حق الدولة في استخدام القوة في الفضاء الإلكتروني للدفاع عن النفس

الأستاذ/ مصطفى نعوس
قسم القانون الدولي
كلية الحقوق - جامعة حلب
الجمهورية العربية السورية

ملخص:

تتمثل حرب الفضاء الإلكتروني، في أشكال عدة؛ مما يقتضي عرض خطرها المحتمل الذي أصبح يشكل تهديداً مباشراً للسلم والأمن الدوليين. إضافة إلى دراسة حرب الفضاء الإلكتروني في إطار القواعد القانونية الدولية القائمة حالياً الناظمة لاستخدام القوة؛ بغية معرفة إذا ما كان يمكن تطبيق معاييرها على الحرب الإلكترونية. وأخيراً، بمعنى آخر، أيمكن تطبيق القواعد القانونية الحالية المتعلقة باستخدام القوة في الفضاء الإلكتروني عن طريق القياس أم أن الحاجة تفرض وضع إطار تنظيمي مصمم خصيصاً يلائم طبيعة حرب الفضاء الإلكتروني؟

الكلمات المفتاحية: حرب الفضاء الإلكترونية – السلم والأمن الدوليان – استخدام القوة للدفاع عن النفس.

تقديم :

تعد المعرفة والمعلومات منذ الأزل بمثابة القوة التي لا تقهر في التاريخ البشري[١]؛ فقد دفعت التقانة الحديثة [٢] وخاصة في مجال الكمبيوتر وشبكات الإنترنت الدول إلى التقدم السريع في كل المجالات الحيوية، إلا أن

الدور الأهم الذي تلعبه حالياً في إجراء التحول الجذري في شؤون الأمن القومي؛ حيث أدخلت المجتمع الدولي في حقبة جديدة في مجال حرب المعلومات[٣]، التي تعتبر الآن من أبرز أنواع القوة[٤]. في العقد الماضي تمكن أحدهم من نشر Love Bug and Sasser Viruses فيروس الحب وفيروس ساسر إلى أكثر من مليون ونصف المليون جهاز كمبيوتر[٥] على التوالي في أقل من أربع ساعات، وبسرعة أكثر بكثير من إمكانية أي دولة في العالم في الدفاع عن نفسها من الدمار الذي قد يلحق بها، وسبق أن أوضحت أكثر من عشرين دولة – من بينها الولايات المتحدة وروسيا والصين وأستراليا وعدد من دول الاتحاد الأوروبي – عزمها على الاندماج التام في حرب المعلومات بوصفها رداً غير متكافئ في أي صراع في المستقبل قد تكون طرفاً فيه[٦]، والأمثلة على حروب الفضاء الإلكتروني التي حدثت في السابق وتحدث الآن خير دليل على ما نبحث فيه؛ فقد استهدفت جرثومة إلكترونية أجهزة الكمبيوتر عائدة للمنشآت النووية الإيرانية؛ مما أدى إلى تعطيل ٤٥ ألف جهاز، يقع ٦٠ بالمائة منها داخل المنشآت النووية الإيرانية، خاصة تلك التي تعمل في إنتاج المياه الخفيفة في بوشهر في محاولة من الكيان الصهيوني لشل القدرة الإيرانية على إنتاج سلاح نووي؛ حيث لم تكن العملية الإسرائيلية ضد إيران الأولى من نوعها لمفاعل بوشهر٢٠١٠، وكذلك الصين وتايوان في عام ٢٠٠٢[(١)]، وفي عمليات حفظ السلام الدولية "عملية Belisi" التي تقودها قوات الدفاع الأسترالية عام

(١) كانت قد وقعت حادثة مشابهة، في الأحداث التي وقعت لمنظمة حلف شمال الأطلسي (الناتو) North Atlantic Treaty Organization في حالة الحرب ضد يوغوسلافيا ولكنها مختلفة نوعاً ما؛ حيث كانت بعض مرافق الفضاء الإلكتروني القائمة في بلغراد هدفاً عسكرياً مستهدفاً من قبل حلف شمال الأطلسي (الناتو) NATO2. وأخيراً في الآونة الأخيرة الصراع الإلكتروني الساخن بين الفلسطينيين والكيان الإسرائيلي، وكذلك الهجوم الذي شنته الصين على شركة جوجل في عام ٢٠٠٩، الفيروس الذي حاول ضرب مفاعل بوشهر النووي المستخدم للأغراض السلمية في إيران، وكل المواقع الإيرانية – ورقة عمل قدمت في مؤتمر كلية الهندسة المعلوماتية الدولي لأمن المعلومات ١٠/١١/٢٠١٠ – جامعة حلب – سورية.

٢٠٠١. فقد سبق للاتحاد الروسي أن شن حرباً إلكترونية ضد أستونيا في عام ٢٠٠٧ وأصابت وزاراتها ومصارفها ودوائر الأمن فيها بالشلل. ثم شنت هذه الحرب على جورجيا في عام ٢٠٠٨، وتمكن الروس من التشويش على الاتصالات بين القيادة العسكرية والوحدات التي كانت تقاتل القوات الروسية. كما تمكنوا من تضليل الطيران الجورجي؛ الأمر الذي أدى إلى الهزيمة التي لحقت بها على الرغم من كل الدعم والمساعدة التي كانت تتلقاها جورجيا من الولايات المتحدة وإسرائيل وحلف شمال الأطلسي. وفي مايو من عام ٢٠٠٧، تمكن الصينيون من اختراق جهاز المعلومات الإلكتروني الخاص في مكتب المستشارة الألمانية أنجيلا ميركل، كما تمكنوا من اختراق أجهزة عدد من الوزارات الألمانية بما فيها وزارة الصناعة ووزارة الدفاع!. وتمكن الصينيون كذلك – بحسب المعلومات الرسمية الألمانية – من ضخ ١٦٠ ميجابايت من المعلومات السرية قبل أن ينكشف أمرهم. وقد اتهمت ألمانيا الجيش الصيني بارتكاب تلك العمليات. حتى الولايات المتحدة التي تعتبر رائدة في الدفاع عن شبكة معلوماتها السرية، تعترف وزارة خارجيتها بأنها تتعرض لمحاولة الاختراق بمعدل مليوني مرة في اليوم الواحد. وأنه في كل جزء من الثانية يتعرض أحد المواقع الإلكترونية الرسمية لمحاولة الاختراق. ومن خلال السلاح الإلكتروني يستطيع «العدو» أن يخرب شبكة الاتصالات العسكرية والسياسية، وأن يشل الدورة الاقتصادية المالية والتجارية والصناعية، وأن يعطل شبكة المواصلات.. إلخ. كل ذلك من دون أن يطلق رصاصة واحدة. لقد أعدت إسرائيل نفسها لهذه الحرب، كما تشير إلى ذلك العملية التي استهدفت إيران. ونتساءل هنا: ما مدى إعداد الدول العربية نفسها أيضاً للدفاع.. وللهجوم عندما تقتضي الضرورة؟. ففي عالم يزداد اعتماداً مدنياً وعسكرياً على الشبكة الإلكترونية، فإن استهداف الشبكات الوطنية الداخلية يلحق بالدولة المستهدفة خسائر كارثية ويدفعها إلى الشلل والانهيار بسرعة ومن دون قتال. من أجل ذلك، تداعت الدول الكبرى الإلكترونية في العالم، وهي

الولايات المتحدة والصين وروسيا والاتحاد الأوروبي، إلى البحث في إعداد معاهدة جديدة تحظر استخدام السلاح الإلكتروني تكون مماثلة في جوهرها لمعاهدة حظر استخدام السلاح النووي، لما يمكن أن يلحق هذا «السلاح النظيف من خراب ودمار وشلل بالحياة المدنية العامة[٧]، ونظراً لأن شبكة الإنترنت تُكون حالياً ترابطاً عالمياً بين نظم المعلومات الحديثة في كل دول العالم، وتتميز بالسرعة العالية، فإن هذا ما جعل جميع البوابات مفتوحة، ويمكن للجميع الدخول غير المأذون به من خلالها [٨]، وتقتضي الحكمة أن تَحذر الدول من جميع الفيروسات وهجمات القراصنة المتوقعة لأن أفعالهم الإجرامية غدت عمليات حرب معلوماتية حقيقية، وتبرز ضرورة اتخاذ كل الخطوات اللازمة لتفادي هذه المخاطر في أسرع ما يمكن؛ مما يقتضي تحديد مصدر الهجمات وتتبعها وملاحقة فاعليها أينما كانوا ومحاسبتهم، أو الرد عليهم باستخدام القوة في ممارسة لحق الدفاع عن النفس. وتبعاً لذلك، نعتقد أن المعايير القانونية القائمة حالياً فيما يتعلق باستخدام الدولة لحق القوة [٩] لم تثبت بشكل كاف في تنظيم مثل هذه الحالات الفريدة والقلقة جداً [١٠] من حرب المعلوماتية. وكما يقول الفقيه أنطوني داماتو: أعتقد أن هناك نوعاً من روح القانون الدولي، وهذه الروح هي التطورية. وإدراكاً منا لأنها تعطينا أساساً للتوقع كيف يمكن لقواعد القانون الدولي أن تتغير لتتناسب مع الأوضاع الجديدة[١١]. وقد نصح البروفيسور يورام دنشتين [12] Yoram Dinstein بعقد مؤتمر دولي لتحديث القواعد القديمة الإنسانية للحرب، وأن القواعد الحالية من نوع التشريعات الدولية سوف تخدمنا جيداً إذا كان لنا ما يكفي من تطبيقها كما هي مكتوبة. إلا أننا نميل إلى الاتجاه الذي يدعو إلى تطوير القواعد الدولية مع الأوضاع الجديدة. وعلى ما يبدو هناك حاجة للحصول على إجابات تستند إلى مبادئ القانون الدولي وقواعده[١٣] هذه النوعية من الأسئلة قد طرحها بعض الفقهاء[١٤]

الذين توقعوا إمكانية استخدام الفضاء الإلكتروني كساحة معركة في القرن الواحد والعشرين .وبناءً على ما تقدم،سنقوم بتقسيم هذه الدراسة إلى أربعة مطالب على نحو ما يلي:

المطلب الأول: حرب المعلومات والدفاع المشروع.

المطلب الثاني: حق الدول في استخدام القوة دفاعاً عن النفس في القضاء الإلكتروني.

المطلب الثالث: حرب المعلومات والحاجة إلى إيجاد تنظيم قانوني جديد.

المطلب الرابع: دور المؤتمرات والاتفاقيات والمنظمات الدولية في تنظيم حماية الفضاء الإلكتروني.

المطلب الأول
حرب المعلومات والدفاع المشروع

تدخل المجموعة الأولى من المبادئ القانونية التي تتعلق بتنظيم حرب الفضاء الإلكتروني في مجال القواعد القانونية الدولية الحديثة(٢)، وبشكل عام في إطار القانون الدولي العرفي[١٥]. تتأصل المعايير القانونية الدولية الحديثة في مجال الدفاع عن النفس أساساً في ميثاق الأمم المتحدة، وتطبق على جميع الهجمات العدوانية التي قد ترتكبها إحدى الدول أو أحد الكيانات والتنظيمات من غير الدول. ونتيجة لذلك، فإن الهجمات العدوانية المتمثلة في الحرب الإلكترونية التي قد تبدؤها بعض الأطراف من الدول أو من غير الدول، لن تدخل في إطار الأحكام المنصوص عليها في ميثاق الأمم المتحدة حتى إذا ثبت تورط أي طرف

(٢) القضية المتعلقة بالأنشطة العسكرية وشبه العسكرية في نيكاراغوا وضدها قرارات، [١٩٨٦] محكمة العدل الدولية.

