جمهورية العراق

وزارة التعليم العالي والبحث العلمي

جامعة بابل

كلية القانون

واجب العناية اللازمة للدول لمنع اضرار الهجمات المعلوماتية

اطروحة تقدم بها

جبر ياسين لفته راشد

إلى مجلس كلية القانون في جامعة بابل وهي جزء من متطلبات نيل درجة الدكتوراه في القانون العام

بأشراف

أ.د.صدام حسين الفتلاوي

أستاذ القانون الدولي العام

١٤٤٤هـ ٢٠٢٢م

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

﴿ وَمَا أُوتِيتُمْ مِنْ الْعِلْمِ إِلاَّ قَلِيلاً ﴾

صدق الله العلي العظيم

سورة الاسراء/آية(٨٥)

الإهداء

إلى من قاد قلوب البشـرية وعقولهم إلى مرفأ الامان، معلم البشـرية الأول سـيدنا محمد (صلى الله عليه وآله وسلم).

إلى من كانوا ولا يزالون سراجاً ينيرون دربي.... والدي ووالدتي.

إلى الذين أثروني على أنفسهم، إلى سندي وملاذي بعد الله ..... أخوتي أخواتي..

إلى من أضاؤوا بعلمهم دربي....

إلى زوجتي و أولادي لكم مني كل الود على ما بذلتموه من أجلي طوال مدة كتابة البحث.

إلى الذين قيل بحقهم من علمني حرفاً جعلني حراً إلى أساتذتي..

إلى من بذلوا الغالي والنفيس ... إلى من فاضت أرواحهم الطاهرة إلى بارئها..

إلى شهداء وطني العزيز..

اهدي هذا الجهد..

الباحث

شكر وعرفان

الحمد لله على توفيقه وإحسـانه، والحمد لله على فضـله وانعامه، والحمد لله على جوده واكرامه، بالشكر تدوم النِعم وتزول النقم، وقد قال الله سبحانه وتعالى في كتابه الكريم (لَئِن شَكَرْتُمْ لَأَزِيدَنَّكُمْ) ولعل خير من أبتدأ بشكره هو الملك القدوس، لمنهِ عليّ وتوفيقه لي وتسديده لإتمام اطروحتي.

فبعد أن منَّ الله تعالى عليَّ بأكمال هذا العمل وأنا أسـطر أخر حرف من حروف أطروحتي فمن العرفان أن أتوجه بالشكر والثناء إلى أستاذي المشرف الدكتور (صدام حسين وادي الفتلاوي)، الذي تفضـل بقبوله الاشراف على اطروحتي ومنحني الثقة ومدني بكل ما يملك بعلم وعون، وقد كان لآراءه السديدة وسعة صدره الأثر الواضح في أثراء هذه الدراسة لتبصر النور بشكلها الحالي فجزاه الله عن ذلك خير جزاء. كما أسـجل جزيل شكري وامتناني إلى أستاذي الفاضـل الدكتور (أحمد عبيس نعمة الفتلاوي) لما قدمه لي من نصـح وأرشـاد وما زودني به من بعض المصـادر طوال مدة دراستي فكان حقاً نبراساً أهتدي بعلمه ومعرفته.

والشكر والامتنان وجزيل العرفان إلى أساتذتي في كلية القانون متمثلةً بعميدها الاستاذ الدكتور (ميري كاظم عبيد) ورئيس فرع القانون العام الاسـتاذ الدكتور (أسـماعيل صـعصـاع) وجميع أساتذتي الافاضـل الذين نهلت من علمهم في السنة التحضـيرية لمرحلة الدكتوراه، ولا يفوتني أن أشـكر جميع زملائي في مرحلة الدكتوراه لما قدموه لي من عون لتذليل العقبات التي واجهتني، والشكر موصـول إلى موظفي مكتبة كلية القانون جامعة بابل، مكتبة كلية القانون جامعة الكوفة، مكتبة معهد العلمين للدراسات العليا، مكتبة الروضـة الحيدرية المطهرة، مكتبة الروضـة الحسينية المطهرة.

وأخيراً أوجه شـكري وتقديري إلى جميع من أسـهم في أتمام هذا البحث ولو بكلمة أو حرف واحد فلهم مني جزيل الشكر والعرفان وجزاهم الله عني خير الجزاء.

قائمة المحتويات

المستخلص

أدى اعتماد الدول المتزايد على استخدام الفضاء المعلوماتي إلى ظهور نوع جديد من النزاعات يطلق عليها، الهجمات المعلوماتية (Cyber Attacks)، وهي هجمات على النقيض من الهجمات التي يتم تنفيذها بواسطة الأسلحة التقليدية. حيث يتم تنفيذ هذهِ الهجمات عبر الانترنت وأجهزة الحاسب الآلي، وقد ساعد على إنتشارها الملحوظ العديد من الخصائص منها، انخفاض التكلفة المادية للأجهزة المستخدمة في شنها، وصعوبة التعرف على هوية المهاجم المعلوماتي، وهي هجمات عابرة للحدود الإقليمية، فضلاً عن غيرها من الخصائص التي تتسم بها، كذلك هذه الهجمات تتميز عن غيرها من العديد من الهجمات التي قد تكون مماثلة لها، كحرب المعلومات والجريمة المعلوماتية والأمن المعلوماتي، والإرهاب المعلوماتي، وأهتم الكثير من الباحثين من المختصين بالشأن القانوني بمحاولة تكييف هذهِ الهجمات التي يكون أغلبها مصاحبة للنزاعات المسلحة الدولية وغير الدولية ، فمنهم من صنفها على أنها استخدام للقوة المسلحة؛ والبعض الآخر حاول تكيفها في إطار النزاع المسلح على وفق اتفاقيات جنيف الأربع لعام ١٩٤٩ والبروتوكولين الملحقين بهما. وأجتهد الكثير من فقهاء القانون الدولي والخبراء الدوليين بالبحث عن مدى ملائمة تلك الهجمات لقواعد ومبادئ القانون الدولي الإنساني سواء المقننة منها أو العرفية وكيفية تطبيق هذهِ المبادئ على الهجمات المعلوماتية.

وأضحت الدول تواجه تحدياً هاماً في مجال اعمال مبدأ واجب العناية على الهجمات المعلوماتية، هذا المبدأ الذي يتسم بطبيعته العرفية، وافتقاره إلى الاساس القانوني الذي يرتكز عليه، فلم يستطيع الفقه الدولي ايجاد تعريف محدد له، إلاّ أن بداية تطبيقه كانت من خلال اجتهادات القضاء الدولي في قرار محكمة العدل الدولية في قضية قناة كورفو لعام ١٩٤٩، بين بريطانياً والبانيا، ثم تلاه العديد من الأحكام والقرارات القضائية ذات الصلة بموضوع الاضرار البيئية. وقد بدأ المجتمع الدولي يتخذ خطوات جدية على الصعيدين العالمي والاقليمي نحو وضع نظام قانوني يكشف معالم هذهِ الهجمات لمواجهة مخاطرها، فعلى سبيل المثال صدرت مجموعة من القرارات عن اجهزة الأمم المتحدة، كالجمعية العامة والمجلس الاقتصادي ، وسعت بعض الدول لبناء استراتيجيات وقائية لمنع أضرار الهجمات المعلوماتية أو الحدّ من آثارها، كالولايات

المتحدة، وروسيا، والصين، وكذلك تبنت بعض المنظمات الاقليمية استراتيجيات الدفاع المعلوماتي، مثل منظمة حلف شمال الاطلسي (الناتو) ومنظمة شنغهاي للتعاون.

وعلى صعيد آخر أصبح الكثير من المختصين في الشأن القانوني والباحثين يهتمون لمناقشة الأسس القانونية التي ترتكز عليها هذه الهجمات في إطار الاتفاقيات والمواثيق الدولية، علاوة على القواعد العرفية، التي يمكن الاستفادة منها في تنظيم هذه الهجمات، وتبقى مسألة امتثال الدول وعدم امتثالها لواجب العناية مسألة ذات أهمية ومحل نظر لدى الدول عند ممارسة تصرفاتها في ضوء سيادتها المعلوماتية. إذ اتخذت الدول من حق الدفاع الشرعي مبرراً قانونياً لها للرد على الهجمات المعلوماتية المعادية، وبدأت الدول تفكر جلياً في اتخاذ اجراءات اكثر مرونة وانسجاماً عند اللجوء إليها، وهي التدابير المضادة الواردة في المادة (٢٢) من مشروع مسؤولية الدول عن اعمالها غير مشروعة دولياً لعام ٢٠٠١، إذ تسعى الدول من خلال اللجوء للتدابير المضادة استعمال حقها في الرد على الهجمات المعلوماتية وحمل الدولة المعتدية على الوفاء بالتزاماتها والكف عن الفعل غير المشروع، وإذا، تعمدت الدولة على تكرار ذلك فأنه يعرضها إلى المسؤولية الدولية الناشئة عن عدم امتثالها لواجب العناية وما يترتب عليها من آثار، والمسؤولية الدولية بعد تحقق شروطها قد تتحملها الدولة أو الأفراد أو الكيانات الذين يعملون تحت سيطرتها أو إشرافها، وقد تكون تلك المسؤولية جنائية فردية كما هو الحال في مسؤولية الرؤساء والقادة عن الافعال المرتكبة من مرؤوسيهم التي تؤدي إلى انتهاكات جسيمة في إطار القانون الدولي الانساني.

قائمة مختصرات

List of Abbreviations

الاختصار	أصل الاختصار	معنى الاختصار باللغة العربية
SCADA	Super visory Control and Data Acquisition	نظام التحكم والسيطرة على البيانات
CCDCOE	Collabara tive Defence center of Excellence	مركز التمييز للدفاع السيبراني التعاوني التابع لحلف الناتو
ILA	Inter national law Association	رابطة القانون الدولي
ILC	Inter national law commission	لجنة القانون الدولي
GGE	Group of governmental Experts	فريق الخبراء الحكوميين التابع للأمم المتحدة
ICC	Inter national Criminal Court	المحكمة الجنائية الدولية
ICJ	Inter national Court of Justice	محكمة العدل الدولية
ICRC	Inter national Committee of Red Cross	اللجنة الدولية للصليب الاحمر
NO.	Number	العدد
Op.cit Ibid	Op. cit, is an abbreviation of the Latin phrase opera Citato. Latin short for ibidem, meaning in the same place	مرجع سابق وهي مختصر للعبارة اللاتينية opera citato المرجع نفسه وهي مختصر للعبارة اللاتينية التي تعني نفس المرجع
DDOS	Distributed Denial of Service	هجمات حجب الخدمة الموزعة
IRRC	Inter national Review of Red Cross	مجلة الدولية للصليب الاحمر

[ل]

U.S	United states	الولايات المتحدة
UN	United Nations	الأمم المتحدة
ITU	Inter national Telecommunication Union	الاتحاد الدولي للاتصالات
NATO	The North Atlantic Treaty Organization	حلف الشمال الاطلسي

المقدمة

أولاً: موضوع البحث

يطرح التطور المضطرد في عالم تكنلوجيا المعلومات والإتصالات وتطبيقاتها تحدياً كبيراً فقد شهد المجتمع الدولي موجة انتشار واسعة لإستخدام الاجهزة الحاسوبية، والشبكة العنكبوتية التي جعلت حياة الإنسان والدول و عرضة لمخاطر الأسلحة المعلوماتية التي تنفذ من خلال الفضاء المعلوماتي.

وقد قامت الدول بالآونة الأخيرة من التطوير أسلحة مستحدثة، يتم استخدامها بوسائل وأنواع متعددة، تتمثل بالهجمات المعلوماتية، التي تتسم بتقنيتها العالية ودرجة تعقيدها، وتكون عابرة للحدود التقليدية، وهي قادرة على إحداث اضراراً جسيمة في البنى التحتية للدول، فضلاً عن تدمير النظام المعلوماتي للدول المستهدفة وبصورة كلية أو جزئية، وقد لا تقتصر الأضرار الناجمة عنها خسائر مادية فقط، بل قد يتعداها ليصل إلى أحداث خسائر بشرية، وخصوصاً إذا ما علمنا أن هذهِ الهجمات هي مصاحبة للنزاعات المسلحة، كذلك تبقى الأنظمة المعلوماتية العسكرية في مرمى هذه الهجمات لما تتعرض له من تجسس معلوماتي وسرقة بيانات والولوج إلى البنية التحتية الحساسة للأمن العسكري، وبذلك أصبح الفضاء المعلوماتي الذي يحتوي على جميع الأنظمة المعلوماتية، وشبكاتها مسرحاً لجميع العمليات المعلوماتية التي تنفذها الدول نفسها أو بواسطة فاعلين من غير الدول ولكن يكونوا تحت إشرافها أو سيطرتها، وتجري هذه العمليات من خلال استخدام الحاسب الآلي وشبكاته لطرف معين، يتم توجيهها إلى حاسب آلي وشبكاته يكون تابع للدولة المعتدى عليها ويروم من خلالها منفذوا الهجمات استهداف المعلومات والبيانات المخزنة أو المنقولة بواسطة تلك الشبكات بهدف إتلافها أو نفيها أو تدميرها كلياً بأستخدام أسلحة معلوماتية متنوعة كالفيروسات وأحصنة طروادة التي هي نوع من البرمجيات الخبيثة، والقنابل المنطقية أو المعلوماتية، وغيرها من الأسلحة المعلوماتية التي تتسم بخصائص معينة مثل انخفاض تلكفتها مقارنة بتكلفة الأسلحة التقليدية، وصعوبة الكشف عن هوية الفاعلين، علاوة على ذلك تكون عابرة للحدود الإقليمية.

ونتيجة الخصـائص الفريدة التي يتميّز بها الفضـاء المعلوماتي من إنعدام الحدود الجغرافية وصـــعوبة معرفة هوية المهاجم المعلوماتي، أصـــبحت الدول في تســارع محموم لإســتخدام هذا الفضاء بأنشطة معلوماتية تنفذ عبر هذا المجال الذي له تأثير سلبي في تدهور العلاقات الدولية وتعريض الأمن والسلم الدوليين للخطر.

وقد أفرزت هذهِ الأنشطة التي يتم شنها في الفضاء المعلوماتي تحدياً أخراً، يتمثل بالمساس بســيادة الدول، حيث أن الســيادة لم تبقى عما كانت عليه في ظل مفهوم الســيادة المطلقة، بل طرأت عليها تغييرات عديدة نتيجة عوامل متنوعة حولتها من ســيادة مطلقة إلى ســيادة نســبية، وبالتالي فأن كان المختصـون في الشـأن القانوني قد أهتموا بدراسـة وتحليل مبادئ القانون الدولي الإنساني، إلا أن قواعد القانون الدولي الإنساني لم تشر صراحةً إلى مدى خضوع هذهِ الهجمات المعلوماتية لتلك القواعد، فقد اختلفوا في مســـألة التكييف القانوني لها، بين مؤيد ومعارض وبين مسـألة خضـوعها من عدمه، على الرغم من شـمولية قواعد القانون الدولي الإنسـاني لاسـتيعاب الكثير من التطورات التكنولوجية ذات الصلة بالأسلحة المستحدثة.

إلاّ إن هناك تحدياً يواجه القانون الدولي الإنســـاني فيما يخص مدى امتثال الهجمات المعلوماتية لقواعده، بســبب التقارب والتداخل بين الشــبكات المعلوماتية التي تكتســي بالصــفة المدنية وأخرى ذات الصـفة العسـكرية، وبالتالي يصـعب الفصـل بين تلك الشـبكات، فعند إطلاق فيروسـات بأسـلحة معلوماتية معادية لا يمكن التكهن باصـابة هدفها العسـكري بدقة دون احداث أضراراً عرضية بالمنشآت المدنية أو بين صفوف المدنيين غير المشتركين بالنزاعات المسلحة.

وأضـــحت الدول تواجه تحدياً آخر هو على قدراً كبيراً من الأهمية إلا وهو كيفية إيلاء واجب العناية اللازمة عند تسيير انشطتها المعلوماتية، فواجب العناية هو معيار يتحدد من خلاله سـلوك الدول بأحترام حقوق الدول الأخرى وعدم الأضـرار بها، حيث يشـير معيار واجب العناية إلى الزام الدول بعدم السـماح بأسـتخدام اراضـيها الخاضـعة لإقليمها وولايتها القضـائية بقصـد الاضـــرار بحقوق الدول الأخرى، وواجب العناية هو ذو طبيعة عرفية، وقد أكدت هذهِ الطبيعة العرفية لهذا المعيار محكمة العدل الدولية عند النظر بقضـية قناة كورفو عام ١٩٤٩بين بريطانيا

والبانيا، وأشـــار إليه دليل تالين في القاعدة (٦) منه على الرغم من عدم إلزامية قواعده، التي نصـت على ممارسـة الدولة لواجب العناية في عدم السـماح باسـتخدام اراضـيها أو بنيتها التحتية المعلوماتية الخاضـعة لسـيطرتها الحكومية في العمليات المعلوماتية التي تؤثر على حقوق الدول الأخرى.

وبالتالي فأن الدول أصـبحت معنية بالإمتثال لواجب العناية المعلوماتية على الرغم من أن هذا المفهوم يتسم بغموضه وعدم تعريفه تعريفاً دقيقاً، إذ تمت الإشارة إليه بصورة غير مباشرة في نصـوص بعض الأتفاقيات ذات الصـلة بالضـرر البيئي. كذلك يكتسـي واجب الحياد المعلوماتي أهمية بالغة تتمثل بالتزام الدول بواجب الحياد المعلوماتي وعدم خرق هذا الالتزام، إذ يحظر على المتحاربين أسـتخدام البنية التحتية المحايدة لغرض شـن هجمات ضـد الخصـم أو ضـد الأخرين. ويوجب كذلك على الدول عدم التدخل الضـــار في البنية التحتية المعلوماتية المحايدة، وبالتالي فهي ملزمة بأنهاء ومنع انتهاك الحياد، ونتيجة لعدم امتثال الدول لواجب العناية اللازمة، ذات الصـــلة بامتثال الأســلحة المعلوماتية لقواعد ومبادئ القانون الدولي الإنســاني فأن هذا الانتهاك يؤدي إلى نشــوء المســؤولية الدولية على عدم امتثال الدول لهذا الواجب لكن تبقى مســألة التزام الدول هي مسألة تقديرية خاضعة لمصلحتها وفي ضوء سيادتها الاقليمية وهي مسألة محل نظر في ضـــوء امتثال الدول لواجب العناية المعلوماتية المتمثل بمنع وانهاء الهجمات المعلوماتية الضارة بالدول الأخرى.

ثانياً: أهمية البحث:

إن لموضوع البحث أهمية كبيرة في القانون الدولي تتمثل بأسباب عدة منها:

السبب الأول: أن موضوع الدراسة هو من الموضوعات التي حازت على اهتمام المختصين في الشـأن القانوني والاكاديميين والخبراء في القانون الدولي، نتيجة حداثة موضـوع واجب العناية المعلوماتية اللازمة للدول، هذا الواجب الذي يلزم الدولة عند ممارسـتها لحقوقها في اطار إقليمها وسيادتها أن تحترم حقوق الدول الأخرى وعدم الإضرار بها.

والسـبب الثاني: يكمن في تزايد اللجوء لإسـتخدام الهجمات المعلوماتية في هذا الفضـاء المعلوماتي، الأمر الذي يستدعي معه امتثال الدول لواجب العناية المعلوماتية اللازمة، خصوصاً إذا ما علمنا أن الهجمات المعلوماتية تفتقر إلى الأسـاس القانوني لتنظيمها، وتكمن الأهمية الأخرى لهذا البحث في كونه يعالج موضـوعاً حديث النشـأة على الرغم من إن مفهوم واجب العناية له جذور قديمة إلا إنه ما زال في طور التبلور الذي لم تكتمل بعد معالمه القانونية.

السـبب الثالث: يتمثل بيان مدى امتثال الدول لواجب العناية من الهجمات المعلوماتية، علاوة على أهميته في سياق المسؤولية المترتبة على عدم امتثال الدول لواجب العناية ، لا سيما في إطار القانون الدولي الإنساني، والقانون الدولي لحقوق الإنسان، فضلاً عن أهمية هذا المبدأ في إطار مسألة حياد الدول المعلوماتي.

ثالثاً: أشكالية البحث:

في البدء لا بد من الإشـارة إلا أنه ليسـت هناك أحكام أو نصـوص أو وثيقة من وثائق القانون الدولي، تناولت بصورة صريحة ومباشرة موضوع واجب العناية اللازمة للدول، في اطار الهجمات المعلوماتية، وهذا ادى بطبيعته إلى اثارة جدلية بين جمهور فقهاء القانون الدولي، عن مدى امتثال الدول لواجب العناية من الهجمات المعلوماتية والمسؤولية الدولية الناشئة عنها، وهذهِ الجدلية انسحبت بآثارها على مدى إمكانية تطبيق واجب العناية في سياق القانون الدولي البيئي والقانون الدولي لحقوق الإنسـان، فضـلاً عن مدى إمكانية تطبيقه في سـياق امتثال الأسـلحة المعلوماتية لهذا الواجب، ومدى التزام الدول بمعيار واجب العناية عند تنفيذ هجمات معلوماتية عبر الفضـاء المعلوماتي والأهم من ذلك هو مدى ملائمة تطبيق قواعد ومبادئ القانون الدولي الإنساني على الهجمات المعلوماتية.

وبالنظر لحداثة الموضـوع في ميدان العلاقات الدولية، فأن أهم التسـاؤلات التي يمكن طرحها بهذا الصدد هي:

١- ما المقصود بالهجمات المعلوماتية؟ وما هي انواعها واساليب استخدامها في الفضاء المعلوماتي؟

٢- ما المقصود بواجب العناية المعلوماتية اللازمة للدول؟

٣- هل إن معيار واجب العناية هو معيار يقاس به سلوك الدول؟ أم أنه نتيجة تسعى الدول لتحقيقها؟

٤- ما المقصود بالسيادة المعلوماتية؟ وهل أن سيادة الدول وولايتها الإقليمية والقضائية هي سيادة مطلقة أم نسبية؟

٥- ما مدى إمكانية تطبيق واجب العناية المعلوماتية في سياق المبادئ العامة للقانون الدولي؟ وما المقصود بالحياد المعلوماتي للدول؟ وما معيار عدم التدخل الضار بالبنية التحتية المعلوماتية؟

٦- إلى ماذا ينصرف مفهوم عدم الامتثال الدولي؟ وما هي أسبابه؟

٧- ماهي التدابير المضادة؟ وما مدى مشروعيتها عند اللجوء إليها كخيار للرد على هجمات معلوماتية معادية؟ وكيف تنتفي المسؤولية الدولية الناشئة عن إستخدامها؟

٨- ما هو نطاق التدابير المضادة؟ وما القيود الواردة عليها؟ وما هي المصلحة من فرض هذهِ القيود القانونية؟

٩- ما المسؤولية المترتبة على عدم امتثال الدول لواجب العناية؟ وهل تشمل الافراد والكيانات أم إنها تقتصر على الدول فقط؟

رابعاً: منهجية البحث:

عندما يسعى الباحث لتكوين رأي قانوني سديد، فأنه يتوجب عليه الخوض في التأصيل والمقارنة كلما كان ذلك مستطاعاً ويتمكن الباحث من إدراكه، وبالتالي يتيح للباحث الوصول لغاية البحث التي يرومها وهي التجديد والإبتعاد عما هو قديم تمهيداً لوضع الحلول الملائمة للمشاكل التي يثيرها البحث، وعند تسليط الضوء على مفهوم واجب العناية اللازمة للدول اعتمدنا على المنهج الوصفي، ثم اعتمدنا كذلك المنهج التحليلي القائم على اساس تحليل القواعد القانونية الدولية، ومن ثم المنهج التطبيقي القائم على الاجتهادات الفقهية والسوابق القضائية.

خامساً: خطة البحث:

ولما تقدم ارتأينا دراسة الموضوع على وفق خطة منهجية تقوم على تقسيمه على مقدمة و ثلاث فصول وعلى النحو الآتي:

الفصل الأول: ماهية الهجمات المعلوماتية: وسنقسمه على مبحثين، نتناول في المبحث الأول، مفهوم الهجمات المعلوماتية، أما في الثاني، سنتطرق فيه للتكييف القانوني للهجمات المعلوماتية.

الفصل الثاني: ماهية واجب العناية اللازمة للدول:

وسنقسمه على مبحثين، كرسنا المبحث الأول منه للتعريف بواجب العناية في اطار الهجمات المعلوماتية، أما الثاني سنفرده للجهود الدولية في اطار واجب العناية للحد من اضرار الهجمات المعلوماتية.

الفصل الثالث: ماهية عدم إمتثال الدول لواجب العناية اللازمة:

وفيه مبحثين، سنقصر المبحث الأول على التعريف بعدم الإمتثال لواجب العناية اللازمة للدول، أما الثاني سنتناول فيه المسؤولية الدولية المترتبة على عدم إمتثال الدول لواجب العناية.

ومن ثم نستتبع ذلك بخاتمة تتضمن جملة من الاستنتاجات والمقترحات التي توصلنا إليها والتي نأمل أن تجد سبيلها للتطبيق، عسى الله أن يلهمنا سبيل الرشاد وهو ولي التوفيق.

الفصل الأول

ماهية الهجمات المعلوماتية

تشـــكل الهجمات المعلوماتية أحد أهم مراحل التطور الكبير في مجال أســـاليب القتال في أوقات السلم أو النزاعات المسلحة، وقد اكتسبت هذه الهجمات أهميتها من توسع استخدام الوسائط المعلوماتية في العديد من القطاعات المدنية ، والتقنيات العســـكرية، والهجمات المعلوماتية هي التي يقوم بشـنها أحد طرفي النزاع والموجهة للحواسـيب والشـبكات، سـواء لتعطيلها أو إتلافها، أو السـيطرة عليها ، وتم توظيف هذه للهجمات باسـتخدامات شـتى تخص الحياة العادية في عمليات القرصـــنة المعلوماتية إلى جانب قدراتها التدميرية الهائلة التي تتســبب في احداث إضــرار مادية على نطاق واســـع والتي اصـــبحت متاحة لإســـتخدامها من قبل جميع الفاعلين في الفضـــاء المعلوماتي من دول أو شركات أو حتى الأفراد أو الكيانات.

إلاّ أن الهجمات المعلوماتية التي تحدث في اطار القانون الدولي الإنســـاني، هي تلك الهجمات التي تستهدف الحواسيب والشبكات العائدة لدولة معينة، مما يهدد الاحتياجات الضرورية للسـكان المدنيين، كالأنظمة التي تتحكم في مصـادر الطاقة الكهربائية والنووية، ومصـادر المياه كالســـدود والابار ووحدات الخدمات الطبية اللازمة لرعاية الســـكان المدنيين، ويمتاز الفضـــاء المعلوماتي الذي تجري فيه هذه الهجمات بخصـــائص فريدة من نوعها في ميدان النزاعات بين الخصـوم، تسـتطيع من خلالها الدولة أو الكيانات من شـن هجمات ضـد خصـوم محددين وعلى مسافات شاسعة جداً من دون تعرضهم للخطر، إذ تمتاز هذهِ الهجمات التي يتم توجيها من خلال الفضـاء الرقمي بأنها صـامته، ولا تحتاج إلى تكاليف باهضـة، فضـلاً عن صـعوبة الكشـف عن هويـة الفـاعلين، وقلـة الموارد التي يتطلبهـا تنفيـذ هجوم معلومـاتي على هدف محـدد، كمـا وأن الخســـائر الناجمة عن هذهِ الهجمات تكاد أن تكون ضـــئيلة أو معدومة بالقياس مع الهجمات بالاسـلحة التقليدية. ومما لا شـك فيه أن من يقود الهجمات المعلوماتية هم القراصـنة المحترفون في الفضـاء المعلوماتي، والذين يطورون برامج الاختراق والقرصـنة ومعظم انشـطتهم المعلوماتية

لاتتصل بنزاع مسلح، فهي تندرج ضمن جرائم القانون الدولي العام، إلا إن الجيوش الحديثة باتت تعتمد على وحدات عسكرية معلوماتية تتولى تنفيذ الهجمات والدفاع في الفضاء المعلوماتي.

وأصبحت الدول اليوم تبحث عن ملاذ أمن ضمن إطار قانوني باستخدام القوة للرد على هجمات معلوماتية غير مشروعة وترى ضرورة تكيف تلك الهجمات ضمن القانون الدولي التقليدي أو القانون الدولي الإنساني ، ومدى انطباق قواعد ومبادئ الحرب على الهجمات المعلوماتية وللإحاطة بموضوع هذا الفصل ارتأينا تقسيمه على مبحثين نتناول في الأول مفهوم الهجمات المعلوماتية ، ونخصص الثاني للتكييف القانوني للهجمات المعلوماتية وعلى الشكل الآتي:

المبحث الأول

مفهوم الهجمات المعلوماتية

نتيجة للتطور التكنلوجي المتسارع في مجال استخدام تكنلوجيا المعلومات من قبل الدول، أصبح الفضاء المعلوماتي تبعاً لذلك مرشحاً بقوة لأن يكون ساحة جديدة للنزاعات التي تحدث بين الخصوم من الدول، والتي تدار بأسلحة وأدوات حديثة مختلفة عما هو شائع في الحروب التقليدية سواء من حيث الشكل أو المضمون، وينتج عن ذلك تغيير في طبيعة الحرب ذاتها، فهي لا تستهدف في غاياتها تدمير الآليات والمعدات العسكرية والقوات البشرية للخصم، ولا تهدف إلى الإستيلاء على أرضه أو إحتلالها، وإنما لإلحاق الضرر البالغ بالبنية التحتية المعلوماتية العائدة بأقل تكلفة مادية وخسائر بشرية.

لذلك شهدت القواميس والموسوعات المعرفية ولادة مفاهيم جديدة مثل حرب المعلومات، والحرب الرقمية، وحرب الشبكات ، والهجمات المعلوماتية، وبالتالي إنتقلت هذهِ المفاهيم من المستوى النظري المجرد، إلى المستوى الواقعي الملموس، وبما إن الهجوم المعلوماتي من المفاهيم الحديثة نسبياً والذي يكتنفه الغموض، ولغايات هذا البحث ارتأينا أن يشتمل مفهوم الهجمات المعلوماتية على التطرق لتعريفها وإيراد أهم الخصائص التي تتصف بها عن غيرها من

الهجمات التقليدية، فضــلاً عن تناول أهم انواع هذه الهجمات ووســائل وإســاليب اســتخدامها، مع التأكيد على أهمية تمييز هذهِ الهجمات المعلوماتية عما يشتبه بها من مفاهيم اخرى.

ولبحث ذلك سنقسم هذا المبحث على مطلبين:

المطلب الأول: تعريف الهجمات المعلوماتية وأنواعها.

المطلب الثاني: خصائص الهجمات المعلوماتية وتميزها عن غيرها من المتشابهات.

المطلب الأول

تعريف الهجمات المعلوماتية وأنواعها

إن مسألة تعريف الهجمات المعلوماتية تعريفاً محدداً عاماً شاملاً ، هي من التحديات التي تشكل عائقاً أمام المختصـــين في القانون الدولي ، وقد يعزى الأمر لحداثتها أو غموضـــها ، أو يعود الســبب في ذلك لعدم اتفاق الدول على تنظيم اســتخدامها أو كيفية مواجهتها . وكان هناك جدل فقهي في تناول تعريف الهجمات المعلوماتية ، فقد تباينت اراء الفقهاء والمفكرين، والمختصين في القانون الدولي عند تعرضــهم لهذا المفهوم ، فضــلاً عن ظهور اتجاهان رئيســيان حاولا تعريف الهجمات المعلوماتية كل حسب وجهة النظر الذي يدافع عنها وهما مدرسة حلف شمال الأطلسي الناتو (NATO)، ومنظمة شنغهاي للتعاون ، ولكل مدرسة من هذه المدارس مؤيدين ومعارضين، إذ يرى أنصــار منظمة حلف شــمال الأطلســي (NATO) ، أن الحرب المعلوماتية تنحصــر في اطار المعلوماتية ، بينما يرى أنصــار منظمة شــنغهاي للتعاون ان الهجمات المعلوماتية تشــكل جزءاً من الحرب المعلوماتية.

علاوة على ذلك فالهجمات المعلوماتية لا تنحصر في نوع محدد وانما لها انواع متعددة مما يشكل عائقاً في كيفية التصــدي لها والحد من تأثيرها على الخصــوم . ولبحث ما تقدم ، ســنناقش هذه المواضيع في فرعين نتناول في الفرع الأول تعريف الهجمات المعلوماتية، أما في الثاني سنتطرق إلى أنواع الهجمات المعلوماتية ووسائلها.

الفرع الأول

تعريف الهجمات المعلوماتية

تكمن المشـكلة الاسـاسـية في إيجاد تعريف مقبول ومحدد للهجمات المعلوماتية ليس فقط من غياب الاجماع بين فقهاء القانون الدولي، بل أيضـــاً من الطبيعة القانونية المتغيرة لهذهِ الهجمات المتطورة التي تتم عن طريق الشـبكة المعلوماتية، والسـبب الرئيسـي إن هذهِ الهجمات على شبكات الحواسيب هي ظاهرة حديثة نسبياً، فالأسلحة المعلوماتية هي فيروسات وبرمجيات ضارة ، يتم تصميمها على شكل برامج حاسوب لشن هجمات معلوماتية على اهداف عسكرية أو مدنية، الغرض منها تدمير النظم ، أو الاجهزة والمعدات أو البرمجيات العائدة للخصـم، أو يكون هدفها الحاق خلل ســـواء كان وظيفياً ام فنياً ، فهذه الاســـلحة المعلوماتية تختلف من حيث خطورتها او درجة تعقيدها ، فمنها ما هو قادر على احداث ضـــرر بالنظم المعلوماتية دون اختراقها، ومنها ما هو قادر على اختراق النظام وتدميره كلياً ، أو ربما توقفه عن الخدمة بصـورة نهائية.

كذلك تمتاز الهجمات المعلوماتية بتعدد أنواعها على وفق معايير محددة كهجمات رفض الخدمة ، والهجمات الطمسـية وهجمات اختراق شـبكات الحاسـوب، وقد يكون معيار تصـنيف الهجمات المعلوماتية حسب أسلوب تنفيذها، أو حسب القطاع المستهدف منها ، أو حسب الهدف النهائي من هذه الهجمات أو الفواعل المشـاركون في تنفيذها، إذ يجري إختراق الحيز الإفتراضـي أو الفضاء المعلوماتي للدول عن طريق مجموعات من قراصنة الحاسوب ، هؤلاء يتمتعون بالقدرة على التحكم في برامج الحاسوب وطرق ادارتها .

والسؤال المطروح للنقاش بهذا الصدد ما المقصود بالهجمات المعلوماتية؟ وماهي اتجاهات المدارس الفقهية وآراء المختصين بالشأن القانوني الدولي حول مسألة تعريفها؟ وللإجابة عن هذهِ التســاؤلات، لابد من بيان تعريف الهجمات بصـــورة عامة ومعنى المعلوماتية ثم تناول بعد ذلك الهجمات المعلوماتية في ضوء الإجتهادات الفقهية وأهم الاتجاهات الفكرية والقانونية التي تطرقت لها بشيء من التفصيل :

لقد عُرفت الهجمات بصورة عامة بأنها (أعمال العنف الهجومية والدفاعية ضد الخصم، وتنطبق أحكام هذا البروتوكول المتعلقة بالهجمات على كافة الهجمات في أي إقليم تشن منه بما في ذلك الاقليم الوطني لأحد اطراف النزاع... وتسري احكام هذا القسم على الأفراد المدنيين أو الأعيان المدنية على البر، كما تنطبق على كافة الهجمات الموجهة من البحر أو من الجو ضد أهداف على البر ولكنها لا تمس بطريقة أخرى قواعد القانون الدولي التي تنطبق على النزاع المسلح في البحر أو الجو)[١] . أما مصطلح المعلوماتية فقد استخدم لأول مرة عام ١٩٦٢، من قبل فيليب دريفس (Philip drefus) [٢] أثناء محاولته تمييز المعالجة الآلية للمعلومات ، ثم تبنت الأكاديمية الفرنسية هذا المصطلح عام ١٩٦٦، وعُرف على أنه "علم المعالجة المنطقية للمعلومات، والتي تعتبر بمثابة دعامة للعلوم الإنسانية والاتصالات في المجالات الفنية والإقتصادية والإجتماعية وذلك باستخدام معدات آلية "[٣] .

اما سبب اختيارنا لتسمية الهجمات المعلوماتية دون غيرها من التسميات الأخرى فقد جاء بناءً على البحث والاستقصاء في المصادر القانونية ذات الصلة ووجدنا هناك تباين في الرؤى والاتجاهات الفكرية التي حاولت أيجاد تسمية مناسبة لهذهِ الهجمات فمنهم من اختار مصطلح الهجمات الالكترونية أو السيبرانية (cyber attacks) كوصف واقعي باعتباره تصرف يدور في عالم افتراضي قائم على اساس استخدام البنى التحتية الرقمية ووسائل اتصال تعمل الكترونياً،

---

[١] المادة (٤٩ / ١) من البروتوكول الاضافي الاول لعام ١٩٧٧ الملحق بإتفاقيات حنيف لعام ١٩٤٩ والمتعلق بحماية ضحايا النزاعات الدولية المسلحة.

[٢] لقد صاغ عالم الكمبيوتر الالماني (كارل ستبينبوش) عام ١٩٥٧، عبارة المعلوماتية من خلال نشر ورقة سماها المعلوماتية، وتعني (تقنية المعلومات: المعالجة التلقائية للمعلومات). ان تقنية المعلومات هي تعبير عن المصطلح بالانجليزية والتي تفهم احياناً كعلم الحاسوب الآلي، ومع ذلك فأن المصطلح الالماني للمعلوماتية هي الترجمة الصحيحة لعلم الحاسبات باللغة الانجليزية، اما علم المعلوماتية الفرنسي فقد صاغه الفرنسي (فيليب دريفوس) عام ١٩٦٢ جنباً إلى جنب اثناء محاولته تمييز المعالجة الآلية للمعلومات.
للمزيد ينظر بهذا الصدد، د.عزة محمود احمد خليل، مشكلات المسؤولية المدنية في مواجهة فيروس الحاسب الآلي ، دراسة مقارنة في القانون المدني والشريعة الاسلامية، اطروحة دكتوراه ، كلية الحقوق، جامعة القاهرة، ١٩٩٤، ص١٨.

[٣] محمد سامي الشوا ، ثورة المعلومات وانعكاساتها على قانون العقوبات ، دار النهضة العربية . القاهرة، ١٩٩٤ ، ص٤

بعد ذلك حدث تطوراً يشـمل مفهوماً اوسـع قائم على تحقيق اهداف عسـكرية أو أمنية ملموسـة ومباشـرة، نتيجة اختراق مواقع الكترونية حساسـة، غالباً ما تؤدي وظائف يتم تصـنيفها على انها ذات أهمية، كأنظمة حماية منشـــآت الطاقة النووية أو الكهربائية او المطارات أو وســـائل النقل الأخرى.[١]

ونعتقد ان هذهِ التسـمية للهجمات قد أقتصـرت على نطاق ضـيق من الهجمات المحددة لتشمل فئات معينة من هذهِ الهجمات التي تستهدف شبكة الحاسوب، ومنها الهجمات على البنى التحتية لدولة معينة، من دون التوسـع باسـتخدام أنشـطة سـيبرانية معادية ذات أبعاد سـياسـية أو اقتصـــادية، علاوة على ذلك فأن المختصـــين في اللغة العربية، يواجهون ثمة تحدياً في اختيار مصـطلح مقارب للسـيبرانية، وذلك بسـبب عدم شـيوع إسـتخدام كلمة المعلوماتية في قواميس اللغة العربية، إذ تم اعتماد مصـطلح القوة الالكترونية للدلالة على القوة السـيبرانية، ومن الجدير بالذكر إن هذا الخطأ الشائع غير دقيق علمياً لكون الترجمة الحرفية للقوة الالكترونية هو (Electronic cyber).[٢] عند استقراء معاني هذهِ التسميات التي تناولت مصطلح المعلوماتية أو الالكترونية، نجد إن مصـطلح الهجمات المعلوماتية اكثر انسـجاماً من التسـميات الأخرى لما له من دلالات تستقيم مع مقتضيات القانون الدولي العام.

من الجدير بالذكر أن هناك اتجاهان رئيسان طرح كل منهما بشكل مختلف تعريف لمفهوم الهجمات المعلوماتية فمنهم من قام بتعريف الهجمات المعلوماتية على اساس الهدف والنتائج من تلك الهجمات، وقد تبنى الاتجاه، الآخر أســـلوباً مغايراً من خلال تعريف الهجمات المعلوماتية على أساس الوسيلة التي تستهدف المنشآت المرتبطة بالفضاء المعلوماتي ،وسنتعرض بشيء من التفصـيل لأهم الآراء التي يتبناها اصـحابها و التي طرحت من قبل هذين الاتجاهين وعلى النحو الآتي:

---

[١] د.حيدر كاظم عبدعلي ورباب محمود عامر، التنظيم القانوني للهجمات السيبرانية على المنشآت ذات القوى الخطرة، مجلة الكوفة للعلوم القانونية والسياسية، ع (٤٧)، كلية القانون جامعة الكوفة، ٢٠١٩، ص١١٠.

[٢] د.ايهاب خليفة، القوة الالكترونية، كيف يمكن ان تدير الدول شؤونها في عصر الانترنت، الولايات المتحدة انموذجاً ، ط١، دار العربي للنشر والتوزيع، القاهرة، ٢٠١٧، ص٥.

أولاً: مدرسة حلف الناتو (التعريف القائم على اساس الهدف أو الغرض).

جرت محاولات عدّة لإخضـــاع الهجمات المعلوماتية الى قواعد القانون الدولي الإنســـاني وخصـوصـا تلك التي تسـتهدف المنشـآت العسـكرية، والأنظمة التي تتحكم بالحاجات الأسـاسـية للسكان المدنيين، كالسدود والآبار، ومحطات الطاقة الكهربائية والنووية ووحدات الخدمات الطبية، ومن بين المحاولات الدولية الســـباقة في معالجة آثار هذه الهجمات جاء "دليل تالين[١]، للقانون الدولي المطبق على الحرب المعلوماتية" المنشـور عام ٢٠١٣. كوثيقة قانونية في وضـــع القواعد والأســـس التي يجب الاســـتناد إليها في مثل هذه الهجمات والذي اعدته مجموعة من الخبراء في القانون الدولي بدعوة من حلف شمال الاطلسي NATO ، وكان الغرض منه دراسة مدى امكانية تطبيق قواعد القانون الدولي الانساني على الحروب المعلوماتية.

وقدم الخبراء في دليل "تالين" روى حديثة حول عدم وجود فراغ قانوني يخص هذا النوع من الأسـاليب الحربية، بحيث يحتاج الامر إلى عملية إسـتعراض مشـروعية هذه الأسـلحة وفق المادة (٣٦) من البروتوكول الإضـافي الأول على ضـوء قواعد القانون الدولي الإنسـاني، وبهذا الصـــدد فقد عرف الخبراء في دليل تالين الهجمات المعلوماتية بأنها "عملية معلوماتية ، ســـواء كانت هجومية أو دفاعية يتوقع منها أن تتسبب في إصابة أو قتل أشخاص أو الأضرار بأعيان وتدميرها"[٢].

هذا يعني أن الخبراء في دليل تأليف قد تبنوا بصـــورة صـــريحة (الاتجاه الضـــيّق) الذي يحاول أن يحصر الهجمات المعلوماتية في نطاق الأضرار كالإصابة ، والوفاة، وتدمير الأهداف وهو نفس الإتجاه التي تبنته القيادة المعلوماتية المشتركة للولايات المتحدة الأمريكية عام ٢٠٠٧،

---

(1) Tallinn Manual on the international Law Applicable to cyber warfare, prepared by the international Group of Experts at the invitation of the NATO cooperative cyber Defence , center of Cambridge U.K and also in New York U.S.A , 2013 ,p.29.

(2) Tallinn Manual .,A Cyber-Attack is a cyber –operation, whether of fensiveor defensive or defensive , that is reasonably expected to cause injury or death to persons or damage or destruction to objects, op. cit, Rule30.

بشـان اسـتخدام الوسـائل المعلوماتية لأغراض عسـكرية، والتي عرفت الهجمات المعلوماتية على أنها "تطويع عمليات نظام الكومبيوتر لغرض منع الخصـوم من الإسـتخدام الامثل لها " وفضـلاً عن إمكانية التسلل إلى نظم المعلومات وشبكات الإتصال بهدف الإستيلاء على المعلومات التي تحتويها والسيطرة عليها وتحليلها"[١].

وبعد فترة وجيزة من إنشـاء القيادة المعلوماتية المشـتركة للولايات المتحدة الأمريكية نشـرت رئاسـة الأركان المشـتركة الأمريكية عام ٢٠١١ في معجمها الخاص بالإسـتخدام العسـكري للعمليات المعلوماتية أول تعريف عسـكري رسـمي للهجوم المعلوماتي على أنه " فعل عدائي يتم باسـتخدام الحاسـوب أو الشـبكات أو الأنظمة ذات الصـلة، يهدف إلى تعطيل أو تدمير أنظمة الانترنت أو الممتلكات أو الوظائف العائدة لأحد الخصـوم "[٢]، ومن مؤيدي هذا الاتجاه الدكتور شـين (shin) الذي يعمل مديرا لقسـم الدراسـات العسـكرية في معهد كوريا الشـمالية للتحليلات الدفاعية الذي بدورة قد عرف الهجوم المعلوماتي على أنه " ... اسـتخدام الطيف الإلكتروني أو المجال الكهرومغناطيسـي لأغراض تخزين ولتعديل وتبادل البيانات وجها لوجه مع أنظمة تحكم في بنى تحتية مرتبطة بها "[٣]، ومن أنصـار هذا الاتجاه مايكل ن شـميت (Micheal N. Schmitt) الذي عرف الهجمات المعلوماتية " بأنها تلك الإجراءات التي تقوم بها الدولة من أجل الهجوم على أنظمة المعلومات المعادية بهدف التأثير والإضـرار فيها، وفي ذات الوقت للدفاع عن نظم المعلومات الخاصـة بالدولة المهاجمة "[٤] نلاحظ من خلال التعريف المتقدم أنه

---

(1) Micheal N.Schmitt, Computer network Attack and the USA of force in international law though A Normative , The Colombia journal of Transitiona law, vol.(27), No.(885-937), 1999,p.7.

(2)Gen.jame SE . cartwright , memorandum for chiefs of the military servs , commanders of the combatant commands, dirs, Of the joint staff directories on joint Terminology for cyber space operation 5 (nov. 2011).

(3) Shin , Beomchul , the cyber warfare and the right self- defence : legal perspectives and the case of the unitedstate , IFANS , vo1.(19), No.1, 2019 . p.105 .

(4)Micheal N.Schmitt, Computer network Attack and the USA of force in international law, Ibid,p.890.

قد جاء قاصـــراً على إســـتعراض قدرة الدولة دون الأفراد بشـــأن الإســـتخدام المزدوج للهجمات المعلوماتية من قبل الدولة، تارة تكون الدولة في وضـــع المهاجم، وتارة أخرى تكون في حالة تصـــدي عن نظم المعلومات الخاصـــة بالدولة المهاجمة، فالفواعل من غير الدول ومنها الأفراد تلعب دورا بارزا بالقيام بالعديد من الهجمات المعلوماتية، بقصـــد الأضـــرار بدولة ما كالهجمات على البنية التحتية الحيوية مثل الطاقة ، والإتصـالات، والمواصـلات، والأجهزة الحكومية وغيرها، وقد تودي لإصـابات لبعض الأفراد أو خسـائر في الممتلكات فضـلاً عن خسـائر إقتصـادية للدولة التي تمت مهاجمتها.

وعلى وفق الاتجاه الذي تبناه الخبراء في دليل تالين وهو التعريف (الضـــيّق) للهجمات المعلومـاتيـة على أســـــاس النهج القـائم على الأهـداف ، فقـد طرحـت أونـا آن هـا ثاواي(OonaA, Hathaway)، أســـتاذة القانون الدولي مع مجموعة من الباحثين رأياً بشـــأن الهجوم المعلوماتي بحسب وجهة نظرهم بأنه "إجراء يتم اتخاذه لتعويض وظائف شبكة الحاسوب وهو أما يكون بدافع سياسي أو أمن قومي، واعتبروا أن الهجمات المعلوماتية هي أوسع نطاقاً من الحرب المعلوماتية فهي قد تحدث خارج نطاق الحروب، وربما قد تكون ســـبباً رئيســـاً لشـــن الحرب"[١]، أي أن الهجمات المعلوماتية هي أحد أســـاليب حرب المعلومات ، وبعبارة أخرى هو الإسلوب الذي يتم من خلاله إستخدام السلاح المعلوماتي.

ومن الأمثلـة التطبيقيـة التي تؤيـد الاتجـاه الضـــيق لمفهوم الهجمـات المعلومـاتيـة هي الهجمات التي شـنتها روسـيا الاتحادية على إسـتونيا عام ٢٠٠٧، فقد اسـتهدف الهجوم شـبكات الطاقة والاتصـالات وأدى إلى تعطيلها، إذ كانت المواقع الحكومية في الدولة الاستونية والصحف،

---

(1) Oona – Hathaway , Rebeca croot–of , William rerdue , philiplevitz , the law of cyber – Attacik, vol.(100), Issue4 , p.833.

الجامعات ، المستشفيات، المصارف ، خدمات الإطفاء والإسعاف، وهي الأكثر إستهدافاً فضلاً عن موقعي رئيس الوزراء ورئيس البرلمان[١].

وكان سبب الهجوم المعلوماتي هو إصدار البرلمان في إستونيا عام ٢٠٠٧، قرارا يقضي بإزالة جميع الأبنية والرموز في العهد الذي كانت فيه إستونيا تحت الاحتلال السوفيتي بعد الحرب العالمية الثانية، وكان من ضمن القرار إزالة تمثال برونزي لضابط من الجيش الأحمر السوفيتي، كان تم وضعه في إستونيا عام ١٩٤٧، وهو أحد الرموز الذي يدل على إنتصار الجيش السوفيتي على الجيش النازي ، وقبل تنفيذ القرار بالإزالة أصبح وجود النصب بؤرة لتجمع الجماعات المتطرفة المعادية للدولة الاستونية، مما دعى البرلمان لإتخاذ قرار بتغيير مكانه[٢].

ونتيجة لهذه التوترات تعرضت إستونيا إلى العديد من الهجمات المعلوماتية واسعة النطاق على نظامها المعلوماتي الذي يتصف بتطوره وقوته ، إذ تم تنفيذ عدد كبير من الهجمات على المواقع الخاصة بالبنوك ، والصحف ، والخدمات الحكومية من بينها هجمات الحرمان من الخدمة ، وتأثرت قدرة تلك المواقع بتقديم الخدمة المنوطة بها، وشعرت إستونيا بخطورة الموقف واستعانت بحلف شمال الأطلسي لمواجهتها، واتهمت إستونيا الحكومة الروسية بأنها تقف وراء تلك الهجمات وعلى الرغم من إنكار روسيا لادعاءات استونيا إلا أنها عادت واعترفت بأنه من الممكن أن يكون الهجوم قد تم من قبل جماعات غاضبة من القرار الاستوني[٣].

ونتيجة لذلك تم تحليل هذا الهجوم من قبل بعض المختصين بالشأن المعلوماتي على أنه على الرغم من صغر حجم استونيا إلا أنها من أكثر الدول اعتماداً على الفضاء المعلوماتي ، فضلاً عن اعتمادها المتزايد على الهيئة المعلوماتية في تيسير شؤون الدولة وتم تقييم هذه

---

(1) Scott j. shackelford , from Nuclear war to Netwar ; Anologizing cyber – Attack in international law , Berkeley journal of international law, vol .(27), issue(1), , 2009 ,p. 193 .

(2) Enekentikk At international cyber in cidents , lagal considertion, CCDCOE publication, 2010 , p.16.

(٣) ريتشارد كلارك وروبرت نيك، حماية الفضاء الالكتروني في دول مجلس التعاون الخليجي ، سلسلة محاضرات ، ط١ ، ابو ظبي ، ٢٠١١ ، ص١١-١٢ .

الهجمات على مرحلتين، الاولى تم استهداف المواقع المعلوماتية الحكومية وبث الأخبار المزيفة، والمرحلة الثانية تستهدف هجمات أشد تعقيداً من الأولى وتم فيها استخدام هجمات الحرمان من الخدمة التي اتسع نطاقها ليطال بشكل واسع البنوك الرئيسية، إذ فاق عدد طلبات الدخول للمواقع على ٤٠٠ موقع بين تجسس وتدمير.[١]

ثانياً: مدرسة شنغهاي للتعاون[٢] (التعريف القائم على اساس الوسيلة)

على النقيض من الاتجاه الضيق الذي تبنته مدرسة حلف شمال الاطلسي (الناتو) ، والذي يركز على حصر الهجمات المعلوماتية في نطاق حدوث الإضرار من هذه الهجمات ، فإن الاتجاه الواسع الذي تبنته مدرسة شنغهاي للتعاون، يمثل نهجا أكثر توسعا تعتمد فيه على الوسائل التي تستخدمها الهجمات المعلوماتية ، فأحد أولويات هذه المنظمة ضمان أمن المعلومات الدولي كأحد العناصر الرئيسة للنظام الموحد للأمن الدولي ضد المخاطر المعلوماتية الناجمة عن إمكانية استخدام وسائل المعلومات والاتصالات الحديثة ، والتي قد تشكل تهديدا مباشراً للسلم والامن الدوليين سواء على الصعيد المدني أو العسكري[٣].

ويرى أنصار هذه المنظمة أن إستخدام تكنولوجيا المعلومات قد يساهم في تقويض الإستقرار السياسي للدول من خلال نشر المعلومات الضارة والتي تهدد الأنظمة الاجتماعية والاقتصادية والثقافية للدول والتي تعد من أهم التهديدات الرئيسية للأمن المعلوماتي[٤].

---

(1) Eneken tikkat, op. cit, p. 17,at, international cyber incidents: Legal eonsidration s, ccd – coe publication, p,16.

(٢) منظمة شنغهاي للتعاون (SCO) تأسست في مدينة شنغهاي الصينية بتاريخ ١٥ حزيران ٢٠٠١ ، ثم اصبحت منظمة دولية اقليمية في عام ٢٠٠٢ ، وتظم في عضويتها كل من الصين وروسيا الاتحادية ، ومعظم جمهوريات الاتحاد السوفيتي السابق في اسيا الوسطى ومراقبيين من الدول الاخرى ، كالهند وايران ، وباكستان ، وتهدف المنظمة إلى مواجهة الارهاب العابر للحدود ، والجريمة المنظمة ، وتجارة الاسلحة ، ولعل أهم هدف تسعى اليه هو لمواجهة حلف شمال الاطلسي (الناتو) ، للمزيد ينظر بهذا الصدد ، ابتسام محمد العامري ، منظمة شنغهاي للتعاون الاقليمي ، اذار – ٢٠١٣ ،ص١–٧، ص١–٧، متاح على الموقع الالكتروني: تاريخ الزيارة ٢٠٢١/٨/١٧ http;lcis.uobaghad.eoduiguploads/workshop/.

(3) Oona A.Hathaway , and others , op. cit , p. 825 .

(4) Shangh cooperation agreement annex1 . at 203 .

وهذا الإتجاه قد تبنى تعريف حرب المعلومات بأنها: "علم النفس الجماعي لغسيل الأدمغة والتي تسعى لزعزعة استقرار المجتمع والدولة ، فضلاً عن إجبار الدولة على إتخاذ القرارات لصالح الطرف المعارض"[١].

والمثال الأبرز لهذه الاتجاه الواسع هو جمهورية الصين الشعبية ، التي توكد أن الهجمات المعلوماتية هي جزء من حرب المعلومات ، في حين تحتل الحرب النفسية موقعا حيويا في إطار الحرب السياسية ، إذ أن الحرب النفسية تستخدم أنماط متعددة من المعلومات بما يتلائم مع خطة شاملة ، الهدف منها التأثير على الخصم ، وميوله، واتجاهاته، ومعرفته ، وتوثر الحرب النفسية على تغير تفسير الخصم للمعلومات فضلا عن التأثير في إرادته ، غالبا ما يتم وضع خطة مدروسة لتقييم هذه المعلومات ومعرفة مدى تأثيرها والنتائج المترتبة عليها[٢]، لذلك تنظر الصين الى المخاطر المعلوماتية من عدة اوجه المتمثلة بالحرب المعلوماتية ، والحرب النفسية ، وحرب الشبكات ، وحرب الاستخبارات ، وحرب القيادة والسيطرة[٣].

وانسجاماً مع ما تقدم فأن منظمة شنغهاي للتعاون يبدو أنها قد تبنت استراتيجية موسعة لهجمات المعلوماتية ، والتي تشمل استخدام تكنلوجيا المعلومات لتقويض الاستقرار السياسي للخصوم ، مما زاد من مخاوف الخبراء من ان هذا التعريف يشكل محاولة لإضفاء الشرعية على الرقابة المتشددة على الخطاب السياسي وحرية ابداء الرأي على الانترنت ، ويتجلى ذلك بصورة خاصة في ضوء قيام الحكومات بمحاولة قمع التنظيمات السياسية المعارضة التي تستخدم وسائل الاعلام في بعض الدول كما هو الحال في الصين ، وبالتالي فأن هذا القمع ينعكس سلبا على الحقوق والحريات الشخصية[٤].

---

(1) Shanjhai cooperation A Gree ment , Annexl, at 209 .

(2) Dean cheng , cyber Dragon inside china's information war fare and cyber operation, praegear , cali fornia , USA , 2017 , p.96 ,

(3) Ibid, p99 .

(4) Oona A . Hathaway and others , op ,cit , p825 .

وهناك امثلة عديدة تؤكد تبني مدرسة شنغهاي للاتجاه الواسع لعل أدلها هو مدى قدرة تأثير الفضاء المعلوماتي على النظام السياسي لدولة معينة ، من خلال التأثير في نتائج الانتخابات وتغيير النظام السياسي فيها، فقد اكدت الكثير من التقارير والدراسات على ان روسيا الاتحادية لعبت دوراً بارزاً ومؤثراً في نتائج الانتخابات الامريكية ، فعلى سبيل المثال تجلى الدور الروسي الواضح من خلال الافصاح عن المراسلات المعلوماتية لمرشح الحزب الديمقراطي (هيلاري كلنتون) والذي أثر بشكل كبير على نتائج الانتخابات الامريكية في حينها ، جاء ذلك من خلال قيام الروس بشراء بعض الاعلانات والتي روجت لمناسبات متعددة خلال حملة الانتخابات الرئاسية الامريكية ، في ذات الوقت اكدت الشركة الامريكية المتخصصة في مجال الاعلان المرتبط بخدمات البحث على الانترنت (غوغل) بعدم وجود اي دليل على صفحاتها الاعلانية يفيد بوجود دعاية روسية [١].

والمثال الأخر المؤيد لهذا الاتجاه هو الهجمات المعلوماتية التي حدثت عام ٢٠١٧، في ظل الأزمة بين روسيا واوكرانيا حول النزاع على شبه جزيرة القرم والمناطق الشرقية والجنوبية الشرقية من البلاد، بدأت سلسلة من الهجمات الروسية المعلوماتية على مواقع المنظمات والمؤسسات الاوكرانية ،بما في ذلك البنوك والوزارات والصحف وشركات الكهرباء ، واستخدام المهاجمون الروس في الهجوم برمجيات ضارة من نوع بيتا[٢].

إن معظم التعاريف التي تناولت الهجمات المعلوماتية تشترك في معنى متقارب وهو استهداف مواقع معلوماتية، أو نظام حاسوب أو جهاز حاسوب من خلال اتصالات معلوماتية

---

[١] حسام ياسر ، اعلانات روسية أثرت على نتائج الانتخابات الامريكية ، وكالة سبوتنيك الروسية ، ٢٠١٧ ،متاح على الرابط الالكتروني تاريخ الزيارة ٢٠٢١/٩/٢٨ : http//:Arabic.sputniknews.com/world /d/2017/09/3/026157443

[2] Saalbeh, Klaus-peter , cyber war methods and practice, Germany – osnabrueck: osnabrueck university, 2019, p.48.

أخرى، مما ينتهك سرية أو سلامة او توفر المعلومات المخزونة عليه، وغالباً ما تكون صادرة من مصدر مجهول أما يسرق أو يغير أو يدمر هدفاً محدداً عن طريق اختراق نظام حساس. [١]

وعلى ضـــوء ما تقدم ذكره من تعريفات ولأجل صـــياغة تعريف جامع مانع يحدد أهداف وأغراض ووســـائل هذه الهجمات في اطار عام محدد يمكننا تعريفها بأنها (طائفة من الأعمال العدائية الموجهة ضـد أنظمة الدولة المعلوماتية، سـواء المخزنة أو التي تمت معالجتها ، أو تلك التي تم تداولها من حاســـوب لأخر بهدف كشـــفها أو ســـرقتها أو تعديلها أو اتلافها أو إيقاف تدفقها).

الفرع الثاني

أنواع الهجمات المعلوماتية ووسائلها

تكون الهجمات المعلوماتية التي تصـــيب النظام المعلوماتي للدول بأنواع متعددة وتتباين درجة خطورتها بحسب شدتها، منها ما يحدث أضراراً في البنية التحتية على نطاق واسع، وقسم منها يؤدي إلى اختراق الأنظمة العســـكرية، فضـــلاً عن أنواع اخرى تهدد انظمة الإتصـــالات والمؤسسات المعلوماتية وغيرها من الانشطة الضارة التي تهدد الأمن والسلم الدوليين، وغالباً ما يتم تصنيف هذه الهجمات حسب الأسلوب المستخدم فيها ، وتارة أخرى يكون تصنيفها بحسب الهدف من هذه الهجمات أو النظام المســـتهدف منها ، لذا ســـنقوم بالتطرق لأنواع هذه الهجمات ووسائل تنفيذها بشيء من التفصيل على النحو الآتي :

اولا:- أنواع الهجمات المعلوماتية: تمتاز الهجمات المعلوماتية بتعدد انواعها وحســـب الغرض من تنفيذها و منها:

١- هجمات رفض الخدمة :

---

[1]pande, Nihar Ranjan: cyber Attacks and counter measures: user perspective, (post-Graduate Diploma in cyber security), uttark hand open university , Haldwani 2016, p1, Available at; http://cutt.ly19ki28jb..

أن هذا النوع من الهجمات هو أحد أخطر أنواع الهجمات المعلوماتية ، إذ يتم اســـتخدام برامج كمبيوتر مخصـــصـــة لهذا الغرض ، أو من خلال الاســـتيلاء على عدد هائل من أجهزة الكمبيوتر وتكوين شبكة روبوتية بينها تسمى (Botent)، يستطيع الاستفادة منها القراصنة في تنفيذ هجمة معلوماتية ضخمة على الضحية واغراقها بالآلاف من الرسائل والطلبات التي تتمكن في النهاية من حجب الخدمة ووقفها ، سواء أكان ذلك موقع انترنت، أم خدمة معلوماتية خاصة أو حكومية[١].

ويقوم هجوم رفض الخدمة على اســـتهداف موارد النظام (Dos) وبالتالي لا يتمكن هذا النظام من الاستجابة لطلبات الخدمة ، كما هو الحال عند تعرض النظام لهجوم الخدمة الموزعة (DDos) ، ولكن الأخير يتم إطلاقه من عدد كبير من الأجهزة المضـــيفة الأخرى ، التي تكون مصابة بأحد البرامج الضارة التي يتحكم فيها المهاجم ، ففي اوقات معينة تصبح هذه الحالات أشد خطورة على حياة الأفراد ، كما هو الحال إذا تسبب الهجوم بإغلاق خطوط الطوارئ في احد المستشفيات المعنية بطلب سيارة إسعاف عندما يتم حجب الخدمة عن مواقعها لفترة طويلة بسبب ارتباطها بشبكة الانترنت .

ولكن هجوم رفض الخدمة الذي يستهدف الأنظمة المعلوماتية وان كان هدفة الرئيسي هو حجب الخدمة عن هذه المواقع ، لغرض أحداث أضرار مادية، وفي بعض الاحيان قد تهدد حياة الأفراد، إلا ان هذه الهجمات يتم تنفيذها بعدة أساليب مختلفة وعلى النحو الآتي :-

أ-حســـب درجة الأتمتة : يتم تنفيذ هذه الهجمات على شـــكل مراحل مثل مرحلة التجنيد والاستغلال والإصابة ، وتحدث الاصابة أما بصورة يدوية أو تلقائية أو شبه تلقائية .

---

[١] إيهاب خليفة، مجتمع ما بعد المعلومات، تأثير الثورة الصـــناعية الرابعة على الأمن القومي، ط١، العربي للنشر والتوزيع، القاهرة ، ٢٠١٩، ص١٢٠.

ب- عن طريق شبكة الهجوم المستخدمة : لإطلاق هجوم (DDos) ، إذ يجوز للمهاجم استخدام ، شبكة مناولة مخصصة لهذا الغرض .

ج- ثغرة أمنية مستغلة : يستفاد منها المهاجم عند وجود ثغرة أمنية في نظام الأمان لرفض الخدمات أو خطأ في تنفيذ بعض البروتوكولات أو التطبيقات المثبتة على نظام الأمان لزيادة التحميل على الموارد التي يعمل من خلالها هذا النظام .

د-حسب ديناميكيات معدل الهجوم : ويكون بالاعتماد على عدد من العوامل التي تستخدم لإنشاء هجوم DDos ، وحسب معدل الهجوم فتارة يكون ثابت وتارة أخرى يكون معدل متغير ، كذلك يمكن العثور على زيادة معدل الهجوم وتذبذب معدل الهجوم بناء على تغيير الآلية.

هـ-حسب نوع الضحية: يمكن انشاء هجوم DDos بالاستناد على أربعة ضحايا مختلفين يمكن الاستناد إليها في إنشاء هجمات DDos، هم هجوم الشبكة أو هجوم المضيف ، وهجوم البنية الأساسية ، وهجوم التطبيق.

و-التاثير: هجوم DDos قد يكون تأثيره اضطرابياً.

ز- الوكيل : يمكن للمهاجم انشاء هجوم DDos من خلال عدة عوامل سواء كانت عوامل متغيرة ام عوامل ثابتة[١]. وهناك أنواع متعددة من هجمات رفض الخدمة الموزعة dos-ddos تتسم بتنوعها وتعقيدها واستخدام أساليب متطورة لتنفيذها إلا أن أكثرها شيوعاً هي هجمات الفيضان [٢].ومن تطبيقات هذا النوع من الهجمات ، هجمات الحرمان من الخدمة الموزعة ، التي تم تنفيذها ضد مواقع حكومية تابعة للحكومة الجورجية عام ٢٠٠٨، كموقع وزارة التعليم وموقع البرلمان والرئاسة فضلا عن البنوك التجارية ومواقع الأخبار ووسائل الإعلام ، كذلك

---

(1) Monowar H.Bhuyan and others, Network Traffic Anomaly Detection and prevention concepts , Technigues, and tools, springer international, publishing, cham, Switzerland, 2017,p.215 .

(2) Bell, camronh, cyber war fare and international law, the need for clarity , Towson university journal of international Affairs, Available At : http://cutt.lyHKdz, Accessed on: 4/10/2021.

تعرض شبكات إخبارية عالمية من بينها السي ان إن والبي بي سي إلى هذا النوع من الهجمات والتي استمرت لعدة ساعات قبل انتهاء الهجوم على هذه المواقع[١].

إلا انه على الرغم من شراسة هجمات الحرمان من الخدمة التي تعرضت لها جورجيا والتي شـــملت عدة مواقع تابعة للحكومة ، إلا ان نطاق القوة التدميرية والإضـــرار الناتجة عنها كان ضـــئيلا نوعاً ما ذلك لأن حجم الخســـائر المترتبة على الهجوم المعلوماتي يرتبط ارتباطا وثيقا بمدى اعتماد الدولة الجورجية على اســـتخدام تكنلوجيا المعلومات في إدارة شـــؤونها، إذ لم تكن جورجيا تعتمد بصـــورة أســـاســـية على تكنلوجيا المعلومات والاتصـــالات في تقديم الخدمات المعلوماتية[٢].

٢- الهجمات الطمسية

يتم شن الهجمات الطمسية من خلال استبدال صفحة الويب الخاصة بالضحية بصفحة أخرى بحيث تقترن محتويات الصفحة الجديدة ببواعث المتسلسل، أو ينطوي أسلوب هذا النوع من الهجوم على إعادة توجيه المســتخدمين نحو موقع شــبكي، وهمي يبدو مطابقاً للموقع الذي كان يستخدمه المستخدمون من قبل، وهذه الهجمات تم تنفيذها عبر استبدال صفحة الويب الخاص بالهدف المهاجم بصفحة أخرى ، بحيث يجعل من الصفحة الجديدة صفحة سياسية ، او غير اخلاقية ، تبعا لبواعث المتسلل ، ومن أحد أساليب تنفيذ هذا الهجوم هو إعادة توجيه المستخدمين نحو موقع شبكي آخر بحيث يبدو مشابها للموقع الذي كان يستعمله المستخدمون سابقاً، إذ يطلب منهم افشـــاء معلومات النفاذ إلى الموقع، ويتم من خلال هجمات التصـــيد الإحتيالي على ســـبيل المثال ، والذي يتعرض فيه الأفراد لعمليات خداع عن طريق توجيهه مواقع يتم من خلالها الحصـــول على أكبر قدر ممكن من المعلومات الخاصـــة بهم، يتم بعد ذلك اســـتخدامها من قبل

---

[١] د. علاء عبد الرزاق محمد السالمي ، المدخل إلى الأمن السيبراني ، الفضاء السيبراني – تهديدات الفضاء السيبراني، الاسلحة الهجومية – وسائل مواجهة التهديدات السيبرانية – استراتيجية الأمن السيبرانية، ط١، دار الذاكرة للنشر والتوزيع ، بغداد ، ٢٠٢١ ، ص١٢٧ .

[٢] د.اماني عصام محمد ، استخدام روسيا للقوة المعلوماتية في تفاعلاتها الدولية، مجلة كلية الاقتصاد والعلوم السياسية ، جامعة القاهرة، م(٢٢)، ع (٤)، ٢٠٢١، ص١٧٧.

المهاجم لتحقيق مغانم مادية وهذه الهجمات دلالية تقلب المحتوى المعلوماتي وتقع ضـــمن فئة الحرب المعلوماتية[١].

وهناك أسـاليب أخرى يسـتخدمها الطرف المهاجم لطمس محتوى المواقع الشـبكية ، يهدف من خلالها الخداع والتضـــليل والتأثير على الرأي العام أو عدم بث الثقة في واقع المحتوى المعلوماتي من خلال إطلاق سيل من الهجمات التي تصيب هذه المواقع ،ومن الأمثلة على ذلك ، عملية اختراق قناة وكالة الأنباء القطرية على شـبكة الانترنت ، من خلال قيام قراصـنة بخرق موقع الوكالة ، بأستخدام أجهزة من داخل الإمارات العربية المتحدة لوضع محتوى زائف يتضمن ملاحظات مثيرة للجدل حول إيران وغيرها من القضـــايا الإقليمية الحســـاســـة على المســـتوى الدبلوماسـي ونسبتها إلى أمير قطر، و أدى هذا الاختراق إلى مقاطعة دولة قطر من قبل مجلس التعاون الخليجي ، وتم توجيه الاتهامات إلى دولة الإمارات التي نأت حكومتها بنفســـها عن المشـاركة في هذا الهجوم . إلا انه بعد فترة وجيزة تسـربت رسـائل محرجة من البريد الإلكتروني للســـفير الإماراتي في الولايات المتحدة الأمريكية ، أعطت انطباعاً إلى أنه دولة قطر قامت بمحاولات القصـد منها الانتقام أو ردة فعل تجاه حكومة الإمارات وسـرعان ما نفت قطر تورطها في هذه الهجمات[٢].

٣- هجمات اختراق شبكات الحاسوب

يجري إختراق الحيز الافتراضي أو الفضاء المعلوماتي للدول عن طريق مجموعات قراصنة الحاسوب، إذ يقوم بهذه العملية شخص، أو مجموعة أشخاص وربما يضع مئات، أو بضع الأف من المســـتخدمين الذين يتمتعون بالقدرة على التحكم في برامج الحاســـب وطرق إدارتها، وهم مبرمجون ذو مســـتوى عالٍ ، يســـتطيعون إختراق أجهزة الحاســـوب والتعرف على محتوياته،

---

[١] د.عبدالعزيز لطفي جادالله ، امن المجتمع الالكتروني بين سياسية السوق الالكترونية والتعاون الدولي في اطار مواجهة الجرائم الالكترونية، ط١، مكتبة الوفاء القانونية، الاسكندرية، ٢٠١٧، ص٢٩٢-٢٩٣.

[٢] عادل رفيق، الجيوبوليتكس السـبيرانية والاسـتقرار في الشـرق الأوسـط كانون الثاني ٢٠١٨، المعهد المصـري للدراسات، ص٧، متاح على الموقع إلكتروني: تاريخ الزيارة ٢٠٢١/١١/٨: http:eipss,eg,org

ومعظمهم يرفضــون التصــريح عن هويتهم الحقيقية خشــية الملاحقة من أجهزة الدولة ويختارون لأنفسهم صفة مجهولة وهناك عدة محاور رئيسية يمكن أن يلجأ إليها الهاكرز ، للولوج إلى شبكة الحواســيب وإن يحدثوا فيها أضــراراً مثل الحصــار الافتراضــي الذي يهدف إلى خلل في آليات ســـريان العمليات التقليدية ، وقنبلة البريد الالكتروني Email Bomb، التي يتم من خلال هذه العملية ارسال كم هائل من الرسائل الالكترونية إلى صندوق البريد الالكتروني للخصم، التي ينشأ عنها تعطل قدرة البريد على تلقي الرسائل والتعامل معها[١].

والمثال الأبرز لهذه الهجمات ، ما حدث في عام ٢٠١٤، حينما تعرضــت شــركة ســوني SONY في الولايات المتحدة الامريكية لقرصـــنة الكترونية مع توقف مفاجئ لعمل الحاســـبات وظهور صـــور هيكل عظمي أحمر على شـــاشـــات هذه الحواســـيب مكتوب تحته تم الاختراق بواســطة HGOP ، في ذات العام تم تســريب خمســة أفلام حديثة الانتاج تعود لنفس الشــركة بالتحميل المجاني غير القانوني، واستمرت تلك الهجمات والإختراقات على شركة سوني ، حيث سرقت البيانات التي تحتوي على معلومات شخصية ذات صلة بموظفي الشركة، وأخرى تخص رواتب الموظفين، وتعطيل اجهزة الحاسوب الخاصــة بموظفي الشركة، والسيطرة على حسابات تويتر Twitter التابعة لشركة سوني[٢].

ثانياً: وسائل الهجمات المعلوماتية

تســـتخدم الاســـلحة المعلوماتية ، لغرض احداث اضـــرار مادية او وظيفية في النظم المعلوماتية ، ويختلف الضـرر الناجم عنها بحسـب درجة خطورتها ودرجة تعقيدها ، البعض منها يحدث ضـــرر جانبي دون اختراق النظام المعلوماتي ، وقســـم منها يســـتهدف إختراق الأنظمة وتدميرها كلياً او جزئياً ونظراً لخطورة استخدام هذه الهجمات لذا سنوضـح أبرز وسـائل الهجمات المعلوماتية فضــلاً عن الأجيال الجديدة من الحروب التي تعتمد بالدرجة الأســاس على الوســائل

---

[١] خالد وليد محمود، الهجمات عبر الانترنيت، ساحة الصراع الالكتروني الجديدة، المركز العربي للابحاث ودراسة السياسات، ٢٠١٣، ص٧-٨.

[2] Zitter , Kim, sony Got Hucked Hard, 214 Avail able on websit: http://www.wried .Accessedon ; 3/ 12/ 2021.

الحركية وهي بهذا المعنى تختلف عن الوسائل التقليدية والتي شاع إستخدامها على المستوى الدولي وعلى النحو الاتي:

١- فيروسات الحاسب الالي:

وهي برامج خارجية صنعت بصورة عمدية الغرض منها احداث تغيير في خصائص الملفات التي تصيبها لتقوم بتنفيذ بعض الايعازات أما بالإزالة أو التعديل أو التخريب وغيرها من العمليات الاخرى ، هدفها الرئيسي هو الحاق الضرر بحاسوب اخر والإستيلاء على محتوياته، وتتم كتابتها بطريقة خاصة ، اذ يقوم البرنامج المصاب فيما بعد بتنفيذ اوامر الفيروس وقد تستخدم هذه الفيروسات لتعطيل شبكات الخدمة والبنية التحتية لطرف الخصم الذي تم مهاجمته بهذه الفيروسات[١]. إلا إن هذا الفيروس وان كان عبارة عن برنامج قادر على تجديد نفسه، الا انه غير قائم بذاته، اي يستلزم الحاقه ببرنامج أو ملف أخر، وبعد ان ينتقل هذا البرنامج او الملف المصاب بالفايروس، والذي يسمى المضيف المصاب" infected host"، الى حاسب أخر ينتقل معه ايضاً الفايروس ، مما يمنحه خاصية احداث الضرر بالجهاز المستهدف ومسح ملفاته أو إغلاقه أو يقوم بتكرار نفسه ليتمكن من اصابه برامج أو ملفات اخرى[٢]. وهذا يعني ان هذا النوع من الفايروسات تكمن خطورتها عند تمكنها من الاتصال بحاسب الي اخر يتم استهدافه بواسطه الفايروس المصاب أو المضيف المصاب ، حيث يتم تفعليه عند فتح الملف المصاب، و بإمكان الخصم الذي تمت مهاجمته تحجيم خطورة هذا الفايروس بأنشاء انظمة مضادة لهجمات الشفرات الضارة ، والتي تؤدي الى اختراق انظمة الحاسب الالي وتدميره جزئياً او كلياً وتسبب توقفه عن العمل.

٢- الديدان

برامج معلوماتية، بإمكانها أن تستغل اي فجوات في نظم التشغيل كي تنتقل من حاسب إلى آخر، مغطية تشكيلة بأكملها، وتتكاثر أثناء عملية انتقالها كالبكتريا بإنتاج نسخ منها، لتحدث آثار تخريبيه للملفات، والبرامج، ونظم التشغيل، وبروتوكولات الاتصال[٣]. وهذه الديدان هي صغيرة قائمة بذاتها ولا تعتمد على غيرها ، تتميز بسرعة انتشارها وعدم القدرة على التخلص منها لقدرتها على الخداع والتلون والتناسخ، وغالبا ما يتم استخدامها في حروب المعلومات، فإنها

---

[١] د.ايهاب خليفة ،القوة الالكترونية ، مصدر سابق ، ص٨٣ .

[٢] صفات أمين سلامة ، أسلحة حروب المستقبل بين الخيال والواقع، دراسات استراتيجية ، مركز الامارات للدراسات والبحوث الاستراتيجية، ع (١١٢)، ابوظبي، ٢٠٠٥، ص٤٣.

[٣] محمد سامي الشوا، مصدر سابق،ص١٩٢

تستهدف الشبكات المالية التي تعتمد على الحاسوب مثل شبكات البنوك[١]، ومن أهمها دودة ستاكسنت ، وهي احد أخطر أنواع الأسلحة المعلوماتية التي تم انتاجها، ,ويعد ذلك تطور في نطاق الحرب المعلوماتية ، يتم من خلالها تدمير المكونات المادية نفسها ونظم التشغيل، بعد أن كان الهدف مقصور على تدمير البيانات ، ويعد هجوم ستاكسنت، من أبرز الهجمات التي نفذتها الولايات المتحدة الأمريكية وإسرائيل ضد ايران في عام ٢٠١٠، وهي جزء من سلسلة هجمات عرفت باسم " الألعاب الأولمبية ، كان غرضها تخريب برنامج إيران النووي ، حيث تم إنزال فيروس على نظم تشغيل أجهزة الطرد المركزي ، الذي يدير عملية تخصيب اليورانيوم، في منشأة نطنز النووية التي تعمل عبر نظام التحكم (SCADA)[٢]، وهو من صنع شركة سيمنز الألمانية والذي تم من خلاله ادارة المصانع والشبكات ومحطات الطاقة الكهربائية ، ونظم المياه والسدود وانابيب النفط والغاز والمفاعلات النووية ويتسم بقدرته على احداث اضرار مادية خطيرة[٣] ، وبالتالي تسبب الهجوم بأتلاف عدد كبير من وحدات الطرد المركزي، إذ كان هذا الهجوم متطورا، ويتسم بقدرته على اتخاذ قرارات مستقلة في البيئة المستهدفة دون التوصل مع الطرف المنفذ للهجوم. لقد تم تصميم (stuxnet) بصورة ذكية لمهاجمة أنظمة التحكم الصناعية التي يستخدم بنطاق واسع في المنشآت النووية، إذ تقوم بالانتقال بين الأجهزة عبر أجهزة (USB)، باستغلال احد نقاط الضعف في احد برنامج تشغيل الوندوز، حيث عمل مصممو هذا البرنامج الضار ستاكسنت ، على مرحلتين، الأولى السيطرة على نظام التحكم الموجود في أجهزة القيادة والسيطرة في المنشأة، للنفاذ إلى نظام(SCADA)، عبر استخدام الحواسب المربوطة بهذه الأنظمة، للبحث عن شفرات بداخلها، والمرحلة الثانية هي التخريب والتلاعب في أجهزة الطرد المركزي من خلال زيارة أو تقليل سرعة هذه الأجهزة كذلك الاستيلاء على شلالات الطرد المركزي وتدميرها لإلحاق اضرار فيها دون تدميرها كلياً. وفي ذات الوقت استطاع هذا الفيروس أن يحمي نفسه من خلال بث رسائل أمنه ومضلله لأنظمة التأمين المعلوماتية خاصة بالمفاعل النووي[٤].

---

[١] د.ايهاب خليفة، الحرب السبيرانية، الاستعداد لقيادة المعارك العسكرية في الميدان الخامس، ط١، دار العربي للنشر والتوزيع، القاهرة، ٢٠٢١،ص١١٠ .

[٢] (SCADA) هو نظام التحكم المركزي الذي يختص بالاشراف على انظمة التحكم وبجميع البيانات، هذا النظام يمثل حزمة برامجية محصنة يتم تصميمها فوق الاجهزة.

[3] Leaders, The meaning of stuxent, The economist, 2010, p.4.

[4] David Albright and Andreastricker, stuxnet worm targets Automated system for freguency conveters: Are larnian centrifuges thetargt? Institute for Science and inter national security, November 17, 2010, p.18 .

مما تقدم يتضح أن الهجوم على منشأة نطنز النووية الإيرانية شكل علامة فارقة في ظهور جيل جديد من الأسلحة المعلوماتية ، التي تكون قادرة على تحقيق أهدافها من خلال الولوج إلى نظم التحكم والسيطرة المسؤولة عن تشغيل أجهزة الطرد المركزي ، إذ عمل فيروس ستاكسنت على أحداث أضرار في العديد من هذه الأجهزة وخروجها عن الخدمة بوقت قياسي، دون أن تكتشف إيران سبب عطل هذه الأجهزة الخاصة بتشغيل المفاعلات النووية ، في ظل تداعيات الهجوم المعلوماتي الذي تعرضت له المنشأة النووية الإيرانية (نطنز) أظهرت تقارير الخبراء المختصون في تكنلوجيا المعلومات ، أن هذا الهجوم قد نفذته كل من الولايات المتحدة وإسرائيل بعد فشل الجهود الدبلوماسية والعقوبات الاقتصادية على إيران، وكان الغرض منه تدمير المفاعل النووية الإيراني، وبسبب عدم اعتراف الولايات المتحدة وإسرائيل بصلتهما بهذا الهجوم ، لم تتمكن إيران من إثبات مسؤولية كلتا الدولتين عن الهجوم[١].

