما يتعلق بمعرفة فعلية أو بناءة للدولة التي يحتمل أن تكون مسؤولة ، و
6. التي يمكن للدولة المسؤولة أن تتصرف بناءً عليها ، لكنها تفشل في اتخاذ جميع التدابير الممكنة.

نحاول فى تلك الدراسة البحث عن فهم وتصور منهجية القانون الدولي فيما يتعلق بسلوك الدولة الدؤوب فى الفضاء الإلكتروني. على الرغم من أنه ليس هناك حلًا سحريًا فى مواجهة تحديات الأمن السيبراني الحالية والتهديدات الناشئة عن تنامي الأنشطة غير السلمية لتقنيات الفضاء السيبراني، بيد أننا نري أن القانون الدولي قادر عي صياغة أساسًا قانونيًا قويًا وشاملًا لمنع الضرر والمساءلة.

ثانياً: منهجية البحث

تقوم تلك الدراسة على المناهج؛ التحليلي، والتطبيقي، والمقارن في شق منها. حيث تحاول تلك الدراسة سبر أغوار تلك القضية عبر تحليل أحكام القانون الدولي، سيما المبادئ الدولية المتجذرة في الاتفاقيات الدولية أو العرف الدولي ، والمستقاة من السوابق القضائية، أضف إلي ذلك أحكام القانون الدولي لحقوق الإنسان وأحكام القانون الدولي الإنساني. حيث يتمحور جوهر تلك الدراسة في تدقيق وفهم طبيعة الالتزام ببذل العناية الواجبة في الفضاء السيبراني في وقت السلم كالتزام حاكم لممارسات الدول في السياق السيبراني. مع بحث إمكانية تطبيق القواعد العامة في القانون الدولى على الفضاء السيبراني وعلاقة تلك المبادئ ببذل العناية الواجبة. مع تسليط الضوء على الموقف التشريعي لبعض الأنظمة القانونية الأكثر نشاطاً في هذا السياق.

ثالثاً: التساؤلات التي تطرحها تلك الدراسة: -

الحديث عن بذل العناية الواجبة فى السياق السيبراني، لا يزال مشوباً بكثير من الغموض، فهل هو المبدأ العام للقانون الدولي، أو التزام قائم بذاته أو معيار للسلوك، وما إذا كانت هناك ثمة قواعد محددة تتطلب السلوك الدؤوب فى الفضاء السيبراني؟ وهل الدول عليها واجب التصدي للهجمات السيبرانية المنطلقة من أراضيها تجاه الدول والأفراد من الغير؟ كيف يمكن تقدير الأضرار السيبرانية ؟ وهل هناك حد أدني لذلك الضرر ؟ ثم كيف يمكن إسناد المسؤولية الدولية عن الأضرار السيبرانية؟

عادة ما يُثار الإخفاق فى بذل العناية الواجبة بعد تعرض الدولة الضحية المدعية للضرر، كيف يمكن نسبة الهجوم السيبراني لدولة أو جهة ما؟ كيف يجمع مقدم الطلب أدلة كافية لإثبات نية الإضرار أو معرفة الدولة المدعى عليها؟ ومن ثم مدي مخالفتها التزام العناية الإلكترونية؟ سيكافح مقدم الطلب لإثبات قضيته فى غياب مساعدة المدعى عليه أو على الأقل الموافقة على جمع الأدلة. الدول الضحية تواجه صعوبات تتعلق بالأدلة، مما يسمح "باللجوء بشكل أكثر ليبرالية إلى استنتاجات الحقائق والأدلة الظرفية. . .

الالتزام الدولي ببذل العناية الواجبة في الفضاء السيبراني
بين التدابير الرادعة ومنع الأضرار السيبرانية العابرة

د. أسامة حمزة محمود عبد الفتاح

مجلة الدراسات القانونية والاقتصادية

مقدمة

اكتسب مفهوم العناية الواجبة مؤخرًا فى السياق السيبراني زخماً متصاعداً، كآلية واعدة لمساءلة الدول عن الأضرار الناجمة بسبب العمليات الإلكترونية التي قد تنشأ من أراضيها أو تمر عبرها، متي توافرت عناصر الإسناد بموجب قواعد المسؤولية الدولية وذلك في خضم الحرب المستعرة بين روسيا وأوكرانيا. ومع ذلك، فإن الالتباس يحيط بطبيعة ومحتوى ونطاق العناية الواجبة.

فالحديث عن تأصيل قواعد القانون الدولي فى هذا المجال الحديث من النشاط البشري الآخذ فى التنامي بشكل متسارع، ينبع من حقيقة مفادها أن تلك الأنشطة باتت تشكل أداة هامة من أدوات الحرب فى عالمنا المعاصر، ومستقبل النزاعات الدولية بشكل عام، نذكر من ذلك على سبيل المثال الهجمات السيبرانية، والاستخدام غير السلمي لتكنولوجيا الذكاء الاصطناعي، والاعتماد على الأسلحة ذاتية التشغيل أو تكنولوجيا حرب الفضاء ما يهدد حفظ السلم والأمن الدوليين.

فهناك وجهات نظر متباينة حول وجود قاعدة أو مبدأ "العناية الواجبة فى الفضاء السيبراني"، أو أخري تدعي بغياب الالتزام بالتصرف بجدية فى الفضاء الإلكتروني. نحاول فى تلك الدراسة تحليل وجهات النظر تلك، فى محاولة للإجابة على تلك الأسئلة.

إن الحكمة من تسليط الضوء على بذل العناية الواجبة ضمن هذا السياق، هو تأصيل الالتزام الدولي باتخاذ خطوات معقولة لمنع و / أو وقف و / أو ردع أفعال العدوان السيبراني الصادرة أو العابرة لإقليم الدولة. فالاهتمام المتجدد بالمفهوم يمكن تفسيره من خلال التحديات المستمرة من الناحية الواقعية والقانونية، كنسبة تلك العمليات السيبرانية الخبيثة إلى أحد أشخاص القانون الدولي، فى ظل تنامى الاعتماد على تقنيات إخفاء الهوية وإعادة التوجيه.

ينبع الالتباس جزئيًا من الاستخدام غير المتسق لمصطلح "العناية الواجبة" كمبدأ عام للقانون، سيما القانون الدولي، أو التزامًا واحدًا، أو أكثر من التزام يقع على عاتق الدولة أو معيارًا للسلوك ينطبق فى مجالات القانون الدولي المختلفة.

لتجنب هذا التناقض، نقترح تحويل النقاش من التسمية إلى المضمون. بدلاً من الاستفسار عما إذا كانت "العناية الواجبة" تنطبق فى الفضاء الإلكتروني، فإن السؤال الذي يجب أن نطرحه هو إلى أي مدى تتحمل الدول التزامات بحماية الدول والأفراد الآخرين من الأضرار السيبرانية.

يمكننا استنتاج، أنه سواء كان المبدأ العام للعناية الواجبة ينطبق على تكنولوجيا المعلومات والاتصالات أم لا أو مدي إلزامية "قاعدة العناية الواجبة" فى الفضاء السيبراني، هناك سؤال يبقي دائما محل جدل، هل الدول تظل ملزمة بواجب لمنع وإيقاف وإنصاف الضرر الناشئ عن الممارسات غير السلمية فى الفضاء الإلكتروني، سيما إن كان عابراً أو صادراً من أراضيها؟

(ISSN: 2356 - 9492)

حيث ترتكز "التزامات الحماية" على العديد من القواعد الأساسية للقانون الدولي التي تكرس معيارًا للعناية الواجبة - أي الالتزامات التي تتطلب من الدول بذل قصارى جهدها فى منع ووقف ومعالجة مجموعة متنوعة من الأضرار، سواء فى السياق السيبراني أو خارجه.

تبدأ هذه الدراسة بشرح سبب اعتقادنا أن "العناية الواجبة" فى القانون الدولي تُفهم بشكل أفضل على أنها معيار للسلوك، على الرغم من الالتباس طويل الأمد المحيط بمعناها ونطاقها. وتحديداً الأهداف المتوخاة من تطبيق هذا المعيار، كمنع الضرر أو التخفيف منه وجبر الضرر، ولكنه يختلف باختلاف الالتزامات "الوقائية" حيث توجد، بالإضافة إلى الحالات والظروف والمجالات التي تنطبق فيها.[1]

نتناول بالشرح تالياً، سبب تطبيق القانون الدولي برمته - بما فى ذلك الالتزامات "الوقائية" بشكل افتراضي على الفضاء الإلكتروني، فى حالة عدم وجود قاعدة على عكس ذلك. هذا الادعاء مدعوم بأدلة على ممارسات الدولة وتعبيراتها ذات الصلة من الرأي القانوني.

علي أن نطرح بعض التطبيقات العملية لمعيار بذل العناية الواجبة، من خلال عرض مجموعات من واجبات الحماية التي تتطلب من الدول منع أو وقف أو تعويض بعض الأضرار من خلال التصرف بجد فى الفضاء الإلكتروني. يمكن إرجاع اثنين من هذه الالتزامات إلى الالتزامات الأساسية للقانون الدولي العام: (1) واجب الدول فى عدم السماح عن قصد باستخدام أراضيهم لأعمال تتعارض مع حقوق الدول الغير، المشار إليها بحكم محكمة العدل الدولية بقضية قناة كورفو[2] ، والتي نشير إليها بمبادئ "قناة كورفو"؛[3] و (2) واجب الدول فى منع وجبر الضرر الجسيم العابر للحدود، حتى لو نجم عن أنشطة مشروعة، المعروف بمبدأ "عدم الضرر".[4]

بالإضافة إلى ذلك، تحدد هيئات معينة من القانون الدولي واجبات العناية الواجبة التي تنطبق أيضًا على الفضاء السيبراني. من الأمور ذات الأهمية الخاصة لتكنولوجيا المعلومات والاتصالات ما يلي: (3) التزام الدول بحماية حقوق الإنسان فى نطاق ولايتها القضائية؛ و (4) واجبات ضمان الاحترام للقانون الدولي الإنساني واتخاذ تدابير احترازية ضد آثار الهجمات فى حالة نشوب نزاع مسلح. نحدد الأساس القانوني لكل من هذه القواعد الأساسية فى القانون الدولي العرفى أو التقليدي، ونفكك المعايير المختلفة للعناية الواجبة التي تكرسها ونستكشف مدى تطبيقها على استخدام الدول لتكنولوجيا المعلومات والاتصالات. أخيرًا، على الرغم من طبيعتها المتعددة الأوجه، فإن السمات المشتركة تتناقض مع التزامات الحماية المختلفة.

بناء عليه، رأينا تقسيم تلك الدراسة إلى فصلين :

---

[1] تشمل الأمثلة القانون البيئي الدولي، وقانون البحار، والحماية الدبلوماسية، وقانون الاستثمار الدولي، والقانون الدولي الإنساني، والقانون الدولي لحقوق الإنسان، بموجب قانون المعاهدات أو القانون الدولي العرفي.

Koivurova, 'Due Diligence', in Max Planck Encyclopedia of Public International Law (MPEPIL) (2010), paras 1–2, available at opil.ouplaw.com/view/10.1093/ law:epil/9780199231690/law-9780199231690-e1034?prd=EPIL (referring to due diligence as 'an obligation of conduct' as well as a 'concept' and a 'general principle of law.

[2] راجع:

Corfu Channel (United Kingdom v. Albania), Judgment, 9 April 1949, ICJ Reports (1949) 4, at 22 (hereinafter 'Corfu Channel').

[3] راجع

Reinisch and Beham, 'Mitigating Risks: Inter-State Due Diligence Obligations in Case of Harmful Cyber-Incidents and Malicious Cyber-Activity – Obligations of the Transit State', 58 German Yearbook of International Law (GYIL) (2015) 101, at 106 (framing the Corfu Channel principle as a 'conflict-related no harm rule').

[4] راجع:

Case Concerning Pulp Mills on the River Uruguay (Argentina v. Uruguay), Judgment, 20 April 2010, ICJ Reports (2010) 14, paras 101, 187, 197, 204, 223 (hereinafter 'Pulp Mills').

الالتزام الدولي ببذل العناية الواجبة في الفضاء السيبراني
بين التدابير الرادعة ومنع الأضرار السيبرانية العابرة

د. أسامة حمزة محمود عبد الفتاح

مجلة الدراسات القانونية والاقتصادية

الفصل الأول: النظام القانوني لبذل العناية الواجبة وتدابير الردع فى الفضاء السيبراني

الفصل الثاني: بذل العناية الواجبة فى الفضاء السيبراني على ضوء قواعد القانون الدولي العام

الفصل الأول

النظام القانوني لبذل العناية الواجبة فى الفضاء السيبراني

تمهيد وتقسيم:

هناك آراء متباينة حول وجود قاعدة أو مبدأ "العناية الواجبة في الفضاء السيبراني" ، فبعض الدول تدافع عن عدم وجود التزام بالعمل الجاد في الفضاء السيبراني، بينما يؤيد جانب آخر من الدول العكس. في هذه الدراسة ، نحاول تحليل وجهات النظر هذه ، في محاولة لسد الفجوة بين وجهتي النظر. الهدف من تسليط الضوء على ممارسة العناية الواجبة في هذا السياق ، هو تعزيز الالتزام الدولي لاتخاذ خطوات معقولة لمنع أو وقف أو ردع أعمال العدوان السيبراني الصادرة أو عبور أراضي الدولة.

يمكن تفسير الاهتمام المتجدد بالمفهوم من خلال التحديات المستمرة من وجهة نظر واقعية وقانونية ، مثل نسبة هذه العمليات السيبرانية الخبيثة إلى شخص في القانون الدولي ، في ضوء الاعتماد المتزايد على تقنيات الإخفاء وإعادة التوجيه . وفي ظل تصاعد العمليات العسكرية في أوكرانيا 2022 ، ازدادت الهجمات الإلكترونية بشكل ملحوظ. لا تظهر ممارسات التهديد الخطيرة هذه على أنها عمليات مؤقتة يمكن القضاء عليها. على العكس من ذلك ، فإنها تتحول تدريجياً إلى نمط ثابت في النزاعات الدولية ، وحقيقة أنها لا ترقى إلى مستوى الهجوم المسلح تلقي بالضرورة الضوء على العناية الواجبة في الفضاء الإلكتروني.

وعلى الرغم من وجود وفرة نسبية من العمل الذي تم إنجازه لاستكشاف ملامح قانون الحرب الإلكترونية، فقد تم إيلاء اهتمام أقل بكثير لمناقشة حالة السلام السيبراني المطبق دون مستوي الهجوم المسلح. فلم تنظر محكمة العدل الدولية صراحةً فى شرعية الأسلحة السيبرانية حتى هذه اللحظة، وإن كان حكمها الصادر فى قضية مضيق كورفو يشير إلى عدم جواز استخدام أراضي دولة ما "فى أعمال تضر بشكل غير قانوني بدول أخرى".

(ISSN: 2356 - 9492)

نبدأ تلك الدراسة بالتعرف علي مضمون الالتزام ببذل العناية الواجبة، وذلك من خلال التعرف على مفهوم الفضاء السيبراني، والأفعال التي تشكل انتهاك للسيادة في الفضاء السيبراني. على أن ندخل بشكل مباشر في الجانب التحليلي لتلك الإشكالية من خلال طرح أوجه الخلاف حول انطباق بذل العناية الواجبة في الفضاء السيبراني.

تم تخصيص هذا القسم، لبحث مضمون الالتزام ببذل العناية الواجبة فى الفضاء السيبراني، من حيث مفهوم بذل العناية الواجبة فى السياق السيبراني، والأفعال التي تشكل انتهاك للسيادة في الفضاء السيبراني، ثم ننطلق للحديث عن الخلاف حول طبيعة الالتزام الدولي ببذل العناية الواجبة فى الفضاء السيبراني، ثم قابلية تطبيق وإلزامية معيار بذل العناية الواجبة فى هذا السياق.

نتناول في ذات الإطار، مشروعية التدابير الاستباقية لمنع الأضرار العابرة فى الفضاء السيبراني، سيما مدي التزام الدولة باتخاذ تدابير وقائية فى الفضاء السيبراني، ثم الاثار المترتبة على تجاهل اتخاذ التدابير الوقائية فى الفضاء السيبراني. حيث نركز على مبادئ القانون الدولي ، المستقاة من مبادئ قناة كورفو وواجب منع الأعمال السيبرانية والالتزام بمنع الضرر السيبراني العابر للحدود ومبدأ عدم التدخل.

على أن نختم هذا الفصل، ببحث بذل العناية الواجبة فى السياق السيبراني من منظوري القانون الدولي لحقوق الإنسان والقانون الدولي الإنساني. حيث نكرس هذا الجزء لبحث الموضوعات التالية: الالتزام ببذل العناية الواجبة تجاه حماية حقوق الإنسان فى الفضاء السيبراني، ثم بذل العناية الواجبة تجاه الانشطة السيبرانية بموجب أحكام القانون الإنساني الدولى ، الواجب العام لضمان احترام القانون الدولي الإنساني فى الفضاء السيبراني، على أن نختم هذا الفصل بواجب اتخاذ التدابير الوقائية للحد من آثار الحرب السيبرانية.

المبحث الأول
مضمون الالتزام ببذل العناية الواجبة فى الفضاء السيبراني

نادرًا ما تغيب جوانب الأمن السيبراني عن الصفحة الأولى، فمن الهجمات على منظومة SWIFT المصرفية إلى الهجمات الإلكترونية على شبكة الكهرباء فى أوكرانيا، يحتل الأمن السيبراني بشكل متزايد مركز الصدارة بمجالات متنوعة من الجغرافيا السياسية، والاقتصاد الدولي، والأمن، والقانون. ومع ذلك، لا يزال مجال قانون وسياسة الأمن السيبراني الدولي ووضع إستراتيجية ناظمة ومستدامة غير ناضج نسبيًا.[1]

على سبيل المثال، مع وجود وفرة نسبية من العمل المنجز لاستكشاف ملامح قانون الحرب الإلكترونية، فقد تم إيلاء اهتمام أقل بكثير لتعريف قانون السلام السيبراني المطبق دون بلوغ مستوي الهجوم المسلح.

هذا أمر مثير للدهشة لأن الغالبية العظمى من الهجمات الإلكترونية لا ترقى لمستوى الهجوم المسلح. ومن بين أهم الأسئلة التي لم تتم الإجابة عليها، ما هي بالضبط التزامات العناية الواجبة للدول لتأمين شبكاتها ومحاكمة المهاجمين السيبرانين أو تسليمهم.

لدى محكمة العدل الدولية ("ICJ") بعض الاجتهادات القضائية التوجيهية بشأن هذه النقطة، مثل قضية مضيق كورفو التي تلزم الدول "بعدم استخدام الأراضي فى أعمال تضر بشكل غير قانوني بدول أخرى"[2] ومن ثم ماهي الخطوات التي يتعين

[1] على الرغم من بعض الخطوات المهمة إلى الأمام في السنوات الأخيرة مثل دليل تالين ومشروعات تالين 2.0.

Schmitt, Michael N., ed. Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press, 2017.

[2] انظر:

Corfu Channel Case (United Kingdom v. Albania), 1949. I.C.J. 244 (Dec.15). de Maizière, Thomas. 2014. 1

(ISSN: 2356 - 9492)

علـى الـدول والشـركات الخاضـعة لولايتهـا القضـائية اتخاذهـا لتـأمين شـبكاتها مـن الهجمـات السـيبرانية، مـع مراعـاة اسـتجلاء حقوق ومسؤوليات دول العبور؟

يسـتعرض هـذا الفصـل الحجـج المحيطـة بإنشـاء معيـار العنايـة الواجبـة للأمـن السـيبراني ويـدافع عـن نظـام اسـتباقي يأخـذ فـى الاعتبار المسؤوليات المشتركة والمتباينة لمختلف أصحاب المصلحة فى الفضاء السيبراني.[1]

المطلب الأول
مفهوم بذل العناية الواجبة فى السياق السيبراني

يمكـن تعريـف "العنايـة الواجبـة السـيبرانية"، بأنهـا "مراجعـة الحوكمـة والعمليـات والضـوابط المسـتخدمة لتـأمين أصـول المعلومـات"[2] هـذا التعريـف يمكـن فهمـه علـى أنـه الالتزامـات الوطنيـة والدوليـة العرفيـة للجهـات الفاعلـة الحكوميـة وغيـر الحكوميـة للمسـاعدة فـى تحديـد وترسـيخ أفضـل ممارسـات الأمـن السـيبراني وآليـات الحوكمـة وذلـك لتحقيـق السـلام السـيبراني مـن خـلال تعزيـز أمـن أجهزة الكمبيوتر والشبكات والبنية التحتية لتكنولوجيا المعلومات والاتصالات.

وانطلاقاً من تعريف القانون الدولي بأنه "مجموعة القواعد القانونية،" القواعد والمعايير التي تطبق "بين الدول ذات السيادة" والجهات الفاعلة من غير الدول، بما فى ذلك المنظمات الدولية والشركات متعددة الجنسيات، التي تتمتع بالشخصية القانونية الدولية.[3]

---

[1] انظر:

Ensign, Rachel Louise. 2014. Cybersecurity due diligence key in M&A deals. W all Street Journal, April 24. http://blogs.wsj.com/riskandcompliance/ 2014/04/24/ cybersecurity-due-diligence-key-in-ma-deals

[2] انظر:

Ryan, Tim, and Leonard Navarro. 2015. Cyber due diligence: Pre-transaction assessments can uncover costly risks. Kroll, January 28. http://blog.kroll.com/2015/cyber-due-diligencepre-transaction-assessments-can-uncover-costly-risks/

[3] يرى أستاذنا الدكتور/ مصطفى أحمد فؤاد ، أن القاعدة القانونية الدولية هي كل قاعدة مكتوبة وغير مكتوبة تحكم السلوك الاجتماعى لأشخاص القانون الدولى وتتصف بالعمومية والتجريد. انظر ا.د / مصطفى أحمد فؤاد ، أحكام القانون الدولي العام ، مكتبة جامعة طنطا ، دون سنة نشر ، ص 25.

والمصادر الأساسية للقانون الدولي هي المعاهدات، والمبادئ العامة للقانون، والعرف، والتي يتطلب ثالثها دليلًا على ممارسة الدولة التي تتبعها الدول انطلاقا من شعور بالالتزام القانوني فى ظل غياب نظام تعاهدي قوي وبالنظر إلى الصعوبات الجيوسياسية للتفاوض بشأن اتفاقيات جديدة فى هذا المجال، من الضروري توضيح دور القانون الدولي العرفي من حيث علاقته بالعناية الواجبة. فبالنظر إلى الطبيعة الحديثة والتطور السريع للقدرات السيبرانية، هناك عدد قليل نسبيًا من المعاهدات التي تتناول على وجه التحديد حقوق والتزامات الدول تجاه هذه القدرات السيبرانية مع استثناء ملحوظ للاتفاقية الأوروبية بشأن الجريمة السيبرانية (المعروفة أيضًا باسم اتفاقية بودابست). راجع:

Shackelford, Scott J., Scott Russell, and Andreas Kuehn. "Defining cybersecurity due diligence under international law: Lessons from the private sector." *Ethics and Policies for Cyber Operations* (2017): 115-137. 25 Mar 2021.

الالتزام الدولي ببذل العناية الواجبة في الفضاء السيبراني
بين التدابير الرادعة ومنع الأضرار السيبرانية العابرة

د. أسامة حمزة محمود عبد الفتاح

مجلة الدراسات القانونية والاقتصادية

قد توجد التزامات بذل العناية الواجبة فى مجال الأمن السيبراني بين الدول[1]، وبين الجهات الفاعلة غير الحكومية (على سبيل المثال، الشركات الخاصة)، وبين الجهات الحكومية وغير الحكومية. تشمل الأدوات القابلة للتطبيق المعايير التقنية والمتطلبات القانونية الناشئة عن معاهدة أو عرف، فضلاً عن السياسات الوطنية وقواعد صناعة القطاع الخاص.

بالرغم من الاهتمام المتجدد ببذل العناية الواجبة[2] ، فإن هذا المفهوم ليس بجديد. ويمكن إرجاع أصوله الحديثة إلى سلسلة من عمليات التحكيم فى القرن التاسع عشر وأوائل القرن العشرين المتعلقة بحماية الأجانب فى الخارج[3]. التي أشارت إلى التصرف بعناية معقولة فى ظل هذه الظروف، وإسناد المسؤولية عن الإهمال المتعمد. فى وقت لاحق، وجد قرار التحكيم في جزيرة بالماس أن هذا الالتزام هو نتيجة طبيعية للحقوق السيادية للدول على أراضيها، مما يتطلب منها حماية حقوق الدول الأخرى فيها.[4] منذ ذلك الحين، تطور المفهوم جنبًا إلى جنب مع العديد من القواعد الأساسية للقانون الدولي.

ويمكننا القول كمبدأ عام أن العناية الواجبة تنبع من السيادة الإقليمية فى الفضاء الإلكتروني فالعناية الواجبة هي نتيجة طبيعية للمساواة بين الدول فى السيادة. حيث تتمتع الدولة بالولاية القضائية على كامل إقليمها [5]و"احترام. . . السيادة الإقليمية ينبع من المساواة والاحترام المتبادل بين الدول.[6]

أولاً، حيث قضت محكمة العدل الدولية فى قضية مضيق كورفو، بأنه "من واجب كل دولة ألا تسمح عن علم باستخدام أراضيها فى أعمال تتعارض مع حقوق الدول الأخرى"[1] ، التي تشكل أفعالًا غير مشروعة دوليًا. ومن تلك الزاوية هذا الواجب المصاغ على أنه "مبدأ

---

[1] راجع في ذلك:

U.N. Charter art. 2(4), art. 51; Schmitt ed., Tallinn Manual, supra note 5, 45, 47-8; Michael Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, 37 Colum. J. Transnat'l L. 914 (1999);

راجع في ذلك

Terry D. Gill & Paul A. L. Ducheine, Anticipatory Self-Defense in the Cyber Context, 89 Int'l. L. Studies. 440 (2013); Matthew C. Waxman, Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), 36 Yale J. Int'l L. 421, 431 (2011).

[2] راجع :

Stephens, Tim, and Duncan French. "ILA Study Group on Due Diligence in International Law, Second Report, July 2016." *International Law Association, London* (2016).

راجع أيضا:

H. Krieger, A. Peters, and L. Kreuzer (eds), Due Diligence and Structural Change in the International Legal Order (2020); J. Kulesza, Due Diligence in International Law (2016);

راجع أيضا:

Pisillo-Mazzeschi, Riccardo. "The due diligence rule and the nature of the international responsibility of states." *German YB Int'l L.* 35 (1992): 9..

[3] انظر لمزيد من التفاصيل كل من :

e.g., Alabama Claims (United States v UK) (1872) 29 RIAA 125, at 127, 129, 131–132; Wipperman (United States v Venezuela) (1887), reprinted in J. Bassett Moore, History and Digest of the International Arbitrations to Which the United States Has Been a Party, vol. 3 (1898) 3039, at 3041.

راجع:

(United States v Mexico) (1926) 4 RIAA 60, at 61–62.

[4] راجع:

Island of Palmas (or Miangas) (theUnited States v Netherlands), 4 April 1928, II RIAA 829 (1928), ICGJ 392 (PCA 1928), at 839 (hereinafter 'Island of Palmas').

[5] Reparation for Injuries Suffered in the Service of the United Nations, Advisory Opinion, 1949 I.C.J. Rep. 174, 180 (Apr. 11).

[6] Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. Rep. 14, 106 para. 202.

(ISSN: 2356 - 9492)

معترف به من مبادئ القانون الدولي"، ينطبق بشكل عام على جميع الدول، والفشل فى ممارسة الدرجة المطلوبة من الاجتهاد يؤدي إلى مسؤولية الدولة.[2]

ثانيًا، نتيجة للقلق المتزايد بشأن الضرر البيئي والمخاطر الأخرى التي تعبر الحدود الوطنية [3]، تظهر العناية الواجبة أيضًا فى الالتزام العام بعدم التسبب فى ضرر جسيم عابر للحدود للأشخاص أو الممتلكات أو البيئة.[4] يوجد هذا الالتزام منذ عام 1941 على الأقل، عندما وجدت هيئة التحكيم فى Trail Smelter أن الدولة "مدينة فى جميع الأوقات بواجب حماية الدول الأخرى من الأفعال الضارة التي يرتكبها أفراد انطلاقا من الإقليم الخاضع لولايتها القضائية".[5]

وبالمثل، تقر المادة 3 من مشروع المواد لعام 2001 الصادر عن لجنة القانون الدولي بشأن منع الضرر العابر للحدود الناجم عن الأنشطة الخطرة بواجب الدول فى "اتخاذ جميع التدابير المناسبة لمنع الضرر الجسيم العابر للحدود أو التقليل إلى أدنى حد من مخاطره فى أي حال من الأحوال". [6]

فالتزام العناية الواجبة "لا يفرض على الدول منع أو وقف الضرر الجسيم العابر للحدود[7] ، ولكن "بذل أفضل الجهود الممكنة للحد من [مثل هذا]] الخطر ".[8] وقد أكدت محكمة العدل الدولية أيضًا الأساس العرفي لهذا الواجب[9] ، وفقاً لمبدأ عدم الضرر أو" حسن الجوار " ذلك إلى جانب مبدأ قناة كورفو.[10] كما توجد واجبات مماثلة للتصرف بجد بموجب القانون الدولي لحقوق الإنسان.

هذه التزامات إيجابية للدول لحماية وضمان حقوق الإنسان الفردية، سواء عبر الفضاء الإلكتروني أو خارجه، إلى أقصى حد ممكن. [11] وبالمثل، فإن واجبات ضمان احترام القانون الدولي الإنساني واتخاذ الاحتياطات اللازمة لحماية المدنيين من الآثار الناجمة عن النزاع المسلح هي أيضًا التزامات بممارسة العناية الواجبة.[1]

---

[1] Corfu Channel, Judgment, 9 April 1949, ICJ Reports (1949), at 22 (emphasis added).

[2] International Law Commission (ILC), Articles on Responsibility of States for Internationally Wrongful Acts, GA Res. 56/83, 12 December 2000, art. 14(3) (hereinafter 'ARSIWA').

[3] Corfu Channel, Judgment, 9 April 1949, ICJ Reports (1949), at 22.

[4] See ILC, Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries, in Report of the International Law Commission on the work of its fifty-third session (23 April–1 June and 2 July–10 August 2001), UN Doc. A/56/10, 144, at 148–149 (hereinafter 'Draft Articles on Prevention).

راجع أيضا:

Brunée and Meshel, 'Teaching an Old Law New Tricks: International Environmental Law Lessons spacefor cyber Governance', 58 GYIL (2015) 129, at 134–135

[5]Trail Smelter (United States v. Canada) (1941) 3 RIAA 1911, at 1963.

[6] راجع في ذلك:

International Law Commission (ILC), Articles on Responsibility of States for Internationally Wrongful Acts, GA Res. 56/83, 12 December 2000, art. 14(3) (hereinafter 'ARSIWA').

[7] Timo Koivurova, Due Diligence, in Max Planck Encyclopedia of Public International Law (Rüdiger Wolfrum ed., Feb. 2010), http://opil.ouplaw.com/view/10.1093/ law:epil/9780199231690/law-9780199231690-e1034; Pulp Mills on the River Uruguay (Arg. v. Uruguay), 2010 I.C.R. Rep. 14, 55-56 para. 101 (Apr. 2010); Legality of the Threat or Use of nuclear weapons, Advisory Opinion, 1996 I.C.J. Rep. 226, 242 paras. 29 (July, 1996); Trail Smelter Arbitration (U.S. v. Can.), Award, 3 R.I.A.A. 1905, 1965 (Perm. Ct. Arb. 1941)

[8]ILC, Draft Articles on Prevention, *supra* note 21, at 154, Commentary to art. 3, para. 7.

[9] *Legality of the Threat or Use of nuclear weapons*, Advisory Opinion, 8 July 1996, ICJ Reports (1996) 226, para. 2(hereinafter '*Nuclear Weapons*').

[10] *Pulp Mills*, Judgment, 20 April 2010, ICJ Reports (2010), para. 101.

[11]United Nations Human Rights Council (HRC), Res. 32/13 ('The promotion, protection and enjoyment of human rights on the Internet'), UN Doc. A/HRC/RES/32/13, 1 July 2016, § 1.

الالتزام الدولي ببذل العناية الواجبة في الفضاء السيبراني
بين التدابير الرادعة ومنع الأضرار السيبرانية العابرة

د. أسامة حمزة محمود عبد الفتاح

مجلة الدراسات القانونية والاقتصادية

فيما يتعلق بأضرار مختلفة، مثل واجب منع الإبادة الجماعية بموجب المادة الأولى من اتفاقية الإبادة الجماعية، الالتزام بمنع التلوث البحري. [2] التأكد من أن أنشطة التعدين فى منطقة قاع البحار العميقة لا تلحق الضرر بالبيئة والحياة البشرية[3] ، وواجبات التعاون فى التحقيق والمقاضاة فى الجرائم عبر الوطنية.[4] تشير هذه المجموعة المتنوعة من القواعد الأساسية التي تعترف بواجب الرعاية المعقولة إلى أن "العناية الواجبة" نفسها هي ببساطة معيار للسلوك يوجد فى التزامات "وقائية" مختلفة تتباين بحسب موضوعات القانون الدولي، والمكلفين بالواجبات والظروف الواقعية.[5]

وهكذا، فإن الإشارات الواردة فى أدبيات القانون الدولى إلى "التزامات العناية الواجبة" تبدو وكأنها اختصار لسلسلة من الالتزامات التي تشترك فى فرض واجب وقائي، يُقاس الالتزام به مقابل معيار معين من السلوك الجاد.. كما أكدت رابطة القانون الدولي (ILA) فى دراستها الأخيرة حول الموضوع[6]:

"فى جوهرها، تُعنى العناية الواجبة بتوفير معيار من الرعاية يمكن تقييم الخطأ بناءً عليه. فهو معيار المعقولية الذي يسعى إلى مراعاة عواقب السلوك غير المشروع ومدى إمكانية تفادي هذه العواقب عمليا من قبل الدولة أو المنظمة الدولية لمنع حدوثها.[7]

يبدو أن هذه الواجبات المختلفة تنطوي فى المقام الأول على علاقة ثلاثية بين (1) الجهة المسؤولة، أي الدولة التي عليها التزام بالتصرف بجدية فى منع، أو وقف، أو تعويض الضرر، أو مخاطره؛ (2) مصدر الضرر، أي الدولة أو الكيان غير الحكومي الذي تسبب فى الضرر؛ و (3) المستفيد من الواجب، أي الكيان الحكومي أو غير الحكومي الذي يعاني من عواقب الضرر.

ولهذا السبب فإننا نصور ونؤطر هذه الواجبات على أنها "التزامات حماية"، من حيث إنها تتطلب من المكلف بالواجب التصرف بجدية فى حماية المستفيد من الأذى. حيث تشمل مصادر الضرر المحتملة وكلاء الدولة والأفراد الذين يتصرفون بمفردهم أو فى مجموعات،

---

[1]Convention on the Prevention and Punishment of the Crime of Genocide, 1948, 78 UNTS 277, art. 1(hereinafter Genocide Convention). See also *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)*, Judgment, 26 February 2007, ICJ Reports (2007) 43, paras 430–431.

[2] UN Convention on the Law of the Sea, 1982, 1833 UNTS 397, art. 194(2) (hereinafter 'UNCLOS').

[3] راجع:

Ibid., arts 139, 153(4) and Annex III, art. 4(4). See also *Responsibilities and Obligations of States with Respect to Activities in the Area*, Advisory Opinion, 1 February 2011, ITLOS Reports (2011) 10, paras 107–123, 136, 141–142, 147, 189, 217, 219, 239.

[4] راجع:

e.g., International Convention for the Suppression of the Financing of Terrorism, 1999, 2178 UNTS 197, art. 18; United Nations Convention against Transnational Organized Crime, 2000, 2225 UNTS209, art. 7.

[5] راجع:

Krieger and Peters, 'Due Diligence and Structural Change in the International Legal Order', in Krieger, Peters and Kreuzer

[6] راجع:

Kolb, 'Reflections on Due Diligence Duties and Cyberspace', 58 *GYIL* (2015) 113, at 116;

راجع أيضا:

Pisillo-Mazzeschi, *supra* note 11, at 40, 42; *Neer (United States v Mexico)* (1926) 4 RIAA 60, at 61.

[7] راجع:

Besson, 'Due Diligence and Extraterritorial Human Rights Obligations – Mind the Gap!', 9 *ESIL Reflections* (2020) 2, at 4–5.

(ISSN: 2356 - 9492)

فضلاً عن الشركات. يمكن أن يكون المستفيدون، الذين قد يمتلكون أو لا يمتلكون حقًا معينًا تجاه المكلف بالواجب، دولًا أو أفرادًا أو شركات خاصة أخرى.

عندما تكون الدولة المكلفة بالواجب هي مصدر الضرر الذي يؤثر على فرد أو شيء ما، وتكون العلاقة مع المستفيد ثنائية وليست ثلاثية، سواء كان واجب الحماية هو واجب العناية الواجبة أم لا، فهذا يعتمد على الالتزام الأساسي المعني. يبدو أن مبدأ مضيق Corfu مقصور على واجب منع أنشطة الأطراف من الغير، التي لا يمكن أن تُنسب إلى صاحب الواجب الأصيل وهو الدولة[1] على النقيض من ذلك، يبدو أن مبدأ عدم الإضرار، وواجبات حماية[2]وضمان حقوق الإنسان[3] ، والالتزامات باتخاذ الاحتياطات بموجب القانون الدولي الإنساني[4] تنطبق جميعها ليس فقط على الحالات التي تفشل فيها الدولة المكلفة بالواجب فى منع الضرر من قبل أطراف من الغير، ولكن أيضًا حيث تتسبب الدولة نفسها فى الضرر المعني وبالتالي تفشل فى منعه أو إيقافه أو تصحيحه.

وبالتالي، ارتبطت الالتزامات الوقائية بشكل عام بفكرة أن الدول يجب أن تتصرف بجدية بهدف منع أو وقف أو معالجة مجموعة متنوعة من الأضرار أو المخاطر التي يتعرض لها الأشخاص أو الممتلكات أو الأراضي، بدءًا من الأفعال غير المشروعة دوليًا إلى الأنشطة المشروعة أو حتى الحوادث.

يتم تقييم مدي وفاء الدولة بمبدأ بذل العناية الواجبة من خلال مجموعة متنوعة من العوامل، بما فى ذلك (1) وجود نوع معين من الضرر أو المخاطر؛ (2) درجة خطورة هذا الضرر (3) الصلة بين الدولة والضرر أو المخاطرة المعنية؛ (4) درجة معينة من المعرفة بالضرر أو الخطر؛ و (5) قدرة الدولة على التصرف فى ظل الظروف.

ومع ذلك، كما سيتضح فى الأقسام التالية، قد يختلف كل عنصر من هذه العناصر عبر واجبات الحماية المختلفة. نحن ندعي أن هذه الواجبات، الموجودة فى مختلف فروع القانون الدولي التقليدي والعرفي، تغطي العديد من الجوانب والاستخدامات والعواقب لتكنولوجيا المعلومات والاتصالات، كما هو الحال مع التقنيات الأخرى. فيما يلي، نؤسس أولاً قابلية التطبيق من بعض تلك الواجبات تجاه تكنولوجيا المعلومات والاتصالات. ثم نتعمق أكثر فى المدى الذي تتطلب فيه هذه الواجبات من الدول منع ووقف وتعويض الأضرار على الإنترنت.

---

1 Pisillo-Mazzeschi, *supra* note 14, at 31–34, citing *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States)*, Judgment, 27 June 1986, ICJ Reports (1987) 14, para. 157 (finding that the United States was responsible for actively supporting the Contras, thus breaching its duty to abstain from such support, whereas Nicaragua was responsible for tolerating arms traffic, thus breaching its due diligence duty to protect).

2 ILC, Draft Articles on Prevention, *ibid* 21, at 159, Commentary to art. 8, para. 2; 169, Commentary to art. 11, para. 1.

3 e.g., Human Rights Committee (HRComm), General Comment No. 36 on Article 6 of the International Covenant on Civil and Political Rights, on the Right to Life, CCPR/C/GC/36, 30 October 2018, §§ 25,28–30; European Court of Human Rights (ECtHR), Guide on Article 2 of the European Convention on Human Rights: Right to Life, updated on 31 December 2019, para. 101.

4 e.g., Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts 1977, 1125 UNTS 3, arts 57–58 (Additional Protocol I); International Committee of the Red Cross (ICRC), Customary IHL Database, Rule 15, available at https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule15.

المطلب الثاني

المقصود بالفضاء السيبراني

بينما يعرف (kybernetes)[1] يشير مصطلح السيبرانية في اللغة إلى) القيادة والتحكم عن بعد) وهو مشتق من الكلمة اليوناني. جانب من المتخصصين الهجمات السيبرانية بأنها: تلك الإجراءات التي تتخذها الدولة من اجل الهجوم على نظم المعلومات للعدو ويهدف) التأثير والأضرار به، والدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة).[2]

عَرف الفضاء السيبراني بأنه المجال أو البيئة الافتراضية التي تتشكل من تفاعل كل من العناصر المادية المتمثلة في البنية التحتية الالكترونية، شبكة الانترنت والخوادم المركزية وغير المادية، ويمكن من خلالها التواصل بين أجزاء مختلفة من العالم عبر الشبكات الالكترونية.[3]

في حين عرفت الوكالة الفرنسية لأمن المنظومة الإعلامية، الفضاء السيبراني بأنه: مجال افتراضي عالمي، يتيح تداول المعلومات المختلفة، والذي يتكون من البنية التحتية التكنولوجية، المتمثلة في أجهزة الحاسب الألي شبكات الانترنت، والمكون البشري المسؤول عن تشغيلها والتحكم فيها.[4]

أيضاً عرّف دليل "تالين2 " لعام 2017 بأنه بيئة الكترونية تتشكل نتيجة التفاعل بين طبقات مادية ومنطقية، واجتماعية، تتمثل الطبقة المادية في عناصر شبكة الاتصالات، أي الأجهزة والبنية التحتية الأخرى، كالكابلات وأجهزة التوجيه، وأجهزة الكمبيوتر، وتتمثل الطبقة المنطقية في الاتصالات التي تتم بين أجهزة الشبكة.[5]

أما الهجوم السيبراني: فقد نصت القاعدة رقم (30) من دليل تالين (1) والقاعدة رقم (92) من دليل تالين (2) على أنه " عملية إلكترونية هجومية أو دفاعية، يتَّوقع وفقاً للمجرى العادي للأور أن تتسبب في أضرار جسيمة كإصابة، أو موت أشخاص، أو تلف، أو تدمير أشياء.[6]

خلال مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين، تم تطوير تعريفين ضمن ورشة عمل حول الجرائم الإلكترونية[1] بالمعنى الضيق (جرائم الكمبيوتر) لتغطي أي سلوك غير قانوني موجه بواسطة العمليات الإلكترونية التي تستهدف أمن أنظمة

---

[1] د. احمد عبيس نعمة الفتالوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، جامعة بابل– كلية القانون، العدد الرابع، السنة الثامنة، 2199 ،ص999.

[2] M. XINMIN, Letter to the Editors: What Kind of Internet Order Do We Need? 14 Chinese Journal of International Law, 2015, PP. 399: 402

[3] Oxford English Dictionary Online, Cyberspace Oxford University Press November 2010, available at: https://www.oxfordlearnersdictionaries.com/definition/english/cyberwarfare (Last visit March 2022)

[4]) T. PLOUG, Ethics in Cyberspace: How Cyberspace May Influence Interpersonal Interaction, 1st. edn., Springer, 2009, P. 70

[5] وذلك بما يشمل التطبيقات ، والبيانات ، والبروتكولات التي تساعد في عمليات تبادل البيانات.
M. N. SCHMITT, L. VIHUL, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, P. R., P. 12

[6] الهجوم الإلكتروني هو عملية إلكترونية ، سواء كانت هجومية أو دفاعية ، من المتوقع بشكل معقول أن تتسبب في إصابة الأشخاص أو موتهم أو إلحاق ضرر أو تدمير للأشياء. راجع
Rule No. (92) Of the Tallinn Manual 2:

(ISSN: 2356 - 9492)

الكمبيوتر والبيانات التي تعالجها. وتغطي الجرائم الإلكترونية بمعناها الأوسع (الجرائم المتعلقة بالكمبيوتر) بمعنى أي سلوك غير قانوني يُرتكب عن طريق نظام أو شبكة كمبيوتر أو فيما يتعلق به، بما في ذلك جرائم مثل الحيازة غير القانونية وتقديم المعلومات أو توزيعها عن طريق نظام أو شبكة كمبيوتر.[2]

المطلب الثالث

الأفعال التي تشكل انتهاك للسيادة في الفضاء السيبراني

إذا كانت العملية التي تقوم بها دولة ما لا تضر بحقوق الدولة المستهدفة، فسيكون من غير المناسب فرض شرط على الدولة الضالعة فى الهجوم لوضع حد للعملية. لذلك، خلص الخبراء إلى أن التزام العناية الواجبة لا ينطبق إلا عندما ترقى العملية الإلكترونية المعنية إلى حد فعل غير مشروع دوليًا. على سبيل المثال، إذا كانت الدولة "أ" تراقب قواعد البيانات الحكومية للدولة "ب" فى عمل من أعمال التجسس الإلكتروني من خلال استخدام البنية التحتية الإلكترونية فى الدولة "ج"، فلا تتحمل الدولة "ج" أي التزام بالعناية الواجبة لإنهاء عمليات الدولة "أ" لأن التجسس فى حد ذاته لا يشكل فعل غير قانوني بموجب القانون الدولي وذلك بموجب القاعدة (القاعدة 32) من دليل تالين.

واتفق الخبراء كذلك على أن التزام العناية الواجبة ينطبق فقط على الدولة عندما تكون العملية الإلكترونية التي يتم شنها من أراضيها أو عبرها غير قانونية بموجب القانون الدولي إذا كانت قد نفذتها الدولة.

فى الحالات التي يكون فيها السلوك المخالف ينتهك التزامًا تدين به الدولة القائمة بالتصرف تجاه الدولة المستهدفة، فإن فرض التزام العناية الواجبة على الدولة من شأنه أن يرقى فعليًا إلى مطالبتها بإنفاذ الالتزامات القانونية التي لا تلتزم بها[3]. لا ينشأ هذا الوضع إلا فى حالة الالتزامات التعاهدية الثنائية أو المتعددة الأطراف لأن القانون الدولي العرفى ملزم لجميع الدول.[4]

على سبيل المثال، النظر فى اتفاقية دولية ثنائية تلزم الدول (أ) و (ب) الامتناع عن إجراء عمليات تجسس ضد بعضهما البعض. تستخدم الدولة "أ" البنية التحتية الإلكترونية فى الدولة "ج" للانخراط فى التجسس ضد الدولة "ب "بطريقة لا تنتهك القانون الدولي بطريقة أخرى. فالدولة "ج" ليست ملزمة بإنهاء العملية على أساس هذه القاعدة لأنها ليست طرفًا فى الاتفاقية الثنائية ولأن التجسس بحد ذاته لا ينتهك القانون الدولي بحسب القاعدة 32 من دليل تالين.[5]

الاستغلال فى الفضاء السيبراني والقانون الدولي

---

[1] راجع

6 Crimes related to computer networks, Background paper for the workshop on crimes related to the computer network, 10th UN Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.187/10, page 5; available at: www.uncjin.org/Documents/congr10/10e.pdf.

[2] انظر:

Kumar, Anupa P. "Cyber law: A view to social security." *Bangalore, India* (2009)., page 29

[3] Sicilianos, Linos-Alexander. "The classification of obligations and the multilateral dimension of the relations of international responsibility." *European Journal of International Law* 13.5 (2002): 1127-1145.

[4] Baxter, Richard R. "Multilateral treaties as evidence of customary international law." *Brit. YB Int'l L.* 41 (1965): 275.

[5] Jensen, Eric Talbot. "Cyber sovereignty: The way ahead." *Tex. Int'l LJ* 50 (2015): 275.

فـى المعجـم السـيبراني، يُعـرِّف المعهـد الـوطني للمعـايير والتكنولوجيـا الثغـرة الأمنيـة بأنهـا "ضـعف فـى نظـام المعلومـات، أو إجـراءات أمـان النظـام، أو الضـوابط الداخليـة، أو التنفيـذ الـذي يمكـن اسـتغلاله أو بـدء تشـغيله بواسـطة مصـدر تهديـد ". لاحظـت شـركات الأمـن السـيبراني، مثـل TrendMicro، أن الاسـتغلال يشـير إلـى "الاسـتفادة مـن الضـعف البرمجـي أو الخلـل الأمني. "[1]

مـاذا عـن الاسـتغلال؟ يعـرّف هيـرب لـين الاسـتغلال السـيبراني فـى سـياق تجسـس بأنـه "عمـل هجـوم إلكترونـي يـتم إجـراؤه بغـرض الحصـول علـى المعلومـات". وهـى إجـراءات [تشـمل] أنشـطة الاسـتخبارات العسـكرية، والمنـاورة، وجمـع المعلومـات، وغيرهـا مـن الإجراءات التمكينية المطلوبة للاستعداد لمستقبل العمليات العسكرية."[2]

فـى هـذا السـياق، يجـب فهـم الاسـتغلال السـيبراني بشـكل عـام علـى أنـه دولـة واحـدة تسـتخدم رمـزًا للاسـتفادة مـن نقـاط الضـعف السـيبرانية للآخـرين بغـرض اكتسـاب مميـزات اسـتراتيجية. فـى الواقـع ، يشـير كـورن إلـى أن اسـتغلال روسـيا الأولـي لخـوادم اللجنـة الوطنيـة الديموقراطيـة أعقبـه سـرقة الاتصـالات الحساسـة ، والتـي تـم اسـتخدامها بعـد ذلـك فـى حملـة معلومـات اسـتراتيجية لتقويض الثقة فى العملية الانتخابية الأمريكية.[3]

المطلب الرابع

الخلاف حول طبيعة الالتزام الدولي ببذل العناية الواجبة فى الفضاء السيبراني

يكمن جوهر تلك القاعدة فى مبادئ القانون الدولي العام التي تلزم الدول بممارسة العناية الواجبة لضمان عدم استخدام إقليمها أو المرافق الخاضعة لسيادتها لإلحاق الضرر بالدول الأخرى.[4]

[1] انظر:

Kissel, Richard, ed. *Glossary of key information security terms*. Diane Publishing, 2011.

[2] راجع:

Lin, Herbert. "Cyber conflict and international humanitarian law." *International Review of the Red Cross* 94.886 (2012): 515-531.

[3] راجع :

P. Fischerkeller, M. (2021, August 31). *Current international law is not an adequate regime for Cyberspace*. Lawfare. Retrieved March 23, 2022, from https://www.lawfareblog.com/current-international-law-not-adequate-regime-cyberspace

[4] راجع:

United States v. Arjona, 120, US 479, 483 (1887); Lotus judgment, at 88 (Mo, - dissenting); Island of Palmas arbitral award, at 839; Corfu Channel judgment, at Secretary-General, Survey of International Law in Relation to the Work of CodifxcaOct * the International Law Commission, para. 57, UN Doc. A/CN.4/1/Rev.l (1 February Permanent Mission of the Federal Republic of Germany to the United Nations, Gce » appreciation of the issues of information security, at 4, Note No. 516/2012; Development* in the Field of Information and Telecommunications in the Context of Inte Security, Report of the Secretary-General, at 9, UN Doc. A/68/156 Add. 1 (9 S: 2013) (Ger.). See also Tehran Hostages judgment, paras. 67-68; Nicaragua y para. 157.

(ISSN: 2356 - 9492)

ويشار لهذا المبدأ " العناية الواجبة"، حيث إن هذا المصطلح الأكثر استخدامًا فيما يتعلق بالتزام الدول بمراقبة الأنشطة على أراضيها، فهو معيار السلوك المتوقع من الدول عند الامتثال لهذا المبدأ الذي تنعكس قواعده فى العديد من فروع القانون الدولي.[1] فهو التزام ينبع من مفهوم السيادة، ويتطلب من الدولة "حماية حقوق الدول الأخرى داخل أراضيها"[2]

حيث نظمت القاعدة السادسة من قواعد تالين للفضاء السيبراني واجب الدولة فى ممارسة العناية الواجبة، ومفاد هذا الالتزام عدم السماح باستخدام أراضيها أو البنية التحتية الإلكترونية الخاضعة لسيطرتها الحكومية فى العمليات الإلكترونية التي تؤثر على حقوق الدول الأخرى وتؤدي إلى عواقب وخيمة.

أقر فريق الخبراء الدولي بوجهة نظر، مفادها أن مبدأ العناية الواجبة العام، وبالتالي تطبيقه فى سياق العمليات السيبرانية، لم يحقق حالة القانون واجب النفاذ. وإن كان المدافعون عن هذا المبدأ متمسكين بدعوة مجموعة الخبراء الحكوميين التابعة للأمم المتحدة (UN GGE) للدول "بضرورة" أن تمتثل لهذا لمبدأ، بغض النظر عن الخلاف حول الالزام القانوني من عدمه.[3]

وتري لجنة الخبراء كذلك إلى أن مبدأ العناية الواجبة المتجذر منذ فترة طويلة فى الفقه هو مبدأ عام تم تحديده فى الأنظمة المتخصصة للقانون الدولي، وقد أقرت فرق الأمم المتحدة الحكومية نفسها بأن مبادئ القانون الدولي التي "تنبع" من مبدأ السيادة ملزمة فى السياق السيبراني.[4]. نظرًا لأن التقنيات الجديدة تخضع لقواعد القانون الدولي الموجود مسبقًا مالم يتم استبعادها بنص قانوني. ومن ثم انتهت لجنة الخبراء إلى أن مبدأ العناية الواجبة ينطبق فى السياق السيبراني، ويشار إليه أيضًا بمبدأ العناية الواجبة على أنه " واجب اليقظة "، أو " واجب المنع ".

تبنت مجموعة الخبراء الدولية مصطلح "العناية الواجبة" فى ضوء انتشار استخدامه، لكنه وافق على أنه يمكن اعتباره مرادفًا لمصطلح "التزام اليقظة".[5] ومع ذلك، رفض فريق الخبراء الدولي استخدام مصطلح "التزام المنع" لأن الخبراء اتفقوا على أن مبدأ العناية الواجبة لا يشمل فرض اتخاذ خطوات وقائية مادية لضمان عدم استخدام أراضي الدولة لانتهاك هذا المبدأ.[6]

---

[1] راجع:

Group on Due Diligence in International Law: First Report, 7 March 2014. In inter- -national environmental law,

راجع أيضا:

Alabama Claims Arbitration (the United States/Great Britain) 29 RIAA 125, 129 (1872) (describing the requirement of due diligence in various contexts); Declaration of the United Nations Conference on the Human Environment, prin. 21, Doc. A/CONF.48/14 (1972); Rio Declaration on Environment and Development, rnn. 2, UN Doc. A/CONF.151/26/Rev.l (Vol. I), Annex I (12 August 1992); Nuclear 'Weapons advisory opinion, para. 29.

[2] أشارت إليه محكمة العدل الدولية في قضية قناة كورفو، الذي يلاحظ أن "من واجب كل دولة ألا تسمح عن علم باستخدام أراضيها لأعمال تتعارض مع حقوق الدول الأخرى"

Tsagourias, Nicholas. "Cyber-attacks, self-defense and the problem of attribution." *Journal of conflict and security law* 17.2 (2012): 229-244.

[3] راجع:

Gaichiri, Mary N. The Role of the United Nations in Dealing with Cyber Insecurity (2007-2017). Diss. United States International University-Africa, 2019.

[4] ثمة توافق على أن تعليقات فريق الخبراء الحكوميين لا تدحض بشكل قاطع وجود مثل هذا المبدأ. ففي الواقع، ينبع بذل العناية الواجبة من مبدأ السيادة، راجع:

Barnidge, Robert. "The due diligence principle under international law." International Community Law Review 8.1 (2006): 81-121.

[5] راجع:

Liu, Ian Yuying. "State responsibility and cyberattacks: Defining due diligence obligations." Indon. J. Int'l & Comp. L. 4 (2017): 191.