مباشرة أو بشكل غير مباشر في تنفيذ مثل هذه الهجمات. بالإضافة إلى ذلك، ووفقاً للمادة ٥١ من الميثاق، يتعلق الإطار التنظيمي من ميثاق الأمم المتحدة[٣] فيما يتصل بأعمال الدفاع عن النفس فقط بالقوة التي تصنف على أنها هجوم مسلح [١٦]، في حين قد لا يكون التسلل إلى أجهزة الكمبيوتر غير المصرح به كبيراً ومن القوة بما يكفي لتصنيفه ضمن بند "الهجمات المسلحة"، ولا بد أن يقع هجوم مسلح حتى يندرج في ظل أحكام ميثاق الأمم المتحدة ونصوصه[١٧]، وقد يكون من الصحيح الاستنتاج القائل: إن الإشارات الإلكترونية لا تشبه القنابل والرصاص، أو القوات أو أي نوع من الأنواع الأخرى من الأسلحة التقليدية. لذلك نرى أن المجتمع الدولي لم يكن لديه أية مشكلة في اعتبار استخدام الأسلحة الكيميائية أو البيولوجية يقع تماماً ضمن تعريف الهجوم المسلح، على الرغم من كون هذه الأسلحة غير قابلة للكشف بوساطة الحواس البشرية المجردة. وهذا يتفق مع وجهة النظر التي تؤيد، أن الأسلحة المستخدمة من قبل مرتكب الهجوم المسلح أمر لا أهمية له، كون المادة ٥١ لا تشير إلى استخدام أية أسلحة محددة، وهذا الأمر ينطبق على أي هجوم مسلح بصرف النظر عن نوع الأسلحة الموظفة في ذلك الهجوم. لذلك ووفقاً لصياغة المادة ٥١، فإن المجتمع الدولي سيوافق على القبول مستقبلاً باعتبار الهجوم بالأسلحة المعلوماتية يشكل هجوماً مسلحاً تبعاً لنتائجه المحتملة، وبغض النظر عن الآلية المستخدمة في إحداث هذه النتائج. لأنه في

(٣) المادة ٢- تعمل الهيئة وأعضاؤها في سعيها وراء المقاصد المذكورة في المادة الأولى وفقاً للمبادئ الآتية: ١ - تقوم الهيئة على مبدأ المساواة في السيادة بين جميع أعضائها. ٢ - لكي يكفل أعضاء الهيئة لأنفسهم جميعاً الحقوق والمزايا المترتبة على صفة العضوية يقومون في حُسن نية بالالتزامات التي أخذوها على أنفسهم بهذا الميثاق. ٣ - يفض جميع أعضاء الهيئة منازعاتهم الدولية بالوسائل السلمية على وجه لا يجعل السلم والأمن والعدل الدولي عُرضة للخطر.٤ - يمتنع أعضاء الهيئة جميعاً في علاقاتهم الدولية عن التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو على أي وجه آخر لا يتفق ومقاصد «الأمم المتحدة».

حالة وقوع هجوم معلوماتي مركز سينجح في إغلاق نظام مراقبة الحركة الجوية للدولة مثلاً، بالإضافة إلى إغلاق الخدمات المصرفية والنظم المالية وكذلك المرافق العامة، ويمكن أن يشمل تأثير الحروب المعلوماتية – مثلاً – على فتح الباب على مصراعيه للسدود المغلقة إلكترونياً؛ الأمر الذي يتسبب في حدوث فيضانات عامة حادة، ووقوع الآلاف من القتلى المدنيين نتيجة لذلك ووقوع خسائر وأضرار بالممتلكات العامة والخاصة.

إن الميزة الأساسية في ميثاق الأمم المتحدة هي اللغة المحددة التي استخدمها واضعو[٤] المواد فيما يتعلق بتنظيم الظروف الدقيقة التي بموجبها يحق للدول اللجوء إلى القوة المضادة، وأهم عنصر فيها، هو تفويض مجلس الأمن بتفسير مصطلح الهجوم المسلح، وفي الوقت نفسه، فإن استخدام مصطلح الهجوم المسلح يعني القبول به، والأمر الذي يشير إلى تفسيرها بشكل صحيح من قبل محكمة العدل الدولية هو قضية نيكاراغوا؛ حيث يفسر قرارها بأنه لا يوجد صك قانوني قادر على تنظيم جميع الجوانب المتعلقة بأي حق قانوني معين أو بوصف حالته الراهنة بشكل كامل ومباشر. وهذا مما يعطي مجلس الأمن صلاحيات واسعة عند التعاطي مع مسألة حرب المعلومات.

ولقد واجه المجتمع الدولي حالات مماثلة في الماضي مع ظهور الابتكارات التكنولوجية فيما يتعلق بمسألة تنظيمها مثل الطائرة، والأسلحة البيولوجية

(٤) إن مفهوم القصد والدافع فيما يتعلق بتصنيف هجوم معين على أنه "هجوم مسلح" يبقى غامضاً ومثيراً للجدل، ومن دون حل، ومن ثم ينبغي أن نتعامل معه بحذر شديد. وفي الواقع، أصبح الجدل الدائر حول هذه المسألة على درجة عالية من الوضوح وخاصة في أثناء المداولات لصياغة تعريف للعدوان، وكان هناك خلاف أساسي على الرغم من المناقشات الطويلة والساخنة المتعلقة بالموضوع نفسه، وتم التوصل في نهاية المطاف، إلى أن هذا الفعل يمكن أن يشكل عملاً من أعمال العدوان فقط إذا كان استخدام القوة فيه متعمداً أو إذا ما كانت هناك نية للدولة ولو جزئياً لارتكاب العدوان.

والكيميائية، وأخيراً الانشطار النووي. إلا أنه تمكن من وضع حد لها وتنظيمها، وجعلها أداة فعالة للغاية في حفظ السلم أو الحرب، وكانت بعض الأسلحة مثل الطائرات الحربية والمواد الكيميائية موضوعاً للتنظيم القانوني الدولي فيما يتعلق بآثارها المدمرة المحتملة إذا استخدمت كوسيلة للحرب.

ويتحتم على جميع القواعد القانونية أن تتكيف وأن يتم تطويعها لتتلاءم بشكل مستمر مع الظروف الجديدة، وبعبارة أخرى –كما يرى الأستاذ كلسن– تكون هذه القواعد مرنة بما فيه الكفاية للتعامل حتى مع كل الحالات والظواهر الجديدة.

ونضيف: إن ميثاق الأمم المتحدة يمنع استخدام القوة بين الدول وفقاً للمادة ٢ (٤)[١٨] من الميثاق التي تنص على أنه "يمتنع على أعضاء الهيئة جميعاً في علاقاتهم الدولية عن التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو على أي وجه آخر لا يتفق ومقاصد الأمم المتحدة". وأكد الفقه القضائي هذا الأمر في عدة قرارات لمحكمة العدل الدولية في فتواها في عام ١٩٩٦ بشأن مشروعية التهديد أو استخدام الأسلحة النووية، وكذلك الفتوى في قضية قناة كورفو [١٩].

ويفهم من هذه الصيغة الواسعة لهذه المادة من الميثاق أن هذا الحظر شامل لأي استخدام أو تهديد باستخدام القوة من دون أي استثناء على الإطلاق، بما في ذلك الأعمال التي تعتبر أقل ضخامة من الحرب الشاملة، وكذلك تلك التي قد تقع خارج نطاق التعريف التقليدي للهجوم المسلح. وهذا النطاق خاص بحكم المادة ٢ (٤)، ولقد تم توضيحها بالإجماع من قبل الجمعية العامة للأمم المتحدة في القرار٢٦٢٥[٢٠] المتعلق بإعلان مبادئ القانون الدولي حول علاقات الصداقة والتعاون بين الدول والقرار ٣٣١٤ [٢١] المتعلق بتعريف العدوان؛ حيث اندمجت العبارات الواردة في المادة ٢ (٤) من الميثاق مع قرارات الجمعية العامة ٢٦٢٥ و ٣٣١٤ على أن السمة الرئيسية للمرحلة التي يستطيع مجلس الأمن التدخل فيها هي التي يكون فيها "الفعل المجرم" عملاً من شأنه أن يشكل تهديداً للأمن والسلم الدوليين، ويعتبر من ثم غير قانوني، وهنا نلاحظ

أنه حتى يعتبر الانتهاك واضحاً للقانون الدولي في موضوع حرب المعلومات، يجب أن يشكل الفعل تهديداً للأمن والسلم الدوليين، وينفرد نص الميثاق هنا باهتمامه بالنتائج الحاصلة وليس بالوسائل المعتمدة لتحقيق مثل هذه النتائج التي يستخدمها الجناة مرتكبو الفعل. لذا فهو يقف على السبب الذي يمكن أن يكون هناك عمل قسري ويعفيه قانوناً من النظام الرقابي عليه وفقاً لأحكام المادة ٢ (٤)، فلمجرد كون هذه الهجمات ذات طبيعة تكنولوجية متقدمة وأدت إلى نتائج وخيمة بدولة ما، نرى أن تعتبر أعمالاً تدخل في نطاق الأفعال التي من شأنها أن تشكل تهديداً للأمن والسلم الدوليين، ويمكن تطبيق القواعد القانونية المنصوص عليها في القانون الدولي على حرب المعلومات[٢٢] ويوجد نوعان من الاستثناءات الواردة على الحظر العام لاستخدام القوة المنصوص عليها في المادة ٢ (٤) من الميثاق، هما: تدخل مجلس الأمن، وحالة الدفاع المشروع.

الفرع الأول
قرار مجلس الأمن بالتدخل

ويتجسد الاستثناء الأول: في المادة٣٩ [٢٣] من ميثاق الأمم المتحدة التي تسمح لمجلس الأمن أن يقرر بموجب الفصل السابع(٥) ما يتخذ من الأعمال في حالات تهديد السلم والأمن الدوليين ووقوع العدوان، ويقرِّر مجلس الأمن إذا ما كان قد وقع تهديد للسلم أو إخلال به أو كان ما وقع[٢٤] عملاً من أعمال العدوان، ويقدِّم في ذلك توصياته أو يقرِّر ما يجب اتخاذه من التدابير طبقاً لأحكام المادتين ٤١ و ٤٢ لحفظ السلم والأمن الدولي أو إعادته إلى نصابه.

(٥) الفصل السابع: فيما يُتخذ من الأعمال في حالات تهديد السلم والإخلال به ووقوع العدوان، المادة ٣٩: يقرِّر مجلس الأمن إذا ما كان قد وقع تهديد للسلم أو إخلال به أو كان ما وقع عملاً من أعمال العدوان، ويقدِّم في ذلك توصياته أو يقرِّر ما يجب اتخاذه من التدابير طبقاً لأحكام المادتين ٤١ و ٤٢ لحفظ السلم والأمن الدولي أو إعادته إلى نصابه.

ويفوض القيام بالعمل القسري وفقاً للمادتين ٤١ و ٤٢؛ حيث تنص المادة ٤١ على ما يأتي: "لمجلس الأمن أن يقرِّر ما يجب اتخاذه من التدابير التي لا تتطلب استخدام القوات المسلحة لتنفيذ قراراته، وله أن يطلب إلى أعضاء «الأمم المتحدة» تطبيق هذه التدابير. ويجوز أن يكون من بينها وقف الصلات الاقتصادية والمواصلات الحديدية والبحرية والجوية والبريدية والبرقية واللاسلكية وغيرها من وسائل المواصلات وقفاً جزئياً أو كلياً، وقطع العلاقات الدبلوماسية. والقرار ٤٢٢٠ اللاحق لما هو منصوص عليه في الشروط التي تعتبر واسعة للغاية من المواد سالفة الذكر، ولا سيما في المادة ٤٢ التي تنص على ما يأتي: إذا رأى مجلس الأمن أن التدابير المنصوص عليها في المادة ٤٢ لا تفي بالغرض أو ثبت أنها لم تفِ به، جاز له أن يتخذ بطريق القوات الجوية والبحرية والبرية من الأعمال ما يلزم لحفظ السلم والأمن الدولي أو لإعادته إلى نصابه. ويجوز أن تتناول هذه الأعمال المظاهرات والحصر والعمليات الأخرى بطريق القوات الجوية أو البحرية أو البرية التابعة لأعضاء «الأمم المتحدة»؛ حيث لا توجد قيود من أي نوع فيما يتعلق بدقة طبيعة "التدابير القسرية" التي قد يتخذها مجلس الأمن[٢٤]. وبناء على ذلك، يمكن السماح باتخاذ "الإجراءات القسرية"، في مجال حرب الفضاء الإلكتروني، وتقع كذلك ضمن حدود العمل المسموح بها للأحكام ذات الصلة بالقرار ٤٢٢٢[٢٥].

