

الحرب الإلكترونية وسبأ
التعمير في القانون الدولي
الإنساني

اعداد

المدرس اسامة صبري محمد

المقدمة

الحرب الالكترونية تعتبر سلاح جديد تلجا اليه الدول في النزاعات المسلحة ، وتعد تكنولوجيا المعلومات من الوسائل القتالية في العصر الحديث ، تسطيع القوات العسكرية للدول التي تملك مثل هذه القدرات ، احداث اصابات مادية بالمتلكات او بالأرواح .

تثير الحرب الالكترونية العديد من المسائل القانونية الشائكة ، والتي تحتاج الى المزيد من البحث القانوني ، شأنها شأن الاسلحة الحديثة التي تعتمد على التكنولوجيا ، سواء كانت تدار عن بعد كالمطائرات المسيرة او تلك التي تنتقل عبر الفضاء السيبراني ، كما هو الحال في الحرب الالكترونية .

الحرب الالكترونية دفعت فقهاء القانون الدولي الى دراسة تلك الحرب ، من خلال مقارنة هذه الحرب مع القواعد القابلة للتطبيق في النزاعات المسلحة ، تلك القواعد المتعلقة بمفهوم الحرب ، وموقف القانون الدولي الانساني من الاسلحة الحديثة ، ومدى تطابق مفهوم المقاتل على المهاجم الالكتروني ، والمدنيين المساهمين في الحرب الالكترونية .

البحث محاولة بحثية متواضعة لدراسة الحرب الالكترونية ، في ضوء المستجدات الفقهية في هذا المجال ، بالرغم من ان موضوع الحرب الالكترونية تم التطرق اليه بعمومية ، في بدايات القرن الماضي .

البحث ركز على العلاقة بين مبدا التمييز والحرب الالكترونية ، لبيان مدى تطابق متطلبات هذا المبدأ مع تلك الحرب . مبدا التمييز الذي يحتل مكان الصدارة في القانون الدولي الانساني ، ومنه تتفرع المبادئ الأخرى ، اهمية مبدا التمييز تكمن في ان احترام هذا المبدأ من قبل المقاتلين ، يترتب عليه منحهم امتيازات المقاتلين المتمثلة بنظام اسرى الحرب عند القبض عليهم ، وعدم محاكمتهم عن المشاركة في القتال . علاوة على ما تقدم تبرز اهمية مبدا التمييز في جانب آخر يتمثل بالاسلحة الحديثة ، حيث ان القانون الدولي الانساني يحظر على الدول تصنيع او استيراد اسلحة من شأنها ان تخل بمبدا التمييز ، ويؤدي استعمالها الى حدوث الهجمات العشوائية ، او التسبب بالالام غير المبررة .

قسم البحث الى مبحثين ، تناول المبحث الاول التعريف بالحرب الالكترونية وتميزها عن غيرها من المصطلحات التي ربما تتداخل معها ، كعمليات المعلومات او جرائم الانترنت ، والتطرق الى بعض صور الهجمات التي تعرضت اليها الدول ، والتي اثارت انتباه الدول الى ضرورة ايجاد الوسائل القانونية التي تحكم مثل هذه الحروب ، والسبب في ذلك هو الجدل القانوني حول

مدى امكانية انطباق القانون الدولي الانساني على الحرب الالكترونية ، والتشكيك في مدى الانطباق القانون الدولي الانساني ، تنطلق من نطاق تطبيقه ، حيث ان القانون الدولي الانساني يطبق في النزاعات المسلحة ، والسؤال الذي يطرح هنا هل تعد تلك الحروب هجمات دفاعية او هجومية لتتدر بوجود النزاع المسلح ؟ وبالتالي يبيح للدول حق الدفاع عن النفس ، الاجابات على تلك الاسئلة تنازولها المطلب الاول .

الحرب الالكترونية وما تتضمنه من تكنولوجيا ، اصبحت وسيلة قتالية تلجا اليها الدول في النزاعات المسلحة ، مبررة اللجوء الى مثل تلك الوسائل ، بان تلك الوسائل كفيلة بتجنب الخسائر العرضية في الممتلكات والارواح ، بما ان تكنولوجيا اصبحت وسيلة قتالية في النزاعات الحديثة ، اصبحت من الضروري البحث في مدى استيفاء تلك الوسائل لمتطلبات القانون الدولي الانساني في مسألة الاسلحة الحديثة ، كانت تلك المسألة مدار البحث في المطلب الثاني .

تناول المبحث الثاني العلاقة بين مبدأ التمييز والحرب الالكترونية . فتم التعريف بمبدأ التمييز في القانون الدولي الانساني بشكل عام ، وبيان المسألة النقاشية المتعلقة بالمقاتلين ، وذلك في المطلب الاول .

يختم البحث بالمطلب الثاني للمبحث الثاني ، الذي يجيب على السؤال المتعلق بمدى امكانية تطبيق مبدأ التمييز على الحرب الالكترونية ، واستيفاء تلك الحرب لمتطلبات المبدأ .

البحث محاولة قانونية متواضعة لاستكشاف التحديات التي تواجه القانون الدولي الانساني في زمن النزاعات المسلحة المعاصرة ، تلك التحديات التي بدأت تثير العديد من الاسئلة حول مدى فعالية القواعد الحالية لتستجيب لمتطلبات تلك النزاعات ، لان من وضع تلك القواعد لم يكن يتوقع المستجدات في النزاعات المسلحة ، والوسائل الجديدة التي تلجا اليها الدول ، ومع ذلك تبقى تلك القواعد الحارس الامين لحماية الفئات الضعيفة التي تجد نفسها تكوى بويلات النزاعات المسلحة .

المبحث الأول

مفهوم الحرب الالكترونية

حظيت المسائل القانونية التي أثارها احتمال شن عمليات عدائية في الفضاء الالكتروني وعبره باهتمام كبير للغاية خلال السنوات الماضية ، فقد اوجد الفضاء الالكتروني على ما يبدو ميدانا جديدا للقتال وساحة جديدة للحرب من صنع الإنسان تضاف الى ساحاتها الطبيعية المتمثلة في الأرض والجو والبحر والفضاء الخارجي وترتبط بجميع هذه الساحات الطبيعية .

يتناول هذا المبحث في المطلب الأول التعريف بالحرب الالكترونية بينما يتناول المطلب الثاني موقف القانون الدولي الإنساني من الأسلحة الجديدة ، وذلك لتحديد العلاقة بين الحرب الالكترونية كسلاح جديد واليات القانون الدولي الإنساني لتقييم مدى مطابقة الأسلحة الجديدة للقانون الدولي الإنساني .

المطلب الأول

التعريف بالحرب الالكترونية

المشكلة الاساسية في ايجاد تعريف مقبول لا يتأتى من غياب الاجماع بين فقهاء القانون الدولي على تعريف موحد للحرب الالكترونية ، بل كذلك من الطبيعة القانونية المتغيرة لمصطلحات متطورة ظهرت في الآونة الأخيرة في سياق النزاعات المسلحة مثل الهجمات الالكترونية عن طريق الشبكة العنكبوتية ، ويرجع السبب في ذلك ان الهجمات على شبكات الحواسيب هي ظاهرة حديثة نسبيا ، وقد تم وصفها بانها عمليات تهدف الى تعطيل ، او منع ، تحلل ، او تدمير المعلومات في اجهزة الكمبيوتر ، وشبكات الانترنت ، وقد تكون الحرب موجهة ضد صناعات وبنى تحتية واتصالات ، او ضد بلدان بأكملها .