[6] راجع:

Bannelier, Karine. "Cyber diligence: a low-intensity due diligence principle for low-intensity cyber operations?" Baltic yearbook of international law 14 (2014).

وفى هذا الصدد، لاحظ فريق الخبراء الدولي أن القانون الدولي يحتوي على قواعد أولية معينة، الهدف منها بالذات هو منع حدوث سلوك معين. والمثال النموذجي هو واجب منع الإبادة الجماعية.[1] بيد أنه، لا يتم الاستدلال على هذه الالتزامات من المبدأ العام للعناية الواجبة، لأنها تمثل التزامات أولية منفصلة. على النقيض من ذلك، لا يوجد مثل هذا الالتزام الأساسي المتميز فيما يتعلق بالعمليات السيبرانية الضارة فى حد ذاتها.[2]

تفترض هذه القاعدة مشاركة ثلاثة أطراف على الأقل: (1) الدولة المستهدفة من العملية الإلكترونية؛ (2) الدولة موضوع القاعدة؛ و (3) طرف ثالث هو الجهة المحركة للهجوم الإلكتروني.[3] تنطبق القواعد على أي عملية إلكترونية لطرف من الغير، بغض النظر عما إذا كان يتم تنفيذها بواسطة شخص خاص، أو شركة، أو مجموعة غير حكومية، أو دولة.[4]

التزام العناية الواجبة ينطبق فى جميع أنحاء اقليم الدولة الخاضع لسيادتها، وهي تشمل أي بنية تحتية إلكترونية مستخدمة، وكذلك الأشخاص الذين ينفذون، عمليات إلكترونية فى تلك المنطقة.[5]

لاحظ أن الطرف الذي يبدأ العملية الإلكترونية المعنية قد يعمل عن بعد من دولة أخري. على سبيل المثال، ضع فى اعتبارك مجموعة من المتسللين تتمركز فى الدولة "أ" لتنفذ عملية إلكترونية مدمرة ضد الدولة "ب "باستخدام البنية التحتية الإلكترونية الموجودة فى الدولة "ج". إذا علمت الدولة "ج" بالاستخدام المذكور وفشلت فى اتخاذ تدابير مجدية لوضع حد للعملية، فإنها تنتهك مبدأ العناية الواجبة.

ومن ثم نجد أنه فى الفضاء السيبراني، تفرض على الدول بذل قصارى جهدها لمنع ووقف ومعالجة مجموعة من الأضرار السيبرانية المعروفة أو المتوقعة الناشئة عن أراضيها أو العابرة لها، بغض النظر عمن تسبب فيها أو قام بها فعلياً. على سبيل المثال، أثناء جائحة COVID-19، طلبت الدول الأعضاء فى الاتحاد الأوروبي من كل دولة ممارسة العناية الواجبة واتخاذ الإجراءات المناسبة ضد الجهات الفاعلة التي تنفذ [عمليات إلكترونية خبيثة] انطلاقاً من أراضيها، بما يتفق وأحكام القانون الدولي.[6]

---

[1] راجع

Milanović, Marko. "State responsibility for genocide." European Journal of International Law 17.3 (2006): 553-604.

[2] وهذا هو الأرجح فيما يتعلق بتطبيق مبدأ العام للعناية الواجبة في السياق السيبراني

Patrick, Colin. "Debugging the Tallinn Manual 2.0's Application of the Due Diligence Principle to Cyber Operations." Wash. Int'l LJ 28 (2019): 581.

[3] Hathaway, Oona A., et al. "The law of cyber-attack." Calif. L. Rev. 100 (2012): 817.

[4] Solomon, Jonathan. Cyperdeterrence Between Nation-States: Plausible Strategy Or A Pipe Dream?. SYSTEMS PLANNING AND ANALYSIS INC ALEXANDRIA VA, 2011.

[5] Schmitt, Michael N. "In Defense Of Due Diligence In Cyberspace." Yale LJF 125 (2015): 68. Liu, Ian Yuying. "State Responsibility And Cyberattacks: Defining Due Diligence Obligations." Indon. J. Int'l & Comp. L. 4 (2017): 191.

[6] انظر:

Council of the European Union, Press Release, 'Declaration by the High Representative Josep Borrell, on Behalf of the European Union, on Malicious Cyber Activities Exploiting the Coronavirus Pandemic' (30 April 2020), available at :www.consilium.europa.eu/en/press/press-releases/2020/04/30/declarationby-the-high representative-josep-borrell-on-behalf-of-the european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/. A similar statement was made by the European Union and endorsed by member states during the UN Security Council Arria-Formula Meeting on Cyber Stability and Conflict Prevention and Capacity Building:

راجع:

Pawel Herczynski, Statement on behalf of the European Union (20 May 2020), at 2, available at:

(ISSN: 2356 - 9492)

مـع ذلـك، لا يـزال الجـدل قائمـا حـول مـا إذا كانـت الـدول ملزمـة بالتصـرف بجديـة فـى الفضـاء السـيبراني، وهـو مجـال نشـاط الدولة الذي يشمل تكنولوجيا المعلومات والاتصالات (ICT) التي لها أبعاد اقتصادية وتشريعية وسياسية.[1]

مـن ناحيـة أخـرى، يشـير تقريـر عـام 2015 الصـادر عـن فريـق الخبـراء الحكـوميين التـابع للأمـم المتحـدة بشـأن تعزيـز سـلوك الدولـة المسـؤول فـى الفضـاء السـيبراني فـى سـياق الأمـن الـدولي (المشـار إليـه فيمـا يلـي بـ "GGE") ، والـذي تـم اعتمـاده بالإجمـاع مـن قبـل الجمعيـة العامـة للأمـم المتحـدة[2] ، إلـى أن الـدول " يجـب ألا يسـمحوا عـن علـم باسـتخدام أراضـيهم فـى الأفعـال غيـر المشـروعة دوليًـا ذات الصـلة بتكنولوجيـا المعلومـات والاتصـالات.[3] حيـث تـم صـياغة التقريـر بشـكل صـريح علـى أنه "معيار طوعي وغير ملزم" لسلوك الدولة المسؤول فى الفضاء الإلكتروني.

مـن ناحيـة أخـرى، اتفـق فريـق الخبـراء المشـاركين فـى الإصـدار الثـاني مـن دليـل تـالين بشـأن القـانون الـدولي المطبـق علـى العمليـات الإلكترونيـة (المشـار إليـه فيمـا يلـي باسـم "دليـل تـالين") علـى أن قاعـدة عامـة أو مبـدأ مـن هـذا النـوع موجـود بالفعـل فـى القانون الدولي العرفي، وينطبق فى الفضاء السيبراني.[4]

حيـث تتطلـب القاعـدة السادسـة مـن الـدليل `` ممارسـة العنايـة الواجبـة فـى عـدم سـماح الـدول باسـتخدام أراضـيها أو البنيـة التحتيـة الإلكترونيـة الخاضـعة لسـيطرتها الحكوميـة فـى العمليـات الإلكترونيـة التـي تـؤثر علـى حقـوق الآخـرين وتـؤدي إلـى عواقب وخيمة ".

---

https://vm.ee/sites/default/files/Estonia_for_UN/20_05_22_arria_cyber_eu_statement_as_delivered_unread_paras.pdf.

راجع:

e.g., Mona Juul, Ambassador, Joint statement from Denmark, Finland, Iceland, Sweden and Norway at the Arria-Meeting on Cyber Stability and Conflict Prevention (22 May 2020), available at *www.norway.no/en/missions/UN/ statements/security- council/2020/arria-cyber-stability-and-conflict-prevention.*

Coco, Antonio, and Talita de Souza Dias. "'Cyber Due Diligence': A Patchwork of Protective Obligations in International Law." *European Journal of International Law* 32.3 (2021): 771-806.

راجع:

Delerue, François. "Covid-19 and the Cyber Pandemic: A Plea for International Law and the Rule of Sovereignty in Cyberspace." *2021 13th International Conference on Cyber Conflict (CyCon)*. IEEE, 2021.

The Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector, available at: https://elac.web.ox.ac.uk/the-oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-hea (last visited 10 July 2021).

[1] راجع في ذلك:

Sullivan, 'The 2014 Sony Hack and the Role of International Law', 8 *Journal of National Security Law and Policy* (2015) 437, at 454 n.88. See also Tsagourias, 'The Legal Status of Cyberspace', in N. Tsagourias and R. Buchan (eds), *Research Handbook on International Law and Cyberspace* (2015) 13; Johnson and Post, 'Law and Borders: The Rise of Law in Cyberspace', 48 *Stanford Law Review* (1996) 1367.

[1] راجع في ذلك:

'Law and Borders: The Rise of Law in Cyberspace', 48 *Stanford Law Review* (1996) 1367.

[2] راجع في ذلك:

GA Res. 70/237, 30 December 2015, §§ 1–2(a).

[3] راجع في ذلك:

Report of the Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/70/174, 22 July 2015, § 13(c) ('UN GGE Report 2015') (emphasis added).

[4] راجع في ذلك:

M. Schmitt (ed.), Tallinn Manual 2.0 (2nd ed. 2017) 30, rule 6; 43, rule 7 (hereinafter Tallinn Manual 2.0).

الالتزام الدولي ببذل العناية الواجبة في الفضاء السيبراني
بين التدابير الرادعة ومنع الأضرار السيبرانية العابرة

د. أسامة حمزة محمود عبد الفتاح

مجلة الدراسات القانونية والاقتصادية

نحن ندعي أن النقاش الحالي يتجاهل جوهر المشكلة من خلال التركيز كثيرًا على معنى "العناية الواجبة" وإمكانية تطبيقها على الفضاء الإلكتروني. وقد أدى ذلك إلى ظهور، وجهتي نظر متناقضتين بين وجود تلك العناية بشكل ملزم أو عدم وجودها على الإطلاق.

يكمن جوهر تلك القضية فى توافق فى الآراء بشأن ما هي "العناية الواجبة فى السياق السيبراني" أو إيجاد حل لسد تلك الفجوة القانونية فى الحماية، وإلا لن يكون ثمة التزامات على عاتق الدول، ولكن تعهدات طوعية فقط للتصرف بجد فى استخدامهم لتكنولوجيا المعلومات والاتصالات. [1]

[1] راجع في ذلك كل من:

Jensen and Watts are cautious about the legal basis of this rule, recognizing its advantages but also warning about its drawbacks. See Jensen and Watts, 'A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?', 95 *Texas Law Review* (2017) 1555, at 1568–1575.

راجع أيضا:

L. Adamson, 'Recommendation 13(c)', in United Nations Office of Disarmament Affairs, *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary* (2017) 49, at 55, § 12.

أبدت مجموعة من الدول شكوك حول تلك القاعدة:

Argentina, Statement at the2nd substantive session of the open-ended working group on developments in the field of information and telecommunications in the context of international security (hereinafter 'OEWG') (11 February2020), available at https://media.un.org/en/asset/k18/k18w6jq6eg (timestamp 02:15:05, hereinafter

راجع أيضا:

'Argentina's OEWG Statement'); Schondorf, 'Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations', *EJIL: Talk!* (9 December 2020), available at:

www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-theapplication- of international-law-to-cyber-operations/; and, albeit in a less clear-cut way, New Zealand, The Application of International Law to State Activity in Cyberspace (1 December 2020), § 17, available at https://dpmc.govt.nz/publications/application-international-law-state-activity-cyberspace; United Kingdom Mission to the United Nations, United Nations Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security: Application of International Law to States' Conduct In Cyberspace (3 June 2021), available at https://www.gov.uk/ government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement, para 10

(ISSN: 2356 - 9492)

المبحث الثاني
الخلاف حول قابلية تطبيق وإلزامية معيار بذل العناية الواجبة فى الفضاء السيبراني

تمهيد: -

على الرغم من أن محكمة العدل الدولية لم تتناول أبدًا بشكل مباشر إجراءات العناية الواجبة المتعلقة بالأمن السيبراني، إلا أن الحالات التي تناقش العناية الواجبة عمومًا يمكن أن تكون بمثابة إرشادات عامة للدول التي قد نستنتج منها التطبيقات الخاصة السيبرانية. وتجدر الإشارة إلى أن هذه الحالات نشأت جميعها قبل ظهور الهجمات الإلكترونية، ولكن بعض المبادئ التي تقوم عليها قد لا يزال لديها بعض التطبيقات التي يمكن الاستعانة بها فى تأصيل المبدأ فى الفضاء السيبراني، بما فى ذلك السوابق القضائية لمحكمة العدل الدولية قناة Corfu و Trail Smelter و Nicaragua). نحاول فيما يلي إلقاء الضوء علي طبيعة الخلاف حول قابلية تطبيق التزام بذل العناية الواجبة في الفضاء السيبراني ، ومدي إلزامية هذا المعيار انطلاقا من طبيعته القانونية فى القانون الدولى العرفى والسوابق القضائية الدولية.

المطلب الأول

الأمن السيبراني فى منظور القانون الدولي العرفى

فى ظل غياب نظام تعاهدي قوي وبالنظر إلى الصعوبات الجيوسياسية للتفاوض بشأن اتفاقيات جديدة فى هذا المجال، من الضروري توضيح دور القانون الدولي العرفى من حيث علاقته بالعناية الواجبة. فقد تم التعبير عن عنصر حيوي من عناصر القانون الدولي العرفى فى قضية محكمة العدل الدولية المرفوعة من نيكاراغوا ضد الولايات المتحدة.[1]

حيث رأت محكمة العدل الدولية أن الالتزامات الدولية العرفية ستنشأ من الممارسة المتسقة والواسعة النطاق للدول المتمثلة فى الانخراط فى أفعال أو امتناع عن أفعال محددة، يتم القيام بها انطلاقاً من الإحساس بالالتزام بأن مثل هذه الأفعال أو الامتناع عنها، مطلب بموجب القانون الدولي (الاعتقاد بالإلزام).

إن الجمع بين ممارسات الدول والاعتقاد بالإلزام، الذي يقوم به عدد كبير من الدول دون التنصل الصريح من جانب عدد كبير من الدول، من شأنه أن يؤدي إلى التزامات دولية بموجب القانون الدولي العرفي.

[1] حول تورط الولايات المتحدة في تمرد الكونترا في نيكاراغوا. (قضية نيكاراغوا 1986)
Chayes, Abram. "Nicaragua, the United States, and the World Court." *Colum. L. Rev.* 85 (1985): 1445.

الالتزام الدولي ببذل العناية الواجبة في الفضاء السيبراني
بين التدابير الرادعة ومنع الأضرار السيبرانية العابرة

د. أسامة حمزة محمود عبد الفتاح

مجلة الدراسات القانونية والاقتصادية

الأساس المنطقي هو أن هذا المزيج يعكس إجماعًا فى المجتمع الدولي على أن الإجراءات المتخذة تمثل التزامًا دوليًا غير معلن. اعتمادًا على نوع القاعدة المتضمنة، متي كانت ممارسات الدولة أكثر أو أقل انتشارًا. يثار الجدل حول أثر تلك الممارسات على المعايير الجديدة، مثل ما يتعلق بالأمن السيبراني.[1]

على الرغم من توضيح نيكاراغوا للقاعدة بشكل واضح، فإن تطوير القانون الدولي العرفي يمثل فى الممارسة معضلة زمنية، حيث إنه لكي تنخرط دولة ما فى أعمال انطلاقاً من إحساسها بالواجب القانوني، فإن هذا يفترض وجود مثل هذا الواجب، وبالتالي وجود القانون الدولي العرفي.[2]

للمساعدة فى حل هذه المعضلة، دعا البروفيسور فريدريك كيرجيس، ردًا على نيكاراغوا، إلى ما أسماه "النهج المتدرج"[3]. حيث يدعو البروفيسور كيرجيس بأنه يجب فهم ممارسات الدول والاعتقاد بالإلزام على نطاق واسع، حيث يزداد شرط الاعتقاد بالإلزام مع تناقص أدلة ممارسة الدول. بدلاً من فرض شروط صارمة على كل من ممارسة الدول والاعتقاد بالإلزام، حيث يدفع هذا نهج بأن وجود تاريخ قوي لممارسات الدول يمكن أن يؤدي إلى التزامات دولية فى غياب الاعتقاد بالإلزام، وأن الاعتقاد بالإلزام القانوني بالمثل يمكن أن يؤدي إلى التزامات دولية مع القليل من الأدلة من الممارسات الدولية التي تتفق مع ذلك.

قد يكون هذا النهج بالغ الأهمية بشكل خاص ضمن نطاق الأنشطة السيبرانية، حيث ظهرت هذه التقنيات الجديدة[4] بسرعة كبيرة للغاية بحيث لم تظهر أدلة على ممارسة الدول على نطاق واسع، ومع ذلك قد تظل الآراء القانونية المقنعة قائمة كأساس للالتزامات الدولية.

تم التعبير عن عنصر حيوي من عناصر القانون الدولي العرفي فى قضية محكمة العدل الدولية (نيكاراغوا ضد الولايات المتحدة)، والتي تضمنت نزاعًا حول تورط الولايات المتحدة فى تمرد الكونترا فى نيكاراغوا[5]. ففى تلك القضية، رأت محكمة العدل الدولية أن الالتزامات الدولية العرفية ستنشأ من الممارسة المتسقة والواسعة النطاق للدول المتمثلة فى الانخراط فى

---

[1] يحيث يكون المعيار بشكل عام "موحدًا تقريبًا" وفقا للممارسات الدولية. لمزيد من التفاصيل، راجع قضية نيكارغوا
N. Sea Continental Shelf (F.R.G./Den. v. Neth.), 1969. I.C.J. 41, 72 (Feb. 20).

[2] Bradley, Curtis A. 2013. The chronological paradox, state preferences, and Opinio Juris. Duke law. http://law.duke.edu/cicl/pdf/opiniojuris/panel_1-bradley-the_chronological_paradox,_state_ preferences, _and_opinio_juris.pdf. Accessed 26 Mar 2022.

[3] Kirgis, Frederic L. 1987. Custom on a sliding scale. The American Journal of International Law 81(1): 146–151. P 118

[4] مثل الشبكات الخاصة الافتراضية (VPNs) وغيرها من برامج انتحال بروتوكول الإنترنت (IP)، تلك الآليات التي ضاعفت مشكلة الإسناد انظر:
Buchan, 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm', 21 *Journal of Conflict & Security Law* (*JCSL*) (2016) 429, at 432.

[5] راجع :
Nicaragua v. US, 1986 I.C.J. Rep. 101 (1986)

(ISSN: 2356 - 9492)

أفعال أو امتناع عن أفعال محددة، يتم إجراؤها انطلاقاً من الإحساس بالالتزام بأن مثل هذه الأفعال أو الامتناع عن العمل مطلوبة بموجب القانون الدولي (الاعتقاد بالإلزام).

وإن الجمع بين ممارسات الدول والاعتقاد بالإلزام، الذي يقوم به عدد كبير من الدول دون التنصل الصريح من جانب عدد كبير من الدول، من شأنه أن يؤدي إلى التزامات دولية بموجب العرف الدولي.

الأساس المنطقي هو أن يعكس هذا المزيج إجماعًا فى المجتمع الدولي على أن الإجراءات المتخذة تمثل التزامًا دوليًا غير معلن. ونظراً لكون ممارسات الدول قليلة نسبياً فى السياق السيبراني، نجد أن هناك صعوبات فى إنشاء معايير عامة وموحدة وملزمة.

على الرغم من توضيح نيكاراغوا للقاعدة بشكل واضح، فإن تطوير القانون الدولي العرفي يمثل فى الممارسة معضلة زمنية، حيث إنه لكي تنخرط دولة ما فى أعمال انطلاقاً من إحساسها بالواجب القانوني، فإن هذا يفترض وجود مثل هذا الواجب، وبالتالي وجود القانون الدولي العرفي[1].

ومع ذلك، فإن إثبات الاعتقاد بالإلزام يعد مهمة صعبة، لا سيما فى عالم الإنترنت، حيث يقترح جانب من الفقه، أن تكون هذه المبادئ العامة متأصلة بالمعاهدات الدولية متعددة الأطراف، والتي تدل على وجود اتفاق واسع النطاق بين الدول، وفى الواقع تعتمد معظم المحاكم على المعاهدات لتحديد مدى الاعتقاد بالإلزام.[2]

ومع ذلك، ضمن سياق الفضاء السيبراني، ركزت المعاهدات حتى الآن إلى حد كبير على تنفيذ قوانين الجرائم الإلكترونية الوطنية، ولم تفعل سوى القليل نسبيًا لمعالجة معايير الأمن السيبراني على الصعيد العالمي، مع ترك الساحة خالية للقرارات الصادرة من للقطاع الخاص[3].

بينما من غير المحتمل أن تلتزم دولة غير موقعة على المعاهدة بالأحكام المحددة – لا سيما على المدى القصير – قد تظل تلك المعاهدة تعمل على تحديد المبادئ العامة التي تسترشد بالإلزام القانوني، وبالتالي يمكنها أن تشكل الأساس للالتزامات الدولية الناشئة.

[1] راجع

Bradley, Curtis A. 2013. The chronological paradox, state preferences, and Opinio Juris. Duke law. http://law.duke.edu/cicl/pdf/opiniojuris/panel_1-bradley-the_chronological_paradox,_state_ preferences, _and_opinio_juris.pdf. Accessed 26 Mar 2021.

[2] تجعل المعضلة الزمنية الإشارة إلى القواعد الحالية أمرًا معقدًا، لذا فإن الطريقة المفضلة هي تحديد المبادئ العامة. راجع:

Gulati, Mitu. "How do courts find international custom." *Duke Law* (2013).

[3] على سبيل المثال، اتفاقية بودابست، واتفاقية الاتحاد الأفريقي التي تتمحور حول الأمن السيبراني وحماية البيانات، أيضاً مختلف مجموعات العمل التابعة لرابطة أمم جنوب شرق آسيا المعنية بالجرائم الإلكترونية، التي يمكن أن تعمل كمصادر مفيدة لممارسات الدول في سن قوانين الجرائم الإلكترونية وإنفاذها داخل أراضيها والتعاون في مقاضاة المجرمين في الجرائم السيبرانية وتسليمهم. ومع ذلك، غالبًا ما تفتقر هذه الاتفاقيات إلى لغة ملزمة. بالمثل، شجعت منظمة الدول الأمريكية أيضًا الدول الأعضاء على الانضمام إلى اتفاقية بودابست وتكثيف التعاون الإقليمي للتخفيف من الجرائم الإلكترونية، في حين أن قرار الجمعية العامة للأمم المتحدة غير الملزم يدعو الدول إلى "القضاء على الملاذات الآمنة" لمجرمي الإنترنت. راجع (قرار الجمعية العامة 55) / 63 ، 2001).

General Assembly resolution 55/63, Combatting the criminal use of information technologies, A/ RES/55/63 (22 Jan 2001). http://www.itu.int/ITUD/cyb/cybersecurity/docs/UN_resolution_55_63.pdf. Accessed 26 Mar 2021

الالتزام الدولي ببذل العناية الواجبة في الفضاء السيبراني
بين التدابير الرادعة ومنع الأضرار السيبرانية العابرة

د. أسامة حمزة محمود عبد الفتاح

مجلة الدراسات القانونية والاقتصادية

ومما يزيد من تعقيد البحث عن أدلة على الاعتقاد بالإلزام، الاستخدام الواسع النطاق للنشاط السيبراني الذي ترعاه الدولة، من التجسس الإلكتروني إلى الجريمة الإلكترونية. فى حين أن تصنيف الأنشطة السيبرانية للدولة يعد مشكلة أخري، فإن مجرد حقيقة أن هذه الأنشطة منتشرة على نطاق واسع يشير إلى عدم وجود الاعتقاد بالإلزام السيبراني طالما لم يعد النشاط العدواني للدولة هجوماً مسلحاً. وقد تم تعزيز ذلك من خلال مناقشة دليل تالين للقانون الدولي المتعلق بالتجسس ووضعه القانوني.[1] وبالمثل، فإن ممارسات الأمن السيبراني متغيرة للغاية، ويمكن أن تنطوي على تثبيت خفي للبرامج الضارة[2]. بالنظر إلى النقص النسبي فى المواثيق الدولية متعدد الأطراف، فإن الادعاء بوجود إجماع واسع النطاق على مبدأ أساسي للأمن السيبراني سيكون أمرًا صعبًا فى هذا المجال.

فعلى الرغم من اتفاق الدول بشكل متزايد على أن القانون الدولي، وتحديداً ميثاق الأمم المتحدة وقواعد القانون الدولي العرفي (CIL) المستمدة من مبادئ الميثاق، تنطبق على الفضاء الإلكتروني. ومع ذلك، كلاهما غير مناسب للأنشطة السيبرانية. فالميثاق يعكس تحيزًا تجاه ما تم تسميته بالبيئة التقليدية للمنازعات الدولية، كما تطورت قواعد العرف الدولي فى ظل كل من البيئات التقليدية والنووية. فى هذه البيئات، تهدد الدول الاستقرار الدولي من خلال السعي لتحقيق مكاسب استراتيجية إما بالقسر أو باستخدام القوة الغاشمة.

فى حين تختلف البيئة الإستراتيجية الإلكترونية، من حيث التهديدات التي تتعرض لها الدولة الضحية، والتي تتبع من الاستغلال، أي أن الدول تستغل نقاط الضعف السيبرانية لدى تلك الدول بغرض تحقيق مكاسب إستراتيجية.

لا ينبغي أن يكون مفاجئًا إذن أن الدول قد كافحت لتقديم رأي قانوني شامل ومتعمق حول كيفية تطبيق القانون الدولي فى السياق السيبراني. ويبقي الجهد الدولي لتأصيل قواعد حاكمة وملزمة، تتناسب مع السمات الأساسية للبيئة الاستراتيجية السيبرانية، وسلوكيات الدولة التي تلزمها، وكيف يمكن مواجهة تلك الأفضلية الاستراتيجية بشكل قانوني من خلال الممارسات الدولية.

الطبيعة الخاصة للمنازعات الدولية فى الفضاء السيبراني

يشكل الفضاء السيبراني ليس مجرد مجال، ولكنه بيئة إستراتيجية، والأهم من ذلك أنها تختلف عن البيئات الاستراتيجية التقليدية.[3] فالقانون الدولي بعد الحرب العالمية الثانية، وتحديداً بموجب ميثاق الأمم المتحدة، كان حريصاً على تجنيب

[1] Schmitt, Michael N. 2013. Tallinn manual on the international law applicable to cyber warfare. Cambridge: Cambridge University Press

[2] كما يزعم مقدمو الاتصالات الصينيون ووكالة الأمن القومي الأمريكية (NSA) على حد سواء
Gruener, Wolfgang. 2012. Many new PCs in China come with malware preinstalled. Tom's Hardware, September 24. http://www.tomshardware.com/news/microsoft-pc-windowssecurity-china,17758.html. Accessed 26 Mar 2021.

[3] في حين أن المجالات القتالية الأمريكية - الجوية والبرية والبحرية والفضائية - تصف العمليات العسكرية تشتمل البيئات الإستراتيجية "الفضائية" على الميزات الأساسية التي تحدد السلوكيات الأمنية للدول. وببساطة، فإن السمات الأساسية للبيئة النووية هي التقسيم، أي السمة التي تتجلى في شكل حدود إقليمية، وتكاليف لا جدال فيها (أي، لا يوجد دفاع صالح ضد الأسلحة النووية) ، مما يؤدي إلى سلوك إكراه مهيمن في شكل استراتيجية الردع (أي التدمير المؤكد المتبادل). تشتمل البيئة الإستراتيجية التقليدية أيضًا على التجزئة، ولكنها تقترن بتكاليف قابلة للجدل (يمكن الدفاع ضد القدرات التقليدية، على عكس الأسلحة النووية). يؤدي هذا إلى سلوكيات عرضية مهيمنة من القوة الغاشمة أو الإكراه، حيث يأخذ هذا الأخير شكل استراتيجية ردع تهدد بفرض تكاليف أو استراتيجية إجبار تفرض تكاليف من خلال الحرب التقليدية.

(ISSN: 2356 - 9492)

"الأجيال المقبلة ويلات الحرب"، حيث ترتكز قواعد سلوك الدول على السيادة، وعدم التدخل، والإكراه، والتهديد باستخدام القوة، والهجوم المسلح. حيث تختلف البيئة الإستراتيجية للفضاء الإلكتروني عن البيئات النووية والتقليدية، مما يشكل تحديًا لأهمية هذه القواعد.

وبالتالي، تواجه الدول حتمية أمنية تتمثل فى الاستمرار فى اقتناص المبادرة والحفاظ عليها لتهيئة الظروف الأمنية لصالحها فى الفضاء السيبراني ومن خلاله. يمكن للدول أن تفعل ذلك من خلال استراتيجيات وسياسات وأنشطة مختلفة تقلل من إمكانية استغلال نقاط ضعفها وتستغل نقاط ضعف الخصوم.

قد تقلل الدول من إمكانية استغلالها من خلال تدابير مواجهة داخلية، مثل أنظمة التصحيح والجدران النارية وكشف التسلل. سوف تستند التدابير التي تواجه الخارج فى المقام الأول على استغلال نقاط الضعف من جانب واحد. الأهم من ذلك، يتم تحفيز الدول على الاستغلال على نطاق واسع لأن القيام بذلك يمكن أن يؤدي إلى ميزة استراتيجية دون الإضرار بالبيئة بالضرورة.

والأهم من ذلك، يمكن للدول تحقيق ميزة استراتيجية – عبر اختلال ميزان القوة عالمياً– من خلال العمليات الإلكترونية المستمرة أو الحملات ذات الآثار التراكمية، فلا يمثل ذلك انتهاكًا للحظر المفروض على التهديد باستخدام القوة، ولا يعادل هجومًا مسلحًا بموجب المادة 51 من ميثاق الأمم المتحدة.

ومع ذلك، قد تظل هذه العمليات أو الحملات تعرض السلم والأمن الدوليين للخطر فى البيئة الإستراتيجية السيبرانية، حيث تحقق الدول ميزة إستراتيجية لا تحتاج إلى القوة الغاشمة أو الإكراه الذي تستخدمه فى البيئات الاستراتيجية التقليدية والنووية.

لهذا السبب، تكافح الدول للاستفادة من مجموعة القوانين الخاصة بالبيئات الاستراتيجية النووية والتقليدية لتكون ذات صلة بالبيئة الاستراتيجية السيبرانية.

بينما دعا عدد قليل من الدول إلى التفاوض حول صكوك جديدة فى القانون الدولي تنظم البيئة الخاصة بالفضاء السيبراني. قد تكون هذه الأدوات ضرورية بالفعل، نظرًا للاختلافات الكبيرة بين البيئات الاستراتيجية التقليدية على عكس البيئة الإستراتيجية السيبرانية. ومع ذلك، يجادل البعض بأن آفاق قانون المعاهدات الإلكترونية الجديد ضئيلة وأن القانون المتعلق بالفضاء الإلكتروني هو أكثر ارتباطا بممارسات الدولة ما يعقد من عملية التفاوض والصياغة. فضلاً عن ضرورة إقناع الدول بعدم كفاية القواعد الحالية لتنظيم الإستراتيجية السيبرانية.

سيكون إنشاء أدوات قانونية جديدة أو تطوير رأي قانوني ذي صلة بالفضاء الإلكتروني أمرًا صعبًا. على سبيل المثال طرح نهج يركز على قاعدة عدم التدخل. بيد أنه يتعين إدراك التفاهمات المختلفة نوعًا ما للإكراه فى الدراسات الأمنية مقابل مواد القانون الدولي، فيجب التعامل مع الإكراه خارج سياق القانون الدولي بعناية. بالإضافة إلى ذلك، هناك اختلافات فى فهم الإكراه بين الدول وفقهاء القانون الدولي. ومع ذلك، يجب متابعة هذه التعديلات وغيرها لأن الوضع الراهن فى البيئة الإستراتيجية السيبرانية ليس بالوضوح الكافي.

المطلب الثاني

مدي قابلية تطبيق معيار بذل العناية الواجبة فى الفضاء السيبراني

كنقطة أولية، قد يستند الطعن فى تطبيق الالتزام ببذل العناية الواجبة فى الفضاء السيبراني إلى التساؤل الدائم عما إذا كانت بعض الالتزامات الدولية الراسخة والمتصورة دائما فى العلاقات الدولية كالالتزام ببذل العناية الواجبة، يتم تطبيقها على ذات النحو وبالتساوي فى الفضاء الإلكتروني، باعتباره "مجالًا" أو تقنية جديدة؟[1]

ثانيًا، يمكن القول إن الدول، فى ممارساتها وتعبيراتها عن الرأي القانوني، قد قطعت بأن أنشطة الفضاء الإلكتروني تدخل ضمن نطاق الالتزام ببذل العناية الواجبة. عند معالجة هذه الاعتراضات المحتملة، من المهم ملاحظة أن العديد من الدول والمؤسسات الدولية قد أكدت باستمرار تطبيق القانون الدولي ككل على الفضاء السيبراني، بما فى ذلك، على وجه الخصوص، القواعد والمبادئ التي تنبع من السيادة.[2]

---

[1] راجع:
mutatis mutandis, Corn and Taylor, 'Sovereignty in the Age of Cyber', 111 *American Journal of International Law* (2017) 207, at 208 (challenging on a similar basis the applicability of a rule of sovereignty to cyberspace).

راجع أيضا:
Note from Mr. Gabriel Juárez Lucas, Fourth Vice Minister of the Interior Ministry of the Republic of Guatemala to Luis Toro Utillano, Technical Secretariat, Inter-American Juridical Committee, 4VM.200–2019/GJL/lr/bm, 14 June 2019,
لا يمكننا تجاهل التأييد و الدعم لتطبيق القانون الدولي على الفضاء السيبراني ولكن مع ملاحظة أنه يمكن أن تكون هناك مجالات "تمنع فيها حداثة الفضاء الإلكتروني تطبيق حقوق أو التزامات دولية معينة. راجع تقرير منظمة البلدان الأمريكية :
cited in Organization of American States (OAS), Improving Transparency – International Law and State Cyber Operations: Fourth Report (Presented by Prof. Duncan B. Hollis), OEA/Ser.Q, CJI/doc. 603/20 rev.1, 5 March 2020, § 21 (hereinafter 'Improving Transparency')

[2] راجع:
e.g., Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/68/98, 24 June 2013, § 19 (hereinafter 'UN GGE Report 2013');

راجع أيضا:
Hon. Paul C. Ney, Jr, US Department of Defense, General Counsel Remarks at US Cyber Command Legal Conference (2 March 2020), available at:
www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference; US Government, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World (May 2011), at 9,
available at: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (hereinafter 'International Strategy for Cyberspace'); Australian Department of Foreign Affairs and Trade (DFAT), 'Australia Non-Paper: Case Studies on the Application of International Law in Cyberspace (2020), at 4, 7–11
Jeremy Wright QC MP, UK Attorney General, Speech, 'Cyber and International Law in the 21st Century (2018), at 3–6, available at www.gov.uk/government/speeches/cyber-and-international law- in-the-21st-century; Ministere de la Defense (France), 'Droit international appliqué aux operations dans le cyberspace', at 6–17, available at:
www.defense.gouv.fr/content/download/565895/9750877/file/Droit+internat+appliqué+aux+opérations+Cyberespace.pdf
(last visited 10 July 2021); Keynote address by the Minister of Defence of the Kingdom of the Netherlands, Ms. An Bijleveld (20 June 2018),
available at https://english.defensie.nl/downloads/speeches/2018/06/21/keynote-address-by-theminister-of-defence-ms.-ank-bijleveld-marking-the-first-anniversary-of-the-tallinn-manual-2.0-onthe-20th-of-june-2018.
تعليقات مماثلة من قبل الدول الأعضاء على المسودة الأولية
OEWG Report, available at www.un.org/disarmament/open-ended-working-group/ (see individual comments from the Czech Republic, at 2; the Netherlands, §§ 17–18; Japan, at 1, 5; Austria, at 2; Germany, at 2–3).

(ISSN: 2356 - 9492)

وذلك لأن قواعد القانون الدولي العام تنطبق، بشكل افتراضي على جميع أنشطة الدولة. هذا هو الحد الذي تندرج فيه الأنشطة المعنية فى نطاق تلك القواعد والاستثناءات.[1]

بينما قد يتم الطعن فى انطباق التزامات الحماية الحالية على الفضاء الإلكتروني على أساس تأكيد عدة دول أن قواعد القانون الدولي محايدة من الناحية التكنولوجية، حتى لو ظلت هناك أسئلة حول كيفية تطبيقها على وسائل الاتصال الجديدة.[2] بعد كل شيء، كوسيلة لمجموعة متنوعة من الغايات، لا يمكن فصل تكنولوجيا المعلومات والاتصالات عن الأنشطة التي تخدمها، وبالتالي، عن القواعد التي تحكمها. فهناك قاعدتان أساسيتان مستمدتان من مبدأ السيادة وتطبقان بشكل عام فى القانون الدولي، هما على وجه التحديد المبادئ المستقاة من قضية قناة كورفو ومبادئ عدم الضرر.[3] وبالتالي، فإن الافتراض الذي يجب أن ننطلق منه هو أنها تنطبق على تكنولوجيا المعلومات والاتصالات، في حالة عدم وجود نصوص تعاهديه تقيد ذلك.[4]وهذا يعني أنه، بشكل افتراضي، ينطبق هذا الواجب على الفضاء السيبراني، فى حالة عدم وجود ضوابط محددة تستبعد تكنولوجيا المعلومات والاتصالات من نطاق تطبيقها.[5]

على العكس من ذلك، لم تكتف الدول بالقانون الدولي العام والقانون الدولي لحقوق الإنسان والقانون الدولي الإنساني فحسب، بل دعمت أيضًا إمكانية تطبيق التزامات الحماية المختلفة فى الفضاء الإلكتروني، حتى لو كان ذلك بطريقة مجزأة إلى حد ما.

---

[1] *S.S. Lotus*, 1927 PCIJ Series A, No. 10, para. 45; ILC

الصعوبات الناشئة عن تنوع وتوسع القانون الدولي ، تقرير مجموعة الدراسة التابعة للجنة القانون الدولي. راجع:

Martti Koskenniemi, UN Doc A/CN.4/L.682, 13 April 2006, § 120 (hereinafter 'Fragmentation Report'). See also Akande, Coco، and de Souza Dias, 'Old Habits Die Hard: Applying Existing International Law in Cyberspace and Beyond', *EJIL: Talk!* (5 January 2021), available at www.ejiltalk.org/old-habits-die-hard-applying-existing-international-law-in-cyberspace-and-beyond/.

[2] OEWG, Second 'Pre-Draft' Report on Developments in the Field of Information and Telecommunications in the Context of International Security (2020), § 21, available at www.un.org/disarmament/openended-working-group/.

راجع أيضا:

Moynihan, 'The Application of International Law to State Cyberattacks Sovereignty and Non-Intervention', Chatham House Research Paper, December 2019, paras 5–6. See also *Tallinn Manual 2.0*, *ibid* 6, at 31, para. 4; 46, para. 12;

راجع:

nuclear weapons, Advisory Opinion,8 July 1996, ICJ Reports (1996), para. 39; ILC, Draft Articles on Prevention, *supra* note 21, at 154.

راجع أيضا كل من:

Commentary to Draft Article 3, para. 11; *Responsibilities and Obligations of States with Respect to Activities in the Area*, Advisory Opinion, 1 February 2011, ITLOS Reports (2011) 10, para. 117; Sullivan, *supra* note 3, at 452;

Geiss and Lahmann, 'Freedom and Security in Cyberspace: Shifting the Focus Away from Military Responses Towards Non-Forcible Countermeasures and Collective Threat-Prevention', in K. Ziolkowski (ed.), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy (2013) 621, at 655.

[3] Tallinn Manual 2.0, ibid 6, at 31, para. 4;

راجع أيضا:

Okwori, 'The Obligation of Due Diligence and Cyber-Attacks: Bridging the Gap Between Universal and Differential Approaches for States', Ethiopian Yearbook of International Law (2018) 205, at 213; Khanna, 'State Sovereignty and Self-Defence in Cyberspace', 5 BRICS Law Journal (2018) 139, at 141. See, generally, nuclear weapons, Advisory Opinion, 8 July 1996, ICJ Reports (1996), para. 39

[4] راجع :

Nuclear Weapons, Advisory Opinion, 8 July 1996, ICJ Reports (1996), para. 86.

[5] ولا يوجد دليل على وجود مثل هذا الاستثناء، ويجب تفسير الاستثناءات المقبولة من هذه الالتزامات بشكل مقيد، نظرًا لطابعها المتوافق مع الكافة

Shackelford, Scott J., Scott Russell, and Andreas Kuehn. "Unpacking the international law on cybersecurity due diligence: Lessons from the public and private sectors." *Chi. J. Int'l L.* 17 (2016): pp 8-9

راجع أيضا:

Coco, Antonio, and Talita de Souza Dias. "'Cyber Due Diligence': A Patchwork of Protective Obligations in International Law." *European Journal of International Law* 32.3 (2021): 771-806.

الالتزام الدولي ببذل العناية الواجبة في الفضاء السيبراني
بين التدابير الرادعة ومنع الأضرار السيبرانية العابرة

د. أسامة حمزة محمود عبد الفتاح

مجلة الدراسات القانونية والاقتصادية

على سبيل المثال، منذ عام 2011، أقرت الولايات المتحدة باحترام الالتزامات التي يفرضها القانون الدولي لحقوق الإنسان عبر الشبكة العنكبوتية، بالإضافة إلى واجب منع الجرائم الإلكترونية. بعد ذلك بوقت قصير، أصدر مجلس أوروبا توصية الاعتراف بإمكانية تطبيق مبدأ عدم إلحاق الضرر بالأنشطة السيبرانية الخبيثة.[1]

تضيف المذكرة التفسيرية أن هذا المبدأ يهدف إلى تحديد معيار الرعاية أو العناية الواجبة لحماية وتعزيز نزاهة وعالمية الإنترنت. . .. بموجب هذا المعيار، يُطلب من الدول اتخاذ تدابير معقولة لمنع وإدارة والاستجابة للعمليات التخريبية الكبيرة العابرة للحدود أو التدخلات فى البنية التحتية أو الموارد الحيوية للإنترنت.[2]

إلى جانب البيان المذكور أعلاه الذي أدلى به ممثل الاتحاد الأوروبي فى سياق أزمة COVID-19 – والذي أيدته صراحة تركيا ومقدونيا الشمالية والجبل الأسود وصربيا وألبانيا والبوسنة والهرسك وأيسلندا وليختنشتاين والنرويج وأوكرانيا، مولدوفا وأرمينيا.[3]

– تواترت عدة دول مؤخرًا على استخدام هذا المصطلح "العناية الواجبة عبر الإنترنت" باعتبارها مسألة من مسائل القانون الدولي. فعلى سبيل المثال، انعكاسًا للحكم الصادر فى قضية مضيق كورفو والقاعدة 6 من دليل تالين، صرحت فرنسا مؤخرًا بأنه: وفقًا لمبدأ العناية الواجبة، تلتزم الدول بعدم السماح عن علم باستخدام أراضيها لارتكاب أعمال يحظرها القانون الدولي ضد دول من الغير من خلال استخدام الوسائل الإلكترونية. وينطبق هذا الالتزام أيضًا على الأنشطة التي تتم فى الفضاء الإلكتروني من قبل جهات فاعلة من غير الدول تقع فى إقليم أو ضمن سيادة الدولة المعنية.[4] وبالمثل، أعربت إستونيا عن وجهة نظر مفادها أنه "يتعين على الدول بذل جهود معقولة لضمان عدم استخدام أراضيها للتأثير سلبًا على حقوق الدول الأخرى".[1]

---

[1] Council of Europe, Recommendation CM/Rec(2011)8 of the Committee of Ministers to member states on the protection and promotion of the universality, integrity and openness of the Internet (21 September 2021), available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cc2f8.

[2] مذكرة تفسيرية لمشروع التوصية CM / Rec (2011) الصادرة عن لجنة الوزراء للدول الأعضاء بشأن حماية وتعزيز عالمية الإنترنت ونزاهته وانفتاحه
, CM Documents, CM(2011)115-add1, 24 August 2011, § 80 and more extensively §§ 71–84, available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805ccaeb.
تقرير الفريق الاستشاري المخصص المعني بالإنترنت عبر الحدود إلى اللجنة التوجيهية المعنية بوسائل الإعلام وخدمات الاتصال الجديدة الذي يتضمن تحليل مقترحات التعاون الدولي و أصحاب المصلحة على الإنترنت عبر الحدود, Strasbourg, December 2010, §§ 59–74, esp. §§ 72–74 (on the standard of due diligence), available at http://humanrightseurope.blogspot.com/ 2011/01/proposals- for-international-cooperation.html

[3] مجلس الاتحاد الأوروبي ، بيان صحفي ، "إعلان للممثل السامي جوزيب بوريل ، نيابة عن الاتحاد الأوروبي ، بشأن الأنشطة الإلكترونية الضارة التي تستغل جائحة فيروس كورونا"
(30 April 2020), available at www.consilium.europa.eu/en/press/press-releases/2020/04/30/declarationby -the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/. A similar statement was made by the European Union and endorsed by member states during the UN Security Council Arria-Formula Meeting on Cyber Stability and Conflict Prevention and Capacity Building: see Pawel Herczynski, Statement on behalf of the EuropeanUnion (20 May 2020), at 2, available at https://vm.ee/sites/default/files/Estonia_for_UN/20_05_22_ arria_cyber_eu_statement_as_delivered_unread_paras.pdf

[4] انظر:
Comments by Member States on the initial predraft of the OEWG report, *supra* note 47, France, at 3 (emphasis added). Cf. Anne Gueguen, French Deputy Permanent Representative at the UN, Statement at the UNSC Arria-Formula Meeting on Cybersecurity (2020), at 1:35:15 min, available at https://youtu.be/K704P5D1n3E; Minister de la Defense (France), *supra* note 47, at 10.

راجع أيضا:
Cf. Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the Secretary- General, UN Doc. A/74/120, 24 June 2019, at 24 (reply by France); Strategies international de la France pour le numérique (2017), at 32, available at:www.diplomatie.gouv.fr/IMG/pdf/strategie_numerique_ a4_02_interactif_cle445a6a.pdf.

(ISSN: 2356 - 9492)

باستخدام صياغة مختلفة، أشارت أستراليا إلى أنه "إلى الحد الذي تتمتع فيه الدولة بالحق فى ممارسة السيادة على الأشياء والأنشطة داخل أراضيها، فإنها تتحمل بالضرورة المسؤوليات المقابلة لضمان عدم استخدام تلك الأشياء والأنشطة لإلحاق الضرر بالدول الأخرى".[2]

وبصورة أكثر بلاغة، ذكرت فنلندا أنه "من الواضح أن الدول ملزمة بعدم السماح عن قصد باستخدام أراضيها فى أنشطة تسبب ضررًا جسيمًا لدول أخرى، سواء باستخدام تكنولوجيا المعلومات والاتصالات أو غير ذلك".[3]

كما أقرت بأن "على كل دولة حماية الأفراد داخل أراضيها والخاضعين لولايتها القضائية من التدخل فى حقوقهم من قبل أطراف أخري". وفيما يبدو أنه يجمع بين قواعد مختلفة، افترضت هولندا ما يلي:

تم توضيح المبدأ من قبل محكمة العدل الدولية، على سبيل المثال، فى حكمها فى قضية قناة كورفو، حيث رأت أن الدول ملزمة بالتصرف إذا كانت تعلم أو من المفترض أن تعلم أن أراضيها تُستخدم لأعمال مخالفة لحقوق دولة أخرى.... من المقبول عمومًا أن مبدأ العناية الواجبة لا ينطبق إلا إذا كانت الدولة التي انتهك حقها أو حقوقها تعاني من عواقب وخيمة بما فيه الكفاية.[4]

على جانب أخر، رفضت بعض الدول القبول بهذا النهج، حيث قامت كل من الأرجنتين وإسرائيل ونيوزيلندا والمملكة المتحدة، إما برفض أو التشكيك فى انطباق واجبات العناية الواجبة على تكنولوجيا المعلومات والاتصالات. والأهم من ذلك أنها تدعم بقوة الرأي القائل بأن التزامات الحماية القائمة التي تحتوي على معيار العناية الواجبة قابلة للتطبيق بالكامل على تكنولوجيا المعلومات والاتصالات، حتى لو كان تنفيذها المحدد يتطلب إرشادات إضافية.

---

[1] راجع:

President of the Republic [of Estonia] at the opening of CyCon 2019 (29 May 2019), available at: www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-ofcycon-2019/index.html (emphasis added).

[2] انظر:

Australia, DFAT, Australia' International Cyber Engagement Strategy, at 90, Annex A: Australia's position on how international law applies to state conduct in cyberspace (2019), available at https://www.internationalcybertech.gov.au/about/2017-International-Cyber-Engagement-Strategy.

[3]

Janne Taalas, Ambassador, Statement at the second session of the open-ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security (February 2020), available at https://ccdcoe.org/uploads/2018/10/Statement-on-International-Law-by-Finnish-Ambassador-Janne-Taalas-at-2nd-session-of-OEWG.pdf (emphasis added).

[4] وأدلت ببيانات مماثلة كل من الجمهورية التشيكية، وجمهورية كوريا، واليابان، والنمسا، و من الجمهورية الدومنيكية، و شيلي ، وإكوادور، وغواتيمالا ، وغيانا ، وبيرو. راجع في ذلك كل من:

- Government of the Netherlands, Letter from the Minister of Foreign Affairs to the President of the House of Representatives on the International Legal Order in Cyberspace (5 July 2019), Appendix: International law in cyberspace at 4–5, available at www.government.nl/documents/parliamentarydocuments/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace (hereinafter 'Netherlands, Letter of 5 July 2019') (emphases added).
- Czech Republic, *supra* note 47, at 3.
- Comments by Member States on the Initial Pre-Draft of the OEWG Report, available at www.un.org/disarmament/open-ended-working-group/: Republic of Korea, at 2.
- Ministry of Foreign Affairs of Japan, Basic Position of the Government of Japan on International Law Applicable to Cyber Operations (28 May 2021), available at https://www.mofa.go.jp/policy/page3e_001114.html, at 5.
- Comments by Member States on the initial pre-draft of the OEWG report: Austria, *supra* note 96, at 2–5.
- H.E. Mr. José Singer Weisinger, Dominican Republic's Ambassador and Special Envoy to the Security Council, Statement (22 May 2020), available at https://vm.ee/sites/default/files/Estonia_for_UN/22-5-_2020_cyber_stability_and_conflict_prevention_-3.pdf. OAS, Improving Transparency, § 58.

ومع ذلك، لا يزال هناك بعض التساؤلات: (1) ما إذا كان "مبدأ العناية الواجبة" بمفهومه الشامل موجودًا بشكل عام فى القانون الدولي؟ و (2) ما إذا كان هناك التزام باتخاذ تدابير وقائية بشكل خاص للفضاء السيبراني؟[1] على وجه الخصوص، اقترح البعض أن القاعدة 6 من دليل تالين والتعبيرات الإلكترونية المماثلة لمفهوم العناية الواجبة هي بمثابة القوانين المقترحة أو المنشودة *lex ferenda*[2]

أو مجرد تفسيرات لكيفية تطبيق "التزام العناية الواجبة" القائم والواسع النطاق على الفضاء الإلكتروني. وقد أشاروا إلى عدة أسباب للسياسة وراء إحجام الدول عن الالتزام بقاعدة جديدة. على سبيل المثال، قد تخشى الدول من أن معيار العناية الواجبة الدقيق للفضاء السيبراني سيكون مرهقًا للغاية بحيث لا يمكن تنفيذه ويمكن أن يخنق المرونة الضرورية فى السياق السيبراني. كما أنه من الممكن أيضًا، من خلال التوسع فى نطاق الأعمال غير المشروعة فى الفضاء الإلكتروني، أن يؤدي الالتزام الجديد المتعلق بـ "العناية الواجبة الإلكترونية عبر الإنترنت" إلى زيادة اللجوء إلى التدابير المضادة والتقاضي بين الدول.

ربما يكون اختيار استخدام "العناية الواجبة" لوصف مجموعة من الواجبات مضللاً: حيث تحجب بساطته تعقيد وتنوع الالتزامات الوقائية التي تتطلب سلوكًا دؤوبًا لمنع ووقف ومعالجة بعض الأضرار.[3] ويبدو أن جزءًا من الالتباس ينشأ أيضًا من تأطير تكنولوجيا المعلومات والاتصالات كمساحة جديدة أو "مجال"، بدلاً من مجموعة جديدة من أدوات المعلومات والاتصالات.

مع ذلك، فإن الخلاصة المهمة هي: عدم اليقين الذي يحيط بمبدأ عام أو نسخة خاصة بالإنترنت من العناية الواجبة لا يعني أن الفضاء الإلكتروني هو "منطقة خالية من الرسوم الجمركية". على الرغم من أننا نسميها، فإن خليطًا قائمًا من "الالتزامات الوقائية" الأولية يتطلب بالفعل من الدول أن تتصرف بجدية فى منع الأنواع المختلفة من العمليات السيبرانية الضارة ووقفها ومعالجتها

المطلب الثاني

الخلاف حول إلزامية بذل العناية الواجبة فى الفضاء السيبراني

يقتضي القانون الدولي ألا تسمح الدولة عن قصد باستخدام أراضيها للقيام بأنشطة عدائية، بما فى ذلك الإرهاب[4]، ضد دولة أخرى. فى السياق السيبراني، قيل إن هذا الالتزام ينطبق بحيث يتطلب من الدولة ممارسة العناية الواجبة لمنع الأنشطة السيبرانية الضارة المنبثقة من أراضي تلك الدولة.

---

[1] يجب ملاحظة أنه لا توافق بين جميع البلدان على أن مبدأ العناية الواجبة يشكل التزامًا في حد ذاته بموجب القانون الدولي. كما أن هولندا، لا تعتبر المبدأ التزامًا في حد ذاته، والذي قد يشكل انتهاكه فعلًا غير مشروع دوليًا ").

The Netherlands, Letter of 5 July 2019, *ibid*, Appendix, at 4

[2] راجع:

Thirlway, Hugh. "Reflections on lex ferenda." *Netherlands Yearbook of International Law* 32 (2001): 3-26.

[3] Comments by Member States on the initial pre-draft of the OEWG report, *supra* note 96, Austria (at 2); Australia (at 2–3, item C2).

.

[4] استخدم مصطلح الإرهاب عبر الإنترنت في التسعينيات ، حيث ركز النقاش على استخدام المنظمات الإرهابية للشبكة العنكبوتية لشن هجمات ضد البنية التحتية الحيوية مثل النقل وإمدادات الطاقة ("الإرهاب الإلكتروني") واستخدام تكنولوجيا المعلومات في النزاعات المسلحة ("الحرب الإلكترونية"). 557

كانت درجة الاتصال البيني صغيرة مقارنةً بالوقت الحاضر ، ومن المحتمل جدًا أن يكون هذا - بصرف النظر عن مصلحة الدول في الحفاظ على سرية الهجمات الناجحة - أحد

(ISSN: 2356 - 9492)

الحجة المعاكسة هي أنه فى السياق السيبراني لا يوجد التزام قانوني، ولكن تطبيق العناية الواجبة سيكون من الممارسات الحسنة. [1] بما أن الحجة الأخيرة واردة بموجب رأي فريق الأمم المتحدة الحكومي، فهي تدل على رأي بعض الدول على الأقل بأنه فى السياق السيبراني لا يوجد التزام قانوني.[2]

فى الوقت نفسه، هناك دعم من الدول لجعل تطبيقه إلزاميا لمواجهة التنامي فى الأنشطة غير المشروعة للنشاط السيبراني، وقد بدأت بعض الدول فى اتخاذ وجهة نظر مفادها أنه أصبح بالفعل مبدأ ملزمًا فى المجال السيبراني.[3]

بما أن الحجة الأخيرة شدد عليها فريق الخبراء الحكوميين التابع للأمم المتحدة، فهي تدل على رأي بعض الدول على الأقل بأنه فى السياق السيبراني لا يوجد التزام قانوني.[4] على الجانب الأخر بدأت بعض الدول فى تبني وجهة نظر مفادها أنه بالفعل مبدأ ملزم فى عالم الإنترنت بشكل حاسم، مع ذلك، الفرق بين "يجب" و "ينبغي" ليس بعد ذو أهمية عملية كبيرة.