٣- القنابل المعلوماتية أو المنطقية

هذا النوع من البرامج قد يتشابه مع احد أنواع احصنة طروادة وهو برنامج أو جزء من برنامج ، فقد تم تصميمها بحيث تعمل عند حصول حدث معين ، أو تحت ظروف معينة ، أو لدى تنفيذ أمر معين ، فهو ينفذ في فترة زمنية منتظمة ، ويوضع على شبكة معلوماتية ، تؤدي بالتالي إلى تدمير البيانات ، أو تعطيل النظام[٢]، والقنابل المعلوماتية المنطقية تختلف عن القنبلة الزمنية التي تثير حدثاً في لحظة زمنية محددة بالساعة واليوم والسنة والتي يتم إدخالها في برنامج بعد أن يتم توقيتها في ثوان أو دقائق محددة ، لتكون جاهزة للانفجار وتحقق الغرض الذي تم برمجتها من أجله ، ولعل خير مثال على ذلك هو ما حدث في جامعة (مونماوث) في الولايات المتحدة الأمريكية ، حيث نجد صورة واضحة عن الأثر المدمر للقنابل المعلوماتية ، من خلال إنفجار قنبلة استهدفت نظام البريد الإلكتروني للجامعة ، الذي يحتوي على مجموعة من الأنشطة في غاية الأهمية لتأدية وظائف الجامعة، كالتسجيل وتبادل الأبحاث ، ودفع الرسوم ، مما أدى الانفجار إلى انهيار نظام البريد الإلكتروني ، والحق بالنظام خسائر فادحة بالأموال ،

---

[١] زياد عبدالرحمن الكوراني، رؤية جيوستراتيجية لمستقبل الصراعات الاقليمية في منطقة تزاحم الاستراتيجيات، ط١، دار امجد للنشر والتوزيع، الاردن، ٢٠١٨، ص١٥٥.

[2] Christophe casa legno , codes malvaeillants ; worms lviruset bombes logigues, p.33, Avili able on site ; http ; // www. Christophe casalegno .com / does / codes-mal vei //ants . pdf.

وكردة فعل للهجوم سارع فريق التحقيق الفدرالي المختص إلى تحديد اليوم والساعة وعنوان الكمبيوتر المستخدم في العملية[١].

٤- أحصنة طروادة

هي شفرة أو برنامج صغير يتخفى في برنامج أكبر من البرامج ذات الشعبية العالية، ويقوم ببعض المهام الخفية كأن يعمل على نشر دودة أو فيروس، وهو مبرمج بمهارة عالية، إذ لا يمكن اكتشاف وجوده حيث غالباً ما يعمل على أثاره التي لا تحمل صفة تخريبية، ودائماً ما يعمل على اضعاف قوى الدفاع لدى الضحية ليسهل اختراق جهازه وسرقة بياناته، كأن يقوم بإرسال بيانات عن الثغرات المتواجدة في نظام معين، فضلاً عن إرسال كلمات المرور السرية الخاصة بالمعلومات الحساسة المخزنة لدى الطرف المستهدف.[٢] ويتم تحميل أحصنة طروادة على الأجهزة الذكية مثل (. And smar watch, tablet, smart phone) سراً ومن ثم تلحق الضرر بصاحب الجهاز ، ومن أشهر انواع احصنة طروادة سارق كلمة السر، أو احصنة طروادة الجاسوسية، أو التي تعمل على تحويل الحاسوب إلى آلة لنشر الرسائل المزعجة.[٣]

---

[١] فاطمة نعناع ، ((قنبلة الكترونية في بريد الجامعة)) مقال منشور في مجلة انترنت العالم العربي ، س(١) ، ع (٧) ، ١٩٩٨ ، ص٦٤-٦٥ .

[٢] ايهاب خليفة، مجتمع ما بعد المعلومات، تأثير الثورة الصناعية الرابعة على الأمن القومي ، مصدر سابق، ص١٣٣.

[٣] حارث عاصم الخطاب، الحرب الخفية، العلاقات الدولية وتأثيرها في الهجمات الالكترونية، ط١، دار الاداب للطباعة والنشر والتوزيع، بغداد، ٢٠١٩، ص٧١.

المطلب الثاني

خصائص الهجمات المعلوماتية وتميزها عن غيرها من المتشابهات

تختلف الهجمات المعلوماتية بخصـــائصـــها عن الهجمات التقليدية العســكرية من حيث أحداث اثار تدميرية في البنى التحتية للخصـــم، فهي غالباً لا تحتاج إلى تكاليف عالية في انتاجها، ومن الممكن ان تحدث أضــراراً مادية أو بشــرية عند شــنها على الطرف الخصــم من الدول، فضــلاً عن صــعوبة الكشــف عن فاعليها سواء من الدول أو الكيانات الأخرى أو الأفراد، ومصــطلح الهجمات المعلوماتية هو مفهوم قد يتشــابه في بعض الاحيان مع بعض المفاهيم مما يتوجب وضــع الحدود الفاصــلة بينه وبين بعض المصــطلحات المشــابهة له، والسؤال الذي يتبادر إلى الذهن ما هي أهم خصــائص الهجمات المعلوماتية التي تتميز بها وتكون قادرة على تحقيق أهدافها؟ وإذا كانت الهجمات المعلوماتية تتشـــابهه مع بعض المفاهيم المقاربة لها إلا إنها تتميز عن غيرها من المتشابهات فما هي أوجه التشابه والاختلاف بينها وبين هذه المفاهيم؟

لذا سنقوم بتقسيم هذا المطلب على فرعين نخصص الفرع الاول لبيان خصائص الهجمات المعلوماتية، أما الفرع الثاني نوضــح فيه تميز الهجمات المعلوماتية عن غيرها من المتشــابهات وعلى وفق الآتي:

الفرع الأول

خصائص الهجمات المعلوماتية

تمتاز الهجمات المعلوماتية بعدد من الخصـــائص التي تميزها عن هجمات الاســـلحة التقليدية التي تحتاج الى تكاليف مرتفعة في عملية إنتاجها وتتسـبب بخسـائر بشـريه فادحة أثناء اســتخدامها في النزاعات المســلحة، فالهجمات المعلوماتية على العكس من الهجمات التقليدية ، تتميز بانخفاض تكلفة المواجهة من خلالها نسـبياً، وتكاد تكون الخسـائر نتيجة اسـتخدامها قليلة جداً او منعدمة وصـــعوبة الكشـــف عن فاعليها ، فضـــلاً عن غياب الحدود المكانية والزمانية

وسرعة تطورها ، اذا ان هذه الخصائص التي تتسم بها تلك الاسلحة المعلوماتية جعلت من الدول تسعى لامتلاكها وتطويرها، لذا ستناول اهم تلك الخصائص وعلى النحو الآتي:

اولا – صعوبة تحديد هوية المهاجم :

يتم تطوير الاسلحة المعلوماتية دون ان يتم اكتشافها أو تحديد مرتكبيها أو المصدر الذي شن منه الهجوم فهي لا تترك أثراً او دليلاً على حصولها، اذ ان معظم الهجمات المعلوماتية يتم اكتشافها بالصدفة، وبالاستعانة بخبرة فنية عالية المستوى لتحديد مصدر الهجوم، و اذا ما تم اكتشاف مصدر الهجوم المعلوماتي، وتبين انها تعود لفاعلين غير حكوميين، فأنه في هذه الحالة لن يكون لديهم اصول او قواعد حتى يتم الرد عليها[١] وغالباً ما يقوم اصحاب الاختصاص في تحديد الهجمات المعلوماتية على دولة معينة بالاعتماد على ثلاث خطوات رئيسية[٢]:

١- تحديد موقع شن الهجوم المعلوماتي ، اي عنوان بروتوكول الانترنت ، والمكان المخصص لصناعة البرنامج ، اذ قد يعمد المهاجم الى تغيير عنوان بروتوكول الانترنت ويجعله يشير الى مواقع مختلفة.

٢- دراسة حالة تقييم البرنامج الضار والمواد المتكون منها، لكن في ذلك صعوبة تحديد توقيت تصميم البرنامج وللغة المستخدمة على الحاسب الآلي الذي صمم عليه، فمن السهولة تزييف هذه المعلومات باقل التكاليف.

٣- معرفة الهدف الرئيسي الذي تم تصميم البرنامج وشن الهجوم من اجله، وهذا الامر ايضا يصعب تحقيقه، لأن الكثير من الهجمات المعلوماتية التي يتم تنفيذها هو للتمويه على اهداف غير معلنه.

ان اهم ما يتميز به الفضاء المعلوماتي هو صعوبة تحديد مصدر الهجوم في اغلب الهجمات المعلوماتية، فكلما ازدادت درجه تعقيد الهجوم المعلوماتي ازدادت معه صعوبة الكشف

---

[١] د.اشرف السعيد احمد، القرصنة الالكترونية، دار النهضة العربية، القاهرة، ٢٠١٣، ص٤٦-٤٧.

[2] Paulo shakarian and others introduction to cyber war fare, A Multidisciplinary Approach, Elsevier, USA , 2013, p,27.

عن هوية الفاعلين أو تتبع مســـار الهجوم ،أو تحديد ذلك الهجوم او توقيته، لذا نجد أن أغلب الدول التي وجهت لها اتهامات بشــن هجمات معلوماتية ضـــارة، كروســيا الاتحادية في حالتي (إستونيا وجورجيا) قد نفت تماماً صلتها بتلك الهجمات، ومما يزيد الامر تعقيداً هو عجز الدولة التي تعرضت للهجوم من اسناد الاتهام للدولة المهاجمة وبالتالي يصعب اثبات مسؤوليتها الدولية عن الهجوم المعلوماتي[١].

ومن الجدير بالذكر ان خاصية صعوبة الكشف عن هوية المهاجم وتحديد موقع انطلاق شن الهجمات المعلوماتية تؤدي الى فشل أو ضعف قدرة الدولة التي تعرضت للهجوم على ردع تلك الهجمات مقارنة بالهجمات التقليدية عند تحديد مصـــدرها والرد عليها بالانتقام أو العقاب، ومن ثم يمكن تطبيق اســـتراتيجية ردع الهجمات التقليدية المصـــاحبة للنزاعات المســـلحة على الهجمات المعلوماتية ، كذلك فان عدم تحديد هوية المهاجم والموقع الذي تم شـــن الهجمات المعلوماتية من خلاله يؤدي الى عدم قدرة الدولة على إثبات الدليل وبالتالي اســـناد الهجوم المعلوماتي للدولة التي انطلقت من اراضـــيها تلك الهجمات ويزداد الأمر أكثر تعقيداً اذا ما قام بتلك الهجمات فاعلين من غير الدول.[٢]

ثانياً- زوال الحدود المكانية والزمانية : أن الهجمات المعلوماتية بصـــورة عامة ، لها القدرة على منح الفاعلين الدوليين ميزة اســـتراتيجية في تخطي عقبة القيود المكانية والزمانية ، فبالنســبة للقيود المكانية، فهي على النقيض من الهجمات العســكرية التقليدية التي تتحدد بنطاق مكاني معين ، تتسم الهجمات المعلوماتية بشمولية نطاقها المكاني ، واتساع مداها، اذ يمكن شن الهجمات الالكترونية من أي مكان من أي موقع في العالم ، كما ان الهجوم المعلوماتي وان كان يستغرق وقتا في تخطيطه الى ان تنفيذه يتم بصورة سريعة ، بغض النظر عن مدى بعد الهدف

---

(1) David Awheelr and Gregoryn,larsan Technigues for cyber Attack Attribuion in statute for Defence Avail able on the websit:
http//www.scis.nova.edu/cannady/ARES/wheelerpdfAccesed.on:january22.2014,p.4

(٢) ريتشارد كلارك، وروبرت نيك ، حرب الفضاء الالكتروني الخطر القادم على الأمن القومي وسبل مواجهته، ط١، مركز الامارات لدراسة السياسات، ٢٠١٢، ص٢٨٩.

أو قربة، بينما الهجمات التقليدية تكون سـرعة الهجوم مرتبطة بالموقع المكاني للهدف والمسـافة بينه وبين المهاجم. [١]

علاوة على ذلك ان الهجمات المعلوماتية لها ميزة مفاجأة الخصـم اثناء الهجوم ، مقارنة بالأسلحة التقليدية ، اذ تتحرك عبر شبكة المعلومات والاتصالات العابرة للحدود الدولية ، والتي يتم توجيها ضد المنشآت الحيوية ، او دسها عن طريق العملاء لأجهزة الاستخبارات ، والتي تتميز بهجمات الكر والفر، والحد من قدرة الخصم من الرد عليها، وبالشكل الذي يجعل عملية استخدام هجمات الكومبيوتر في اي نزاع ذو طابع سياسي اقرب لوصفها بالإرهاب عن كونها حرباً[٢]، على سبيل المثال ، اعتماد اسرائيل على الاسلحة المعلوماتية لمهاجمة أهداف حيوية تابعة للدولة السورية ليس الهدف منها احداث تدمير موقع حيوي معين، وانما لتحقيق عنصر المفاجأة ، و أضعاف قدرة الخصم على الرد ، فبدلاً من مهاجمة الرادار من خلال الاسلحة التقليدية وهو الهجوم الذي لن يتحقق فيه عنصر مفاجأة الخصم ، تم الاعتماد اولا على هجمة معلوماتية لتحقيق عنصر المفاجأة ومن ثم تزيد من فاعلية الهجوم التقليدي[٣]. وبالتالي لن تتمكن سوريا من اغتنام الفرصة وردع الهجمة الصاروخية. [٤]

ان حادثة ((بيرل هاربر)) المعلوماتية التي تم من خلالها مهاجمة القوات البحرية والجوية الامريكية من قبل الاسطول البحري الياباني في هاواي عام ١٩٤١ ، على الرغم من أنها لم تحدث أضراراً تدميرية واسعة ، لكن صاحبها عنصر المفاجأة ، الامر الذي جعل الولايات المتحدة تدخل حرباً وتنتصر فيها على القوات اليابانية ، وهنا يدل ان عامل الصدفة هو الهدف من هذه الهجمات وليس احداث تدمير واسع النطاق، لذلك زادت مخاوف المحللين الأمنيين من

---

[١] نوران شفيق، اثر التهديدات الالكترونية على العلاقات الدولية ، دراسة في أبعاد الأمن الالكتروني ، المكتب العربي للمعارف، ط١، ٢٠١٦، ص١٦٩.

[٢] د.عادل عبد الصادق. الارهاب الالكتروني القوة في العلاقات لدولية نمط جديد وتحديات مختلفة، مركز الاهرام للدراسات السياسية والاستراتيجية ٢٠٠٩، القاهرة، ص٢٢٥ – ٢٢٨.

[3] Jame Alewis, thresholds for cyber war , center for strategic and international. studies , , 2010, p4-6 .

[٤] د.اشرف السيد سعيد، القرصنة الالكترونية، مصدر سابق، ص٩٩.

ان الهجمات المعلوماتية قد تحدث اثاراً بالغة على المنشآت الحيوية والانظمة المعلوماتية للولايات المتحدة ، لا يكون باستطاعة الولايات المتحدة التنبؤ بحدوثها ، أو اتخاذ التدابير اللازمة للوقاية منها أو منع حدوثها[١].

نلاحظ مما تقدم أن إنعدام الحدود المكانية والزمانية ، هو أحد المميزات التي يتسم بها الفضاء المعلوماتي، مقارنة بالهجمات العسكرية التقليدية ، عندما تجد الدول صعوبة في تحديد موقع شن الهجمات المعلوماتية فالمخاطر المعلوماتية هي عالمية بطبيعتها ،عابرة للحدود، فقد تأتي الهجمات المعلوماتية من مواقع ليست بحسابات استراتيجية الدول التي تم مهاجمتها من هذه المواقع، لذلك تستبعدها الدول الاقليمية كأساس لتطوير استراتيجيتها الخاصة بالأمن المعلوماتي، لأنها غير محددة الأهداف والنتائج، إذ قد تتعدى مخاطرها ميادين القتال التقليدية لتصل بدمارها إلى مواقع سيادية محصنة.

ثالثاً- التكلفة المادية: بحساب التكلفة المادية المتدنية نسبياً للأدوات اللازمة لشنها ، فلا تحتاج الدول الى تخصيص ميزانيات ضخمة لإنتاج اسلحتها المعلوماتية اسوة بالأسلحة المستخدمة في النزاعات التقليدية ، التي غالبا ما تكون عالية الكلفة كحاملات الطائرات والمقاتلات المتطورة ، لتشكل تهديداً خطيراً وجدياً على الدول الكبرى مثل روسيا الاتحادية والولايات المتحدة الامريكية[٢] ،وأن رخص تكاليف إنتاج الأسلحة المعلوماتية يشجع الدول على تشكيل تحالفات في الفضاء المعلوماتي ذات قدرات هجومية متطورة بأقل التكاليف ، كذلك باستطاعة منظمات أو جماعات أن تتسلح وتشن هجمات عبر الفضاء المعلوماتي[٣]، إذ تضم التحالفات في الحروب المعلوماتية اطرافاً متعددة مثل الدول والكيانات العابرة للحدود الوطنية،

---

(1) Andrewf . krepinevich , cyber war fare, center for strategic and Budgetary Assessments, 2012. P.14 .

[٢] د.شادي عبدالوهاب، حروب الجيل الخامس، ط١، دار العربي النشر والتوزيع، القاهرة، ٢٠١٩، ص٧٨.

[٣] د.عادل عبدالصادق، اسلحة الفضاء الالكتروني في ضوء القانون الدولي الإنساني، مكتبة الاسكندرية، الاسكندرية، ٢٠١٦، ص٦٣.

والشـــبكات، والجماعات والافراد ، مثل الذئاب المنفردة[١]، التي غالبا ما يقوم بها افراد بتنفيذ عمليات ارهابية دون الحاجة الى تشكيل تنظيم إرهابي.

كذلك قيام الولايات المتحدة الامريكية بالتعاون مع اسـرى الحرب في افغانسـتان للقضـاء على قائد تنظيم القاعدة لأسامة بن لادن، إذ سمحت لهم مقابل ذلك الاتجار بالمخدرات[٢].

ونسـتطيع القول إن اللجوء إلى اسـتخدام الهجمات المعلوماتية ، يتيح للدول التغلب على محدودية الموارد وتعظيم قدراتها العسـكرية ، إذ إن الدول تلجأ الى اسـتخدام الفضـاء المعلوماتي لشن هجمات على خصومها بعيداً عن الخوض في صراعات تقليدية تكون التكلفة المادية لتصنيع اسلحتها باهظة الثمن بالمقارنة مع التكلفة المادية للأسلحة المعلوماتية ، وبالتالي يصـعب هزيمة الخصـم الذي يسـتخدم تقنية معلوماتية متطورة من خلال إسـتخدام الهجوم المضـاد بواسـطة القوة العسكرية التقليدية وحدها.

رابعاً: قوة تدميرية لا تصاحبها خسائر بشرية فادحة:

تتميز الحرب بالأسـلحة المعلوماتية ضـد الخصـوم بانها تدمير للبنية التحتية للخصـم دون ضرورة حدوث خسائر بشرية، اذ يتضمن التجسس والتسلل ثم النسف لكن من دون ، دخان ، أو غبار، أو انقاض ، ويتميز اطرافه بعدم الوضوح وتكون تداعياته خطيرة ، سواء عن طريق تدمير المواقع على الانترنت وقصـفها بوابل من الفيروسـات ، أو العمل على اسـتخدام أسـلحة الفضـاء المعلوماتي المتطورة والمتعددة لاستهداف تلك المواقع ، فهي أسلحة من السهولة الإستحواذ عليها من خلال مواقع الانترنت ايضـاً، فضـلاً عن سـهولة الولوج الى الفضـاء المعلوماتي والذي يعتبر

---

(1) Donald j.Reeds, Beyond war on Terror: in to the fifth Generation of war and conflict, studies in Terrosim, vol.31, Issue8, 2008,p.698.

(2) Mathilde simon , the Drug trade in Afghnistan: under standing Motives behind farmer's Decision to cultivate opiu peppies, foreign policy journal, November 27, 2015, p.3.

عامل مساعد في توسيع دائرة المواقع وزيادة عدد المهاجمين[١]. كما يمكن للأسلحة المعلوماتية إن تنفذ أهداف الهجوم دون الحاق ضرر مادي بالبنية التحتية او بالبشر وهذه الميزة لا يمكن إن تتوفر في الأسلحة التقليدية، كذلك يمكن للهجمات المعلوماتية ايضا أحداث أضرار بالغة بالأرواح البشرية، بواسطة استهداف الانظمة الموجودة في المجالات المادية والتي تتصل بالفضاء المعلوماتي[٢]. هذا يدل على ان هناك ثمة امكانية أن تسبب الهجمات المعلوماتية خسائر مالية فادحة للخصم ، وقد تفضي الى خسائر في الارواح ، اذا ما تجاوزت اهداف هذه الهجمات منشآت حساسة جداً ، مثل انظمة المستشفيات وانظمة اجهزة التبريد التي تساعد في عمل المفاعلات النووية. و يمكننا القول بان انحسار الخسائر البشرية من جراء الهجمات المعلوماتية سواء من قبل المهاجم أم الطرف الذي تم مهاجمته يمنحها ميزة نسبية مقارنة بالأسلحة التقليدية ، فالهجمات المعلوماتية تحدث اضرارها على الهدف دون ان يتضرر المهاجم أو يتكبد خسائر في المعدات او الارواح.

الفرع الثاني

تمييز الهجمات المعلوماتية عن غيرها من المتشابهات

شهد العصر الحديث ظهور العديد من المفاهيم والمصطلحات ، التي كانت نتيجة حتمية للتطور في عالم تكنلوجيا المعلومات، إذ يتم في بعض الاحيان إستخدام مفهوم الهجمات المعلوماتية بدلالة مفاهيم أخرى مشابهة بسبب التداخل الذي قد يحصل بينها من حيث الطبيعة والوظيفة مع هذهِ المفاهيم ولغرض وضع الحدود الفاصلة بين تلك المفاهيم ومفهوم الهجمات المعلوماتية وتجنب الخلط الحاصل بينهما، جرى تقسيم هذا الفرع على المحاور الآتية :

---

[١] نورة شلوش ، القرصنة الالكترونية في الفضاء السيبراني : التهديد المتصاعد لأمن الدول ، مجلة مركز بابل للدراسات الانسانية ، م ٨ ، ع ٢ ، ٢٠١٨ ، ص١٩٥ .

[٢] د.عادل عبدالصادق، اسلحة الفضاء الالكتروني في ضوء القانون الدولي الانساني، مصدر سابق ، ص٦١.

اولا : تمييز الهجمات المعلوماتية عن حرب المعلومات :

للوهلة الأولى لا يمكن- بحال من الأحوال- إيجاد الفارق النوعي، أوفض الاشتباك والتداخل، بين المفهومين، بسبب أن العديد من المختصين بالشأن القانوني قد وظفوا هذين المفهومين بصورة متبادلة، وبتثبيت المعيار المعرفي لمفهوم حرب المعلومات كنقطة انطلاق للتمييز بين المفهومين، وجدنا أن هناك من عرفها على أنها : "المواجهات الحاصلة بين الدول في مجالات المعلوماتية ، مثل إلحاق الضرر بالنظم المعلوماتية، وعمليات تبادل المعلومات، والموارد الحيوية للإجهزة العامة، وتخريب النظم السياسية ، والإقتصادية، والإجتماعية والسيطرة على الحالة النفسية العامة للسكان، وإلحاق الضرر باستقرار المجتمع والدولة"[١].

كما انها تتقسم على نوعين هما حرب معلومات هجومية : تقوم بها في أغلب الأحيان الدولة أو أحد أجهزتها الإستخباراتية لأغراض سياسية أو عسكرية او غيرها، إذ يستحوذ المهاجم على المعلوماتية ونظمها ويقوم بسرقة البرامج المعلوماتية أو يقوم بتخريب أو تعطيل نظم معلوماتية، أما الحرب الدفاعية :فتعمل على حدود الوقاية من الأعمال التخريبية التي قد تتعرض لها، إذ تختلف الوسائل الدفاعية باختلاف أدوات التخريب والأضرار التي قد تحدثها[٢] .

ومصطلح حرب المعلومات يستخدم في وسائل الإعلام على إختلاف أنواعها ومسمياتها، وغالبا ما يساء فهمه على أنه يعني استخدام الأسلحة عالية التقنية في الجيوش التقليدية، والاصح أن حرب المعلومات تختفي منها المدافع والصواريخ أو تتأخر للخلف وتتقدم الحواسيب للخطوط الأمامية للهجمات وفي كل مكان وفي اللامكان ولامجال للألتحام بالبشر[٣]. فالحرب المعلوماتية لها أهداف أشمل يتم تحقيقها بوسائل عديدة، فهي جزء من العمليات المعلوماتية ، إذ هي قائمة

---

[١] د.عادل عبدالجواد محمد ، دور مراكز المعلومات في التعامل مع الازمات، مجلة الأمن والحياة، الرياض، ع(٣٥)، ٢٠١٦، ص٧٠.

[٢] هشام سلمان، تكنلوجيا المعلومات والاتصال ، مجلة علوم التكنلوجيا، ع(٢)، من دون مكان نشر، ٢٠٠١ ص ٢٥.

[٣] الفن توفلر، تحول السلطة بين العنف والمعرفة، ترجمة فتحي بن شنوان ،الدار الجماهيرية للنشر والتوزيع والإعلام، ليبيا، ١٩٩٢،ص٩٧.

على إختراق المواقع في شبكة الانترنت ونشر الفيروسات وما شابهها من البرامج المؤذية لإرباك وإتلاف محتويات الحاسبات الآلية التي تختلف بدورها جوهريا عن الحرب التقليدية الصلبة ، فحرب المعلومات تعمل بالجذب والترغيب لا بالوعيد والترهيب وتخاطب العقول والقلوب ، من أجل اكتساب الآراء ، ومن أجل انتزاع الإرادة الجماهيرية ، لذلك أصبح توسيع نطاق الإعلام يحل محل نشر القوات والفضائيات في مقام ترسانة الأسلحة ومضادات الصواريخ ، وأصبحت معظم وسائل الإعلام هي الآت حرب ، وتختلف حرب المعلومات من حيث طريقة ممارستها عن نظيراتها في القدرة الهائلة وسواء كان زمنياً أم جغرافيا ً، ويمكن ممارستها بصورة دائمة ومستمرة ، على العكس من استخدام القوة في نطاق الحرب التقليدية فلا تتم الا في حالة الضرورة[١]. ومن أهم أنواع حرب المعلومات هي حرب المعلومات النفسية التي تشمل أفعال ترمي إلى طمس الحقائق وبث الأكاذيب والاشاعات في المجتمع والتأثير على الخصم من أجل القيام بأفعال لا يهدف الفاعل فيها إلى تحقيقها ضد خصمه[٢] وتكون حقيقة الأهداف سياسية ، عسكرية، اجتماعية ، وهي غير حرب وسائل المعلومات التي تعتمد على استغلال المعلومات والتلاعب بها ، مما يشكل مكونا مركزيا في مجال الحرب النفسية بالخدعة والدعاية ، وكشف معلومات يحرص الخصم على اخفائها[٣] ، إلا ان هاتين الحربين تختلفان عن حرب قراصنة المعلومات والتي تستخدم أنظمة المعلومات والشبكات الإلكترونية بطرق غير مشروعة للحصول على المعلومات المخزنة في الحواسيب والشبكات المرتبطة بها وتنفذ غالباً أهداف مالية أو إقتصادية[٤].

---

[١] محمد طوالبيه، ايدلوجية الفضاء الرقمي دراسة في الخلفيات المرجعية، مجلة أكاديمية الدراسات الاجتماعية والإنسانية، ع(٢١)، جامعة الشلف، ٢٠١٩،ص٤٧-٤٨.

[٢] سراب ثامر أحمد ، الهجمات على شبكات الحاسوب في القانون الدولي الإنساني، أطروحة دكتوراه، مقدمة إلى مجلس كلية الحقوق ، جامعة النهرين،٢٠١٥ ،ص٥٦.

[٣] سعيد عياش، الحرب في الحيز الافتراضي، مجلة قضايا إسرائيلية، ع (٤٣، ٤٤) ، المركز الفلسطيني للدراسات الإسرائيلية، فلسطين، ٢٠١٢ص٩٨.

[٤] سراب ثامر أحمد، المصدر السابق، ص٥٦.

فأذا كانت حرب المعلومات تشترك مع الهجمات المعلوماتية بالمعلومة التي يجري توظيفها لتحقيق النصر على الخصم، فأن أوجه الاختلاف بينهما تتجسد بالآتي:

١- من حيث الشـــمولية: فأن حرب المعلومات اكثر اتســـاعاً وشـــمولاً من الهجمات المعلوماتية ســواء في ادواتها التي تتعدى الأنظمة الحوســبية لتشــمل انظمة الإتصــال والاعلام أوالسيطرة وغيرها، أو في مساحاتها التي تشمل الفضاء المعلوماتي والكهرومغناطيسي ايضاً.

٢- من حيث الهدف: إن هدف حرب المعلومات يتعدى احياناً ابعاد التدمير المادي ليصل إلى التأثير في معنويات الخصــم وهو ما يتناقض مع هدف الهجمات المعلوماتية الذي ينحصــر في التدمير المادي للبنى التحتية المعلوماتية لتحقيق غاية النصــر اخضــاع الخصــم، إذ يقتصــر مضمارها على الشبكة المعلوماتية، وميدانها الحاسوب الآلي.[١]

وصـفوة القول، فإن حرب المعلومات وأن كانت تتشـابه مع الهجمات المعلوماتية من حيث اشـــتراكها بالمعلومة التي يجري توظيفها من قبل الطرف المهاجم والتي ينبغي من ورائها تحقيق تقدم لصـــالحه في مجال المعلوماتية ،إلا أن أوجه الاختلاف بين المفهومين يبرز لنا الكثير من الفوارق بينهما ، فالهجمات المعلوماتية باتت اكثر دقة وأوســع ، وتعدت مفهوم المعلومات لتطال البنى التحتية للدولة التي تمت مهاجمتها بصــورة غير مشــروعة مثل قطاع الصــحة، والكهرباء والمنشآت النووية ، والقطاعات الاقتصادية وغيرها، أما هدف حرب المعلومات بات أكثر شمولية فهي تتعدى أهداف تنفيذ الهجمات المعلوماتية المادية لتصـل إلى أبعاد تدميرية معنوية لإضـعاف الثقة بقدرات الخصم وبالتالي هزيمته .

ثانياً: تميز الهجمات المعلوماتية عن الارهاب المعلوماتي

انقسم الفقه في ايجاد تعريف موحد للإرهاب المعلوماتي وسار على اتجاهين الاتجاه الاول هو الاتجاه الموســع. الذي يصــف الارهاب المعلوماتي بانه: تلك الحالات التي تســتخدم فيها التكنلوجيا لتسـهيل انشـطة ارهابية. مثال على ذلك اسـتخدام هجمات (Dos) ضـد مواقع ويب

---

[١] د.سامر مؤيد عبداللطيف، الحرب في الفضاء الرقمي، رؤية مستقبلية، مجلة رسالة الحقوق، مركز الدراسات القانونية والدستورية ، س(٧) ، ع(٢)، ٢٠١٥، ص٧٩.

(website) أو الخوادم التابعة للحكومة وقد تستخدم حسابات البريد الالكتروني المجهولة والتشفير للتغطية على الإتصالات الارهابية. فضلاً عن استخدام المواقع لنشر دعاية او لتجنيد اعضاء ، كذلك يمكن استخدام الانترنت كطريقة لجمع المعلومات الاستخبارية بشأن الاسلحة او التدريب على الاسلحة. وفضلاً عن تطويع التكنلوجيا في تمويل الارهاب [١]، أما أصحاب الاتجاه الثاني المضيّق للمفهوم فهم يرون بأن الارهاب المعلوماتي هو الذي تستخدم فيه ادوات الشبكة والحاسوب للإضرار بالبنية التحتية الوطنية الحرجة مثل قطاع النقل، الطاقة، اذ يرى اصحاب هذا الإتجاه بان هذه الافعال تعبير عن الارهاب المعلوماتي بالمعنى القانوني الدقيق نتيجة للضرر الفعلي أو الذي يهدد الاشخاص او الخدمات الاساسية، وغالبا ما تكون اهدافه متعددة الأغراض، يقصد منها ارباك عمل الحكومات وترويع المدنيين ،وبهذا الصدد يحذر الخبراء من خطر قادم يكمن في تحول الإرهاب من الدعاية والتجنيد إلى شن هجمات معلوماتية على البنية التحتية والانظمة وسرقة معلومات حساسة، كالخطط والخرائط والإستراتيجيات العسكرية.[٢]

ان ما يهمنا في هذه الدراسة ليس فقط التعريف بمفهوم الارهاب المعلوماتي، وأن كانت له أهمية لا يمكن انكارها لما يشكل من خطر محدق على الاشخاص والممتلكات العامة أو البنية التحتية المعلوماتية للدول. إنما البحث عن اوجه الشبه والاختلاف بين المفهومين.

فأذا كانت أوجه الشبه بين المفهومين تتمثل في إن كل من الإرهاب المعلوماتي والهجمات المعلوماتية يستخدمان ذات الأسلوب المتمثل بأنظمة الشبكة المعلوماتية التي تعد الوسيط الذي ينفذ من خلاله تلك الهجمات فأن أوجه الأختلاف بين المفهومين تتمثل بالآتي:

---

[١] بعد احداث ١١ سبتمبر / ايلول ٢٠٠١ ، شهد العالم ظهور مصطلح الارهاب السيبراني حيث كان الانترنت عامل ساعد بالتحضير للاعتداء ، لكن قبل ذلك التاريخ وبالتحديد في ١٠ أيار ٢٠٠٠ كانت أول حادثة بهذا الصدد ، لها صدى اعلامي واسع ، هي هجمات رفض الخدمة ، التي تقوم بحجب الخدمة أو بطئها، لوحظ بعد التحري عنها انها كانت من صنع شاب يبلغ (١٥) من العمر يحمل اسم شهرة (مافيا بوي) ، ظهر بعد إلقاء القبض عليه بأن اعماله ذو طابع سياسي ، للمزيد ينظر : سولانغ غبير ناوني هيلي واليكساندر نتوكو ، دليل الأمن السيبراني للبلدان النامية ، الاتحاد الدولي للاتصالات ، جنيف ، ٢٠٠٦ ، ص٣٤ .

[٢] منى الاشقر جبور، المعلوماتية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، من دون سنة طبع، ص٨٩.

١- يختلف الإرهاب المعلوماتي عن الهجمات المعلوماتية من حيث تحديد الفاعلين وأهدافهم في الفضـــاء المعلوماتي، كثيراً ما نجد الإرهاب المعلوماتي يقوم به افراد، أو كيانات، أو جماعات دون مســـتوى الدول، أما الهجمات المعلوماتية قد يتم تنفيذها من قبل دول في حالات معينة، بيد إنها تختفي عن الانظار لتتخلص من افعالها غير المشروعة دولياً.

٢- من حيث مشروعية الأهداف: فعلى صعيد الاهداف فانه في جميع الاحوال والظروف يفتقد الارهاب المعلوماتي الى عنصر المشروعية بينما أهداف الهجمات المعلوماتية في مناسبات عدة قد تكون مشـــروعة دولياً إذا كانت في اطار الرد على هجمات معلوماتية غير مشـــروعة دولياً[١].

ثالثاً: تميز الهجمات المعلوماتية عن الجرائم المعلوماتية

أن الجرائم المعلوماتية قد تباينت تسمياتها بمراحل تطورها الزمني، فكانت البداية بمصطلح إساءة إستخدام الكومبيوتر، ثم تلاه مصطلح إحتيال الكومبيوتر، والجريمة المعلوماتية، والجريمة المرتبطة بالكومبيوتر وجريمة التقنية العالية، الى جرائم الهاكرز، فجرائم الانترنت، ثم جاء آخر المصـــطلحات وهو المعلوماتية[٢]، ولعل هناك تســـاؤلاً يثار بهذا الصـــدد وهو هل أن الجريمة المعلوماتية يمكن أن تتداخل بمفهومها مع الهجمات المعلوماتية؟ وهل هناك فروق جوهرية بين المفهومين؟ وما معيار التفرقة بينهما؟

للإجابة عن هذه التساؤلات، لابد قبل كل شيء التطرق لبيان مفهوم الجريمة المعلوماتية.

أختلف الفقه في إيجاد تعريف محدد للجريمة المعلوماتية، فمنهم من عرفها بأنها (نشـــاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الاجرامي المقصود)[٣]، وهناك رأي فقهي اخر ينظر للجريمة المعلوماتية بأنها (كل سلوك

---

[١] د.سامر مؤيد عبداللطيف، مصدر سابق، ص٨٠.

[٢] د. عبد العزيز بن غرم الله جار الله ، جرائم الانترنت وعقوباتها وفق نظام ومكافحة الجرائم المعلوماتية السعودي ، دراسة مقارنة ، ط١، دار الكتاب الجامعي ، الرياض ، ٢٠١٧ ، ص٧٩ .

[٣] محمد أحمد القرعان ، الجرائم الالكترونية ، ط١ ، دار وائل للنشر والتوزيع ، عمان ، ٢٠١٧ ، ص١٩ .

إجرامي يقوم به الجاني إضراراً بمكونات الحاسوب الآلي وشبكات الإتصال الخاصة به، الذي يحميها قانون العقوبات ويفرض له عقاباً)[١]، ويرى أنصار هذا التعريف بان الجريمة المعلوماتية هي من الجرائم العابرة للحدود والتي يتم تنفيذها في اكثر من دولة، وقد ذهب مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في فيينا عام ٢٠٠٠ الى تعريف الجريمة المعلوماتية بأنها (أي جريمة يمكن ارتكابها على نظام حاسوبي أو شبكة حاسوبية، وتشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية)[٢].

ومن نافلة القول ان التعريف المتقدم قد حاول الإحاطة بجميع اشكال الجريمة المعلوماتية، سواء الجرائم الواقعة على الانظمة المعلوماتية ، أو تلك التي يتم فيها اختراق النظام والاستيلاء على البرامج والمعلومات المخزنة بداخلة، فهذا التعريف قد وسع نطاق الجريمة المعلوماتية، ولم يحصرها في مجال محدد، حتى لا يخرج بعض من الأفعال المعلوماتية. الإفلات من دائرة العقاب، ونعتقد من وجهة نظرنا المتواضعة إن هذا التعريف جاء شاملاً لجميع انواع الجريمة المعلوماتية.

إن الجرائم المعلوماتية وإن كانت تتحد مع الهجمات المعلوماتية في البيئة التي تحدث فيها هذه الانشطة ، أي الفضاء المعلوماتي ، إلا إنها تختلف عنها من حيث الأشخاص أوالباعث أو الهدف:

١- **من حيث الأشخاص** : الهجوم المعلوماتي تقوم به دولة أو منظمات أرهابية من أجل مقتضيات الأمن القومي، أما الجريمة المعلوماتية يمكن أن يقوم بها أشخاص أو مجاميع قرصنة تقوم بتنفيذها بعيداً عن سياسة الدولة.[٣] إذ أن الجريمة المعلوماتية هي مخالفة ترتكب ضد الأشخاص أو الكيانات بدافع إجرامي كالدخول غير المصرح به وإتلاف البيانات المخزونة في

---

[١] د.محمد علي العرين، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الاسكندرية، ٢٠١١، ص٥٦. .

[٢]. محمد أمين أحمد الشوابكة، جرائم الحاسوب والانترنيت- الجريمة المعلوماتية، دار الثقافة، عمان، الاردن، ٢٠٠٤، ص١٠.

[٣] د.كامل سعيد، جرائم الكمبيوتر والجرائم الاخرى في مجال التكنلوجيا، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، ١٩٩٣، ص٥١٦.

الانظمة، أو الاعتراض غير القانوني لها، أو تعد سلوك غير مشروع يعاقب عليه قانوناً صادراً عن ارادة جرمية محلة معطيات الحاسوب.[١]

٢- **من حيث الباعث أو الهدف:** غالباً ما يكون الباعث على الهجمة المعلوماتية يتمثل أساساً في محاولة إضعاف شبكات الحاسوب المستهدفة في دولة اخرى لتحقيق أهداف سياسية أو أمنية أو عسكرية، علاوة على ذلك ان القواعد القانونية ذات الصلة في الهجمات المعلوماتية هي قواعد القانون الدولي العام، وبالتحديد هي قواعد اللجوء الى استخدام القوة[٢]، أما الجريمة المعلوماتية فهي تصرف، للسعي وراء هدف جرمي يتحقق عند اختراق اجهزة الكترونية معينة لأغراض شخصية بهدف التسلية، ومن الجدير بالذكر أن هذا التصرف لا يرقى الى مستوى الجريمة الالكترونية الا اذا شكل جريمة وفقا للقانون الجنائي الداخلي استنادا لمبدأ " لا جريمة ولا عقوبة إلا بنص" . وهو من المبادئ الاساسية التي تقوم عليها العدالة الجنائية[٣].

يتضح مما تقدم ان الهجوم المعلوماتي يكون من إختصاص القانون الدولي العام إذا كان يمثل خرقاً لسيادة الدولة المعتدى عليها، بينما تكون الجريمة المعلوماتية من إختصاص القانون الوطني وفقاً لمبدأ إقليمية القانون، ونعتقد إن أهم ما يميز الهجوم المعلوماتي عن الجريمة المعلوماتية هو هدفه الاساس الذي يسعى لإضعاف أو تدمير قدرات الدولة، من خلال الولوج لشبكات الانترنت لغرض سياسي أو مقتضيات الأمن القومي، وهذا على النقيض من الجريمة المعلوماتية التي قد يكون هدفها مقتصراً على السرقة مثلاً لتحقيق منافع مادية لصالح الطرف المهاجم، كذلك فإن الإضرار المحتملة لكل من الهجمات المعلوماتية والجرائم تكون مختلفة بشكل كبير، إذ تهدف الهجمات المعلوماتية إلى إلحاق ضرر شامل سواء بالإشخاص أو الإنظمة المعلوماتية للدولة، بينما ينحصر ضرر الجريمة المعلوماتية في إطار مستخدمين محددين.

---

[١] د.طارق ابراهيم الدسوقي، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، الاسكندرية، مصر، ٢٠٠٩، ص١٥٨.

[2] Oona A Hathaway and others, op.cit,p. 835.

[٣] د.ذياب موسى البداينة ، الجرائم المستحدثة في ظل المتغيرات والتحولات الأقليمية والدولية ، ، ورقة علمية مقدمة إلى الملتقى العلمي في كلية العلوم الاستراتيجية، عمان، الأردن، للفترة من ٢-٤ أيلول ٢٠١٤ .

المبحث الثاني

التكييف القانوني للهجمات المعلوماتية

عند البحث عن التكييف القانوني للهجمات المعلوماتية يجب الركون أولاً إلى قوانين الحرب التي تحكم النزاعات المسلحة أو بعبارة أخرى تكييفها في إطار القانون الدولي بصورة عامة والذي يميز بين اسباب الحرب والحرب ذاتها، إذ يتفرع قانون الحرب إلى فرعين رئيسيين هما قانون حق اللجوء إلى الحرب الذي يتضمن تطبيق القواعد في الفترة السابقة على النزاع المسلح ذات الصلة بالتمييز بين شرعية وعدم شرعية إستخدام القوة في إطار العلاقات الدولية، والقانون الذي يطبق في سياق النزاع المسلح.

وبما إن الهجمات المعلوماتية لم يكن لها وجود يذكر في ظل تقنين القواعد القانونية ذات الصلة باستخدام وسائل واساليب القتال ، فهي بالتالي غير منظمة على وفق القواعد الدولية المعمول بها، كما هو الحال في اتفاقيات لاهاي لعام ١٩٠٧، وما تلاها من اتفاقيات جنيف الأربع لعام١٩٤٩ ، الأمر الذي أدى إلى إختلاف الآراء الفقهية في ايجاد تكييف قانوني محدد لهذه الهجمات في ظل غياب الاساس القانوني الناظم لإستخدامها، ومن الأهمية بمكان لابد من تكييف وتصنيف هذه الهجمات في ظل قواعد ومبادئ القانون الدولي العام إلى جانب تكييفها وتصنيفها ومدى خضوعها للتطبيق في اطار قواعد ومبادئ القانون الدولي الإنساني.

وفقاً لما تقدم فأن هناك عدة أسئلة تثار عند البحث في مدار تكييف الهجمات المعلوماتية، خاصة في ظل عدم وجود قواعد قانونية محددة تختص بتنظيم الهجمات المعلوماتية واستخدامها في الفضاء المعلوماتي، هل يمكن تصنيف الهجوم المعلوماتي إستخداماً للقوة؟ هذهِ القوة التي حظرتها المادة (٤/٢) من ميثاق الأمم المتحدة، حيث أن الافراط في إستخدام هذه القوة أو التهديد فيها يهدد الأمن والسلم الدوليين، وما مدى امكانية تطبيق المادة (٥١) من ميثاق الأمم المتحدة على الهجمات المعلوماتية ذات الصلة بحق الدفاع الشرعي للرد باستخدام القوة ضد الهجمات غير المشروعة؟ وما مدى امكانية تكييف مبادئ وقواعد القانون الدولي الانساني وتطبيقها في اطار الهجمات المعلوماتية؟.

لذا سنحاول الاجابة عن هذه التساؤلات تباعاً من خلال تقسيم هذا المبحث على مطلبين ، نبين في المطلب الأول ، التكييف القانوني للهجمات المعلوماتية في ضوء القانون الدولي العام ، أما المطلب الثاني سنتطرق فيه إلى التكييف القانوني للهجمات المعلوماتية في اطار قانون النزاعات المسلحة وعلى فق الآتي:

المطلب الأول

التكييف القانوني للهجمات المعلوماتية في ضوء القانون الدولي العام

أضحى المجتمع الدولي نتيجة للتقدم العلمي والتكنولوجي يواجه نوعاً حديثاً من الحروب المتطورة والمتمثلة بالهجمات المعلوماتية، بعد أن كانت الحروب تجري في إطار إستخدام الأسلحة التقليدية، وفي ظل إستخدام هذهِ الوسائل المستحدثة في النزاعات بين الدول والتي تصل في بعض الأحيان لمستوى الهجوم المسلح، ولا يمكن بأي حال من الأحوال تجاهل الآثار المادية الملموسة الناشئة عنها، لذلك انقسم الفقه الدولي بين مؤيد ومعارض في تكييف إستخدام الهجمات المعلومات على أساس انها استخدام للقوة العسكرية، وبالتالي تبرر للدول اللجوء إلى استخدام حق الدفاع الشرعي المنصوص عليه في المادة (٥١) من ميثاق الأمم المتحدة، و أوجد البعض من فقهاء القانون الدولي عدة معايير مقبولة في محاولتهم لتصنيف الهجمة المعلوماتية على أنها نوع من استخدام القوة على النحو الوارد في احكام المادة (٤/٢) من ميثاق الأمم المتحدة إلا إن مسألة تصنيف الهجمات المعلوماتية وتكييفها لا يزال يواجه تحدياً نتيجة تباين مواقف وممارسات الدول، إلا أنه في ذات الوقت تولي الدول اهتماماً لهذهِ الهجمات التي يمكن أن تصل إلى حد الاعتداء المسلح وتتسبب في زيادة حجم الدمار بالبنى التحتية المعلوماتية وأحداث خسائر بشرية.

والسؤال المطروح للنقاش بهذا الصدد ، هل يمكن اعتبار الهجمات المعلوماتية مخالفاً لنص المادة (٤/٢) من الميثاق؟ ومتى يكون استخدامها مشروعاً؟ وهل يمكن استخدام حق الدفاع الشرعي ضد الهجمات المعلوماتية؟ لذا سنحاول الاجابة عن هذهِ التساؤلات في ضوء الاجتهادات الفقهية والسوابق القضائية من خلال تقسيم هذا المطلب على فرعين، نبين في الفرع الأول مبدأ

حظر اســـتخدام القوة في إطار الهجمات المعلوماتية، ونناقش في الثاني تصـــنيف الهجمات المعلوماتية كأستخدام للقوة في القانون الدولي، كما يأتي :

الفرع الأول

مبدأ حظر استخدام القوة في إطار الهجمات المعلوماتية

على الرغم من إنّ مبدأ حظر استخدام القوة أو التهديد بها في العلاقات الدولية من المبادئ الاساسية التي نص عليها ميثاق الأمم المتحدة في المادة (٤/٢) منه على إنّ ((يمتنع أعضاء المنظمة جميعاً في علاقاتهم الدولية عن التهديد بأســتعمال القوة أو إســتخدامها ضــد ســلامة الأراضــي أو الاستقلال السياسي لأية دولة أو إلى وجه أخر لا يتفق و مقاصد الأمم المتحدة))[١]، إلاّ أن الميثاق لم يتطرق لما هو المقصود بالقوة التي يمتنع على أعضاء المنظمة التهديد بها وإســـتخدامها في علاقاتهم الدولية ، إذ جرى العرف الدولي على أن طائفة من الأعمال غير الودية مثل الإكراه الاقتصادي والسياسي، وأعمال التجسس، والمقاطعة الإقتصادية وغيرها ، لا ترقى إلى عتبة استخدام القوة، بصرف النظر عن نطاق آثارها.[٢]

وقد آثار النص متقدم الذكر تساؤلاً حول تفسير مصطلح " القوة " سالف الذكر حول ما إذا كان إســـتخدام القوة أو تهديد بإســـتخدامها ، يندرج تحت مفهوم القوة المحظورة، بموجب المادة (٤/٢)، والتي يتطلب الإخلال بها تطبيق العقوبات المنصــوص عليها في الفصــل الســابع من ميثاق الأمم المتحدة أم أنها خارج نطاق الحظر المقصود؟

وقد تنازع اتجاهان حول تكييف مفهوم القوة المحظور إستخدامها في العلاقات الدولية على وفق أحكام الفقرة (٤) من المادة (٢) من ميثاق الأمم المتحدة وعلى النحو الآتي:

– **الاتجاه الأول (الاتجاه المضـــيّق):** يرى أصـــحاب هذا الاتجاه إن المقصـــود من مصـــطلح القوة الذي ورد لفظه في نص المادة (٤/٢) هو القوة المســـلحة التي تأخذ شـــكل

---

(١) ينظر : المادة (٤/٢) من ميثاق الأمم المتحدة لعام ١٩٤٥.

(2) Myriam A.Dunn, the internet and the changing Face, volumenuter: 7, of international Relations and Security, Bulgaria, sofia, proconltd, Issue (1) ,2001

الإعتداءات العسكرية ضد سلامة الأراضي أو الإستقلال السياسي للدول، وأن تطبيق هذهِ القوة أو استخدامها يتم بواسطة عدوان أو هجوم مسلح ترتكبه الدول بإستخدام قواتها المسلحة، أو جماعات منظمة تابعة لها أو مسنده من قبلها.[١]

وقد أنتهج اصحاب هذا الإتجاه في تفسير لفظ " القوة " تفسيراً ضيقاً إذ عَدّ أن تفسير القوة غير المسلحة لا تدخل ضمن تعريف هذا المفهوم، وأن الاشكال المختلفة من القوة لا تدخل ضمن هذا الحظر، والدليل على ذلك ما تضمنته ديباجة الميثاق بمنع إستخدام القوة المسلحة إلا للاغراض العسكرية، وكذلك الأعمال التحضيرية للمادة (٤/٢) تؤكد هي الأخرى إن المقصود من لفظ القوة هو القوة المسلحة فقط، ونتيجة لذلك تم استبعاد اقتراح " البرازيل " إعتبار إجراءات الضغوط الإقتصادية ضمن الإستخدام غير المشروع للقوة.[٢]

- **الاتجاه الثاني (الموسع):** يرى أنصار هذا الاتجاه أن لفظ القوة في نص المادة (٤/٢) يتضمن جميع أعمال العدوان التي يحرمها القانون الدولي، متى ما كانت هذهِ الأعمال تنتهك سيادة الدول، بما في ذلك أعمال التحريض وإثارة الاضطرابات الداخلية عن طريق وسائل الاعلام، فضلاً عن صور أخرى من الإعتداءات التي تدخل في مفهوم القوة طبقاً لنص المادة (٤/٢) من ميثاق الأمم المتحدة .[٣]

وهذا الإتجاه هو على نقيض من الإتجاه الضيّق حيث تبنى انصاره تفسيراً واسعاً للمادة (٤/٢)، إذ يرون أنه ليس من الضروري إعتبار الهجمات المعلوماتية إستخداماً للقوة مشروطاً بأحداث إضراراً مادية جسيمة، بل أن أية هجمات معلوماتية يمكن أن تتسبب في تعطيل لأنظمة

---

[١] علاء الدين حسين مكي، استخدام القوة في القانون الدولي، المطابع العسكرية ، بغداد، ١٩٨٢، ص٦٧.

[2] Kamal Ahmed Khan, use of Force and Human Rights under international Law, Athens institute for Education and Research, conference paper series BLE 2017.

[٣] خالد ابو سجود حساني، استخدام القوة بترخيص من مجلس الأمن في اطار الأمن الجماعي، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، م (١٢)، ع(١)، حزيران ٢٠١٥، ص٣٢٧.

الحواسيب الرئيسية للدولة، أو قادرة على أحداث أضرار اقتصادية يمكن عدها استخداماً للقوة على وفق احكام المادة (٤/٢) من ميثاق الأمم المتحدة.[١]

وعند إمعان النظر في الحجج التي ساقها أنصار هاذين الإتجاهين، نرى أنهما لا يمتان إلى الواقع الدولي بأية صلة، فوفقاً للاتجاه الأول (المضيّق) ، هناك العديد من الهجمات التي تخرج من اطار استخدام القوة لا سيما الهجمات البايلوجية والجرثومية التي تخلو من إستخدام الأسلحة التقليدية كذلك فأن العديد من الهجمات التي صنفها الميثاق استخداماً للقوة يستوعبها الإتجاه المضيق كتدابير الحصار الجوي والبحري .[٢] وحاول الفقيه " Micheal Schmitt "، التوفيق بين الإتجاهين السابقين ، من خلال تأكيده على إنّ الهجمات المعلوماتية يجب أن تكون منسجمة مع الهدف القائم على أحداث الاضرار الجسيمة كأستخدام للقوة، لكن ليس من الضروري أن تنحصر اضرارها بأهداف عسكرية فقط ، فهناك الهجمات التي تحدث اضراراً إقتصادية جسيمة يمكن اعتبارها استخداماً للقوة، وقد وضع Schmitt، خمسة معايير رئيسية لتكييف الهجمات المعلوماتية كاستخدام للقوة هي: شدة الضرر، والضرر الفوري اللاحق، ووجود علاقة مباشرة بين القوة المسلحة وعواقبها، والهجوم المعلوماتي يكون عابراً للحدود الدولية، والقدرة على تقييم أو تمييز الفعل المادي .[٣]

نخلص مما تقدم أن إعتماد أي من الاتجاهين له بالغ الأثر في ترتيب نتائج معينة، وذلك لأن الأخذ بالإتجاه (المضيّق)، سيؤدي إلى حرمان الدول التي تتعرض إلى هجمات غير مشروعة من الرد دفاعاً عن نفسها تجاه أي اعتداء غير مسلح والعكس صحيح، ونعتقد أن رأي الفقيه مايكل ن شميت ، هو الأقرب للصواب، إذ أن العبرة من ذلك ما تحدثه الهجمات المعلوماتية من أضرار جسيمة، كذلك يمكن أن تشمل القوة جميع الضغوط الاقتصادية والسياسية،

---

(1) Titiriga Remus, cyber Attack and international Law of Armed', journal of international , conflicts: ajus ad Bellum perspective, 2013, p.179.

[٢] ينظر نص المادة (٤١) من ميثاق الأمم المتحدة لعام ١٩٤٥ .

(3) Michael N.Schmitt , Computer network Attack and the USA of force in inter- national law though Normative , The Colombia journal of Transitiona law, vol.(37), No.(3), 1998-1999, p,14- 915.

علاوة على ذلك تعد الهجمات التي يتم تنفيذها عبر الفضـــاء المعلوماتي هي الاخرى من القوة المحظور إســـتخدامها في العلاقات الدولية، وهي بهذا الشـــكل تعد تطوراً حديثاً لمفهوم القوة في مجال الاتصالات والتكنولوجيا وأثرها على سيادة الدول.

وعلى الرغم من ان ميثاق الامم المتحدة قد تضـمن صـراحةً مبدأ حظر إسـتخدام القوة في العلاقات الدولية بموجب أحكام المادة (٤/٢) منه، إلا إن هذا المبدأ قد ورد عليه إستثناءان هما: حق الدفاع الشـــرعي، وتدابير الأمن الجماعي حيث اجازهما، القانون الدولي كأســـباب إباحة أو أسباب تبرير ينتقل بموجبها السلوك من حالة التحريم إلى حالة الإباحة، لذا سنتناول كلاهما على وفق الآتي:

أولاً: حق الدفاع الشرعي وفقاً للمادة ٥١ من ميثاق الأمم المتحدة

تطرق ميثاق الأمم المتحدة إلى حق الدفاع الشرعي الفردي أو الجماعي على النحو المبين في المادة (٥١) التي تنص على أنه " ليس في هذا الميثاق ما يضعف أو ينقص الحق الطبيعي للدول، بشـــكل فردي أو جماعي، في الدفاع عن نفســـها في حال اعتداء قوة مســـلحة على أحد أعضـــاء الأمم المتحدة ..". إلا إن هذا الميثاق لم يترك ممارسـة حق الدفاع الشـرعي دون قيد أو شرط، وإنما وضـع له شروط يتوجب على الدول إتباعها، حتى تكون هذه الممارسة مشروعة في اطار نظام الأمن الجماعي ومن هذهِ الشروط بـ:

١- **وقوع اعتداء مسـلح** : تشـترط المادة (٥١) من الميثاق وقوع اعتداء مسلح على دولة معينة وأن يكون قد وقع بالفعل ولا زال مسـتمراً ، حتى تتمكن هذه الأخيرة من اسـتخدام القوة كرد على هذا الاعتداء بعيداً عن موافقة مجلس الأمن، فلا مجال لأثارة حق الدفاع الشـرعي، إذا كان العدوان لم يقع بعد، أو أنه وقع وأنتهى، ففي هذه الحالة يتعين إخطار مجلس الأمن، الذي يتعين عليه أتخاذ الإجراءات والتدابير الملائمة لمواجهة مثل هذه الحالات [١] ، وبهذا الصـدد يثار مدى

---

[١] محمود محمد خلف، حق الدفاع الشـــرعي في القانون الدولي الجنائي، ط١، دار النهضـــة العربية، ١٩٧٣، ص٣٠.

الاختلاف حول المصطلح المستخدم في المادة (٥١)، وهو شرط الاعتداء المسلح لاستعمال الحق في الدفاع عن النفس، ومصطلح استخدام القوة أو التهديد بها على وفق المادة (٤/٢).

وعند امعان النظر في هاتين المادتين، نجد أن كل منهما قد استخدم مصطلح مختلف عن الأخر، وبالتالي يؤدي إلى خيارات قانونية متباينة أمام الدولة المعتدى عليها ، فالاعتداء المسلح يضع الدولة التي تم الاعتداء عليها أمام خيار وحيد هو استخدام القوة ، حيث يشار إلى استخدام القوة في سياق الدفاع عن النفس سواء الفردي أم الجماعي حسب أحكام المادة (٥١)، أما استخدام القوة أو التهديد بها، والذي لا يرقى إلى كونه اعتداءً مسلحاً ، فأنه يضع الدولة المعتدى عليها أمام عدة خيارات قانونية أبرزها إجراءات الرد والذي يمنح بموجبه الدولة المتضررة رد الإعتداء بطرق ما دون استخدام القوة.[١]

إن هذهِ التفرقة تجد اساسها في القانون الدولي والذي وفر شيء من الحماية للدولة التي نستخدم القوة تجاه دولة أخرى، عندما لا يرقى استخدام القوة بوصفة هذا إلى مستوى الاعتداء المسلح الفعلي.[٢] والسؤال المطروح في هذا السياق والذي يتعلق باستخدام حق الدفاع عن النفس، هل يمكن ادراج الهجمات المعلوماتية تحت تصنيف (الهجوم المسلح) الذي يبرر اللجوء إلى الإجراء الدفاعي؟

عند الاجابة على هذا السؤال لا بد من التركيز على الوسائل المستخدمة في الهجوم المعلوماتي، فمثلاً يمكننا أن نستنتج بأنه يمكن للإشارات المعلوماتية أن تتشابه مع طلقات الرصاص والقنابل والقذائف، أو أية أشكال أخرى مختلفة من الاسلحة التقليدية، بشرط أن يكون لديها التأثير ذاته، وحيال ذلك فأن المجتمع الدولي ينتابه الشعور بالقلق من العواقب التي لا تحمد عقباها، والتي قد تنجم عنها حروب الفضاء المعلوماتي، وعلى الرغم من وضوح الدلالة على التفرقة بين المفهومين وما يترشح عنهما من نتائج قانونية، فأنه يبرز للعلن التعقيد في

---

(1)omer Elegab, the Legality of Non- forcible counter- Measures in international Law (oxford Monographs in international Law), 1988.

(2) Randelzhofer, Article 51, in The charter of the united Nations: A Commentary 661, 664 (B.simma ed).1995,

حالات معينة، عند محاولة وضع حدود فاصلة بين استخدام القوة والاعتداء المسلح، وهو في كثير من الحالات غير واضح المعالم، خاصة في ظل خلو ميثاق الأمم المتحدة من أي نص يبيّن هذا الفرق بين المصطلحين، إلاّ أنه على الرغم من ذلك ، يمكن الإستدلال على هذا الفرق من خلال الاطلاع على قرار محكمة العدل الدولية في قضية نيكاواغوا، إذ وصفت الاعتداء المسلح بأنه " من أخطر اشكال استخدام القوة "، حيث بينت المحكمة بهذا الصدد، إن المناوشات المسلحة على الحدود مثلاً لا ترقى إلى مرتبة الاعتداء المسلح الذي من شأنه تفعيل خيار الدفاع عن النفس على وفق المادة (٥١)من الميثاق[١]. ويزداد الأمر سوءً إذا ما تسببت تلك الهجمات بأحداث خسائر فادحة بالأرواح.

وبالتالي فان حق الدفاع الشرعي يكفل لكل دولة الحق في أن تتخذ من الوسائل الدفاعية مما تراه مناسباً لتنأى بنفسها عن الاخطار الداخلية أو الخارجية ، والتي تهدد أمنها ومصالحها الحيوية ، على نحو يكفل لها دوام البقاء والاستقرار[٢]، نظراً لأن هذه الهجمات المعلوماتية، يمكن أن تكون ذات بعد دولي خارج حدود السيادة الوطنية للدولة، وفي سبيل تحقيق السلم والأمن الدوليين، لا بد من تظافر الجهود الدولية لمواجهة تلك الهجمات.

٢- شرط الضرورة والتناسب في استخدام القوة

يقصد بالتناسب أن تكون اعمال الدفاع التي تقوم بها الدولة المعتدى عليها متناسبة مع حجم العدوان وإلا تتجاوزه، أي يجب أن يتحقق التناسب بين جسامة الخطر وجسامة فعل الاعتداء، وبخلاف ذلك يعتبر تجاوزاً في استعمال حق الدفاع الشرعي و بالتالي يعد عدواناً وليس دفاعاً.[٣]

---

(1) I,CJ,case Military and paramilitary Activities in and Against Nicaragua (Nicaragua V.United states), Reports 1986, p.191.

[٢] د.اسماعيل صبري مقلد، اصول العلاقات الدولية في اطار عام ، ط١، دار النهضة العربية ، القاهرة، ٢٠٠٧، ص١١-٢٦.

[٣] د.سعيد سالم جويلي، الجوانب الاقتصادية للتدابير المضادة في القانون الدولي، المجلة القانونية والاقتصادية، كلية الحقوق ، جامعة الزقازيق، ع (٦)، ١٩٩٤، ص١٠١.

والتناســـب هو العلاقة بين التصـــرف الذي تلجأ إليه الدولة والهدف الذي تبتغي تحقيقه والمتمثل في الدفاع الشرعي بدفع العدوان أو ايقافه، إذ إن التناسب في حالة الدفاع الشرعي يهتم بالنتيجة أو الغاية من فعل الدفاع وليس بمضـمون أو قوة العمل نفسـه، مع مراعاة إيجاد نوع من التماثل وليس التقابل بين الوسـائل المسـتخدمة في فعل الدفاع والعدوان، خصـوصـاً إذا ما تعلق الأمر باسـتخدام وسـائل قتالية تندرج في اطار الاسـلحة النووية بالمقارنة مع الاسـلحة التقليدية مثلاً، لما تشتمل عليه الاسلحة النووية من قوة تدميرية هائلة، خصوصاً أن مدى الأسلحة النووية يتجاوز حدود الدولة المعتدى عليها ويمتد أثرها إلى غيرها من الدول المجاورة.[١]

وعلى الرغم أن معايير الضـرورة والتناسـب ذات العلاقة بالهجمات المعلوماتية غير مدرجة في المادة (٥١) من الميثاق، والمتعلقة بحق الدفاع الشـــرعي، إلا إن التزام الدول بها يقوم على اساس انها جزء من القانون الدولي العرفي والذي يعد أمراً هاماً للدول باستخدام القوة على أساس حقها في الدفاع الشـــرعي ضـــد أي هجمات معلوماتية تتعرض لها، وأن عدم التزام الدول بهذه المعايير في نطاق الهجمات المعلوماتية يسبب ضرراً وعملاً غير مشروع.[٢]

إلا إن تطبيق شـرط التناسـب على الهجمات المعلوماتية لازال يواجه تحدياً خطيراً بشـأن الموائمة بين الهجوم والرد عليه، حيث إن شـبكات الحاسـوب تسـمح من خلالها إن تتعدى آثار الهجوم لأكثر من دولة، كذلك الرد عليها يتعدى لأكثر من دولة، دون معرفة أو تحديد الجهة المنفذة للهجوم، وفي هذه الحالة يتحول الدفاع الشـــرعي إلى عدوان، فضـــلاً عن امكانية إحداثه اضراراً لا مبرر لها، إذ من الممكن أن تشمل الاضرار الناشئة عن الهجمات المعلوماتية منشآت حيوية وفّر لها القانون الدولي حماية خاصة اثناء النزاعات المسلحة.[٣]

وغالباً ما يتم اللجوء إلى تقييم الضـرورة التي اسـتدعت حالة الدفاع الشـرعي على اسـاس اتخاذ القرار بالشروع للحصـول على القوة، ووفقاً لهذه الحالة فأن شرط الضـرورة سيكمل وظيفته،

---

[١] د.محمد محمود خلف، مصدر سابق، ص٤٥١.

[2] Claywilson, bootnets, cyber crime, and cyber terrorism, vulnerabilities and polic issues for congress, 2007.

[٣] د.عادل عبدالصادق، اسلحة الفضاء الالكتروني في ضوء القانون الدولي المعاصر، مصدر سابق، ص١١٣.

ومع ذلك فأن وقوع الهجوم المعلوماتي، والذي يعد هجوماً مسلحاً لا يعني بالضرورة هي ضرورة الدفاع الشرعي، عليه يجب على الدولة المعتدى عليها التي تعرضت للهجوم المسلح، أن تثبت أنه ليس لديها وسيلة أخرى سوى الدفاع عن نفسها[١].

ثانياً: تدابير الأمن الجماعي

إن تطبيق تدابير الأمن الجماعي، من قبل مجلس الأمن الدولي، لا يمكن ان يتم إلا بعد أن يقرر أن الوقائع المعروضة عليه تشكل تهديداً للسلم او اخلالاً به، أو عملاً من اعمال العدوان استناداً إلى المادة (٣٩) من الميثاق.[٢]

وتكمن أهمية التدابير بمنع تفاقم الموقف بين الأطراف المتنازعة والذي يؤدي احياناً لنشوب حالة الحرب، من خلال دعوة اطراف النزاع لحل نزاعاتهم بالطرق السلمية، فالغرض من التدابير المؤقتة بموجب المادة (٤٠) من الميثاق هو لمنع تفاقم الوضع القائم، على الرغم من عدم وجود إشارة في الميثاق لتنظيم هذه التدابير، إلا إن مجلس الأمن سعى لأتخاذ تدابير مؤقتة مثل وقف النزاعات وانسحاب القوات المسلحة، أما التدابير القسرية التي ورد ذكرها في المادة (٤١) من الميثاق وهي على نوعين: تدابير لا يتطلب استخدام القوة المسلحة مثل قطع العلاقات الدبلوماسية والإقتصادية واخرى تطلب إستخدام القوة عن طريق القوات الجوية والبحرية والبرية في حال قيام حالة الضرورة.[٣]

وبالرجوع إلى أحكام المادة (٣٩) من الميثاق ، نجد انه الحق فعل العدوان وربطها بتهديد السلم والاخلال به، حيث ان مصطلح وتهديد السلم ، من الممكن ان لا يتطابق نوعاً ما مع

---

[١] عبدالمطلب ممدوح عبدالحميد، جواز استخدام الكمبيوتر– شبكة المعلومات العالمية، الجريمة عبر الانترنت، ط١، مكتبة دار الحقوق، الشارقة، ٢٠٠١، ص١٥٦.

[٢] نصت المادة (٣٩) من ميثاق الأمم المتحدة على انه "يقرر مجلس الأمن ما اذا كان قد وقع تهديداً للسلم أو الأخلال به أو كان ما وقع عملاً من اعمال العدوان، ويقدم في ذلك توصياته أو يقرر ما يجب اتخاذه من التدابير طبقاً للمادتين ٤١و ٤٢ لحفظ السلم والأمن الدولي او اعادته إلى نصابة).

[٣] عدنان عبدالعزيز مهدي الدوري، سلطة مجلس الأمن الدولي في اتخاذ التدابير المؤقتة، ط١، م (٢١)، ع(٤)، دار الشؤون الثقافية العامة، بغداد، ٢٠٠١، ص٢٥–٢٧.

الهجمات المعلوماتية الدولية لانه موضـوع تهديد السـلم في غاية الخطورة والدقة، ولكن اذا تأملنا ما يجري على صعيد الدول المتقدمة من اجراءات وتدابير، نصل إلى نتيجة مفادها ان هذا العمل لا يقل خطورة عن العدوان ، ولعل ما فعلته بريطانيا عام ٢٠١٤ بأتخاذها اجراءات أمنية لتعزيز قدراتها المعلوماتية ، حيث تم اختيار مجموعة بنوك وبورصـــات الاســـتثمار في مواجهة هجوم منسـق وتدريبي، وهمي على الانترنت من جانب دولة معادية تتسـبب بعطل كبير وخلل واضـح وشـــارك في التمرين عدد كبير من الخبراء والمســـؤولين الحكوميين ومقدمي خدمات البنية التحتية.[١]

ومن الامثلة التطبيقية على فعل العدوان من خلال الهجمات المعلوماتية هو اســـتهداف المنشـآت الايرانية النووية بفيروسـات ضـارة عام ٢٠١٤ أخترقت انظمة التحكم الصـناعية على نطاق واسـع في مراقبة الوحدات التي تعمل بنظام آلي، وكانت اصـابع الاتهام تشـير إلى ان فعل العدوان بالهجمات المعلوماتية تشـير إلى توجيه اتهامات لدول متعددة وهي روسـيا ، الصـين، الولايات المتحدة، إســـرائيل، وتم ذكر هذه الدول التي يشـــتبه في إنها كانت وراء إطلاق هذا الفيروس الذي حطم مفاعل بوشهر الإيراني والكثير من محطات تخصيب اليورانيوم في إيران.[٢]

وأما مســـألة تحديد فيما اذا كانت أنشـــطة معلوماتية معينة تشـــكل تهديداً للســـلم والأمن الدوليين فأن سـلطة مجلس الأمن ليسـت مطلقة تماماً كما هو الحال عند اسـتخدام صـلاحيته المنصـــوص عليها في الميثاق، على أقل تقدير يكون مجلس الأمن ملزماً بالتصـــرف على نحو يتفق مع مقاصـــد ومبادئ الميثاق، وبصـــورة أشـــمل مع مبادئ العدالة والقانون الدولي.[٣] وعند الحديث عن الحاق الهجمات المعلوماتية بفعل العدوان فعلياً لم نجد ما يشـير إلى أي ممارسـات دولية تسـتطيع الركون إليها في شـأن قيام مجلس الأمن باتخاذ تدابير رداً على هجمة معلوماتية

---

[١] جمال العظامات، جريمة العدوان في الهجمات الالكترونية في نطاق القانون الدولي العام، مجلة المنارة، م (٢١)، ع (٤)، ٢٠١٥، ص١٦.

[٢] جمال العظامات، المصدر نفسه، ص١٩.

[3] NilS Melzer, cyber war fare and inter-national law ,Geneve: UNIDIR Resources, 2011, p.19.

دولية لأن مجلس الأمن لا يضـــع معياراً محدداً ينتهجه في تكييف ما يعرض عليه من وقائع، إذ أن مجلس الأمن لا يتقبل وضع قيود محددة لسلطته التقديرية.[١]

الفرع الثاني

تصنيف الهجمات المعلوماتية كاستخدام للقوة في القانون الدولي

الهجمات المعلوماتية هي كغيرها من الهجمات المسلحة، يتوجب على الدول التي تعرضت للاعتداء أن تكون قادرة على تصنيف اشكال الهجوم المعلوماتي على انه هجوم مسلح أو هجوم مسلح وشيك، قبل استعمال الدولة المعتدى عليها لحقها في الرد بأستخدام وسائل دفاعية نشطة، فهناك الهجمات المعلوماتية التي تصنف بأنها هجمات مسلحة، أو هجمات مسلحة وشيكة، او أنها استخدام اقل للقوة .

ونظراً لأن الهجمات المعلوماتية هي شكل جديد نسبياً من اشكال الهجمات، لذلك لا زالت الجهود الدولية غير قادرة على تصـــنيفها على نحو دقيق على الرغم من أن القانون الدولي قد تضمن المبادئ القانونية الاساسية الحاكمة لتلك الهجمات، والسؤال الذي يتبادر إلى الذهن هل يمكن إعتبار الهجمات المعلوماتية هجمات مسلحة؟ يتطلب الإجابه عن هذا السؤال البحث عن مدى انطباق المبادئ القانونية الاساسية التي تحكم الهجمات المسلحة التقليدية ومحاولة تطويعها على الهجمات المعلوماتية، لذا سنقوم بأستعراض بعض الآراء الفقهية والسوابق القضائية التي تتعلق بهذا الصدد والتي من خلالها يمكن مناقشة الاجابة عن امكانية تصنيف هذهِ الهجمات كأستخدام للقوة في اطار القانون الدولي:

تصدت محكمة العدل الدولية في قضية الأنشطة العسكرية وشبه العسكرية في نيكاراجوا[٢] Nicaragua case إلى المادة (٤/٢) من ميثاق الأمم المتحدة من زاويتين، الزاوية الأولى : عندما تطرقت المحكمة إلى طبيعة هذه المادة، أكدت في الفقرة (١٨٧) من حكمها على تحول

---

[١] جمال العظامات، مصدر سابق، ص١٩.

[2] ICJ, Nicaragua case 1986, op,cit , para, 187.

مبدأ حظر اســـتخدام القوة أو التهديد بها إلى قاعدة عرفية دولية يتعين على جميع الدول واجب التقيد والالتزام بها[١] ، يشـــار إلى إن ذلك جاء منســـجماً مع حقيقة أن معظم بنود ميثاق الأمم المتحدة هي أصلاً مبادئ أساسية لا يحق لأي دولة مخالفتها أو الخروج عنها.

اما الزاوية الثانية: تتمثل في الحالات التي يمكن أن تعتبر أســـتخداماً للقوة خلافاً لما جاء بنص هذهِ المادة ، وبهذا الصـدد قد أقرت المحكمة المذكورة بعمومية المادة وعدم إقتصـارها على اســتخدام القوة بالمعنى التقليدي لها، والمتمثل في اســتخدام قوات عســكرية نظامية خارج حدود الدولة الاقليمية، حيث أسهبت واقرت أن ارسال القوات من قبل الدولة أو بالنيابة عنها سواء كانت على شــكل مجموعات نظامية أو غير نظامية، أو أية ادوات أخرى، تعد مخالفة صــريحة للمادة (٤/٢) من الميثاق، وبناءً على ذلك يمكن اعتبار هذا التصــرف هجوماً مســلحاً على وفق أحكام المادة (٥١) من الميثاق بالاستناد إلى حجم وتأثير استخدام القوة.[٢]

عند تحليل مضــمون القرار الذي اصــدرته محكمة العدل الدولية بخصــوص القضــية آنفة الذكر، نلحظ أنها قد حادت بوضــوح عن النهج التقليدي لمفهوم اســتخدام القوة ، ذلك الإســتخدام للوســـائل التقليدية في الإعتداء، والذي يفترض فيه أن تقوم الدولة بأتخاذ قراراً مباشـــراً يتعلق بأستخدام القوة في إقليم دولة أخرى.[٣]

وإن موقف المحكمة بهذا الشـــأن أنما جاء تأكيداً على نية الدول الحقيقية المشـــاركة في صياغة نص المادة (٤/٢) من الميثاق، إذ إن الأعمال التحضيرية لهذه المادة تشير بوضوح إلى إن أي استخدام للقوة أو مجرد التهديد بها بين الدول الأعضـاء سوف يشكل انتهاكاً لهذه المادة، على شرط أن يكون مخالفاً لمبادئ الميثاق الذي تمت صياغته بإرادة الجماعة الدولية.[٤]

---

(1) See, Kamrul Hossain, The concept of jus Cogens and the obligation under the U.N. charter, santa clara joumal of international law , vol.39, Issue (1), 2005.

(2) ICJ, Nicaragua case, op. cit, 1986, para, 195.

(3) Milorad Petreski, The international public law and the use of force by states, journal of Liberty and international Affairs, vol.(1), No.2, 2015.

(4) Doc,784, 1/1/27. 6 U.N.C.I.O.Docs (1945).

علاوة على ذلك، فأن المحكمة بأتخاذها هذا الموقف أنما هو بمثابة تأكيد لفكرة مسؤولية الدولة عن ممارساتها الخاطئة سواء المباشرة منها أم غير المباشرة، بما فيها تلك الناشئة عن تقصيرها بواجب عدم التسبب بالحاق الضرر بالدول الأخرى خارج نطاق ولايتها الاقليمية، وهو ما يعرف بواجب العناية "Due Diligence" ، والذي سيأتي ذكره لاحقاً في الفصل الثاني من هذه الدراسة، عند التعرض لمفهوم واجب العناية اللازمة للدول ، ومن الواضح أن المحكمة قد أسهمت بشكل فعال في تطوير هذا المفهوم وبالتحديد في قضية قناة كورفو بين البانيا والمملكة المتحدة في العام ١٩٤٩.[١]

نلحظ من خلال ما تقدم أن المحكمة من خلال حكمها في قضية نيكاراغوا، قد كانت مهيئة لإحتواء أصناف أخرى غير الهجوم العسكري التقليدي في إطار التصرفات التي يمكن أن تشكل انتهاك لأحكام المادة (٤/٢) من الميثاق، ومن الجدير بالذكر أن موضوع الفصل في النزاع المعروض أمام هذهِ المحكمة في القضية المذكورة ، لم يكن في إطار الهجمات المعلوماتية، وإنما كان يتمحور حول الدعم العسكري غير المباشر الذي كانت تقدمه الولايات المتحدة لعناصر ومناهضة للحكومة في نيكاراغوا، وبسبب الاتصال بين هذهِ العناصر وحكومة الولايات المتحدة الذي نتج عنه علاقة غير مشروعة بينهما، أقرت المحكمة بوجود خرق من جانب الولايات المتحدة للمادة (٤/٢) من الميثاق، وحيث أن أحكام هذهِ الفقرة لها صفة الزامية على جميع الدول الأعضاء كحال باقي نصوص الميثاق فقد توصلت المحكمة إلى نتيجة الحكم الذي صدر لصالح نيكاراغوا ضد الولايات المتحدة.

وعند الاطلاع على حيثيات القضية التي استندت إليها المحكمة في حكمها آنف الذكر ، نجد أن هذا الحكم هو قابل للقياس على حالات مشابهة، كما هو الحال عند ادعاء دولة معينة ضد أخرى بشأن تعرضها لهجمة معلوماتية خاصة إذا ما حققت هذهِ الهجمة معيار الحجم والتأثير على الدولة التي تتعرض للهجوم، لكن يشترط في ذلك شرط جوهري هو إسنادها إلى

---

(1) ICJ, Corfu channel case (UK.V.Albania), Judgment, 1949 I.CJ, ReP.4,22 (Apr,9): See also Robert P.Barnidge, The Due Diligence priniciple under inter national law, community Review, vol.(81), Issue 8, 2006.

الدولة المدعى عليها، تأكيداً على ذلك ، جاءت النســـخة الأولى من دليل تالين لعام ٢٠١٣، لتؤسس لهذا التصور بالقياس، حيث جاءت المادة (١١) منه لتؤكد على أن "العمليات المعلوماتية تعتبر اســـتخداماً للقوة عند ما يكون محتواها وتأثيرها متقارباً مع العمليات غير المعلوماتية"[١]. والتســـاؤلات المطروحة للنقاش بهذا الصـــدد هل تنتهك هذه الهجمات الحظر الوارد في المادة (٤/٢) من ميثاق الأمم المتحدة؟ وهل تشـكل هجوماً مسـلحاً أم يعد ذلك شـكل أخر من أشـكال القوة كالإكراه الاقتصـادي أو السـياسـي؟ وهل يعد ذلك مبرراً للدولة باسـتخدام حق الدفاع الشرعي عند تعرضها لهجوم معلوماتي؟

إبتداءً تشكل الهجمات المعلوماتية نمطاً مستحدثاً من أنماط الهجمات المتطورة تكنولوجيا، إذ لم يكن بحسـبان واضـعوا مسـودة ميثاق الأمم المتحدة أن تطرأ مثل هكذا أنماط من الهجمات مستقبلاً، وبالتالي فهي تثير صعوبات وتحديات في كيفية تصنيف هذهِ الهجمات كأستخدام للقوة المسلحة أو بأعتبارها شكل اخر من أشكال القوة ، لذلك اجتهد الفقهاء في تطوير بعض النماذج التحليلية للتعامل مع هذهِ الهجمات المعلوماتية وبيان طبيعتها ونطاقها، ونتيجة لذلك ظهرت عدة اتجاهات فقهية حول كيفية تصنيفها في إطار إستخدام القوة المسلحة وعلى النحو الآتي:

أولاً": النهج القائم على الوسيلة (Instrument-Based Approach)

يذهب انصـار هذا الاتجاه إلى تبني الوسـائل التقليدية العسكرية كمعيار لتحديد ما إذا كان نشاطاً معين يشكل استخدام للقوة في القانون الدولي، ويرى هؤلاء أن الهجمات المعلوماتية طالما أنها لم تستخدم الاسلحة العسكرية التقليدية فلا تعد هجوماً مسلحاً استخداماً للقوة[٢]، إذ ينظرون هؤلاء الفقهاء للهجمات المعلوماتية على إنها استخداماً للقوة وهجوماً مسلحاً فقط عندما تكون هذهِ

---

(1) Micheal N.Schmitt (ed), Tallinn manual on the international law Applicable to cyber ware fare (Cambridge university press , 2013) at paragraph 11.

(2) Christopher D.Deluca, The need for international laws of war to include cyber Attacks involving state Actors, pace international law Review on line companion, 2013, vol.(3), No.(9), p.845-846.

الهجمات ناجمة عن إستخدام أسلحة عسكرية تقليدية، أو تكون مصاحبة للهجوم التقليدي[١]، وهو بهذا المعنى لا يكون هناك مبرراً للدولة باستخدام حقها في الدفاع الشرعي الوارد في المادة (٥١) من الميثاق والناجم عن هجوم مسلح ، لأنه يخلو من الخصائص الفيزيائية المرتبطة بالإكراه العسكري ، وبصورة عامة لا يحتوي على طاقة حركية (Kintinc) ، كما هو سائد في الاسلحة التقليدية[٢].

على سبيل المثال في ظل النهج القائم على الوسيلة، فأن الهجوم المعلوماتي المستخدم لإغلاق شبكة كهرباء معينة هو هجوم مسلح، وذلك لأن مرفق الخدمة التي تدعمها شبكة الطاقة، عادة ما يتطلب إسقاط قنبلة على محطة لتوليد الكهرباء، أو بعض الاستخدامات الحركية الاخرى لإعاقة الشبكة، بسبب أن هذه الذخائر التقليدية كانت معدة مسبقاً لتحقيق النتيجة، في ضوء هذا النهج القائم على الوسيلة، يتم التعامل مع الهجوم المعلوماتي بذات الأسلوب[٣] ومما يدعم أنصار هذا الاتجاه ما تضمنه ميثاق الأمم المتحدة باعتبار أن قطع الإتصالات البريدية، ووسائل الاتصال الاخرى ، هي تدابير ليس من الضروري إستخدام القوة فيها[٤].

ولكن محكمة العدل الدولية قد ذهبت إلى رأي مغاير لمعيار أصحاب هذا الاتجاه، وتجسد ذلك من خلال رأيها بخصوص مشروعية التهديد أو أستخدام الأسلحة النووية، إذ أوضحت بأن النص المتعلق بحظر استخدام القوة في العلاقات الدولية هو غير محدد بإستعمال صورة معينة من الاسلحة ، بل تشمل جميع اشكال القوة من دون التقييد بالأسلحة المستخدمة فقط[٥].

---

[٣] سراب ثامر أحمد، مصدر سابق، ص١١٠.