عرف ايدكنز الحرب الالكترونية بانها (اي عمل الغاية منه ارغام الخصم على الخضوع لأرادتنا الوطنية ، وتنفيذ برنامج الغاية منه السيطرة على نظام معلوماته) ، بينما عرف وينكفيلد هجمات انظمة الحاسوب (بانه نوع من حرب المعلومات التي تؤدي الى احداث خلل في انظمة

المعلومات للخصم) ، بينما يعرف حرب المعلومات السيد شايفورد (حرب المعلومات يقصد بها توظيف اجهزة الحاسب وكل ما يتعلق بتكنولوجيا المعلومات لمهاجمة شبكات الانترنت ذات الصلة بمصادر المعلومات المدنية او العسكرية او الحكومية للخصم) . (١)

يبين السيد ريتشارد كليرك في كتابه (حرب الانترنت) السيناريوهات التي تلجا اليها الدول في اطار حرب الانترنت ، مثل قيام حكومات الدول الاجنبية بتوجيه هجمات الى محطات توليد الطاقة الكهربائية او مراكز ضخ البترول ، في عام ٢٠٠٧ قامت اسرائيل بتوجيه هجمات الكترونية الى ضد سوريا تمكنت من خلالها تعطيل منظومة الصواريخ المضادة للطائرات مما مكنها من توجيه ضربات الى المفاعل النووي السوري السري . (٢) كما تعرضت شبكات الانترنت الحكومية والبنكية الاستونية في ٢٠٠٧ (٣) ، وفي ٢٠٠٨ شنت روسيا هجوم الكتروني ضد جورجيا (٤) ، وما تعرضت الية المنشآت النووية الايرانية عن طريق توجيه فيروس أطلق عليه (Stuxnet) في ٢٠١٠ والذي يعتبر اول فايروس يصيب اجهزة السيطرة في معدات التصنيع والمسؤولة عن السيطرة الحساسة في تلك الاجهزة . (٥)

ولا بد من التميز بين حرب المعلومات وعمليات المعلومات ، حيث تعرف العمليات المعلوماتية بانها (الاعمال التي تنفذ للتأثير على معلومات العدو ونظم معلوماته ، في نفس الوقت حماية المعلومات ونظم المعلومات الخاصة بالمهاجم ، وتشمل هذه العمليات في الواقع اي اجراءات تتخذ بغير رضا متبادل بهدف اكتشاف العمليات المخزنة في احد اجهزة الحاسوب او تغييرها او تدميرها او تشويها او تحويلها ، او البيانات التي تستخدم او تنقل عن طريق احد الاجهزة . ويمكن ان يحدث ذلك في اوقات السلم او في الازمات على حد سواء ، او على المستويات الاستراتيجية او العملياتية او التكتيكية في نزاع مسلح) . اما حرب المعلومات فأضيق من ذلك ، فهي عمليات معلوماتية تجري اثناء الازمات او النزاع لتحقيق او تعزيز اهداف معينة ازاء عدد او اعداد محددين ، لذلك تختلف حرب المعلومات عن العمليات المعلوماتية الاخرى من حيث السياق الذي تجري فيه ، وهي الازمات او المنازعات (٦) ، كما تميز عن الهجمات الحركية ، حيث تهدف الاخيرة الى تحقيق اهداف مادية ، كالسيطرة على ارض الخصم ، بينما الهجمات الالكترونية لا تؤدي بالنهاية الى نتائج مادية ملموسة على ارض الدولة المستهدفة . الهجمات الإلكترونية تدار عن بعد ولها اهداف متعددة ، فقد يكون الهدف من الهجوم او سلسلة الهجمات تحقيق اهداف بسيطة للمهاجم كإيقاف شبكة المعلومات المستهدفة لوقت قصير ، وذلك لمنع الدولة المستهدفة من الاستفادة من هذه الشبكة ، وبالتالي تقويض نظام الامن فيها . (٧)

وعرف التقرير الحادي والثلاثين للجنة الدولية للصليب الأحمر العمليات السببرانية (المعلوماتية) بأنها ((عمليات تشن ضد او عبر حاسوب او نظام حاسوبي بواسطة تيار بيانات . وقد تهدف هذه العمليات الى تحقيق أغراض مختلفة تضم على سبيل المثال اختراق نظام معين وجمع او نقل او تدمير او تغيير او تشفير البيانات ، او إجراء او تعديل العمليات التي يتحكم بها الجهاز الحاسوبي المخترق او التلاعب بهذه العمليات . ويمكن بالتالي استخدام هذه الوسائل لتدمير او تعديل او تعطيل مجموعة متنوعة من الأهداف في العالم الحقيقي ، كالصناعات والبنى الأساسية والاتصالات المالية))^(٨)

الاتفاقية الوحيدة التي عرفت هجمات المعلومات هي اتفاقية جرائم الانترنت^(٩) ، الا ان عدم تبني الاتفاقية من عدد كبير من الدول لم يجعلها ملزمة بموجب القانون الدولي العرفي ، علاوة على انها لا تتعلق بهجمات الانترنت بقدر تعلقها بكيفية موازنة التشريعات الوطنية للدول الموقعة للاتفاقية، وتشريع قوانين مناسبة لتجريم الاعمال المتعلقة بأساءه استخدام الانترنت^(١٠)

وهناك سيناريوهات عديدة لحرب المعلومات ، تتمثل في إغلاق محطات الدفاع الجوي حيث يقوم المبرمجين العسكريين من خلال هجمات حاسوبية لتعطيل محطات الدفاع الجوي لفترة من الزمن لغرض تنفيذ الضربات الجوية ، من خلال إرسال فيروس لتعطيل الدفاعات الجوية دون ألاحق ضرر مادي او تدمري بالمحطة . او اختراق شبكة الدفاع المركزية كما حصل في عام ١٩٩٠ خلال حملة النانو على كوسوفو ، حيث قام المخططين العسكريين المعنيين بتكنولوجيا المعلومات بإرسال رسائل خاطئة الى شبكة القيادة المركزية للدفاع الجوي الصربي ، والتي ادت الى تقليل قدرة الصرب بتحديد الأهداف المتوقع ضربها من قبل النانو . توجيه هجمات الى مراكز إنتاج الطاقة للحيلولة دون استخدامها لأغراض مدنية او عسكرية ، حيث تلجأ الولايات المتحدة الأمريكية الى توجيه مثل هذه الهجمات الى محطات إنتاج الطاقة والاتصالات والبنى التحتية للنقل ، وذلك للحيلولة دون استفادة الخصم منها في إدامة زخم المعركة . واستخدام حرب المعلومات لإسكات مراكز البث الإذاعي والتلفزيوني التي تساهم في الدعاية الحربية للخصم.^(١١)

نتيجة للتطور المطرد لتكنولوجيا المعلومات ، وغياب القواعد القانونية التي تحظر حرب المعلومات في القانون الدولي ، هذا الغياب يشير الى وجود تصريح ضمني بها ، مما يدفعنا الى البحث عن وثائق قانونية دولية يمكن ان تساعد في إيجاد قواعد تحظر تلك الحرب .أدرجت هجمات الانترنت في معاهدة الاتصالات الدولية ، والتي تطبق على الاتصالات السلكية واللاسلكية الدولية ، من الناحية العملية المعاهدة لا تحد من هجمات الانترنت ، الا انه يمكن تطبيق بعض القواعد الواردة في الاتفاقية على هجمات الانترنت كذلك المتعلقة بمحطات الإذاعة

