Journal Of the Iraqia University (74-9) January (2026)

ISSN(Print): 1813-4521 OnIine ISSN:2663-7502
Journal Of the Iraqia University
available online at: https://www.mabdaa.edu.iq

العقوبات الدولية على الهجمات السيبرانية الإطار القانوني والتحديات والفعالية

المشرف الأستاذ الدكتور مصطفى فضائلي /كلية القانون / جامعة قم

حسن سامي نور المحنا / كلية القانون / جامعة قم

International sanctions on cyberattacks: legal framework, challenges, and effectiveness

supervior: Dr.Mostaf Fazaeli
fazaeli2007@gmail.com
University : Qom University - College of Law
Rescarcher: Hasan Sami Noor Al-Mohana
hasan.iraq7777@gmail.com

هناك من يعرف العقوبات السيبرانية بأنها تشير إلى تبني قيود اقتصادية أحادية الجانب يتم فرضها وفقًا للقوانين المحلية للدولة، وتهدف إلى ردع ومعاقبة الجهات الفاعلة المسئولية عن السلوك الخبيث القائم على الإنترنت.وهذه العقوبات قد تفرض بشكل مؤقت أو دائم وتأخذ أنماطا عدة، منها تجميد الأصول وفرض قيود على العلاقات الاقتصادية مع الأشخاص أو الكيانات الخاضعة للعقوبات إلى جانب حظر السفر على الأفراد وغيرها من التدابير المضادة، مثر فرض الغرامات المالية، أو منع تصدير أو استيراد سلعة أو تقنيات مرتبطة، بينما تشير العقوبات السيبرانية إلى فرض العزلة الرقمية القسرية ليس على الدولة المستهدفة ففقط، بل كذلك على الأفراد والشركاء التجاريين من الخارج، سواء كانت شركات أو دول أخرى، والتهديد برفض العقوبات في الة اختراق الحظر، أو عدم الالتزام بلائحة العقوبات المعلنة من قبل دولة أو أكثر [1]واستقت العقوبات السيبرانية Cyber Sanctions بعضا من خصائصها من التعريف التقليدي للعقوبات الدولية، ولكن أصبحمجال تطبيقها ومدى تأثيرها مختلفا، إن العقوبات السيبرانية كغيرها من العقوبات الدولية لا تتطلب إعلان المسئولية عن الإجراء المستلزم للعقوبات، ومن ثم تبتعد عن الطبيعة القانونية لما إلى الطابع السياسي، خاصة إذا تمت من قبل أطراف دولية خارج نظام الأمم المتحدة.وتحد العقوبات السيبرانية من فرص التعاون الدولي في مجال المعرفة والتقنية، وهو ما يعني أن فرضها يحمل تأثيرات سلبية على تقدم الحضارة الإنسانيةوعليه تم تقسيم الفصل الى المبحث الأول لبيان الأنظمة القانونية الدولية الحالية للعقوبات، والمبحث الثاني لبيان فعالية العقوبات الدولية في مكافحة الهجمات السيبرانية

المبحث الأول: الأنظمة القانونية الدولية الحالية للعقوبات

يختلف تأثير فرض العقوبات السيبرانية عن تأثيرات الفجوة الرقمية Digital Divide التي تتعلق بالفجوة بين الذين بمقدورهم استخدام الإنترنت بسبب امتلاكهم المهارة اللازمة والقدرة المادية والذين لا يستطيعون، ويكون ذلك غير مقصود لكنه قد يحمل دلالات سياسية وتنموية كحالة منع الدول الكبرى تصدير التكنولوجيا المتقدمة إلى الدول النامية بما تسبب في وجود فجوة رقمية وتكنولوجية ترتبط في جزء منها بالورث الاستعماري الغربي.وهناك فجوة رقمية غير متعمدة بين الريف والحضر داخل الدولة لكنها قد ترجع لأسباب جغرافية أو اقتصادية، وذلك كأثر التعليم ومستوى الدخل على حجم التفاوت بين مواطني الدولة في الحصول على خدمات الإنترنت أو الهواتف الذكية.[2]وعليه تم تقسيم المبحث الى المطلب الأول لبيان العقوبات المستهدفة للهجمات السيبرانية، والمطلب الثاني لبيان التحديات في فرض العقوبات على الهجمات السيبرانية

المطلب الأول: العقوبات المستهدفة للهجمات السيبرانية

تتميز العقوبات السيبرانية بطبيعة متداخلة من التأثير الاقتصادي أو العسكري أو الدبلوماسي وغيره من الأبعاد المرتبطة بالنشاط السيبراني وعلاقته بتلبية الاحتياجات الإنسانية، وهو الأمر الذي أحدث تأثيرات عميقة تتجاوز التأثير التقليدي لباقي أنماط العقوبات الدولية الأخرى، وذلك بالنظر

إلى مداها وانتشارها والخسائر المتوقعة منها، وتأثيرها العابر للحدود، وإمكانية إصابة أطراف ثالثة ليست معنية أو طرفا في الصراع المباشر مع الدولة التي فرضت تلك العقوبات السيبرانية.[٣]وأصبح لعزل الدولة كليا أو جزئيًا عن المجال السيبراني بشكل قسري تأثيرات متعددة على السكان المدنين الأبرياء، ويتم فرضها من قبل دولة أو أكثر، ويكون للشركات التقنية العابرة دور فيها، ويكون لها تأثير عميق بشكل مباشر وغير مباشر في كافة القطاعات داخل الدولة، بما في ذلك المنشآت المدنية والخدمات المقدمة إلى المدنيين، إلى جانب التأثير في الجهات الرسمية داخل الدولة.ويتوقف نجاح العقوبات السيبرانية وتقييم أثرها على الجهات التي تفرضها، سواء تمت تحت مظلة أممية أو سلوك أحادي من جانب الدولة، وانعكاس ذلك على المشروعية والاعتراف الدولي بها، وعلى امتلاك تلك الدول نظام للعقوبات يتميز بالمراجعة والفاعلية.

البند الأول: العقوبات الماليةفي عالم اليوم الذي أصبح مترابطاً بشكل غير مسبوق عبر الشبكات الرقمية، أصبحت الهجمات السيبرانية أحد أبرز التهديدات الأمنية العالمية، حيث تتجاوز تأثيراتها الحدود الجغرافية وتؤثر على الاقتصادات والأنظمة الحكومية والمؤسسات الخاصة على حد سواء. وفي هذا السياق، برزت العقوبات المالية كأداة دولية مستهدفة لمواجهة هذه الهجمات، حيث تُعتبر شكلاً من أشكال الرد غير العسكري الذي يهدف إلى عزل الجهات المسؤولة مالياً وتقييد قدراتها على التمويل والتوسع، دون الحاجة إلى تدخل عسكري مباشر. العقوبات المالية المستهدفة، المعروفة أيضاً باسم "العقوبات الذكية" أو "القيود المالية الدقيقة"، تركز على تجميد الأصول، حظر السفر، ومنع التعاملات المالية مع أفراد أو كيانات محددة، مما يجعلها أداة فعالة للرد على النشاط السيبراني الضار الذي غالباً ما يكون مدعوماً من قبل دول أو مجموعات إجرامية. هذه العقوبات ليست جديدة في السياسة الدولية، إذ استخدمت تاريخياً ضد الإرهاب والانتشار النووي، لكن تطبيقها على الهجمات السيبرانية يمثل تطوراً حديثاً يعكس الطبيعة المتغيرة للتهديدات في عصر الرقمنة.[٤]على سبيل المثال، في عام ٢٠١٥، أصدرت الولايات المتحدة أول أمر تنفيذي يستهدف النشاط السيبراني الضار، مما مهد الطريق لسلسلة من الإجراءات الدولية التي ساهمت في تشكيل إطار قانوني عالمي لمواجهة هذه التهديدات. ومع تزايد تعقيد الهجمات، مثل هجوم WannaCry في ٢٠١٧ الذي أصاب مئات الآلاف من الأجهزة في أكثر من ١٥٠ دولة، أصبحت هذه العقوبات ضرورة استراتيجية للحفاظ على الاستقرار الدولي، حيث تُظهر الدراسات أن الخسائر الاقتصادية الناتجة عن الهجمات السيبرانية قد تصل إلى تريليونات الدولارات سنوياً بحلول نهاية العقد الحالي[5].يبدأ تاريخ استخدام العقوبات المالية المستهدفة ضد الهجمات السيبرانية في الولايات المتحدة، حيث أصدر الرئيس باراك أوباما في ١ أبريل ٢٠١٥ الأمر التنفيذي رقم ١٣٦٩٤، الذي أعلن حالة طوارئ وطنية بسبب "التهديد غير العادي والاستثنائي" الناتج عن النشاط السيبراني الضار الذي ينشأ من خارج الولايات المتحدة أو يُدير من قبل أشخاص خارجها. كان هذا الأمر يسمح بفرض عقوبات على الأفراد والكيانات المسؤولة عن أو متورطة في أنشطة سيبرانية تهدد الأمن القومي أو الاقتصاد الأمريكي، مثل سرقة الأسرار التجارية أو التجسس الرقمي وفي ديسمبر ٢٠١٦، عدل الرئيس دونالد ترامب هذا الأمر بموجب الأمر التنفيذي ١٣٧٥٧، ليوسع نطاقه ليشمل أي نشاط يهدف إلى التأثير على الانتخابات أو البنية التحتية الحرجة. ثم جاء الأمر ١٣٨٤٨ في سبتمبر ٢٠١٨، الذي ركز تحديداً على التدخل في الانتخابات الأمريكية عبر الهجمات السيبرانية، مما أدى إلى فرض عقوبات على أكثر من ٣٠٠ فرد وكيان بحلول عام ٢٠٢١، وفقاً لتقارير المعهد الوطني للعلاقات الخارجية. هذه الإجراءات الأمريكية كانت الأولى من نوعها على المستوى الدولي، وألهمت دولاً أخرى لتبني نماذج مشابهة، حيث أظهرت فعاليتها في حالات مثل هجوم Sony Pictures في ٢٠١٤، الذي نسبت إليه كوريا الشمالية، مما أدى إلى عقوبات مالية على كيانات كورية شمالية مرتبطة بالهجوم. ومع ذلك، لم تكن هذه العقوبات خالية من التحديات، إذ تعتمد على عملية الإسناد (attribution) التي غالباً ما تكون معقدة فنياً وقانونياً، حيث يصعب إثبات الروابط بين المهاجمين والدول الداعمة دون كشف مصادر الاستخبارات[6].في أوروبا، تبنت الاتحاد الأوروبي نهجاً جماعياً أكثر، حيث أقر في مايو ٢٠١٩ نظاماً للعقوبات السيبرانية الأفقي (horizontal cyber sanctions regime)بموجب اللائحة 2019/796 (EU) وقرار 2019/797 (CFSP) ، وهو يسمح بفرض قيود مالية وتجميد أصول وحظر سفر على الأفراد والكيانات المسؤولة عن هجمات سيبرانية تستهدف الاتحاد أو دوله الأعضاء أو منظمات دولية[٧]. كان هذا النظام رد فعل على سلسلة من الهجمات، مثل محاولة اختراق منظمة حظر الأسلحة الكيميائية (OPCW) في ٢٠١٨، والتي نسبت إلى وحدة ٢٩١٥٥ التابعة للاستخبارات الروسية .(GRU) بحلول يناير ٢٠٢٥، أضاف الاتحاد ثلاثة أفراد روس إلى قائمة العقوبات بسبب هجمات على إستونيا في ٢٠٢٠، حيث سرقوا آلاف الوثائق السرية من وزارات الاقتصاد والشؤون الاجتماعية، مما يرفع إجمالي المدرجين إلى ١٧ فرداً و٤ كيانات. كما أضاف ستة أشخاص في يونيو ٢٠٢٤ بسبب هجمات على أوكرانيا ودول أوروبية أخرى، بما في ذلك هجوم NotPetya في ٢٠١٧ الذي تسبب في خسائر تصل إلى ١٠ مليارات دولار عالمياً، وهو هجوم مدمر استخدم برمجيات خبيثة لتعطيل الأنظمة المالية والصحية. هذا النظام الأوروبي يتميز بتركيزه على غير الدول(non-state actors) ، لكنه يسمح باستهداف الوكلاء الحكوميين، ويعتمد على إطار الرد الدبلوماسي المشترك للاتحاد على النشاط

السيبراني الضار الذي أقر في ٢٠١٧. ومع ذلك، يواجه تحديات في عملية الإسناد، حيث تختلف قدرات الدول الأعضاء في التحقيق، مما يؤدي إلى تأخير في التنفيذ يصل إلى سنوات، كما حدث في حالة هجوم Bundestag الألماني في ٢٠١٥ الذي لم يُعاقب عليه إلا في ٢٠٢٠[8].أما المملكة المتحدة، فقد اعتمدت بعد بريكست نظاماً خاصاً بها في ٢٠٢٠ بموجب قوانين"Cyber (Sanctions) (EU Exit) Regulations" ، والتي تمنع النشاط السيبراني الذي يهدد السلامة أو الاقتصاد البريطاني، وتشمل فرض عقوبات على الجماعات الإجرامية مثل Evil Corp الروسية، التي تسببت في خسائر بملايين الدولارات من خلال برمجيات الفدية. في فبراير ٢٠٢٣، فرضت المملكة عقوبات مشتركة مع الولايات المتحدة وأستراليا على سبعة مجرمين روس مرتبطين بهذه الجماعة، مما يعكس التعاون الدولي المتزايد. وبالمثل، أعلنت أستراليا في ٢٠٢٣ عقوبات مالية ومنع سفر على ثلاثة روس منEvil Corp ، كجزء من إطارها السيبراني المستقل الذي استخدم للمرة الثالثة، بهدف حماية القطاعات الحرجة مثل الصحة والبنية التحتية. هذه الإجراءات الأسترالية تكمل جهودها في مكافحة الجرائم السيبرانية، حيث أنشأت خطاً ساخناً للإبلاغ عن الهجمات وتقدم نصائح لتجنب دفع الفديات.بالنسبة للأمم المتحدة، لا يوجد نظام عقوبات سيبرانية متخصص، لكن يمكن استخدام اللجان المعنية بالعقوبات الحالية، مثل تلك المتعلقة بكوريا الشمالية أو إيران، لاستهداف النشاط السيبراني.[9] على سبيل المثال، في ٢٠١٩، فرضت مكتب الرقابة على الأصول الأجنبية الأمريكي (OFAC) عقوبات على ثلاث مجموعات كورية شمالية مدعومة من الدولةLazarus Group :، Bluenoroff، وAndariel، التابعة لمكتب الاستطلاع العام .(RGB) كانت Lazarus مسؤولة عن WannaCry الذي أغلق ٣٠٠,٠٠٠ جهاز حول العالم وتسبب في خسائر تزيد عن ١١٢ مليون دولار في المملكة المتحدة وحدها، بالإضافة إلى هجوم Sony وسرقة ٨١ مليون دولار من بنك بنغلاديش في ٢٠١٦ عبر نظام .SWIFT أماBluenoroff ، فهي متخصصة في السرقات المالية، حيث حاولت سرقة ١.١ مليار دولار من بنوك في آسيا وأمريكا اللاتينية، بينما ركزت Andariel على سرقة بيانات البطاقات المصرفية والتجسس على الدفاع الكوري الجنوبي. هذه العقوبات تجمد الأصول وتمنع التعاملات، مما يعيق تمويل البرامج النووية الكورية الشمالية عبر الجرائم السيبرانية[10].

فيما يتعلق بالصين، شهدت السنوات الأخيرة تصعيداً في العقوبات بسبب هجمات نسبت إلى مجموعات مدعومة من الحكومة، مثل Operation Cloud Hopperفي ٢٠١٦، الذي استهدف شركات عالمية مثل IBM و HPلسرقة أسرار تجارية، مما أدى إلى عقوبات أوروبية على اثنين من الصينيين Gao Qiang وZhang Shilong، بالإضافة إلى شركة .Huaying Haitai كما اتهمت وزارة العدل الأمريكية في مارس ٢٠٢٥ اثني عشر هاكر صينياً وعناصر أمنية باختراقات عالمية، بما في ذلك سرقة بيانات من الولايات المتحدة، مما أدى إلى عقوبات مالية. وفي يناير ٢٠٢٥، فرضت الخزانة الأمريكية عقوبات على شركة Integrity Technology Group الصينية لدعم مجموعةFlax Typhoon ، التي اخترقت بنى تحتية أمريكية منذ ٢٠٢١، مستهدفة القطاعات الحيوية في أمريكا الشمالية وأوروبا وآسيا، خاصة تايوان[11].أما الجماعات الإجرامية غير المدعومة من الدول، مثل تلك المسؤولة عن برمجيات الفدية، فقد أصبحت هدفاً رئيسياً للعقوبات، كما في حالة Evil Corp التي ذكرت سابقاً، والتي سرقت ملايين من المؤسسات المالية الأمريكية والأوروبية منذ ٢٠١٣. في ديسمبر ٢٠١٩، فرضت الخزانة الأمريكية عقوبات على هذه الجماعة الروسية لاستخدام برمجية Dridex الضارة، التي تسببت في ملايين الدولارات من الخسائر. كذلك، في فبراير ٢٠٢٣، تعاونت الولايات المتحدة والمملكة المتحدة وأستراليا لعقاب سبعة أعضاء من جماعةransomware ، مما أدى إلى تجميد أصول ومنع سفر، وهو جزء من حملة أوسع ضد الجرائم السيبرانية التي تستهدف القطاع المالي، حيث سجلت حوادث مثل هجوم Carbanak الذي سرق مليار دولار من البنوك بين ٢٠١٣ و٢٠١٨[12].رغم فعاليتها الظاهرية، تواجه هذه العقوبات تحديات جوهرية، أبرزها عملية الإسناد، التي تتطلب دليلاً فنياً قوياً لربط الهجوم بالمستهدف، وغالباً ما تتأخر بسبب الحاجة إلى مشاركة الاستخبارات مع حلفاء مثل تحالف Five Eyes (الولايات المتحدة، المملكة المتحدة، كندا، أستراليا، نيوزيلندا). في الاتحاد الأوروبي، يؤدي الإجماع بين ٢٧ دولة إلى بطء في التنفيذ، كما في حالة NotPetya حيث استغرق الأمر ثلاث سنوات للعقاب، مما يقلل من التأثير الرادع. كما أن الفعالية محدودة في حالات الدول المعزولة مثل كوريا الشمالية، حيث تعتمد على الاقتصاد غير الرسمي والعملات الرقمية للالتفاف، وفقاً لتقارير مركز الدراسات الاستراتيجية والدولية .(CSIS) ومع ذلك، أظهرت الدراسات أن هذه العقوبات نجحت في ٣٠٪ من الحالات في تغيير السلوكيات، خاصة عندما تكون مستهدفة ومتعددة الأطراف، كما في حملات ضد روسيا بعد هجوم SolarWinds في ٢٠٢٠، الذي اخترق آلاف الشبكات الحكومية الأمريكية، مما أدى إلى عقوبات مشتركة أدت إلى تعزيز الدفاعات السيبرانية العالمية[13].يبرز التعاون الدولي كعامل رئيسي في تعزيز فعالية هذه العقوبات، حيث أنشأت الولايات المتحدة وأوروبا آليات للتنسيق مثل وحدة الاتحاد الأوروبي المشتركة للسيبران(EU Joint Cyber Unit) ، التي تعمل على تبادل المعلومات وتنسيق الردود. كما ساهمت منظمة الناتو في تعزيز الردود الجماعية، خاصة بعد إعلان الهجمات السيبرانية كتهديد أمني في قمة وارسو ٢٠١٦. وفي السياق المالي،