[2] Michael N.Schmitt, computer Network Attack and the use of force in international law, op.cit, p.846.

[3] Jeffrey carr, inside cyber war fare, second Edition, published by O 'Reilly Media, Ink, Sebastopol, USA, 2012.

[٤] المادة (٤١) من ميثاق الامم المتحدة لعام ١٩٤٥.

[٥] للمزيد ينظر : الفتوى التي اصدرتها محكمة العدول الدولية بشأن مشروعية استخدام الاسلحة النووية أو التهديد بها، رأي استشاري ١٩٩٦، الفقرة ٣٩، ص٢٣.

كما ساند حلف شمال الاطلسي الناتو (NATO)، أصحاب هذا الاتجاه وأيد هذا المعيار من خلال إدراج نص في منهج الدفاع السيبراني المشترك التابع له عام ٢٠١٤ على "إنّ الهجوم المعلوماتي سيلزم الدول الأعضاء بالتشاور فيما بينهم بموجب المادة (٤) من معاهدة الناتو..." لكن الهجوم المعلوماتي لا يمكن أن يشكل هجوماً مسلحاً يلزم الدول الأعضاء بمساعدة بعضها البعض الأخر بموجب المادة (٥) من هذهِ المعاهدة[١].

يتضح مما تقدم إن النهج القائم على الوسيلة يمتاز بمرونة تطبيقه، وذلك بسبب سهولة اللجوء إلى إستخدامات الاسلحة والقوة العسكرية التقليدية، إلاّ أنها تغض النظر عن الانشطة المعلوماتية التي تتميز بقدرتها الهائلة التي يمكن أن تتسبب بأحداث اضرار من دون إستخدام أسلحة عسكرية تقليدية.[٢] وعلى الرغم من الخصائص التي يتميز بها النهج القائم على الوسيلة لكن عيوبه دعت انصار هذا الاتجاه إلى التخلي عنه عند التعرض لتعريف الهجوم المسلح.

ثانياً: النهج القائم على الحجم والآثار (Scale and Effect)

استخدام هذا الإتجاه في دليل تالين، إذ ذهب الخبراء في دليل تالين إلى أن الهجمات المعلوماتية تعتبر استخداماً للقوة متى ما كانت بحجم وتأثير الهجمات غير المعلوماتية التي تصل إلى مستوى إستخدام القوة[٣]، وعمل بعض من الفقهاء المؤيدين لهذا الاتجاه إلى تحديد الشروط التي يمكن القياس عليها لتصنيف الهجوم المعلوماتي كهجوم مسلح وهذهِ الشروط: الفورية في تحقق العواقب، وشدة الدمار، الخطورة، وإمكانية قياس الآثار[٤]،إذ يرى انصار هذا الاتجاه إن كل نشاط غير مشروع يمكن ردعه على وفق آثاره على الدول الأخرى[٥].

---

(1) North Atlantic Treaty, supra note 98,artcle 4,5, NATO Agree common Approach to cyber Defence , supranot 97.

(2) Oona Hathway,and others, op.cit, p.846.

(3) Tallinn Manual, op. cit, Rule (11).

(4) Micheal N.Schmitt, computer Network Attack and the use of force in international law, op.cit,p.914.

(5) Sean P.Kanuck, Recent Devlopment: infor mation war fare: New challenges for public international law, 37 Harvard international law journal, 1.274, 290, 1996.

وعلى الرغم من الاختلاف التفصـــيلي بين فقه محكمة العدل الدولية، وموقف الخبراء في دليل تالين، نلاحظ أن هناك ثمة عاملاً مشــتركاً بينهما يتجلى في الحجم والآثار كمعيارين يمكن الركون إليهما لتفعيل اللجوء إلى الدفاع عن النفس على وفق أحكام المادة (٥١) في ميثاق الامم المتحدة، حيث أن كلاً من لجنة الخبراء والمحكمة ، ينظران إلى إن أي اعتداء على الدولة وبأي شــكل كان، بما فيها الهجمات المعلوماتية، يعد انتهاكاً لســيادتها مما يمنح الحق للدولة المعتدى عليها رد هذا الاعتداء ضمن شرط اساسي وحيد هو أن يكون حجم وآثار هذا الهجوم على الدولة المعتدى عليها ضـــمن مســـتويات محدودة، وهذا ما عملت عليه لجنة الخبراء وقامت بجهود متواصــلة لغرض معرفة الهجمات المعلوماتية التي يمكن إن ترقى إلى عتبة الهجوم المســلح بعد دراسة مجموعة من الخصـائص التي تتسم بها هذه الهجمات، وتؤول إلى نتيجة مفادها أن الدولة المعتدى عليها يمكنها اســـتخدام حقها في الدفاع عن نفســـها على وفق احكام المادة (٥١) من ميثاق الامم المتحدة ، وقد ذهب الكاتب **(Micheal N.Schmitt)** إلى وضـع إطار معياري يتمثل بعدة شروط جوهرية لغرض تصنيف الهجوم المسلح كهجمات معلوماتية ومن اهمها:

١- شرط شدة الدمار (Severity)

على وفق هذا المعيار يمكن تحديد نطاق وكثافة الهجوم ، بالإســتناد إلى تحليل اســتخدام القوة في اطار هذا المعيار يتم النظر إلى حجم الخسـائر البشـرية، وطبيعة المنطقة التي تتعرض للهجوم ، وشــدة الضــرر الذي تعرضُــت له الممتلكات وهناك علاقة بين شــدة الاضــرار الذي يحدثها الهجوم وتصــنيفه إلى هجوم معلوماتي، وبالتالي يمكن من خلاله معرفة فيما إذا كان هذا الهجوم المعلوماتي بمثابة هجوم مسلح أو استخدام للقوة.[١]

حاول دانيل سـيلفر (Daniel B.Silver) المسـتشـار العام السـابق لوكالة الاسـتخبارات المركزية ووكالة الأمن القومي الامريكية إيجاد علاقة وثيقة بين الفعل الناجم عن الهجوم وبين النتيجة المتوقعة من هذا الهجوم، حتى يكون مســـوغ للدولة المعتدى عليها تفعيل حق الدفاع الشرعي، إذ ذهب بالقول إنّ : "الهجوم المعلوماتي يسوغ الدفاع الشرعي إذا كانت نتيجة المتوقعة،

---

(1) Jeffrey carr, op, cit, p.60.

إحداث اصابات جسدية أو أضرار مادية تماثل النتائج المرتبطة بالهجوم المسلح"[١]، ولذلك فأن نطاق الهجوم وكثافة العواقب المترتبة على هذا الهجوم، لها أثر بالغ في تقييم شـــدة الدمار التي نجمت عن هذا الهجوم[٢].

ومن الجدير بالذكر إن الهجمات المعلوماتية لها القدرة على أن تحدث الضـــرر المماثل المتصـور في الهجمات العسـكرية التقليدية، أو ربما يكون أكثر من ذلك، ولكن هناك سـؤال في غاية الأهمية هو ما مســتوى شــدة الضــرر الذي يمكن أن تحدثه الهجمات المعلوماتية؟ وهل تتماثل بمســـتوى الضـــرر مع الهجمات التقليدية العســـكرية؟ من الطبيعي أن تحدث هجمات معلوماتية دون أن ترافقها أضـــرار مادية على الافراد أو الممتلكات لدولة معينة، كذلك يمكننا أن نتصــور أن تكون النتائج المترشــحة عن الهجوم المعلوماتي تختلف عن تلك النتائج الناجمة من الهجوم العسكري التقليدي.

فعلى سبيل المثال فمن الممكن أن يحدث اعتداءاً بالأسلحة المعلوماتية على مؤسسة معينة تابعة لدولة معينة يؤدي إلى إحداث فوضى بعمل هذه المؤسسة دون أن ينتج اضراراً مادية، لكن في ذات الوقت يمكن أن نتصور هجوماً معلوماتياً أخر على شبكات الحاسوب في قطاع الصحة لدولة معينة يؤدي إلى حجب الخدمة عن اقســام الطوارئ وبالتالي عطل أجهزة التنفس مما يؤدي إلى حدوث وفيات كثيرة نتيجة هذا الهجوم، ولكن السؤال المطروح للنقاش بهذا الصدد هل إن كلاً الاعتدائين يمثلان هجوماً معلوماتياً يبرر للدولة المعتدى عليها أن تســـتخدم حق الدفاع عن النفس؟

للأجابة عن هذا الســـؤال ، عمدت لجنة الخبراء في دليل تالين إلى ضـــع معيار جوهري بالاستناد إلى وقوع الضرر المادي على الدولة المعتدى عليها سواء وقع هذا الضرر على الافراد أم الممتلكات، وقياســـاً على هذهِ الحالة تعد الهجمات المعلوماتية هجوماً عســـكرياً ، اما تلك

---

(1) Daniel B.silver, computer Network Attack as a use of force under article 2(4) of united Nations charter, in computer network attack and international law 73, 80- 82 ,Editors Michael N.Schmitt and Brian T.Donnell eds, 2002, p.92.

(2) Tallinn Manual, op. cit, comment (9/a) on Rule (11).

الإعتداءات التي لا تلحق مثل هذا النوع من الضـرر فهي خارج نطاق الهجوم العسكري بحسب رأي اللجنة المعنية، باستثناء حالة واحدة هي أن تتسبب هذه الهجمات المعلوماتية بأحداث ضرر لمصلحة وطنية حساسة للدولة التي تم الاعتداء عليها ، دون أن تتعلق بضرر مادي محسوس[١].

ومن الجدير بالذكر قامت اللجنة المذكورة بأخراج طائفة من الهجمات المعلوماتية من دائرة تصـنيفها كهجوم مسـلح، كتلك التي تؤدي إلى خلق (حالة من الفوضـى) في الدولة المتضـررة دون أن يرافقها أي ضرر في مصلحة حيوية للدولة، فأن حالة الفوضى التي خلفها الاعتداء على أحدى مؤسسات الدولة الادارية لا يرقى إلى كونه هجوماً يستدعي تنطبق أحكام المادة (٥١) من الميثاق، ولكن الهجمة المعلوماتية التي يكون لها تأثير مباشـر في مصـلحة وطنية تهم الدولة، كسـرقة البيانات المخزنة داخل حواسـيب عائدة لمؤسـسـة عسـكرية في الدولة المعتدى عليها، وبالتالي فهي وفقاً لهذا المعيار تكون هجوماً عسكرياً يبيح للدولة استخدام حق الدفاع الشرعي.

وقد أيد هذا الاتجاه الفقيه ماركو روسـيني (Marco Roscini) فقد ذهب بالقول ".. من الممكن عد الهجمات المعلوماتية بمثابة انتهاك واضـح لأحكام الفقرة (٤) من المادة (٢) من ميثاق الأمم المتحدة ، على شـرط أن تتسـبب بتعطيل أو دمار واسـع للبنى التحتية التي تمس مصـلحة الدولة الوطنية، أو التي تكون ضـرورية في حياة الإنسـان، وينتج عن ذلك حق الدولة المعتدى عليها في اللجوء إلى استخدام القوة بموجب المادة (٥١) من الميثاق نفسه، والتي تتعلق بحق الدفاع عن النفس"[٢].

وعلاوة على ذلك إن الهجمات المعلوماتية التي ترقى إلى عتبة الهجوم المسـلح، وإن كانت تبيح حق الدفاع عن النفس، إلاّ إن هذا الحق مقيداً وليس مطلقاً، لأن اسـتخدام الدولة للقوة المسـلحة رداً على الهجوم المعلوماتي، يجب أن يتوائم ليس فقط مع ميثاق الأمم المتحدة بل وقواعد القانون الدولي العرفي، وما تضـمنته مبادئ القانون الدولي الانسـاني من إسـتخدام القوة

---

[١].للمزيد ينظر بهذا الصدد: الشروط التي وضعتها لجنة الخبراء في دليل تالين وبالتحديد شرط الآنية أو الفورية ، حيث أوجبت أن يكون الضرر محدداً وحالاً وليس متوقعاً. كذلك ينظر: Jeffrey car , op,cit, p.60.

[2] Marco Roscini, " world wide war fare- jusad Bellum and the use of cyber force , " Max plank year book of united Nations law, vol.(14), 2010, p.85, 130.

العسكرية كمبدأي التناسب والضرورة العسكرية في استخدام القوة المسلحة ايضاً[١]. والتي سنتطرق لهذهِ المبادئ تباعاً في المطلب الثاني من هذا المبحث عن التعرض لمدى انطباق القانون الدولي الإنساني على الهجمات المعلوماتية.

ونود أن نوضـــح بهذا الصـــدد أن آراء الفقهاء قد أكدتها مجموعة من الخبراء التي اعدت دليل تالين، حيث إنها قد اســتندت إلى معيار الحجم والآثار ، وذلك لبيان فيما إذا كانت الهجمة المعلوماتية ترقى إلى مستوى إستخدام القوة غير المشروع والتي تشكل إنتهاكاً للمادة (٤/٢) من ميثاق الأمم المتحدة ، كذلك لبيان فيما إذا كان هجوماً عسكرياً معيناً يعد مبرراً للدفاع عن النفس وفق المادة (٥١) من الميثاق نفسـه، وبهذا فأن المحكمة اسـتندت إلى ذات المعيارين في قضـية نيكاراغوا متقدمة الذكر.

والسـؤال المطروح بهذا الصـــدد حول تحديد ما المعنى الدقيق لمصـــطلحي الحجم والآثار الخاص بالهجمة المعلوماتية، الذي يبرر للدولة المعتدى عليها بموجب هذين المعيارين أن تسـتند إلى المادة (٥١) من الميثاق للدفاع عن نفسها من عدمه؟

للاجابة على هذا السؤال، يتعيّن الاطلاع مرة أخرى إلى ما قررته محكمة العدل الدولية في قضـية نيكاراغوا، فقد أجرت المحكمة مقارنة بين اشـكال اسـتخدام القوة (الأكثر خطورة) والتي تصـل إلى الهجوم المسـلح ، والاشـكال التي تكون (أقل خطورة) ، لأن في حالة الدفاع الفردي عن النفس ، تخضـــع ممارســـة هذا الحق للدولة المعنية لكونها هي الدولة المعتدى عليها نتيجة الهجوم المسلح[٢].

وبعبارة أخرى فأن محكمة العدل الدولية تســـتخدم المقاربة القائمة على الآثار التي تمنح أهمية إلى النطاق والآثار[٣]، والتي تمنح حق الدولة في الدفاع عن نفســـها وفقاً للمادة (٥١) من

---

(1) Oona A.Hathway, op. cit, p.849.

(2) ICJ,Nicaragua case, op.cit, para, 191.

(3) See: the test enunciated by the ICJ in Nicaragua USA.ICJ Rep.1986, at para, 195. iF "suchan operation, because of its scalea and Effects, would have been classified asan armed attack.

الميثاق، بدلاً من المقاربة المبنية على مجرد استخدام القوة بموجب المادة (٤/٢) من الميثاق، فقد تحدث هناك فجوة لا تلجأ فيها الدولة الضحية إلى حق الدفاع عن النفس، ولكن فقط إلى أعمال وتدابير مضادة مشروعة ، أو اللجوء إلى مجلس الأمن الدولي ، ما دون الدفاع عن النفس وفقاً للمادة (٥١) من الميثاق، رداً على قيام الدولة بارتكاب فعل ضدها[١].

ومع ذلك فقد أوضحت محكمة العدل الدولية في قضية المنصات النفطية، بين إيران والولايات المتحدة، والتي تمحورت حول حادثة تدمير مجموعة من منصات النفط الإيرانية من قبل الولايات المتحدة الامريكية في عام ١٩٨٧، أن الهجوم المسلح بموجب المادة (٥١) من ميثاق الأمم المتحدة والقانون العرفي الدولي ليس مرادفين لمبدأ حظر استخدام القوة في القانون الدولي ، وبالتالي بما أنه هجوم مسلح أدى إلى اثارة حق الدفاع عن النفس فهو أخطر اشكال إستخدام القوة[٢].

٢- شرط الفورية أو الآنية (Immediacy)

يعنى هذا الشرط بتحليل مقدار الوقت الذي يستغرقه الهجوم، فضلاً عن المدة الزمنية بين الهجوم وتحقق الآثار[٣]. وفي هذا السياق استندت لجنة الخبراء إلى معيار (الفترة الزمنية الكافية) التي تستفيد منها الدولة المعتدى عليها لتفادي وقوع الضرر من خلال اتصالها بالدولة المعتدية للكف عن هذا التصرف، فلا يمكن للاعتداء على وفق هذا المعيار أن يرقى إلى كونه استخداماً للقوة، إذا ثبت أن الدولة التي تمت مهاجمتها قد فرطت بأي فترة زمنية كان يمكن أن تستفاد منها لتجنب الضرر، وبعبارة أخرى أن الخطر الآني أو الحال هو الذي سوف يقع لا محالة ، دون

---

(1) Micheal N.Schmitt, cyber operations, and the Jud Ad Bellum Revisited, Published by Villanova University Charles widger School of Law Digital Repository, Villanova Law. Review, Vol.(56), issue.(3), Unitedstate , 2011, p.587.

(2) ICJ, ReP.2003, para, 51, 72.

(3) Jeffry carr, op.cit, p.60.

استطاعة الدولة المعتدى عليها القيام بدرء هذا الخطر بأي وسيلة كانت[١]. فعواقب الهجوم التي تظهر للعلن بعد فترة وجيزة من الهجوم، تجعل من البساطة تكييف هذا الهجوم على انه استخدام للقوة بالمقارنة مع وسائل الإكراه ومختلف القوى التي تظهر آثارها بطيئة بصورة تدريجية[٢]. أن شرط الفورية ينسجم مع اختبار كارولاين (caroline test) ، والذي يعد تعبير صادق لفكرة الآنية أو الفورية، ومن الممكن الاستفادة منه في سياق الدفاع عن النفس ضد خطر محتمل الوقوع ، إذ يحق للدولة المعتدى عليها بموجبه أن تدافع عن نفسها ضد هجوم عسكري وشيك الوقوع، ولكنه فوري لا يترك أي خيار امام الدولة لغرض التداول[٣].

وبتحليل ما تقدم نجد أن لجنة الخبراء في دليل تالين لم تناقش الحالة التي يمكن فيها للدولة المعتدى عليها من جراء هذا الهجوم أن تكون بأستطاعتها منع هذا الضرر الناشئ عن الهجوم، أو على أقل تقدير أن تحد من آثاره لوحدها، من دون حاجتها للإتصال بالدولة التي بادرت بالهجوم، إلا أنه على الرغم من ذلك يمكننا أن نستنتج بأن إغفال هذهِ الحالة من قبل اللجنة قد جاء بحسن نية مبني على اساس أنها حالة مفترضة ولا داعي لمناقشتها ، على اعتبار أن درء الضرر أو الحد منه باستخدام أي وسيلة ضد الهجوم هي اصلاً تمثل جوهر هذا المعيار.

---

(1) See: Daniel Bathlehem . principles Relevent to the scope of self- De fence Against imminemt of Actual Armed Attack by Non state Actors, American journal of international law , vol. (106), 769, 2012.

(2) Micheal N.Schmitt, Thoughts on A NorMative Frame work, op. cit, p.914.

(٣) يشار بهذا الصدد هذا المبدأ الذي ترشح عن حادثة كارولاين بين المملكة المتحدة والولايات المتحدة الامريكية قد تأكد عرفاً دولياً بشأن استخدام حق الدفاع عن النفس ضد أي خطر محتمل الوقوع ، للمزيد ينظر بهذا الصدد :

Larry May, war crimes and just war, Cambridge University press, 2007, p.206.

ثالثاً: النهج القائم على المسؤولية المتشددة (strict Liability).

يرى انصـــار هذا الاتجاه أن أي هجوم معلوماتي ضـــد البنية التحتية الحيوية للدولة هو اسـتخدام للقوة ويكون بمثابة هجوم مسـلح يتيح للدولة المعتدى عليها الدفاع عن نفسـها ضـد أي هجمات تسبب ضرراً لها[١] ، إذ يتم التعامل بصورة تلقائية مع الهجمات المعلوماتية نظراً للعواقب التدميرية التي تنجم عن تعطيل أنظمة البنى التحتية للدولة المتضـررة، حيث إن أي تعامل تلقائي مع هذهِ الهجمات المعلوماتية يكون الهدف منه تبرير الدفاع الاسـتباقي عن النفس قبل أن يحدث أي ضـرراً فعلياً، نتيجة للسـرعة التي يمكن من خلالها النفاذ للحاسـوب ثم بعد ذلك الإنتقال إلى هجوم تدميري ضـــد البنية الحيوية ، إذ بمجرد حدوث ثغرة يحدث تهديد وشـــيك يكون قادراً على انتاج ضـرر شـديد المدى والكثافة عبر فترة زمنية وجيزة. الأمر الذي يسـتدعي الدفاع عن النفس بصورة استباقية.[٢]

وعلى الرغم من أن انصـــار هذا الاتجاه يرون فيه هو النموذج الأنســب لتكييف الهجمات المعلوماتية وذلك للطبيعة التدميرية لهذهِ الهجمات، إلا أنه لاقى عدة انتقادات منها على ســـبيل المثال ، عشوائية الهجمات المعلوماتية، وعدم دقتها في حالات متعددة.[٣]

نسـتنتج من خلال ما تقدم ذكره وعند تحليل آراء الاتجاهات الفقهية، نجد أن معيار الحجم والآثار هو أسب المعايير التي يمكن أن يتم اللجوء إليه عند تكييف هذهِ الهجمات المعلوماتية، إذ أن تصنيف الهجوم على اساس حجم وآثار تلك الهجمات على الدولة المعتدى عليها، سواء كانت تلك الهجمات هي تقليدية أم جاءت في اطار الهجمات المعلوماتية ، فكلاهما يترك آثار تتفاوت بشدتها على الدولة التي تمت مهاجمتها.

---

(1) Michael Gervais, cyber Attack and The law of war, Berkeley journal of international law, vol.(30), Issue 2, 2012, p.538.

(2) See walter Gary sharpsr, cyber space and the use of force , Ageis Research corp, 1999, p.129-131.

(3) Anderew Moore, stuxnet and Article 2(4)'s prohibition Againts the use of force : customary law and potential Models, Naval law Review, vol, 64, 2015,p.4.

المطلب الثاني

التكييف القانوني للهجمات المعلوماتية في اطار قانون النزاعات المسلحة

إن مسألة التكييف القانوني للهجمات المعلوماتية في سياق قانون النزاعات المسلحة هي محل نظر بين المختصين في الشأن القانوني، فمنهم من يرى هذهِ الهجمات هي بمثابة نزاع مسلح في حال توافر شروطه، التي أشارت إليها الصكوك الدولية، وذهب أتجاه آخر منهم للبحث عن مدى إمكانية تطويع مبادئ وقواعد القانون الدولي الإنساني وتطبيقها على الهجمات المعلوماتية.

إلا أن ذلك يثير العديد من المشاكل القانونية عند تناول البحث في تكييف هذهِ الهجمات، إذ إن قواعد القانون الدولي الإنساني المتمثلة بأتفاقيتي لاهاي (١٨٩٩، ١٩٠٧) وإتفاقيات جنيف الأربع لعام (١٩٤٩) والبروتوكولان الملحقة بهما لعام ١٩٧٧، لم تتضمن مسألة تنظيم الهجمات المعلوماتية في حينها، إذ إن تلك الهجمات لم يكن لها وجود عند صدور هذهِ الأتفاقيات الدولية، ولكن هذا لا يعني إن يتم التسليم لخطورة الهجمات المعلوماتية وأثرها على السلم والأمن الدوليين، حيث حاول بعض الأكاديميين والخبراء الدوليين، تنظيم هذهِ الهجمات في سياق قواعد ومبادئ القانون الدولي الإنساني وإمكانية توظيفها وانطباقها عليها، وهنا يمكن أن تتسائل: هل يمكن تكييف الهجمات المعلوماتية على أنها نزاع مسلح؟ وما مدى إمكانية انطباق قواعد ومبادئ القانون الدولي الإنساني على الهجمات المعلوماتية؟ للأجابة عن هذه التساؤلات، سنبحث هذه المواضيع في فرعين، نتطرق في الأول إلى تكييف الهجمات المعلوماتية كنزاع مسلح أو أعمال عدائية في ضوء القانون الدولي الإنساني، أما الثاني سنكرسه لمدى خضوع الهجمات المعلوماتية لقواعد ومبادئ القانون الدولي الإنساني.

الفرع الأول

تكييف الهجمات المعلوماتية كنزاع مسلح أو أعمال عدائية في ضوء القانون الدولي الإنساني

أولاً: تكيفها كنزاع مسلح دولي وغير دولي:

ظهر مصطلح النزاعات المسلحة في اتفاقيات جنيف الأربعة المبرمة عام ١٩٤٩، والتي تتعلق بحماية الاشخاص غير المشاركين في القتال اثناء النزاعات المسلحة ويؤكد فقهاء القانون الدولي على إلزامية قواعدها العرفية. وصنفت هذه الاتفاقيات النزاعات المسلحة إلى صنفين ، نزاع مسلح دولي ، ونزاع مسلح غير دولي كما مبين في ادناه :-

١- النزاع المسلح الدولي:

باستقراء نص المادة الثانية المشتركة لاتفاقيات جنيف الاربع لعام ١٩٤٩[١] ، والمادة الاولى من البروتوكول الاضافي الاول الملحق بهما لعام ١٩٧٧، نجد أننا نكون أمام نزاع مسلح دولي في حالات ثلاث:

أ- حالة إستخدام القوة المسلحة في العلاقات الدولية .

ب- حالة الإحتلال .

جـ- حالة قيام مقاومة مسلحة في جانب حركات التحرير[٢].

ومن الجدير بالذكر ان اتفاقيات جنيف الاربع لعام ١٩٤٩ ، استبدلت مصطلح " الحرب " الذي كان يستخدم في اتفاقيات لاهاي بمصطلح " النزاع المسلح " من اجل توسيع النطاق المادي

---

[١] انظر المادة (الثانية) المشتركة لاتفاقيات جنيف الاربع لعام ١٩٤٩ : (علاوة على الاحكام التي تسري في وقت السلم ، تنطبق هذه الاتفاقية في حالة الحرب المعلنة أو أي اشتباك مسلح أخر ينشب بين طرفين أو اكثر من الاطراف السامية المتعاقدة ، حتى لو لم يعترف احدهما بحالة الحرب .
تنطبق هذه الاتفاقية ايضاً في جميع حالات الاحتلال الجزئي أو الكلي لإقليم أحد الاطراف السامية المتعاقدة ، حتى لو لم يواجه هذ الاحتلال مقاومة مسلحة).

[٢] الفقرة رابعاً من المادة الاولى من البروتوكول الاضافي الاول لاتفاقيات جنيف الاربع المتعلق بحماية ضحايا النزاعات المسلحة الدولية لعام ١٩٧٧ : (النزاعات المسلحة التي تناضل بها الشعوب ضد التسلط الاستعماري والاحتلال الاجنبي ، وضد الانظمة العنصرية وذلك في ممارستها لحق الشعوب في تقرير المصير).

لتطبيق الاتفاقيات وجعل القانون الدولي الإنساني قابلاً للتطبيق وشاملاً لحالات اخرى وحسب تقييمه لها ، فعلى سبيل المثال لكي نكون امام نزاع مسلح دولي اشترطت الدائرة الاستئنافية للمحكمة الجنائية الدولية ليوغسلافيا السابقة في قضية تاديش لعام ١٩٩٥، توافر عنصرين هما[١]:

أ) ان يكون النزاع بيت دولتين على الاقل .

ب) لجوئهما إلى استخدام القوة المسلحة ، أي اللجوء إلى الاعمال العدائية الحربية ضد دولة اخرى ، وهذا ما تبناه دليل تالين ، إذ نص على انه " يوجد نزاع مسلح دولي عندما تكون هناك اعمال عدائية ، والتي تشمل أو تقتصر على العمليات المعلوماتية ، التي تحدث بين دولتين او اكثر " ، والمقصود بالأعمال العدائية التطبيق الجماعي لوسائل واساليب (الحرب) فالقانون الدولي الإنساني يعتمد بالدرجة الاساس في تطبيقه على تقييم الحالة الواقعية وليس على ادراك حالة النزاع المسلح من جانب الاطراف فيه [٢]، ويقصد بالنزاع المسلح الدولي هو ((حالة اللجوء إلى العنف المسلح بين دولتين أو اكثر ، سواء كان بإعلان سابق أو بدونه ، كما وتطبق الاطراف المتعاقدة المتحاربة أحكام القانون الدولي الإنساني سواء أعترف بحالة قيام نزاع مسلح أو لم يعترف به، كما تطبق في حالة الإحتلال اتفاقيات جنيف الأربع لعام ١٩٤٩)).[٣].

ومن نافلة القول، أن الهجمات على شبكات الحاسوب التي تقوم بتنفيذها دولة معينة كان تكون من قبل قواتها المسلحة، أو تلك التي تشن من قبل هيئات الدولة كالوكالات الاستخبارية أو الجهات المختصة بفرض القانون كقوات الشرطة مثلاً ، جميعها تعد كافية لتحقيق المعيار الدولي للنزاع وهذا ما اكدته المحكمة الجنائية الدولية ليوغوسلافيا السابقة في قضية تاديش عام ١٩٩٥

---

(1) Micheal N.Schmitt, classification of cyber conflict, Journal of Conflict and Security Law, Vol.(17), No.2, 2012, p.245-249.

[٢]كوردولا دوريجي ، لا تقترب من حدود فضائي الالكتروني : الحرب الالكترونية والقانون الدولي الانساني وحماية المدنيين ، المجلة الدولية للصليب الاحمر ، م (٩٤) جنيف، ٢٠١٢ ، ص٥٤٣ .

[٣] د. عامر الزمالي ، القانون الدولي الانساني وتطور محتواه وتحديات النزاعات المعاصرة (مدخل في القانون الدولي الانساني والرقابة على استخدام الاسلحة) ، تونس ، من دون سنة طبع ، ص٢١٨ – ٢١٩ .

على ان " الافراد الذين يعملون في اطار القوات المسلحة التابعة لدولة معينة أو بالارتباط معها ، تعد بمثابة احدى هيئات الدولة "[١] وبالتالي فأن قيامها بشـن هجمات على شـبكات الحاسـوب ينسب إلى الدولة المعنية باعتباره صادراً عن احدى هيئاتها.

٢- النزاع المسلح غير الدولي

تم التأكيد على النزاع المسلح غير الدولي من خلال نص المادة الثالثة المشتركة لاتفاقيات جنيف الاربع لعام ١٩٤٩ على انه : " في حالة قيام نزاع مسـلح ليس له طابع دولي في اراضـي احد الاطراف السامية المتعاقدة ..." [٢].

اما البروتوكول الاضـافي الثاني لعام ١٩٧٧ فقد حدد هذا البروتوكول النطاق المادي لتطبيقه في مادته الأولى التي جاء فيها :" يسـري هذا اللحق " البروتوكول " الذي يطور ويكمل المادة الثالثة المشتركة بين اتفاقيات جنيف لعام ١٩٤٩ دون أن يعدل من الشروط الراهنة لتطبيقها على جميع المنازعات المسـلحة التي لا تشـملها المادة الاولى من اللحق " البروتوكول " ... المتعلق بحماية ضـحايا النزاعات الدولية المسلحة .... التي تدور على إقليم احد الأطراف السامية المتعاقدة بين قواته المسلحة وقوات مسلحة منشقة أو جماعات نظامية مسلحة اخرى تمارس تحت قيادة مسؤولة على جزء من إقليمه من السـيطرة ما يمكنها من القيام بعمليات عسـكرية متواصـلة ومنسـقة ، وتستطيع تنفيذ هذه البروتوكول "[٣].

وحتى نستطيع تحديد ان يكون نزاعاً غير ذي طابع دولي يجب توافر شرطين هما :

أ- اشـترطت المادة الثالثة المشـتركة عمومية حجم التمرد وانتشـاره على نطاق جغرافي واسـع ، وضرورة إستيفاء مقتضيات التنظيم بوجود قيادة مسؤولة .

---

(1) ICTY, Tadic, cases, No.1 t-94-I-A, 1999, para, 144.

[٢] تنظر المادة الثالثة المشتركة لاتفاقيات الاربع لعام ١٩٤٩ .

[٣] د. عامر الزمالي ، المدخل إلى القانون الدولي الانساني ، مكتبة دار السلام القانونية ، النجف ، ط٦ ، ٢٠١٦ ، ص٤٥ .

ب- كما اشترط البروتوكول الإضافي الثاني شرطاً اخر هو شرط الرقابة الإقليمية ، من خلال النص عليه بعبارة " وتمارس تحت قيادة مسؤولة على جزء من إقليمه من السيطرة ما يمكنها من القيام بعمليات عسكرية ومتواصلة " .

وفي سياق الهجمات المعلوماتية فأن المجموعات المسلحة المنظمة معلوماتياً يمكن ان تطبق نفس المعايير الخاصة باستخدام العنف الحركي بموجب القانون الدولي الإنساني ، اذ ما تطلب الموقف تقدير وجود نزاع مسلح غير دولي ينطوي على هجمات معلوماتية ، أي يشترط في هذه الجماعة المسلحة أن تكون على قدر من التنظيم ولديها القابلية على الإنخراط في عنف شديد بما فيه الكفاية[١]. فالنزاع المسلح غير الدولي يتحقق بوجود أعمال عنف مسلحة متواصلة تشتمل على الهجمات المعلوماتية أو تقتصر عليها ضمن القوات المسلحة الحكومية والقوات التابعة لمجموعة أو اكثر من المجموعات المسلحة ، او بين تلك المجموعات ، على شرط ان تصل المواجهات إلى الحدود الدنيا من الكثافة وان تكون الاطراف المنخرطة في النزاع تتحلى بدرجة معينة من التنظيم[٢].

أما في سياق التنظيم المطلوب في الهجمات المعلوماتية، فأن الأمر ليس بهذه السهولة ولا يخلو من التعقيد، إذ إن من يقوم بتنفيذ هذهِ الهجمات يفتقرون إلى التواجد المادي والمشكلة الأشد تعقيداً التي تواجه مسألة لتنظيم في إطار الهجمات المعلوماتية وبحسب غالبية الخبراء في دليل تالين، تتمثل بقيام مجموعة من الأفراد الذين يعملون بصورة جماعية وغير منسقة، أي بمعنى أن يكون لهم غرض مشترك كقيامهم بأختراق الموقع الإلكتروني (website) الذي يضم الوسائل المعلوماتية والأهداف القابلة للأختراق، إلا أن تلك المجموعة لا تنظم هجماتها على ضوء

---

[١] اللجنة الدولية للصليب الاحمر ، تعليقها على احكام المادة الثالثة المشتركة ، منشورات اللجنة الدولية للصليب الاحمر ، ص٤١ ، متاح على الموقع الالكتروني https//:cut.lu/akp3hqm. تاريخ الزيارة ٤ / ١٢ / ٢٠٢١ .

[2]Tallinn Manual, op.cit , Rule (23), p76.

المعايير المطلوبة في النزاع غير الدولي، وبالتالي فهم لا ينطبق عليهم وصف المجموعة المسلحة المنظمة التي يمكن من خلالها تصنيف الوضع على أنه نزاع غير دولي[١].

ومن خلال ما تقدم نستطيع القول إنه إذا ما أفضت الهجمات المعلوماتية إلى نفس العواقب التي تؤدي إليها العمليات الحركية والتي تستخدمها الجماعات المسلحة التي تنخرط في عنف شديد بما فيه الكفاية ، كما هو الحال مثلاً عند فتح بوابات السدود أو التسبب في اصطدام الطائرات أو القطارات ، فأنها تصل إلى درجة الحدة اللازمة لإعتبار الجماعات المسلحة المنظمة افتراضياً طرفا في نزاع مسلح غير دولي ، أما اذا كانت تقتصر فقط على اعاقة وظائف الانترنت أو استغلال الشبكات أو سرقة البيانات أو خدمتها او اتلافها ، فهي بهذه الحالة لا تصل إلى درجة حده العنف التي يتطلب توفرها في القانون الدولي الإنساني ، وبالتالي لا يمكن عدها طرفاً في النزاع المسلح غير الدولي[٢].

أما بالنسبة للأقليم الذي يدور عليه النزاع المسلح غير الدولي، والذي تستخدمه الجماعات المنظمة أو المنشقة أو المراد من خلاله إمكانية تطبيق قواعد القانون الدولي الإنساني على الهجمات المعلوماتية، فتجدر الإشارة إلى أن الفضاء المعلوماتي لا يمكن أن يكون منطقة غير خاضعة للقانون، وأن كان من غير الممكن وضع حدود جغرافية لهذهِ الإنتهاكات، ووفقاً للقواعد التقليدية للقانون الدولي الإنساني، يلزم من خلالها تحديد النطاق الجغرافي ليكون ضمن حدود الدولة الذي حدث النزاع الداخلي فيها، يكون من غير الممكن تطبيق هذهِ القواعد على هذا النوع من النزاعات، على الرغم من إن بعض الخبراء في دليل تالين يرون أنه من الممكن ان يمتد النزاع غير الدولي إلى خارج حدود الدولة الإقليمية، إذ إن قانون النزاعات المسلحة ينطبق على جميع الآثار المرتبطة بالنزاع المسلح ومنها على الأنشطة التي تجري في سياق نزاع المسلح، فقد تستغل بعض الجماعات المسلحة المنظمة المنشقة عن الدولة ضعف التشريعات المتعلقة بمعالجة انتهاكات القانون الدولي الإنساني التي تحدث نتيجة لعمليات معلوماتية ، فتنفذ هجوماً

---

[1]Micheal N.Schmitt, classification of cyber conflict, op.cit p.256.

[٢] اللجنة الدولية للصليب الاحمر ، تعليق اللجنة الدولية على احكام المادة الثالثة المشتركة ، مصدر سابق،ص٤٢ .

معلوماتياً على الدولة من خارج إقليمها يؤدي إلى حدوث اضـرار وخسـائر للمدنيين أو الممتلكات المدنية ، وفي هذه الحالة تكون امام انتهاك للقواعد القانون الدولي الإنسـاني في نزاع مسـلح غير دولي عابر للحدود الاقليمية[١].

وقد اشار دليل تالين للحرب المعلوماتية في القاعدة (٢١) منه على خضوع الهجمات المعلوماتية للقيود الجغرافية التي تفرضـــها قواعد القانون الدولي ذات الصـــلة والتي تكون قابلة للتطبيق اثناء النزاعات المسلحة الدولية وغير الدولية [٢]. وهذا يدل على ان قانون النزاع المسلح يحدد المجال الجغرافي الذي يتيح تنفيذ الهجمات المعلوماتية من خلاله.

وبالتالي نعتقد أن هذه الهجمات يمكن القيام بتنفيذها من داخل إقليم احد اطراف النزاع باسـتهداف المجال الجغرافي ولها القدرة على احداث الآثار التي ترمي إلى تحقيقها فيه ، وخلاف ذلك فأن العمليات التي تشن على شبكات الحاسوب تعد محظورة خارج القيود الجغرافية[٣].

ثانياً: تكييف الهجمات المعلوماتية كأعمال عدائية أو مشاركة مباشرة فيها

يقوم مفهوم المشـــاركة المباشـــرة في العمليات العدائية على عنصـــرين رئيســـيين هما " عنصـــر المشـــاركة المباشـــرة " وعنصـــر الاعمال العدائية ، ففي الوقت الذي يشـــير العنصـــر الأول إلى مساهمة فرد من الأفراد في هذه العمليات ، فان العنصر الثاني يشير إلى اللجوء الجماعي لطرف من اطراف النزاع إلى اتباع وسائل من شأنها ان تلحق ضرراً بالطرف الاخر [٤].

---

[١] د. سلافة طارق الشعلان ، تكييف استخدام الحرب الالكترونية في النزاعات المسلحة وفقاً للقانون الدولي الإنساني ، مجلة الكوفة للعلوم القانونية والسياسية، كلية القانون، جامعة الكوفة ، م (٩) ، ع (٢٦) ، ٢٠١٦ ، ص١٣٦ .

[2]Tallinn Manual, op.cit , rule(21).

[٣] سراب ثامر احمد ، مصدر سابق ، ص١٥٦ .

[٤] ميلزر نيلس ، الدليل التفسيري لمفهوم المشاركة المباشرة في العمليات العدائية بموجب القانون الدولي الإنساني ، اللجنة الدولية للصليب الاحمر ، ط١ ، القاهرة ، ٢٠١٠ ، ص٤٢ .

اما في اطار الاتفاقيات الدولية ذات الصلة بمفهوم المشاركة المباشرة في الاعمال العدائية فأنها قدمت وصفاً لهذا المفهوم على انه سلوك الذي اذا قام به مدنيون فأنه يستلزم تعليق الحماية المقررة لهم من الهجوم المباشر [١].

تضمنت قواعد القانون الدولي الإنساني المطبق في النزاعات المسلحة على تمتع المدنيون بحصانة من الهجمات ما لم يقوموا بدور مباشر في الاعمال العدائية على مدى الوقت الذي يقومون خلاله بهذا الدور ، إلا أنه في ذات الوقت لا يوجد نص في المعاهدات او القانون الدولي العرفي يحظر على المدنيين من المشاركة في العمليات العدائية ، فضلاً عن غياب النص القانوني الذي يعرفّ المشاركة المباشرة في العمليات العدائية ، لكن إذا ما قاموا المدنيين بذلك فأنهم يفقدون حصانتهم طوال هذه المشاركة المباشرة ، وعلى وفق اراء فقهاء القانون الدولي فان ضرورة الاحتفاظ بالصفة المدنية للمدني ، حتى لو شارك في العمليات العدائية، لان استهدافه يؤدي إلى انتهاك مبدأ التمييز احد اهم المبادئ التي يرتكز عليها القانون الدولي الإنساني ، ومن الممكن التعامل مع كل حالة يشارك فيها المدنيين في شن هجمات معلوماتية على انها مشاركة مباشرة على ضوء نوع المشاركة المباشرة ودرجة خطورتها في كل حالة ومقدار حجم الضرر الذي نجم عنها [٢].

وعلى وفق ما جاء في الموقف الرسمي للجنة الدولية للصليب الاحمر ، فان مفهوم المشاركة المباشرة في الاعمال العدائية ، يعد اوسع من مفهوم الهجوم ولا يشمل فقط الحاق الموت او الاصابة او التدمير ، وانما يتعداه ليشمل فعل معين من المحتمل ان يؤثر بصورة سلبية على العمليات العسكرية لأحد طرفي النزاع والذي يسمى (عتبة الضرر) ، وكذلك لتحديد العلاقة السببية بين عملية محددة والضرر الناجم عنها يعتمد اساساً كونها مباشرة أو غير مباشرة في جوهرها ، وحول ما اذا كانت تبنى على قياس قدرة طرف نزاع على الحاق الضرر بالخصم (غير مباشر) وما اذا كانت جزء لا يتجزأ (من عملية تستخدم هذه القدرة على الحاق الضرر

---

[١]الفقرة (٣) من المادة (٥١) من البروتوكول الاضافي الاول لعام ١٩٧٧ ، و الفقرة (٣) من المادة (١٣) من البروتوكول الاضافي الثاني لعام ١٩٧٧.

[٢] د. سلافة طارق الشعلان ، مصدر سابق ، ص١٣٧ – ١٣٨ .

الفعلي للخصم مباشراً)[١]. ومن الصور التي يمكن ان تتحقق بها المشاركة المباشرة من عدمها في سياق هجوم معلوماتي ، هي حالة قيام المدني بالإتفاق مع أي طرف في النزاع ، لغرض القيام بتصميم شفرات معلوماتية أو أي عمل يدخل ضمن الهجمات المعلوماتية ، كما حدث فعلا عند قيام الولايات المتحدة الامريكية باستخدام المدنيين لقيادة الطائرات المسيرة لغرض تنفيذ هجمات تستهدف أشخاص ومواقع ، أو تشغيل متعاقدين عسكريين أو أمنيين في بلدان مختلفة مثل افغانستان والعراق[٢] ، ولكن المدني الذي يقوم باعمال صيانه لشبكة الحواسيب العائدة للقوات العسكرية لا يعد مشاركاً في العملية العسكرية ، على خلاف المتعاقد الذي يساهم بعمل عدائي بواسطة الهجمات المعلوماتية فان يعد مشاركاً مباشراً في العمليات العسكرية[٣]، والسؤال المطروح بهذا الصدد هل يمكن تطويع شروط المشاركة المباشرة في الاعمال العدائية على الهجمات المعلوماتية التي يقوم بها المدنيين في اطار نزاع مسلح ؟

من اجل وصف عمل محدد يقوم به شخص مدني بانه يشكل مشاركة مباشرة في عمل عدائي يجب أن تتوافر فيه الشروط الثلاثة التي اوردها دليل اللجنة الدولية للصليب الأحمر ، وهذه الشروط يتطلبها القانون الدولي الانساني لإضفاء وصف المشاركة المباشرة على شخص من المدنيين وهذهِ الشروط هي: حد حصول الضرر ، والارتباط بالعمل الحربي ، والعلاقة السببية بينهما ، وفي سياق الهجمات المعلوماتية فان الاعمال التحضيرية المهيئة لتنفيذها غالبا مايتم تصميم وبرمجة الأسلحة المعلوماتية بصورة خاصة لشنها على اهداف محددة سلفاً ، وبالتالي يجعل من جميع هذه الافعال بصورة واضحة مشاركة مباشرة في العمليات المعلوماتية ، التي يترتب عليها فقدان الحماية من الهجمات المباشرة ، علاوة على العقوبات التي يواجهها المدني

---

(1) Nils melzer , inter pretive guidance on the notion of direct participation inhostilities, under international human hitarian law , TCRC, 2009 , p47- 63 .

(٢) ميلزر نيلس، مصدر سابق ، ص٣٩ .

(3)Emily Crawford, virtual battlegrounds,dirct participation cyber war fare , Sydney law school , legal studies research paper , 2012, p.18

المشــارك مشــاركة مباشــرة في الاعمال العدائية المعلوماتية بموجب التشــريعات الوطنية لقيامه بافعال تصميم وبرمجة الفيروسات والاسلحة المعلوماتية [١].

وتعد حماية الصــفة المدنية ذات اهمية خاصــة ، لان من شــأنها الحد من الاضــرار التي تلحق بالمدنيين ، ولكن دائماً ما تكون هناك صــعوبة الفصــل بين ما اذا كان المشــارك في الاعمال العدائية هو مدنياً أم عسكرياً ، فقد يمتلك الفرد خبرة باستخدام الحاسوب ، وقد يشارك في الهجوم ، ولكنه لا يحمل صـفة عسـكرية رسـمية وهذا ما يُفقد ذلك المدني صـفته المدنية ، والحماية من الهجوم ، وبالتالي يستلزم معرفة من المتسبب في إحداث الضرر أو من أستخدام هجمات الفضاء المعلوماتي ، وقد اجمع عدد من الفقهاء على ان اسـتخدام الوسـائل المعلوماتية كوسـلية لهجمات شبكة الحاسوب يمكن اعتباره مشاركة مباشرة في الاعمال العدائية إلا انه لا يعد مشاركة مباشرة في القتال إلاّ اذا نتج عنه الموت أو الجرح أو ضــرر طبيعي ، ولكن أســتخدام أنظمة التســلح ووسائل الإتصالات والشبكات المعلوماتية في العمليات العسكرية يمكن عدها مشاركة مباشرة في الأعمال العدائية[٢].

وينبغي الاشــارة إلى انه بحســب ما جاء بدليل تالين فان التصــرفات التي تعد مرتبطة بالعمل العدائي في ســياق الهجمات المعلوماتية تعتبر اعمال عدائية معلوماتية مثال على ذلك، الهجوم على منظومة القيادة والسـيطرة الخاصـة بإدارة العمليات بصـورة مباشـرة لاحد اطراف النزاع حتى في حال حصول أي دعم ومنفعة لطرف النزاع الاخر [٣]. وتأسياً على ماتقدم ذكره بشأن المشاركة

---

[١] د. حيدر ادهم الطائي وعلي محمد كاظم الموسوي ، المشاركة المباشرة للهبة الجماعية في الهجمات السيبرانيه ، مجلة كلية الحقوق ، جامعة النهرين ، بغداد ، ٢٠١٩ ، ص٢٧-٤٢

[٢] د. عادل عبد الصادق ، اسلحة الفضاء الالكتروني في ضوء القانون الدولي الانساني ، مصدر سابق ، ص١٠٢ – ١٠٣.

[3] Tallinn manual ,op.cit, comment (4) on rule (35) .

المباشـــرة في الاعمال العدائية في إطار الهجمات المعلوماتية ، نســـتطيع القول ان أي عمليات عدائية تسـبب فيها احد طرفي النزاع وتنسـب اليه وحصـل من خلالها ايذاء الخصـم عن طريق التسبب مباشرة في إحداث وفاة أو الاصـابة أو الحاق دمار أو قصـد الاضـرار بصـورة مباشـرة بالاهداف العسكرية ، كل هذه الافعال تندرج تحت مفهوم المشاركة المباشرة في الاعمال العدائية المعلوماتية ، وبالتالي فهي تخضـــع لجميع القيود الحاكمة لســير الاعمال العدائية التي يتطلبها القانون الدولي الانســـاني ، وعليه أن قيام المدنيين بهكذا عمليات فانهم ســوف يفقدون حقهم في الحماية المقررة لهم من جراء الهجمات التي يتعرضون لها .

الفرع الثاني

مدى خضوع الهجمات المعلوماتية لقواعد ومبادئ قانون الدولي الانساني

إن توظيف الهجمات المعلوماتية في النزاع المســـلح كما ورد في تقرير اللجنة الدولية للصـــليب الأحمر عام ٢٠١١، يشـترط فيه أن يتلائم مع جميع مبادئ القانون الدولي الإنســاني وقواعده وكما هو معلوم مع أي وســيلة أو ســـلاح أو أســلوب حرب آخر، ســواء كان قديماً أم حديثاً[١]، إذ إن حق الأطراف المتنازعة في اختيار وسـائل القتال واسـاليبه هو ليس حقاً مطلقاً لا تقيده أي قيود.[٢] وهذا ما اكدته محكمة العدل الدولية بقولها إن: "مبادئ وقواعد القانون الدولي الإنســـاني المنطبق في النزاع المســـلح، تنطبق على جميع أشـــكال الحروب وعلى جميع أنواع الأسلحة .. بما في ذلك تلك المستقبلية".[٣]

---

[١] اللجنة الدولية للصليب الأحمر، القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، تقرير صادر عنها في تشرين الأول، اكتوبر ٢٠١١، متاح عبر الموقع الالكتروني، تاريخ الزيارة ٢٠٢١/١٠/١٤.

[٢] للمزيد ينظر: نص المادة (٢٢) من اللائحة ذات الصـــلة بقوانين وأعراف الحرب البرية، لاهاي ١٩٠٧والمادة (١/٣٥) من البروتوكول الإضافي الأول لإتفاقيات جنيف لعام ١٩٧٧.

[3] ICJ, Nuclear weapons advisory opinion, legality of therats or use of Nuclear weapons, para, (8 july)1996, p. 86.

علاوة على ذلك إن فريق الخبراء في الأمم المتحدة جاء رأيهم متسقاً مع قرار محكمة العدل الدولية آنف الذكر، إذ يرون إمكانية انطباق المبادئ القانونية المستقرة كمبادئ الضرورة العسكرية والتناسب في استخدام القوة والتمييز على الهجمات المعلوماتية اثناء النزاع المسلح .[١]

ومن أجل دراســـة توظيف أهم مبادئ القانون الدولي الإنســـاني وقواعده على الهجمات المعلوماتية لا بد من الخوض في تفاصيل هذهِ المبادئ ومدى إنطباقها على الهجمات المعلوماتية أثناء النزاع المسلح وعلى النحو الآتي:

أولاً: الهجمات المعلوماتية في إطار مبدأ الضرورة العسكرية

مبدأ الضـرورة العسكرية هو من المبادئ الأساسية الحاكمة لنظام سير الأعمال العدائية، كونه يهدف إلى تخفيف الغرض من العملية العسـكرية بأقل الاضـرار، إذ اثار هذا المبدأ مسـألة خلافية بين فقهاء القانون الدولي فمنهم من يجد في الضــرورة العســكرية بأنها أحد اركان النزاع المسلح، وهناك ضرورة تدفع لشن الحرب العادلة هي الضرورة العسكرية، وقد ساند هذا الاتجاه الفقيه دي فورتس، إذ ذهب بالقول: " أن الضــرورة العســكرية هي من العناصــر الرئيســية في العمليات القتالية" [٢]، وأيده في ذلك الفقيه هنري ميروفتز (Henri Meyrowitz)، حيث أقام هذا الاتجاه حجته على حيثيات مؤتمر بروكسل للسلام عام ١٨٧٤ الذي علق الوفد الروسي فيه

---

[١] ينظر بهذا الصـدد: تقرير الخبراء الحكوميين بشـأن التطورات الحاصـلة في ميدان المعلومات والاتصـالات السـلكية واللاسـلكية في سـياق الأمن الدولي، المرقم A/٧٠/١٧٤ في ٢٢ تموز ٢٠١٥، متاح عبر الموقع الالكتروني: تاريخ الزيارة ٢٠٢١/١١/٣

www.un.org/ga/search/viewdoc.asp/symbol=A/70/174,para.28.

[2] Rebaca Grant, In " Determining Millitary Necessity and proportionality, the commanders judgment is more critical than even, in search of law ful target's", Air force Magazine, feb, 2003, p.40.

قائلاً:" إن الضـــرورة العســـكرية تنعقد متى ما عقدت النية على تحقيق الهدف العســـكري المشروع".[١]

ولكن هناك فريق أخر من الفقهاء كانت لهم وجهة نظر مغايره لآراء الفريق المؤيد لفكرة الضرورة العسكرية باعتبارها ركن من أركان النزاع المسلح ، إذ يرون إن الضرورة العسكرية هي إستثناء من الأصل، ولا يمكن اللجوء إليها إلا وفق حالات وظروف معينة على أن يتم إستخدامها بناءً على شروط محددة[٢]، حيث جاء مبدأ الضرورة العسكرية ليشكل أحد المبادئ التفسيرية لحقوق المقاتلين وواجباتهم ضمن معايير محددة لأحكام القانون الدولي الإنساني.[٣]

وفي إطار الهجمات المعلوماتية ، يتوجب أن تكون الهجمات الموجهة إلى العدو والتي يتطلب تدمير معداته وممتلكاته الغرض منها هو تحقيق ميزة عســـكرية محددة، وأن لا يتعدى هدف هذا الهجوم تحقيق تلك الميزة العسكرية وإلا عدّ ذلك إنتهاكاً لقواعد القانون الدولي الإنساني ومبادئه[٤].

وفي ذات السياق اشارة المادة (٥٢) من البروتوكول الاضافي الأول لعام ١٩٧٧ في الفقرة الثانية إلى " تقتصـــر الهجمات على الأهداف العســـكرية فحســـب.. والتي يحقق تدميرها التام أو الجزئي أو الاستيلاء عليها أو تعطيلها ، في الظروف السائدة حينذاك ميزة عسكرية اكيدة".

أما دليل تالين للقانون الدولي المطبق على الهجمات المعلوماتية فقد جاء موقفه ضـــعيفاً بخصـوص مبدأ الضـرورة العسـكرية، إذ أورد قواعد بسـيطة بشـأن مبدأ الضـرورة العسـكرية في القاعدة (٥٦) من هذا الدليل، حيث اشـــار دليل تالين إلى:" أنه في الحالات التي يكون الخيار

---

(1) Henri Meyrowitz, " the priniciple of super fluous injury or unnecessary suffering- From declaration of st peters burg of 1868 to Additional protocol of 1977, " extract print of IRRC, No.(299), March- April 1994.

(2) Richard P.Dimegllo, The Evolution of the just war tradition, Defining jus post bellum," military law Review, vol.(186), 2005, p.120.

(3) ICRC Report DPH 2006, Fourth Expertmeeting, PP 74-79.

(4) Adam Roberts, and Richard Guelff, Documents on the laws of war, N.Y.pub, 1989, p.12.

ممكناً للمقارنة بين عدة أهداف عسكرية لتحقيق ميزة عسكرية مماثلة، فالهدف الذي يتم انتقائه للهجوم المعلوماتي هو ذلك الهدف الذي يتوقع منه أن يسبب أقل خطورة على المدنيين والاعيان المدنية"[١].

وقد اشار الخبراء في دليل تالين إلى أن تطبيق القاعدة (٥٦) من الدليل والموضوعات ذات العلاقة بقاعدة الضرورة العسكرية يمكن تطبيقها على الهجمات المعلوماتية التي تتصف بوصف الهجمات فقط، ومن يبادر بالهجوم هو غير ملزم بمراعاتها في نطاق الهجمات المعلوماتية التي لا تصل لعتبة الهجوم المعلوماتي[٢].

ومن الجدير بالذكر أن تداعيات الخطر الذي يستدعي مراعاة الضرورة من قبل القائم بالهجوم على وفق قاعدة الضرورة لا يقتصر فقط على احداث أصابات أوفيات أو ضرراً أو التدمير الذي يصيب المدنيين والأعيان المدنية الذي ينجم نتيجة الآثار المباشرة أو غير المباشرة للهجوم المعلوماتي، إذ يرى أغلبية الخبراء في دليل تالين أن الخطر والضرر الذي يتوجب تفادية وفق مبدأ الضرورة يشمل الحرمان من الوظائف (Deprivation of functionality)، في ظروف معينة.[٣]

مثال على ذلك الهجوم المعلوماتي الذي يستهدف البيانات والأنظمة المعلوماتية للمؤسسات، والبنية الحيوية التي تخص المدنيين ويتسبب بحرمان المدنيين من وظائف هذهِ المؤسسات وما تقدمه من خدمات لهم من دون أن يترك الآثار مادية، يعد هجوماً يستفاد منه في تطبيق ميدأ الضرورة العسكرية.

وبتحليل ما تقدم نجد إن اللجوء لتنفيذ هجمات معلوماتية ينبغي أن يكون ضرورياً لتحقيق ميزة اكيدة من خلال الهدف العسكري المشروع، علاوة على ذلك فأن مسألة تحديد الأهداف العسكرية والمنشآت المستخدمة للأغراض عسكرية، تثير نقاشاً واسعاً لدى المختصين في الشأن

---

(1) Tallinn manual, op. cit, Rule (56).

(2) Ibid, comment (2) on Rule (56).

(3) Ibid, comment (6& 10) on Rule (30)

القانوني الدولي والذي ينعكس سلباً على التحديات التي تواجه المجتمع الدولي في ظل تزايد تنفيذ الهجمات المعلوماتية من خلال الفضاء المعلوماتي، ولكن هذا لا يمنع من اخضاع تلك الهجمات للقانون الدولي الإنساني في مبادئه العامة، إذ إن هجمات الفضاء المعلوماتي قد احدثت تداخلاً لما تقوم به الدول باستهداف الاشخاص والاعتداء على الحقوق والحريات الشخصية في صورة أرهاب الدولة، فضلاً عن تعرض الدول لشتى المخاطر التي تهدد سيادتها وامنها القومي ومنشآتها والبنى الاساسية التحتية.

ثانياً: مبدأ التناسب في استخدام القوة

إن مبدأ التناسب هو من المبادئ الهامة والاساسية في مجال سير الاعمال العدائية[١]، إذ إن فكرة التناسب لها استخدامات متنوعة فهي تتعلق بقانون اللجوء إلى الحرب (jus Adbellum) بخصوص تحقيق التناسب في عملية الدفاع الشرعي على وفق ميثاق الأمم المتحدة[٢]، وبموجب هذا المبدأ يحظر الهجوم الذي قد يتوقع منه أن يسبب بصورة عرضية خسائر في أرواح المدنيين أو حدوث إصابات بينهم أو الإضرار بالاعيان المدنية ، أو قد يكون مفرطاً في تجاوز ما يتوقع أن يسفر عنه من ميزة عسكرية ملموسة ومباشرة[٣].

كما يثير المبدأ عدة إشكالات فيما يخص مفهوم " الميزة العسكرية " كأمر غير مضبوط ومتفاوت، مما يثير الجدل حول الحد المطلوب في الاصابات العرضية المفرطة "، وكيف يمكن للمقاتل الأقل رتبة أن يوازن بين تنفيذ اوامر رؤسائه وترجيح لغة الاعتبارات الإنسانية.[٤]

---

(1) Michal N.Schmitt, " military necessity and Humanity in international Human itarian law: preserving the Delicate Blance", V.J.L, vol.50, Issue 4, university of Virginia, USA, 2010, p.816.

(2) Mohamed Bousoltane, Du droita al guerre au droit de la guerre: le recourse la Force armee an droit international of , Edition Dar Houma, Alger, 2010, pp. 25-28.

(٣) الفقرة (٢/أ) ثالثاً من المادة (٥٧) من البروتوكول الاضافي الاول س ١٩٧٧ كذلك ينظر: دراسة اللجنة الدولية للقانون الدولي الإنساني العرفي، الحاشية ١٢، القاعدة ١٦.

(٤) كالسهوفين فريتس ، تسغفلد ليزابيث، ضوابط تحكم خوض الحرب ، مدخل للقانون الدولي الإنساني، ترجمة احمد عبد الحليم، منشورات اللجنة الدولية للصليب الأحمر، جنيف، ط١، ٢٠٠٤، ص١٢٨.

يبدوا أن الأمر في غاية الصعوبة ويتسم بالتعقيد ، خاصة في تنفيذ الأوامر من قبل الجنود أو المحاربين الذين يتلقونها من رؤوسائهم الأعلى رتبة عسكرية، وبالتالي فأن المسؤولية في تطبيق هذهِ القاعدة تقع على عاتق القادة العسكريين وضمن العمليات الموسعة والتي يتوقع منها أن تحدث اضرار كبيرة بالاشخاص المدنيين، إلاّ إن هذهِ الصعوبات التقديرية لا يجب ان تتجاوز الالتزام الواقع على المقاتل بالقيام بالهجوم أو الامتناع عنه وفقاً لضرورات التمييز ومقتضيات التناسب.

إن من شأن مبدأ التناسب بأن يقلص من مقدار القوة التي يمكن استخدامها في الهجوم على الأهداف العسكرية وتدميرها على وفق الصورة التي لا تسبب أية أضرار بين صفوف المدنيين والأعيان المدنية وأن لا تسبب أية الام أو معاناة لا مبرر لها في صفوف السكان المدنيين[١]، لذا يتوجب الالتزام بجميع التدابير والاحتياطات الممكنة عند اختيار وسائل واساليب الهجوم، لتفادي الاضرار العرضية المتوقعة.[٢]

والسؤال الذي يتبادر إلى الذهن ما مدى إمكانية تطبيق قواعد مبدأ التناسب على الهجمات المعلوماتية؟

للاجابة على هذا السؤال لابد من استعراض آراء الفقهاء سواء كانت المؤيدة لتطبيق هذا المبدأ على الهجمات المعلوماتية ، أو تلك الآراء الرافضة لتطبيق مبدأ التناسب على الهجمات المعلوماتية التي يتمسك بها كل طرف عند تناوله لمفهوم تطبيق هذا المبدأ من عدمه.

انقسم الفقهاء بين مؤيد لإمكانية تطبيق مبدأ التناسب على الهجمات المعلوماتية، وبين رأي آخر يرفض تطبيق هذا المبدأ على الهجمات المعلوماتية، حيث أن الأتجاه الرافض لتطبيقه يرى بأن الاضرار العرضية الناجمة عن الهجوم وانتهاك هذا المبدأ هو أمر مؤكد، بسبب انعدام الحدود الفاصلة بين الفضاء المعلوماتي الذي يستخدم من قبل القوات والجماعات المسلحة

---

(1) Shaun Roberts, cyber wars: Applying conventional laws of war to cyber war fare and Non- state Actors, Northern Kentucky law Review, (vol) .41, No.3,2014, p.551.

[٢]الفقرة (٢/أ) ثانياً من المادة (٥٧) من البروتوكول الاضافي الاول س ١٩٧٧.

والمدنيين المشـــاركين في العمليات العدائية[١]، وعلى النقيض من هذا الرأي يذهب الأغلبية من الكتاب والفقهاء إلى أن مبدأ التناســـب يمكن تطبيقه بأنســـيابيه مثلى في ســـياق الهجمات المعلوماتية، محاولين تبرير ذلك على إن تطبيق هذا المبدأ من شـــأنه أن يســـاهم في الحد من الاضـــرار العرضـــية والعشـــوائية للهجمات مقارنة مع غيرها من الهجمات الحركية والتقليدية ، وبالتالي تقليل المعاناة غير الضـــرورية بين الســـكان والاعيان المدنية الأخرى وتجنب آثارها المدمرة[٢].

ومن نافلة القول إن الهجمات المعلوماتية تختلف بطبيعتها ووســـائل إســـتخدامها عن تلك الهجمات التقليدية، فهي تتم عبر وســـيط مختلف لكي تتمكن هجمات الحاســـوب من إصـــابة المطارات والبنية التحتية والإتصـــالات، وبما ينجم عن ذلك من تداعيات ســـياســـية وإقتصـــادية وإجتماعية جسيمة تتعلق بالحياة المدنية بصفة عامة مقارنة بالهجمات الحركية والتقليدية[٣].

فعلى ســبيل المثال ان نشــر رســالة واحدة عبر البريد المعلوماتي، مفادها إن هناك دماء ملوثة في المســتشــفيات وما إلى ذلك، يمكن لها أن تحدث آثار مدمرة على الصــعيد الإنســاني، ويعد القطاع الصـــحي اكثر عرضـــة للهجمات المعلوماتية، كما لها تأثيرات على قطاعات أخرى من البنية التحتية المدنية ، من بينها انظمة الكهرباء والمياه والصـرف الصـحي، وتفيد التقارير إن الهجمات في تزايد مســتمر، وتتعاظم حدتها بســرعة اكبر من أي توقعات ، وبالتالي لا يجوز في ايّ حال الهجوم على المستشفيات المدنية المخصصة لتقديم الرعاية الصحية للجرحى والمرضى والعجزة والنســـاء[٤]. وكان للفقيه (شـــين) رأياً في امكانية تطبيق مبدأ التناســـب على الهجمات

---

(1) Papanastasiou Afroditi, Application of inter national law in cyber war fare operations, Research paper, university of Leicester, UK, 2010, p.28.

(2) See Fore .e.g.: Davide Graham cyber Threats and the law of war , journal of National security law policy , vol. (4), No.(1),2010 p.99.

(3) Micheal N.Schmitt, " computer Net work Attack and use of force in inter national law, op. cit, p920.

(٤) اللجنة الدولية للصليب الاحمر، الحرب السيبرانية، القانون الدولي الإنساني يوفر طبقة إضافية من الحماية ، ١٠ ايلول ٢٠١٩.

المعلوماتية ، مبدياً تساؤله فيما إذا كانت هذهِ الهجمات المعلوماتية تشكل عدواناً لا يختلف عن الهجوم التقليدي باستخدام الصواريخ على سبيل المثال[١] .ويستدرك بالقول : إن مبدأ التناسب في استخدام القوة المعلوماتية لا يزال يشوبه نوعاً من الغموض ، ويحتاج إلى أجوبة في غاية الأهمية منها كيفية تحقيق التناسب في الرد على الهجمات المعلوماتية.

ويبدو أن (هيوز) قد ساير الرأي الذي أبداه الدكتور (شين) ، حول صعوبة تحقيق مبدأ التناسب على الهجمات المعلوماتية في ظل غموض هذا المبدأ، إذ ذهب بالقول:" إذا تم توجيه هجمات معلوماتية ضد بنى تحتية تستعمل لاغراض مزدوجة (مدنية – عسكرية) ، وعن بعد فلا يبدو أن الميزة العسكرية ستكون واضحة، مما يزيد في صعوبة تطبيق مبدأ التناسب على الهجمات المعلوماتية"[٢].

اما دليل تالين الخاص بالقانون الدولي المطبق على الحروب المعلوماتية، فقد أبدى الخبراء عند اعداد هذا الدليل مرونة نسبية حول تطبيق مبدأ التناسب على الهجمات المعلوماتية، وهو بهذا المعنى قد ساير رأي الأغلبية المؤيدة لتطبيق هذا المبدأ على الهجمات المعلوماتية، إذ تطرق إلى أن الهجمات المعلوماتية التي من شأنها أن تسبب الخسائر في ارواح المدنيين أو الاصابة بين صفوف المدنيين أو حتى الاضرار في الأعيان المدنية، والتي تكون مفرطة مقارنة بالميزة العسكرية الملموسة والمباشرة، والتي يتوقع الحصول عليها من خلال الهجوم، تكون محظورة[٣].

علاوة على ذلك فقد بين الخبراء بأن ما قد ينجم من إصابات بين صفوف المدنيين والأعيان المدنية خلال هجوم مباشر على أحد الأهداف المشروعة لا يدل ذلك على إن ذلك الهجوم هو غير شرعي، بل ينبغي التحقق من شرعية الهجوم من خلال النظر إلى التناسب بين

---

(1) Shin Beomuchul, op, cit, p,118.

(2) Rex Hughes, A Trealy for cyber space , inter national Affairs journal, vol.(86), No,(2), 2010, p.538.

(3) Tallinn Manualm, op.cit, Rule(51).

الاضرار الحاصلة بين صفوف المدنيين والأعيان المدنية مقارنة مع الميزة العسكرية التي يتوقع المهاجم الحصول عليها نتيجة هذا الهجوم[١].

وبتحليل ما تقدم نجد من خلال ذلك أن هناك وجه للمقارنة بين الأضـــرار الناجمة عن الهجوم والميزة العسكرية التي يروم الطرف المهاجم تحقيقها، فإذا كانت الأضرار التي اصابت المدنيين مفرطة قياساً مع أهمية الميزة العسكرية التي يراد الحصول عليها ، فيعد هذا الهجوم غير شرعي ويشكل انتهاكاً لمبدأ التناسب في استعمال القوة العسكرية، وبهذا الصدد فأن المحكمة الجنائية الدولية ليوغســلافيا الســابقة قد درجت في حكمها على أن مقياس التحقق من تناســب هجوم ما، فمن الضروري التأكد من أنه في الظروف المعقولة وعلى وفق المعلومات المتاحة في ذلك الوقت لدى الجاني ، وبناء على الاستخدام المعقول والاعتيادي للمعلومات المتوفرة لديه، هو معرفة مدى التوقع لدى الجاني الذي قام بتنفيذ الهجوم حول سقوط الضحايا بين صفوف المدنيين من عدمه[٢].

وعلى أية حال فأن تطبيق مبدأ التناسب على الهجمات المعلوماتية يواجه صعوبة في تقييم أثر الهجوم بسبب التداخل الحاصل بين الأهداف المدنية والعسكرية ، فضلاً عن صعوبة توقع النتائج من قبل القادة العسكريين، وبالنظر لدرجة التعقيد التي تتسم بها الهجمات المعلوماتية ، فهناك احتمالية اصابة النظم المدنية، كذلك قلة الوعي لدى مصدري قرارات الهجوم بطبيعة وآثار تلك الهجمات، مما يتطلب وجود خبراء للحاســوب لغرض تقيم الآثار المصـــاحبة والمحتملة والفرضـــية، عند التخطيط لتنفيذ الهجمات ، كما أن عملية النمذجة والمحاكاة كتلك التي جرت

---

(1) Tallinn Manualm, op.cit, Comment (2) on Rule (51).

(2) ICTY, prosecutor v.stanislav Galic, Trial chamber1, case No. (IT-98-29-T), judgement of 5 December 2003, para 58, p26.

فعلاً في اســـتخدام الأســـلحة النووية لها قيمة كبيرة في تحديد المخاطر المحتملة للهجمات المعلوماتية[١].

ثالثاً: الهجمات المعلوماتية في إطار مبدأ التمييز

إن قانون الحرب يحث اطراف النزاع المســـلح والتأكيد عليهم، بأن الهجمات توجه إلى المقاتلين وليس المدنيين، وإذا كان المدنيين هم المســـتهدفين، فيجب على تلك الاطراف أن تتأكد من أن المدنيين قد فقدوا الحماية المقررة لهم بموجب القانون الدولي الإنســـاني، نتيجة مشـــاركتهم في العمليات العســـكرية بصـــورة مباشـــرة [٢]، والســـؤال المطروح بهذا الصـــدد، هل الهجمات المعلوماتية لها القدرة على التمييز بين المقاتلين والمدنيين؟

إن مبدأ التمييز بين المقاتلين والمدنيين هو أحد أهم مبادئ القانون الدولي الإنساني العرفي المطبقة في النزاعات المســـلحة الدولية وغير الدولية، إذ يشـــكل مبدأ وقائياً يحكم ســـير الأعمال العدائية وتلزم قواعده اطراف النزاع المســـلح بضـــرورة التمييز بين المدنيين والمقاتلين ، وتوجيه هجماتهم إلى المقاتلين فحســـب دون غيرهم من المدنيين[٣]، وتأكد هذا المبدأ في البروتوكول الإضـــافي الأول لعام ١٩٧٧، الذي جاء في مادته (٤٨) على أنه :" تعمل اطراف النزاع على التمييز بين السكان المدنيين والمقاتلين وبين الأعيان المدنية والأهداف العسكرية، ومن ثم توجيه هجمات، ضـــد الأهداف العســـكرية دون غيرها، وذلك من أجل تأمين احترام وحماية الســـكان المدنيين والاعيان المدنية[٤].

---

(1) Micheal N.schmitt, " wired war fare: computer Net work Attack and the jus in Bello in computer Network Attack and inter national Law, inter national Law studies, Vol.76, 2002 , p392-393.

[٢] جون ماري هنكرتس، القانون الدولي الإنســـاني العرفي، (م الأول : القواعد) ، اللجنة الدولية للصـــليب الأحمر، بعثة القاهرة، القاهرة، ٢٠٠٧، ص٣.

[٣] محمد فهاد الشلالدة، القانون الدولي الإنساني، ط١، منشأة المعارف، الاسكندرية، ٢٠٠٥، ص١٥٣.

[٤] موسوعة اتفاقيات القانون الدولي الإنساني، (اعداد شريف عتلم ، محمد ماهر عبد الواحد)، اللجنة الدولية للصليب الأحمر، بعثة القاهرة، ط٩، القاهرة ، ٢٠٠٩، ص٢٨٩.

أما في سياق الهجمات المعلوماتية فأن تطبيق مبدأ التمييز يثير صعوبات عملية كبيرة، إذ إن القانون الدولي الإنساني لم يعترف بالحماية للأفراد الذين يشاركون بصورة طوعية في الهجمات المعلوماتية ضد الخصم، بسبب أن هؤلاء لا يعدون ضمن فئة المقاتلين الشرعيين، فهو لا يوفر الحماية المقررة لهم وعدهم ضمن فئة المقاتلين غير الشرعيين ، أو مدنيين غير محميين، طالما أنهم يشاركون في العمليات العدائية، فعلى سبيل المثال القراصنة الهواة الذين يشرعون بتنفيذ هجمات ضد الدولة الخصم، هذه الهجمات تكون مبرراً للدولة الخصم المستهدفة بالرد على تلك الهجمات، وبالتالي فأن القراصنة المشاركين في تلك الهجمات يكونوا هدفاً مشروعاً للاستهداف[١].

من الجدير بالذكر إنّ مبدأ التمييز في القانون الدولي الإنساني يشترط وجود علامات دالة على فئة المقاتلين لتمييزهم عن المدنيين، كالعلامة البارزة المرئية عن بعد واللباس العسكري ورفع السلاح علناً ، والسؤال المطروح هل يمكن تصنيف المهاجم المعلوماتي مقاتل على وفق الاشتراطات التي وضعها القانون الدولي الإنساني في البروتوكول الإضافي الأول؟

إن الاجابة على هذا السؤال تحتاج إلى توضيح دقيق إذا ما أريد للمدنيين المعرضين للهجمات المعلوماتية أن يحصلوا على الحماية المقررة لهم بموجب القانون الدولي الإنساني، بالاضافة إلى ذلك فأنه عند حدوث حالة الشك، يجب افتراض أن أي شخص مدني محمياً من أي هجوم مباشر يتعرض له[٢].

ولذا يمكننا القول إن القانون الدولي الإنساني يشترط في المقاتل حمل الشارة المميزة وارتداء اللباس العسكري ، ورفع السلاح علناً، إلاّ إن الأمر قد يختلف في حالة المهاجم المعلوماتي، إذ إن الأشخاص الذين ينفذون الهجمات المعلوماتية غالباً ما يكونون بعيداً عن الهدف وبالتالي من الصعوبة تمييزهم، كما إن القيادة المسؤولة غالباً ما تفتقر إلى الدقة في اتخاذ قرارها بشأن الهجمات المعلوماتية، لأن المهاجم المعلوماتي يتخذ قراراته بصورة آنية في ضوء الظروف

---

(1) Nils Melzer,op.cit p.47-50.

(٢) ينظر المادة (٥١) الخاصة بحماية السكان المدنيين من البروتوكول الإضافي الأول لعام ١٩٧٧.

المصـاحبة للهجمات المعلوماتية ، هذه الظروف التي لا يتوقعها القائم بتنفيذ الهجوم المعلوماتي، فضـلاً عن إن المهاجم المعلوماتي غالباً ما تم خضـوعه لإجراءات داخلية وليس لنظام قضـائي عسكري.

ومن نافلة القول يتعين أن تكون الأعمال العسـكرية موجهة ضـد الأهداف التي تسـهم مساهمة فعالة في الأنشطة العسكرية، التي يعطي تدميرها ميزة عسكرية ، والحث على الابتعاد عن الأعيان المدنية التي تكون محمية بموجب القانون الدولي من أن تكون هدفاً لهجوم عسكري، علاوة على ذلك فلا تعد كل هجمة معلوماتية تسـتهدف الأعيان المدنية فعلاً يخالف قواعد النزاعات المسلحة، كما هو الحال عند اختراق شبكة مدنية لأحدى الدول لغرض إرسال رسائل معلوماتية للمدنيين تطالبهم فيها بضرورة الاستسلام[١]. ولكن يكون الأمر اكثر صعوبة عندما يتم استخدام هدف أو منشآة مدنية ، لأغراض عسكرية، فأنها تصبح هدفاً عسكرياً من خلال معيار الأستخدام، فعلى سبيل المثال: محطات التلفزيون أو الإذاعة المدنية التي تبث بصورة منتظمة معلومات عسكرية، وبالتالي فأن استخدام أحد أطراف النزاع شبكة حاسوب مدنية لأغراض عسكرية، تفقد الشبكة طابعها المدني وتصبح هدفاً عسكرياً ، حينها تبقى هذه الشبكة هدفاً عسكرياً للخصم حتى في حال استمرار استخدامها لأغراض مدنية[٢]. ومن الجدير بالذكر إن هذهِ الإعيان المدنية التي اصبحت أهدافاً عسكرية عن طريق الاستخدام، يمكنها أن تعود إلى طبيعتها المدنية إذا توقف الاستخدام العسكري لها ، وبالتالي يستعيدون الحماية المقررة لهم ضد أي هجوم[٣].

هناك مسألة تثير نقاشاً واسعاً حول الهجمات المعلوماتية الموجهة للأهداف المخصصة للإستخدام المزدوج، التي تؤدي إلى خسائر عرضية كبيرة بالمقارنة مع الميزة العسكرية المتحققة

---

(1) Clarke, R.and Knake, R., cyber war fare: Th Next Threat to National security and what to Do about it, 2010 , p.9-10.

(2) Micheal Schmitt, Tallinn Munual on the international law Applicable to cyber war fare, op. cit, comment on Rule (38).

(3) Ibid, comment (10) on Rule (38).

منها، والسـؤال الذي يطرح للنقاش بهذا الصـدد هل تعد الأعيان المدنية التي تسـتخدم لأغراض عسكرية أهداف مشروعة؟

إن التداخل الحاصـل بين الأنظمة ذات الاسـتخدام المدني والعسـكري يكون من الصـعوبة فصـل تلك الأهداف عن بعضـها البعض، مثل تداخل الاتصـالات العسـكرية الجوية مع انظمة السـيطرة الملاحية الجوية، فوفقاً لهذا الاسـتخدام فأن الأعيان المدنية التي تسـتخدم لأغراض عسكرية في ذات الوقت تصبح هدفاً عسكرياً مشروعاً[١].

وبالتالي فأن الهجمات المعلوماتية تشكل تحديات خطيرة بشأن التمييز بين الأعيان المدنية والأهداف العسكرية، فعلى سبيل المثال الشبكة المعلوماتية التي تستخدم للأغراض العسكرية ، والمدنية في ذات الوقت، قد يكون من الصعوبة معرفة أي جزء من الشبكة سيمر عبر الإرسالات العسـكرية، وأي منها في الأجزاء المدنية، ففي هذه الحالة تكون الشـبكة بأكملها ، أو على الأقل الجزء الذي من المحتمل أن يتم الأرسـال فيها، تكون مؤهلة كهدف عسكري[٢]، والوسيلة الوحيدة التي يمكن من خلالها حماية المدنيين من الهجمات الموجهة ضد شبكات ذات الإستخدام المزدوج لأغراض عسـكرية أم مدنية في ذات الوقت، هو عزل الاسـتخدامات العسـكرية عن الشـبكات المخصـصـة لأغراض مدنية، وبالتالي إضفاء الحماية على الأهداف المدنية وعدم إعتبارها اهدافاً عسكرية مشروعة لتنفيذ هجمات معلوماتية ضدها.

من المؤكد إن البنية التحتية التي تحمل الاسـتخدام المزدوج هي الأداة الأولى في الهجمات المعلوماتية وتدميرها بشـكل تام أو جزئي سـيؤدي إلى تحقيق ميزة عسـكرية أكيدة فعلى سـبيل المثال، تم استخدام نفس المعايير التي أستخدمت ضد العراق خلال الحصار المفروض عليه، إذ تم منع العراق من استيراد أقلام الرصاص بحجة الاستخدام المزدوج[٣].

---

(1) Tallinn Manual, op.cit,, comment (11) on Rule (38).

(2) Micheal Schmitt, Tallinn munual on the international law Applicable to cyber war fare, op. cit, comment (3) on Rule (39)

(3) Arnove, A. IRaq under siege: The Deadly impact of sancitions and war, 2003, p.24-25.

ونستنتج من خلال ما تقدم إن الأعيان المدنية التي تستخدم لأغراض مدنية وعسكرية وأجهزة الحاسوب، وشبكات الحاسوب والبنية التحتية المعلوماتية تتحول بشكل تلقائي لهدف عسكري مشروع، فعلى سبيل المثال اجهزة الرادار المستخدمة لمراقبة السفن والطائرات المدنية، يكون هدفاً مشروعاً لطرف النزاع في حال تم استخدامه لرصد أي طائرة او سفينة عسكرية، مع العلم أن هذا الجهاز يختص بوظيفة رصد هذهِ المركبات بغض النظر عن تصنيفها سواء كانت مدنية أم عسكرية، فمجرد أن يتم رصد هذهِ المركبات فإنها تصبح في دائرة الأهداف المشروعة ، وحتى شبكة الاتصالات المدنية هي الأخرى في حال استخدامها تصبح هدفاً مشروعاً لكونها تعد من الأهداف مزدوجة الاستخدام.

رابعاً: الحالات العرفية غير المقننة (شرط مارتنيز Martinus)

ينص شرط مارتنيز على أنه :" في الحالات التي لا تغطيها الإتفاقيات والمواثيق الدولية، يظل المدنيون والمقاتلون تحت حماية وسلطة مبادئ القانون الدولي المستمدة من الأعراف الراسخة، ومن مبادئ وقواعد الإنسانية وما يمليه الضمير العام"، ويرى أصحاب الأتجاه المؤيد لاخضاع الهجمات المعلوماتية لقواعد القانون الدولي الإنساني أنه من الممكن الاحتجاج بهذا الشرط لتفسير أحكام وقواعد وأتفاقيات القانون الدولي الإنساني في حالة وجود شك حول بعض الأحكام الواردة فيه[١]. وقد أكد على هذا الشرط البروتوكول الإضافي الثاني لعام ١٩٧٧ في ديباجته على إنه : " في الحالات التي لا تشملها القوانين السارية، يبقى شخص الإنسان في حماية مبادئ الإنسانية وما يمليه الضمير العام"[٢].

وقد أكدت محكمة العدل الدولية على أهمية شرط في الحالات والمواقف التي لم يرد فيها نص إتفاقي، في رأيها الإستشاري لعام ١٩٩٦ الخاص بشرعية التهديد أو أستعمال الأسلحة النووية وقد جاء في رأيها على أنه " يمنح شرط مارتنيز سلطة معالجة مبادئ القانون الدولي وما

---

(1) See: Marco Roscini, Cyber operations and the Use of Force ininter national Law, oxford University press, First Editionm UK, 2014, P.22.