هذا لأنه من غير الواضح حاليًا ماهية تطبيق مبدأ العناية الواجبة على الفضاء السيبراني. فتطبيقه على سياق الفضاء السيبراني، يقتضي أن يتألف المبدأ فى الواقع من عدد من الواجبات الأصغر[5]، وفيما يتعلق بالفضاء الإلكتروني، لم توضح الدول بعد ماهية تلك "الواجبات الفرعية".[1]

الأسباب الرئيسية لعدم الإبلاغ إلا عن عدد قليل جدًا من هذه الحوادث.

تغير هذا الوضع بعد هجمات الحادي عشر من سبتمبر ، مما دفع إلى بدء مناقشة مكثفة حول استخدام الإرهابيين لتكنولوجيا المعلومات والاتصالات. فالجناة استخدموا الإنترنت في تحضيرهم للهجوم. رغم أن الهجمات لم تكن هجمات إلكترونية ، في هذا السياق ، تم اكتشاف طرق مختلفة لاستخدام المنظمات الإرهابية للإنترنت. اليوم ، من المعروف أن الإرهابيين يستخدمون تكنولوجيا المعلومات والاتصالات والإنترنت من أجل:

- دعاية
- جمع المعلومات
- التحضير لهجمات العالم الحقيقي
- نشر المواد التدريبية
- الاتصالات
- تمويل الإرهاب
- الهجمات على البنى التحتية الحيوية. راجع كل من

-: Rollins, John, And Clay Wilson. "Terrorist Capabilities For Cyberattack: Overview And Policy Issues." LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE, 2007.: Lewis, The Internet And Terrorism, Available At: Www.Csis.Org/Media/Csis/Pubs/050401_Internetandterrorism.Pdf; Lewis, Cyber-Terrorism And Cybersecurity; Www.Csis.Org/Media/Csis/Pubs/020106_Cyberterror_Cybersecurity.Pdf; Gercke, Cyberterrorism, How Terrorists Use The Internet, Computer Und Recht, 2007, Page 62

[1] The 2015 consensus report of the UN GGE show that states agreed that they 'should' exercise due diligence: UN A/70/174, para 13(c). See also 2013 report of the UN GGE, UN A/68/98, para 23.

بشأن التدابير التقييدية ضد الهجمات الإلكترونية التي تهدد الاتحاد أو الدول الأعضاء فيه ، والتي تنص على أن "[الدول] يجب أن تسعى إلى ضمان عدم استخدام أراضيها من قبل جهات فاعلة من غير الدول لارتكاب مثل هذه الأعمال" راجع أيضا:

EU Council Decision, preambular para 4.

[2] في هذا الصدد ، يجب التمييز بين الأفعال التي تتم على أراضي الدولة والتي لها آثار ضارة كبيرة على دولة (دول) أخرى ، والتي من الواضح أن الدولة الإقليمية لديها المعرفة والقدرة والفرصة على منعها من ناحية ، ومن ناحية أخرى ، هناك واجب عام باليقظة تجاه أي عمل من جانب جهة فاعلة غير حكومية أو فرد قد يكون له تأثير على دولة أخرى

. See also Chircop, L. (2018), 'A Due Diligence Standard of Attribution in Cyberspace', ICLQ, 67(3): pp. 665–668.

[3] For example, France and the Netherlands (as set out in official statements at footnotes 42 and 43).

راجع أيضا:

Schmitt, M. (2019), 'France's Major Statement on International Law and Cyber: An Assessment', Just Security, 16 September 2019; Jensen, E. T. and Watts, S. A. (2017), 'A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?', Texas Law Review, 95: pp. 1555–1577

[4] راجع :

Chircop, Luke. "A due diligence standard of attribution in cyberspace." *International & Comparative Law Quarterly* 67.3 (2018): 67(3): pp. 665–668.

[5] انظر بتفصيل:

Sklerov, M. J. (2009), 'Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses against States

الالتزام الدولي ببذل العناية الواجبة في الفضاء السيبراني
بين التدابير الرادعة ومنع الأضرار السيبرانية العابرة

د. أسامة حمزة محمود عبد الفتاح

مجلة الدراسات القانونية والاقتصادية

على سبيل المثال، هل ستشمل العناية الواجبة التزامات بإجراء تحقيق أو مجرد الرد على نشاط محدد، ومراجعة وتأمين استخدام الفضاء الإلكتروني من داخل أراضي الدولة، ومشاركة المعلومات مع الدول الأخرى؟ يجب أيضًا التأكيد على أن المبدأ هو مبدأ حاكم لسلوك الدول وليس النتيجة: ليس من واجبه منع النشاط السيبراني الضار، ولكن اتخاذ خطوات معقولة لمحاولة القيام بذلك.

صاحب تدفق المعلومات إساءة استخدام تلك الوسيلة مع تطور الفضاء الإلكتروني[2]. وفى المقابل حرصت الدول على إنفاذ استراتيجيات الأمن السيبراني لحماية البنية التحتية السيبرانية الوطنية.[3] على الرغم من هذه الجهود، لم تتجاوز قضية الأمن السيبراني مرحلة الاتفاقات غير الملزمة.[4] فمع تضارب الأجندات السياسية. . . التجسس [و] المنافسة على النفوذ العالمي[5]" باتت بعض القوي الدولية عازمة على مناهضة تبلور التزام دولي ببذل العناية الواجبة فى الفضاء السيبراني.

إن إلزام كل دولة باتخاذ جميع التدابير المتاحة لوقف الهجمات الإلكترونية التي تنطلق من أراضيها من شأنه تحسين أمن الشبكات المترابطة عالمياً[6] فمع تسجيل أجهزة التتبع الحية أكثر من ستة ملايين هجوم إلكتروني يوميًا الخوف من انعدام الأمن السيبراني الذي سيطر على العالم.[7]

تستثمر الدول بشكل متزايد فى القدرات الإلكترونية للحماية من التصعيد فى شدة الهجمات الإلكترونية،[8] مع توقع عسكرة الفضاء الإلكتروني على نطاق واسع.[9] يرى بعض المعلقين أن الأسلحة السيبرانية هي "السلاح المفضل" للأنشطة للإرهابية وهو واقع بات ملموساً فى الصراعات الحالية.[10]

Who Neglect Their Duty to Prevent', Military Law Review, 201: pp. 1–85.

[1] Having said this, as long ago as 2000, the UN General Assembly 'not[ed] the value of' states taking various measures that could be required under a duty of due diligence in the cyber context: GA Res. 55/63 (4 December 2000).

[2] Ian Brown, Expert Witness Statement for Big Brother Watch and Others Re: Large-Scale Internet Surveillance by the U.K. 3 para. 7 (App. No. 58170/13 to Eur. Ct H. R. (Sept. 27, 2013)), available at https://papers.ssrn.com/sol3/papers.cfm?abstract _id=2336609 (last visited Jan. 18, 2021)

[3] ; Dep't Prime Minister & Cabinet, Australia's Cyber Security Strategy (2016); Gov't of the U.K., The U.K. Cyber Security Strategy (2011); Executive Off. of the President of the U.S., The National Strategy to Secure Cyberspace (2003).

[4] راجع:

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. GAOR, 17th sess., Agenda Item 93, U.N. Doc A/70/174 (July 22, 2015).

[5] راجع:

Scott J. Shackleford, Scott Russell & Andreas Kuehn, Unpacking the International Law on Cybersecurity Due Diligence: Lessons From the Public and Private Sectors, 17 Chi. J. Int'l L. 1, 25-34 (2016)

[6] راجع:

Division for Treaty Aff., U.N. Off. on Drugs & Crime, Comprehensive Study on Cybercrime (Draft) 1-22 (Feb. 2013).

[7] راجع:

Xu Longdi, China's Internet Development and Cybersecurity: Policies and Practices, in Chinese Cybersecurity and Defence 46 (Daniel Ventre ed., 2014); Kara Scannell & Gina Chon, F.T. Investigation: Cyber Insecurity U.S. Agencies are Revealed to Lack Basic I.T. Defences, Financial Times (July 15, 2015), available at https://www.ft.com/content/698deb42-200b-11e5-aa5a-398b2169cf79 (last visited Oct. 21, 2021)

[8] راجع:

U.N. Institute For Disarmament Res., The Cyber Index International Security Trends and Realities xi, 1, 3, 9-55, 117 (Mar. 2013).

[9] راجع:

E.g., Cyberwar, Law and Ethics for Virtual Conflicts (Jens David Ohlin, Kevin Govern & Claire Finkelstein eds, 2

[10] راجع:

(ISSN: 2356 - 9492)

المبحث الثالث

مشروعية التدابير الاستباقية لمنع الأضرار العابرة فى الفضاء السيبراني

ما هي الخطوات التي يتعين على الدول والشركات الخاضعة لولايتها القضائية أن تتخذها بالضبط بموجب القانون الدولي لتأمين شبكاتها، وماذا عن حقوق ومسؤوليات دول العبور؟ يستعرض هذا المبحث الحجج المحيطة بإنشاء معيار العناية الواجبة للأمن السيبراني ويدافع عن نظام استباقي يأخذ فى الاعتبار المسؤوليات المشتركة، ولكن المتباينة للجهات الفاعلة فى القطاعين العام والخاص فى الفضاء السيبراني.

Matthew J Sklerov, Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent, 201 Military. L. Rev. 1, 79 (2009) (citing Richard Garnett & Paul Clarke, Cyberterrorism: A New Challenge for International Law, in Enforcing International Law Norms Against Terrorism (Andrea Bianchi & Yasmin Naqvi eds, 2004)).

الالتزام الدولي ببذل العناية الواجبة في الفضاء السيبراني
بين التدابير الرادعة ومنع الأضرار السيبرانية العابرة

د. أسامة حمزة محمود عبد الفتاح

المطلب الأول

مدي التزام الدولة باتخاذ تدابير وقائية فى الفضاء السيبراني

اتفق فريق الخبراء الدولي على أنه بمجرد أن تتوفر المعرفة لدى الدولة (القاعدة 6) بحقيقة أن أراضيها تُستخدم بطريقة تسبب عواقب وخيمة لدولة أخرى فيما يتعلق بحق بموجب القانون الدولي، يجب على الدولة اتخاذ جميع التدابير المتاحة بشكل معقول لوقف تلك العملية السيبرانية. ومع ذلك، كما سيتم توضيحه، فإن النطاق الدقيق للعمل الذي يتطلبه مبدأ العناية الواجبة غير مستقر.

عندما يتم النظر فى التدابير الوقائية أحادية الجانب ضد الهجمات الإلكترونية ، فمن الممكن أن تتطلب السيناريوهات المختلفة تقييمًا قانونيًا مختلفًا ومتميزًا. حتى الآن ، عندما أخذ المعلقون فى الاعتبار التدابير المضادة فى السياق السيبراني.

فهناك سيناريوهات الهجوم ، التي كان الدافع وراءها فى الغالب هو الإدراك بأنه لا يتعين على الدول السماح ببلوغ النشاط السيبراني غير المشروع مستوي الهجوم المسلح وفقًا للمادة 51 من ميثاق الأمم المتحدة .[1]

بيد أن الجدل دائما ما يثار حول ماهية تلك الإجراءات وما القواعد التي تحكمها ، فما الإجراءات (التدابير) الاستباقية لاكتشاف أو الحصول على معلومات تتعلق بالتدخل الإلكتروني أو الهجوم السيبراني أو العملية الإلكترونية الوشيكة ، أو لتحديد أصل العملية التي تنطوي على تهديد سيبراني صادر من دولة أجنبية أو كيانات غير دولية.[2]

بعبارة أخرى ، "الدفاعات النشطة" 'active defences' هي "ردود عينية " من أجل "تعطيل مصدر الهجوم" بشكل استباقي. بالنسبة لمؤيديهم ، فإن ميزة هذا الدفاعات النشطة داخل السياق الذي تم تحليله هي أنها تتوافق مع مبدأ المعاملة بالمثل، الذي لا يشكل شرطا مسبقا لشرعية الإجراءات المضادة ، فإن لجنة القانون الدولي فى إشارة إلى تحكيم اتفاقية الخدمة الجوية.[3] مع ذلك ترى أن "[ج] التدابير المضادة من المرجح أن تفي بمتطلبات الضرورة والتناسب إذا تم اتخاذها فيما يتعلق بالالتزام نفسه أو التزام وثيق الصلة.

المشكلة الرئيسية ذات الصلة بمشروعية التدابير المضادة ، تكمن فى إسناد السلوك غير المشروع ؛ والسلوك غير المشروع هنا ليس هجومًا مسلحًا ، بل هجومًا إلكترونيًا ينتهك القواعد الدولية الأخرى مثل حظر استخدام القوة وفقًا للمادة 2 (4) من ميثاق الأمم المتحدة (بدون الوصول إلى درجة الهجوم المسلح) ، أو مبدأ عدم التدخل.[4]

---

[1] Hinkle, Katharine C. "Countermeasures in the cyber context: One more thing to worry about." *Yale Journal of International Law* 37.Fall (2011): 11-21.

[2] 4 U.S. Department of Defense, 1999, An Assessment of International Legal Issues in Information Operations, 16 et seq.; speech by the Secretary of State of the German Federal Ministry of the Interior, International Cooperation in Developing Norms of State Behaviour for Cyberspace, Berlin, 13 December 2011.

[3] the ILC in reference to the Air Service Agreement arbitration79 nonetheless holds that '[c]countermeasures are more likely to satisfy the requirements of necessity and proportionality if they are taken in relation to the same or a closely related obligation. ILC Commentaries, Part Three, Chapter II, at para. 5

[4] Hinkle, Katharine C. "Countermeasures in the cyber context: One more thing to worry about." *Yale Journal of International Law* 37.Fall (2011): 11-21.

(ISSN: 2356 - 9492)

إذا كان الإسناد من أجل إثبات مسؤولية الدولة المهاجمة المزعومة شرطًا مسبقًا، فسيترتب على ذلك أن نفس معيار الإثبات ينطبق على النحو المبين أعلاه .[1] ونتيجة لذلك ، تواجه الدولة الضحية نفس المشاكل القانونية والواقعية عند محاولتها وضع أساس قانوني للرد مع الدفاعات النشطة .

ففى معظم الحالات، ما قد تلجأ إليه الدولة فى الواقع فى مثل هذه الحالة الطارئة هو ما يسمى بـ "الإجراءات المضادة العاجلة" كما هو موضح فى المادة 52 (2) من مواد لجنة القانون الدولي بشأن مسؤولية الدولة. ومع ذلك، فى حين أنه وفقًا لصياغة المادة 52 ، "يجوز للدولة المتضررة أن تتخذ التدابير المضادة العاجلة اللازمة للحفاظ على حقوقها" ، فإن هذا يعفيها صراحةً فقط من الالتزام المفصل فى المادة 52 (1) (ب) إلى " إخطار الدولة المسؤولة بأي قرار لاتخاذ تدابير مضادة وعرض التفاوض مع تلك الدولة. 'وبالتالي، فإن ما يتم تغييره فى حالات الاستعجال هو مجرد مطلب إجرائي.[2]

لذلك، لا يمكن استنتاج أن الدول تتمتع بسلطة تقديرية أوسع عندما يتعلق الأمر باتخاذ تدابير مضادة فى حالات الطوارئ الناجمة عن الهجمات الإلكترونية. فبعد كل شيء، الإجراءات المضادة العاجلة ليست سوى شكل من أشكال التدابير المضادة فى حالة عاجلة، ويجب إظهار ضرورتها بطريقة دقيقة"[3] لأن الإجراءات المضادة تنطوي بطبيعتها على مخاطر تصعيد النزاع ، عندما يكون أحد الإجراءات الإجرائية تم التخلي عن الضمانات لأخذ الإلحاح فى الاعتبار ، ويصبح من الأهمية بمكان أن تكون الدولة العاملة قد تأكدت من الحقائق التي يتم الاعتماد عليها كأساس قانوني لسلوكها. ويترتب على ذلك أن عزو الهجوم السيبراني بشكل مباشر من أجل تبرير الإجراءات المضادة النشطة ترقى إلى مستوى هجوم مسلح.

فى ضوء رفضهم للالتزام باتخاذ تدابير وقائية، اتفق الخبراء على أن الدولة ليست ملزمة بمراقبة الأنشطة الإلكترونية على أراضيها. ومع ذلك، إذا اختارت دولة ما مراقبة الأنشطة الإلكترونية على أراضيها، فإن حقيقة قيامها بذلك قد تؤثر على ما إذا كانت لديها معرفة بأي عمليات إلكترونية موجهة إلى دولة أخرى من أراضيها.[4]

واعترف فريق الخبراء الدولي بالرأي المعاكس، وهو أن الالتزام ببذل العناية الواجبة يمتد إلى الحالات التي تكون فيها الأفعال الضارة ذات الصلة ممكنة فقط. وبموجبه، يجب على الدول اتخاذ تدابير معقولة لمنعهم من الخروج من أراضيهم.

ويستند هذا الرأي جزئيًا إلى وجود التزام باتخاذ تدابير وقائية فى سياق الضرر البيئي العابر للحدود.[5] علاوة على ذلك، فى ضوء طبيعة الأنشطة السيبرانية، يمكن القول إن التدابير الوقائية جوهرية. على سبيل المثال، غالبًا ما تعقد سرعة العمليات الإلكترونية إجراءات مواجهتها ما يجعل فرصها فى التصدي أقل فعالية.[6]

---

[1] ILC Commentaries, Part Three, Chapter II, at para. 2.2

[2] Geiß, Robin, and Henning Lahmann. "Freedom and Security in Cyberspace: Shifting the Focus Away from Military Responses Towards Non-Forcible Countermeasures and Collective Threat-Prevention." *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy, Tallinn* (2013).

[3] Iwasawa, Yuji, and Naoki Iwatsuki. "Procedural Conditions." *The Law of International Responsibility* (2010): 1149, 1155; likewise, Krieger, op. cit., at 16

[4] Ziolkowski, Katharina. "Confidence Building Measures for Cyberspace–Legal Implications." *NATO CCD COE Publication* (2013): 1-88.

[5] Rosas, Allan. "Issues of State Liability for Transboundary Environmental Damage." *Nordic J. Int'l L.* 60 (1991): 29.

[6] Roguski, Przemysław. "Collective Countermeasures in Cyberspace–Lex Lata, Progressive Development or a Bad Idea?." *2020 12th International Conference on Cyber Conflict (CyCon)*. Vol. 1300. IEEE, 2020.

ووفقًا لهذا الموقف، يجب على الدولة أن تتخذ تدابير وقائية مجدية تتناسب مع خطر الضرر المحتمل. وعليهم أن يأخذوا فى الحسبان التطورات التكنولوجية والعلمية، فضلاً عن الظروف الفريدة لكل حالة تشمل الأمثلة إدخال سياسات أمن المعلومات، وإنشاء فرق الاستجابة للطوارئ الحاسوبية، واعتماد التشريعات المحلية المناسبة التي تتطلب من الشركات الإبلاغ عن الحوادث الإلكترونية من أجل التمكن من إجراء تقييمات دقيقة للتهديدات.

على الرغم من أن الخبراء رفضوا الحجة القائلة بأن واجب العناية الواجبة يتطلب تدابير وقائية، إلا أنهم لاحظوا أنه إذا كان سيتم اعتماد هذا النهج، فلن يكون من الواضح متى يتم خرق هذا الالتزام. أحد الاحتمالات هو أن يحدث الخرق عندما تكون الدولة المستهدفة معرضة لخطر الضرر بحكم عدم اتخاذ الدولة التدابير المناسبة لمنع شن عمليات إلكترونية ضارة من أو عبر أراضيها.

انقسم فريق الخبراء الدولي حول المواقف التي تتوقع فيها الدولة بدرجة معقولة من اليقين أن البنية التحتية الإلكترونية على أراضيها، بعد أن تم استخدامها سابقًا، سيتم استخدامها مرة أخرى فى عمليات إلكترونية ضارة يتم توجيهها لدولة أخرى، لكنها تفشل فى التصرف. على سبيل المثال، إذا تم استغلال بنية تحتية إلكترونية معينة بشكل متكرر لأغراض تنفيذ عمليات إلكترونية ضارة ضد دول أخرى، فقد يكون من المعقول استنتاج أنها ستكون كذلك حتى تستخدم مرة أخرى.

وبالمثل، إذا قامت مجموعة معينة بشن مثل هذه العمليات بشكل متكرر، فمن المحتمل جدًا أن تكرر ذلك فى المستقبل. السؤال هو ما إذا كان التزام العناية الواجبة قد تم خرقه نظراً لتقاعس الدولة عن اتخاذ تدابير لمنع العمليات السيبرانية المتوقعة.[1] والسبب الآخر هو أنه على الرغم من أن مبدأ العناية الواجبة يتطلب من الدول اتخاذ تدابير وقائية مناسبة، فعواقب المسؤولية عن فشلها فى القيام بذلك تتوقف على تعرض الدولة المستهدفة بالفعل للضرر المطلوب.[2] انقسم فريق الخبراء الدولي حول المواقف التي تتوقع فيها الدولة بدرجة معقولة من اليقين أن البنية التحتية الإلكترونية على أراضيها، بعد أن تم استخدامها سابقًا، سيتم استخدامها مرة أخرى فى عمليات إلكترونية ضارة موجهة إلى دولة أخرى، لكنها تفشل فى التصرف. [3]

اتخذ أغلبية فريق الخبراء الدولي موقفًا مفاده أن فرض التزام بالعمل فى مثل هذه الحالات يتوافق مع هدف هذه القاعدة والغرض منها. نظرًا لأن العمليات السيبرانية المعنية ليست تخمينية، وقد تستنتج دولة ضمن الإطار المنطقي للأحداث أنها ستطلق فى الواقع إذا فشلت فى التصرف، فقد يتم تشبيهها بالعمليات الجارية.

[1] راجع:

Liu, Ian Yuying. "State responsibility and cyberattacks: Defining due diligence obligations." *Indon. J. Int'l & Comp. L.* 4 (2017): 191.

[2] راجع

Takano, Akiko. "Due diligence obligations and transboundary environmental harm: Cybersecurity applications." *Laws* 7.4 (2018): 36.

[3] على سبيل المثال، إذا تم استغلال بنية تحتية إلكترونية معينة بشكل متكرر لأغراض تنفيذ عمليات إلكترونية ضارة ضد دول أخرى، فقد يكون من المعقول استنتاج أنها ستكون كذلك حتى تستخدم مرة أخرى. وبالمثل، إذا قامت مجموعة معينة بشن مثل هذه العمليات بشكل متكرر، فمن المحتمل جدًا أن تقوم المجموعة بذلك فى المستقبل. السؤال هو ما إذا كان التزام العناية الواجبة قد تم خرقها لتقاعس الدولة عن اتخاذ تدابير لمنع العمليات السيبرانية المتوقعة. راجع:

Lewis, James Andrew. *Rethinking Cybersecurity: Strategy, Mass Effect, and States*. Rowman & Littlefield, 2018.

(ISSN: 2356 - 9492)

كان رأي الأقلية أن شرط اتخاذ تدابير ردعية هو فى الواقع شرط من متطلبات الردع، فيما يتعلق بنطاق التدابير المطلوبة بموجب هذه القاعدة، اتفق الخبراء على أن الدول يجب أن تستخدم جميع الوسائل الممكنة، والمتاحة بشكل معقول، ضمن صلاحياتها السيادية، كما يتعين على الدولة أن تتصرف بشكل معقول فى نفس الظروف أو ظروف مماثلة (أي القيام بما يسمى "أفضل الجهود")، فجدوي تدابير معينة هي دائما سياقية.

غالبًا ما تكون الدول المتقدمة أكثر قدرة على إيقاف العمليات السيبرانية الضارة التي تنطلق من أراضيها من الدول النامية. تعتمد الجدوى، فى جملة أمور، على الوسائل التقنية للدولة المعنية، والموارد الفكرية والمالية المتاحة لها، والقدرة المؤسسية للدولة على اتخاذ التدابير، ومدى سيطرتها على البنية التحتية الإلكترونية الموجودة على أراضيها.

لتوضيح ذلك، إذا أبلغت الدولة المستهدفة دولة بأن العمليات السيبرانية الشديدة تنشأ من بعض عناوين IP التي تم تخصيصها للدولة الإقليمية، فمن المعقول أن تتخذ الدولة الإقليمية تدابير لحظر عناوين IP هذه منذ ذلك الحين تقريبا كل الدول لديها القدرة على اتخاذ مثل هذه الخطوات.

وعلى النقيض من ذلك، قد تفتقر الدولة إلى القدرة على الاستجابة بفعالية للعمليات السيبرانية المعقدة والديناميكية للغاية التي تنطلق من البنية التحتية السيبرانية على أراضيها. إذا كان هذا هو الحال، فلن يكون هناك خرق لالتزام العناية الواجبة، حيث إن التدابير الوقائية تكون غير مجدية. لاحظ، مع ذلك، أنه إذا كانت الدولة تفتقر إلى القدرة المطلوبة لوقف العمليات السيبرانية الضارة المستمرة بنفسها، فقد يكون التدبير المعقول المجدي هو استئجار شركة خاصة لأداء هذه المهمة.

عند النظر فى الجدوى، من الضروري تطبيق القاعدة بطريقة فعالة. ضع فى اعتبارك حالة جماعة إرهابية تنفذ عمليات إلكترونية ضارة من أراضي دولة ضد دولة أخرى. هذا الأخير ليس على علم بالعمليات. قد يكون من الحكمة مراقبة الأنشطة للحصول على مزيد من المعلومات الاستخباراتية بدلاً من إنهائها على الفور.

فى الواقع، قد تفوق الفوائد التي تعود على الدولة المستهدفة من العمل المتأخر فوائد الإجراء الفوري لأن إجراءات المجموعة يمكن إحباطها بشكل أكثر فعالية ونهائيًا بمجرد أن تتمكن الدولة من الاستفادة من المعلومات الاستخبارية المكتسبة خلال فترة التأخير.

تنطبق هذه القاعدة إذا كان بالإمكان تنفيذ العمليات الإلكترونية التصحيحية ذات الصلة من قبل أجهزة الدولة أو من قبل الأفراد الخاضعين لسيطرة الدولة. كما اتفق فريق الخبراء الدولي على أنه إذا كان لا يمكن تنفيذ الإجراءات الردعية إلا بواسطة كيان خاص، مثل مقدم خدمة الإنترنت، فإن الدولة ملزمة باستخدام جميع الوسائل المتاحة لها لمطالبة هذا الكيان باتخاذ الإجراءات اللازمة لإنهاء النشاط المخالف.

قد يكون الكيان الخاص أو الفرد الذي يتحكم فى البنية التحتية الإلكترونية التي تستخدمها دولة أو جهة فاعلة من غير الدول لإجراء عمليات إلكترونية ضارة فى الخارج يرفض التعاون الكامل مع الدولة الإقليمية فى وضع حد للعمليات.

واتخذ الخبراء موقفًا مفاده أن هذا الافتقار إلى التعاون لا ينفى عدم مشروعية انتهاك الدولة لبذل العناية الواجبة. وبدلاً من ذلك، يجب على الدولة أن تستنفد جميع الوسائل الممكنة لتأمين تعاون الشخص أو الكيان المعني، طالما أن هذه التدابير تتفق مع القانون الدولي. فقط إذا فعلت الدولة ذلك ولا تزال غير قادرة على تأمين التعاون الضروري لإنهاء العمليات الضارة، فلن تنتهك هذا المبدأ.

الالتزام الدولي ببذل العناية الواجبة في الفضاء السيبراني
بين التدابير الرادعة ومنع الأضرار السيبرانية العابرة

د. أسامة حمزة محمود عبد الفتاح

مجلة الدراسات القانونية والاقتصادية

نظر فريق الخبراء الدولي بعناية فى مسألة ما إذا كان يجب على الدولة أن تضع الشروط القانونية لتكون قادرة على الامتثال لالتزام العناية الواجبة، أو على الأقل إزالة أي عقبات قانونية أمام هذه القدرة. وخلصت إلى أنه لا يوجد مثل هذا الالتزام على هذا النحو، على الرغم من أن العديد من الدول قد فعلت ذلك، وأن الاتفاقات الدولية تتطلب أحيانًا من الدول الأطراف اعتماد تدابير تشريعية تمكنها من التصدي للعمليات الإلكترونية التي تشكل جرائم. ولا يوجد أي التزام بموجب مبدأ العناية الواجبة للدولة لمقاضاة أولئك المنخرطين فى العمليات الإلكترونية الأساسية؛ بدلاً من ذلك، يقتصر الالتزام على اتخاذ الإجراءات الممكنة لإنهاء العمليات.

بالإضافة إلى ذلك، اتفق الخبراء على أن القيود القانونية المحلية لا تبرر عدم امتثال الدولة لالتزامها ببذل العناية الواجبة. على سبيل المثال، إذا كان النظام القانوني المحلي لدولة ما يتطلب أمرًا من المحكمة لاتخاذ التدابير اللازمة لإنهاء العملية السيبرانية الضارة، فإن عدم القدرة على الحصول على مثل هذا الأمر لا يمنع عدم مشروعية فشل الدولة فى إنهاء العملية الضارة ما لم يكن هذا العجز هو على أساس الامتثال للقانون الدولي (كما فى حالة القانون الدولي لحقوق الإنسان.

ومع ذلك، اتفق الخبراء على أنه، من الناحية العملية، ينبغي للدول أن تتخذ خطوات لضمان توفر التدابير التي قد يتعين عليها اتخاذها للرد على مثل هذه العمليات بموجب قوانينها المحلية. على سبيل المثال، يمكن لدولة ما أن تسن تشريعًا يمكّنها من مطالبة مزودي خدمة الإنترنت بإلغاء خوادم القيادة والسيطرة على شبكة الروبوتات فى حالة إنشاء مثل هذه الخوادم على أراضيها. من شأن هذا التشريع أن يسمح للدولة بالرد بسرعة وفعالية للامتثال لهذه القاعدة.

إن مطلب إنهاء العمليات السيبرانية التي تشملها هذه القاعدة معقد بسبب طبيعة العمليات السيبرانية الضارة، لا سيما ضغط الزمان والمكان وحقيقة أنها غالبًا ما تكون خاصة بنقطة ضعف أو نظام معين. إذا استنفدت دولة ما بجدية جميع التدابير الممكنة لوقف الأنشطة السيبرانية الضارة من أراضيها، ولكن ثبت أن محاولاتها عقيمة وتعاني الدولة المستهدفة مع ذلك من الضرر، فلن تكون الدولة قد انتهكت هذه القاعدة. بما أن مبدأ العناية الواجبة هو التزام بسلوك وليس نتيجة، فإنه لا يطالب بأن تنجح دولة الإقليم دائمًا فى إنهاء الاستخدامات الضارة لإقليمها، بل يتطلب فقط أن تتصرف الدولة بجدية فى جهودها من أجل القيام بذلك.

إن مطلب إنهاء العمليات السيبرانية التي تشملها هذه القاعدة معقد بسبب طبيعة العمليات السيبرانية الضارة، لا سيما ضغط الزمان والمكان وحقيقة أنها غالبًا ما تكون خاصة بنقطة ضعف أو نظام معين.

إذا استنفدت دولة ما بجدية جميع التدابير الممكنة لوقف الأنشطة السيبرانية الضارة من أراضيها، ولكن ثبت أن محاولاتها عقيمة وتعاني الدولة المستهدفة مع ذلك من الضرر، فلن تكون الدولة الإقليمية قد انتهكت هذه القاعدة.

من حيث إن مبدأ العناية الواجبة هو التزام بسلوك وليس نتيجة، فإنه لا يطالب بأن تنجح دولة الإقليم دائمًا فى إنهاء الاستخدامات الضارة لإقليمها، بل يتطلب فقط أن تتصرف الدولة بجدية فى جهودها من أجل القيام بذلك. ومع ذلك، إذا كان عدم النجاح ناتجًا عن فشل الدولة فى استنفاد التدابير المتاحة بشكل معقول لإنهاء العمليات السيبرانية الضارة، فهذا يعد انتهاكًا لهذه القاعدة.

(ISSN: 2356 - 9492)

على سبيل المثال، قد لا تتصرف الدولة الإقليمية بالسرعة الكافية لمنع الضرر الذي تسببه العمليات الإلكترونية من أراضيها. إذا كان من الممكن أن يكون رد فعلها أسرع فى الظروف المصاحبة، فهذا خرق.

قد تكون هناك ظروف يكون فيها من غير المعقول التصرف لمنع الضرر الذي يلحق بدولة أخرى من العمليات الإلكترونية التي تنشأ من أراضيها. على سبيل المثال، قد تعلم الدولة أنه يتم التحضير لعملية إلكترونية ضارة وسيتم إطلاقها من أراضيها ضد الدولة المستهدفة. ومع ذلك، نظرًا لأنه لم يحدد الموقع الدقيق للهجوم وتوقيته، فقد يكون العامل الفعال الوحيد هو عزل الشبكة التي سيتم استخدامها لإجراء عملية ضد الإنترنت أو البنية التحتية فى دولة أخرى.

من أجل إنهاء العملية، سيكون من الضروري إغلاق عدد من الشبكات الأساسية على أراضي الدولة. فى مثل هذه الحالات، يجب تقييم طبيعة الضرر (المحتمل) الذي يلحق بكلتا الدولتين وحجمه ونطاقه لتحديد ما إذا كان التدبير الوقائي مطلوبًا أم لا. الاختبار فى مثل هذه الظروف هو المعقولية.

قد يحدث فى بعض الأحيان أن الدولة الإقليمية غير قادرة على إنهاء استخدام أراضيها، ولكن الدول الأخرى القادرة على استعداد لتقديم المساعدة. وهذا يثير التساؤل عما إذا كانت الدولة الإقليمية تتحمل التزامًا بطلب المساعدة من الدول الأخرى فى مثل هذه الحالات. أجاب فريق الخبراء الدولي على هذا السؤال بالنفى. ينبع مبدأ العناية الواجبة من مبدأ السيادة. فهو ينشئ فقط التزامات تقع ضمن نطاق الامتيازات السيادية للدولة الإقليمية.

وبعبارة أخرى، لا تحتاج الدولة إلا إلى الانخراط فى الأعمال التي تتعارض مع ممارستها للسيادة. وهكذا، فى حين أن الدولة قد تسعى للحصول على مساعدة خارجية، فهي ليست ملزمة قانونا للقيام بذلك. إذا كانت الدولة غير راغبة فى إنهاء العمليات السيبرانية الضارة مشمولًا بمبدأ العناية الواجبة بدلاً من عدم القدرة على القيام بذلك، يجوز للدولة المضرورة اللجوء إلى التدابير المضادة (القاعدة 20) بناءً على عدم امتثال الدولة الإقليمية لهذه القاعدة. انظر القاعدة 23 لمعرفة كيفية تقييم تناسب التدبير المضاد فى مثل هذه الحالات. – فيما يتعلق باستخدام البنية التحتية السيبرانية أو إجراء عمليات إلكترونية من أراضي دولة محايدة خلال فترة دولية النزاع المسلح.

المطلب الثاني

الاثار المترتبة على تجاهل اتخاذ التدابير الوقائية فى الفضاء السيبراني

مبدأ العناية الواجبة هو التزام قانوني ينتهك بالإهمال أو بمعني أخر التقاعس عن اتخاذ التدابير الواجبة لمنع وقوع الضرر. ولا يشمل الإغفال التقاعس عن العمل فحسب، بل يشمل أيضًا اتخاذ تدابير غير فعالة أو غير كافية عندما تكون التدابير الأخرى الأكثر ملاءمة ممكنة، أي متوفرة بشكل معقول وقابلة للتطبيق.

على سبيل المثال، الدولة التي تقف مكتوفة الأيدي حيث يتم استخدام البنية التحتية الالكترونية على أراضيها: من قبل جماعة إرهابية للقيام بعملية إلكترونية ضد دولة أخرى، وهي تنتهك هذه القاعدة، كما هو الحال بالنسبة لدولة لا تقوم، بناءً على إخطار موثوق من دولة أخرى، باستنفاد التدابير الممكنة لإنهاء الهجوم السيبراني. [1]

[1] Finch, Brian E., and Leslie H. Spiegel. "Litigation Following a Cyber Attack: Possible Outcomes and Mitigation Strategies Utilizing the Safety

الالتزام الدولي ببذل العناية الواجبة في الفضاء السيبراني
بين التدابير الرادعة ومنع الأضرار السيبرانية العابرة

د. أسامة حمزة محمود عبد الفتاح

مجلة الدراسات القانونية والاقتصادية

كانت غالبية فريق الخبراء الدولي مع الرأي القائل بأن هذه القاعدة تنطبق أيضًا على عمليات سيبرانية محددة لم يتم إطلاقها بعد، ولكن فيما يتعلق بالخطوات المادية لتنفيذ العملية التي من المفترض أن يجري اتخاذها. فعندما تكتشف دولة أن مجموعة قامت بشكل مدمر بإرسال البرمجيات الخبيثة في البنية التحتية الإلكترونية لبورصة دولة أخرى. في هذه الحالة، يجب على الدولة أن تتصرف تجاه العملية السيبرانية لأنه من المحتمل جدًا أن تحدث وأن يتم تكرارها[1]، في مثل هذه الحالات، يكون لدى الدولة معرفة موثوقة بأن أراضيها ستُستخدم في عملية إلكترونية ضد دولة أخرى، وقد تم اتخاذ خطوة جوهرية لتفعيلها.

على النقيض من ذلك، رأت الأقلية أن الالتزام لن يدخل حيز التنفيذ حتى تكون العمليات الهجومية جارية بالفعل. وأعرب هؤلاء الخبراء عن قلقهم من أن التمسك بغير ذلك من شأنه أن يفرض عبئاً غير معقول على الدول. كما أعربوا عن قلقهم من احتمال إساءة تفسير الأنشطة الإلكترونية على أراضي دولة ما على أنها خطوات مادية، وإذا لم تتخذ الدولة إجراءات لإنهائها، فقد تكون تلك الدولة هدفاً لتدابير ردعية مشروعة مصدرها الدولة المستهدفة، وهذا الوضع من شأنه أن يزعزع الاستقرار.

ناقش فريق الخبراء الدولي حالة يصل فيها إلى علم الدولة وجود خطراً دوليًا بإجراء عملية إلكترونية بالمستوى المطلوب من الخطورة من أراضيها ضد دولة أخرى، لكن الدولة المستهدفة ليست على علم بالعملية. يثير هذا السيناريو، على وجه الخصوص، قضايا حساسة تتعلق بتبادل المعلومات الاستخباراتية. حيث أقر فريق الخبراء الدولي بأن الدول المالكة للبني التحتية المستخدمة، قد تكون مترددة في إبلاغ الدول المستهدفة بتفاصيل العملية لأن القيام بذلك قد يكشف عن قدراتها السيبرانية والاستخباراتية.

على أنه ثمة توافق بين الخبراء على أن تلك الدولة يجب أن تتصرف لإنهاء العملية غير المشروعة، مع سلطتها التقديرية في تحديد وسائل الامتثال لهذه القاعدة. على سبيل المثال، إيقاف العملية السيبرانية الضارة عن طريق إلقاء القبض على الجهات الفاعلة وإجبارها على إزالة البرامج الضارة، وإيقاف تسلل المجموعات الإرهابية إلى المرافق الحيوية للدولة الأجنبية وإنهاء العملية نفسها، أو إبلاغ الدولة المستهدفة، وبالتالي السماح لتلك الدولة باتخاذ إجراءات تصحيحية للوفاء بالتزامها بموجب هذا المبدأ تجاه الهجمات السيبرانية المنبثقة من أراضيها.

نظر فريق الخبراء الدولي فيما إذا كان مبدأ العناية الواجبة يفرض شرطًا لاتخاذ إجراءات وقائية؛ تدابير، مثل تقوية البنية التحتية الإلكترونية للفرد، لتقليل المخاطر، بخلاف تلك المحددة، للعمليات الإلكترونية المستقبلية التي تقع ضمن اختصاص هذه القاعدة. ورفضت فرضية اشتراط اتخاذ تدابير وقائية بحتة ذات طبيعة عامة. استمد الخبراء الدعم من حكم الإبادة

Act." *Santa Clara High Tech. LJ* 30 (2013): 349.

[1] راجع:

O'Connell, Mary Ellen. "Cyber security without cyberwar." *Journal of Conflict and Security Law* 17.2 (2012): 187-209.

(ISSN: 2356 - 9492)

الجماعية، والذي بموجبه "تلتزم الدولة بالمنع، وواجب العمل المقابل، الذي تعلم به الدولة ... وجود خطر جسيم من فعل الإبادة الجماعية الذي يتم ارتكابه.

اقترح الخبراء أنه نظرًا لصعوبة اتخاذ التدابير الشاملة والفعالة ضد جميع التهديدات السيبرانية المحتملة، سيكون من غير المعقول التأكيد على وجود التزام بالمنع فى السياق السيبراني. ومن شأن هذا الشرط أن يفرض على الدول عبئا لا داعي له، وهو عبء لا يوجد له أساس سواء فى القانون الحالي أو فى ممارسات الدول الحالية. وأشاروا إلى أن الدول لم تشر إلى أنها تعتقد أن مثل هذا الالتزام القانوني موجود فيما يتعلق بالعمليات السيبرانية، إما من خلال اتخاذ تدابير وقائية على هذا الأساس أو عن طريق إدانة عدم قيام الدول الأخرى باعتماد مثل هذه التدابير. وأشار الخبراء كذلك إلى أن التزامات الدول بموجب القانون الدولي لحقوق الإنسان يمكن أن تتعارض مع هذا الواجب، اعتمادًا على كيفية الوفاء به.

أخيرًا، نظرًا لأن المعرفة مطلب بموجب هذه القاعدة، سيكون من التناقض، فى رأي مجموعة الخبراء الدولية، توسيع القاعدة لتشمل العمليات الإلكترونية الافتراضية فى المستقبل. لا يمكن للدولة أن تعرف (سواء فى الواقع أو بشكل بناء) عملية إلكترونية لم يقررها الفاعل بعد. إن توسيع هذه القاعدة إلى واجب عام للمنع من شأنه أن يجعل المعرفة وفقًا لذلك المطلب الذي اتفق جميع الخبراء على أنه ضروري لخرق الالتزام.

المطلب الثالث

مبادئ قناة كورفو وواجب منع الأعمال السيبرانية

التي تنتهك حقوق الدول الأخرى

هناك قابلية للاستعانة بمبادئ القانون الدولي، كالمبدأ الخاص بمنع الإضرار بالغير فى الفضاء الإلكتروني، ومفاد المبدأ فى هذا السياق يشمل مطالبة الدول "بعدم السماح عن علم باستخدام أراضيها فى أعمال تتعارض مع حقوق الدول الأخرى". هذا الواجب هو نتيجة طبيعية للحقوق السيادية للدول فوق أراضيها، وفى جوهره، يتطلب منها حماية حقوق الدول الأخرى. [1]

[1] See, e.g., *Tallinn Manual 2.0*, *ibid* 6, at 35–36, para. 21; Milanovic and Schmitt, *supra* note 72, at 280; Schmitt, 'In Defense of Due Diligence in Cyberspace', 125 *Yale Law Journal Forum* (2015) 68; Bannelier-Christakis, 'Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?', 14 *Baltic Yearbook of International Law* (2014) 23, at 25–26;

راجع في ذلك:

Kulesza, 'Due Diligence in International Internet Law', *Journal of Internet Law* (2014) 24, at 27–28; Geiss and Lahmann, *supra* note 49, at 635; Gross, 'Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents', 48 *Cornell International Law Journal* (2015) 481, at 494; Ney and Zimmermann.

لا يشمل الالتزام فقط الأفعال التي تنتهك حقوق الدول من الغير بشكل مباشر [1]، بما فى ذلك حقوقها فى الأراضي والممتلكات [2]، بل يشمل أيضًا حقوق مواطنيها، حتى عندما يكونون فى الخارج.[3]ويشمل واجب منع ووقف الأفعال الضارة ويظهر بمجرد أن تعلم الدولة أو كان ينبغي أن تعلم[4] أن هذا الفعل ينشأ من أراضيها أو البنية التحتية الإلكترونية لديها أو يمر عبرها.[5]

على الرغم من أنه واجب وقائي فى جوهره، إلا أن الالتزام لا ينتهك إلا عندما يتحقق الضرر[6] ، ومن ثم يصعب تأصيل المسؤولية الدولية فى حالة عدم الامتثال، ما لم يحدث ضرر فعلى. غالبا يمكن تفسير هذا الهيكل المعياري، الذي يُنظر إليه على أنه عيب، بالحاجة إلى تشجيع الدول على منع الضرر بشكل مستمر لتفادي مسؤوليتها عن انتهاك بذل العناية الواجبة.

يبدو أن القاعدة 6 من دليل تالين تفكر فى صياغة خاصة للإنترنت، على غرار مفهوم بذل العناية الواجبة الذي طرحته قضية مضيق كورفو هذه الصيغة – التي تبنتها بعض الدول[1]– لها أربع سمات جديرة بالملاحظة تتمحور حول : نوع الضرر المتصور؛ مستوي الضرر؛ نطاق المهام الوقائية؛ ومتطلبات المعرفة.

---

[1] راجع:

Island of Palmas, Award, 4 April 1928, II RIAA 829 (1928), ICGJ 392 (PCA 1928), at 839.

[2] راجع:

Island of Palmas, Award,*ibid* , ICGJ 392 (PCA 1928), at 839; *Affaire des biens britanniques au Maroc espagnol (Spain v United Kingdom)*, 2 RIAA (1925) 615, at 643–644.

[3] راجع:

Corfu Channel, Judgment, 9 April 1949, ICJ Reports (1949), at 18. On the requirement of knowledge as applied to cyberspace, see *Tallinn Manual 2.0*, *ibid* 6, at 40–41.

[4]راجع:

Corfu Channel, Judgment, 9 April 1949, ICJ Reports (1949), at 18. On the requirement of knowledge as applied to cyberspace, see *Tallinn Manual 2.0*, *ibid* 6, at 40–41.

[5] راجع:

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States), Judgment, 27 June 1986, ICJ Reports (1987) 14, para. 157

[6]راجع:

Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia-Herzegovina v. Yugoslavia), Judgment, 26 February 2007, ICJ Reports 2007, at 43, para. 431 (hereinafter '*Bosnian Genocide'*); Bandelier-Christakis, *ibid*, at 37.

راجع أيضا:

contra Antonopoulos, 'State Responsibility in Cyberspace', in N. Tsagourias and R. Buchan (eds), *Research Handbook on International Law and Cyberspace* (2015) 55, at 69.

[6] راجع:

e.g., Comments by the Member States on the initial pre-draft of the OEWG report: France, *supra* note 47, at 3; The Netherlands, Letter of 5 July 2019

(ISSN: 2356 - 9492)

- **نوعية الضرر المتوخي فى العمليات السيبرانية استنادا لمبادئ قناة كورفو**

يفترض التعليق على القاعدة 6 من دليل تالين أن الفعل الذي "يؤثر على حقوق الدول الأخرى" يجب أن يُفهم على أنه فعل غير مشروع دوليًا.[2] كما يشير إلى أن هذا لا ينبغي أن يشمل فقط انتهاكات القانون الدولي المنسوبة إلى الدول، ولكن أيضًا الممارسات التي كان من الممكن أن تكون غير قانونية إذا ارتكبت من قبل الدولة "المضيفة" التي تستغل البنية التحتية لديها فى الهجوم السيبراني، بغض النظر عن الاسناد. لكن بالاستناد للمبادئ التي أكدتها قضية قناة كورفو، يمكن الاعتراف بمسؤولية الدولة بسبب عدم الاجتهاد فى منع أو وقف أفعال الجهات الفاعلة غير الحكومية.[3]

فى رأينا، لا تعكس هذه اللغة المفهوم الوارد بالمادة 6 من دليل تالين، فعلى الرغم من أن غالبية الأعمال التي تتعارض مع حقوق الدول الأخرى هي أفعال غير مشروعة دوليًا، يجب أن يؤخذ بعين الاعتبار. أولاً، ليست كل الأفعال التي ترتكبها الجماعات من غير الدول والتي تتعارض مع حقوق الدول الأخرى تشكل أيضًا أفعالًا غير مشروعة دوليًا أو كانت ستعد كذلك إذا ارتكبتها الدولة انطلاقاً من إقليمها.[4]

ثانياً: إذا كان السلوك غير قانوني إذا ارتكبته الدولة المضيفة، يجب على المرء أن يأخذ بعين الاعتبار الظروف الملموسة السائدة فى ذلك الوقت أو التزامات الدولة المضيفة بشكل تجريدي سيما فى السياق السيبراني.[5] ويتعلق هذا المعيار بوجود ظروف تمنع عدم المشروعية، ولكنها مع ذلك تمنح الدولة "الضحية" الحق فى المطالبة بالتعويض عن خسارة مادية.[6]

وبالتالي، فإن وضع إطار عام لنوع الضرر على غرار قضية قناة كورفو على أنه "أفعال غير مشروعة دوليًا" ليس دقيقًا تمامًا. ولا توصيفها على أنها "أفعال تؤثر على حقوق الدول الأخرى". هذا لأنه لا تؤثر جميع الأفعال فقط على حقوق الدول من الغير – مثل بعض حالات التجسس السيبراني[7].

---

[2] Johanna Weaver, Submission of Australia's independent expert to the United Nations Group of Governmental Experts on advancing responsible State behaviour in cyberspace in the context of international security (2020), at 4, available at www.dfat.gov.au/sites/default/files/submission-by-australias-representative-to-the-gge-norm-implementation- may-2020.pdf;

Boyle, Alan E. "State Responsibility and International Liability for Injurious Consequences of Acts Not Prohibited by International Law: A Necessary Distinction?." *International & Comparative Law Quarterly* 39.1 (1990): 1-26.[2] راجع في ذلك:

Sander, 'Democracy Under The Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections', 18 *Chinese Journal of International Law* (2019) 1, at 25–26; Milanovic and Schmitt, *supra* note 72, at 280.

[3] لا توجد إشارة إلى الأفعال التي تؤثر فقط على حقوق الدول الأخرى أو الأفعال غير المشروعة دوليًا بالكامل، أي انتهاكات القانون الدولي "المنسوبة إلى دولة ما. بدلاً من ذلك، فإن اللغة المستخدمة في قناة كورفو هي لغة "الأفعال المخالفة لحقوق الدول الأخرى".

Corfu Channel, Judgment, 9 April 1949, ICJ Reports (1949), at 22.

Hathaway, Oona A., et al. "Ensuring responsibility: Common article 1 and state responsibility for non-state actors." *Tex. L. Rev.* 95 (2016): 539.

[4] during a cross-border non-international armed conflict, the targeting of foreign enemy combatants by a non-state group is contrary to the rights of the foreign state to protect their nationals, yet this may not amount to an internationally wrongful act if committed by the host state itself.

[5] ARSIWA, *supra* note 50, art. 27.

[6] ARSIWA, *supra* note 50, art. 27.

[7] راجع

Stinissen, Jan, and Kenneth Geers. "A legal framework for cyber operations in Ukraine." *Cyber War in Perspective: Russian Aggression*

علاوة على ذلك، لا يلزم أن تؤدي الأعمال غير المشروعة بموجب مبادئ قناة كورفو إلى ضرر مادي. هذا مهم بشكل خاص فى الفضاء السيبراني، حيث العديد من الأضرار ليس لها تأثير مادي مباشر ومع ذلك قد تعوق تشغيل الوظائف الحكومية أو الخاصة، مثل تعطيل الخدمات المالية أو البنية التحتية والخدمات الحكومية.[1]

يمكن العثور على مثال للأنشطة الإلكترونية "المخالفة لحقوق الدول الأخرى" فى إدانة المملكة المتحدة الأخيرة "للنشاط غير المسؤول الذي تقوم به الجماعات الإجرامية" و "الهجمات الإلكترونية من قبل الدول والجهات الفاعلة من غير الدول" خلال وباء COVID-19[2] تتألف الأعمال المعنية من "حملات إلكترونية خبيثة تستهدف مؤسسات الرعاية الصحية والبحث الطبي الدولية المشاركة فى الاستجابة لفيروس كورونا"، والتي كانت تتعارض بوضوح مع حقوق الدول المستهدفة، بغض النظر عن أي ضرر مادي تسبب فيه.

تشترط القاعدة 6 من دليل تالين، أن يكون للفعل غير المشروع دوليًا "عواقب وخيمة" على الدول الأخرى.[3] بينما لم تتضمن المبادئ المستقاة من قضية قناة كورفو إشارة لمستوي الضرر. وبدلاً من ذلك، يبدو أنه تم استعارته من مبدأ عدم الضرر[4]، الذي يتطلب ضررًا جسيمًا عابرًا للحدود، ولكن ليس بالضرورة فعلًا مخالفًا لحقوق الدول الأخرى. ومثل الكثير من الأدبيات الموجودة حول العناية الواجبة، يبدو أن الدليل قد دمج المبدأين فى قاعدة واحدة أو مبدأ واحد يتطلب العناية الواجبة فى الفضاء السيبراني.[5]

ومع ذلك، هذا لا يعني أن الإخفاق فى منع أو وقف أي ضرر إلكتروني، بغض النظر عن خطورته، يرقى إلى تطبيق القواعد التي رسختها قضية مضيق كورفو. فالدول ليست مسؤولة عن الفشل فى تجنب الاضطرابات الطفيفة أو التي لا تذكر، مثل التشويه المؤقت للمواقع الحكومية غير الأساسية. لكن هذا ليس لأن المبدأ يحتوي على حد معين للضرر. بل لأن هذه الأضرار قد لا تتعارض مع حقوق الدول الأخرى.

على سبيل المثال، فى العديد من الظروف، قد لا يتعارض مجرد تهريب البيانات أو فسادها – وفقًا للبعض – مع الحقوق السيادية للدولة الضحية على أراضيها[6] أو حقها فى عدم التعرض للتدخل الأجنبي. بينما منع أو إيقاف العمليات السيبرانية الضارة التي تتداخل

against Ukraine. NATO CCD COE Publications, Tallinn (2015): 123-134.

[1] *Tallinn Manual 2.0, ibid* , at 38.

[2] Press Release, 'UK Condemns Cyber Actors Seeking to Benefit from Global Coronavirus Pandemic' (5 May 2020), available at www.gov.uk/government/news/uk-condemns-cyber-actors-seeking-to-benefitfrom- global-coronavirus-pandemic

[3]Comments by Member States on the initial pre-draft of the OEWG report: Canada, *supra* note 47, at 3.

[4] Schmitt, '"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law', 19 *Chicago Journal of International Law* (2018) 30, at 54

[5]Milanovic and Schmitt, 'Cyber Attacks and Cyber (Mis)information Operations during a Pandemic', 11 *Journal of National Security Law & Policy* (2020) 247, at 280

[6] Buchan, Russell, and Iñaki Navarrete. "Cyber espionage and international law." *Research Handbook on International Law and Cyberspace*.

(ISSN: 2356 - 9492)

مع الوظائف السيادية بطبيعتها للدولة أو الاحتفاظ بولايتها القضائية، مثل قدرتها على وضع سياسات الصحة العامة أو إجراء الانتخابات، قد ينتهك مبدأ قناة كورفو. وهذا يشمل الأفعال التي تحدث بالكامل داخل أراضي الجهة المسؤولة، حيث لا يتطلب مبدأ قناة كورفو العبور المادي للحدود الإقليمية.[1]

• نطاق الالتزام ببذل العناية الواجبة تجاه النشاط السيبراني العدائي

رفض فريق الخبراء المشتركين فى تالين 2.0 وجهة النظر القائلة بأن على الدول "واجب عام للوقاية" ، أي واجب منع العمليات السيبرانية الخبيثة فى المستقبل، وذلك على غرار الالتزام الدولي بمنع الإبادة الجماعية.[2] فالالتزام يسري فقط على العمليات الجارية ، أو الوشيكة على الأكثر فيما يتعلق بالفضاء الإلكتروني .[3]

وهذا من شأنه أن يقصر نطاق الواجب على الالتزام بوقف العمليات الإلكترونية الضارة. وقد تم تبرير هذا الرأي من خلال الافتقار الحالي للجدوى التقنية لمنع الأضرار عبر الإنترنت[4] ، نظرًا لتكرارها وسرعتها، فضلاً عن مخاوف انتهاك حقوق الانسان، سيما الحق فى الخصوصية.