ساعدت منظمة التعاون الاقتصادي والتنمية (OECD) في وضع معايير لمكافحة غسيل الأموال الناتج عن الجرائم السيبرانية، مما يدعم تنفيذ العقوبات. ومع ذلك، يظل التحدي في توسيع هذا التعاون إلى دول نامية، حيث تفتقر إلى القدرات الفنية، مما يجعلها عرضة للهجمات دون قدرة على الرد حيث تمثل العقوبات المالية المستهدفة أداة حيوية في ترسانة الرد الدولي على الهجمات السيبرانية، حيث توازن بين الفعالية الاقتصادية والحد من التصعيد العسكري، لكن نجاحها يعتمد على تحسين الإسناد والتنسيق الدولي. مع تزايد التهديدات، مثل استخدام الذكاء الاصطناعي في الهجمات، يجب على المجتمع الدولي تعزيز هذه الأطر لضمان فضاء سيبراني آمن، حيث أن الفشل في ذلك قد يؤدي إلى اضطرابات اقتصادية عالمية غير مسبوقة[14].**البند الثاني: العقوبات غير المالية**في عصرنا الرقمي الذي يشهد تكاملاً متزايداً بين الأنظمة الإلكترونية والحياة اليومية، أصبحت الهجمات السيبرانية تهديداً عابرًا للحدود يهز أركان الاقتصادات والأمن القومي والاستقرار الدولي، مما دفع المجتمع الدولي إلى ابتكار أدوات رد غير تقليدية لمواجهتها. من بين هذه الأدوات، تبرز العقوبات غير المالية كوسيلة مستهدفة للرد على الجهات المسؤولة عن هذه الهجمات، حيث تركز على تقييد الحركة، منع نقل التكنولوجيا، والعزل الدبلوماسي، دون اللجوء إلى الإجراءات الاقتصادية الشاملة التي قد تؤثر على السكان العاديين. هذه العقوبات، المعروفة أيضاً باسم "العقوبات الذكية غير المالية"، تهدف إلى عزل المعتدين فردياً أو جماعياً، مما يحد من قدرتهم على التخطيط أو التنفيذ المستقبلي، وتعزيز الردع الدولي ضد النشاط السيبراني الضار الذي غالباً ما يكون مدعوماً من قبل دول أو مجموعات غير حكومية. على سبيل المثال، في السنوات الأخيرة، شهد العالم سلسلة من الهجمات السيبرانية المدعومة من دول مثل روسيا والصين وكوريا الشمالية، مثل هجوم SolarWinds الذي أثر على آلاف الشبكات الحكومية الأمريكية في ٢٠٢٠، أو هجوم NotPetya في ٢٠١٧ الذي أدى إلى خسائر اقتصادية هائلة، مما أدى إلى فرض عقوبات غير مالية لمنع تكرار مثل هذه الانتهاكات. [١٥]هذه الإجراءات ليست مجرد رد فعل، بل جزء من استراتيجية أوسع للحفاظ على الفضاء السيبراني كبيئة آمنة، حيث تظهر التقارير أن الهجمات السيبرانية قد تكلف العالم أكثر من ١٠ تريليون دولار سنوياً بحلول ٢٠٢٥، مما يجعل العقوبات غير المالية أداة حاسمة في مواجهة هذا التحدي.بدأ تطور هذه العقوبات مع الاعتراف الدولي بأن الهجمات السيبرانية تشكل تهديداً يشبه التهديدات التقليدية، لكنها تتطلب ردوداً مرنة ودقيقة. في الاتحاد الأوروبي، على سبيل المثال، أقر نظاماً متخصصاً للعقوبات السيبرانية في ٢٠١٩، يشمل حظر السفر على الأفراد المسؤولين عن الهجمات التي تهدد أمن الاتحاد أو دوله الأعضاء، بالإضافة إلى إجراءات دبلوماسية مشتركة للرد على النشاط الضار. هذا النظام يركز على الأشخاص والكيانات غير الدولية، لكنه يمكن أن يمتد إلى الوكلاء الحكوميين، وفي ٢٠٢٥، مدد الاتحاد هذه الإجراءات حتى ٢٠٢٦، مع إضافة أفراد روس مسؤولين عن هجمات على إستونيا في ٢٠٢٠، حيث سرقوا آلاف الوثائق السرية من الوزارات الحكومية. هذه الحظر على السفر يمنع المهاجمين من الوصول إلى الاتحاد الأوروبي،[١٦] مما يحد من قدرتهم على بناء شبكات أو التعلم من التكنولوجيا الأوروبية، وفي حالة هجوم على منظمة حظر الأسلحة الكيميائية في ٢٠١٨، الذي نسبت إليه وحدات روسية، أدى إلى حظر سفر لعدة ضباط استخبارات، مما عزل هؤلاء الأفراد عن النشاط الدولي. كما يشمل النظام إجراءات دبلوماسية مثل التنسيق بين الدول الأعضاء لإصدار بيانات مشتركة أو تقليل التمثيل الدبلوماسي، كما حدث في ٢٠٢٤ عندما أضاف الاتحاد ستة أشخاص إلى القائمة بسبب هجمات على أوكرانيا ودول أوروبية أخرى، مما أدى إلى حظر سفرهم وتعزيز الضغط الدبلوماسي على الجهات الداعمة. هذه الإجراءات غير المالية تكمل الجهود الأمنية، حيث أنشأ الاتحاد وحدة مشتركة للسيبران لتبادل المعلومات، مما يسرع عملية الإسناد ويضمن تطبيق الحظر بفعالية[17].أما في الولايات المتحدة، فقد اعتمدت استراتيجية مشابهة تعتمد على حظر السفر والتصدير كأدوات رئيسية للرد على الهجمات السيبرانية المدعومة من الدول. منذ ٢٠١٥، أصدرت الولايات المتحدة أوامر تنفيذية تسمح بفرض حظر سفر على الأفراد والكيانات المسؤولة عن النشاط السيبراني الضار، مثل سرقة البيانات أو تعطيل البنى التحتية، وفي ٢٠٢٥، فرضت عقوبات على هاكرز صينيين مرتبطين بمجموعةFlax Typhoon ، التي اخترقت شبكات أمريكية منذ ٢٠٢١، مما شمل حظر سفر ومنع الدخول للولايات المتحدة، بالإضافة إلى حظر تصدير التقنيات السيبرانية إليهم. هذا الحظر على التصدير، الذي يدار من قبل مكتب الصناعة والأمن، يمنع نقل البرمجيات أو الأجهزة التي يمكن استخدامها في الهجمات، كما في حالة كوريا الشمالية، حيث حظرت الولايات المتحدة تصدير أي تكنولوجيا مزدوجة الاستخدام إلى مجموعات مثلLazarus Group ، المسؤولة عن هجوم WannaCry في ٢٠١٧ الذي أصاب مئات الآلاف من الأجهزة عالمياً. فيما يتعلق بالإجراءات الدبلوماسية، شهدت الولايات المتحدة في ٢٠٢٤ طرد دبلوماسيين روس كرد فعل على هجمات سيبرانية على الانتخابات، مما أدى إلى تقليل التمثيل الروسي في واشنطن، وكذلك في ٢٠٢٥، تعاونت مع حلفاء في تحالف Five Eyes لفرض حظر سفر مشترك على مجرمي سيبرانيين روس من جماعةEvil Corp ، رغم تركيزها الأساسي على الجرائم المالية، لكن الإجراءات امتدت إلى الحد من حركتهم الدولية[١٨]هذه العقوبات غير المالية أثبتت فعاليتها في حالات مثل هجوم Sony Pictures في ٢٠١٤، الذي نسبت إليه كوريا الشمالية، حيث

أدى حظر السفر إلى عزل المهاجمين عن الشبكات الدولية[19].في المملكة المتحدة، بعد انفصالها عن الاتحاد الأوروبي، اعتمدت نظاماً مستقلًا يركز على حظر السفر والتصدير لمواجهة التهديدات السيبرانية، خاصة من روسيا والصين. في ٢٠٢٣، فرضت المملكة عقوبات مشتركة مع الولايات المتحدة وأستراليا على سبعة روس من جماعة إجرامية، شملت حظر سفر وحظر تصدير تقنيات التشفير إليهم، مما حد من قدرتهم على تطوير برمجيات خبيثة. كما في ٢٠٢٥، أعلنت المملكة حظر سفر لأفراد صينيين مرتبطين بهجمات على البنى التحتية البريطانية، كرد على محاولات اختراق الشبكات الحكومية، بالإضافة إلى إجراءات دبلوماسية مثل استدعاء السفراء الصينيين للتوضيح، كما حدث في حالة التشيك في ٢٠٢٥، حيث اتهمت التشيك الصين بهجوم سيبراني على وزارة خارجيتها واستدعت السفير، مما أدى إلى طرد دبلوماسيين وتقليل الروابط. هذه الإجراءات تعكس نهجاً بريطانياً يجمع بين الرد الفوري والتعاون الدولي، حيث ساهمت في تعزيز الدفاعات السيبرانية من خلال مشاركة المعلومات مع الناتو.أما أستراليا، فقد استخدمت عقوبات غير مالية للدفاع عن مصالحها السيبرانية، خاصة ضد الصين وكوريا الشمالية. في ٢٠٢٣، فرضت أستراليا حظر سفر وتصدير على ثلاثة روس من جماعة إجرامية، وفي ٢٠٢٥، أعلنت حظر تصدير تقنيات الذكاء الاصطناعي إلى كيانات كورية شمالية مرتبطة بهجماتransomware ، مما منع نقل التكنولوجيا التي يمكن استخدامها في الهجمات المستقبلية. كذلك، في إطار التعاون مع الولايات المتحدة، أدت إلى طرد دبلوماسيين صينيين في ٢٠٢٤ كرد على هجمات على البرلمان الأسترالي، مما عزز الردع الإقليمي في آسيا–المحيط الهادئ[20].على المستوى الدولي، ساهمت الأمم المتحدة في تعزيز هذه العقوبات من خلال لجان متخصصة، مثل تلك المتعلقة بكوريا الشمالية، حيث حظرت تصدير التكنولوجيا السيبرانية إلى الدولة، وفي ٢٠٢٥، أكدت اللجنة على حظر السفر لأفراد مرتبطين بـ Lazarus Group، بالإضافة إلى إجراءات دبلوماسية مثل حظر مشاركة كوريا الشمالية في مؤتمرات الأمم المتحدة المتعلقة بالأمن السيبراني. هذه الإجراءات غير المالية ساعدت في عزل الدول المعتدية، كما في حالة روسيا بعد هجومSolarWinds ، حيث أدى التعاون الدولي إلى حظر سفر لعشرات الأفراد وطرد دبلوماسيين من عدة دول.رغم فعاليتها، تواجه هذه العقوبات تحديات مثل صعوبة الإسناد، حيث يصعب ربط الهجوم بالمستهدف دون كشف الاستخبارات، مما يؤخر التطبيق، كما في حالة NotPetya حيث استغرق الأمر سنوات لفرض حظر السفر. كما أن الدول المعزولة مثل كوريا الشمالية تلتف حول الحظر عبر شبكات غير رسمية، ومع ذلك، أظهرت الدراسات نجاحاً في ٤٠٪ من الحالات في تغيير السلوكيات عندما تكون متعددة الأطراف[21].يبرز التعاون الدولي كمفتاح للنجاح، حيث أنشأ الناتو في ٢٠١٦ إعلاناً يعتبر الهجمات السيبرانية تهديداً أمنياً، مما أدى إلى إجراءات مشتركة مثل حظر السفر في ٢٠٢٥ ضد روس. كذلك، ساعدت منظمة التعاون الاقتصادي والتنمية في وضع معايير للتصدير السيبراني، مما يدعم التنفيذ العالمي حيث تمثل العقوبات غير المالية أداة أساسية للرد على الهجمات السيبرانية، حيث توازن بين الدقة والفعالية، ومع تزايد التهديدات مثل استخدام الذكاء الاصطناعي، يجب تعزيزها لضمان أمن عالمي مستدام[22].

المطلب الثاني: التحديات في فرض العقوبات على الهجمات السيبرانية

لقد تحول الفضاء السيبراني إلى ساحة المعركة الخامسة بين القوى الدولية وذلك بعد البر والبحر والجو والفضاء الخارجي، ويعد هذا المجال التكنولوجي المتطور ساحة جديدة للصراعات العالمية، اذ أصبحت الهجمات السيبرانية التي تستهدف البنية التحتية المعلوماتية إحدى أخطر الأدوات المستخدمة في الحروب الحديثة فمثل هذه الهجمات قد تؤدي إلى انهيار اقتصادي كامل لدولة من الدول أو التسبب في أضرار كارثية تمتد إلى كافة القطاعات سواء كانت عسكرية أو مدنية، أن هذا الخطر يتضاعف مع ازدياد الاعتماد العالمي على التكنولوجيا والأنظمة الرقمية في كافة جوانب الحياة اليومية والإستراتيجية، إن الطبيعة الفريدة للفضاء السيبراني بوصفه بعدا افتراضيا لا يخضع للسيادة المباشرة للدول تجعله بيئة مثالية للأعمال العدائية، فبينما يمكن للدول فرض سيطرتها على أراضيها أو أجوائها أو مياهها الإقليمية فإنها لا تستطيع بنفس السهولة فرض سيادتها على الفضاء السيبراني، هذا الفضاء المشترك بين الجميع يعتمد على التكنولوجيا التي يستخدمها الأفراد والمؤسسات والشركات والحكومات، مما يجعله عرضة للاستغلال من قبل المهاجمين السيبرانيين.[٢٣]**البند الأول: صعوبة تحديد الجهة المسؤولة عن الهجمات السيبرانية**في عالم اليوم الذي أصبح فيه الفضاء السيبراني عماد التواصل والاقتصاد والأمن، تبرز الهجمات السيبرانية كواحدة من أكبر التهديدات المعاصرة، ليس فقط بسبب قدرتها على إحداث أضرار فورية هائلة، بل أيضًا بسبب التحديات الجوهرية التي تفرضها على النظام القانوني الدولي. يتمثل أحد أبرز هذه التحديات في صعوبة تحديد الجهة المسؤولة عن هذه الهجمات، أو ما يُعرف بـ"مشكلة الإسناد(attribution problem) "، والتي تعيق بشكل مباشر فرض العقوبات الدولية الفعالة. هذه الصعوبة ليست مجرد عقبة تقنية، بل هي مزيج معقد من العوامل التقنية والسياسية والقانونية، تجعل من الردود الدولية المتناسقة أمرًا شبه مستحيل في كثير من الحالات. في هذا البيان المفصل، سنستعرض هذه الصعوبات بعمق، مع الاستناد إلى مواد القانون الدولي ووثائق أخرى ذات صلة، مستخدمين أمثلة تاريخية لتوضيح كيفية تأثيرها على آليات العقاب، دون التقيد بعناوين جانبية، بل

بتدفق سلس يعكس تعقيد الموضوع[24].لنبدأ بفهم جوهر مشكلة الإسناد في سياق الهجمات السيبرانية. على عكس الهجمات التقليدية، مثل الغارات الجوية أو الغزوات البرية، حيث تكون الإسناد مباشرًا من خلال الأدلة المادية أو الشهود، تتميز الهجمات السيبرانية بطبيعتها اللامادية واللامحدودة جغرافيًا. يمكن لمهاجم أن يخفي هويته باستخدام شبكات الوكلاء(proxies) ، أو الشبكات الخبيثة الموزعة(botnets) ، أو حتى سرقة هويات الآخرين، مما يجعل تتبع المصدر الأصلي عملية معقدة وغير مضمونة. هذا الغموض التقني يُعزى إلى تصميم الإنترنت نفسه، الذي كان يهدف أساسًا إلى الاتصال السريع والآمن، لكنه أصبح اليوم سلاحًا مزدوج الحد. وفقًا لتقرير صادر عن المجلس الأطلسي، فإن هذه الصعوبة في الإسناد ليست جديدة، بل تعود إلى أكثر من عقدين من الزمن، حيث يصعب على الدفاع السيبراني والمخابرات تحديد مصدر الهجمات الضارة بدقة، مما يعيق الردود الدبلوماسية أو العسكرية[٢٥]هذا الغموض يمتد إلى الجانب السياسي، إذ ينفي الدول المتهمة دائمًا تورطها، مستغلة الشكوك لتجنب المساءلة، كما حدث في حالة هجوم WannaCry عام ٢٠١٧، الذي أُسند إلى كوريا الشمالية، لكن الإسناد كان قائمًا على أدلة غير مباشرة مثل رموز البرمجة المشابهة لأدوات هجومية سابقة، مما أثار جدلاً حول مدى اليقين.من الناحية القانونية، يُعد القانون الدولي العرفي والمعاهدات الدولية الأساس لمعالجة هذه الهجمات، لكنه يواجه تحديات في تطبيق قواعد الإسناد. يُشير الدليل ١١ من الدليل التاليني ٢.٠ Tallinn) (Manual 2.0، الذي صدر عام ٢٠١٧ تحت رعاية معهد كوبرنيكوس للقانون الدولي الإنساني، إلى أن الإسناد يتطلب إثباتًا كافيًا بأن الدولة كانت على علم بالعمليات السيبرانية أو ساهمت فيها، مستندًا إلى مواد مسودة لجنة القانون الدولي حول مسؤولية الدول Draft Articles on) State Responsibility، ٢٠٠١ .(هذا الدليل، الذي يُعتبر مرجعًا غير ملزم لكنه مؤثر، يحدد أن الهجوم السيبراني يُعتبر "هجومًا مسلحًا" إذا أدى إلى أضرار جسيمة، وفقًا للمادة ٢(٤) من ميثاق الأمم المتحدة، مما يفتح الباب للرد الجماعي أو الفردي تحت المادة ٥١. ومع ذلك، يعترف الدليل نفسه بأن الإسناد الفني غير كافٍ لوحده؛ يجب أن يُدعم بأدلة استخباراتية أو دبلوماسية، وهو ما يثير مشكلة السرية، إذ لا يمكن الكشف عن مصادر الاستخبارات دون تعريضها للخطر. هنا، تبرز صعوبة فرض العقوبات، لأن مجلس الأمن التابع للأمم المتحدة يتطلب إجماعًا لإصدار قرارات ملزمة، كما في القرار ٢٣٩٧ (٢٠١٧) الذي فرض عقوبات على كوريا الشمالية بسبب برنامجها النووي، لكنه لم يتطرق مباشرة إلى هجماتها السيبرانية بسبب نقص الإسناد الدامغ[26].تتفاقم هذه الصعوبة عند النظر إلى الدول غير الديمقراطية، مثل روسيا وكوريا الشمالية والصين، التي غالبًا ما تُتهم بتوجيه هجمات سيبرانية لكنها تنفي ذلك بقوة. خذ على سبيل المثال هجوم NotPetya عام ٢٠١٧، الذي أدى إلى خسائر اقتصادية تجاوزت ١٠ مليارات دولار، وأُسند إلى مجموعة APT28 الروسية(Fancy Bear) ، لكن الحكومة الروسية نفت أي تورط، مدعية أنها كانت هجومًا أوكرانيًا. هنا، كشف تقرير صادر عن وزارة العدل الأمريكية عام ٢٠١٨ عن تهم جنائية ضد ١٢ ضابطًا روسيًا، لكن فرض عقوبات دولية واسعة النطاق تعثر بسبب الفيتو الروسي في مجلس الأمن، مما يبرز كيف يُستخدم الإسناد الغامض كأداة سياسية للتهرب من المساءلة[٢٧]في حالة كوريا الشمالية، هجوم Sony Pictures عام ٢٠١٤، الذي أُسند إلى وحدة الاستطلاع ١٢١ التابعة للجيش الكوري الشمالي، أدى إلى عقوبات أمريكية فردية، لكن الإسناد اعتمد على تشابه الأدوات الرقمية مع هجمات سابقة مثلDarkSeoul ، دون أدلة مادية مباشرة، مما جعل الرد الدولي محدودًا وغير فعال، إذ لم يتمكن مجلس الأمن من إصدار قرار يربط الهجوم بالعقوبات الشاملة. أما الصين، ففي هجمات OPM (مكتب إدارة الموظفين الفيدرالي الأمريكي) عام ٢٠١٥، التي سرقت بيانات ٢١ مليون موظف حكومي، أُسندت إلى وحدة ٦١٣٩٨ التابعة للجيش الصيني، لكن الإسناد كان فنيًا بناءً على عناوين IP وأساليب البرمجة، مما أدى إلى عقوبات أمريكية لكن بدون دعم دولي واسع، بسبب الاعتماد الاقتصادي على الصين[28].يُضيف القانون الدولي طبقة أخرى من التعقيد من خلال اتفاقية بودابست بشأن الجرائم الإلكترونية (٢٠٠١)، التي وقعتها ٦٨ دولة حتى الآن، والتي تركز على الجرائم الإلكترونية الفردية مثل الاحتيال والتجسس، لكنها لا تتناول الهجمات المدعومة من الدول. المادة ٢ من الاتفاقية تحدد نطاق الجرائم، لكنها تفتقر إلى آليات إسناد دولي، مما يجعل فرض العقوبات على الدول المسؤولة أمرًا خارج نطاقها. هذا النقص يدفع نحو الحاجة إلى تطوير قواعد جديدة، كما اقترحت مجموعة العشرين في قمة ٢٠١٥، لكن التقدم بطيء بسبب الخلافات حول السيادة السيبرانية. كما أن قرارات الأمم المتحدة، مثل القرار ٦٣/٥٥ (٢٠٠١) الذي يدعو إلى مكافحة الاستخدام الإجرامي للتكنولوجيا، أو القرار ١٢١/٥٦ (٢٠٠٢) الذي يركز على التعاون الدولي، تظل توصيات عامة دون آليات تنفيذية للإسناد، مما يعيق العقوبات الملزمة[29].في سياق أوسع، يُبرز الدليل التاليني ٢.٠ في الفصل الثالث قواعد الإسناد، مستندًا إلى المادة ٨ من مسودة لجنة القانون الدولي، التي تنص على أن سلوك فرد أو مجموعة يُنسب إلى الدولة إذا كان يعمل بأمرها أو تحت سيطرتها. ومع ذلك، في الهجمات السيبرانية، غالبًا ما تكون الجماعات المستقلة مثل Anonymous أو مجموعات إجرامية، مما يثير تساؤلات حول "السيطرة الفعالة(effective control) "، كما حددتها محكمة العدل الدولية في قضية نيكاراغوا ضد الولايات المتحدة (١٩٨٦). هذا الاختلاف بين الإسناد الفني والقانوني يجعل فرض العقوبات تحديًا،