(٢) اللجنة الدولية للصليب الأحمر ، الملحقان البروتوكولان ، الملحقان بأتفاقية جنيف المنعقده في ١٢/ أب/ اغسطس ١٩٤٩، جنيف، سويسرا، ط٤، ١٩٩٧، ص١١٨.

يمليه الضـــمير العام بوصـــفها مبادئ من القانون الدولي، تاركاً المحتوى الدقيق للمعيار الذي تســتلزمه مبادئ القانون الدولي على ضــوء الظروف المتغيرة، بما في ذلك التغيرات في وســائل الحرب وتسامحه"[١]، هذا يدل على إن المحكمة في رأيها الاستشاري سالف الذكر قد استندت إلى شــرط مارتنيز كأطار قانوني لأي ســلاح جديد لم يكن ســابقاً محل قواعد اتفاقية تنظم إنتاجه وأستخدامه أو التهديد به ، وكان أهم المبادئ التي تهتم بمسألة حظر الأسلحة النووية وغيرها من الأسلحة التي لم تتناولها المعاهدات الدولية.

وهناك سـؤال مطروح للنقاش في غاية الأهمية وهو ما مدى ملائمة شـرط مارتنيز لتطبيقه على الهجمات المعلوماتية؟ للأجابة على هذا السـؤال لابد من بيان أن القانون الدولي الإنسـاني يطبق في النزاعات المسـلحة، والهجمات المعلوماتية هي ليسـت مسـلحة ، ولكن غياب القواعد المتعلقة بصورة خاصة في الهجمات المعلوماتية لا يعني إن مثل هذهِ الهجمات لا تخضع لقواعد القانون الدولي الإنسـاني، وعند الرجوع إلى فتوى محكمة العدل الدولية بشـأن مشـروعية التهديد بالأسـلحة النووية أو اسـتخدامها، نجد أنها قد أكدت على أهمية هذا الشـرط، ولا يمكن الشـك في اسـتمرار وجوده وقابلية تطبيقه، ويعد هذا الشـرط هو وسـيلة فاعلة لمواجهة التطور السـريع في التكنولوجيا العســكرية[٢]. علاوة على ذلك يمكن الإســتدلال بما ورد في حكم محكمة الولايات المتحدة الأمريكية العسكرية في قضـية (كروب) عام ١٩٤٨، إذ تطرقت إلى إن شـرط مارتنيز هو يمثل اكثر من كونه مجرد إعلان، وأنه شـرط عام يجعل العادات المسـتقرة بين الأمم المتمدنة وقوانين الإنسانية وما يمليه الضمير العام جزءاً من المقاييس القانونية التي يتحتم تطبيقها عندما لا تغطي احكام الاتفاقيات حالات محددة[٣]. وقد تناول شـميت (Schmitt) مسـألة تطبيق هذا الشــرط وملائمته على الهجمات المعلوماتية بقوله " يعد مبدأ مارتنيز المبدأ الأكثر قرباً لكونه

---

(1) ICJ Nuclear weapons Advisory opinion ,op, cit, para 78.

(2) Bilinding weapons: Reports of the meetings of experts convened bay the international committee of the red cross on battle field laser weapons, 1989-1999, ICRC, 1993, p.78.

(3) Ibid, p22-23.

يغطي حالات غير منصـــوص على تنظيمها في الإتفاقيات الدولية، ولا يكون ذلك ممكناً إلى باللجوء إلى القانون الدولي الإنسـاني العرفي، ذلك المصـدر المهم الذي اشـارت إليه المادة (٣٨) من النظام الاســـاس لمحكمة العدل الدولية"[١]. وبهذا الصـــدد نود أن نشـــير إلى إن الظروف المصـاحبة لأنتهاك المعايير الإنسـانية يمكن إن تكون أكثر تطوراً في الوقت الراهن مما كان عليه الحال عند وضـع شـرط (مارتنز)، وتتجلى فلسـفة واضـعي هذا الشـرط هو في إن ما لم يحظر صـراحة في المعاهدات أو العرف، لا يمكن إباحته إذا كان يتعارض مع مبدأ الإنسـانية وما يمليه الضـــمير العام. وهذا يعني أن عدم وجود قواعد دولية محددة، عرفية كانت أم تعاهدية تنظم الهجمات المعلوماتية ، لا يعني منح الحق ضمناً بجواز اللجوء إليها، لأنها تتعارض بطبيعتها مع القوانين الإنسـانية وما يمليه الضـمير العام العالمي إذا ما ثبت اسـتهدافها لمنشـآت تحوي قوى خطرة كأنابيب النفط والمحطات النووية، وأعيان اخرى مدنية تكون ضـــرورية لبقاء الســـكان المدنيين، كشبكات الماء والكهرباء.[٢]

---

(1) Micheal N.schmitt, " wired war fare: computer Network Attack and jus in Bello , op, cit, p369.

(٢) د. أحمد عبيس نعمة الفتلاوي، مصدر سابق، ص٦٣٩.

الفصل الثاني

ماهية واجب العناية اللازمة للدول

يشـــير واجب العناية إلى المبدأ أو المعيار الذي تلتزم به الدولة تجاه الدول الأخرى في اطار علاقتها الدولية، وقد ظهر واجب العناية في القانون الدولي وأخذ يسـتقر تدريجياً من خلال قرارات التحكيم ومطالبات اللجان المختلطة، وممارسات الدول مع نهاية القرن التاسع عشر وبداية القرن العشـرين إلا أن اصـبح واجب العناية مبدأ راسـخ في القانون الدولي والذي أضـحى تطبيقه مقياس لتقييم مدى امتثال الدول لالتزاماتها الدولية.

إن التزامات الدول في الفضـاء المعلوماتي نابعة من تمسـكها بمبدأ سـيادتها على إقليمها البري والبحري والجوي، وولايتها القضـــائية عليه، فإذا ما أباح لها القانون الدولي ممارســـة هذا المبدأ، فانه في المقابل يتوجب عليها الحفاظ على حقوق الدول الأخرى المجاورة وعدم الإعتداء عليها بأي أنشـطة معلوماتية غير مشـروعة، الأمر الذي يترتب عليه انتهاك مبدأ السـيادة الذي تستطيع الدولة من خلاله مباشرة حقها في السيطرة على اقليمها وتمتعها بممارسة سلطاتها عليه، وهناك عدة تطبيقات لممارســات الدول، فضــلاً عن تطبيقات قضــائية أخرى لواجب العناية في الفضاء المعلوماتي سواء في اطار القانون الدولي للبيئة، أم في سياق حقوق الإنسان المعلوماتية.

وعندما شـــعرت الدول أنها بات تواجهه تحديات ومخاطر من أنشـــطة معلوماتية عابره للحدود سعت إلى بناء استراتيجيات وقائية– دفاعية لمنع الهجمات المعلوماتية أو الحد منها على أقل تقدير، ولدراســة ماهية واجب العناية اللازمة للدول، ينبغي البحث فيه في ضــوء ممارســات الدول والتطبيقات القضـــائية، لذلك قســمنا هذا الفصـــل على مبحثين نتناول في الأول التعريف

بواجب العناية في اطار الهجمات المعلوماتية، أما الثاني سنكرسه للجهود الدولية في اطار واجب العناية للحد من اضرار الهجمات المعلوماتية، وعلى الشكل الآتي:

المبحث الأول

التعريف بواجب العناية في اطار الهجمات المعلوماتية

حظي مبدأ واجب العناية بأهتمام واسع النطاق، سواء من خلال كتابات الفقهاء، أو الاجتهادات القضائية، ومحاكم التحكيم، وهناك العديد من القرارات القضائية التي صدرت بهذا الشأن، والزمت الدول بضرورة إعمال واجب العناية في ممارساتهم الدولية، وتجنب الاضرار بالدول الأخرى، إلا أنه على الرغم من أهمية واجب العناية كمعيار لتقييم ممارسات الدول، إلا لكنه يفتقر إلى الأساس القانوني الذي يرتكز عليه بصورة صريحة وواضحة سواء في القانون الدولي التعاهدي أو العرفي ، إلا أن لواجب العناية تطبيقات عملية ذات اهمية سواء في مجال القانون الدولي للبيئة، أو في سياق القانون الدولي لحقوق الإنسان، ونتيجة لأزدياد استخدام الدول للفضاء المعلوماتي، وما يحتويه هذا المجال من انشطة معلوماتية، أضحت سيادة الدول بمواجهة خطر هذهِ الانشطة، خصوصاً إذا ما علمنا أن الفضاء المعلوماتي يتسم بعدد من الخصائص المعقدة التي تثير صعوبة بالغة في منع هذهِ الانشطة أو السيطرة عليها.

والاسئلة المطروحة بهذا الصدد ما المقصود بواجب العناية؟ وهل هو معيار لقياس سلوك الدول في منع الهجمات المعلوماتية، أم أن الدولة يقع عليها التزام واجب المنع كنتيجة لممارستها الانشطة المعلوماتية؟ وما هي السيادة المعلوماتية؟

وتبقى المسألة الأكثر أهمية ، وهي إمكانية تطبيق واجب العناية اللازمة للدول في مواجهة أضرار الانشطة المعلوماتية، لاسيما في اطار القانون الدولي للبيئة والقانون الدولي لحقوق

الإنســـان، إذا ما علمنا إن واجب العناية يفتقر للإســـاس القانوني الذي يقوم عليه، الذي لطالما تذرعت به الدول عند انتهاكها لحقوق وسيادة الدول الأخرى المجاورة.

وسنحاول الاجابة عن هذه التساؤلات من خلال تقسيم هذا المبحث على مطلبين: المطلب الأول نتطرق فيه إلى مفهوم واجب العناية، أما الثاني، نتناول فيه ممارســـات الدول لواجب العناية.

المطلب الأول

مفهوم واجب العناية

باتت الدول اليوم معنية بالتزام واجب العناية عند ممارســتها لحقوقها الســيادية وفي حدود نطاقها الاقليمي، وإذا كان ميثاق الأمم المتحدة قد اورد قيوداً على الدول عند ممارســتها لحقوقها، في ضـــوء مبادئ القانون الدولي العام، إلا أن الأمر ليس بهذهِ الســـهولة عند اســـتخدام الدول للفضـــاء المعلوماتي، وما ينجم عن هذا الإســـتخدام من ضـــرر عابر للحدود وقد يلحق بالدول الأخرى المجاورة، والســؤال الذي يثار بهذا الشــأن، ما مدى امكانية تطويع مبادئ القانون الدولي العام على الفضاء المعلوماتي؟ وما هي شروط تطبيق واجب العناية المعلوماتية؟

ولأهمية واجب العناية على صـــعيد القانون الدولي، لذلك ســـنتناوله في هذا المطلب وفي فرعين نتطرق إلى: تعريف واجب العناية وشروط تطبيقه في الفرع الأول، اما الثاني سنتناول فيه التزامات الدول في الفضاء المعلوماتي لذا سنبحث هذهِ المواضيع على وفق الآتي:

الفرع الأول

تعريف واجب العناية وشروط تطبيقه

لأهمية واجب العناية على صـــعيد القانون الدولي وخصـــوصـــاً في ســـياق الهجمات المعلوماتية، ســنتناول في هذا الفرع واجب العناية اللازمة للدول من خلال تعريفه وبيان شــروط تطبيقه وعلى النحو الآتي:

أولاً: تعريف واجب العناية

يعد مفهوم واجب العناية من أهم المفاهيم التي نالت اهتمام القانون الدولي ، جاء ذلك من خلال العديد من قرارات التحكيم ذات الصلة بالمسؤولية الدولية ، على الرغم من ان معالمه لا زالت غير مكتملة الوضوح وعدم حصول الاتفاق بشأنه ، وقد يعزى ذلك لاختلاف ظروف كل قضية عن الاخرى تبعاً للظروف المحيطة بها ، وتعود جذور مصطلح واجب العناية إلى القانون الروماني ، والذي كان بموجبه أن الشخص يتحمل تبعة مسؤولية إحداث أي ضرر عرضي قد طرف يلحق بالأخرين، ولقد تعددت وتنوعت التعريفات التي تناولت واجب العناية، فمنهم من عرف واجب العناية بالقول:" الرعاية التي يجب على الشخص المعتاد القيام بها قبل الدخول في اتفاق معين مع الطرف الآخر أو معيار معين من الرعاية التي يقدر من خلالها الشخص المعتاد ، لتوخي الحذر من حصول الضرر المتوقع أن ينشأ من إستخدامه لممتلكاته أتجاه الاخرين"[١].

وواجب العناية هو نتيجة طبيعية للمساواة في السيادة بين الدول حيث تتمتع الدولة بالسيطرة على ما موجود داخل حدود اقليمها ، ولكن في ذات الوقت يجب عليها ايضاً احترام سيادة الدول وعدم المساس بحقوقها، وتطبيقاً لذلك وفي ضوء الاجتهادات القضائية صاغت محكمة العدل الدولية بشكل واضح تعريفاً حول واجب العناية اللازمة الدول بالمحافظة على حقوق الدول الاخرى بالقول:" التزام الدول بعدم السماح عن علم باستخدام اراضيها للقيام بأعمال تتعارض مع حقوق الدول الاخرى"[٢]. وقد وضع الفيلسوف الهولندي(غروسيوس) الأسس الفكرية لهذا المفهوم في القرن السابع عشر ولم يتبلور هذا المفهوم بصيغته المعروفة حتى القرن التاسع عشر، حيث اتخذ كمعيار واجب وقيد على سلوك الدولة وبات من المقبول أن تتخذ الحكومات تدابير معقولة لحماية الأجانب داخل أراضيهم، خصوصاً في ظل هجرة أعداد كبيرة من مواطني

---

[١] د. احمد عبيس الفتلاوي، وازهر عبد الامير راهي ، الاطار المفاهيمي للعناية الواجبة والاخطار في ضوء قواعد المسؤولية الدولية (جائحة كورونا) مجلة الرافدين للحقوق، (م ٢٢) ، ع (٧٩) كلية الحقوق جامعة الموصل، ٢٠٢٢ ، ص٧٦ .

[2] ICJ, UK V.Albania, The corfu channel Case (Merites), judgment of April, th, 1949, p.22.

بعض الدول عبر الحدود الإقليمية، حيث اشـــار القاضـــي (moore) وفي قرار المحكمة العليا الامريكية عام ١٨٨٧ ذات الصـلة بتزوير العملة الاجنبية في قضـية (lottus) ، على أنه " من المســـتقر ان الدولة ملزمة ببذل واجب العناية لمنع ارتكاب الاعمال الاجرامية التي ارتكبت في حدود سيادتها والمرتكبة ضد مواطنين أخرين أو ضد شعبها "[١].

وقد فسرت محكمة العدل الدولية في حكمها الصادر ٢٤ / ايار عام ١٩٨٣ ، اثناء نظرها القضـــية المتعلقة بالرهائن الدبلوماســـيين والقنصـــلين في طهران من موظفي الولايات المتحدة الامريكية ، معيار واجب العناية على انه "ما يتوجب على الدولة المســـؤولة القيام في الظروف الاعتيادية ومعالجة الموقف باستخدام الوسائل المتاحة لغرض الوفاء بالتزاماتها الدولية" وهي بهذا التغيير انتهجت مســتوى مقبول من الرعاية والحكم الرشــيد والمتوقع من الدولة القيام به في ظل ظروف معينة للوفاء بالتزاماتها الدولية[٢].

وفي قضــية حكم الالباما ، فقد عُدّ واجب العناية اللازمة معياراً لحياد الدولة والتزاماتها في مســـألة الحياد ، وكانت القضـــية التي نظرتها المحكمة تتمثل في انتهاك بريطانيا لجانب الحياد ومخالفتها لالتزاماتها في الحياد، ورأت بريطانيا ان أنتفاء معيار واجب العناية يعني الفشـــل في اتخاذ عناية ما من جانب وظيفة حكومية على النحو المألوف أو العادي في المســـائل الداخلية وتوقعها على نحو معقول في بذل مســائل ذات مزايا والتزامات دولية [٣]. وعرف قاموس كولينز (colins) واجب العناية على انه "درجة الرعاية المتوقعة بشـــكل معقول ، أو المطلوب قانوناً خصوصاً من الاشخاص الذين يقدمون المشورة المهنية واجراء تقييم لجذور عناية ضرورية "[٤]،

---

[١] حيدر عبد محســـن شـــهد الجبوري ، معيار العناية الواجبة في القانون الدولي البيئي ، مجلة كلية التربية الاساسـية للعلوم التربوية والانسـانية، الجزء (٢) ، م (١٣) ، ع (٥٢) ، كلية التربية الأسـاسـية، جامعة بابل ، ٢٠٢١ ، ص٣١٣ .

[٢] د.أحمد عبيس نعمة الفتلاوي، وازهر عبدالامير راهي، مصدر سابق، ص٧٨.

[٣] د. حيدر عبد محسن شهد الجبوري ، مصدر سابق ، ص٣١٤ .

[4] Jona than Bonnit cha and Robert Mccorhuodale, The Concept of Due Diligen the UN Guiding Principles on Business and Human Rights, The European Journal of international Law, 28 No.(3), 2017, p.901.

كذلك عرفت على أنها "السـلوك الجيد المتوقع من حكومة دولة معينة الذي يكون الغرض منه حماية مصـالح الدول الأخرى بشـكل فعال، وليس من الضـروري أن تكون العناية التي تبذلها الدولة متماثلة مع الأهمال الصـادر عنها، أي أنها حتى وأن فشـلت في الوفاء بمعيار السـلوك المتوقع فقد بذلت جهداً مقبولاً في التقليل من الأضرار". (١)

والعناية الواجبة تعني التحقيق أو ممارسة الرعاية التي من المتوقع ان يقوم بها الشخص ، قبل الدخول في اتفاق مع طرف اخر ، أي بمعنى انها معيار الرعاية الذي يتوقع من شـخص عادل ومعقول ومن عادته ان يقوم بها ، أو في ظل ظروف مماثلة للوضع المعني ، أي يمارسها اتجاه ممتلكاته ، وهذا المعيار يمكن ان يكون التزاماً قانونياً، عندما يسـتخدم لأثارة المسـؤولية الدولية الناشئة عن الأهمال(٢).

يشـار في بعض الاحيان إلى مبدأ واجب العناية على انه التزام اليقظة obligation of vigilance ، أو أنه التزام المنع obligation of prevention ، أو واجب المنع duty of prevention ، علاوة على ذلك فقد اعتمد فريق الخبراء الدوليين مصـطلح واجب العناية في ضـوء الاسـتخدام الشـائع، لكنهم اتفقوا على أنه يمكن اعتباره مرادفاً لمصـطلح اليقظة الا انه في ذات الوقت ، رفض فريق الخبراء الدوليين اسـتخدام مصـطلح الالتزام بالمنع لانهم بالنتيجة سـاد الاتفاق فيما بينهم على أن واجب العناية لا يتضمن الالتزام باتخاذ اجراءات وقائية مادية لضمان عدم اسـتخدام اراضـي الدول في انتهاك سـيادة الدول الاخرى(٣). وعلى وفق ما جاء بدليل تالين فقد أشارت القاعدة (٦) لأعمال مبدأ واجب العناية اثناء ممارسة الدول لأنشطتها المعلوماتية من خلال عدم السماح باستخدام اراضيها أو بنيتها التحتية المعلوماتية الخاضعة لسيطرتها الحكومية والتي تؤثر على حقوق الدول الاخرى وما ينتج عنها من آثار سلبية (٤).

---

(1) Maria Flemme, Due Diligence in international Law, Master thesis, Faculty of law, university of land, 2004, p.15.

(2) Hitt, Michela , Hoskisson , Roberte E, competing for advantage , mason , 2004 .

(3) Tallinn manual 2.0,op. cit, Rule (6) , p.32.

(4)Ibid, Rule (6), p31.

على أية حال فأن هذه القاعدة ترتكز على مبدأ القانون الدولي العام والذي يقضي بضرورة ممارسة الدول لواجب العناية في ضمان عدم استخدام الاراضي والممتلكات المادية العائدة لها والتي تقع تحت سيادتها من اجل الحاق الضرر بالدول الاخرى ، وواجب العناية هو معيار السلوك الذي يتوقع من الدول انتهاجه عند الامتثال لقواعد القانون الدولي العام ، وهو ما اكدته محكمة الدول في حكمها الشهير في قضية قناة كورفو ، والذي أصبح قيداً على كل دولة بأن إلا تسمح عن قصد باستخدام اراضيها في ممارسات مخالفة لحقوق الدول الاخرى ، وتبعا لهذا الحكم فقد تم تحديد التعريف المعاصر والمعترف به بصورة عامة بشأن مبدأ واجب العناية ، فهو "التزام ناشئ عن مفهوم السيادة يتطلب من دولة معينة ان تحافظ على حقوق دول اخرى خاضعة لسيطرتها الاقليمية"[1]. وبالاستناد لهذه القاعدة فقد استنتج فريق الخبراء الدوليين ان مبدأ واجب العناية من الممكن تطبيقه في إطار المعلوماتية، اذ تفترض هذه القاعدة ان النشاط المعلوماتي الضار ترتكبه الاطراف الاتية :-

١- الدولة المستهدفة بالهجمة المعلوماتية.

٢- الدولة الاقليمية موضوع الحكم.

٣- طرف اخر هو صاحب الهجمة المعلوماتية ، بغض النظر فيما اذا كان يتم شنها بواسطة فرد او شركة ، او جهات فاعلة غير حكومية ، أو دولة . ويشتمل الالتزام ببذل واجب العناية على جميع الاراضي الخاضعة لسيادة الدولة الاقليمية ، وهو يتضمن أي بنية تحتية معلوماتية مستخدمة ، فضلاً عن الافراد الذي يقومون بشن الهجمة المعلوماتية في تلك المنطقة ، ويفترض كذلك أن من يقوم بتنفيذ هجمة معلوماتية معينة من الممكن ان يتم شنها باستخدام اراضي دولة ثالثة ، مثال على ذلك قيام قراصنة متسللين في الدولة (أ) ، والتي تنفذ هجمة معلوماتية ضارة بالدولة (ب) من خلال استخدام البنية التحتية المعلوماتية التابعة للدولة (ج) ، اذا كانت الدولة (ج) على علم باستخدام اراضيها وفشلت

---

(1) Tallinn manual 2.0 , op . cit , Rule (6), p.32.

في اتخاذ التدابير الممكنة لوضـــع حد لهذه الهجمة ، فأنها بهذا المعنى قد انتهكت مبدأ واجب العناية [١].

ومن الجدير بالذكر ان فريق الخبراء الدوليين قد ابدى رؤيته بإمكانية ان يمتد مبدأ واجب العناية لأوسع نطاق خارج حدود ولاية الدولة الإقليمية في حالتين هما : حالة ضم الإقليم ، وحالة الاحتلال العسـكري ، اذا كانت الدولة تسـيطر على اراضـي في الخارج دون ان تمارس السـيادة عليهـا . كـذلـك من الواجـب على الـدول ان تمـارس مبـدأ واجـب العنـايـة على البنيـة التحتيـة المعلوماتية الحكومية الخاضـعة لسيطرتها في خارج اقليمها ، ويستخدم في هذا السياق مصـطلح الرقابة الحكومية لغرض التمييز بينها وبين تلك التابعة للقطاع الخاص. ومن الامثلة التطبيقية لمبدأ واجب العناية على البنية التحتية المعلوماتية الحكومية خارج الحدود الاقليمية للدولة ، شبكة وطنية عائدة للدولة موضـوعة على منشـآت عسـكرية في بلد اجنبي ، والبنية التحتية المعلوماتية على متن المنصـــات الســـيادية في اعالي البحار أو في المجال الجوي الدولي ، والبنية التحتية المعلوماتية في مقر دبلوماسي[٢].

أما ما يخص الضـــرر المادي الذي يجب على الدولة المســـتهدفة ان تتحمله في ســـياق تطبيق هذه القاعدة ، فقد وافق فريق الخبراء الدوليين على ان هذه القاعدة تتضمن جميع الهجمات المعلوماتية التي تتعارض مع حقوق الدولة المتضـــررة بموجب القانون الدولي العام، وهي ذات عواقب خطيرة وآثار ســـلبية ، ومثال على ذلك حالة قيام الدولة (أ) بأطلاق برامج ضـــارة يتم التحكم بها من خلال البنية التحتية للقيادة والتحكم في الدولة (ب) ، وتقدم تقارير عنها إلى الدولة (ب) ، ادخال فيروس بواسـطة البرنامج الضـار إلى داخل نظام التحكم والسـيطرة في خط انابيب الغاز في الدولة (ج) ، مما يتسـبب بحدوث انفجار ، وبالتالي بما ان الدولة (أ) تصـرفت بشـكل

---

(1) Ibid, Rule(6) , p.32.

(2) Tallinn manual 2.0 , op . cit , Rule (6), p. 33.

مخالف للقانون فيما يتعلق بالدولة (ج) ، يجب ان تتخذ الدولة (ب) التدابير اللازمة لأنهاء هذه العملية ، اذا كانت لديها القدرة على فعل ذلك[١].

ثانياً: شروط تطبيق واجب العناية اللازمة

تلتزم الدول عموماً بضرورة تطبيق واجب العناية من خلال استخدامها للفضاء المعلوماتي والحفاظ على حقوق الدول الاخرى على وفق مبادئ القانون الدولي العام، ولكن هذا الالتزام الذي يقع على عاتق الدول محدد بشروط معينة وهي :-

١- شرط المعرفة أو العلم

لكي تلتزم الدولة بواجب منع الأنشـــطة المعلوماتية التي تنطلق من اراضـــيها ، أن تكون على معرفة أو دراية بانه هناك خطراً يهدد مصالح وحقوق الدول الاخرى ، وأن هذا الخطر سوف يصدر من داخل إقليمها ، إذ أن العلم بهذا النشاط ومعرفته يشكل عنصراً هاماً وحاسماً في اتخاذ واجب العناية من قبل الدولة لمنع الضـرر العابر للحدود[٢]. وتجدر الاشـارة إلى أن مجرد حدوث تهديد من اقليم دولة معينة أو ممارســـة بعض الحقوق الســـيادية على الاقليم لا يكون مبرراً أن هناك واجب يقع على الدولة ان تكون على علم بهذا التهديد[٣]. وفي سياق الهجمات المعلوماتية ان مجرد الإشـــتباه بوجود هجمة معلوماتية انطلقت من جانب البنية التحتية المعلوماتية الحكومية لا يعد ذلك دليلاً كافياً لإسـناد العملية لتلك الدولة، بل هي ربما تكون مؤشـر على ارتباط الدولة المعنية بهذه العملية[٤].

---

(1) Ibid, Rule (6) , p.34.

(2) Karine Bannetier – Christakis , cyber diligence ; A law – intensity Duediligence principle for low – intensity cyber operatio ? , Baltic yearbook of inter national – law , 2014 , vol . (14) , p28 .

(3) ICJ , corfu channel case (United Kingdom of Great Britain and northern Ireland V.Albania , 1949, p18 .

(4) Tallinn manual , op . cit , rule (7) .

كما أن حقيقة تنفيذ هجمة معلوماتية أو شنها من خلال البنية التحتية المعلوماتية الخاضعة لسيطرة دولة معينة ، لا يعد دليلاً كافياً لإسناد تلك الهجمة لهذه الدولة ، أو افتراض ان تكون هذه الدولة على علم بذلك[١]. فعلى سبيل المثال أن المحكمة التي تنظر في مسألة معرفة الدولة بوجود التهديد وتتهيأ للفصل فيها ، ينبغي لها أن تتأكد من توافر شرط المعرفة بصورة حتمية لا تمكن الدولة من إنكارها ، كحالة نشر الخبر وحالة التهديد في وسائل الاعلام الحكومية وغيرها من وسائل الاعلام التابعة لجهات خاصة[٢]. وبهذا الصدد ترى محكمة العدل الدولية أن الحالة التي تكون فيها الدولة تعلم بوجود التهديد بالصورة الطبيعية وبحسب الظروف فأن هذا يكفي لتحملها المسؤولية الدولية[٣].

وعلى أية حال، فأن وجوب العلم بوجود التهديد في ظل الظروف الطبيعية ، يشمل ايضاً قدرات الدولة الموجة من أراضيها التهديد، اذ لا يمكن أن يتوقع من دولة اقل تقدماً في المجال التقني كشف التهديدات المعلوماتية بحسب الظروف والاحوال التي تقوم بها دولة متقدمة بهذا المجال ، وذلك نظراً لسرعة تطور الهجمات المعلوماتية وطبيعتها المعقدة [٤]. وهذا ما اكدته محكمة العدل الدولية من أن التزام الدولة بمنع حدوث الضرر يكون على اساس تلك التدابير المعقولة والمتوافرة (reasonably available) لدى تلك الدولة والتي يكون في وسعها وقدرتها (within its power) إستخدام هذه التدابير [٥].

---

(1) Ibid , rule (8) .

(2) Russell Buchan , cyber space Non, state Actors and the on the obligation to prevent Transbooundary Harm, journal of conflict a security Law , oxford university press, Vol, (21), No. 3, 2016, p.33 .

(3) Icj , bosnia Genocide case , Concerning application of the Convention on the prevention and punishment of the crime of Genocide judgment of 26, February, 2007 , para 432 , p223 .

(4) Russel Buchan , op. cit , p 441 .

(5) Icj , bosnia genocide case , op . cit , para 430 , p221.

ومن الجدير بالذكر أن من الممكن أن يتغير مستوى واجب العناية المطلوبة من القيام به مع مرور الزمن او حصول بعض التغيرات الهامة كالتقدم التقني والعلمي [١]. أما بالنسبة لالتزامات دول العبور فيما يخص شرط العلم والمعرفة بالنشاط المعلوماتي الضار، فغالبا ما يتم توجيه هجمات معلوماتية عبر عدة دول قبل الوصول إلى اهدافهم النهائية ، ويهدف المهاجمون من وراء ذلك إخفاء هوية منفذ الهجوم ، إذ تعمد الدول في الغالب إرسال رسائل كيدية عبر الأنترنت للأضرار بدولة أخرى بالاعتماد على إعادة إرسال هذه الرسائل من مكان أخر من دولة أخرى ، وتكون هذه الدولة على علم بان تلك الرسائل المعلوماتية تكون سبباً بأحداث ضرراً بدولة أخرى. ولكن هذا لا يعني أن الدول ملزمة دائماً بموجب القانون الدولي بمنع الأنشطة الضارة، إذا لم يكن لديها علم بهذه الانشطة ، فقد أشارت محكمة العدل الدولية في قضية قناة كورفو ان الالتزام بأخطار السفن البحرية بوجود الغام كانت تعتمد في ذلك على علم الدولة ومعرفتها بهذه الحقيقة في وقت كافٍ يسبق التاريخ الذي ضربت فيه هذه الالغام السفن البحرية[٢].

على أية حال، ليس من المعقول ان تنشأ مسؤولية الدولة جراء عدم التزامها بذلك اذا لم تكن على علم بهذه الالغام، وعلقت محكمة العدل الدولية كذلك " ان ذلك لا يمكن إستنتاجه من مجرد حقيقة السيطرة التي تمارسها الدولة على الأراضي والمياه الخاضعة لها ، أو بعبارة اخرى أن الدول ليس لديها معرفة مطلقة بكل شيء بما يحدث على أراضيها ، و مع ذلك قد يكون من المعقول إن نطلب من الدولة بذل قصارى جهدها لاكتساب المعرفة بالنشاط داخل أراضيها أو ولايتها القضائية "[٣].

---

(1) ITLOS , Responsibilities and obligations of states sponsoring persons and Entites with respected activities in the Area , op . cit , para 117 , p36 .

[٢] سكوت جيه شاكلفورد، وأخرون، تفريغ القانون الدولي بشأن العناية الواجبة في مجال الأمن السيبراني، دروس من القطاعين العام والخاص، مجلة شيكاغو الدولية، م (١٧)، ع (١)، متاح على الموقع الالكتروني https://chicagounbound.uchicago.edu/cji/. تاريخ الزيارة ٢٠٢١/١٢/٢٦.

[٣] رابطة القانون الدولي (ILA) ، فريق الدراسة حول العناية الواجبة في القانون الدولي، التقرير الثاني ، ٢٠١٦، ص١٢.

وقد تناول دليل تالين شـــرط العلم والمعرفة من خلال نصـــه على أنه " بمجرد أن تكون الدولة على علم بالهجمة المعلوماتية يجب على الدولة اتخاذ جميع التدابير المتاحة بشكل معقول لوقف هذه الانشطة الضارة عبر الأنترنت وفي حال فشل الدولة في ذلك أو عدم قيامها في الوفاء بهذا الالتزام يحق للدولة المعتدى عليها اللجوء إلى حق الدفاع الشرعي أو التدابير المضادة للرد على هذه الافعال غير المشروعة دولياً[١].

ويمكننا القول أن دليل تالين يعطي مثالاً للدولة عن كيفية امتلاكها معرفة فعلية عندما تكتشف وكالات استخباراتها وجود نشاط معلوماتي ضار ينطلق من داخل أراضيها ، أو اذا تلقت الدولة معلومات موثوقة حول فعل هذا النشاط ولكن المشكلة الرئيسية تكمن في كيفية إثبات أن الدولة كانت على علم أو معرفة بهذه الانشطة الضارة؟

والسؤال الذي يطرح بهذا الصدد ما إمكانية تطبيق واجب العناية عندما تكون الدولة على علم بهذه الهجمة المعلوماتية؟ خلص فريق الخبراء الدوليين في دليل تالين انه اذا لم تكن الدولة على علم بهذه الهجمة المعلوماتية الضارة ، فأنه يقع عليها واجب التقصي عنها وبذل قصارى جهدها للوصـــول إلى حقيقة المعرفة بها ، وتبقى أيضـــاً هناك امكانية تطبيق واجب العناية في سياق العلم والمعرفة من خلال السوابق القضائية بهذا الصدد، فقد خلصت محكمة العدل الدولية في قضية قناة كورفو سالفة الذكر "ان البانيا كانت ينبغي ان تعرفها " و ذهب بهذا الاتجاه فريق الخبراء الدوليين إلى إن هناك مجموعة من العوامل المؤثرة في مدى معرفة النشاط الضار، على سبيل المثال قالوا أنه من المرجح ان تلتقي الولاية بمعيار " كان يجب أن يعرف" اذا كانت البنية التحتية المعلوماتية الحكومية للدولة موجودة ، بدلاً من استخدام بنية تحتية خاصة ، وهناك عامل مؤثر اخر للدلالة على حصول علم الدولة ومعرفتها بالنشاط المعلوماتي هو اذا كان هذا النشاط

---

(1) Tallinn Manual . op.cit, Rule (7).

من النوع الذي يتم اكتشافه دائماً بشكل عام ، فمن السهل أن ينسب للدولة إذا كانت على علم ومعرفة بهذه الإنشطة المعلوماتية الضارة[١].

٢- شرط معقولية ومرونة واجب العناية

أن مبدأ واجب العناية من غير الممكن ان يفرض عبئاً غير معقول على الدول ، ويمكن تبرير ذلك ان شرط المعقولية والمرونة غالباً ما يتم في الواقع بوصف واجب العناية على أنه كمعيار معقول لسلوك الدولة ، إذا انه مفهوم مرن فقط ينص على أن تعمل الدولة بجدية على النحو الواجب ولا يهتم بالنتيجة النهائية ، وبالتالي فهو التزام بسلوك وليس إلتزام بتحقيق نتيجة لأنه يميل إلى التركيز على سلوك الدول بدلاً من نتائجها ، وهذا الالتزام يعني بسهولة ويسر أن الدولة مطالبة باتخاذ التدابير المعقولة التي تتماشى مع مبدأ واجب العناية ، وهذا ما يمكن تطبيقه في نطاق الضرر العابر للحدود ، فعلى سبيل المثال أن الدول غير مطلوب منها فعل اكثر مما هو ممكن بمنع الهجمات المعلوماتية فهي بالتالي ليست ملزمة بمراقبة جميع الأنشطة الضارة على أراضيها، حيث أن مسألة تكييف هذا الشرط بسهولة يعتمد بالدرجة الاساس على السياق المطلوب من الدول، ومما لاشك فيه أن من الصعب تحديد ما هو معقول ، ولكن من الضروري القول أن معيار واجب العناية يشير إلى أن الدول لديها التزامات مختلفة متعددة بالاعتماد على الظروف التي تحدث وتنشأ من خلالها هذه الالتزامات ، وينبغي كذلك الاشارة ضمناً إلى أن الدول تتمتع بسلطة تقديرية واسعة في إختيار وسائل منع الهجمة المعلوماتية الضارة[٢].

ومن العوامل الاخرى المهمة والمؤثرة في شرط المعقولية على سبيل المثال هي (السيطرة على الارض وتحديد درجة الخطر ، ووجود أو غياب أفعال حسنة النية) ، كما ان حكم محكمة العدل الدولية في قضية الرهائن الأمريكيين في طهران قد تبنت هذا الشرط في قولها المأثور "

---

[١] الجمعية العامة للأمم المتحدة، فريق الخبراء الحكوميين المعني بالتطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي (٨/٧٠/١٧٤) ٢٢ تموز/ يوليو ٢٠١٥.

[٢] ايرين كوزيجو، تأمين الفضاء السيبراني- التزام الدول بمنع الفضاء السيبراني الدولي الضار، متاح على الموقع الالكتروني :

https://translate.googeluserontent.com تاريخ الزيارة ٢٠٢٢/١/٢٤.

يتعين على الدول أن تتخذ فقط الخطوات المناسبة لمنع الضرر الذي يلحق بدولة ثالثة اذا كان لديها من الوسائل الموجودة تحت تصرفها لإداء التزاماتها " علاوة على ذلك فان ما جاء بالتعليق على مواد لجنة القانون الدولي بشأن مسؤولية الدولة ومدى التزامها بالوقاية التي تعتبر بمثابة واجب العناية التي تلتزم بها الدول " عادة ما تفسر على إنها افضل الجهود التي تتطلب من الدول اتخاذ جميع التدابير المعقولة أو اللازمة لمنع حدث معين من الحدوث ، ولكن دون ضمان ان هذا الحدث لن يقع "[١].

علاوة على ذلك يعبر عن شرط المعقولية من خلال فهمه على انه شرط لسلوك الدولة الذي يعد بمثابة المعيار المعقول في الظروف السائدة، وقد تناول الخبراء الدوليين شرط المعقولية والمرونة في دليل تالين سالف الذكر والذي تضمنته القاعدة (٦) من هذا الدليل على انه " اذا كان من غير المعقول توقع أن تكون دولة الإقليم على علم بالعملية في الدولة المضيفة وفي ظل ظروف معينة ولكي تكون قادرة على انهائه..." ، ولقد تناولت القاعدة (٧) من دليل تالين شرط المعقولية بشيء من التفصيل حول امتثال الدول لواجب العناية ، الذي ينص على انه "يتطلب مبدأ واجب العناية ان تتخذ الدولة جميع التدابير اللازمة ، والتي من الممكن في ظل ظروف معينة ، وضع حد للعمليات المعلوماتية التي تؤثر على حقوق الدول الاخرى"، وتؤدي إلى عواقب وخيمة بالنسبة لها[٢].

توضح القاعدة (٧) آنفة الذكر أن من واجب الدولة الإقليمية إتخاذ جميع التدابير المتاحة بشكل معقول لمنع أو وقف الهجوم ، كما أوضحت مجموعة رابطة القانون الدولي أن الدول النامية قد لا يكون باستطاعتها السيطرة على الأنشطة داخل أراضيها في منطقة مماثلة بالنسبة لما تفعله الدول المتقدمة ، وان هذا سيؤثر على تقييم ما اذا كان لديهم فرق التزام بواجب العناية

---

[١] رابطة القانون الدولي ILA، فريق الدراسة حول العناية الواجبة في القانون الدولي، مصدر سابق، ص٤٧.

[2] Tallinn Manuall, op.cit, comment on Rule (7).

، كذلك قد يتم السماح لدولة نامية وذات قدرات محدودة باستخدام اقل اجتهاد من الدول المتقدمة بمنع هذا الضرر الناشيء عن الانشطة المعلوماتية[١].

وبناء على ما تقدم نستطيع القول ان قدرات الدول تتفاوت بمستويات مختلفة، فقدرات الدول المتقدمة تكون ذات مستوى عالٍ من التطور اللازم لمنع الهجمات المعلوماتية الضارة وهي أفضل بكثير من قدرات الدول النامية التي غالباً ما تكون قدراتها الفنية محدودة، إذ أن مسألة تقييم شرط المعقولية والمرونة يمكن قياسه تبعاً لظروف كل دولة على حده، وعليه فان تطبيق هذا الشرط بالنسبة لواجب العناية من غير المستساغ ان يكون عبئاً على الدول .

الفرع الثاني

التزامات الدول في الفضاء المعلوماتي

إن غياب المعاهدات والاتفاقات الدولية الخاصة في تنظيم الهجمات في الفضاء المعلوماتي، كان له أثر سلبي على عدم استقرار الدول وبالتالي يشكل تهديداً للأمن والسلم الدوليين. فضلاً عن عدم التزام الدول بمنع الهجمات المعلوماتية الذي غالباً ما يصطدم بمبدأ سيادة الدولة على ولايتها الإقليمية والقضائية، وهذا يشكل أهم التحديات التي يواجها القانون الدولي في ظل غياب تطبيق هذه القوانين ذات الصلة بوجود نزاع مسلح دولي، خصوصاً إذا ما

---

[١] رابطة القانون الدولي ILA، فريق الدراسة حول العناية الواجبة في القانون الدولي، التقرير الاول، ٢٠١٤، ص١٢٧.

علمنا أن الأمم المتحدة وفقاً لصـــلاحياتها يحق لها ان تخول مجلس الأمن بأســتخدام القوة لحفظ السلم والأمن الدوليين، أو إستعادته إذا اختل نصـابه، إلا أن مجلس الأمن الدولي لا يمتلك قوات دائمة موضوعة تحت تصرفه للقيام بواجبه في حال مخالفة تطبيق قواعد القانون الدولي الخاصـة بسوء إستخدام الانشطة المعلوماتية غير المشروعة دولياً.

ولكن على الرغم من ذلك؛ فأن هذا لا يعني ان الدولـة لا يمكن ان تتمتع بحريـة مطلقة للتصـرف من خلال فضـائها المعلوماتي ، إذ يرى البعض من المختصـين في القانون الدولي ان المبادئ العامة ذات الصـلة بالفضـاء المعلوماتي ربما تشكل الحجر الاساس لإنشاء قوانين دولية خاصـة بالفضـاء المعلوماتي، والسؤال الذي يطرح بهذا الصـدد ماالمقصـود بالفضـاء المعلوماتي؟ وماهي السـيادة المعلوماتية ؟ وما أثر الهجمات المعلوماتية على مبدأ السـيادة؟ للاجابة عن هذه التساؤلات سنتناول بشيء من التفصيل معنى الفضاء المعلوماتي والمقصود بمفهوم السيادة وعلى النحو الآتي:

أولاً : الفضاء المعلوماتي:

يقصـــد بالفضـــاء المعلوماتي : هو مجال افتراضـــي من صـــنع الانســـان يعتمد على نظم الحاســـوب وشـــبكات الانترنت وكم هائل من البيانات والمعلومات والاجهزة ، كما ان هناك من يوصـــفه بالذراع الرابعة للجيوش الحديثة[١]. إلا أنه يؤخذ على هذا التعريف أنه جاء قاصـــراً على إستخدامات الفضاء المعلوماتي للاغراض العسكرية فقط.

وهناك عدة تعريفات طرحت بهذا الشـأن، فقد عرفته الوكالة الفرنسـية لأمن انظمة الاعلام (ANssi)على انه " فضـاء التواصـل المشـكل من خلال الربط البيني العالمي لمعدات المعالجة الاتية للمعطيات الرقمية"[٢]. وهذا التعريف يرتكز على الجانب التقني كما يغفل الجانب البشري ، و الذي يعد جزءاً أساسياً في فهم الفضاء المعلوماتي.

---

[١] عباس بدران ، الحروب الالكترونية الاشـــتباك في عالم المعلومات ، مركز دراســـات الحكومة الالكترونية ، بيروت ، ٢٠١٠ ، ص٤ .

[2] Oliver kempf , introduction a'la cyber strategie , paris , economica , 2012 , p,9 .

كذلك عرفه الاتحاد الدولي للاتصـــالات (Inter national Telecommunication Union) على انه " المجال المادي وغير المادي الذي يتكون و ينتج من عناصـــر هي : اجهزه الحاسـوب ، الشـبكات ، البرمجيات ، حوسـبة المعلومات ، المحتوى ، معطيات النقل والتحكم ، ومستخدموا كل هذه العناصر"[١]، وعرفهُ البعض الأخر على أنه "المجال المعلوماتي الذي يسمح بالتواصل العالمي بين الأفراد والكيانات والدول وتداول المعلومات وبيان تخزينها، وهو يتشكل من تفاعل العنصر البشري من مستخدمين ومشغلين مع العديد من الوسائل الخاصة بالتقنية كأجهزة الحاسب الآلي، وشبكة الانترنيت، وبرامج التشغيل، ويمكن من خلاله توجيه عمليات مثل (التسلل المعلوماتي، والجريمة المعلوماتية، والهجمات المعلوماتية، والحرب المعلوماتية، والتجســـس المعلوماتي)، والتي تشترك في كونها تمثل اختراقاً للأنظمة المعلوماتية للدولة الضحية"[٢].

ومن ابرز الأمثلة على اســتخدام الفضـــاء المعلوماتي في تنفيذ انشـــطة معلومات غير مشروعة هي عملية "القنابل المعتمة"، نهاية القرن العشرين، اثناء قصف حلف شمال الاطلسي (الناتو) لصـــربيا، إذ تســببت هذه العملية في شـــل أنظمة الحاســوب الخاصـــة بوزارة الدفاع ليوغسلافيا، كذلك أدت العملية إلى التشويش على أنظمة الاتصالات[٣].

ومن الجدير بالذكر أهم العوامل التي ساعدت على إنتشار الانشطة غير المشروعة في الفضاء المعلوماتي هي[٤]:

---

(1) The international telecommunication union , ITu tookit for cyber crime legislation , Geneva , 2010 , p12 .

(2) U.M.Mbanaso, and E.S.Dandaura, the cyber space : Redefining A New, world, IOSR journal of computer engineering, center for cyber space studies , Nasarawa state unvirsity, Vol.(17), ISSUe.3 Ver. VI, Nigeria, 2015, p.18.

[٣] علاء الدين فرحات وعمروس عمارة، الفضـــاء الســـيبراني وتأكل مفهوم الســـيادة الوطنية، المجلة الجزائرية للدراسات السياسية، م (٨)، ع (٢) ، الجزائر، ٢٠٢١، ص١٦٨.

[٤] د.عادل عبدالصاحب، أسلحة الفضاء الالكتروني في ضوء القانون الدولي الانساني، مصدر سابق، ص١٧-١٨.

١- ارتباط العالم المتزايد بالفضـــاء المعلوماتي وزيادة خطر تعرض البنية التحتية الكونية للمعلومات لهجمات معلوماتية.

٢- استخدام الفاعلين من غير الدول للفضاء المعلوماتي لتحقيق أهدافهم وتأثير ذلك على سيادة الدولة.

٣- انسحاب الدولة من قطاعات إستراتيجية والتخلي عنها لصالح القطاع الخاص.

٤- إشكالية تعاون الدول مع الشركات التكنولوجية متعددة الجنسيات التي أضحت تتفوق على قدرات الدول، مثل مواقع التواصل الاجتماعي كالفيسبوك، وتويتر، واليوتيوب، وغيرها من المواقع الاخرى.

وعليه يمكن القول بأن الفضاء المعلوماتي هو بيئة تفاعلية حديثة ، تشمل عناصر مادية وغير مادية ، والمستخدمين لهذا الفضاء هم من المشغلين والمستعملين ، علاوة على ذلك إن مسألة تحديد مفهوم الفضاء المعلوماتي هي مسألة تتوقف على طبيعة ادراك وفهم كل من الدول والهيئات كل حسب رؤيته وإستراتيجية وقدرته على استغلال المزايا المتاحة ومواجهة المخاطر الكامنة في هذا الفضاء.

ثانياً: مفهوم السيادة المعلوماتية:

يعد مفهوم السيادة والاعتراف بها من قبل الدول من المبادئ المتفق عليها في ميثاق الأمم المتحدة والاتفاقيات الدولية ذات العلاقة بسيادة الدول، كما يرتبط مفهوم مبدأ السيادة في القانون الدولي العام مع نشـــوء الدولة الحديثة في أوربا بعد معاهدة وســـتفاليا عام ١٦٤٨، إذ أن هذه المعاهدة أقرت مفهوم سيادة الدولة، باعتبار هذهِ السيادة هي السلطة العليا والمطلقة على إقليمها، دون تدخل من الدول الآخرى.[١]

---

[١] محسن افكيرين، القانون الدولي العام، ط١، دار النهضة العربية، ٢٠٠٥، ص٣٤٦.

وأول من نادى بفكرة السـيادة هو الفقيه الفرنسـي جان بودان (jean Bodin) إذ عرف بودان السـيادة من خلال مؤلفه المشـهور الكتب السـتة للجمهورية (Les six Livers La Republigue) والذي تم نشـره في سـنة ١٥٧٦ بأنها "سـلطة الدولة العليا المطلقة والابدية الحازمة والدائمة التي يخضع لها جميع الافراد رضاءاً أو كرهاً".[١]

ومن الجدير بالذكر أن هناك مبادئ وأهداف عامة للقانون الدولي يكون من الجائز تطبيقها على الفضـاء المعلوماتي الذي تجري من خلاله العمليات المعلوماتية ويكون لها مساس بالسيادة المعلوماتية للدول وهي:- حفظ السلم والامن الدوليين ، المساواة في السيادة بين الدول الاعضاء ، وواجب التعاون الدولي. و هذه المبادئ والأهداف العامة تعمل كقاعدة اساسية لتطوير القوانين الخاصة في استخدام الأنشطة المعلوماتية والذي أضحى تطورها سريعاً في الفضاء المعلوماتي، لذا سنتناول مفهوم السيادة المعلوماتية في ضوء بعض مبادئ وأهداف القانون الدولي العامة، ففي ضوء المبادئ العامة للقانون الدولي يتجسد واجب العناية على وفق الآتي:

١- المساواة في السيادة بين الدول:

لم تعد السيادة كما كانت عليه في ظل المفهوم التقليدي لها بعد تحولها إلى سيادة نسبية بعد ان كانت سيادة الدول على اقليمها هي سيادة مطلقة لا يجوز المساس بها ، فلا يمكن بأي حال من الاحوال التمسك بمبدأ السيادة المطلقة في ظل ازدياد وتشابك حزم الانترنت ودخولها الفضاء المعلوماتي بصورة متسارعة دون السيطرة عليها نتيجة لكثافتها وسرعة تطورها ، فالفضاء المعلوماتي يمتاز بالعديد من العناصـر المرئية وغير المرئية وتبادل الروابط بين القطاعين العام والخاص ، والشـركات والافراد ونتيجة لذلك يتفرع عن مبدأ المسـاواة في السـيادة بين الدول الأعضـاء، مبدأ السـيادة الإقليمية والولاية القضـائية، ففي سـياق السـيادة الاقليمية ذات العلاقة بالفضـاء المعلوماتي ووفقاً لمبدأ السـيادة فأن الدول لها كامل الحرية في ممارسـة حماية جميع الانشطة التي تجري داخل اقليمها وولايتها القضائية ولكن هذه الممارسة أو الحماية مقيدة بشرط

---

[١] جان بودان، اصول السلطة والسيادة، متاح على الرابط الالكتروني:
http://www.marafa.org. تاريخ الزيارة ٢٠٢٢/٢/٧

عدم الإضـــرار بحقوق الدول الأخرى ، ونتيجة لذلك يقع عليها واجب حماية البنية التحتية المعلوماتية الموجودة داخل اقليمها وتحت ولايتها القضـائية ، فضـلاً عن ذلك فإن الاختصـاص القضـائي الذي تمارسـه الدولة ينطبق أيضـاً على جميع الأجهزة الموجودة داخل اقليم الدولة، وكذلك فأن أي نشـاط معلوماتي معادي يتم من اقليم أحدى الدول أو ولايتها القضـائية ويسـبب ضـرراً مادياً لدولة اخرى يعد انتهاكاً لسـيادة تلك الدولة المضـرورة من هذا النشـاط المعلوماتي، وبالتالي ينتهك ســيادتها الاقليمية[١]، مثال على ذلك ما حدث عام ٢٠١٠ من خلال اطلاق البرنامج الضـار (stuxnet) الذي أسـتهدف الإضـرار بالبرنامج النووي الايراني في منشـآت نطنز النووية حيث تسبب هذا الفيروس بأصابة وتدمير واسع النطاق داخل هذه المنشآت وبالتالي تم تصـنيف الهجوم من بعض الخبراء هجوماً مسـلحاً معلوماتياً ، إلا أن الخبراء قد اختلفوا فيما بينهم حول كيفية تصـنيف هذا الهجوم وعده عملاً من أعمال القوة الذي يشـكل هجوماً مسـلحاً بسبب أن الانشطة المعلوماتية الضارة يمكن ان تؤدي ايضاً إلى أحداث أضرار أو تأثيرات غير مادية ، ومع ذلك فهي مرئية وتؤدي لانتهاك سـيادة الدولة من خلال أحداث اثار مادية ملموسـة على البنيـة التحتيـة للدولـة نتيجـة هذه العمليات المعلومـاتيـة وتعمدها انتهـاك ســـيادة الدولـة الاقليمية[٢]. ومثال أخر على انتهاك السـيادة الإقليمية هو ذلك الهجوم الذي تعرضـت له شـبكة التوزيع الكهربائية لدولة اوكرانيا ، مما ادى إلى انقطاع التيار الكهربائي ، كذلك يعد التجســـس المعلوماتي هو الآخر نشـاط معادي يؤثر على سـيادة الدولة ، لكن من الواضـح أن التجسس تم التغاضـــي عنه دولياً في ظل عدم وجود أي معاهدة دولية محددة تنظم التجســس المعلوماتي أو السـيطرة على هذه الممارسـات غير الشـرعية، ومع ذلك فأن التجسـس المعلوماتي قد يكون غير قانوني عندما يتعارض مع المبادئ العامة للقانون الدولي وعلى وجه الخصـوص مبدأي السـيادة

---

[١] تشير كوب، لوك، السيادة الاقليمية في الفضاء الالكتروني، مجلة بلورن للقانون الدولي، ٢٠١٩، متاح على الموقع الالكتروني:

https://classic.austil.edu.au. تاريخ الزيارة ٢٠٢٢/٣/١٢.

[٢] د.عدنان النقيب، الحرب الالكترونية في ضوء بروتوكولي سبع وسبعين الملحقين باتفاقات جنيف الاربع سنة تسع واربعين، (الهجمات السيبرانية)، ط١، المركز العربي للنشر والتوزيع، القاهرة، مصر، ٢٠٢٢، ص٧٩.

الإقليمية وعدم التدخل في شـــؤون الدول، اللذان ينطبقان أيضـــاً على التجســـس في الفضـــاء المعلوماتي.[١]

وبالتالي يحتم مبدأ السـيادة الإقليمية والولاية القضـائية عدم السـماح باسـتخدام اراضـيها السيادية للأنشطة التي تسبب احداث اضرار تلحق بالأشخاص او الاشياء التي تحميها سيادة دولة اخرى ، يقع كذلك على الدولة التزاماً باتخاذ تدابير وقائية في بعض الحالات التي تكون فيها الدولة لديها معرفة أو إفتراض بوجود خطر فعلي لإلحاق ضـرر بالدول الاخرى ، ومصـدر هذا الخطر أراضـي دولة اخرى خاضـعة لسيادتها وولايتها القضـائية ، فضـلاً عن ذلك فأن الدولة ملزمة باتخاذ تدابير إحترازية فيما يتعلق بالتهديدات المعلوماتية التي تشـــكل خطراً دولياً عابراً للحدود الإقليمية وهذا الالتزام يشمل ايضاً الانشطة المعلوماتية التي تقوم بها الجهات الفاعلة غير الحكومية والناشئة من اراضي الدولة الاخرى والتي تستهدف الاضرار بحقوق الدولة الاخرى[٢].

٢- **مبدأ عدم التدخل في الشؤون الداخلية للدول** : أن مبدأ عدم التدخل هو من المبادئ الأساسية للأمم المتحدة وهو ضمانة أكيدة من ضمانات سيادة الدولة، ولأهمية هذا المبدأ فقد ورد ذكره في الفقرة السابعة من المادة الثانية من ميثاق الأمم المتحدة لعام ١٩٤٥، إذ نصت على أنه " ليس في هذا الميثاق ما يســمح للأمم المتحدة أن نتدخل في الشــؤون التي تكون من صــميم السلطان الداخلي لدولة ما.."، ويتضـمن هذا المبدأ عدم التدخل في الشؤون الداخلية أو الخارجية للدول الاخرى، ولغرض تطبيق هذا المبدأ في الفضـــاء المعلوماتي واعتبار الفعل الصـــادر من الدولة انتهاكاً لمبدأ التدخل يجب أن يكون هناك إكراه، فعلى سـبيل المثال عندما تقوم دولة معينة بأنشـطة معلوماتية قسـرية للتأثير على عملية صـنع القرار والتأثير على سيادة الدولة الاخرى كما

---

[١] راسـل بوكان، اللائحة القانونية الدولية للتجسـس السـيبراني التي ترعاه الدولة في المعايير السـيبرانية الدولية، منشورات الناتو، تالين، ٢٠١٦، ص٦٨.

[٢] خانا بالافي، سيادة الدولة والدفاع عن النفس في الفضاء السيبراني، متاح على الموقع الالكتروني: https://cyberieninka.ru. تاريخ الزيارة ٢٠٢٢/٤/٢٧.

هو الحال في الانشـــطة المعلوماتية الصـــادرة من بعض الوكالات الاجنبية ، وقد لا تكون هذه الانشطة قسرية اذا طلبت الدولة المضيفة من دولة اخرى الاذن بتنفيذ مثل هذه الانشطة.[١]

ووفقاً لما تقدم نستطيع القول: أن الدولة ملزمة بأعمال مبدأ المنع الذي يوجب على الدول إبلاغ الدول الاخرى في حالات الضـرر الجسيم العابر للحدود ، كما هي ملزمة أيضـاً من خلال أتخاذ التدابير الوقائية والاحترازية قبل وقت طويل من حدوث مثل هكذا اضرار.

أما أهم الأهداف الرئيســـية للقانون الدولي العام التي تبنتها الأمم المتحدة ذات العلاقة بالسيادة هما: الحفاظ على السلم والأمن الدوليين، والتعاون والتضامن الدولي.

١- الحفاظ على السلم والأمن الدوليين:

وهو من الأهداف الرئيســية للقانون الدولي التي تبنتها الأمم المتحدة ولا زالت تســعى إلى تحقيقهـا، فـالأمر لا يتوقف على غيـاب حـالـة الحرب فقط بـل يعني أكثر من ذلـك من خلال القضــاء على كل التهديدات التي تمس الســلم والأمن الدوليين واتخاذ جميع التدابير اللازمة التي تســهم في تعزيز الأمن والســلم الدوليين وهو هدف أســاســي للحفاظ على العلاقات الدولية إذ أن بموجبه تمتنع الدول عن اللجوء لإستخدام القوة ، أو التهديد بها ، كما تسـعى الدول إلى حل أي نزاع دولي قائم او على وشـك الحدوث بالطرق السـلمية والتخلي عن أسـتخدام القوة في العلاقات الدولية، إذ أن مسـألة اسـتخدام الأسـلحة في الفضــاء المعلوماتي ، يشـكل تهديداً خطيراً لأمن وسيادة الدول وبهذا الصدد يرى مايكل ن . شميت ومجموعة من الخبراء القانونيين الذين وضـعوا دليل تالين المطبق على الحروب المعلوماتية ، أن مســـألة تدمير البيانات لا تعد بحد ذاتها اسـتخداماً للقوة المسـلحة ، كما هو الحال في أحداث أصـابات أو وفيات أو أحداث آثار تدميرية مباشـرة وغير مباشـرة ، إلا أن النزاعات غير المحسـومة تحدث فوضــى داخل المجتمع الدولي وبالتالي تؤدي إلى عدم الاستقرار الذي يهدد الأمن والسلم الدوليين ، لذلك من الضـروري أن يقع

---

[١] مايكل أن شميت، احترام السيادة في الفضاء المعلوماتي، متاح على الموقع الالكتروني : https://texaslawreview.org. تاريخ الزيارة ٢٠٢٢/٣/٢.

التزام على الدول يوجب عليها تسـوية النزاعات بالطرق السـلمية والابتعاد عن اسـتخدام القوة أو التهديد، حتى في سياق تطبيق هذا المبدأ على الفضاء المعلوماتي.[١]

٢- التعاون والتضامن الدولي:

أن من أهم الأهداف الرئيسـية للأمم المتحدة هي تحقيق التعاون الدولي في إطار العلاقات الدولية إلا أنه لم تتضـح بعد معالم وجود اساس قانوني وواجب عام للتعاون فيما بين الدول وبين الدول والمنظمات الحكومية الدولية من خلال إبرام الاتفاقيات الدولية ذات الصلة بواجب التعاون، كذلك تم اقرار واجب التعاون في ميثاق الامم المتحدة وهذا الواجب يجب اقراره كمعيار يقع على عاتق الدول بالالتزام بالتعاون الدولي لدعم حفظ السـلم والامن الدوليين ، أما في سـياق الفضـاء المعلوماتي فان مصطلح التعاون الدولي هو مصطلح غامض بعض الشيء اذ لم يتم تعريفه من خلال معاهدة دولية أو تضـمينه في وثيقة اخرى متعددة الاطراف، ومن الممكن النظر إلية على انه عمل مشـترك طوعي واسـتباقي لدولتين أو اكثر يخدم دولة معينة وبالتالي الدفاع عن القيم والمصـالح المشـتركة، ونتيجة تطور الفضـاء المعلوماتي تطوراً متسـارعاً فقد منح فضـاءً مشـتركاً لجميع الدول من خلال الاعتماد المتبادل لتداول البيانات والمعلومات عبر هذا الفضـاء الذي يصـب في مصـلحة المجتمع الدولي ، إلا انه في ذات الوقت يقع على الدول التزام قانوني بالتعاون فيما بينها للحد من استخدام الانشطة المعلوماتية غير المشروعة التي تهدد الأمن والسلم الدوليين ، ومع ذلك تتمتع الدولة بسـلطة تقديرية واسـعة فيما يتعلق بكيفية القيام بهذا الواجب القانوني أو الوفاء به[٢].

ومن الجدير بالذكر أن ميثاق الامم المتحدة أولى مفهوم السـيادة أهتماماً واسـعاً على المسـتوى الدولي، إذ تناولت محكمة العدل الدولية وهي الجهاز القضـائي للأمم المتحدة تعريف

---

[١] شـريف نسـيم قلته، دليل تالين، الهجمات الالكترونية وحظر اسـتخدام القوة في القانون الدولي، المركز العربي لابحاث الفضاء الالكتروني، متاح على الرابط الالكتروني:
https://accronline.com. تاريخ الزيارة ٢٠٢٢/٤/٦.

[٢] كاترينا زيولكوفسكي، المبادئ العامة للقانون الدولي كما تنطبق في الفضاء السيبراني، في وقت السلم لانشطة الدولة في الفضاء الالكتروني والقانون الدولي والعلاقات الدبلوماسية، الناتو، تالين، ٢٠١٣، ص١٧٢.

السيادة في قضية مضيق قناه كورفو سنه ١٩٤٩ سالفة الذكر، على ان " السيادة بحكم الضرورة هي ولاية الدولة في حدود إقليمها ولاية إنفرادية ومطلقة " وان احترام السيادة الاقليمية فيما بين الدول المستقلة يعد اساسا جوهريا في العلاقات الدولية[١].

وللسيادة مظهران أحدهما يتصل بعلاقة الدولة مع غيرها من الدول الأخرى، أما الاخر يمثل اتصال الدول مع بعضها بعلاقة الدولة بإقليمها وبرعاياها ، والسيادة الخارجية أول هذه المظاهر ، إذ تعني قيام الدولة بإدارة علاقاتها الخارجية بدون ان تخضع في ذلك لأية سلطة عليا ، أما المظهر الثاني فهو السيادة الداخلية الذي يعني بان الدولة تملك حرية التصرف في شؤونها الداخلية ذات الصلة بتنظيم الهيئات الحكومية والمرافق العامة ، ولا تقيدها قيود في فرض سلطتها على كافه الاشياء والاشخاص الموجودة ضمن نطاق إقليمها المادي[٢].

وقد اسهمت ثورة المعلومات والاتصالات في انتهاك مبدأ السيادة ففي ظل الفضاء المعلوماتي انعدمت الحدود الوطنية للدول ، اذ يفترض انه توجد خلال هذا المجال الافتراضي حدود غير مرئية ، ترسمها شبكه الاتصالات المعلوماتية مثبتة على اساس سياسي واقتصادي وثقافي لتنشيء عالماً من دون دولة ومن دون امة ومن دون وطن ، هو عالم المؤسسات والشبكات التي تتمركز وتعمل في إطار منظمات ذات طبيعة خاصة وشركات متعددة الجنسيات عابرة للحدود الوطنية[٣].

ومن الجدير بالذكر أن ثورة المعلومات والاتصالات أدت إلى حدوث تشابك العلاقات بين الدول في سياق السياسات الاقتصادية الحرة ، والانفتاح ، فالتحرر الاقتصادي والتطور الذي شهده قطاع الإتصالات عمل على إتاحة الفرصة لحركة رؤوس الاموال على الصعيد العالمي

---

[١] احلال نوادي ، تراجع السيادة في ظل التحولات الدولية ، مجلة دفاتر السياسية والقانون ، جامعة سعيدة ، الجزائر ، ع (٤) ، ٢٠١١ ، ص٢٦ .

[٢] فيصل اياد جعفر فرج الله ، مبدأ السيادة في القانون الدولية العام ، مجلة جامعة الكوفة للعلوم القانونية والسياسية ، م (١) ، ع (١٤) ، ص٣٤٥ – ٣٤٧ .

[٣] د. شهاب احمد العنبكي ، أثر العولمة على سيادة الدولة في القانون الدولي، دراسة تحليلية مقارنة، ط١، بغداد، ٢٠١٥ ، ص١٤٠ .

بحرية كبيرة لم تكن موجودة قبل ظهور الانترنت، ونتيجة للتحرر الاقتصـــادي العابر للحدود لم تعد الدولة قادرة في ظل التطور التقني لاسـتخدام فضـاء المعلومات على احكام سـيطرتها على كامل حدودها الإقليمية على الرغم من ان السيطرة على الإقليم هو من أهم عناصر سيادة الدولة، هذه السيطرة الإقليمية التي باتت أمراً معقدا في ظل طبيعة وأهمية التطور التقني لشبكة الانترنت و تقنيات الإتصـــال ، فتخطي المعلومات للحدود الوطنية هو إحدث عملية تغيير جوهرية في وسـائل تحديث واسـترجاع ومعالجة البيانات والمعلومات وسـرعة تطورها ، مما حدى بالدولة الى أن أصبحت غير قادرة امام هذا السيل من المعلومات التي تنساب بسهولة ويسر عالميا مما ادى إلى احداث اثار سلبية على سيادة الدولة الوطنية[١].

ومن نافلة القول: أن سـيادة الدولة ونطاقها الاقليمي وفي ظل المتغيرات التكنولوجية الهائلة باتت أمام تحديات هائلة، منها ظهور الهجمات المعلوماتية، وتطورات اســتخدام الحاســوب وشـبكات الاتصـالات والتي لا تعترف بالحدود الجغرافية، قد خلقت فضـاءً جديداً إلى جانب البر والبحر والفضاء الخارجي ، وهو الفضاء المعلوماتي.[٢]

المطلب الثاني

ممارسة الدول لواجب العناية

للدول حقوق سـيادية في اسـتغلال مواردها الطبيعية ضـمن نطاق إقليمها أو خارج حدود ولايتها الاقليمية على وفق ميثاق الامم المتحدة ومبادئ القانون الدولي ،فضـــلاً عن مســؤوليتها القائمة باحترام حقوق الدول الاخرى وضـــمان أن الانشـــطة التي تقوم بها، وتقع ضـــمن ولايتها القضـائية أن لا تسـبب اضـرارا بيئية للدول الاخرى ، حيث باتت الدول اليوم تعاني من صـعوبة بالغة في تحديد معيار التزاماتها وواجباتها إذ أن التزامات واجب العناية لا تشـــمل محتوى محدد

---

[١] د. فايق حســن جاســم ، اثر الانفتاح المعلوماتي على ســيادة الوطنية ، مجلة الســياســة الدولية ، الجامعة المستنصرية ، بغداد ، ع (١٨) ، ٢٠١١ ، ص٢٠٦- ٢١٢ .

[٢] مصـطفى عصـام نعوس، سـيادة الدولة في الفضـاء الالكتروني، سـلسـلة دراسـات عالمية، مركز الامارات للدراسات والبحوث الاستراتيجية، أبو ظبي، ع (٩٥) ، ٢٠١١، ص١٣.

بذاته لذا من الصـعب تحديد العناصـر الاسـاسـية وفقاً للقانون الدولي، إذ أن واجب العناية لم تتناوله معاهدة دولية سواء كانت معقودة بين دولتين أو كانت معاهدة جماعية، ولكن من الممكن أن يوجد معيار واجب العناية في القانون الدولي العرفي عندما تسـتخدم الدول قدرتها على منع بنيتها التحتية المعلوماتية من اسـتخدامها من قبل الجهات الفاعلة غير الحكومية لتنفيذ عمليات معلوماتية ضـارة عابرة للحدود، كالتلوث البيئي الناجم عن الانشـطة المعلوماتية، وتبعا لذلك يتطلب هذا الالتزام من الدول أيضـاً اتخاذ تدابير لحمايه الاشـخاص المدنيين الذين يخضـعون للحماية التي يوفرها القانون الدولي لحقوق الانسـان لمنع هذه الانشـطة التي تسـتهدفهم خارج أراضيهم، وسنبحث موضوع هذا المطلب في فرعين على وفق الآتي:

الفرع الأول: الممارسة في إطار القانون الدولي للبيئة.

الفرع الثاني: الممارسة في إطار القانون الدولي لحقوق الانسان.

الفرع الاول

الممارسة في إطار القانون الدولي للبيئة

اكدت محكمه العدل الدولية الطبيعة العرفية لهذا المبدأ في عام ١٩٤٩ في قضـية قناة كورفو عند الاشـارة إلى التزام الدولة بعدم السـماح عن علم باسـتخدام إقليمها في اعمال تتعارض مع حقوق الدول الاخرى [١]، لذلك جاء تأكيد هذا المبدأ من خلال مشـروع مواد لجنة القانون الدولي، والتي اشـارت الى واجب الدول بمنع الضـرر المحتمل العابر للحدود ،علاوة على ذلك تؤكد قضية مصهر تريل Trail smelter، بين الولايات المتحدة وكندا وجوب اللجوء لهذا المبدأ على انه "لا يحق لأي دولة استخدام اراضـيها أو السـماح باسـتخدام اراضـيها بطريقة تسـبب ذلك الضـرر الناجم عن انبعاث ابخرة او نقلها إلى اراضـي دولة اخرى ـــو الممتلكات أو الاشـخاص فيها" ، عندما تكون القضـية ذات عواقب وخيمة ويتم اثبات الضـرر بشكل واضـح وأدلة مقنعه[٢]، وبالتالي فقد تم الاعتراف على نطاق واسـع بمبدأ عدم الاضـرار ، كقانون عرفي فضـلاً عن ذلك،

---

[١] د.احمد عبيس نعمة الفتلاوي ، وازهر عبدالامير راهي، مصدر سابق، ص٧٩.

[٢]سكوت جيه، شاكلفورد ، مصدر سابق، ص١٢.

فان المبدأ (٢١) من اعلان ســتوكهولم لعام ١٩٧٢ والمبدأ (٢) من اعلان ريو لعام ١٩٩٢، هو الاســاس القانوني للمعيار الدولي فيما يتعلق بواجب المنع لجميع الاضــرار الجســيمة العابرة للحدود[١].

ويقصد بالتلوث العابر للحدود بأنه التلوث الذي تحدثه الأنشطة التي تمارس في أقليم دولة أو تحت اشــرافها وتنتج آثارها الضــارة في بيئة دولة أخرى أو بيئة المناطق التي لا تخضــع للاختصاص الوطني[٢].

وهناك العديد من الاتفاقيات الدولية التي أهتمت بحماية البيئة من التلوث الناشــيء عن الضــرر العابر للحدود فقد عالجت اتفاقية جنيف لعام ١٩٧٩، الخاصــة بتلوث الهواء العابر للحدود ، وعرفته على أنه " تلوث الهواء الذي يجد مصــدره الطبيعي بصــفة كلية أو جزئية في منطقة تخضع للإختصاص الوطني لدولة ما ويحدث آثاره الضارة في منطقة تخضع لأختصاص دولة أخرى تقع على مسافات بعيدة بحيث يتعذر بصفة عامة تمييز مقدار ما تسهم به المصادر الفردية أو مجموع مصادر الإنبعاث"[٣].

كما إشارت اتفاقية قانون البحار لعام ١٩٨٢ في المادة (١٩٥) منها، وبصورة غير مباشرة إلى أن تتصرف الدول عند اتخاذها التدابير الرامية إلى منع تلوث البيئة البحرية وخفضه والسيطرة عليه بحيث لا تنقل بصورة مباشرة أو غير مباشرة، الضرر من منطقة إلى أخرى[٤].

كذلك اتفاقية بازل لعام ١٩٨٩ الخاصــة بالتحكم في نقل النفايات الخطرة والتخلص منها عبر الحدود، إذ تطرقت هذهِ الاتفاقية لمسؤولية الدولة عن انشطة الكيانات الخاصة التابعة لها،

---

[١] د.حيدر عبد محسن شهد الجبوري، مصدر سابق ، ص٣١٩.

[٢] مخيمر عبدالعزيز هادي، تعليق على مجموعة المبادئ والقواعد القانونية المتعلقة بحماية البيئة من التلوث العابر للحدود، المجلة المصرية للقانون الدولي، ع (٤٣)، ١٩٨٧، ص٢٤٠.

[٣] ينظر المادة الأولى من اتفاقية جنيف الخاصة بتلوث الهواء العابر للحدود لعام ١٩٧٩.

[٤] ينظر المادة (١٩٥) من اتفاقية الأمم المتحدة لقانون البحار لعام ١٩٨٢.

إذا فقد اشـــارت إلى أنه" في حالة نقل نفايات خطرة أو نفايات اخرى عبر الحدود يعتبر اتجاراً غير مشروع يستوجب المسؤولية الدولية"[١].

ومن الأهمية بمكان أن نتناول الضـــرر العابر للحدود في ضـــوء مبادئ القانون الدولي المتعلقة بحماية البيئة من التلوث:

أولاً:- مبدأ عدم الأضرار

نشـــأ هذا المبدأ كقاعدة عرفية من قواعد القانون الدولي العرفي وهو كقاعدة يتطلب من الدول اتخاذ التدابير اللازمة والمقبولة للحيلولة دون وقوع الاضـــرار الجســـيمة العابرة للحدود، وبالتالي فأن العمل بهذهِ التدابير يعني عدم تحمل أي من التبعات القانونية الناشـــئة عن ذلك الضرر، في حال لم تقم الدولة المتضررة من القيام بالواجب الملقى على عاتقها[٢].

وكان أول ظهور لهذا المبدأ من خلال القضاء الدولي في قضية مصهر تريل، إذ جاء في الحكم الصادر عن محكمة التحكيم الأمريكية الكندية على أنه "وفقاً لقواعد القانون الدولي ، قانون الولايات المتحدة، لا يجوز لأي دولة أن تقوم بأستعمال إقليمها، أو تسمح باستعماله بطريقة ضارة ينتج عنها وصـــول ابخرة إلى اقليم دولة أجنبية أو إلى ممتلكات الاشـــخاص في هذهِ الدولة الأجنبية، يشـترط في ذلك أن تكون المسـألة على درجة من الجسـامة أو يمكن اثبات الضـرر بطريقة واضـــحة ومقنعة"[٣]، وعند التمعن بقرار المحكمة الأمريكية الكندية، نجد أن المحكمة قد تبنت معيار واجب العناية في الحكم بالقضـــية المعروضـــة أمامها، من أجل منع أو الحد من الضـرر العابر للحدود، حيث أن المحكمة لم تتوفر لديها سـابقة قضـائية تؤسـس حكمها عليها،

---

[١] المادة (٣/٩) من اتفاقية بازل الخاصـــة بالتحكم في نقل النفايات الخطرة والتخلص منها عبر الحدود لعام ١٩٨٩.

[٢] د.أحمد عبيس نعمة الفتلاوي، د.أزهر عبدالامير، الاطار المفاهيمي للعناية الواجبة والإخطار في ضوء قواعد المسؤولية الدولية (دراسة قانونية في جائحة كورونا)، مصدر سابق، ص٧٩.

[٣] بشـير جمعة عبدالجبار الكبيسـي، الضـرر العابر للحدود عن انشـطة لا يحظرها القانون الدولي، منشـورات الحلبي الحقوقية، ط١، بيروت، لبنان، ٢٠١٣، ص١٥٨.

وهي بهذا الحكم قد أشـــارت لقيام المســـؤولية تجاه كندا على أســـاس معيار واجب العناية من الضرر العابر للحدود.

ونستطيع القول أن مبدأ عدم الاضـرار، أخذ مداه الواسـع في القانون البيئي، إلا أنه يمكن أن يطبق في القانون الدولي بالشكل الذي يمكن أن يشمل عواقب إنتشار الأوبئة، مثال على ذلك تفشي جائحة كورونا، إذ إن الالتزام هنا يوجب على الدول اتخاذ التدابير دون النظر إلى الشخص المسؤول عن الضرر فيما إذا كان النشاط مشروعاً أم لا، وبالتالي فأن مبدأ عدم الاضرار يشمل كذلك الحوادث البشرية التي تسببها الكيانات الخاصة وتلك التي تسببها الكوارث الطبيعية[١].

وقد حرصت لجنة القانون الدولي المكلفة بتقنين قواعد المسؤولية الدولية عن النتائج الضارة التي لا يحظرها القانون الدولي، على تضـــمين هذا المبدأ بصـــورة صـــريحة والتأكيد على بذل واجب العناية من الضـــرر العابر للحدود، حيث جاء في نص المادة (٤) من مشـــروع المواد المتعلقة بمنع الضـــرر العابر للحدود أنه يجب على الدول أن تتخذ جميع التدابير الملائمة لمنع ضـــرر جســـيم عابر للحدود أو للتقليل منها إلى الحد الأدنى، في حال وقوعها يجب التقليل من آثارها إلى الحد الادنى[٢].

ومن نافلة القول إن معيار واجب العناية من الضرر البيئي الذي ينبغي أن يقاس به سلوك الدولة، هو ذلك المعيار الذي يكون بصـــورة عامة متناســـباً مع درجة مخاطر الضـــرر، وتطبيقاً لذلك فأن الانشـــطة التي تعد بالغة الخطورة، تتطلب عناية وحزم اكثر من جانب الدولة لغرض تنفيذها، ومن ثمة فأن ما يمكن عده معياراً متزناً ومعقولاً لواجب العناية قد يطرأ عليه تغير مع مرور الزمن، لذلك فأن واجب العناية لضـــمان الوقاية من الأضـــرار البيئية العابرة للحدود تتطلب من الدولة أن تتماشى مع التغيرات التكنولوجية[٣].

---

[١] د.أحمد عبيس نعمة الفتلاوي، د.أزهر عبدالأمير، مصدر سابق، ص٧٩.

[٢] الوثائق الرســـمية للجمعية العامة، الدورة الحادية والخمســـين، تقرير لجنة القانون الدولي عن أعمال دورتها الثامنة والاربعين، ١٩٩٦/٥/٦، الملحق رقم (١) ، ص٢٢٨-٢٢٩.

[٣] تم التأكيد على واجب العناية في المبدأ (١١) من إعلان ريو الخاص بالبيئة والتنمية لعام ١٩٩٢ والذي نص على " تســن الدول تشــريعات فعالة بشــأن البيئة، وينبغي أن تعكس المعايير البيئة والأهداف في الإطار البيئي

أما عن كيفية تطبيق مبدأ عام الأضـــرار في ســـياق الهجمات المعلوماتية نعتقد أن من مصـلحة الدول تكمن في أعمال هذا المبدأ في الفضـاء المعلوماتي للحد من التلوث الناشـيء عن الضــرر العابر للحدود أو التقليل من آثاره وخفضــها، فعلى ســبل المثال أذا تســببت الأنشــطة المعلوماتية الصادرة من دولة معينة فأن لها تداعيات خطرة على دولة أخرى مجاورة، ومن ثم فأن الدولة المخالفة يقع عليها واجب منع الضرر أو خفضه، فمن الممكن أن يؤدي الأستخدام المفرط للأنشطة في الفضـاء المعلوماتي كما هو الحال عند البريد العشوائي فأن الرسائل تستهلك نطاقاً ترددياً محدداً وهو ما يطلق عليه شكل من أشكال تلوث المعلومات، كذلك هجمات رفض الخدمة الموزعة التي تستهدف تعطيل مواقع الويب[١].

ثانياً: مبدأ الملوث يدفع

ظهر هذا المبدأ الذي يتميز بطابعه الإقتصـــادي لأول مرة عام ١٩٧٢، وكان يقضـــي بتحميل الملوثين تكلفة حماية البيئة من الأضرار الناشئة عن التلوث البيئي من دون تلقي إعانات لهذا الغرض[٢].

إلا إن هذا المبدأ قد تطور لاحقاً إلى مبدأ قانوني، وقد تناولته العديد من الإتفاقيات الدولية للبيئة والإعلانات الدولية، فقد تم تكريســه في إعلان ريو دي جانيرو عام ١٩٩٢ حيث نصــت المادة (١٦) منه على أنه "ينبغي أن تسعى السلطات الوطنية إلى تحفيز حساب التكاليف البيئة من ضمن عناصر الإنتاج واستخدام الادوات الإقتصادية أخذه بنظر الاعتبار النهج القاضي بأن

والإنمائي الذي تنطبق عليه ، والمعايير التي تطبقها بعض البلدان قد تصـبح غير ملائمة، وتترتب عليها تكاليف إقتصادية لا مسوغ لها بالنسبة لبلدان أخرى ومنها البلدان النامية).

[١] سكوت جيه شاكلفورد، مصدر سابق، ص١٢.

[٢] عبدالناصر زياد هياجنة، القانون البيئي، النظرية العامة للقانون البيئي مع شرح التشريعات البيئية)، ط١، دار الثقافة للنشر والتوزيع، الاردن، ٢٠١٢، ص٧٠.

الملوث يجب أن يتحمل من حيث المبدأ، تكلفة التلوث مع مراعاة المصلحة الراجحة للصالح العام ..."[١].

وتم تطبيق مبدأ الملوث الدافع في العديد من الوقائع كأساس قانوني لتحميل المتسبب في الاضرار البيئة المسؤولية الدولية، وبالتالي الزامه بالتعويض، ومن الامثلة على ذلك هي قضية تلوث نهر الراين بمادة الكلوريد، بين هولندا وفرنسا عام ١٩٨٠، إذ اعلنت محكمة روتندام إن المتسبب في حدوث التلوث هو شركة بوتاس الاسكا الفرنسية، وقد حملت فرنسا المسؤولية عن الأضرار التي لحقت بالمزروعات والكائنات الحية في هولندا لكنها طلبت استشارة خبير لتقييم حجم الأضرار الناشئة عن التلوث، وبالتالي اتفق الطرفان على مبلغ التعويض[٢].

أما عن كيفية تطبيق مبدأ الملوث يدفع على الفضاء المعلوماتي يمكننا القول بأمكانية اعمال واجب العناية على الانشطة المعلوماتية المسببة للضرر على وفق الآتي:

١- الزام الدول بواجب تحديد الملوث المعلوماتي الذي تترتب عليه المسؤولية الدولية في إطار القانون البيئي، حيث أن المسؤولية تكون مرتبطة بالمشغل الذي تسبب بأحداث التلوث، وتشمل المسؤولية كذلك الأشخاص الذين تم تحديدهم بصورة مؤكدة على أنهم مصدر الضرر، ومن الأشخاص المسؤولين عن أحداث الضرر على سبيل المثال، ناقل البضائع الخطرة الملوثة للبيئة، وصاحب السفينة الذي هرّب بها الزيت الملوث.

٢- في الفضاء المعلوماتي، يجب توسيع مدفوعات الملوث وامتدادها إلى مابعد التعويض المالي، ليشمل كذلك المسؤولية المدنية والجنائية الفردية، ويجب أن يشمل الملوث المعلوماتي كلاً من المتسللين الأفراد ومشغلي البنية التحتية، والمتسللون مسؤولون عن النشاط المسبب للضرر، فهم ينفذون هجمات تؤدي إلى اصابة الشبكة المعلوماتية بأضرار جسيمة.