ولكن الأخذ بتلك القاعدة على إطلاقها قد يجانب الصواب، فالتزامات الحماية، بما فى ذلك ما أقرته قواعد كورفو، مرنة بطبيعتها. فهي تعتمد على قدرة كل دولة وموقفها لمنع أو وقف الضرر المعني، سواء كانت العملية الإلكترونية قد نشأت من أراضيها أو مرت عبرها.[5]

وبالتالي، فإن الدولة ليست مطالبة بفعل المستحيل، وقد يُطلب من الدول اعتماد تدابير متباينة فى ظروف مختلفة. فتكشف ممارسات الدول فى هذا الصدد أنه تم اعتماد مجموعة من التدابير لمنع العمليات السيبرانية الضارة. وقد اشتملت هذه على مراقبة التهديدات الإلكترونية [6] وإصدار التنبيهات والإرشادات لمعالجة ثغرات البرامج أو الأجهزة.[7]

Edward Elgar Publishing, 2021.at 51

[1] M. Schmitt (ed.), *Tallinn Manual 2.0* (2nd ed. 2017) 30, rule 6; 43 at 36, para. 23.

[2] *Ibid*., at 31, para. 5; 41–42, para. 42; 44–45, paras 7, 10

[3] *Ibid.*, at 43–44, paras 3–4

[4] Takano, 'Due Diligence Obligations and Transboundary Environmental Harm: Cybersecurity Applications', 36 *Laws* (2018) 7, at 8; Comments by Member States on the initial pre-draft of the OEWG report: Canada, at 3; Comments by Member States on the initial pre-draft of the OEWG report: Ecuador, at 2.

[5] similarly Comments by Member States on the Initial Pre-Draft of the OEWG Report, available at www.un.org/disarmament/open-ended-working-group/ (see individual comments from the Czech Republic, at 2; the Netherlands, §§ 17–18; Japan, at 1, 5; Austria, at 2; Germany, at 2–3). See also HRC, Res. 32/13,

[6] e.g., Cybersecurity Law (promulgated by the Standing Committee of the National People's Congress, 7 November 2016, effective 1 June 2017), arts. 21(3), 51 (China); UK Network and Information Systems Regulations 2018, 10 May 2018, Part II, s. 5(2)(a); Japan Cybersecurity Strategy (27 July 2018), at27–29, 31, 35.

[7] e.g., US Cybersecurity & Infrastructure Security Agency, Alert: Technical Approaches to Uncovering and Remediating Malicious Activity, AA20-245A (1 September 2020), available at https://us-cert.cisa. gov/ncas/alerts/aa20-245a; Canada's Implementation of the 2015 GGE Norms, at 5, available at www. un.org/disarmament/wp-content/uploads/2019/11/canada-implementation-2015-gge-norms-nov-16-en.pdf (last visited 17 July 2021).

ومع ذلك، فإن هذه المرونة ليست عذراً للتقاعس عن العمل. الشرط المنطقي المسبق للالتزامات الوقائية للسلوك هو التزام منفصل بوضع الحد الأدنى من الرقابة المعقولة على البنية التحتية الحكومية، مما يمكّن الدولة من ممارسة الدرجة اللازمة من بذل العناية الواجبة.[1]

فى الواقع، إذا تمكنت دولة ما من الادعاء ببساطة أنها بذلت قصارى جهدها لهذا الغرض، فيمكن التهرب بسهولة من الواجب الرئيسي المتمثل فى منع الضرر. ومع ذلك، فإن محتوى هذا الالتزام ببناء القدرات – النتيجة المطلوبة من كل دولة – لا يبدو أنه ثابت، ولكنه يعتمد على الظروف، ولا سيما الموارد البشرية والمالية المتاحة.

وهكذا، فإن مبدأ قناة كورفو يحتوي على طرفين متميزين لكن مترابطين

أولاً، هناك التزام بإنشاء الحد الأدنى من أجهزة الدولة – وهو واجب "بناء القدرات" الأساسي. تشير ممارسات الدول الحديثة فى السياق السيبراني إلى أن هذا الواجب قد يشمل اعتماد وتنفيذ إطار قانوني وطني مناسب للتصدي للجرائم الإلكترونية وإساءة استخدام تكنولوجيا المعلومات والاتصالاتICTs.

ثانيًا، هناك التزام بسلوك لممارسة العناية الواجبة لمنع ووقف العمليات السيبرانية المحتملة أو الفعلية التي تتعارض مع حقوق الدول الأخرى، إلى حد قدرة الدولة على التصرف فى هذه الظروف. وبالتالي، فإن قدرة الدولة على التصرف لا تؤدي فقط إلى التزامها بالسلوك، بل تحد أيضًا من التدابير التي يتعين عليها اعتمادها وتعديلها.

ومع ذلك، كما هو الحال مع واجبات الحماية الأخرى ، قد تتغير التدابير المطلوبة على أساس التطورات التكنولوجية الجديدة. قدر الإمكان. بينما قد تثير هذه التقنيات مخاوف بشأن الخصوصية والحقوق الأخرى، يكفى ملاحظة أن تنفيذ هذه التدابير يجب أن يتماشى مع تدابير العناية الواجبة بموجب مبدأ قناة كورفو مع القانون الدولي لحقوق الإنسان وقواعد القانون الدولي الأخرى.[2]

• متطلبات المعرفة وفقا لمبادئ قضية كورفو

على أي حال، لا يتم تفعيل الالتزام بالتصرف وفقًا للمبادئ التي أرستها قضية مضيق كورفو إلا عندما تكون الدولة على علم، أو كان ينبغي أن تعلم، بوجود خطر جسيم يتمثل فى حدوث عملية إلكترونية غير قانونية، بغض النظر عن مدى بُعد هذه المخاطر.[1]

[1] ILC, Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries, in Report of the International Law Commission on the work of its fifty-third session (23 April–1 June and 2 July–10 August 2001), UN Doc. A/56/10, 144, at 148–149, at 155, Commentary to art. 3, paras 15–17.

[2] Bannelier-Christakis, 'Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?', 14 *Baltic Yearbook of International Law* (2014) 23, at 31

(ISSN: 2356 - 9492)

وبالتالي، فإن العامل الحاسم هو مقدار المعلومات واليقين الذي تمتلكه الدولة بشأن الفعل الضار المعني، وليس مدى قربه.[2] وينطبق الشيء نفسه على دول العبور، إلى الحد الذي يكون لديها معرفة فعلية أو بناءة بمخاطر العملية الإلكترونية غير القانونية، فضلاً عن القدرة على منعها.

فى الوقت نفسه، لا يبدو أن مبدأ قناة كورفو يفرض على الدول واجب السعي بنشاط للحصول على معرفة بالأفعال المنبثقة من أراضيها أو العابرة لها والتي قد تتعارض مع حقوق الدول الأخرى. ما يتطلبه الأمر هو الحد الأدنى من البنية التحتية الحكومية أو القدرة التي تمكن الدول من اكتساب مثل هذه المعرفة ومع ذلك فقد تم اقتراح أن شرط المعرفة يمكن إثباته من خلال افتراض (قابل للنفى) عندما تنشأ عملية إلكترونية غير قانونية فى بنية تحتية إلكترونية غير تجارية تحت السيطرة الحكومية الحصرية للدولة.[3]

قد يمنع هذا الدول من التهرب بسهولة من التزاماتها الوقائية من خلال إنكار المعرفة بعملية إلكترونية غير قانونية معينة. باختصار، "كلما زاد عدد الدول التي تستطيع القيام بها، كان يجب عليها فعل المزيد"[4]

ولا يمكننا إغفال مدي تقدم الدولة كعامل مؤثر فى تحديد مدي قدرتها على اتخاذ التدابير اللازمة [5]. لذلك، لا ينبغي أن يكون الامتثال لمبدأ قناة كورفو فى الفضاء الإلكتروني عملاً لا يمكن التغلب عليه: فهو يتطلب ببساطة من الدول بناء الحد الأدنى من القدرات المتوقعة منها بشكل معقول، فضلاً عن توظيف هذه القدرة بجدية فى محاولة حماية حقوق الدول الأخرى.[6] فى كثير من الظروف، يكفى الإبلاغ عن الحوادث الإلكترونية وتبادل المعلومات بشأنها.[7]

---

[1] اعتمد حكم الأغلبية الصادر عن محكمة العدل الدولية على لاستنتاج بأن زرع حقل الألغام "لا يمكن أن يتم بدون علم ألبانيا". استنتجت الأغلبية معرفة ألبانيا وفقًا لمعايير موضوعية. ولم يكن مطلوبًا من المملكة المتحدة إثبات أن ألبانيا تعرف (شخصيًا) بوجود الألغام. والجدير بالذكر أن اثنين من المعارضين (القاضي أزيفيدو والقاضي كريلوف) اعتبروا أن ألبانيا تخضع لواجب مستمر لإبلاغ عن التهديدات التي يمكن توقعها بشكل معقول فى أراضيها.

فى قضية الإبادة الجماعية البوسنية، وجدت المحكمة أن التزام الدولة بمنع وقوع الإبادة الجماعية "فى اللحظة التي علمت فيها الدولة، أو كان ينبغي أن تعلم بها عادة، بوجود خطر جدي بارتكاب الإبادة الجماعية". إن الانخراط فى الالتزام بمنع الإبادة الجماعية يرقى إلى إطلاق اليقظة الإلكترونية إذا كان ينبغي للدولة أن تكون على علم بشكل معقول بحدوث الهجوم. تشير لغة هذه الحالات إلى أنه ينبغي إثبات المعرفة البناءة إذا كان لدى الدولة معلومات تفيد باحتمال وقوع هجوم إلكتروني انطلاقا من إقليمها أومن خلال البنية التحتية الخاضعة لسيادتها وفشلت فى إجراء مزيد من التحقيقات أو اتخاذ التدابير اللازمة لتجنب وقوعه.

Kolb, *ibid* 34, at 123–124; *Tallinn Manual 2.0*, *supra* note 6, at 45, para. 9 and *ibid*., at 44–45, para. 7, citing *Bosnian Genocide*, Judgment, 26 February 2007, ICJ Reports 2007, *supra* note 85, para. 431

[2] *mutatis mutandis*, *Bosnian Genocide*, Judgment, 26 February 2007, ICJ Reports 2007, para. 436. *mutatis mutandis*, *Bosnian Genocide*, Judgment, 26 February 2007, ICJ Reports 2007, para. 436.

[3] Heintschel von Heinegg, 'Legal Implications of Territorial Sovereignty in Cyberspace', in C. Czosseck, R. Ottis and K. Ziolkowski (eds), *2012 4th International Conference on Cyber Conflict* (2012) 7, at 17.

[4] Heieck, *Symposium: A Duty to Prevent Genocide – Due Diligence Obligations among the P5 (Part One)* (2018), available at http://opiniojuris.org/2018/12/10/symposium-a-duty-to-prevent-genocide-due-diligenceobligations-among-the-p5-part-one/ (emphasis added).

[5] *راجع*

Collection générale des décrets rendus par la Convention Nationale: *Mois de mai 1793* (1793), at 72. The adage has been popularized by the Spiderman comic books.

[6] See Kolb, 'Reflections on Due Diligence Duties and Cyberspace', 58 GYIL (2015) , at 123.

[7] راجع

Gross, *ibid 112*, at 506.

See also Secretariat Général de la Défense et la Sécurité Nationale (France), Revue stratégique de cyberdéfense (12 March 2018), at 83–84, available at www.sgdsn.gouv.fr/ evenement/revue-stratégique-de-cyberdefense

المطلب الرابع

الالتزام بمنع الضرر السيبراني العابر للحدود

على الرغم من أوجه التشابه بينهما، لا سيما مطلب "القدرة على التصرف"، يجب التمييز بين مبادئ "منع الضرر" و "قناة كورفو"، نظرًا لعناصرها المتميزة والعواقب القانونية وذلك من حيث. (نوع الضرر؛ مستوي الضرر؛ متطلبات المعرفة؛ والعواقب القانونية) لعدم الامتثال للواجب.[1]

1- نوع الضرر

على عكس مبدأ قناة كورفو، لا يتطلب مبدأ عدم الضرر ارتكاب فعل مخالف لحقوق الدول الأخرى، ولكنه يغطي أي "ضرر جسيم عابر للحدود" أو خطر حدوثه، حتى لو كان ناتجًا عن أنشطة قانونية أو لم يكن هناك حق للدولة تم تقويضه.[2] فى "الفضاء الإلكتروني" كما هو الحال فى "النطاق" التقليدي، مثل الأرض والجو والبحر، يحدث عبور الحدود عندما يحدث ضرر أو يشعر به فى إقليم – أو فى أماكن أخرى أو بنى تحتية خاضعة لولاية أو سيطرة– دولة أخرى غير دولة المنشأ.[3]

بينما تساءل البعض عما إذا كان هذا الالتزام ينطبق خارج الإطار القانوني البيئي، هناك أسباب قوية تشير إلى أنه يغطي أي نوع من الضرر العابر للحدود.[4] بما فى ذلك الضرر الناجم عن تكنولوجيا المعلومات والاتصالات. وعلى وجه الخصوص، وجدت هيئة التحكيم فى Trail Smelter أن الالتزام بعدم التسبب فى الضرر العابر يشمل أي "عمل ضار" لإقليم دولة أخرى أو أشخاص أو ممتلكات فيها.[5]

---

[1] راجع:

See ILC, Summary Record of the 1251st Meeting, Topic: State Responsibility, A/CN.4/SR.1251, Extract from the Yearbook of the International Law Commission 1974 vol. 1, available at https://legal.un.org ilc/documentation/english/summary_records/a_cn4_sr1251.pdf (last accessed 17 July 2021), at 7 .

راجع أيضا :

Crootof, Rebecca, and Oona A. Hathaway. "The law of cyber-attack." *California Law Review* 100.4 (2012): 817., at 600; Walton, 'Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law', 126 *Yale Law Journal* (2016) 1460, at 1486–1487; Sander, *ibid*, at 49.

[2]ILC, Draft Articles on Prevention, *ibid* 21, at 150, Commentary to Article 1, para. 6; 152, Commentary to art. 2, para. 5.

Crootof, 'International Cybertorts: Expanding State Accountability in Cyberspace', 103 Cornell Law Review (2018) *AT* 103,

[3] هذا هو الحد الذي تظل فيه تكنولوجيا المعلومات والاتصالات متجذرة في المادية، ويستخدمها البشر أو يتحكمون فيها، حتى إذا كانت بعض الأنشطة عبر الإنترنت تسبب آثارًا غير مادية في المقام الأول.

[4] See ILC, Draft Articles on Prevention, *ibid* 21, at 148–149; Crootof, *ibid* 148, at 603–604;

راجع:

Walton, 'Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law', 126 Yale Law Journal (2016) at 1465.

[5] *Trail Smelter*, (*United States v. Canada*) (1941) 3 RIAA 1911, at 1963

(ISSN: 2356 - 9492)

وفقا لمحكمة العدل الدولية، تم منح هذا الاستنتاج العام فى سياق التزام الدولة "باستخدام جميع الوسائل المتاحة لها من أجل تجنب الأنشطة التي تحدث فى أراضيها، أو فى أي منطقة خاضعة لولايتها القضائية، مما يتسبب فى ضرر كبير لبيئة دولة أخرى ". [1]

ومع ذلك، فإن المحكمة سلطت الضوء على وجه التحديد على وجود هذا الواجب، "مؤكدة أنه لا يوجد استثناء خاص بالقضايا المتعلقة بالبيئة"[2]، ما ينتفى معه بحال من الأحوال تطبيق عدم الإضرار كمبدأ عام، كما أوضحت لجنة القانون الدولي فى مسودتها.[3]

حيث أنه تنطبق المواد المتعلقة بمنع الضرر العابر للحدود على "الضرر الذي يلحق بالأشخاص أو الممتلكات أو البيئة"، والذي يتضمن "الآثار الضارة على أمور مثل، على سبيل المثال، صحة الإنسان، أو الصناعة، أو الممتلكات، أو البيئة أو الزراعة".[4] لهذه الأسباب، أعرب العديد من المعلقين بشكل مقنع عن وجهة نظر مفادها أن مبدأ عدم الضرر ينطبق على مجموعة من الأضرار التي تُرتكب من خلال تكنولوجيا المعلومات والاتصالات، سواء كانت تتعارض مع حقوق الدول الأخرى أم لا. [5]

ومن المسلم به أن العديد من العمليات السيبرانية الضارة حتماً ستتعارض مع قاعدة واحدة على الأقل من قواعد القانون الدولي، ومن المرجح أن تتعارض مع حقوق الدول الأخرى. [6] فعلى وجه الخصوص، إذا كانت السيادة قاعدة ثابتة فى القانون الدولي، فإن التدخلات فى الشبكات أو الأنظمة الحكومية من قبل دولة أخرى والتي تسبب ضررًا ماديًا أو وظيفيًا فى أراضي دولة أخرى قد تنتهك هذه القاعدة.[7]

وبالمثل، فإن التدخل الإلكتروني القسري فى المهام الحكومية الحصرية للدولة، مثل عد الأصوات أو الأنظمة الوطنية المصرفية، من شأنه أن ينتهك مبدأ عدم التدخل.[8] وبقدر ما تنتهك هذه الهجمات الإلكترونية حقوق الأفراد، مثل حقهم فى انتخابات حرة أو خصوصية أو ملكية، فمن المحتمل أن تنتهك القانون الدولي لحقوق الإنسان.

يجب أن يكون هذا صحيحًا على الأقل بالنسبة لالتزامات حقوق الإنسان السلبية[1]، التي قد يتم تفعيل اختصاص الدولة فيها من خلال ممارسة السيطرة على النشاط المعني[2]، البنية التحتية للاتصالات الرقمية[3] أو التمتع بحقوق الإنسان للضحية. [4] بغض النظر عن القرب المادي بين الجاني والضحية.

[1] لبحث تلك المسألة، نظرت لجنة الخبراء في السوابق التي لا تتعلق فقط بالمخاطر البيئية، ولكن أيضًا باستخدام الأسلحة ومعاملة الأجانب. يرتبط ارتباطًا وثيقًا بقاعدة قناة كورفو *Pulp Mills*, Judgment, 20 April 2010, ICJ Reports (2010), para. 101.

[2] nuclear weapons, Advisory Opinion, 8 July 1996, ICJ Reports (1996), para. 29.

[3] ILC, Draft Articles on Prevention, *ibid* 21, art. 2, at 153, para. 8; Commentary, at 152, para. 4 (emphasis added). See also Robert Q. Quentin-Baxter, Special Rapporteur, Fourth Report on International Liability for Injurious Consequences Arising out of Acts Not Prohibited by International Law, UN Doc. A/ CN.4/373 and Corr.1&.2 (27 June 1983), para. 17 (clarifying that 'there was never an intention to propose a reduction in the scope of the topic to questions of an ecological nature').

[4] ILC, Draft Articles on Prevention, ibid 21, art. 2, at 153, para. 8; Commentary, at 152, para. 4 (emphasis added). See also Robert Q. Quentin-Baxter, Special Rapporteur, Fourth Report on International Liability for Injurious Consequences Arising out of Acts Not Prohibited by International Law, UN Doc. A/ CN.4/373 and Corr.1&.2 (27 June 1983), para. 17 (clarifying that 'there was never an intention to propose a reduction in the scope of the topic to questions of an ecological natur

[5] e.g., Crootof *ibid* 148, at 603–604; Walton, ibid 148, at 1480–1482, 1497; Sander, supra note 88, a 49–50; Reinisch and Beham, supra note 11, at 104–106; Dörr, supra note 78, at 93; Buchan, supra note 1, at 439–452; Okwori, ibid 74, at 210; Takano, supra note 110. See also Interim Report of the Ad-Hoc Advisory Group on Cross-Border Internet, supra note 55, paras 60–65.

[6] e.g., Crootof, *ibid* 148, at 603–604; Walton, ibid 148, at 1480–1482, 1497; Sander, supra note 88, a 49–50; Reinisch and Beham, supra note 11, at 104–106; Dörr, supra note 78, at 93; Buchan, supra note 1, at 439–452; Okwori, ibid 74, at 210; Takano, supra note 110. See also Interim Report of the Ad-Hoc Advisory Group on Cross-Border Internet, supra note 55, paras 60–65.

[7] Tallinn Manual 2.0, ibid 6, at 19–22; Schmitt and Vihul, 'Respect for Sovereignty in Cyberspace', 95 Texas Law Review (2017) 1639, at 1648–1649. Granted, controversies as to the existence and extent of such rule may lead to diverging views about the occurrence of 'harm'. This does not deny, however, that if such harm may be established the 'no-harm' principle would apply.

[8] , Watts, 'Low-Intensity Cyber Operations and the Principle of Non-Intervention', in J. D. Ohlin et al. (eds), Cyber War: Law and Ethics for Virtual Conflicts (2015) 250, at 257. But see Sander, supra note 88, at 20

ومع ذلك، لا يلزم انتهاك أي قاعدة من قواعد القانون الدولي حتى يتم تطبيق مبدأ عدم الضرر. وهذا يعطي المبدأ نطاقًا واسعًا محتملًا للتطبيق الذي يكون مناسبًا بشكل خاص للفضاء السيبراني، حيث تستمر المناقشات حول طبيعة السيادة والولاية القضائية والتدخل المحظور والإنصاف فى المنازعات ذات الصلة بالعمليات السيبرانية ذات الأضرار المحدودة. [5]

على الرغم من أن مبدأ عدم الضرر يتطلب عبور الحدود الدولية[6]. لا يقتصر الأمر على الأضرار المادية.[7] يُشار إليها غالبًا باسم "المحاكمات الإلكترونية الدولية"[8]، قد تتضمن هذه العمليات العابرة للحدود خسارة مالية كبيرة أو ضررًا وظيفيًا و / أو ماديًا للشبكات، أو الأنظمة الخاصة، أو تلف البيانات، أو ضياعها، أو الإضرار بالسمعة، أو العواقب السياسية.[9]

وفى الوقت نفسه، لا يتم تطبيق مبدأ عدم الضرر إلا من خلال الضرر الجسيم العابر للحدود أو خطر حدوثه. على حد تعبير لجنة القانون الدولي: "يجب أن نفهم أن كلمة" significant " أن الضرر لا يلزم أن يكون على مستوى" خطير "أو" جوهري ". وإن تعين وجود تأثير ضار حقيقي على أمور مثل، على سبيل المثال، صحة الإنسان، أو الصناعة، أو الممتلكات، أو البيئة، أو الزراعة فى دول أخرى يشمل الضرر الجسيم "، فى هذا السياق،" التأثير المشترك لاحتمال وقوع حادث وحجم تأثيره الضار ".[10]

وبالتالي، فهو يغطي الأنشطة التي تنطوي على "احتمالات ضعيفًة للتسبب فى ضرر كارثي"، وكذلك العمليات التي يوجد فيها "احتمال كبير للتسبب فى ضرر جسيم". فى الفضاء الإلكتروني، ويشمل ذلك الضرر المادي، أو الوظيفي، أو غير المادي للأجهزة، أو البرامج، أو البيانات، أو الأفراد. قد تكون هذه الأضرار ناجمة عن حملات التضليل عبر الإنترنت، لا سيما تلك التي تحدث أثناء الانتخابات[11] أو أزمات الصحة العامة[12]، فضلاً عن استغلال نقاط الضعف فى منتجات سلسلة توريد تكنولوجيا المعلومات المستخدمة على نطاق

[1] See M. Milanovic, Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy (2011), at 209; Sander, supra note 88, at 39–43. On extraterritorial jurisdiction over online harms, see Section 4.C.1.

[2] Sergio Euben Lopez Burgos v. Uruguay, HRComm Communication No. 52/1979, UN Doc. CCPR/ C/13/D/52/1979, 29 July 1981, § 12.3; Lilian Celiberti de Casariego v. Uruguay, HRComm Communication No 56/1979, UN Doc. CCPR/C/13/D/56/1979, 29 July 1981, § 10.3

[3] Report of the Office of the UN High Commissioner for Human Rights: The Right to Privacy in the Digital Age, UN Doc. A/HRC/27/37, 30 June 2014, § 34.

[4]HRComm, General Comment No. 36, supra note 43, § 63; ECtHR, Issa and Others v. Turkey, Appl. no. 31821/96, Judgment of 16 November 2004, para. 71; ECtHR, Jaloud v. The Netherlands, Appl. no. 47708/08, Judgment of 20 November 2014, para. 152.

Walton, ibid 148, at 1497–1499, 1512[5]

[6] 4 ILC, Draft Articles on Prevention, ibid 21, at 152–153, art. 3(c)–(e) and Commentary, paras 9–12

[7] According to the ILC, the Draft Articles on Prevention were limited to physical harms 'to bring this topic within a manageable scope'. See ibid., at 151; Commentary to art. 1, para. 16; Trail Smelter (United States v. Canada) (1941) 3 RIAA 1911, at 1926–1927; nuclear weapons, Advisory Opinion, 8 July 1996, ICJ Reports (1996), paras 29 and 36. See also Crootof, *ibid* 148, at 603; Walton, supra note 103, at 1482; Buchan, supra note 1, at 449–450; Takano, supra note 110, at 1.

[8] See Crootof, *ibid* 148, at 588–589, 592, 595–597; Walton, ibid 148, at 1513.

[9] 7 Crootof, ibid 103, at 608–609; Gross, ibid, at 484; Takano, ibid, at 6–7. See also US Department of Defense Cyber Strategy (2015), at 5, available ahttps://archive.defense.\gov/home/features/2015/0415_cyberstrategy/final_2015_dod_cyber_strategy_for_web.pdf

[10] ILC, Draft Articles on Prevention, ibid 21, at 152, Commentary to art. 2, para. 4 (emphases in the original).

[12]Milanovic and Schmitt, supra note 72. See also Robinson and Spring, 'Coronavirus: How Bad Information Goes Viral', BBC (2020), available at www.bbc.co.uk/news/blogs-trending-51931394; Rankin, 'Russian media "spreading Covid-19 disinformation"', Guardian (2020), available at www. theguardian.com/world/2020/mar/18/russian-media-spreading-covid-19-disinformation.

Committee on Economic, Social and Cultural Rights (CESCR), General Comment No. 14: The Right to the Highest Attainable Standard of Health (Article 12), E/C.12/2000/4, 11 August 2000, § 34. On due diligence obligations applying in relation to COVID-19, see Coco and

(ISSN: 2356 - 9492)

واسع.[1] وإن كان تحديد ما يرقى إلى الضرر الجسيم يتضمن تقييمًا شخصيًا، يختلف باختلاف الظروف السائدة فى إطار زمني محدد، ولا سيما المعرفة العلمية الحالية والقيمة الاقتصادية للنشاط أو السلعة المعنية ومدى الضرر الناجم.[2]

وينطلق مبدأ عدم الضرر والمعايير المستقاة من قضية مضيق كورفو من المعرفة الفعلية أو البناءة بالمخاطر واستبعاد الأضرار غير المتوقعة. الأمر الذي يتطلب تدابير أكثر استباقية لليقظة أو المراقبة،[3] على أساس خطورة الضرر. ومرة أخرى، فإن اشتراط توخي اليقظة المستمرة فى استخدام تكنولوجيا المعلومات والاتصالات أو أي تقنية أخرى فى هذا الشأن – يعتمد على قدرة كل دولة على التصرف، ويجب أن تكون متسقة مع عمليات الربط الدولية الأخرى. بشكل عام، كلما كان من المجدي أكثر للدول أن تتنبأ بأن عملية سيبرانية مؤذية وشيكة، زادت درجة الاجتهاد المطلوب.

ومع ذلك، يجب دائمًا تقييم هذه المرونة مقابل عنصر أساسي لمبدأ عدم الضرر، أي واجب الدولة فى "مواكبة التغيرات التكنولوجية والتطورات العلمية"[4]، الذي يشير إلى ضرورة المشاركة باستمرار فى بناء القدرات، إلى الحد الممكن فى ظل الظروف.[5]

الأثار القانونية للأضرار الناشئة عن استخدام البنية التحتية فى الهجمات السيبرانية

كما رأينا سابقًا، يتم تفعيل مبدأ قناة كورفو بمجرد أن تعرف الدولة أو كان ينبغي أن تكون على علم بالخطر الجسيم لعمل مخالف لحقوق الدول الأخرى المنبثقة من أراضيها أو تمر عبر بنيتها التحتية ويتم انتهاكه عند حدوث الفعل المعني.[6]

فى هذه المرحلة، يتم التعامل مع مسؤولية صاحب الواجب ويمكن للدول الأخرى الرد بإجراءات مضادة. [7] وعلى العكس من ذلك، وبموجب مبدأ عدم الضرر، فإن حدوث الضرر أو خطر حدوثه، والذي فشلت الدولة فى منعه أو إيقافه، لا يؤدي تلقائيًا إلى تحمل الدولة المسؤولية. فتلك المسؤولية تنشأ بعد أن تفشل الدولة فى تعويض الضحية عن الضرر الذي تسببت فيه[8].

وعلى هذا المنوال، فإن مبدأ عدم الضرر يفرض على الدول التزامات أولية وثانوية: فهو يطلب من الدول اتخاذ إجراءات أو الامتناع عن تصرفات محددة، ويتوقع النتائج الناشئة عن الفشل فى التصرف، حيث تتحمل الدولة المسؤولية عن الإخفاق النهائي فى إصلاحه.

هذا الهيكل المعياري هو نتيجة منطقية لتأكيد المبدأ على جبر الضرر: حيث تُمنح الدول فرصة لتصحيح الضرر قبل تحمل مسؤوليتها. ليس الأذى نفسه أو عدم منعه من التصرف غير المشروع.[9] لكن الفشل فى تصحيحه. تشمل مزايا تطبيق هذا النظام على

---

de Souza Dias, 'Prevent, Respond, Cooperate: States' Due Diligence Duties vis-à-vis the Covid-19 Pandemic', 11 Journal of Humanitarian Legal Studies (2020) 218.

[1] See, e.g., reports on the widespread impact of the SolarWinds Hack: Sanger, Perlroth and Barnes, 'As Understanding of Russian Hacking Grows, So Does Alarm', New York Times, 2 January 2021, available at https://nyti.ms/3hvBUfA.

[2] 4 ILC, Draft Articles on Prevention, ibid, at 153, Commentary to art. 2, para. 7.

[3] Ibid., at 154–155, Commentary to art. 3, paras 11 and 18; ILA Study, at 12; Responsibilities and Obligations of States with Respect to Activities in the Area, Advisory Opinion, 1 February 2011, ITLOS Reports (2011) 10, para. 117; Koivurova, , ibid, para. 17.

[4] ILC, Draft Articles on Prevention, ibid 21, at 154 Commentary to art. 3, para. 11.

[5] States seem to be adamant about the need for capacity building. For recent practice, see Canada's Implementation of the 2015 GGE Norms, supra note 114, at 5; UK Multi-Stakeholder Advisory Group on Cyber Issues, 'Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015', at 5, available at www.un.org/disarmament/wp-content/uploads/2019/12/efforts-implement-norms-uk-stakeholders-12419.pdf (last visited 10 June 2021).

[6] ILC, Draft Articles on Prevention, ibid 21, at 148, General Commentary, para. 1; at 150, Commentary to art. 1, para. 6. See also Walton, ibid 148, at 1486–1488; Sander, supra note 88, at 51.

[7] See ILC, Draft Articles on Prevention, supra note 21, at 154, Commentary to art. 3, para. 7.

[8] Walton ibid 148at 603

[9] Crootof, *ibid* 148, at 597–599, 604–608, 614; Walton, ibid 148, at 1511–1516

الفضاء الإلكتروني زيادة تكاليف العمليات السيبرانية الضارة وردعها، وتجنب الوصم والعداء المرتبطين بالأفعال غير القانونية وتعزيز إنصاف الضحايا.[1] فى سياق تكنولوجيا المعلومات والاتصالات، نظرًا للترابط والاعتماد المتبادل بين مختلف الشبكات، فقد تم تسليط الضوء على الكشف عن نقاط الضعف [2] وخطط تغطية الحوادث الإلكترونية باعتبارها تدابير أساسية للانتصاف.[3]

المطلب الخامس

بذل العناية الواجبة فى الفضاء السيبراني وتطبيق مبدأ عدم التدخل

مبدأ عدم التدخل هو نتيجة طبيعية لحق كل دولة في السيادة والسلامة الإقليمية والاستقلال السياسي.[4]وهو مستمد من مبدأ السيادة العام. حيث وافق أعضاء فريق الخبراء الحكوميين التابع للأمم المتحدة على أن حظر عدم التدخل ينطبق من حيث المبدأ على العمليات السيبرانية للدول في دولة أخرى[5] ، والتي لا ترقى لمستوى استخدام القوة.

.ينص إعلان عام 1970 بشأن مبادئ القانون الدولي المتعلقة بالعلاقات الودية والتعاون بين الدول وفقا لميثاق الأمم المتحدة (إعلان العلاقات الودية) على ما يلي: " لا يحق لأي دولة أو مجموعة دول التدخل ، بشكل مباشر أو غير مباشر ، لأي سبب كان ، في الشؤون الداخلية أو الخارجية لدولة أخرى. وبالتالي ، فإن التدخل المسلح وجميع أشكال التدخل أو محاولات التهديد الأخرى ضد شخصية الدولة أو ضد عناصرها السياسية والاقتصادية والثقافية ، تنتهك القانون الدولي".[6]

هذا المبدأ منصوص عليه في العديد من مصادر القانون الدولي ، وهو متجذر في المادة 2 (7) من الميثاق ، والتي تحظر على الأمم المتحدة التدخل في "الأمور التي تقع أساسًا ضمن اختصاص أي دولة"[7]. . قالت محكمة العدل الدولية في نيكاراغوا إن مبدأ عدم التدخل هو "جزء لا يتجزأ من القانون الدولي العرفي" ، على الرغم من حقيقة أن "أمثلة التعدي على هذا المبدأ ليست نادرة."[1]

---

[1] Stratégie international de la France pour le numérique, at 32, available at www.diplomatie.gouv.fr/IMG/ pdf/strategie_numerique_a4_02_interactif_cle445a6a.pdf (last visited 10 July 2021)

[2] G7, 'Cyber Norm Initiative: Synthesis of Lessons Learned and Best Practices', 26 August 2019, at www.diplomatie.gouv.fr/IMG/pdf/_eng_synthesis_cyber_norm_initiative_cle44136e.pdf.

[3] UK Network and Information Systems Regulations 2018, supra note 113, pt. 2

[4] *Oppenheim (1996), Oppenheim's International Law, Vol. 1: Peace, p. 428*

[5] *وافق أعضاء فريق الخبراء الحكوميين التابع للأمم المتحدة على أن حظر عدم التدخل ينطبق من حيث المبدأ على العمليات السيبرانية للدول في دولة أخرى أقل من درجة استخدام القوة*

انظر كل من :

Watts, Sean. "Low-intensity cyber operations and the principle of non-intervention." Available at SSRN 2479609 (2014).
Trifunovska, Snezana. "The Principle of Non-Interference and Cyber Operations." Hungarian YB Int'l L. & Eur. L. (2017): 131.
Pomson, Ori. "The Prohibition on Intervention Under International Law and Cyber Operations." International Law Studies 99.1 (2022): 7.
Jiang, Zhifeng. "Regulating the Use and Conduct of Cyber Operations through International Law: Challenges and Fact-Finding Body Proposal." LSE Law Review 5 (2019).

[6] *انظر:*

United Nations. Department of Public Information. Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations-Pamphlet. 1970.

[7] *راجع:*

Gilmour, David R. "The Meaning of "Intervene" within Article 2 (7) of the United Nations Charter—An Historical Perspective." International &

(ISSN: 2356 - 9492)

الرغم من تدوينه في العديد من الاتفاقيات والوثائق الدولية ، فقد وصف العلماء حظر عدم التدخل بأنه غامض و "بعيد المنال". ويصعب معرفة ماهية هذا الالتزام خارج سياق استخدام القوة.[2] ومع ذلك ، قدمت محكمة العدل الدولية في قضية نيكاراغوا بعض الإرشادات.[3] رأت محكمة العدل الدولية أن مبدأ عدم التدخل (خارج سياق استخدام القوة) ينطبق على تصرفات دولة ما فيما يتعلق بدولة أخرى حيث يوجد عنصران:

الإكراه من قبل دولة لدولة أخرى ؛

فيما يتعلق بالمسائل التي يُسمح فيها لكل دولة ، بموجب مبدأ سيادة الدولة ، أن تقرر بحرية. أحد هذه الخيارات هو اختيار النظام السياسي والاقتصادي والاجتماعي والثقافي ، وصياغة السياسة الخارجية

ولا ينبغي قراءة إملاء محكمة العدل الدولية بشأن حظر عدم التدخل في نيكاراغوا بشكل إرشادي لأن محكمة العدل الدولية كانت واضحة أن "المحكمة ستحدد فقط جوانب المبدأ التي يبدو أنها ذات صلة بحل النزاع". نظرًا لأن النزاع المعني يتعلق في المقام الأول بالتدخل القسري ، لم تبد المحكمة أي رأي تفصيلي حول كيفية تعريف التدخل والإكراه خارج سياق استخدام القوة. خارج منطقة استخدام القوة ، "غالبًا ما يكون من غير الواضح ما هو المحظور وما هو غير المحظور بموجب القانون الدولي العرفي. يعتمد الكثير على السياق ، وحتى على حالة العلاقات بين الدول المعنية. على سبيل المثال ، تتضمن مبادئ الصين للتعايش السلمي "الاحترام المتبادل للسيادة وسلامة الأراضي" و "عدم التدخل في الشؤون الداخلية للدول للآخر"..

الإكراه – وبموجب مبدأ عدم التدخل ، يجب أن يحدث الإكراه فيما يتعلق "بالمسائل ذات الطبيعة السيادية بطبيعتها" ، أي تلك التي تكون للدولة سلطة حصرية عليها ، بما في ذلك الأنظمة السياسية والاقتصادية والاجتماعية والثقافية للدولة. مبدأ عدم التدخل ، بقدر ما يتعلق بالتدخلات غير القسرية ، يتعلق بالتالي بعنصر السيادة الذي يحق للدول بموجبه ممارسة سلطاتها الحكومية بشكل مستقل وبعيد عن تدخل الدول الأخرى. حظر عدم التدخل وغيره من انتهاكات السيادة هو عنصر الإكراه. يتوافق هذا مع الحكم الصادر عن محكمة العدل الدولية في نيكاراغوا ، والذي أشارت فيه المحكمة إلى ما يلي:

يعتبر التدخل غير مشروع عندما يستخدم أساليب الإكراه فيما يتعلق بمثل هذه الخيارات ، والتي يجب أن تظل حرة ... عنصر الإكراه ... يحدد ويشكل بالفعل جوهر يعتبر التدخل فى "الشؤون الداخلية أو الخارجية" للدول الأخرى فعلًا غير مشروع دوليًا. يجب استيفاء شرطين لتحديد مخالفة الحظر. أولاً، لا ينطبق الحظر إلا على الأمور التي تقع ضمن نطاق خدمة دولة أخرى. هذه أمور يتركها القانون

Comparative Law Quarterly 16.2 (1967): 330-351.

[1] *إن حظر التدخل هو مبدأ مشترك بين الدول ، ولا ينطبق على التدخل من قبل الجماعات غير الحكومية أو فيما يتعلق بأنشطة الجماعات غير الحكومية ما لم تُنسب أنشطة الجماعات من غير الدول إلى دولة بموجب قواعد الإسناد في القانون الدولي .*

Kingsbury, Benedict. "Claims by non-state groups in international law." Cornell Int'l LJ 25 (1992): 481.

[2] *انظر:*

Jamnejad, Maziar, and Michael Wood. "The principle of non-intervention." Leiden Journal of International Law 22.2 (2009): 345-381.

[3] انظر:

Kohen, Marcelo. "The principle of non-intervention 25 years after the Nicaragua judgment." *Leiden Journal of International Law* 25.1 (2012): 157-164.

الدولي لتقدير الدولة المعنية وحدها، والتي تم وصفها فى إعلان مبادئ القانون الدولي والعلاقات الودية والتعاون بين الدول على أنها "اختيار نظام سياسي واقتصادي واجتماعي وثقافي، وصياغة السياسة الخارجية ".

ثانيًا، يجب أن ينطوي الفعل على إكراه. وبتعبير بسيط، فإن الفعل الجبري كما هو مفهوم فى القانون الدولي هو عمل مصمم لإجبار دولة أخرى على اتخاذ إجراء ما كانت لتتخذه أو تمتنع عن اتخاذ إجراء قد تشارك فيه بطريقة أخرى.

تشير حكومة هولندا، مع ذلك، إلى أن "التعريف الدقيق للإكراه، وبالتالي للتدخل غير المصرح به، لم يتبلور بالكامل بعد فى القوانين الدولية". بينما وجهة نظر الخبراء المشاركين فى مشروع تالين أن الإكراه يشير إلى "عمل إيجابي يهدف إلى حرمان دولة أخرى من حريتها فى الاختيار، أي إجبار تلك الدولة على التصرف بطريقة غير طوعية أو الامتناع كرها عن التصرف بطريقة معينة".

يجادل مونيهان بأنه يجب على الدول، بدلاً من ذلك، فهم السلوك القسري "على أنه ضغط تمارسه دولة واحدة لحرمان الدولة المستهدفة من إرادتها الحرة فيما يتعلق بممارسة حقوقها السيادية فى محاولة لفرض نتيجة أو سلوك معين، وهي مسألة تخص الدولة المستهدفة ". وفى الوقت نفسه، يدافع آخرون عن خفض الحد الذي يصبح عنده مجرد التأثير إكراهًا غير قانوني، مدعين أن العملية الإلكترونية العدائية لا ينبغي بالضرورة أن تحرم الدولة من كل الخيارات المعقولة، طالما أنها تجعل الاختيار صعبًا.

يمكن أن تؤدي هذه الآراء المتباينة إلى تفسيرات مختلفة للحملات الإلكترونية. على سبيل المثال، تختلف الآراء بين الخبراء القانونيين الدوليين حول ما إذا كانت الحملة الإلكترونية الروسية لعام 2016، بما فى ذلك اختراق خوادم الحزب الديمقراطي هي عملية قسرية.

جادل غاري كورن بأن قاعدة عدم التدخل يجب أن تُفهم على أنها تهدف إلى منع الدول من استخدام تدابير تهدف إلى حرمان دولة مستهدفة من الممارسة الحرة لإرادتها على المسائل السيادية المحمية. إذا فهمت على هذا النحو، فإن شرطًا من الإكراه يمكن أن يتم تلبيته من قبل الدول التي تشارك فى حملات "خداع استراتيجي خفي" مدعومة عبر الإنترنت، حيث يتم التعرف بشكل عام على تدابير الخداع فى النظم القانونية المحلية على أنها أضرار يمكن إدراكها لأنها وسيلة لتقويض الممارسة. من الإرادة الحرة. يربط كورن هذا بالعودة إلى الإكراه، بحجة أن الدول كثيرًا ما تنظم الخداع إما بشكل مباشر فى شكل تحريم قائم على الاحتيال، أو بشكل غير مباشر عن طريق جعل الخداع بديلاً بنّاءً لعناصر القوة أو الإكراه فى الجرائم الأخرى.

إن تصور عدم التدخل والإكراه بهذه الطريقة هو جهد جديد وجدير بالثناء. إنه يسلط الضوء على مستوى الجهد المطلوب لتطبيق نظام قانوني على البيئة الاستراتيجية التي هو ضدها منحاز. يوافق كورن على أن جهوده "لتعزيز البنية القانونية الدولية الحالية" من أجل "بيئة المعلومات الحديثة" ليست حلاً سحريًا وأن المطلوب هو "أكثر من ذلك بكثير، حيث الهدف هو نهج شامل ومتضافر [.] "وتجدر الإشارة إلى أنه لا يعالج سوى مجموعة فرعية من السلوك السيبراني الاستراتيجي للدولة. منطقه لن يدعم بالضرورة الاستنتاجات التي، على سبيل المثال ، الصين ضخمة شكلت حملة سرقة الملكية الفكرية عبر الإنترنت – أو استغلال روسيا المهم من خلال منصة SolarWinds – عملاً قسريًا.

(ISSN: 2356 - 9492)

قد يكون النهج البديل هو فهم عدم التدخل من خلال عدسة نظرية المثابرة الإلكترونية. بموجب هذه النظرية ، لا يُفهم السلوك المهيمن للدول على أنه إكراه تحت أي ظرف

من التعاريف المختلفة المذكورة أعلاه، ولكن ، بدلاً من ذلك ، كأشكال للاستغلال – أي السلوك الأحادي الذي يستفيد من نقاط ضعف الآخرين فى الفضاء السيبراني ومن خلاله. هذا المنطق تتماشى بشكل أفضل مع البيئة الإستراتيجية السيبرانية.

الفصل الثاني

بذل العناية الواجبة فى الفضاء السيبراني على ضوء قواعد القانون الدولي العام

إن استخدام الدول للعمليات السيبرانية لإلحاق الضرر بالمواطنين والمؤسسات فى الدول الأخرى أو تعطيلهم أو التأثير عليهم أو حتى مجرد إزعاجهم هى ظاهرة تتنافى مع قواعد القانون الدولي القائمة، ولكن لا تخلو من الجدل. فبينما كان هناك فى السابق بعض الخلاف حول ما إذا كانت قواعد القانون الدولي الحالية تنطبق على الفضاء السيبراني على الإطلاق. اتفقت الدول المشاركة فى اجتماع مجلس الأمن التابع للأمم المتحدة فى عامي 2013 و2015 على أن القانون الدولي، بما فى ذلك مبادئ السيادة وعدم التدخل، تنطبق على أنشطة الدول فى الفضاء الإلكتروني، كما هو الحال فى السياق غير الإلكتروني.

حيث تنطبق سيادة الدول والأعراف والمبادئ الدولية المنبثقة عن السيادة على سلوك الدول المتعلق بتكنولوجيا المعلومات والاتصالات، وعلى ولايتها القضائية على البنية التحتية لتكنولوجيا المعلومات والاتصالات داخل أراضيها.[1] كما اتفق الخبراء على أن مبادئ ميثاق الأمم المتحدة تنطبق: " على الدول، عند استخدامها لتكنولوجيا المعلومات والاتصالات، مع مراعاة، مبادئ القانون الدولي ذات الصلة، وفى مقدمتها سيادة الدول، المساواة فى السيادة، وتسوية المنازعات بالوسائل السلمية، وعدم التدخل فى الشؤون الداخلية للدول الأخرى. وبناء عليه رأينا تقسيم هذا الفصل لثلاث مباحث على النحو التالي:

المبحث الأول: بذل العناية الواجبة فى السياق السيبراني من منظوري القانون الدولي لحقوق الإنسان والقانون الدولي الانساني

المبحث الثاني: تطبيق مبدأ السيادة فى الفضاء السيبراني

المبحث الثاني: :تقدير الأضرار الناجمة عن الانتهاكات غير الجسيمة المحتملة فى الفضاء السيبراني

[1] حول مجموعة الخبراء الحكوميين حول التطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي
5 UNGA (2013), Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 24 June 2013, UN Doc A/68/98, para 20; UNGA (2015), Report of the Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, 22 July 2015, para 27

(ISSN: 2356 - 9492)

المبحث الثالث: الالتزام ببذل العناية الواجبة فى الفضاء السيبراني من منظور التشريعات الوطنية

حيث نتناول، القواعد العامة للسيادة ومدي انطباقها على الفضاء السيبراني ، وتطبيق مبدأ السيادة والالتزام ببذل العناية السيبرانية خارج الحدود الإقليمية ، فضلا عن معايير تحديد انتهاكات السيادة فى الفضاء السيبراني

على أن يخصص المبحث الثاني لتقدير الأضرار الناجمة عن الانتهاكات غير الجسيمة في الفضاء السيبراني بذل العناية الواجبة فى مواجهة الأنشطة السيبرانية للكيانات الخاصة، وتحديدا مسؤولية الكيانات الفاعلة غير الدولية عن الهجمات السيبرانية، مع إلقاء الضوء على نظرية الحد الأدنى للضرر في الفضاء السيبراني.

المبحث الأول
بذل العناية الواجبة فى السياق السيبراني من منظوري القانون الدولي لحقوق الإنسان والقانون الدولي الانساني

تمهيد:

تأتي الهجمات الإلكترونية وعواقبها على رأس جدول الأعمال في جميع أنحاء العالم. لعل من أبرز المنظمات الدولية تسليطاً للضوء على تلك التهديدات هي المنظمات الدولية العاملة في مجال حقوق الإنسان والمنظمة الدولية للصليب الأحمر، فمناطق العمليات العسكرية السيبرانية أصبحت أيضًا جزءًا من النزاعات المسلحة اليوم ويمكن أن تعطل عمل البنية التحتية الحيوية والخدمات الحيوية للسكان المدنيين. على سبيل المثال ، أصبحت أنظمة الرعاية الصحية رقمية ومتصلة بشكل متزايد ولكنها غالبًا ما تكون غير محمية ، لذلك معرضة بشكل خاص للهجمات الإلكترونية في كثير من الأحيان ، تتعرض البنية التحتية للمياه والكهرباء ، أو المستشفيات ، للضرر بسبب القصف ، ولا تعمل الخدمات إلا جزئيًا على الإطلاق: تخيل وقوع حادث إلكتروني كبير فوقها، ما يمكن أن يكون له عواقب وخيمة على المدنيون المحاصرون فى الصراع والعنف يكافحون بالفعل بما يكفي لرؤية معاناتهم تتفاقم.

يواكب تلك التهديدات بشكل متزايد الاعتماد على التقنيات الجديدة والرقمية لدعم البرامج الإنسانية ، على سبيل المثال عن طريق التقاط المعلومات واستخدامها لإبلاغ وتعديل الاستجابات أو عن طريق تسهيل الاتصال ثنائي الاتجاه بين بين العاملين في المجال الإنساني والمدنيين المتضررين من الصراع أو العنف. لكن هذا أيضًا يجعلنا عرضة للعمليات الإلكترونية التي يمكن أن تؤثر على قدرتنا على الحماية والمساعدة أثناء حالات الطوارئ الإنسانية.

ونرى أيضًا خطرًا متزايدًا من حدوث ضرر متعمد وغير مقصود للسكان المتضررين ، لا سيما من خلال (سوء) استخدام البيانات من قبل الأطراف المتحاربة و / أو نشر المعلومات المضللة وخطاب الكراهية. بينما أقرت دول قليلة علانية أنها استخدمت الوسائل الإلكترونية لدعم عملياتها العسكرية ، تشير التقديرات إلى أن أكثر من 100 دولة طورت - أو تعمل على تطوير - قدرات عسكرية إلكترونية. لحسن الحظ ، لا تحدث العمليات الإلكترونية أثناء النزاعات المسلحة في فراغ قانوني: فهي تخضع للقانون الدولي الإنساني.

الالتزام الدولي ببذل العناية الواجبة في الفضاء السيبراني
بين التدابير الرادعة ومنع الأضرار السيبرانية العابرة

د. أسامة حمزة محمود عبد الفتاح

مجلة الدراسات القانونية والاقتصادية

هناك بالفعل عدد لا يحصى من العمليات السيبرانية التي تحدث كل يوم ، من الجريمة الإلكترونية إلى التجسس الإلكتروني ، إلى ما يشير إليه الكثيرون باسم "العمليات التي ترعاها الدولة". لا ينطبق القانون الدولي الإنساني على معظمها: ينطبق القانون الدولي الإنساني فقط على العمليات الإلكترونية التي تُجرى في سياق نزاع مسلح.

من المسلم به أن مسألة ما إذا كان القانون الدولي الإنساني ينطبق على العمليات السيبرانية هي نقطة خلاف في العمليات السيبرانية الجارية من منظور القانون الدولى العام. لكن القضية أقل إثارة للجدل عندما نتحدث إلى الممارسين. هنا ، لا يكاد أي شخص يجادل في أن القانون الدولي الإنساني ينطبق على العمليات الإلكترونية أثناء النزاع المسلح. إن القول بخلاف ذلك من شأنه أن يؤدي إلى موقف سخيف حيث يحظر القانون الدولي الإنساني مهاجمة مستشفى بصاروخ ، لكن هذا الحظر لن يحمي أجهزة الكمبيوتر والأجهزة الطبية وشبكات نفس المستشفى من مخاطر الهجمات الإلكترونية.

السؤال الأكثر تعقيدًا هو ما إذا كانت العملية الإلكترونية يمكن أن تؤدي بحد ذاتها إلى تطبيق القانون الدولي الإنساني. فيما يتعلق بالنزاعات المسلحة الدولية ، فإن الإجماع هو أن "النزاع المسلح يوجد كلما كان هناك لجوء إلى القوة المسلحة بين الدول". ولكن متى يتم الوصول إلى هذه النقطة في المواقف التي تنطوي على عمليات إلكترونية لا تدمر أو تلحق الضرر بالبنية التحتية العسكرية أو المدنية؟ لا يزال هذا غير واضح.

يتم شن هجمات في الفضاء الإلكتروني ضد دولة واحدة ، بيد أن الأثار يمتد ليشمل العديد من الدول ، عمدًا أو عرضيًا ، فالدول قد تتأثر، بتجميد الوكالات الحكومية ، وشل الشركات ، وشل المراكز اللوجستية ، وتكبد المليارات من الخسائر والإصلاحات. في أوقات النزاع المسلح ، يمكن تجنب هذه الآثار العشوائية والعالمية للعمليات العسكرية السيبرانية ، أو على الأقل الحد منها إذا تم احترام القانون الدولي الإنساني. وبالتالي ، فإن التنظيم الفعال للعمليات الإلكترونية أثناء النزاع المسلح هو مصدر قلق لجميع الدول ، بغض النظر عن مستوى تطورها التكنولوجي ، أو قدراتها العسكرية الإلكترونية ، أو مشاركتها في النزاعات المسلحة.

هل القانون الإنساني الدولي الحالي ملائم وكافٍ للتطبيق في الفضاء السيبراني ، أم أن هناك حاجة إلى اتفاقية إلكترونية جديدة؟ تتمثل إحدى نقاط القوة العظيمة في القانون الدولي الإنساني - كما أشارت محكمة العدل الدولية - في أنه مصمم بطريقة تجعله ينطبق "على جميع أشكال الحرب وعلى جميع أنواع الأسلحة" ، بما في ذلك "أسلحة مستقبل. القواعد الأساسية مباشرة: استهداف المدنيين والأعيان المدنية محظور ؛ يجب عدم استخدام الأسلحة والهجمات العشوائية ؛ غير متناسب.

على صعيد القانون الدولى لحقوق الانسان، بالرغم من أن بعض القوانين المحلية والدولية تحاول معالجة اعتبارات حقوق الإنسان في تشكيل معايير الأمن السيبراني ، إلا أن التأثير السلبي على حقوق الإنسان الناجم عن قوانين ومبادئ الأمن السيبراني الشاملة والواسعة أصبح واضحًا لمناصري المجتمع المدني وغيرهم. عندما نتحدث عن حقوق الإنسان ، فإننا نشير في الغالب إلى تلك الحقوق المكفولة

(ISSN: 2356 - 9492)

بموجب الإعلان العالمي لحقوق الإنسان (UDHR) للأمم المتحدة والعهد الدولي الخاص بالحقوق المدنية والسياسية (ICCPR) ، بما في ذلك حرية التعبير والحق في الخصوصية وحرية الرأي والمشاركة في الحياة السياسية.

وفي يوليو 2012 أكد مجلس حقوق الإنسان التابع للأمم المتحدة أيضًا أن "نفس الحقوق التي يتمتع بها الأشخاص خارج الإنترنت يجب أن تكون محمية أيضًا عبر الإنترنت" ، مما يجعل إعلانات حقوق الإنسان المذكورة سابقًا في الإعلان العالمي لحقوق الإنسان ، والعهد الدولي الخاص بالحقوق المدنية والسياسية المنطبقة على الإنترنت. يمكن أن يكون لعدد من قوانين وتدابير الأمن السيبراني التي اتخذتها الدول الفردية تأثير سلبي على الكلام عبر الإنترنت وحرية التعبير من خلال التعدي المباشر على هذه الحقوق أو إحداث تأثير مخيف على رغبة الناس في التعبير عن حقوقهم.