وعدم جواز تداخل ارسالها مع ارسال اذاعات الدول الاخرى دون موافقة الاخيرة ، بالإضافة الى واجب الدول في حماية خصوصية اجهزة الارسال الدولية اذ لا يجوز لتلك الدول ايقاف العمل بتلك الاذاعات لا سباب امنية . الا انه مع ذلك ان تلك القواعد المتعلقة بالاتصالات اللاسلكية لا يمكن ان تطبق على المقاتلين في النزاعات المسلحة ، كما انه يلاحظ ان مخالفة هجمات المعلومات لبند الاتفاقيات تعد مخالفة للالتزامات تعاقدية بموجب المعاهدة ، مع الاخذ بنظر الاعتبار ان فعل الاعتداء يبيح استخدام القوة في اطار الدفاع عن النفس ، وهذا رد الفعل لا يمكن تصوره في حالة مخالفة التزامات تعاقدية .^(١٢)

استنادا الى الاستراتيجية الامم المتحدة العسكرية فيما يتعلق بحرب المعلومات عام ٢٠٠٦ (عمليات شبكات الحاسبة تتضمن هجمات شبكات الحاسبات والدفاع المعلوماتي واستغلال شبكات الحاسبات ، وكلها تشكل حرب المعلومات) . وتتمثل هجمات المعلومات بتوجيهها ضد شبكات الحاسبات لتقليل او تعطيل فعاليتها وغالبا ما توجه تلك الهجمات الى شبكة الحاسبات الخاصة بمراكز القيادة مما يؤدي الى احداث اضرار جسيمة في صفوف القوات التي تتلقى توجيهات من مراكز السيطرة التي تم مهاجمتها من قبل الخصم ، ويحدث الضرر بأشكال مختلفة كإرسال معلومات متدفقة الى تلك الاجهزة او احداث اضرار مادية او تعطيل الاقراص الصلبة او ارسال فيروسات مثل فايروس تورجان .^(١٣)

السؤال المطروح هنا ، هل تخضع الهجمات الالكترونية الى القانون الدولي الانساني ؟ ابتداء لا توجد قواعد قانونية في اتفاقيات القانون الدولي الانساني تتعامل بشكل مباشر مع الهجمات الالكترونية ، الهجمات الالكترونية والعمليات الالكترونية غير منظمة في النزاعات المسلحة ، اضافة الى ان تطوير الهجمات الالكترونية حصل في فترة لاحقة على اعداد صكوك القانون الدولي الانساني، كما ان القانون الدولي الانساني وضعت قواعده لتنظيم وسائل واساليب القتال ذات الطبيعة المتحركة التي تنتج عنها اثار مادية غير متوفرة في الهجمات الالكترونية ، وبالتالي فان الهجمات الالكترونية تكون خارج نطاق القانون الدولي الانساني ، اي بعبارة اخرى ان القانون الدولي الانساني يطبق في النزاعات المسلحة ، والهجمات الالكترونية ليست مسلحة، ولكن يمكن تطبيق شرط مارتنز على الهجمات الالكترونية .^(١٤) مع ذلك غياب القواعد المتعلقة بصورة خاصة بالهجمات الالكترونية ، لا يعني ذلك ان مثل هذه الهجمات لا تخضع لقواعد القانون الدولي الانساني، اذا وسائل واساليب الحرب الالكترونية تنتج نفس الاثار التي تنتجها الاسلحة التقليدية (كأحداث الدمار او اصابة الافراد بجروح او التسبب بالموت) ، فأنها تخضع لنفس القواعد التي تحكم الاسلحة التقليدية ، الا انه مازالت هناك صعوبة في تطبيق تلك القواعد على الحرب الالكترونية ، والسبب في ذلك يعود الى طبيعة وسائل تلك الحرب التي مازالت غير

مفهومة ، ويقنصر الفهم على الخبراء الذين يطورون تلك الوسائل ، كما ان تطويرها دائما يحاط بسرية ، وعليه فان نقطة الابتداء هي التعرف عن كئب على تلك الوسائل واثارها في النزاعات المسلحة .^(١٥)

القواعد القانونية الخاصة بالهجمات الالكترونية لا تشتق من القانون الدولي الانساني ، بل من المبادئ والقواعد المشتقة من القانون الدولي وقت السلم ، بل من قواعد حقوق الانسان التي لا تلزم الدول فقط بل الجماعات المسلحة أيضا.^(١٦)

السؤال القابل للطرح هنا ، هل تعد الهجمات الالكترونية هجمات مسلحة ؟ . عرفت المادة ٤٩ فقرة ١ وفقرة ٢ من البروتوكول الاضافي الاول الملحق باتفاقيات جنيف الهجوم بانه ((١-تعني الهجمات اعمال العنف الهجومية والدفاعية ضد الخصم ٢- تنطبق احكام هذا اللحق البروتوكول المتعلقة بالهجمات على كافة الهجمات في اي اقليم نشن منه بما في ذلك الاقليم الوطني لاحد اطراف النزاع والواقع تحت سيطرة الخصم)) . استنادا الى ذلك التعريف ، ان الهجمات لا تقتصر على استعمال السلاح بل يمكن ان تمتد الى الوسائل التي يشكل اللجوء اليها عمل عدائيا . اجابة الاستاذة Ziolkowski على ذلك التساؤل بالقول (تعد الهجمات الالكترونية شبه هجمات عسكرية ، اذا تأثر الافراد او الممتلكات) وتضيف بالرغم من النقص في القواعد المنظمة للهجمات الالكترونية ، يلاحظ ان البروتوكول الاضافي يشير الى انه قابل للتطبيق في الظروف التي لم تؤخذ بنظر الاعتبار في المؤتمر الدبلوماسي ١٩٧٧ ، فعلى سبيل المثال المادتين ٣٨ و ٣٩ من البروتوكول الاضافي الاول والمادة ١٢ من البروتوكول الاضافي الثاني ، التي تحظر اساءة استعمال الشارة المميزة او اخفاء العلامات الالكترونية ، مع ذلك يمكن ان نعد الهجمات الالكترونية خاضعة لحظر الغدر ، الذي ورد في المواد ٣٧ و ٤٨ من البروتوكول الاضافي الثاني والمادة ١٣ من البروتوكول الاضافي الثاني .^(١٧) يذهب الاستاذ Zemanek الى القول (ليس تصميم الالة او الاستخدام الطبيعي لها تجعل منه سلاحا ، بل نية المستخدم في توظيف تلك الالة في احداث اضرار ، وعليه فان استخدام الآلات ، استخداما من شأنه تدمير الممتلكات او احداث اضرار بالأنفس ، عندها تستوفى متطلبات النزاع المسلح ، ذلك الاستنتاج تم تأييده عند اعادة مجلس الامن التأكيد على حق الدفاع عن النفس بعد احداث ١١ ايلول ٢٠٠١ .^(١٨)

اتجاه الدول الى معاهدة دولية تتعلق بالحرب الالكترونية ، يواجه تحديات عديدة ، تتمثل في ضعف الارادة لدى الدول التي تتعامل مع الفضاء الالكتروني ، اذا امكن التوصل الى مثل هذا التوافق بين الدول ، فان تطبيق الاتفاقية سيواجه بتحديات تقنية سلبية ، اي فرض لتلك البنود

