

موقف القانون الدولي من الأمن السيبراني

م.م هدى حبيب كاظم

جامعة الكوت

The Position of International Law on Cybersecurity

LyI844878@gmail .com

المستخلص

أصبح الأمن السيبراني من الموضوعات الرئيسية التي تحظى باهتمام متزايد على المستوى الدولي نتيجة التطور التكنولوجي المتسارع واعتماد الدول والمؤسسات والأفراد على الأنظمة الرقمية في مختلف المجالات. وقد أدى هذا التطور إلى ظهور تحديات جديدة تمثلت في الجرائم الإلكترونية والهجمات السيبرانية التي تستهدف البنى التحتية الحيوية والأنظمة الحكومية والاقتصادية. ويهدف هذا البحث إلى دراسة موقف القانون الدولي من الأمن السيبراني من خلال بيان مفهوم الأمن السيبراني وأبعاده القانونية، وتحليل مدى انطباق قواعد القانون الدولي التقليدية على الفضاء السيبراني، فضلاً عن دراسة المسؤولية الدولية الناشئة عن الهجمات الإلكترونية والجهود الدولية الرامية إلى تنظيم هذا المجال. كما يسلط البحث الضوء على التحديات القانونية التي تواجه المجتمع الدولي في سبيل تحقيق أمن سيبراني عالمي فعال.

الكلمات المفتاحية: الأمن السيبراني، القانون الدولي، الهجمات الإلكترونية، الجرائم الإلكترونية، المسؤولية الدولية.

Abstract

Cybersecurity has become one of the most important issues receiving increasing attention at the international level due to rapid technological development and the growing reliance on digital systems in various sectors. This development has led to the emergence of new challenges represented by cybercrimes and cyberattacks targeting critical infrastructure, governmental institutions, and economic systems. This research aims to examine the position of international law on cybersecurity by clarifying the concept of cybersecurity and its legal dimensions, analyzing the applicability of traditional international law rules to cyberspace, and studying international responsibility arising from cyberattacks. The research also highlights international efforts to regulate cyberspace and the legal challenges facing the international community in achieving effective global cybersecurity.

Keywords: Cybersecurity, International Law, Cyberattacks, Cybercrime, International Responsibility.

المقدمة

شهد العالم خلال العقود الأخيرة تطوراً هائلاً في مجال تكنولوجيا المعلومات والاتصالات، الأمر الذي أدى إلى توسع استخدام الوسائل الرقمية في مختلف جوانب الحياة السياسية والاقتصادية والاجتماعية والعسكرية. وقد نتج عن هذا التطور ظهور الفضاء السيبراني بوصفه مجالاً جديداً للتفاعل بين الدول والأفراد والمؤسسات، مما أوجد تحديات قانونية وأمنية غير مسبقة تتطلب استجابة قانونية دولية فعالة. (محمد المجنوب، ص ٨٥). ومع ازدياد الاعتماد على الأنظمة الرقمية أصبحت الهجمات الإلكترونية تشكل تهديداً مباشراً للأمن الوطني للدول، حيث يمكن أن تستهدف المنشآت الحيوية والبنى التحتية الحساسة مثل شبكات الطاقة والمياه والمصارف وأنظمة الاتصالات. كما أن الطبيعة العابرة للحدود للفضاء السيبراني تجعل من الصعب تحديد الجهة المسؤولة عن هذه الهجمات، الأمر الذي يثير العديد من الإشكالات القانونية المتعلقة بالمسؤولية الدولية وسبل المساءلة. (عبد الفتاح بيومي حجازي، ص ٤٢). وتكمن أهمية هذا البحث في بيان موقف القانون الدولي من الأمن السيبراني وتوضيح مدى قدرة القواعد القانونية الدولية الحالية على مواجهة التهديدات الإلكترونية الحديثة، فضلاً عن دراسة الجهود الدولية الرامية إلى وضع إطار قانوني ينظم استخدام الفضاء السيبراني ويعزز الأمن والاستقرار الدوليين. (Malcolm N. Shaw، ص ٢٤٥).