إذ يمكن للدول الادعاء بأن الهجمات كانت من "مرتزقة" غير مرتبطين، كما في حالة هجوم SolarWinds عام ٢٠٢٠، الذي أُسند إلى SVR الروسي، لكن الإسناد استغرق أشهرًا واعتمد على تحليلات خاصة، مما أدى إلى عقوبات أمريكية وأوروبية لكن بدون تأثير كبير على روسيا[30].بالإضافة إلى ذلك، تُعقد المسألة دور الدول الثالثة، مثل استخدام كوريا الشمالية لخوادم في الصين أو أوروبا الشرقية لإخفاء هجماتها، كما في هجوم Bangladeshi Bank عام ٢٠١٦، الذي سرق ٨١ مليون دولار، وأُسند إلى Lazarus Group الكورية الشمالية، لكن التحويلات مرت عبر الفلبين والصين، مما أثار مشكلات في الإسناد الجغرافي وفرض العقوبات على الوسطاء. هنا، يأتي دور اتفاقية الأمم المتحدة الجديدة بشأن الجرائم الإلكترونية (٢٠٢٣-٢٠٢٤)، التي تهدف إلى تعزيز التعاون الدولي، لكنها لا تزال في مراحلها الأولى وتواجه انتقادات من منظمات حقوقية بسبب مخاوف من الاستخدام السياسي.من منظور أوروبي، يُظهر نظام عقوبات الاتحاد الأوروبي السيبرانية (EU Cyber Sanctions Regime)، ٢٠٢٠ (محاولة للتغلب على هذه الصعوبات، حيث يسمح بفرض عقوبات على أفراد أو كيانات مسؤولة عن هجمات، كما في حالة عقوبات ضد مجموعات روسية عام ٢٠٢١ بسبب هجوم على مستشفيات أوروبية أثناء جائحة كوفيد-١٩. ومع ذلك، يعترف التقرير الصادر عن معهد العلوم السياسية في برلين بأن الإسناد يظل "مشكلة مركزية" في الدبلوماسية السيبرانية الأوروبية، إذ يتطلب الإسناد مستوى عاليًا من اليقين لتجنب التصعيد غير المقصود. هذا يعكس التوتر بين الحاجة إلى الرد السريع والمخاطر القانونية، حيث يُعتبر الإسناد غير الدقيق انتهاكًا لمبدأ السيادة[31].في السياق الأمريكي، أصدرت إدارة بايدن استراتيجية الأمن السيبراني الوطني (٢٠٢٣)، التي تؤكد على تعزيز الإسناد من خلال التعاون الدولي، لكنها تعترف بأن "الإسناد السياسي" أصعب من الفني، كما في حالة هجمات إيرانية مدعومة من الحرس الثوري ضد بنية تحتية أمريكية. هنا، فرضت الولايات المتحدة عقوبات تحت قانون CAATSA (2017) ضد روسيا، لكن الفعالية محدودة بسبب الاعتماد على الأدلة الاستخباراتية السرية[32].لنعمق النظر في الآثار الاقتصادية والاجتماعية لهذه الصعوبة. الهجمات السيبرانية تكلف الاقتصاد العالمي تريليونات الدولارات سنويًا، وفقًا لتقديرات شركةMcAfee ، لكن غياب العقوبات الفعالة يشجع على التكرار، كما في حملات التجسس الصينية المستمرة ضد الشركات الأمريكية، التي أدت إلى سرقة ملكيات فكرية بقيمة ٦٠٠ مليار دولار سنويًا، دون عقوبات دولية موحدة بسبب الشكوك في الإسناد. هذا يؤدي إلى "سباق تسلح سيبراني"، حيث تستثمر الدول في القدرات الهجومية بدلاً من الدفاع، مما يهدد الاستقرار العالمي.من الناحية الأخلاقية والقانونية، يثير الإسناد تساؤلات حول مبدأ "الرد النسبي" في القانون الدولي الإنساني، كما في الملحق الإضافي الأول لاتفاقيات جنيف (١٩٧٧)، الذي ينطبق على الهجمات السيبرانية إذا اعتبرت نزاعًا مسلحًا. الدليل التاليني يحدد في الدليل ١٤٩ أن الرد يجب أن يكون متناسبًا، لكن بدون إسناد دقيق، يصبح الرد عشوائيًا، مما قد يؤدي إلى تصعيد غير مرغوب، كما حذرت منه دراسة صادرة عن جامعة كامبريدج عام ٢٠٢٣ حول مخاطر عدم استدعاء مسؤولية الدول في الهجمات السيبرانية[33].للتغلب على هذه التحديات، اقترح خبراء في تقرير صادر عن الاتحاد الأطلسي إنشاء "شبكات استجابة سريعة" دولية تشمل تبادل معلومات استخباراتية، مع ضمانات للحفاظ على السرية، بالإضافة إلى تطوير معايير تقنية للإسناد مثل blockchain لتتبع الأنشطة السيبرانية. كما دعت ألمانيا في ورقة موقفها عام ٢٠٢١ إلى تطبيق القانون الدولي على الفضاء السيبراني، مشيرة إلى أن العمليات السيبرانية التي تؤدي إلى أضرار جسيمة يجب أن تُعامل كانتهاك للسيادة كصعوبة تحديد الجهة المسؤولة عن الهجمات السيبرانية تمثل تحديًا أساسيًا لفرض العقوبات، إذ تحول دون الرد الدولي المنسق والفعال. من خلال الاستناد إلى القانون الدولي مثل الدليل التاليني ومسودة لجنة القانون الدولي، وقرارات الأمم المتحدة، وأمثلة مثل هجمات روسيا وكوريا الشمالية والصين، يتضح أن الحل يتطلب تعزيز التعاون الدولي والابتكار التقني. دون ذلك، سيظل الفضاء السيبراني ساحة للإفلات من العقاب، مهددًا السلام العالمي. [٣٤]**البند الثاني: مخاطر التصعيد** في عصرنا الرقمي الحالي، حيث أصبحت الهجمات السيبرانية جزءًا لا يتجزأ من الصراعات الدولية، تبرز مخاطر التصعيد كواحدة من أبرز التحديات التي تواجه فرض العقوبات على هذه الهجمات، إذ تحول دون الردود الفعالة والمنضبطة التي تحافظ على الاستقرار العالمي. هذه المخاطر ليست مجرد افتراضات نظرية، بل هي نتاج تفاعل معقد بين التقنيات السيبرانية المتطورة والقوانين الدولية التي صُممت أساسًا لعصر ما قبل الرقمي، مما يجعل أي محاولة لفرض عقوبات محفوفة باحتمالات التصعيد غير المتعمد أو المتعمد، سواء كان ذلك من خلال ردود سيبرانية متبادلة أو تصعيد إلى صراعات تقليدية. يعتمد هذا التحدي على طبيعة الهجمات السيبرانية نفسها، التي غالبًا ما تكون غامضة في الإسناد وسريعة التأثير، مما يزيد من خطر سوء التقدير أو الرد المفرط، كما يُبرز ذلك في تقارير متعددة حول النزاعات السيبرانية بين القوى الكبرى. على سبيل المثال، في سياق الغزو الروسي لأوكرانيا عام ٢٠٢٢، أدت العقوبات الغربية إلى مخاوف من تصعيد سيبراني روسي، حيث حذر الخبراء من أن مثل هذه العقوبات قد تثير ردودًا سيبرانية تستهدف البنية التحتية الحيوية، مما يؤدي إلى دورة من التصعيد قد تتجاوز الحدود السيبرانية. هذا التصعيد المحتمل يعكس كيف يمكن للعقوبات، التي تهدف إلى الردع، أن تتحول إلى محفز للصراع، خاصة في ظل غياب آليات واضحة في

القانون الدولي لتنظيم الردود[35].لنفهم جذور هذه المخاطر، يجب النظر إلى كيفية تفسير القانون الدولي للهجمات السيبرانية كشكل من أشكال "القوة" أو "التهديد"، كما حددته المادة ٢(٤) من ميثاق الأمم المتحدة، التي تحظر استخدام القوة ضد سيادة الدول أو سلامتها الإقليمية. في هذا السياق، يُعتبر الهجوم السيبراني الذي يسبب أضرارًا جسيمة، مثل تعطيل شبكات الكهرباء أو الخدمات المالية، انتهاكًا لهذه المادة، مما يفتح الباب للردود بما في ذلك العقوبات. ومع ذلك، يثير فرض هذه العقوبات مخاطر التصعيد لأن الدول المستهدفة قد ترى فيها اعتداءً اقتصاديًا يبرر ردًا سيبرانيًا أو عسكريًا، كما حدث في حالة العقوبات الأمريكية على روسيا بعد تدخلها في الانتخابات الأمريكية عام ٢٠١٦، حيث أدت إلى مخاوف من تصعيد سيبراني روسي لم يحدث بشكل كبير، الذي يُعد مرجعًا رئيسيًا لتطبيق القانون الدولي على العمليات السيبرانية، يحدد في قاعدته ١١ أن الهجوم السيبراني يُعتبر "استخدام قوة" إذا أدى إلى أضرار مشابهة للهجوم التقليدي، مما يسمح بالرد الذاتي تحت المادة ٥١ من الميثاق، لكن هذا الرد يجب أن يكون متناسبًا، وهنا تكمن المخاطر، إذ قد يؤدي رد غير متناسب، مثل عقوبات اقتصادية واسعة، إلى تصعيد غير متوقع. هذا الدليل، الذي أعدته مجموعة من الخبراء تحت رعاية مركز التميز التعاوني للدفاع السيبراني التابع لحلف الناتو، يؤكد على أهمية التمييز بين العمليات السيبرانية تحت عتبة النزاع المسلح وبين تلك التي تتجاوزها، لكن في حالة العقوبات، غالبًا ما تكون هذه الحدود غامضة، مما يزيد من خطر التصعيد العرضي[36].تتفاقم هذه المخاطر عند النظر إلى مفهوم "التصعيد المقلوب(escalation inversion) "، الذي يصف كيف يمكن للعمليات السيبرانية أن تكون مستقرة في أوقات السلام النسبي لكنها تصبح محفزة للتصعيد في أزمات حادة، حيث تُستخدم كأداة للضربة الأولى بسبب عنصر المفاجأة والتأثير غير المتوقع. في دراسة نشرتها مجلة Texas National Security Review عام ٢٠٢٠، يُبرز الباحثون أن هذا التصعيد المقلوب يحدث عندما ترى الدول في القدرات السيبرانية فرصة للهجوم المبكر، مما يعكس الاستقرار السيبراني ويزيد من مخاطر التصعيد، خاصة إذا أدت العقوبات إلى تفاقم التوترات. [٣٧]على سبيل المثال، خلال أزمة مضيق هرمز عام ٢٠١٩، اختارت الولايات المتحدة ردًا سيبرانيًا محدودًا على إيران بدلاً من ضربات جوية، لكن هذا الاختيار كان محفوفًا بمخاطر تصعيد إذا فُسر الرد السيبراني كتهديد أكبر، مما يظهر كيف يمكن للعقوبات المرتبطة بالهجمات السيبرانية أن تؤدي إلى دوامة من الردود المتزايدة. كما أن الاستخدام الواسع للوكلاء والأدوات الغامضة في الهجمات السيبرانية، كما في هجوم NotPetya الروسي عام ٢٠١٧ الذي أثر على العالم بأسره، يجعل الرد بالعقوبات مخاطرة، إذ قد يؤدي إلى استهداف خاطئ أو تصعيد غير مقصود مع دول ثالثة[38].من الناحية القانونية، تُضيف اتفاقية بودابست بشأن الجرائم الإلكترونية (٢٠٠١) طبقة أخرى من التعقيد، إذ تركز على التعاون في مكافحة الجرائم السيبرانية الفردية، لكنها لا توفر آليات واضحة لفرض عقوبات على الهجمات المدعومة من الدول دون مخاطر تصعيد. المادة ٢ من الاتفاقية تحدد الجرائم، لكن في حالة هجمات مثل SolarWinds عام ٢٠٢٠، التي أُسندت إلى روسيا، أدت العقوبات الأمريكية والأوروبية إلى توترات دبلوماسية، مع مخاوف من رد روسي سيبراني يستهدف البنية التحتية، مما يبرز كيف يمكن للعقوبات أن تكون محفزًا للتصعيد بدلاً من الردع. كذلك، في تقرير صادر عن مجلس الأطلسي عام ٢٠١٩، يُناقش الباحثون ما نعرفه عن التصعيد السيبراني من خلال محاكيات واستطلاعات، مشيرين إلى أن العمليات السيبرانية غالبًا ما تكون مستقرة وتوفر مخرجًا من التصعيد، لكن عند ربطها بعقوبات اقتصادية، كما في حالة الرد الأمريكي على إيران عام ٢٠١٩، قد تقلل من استخدام العقوبات الفردية لصالح الإشارات السيبرانية، مما يقلل من مخاطر التصعيد لكنه يعتمد على التواصل الفعال. هذا التقرير يستند إلى أمثلة تاريخية مثل رد روسيا السيبراني على تركيا عام ٢٠١٥، حيث استخدمت هجمات رفض الخدمة بدلاً من القوة العسكرية، مما يظهر إمكانية تجنب التصعيد إذا تم التعامل مع العقوبات بحذر[39].بالإضافة إلى ذلك، يُبرز نظام عقوبات الاتحاد الأوروبي السيبراني (٢٠٢٠) محاولة لمواجهة هذه المخاطر، إذ يسمح بفرض عقوبات على أفراد أو كيانات مسؤولة عن هجمات سيبرانية ذات تأثير كبير، كما في عقوبات ضد مجموعات روسية عام ٢٠٢١ بسبب هجمات على مستشفيات أثناء جائحة كوفيد-١٩. ومع ذلك، يعترف الخبراء بأن هذا النظام يحمل مخاطر تصعيد إذا أدى إلى ردود من الدول المستهدفة، خاصة في ظل غموض الإسناد، كما حدث في هجوم WannaCry عام ٢٠١٧ المنسوب إلى كوريا الشمالية، حيث أدت العقوبات إلى مخاوف من تصعيد نووي أو سيبراني. في سياق أوسع، يُناقش تقرير من European Leadership Network عام ٢٠٢٥ مخاطر استخدام الردع النووي ضد الهجمات السيبرانية، مشيرًا إلى أن مثل هذا النهج ينتهك مبادئ التناسب في القانون الدولي، كما في المادة ٥١ من ميثاق الأمم المتحدة، ويزيد من مخاطر التصعيد غير المتعمد بسبب صعوبة الإسناد، مستشهدًا بهجمات روسية هجينة مثل NotPetya كأمثلة على استخدام الغموض لتجنب المساءلة. هذا التقرير يؤكد على معاهدة عدم انتشار الأسلحة النووية(NPT) ، محذرًا من أن توسيع الردع النووي ليشمل السيبراني قد يقوض أهدافها، مما يؤدي إلى سباق تسلح يزيد من مخاطر التصعيد العالمي[40].من الجوانب الاقتصادية، تكلف الهجمات السيبرانية الاقتصاد العالمي تريليونات الدولارات سنويًا، وفرض العقوبات كرد عليها قد يؤدي إلى تصعيد اقتصادي، كما في حالة العقوبات على روسيا بعد غزو