يحتاج مشاركة عامة وخاصة ، وجهود تبذل للتمييز بين الدول والجماعات المسلحة ، والحاجة الى تشريعات لتفعيل بنود الاتفاقية .^(١٩)

المطلب الثاني

القانون الدولي الإنساني والأسلحة الجديدة

حق المقاتلين في اختيار وسائلهم القتالية واساليبهم في المعركة ليست مطلقة . حقوق المقاتلين في اختيار وسائلهم واساليبهم القتالية مقيدة بالعديد من قواعد القانون الدولي الانساني المتعلقة بأسلوب القتال ، العديد منها يتضمنه البرتوكول الاضافي الاول الملحق باتفاقيات جنيف لعام ١٩٧٧ . وهناك عدد من الاتفاقيات التي تحظر او تقيد استخدام نوع معين من الاسلحة مثل الاسلحة الكيميائية والبيولوجية واسلحة الليزر التي تسبب العمى^(٢٠) ، كما توجد العديد من القواعد العرفية في القانون الدولي التي تحظر او تمنع بعض اساليب ووسائل القتال .^(٢١)

اول وثيقة دولية دعت الى ضرورة اجراء المراجعة القانونية للأسلحة الحديثة هي اعلان سان بطرسبورغ عام ١٨٦٨ . وسبق الاعلان جهود الفقيه كروسيوس في كتابه *Deiure belli ac pacis* المنشور في ١٦٢٥ الذي اشار الى ضرورة فرض قيود على القوة المدمرة للأسلحة وقد واجه هذا المبدأ اعتراض بين عامين ١٦٢٥ و ١٩٠٧ ، واعيد التأكيد على هذا المبدأ في اتفاقية لاهاي ١٩٠٧ في المادة ٢٢ التي تنص على ((ليس للمتحاربين حق مطلق في اختيار وسائل الحاق الضرر بالعدو)) . وفي عام ١٩٦٥ وخلال المؤتمر العشرين للجنة الدولية للصليب الاحمر تبنى المشاركون المبدأ الذي يقضي بان حق المحاربين في استخدام الاسلحة التي تلحق ضرر بالخصم ليس مطلق ، وهذا الاتجاه تبنته الجمعية العامة للأمم المتحدة في عام ١٩٦٩ .^(٢٢)

العلاقة بين القانون الدولي الانساني والاسلحة الحديثة تتجسد في المادة ٣٦ من البرتوكول الاضافي الاول لعام ١٩٧٧ التي تنص على ((يلتزم اي طرف سام متعاقد ، عند دراسة او تطوير او اقتناء سلاح جديد او اداة للحرب او اتباع اسلوب للحرب ، بان يتحقق مما اذا كان ذلك محظورا في جميع الاحوال او في بعضها بمقتضى هذا اللحق -البرتوكول - او اي قاعدة اخرى من قواعد القانون الدولي التي يلتزم بها الطرف السامي المتعاقد)) .^(٢٤)

الغرض من المادة ٣٦ منع استخدام الأسلحة التي من المحتمل استخدامها يشكل ، انتهاك للقانون الدولي في كل الظروف ، وفرض قيود على استخدام الأسلحة التي تخالف القانون الدولي في بعض الظروف ، من خلال تحديد الجوانب القانونية قبل تطويرها والاستحواذ عليها ، المادة ٣٦ تستكمل بالمادة ٨٢ من البرتوكول الإضافي الأول التي تلزم الدول الأطراف بتوفير المستشارين القانونيين في كل وقت لتقديم المشورة القانونية للقادة ، كلا المادتين تشكلان الإطار القانوني لضمان قدرة القوات المسلحة بالقيام بأعمال عسكرية متوافقة مع القانون الدولي الإنساني، من خلال تقييم وسائل وأساليب القتال .^(٢٥)

المادة ٣٦ مثلت محاولة البرتوكول انشاء علاقة بين نصوصه تلك الواردة في المادة ٣٥ (القواعد العامة)^(٢٦) وانتاج الاسلحة من قبل الدول (المادة ٣٦) . المبدأ الاساس في هذه المادة ان الدول المتعاقدة تأخذ على عاتقها بقدر الامكان تحديد احتمالية ان تكون الاسلحة الحديثة ذات طبيعة غير قانونية وفقا لمواد البرتوكول واية مادة قانونية قابلة للتطبيق من قواعد القانون الدولي العام.^(٢٧)

هناك عاملان يحددان ما اذا كان السلاح جديد ام لا اولا : بالرجوع الى الدولة التي تنوي استخدامه ، فواقع ان سلاحا ما اذا كان موجودا في الخدمة في دولة معينة لبعض الوقت قبل بيعه لدولة اخرى لا يمنع الدولة المتلقية من اعتبار السلاح جديد وفقا لنص المادة ٣٦ . ثانيا : بالرجوع الى تاريخ دخول السلاح الخدمة ، فعند تصديق الدولة على البرتوكول الاضافي الاول ، لا يمكن اعتبار الاسلحة الموجودة بالفعل في الخدمة جديدة في اطار نص المادة ٣٦ . ولكن ربما يكون من قبيل الحيلة للدولة ان تجري مراجعة لهذه الاسلحة التي تخضع للفحص الدولي الدقيق حتى تستطيع الدفاع عن امتلاكها واستخدامها لها بشكل اكثر قوة ، وان كانت المادة ٣٦ لا تستوجب ذلك.^(٢٨)

ومعايير المراجعة التي تلجا اليها الدول للتأكد من مدى توافق الاسلحة ووسائل الحرب مع الالتزامات القانونية للدول بموجب القانون الدولي ، لا بد من وضع خمسة مجالات في الاعتبار . وبداية ، لا بد من الاقرار بالتوازن الواجب تأمينه بين الضرورة العسكرية من جانب ، ومستوى المعاناة من جانب اخر وهو ما يشار اليه غالبا بمبدأ التناسب ، ويتصدر هذا التوازن الاهمية عند دراسة المعايير ، لأنه يؤثر على نوع الادلة المطلوبة لأجراء المراجعة القانونية .^(٢٩)

هذه الالتزامات لا تطبق فقط على الدول المصنعة بل كذلك على الدول القائمة بالشراء ايضا ، بالرغم من المادة ٣٦ لا تطالب تحديدا بالنظر في شرعية الاسلحة المصدرة ، فان على الدول ان

تفعل ذلك وهذا امتداد منطقي للواجب المنصوص عليه في المادة ١ المشتركة لاتفاقيات جنيف ١٩٤٩ . (٣٠)

العديد من الدول تقوم بشراء الاسلحة من الدول المصنعة لها ويمكن ان تكون الأخيرة طرفا في البروتوكول وبالتالي تلتزم بما ورد في المادة ٣٦ تعتمد على المراجعة القانونية من قبل هذه الدول، الا انه لا يجوز للدولة (المشتري) ان تعتمد على الاجراءات التي اتخذتها الدولة المصنعة ، بل يجب عليها ان تقوم بإجراءات ذاتية لتقييم استخدام الاسلحة المشتراه ومدى مطابقتها للبروتوكول او اية قاعدة قانونية قابلة للتطبيق من قواعد القانون الدولي ذات الصلة . ولكن يجب ان لا تفسر المادة على انها تحظر بيع او استيراد الاسلحة . نطاق المادة ٣٦ لا تعني انها تحظر انتاج الاسلحة التي تحاكي المستقبل وذلك لأنه ليس من المعقول ان الدول عندما تقوم بإنتاج هذه الاسلحة ستنتهك قواعد القانون الدولي التي تحظر الاسلحة التي لا تتوافق مع متطلبات القواعد العامة التي وردت في المادة ٣٥ من البروتوكول الاضافي الاول . (٣١)