الفرع الثاني
حق الدول في الدفاع الفردي أو الجماعي عن النفس

والاستثناء الثاني الوارد في ميثاق الأمم المتحدة هو الحق في الدفاع الفردي والجماعي عن النفس على النحو المبين في المادة ٥١ التي تنص على أنه ليس في هذا الميثاق ما يُضعف أو يُنقص الحق الطبيعي للدول، فرادى أو جماعات، في الدفاع عن أنفسها إذا اعتدت قوة مسلحة على أحد أعضاء «الأمم المتحدة»، وذلك إلى أن يتخذ مجلس الأمن التدابير اللازمة لحفظ السلم والأمن الدولي، والتدابير التي اتخذها الأعضاء استعمالاً لحق الدفاع عن النفس تبلَّغ إلى

المجلس فوراً، ولا تؤثر تلك التدابير – بأي حال – فيما للمجلس – بمقتضى سلطته ومسؤولياته المستمرة من أحكام هذا الميثاق – من الحق في أن يتخذ في أي وقت ما يرى ضرورة لاتخاذه من الأعمال لحفظ السلم والأمن الدولي أو إعادته إلى نصابه. ويجب عدم تفسير مصطلح "المسلحة" في نص المادة على أنه تقييد لاستخدام الحق؛ لأنه من المهم أن نأخذ هذا في الاعتبار لأن المادة ٥١ لا تعرض الحق في الدفاع عن النفس لأول مرة في الميثاق، ولكن تكرسه؛ لأنه حق معترف به منذ فترة طويلة، ويعتبر مفهومه في الواقع أوسع بكثير من الصيغة التي يستخدم بها في نص هذه المادة[٢٦]. وهذا يتطابق مع المفهوم الحقيقي الفعلي للهجمات المسلحة، التي في معظم الحالات لا تشمل فقط الأسلحة العسكرية التقليدية والتكتيكات.

وتعتبر عمليات حرب المعلومات حالياً المثال الحي لشكل من أشكال الهجوم المسلح التي تم تطويرها حديثاً، وعلى الرغم من كونها قادرة على إحداث دمار واسع النطاق فإنها حالياً لا يشملها التعريف التقليدي للمصطلح «هجوم مسلح» في الواقع، بقدر ما يتعلق الأمر بحرب الفضاء الإلكتروني، ومن خلال استعراض صيغة المادة ٥١، فإن السؤال الحاسم هو: هل يمكن إدراج مفهوم "هجوم حرب المعلومات " تحت تصنيف الهجوم المسلح الذي يبرر اللجوء إلى العمل الدفاعي القسري[٢٧]؟ ومن خلال التركيز على الوسائل المستخدمة في هجوم حرب المعلومات يمكن للمرء أن يستنتج بأنه يمكن للإشارات الإلكترونية أن تشبه القنابل وطلقات الرصاص والقذائف وأية أنواع أخرى من الأسلحة التقليدية إذا كان لديها التأثير نفسه، والمجتمع الدولي حالياً قلق جداً من العواقب الوخيمة التي قد تنجم عن حرب الفضاء الإلكتروني(٦)، وخاصة إذا ما تسببت في إحداث خسائر بشرية[٢٨]. ونرى أن هذا الميثاق

(٦) هذا ما عبر عنه رئيس الاتحاد الدولي للاتصالات في مؤتمر المنتدى الاقتصادي العالمي٢٠١٠ في مدينة دافوس – سويسرا وكذلك كلاوس شواب الرئيس التنفيذي ومؤسس المنتدى الاقتصادي العالمي. إن الأضرار التي قد تنجم عن حرب الفضاء الإلكتروني قد تتجاوز أضرار كارثة تسونامي.

سيكون مميزاً إذا ما اعتبر هجوم الحرب المعلوماتية من خلال التحليل القانوني أنه يدخل ضمن تصنيف "الهجوم المسلح".

وباعتبار أن الميثاق ينظم المواد التي يحق بموجبها للدول أن تلجأ إلى استخدام القوة في الفصل التنظيمي، نرى أنه يجب ألا ينظر إليه من وجهة نظر تقييدية محضة، بل يجب أن يكون قادراً على إعادة إدراج العديد من المفاهيم الحديثة مثل مفهوم حرب المعلومات وغيرها من المفاهيم والنص عليها بالكامل بشكل مباشر لتشمل نصوصه جميع هذه الجوانب وتغطيها بشكل قانوني سليم[٢٩].

المطلب الثاني
حق الدول في استخدام القوة دفاعاً عن النفس في الفضاء الإلكتروني

تتسم المجموعة الثانية من المبادئ القانونية بأهمية كبرى بالنسبة إلى تنظيم حرب الفضاء الإلكتروني في مختلف الصكوك والوثائق القانونية الدولية التي تتضمن قواعد قانونية، يمكن أن تدعم حق الدول في استخدام القوة في الفضاء الإلكتروني دفاعاً عن النفس.

الفرع الأول
حرب المعلومات وقواعد الحرب الآمرة

تعد قواعد الحرب الآمرة واحداً من أهم المبادئ الأساسية التي يمكن أن تكون قابلة للتطبيق مستقبلاً على وسائل شن حرب معلومات؛ حيث يبدأ تطبيق هذه القواعد من بداية بدء الأعمال العدائية بين المتحاربين [٣٠]، وذلك بهدف أساسي يكمن في وضع بعض المعايير الدنيا لحماية المدنيين والعسكريين من أجل منع المعاناة غير الضرورية والتدمير[٣١]، كما كرسته قواعد القانون الدولي الإنساني.

ويحكم قانون الحرب مبدآن، هما الضرورة العسكرية، والتناسب، والضرورة تستوجب بصورة قانونية فقط الأهداف العسكرية حصراً وما يتصل بها من البنية التحية الوطنية الحيوية [٣٢]، وقد يكون هناك هجوم أحياناً على الأهداف التي ليست من طبيعة عسكرية، ويكون شرعياً إذا كان هجوم الدولة المهاجمة على دولة أخرى فقط من أجل عرض مزاياها العسكرية من هذا الهجوم[٣٣] أو شيء من هذا القبيل، ويمكن من ثم تطبيق هذين المبدأين على حرب المعلومات والاستفادة منهما.

وهناك مبدأ إضافي من القواعد الآمرة "في الحرب" يمكن أن ينطبق مباشرة على حرب الإنترنت هو "التمييز بين المقاتلين وغير المقاتلين"، وهو شرط مهم جداً فيما يتعلق بعمليات حرب المعلومات، ويحتاج إلى إذن شرعي لاتخاذ الإجراءات القسرية في أثناء وجود النزاع الدولي[٣٤]، في حال قيام بعض الأفراد بهجوم وشن حرب إلكترونية، فهؤلاء المهاجمون يقعون خارج نطاق التعريف القانوني للمقاتلين وسيصبحون أهدافاً عسكرية مشروعة، ويكونون أيضاً عرضة للملاحقة الجنائية، وكذلك ترتيب مسؤولية الدولة التي ينتمون إليها وسيكونون منتهكين لقانون الحرب [٣٥]، ويمكن تطبيق مبادئ أخرى على الحرب الإلكترونية، هي تلك التي تحظر استخدام الأسلحة التقنية ووسائل الحرب التي يمكن أن تسبب إصابات زائدة ومعاناة لا داعي لها وتلحق أضراراً في المدى البعيد بالبيئة[٣٦]. إن تطبيق هذا المبدأ – خاصة في عمليات الحرب الإلكترونية – له أهمية خاصة(٧)، حيث يتعرض مجموع شبكات المعلومات الحديثة المترابطة لأضرار جانبية بشدة، وقد تكون ناجمة عن أسلحة الحرب الإلكترونية التي تستخدم عشوائياً [٣٧]، ونرى أنه سيكون ملزماً التحديد القانوني بأن أياً من هذه الوسائل محظورة بأي شكل من الأشكال من قبل القانون الدولي [٣٩]، وتحتاج عمليات حرب المعلومات أيضاً إلى الامتثال

(٧) ملاحظة من الباحث: هجوم حرب المعلومات استهداف كبير للمدنيين وللمنشآت الحيوية والكيميائية أو لسدود توليد الطاقة الكهربائية، ويعتبر ذلك تجاهلاً تاماً للمبادئ التي وضعتها القواعد الآمرة "في الحرب": سوف تقع هذه الهجومات ضمن المعايير المذكورة أعلاه من خلال ما تسببه من أضرار جسيمة للأشخاص والبيئة.

للقواعد الآمرة "في الحرب"(٨) التي تقضي بإعمال مبدأ الفروسية والشرف وعدم اللجوء إلى أسلوب الغدر، ومهما كانت التقنيات الحربية المستخدمة فلا يجوز استخدامها[٤٠].

المبدأ الأخير من "قواعد الحرب الآمرة" الذي ينطبق على عمليات حرب المعلومات هو مبدأ الحياد الذي ينص على ما يأتي: أولاً، يلزم المحاربون قانوناً باحترام حقوق وأراضي الدول المحايدة في أي صراع بينهما، وثانياً، منع الدول المحايدة – بكل الوسائل الضرورية، بما في ذلك استخدام القوة – من استخدام أراضيها من قبل أحد الأطراف المتحاربة، وثالثاً، امتناع الدول المحايدة عن تقديم المساعدة بأي طريق للأطراف المتحاربة. وتكمن أهمية هذه القاعدة القانونية – ولا سيما فيما يتعلق بالحرب الإلكترونية – في أن المعتدين المحتملين من المرجح أن يكونوا دائماً متخفين عند الهجوم الإلكتروني ويوجهون ضرباتهم من خلال واحدة من شبكات المعلومات المتصلة والموجودة في أكثر من دولة، وقد تتدخل أحياناً بعض الدول المحايدة للمساعدة دون موافقة أو معرفة من الدول الأخرى أو شيء من هذا القبيل.

الفرع الثاني
حرب المعلومات وقانون الفضاء الخارجي

هناك فرع آخر في القانون الدولي يمكن أن يضم عدداً قليلاً من القواعد القانونية القابلة للتطبيق على الحرب الإلكترونية هو قانون الفضاء. ينبع هذا الانطباق أساساً من حقيقة أن الشبكات العالمية، والجوانب الرئيسية لتكنولوجيا المعلومات الحديثة، تعتمد على منصات فضائية متعددة تدور حول الأرض من أجل دعم المحطات الأرضية[٤١]، وفضلاً عن ذلك، تعتبر هذه المنصات الفضائية غاية في

(٨) ملاحظة من الباحث: مرة أخرى، يتعلق الغدر باستخدام الرموز البصرية أو الإلكترونية التي تستخدم لتحديد هوية الأشخاص والممتلكات المحمية من الهجوم من أجل جعلها هدفاً مشروعاً للهجوم العسكري أيضاً.

الأهمية في عمليات حرب المعلومات؛ وذلك لسببين، الأول: تعتبر هذه المنصات من العناصر الأكثر ضعفاً في نظام المعلومات؛ لأنه يستحيل صد أي هجوم قد يقع عليها، والثاني: أنها كذلك تمثل القوة الأكثر حيوية ومقدرة لأي دولة تريد القيام بعمليات حرب معلوماتية بشكل ناجح، ومن ثم ستكون هذه المنصات الفضائية مشتركة بالضرورة في صلب أي حرب معلوماتية رئيسية معاصرة سواء لعملية دفاعية أو هجومية[٤٢]. ومن ثم يمكن أن تندرج عمليات حرب المعلومات في إطار القواعد القانونية التي تنظم الأنشطة في الفضاء والتي صيغت في الغالب في معاهدة الفضاء الخارجي منذ عام ١٩٦٧[٤٣]؛ إذ تعد هذه المبادئ معتمدة وملزمة في المجتمع الدولي وتعتبر من قبيل القانون [٤٤] الدولي العرفي، أولاً وقبل كل شيء: لا تزال أنشطة حرب المعلومات في الفضاء الخارجي تخضع للإطار القانوني القائم حالياً الذي ينظم استخدام القوة. ثانياً، مشاركة جميع الدول في أنشطة حرب المعلومات في الفضاء الخارجي تتوجب الامتناع عن التسبب في أي تدخل يمكن أن يكون ضاراً مع أنشطة الدول الأخرى. ثالثاً: تتحمل الدول المشاركة في أنشطة حرب المعلومات المسؤولية الدولية عن جميع هذه الأنشطة التي تقوم بها في الفضاء الخارجي، وبغض النظر عن هذه الأنشطة إذا ما كانت تقوم بها الحكومات أوالكيانات الأخرى غير الحكومية، ونستطيع أن نأخذ مثالين من الصكوك التنظيمية المتخصصة في القانون الدولي للفضاء الخارجي(٩) مع التطبيق المباشر على عمليات حرب المعلومات [٤٥]، وهما اتفاقيات إنتلسات [٤٦] واتفاقيات إنمارسات[٤٧].