---

[١] سمير ابراهيم حاجم الهيتي، الآليات القانونية الدولية لحماية البيئة في اطار التنمية المستدامة، ط١، منشورات الحلبي الحقوقية، بيروت، لبنان، ٢٠١٤، ص٢١٨.

[٢] منصور مجاجي، مبدأ الملوث الدافع، المدلول الاقتصادي والمفهوم القانوني، م (٣٤)، ع (١)، جامعة يحيى فارس، الجزائر، ٢٠٢٠، ص١٦١.

٣- يتيح للمشـــغلون الذين يفشـــلون في تأمين بنيتهم التحتية المعلوماتية إمكانية توجيه هجمات معلوماتية من شـبكاتهم أو توجيهها عبرها، وبالتالي من الواجب أن تمتد المسـؤولية على كلا طرفي مصـدر الضـرر، والزام الدول بسن وانفاذ تشريعات وطنية تجرم الهجمات المعلوماتية، وبالتالي يتيح للدولة الأمتثال لواجب العناية المعلوماتية[١].

السـؤال المطروح بهذا الشـأن ما هو المعيار المحدد لواجب العناية الذي يجب على الدول الالتزام به لمنع استخدام بنيتها المعلوماتية للأضرار بالدول الاخرى؟

تشـــير مذكرة فريق الخبراء الحكوميين التابعة للأمم المتحدة (GGE) التزام الدول بمنع الضـــرر العابر للحدود و تشـــجيع الدول على التعاون فيما بينها للتخفيف من نشـــاط تكنولوجيا المعلومات والاتصالات الضارة خارج اراضيهم قد يتوقع من الدول الوفاء بالتزاماتها بواجب العناية ولديها نظام دفاع عن حوادث الامن المعلوماتي اذا تطلب الامر مراقبة تنفيذ الانشطة اي ممارسة الرقابة الفعالة على من يقوم بهذه الانشـــطة ســـواء من القطاع العام أو القطاع الخاص ، وفي الواقع أن الدول ملزمة بمراقبة الانشـــطة المعلوماتية التي تنطلق من اراضـــيها، ويقع على الدول واجب مراقبة الانترنت بشكل افضل وينبع هذا الالتزام من مبدأ سياده الدولة على اقليمها، والدولة ايضـا ملزمة باحترام الحق في الخصـوصـية عن مراقبة الانشـطة ، علاوة على ذلك تلتزم الدول ايضاً باليقظة المعلوماتية فيما يخص الهجمات التي تحدث على اراضيها[٢].

على أية حال فأن المقارنة في النهج الوقائي لقانون البيئة امر في غاية الصـــعوبة، ويوفر القانون البيئي الدولي الحماية القانونية ضـد الانشـطة الخطرة التي تهدد صـحة الموارد الطبيعية مثل الهواء والماء والتربة والحيوانات والنباتات ويمكن تكييف المبدأ الوقائي في اطار الفضـــاء المعلوماتي من خلال الفروقات التالية :-

---

[١] أيان يو ينغ ليو، مسـؤولية الدولة والهجمات الالكترونية- تحديد التزامات العناية الواجبة، المجلة الاندونيسـية للقانون الدولي المقارن، مطبعة معهد حقوق المهاجرين، ٢٠١٧، ص٢٠٨-٢٠٩.

[٢] اكيكو تاكانوا، التزامات العناية الواجبة والعابرة للحدود، الضـرر البيئي، تطبيقات الامن السـيبراني، المدرسـة العليا للدراسات البيئية العالمية، جامعة كيوتو، ٢٠١٨، ص٨. متاح على الموقع الالكتروني:
https//:translate.googleusercontent.com/translate. تاريخ الزيارة ٢٠٢٢/١/١٧

١- ان الفضاء المعلوماتي ليس مورداً طبيعياً ، ولكن هو من نتاج الانسان فهو يختصر الزمن ويقرب من المسافات وازالة الحواجز ، لذلك ينبغي أن لا تكون الاقليمية هو بؤرة تركيزه الوقائي لاستخدام اللوائح في التفسير المعلوماتي التي اشارت إلى أن: لا يقتصر مصدر الضرر على جغرافيا دولة مجاورة التي يمكن من خلالها توجيه هجوم معلوماتي للعديد من الدول قبل أن تغير بالشبكة[١].

٢- تعزيز فقه محكمة العدل الدولية بشأن الوقاية والضرر البيئي حيث يهدف المبدأ إلى ضمان استدامة البيئة على المدى الطويل وتجنب الاختلال بتوازنها البيئي ، ويظهر ان عدم الرجوع عن الضرر البيئي هو الاساس في رغبة المجتمعات في تبني خطوات عدوانية مسيطرة على النشاط البيئي الضار، هذا الاساس ربما هو ليس نفس المستوى من حيث تطبيقه على الفضاء المعلوماتي ، اذ لا يشكل تدهور البيئة اهمية لدى مستخدمي الفضاء المعلوماتي ، فهم يستطيعون استعادة الخوادم بعد انتهاء الهجمات المعلوماتية (٢)، وبالتالي يمكن اصلاح الخروقات الامنية فالدول ليس لديها ادنى دافع لتقييد الهجمات الفاعلة التي تقوم بتلويث الفضاء المعلوماتي لذلك بات من الضروري تقييد استخدام الفضاء المعلوماتي في انشطة تسبب الضرر البيئي لباقي الدول ، ويجب تطبيق مبدأ (الملوث يدفع) عند القيام في أي نشاط معلوماتي ضار بالبيئة الخاصة بالدول معينة ، وعلى الدول القيام بواجبها في تجريم الافعال الناجمة عن انشطة معلوماتية غير مشروعة واستنادا لقواعد المسؤولية الجنائية الفردية، كذلك يقع على اصحاب الشركات التي تمتلك الخوادم ومعدات التشغيل الذين هم انفسهم المشغلون (اصحاب الشبكات) عبء المسؤولية التصحيحية للتأكد من ان شبكاتهم لا تهمل الهجمات المعلوماتية ويمكن الاستشهاد بما جاء في اعلان ريو بشأن الملوث يدفع وتطويعه على الهجمات المعلوماتية من خلال تحميل الدول التي صدر منها التلويث المعلوماتي تكاليف التلوث البيئي، ويمكن ان تثار مسؤولية الدولة يصدر عن حجم الاصابات الناجمة عن الهجمات المعلوماتية وتقع على الدولة مسؤولية تنفيذ التزاماتها وفقاً للمسؤولية الجنائية والدولية والمدنية ومن شأن هذا الالتزام أن

---

[١]أيان يو ينغ ليو، مصدر سابق، ص٩.

[٢]سكوت جيه شاكلفورد، مصدر سابق ، ص٩.

يوفق بين مصالح الدول الاقليمية المعتدية والدول الضحية للوصول إلى الانصاف القانوني على المستويين المحلي والدولي .

وبتحليل ما تقدم نجد أن الدول يتوجب عليها أن تحدد الملوثات المعلوماتية التي تتحمل المسؤولية اتجاهها .ففي نطاق القانون البيئي ووفقاً لهذا لمبدأ تقع المسؤولية على المشغل التي تتسبب في التلوث ، ولكن ايضاً مع الاشخاص الاخرين الذين تم تحديدهم على انهم هم من تسببوا في احداث هذه الاضرار ، مثال على ذلك الاشخاص المسؤولون عن نقل البضائع الخطرة الملوثة للبيئة ، وصاحب السفينة التي انبعث تسرب منها النفط الملوث وفي الفضاء المعلوماتي يجب توسيع مدفوعات الملوث إلى ابعد من ذلك خلال دفع التعويضات المالية والاضرار للأفراد المدنيين فضلاً عن المسؤولية الجنائية ، ويجب ان يشمل الملوث المعلوماتي كل من الافراد المتسللين ومشغلي البنية التحتية كذلك القراصنة مسؤولون عن النشاط المسبب لتلويث البيئة الذين يوجهون هجمات معلوماتية تصيب الشبكة عندما يفشلون .

ولذلك يقع على الدول واجب التزام في تنظيم بيئتها المعلوماتية ان تقوم :

١- سن وتنفيذ تشريعات وطنية خاصة بتجريم الانشطة المعلوماتية الضارة .

٢- تحميل البيانات وشركات القطاع الخاص المسؤولية عن أي انتهاكات خطيرة لشبكات الدول الاخرى التي تؤدي إلى التلوث المعلوماتي وتحميلهم مسؤولية الملوث عندما تسبب الهجمات المعلوماتية احداث اصابات محققة وجدية في بنية الدول المجاورة الاخرى .

ثانياً : مبدأ التعسف باستعمال الحق : يقوم هذا المبدأ على الصورة مفادها ان لا يجوز ممارسة الاضطهادات او استخدام السلطات بطريقة يترتب عليها الحاق الضرر بالآخرين ، وبمعنى اخر فان العمل الذي يقوم به الشخص على الرغم من مشروعيته إلا انه اساءة استخدامه أو الانحراف به يؤدي الاضرار بالغير ويحوله من نطاق المشروعية إلى عدم المشروعية [١].

لقد ابدى عدد من الفقهاء في القانون الدولي رأيهم في نظرية التعسف باستعمال الحق ، اذ تعتبر من اهم النظريات التي تساعد على تطوير قواعد القانون الدولي المتعلقة بالمسؤولية الدولية

---

[١] هناء الحموي، التأصيل الفقهي لمسؤولية الدولة عن الضرر البيئي، مجلة الفقه والقانون، ع(٣٣)، ٢٠١٥، ص٨٧.

، وان من الضـــروري تطبيقها في ميدان العلاقات الدولية باعتبارها من مبادئ القانون العامة استنادا الى للمادة (٣٨) من النظام الاساسي لمحكمه الدول العدل الدولية ، وذلك عندما تشمل المدونة احد الحقوق بطريقة تحكيمية يكون من شـانها الحاق الضـرر بدولة اخرى لا يكفي تبريره على اساس مصلحة مشروعة للدولة الاولى[١].

ومن التطبيقات الحديثة لفكرة التعسـف في اسـتعمال الحق دولياً ، هو اعتبار الدولة التي تستعمل اقليمها بقصد اجراء تجارب ذرية مسؤوله عن الاضرار التي تنتج عن الاشعاعات الذرية وعن الغبار الذري التي تصـل الى اقليم الدول الاخرى ، وما تنتجه من اضـرار بيئية تؤثر علي الكائنات الحية[٢].

كما تم التأكيد على مبدا عدم التعسف في استعمال الحق في العديد من الاتفاقيات الدولية ، اذ نص اعلان البيئة لمؤتمر اسـتوكهولم ١٩٧٢ في المادة (٢١) على واجب التأكد من النشـاطات التي تمارس داخل حدود اية دولة او تحت اشـرافها أن لا تحدث اضـراراً بيئية للدول الاخرى، كذلك جاء النص ايضـا على هذا المبدأ في اتفاقيتي الامم المتحدة لقانون البحار عام ١٩٨٢ في المادة (٣٠٠) واتفاقيه جنيف الخاصـة باعالي البحار لعام ١٩٨٥[٣]. وطبقت محكمه العدل الدولية مبدا العام التعسـف في اسـتعمال الحق في قضـية المعابر الانجليزية النرويجية عام ١٩٥١ اذ قررت المحكمة ان بريطانيا قد تعسفت في استخدام حقها ، كما طبقت لجان التهم الدولية هذا المبدأ في قضـيه التحكيم بين الولايات المتحدة الامريكية وكندا في ما يخص الاضـرار التي تعرضـت لها الأشـجار والمحاصـيل الزراعية الامريكية نتيجة لغازات ديو

---

[١] د. هادي نعيم المالكي ود. هديل صـالح الجنابي ، مبدأ الملوث يدفع في اطار المسؤولية الدولية الناجمة عن تلوث البيئة ، مجلة العلوم القانونية ، كلية القانون جامعة بغداد ، م (٢٨) ، ع (٢) ، العراق ، ٢٠١٣ ، ص١٣-١٧.

[٢] الامم المتحدة ، مكتب الاعلان ، دراسة بعنوان (النفايات الخطرة)، بيروت ، ١٩٩٢ ، ص١٠ .

[٣] د. محمد حافظ غانم ، المسؤولية الدولية – دراسة لاحكام القانون الدولي وتطبيقاتها التي تهم الدول العربية ، جامعة الدول العربية – معهد الدراسات العربية العالمية ، مصر ، بدون سنة طبع ، ص٨٧-٨٨ .

كسـيد الكبريت التي كانت تنقل إلى الولايات المتحدة الامريكية تحملها الرياح من كندا حيث توجد بعض المصانع تسبب انبعاث هذه الغازات [١].

ومن الجدير بالذكر ان الطريقة المثلى لحماية البيئة من خطر التلوث تكمن في منع وقوع الضـرر وليس الحد من اثاره السلبية ومحاولة وضـع الحلول لمعالجتها بعد حدوثه ، اذ ان الالتزام بمنع التلوث البيئي والاحكام الخاصـة به تشـمل مجموعة من الاجراءات التي يتوجب على الدولة الالتزام بها من خلال تشـريعاتها الوطنية ذات الصـلة بالأنشـطة التي لا تهدد بحدوث اثار سـلبية مدمرة ، وعليه فمن الممكن ان ينشأ التزام يقضـي بإيقاف او منع الانشطة التي تسبب اثاراً ضـارة بالبيئة ، كما يحدث عند منع الانتاج الاضـافي للكيمياويات الخطيرة ، فأن هذا الالتزام يتضـمن تحديداً مقدار الضـرر الناشـئ عن الانشـطة عن طريق وضـع تقنيات قانونية تعمل على تخفيف اثار التلوث [٢].

ان ترتيب المسؤولية الدولية تكون مرتبطة بالالتزام وتطبيق الاجراءات لمنع وقوع الاضـرار البيئية حيث ان المسـؤولية الدولية تدور وجوداً وعدماً مع الالتزام ، حيث اصـبحت المسـؤولية الدولية الناشـئ عنها الضـرر تتمثل باضـطلاع الدول بواجب مهم وهو حماية البيئة من وقوع الضـرر ، وهو واجب اقرته قواعد القانون الدولي ، اذ ان منع وقوع الضـرر البيئي هو في الغالب افضـل من استيفاء التعويض عن الضـرر بعد حدوثه ، وقد اكد مؤتمر استوكهولم للبيئة البشرية لعام ١٩٧٢ على مبدأ عام اصـبحت جميع الدول ملزمة بتطبيقه وهو مبدأ حماية البيئة من التلوث ، الذي يعد مبدأً عرفياً جرى العمل به بين الدول ، لما ينطوي عليه من واجب الحيطة ، أي ما يقع من واجب على كل دولة بالامتناع عن تلويث البيئة ، باتخاذ عدد من الاجراءات لمنع حدوث التلوث ، وواجب التعاون مع الدول والهيئات الدولية لوقاية البيئة من التلوث ، وهذا

---

(1) Davad hunter , jems salzman , durwoodzaelh , international environmental law and policy – second edition– New york – 2002 , p. 904 .

(2) Aleen . springer , the international of pollution ; protection of the , global environ ment in a world of sovereign states , Westport , connectict , Quorum books , 1983 , p , 232 .

الواجب مستمد من مبدأ حسن الجوار ومبدأ عدم التعسف في استعمال الحق ، ويترتب على ذلك عدد من الواجبات الملقاة على عاتق الدول في نطاق الحفاظ على البيئة وحمايتها [١].

الفرع الثاني

الممارسة في إطار القانون الدولي لحقوق الانسان

في ظل التطور التكنلوجي الحديث ، هناك تزايداً ملحوظاً وصـــريحاً للمســـاس بحقوق الانســـان المعلوماتية ، نتيجة للاســـتخدام المفرط للأنشـــطة المعلوماتية ، وقد حاول العديد من المفكرين القانونيين وضـــع معنى محدد لهذه الحقوق إلا انهم لم يتمكنوا من ذلك بسـبب اختلافهم حول ما تشتمل عليه هذه الحقوق أو ما تضمه من عناصر ، فضلاً عن حداثه الموضوع وعدم تناوله من قبل الدراسات المعاصرة لحقوق الانسان إلا في نطاق محدود ، وبالتالي فان أي تعريف يتم طرحه بهذا الشأن قد لا يستوعب مضمون هذه الحقوق، إذ عرفها البعض بانها : حق كل فرد في الوصول واستخدام وانشاء ونشر محتوى معلوماتي واستخدام أي حواسيب او أي اجهزة اخرى، أو برمجيات أو شبكات اتصال دون قيود[٢].

وتتفرع عن هذه الحقوق العديد من الحقوق والحريات الاخرى كالحق في الحياة والحق في حرية التعبير ، والحق في الخصـــوصـــية وحرية تداول المعلومات وغيرها من الحقوق والحريات الاخرى والسؤال الذي يثار بهذا الصدد، ماهي حقوق الانسان المعلوماتية ؟ وهل ان الدول ملزمة بواجب العناية ومنع انتهاك هذه الحقوق ؟

سنحاول الاجابة عن هذه التساؤلات من خلال الوقوف على أهم حقوق الانسان في الفضاء المعلوماتي في هذا الفرع وعلى النحو الاتي :

اولاً :- الحق في الحياة

ان من اهم حقوق الانســـان التي يحتمل ان تكون عرضـــه للانتهاكات بواســـطة الهجمات المعلوماتية هو الحق في الحياة وان حماية هذا الحق هو واجب يقع على عاتق جميع الدول ،

---

[١] د . هادي نعيم المالكي و هديل صالح الجنابي ، مصدر سابق، ص١٠.

[٢] محمد الطاهر ، الحريات الرقمية – المفاهيم الاســاســية ، ط١، مؤســســة حرية الفكر والتغيير ، القاهرة ، ٢٠١٣، ص٥.

فقد تم تكريس الحق في الحياة في جميع الصكوك الدولية المعنية بحقوق الانسان ابرزها الاعلان العالمي لحقوق الانسان الصادر عام ١٩٤٨ ، اذ جاء في نص المادة (٣) منه على ان " لكل فرد الحق في الحياة والحرية وسلامة شخصه "[١]. وتم تأكيد هذا النص المقرر لحماية الحق في الحياة في العهد الدولي الخاص بالحقوق المدنية والسياسية ، اذ نصت الفقرة (١) من المادة (٦) منه على ان : " الحق في الحياة حق ملازم لكل انسان ، وعلى القانون ان يحمي هذا الحق ، ولا يجوز حرمان احد من حياته تعسفاً"[٢].

أن الحق في الحياة من أهم الحقوق المشمولة بكفالة الاحترام وهو اساس جميع الحقوق الاخرى ، وهو من الحقوق الطبيعية، وحماية هذا الحق وكفالة احترامه ليس فقط عدم المساس به من قبل اطراف النزاع، والسلطة العامة في الدولة ، بل تلتزم الدول بمنع انتهاكه وتهديده من جانب الافراد، فضلاً عن تشريع القوانين التي تضمن هذه الحماية والاحترام وكيفية تنفيذها بصورة عملية[٣].

ومن نافلة القول ان مدونة قواعد سلوك الموظفين المكلفين بإنفاذ القوانين الصادرة من الأمم المتحدة بموجب قرار الجمعية العامة للأمم المتحدة ذي العدد (٣٤ / ١٦٩) بتاريخ ١٧ / كانون الثاني / ١٩٧٩ قد جاء فيها اشارة صريحة وواضحة في المادة الثانية منها في التأكيد على حقوق الانسان والمحافظة عليها وتعزيزها لجميع الناس دون استثناء ومنها الحق في الحياة[٤].

وفي ذات السياق اعربت لجنة حقوق الانسان عن شعورها بالقلق ازاء الخسائر البشرية التي تحدثها استخدام الاسلحة التقليدية اثناء النزاعات المسلحة، واكدت قلقها المستمر نتيجة تطوير ونشر أسلحة الدمار الشامل، وهو ما يشكل تهديداً للحق في الحياة، وأوصت اللجنة

---

[١] الاعلان العالمي لحقوق الانسان الصادر عام ١٩٤٨ .

[٢] العهد الدولي الخاص بالحقوق المدنية والسياسية لعام ١٩٦٦ .

[٣] خالد مجيد بريسم المجمعي ، كفالة احترام قواعد القانون الدولي الانساني ، رسالة ماجستير ، كلية الحقوق ، جامعة تكريت ، العراق ، ٢٠١٩ ، ص٣٢ .

[٤] اشارة المادة (٢) من مدونه السلوك على ان (يحترم الموظفون المكلفون بإنفاذ القوانين بمناسبة قيامهم بواجباتهم الكرامة الانسانية ويحمونها ، ويحافظون على حقوق الانسان لكل الاشخاص ويوطدونها) .

بضرورة حظر انتاج الاسلحة التي تنتهك حقوق الانسان، ومنها الاسلحة النووية، وحثت المجتمع الدولي على اتخاذ خطوات عاجلة للحد من خطر الاسلحة الفتاكة وحظرها[١].

ومن الامثلة التطبيقية التي من المحتمل أن تجعل الحق في الحياة عرضة للأنتهاك نتيجة الهجمات المعلوماتية هو مهاجمة أحدى مستشفيات هوليود في الولايات المتحدة الأمريكية عام ٢٠١٦، التي تقوم بتقديم خدمة الرعاية الصحية للراقدين فيها من خلال تعطيل برامج الطوارئ للحالات الحرجة بواسطة نشر الفيروسات في أنظمة المستشفى المذكور، ونتج عن الهجوم عدم حصول المرضى الراقدين فيها على الرعاية الصحية اللازمة لعدة ايام، مما ساعد في سرعة انتقال العدوى بين المرضى وجعل حقهم في الحياة عرضه للتهديد بسبب ارتفاع نسبة الاصابات الفتاكة المؤدية إلى ارتفاع نسبة الوفيات بين المرضى [٢].

ثانياً: الحق في الخصوصية المعلوماتية

لقد اختلفت التعريفات وتباينت الآراء التي تناولت الحق في الخصوصية كأحد حقوق الإنسان الواجب حمايتها ، وبحسب وجهات النظر لكل منهم ، فلم نجد لهذا الحق تعريف محدد وواضح ، إذ أن اغلب الصكوك الدولية والاقليمية وإعلانات حقوق الانسان تشير الى ما يشتمل عليه هذا الحق من واجب الحماية و كفالة احترامه ، إلا أنها اغفلت التطرق لتعريفه بصورة واضحة ومحددة ، فقد جاء في الاعلان العالمي لحقوق الانسان في المادة ١٢ منه على ان " لا يعرض أحد له تدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته .... ولكل شخص الحق في حماية القانون من مثل هذا التدخل ..."[٣].

---

[١] تعليق اللجنة المعنية بحقوق الانسان رقم (٣٦) في تشرين ثاني عام ٢٠١٨ .

[٢] د.احمد عبيس نعمة الفتلاوي وازهر عبد الامير الفتلاوي ، المسؤولية الناشئة عن استخدام وسائل القتال الفتاكة في نشر الاوبئة، (الهجمات السيبرانية في مقابل جائحة كورونا انموذجاً) ، مجلة الحقوق ، ع (٤١) ، ٢٠٢١ ، ص٨٢ .

[٣] المادة (١٢) من الاعلان العالمي لحقوق الانسان الصادر عام ١٩٤٨ ، للمزيد ينظر د. صلاح عبد الرحمن الحديثي ود. سلافة طارق الشعلان ، حقوق الانسان بين الامتثال والاكراه في منظمة الامم المتحدة م ط٢ ، مؤسسة النبراس للطباعة والنشر والتوزيع ، النجف الاشرف ، ٢٠٠٨ ، ص٤٩-٥٧ .

واكدت هذا الحق المادة (١٧) من العهد الدولي الخاص بالحقوق المدنية السياسية، وهي جاءت على غرار المادة (١٢) من الاعلان العالمي لحقوق الانسان ، اذ نصت على ان " ١- لا يجوز تعريض أي شخص ، على نحو تعسفي أو غير قانوني ، لتدخل في خصوصياته أو شؤون أسرته أو مراسلاته ، ولا لأي حملات غير قانونية تمس شرفه وسمعته ، ٢- من حق أي شخص أن يحميه القانون من مثل هذا التدخل او المساس"[١] .

أما الاتحاد الاوربي فقد عرف البيانات الشخصية بانها " أي معلومات ذات صلة وثيقة بشخص طبيعي أو يمكن تحديده ، والفرد الذي يمكن تحديده هو ذلك الشخص الذي يمكن تعريفه بطريقة مباشرة أو غير مباشرة ، من خلال الرجوع إلى رقم الهوية ، أو الاعتماد على عامل أو أكثر من العوامل المحددة لهويته البدنية والعقلية والفيسلوجية"[٢].

أن تزايد اعتماد الدول على الفضاء المعلوماتي يشكل تحديات خطيرة في انتهاك حق الخصوصية ، إذ أن الحكومات في إطار اعتمادها على التطور التكنلوجي في تقديم الخدمات لمواطنيها فأنها تقوم بجمع وتحليل البيانات لغرض تحديد هوية المواطنين أو جوازات السفر وغيرها من الأمور الاخرى ذات الصلة بالأمن القومي مما يجعل حق الخصوصية في خطر نتيجة الإستخدام غير المشروع لهذه البيانات الشخصية[٣].

وقد نال الحق في الخصوصية إهتمام واسع النطاق من قبل الجمعية العامة للأمم المتحدة مؤكدة ان هذا الحق من الحقوق التي يتمتع بها الافراد وحثت الدول على احترام وحماية الحق في الخصوصية بما في ذلك استخدام الإتصالات الرقمية المعلوماتية وضمان الامتثال التام لالتزاماتها بموجب القانون الدولي لحقوق الانسان، وطلبت الامم المتحدة من المفوضية السامية

---

[١] المادة (١٧) من العهد الدولي الخاص بالحقوق المدنية والسياسية لعام ١٩٦٦ .

[٢] المادة (٤) الفقرة (١) من لائحة الاتحاد الاوربي ٢٠١٦ / ٦٧٩ الصادرة عن البرلمان الاوربي بتاريخ ٢٧ نيسان ٢٠١٦ الخاصة بحماية الاشخاص الطبيعيين ذات الصلة بمعالجة البيانات الشخصية وحرية نقل البيانات للمزيد ينظر:

Olgamironeko fnerst vedt , Aviation security , privacy , data protection and other human rights ; Technologires and legel principles , springer , Gewerbestrasse , Switzerland , 2017 , p. 32 .

[٣] د. منى الاشقر جبور ، مصدر سابق ، ص١٢٣ .

لحقوق الانسان، أن تقدم تقريراً يتضمن حماية وتقرير الحق في الخصوصية في اطار المراقبة المحلية وخارج الحدود الاقليمية، واعتراض الاتصالات المعلوماتية وجمع البيانات الشخصية ، ويكون هذا التقرير شاملاً تفصيلياً، يقدم إلى مجلس حقوق الانسان في دورته (٢٧)، وإلى الجمعية العامة في دورتها (٦٩)، وأكدت المفوضية السامية على ان الحق في الخصوصية ، والحق في الوصول إلى المعلومات ، وحرية التعبير مرتبطة ارتباطاً وثيقاً بعضها بالبعض الاخر ، ومنحت الجمهور الحق في المشاركة في الشؤون العامة وهذا الحق لا يمكن ممارسته على الوجه الامثل من خلال الاعتماد فقط على ما تم تداوله من معلومات مصرح بها[١].

ومن الامثلة على الهجمات المعلوماتية التي تشكل انتهاكاً للحق في الخصوصية، تزييف المستندات الموجودة على الحاسوب الشخصي ، أو الافصاح عن المعلومات المتعلقة لشخص معين ، فضلاً عن اختراق البريد الالكتروني لرؤساء الدول وافشاء اسرارهم والاطلاع على معلوماتهم وبياناتهم الشخصية والتجسس عليها لمعرفة مراسلاتهم ومخاطباتهم[٢].

كذلك الهجوم المعلوماتي الذي قامت به روسيا وكان الغرض منه استهداف البريد الالكتروني للمرشحة السابقة لرئاسة الولايات المتحدة الامريكية هيلاري كلينتون (Hilary Clinton)[٣].

ثالثاً : الحق في حرية التعبير المعلوماتية

يقصد بحرية الرأي والتعبير " حرية الشخص في ان يبدي ما يفكر به دون ان يلاحق ، وتشمل الحرية في إستقصاء الاخبار وتلقيها وتداولها وبثها بأي وسيلة كانت دون التقيد بالحدود

---

[١] الجمعية العامة للأمم المتحدة تؤكد على الحق في الخصوصية في العصر الرقمي ، صحيفة الوقائع التابعة للأمم المتحدة ، ٢ك١ ، ٢٠١٣ ، مطبوعات الامم المتحدة نيويورك ، ٢٠١٣ ، ص١٩ .

[٢] سارة بو حادة ، اثر الارهاب الالكتروني على امن واستقرار الدول ، متاح على الموقع الالكتروني:
https//:manifest . univ – ouargla . dzldocuments archiv
تاريخ الزيارة ١٨- ١١ / ٢٠٢١.

[3] See . Roberts . Mueller , Rebort on the investigation into Russian inter ference in the 2016, U.S. Depart ment of justice , vol . of II Washington , march 2019 , p. 43.

الجغرافية وبأي شـكل سـواء كانت مكتوبة أو شـفوية أو مطبوعة، وبأي وسـيلة اخرى يختارها الشخص في التعبير عن رأيه بكل حرية"[١].

وحرية التعبير الوارد ذكرها في القانون الدولي لحقوق الانسـان يكون نطاقها أوسـع وأشـمل من تلك الحرية ذاتها التي تضمنها القانون الدولي الانساني ، فقد نصت ف (١) من المادة(١٩) من العهد الدولي للحقوق المدنية والسياسية لعام ١٩٦٦ ، على ان "لكل انسان الحق في اعتناق اراء دون مضـايقه" نصـت الفقرة (٢) من المادة (١٩) من نفس العهد على أن لكل إنسـان حرية التعبير عن ارائه ، يسـتتبعها حقه في تداول المعلومات والافكار ونقلها إلى الغير بغض النظر عن الحدود ، سواء كان نقل وتداول هذه المعلومات والافكار بصـيغة مكتوبة او مطبوعة او بأي وسيلة اخرى"، وهذا يدل ان هاتين الفقرتين تقدمان حقاً موسعاً للإنسان من خلال :-

١- التحري عن المعلومات بكافة أنواعها وأشكالها.

٢- تداول المعلومات ونقلها من جميع انواعها.

٣- تلقي وتداول المعلومات دون التقييد بالحدود الجغرافية ، أو أي وسيلة اخرى مكتوبة او غير مكتوبة ، أو بواسـطة وسـائل الاعلام بضـمنها وسـائل الاعلام المعلوماتية: بمختلف انواعها[٢].

وقد اسـتوعبت نصـوص الصـكوك الدولية واعلانات حقوق الانسـان ذات الصـلة بحقوق الانسان كالإعلان العالمي لحقوق الانسان لعام ١٩٤٨ ، والعهد الدولي للحقوق المدنية والسياسية ، العديد من التطورات الحاصلة في عالم تكنلوجيا المعلومات ، وقد اتاحت للعديد من البشر حرية التعبير عن آرائهم بصورة واسعة بشتى الوسائل سواء في مجال النشر أو التفاعل[٣].

---

[١] د. بصـائر علي محمد ، انتهاكات الحق في حرية التعبير ، دراسـة خاصـة عن التدوين الالكتروني ، مجلة كلية الحقوق ، جامعة النهرين ، م (١٧)، ع(٢)، بغداد ، ٢٠١٥ ، ص٢٩.

[٢] جون . اس .جيسون ، معجم قانون حقوق الانسان العالمي ، ترجمة سمير عزت نصار ، دار النشر والتوزيع ، عمان ، ١٩٩١ ، ص٧١.

[٣] هديل مالك ونضـال عباس ، دور القانون الدولي في حماية حرية الرأي والتعبير ، مجلة السـياسـية الدولية ، الجامعة المستنصرية ، بغداد ، ٢٠١٢ ، ص٣٢٢ .

ومن نافلة القول أن أغلب المواثيق والأعلانات الدولية والإقليمية كرست حق الفرد في حرية الرأي و التعبير عنها وينتج عن ذلك أقرار حقين أساسيين للفرد هما :

١- حرية الرأي : وتشمل حرية اعتناق الآراء وتبني الافكار من دون تدخل أحد فهي حرية مطلقة غير نسبية .

٢- حرية التعبير عن الرأي بأي وسيلة إعلامية سواء كان ذلك من خلال الوسائل المرئية والمسموعة ، أو النشر في الصحف وغيرها من الوسائل المختلفة ، مما يتيح لكل فرد التثبت من صحة الوقائع وابداء رأيه بصورة موضوعية .

ولكن الحق في حرية الرأي ليس حقاً مطلقاً في جميع الاحوال بل هو مقيد في القوانين التي يضعها القانون الداخلي لكل دولة والتي يتم فرضها لأجل حماية الأمن القومي لها، أو النظام او الصحة العامة أو الاخلاق العامة، أو احترام حقوق الاخرين وحرياتهم الاساسية، ومنع ارتكاب الجرائم[١].

وبتحليل ما تقدم نجد ان الصكوك والمواثيق الدولية واعلانات حقوق الانسان قد كفلت حق حرية التعبير والرأي وتبني افكاره بالصورة التي يرغب فيها ، وهذا يمثل مكاسب ذو فائدة كبيرة عادت بالنفع على المجتمع الدولي على اساس انها تتلائم مع التطور التكنلوجي والتقدم العلمي ، وغالباً ما تتفق مع مبادئ القانون الدولي المعاصر ، وقد اكدت هذه الصكوك الدولية على حرية التعبير بصورة مباشرة دون تدخل الدولة ن ولكن في ذات الوقت هناك ضرر يقع على بعض الدول نتيجة اطلاق هذا الحق دون تقييده عندما لم يتم استخدامه بصورة صحيحة ، ومن الضروري ايجاد توازن بين هذا الحق وحق الدولة في حماية امنها القومي.

ومن الامثلة على الهجمات المعلوماتية التي تشكل انتهاكاً لحق الفرد في حرية العبير عن الرأي، هي الهجمات المعلوماتية التي قامت بها روسيا وكان الغرض منها التأثير على نتائج

---

[١] ينظر ف (٣) من المادة (١٩) من العهد الدولي للحقوق المدنية الاساسية لعام ١٩٦٦) فقرة (٢) المادة(١٠) من الاتفاقية الاوربية ، وفقرة (٢) من م (١٣) من الاتفاقية الامريكية لحقوق الانسان لعام ١٩٦٩. كذلك نص المادة(٩) من الميثاق الافريقي لحقوق الأنسان لعام ١٩٨١.

التصـويت والتلاعب في حملة الاسـتفتاء الخاصـة بخروج بريطانيا من الاتحاد الاوربي اذ ادعى نائب البرلمان بن برادشـو خلال خطابة داخل البرلمان ان روسـيا تدخلت سـلبياً في التأثير على حملة الاســتفتاء على خروج بريطانيا من الاتحاد الاوربي ، وفي عام ٢٠١٧ ، اصــدرت لجنة الادارة العامة والشــؤون الدســتورية التابعة لمجلس العموم البريطاني تقريراً يبين فيه انهيار موقع تسجيل الناخبين الحكومي في حزيران ٢٠١٦ ، قبل اقل من ساعتين من الموعد النهائي للتسجيل المقرر اصــلاً ، وأشــار التقرير إلى أن هناك دوراً بارزاً للاسـتخبارات المعلوماتية الروسـية للقيام بهذه الهجمات التي تحث الناخبين على التصــــويت بنعم للخروج من الاتحاد الاوربي من خلال حملة تمويل دعاية معلوماتية[١].

رابعاً : واجب العناية المعلوماتية للدول في حماية حقوق الانسان

كان للجهود الدولية الرامية للاعتراف بحقوق الانســـان المعلوماتية من ابرز العوامل التي ســاعدت على دعم حقوق الانســان تكنلوجياً في الاطار الدولي ، ومن ابرز تلك الجهود الدولية هي :-

١- انشــاء القمة العالمية لمجتمع المعلومات : وهي قمة لزعماء العالم الملتزمين بتســخير امكانات تكنلوجيا المعلومات والاتصالات لتعزيز واحترام حقوق الانسان المعلوماتية .

٢- اقرت الامم المتحدة ضـرورة الاعتراف بالحقوق المعلوماتية نتيجة اسـتحداثها لمنصـب المقر الخاص بتعزيز وحماية الحق في حرية التعبير والراي ، اذ تم تحديد العديد من المســـائل الجوهرية المتصــلة بالحقوق المعلوماتية من خلال التقرير الذي صــدر عنه عام ٢٠١١ ، والذي تم عرضــه على مجلس حقوق الانسـان التابع للأمم المتحدة ، وقد تضـمن هذا التقرير العديد من التوصـيات التي أسـهمت في اقرار العديد من الخصـائص المميزة للحقوق التكنلوجية ، وقد دعى المقرر الخاص الدول إلى ضـمان توفير الوصـول إلى شـبكة الانترنت بصـفة دائمة ، وضـمان وصـول جميع الدول لشبكة الانترنت ، وحث الدول على تطوير سياسـة فاعلة وراسـخة بالتشاور

---

[١] علي زياد العلي ، الصراع والامن الجيوسيبراني في السياسة الدولية ، دراسة في استراتيجيات الاشتباك الرقمي ، ط١ ، دار امجد للنشر والتوزيع ، الاردن ، ٢٠١٩ ، ص١٦٠ .

مع الافراد في كل قطاعات المجتمع بما في ذلك القطاع الخاص من اجل إتاحة الوصـــول للأنترنت.

٣- تيسير تبادل المعلومات في مجال حوكمة الانترنت في البلدان النامية والاستفادة بشكل كامل من الموارد المحلية[١].

ولقد اصــبح للفضــاء المعلوماتي دوراً هاماً في ممارســة حقوق الانســان ، لذلك فأن أي انشــطة معلوماتية خطرة في هذا الفضــاء تؤثر ســلباً على تلك الحقوق لا ســيما الحق في الخصوصية وحرية المعلومات والحق في الحياة ، فضلاً عما تقدمه شبكة المعلومات الدولية من مجموعة متنوعة ومعقدة من الاستخدامات في شتى المجالات وبالتالي يزداد معها حالات انتهاك تلك الحقوق بقصد التجسس أو السرقة ، ولذلك أصبحت الدول مدعوة إلى ضرورة انشاء وحدات خاصــة لمكافحة الجريمة المعلوماتية بواســطة الحاســب الآلي والانترنت ، وايجاد آليه ملائمة للتعاون الدولي لمكافحة الجرائم الخاصة بالحاسب وشبكة المعلومات الدولية وسبل مكافحتها [٢].

وفي الثامن عشر من شباط عام ٢٠١٣ اصدرت الجمعية العامة للأمم المتحدة قراراً بشأن الخصوصية في العصر المعلوماتي ، وجاء هذا القرار نتيجة القدرة المتنامية للمؤسسات الحكومية على الوصول إلى خصوصيات الافراد من خلال المراقبة عبر الوسائل المعلوماتية سواء كانوا الاشــخاص المراقبين يقطنون اقليم الدولة أو خارجها وقد جاء القرار باتجاهين، الاتجاه الأول يتضمن التأكيد على حق الافراد في الخصوصية في ظل التطور التكنلوجي، أما الاتجاه الثاني الذي تضمنه القرار ، فقد كان في سياق عدم اجماع الدول على موقف موحد بشأن ما يمكن عده تدخلاً تعسفياً في خصوصية الافراد، وقد كان نتيجة صدور هذا القرار هو عدم التصويت عليه،

---

[١] د. وسام نعمت السعدي ، الحقوق الرقمية وآليات الحماية الدولية المقررة لها في اطار القانون الدولي لحقوق الانسان ، الناشر وقائع المؤتمر العلمي لجامعة نولج متاح على الموقع الالكتروني :
https://portal.aird.my.
تاريخ الزيارة ٩/ ١ / ٢٠٢٢ .

[٢] د. هشام محمد فريد ، قانون العقوبات ومخاطر تقنية المعلومات ، مكتبة الآلات الحديثة ، ١٩٩٢ ، ص٤٧.

وطالب القرار المفوض السامي لحقوق الانسان اعداد تقرير حول حماية حق الخصوصية في ضوء التقدم التكنلوجي[١].

ومن الجدير بالذكر أن القانون الدولي بشقيه العرفي والتقليدي يلزم الدول بحكم معيار واجب العناية بمنع الأعمال المنافية لحقوق الإنسان والتصدي لها وتوفير سبل الإنتصاف والحماية، من الانتهاكات التي تتعرض لها تلك الحقوق، فلا يجوز للدولة أن تفوض التزاماتها بتوخي واجب العناية إلى جهة أخرى حتى في الحالات التي يتولى فيها القيام ببعض المهام طرف أخر خاضع أو غير خاضع لها، إذ أن الدولة الإقليمية أو أي دولة أخرى تمارس الولاية القضائية أو السيطرة الفعلية على تلك الأراضي وهي المسؤولة في نهاية المطاف عن كفالة الوفاء بالالتزامات ذات العلاقة بالامتثال لواجب العناية[٢].

وتطبيقاً لواجب العناية اللازمة في سياق العنف المنزلي، كانت قضية اويوز ضد تركيا التي نظرتها المحكمة الاوربية لحقوق الانسان واصدرت قرارها في عام ٢٠٠٩ لصالح اويوز ، وكان لقرار المحكمة اثراً في مدى التزام الدولة بمعيار واجب العناية بحقوق الانسان المتعلقة بالعنف المنزلي. ومن الامثلة التطبيقية الاخرى لواجب عناية الدول بحقوق الانسان هي قضية جيسكا غونزاليس واخرون ضد الولايات المتحدة الامريكية وتم رفع القضية ضد زوجها الذي تسبب بقتل اطفالها الثلاث ونجاتها ، وقد وجدت لجنة البلدان الامريكية بقرارها التاريخي ان الولايات المتحدة الامريكية مسؤولة عن انتهاكات حقوق الانسان التي تعرضت لها السيدة جيسيكا ، وأن الولايات المتحدة فشلت في الوفاء بالتزام واجب العناية وحماية السيدة جيسيكا من العنف المنزلي[٣].

---

[١] رزق سلمودي واخرون ، الموقف المعاصر لقواعد القانون الدولي العام من الحق في الخصوصية في العصر الرقمي ، مجلة الجامعة العربية الامريكية للبحوث ، م (٣) ، ع (٢) ، ٢٠١٧ ، ص١٢-١٣.

[٢] الأمم المتحدة، المجلس الاقتصادي والإجتماعي، لجنة حقوق الإنسان، الدورة (٦٢) المنعقدة في ٢٠ شباط ٢٠٠٦، بنيويورك، البند (١٢/أ) من جدول الأعمال المؤقت- معيار العناية الواجبة بوصفه أداة للقضاء على العنف ضد المرأة، تقرير المقررة الخاصة المعينة بالعنف ضد المرأة وأسبابه وعواقبه- السيدة ياكين إرتوك، ص٩.

[٣] شازية قريشي ، تمديد معيار العناية الواجبة إلى تقديم استجابة الدولة تجاه العنف ضد المرأة ، العنف المنزلي ، جامعة البنجاب ، م (٢٨) ع (١) ، ٢٠١٣ ، ص٥٦-٥٨ .

وقد حرص المشرع العراقي على حماية الحق في الخصوصية اذ جاء في المادة (١٧) من دستور جمهورية العراق لسنة ٢٠٠٥ (النافذ) على انه " لكل فرد الحق في الخصوصية الشخصية بما لا يتنافى مع حقوق الاخرين والآداب العامة".

وعد المشرع العراقي تداول الصور ونشرها ما يخص الحياة العائلية والافراد هي من الجرائم التي يعاقب عليها القانون كجريمة افشاء السر فقد نصت (المادة ٤٣٨) اولاً " يعاقب بالحبس مدة لا تزيد على سنة من نشر بإحدى الطرق العلانية اخباراً او صوراً او تعليقات تتصل بأسرار الحياة الخاصة او العائلية للأفراد ولو كانت صحيحة ....". وقد تضمن مشروع قانون مكافحة الجرائم المعلوماتية في المادة (١٣ – اولاً ج) على ان " يعاقب بالحبس مدة لا تقل عن ثلاث سنوات او بغرامة لا تقل عن خمسة ملايين ولا يزيد على عشرة ملايين ..... كل من علم بحكم عمله ببيانات التوقيع الالكتروني أو الوسائل الالكترونية ، او المعلومات فأفشأها..".

المبحث الثاني

الجهود الدولية في اطار واجب العناية للحد من اضرار الهجمات المعلوماتية

أضحى الفضاء المعلوماتي يواجه تهديدات خطيرة بأنشطة معلوماتية غير مشروعة لن تكون أي دولة بمنجاة منها ، لذا باتت الدول اليوم تبحث عن استراتيجيات وقائية ، واتفاقيات دولية واقليمية واصدار القوانين والتشريعات لحماية امنها المعلوماتي من استخدام غير آمن لتكنلوجيا المعلومات والاتصالات ، فضلاً عن التعاون الدولي والتنسيق الدائم مع الاجهزة الدولية ذات الصلة في مجال تبادل المعلومات والخبرات الامنية والفنية .

وادى انتشار تقنية المعلومات والإتصالات وما يرتبط منها بجرائم مستحدثه إلى زيادة اهتمام الدول والمنظمات الدولية ببذل العناية اللازمة وتكثيف الجهود لمواجهة مخاطر المعلوماتية ، لا سيما أن اغلب هذه الجرائم هي جرائم عابره للحدود ، وبهذا الصدد عملت عدد من المنظمات الدولية باستمرار لمواكبة المستجدات في أمن الفضاء المعلوماتي ووضعت إستراتيجيات لمحاكمة جرائم الانترنت وصدر عنها تدابير أمنية وتبادل لوجهة واساليب ادارة الازمات والمخاطر الخاصة بأمن المعلومات واجهزة الكومبيوتر ، والبنى التحتية ، وبرامج المعلوماتية ، وانظمة الإتصالات السلكية واللاسلكية حيث اثارت تحديات المخاطر المعلوماتية هاجساً لدى الدول حول أمنها القومي، مما حدى الامر بها إلى تبني حكوماتها إستراتيجيات جديدة للأمن المعلوماتي تتمثل بالعمليات في الفضاء المعلوماتي ، وردع الهجمات المعلوماتية والمشاركة الدولية ، والهدف من هذه الاستراتيجيات هو وضع أساس للإطار القانوني في مجال الامن المعلوماتي ، وتهيئة الظروف الملائمة للتعاون بين القطاعين العام والخاص والدولة في مواجهة التهديدات المعلوماتية ، فضلاً عن العمل على حماية أمن المعلومات ، وخلق بيئة لتطوير التعليم والتدريب في مجال الأمن المعلوماتي . وللإحاطة بموضوع الآليات القانونية في مواجهة الهجمات المعلوماتية سنقوم بتقسيم هذا المبحث على مطلبين، سنتناول في المطلب الاول الجهود الدولية في إطار المنظمات الدولية، أما الثاني سنتطرق فيه لاستراتيجية الدول الوقائية لمنع الهجمات المعلوماتية وعلى النحو الآتي:-

المطلب الاول

الجهود الدولية في اطار المنظمات الدولية

تتطلب مواجهة مخاطر الانشـطة المعلوماتية تظافر الجهود الدولية لمنع تلك الهجمات أو الحد منها على اقل تقدير ، والدول وحدها غير قادرة على مكافحة هذه الانشطة غير المشروعة في الفضـــاء المعلوماتي لذا فأن تحقيق الامن المعلوماتي يتطلب تعاوناً فيما بين الدول وبين المنظمات الدولية والإقليمية وفي مقدمتها منظمة الامم المتحدة ومنظمة حلف شـمال الأطلسـي وغيرها من المنظمات الدولية والإقليمية الاخرى ، ونتيجة الاهتمام المتزايد لمواجهة الهجمات المعلوماتية من خلال وضـع اطر قانونية مشـتركة ، ذهبت المنظمات الدولية إلى انشـاء نظام قانوني ينظم هذه الهجمات ويهدف إلى كبح الانشـطة المعلوماتية الضـارة ، ولأهمية الموضـوع سـنتناوله في فرعين ، نخصـص الفرع الاول إلى جهود الامم المتحدة في مواجهة الهجمات المعلوماتية اما الثاني نتطرق فيه إلى جهود المنظمات الاقليمية في الحد من الهجمات المعلوماتية.

الفرع الاول

منظمة الامم المتحدة

كانت بداية الجهود الدولية من خلال نشـر الجمعية العامة للأمم المتحدة للدليل المعروف باسـم " دليل منع الجرائم المتعلقة بأجهزة الحاسـوب ومكافحتها " في العام ١٩٩٤ ، واشـار هذا الدليل إلى مدى انتشار هذه الجرائم الذي قد يكون بقدر إتساع نظم الاتصالات الدولية ، إلا ان هذا الدليل لم يتطرق إلى جرائم الفضاء المعلوماتي أو الهجمات المعلوماتية ، بل انصب اهتمامه على الجرائم الحاسوبية ، فهو لم يتناول مفهوم الهجمات المعلوماتية بشكلها الحالي المعتمد على

تكنلوجيا المعلومات والاتصـــالات ، متمثلة في شـــبكة الانترنت و ما ينجم عن اســـتخدامها من ارتكاب جرائم معلوماتية ذات نطاق دولي [١].

وســـعت الامم المتحدة من خلال اجهزتها المرتبطة بها إلى تامين ســـلامة تكنلوجيا المعلومات ، والشبكات المعلوماتية بصورة عامة ، وعملت هذه الاجهزة بصورة توافقية عن طريق المشاركة فيما بينها لإيجاد معايير تضمن الحماية لشبكة الانترنت[٢].

وقد بادرت الامم المتحدة إلى بذل مجهودات واسعة بشأن تنظيم الهجمات المعلوماتية منها ما صدر عنها من قرارات وتوصيات ، فضلاً عن قيامها بأنشاء عدة فرق من الخبراء الحكوميين الذين يقومون بإصـــدار التقارير التي تكون لها صـــفة رســـمية تتعلق بطبيعة عملهم وســـنتعرض بشيء من التفصيل عن جهود منظمة الامم المتحدة على وفق الاتي :-

اولاً : قرارات الامم المتحدة ذات الصلة بالهجمات المعلوماتية:

تبنت الامم المتحدة اصدار مجموعة من القرارات بهذا الصدد من اهمها :

١- قرار الجمعية العامة للأمم المتحدة القرار رقم ٥٦ / ١٢١ المتعلق بمكافحة اســتخدام نظم المعلومات الادارية الجنائية لتقنية المعلومات ، وتضـــمن القرار حث الدول الاعضـــاء غلى وضع تشريعات وطنية للحد من اساءة استعمال تكنلوجيا المعلومات [٣].

٢- قرار الجمعية العامة للأمم المتحدة رقم (٥٧ / ٢٣٩) الذي تضـــمن انشـــاء ثقافة عالمية لحماية الفضـــاء المعلوماتي وحماية الهياكل الاســـاســـية للمعلومات ، ويحث الدول

---

(1) United nations , manual on the prevent and control of computer – related crime , international review of criminal policy, No (43-44) , united nations publication , 1994 .

(٢) لبكي جورج ، المعاهدات الدولية للأنترنت : حقائق وتحديات ، مجلة الدفاع الوطني ، بيروت ، ع (٨٣) ، ٢٠١٣ ، متاح على الرابط الالكتروني : https//:cult.ly/.nh5hell.
تاريخ الزيارة ٤/ ٦ / ٢٠٢١.

(3) Ga. Res.56/12/un.Doc,noa / res 15/ 121/ 2002 . avail able at:https//;undocs. org/iar / res /15 ,/121.

تاريخ الزيارة ١٤ / ٣ / ٢٠٢٢ .

والمنظمات الدولية إلى تبادل افضـــل الممارســـات وتبني اســـتراتيجيات لحماية أمن الفضـــاء المعلوماتي [١].

٣- قرار الجمعية العامة للأمم المتحدة رقم (٣٢/٥٨) الخاص بالتطورات الحاصـــلة في ميدان المعلومات والاتصالات في سياق الامن الدولي ونزع السلاح ، والحث على تطوير وتطبيق المعلومات ووسائل الاتصالات السلكية واللاسلكية واكد على ان تكنلوجيا المعلومات والاتصالات هي ذات استخدام مزدوج سواء لأغراض مشروعة أو غير مشروعة[٢].

٤- قرار الجمعية العامة للأمم المتحدة رقم (١٧٧/٦٠) الخاص بضـرورة تنسـيق القوانين لمكافحة الجرائم المعلوماتية ، الذي جاء تأييداً لإعلان بانكوك عام ٢٠٠٥ وقد شـجع هذا الاعلان جهود المجتمع الـدولي الراميـة غلى تعزيز التعـاون المشـــترك لمنع الجرائم المعلوماتية بما في ذلك تسليم المجرمين والمساعدة القانونية المتبادلة[٣].

ثانياً :- قرارات المجلس الإقتصادي والإجتماعي

صـــدر عن المجلس الإقتصـــادي والإجتماعي قرارات عدة لمواجهة خطر الهجمات المعلوماتية ، والتي دعت فيه اللجنة المعنية إلى تســـخير العلم والتكنلوجيا لأغراض التنمية. من القرارات التي صدرت عن المجلس الإقتصادي والإجتماعي هي:

١- القرار (٤٦/٢٠٠٦) والخاص بمتابعة نتائج مؤتمر القمة العالمي لمجتمع المعلومات واستعراض لجنة تسخير العلم والتكنولوجيا لأغراض التنمية.

٢- القرار (٨/٢٠٠٧) بشـــأن تدفق المعلومات لمتابعة مؤتمر القمة العالمي لمجتمع المعلومات بما في ذلك التطبيقات المعلوماتية، واحاطت اللجنة المعنية علماً بما أسفر عنه مؤتمر

---

[١] ينظر : الجمعية العامة للأمم المتحدة ، القرار رقم (٢٣٩/٥٧) في ٣١ كانون الأول ٢٠٠٣، ينظر الوثيقة (A/RES/57/239).

[٢] ينظر: الجمعية العامة للأمم المتحدة ، القرار رقم (٣٢/٥٨) في ١٨ كانون الأول ٢٠٠٣، ينظر الوثيقة: (A/RES/58/32)

[٣] ينظر: الجمعية العامة للأمم المتحدة ، القرار رقم (١٧٧/٦٠) في ١٦ كانون الأول ٢٠٠٥، ينظر الوثيقة: (A/RES/60/177)

القمة العالمي لمجتمع المعلومات والذي أنعقد على مرحلتين، الأولى في جنيف عام ٢٠٠٣، والثانية في تؤسس عام ٢٠٠٥ بالإستناد إلى ما ورده من مساهمات ذات الصلة بالموضوع[١].

علاوة على ذلك شهد المجلس الإقتصادي والإجتماعي إنعقاد دورته لعام ٢٠١٠ ، التي تضمنت التحديات التي يواجها الامن المعلوماتي الناجمة عن استخدام الانترنت غير المشروع ، وقد دعا المجلس لطرح عدة مبادرات دولية تكفل تبادل المعلومات وافضل الممارسات والبحث والتدريب ، ودعى القرار كذلك إلى اتباع نهج قائم على ادراك المخاطر ، واحاطة جميع اصحاب المصلحة علماً بالمخاطر ذات الصلة بالتدابير الوقائية ، والردود الفعالة على نحو مناسب وحث القرار الدول على بذل المزيد من العناية الواجبة بموضوع الامن المعلوماتي وحماية الهياكل الاساسية الحيوية للمعلومات ، كما دعى القرار إلى ضرورة استخدام موظفين ذات خبرات ومهارات عالية في مجال تكنلوجيا المعلومات ، خصوصاً في ظل تزايد الهجمات المعلوماتية [٢].

الفرع الثاني

المنظمات الاقليمية

قامت للمنظمات الاقليمية بجهود بارزة في مجال تنظيم الهجمات المعلوماتية وركزت على استراتيجيات محددة في مجال الأمن المعلوماتي ، ومن أبرز هذه المنظمات الاقليمية هي: الاتحاد الاوربي، منظمة حلف شمال الاطلسي ، ومنظمة شنغهاي للتعاون، لذا سنتناول جهود كل منظمة بما أسهمت به في مجال تحقيق الأمن المعلوماتي وعلى النحو الآتي:

اولاً : الإتحاد الاوربي

تبنى الاتحاد الاوربي في عام ٢٠١٣ استراتيجية جديدة للأمن المعلوماتي، وهي أول لمبادرة مهمة ذات أثر فعال نحو إرساء قواعد الأمن المعلوماتي الاوربي، تضمنت الاستراتيجية

---

[١] ينظر : الجمعية الأمم المتحدة ، المجلس الاقتصادي والاجتماعي، القرارات المرقمة (٤٦) في ٢٠٠٦و ((l . rev / 3 / 62 /a ٢٠٠٧، والقرارين (٧، ٨) في ٢٠٠٩.

[٢] الأمم المتحدة، المجلس الاقتصادي والاجتماعي ، الدورة الموضوعية ، البند (١٣ / ب) من جدول الاعمال المؤقت المسائل الاقتصادية والبيئة : تسخير العلم والتكنلوجيا لأغراض التنمية والتقدم المحرز في تنفيذ ومتابعة نتائج مؤتمر القمة العالمي المجتمع المعلومات على الصعيدين الاقليمي والدولي نيويورك ٢٨ حزيران ٢٣ تموز ٢٠١٠.

رؤية الاتحاد حول جعل فضـــاء معلوماتي خالي من الاضـــطرابات ، واحتوت الوثيقة على جملة من المبادئ اهمها[١]:

١- العمل على تطوير ســياســة الدفاع المعلوماتي والقدرات ذات العلاقة بســياســة الامن والدفاع المشتركة .

٢- تطوير الموارد الصناعية والتكنلوجية للأمن المعلوماتي .

٣- ارساء سياسة ذات صبغة دولية متماسكة للفضاء المعلوماتي خاصة بالاتحاد الاوربي وتعزيز القيّم الاساسية لهذا الاتحاد.

وفي عام ٢٠١٤ اعتمد المجلس الاوربي ســياســة الدفاع المعلوماتي الإطارية اثناء إجتماع وزراء دفاع الدول الاعضــاء في الاتحاد وقد تم مناقشــة قضــايا الامن المعلوماتي في الإجتماع ، والهدف من هذه السياسة هو تعزيز التضامن والتعاون مع جميع الاطراف الفاعلة في هذا الاطار من غير الدول الاعضـــاء في الاتحاد والتأكيد على البحوث والعلوم الاخرى التي تعنى بقضـــايا الامن المعلوماتي[٢].

كذلك صدر عن الاتحاد الاوربي التوجيه الخاص بحماية البيانات الشخصية عام ٢٠١٦ ، ويهدف التوجيه (Etu 2016 / 679) إلى توفير الحماية للأشـــخاص الطبيعيين فيما يتعلق بمواجهة البيانات الشــخصــية ، فضــلاً عن تعزيز حرية نقل هذه البيانات ، إذ بموجبة تم الغاء التوجيه (Ec / 46 / 95) المتعلق بتنظيم حماية البيانات العامة وهدف هذا التوجيه المساهمة في تحقيق حيز من الحرية والأمن والعدالة والوحدة الاقتصــادية ، وحماية الاشــخاص الطبيعيين فيما يتعلق بتنسيق الجهود لغرض معالجة بياناتهم الشخصية [٣].

---

(1) Laszlo kovacs , cyber security policy and strategy in the European union and NATO , national Unirersity of public service , land force academy review, Vol.(3) , No.(1) (89) , Budabst , hungary , 2018 , p. 17 .

(2) See ; An outline for Euoropean cyber diplomacy Engagement , 9967 / 4 / 14 rev4 , DGDIC , Brussels , septemper 2014 .

[٣] للاطلاع على التوجيه منشور على الرابط الالكتروني :

https//:eur – lex . Europa . eu I legal – content / eu / txt / pdf .

تاريخ الزيارة ١٤ / ٩ / ٢٠١٢ .

علاوة على ذلك وفي السادس من حزيران من عام ٢٠١٦ تبنى الاتحاد الاوربي بصورة رسمية التوصية رقم (٢٠١٦ / ١١٤٨) ذات الصلة بالتدابير الخاصة بمستوى عالٍ من أمن الشبكات وانظمة المعلومات عبر الاتحاد ، وكان الهدف الاساسي من هذه التوجيه هو ضمان توفير مستوى عالٍ من الامن المشترك للشبكات وانظمة المعلومات عبر الدول الاعضاء في الاتحاد واتخاذ استراتيجية وطنية لأمن الشبكات والمعلومات وتدابير فنية للحد من الهجمات المعلوماتية[١].

وقبل ذلك قام مجلس اوروبا ، باتخاذ خطوات جادة ومباشرة في اطار تنظيم الامن المعلوماتي لأي منظمة دولية أو إقليمية اخرى ، فقد قام بوضع اتفاقية بودابست ذات الصلة بالجريمة المعلوماتية ، وكانت أول معاهدة دولية ساهمت في مكافحة الجرائم المعلوماتية من خلال تفعيل التشريعات الوطنية وتنسيقها ، والحث على التعاون بين الدول في مواجهة الجرائم المعلوماتية ، وعقدت في العاصمة المجرية بودابست عام ٢٠٠١ ، وكان التوقيع على تلك المعاهدة بمثابة الخطوة الاولى نحو التضامن الدولي لمكافحة هذه الجرائم التي تمر عبر شبكة الانترنت[٢].

وادراكا من الدول بأهمية الاتفاقية الاوربية فقد انصب اهتمامها اثناء صياغة الاتفاقية على التوصيات التي صدرت عن لجنة الوزراء بالاتحاد الاوربي ومن اهمها: [٣]

- التوصية رقم ٨٥ / ١٠ ذات الصلة بتنفيذ الإتفاقية الاوربية للمساعدة المتبادلة في المسائل الجنائية فيما يتعلق بالإنابة القضائية بشأن اغراض الإتصالات السلكية واللاسلكية .
- التوصية رقم ٨٨ / ٢ ، المتعلقة بالقرصنة في مجال حقوق التأليف والنشر والحقوق المجاورة .
- التوصية رقم ٨٧ / ١٥ المتضمنة تنظيم استخدام البيانات الشخصية في قطاع الشرطة.
- التوصية رقم ٩٥ / ٤ المتعلقة بحماية البيانات الشخصية في مجال خدمات الاتصالات.

---

(1) See ; Directive 2016 / 1148 /concerning measures for ahigh common level of security of network and in formation systems 2 statory instrument 360 of 2018 .

[٢] شيخة حسين الزهراني ، التعاون الدولي في مواجهة الهجوم السيبراني ، مجلة جامعة الشارقة للعلوم القانونية ، م (١٧) ، ع (١) جامعة الشارقة – كلية القانون ، الامارات العربية المتحدة ، ٢٠٢٠ ، ص٧٥٣ .

[٣] د. رامي متولي القاضي ، مكافحة الجرائم المعلوماتية ، دراسة مقارنة ، ط١ ، دار النهضة ، ٢٠٠٠ ، ص٦١-٦٢ .

- التوصـية رقم ٨٩ / ٩ المتعلقة بالجرائم المتصـلة بالكومبيوتر التي توفر مبادئ توجيهية للجهات التشريعية الوطنية بشأن تعريف بعض جرائم الكومبيوتر.

- التوصـية رقم ٩٥ / ١٣ ذات الصـلة بالمشـاكل التي يطرحها قانون الاجراءات ذات العلاقة بقانون تكنلوجيا المعلومات.

وفي عام ٢٠٠٥ اعتمد المجلس قراراً يتعلق بالهجمات ضـد المعلومات (jtla/ 2005 /222)[١]. وجاء هذا القرار مكملاً ومتسـقاً لما ورد في اتفاقية بودابسـت لعام ٢٠٠١ وهو مخصص لمكافحة الجريمة المعلوماتية التي تستهدف الحاق اضراراً فادحة بالبنى التحتية للدول.

ثانياً : منظمة حلف شمال الاطلسي (NATO)

إن اهتمام حلف شمال الاطلسي بالأمن المعلوماتي (NATO) ، لم يأتٍ من فراغ وأنما جاء نتيجة لما تعرضـت له بعض الدول التابعة له لهجمات معلوماتية اسـتهدفت البنى التحتية المعلوماتية لهذهِ الدول ، وخير مثال على ذلك ما تعرضـت له اسـتونيا عام ٢٠٠٧ من هجمات معلوماتية، كذلك الهجمات المعلوماتية التي تعرضـت لها جورجيا اثناء نزاعها المسـلح مع روسـيا وعلى اثر ذلك تبنى حلف شـمال الاطلسـي (الناتو) في عام ٢٠٠٨، عقد قمة بوخارسـت وهي تعبر عن سياسـة الدفاع المعلوماتي الهادفة إلى حماية انظمة المعلومات الرئيسـية ومساعدة دول الحلفاء لمواجهة أي هجوم معلوماتي[٢].

وبادر الحلف إلى انشاء مركز الدفاع المعلوماتي التعاوني للتمييز في مدينة تالين عاصمة اسـتونيا، للفترة من عام ٢٠٠٩ إلى عام ٢٠١٢، وبطلب من مركز الدفاع المعلوماتي للتمييز، حيث عملت مجموعة من الخبراء والباحثين على مدى امكانية تطويع المبادئ القانونية على الهجمات المعلوماتية[٣].

وأدراكاً منه بأهمية الأمن المعلوماتي أوضـح رئيس وحدة الدفاع المعلوماتي التابع لحلف شمال الاطلسـي سليمان انيل (suleyman Anil) إلى أنه "الهجمات المعلوماتية التي تستهدف

---

[١] للاطلاع على فحوى القرار – متاح على الرابط الالكتروني:
https//:Eur/lex/Europa.eu//ex uriseiv//ex uriserv do.uri=CELEX;32005 fozzz;en; htmz
.
تاريخ الزيارة ١٧ / ٦ / ٢٠٢١ .

[2] MAX Smeets, NATO allies offensive cyber policy: agrowing divide , The Haqu center for strategic studies, Agust 2021, availableat: http://cutt.us/sk1j.

[٣] بشـار خليل، ماهي الحرب السـيبرانية؟ مسـتقبل مخيف للصـراع المرقمي، مجلة المعلوماتية ، ع (١٥٤)، الجمعية السورية المعلوماتية، ٢٠٢٠، متاح على الموقع الالكتروني: تاريخ الزيارة ٢٠٢٢/٤/٢٥.
Http://www.scs.org.sy/?=scs/informag/showarticlendos.

البنية التحتية لا يمكن عملياً إيقافها، ومن ثم فأن الدول بحاجة الى تقوية بنيتها المعلوماتية الاساسية نتيجة لما تمثله هذهِ الهجمات من مشكلة عالمية مستقبلية[١].

ومن أهم الجهود التي قام بها حلف الشمال الاطلسي في اطار بذل واجب العناية لحماية البنى التحتية المعلوماتية لدول حلف الناتو، هي اجراء تمارين في مجال الدفاع المعلوماتي، حيث تم تشكيل عدة فرق من الدول الاعضاء في الحلف لإجراء ممارسات وتمارين للدفاع عن شبكات الحاسوب الافتراضية من خطر الهجمات المعلوماتية، وكان الغرض من هذه التمارين هو تكثيف التعرف على البيئة المعلوماتية الدولية وتقرير أطر التعاون الدولي للحد من الحوادث ذات العلاقة بالهجمات المعلوماتية.[٢]

ثالثاً: مبادرات منظمة شنغهاي للتعاون

بادرت منظمة شنغهاي للتعاون التي سبق ذكرها في الفصل الأول من هذهِ الدراسة في معرض التعريف بالهجمات المعلوماتية الى إتخاذ العديد من الخطوات الجادة والمهمة في اطار التعاون في مجال الأمن المعلوماتي: ففي العام ٢٠٠٩ تم صدور إعلان يكاتر ينبورغ وذلك في قمة منظمة شنغهاي للتعاون التي عقدت في يكاتر ببنبورغ في روسيا الاتحادية والذي اشار إلى رغبة المنظمة في التعاون والالتزام لغرض منع الحرب والهجمات المعلوماتية[٣].

وقد تضمنت الفقرة (٣) من المادة (٣) من اتفاقية أمن المعلومات التي وافقت عليها دول المنظمة عام ٢٠٠٩، وضع تدابير مشتركة لتطوير أحكام القانون الدولي التي تحد من إنتشار واستخدام الاسلحة المعلوماتية التي تهدد القدرة الدفاعية والأمن القومي، إذ تسعى الدول إلى تطوير قواعد القانون الدولي للحد من استخدام الفضاء المعلوماتي بشكل غير مشروع، ومن أهم ما قدمته منظمة شنغهاي للتعاون فيما يخص أمن المعلومات هي مدونة السلوك الدولية لأمن المعلومات المدونة التي تم تقديمها إلى الجمعية العامة للأمم المتحدة عام ٢٠١١، وهي جهد

---

[١] د.عادل عبدالصادق، الارهاب الالكتروني: القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة، مركز الاهرام للدراسات السياسية والاستراتيجية، ط١، القاهرة، ٢٠٠٩، ص٣٦٧.

[2] Alexander klimbury , Nional cyber security farme work manual, NATO CCD COE, Tallinn Estonia, 2012, p124, 185.

[3] Maonga, sharon keubo: Acase of in capacity : The interrogation of inter national (Human itarian law as A satis factory Regulator of cyber war fare, strathmor university strat hmore law school, 2017, p.40,A: Avali ableat :http://cut.ly/qigua9h.

دولي يحث على تطوير قواعد السلوك والتأكيد على سيادة الدولة وإقليمها في الفضاء المعلوماتي.[١]

وقد نصت الإتفاقية على قائمة من التهديدات التي تعد تهديدات رئيسية لأمن المعلومات في المجال الدولي، وحث الدول الأعضاء على التعاون في مجال أمن المعلومات الدولي من خلال[٢]:

١- تطوير واستخدام اسلحة المعلومات، وأعداد وإدارة حرب المعلومات.
٢- الإرهاب المعلوماتي.
٣- الجرائم المعلوماتية.
٤- نشر المعلومات الضارة على النظم الإجتماعية والإقتصادية والسياسية.
٥- تهديدات لضمان التشغيل المستقر والبنى التحتية للمعلومات العالمية والوطنية.

المطلب الثاني

إستراتيجية الدول الوقائية لمنع الهجمات المعلوماتية

إن أهم التحديات والصعوبات التي تواجه الدول التي هي مسألة توفير الحماية اللازمة لأنظمتها المعلوماتية، خاصة في ظل الأستغلال المتزايد والمفرط لتكنولوجيا المعلومات والإتصالات، وأن سوء استخدام الفضاء المعلوماتي بصورة غير مشروعة جعل من الدول في حالة حرب دائمة مع من يستخدمون الأنشطة المعلوماتية المارة عبر الفضاء المعلوماتي سواء كانوا دولاً ، أم فواعل من غير الدول ممن لديهم المهارات والوسائل المعلوماتية ويمتلكون القابلية على توظيفها لإختراق الانظمة المعلوماتية الحساسة، حتى وأن كانت تلك الدول قد اتخذت نوعاً من الاحتياطات والتدابير الاحترازية، فالهجمات المعلوماتية التي تحدث في الفضاء المعلوماتي من شانها انتهاك الأمن القومي للدول، ان لم تقم تلك الدول بتفعيل استراتيجيات اليقظة المعلوماتية من خلال مراقبة الأنشطة التي تستهدف الأنظمة المعلوماتية، حتى يتم الاستباق في وضع الآليات القانونية والفنية التي تواجهه التحديات الناشئة عن التطورات التكنولوجية ومن أجل

---

(1) See Henry Roigas, An Upolated Draft of the code of conduct distributed in the united Nations-wats New? Availabe at:http://CCDOE.org/incyber-articles/an-upolacted.

[٢] ينظر المادة (٢) من أتفاقية شنغهاي للتعاون في مجال أمن المعلومات لعام ٢٠١١.

السـيطرة أو الحد من الهجمات المعلوماتية المارة عبر الفضـاء المعلوماتي إعتمدت بعض الدول اسـتراتيجيات وقائية لحماية أمنها المعلوماتي من خطر هذه الهجمات ومن هذهِ الدول الولايات المتحدة الامريكية، وروسيا الاتحادية والصين وغيرها من الدول الأخرى.

ومن الأهمية بمكان، أرتأينا أن نتناول في هذا المطلب الاستراتيجيات الوقائية ذات الصلة بمنع أو الحد من انتشـار الانشـطة المعلوماتية وعلى فرعين خصـصـنا الفرع الأول لتعريف الاستراتيجية الوقائية ووسائل تطبيقها، وفي الفرع الثاني، نتناول استراتيجيات بعض الدول الوقائية في منع الهجمات المعلوماتية وعلى النحو الآتي:

الفرع الأول

تعريف الاستراتيجية الوقائية ووسائل تطبيقها

أولاً: تعريف الاستراتيجية الوقائية

يعد جوزيف ناي ابرز المهتمين بايجاد تعريف ملائم للاسـتراتيجية الوقائية في المجال المعلوماتي إذ يعرفها على انها "القدرة على الحصـول على النتائج المرجوة عن طريق إسـتخدام الفضاء المعلوماتي"[١]

أما الكاتبان جون ارغولا وديفيد رونفليت، فقد حاولا في مقالهما المنشـور عام ١٩٩٣، بعنوان (الحرب المعلوماتية قادمة) وضـع تعريف للاستراتيجية المعلوماتية على أنها "الاستعداد لتنفيذ العمليات العسكرية وفقاً للفضاء المعلوماتي العالمي".[٢]

كذلك الكاتبان نيتان ميكي وليهاتو بيكا قدما تعريفاً آخر للاسـتراتيجية الوقائية الأمنية في كتابهما (الأمن المعلوماتي) على أنها "مجموعة من الأجراءات التي اتخذت في الدفاع ضـد هجمات قراصنة الحاسوب ، ويتضمن تنفيذ التدابير المضادة".[٣]

---

(1) Joseph s.Naye, cyber powr, harvad Kennedy schod, 2010, p.3.

(2) John Arguilla and David Ronfeldt, cyber is coming, RAND corporation, 1993, p.5.

(3) Marttilehto and Pakka Neittaan maki, cyber security: power and Technology, Newyork, 2018 . p.77.

ونســـتطيع القول أن ما يؤخذ على هذا التعريف المتقدم قد حاولا فيه الكاتبان الخلط بين اســـتراتيجية الأمن المعلوماتي التي تضـــعها الدول لحماية أمنها القومي من خطر الهجمات المعلوماتية وبين التدابير المضـادة والتي سـنأتي على ذكرها في الفصـل الثالث من هذهِ الدراسـة، والتي تلجأ إليها الدول لمنع الهجمات المعلوماتية غير المشروعة عبر فضائها المعلوماتي كإجراء للرد على هجمات غير مشروعة أستهدفت انظمتها المعلوماتية وإخترقت سيادتها المعلوماتية وهي ناشـــئة عن ردة فعل الدولة المعتدى عليها، إذ هناك شـــروط محددة لإباحة اســـتخدام التدابير المضادة والتي تدخل في إطار المشروعية الدولية.

إلا أن وزارة الدفاع الامريكية (البنتاغون) بادرت إلى وضـع تعريف للاسـتراتيجية الامنية المعلوماتية يوصـــف على أنه متزن ودقيق نوعاً ما، فقد عرفتها على أنها "مجموعة الاجراءات التنظيمية اللازمة لضـــمان حماية المعلومات والحفاظ عليها بجميع اشـــكالها المادية والمعلوماتية ضد مختلف الجرائم مثل الهجمات، التخريب والحوادث"[١].

ثانياً: وسائل تطبيق الاستراتيجية الوقائية المعلوماتية

عندما تبادر الدول في وضـــع اســـتراتيجية وقائية أمنية لحماية فضـــائها المعلوماتي فهي تبتغي أن تكون تلك الاســـتراتيجية ناجحة ومحققة لأهدافها، ولكي تحقق الاســـتراتيجية الوقائية أغراضـــها التي أعدت من أجلها هناك وســـيلتان أحدهما مكملة للأخرى لتوفير مثل هذه الحماية وهما الدفاع عن اصـــول البلد من الهجمات المعلوماتية، وردع الطرف المعتدي عن القيام بمثل هذه الهجمات[٢]:

١- **الدفاع المعلوماتي:** ويقصـــد به الدفاع عن شـــبكات الحاســـب الآلي من أي اختراق خارجي عبر وضـــع إجراءات معينة لغرض تأمينها، يقوم بها حراس الشـــبكات بواســـطة برامج وتطبيقات تؤدي وظيفة المراقبة للزائرين غير المرغوب بهم (المخترقون)، واســـتباقهم للتعرف على هوياتهم أمام بوابات افتراضـــية للشـــبكات، إلى جانب المســـح الشـــامل للشـــبكات بحثاً عن

---

[١] صلاح مهدي هادي وزيد محمد علي اسماعيل، الأمن السيبراني كمرتكز جديد في الاستراتيجية العراقية، مجلة قضايا سياسية، مكتبة العلوم السياسية، جامعة النهرين، ع (٦٢)، اس (١٢) ، ٢٠٢٠، ص٢٧٦.

[٢] هوبرت لين، النزاع السيبراني والقانون الدولي الانساني، مصدر سابق، ص٥٢٢.

فيروســـات معلوماتية[١] ويتضـــمن الدفاع الوقائي اتخاذ تدابير تقلل من احتمالية نجاح عملية هجومية، وتتمثل بإجراءات تمنع الخصـم المعتدي من الوصـول لإهدافه، أو تمكن الضـحية من التعافي بصورة سريعة من آثار عملية هجومية ناجحة.[٢]

ويقصد به كذلك مجموعة الوسائل الفنية وغير الفنية التي تسمح للدولة بالدفاع في الفضاء المعلوماتي من خطر الهجمات المعلوماتية ضد نظم المعلومات الحرجة.[٣]

وغالباً ما تتبع الدول استراتيجية الدفاع عبر وسائل مختلفة لتحقيق الأمن المعلوماتي، ومن خلال قيام الدول بإنشاء انظمة معلوماتية دفاعية ذات مستويات عالية من الاجهزة، للحيلولة دون اختراقها من قبل الخصوم، إلا إن أهم التحديات التي تواجهه الفواعل في مجال الدفاع المعلوماتي هي صـــعوبة تطوير نظام دفاعي متكامل يحول دون تعرضـــها لهجمات، أو حتى إيقافها فور وقوعها، إذ أن معظم انظمة الدفاع تحقق قدراً من التأمين للأنظمة والشـــبكات المعلوماتية لفترة محددة إلى أن يتم اكتشـاف نقاط الضـعف فيها والعودة إلى مهاجمتها مرة أخرى، وبالتالي تصـبح عديمة الفائدة، فقوة النظام المعلوماتي وحمايته من خلال مستويات مختلفة من الدفاع لا يستطيع توفير ضـــماناً كاملاً لحمايته بشـــكل كامل، وإنما فقط يطيل مدة التأمين لحين اكتشـــاف مواطن الخلل والضعف فيه تمهيداً لمهاجمته مرة أخرى.[٤]

والهدف الأســـاس من عملية الدفاع المعلوماتي بصـــورة عامة يتمثل بمنع الهجمات على شبكات البنية التحتية المدنية والعسكرية، كذلك على شبكات الشركات الخاصة وشركات الأفراد، وعادة ما يكون من الصـــعب الحد من هذهِ الهجمات التي تقوم الدول بتنفيذها وعلى العكس من القدرات التكنولوجية التي تمتلكها المنظمات غير الحكومية والأفراد هي قدرات في العادة أقل تطوراً، ويمكن معالجتها من خلال وضـــع حلول تكنولوجية آنية على درجة من البســـاطة، تقوم

---

[١] د.سيف نصرت الهرمزي، وصف المقاربات لمنظورات الفاعل الرقمي والإنكشاف الاستراتيجي في ظل الفضاء المعلوماتي، مجلة اداب الفراهيدي، ع(٣٧)، ٢٠١٩، ص٤٣٣.

[٢] هربرت لين ، مصدر سابق، ص٥٢٢.

[٣] د.ايهاب خليفة، الحرب السيبرانية، الاستعداد لقيادة المعارك في الميدان الخامس، مصدر سابق، ص١٨٧.

[4] Amit sharma, cyber wars: Aparadigm shift from means to Ends, strategic Anolysis, vol (34), 2010, p.71.

بدور مركزي في بذل الجهود الدفاعية، وقد سارعت الدول فضلاً في زيادة تطوير برامج المساعدة في الدفاع عن الشبكات والأنظمة المعلوماتية، إلى إقامة علاقات شراكة مع مؤسسات القطاع الخاص لضمان تحديث انظمة الأمن على الشبكات التي يكون لها اتصال مباشر بالأنظمة الحكومية[١].

وعلاوة على ذلك ليس من السهولة القيام بإجراء الدفاع المعلوماتي عبر الانترنيت فقط ، بل يتطلب الأمر الاعتماد على وسائل أخرى متعددة الأنواع مثل جمع المعلومات الاستخبارية، وتأمين الشبكات، واعتراض الهجمات، واتخاذ تدابير قانونية، فليس هناك معايير أو قوانين دولية واضحة وذات أثر ملزم بشأن السلوك في الفضاء المعلوماتي[٢].

ويختلف الدفاع الوقائي المعلوماتي عن نظيرة الدفاع العادي في عنصرين هما: الاكتشاف المبكر للهجمات المعلوماتية و التعامل معها في حال حدوثها، فبينما يعمل الدفاع العادي على التحقق من حدة الهجمات والتعافي السريع منها، يعمل الدفاع الوقائي في استباق وإعاقة الخصم عن تنفيذ الهجمة المعلوماتية، إذ يعمل الدفاع المعلوماتي الوقائي من خلال اساليب رئيسية أهمها هي[٣] :

١- الكشف المبكر للهجمات: من خلال استخدام مجسات على الشبكات والبرامج والتطبيقات.

٢- الهجوم المعلوماتي الاستباقي: من خلال استخدام ونشر الديدان البيضاء White wormss، وهي برامج تكون لها القدرة على اكتشاف التطبيقات الضارة وتدميرها قبل توظيفها باطلاق هجمة معلوماتية محتملة.

---

(1) Milton L.Mueller, Andreas Schmidt and Brenden Kuerbis: internet security and Networked Governance in inter national, inter national studies Review 15 No (1), 2013, pp.86-102.

(2) David Clark and Whifield Diffe, cyber security and inter national Agree ments, procedings of awork shop on Deterring cyber Attaks: informing strategies and Developing options for U.S.policy National Academies press , 2010, p.99.

(٣) د.أيهاب خليفة، مجتمع ما بعد المعلومات، مصدر سابق، ص٢٠٣.

ثانياً: الردع المعلوماتي

تعود أصـــول الردع المعلوماتي إلى عملية عاصـــفة الصـــحراء في عام ١٩٩١، عندما اكتسبت فكرة : الثورة في الشؤون العسكرية" صدى واسعاً، فخلال المراحل الأولى من العملية، نفذت الولايات المتحدة " حرب المعلومات" information warefare، ضـــد الحكومة العراقية السابقة، وقد أدى الهجوم إلى ايقاف عمل شبكات اتصالاتها العسكرية ليكشف هذا الموقف عن أهمية الردع المعلوماتي وأثره في النزاعات المعاصرة.[١]

ويقصد بالردع المعلوماتي على أنه "منع الاعمال الضارة ضد الاصول الوطنية في الفضاء المعلوماتي والأصول التي تدعم العمليات الفضائية".[٢]

ويختلف الردع المعلوماتي عن الردع التقليدي الذي هو انعكاس للردع النووي، وذلك بسب إن البيئة التي يتم توظيفها للانترنت مختلفة تماماً من عدة جوانب أهمها[٣]:

١- صعوبة معرفة الطرف المعتدي والذي يتم من خلال التتبع المتواصل والمصداقية.

٢- صعوبة جعل الخصم في وضع التهديد فالدول التي تتعرض لهجمات معلوماتية هي وحدها من تستطيع معرفة مدة نجاح وفشل هذه الهجمات.

٣- صعوبة منع الهجمات الصفرية، حيث إن الفضاء المعلوماتي يتميز بالتحديث المستمر فيتم انتاج فيروســـات جديدة تســـتوعب التغييرات الحديثة التي تظهر في الانظمة قبل ان يتم معالجتها.

ومن نافلة القول أن صدور الفعل في الردع يستند على ثلاثة ركائز اساسية، حيث تتمثل الاولى في مدى مصداقية الدفاع عن انظمة المعلومات ومنع أي محاولات لإختراقها عبر أنظمة نسخ احتياطية (Backup system) وهذا يعني أن أي هجوم يتم تنفيذه في هذه الحالة لن يسفر

---

[١] حســين قؤادرة، الردع الســيبراني بين النظرية والتطبيق، المجلة الجزائرية للأمن والتنمية، م (٩)، ع (١٦) ، جامعة أم البواقي، الجزائر، ٢٠٢٠، ص٥١٨-٥٣١.