بالإضافة الى القانون الدولي الاتفاقي القابل للتطبيق على الموضوع ، مراجعة الدول يجب ان تكون في اطار قواعد القانون الدولي العرفية المتعلقة بأساليب ووسائل القتال ، دون الحاجة الى البحث عن الطبيعة العرفية للقواعد . محكمة العدل الدولية في رايها الاستشاري فيما يتعلق بشرعية استخدام الاسلحة النووية ، بينت المبادئ الاساسية التي تكون القواعد العرفية للقانون الدولي الانساني . كمبدأ التمييز وعدم استخدام الاسلحة التي لا تستطيع التمييز بين الاهداف المدنية والعسكرية وحظر الاسلحة التي تسبب الالام غير مبررة للمقاتلين . كذلك في حالة فشل الدول في اجراء التقييم بموجب قواعد القانون الدولي الاتفاقي او العرفية ، فيمكن اجراء التقييم في ضوء قواعد تتضمن المبادئ العامة التي وردت في الراي الاستشاري والتي نجدها في المادة ٣٥ ف٢ والمادة ٤٨ وكذلك المادة ٥١ من البروتوكول الاضافي الاول . علاوة على ما تقدم فانه يمكن الركون الى شرط مارتنز ، الأسلحة التي تغضب المجتمع الدولي تعتبر محظورة بموجب الشرط ، والذي اكدت محكمة العدل الدولية اهمية شرط مارتنز باعتباره قابلا للتطبيق دون ادنى شك ، مع ذلك ان المادة ٣٦ لا تقيد أنواع الأسلحة الجديدة او الأسلحة المستقبلية ، بل تطبق على الأسلحة الحالية . (٣٢)

لغرض تهيئة وسائل تساعد الدول في تبني اليات مراجعة قانونية للأسلحة ، في عام ٢٠٠٦ اللجنة الدولية للصليب الاحمر اعتمدت الدليل الارشادي للمراجعة القانونية للأسلحة الحديثة ، واساليب ووسائل القتال ، الذي اعد بالتشاور مع ما يقارب من ثلاثين من الخبراء العسكريين

والقانونيين ، بضمنهم خبراء حكوميين من عشرة دول . الدليل يعتمد على مصادر اولية واليات رسمية مكتوبة موجودة بصورة عامة او توفر من قبل الدول للجنة الدولية للصليب الاحمر .

اللجنة الدولية للصليب الاحمر خلال المؤتمر السابع والعشرين والثامن والعشرين للصليب الاحمر والهلال الاحمر دعت الدول الى تبادل المعلومات ، فيما يتعلق بالياتها الخاصة بالمراجعة القانونية ، كما ان الدليل ناشد الدول الاطراف بالبروتوكول الاضافي الاول ، بضرورة تقاسم المعلومات واجراءات المراجعة مع الدول الاخرى الاطراف بموجب المادة ٨٤ ، التي تلزم الدول بالتشاور فيما بينها .^(٣٣)

الالتزامات المتعلقة بالمراجعة القانونية للأسلحة الحديثة تتلخص ، اولا الدولة عليها اتخاذ اجراءات دائمة اي الية ثابتة تنشط تلقائيا لتقييم الاسلحة الحديثة ، والثاني يتعلق بأنشاء هيئة تكون مسؤولة عن التطوير للأسلحة .^(٣٤)

ممارسة الدول فيما يتعلق بتطبيق المادة ٣٦ محدودة ، حيث عدد قليل من الدول تبنت اجراءات للمعالجة القانونية ، ومن هذه الدول استراليا ، النرويج ، السويد و الولايات المتحدة الامريكية ، ومعلومات تشير الى تبني دول اخرى كبلجيكا ، كندا ، الدنمارك ، المانيا و هولندا حيث تبنت اما اليات وطنية او اجراءات للمراجعة القانونية .^(٣٥)

وتعتبر السويد الدولة الأولى التي قامت بتشكيل هيئة مستقلة مسؤولة عن المراجعة القانونية لشرعية الأسلحة ، الذي أطلقت عليه مشروع القانون الدولي الإنساني لمراقبة الأسلحة الذي تشكل في عام ١٩٧٤ اي قبل تبني البرتوكول الإضافي الأول ١٩٧٧ ، والغاية من تشكيله التأكد من أن الأسلحة المستخدمة من قبل القوات السويدية متطابقة مع الالتزامات الدولية ، والولايات المتحدة الأمريكية الموقعة على البرتوكول الإضافي الأول في ١٢/١٢/١٩٧٧ تبنت إجراءات كفيلة بضمان ان تكون الأسلحة خاضعة للمراجعة القانونية ، وهذا النظام تم تأسيسه في ١٩٧٤ نتيجة لحرب فيتنام ، الذي دعا وزارة الدفاع الأمريكية لتقييم مدى التزام الولايات المتحدة لالتزاماتها الدولية في ضوء قانون الحرب ، وتعتبر المراجعة القانونية في الولايات المتحدة من الوظائف التنفيذية للوكالات المتخصصة ، حيث تعتبر المسؤولة ابتداءً في إجراء المراجعة .^(٣٦)

في ضوء التطور المطرد لتكنولوجيا التسليح في الوقت الحاضر ، تبقى المادة ٣٦ ذات أهمية من الناحية التطبيقية، ومن المؤمل ان تتضافر الجهود الدولية وتقاسم المعلومات من خلال إجراءات مراجعة وطنية ، التي تتيح للدول الفهم الجيد لإجراءات المراجعة وتطويرها وتدعيم التعاون ما بين الدول ، ولا يتأتى ذلك الا من خلال تفعيل المادة ٣٦ وتشجيع الدول لتبني آليات مراجعة

على المستوى الوطني ، بالإضافة إلى أساليب تنظيمية تشمل الخبراء القانونيين وغيرهم ممن له صلة بمجال التسليح .^(٣٧)

ويعد مجالات الاتصالات مثالا جيدا على أسلوب تطبيق نص المادة ٣٦ في مواجهة التقنيات المستجدة ، فلا شك أن نظم الاتصالات تتزايد تعقيدا يوما بعد يوم ، وهي لا تنقل المعلومات فحسب ، بل لها القدرة أيضا على ترتيب المعلومات المنتجة وتحليلها ، ونشرها ، وتخزينها ، واسترجاعها ، وعرضها في مراحل أعداد العمليات العسكرية و تنفيذها ، وإدخال المعلومات الرقمية الى ساحة المعركة يعزز من قدرة الاتصال بالشبكات التي تتيحها هذه التقنية ، وعند تحديد مدى انطباق المادة ٣٦ ، لا بد من فهم كيفية عمل نظم الاتصالات في الواقع ، و لا يتضمن ذلك فهم العلم وحسب ، بل أيضا فهم الاستخدام الحربي لهذا العلم ، وحينئذ فقط يمكن تحديد اذا ما كان النظام يمتلك قدرة هجومية ام لا ، فإذا كان يمتلك ، فما هو الأسلوب المتوخى لاستخدام هذه القدرة ، هل سوف يستخدم النظام على سبيل المثال لتحليل بيانات الهدف ومن ثم تقديم حل له او صوره عنه ؟ فإذا كان الأمر كذلك ، فمن المنطقي ان يقع دور نظام الاتصال في أطار معنى وسائل وأساليب الحرب لأنه بذلك يوفر جزءا لا يتجزأ من عملية اتخاذ قرار الاستهداف ، أما اذا كان نظام الاتصال يجمع البيانات ويصنفها بطريقة بحيث يضع صورة بيانية لمواقع التشكيلات العسكرية دون تغيير طبيعة البيانات او فحواها ، او اذا كان ببساطة ينقل البيانات من موقع إلى آخر ، فلا يعد واقعا في نطاق وسائل وأساليب الحرب .^(٣٨)