(٩) حدد اتفاق إنتلسات الإطار التنظيمي لإنشاء وتشغيل منظمة إنتلسات، وهو المسؤول عن كوكبة من الأقمار الصناعية للاتصالات تربط بين مختلف الاتصالات الأرضية الثابتة. يتألف إنتلسات من جزأين، الأول: مستقل ومسؤول عن تقديم خدمات الاتصالات العامة، والثاني: مسؤول عن توفير خدمات الاتصالات السلكية واللاسلكية المتخصصة. وفق ما هو منصوص عليه في الاتفاق فإن إنتلسات هو فقط الجزء الخاص بتقديم خدمات الاتصالات العامة التي تستخدم لأغراض عسكرية، بما في ذلك عمليات حرب المعلومات. ينظم اتفاق إنمارسات المنظمة الدولية التي تسيطر على عدد كبير من الأقمار الصناعية وتوفير وصلات الاتصالات السلكية واللاسلكية بين المنشآت الأرضية المتحركة، على النحو المنصوص عليه في المواد ذات الصلة من الاتفاق، ويمكن استخدام موارد إنمارسات للاستخدامات العسكرية المشروعة كافة، التي تشمل عمليات حرب المعلومات.

الفرع الثالث
حرب المعلومات وقانون البحار

نصت اتفاقية الأمم المتحدة لقانون البحار لعام ١٩٨٢ على عدة قواعد قانونية يمكن أن تنطبق على أنشطة حرب المعلومات [٤٨]. أولها: أن الاتفاقية تنص على أن جميع السفن البحرية تستطيع استخدام حق المرور البريء في المياه الإقليمية للدولة ويجب الامتناع عن المشاركة في الأنشطة التي تضر بالسلام وحسن النظام والأمن في الدول الساحلية؛ حيث يمكن لكل واحدة من سلسلة قوائم الاتفاقية المحددة للأنشطة "الضارة" أن تكون جزءاً رئيسياً(١٠) لا يتجزأ من عمليات الحرب الإلكترونية[٤٩]، وعلاوة على ذلك، تدعو الاتفاقية جميع الدول للتعاون في مجال قمع البث غير المصرح به من أعالي البحار[٥٠]، في حين يستغرق أيضاً عدة خطوات لضمان ملاحقة مرتكبي البث غير المصرح به من أعالي البحار. وأخيراً، فإن الاتفاقية تنص أيضاً على حماية الكوابل الغواصة.

الفرع الرابع
حرب المعلومات وقانون الاتصالات

يعد قانون الاتصالات فرعاً من القانون الدولي الذي يمكن أن تطبق قواعده القانونية على عمليات حرب المعلومات. ويجري تعيين هذه القواعد القانونية المنصوص عليها في الاتفاقية الدولية للاتصالات[٥١]؛ حيث تسمح الاتفاقية بقطع أي اتصالات سلكية أو لاسلكية قد تظهر بأنها قد تشكل خطراً على أمن أي دولة طرف في الاتفاقية، وعلاوة على ذلك، يحق للدول تعليق جميع خدمات الاتصالات

(١٠) الأنشطة الضارة المشار إليها في المادة ١٩ هي: (أ) أي تهديد أو استخدام القوة ضد سيادة وسلامة الأراضي أو الاستقلال السياسي للدولة الساحلية، أو على أي وجه آخر لا يتفق مع المبادئ الواردة في ميثاق الأمم المتحدة، (ب) أي عمل يهدف إلى جمع المعلومات والمساس بالدفاع، أو أمن الدولة الساحلية، (ج) أي عمل من أعمال الدعاية التي تهدف إلى التأثير في الدفاع أو أمن الدولة الساحلية، (د) أي عمل يهدف إلى التداخل مع أي من أنظمة الاتصالات أو أي تسهيلات أخرى من الدولة الساحلية.

الدولية لمدة غير محدودة لأسباب تتعلق بالأمن الوطني، وتقوم على الفور بإخطار الأمين العام للأمم المتحدة. وينبغي بالإضافة إلى ذلك، وضع جميع المحطات اللاسلكية وتشغيلها بطريقة لا تتسبب بتداخلات ضارة للغير. في نهاية المطاف، وكما هو منصوص عليه حول حرب المعلومات ذات الصلة، يحق للدول الأطراف في الاتفاقية الاحتفاظ بحرية مطلقة فيما يتعلق باحتمال استخدام منشآتها الاتصالاتية العسكرية ما دامت تتخذ جميع الخطوات اللازمة لمنع أي تدخل ضار.

الفرع الخامس
حرب المعلومات والقانون الدولي الاتفاقي

يعد قانون المعاهدات من أهم الفروع في القانون الدولي الممكن تطبيق قواعده على عمليات حرب المعلومات، ويرجع ذلك إلى أن المعاهدات تمثل الوسيلة الأساسية التي يتعامل بها أعضاء المجتمع الدولي في مختلف المجالات فيما بينهم [٥٢]. وفي حال قيام الحرب ثمة تساؤل يطرح، هو: هل بالإمكان تطبيق أحكام المعاهدة بين الدول المتحاربة في زمن الحرب؟ فعندما لا يتم ذلك سيكون الموضوع رهناً "بقواعد الحرب الآمرة"، ومن ثم يمكن تطبيق قواعد الحرب على حرب المعلومات، كما أشرنا [٥٣]. وعند تطبيق أحكام الاتفاقيات والمعاهدات يمكن أن تكون هناك بضعة جوانب من قانون الاتفاقات الدولية التي يمكن تطبيقها بشكل مباشر على سير عمليات حرب المعلومات[٥٤]. مثل معاهدات تسليم المجرمين، وكذلك على اتفاقيات المساعدة القضائية وهي الأكثر أهمية، خاصة التعاون بين الدول في الوسائل المتاحة لاتخاذ إجراءات صارمة ضد مرتكبي جرائم التسلل إلى أجهزة الكمبيوتر التي تبدو وكأنها غير مصرح بها في معظم الدول، ولأنه في الحالات التي يكون فيها (التسلل للكمبيوتر غير مصرح به) غير محدد بوصفه عملاً إجرامياً، ستحجم الحكومات عن تقديم مثل هذه المساعدة القضائية في جميع الأشكال المتعلقة به، وهذا ما ساهمت في تحديده وتوضيحه الاتفاقية الأوروبية للجرائم المرتكبة عبر الإنترنت ٢٠٠١، من خلال تحديد الإجراءات وآليات التعاون بين الدول في مجال مكافحة الإجرام عبر

الإنترنت [٥٥]، ومن ثم، فإنه من الأهمية الكبرى تصور كل من الأنواع المذكورة من المعاهدات في مثل هذه الطريقة وكأنها تغطي بعض أنشطة حرب المعلومات، سواء من خلال توسيع هذه الاتفاقيات بما فيه الكفاية لتدارك الموقف المطلوب، أو من خلال إدراج أحكام محددة تهدف إلى تنظيم الحرب الإلكترونية.

وتشمل الاتفاقيات الدولية التي تنظم الطيران المدني أيضاً أحكاماً تنظم سلوك حرب المعلومات. أولاً، تعتبر جميع الدول ملزمة، في جميع الظروف، مراعاة الشروط الواجب توافرها من أجل سلامة الملاحة بالنسبة إلى الطائرات المدنية وعدم التدخل بأي شكل من الأشكال في السلامة الأمنية لها، ويحظر على الدول اللجوء إلى استخدام جميع أنواع الأسلحة ضد الطيران المدني. وعلاوة على ذلك – كما هو منصوص عليه في المعاهدات التي تنظم العلاقات الدبلوماسية – يجب على أعضاء المجتمع الدولي عدم المشاركة بأي شكل في أنشطة حرب المعلومات التي تنال من الموظفين الدبلوماسيين أو المباني أو المعدات، وأن يؤخذ في الاعتبار أن الموظفين الدبلوماسيين أو المباني أو المعدات لا يمكن أن تكون هدفاً لأي من هذه الأنشطة(١١)؛ لأنها لا تستخدم إلا بما يتفق مع الأغراض الرسمية بشكل دقيق[٥٦]، وتمثل الاتفاقيات النوع الأخير من الاتفاقات الدولية التي تتحمل صلة مباشرة بتنظيم عملية حرب المعلومات. وتشترط هذه الاتفاقيات جعل جميع عمليات حرب المعلومات التي قد تبدؤها القوات العسكرية المرابطة في الخارج للشروط القانونية التالية: (أ) إذا ما كانت الدولة المضيفة قد قامت بالإخطار قبل البدء بأي عملية حرب معلومات، (ب) إذا ما كانت المعدات الفعلية التي تنطوي عليها أية معلومات معينة سوف تكون العملية الحربية في خرق التزام قانوني محدد بموجب اتفاق معين، (ج) إذا

(١١) مصطلح "الغرض المزدوج" الذي يتم استخدامه هنا في صورتها الكلاسيكية الأمن القومي معنى القانون الذي يكون الأكثر شيوعا في النظام للدلالة على التكنولوجيات التي يمكن استخدامها مع فعالية متساوية لكلا الأغراض السلمية وغير السلمية.

ما كانت حرب المعلومات الواردة تتطلب استخدام الدولة المضيفة لنظم المعلومات الخاصة بها، (د) وأخيراً، إذا كان الشروع في عملية الحرب على معلومات من الدولة المضيفة يعرضها لأعمال انتقامية محتملة. وعلى الرغم من أن الغالبية العظمى من الصكوك القانونية الدولية الحديثة لا تحتوي إلا على عدد قليل جداً من الأحكام التي تنطبق على الجوانب الأوسع لعمليات حرب المعلومات، ولا يزال هناك عدم وجود إطار قانوني دولي موجود خصيصاً لتنظيم هذه الظاهرة الناشئة. وسيبقى التهديد مستمراً، في حال عدم وجود إطار قانوني دولي معتمد عالمياً يقوم بتنظيم حرب المعلومات عبر السنوات القادمة؛ لأن هذا التنظيم سوف يلزم الدول بتوحيد قواها في تقليل وخفض الأنشطة غير المشروعة في حرب المعلومات، وفي حال عدم وجوده سوف يجعل أي محاولة لتوجيه الاتهام لمرتكبي مثل هذه الأنشطة لا معنى له وسيبقى معتمداً فقط على حسن نية الحكومات[٥٧].

الفرع السادس
حرب المعلومات والقانون الدولي العرفي

لقد أكدت محكمة العدل الدولية مراراً في أحكامها، أن القواعد القانونية المتعلقة بحق الدول في استخدام القوة في الدفاع عن النفس ليست مبنية فقط على أساس ميثاق الأمم المتحدة ولكن أيضاً على مبادئ القانون الدولي العام العرفي.

ويمكن اعتبار الإجراءات التي اتخذت في الدفاع عن النفس شرعية إذا ما كانت تخضع لشرطي الضرورة والتناسب، وهما الشرطان اللذان يجب أن يكونا متلازمين مع ضرورات الدفاع عن النفس. ويبدو أن "مبدأ كارولين" الذي أنشأه السيد دانيال وبستر في ١٨٤١ قد نجح في صياغة الاختبار النهائي لأية دولة، في اعتبار الإجراءات القسرية المتخذة من قبلها مشروعة في مفهوم الدفاع عن النفس في حال انطباق شرطي هذا المبدأ، لذلك نرى أنه يمكن الاستفادة منه وتطبيقه على التصرفات المستقبلية للدول في حرب المعلومات.

وهذا المبدأ "مبدأ كارولين" معترف به منذ أكثر من قرن ونصف القرن، ويعد من القواعد القانونية الدولية العرفية، وهو يسمح للدولة باللجوء إلى القوة لأغراض الدفاع عن النفس بالاستناد إلى شرطي الضرورة، والتناسب والموازنة في استخدامها، وبصرف النظر عما إذا كان اللجوء إلى القوة قد تم باستخدام الوسائل التقليدية للحرب أو الوسائل الحديثة منها أو باستخدام وسائل تقنية تم تطويرها حديثاً.

ومن ثم يمكن لأعضاء المجتمع الدولي الذين يجدون أنفسهم في وضع يضطرهم للدفاع عن النفس المراعاة قدر المستطاع لشروط "مبدأ كارولين" المؤسس على شرطي الضرورة والتناسب (قياساً على المبدأ الفقهي الشرعي القائل: إن الضرورات تقدر بقدرها) ومن ثم يمكن للدول استخدام القوة في الفضاء الإلكتروني للدفاع عن النفس من دون ارتكاب أي خرق لميثاق الأمم المتحدة، ومن ثم تظهر وكأنها تعمل بصورة قانونية وتمارس سيادتها استناداً لمبدأ "الاختصاص المكاني" وفي ممارسة لحقها الطبيعي في الدفاع عن النفس، شريطة الالتزام كذلك بـ "قانون الحرب". في الواقع، ليست هناك أية وسيلة ممكنة للتنبؤ بما يأتي: بأي شكل من الأشكال يمكن أن تتطور فيها حرب المعلومات، وما الإمكانيات المتاحة لشبكات الكمبيوتر المنتشرة على نطاق واسع؟ وكيف يمكن أن يتم الهجوم على الشبكات منها أو عليها تماماً؟، وفوق كل ذلك كيف يمكن للمجتمع الدولي أن يتجه نحو تطبيق القواعد القانونية الدولية القائمة المتعلقة بتنظيم استخدام القوة بشكل عام والقواعد العرفية على وجه الخصوص، في مجال حرب المعلومات؟، كل ذلك دفع دول العالم الآن إلى البحث عن آليات تنظيم جديد يقوم بالاستفادة من المعطيات السابقة والقيام بالمهمة الموكولة إليه.