أوكرانيا، حيث حذر الخبراء من ردود سيبرانية تستهدف المؤسسات المالية الغربية، مما يؤدي إلى اضطرابات عالمية. على سبيل المثال، في مقال نشرته Krebs on Security عام ٢٠٢٢، يُناقش كيف قد تؤدي العقوبات على روسيا إلى تصعيد سيبراني، مستشهدًا بتاريخ روسيا في مهاجمة شبكات الكهرباء الأوكرانية عام ٢٠١٥، ومحذرًا من هجمات مشابهة على الطاقة الغربية، مع اقتراحات بتجنب التصعيد من خلال ردود غير مباشرة. كذلك، في مقال بمجلة Foreign Affairs عام ٢٠٢٢، يُجادل الكاتب بأن فكرة التصعيد السيبراني قد تكون وهمًا، إذ لم يؤد أي هجوم سيبراني إلى حرب، مستشهدًا بهجمات كوريا الشمالية على الجنوبية دون تصعيد، لكن يحذر من أن العقوبات قد تُفسر كتصعيد إذا لم تُدار بعناية، مما يتطلب تواصلًا واضحًا لتجنب سوء الفهم[41].في السياق الإيراني، أدت العقوبات الأمريكية على إيران بعد هجمات سيبرانية إلى مخاوف من تصعيد، كما في أزمة ٢٠١٩ حيث اختارت أمريكا ردًا سيبرانيًا بدلاً من عسكري، لكن هذا النهج يحمل مخاطر إذا أدى إلى دورة ردود متبادلة. تقرير من War on the Rocks عام ٢٠٢٢ يناقش منع التصعيد السيبراني في أوكرانيا، مشيرًا إلى أهمية النظر في الأخطاء والحسابات الخاطئة التي قد تؤدي إلى تصعيد، خاصة مع عقوبات تؤثر على الاقتصاد الروسي. كما أن قرارات الأمم المتحدة، مثل القرار ٦٣/٥٥ (٢٠٠١) الذي يدعو إلى مكافحة الاستخدام الإجرامي للتكنولوجيا، تظل عامة وغير كافية لمنع التصعيد، مما يتطلب تطوير اتفاقيات جديدة[42].للتغلب على هذه المخاطر، يُقترح إنشاء خطوط اتصال ساخنة سيبرانية ومعايير دولية للرد، كما في الاتفاق الأمريكي الروسي عام ٢٠١٣، لكن في ظل التوترات الحالية، يظل التحدي قائمًا. في الختام، مخاطر التصعيد تحول دون فرض عقوبات فعالة على الهجمات السيبرانية، مما يتطلب توازنًا دقيقًا بين الردع والاستقرار، مستندًا إلى القانون الدولي لتجنب التصعيد غير المتعمد.**البند الثالث: قلة التعاون الدولي**يعتبر التعاون الدولي في المجال الأمني ضرورة ملحة واستراتيجية لمواجهة التحديات المتعلقة بالهجمات السيبرانية ضد أمن واستقرار الدول، حيث أصبحت أساليب الحرب ووسائلها تعتمد على تكنولوجيا المعلومات وتستخدم في سياق نزاع مسلح، انطلاقا من الهجمات والعمليات التي ترتكب ضد أو بواسطة شبكات الحواسيب وأنظمة البيانات بين الدول أو الجماعات المسلحة المنظمة في سياق النزاعات أو الأعمال الردعية المتبادلة[43].وبذلك فإن الهجمات السيبرانية تعتبر ضمن أبرز المخاطر التي تحيط بالدول نتيجة استهدافها للأنظمة العسكرية والبنية التحتية الحيوية للدول فضلا عن الشبكات الذكية وشبكات المراقبة وحيازة البيانات التي تسمح لها بالدفاع عن نفسها.وأكثر الأمور أهمية هو العمل على تكثيف الجهود الدولية للتعاون الأمني خاصة في ظل ضعف بعض أجهزة العدالة الجزائية، فيمكن الاستفادة من الجوانب التقنية والتكنولوجية التي تتمتع بها بعض الدول للتمكن من مواجهة الجرائم بالاستناد على الجوانب التشريعية والفنية.[٤٤]ففي هذا السياق ينبغي التأكيد على أهمية التعاون بين الدول والمنظمات الدولية والإقليمية بسبب مختلف التهديدات السيبرانية، وعلى الرغم من بعض الاختلافات الواقعة بين السياسات الوطنية والاتفاقيات الدولية حول المبادرات المتعلقة بالأمن السيبراني لكنها متفقة على البعد الدولي للفضاء السيبراني.الأمر الذي أكدت عليه الجمعية العامة في العديد من قراراتها في هذا المجال على تحسين قدرات الدول على التعاون والعمل الجماعي من أجل تعزيز استخدام تكنولوجيا المعلومات للأغراض السلمية.وتم فتح المجال لمكتب شؤون نزع السلاح بالأمانة العامة للأمم المتحدة من أجل التعاون مع المنظمات الإقليمية ذات الصلة، كالاتحاد الأوروبي والاتحاد الأفريقي ومنظمة الدول الأمريكية ومنظمة الأمن والتعاون في أوروبا والمنتدى الإقليمي لرابطة أمم جنوب شرق آسيا لعقد تشاورات مع أعضاء فريق الخبراء الحكوميين في مجال التعاون لدراسة التطورات الحاصلة في مجال المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدوليينبغي على الدول ألا تسمح لدولة أخرى أو أية جهة فاعلة باستخدام إقليمها في تكنولوجيا المعلومات والاتصالات للقيام بارتكاب أفعال غير مشروعة وفقا للاتفاقيات والعرف الدوليين، ويكون على الدولة المتضررة إخطار الدولة التي صدر من أراضيها هذا النشاط لتقوم بتوضيح الأمر والتعاون للتدخل وتوقيف هذه الأفعال، ولا يعني ذلك بأن الدولة الثالثة التي استخدم إقليمها مسؤولة عن تلك الأعمال ويجب على الدول ألا تستخدم وكلاء عنها للقيام بهجومات سيبرانية وأن تحرص في نفس الوقت على ضمان عدم استخدام إقليمها من قبل جهات أخرى.ومن المبادرات كذلك تذكر مشروع اتفاقية الاتحاد الأفريقي بشأن إنشاء إطار قانوني للأمن السيبراني في إفريقيا، وتعتبر اتفاقية "مالابو[٤٥] اتفاقية طموحة لأمن المعلومات على مستوى القارة وعلى الرغم من أن دول الاتحاد الأفريقي تواجه تحديات كبيرة فيما يتعلق بالأمن السيبراني بسبب الاختلافات الكبيرة في المجالات السياسية والثقافية والاجتماعية، برزت فكرة أهمية التعاون في مجال الأمن السيبراني من خلال قمة الاتحاد الأفريقي واعتماد موقف موحد وهو العمل على تطبيق القانون الدولي في الفضاء السيبراني، فقاد العملية مجلس السلام والأمن التابع للاتحاد الأفريقي[٤٦]كما قام الاتحاد الأوروبي بوضع وثيقة سياسية شاملة تعبر عن وجهة نظر جميع الدول الأعضاء من خلال نشر بيانا مشتركا يتعلق بالاستراتيجية المتعلقة بالأمن السيبراني للاتحاد الأوروبي من خلال إبرام اتفاقية بودابست بشأن الجريمة السيبرانية المحررة في ٢٣ نوفمبر ٢٠٠١ من أجل تحقيق وحدة بين الأعضاء وتعزيز التعاون بين الأطراف لاتباع سياسية جنائية مشتركة لحماية المجتمع من الجرائم الحاسوبية ولحماية المصالح المشروعة في استخدام تكنولوجيا المعلومات وتوفير الترتيبات

اللازمة للتعاون الدولي السريع. [٤٧]إن المعاهدات المتعددة الأطراف أكثر الوسائل العملية لموائمة النظم القانونية الوطنية بما يصبو إليه النظام الدولي ولإماطة الغموض المتعلق بالقانون الدولي في سياق الأمن السيبراني ويعتبر بذلك التعاون الدولي هو حجر الزاوية لمواجهة مخاطر الحروب السيبرانية.

المبحث الثاني: فعالية العقوبات الدولية في مكافحة الهجمات السيبرانية

أصبحت الهجمات السيبرانية تهديدًا عالميًا يتجاوز الحدود الجغرافية، مما يجعل العقوبات الدولية أداة أساسية في استراتيجيات المكافحة. تهدف هذه العقوبات، سواء من خلال قرارات مجلس الأمن التابع للأمم المتحدة أو آليات الاتحاد الأوروبي والولايات المتحدة، إلى ردع الجهات المسؤولة عن الهجمات، مثل الدول أو الجماعات المدعومة منها، من خلال فرض قيود اقتصادية أو مالية أو تقنية. ومع ذلك، تثير فعاليتها جدلاً واسعًا، إذ أنها نجحت في بعض الحالات في الحد من قدرات المهاجمين، كما في عقوبات الاتحاد الأوروبي كرد على الهجمات السيبرانية، حيث ساهمت في زيادة الضغط على الجهات الإجرامية وتعزيز التعاون الدولي. إلا أن التحديات التقنية والسياسية، مثل صعوبة الإسناد الدقيق والتجنب السيبراني للعقوبات، تقلل من تأثيرها، كما يبرز ذلك في تقارير حول تجنب العقوبات في الفضاء السيبراني[48].رغم التقدم في تطوير أطر قانونية مثل استراتيجية السياسة السيبرانية والرقمية الدولية الأمريكية لعام ٢٠٢٥، التي تركز على بناء القدرات لمواجهة التهديدات الناشئة، إلا أن فعالية العقوبات الدولية في مكافحة الهجمات السيبرانية تظل محدودة بسبب الطبيعة المتطورة لهذه الهجمات واعتمادها على تقنيات متقدمة. في الواقع، أظهرت دراسات حديثة أن العقوبات قد تكون ردودًا قديمة على تهديدات جديدة، مما يتطلب تكييفها مع التعاون الدولي المعزز لتحقيق تأثير أكبر، كما في اقتراحات لزيادة التعاون في الأمن السيبراني لمواجهة الأضرار الاقتصادية والاجتماعية الهائلة. ومع ذلك، فإن الزيادة في استخدام العقوبات في السنوات الأخيرة، كما في تحديثات ٢٠٢٥، تشير إلى إمكانية تحسينها لتصبح أكثر فعالية في مواجهة الصراعات العالمية المستمرة[٤٩] وعليه تم تقسيم المبحث الى دراسة حالات في المطلب الأول، وفي المطلب الثاني بيان التقييم النقدي لفعالية العقوبات

المطلب الأول: دراسات الحالة

إن البحث في امكانية تطبيق قواعد القانون الدولي على الحرب السيبرانية يستلزم ابتداءً التكييف القانوني لتلك المسألة من حيث شرعية وعدم شرعية الحرب السيبرانية في ضوء استخدام القوة في العلاقات الدولية، فالعلاقة بين حق اللجوء إلى الحرب وقانون الحرب تتسم بأنها علاقة توتر لا بد منه، فالقواعد المعاصرة للقانون الدولي تحظر استخدام القوة، باستثناء حق الدول فرادى أو جماعات في الدفاع عن إما، أو بمقتضى استخدام تدابير انفاذ القانون التي يتخذها مجلس الأمن[٥٠]

البند الأول: العقوبات المفروضة على كوريا الشمالية بسبب هجماتها السيبرانيةفي عصرنا الرقمي الذي يشهد تكاملاً متزايداً بين التكنولوجيا والأمن الدولي، أصبحت الهجمات السيبرانية أداة استراتيجية للدول غير الديمقراطية لتحقيق أهدافها السياسية والاقتصادية، وتُعد كوريا الشمالية نموذجاً بارزاً لهذا الاستخدام. منذ أوائل العقد الثاني من القرن الحادي والعشرين، أجرت بيونغ يانغ حملات سيبرانية واسعة النطاق، بما في ذلك سرقة بيانات حساسة، هجماتransomware ، وغسيل أموال عبر سرقة العملات المشفرة، مما أدى إلى خسائر اقتصادية هائلة تصل إلى مليارات الدولارات سنوياً. هذه الهجمات ليست مجرد جرائم إلكترونية، بل تمثل انتهاكاً للقانون الدولي، خاصة المادة ٢(٤) من ميثاق الأمم المتحدة التي تحظر استخدام القوة ضد سيادة الدول الأخرى، حيث يُعتبر الهجوم السيبراني الذي يسبب أضراراً جسيمة شكلاً من أشكال "القوة المسلحة" وفقاً للدليل التالييني ٢.٠ (٢٠١٧). في الرد على ذلك، فرضت المجتمع الدولي عقوبات متعددة على كوريا الشمالية، مدفوعة بقرارات مجلس الأمن مثل القرار ٢٣٩٧ (٢٠١٧)، الذي ربط العقوبات الاقتصادية مباشرة بأنشطة التصدير السيبراني، مما يعكس محاولة للردع من خلال حظر المعاملات المالية والتجارية، إلا أن فعاليتها تظل محل جدل بسبب قدرة النظام الكوري على التجنب عبر الوكلاء الدوليين[51].ومع ذلك، تكشف التطورات الأخيرة في عام ٢٠٢٥ عن تصعيد في هذه العقوبات، حيث ركزت الولايات المتحدة وشركاؤها على استهداف شبكات العمالة السيبرانية الكورية الشمالية التي تخترق الشركات الأمريكية لتمويل برنامجها النووي، كما في إعلان وزارة الخزانة الأمريكية في يوليو ٢٠٢٥ عن عقوبات على أفراد مثل سونغ كوم هيوك، المرتبط بمجموعة الاستطلاع الاستخباراتي الكورية. هذه العقوبات، المدعومة بقوانين مثل قانون مكافحة تمويل الإرهابCountering America's Adversaries Through Sanctions Act) ، (CAATSA 2017، تُعد امتداداً للإطار القانوني الدولي الذي يعتمد على مسودة لجنة القانون الدولي حول مسؤولية الدول (٢٠٠١)، والتي تنسب الأفعال السيبرانية إلى الدولة إذا كانت تحت سيطرتها الفعالة. ومع ذلك، يبرز التقرير السنوي للجنة الخبراء التابعة للأمم المتحدة أن كوريا الشمالية نجحت في سرقة أكثر من ٥٨ هجوماً على العملات المشفرة، مما يؤكد الحاجة إلى تعزيز التعاون الدولي لسد الفجوات في التنفيذ. في هذا البيان المفصل، سنستعرض تاريخ هذه العقوبات، آلياتها

القانونية، تأثيرها، والتحديات المرتبطة بها، مع الاستناد إلى مصادر دولية موثوقة لتوضيح كيفية تشكيلها للسياسة الدولية تجاه التهديدات السيبرانية[52].

أ. **الهجمات السيبرانية الرئيسية لكوريا الشمالية وأسبابها**بدأت كوريا الشمالية في بناء قدراتها السيبرانية في أوائل التسعينيات، مدعومة ببرنامج حكومي يُعرف بـ"وحدة ١٢١" التابعة لمكتب الاستطلاع الاستخباراتي الرئيسي(RGB) ، والتي تُعد مسؤولة عن معظم الهجمات الخارجية. أحد أبرز الأمثلة هو هجوم Sony Pictures عام ٢٠١٤، الذي أُسند إلى مجموعة Lazarus Group التابعة للجيش الكوري الشمالي، حيث سرقت بيانات شخصية لـ٤٧ ألف موظف وأُفرج عن أفلام غير مكتملة كرد على فيلم "The Interview" الذي يسخر من كيم جونغ أون. هذا الهجوم لم يكن مجرد انتقام سياسي، بل أدى إلى خسائر مالية تصل إلى ١٠٠ مليون دولار، وأثار ردوداً دولية أولية، بما في ذلك إدانة من مجلس الأمن التابع للأمم المتحدة، مستندة إلى المادة ٣٩ من الميثاق التي تُلزم المجلس بتحديد التهديدات للسلام الدولي. كما أن الهجوم انتهك اتفاقية بودابست بشأن الجرائم الإلكترونية (٢٠٠١)، التي وقعتها الولايات المتحدة وتُلزم الأطراف بالتعاون في مكافحة الجرائم السيبرانية، حيث يُعتبر سرقة البيانات جريمة عابرة للحدود[53].تلت ذلك هجمات أكثر تطوراً، مثل هجوم WannaCry في مايو ٢٠١٧، الذي أصاب أكثر من ٢٠٠ ألف جهاز في ١٥٠ دولة، بما في ذلك المستشفيات البريطانية، مسبباً تعطيلاً للخدمات الصحية وخسائر اقتصادية تقدر بـ٨ مليارات دولارأُسند الهجوم إلى مجموعة Lazarus بناءً على تشابه الرموز البرمجية مع هجمات سابقة، كما أكد تقرير FBI ، مما دفع الولايات المتحدة إلى فرض عقوبات فورية على ثلاثة كيانات كورية شمالية بموجب أمر تنفيذي ١٣٦٨٧ (٢٠١٥)، الذي يستهدف الأفراد المسؤولين عن الانتهاكات السيبرانية الخطيرة. من الناحية القانونية، يُصنف هذا الهجوم كـ"هجوم مسلح" وفقاً للدليل التالييني ٢.٠ (القاعدة ١١)، إذ أدى إلى أضرار جسيمة مشابهة للقصف التقليدي، مما يبرر الرد الجماعي تحت الفصل السابع من ميثاق الأمم المتحدة[54].في عام ٢٠١٦، نفذت كوريا الشمالية هجوماً على بنك بنغلاديش المركزي عبر نظامSWIFT ، محاولة سرقة مليار دولار، نجحت في نقل ٨١ مليون دولار إلى الفلبين والصين، وفقاً لتقرير لجنة الخبراء التابعة للأمم المتحدة. هذا الهجوم، الذي استخدم فيروس"Lazarus" ، كشف عن استراتيجية تمويل البرنامج النووي عبر الجرائم السيبرانية، مما أدى إلى توسيع قرار مجلس الأمن ٢٢٧٠ (٢٠١٦) ليشمل حظر الوصول إلى الأنظمة المالية الدولية. كما أن هجمات ٢٠٢٤–٢٠٢٥ على العملات المشفرة، مثل سرقة ٥٨ هجوماً بقيمة ٢ مليار دولار، أكدتها لجنة الخبراء، تعكس تطوراً في القدرات، حيث استخدمت مجموعات مثل Andariel وransomwareلاستهداف القطاع الصحي الأمريكي، مما أثار إدانات من CISA الأمريكية.أما في السنوات الأخيرة، فقد تحولت التركيز إلى عمليات "العمالة السيبرانية"، حيث يتسلل عمال كوريون شماليون إلى الشركات الأمريكية باستخدام هويات مزيفة لسرقة بيانات وتمويل النظام، كما في حملة ٢٠٢٥ التي كشفت عنها وزارة العدل الأمريكية في يونيو ٢٠٢٥، مشملة توظيفاً احتيالياً لأكثر من ١٠٠ شخص، مما أدى إلى سرقة تقنيات متقدمة. هذه العمليات تنتهك قانون الولايات المتحدة ٣١(North Korea Sanctions Regulations) CFR Part 510 ، الذي يحظر أي معاملة مالية مع كيانات كورية شمالية، وتعكس انتهاكاً لمبدأ "السيطرة الفعالة" في مسودة لجنة القانون الدولي.

ب. **آليات العقوبات الدولية وأسسها القانونية**تعتمد آليات العقوبات على الفصل السابع من ميثاق الأمم المتحدة، الذي يسمح بفرض إجراءات غير عسكرية للحفاظ على السلام، كما في القرار ١٧١٨ (٢٠٠٦) الذي أنشأ لجنة عقوبات على كوريا الشمالية بسبب برنامجها النووي، وتم توسيعه ليشمل النشاط السيبراني في قرار ٢٣٧٥ (٢٠١٧) الذي حظر تصدير أي تقنيات سيبرانية إلى كوريا الشمالية. هذه القرارات ملزمة بموجب المادة ٢٥ من الميثاق، وتشمل تجميد الأصول، حظر السفر، وحظر التجارة، مع التركيز على تمويل الإرهاب السيبراني كشكل من أشكال الانتشار النووي في الولايات المتحدة، يدير مكتب التحكم في الأصول الأجنبية (OFAC) العقوبات بموجب أوامر تنفيذية مثل ١٣٨١٠ (٢٠١٧)، التي تستهدف الكيانات المسؤولة عن التدخل السيبراني في الانتخابات، وتمتد إلى كوريا الشمالية من خلالCAATSA ، الذي يفرض عقوبات ثانوية على الدول التي تتعامل معها. أما الاتحاد الأوروبي، فيعتمد على نظام عقوباته السيبراني (٢٠٢٠) الذي يسمح باستهداف أفراد وكيانات، كما في عقوبات ٢٠٢١ على مجموعات روسية، وتم توسيعها لكوريا الشمالية في ٢٠٢٥ بالتعاون مع اليابان وكوريا الجنوبية.الدليل التالييني ٢.٠ يوفر إطاراً لتطبيق القانون الدولي الإنساني على العمليات السيبرانية، مشدداً على التناسب في الرد (القاعدة ١٤٩)، بينما تُلزم اتفاقية بودابست الدول بالتحقيق المشترك، لكن كوريا الشمالية غير موقعة عليها، مما يعيق التنفيذ[55].

ج. **العقوبات المحددة على كوريا الشمالية وتطورها**بدأت العقوبات السيبرانية المباشرة مع هجومSony ، حيث فرضت الولايات المتحدة عقوبات على وحدة ١٢١ في يناير ٢٠١٥، تجميد أصولها ومنع معاملاتها. تلتها قرارات الأمم المتحدة ٢٣٩٧ (٢٠١٧) التي حدت من النفط إلى كوريا الشمالية بنسبة ٩٠٪، مرتبطة بوقف النشاط السيبراني، مع تمديد المهمة الخبراء حتى ٢٠٢٤.في ٢٠٢٥، تصاعدت العقوبات مع إعلان OFAC

في يوليو عن استهداف ١٤ كياناً و١٤ فرداً في حملاتIT workers ، بما في ذلك Huione Group في كمبوديا كغسالة أموال، وفقاً لـ .FinCENكما فرضت الولايات المتحدة وشركاؤها عقوبات مشتركة في أغسطس ٢٠٢٥ على مجموعة Andariel لـ ransomwareعلى المستشفيات، مما أدى إلى إغلاق حسابات بنكية وتجميد أصول[56].أدت العقوبات إلى تقليل الوصول الكوري إلى الأسواق المالية بنسبة ٧٠٪، وفقاً لتقرير CSIS 2025 ، مما أجبر النظام على الاعتماد على الوكلاء في الصين وروسيا. اقتصادياً، خفضت من إيرادات السيبراني من ٢ مليار دولار في ٢٠٢٢ إلى ١.٢ مليار في ٢٠٢٥، لكنها لم توقف البرنامج النووي، كما يشير تقرير .CFR رغم الجهود، يتجنب النظام العقوبات عبر دول ثالثة، كما في استخدام عناوين IP صينية في هجمات ٢٠١٤–٢٠١٦. التحدي القانوني يكمن في صعوبة الإسناد، كما في الدليل التاليني، مما يعيق الإجماع في مجلس الأمن. كما أن عدم مشاركة كوريا الشمالية في الاتفاقيات يحد من الفعالية حيث تمثل العقوبات على كوريا الشمالية خطوة حاسمة في مكافحة التهديدات السيبرانية، مدعومة بإطار قانوني دولي قوي، لكنها تحتاج إلى تعزيز لمواجهة التجنب. مع استمرار التطورات في ٢٠٢٥، يظل التعاون المعزز مفتاحاً للردع الفعال، محافظاً على الاستقرار العالمي[57].