المطلب الأول

الالتزام ببذل العناية الواجبة تجاه حماية حقوق الإنسان فى الفضاء السيبراني

أدى العدد المتزايد من الأنشطة اليومية التي يتم إجراؤها عبر الإنترنت إلى تعريض حقوق الإنسان لمخاطر يصعب حصرها. نذكر فقط على سبيل المثال لحق فى الخصوصية، فهو معرض لخطر شديد من خلال التتبع المستمر والتعدين المستمر للأنشطة والبيانات عبر الإنترنت. وبالمثل، فإن الحق فى حرية الفكر والمعلومات والتعبير قد يكون منقوصًا بسبب حملات التضليل عبر الإنترنت أو انتشار الأخبار المزيفة أو الرقابة. كما يمكن أن ينتشر التسلط عبر الإنترنت والتشهير وخطاب الكراهية بسرعة مذهلة، ما يخلف آثار ضارة على حقوق الأفراد وسمعتهم.[1]

يفرض القانون الدولي لحقوق الإنسان على الدول مجموعة من الالتزامات الوقائية ضد هذه الأضرار. أنها تغطي الأنشطة عبر الإنترنت إلى الحد الذي تحدث فيه تحت سلطة الدولة فى عالم الإنترنت كما هو الحال فى أي مجال آخر من مجالات النشاط البشري، فلا تتحمل الدول فقط واجبًا "سلبيًا" فيما يتعلق باحترام حقوق الإنسان عبر الإنترنت – أي لا يقتصر التزامها على تفادي انتهاك تلك الحقوق بأفعال أجهزتها. فالدولة عليها واجب إيجابي فى تبني جميع التدابير المعقولة لحماية حقوق الإنسان للأشخاص الخاضعين لولايتها القضائية ضد التهديدات التي تشكلها الكيانات الأخرى، سواء كانت حكومات، أو شركات، أو كيانات أجنبية، أو جهات فاعلة أخرى[2] . بالإضافة إلى ذلك، يجب على الدول ضمان التمتع الفعلي بحقوق الإنسان فى الفضاء السيبراني.[3]

1

[2] ECtHR, Bărbulescu v. Romania, Appl. no. 61496/08, Judgment of 12 January 2016, para. 110, with respect to the right to privacy. In this sense, see also Milanovic and Schmitt, supra note 72, at 270ff.

[3] Cf. HRComm, General Comment No. 31 [80], The nature of the general legal obligation imposed on States Parties to the Covenant, UN Doc CCPR/C/21/Rev.1/Add.13, 26 May 2004, § 8. See also HRComm, CESCR General Comment No. 3: The Nature of States Parties' Obligations (Article 2(1) of the Covenant), E/1991/23, 14 December 1990, § 1; IACtHR, Velasquez Rodriguez v. Honduras, Judgment (Merits), 29 July 1988, paras 166–167.

الالتزام الدولي ببذل العناية الواجبة في الفضاء السيبراني
بين التدابير الرادعة ومنع الأضرار السيبرانية العابرة

د. أسامة حمزة محمود عبد الفتاح

مجلة الدراسات القانونية والاقتصادية

يمكن تحديد الالتزامات الإيجابية بالحماية والضمان بشكل مؤثر لجميع حقوق الإنسان.[1] مع إشارة محددة إلى الحقوق الأكثر شيوعًا المعرضة للخطر على الإنترنت، يمكن للمرء أن يسلط الضوء على الحق فى الخصوصية[2]، الشرف والسمعة[3]، وحرية المعلومات والتعبير.[4]

العناية الواجبة، فى هذا السياق، تحدد معيار السلوك الذي يجب على الدول اتباعه للوفاء بالالتزامات الإيجابية سالفة الذكر.[5] والجدير بالذكر أن واجبات حقوق الإنسان الإيجابية مستحقة ليس فقط للدول، ولكن أيضًا للأفراد والمجتمع الدولي ككل.[6] فكافة الدول مطالبة بمنع التهديدات التي تتعرض لها حقوق الإنسان، ووقف الأضرار بمجرد أن تبدأ ومعالجة آثارها، إلى أقصى حد ممكن. حيث يتمثل انتهاك الالتزام ببذل العناية الواجبة فى إثبات فشل الدولة فى اتخاذ تدابير الحماية الضرورية والمعقولة، بغض النظر عمن تسبب فى الضرر أو ما هو مبرره.[7]

قد تختلف هذه التدابير اعتمادًا على حق الإنسان المعني، ونوع التهديد أو الضرر الذي تحاول الدولة منعه، والظروف السائدة فى ذلك الوقت. عندما يتعلق الأمر بالامتثال للالتزامات الدولية فى مجال حقوق الانسان، نجد ان المعاهدات الدولية اعتمدت صيغة غير محددة المدة نسبيًا. على سبيل المثال، تم حث الدول على إنشاء إطار قانوني ملائم[8] يوفر سبل الانصاف المدنية والأحكام الجنائية التي تمكن من إجراء تحقيقات وملاحقات قضائية فعالة لانتهاكات تلك الحقوق.[9]

[1] See, e.g., International Covenant on Civil and Political Rights 1966, 999 UNTS 171, art. 2(1)–(2) (hereinafter 'ICCPR'); International Covenant on Economic, Social and Cultural Rights 1966, 993 UNTS 3, art. 2(1) (hereinafter 'ICESCR'); American Convention on Human Rights 1978, OAS Treaty Series No. 36, 1144 UNTS 123, art. 1(1) (hereinafter 'ACHR'); European Convention for the Protection of Human Rights and Fundamental Freedoms, 1953, 213 UNTS 221, art. 1 (hereinafter 'ECHR').

[2] ECtHR, X and Y v. the Netherlands, Appl. no. 8978/80, Judgment of 26 March 1985, para. 23; ECtHR, Bărbulescu v. Romania, Appl. no. 61496/08, Judgment of 12 January 2016, para. 108; ECtHR, Hämäläinen v. Finland, Appl. no. 37359/09, Judgment of 16 July 2014, para. 62; ECtHR, Nicolae Virgiliu Tănase v. Romania, Appl. no. 41720/13, Judgment of 25 June 2019, para. 125. Cf. also HRComm, CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, UN Doc. HRI/GEN/1/Rev.9, 8 April 1988, § 10.

[3] HRComm, General Comment No. 16, supra note 186, §§ 1 and 11. The principles established therein, even though not referred to ICTs specifically, are in principle applicable to such technologies as well.

[4] HRComm, General Comment No. 34, Article 19: Freedoms of opinion and expression, UN Doc CCPR/C/ GC/34, 12 September 2011, §§ 12, 15.

[5] HRComm, General Comment No. 31, supra note 184, § 8; Besson, supra note 39, at 2, 4–5; Milanovic and Schmitt, supra note 72, at 270ff.

[6] With respect to civil and political rights, see HRComm, General Comment No. 31, supra note 184, §§ 8, 17; for economic, social and cultural rights, see, e.g., CESCR, General Comment No. 24 on State obligations under the International Covenant on Economic, Social and Cultural Rights in the context of business activities, UN Doc E/C.12/GC/24, 10 August 2017, § 1

[7] Seibert-Fohr, 'From Complicity to Due Diligence: When Do States Incur Responsibility for Their Involvement in Serious International Wrongdoing?', 60 GYIL (2017) 667, at 670; Keller and Walther, 'Evasion of the International Law of State Responsibility? The ECtHR's Jurisprudence on Positive and Preventive Obligations under Article 3', International Journal of Human Rights (2019) 1, at 3; HRComm, General Comment No. 31, supra note 184, § 8.

[8] Bărbulescu v. Romania, Appl. no. 61496/08, Judgment of 12 January 2016, paras 115–116; HRComm, General Comment No. 31, supra note 184, §§ 7, 13; HRComm, General Comment No. 36, supra note 43, §§ 4, 13, 22

[9] ECtHR, Nicolae Virgiliu Tănase v. Romania, Appl. no. 41720/13, Judgment of 25 June 2019, para. 127; HRComm, General Comment No. 31, supra note 184, §§ 8, 18; HRComm, General Comment No. 36, supra note 43, §§ 13, 19, 27–28.

(ISSN: 2356 - 9492)

يجب أن تغطي هذه القوانين، فى جملة أمور، حظر الكلام عبر الإنترنت الذي يشكل تحريضًا على الكراهية أو التمييز أو العنف بناءً على خصائص معينة، وآليات تعديل المحتوى، والحملات الدعائية لأغراض سياسية أو لإنسانية، التعطيل القسري لخدمات الإنترنت وعمليات الإزالة التعسفية للمحتوى[1]، وكذلك مسؤولية الشركات، العامة والخاصة ومراقبة تصدير منتجات تكنولوجيا المعلومات.[2]

يجب عدم الخلط بين الالتزامات الإيجابية للدول فى مجال حقوق الإنسان التي تحتوي على معيار العناية الواجبة وبين المفهوم ذي الصلة "العناية الواجبة بحقوق الإنسان" للشركات، أي المسؤولية غير الملزمة للشركات للتخفيف من تأثير أنشطتها على حقوق الإنسان.[3] ومع ذلك، الدول نفسها لديها التزام إيجابي لإنشاء إطار قانوني يتطلب من الشركات، بدورها، ممارسة مسؤوليتها الخاصة .[4] وهذا هو الأهم فى السياق السيبراني، نظرًا لأن الإنترنت وتكنولوجيا المعلومات والاتصالات الأخرى مملوكة أو مسيطر عليها أو مصممة من قبل كيانات خاصة.[5]

الفرع الأول

إشكالية الولاية القضائية على انتهاكات حقوق الانسان ضمن سياق الأنشطة السيبرانية العابرة للحدود

بموجب بعض معاهدات القانون الدولي لحقوق الإنسان، قبل أن يتم تفعيل الالتزامات الإيجابية للدول فيما يتعلق بالأضرار عبر الإنترنت أو خارجها، يجب تحديد الولاية القضائية، بالنظر إلى الطبيعة العابرة للحدود للفضاء السيبراني، الذي يشمل البنية التحتية المادية والأنظمة المنطقية والبيانات والنشاط البشري عبر حدود متعددة.

تعتبر نماذج الولاية القضائية خارج الحدود الإقليمية ذات صلة بشكل خاص فى سياق التزامات الحماية للدول بموجب القانون الدولي لحقوق الإنسان. أولاً، هناك اتفاق واسع على أن الولاية القضائية خارج الإقليم "تتبع" الأفراد حيثما تمارس الدولة شكلاً من أشكال السيطرة المادية أو السيادة عليهم.[6]

[1] Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc. A/74/486, 9 October 2019, §§ 29, 34, 40–55, 57(b).

[2] Human Rights Council, Surveillance and Human Rights: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc. A/HRC/41/35, 28 May 2019, §§ 15–20, 29–38.

[3] On this principle, see Bonnitcha and McCorquodale, 'The Concept of "Due Diligence" in the UN Guiding Principles on Business and Human Rights', 28 European Journal of International Law (EJIL) (2017) 899; Ruggie and Sherman, 'The Concept of "Due Diligence" in the UN Guiding Principles on Business and Human Rights: A Reply to Jonathan Bonnitcha and Robert McCorquodale', 28 EJIL (2017) 921.

[4] CESCR, General Comment No. 24, supra note 190, §§ 16–18, with respect to economic, social and cultural rights, but with a principle that could be extended to civil and political rights as well; Besson, supra note 39, at 8

[5] Smith, 'A Moment of Reckoning: The Need for a Strong and Global Cybersecurity Response', Microsoft on the Issues, 17 December 2020, available at https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/.

في حين أن واجبات الحماية التي تقع على عاتق الدول بموجب القانون الدولي لحقوق الإنسان تخضع أيضًا لمتطلبات الحد الأقصى من القدرة على التصرف، وهو أمر شائع في التزامات العناية الواجبة الأخرى، قد تكون "بشكل جوهري ... أكثر إلحاحًا" من تلك المستمدة من القانون الدولي العام، والتي تتضمن غالبًا واجبات السعي بنشاط لكشف النقاب عن تلك الانتهاكات.

McGonagle, Tarlach. "Committee of Ministers:: Human Rights Guide for Internet Users." *IRIS: Legal Observations of the European Audiovisual Observatory* 8 (2014): 4-5. See, Shackelford, Scott J. "Human Rights and Cybersecurity Due Diligence: A Comparative Study." *U. Mich. JL Reform* 50 (2016): 859.

[6] UN Human Rights Committee (HRC), General comment no. 31 [80], The nature of the general legal obligation imposed on States Parties to the Covenant, 26 May 2004, CCPR/C/21/Rev.1/Add.13, available at: https://www.refworld.org/docid/478b26ae2.html [accessed 9 March 2022]§ 10

الالتزام الدولي ببذل العناية الواجبة في الفضاء السيبراني
بين التدابير الرادعة ومنع الأضرار السيبرانية العابرة

د. أسامة حمزة محمود عبد الفتاح

مجلة الدراسات القانونية والاقتصادية

أعربت العديد من هيئات حقوق الإنسان عن تعهدها بأن الولاية القضائية يمكن أيضًا أن تمتد خارج الإقليم لتشمل تأثير حقوق الإنسان الذي يمكن توقعه بشكل معقول لأنشطة الكيانات، مثل الشركات، التي تم تأسيسها أو تقع فى إقليم الجهة المسؤولة، أو تخضع بشكل آخر لسلطة الدولة من خلال المراقبة الفعالة[1].

كما قدمت اللجنة المعنية بحقوق الإنسان نهجًا "وظيفيًا" أكثر شمولاً للولاية القضائية خارج الإقليم، يرتكز على ممارسة السيطرة على التمتع بالحقوق المعنية، بغض النظر عن أي سيطرة مادية على الإقليم أو الجناة أو الضحية.[2]

يمكن القول إن النهج الوظيفي للولاية القضائية هو الأنسب لمعالجة الأشكال المعاصرة للسيطرة الفعالة المكتسبة عن بُعد من خلال تكنولوجيا المعلومات والاتصالات على الضحايا والجناة والأحداث. لكن بينما تلقى النموذج الوظيفي بعض الدعم فيما يتعلق بواجبات حقوق الإنسان السلبية[3]. يعارض الكثيرون قابليته للتطبيق على الالتزامات الإيجابية لحقوق الإنسان، خوفًا من عدم وجود سلطات حكومية ضرورية خارج أراضي الدولة أو افتقاد الصلاحيات المتصلة بالولاية القضائية.

بما أن صاحب الواجب لديه القدرة على اعتماد التدابير اللازمة.[4]القدرة فى هذا السياق تشمل القدرة على التأثير على سلوك الجناة،[5] أو توقع الأحداث، وتوافر الموارد وواجب احترام حماية حقوق الإنسان الأخرى[6]

بالطبع، هناك فرق بين دولة ليس لها ولاية قضائية على الإطلاق وعدم قدرتها على حماية حقوق الإنسان فى نطاق ولايتها القضائية: ففى الحالة الأخيرة، لا يزال يتعين تقييم قدرة الدولة على التصرف، إلى جانب العناصر الأخرى للالتزام.. ومع ذلك، لا يُطلب من الدول أن تفعل المستحيل أو أن تتحمل "عبئًا غير متناسب" [7]. ولكن من المتوقع أن تتبنى تدابير معقولة فى ظل الظروف[1]. وهكذا، كما هو

---

[1] HRComm, General Comment No. 36, ibid at 43, § 22, with respect to the right to life; CESCR, General Comment No. 14, supra note 162, § 39; CESCR, General Comment No. 15: The Right to Water (Articles 11 and 12 of the Covenant), UN Doc E/C.12/2002/11, 20 January 2003, § 33; CESCR, Statement on the Obligations of States parties regarding the corporate sector and economic social and cultural rights, UN Doc E/C.12/2011/1, 20 May 2011, § 5; IACtHR, Advisory Opinion OC-23/17, Requested by the Republic of Colombia: The Environment and Human Rights, 15 November 2017, paras 101–102. See also Milanovic and Schmitt, supra note 72, at 264–265.

هذا هو ما يُعرف بالنموذج "الشخصي" للولاية القضائية خارج الإقليم ، حيث تؤيد هيئات حقوق الإنسان أنه ينطبق على الالتزامات السلبية والإيجابية في مجال حقوق الإنسان.

See, e.g., Inter-American Commission on Human Rights (IAComHR), Coard et al. v. United States, Report No. 109/99, 29 September 1999, para. 37; ECtHR, Al-Skeini and others v. United Kingdom, Appl. no 55721/07, Judgment of 7 July 2011, paras 136–139. 205 Milanovic, supra note 147, at 119.

على الرغم من أن نموذج الولاية القضائية هذا قد يتداخل مع متطلبات قدرة الدولة على التصرف ، إلا أن هذين النموذجين يرتكزان على معايير مختلفة ومبررات أساسية. يجسد الاختصاص العلاقة بين الدولة وحق الإنسان المحمي على أساس السيطرة الفعالة على جوانب مختلفة من هذا الارتباط. وعلى العكس من ذلك ، فإن القدرة على التصرف تحد من التزامات الدولة الوقائية على أساس مجموعة من العوامل ، بما في ذلك السيطرة على الأنشطة أو الجناة المعنيين ، أو قدرة أقل تطلبًا للتأثير على سلوكهم

[2] HRComm, General Comment No. 36, supra note 43, § 63.

[3] Human Rights Law', 7 Law & Ethics of Human Rights (2013) 47. 210 Milanovic, supra note 147, at 209; Goodman, Heyns and Shany, 'Human Rights, Deprivation of Life and National Security: Q&A with Christof Heyns and Yuval Shany on General Comment 36' (2019), at 1–2, available at www.justsecurity.org/62467/human-life-national-security-qa-christof-heyns-yuval-shanygeneral-comment-36/; Sergio Euben Lopez Burgos v. Uruguay, Human Rights Committee (HRComm) Communication No. 52/1979, UN Doc. CCPR/C/13/D/52/1979, 29 July 1981, § 12.3; Lilian Celiberti de Casariego v. Uruguay, HRComm Communication No 56/1979, UN Doc. CCPR/C/13/D/56/1979, 29 July 1981, § 10.3; ECtHR, Issa and Others v. Turkey, Appl. no. 31821/96, Judgment of 16 November 2004, § 71

[4] For example, the ICESCR, supra note 184, has no express jurisdictional threshold and yet most of its obligations are positive ones, i.e. duties to protect and ensure social, economic and cultural human rights

[5] Bosnian Genocide, Judgment, 26 February 2007, ICJ Reports 2007, para. 430.

[6] Cf. ECtHR, Osman v. United Kingdom, Appl. no. 87/1997/871/1083, Judgment of 28 October 1998, para. 116.

[7] ECtHR, Nicolae Virgiliu Tănase v. Romania, Appl. no. 41720/13, Judgment of 25 June 2019, para. 136

(ISSN: 2356 - 9492)

الحال فى أي نموذج قضائي آخر، فإن شرط القدرة على التصرف يتداخل مع الاختصاص الوظيفي لدولة تبعاً للمخاطر المتوخاة ، وهو ما ينطبق على السياق السيبراني.

الفرع الثاني

التبعات القانونية لانتهاك الالتزام بحماية حقوق الانسان

فى سياق الأنشطة السيبرانية

على عكس مبادئ قناة كورفو ومبادئ عدم الإضرار، فإن الالتزامات الإيجابية بحماية وضمان حقوق الإنسان تنتهك بمجرد الافتقار إلى الاجتهاد، أي الإغفال غير المشروع أو التقاعس عن اتخاذ التدابير المطلوبة.

هذا صحيح إلى الحد الذي يجب على الدول أن تمنع التهديدات المتوقعة بشكل موضوعي لحقوق الإنسان.[2] وعلى هذا النحو، فإن مجرد ظهور خطر الأضرار، بغض النظر عما إذا كان قد تحقق أم لا، قد ينتهك الالتزامات الإيجابية بحقوق الإنسان.[3]

على الرغم من أن الحدوث الفعلي للضرر المحظور يشير بشكل عام إلى أن الدولة فشلت فى ممارسة العناية الواجبة، فإن إثبات العلاقة السببية بين عدم العناية والضرر ليس ضروريًا. وفقًا للمحكمة الأوروبية لحقوق الإنسان، فإن معرفة الدولة بانتهاكات حقوق الإنسان التي ترتكبها أطراف ثالثة أو قبولها أو تواطؤها معها يكفى لإثبات انتهاك واجبات الدولة الإيجابية لحماية تلك الحقوق.[4]

والأهم من ذلك، أن خرق الالتزامات الإيجابية فى مجال حقوق الإنسان لا ينشأ فقط من التراخي التام، ولكن أيضًا من اعتماد تدابير غير كافية أو غير فعالة، عندما تكون هناك تدابير أكثر ملاءمة.[5] الدولة انتهكت واجبات العناية الواجبة بموجب القانون الدولي لحقوق الإنسان. لا ينشأ الانتهاك إلا إذا ثبت أن الدولة فشلت فى اتخاذ تدابير وقائية كان من الممكن تنفيذها بشكل معقول.[6]

تغطي الالتزامات الوقائية بموجب القانون الدولي لحقوق الإنسان مجموعة واسعة من الأضرار، بما فى ذلك أي سلوك من قبل الكيانات العامة أو الخاصة يحول دون التمتع بحقوق الإنسان على الإنترنت أو خارجها، مثل الخصوصية وحرية التعبير. على عكس مبدأ عدم

---

[1] ECtHR, McCann and Others v. United Kingdom, Appl. no. 19009/04, Judgment of 27 September 1995, para. 151; Velasquez Rodriguez v. Honduras, Judgment (Merits), 29 July 1988, para. 167. See also The Netherlands, Letter of 5 July 2019, supra note 62, Appendix, at 4; Comments by Member States on the initial pre-draft of the OEWG report: Republic of Korea, supra note 96, at 5

[2] Todeschini, 'The Human Rights Committee's General Comment No. 36 and the Right to Life in Armed Conflict', OpinioJuris (21 January 2019), available at http://opiniojuris.org/2019/01/21/ the-human-rights-committees-general-comment-no-36-and-the-right-to-life-in-armed-conflict/.

[3] This principle applies at the very least to the right to life and the right not to be subjected to torture and ill-treatment (see, e.g., HRComm, General Comment No. 36, supra note 43, § 7; ECtHR, Keller v. Russia, Appl. no. 26824/04, Judgment of 17 October 2013, para. 82; ECtHR, Osman v. United Kingdom, Appl. no. 87/1997/871/1083, Judgment of 28 October 1998, para. 116; ECtHR, O'Keeffe v. Ireland, Appl. no. 35810/09, Judgment of 28 January 2014, paras 16, 162; ECtHR, Kurt v. Turkey, Appl. no. 15/1997/799/1002, Judgment of 25 May 1998, para. 69. It also seems to apply to the right to non-discrimination, including in the context of online hate speech (see Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc A/74/486, 9 October 2019, §§ 13, 14(f), 16).

See, generally, Stoyanova, 'Fault, Knowledge and Risk Within the Framework of Positive Obligations Under the European Convention on Human Rights', 33 Leiden Journal of International Law 601 (2020).

[4] See European Commission of Human rights (ECommHR), Yaşa v. Turkey, Appl. no. 22495/93, Report, 8 April 1997, paras 106–107; ECtHR, Özgür Gündem v. Turkey, Appl. no. 23144/93, 16 March 2000, paras 38–46; ECtHR, Kılıç v. Turkey, Appl. no. 22492/93, Judgment of 28 March 2000, paras 57, 64, 68; EctHR, Mahmut Kaya v. Turkey, Appl. no. 22535/93, Judgment, 28 March 2000, paras 74, 80, 85–92. All these cases are discussed in Milanovic, 'State Acquiescence or Connivance in the Wrongful Conduct of Third Parties in the Jurisprudence of the European Court of Human Rights' (15 September 2019), at 3–6, available at https://ssrn.com/abstract=3454007

[5] Cf. ECtHR, Hatton v. UK, Appl. no. 36022/97, Judgment of 8 July 2003, paras 138–142.

[6] Cf. ECtHR, E. and others v UK, Appl. no. 33218/96, Judgment of 26 November 2002, paras 99–100.

الضرر، لا يلزم أن يكون للضرر المعني عبر الإنترنت طبيعة عابرة للحدود ، فيجب على الدولة حماية حقوق الإنسان بغض النظر عن مصدر الضرر أو مساره.

ونظرًا لتعدد التهديدات التي تتعرض لها حقوق الإنسان، سيكون من غير الواقعي وغير المنطقي توقع أن تكون الدولة فى وضع يمكنها من اعتماد تدابير وقائية ضد أي تهديدات من هذا القبيل. بدلاً من ذلك، فإن الدول قادرة فقط وبالتالي فهي مطالبة بالتصرف فى ظل وجود مستوى معين من المعرفة بأن هناك خطرًا على حقوق الإنسان. فيما يتعلق الحق فى الحياة على سبيل المثال[1]، شددت لجنة حقوق الإنسان ومحكمة البلدان الأمريكية لحقوق الإنسان على شرط إمكانية التنبؤ المعقول بالتهديدات، والمعرفة البناءة لمخاطر فورية ومحددة، على التوالي[2].

يتعلق هذا الموقف بحماية الحق فى الحياة، وإن كان لا يوجد ما يمنع التوسع فى نطاق الحماية لتشمل الالتزامات الإيجابية لحقوق الإنسان الأخرى، بما فى ذلك الفضاء الإلكتروني. وهذا يعني أنه بموجب القانون الدولي لحقوق الإنسان، يجب على الدول أيضًا ممارسة العناية الواجبة فى السعي النشط إلى تقييم المعلومات المتاحة حول التهديدات التي تتعرض لها حقوق الإنسان الخاضعة لولايتها القضائية.[3]

المطلب الثاني

بذل العناية الواجبة تجاه الانشطة السيبرانية بموجب

أحكام القانون الإنساني الدولي

أولا : هل الإنترنت هدف عسكري؟

يمكن أن يتعطل الإنترنت عن طريق مهاجمة مكونات أجهزته أو برامجه. يستهدف النوع السابق من الهجوم الخوادم وكابلات الألياف الضوئية والبنية التحتية المادية الأخرى بين الشبكات المستخدمة لضمان الاتصال، بينما يؤثر النوع الأخير على أنظمة مثل نظام اسم المجال (DNS) ، الذي يترجم أسماء النطاقات إلى عناوين IP: إذا تم اختراق DNS ، فلن يعرف متصفح الويب إلى أين يتوجه.

[1] HRC with respect to the right to life. See HRComm, General Comment No. 36, supra note 43, § 21; cf. also ECtHR, Osman v. United Kingdom, App. No. 87/1997/871/1083, Judgment of 28 October 1998, paras 115–116.
[2] IACtHR, Sawhoyamaxa Indigenous Community v. Paraguay, Judgment (Merits, Reparations and Costs), 29 March 2006, § 155; cf. very similar language in ECtHR, Nicolae Virgiliu Tănase v. Romania, Appl. no. 41720/13, Judgment of 25 June 2019, para. 136.
[3] HRComm, General Comment No. 36, supra note 43, §§ 13, 23, 27.

(ISSN: 2356 - 9492)

أفاد مركز معلومات شبكة الإنترنت الصينية (CNNIC) ، على سبيل المثال ، أن سجل تحليل اسم النطاق الوطني تعرض لسلسلة من هجوم DDoS المستمر فى 25 أغسطس 2013 ، والذي أوقف الزيارات أو أبطأها.[1] يمكن اعتبار العملية الإلكترونية ضد مكونات الأجهزة أو البرامج الخاصة بالإنترنت بمثابة "هجوم" بالمعنى الوارد فى المادة 49 (1) من البروتوكول الإضافي الأول إذا حدث ضرر مادي أو خسارة كبيرة فى وظائف البنية التحتية.

فقد أصبحت العمليات السيبرانية الآن جزءًا لا يتجزأ من الحرب الحديثة. فى حين أنها قد تستهدف على وجه التحديد البنية التحتية العسكرية، فإن الأسلحة والتكتيكات السيبرانية لها الحق بشكل مقصود أو عشوائي[2] فى تعطيل البنية التحتية المدنية وتعطيل الخدمات الأساسية للسكان المدنيين.

يتفق العديد من الدول[3] ومعظم المعلقين على أن العمليات الإلكترونية التي لها آثار حركية مماثلة لتلك الخاصة بالاستخدامات التقليدية للقوة المسلحة – على سبيل المثال، تدمير الأعيان المدنية أو إلحاق الضرر بالمدنيين – مشمولة بأحكام القانون الدولي الإنساني عند تنفيذها خلال النزاعات المسلحة.[4]

لكن لا يزال من غير الواضح ما إذا كان مجرد تلف البيانات أو اضطرابات النظام الوظيفي، فى حالة عدم وجود ضرر مادي، يرقى إلى مستوى الهجمات التي يحكمها القانون الدولي الإنساني. [5]

تنص العديد من قواعد القانون الدولي الإنساني على التزامات وقائية تتطلب من الدول ممارسة العناية الواجبة.[6] ومن الأمور ذات الصلة بشكل خاص بتكنولوجيا المعلومات والاتصالات الالتزامات بضمان احترام القانون الدولي الإنساني، بما فى ذلك من قبل الأطراف من الغير، واعتماد تدابير وقائية لتجنب أو تقليل الإضرار بالأعيان المدنية والسكان المدنيين.

ثانيا: الواجب العام لضمان احترام القانون الدولي الإنساني فى الفضاء السيبراني

الالتزام بالحماية مقنن بموجب المادة 1 المشتركة فى اتفاقيات جنيف لعام 1949 بشأن حماية ضحايا الحرب، والتي تتطلب من الدول احترام الأحكام الواردة باتفاقيات جنيف [7]. اعترفت محكمة العدل الدولية بالوضع العرفي لهذه القاعدة، فضلاً عن تطبيقها على كل من النزاعات المسلحة الدولية وغير الدولية.[1]

1

[2] ICRC, Position Paper, 'International Humanitarian Law and Cyber Operations during Armed Conflicts' (2019), at 5, available at www.icrc.org/en/document/international-humanitarian-law-andcyber-operations-during-armed-conflict

[3] See, e.g., Jeremy Wright, UK Attorney General's Office, Speech, 'Cyber and International Law in the 21st Century' (23 May 2018), available at www.gov.uk/government/speeches/cyber-and-international-lawin-the-21st-century; Comments by Member States on the Initial Pre-Draft of the OEWG Report: United States, supra note 96, at 2

[4] 9 See, e.g., Tallinn Manual 2.0, supra note 6, rule 82, para. 16; nuclear weapons, Advisory Opinion, 8 July 1996, ICJ Reports (1996), para. 86. See also Durham, 'Cyber Operations During Armed Conflict: 7 Essential Law and Policy Questions', Humanitarian Law & Policyt (26 March 2020), available at https:// blogs.icrc.org/law-and-policy/2020/03/26/cyber-armed-conflict-7-law-policy-questions/.

[5] Rödenhauser, 'Hacking Humanitarians? IHL and the Protection of Humanitarian Organizations Against Cyber Operations', EJIL: Talk! (16 March 2020), available at www.ejiltalk.org/hacking-humanitarians-ihl-and-the-protection-of-humanitarian-organizations-against-cyber-operations/.

[6] Longobardo, 'The Relevance of the Concept of Due Diligence for International Humanitarian Law', 37 Wisconsin International Law Journal (2020) 44; and Berkes, 'The Standard of "Due Diligence" as a Result of Interchange between the Law of Armed Conflict and General International Law', 23 Journal of Conflict & Security Law (2018) 433.

[7] Article 1 common to: Geneva Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field 1949, 75 UNTS 31; Geneva Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of

نظرًا لطبيعة القانون الدولي الإنساني الملزمة لكافة أعضاء المجتمع الدولي، لا يقتصر الأمر على الأطراف فى نزاع مسلح، ولكن جميع الدول ملزمة بفعل "كل ما فى وسعها لضمان تطبيق المبادئ الإنسانية التي تقوم عليها الاتفاقيات عالميًا".[2]

وفقًا للقاعدة 144 من دراسة القانون الدولي الإنساني العرفي الصادرة عن اللجنة الدولية للصليب الأحمر[3] ، يتطلب هذا الالتزام من الدول ليس فقط الامتناع عن ارتكاب انتهاكات للقانون الدولي الإنساني[4] أو تشجيعها، ولكن أيضًا اتخاذ خطوات إيجابية لضمان – حتى فى وقت السلم[5] – امتثال كافة الكيانات للقانون الدولي الإنساني[6]

وينطبق هذا الالتزام أيضًا على الفضاء الإلكتروني وينطوي على واجب التصرف قدر الإمكان لمنع ووقف العمليات الإلكترونية التي تشكل انتهاكات للقانون الدولي الإنساني. فنطاق تطبيقه الواسع يغطي الانتهاكات المحتملة من قبل وكلاء الدولة، فضلا عن الكيانات الخاصة الخاضعة لسيادة الدولة [7]، أو تملك الدولة تجاهها درجة معقولة من النفوذ، بما فى ذلك الدول الأخرى والجماعات غير الحكومية الموجودة فى أجزاء مختلفة من العالم.

Armed Forces at Sea 1949, 75 UNTS 85; Geneva Convention (III) relative to the Treatment of Prisoners of War 1949, 75 UNTS 135; Geneva Convention (IV) relative to the Protection of Civilian Persons in Time of War, 75 UNTS 287.

وهو حكم مكرر حرفيا تقريبا في المادة 1 (1) من المواد الإضافية البروتوكول الأول

International Committee of the Red Cross (ICRC), Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, 1125 UNTS 3, available at: https://www.refworld.org/docid/3ae6b36b4.html [accessed 10 March 2022] art. 1(1).

[1] Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States), Judgment, 27 June 1986, ICJ Reports (1987) 14, para. 220; ICRC, Commentary on the First Geneva Convention (2016), art. 1 ('Respect for the Convention'), paras 125–126, available at https://ihldatabases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=72239588AFA66200C1257F7D00367DBD (hereinafter '2016 Commentary').

[2] ICRC, Geneva Convention Relative to the Protection of Civilian Persons in Time of War: Commentary (1958), at 16; Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 9 July 2004, ICJ Reports (2004) 136, paras 158–159.

[3] 6 J.-M. Henckaerts and L. Doswald-Beck (eds), Customary International Law. Volume 1: Rules (2009), at 509–513. Rule 139, instead, reproduces verbatim the language of common Article 1, but it limits its scope of application to armed forces and other entities acting on the instructions, or under the direction or control of a party to the conflict. See ibid., at 495ff.

[4] ICRC, 2016 Commentary, supra note 234, paras 154. 158–163.

[5] Ibid., paras 127–128 and 185.

[6] Ibid., paras 121, 153–154, 164–173. On this obligation generally, see Dörmann and Serralvo, 'Common Article 1 to the Geneva Conventions and the Obligation to Prevent International Humanitarian Law Violations', 96 International Review of the Red Cross (IRRC) (2014) 707. See also Longobardo, supra note 231, at 57–60; and Berkes, supra note 231, at 442.

راجع أيضا:

Zych, 'The Scope of the Obligation to Respect and to Ensure Respect for International Humanitarian Law', 27 Windsor Yearbook of Access to Justice (2009) 251; Robson, 'The Common Approach to Article 1: The Scope of Each State's Obligation to Ensure Respect for the Geneva Conventions', 25 Journal of Conflict and Security Law (2020) 101. On examples of operational measures, see European Union, Updated European Union Guidelines on Promoting Compliance with International Humanitarian Law, 2009/C 303/06, 15 December 2009, § 16.

[7] ICRC, 2016 Commentary, ibid, para. 150.

(ISSN: 2356 - 9492)

كما هو الحال مع الالتزامات الوقائية الأخرى، فإن واجب احترام وضمان احترام القانون الدولي الإنساني ينطلق ويحد من قدرة الدولة على التصرف [1]. وهذا بدوره يعتمد على مجموعة من العوامل، مثل الموارد المتاحة، وخطورة الانتهاك ودرجة السيطرة أو التأثير الذي تمارسه الدولة على الجناة المباشرين[2].

ومع ذلك، فإن الافتقار إلى الموارد العسكرية أو الاقتصادية أو غيرها لا يعفى الدول مما يظل التزامًا قانونيًا ملزمًا لاكتساب واستخدام جميع الوسائل المعقولة لضمان احترام القانون الدولي الإنساني، بما فى ذلك الفضاء الإلكتروني.[3] لا يتم تفعيل الواجب فقط من خلال معرفة الدولة بالانتهاكات، ولكن أيضًا من خلال إمكانية التنبؤ الموضوعي.

ومع ذلك، على الرغم من أنه ينشأ منذ اللحظة التي تصبح فيها انتهاكات القانون الدولي الإنساني معروفة أو متوقعة، فإن الانتهاك لا يحدث إلا إذا تحقق الضرر الفعلى.[4] بيد أن الدولة قد تمتثل لهذه القاعدة من خلال تبني تدابير رادعة تتوقى بها حدوث الضرر وتدفع بها المسؤولية الدولية، وذلك تفادياً لدفع الدولة الضحية بانتهاك القانون الدولي الإنساني من خلال الوسائل القضائية أو الدبلوماسية.[5] ما يستتبع المطالبة بوقف الانتهاك، وتقديم ضمانات عدم التكرار والتعويضات[6]، والامتناع عن الاعتراف بأن الوضع قانوني والامتناع أيضاً عن تقديم المساعدة للدولة المخالفة[7]، فضلاً عن اتخاذ خطوات فعالة لملاحقة مرتكبي تلك الانتهاكات وإنصاف الضحايا.

ثالثا: واجب اتخاذ التدابير الوقائية للحد من آثار الحرب السيبرانية

كما يجسد مبدأ الاحتياط المنصوص عليه فى العديد من أحكام القانون الدولي الإنساني مجموعة من واجبات الحماية. تنص المادة 51 من البروتوكول الإضافي الأول بشكل عام على أن "السكان المدنيين والأفراد يجب أن يتمتعوا بحماية عامة ضد الأخطار الناشئة عن العمليات العسكرية". [8] ومن الواضح على الفور كيف أن الحرب السيبرانية قد تشكل تحديًا لتطبيق هذه القاعدة. بادئ ذي بدء، قد لا يمكن تمييز الهياكل الأساسية الإلكترونية المدنية بسهولة عن الأهداف العسكرية المشروعة، لأنها تعتمد فى الغالب على الخدمات والموارد التي توفرها الكيانات الخاصة.[9] فقد تستهدف تلك الهجمات الإلكترونية الأنظمة المدنية، ما يتسبب فى تعطيل أو فقدان قدرات البني التحتية للدولة[10].

[1] Ibid., paras 166, 187.
[2] Ibid., paras 165–166 and, mutatis mutandis, Bosnian Genocide, Judgment, 26 February 2007, ICJ Reports 2007, para. 4302
[3] ICRC, 2016 Commentary, ibid, para. 187
[4] ICRC, 2016 Commentary, ibid, para. 166 establishes a parallelism between common Article 1 to the Geneva Conventions, supra note 231, and Genocide Convention, supra note 31, art. 1. The ICJ in Bosnian Genocide, Judgment, 26 February 2007, ICJ Reports 2007, para. 431, established that a breach of the duty to prevent occurs only if genocide is actually committed, in line with ARSIWA, supra note 20, art. 14(3).
[5] ICRC, 2016 Commentary, ibid, para. 181
[6] Cf. ICRC, Memorandum to the States Parties to the Geneva Conventions of 12 August 1949 concerning the conflict between Islamic Republic of Iran and Republic of Iraq (1983), available at https://casebook.icrc.org/case-study/icrc-iraniraq-memoranda.
[7] ARSIWA, supra note 20, arts. 16, 40–41; cf. ICRC, 2016 Commentary, supra note 234, paras 158–163
[8] Additional Protocol I, supra note 44, art. 51. See generally Jensen, 'Precautions against the Effects of Attacks in Urban Areas', 98 IRRC (2016) 147; Quéguiner, 'Precautions under the Law Governing the Conduct of Hostilities', 88 IRRC (2006) 793.
[9] Sandoz, Swinarski and Zimmermann, Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 (1987), at 692, para. 2239.
[10] See Gisel and Rodenhäuser, Cyber Operations and International Humanitarian Law: Five Key Points (2019) available at https://blogs.icrc.org/law-and-policy/2019/11/28/cyber-operations-ihl-five-key-points/.

لتجنب مثل هذه النتائج غير المرغوب فيها، تطلب المادة 58 من البروتوكول الإضافي الأول من أطراف النزاع اتخاذ تدابير احترازية لحماية السكان المدنيين والأعيان من آثار الهجمات[1]، شريطة أن يمارسوا السيطرة على المجال الأرضي أو البنية التحتية المادية أو، وأنظمة التشغيل التي قد تكون مستهدفة.

لقد حققت القاعدة وضعًا عرفيًا، على النحو المعترف به فى القواعد 22–24 من دراسة اللجنة الدولية للصليب الأحمر حول القانون الدولي الإنساني العرفي، وهي قابلة للتطبيق ليس فقط فى النزاعات المسلحة الدولية بل وغير الدولية أيضاً.[2]

إلى جانب الالتزامات الوقائية الأخرى، فإن واجب اتخاذ الاحتياطات ضد آثار الهجمات ينطلق ويحد من قدرة الدولة على التصرف، ويغطي فقط التدابير "القابلة للتطبيق أو الممكنة عمليًا".[3]

فيما يتعلق بالهجمات الإلكترونية، قد يتطلب ذلك من الدول أن تتبنى، إلى أقصى حد ممكن، تدابير مثل الفصل الواضح بين البنية التحتية الإلكترونية العسكرية والمدنية والشبكات تحديد وحماية البنية التحتية والخدمات المدنية الحيوية – مثل تلك المتعلقة بتوفير المساعدة الطبية والكهرباء والاتصالات السلكية واللاسلكية ونقل الموانئ وتوزيع الأشياء التي لا غنى عنها لبقاء المدنيين على قيد الحياة – من العمليات الإلكترونية التخريبية المحتملة، التي قد تستهدف تعطيلها.[4]

رابعاً: التزامات العناية الواجبة فى مجال الأمن السيبراني لدول العبور

علاوة على ذلك، قد يؤدي النشاط السيبراني المتكرر أو المستمر من خلال الشبكات المحلية للدولة إلى افتراض المعرفة، ويمكن أن يكون الاستخدام المباشر للبنية التحتية الحيوية التي تسيطر عليها الدولة بمثابة دليل على علم دولة العبور أو كان ينبغي أن تكون على علم بهجوم سيبراني قيد التقدم[5].

الهجمات السيبرانية معقدة، وغالبًا ما تتكون من عدد لا يحصى من المكونات، وبالتالي فإن معرفة الاستغلال الفردي لا يعني بالضرورة معرفة الحملة الشاملة. قد يتم تقسيم الهجمات إلى أجزاء من التعليمات البرمجية التي تبدو بريئة أو غير مفهومة، فقط ليتم التعرف عليها كتهديد إلكتروني عند إعادة بنائها فى هدف معين.[6]

---

[1] Additional Protocol I, supra note 44, art. 51. See generally Jensen, 'Precautions against the Effects of Attacks in Urban Areas', 98 IRRC (2016) 147; Quéguiner, 'Precautions under the Law Governing the Conduct of Hostilities', 88 IRRC (2006) 793.

[2] Henckaerts and Doswald-Beck, supra note 236, at 69–70

[3] راجع:

Cf., e.g., US Department of Defense, Law of War Manual (June 2015, updated December 2016), at 192, § 5.2.3.2.

[4] راجع:

Cf. ICRC, Position Paper, supra note 227, at 6. See also Mačák, Gisel and Rodenhäuser, 'Cyber Attacks against Hospitals and the COVID-19 Pandemic: How Strong Are International Law Protections?', Just Security (2020), available at www.justsecurity.org/69407/cyber-attacks-against-hospitals-and-thecovid-19-pandemic-how-strong-are-international-law-protections/.

[5] ومع ذلك، يجب فهم معرفة الدولة في السياق، لأن الحزم الفردية المنقولة عبر شبكة الدولة قد تكون، بمفردها، غير ضارة راجع

Heintschel von Heinegg, Wolff. "Territorial sovereignty and neutrality in cyberspace." International Law Studies 89.1 (2013): 17.

[6] تم تصميم Stuxnet ، على سبيل المثال ، بطريقة تجعله كذلك فقط على أجهزة وأنظمة متخصصة محددة ، راجع:

(ISSN: 2356 - 9492)

بالنسبة للواجبات المحددة التي قد تكون مطلوبة من دول العبور، فمن المحتمل أن تعكس هذه الدور الذي لعبته البنية التحتية لدولة معينة فى الهجوم. سيكون أعلى مستوى من العناية الواجبة التي يمكن أن تكون مطلوبة بشكل معقول هو الالتزام الفعلي بمراقبة شبكات الدولة للهجمات الإلكترونية والتخفيف من أي تهديد من خلال واجب المساعدة بحد أدنى.

سيكون هذا أقرب إلى التزامات الدول المحايدة فى وقت الحرب، والتي يُطلب منها منع ومقاومة أي قوة محاربة من نقل القوات أو الذخائر عبر إقليم محايد. من المحتمل أن تكون المتطلبات الأقل مشقة، ولكن الأكثر احتمالية بكثير هي واجب تحذير الدول التي تعرضت للهجمات التي تم اكتشافها على شبكاتها وواجب التعاون مع التحقيقات التي تجريها الدولة المستهدفة لتحديد مصدر الهجوم الإلكتروني وتقديم الأدلة الجنائية الإلكترونية. قد تظل دولة العبور خاضعة لالتزام عام بسن وإنفاذ التشريع المحلي للجرائم الإلكترونية.

على نطاق أوسع، قد تخضع الدولة لواجب عام للحفاظ على الحد الأدنى من معايير رعاية الأمن السيبراني، كما نوقش أعلاه للدول التي نشأ فيها الهجوم سيعكس دور دول العبور فى نهاية المطاف الدرجة التي ساهمت بها أفعالها أو امتناعها فى الهجوم. فى حين أن هذه الالتزامات هي بالتأكيد أقل إلحاحًا من تلك الخاصة بالدولة التي نشأ فيها الهجوم، فإن دول العبور قد لا يكون لديها بعض الالتزامات، ويجب أن تأخذ بعين الاعتبار الأبعاد الدولية لإنفاذ استراتيجيات الأمن السيبراني الوطني الخاصة بهم. ومع ذلك، تجدر الإشارة إلى أنه مع انتقال خوادم أوامر التحكم والسيطرة إلى الدول المستهدفة، قد تتغير معايير العناية الواجبة.[1]

وبغض النظر عن ذلك، هناك حاجة لتوضيح قانون الحياد الدولي على نطاق أوسع لتحديد ما إذا كان بإمكان الدول الضحية أو يجب عليها أن تحاسب الدول المحايدة التي عبرت الهجمات السيبرانية من خلالها لعدم التزامها بصد المهاجمين.

تقييم المعيار التقليدي لبذل العناية الواجبة

على الرغم من أن جميع هذه الحالات تتناول مفهوم العناية الدولية الواجبة، فمن غير الواضح إلى أي مدى ينبغي أن تشكل هذه الآراء القانون والسياسة الدولية للأمن السيبراني.

يمكن التمييز بين كل من قناة Corfu و Trail Smelter على أساس القرب المادي. تضمنت قناة كورفو التزامات الدولة فى مياهها السيادية الحدودية وتناولت القضايا التي أثارتها سفن الدول الأخرى التي تحتل هذه المياه فعليًا، فى حين تضمن Trail Smelter التصريف البيئي عبر حدود الجار. تعترف كلتا الحالتين بأن الإجراءات التي تتخذها دولة ما داخل إقليمها يمكن أن يكون لها عواقب تتجاوز ذلك الإقليم، ولكنها مع ذلك مقيدة بأقاليم قريبة جغرافيًا.

لكن هذا القيد الجغرافي لا ينعكس فى مجال الأمن السيبراني، حيث يمكن أن تؤثر الإجراءات المتخذة داخل حدود الدولة فى أي مكان يمكن الوصول إليه عبر الشبكات العالمية. قد يكون هذا التوسع الكبير للإقليم الذي قد يحدث فيه نشاط ضار هو المنحدر الزلق الذي يعرقل هذا الجانب من متطلبات العناية الواجبة للأمن السيبراني للدول. بعد كل شيء، إذا كان الأمر بخلاف ذلك، فإن العديد من الدول ستكون قد انتهكت الالتزامات البيئية تجاه بعضها البعض من خلال انبعاث غازات الدفيئة المسؤولة عن تغير المناخ العالمي.

Zetter, Kim. Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon. Broadway books, 2014.

[1] Shackelford, Scott J., Scott Russell, and Andreas Kuehn. "Defining Cybersecurity Due Diligence Under International Law: Lessons from the Private Sector." *Ethics and Policies for Cyber Operations* (2017): 115-137.

الالتزام الدولي ببذل العناية الواجبة في الفضاء السيبراني
بين التدابير الرادعة ومنع الأضرار السيبرانية العابرة

د. أسامة حمزة محمود عبد الفتاح

مجلة الدراسات القانونية والاقتصادية

فالالتزامات البيئية الدولية، على الرغم من كونها مقيدة جغرافيًا فى الأصل، إلا أنها زادت من نطاق تأثيرها، مع وقوع كوارث بيئية كبرى مثل مفاعل فوكوشيما النووي وانسكاب النفط فى ديب ووتر هورايزون مما يدل على أن الإجراءات البيئية لصاحب المصلحة الواحد وإغفالاتها يمكن أن تؤدي إلى التحديات البيئية العالمية. [1]

ربما لا ينبغي أن تكون التغييرات التكنولوجية والعزلة الجغرافية ذريعة لإهمال الالتزامات المشتركة "بعدم إلحاق الضرر". فى الواقع، جادل بعض المعلقين بالفعل بأن "الدول عليها التزام بالعناية الواجبة لمنع هجمات إلكترونية عدوانية عابرة للحدود على البني التحتية لدولة أخرى.[2]

يعترف القانون الدولي العرفي بمجموعة من الاستثناءات المتعلقة بالأمن القومي: كتغيير الظروف، التدابير المضادة، الدفاع عن النفس ومبدأ الضرورة.[3] يتم الدفع عادة بتلك الاستثناءات بالحالات التي يمكن فيها وقف الالتزامات الدولية للدولة بسبب أفعال دولة أخرى أو التهديد باتخاذها قائماً. فى حين أن هذه الاستثناءات ضيقة النطاق، فإنها تضيف مزيدًا من عدم اليقين إلى ساحة غير مؤكدة بالفعل، حيث لا يوجد شيء تم توضيحها فى مجال الأنشطة السيبرانية ، والتي غالبًا ما تنطوي على قضايا تتعلق بالأمن القومي[4].

على الرغم من قيود اتفاقية الجات على العقوبات الاقتصادية أحادية الجانب، فقد استخدمت الولايات المتحدة فى مناسبات عديدة استثناء الأمن القومي لفرض عقوبات اقتصادية أحادية الجانب، كان آخرها ضد روسيا. هذا الاستثناء للأمن الوطني هو جانب مرغوب فيه فى كثير من الأحيان من القانون الدولي، لكنه مع ذلك يقترح تقييم أساسي فى المجتمع الدولي بأن سيادة الدولة يجب أن تعطى الأفضلية فى القضايا التي تنطوي على مصالح أمنية أساسية.

لذلك، يجب فهم أي معايير للعناية الواجبة للأمن السيبراني على أنها تحتوي على الأرجح على استثناء للأمن القومي، وقد تؤدي الأهمية المتزايدة للأمن السيبراني لمصالح الأمن القومي إلى مثل هذا الاستثناء لابتلاع

---

[1] Keohane, Robert O., and David G. Victor. 2011. The regime complex for climate change. Perspectives on Policy 9: 7–23

[2] Messerschmidt, Jan E. 2013. Hackback: Permitting retaliatory hacking by non-state actors as proportionate countermeasures to transboundary cyberharm. Columbia Journal of Transnational Law 52: 275–323. At 279

[3] Rose-Ackerman, Susan, and Benjamin Billa. 2008. Treaties and national security. New York University Journal of International Law and Politics 40: 437–495.

[4] راجع:

Schmitt, Michael N. 2014. "Below the threshold" cyber operations: The countermeasures response option and international Law. Virginia Journal of International Law 54: 697–732. Segal, Adam. 2012. China moves forward on cybersecurity policy. Council on Foreign Relations, July 24. http://blogs.cfr.org/asia/2012/07/24/china-moves-forward-on-cybersecurity-policy/. Accessed 26 Mar 2021.

على سبيل المثال، منظمة التجارة العالمية ("منظمة التجارة العالمية")، التي تتضمن الاتفاقية العامة للتعريفات الجمركية والتجارة ("الجات") ، تستخدم إستثناءا واسعًا لـ "المصالح الأمنية الأساسية" ، والتي تعمل فعليًا باعتبارها غير قابلة للاستئناف وذاتية القرار).

GATT 1994: General Agreement on Tariffs and Trade 1994, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1A, THE LEGAL TEXTS: THE RESULTS OF THE URUGUAY ROUND OF MULTILATERAL TRADE NEGOTIATIONS 17 (1999), 1867 U.N.T.S. 187, 33 I.L.M. 1153 (1994)

(ISSN: 2356 - 9492)

فى نهاية المطاف، فإن وجود هذه المحاذير والاستثناءات يجعل أي بيان نهائي بشأن حالة معايير العناية الواجبة الدولية أكثر صعوبة، مما يؤدي إلى ضرورة فحص نهج القطاعين العام والخاص للمساعدة فى توضيح بعض العناصر المفقودة فى العناية الواجبة ضمن الأمن السيبراني.

المبحث الثاني
تطبيق مبدأ السيادة فى الفضاء السيبراني

تمهيد:

حاول جانب من الفقه إعادة النظر فى النهج الشامل للسيادة فى سياق الهجمات السيبرانية، كونه ينطوي على صعوبات أبرزها الطبيعة الخاصة لتلك الممارسات كما أوضحنا سلفا، ولكن فقط إذا وصل لدرجة معينة. يصبح السؤال بعد ذلك ما هي المعايير التي يتعين أخذها بعين الاعتبار للحكم على التصرفات غير المشروعة للدول والذي بموجبه ينتهك نشاط إلكتروني للدولة سيادة دولة أخرى - هل الحد الأدنى لتلك الممارسات يعتمد على العوامل الكمية مثل حجم الضرر فى الدولة المستهدفة، أو عدد المواطنين المتضررين، أو النطاق الجغرافي للهجوم؛ أم أنها تستند إلى عوامل نوعية مثل طبيعة الهجوم - أم كليهما؟[1] كما اعترفت العديد من الهيئات الدولية بخضوع أنشطة الدول بالفضاء السيبراني لتلك القواعد[2].

غير أن ذلك لم يحسم الجدل المثار حول خضوع السياق السيبراني لقواعد القانون الدولى، فهناك مدرستان حول كيفية تطبيق القانون الدولي على النشاط السيبراني الذي ترعاه الدولة والذي لا يمكن تصنيفه كاستخدام للقوة المسلحة. الأول هو أن مبدأ عدم التدخل ينطبق على بعض التدخلات السيبرانية التي ترعاها الدولة، وأنه دون مستوى هذا المبدأ، قد يكون النشاط غير ودي، ولكنه لن يشكل انتهاكًا للقانون الدولي ومن ثم المسؤولية الدولية.[3]

[1] UNGA (2013), Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 24 June 2013, UN Doc A/68/98, paras 19–20; UNGA (2015), Report of the Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, 22 July 2015, para 28(b). The 2015 UN GGE also agreed 11 voluntary and non-binding norms, rules, and principles of responsible state behavior in the ICT environment.

[2] NATO (2014), Wales Summit Declaration, 5 September 2015, para 72, https://www.nato.int/cps/en/natohq/official_ texts_112964.htm (accessed 22 Oct. 2019); Organization for Security and Co-operation in Europe (OSCE) (2016), OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies, Decision No. 1202, Permanent Council, 10 March 2016, PC.DEC/1202, calling on the international community to 'develop a peaceful, secure, fair and open information space based on the principles of cooperation and respect for sovereignty and non-interference in the internal affairs of other countries'; Embassy of the Republic of Uzbekistan to the Republic of Latvia (2016), 'The Tashkent Declaration of the Fifteenth Anniversary of the Shanghai Cooperation Organization', https://uzbekistan.lv/en/the-tashkent-declaration-of-the-fifteenth-anniversary-of-the-shanghai-cooperation-organization/ (accessed 22 Oct. 2019); Council of the EU (2017), 'EU Council Conclusions of 20 November 2017', https://www.consilium.europa.eu/media/31666/st14435en17.pdf (accessed 22 Oct. 2019); The Commonwealth (2018), 'Commonwealth Cyber Declaration', https://thecommonwealth.org/commonwealth-cyberdeclaration (accessed 22 Oct. 2019).