المبحث الأول ماهية الأمن السيبراني والإطار القانوني له

المطلب الأول مفهوم الأمن السيبراني وأهميته

أولاً: تعريف الأمن السيبراني

يقصد بالأمن السيبراني مجموعة التدابير والإجراءات التقنية والقانونية والتنظيمية التي تهدف إلى حماية الأنظمة المعلوماتية والشبكات الإلكترونية والبيانات الرقمية من الاختراق أو التعطيل أو التلاعب أو الاستخدام غير المشروع. كما يشمل حماية سرية المعلومات وسلامتها وضمان استمرارية الخدمات الرقمية في مواجهة المخاطر والتهديدات الإلكترونية المختلفة. (عبد الفتاح بيومي حجازي، ص ٣١) ويعد الأمن السيبراني من المفاهيم الحديثة التي ارتبطت بالتطور المتسارع في تكنولوجيا المعلومات والاتصالات، إذ لم يعد يقتصر على حماية الأجهزة والبرمجيات فحسب، بل امتد ليشمل حماية الأمن الوطني والاقتصاد الوطني والمصالح الاستراتيجية للدول. وقد أصبح الفضاء السيبراني أحد المجالات الحيوية التي تتطلب حماية مستمرة بسبب تزايد الاعتماد العالمي على التكنولوجيا الرقمية. (أحمد إبراهيم الشريف، ص ٥٤).

ثانياً: أهمية الأمن السيبراني

تتبع أهمية الأمن السيبراني من الدور المحوري الذي يؤديه في حماية البنية التحتية الرقمية التي تعتمد عليها المؤسسات الحكومية والخاصة في إدارة أعمالها اليومية. فالهجمات الإلكترونية قد تؤدي إلى خسائر اقتصادية جسيمة وتعطيل الخدمات الأساسية وإفشاء المعلومات السرية، مما ينعكس سلباً على استقرار الدولة وأمنها القومي. (عبد الفتاح بيومي حجازي، ص ٥٨) كما يسهم الأمن السيبراني في تعزيز الثقة بالتعاملات الإلكترونية والتجارة الرقمية والخدمات الحكومية الإلكترونية، حيث يشعر الأفراد والمؤسسات بالأمان عند استخدام التقنيات الحديثة في ظل وجود أنظمة حماية فعالة. ولذلك أصبح الأمن السيبراني عنصراً أساسياً من عناصر التنمية المستدامة والتحول الرقمي في مختلف دول العالم. (أحمد إبراهيم الشريف، ص ٦١).

المطلب الثاني الإطار القانوني الدولي للأمن السيبراني

أولاً: مفهوم القانون الدولي السيبراني

يشير القانون الدولي السيبراني إلى مجموعة القواعد والمبادئ القانونية التي تنظم سلوك الدول والجهات الفاعلة الأخرى في الفضاء الإلكتروني. ويستند هذا القانون إلى قواعد القانون الدولي العام التقليدية، بما في ذلك مبادئ السيادة وعدم التدخل في الشؤون الداخلية للدول وحظر استخدام القوة وتسوية المنازعات بالطرق السلمية، مع مراعاة خصوصية البيئة الرقمية وطبيعة الفضاء السيبراني. (Malcolm N. Shaw، ص ٢٥١). وقد أدى التوسع في استخدام التكنولوجيا الرقمية إلى ظهور اتجاهات فقهية تدعو إلى تطوير قواعد قانونية دولية جديدة تتلاءم مع طبيعة التهديدات السيبرانية، نظراً لأن بعض القواعد التقليدية لم تعد كافية لمعالجة المشكلات الناشئة عن الجرائم والهجمات الإلكترونية العابرة للحدود. (Duncan Hollis، ص ٥٨).