المطلب الثالث

حرب المعلومات والحاجة إلى إيجاد تنظيم قانوني جديد

يحتاج القانون الدولي إلى إضافة تشريعات جديدة لسد الثغرات القانونية والاستفادة كذلك من التشريعات الوضعية.

الفرع الأول
سد الثغرات القانونية

المقترح الأول: إن السمة الأولى للمقترح من هذا القبيل سوف تقوم بسد أية ثغرات في التشريعات الموجودة حالياً [٥٧]، وكذلك تضمن تحديث القواعد القانونية القائمة المطبقة بالفعل حالياً على أنشطة حرب المعلومات سواء كان ذلك على المستوى المحلي، من خلال اعتماد القوانين الجنائية اللازمة، أم على المستوى الدولي، من خلال اعتماد الآليات القانونية الدولية التي تكفل تقديم المساعدة القضائية المتبادلة. ويمكن الركون في ذلك إلى المبادئ والقواعد التي أرستها الاتفاقية الأوربية للجرائم المرتكبة عبر الإنترنت ٢٠٠١.

الفرع الثاني
الاستفادة من التشريعات الوضعية

أما الاقتراح الثاني: فهو للاستفادة من الإطار التنظيمي القائم بالفعل الذي يضم جميع الوثائق القانونية الدولية التي تتضمن أحكاماً محددة لتنطبق على عمليات حرب المعلومات. جميع هذه الصكوك القانونية، في جميع أقسامها الخاصة، ومكافحة كل أشكال التسلل غير المشروع إلى أجهزة الكمبيوتر ونظم المعلومات، وتوجيه دعوة عامة إلى جميع الدول للتعاون فيما بينها للحد من مثل هذه الأفعال الجرمية في جميع أشكالها. عموماً كالوثائق القانونية الدولية التي تقع ضمن هذه الفئة المذكورة، أو حتى التي يجري النظر فيها حالياً للتعبير عنها بمثابة قانون دولي عرفي، ومن حيث النتيجة تصبح ملزمة لجميع الدول على قدم المساواة حتى لو لم تكن بعض الدول طرفاً في هذه الصكوك[٥٨]. ويوجد مصلحة كاملة للدول للاستفادة من تقانة المعلومات الحديثة والدفع نحو الالتزام الصارم بالقواعد القانونية القائمة حالياً، التي تنطبق منها على أنشطة الحرب الإلكترونية.

ومع ذلك، وعلى الرغم من حقيقة أن هناك بعض الجوانب من الإطارات القانونية الدولية التي يمكن تطبيقها على المسائل التي هي حالياً في متناول

اليد، إلا أن الطبيعة الخاصة جداً للإنترنت تجعلها جديدة تماماً، وعلى درجة عالية من التخصص ومن الاختلاف الكلي بشدة، وهذا يجعل من بعض المصالح الوطنية تتعارض بعضها مع بعض في أكثر الأحيان. ونتيجة لذلك، هناك ضرورة تدفع دول العالم حالياً للتحرك في اتجاه اعتماد صك قانوني دولي مصمم خصيصاً لتنظيم قانون للإنترنت بشكل عام، وقانون لحرب المعلومات على وجه الخصوص.

من وجهة نظر القانون الدولي، فإن السؤال الأول الذي يجب الإجابة عنه هو: هل يمكن اعتبار الهجمات على شبكات الحواسيب مبرراً للدول لاستخدام القوة، أو حتى القيام بهجوم مسلح؟ ومتى؟ قبل أن نحاول أي تحليل، سيكون من الجيد أن نأخذ في الاعتبار بعض الافتراضات مثلاً فيما يتعلق بمسألة الاختصاص القضائي، أيجب تحديد مكان نشوء الهجوم ونأخذ بالاختصاص الإقليمي أم بالمكان الذي ظهرت فيه نتائج هذا الهجوم "ونأخذ بمبدأ الآثار"؟ وطبعاً سيكون تحديد الموقع الجغرافي للمهاجمين، على درجة عالية من الأهمية وكذلك مكان وقوع آثار هذا الهجوم[٥٩] وهناك أيضاً أشكال عديدة من الهجمات المحتملة، وهذا يعني أنه ليس كل هجوم سيكون على المستوى الذي يؤدي بالدولة إلى استخدام القوة ضده. ولتوضيح هذه الفكرة، ينبغي العودة إلى بعض الأمثلة من الهجمات التي حدثت ضد شبكات الكمبيوتر العالمية، مثل الهجوم الذي حدث على بورصة نيويورك للأوراق المالية، الذي أدى إلى إغلاق الأسواق المالية، والهجوم على نظام مترو الأنفاق لمدينة نيويورك مما تسبب في اصطدام هائل وعرقلة، أو على نظام المراقبة الجوية الأمريكية الذي أدى إلى تحطم طائرة مدنية. والسؤال الذي يطرح نفسه هو: أمثل هذا الهجوم سيبرر استخدام القوة أم لا؟ في الواقع، هناك سابقة قوية مشابهة في المجتمع الدولي يمكن الركون إليها والاستفادة منها من أجل إنشاء قواعد قانونية تنطبق على حرب المعلومات وقدمت أفضل السبل الممكنة لهذا التنظيم الخاص، وهي التي ظهرت حديثاً ولها من الملامح الخاصة بها جداً أيضاً، وشكلت تحدياً للحدود الوطنية التقليدية، وأهي تقع في الوقت نفسه وسط مجموعة من المصالح

الوطنية المهمة المتعارضة بعضها مع بعض بشدة [٦٠]. هذه السابقة تضم اثنين من الصكوك القانونية الأكثر أهمية في تاريخ القانون الدولي، الأولى هي اتفاقية الأمم المتحدة لقانون البحار لعام ١٩٨٢ والثانية هي معاهدة عام ١٩٦٧ بشأن الفضاء الخارجي. ويمكننا من ثم المضي قدماً في نفس العمليات المشابهة لتلك التي أدت إلى اعتماد المعاهدتين المذكورتين والتي من شأنها أن تؤدي إلى اعتماد صك قانوني دولي لمواجهة التحديات المفروضة في تنظيم الإنترنت بشكل ناجح.

أولاً – سمات الفضاء الإلكتروني:

للفضاء الإلكتروني سمات محددة لابد من مراعاتها، ألا وهي:

التحدي الأول والأكثر شهرة لحرب المعلومات هو: (أ) بدء هجوم المهاجمين يتسبب في حدوث أضرار خطيرة فور الوصول غير المصرح به إلى نظم المعلومات. (ب) طبيعة الهجوم الخفي للغاية يجعل من الصعب جداً تحديد الموقع الدقيق للهجوم والمهاجمين وحرب المعلومات المعينة؛ مما يعقد عمل الضحية للجوء للعمل الدفاعي القسري واستخدام القوة. (ج) حرب المعلومات هو مثال حي منهجي على حقل في الدولة لا يمكن أن نأمل فيه تحقيق التفوق أو أن تجعل نفسها منيعة من الهجوم عليها. ومن شأن الفهم الكامل لهذه الميزات التأكد من أن أية قواعد تنظيمية سوف تنشأ يجب فيها تحقيق التوازن الصحيح بين الهجوم والمصالح الدفاعية لكل دول العالم فيما يتعلق بحرب المعلومات، ومن ثم ضمان أن تكون فعالة وأن تحظى بأكبر دعم ممكن في المجتمع الدولي.

ثانياً – توافق القانون الجديد مع القواعد الدولية الحالية:

وأما التحدي الثاني فهو أن يتوافق ويتطابق أي صك قانوني دولي جديد مع القواعد القانونية القائمة حالياً في الدفاع عن النفس، ويتعلق بتنظيم حرب المعلومات. وعلاوة على ذلك، فإن تصور أية أحكام اتفاقية مستقبلية ممكنة

لتنظيم حرب المعلومات يجب أن تدرج في نصوصها قواعد "قانون الحرب" التي تتعلق بها لتستهدفها تماماً، فضلاً عن وضع قواعد للتمييز بين المقاتلين وغير المقاتلين والمرتزقة. بالإضافة إلى ذلك، ينبغي أن تتخذ كل الخطوات الممكنة من أجل تفادي الأخطار المحدقة للوصول إلى مجتمع الفضاء الإلكتروني، وكذلك لضمان الوصول إلى أعلى الدرجات الممكنة.

ثالثاً – الأولوية لضمانات توفير المساعدات القضائية:

والتحدي الثالث الذي يواجه واضعي أي تنظيم لحرب المعلومات في المستقبل هو إيلاء الأولوية في النص لضمانات توفير المساعدات القضائية الكاملة بين الحكومات في حالات تعرض إحداها لهجمات من نوع حرب المعلومات ليعرف منشئها. ويجب على النظام القانوني المقترح أن لا يترك أدنى شك في تحديد الحالات التي يتم فيها تعرف دولة معينة ومن دون أي شك بأنها تشكل مصدراً لهجوم أو حرب معلومات خطيرة وبدقة متناهية، والحالات التي ترفض فيها الحكومات تقديم المساعدة القضائية بشأن تقديم مرتكبي الهجوم إلى العدالة، وتحديد إذا ما سيكون هناك افتراض اعتبار الدولة تشارك بالجرم والمسؤولية واحتمال القيام ضدها بعمل دفاعي قسري.

رابعاً – الحاجة إلى نموذج جديد فعّال لحرب المعلومات:

وهذا هو التحدي الأخير على وجه الخصوص، وهو الأبرز من أي وقت مضى؛ حيث يؤكد حاجة مجتمع القانون الدولي لنموذج جديد فيما يتعلق بالتنظيم الفعّال لحرب المعلومات، وجميع الإجراءات القسرية المحتملة المتصلة به. ويرجع ذلك فقط إلى أن ظهور أدوات الحرب الإلكترونية والتقنيات الحديثة التي وفرت لبعض الجهات العدوانية السلاح الفعّال والبسيط للغاية حتى الآن و لم يسبق لها مثيل من القوة المسلحة وعلى الرغم من كونها لا تزال في مراحلها الأولى من عملية التطور.

الفرع الثالث
حرب المعلومات وخصائصها الفريدة

إن أي محاولة للتنبؤ بأن حرب المعلومات ستشكل في نهاية المطاف تهديداً رئيسياً للسلام والأمن الدوليين، سيكون من السابق لأوانه في الوقت الراهن التكهن بذلك، ولكن – في الوقت نفسه – تنطوي هذه الحرب على الكثير من المخاطر التي لا يمكن تجاهلها بحال من الأحوال. والحقيقة التي لا يمكن إغفالها هي أن هذا المجال الواسع نفسه من شبكات المعلومات العالمية حالياً هو المسؤول عن قيادة الطريق إلى الازدهار والتنمية والرفاه لجميع أعضاء المجتمع الدولي، ويجعل في الوقت نفسه من كل تلك الدول التي تحاول تحقيق الاستفادة القصوى منه، عرضة لهجمات حرب معلوماتية[٦١].

لا تستطيع حالياً أي دولة ذات قوة عظمى ومتفوقة سياسياً أو عسكرياً، أو اقتصادياً أن تقاوم الاستفادة من المزايا التي تتيحها الشبكات العالمية للمعلومات، أو أن تستغني عنها، وبالإضافة إلى ذلك، تستطيع أن تعتمد عليها أيضاً من أجل شن "حرب معلوماتية" ضد أعدائها، بدلاً من أن تستخدم الطرق التقليدية للقوة المسلحة.نظراً للمزايا التي تجعل منها النموذج الأكثر إغراء لشن حرب هجمات حرب إلكترونية، بسبب الصعوبة البالغة في تحديد مصدر هذه الهجمات. وخاصة أنها تستطيع الإنكار وصعوبة الإثبات ضدها بأنها من قامت بالهجوم بشكل كبير، وكذلك تتجنب قوة خصومها.

وهناك سمة إضافية فريدة من حرب المعلومات لا يمكن لأي دولة أن تتخذ خطوات دفاعية كافية ضد هذا النوع من الهجوم، ولكن يمكن أن توجد هناك فرصة في الدفاع والذود عن الحمى من خلال التعاون والتنسيق بين الحكومات فيما بينها وكذلك التعاون بين الحكومات والقطاع الخاص. وربما هذا يتناقض مع الشكل التقليدي للقانون الدولي الحالي المتعلق بقانون الحرب والمسؤولية عن الحرب التي تقع تحت الولاية القضائية لحكومات الدول المعينة.