السؤال هنا ، هل تعد الهجمات الالكترونية وسيلة قتال خاضعة للقيود القانون الدولي الإنساني ؟

الاجابة على ذلك تتلخص في انه ، اذا وجهت الهجمات الالكترونية بصورة مباشرة ضد الخصم ، بقصد احداث اضرار له ، مثل تعطيل نظام المراقبة الجوية ، مما يؤدي الى حدوث اصطدام جوي ، هنا تعتبر الهجمات الالكترونية وسيلة من وسائل القتال الخاضعة لقيود القانون الدولي الانساني .^(٣٩)

المبحث الثاني

تطبيق مبدأ التمييز في الحرب الالكترونية

يعد مبدأ التمييز من المبادئ الأساسية في القانون الدولي الإنساني ، وعلى هذا الأساس يتمتع المقاتلون بامتيازات تتمثل في نظام أسرى الحرب وعدم محاكمتهم عن فعل القتال ، يتحقق ذلك عندما يحترم المقاتلون هذا المبدأ في العمليات العسكرية ، كما ان شرعية استخدام الاسلحة تستمد من مدى قابلية تلك الاسلحة للمحافظة على هذا المبدأ والابتعاد عن توجيه الهجمات العشوائية ، وبما ان الحرب الالكترونية تعتبر من اساليب القتال الحديثة فان هذا المبحث يسلط الضوء على مدى استيفاء هذا الاسلوب لمتطلبات مبدأ التمييز ، الا انه قبل الشروع في بيان هذه العلاقة ، لا بد من تعريف مبدأ التمييز في القانون الدولي الإنساني وذلك في المطلب الاول ، ثم دراسة العلاقة مدى امكانية تطبيق المبدأ في الحرب الالكترونية في المطلب الثاني.

المطلب الأول

تعريف مبدأ التمييز في القانون الدولي الإنساني

عرفت الشريعة الإسلامية مبدأ التمييز ، عندما نهى الرسول عليه الصلاة والسلام عن قتل النساء والأطفال ورجال الدين المعتزلين والشيوخ .^(٤٠) وشهدت نهايات القرن الثامن عشر وبدايات القرن التاسع عشر استقرار التفرقة بين المقاتلين وبين غير المقاتلين ، ولم تعد الخصومات الحربية معتبرة كقتال بين المدنيين بعضهم البعض وإنما كقتال بين سلطات الدول ، وقد عبر بورتاليس عن ذلك الفقه ، في مطلع القرن التاسع عشر ، في افتتاح محكمة الغنائم الفرنسية ١٨٠١ عندما قرر أن الحرب علاقة دولة بدولة لا فرد بفرد ، وانه بين آمتين متحاربتين ، لا يكون الأفراد الذي تتكون منهم تلك الأمم أعداء إلا بصفة عرضية ، وليس بوصفهم كرجال او كمواطنين وإنما فقط بوصفهم كجنود .^(٤١)

ورد مبدأ التمييز بين المدنيين والمقاتلين للمرة الأولى في إعلان سان بطرسبورغ الذي ينص على (ان الهدف المشروع الوحيد الذي يتعين على الدول ان تسعى الى تحقيقه أثناء الحرب هو أضعاف القوات العسكرية للعدو) . ولا تنص لائحة لاهاي المتعلقة بقوانين الحرب البرية في حد ذاتها على وجوب التمييز بين المدنيين والمقاتلين ، ولكن المادة ٢٥ التي تحظر مهاجمة او قصف المدن والقرى والأماكن السكنية او المباني المجردة من وسائل الدفاع ايا كانت الوسيلة المستعملة تستند الى هذا المبدأ .^(٤٢)

وورد مبدأ التمييز في المادة ٢٢ من مدونة لير التي تعد اول وثيقة دولية جامعة للقواعد التي تحكم الحرب .

قنن مبدأ التمييز في المادة ٤٨ من البرتوكول الإضافي الأول التي نصت على ((تعمل أطراف النزاع على التمييز بين السكان المدنيين والمقاتلين وبين الأعيان المدنية والأهداف العسكرية ، ومن ثم توجه عملياتها ضد الأهداف العسكرية دون غيرها ، وذلك من اجل تأمين احترام وحماية السكان المدنيين والأعيان المدنية))^(٤٣)، وكذلك في المادة ٥١ ف٢ التي نصت على ((لا يجوز ان يكون السكان المدنيون بوصفهم هذا وكذا الأشخاص المدنيون محلا للهجوم، وتحظر أعمال العنف او التهديد به الرامية أساسا الى بث الذعر بين السكان المدنيين)) والمادة ٥٢ ف٢ ((تقصر الهجمات على الأهداف العسكرية فحسب، وتتحصر الأهداف العسكرية فيما يتعلق بالأعيان على تلك التي تسهم مساهمة فعالة في العمل العسكري سواء كان بطبيعتها ام بموقعها ام بغايتها ام باستخدامها ، والتي يحقق تدميرها التام او الجزئي او الاستيلاء عليها او تعطيلها في الظروف السائدة حينذاك ميزة عسكرية أكيدة)) .

وكذلك حظرت المادة ١٣ ف٢ من البرتوكول الإضافي الثاني جعل السكان المدنيين ، بصفتهم هذه ، وكذلك الأفراد المدنيين محلا للهجوم . وأفتت محكمة العدل الدولية في رأيها الاستشاري بشأن الأسلحة النووية ((أن مبدأ التمييز هو احد المبادئ الرئيسية في القانون الدولي الإنساني واحد مبادئ القانون الدولي العرفي التي لا يجوز انتهاكها)) ، إضافة إلى اجتهاد محكمة العدل الدولية في تقرير عرفية المبدأ ، هناك اجتهادات للمحكمة الجنائية الدولية ليوغسلافيا السابقة ، وخاصة في قضية تاديش ، وقضية ماريتيش ، وقضية كوبريسكيتش ، واجتهادات اللجنة الأمريكية لحقوق الإنسان في القضية المتعلقة بالأحداث التي وقعت في لاتابلا في الأرجنتين .^(٤٤)

في العمليات العسكرية ، يتطلب من المقاتلين اتخاذ اعلى درجة الحيطة لتقليل الخسائر في صفوف المدنيين ، ولذلك فان القادة العسكريين عليهم عند اعداد الخطة العسكرية ، تحديد

الاهداف العسكرية بدقة ، وتجنب ضرب الاهداف البيئية او الاماكن التي تحتوي على مواد خطرة ، وكذلك المنشآت ذات الاستخدام المزدوج التي تشكل صعوبة فيما يتعلق بمبدأ التمييز .