ثانياً: تطور الاهتمام الدولي بالأمن السيبراني

بدأ الاهتمام الدولي بالأمن السيبراني بصورة واضحة مع تزايد الهجمات الإلكترونية التي استهدفت المؤسسات الحكومية والبنى التحتية الحيوية في العديد من الدول. وقد دفعت هذه التطورات المجتمع الدولي إلى البحث عن آليات قانونية وتنظيمية للحد من المخاطر الناجمة عن استخدام التكنولوجيا الرقمية بصورة غير مشروعة. (United Nations Report، ص ١٧) كما عملت الأمم المتحدة والمنظمات الدولية المتخصصة على عقد المؤتمرات والندوات وتشكيل لجان الخبراء لمناقشة سبل تعزيز الأمن السيبراني ووضع مبادئ توجيهية لاستخدام تكنولوجيا المعلومات والاتصالات بما يحقق الأمن والاستقرار الدوليين. (United Nations Report، ص ٢٠).

المبحث الثاني موقف القانون الدولي من الهجمات السيبرانية

المطلب الأول تكييف الهجمات السيبرانية في القانون الدولي

أولاً: الهجمات السيبرانية واستخدام القوة

أثارت الهجمات الإلكترونية تساؤلات قانونية عديدة حول إمكانية اعتبارها شكلاً من أشكال استخدام القوة المحظور بموجب ميثاق الأمم المتحدة. ويرى جانب من الفقه الدولي أن الهجمات السيبرانية التي تؤدي إلى أضرار مادية جسيمة أو خسائر بشرية يمكن أن تندرج ضمن مفهوم استخدام القوة إذا كانت نتائجها مماثلة للنتائج التي تترتب على الهجمات العسكرية التقليدية. (Michael N. Schmitt، ص ٣٤١) ومن الأمثلة على ذلك

الهجمات الإلكترونية التي تستهدف شبكات الطاقة أو أنظمة الدفاع الجوي أو المنشآت النووية، حيث يمكن أن تؤدي إلى تعطيل خدمات أساسية أو إحداث أضرار واسعة النطاق تهدد أمن الدولة واستقرارها. (Michael N. Schmitt ص ٣٥٢).

ثانياً: حق الدفاع الشرعي ضد الهجمات السيبرانية

يعترف القانون الدولي بحق الدول في الدفاع الشرعي عن النفس عند تعرضها لهجوم مسلح وفقاً للمادة (٥١) من ميثاق الأمم المتحدة. وقد ثار جدل فقهي حول مدى إمكانية تطبيق هذا الحق على الهجمات السيبرانية، خاصة إذا كانت هذه الهجمات تؤدي إلى نتائج خطيرة تماثل نتائج الهجمات العسكرية التقليدية. (Yoram Dinstein ص ٢٨٦) ويرى العديد من الباحثين أن الدولة المتضررة من هجوم إلكتروني واسع النطاق يمكنها ممارسة حق الدفاع الشرعي إذا ثبت أن الهجوم بلغ مستوى الهجوم المسلح وألحق ضرراً جسيماً بأمنها الوطني أو بمرافقها الحيوية. (Yoram Dinstein ص ٢٩٤).

المطلب الثاني المسؤولية الدولية عن الهجمات السيبرانية

أولاً: أساس المسؤولية الدولية

تقوم المسؤولية الدولية للدولة عندما ترتكب فعلاً غير مشروع دولياً يترتب عليه ضرر يصيب دولة أخرى أو المجتمع الدولي. وينطبق هذا المبدأ على الأنشطة السيبرانية إذا ثبت أن الهجوم الإلكتروني قد نُفذ بواسطة أجهزة الدولة أو تحت إشرافها أو بدعم منها. (James Crawford ص ١٠٢) ويستلزم قيام المسؤولية الدولية توافر عنصرين أساسيين، يتمثل الأول في مخالفة قاعدة من قواعد القانون الدولي، بينما يتمثل الثاني في إمكانية إسناد الفعل إلى الدولة وفقاً لقواعد المسؤولية الدولية المعترف بها. (James Crawford ص ١١٠).

ثانياً: صعوبة إسناد الهجمات الإلكترونية

تُعد مسألة الإسناد من أكثر المسائل تعقيداً في مجال الأمن السيبراني، إذ غالباً ما يلجأ منفذو الهجمات الإلكترونية إلى إخفاء هوياتهم الحقيقية أو استخدام خوادم موجودة في دول مختلفة لإخفاء مصدر الهجوم. (Marco Roscini ص ١٧٦). ويؤدي هذا الوضع إلى صعوبة تحديد الجهة المسؤولة عن الهجوم بصورة دقيقة، الأمر الذي يعرقل تطبيق قواعد المسؤولية الدولية ويجعل من الصعب اتخاذ إجراءات قانونية أو دبلوماسية ضد الدولة المسؤولة. (Marco Roscini ص ١٨٢).