وتتسبب هجمات حرب المعلومات في أضرار كبيرة باستخدام أدوات وآليات قليلة جداً. ولذلك فإن الدول التي تجد نفسها تحت أي شكل من أشكال هجوم الحرب الإلكترونية عليها أن تتخذ من الإجراءات الكافية من أجل التصدي لأي هجوم، وتحييد ما تستطيع من آثارها الضارة وتعرف مصدرها أيضاً، وخاصة ما يتعلق في مجال التجارة الإلكترونية، وأن تتسلح الدولة بجميع التقنيات الدفاعية من أجل ذلك.

المطلب الرابع
دور المؤتمرات والاتفاقيات والمنظمات الدولية
في حماية الفضاء الإلكتروني

تؤدي المؤتمرات الدولية دوراً مهماً جداً في تكوين المبادئ والقواعد القانونية التي تتعلق بتنظيم أي ظاهرة جديدة تطرق باب القانون الدولي لتنظيمها، ومن المتعارف عليه أن معظم المنظمات الدولية قد نشأت في أحشاء المؤتمرات الدولية، وقد كان للمنظمات الدولية والإقليمية (كالأمم المتحدة ووكالاتها المتخصصة كاليونيسكو والاتحاد الدولي للاتصالات ومنظمة التعاون الاقتصادي والاجتماعي والاتحاد الأوروبي)[٦٤] دور لا يستهان به في الدعوة إلى تلك المؤتمرات. سنعرض فيما يلي لأهم المؤتمرات التي تعرضت لمسألة تنظيم الفضاء الإلكتروني وبخاصة ما تعلق منها بحرب المعلومات، وإن التعاون بين المنظمات الدولية يساعد على رسم استراتيجية واضحة المعالم ومنع التضارب بين الدراسات والأبحاث التي تقوم عليها الدول في هذا المجال؛ مما يؤدي إلى إتاحة الفرصة لاستفادة الدول النامية من خبرات الدول المتقدمة وتجاربها.

الفرع الأول
دور المؤتمرات والاتفاقيات الدولية

لقد أسهمت المؤتمرات الدولية من خلال المبادئ والتوصيات الصادرة عنها، في تنظيم العديد من النقاط الجوهرية المتعلقة بالفضاء الإلكتروني[٦٥]، في مختلف قطاعاته، وقد ساعدت هذه المؤتمرات في وضع العديد من القواعد

القانونية التي شكلت اللبنة الأولى في صرح القانون الدولي المتعلق بتنظيم الفضاء الإلكتروني، وربما أمكننا أن نطلق عليه القانون الدولي للإنترنت.

ومن أهم هذه المؤتمرات نذكر:

أولاً – مؤتمر القمة العالمية لمجتمع المعلومات في جنيف ٢٠٠٣:

أمام تزايد الأخطار التي تحدث في شبكة الإنترنت وخاصة ما يحدث من حروب معلوماتية، وبناء على قرار مجلس الاتحاد الدولي للاتصالات وقراري الجمعية العامة ٥٧/٢٣٨ و ٥٦/١٨٣. تم عقد مؤتمر القمة العالمية لمجتمع المعلومات في جنيف – بالكسبو ٢٠٠٣، في الفترة من ١٠ إلى ١٢ كانون الأول ٢٠٠٣، تحت عنوان (بناء مجتمع المعلومات: تحد عالمي في الألفية الجديدة)، ولقد حضر المؤتمر أكثر من ١١,٠٤٧ شخصاً يمثلون ١٧٦ دولة و١٠٠ منظمة دولية و٤٨١ منظمة غير حكومية و٩٨ شركة خاصة و٦٣١ وسيلة إعلامية، في حين حضر ٤٠ رئيس دولة وحكومة فقط من أصل ٦٠ كانوا قد أعلنوا مشاركتهم؛ ليشهدوا ولادة المجتمع المعلوماتي الذي سيميز الألفية الثالثة، وكان هذا المؤتمر يستهدف تحقيق رؤية ومبادئ مشتركة من أجل ضمان أمن الإنترنت واستمرارها وتنميتها واستفادة جميع البشرية من الإمكانات التي يمكن أن تقدمها، وكذلك لبحث السبل لتشجيع الحكومات والمنظمات الدولية للقيام بما يجب لتحقيق هذه الأغراض، ولقد أقر رؤساء الدول الحاضرون والمنظمات الدولية بأهمية الإنترنت، وسلموا[١٢] بأنها عنصر محوري في البنية التحتية لمجتمع المعلومات الناشئ، وصدر عن هذا المؤتمر في ختام أعماله إعلان[١٣]، يتضمن ضرورة حماية بيئة الإنترنت الافتراضية،

---

(١٢) إعلان مبادئ مؤتمر القمة، الفقرات من ٤٨ إلى ٥٠ (WSIS-03/GENEVA/ 9(Rev.1)-A).2003- جنيف – سويسرا.

(١٣) التعاون الدولي والإقليمي: إننا نسعى إلى الاستفادة الكاملة من الفرص التي تتيحها تكنولوجيا المعلومات والاتصالات في جهودنا لبلوغ الأهداف الإنمائية المتفق عليها دولياً، بما فيها الأهداف الواردة في إعلان الألفية، ولدعم المبادئ الرئيسية الواردة في =

متضمناً أول وثيقة دولية تتعلق بمبادئ العلاقات بين الدول في شأن الإنترنت وكيفية التعامل معها، بالإضافة إلى خطة عمل. وإذا نظرنا إلى الإعلان نجده(١٤) قد أكد في مبادئه أهمية بناء الثقة والطمأنينة والأمن في استعمال تكنولوجيا المعلومات والاتصالات، حيث تمخض عنه تشكيل الفريق العامل لإدارة الإنترنت، الذي شكله الأمين العام للأمم المتحدة من مجموعة من الخبراء من كل الاختصاصات لإعداد تقرير كامل حول إدارة الإنترنت، وقد صدر قبيل انعقاد المؤتمر الثاني الذي تقرر عقده في تونس ٢٠٠٥.

ثانياً – مؤتمر القمة العالمية لمجتمع المعلومات في تونس ٢٠٠٥:

افتتح السيد يوشيو أوتسومي الأمين العام للاتحاد الدولي للاتصالات المرحلة الثانية من القمة العالمية لمجتمع المعلومات في تونس، وقد جاء في أهم مقررات هذا المؤتمر: السعي إلى بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات وتأكيد ضرورة المضي، بالتعاون مع جميع أصحاب المصلحة، في تعزيز ثقافة عالمية للأمن السيبراني وتنميتها وتنفيذها، كما ورد في قرار الجمعية العامة للأمم المتحدة ٥٧/٢٣٩، وفي قرارات بعض المحافل الإقليمية ذات الصلة. وتتطلب هذه الثقافة إجراءات وطنية ومزيداً من التعاون الدولي لتعزيز الأمن، والعمل في الوقت ذاته على النهوض بحماية المعلومات الشخصية وحماية الخصوصية والبيانات. وينبغي أن يعزِّز استمرار تنمية ثقافة

= هذا الإعلان. إن مجتمع المعلومات هو في جوهره عالمي الطابع، ومن ثم لا بد من تدعيم الجهود الوطنية، بإقامة تعاون دولي وإقليمي فعال بين الحكومات والقطاع الخاص والمجتمع المدني وأصحاب المصلحة الآخرين، بما في ذلك المؤسسات المالية الدولية.

(١٤) تضطلع الحكومات، وكذلك القطاع الخاص والمجتمع المدني والأمم المتحدة والمنظمات الدولية الأخرى، بدور مهم وبمسؤولية كبيرة في تطوير مجتمع المعلومات، وكذلك في عمليات صنع القرارات بحسب الاقتضاء. إن بناء مجتمع معلومات غايته الناس هو جهد مشترك يتطلب التعاون والشراكة بين جميع أصحاب المصلحة.

الأمن السيبراني إمكانيات النفاذ والتجارة، وأن يراعي مستوى التنمية الاجتماعية والاقتصادية في كل بلد، وأن يحترم الجوانب الموجهة نحو التنمية في مجتمع المعلومات، وتأكيد أهمية ملاحقة الجرائم السيبرانية قضائياً، بما فيها الجرائم السيبرانية التي تُرتكب ضمن الولاية القانونية ولكنها تؤثر على ولايات قانونية أخرى. ودعوة الحكومات بالتعاون مع أصحاب المصلحة الآخرين إلى وضع التشريعات اللازمة للتحقيق في الجرائم السيبرانية وملاحقتها قضائياً، مع الاستفادة من الأطر القائمة، ومنها – على سبيل المثال – قرار الجمعية العامة للأمم المتحدة ٦٣/٥٥ وقرارها ١٢١/٥٦ بشأن "مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية"، واتفاقية المجلس الأوروبي بشأن الجرائم السيبرانية[٦٦]. ويمكن القول إن هذا المؤتمر قد شكل منعطفاً تاريخياً خطيراً، وكان بداية الانطلاق الحقيقية لبدء الاهتمام بالفضاء الإلكتروني عموماً، ومازال الفريق العامل لإدارة الإنترنت مستمراً في عمله، في شكل منتدى دولي لقانون الإنترنت، الذي يعتبر النواة الأولى لوضع النقاط الأساسية الأولى لتنظيم الإنترنت بشكل عام وحرب المعلومات بشكل خاص وعقد عدة مؤتمرات أخرى في اليونان – أثينا ٢٠٠٦، والبرازيل ٢٠٠٧، وإسلام آباد ٢٠٠٨، وشرم الشيخ ٢٠٠٩، غير أن هذه القمم لم تحقق التوقعات المرجوة منها، وأخفقت في علاج كثير من القضايا المتعلقة بالفضاء الإلكتروني المهمة، وخاصة فيما يتعلق بمساعدات الدول النامية التي تقدمها الدول الغنية للدول الفقيرة، كما أن إعلان القمة العالمية لمجتمع المعلومات في جنيف ٢٠٠٣ وتونس ٢٠٠٥، إنما هو نصوص غير مفصلة وغير ملزمة إلا في القليل منها[٦٧].

وأخيراً، فإنه وإن كانت معظم أعمال المؤتمرات الدولية تأخذ شكل توصيات غير ملزمة للدول التي قد ترفض تنفيذها[٦٨]، ولا توجد قوة حقيقية ملزمة لهذه التوصيات فإنها بتواترها وانسجامها بعضها مع بعض، فضلاً عن إجماع الدول المشاركة فإنها تشكل اللبنة الأولى في بناء القانون الدولي للإنترنت، فهي تسهم في نشأة قواعد عرفية جديدة في نطاق هذا القانون.

ثالثاً – الاتفاقية الأوروبية للجرائم المرتكبة عبر الإنترنت وحرب المعلومات(١٥) Convention on Cybercrime2001:

سميت باتفاقية بودابست، وقد تم التوقيع عليها في تشرين الثاني ٢٠٠١، ودخلت حيز التنفيذ في ١ أيلول ٢٠٠٤، وقد صيغت هذه الاتفاقية من قبل الاتحاد الأوروبي سعياً منه إلى الحد من حركة الإجرام عبر الإنترنت، وأضيف إلى هذه الاتفاقية بروتوكول معني بوضع نموذج لمكافحة جرائم الكراهية ضد الأجانب عبر الإنترنت وهو البروتوكول المسمى بروتوكول ستراسبورج المؤرخ ٧ تشرين الثاني ٢٠٠٢، وضمت هذه الاتفاقية العديد من الدول الأوروبية وغير الأوروبية، وهي تؤدي دوراً في تحسين التعاون الدولي في مجال مكافحة الجرائم عبر الفضاء الإلكتروني والتركيز على تبني تشريعات مناسبة وطنية لتتلاءم مع الاتفاقية الدولية والتعريف بالجرائم المرتكبة عبر الفضاء الإلكتروني وتحديد أركانها.