[٢] د.رغدة البهي، الردع السيبراني، المفهوم والاشكاليات والمتطلبات، مجلة العلوم السياسية، القانون ، المركز الديمقراطي، برلين، ع (١) ، ٢٠١٦، ص١٠.

[٣] د.ايهاب خليفة، امكانية تحقيق الردع في صراعات الفضاء الالكتروني، مجلة اتجاهات الأحداث المتقدمة، ع (١٣)، ٢٠١٥ ، ص٤٩.

عن احداث التدمير الكلي في ظل امكانيات الاســـتعادة الذاتية، أما الركيزة الثانية فتتمثل في القابلية على الإنتقام التي يتطلب توافر آليات للرد على الهجمات، ما يمنح الطرف الذي تعرض للهجوم ميزة القدرة على تحقيق التوازن مع الطرف المهاجم، أما الركيزة الثالثة فهي عملية الرغبة في الرد مع وجود القدرة على القيام بالفعل.[١]

ومن الجدير بالذكر أن الدول اليوم بحاجة ماسـة إلى الكشـف المبكر، أو الأنذار المسـبق عن الهجمات المعلوماتية الوشيكة وهو أمر حيوي في المجال المعلوماتي، إذ يعد الكشف المبكر عن الهجمات أحد مبادئ الردع المعلوماتي، ذلك بأن منع الهجمات المعلوماتية غير ممكن في حـالـة وجود انـذار مبكر فعـال وكـافٍ، فـالـدول بحـاجـة إلى تقديم الإنـذار المبكر ليس فقط إلى الانظمة المعلوماتية الحكومية فقط بل يتوجب تقديمة إلى المنظمات والشـركات ايضـاً، وقد بدأت الدول فعلاً ببذل جهود حثيثة في جمع المعلومات الاســتخبارية، ووســعت نطاق المشــاركة في المعلومات مع القطاع الخاص، إلا أن هذه المشـــاركة لا زالت تواجه تحدياً كبيراً ، الأمر الذي يستدعي إلى اجراء تغييرات وحلول قانونية وتنظيمية في الحكومات والشركات على حد سواء[٢].

---

[١] د.رغدة البهي، مصدر سابق، ص٥٢.

[2] Aviram Zrahia, A Multidisciplinary Analysis of cyber in for mation sharing, military and Affairs, No(3), 2014, pp.59-76.

الفرع الثاني

استراتيجية بعض الدول الوقائية لمنع الهجمات المعلوماتية

اتخذت بعض الدول في حماية فضائها المعلوماتي العديد من التدابير القانونية والإجراءات الداخلية في سبيل مواجهة خطر الهجمات المعلوماتية ومحاولة منعها أو الحد منها على أقل تقدير، ومن هذهِ الدول الولايات المتحدة الامريكية، وروسيا الاتحادية، والصين ، وغيرها من الدول الاخرى، لذا سنتعرض بشيء من التفصيل لاستراتيجيات هذه الدول الوقائية في مجال الأمن المعلوماتي وعلى النحو الآتي:

أولاً: الولايات المتحدة الامريكية:

مع تصاعد التهديدات الإرهابية داخل الولايات المتحدة الامريكية بعد هجمات ايلول ٢٠٠١ ، تنبهت الإدارة الأمريكية في عهد بوش الأبن إلى خطورة الهجمات والتحديات غير التقليدية التي تواجها، بما فيها حرب المعلومات التي تهدد الأمن القومي الأمريكي، وتستدعي اتخاذ تدابير حاسمة للتصدي لها، لاسيما مع انتشار مثل هذهِ القدرات (المعلوماتية)، في ايد الخصوم المحتملين، وتزايد احتمال لجوئهم إلى اعتماد مثل هذهِ الوسائل في وجه الهيمنة الساحقة التقليدية للولايات المتحدة الامريكية، ونتيجة لذلك قد قرمت وزارة الدفاع الامريكية للكونغرس تقرير المراجعة الرباعية وهو بمثابة اطار رسمي تضمن الاشارة الأولى لهذهِ، الاحتمالات، تكلل بالاشارة التي اوردها نائب وزير الدفاع الامريكي عام ٢٠٠١، ولفوتز إلى " ضرورة تبني الولايات المتحدة لاستراتيجيات جديدة للدفاع ضد أنماط غير تقليدية من الحروب وفي مقدمتها حرب الشبكة الدولية للمعلومات[١]، وفي شباط عام ٢٠٠٣، اطلق الرئيس بوش الأبن الاستراتيجية القومية لتأمين الفضاء المعلوماتي، وأهم ما اشتملت عليه هذهِ الاستراتيجية هو تأمين البنية التحتية للولايات المتحدة الامريكية في كافة مؤسسات الدولة وكان الهدف منها[٢] :

١- منع الهجمات المعلوماتية.

---

[١] د.سامر مؤيد عبداللطيف، مصدر سابق، ص٩٣.

[٢] د.ايهاب خليفة، القوة الالكترونية، كيف يمكن تدبير الدول شؤونها في عصر الانترنت، مصدر سابق، ص١٣٣.

٢- تقليل نقاط الضعف التي تسهل عملية الاختراق.

٣- سرعة التعامل مع الهجمات المعلوماتية.

وقد تضـمت التوجيه الرئاسـي في عام ٢٠٠٣ ضـرورة توفير مضـلة الحماية المعلوماتية لشبكة الحاسوب في البنى التحتية الحرجة للولايات المتحدة الامريكية بوصفها الحلقة الأضعف في بنية الأمن القومي الأمريكي والأكثر عرضـة للهجمات المعلوماتية الشـرسـة من دول مختلفة ودوافع متنوعة[١].

وفي عام ٢٠٠٥ قامت الولايات المتحدة بمناورات عسكرية بأسم cyber storm، لأختبار قدرتها على مواجهة عمليات الاختراق التي تتعرض لها شـــبكاتها الدفاعية ، وفي عام ٢٠٠٦، أصبحت المعلوماتية تقترن بالفضاء بوصفها وسيلة مهمة لتدعيم القدرات العسكرية تجاه المخاطر التي تواجهها من الخارج[٢].

وفي سبيل الرد على البيئة التنافسية الدولية، انشأ البنتاغون وحدة خاصة بالقوة المعلوماتية القتالية وقيادة الأمن المعلوماتي، وكأن الهدف منها تنسـيق الجهود اللامركزية للأمن المعلوماتي، وعمل قيادة موحدة لجميع العمليات الدفاعية والهجومية، ففي اطار الجانب الدفاعي، تعد القيادة المعلوماتية هي المسؤولة عن الإجراءات الهادفة إلى الحماية والاستجابة للنشاط الخفي في سياق نظم المعلومات وشـبكات الانترنت للبنتاغون، كذلك تؤدي العمليات المعلوماتية إلى تعطيل ومنع وتدمير المعلومات ، فالهجوم المعلوماتي يهدف إلى تدمير البنية التحتية بصورة عامة سواء كانت عسكرية أم مدنية للطرف الخصم[٣].

و في عام ٢٠١٤، أكدت وزارة الدفاع الامريكية في تقريرها الاســـتراتيجي إنها تعمل على إعادة تنظيم مواردها لبناء قدراتها في مجال الأمن المعلوماتي، للوقوف بوجه التهديدات التي تؤثر

---

[١] د.سامر مؤيد عبداللطيف، مصدر سابق، ص٩٣.

[٢] مصـطفى يونس مؤيد يونس، اسـتراتيجية الولايات المتحدة الامريكية للامن السـيبراني، الموصـل، كلية العلوم السياسية، جامعة الموصل، ٢٠١٩، ص١٤٠.

[٣] مروة صـبحي، تسـليح تكنولوجي ، تنافس غير تقليدي في مجال التكلنولوجيا العسـكرية، مركز المسـتقبل، لـلابـحـاث والـدراســـات الـمســـتـقـبـلـيـة، مـتـاح عـلـى الـرابـط الالـكـتـرونـي http://rawabetcenter.com/archives/6591. تاريخ الزيارة ٢٠٢١/٨/٢٣.

على الأمن القومي ضـــمن مجالات ثلاث هي حماية الشـــبكات، وحماية الدفاع الوطني، والعمل على ايقاف وشل قدرة الخصم المعلوماتية[١].

أما خلال فترة الرئيس الامريكي الســـابق (دونالد ترامب)، فقد طرح اســـتراتيجية ســـميت بـــــ(الاســـتراتيجية القومية المعلوماتية) في عام ٢٠١٨، وقد عدت هذه الاســـتراتيجية الفضـــاء المعلوماتي أمر لازماً واساسياً، وبموجب هذهِ الاستراتيجية أصبح لدى الولايات المتحدة الامريكية القوة في الدفاع عن امنها المعلوماتي بشـكل خاص، وأمنها القومي بشـكل عام والتي ركزت على ما يأتي[٢]:

١- الدفاع عن الوطن من خلال حماية الشبكات والأنظمة البيانات.

٢- تعزيز الدفاع الأمريكي من خلال رعاية وتعزيز إقتصاد رقمي آمن.

٣- الحفاظ على السـلم والأمن الدوليين من خلال تعزيز قدرات الولايات المتحدة الامريكية بالتنسيق مع الحلفاء والشركاء لردع ومعاقبة الخصوم الذين يستخدمون الاسلحة المعلوماتية من أجل الاضرار بالأمن القومي الأمريكي.

٤- تعزيز قدرات الشركاء في مجال الأمن القومي المعلوماتي للحفاظ على النفوذ الامريكي ضد المنافسين الاقليمين والعالميين.

وتجدر الأشارة إلى أنه سبق وأن أعلن البنتاغون في عام ٢٠١٢ عن زيادة التمويل لتطوير قـدرات الأمن المعلومـاتي، جنبـاً إلى جنـب مع الطـائرات من دون طيـار (الـدرون)، فقد تم مضـاعفة تخصـيصـات ميزانية عام ٢٠١٢، لمواجهة المخاطر المعلوماتية، وتطوير اسـلحة هذهِ الحرب وأدواتها، وانتاج فايروسات تكون لها القدرة على تخريب شبكات الخصم، وتصنيع اسلحة هجومية فضلاً عن زيادة تمويل الابحاث المعلوماتية[٣].

---

[١] مصطفى يونس مؤيد يونس، مصدر سابق، ص١٤٣.

[٢] د.كرار عباس متعب، الحرب السيبرانية، دراسة في استراتيجية الهجمات السيبرنية بين الولايات المتحدة وايران، مجلة حمورابي للدراسات، ع (٤٠)، س (١٠) ، (٢٠٢١)، ص٢٠٦-٢٠٧.

[٣] مصطفى يونس مؤيد يونس، المصدر السابق، ص١٤٣.

وبدأت عام ٢٠١٢ ، اســـتراتيجية الرئيس الأمريكي (جو بايدن) في الفضـــاء المعلوماتي لمواجهة الهجمات المعلوماتية والتي ركزت على منع الانشـــطة المعلوماتية المعادية، وتحســـين الدفاعات المعلوماتية وردع العمليات المعلوماتية ومواجهتها، وفي ذات العام أكد جو بايدن على ضـــرورة أن تشـــن الولايات المتحدة هجمات معلوماتية على الخوادم المســـتخدمة في الهجمات المعلوماتية ضد الولايات المتحدة الامريكية[١].

ثانياً: روسيا الاتحادية

عملت روســـيا الاتحادية منذ عام ١٩٩٩، على تطوير اســـتراتيجيتها في مجال أمن المعلومات وأسـلحة البرمجيات، فأنصـرفت الجهود الحكومية إلى تأمين الفضـاء المعلوماتي، بعد أن تم عام ٢٠٠٢ انشاء إدارة تتولى مسؤولية أمن المعلومات يكون اتصالها بوكالة الأمن القومي الروســـي (FSB)، لتطوير نظم المعلومات وحماية البيانات، وقامت وزارة الدفاع بالتعاون مع بعض شـركات البرامجيات والأوسـاط والاكاديمية إلى أنشـاء عقيدة (الحرب المعلوماتية)، التي أنطوت على سـلسـلة من التدابير الهجومية والدفاعية لضـمان نجاحها وتحقيق أهدافها[٢]، وكذلك أنشأت روسيا الاتحادية وكالة أبحاث الانترنت، أو ما يعرف بجيش المتصيدين Troll Army في اطار إسـتراتيجيتها المعلوماتية، وهو جهاز تابع لوكالة الأمن الاتحادي الروسـي، وتتلخص مهام الجيش المعلوماتي الروسي بالأتي:

١- القيام بعمليات التجسس على الخصوم.

٢- تنفيذ الهجمات المعلوماتية التي تحدث الضـــرر بالبنى التحتية والمواقع المعلوماتية الحكومية في الدول الاجنبية المعادية.

٣- شـن حروب معلوماتية عن طريق القيام بعمليات اختراق الحسـابات والبريد الالكتروني للرد على المقالات، ونشر الشائعات وتزييف الحقائق وتوجيه الرأي العام ضد الخصوم[٣].

---

[١] كرار عباس متعب، مصدر سابق، ص٢٠٧-٢٠٨.

[٢] د.سامر مؤيد عبداللطيف، مصدر سابق، ص٩٥.

[3] Bodner, Matew, Russian Military Maerges Air force and space command, The Moscow Times online, August 2015, p.77.

وفي ذات السـياق حددت روسـيا أدوات الحرب المعلوماتية لها، وهي مكافحة التجسـس، وتوحيد الذكاء، وأضـعاف إتصـالات العدو، وتدمير قدرات حاسـوب الخصـم، وتنظر روسـيا لهذه الادوات على أنها سـلاحاً فعالاً وبآثار متنوعة وتكون آثار هذهِ الأسـلحة مشـابهة الأسـلحة الدمار الشـامل، وعلى الرغم من محاولة الولايات المتحدة الامريكية الابتعاد عن معاداة روسـيا في جانب الفضـاء المعلوماتي، إلا أن اسـتراتيجية روسـيا أصـبحت ذات آثار سـلبية تجاه الولايات المتحدة الامريكية(١).

وقد ساهمت روسيا الاتحادية في اطار تدعيم الأمن الدولي، بعد أن شعرت بخطورة تطور المعلومات والاتصـــالات، فقد بادرت الى تقديم اقتراحاً للجمعية العامة للأمم المتحدة، طالبت فيه بضـرورة وضـع مسـودة قرار يتعلق بأمن المعلومات تحت مسـمى" التطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي "، وقد وافقت الجمعية العامة على هذا الاقتراح بالاجماع(٢).

وفي عام ٢٠١٤، أعلنت وزارة الدفاع الروسية بأنها تخطط لأنشاء لنظام معلوماتي شـامل ينتهي به العمل عام ٢٠١٧، تكون وظيفته حماية البنية الاساسية للقوات المسلحة من الهجمات المعلوماتية، فضـلاً عن التدريب على استخدام الحواسيب الآلية لدعم الأمن المعلوماتي الروسي، إذ أن روســـيا تمتلك عناصـــر بشـــرية مؤهلة لتنفيذ هجمات معلوماتية، ولديها اعداد كثيرة من القراصنة المتطوعين، الذين يتم تأهيلهم للمساعدة في حمايته المنشآت العسكرية(٣).

ثالثاً: الصين

أصـدر المكتب الصـيني لمعلومات شـبكة الانترنت لأول مرة الاسـتراتيجية الوطنية لأمن الفضـــاء المعلوماتي، وقد بينت الصـــين على ضـــوء اســـتراتيجتها موقفها تجاه تنمية الفضـــاء

---

(1) Cvonish, paul, one cyber war far, Achatham House Report, The Royal institute of inter national Affairs London, 2011, p.18.

(2) General Assembly, Developments in the field of in formation and Telecommunication in the context of inter national security, UN document A/RES/53/70, 4 January 1999.

(٣) د.ايهاب خليفة، الحرب السيبرانية، مراجعة العقيدة العسكرية استعداد للمعركة القادمة، مجلة السياسية الدولية، م (٥٣)، ع (٢١١) ، القاهرة ، مصر ، ٢٠١٨، ص٢٠.

المعلوماتي وأمنه، وقد اشـــارت الاســـتراتيجية أنه في ظل التطور التقني المعلوماتي، فأن الأمن المعلوماتي يواجه مخاطر مســـتمرة، وإن التدخل في الشـــؤون الداخلية للدول الأخرى من خلال شـبكة الانترنت، والتجسـس المعلوماتي، وغيرها من الاسـاليب المعلوماتية من شـأنها الاضـرار بالأمن القومي والاقتصادي للدول، وسلامة معلومات مستخدمي شبكة الانترنت[١].

وضـمن سـياق الاعداد الاسـتراتيجي لمنظومة الحرب المعلوماتية الصـينية حضـي التدريب على تنفيذ الهجمات المعلوماتية المسـتقبلية باهمية بالغة لدى الجيش الصـيني بأسـتخدام مراكز التدريب المخصـصـــة للحرب المعلوماتية التابعة للجيش، وأكاديمية القيادة للاتصـــالات، وجامعة لهندسـة المعلومات، وغيرها من المؤسـسـات الاخرى، وقد اعتمدت اسـتراتيجية الحرب المعلوماتية الصـينية ما يسـمى "بشـكبة الحرب المعلوماتية المتكاملة"، وتسـعى هذه الاسـتراتيجية إلى تطوير البنية الشـاملة للشـبكة المعلوماتية القادرة على التنسـيق بين العمليات العسـكرية في البر والبحر والجو، عبر الســيطرة على الطيف الكهرومغناطيســي، كما تتميز بقدرتها العالية على التوظيف الشامل لقدرات الحرب التقليدية والمعلوماتية[٢].

و في عام ٢٠١٤، أنشـــأت مجموعة قيادة الأمن المعلوماتي (GILG) برئاســـة الرئيس الصـــيني (شـــي جين بينغ)، وقد ســـاعدت هذه المجموعة على وضـــع إســـتراتيجيات لمواجهة التهديدات المعلوماتية، وفي عام ٢٠١٦، اقرت الهيئة العليا في الصـــين مشـــروع" قانون الأمن المعلوماتي الصـــيني"، الذي قدمته قيادة الأمن المعلوماتي، ودخل حيز التنفيذ عام ٢٠١٧، إذ يعكس هذا القانون جهود الصـــين الواســـعة في تنظيم انشـــطة الفضـــاء المعلوماتي، ومكافحة التهديدات المعلوماتية، وركز هذا القانون على توحيد المعلومات وتأمينها، واتخاذ تدابير تقنية لحماية الشبكات ومنع تسرب البيانات وسرقتها، والابلاغ عن حوادث الأمن المعلوماتي، وفي عام

---

[١] نعمان عبدالباري، أثر التكنولوجيا في حروب القرن الواحد والعشـــرون، ط١، دار الافتاء للطباعة والتوزيع، القاهرة، ٢٠١٥، ص٦٩.

[٢] د.سامر مؤيد عبداللطيف، مصدر سابق، ص٧٣.

٢٠١٨، اصبحت شركات الاتصالات تحتاج موافقات مسبقة قبل تقديم خدمات الشبكة الافتراضية الخاصة[١].

أما في مجال التعاون الدولي فقد وقعت الصـــين في عام ٢٠١١، مع مجموعة من الدول كروسيا وطاجيكستان واوزباكستان على مشروع مدونة السلوك لضمان امن المعلومات الدولي في الدورة (٦٦) للجمعية العامة للأمم المتحدة والتي حثت عليها مبادئ الأمم المتحدة التوجيهية لإطار نشاط الانترنت[٢].

أما في عام ٢٠١٥ أبرمت الصـين اتفاقية مع روسـيا الاتحادية تضـمنت أتفاقاً في اطار حماية أمن الشبكات ويقصد بعدم تنفيذ هجمات معلوماتية وتقدم الدعم المتبادل لكلا الدولتين[٣].

وفي عام ٢٠١٧ أتفقت الصين مع استراليا على انشاء آلية موحدة لمناقشة قضايا الأمن المعلوماتي والجرائم المعلوماتية من أجل منع الحوادث المعلوماتية، وقد ابرمت اتفاقية امن الانترنت في مدينة سدني الاسترالية ووفقاً لهذه الاتفاقية يتعهد كلا الطرفين بعدم الانخراط أو دعم سـرقة حقوق الملكية الفكرية، واتفقتا على متابعة تقرير فريق خبراء الأمن المعلوماتي التابع للأمم المتحدة بما في ذلك الأمتثال لمدونة السلوك الوطنية المسؤولة في الفضاء المعلوماتي[٤].

وبتحليل ما تقدم نسـتطيع القول، أن جميع اسـتراتيجيات الدول الوقائية التي اعدتها الدول لمنع أو الحد من الهجمات المعلوماتية، غير المشـــروعة دولياً، هي مجرد محاولات ومبادرات لمواجهة خطر تلك الهجمات المتنامي والذي أصـبح عابراً للحدود الجغرافية بسـبب الخصـائص الفريدة التي يتصـف بها الفضـاء المعلوماتي، فضـلاً عن الصـعوبة والتعقيد في ضـل ازدياد عدد المهاجمين من دول وفواعل اخرى من غير الدول كالافراد والشـــركات، كذلك تنوع الأســـلحة المعلوماتية التي يتم بها مهاجمة الدول، وبالتالي تبرز اهمية ابرام معاهدة دولية جماعية لمنع

---

[١] أحمد يوسف كيطان، استراتيجية الأمن الوطني السيبراني للصين، قراءة في قانون الأمن السيبراني الصيني، متاح على الرابط الالكتروني تاريخ الزيارة ٢٠٢٢/٤/٢٩، https://www.politicsdz.com

[٢] فريدة طاجين، تأثير القوة السـيبرانية على اسـتراتيجيات الأمنية للدول الكبرى، دراسـة حالة الصـين، رسـالة ماجستير مقدمة إلى كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، الجزائر، ٢٠١٨، ص٧٤.

[3] See: Nikola pijovic, the cyber space Great Game. The Five Eyes, The sino-Russian Bloc and the Growing compectition to shape Global cyber space Norms. 13 th international conferece on cyber conflict Going NATO CCDCOE publications, Tallinn, 2012, p.225.

[٤] فريدة طاجين، مصدر سابق، ص٧٦.

الانشطة المعلوماتية أو الحد منها على أقل تقدير، فضلاً عن الزام الدول بتبني تشريعات وطنية تجرم هذه الهجمات المعلوماتية.

الفصل الثالث

ماهية عدم امتثال الدول لواجب العناية اللازمة

تطرقنا في الفصـــل الثاني من هذه الدراســـة الى مفهوم واجب العناية اللازمة التي يتوجب على الدول الالتزام به، خصوصاً في سياق استخدام الهجمات المعلوماتية، فإذا كانت الدول وفقاً لذلك تمتلك حرية التصرف بموجب سيادتها الإقليمية والقضائية، ولها أن تمارس كافة التصرفات والأنشـــطة المعلوماتية في مجالها المعلوماتي، إلا إن حرية التصـــرف هذهِ مقيدة بواجب العناية واحترام حقوق الدول الأخرى بعدم الاضرار بها.

والدول اليوم باتت ملزمة بالامتثال لواجب العناية الذي يمثل التزام بمنع الضـــرر الناشـــيء عن الأنشـــطة المعلوماتية، فإذا ما اصـــرت الدول أو تمادت بعدم الامتثال لواجب العناية، فأنها تكون عرضـــة لتحمل المسؤولية الدولية، فضـــلاً عن المسؤولية الجنائية الفردية عن الأفعال غير المشـــروعة التي يرتكبها الافراد والكيانات الخاضـــعين لسيطرتها واشـــرافها، بالإضـــافة إلى التزامها بواجب الحياد في الفضاء المعلوماتي.

وفي ســـبيل ذلك فأن للدولة المعتدى عليها حق اللجوء إلى اتخاذ تدابير العناية اللازمة لوقف الانشـــطة المعلوماتية الضـــارة، فلها أن تلجأ لاتخاذ التدابير المضـــادة للرد على الهجمات الصـــادرة من الدولة المعتدية وحملها على الكف والتوقف عن الفعل غير المشـــروع دولياً والامتثال لقواعد القانون الدولي.

وللإحاطة بموضـــوع عدم امتثال الدول لواجب العناية سنناقش ذلك في مبحثين، نتناول في المبحث الأول: التعريف بعدم امتثال الدول لواجب العناية، ونفرد الثاني للمسؤولية الدولية المترتبة على عدم امتثال الدول لواجب العناية وعلى النحو الآتي:

المبحث الأول

التعريف بعدم امتثال الدول لواجب العناية اللازمة

إن امتثال الدول لمبادئ وقواعد القانون الدولي، سواء كان هذا الالتزام ناشيء عن اتفاقات دولية، أو كان مصـــدره العرف الدولي، فهي بالتالي تكون ملزمة بالوفاء بالتزاماتها تجاه الاطراف المتعاقدة، إلا إن هذا الالتزام قد يتعرض في حالات معينة للأنتهاك، من قبل دولة معينة وبالتالي قد يفضي إلى حالة عدم امتثال الدول للوفاء بالتزاماتها تجاه الدول الأخرى، وغالباً ما تتردد الدول عن خرق أي التزام قانوني لما له من أثار قانونية، كالجزاء والتعويض عن الفعل غير المشـروع، إلا أن الامر يبدو مختلفاً في حالة عدم وجود اتفاقات أو صـكوك دولية تنظم حالات عدم امتثال الدول، فعلى سبيل المثال يثير موضوع الحياد المعلوماتي مشكلات قانونية عديدة تواجهها الدول عند امتثالها لواجب الحياد، لا ســـيما في اطار الهجمات المعلوماتية العابرة للحدود، كذلك يحتم واجب العناية على الدول أن تمتثل بعدم قيامها بشـــن هجمات معلوماتية تنطلق من أراضـــيها وتشـــكل اعتداءاً على دولة أخرى. وقد تلجأ الدول لاتخاذ تدابير معينة للرد على الهجمات المعلوماتية غير المشروعة دولياً وهي ما تسمى بالتدابير المضادة.

ولما تقدم ارتأينا تقسيم هذا المبحث على مطلبين:

المطلب الأول: مفهوم عدم الامتثال لواجب العناية اللازمة.

المطلب الثاني: التدابير المضـــادة التي تتخذها الدولة للرد على عدم امتثال الدول المعتدية منع الهجمات المعلوماتية.

المطلب الاول

مفهوم عدم الامتثال لواجب العناية اللازمة

ينصرف مفهوم الامتثال في القانون الدولي الى كيفية امتثال الدول للوفاء بالتزاماتها الدولية تجاه الاطراف الاخرى المتعاقدة سـواء كان هذا الالتزام مصـدره المعاهدات أو الاتفاقيات الدولية أو غيرها من الصـــكوك الدولية الاخرى، وإذا ما نظرنا إليه من مفهوم المخالفة نجد أن المفهوم

المعاكس للإمتثال هو عدم الامتثال الذي تقرره الدول للتحلل من التزاماتها تجاه الاطراف الاخرى، الذي ربما يكون لفترة مؤقتة، وغالباً ما يكون ناشئ عن اسباب عديدة منها عجز الدول عن تحمل تكاليف ما التزمت به، أو أن الدولة كان التزامها بناء على ضغوط تعرضت لها، أو راجع لعدم قدرة مؤسسات الدولة على الامتثال.

ومن الجدير بالذكر أن الامتثال في القانون الدولي مقرر على وفق قواعد دولية آمرة، وهي ذات القواعد المقررة في القانون الدولي الانساني ومنها القواعد العرفية ذات الصلة بنظام الامتثال، علاوة على أن هناك واجب يقع على الدول يلزمها بالامتثال للحياد المعلوماتي عند تنفيذ انشطة معلوماتية، عبر الفضاء المعلوماتي، ويتوجب عليها عدم استخدام أراضي دولة الحياد وهذا الالتزام نابع من سيادتها على اقليمها، سواء كان البري أو البحري أو الجوي.

ومن خلال ما تقدم سنتناول هذا المطلب في فرعين، نخصص الاول لتعريف عدم الامتثال لواجب العناية اللازمة واسبابه ونفرد الثاني لحالات عدم امتثال الدول في الفضاء المعلوماتي وعلى الشكل الاتي:

الفرع الاول

تعريف عدم الامتثال لواجب العناية وأسبابه

سنتناول في هذا الفرع تعريف عدم الامتثال لواجب العناية فضلاً عن الاسباب التي تؤدي الى عدم امتثال الدول لواجب العناية وعلى وفق الاتي:

اولا: تعريف عدم الامتثال لواجب العناية: لا يوجد تعريف محدد لعدم امتثال الدول لواجب العناية اللازمة، سواء كان ذلك على المستوى الفقهي، أم الاتفاقي، أم القضائي، لكن هناك اشارات بصورة غير صريحة لمعنى عدم الامتثال عندما يكون في سياق عدم القيام بعمل معين، كالامتناع عن الانشطة العسكرية وشبه العسكرية، التي تنفذها دولة ضد إقليم دولة اخرى، أو استقلالها السياسي، وعدم التدخل في شؤونها الداخلية، والامتناع عن حصارها البحري، أو تعريض سيادتها الوطنية للانتهاك كما حدث في قضية نيكاراغوا ضد الولايات المتحدة الامريكية،

حيث بينت محكمة العدل الدولية في أمرها الصـــادر ١ ايار/ مايو ١٩٨٤ بالقول: (ان تكف الولايـات المتحـدة الامريكيـة، وتمتنع عن القيـام بـاي عمـل الغرض منـه الوصـــول الى موانئ نيكاراغوا، ومنها على وجه الخصـوص زرع الالغام، وان تحترم حق السيادة والاستقلال السياسـي لجمهورية نيكاراغوا)[١]، وقد جاء هذا الحكم في ســـياق اتخاذ تدابير مؤقتة لحمل الدولة المعتدية على الكف عن الاعمال غير المشـــروعة التي تقوم بها ضـــد دولة اخرى، إذ أن عدم الامتثال بصـورة عامة هو يمثل الخروج على مبدأ المشـروعية الدولية، التي تلتزم الدول بها، ومن الامثلة التطبيقية لحالات عدم الامتثال المتعلقة ببروتوكول مونتريال لعام ١٩٨٧، قدمت روسيا الاتحادية بياناً الى لجنة التنفيذ عام ١٩٩٥ أشـــارت فيه الى عدم قدرتها على الوفاء بالتزاماتها المقررة بموجب البروتوكول اعتبـارا من عـام ١٩٩٦، واســـتنـدت في ذلـك الى نص الفقرة الرابعـة من تعديلات كوبنهاكن ١٩٩٢، وبناء على ذلك قدمت لجنة التنفيذ بالمشـاورات اللازمة تقريرها الذي يقضـــي بان روســـيا كانت في حالة امتثال لالتزاماتها الا انها من المحتمل ان لا تســـتطيع من الامتثال في عام ١٩٩٦ لالتزاماتها المقررة لهذا البروتوكول[٢].

والحالـة الاخرى على عدم الامتثال هي عدم امتثال جمهوريـة اذربيجان لمـا ورد في بروتوكول مونتريال لعام ١٩٨٧ المتعلق بالمواد المســـتنفذة لطبقة الاوزون في اتفاقية فينا لعام ١٩٨٥ لحماية طبقة الاوزون، اذ تم تصـــنيفها على انها دولة غير عاملة بالمادة الخامســـة من البروتوكول التي اصـبحت عضـوا فيه، حيث تعهدت بموجبه بانشـاء نظام التراخيص للصـادرات والواردات، وفرض الضـــرائب على واردات المواد المســـتنفذة للاوزون، إلا أنها لم تلتزم بالوفاء بالتعهد الذي وافقت عليه، واعلنت انها في حالة عدم امتثال تســـتمر حتى عام ٢٠٠٠، اي لمدة اربع ســـنوات، وقد قدمت اطرافا بالاتفاقية عدة مذكرات الى امانة البروتوكول بشـــأن عدم امتثال اذربيجان لمواد البروتوكول وتعديلاته[٣].

---

[١] . موجز الاحكام والفتاوي والاوامر الصادرة عن محكمة العدل الدولية، ١٩٤٨-١٩٩١.

[٢] بشـــير جمعة عبد الجبار، الحماية الدولية للغلاف الجوي، اطروحة دكتوراه، كلية القانون، جامعة بغداد، ٢٠٠٦، ص١٧٠.

[٣] بشير جمعة الكبيسي، المصدر نفسه، ص١٧٢.

ومن الجدير بالذكر ان المادة (٨) من بروتوكول مونتريال الزمت الدول الاطراف بوضع واعتماد اجراءات وآليات مؤسسية لتحديد حالات عدم الامتثال لاحكام البروتوكول، ولمعالجة حالات الاطراف التي يثبت عدم امتثالها، اذ ان اجراء عدم الامتثال يشتمل على نظام للحصول على التقارير المتعلقة بعدم الامتثال والنظر فيها، ووفقا لذلك يحق للاطراف في البروتوكول من اتخاذ تدابير لمساعدة الاطراف على الامتثال لاحكام البروتوكول[١].

كذلك أعلنت دولة بلغاريا عن عدم الامتثال للوفاء بالتزاماتهما الواردة بالاتفاقية، فقد قدمت دولة بلغاريا عام ١٩٩٥ بيانا اشارت فيه الى انها لن تستطيع الامتثال لالتزاماتها المقررة بموجب بروتوكول مونتريال سالف الذكر، وعلى الرغم من اتخاذ بلغاريا الخطوات اللازمة للامتثال والتخلص من المواد المستنفدة لطبقة الاوزون، الا انها اثارت الانتباه الى جملة من القضايا ذات الصلة بامتثال دولتها مثل، تبديل واعادة النظر في المشاريع التي يدعمها برنامج تسهيل البيئة العالمية (GEF)، وبالتالي قررت لجنة الامتثال المختصة تصنيف بلغاريا من الدول غير العاملة وفقاً للمادة الخامسة من البروتوكول، ونتيجة لذلك فقد أصبحت في حالة عدم امتثال لالتزامات الرقابة المنصوص عليها في البروتوكول[٢].

ثانيا: اسباب عدم امتثال الدول لواجب العناية:

١- في الاتفاقيات الدولية: أن الامتثال يعتمد بصورة اساسية على رغبة الدول وقدرتها على الوفاء بالتزاماتها، لذا فأن أي، نظام للامتثال يجب أن يأخذ بنظر الاعتبار إحتمالية عدم استطاعة الدول على الامتثال، واسباب عدم الامتثال كثيرة ومتنوعة نورد منها على سبيل المثال لا الحصر ما يأتي [٣]:

---

[١] اجراء عدم الامتثال لعام١٩٩٨، الفقرة ٩ من المرفق الثاني عن تقرير الاجتماع العاشر للاطراف في بروتوكول مونتريال ذات الصلة بالمواد المستنفدة لطبقة الاوزون، ٣ ديسمبر/ ك ١ ١٩٩٨.

[٢] د. بشير جمعة الكبيسي، مصدر سابق، ص١٧١.

[٣] د. بشير جمعة الكبيسي، المصدر نفسه، ص١٣٦.

أ- هناك بعض الدول قد تختار الامتثال نتيجة عدم وجود تكافئ بين ما تحصل عليه من فائدة الامتثال وبين ما تتحمله من تكاليف الامتثال، اي تكون الفوائد اقل من التكاليف التي تتحملها.

ب- قد تضطر الدول للامتثال والتوقيع على الاتفاقية، بسبب ما تتعرض له من ضغط داخلي أو خارجي.

ج- ان اغلب حالات عدم الامتثال في القانون الدولي سببها عدم استطاعة او امكانية مؤسسات الدولة على الامتثال، اكثر ما يوصف بانه سوء نية من تلك الدولة.

د- ان حالات عدم الامتثال تكون خارج ارادة الدولة على الرغم من بذلها الجهود المطلوبة.

هـ- من الممكن ان تمتثل الدول لبعض نصوص الاتفاقية وقد تفشل في الامتثال لنصوص اخرى منها. واذا كانت الدول لها اسباب متنوعة ومتعددة في عدم امتثالها لالتزاماتها الدولية التي وافقت عليها فما هي آليات عدم الامتثال؟

باستطاعة الدول ان تنظر في ادراج احكام بشأن عدم الامتثال في اتفاق بيئي متعدد الاطراف، على سبيل المثال لغرض مساعدة الاطراف التي تواجه صعوبات إمتثال معينة، ومعالجة حالات عدم الامتثال الفردية، آخذتاً بنظر الاعتبار أهمية كون احكام الامتثال وآلياته تتلائم مع الالتزامات المحددة التي يفرضها الاتفاق، وعليه بالإمكان الاعتماد على بعض الاليات ووضعها بنظر الاعتبار منها: [١].

أ- يمكن أن تنظر الاطراف في انشاء هيئة، مثل لجنة الامتثال، لمعالجة قضايا الامتثال، كما يمكن أن يكون أعضاء هذه الهيئة ممثلين لأطراف او خبراء معينين من اطراف.

ب- يحق للأطراف المتعاقدة ان تستخدم اليات عدم الامتثال كوسيلة لتحديد حالات عدم الامتثال الممكنة في مرحلة مبكرة ومعرفة اسباب عدم الامتثال، وقيامها باستجابات مناسبة تشمل، حسب الاقتضاء، التصدي لحالة عدم الامتثال او تصحيحها دون تأخير، وبالامكان

---

[١] . الامم المتحدة، برنامج الامم المتحدة للبيئة، مبادئ توجيهية بشأن الامتثال للاتفاقات البيئية متعددة الاطراف وانفاذها، متاح على الموقع الالكتروني: https://wedocs.unep.org. تاريخ الزيارة ٢٠٢٢/٩/٨.

تعديل هذه الاستجابات لتغطية احتياجات حالات عدم الامتثال، وقد تشمل كلا من التدابير التيسيرية والتدابير الاشد حسب الحاجة وبما يتماشى مع القانون الدولي.

ج- يمكن لآليات عدم الامتثال ان تكون غير تخاصـــمية وتشـــمل ضـــمانات اجرائية للمشتركين بها، فضلا عن ذلك يمكن لآليات عدم الامتثال ان تفرز تطبيق احكام الاتفاق وتودي الى منع وقوع النزاعات.

د- يمكن لأي طرف في الإتفاق أن يتخذ القرار النهائي بشـــأن عدم الامتثال عن طريق مؤتمر الدول الاطراف في الاتفاق بتعدد الاطراف، أو عن طريق أي هيئة اخرى في اطار ذلك الاتفاق.

لذا فأن غالبية الدول في الاتفاقيات البيئية وخاصـــة المتعلقة بالغلاف الجوي، بادرت الى إتخاذ عدة آليات يمكن من خلالها تشـجيع الدول على المشـاركة في الاتفاقية أو الانضـمام لها لاحقا ومنها[١]:

- الاخذ بالمنهج التدريجي للالتزامات.
- الاخذ بمبدأ تنوع المسؤوليات.
- منح الاطراف فرصة للإنسحاب من الاتفاقية.
- منح الاطراف الفرصة لإعادة النظر بالاتفاقية.

٢- أما في مشروع اتفاقية حظر الهجمات المعلوماتية التي ترغب بعض الدول في ابرامها، تطرح طبيعة هجمات الفضـاء المعلوماتي بعض الصـعوبات والمشـكلات القانونية المتمثلة بمدى إمكانية تطبيق قواعد القانون الدولي التي تنبثق من ميثاق الامم المتحدة والتي تضـع المعالجة القانونية، بالإضـافة الى أن الاطر القانونية غير كافية للتوصـل الى حلول تعالج معضـلة الامن المعلوماتي التي تفرضـها الهجمات المعلوماتية، والسـبب في ذلك يعود الى اختلاف وجهات النظر حيال الموضـــوع، فهناك وجهتان مختلفتان: الاولى ترى وجود

---

[١] .د. بشير جمعة عبدالجبار الكبيسي، مصدر سابق، ص١٥.

ضـــرورة ملحة لوجود إطار قانوني جديد، اما الثانية فترى الإقتصـــار على تبني النظم القانونية المعمول بها فقط[١].

ومن نافلة القول: أن الرغبة الثنائية في مســـالة تنظيم اللجان المعلوماتية على هيئة اتفاقية دولية، قد تم تحديدها بالفعل عام ٢٠١٠، من خلال محاورات جمعت بين الجانبين الامريكي والروسي ولغرض طرح مناقشة تنظيم إستخدام الهجمات المعلوماتية[٢].

بيد أن هناك اســـباب حقيقية كانت عقبة امام ابرام اتفاقية تتضـــمن تنظيم الهجمات في الفضاء المعلوماتي والحد من الاسلحة المعلوماتية ومنها[٣]:

أ- صـــعوبة انفاذ الاتفاقية: وهي اولى العقبات التي تقف امام امكانية ابرام اتفاقية دولية ملزمة في مجال الدفاع المعلوماتي الذي يســتلزم بالضــرورة وجود اجراءات عقابية ضــد المهاجم تتماثل مع القوانين الخاصـــة بالجرائم التقليدية، اذ ان الدفاع المعلوماتي واجراءات حماية الشبكات المعلوماتية، تتعارض في كثير من الاحيان مع خصوصية الافراد وحقوق الانســـان، ويعد ذلك اهم الاســـباب التي تقف خلف رفض العديد من الدول وعلى رأســـها الولايات المتحدة الامريكية للمقترحات الروسية بخصوص ابرام اتفاقية دولية تتعلق بالدفاع المعلوماتي.

ب- تعارض المصالح: أن احد شروط الاتفاقيات الدولية هو وجود مصالح مشتركة بين اطرافها ما بين اعضائها، بخلافه يغيب الدافع للالتزام بالاتفاقية، وتطبيق شروطها.

ج- خصوصية الأسلحة المعلوماتية: أن الخصوصية التي تتميز بها الاسلحة المعلوماتية واختلاف خصائصها واستخدامها عن تلك الخاصة بالأسلحة التقليدية، من أهم التحديات التي تقف عائقاً أمام إبرام اتفاقية تحظر بموجبها الهجمات المعلوماتية.

---

[١] . د. عادل عبد الصادق، اسس الفضاء الالكتروني في ضوء القانون الدولي الانساني، مصدر سابق، ص١٥٠.

[٢] . د. عدنان النقيب، الحرب الالكترونية في ضوء بروتوكولي سبع وسبعين الملحقين باتفاقات جنيف الاربع سنة تسع واربعين، ط١، المركز العربي للنشر والتوزيع،الهجمات السيبرانية، القاهرة، مصر، ٢٠٢٢، ص٣٧٥.

[٣] . د. نوران شفيق، مصدر سابق، ص١٢٧-١٢٩.

ومن الجدير بالذكر هناك اسباب اخرى ذات صلة بمواقف الدول تقف عائقا امام إبرام اتفاقية دولية تعنى بحظر أو تقييد اســـتخدام الوســـائل المعلوماتية التي تتعلق بتنفيذ الهجمات معلوماتية وتتجسد بالاتي[١]:-

-بناء الثقة بين الدول (الشـــفافية): ان تدابير بناء الثقة بين الدول تمثل نقطة ارتكاز لاي إتفاقية تعنى بحظر أو تقييد إستخدام ايّ سلاح.

-آليات التحقق من وقوع انشـطة محضـورة في الاتفاقية: ان آلية امتثال الدول لاي اتفاقية دولية يكون من خلال التحقق من وقوع شـــكوك بانتهاك احكامها، وهي اجراءات تتضـــمنها الاتفاقات الدولية وبالذات في حقل نزع الاسلحة او الحد منها.

وتأسـيسـاً على ما تقدم، نعتقد انه في ظل عدم وجود صـك دولي ملزم لمواجهة الهجمات المعلوماتية ســـواء بتقييدها أو حظرها نهائياً، فان ذلك ســـيجعل خطر تهديدها قائما وخاصـــة الهجمات المعلوماتية التي ينفذها فواعل من غير الدول كالأفراد والشـــركات، كما هو الحال في الهجمات المعلوماتية التي يشـــنها الارهابيين باســـتخدامهم الفضـــاء المعلوماتي لمهاجمة اهداف حيوية لدول معينة، سـواء كانت عسـكرية أم مدنية وهذا يحتم على الدول تكثيف امتثالها لاحكام وقواعد القانون الدولي، لاسـيما القانون الدولي العرفي مع امكانية إنشـاء أجهزة متخصـصـة على مسـتوى الدول تتولى الرقابة الشـاملة على الهجمات المعلوماتية وبذل الجهود الدولية في الكشـف عن الفاعلين وتحديد هويتهم، غير أن ذلك لا يخلو من الصـــعوبة والتعقيد بالنظر للخصـــائص الفريدة التي تتصف بها تلك الهجمات.

الفرع الثاني

حالات عدم امتثال الدول في الفضاء المعلوماتي

يشـــير الامتثال الى قدرة الدولة على الوفاء بالتزاماتها تجاه الاطراف المتعاقدة على وفق الحقوق والالتزامات الواردة في الاتفاقية التي قبلتها ووقعت عليها، والدول باتت اليوم ملزمة

---

[١] . د. احمد عبيس نعمة الفتلاوي، الهجمات السيبرانية، دراسة قانونية تحليلية بشأن تحديات تنظيمها، مصدر سابق، ص١٠٠-١٠٢.

بالامتثال وكفالة احترام القانون الدولي الانســـاني وهذا الالتزام يكون في حالات معينة إمتثالاً لقواعد عرفية في حال عدم النص عليها صـراحة أو قصـور تلك النصـوص عن تغطيتها، كذلك الدول عليها التزام قانوني يوجب إحترام حياد الدول الاخرى لاسيما الحياد المعلوماتي، لذا سنتناول في هذا الفرع بعض الحالات التي يستدل من خلالها على عدم امتثال الأسلحة المعلوماتية لقواعد القانون الدولي الإنساني، وحياد الدول المعلوماتي وعلى الشكل الاتي:

أولاً: عدم امتثال الاسـلحة المعلوماتية لقواعد القانون الدولي الانسـاني: يشـتمل القانون الدولي الانساني على العديد من المبادئ التي تقوم على حظر استخدام بعض انواع من الاسلحة التي تحدث آثار غير مشـروعة قياسـا الى تحقيق الغرض من الحرب[١]، ومن هذه الاسـلحة هي الاسـلحة المسـتحدثة ذات الخصـائص التدميرية الهائلة وغالبا ما يصـطلح على تسـميتها اسـلحة الدمار الشامل[٢].

وكان للقضـاء الدولي دوراً بارزاً في تحديد مدى مشـروعية اسـتخدام الأسـلحة النووية من عدمها، إذ أكدت محكمة العدل الدولية من خلال فتواها الصـادرة عام ١٩٩٦، حول مشـروعية اسـتخدام الاسـلحة النووية او التهديد بها أن القانون الدولي الإنسـاني يتضـمن القواعد المتعلقة بتسـيير الأعمال القتالية، وكذلك القواعد التي تحمي الأشـخاص الخاضـعين لسـلطة الطرف الخصم، حيث تعد الاسلحة النووية أخطر انواع اسلحة الدمار الشامل على الانسان والبيئة، نظراً لقدرتها التدميرية الواسـعة التي تتسـم بها وتمتد لأمد طويل جداً ومسـاحات واسـعة، وتتأثر بها الكائنات الحية والبيئة الطبيعية[٣]، لذلك يقع على الدول التزام قانوني وفقاً لقواعد القانون الدولي

---

[١] . ابو الخير احمد عطية، حماية السكان المدنيين والاعيان المدنية أبان النزاعات المسلحة، دراسة مقارنة، دار النهضة العربية، القاهرة، ١٩٩٨، ص٣٨.

[٢] . نعمان عطا الله الهيتي، الاسـلحة المحرمة دوليا، القواعد والاليات، دار رسـلان للطباعة والنشـر والتوزيع، دمشق، سوريا، ٢٠٠٧، ص٧.

[٣] . فتوى محكمة العدل الدولية بشـان مشـروعية اسـتخدام الاسـلحة النووية او التهديد بها، ملحق لمذكرة الامين العام للامم المتحدة لنزع السـلاح، مقدم الى الدورة الحادية والخمسين للجمعية العامة بتاريخ ١٩٩٦/١٠/١٥، رقم الوثيقة(A/51 / 2018)، ص٢٣.

الانسـاني كما هو الحال في القانون الدولي[١]، والسـؤال الذي يثار بهذا الصـدد هل تعد القواعد الامرة والالتزامات المطلقة كأساس لامتثال الاسلحة المعلوماتية لقواعد القانون الدولي الانساني؟

في البدء لا بد من الاشارة إلى قواعد القانون الدولي الانساني هي من القواعد الامرة إسوة بقواعد القانون الدولي العام، وهي تلك القواعد التي لا يجوز الاخلال بها ولا يمكن تغييرها الا بقاعدة لاحقة من قواعد القانون الدولي لها نفس الصـــفة، تلك التي تحرم القوة أو التهديد بها، وتحرم العدوان والمساواة بين الدول، وكذلك المبادئ المتعلقة بحقوق الانسان كتحريم ابادة الجنس البشري، والتفرقة العنصرية، والقرصنة، وكل ما يتعلق بالشخصية الانسانية، فلا يجوز الاتفاق بين دولتين على ان تقدم احداهما للاخرى عدد من مواطنيها لاجراء تجارب بيولوجية او طبية عليهم[٢]، لذلك نســـتطيع القول ان قواعد القانون الدولي الانســـاني قواعد آمرة ملزمة لجميع الاشخاص الدولية، وهذه النتيجة يمكن الوصول اليها من خلال فهم الطبيعة الآمرة للنظام العام، فقواعد القانون الانساني قد تبدو في بادئ الامر قواعد غير ملزمة ولها صفة اخلاقية، الا ان هذه النظرة يخالفها ما ورد بالمادة الاولى من اتفاقيات جنيف لعام ١٩٤٩، فضـــلا عن المادة الاولى من البروتوكول الاضـافي الاول لعام ١٩٧٧، إذ تنص كل منها على التزام الأطراف بأن تفرض هذا الاحترام لنصوص المعاهدات[٣]، إذ أن اساس التزام الدول في الامتثال لأحكام القانون الدولي الانساني يكمن في المادة المشتركة الاولى، حيث وبينت دراسة قامت بها اللجنة الدولية للصليب الاحمر بشـأن القانون الدولي الانسـاني العرفي على أن هناك واجب يقع على الدول يتمثل بعدم تشجيعها لانتهاك القانون الدولي الانساني من قبل اطراف النزاع، وتوجب عليها أن تلتزم في الحد من انتهاكات القانون الدولي الانساني[٤].

---

[١] . د. صـلاح الدين عامر، مقدمة لدراسـة القانون الدولي العام، ط٢، دار النهضـة العربية، القاهرة، ٢٠٠٧، ص١٠٥.

[٢] . محمد نعيم علوة، موسوعة القانون الدولي العام، المبادئ، (المبادئ والمصادر)، ج(١)، ط١، منشورات زين الحقوقية، بيروت، ٢٠١٢، ص٢٢٣.

[٣] د.مصطفى أحمد فؤاد، القانون الدولي الإنساني، دار المطبوعات، مصر ، ٢٠١٩، ص٨٢.

[٤] جون- ماري هنكرتس، ولويزدوزال- بك القانون الدولي الإنســـاني العرفي، م (١)، القواعد اللجنة الدولية للصليب الأحمر، القاعدة (١٤٤)، القاهرة، ٢٠٠٧، ص٤٤٥.

فأشخاص القانون الدولي ومنها الدول ملزمة بالامتثال وتنفيذ الالتزامات الدولية الناشئة عن العرف إعمالاً لما يقتضـــيه مبدا حســـن النية في العلاقات الدولية، وبمعنى آخر يجب مراعاة المصلحة الانسانية المشتركة ضمن المدى الذي يبسط فيه العرف قوته الملزمة وهذا يتأتى عن طريق اتخاذ اجراءات وتدابير عملية لوضع الالتزام العرفي موضع التنفيذ[١]، ومن الجدير بالذكر ان إمتثال الاســلحة المعلوماتية لقواعد القانون الدولي الإنســاني يتجســد من خلال توفير القدر الكافي من الحماية للبنية التحتية الحيوية لمنع التدمير الهائل والاذى والمعاناة غير الضـــرورية، وضمان الحد الادنى من الاتصالات الاساسية ذات الصلة بحماية المدنيين وان قواعد القانون الدولي الانساني قد شملت بحمايتها المستشفيات والمرافق الطبية، والنظم المالية وسلاسل الامداد، ووســائل النقل، ودور العبادة، والمراكز الدينية. وغالبا ما نجد ان كل انظمة الاســلحة المتطورة عمليا، تســتخدم تكنولوجيا المعلومات والاتصــالات لذلك من الصــعوبة والتعقيد عزل الاســلحة المعلوماتية عن الطائفة الكاملة للأســلحة وحيث ان الحرب المعلوماتية هي ظاهرة ذات نشــاط مستمر في الفضاء المعلوماتي لا يمكن التكهن بانتهائها بالنظر لمستوياتها المتعددة[٢].

وهذا الامتثال يتحقق بغض النظر عن اســم الاســلحة المعلوماتية ونوعها والتي تكون لها القدرة على الحاق اضرار تدميرية بالبنية التحتية المعلوماتية، فعلى سبيل المثال ليس هناك اهمية لنوع الجهاز الذي يستخدم في تعطيل نظام التحكم بالاقتصاد الوطني، او الاسلحة او المعلومات القومية سواء كان هذا الجهاز شفرة برنامجية، أم نبضة معلوماتية شديدة، وهناك نهج قائم يمكن بمقتضاه عد الاسلحة المعلوماتية على انها تشمل كل وسائل التدمير التي تستخدم تكنولوجيا المعلومات والإتصالات وهنا تتفق الدول على إعتبارها كذلك على وفق هذا النهج وبالتالي يتطلب التزامها بمكافحة هذه الاسلحة المعلوماتية بصرف النظر عن أسمها أو نوعها[٣]، والسؤال الذي

---

[١] . د. شريف عتلم، تطبيق القانون الدولي الانساني على الاصعدة الوطنية، بحث منشور في كتاب القانون الدولي الانساني، دليل التطبيق على الصعيد الوطني، دار المستقبل العربي، القاهرة، ٢٠٠، ص٣٠٧.

[٢] بن تغري موسى، الحرب السيبرانية والقانون الدولي الانساني، مجلة الاجتهاد القضائي، م (١٢)، ع(٢٢)، جامعة محمد خيضر بسكرة، الجزائر، ٢٠٢٠، ص٢٠٧-٢٠٨.

[٣] بن تغري موسى، المصدر نفسه، ص٢٠٣.

يتبادر الى الذهن ما الاســـاس القانوني الذي بموجبه تتمثل الأســـلحة المعلوماتية لقواعد القانون الدولي الإنساني؟ للإجابة على هذا السؤال.

يمكننا القول أن هذا الاســـاس القانوني يتجســـد في نص المادة (٣٦) من البروتوكول الاضـافي الاول لعام ١٩٧٧ والتي تنص على "يلتزم اي طرف سام متعاقد عند دراسة أو تطوير أو اقتناء ســـلاح جديد أو أداة للحرب أو إتباع أســـلوب للحرب، بان يتحقق مما اذا كان ذلك محضـــوراً في جميع الاحوال او في بعضـــها بمقتضـــى هذا الملحق – البروتوكول– أو أي قاعدة اخرى من قواعد القانون الدولي التي يلتزم بها الطرف السامي المتعاقد[١]، مع امكانية تطبيق نص المادة المذكور على الاسلحة المعلوماتية باعتبارها احد الاسلحة المستحدثة.

ومن الجدير بالذكر ان الخبراء في دليل تالين ذهبوا الى ادراج قاعدة تقضـي بامتثال جميع الدول الاطراف في البروتوكول الاضافي الاول إلى إجراء المراجعة القانونية عند دراسة او تطوير أو اقتناء سلاح أو وسيلة معلوماتية، أو اتباع اسلوب معين للحرب المعلوماتية، لغرض التأكد من مدى مطابقة هذه الاســـلحة المعلوماتية لقواعد النزاع المســـلح الذي تلتزم به، ولتقرير ما اذا كان محظوراً ســـواء في جميع الظروف أو بعضـــها بموجب أي قاعدة دولية أو احكام البروتوكول الاول[٢].

ثانياً: واجب الحياد المعلوماتي: أن استخدام الفضـاء المعلوماتي يمثل انتهاكا لمبدأ الحياد في القانون الدولي إذ أن الفضـــاء المعلوماتي يغطي حدود العديد من الدول وبالتالي فان الطابع الدولي للفضـاء المعلوماتي يجعل أياً من اطراف النظام الدولي في خطر شـن هجمات معلوماتية والتي قد تحدث اضـرار بالغة سـواء مادية أم عسـكرية، وبالتالي تهدد السـلم والامن الدوليين وهذا ما يؤكد على عدم امتثال الدول لواجب الحياد[٣]، والاسـئلة التي تطرح بهذا الصـدد ما الاسـاس

---

[١] ينظر المادة (٣٦) من البروتوكول الاضافي الاول لعام ١٩٧٧.

[2] . Tallinn Manual, ch. VII ,Sec 5, Rule (48), p128.

[٣] د. عادل عبد الصـادق، اسـلحة الفضـاء الالكتروني في ضـوء القانون الدولي الانسـاني، مصـدر سـابق، ص١٠٥.

القانوني للحياد؟ وهل يمكن تطبيقه في الفضـــاء المعلوماتي؟ وما مدى امتثال اطراف النزاع تجاه الدولة المحايدة؟ وهل هناك آثار تترتب على إنتهاك الحياد؟

كقاعدة عامة فان الحياد يعبر عن موقف الدولة التي لا تشترك في حرب قائمة مع الابقاء على علاقاتها الودية مع الدولتين المتحاربتين وتلتزم في مقابل ذلك بالأحجام عن تقديم أي مساعدة لأي من طرفي الحرب، وعدم الانحياز لطرف ضد طرف آخر[١].

وتجدر الأشـــارة إلى أن الفضـــاء المعلوماتي هو النطاق الذي تمر من خلاله الهجمات المعلوماتية العابرة للحدود وبالتالي فإنها تمر بدولة محايدة، ويمكن أن تحمل أسلحة خاصة تتنوع في التكتيك وطرق العمل، إلاّ إنّها تدخل ضمن تعريف الاسلحة باعتبارها أدوات للقتل واحداث الضرر أو تتسبب بجرح المدنيين او تدمير ممتلكات الخصم وبالتالي فإن الدولة المحايدة ملزمة بالامتناع عن نقل الاسلحة المعلوماتية عبر شبكات الاتصال والمعلومات المارة عبر اراضيها[٢]. حيث أن اقليم الدولة المحايدة يمتد ليشتمل على جميع اراضيها ومياهها الداخلية وبحرها الاقليمي والمياه الارخبيلية وطبقات الجو التي تعلوها والتي تكون خاضعة للسيادة الاقليمية لدولة الحياد[٣].

واذا ما بحثنا عن الاســاس القانوني لواجب الحياد لوجدناه بين ثنايا المعاهدات والاتفاقيات الدولية، كاتفاقية لاهاي رقم (٥) لعام ١٩٠٧ المتعلقة بحقوق وواجبات الدول المحايدة والاشخاص في حالة الحرب البرية، كذلك اتفاقية لاهاي رقم ١٣ لعام ١٩٠٧ المتعلقة بحقوق وواجبات الدول المحايدة في الحرب البحرية، علاوة عن اتفاقيات جنيف الاربع لعام ١٩٤٩ والبروتوكول الاضافي الاول لعام ١٩٧٧ كما ان ميثاق الامم المتحدة لعام ١٩٤٥ وبعض قرارات مجلس الأمن يمكنها

---

[١] د. علي صادق ابو هيف، القانون الدولي العام، ط١، منشأة المعارف، الاسكندرية، ١٩٧١، ص٩٤٩.

[٢] . د. عادل عبد الصادق، مصدر سابق، ص١٠٥.

[٣] . اشار دليل سان ريمو بشان القانون الدولي المطبق اثناء النزاعات المسلحة لعام ١٩٩٤ في الفقرة ١٤ على انه: (تشـمل المياه المحايدة المياه الداخلية المحايدة وبحارها الاقليمية وعند الاقتضـاء المياه الارخبيلية، ويشـمل الفضاء الجوي المحايد الممتد فوق المياه المحايدة للدولة المحايدة واراضيها).

في حالات معينة ان تجري تعديلات على قانون الحياد[١]. وكقاعدة عامة فأن الغرض من انتهاك البنية التحتية التابعة للدول المحايدة هي التأثير عليها على نحو سلبي كالعمليات التي تمر من خلالها، أو تلك التي يتم استخدامها للقيام بعمليات على شبكة الحاسوب ضد الطرف الخصم[٢].

وفي سياق حياد الدول المعلوماتي، فانه يحظر على الاطراف المتحاربة استخدام البنية التحتية المعلوماتية المحايدة، لغرض تنفيذ انشطة معلوماتية ضد الخصم او ضد آخرين، وينطبق هذا الحضر كذلك على ممارسة الاطراف المتحاربة لحقوقها من خلال استخدام المنشآت الحيوية التي تتمتع بالحصانة السيادية لانه يستخدم من قبل اجهزة دولة محايدة لاغراض حكومية ذات صبغة غير تجارية حصرياً والتي تقع خارج المنطقة المحايدة[٣]. الا ان هذا لا يمنع من وجود استثناءات محددة خارج نطاق الحضر الوارد على اساءة استخدام البنية التحتية للدولة المحايدة من قبل طرف النزاع، الا وهو استثناء الشبكات العالمية المفتوحة، كشبكة الانترنت فان استخدامها للاغراض العسكرية لا يؤدي الى انتهاك قانون الحياد، وان كانت مشيدة على اقليمها، وعلى الرغم من غياب النص القانوني المباشر الا ان غالبية الخبراء في دليل تالين اجمعوا على ان ما اشارت اليه المادة (٨) من اتفاقية لاهاي هي استثناء من الاصل العام التي بينت على انه "لا تكون الدولة المحايدة مطالبة بالمنع أو الحد من استخدام البرق أو الهاتف او اللاسلكي العائد لها أو للشركات أو افراد لصالح الاطراف المتحاربة"، إلا انه باستطاعة دولة الحياد فرض القيود على

---

(1) . See: Eric Talpot jensen, soverejnty and nutralityin conflict, fordham inter national law journal, volume35, issue(3), Articale2, 2012, p819 and Georgewalker Neutrality and information warfare, internatonal law studies, folume76, 2002, p244.

(٢) نصت المادة (١) من اتفاقية لاهاي الخاصة بحقوق وواجبات الدول المحايدة والاشخاص المحايدين في حالة الحرب البرية على انه: (لا تنتهك حرمة اراضي القوى المحايدة)، كذلك تضمنن المادة (١) من اتفاقية لاهاي ذات الصلة بحقوق وواجبات الدول المحايدة بالحرب البحرية على (ان الاطراف المتحاربة يقع عليها التزام باحترام الحقوق الثابتة للدول المحايدة والامتناع عن القيام بعمل بالاراضي او المياه المحايدة من شأنه ان يكون مخالفا للحياد).

(3) . See: Eric Talpot jensen, soverejnty and Neutrality in conflict, op. cit, p826.

استخدام مثل تلك الشبكات المعلوماتية مع ضرورة أن تكون مثل تلك القيود سارية في مواجهة اطراف النزاع دون تمييز بدلالة المواد (٧، ٨ ،٩) من اتفاقية لاهاي[١].

وبتحليل ما تقدم نجد إن قانون الحياد يوفر غطاء الحماية للدولة المحايدة ويوجب على الدول الامتثال للقواعد الواردة في المعاهدات والاتفاقات الدولية ذات الصلة بعدم استخدام البنى التحتية المعلوماتية لدول الحياد مع ضرورة ضمان احترام السيادة المعلوماتية لدولة الحياد لما تتمتع به الدول من ولاية إقليمية وقضائية تلزم جميع الاطراف المتحاربة بعدم تنفيذ هجمات معلوماتية من داخل الدولة المحايدة أو السيطرة أو التحكم بها من خلال الاسلحة المعلوماتية وباي وسيلة كانت.

المطلب الثاني

التدابير المضادة التي تتخذها الدولة للرد على عدم امتثال الدول المعتدية منع الهجمات المعلوماتية

أضحى الفضاء المعلوماتي مجالاً نشطاً لتنفيذ عمليات غير مشروعة دولياً ، لها تأثير مباشر على سيادة الدولة وما تتمتع به هذه السيادة من حصانة تقضي بعدم انتهاكها من قبل الغير، ومع ازدياد الأنشطة المعلوماتية المعادية باتت الدول تواجه صعوبة الرد على هذه الأنشطة المعلوماتية الضارة، وفي الفصل الاول من هذه الدراسة تناولنا حق الدفاع الشرعي في مواجهة الهجمات المعلوماتية والرد عليها ، هذا الحق الذي تناولته آراء القانونين المختصين، والإجتهادات الفقهية كخيار للرد على هجمات معلوماتية معادية على النحو الوارد في المادة

---

[١] . نصت المادة (٧) من اتفاقية لاهاي المتعلقة بحقوق وواجبات الدول المحايدة والاشخاص المحايدين في حالة الحرب البرية "لا تكون الدولة المحايدة ملزمة بمنح تصدير او نقل اسلحة او ذخيرة حربية لصالح احد الاطراف المتحاربة او شيء آخر قد يصلح لجيش او اسطول" فيما نصت المادة (٩) من نفس الاتفاقية على انه: "تطبق على كلا الطرفين المتحاربين اجراءات التقييد والحضر التي تتخذها الدولة المحايدة ضد مرتكبي الاعمال المشار اليها في المادتين (٧،٨) دون تمييز وتلتزم الدولة المحايدة بضمان احترام هذه القواعد ذاتها من قبل الشركات او الاشخاص اصحاب الاجهزة التلغرافية او الهاتفية او اللاسلكية"

(٥١) من ميثاق الأمم المتحدة ، الذي يتيح استخدام القوة للدولة في الدفاع عن نفسها، وهو بهذا المعنى إستثناء على مبدأ عدم اللجوء إلى القوة المسلحة.

إلا أن نظرة الفقهاء القانونيين لمفهوم الدفاع الشـرعي بعد بروز الأنشـطة الإرهابية وتفاقم خطرها ، قد تبلورت كثيراً وحاولت تجاوز المعنى اللفظي لنص المادة (٥١) من ميثاق الأمم المتحدة ، علاوة على تجاهل خيار أتخاذ تدابير مضـادة وردت الإشـارة إليها صـراحةً في المادة (٢٢) من مشـروع المواد ذات العلاقة بمسـؤولية الدول عن الأفعال غير المشـروعة دولياً لعام ٢٠٠١. هذه التدابير وردت تحديداً تحت الفصـــل الخامس ذات العلاقة بالظروف النافية لعدم المشروعية ذات الصلة بالهجمات المعلوماتية ، كإجراءات بديلة تحقق غرضها بكفاءة عالية بدلاً من حق الدفاع عن النفس الوارد في المادة (٢١) من ذات الفصل.

والسؤال الذي يطرح بهذا الصـدد: ما المقصـود بالتدابير المضـادة؟ وما مدى مشـروعيتها كخيار للرد على هجمات غير مشروعة دولياً؟ وما هي شروط استخدامها؟

ومن خلال ما تقدم سنتناول في هذا المطلب موضوع التدابير المضادة في فرعين ، نتطرق في الفرع الاول منه لتعريف التدابير المضـــادة وتميزها عن غيرها من المتشـــابهات، وفي الثاني نتناول شروط استخدام التدابير المضـادة للهجمات المعلوماتية ، والقيود الواردة عليها تباعاً وعلى النحو الآتي:

الفرع الاول

تعريف التدابير المضادة وتميزها عن غيرها من المتشابهات

سـنحاول بيان المقصـود بالتدابير المضـادة ومدى مشـروعيتها في الرد على الهجمات غير المشروعة دولياً ، فضلاً عن وضع الحدود الفاصلة بينها وبين بعض المفاهيم التي تتشابه معها:

أولاً : تعريف التدابير المضادة ومدى مشروعيتها :

تعرف التدابير المضادة على وفق الرأي السائد في فقه القانون الدولي العام بأنها: التدابير السلمية غير المصحوبة باستعمال القوة العسكرية[١]، وكان نتيجة للتغيرات الكبيرة التي طرأت على المجتمع الدولي إنتشار حركات فقهية وتشريعية على مستوى واسع رسخت الإتجاهات الحديثة للقانون الدولي ، وكان لها أثر هام في تسوية النزاعات بالوسائل السلمية وكان أهمها التدابير المضادة[٢]، وعلى الرغم من إن مصطلح التدابير المضادة من المصطلحات الحديثة نسبياً، إلاّ إن الإجراءات التي تتضمنها التدابير المضادة تعد قديمة نسبياً، حيث تعتبر أعمال الإنتقام المشروعة أحد مرادفتها، ومن الجدير بالذكر أن مصطلح التدابير المضادة كان قد ظهر بصورة فعلية في قرار التحكيم الدولي الخاص في قضية إتفاق الخدمات الجوية في عام ١٩٧٨ بين فرنسا والولايات المتحدة الامريكية.[٣]

وعلى الرغم من إن المصطلح قد لاقى رواجاً واسعاً لدى الفقه والقضاء، والممارسات الدولية، إلا إنه لا زال محل خلاف بين جمهور الفقهاء في القانون الدولي فيما يتعلق بمضمون هذهِ التدابير، والسبب في ذلك هو تباين تلك التدابير واركانها.[٤]

ومن المعلوم إن عبارة "التدابير المضادة"، هي صعبة التعريف إذا ما جاءت في سياق التدابير القسرية الإنفرادية، إذ إنها في الغالب تعني اتخاذ تدابير اقتصادية من قبل دولة لأجل حمل دولة أخرى على تغير سياستها.[٥]

---

[١] حسن خميس مصطفى السعدني، العلاقة بين التدابير المضادة والجزاءات في القانون الدولي المعاصر دراسة لحالة الملف النووي الايراني ، أطروحة دكتوراه ، كلية الاقتصاد والعلوم السياسية ، جامعة القاهرة ، ٢٠١٣، ص٣٩.

[٢] د.محمد حافظ غانم، مبادئ القانون الدولي، دار النهضة العربية، القاهرة، ١٩٦٨، ص١٧.

[٣] عبدالمنعم عبدالغفار نجم، الاجراءات المضادة في القانون الدولي العام، دار النهضة العربية، القاهرة، ١٩٨٨، ص١٤.

[٤] د.حسن خميس السعدني، مصدر سابق، ص٢٦-٢٧.

[5] See:F.Lowen Feld, international Economie Low (oxford.oxford).

وعُرفت التدابير المضادة على أنها" رد فعل على تصرف غير مشروع من جانب دولة ما، شريطة استيفاء شروط معينة من حيث الشكل والمضمون".[١]

ومن الجدير بالذكر إن قواعد القانون الدولي الخاصة بالمسؤولية الدولية قد تضمنت بنداً خاصاً بالتدابير المضادة التي يمكن اللجوء إليها عند الإقتضاء، فهذهِ التدابير لا يجوز تطبيقها في الاحوال العادية بالإستناد إلى الفعل الذي يعبر عنها لأن ذلك سيكون عادة مخالفاً لقواعد القانون الدولي، وهي بالنتيجة ليست سوى تمكين لدولة متضررة من القيام بسلوك، أو إلانتهاء عن القيام بسلوك، في وجه دولة اخرى تسببت بالضرر، ومن أمثلة التدابير المضادة الخاصة بأرغام الدولة المخالفة للعدول عن مخالفتها الالتزاماتها الدولية، هي التدابير التي يلجأ إليها كوسيلة ضغط في حالة غياب العقوبات الرادعة، والأصل هو منع تلك التدابير في الظروف الاعتيادية، إلا إن من ينظر لأحكام القضاء الدولي يجد بأن هناك العديد من القرارات القضائية الدولية التي أباحت بعض التدابير المضادة بسبب ما ينشأ عنها من جوانب إيجابية قد تغني عن اللجوء للقضاء[٢].

أما معهد القانون الدولي فقد أوجد لها تعريفاً في دورته المنعقدة عام ١٩٣٤، على أنها" تدابير قسرية استثنائية من وجهة القواعد الاعتيادية للقانون الدولي، تلجأ إليها الدولة على أثر فعل غير مشروع ضار بها ناشيء عن دولة أخرى بغية حمل الأخيرة على الامتثال للقانون وعدم الاضرار بها[٣].

كذلك عرفت على أنها: الإجراءات التي تشتمل على عدم تنفيذ التزام دولي تجاه دولة قامت بأنتهاك التزاماتها، ويخضع تقييم هذهِ الالتزامات للدولة المتضررة، شريطة أن تكون متناسبة

---

[١] ولد جيلاني هواري، العقوبات الاقتصادية الدولية وتأثيرها على خطط التنمية المحلية، رسالة ماجستير، مستغانم، الجزائر، ٢٠١٤، ص١٩.

[٢] ينظر بهذا الصدد: قضية مشروع غابشيكوفو– ناغيماروس بين هنغاريا وسلوفاكيا:
Gabcikovo– Nagymarosproject (Hungary and Slovakia), ICJ97, judgment of 25 september 1997, p.83.

[٣] التعليق على المادة (٤٩) بشأن موضوع التدابير المضادة وقيودها من مشروع لجنة القانون الدولي لعام ٢٠٠١.

وحجم الانتهاك المذكور، ويمكن تبرير اللجوء التدابير المضادة بصفتها تدابير مؤقتة ينتهي العمل بها حال تحقيق أهدافها، ومع ذلك يجب أن لا يمتد تأثير التدابير المضـادة إلى حظر اللجوء إلى القوة وفي الالتزامات الخاصـــة بحماية حقوق الإنســـان والالتزامات التي تحظر عمليات الانتقام وغيرها من الالتزامات بموجب القواعد ذات الصفة الأمرة في القانون الدولي.[١]

وخلاصـــة القول نعتقد أن أغلب التعاريف ســـالفة الذكر تذهب إلى إن الغرض من لجوء الدولة لاتخاذ تدابير مضادة، هو لحمل الدولة المعتدية على الامتثال لقواعد القانون الدولي والكف عن القيام بفعل غير مشروع دولياً، تجاه دولة أخرى.

وإذا كانت التدابير المضـادة قد جاءت على هذا الوصـف القانوني فلا بد لنا من أن نبحث عن مدى مشـروعيتها كتصـرفات صـادره من دولة ضـد دولة أخرى، فالتدابير المضـادة تصـرف قانوني دولي والتصـــرف القانوني يقصـــد به التعبير عن إرادة الدولة لغرض أحداث آثار معينة، ووفقاً لما جاء باحكام المادة (٢٢) ذات الصـلة بالتدابير المضـادة فيما يتعلق بفعل غير مشـروع دولياً، فأنه تنتفي صـــفة عدم المشـــروعية عن فعل الدولة المخالف لالتزاماتها الدولية تجاه دولة اخرى، إذا كان هذا الفعل يشـكل تدبيراً مضـاداً متخذاً ضـد الدولة الأخيرة، وبالقدر الذي يتناسـب مع هذا الفعل، وفقاً لأحكام الفصل الثاني من الباب الثالث[٢].

وعلى الرغم من أن مشـروع المواد المتعلقة بمسـؤولية الدول عن الأعمال غير المشـروعة دولياً لا تعد من قبيل الاتفاقية الدولية على نحو المعنى الوارد (الذي يجعلها خارج نطاق الاتفاقيات الملزمة والمقررة في قواعد اتفاقية فينا لقانون المعاهدات)، إلا إنها تتمتع بصفة القواعد القانونية الملزمة، باعتبار أن الجمعية العامة للأمم المتحدة عملت على تطوير قواعدها والتوصية بنفاذ بنودها، بل أنه يمكن القول بأن الكثير من قواعد هذا المشـروع هو انعكاس لمضـمون قواعد

---

[١] د.اياد يونس محمد الصـــقيلي، الحظر الدولي في القانون الدولي العام، دراســـة قانونية، دار الفكر الجامعي، الاسكندرية، مصر ، ٢٠١٤، ص٦٨.

[٢] مشروع المادة (٢٢) من مشاريع مواد المسؤولية الدولية عن الفعل غير المشروع دولياً – حولية القانون الدولي ٢٠٠١، م (١)، عن اعمال الدورة الثالثة والخميس للجمعية العام للأمم المتحدة (٢٣) ابريل/١ حزيران– ٢ تموز/ ١٠ آب ٢٠٠١، ص٣٢٨.

عرفية ملزمة، ومن الدلائل على ذلك قيام المحاكم الدولية وبصورة متكررة بأستخدام هذا المشروع لأصـــدار الكثير من قراراتها والتي تجاوزت المائة والخمســـين مرة[١]. لذا نعتقد بإمكانية تطبيق قواعد القانون الدولي ذات الصـــلة بالمســـؤولية الدولية عن افعال الدول غير المشـــروعة دولياً وبصـــورة مباشـــرة، وعلى ســـبيل المثال قيامها بفعل غير مشـــروع يدخل في ســـياق الانشـــطة المعلوماتية الضارة بدولة أخرى.

ومن الجدير بالذكر إن الفقه الدولي انقسم بين مؤيد ومعارض لإضـفاء صـفة المشـروعية على اللجوء للتدابير المضـــادة فوفقاً للاتجاه المؤيد للصـــفة القانونية للتدابير المضـــادة، يذهب اصـحاب هذا الاتجاه إلى إضـفاء صـفة المشـروعية على التدابير المضـادة، ويرى انصـار هذا الاتجاه ان التدابير المضـادة هي جزاءات دولية قانونية الغرض منها حفظ السـلم والأمن الدوليين للمجتمع الدولي ككل.[٢]

اما الاتجاه المنكر للصـــفة القانونية للتدابير المضـــادة، فيذهب هذا الاتجاه إلى عدم عد التدابير المضادة جزاءات قانونية، فهي وأن تمتعت بالصفة الجزائية إلا إنها لا تتسم بالشرعية.[٣]

ونعتقد أن الرأي المؤيد لإضـفاء الصـفة الشـرعية على لجوء الدول للتدابير المضـادة هو الأقرب للصـواب، والذي يعدها بمثابة جزاءات قانونية دولية لحمل الدولة المعتدية للامتثال لقواعد القانون الدولي وحثها على الكف عن الفعل غير المشـــروع دولياً، والقول بخلاف ذلك يجعل من الدول تتمادى في إرتكاب أفعال غير مشـروعة دولياً وبصـورة متكررة ينجم عنها اضـرار بالدولة المعتدى عليها.

ثانياً: تمييز التدابير المضادة عن غيرها من المتشابهات

---

(1) U.N.Doc.ST/LEG/SER.B/25 (2012).

[٢] د.محمد سـعيد الدقاق، عدم الاعتراف بالاوضـاع الإقليمية غير المشـروعة ، دراسـة لنظرية الجزاء في القانون الدولي، دار المطبوعات الجامعية، القاهرة، ١٩٩١، ص١٦.

[٣] د.عبدالمعز عبدالغفار نجم، مصدر سابق، ص١٣٨.

لغرض الوقوف على معنى أدق لمصطلح التدابير المضادة، لا بد من التفرقة بينها وبين الإجراءات الأخرى النافية لعدم المشروعية وعلى وفق الآتي:

١- الدفاع الشرعي: يتمثل الدفاع الشرعي بأحد صور المساعدة الذاتية، بل تكاد تكون الصورة الوحيدة التي تتمتع بالشرعية الدولية[١]، ويشترك الدفاع الشرعي مع التدابير المضادة في كونه يشكل رداً على انتهاك القاعدة القانونية لغرض منع الضرر أو حفظ الحقوق للطرف المتضرر[٢]، ويقتصر الدفاع الشرعي على الرد على العدوان المسلح، وهو استخدام القوة لحل المنازعات الدولية، بينما يمتد نطاق التدابير المضادة ليشمل جميع الاجراءات السلمية بمختلف انواعها التي من شانها أن تعطل الالتزامات التي تقع على عاتق الدولة المتضررة تجاه الدولة المخالفة[٣].

ويتميز الدفاع الشرعي بانه رد مباشر على عدوان مسلح قائم فعلاً عند حصول هذا الرد، لوقف الفعل غير المشروع ومنع ترتيب آثاره التامة، في الوقت التي تكون التدابير المضادة رداً على فعل غير مشروع استغرق فترة زمنية كافية لترتيب بعض الآثار القانونية الضارة، وغالباً ما تقترن هذهِ التدابير بالطلب إلى مرتكب المخالفة الدولية بالعدول عنها أو بأصلاح الضرر الناشيء عنها[٤].

٢- **الأعمال الانتقامية:** يقصد بالأعمال الإنتقامية هي التي تحدث خلال نزاع مسلح، وتشكل بذاتها انتهاكاً للقانون الدولي الإنساني، وأن وردت على شكل رد تجاه سلوك عسكري غير

---

[١] د.منى محمود مصطفى، استخدام القوة المسلحة في القانون الدولي بين الحظر والاباحة ، دار النهضة العربية، ١٩٨٩، ص٢٢.

[2] Dennis alland, La Leg'itime defence et Les contre-mesures dans la condification du droit international de La responsabilite. Journal de droit international , No(3), 1983, p.734-735.

[٣] د.زهير الحسني، التدابير المضادة في القانون الدولي العام، دراسة في وسيلة ضمان الاداء إزاء انتهاك القانون الدولي دون إثارة المسؤولية الدولية، ط١، المركز العربي للنشر والتوزيع، القاهرة، مصر، ٢٠٢٠، ص١٩.

[٤] د.زهير الحسني، المصدر نفسه، ص١٩-٢٠.

قانوني من العدو[١]، وهي على النقيض من التدابير المضـــادة، والتي تتمثل في محاولة إعادة الفعل غير المشروع إلى ما كان عليه ليصبح مشروعاً[٢].

٣- **الأعمال غير الصـديقة:** يقصـد بالاعمال غير الصـديقة هي التي لا يشـترط بها أن تكون تصرفات غير مشروعة، ولا تنتمي اساساً إلى طائفة التصرفات غير المشروعة[٣].

وخير مثال على ذلك ما ورد في المبدأ الثاني من مبادئ تالين، قيام الدولة باعتراض موجات معلوماتية خارجية على اعتبار أنها تتمتع بسـلطة على المنشـآت المعلوماتية الداخلة في اقليمها.[٤]

وهذا التصرف هو تصرف قانوني حتى وأن كان متعارضاً مع مصالح الدولة التي انبعثت من اراضـــيها الموجات المعلوماتية طالما أنه لم يخالف اتفاقاً مبرماً بين الدولتين، أو جاء مخالفاً لعرف دولي، بل إن انهاء الإتفاق ذاته بصـورة منفردة وأن كان جائزاً بموجب الاتفاق، فأنه لا يعد بذاته من قبيل التدابير المضادة.[٥]

٤- الجزاء الدولي: أن أهم ما يميز الجزاء الدولي عن التدابير المضـــادة هو تردد الهيئات الدولية والقضـائية والسـياسـية في النطق بالجزاء الدولي، لصـعوبة اتخاذ قرارات، فضـلاً عن قدرة

---

[١] ينظر: المادة (١/٤٩) من النصـوص ذات الصـلة بمسـؤولية الدول عن الافعال غير المشـروعة دولياً لعام ٢٠٠١.

[٢] تضمنت المادة (٥٣) من المشروع الحالة التي تكون فيها الدولة المسؤولة قد امتثلت لالتزاماتها بالكف والجبر بموجب الباب الثاني استجابة للتدابير المضـادة التي لجأت إليها الدولة المتضـررة، وطالماً أن الدولة المسؤولة قد أوفت بالتزاماتها بموجب الباب الثاني، لا يكون هناك أي سبب يدعو للابقاء على التدابير المضـادة ويجب وضـع حد لها بصورة فورية.

[3] See:T.G.Retorsion, 8 MAX planck Ency Clopedia of the international Law, 976, 2012.

[٤] مايكل ن.شميت، الحرب بواسطة شبكات الاتصـال، الهجوم على شبكات الكمبيوتر (الحاسوب) والقانون في الحرب، اللجنة الدولية للصليب الأحمر، ٢٠٠٢، ص١٢ وما بعدها.

[٥] ينظر نص المادة (٤٢) من اتفاقية فيينا لقانون المعاهدات لعام ١٩٦٩.

وضع هذهِ التدابير موضع التنفيذ[١] وغالباً ما تستهدف الجزاءات حماية المصلحة العامة ، إلا إن التدابير المضادة كمبدأ عام ترمي إلى حماية المصالح الذاتية للدول.[٢]

ومن نافلة القول، لا يمكن عد العقوبات التي يفرضـــها مجلس الأمن من قبيل التدابير المضادة، وخصوصاً تلك العقوبات الواردة بالاستناد إلى الفصل السابع من ميثاق الأمم المتحدة، وعليه يكون اعتراض الاتصـــالات بموجب قرار مجلس الأمن، واســتناداً لأحكام المادة (٤١) من الميثاق هو مشــروعاً لمن يقوم بتنفيذه، ولا يمكن وصــف اعمال تحطيم وأحداث اضــرار بالبنية التحتية الخاصــة بشـبكة الاتصــالات والمعلومات لدولة صــدر بحقها مثل هذا القرار بالاجراءات المضادة.[٣]

٥- الضرورة: تختلف التدابير المضادة عن أعمال الضرورة في الحالات الآتية:

أ- يشــترط وقوع عمل دولي غير مشــروع لغرض اللجوء إلى اعمال الضــرورة، بينما لا يشترط ذلك للجوء إلى التدابير المضادة.