ثالثاً: مسؤولية الأفراد والجماعات الإلكترونية

لا تقتصر المسؤولية عن الجرائم السيبرانية على الدول فقط، بل يمكن أن تمتد إلى الأفراد والجماعات المنظمة التي تنفذ هجمات إلكترونية تستهدف الأنظمة والمعلومات الرقمية. وقد عملت العديد من الاتفاقيات الدولية على تعزيز التعاون القضائي بين الدول لملاحقة مرتكبي الجرائم الإلكترونية وتسليمهم ومحاكمتهم. (Budapest Convention ص ٣٤). كما أصبح التعاون الدولي ضرورة ملحة لمواجهة الجماعات الإجرامية التي تستغل الفضاء السيبراني في تنفيذ عمليات الاختتيال الإلكتروني وسرقة البيانات ونشر البرمجيات الخبيثة التي تهدد الأمن الرقمي العالمي (Budapest Convention ص ٤١).

المبحث الثالث التحديات الدولية والجهود الدولية في مجال الأمن السيبراني

المطلب الأول التحديات القانونية والتنظيمية للأمن السيبراني

أولاً: غياب تعريف دولي موحد للهجمات السيبرانية

يُعد غياب تعريف دولي موحد ودقيق لمفهوم الهجمات السيبرانية من أبرز التحديات التي تواجه المجتمع الدولي، إذ تختلف وجهات نظر الدول حول تحديد ما إذا كان الفعل الإلكتروني يشكل "هجوماً مسلحاً" أو مجرد نشاط غير مشروع. هذا الاختلاف يؤدي إلى صعوبة تطبيق قواعد القانون الدولي بشكل موحد على الفضاء السيبراني. (Marco Roscini ص ١٩٠) كما أن بعض الدول تعتمد تعريفات وطنية خاصة بها للأمن السيبراني، مما يخلق تبايناً في المعايير القانونية ويؤثر على التعاون الدولي في مواجهة التهديدات الإلكترونية. (Duncan Hollis ص ٦٦).

ثانياً: الطبيعة العابرة للحدود للفضاء السيبراني

تتميز الهجمات السيبرانية بأنها عابرة للحدود، حيث يمكن تنفيذ الهجوم من دولة معينة واستهداف دولة أخرى عبر خوادم وسيطة متعددة، مما يجعل من الصعب تحديد مكان وقوع الفعل غير المشروع أو الجهة الفاعلة الحقيقية. (Michael N. Schmitt ص ٣٦٠) هذا الواقع يضعف من قدرة القواعد التقليدية في القانون الدولي على ضبط السلوك في الفضاء السيبراني، ويجعل مسألة الاختصاص القضائي أكثر تعقيداً. (James Crawford ص ١١٨).

ثالثاً: ضعف آليات الإسناد القانوني

تُعد مشكلة إسناد الهجمات الإلكترونية إلى دولة معينة من أبرز التحديات، إذ تعتمد عملية الإسناد على أدلة تقنية معقدة قد لا تكون كافية من الناحية القانونية لإثبات مسؤولية الدولة. (Marco Roscini، ص١٨٥) كما أن الفاعلين في الفضاء السيبراني يستخدمون تقنيات إخفاء الهوية مثل الشبكات المظلمة (Dark Web) والبروكسيات، مما يزيد من صعوبة التتبع القانوني. (United Nations Report، ص٢٨).

المطلب الثاني الجهود الدولية لتنظيم الأمن السيبراني

أولاً: دور منظمة الأمم المتحدة

تعد الأمم المتحدة من أبرز الجهات الدولية التي أولت اهتماماً متزايداً بالأمن السيبراني، حيث تم إنشاء مجموعات خبراء حكوميين (GGE) لدراسة سبل تعزيز سلوك الدول المسؤول في الفضاء السيبراني. (United Nations Report، ص٣١) وقد أكدت هذه التقارير على ضرورة احترام مبادئ القانون الدولي، بما في ذلك سيادة الدول وعدم التدخل في شؤونها الداخلية عند استخدام تكنولوجيا المعلومات. (United Nations Report، ص٣٣).