إلا أن أهم ما جاءت به الاتفاقية هو تحديد التعاريف الهامة والضرورية في التعامل مع شبكة الإنترنت "كمنظومة الكمبيوتر، وبيانات الكمبيوتر، ومزود الخدمة، وخط سير البيانات، في المادة الأولى من الفصل الأول، وقد تساعد هذه المصطلحات الإلكترونية ضمن الصياغة الدولية في الاتفاقية الأوربية إلى اعتمادها، كمصطلحات قانونية دولية في الاتفاقيات الدولية المعتمدة عالمياً، وكذلك من خلال تحديدها إلى نوعية وأركان الجرائم التي قد ترتكب مثل جريمة "الدخول غير المشروع" والاعتراض الغير مشروع وإساءة استخدام الأجهزة و"التدخل غير المشروع" في المنظومة، في الفصل الثاني منها، وحل بعض التحديات التي تواجهنا في حرب المعلومات، مثل استخدام التعابير وشرح لبعض المصطلحات، وتحديد ماهية الجرائم التي قد تحدث في الإنترنت، لذلك تعتبر هذه المعاهدة الدولية الأولى

(١٥) Convention on CyberCrime - Explanatory Report, adopted on 8 Nov. 2001. Committee of Ministers of the Council of Europe, 109th Session (8 Nov. 2001). P. 5, available online in Nov. 2001 at: Uhttp://conventions.coe.int/treaty/EN/projects/FinalCyberapex.html

من شأنها في تحديد الجرائم التي ترتكب عبر شبكة الإنترنت، ويمكن الركون إليها في تحديد معظم الجرائم التي قد ترتكب في حرب المعلومات.

الفرع الثاني
دور المنظمات الدولية

قامت منظمة الأمم المتحدة وكذلك المنظمات المتخصصة بدور فعال في مجال حماية الفضاء الإلكتروني وتطوير القانون الدولي للإنترنت، من خلال تبني استراتيجيات خاصة بهذا الشأن إلى جانب الأنشطة الأخرى التي تقوم بها، ومحاولة إعادة تفعيل دورها الرئيسي في حفظ الأمن والسلم الدوليين، ومن أجل صياغة معاهدة لمنع الحرب، والحاجة إلى معاهدة دولية بإشراف الأمم المتحدة(١٦).

أولاً – دور منظمة الأمم المتحدة:

لقد أدت الأمم المتحدة دوراً بارزاً في صياغة القانون الدولي للإنترنت سواء من خلال تنظيم مؤتمرات دولية حول تنظيم الفضاء الإلكتروني، أو من خلال إنشاء الأجهزة والفرق واللجان والبرامج المعنية بحماية الفضاء الإلكتروني، وتشجيع التعاون الدولي لصيانته، أو من خلال إصدار القرارات والتوصيات التي تؤكد مطالبة الحكومات بالتعاون الوثيق لوضع وتطبيق سياسة جماعية للتنمية الاقتصادية والاجتماعية، من بين أهدافها تنظيم العمل في الفضاء الإلكتروني.

ويعتبر مؤتمرا القمة العالمية لمجتمع المعلومات في جنيف٢٠٠٣ وتونس ٢٠٠٥، اللذان عقدا تحت مظلة الأمم المتحدة العمل التقني الأول في مجال القانون الدولي للفضاء الإلكتروني؛ لكونه يحتوي على مجموعة من المبادئ المتعارف عليها لتنظيم العلاقة في مجال التعامل في الفضاء الإلكتروني في

(١٦) مؤتمر الأمم المتحدة لمنع الجريمة والعدالة الجنائية «بشأن الأمن السيبراني والجرائم الحاسوبية» الثاني عشر، سلفادور، ١٠/٤/٢٠١٠– ولغاية ١٣/٤/٢٠١٠ ومنشور على الإنترنت: www.cybercrimelaw.net/ - www.un.org/en/conf/crimecongress

الوقت الذي صدرت عنه. ومن الإنجازات المهمة لمؤتمري القمة تشكيل الفريق العامل المعني بإدارة الإنترنت، الذي تمخض عنه فيما بعد منتدى حكم الإنترنت Global Internet governance: كهيئة دولية مختصة، وتعقد الآن العديد من الندوات العالمية لمناقشة موضوع الأمن السيبراني تحت إشراف منظمة اليونيسكو(١٧) وصدرت العديد من المؤلفات التي تنادي بضرورة إيجاد معاهدة دولية للإنترنت ولحروب المعلومات.

الخلاصة:

تمثل حرب المعلومات حالياً مفهوماً جديداً تماماً من مفاهيم اللجوء إلى اتخاذ الإجراءات القسرية، وعلى الرغم من أنها لا تزال في المرحلة الأولى من العملية التطورية، فإنها قد وصلت بالفعل إلى النقطة التي لا بد من إخضاعها لنظام رقابي مصمم خصيصاً لمواجهة التحديات المعينة القائمة.

إن القواعد القانونية الدولية الحالية والمتعلقة باستخدام القوة بصورة عامة، والدفاع عن النفس بوجه خاص، يمكنها تنظيم الحرب الإلكترونية ولكن بشكل بسيط، حيث تم وضع تصور لمعالجة أقل أشكال العمل القسري والأكثر تقليدية. ولو أنها تعتبر الأمل الوحيد حالياً لتحقيق هذا التنظيم، في شكل مبدأ كارولين [62]Caroline Principle الذي إذا طبق في نهاية المطاف على أنه النظام التنظيمي الرئيسي في عمليات حرب المعلومات فإنه لا بد من أنه سوف يعقد الأمور، بدلاً من جعلها أكثر بساطة؛ لأنه أبعد ما يكون قدرة على الإجابة عن التداخل السياسي، والقانوني، والتحديات الاقتصادية والعسكرية المختلفة التي أدخلها المفهوم الثوري للحرب الإلكترونية.

(١٧) ANNA MARIA BALSANO-AN International Legal Instrument For Cyber-space?-: T. Fuentes Camacho, The International Dimensions of Cyberspace Law, 2000, 71 et seq. (90-91).

أوجدت هذه التحديات حالياً قواعد تتعلق بالدفاع عن النفس، وفشلت في مخاطبات عدة تحديات أخرى كانت قد واجهتها، وتتطلب أجوبة دقيقة تنظيمية تكون ممكنة إذا أريد للسلام والأمن الدوليين أن يكونا مضمونين في العقود القادمة، واحتواء جميع التهديدات التي تتعلق بشن هجمات على الإنترنت[٦٣].

التحدي الأول من نوعه الذي فشل في التعامل مع القواعد القانونية الدولية التقليدية في الدفاع عن النفس كان مسألة المصطلحات المشتركة والمتجانسة. حيث ينطوي كل مفهوم جديد على مصطلح جديد حتماً. وتصبح الحاجة إليه أكثر إلحاحاً عندما ينطوي المفهوم الجديد على قضايا قانونية وتكنولوجية معقدة، وهي بحاجة إلى التنظيم. كيف لنا أن نعرف هذا المفهوم الجديد وجميع الجوانب المتصلة به، التي لديها تأثير مباشر على الإطار القانوني الفعلي وكيف سيتم تطبيقها على ذلك النظام الجديد، ويجب أن يكون هناك تنظيم محدد، وعلاوة على ذلك، فإن وضع المصطلحات الصحيحة والتعريفات لهذه المفاهيم المتطورة حديثاً، مثل حرب الفضاء الإلكتروني ضروري جداً، وتبيان مدى تأثير بعض القضايا الأخرى على هذا المفهوم، مثل قضايا السياسة الجبرية، وتوفير التمويل الكافي لتطوير وسائل الدفاع اللازمة، أو حل المسائل والتعاون بين جميع الوكالات الحكومية والأشخاص المسؤولين عنها قانوناً للتعامل مع هذا الوضع الجديد، ليس في داخل الدول فقط ولكن على مستوى العلاقات بين الدول أيضاً. والمشكلة أكبر من ذلك فيما يتعلق بالإجراءات القسرية في الفضاء الإلكتروني؛ نظراً للمضاعفات العديدة المتأصلة في هذا الشكل المعين من أشكال العمل القسري.

هذا؛ لأنه من الصعب التمييز بين الهجمات التي تقع على شبكات الحواسيب والتي قد تعزى إلى نشاط إجرامي عادي أو نشاط إرهابي أو حتى الهجمات الواسعة النطاق من قبل دولة ما، وهناك حاجة للتحديد بالضبط فكرة "الهجوم المسلح" في الفضاء الإلكتروني. وكما تبدو الأمور اليوم هناك نقص في القواعد القانونية الدولية بوجه عام، والمبدأ القانوني الحالي للدفاع عن النفس بوجه خاص، ليس فقط وجود تعريف كاف للعمل الفعلي الذي يمكن تسميته

«هجوم الإنترنت» ولكن أيضاً من خلال توافق في الآراء بشأن إذا ما كانت الهجمات على شبكات الحواسيب تشكل خطراً كافياً وتبرر بذل جهود متضافرة دفاعية ضد الهجوم من هذا القبيل[٦٤] وعلاوة على ذلك، هناك عدد قليل جداً من المصطلحات والتعاريف المتصلة بحرب الفضاء الإلكتروني التي يمكن أن تفسر بطرق مختلفة اعتماداً على من يستخدم هذا المصطلح بالفعل. على سبيل المثال، قد يكون مصطلح "monitoring"، الرصد أو المراقبة "قد يكون له معنى محدد للمؤسسة الدفاعية في بلد معين، ولكنه قد يكون له معنى آخر مختلف تماماً إذا نظر إليه من خلال تطبيق القانون أو وجهة النظر القضائية، وأنه بالتأكيد لديه معنى آخر مختلف عندما نراه من وجهة نظر الحريات المدنية.

أما التحدي الثاني: المنصوص عليه وفقاً للنشاط فهو حرب المعلومات التي لها تأثير مباشر على المسألة الثانية، التي تعتبر جزءاً لا يتجزأ من مجموعة الإمكانيات والجهود المتضافرة لتنظيم الهجمات على شبكات الحواسيب والتي لا يتم تناولها من قبل القواعد القانونية القائمة في الدفاع عن النفس، وهي حقيقة حرب الفضاء الإلكتروني ألا وهي وجود المظهر العسكري والمدني. ويتطلب الهجوم والدفاع في حرب المعلومات، على مستوى متساو تقريباً، علاقة عمل متقاربة جداً بين الدولة والقطاعين الخاص والعام؛ لأن تكنولوجيا المعلومات هي واحد من الميادين القليلة التي يوجد فيها القطاع المدني من الناحية الفنية قبل العسكري. وإذا كان لهذه العلاقة أن تنجح فإنه سيتعين أن ينظمها إطار قانوني مصمم خصيصاً لسد الفجوة التقليدية بين القطاع الخاص والحكومات الوطنية، وخصوصاً عندما يتعلق الأمر بالمشاريع الحرة، والعائد من السيطرة حيث الوكالات الحكومية، والقطاع العام الذي ينظم مركزياً، وخاصة في المسائل المتعلقة بالدفاع والأمن القومي.

المحاولات التنظيمية المتعلقة بأنشطة حرب الفضاء الإلكترونية، لم يسبق لها مثيل بشأن التعاون فيما بين الدول، ولا يرجع هذا فقط إلى حقيقة أن الشبكات العالمية يمكن الهجوم عليها ويمكن توجيه هذه الحرب عبر الحدود من قبل بلدان متعددة، ولكن نتيجة لطبيعة الحرب الإلكترونية في التخفي بدقة؛ مما

يجعل من الصعب للغاية بالنسبة للهجوم معرفة إذا ما كان موجهو الضربات هم من القراصنة العاديين أو هم من دولة أخرى. ولمعالجة هذه المسألة بالذات ستكون ذات أهمية بالغة من وجهة النظر التنظيمية، وذلك لسبب إضافي من المحتمل جداً لتعيين العتبة والمسؤولية القانونية التي قد تكون وراءه سواء أكانوا دولاً أم غير ذلك، والمبرر القانوني في اتخاذ الإجراءات القسرية للرد على هذه النشاطات الموجه ضدهم.

وعلى الرغم من أن هناك بعض الجوانب من القانون الدولي التي يمكن تطبيقها على المسائل التي هي حالياً في متناول اليد، إلا أنه نظراً للطبيعة الخاصة جداً التي يتمتع بها الفضاء الإلكتروني كونه فضاء جديداً تماماً، ويحتاج إلى تنظيم على درجة عالية من التخصص والتكامل لتحقيق المصالح الوطنية المختلفة المتعارضة بشدة. ونتيجة لذلك، هناك ضرورة قصوى تدعو وتحفز كل دول العالم للتحرك في اتجاه اعتماد صك قانوني دولي مصمم خصيصاً لتنظيم قانون الإنترنت بشكل عام، وقانون لحرب المعلومات على وجه الخصوص،حتى تستطيع الدول ممارسة حقوقها في استخدام القوة أو الدفاع عن النفس في حال تعرضها لأي هجوم، وتطبيق ميثاق الأمم المتحدة بشكل دقيق ضماناً لتحقيق الأمن والسلم الدوليين.