وانطلاقاً من ذلك دأبت اللجنة الدولية للصليب الاحمر ومنذ بدء عملها على ضرورة ادراج مبدأ التمييز في الاتفاقية ، وبعد المداولات التي حصلت خلال جلستي لمؤتمر الخبراء الحكوميين بين عامي ١٩٧١ و ١٩٧٢ ، قدمت اللجنة الدولية للصليب الأحمر مسودة الى المؤتمر الدبلوماسي تتعلق بالقاعدة الأساسية لمبدأ التمييز (لغرض ضمان الاحترام للسكان المدنيين ، وعلى أطراف النزاع قصر عملياتهم العسكرية على تحقيق ميزة واحدة هي تدمير واضعاف الموارد العسكرية للخصم مع المحافظة على التمييز بين السكان المدنيين والمقاتلين ، والاهداف العسكرية والمدنية)^(٤٥) ، وللجنة الدولية للصليب الاحمر وجمعية الهلال الاحمر ممارسات في تأكيد مبدأ التمييز ، فخلال الحرب العراقية - الايرانية اكدت في مذكرة قانونية صدرت في عام ١٩٨٤ ((انتهاكات قواعد واعراف الحرب ، وبصورة خاصة المبدأ الخاص بوجوب تمييز الاهداف العسكرية عن الاهداف والاشخاص المدنيين)) وتذكير اللجنة الدولية في عام ١٩٩٣ اطراف النزاع في ناكورون-كارباخ وتكرر الامر في النزاع المسلح في جورجيا وانغولا .^(٤٦)

المادة ٤٨ من البروتوكول الاضافي الاول ، وردت فيها تعابير متعددة اکتفت بالإشارة اليها ، اي تحيل المادة تلك التعابير الى المواد التي وردت فيها ، فاصطلاح المقاتلين ورد في المادة ٤ من اتفاقية جنيف الثالثة ، ومصطلح السكان المدنيين في المادة ٥٠ من البروتوكول الإضافي الأول ، والاهداف العسكرية في المادة ٥٢ من البروتوكول الإضافي الأول ، ومصطلحي الاحترام والحماية وردا في المادتين ١٢ و ٢٤ من اتفاقية جنيف الأولى لتحسين حال الجرحى والمرضى بالقوات المسلحة في الميدان لعام ١٩٤٩.^(٤٧)

النظام الاساسي للمحكمة الجنائية الدولية يقر بمبدأ التمييز ، المدنيين لا يجوز اعتبارهم اهداف مشروعة لتوجيه الضربات اليهم ، بمعنى ان توجيه الضربات المباشرة اليهم لا يبرر على اساس الميزة العسكرية ، وبعد الفعل انتهاك صريح لمتطلبات الانسانية ، وهذا ما ذهبت اليه محكمة يوغسلافيا السابقة في قضية *Prosecutor v. Martić* (على ان عدم مهاجمة المدنيين من القواعد الاساسية في القانون الدولي الانسانية التي تطبق في كافة النزاعات المسلحة)^(٤٨).

تطور القانون الدولي الانساني لم يتوقف في عام ١٩٤٩ من خلال الرؤية الضيقة لاتفاقية جنيف الثالثة لفئة المقاتلين ، ونتيجة للتطورات التي شهدتها العالم بين عامي ١٩٦٠ و ١٩٧٠ بظهور حركات التحرر الوطني ، صدر البروتوكول الاضافي الاول لعام ١٩٧٧ الملحق باتفاقيات جنيف، ليوسع من نطاق فئة المقاتلين وهذا ما ورد في المادة ٤٣ ف ١ التي نصت على (١- تتكون

القوات المسلحة لطرف النزاع من كافة القوات المسلحة والمجموعات والوحدات النظامية التي تكون تحت قيادة مسؤولة عن سلوك مرؤوسيهيها قبل ذلك الطرف حتى ولو كان ذلك الطرف ممثلاً بحكومة او بسلطة لا يعترف الخصم بها ، ويجب ان تخضع مثل هذه القوات المسلحة لنظام داخلي يكفل فيما يكفل اتباع قواعد القانون الدولي التي تطبق في النزاع المسلح (...). . البرتوكول الاضافي الاول يتطلب شرطين لا طفاء صفة المقاتل ١- القيادة المسؤولة ٢- احترام اعراف الحرب ، اي ان البرتوكول لا يعول على مسالة رفع السلاح علنا او ارتداء الملابس العسكرية حيث يعتبر البرتوكول ان هذه المتطلبات لا تؤدي الغرض فيما يتعلق بتعريف المقاتلين.^(٤٩)

مبدأ التمييز يواجه تحديات كبيرة في ضوء النزاعات الجديدة وذلك لعدة اعتبارات . بعد انتهاء الحرب الباردة أصبحت النزاعات تتخذ طابع داخلي ، حيث أصبحت الدول تقاتل جماعات مسلحة ، تلك الجماعات التي استفادت من التطور التكنولوجي والاقتصادي والسياسي التي شهدها القرن الماضي . في دول مثل أفغانستان ، والكونغو ، والمكسيك ، والصومال ، سيطرت الجماعات المسلحة على أجزاء من البلد . ويتمثل التحدي في اتباع عناصر الجماعات المسلحة أساليب قتال مختلفة ، البعض منها منظم والبعض الآخر غير ذلك ، بل انه في بعض الأحيان لا يرتدون ملابس مميزة ، تسمح بتمييز العدو من الصديق . ونتيجة لذلك عدم تميز المقاتلين انفسهم عن سواهم شكل تحديا كبيرا ، يشير اريك تالبوت الى (ان ازدياد خسائر المدنيين هي نتيجة لعدم القدرة على التمييز بين من هو مستهدف ومن هو محمي) . وتلك النتيجة سببها عدم تميز المقاتلين غير النظاميين لأنفسهم عن المدنيين ، وكذلك المشاركة الواسعة للمدنيين في العمليات العسكرية في النزاعات الحالية .^(٥٠)

المسالة القانونية القابلة للنقاش فيما يتعلق بمبدأ التمييز تتعلق بتعريف المقاتلين ، حيث ان اتفاقيات جنيف عرفت المقاتلين على أساس تقديري ، مع ذلك فان تعريف المقاتلين الذي ورد في البرتوكول الإضافي الأول ليس ذا طبيعة عرفية عند أعداد مسودة البرتوكول ، وهذا يفسر استغراق دول مثل فرنسا وبريطانيا وقتا طويلا في دراسة مسودة البرتوكول قبل المصادقة عليه وذلك لان قواعده ليست عرفية وخاصة فيما يتعلق بالمقاتلين .^(٥١)

اتفاقية جنيف الثالثة عرفت المقاتلين من خلال بيان فئاتهم وذلك في المادة ٤ ، وبدأت بأفراد القوات المسلحة في الفقرة الاولى . مصطلح أفراد القوات المسلحة حل محل مصطلح الجيش الذي ورد في المادة الأول من اتفاقية لاهاي (ان قوانين الحرب وحقوقها وواجباتها لا تنطبق على جيش فقط ، بل تنطبق أيضا على أفراد الميليشيات) ، وتتسع دائرة المصطلح لتشمل

كل افراد الجيش في كافة صنوفه القتالية المختلفة .^(٥٢) وأشارت الفقرة الثانية الى الفئة الاخرى ((افراد الميليشيات الاخرى والوحدات المتطوعة الاخرى ، بمن فيهم اعضاء حركات المقاومة المنظمة ، الذين ينتمون الى احد اطراف النزاع)) نجد ان هذه الفقرة تتطلب شرط الانتماء على خلاف الفقرة السابقة ، في قضية تاديش امام محكمة يوغسلافيا السابقة بينت المحكمة ان عناصر الانتماء تتلخص بالسيطرة ، اي ممارسة الدولة للسيطرة على هذه المجموعات .^(٥٣)