ب- لا يتم اللجوء لأعمال الضرورة إلا في الحالات الإضطرارية الملحة، وعوضاً عن ذلك يتاح للدولة اللجوء للتدابير المضادة لردع التصرفات الخارجية غير القانونية، ولكن الأقل الحاحاً، ويبدو أن الأمر غير مختلف في ســـياق الهجمات المعلوماتية المعادية فالإمكان قبول أن يكون الرد جاء بالاستناد لمبدأ الضـرورة في مواجهة التصـرفات التي تهدد البنية المعلوماتية للدولة التي تتعرض لخطر اعتداء معلوماتي من طرف خارجي[٤].

علاوة على ذلك فأن التدابير المضادة تختلف عن الأعمال التي يلجأ إليها بحجة الضرورة، ففي الحالات التي لا يسـتطيع من خلالها درء خطر داهم على مصـلحة دولية مهمة، فأن اللجوء

---

[١] د.زهير الحسني، مصدر سابق، ص١٧.

[٢] د.حسن خميس مصطفى السعدني، مصدرسابق، ص٢٨.

[٣] ينظر المادة (٤١) من ميثاق الامم المتحدة لعام ١٩٤٥.

[٤] مايكل ن.شميت، الحرب بواسطة شبكات الاتصـال، الهجوم على شبكات الكمبيوتر (الحاسوب) والقانون في الحرب، مصـــدرســـابق، ص١٤، كذلك ينظر: مبادئ تالين، الخاصـــة بالقانون الدولي المســـتخدمة في الحروب السيبرانية.

إلى التدابير المضادة سواء اتخذت بشكل (هجمات معلوماتية أو غير معلوماتية)، يصبح مشروعاً بحكم تلك الضـــرورة، طالماً إن تلك التدابير اتخذت في حدود رد الاعتداء، أو الحماية مصـــلحة دولية اساسية[١].

أما الشروط السابقة لحق اللجوء إلى التدابير المضادة هي :

أ- وجود مخالفة لالتزام دولي تجاه دولة اخرى.

ب- اسناد الفعل غير المشروع للدولة، وهي نفس شروط تحقق المسؤولية الدولية الناشئة عن الهجمات المعلوماتية، والتي سنأتي على ذكرها بالتفصيل في المبحث الثاني من هذا الفصل عند التعرض للمسؤولية الدولية الناشئة عن عدم امتثال الدول لواجب العناية اللازمة للدول.

الفرع الثاني

نطاق التدابير المضادة والقيود الواردة عليها

إن فرض القيود على سلطة الدولة بغية الحفاظ على شروط ممارسة التدابير المضادة غير كافية، مهما كانت قيمتها وأهميتها، لأنها خاضـــعة لاعتبارات الدول الآنية ومصـــالحها الذاتية[٢]، وتماشـــياً مع طبيعة قواعد القانون الدولي، هناك قيود واضـــحة على الاجراءات التي باســـتطاعت الدولة التي تعرضـــت لهجوم غير مشـــروع أن تلجأ إليها بموجب مبدأ التدابير المضـــادة تتمثل بصـعوبة إتخاذ تدبير مضـاد معلوماتي إلا بسبب فعل سـابق غير مشروع دولياً نفذته دولة ما[٣]، أي أنه يتناول حدود التدابير التي كان اتخاذها ســـيتعارض مع التزامات الدولة المتضـــررة لو تم اتخاذها في الظروف الاعتيادية ضد الدولة المتسببة بالضرر من أجل حملها على الكف عن هذا الفعل الضار وجبر الضرر.

---

[١] ينظر : فتوى محكمة العدل الدولية في قضية حائط الفصل العنصري، (I.C.J.l36,140,2004).

[٢] د.زهير الحسني، مصدر سابق، ص٥٨.

[٣] د.حسن خميس مصطفى السعدني، مصدر سابق، ص٦٢.

ومن الاهمية بمكان أن نتطرق لنطاق التدابير المضـــادة والقيود الواردة عليها على وفق الآتي:

أولاً: نطاق التدابير المضادة ومدى تناسبها

اشـارت المادة (٥٥) من مشـروع مسـؤولية الدول الى التدابير المضـادة، وحددت الشـروط المتعلقة باتخاذ التدابير المضـادة ، حيث أنه قبل اللجوء للتدبير المضـاد تقوم الدولة المضـرورة بدعوة الدولة المســؤولة وفقاً للمادة (٤٤)،الى الوفاء بالتزاماتها المقررة ، وعليها توجيه اخطار للدولة المسـؤولة قبل القرار باللجوء للتدابير المضـادة وتعرض عليها اجراء مفاوضـات قبل البدء بالتنفيذ[١]، وكقاعدة عامة يجوز للدولة المتضـررة حق اتخاذ تدابير مضـادة ،وذلك باسـتثناء حالتين نصت عليهما المادة (٨٤)، من مشروع المواد المتعلقة بمسؤولية الدول عن الافعال غير المشروعة دولياً لعام٢٠٠١وهما: احتجاج دولة غير مضرورة بمسؤولية دولة اخرى، اذا كان التزام الذي انتهك واجباً ضـد مجموعة من الدول تضـم تلك الدولة ،وكان الهدف منه رعاية مصـلحة جماعية دولية ،ثانياً: احتجاج الدولة الغير مضـرورة اذا كان الالتزام الذي انتهك واجباً تجاه المجتمع الدولي ككل ،ويتطلب في هذهِ الاسـتثناءات ان تكون صـادرة عن مجموعة من الدول ،ولذلك فانه لا يحق لدولة منفردة غير متضـررة اللجوء للتدابير المضـادة[٢]، وبالرجوع للمادة (٤٤)من مشروع المواد ذات الصلة بالمسؤولية الدولية من الاعمال غير المشروعية دولياً ، نجد انها حددت شرطين لازمين قبل بدء الدولة المتضررة من اللجوء للتدابير المضادة وهما:

١- تقديم طلب الى الدولة المعتدية للوفاء بالتزاماتها الدولية :

يشـترط على الدولة المضـرورة تقديم طلب إلى الدولة التي ارتكبت الفعل غير المشـروع لغرض الوفاء بالتزاماتها الدولية، وقد اشارت المادة (٣٤) من المشروع إلى تبليغ الدولة المتضررة التي تحتج بمسـؤولية دولة أخرى طلبها إلى هذهِ الدولة، ويجوز للدولة المتضـررة أن تحدد بشكل

---

[١] حولية لجنة القانون الدولي لعام ٢٠٠١، م (٢)،الجزء (٢) ص٣٧.

[٢] حولية لجنة القانون الدولي لعام ٢٠٠١،م (٢) ،الجزء (٢)،في التعليق على احكام المادة (٤٨)منه، ص١٦٢.

خاص السلوك الذي يتوجب ان تنتهجه الدولة المسؤولة لوقف الفعل غير المشروع إذا كان مستمراً بالشكل الذي ينبغي ان يتخذه التعويض[١].

ونستطيع القول أن بعض الأعضاء الذين ساهموا بوضع المشروع، أدركوا إن التدابير المضادة تؤدي دوراً مهماً وحاسماً في أعمال الغرض من المسؤولية الذي يتمثل بحث الدولة المعتدية على الامتثال لالتزاماتها، وليس الكف عن الفعل فحسب، وانما لجبر الضرر أيضاً وعلى أية حال، فأن الطلب من الدولة المسؤولة القيام بالوفاء بالتزاماتها أو ضرورة اخطارها المسبق بأي قرار باتخاذ تدابير مضادة، والتفاوض معها على قدر الامكان، ليس بالأمر الهيّن أو يكون متاح دائماً ، فقد ورد في قرار صادر عن محكمة التحكيم الدولية في قضية الخدمات الجوية انه في ظل تعقيد العلاقات الدولية، فأنه ليس بالأمر اليسير دائماً تعطيل استخدام التدابير المضادة خلال فترة التفاوض[٢].

٢- إخطار الدولة المعتدية بالتدابير المضادة والالتزام بالتفاوض معها:

يستتبع طلب وقف الفعل غير المشروع فترة زمنية تستطيع من خلالها الدولة المسؤولة التصرف لإصلاح الوضع الناجم عن فعل الاعتداء بوقفهِ، أو التعويض عنه، أو بإعادة الحال إلى ما كان عليه حتى ما كان ذلك ممكناً، وفي حالة عدم الإستحالة لطلب وقف الانتهاك، فأن الدولة المتضررة بأستطاعتها اللجوء إلى التدابير المضادة، لكن مع احترام شرط الاخطار المنصوص عليه في المادة (٥٢) من مشروع المسؤولية الدولية، أي بمعنى آخر تبليغ الطرف المعتدي بقرار اللجوء للتدابير المضادة في مواجهته، واجراء مفاوضات معه قبل تنفيذه[٣].

---

[١] ينظر المادة (٣٤) من المشروع المتعلق بمسؤولية الدول من الافعال غي المشروعة دولياً لعام ٢٠٠١.

[٢] د.عبدالمعز عبدالغفار نجم، مصدر سابق، ص١٥٣.

[٣] د.حسن خميس مصطفى السعدني، مصدر سابق، ص٦٠ وما بعدها.

وتبرز فائدة هذا الشرط في استبعاد عنصر المفاجأة بالنسبة لبعض التدابير المضادة التي يتم اللجوء إليها، وعدم اتخاذ تلك التدابير إلى في حالة الضرورة، وإيجاد حلول سلمية لتسوية النزاع القائم بينهما قبل اللجوء لهذهِ التدابير[١].

وتأسيساً على ما تقدم نستطيع القول أن مشروع المواد المتعلقة بمسؤولية الدول عن الافعال غير مشروعة دولياً قد وضع الحدود المعتبرة قانوناً، قبل أن تلجأ الدولة المتضررة من الفعل غير المشروع إلى اتخاذ التدابير المضادة، وهي بالتأكيد اجراءات ضرورية لكلا الطرفين، ففائدة الطرف المعتدى عليه اللجوء للطرق السلمية في تسوية النزاع حتى لا يتفاقم ويؤدي إلى استمراره وبالتالي حدوث أضرار أخرى ناجمة عن اعتداءات على النظام المعلوماتي والبنى التحتية للدولة المعتدى عليها ، اما فائدة الدولة المعتدية من وضع هذهِ الحدود، فهي حتما لا تقع في عنصر المفاجأة وتجد نفسها في تدابير مضادة بمواجهتها، مع منحها الفرصة الكافية للتوقف عن فعلها غير المشروع دولياً، أو التعويض عنه، وعلى أقل تقدير إعادة الحال إلى كان عليه قبل الاعتداء، وهي بذلك تكون قد امتثلت للوفاء بالتزاماتها الدولية واحترام قواعد القانون الدولي، وتترشح عن هذهِ الحدود، نتيجة مفادها، أنه ما دامت الهجمات المعلوماتية قائمة، وهي بهذا الوصف تشكل جزءاً من سلسلة اعتداءات متكررة، وأن الخطأ سوف ينشأ عنه سلسلة من الاضرار المتعاقبة، فالحق في اتخاذ التدابير المضادة يبقى قائماً، طالما إن الدولة المعتدية تؤكد اصرارها بارتكاب الاعتداءات القائمة.

وإذا كانت التدابير المضادة تتطلب وضع حدود معينة لغرض اللجوء إليها، فإن التدابير المضادة حتى تكون في نطاق الشرعية الدولية، فلا بد من أن تكون متناسبة مع الضرر الذي أصاب الدولة المعتدى عليها، والسؤال المطروح للنقاش ما المقصود بالتناسب؟ وكيف يتم تقديره؟

---

[١] د.حسن خميس مصطفى السعدني، المصدر نفسه، ص٤٤.

أن مضمون التناسب في المعاملة بالمثل قد يكون بالتماثل، أو التعادل فيما بين الالتزامات المتقابلة، أما بالنسبة للانتقام فهو على النقيض من المعاملة بالمثل[١]، ذلك أن التدبير المتخذ على سبيل الانتقام قد يكون له صلة بالالتزامات تختلف بطبيعتها عن الالتزام الذي تم الاخلال به[٢].

وعلى أية حال فأن التناسب هو الذي يدل على مشروعية الرد، فقد اشارت المادة (٥١) من مشروع لجنة القانون الدولي إلى أنه عدم الاكتفاء بالربط بين الضرر الناجم عنها، بل بمراعاة عنصرين هما: خطورة الفعل الغير مشروع دولياً من جهة، والحقوق ذات الصلة من جهة اخرى، وأكدت المادة المذكورة على اهمية أن تكون التدابير المضادة متناسبة مع الضرر الحاصل، ويفهم من نص هذهِ المادة إن التطبيق العملي لمبدأ التناسب يتوقف على :

١- محدودية الرد: هو أن يكون رد الفعل على خرق الالتزام متماثلاً من حيث الدرجة مع الفعل غير المشروع.

٢- عدم المعاملة بالمثل: إذ إن بعض الالتزامات الدولية وخصوصاً القائمة منها تجاه الكافة، تؤدي إلى ابطال دور التدابير المضادة كوسيلة لوقف الضرر وهذا يعني إن الرد المماثل يؤدي إلى اضرار لا تمس الدولة المخالفة فحسب بل يمتد أثرها إلى غيرها من الدول، وبالتالي يجعل الرد غير ذي فائدة ومضراً بالغير الذي لم يصدر عنه أي فعل مخالف للقانون الدولي[٣].

وأما عن كيفية تقدير التناسب، فيجب عند تقديره عدم الاقتصار على مراعاة العنصر الكمي المحض للضرر الذي وقع، بل يجب مراعاة أيضاً عوامل كيفية، كأهمية المصلحة المشمولة بحماية القاعدة التي انتهكت، ومقدار خطورة الانتهاك، فالمادة (٥١) من المشروع تأخذ

---

[١] د.سعيد سالم جويلي، مبدأ التعسف في استعمال الحق في القانون الدولي العام، دار الفكر العربي، ١٩٨٥، ص١٦٤.

[٢] د.زهير الحسني، مصدر سابق، ص٤٨.

[٣] د.زهير الحسني، مصدر سابق، ص٥١.

بنظر الاعتبار آثار حقوق الدولة المسؤولة، ولا تشمل فقط أثر الفعل غير المشروع على الدولة المتضررة[١].

ثانياً: القيود الواردة على حق اللجوء للتدابير المضـــادة للرد على الهجمات المعلوماتية للدولة المعتدية.

أنطوت المادة (٥٠) من مشروع مسؤولية الدول عن الافعال غير المشروعة دولياً على بعض القيود والتي هي بمثابة التزامات دولية عند استخدام حقها في اللجوء للتدابير المضادة في مواجهة الأنشطة المعلوماتية المعادية، وهي الالتزامات بطبيعة الحال لا تتأثر بالتدابير المضادة وتشمل:

١- الالتزامات المتعلقة بالامتناع عن اســـتخدام القوة، أو التهديد بها، وإن أهم ما يميز التدابير المضـــادة في مفهومها الجديد، هي انها تدابير ذات طابع ســـلمي، إذ أن الالتزام المنصـــوص عليه في ميثاق الامم المتحدة وتحديداً في نص المادة (٢)، يعكس عرفاً دولياً قائماً لا يجوز الاخلال به[٢].

والسؤال المطروح بهذا الصدد، هل تشكل التدابير المضادة في بعض انواعها سبيلاً لاستخدام القوة؟

للأجابة على هذا السؤال نجد أنه من الصعوبة أن يتم تمييز بين ما يمكن عده من قبيل التدابير المضادة أو انه يعد استخدام للقوة، وبعد طول مناقشات بين الخبراء ممن ساهموا في وضـــع دليل تالين المطبق على الحروب المعلوماتية اكدوا على أن "العمليات المعلوماتية ترقى لمصاف استخدام القوة اذا امتد أثرها بطريقة مشابهة للأثر الذي يحدثه استخدام العمليات غير المعلوماتية التي تصل إلى مستوى استخدام القوة[٣].

---

[١] حولية لجنة القانون الدولي، ٢٠٠١، م (٢) ، الجزء (٢)، في شأن التعليق على أحكام المادة (٥١) الفقرة ٦، ص١٧٥.

[٢] د.زهير الحسني، المصدر السابق، ص١٢٤.

[3] Tallinn Manual, op, cit, Rule (11).

وبتحليل ما تقدم، تســـتطيع القول إن ما جرى من التأويلات التي أدت إلى اختلاف الآراء بين الخبراء في دليل تالين هي مســـألة تحديد فيما إذا كان الرد على الاعتداءات المعلوماتية هو بمثابة اســـتخدام للقوة، وليس اســـتخداماً لحق اللجوء في التدابير المضـــادة وبالتالي يجعل من الممكن تصور استخدام لقوة مناسبة لمواجهة انشطة معلوماتية معادية، دون أن يفقد هذا السلوك تصنيفه بأنه من التدابير المضادة، خصوصاً إذا لم يرقى الصدام إلى عتبة نزاع مسلح، وهذا يدل على أن هناك فرق بين الحالات التي يجوز فيها للدولة اســتخدام حق اللجوء للتدابير المضــادة، وتلك التي تمنحها اتخاذ حق الدفاع الشـرعي المسـلح، ومن نتائج هذا الاختلاف انه يمكن للدفاع الشرعي أن يأتي بصورة منفردة أو جماعياً، على النقيض من التدابير المضـادة التي لا تحبذ إلا إن تتخذ بشكل منفرد من قبل الدولة الي تعرضـت الاعتداء، ففي الحالة الأخيرة يحق لتلك الدولة اللجوء للتدابير المضـادة سواء كانت اعتيادية أو دفاع شرعي، حتى وأن أقتضـى الأمر استخدام القوة العسكرية.

و خير مثال على ذلك هو ما أوضـحه القاضـي (سيما) في قضـية موانئ النفط بقوله "في الحالات التي لا تصـل فيها المشـاكسـات الدولية مسـتوى الهجوم المسـلح بحسـب ما ورد المادة (٥١) من ميثاق الأمم المتحدة الخاصــة يحق للدولة الدفاع الشـرعي، يجوز للدولة فقط الحق في الرد المناسب والمتناسب لا غير"[١].

٢- عدم جواز اتخاذ تدابير مضـادة من شـأنها الاخلال بالالتزامات المتعلقة بحماية حقوق الانســـان الاســـاســـية: التدابير المحظورة، تلك التدابير التي تؤثر على حقوق الإنســـان وحرياته الاساسية التي لا يجوز المساس فيها كنتيجة مباشرة بصورة ما للجوء إلى التدابير المضـادة مثل الحق في الحياة والســلامة البدنية.[٢] لذلك لا يجوز اللجوء إلى التدابير المضــادة التي تســتهدف

---

[١] ينظر : قضـــية الانشـــطة المســـلحة في الكونغو بين الولايات المتحدة الامريكية والكونغو ينظر الوثيقة، (I.C.J.168,147, 2005).

[٢] د.سـعيد سـالم جويلي، الجوانب القانونية للتدابير المضـادة في القانون الدولي، مصـدر سـابق، ص١٨٣ وما بعدها.

الأفراد بصـورة مطلقة، لأن تلك التدابير يتحدد نطاق اللجوء إليها بالدول فقط.[١] كما يسـتند هذا القيد على عدة اعتبارات من أهمها:

أ- صعوبة وضع معيار للتناسب في حالات حقوق الأنسان، المتنوعة والمتعددة .

ب- عدم خضـــوع مواطني الدولة المعتدية لتدابير تتعارض مع المبادئ التي تحكم حقوق الانسـان ومعاملة المواطنين الاجانب وحماية ضـحايا الحرب[٢]، فعلى سـبيل المثال لا يجوز في جميع الأحوال والظروف أن تسـتهدف التدابير المضـادة المعلوماتية الحق في الحياة والسـلامة البدنية، ولكن إذا لجأت الدولة إلى اعاقة حركة الاجانب على اقليمها، فأنه يجوز للدولة التابع لها هؤلاء الاجانب، أن تلجأ للتدابير المضـــادة وكذلك ان تفرض قيود على حرية مواطنين تلك الدولة[٣].

٣- عدم جواز اللجوء للتدابير المضـــادة التي تتعارض مع الالتزامات ذات الصـــلة بالحصـانات والامتيازات الدبلوماسـية: إذ بموجب هذا الحظر، لا تعفى الدولة التي تلجأ للتدابير المضـادة من الوفاء بالتزاماتها بموجب أي اجراء يشـمل تسـوية المنازعات يكون تأخذ بينها وبين الدولة المعتدية، أو فيما يتعلق بالحفاظ على حرمة الأماكن الخاصـة بالممثلين الدبلوماسـيين أو القنصليين، أو غيرها من الاماكن والوثائق الدبلوماسية والقنصلية[٤].

وهذا اشـارت إليه محكمة العدل الدولية في حكمها الخاص بالنزاع الامريكي الايراني حول احتجاز طاقم موظفي السفارة الامريكية في طهران وتوصلت المحكمة إلى ان حكومة ايران لجأت إلى أساليب الإكراه ضد السفارة الامريكية وموظفيها بدلاً من اتباع الوسائل العادية المتاحة لها، وعدت أن احتجاز ايران لطاقم السفارة هو تدبيراً مضاداً باعتباره فعلاً غير مشروع ابتداءً، لكنه

---

[١] حسن خميس مصطفى السعدني، مصدر سابق، ص٣٣.

[٢] د.سعيد سالم جويلي، المصدر السابق، ص١٣٩.

[٣] ينظر المادة (٤) من العهد الدولي الخاص بالحقوق المدنية والسـياسـية لعام ١٩٦٦، كذلك المادة (١٥) من الاتفاقية الاوربية لحقوق الانسان لعام ١٩٥٠.

[٤] المادة (٥٠) (٢) (أ) من مشروع مواد المسؤولية الدول عن أعمالها غير المشروعة دولياً لعام ٢٠٠١، مصدر سابق. ص١٨٤.

يمنع من المسؤولية الدولية، لأنه بمثابة رد فعل تجاه تدخل الولايات المتحدة في شؤونها الداخلية، وعدم تسـليم المتهمين للمحاكمة في ايران، لذلك يسـتفاد من حكم المحكمة آنف الذكر أنه ينطبق على التدابير المضـــادة المعلوماتية بالقياس على التدابير المضـــادة غير المعلوماتية التي أقرتها المحكمة[١].

المبحث الثاني

المسؤولية الدولية المترتبة على عدم إمتثال الدول لواجب العناية

تعد المسـؤولية الدولية هي علاقة قانونية دولية، وأطراف هذه العلاقة هم أشـخاص القانون الدولي العام كالدول والمنظمات الدولية، وينصـرف مدلول الدولة إلى الدولة تامة السـيادة، وتنشـأ هذه المسؤولية الدولية نتيجة ارتكاب شخص من أشخاص القانون الدولي عملاً غير مشروع دولياً على وفق احكام القانون الدولي، ينجم عنه إلحاق ضـرراً بأفراداً أو أموالاً لشـخص من أشـخاص القانون الدولي.

والمسـؤولية الدولية هي الأداة التي تكفل تنفيذ الالتزامات التي يفرضـها القانون الدولي على أشـــخاصـــه، والدولة تبعاً لذلك تكون مســؤولة وفقاً لقواعد القانون الدولي ومبادئه عن تصـــرفات الأفراد والكيانات، متى ما كانوا يعملون تحت سيطرتها او أشرافها وبتوجيه منها، علاوة على ذلك وفي ظل التنظيم الدولي المعاصـــر فأنه من الطبيعي أن تترتب المســؤولية الجنائية الفردية على الأفراد الطبيعيين في حال ثبت ارتكابهم لجرائم ناشـــئة عن أفعال غير مشـــروعة دولياً تؤدي للأضـــرار بحقوق أفراد آخرين يخضـــعون للحماية المقررة لهم في ظل القانون الدولي الإنســاني والقانون الدولي لحقوق الأنسان، لا سيما في سياق الهجمات المعلوماتية التي تنفذها جماعات أو كيانات خاضعة لسيطرة الدولة الأخرى ، وقد تكون هذه الانشطة المعلوماتية تمر بأقليم أكثر من دولة، وتنطلق من أقليم الدولة المعتدية.

---

[١] د.أحمد حلمي ابراهيم، الدبلوماسية البروتوكول- الأتيكيت، المجاملة، القاهرة، دار عالم الكتب، من دون تاريخ نشر، ص٨٩.

ومن خلال ما تقدم سنبحث هذهِ المواضيع في مطلبين وعلى الشكل الآتي:

المطلب الأول: المسؤولية الدولية المترتبة على الأضرار التي تحدثها الهجمات المعلوماتية.

المطلب الثاني: المسؤولية الجنائية الفردية الناشئة عن عدم الامتثال لواجب العناية.

المطلب الأول

المسؤولية الدولية المترتبة على الأضرار التي تحدثها الهجمات المعلوماتية

تعد المسـؤولية الدولية من أهم المواضـيع الذي يرتكز عليها القانون الدولي، وغالباً ما يثير نشـــاط الدولة في اطار العلاقات الدولية كثيراً من المواقف التي تدعو الدولة إلى كفالة أحترام وتنفيذ أحكام وقواعد القانون الدولي العام، وإن التطورات التكنولوجية الحديثة أدت إلى ظهور مشـــكلات عملية جديدة لم تتناولها قواعد القانون الدولي بالتنظيم، وبالتالي ظهرت الحاجة إلى ضرورة معالجة هذهِ المشاكل بوسائل تتلائم مع طبيعتها، خصوصاً في ظل تعمد الدولة واصرارها الخروج على أحكام القانون الدولي العام، وسعيها لإلحاق الضـرر بدولة أو أكثر وبأي شكل من الأشكال. ومن خلال ما تقدم سنبحث هذا الموضوع في فرعين وعلى وفق الاتي:

الفرع الأول: تعريف المسؤولية الدولية والشروط اللازمة لقيامها.

الفرع الثاني: المسؤولية الدولية الناشئة في ضوء مفهوم واجب العناية.

الفرع الأول

تعريف المسؤولية الدولية والشروط اللازمة لقيامها

سـنتعرض في هذا الفرع إلى تعريف المسـؤولية الدولية بشـيء من التفصـيل من خلال اسـتعراض آراء الفقهاء القانونيين والاتجاهات الفكرية التي تناولتها، فضـلاً عن إيراد الشـروط اللازمة لقيام المسؤولية الدولية وعلى النحو الآتي:

أولاً: تعريف المسؤولية الدولية:

لا بد أن نشـير إلى إن المسـؤولية الدولية لا تتعارض مطلقاً مع فكرة سـيادة الدولة، فقيام المسـؤولية في الحقيقة هو نتيجة حتمية لتمتع الدولة بكامل سـيادتها[١]، فإذا كانت الدولة تتمتع بجميع الحقوق السـيادية ضـمن نطاق إقليمها، فهذا لا يمنع من إثارة مسـؤوليتها الدولية عند ارتكابها لفعل غير مشـروع دولياً لذلك أجتهد الكثير من الفقهاء والمختصـين بالشـأن القانوني في محاولات منهم لوضع تعريف شامل محدد للمسؤولية الدولية، فضلاً عما ورد في نصوص بعض الإتفاقيات الدولية من أشـارات واضـحة وصـريحة للمسـؤولية الدولية إذ يرى جانب من الفقه وفي مقدمتهم شـارل روسـو أن المسـؤولية الدولية هي :"وضـع قانوني تلتزم بمقتضـاه الدول المنسـوب إليها ارتكاب فعل غير مشـروع على وفق القانون الدولي بتعويض الدولة التي يقع في مواجهتها هذا الفعل"[٢].

ونسـتطيع القول أن الاقرار بالمسـؤولية الدولية ورد النص عليه في أكثر من موضـع، منها ما أشـارت إليه اتفاقية لاهاي الخاصـة بقواعد الحرب البرية لعام ١٩٠٧ بأن "الدولة التي تخل بأحكام هذهِ الاتفاقية يقع عليها التزام بالتعويض أن كان لذلك محل، وتكون مسـؤولة عن كل الافعال التي تحدث من أي فرد من أفراد قواتها المسـلحة"[٣]، ونلاحظ أن هذا التعريف قد ركز على إن الطرف الذي انتهك القواعد المنظمة لحالة الحرب يكون مسـؤولاً عن تلك الانتهاكات وما يترتب عليها من حدوث الأضرار التي يقوم بها الافراد المنتمين لقواته المسلحة.

أما المادة (١) من مشـروع مواد مسـؤولية الدول الناشـئة عن الاضـرار التي تصـيب الاشـخاص وأموال الأجانب في اقليمها التي اعدتها لجنة القانون الدولي العام فقد ورد فيها:" المسؤولية الدولية للدول بسبب الاضرار التي تصيب الأشخاص وأموال الأجانب في اقليمها ينشأ عنها الالتزام بتعويض هذهِ الاضـرار متى ما كانت نتيجة لأفعال ايجابية أو مواقف سـلبية منافية

---

[١] د.محمد المجذوب، القانون الدولي العام،ط١، منشورات الحلبي الحقوقية، بيروت، لبنان ، ٢٠٠٣، ص٢٥٣.

[٢] مفيد محمد شـهاب، القانون الدولي العام، المصـادر والاشـخاص، دار النهضـة العربية، القاهرة، ١٩٩٥، ص٢٧.

[٣] اتفاقية لاهاي الرابعة الخاصة بقواعد الحرب البرية لعام ١٩٠٧.

للالتزامات الدولية التي اتخذتها سلطاتها... ولا يجوز للدول أن تحتج بنصوص قانونها الداخلي لكي تتخلص من المسؤولية الناشئة عن الاخلال بالتزام دولي أو عن عدم تنفيذه[١].

كما عرفها انزلوتي على أنها "اسناد الفعل غير المشروع دولياً إلى أحد اشخاص القانون الدولي العام بسبب انتهاكه لالتزام دولي أو فعل غير مشروع دولياً، وبالتالي تلتزم الدولة المعتدية بأداء التعويض"[٢].

كذلك عرفها معهد القانون الدولي على أن:" تسأل الدولة عن القيام بفعل أو الامتناع عن فعل بما يتنافى مع التزاماتها الدولية أياً كانت سلطة الدولة التي قامت به، تأسيسية كانت أم قضائية أم تنفيذية"[٣].

ثم توالت التعريفات التي تناولت المسؤولية الدولية ، كل حسب وجهة نظرة التي يدافع عنها، فقد عرفها الدكتور عبد العزيز محمد سرحان بأنها :"الجزاء القانوني الذي يفرضه القانون الدولي العام على عدم احترام أحد الأشخاص هذا القانون لإلتزاماته الدولية"[٤].

أما الأستاذ عصام العطية فقد تناول المسؤولية الدولية على اساس الضرر الناشئ عن الفعل غير المشروع بالقول : "أن نظرية الفعل غير المشروع لم تعد كافية لتغطية جميع التصرفات الدولية الضارة ، إذ أضحت أغلب الأعمال المشروعة التي تمارسها الدول، تؤدي إلى إلحاق أضرار بغيرها من الدول الأخرى ، كالأنشطة النووية، التي هي الأخرى تكون مصدراً أو تعد سبباً لنشوء المسؤولية الدولية[٥].

وتأسيساً على ما تقدم يمكننا إيراد جملة من الملاحظات ذات الصلة بالمسؤولية الدولية:

---

(1) UN, ILC, state Responsibility, Agenda item5, Document A/CN/4/106, 1957, p.105.

(٢) السيد ابو عيطة، الجزاءات الدولية بين النظرية والتطبيق، مؤسسة الثقافة الجامعية، الاسكندرية، ٢٠٠١، ص٢٤٧.

(٣) نقلاً عن اسلام دسوقي عبد النبي دسوقي ، النظرية العامة للمسؤولية الدولية بدون خطأ، المسؤولية الدولية الموضوعية ، ط١، مركز الدراسات العربية ، القاهرة ، مصر ، ٢٠١٦، ص٦٣.

(٤) د.عبدالعزيز محمد سرحان، القانون الدولي العام، دار النهضة العربية، القاهرة، ١٩٨٠، ص٤٩٧.

(٥) د.عصام العطية ،القانون الدولي العام ،ط١، مكتبة النهضة، بغداد ، ٢٠٠٨، ص١٦.

١- إن مضـمون المسـؤولية الدولية يتمثل بقيام الدولة بفعل غير مشـروع دولياً أو انتهاك التزام دولي قائم.

٢- اختلفت الآراء واجتهدت كثيراً في محاولة وضـع تعريف محدد للمسؤولية الدولية فمنهم من ضـــيّق من مفهوم المســـؤولية الدولية باعتبارها مجرد إخلال من أحد أطراف العلاقة بالتزام دولي ، أما أصـــحاب الإتجاه الذي حاول التوســـع في مفهوم المســـؤولية الدولية، فهو يصـــور المسـؤولية الدولية على أنها ليس مجرد علاقة بين دولتين بل يشـترك في هذه المسـؤولية فضـلاً عن الدول والأفراد والكيانات الدولية.

٣- إن من النتائج المترتبة على قيام المسؤولية الدولية هي التعويض عن الفعل الضار أو إعادة الحال إلى ما كان عليه قبل حدوث الفعل غير المشروع.

وفي ضوء ما تقدم يمكننا صياغة تعريف للمسؤولية الدولية بأنها (قيام الدولة بارتكاب فعل سواء كان هذا الفعل مشروع أم غير مشروع دولياً ، ويؤدي إلى إحداث أضرار بدولة أو عدة دول اخرى ، مما يترتب عليه التعويض ، أو إعادة الحال إلى ما كان عليه).

ثانياً: شروط قيام المسؤولية الدولية عن انتهاك واجب العناية المعلوماتية

إن المســؤولية الدولية لا يمكن إثارتها في مواجهة دولة ما والتي تســببت بإلحاق اضــرار بدولة أخرى من دون توافر بعض الشروط اللازمة لذلك والمتمثلة بالآتي:

١- القيام بفعل غير مشروع دولياً

يشـترط لتحقق المسـؤولية الدولية أن يكون الفعل المنسـوب للدولة غير مشـروع ، ويمكن تعريف الفعل غير المشـــروع على أنه:" ذلك الفعل الذي يتضـــمن انتهاكاً لإحدى قواعد القانون الدولي العام أياً كان مصدرها ، أو اخلالاً بأحد الالتزامات الدولية سواء كان هذا الفعل إيجابياً أم سـلبياً"[١]، أو إذا شـكل هذا الفعل انتهاكاً لالتزام دولي من نوع (الإلتزام بإتباع سـلوك) كالالتزام

---

[١] لفقير بولنوار، جرائم الحرب في ضوء أحكام القانون الدولي الإنساني، دار الأيام للنشر والتوزيع، عمان، الأردن، ٢٠١٥ ، ص١٦٥.

بالتفاوض ، أو يكون من نوع (الالتزام بتحقيق نتيجة) كالالتزام بإعادة الاشـــياء التي جرت مصادرتها بصورة غير مشروعة[١].

ولكي تشكل الهجمات المعلوماتية فعلاً غير مشروعاً وضار بالدول الأخرى يجب أن يكون هذا الفعل على وفق الآتي:

١- خرق مبادئ ميثاق الأمم المتحدة كأن يرقى الهجوم إلى مســـتوى اســـتخدام القوة من خلال استخدام الوسائل المعلوماتية في حال إسنادها لدولة معينة.

٢- انتهاك الالتزامات الدولية التي يفرضـها القانون الدولي الإنسـاني ومثال ذلك اسـتهداف الأعيـان المـدنيـة بهجمـات معلومـاتيـة ، كـالنظم المعلومـاتيـة التي تتحكم في الإمـداد بـالطـاقـة الكهربائية ، إذا ما أسندت إلى دولة معينة.

٣- انتهاك القواعد الدولية في وقت السـلم وخارج سـياق النزاع المسـلح كانتهاك مبدأ عدم التدخل في الشؤون الداخلية للدول والاعضاء[٢].

ثانياً: نسبة الفعل غير المشروع إلى الدولة (الإسناد)

هناك إشـكالية على درجة من التعقيد تتمثل في تحديد مسـؤولية الدولة عن شـن هجمات معلوماتية توصـف على أنها تحدياً قانونياً، ونتيجة لذلك أضـحت الدول تواجه صـعوبة بالغة في تمييز ذلك الهجوم والتحقق منه، وحتى إذا كانت الهجمات مجرد ردة فعل، فإنها غير قادرة على التمييز بين الأطراف وبالتالي تصـــبح غير قانونية، نتيجة لعبور الشـــبكات الحدود الدولية ، وأحداث إصـابات في أطراف محايدة كما إن التحقيقات بخصـوص الهجمات المعلوماتية قد تجمع

---

[١] د.احسان هندي، مبادىء القانون الدولي العام في السلم والحرب، ط١، دار الجليل للطباعة والنشر ، دمشق ، ١٩٨٤ ، ص٢٢٦.

[٢] سراب ثامر أحمد ، مصدر سابق ، ص١٢٨.

بين المباديء الأساسية لعمل اجهزه الاستخبارات بوصفها عملاً مادياً وبين الأنشطة المعلوماتية العابرة للحدود الدولية[١].

علاوة على ذلك فأن المسؤولية الدولية تكون إما مباشرة أو غير مباشرة ، ويمكن أن تثار المسؤولية الدولية عن الهجمات المعلوماتية في حال قيام أياً من هيئاتها كالوكالات الاستخباراتية أو الجيش مثلاً، بأنشطة معلوماتية تؤدي لانتهاك التزام قانوني دولي وليس مهم كون الفعل محل النقاش قد تم تطبيقه بالاستناد لتعليمات من الدولة أم من دونها طالما أن تلك الهيئة تتصرف بصفة رسمية بوصفها أداة للتعبير عن إرادة الدولة[٢].

والسؤال الذي يثار بهذا الصدد ما مدى مسؤولية الدولة عن تصرفات الأفراد القراصنة الخاضعين لسيطرتها؟

من المعلوم أن هناك إجماعاً بين الخبراء الدوليين على أن القانون الدولي ينطبق على شبكة الانترنيت، ومن الممكن أثارة المسؤولية الدولية الناشئة عن الفعل الضار، إلا إن مسألة اسناد تصرف معين إلى دولة بموجب القانون الدولي يكون بحاجة إلى دليل واضح لإثبات سيطرة تلك الدولة في ضوء قواعد المسؤولية الدولية غير المباشرة، عن تصرفات الأفراد الذين يخضعون لسيطرتها الفعلية، ويعملون تحت اشرافها وكذلك عن رعاياها بشرط أن تحقق السيطرة الكاملة والفعلية.[٣]

ويبقى السؤال الأهم وهو كيف يمكن للدولة المعتدى عليها بهجمات معلوماتية غير مشروعة أثبات مسؤولية الدولة عن أعمال الجماعات المسلحة والأفراد؟

---

[١] سعيد درويش، ماهية الحرب الإلكترونية في ضوء قواعد القانون الدولي ، مجلة جامعة الجزائر ، ع(٢٩) ، (ج٢)، ٢٠١٦، ص١٢٧.

[٢] د.عبد الكريم علوان، الوسيط في القانون الدولي العام ، دار الثقافة ، عمان، ٢٠١٠، ص١٦٣.

[٣] د.أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة في ضوء التنظيم الدولي المعاصر، مصدر سابق، ص٦٤٢-٦٤٣.

للأجابة عن هنا السؤال لا بد من إثبات مدى سيطرة الدولة على هذهِ الأفراد أو الجماعات المسلحة التي تقوم بتنفيذ عمليات غير مشروعة دولياً خارج أقليمها.

وفيما يتعلق بمعيار السيطرة أوجد الفقه القانوني معياران للسيطرة وهما معيار السيطرة الفعالة(Effective Control)، ومعيار السيطرة الكاملة (Orevall Control).

١- معيار السيطرة الكاملة (Orevall Control) يعرف معيار السيطرة الكاملة على أنه" معيار يتطلب وجوده أن يكون للدولة موضوع الاتهام بالتدخل، في أي دور سواء في التنظيم والتنسيق أم التخطيط في عمليات أم تصرفات محددة تقوم بها مجموعات مسلحة، علاوة على وجود إشراف على شن تلك العمليات"[١].

وقد طبقت محكمة العدل الدولية معيار السيطرة الكاملة لأول مرة في قضية الأنشطة العسكرية وشبه العسكرية بين الولايات المتحدة الامريكية و نيكاراغوا عام ١٩٨٦، حيث ذهبت بالقول " معيار يحدد اسناد تصرفات الأفراد أو المجموعات المسلحة أو الكيانات إلى الدولة بذاتها، وأن مثل هذهِ التصرفات يجب أن تكون تحت رقابة صارمة من الدول... وفي حال ثبوت ذلك يجوز تحريك المسؤولية الدولية الناشئة عن انتهاكات الأفراد ضد الدولة أو المجموعات المسلحة والكيانات"[٢].

وهناك العديد من السوابق القضائية التي اعتمدت معيار السيطرة الكاملة لإثبات علاقة الدولة مع الجماعات المسلحة التي ارتكبت انتهاكات جسيمة وكان أهما، قضية تادتش (Tadic): حيث تم اعتماد معيار السيطرة الكاملة من قبل المحكمة الجنائية الخاصة بيوغسلافيا لغرض اثارة المسؤولية الدولية عن ما ينسب إليها من انتهاكات ارتكبتها مجموعات مسلحة مدعومة من قبلها ففي حكمها الصادر بقضية تادتش (Tadic)، ذهبت بالقول إلى " إن مثل هذهِ التصرفات لابد

---

(1) Erik Nyman, Orevall Control the case against Dusko Tadic and the concept of Control in the ILC-Articles on State Responsibility, Master thesis public inter national Law Faculty of law, university of laud, Sweden, spring , 2008, p.67.

(2) ICJ, Military and parmilitary Activities in and aginst Nicaragua (Nicar.v.us) op, cit, para, 109.

أن تكون تحت رقابة صارمة من الدول ويعامل الطرف الأخر..." واشارت إلى " كان للدولة دور في التنظيم والتنسيق، فضلاً عن تزويد المجموعة المسلحة بالدعم، وهذا يدل على أن لها السيطرة الكاملة عليها، وما يصدر عن المجموعات المسلحة، يكون صادر عن ذات الدولة"[١].

وفي سياق الهجمات المعلوماتية، فإذا ما قامت دولة ما بتزويد الجماعات المنظمة التي تقوم بالهجمات المعلوماتية، بالاسلحة المعلوماتية، وشاركت هذهِ الدولة مع الجماعات المنظمة في رصد الأهداف التي تمت مهاجمتها بصورة عامة، فسوف تكون هذهِ الدولة مسؤولة عن جميع الهجمات المعلوماتية التي تشنها الجماعات المسلحة وبموجب معيار السيطرة الكاملة[٢].

٢- معيار السيطرة الفعالة (Effective Control):

يقصد بمعيار السيطرة الفعالة إن "هناك دولة ما، تبسط سيطرتها على جزء من أنشطة المجموعات المسلحة، أو كان باستطاعتها اللجوء لاتخاذ التدابير اللازمة لمنع تلك الأنشطة والتي تنطوي على انتهاكات جسيمة، لكنها تراخت أو أمتنعت عن اتخاذ التدابير اللازمة لكبحها"[٣].

وقد ساهم القضاء الدولي في تقرير المسؤولية الدولية من عدمها في ضوء معيار السيطرة الفعالة، في العديد من القضايا ، فعلى سبيل المثال في قضية الإبادة الجماعية بين البوسنة والهرسك ضد جمهورية يوغسلافيا الاتحادية قد خلصت محكمة العدل الدولية إلى أن :" جريمة الإبادة الجماعية والأعمال الوحشية التي ارتكبت في أرجاء البوسنة والهرسك لم تكن بنية التدمير الجماعي التي تتطلبها جريمة الابادة الجماعية لعام ١٩٤٨، .. حيث أن الأدلة المعروضة على

---

(1) Conrad Wegalin'ski, cyber war fare and Responsibility of states, Torun inter national studies, the john paul II catholic university of Lublin, Vol.9, No(1), Poland , 2016, p.82.

(2) Kubo Macak, Decoding Articte of The inter national Law Commission's Articks on state Responsibility: Attribution of cyber operations by Non- state Actors , journal of Conflict And Security law of ford university press, Vol.21, No (3), 2016, p.422.

(٣) صادق باقر ابراهيم العلوي، المسؤولية الدولية الناشئة عن دعم المجموعات المسلحة، دراسة تحليلية في ضوء معيار السيطرة الكاملة، ط١، مكتبة زين الحقوقية والادبية، بيروت، ٢٠١٩، ص٦٢.

المحكمة لا تثبت أن الأعمال التي قام بها جيش جمهورية صـربيا يمكن اسـنادها إلى الخصـم المدعى عليه بموجب قواعد القانون الدولي لمسؤولية الدول[١].

ولا يمتد هذا المعيار لكي يشـمل التصـرفات التي لا تكون ذات صـلة بالدولة إلا إرتباطاً عرضياً أو هامشياً بعملية معينة، والتي لم تخضع لرقابة توجيه الدولة.[٢]

ومن الأمثلة التطبيقية لتحريك المسؤولية الدولية ضد دولة ما ، بالاستناد لمعيار السيطرة الفعالة في سياق الهجمات المعلوماتية، عندما تقوم دولة معينة بالتعاقد مع شركة وتوجيهها بشن هجوم معلوماتي ضـد دولة أخرى بهدف الدفاع عن نفسـها، كإجراء قانوني مشـروع دولياً، إلا إن الوسائل المستخدمة في العملية (الفيروسات) من قبل الشركة انتشرت وأصابت انظمة معلوماتية لدولة ثالثة مما أدى إلى إلحاق تدمير واسـع النطاق فيها، ففي هذهِ الحالة يجوز اسـناد الضـرر الناجم عن الهجمات الذي لحق بالدولة الثالثة إلى الدولة الأولى التي تعاقدت مع الشركة[٣].

ثالثاً: الضـرر: يعد الضـرر من أهم عناصـر تحقق المسـؤولية الدولية، فهو يدور وجوداً وعدماً مع المسؤولية الدولية، ويقصد بالضرر في مجال القانون الدولي" المساس بحق أو مصلحة مشروعة لأحد أشخاص القانون الدولي العام"[٤].

ويشـترط في الضـرر أن يكون فعلياً، أي يجب أن يكون هناك انتهاك حقيقي بحق الدولة المضرورة، وأن يكون مباشراً، فمن الطبيعي أن تسأل الدولة عن الضرر المباشر الذي تسبب به

---

[١] الأمم المتحدة، الجمعية العامة – تقرير محكمة العدل الدولية، ١آب أغسـطس ٢٠٠٦، ٣١ تموز/ يوليو ٢٠٠٦، الدورة الثانية والخمسون، الملحق رقم (٤) ، الوثيقة (A/62/4)، ص٥ ، الفقرة ١٥.

[٢] المادة (٨) التعليق (٣) من مشروع مسؤولية الدول عن الأفعال غير المشروعة دولياً لعام ٢٠٠١.

[3] Antonio Cassese , the Nicaragua and Tadic Tests Revisited in light of the ICJ. Judgment on Genocide in Bosnia , The European journal of Xford University, Vol.18, No.(4) EJIL, United Kingdom, 2007, p.652.

[٤] لفقير بولنوار بن الصديق، مصدر سابق، ص١٦٦.

تجاه الدولة الأخرى، وعلى النقيض من الضـــرر غير المباشـــر الذي ينشـــأ عن الفعل غير المشروع[١].

وما يؤكد هذا الشـرط ما جاء في حكم لجنة التحكيم في قضـية (Alabma) الصـادر عام ١٨٧٢، المتضـمن صـدور قرار من لجنة التحكيم تلزم فيه بريطانيا بصـرف تعويضـات للولايات المتحدة عن الضرر المباشر الذي تعرضت له، بسبب نشاطات سفينة في بريطانيا، خلال الحرب الأهلية الأمريكية، إلا إن المحكمة رفضـت في ذات الوقت صـرف تعويض عن الاضـرار غير المباشرة التي اصابت الولايات المتحدة الامريكية[٢].

الفرع الثاني

المسؤولية الدولية الناشئة في ضوء مفهوم واجب العناية

يقصد بمفهوم واجب العناية إن أي تصرف قانوني لا ينسب بصورة مباشرة إلى الدولة ولا يكون هناك أي التزام على الدولة لمنع هذا التصرف من الوقوع، لكن الدولة يقع عليها التزام ببذل عناية للسيطرة على هذا التصـرف قبل حدوث الضـرر، وبالتالي يتعين اتباع الخطوات المناسبة لضـمان امتثال الدولة لعدم انتهاك أي قاعدة قانونية ملزمة[٣]، ويمكن أن تنشأ المسؤولية الدولية عن عدم الامتثال لواجب العناية من خلال:

١- الاخلال بواجب (المنع)

كما بينا ســابقاً في معرض البحث عن مفهوم واجب العناية أن المقصـــود بهذا المبدأ هو امتناع الدولة عن اسـتخدام اراضـيها لتنفيذ أنشـطة تتعارض مع حقوق الدول الاخرى، وهو التزام عرفي تضـمنه المبدأ(٢١) من إعلان اسـتوكهولم وتم التأكيد عليه وتدوينه في تقرير لجنة القانون

---

[١] د.محمد ســعيد الدقاق، مصـــطفى ســلامة حســين، القانون الدولي المعاصـــر، دار المطبوعات الجامعية، الاسكندرية، ٢٠١٥، ص٣١٥.

[٢] د.غسان الجندي، المسؤولية الدولية، ط١، مطبعة توفيق، عمان، الاردن، ١٩٩٠، ص٧.

[3] Feredrik Von Bothmer, Contextualising legal Reviews for Autonomous weapon system, Dissertation university of sT, GALLEN, Germany, 2018, p.23.

الدولي في إطار المسـؤولية عن أعمال لا يحظرها القانون الدولي في واجب المنع في المادة (٣) منه بقوله " تتخذ دولة المصـدر جميع التدابير المناسـبة لمنع وقوع ضـرر جسـيم عابر للحدود والتقليل من مخاطرة للحد الأدنى"، ويستدل من ذلك على أن الدولة يقع عليها واجب منع الضرر العابر للحدود، ويسـمى بالتزام واجب العناية ايضـاً، وهذا الالتزام هو التزام بسـلوك وليس بتحقيق نتيجة، وهو بالتأكيد يخضـع لتقدير الدولة ويتأثر بعدة عوامل منها ، قدرة الدولة، وخطورة الفعل، الضرر الحاصل، ويشترط في الضرر المطلوب لبذل العناية اللازمة، هو الضرر الجسيم العابر للحدود، كالاضرار البيئة التي سبق وأن تطرقنا لها في الفصل الثاني من هذهِ الدراسة، وإضرار استخدام الفضاء الخارجي، والانشطة النووية، فعلى الدولة تحديد مخاطر الانشطة واتخاذ التدابير اللازمة ذات الطابع المستمر[١].

ومن خلال الاطلاع على المشـروعات الدولية ذات العلاقة بمسـؤولية الدول عن افعال الضارة لا يحظرها القانون الدولي، نجد أنها تقوم على ثلاث شروط هي:

١- ان يكون الضرر جسيماً.

٢- ان يكون الضرر مستمراً.

٣- ان يكون الضرر مادياً وواضحاً.

ويعد قرار لجنة القانون الدولي رقم (١٧/٣١) في ١٩٧٦/١٠/١٥ من القرارات المهمة التي عالجت إدراج المسـؤولية عن الافعال الضـارة التي لا يحظرها القانون الدولي ضـمن انشطتها[٢]

ونسـتطيع القول ان الدولة ملزمة بمنع المخاطر والتخفيف من حدة الضـرر في مرحلة تطوير الاسلحة المعلوماتية وقبل ان يتم نشرها واستخدامها.

---

[١] د.لمى عبدالباقي ، واسراء نادر كيطان، مصدر سابق، ص٣٥٠.

[٢] د.أحمد عبيس نعمة الفتلاوي، وأزهر عبدالامير، المسؤولية الناشئة عن استخدام وسائل القتال الفتاكة في نشر الاوبئة (الهجمات السيبرانيه في مقابل جائحة كورونا)، مصدر سابق، ص ٦٧ .

وأن واجب الدولة بمنع الضـرر العابر للحدود لا سـيما في الفضـاء المعلوماتي يتكون من التزامين، الاول هو التزام بالامتلاك (possessing) والذي تلتزم الدولة بموجبه بأن يكون لديها اجهزه قانونيه واداريه تكون قادرة على مواجهه الضـــرر العابر للحدود والوقاية منه، اما الالتزام الثاني هو التزام بالاســتعمال (using) ويتوجب على الدولة امتلاك اســتخدام وتحريك الاجهزة التابعة لها، في مده حدوث التصـرف الضـار الغير مشـروع، واسـتعمال هذه الاجهزة على وفق واجب العناية الذي تتطلبها الظروف وبموجب معيار الدولة المعتادة[١].

ومن ناقلة القول ان معيار واجب العناية لا يتطلب تحقيق نتيجة معينه، ولكن يســتلزم جهود افضل للقيام بما هو ممكن لمنع وقوع الفعل غير المشروع في حدود سلطة الدولة وقدرتها، فعلى سـبيل المثال أن محكمة العدل الدولية لن تكون باسـتطاعتها منع الابادة الجماعية، لكنها تستطيع أن تطلب من الدولة بذل واجب العناية وتسخير كل قدراتها لمنع وقوع الضـرر، الا ان ذلك لا يعد شرطا للنجاح وانما وسيله للمساعدة في الحد من الضرر[٢].

ولغرض اعمال واجب المنع، يتطلب ان تقوم الدولة باسـتخدام اطارها التشـريعي واجهزتها الادارية في مواجهه الأنشطة المعلوماتية وفي حالة وقوع اي ضـرر، كذلك يقع على الدولة التزام بتسخير قدراتها للتحقيق ومعاقبه مرتكبي الانشطة المعلوماتية الضارة، وبهذا المعنى يشمل واجب الدولة اجرائاً وقائياً حيوياً لغرض اعمال التدابير الوقائية ومنع المخالفة والحد من خطورة باقي المخالفين[٣]. ومن الجدير بالذكر ان مســاله تطبيق واجب العناية على الهجمات المعلوماتية قد لاقى معارضـه من بعض الدول لأنها تخشـى العبء الذي يفرضـه هذا الالتزام ، لكن في المقابل هناك بعض الدول مؤيده لتطبيق التزام واجب العناية على الانشـطة المعلوماتية الضـارة، وعلى الرغم من هذا الخلاف فانه فريق الخبراء الحكوميين قد اجمعوا على التزام الدولة بواجب العناية

---

(1) ICJ, Argentina v. Uruguay, pulp milis case, case concerning pulp milis on the River Uruguay, judgment of 20 April. Para 1970, p.79.

(2) fredrik von Bothmer , op.cit, p.23

(3) Russel Buchan, cyber space, Non-state Actors and the obligations to prevent Transboundary Harm, journal of conglict and Security law, oxford university press, Vol.21, No (3), 2016, p.433.

فيما يتعلق بالبنى التحتية المعلوماتية والانشـطة المنبعثة من اراضـيها، او التي قد تدخل مجالها المعلوماتي ويكون القائم بتنفيذها جهات فاعلة غير حكومية[١].

ومن الجدير بالذكر أن عدم اســـتطاعت الدولة توظيف قدراتها الفنية في منع الهجوم المعلوماتي الذي ينشأ عنه الضرر العابر للحدود، لا ينهي التزامات الدولة حيث يمتد التزام الدولة يمنع الضـرر العابر للحدود لكي يغطي حالات عدم قدره الدولة على منع الضـرر، واشعار الدول التي سـوف تكون ضـحيه هذه الهجمات، وابداء المسـاعدة للدول لمنع هذا الضـرر أو الحد من اثاره الضارة[٢].

ثانياً : الالتزام بواجب كفاله الامتثال وضمان الاحترام

هناك التزام ايجابي يقع على الدولة والذي بموجبه يتعين عليها اتخاذ خطوات اسـتباقيه من شانها وضع حد للانتهاكات قواعد القانون الدولي الانساني، المرتكبة من اطراف النزاع فضلا عن حمل الطرف المعتدي للامتثال لقواعد القانون الدولي الانســـاني ، وواجب ضـــمان الاحترام يلزم الدولة بذل العناية اللازمة، والذي يعتمد مضـــمونها على ظروف محدده بما فيها مدى خطورة الانتهاك والوســـائل المتوفرة لدى الدولة وفق الحدود المعقولة، فضـــلاً عن درجه التأثير التي تمارســـها الدولة على اطراف النزاع والمســـؤولين عن هذه الانتهاكات[٣]، والدول باتت ملزمة بامتثالها لقواعد القانون الدولي الانسـاني، فقد حددت المادة الاولى المشـتركة من اتفاقيات جنيف الاربع لعام ١٩٤٩، المسـؤولية الدولية على النحو البارز الذي تلتزم بمقتضـاه الدول باحترام هذه الاتفاقية مع كفاله احترامها في جميع الاحوال والظروف[٤].

---

[١] د. لمى عبد الباقي واسراء نادر كيطان ، مصدر سابق، ص٣٥٠.

[2] Russell Buchan , op. cit , p445.

[3] Lindsey Cameron and others , the update comment on the first Geneve convention anew toll for generating forinter national humanitarian law , intern national review of the red cross, 2015 .no 900 p.1215

[٤] كريســتينا بيلانديني، كفاله الامتثال للقانون الدولي الانســاني على الصــعيد الوطني ، دور اللجان الوطنية للقانون الدولي الانسـاني واثارها ، الناشـر : المجلة الدولية للصـليب الاحمر، مختارات المجلة الدولية للصـليب الاحمر ،٢٠١٥ ،ص١٠٤٤.

كما اشـار البروتوكول الاضـافي الاول لعام ١٩٧٧ الى تعهد الاطراف السـامية المتعاقدة بالعمل، بصـــوره جماعيه ، أو فرديه، للعمل على كبح الانتهاكات الجســـيمة لاتفاقيات جنيف والبروتوكول الاضـــافي الاول، وبالتعاون مع الامم المتحدة و بما يتفق مع ميثاق الامم المتحدة لوقف هذه الانتهاكات[١].

على أية حال فأن نشـوء المسـؤولية الدولية يكون عند الفشـل في ممارسـه واجب العناية كضـــمان احترام القانون الدولي الانســـاني وقواعده، وعندما يثبت ان تلك الدولة لم تتخذ تدابير كافية لوقف الانتهاك ومنعه[٢].

وبتحليل ما تقدم أن نعتقد بأن هناك امكانيه تطبيق واجب العناية المتمثل بالتزام الدولة بكفالة احترام وضمان قواعد القانون الدولي الانساني وخصوصاً القواعد الامرة، وهذا الالتزام ينشا بمجرد حصـول علم الدولة بوجود انتهاكات احكام المادة الاولى المشـتركة من الاتفاقيات جنيف الاربع لعام ١٩٤٩، ومثال ذلك قيامها بتحريض الافراد بتنفيذ هجمات معلوماتية غير مشـروعه، أو تقوم بتسـهيل مهمة من يقوم بشـن هذه الهجمات على دولة اخرى باسـتخدام اسـلحه معلوماتية تهدف للإضـرار بالنظم المعلوماتية للدول المسـتهدفة، وأياً كانت الوسـائل المسـتخدمة في الهجوم المعلوماتي ، ويظهر جلياً امتثال الدولة لواجب العناية حالة قيامها بتحييد البنيه التحتية التي تنطلق منها الهجمات المعلوماتية، علاوة على ردع من يقوم بهذه الانشـطة ومعاقبته على انتهاك قواعد القانون الدولي الانساني ، وهذا يتمثل بالتزام الدولة الايجابي.

---

[١] ينظر نص المادة (٨٩) من البروتكول الاضافي الاول لعام ١٩٧٧.

[2] General for Global legal challenges , state responsibility for non-state actors that dettein in the course of NICE , yale law school December 7,2015,p.30.

المطلب الثاني

المسؤولية الجنائية الفردية الناشئة عن عدم الامتثال لواجب العناية

في ظل التطورات الحاصلة في تقنيه تكنولوجيا المعلومات والاتصالات، لم يعد الانسان وحده هو المسؤول عن الجرائم الناشئة عن المسؤولية الجنائية، فبعد تنامي دور الاشخاص المعنوية في العصر الحديث، واتساع دائرة نشاطها، عملت التشريعات الحديثة على اخضاع هذه الاشخاص الي معامله قانونيه من نوع خاص، لا سيما فيما يتعلق بأثارة المسؤولية الجنائية

وتثار المسؤولية الجنائية للفرد في حال قيامه بارتكاب افعال مجرمة بموجب القانون الدولي، أو انتهاكات جسيمه لقواعد واحكام القانون الدولي ، ولا يهم في هذا الامر سواء ارتكبت في هذه الافعال من قبل الفرد نفسه او ارتكبها بمساهمه غيره، وبالتالي يتم معاقبته بغض النظر عن الوصف الذي يشكله هذا الفعل في القانون الوطني، ولا يهم ان يكون مرتكب الفعل شخصا عاديا (مرؤوس) أم كان يتبوا منصباً قيادياً عالياً ك(رئيس دولة مثلاً)، وحيث ان الموضوع ذات اهمية ، سنقسم هذا المطلب على فرعين، نتناول في الفرع الاول ، المسؤولية الجنائية الفردية للفاعلين في الفضاء المعلوماتي ، وفي الثاني نتطرق الى المسؤولية الجنائية للقادة والرؤساء و على وفق الاتي:

الفرع الأول

المسؤولية الجنائية الفردية للفاعلين في الفضاء المعلوماتي

بعد نشوء فكرة المسؤولية الجنائية للفرد أضحى كل شخص يرتكب جريمة بحسب القانون الدولي يسأل عن فعله ويترتب عليه العقاب ، وهذا ما تضمنته اتفاقيه لاهاي لعام ١٩٠٧ ، حيث أشارت إلى أن الاطراف المتحاربة ستكون مسؤولة عن كل الافعال التي يرتكبها اشخاص ينتمون الى القوات المسلحة، اي امكانية مسألة الافراد عن الجرائم الدولية[١].

---

[١] يوسف حسن يوسف المسؤولية الجنائية لرئيس الدولة عن الجرائم الدولية ، منشأة المعارف ، الاسكندرية ، مصر ، ٢٠١١ ، ص٣٦.

وهذه المسؤولية تنشيء على عاتق ممثلي الدول سواء كانوا عسكرين أم سياسيين ، والذين يرتكبون جرائمهم باسـم الدولة او لحسـابها ، او الذين يقومون بانتهاكات جسـيمة للقانون الدولي الانســاني اثناء تنفيذهم للأعمال القتالية وادارتها[١]، وبعد الحرب العالمية الثانية شــهد القانون الدولي الجنائي تطورا كبيرا اثمر عن اقرار المســؤولية الجنائية للأفراد الطبيعيين عن الجريمة الدولية وخاصــه بعد محاكمات نورمبرغ وطوكيو، اذ اباحت تلك المحاكم القيام بأجراء محاكمات للزعماء بصــفاتهم افرادا، وتعتبر محاكمات الحرب العالمية الثانية نورمبرغ ، وطوكيو[٢]. هي سابقة ذات اهميه في مجال تدعيم مسؤوليه الفرد عن الجريمة الدولية[٣].

واســتنادا لأحكام محكمة نورمبرغ الدولية، فأن جرائم القانون الدولي هي التي لايرتكبها إلاّ الافراد، وليس الاشــخاص المعنوية، وبدون معاقبه هؤلاء الافراد الذين يرتكبون هذه الجرائم لا يمكن انفاذ احكام القضــاء الدولي الجنائي، وخصــوصــا ان القانون الدولي الجنائي اعترف بالمســؤولية الجنائية للفرد الذي ارتكب الجرائم الدولية، وهذا ما نصــت عليه بعض الاتفاقات الدولية، وكما هو الحال في الاتفاقيات الدولية لمنع ومعاقبة اباده الجنس البشـري لعام ١٩٤٩[٤]. وعند امعان النظر فيما تضــمنته محكمة نورمبرغ الدولية نجد أنها جاءت باحكام تفرض بموجبها الامتثال لقواعد القانون الدولي الانساني.

ومن الجدير بالذكر قد اشــارت اتفاقيات جنيف لعام ١٩٤٩، على انه " تتعهد الاطراف السـامية المتعاقدة بان تتخذ اي اجراء تشـريعي يلزم لغرض عقوبة جزائية فعاله على الافراد الذين يرتكبون او يأمرون بارتكاب احدى المخالفات الجسـيمة لهذه الاتفاقية، ويلتزم كل طرف بملاحقه

---

[١] د. نزار العنبكي ، القانون الدولي الانساني، ط١ ، دار وائل للنشر والتوزيع ، عمان ، الاردن ، ص٤٠١٠ ، ص٤٩٤.

[٢] علي عبد القادر الكهوجي، القانون الدولي الجنائي (اهم الجرائم الدولية)، المحاكم الدولية، منشـورات الحلبي، بيروت، ٢٠٠١ ، ص٢٦٠.

[٣] د. عبد الواحد محمد يوسف الفار، الجرائم الدولية وسلطه العقاب عليها، دار النهضة العربية، القاهرة ،١٩٩٥ ص١١٧.

[٤] د. محمد منصـور الصـاوي، احكام القانون الدولي المتعلقة بمكافحه الجرائم ذات الطبعة الدولية، دراسـة في القانون الدولي الاجتماعي، دار المطبوعات، الاسكندرية ، من دون سنه نشر ،ص١٤-١٥.

المتهمين بارتكاب مثل هذه المخالفات الجسيمة او الامر بارتكابها وتقديمهم للمحاكمة، أياً كانت جنسيتهم وله في سبيل ذلك اذا رغب، وطبقا لنصوص تشريعيه ، ان يسلمهم الى طرف متعاقد معني بمحاكمتهم ، مادامت تتوفر لدى الطرف المذكور ادله اتهام كافيه لأدانه هؤلاء الافراد".[١]

واكدت ديباجه نظام روما الاساسي للمحكمة الجنائية الدولية لعام ١٩٩٨ على "ان اخطر الجرائم التي تثير مخاوف لدى المجتمع الدولي باسره ، هي التي تمر دون عقاب، وانه يجب مقاضاة مرتكبيها على نحو فعال من خلال اتخاذ تدابير على الصعيد الوطني ، وكذلك من خلال تعزيز التعاون الدولي"، ونصت المادة (٢٥/ ٢) من النظام الاساسي للمحكمة على المسؤولية الجنائية الفردية، حيث قررت ان " الشخص الذي يرتكب جريمة تدخل في اختصاص المحكمة يكون مسؤول عنها بصفته الفردية وعرضه للعقاب على وفق هذا النظام الاساسي، وفي الحقيقة ان المسؤولية الجنائية الدولية للفرد تحتاج بصوره اصليه الى ارتكاب جريمة دولية، اي ان المسؤولية الفرد الجنائية تنهض سواء التصرف بصفته الشخصية ام لحساب شخص اخر من اشخاص القانون الدولي[٢].

اما عن كيفية ارتكاب الافعال التي تنشا عنها المسؤولية الجنائية الفردية في سياق الهجمات المعلوماتية، فقد تطرق لها دليل تالين، الاصدار الثاني لعام ٢٠١٧، في مادته (٨٤) ذات الصلة بالمسؤولية الجنائية الفردية عن العمليات المعلوماتية التي تشكل جرائم حرب او الانتهاكات الجسيمة لقواعد القانون الدولي الانساني التي تضمنتها المواد (٥٠، ٥١، ١٣٠، ١٤٧) من اتفاقيات جنيف الاربع لعام ١٩٤٩ على التوالي[٣]، كذلك ما جاء في احكام المادة (٨٥) من البروتوكول الاضافي الاول لعام ١٩٧٧ [٤]، فضلاً عن الجرائم المذكورة في المادة (٨)

---

[١] ينظر المواد (٤٩، ٥٠، ١٢٩ ، ١٤٦) من اتفاقيات جنيف الاربعة المعقودة في ١٢ اب ١٩٤٩، الاولى، الثانية، والثالثة، والرابعة.

[٢] د. طارق عبد العزيز حمدي ، المسؤولية الدولية الجنائية والمرتبة عن جرائم الإرهاب الدولي ، مصر ، دار الكتب القانونية ، ٢٠٠٨ ، ص١٨٧.

[٣]ينظر المواد (٥٠ ، ٥١ ، ١٣١ ، ١٤٧) من اتفاقيات جنيف الاربع لعام ١٩٤٩.

[٤] ينظر نص المادة (٨٥) من البروتوكول الاضافي الاول لعام ١٩٧٧.

من نظام روما الاساسي للمحكمة الجنائية الدولية ١٩٩٨[١]. ونستدل من ذلك على ان جميع الافعال المنصوص عليها في المواد انفه الذكر يمكن ارتكابها بأسلحة معلوماتية تشكل جرائم حرب، وبالتالي تنطبق عليها قواعد القانون الدولي الانساني، باعتبارها وسيله او اسلوب حديث من الوسائل والاساليب المستحدثة في الحرب[٢].

ومن الجدير بالذكر ان المسؤولية الجنائية الفردية يمكن ان تتحقق في أحدى الحالات الاتية :-

اولاً – قيام احد الافراد بأحداث أضرار بالغة بأرتكابه جريمة اتلاف الانظمة المعلوماتية لدولة معينة باستخدام الحاسوب والاعتداء على المعطيات المخزونة داخل ذاكرة الحاسوب الرئيسية ، والثانوية لدولة أخرى وهي تتم اما عن طريق التدخل المباشر بصورة غير مشروعة في أنظمة الحاسوب ، أو عن طريق الاختراق باستخدام الشبكة العنكبوتية (الانترنت)[٣].

ثانياً: قيام أحد الارهابيين بصناعة فايروسات، ذات نوعية نشطة ونشرها داخل أنظمة الحاسوب لدولة معينة، لغرض أحداث اضراراً بالاجزاء المنطقية للحاسوب، وبالتالي تنشئ المسؤولية الجنائية الفردية عن هذا الفعل الذي ارتكب بدوافع قد تكون ايديولوجية معادية[٤].

وعلى الرغم من ازدياد الانشطة المعلوماتية التي تثير مسؤولية الجاني الفردية، إلا إذ هناك رأي يرى استبعاد المسؤولية الجنائية الفردية لمن يستخدم هذهِ الاسلحة المعلوماتية للأسباب الآتية:

---

[١] ينظر نص المادة (٨) من نظام روما الاساسي للمحكمة الجنائية الدولية س ١٩٩٨.

[2] see : Micheal .N. Schmitt, Tallinn Manuel 2017 , op . Cit, rule 48

[٣] يمامة خضير الحربي ، جوانب قانونية في الحكومة التكنلوجية للانترنت ، مجلة كلية القانون الكويتية العالمية ، س (٦) ،ع (٤)، الكويت ، ٢٠١٨ ، ص٥٧.

[٤] حسن طاهر داود، أمن المعلومات، مطابع اكاديمية نايف للعلوم الأمنية، الرياض، السعودية، ١٩٩٧، ص٣.

١- أن الفرد الذي يقوم بتطوير نظام اسلحة معلوماتية مستحدثة يكون بعيداً عن مسرح الجريمة، ومن ثم لا يستطيع التحكم بتصرف السلاح، أي أن عملية ضع القرار ستكون هي نتيجة حتمية لبيئة مفتوحة وغير منظمة[١].

٢- ربما يكون البرنامج الذي يعمل بواسطته السلاح المعلوماتي تم منعه أو تصميمه من قبل أكثر من شخص واحد، وبالتالي قد يعقد جانب المسؤولية[٢].

الفرع الثاني

المسؤولية الجنائية الفردية للقادة والرؤساء

يتوجب على الأشخاص الذين يشغلون مناصب ذات سلطة عليها، إلزام الآخرين للقيام بمنع مرؤوسيهم والخاضعين لأوامرهم بأية أفعال تشكل انتهاكاً لقواعد القانون الدولي الإنساني، وإلا فإنهم يكونوا خاضعين للمسائلة والمحاكمة بعدم الإلتزام بذلك[٣].

وقد تم ترسيخ مبدأ مسؤولية القادة والرؤساء الجنائية في الفقرة (٢) من المادة (٨٦) من البروتوكول الاضافي الأول لعام ١٩٧٧، التي نصت على :" لا يعفى قيام أي مرؤوس بأنتهاك الاتفاقيات وهذا الملحق البروتوكول" رؤساء من المسؤولية الجنائية أو التأديبية، حسب الأحوال اذا علموا، أو توافرت لديهم معلومات تتيح لهم في تلك الظروف، أن يخلصوا إلى أنه كان

---

(1) Naha jian, Human Mwchine inter national in Terms of Various Degress of Autonomy as well as political and Legal Responsibility for Actions of Autonomous system federal Foreign office, p.145.

(2) Jarna Petman , Autonomous weapons system and inter national Humanitarian Law – out of the loop, Faculty of law, university do Helsinki, publisher by Erik Castre'n institute of inter national law and Human Rights , 2017, p.32.

(٣) محمد يوسف علوان، اختصاص المحكمة الجنائية الدولية، مجلة الأمن والقانون، أكاديمية شرطة دبي، ع (١)، ٢٠٠٢، دبي، ص١٦٧.

يرتكب، أو أنه في سبيله لارتكاب مثل هذا الانتهاك، ولم يتخذوا كل ما في وسعهم من احتياطات مستطاعه لمنع أو قمع هذا الانتهاك[١].

علاوةً على ذلك فقد أشـــارت الفقرة (١) من المادة (٨٧) من ذات البروتوكول على أنه " يتعين على الأطراف الســـامية المتعاقدة وعلى أطراف النزاع أن تكلف القادة العســـكريين بمنع الانتهاكات للاتفاقيات ولهذا الملحق "البروتوكول" وإذا لزم الأمر بقمع هذه الانتهاكات وإبلاغ السلطات المختصة عنها، وذلك فيما له صلة بأفراد القوات المسلحة الذين يعملون تحت امرتهم وغيرهم ممن يعملون تحت اشرافهم[٢].

وبتحليل ما جاء بنص أحكام المادتين أعلاه نجد أن المسؤولية الجنائية الفردية تترتب على القادة والرؤســـاء اذا لم يقوموا بأعمالهم وواجباتهم المناطة بهم، واهمها اتخاذ التدابير المناســـبة والاحتياطات المســـتطاعة في إطار علاقاتهم وبحكم مناصـــبهم لمن هم أدنى منهم رتباً ، وهذا الإلتزام يتخذ صورتين:

الصـــورة الأولى هي **(التزام المنع)** وهو إجراء وقائي يتمثل ببذل عناية القائد العســـكري والسيطرة على مرؤوسية ، أما الصورة الثانية فهي إلتزام ذا **(طابع عقابي)**، يلزم القادة والرؤساء معاقبة مرؤوسيهم الذين ينتهكون قواعد القانون الدولي الإنساني.

أما المحكمة الجنائية الدولية قد أكدت على مبدأ مســؤولية القادة والرؤســاء عندما تناولته الفقرة (١) من المادة (٢٧)من نظامها الأساسي في مبدأ "عدم جواز الاعتداء بالصفة الرسمية لدفع المسؤولية" واوضحت إن نظامها الأساسي يخضع له جميع الأشخاص من دون استثناء ، ســواء كان هذا الشــخص رئيس دولة، أم من هم أدنى منه وظيفة ، والصــفة الرســمية لا تعفي مرتكب الجرائم التي تترتب عليها المســـؤولية الجنائية الفردية وفي جميع الظروف والاحوال، بل

---

[١] البروتوكول الاضافي الأول لعام ١٩٧٧.

[٢] البروتوكول الاضافي الأول لعام ١٩٧٧.

وحتى إن الصفة الرسمية التي يتمتع بها الشخص لا يمكن أن تكون سبباً في تخفيف العقوبة عنه[١].

وجاءت المادة (٢٨) من نفس النظام الأساسي للمحكمة الجنائية الدولية لتؤكد مرة أخرى أهمية هذا المبدأ تحت عنوان "مسؤولية القادة والرؤساء الآخرين" إذ أشارت إلى الأسباب الأخرى للمسؤولية الجنائية عن الجرائم التي تكون داخلة في اختصاص المحكمة في سياق مسؤولية القائد عن أعمال مرؤوسيه، إذا ما علم القائد ذلك، أو تجاهل القائد عن وعمد أن قواته على وشك ارتكاب إحدى هذه الجرائم أو إن قواته قامت بارتكاب هذه الجرائم ، ولم يقم باستخدام سلطته لمنع هذه الجرائم أو حتى عرضها على السلطات المختصة للتحقيق والمقاضاة لمعاقبة مرتكبي هذه الأفعال[٢].

ولذلك يتوجب على القائد العسكري أن يؤسس لنظام فعال لجمع وتقسيم المعلومات الاستخبارية ذات الصلة بالاهداف المحتملة، وعليه يقع واجب ارشاد وتوجيه قواته العسكرية لاستخدام الوسائل التقنية لتحديد الأهداف بصورة صحيحة خلال العمليات العسكرية وذات الأمر ينطبق على الهجمات المعلوماتية ، من حيث ضرورة توافر المعلومات الموثوقة بشأن الأهداف المحتملة وهذه تدخل ضمن مهام فريق خبراء (الحاسوب) ، وبالتالي فإن مراعاة الاحتياطات المستطاعة في السياق المعلوماتي تتضمن جمع المعلومات الاستخبارية من الشبكة المعلوماتية ، من خلال وضع خريطة لتلك الشبكة المستهدفة ، على أن الإجراءات غير المستطاعة لا تدخل ضمن هذا الالتزام، إذ يكون من غير الممكن وضع مخطط لشبكة نظام معلوماتي على سبيل المثال ، لأن القيام بذلك يؤدي إلى كشف العملية العسكرية المزمع القيام بها ، وبالتالي باستطاعة الإجراءات الدفاعية المعلوماتية للطرف الخصم التصدي لها وعليه فإن هذا الالتزام لا يعد واجباً ، أما عند عدم قدرة المهاجم من جمع المعلومات الموثوقة بشأن طبيعة ذلك الهدف ، فإن على

---

[١] ينظر نص المادة (٢٧) الفقرة (١) من نظام روما الأساسي للمحكمة الجنائية الدولية لعام ١٩٩٨.

[٢] ينظر نص المادة (٢٨) من نظام روما الأساسي لعام ١٩٩٨.

القائد العســـكري أو المســـؤول عن اتخاذ القرار الالتزام بتقييد نطاق الهجوم على أجزاء النظام المعلوماتي الذي تتوافر بخصوصه المعلومات اللازمة[١].

يتضــح مما تقدم، أن القادة العسـكريين مسـؤولون عن السـلوك الصــادر عن أفراد القوات المسـلحة ، وغيرهم من الأشـخاص العاملين تحت اشـرافهم في حال عدم إتخاذ القادة الإجراءات اللازمة لمنع أو قمع مثل هذه الجرائم.

ومع زيـادة التقدم العلمي والتكنولوجي فقد ذهـب البعض إلى القول بـأن الجيل الثـاني من الأسـلحة في الترسـانة العسـكرية ، هي الآت قادرة على اختيار أهداف محددة وتدميرها من دون تدخل بشـــري آخر ،الأمر الذي يؤدي إلى ازدياد احتمالية تعرض القائد العســـكري للمســـؤولية الجنائية الفردية في حال تم انتهاك قوانين وأعراف الحرب[٢].

ويلتزم كل قائد عسـكري بخطط للهجوم أو يتخذ قراراً بشـأنه أن يضـع في حسـابه جميع الاحتياطات التي أشـارت إليها المادة (٥٧) من البروتوكول الإضـافي الأول سـالف الذكر ومن ذلك الامتناع عن اتخاذ أي قرار بشـن هجوم قد يتوقع منه أن يسـفر عن إلحاق أضـرار بالاعيان المدنية بصـورة عرضـية، ففي سـياق الهجمات المعلوماتية، أورد دليل تالين قاعدة عامة بشـأن المسؤولية الجنائية للقادة والرؤساء في حال اعطائهم الأوامر للقيام بتلك الهجمات التي ترقى إلى جرائم حرب هو أن يكون القائد العسكري قد علم أو كان على يفترض به أن يكون قد علم بسبب الظروف السائدة في ذلك الوقت ، بأن القوات ترتكب أو تكون على وشك إرتكاب هذه الجرائم ولم يتخذ جميع التدابير اللازمة والمعقولة وفي حدود ســـلطته لمنع أو قمع إرتكاب هذه الجرائم او لعرض المسألة على السلطات المختصة للتحقيق والمقاضاة[٣].

كما أن المسـؤولية تمتد إلى كل من القائد العسـكري أو الرئيس المدني ومثال ذلك الرئيس المدني في دوائر الأمن أو الاســتخبارات المدنية الذي يتحمل المســؤولية الجنائية عن الهجمات

---

[١] سراب ثامر أحمد ، مصدر سابق ، ص٢٦٦-٢٦٧.

[٢] د.لمى عبد الباقي محمود العزاوي، و دعاء جليل حاتم، الذكاء الاصطناعي والمسؤولية الجنائية الدولية، مجلة المفكر ، ع (١٨) ، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر ، ٢٠١٩، ص٣٣.

[3] Tallinn Manual , Rule 24, p.80

المعلوماتية التي ترقى إلى جرائم حرب في سـياق النزاع المسـلح الدولي وغير الدولي والتي تتميز بالتعقيد التكنولوجي الذي يصـعب معه إمكانية علم القادة بهذه الجرائم مقارنة بالعمليات العسكرية التقليدية إلا أن ذلك لا يمكن عده عذراً مخففاً من مسؤوليتهم في مباشرة السيطرة على مرؤوسيهم، فالجهل بمثل تلك العمليات لا يعد عذراً ، لأن القانون يفترض في كل قائد عسـكري تمنعه بدرجة من العلم الذي يتسـع به الرجل المعتاد بذات المسـتوى القيادي وفي سـياق عمليات متشـابهه وبما يعد كافياً لقدرتهم من القيام بواجباتهم وعلى نحو معقول بهدف تشخيص أو منع أو إيقاف ارتكاب جرائم الحرب المعلوماتية[١].

[١] سراب ثامر أحمد ، مصدر سابق ، ص٢٨٦.

الخاتمة

خلصنا في هذه الدراسة إلى أن الهجمات المعلوماتية يمكن عدّها أحد وسائل القتال المستحدثة والتي تستخدم في سياق النزاعات المسلحة، من خلال تنفيذها عبر الفضاء المعلوماتي الذي أصبح ميداناً جديداً للقتال، وعلى الرغم من عدم وجود اتفاقيات دولية صريحة تنظم هذه الهجمات في اطار قانوني ملزم إلا أن الباحثين في الشأن القانوني والخبراء الدوليين بذلوا جهود حثيثة لتوفير غطاء قانوني يمكن من خلاله تطبيق قواعد ومبادئ القانون الدولي الإنساني على تلك الهجمات.

غالباً ما تقوم الدول بممارسة حقوقها السيادية ضمن اقليمها وولايتها القضائية إلا أنه قد يؤدي تعسفها باستعمال هذا الحق إلى الأضرار بحقوق الدول الأخرى المجاورة ، مما ادت الحاجة إلى ظهور مبدأ واجب العناية الذي يقتضي بموجبه التزام الدول بعدم السماح باستخدام اراضيها بأنشطة غير مشروعة ماسة بحقوق الدول الأخرى ويقع التزام الدول بموجب مبدأ واجب العناية بالامتثال لقواعد ومبادئ القانون الدولي، وهذا الواجب هو معيار لسلوك الدول ، إذ أن الدول ليست معنية بتحقيق نتيجة معينة، إلا أن أي خرق لهذا الواجب يثير المسؤولية الدولية عن الفعل غير المشروع الصادر من الدولة المعتدية.

وتبعاً لذلك قد توصلنا إلى عدة استنتاجات ومقترحات وعلى النحو الآتي :-

أولاً: الاستنتاجات

١- إن استخدام مصطلح المعلوماتية، هو المصطلح الذي يعد اكثر انسجاماً للدلالة على مفهوم هذهِ الهجمات، فهناك من درج على تسميتها بالسيبرانية، أو الالكترونية، وذلك لعدم ورود هذهِ المصطلحات في معاجم اللغة العربية بصورة صريحة، على الرغم من أن المصطلحات الأخرى سالفة الذكر قد تم استخدامها من قبل الفقه الدولي، وبعض الدراسات الدولية الصادرة بهذا الشأن، ولاقت رواجاً لدى المهتمين بالشأن القانوني.