المراجع بحسب تسلسل ورودها في البحث:

1 - D. Kuehl, Information Operations: The Hard Reality of Soft Power 118 (Washington DC Department of Defense, 2004-pp31 et seq -40.

2 - J Elliston, The Right To national self-Defence: in information warfare operations -pp-45 et seq -47- at http://www.Parascope.com/ds/cyber1.htm (1999).

3 - J F Dunnigan, The Next War Zone: Confronting the Global Threat of Cyberterrorism, New York NY; Osborne/McGraw-Hill (2002)-pp200 et seq -224.

4 - Joint Command, Control and Information Warfare School, Joint Information Operations Planning Handbook 118 (Washington DC: Joint Command, Control and Information Warfare School, 2003)pp-. V-14 et seq - V-20

5 - L J Freeh, Director of the FBI speech at the 1997 International Computer Crime Conference (March 4, 1997). Available at http://www.fbi.gov/dirspch/compcrim.htm.

6 - Dimitrios Delibasis, State Use of Force in Cyberspace for Self-Defence: A New Challenge for a New Century Peace Conflict and Development: An Interdisciplinary Journal, Issue 8, February 2006-pp14-16.

7 - "B. Simma, ‘‘NATO, the UN and the Use of Force: Legal Aspects’’, EJIL 10 (1999), 1 et seq. (11) - pp1-11

8 - Office of the Undersecretary of Defense for Acquisition, Technology and Logistics, Protecting the Homeland, Report

of the Defense Science Board Task Force on Defensive Information Operations: Memorandum for the Chairman, Defense Science Board 1 (Washington DC: Department of Defense, 2001)- Volume II-March -2001-pp12 et seq -15

9 - A Campen, D Dearth and R T Gooden Eds, Cyberwar: Security, Strategy and Conflict in the Information Age, Fairfax VA; AFCEA Press (1996).

10 - Y. Dinstein, War, Aggression and Self-Defense (Cambridge: Cambridge University Press, 2001) pp 170-173 and 174.

10 - C.C. Joyner/ C. Lotrionte, ''Information Warfare as International Coercion:Elements of a Legal Framework'', EJIL 12 (2001)pp, 825 et seq. (827) (مما يدل على أن القواعد القانونية الموجودة في القانون المعاصر وميثاق الأمم المتحدة مفيدة ولكنها غير كافية للوصول إلى حلول مقبولة).

11 - W.G. Sharp, Sr., CyberSpace and the Use of Force, 1999, 7; E.T. Jensen, ''Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense'', Stanford J. Intl L. 38 (2002), 207 et seq. (208). القضية المتعلقة بالأنشطة العسكرية وشبه العسكرية في نيكاراغوا وضدها قرارات، A/56/ 770 [١٩٨٦] محكمة العدل الدولية –

12 - Simma, NATO the UN and the Use of Force - Legal Aspects, 10 E.J.I.L. (1999). Ludwig Maximilians University of Munich - Faculty of Law- European Journal of International Law, Vol. 10, pp. 1-22, 1999

13 - D A Fulghum and R Wall, US Weather Operations in the Transformation Era - Air University Press Maxwell Air Force Base, Alabama-March 2003 at- pp-11-14-

14 - Charter of the United Nations, 59 Stat. 1031 T. S. No. 993, 3 Bevans 1153, Art. 51 (1945).

15 - Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations, UN Doc. A/8028, General Assembly Resolution 2625, UN GAOR 25TH Session Supplement 28, 121 (1970).

16 - Definition of Aggression, UN Doc. A/9631, General Assembly Resolution 3314, UN GAOR 29TH Session Supplement 31, 142 (1974).

17 - Y. Dinstein, War, Aggression and Self-Defense 170-173 and 174 (Cambridge: Cambridge University Press, 2001). Also, US Department of Defense, Active Defense against Computer Intrusions 5-8 Washington DC: Department of Defense, December 2nd 1998 -pp14-26.

18 - D Chereshekin, V Tsygichko and G Smolyan, A Weapon That May Be More Dangerous than A Nuclear Weapon: The Realities of Information Warfare (1995).pp112-114 Available at: http://www.iwar.org.uk/iwar/resources/parameters/iw-deterrence.htm

19 - J F Dunnigan, The Next War Zone: Confronting the Global Threat of Cyberterrorism, New York NY; Osborne/ McGraw-Hill (2002).).pp1-2

20 - D C Gompert, Right Makes Might: Freedom and Power in the Information Age, Institute for National Strategic Studies-Strategic Appraisal: The Changing Role of Information in

Warfare National Defense University Washington, DC, McNair Paper 59 (May 1998 -pp52-60.

21 - V ADM A K Cebrowski, Sea, Space, Cyberspace: Borderless Domains (1999). Available at http://www.nwc.navy.mil/press/speeches/borderless.htm

٢٢- د. محمود مرشحة - الوجيز في القانون الدولي العام - منشورات جامعة حلب - ٢٠٠٨ - ص١١٢-١١٥.

23 - US Department of Defense - Office of the General Counsel, Active Defense against Peacetime Computer Intrusions 7 (Washington: Department of Defense, 1998).

24 - D C Gompert, National Security in the Information Age, Naval War College Review (Autumn 1998). Newport RI; Naval War College Press-pp22-25.

25 - S T Hosmer, The Information Revolution and Psychological Effects, Santa Monica CA; Rand, Y. Dinstein, War, Aggression and Self-Defense 207-13 (Cambridge: Cambridge University Press, 2001)-pp12-23.

26 - The Annotated Supplement to the Commanders Handbook on the Law of Naval Operations, U. S. Naval War College - Intl Law Studies - Volume 73-pp- 290-292 (Annapolis VA: US Naval War College, 1997)

27 - Case Concerning United States Diplomatic and Consular Staff in Tehran, [1980] I. C. J. Rep. 3, 43.

28 - Tadic Case (The Verdict), [May 7, 1997] I.T. Press Release CC/PIO/190-E.-

٢٩- البروتوكول (الأول)، الإضافي لاتفاقيات جنيف المؤرخة في ١٢ أغسطس ١٩٤٩ المتعلق بحماية ضحايا المنازعات الدولية المسلحة، UNJY 95-117. 4 و ٤٣-٥١ (١٩٧٧).

30 - L. C. Green, The Contemporary Law of Armed Conflictpp-105-08 and 114-18 (Manchester: Manchester University Press, 2000).

31 - Tadic Case (The Verdict), [May 7, 1997] I.T. Press Release CC/PIO/190-E

32 - A Rathmell, Strategic Information Warfare: Responding to the Threat, Centre for Defense studies, Brasseys Defense Yearbook (1998)-pp10-11.

33 - L. C. Green, the Contemporary Law of Armed Conflict 268-72 and 274 (Manchester: Manchester University Press, 2000). pp2-3

34 - K W Quigley, A Framework for Evaluating the Legality of the United States Intervention in Nicaragua, 17 N.Y.U.-J.I.L.P. (1985).

35 - A. Roberts and R. Guelff, Documents on the Laws of War 59 et seq. (Oxford: Oxford University Press, 2000). pp12-13

36 - J. P. Terry, (Colonel United States Marine Corps Ret.), Responding to Attacks on Critical Computer Infrastructure XLVI Naval Law Review 170 et seq. (1999). Also, see generally, T. C. Wingfield, Legal Aspects of Offensive Information Operations in Space 2 et seq. (2003). pp112-114 via http://www.usafa.mil/dfl/documents/wingfield.doc

37 - T. C. Wingfield, Legal Aspects of Offensive Information Operations in Space 1-4 (2003) via http://www.usafa.mil/dfl/documents/wingfield.doc

38 - Treaty on the Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, 610 U.N.T.S. 205 (1967).

39 - P. A. Johnson (Colonel USAF/JAG Ret.), An Assessment of International Legal Issues in Information Operations 27. (Washington DC: Department of Defense, 1999).

40 - Agreement Relating to the International Telecommunications Satellite Organization, 23 U. S. T. 3813 (1971).

41 - Convention of the International Maritime Satellite Organization 31 U. S. T. 1 T. I. A. S. No. 9605 (1976).

42 - A Pearce, The Hague Conference and other International Conferences concerning the Laws and Usages of War: Text of Conventions with Notes, London; Stevens and Sons (1904).

43 - United Nations Conventions on the Law of the Sea". UN Doc. A/CONF.62/122, 21 I. L. M. 1261 (1982).

44 - United Nations Manual on the Prevention and Control of Computer Related Crime (2000). Available at http://www.if-s.univie.ac.at/~pr2gq1/rev434.html

45 - T. C. Wingfield, Legal Aspects of Offensive Information Operations in Space-pp 1-4 (2003) via http://www.usafa.mil/dfl/documents/wingfield.doc

٤٦- اتفاقية الاتصالات السلكية واللاسلكية الدولية، مع الملاحق والبروتوكولات، ٦ تشرين الأول ١٩٨٢ وثيقة المعاهدة ٩٩-٦ (١٩٨٢) مجلس الشيوخ الأميركي.

47 - D. J. Harris, Cases and Materials in International Law 765-70 (London: Thomson-Sweet and Maxwell, 2005)pp-12-22.

48 - L. C. Green, The Contemporary Law of Armed Conflict 57-8. (Manchester: Manchester University Press, 2000)-pp45-49

49 - A. D. McNair, The Functions and Differing Legal Character of Treaties, 11 B. Y. I. L. 100 (1930).

50 - The Chicago Convention "Chicago International Air Services Transit Agreement, U. K. T. S. 8 1953 Cmd. 8742-171 U.N. T. S. 387 Art. 3(d), 28 and 37 (1944).

51 - J. Adams, The Next World War: The Warriors and Weapons in the New Battlefields in Cyberspace 199 et seq. (London: Hutchinson, 1998). Also, J. F. Dunnigan, The Next War Zone: Confronting the Global Threat of Cyber terrorism 1 et seq. (New York NY: Osborne/McGraw-Hill, 2002).

52 - H. Thirlway, International Customary Law and Codification 4 et seq. (Lieden: A. W. Sijthoff, 1972).

53 - S.P. Kanuck, "Information Warfare: New Challenges for Public International Law", Harv. Intl L. J. 37 (1996), 272 et seq. (286-287).

54 - Office of the Undersecretary of Defense - for Acquisition, Technology and Logistics, Protecting the Homeland: Report of the Defense Science Board on Defensive Information

Operations 85 (Washington DC: Department of Defense, 2001).pp3-6

55- G K Walker, Information Warfare and Neutrality, 33 Vanderbilt Journal of Transnational Law 1082 (2000).

56- Office of the Undersecretary of Defense for Acquisition, Technology and Logistics, Protecting the Homeland: Report of the Defense Science Board Task Force on Defensive Information Operations 85 et seq. (Washington DC: Department of Defense, 2001)

57- Office of the Undersecretary of Defense for Acquisition, Technology and Logistics, Protecting the Homeland: Report on the Defense Science Board Task Force on Defensive Information Operations 86 (Washington DC: Department of Defense, 2001)

58- KAMAL A., 2005- The Law of Cyber-Space-Switzerland-United Nations Institute For Training and Research,197-254 Published by the United Nations Institute for Training and Research -Palais des Nations-CH 1211 Geneva 10-Switzerland-First Edition: October 2005-- KAMAL A., 2005- The Law of Cyber-Space-Switzerland- United Nations Institute For Training and Research-pp,197-254

59- Antonio Segura-Serrano-., Internet regulation and the Role of International Law - Max Planck Yearbook of United Nations Law, Volume 10, 2006, p. 191-272-2006 Koninklijke Brill N.V. Printed in The Netherlands-pp22-32

٦٠- د. محمود مرشحة - الوجيز في المنظمات الدولية - مديرية الكتب والمطبوعات الجامعية - ٢٠٠٩/ ٢٠١٠ - ص ٢٣-٤٥.

٦١- د. بولين أنطونيوس أيوب - الحماية القانونية للحياة الشخصية في مجال المعلوماتية - منشورات الحلبي - لبنان - بيروت -٢٠٠٩-٣٤-٣٩.

٦٢- د. محمود مرشحة - المنظمات الدولية - منشورات جامعة حلب - ٢٠٠٦- ص ١١٢-١٢٠.

٦٣- د. محمد المجذوب - التنظيم الدولي - النظرية العامة والمنظمات العالمية والإقليمية والمتخصصة - منشورات الحلبي الحقوقية - ٢٠٠٥ - ص ٢١١-٢١٤.

٦٤- طوني عيسى: التنظيم القانوني لشبكة الإنترنت (دراسة مقارنة في ضوء القوانين الوضعية والاتفاقيات الدولية)، منشورات صادر، ٢٠٠١، ص ٩٢-٩٩.