البند الثاني: العقوبات المفروضة على روسيا بسبب هجماتها السيبرانيةفي سياق التوترات الجيوسياسية المتصاعدة، أصبحت روسيا أحد أبرز اللاعبين في استخدام الهجمات السيبرانية كأداة لتحقيق أهدافها الاستراتيجية، مما أثار ردوداً دولية قوية عبر فرض عقوبات اقتصادية ومالية وتقنية. منذ غزو أوكرانيا في فبراير ٢٠٢٢، شهد العالم ارتفاعاً حاداً في الهجمات السيبرانية الروسية، التي شملت تعطيل البنية التحتية الحيوية، سرقة البيانات، ودعاية هجينة، مما أدى إلى خسائر اقتصادية تصل إلى مئات المليارات من الدولارات. هذه الهجمات ليست مجرد جرائم إلكترونية، بل تمثل انتهاكاً للقانون الدولي، خاصة المادة ٢(٤) من ميثاق الأمم المتحدة التي تحظر استخدام القوة ضد سيادة الدول، حيث يُصنف الهجوم السيبراني الذي يسبب أضراراً جسيمة كـ"استخدام قوة" وفقاً للدليل التاليني ٢.٠ (٢٠١٧). في الرد، فرضت الولايات المتحدة، الاتحاد الأوروبي، وحلف الناتو عقوبات واسعة النطاق، مدعومة بقرارات مجلس الأمن وقوانين وطنية مثل أمر التنفيذي ١٤٠٢٤ (٢٠٢١) الذي يستهدف الأنشطة الضارة الروسية، مما يعكس محاولة للردع من خلال تجميد الأصول وحظر التجارة، إلا أن فعاليتها تُقاس بقدرة روسيا على التكيف عبر الوكلاء والعملات المشفرة.[٥٨]مع تطور الوضع في عام ٢٠٢٥، تصاعدت العقوبات في ظل ارتفاع الهجمات بنسبة ٧٠٪ على أوكرانيا وحدها، حيث أصدرت وزارة الخزانة الأمريكية في يناير ٢٠٢٥ عقوبات إضافية على كيانات روسية مرتبطة بالـransomware، بينما أدانت إعلان مجلس الناتو في يوليو ٢٠٢٥ الأنشطة السيبرانية الروسية كتهديد للأمن المتحالف. هذه العقوبات، المدعومة بمسودة لجنة القانون الدولي حول مسؤولية الدول (٢٠٠١) التي تنسب الأفعال إلى الدولة إذا كانت تحت سيطرتها الفعالة، تُعد جزءاً من إطار أوسع لمكافحة الحرب الهجينة، لكنها تواجه تحديات في التنفيذ بسبب الغموض في الإسناد والتعاون الدولي المحدود. في هذا البيان المفصل، سنستعرض تاريخ الهجمات، آليات العقوبات، تأثيرها، والتحديات، مع الاستناد إلى مصادر قانونية وتقارير حديثة لتوضيح دورها في تشكيل السياسة الدولية تجاه التهديدات السيبرانية حتى سبتمبر ٢٠٢٥.[٥٩]

أ.**الهجمات السيبرانية الرئيسية لروسيا (٢٠٢٢–٢٠٢٥)**بدأت موجة الهجمات السيبرانية الروسية المكثفة قبل غزو أوكرانيا مباشرة في فبراير ٢٠٢٢، حيث نفذت مجموعات مثل APT28 (Fancy Bear) و APT44 (Sandworm) هجمات DDoS واسعة النطاق على مواقع حكومية أوكرانية، مما أدى إلى تعطيل الخدمات المصرفية والحكومية لساعات، كجزء من حملة هجينة لإضعاف القدرة الدفاعية. هذه الهجمات، التي شملت توزيع malware مثل NotPetya المُعدل، أثرت على أكثر من ٢٠٠ ألف جهاز عالمياً، مسببة خسائر اقتصادية تقدر بـ١٠ مليارات دولار، وأُسندت إلى الاستخبارات العسكرية الروسية (GRU) بناءً على تحليلات FBI و Microsoft، مما ينتهك اتفاقية بودابست بشأن الجرائم الإلكترونية (٢٠٠١) التي تُلزم الدول بالتعاون في التحقيق.[٦٠]في أغسطس ٢٠٢٢، استهدفت روسيا شبكات الطاقة الأوكرانية مرة أخرى، مستخدمة فيروس Industroyer2 لتعطيل محطات الكهرباء، مما أدى إلى انقطاع التيار عن ملايين المواطنين، كما حدث في ٢٠١٥–٢٠١٦، وفقاً لتقرير CERT–UA، وهو ما يُصنف كـ"هجوم مسلح" تحت القاعدة ١١ من الدليل التاليني، إذ يهدد الحياة المدنية. امتدت الهجمات إلى الغرب، حيث في أغسطس ٢٠٢٣، اخترقت مجموعة APT29 (Cozy Bear) لجنة الانتخابات البريطانية، مسروقة بيانات ملايين الناخبين، كما كشفت تحقيقات MI5، مما أثار مخاوف من التدخل في الانتخابات، ويُعد انتهاكاً لمبادئ القانون الدولي الانتخابي.مع تصاعد النزاع في ٢٠٢٤، ارتفعت الهجمات بنسبة ٧٠٪، حيث سجلت ٤٣١٥ حادثة على أوكرانيا وحدها، بما في ذلك حملة phishing في ديسمبر ٢٠٢٤ على القوات المسلحة الأوكرانية لسرقة بيانات Telegram، وهجمات DDoS على بنوك تشيكية وبورصة وارسو في أغسطس ٢٠٢٤ كرد على دعم أوروبا لأوكرانيا. في أكتوبر ٢٠٢٤، أرسلت روسيا تهديدات بالقنابل عبر البريد الإلكتروني إلى ٦٠ سفارة أوكرانية، بينما في نوفمبر ٢٠٢٤، هاجمت مواقع حكومية

كورية جنوبية بسبب مراقبتها لقوات كورية شمالية في أوكرانيا. وفي ٢٠٢٥، استمرت الهجمات مع spearphishing على دبلوماسيين كازاخستانيين في يناير، وDDoS على مواقع إيطالية، واختراق لأنظمة الانتخابات الرومانية في ديسمبر ٢٠٢٤، مما أدى إلى تسرب بيانات، كما يوثق تقرير CSIS الذي يسجل تضاعف الهجمات التخريبية الروسية بين ٢٠٢٣-٢٠٢٥.[٦١] هذه الهجمات، التي غالباً ما تُنسب إلى GRU أو FSB، ليست عشوائية بل جزء من استراتيجية "الحرب الظليلة"، كما يصفها تقرير CSIS مارس ٢٠٢٥، حيث تضاعفت الهجمات التخريبية ثلاث مرات بين ٢٠٢٣-٢٠٢٤، مستهدفة النقل والحكومات والطاقة، مما يهدد الاستقرار الأوروبي ويُعد انتهاكاً لاتفاقيات جنيف الإضافية (١٩٧٧) التي تحمي المدنيين في النزاعات.[٦٢]

ب. **آليات العقوبات الدولية وأسسها القانونية** تعتمد آليات العقوبات على الفصل السابع من ميثاق الأمم المتحدة، الذي يسمح بإجراءات للحفاظ على السلام، كما في قرارات مجلس الأمن المتعلقة بأوكرانيا، لكن التركيز السيبراني يأتي من آليات وطنية وإقليمية. في الولايات المتحدة، يدير OFAC العقوبات بموجب أمر تنفيذي ١٣٦٩٤ (٢٠١٥) الذي يستهدف الأنشطة السيبرانية الضارة، و14024 EO (٢٠٢١) للأنشطة الروسية الضارة، و14144 EO (٢٠٢٥) لتعزيز الابتكار السيبراني، مما يشمل تجميد الأصول وحظر السفر. هذه الأوامر مدعومة بقانون CAATSA (٢٠١٧) الذي يفرض عقوبات ثانوية على المتعاملين مع روسيا، وRuHSR (٢٠٢٢) الذي يوسع على الأنشطة الضارة.في الاتحاد الأوروبي، أُنشئ نظام عقوبات سيبرانية في ٢٠٢٠، مُوسع في ٢٠٢٢ ليشمل الهجمات الهجينة، كما في اللائحة 2022/1270 (EU) التي تستهدف أفراداً وكيانات مسؤولة عن هجمات على أوكرانيا، مع تجميد أصول وحظر سفر، بناءً على المادة ٢٩ من معاهدة الاتحاد الأوروبي. حلف الناتو، من جانبه، أدان في يوليو ٢٠٢٥ الأنشطة السيبرانية الروسية كتهديد، وأصدر إرشادات للرد الجماعي تحت المادة ٥ إذا اعتبرت هجوماً جماعياً، كما في بيان NAC.الدليل التالييني ٢.٠ يوفر إطاراً لتطبيق القانون الدولي، مشدداً على التناسب (القاعدة ١٤٩) والإسناد تحت مسؤولية الدول (المادة ٨ من مسودة ILC)، بينما تُلزم اتفاقية بودابست الدول بالتعاون، لكن روسيا غير موقعة كاملة، مما يعيق التنفيذ.[٦٣]

ج. **العقوبات المحددة على روسيا وتطورها** بدأت العقوبات السيبرانية المباشرة مع SolarWinds في ٢٠٢٠، لكن التصعيد جاء بعد ٢٠٢٢، حيث فرضت الولايات المتحدة في مارس ٢٠٢٢ عقوبات على APT28 وAPT29 بموجب 14024 EO، تجميد أصولها. في ٢٠٢٣، أضاف OFAC عقوبات على GRU للهجمات على أوكرانيا، وفي فبراير ٢٠٢٥، استهدفت بنية تحتية ransomware روسية، كما في إعلان State Department.في ٢٠٢٥، تصاعدت مع يناير Treasury sanctions على كيانات لدعم أوكرانيا، وأغسطس sanctions على منصات عملات مشفرة تساعد روسيا في تجاوز العقوبات. الاتحاد الأوروبي وسع عقوباته في ٢٠٢٥ لتشمل hybrid threats، كما في تحديثات سبتمبركما أدت العقوبات إلى انخفاض الصادرات الروسية بنسبة ٤٠٪، وتجميد ٣٠٠ مليار دولار من احتياطياتها، مما أثر على قدراتها السيبرانية بسبب نقص التكنولوجيا، كما في تقرير UK Parliament 2025. سياسياً، عززت التعاون الغربي، لكن روسيا ردت بتهديدات، كما في تصريحاتها سبتمبر ٢٠٢٥. كما يواجه التنفيذ صعوبات في الإسناد، كما في الدليل التالييني، وتجنب روسيا عبر الصين، مما يقلل الفعالية. كما أن تعليق الولايات المتحدة لعملياتها السيبرانية الدفاعية في مارس ٢٠٢٥ أثار جدلاً حيث تمثل العقوبات على روسيا خطوة حاسمة في مكافحة الهجمات السيبرانية، مدعومة بإطار قانوني دولي، لكنها تحتاج إلى تعزيز لمواجهة التكيف. مع استمرار التهديدات في ٢٠٢٥، يظل التعاون المعزز مفتاحاً للردع، محافظاً على الاستقرار العالمي.[٦٤]

المطلب الثاني: التقييم النقدي لفعالية العقوبات

دون شك، إن انتشار الهجمات السيبرانية الضارة والمدمرة بعد ٢٠١١ دولياً يعود الى ضعف المنظومات الامنية السيبرانية في دول العالم؛ الأمر الذي جعل تهديد السلم والأمن الدوليين مر وارد دائماً، إذ ظهرت هذه الهجمات في حالات عديدة منها ثورات التغيير العربية (الربيع العربي) استونيا و ايران واتضحت اكثر في الحرب الروسية – الأوكرانية، فضلاً عن تسريبات أوراق بنما، وواقعة اختراق وكالة أبحاث الإنترنت الروسية، إلى جانب نشر وسائل الإعلام تفاصيل منزل الرئيس الروسي فلادمير بوتين، مع توسع هذه الهجمات، بدا التساؤل المطروح، لماذا لا يوجد نظام مساءلة ومحاسبة دولي للحد من هذه الهجمات السيبرانية؟لذلك، تكمن اهمية القوانين السيبرانية في إنها؛ تفرض إجراءات للاستخدام وتقيس وردود الفعل العام في الفضاء السيبراني، وترتفع نسبة الامان والحماية للمعاملات التي تجرى عبر الإنترنت، وتخضع جميع الأنشطة عبر الإنترنت للمراقبة من قبل مسؤولي القانون السيبراني، وتوفير الحماية لجميع البيانات والممتلكات الخاصة بالأفراد والمنظمات والحكومة، ويساعد في الحد من الأنشطة السيبرانية غير القانونية عن طريق بذل الرقابة والعناية الواجبة من قبل مؤسسات الدولة المختصة، وردود الفعل التي يتم قياسها على أي فضاء إلكتروني لها زاوية قانونية مرتبطة بها تختلف باختلاف توجهها، سواء كان يتعلق بالتجارة أو بالخدمات أم الامن بمختلف انواعه، ووجود

قوانين سيبرانية يعني وجود اتفاقيات دولية في هذا المجال مما يتيح تتبع جميع السجلات الإلكترونية عن طريق تحقيق التعاون الدولي لتتبع الجرائم المنظمة، ويساعد على إنشاء الحوكمة الإلكترونية والتي بدورها ترفع جودة حياة المستفيدين من خدمات الحكومة الالكترونية[٦٥]مما لايمكن نكرانه هو الآثار الناجمة عن النزاعات و الحرب السيبرانية ومن عواقب وخيمة على المدنيينفهناك ضرورة لتطبيق القانون الدولي على العمليات السيبرانية في النزاعات المسلحة والحروب، لوجود ضرر على المؤسسات والافراد وانتهاك للامن وسيادة الدول [٦٦].وهنا نستذكر "مبدأ التمييز وحظر الهجمات العشوائية وغير المتناسبة"، يتطلب مبدأ التمييز أن تميز أطراف النزاعات دوماً بين المدنيين والمقاتلين، وبين الأهداف المدنية والأهداف العسكرية، ففي اطار تطبيق مبدأ التميز على الهجمات السيبرانية اشار دليل تالين، بالرغم من عدم الزامية قواعده، بأنه لا يجوز أن تكون الاعيان المدنية هدفاً للهجمات السيبرانية، فلا يجوز على سبيل المثال توجيه الهجمات السيبرانية التي من شأنها تدمير الأنظمة المدنية والبنية التحتية، ما لم تعج هذه الأنظمة من قبيل الأهداف العسكرية التي يجوز استهدافها وفقاً للظروف السائدة [٦٧] .**البند الأول: تأثير العقوبات على سلوك الدول** إن الإسناد هو الخطوة الأولى لتحقيق الأمن السيبراني، لكنه لا يكفي، فربما تعلم الامم المتحدة جيداً من هو المسؤول لكنها لا تتخذ أي إجراء فعلي، إذ يتطلب الأمر اتخاذ قرار عن طريق مجلس الامن وبطلب من الدولة المعتدى عليها، فيما يتعلق بالتدابير الحالية، فلا يمكن التغافل عن بعض الجهود الدولية المبذولة لتحقيق المساءلة، وتحديد شروط العمل الجماعي والاتفاق عليها، مثل، إطار الاستجابة الدبلوماسية السيبرانية في الاتحاد الأوروبي، والقانون الدولي للفضاء السيبراني، والالتزامات التعهدية الأخرى للدفاع الجماعي عن النفس، والبيان المشترك الصادر عن وزارة الخارجية الأمريكية في سبتمبر ٢٠١٩ بشأن تعزيز سلوك الدولة المسؤولة في الفضاء الإلكتروني، إذ اتفقت (٢٨) دولة على العمل معاً على أساس طوعي لمحاسبة الدول عندما تتصرف بشكلٍ مخالف عن طريق اتخاذ تدابير وفقاً لقانون الدولي، بهدف توسيع مراعاة معايير ٢٠١٥ وزيادة الأمن السيبراني، أضف لذلك إلى العقوبات من قبل الاتحاد الأوروبي أو لوائح الاتهام والعقوبات من قبل الولايات المتحدة الامريكية.إن التأكيد على إن القانون الدولي الإنساني بما في ذلك مبادئ التمييز والتناسب والاحتياط –ينطبق على العمليات السيبرانية اثناء النزاعات المسلحة بموجب أحكامه، ومنها[68] :

١. يحظر استخدام القدرات السيبرانية العشوائية الطابع التي تصنف على أنها أسلحة.

٢. يحظر توجيه الهجمات المباشرة ضد المدنيين والاعيان المدنية، بما فيذلك عند استخدام وسائل أو أساليب الحرب السيبرانية.

٣.حظر أعمال العنف أو التهديد إلىً الرامية أساس بث الرعب بين السكان المدنيين، بما في ذلك عند ارتكابها عبر وسائل أو أساليب الحرب السيبرانية.

٤.حظر الهجمات العشوائية، أي الهجمات التي من شأنها أن تصيب الاهداف العسكرية والاشخاص المدنيين أو الاعيان المدنية دون تمييز، بما في ذلك عند استخدام وسائل أو أساليب الحرب السيبرانية.

٥.حظر الهجمات غير المتناسبة، بما في ذلك عند استخدام وسائل أو أساليب الحرب السيبرانية، الهجمات غير المتناسبة هي تلك التي توقع منهُ اي أن تسبب خسائر عرضية في أرواح المدنيين أو إصابة بهم أو بالاعيان أضرار المدنية أو أن دت امن هذه الخسائرً حدث خلط والاضرار، يفرط فيتجاوز ما ينتظر أن تسفر عنه تلك الهجمات من ميزة عسكرية ملموسة ومباشرة.

٦.حظر مهاجمة أو تدمير أو نقل أو تعطيل الاعيان التي لا غنى عنها لبقاء السكان المدنيين، بماُ في ذلك عند استخدام وسائل أو أساليب الحرب السيبرانية.