[3] من وجهة النظر هذه، تعتبر السيادة أحد مبادئ القانون الدولي التي قد توجه تفاعلات الدول، لكنها لا ترقى إلى مستوى قاعدة أساسية قائمة بذاتها، على الأقل ليس فى السياق السيبراني.

Lotrionte, Catherine. "Reconsidering the consequences for state-sponsored hostile cyber operations under international law." *The Cyber Defense Review* 3.2 (2018): 73-114.

الالتزام الدولي ببذل العناية الواجبة في الفضاء السيبراني
بين التدابير الرادعة ومنع الأضرار السيبرانية العابرة

د. أسامة حمزة محمود عبد الفتاح

رأي آخر يرى أن العمليات الإلكترونية التي لا تشكل انتهاك لمبدأ عدم التدخل قد تكون غير قانونية باعتبارها انتهاكاً لسيادة الدولة المستهدفة. هذا هو النهج المعتمد فى دليل تالين، والذي يستمد القواعد من السيادة وعدم التدخل ويطبقها على العمليات فى الفضاء السيبراني[1].

منذ نشر دليل تالين 2.0، نوقش جدل "السيادة كقاعدة" كثيرًا بين المعلقين فى السياق السيبراني، ولكن حتى وقت قريب كان هناك القليل من ممارسات الدولة العامة للمساعدة فى إثراء هذا النقاش. اختارت الدول أن تتبنى "سياسة الغموض والصمت" حول كيفية تطبيق القانون الدولي في الفضاء السيبراني.

علقت بعض الدول بشكل عام على تطبيق القانون الدولي فى الفضاء السيبراني، ولكن دون أن توضح كيف تنظر فى تطبيق مبادئ السيادة وعدم التدخل. على سبيل المثال، تناول بيان إستونيا بشأن القانون السيبراني والقانون الدولي عددًا من جوانب تطبيق القانون الدولي على الفضاء السيبراني، لكنه لم يتطرق صراحة إلى السيادة وعدم التدخل.[2] كونها تشكل تهديد خطير وشيك بانتهاك سيادة الدول وشؤونها الداخلية،[3] ولكن دون تحديد كيفية تطبيق هذه المبادئ فى الممارسة العملية.

سجلت المملكة المتحدة وجهة نظرها القائلة بأن مبدأ عدم التدخل ينطبق على العمليات السيبرانية للدول وقدمت أمثلة محددة للحالات التي ترى أن هذا المبدأ قد ينطبق فيها. صرحت المملكة المتحدة أيضًا أنه فى رأيها، لا يوجد حظر إضافي على النشاط السيبراني يمكن استقراءه من مبدأ السيادة. واتخذت مذكرة عام 2017 الصادرة عن المستشار العام المنتهية ولايته لوزارة الدفاع الأمريكية موقفًا مماثلاً بشأن السيادة.[4] على الرغم من أن هذا الموقف يتعارض مع تصريحات أخرى لمسؤولي حكومة الولايات المتحدة، والتي توقعت دورًا للسيادة فى تطبيق القانون الدولي على الفضاء الإلكتروني.[5]

وعلقت دول أخرى على أن مبدأ عدم التدخل ينطبق، لكنها لم تعلق على ما إذا كان مبدأ السيادة الأكثر عمومية ينطبق فى الفضاء الإلكتروني[6] .

---

[1] The Tallinn Manual 2.0 has become an important reference point for states, international organizations and academics; see, for example, the NATO cyber toolkit, NATO CCDCOE (n.d.), 'Cyber Law Toolkit', https://cyberlaw.ccdcoe.org/wiki/Main_Page (accessed 3 Oct. 2019). For a critique of both Tallinn Manuals, drawing the conclusion that there is currently limited support in state practice to support certain key rules, see Efrony and Shany (2018), 'A Rule Book on the Shelf?', p. 585; and discussion of this article in the Symposium on 'Sovereignty, Cyberspace and Tallinn Manual 2.0', AJIL Unbound 2017.

[2] 3 Kaljulaid, K. (2019), 'President of the Republic of Estonia at the opening of CyCon 2019', https://president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/ (accessed 4 Oct. 2019). In the context of noting that states are responsible for their activities in cyberspace, the President stated that 'sovereignty entails not only rights, but also obligations, but beyond that did not address the issue of how sovereignty applies in cyberspace.

[3] صرح المدعي العام السابق لإنجلترا وويلز: "أنا لست مقتنعًا بأنه يمكننا حاليًا استقراء قاعدة محددة أو حظر إضافي للنشاط السيبراني بخلاف التدخل المحظور من هذا المبدأ العام. وموقف حكومة المملكة المتحدة هو أنه لا توجد قاعدة من هذا القبيل باعتبارها مسألة تتعلق بالقانون الدولي الحالي "

, Wright, J. (2018), 'Cyber and International Law in the 21st Century', speech at Chatham House event May 2018.

[4] Memo from Jennifer M. O'Connor to the US Combatant Command, entitled International Law framework for employing Cyber Capabilities in Military Operations: '[m]ilitary cyber activities that are neither a use of force nor that violate the principle of non-intervention are largely unregulated by international law at this time…' (the memo is no longer publicly available but is quoted by Watts, S. and Richard, T. (2018), 'Baseline Territorial Sovereignty and Cyberspace', p. 827).

[5] U.S. Department of Defense, Office of General Counsel (1999), An Assessment of International Legal Issues in Information Operations 19 (2nd edition), which argued that 'an unauthorized electronic intrusion into another nation's computer systems may very well end up being regarded as a violation of the victim's sovereignty' (discussed by Watts at p. 853); Koh, H. H. (2012), 'International Law in Cyberspace', speech, response to question 9 on state sovereignty, https://2009 2017.state.gov/ s/l/releases/ remarks/ 197924.htm (accessed 4 Oct. 2019).

[6] أشار ملحق القانون الدولي لاستراتيجية أستراليا الدولية للمشاركة الإلكترونية إلى أنه "قد يشكل السلوك الضار في الفضاء الإلكتروني الذي لا يشكل استخدامًا للقوة انتهاكًا لواجب عدم التدخل في الشؤون الداخلية أو الخارجية لدولة أخرى". ولم يشر البيان الى السيادة. وزارة الشؤون الخارجية والتجارة بالحكومة الأسترالية (2019)، "ملحق لموقف أستراليا بشأن تطبيق القانون الدولي على سلوك الدولة في الفضاء الإلكتروني"

2019 International Law Supplement to Australia's International Cyber Engagement Strategy, Annex A, p. 1/5:

(ISSN: 2356 - 9492)

تنص الاستراتيجية الدولية للصين للتعاون فى الفضاء السيبراني، على أن مبدأ السيادة ينطبق فى الفضاء السيبراني، وأنه " لا ينبغي لأي دولة أن تسعى للهيمنة السيبرانية"، أو التدخل فى الشؤون الداخلية للدول الأخرى، أو الانخراط فى أو التغاضي أو دعم الأنشطة الإلكترونية التي تؤدي إلى تقويض الأمن القومي للدول الأخرى.

ومع ذلك، نظرًا لأن انتهاكات السيادة يمكن أن تغطي مجموعة من الأنشطة، بما فى ذلك فى سياق القواعد المحددة بشأن استخدام القوة وعدم التدخل المستمدة من مبدأ السيادة، فإن المعيار الذي تأخذه الدول بالحسبان عند تصنيف اعتداء ما من قبيل النزاعات المسلحة، ومن ثم يشكل انتهاكا للسيادة غير واضحة. يجب أيضًا قراءة البيانات الحكومية حول السيادة بشكل عام بعناية نظرًا لأن السيادة هي كلمة يمكن استخدامها بمعاني مختلفة فى السياقات غير السيبرانية والسيبرانية. [1]

فى سبتمبر 2019، عرضت فرنسا بشيء من التفصيل وجهات نظرها بشأن تطبيق القانون الدولي على الفضاء الإلكتروني، بما فى ذلك التدخلات السيبرانية الحكومية غير المصرح بها للأنظمة الفرنسية، أو أي إنتاج للتأثيرات على الأراضي الفرنسية بسبب الوسائل السيبرانية، قد تشكل انتهاكًا للسيادة.[2] .

المطلب الأول

القواعد العامة للسيادة ومدي انطباقها على الفضاء السيبراني

السيادة كعنصر أساسي للدولة هي الاستقلال، بقدر ما تستثنى الخضوع لأية سلطة أخرى، ولا سيما سلطة دولة أخرى. [3] كما علق القاضي ألفاريز فى قضية قناة كورفو[4] أنه، من خلال السيادة، "نفهم مجموعة الحقوق والصفات الكاملة التي تتمتع بها الدولة فى أراضيها، مع استبعاد جميع الدول الأخرى، وكذلك فى علاقاتها مع الدول الأخرى. يشير إعلان العلاقات الودية إلى "الحقوق المتأصلة فى السيادة الكاملة"[5]، وتنعكس هذه اللغة فى الصكوك الدولية الأخرى. فقانون هلسنكي على سبيل المثال: يشير إلى احترام المساواة فى السيادة على أنه حق كل دولة فى المساواة القانونية وسلامة الأراضي والحرية والاستقلال السياسي. كما أنه حرية الدولة في اختيار وتطوير أنظمتها السياسية والاجتماعية والاقتصادية والثقافية، فضلاً عن حقه فى تقرير قوانينه وأنظمته.[6]

---

https://dfat.gov.au/internationalrelations/themes/cyberaffairs/aices/chapters/2019_international_law_supplement.html (accessed 20 May 2021).

صرح المستشار القانوني لوزارة الخارجية الأمريكية آنذاك، برايان إيغان ، أن التدخل في الانتخابات سيكون انتهاكًا واضحًا لقاعدة عدم التدخل ، ولكنه كان أكثر دقة عند مناقشة السيادة: ينتهك سيادة دولة أخرى هو سؤال يواصل المحامون داخل حكومة الولايات المتحدة دراسته بعناية ، وهو سؤال سيتم حله في النهاية من خلال الممارسة والاعتقاد القانوني للدول.

Egan, B. (2017), 'International Law and Stability in Cyberspace', Berkeley Journal of International Law, 35(1): p. 13.

[1] نظرًا لأن انتهاكات السيادة يمكن أن تغطي مجموعة من الأنشطة، فإن المدى الذي تعتبر فيه الصين أو دول أخرى أن الأنشطة التي لا ترقى لمستوى عدم التدخل يمثل انتهاكًا للسيادة غير واضح. فى العام الماضي، بدأت بعض الدول فى نشر مواقفها بشأن السيادة بمزيد من التفصيل. فى يوليو 2019، حددت هولندا وجهة نظرها بأن كلا الجانبين الداخلي والخارجي للسيادة تنطبق بالكامل على المجال السيبراني وأنه لا يُسمح للدول بإجراء عمليات إلكترونية تنتهك سيادة دولة أخرى.

Government of the Netherlands (2019),'Letter to the parliament on the international legal order in cyberspace', https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the international-legal order-in-cyberspace (accessed 25 Nov. 2021)

[2] يبدو أن الحكم علي مدى مشروعية العمليات الإلكترونية التي لا ترقى لدرجة انتهاكا لمبدأ عدم التدخل ولسيادة الدولة المستهدفة، هي وجهة نظر معلنة لبعض الحكومات الأخرى

Ministère des Armées (2019), 'Droit International Applique Aux Operations Dans Le Cyberspace', https://www.defense.gouv.fr/salle-de-presse/ communiques/communiques-du-ministere-des-armees/communique_la-france-s-engage-a-promouvoir-un-cyberespace stable-fonde-sur-la-confianceet-le-respect-du-droit-international (accessed 5 Oct. 2021).

حتى الآن، عدد قليل نسبيًا من الدول عبرت عن موقفها من مبادئ القانون الدولى القابلة للتطبيق على الأنشطة في الفضاء السيبراني؛ مع غياب معاهدات بهذا الخصوص

Aside from the Council of Europe's Budapest Convention on Cybercrime, which focuses on criminal justice for cybercrime

[3] يشير أوبنهايم إلي السيادة، بأنها ممارسة السلطة العليا على جميع الأشخاص والأشياء داخل أراضيها، فالسيادة تنطوي على سلطة إقليمية.

Oppenheim, L. (1996), Oppenheim's International Law, Vol. 1: Peace, 9th edn, Jennings, R. Y. and Watts, A. (eds), London; New York: Longmans, p. 382.

[4] 7 Corfu Channel Case (United Kingdom v. Albania); Separate Opinion, 9 April 1949, ICJ Rep 43.

[5] Resolution 2625 (XXV) of 24 October 1970 containing the Declaration of Principles of International Law, Friendly Relations and Cooperation Among States in Accordance with The Charter of the UN, UN Doc. A/Res/2625.

[6] المادة الأولى من الوثيقة الختامية لمؤتمر الأمن والتعاون في أوروبا ("وثيقة هلسنكي النهائية") ، هلسنكي 1975 ؛ انظر أيضًا ، كمثال معاهدة الصداقة وحسن الجوار والتعاون بين

فالحقوق التي يجسدها مفهوم السيادة ستكون أساس أي مطالبة تقدمها دولة بأن دولة أخرى قد انتهكت سيادتها، ويشمل ذلك حقوق الدولة فيما يتعلق بأراضيها وحدودها البرية، والمجال الجوي، والبحر الإقليمي، وغيرها من المناطق البحرية. حيث تعكس أحكام المعاهدات وواجبات القانون العرفي المتعلقة بالمناطق البرية والبحرية والجوية واجب احترام سيادة الدولة على إقليمها ووحدة أراضيها؛ وكذلك الحال بالنسبة لقانون حظر استخدام القوة.

لا يقترن انتهاك السيادة الإقليمية دائماً باستعمال القوة. فى بعض الأنشطة التي قامت بها نيكاراغوا فى المنطقة الحدودية (كوستاريكا ضد نيكاراغوا)، وجدت محكمة العدل الدولية (ICJ) ، دون أن تجد ضرورة للنظر فى الادعاء المنفصل بوجود استخدام غير قانوني للقوة ، أن " نفذت نيكاراغوا أنشطة مختلفة فى المنطقة المتنازع عليها منذ عام 2010 ، بما فى ذلك الوجود العسكري فى أجزاء من تلك المنطقة. كانت هذه الأنشطة خرقا لسيادة كوستاريكا الإقليمية. "[1]

يشمل مبدأ السيادة الإقليمية حق الدولة فى ممارسة ولايتها داخل إقليمها. يمكن تقسيم الاختصاص القضائي هنا بشكل مفيد إلى سلطات التقادم والتنفيذ والمقاضاة. يمكن أيضًا اعتبار حق الدولة فى ممارسة جميع أشكال الولاية القضائية داخل أراضيها أحد الحقوق الناشئة عن جانب السيادة المتعلق باستقلال سلطات الدولة.

استقلالية سلطات الدولة

ومن الجوانب ذات الصلة فى حزمة الحقوق السيادية حرية الدول فى إدارة شؤونها الخاصة بشكل مستقل فيما يتعلق بأراضيها. يشار إلى عنصر السيادة هذا، المرتبط بالسيادة الإقليمية، فى حالة جزيرة بالماس: "السيادة فى العلاقات بين الدول تعني الاستقلال. الاستقلال فيما يتعلق بجزء من الكرة الأرضية هو الحق فى ممارسة وظائف الدولة فيه، باستثناء أي دولة أخرى.

ينص مشروع إعلان لجنة القانون الدولي بشأن حقوق الدول وواجباتها فى المادة 1 على أن `` لكل دولة الحق فى الاستقلال وبالتالي أن تمارس بحرية، دون إملاء من أي دولة أخرى، جميع سلطاتها القانونية، بما فى ذلك اختيار شكلها الخاص. الحكومة ".54 ينعكس هذا الحق فى المادة 2 (7) من ميثاق الأمم المتحدة، بإشارتها إلى المسائل" التي تدخل أساسًا فى الاختصاص المحلي لأي دولة ". [2]تشمل سلطات وحقوق الدول التي تندرج ضمن هذا الجانب من السيادة حق الدولة فى الاستقلال السياسي، بما فى ذلك الحق فى حرية اختيار نظامها السياسي والاجتماعي والاقتصادي والثقافي وتطويره، والحق فى ممارسة الولاية القضائية.[3] فى حين أن هذه السلطات الحكومية واسعة جدًا، يجب على الدول أن

إسبانيا والمغرب ، والتي تشير إلى 'جميع الحقوق المتأصلة والمتجسدة في ... السيادة ، على وجه الخصوص ، الحق في المساواة أمام القانون ، وسلامة الأراضي ، الحرية والاستقلال السياسي. علاوة على ذلك، تحترم [الأطراف] حق كل طرف في حرية اختيار وتطوير نظامه السياسي والاجتماعي والاقتصادي والثقافي ، وباستخلاص المصادر المذكورة أعلاه، يمكن وصف الحقوق الأساسية الثلاثة المتأصلة فى السيادة (مع واجبات مرتبطة بالدول الأخرى) على النحو التالي:

- الحق فى السلامة الإقليمية والسلطة الإقليمية (السيادة الإقليمية)؛
- الحق فى استقلال سلطات الدولة؛
- مساواة الدول فى النظام الدولي، والتي يشار إليها أحيانًا باسم "السيادة الخارجية" حيث ينص مشروع إعلان لجنة القانون الدولي بشأن حقوق الدول وواجباتها في المادة 1 على أن " لكل دولة الحق في الاستقلال وبالتالي أن تمارس بحرية، دون إملاء من أي دولة أخرى، جميع سلطاتها القانونية، بما في ذلك اختيار الحكومة.

Treaty of Friendship, Good-Neighbourliness and Cooperation between Spain and Morocco, signed at Rabat on 4 July 1991, General Principle 2.

[1] Certain Activities carried out by Nicaragua in the Border Area (Costa Rica v Nicaragua), Judgment, ICJ Reports 2015, para. 93. See also Corfu Channel (Merits) Judgment 9 April 1949.

[2] 5 UN Security Council (n.d.), 'Charter of the United Nations', Article 2(7). 'Nothing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any state'.

[3] محكمة العدل الدولية في القضية المتعلقة بالأنشطة العسكرية وشبه العسكرية في نيكاراغوا وضدها (نيكاراغوا ضد الولايات المتحدة الأمريكية)، الوقائع ، 27 يونيو 1986 ، محكمة العدل

(ISSN: 2356 - 9492)

تتصرف فى إطار القانون الدولي. بالإضافة إلى أي التزامات تعاهديه سارية، يجب على الدول أيضًا الالتزام بقواعد القانون العرفي، مثل تلك المتعلقة بعدم التدخل واحترام السيادة، إلى جانب الالتزامات المتعلقة بوضع الفرد وحمايته بموجب القانون الإنساني الدولي وقانون حقوق الإنسان.

المساواة فى السيادة

جانب آخر من جوانب السيادة هو المساواة بين الدول فى النظام الدولي، والتي يشار إليها أحيانا باسم "السيادة الخارجية". حيث يشير المبدأ إلى الاعتراف فى النظام الدولي بالمساواة المطلقة بين جميع الدول فيما يتعلق بحقوقها وواجباتها فى القانون الدولي، وليس المساواة فى السلطة أو فى الواقع. يعزز المبدأ فكرة أن كل دولة تتمتع بالحقوق المتأصلة فى السيادة مع الالتزام باحترام استقلال وسلطة الدول الأخرى.

كما يشمل حق الدولة فى ممارسة ولايتها القضائية على أراضيها السيادة الإقليمية وحق الدولة فى ممارسة سلطات الدولة المستقلة. وتتبع الطبيعة المستقلة والحصرية لهذا الحق من مبدأ المساواة فى السيادة. يتعامل أوبنهايم مع انتهاكات الاستقلال الداخلي والسيادة الإقليمية معًا، دون تمييز أي جانب تم انتهاكه.[1]

السيادة مبدأ شامل

هناك بعض القواعد المحددة التي تعكس المبدأ العام للسيادة والتي تنظم أو تحظر ممارسة دولة ما للسلطة فى إقليم دولة أخرى. وتشمل هذه القواعد الخاصة باستخدام القوة، والتي توجد فى ميثاق الأمم المتحدة والقانون الدولي العرفي.[2]

مبدأ عدم التدخل فى الشؤون الداخلية للدول الأخرى؛ وقانون البحار والجو، كما هو مدرج فى اتفاقية الأمم المتحدة لقانون البحار واتفاقية الطيران المدني الدولي (اتفاقية شيكاغو)، وكذلك القانون الدولي العرفي. هناك أيضًا معاهدات تمنح الموافقة أو تنظم أنشطة محددة داخل أراضي الدولة، مثل اتفاقيات فيينا للعلاقات الدبلوماسية والعلاقات القنصلية.

قد تنطبق هذه القواعد والقواعد المحددة الأخرى باعتبارها قانونًا خاصًا فيما يتعلق بممارسة سلطة الدولة بالمنطقة التي تتمتع فيها تلك الدولة بسلطات حصرية. حيث لا يوجد القانون الخاص المعمول به، تظل ممارسة دولة ما لسلطة الدولة فيما يتعلق بدولة أخرى محكومة بالقواعد العامة بشأن السيادة التي نوقشت أعلاه.

المطلب الثاني

تطبيق مبدأ السيادة فى الفضاء السيبراني

كان هناك بعض الجدل حول مدى انطباق مفهوم السيادة الإقليمية على الفضاء الإلكتروني.[3] ففى حين يرتبط انتهاك السيادة الإقليمية للدولة عادة ببعض التوغل المادي فى أراضي الدولة، سواء عن طريق البر أو البحر أو الجو. نجد أن الأنشطة السيبرانية للدول لها جانب مادي ملموس (على سبيل المثال أجهزة الكمبيوتر والبنية التحتية السيبرانية)، فالأنشطة فى الفضاء الإلكتروني لها أيضًا بُعد "افتراضي"، من خلال نقل البيانات، وإرسال الإشارات، وإرسال المحتوى بين الأجهزة المادية.

الدولية 14 ("قضية نيكاراغوا") ، والتي أشارت إلى "المسائل التي يسمح لكل دولة ، وفقًا لمبدأ سيادة الدولة ، أن تقرر بحرية. أحدها هو اختيار النظام السياسي والاقتصادي والاجتماعي والثقافي، وصياغة السياسة الخارجية (الفقرة 205). على الرغم من أن هذا تم ذكره في سياق مبدأ عدم التدخل، إلا أنه لا يزال وثيق الصلة بالسيادة لأن مبدأ عدم التدخل هو في حد ذاته انعكاس لمبدأ السيادة

[1] For example in para. 119, headed 'Violations of independence and territorial and personal authority', Oppenheim notes that 'It is not feasible to enumerate all such actions as might constitute a breach of a state's duty not to violate another state's independence or territorial or personal authority', and then goes on to give some examples; Oppenheim (1996), Oppenheim's International Law, Vol. 1: Peace, p. 385.

[2] Including consensus resolutions of the UN General Assembly, e.g. the Friendly Relations Declaration and Resolution 3314 (XXIX) of December 14, 1974 recommending to the United Nations Security Council a definition it should use for the crime of aggression.

[3] Tsagourias, N. (2015), 'The legal status of cyberspace,' in Buchan, R. and Tsagourias, N. (eds) (2015), Research Handbook on International Law and Cyberspace, Edward Elgar Publishing, p. 13

الالتزام الدولي ببذل العناية الواجبة في الفضاء السيبراني
بين التدابير الرادعة ومنع الأضرار السيبرانية العابرة

د. أسامة حمزة محمود عبد الفتاح

مجلة الدراسات القانونية والاقتصادية

وعلاوة على ذلك، فإن الفضاء الإلكتروني فى حد ذاته ليس له حدود إقليمية ثابتة. هناك العديد من أنواع بنية الشبكة والعديد من الطرق التي يتم بها تخزين البيانات، والتي قد تعبر الحدود الإقليمية. قد تكون البنية التحتية السيبرانية مثل خوادم الإنترنت موجودة فى منطقة معينة، لكن التفاعلات فى الفضاء الإلكتروني غالبًا ما تكون غير إقليمية، وفى بعض الأحيان تخضع لرقابة تنظيمية أكبر من قبل الشركات التكنولوجية العالمية، مثل Google وFacebook،[1] من الدول. أشار بعض الأكاديميين إلى صعوبة تعيين حدود الشبكة مباشرة من خلال الحدود الجغرافية.[2]

مع ذلك، فإن للفضاء السيبراني جانب مادي يتكون من حواسيب ودوائر متكاملة وكابلات وبنية تحتية للاتصالات. كما أن لها أبعاد تكنولوجية غير ملموسة تتكون من منطق البرمجيات وحزم البيانات؛ وهناك البعد البشرى أيضاً.[3] تقع هذه المعدات المادية داخل أراضي الدولة، وتملكها الحكومات والشركات. وهكذا، فإن الفضاء السيبراني لا يوجد بشكل مستقل عن العالم المادي، ولكنه متجذر فيه.[4]

يمكن للدولة أن تمارس سيادتها على البنية التحتية السيبرانية داخل حدودها الإقليمية (وفيما يتعلق بالأقمار الصناعية، فى نطاق ولايتها القضائية). وعلى الأشخاص الموجودين على أراضيها وفيما يتعلق بمواطنيها فى الخارج. لذلك، ينطبق مبدأ السيادة فيما يتعلق بالأنشطة الإلكترونية للدول، من خلال قدرة الدولة على تنظيم مثل هذه الأمور داخل حدودها الإقليمية وممارسة سلطات الدولة المستقلة.[5]

للدول الحق فى ممارسة سلطاتها السيادية على البنية التحتية السيبرانية فى أراضيها بشكل حصري ومستقل، كما هو الحال فى السياق غير السيبراني. حيث تخضع بعض الصلاحيات ذات الصلة بالبنية التحتية الإلكترونية لالتزامات الدول بموجب القانون الدولي لحقوق الإنسان.[6] فقد تختار بعض الدول تنظيم جوانب معينة من النشاط الإلكتروني فى أراضيها، على سبيل المثال من خلال القوانين المتعلقة بمعالجة البيانات الشخصية والمحتوى المسموح به على الإنترنت.

---

[1] Increasingly state cyber activity takes place in relation to other state's territories through cyber infrastructure owned or controlled by powerful private companies such as Facebook or Google rather than by states,

راجع أيضاً:

Shapshak, T. (2019), 'Google and Facebook to Build Own Undersea Cables Around Africa', Forbes, 3 July 2019, https://www.forbes.com/sites/tobyshapshak/2019/07/03/google-and-facebook-to-build-own-underseacables-around-africa/ (accessed 4 Oct. 2021). Efrony and Shany argue that the deterritorialized and virtual aspects of cyberspace put in question the long-term sustainability of key assertions of the Tallinn Manual 2.0, Efrony and Shany (2018), 'A Rule Book on the Shelf?', p. 652.

[2] Yuan Yi for example has argued that it is unfair to use the geographic locations of cyber infrastructure, as in the Tallinn Manual 2.0, as the sole criterion to define network frontiers: 'If we applied this rule, much of the internet would be American territory and subject to US sovereignty, as most Internet root servers and many enterprise servers are located there': Zeng, J., Stevens, T., and Chen, Y. (2017), 'China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty"', Politics & Policy, 45(3): pp. 432–464

[3] Tsagourias (2018), 'Law, Borders and the Territorialisation of Cyberspace', p. 16

[4] تشمل المعاملات فى الفضاء السيبراني أشخاصًا حقيقيين فى ولاية قضائية

Goldsmith, J. L. (1998), 'Against Cyberanarchy', The University of Chicago Law Review, 65(2): p. 32.

راجع أيضا:

Buchan, R. (2018), Cyber Espionage and International Law, Hart Publishing, p. 50.

[5]6 The international group of experts involved in the Tallinn Manual 2.0 agreed that '[a] State enjoys sovereignty authority with regard to the cyber infrastructure… located within its territory', Schmitt (2017), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, p. 13. See also Tsagourias, N. (2019), 'The Slow Process of Normativizing Cyberspace', AJIL Unbound, 113: pp. 71–75, p. 73; Schmitt and Vihul (2017), 'Respect for Sovereignty in Cyberspace', Texas Law Review, 95(7): pp. 1639–1670.

[6] قرر مجلس حقوق الإنسان التابع للأمم المتحدة أن حقوق الإنسان مثل حرية التعبير وحرية التجمع والخصوصية تنطبق على الإنترنت بقدر ما تنطبق خارج الإنترنت: قرار بشأن تعزيز حقوق الإنسان وحمايتها والتمتع بها على الإنترنت inbehavior, UN Doc A/HRC/20/L.13. One of the voluntary, non-binding norms for responsible state the use of ICT technology agreed by the UN GGE in 2015 was that states should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the internet (para 13(e) of the UN GGE's 2015 report).

(ISSN: 2356 - 9492)

حيث تفرض بعض الدول الاستبدادية ضوابط أكثر صرامة على الوصول إلى الإنترنت والبيانات الشخصية، وهو المفهوم الذي تمت الإشارة إليه باسم "الإنترنت".[1] فالدول التي تتبنى مقاربة واسعة لوجود سلطاتها على جميع جوانب سلوك المواطنين تأخذ نظرة واسعة مماثلة لواجبات الدول الأخرى فى احترام سيادتها وقد تتذرع بانتهاكات السيادة أو مبدأ عدم التدخل بشكل أكثر انتظامًا من الآخرين لكن السلطات التي تختار الدول أن تتحملها بموجب القانون الوطنى فيما يتعلق بالنشاط السيبراني (سواء كانت متوافقة مع القانون الدولي لحقوق الإنسان أم لا) هي قضية منفصلة عن نطاق الوظائف السيادية للدولة بطبيعتها. وبالتالي، فإن مبدأ السيادة ينطبق فيما يتعلق بالأنشطة الإلكترونية للدول، من خلال قدرة الدولة على تنظيم مثل هذه الأمور داخل حدودها الإقليمية وممارسة سلطات الدولة المستقلة.[2]

لا تشمل هذه الوظائف تنظيم الدولة لأنشطة المواطنين العاديين أو الأمور التجارية. حيث ينعكس هذا النهج فى قضية نيكاراغوا، حيث استشهدت محكمة العدل الدولية "باختيار نظام سياسي واقتصادي واجتماعي وثقافي، وصياغة السياسة الخارجية"، كأمثلة على الأمور التي يمكن للدولة أن تقرر فيها بحرية بموجب هذا المبدأ لسيادة الدولة. وبالتالي، يجب إعطاء مصطلح "الوظائف السيادية بطبيعتها" قراءة موضوعية.

المطلب الثالث

الالتزام ببذل العناية السيبرانية خارج الحدود الإقليمية

قد يمتد الالتزام ببذل العناية الواجبة خارج الحدود الإقليمية فى حالتين. عندما تسيطر دولة ما على إقليم فى الخارج دون ممارسة السيادة عليها، كما فى حالة ضم إقليم أو احتلال عسكري. عندما يكون الأمر كذلك، يقع على عاتق الدولة التزام ببذل العناية الواجبة تجاه البنية التحتية السيبرانية والأنشطة المتعلقة بها.[3]

وحذر الخبراء من أن مفهوم السيطرة ليس بالضرورة مرادفًا لمفهوم الولاية القضائية. على سبيل المثال، قد تتمتع الدولة بالاختصاص القضائي على أنشطة شركاتها فى الخارج، لكنها تفتقر إلى القدرة على التحكم فى البنية التحتية السيبرانية التي تديرها. وبالتالي إن مناط تحمل الدولة لالتزام العناية الواجبة خارج الحدود الإقليمية هو أن الدولة تسيطر فعليًا على البنية التحتية الإلكترونية المعنية لأنها تشغل البنية التحتية المذكورة أو أن البنية التحتية موجودة فى إقليم أو مباني أو أشياء تتحكم فيها بشكل واقعي.[4]

من الواضح أن إرفاق الالتزام ببذل العناية الواجبة خارج الحدود الإقليمية يحدث عندما تمارس دولة سيطرة حصرية على شيء معين (البنية التحتية السيبرانية أو الأنشطة).[5] فى حالات السيطرة المتزامنة من قبل أكثر من دولة واحدة، تتحمل كلتا الدولتين التزام العناية الواجبة. ومن الأمثلة على ذلك، منشأة للعمليات السيبرانية تديرها دولتان على نحو مشترك.

---

[1] في الصين، ترى الحكومة أنه يجب أن يكون لها سلطة قضائية حصرية على المحتوى والبيانات والخدمات التي يمكن توفيرها أو الوصول إليها على الإنترنت داخل أراضي الدولة ("السيادة الإلكترونية، والتي تتجلى جزئيًا من خلال" جدار الحماية العظيم "). نجحت الصين إلى حد كبير في التحكم في وصول مواطنيها إلى الفضاء الإلكتروني داخل حدودها الإقليمية، وهو نموذج يتم نسخه في عدد من الدول الأخرى. في نوفمبر 2019، سنت روسيا قانونًا (يُعرف باسم "قانون الإنترنت السيادي") الذي يقدم صلاحيات واسعة النطاق لتقييد حركة الإنترنت داخل روسيا . كما اتخذت الدولة مجموعة من الإجراءات التقييدية تتضمن الحظر الشامل لبعض منصات التواصل الاجتماعي (Facebook , Twitter) بمناسبة العمليات العسكرية التي تشنها على أوكرانيا.

[2] أن مضمون "السلطات السيادية بطبيعتها" أو "الوظائف الحكومية بطبيعتها" محدد فى القانون الدولي؛ توفر القواعد الخاصة بحصانة الدولة سياقًا واحدًا. تُفهم هذه الوظائف على أنها نشاط يقع فى صميم سلطة الدولة، بما فى ذلك أنشطة السلطات المسؤولة عن الشؤون الخارجية والعسكرية؛ التشريع، السلطة التنفيذية والسلطة القضائية.

Fox, H. and Webb, P. (2015), The Law of State Immunity, 3rd edition, Oxford University Press, p. 399.

[3] Hessbruegge, Jan Arno. "The Historical Development Of The Doctrines Of Attribution And Due Diligence In International Law." NYUJ Int'l. L. & Pol. 36 (2003): 265.

[4] Patrick, Colin. "Debugging The Tallinn Manual 2.0's Application Of The Due Diligence Principle To Cyber Operations." Wash. Int'l LJ 28 (2019): 581.

[5] Jensen, Eric Talbot. "Cyber sovereignty: The way ahead." *Tex. Int'l LJ* 50 (2015): 275. Bendiek, Annegret. "Due diligence in cyberspace: guidelines for international and European cyber policy and cybersecurity policy." (2016): 33.

أيضاً ناقش فريق الخبراء الدولي "مسؤولية الدولة" التي تمر من خلالها البيانات فقط، على سبيل المثال من خلال كابل ألياف بصرية، ومدى تحملها التزام العناية الواجبة. ميّز الخبراء هذا الوضع عن الوضع الذي يتم فيه إنشاء بنية تحتية إلكترونية محددة على أراضي الدولة لأغراض ضارة، مثل التي تشتمل على الروبوتات القاتلة. واتفقوا على أنه، كمسألة قانونية صارمة، تتحمل دولة العبور واجب العناية الواجبة[1] ويجب أن تتصرف وفقًا للقاعدة 7 عندما:

(1) تمتلك المعرفة (بناءً على المعرفة الفعلية والبناءة) بعملية مخالفة تصل إلى مستوي الضرر. (2) يمكن أن تتخذ تدابير مجدية لإنهائه بشكل فعال.

ومع ذلك، فإن الخبراء، مع مراعاة الوضع الحالي، لتكنولوجيا الهجمات السيبرانية وتطور أنماط الاتصالات الإلكترونية[2]، أقرت بأنه من غير المحتمل عادةً أن تعرف "دول العبور" هذه الأنشطة الضارة التي تمر عبر بنيتها التحتية الإلكترونية وأن تكون قادرة على تحديدها. قد تكون تلك البرامج الضارة غير معروفة ولن يتم اكتشافها بواسطة البرامج التقليدية ، ربما ذلك بفضل التكنولوجيا فائقة التعقيد التي يتم الاعتماد عليها في الهجمات السيبرانية.[3]

بالإضافة إلى ذلك، تمر معظم حركة الإنترنت عبر البنية التحتية السيبرانية المملوكة للقطاع الخاص لمزودي خدمة الإنترنت (ISP). وفى حالة اكتشاف برامج ضارة، يحدد القانون الوطني ما إذا كان مزود خدمة الإنترنت لديه واجب قانوني لإبلاغ سلطات الدولة. ومع ذلك، اتفق الخبراء على أن المبدأ القانوني المنصوص عليه فى الفقرة السابقة يعكس الالتزام القانوني الذي تتحمله دول العبور. إن القضية تتعلق بالمعرفة، وليس قابلية تطبيق مبدأ العناية الواجبة.

المطلب الرابع

معايير تحديد انتهاكات السيادة فى الفضاء السيبراني

قام فريق الخبراء الدولي المشتركين فى دليل تالين 2.0 باستكشاف ما إذا كان من الممكن تحديد معايير التعدي على "السلامة الإقليمية" للدولة المستهدفة[4]، حيث لن تصل عمليات الاقتحام السيبراني عن بُعد إلا إلى مستوى انتهاك السيادة حيث يحدث مستوى معين من الآثار الضارة على أراضي الدولة الضحية. لقد فعلوا ذلك بالرجوع إلى تسلسل هرمي للسيناريوهات، على النحو التالي:

• التلف المادي أو الإصابة (مثل البرمجيات الخبيثة التي تسبب خللًا فى عناصر تبريد المعدات، مما يجعل المكونات غير قابلة للتشغيل، كما هو الحال فى عملية Stuxnet)؛

• فقدان وظائف البنية التحتية السيبرانية (مثل اختراق جهاز كمبيوتر ونشر فيروس قوي يعطل الوظائف، مما قد يؤدي أيضًا إلى الحاجة إلى استبدال أجهزة الكمبيوتر، كما هو الحال فى عملية "شمعون" الإلكترونية ضد شركة النفط السعودية، أرامكو) [5]؛ و

---

[1] Jensen, Eric Talbot, and Sean Watts. "Cyber Due Diligence." *Okla. L. Rev.* 73 (2020): 645. Schmitt, Michael N. "In defense of due diligence in cyberspace." *Yale LJF* 125 (2015): 68.

[2] Payne, Christian, and Lorraine Finlay. "Addressing obstacles to cyber-attribution: A model based on state response to cyber-attack." *Geo. Wash. Int'l L. Rev.* 49 (2016): 535.

[3] Jones, Malachi, Georgios Kotsalis, and Jeff S. Shamma. "Cyber-attack forecast modeling and complexity reduction using a game-theoretic framework." Control of cyber-physical systems. Springer, Heidelberg, 2013. 65-84

[4] من المسلم به أن مصطلح `` السيادة الإقليمية " قد يكون أكثر ملاءمة هنا من انتهاك `` وحدة أراضي الدولة ''، حيث يشير الأخير إلى أن جزءًا من الأرض يتم الاستيلاء عليه من قبل دولة أخرى، والذي لا يتناسب بشكل جيد مع نوع الضرر الذي تسبب فيه من خلال الهجمات الإلكترونية الحكومية. تمت الإشارة أيضًا في الفقرة 37 إلى أن المحاكم والمعلقين الدوليين في السياق غير الإلكتروني تعاملوا مع عناصر السيادة على أنها مترابطة، بدلاً من تقسيم السيادة إلى عناصر منفصلة، ولا يبدو أن هناك سببًا لعدم اتباع نفس النهج في السياق السيبراني. عملية Stuxnet ، التي تم الكشف عنها في عام 2010 ، استهدفت منشأة تخصيب اليورانيوم الإيرانية ، وأسفرت عن أضرار مادية لعدد كبير من أجهزة الطرد المركزي النووية

[5] The Shamoon virus, uncovered in 2012, overwrote the master boot record of infected computers, rendering the computers unusable thereafter.

(ISSN: 2356 - 9492)

• نشاط أقل من فقدان الوظيفة، على سبيل المثال تباطؤ الكمبيوتر. التسبب فى عمل البنية التحتية الإلكترونية أو البرامج بشكل مختلف؛ أو تعديل أو حذف البيانات دون عواقب مادية أو وظيفية.

فكرة انتهاك السيادة على أساس مستويات مختلفة من التأثير الضار قد استُلهمت جزئياً على الأقل من مناقشة "مبدأ الآثار" فى سياق القواعد المتعلقة باستخدام القوة، والتي أشار إليها فريق الخبراء الدولي تعتبر أيضا فى سياق الهجمات الالكترونية ترعاها الدولة.[1] فمن الناحية العملية، يعد الضرر المادي الذي يلحق بالبنية التحتية الإلكترونية نتيجة للتدخل الإلكتروني أقل شيوعًا من فقدان الوظائف أو بعض التأثير أدناه ، لذا فإن المعيارين الأخيرين أعلاه سيكونان الأكثر أهمية لغرض التدخلات السيبرانية منخفضة المستوى.[2] لكن وضع حد أدنى بناءً على التأثيرات فى الحالة المستهدفة يثير عددًا من التحديات .[3]

اتخذ فريق الخبراء الدولي مواقف مختلفة بشأن المكان الذي ينبغي رسم الخط فيه، سواء فيما يتعلق بالمعيار المقترح "فقدان الوظيفة"[4] وفيما يتعلق بالضرر دون فقدان الوظيفة.[5]

السيناريوهات المذكورة أعلاه - التأثيرات، الهدف وطبيعة التداخل- تدل على مقياس تنازلي من الخطورة، لكنها فى الممارسة العملية ليست بهذه البساطة.

لا يؤدي حذف بيانات حكومية مهمة لدولة ما من قبل دولة خارجية بالضرورة إلى آثار مادية أو فقدان للوظائف، ولكن قد يكون له تأثير أكثر خطورة على قدرة الدولة المستهدفة على ممارسة وظائفها الحكومية. هل يجب قياس "الضرر" الناجم عن التدخل السيبراني من الناحية الكمية أو النوعية، أم كليهما؟

افترضت بعض الدول أنه بالإضافة إلى الخطورة، قد يكون حجم التأثيرات على المجتمع عاملاً يجب أخذه فى الاعتبار عند النظر فيما إذا كان الهجوم الإلكتروني يمكن أن يشكل انتهاكًا للسيادة.

ليس من الواضح حاليًا ما تعتقده معظم الدول حول فكرة النهج "القائم على التأثيرات" لانتهاكات السيادة فى الفضاء الإلكتروني (بما يتجاوز موقف المملكة المتحدة بعدم الاعتراف بقاعدة السيادة فى الفضاء الإلكتروني) نظرًا لأن عددًا قليلاً من الدول، كما هو مذكور أعلاه قد سجلوا وجهات نظرهم. أشارت الحكومة الفرنسية، فى تقريرها الصادر فى سبتمبر 2019، بالإضافة إلى أن أي اقتحام إلكتروني غير مصرح به للنظام الفرنسي من شأنه أن يشكل انتهاكًا للسيادة، إلى أن السيادة يمكن انتهاكها من خلال `` أي إنتاج للآثار بالوسائل الإلكترونية على الأراضي الفرنسية.[6] يعتمد نظام تصنيف الحوادث السيبرانية الوطني فى فرنسا على تقييم تقني وقائم على التأثيرات للعملية الإلكترونية.

هناك مؤشرات على أن الدول الأخرى تفكر بجدية أيضًا فى اتباع نهج قائم على تقييم الأثار الناجمة عن تلك الانتهاكات. تلمح حكومة هولندا إلى حدود السيادة فى بيانها الأخير بشأن تطبيق السيادة على الفضاء الإلكتروني، وتشير إلى أنها "بشكل عام" تؤيد القاعدة 4 من دليل تالين 2.0 "لوضع حدود السيادة فى المجال السيبراني".[7]

[1] Commentary to Rule 69 of the Tallinn Manual 2.0. Schmitt has proposed that the criteria used to decide whether a cyberattack constitutes a use of force should be focused predominantly on the consequences of the attack. The first of his seven proposed criteria is severity, i.e. the level of destruction caused by the attack. Under this criterion, the scope, duration and intensity of the attack are taken into consideration.

[2] The Stuxnet operation is a relatively rare example of the causation of physical damage

[3] Schmitt, M. N. (2017), 'Grey Zones in the International Law of Cyberspace', The Yale Journal of International Law, 42(2): p. 11, referring to a 'confusing melange of views' on this issue. Von Heinegg, W. H. (2012), 'Legal Implications of Territorial Sovereignty in Cyberspace', 2012 4th International Conference on Cyber Conflict, NATO CCD COE Publications, Tallinn, p. 5, states that 'if … there is no or merely minor material damage to the cyber infrastructure it is not really settled whether that activity can be considered a violation of sovereignty'.

[4] The international group of experts involved in the Tallinn Manual 2.0 could not agree on the threshold at which cyber intrusions that result in a loss of functionality could qualify as a violation of sovereignty: Tallinn Manual 2.0, pp. 20–21, para 13 of commentary to Rule 4

[5] Below the threshold of loss of functionality, there was also no agreement among the experts: ibid., para 14 of the commentary to Rule 4.

[6] Ministère des Armées (2019), 'Droit International Applique Aux Operations Dans Le Cyberspace'.

[7] 'It should be noted that the precise limits of what is allowed and what is not allowed have not been fully crystallized', Minister of the Netherlands (2019), 'Statement to parliament on 5 July 2019'.

وقد افترضت بعض الدول أنه بالإضافة إلى الخطورة، فإن حجم التأثيرات على المجتمع قد يكون عاملاً يجب أخذه فى الاعتبار عند النظر فيما إذا كان الهجوم الإلكتروني يمكن أن يشكل انتهاكًا للسيادة.[1] ركز آخرون على الآثار العملية على الدولة الضحية. سيما تأثير تلك الممارسات على تنظيم الدولة وظائفها السيادية داخل أراضيها.

إن فكرة النهج القائم على تقييم الأثار الناجمة عن النشاط السيبراني من خارج الاتحاد الأوروبي داخل أقاليم الدول الأعضاء، هي أيضًا فكرة اعتمدها الاتحاد الأوروبي مؤخرًا فيما يتعلق بنظام العقوبات السيبرانية الذي تم سنه حديثًا.[2]

حيث تستهدف العقوبات الهجمات الإلكترونية التي لها (يحتمل) أن يكون لها "تأثير كبير"، والتي تشكل تهديدًا خارجيًا للاتحاد الأوروبي أو الدول الأعضاء فيه. يسرد قرار الاتحاد الأوروبي العناصر التالية باعتبارها العوامل التي تحدد عوامل تقييم الهجوم الإلكتروني وما ينتجه من أثار.

1. نطاق، أو حجم، أو تأثير، أو شدة الاضطراب الناجم، بما فى ذلك الأنشطة الاقتصادية والاجتماعية، أو الخدمات الأساسية، أو وظائف الدولة الحيوية، أو النظام العام، أو السلامة العامة؛
2. عدد الأشخاص الطبيعيين، أو الاعتباريين، أو الكيانات، أو الهيئات المتضررة؛
3. عدد الدول الأعضاء المتضررة؛
4. مقدار الخسارة الاقتصادية الناتجة، على سبيل المثال من السرقة على نطاق واسع للأموال أو الموارد الاقتصادية أو الملكية الفكرية؛
5. المنفعة الاقتصادية التي يجنيها الجاني لنفسه أو لغيره؛
6. كمية أو طبيعة البيانات المسروقة أو حجم انتهاكات البيانات؛ أو
7. طبيعة البيانات الحساسة تجارياً التي تم الوصول إليها.[3]

فى حين أن قرار الاتحاد الأوروبي لا يشير إلى السيادة أو التدخل، إلا أنه مثال مثير للاهتمام للدول التي تضع معايير لعدم مشروعية النشاط السيبراني بناءً على قائمة واسعة النطاق من العوامل،

من الناحيتين الكمية والنوعية. نلاحظ أن الإشارة إلى "النطاق، أو التأثير، أو شدة الاضطراب الناجم" مرتبطة كما أوضحنا أعلاه، بالتأثير فى وظائف الدولة بطبيعتها، مثل الأنشطة الاقتصادية والمجتمعية؛ الخدمات الضرورية؛ وظائف الدولة الحرجة ذات الصلة بالنظام عام؛ أو السلامة العامة.

هذه العلاقة السببية بين السلوك وتنفيذ الدولة لوظائفها الحصرية والمستقلة، قريبة جدًا من فكرة انتهاك السيادة (أي الممارسة غير المصرح بها للسلطة فيما يتعلق بالوظائف السيادية لدولة أخرى) ومع ذلك، من الواضح أن معايير الاتحاد الأوروبي أوسع نطاقًا، وتتجاوز النطاق والتأثير لتشمل، على سبيل المثال، الخسارة الاقتصادية ونوع البيانات المسروقة.

تكمن الصعوبة فى أنه كما ذكر أعلاه، خارج السياق السيبراني، من الصعب تحديد معايير أو معايير لما يشكل انتهاكًا للسيادة، بما يتجاوز الصيغة العامة لممارسة السيادة من قبل دولة فى أراضي دولة أخرى دون موافقة فيما يتعلق بمنطقة يكون للدولة الإقليمية نفسها الحق الحصري فى ممارسة سلطات الدولة عليها بشكل مستقل.[1]

[1]

[2] EU Council (2019), EU Council decision (CFSP) 7299/19 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, 14 May 2019, https://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/en/pdf (accessed 6 Oct. 2021).

[3] Ibid., Article 3.

(ISSN: 2356 - 9492)

قد يجادل مؤيدي النهج الشامل للسيادة بأن نطاق والأثار الناجمة عن الفعل غير المشروع قد تكون مصدرًا لمعايير مثل تلك المتعلقة بالتدخل واستخدام القوة، ولكنها لن تكون فعالة عندما يتعلق الحال بانتهاك السيادة، وأن الآثار هي بالأحرى مسألة تتعلق بالإنفاذ وتقدير التعويض.

الأمر ليس واضحًا أو محسومًا، كما أن عدم وجود اتفاق حول ما إذا كان هناك حد أدنى لانتهاكات السيادة فى السياق غير السيبراني يلقي بظلاله فى السياق السيبراني. حتى الآن، يبدو أيضًا أنه لا يوجد اتفاق بشأن أنواع التأثيرات التي ستكون مطلوبة بموجب عتبة الحد الأدنى. صيغة Tallinn Manual 2.0، التي تستورد عقيدة تستند إلى الشدة الآثار المستمدة من قواعد استخدام القوة، هي نسخة واحدة؛ والآخر هو التأثيرات العملية على قدرة الدولة الضحية على ممارسة سلطاتها المستقلة على المجتمع (وهي قريبة من كيفية مبدأ عدم التدخل يعمل فى الممارسة).

تقدم التدابير التقييدية للاتحاد الأوروبي مجموعة من العوامل الأخرى التي يجب مراعاتها فى سياق تنظيم الهجمات الإلكترونية التي يتم إجراؤها عن بُعد بناءً على شدة الأثار الناجمة. أن الاتفاق على معايير تحديد الانتهاكات فى الفضاء غير موجود حاليًا. حتى يتم التوصل إلى مثل هذا الاتفاق بين الدول، إن تحديد ما يعد حدوث انتهاك للسيادة يخاطر بأن يصبح ممارسة ذاتية بدلاً من ممارسة قائمة على تفسير متفق عليه بشكل متبادل لتطبيق السيادة فى الفضاء السيبراني.

المبحث الثاني
تقدير الأضرار الناجمة عن الانتهاكات غير الجسيمة المحتملة فى الفضاء السيبراني

من بين المسائل التي لم يحسمها الفقه القانوني، هي آليات تقدير الأضرار الناجمة عن العمليات السيبرانية وأثارها على مبدأ بذل العناية الواجبة ومسؤولية الدولة المالكة للبنية التحتية السيبرانية، حيث اتفق فريق الخبراء الدولي على أن القاعدة تشمل جميع العمليات الإلكترونية التي تنتهك حقوق الدولة المتضررة بموجب القانون الدولي ولها "عواقب وخيمة".

ويشمل ذلك، تلك العمليات الإلكترونية التي تقوم بها دولة ما والتي تنتهك التزامًا قانونيًا دوليًا تجاه الدولة المستهدفة. وغالباً ما يثار الجدل حول مسؤولية الكيانات الخاصة كالتنظيمات الإرهابية أو العصابات الاجرامية المتخصصة في القرصنة عبر الانترنت. وهو ما نحاول تسليط الضوء عليه فيما يلي. سيما أن غالبية التهديدات السيبرانية وإن كانت بترتيب من دولة ما، إلا أنها تتم عبر تلك الكيانات.

نحاول في هذا الشق من الدراسة تسليط الضوء على بعض إشكاليات العناية الواجبة ذات الصلة بطبيعة النشاط السيبراني:

1

- بذل العناية الواجبة فى مواجهة الأعمال الانتقامية للكيانات الخاصة
- مسؤولية الكيانات الفاعلة غير الدولية عن الهجمات السيبرانية
- **نظرية الحد الأدنى للضرر في الفضاء السيبراني**
- طبيعة الالتزام بمنع الضرر العابر فى القانون الدولي

ومدي انطباقه فى السياق السيبراني

المطلب الأول

بذل العناية الواجبة فى مواجهة الأنشطة السيبرانية للكيانات الخاصة

تنامت أنشطة الجهات الفاعلة غير الحكومية على المسرح الدولي بشكل مطرد فى السنوات الأخيرة .فالميزات الفريدة للفضاء السيبراني، بما فى ذلك طابعه الذي لا حدود له، وترابطه المتأصل، وإخفاء الهوية الذي يوفره وإمكانية الوصول إليه، قد وفّر بيئة مزدهرة للجهات الفاعلة غير الحكومية. فقد مكّن الفضاء الإلكتروني الجهات الفاعلة غير الحكومية من العمل بشكل مستقل عن الدول فى الساحة الدولية . فمن المرجح أن الأعمال العدائية السيبرانية العابرة للحدود تتجاوز الآن السلوك الذي ترتكبه الدول .[1]

فى مجتمع دولي قائم على المساواة فى السيادة بين الدول الأعضاء فيه، يطالب القانون الدولي بوجود قواعد قانونية دولية فعالة توفر للدول الحماية من الجهات الفاعلة غير الحكومية التي ترتكب سلوكًا إلكترونيًا ضارًا من أراضي دول أخرى.

وذلك من خلال، اتخاذ خطوات نحو إرساء مسؤولية الجهات الفاعلة غير الحكومية عن سلوكها بموجب القانون الدولي، حيث كانت التطورات فى هذا السياق بطيئة ومجزأة. والدول ليست مسؤولة بشكل عام عن سلوك الجهات الفاعلة غير الحكومية التي تلحق الضرر بالدول الأخرى لمجرد وجود صلة إقليمية؛ أي مسؤولية الدولة على أساس أن كيان خاص غير الدول قد ارتكب مثل هذا السلوك أثناء وجوده داخل أراضي تلك الدولة، ومع ذلك، هناك طريقتان أساسيتان يمكن من خلالهما أن تتحمل الدول المسؤولية فى مثل هذه الظروف[2].:

أولاً، تكون الدولة مسؤولة عن أفعال جهة فاعلة من غير الدول حين تشكل هذه التصرفات سلوكًا غير مشروع دوليًا ويمكن أن ينسب هذا السلوك إلى الدولة؛ وذلك عندما تمارس الدولة سيطرة فعلية على السلوك غير القانوني المعني، كالسلوك السيبراني الضار الذي ترتكبه جهات غير حكومية دون أن تبذل الدولة العناية الواجبة فى إيقاف هذا السلوك[3].

ومع ذلك نرى أن هناك بعض المعوقات بصدد تطبيق هذا المعيار، فإسناد المسؤولية الدولية عن السلوك السيبراني الضار الذي ترتكبه جهات فاعلة من غير الدول يواجه صعوبة إيجاد الصلة الواقعية بين الدولة والتصرفات الصادرة من الجهات الفاعلة غير الحكومية، فـيجب بالضرورة أن يتحقق الإسناد التقني للفاعل الذي ارتكب الفعل غير المشروع دوليًا بدقة.

[1] Blank, Laurie R. "International law and cyber threats from non-state actors." *Israel Yearbook on Human Rights, Volume 43 (2013)*. Brill Nijhoff, 2013. 111-139.