ثانياً: الاتفاقيات الدولية والتعاون القضائي

من أهم الجهود الدولية في هذا المجال اتفاقية بودابست لمكافحة الجرائم السيبرانية، التي تُعد أول إطار قانوني دولي ملزم نسبياً لتنظيم الجرائم الإلكترونية وتعزيز التعاون بين الدول في التحقيق والملاحقة القضائية. (Budapest Convention، ص٥٢) وتشجع هذه الاتفاقية على تبادل المعلومات بين الدول وتسليم المجرمين وتوحيد الإجراءات القانونية لمكافحة الجرائم الإلكترونية. (Budapest Convention، ص٥٨).

ثالثاً: التعاون الإقليمي والدولي

بالإضافة إلى الجهود الأممية، ظهرت مبادرات إقليمية لتعزيز الأمن السيبراني مثل الاتحاد الأوروبي ومنظمة التعاون الاقتصادي، والتي وضعت استراتيجيات مشتركة لتعزيز حماية البنى التحتية الرقمية. (Malcolm N. Shaw، ص٢٦٨) كما بدأت بعض الدول في إنشاء مراكز وطنية للأمن السيبراني لتعزيز التعاون الدولي في تبادل المعلومات حول التهديدات والهجمات الإلكترونية. (Duncan Hollis، ص٧٤).

الذاتة

في ختام هذا البحث يتضح أن الأمن السيبراني أصبح من القضايا الجوهرية في القانون الدولي المعاصر، نظراً لارتباطه الوثيق بالأمن الوطني والدولي على حد سواء. وقد أظهرت الدراسة أن القواعد التقليدية للقانون الدولي ما زالت قاصرة إلى حد ما عن مواكبة التطور السريع في الفضاء السيبراني، خاصة فيما يتعلق بتحديد المسؤولية الدولية وإسناد الهجمات الإلكترونية. كما تبين أن المجتمع الدولي بدأ فعلياً في اتخاذ خطوات مهمة نحو تنظيم هذا المجال من خلال الأمم المتحدة والاتفاقيات الدولية مثل اتفاقية بودابست، إلا أن هذه الجهود لا تزال بحاجة إلى تطوير إطار قانوني دولي أكثر شمولاً وملاءمة لطبيعة التهديدات السيبرانية المتجددة.

التوصيات

- ضرورة وضع تعريف دولي موحد للهجمات السيبرانية ضمن إطار الأمم المتحدة.
- تطوير قواعد القانون الدولي بما يتلاءم مع طبيعة الفضاء السيبراني.
- تعزيز التعاون الدولي في مجال تبادل المعلومات الاستخبارية السيبرانية.
- دعم بناء قدرات الدول النامية في مجال الأمن السيبراني.
- تشديد العقوبات الدولية على مرتكبي الجرائم الإلكترونية.

المصادر والمراجع

- عبد الفتاح بيومي حجازي، الأمن المعلوماتي والقانون السيبراني، ص ٣١-٥٨.
- أحمد إبراهيم الشريف، الأمن السيبراني والتحول الرقمي، ص ٥٤-٦١.
- محمد المجذوب، القانون الدولي العام، ص ٨٥.

- Malcolm N. Shaw, International Law, p. ٢٦٨-٢٤٥
- James Crawford, State Responsibility in International Law, p. ١١٨-١٠٢
- Marco Roscini, Cyber Operations and the Use of Force in International Law, p. ١٩٠-١٧٦
- Michael N. Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare, p. ٣٦٠-٣٤١

- Yoram Dinstein, War, Aggression and Self-Defence, p..٢٩٤-٢٨٦
- Duncan Hollis, Cyberwar, Cyberterrorism and Cybercrime, p..٧٤-٥٨
- United Nations Report on Cybersecurity, p..٣٣-١٧
- Budapest Convention on Cybercrime, p..٥٨-٣٤