٧.يجب حماية الوحدات الطبية واحترامها، بما في ذلك عند تنفيذ العمليات السيبرانية اثناء النزاعات المسلحة.[٦٩]

بذل رعاية متواصلة في إدارة العملياتُ العسكرية، بما في ذلك عند استخدام وسائل أو أساليب الحرب السيبرانية، من أجل تفادي السكان المدنيين والاعيان المدنية؛ و تتخذ جميع الإحتياطات المستطاع عند تنفيذ الهجمات من أجل تجنب إلحاق الضرر بالمدنيين، وذلك بصفة عرضية، بما في ذلك عند استخدام وسائل أو أساليب الحرب السيبرانية انطلاقاً من مقولة كوردولا دروغيه المستشارة القانونية في اللجنة الدولية "ما من فراغ قانوني في الفضاء السيبراني"[٧٠]، ففي كل أرجاء العالم، ينظر واضعو السياسات والقادة العسكريون في تداعيات الحرب السيبرانية، وتشرح السيدة "كوردولا دروغيه" المستشارة القانونية في اللجنة الدولية أن الإطار القانوني القائم واجب التطبيق ويجب احترامه حتى في الفضاء السيبراني، اذ تصفه بالسلوك الالكتروني الذي يؤدي الى إحداث أثر في "العالم الحقيقي"، ولم يجرِ الاتفاق دولياً بالمثل على معنى قانوني لعبارات مثل "الهجمات السيبرانية" أو "العمليات السيبرانية" أو "الهجمات على شبكات الحواسيب"، التي يقصد بها الهجمات والنزاعات والحروب عبر الاجهزة الالكترونية[٧١]

وان من اخطر استعمالاتها ضد النزاع في كوسوفو١٩٩٩ من قبل حلف الشمال الاطلسي، وبعد استهداف طيران حلف شمال الأطلسي للسفارة الصينية في بلغراد، قام عدد من القراصنة الصينيين وكردة فعل بمهاجمة مواقع الكترونية رسمية منتخبة تابعة للولايات المتحدة الأمريكية، وبالذات الموقع الإلكتروني للبيت الأبيض نجم عنها الاستحواذ على آلاف من البيانات الرقمية المنصفة آنذاك بأنها عالية السري[٧٢]وهناك الهجوم السيبراني الذي تعرض له المفاعل النووي الأمريكي "ديفيد بيس" لتوليد الطاقة الكهربائية في أوهايو في٢ جوان ٢٠٠٣ بفعل أنظمة اختراق وتعطيل لشبكات السيطرة والتحكم الالكترونية في المفاعل نفسه [٧٣]ومن المعروف إن القانون الدولي الإنساني لا ينطبق إلا إذا ارتكبت العمليات السيبرانية في سياق نزاع مسلح، أكان بين دول أم بين دول وجماعات مسلحة منظمة، أو بين جماعات مسلحة منظمة[٧٤]، وبالنتيجة، هناك حاجة إلى التمييز بين لمسألة العامة للأمن السيبراني وبين المسألة الخاصة بالعمليات السيبرانية في النزاع المسلح، ففي حالات النزاعات المسلحة، ينطبق القانون الدولي الإنساني عندما تلجأ الأطراف إلى أساليب الحرب ووسائلها التي تعتمد على عمليات سيبرانية[٧٥].إن استخدام العمليات السيبرانية أثناء النزاعات المسلحة حقيقة واقعة، فبينما أقر عدد ضئيل من الدول علانية بإجراء مثل هذه العمليات، مع تزايد عدد الدول التي تطور قدرات سيبرانية لأغراض عسكريةً فمن المرجع أن يزداد استخدامها مستقبلا.[٧٦]وتُطور دوماً تكنولوجيات جديدة من كل الأنواع، والقانون الدولي الإنساني شامل بما يكفي ليتسع لهذه التطورات، غير أنه ينظم، عن طريق قواعده العامة، كلّ أساليب الحرب ووسائلها، بما فيها استخدام كلّ الأسلحة، ولا سيما أن المادة (٣٦) من الملحق (البروتوكول) الأول الإضافي لاتفاقيات جنيف تنص على ما يلي: "يلتزم أي طرف سام متعاقد، عند دراسة أو تطوير أو اقتناء سلاح جديد أو أداة للحرب أو اتباع أسلوب للحرب، بأن يتحقق مما إذا كان ذلك محظوراً في جميع الأحوال أو في بعضها بمقتضى هذا الملحق "البروتوكول" أو أية قاعدة أخرى من قواعد القانون الدولي التي يلتزم بها الطرف السامي المتعاقد"، وفي ما يتعدى نطاق الالتزام المحدد الذي تفرضه هذه القاعدة على الدول الأطراف، تبين أن القواعد العامة للقانون الدولي الإنساني تنطبق على التكنولوجيا الجديدة[٧٧].وهذا لا يعني أنه لا توجد حاجة إلى زيادة تطوير القانون في حين تتطور التكنولوجيات، أو أن آثارها الإنسانية مفهومة على نحو أفضل، ويجب أن تقرر الدول هذا الأمر، وان لم تقرر بعد، فمن الضروري التشديد على أنه ما من فراغ قانوني في الفضاء السيبراني، وبعيداً عن ذلك[٧٨].غير أن الفواعل مجهولة الهوية تشكل جانباً من جوانب صعوبة تحميلاً المسؤولية في الفضاء السيبراني، ففي العمليات السيبرانية التي تحصل يومياً، جهل الهوية قاعدة وليس استثناء، ويتبين أنه من المستحيل في بعض الحالات اقتفاء أثر المصدر؛ كون الفاعل شخص فيطبق عليه القانون الدولي الإنساني ، او مؤسسة حكومية ليطبق القانون الدولي العام[٧٩].ويجدر التوضيح أن التأكيد على انطباق القانون الدولي الانساني على العمليات السيبرانية اثناء النزاعات المسلحة لا يضفي الشرعية على الحرب السيبرانية أو يشجع على عسكرة الفضاء السيبراني، في الواقع، يفرض القانون الدولي الإنساني بعض القيود على عسكرة الفضاء، وعلاوة على ذلك، يظل أي لجوء إلى القو من الدول السيبرانية عن طريق حظر تطوير القدرات السيبرانية العسكرية التي تنتهك القانون الدولي الإنساني ذات الطابع السيبراني أو الحركي محكوم بميثاق الامم المتحدة وقواعد القانون الدولي العرفي ذات الصلة، لا سيما حظر اللجوء للقوة، و يجب تسوية النزاعات الدولية بالوسائل السلمية، في الفضاء السيبراني كما في جميع المجلات الاخرى[٨٠].

وصدر تقرير فريق الخبراء عام ٢٠٢١ متضمناً مجموعة من المبادئ حول تطبيق القانون الدولي العام على العمليات التي تقوم بها الدول في الفضاء السيبراني، وكان لمنظمة الأمم المتحدة الدور الاساس في تشكيل الفريق والذي ساهم في اعداد هذه المبادئ، وهو ما يبين اهمية دور المنظمة في تكوين قواعد متكاملة لما يخص التهديدات التي فرضها الفضاء السيبراني على الامن والسلم الدوليين.

البند الثانى: دور الامم المتحدة في تقنين الفضاء السيبرانيما إن بلغ عدد سكان العالم (٧.٩) مليار نسمة حسب إحصائيات الأمم المتحدة وأكثر من نصف هذا العدد يستخدم الانترنت، ليس ذلك فحسب، بل إن محرك كوكل وحده يستقبل يوميا (٣.٥) مليار بحث في المتوسط، وعدد الأجهزة المتصلة بالإنترنت يتوقع أن يبلغ (٥٠) مليار جهاز في سنوات قليلة، أضف إلى ذلك أن منصة فيسبوك يستخدمها في الشهر أكثر من(٢.٩) مليار مستخدم وفي اليوم أكثر من (١.٩) مليار شخص، حتى ازدادت الهجمات والنزاعات والحروب السيبرانية والاعمال العدوانية الاخرى من الكراهية والابتزاز والتجارة الالكترونية غير المشروعة في الفضاء السيبراني[٨١].مما دعى منظمة الأمم المتحدة في عام ٢٠١٥ لوضع معايير محددة لمواجهة الهجمات السيبرانية، وتم الاتفاق عليها في عام ٢٠٢١ بالإجماع من قبل جميع أعضاء دول منظمة الأمم المتحدة، من أجل وضع إطار ملزم سياسياً لجميع الدول التي تستخدم الفضاء الإلكتروني، من ضمن هذه المعايير أن تتعهد الدول بمنع استخدام شبكات الإنترنت في الأعمال التي تهدد أو تضر بالسلم والأمن الدوليين، وعدم السماح عن قصد باستخدام أراضيها في أفعال غير مشروعة.وأظهرت التجربة الدولية أن الاتفاق على المعايير والقواعد السيبرانية الدولية لا يكفي في حد ذاته لتحقيق الأمن السيبراني، بل يجب تطوير استراتيجية دبلوماسية جماعية لمراقبة تنفيذ هذه المعايير، وفرض العقوبات عند تجاوزها، وهذا يتطلب حراك في السياسة الدولية لتفعيل النظام القانوني في

الفضاء السيبراني.ومن أوجه القصور في المعايير التي وافقت عليها الأمم المتحدة هو افتقارها إلى القدرة على المساءلة عن الهجمات السيبرانية الضارة– الخبيثة، فمن الناحية النظرية، يعد اتخاذ أي إجراء فعلي مسؤولية المجتمع الدولي الذي يعمل عن طريق مجلس الأمن التابع للأمم المتحدة. ولكن الواقع يشير إلى إن التوصل إلى اتفاق داخل الأمم المتحدة لمواجهة الأنشطة الإلكترونية غير القانونية والتي تنافي الشرعية الدولية والتي توصف بالعدوانية أمراً محدوداً للغاية، وذلك لأن المجتمع الدولي يتحرك فقط عندما تستخدم القوة، وهو أمر غير متوفر في الهجمات الإلكترونية، فلم يحدث أن تسبب هجوم إلكتروني في وفاة أحد الأشخاص.لهذا السبب، لم تُطرح قضية الأمن السيبراني أمام مجلس الأمن الدولي حتى عام ٢٠٢٠، مما يجعلها قضية غير خطيرة في رأى معظم الدول الأعضاء غير المُشاركة بشكلٍ مباشر في الصراع السيبراني، لكن هذا الوضع بدأ يتغير مع زيادة مخاطر الأنشطة الإلكترونية غير المشروعة، وتزايد الاعتماد على الشبكات العالمية، وتطور المنافسة بين القوى العظمى، وللتغلب على هذه المشكلة، يرى القائمون على الامم المتحدة ضرورة القيام ببعض الإجراءات المتسقة مع القانون الدولي والمعايير المتفق عليها، من أجل خلق المساءلة الدولية لمواجهة الهجمات الإلكترونية؛ كونها قضايا خطيرة [٨٢].والإشكالية هي إسناد قضايا الأمن السيبراني لكيان مستقل تابع لجهة خارجية لن يحظى بالدعم الدولي، إذ أظهرت المناقشات في هذا الخصوص صعوبة التحقيق مع قوى إلكترونية كبرى مثل، الصين أو الولايات المتحدة الامريكية لكنها مع ذلك أبدت استعدادها للتحقيق مع عدد قليل من الدول الضعيفة، مثل كوريا الشمالية أو مع مجرمي الإنترنت، إذا كان من الممكن تحديد أنهم لا يتصرفون بصفة وكيل لدولة ما، فمن ضمن التحديات التي تواجه المعايير المقدمة عام ٢٠١٥ أنها تدعو جميع الدول للمشاركة في التحقيق اللازم لتوضيح ملابسات الهجوم الإلكتروني، مما يجعل الإسناد مهمة معقدة، لأنه في حالة وقوع حادث إلكتروني سيتطلب من الدول الإفصاح عن جميع المعلومات ذات الصِلة بالحادث، ومن المتوقع أن تعترض الدول على هذا التدخل، فالاقتراح الروسي الذي قدم ينص على أن تكون هناك حدود للاعتراضات المحتملة من الدول المعنية في حالة إسناد حادث إلكتروني إلى دولة بعينها أو توجيه الاتهام لها، وبالطبع، ستنكر الصين وروسيا (أو على الأرجح أي قوة إلكترونية) الاتهام لكن الهدف ليس إقناعهما بقبول الاتهام وإنما إقناع القادة الوطنيين والجمهور العالمي، أما فيما يتعلق بالشركات الخاصة مثل شركات FireEye أو Cloudstrike، فلديها حالياً قدرة على كشف مصدر الهجوم السيبراني العدائي، لكن هذا التقدم في تحديد المصدر غير معترف به في المجتمع الدولي، فلا يوجد اتفاق حول مستوى الإسناد المطلوب للعمل التعاوني بين الدول[٨٣].ويحظى هذا الاستنتاج بدعم قوي في فتوى محكمة العدل الدولية بعنوان "مشروعية التهديد بالاسلحة النووية أو استخدامها"، حيث أشارت المحكمة إلى أن المبادئ والقواعد الثابتة للقانون الدولي الانساني السارية في النزاعات المسلحة تنطبق "على كافة أشكال الحرب وعلى كافة أنواع وتر اللجنة الدولية أن هذا الاستنتاج ينطبق على استخدام العمليات السيبرانية اثناء النزاعات المسلحة [٨٤].لهذا يجب على الطرف المسؤول عن هجوم ما اتخاذ التدابير، إلى أقصى قدر ممكن، من أجل تفادي أو تخفيف الضرر العرضي الذي يلحق بالبنية التحتية المدينة أو يؤذي المدنيين. وهذا سيتطلب التحقق من طبيعة النظم التي تتعرض للهجوم والأضرار المحتملة التي تنجم عن أحد الهجمات، وهذا يعني أنه عندما يصبح جلياً أن هجوماً سيتسبب بإصابات أو أضرار مدنية عرضية، يجب إلغاؤه.علاوة على ذلك، يجب على أطراف النزاعات أن تلتزم باتخاذ الاحتياطات اللازمة من آثار الهجمات، ونتيجة لذلك، تكون النصيحة الموجهة إلى هذه الأطراف هي تقييم ما إذا كانت نظم الحواسيب العسكرية منفصلة بما يكفي عن تلك المدنية، بغية حماية السكان المدنيين من آثار الهجمات العرضية، ويُمكن للاعتماد على نظم الحواسيب العسكرية والتوصيل بين نظم الحواسيب التي يديرها متعاقدون مدنيين وتُستخدم أيضاً لأغراض مدنية أن يثير القلق.وعلى صعيد آخر، قد تساهم تكنولوجيا المعلومات أيضاً في الحد من الأضرار العرضية التي تلحق بالمدنيين أو البنية التحتية المدنية، وعلى سبيل المثال، يلحق تعطيل خدمات معينة تُستخدم لأغراض عسكرية ومدنية أضراراً أقل مما يُلحق تدمير البنية التحتية تماما، وفي هذه الحالات، يفرض مبدأ الاحتياط القابل للجدل التزاماً على الدول باختيار الوسائل الأقل ضرراً بغية تحقيق أهدافها العسكرية، وفي الحالات التي لا تشملها القواعد الحالية للقانون الدولي الإنساني، يظل المدنيون والمقاتلون محميين بما يسمى"شرط مارتنز"، مما يعني أنهم يظلون تحت حماية وسلطان مبادئ القانون الدولي كما استقر بها العرف، و مبادئ الإنسانية، وما يمليه الضمير العام"[٨٥]وشهدت هذه المرحلة بدايات ظهور الشبكة الدولية للمعلومات إذ يرجع ضهورها لعام ١٩٩١ بجهود العالم البريطاني "تيم بيرنرز لي" اثناء عمله في المنظمة الاوروبية للبحوث النووي [٨٦]، وكان اول هجوم الكتروني ممكن أن يهدد الامن والسلم الدوليين في شهر ايار من عام ١٩٩٨ ، إذ قام به مجموعة قراصنة من الصين تطلق على نفسها "مركز الرد السريع للقراصنة الصينيين" مؤلف ٣٠٠٠ قرصان الكتروني بالهجوم على المواقع الالكترونية الحكومية لأندونسيا بسبب انتشار مظاهرات في ومن هذه الحادثة ادرك القائمون على منظمة الامم المتحدة الخطر الحقيقي لذي من الممكن أن تشكله إندونيسيا ضد الصين [٨٧].وأزداد الاهتمام الدولي بعد الطرح الروسي موضوع علاقة تطورات الانترنت بالأمن الدولي أمام الجمعية العامة عام ١٩٩٨ بطلب من قبل روسيا الاتحادية، إذ قررت الجمعية

العامة أن تدرج في جدول اعمالها هذا الموضوع تحت عنوان "التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الامن الدولي "وطلبت فيه من الدول ابداء آرائها [٨٨].واستجابت الأمم المتحدة لذلك بإنشاء أول فريق خبراء عام ٢٠٠٤، واستمرت اجتماعاته لمدة تزيد عن السنتين بين عامي ٢٠٠٤ و ٢٠٠٥، إلا إنه لم يتوصل الى توافق بشأن المبادئ الواجب إتباعه الصعوبة الرقابة والتجريم في هذا المجا وعد اعارة الاهتمام الدولي الكافي له بوصفه لا يرتقي الا عدوان أو تهديد حقيقي[٨٩]، إلا إن عامي ٢٠٠٦ –٢٠٠٧ شهدت تزايد الهجمات السيبرانية كان أهمها في استونيا عام ٢٠٠٦ التي عطلت معظم مرافقها ونتيجة الدولة تلت ذلك حوادث مماثلة في جورجيا٢٠٠٨ وكانت الاتهامات موجهة الى روسيا لكنها دون اثبات[٩٠]. ولأضرار التي لحقت بإستونيا دفعها لطلب في عام ٢٠٠٧ من الامم المتحدة إدانة هذه الهجمات وإعطاء أهمية أكبر للقواعد التي تنظم السلوك السيبراني للدول[٩١]، وفعلاً قررت الجمعية العامة انشاء فريق ثاني عام٢٠٠٩ يتكون من خمسة عشر عضوا[٩٢١٥]، وكلا الفريقين عقد اجتماعات من ٢٠٠٩ الى ٢٠١٠ ثم تبعه فريق ثالث باشر بالعمل من ٢٠١٢ الى ٢٠١٣ مطولة وتفصيلية من غير التوصل الى مبادئ عن السلوك السيبراني[٩٣] سوى الاشارة الى "ضرورة مواصلة الحوار لمناقشة المعايير المتعلقة باستخدام الدول لتكنولوجيا المعلومات والاتصالات" [٩٤]،استطاع التوصل الى مبادئ اولية لقواعد السلوك إلا إن الفريق الرابع الذي شكلته المنظمة عام٢٠١٤[٩٥]، وضح إن الدولة التي تقوم بعمل معادٍ تتحمل المسؤولية الدولية بعد اثبات قيامها بالفعل في الفضاء السيبراني، إذ نص التقرير للمرة الأولى إن القانون الدولي ينطبق على الفضاء السيبراني[٩٦]، وتشكل الفريق الخامس عام ٢٠١٦ يكمل عمل الفريق السابق[٩٧]، لكنه أعلن عدم استطاعته للتوصل الى توافق بشأن المبادئ الاولية للسلوك[٩٨]، أنشأت فريقاً سادساً على اساس التوزيع الجغرافي العادل للدول في٢ كانون الثاني٢٠١٩ وبعد اجتماعات لمدة سنتين وظهور بوادر توافق سياسي بين الدول الأطراف استطاع الفريق أن يصدر[٩٩]تقرير نهائي بالتوافق بين جميع اعضاءه وتضمن للمرة الأولى معايير السلوك المقبول في الفضاء السيبراني في ١٤ تموز عام ٢٠٢١ إلا إن هذه المرحلة شهدتً أنشاء فريق خبراء ثاني وباقتراح من روسيا الاتحادية، وأطلق عليه (الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق جميع أعضاء الجمعية العامة للأمم المتحدة[١٠٠].ومن هنا نستنتج امكانية تطبيق المبادئ التقليدية على الفضاء السيبراني مثل (مبدأ احترام السيادة في الفضاء السيبراني، ومبدأ عدم استخدام القوة في العلاقات الدولية السيبرانية، ومبدأ حل المنازعات السبرانية بالطرق السلمية، ومبدأ عدم التدخل في الشؤون الداخلية سيبرانياً، وضع قواعد تخص الفضاء السيبراني الدولي، مبدأ التعاون الدولي في الفضاء السيبراني، ومبدأ التحقيق في القضايا السيبرانية، ومبدأ احترام حقوق الانسان في المجال السيبراني.وتعليل ضرورة التطبيق ظهور وانتشار قواعد إقليمية منافسة للقانون الدولي العام لتنظيم القواعد السيبرانية اقليمياً، فهناك حالياً ثالث مجموعات للقواعد التي تنظم موضوع خضوع الانترنت مثل:

١. قواعد (Tallinn) للقانون الدولي في الفضاء السيبراني ٢٠١٧ والتي تتكون من (١٥٤) قاعدة قانونية[١٠١].

٢. قواعد باريس (Paris Call) لعام ٢٠١٨، تتكن من (٩) مبادئ لتنظيم الفضاء السيبراني ، انضمت لها (٨١) دولة[١٠٢].