[2] Although on the international legal responsibility of non-state actors that commit malicious cyber operations from the territory of failed states or ungoverned spaces see in this volume (Responsibility for Malicious Cyber Activities by Non-State Actors Operating from Failed States or Ungoverned)

[3] Application of the Convention on the Protection and Punishment of the Crime of Genocide (Bosnia v Serbia) (2007) ICJ Rep 1, para 400.

(ISSN: 2356 - 9492)

يعد هذا أمرًا صعبًا فى الفضاء السيبراني لأنه على الرغم من تخصيص عناوين بروتوكول الإنترنت (IP) للأجهزة المتصلة بالإنترنت، إلا أنها لا تكشف عن الهوية المحددة للجهاز للمستخدمين الآخرين، ولكن فقط عن موقعهم الجغرافي العام.[1]

تحول تقنيات وبرامج إخفاء الهوية فى جوهرها دون هذه الإسناد التقني بشكل كبير، لأنها تعيد توجيه السلوك السيبراني الضار من خلال البنية التحتية السيبرانية للدول الأخرى وفى هذه العملية يتم تخصيص عناوين IP مختلفة، مما يشير إلى الضحية أن السلوك الضار قد تم إطلاقه من جهاز كمبيوتر فى موقع جغرافي مختلف عن مصدره الأصلي.

فى حين أن التطورات التكنولوجية الأخيرة تعني أن التتبع الدقيق عبر الإنترنت أصبح ممكنًا الآن، إلا أنه لا يزال صعبًا للغاية .فالسيطرة الفعالة أو، على حد تعبير لجنة القانون الدولي (ILC) ، يجب أن تكون الدولة قد وجهت أو تحكمت فى السلوك غير القانوني كما هو موثق جيدًا فى الأدبيات ، وهذا يتطلب ؛ الدرجة العالية بشكل استثنائي من السيطرة الواقعية التي يجب ممارستها من أجل إثبات الإسناد القانوني.[2]

ثانيًا، يمكن أن تتحمل الدولة المسؤولية عندما تفشل فى الوفاء بالتزام أساسي، سواء كان تقليديًا أو عرفيًا، لاتخاذ إجراء إيجابي فيما يتعلق بسلوك جهة فاعلة من غير الدول تعمل داخل أراضيها أو، على نطاق أوسع، تخضع لولايتها القضائية، وهو التزام مصدره العرف الدولى يتطلب منع هذا السلوك.

فاستخدام البنية التحتية للدولة بطريقة تضر بمصالح الدول الأخرى، يبعث على التساؤل حول تقييم فعالية القانون الدولي لقمع السلوك السيبراني الضار العابر للحدود الذي ترتكبه جهات فاعلة من غير الدول، فإن فائدة هذا الالتزام العرفي ذات شقين .

أولاً، على عكس الإسناد، فإن الالتزام بمنع الضرر يغني عن الحاجة إلى تحديد هوية الجهة المؤلفة للسلوك السيبراني (الإسناد التقني) على وجه التحديد لأنه ينطبق عندما ينشأ السلوك الضار عن الانتهاك السيبراني الموجود فى أراضي الدول.[3]

ثانيًا، فى حين أن الإسناد يتطلب من الدولة أن تمارس سيطرة فعالة على الفرد الذي يرتكب السلوك غير القانوني، فإن مخالفة الالتزام بمنع الضرر من حيث الاثبات هى (الأقل عبئًا) حيث يكفي إثبات أن الدولة كانت تعلم أو يجب أن تعلم أن السلوك الضار كان ينبع من أراضيها وفشلت فى اتخاذ كل ما هو معقول من تدابير لإنهاء هذا السلوك أو التخفيف من مدى آثاره الضارة.[4]

مشروعية التدابير المضادة في مواجهة الأنشطة السيبرانية العدائية الصادرة من الدولة

أو الكيانات الخاصة الخاضعة لسيادتها

التزام بذل العناية الواجبة مرن بطبيعته، فيمكن التخفيف من خطورة عواقب معينة بدرجة أكبر أو أقل من خلال الظروف الأساسية، على وجه الخصوص أنشطة الدولة التي تدفع بانتهاك حقوقها ذات الصلة. على سبيل المثال، لنفترض أن دولة ما تقوم بعملية بالغة الضرر ضد كيان خاص فى دولة أخرى، حيث تشكل العملية انتهاكًا لسيادة الدولة.[5] وقد لا تستجيب تلك الدولة بإجراءات مضادة لأنها

[1] علاوة على ذلك، فإن استخدام تقنيات إخفاء الهوية مثل Botnets وبرامج إخفاء الهوية مثل الشبكات الافتراضية الخاصة (VPN) أو The Onion Router (Tor) قد جعل من غير المحتمل تحديد مؤلفي السلوك السيبراني الضار راجع في ذلك:

Tsagourias, Nicholas. "Cyber-attacks, self-defense and the problem of attribution." *Journal of conflict and security law* 17.2 (2012): 229-244. at 229

[2] Milanović, Marko. "State responsibility for genocide." *European Journal of International Law* 17.3 (2006): 553-604.

[3] كما نعلم، تكشف عناوين IP عن الموقع الجغرافي العام للكمبيوتر المستخدم لبدء العملية السيبرانية. إلى حد كبير، ينطبق هذا الالتزام العرفي بغض النظر عما إذا كان السلوك الضار قد نشأ فى تلك المنطقة أو أنه يمر عبرها بدلاً من ذلك، كما هو الحال عندما تقوم جهة فاعلة غير حكومية بإعادة توجيه السلوك السيبراني الضار من خلال البنية التحتية الإلكترونية الموجودة فى أراضي دولة أخرى باستخدام برامج انتحال الروبوتات أو عناوين IP مثل VPN أو Tor. .

[4] Shackelford, Scott J., Scott Russell, and Andreas Kuehn. "Unpacking the international law on cybersecurity due diligence: Lessons from the public and private sectors." *Chi. J. Int'l L.* 17 (2016): 1.

[5] Tsagourias, Nicholas. "Non-state actors, ungoverned spaces and international responsibility for cyber acts." *Journal of Conflict and Security*

الالتزام الدولي ببذل العناية الواجبة في الفضاء السيبراني
بين التدابير الرادعة ومنع الأضرار السيبرانية العابرة

د. أسامة حمزة محمود عبد الفتاح

تفتقر القدرة على القيام بذلك، أو تخشى التصعيد، أو أن الهجوم يتصاعد بسرعة كبيرة للغاية بحيث يتعذر على أجهزتها التصرف بشكل رادع.[1]

وعندما، تبدأ الدولة المتضررة فى اتخاذ ما ترى أنه تدابير مضادة فى شكل مزيد من العمليات الإلكترونية الضارة ضد الدولة المعتدية، أو فى مواجهة العدوان غير المشروع للكيان الخاص التابع لها. فأنه وفقًا لالتزام العناية الواجبة، إذا افترضنا أن هناك دولة يتم الاستعانة ببنيتها التحتية للقيام بهذا التصرف غير المشروع، فتلك الدولة تلتزم ببذل العناية الواجبة لاتخاذ الإجراءات اللازمة لردع عدوان الكيان الخاص.[2]

لا يعتمد تطبيق مبدأ العناية الواجبة على ما إذا كانت البنية التحتية الإلكترونية المستهدفة حكومية أو خاصة بطبيعتها. على سبيل المثال، إذا شنت شركة نفط مقرها إحدى الدول عملية إلكترونية مدمرة ضد منافس خاص مقره فى دولة أخرى، فإن الدولة التي يقع مقر الشركة الضحية لديها تنتهك الالتزام ببذل العناية الواجبة إذا كانت على علم بهذا العدوان، وفشلت باتخاذ تدابير فعّالة لإيقافه، وتصل العواقب إلى حد الخطورة المطلوب.

تطبق تلك القاعدة إذا كانت الدولة على علم بحقيقة أن أراضيها تُستخدم فى عمليات إلكترونية معادية ضد دول أخرى.[3] يُنظر إلى الدولة على أنها تمتلك معرفة فعلية إذا، على سبيل المثال، اكتشفت أجهزة الدولة، مثل وكالات الاستخبارات، عملية إلكترونية نشأت من أراضيها أو إذا تلقت معلومات موثوقة تفيد بأن عملية إلكترونية ضارة انطلقت من أراضيها.

غير أنه، من الصعب للغاية إثبات أن الدولة من الغير كانت تعلم أن أراضيها تستخدم بهذه الطريقة ومع ذلك لم تتخذ الإجراءات اللازمة لوقف هذا السلوك. هذه الصعوبة العملية قد توفر لتلك الدول غير المتعاونة إمكانية الإنكار، ما يجعل الدفع بمخالفة الالتزام ببذل العناية الواجبة موضع نقاش.[4]

بشكل عام، إذا كانت الظروف الواقعية تجعل الدولة فى المسار الطبيعي للأحداث قد أدركت تلك التهديدات، فمن المنطقى أن تكون الدولة على علم. وبناءً على ذلك، فإن الدولة تخرق التزامها ببذل العناية الواجبة إذا كانت فى الواقع غير مدركة للعمليات السيبرانية المعنية، أو أن الدولة كانت تعلم بشكل موضوعي أن أراضيها تُستخدم فى العملية.[5]

قد تؤثر مجموعة من العوامل على تحديد مدى استغلال البنية التحتية للدولة في الهجوم، ومتي كان ينبغي أن تكون على علم بالعمليات السيبرانية المعنية. على سبيل المثال، عندما يتم استغلال البنية التحتية الإلكترونية الحكومية لدولة ما من قبل دولة أخرى أو جهة فاعلة غير

Law 21.3 (2016): 455-474.

[1] فى مواجهة الدولة، يقوم الكيان الخاص بالقرصنة ضد الدولة لإنهاء عملياتها السيبرانية الضارة. نظرًا لأن الجهات الفاعلة من غير الدول لا يحق لها اتخاذ تدابير مضادة، لا يوجد أساس قانوني دولي أساسي لعمليات الكيانات الخاصة غير الدولية.

Corn, Gary, and Eric Jensen. "The use of force and cyber countermeasures." *Temp. Int'l & Comp. LJ* 32 (2018): 127.

[2] وبالتالي، فإن العمليات العدائية للدولة المهاجمة ستشكل فعلًا غير مشروع دوليًا، ما يمنعها من المطالبة بالحق فى اتخاذ تدابير مضادة. وذلك لأن أي عواقب وخيمة تعاني منها هي فى الأساس من صنعها. واتفق الخبراء على أنه لا يجوز للدول أن تستفيد من سلوكها غير القانوني، ولا يجوز لها أن تتخذ إجراءات على حساب الدول الأخرى فى الرد على الأنشطة التي لم تكن لتحدث لولا مثل هذا السلوك.

[3] Brownlie, Ian. "Principles of public international law." *VRÜ Verfassung und Recht in Übersee* 14.1 (1980): 92-93.

[4]

[5] اتفق فريق الخبراء الدولي على أن المعرفة تشمل المعرفة البناءة لأغراض هذه القاعدة.

Corfu Channel judgment, at 44 (separate opinion of Judge Alvarez); Genocide judgment, para. 432. The International Group of Experts acknowledged that in international law generally, the constructive knowledge standard is somewhat controversial.

(ISSN: 2356 - 9492)

حكومية فى عملية ما، فمن المرجح أن يتم الوفاء بمعيار "كان يجب أن يكون على علم" أكثر مما هو عليه فى حالة استخدام البنية التحتية الخاصة.[1]

ومع ذلك، فصعوبة اكتشاف بعض الاستخدامات العدائية للبنية التحتية الإلكترونية الحكومية لدولة ما قد تجعل تأكيد العلم المفترض أمرًا غير معقول. على سبيل المثال، يجوز لطرف ثالث فى الدولة يقوم بعملية إلكترونية ضد دولة مستهدفة استخدام برامج ضارة معقدة وغير معروفة من قبل عند استغلال البنية التحتية الإلكترونية الحكومية للدولة الإقليمية. إذا كان من غير المعقول توقع أن تكون الدولة على علم بالعملية فى الظروف المصاحبة لها وأن تكون قادرة على إنهائها، فلن يتم انتهاك هذه القاعدة.

ومع ذلك، اتفق فريق الخبراء الدولي على أن معيار العلم المفترض لا يقتضي فى حد ذاته، أي التزام باتخاذ تدابير وقائية. على وجه الخصوص، لا ينبغي تفسير هذه القاعدة على أنها تتضمن شرطًا للمراقبة أو اتخاذ خطوات أخرى مصممة لتنبيه السلطات إلى إساءة استخدام البنية التحتية الإلكترونية الموجودة على أراضي الدولة. بدلا من ذلك، يجب على الدول أن تتصرف بمعقولية فى ظروف مماثلة. إذا كانت تلك الظروف الواقعية تجعل الدولة فى وضع مماثل ومجهزة فى المسار الطبيعي للأحداث قد اكتشفت استخدام البنية التحتية الإلكترونية المعنية، فمن المناسب استنتاج أن معيار المعرفة مستوفى.

يجب التمييز بين عدم ممارسة العناية الواجبة وبين المساعدة فى العمليات السيبرانية لدولة أخرى. على سبيل المثال، فإن الدولة التي تجعل بنيتها التحتية السيبرانية متاحة لاستخدام دولة أخرى بهدف تسهيل ارتكاب فعل غير جائز دوليًا من قبل هذه الدولة هي بمثابة المساعدة. وعلى النقيض من ذلك، فإن الدولة التي تفشل فى التصرف عندما تعمل دولة أخرى انطلاقا من إقليمها، تكون مسؤولة عن خرق التزامها ببذل العناية الواجبة.

يجب على المرء أيضًا أن يكون حريصًا على التمييز بين تطبيق مبدأ العناية الواجبة وعدم المشروعية الدولية للعملية الإلكترونية المعينة التي تم إطلاقها من أو استخدام البنية التحتية الإلكترونية على أراضي الدولة. على سبيل المثال، إذا أطلقت الدولة "أ" عملية إلكترونية مدمرة ضد الدولة "ب" باستخدام البنية التحتية الإلكترونية للقيادة والتحكم الموجودة فى الدولة "ج"، فقد تنتهك الدولة "ج" هذه القاعدة، فى حين أن الدولة "أ" قد تكون قد انتهكت سيادة الدولة "ب".

إذا كانت العملية الإلكترونية للأطراف من الغير منسوبة إلى الدولة التي ينطلق الهجوم من اقليمها بموجب قانون مسؤولية الدولة، فلن يتم تضمين هذه القاعدة. على سبيل المثال، إذا كان المتسللون فى إحدى الدول يعملون تحت السيطرة الفعلية لتلك الدولة (القاعدة 17) ويوجهون عملياتهم الإلكترونية المدمرة ضد دولة أخرى، فإن عمليات المتسللين الإلكترونية تُنسب إلى الدولة التي انطلقت منها. على الرغم من أن تلك الدولة ستكون قد ارتكبت عملاً غير مشروع دوليًا ، يتمثل فى (على الأقل) انتهاك سيادة الدولة المستهدفة، إلا أنه لا ينتهك التزامها ببذل العناية الواجبة.

فى الحالات التي تنطوي على نزاع مسلح دولي، لا يخل تطبيق هذه القاعدة بالتزام الدول المحايدة تجاه أنشطة الأطراف المتحاربة فى إقليم محايد أو التي تنطوي على استغلال البنية التحتية الموجودة في الاقليم.

المطلب الثاني

مسؤولية الكيانات الفاعلة غير الدولية عن الهجمات السيبرانية

بشكل عام، تنتهك الدول، وليس الأفراد أو الكيانات الخاصة، القانون الدولي.[1] حيث إن العمليات الإلكترونية التي تجريها الدول أو تُنسب إليها هي فقط التي تنتهك مبدأ احترام سيادة الدولة أو حظر استخدام القوة.

[1] وبالمثل، فإن إسناد المعرفة البناءة يكون أكثر ملاءمة عند استخدام البرامج الضارة ونقاط الضعف المعروفة للجمهور، مثل ثغرة Heartbleed التي تم اكتشافها فى عام 2014، وعند تضمين العمليات الإلكترونية التي يتم اكتشافها دائمًا بشكل عام، مثل هجمات DDoS التي تزيد بشكل كبير من استخدام النطاق الترددي مقارنة إلى الاستخدام العادي.

ومع ذلك، ثمة اتفاق على أن مبدأ العناية الواجبة يمتد ليشمل العمليات الإلكترونية التي تجريها جهات فاعلة من غير الدول[2] والتي، على الرغم من عدم انتهاك القانون الدولي فى حد ذاته، فإنها تؤدي مع ذلك إلى عواقب وخيمة تؤثر على حقوق الدولة المستهدفة.

لا تشمل هذه القاعدة جميع العمليات السيبرانية الضارة غير الحكومية من أراضي دولة ما، والمقصود هو تلك العمليات التي ينتج عنها "عواقب وخيمة" فى دولة أخرى.[3] كما هو الحال مع العمليات السيبرانية للدول، ومن ثم يتولد التزام العناية الواجبة عندما تنخرط جهة فاعلة من غير الدول فى سلوك يؤثر على حق الدولة المستهدفة.[4]

ولاحظ الخبراء أنه فى مختلف مجالات القانون الدولي، تبلورت التزامات بذل العناية الواجبة بشكل واضح فى ضوء الخطر المتزايد الذي تشكله الجهات الفاعلة من غير الدول.[5] فلم يحدد فريق الخبراء الدولي أي أساس منطقي مقنع لاستبعاد العمليات السيبرانية للجهات الفاعلة من غير الدول التي تترتب عليها عواقب وخيمة خارج الحدود الإقليمية من نطاق التزام الدولة ببذل العناية الواجبة.

على سبيل المثال، إذا شنت جهات فاعلة من غير الدول عمليات إلكترونية ضد دولة من شأنها، إذا قامت بها دولة، أن تشكل تدخلاً محظورًا، فإن الدولة التي تقع البنية التحتية المستخدمة ضمن نطاق سيادتها تتحمل التزام العناية الواجبة تجاه تلك العمليات.[6]

إن الاعتقاد بخلاف ذلك من شأنه أن يخلق حالة متناقضة تكون فيها الدولة قد انتهكت التزامها ببذل العناية الواجبة عندما تنخرط جهات فاعلة من غير الدول فى عمليات إلكترونية معينة انطلاقا من أراضيها، ولكن ليس إذا كانت قد شاركت فى ذات السلوك بنفسها.

المطلب الثالث

نظرية الحد الأدنى للضرر في الفضاء السيبراني

الحد الأدنى للضرر الذي يرتبط بتطبيق مبدأ العناية الواجبة غير مستقر فى القانون الدولي[7]. غير أنه ثمة توافق على أن شرط العناية الواجبة ينشأ عندما ينطوي الموقف على عملية إلكترونية تؤدي إلى `` عواقب سلبية خطيرة ''، على الرغم من عدم وضع حد معين للضرر، فالاعتماد على هذا المعيار جاء بطريق القياس على تطبيق مبدأ العناية الواجبة فى سياق القانون الدولي للبيئة.[1]

---

[1] Paust, Jordan J. "Nonstate Actor Participation in International Law and the Pretense of Exclusion." *Va. J. Int'l L.* 51 (2010): 977.

[2] Buchan, Russell. "Cyberspace, non-state actors and the obligation to prevent transboundary harm." *Journal of Conflict and Security Law* 21.3 (2016): 429-453.

[3] Shackelford, Scott J., Scott Russell, and Andreas Kuehn. "Unpacking the international law on cybersecurity due diligence: Lessons from the public and private sectors." *Chi. J. Int'l L.* 17 (2016): 1.

[4] Tsagourias, Nicholas. "The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II—The Use of Force." *Yearbook of International Humanitarian Law* 15 (2012): 19-43.

[5] Sigholm, Johan. "Non-state actors in cyberspace operations." *Journal of Military Studies* 4.1 (2013): 1-37.

DeLuca, Christopher D. "The need for international laws of war to include cyber-attacks involving state and non-state actors." *Pace Int'l L. Rev. Online Companion* (2013): ii.

[6] Schmitt, Michael N., ed. *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press, 2017.

ضع فى اعتبارك حالة تقوم فيها شركة خاصة تمتلك وثائق سرية خاصة بإحدى الدول بنشرها عبر الإنترنت فى دولة أخرى. على الرغم من أن نشرها يتسبب فى عواقب وخيمة على الدولة التي تم الإفراج عن وثائقها، فإن الدولة التي تم نشرها فيها ليست ملزمة بضمان إزالة الوثائق من الإنترنت لأنه لا يؤثر على أي حق من حقوق الدولة المستهدفة القانون الدولي.

[7] In the context of international environmental law, international case law provides that -r.der the principles of international law .. . no State

(ISSN: 2356 - 9492)

فعندما تمارس دولة سلطتها فى إقليم دولة أخرى دون موافقتها[2] ، ما يحول دون ممارسة تلك الأخيرة سيادتها الحصرية بشكل مستقل، فإن ذلك يشكل انتهاكًا للسيادة. يظهر هذا المبدأ جلياً فى الفقه الدولي، حيث قالت المحكمة الدائمة للعدالة الدولية (PCIJ) فى قضية لوتس إن `` القيد الأول والأهم الذي يفرضه القانون الدولي على دولة ما هو أنه - فى حالة عدم وجود قاعدة تسمح بعكس ذلك - لا يجوز لها ممارسة سلطتها فى أراضي دولة أخرى "[3]

وفى بعض الأنشطة التي قامت بها نيكاراغوا فى المنطقة الحدودية (كوستاريكا ضد نيكاراغوا)، اعتبرت محكمة العدل الدولية أن انتهاك السلامة الإقليمية والسيادة ينطوي على ممارسة السلطة فى إقليم دولة أخرى.[4] ورأت المحكمة أن نيكاراغوا انتهكت السيادة الإقليمية لكوستاريكا من خلال القيام بأنشطة معينة على أراضيها دون موافقة.[5]

فى الأنشطة العسكرية وشبه العسكرية فى نيكاراغوا وضدها، أشارت محكمة العدل الدولية إلى "واجب كل دولة فى احترام السيادة الإقليمية للآخرين". عمليات إزالة الألغام فى المياه الإقليمية لألبانيا دون موافقة.[6] فى كل حالة من هذه القضايا، نظرت المحكمة فى انتهاك السيادة بشكل منفصل عن قواعد استخدام القوة والتدخل، واعتبرت أن لها عواقب قانونية.

هناك العديد من الأمثلة على انتهاك سيادة الدولة، لعل أبرزها عمليات اقتحام الفضاء المادي مثل المجال الجوي أو المياه الإقليمية أو ممارسة سلطات سياسية مثل إنفاذ القانون. لكن هل يمكن للدولة أن تنتهك أيضًا سيادة دولة أخرى من خلال النشاط الذي تمارسه الدولة انطلاقا من خارج أراضي الدولة الضحية وبدون آثار مادية فى النطاق المتضرر؟

قد يكون التحدي الأصعب من الناحية العملية هو إثبات انتهاكات السيادة التي تتم من خارج الإقليم مع آثار فى الإقليم، حيث سيكون النشاط غير ملموس مقارنة بالنشاط المادي وقد يكون من الصعب إثبات ذلك. بغض النظر عن هذه الاختلافات المحتملة فى التطبيق والإثبات، تنطبق نفس القواعد المتعلقة بانتهاك السيادة سواء كانت الدولة المعتدية تتصرف من خلال التواجد المادي على أراضي الدولة المتضررة أو عن بُعد من خارج المنطقة المتأثرة. من الناحية

---

has the right to use or permit these of its territory in such a manner as to cause injury by fumes in or to the territory of i_-other or the properties or persons therein, when the case is of serious consequence ...trail Smelter arbitral award, at 1965. In that field of law, the damage sustained by the directed State must meet a certain threshold, that, in addition to 'serious', has also been characterized as 'significant' or 'substantial'. Articles on Transboundary Harm, Art. 2, M--2S. 4, 6 of commentary.

[1] اتفق فريق الخبراء الدولي على أن مجرد التأثير على مصالح الدولة المستهدفة، كما في حالة التسبب في إزعاج أو اضطراب طفيف أو تكاليف لا تذكر، ليس من نوع الضرر المتوخى؛ وبالتالي، فليس كل استخدام لإقليم دولة ينتج عنه آثار سلبية لدولة مستهدفة ينطوي على مبدأ العناية الواجبة.

Schmitt, Michael N., ed. *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press, 2013. pp39-45

[2] يُقصد بعبارة "الدولة" هنا أن تشمل وكلاء الدولة أو أجهزة الدولة أو الجهات الفاعلة والوكلاء من غير الدول إذا كان من الممكن عزو أفعالهم إلى الدولة بموجب قواعد الإسناد المنصوص عليها في مواد لجنة القانون الدولي بشأن مسؤولية الدولة. والسيادة هنا بمعنى السلطة العليا للدولة وهي قادرة على تغطية جميع العناصر التي تمت مناقشتها أعلاه. ويشير أوبنهايم إلى انتهاك "استقلال دولة أخرى أو سلطتها الإقليمية أو الشخصية.

Oppenheim (1996), Oppenheim's International Law, Vol. 1: Peace, p. 385.

[3] راجع:

S. S. Lotus (France v Turkey), Judgment, 7 September 1927, PCIJ (series A) No. 1, p. 18, emphasis added.

[4] بعض الأنشطة التي نفذتها نيكاراغوا في المنطقة الحدودية (كوستاريكا ضد نيكاراغوا) ، الحكم ، تقارير محكمة العدل الدولية 2015 ، الفقرات 221-3: "لا يوجد دليل على أن كوستاريكا مارست أي سلطة على أراضي نيكاراغوا أو نفذت أي نشاط فيها ... لذلك ، يجب رفض ادعاء نيكاراغوا بشأن انتهاك سلامتها الإقليمية وسيادتها '.

[5] وجدت محكمة العدل الدولية أن نيكاراغوا نفذت أنشطة مختلفة في المنطقة المتنازع عليها منذ عام 2010، بما في ذلك إنشاء وجود عسكري في أجزاء من تلك المنطقة. وتشكل هذه الأنشطة خرقا لسيادة كوستاريكا الإقليمية.

[6] كثيرا ما تبرم الدول اتفاقيات للسماح بالنشاط داخل أراضي بعضها البعض (مثل اتفاقيات وضع القوات، التي تسمح عادة بالوجود، والمناورات، والتدريب، والنشاط التجاري، إلخ). بدون ذلك، يمكن انتهاك سيادة الدولة الإقليمية من خلال النشاط المعني

Corfu Channel (UK v Albania) Judgment (Merits) 1949 ICJ Rep 4, 9 April 2015 Judgment, paras 69–70.

قدمت الولايات المتحدة دعوى بانتهاك سيادتها من خلال الضرر الناجم عن نشاط منشأة كندية تقع على الأراضي الكندية. لم تشر المحكمة صراحةً إلى السيادة في حكمها، ولكنها لاحظت أنه "بموجب مبادئ القانون الدولي ... لا يحق لدولة استخدام أراضيها أو السماح باستخدامها بطريقة تؤدي إلى إحداث ضرر بواسطة الأبخرة في أو أراضي شخص آخر أو ممتلكات الأشخاص الموجودين فيه، عندما تكون القضية ذات عواقب وخيمة ويكون الضرر مثبتًا بدليل واضح ومقنع '. راجع:

In the Trail Smelter arbitration (Trail Smelter Arbitration (United States v. Canada), Arbitral Trib., 3 U.N. Rep. Int'l Arb. Awards 1905 (1941)),

العمليـة، تميـل الانتهاكـات البعيـدة التـي تنطـوي علـى عنصـر قسـري إلـى النظـر فيهـا مـن منظـور مبـدأ عـدم التـدخل أو مـن خـلال قواعد محددة من القانون الدولي تم تطويرها.[1]

فكرة الضرر المادي المباشر والضرر العابر

يعتبر جانب من الفقه السيادة هي مبدأ "شامل" يرفض أي تدخل فى السلطة الداخلية والخارجية الحصرية للدولة مثل عدم التدخل أو عدم استخدام القوة.[2] ويؤكد أولئك الذين يتخذون هذا الموقف أن التوغل القسري من قبل وكيل الدولة فى أراضي دولة أخرى يمكن أن يرقى إلى مستوى ممارسة سلطة الدولة نفسها، ما يشكل انتهاك لسيادة الدولة الضحية. بغض النظر عما إذا كان هذا التوغل ينتج عنه ضرر أو ينتهك بشكل آخر القوانين الوطنية والدولية، وبغض النظر عما إذا كانت ممارسة السلطة تتجلى من خلال الوجود المادي على الإقليم أو عن بعد.[3]

بينما يؤيد جانب أخر، أنه ليست كل ممارسات السلطة التي تتم بدون موافقة والتي لم يتم تضمينها فى قواعد محددة ترقى إلى مستوى انتهاك السيادة. [4] فمن المجالات التي لا يكون فيها التساؤل حول ما هو غير قانوني واضحًا، ما يتعلق بأعمال وكالات استخبارات الدول، والتي تعمل بشكل روتيني على أراضي دول أخرى دون الكشف عنها رسميًا للسلطات. حيث يدفع بعض الفقه بأن أشكال التجسس المتطفلة داخل إقليم الدولة تنتهك مبدأ السيادة الإقليمية.[5]

بينما يتمثل أحد أوجه المعارضة الرئيسية لهذه الحجة فى انتشار عملاء استخبارات الدول فى كل مكان فى الدول الأخرى، وعادةً ما يكون ذلك بدون تعليق من تلك الدول. بينما تحظر الدول بشكل روتيني أشكال التجسس بموجب قانونها الوطنى، وبينما قد تؤدي أنشطة معينة إلى إثارة الاحتجاج، إلا أن الدول أو المعلقين فى أغلب الأحيان لم تعامل أنشطة وكالات الاستخبارات على أنها غير قانونية دوليًا فى حد ذاتها.[6]

---

[1] راجع:

Higgins, R. (2009), 'Intervention and International Law', in Themes and Theories: Selected Essays, Speeches and Writings in International Law, Vol. 1 (2009), OUP, pp. 275–5, discussing specific rules relevant to economic intervention. The non-intervention principle is considered in Chapter 3.

[2] راجع:

Tsagourias (2018), 'Law, Borders and the Territorialization of Cyberspace', p. 19. See also Watts, S. and Richard, T. (2018), 'Baseline Territorial Sovereignty and Cyberspace', Lewis & Clark Law Review, 22(3): pp. 803–872.

[3] راجع

Buchan (2018), Cyber Espionage and International Law, p. 51 ff.; Watts and Richard (2018), 'Baseline Territorial Sovereignty and Cyberspace', pp. 866–867

[4] Buchan (2018), Cyber Espionage and International Law, p. 51 ff.; Watts and Richard (2018), 'Baseline Territorial Sovereignty and Cyberspace', pp. 866–867.

[5] يجادل بوكان بأن مجموعة متزايدة من قرارات المحاكم الوطنية تدعم هذا ، ولا سيما قانون خدمة المخابرات الأمنية الكندي ، الذي رفضت بموجبه المحكمة الفيدرالية الكندية منح أمر قضائي إلى دائرة المخابرات الأمنية الكندية للقيام بأنشطة تجسس في الخارج على أساس أن هذه الأنشطة من شأنها مخالفة القانون الدولي. في رفض إصدار الأمر ، لاحظت المحكمة الفيدرالية أن الأنشطة التدخلية المتوخاة "تمس بشكل واضح ... مبادئ المساواة في السيادة الإقليمية وعدم التدخل"

(Re Canadian Security Intelligence Service Act [2008] FC 301 paras 50–52), cited in Cyber Espionage and International Law, p. 52. Buchan also cites some cases from other national courts (at footnote 27) and statements by certain states objecting to the activities of the US's National Security Agency leaked by Snowden as a violation of their sovereignty (pp. 54–55).

[6] Oppenheim (OUP 2008) Vol I, at p. 403 (para 122). Oppenheim states that 'intervention must neither be confounded with good offices, nor with mediation, nor with intercession, nor with co-operation, because none of these imply a dictatorial interference' [p. 222]; Jamnejad and Wood discuss rules relevant to allegedly intervention ARY activities of diplomats: Jamnejad, M. and Wood, M. (2009), 'The Principle of Non-intervention', Leiden Journal of International Law, 22(2): p. 364

(ISSN: 2356 - 9492)

تنص القاعدة 4 من دليل تالين 2.0 على أنه "يجب على الدولة ألا تجري عمليات إلكترونية تنتهك سيادة دولة أخرى". وهذا يدعو إلى التساؤل حول متى تكون العملية السيبرانية برعاية الدولة تنتهك سيادة دولة أجنبية. - يتمثل أحد السيناريوهات فى أن النشاط السيبراني غير المصرح به يقوم به وكيل دولة ما أثناء وجوده فعليًا على أراضي دولة أخرى.[1]

فى كثير من الأحيان، يتم إجراء عمليات التطفل السيبراني الحكومية عن بُعد من خارج إقليم الدولة المستهدفة بدلاً من الوكلاء الموجودين فعليًا داخل أراضي الدولة المتضررة.[2] يمكن اعتبار الوكيل الذي يخترق شبكة الطاقة الوطنية للدولة ويغلقها من خارج إقليم الدولة الضحية أنه "يصل" (بدون موافقة) إلى الإقليم الخاضع لسيادة الدولة الضحية، إذا كان الخادم المتأثر موجودًا فى أراضي الدولة الضحية.

فى بعض الأحيان، سيكون للتطفل السيبراني الناجم عن بُعد آثار مادية على المنطقة، على سبيل المثال الضرر المادي للبنية التحتية الالكترونية. وبالمثل، فى السياق غير الإلكتروني، يمكن أن يكون للضرر البيئي العابر للحدود الناجم عن بُعد آثار مادية فى إقليم الدولة المتضررة.

أيضاً في أحيان أخرى لن يكون هناك أثر مادي على الإطلاق فى الإقليم، على سبيل المثال، دولة تستهدف خوادم دولة أخرى، وتجمع المعلومات؛ أو استخدام البرامج الضارة لتعديل البيانات الموجودة دون ترك أي أثر. ومع ذلك، فإن التسلل الإلكتروني[3] يصل إلى البنية التحتية على أراضي الدولة الضحية دون موافقة الدولة الضحية. طالما أن الخوادم المتأثرة موجودة فى إقليم الدولة الضحية (أو فى حالة الأقمار الصناعية، ضمن اختصاص الدولة المتأثرة)، فإن ممارسة السلطة غير المصرح بها من قبل دولة ما عن طريق الوسائل الإلكترونية فى إقليم دولة أخرى يمكن أن يشكل انتهاكًا لسيادة الدولة الضحية[4].

ويمكننا القول، أنه فى كثير من الأحيان، يتم إجراء الهجوم الإلكتروني عن بُعد من خارج إقليم الدولة المستهدفة بدلاً من القيام به عبر الوكلاء الموجودين فعليًا داخل أراضي الدولة المتأثرة. يبدو أن المنطق يقتضي من حيث المبدأ عدم التمييز بين الانتهاكات المادية المباشرة (أي النشاط الذي يقوم به وكيل الدولة مباشرة أراضي الدولة الضحية) والانتهاكات البعيدة (أي النشاط المنفذ من خارج أراضي الدولة المتضررة)[5]. فى الواقع، سيكون من الغريب القول إنه إذا قام وكيل الدولة بإغلاق شبكة كهرباء دولة أخرى أثناء تواجده على

[1] ومن الأمثلة الحديثة على ذلك محاولة اختراق منظمة منع الأسلحة الكيميائية (OPCW)، القائمة فى لاهاي بهولندا. من قبل وكالة المخابرات العسكرية الروسية، GRU. فى أبريل 2018، انتقل ضباط المخابرات الروسية إلى موقع قريب من مقر منظمة حظر الأسلحة الكيميائية وكانوا يجرون الاستعدادات لاختراق شبكات منظمة حظر الأسلحة الكيميائية. من أجل حماية نزاهة منظمة حظر الأسلحة الكيميائية، استبق جهاز استخبارات الدفاع والأمن الهولندي عملية GRU الإلكترونية ورافق ضباط المخابرات الروس خارج هولندا فى نفس اليوم. فى هذه الحالة، قد يبدو أن مبدأ عدم التدخل غير قابل للتطبيق، لأن النشاط لا يفي بمتطلبات الإكراه. من القانون ، يشير إلى أن الحكومة اعتبرت أن نشاط GRU غير مشروع دوليًا، دون تحديد بأي طريقة.

The Tallinn Manual 2.0 gives the example of one state using a USB flash drive to introduce malware into cyber infrastructure located in another state: para 6 of commentary to Rule 4, Schmitt (2017), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.

راجع أيضا:

Global Affairs Canada (Canada's Foreign Ministry) citing inter alia the GRU attack on the OPCW, which stated that such activities 'underscore the Russian government's disregard for the rules-based international order, international law and established norms': Government of Canada (2018), 'Canada identifies malicious cyber-activity by Russia', Canada Global Affairs, https://www.canada.ca/en/global-affairs/ news/2018/10/canada-identifies-malicious-cyber-activity-by-russia.html (accessed 5 Oct. 2021).

[2] As a reflection of this, the EU's restrictive measures against cyberattacks threatening the EU or its member states only focus on cyberattacks that originate from outside the EU

[3] حيث تبدأ العمليات السيبرانية بالدخول غير المصرح به للشبكة الالكترونية، بحثاً عن البيانات السرية المحمية والمخزنة ، حيث يدلف المتسلل لشبكة المعلومات الخاصة بالدولة الضحية كأول خطوات الهجوم السيبراني.

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

[4] Watts and Richards,'If one accepts that sovereignty is an aspect of the existing international law that States have conceded applies to cyberspace and if one accepts that sovereignty, at a minimum, protects states from interference with the independent and exclusive control of their territory by other States, the conclusion that interferences with cyber infrastructure violate sovereignty is not an especially difficult one to reach', Watts and Richards (2018), 'Baseline Territorial Sovereignty and Cyberspace', p. 866.

[5] International courts and commentators in the non-cyber context have treated the elements of sovereignty as inter-linked, para 37

أراضي الدولة الأخيرة، فهذا انتهاك للسيادة، ولكن هذا لن يشكل انتهاك إذا كانت الدولة الجانية قد فعلت ذلك من خلال الهجوم السيبراني عن بُعد.

الخلاف الفقهي حول الحد الأدنى للسيادة في الفضاء السيبراني

كما هو الحال فى السياق غير السيبراني، لا يزال هناك سؤال حول ما إذا كانت أي ممارسة غير مصرح بها داخل إقليم الدولة المتأثرة تشكل انتهاكًا للسيادة أو ما إذا كان هناك شكل من أشكال الحد الأدنى للأفعال المنشئة للمسؤولية الدولية؟

هناك خلاف حول فكرة الحد الأدنى لانتهاك السيادة، ومدى وضوحها فى سياق ممارسة السلطة عن بُعد من قبل دولة ما فيما يتعلق بسيادة أراضي دولة أخرى. فأجهزة التحكم عن بعد عادة ما تؤثر على ممارسة السلطة من قبل دولة ما على الاستقلال السياسي للدولة الضحية - كما هو فى حالة التدخل السياسي أو الاقتصادي فى شؤون دولة أخرى، أو ممارسة الاختصاص خارج الحدود الإقليمية. يلاحظ أوبنهايم أن الاستقلال له حد أدنى، وما إذا كان يتم انتهاك هذا الجانب من السيادة أم لا، فسيكون ذلك تبعاً لتخطى هذا الحد الأدنى. على سبيل المثال، الاحتجاجات الدبلوماسية أو مجرد انتقاد لحكومة أجنبية. غير أنه ليس من الواضح ما إذا كان هناك شكل من أشكال قواعد الحد الأدنى فى الممارسات الدولية.[1]

يمكننا القول، إن حدود قاعدة السيادة ليست واضحة. فليس هناك ثمة توافق حول مضمون قواعد الحد الأدنى، وهو ما تكشف عنه الطريقة التي تعامل بها الدول أنشطة الدول الأخرى فى الممارسة. وبالتالي، فإن تقييم ما إذا كانت السيادة قد انتهكت يجب أن يتم على أساس كل حالة على حدة، إذا لم يتم تطبيق قواعد أخرى أكثر تحديدًا فى القانون الدولي.

ويجادل بعض الفقهاء، بأنه وإن كانت لا توجد قاعدة فى السياق السيبراني محددة للسيادة لها عواقب قانونية. فمن وجهة نظرهم، إن الاختلافات فى كيفية انعكاس السيادة فى القانون الدولي يرتبط بمجال التطبيق. ويدعم هذا الرأي أن السيادة هي مبدأ يخضع للتعديل حسب المجال والضرورات العملية للدول ومن ثم فهي تتسم بالمرونة وليس الجمود.[2]

ولكن يتضح من السوابق القضائية أعلاه أنه من الممكن انتهاك سيادة الدولة دون الرجوع فقط إلى قواعد القانون الدولي التي تنظم المجالات التقليدية للنزاعات الدولية، وأن هذا الانتهاك يرقى إلى ارتكاب فعل غير مشروع دوليًا له عواقب قانونية.

نذكر من ذلك على سبيل المثال التوجه الخاص بالأستاذ *Specter*، حيث يشير إلى أنه " سواء اختار المرء أن يطلق عليها سيادة، أو سيادة إقليمية، أو وحدة أراضي، أو أي شيء آخر تمامًا، فإن مجموعة ساحقة وحتمية من المعاهدات والاجتهاد القضائي والرأي

[1] فمن الصعب رسم الخط الفاصل بين الدبلوماسية القانونية وانتهاك السيادة وسيكون تحقيقًا محددًا يتناول كل قضية على حده مسألة جوهرية. كما لم يتم وضع حدود للسيادة. ، كما يتضح من الطريقة التي تعامل بها الدول أنشطة الدول الأخرى فى الممارسة.

Jamnejad, Maziar, and Michael Wood. "The principle of non-intervention." *Leiden Journal of International Law* 22.2 (2009): 345-381.; ibid., pp. 368–369.

[2] على سبيل المثال، يجادل كورن وتايلور بأن "القانون وممارسات الدولة ... تشير إلى أن السيادة تعمل كمبدأ من مبادئ القانون الدولي الذي يوجه تفاعلات الدول ، ولكنها ليست في حد ذاتها قاعدة ملزمة تملي النتائج بموجب القانون الدولي"

Corn, G. P. and Taylor, R. (2017), 'Sovereignty in the Age of Cyber', AJIL Unbound, 111: p. 210.

(ISSN: 2356 - 9492)

الأكاديمي تؤيد الافتراض القائل بوجود قاعدة أساسية فى القانون الدولي، مفادها " ضرورة امتناع دولة ما عن القيام بعمل عام أو ممارسة سلطة فى أراضي دولة أخرى، فى حالة عدم وجود موافقة أو أي حكم آخر من أحكام القانون الدولي على خلاف ذلك".[1]

المفهوم الشامل للسيادة في الفضاء السيبراني

إذا تبنى المرء موقف معيار السيادة الشامل، فإن ذلك يجعل احتمالية الانتهاكات كبيرة جدًا بالفعل. وفقًا لوجهة النظر هذه على سبيل المثال، سيكون من الناحية الفنية انتهاكًا للسيادة وبالتالي عملًا غير مشروع دوليًا أن تقوم الدولة بتثبيت آلية وصول على البنية التحتية لدولة أخرى، وإن لم يتم التدخل فى وظائف البنية التحتية الإلكترونية للدولة المستهدفة؛ أو لجمع المعلومات لأغراض التجسس؛ أو للقيام بنشاط سيبراني استكشافي من قبل الدول التي تتطلع إلى تحديد نقاط الضعف داخل النظام والتي قد تكون مفيدة لهجوم مستقبلي. يبدو أن هذا النهج الوقائي الذي لا يفرض نطاق أقصي لانتهاك السيادة فى السياق السيبراني يتعارض مع واقع التفاعلات اليومية للدول فى الفضاء الإلكتروني.

فهذا الرأي يتناقض مع الممارسات الدولية ضمن هذا السياق، فعلى سبيل المثال "قد يؤدي تصميم الإنترنت ذاته إلى بعض التعدي على السلطات القضائية السيادية الأخرى"[2] فطبيعة عالم الإنترنت المترابط تكمن فى أن الدول تمر باستمرار عبر بوابات بعضها البعض، غالبًا بدون إذن صريح، لا سيما وكالات الاستخبارات التابعة للدول. قد "يصل" النشاط السيبراني للدولة إلى أراضي الدول الأخرى بطرق متنوعة بما فى ذلك لأغراض "حميدة" مثل مكافحة الإرهاب، دون علم الدول الأخرى، على الأقل فى الوقت الفعلي. فى ظل النهج الشامل للسيادة، ستكون سيادة الدول من الناحية الفنية فى حالة انتهاك مستمرة.

قد يدفع مؤيدي نهج السيادة الشامل بأنه من الناحية العملية، تتمتع الدول بسلطة تقديرية بشأن ما إذا كانت ترغب فى تأطير مثل هذا النشاط بلغة انتهاك السيادة، أو التعامل معها بطرق أخرى، على سبيل المثال دبلوماسياً أو من خلال القانون الجنائي الوطني. ولكن إذا كانت مثل هذه الأنشطة يمكن أن تشكل بالفعل انتهاكات للسيادة، فقد يؤدي ذلك إلى زيادة خطر المواجهة والتصعيد، لأن انتهاك السيادة يمنح الدولة المتضررة الحق فى اتخاذ إجراءات مضادة للرد إذا فشلت الأطراف الأخرى فى معالجة الوضع.

ومن المتوقع أيضًا أن الدول التي تدعي مفهومًا واسعًا للسيادة، بما فى ذلك الدول القوية النشطة عبر الإنترنت مثل روسيا والصين، سوف تتذرع بانتهاكات السيادة ضد الأنشطة الدولية للدول الأخرى من أي نوع بشكل متكرر أكثر من غيرها.

هذه إحدى مشكلات الاعتماد على مفهوم شامل للسيادة فى هذا السياق. ما يوجب تطبيق القانون الدولي بشكل موضوعي، بدلاً من السيادة فعدم وجود أي معايير محددة للانتهاكات يزيد من خطر قيام الدول بتفسير السيادة بشكل ذاتي.

عندما تدلي الدول ببيانات تتعلق بالتدخلات السيبرانية للدولة، فإنها لم تؤطر عادة هذه التدخلات على أنها انتهاكات للسيادة. ليس من الواضح ما إذا كان هذا بسبب أن الدول المعنية لا تريد رفع الوضع إلى هذا المستوى (مع الإشارة ضمنيًا إلى أن الدولة الضحية يحق لها بعد ذلك اتخاذ إجراءات مضادة) أو لأنها لا تنظر إلى النشاط على أنه انتهاك للسيادة فى المقام الأول. إن الفكرة القائلة بأن جميع الممارسات غير المصرح بها لسلطة الدولة بالوسائل الإلكترونية تشكل انتهاكات للسيادة لا يمكن التوفيق بينها بسهولة مع المتعارف عليه في الممارسات الدولية.

كما أنه لا يبدو أنه يتوافق مع ممارسات الدولة الحالية. أحكام المحاكم الدولية على أساس مبدأ السيادة، والتي تبدو من حيث المبدأ قادرة على التطبيق على جميع الممارسات غير المصرح بها لسلطة الدولة، السيبرانية أو غير ذلك. يتفق فريق الخبراء الدولي على أنه لا يوجد شرط بأن تؤدي العملية الإلكترونية المعنية إلى أضرار مادية للأشياء أو إصابات للأفراد. فى سياق مبدأ العناية الواجبة، يمكن أن تشمل العواقب السلبية الخطيرة، على سبيل المثال، التدخل فى تشغيل البنية التحتية الحيوية أو التأثير الكبير على الاقتصاد.[3]

[1] Spector, P. (2017), 'In Defense of Sovereignty, in the Wake of Tallinn 2.0', AJIL Unbound, 111: pp. 219–223; Ginsburg, T. (2017), 'Introduction to Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0', AJIL Unbound, 111: p. 222. For a detailed discussion of the evidence in support of violation of sovereignty having legal consequences see Schmitt and Vihul (2017), 'Respect for Sovereignty in Cyberspace', p. 1649 ff.

[2] Egan (2017), 'International law and stability in cyberspace', p. 13

[3] Schmitt, Michael N. "Peacetime cyber responses and wartime cyber operations under international law: An analytical vade

الالتزام الدولي ببذل العناية الواجبة في الفضاء السيبراني
بين التدابير الرادعة ومنع الأضرار السيبرانية العابرة

د. أسامة حمزة محمود عبد الفتاح

لعل أخطر العمليات السيبرانية، تلك التي تستهدف دولة ما والتي يتم تنفيذها بشكل أساسي من قبل متسللين متمركزين فى دولة أخرى والتي تسبب اضطرابًا شديدًا فى الخدمات المصرفية عبر الإنترنت، ووسائل الإعلام، والوظائف الحكومية، وقطاع الأعمال.[1] وفى تلك الحالات يكون الضرر المتكبّد خطير بما يكفي لتطبيق مبدأ العناية الواجبة على الرغم من عدم حدوث أضرار جسدية أو إصابات.

المسؤولية التضامنية للأطراف من الغير عن الضرر السيبراني[2]

هناك انقسام حول هذه المسألة بين الفريق العامل علي دليل تالين للفضاء السيبراني، حيث ذهب جانب منهم إلى ضرورة الأخذ بالنهج المتبع فيما يتعلق بالحوادث الإلكترونية لأغراض الدفاع عن النفس[3] . فى هذا السياق، خلصت أقلية من الخبراء إلى أنه يمكن التعامل مع العمليات على أنها هجوم مسلح مركب إذا تم إجراؤها من قبل نفس المنشئ أو من قبل المنشئين الذين يعملون بالتنسيق، اقترحت أقلية من الخبراء أنه يمكن حصر جميع الأضرار الناجمة عن تلك العمليات من الدول التي تتشتت فيها حتى مع تباين البني التحتية. بحيث يتم الوصول إلى الحد الأدنى من الضرر، والذي بموجبه تتحمل كل دولة معنية التزام العناية الواجبة[4]. يركز هذا النهج على منظور الدولة المستهدفة؛ فيتعامل مع مبدأ العناية الواجبة على أنه مصمم لحماية حقوق الدول الأخرى. لاحظ أنه من خلال هذا النهج، سيتم تقييم دور كل دولة على حدة فيما يتعلق بما إذا كانت قد مارست الدرجة المطلوبة من العناية الواجبة لإنهاء مشاركة البني التحتية الخاضعة لسيادتها في الهجوم السيبراني.

ومع ذلك، أشارت غالبية أعضاء فريق الخبراء الدولي إلى أن فكرة (حصر جميع الأضرار) غير مناسبة. بالنسبة لهم، فإن مبدأ العناية الواجبة مستمد من الامتيازات السيادية للدولة على إقليمها.[5] وذلك من شأنه أن يؤدي إلى عدم تحقيق توازن بين الحق فى السيطرة على الأراضي وواجب ضمان عدم استخدامه لإلحاق الضرر بالدول الأخرى لفرض التزام العناية الواجبة فى مثل هذه الحالات.[6]

سيكون من غير المناسب التأكيد على مسؤولية الدولة عن بذل العناية الواجبة، ومراعاة حقوق الدولة المستهدفة فى الحالات التي يكون فيها ارتباطها بالضرر طفيفًا. علاوة على ذلك، اقترحوا أن تفسير مبدأ العناية الواجبة على طريقة الأقلية سيعني أنه يمكن أن تتحمل الدول المسؤولية عن فعل غير قانوني دوليًا يستند أساسًا إلى التصرفات غير المشروعة للدول الأخرى.

اتخذ فريق الخبراء الدولي موقفًا مفاده أنه طالما أن الضرر الذي تتعرض له دولة ما يفي بالحد المنصوص عليه فى هذه القاعدة، فلا صلة بعامل المكان بذلك الضرر. على سبيل المثال حالة تقوم فيها الدولة "أ" بتخزين البيانات الحكومية المطلوبة لأداء وظائف حكومية بطبيعتها (القاعدة 4) على الخوادم فى الدولة "ب "، حيث تقوم مجموعة غير حكومية تعمل فى الدولة "ج" بإجراء عمليات إلكترونية ضد الخوادم، مما يؤدي إلى إفساد البيانات الخاصة بالدولة "أ". من ثم يتعين التزام الدولة "ج" العناية الواجبة تجاه الدولة "أ" لأن أراضيها تستخدم لإلحاق الضرر بدولة أخرى.

---

mecum." *Harv. Nat'l Sec. J.* 8 (2017): 239.

[1] Giri, Shailendra. "Cyber crime, cyber threat, cyber security strategies and cyber law in Nepal." *Pramana Research Journal* 9.3 (2019): 662-672.

Gordon, Matthew S. *Economic and national security effects of cyber-attacks against small business communities*. Diss. Utica College, 2018.

[2] Buchan, Russell. "Cyberspace, non-state actors and the obligation to prevent transboundary harm." *Journal of Conflict and Security Law* 21.3 (2016): 429-453.

[3] Ball, Antonia. "Self-Defence and the Notion of Armed Attack in the Context of Hybrid Warfare: Accumulation of events; a hybrid solution to a hybrid problem." (2020).

[4] Shane, Peter M., and Jeffrey Hunker. "Cybersecurity: Shared Risks, Shared Responsibility." (2011).

[5] Pisillo-Mazzeschi, Riccardo. "The due diligence rule and the nature of the international responsibility of states." *German YB Int'l L.* 35 (1992): 9.

[6] Hessbruegge, Jan Arno. "The historical development of the doctrines of attribution and due diligence in international law." *NYUJ Int'l. L. & Pol.* 36 (2003): 265.

(ISSN: 2356 - 9492)

لا ينفى ذلك أهمية الجهد الأكاديمي لبحث آليات الإسناد فى سياق الفضاء الإلكتروني، ومحاولة ربط ذلك بالالتزام بمنع الضرر العابر للحدود كآلية قانونية لحماية سيادة الدولة من العمليات السيبرانية الخبيثة التي حظيت باهتمام أقل. فى ضوء ذلك، نهدف إلي تقييم الالتزام بمنع الدول التي تكون بنيتها التحتية السيبرانية متورطة أو تستخدمها جهات فاعلة من غير الدول لارتكاب سلوك سيبراني ضار عابر للحدود، وبشكل أكثر تحديدًا، طبيعة ونطاق ومحتوى هذا الالتزام القانوني.

المطلب الرابع

طبيعة الالتزام بمنع الضرر العابر فى القانون الدولي

ومدي انطباقه فى السياق السيبراني

الالتزام بمنع الضرر العابر للحدود كالتزام عام بموجب القانون الدولي العرفي، هو التزام يقتضى من الدول امتلاك حد أدنى من الأجهزة القانونية والإدارية القادرة على منع الجهات غير الحكومية من استخدام البنية التحتية السيبرانية لارتكاب سلوك ضار عبر الحدود ، مع استخدام هذا الجهاز بجد لقمع التهديدات الصادرة من أراضيها.

مضمون الالتزام بالمنع هو التزام باعتماد التدابير التشريعية والإدارية التي يجب أن تظهرها الدولة من أجل قمع السلوك السيبراني الضار. أما الشق الثاني لهذا الالتزام فهو الوفاء بمعيار العناية الواجبة الذي ستخضع له الدولة عند استخدام مواردها للتصدي للتهديدات السيبرانية الناشئة عن الإنترنت.

تشير ممارسات الدول الحديثة إلى أن الدول تفرض فى الواقع سيادتها الإقليمية على جوانب الفضاء السيبراني التي تدعمها البنية التحتية المادية الموجودة داخل إقليمها. ونتيجة لذلك، أدركت الدول قابلية تطبيق التزام القانون الدولي العرفي بمنع الضرر العابر للحدود على التهديدات التي تنشأ من بنيتها التحتية الإلكترونية .تأكيد قابلية تطبيق هذا الالتزام على الفضاء الإلكتروني جاء من خلال القاعدة 5 من دليل تالين، والتي توضح أنه يجب على الدول الاعتراف بمسؤوليتها والتصرف بناءً عليها لحماية المعلومات وتأمين النظام الوطني من سوء الاستخدام، متي كانت تلك البنية التحتية تحت سيطرتها الحكومية الحصرية لاستخدامها فى الأعمال التي تؤثر بشكل سلبي وغير قانوني، والتي تشمل الدول المضيفة، ولكن أيضًا الدول العابرة .على سبيل المثال، فى قضية نيكاراغوا، رأت محكمة العدل الدولية أن نيكاراغوا كانت ملزمة بمنع استخدام أراضيها لتهريب المعدات العسكرية المخصصة للمتمردين فى السلفادور

بالقياس، فى الفضاء السيبراني، لا ينطبق الالتزام المعتاد بمنع الضرر العابر للحدود فقط على الدول التي تستخدم بنيتها التحتية السيبرانية من قبل جهات فاعلة من غير الدول كمنصة انطلاق للسلوك السيبراني الضار، بل يمتد أيضًا إلى تلك الدول التي تُستخدم بنيتها التحتية السيبرانية كمنصة للعمليات السيبرانية الخبيثة التي تم اختلاقها وارتكابها من قبل جهات فاعلة من غير الدول فى دولة أخرى وتشق طريقها إلى وجهتها النهائية فى مكان آخر.