٢- اختلف الفقه الدولي حول مسألة تكييف الهجمات المعلوماتية، فعلى الرغم من عدّ الهجمات المعلوماتية المصاحبة للنزاع المسلح، بأنها نزاعات خاضعة للقانون الدولي الإنساني، إلاّ إن

جانب أخر من الفقه لم يتقبل فكرة خضـــوع الهجمات المعلوماتية لقواعد ومبادئ القانون الدولي الإنســاني في وقت السـلم، ومدى إمكانية تطبيق الاسـتثناءات الواردة عليها في المادة (٢/رابعاً) الخاصـــة بحظر اســتخدام القوة أو التهديد بها في العلاقات الدولية، كذلك المادة (٥١) من ذات الميثاق المتعلقة بأستخدام حق الدفاع الشرعي لمواجهة تلك الهجمات.

٣- على الرغم من عدم النص بصـــورة صـــريحة على الهجمات المعلوماتية في المعاهدات والاتفاقيات الدولية وباقي الصـــكوك الدولية، إلاّ إن غياب هذهِ النصـــوص لم يكن مانعاً من معالجتهاو الآثار الناشئة عنها، فهناك مجموعة من القواعد القانونية الدولية، سواء كانت مقننة أو عرفيـة، علاوة على الكثير من الإجتهـادات القضـــائيـة التي يمكن تطويعهـا على الهجمـات المعلوماتية، وهناك الكثير من الشواهد، بهذا الصدد أهمها القرارات القضائية الصادرة من المحاكم الدولية المختصة.

٤- إن الهجمات المعلوماتية هي أحد وسـائل القتال المسـتحدثة التي أضـحت الدول تتسـارع في اللجوء إليها بالنزاعات الحديثة، ومع إمكانية خضـــوعها لأحكام المادة (٣٦) من البروتوكول الاضـــافي الأول لعام ١٩٧٧، فأن الدول باتت ملزمة بإجراء مراجعة قانونية لمثل اســتخدام هذهِ الأســـلحة المعلوماتية، ومدى مطابقتها مع معايير القانون الدولي الإنســـاني، وينبغي عدم أثارة مسألة عدم خضوع هذهِ الأسلحة المعلوماتية لتلك المعايير بحجة غياب القواعد المنظمة للهجمات المعلوماتية.

٥- لقد أصبح الفضاء المعلوماتي مجالاً نشطاً للدول والفاعلين من غير الدول لممارسة الانشطة المعلوماتية، وما يتميز به هذا الفضـــاء من خصـــائص فريدة، يكون من المرجح معه أن تحدث الهجمات المعلوماتية آثاراً سـلبية على البنية التحتية المعلوماتية للدول المحايدة، وبالتالي تشـكل هذهِ الانشطة خرقاً لواجب الحياد المعلوماتي، يلزم اطراف النزاع بمنع تنفيذ مثل تلك الهجمات من داخل اقليم الدولة المحايدة، أو محاولة إخضـاع تلك البنية التحتية لسيطرة المهاجمين واستخدامها لاغراض غير ســـلمية، ويقع ذات الالتزام ايضـــاً على دولة الحياد بالامتناع عن الســـماح او التغاضـي بشـن هجمات وبعلم منها عند انطلاقها من البنى التحتية المعلوماتية العائدة لها وعليها اتخاذ تدابير الوقاية والمنع لردع تلك الهجمات الضارة.

٦- تم تصنيف الهجمات المعلوماتية وخضوعها لمعايير محددة تم طرحها من قبل المختصين في الشأن القانوني، فعلى وفق معيار التماثل مع الهجمات التقليدية تعد الهجمات المعلوماتية بمثابة استخدام للقوة عند قدرة هذهِ الهجمات أحداث آثار مشابهة لتلك الآثار التي تحدثها الهجمات التقليدية، أما استناداً لمعيار المسؤولية المتشددة فأنه يعد أي هجوم يستهدف البنية التحتية للدولة المعتدى عليها استخداماً للقوة، بينما ووفقاً لمعيار الحجم والآثار ينظر إلى الهجمات المعلوماتية بأعتبارها استخداماً للقوة متى ما كانت بحجم العمليات التقليدية وآثأرها التي تصل لمستوى استخدام القوة.

٧- بعد أن كانت المفهوم التقليدي للسيادة مطلقاً، إلا إن هذا المفهوم لم يعد له وجود اليوم، بسبب الكثير من المتغيرات التي طرأت على هذا المفهوم، فضلاً عن التطورات العلمية والتكنولوجية، مما سبب أن يواجه هذا المفهوم العديد من المشكلات القانونية، منها ظهور مفهوم السيادة المعلوماتية، وهو مفهوم حديث النشأة، هذهِ السيادة التي فرضت على الدول التعامل مع الهجمات المعلوماتية التي يتم تنفيذها عبر الفضاء المعلوماتي وهي هجمات متعددة الأنواع والوسائل، مما يستوجب على الدول بذل العناية اللازمة في مراقبة هذهِ الانشطة والسيطرة والتحكم بالانظمة التكنولوجية، ونظم الاتصالات، وغالباً ما تحدث انشطة معلوماتية بصورة غير مشروعة يترتب عليها العديد من الجرائم المعلوماتية.

٨- أن الفقرة (٤) من المادة (٢) من ميثاق الأمم المتحدة تمتاز بمرونتها الكافية لإستيعاب أو تكييف الهجمات المعلوماتية وما ينشئ عنها من آثار مادية ملموسة تكون ذات الآثار الناجمة عن استخدام القوة العسكرية بمعناها التقليدي، ومع ذلك لا يوجد إجماع بشأن تحديد المستوى الدقيق الذي يمكن من خلاله تصنيف الهجمات المعلوماتية كأستخدام للقوة على وفق ما ورد في المادة آنفة الذكر.

٩- إن القواعد التي تضمنها (دليل تالين)، ذات الصلة باستخدام الفضاء المعلوماتي كوسيلة حرب، لم ترقَ لحد الأن إلى مرتبة القواعد الدولية الملزمة، ومن الممكن أن تكتسب الصفة الالزامية إذا ما تحولت تلك القواعد إلى قواعد عرفية، أو وضعها بصيغة اتفاقية دولية ملزمة.

١٠- تجسد الحقوق المعلوماتية مظهراً بارزاً وتعكس مدى تطور حقوق الإنسان في سياق القانون الدولي لحقوق الإنسان.

١١- هناك تنوع في وسائل وإشكال الأسلحة المعلوماتية مثل اطلاق الفيروسات والبرامج الضارة والمدمرة للأنظمة، والشبكات الحاسوبية، فضلاً عن اختراق حسابات وسرقة معلومات سرية ونشرها، وقد تكون هذهِ المعلومات تتعلق بأنظمة المعلومات العسكرية والأمنية، كما يوجد هناك تنوع في المواقع المستهدفة بواسطة الهجمات المعلوماتية، فهي لا تقتصر على مواقع عسكرية فحسب، بل مواقع مدنية، وأخرى خدمية وصناعية.

١٢- يعتمد مفهوم المشاركة المباشرة في العمليات العدائية على ثلاث عناصر أساسية، وهذهِ العناصر تشتمل على: هو حصول الضرر، والذي يؤثر بصورة سلبية في القدرات العسكرية للطرف الأخر الذي يتعرض لهجمات معلوماتية وبالتالي يؤدي إلى إلحاق اضرار جسيمة في منشأته العسكرية، والعنصر الأخر هو العلاقة السببية ذات الأثر المباشر وهي حلقة الوصل بين فعل الاعتداء وبين الضرر الناشئ عن ذلك الفعل، أما العنصر الأخر فهو الارتباط بالعمل الحربي، الذي يشترط فيه ارتباطه بصورة مباشرة بالأعمال العدائية الحاصلة بين طرفي النزاع.

١٣- إن من أهم التزامات واجب العناية اللازمة في سياق القانون الدولي الإنساني هي الالتزام باتخاذ تدابير وقائية، إذ يجب على الدول القيام بها في وقت السلم واثناء النزاع المسلح، وتعد المادة الاولى المشتركة لاتفاقيات جنيف الاربع لعام ١٩٤٩ والمادة (١/ثانياً) من البروتوكول الاضافي الأول هي تجسيد لضمان احترام قواعد القانون الدولي الإنساني.

١٤- هناك التزام على الدول يتمثل بواجب العناية اللازمة بعدم إلحاق اضراراً بالدول الأخرى المجاورة عند ممارستها لحقوقها السيادية وهو واجب عدم الاضرار وقد اكدت محكمة العدل الدولية الطبيعية العرفية لهذا المبدأ، والتي كانت اغلب تطبيقاته في سياق القانون الدولي البيئي، إذ نص قرار المحكمة في قضية قناة كورفو عام ١٩٤٩، على التزام الدول بعدم السماح من علم لاستخدام اقليمها في أعمال تتعارض مع حقوق الدول الأخرى، وبالتالي تؤدي إلحاق اضرار عن طريق التلوث البيئي الناجم عن الالغام، وهذا الحكم من الممكن أن يستوعب الهجمات المعلوماتية الضارة التي ينشأ عنها كما هو الحال عند الهجوم المعلوماتي عند الاستخدام المفرط للرسائل

المعلوماتية داخل الفضـــاء المعلوماتي التي تعد شـكل من اشـكال تلوث المعلومات فضـــلاً عن هجمات رفض الخدمة المعلوماتية(DDos).

١٥- تم التأكيد على الاســـاس القانوني لواجب عدم الاضـــرار في المبدأ (٢١) من إعلان اســـتكهولوم لعام١٩٧٢ ، والمبدأ (٢) من إعلان ريو لعام ١٩٩٢. وقد اشـــارت تلك المواد إلى الالتزام بمنع جميع الاضرار البيئية العابرة للحدود.

١٦- يعد واجب العناية اللازمة للدول هو بمثابة التزام ســـلوك وليس التزام بتحقيق نتيجة، وفي هذه الحالة لا يوجد التزام مطلق في تحقيق النتيجة الملزمة لها، فالدولة مطالبة فقط وفقاً لهذا الالتزام اتباع الوسائل الملائمة الكافية وبذل اقصى الجهود الممكنة في سبيل منع الضرر الذي يستهدف دولة آخرى وينطلق من أراضيها.

ثانياً: المقترحات

١- الدعوة إلى إنشـــاء هيئة دولية مســـتقلة لتقصـــي الحقائق تتولى معالجة القيود التي يواجها القانون الدولي في تنظيم اســـتخدام الهجمات المعلوماتية وتنفيذها وتعمل على إدارة الأزمات الناشئة عن الأنشطة المعلوماتية والعمل على أجراء تحقيق دولي مستقل وبيان المسؤولية حول تلك الهجمات، وتتولى أحد أجهزة الأمم المختصـــة الاليات القانونية في إنشـــائها وتنظيم عملها وتحديد عدد اعضائها.

٢- إن مســألة تنظيم الهجمات المعلوماتية هي من مســألة ذات اهمية على المســتوى الدولي، وحيث أن التنظيم الدولي المعاصـر يفتقر إلى اتفاقية دولية ملزمة تنظيم هذهِ الهجمات، عليه من المهم الدعوة إلى عقد اتفاقية دولية جماعية. تتولى تنظيم تلك الهجمات ووضـــع الاطر القانونية اللازمة لكبح جماح الانشـطة المعلوماتية الضـارة، ومن الممكن أن يكون دليل تالين على الرغم من عدم إلزامية دليلاً مرجعياً من خلال تبني القواعد الواردة فيه من قبل الدول لحماية أمنها المعلوماتي من مخاطر الهجمات المعلوماتية.

٣- نأمل تعديل النظام الاساس للمحكمة الجنائية الدولية الذي تم وضعه في اوقات وظروف لم تكن الهجمات المعلوماتية قائمة أنذاك لجعله يســتوعب جميع الهجمات المعلوماتية بكافة أنواعها

ووسائل استخدامها أو ملاحقة مرتكبها، وتحميلهم المسؤولية الجنائية الفردية سواء كانوا قادة أم رؤساء وفرض العقوبات المخصصة لكل جريمة دولية مثل الجرائم ضد الانسانية وجرائم الإبادة الجماعية وجرائم العدوان.

٤- مساعدة الدول النامية والسعي لتطوير قدراتها المعلوماتية بما يدعم أمنها المعلوماتي ودرء الاخطار التي تتعرض لها منشأتها وبنيتها التحتية.

٥- ضرورة قيام الأمم المتحدة بدعوة الدول الأعضاء وحثها على استخدام فضائها المعلوماتي للأغراض والأنشطة السلمية حصراً، والكف عن استخدامها لأغراض غير مشروعة دولياً، تؤدي إلحاق اضراراً جسيمة بالدول الأخرى وبالتالي تهدد السلم والأمن الدوليين.

٦- يتوجب على الدولة المعتدى عليها، قبل استخدام حقها في اللجوء إلى التدابير المضادة، ان تقوم بأخطار الدولة المعتدية والطلب منها بأن تكف عن فعلها غير المشروع بأستخدام الهجمات المعلوماتية، واشعارها بضرورة الوفاء بالتزاماتها الدولية وأن تقوم بعرض التفاوض عليها قبل البدء بتنفيذ التدابير المعلوماتية المضادة.

٧- تشكيل جهاز دولي من قبل الأمم المتحدة يتولى فحص مشروعية التدابير المضادة التي تلجأ إليها وفرض رقابة سابقة على التدابير المضادة المعلوماتية وأن تسعى لجعلها في اطارها الشرعي، لأن هذهِ التدابير هي استثناء من الأصل الذي لا يبيح الفعل غير المشروع، ولا يجوز التوسع باستخدام الاستثناء.

٨- حث الدول على تبني استراتيجية وقائية لحماية أمنها المعلوماتي على غرار تجارب بعض الدول كالولايات المتحدة وروسيا الاتحادية، والصين، فضلاً عن إنشاء مراكز خاصة تتبنى عملية الدفاع المعلوماتي لغرض منع تلك الهجمات المعلوماتية أو ألحد منها على أقل تقدير.

٩- دعوة المشرع العراقي إلى وضع تشريعات توفر الغطاء القانوني الذي يحد من استخدام الفضاء المعلوماتي بصورة غير مشروعة على أن تكون هذه التشريعات كافية ومرنة تستوعب جميع المستجدات الناشئة عن تطور تكنولوجيا المعلومات والاتصالات.

١٠- حث الدول ذات القدرات التكنولوجية المتطورة على الحد من انتاج الأسلحة المعلوماتية أو تقييد استخدامها بالقدر اللازم الذي لا يؤثر على حقوق الدول الأخرى نتيجة الاضرار الناشئة عنها.

١١- نأمل من منظمة الأمم المتحدة توجيه الدعوة لجميع الدول من أجل الامتثال لواجب العناية اللازمة وعدم الاضرار بالدول الأخرى المجاورة سواء كان في سياق القانون الدولي للبيئة، أو القانون الدولي الإنساني أو القانون الدولي لحقوق الإنسان المعلوماتية، خصوصاً إذا ما عملنا إن مفهوم عدم الامتثال مفهوم مرن ومبهم في ذات الوقت ولم يتعرض الفقه الدولي لتعريفه بصورة دقيقة وانما هناك بعض الاجتهادات الفقهية في سياق الاضرار البيئية، وبعض الاتفاقيات ذات الصلة بالقانون البيئي.

١٢- دعوة الجامعات والمعاهد القانونية العراقية إلى تضمين مادة الأمن المعلوماتي ضمن مناهجها القانونية، والتي تعنى بدراسة الهجمات المعلوماتية والعمليات المعلوماتية الاخرى والتجسس المعلوماتي وبيان وسائل الحماية منها والتصدي لمخاطرها واضرارها على البنى التحتية للبلاد.

١٣- حث الدول على تسوية منازعتها الدولية ذات الصلة بالانشطة المعلوماتية التي تعرض السلم والأمن الدوليين للخطر، بالطرق السلمية وبما يتفق مع ما تضمنه ميثاق الأمم المتحدة من مبادئ وأهداف.

قائمة المصادر

أولاً: الكتب

١. ابو الخير احمد عطية، حماية السكان المدنيين والاعيان المدنية أبان النزاعات المسلحة، دراسة مقارنة، دار النهضة العربية، القاهرة، ١٩٩٨.

٢. د.احسان هندي، مبادىء القانون الدولي العام في السلم والحرب، ط١، دار الجليل للطباعة والنشر ، دمشق ، ١٩٨٤.

٣. د.أحمد حلمي ابراهيم، الدبلوماسية البروتوكول- الأتيكيت، المجاملة، القاهرة، دار عالم الكتب، من دون تاريخ نشر.

٤. اسلام دسوقي عبد النبي دسوقي ، النظرية العامة للمسؤولية الدولية بدون خطأ، المسؤولية الدولية الموضوعية ، ط١، مركز الدراسات العربية ، القاهرة ، مصر ، ٢٠١٦.

٥. د.اسماعيل صبري مقلد، اصول العلاقات الدولية في اطار عام ، ط١، دار النهضة العربية ، القاهرة، ٢٠٠٧.

٦. د.اشرف السعيد احمد، القرصنة الالكترونية، دار النهضة العربية، القاهرة، ٢٠١٣.

٧. السيد ابو عيطة، الجزاءات الدولية بين النظرية والتطبيق، مؤسسة الثقافة الجامعية، الاسكندرية، ٢٠٠١.

٨. الفن توفلر، تحول السلطة بين العنف والمعرفة، ترجمة فتحي بن شنوان ،الدار الجماهيرية للنشر والتوزيع والإعلام، ليبيا، ١٩٩٢.

٩. د.اياد يونس محمد الصقيلي، الحظر الدولي في القانون الدولي العام، دراسة قانونية، دار الفكر الجامعي، الاسكندرية، مصر ، ٢٠١٤.

١٠. د.ايهاب خليفة ،القوة الالكترونية ، كيف يمكن أن تدير الدول شؤونها من عصر الانترنت ؟ " الولايات المتحدة الامريكية انموذجاً " ، ط١ ، دار العربي للنشر والتوزيع ، القاهرة ، ٢٠١٧.

١١. د.ايهاب خليفة، مجتمع ما بعد المعلومات، تأثير الثورة الصناعية الرابعة على الأمن القومي ، ط١، العربية للنشر والتوزيع، ٢٠١٩.

١٢. د.ايهاب خليفة، الحرب السبيرانية، الاستعداد لقيادة المعارك العسكرية في الميدان الخامس، ط١، دار العربي للنشر والتوزيع، القاهرة، ٢٠٢١.

١٣. د.بشير جمعة عبدالجبار الكبيسي، الضرر العابر للحدود عن انشطة لا يحظرها القانون الدولي، منشورات الحلبي الحقوقية، ط١، بيروت، لبنان، ٢٠١٣.

١٤. جون . اس ز جيسـون ، معجم قانون حقوق الانسـان العالمي ، ترجمة سـمير عزت نصار ، دار النشر والتوزيع ، عمان ، ١٩٩١.
١٥. حارث عاصم الخطاب، الحرب الخفية، العلاقات الدولية وتأثيرها في الهجمات الالكترونية، ط١، دار الاداب للطباعة والنشر والتوزيع، بغداد، ٢٠١٩.
١٦. حسـن طاهر داود، أمن المعلومات، مطابع اكاديمية نايف للعلوم الأمنية، الرياض، السعودية، ١٩٩٧.
١٧. د.ذياب موسى البداينة ، الجرائم المستحدثة في ظل المتغيرات والتحولات الأقليمية والدولية ، ، ورقة علمية مقدمة إلى الملتقى العلمي في كلية العلوم الاستراتيجية، عمان، الأردن، للفترة من ٢-٤ أيلول ٢٠١٤ .
١٨. رابطة القانون الدولي ILA ، فريق الدراسـة حول العناية الواجبة في القانون الدولي، التقرير الثاني ، ٢٠١٦.
١٩. راسل بوكان، اللائحة القانونية الدولية للتجسس السيبرانية التي ترعاه الدولة في المعايير السيبرانية الدولية، منشورات الناتو، تالين، ٢٠١٦.
٢٠. د.رامي متولي القاضـي ، مكافحة الجرائم المعلوماتية ، دراسـة مقارنة ، ط١ ، دار النهضة ، ٢٠٠٠.
٢١. د.رياض صـالح ابو العطا، حماية البيئة من منظور القانون الدولي العام، دار الجامعة الجديدة، مصر ، ٢٠٠٩.
٢٢. ريتشارد كلارك وروبرت نيك : حماية الفضاء الالكتروني في دول مجلس التعاون الخليجي ، سلسلة محاضرات ، ط١ ، ابو ظبي ، ٢٠١١.
٢٣. ريتشارد كلارك، وروبرت نيك ، حرب الفضاء الالكتروني الخطر القادم على الأمن القومي وسبل مواجهته، ط١، مركز الامارات لدراسة السياسات، ٢٠١٢.
٢٤. د.زهير الحسـني، التدابير المضـادة في القانون الدولي العام، دراسـة في وسـيلة ضـمان الاداء إزاء انتهاك القانون الدولي دون إثارة المسـؤولية الدولية، ط١، المركز العربي للنشر والتوزيع، القاهرة، مصر، ٢٠٢٠.
٢٥. زياد عبدالرحمن الكوراني، رؤية جيوستراتيجية لمستقبل الصراعات الاقليمية في منطقة تزاحم الاستراتيجيات، المنهل، ٢٠١٨.
٢٦. د.سعيد سالم جويلي، مبدأ التعسف في استعمال الحق في القانون الدولي العام، دار الفكر العربي، ١٩٨٥.
٢٧. سـمير ابراهيم حاجم الهيتي، الآليات القانونية الدولية لحماية البيئة في اطار التنمية المستدامة، ط١، منشورات الحلبي الحقوقية، بيروت، لبنان، ٢٠١٤.

٢٨. سولانغ غبير ناوني هيلي واليكساندر نتوكو ، دليل الأمن السيبراني للبلدان النامية ، الاتحاد الدولي للاتصالات ، جنيف ، ٢٠٠٦.

٢٩. د.شادي عبدالوهاب، حروب الجيل الخامس، ط١، العربي النشر والتوزيع، القاهرة، ٢٠١٩.

٣٠. د.شـــهاب احمد العنبكي ، أثر العولمة على ســـيادة الدولة في القانون الدولي، دراسة تحليلية مقارنة، ط١، بغداد، ٢٠١٥.

٣١. صـــادق باقر ابراهيم العلوي، المســـؤولية الدولية الناشـــئة عن دعم المجموعات المسلحة، دراسة تحليلية في ضوء معيار السيطرة الكاملة، ط١، مكتبة زين الحقوقية والادبية، بيروت، ٢٠١٩.

٣٢. د.صلاح عبد الرحمن الحديثي ود. سلامة طارق شعلان ، حقوق الانسان بين الامتثال والاكراه في منظمة الامم المتحدة م ط٢ ، مؤسسة النبراس للطباعة والنشر والتوزيع ، النجف الاشرف ، ٢٠٠٨.

٣٣. د.ضاري خليل محمود و د. باسل يوسف ، المحكمة الجنائية الدولية ، هيمنة القانون أو قانون الهيمنة ، منشأة العارف ، الاسكندرية ، ٢٠٠٨.

٣٤. د.طارق ابراهيم الدسوقي، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، الاسكندرية، مصر، ٢٠٠٩.

٣٥. د.طارق عبد العزيز حمدي ، المســـؤولية الدولية الجنائية والمرتبة عن جرائم الإرهاب الدولي ، مصر ، دار الكتب القانونية ، ٢٠٠٨.

٣٦. د.عادل عبد الصادق. الارهاب الالكتروني القوة في العلاقات لدولية نمط جديد وتحديات مختلفة، القاهرة، مركز الاهرام للدراسات السياسية والاستراتيجية ٢٠٠٩.

٣٧. د.عادل عبدالصادق، اسلحة الفضاء الالكتروني في ضوء القانون الدولي الإنساني، مكتبة الاسكندرية، الاسكندرية، ٢٠١٦.

٣٨. د.عادل عبدالصادق، الارهاب الالكتروني: القوة في العلاقات الدولية، نمط جديد وتحديات مختلفة، مركز الاهرام للدراســات الســياســية والاســتراتيجية، ط١، القاهرة، ٢٠٠٩.

٣٩. د.عامر الزمالي ، القانون الدولي الانساني وتطور محتواه وتحديات النزاعات المعاصرة (مدخل في القانون الدولي الانساني والرقابة على استخدام الاسلحة) ، تونس ، من دون سنة طبع.

٤٠. د.عامر الزمالي ، المدخل إلى القانون الدولي الانساني ، مكتبة دار السلام القانونية ، النجف ، ط٦ ، ٢٠١٦.

٤١. عباس بدران ، الحروب الالكترونية ؛ الاشتباك في عالم متغير ، مركز دراسات الحكومة الالكترونية ، بيروت ، ٢٠١٠.

٤٢. د.عبد العزيز بن غرم الله جار الله ، جرائم الانترنت وعقوباتها وفق نظام ومكافحة الجرائم المعلوماتية السعودي ، دراسة مقارنة ، ط١ / دار الكتاب الجامعي ، الرياض ، ٢٠١٧.

٤٣. د.عبد الكريم علوان، الوسـيط في القانون الدولي العام ، دار الثقافة ، عمان، ٢٠١٠.

٤٤. د.عبد الواحد محمد يوسـف الفار، الجرائم الدولية وسـلطه العقاب عليها، دار النهضة العربية، القاهرة ،١٩٩٥.

٤٥. د.عبدالعزيز محمد سرحان، القانون الدولي العام، دار النهضـة العربية، القاهرة، ١٩٨٠.

٤٦. د.عبدالعزيز لطفي جادالله ، امن المجتمع الالكتروني بين سياسية السوق الالكترونية والتعاون الدولي في اطار مواجهة الجرائم الالكترونية، ط١، مكتبة الوفاء القانونية، الاسكندرية، ٢٠١٧.

٤٧. عبدالمطلب ممدوح عبدالحميد، جواز استخدام الكمبيوتر شبكة المعلومات العالمية، الجريمة عبر الانترنت، ط١، مكتبة دار الحقوق، الشارقة، ٢٠٠١.

٤٨. د.عبدالمعز عبدالغفار نجم، الاجراءات المضادة في القانون الدولي، دار النهضة العربية، القاهرة، ط١، ١٩٨٨.

٤٩. عبدالمنعم عبدالغفار نجم، الاجراءات المضـادة في القانون الدولي العام، دار النهضة العربية، القاهرة، ١٩٨٨.

٥٠. د.عبدالناصـر زياد هياجنة، القانون البيئي، النظرية العامة للقانون البيئي مع شرح التشريعات البيئية، ط١، دار الثقافة للنشر والتوزيع، الاردن، ٢٠١٢.

٥١. د.عدنان النقيب، الحرب الالكترونية في ضوء بروتوكولي سبع وسبعين الملحقين باتفاقات جنيف الاربع لسنة تسع واربعين، (الهجمات السيبرانية)، ط١، المركز العربي للنشر والتوزيع، القاهرة، مصر، ٢٠٢٢.

٥٢. عدنان عبدالعزيز مهدي الدوري، سلطة مجلس الأمن في اتخاذ التدابير المؤقتة، ط١، دار الشؤون الثقافية العامة، بغداد، ٢٠٠١.

٥٣. د.عصام العطية ،القانون الدولي العام ، مكتبة النهضة، بغداد ، ط٨، ٢٠٠٨.

٥٤. د.علاء الدين حسين مكي، استخدام القوة في القانون الدولي، المطابع العسكرية ، بغداد، ١٩٨٢.

٥٥. د. علاء عبد الرزاق محمد السالمي ، المدخل إلى الأمن السيبراني ، الفضاء السيبراني – تهديدات الفضاء السيبراني، الاسلحة الهجومية – وسائل مواجهة التهديدات السيبرانية – استراتيجية الأمن السيبرانية، ط١، دار الذاكرة للنشر والتوزيع ، بغداد ، ٢٠٢١.

٥٦. علي زياد العلي ، الصراع والامن الجيوسيبراني في السياسة الدولية ، دراسة في استراتيجيات الاشتباك الرقمي ، ط١ ، دار امجد للنشر والتوزيع ، الاردن ، ٢٠١٩.

٥٧. علي صادق ابو هيف، القانون الدولي العام، منشأة المعارف، الاسكندرية، ١٩٧١.

٥٨. د.علي عبد القادر الكهوجي، القانون الدولي الجنائي (اهم الجرائم الدولية)، المحاكم الدولية، منشورات الحلبي، بيروت، ٢٠٠١.

٥٩. د.غسان الجندي، المسؤولية الدولية، ط١، مطبعة توفيق، عمان، الاردن، ١٩٩٠.

٦٠. كاترينا زيولكوفسكي، المبادئ العامة للقانون الدولي كما تنطبق في الفضاء السيبراني، في وقت السلم لانشطة الدولة في الفضاء الالكتروني والقانون الدولي والعلاقات الدبلوماسية، الناتو، تالين، ٢٠١٣.

٦١. كالسهوفين فريتس ، تسغفلد ليزابيث، ضوابط تحكم خوض الحرب ، مدخل للقانون الدولي الإنساني، ترجمة احمد عبد الحليم، منشورات اللجنة الدولية للصليب الأحمر، جنيف، ط١، ٢٠٠٤.

٦٢. د.كامل سعيد، جرائم الكمبيوتر والجرائم الاخرى في مجال التكنلوجيا، بحث مقدم إلى مؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، ١٩٩٣.

٦٣. لفقير بولنوار بن الصديق، جرائم الحرب في ضوء أحكام القانون الدولي الإنساني ، دار الايام للنشر والتوزيع ، عمان، الاردن ، ٢٠١٥.

٦٤. مايكل ن.شميت، الحرب بواسطة شبكات الاتصال، الهجوم على شبكات الكمبيوتر (الحاسوب) والقانون في الحرب، اللجنة الدولية للصليب الأحمر، ٢٠٠٢.

٦٥. محسن افكيرين، القانون الدولي العام، ط١، دار النهضة العربية، ٢٠٠٥.

٦٦. محمد أحمد القرعان ، الجرائم الالكترونية ، ط١ ، دار وائل للنشر والتوزيع ، عمان ، ٢٠١٧.

٦٧. د.محمد المجذوب، القانون الدولي العام، منشـــورات الحلبي الحقوقية، بيروت، لبنان ، ٢٠٠٣.

٦٨. محمد أمين أحمد الشـوابكة، جرائم الحاسـوب والانترنيت– الجريمة المعلوماتية، ط١، دار الثقافة، عمان، الاردن، ٢٠٠٤.

٦٩. د.محمد حافظ غانم ، المســؤولية الدولية – دراســة لاحكام القانون الدولي وتطبيقاتها التي تهم الدول العربية ، جامعة الدول العربية – معهد الدراســات العربية العالمية ، مصر ، بدون سنة طبع.

٧٠. د.محمد حافظ غانم، مبادئ القانون الدولي، دار النهضة العربية، ١٩٦٨.

٧١. د.محمد سامي الشوا ، ثورة المعلومات وانعكاساتها على قانون العقوبات ، دار النهضة العربية . القاهرة، ١٩٩٤.

٧٢. د.محمد ســعيد الدقاق، عدم الاعتراف بالاوضــاع الإقليمية غير المشــروعة ، دراسة لنظرية الجزاء في القانون الدولي، دار المطبوعات الجامعية، القاهرة، ١٩٩١.

٧٣. د.محمد سعيد الدقاق ومصطفى سلامة حسين، القانون الدولي المعاصر، دار المطبوعات الجامعية، الاسكندرية، ٢٠١٥.

٧٤. محمد طاهر ، الحريات الرقمية – المفاهيم الاساسية ، مؤسسة حرية التعبير ، ط١ ، القاهرة ، ٢٠١٣.

٧٥. د.محمد علي العرين، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الاسكندرية، ٢٠١١.

٧٦. د.محمد فهاد الشــلالدة، القانون الدولي الإنســاني، ط١، منشــأة المعارف، الاسكندرية، ٢٠٠٥.

٧٧. د.محمد محمود خلف، حق الدفاع الشرعي في القانون الدولي الجنائي، ط١، دار النهضة العربية، القاهرة، ١٩٧٣.

٧٨. د.محمد منصـور الصـاوي، احكام القانون الدولي المتعلقة بمكافحه الجرائم ذات الطبعة الدولية، دراسـة في القانون الدولي الاجتماعي، دار المطبوعات، الاسـكندرية ، من دون سنه نشر.

٧٩. محمد نعيم علوة، موسوعة القانون الدولي العام، المبادئ، (المبادئ والمصـادر)، الجزء الاول، منشورات زين الحقوقية، بيروت، ٢٠١٢.

٨٠. مصــطفى يونس مؤيد يونس، اســتراتيجية الولايات المتحدة الامريكية للامن السيبرانية، الموصل، كلية العلوم السياسية، جامعة الموصل، ٢٠١٩.

٨١. مفيد محمد شهاب، القانون الدولي العام، المصادر والاشخاص، دار النهضة العربية، القاهرة، ١٩٨٥.
٨٢. منى الاشقر جبور، المعلوماتية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية.
٨٣. د.منى محمود مصطفى، استخدام القوة المسلحة في القانون الدولي بين الحظر والاباحة ، دار النهضة العربية، ١٩٨٩.
٨٤. ميلدز نيلز ، دليل تفسير لمفهوم المشاركة المباشرة في العمليات العدائية بموجب القانون الدولي الإنساني ، اللجنة الدولية للصليب الاحمر ، ط١ ، القاهرة ، ٢٠١٠.
٨٥. د.نزار العنبكي ، القانون الدولي الانساني ، دار وائل للنشر والتوزيع ، ط١ ، عمان ، الاردن.
٨٦. نعمان عبدالباري، أثر التكنولوجيا في حروب القرن الواحد والعشرون، ط١، دار الافتاء للطباعة والتوزيع، القاهرة، ٢٠١٥.
٨٧. نعمان عطا الله الهيتي، الاسلحة المحرمة دوليا، القواعد والاليات، دار رسلان للطباعة والنشر والتوزيع، دمشق، سوريا، ٢٠٠٧.
٨٨. نوران شفيق، اثر التهديدات الالكترونية على العلاقات الدولية ، دراسة في أبعاد الأمن الالكتروني ، المكتب العربي للمعارف، ط١، ٢٠١٦.
٨٩. د.هادي نعيم المالكي و هديل صالح الجنابي ، مبدأ الملوث يدفع في اطار المسؤولية الدولية الناجمة عن تلويث البيئة ، من دون سنة نشر ، ٢٠١٥.
٩٠. هشام محمد فريد ، قانون العقوبات ومخاطر تقنية المعلومات ، مكتبة الآلات الحديثة ، ١٩٩٢.
٩١. يوسف حسن يوسف، المسؤولية الجنائية لرئيس الدولة عن الجرائم الدولية، ط١ ، منشأة المعارف ، الاسكندرية ، مصر ، ٢٠١١.

ثانياً: الاطاريح والرسائل الجامعية

١. بشير جمعة عبد الجبار، الحماية الدولية للغلاف الجوي، اطروحة دكتوراه، كلية القانون، جامعة بغداد، ٢٠٠٦.

٢. حسن خميس مصطفى السعدني، العلاقة بين التدابير المضادة والجزاءات في القانون الدولي المعاصر دراسة لحالة الملف النووي الايراني ، أطروحة دكتوراه ، كلية الاقتصاد والعلوم السياسية ، جامعة القاهرة ، ٢٠١٣.

٣. خالد مجيد بريسم المجمعي ، كفالة احترام قواعد القانون الدولي الانساني ، رسالة ماجستير ، كلية الحقوق ، جامعة تكريت ، العراق ، ٢٠١٩.

٤. سراب ثامر أحمد ، الهجمات في شبكات الحاسوب في القانون الدولي الإنساني، اطروحة دكتوراه، مقدمة إلى مجلس كلية الحقوق ، جامعة النهرين،٢٠١٥.

٥. صغير يوسف، الجريمة المرتكبة عبر الانترنت، رسالة ماجستير، جامعة مولودي معمري، الجزائر، ٢٠١٢.

٦. عزة محمود احمد خليل، مشكلات المسؤولية المدنية في مواجهة فيروس الحاسب الآلي ، دراسة مقارنة في القانون المدني والشريعة الاسلامية، اطروحة دكتوراه ، كلية الحقوق، جامعة القاهرة، ١٩٩٤.

٧. فريدة طاجين، تأثير القوة السيبرانية على استراتيجيات الأمنية للدول الكبرى، دراسة حالة الصين، رسالة ماجستير مقدمة إلى كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، الجزائر، ٢٠١٨.

٨. ولد جيلاني هواري، العقوبات الاقتصادية الدولية وتأثيرها على خطط التنمية المحلية، رسالة ماجستير، مستغانم،الجزائر، ٢٠١٤.

ثالثاً: البحوث

١. احلال نواري ، تراجع السيادة في ظل التحولات الدولية ، مجلة دفاتر السياسية والقانون ، جامعة سعيدة ، الجزائر ، ع (٤) ، ٢٠١١.

٢. د.احمد عبد الكريم سـلامة ، الانترنت والقانون الدولي الخاص فراق ام تلاقي، بحوث مؤتمر القانون والكومبيوتر والانترنت المنعقد بتاريخ مايو / ٢٠٠٠ ، جامعة الامارات العربية المتحدة ، كلية الشريعة والقانون ، المجلد (١) ، ٢٠٠٤.

٣. د.احمد عبيس نعمة الفتلاوي ود. ازهر عبد الامير الفتلاوي ، المسـؤولية الناشـئة عن استخدام وسائل القتال الفتاكة في نشر الاوبئة / الهجمات السيبرانية في مقابل جائحة كورونا انموذجاً ، مجلة الحقوق ، ع (٤١) ، ٢٠٢١.

٤. د.احمد عبيس نعمة الفتلاوي، وازهر عبد الامير راهي ، الاطار المفاهيمي للعناية الواجب والاخطار في ضـوء قواعد المسـؤولية الدولية (جائحة كورونا) مجلة الرافدين للحقوق (المجلد ٢٢) ، ع (٧٩) كلية الحقوق جامعة الموصل.

٥. اماني عصام محمد ، استخدام روسيا للقوة المعلوماتية في تفاعلاتها الدولية، المجلد (٢٢)، ع (٤)، مجلة كلية الاقتصاد العلوم السياسية ، جامعة القاهرة، ٢٠٢١.
٦. د.ايهاب خليفة، الحرب السيبرانية، مراجعة العقيدة العسكرية استعداد للمعركة القادمة، مجلة السياسية الدولية، ع (٢١١) ، المجلد (٥٣)، القاهرة ، مصر ، ٢٠١٨.
٧. د.ايهاب خليفة، امكانية تحقيق الردع في صراعات الفضاء الالكتروني، مركز المستقبل للابحاث والدراسات المتقدمة، ع (١٣)، ٢٠١٥.
٨. أيان يو ينغ ليو، مسؤولية الدولة والهجمات الالكترونية– تحديد التزامات العناية الواجبة، المجلة الاندونيسية للقانون الدولي المقارن، مطبعة معهد حقوق المهاجرين، ٢٠١٧.
٩. بصائر علي محمد ، انتهاكات الحق في حرية التعبير ، دراسة خاصة عن التدوين الالكتروني ، مجلة كلية الحقوق ، جامعة النهرين ، المجلد (١٧) ، ٢٠١٥.
١٠. بن تغري موسى، الحرب السيبرانية والقانون الدولي الانساني، مجلة الاجتهاد القضائي، المجلد (١٢)، عدد خاص (٢٢)، جامعة محمد خيضر بسكرة، الجزائر، ٢٠٢٠.
١١. جمال العظامات، جريمة العدوان في الهجمات الالكترونية في نطاق القانون الدولي العام، مجلة المنارة، ع (٤)، المجلد (٢١)، ٢٠١٥.
١٢. جون ماري هنكرتس، القانون الدولي الإنساني العرفي، (المجلد الأول : القواعد) ، اللجنة الدولية للصليب الأحمر، بعثة القاهرة، القاهرة، ٢٠٠٧.
١٣. حسين قؤادرة، الردع السيبراني بين النظرية والتطبيق المجلة الجزائرية للأمن والتنمية، المجلد (٩)، ع (١٦) ، جامعة أم البواقي، الجزائر، ٢٠٢٠.
١٤. د.حيدر ادهم الطائي وعلي محمد كاظم الموسوي ، المشاركة المباشرة للهبة الجماعية في الهجمات السيبرانيه ، مجلة كلية الحقوق ، جامعة النهرين ، بغداد ، ٢٠١٩.
١٥. د.حيدر عبد محسن شهد الجبوري ، معيار العناية الواجبة في القانون الدولي البيئي ، مجلة كلية التربية الاساسية للعلوم التربوية والانسانية ، مجلد (١٣) ، ع (٥٢) ، جامعة بابل ، ٢٠٢١.
١٦. د.حيدر كاظم عبدعلي ورباب محمود عامر، التنظيم القانوني للهجمات المعلوماتية على المنشآت ذات القوى الخطرة، مجلة الكوفة، ع (٤٧) ، ٢٠١٩.

١٧. خالد ابو سجود حساني، استخدام القوة بترخيص من مجلس الأمن في اطار الأمن الجماعي، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، المجلد (١٢)، ع(١)، حزيران ٢٠١٥.

١٨. خالد وليد محمود، الهجمات عبر الانترنيت، ساحة الصراع الالكتروني الجديدة، المركز العربي للابحاث ودراسة السياسات، ٢٠١٣.

١٩. دوديجي كودولار ، لا تقترب من حدود فضائي الالكتروني : الحرب الالكترونية والقانون الدولي الانساني وحماية المدنيين ، المجلة الدولية للصليب الاحمر ، المجلد (٩٤) ، ٢٠١٢.

٢٠. رزق سلمودي واخرون ، الموقف المعاصر لقواعد القانون الدولي العام من الحق في الخصوصية في العصر الرقمي ، مجلة الجامعة العربية الامريكية للبحوث ، مجلد (٣) ، ع (٢).

٢١. د.رغدة البهي، الردع السيبراني، المفهوم والاشكاليات والمتطلبات، مجلة العلوم السياسية والقانون ، المركز العربي الديمقراطي، برلين، ع (١) ، ٢٠١٦.

٢٢. سامر مؤيد عبداللطيف، الحرب في الفضاء الرقمي، رؤية مستقبلية، مجلة رسالة الحقوق، س (٧) ، ع(٢)، ٢٠١٥.

٢٣. سعيد درويش، ماهية الحرب الإلكترونية في ضوء قواعد القانون الدولي ، حولية جامعة الجزائر ج(٢)، ، ع (٢٩) ، ٢٠١٦.

٢٤. د.سعيد سالم جويلي، الجوانب الاقتصادية للتدابير المضادة في القانون الدولي، المجلة القانونية الاقتصادية، كلية الحقوق ، جامعة الزقازيق، ع (٦)، ١٩٩٤.

٢٥. سعيد عياش، الحرب في الحيز الافتراضي، مجلة قضايا إسرائيلية، عين (٤٣، ٤٤) ، المركز الفلسطيني للدراسات الإسرائيلية، فلسطين، ٢٠١٢.

٢٦. د.سلافة طارق الشعلان ، تكييف استخدام الحرب الالكترونية في النزاعات المسلحة وفقاً للقانون الدولي الإنساني ، مجلة الكوفة للعلوم القانونية والسياسية ، المجلد (١) ، ع (٢٦) ، ٢٠١٦.

٢٧. د.سيف نصرت الهرمزي، وصف المقاربات لمنظورات الفاعل الرقمي والإنكشاف الاستراتيجي في ظل الفضاء المعلوماتي، مجلة اداب الفراهيدي، ع(٣٧)، ٢٠١٩.

٢٨. شازية قريشي ، تمديد معيار العناية الواجبة إلى تقديم استجابة الدولة تجاه العنف ضد المرأة ، العنف المنزلي ، جامعة البنجاب ، المجلد (٢٨) ع (١) ، ٢٠١٣.

٢٩. د.شـريف عتلم، تطبيق القانون الدولي الانسـاني على الاصـعدة الوطنية، بحث منشـور في كتاب القانون الدولي الانسـاني، دليل التطبيق على الصـعيد الوطني، دار المستقبل العربي، القاهرة، ٢٠٠.

٣٠. شـيخة حسـين الزهراني ، التعاون الدولي في مواجهة الهجوم السـيبراني ، مجلة جامعة الشارقة للعلوم القانونية ، المجلد (١٧) ، ع (١) جامعة الشارقة – كلية القانون ، الامارات العربية المتحدة ، ٢٠٢٠.

٣١. صفات أمين سلامة ، أسلحة حروب المستقبل بين الخيال والواقع، دراسات استراتيجية ، ع (١١٢) مركز الامارات للدراسات والبحوث الاستراتيجية، ابوظبي، ٢٠٠٥.

٣٢. صـــلاح الدين عامر، حماية البيئة إبان النزاعات المســـلحة في البحار، المجلة المصرية للقانون الدولي ، ع (٤٩)، ١٩٩٣.

٣٣. صـلاح مهدي هادي وزيد محمد علي اسـماعيل، الأمن السـيبراني كمرتكز جديد في الاستراتيجية العراقية، مجلة قضـايا سياسية، مكتبة العلوم السياسية، جامعة النهرين، ع (٦٢)، السنة (١٢)، ٢٠٢٠.

٣٤. د.عـادل عبـدالجواد محمـد ، دور مراكز المعلومـات في التعـامـل مع الازمـات، بحث منشور في مجلة الأمن والحياة، الرياض، ع(٣٥)، ٢٠١٦.

٣٥. علاء الدين فرحات وعمروس عمارة، الفضـــاء السـيبراني وتأكل مفهوم السـيادة الوطنية، المجلة الجزائرية للدراسات السياسية، المجلد (٨)، ع (٢) ، الجزائر، ٢٠٢١.

٣٦. فاطمة نعناع ، ((قنبلة الكترونية في بريد الجامعة)) مقال منشور في مجلة انترنت العالم العربي ، السنة (1) ، ع (٧) ، ١٩٩٨.

٣٧. د.فايق حســـن جاســـم ، اثر الانفتاح المعلوماتي على ســـيادة الوطنية ، مجلة السياسة الدولية ، الجامعة المستنصرية ، بغداد ، ع (١٨) ، ٢٠١١.

٣٨. فيصل اياد جعفر فرج الله ، مبدأ السيادة في القانون الدولية العام ، مجلة جامعة الكوفة للعلوم القانونية والسياسية ، المجلد (١) ، ع (١٤).

٣٩. د.كرار عباس متعب، الحرب الســـيبرانية، دراســـة في اســـتراتيجية الهجمات السـيبرنية بين الولايات المتحدة وايران، مجلة حمورابي للدراسـات، ع (٤٠)، س (١٠) ، (٢٠٢١).

٤٠. كريســـتينا بيلانديني، كفاله الامتثال للقانون الدولي الانســـاني على الصـــعيد الوطني ، دور اللجان الوطنية للقانون الدولي الانساني واثارها ، الناشر : المجلة الدولية للصليب الاحمر، مختارات المجلة الدولية للصليب الاحمر ،٢٠١٥.

٤١. كوردولا دوريجي ، لا تقترب من حدود فضـــائي الالكتروني : الحرب الالكترونية والقانون الدولي الانساني وحماية المدنيين ، المجلة الدولية للصليب الاحمر ، م (٩٤) جنيف، ٢٠١٢.

٤٢. اللجنة الدولية للصـليب الاحمر، الحرب المعلوماتية، القانون الدولي الإنسـاني ، يوفر طبقة إضافية من الحماية ، ١٠ ايلول ٢٠١٩.

٤٣. د.لمى عبد الباقي محمود العزاوي، و دعاء جليل حاتم، الذكاء الاصـــطناعي والمسـؤولية الجنائية الدولية، مجلة المفكر ، ع (١٨) ، كلية الحقوق والعلوم السـياسـية، جامعة محمد خيضر بسكرة، الجزائر ، ٢٠١٩.

٤٤. محمد طوالبيه، ايدلوجية القضـــاء الرقمي دراســة في الخلفيات المرجعية، بحث منشـور في مجلة أكاديمية الدراسـات الاجتماعية والإنسـانية، ع(٢١)، جامعة الشـلف، ٢٠١٩.

٤٥. محمد يوسف علوان، اختصاص المحكمة الجنائية الدولية، مجلة الأمن والقانون، أكاديمية شرطة دبي، ع (١)، ٢٠٠٢.

٤٦. مخيمر عبدالعزيز هادي، تعليق على مبادئ القواعد القانونية المتعلقة بحماية البيئة من التلوث العابر للحدود، المجلة المصرية للقانون الدولي، ع (٤٣)، ١٩٨٧.

٤٧. مصطفى عصام نعوس، سيادة الدولة في الفضاء الالكتروني، سلسلة دراسات عالمية، مركز الامارات للدراسات والبحوث الاستراتيجية، أبو ظبي، ع (٩٥) ، ٢٠١١.

٤٨. منصـــور مجاجي، مبدأ الملوث الدافع، المدلول الاقتصـــادي والمفهوم القانوني، المجلد (٣٤)، ع(١)، جامعة يحيى فارس، الجزائر، ٢٠٢٠.

٤٩. نورة شلوش ، القرصنة الالكترونية في الفضاء السيبراني : التهديد المتصاعد لأمن الدول ، مجلة مركز بابل للدراسات الانسانية ، المجلد ٨ ، ع ٢ ، ٢٠١٨.

٥٠. د.هادي نعيم المالكي ود. هديل صـــالح الجنابي ، مبدأ الملوث يدفع في اطار المسـؤولية الدولية الناجمة عن تلوث البيئة ، مجلة العلوم القانونية ، كلية القانون جامعة بغداد ، المجلد (٢٨) ، ع (٢) ، العراق ، ٢٠١٣.

٥١. هديل مالك ونضـال عباس ، دور القانون الدولي في حماية حرية الرأي والتعبير ، مجلة السياسية الدولية ، الجامعة المستنصرية ، بغداد ، ٢٠١٢.

٥٢. موسـوعة اتفاقيات القانون الدولي الإنسـاني، اعداد شـريف عتلم ، محمد ماهر عبد الواحد، اللجنة الدولية للصليب الأحمر، بعثة القاهرة، ط٩، القاهرة ، ٢٠٠٩.

٥٣. هشام سلمان، تكنلوجيا المعلومات والاتصال ، مجلة علوم التكنلوجيا، ع(٢)، من دون مكان نشر، ٢٠٠١.

٥٤. هناء الحموي، التأصيل الفقهي لمسؤولية الدولة عن الضرر البيئي، مجلة الفقه والقانون، ع(٣٣)، ٢٠١٥، ص٨٧.

٥٥. يمامة خضـير الحربي ، جوانب قانونية في الحكومة التكنلوجية للانترنت ، مجلة كلية القانون الكويتية العالمية ، لسنة السادسة ، لعدد (٤) ، ع التسلسلي ٢٤ ، الكويت، ٢٠١٨.

رابعاً: الاتفاقيات والاعلانات والمواثيق الدولية

١) اتفاقية لاهاي لعام ١٩٠٧ الخاصـــة بحقوق وواجبات الدول المحايدة والأشـــخاص المحايدين في حالة الحرب البرية.

٢) ميثاق الامم المتحدة للعام ١٩٤٥.

٣) اتفاقيات جنيف الاربع لعام ١٩٤٩.

٤) البروتوكول الاضافي الأول لعام ١٩٧٧ الملحق باتفاقيات جنيف الأربع لعام ١٩٤٩ .

٥) البروتوكول الاضافي الثاني لعام ١٩٧٧ الملحق باتفاقيات جنيف الأربع لعام ١٩٤٩.

٦) العهد الدولي الخاص بالحقوق المدنية والسياسية لعام ١٩٦٦.

٧) اتفاقية فينا لقانون المعاهدات لعام ١٩٦٩.

٨) الاتفاقية الامريكية لحقوق الانسان لعام ١٩٦٩.

٩) اعلان استوكهولم لعام ١٩٧٢ المعني بالبيئة البشرية.

١٠) اتفاقية جنيف الخاصة بالضرر العابر للحدود لعام ١٩٧٩.

١١) الميثاق الافريقي لحقوق الأنسان لعام ١٩٨١.

١٢) اتفاقية الأمم المتحدة لقانون البحار لعام ١٩٨٢.

١٣) اتفاقية بازل لعام ١٩٨٩ الخاصة بالتحكم بنقل النفايات.

١٤) اعلان ريو لعام ١٩٩٢ الخاص بالتنمية البيئية المستدامة.

١٥) النظام الاساسي للمحكمة الجنائية ليوغسلافيا السابقة ١٩٩٣.

١٦) اتفاقية شنغهاي للتعاون في مجال أمن المعلومات لعام ٢٠١١.

١٧) نظام روما الاساسي للمحكمة الجنائية الدولية لعام ١٩٩٨.

خامساً: التقارير والوثائق الدولية.

١. الأمم المتحدة، المجلس الاقتصـــادي والإجتماعي، لجنة حقوق الإنســـان، الدورة (٦٢) المنعقدة في ٢٠ شـــباط ٢٠٠٦، بنيويورك، البند (١٢/أ) من جدول الأعمال المؤقت-

معيار العناية الواجبة بوصفه أداة للقضاء على العنف ضد المرأة، تقرير المقررة الخاصة المعينة بالعنف ضد المرأة وأسبابه وعواقبه– السيدة ياكين إرتوك.

٢. الأمم المتحدة ، المجلس الاقتصادي والاجتماعي، القرارات المرقمة في ٢٠٠٦و ٢٠٠٧، الوثيقة:(A/2/3/rev.1) والقرارين (٧، ٨) في ٢٠٠٩.

٣. الأمم المتحدة، المجلس الاقتصادي والاجتماعي ، الدورة الموضوعية ، البند (١٣ / ب) من جدول الاعمال المؤقت المسائل الاقتصادية والبيئة : تسخير العلم والتكنلوجيا لأغراض التنمية والتقدم المحرز في تنفيذ ومتابعة نتائج مؤتمر القمة العالمي المجتمع المعلومات على الصعيدين الاقليمي والدولي نيويورك ٢٨ حزيران ٢٣ تموز ٢٠١٠.

٤. الجمعية العامة للأمم المتحدة، القرار رقم (٢٣٩/٥٧) في ١٣ كانون الاول، ٢٠٠٣.

٥. الجمعية العامة للأمم المتحدة، القرار رقم (٣٢/٥٨) في ٣٠ كانون الثاني ٢٠٠٣.

٦. الجمعية العامة للأمم المتحدة، فريق الخبراء الحكوميين المعني بالتطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي (٨/٧٠/١٧٤) ٢٢ تموز/ يوليو ٢٠١٥.

٧. الجمعية العامة للأمم المتحدة تؤكد على الحق في الخصوصية في العصر الرقمي ، صحيفة الوقائع التابعة للأمم المتحدة ، ٢ك١ ، ٢٠١٣ ، مطبوعات الامم المتحدة نيويورك ، ٢٠١٣.

٨. الجمعية العامة للأمم المتحدة، ارساء ثقافة أمنية عالمية لحماية الفضاء الحاسوبي، ينظر الوثيقة (A/RES/57/239) والهياكل الاساسية للمعلومات ، القرار رقم (٥٧ / ٢٣٩) في ١٣ك ٢٠٠٣ .

٩. مؤتمر الامم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية، ٢٠٠٥، الوثيقة المرقمة، (ARES/60/177).

١٠. الوثائق الرسمية للجمعية العامة للأمم المتحدة، الدورة الحادية والخمسين، تقرير لجنة القانون الدولي عن اعمال دورتها الثامنة والأربعين، ١٩٩٦/٥/٦، الملحق رقم (١).

١١. اجراء عدم الامتثال لعام١٩٩٨، الفقرة ٩ من المرفق الثاني عن تقرير الاجتماع العاشر للاطراف في بروتوكول مونتريال ذات الصلة بالمواد المستنفدة لطبقة الاوزون، ٣ ديسمبر/ ك ١ ١٩٩٨.

١٢. فتوى محكمة العدل الدولية بشان مشروعية استخدام الاسلحة النووية او التهديد بها لعام ١٩٩٦، ملحق لمذكرة الامين العام للامم المتحدة لنزع السلاح، مقدم الى الوحدة الحادية والخمسين للجمعية العامة بتاريخ ١٥/١٠/١٩٩٦، رقم الوثيقة(A/٥١/٢٠١٨).

١٣. قضية الأنشطة المسلحة في الكونغو بين الولايات المتحدة الأمريكية والكونغو رقم الوثيقة (I.c.j. 168,144,2005).

١٤. لجنة القانون الدولي، مسؤولية الدول عن أفعالها غير المشروعة دولياً لعام ٢٠٠١.

١٥. فتوى محكمة العدل الدولية في قضية حائط الفصل العنصري (I.C.J.136, K10, 2004).

١٦. قضية الأنشطة المسلحة في الكونغو بين الولايات المتحدة الامريكية والكونغو، ينظر وثيقة (I.C.J.168, 147, 2005).

سادساً : المصادر الالكترونية

١- ايرين كوزيجو، تأمين الفضاء السيبراني- التزام الدول بمنع الفضاء السيبراني الدولي الضار، متاح على الموقع الالكتروني :

https://translate.googeluserontent.com تاريخ الزيارة ٢٠٢٢/١/٢٤.

٢- اكيكو تاكانوا، التزامات العناية الواجبة والعابرة للحدود، الضرر البيئي، تطبيقات الامن السيبراني، المدرسة العليا للدراسات البيئية العالمية، جامعة كيوتو، ٢٠١٨، ص٨. متاح على الموقع الالكتروني:

https//:translate.googleusercontent.com/translate. تاريخ الزيارة ٢٠٢٢/١/١٧

٣- بشار خليل، ماهي الحرب السيبرانية؟ مستقبل مخيف للصراع الرقمي، مجلة المعلوماتية ، ع (١٥٤)، الجمعية السورية المعلوماتية، ٢٠٢٠، متاح على الموقع الالكتروني: تاريخ الزيارة ٢٠٢٢/٤/٢٥.

Http://www.scs.org.sy/?=scs/informag/showarticlendos.

٤- تشير كوب، لوك، السيادة الاقليمية في الفضاء الالكتروني، مجلة بلورن للقانون الدولي، ٢٠١٩، متاح على الموقع الالكتروني:

https://classic.austil.edu.au. تاريخ الزيارة ٢٠٢٢/٣/١٢.

٥- الامم المتحدة، برنامج الامم المتحدة للبيئة، مبادئ توجيهية بشـــأن الامتثال للاتفاقات . البـيـئـيـة مـتـعـددة الاطـراف وانـفـاذهـا، مـتـاح عـلـى الـمـوقـع الالـكـتـرونـي: تاريخ الزيارة ٢٠٢٢/٩/٨.https://wedocs.unep.org.

٦- أحمد يوسـف كيطان، اسـتراتيجية الأمن الوطني السـيبراني للصـين، قراءة في قانون الأمن الســـيبراني الصـــيني، متـاح على الرابط الالكتروني تـاريخ الزيـارة ٢٠٢٢/٤/٢٩، ٧https://www.politicsdz.com

٧- اللجنة الدولية للصـــليب الاحمر ، تعليقها على احكام المادة الثالثة المشـــتركة ، منشـــورات اللجنة الدولية للصـــليب الاحمر ، متاح على الموقع الالكتروني .http://cut.lu/akp3hqm تاريخ الزيارة ٤ / ١٢ / ٢٠٢١ .

٨- الامم المتحدة، برنامج الامم المتحدة للبيئة، مبادئ توجيهية بشـــأن الامتثال للاتفاقات البيئية متعددة الاطراف وانفاذها، متاح على الموقع الالكتروني: .https://wedocs.unep.orgتاريخ الزيارة ٢٠٢٢/٩/٨.

9- جان بودان، اصول السلطة والسيادة، متاح على الرابط الالكتروني:

.http://www.marafa.org تاريخ الزيارة ٢٠٢٢/٢/٧.

١٠- حسام ياسر ، اعلانات روسية أثرت على نتائج الانتخابات الامريكية ، وكالة سبوتنيك الروسية ، ٢٠١٧ ،متاح على الرابط الالكتروني تاريخ الزيارة ٢٠٢١/٩/٢٨ : https://sputniknews . com/world /d/2017/09/3/026157443

١١- خانا بالافي، سـيادة الدولة والدفاع عن النفس في الفضـــاء السـيبراني، متاح على الموقع الالكتروني:

.https://cyberieninka.ru تاريخ الزيارة ٢٠٢٢/٤/٢٧.

١٢- ســـارة بو حادة ، اثر الارهاب الالكتروني على امن واســـتقرار الدول ، متاح على الموقع الالكتروني:

https//:manifest . univ – ouargla . dzldocuments archiv

تاريخ الزيارة ١١/١٨ / ٢٠٢١.

١٣- شـــريف نســـيم قلته، دليل تالين، الهجمات الالكترونية وحظر اســـتخدام القوة في القانون الدولي، المركز العربي لابحاث الفضاء الالكتروني، متاح على الرابط الالكتروني: https://accronline.com. تاريخ الزيارة ٢٠٢٢/٤/٦.

١٤- مروة صبحي، تسليح تكنولوجي ، تنافس غير تقليدي في مجال التكلنولوجيا العسكرية، مركز المستقبل، للابحاث والدراسات المستقبلية، متاح على الرابط الالكتروني http://rawabetcenter.com/archives/6591. تاريخ الزيارة ٢٠٢١/٨/٢٣.

١٥- عادل رفيق، الجيوبوليتكس السبيرانية والاستقرار في الشرق الأوسط كانون الثاني ٢٠١٨، المعهد المصـــري للدراســـات، ص٧ متاح على الموقع إلكتروني تاريخ الزيارة ٢٠٢١/١١/٨: http:eipss,eg,org

١٦- لبكي جورج ، المعاهدات الدولية للأنترنت : حقائق وتحديات ، مجلة الدفاع الوطني ، بيروت ، ع (٨٣) ، ٢٠١٣ ، متاح على الرابط الالكتروني : https//:cult.ly/.nh5hell. تاريخ الزيارة ٤/ ٦ / ٢٠٢١.

١٧- مايكل أن شميت، احترام السيادة في الفضاء المعلوماتي، متاح على الموقع الالكتروني : https://texaslawreview.org. تاريخ الزيارة ٢٠٢٢/٣/٢.

١٨- وسام نعمت السعدي ، الحقوق الرقمية وآليات الحماية الدولية المقررة لها في اطار القانون الدولي لحقوق الانســـان ، الناشـــر وقائع المؤتمر العلمي لجامعة نولج متاح على الرابط الالكتروني: . https://portal.aird.my تاريخ الزيارة ٢٠٢٢/٣/٢٩.

سابعاً:المصادر الأجنبية

1. Adam Roberts, and Richard Guelff, Documents on the laws of war, N,Y.pub, 1989.
2. Aleen . springer , the international of pollution ; protection of the, global environ ment ina world of sovereign states , Westport, connectioct , auorum books , 1983.
3. Alexander klimbury , Nional cyber security farme work manual, NATO CCDCOE, Tallinn Estonia, 2012.
4. Amit sharma, cyber wars: Aparadigm shift from means to Ends, strategic Anolysis, vol.(34), 2010.

5. An outline for euoropean cyber diplomacy engagement , 9967/4/14 rev4 , dgdic , Brussels , septemper 2014 .
6. Anderew Moore, stuxnet and Article 2(4)'s prohibition Againts the use of force : customary law and potential Models, Naval law Review, vol. 64, 2015.
7. Andrewf . krepinevich , cyber war fare, center for strategic and Budgetary Assessments, 2012.
8. Antonio Cassese , the Nicaragua and Tadic Tests Revisited in light of the ICJ. Judgment on Genocide in Bosnia , The European journal of Xford University, Vol.(18), No.(4) EJIL, United Kingdom, 2007.
9. Arnove, A. IRag under siege: The Deadly impact of sancitions and war, (2003).
10. Aviram Zrahia, A Multidisciplinary Analysis of cyber in for mation sharing, military and Affairs, No(3), 2014.
11. Bell, camronh, cyber war fare and international law, the need for clarity , Towson university journal of international Affairs, Available At : http://cutt.lyHKdz ,Accessed on :16/1/2021.
12. Bilinding weapons: Reports of the meetings of experts convened bay the international committee of the red cross on battle field laser weapons, 1989-1999, ICRC, 1993.
13. Bodner, Matew, Russian Military Maerges Air force and space command, The Moscow Times online, August 2015.
14. Brahim Belhout, Liber propos sur les principes Fondamentaux du droit international de lenvieonnement, revue idare, rolume (18), No(1).
15. Christopher D.Deluca, The need for international laws of war to include cyber Attacks involving state Actors, pace international law Review on line companion, vol.(3), No.(9), 2013.
16. Clarke, R.and Knake, R.cyber war fare: Th Next Threat to National security and what to Do about it, 2010.

17. Claywilson, bootnets, cybercrime, and cyber terrorism, vulnerabilities and polic issues for congress, 2007.

18. Conral Wegalin'ski, cyber war fare and Responsibility of states, Torun international studies, the john paul II catholic university of Lublin, Vol.(9), No(1), Poland , 2016.

19. Constitution of the interternal ioval telecommunication union , article 34 .

20. Cvonish, paul, one cyber war far, Achatham House Report, The Royal institute of international Affairs London, 2011.

21. Cynthia eid , water the environ ments regulations et oplicies in the mediterranean sea counries ? , u. p. a, 2008.

22. Daniel B.silver, computer Network Attack as ause of force under article 2(4) of united Nations charter, in computer network attack and international law 73, 80- 82 (Michael N.Schmitt and Brian T.Donnell eds, 2002).

23. Daniel Bathlehem . principles Relevent to the scope of self- De fence Against imminemt of Actual Armed Attack by Non state Actors, American journal of international law , vol.(106), 769, 2012.

24. David Albright and Andreastricker, stuxnet worm targets Automated system for freguency conveters: Are larnian centrifuges thetargt? Institute for Science and international security, November 17, 2010.

25. David Awheelr and Gregoryn,larsan Technigues for cyber Attack Attribuion in statute for Defence Available on the websit:

26. David Clark and Whifield Diffe, cyber security and international Agree ments, procedings of a work shop on Deterring cyber Attaks: informing strategies and Developing options for U.S.policy National Academies press , 2010.

27. David hunter , jems salzman , durwoodzaelh , international environmental law and policy – second edition- newyork – 2002 .

28. Deancheng , cyber Dragon inside chinas information war fare and cyber operation, praegear , cali fornia , USA , 2017.

29. Dennis alland, La Leg'itime defence et Les contre-mesures dans la condification du droit international de La responsabilite. Journal de droit international, No.(3), 1983.

30. Doc,784, 1/1/27. 6 U.N.C.IODocs (1945).

31. Donald J.Reed, Beyond War on Terror sim into the the Fifth Generation of War and conflict, studies in conflict and Terrorism, vol.(31), Issue 8 , 2008.

32. Donald j.Reeds, Beyond war on Terror: in to the fifth Generation of war and conflict, studies in Terrosim, vol.(31), Issue8, 2008.

33. Emily Crawford, virtual battlegrounds,dirct participation cyber war fare , Sydney law school , legal studies reseaech paper, 2012.

34. Enekentikk at international cyber in cidents , lagal considertion, ccdioe bublication , 2010.

35. Eric Talpot jensen, soverejnty and eutralityin conflict, fordham international law journal, vol.(53), issue(3), articale2, 2012, p819 and georgewalkerneutrality and information warfare, internatonal law studies, Vol.(76), 2002.

36. Erik Nyman, Orevall Control the case against Dusko Tadic and the concept of Control in the ILC-Articles on State Responsibility, Master thesis public international Law Faculty of law, university of laud, Sweden, spring , 2008.

37. F.Lowen Feld, international Economie Low (oxford.oxford).

38. Feredrik Von Bothmer, Contextualising legal Reviews for Autonomous weapon system, Dissertation university of sT, GALLEN, Germany, 2018.

39. Fore .e.g.: Davide Graham cyber Threats and the law of war , journal of National security law policy, vol. 4, No.(1), 2010.

40. Frik Nyman, Orevall Control the case against Dusko Tadic and the co and the concept of Control in the ILC-Articles on State Responsibility, Master thesis public international Law Faculty of law, university of laud, Sweden, spring , 2008.

41. Ga Res . 56 / 121 , un . doc , noa / Res 15 / 121 , 2002 . avaliableal ; http ; llundocs . orgiar lal Res /15 /121/.

42. Gabcikovo- Nagymarosproject (Hungary and Slovakia), ICJ97, judgment of 25 september 1997.

43. Gen.jame SE . cartwright , memorandum for chiefs of the military servs , commanders of the combatant commands, dirs, Of the joint staff directories on joint Terminology for cyber space operation 5 (nov. 2011).

44. General Assembly, Developments in the field of information and Telecommunication in the context of international security, UN document A/RES/53/70, 4 January 1999.

45. General for global legal challenges , state responsibility for non-state actors that dettein in the course of niac , yale law school December 7,2015.

46. Henri Meyrowitz, " the priniciple of super fluous injury or unnecessary suffering- From declaration of st peters burg of 1868 to Additional protocol of 1977, " extract print of IRRC, No.(299) March- April 1994.

47. Henri Roigas, An Upolated Draft of the code of conduct distributed in the united Nations- ats New Availabe at:http://ccdeoe.org/incyber-articles/an-upolacted.

48. Hitt, Michela , Hoskisson , Roberte , competing for advantage , mason , 2004 .

49. I,CJ, case concenrning Military and paramilitary Activities in and Against Nicaragua (Nicaragua V.United states), Reports 1986.

50. Icj , bosnia Genocide case , Concerning application of the Convention on the prevention and punishment of the crime of Genocide gjudment of 26, February, 2007 , para 432.

51. ICJ, Argentinav. Uruguay, pulp milis case, case concerning pulp milis on the River Uruguay, judgment of 20 April. Para 1970.

52. ICJ, case of: Bosnia and Herzegovina.V.Serbiq and Monteregro, 2007.

53. ICJ, Corfu channel case (UK.V.Albania), Judgment, 1949 I.CJ, ReP.4,22 (Apr,9): See also Robert P.Barnidge, The Due Diligence under prinicipleunder international law, community Review, vol.(81), Issue 8, 2006.

54. ICJ, Nuclear weapons advisory opinion, logality of therats or use of Nuclear weapons, Advisory opinior, 1996, I.C.J, 226 (8 july), para, 86.

55. ICRC Report DPH 2006, Fourth Expertmeeting.

56. ICTY, prosecutor v.stanislav Galic, Trial chamber1, case No. (TT-98-29-T), judgement of 5 December 2003, para 58.

57. ITLOS , Responsibilities and obligations of states sponsoring persons and Entites with respected activities in the Area , para 117.

58. Jame . Alewis, thresholds for cyber war , center for strategic and international . studies, 2010.

59. Jame Alewis, thresholds for cyber war , center for strategic and international. studies, 2010.

60. Jarna Petman , Autonomous weapons system and international Humanitarian Law – out of the loop, Faculty of law, university do Helsinki, publisher by Erik Castre'n institute of international law and Human Rights , 2017.

61. Jeffrey carr, inside cyber war fare, second Edition, published by O Reilly Media, Ink, Sebastopol, USA, 2012.

62. John Arguilla and David Ronfeldt, cyber is coming, RAND corporation, 1993.

63. John Arguilla and David Ronfeldt, cyber is coming, RAND corporation, 1993.

64. Jona than Bonnit cha and Robert Mccorhuodale, The Concept of Due Diligen the UN Guiding Principles on Business and Human Rights, The European Journal of inter national Law, 28 No.(3), 2017.

65. Joseph s.Naye, cyber powr, harvad Kennedy schod, 2010.

66. Kamal Ahmed Khan, use of Force and Human Rights under international Law, Athens institute for Education and Research, conference paper series BLE 2017.

67. Kamrul Hossain, The concept of jus Cogens and the obligation under the U.N. charter, santa clara joumal of international law , vol.(3), Issue 1, 2005.

68. Karine Bannetier – Christakis , cyber diligence, A law – intensity duediligence principle for low – intensity cyber operatio ? , baltic yearbook of international – law, vol.(14) , 2014.

69. Kubo Macak, Decoding Articte of The international Law Commission's Articks on state Responsibility: Attribution of cyber

operations by Non- state Actors , journal of Conflict And Security law of ford university press, Vol.(21), No.(3), 2016.

70. Larry May, war crimes and just war, Cambridge University press, 2007.

71. Laszlo kovacs , cyber security policy and strategy in the European union and nato , national unirer sity of public service , land force academy review , No.(1) ,(89) , budast , hungary , 2018.

72. Leaders, The meaning of stuxent, The economist, 2014.

73. Lindsey Cameron and others , the update comment on the first eneve convention anew toll for generating forinter national humanitarian law , intern national review of the red cross.no 900 , 2015.

74. Rebaca Grant, In " Determining Millitary Necessity and proportionality, the commanders judgment is more critical than even, in search of law ful target's", Air force Magazine, feb, 2003.

75. Maonga, skaron keuba: Acase of in capacity : The interrogation of international (Human itarian law as a satis factory Regulator of cyber war fare, strathmor university strat hmore law school, 2017, Availableat:http://cut.ly/qigua9h. Accessed on : 7/2/2021.

76. Marco Roscini, " worldwide war fare- jusad Bellum and the use of cyber force , " Max plank year book of united Nations law, vol.(14), 2010.

77. Marco Roscini, Cyber operations and the Use of Force in international Law, oxford University press, First Editionm UK, 2014.

78. Marttilehto and Pakka Neittaan maki, cyber security: power and Technology, Newyork, 2018.

79. Mathilde simon , the Drug trade in Afghnistan: understanding Motives behind farmer's Decision to cultivate opiu peppies, foreign policy journal, November 27, 2015.

80. Maria Flemme, Due Diligence in international Law, Master thesis, Faculty of law, university of land, 2004.

81. MAX Smeets, NATO alties of fensive cyber policy: agrowing divide , The Haqu center for strategic studies, Agust 2021, availableat: http://cutt.us/sk1j.

82. Michael Gervais, cyber Attack and The law of war, Berkeley journal of international law, vol.(30), Issue 2, 2012.

83. Michael N.Schmitt , Computer network Attack and the USA of force in international law though Normative , The Colombia journal of Transitiona law, vol.(37), No.(3), 1998-1999.

84. Michael N.Schmitt, " computer Network Attack and the use of force in international Law, thought on a Normative, the colombia journal of Transitional law, 1999, vol.(37), No.3.

85. Michale Schmitt, Computer network Attack and theuse USA of force in international law though aNormative , The Colombia journal of Transitiona law,vol.(27), No.885-937, 1999.

86. Micheal N.Schmitt, " military necessity and Humanity in international Human itarian law: preserving the Delicate Blance", V.JIL, vol.50, Issue 4, university of Virginia, USA, 2010.

87. Micheal .N. Schmitt, Tallinn Manuel 2011, rule (48).

Micheal N.Schmitt (ed),Tallinn manual on the international law Applicable to cyber ware fare (Cambridge university press , 2013) at paragraph 11.

92. Micheal N.schmitt, " wired war fare: computer Network Attack and the jus in Bello in computer Network Attack and international Law, international Law studies, Vol.(76), 2002.

93. Micheal N.Schmitt, cyber operations, and the Jud Ad Bellum Revisited, Published by Villanova University Charles widger School of Law Digital Repository, Villanova Law. Review, Vol.(56), issue.(3), Unitedstate , 2011.

94. Milorad Petreski, The international public law and the use of force by states, journal of Liberty and international Affairs, vol.(1), No.(2), 2015.

95. Milton L.Mueller, Andreas Schmidt and Brenden Kuerbis: internet security and Networked Govermance in international, international studies Review 5 No.(1), 2013,.

96. Mohamed Bousoltane, Du droita al guerre au droit de la guerre: le recourse la Force armee an droit international of , Edition Dar Houma, Alger, 2010.

98. Monowar H.Bhuyan and others, Network Traffic Anomaly Detection and prevention concepts , Technigues, and tools, springer international, publishing, cham, Switzerland, 2017.

99. Myriam A.Dunn, "the internet and the changing Face", volumenuter: 7, of international Relations and Security. 2001, Bulgaria, sofia, proconltd, Issue number:1.

100. Naha jian, Human Mwchine international in Terms of Various Degress of Autonomy as well as political and Legal Responsibility for Actions of Autonomous system federal Forrignoffice.

101. NILS Melzer, cyber war fare and international law (Geneve UNIDIR Resources, 2011.

102. Nikola pijovic, the cyber space Great Game. The Five Eyes, The sino- Russian Bloc and the Growing compectition to shape Global cyber space Norms. 13 th international conferece on cyber cinflict Going viral, NATO CCDCOE publications, Tallinn, 2012.

104. Nils Melzer, inter pretive guidance on the notion of Direct participation in hostilities, under international human itarian law ICRC, 2009.

105. North Atlantic Treaty, supra note 98,artcle 4,5, NATO Agree common Approach to cyber Defence , supranot 97.

106. Olga mironeko fnerst vedt , aviation security , privacy , data protection and other human rights ; technologires and legel principles , springer , gewerbestrasse , Switzerland , 2017.

107. Oliver kempf , introduction la cyber strategie , paris , economica , 2012.

108. omer Elegab, the Legality of Non- forcible counter- Measures in international Law (oxford Monographs in international Law), 1988.

109. Oona A Hathaway , Rebeca croot of , William rerdue , philiplevitz , the law of cyber – Attacik, vol.(100), Issue4.

110. pande, Nihar Ranjan: cyber Attacks and counter measures: user perspective, (post- Graduate Diploma in cyber security), uttark hand open university , Haldwani 2016, p1, Available at; http://cutt.ly19ki28jb..

111. Papanastasiou Afroditi, Application of international law in cyber war fare operations, Research paper, university of Leicester, UK, 2010.

112. Paulo shakarian and others, introduction to cyber war fare, A Multidisciplinary Approach, Elsevier, USA , 2013.

113. Prieur Michel , Lanaly see conomigue du droit de lenvironment, BRUYLANT, BRUXELLES, 2007.

114. Randelzhofer, Article 51, in The charter of the united Nations: A Commentary 661, 664 (B.simma ed).1995.

115. Rebaca Grant, In " Determining Millitary Necessity and proportionality, the commanders judgment is more critical than even, in search of law ful target's", Air force Magazine, feb, 2003.

116. Rex Hughes, A Trealy for cyber space , international Affairs journal, vol.86, No.(2), 2010.

117. Richard P.Dimegllo, The Evolution of the just war tradition, Defining jus post bellum," military law Review, vol.(186), winter 2005.

118. Roberts . Mueller , reporton the investigation into Russian inter ference in the 2016 , U.s.depart ment of justice , vol . of II Washington , march 2019 .

119. Rupert TICEHURST, The Martens clause and the laws of armed conflict", In I.R.R.C., I.C.R.C, Thirty- seventh year, No(317), Geneva, March- April 1999.

120. Russel Buchan, cyber space, Non-state Actors and the obligations to prevent Transboundary Harm, journal of conglict and Security law, oxford university press, Vol.(21), No.(3), 2016.

121. Saalbeh, Klaus-peter , cyber war methods and practice, Germany – osnabrueck: osnabrueck university, 2019.

122. Scott j. shackelford , from Nuclear war to Netwar ; Anologizing cyber – Attack in international law , Berkeley journal of international law, vol .(27), issue1, 2009.

123. Sean P.Kanuck, Recent Devlopment: infor mation war fare: New challenges for public international law 937 Harvard international law journal, 1.274, 290, 1996.

124. Shangh cooperation agreement , annex1 . at 203 .

125. Shanjhai cooperation A Gree ment , Annexl, at 209 .

126. Shaun Roberts, cyber wars: Applying conventional laws of war to cyber war fare and Non- state Actors, Northern Kentucky law Review, 2014, vol.(41), No.(3).

127. Shin , Bromchul , the cyber warfare and the right self- defen : legal perspectives and the case of the unitedstate , IFANS , vo1 (19), No.1, 2019.

128. T.G.Retorsion, 8 MAX planck Ency Clopedia of the international Law, 976, 2012.

129. Tallainn Manual on the international Law Applicable to cyber warfare, prepared by the international , Group of experts at the invitation of the NATO cooperative cyber Defence , center of Cambridge U.K and also in New York U.S.A , 2013.

130. The international telecommunication union , itw tookit for cybercrimelegislation , Geneva , 2010.

131. The test enunciated by the ICJ in Nicaragua USA.ICJ Rep.1986, at para, 195. iF suchan operation, because of its scalea and effects, would have been classified asan armed attack.

132. Titiriga Remus, cyber Attack and international Law of Armed', journal of international , conflicts: ajus ad Bellum perspective, 2013.

133. Titiriga Remus, cyber Attack and international Law of Armed, journal of international , conflicts: ajus ad Bellum perspective, 2013.

134. U.M.Mbanaso, and E.SDandaura, the cyber space : Redefining A New, world, IOSR journal of computer engineering, center for cyber space studies , Nasarawa state unvirsity, Vol.(17), ISSUe.3 Ver. VI, Nigeria, 2015.

135. U.N.Doc.ST/LEG/SER.B/25 (2012).

136. UN, ILC, state Responsibility, Agenda items, Document AICNI.4/106, 1957.

137. United nations , manual on the prevent and control of computer – related crime , international review of criminal policy m no (43-44) , united nations publication , 1994 .

138. walter Gary sharpsr, cyber space and the use of force , Ageis Research corp,1999.

139- Zitter , Kim, sony Got Hucked Hard, 214 A vail able on websit: http://www.wried.com , accessed on : 3/12/2021

140- Kutnayeava: cyber security incentral asia, unipath- Magazin, united states central command (CENTCOM), Agust 20, 2015, Avaliable At https://cutt.lyijgu7A.

141- Christophe casa legno , codes malvaeillants ; worms lviruset bombes logigues, , Avili able on site ; http://www.Christophecasalegno.com/does/codes-malvei//ants.pdf.

[a]

Aubstract

The increasing dependence of states on the use of cyberspace has led to the emergence of a new type of conflict called cyber attacks, which are attacks in contrast to the attacks carried out by conventional weapons.

These attacks are carried out via the Internet and computers, and their remarkable spread has helped by many characteristics, including, the low material cost of the devices used to launch them, and the difficulty of identifying the identity of the information attacker, which are transnational attacks, and other characteristics that characterize them,

These attacks are also distinguished from many other attacks that may be similar to them, such as information war, information crime, information security, and information terrorism, and many researchers from legal affairs have been interested in trying to adapt these attacks, most of which are associated with international and non-international armed conflicts. including it as the use of armed force; Others tried to adapt it in the context of armed conflict in accordance with the four Geneva Conventions of 1949 and the two protocols attached to them.

Many international legal scholars and experts have worked hard to search for the suitability of these attacks to the rules and principles of international humanitarian law, whether codified or customary, and how these principles are applied to information attacks.

Today, states are facing an important challenge in the implementation of the principle of duty of care and the reason for its impact on information attacks. This principle is characterized by its customary nature, and its lack of a legal basis on which to base it. International jurisprudence was unable to find a specific definition for it, but the beginning of its application was through jurisprudence. The international judiciary, in the decision of the International Court of Justice in the Corfu Channel case of 1949, between Britain and Albania, and then followed by many judgments and judicial decisions related to the issue of environmental damage

The international community has begun to take serious steps at the global and regional levels towards developing a legal system that reveals the features of these attacks to face their dangers. Limiting its effects, such as the United States, Russia, and China, as well as regional organizations

[b]

adopted information defense strategies, such as the North Atlantic Treaty Organization (NATO) and the Shanghai Cooperation Organization.

On the other hand, many legal specialists and researchers are interested in discussing the legal bases on which these attacks are based within the framework of international conventions and covenants, in addition to customary rules that can be used to organize these attacks, and the issue of states' compliance and non-compliance with the duty of care remains a relevant issue. Importance

And the consideration of states when exercising their actions in the light of their informational sovereignty and after. The defense took the right of legitimate defense as a legal justification in it to respond to hostile information attacks. Countries began to think clearly about taking more flexible and harmonious measures when resorting to them, which are the countermeasures contained in Article (22) of the Internationally Illegal Acts of 2001 Draft.

As states seek, by resorting to countermeasures, to use their right to respond to information attacks and replace the aggressor state to fulfill its obligations to refrain from the illegal act. International responsibility, after its conditions are met, may be borne by the state or by individuals or entities working under its control and supervision.

This responsibility may be individual criminal, as is the case in the responsibility of superiors and commanders, for the actions committed by their subordinates that lead to serious violations within the framework of international humanitarian law

[c]

The Republic of Iraq
Ministry of Higher Education and
Scientific Research
University of Babylon
College of Law

The Due Diligence Duty For States to Prevent the Cyber Attacks Damage

A thesis submitted by

Jabr Yassin Laftah Rashid

to the Council of the College of Law University of Babylon
As part of the requirements for obtaining a doctorate in public law

Supervised by

Prof. Dr. Saddam Hussein Al-Fatlawy

Professor of public international law

2022 (AD) 1444 (AH)