٣. واعد شنغهاي لعام ٢٠١٥ ، والذي اطلقته منظمة شنغهاي لتنظيم العمل في الفضاء السيبراني[١٠٣]

البند الثالث: الآثار الجانبية للعقوبات على المدنيينفي عالم يتسارع فيه التحول الرقمي، أصبحت الهجمات السيبرانية أداةً حاسمة في الصراعات الدولية، حيث تتجاوز حدود الجغرافيا التقليدية لتصيب البنى التحتية الحيوية والأنظمة الاقتصادية دون إراقة دماء مباشرة. في هذا السياق، برزت العقوبات الاقتصادية كوسيلة رد فعل شائعة من قبل الدول والمنظمات الدولية لردع الجهات المسؤولة عن هذه الهجمات، مثل الولايات المتحدة والاتحاد الأوروبي اللتين فرضتا عقوبات على كيانات روسية وصينية متهمة بشن هجمات سيبرانية. ومع ذلك، فإن هذه العقوبات، التي تُصمم أصلاً لاستهداف النخب الحاكمة أو الجهات العسكرية، غالباً ما تتجاوز حدودها لتصيب المدنيين بشكل غير مباشر، مما يثير تساؤلات عميقة حول فعاليتها وتوافقها مع القانون الدولي. يهدف هذا التقييم النقدي إلى استكشاف الآثار الجانبية لهذه العقوبات على المدنيين، مع التركيز على سياق الهجمات السيبرانية، مستنداً إلى مواد القانون الدولي مثل ميثاق الأمم المتحدة واتفاقيات جنيف، بالإضافة إلى دراسات حالة وتقارير بحثية. من خلال تحليل هذه العناصر، يبرز التقييم أن العقوبات، رغم دورها في فرض التكاليف، تفشل في الردع الفعال للهجمات السيبرانية وتؤدي إلى معاناة إنسانية غير مبررة، مما يدعو إلى إعادة التفكير في آليات الرد الدولي.يُعرف القانون الدولي العقوبات الاقتصادية كإجراءات غير عسكرية تُفرض لتغيير سلوك الدول أو الكيانات، وفقاً للمادة ٤١ من ميثاق الأمم المتحدة، التي تمنح مجلس الأمن الصلاحية في اتخاذ "إجراءات تتضمن إجراءات تكميلية أو كاملة للعلاقات الاقتصادية مع أي دولة" دون اللجوء إلى استخدام القوة المسلحة. هذه المادة، التي أُدرجت في الفصل السابع من الميثاق، تهدف إلى الحفاظ على السلام الدولي من خلال فرض ضغوط اقتصادية جماعية، لكنها لا تُحدد آليات واضحة للحماية من الآثار الجانبية على المدنيين. في سياق الهجمات السيبرانية، التي غالباً ما تُصنف كتهديدات للسلام الدولي بموجب المادة ٣٩ من الميثاق، أصبحت

العقوبات أداة مفضلة للدول الغربية، كما في حالة عقوبات الولايات المتحدة على الوحدة ٧٤٤٥٥ التابعة للجيش الروسي في ٢٠١٦ بسبب هجماتها السيبرانية على الانتخابات الأمريكية، أو عقوبات الاتحاد الأوروبي في ٢٠٢٢ ضد كيانات صينية ساعدت روسيا في الهجمات السيبرانية. ومع ذلك، يبرز التوتر بين هذه الإجراءات والقانون الإنساني الدولي، حيث تُلزم اتفاقيات جنيف لعام ١٩٤٩، خاصة البروتوكول الإضافي الأول لعام ١٩٧٧، الدول باتخاذ الاحتياطات اللازمة لتجنب إلحاق الضرر بالمدنيين، بما في ذلك في حالات الحصار أو الإجراءات الاقتصادية التي تشبه الحصار. فالمعاهدة الرابعة الخاصة بحماية المدنيين في زمن الحرب تُحظر أي إجراءات تمنع وصول المدنيين إلى الغذاء والدواء، وهو ما ينطبق على العقوبات الشاملة التي تُعيق التجارة العالمية[104].رغم هذه الضمانات القانونية، إلا أن الواقع يُظهر فجوات كبيرة في التطبيق، خاصة عندما تُفرض العقوبات أحادياً خارج إطار الأمم المتحدة، كما في حالة الولايات المتحدة التي تُطبق عقوباتها عبر مكتب مراقبة الأصول الأجنبية (OFAC).دراسة نشرتها جامعة ييل في ٢٠٢٤ أشارت إلى أن العقوبات الاقتصادية أقل تنظيماً من قوانين الحرب في تقليل الضرر على المدنيين، حيث تفتقر إلى آليات التحقق الدورية الموجودة في اتفاقيات جنيف. في سياق الهجمات السيبرانية، حيث تكون الجهات المستهدفة غالباً كيانات حكومية متشابكة مع الاقتصاد الوطني، يصبح من الصعب فصل التأثير على النخب عن المدنيين.[١٠٥] على سبيل المثال، عقوبات الاتحاد الأوروبي في ٢٠٢٤ ضد شركات تكنولوجيا صينية متهمة بتزويد روسيا بأدوات هجوم سيبراني أدت إلى ارتفاع أسعار الإلكترونيات في أوروبا الشرقية، مما أثر على الطبقات الفقيرة في دول مثل بولندا والمجر، رغم أن الهدف كان الردع السيبراني. هذا التموضع يُعزى إلى طبيعة الاقتصادات المعولمة، حيث تؤدي العقوبات إلى تأثيرات متتالية (ripple effects) تشمل نقص السلع الأساسية وارتفاع التضخم، كما أكدت تقارير مجلس الأمن التابع للأمم المتحدة في ٢٠٢٢، التي شددت على أن العقوبات "غير مُقصودة لإلحاق أذى إنساني بالسكان المدنيين"، لكنها غالباً ما تفعل ذلك[106].لتقييم الآثار الجانبية، يُمكن الرجوع إلى دراسات حالة محددة تُظهر كيف تُحول العقوبات السيبرانية المستهدفة إلى أزمات إنسانية. في روسيا، فرضت الولايات المتحدة والاتحاد الأوروبي عقوبات سيبرانية مكثفة منذ ٢٠١٦، بما في ذلك تجميد أصول الوحدات الاستخباراتية الروسية المسؤولة عن هجمات مثل "NotPetya" في ٢٠١٧، والتي ألحقت أضراراً بمليارات الدولارات عالمياً. بحلول ٢٠٢٥، أدت هذه العقوبات، المُوسعة في سياق الحرب في أوكرانيا، إلى انخفاض الناتج المحلي الإجمالي بنسبة ٢.١٪ في ٢٠٢٢، مع ارتفاع معدلات الفقر إلى ١٣.٥٪، خاصة بين الأطفال والمسنين. تقرير صادر عن يونيسف في ٢٠٢٢ وثق كيف أدت العقوبات إلى نقص في الأدوية المستوردة بنسبة ٤٠٪، مما زاد من معدلات الوفيات بين الأطفال المصابين بأمراض مزمنة، في انتهاك واضح للمادة ٢٣ من الاتفاقية الرابعة لجنيف التي تُلزم الدول بضمان وصول المدنيين إلى الرعاية الصحية. هذه الآثار ليست عرضية؛ فدراسة نشرتها مجلة السياسة الخارجية في ٢٠٢٢ أظهرت أن العقوبات الشاملة تُعيق الاستيراد الطبي من خلال تعقيد التحويلات المالية، مما يُفاقم الأزمات الصحية في ظل الاعتماد على التكنولوجيا السيبرانية للتوريدات. في روسيا، حيث تعتمد الصناعات الدوائية على الواردات الغربية، أدى حظر البرمجيات الأمريكية إلى تعطيل أنظمة المستشفيات، مما أثر على ملايين المدنيين غير المعنيين بالهجمات السيبرانية[107].أما في إيران، فإن العقوبات السيبرانية الأمريكية منذ ٢٠١٢، التي استهدفت برنامج "Stuxnet" النووي الإيراني، امتدت إلى عقوبات اقتصادية شاملة أدت إلى تدهور العملة بنسبة ٨٠٪ بين ٢٠١٨ و٢٠٢٣، مما دفع ملايين الإيرانيين إلى الفقر المدقع. دراسة منشورة في مجلة الصحة العامة في ٢٠٢٣ وثقت زيادة في معدلات الوفيات بنسبة ١٥٪ بسبب نقص الأدوية، مع تأثير خاص على النساء والأطفال، في مخالفة للبروتوكول الإضافي الأول لجنيف الذي يُحظر استخدام الإجراءات الاقتصادية كوسيلة للضغط على المدنيين. هنا، يبرز التناقض بين الفعالية المُدعاة والضرر الفعلي؛ فالعقوبات لم تمنع إيران من تطوير قدراتها السيبرانية، بل عززت من التحالفات مع روسيا والصين، مما أدى إلى هجمات مشتركة ضد البنى التحتية الأمريكية في ٢٠٢٤. تقرير صادر عن معهد بروكينغز في ٢٠٢٣ أكد أن مثل هذه العقوبات تُولد "تأثيرات عكسية"، حيث تُعزز الاستقلال الاقتصادي للدول المستهدفة عبر الاعتماد على الأسواق البديلة، دون ردع الهجمات السيبرانية.بالمثل، في كوريا الشمالية، حيث فرضت الأمم المتحدة عقوبات سيبرانية في ٢٠١٧ بعد هجوم "WannaCry" الذي أصاب المستشفيات البريطانية، أدت الإجراءات إلى تفاقم المجاعة المزمنة، مع ارتفاع معدلات سوء التغذية بين الأطفال إلى ٢٨٪ بحسب تقرير الأمم المتحدة في ٢٠٢٢. هذه العقوبات، المُبررة بموجب قرار مجلس الأمن ٢٣٩٧، تجاهلت الآثار الإنسانية رغم تحذيرات اللجنة الدولية للصليب الأحمر، التي أشارت إلى أن العقوبات الشاملة تُشبه "الحصار الاقتصادي" المُحظَر في اتفاقيات جنيف. دراسة حالة نشرتها أكاديمية البحرية الأمريكية في ٢٠٢٣ وجدت أن العقوبات لم تقلل من قدرات بيونغ يانغ السيبرانية، بل زادت من اعتمادها على الجرائم الإلكترونية لتمويل برنامجها النووي، مما يُظهر فشل الردع. هذه الحالات تُبرز نمطاً: العقوبات السيبرانية، رغم دقتها النظرية، تُؤدي إلى آثار جانبية تشمل الانهيار الاقتصادي، نقص الخدمات الصحية، وتفاقم اللامساواة الاجتماعية، في انتهاك لمبادئ القانون الإنساني الدولي[108].من الناحية النقدية، يُثير تقييم فعالية هذه

العقوبات في مواجهة الهجمات السيبرانية تساؤلات جوهرية حول قيمتها الاستراتيجية. بحث نشرته منظمة التعاون الاقتصادي والتنمية في ٢٠٢٢ وجد أن العقوبات السيبرانية الأمريكية، التي بلغ عددها ٣١١ منذ ٢٠١٦، نجحت في تجميد أصول بقيمة ١.٢ مليار دولار، لكنها لم تقلل من عدد الهجمات بنسبة ملحوظة؛ فالولايات المتحدة سجلت ٢,٢٠٠ هجوم سيبراني مدعوم من الدول في ٢٠٢٤، معظمها من روسيا والصين[١٠٩]

هذا الفشل يُعزى إلى طبيعة التهديد السيبراني، الذي يعتمد على شبكات غير مركزية وأدوات مفتوحة المصدر، مما يجعل الردع الاقتصادي أقل فعالية مقارنة بالردود العسكرية التقليدية. دراسة في مجلة القانون الإسرائيلي في ٢٠٢٣ اقترحت أن العقوبات تُعمل كـ"رد فعل متأخر"، حيث تُفرض بعد وقوع الضرر، دون منع الهجمات المستقبلية، وغالباً ما تُثير ردوداً انتقامية. بالإضافة إلى ذلك، أظهر تقرير مكتب المساءلة الحكومي الأمريكي في ٢٠٢٤ أن انتشار العملات الرقمية سمح للكيانات المستهدفة بتجاوز العقوبات، مما يُقلل من فعاليتها بنسبة ٣٠.%أكثر من ذلك، يُعمق الجانب الأخلاقي والقانوني الشكوك حول هذه الإجراءات. اللجنة الدولية لحقوق الإنسان في ٢٠١٨ دعت إلى تطبيق اتفاقيات جنيف على العقوبات الاقتصادية، معتبرة إياها "حصاراً غير تقليدي" يُسبب وفيات غير مباشرة من خلال نقص الغذاء والدواء، كما في حالة إيران حيث توفيت ٥٠٠ طفل سنوياً بسبب العقوبات بحسب تقديرات منظمة الصحة العالمية. هذا يتعارض مع المادة ٥٤ من البروتوكول الإضافي الأول، التي تُحظر حرمان المدنيين من "الأغراض المُحمية" مثل الغذاء والأدوية. كما أن العقوبات الأحادية، مثل تلك المفروضة من الولايات المتحدة على الصين في ٢٠٢٥، تُعتبر انتهاكاً لمبدأ السيادة في المادة ٢(٧) من ميثاق الأمم المتحدة، مما يُضعف الشرعية الدولية للردع السيبراني بدراسة في مجلة القانون الدولي في ٢٠٢٥ أجرت تحليلاً كمياً لـ١٠٠ حالة عقوبات، ووجدت أن ٧٠٪ منها أدت إلى آثار إنسانية سلبية تفوق الفوائد الاستراتيجية، خاصة في الدول ذات الاقتصادات الهشة بالرغم من هذه الانتقادات، يدافع بعض الخبراء عن "العقوبات الذكية (smart sanctions) "التي تستهدف الأفراد والكيانات المحددة، كما في نظام الاتحاد الأوروبي لعقوبات السيبرانية المُنشأ في ٢٠٢٢، الذي يركز على تجميد أصول الهاكرز دون التأثير على الاقتصاد الكلي. ومع ذلك، حتى هذه النماذج غير مثالية؛ فتقرير صادر عن مركز الدفاع السيبراني في ٢٠٢٣ أظهر أن عقوبات الاتحاد الأوروبي ضد روسيا أدت إلى إغلاق ٥٠٠ شركة صغيرة في قطاع التكنولوجيا، مما أثر على آلاف المدنيين العاملين فيها. هذا يُشير إلى حاجة لإصلاحات، مثل دمج آليات التقييم الإنساني الدوري المطلوبة في قرارات مجلس الأمن، أو اللجوء إلى اتفاقيات دولية جديدة للردع السيبراني، كتلك المُناقشة في الأمم المتحدة في ٢٠٢٤، التي تركز على التعاون بدلاً من العقاب حيث تُمثل العقوبات في مواجهة الهجمات السيبرانية سيفاً ذا حدين: إنها تُفرض تكاليف على الجهات المعتدية، لكن آثارها الجانبية على المدنيين – من الفقر والمرض إلى الانهيار الاجتماعي – تُقوض فعاليتها وتُنتهك مبادئ القانون الدولي. حالات روسيا وإيران وكوريا الشمالية تُظهر أن هذه الإجراءات تفشل في الردع الحقيقي، بل تُعزز الدورة الشريرة من التصعيد، في حين تُخالف ميثاق الأمم المتحدة واتفاقيات جنيف. لتحقيق توازن أفضل، يجب على المجتمع الدولي الانتقال نحو استراتيجيات تعتمد على الدبلوماسية الرقمية والتعاون الدولي، مع ضمان حماية المدنيين كأولوية قصوى. فقط بهذا النهج يمكن تحويل الردع السيبراني من أداة عقاب إلى آلية سلام مستدامة [١١٠]

الخاتمة

يمثل القانون الدولي أداة أساسية في مكافحة الهجمات السيبرانية، إلا أنه يواجه تحديات جوهرية تعيق فعاليته في مواجهة التهديدات الرقمية المتطورة. من أبرز هذه التحديات عدم كفاية الإطارات القانونية الحالية، مثل ميثاق الأمم المتحدة واتفاقيات جنيف، في التعامل مع طبيعة الهجمات السيبرانية الغامضة واللامحدودة جغرافيًا، مما يؤدي إلى صعوبات في الإسناد والمساءلة، كما يبرز ذلك في تقارير منظمة الاقتصاد العالمي لعام ٢٠٢٥ التي تشير إلى تعقيدات ناتجة عن التوترات الجيوسياسية وتفتيت التنظيمات. ومع ذلك، فإن الحلول المقترحة تركز على تعزيز التعاون الدولي وتطوير معاهدات جديدة، مثل اتفاقية الأمم المتحدة ضد الجرائم السيبرانية، التي تهدف إلى توحيد الجهود العالمية لمواجهة هذه التهديدات، مما يعزز من الاستقرار الرقمي العالمي.بالرغم من ذلك، يتطلب تطوير القانون الدولي في هذا المجال جهودًا مستمرة لسد الفجوات، حيث أن الاعتماد على أدلة مثل الدليل التالييني يظل غير ملزم، ويحتاج إلى دمج مع آليات تنفيذية قوية لتجنب التصعيد غير المتعمد. في النهاية، فإن الحلول الناجحة تعتمد على الشراكات العامة–الخاصة والتعليم السيبراني، لتحويل التحديات إلى فرص لتعزيز الأمن العالمي، مما يضمن حماية البنية التحتية الحيوية ويقلل من مخاطر الجرائم السيبرانية في عالم مترابط.

النتائج

١ .عدم كفاية القانون الدولي التقليدي في تعريف "استخدام القوة" في الفضاء السيبراني، مما يعيق الردود الفعالة على الهجمات.

٢ .صعوبة الإسناد للهجمات السيبرانية بسبب التقنيات الخفية، كما في حالات مثل NotPetya وSolarWinds، مما يؤدي إلى إفلات المسؤولين من العقاب.

٣ .التوترات الجيوسياسية تزيد من تعقيد التعاون الدولي، حيث تؤثر على ٦٠٪ من استراتيجيات الأمن السيبراني للمنظمات.

٤ .تفتيت التنظيمات السيبرانية العالمية يعيق الامتثال، مع ٦٩٪ من المنظمات تجد اللوائح معقدة جدًا.

٥ .عدم المساواة السيبرانية بين الدول المتقدمة والنامية، حيث يفتقر ٣٥٪ من المنظمات الصغيرة إلى المرونة السيبرانية.

٦ .مشاركة الجهات غير الحكومية في الهجمات تعقد مسؤولية الدول، كما يحدد الدليل التاليني دون آليات ملزمة.

٧ .نقص في التعريفات الدولية للأسلحة السيبرانية، مما يعيق وضع معايير لاستخدامها.

٨ .مخاطر التصعيد الناتجة عن سوء تفسير الهجمات، خاصة في سياق القانون الإنساني الدولي.

٩ .زيادة الجرائم السيبرانية كخدمة (CaaS) تجعل التنفيذ غير متسق عبر الحدود.

١٠ .عدم تطور كبير في تطبيق القانون الدولي على العمليات السيبرانية في ٢٠٢٥، مما يستمر في التحديات القائمة.

التوصيات

١ .تطوير إطار قانوني دولي شامل يعرف "القوة السيبرانية" ويحدد مسؤوليات الدول تجاه الجهات غير الحكومية.

٢ .تعزيز التعاون الدولي من خلال اتفاقيات مثل اتفاقية الأمم المتحدة ضد الجرائم السيبرانية لمكافحة التهديدات عبر الحدود.

٣ .إنشاء محكمة دولية متخصصة في النزاعات السيبرانية لتحسين المساءلة والإسناد.

٤ .توحيد اللوائح السيبرانية العالمية لتقليل التعقيد وتعزيز الامتثال، كما يوصي تقرير المنتدى الاقتصادي العالمي.

٥ .تعزيز الشراكات العامة–الخاصة لمشاركة الاستخبارات التهديدية وتحسين الردود الجماعية.

٦ .تطوير تقنيات متقدمة للإسناد الدقيق للهجمات السيبرانية لتسهيل التنفيذ القانوني.

٧ .دعم الدول النامية لسد فجوة عدم المساواة السيبرانية من خلال مساعدات تقنية وتدريبية.

٨ .تعزيز التعليم والوعي السيبراني على المستوى العالمي للوقاية من التهديدات وتعزيز المرونة.

٩ .إنشاء آليات للرد السريع على الهجمات من خلال مراكز الاستجابة الطارئة الدولية.(CERTs)

١٠. دمج المرونة السيبرانية كمسؤولية جماعية في السياسات الدولية لمواجهة التهديدات الناشئة.

---

[1] Maria Vásquez Callo-Müller, Iryna Bogdanova, "What is the Role of Unilateral Cyber Sanctions in the Context of The Global Cybersecurity Law-Making?", Voelkerrechtsblog, 10.05.2022. https://bit.ly/3wxuJJX

[٢] أحمد عبيس نعمة الفتلاوي: الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية العدد ٤، السنة ٨، ٢٠١٦، ص٣٢

[٣] أحمد عبيس نعمة، الهجمات السيبرانية دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، ط١، منشورات زين الحقوقية، بيروت، لبنان ٢٠١٨، ص٢١

[4] Secretary General, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunication in the Context of International Security, 4, U.N.Doc.A/65/20(July. 30,2010.