نطاق وطبيعة الالتزام بمنع الضرر العابر للحدود

عندما يفرض القانون الدولي على دولة ما التزاما باتخاذ إجراء إيجابي، فمن الضروري تصنيف ذلك الواجب القانوني الدولي إما على أنه التزام بنتيجة أو التزام بسلوك .[1]تفرض الالتزامات بالنتيجة التزامًا مطلقًا[2] على الدول لضمان الحصول على نتيجة دقيقة. سيشكل فشل الدولة فى الوفاء بهذا الالتزام فعلًا غير مشروع دوليًا بغض النظر عما إذا كانت الدولة مخطئة فى الفشل فى تحقيق النتيجة .

وعلى النقيض من ذلك، فإن الالتزامات بالسلوك غير غائبة[3]، ولا تتطلب تحقيق نتائج محددة، ولكنها تتطلب بدلاً من ذلك أن تنشر الدول وسائل مناسبة، لبذل أفضل الجهود الممكنة - للقيام بأقصى حد- للحصول على [النتيجة][4]، فإن التعدي على الالتزام بالسلوك يحدث فقط عندما يمكن إثبات أن الدولة مخطئة؛ تتوقف المسؤولية على فشل الدول فى ممارسة اليقظة أو العناية أو الحكمة الكافية.

من الواضح أن الالتزام المعني هو التزام بالسلوك وليس التزاما بنتيجة، فالتزام الدول الأطراف هو بالأحرى استخدام جميع الوسائل المتاحة لهم فى حدود المعقول ، من أجل منع التهديدات السيبرانية قدر الإمكان.

المبحث الثالث

الالتزام ببذل العناية الواجبة فى الفضاء السيبراني

من منظور التشريعات الوطنية

لا يوضح القانون الدولي بالتفصيل كيف ينبغي للدول أن تشرع فى تعزيز أمنها السيبراني لمراعاة التزامات العناية الواجبة الناشئة. ونتيجة لذلك، من المفيد النظر فى نهج كل من القطاعين العام والخاص لتحديد العناية الواجبة. يمكن لمثل هذه الاستراتيجيات الوطنية، بمرور الوقت، أن تتبلور فى القانون الدولي العرفي كما توضح ممارسات الدول.[5]

وبالمثل، نظرًا للتكامل بين القطاعين العام والخاص، سيما فيما يتعلق بأفضل ممارسات الأمن السيبراني، فإن جهود القطاع الخاص الهادفة إلى تعزيز الأمن السيبراني يتعين أن تؤخذ بعين الاعتبار عند رسم السياسات الوطنية بشأن هذا السياق. وهكذا، رأينا أن نطرح

[1] Dupuy, Pierre-Marie. "Reviewing the difficulties of codification: on Ago's classification of obligations of means and obligations of result in relation to state responsibility." *European Journal of International Law* 10.2 (1999): 371-385.

[2] Pisillo-Mazzeschi, Riccardo. "The due diligence rule and the nature of the international responsibility of states." *German YB Int'l L.* 35 (1992): 9.

[3] j kulesza "due designs in cyberspace" in IM Portela and F Almeida, Organizational, Legal, and Technological Doimeisons of Information System Administration (Information Science, 2014) 76, 79.

[4] *Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area*, Seabed Disputes Chamber of the International Tribunal for the Law of the Sea, Advisory Opinion (2011) para 110.

[5] راجع:
Henckaerts, Jean-Marie, and Doswald-Beck, Louise. 2005. Assessment of customary international law. ICRC. http://www.icrc.org/customary-ihl/eng/docs/v1_rul_in_asofcuin. Accessed 26 Mar 2021.

(ISSN: 2356 - 9492)

فى هذا القسم الأخير مناقشة لعدة حالات وطنية ومنهجها فى إنفاذ مبدأ العناية الواجبة للأمن السيبراني بما فى ذلك الولايات المتحدة وألمانيا والصين كخطوة أولى للكشف عن طيف حوكمة العناية الواجبة.

يستعرض هذا القسم الفرعي بإيجاز الأساليب الوطنية للولايات المتحدة وألمانيا والصين فيما يتعلق بتنظيم العناية الواجبة للأمن السيبراني. تم اختيار تلك الحالات لأبعاد واقعية تتعلق بكون تلك الدول الأكثر تعرضا لتلك الانتهاكات والأكثر نشاطاً فى مواجهتها، أيضاً لأبعاد قانونية كون تلك الدول تمثل مدارس قانونية مختلفة بين القانون العام والقانون المدني، بالإضافة إلى وجهات نظر الأسواق المتقدمة والناشئة حول هذه القضية. لا يُقصد بهذا التحليل أن يكون حسمًا للموضوع قيد النظر، ولكن بدلاً من ذلك لتقديم لمحة سريعة عن كيفية تعامل هذه المجموعة الفرعية المؤثرة من الدول مع موضوع العناية الواجبة للأمن السيبراني. هناك حاجة إلى مزيد من البحث لتوضيح ما إذا كانت الاتجاهات الملحوظة تعمل على مستوى العالم.

الولايات المتحدة الأمريكية

لم يحظ موضوع العناية الواجبة للأمن السيبراني فى حد ذاته بقدر كبير من الاهتمام من قبل إدارة أوباما، على الرغم من أنها أشارت إلى الموضوع فى استراتيجيتها الدولية للفضاء السيبراني. فى ذلك، لتنص الإدارة على العناية الواجبة للأمن السيبراني بما يلي: "يجب على الدول الاعتراف بمسؤوليتها والتصرف بناءً على مسؤوليتها لحماية البنى التحتية للمعلومات وتأمين الأنظمة الوطنية من التلف أو سوء الاستخدام".[1]

ويمثل هذا جهدًا لمساعدة الأشخاص الذين يدافعون عن إرساء معيار العناية الواجبة للأمن السيبراني فى القانون الدولي الضروري، كخطوة للجهود الأوسع نطاقًا لتعزيز السلام السيبراني[2]. تذهب الحجة إلى أنه نظرًا للصعوبات العملية والسياسية المحيطة بتطوير المعاهدات المتعددة الأطراف فى مجال الأمن السيبراني، فإن إنشاء المعايير يوفر فرصة لتعزيز الأمن السيبراني العالمي دون انتظار اتفاقية عالمية شاملة، والتي قد تأتي بعد فوات الأوان على الإطلاق.[3]

لكن على الرغم من الاتفاق العام على قيمة الأمن السيبراني بما فى ذلك العناية الواجبة، لا تزال "حتى المعايير البسيطة تواجه معارضة شديدة. حيث تتضارب الأجندات السياسية، والأعمال العسكرية السرية، والتجسس [،] والتنافس على النفوذ العالمي حيث يواجه " سياقًا صعبًا لتطوير ونشر المعايير السيبرانية[4] ؛ وهو وضع يمكن القول إن تسريبات وكالة الأمن القومي قد فاقمته. نتيجة لذلك، لكي تنجح فى مثل هذا المناخ الصعب، يجب أن تكون المعايير "واضحة ومفيدة وقابلة للتنفيذ ..."[5].

كيف ستبدو معايير العناية الواجبة للأمن السيبراني إذن؟ من المفيد إجراء مراجعة موجزة لمقاربات الولايات المتحدة تجاه هذا الموضوع من أجل توفير إطار بناء للمناقشة.

كانت الولايات المتحدة رائدة من نواح كثيرة فى مجال الأمن السيبراني على المستوى الوطني، بدءًا من إنشاء أول فريق للاستجابة للطوارئ السيبرانية فى جامعة كارنيجي ميلون فى عام 1988 استجابة لعدد متزايد من عمليات اقتحام الشبكات.[6]

---

[1] Obama, Barack. 2011. International strategy for cyberspace: Prosperity, security, and openness in a networked world. White House. https://www.whitehouse .gov/ sites/ default/files/rss_viewer/ international_strategy_for_cyberspace.pdf. Accessed 26 Mar 2015.

[2] Shackelford, Scott J. 2014. Managing cyber-attacks in international law, business, and relations: In search of cyber peace. Cambridge: Cambridge University Press.

[3] Craig, Amanda N., Scott J. Shackelford, and Janine S. Hiller. "Proactive cybersecurity: A comparative industry and regulatory analysis." *American Business Law Journal* 52.4 (2015): 721-787.

راجع أيضا:

Shackelford, Scott J., Scott Russell, and Andreas Kuehn. "Unpacking the international law on cybersecurity due diligence: Lessons from the public and private sectors." *Chi. J. Int'l L.* 17 (2016): 1.

[4] Lewis, James A. 2013. Raising the bar for cybersecurity. CSIS. http://csis.org/files/publication/130212_Lewis_RaisingBarCyb at 58

[5] Finnemore, Martha. 2011. Cultivating international cyber norms. In America's cyber future: Security and prosperity in the information age, eds. Kristin M. Lord and Travis Sharp, 87–102. Washington, DC: CNAS. At 90

[6] والمنظمات المسؤولة عن مختلف جوانب الأمن السيبراني للدولة. يقال إن وزارة الدفاع الأمريكية تدير اليوم، على الرغم من ذلك، فإن الحقل مزدحم بمجموعة كبيرة من الوكالات الأبجدية أكثر من 15000 شبكة في 4000 منشأة منتشرة في حوالي 88 دولة.

Lord, Kristin M., and Travis Sharp. 2011. Executive summary. In America's cyber future: Security and prosperity in the information age.

ومع ذلك، ركزت غالبية جهود الولايات المتحدة فى هذا المجال على تأمين البنية التحتية الحساسة ("CI"). على الرغم من أن الكونجرس كان نشطًا فى هذا الصدد، إلا أن الإدارات الناجحة - بما فى ذلك إدارات الرؤساء كلينتون وبوش وأوباما - قد دفعت الكرة للأمام لتأمين ثغرة أمنية ضعيفة.[1]

قبل مغادرته البيت الأبيض، أعلن الرئيس أوباما أن المخابرات المركزية الأمريكية هي "أصول وطنية استراتيجية" فى عام 2009 على الرغم من أن سياسة الأمن السيبراني الأمريكية المتكاملة لم يتم وضعها بعد.[2] فى مواجهة تقاعس الكونغرس ، أصدر الرئيس أوباما أمرًا تنفيذيًا ، من بين أمور أخرى ، حيث وسّع مشاركة المعلومات بين القطاعين العام والخاص وأنشأ إطار عمل NIST الذي يتألف جزئيًا من أفضل ممارسات القطاع الخاص التي يمكن للشركات اعتمادها لتأمين البني التحتية CI بشكل أفضل هذا الإطار مهم منذ ذلك الحين [3] ، يمكن القول إنه يحفز تطوير معيار بذل العناية الواجبة فى الأمن السيبراني فى الولايات المتحدة .[4]

المانيا

تعترف الإستراتيجية بالفضاء الإلكتروني كمجال أساسي للدولة الألمانية والاقتصاد والمجتمع، وتؤكد على حماية البنية التحتية للدولة كأولوية أساسية لاستراتيجية الأمن السيبراني. علاوة على ذلك، تقوم استراتيجية العناية الواجبة للأمن السيبراني على الاعتراف بأن "الحوادث فى البنى التحتية للمعلومات فى البلدان الأخرى قد تؤثر أيضًا بشكل غير مباشر على ألمانيا". كما يدعو إلى وضع مدونة لقواعد السلوك، والتنسيق القانوني الدولي والتعاون ، وينص على أن مقدمي الخدمات قد يحتاجون إلى تحمل مسؤولية أكبر عن أمن منتجاتهم الرقمية ومستخدميهم بحسب وزارة الداخلية الفيدرالية الألمانية.[5]

Washington, DC: CNAS.

[1] Jensen, Eric Talbot. "Cyber warfare and precautions against the effects of attacks." *Tex. L. Rev.* 88 (2009): 1533.

[2] Obama, Barack. 2009. Remarks by the president on securing our nation's cyber infrastructure. White House, Office of the Press Secretary. http://www.whitehouse.gov/the-press-office/ remarks-president-securing-our-nations-cyber-infrastructure. Accessed 26 Mar 2021.

[3] Armerding, Taylor. 2014. NIST's finalized cybersecurity framework receives mixed reviews. CSO, January 31. http://www.csoonline.com/ article/2134338/security-leadership/ nist-s-finalizedcybersecurity framework-receives-mixed-reviews.html. Accessed 26 Mar 2021.

[4] على وجه الخصوص، ينسق إطار عمل NIST معايير الإجماع وأفضل ممارسات الصناعة لتوفير نهج مرن وفعال من حيث التكلفة لتعزيز الأمن السيبراني ، كما يجادل مؤيدوها ، والذي يساعد مالكي ومشغلي البنية التحتية الحيوية في تقييم وإدارة المخاطر السيبرانية.

على الرغم من أن إطار عمل NIST لم يعد موجودًا إلا لفترة قصيرة نسبيًا، إلا أن بعض عملاء القطاع الخاص يتلقون بالفعل النصيحة بأنه إذا تم التشكيك في "ممارسات الأمن السيبراني الخاصة بهم أثناء التقاضي أو التحقيق التنظيمي، فإن" المعيار "لـ" العناية الواجبة "أصبح الآن إطار عمل الأمن السيبراني.

بمرور الوقت، لا يمتلك إطار عمل NIST القدرة على تشكيل معيار رعاية لمنظمات البنية التحتية الحيوية المحلية فحسب، بل يمكن أن يساعد أيضًا في تنسيق أفضل ممارسات الأمن السيبراني العالمي للقطاع الخاص نظرًا لتعاون NIST النشط مع عدد من الدول بما في ذلك الأمم المتحدة. المملكة واليابان وكوريا وإستونيا وإسرائيل وألمانيا.

[5] تعتمد جهود العناية الواجبة في مجال الأمن السيبراني في ألمانيا على التعاون الوثيق بين القطاعين العام والخاص، على الصعيدين الوطني والعالمي (وزارة الداخلية الفيدرالية الألمانية 2011). تشتهر ألمانيا منذ فترة طويلة بقانونها الوطني القوي لحماية البيانات مع غرامات تصل إلى 300000 يورو، وهي تتحرك الآن من خلال فرض معايير صارمة للأمن السيبراني لـحماية البنية التحتية،

Bundesministerium des Innern. 2008. Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement: Leitfaden für Unternehmen und Behörden. http://www.bmi.bund.de/ SharedDocs/Downloads/DE/Broschueren/2008/Leitfaden_Schutz_kritischer_Infrastrukturen. pdf?__blob=publicationFile. Accessed 26 Mar 2021.

على وجه الخصوص، وافقت الحكومة الفيدرالية على استراتيجية الأمن السيبراني الألمانية ("Cyber-Sicherheitsstrategie für Deutschland") في فبراير 2011. نشطت ألمانيا أيضًا في تحديد ونشر أفضل ممارسات الأمن السيبراني في سياق مماثل لإطار عمل NIST. أصدر المكتب الفدرالي لأمن المعلومات لأول مرة حماية خط الأساس لتكنولوجيا المعلومات ("IT-Grundschutz") في عام 1994.

(ISSN: 2356 - 9492)

تحتوي هذه المجموعة من معايير BSI على توصيات للأمن السيبراني وقد تم تبنيها من قبل الشركات الألمانية وأصحاب المصلحة الدوليين؛ بعض المعايير متاحة الآن باللغات الإنجليزية والسويدية والإستونية. هذه المعايير هي توصيات لأفضل الممارسات التي أصبحت "معايير فعلية لأمن تكنولوجيا المعلومات [الألمانية]" (مراجعة OWASP)، ولكنها ليست قابلة للتنفيذ قانونيًا باستثناء غرامات حماية البيانات المذكورة سابقًا.

الجهود جارية أيضًا فى القطاع الخاص فى ألمانيا لتوسيع مناقشة ونشر أفضل ممارسات الأمن السيبراني. على سبيل المثال، تأسس التحالف من أجل الأمن السيبراني فى عام وهو مبادرة تحت رعاية المكتب الفيدرالي لأمن المعلومات. يجمع أكثر من

ألف جهة مشاركة عامة وخاصة لتبادل أفضل الممارسات وتعزيز قضية العناية الواجبة للأمن السيبراني الألمانية.

يشجع التحالف الإبلاغ الطوعي عن الحوادث والهجمات السيبرانية لجمع المعلومات حول التهديدات الإلكترونية الحالية ضد المنظمات الألمانية. هذه الجهود الخاصة تساعد فى تشكيل معايير الصناعة والمساهمة فى السلوك السيبراني المسؤول.[1]

الصين

تطبق الصين ضوابط صارمة على الإنترنت المحلي من أجل تعزيز المصالح الاقتصادية والسياسية والعسكرية للحزب الشيوعي ولتأمين حكمه[2] على الصعيد الدولي، تواصل السعي إلى التعاون "لتعزيز بناء فضاء إلكتروني سلمي وآمن ومفتوح وتعاوني" ومحاولات لتشكيل المعايير الدولية، لا سيما فيما يتعلق بسيطرة الدولة ذات السيادة على الإنترنت المحلي والرقابة بموجب أمن المعلومات.[3]

فى الوقت نفسه، هناك توترات متزايدة بين الولايات المتحدة والصين حول الاستغلال السيبراني المزعوم بشكل متبادل. فى عام 2014، وجهت الولايات المتحدة لائحة اتهام لخمسة قراصنة تابعين لجيش التحرير الشعبي بتهمة التجسس الإلكتروني الاقتصادي.[4] وقد احتجت الصين بشدة[5] ، بعدما وصفتها الحكومة الأمريكية بأنها "أكثر مرتكبي التجسس الاقتصادي نشاطاً واستمراراً فى العالم" (DNI

Schallbruch, Martin, and Isabel Skierka. *Cybersecurity in Germany*. Springer International Publishing, 2018. Guitton, Clement. "Cyber insecurity as a national threat: overreaction from Germany, France and the UK?." *European Security* 22.1 (2013): 21-35.

[1] تحدث وزير الداخلية الألماني الدكتور توماس دي ميزير مؤخرًا عن موضوع العناية الواجبة للأمن السيبراني على وجه الخصوص خلال قمة التعاون الفضائي العالمي لعام 2014 في برلين. في إشارة إلى الحاجة إلى مراعاة مبدأ المسؤولية في الفضاء الإلكتروني بعناية، أشار دي ميزير إلى مبدأ أساسي في القانون: من يخلق خطرًا على الآخرين هو المسؤول عن ذلك. كلما زاد حجم المخاطرة، كلما زادت المسؤولية

Goodwin, Cristin, et al. "A framework for cybersecurity information sharing and risk reduction." *Microsoft* (2015).

Dimmroth, Katharina, and Wolf J. Schünemann. "The ambiguous relation between privacy and security in German cyber politics." *Privacy, Data Protection and Cybersecurity in Europe*. Springer, Cham, 2017. 97-112.

يلتزم عملاء المخابرات المركزية بإبلاغ السلطات عن الهجمات الإلكترونية. ويُقدر أن جهود سياسة الأمن السيبراني هذه تحتاج إلى ما بين 200 و 425 وظيفة جديدة عبر الحكومة الفيدرالية وتكلفة الموظفين والموارد تصل إلى 38 مليون يورو سنويًا.

Greis, Friendhelm. 2014. Kabinett beschließt Meldepflicht für Cyberangriffe. Golem.de, December 17. http://www.golem.de/news/it-sicherheitsgesetz-regierung-beschliesst-meldepflicht-fuercyberangriffe-1412-111234.html. Accessed 26 Mar 201

[2] راجع :

Wong, Edward. 2014. For China, cybersecurity is part of strategy for protecting the communist party. New York Times, December 3. http://sinosphere .blogs .nytimes.com/ 2014/12/03/for-chinacybersecurity-is-part-of-strategy-for-protecting-the-communist-party/. Accessed 26 Mar 2021

[3] راجع

Sceats, Sonya. 2015. China's cyber diplomacy: A taste of law to come? The Diplomat, January 14. http://thediplomat.com/2015/01/chinas-cyber-diplomacy-a-taste-of-law-to-come/

[4] راجع:

Lindsay, Jon R. "The impact of China on cybersecurity: Fiction and friction." *International Security* 39.3 (2014): 7-47.

راجع أيضاً كل من :

Kshetri, Nir. "Cybersecurity and international relations: The US engagement with China and Russia." *Proc. FLACO-ISA Joint Conf*. 2014.
Shull, Aaron. "Global cybercrime: the interplay of politics and law." *Organized Chaos: Reimagining the Internet* (2014): 97.

[5] راجع:

الالتزام الدولي ببذل العناية الواجبة في الفضاء السيبراني
بين التدابير الرادعة ومنع الأضرار السيبرانية العابرة

د. أسامة حمزة محمود عبد الفتاح

مجلة الدراسات القانونية والاقتصادية

2011) ، بينما حذر الرئيس أوباما فى يونيو 2013 من أن استمرار سرقة الملكية الفكرية الأمريكية يعد أمرًا خطيرًا سيعوق المزيد من التطور. العلاقات التجارية الاقتصادية مع الصين. يمكن اعتبار رد فعل الولايات المتحدة بمثابة نهج لتشكيل معايير العناية الواجبة للأمن السيبراني، من خلال دعوة الصين لتحمل مسؤوليات الاستغلال السيبراني المزعوم.

فى الواقع، كان هناك تقدم فى هذه النتيجة مع إعلان مدونة قواعد السلوك للأمن السيبراني G2 فى عام 2015 ، والتي تلزم ، من بين أمور أخرى ، الولايات المتحدة والصين بوقف التجسس الاقتصادي الثنائي بشكل تعاوني. هذه المعايير لها بعد سياسي قوي ، كما تظهر دراسة حالة الصين.

كما هو الحال مع الولايات المتحدة، فإن استراتيجية الأمن السيبراني فى الصين مجزأة، لكن تطويرها وتنفيذها قد حصل مؤخرًا على دعم سياسي من كبار المسؤولين الحكوميين. [1]

من نواح كثيرة، تعد استراتيجية الأمن السيبراني للصين أوسع نطاقًا من نظيراتها فى الولايات المتحدة أو ألمانيا. حيث تتضمن استراتيجية معالجة أمن الشبكات وأجهزة الحاسوب، الرقابة على المحتوى والتحكم فى المعلومات إلى حد أكبر بكثير مما هو الحال فى هذه الدول الغربية. فالموقف الرسمي للحكومة الصينية هو أن "توجيه الرأي على الإنترنت بشكل صحيح هو إجراء رئيسي لحماية أمن معلومات الإنترنت"[2]. ينعكس موقف الصين بشأن الأمن السيبراني فى فكرة سيادة الإنترنت واستخدامه كوسيلة لبناء اقتصاد معلومات محلي وشبكة آمنة على مستوي البنية التحتية التي تفيد التنمية المحلية والاستقرار السياسي.[3]

تتماشى بعض هذه التدابير مع جهود العناية الواجبة للأمن السيبراني؛ البعض الآخر أوسع نطاقًا وأثار مخاوف ، لا سيما من نظرائهم فى الولايات المتحدة وأوروبا. على سبيل المثال، فى عام 2007، أنشأت الصين مجموعة من معايير الأمان التي تتضمن، "لوائح الحماية السرية لأمن المعلومات" (والتي يشار إليها أيضًا باسم نظام الحماية متعدد المستويات، "MLPS") بهدف حماية المعلومات وحماية الأمن القومي.[4] أعربت الشركات والمنظمات الغربية مرارًا عن رفضها لأن هذه المعايير الفنية لا تتوافق مع معايير أمن تكنولوجيا المعلومات

Weihua, Chen. 2014. China protests against US indictment. China Daily, May 20. http://usa.chinadaily.com.cn/world/2014-05/20/content_17519650.htm. A

[1] في أوائل عام 2014، شدد الرئيس الصيني شي جين بينغ على ضرورة اتباع نهج موحد وشامل لـ "أمن الشبكة" مع تحول الصين إلى "قوة إلكترونية". تزامن الخطاب مع إنشاء "المجموعة المركزية لقيادة الأمن السيبراني والمعلوماتية" ، والتي ستدير الأمن السيبراني الصيني تحت قيادة الرئيس شي جين بينغ

Jinping, Xi: China must evolve from a large internet nation to a powerful internet nation. Xinhuanet. com, February 27, 2014. http://news.xinhuanet.com/politics/2014-02/27/c_119538788.htm. Accessed 26 Mar 2021.

[2] راجع

Buckley, Chris and Lucy Hornby. 2010. China defends censorship after Google threat. Reuters, January 14. http://www.reuters.com/article/2010/01/14/us-china-usa-google-idUSTRE60C1TR20100114. Accessed 26 Mar 2 2021

[3] يعود تاريخ أول استراتيجية للأمن السيبراني في الصين إلى عام 2003. ويشار إليها باسم "الوثيقة 27: حيث تتضمن آراء لتعزيز ضمان أمن المعلومات وتغطي - من بين أمور أخرى – حماية البنية التحتية للدولة ، تواصل استراتيجية الأمن السيبراني الحالية لعام 2012 بعض اعتبارات الأمن السيبراني السابقة (بما في ذلك حماية CI) بينما تتناول أيضًا اعتماد الصين على التكنولوجيا الأجنبية كمسألة أمنية ، وتعزيز معايير التشفير الصينية ، وبناء البنية التحتية للنطاق العريض ، والجيل القادم من الهواتف المحمولة التكنولوجيا والخدمات الحكومية الإلكترونية. انتقد المراقبون الوثيقة باعتبارها "حقيبة انتزاع من مقترحات السياسة الغامضة" غير المتسقة. راجع في ذلك كل من

Sceats, Sonya. 2015. China's cyber diplomacy: A taste of law to come? The Diplomat, January14. http://thediplomat.com/2015/01/chinas-cyber-diplomacy-a-taste-of-law-to-come/.

Segal, Adam. 2012. China moves forward on cybersecurity policy. Council on Foreign Relations,July24.http://blogs.cfr.org/asia/2012/07/24/china-moves-forward-oncybersecurity-policy/. Accessed 26 Mar 2021

[4] راجع:

Ahrens, Nathaniel. 2012. National security and China's information security standards: Of Shoes, Buttons, and Routers. Center for Strategic and International Studies, November 8. http://csis. org/publication/national-security-and-chinas-information-security-standards. Accessed 26

(ISSN: 2356 - 9492)

الدولية. وبدلاً من حماية الأمن القومي، كان يُنظر إلى هذه المعايير على أنها تدابير لحماية شركات تكنولوجيا المعلومات المحلية الصينية من المنافسة العالمية. يجادل البعض بأن مثل هذه الجهود أدت فى الواقع إلى معايير وتكنولوجيا صينية أقل أمانًا.[1]

لا تزال التشريعات الصينية الحديثة أو المعلقة الأخرى تنذر بمزيد من الحماية، مثل مطالبة شركات التكنولوجيا التي تبيع البنوك الصينية بتقديم كود المصدر الخاص بها للفحص الحكومي وحتى الكشف عن مفاتيح التشفير وتثبيت الأبواب الخلفية لمنح السلطات الصينية إمكانية الوصول إلى البيانات والاتصالات المؤمنة.[2]

تؤثر مثل هذه السياسات على شركات التكنولوجيا الغربية، وقد تمنعها حتى من دخول السوق الصيني المتنامي. باختصار ، تعرب الصين عن الحاجة إلى السيطرة على المعلومات واستبعاد تقنيات الأمن المملوكة للأجانب من أجل حماية استقرارها المجتمعي. ونتيجة لذلك، تركز استراتيجيتها على الأمن القومي والتقدم الاقتصادي.

وبالتالي تبدو عناصر العناية الواجبة الإلكترونية مختلفة تمامًا عند مقارنتها بالحالات الأمريكية أو الألمانية، مما يدل على صعوبة صياغة معيار عالمي فى هذا المجال. ومع ذلك، يمكن للمرء أن يفسر نسخة صينية من العناية الواجبة للأمن السيبراني والتي هي فى الطرف الآخر من الطيف المحتمل والتي تشمل المبررات الاقتصادية المحلية والتدابير الوقائية بدلاً من التركيز الضيق على تأمين البني التحتية للدولة CI. فى الواقع، العديد من أهداف السياسة متشابهة عبر دراسات الحالة الثلاث؛ ما يختلف هو الوسيلة.

يتطلب العرف ممارسة الدولة واسعة النطاق التي يتم الاضطلاع بها من منطلق الشعور بالالتزام القانوني. اعتمادًا على نوع القاعدة المتضمنة، يجب أن تكون ممارسة الدولة أكثر أو أقل انتشارًا. بالنسبة للمعايير الجديدة، مثل الأمن السيبراني، يكون المعيار عمومًا "موحدًا تقريبًا" من ممارسات الدولة.

لا يمكننا الادعاء ببلوغ سياق العناية الواجبة للأمن السيبراني درجة العرف الدولى، يتضح ذلك من الموقف الذى اتخذته هذه الدول مع كون الولايات المتحدة أكثر تطوعية، وألمانيا تتخذ نهجًا تنظيميًا أكثر نسبيًا، وجهود الصين الاقتصادية والأمن القومي الأوسع. . ومع ذلك، وبغض النظر عن دراسات الحالة الوطنية، هناك أيضًا دروس قيمة من القطاع الخاص يمكن أن تحدد الشكل النهائي لمعايير العناية الواجبة للأمن السيبراني.

لا يزال مجال العناية الواجبة للأمن السيبراني الدولي مجالًا معقدًا وصعبًا، ولكنه يتطلب مشاركة أكاديمية وخاصة وعامة مستدامة لإحراز تقدم. فمن بين المقترحات على سبيل المثال، يمكن للدول ممارسة العناية الواجبة من خلال الوسائل السلبية ، وتعزيز المرونة فى شبكات الدول الشريكة والمحلية.[3] أنظمة التحذير من أنواع مختلفة من الهجمات الإلكترونية التي تسهلها فرق الاستجابة للطوارئ الإلكترونية ، والمشاركة النشطة (ثنائية الاتجاه) لمعلومات القطاع الخاص والتعاون بشأن تحديد ونشر أفضل ممارسات الأمن السيبراني ، ويمكن اعتبار حملة قوية للنظافة السيبرانية ضرورية أخرى عناصر العناية الواجبة للأمن السيبراني.[4]

Mar 2021.

[1] راجع

Gierow, Hauke Johannes. 2014. Cyber security in China: New political leadership focuses on boosting national security. Mercator Institute for China Studies .http:// www .merics.org/fileadmin/templates/download/china-monitor/China_Monitor_No_20_eng.pdf. Accessed 26 Mar 2021

من المنافسة في سوق الشركات الصينية للمؤسسات المالية ومرافق الطاقة، على سبيل المثال. قد تساعد مثل Symantec وKasperskyتم منع شركات الأمن السيبراني الرائدة مثل هذه التطورات في فتح الباب أمام الهجمات الإلكترونية على المخابرات المركزية الصينية؛ يضر بأسباب العناية الواجبة للأمن السيبراني.

[2] راجع

Mozur, Paul. 2015. New rules in China upset Western Tech Companies. New York Times, January 28. http://www.nytimes.com/2015/01/29/technology/in-china-new-cybersecurity-rules- - perturb-western-tech-companies.html. Accessed 26 Mar 2021.

[3] راجع

Edwards, Dennis et al. 2007. Prevention, detection and recovery from cyber-attacks using a multilevel agent architecture. System of systems engineering 1, 1 (2007). doi:10.1109/SYSOSE.2007.4304228.

[4] تشمل أفضل الممارسات الأخرى تقسيم الوصول إلى الكود والأنظمة وعمليات التدقيق واختبار الاختراق المنتظم، وتعزيز التكرار وبناء الشبكة الموازية لبناء مزيد من المرونة، بالإضافة إلى تسخير خبرة الأمن السيبراني خارج الحدود التنظيمية للفرد من خلال مكافآت الأخطاء وبرامج مكافآت الثغرات الأمنية

بمرور الوقت، مع تقدم التنسيق القانوني، ستكون هناك فرص لإيجاد روابط متزايدة لبناء معايير الأمن السيبراني، بما فى ذلك تلك المتعلقة بمسألة العناية الواجبة. بالفعل، أصدرت عدد من الحكومات الوطنية المشار إليها أعلاه، وحتى بعض الشركات مثل Microsoft، قوائم بمسودة المعايير للنظر فيها من جانب أصحاب المصلحة[1]

وبالنظر لأفضل ممارسات الأمن السيبراني والتهديد السيبراني للقطاعين العام والخاص، ينبغي استخلاص مفاهيم العناية الواجبة للأمن السيبراني من القانون الدولي العرفي الحالي، ولكن يتم بناؤها من خلال مراجعة الصناعة القواعد التي بدورها توجه السياسات الوطنية.[2] يتطلب تحقيق قدر من السلام السيبراني المشاركة النشطة من جانب أصحاب المصلحة من القطاعين العام والخاص.

الخاتمة

تثير هذه الخيوط المشتركة السؤال التالي، الذي تم تحديده فى بداية هذه الورقة: هل يوجد مبدأ عام للعناية الواجبة فى القانون الدولي؟ ربما. هذا ما بدا أن محكمة العدل الدولية تشير إليه عندما ذكرت، أن "مبدأ المنع هو قاعدة عرفية، وعلى هذا النحو ترجع أصوله إلى [معيار] العناية الواجبة المطلوب من دولة فى إقليمها ،والذى أشرنا إليه سلفاً من خلال السوابق القضائية في قضية مضيق كورفو. وعلى نفس المنوال، نقلاً عن تحكيم مطالبات ألاباما، رأت هيئة التحكيم فى Trail Smelter أنه تم البت فى كلا الحالتين على أساس "نفس المبدأ العام" الذي بموجبه :-

تلتزم الدولة بواجب حماية الدول الأخرى من الأفعال الضارة الصادرة من أجهزتها أو من قبل الأفراد الخاضعين لولايتها القضائية. ولا ينبغي أن ينتقص من إعمال هذا المبدأ أن الإطار القانوني الشامل للالتزامات الوقائية الملزمة لمنع ووقف وجبر الضرر فى الفضاء الإلكتروني ، لا تزال غير مكتملة أو لا ينبغي أن تعامل كالنطاق الاستراتيجي التقليدي للنزاعات الدولية.

بالإضافة إلى ذلك، فإن الالتزامات المختلفة ببذل العناية الواجبة الناشئة فى إطار الفروع المتخصصة للقانون الدولي تنطبق بشكل متزامن لتغطية الاستخدامات والجوانب والعواقب المختلفة لتكنولوجيا المعلومات والاتصالات. من بينها، سلطنا

Kuehn, A., and M. Mueller. 2014. Analyzing bug bounty programs: An institutional perspective on the economics of software vulnerabilities. Proceedings of the 42nd research conference on communication, information, and internet policy. 12–14 September 2014, Arlington, VA. http://papers.ssrn. com/sol3/papers. cfm?abstract_ id =2418812.

[1] تفيد التقارير أن الحكومة الأسترالية نجحت في منع 85٪ من الهجمات الإلكترونية من خلال اتباع ثلاث تقنيات منطقية: تطبيق القائمة البيضاء (السماح فقط للبرامج المعتمدة مسبقًا للعمل على الشبكات) ، وإصلاح التطبيقات وأنظمة التشغيل بانتظام ، و "تقليل العدد إلى الحد الأدنى من الأشخاص على شبكة ما لديهم امتيازات "المسؤول"

Lewis, James A. 2013. Raising the bar for cybersecurity. CSIS. http://csis.org/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf. Accessed 26 Mar 2021

[2] راجع:

McKay et al. 2014. International cybersecurity norms: Reducing conflict in an Internet-dependent world. Microsoft. http://tinyurl.com/ogv9qzq. Accessed 26 Mar 2015.

(ISSN: 2356 - 9492)

الضوء على الالتزام الإيجابي بحماية حقوق الإنسان على الإنترنت، فضلاً عن واجب ضمان احترام القانون الدولي الإنساني واعتماد الاحتياطات ضد آثار الهجمات الإلكترونية فى النزاعات المسلحة.

فى حين أن القواعد المذكورة تتداخل ويمكن تفسيرها بشكل منهجي، بقدر ما تعمل على تحقيق أهداف مماثلة، فإنها تظل منفصلة ولا ينبغي الخلط بينها. لكل منها محفزات ومتطلبات ومعايير رعاية مختلفة. قد يكون من الممكن، من خلال أوجه التشابه بينهما، اشتقاق مبدأ عام من مبادئ القانون الدولي. علاوة على ذلك، تحتفظ الدول بصلاحية تطوير - من خلال القانون الدولي التقليدي أو العرفي - واجب متخصص جديد يحتوي على معيار "العناية الواجبة عبر الفضاء السيبراني".

يمكن صياغة هذا الواجب بناءً على أي من التزامات الحماية الحالية أو مزيج منها، مما يعكس القاعدة 6 من دليل تالين. ومع ذلك، فى المناقشات حول سلوك الدولة الدؤوب فى الفضاء الإلكتروني، لا ينبغي تقديم الشكوك حول مبدأ عام أو التزام حماية خاص بالإنترنت كبديل للفراغ القانوني.

يوفر القانون الدولي بالفعل مزيج من واجبات الحماية التي تتطلب مجتمعة من الدول بذل قصارى جهدها لمنع مجموعة واسعة من الأضرار عبر الفضاء السيبراني ووقفها والاستجابة لها.

نتائج الدراسة

- خلال هذه المساهمة، أكدنا أن مفهوم العناية الواجبة يمكن فهمه بشكل أفضل على أنه معيار مرن للرعاية أو الحكم الرشيد الموجود فى مجموعة متنوعة من القواعد الأساسية للقانون الدولي عبر مجموعة من المجالات. وهكذا، بطريقة ما، هناك خليط من الالتزامات الوقائية المختلفة، ولكن المتداخلة التي تتطلب أن يكون هذا المعيار قابلاً للتطبيق فى الفضاء السيبراني. ومع ذلك، فإن مجموعة من العناصر الأساسية تربطها ببعضها البعض.
- أولاً، تفترض جميع التزامات الحماية التي تم استطلاعها أعلاه ممارسة سلطة الدولة أو الولاية القضائية أو مستوى معين من السيطرة على إقليم، أو صاحب الحق، أو الجاني، أو الأحداث المعنية.
- ثانياً، وعلى نحو متصل، هذه الالتزامات خاضعة ومحدودة لقدرة الدولة على التصرف' مما يعطي تأثيرًا لفكرة أن للدول مسؤوليات مشتركة، ولكن متباينة فى القانون الدولي[1].
- ثالثًا، تقترن التزامات السلوك المرنة هذه بالتزامات النتيجة لوضع الحد الأدنى من البنية التحتية التشريعية والقضائية والتنفيذية اللازمة لممارسة العناية الواجبة. الضرر أو الخطر المعني، بدءًا من المعرفة الفعلية أو البناءة إلى إمكانية التنبؤ الموضوعية أخيرًا[2]

[1] Alabama Claims (United States v UK) (1872) 29 RIAA 125, supra note 15, at 129; ILA Study, supra note 14, at 20, 47; HRComm, General Comment No. 36, supra note 43, § 21; Bosnian Genocide, Judgment, 26 February 2007, ICJ Reports 2007, paras 430–432; Nicaragua, supra note 41, para. 157. See also Koivurova, supra note 9, paras 17, 19.

[2] ILC, Draft Articles on Prevention, supra note 21, at 155–156, Commentary to art. 3, para. 17; art. 5 and Commentary; ILA Study, supra note 14, at 124; Alabama Claims (United States v UK) (1872) 29 RIAA 125, 131; Koivurova, supra note 9, para. 21; Pisillo-Mazzeschi, supra note 14, at 26–27; Kolb, supra note 37, at 117, 127; Couzigou, supra note 101, at 50–51; Okwori, ibid 74, at 223; Krieger & Peters, supra note 35

- لا شك أن فكرة تطبيق نظرية المسؤولية الموضوعية على الالتزام الدولي ببذل العناية السيبرانية، اعتمادا على مؤشرات مثل مشاركة البنية التحتية الحكومية فى هجوم إلكتروني خادعًا. وذلك للأسباب التالية: –

- أولاً، قد يخترق المتسللون من غير الدول خادمًا حكوميًا خلال الهجمات الإلكترونية التي يتم شنها من البنية التحتية الحكومية، ما يجعل هذا المعيار غير كافياً بحد ذاته لإثبات المسؤولية الدولية فى السياق السيبراني.
- ثانيًا، غالبًا ما تنطوي الهجمات الإلكترونية على إخفاء هوية الجهة الفاعلة "الانتحال" وذلك من خلال التقنيات. حيث تستخدم غالبية الهجمات الإلكترونية مثل هذه التكتيكات التنكرية. حتى إذا كانت سجلات الشبكة تشير إلى أن هجومًا إلكترونيًا استغل البنية التحتية الحكومية لدولة ما.
- ناقشنا في تلك الدراسة فكرة نقل عبء الاثبات في الهجمات السيبرانية كآلية داعمة لتأسيس المسؤولية الدولية في الفضاء السيبراني: كلما ارتبط هجوم إلكتروني بالبنية التحتية الحكومية، أو عندما "يمكن تتبع نشاط إلكتروني ضار إلى إقليم دولة واحدة". حيث يمكن أن تنقل المحاكم الدولية عبء الإثبات إلى الدولة الضحية، التي يجب أن تنفى معرفتهم البناءة المفترضة.
- يتعارض نقل عبء الإثبات مع فقه محكمة العدل الدولية[1]. فلا يمكن تأسيس المسؤولية الدولية على السيادة الإقليمية ". فلا تؤدي سيطرة الدولة على الشبكات الحكومية إلا إلى ظهور "معرفة مجردة وغير مادية" للهجوم الإلكتروني، وهي غير كافية لتحمل مسؤولية الدولة. بيد أن الدول الضحية قد تستخدم سيطرة الدولة المتهمة على البنية التحتية الحكومية كدليل.
- اخيـرًا، كـل هـذه العناصـر موجهـة نحـو واجـب مركـزي لمنـع و / أو وقـف و / أو جبـر الضـرر أو مخـاطره، والـذي يتكـون مـن فعـل مخـالف لحقـوق الـدول الأخـرى، أو ضـرر جسـيم عـابر للحـدود أو انتهـاك لقواعـد دوليـة أكثـر تحديـدًا.، مثـل القـانون الدولي لحقوق الإنسان والقانون الدولي الإنساني.

[1] Marco Roscini, Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations, 50 Tex. Int'l L. J. 233, 245-48 (2014).

(ISSN: 2356 - 9492)

قائمة المراجع:-

المراجع العربية

- ا.د/ أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية ، ط 2000
- ا.د/ الشافعي محمد بشير، قانون حقوق الانسان مصادره وتطبيقاته الوطنية والدولية، منشاة المعارف، الطبعة الثالثة، 2004
- ا.د / محمد مصطفي يونس، الاستاذ الدكتور جعفر عبد السلام، مبادئ القانون الدولي العام، دون سنة نشر
- ا. د/ محمود نجيب حسني، شرح قانون العقوبات- القسم العام، الطبعة السادسة، دار النهضة العربية، 1989.
- ا.د / مصطفي أحمد فؤاد، أحكام القانون الدولي العام، مطبعة النهضة، دون سنة نشر
- ا.د / مصطفي أحمد فؤاد، العلاقات الدولية في منظور المنظمات الدولية، دون سنة نشر.
- ا.د/ مصطفي أحمد فؤاد، أصول القانون الدولي العام، الجزء الثاني (النظام القانوني الدولي) ، دون سنة نشر
- ا.د/ محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية
- ا.د/ سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، دار النهضة العربية، ط 1999
- ا.د/ محمد عادل محمد عسكر ، وضع العمليات السيبرانية في القانون الدولى مع التطبيق على ممارسة التجسس وقت السلم. مجلة البحوث القانونية والاقتصادية، المجلد 33 ، العدد 1 ، يناير 2021 ،

قائمة المراجع الأجنبية

- Bannelier, K. J. B. y. o. i. l. (2014). "Cyber diligence: a low-intensity due diligence principle for low-intensity cyber operations?" 14.
- Barnidge, R. J. I. C. L. R. (2006). "The due diligence principle under international law." 8(1): 81-121.
- Baxter, R. R. J. B. Y. I. l. L. (1965). "Multilateral treaties as evidence of customary international law." 41: 275.
- Besson, S. J. E. R. (2020). "Due Diligence and Extraterritorial Human Rights Obligations-Mind the Gap."!
- Chircop, L. J. I. and C. L. Quarterly (2018). "A due diligence standard of attribution in cyberspace." 67(3): 643-668.
- Coco, A. and T. J. E. J. o. I. L. de Souza Dias (2021). "'Cyber Due Diligence': A Patchwork of Protective Obligations in International Law." 32(3): 771-806.
- Corn, G. P. and R. J. A. J. o. I. L. Taylor (2017). "Sovereignty in the Age of Cyber." 111: 207-212.
- Geiß, R., et al. (2013). "Freedom and Security in Cyberspace: Shifting the Focus Away from Military Responses Towards Non-Forcible Countermeasures and Collective Threat-Prevention".
- Gill, T. D. and P. A. Ducheine (2013). Anticipatory self-defense in the cyber context. Israel Yearbook on Human Rights, Volume 43 (2013), Brill Nijhoff: 81-110.
- Gulati, M. J. D. L. (2013). "How do courts find international custom".
- Hathaway, O. A., et al. (2012). "The law of cyber-attack." 100: 817.

- Hinkle, K. C. J. Y. J. o. I. L. (2011). "Countermeasures in the cyber context: One more thing to worry about." 37(Fall): 11-21.
- Koivurova, T. (2008). Due diligence. The Max Planck Encyclopedia of Public International Law (MPEPIL), Oxford University Press.
- Koivurova, T. (2010). Due Diligence, Max Planck Encyclopedia of Public International Law, Oxford.
- Kolb, R. J. G. Y. I. l. L. (2015). "Reflections on due diligence duties and cyberspace." 58: 113.
- Krieger, H., et al. (2020). Due diligence in the international legal order, Oxford University Press.
- Kulesza, J. (2021). Cybersecurity Due Diligence, EasyChair.
- Kumar, A. P. J. B., India (2009). "Cyber law: A view to social security".
- Lazićć, D. J. I. L. M. (2010). "Pulp Mills on the River Uruguay (Arg. v. Uru.)(ICJ), Introductory Note by Djurdja Lazićć." 49(4): 1118-1180.
- Lewis, J. A. and G. Neuneck (2013). The Cyber Index: International Security Trends and Realities, UN.
- Lin, H. J. I. R. o. t. R. C. (2012). "Cyber conflict and international humanitarian law." 94(886): 515-531.
- Liu, I. Y. J. I. J. I. l. and C. L. (2017). "State responsibility and cyberattacks: Defining due diligence obligations." 4: 191.
- Milanović, M. J. E. J. o. I. L. (2006). "State responsibility for genocide." 17(3): 553-604.
- Ohlin, J. D., Et Al. (2015). Cyber War: Law And Ethics For Virtual Conflicts, Oup Oxford.
- Patrick, C. J. W. I. L. L. (2019). "Debugging The Tallinn Manual 2.0's Application Of The Due Diligence Principle To Cyber Operations." 28: 581.
- Pisillo-Mazzeschi, R. J. G. Y. I. L. L. (1992). "The Due Diligence Rule And The Nature Of The International Responsibility Of States." 35: 9.
- Reinisch, A. And M. J. G. Y. I. L. L. Beham (2015). "Mitigating Risks: Inter-State Due Diligence Obligations In Case Of Harmful Cyber Incidents And Malicious Cyber Activity-Obligations Of The Transit State." 58: 101.
- Rollins, J. And C. Wilson (2007). Terrorist Capabilities For Cyberattack: Overview And Policy Issues, Library Of Congress Washington Dc Congressional Research Service.
- Rosas, A. J. N. J. I. L. L. (1991). "Issues Of State Liability For Transboundary Environmental Damage." 60: 29.
- Schmitt, M. N. (2017). Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations, Cambridge University Press.
- Schmitt, M. N. J. C. J. T. L. L. (1998). "Computer Network Attack And The Use Of Force In International Law: Thoughts On A Normative Framework." 37: 885.
- Schmitt, M. N. J. P. R. F. S. A. I. C. (2013). "Cyber Activities And The Law Of Countermeasures." 3: 659-688.
- Seck, S. (2016). "International Law Association Study Group On Due Diligence In International Law".
- Shackelford, S. J., Et Al. (2016). "Unpacking The International Law On Cybersecurity Due Diligence: Lessons From The Public And Private Sectors." 17: 1.
- Shackelford, S. J., Et Al. (2017). "Defining Cybersecurity Due Diligence Under International Law: Lessons From The Private Sector." 115-137.
- Sicilianos, L. A. J. E. J. O. I. L. (2002). "The Classification Of Obligations And The Multilateral Dimension Of The Relations Of International Responsibility." 13(5): 1127-1145.
- Sklerov, M. J. J. M. L. R. (2009). "Solving The Dilemma Of Sate Responses To Cyberattacks: A Justification For The Use Of Active Defenses Against States Who Neglect Their Duty To Prevent." 201: 1.
- Solomon, J. (2011). Cyberdeterrence Between Nation-States: Plausible Strategy Or A Pipe Dream?, Systems Planning And Analysis Inc Alexandria Va.
- Stephens, T. And D. J. I. L. A. French, London (2016). "Ila Study Group On Due Diligence In International Law, Second Report, July 2016".
- Thirlway, H. J. N. Y. O. I. L. (2001). "Reflections On Lex Ferenda." 32: 3-26.
- Ventre, D. (2014). Chinese Cybersecurity And Defense, John Wiley & Sons.

(ISSN: 2356 - 9492)

- Waxman, M. C. J. Y. J. I. L. L. (2011). "Cyber-Attacks And The Use Of Force: Back to the future of article 2 (4)." 36: 421.
- Wright, Q. J. A. J. o. I. L. (1949). "The corfu channel case." 43(3): 491-494.
- Ziolkowski, K. J. N. C. C. P. (2013). "Confidence Building Measures for Cyberspace–Legal Implications." 1-88.

قائمة الاتفاقيات والتقارير الدولية

- Stephens, Tim, and Duncan French. "ILA Study Group on Due Diligence in International Law, Second Report, July 2016." *International Law Association, London* (2016).
- Reparation for Injuries Suffered in the Service of the United Nations, Advisory Opinion, 1949 I.C.J. Rep. 174, 180 (Apr. 11).
- Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. Rep. 14, 106 para. 202.
- Corfu Channel, Judgment, 9 April 1949, ICJ Reports (1949), at 22 (emphasis added).
- International Law Commission (ILC), Articles on Responsibility of States for Internationally Wrongful Acts, GA Res. 56/83, 12 December 2000, art. 14(3) (hereinafter 'ARSIWA').
- Corfu Channel, Judgment, 9 April 1949, ICJ Reports (1949), at 22.
- ILC, Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries, in Report of the International Law Commission on the work of its fifty-third session (23 April–1 June and 2 July–10 August 2001), UN Doc. A/56/10,
- Brunée and Meshel, 'Teaching an Old Law New Tricks: International Environmental Law Lessons for cyberspace Governance', 58 GYIL (2015) 129, at 134–135
- Trail Smelter (United States v. Canada) (1941) 3 RIAA 1911, at 1963.
- International Law Commission (ILC), Articles on Responsibility of States for Internationally Wrongful Acts, GA Res. 56/83, 12 December 2000, art. 14(3) (hereinafter 'ARSIWA').
- *Pulp Mills*, Judgment, 20 April 2010, ICJ Reports (2010), para. 101.
- [1]United Nations Human Rights Council (HRC), Res. 32/13 ('The promotion, protection and enjoyment of human rights on the Internet'), UN Doc. A/HRC/RES/32/13, 1 July 2016, § 1.
- Convention on the Prevention and Punishment of the Crime of Genocide, 1948, 78 UNTS 277, art. 1(hereinafter Genocide Convention). See also *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)*, Judgment, 26 February 2007, ICJ Reports (2007) 43, paras 430–431.
- UN Convention on the Law of the Sea, 1982, 1833 UNTS 397, art. 194(2) (hereinafter
    - UNCLOS').
- e.g., International Convention for the Suppression of the Financing of Terrorism, 1999, 2178 UNTS 197, art. 18; United Nations Convention against Transnational Organized Crime, 2000, 2225 UNTS209
- Island of Palmas arbitral award, at 839;
- Comments by Member States on the Initial Pre-Draft of the OEWG Report, available at www.un.org/disarmament/open-ended-working-group/
- Comments by Member States on the Initial Pre-Draft of the OEWG Report, available at www.un.org/disarmament/open-ended-working-group/
- the International Law Commission, para. 57, UN Doc. A/CN.4/1/Rev.l (1 February Permanent Mission of the Federal Republic of Germany to the United Nations, Gce » appreciation of the issues of information security, at 4, Note No. 516/2012; Development* in the Field of Information and Telecommunications in the Context of Inte Security, Report of the Secretary-General, at 9, UN Doc. A/68/156 Add. 1 (9 S: 2013) (Ger.).

- Report of the Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/70/174, 22 July 2015, § 13(c) ('UN GGE Report 2015')
- e.g., Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/68/98, 24 June 2013, § 19
- Martti Koskenniemi, UN Doc A/CN.4/L.682, 13 April 2006, § 120 (hereinafter 'Fragmentation Report'). See also Akande, Coco، and de Souza Dias, 'Old Habits Die Hard: Applying Existing International Law in Cyberspace and Beyond', *EJIL: Talk!* (5 January 2021), available at www.ejiltalk.org/old-habits-die-hard-applying-existing-international-law-in-cyberspace-and-beyond/.
- Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. GAOR, 17th sess., Agenda Item 93, U.N. Doc A/70/174 (July 22, 2015).
- OEWG, Second 'Pre-Draft' Report on Developments in the Field of Information and Telecommunications in the Context of International Security (2020), § 21, available at www.un.org/disarmament/openended-working-group/.
- Nuclear Weapons, Advisory Opinion, 8 July 1996, ICJ Reports (1996), para. 86
- The 2015 consensus report of the UN GGE show that states agreed that they 'should' exercise due diligence: UN A/70/174, para 13(c). See also 2013 report of the UN GGE, UN A/68/98

قائمة القضايا الدولية

- Corfu Channel (United Kingdom v. Albania), Judgment, 9 April 1949, ICJ Reports (1949) 4
- Case Concerning Pulp Mills on the River Uruguay (Argentina v. Uruguay), Judgment, 20 April 2010, ICJ Reports (2010)
- Corfu Channel Case (United Kingdom v. Albania), 1949. I.C.J. 244 (Dec.15). de Maizière, Thomas. 2014. 1
- Alabama Claims (United States v UK) (1872) 29 RIAA 125, at 127, 129, 131–132; Wipperman (United States v Venezuela) (1887), reprinted in J. Bassett Moore, History and Digest of the International Arbitrations to Which the United States Has Been a Party, vol. 3 (1898) 3039, at 3041
- (United States v Mexico) (1926) 4 RIAA 60, at 61–62.
- Island of Palmas (or Miangas) (theUnited States v Netherlands), 4 April 1928, II RIAA 829 (1928), ICGJ 392 (PCA 1928), at 839 (hereinafter 'Island of Palmas').
- Chayes, Abram. "Nicaragua, the United States, and the World Court." *Colum. L. Rev.* 85 (1985): 1445
- N. Sea Continental Shelf (F.R.G./Den. v. Neth.), 1969. I.C.J. 41, 72 (Feb. 20).
- *Nicaragua v. US*, 1986 I.C.J. Rep. 101 (1986)

الفهرس

(ISSN: 2356 - 9492)