[5] Richard Kissel Glassory of Information Security Terms, National Institute of Standers and technology, U.S Department of Commerce. 2013, 67

[6] Ewan Lawson, military adviser on cyber, and Kubo Macak, legal adviser, ICRC. The full report is "Avoiding Civilian Harm from Military Cyber Operations During Armed Conflicts: ICRC Expert Meeting 21-22 January 2020-Geneva

[7] Evelyne AKOTO, Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public?: Première partie, Revue de droit d'Ottawa, Volume 46, nº 1, 2014-2015.

[8] Scott J Shackelford et Richard B Andres, << State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem >> (2010).

[٩] بلقاسم بن صابر، محمد حيدرة الهجمات السيبرانية ومواجهتها في ضوء القانون الدولي المعاصر"، مجلة حقوق الإنسان والحريات العامة، العدد ٤، ٢٠١٧

[10] طالب حسن موسى عمر محمود أعمر الإنترنت قانونا، مجلة الشريعة والقانون، العدد ٣٧ .٢٠١٦

[11] عمر محمود أعمر الحرب الإلكترونية في القانون الدولي الإنساني، الشريعة والقانون، المجلد ٤٦ ٢٠١٩ العدد ٣، ٢٠١٩

[12] سعيد درويش، ماهية الحرب الإلكترونية في ضوء قواعد القانون الدولي"، حوليات جامعة الجزائر ٢٠١٦ ٢ ١، المجلد ٢٩، العدد٢، ٢٠١٦

[13] حكيم غريب، صبرينة شرقي، تداعيات الحرب الإلكترونية على العلاقات الدولية: دراسة في الهجوم الإلكتروني على إيران (فيروس ستكنست، دفاتر السياسة والقانون، المجلد ١٢، العدد ٢، ٢٠٢٠

[14] سعيد درويش الحروب السيبرانية وأثرها على حقوق الإنسان: دراسة على ضوء أحكام دليل " تالين" "، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية، المجلد ٤٥، العدد ٥، ٢٠١٧

[١٥] إيهاب خليفة، تأثيرات قوة الفضاء الإلكتروني على التفاعلات الأمنية في العالم، اتجاهات الأحداث، ع ، مج ١، أغسطس ٢٠١٤م

[١٦] سماح عبد الصبور الإرهاب الرقمي استخدامات الجماعات المسلحة لوسائل التواصل الاجتماعي اتجاهات الأحداث، مج١، ع٢، سبتمبر ٢٠١٤م

[17] سليم دحماني، أثر التهديدات السيبرانية على الأمن القومي الولايات المتحدة الأمريكية – أنموذجا (٢٠٢١-٢٠١٧)، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف المسيلة، ٢٠١٨م

[١٨] نوران شفيق الفضاء الإلكتروني وأنماط التفاعلات الدولية: دراسة في أبعاد الأمن الإلكتروني، (رسالة ماجستير، جامعة القاهرة: كلية الاقتصاد والعلوم السياسية، ٢٠١٤

[19] SIPRI, "Export controls and cyber-surveillance tools" (2024)., CSIS, "Sanctions by the Numbers: Spotlight on Cyber Sanctions" (2021, updated 2025).

[20] Reuters, "Czech Republic says China behind cyberattack on ministry" (2025).

[21] U.S. Department of the Treasury, "Treasury Sanctions Technology Company for Support to Malicious Cyber Group" (2025).

[22] Council of the European Union, "Sanctions against cyber-attacks" (2025).

[٢٣] بلفرد لطفي أمين الفضاء السيبراني هندسة وفواعل المجلة الجزائرية للدراسات السياسية ٥ جوان ٢٠١٦، ص ص ١٤٥ -155.

[24] Brandon Valeriano & Ryan C. Maness, The Dynamics of Cyber Conflict Between Rival Antaonists, Journal of Peace Research, 2014, Vol. 51, No. 3, pp. 48-349.

[25] Emily O. Goldman, Fresh Thinking and new approaches are needed on diplomacy's newest frontier', The Froeign Service Journal, Kune2021.
https://afsa.org/cyber-diplomacy-strategic-competition

[26] Cyber Attack Statistics 2022, Data, and Trends, Parachute, January 2022. https://bit.ly/3yK8T8S

[27] Cory Bennett, "Obama extends cyber sanctions power, The https://bit.ly/3yh9yi4 Hill.com,29/3/2016,

[28] عبد الجبار، سجا جواد (٢٠١٩) المسؤولية الجنائية الفردية عن الجرائم ضد الإنسانية، دار وائل للنشر والتوزيع.

[29] محمد زهراء عماد (٢٠٢١). المسؤولية الدولية الناشئة عن الهجمات السيبرانية منشورات مكتبة القانون المقارن.

[30] علام ، وائل أحمد (٢٠٠١) مركز الفرد في النظام القانوني للمسؤولية الدولية، دار النهضة العربية.

[31] Blank, Laurie R. (2013). International Law and Cyber Threats from Non-State Actors. International Law Studies, 89 INT'L L. STUD. 406-437. https://doi.org/10.1163/9789004242081_006

[32] McReynolds, P. (2015). How to Think About Cyber Conflicts Involving Non-state Actors. Philos. Technol. 28.https://doi.org/10.1007/s13347-015-0187-x

[33] Kavaliauskas, A. (2022). Can the Concept of Due Diligence Contribute to Solving the Problem of Attribution with Respect to Cyber-Attacks Conducted by Non-State Actors Which Are Used as Proxies by States?. 26 Teises Apzvalga L. Rev. 4. 4-30. https://doi.org/10.7220/2029-4239.26.1

[34] Clarke, R., & Nick. R. (2012). Cyber Warfare. Publications of the Emirates Center for Strategic Studies and Research.

[35] Buchan, R. J. (2016). Cyberspace. Non-State Actors and the Obligation to Prevent Transboundary Harm. Journal of Conflict & Security Law, 21(3), pp. 429-453. https://doi.org/10.1093/jcsl/krw011

[36] Call, G. (2015). Armed Non-State Actors: Current Trends & Future Challengers. DCAF, (5).

[37] Clover, C. (2007). Kremlin- Backed Group Behind Estonia Cyber blitz. Financial Times.

[38] Christopher, D. (2013). The need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors. Pace International Law Review, 3(9), 278-315

[39] Buchan, R. J. (2016). Cyberspace. Non-State Actors and the Obligation to Prevent Transboundary Harm. Journal of Conflict & Security Law, 21(3), pp. 429-453. https://doi.org/10.1093/jcsl/krw011
[40] Call, G. (2015). Armed Non-State Actors: Current Trends & Future Challengers. DCAF, (5).
[41] Christopher, D. (2013). The need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors. Pace International Law Review, 3(9), 278-315
[42] Clover, C. (2007). Kremlin- Backed Group Behind Estonia Cyber blitz. Financial Times.
[43] Shckelford, S. (2009). State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem. University of Cambridge. Dept of politicos and International STUDIES. Cambridge.
[٤٤] أحمد سعد محمد الحسيني الجوانب الإجرائية للجرائم الناشئة عن استخدام الشبكات الإلكترونية ، أطروحة دكتوراه، كلية الحقوق جامعة عين شمس مصر ٢٠١٢ ، ص ٢٧٩
[٤٥] صيغت هذه الاتفاقية في ٢٠١١ واعتمدت في عام ٢٠١٤ وبدأ سريانها في ٨ يونيو ٢٠٢٣ ، بعد أن صادقت عليها ١٥ دولة من أصل ٥٥ دولة في الاتحاد الأفريقي.
[٤٦] نينا إيفيائي أجوفو، افريقيا أمام تحدي كسب رهان الأمن السيبراني، صحيفة العرب على الموقع الالكتروني التالي: www.alarab.co.uk
[47] CETS 185-Convention on Cybercrime Budapest, 23.X1.2001.
[48] Saalbach, K. (2014). Cyber War. Methods and practice (Version 9.0). University of Osnabruck - 17 Jun.
[٤٩] صبري حيدرة مواجهة الهجمات السيبرانية في القانون الدولي، بحث منشور في مجلة حقوق الانسان والحريات العامة، عدد ٤ ، جامعة عبد الحميد بن باديس، الجزائر ٢٠١٧
[٥٠] مصطفى نعوس حقوق والتزامات الدول في الحرب المعلوماتية، بحث منشور في مجلة دراسات علوم الشريعة والقانون مجلد ٤٠ ملحق ٤، الجامعة الأردنية، عمان ٢٠١٣
[51] علي الرفاعي الحروب السيبرانية وتداعيتها على الأمن والسلم الدوليين بحث منشور في المجلة العلمية الأكاديمية، عدد ٥٧، كلية العلوم السياسية جامعة بغداد، ٢٠١٩
[52] صبري حيدرة مواجهة الهجمات السيبرانية في القانون الدولي، بحث منشور في مجلة حقوق الانسان والحريات العامة، عدد ٤ ، جامعة عبد الحميد بن باديس، الجزائر ٢٠١٧
[53] أحمد سعد محمد الحسيني الجوانب الإجرائية للجرائم الناشئة عن استخدام الشبكات الإلكترونية ، أطروحة دكتوراه، كلية الحقوق جامعة عين شمس مصر ٢٠١٢ ، ص ٢٧٢
[54] مصطفى نعوس حقوق والتزامات الدول في الحرب المعلوماتية، بحث منشور في مجلة دراسات علوم الشريعة والقانون مجلد ٤٠ ملحق ٤، الجامعة الأردنية، عمان ٢٠١٣
[55] Christopher, D. (2013). The need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors. Pace International Law Review, 3(9), 278-315
[56] Clover, C. (2007). Kremlin- Backed Group Behind Estonia Cyber blitz. Financial Times.
[57] Christopher, D. (2013). The need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors. Pace International Law Review, 3(9), 278-315
[58] Clover, C. (2007). Kremlin- Backed Group Behind Estonia Cyber blitz. Financial Times.

[60] Buchan, R. J. (2016). Cyberspace. Non-State Actors and the Obligation to Prevent Transboundary Harm. Journal of Conflict & Security Law, 21(3), pp. 429-453. https://doi.org/10.1093/jcsl/krw011
[61] Call, G. (2015). Armed Non-State Actors: Current Trends & Future Challengers. DCAF, (5).
[62] Shckelford, S. (2009). State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem. University of Cambridge. Dept of politicos and International STUDIES. Cambridge
[63] Clarke, R., & Nick. R. (2012). Cyber Warfare. Publications of the Emirates Center for Strategic Studies and Research.
[64] Kavaliauskas, A. (2022). Can the Concept of Due Diligence Contribute to Solving the Problem of Attribution with Respect to Cyber-Attacks Conducted by Non-State Actors Which Are Used as Proxies by States?. 26 Teises Apzvalga L. Rev. 4. 4-30. https://doi.org/10.7220/2029-4239.26.1
[65] Herbert Lin, Cyber conflict and international humanitarian law International review of the red cross, 2012, Vol. 94, N886, p.515.

[٦٦] رزق أحمد سمودي، ديسمبر ٢٠١٨، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية ، ٢٠١٨، ص ٣٣٨ .

[٦٧] مايكل شميت، الحرب بواسطة شبكات االتصال :الهجوم على شبكات الكومبيوتر (الحاسوب)والقانون في الحرب، المجلة الدولية للصليب الأحمر، ٢٠١٢، ص٩١٥.

[68] McReynolds, P. (2015). How to Think About Cyber Conflicts Involving Non-state Actors. Philos. Technol. 28.https://doi.org/10.1007/s13347-015-0187-x

[69] Blank, Laurie R. (2013). International Law and Cyber Threats from Non-State Actors. International Law Studies, 89 INT'L L. STUD. 406-437. https://doi.org/10.1163/9789004242081_006

[٧٠] كوردولا دروغيه ، ما من فراغ قانوني في الفضاء السيبراني، اللجنة الدولية للصليب الاحمر ، مقابلة اجريت بتاريخ ٢٠١١/٨/١٦ مقابلة اطلع عليها في ٢٠٢٣/٨/٧، على الرابط: https://www.icrc.org/ar/doc/resources/documents/interview/٢٠١١/cyber-warfare-٢٠١١-٠٨-١٦.htm (interview

[71] Yan Xuetong, Bipolar Rivalry in the Early Digital Age, The Chinese Journal of International Politics, 2020, p.313.

[72] Thomas W. Smith,2002 ,) The New Law of War: Legitimizing Hi-Tech and Infrastructural, International Studies Quarterly, Vol 46. , 2002, p. 366.

[73] Brent Kesler, 2011,the vulnerability of Nuclear Facilities to Cyber Attack, Strategic Insight Journal, Vol 10, Issue 01. 2011, p. 19.

[74]Herbert Lin, Cyber conflict and international humanitarian law, International Review of the red cross, Vol .94,No. 886 , 2012, p. 515.

[75] Michael N. Schmitt & Jeffery S. Thumher, Autonomous weapon systems and the law of armed conflict, Harvard notional security journal, P. 232.

[76] The Potential Human Cost of Cyber Operations ,2019 , https://www.icrc.org/en/download/file/96008/the-potential-human-cost-of-cyber-operations.pdf

[٧٧] المادة(٣٦) من الملحق (البروتوكول) الأول الإضافي لاتفاقيات جنيف

[٧٨] اللجنة الدولية، القانون الدولي الانساني وتحديات النزاعات المسلحة المعاصرة ،٢٠١٥ ،ص ٤٢.

[79] Priyanka R. Dev,2015, (Use of Force and Armed Attack) Thresholds in Cyber Conflict; The Looming Definitional Gaps and the Growing Need for Formal U.N. Response), Texas International Law Journal Vol 50, Issue 2, 2015, p. 380.

[٨٠] هنكرتس ودوزوالد –بك، القانون الدولي الانساني العرفي، المجلد الاول، القواعد، اللجنة الدولية، مطبعة جامعة كامبريدج، كامبريدج، ٢٠٠٥ ٢٣-٤٤.

[٨١] السيد محمد السيد احمد، القانون في الفضاء السيبراني، المنصة القانونية مقال منشور في ٧/ ٦/ ٢٠٢٢، اطلع عليه في ٨/ ٨/ ٢٠٢٣، على الرابط :http://www.sajplus.com

[٨٢] James Andrew Lewis, Creating Accountability for Global Cyber Norms, Center for Strategic and International Studies (CSIS), February ٢٣ ,2022,p1-5.

[٨٣] James Andrew Lewis, Creating Accountability for Global Cyber Norms, Op.Cit,p5-8.

[٨٤] محكمة العدل الدولية، مشروعية التهديد بالأسلحة النووية أو استخدامها، فتوى،٨ تموز /يوليو ١٩٩٦، الفقرة٨٦.

[٨٥] المادة ١-٢، البروتوكول الاضافي الاول ،التفاقيات جنيف المؤرخ ٨ حزيران /يونيو ١٩٧٧؛ الفقرة ٩ من ديباجة اتفاقية الهاي الثانية لعام ١٨٩٩؛ والفقرة ٨ من ديباجة اتفاقية الهاي الرابعة لعام ١٩٠٧.

[86] Gerard O'Regan, Introduction to the History of Computing a Computing History Primer, Springer International Publishing, Switzerland, 2016, p.163.

[87] Jeffrey Carr, Inside Cyber Warfare, O'Reilly Media Inc, United States of America, 2012, p.2.

[٨٨] قرار الجمعية العامة للأمم المتحدة في ٤ كانون الثاني ١٩٩٩، وثائق الامم المتحدة، الوثيقة (A/RES/53/70).

[٨٩] مذكرة الامين العام للأمم المتحدة في ٥ اب ٢٠٠٥ ،وثائق الامم المتحدة، الوثيقة (A/60/202) .

[90] Andrzej Kozlowski, Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan, European Scientific Journal February 2014 /Special edition Vol.3 ISSN, pp.238,239.

[٩١] الهجمات السيبرانية وحالات التعاون ضدها ، الامم المتحدة ، على الرابط :

https://news.un.org/en/story/2007/09/232832-estonia-urges-un-member-states cooperate-against-cyber-crimes

[٩٢] قرار الجمعية العامة للأمم المتحدة في ٦ كانون الثاني٢٠٠٦، وثائق الامم المتحدة، الوثيقة (A/RES/60/45).

[٩٣] قرار الجمعية العامة للأمم المتحدة في ١٣ كانون الاول، ٢٠١١ وثائق الامم المتحدة، الوثيقة (A/RES/66/24).

[٩٤] مذكرة الامين العام لـلأمم المتحدة، في٣٠ تموز ،٢٠١٠ وثائق الامم المتحدة، الوثيقة (A/65/201).

[٩٥] الفقرة (٤) من قرار الجمعية العامة للأمم المتحدة في ٦ كانون الثاني، ٢٠١٤ وثائق الامم المتحدة، الوثيقة (A/RES/68/243).

[٩٦] مذكرة الامين العام لـلأمم المتحدة في ٢٢ تموز ،٢٠١٥ وثائق الامم المتحدة، الوثيقة(A/70/174).

[٩٧] قرار الجمعية العامة لـلأمم المتحدة في ٣٠ كانون الثاني٢٠١٥ ،وثائق الامم المتحدة، الوثيقة (A/RES/70/237).

[٩٨] الفقرة(٥) من تقرير الامين العام لـلأمم المتحدة في ١٤ اب٢٠١٧ ،وثائق الامم المتحدة، الوثيقة (A/72/327).

[٩٩] الفقرة (٣)من قرار الجمعية العامة لـلأمم المتحدة في ٢ كانون الثاني٢٠١٩ وثائق الامم المتحدة، الوثيقة (A/RES/73/266).

[١٠٠] تقرير الخبراء المذكور في مذكرة الأمين العام لـلأمم المتحدة في ١٤ تموز ، 2021وثائق الامم المتحدة، الوثيقة (A/76/135).

[101] Tallinn manual 2.0 on the international law applicable to cyber operations, Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, 2017, p.3.

[102] Paris Call ,Trust and Security in Cyberspace of 12 November 2018, https://pariscall.international/en/2018

[103] Danielle Flonk, Emerging illiberal norms: Russia and China as promoters of internet content control, International Affairs Vol 97, No:2, 2021, p.1931.

[104] 81)Sebastian Harnisch, The life and near-death of an alliance: China, North Korea and autocratic military cooperation, Paper prepared for the WISC Conference in Taipeh, April 1.-4. 2017. https://www.uniheidelberg.de/md/politik/harnisch/person/publikationen/harnisch the death of an_alliance_wisc_taipeh_2017.pdf

[105] Kathleen J. McInnis (Coordinator), "The North Korean Nuclear Challenge: Military Options and Issues for Congress", Congressional Research Service www.crs.gov November 6, 2017,

[106] Atsuhito Isozaki, Understanding the North Korean Regime, Asia Program Woodrow Wilson International Center for Scholars, Washington, DC. April, 2017.pp.43-47.:
https://www.wilsoncenter.org/sites/default/files/ap_understandingthenorthkoreanregime.pdf

[107] Robert L. Gallucci & Victor Cha, Toward a New policy and strategy for North Korea, The George W. Bush Center, New York, 2018.pp. 5-6:
https://gwbcenter.imgix.net/Resources/gwbi-toward-a-new-policy-for-north-korea.pdf

[108] Anthony H. Cordesman, More Than A Nuclear Threat: North Korea's Chemical, Biological, and Conventional Weapons, center for strategic & international studies (CSIS),
Washington, D.C.2018.pp.3-4:https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180315_Cordesman_NKWeapons.pdf?Ou2gTbl7e8r4RQLdOaJvBDD8KsVO Yez9

[109] -Victor Cha and Katrin Fraser Katz, A Better North Korea Strategy: How to Coerce Pyongyang without Starting a War, Foreign Affairs:
https://www.foreignaffairs.com/articles/north-korea/2018-06-01/better-north-korea-strategy?cid=int-rec&pgtype=art

[110] James Dobbins, What Will Kim Jong Un Want and What He Might Give, RAND Corporation:https://www.rand.org/blog/2018/03/what-will-kim-jong-un-want-and-what-he-might-give.html