المطلب الثاني

تطبيق مبدأ التمييز في الحرب الالكترونية

قانون الحرب يدعو أطراف النزاع للتأكد خلال النزاع المسلح ، بان الهجمات توجهه الى المقاتلين وليس المدنيين ، وإذا كان المدنيين هم المستهدفين فعلى تلك الأطراف ان تتأكد من ان المدنيين قد فقدوا الحماية المقررة لهم بموجب القانون الدولي الإنساني ، نتيجة مشاركتهم في العمليات العسكرية بصورة مباشرة ، والسؤال المطروح هنا ، هل تستطيع الهجمات الالكترونية ان تميز بين المقاتلين والمدنيين ؟

تعريف المقاتلين في القانون الدولي الإنساني ، يتطلب درجة من التنظيم والقيادة المسؤولة تلك المستلزمات توجد في الدول التي تملك جيوشها قدرات الحرب الالكترونية . القانون الدولي الانساني عرف المقاتلين بصورة مرتبكة فيما يتعلق بالفضاء الالكتروني ، حيث لم يعترف للأفراد الذين يشاركون بصورة طوعية في الهجمات الالكترونية ضد الخصم ، فعلى سبيل المثال ، القراصنة الهواة الذين يقومون بهجمات ضد دولة خصم لمبررات سياسية او ايدولوجية ، تلك الهجمات تبرر للدولة المستهدفة الرد بوسائل مناسبة ، في ضوء الحرب الالكترونية لا يعد هؤلاء ضمن فئة المقاتلين الشرعيين ، بل ضمن فئة المقاتلين غير الشرعيين او مدنيين غير محميين طالما يشاركون في العمليات العدائية . لذلك فان فان القراصنة المشاركين في تلك العمليات يعدون هدف مشروع للاستهداف .^(٥٤)

استخدام القوة من الدولة المستهدفة ضدهم يجب ان يقيد بمبدأ التناسب ، ويشبه هؤلاء بالهبة الجماعية التي يشترط على المدنيين المشاركين ان يحملوا السلاح علنيا ، لا ان مفهوم حمل السلاح علنيا في الهجمات الالكترونية غير معرف لحد الان ، حيث ان فعالية الاسلحة

الإلكترونية تتبع من قدرتها على السماح للمهاجم الإلكتروني ، اختراق أجهزة الحاسوب غير المؤمنة .^(٥٥)

المستشارة القانونية السابقة للجنة الدولية للصليب الأحمر الاستاذة Louise Doswald – Bec استنتجت ان القواعد الخاصة بتقسيم وامتيازات المقاتلين لا تختلف في حالة الحرب الإلكترونية ، وأشارت الى ان الاشخاص الذين يساهمون في العمليات الإلكترونية ، لا يستفيدون من نظام اسرى الحرب عند سقوطه بيد الخصم ، كما نصحت الدول بعدم اصدار تعليمات بزج هؤلاء في القوات المسلحة . بينما يعتبر السيد Michael Schmitt المدنيين المشاركين في الهجمات الإلكترونية التي تسبب اضرار مادية او جسدية بالمقاتلين غير الشرعيين ، ويتفق مع الاستاذة Doswald في ضرورة اتخاذ الدول منهج حكيم فيما يتعلق بقصر العمليات الإلكترونية على الاشخاص العسكريين .^(٥٦) البروفسورة Susan Brenner قدمت نهج اكثر انتقادا لموضوع مشاركة المدنيين في الهجمات الإلكترونية ، حيث دعت الى اعادة تقييم القواعد التي تحكم المشاركة في العمليات العدائية في ضوء حقائق الهجمات الإلكترونية، وتستنجد في غياب القواعد الخاصة بالمشاركة المباشرة فيما يتعلق بالهجمات الإلكترونية، الى ضرورة وجود اليات قانونية منظمة ، تقود الى تشكيل هيئة تهتم بالأمن الإلكتروني ، تأخذ على عاتقها فرض القانون.^(٥٧)

المشاركة المباشرة في العمليات العدائية ، تتمثل في النزاعات المسلحة التقليدية ، بقيام المدني بحمل السلاح في مواجهة الخصم ، وتلك الصورة تمثل الصورة الكلاسيكية للمشاركة المباشرة في العمليات العسكرية ، اما في الهجمات الإلكترونية فان المسألة اكثر ضبابية ، بالنسبة الى المدني الذي يتم تجنيده في مهمة تتعلق بالهجمات الإلكترونية دون ان يعلم بذلك ، كالأشخاص الذين ساهموا في افعال الانظمة لإلكترونية في جورجيا من خلال تحميل البرامج والضغط على الازرار، القواعد التي تحظر استهداف المدنيين الذين يقومون بأعمال لا تنطوي من حيث الطبيعة او غرض الى احداث ضرر حقيقي لقوات الخصم ، مثل هذه القواعد يجب ان تستمر وتطبق على المدنيين الذين يساهمون عن غير قصد في العمليات الإلكترونية .^(٥٨)

فالمشاركة تتحقق عندما تتحقق السببية بين فعل المدني المساهم والنتيجة المتحققة التي تظهر نتائج ملموسة على قوة الخصم ، فالمشاركة بعمل لا يؤدي الى تلك النتيجة ، لا يحقق معنى المشاركة المباشرة ، وهذا ينصرف الى الحرب الإلكترونية كما هو الحال في الحرب التقليدية ، فالمدني الذي يساهم في الهجمات الإلكترونية الموزعة ، يجب ان تكون المساهمة مؤثرة ، تؤدي بالسير العادي للأمر الى تحقيق النتيجة المتوقعة ، اما المساهمة بجزء بسيط لا يحقق النتيجة بمفرده ، لا نكون امام مشاركة مباشرة ، كسائق عربة يحمل سلاح في اطار المجهود الحربي ،

مثله الباحث في الجامعة او المتعاقد لتطوير برنامج اختراق حاسوبي ، لا يعد عمله وفق سلسلة الاحداث كافيا لان يفقد الحماية .^(٥٩)

هناك العديد من الصور التي تحقق بها المباشرة من عدمها ، عندما يتعاقد المدني مع القوات المسلحة او اي طرف في نزاع مسلح ، للقيام بأعداد شيفرات الكترونية او اي عمل ضمن الهجمات الإلكترونية، كما هو الحال في قيام الولايات المتحدة باستخدام المدنيين لقيادة الطائرات بدون طيار للقيام بعمليات لاستهداف اشخاص او مواقع ، او تشغيل متعاقدين عسكريين او امنيين في مناطق مثل العراق وافغانستان^(٦٠) ، الدليل الارشادي للمشاركة المباشرة في العمليات العدائية اشار في هذا الموضوع الى ((المتعاقدون من القطاع الخاص والموظفون المدنيون الذين لم يدمجوا في القوات المسلحة ، فلا تنزع عنهم صفة المدنيين بمجرد انهم يرافقون القوات المسلحة او يتولون وظائف غير القيام بعمليات عدائية كان يقومون بها في العادة موظفون عسكريون. وعندما يشارك هؤلاء الموظفون مشاركة مباشرة في العمليات العدائية بدون اذن صريح او ضمني من الدولة الطرف في النزاع ، يظلون اشخاصا مدنيين ويفقدون الحماية الممنوحة لهم من الهجمات المباشرة طوال المدة التي تدوم فيها المشاركة المباشرة . ويجب التوصل الى استنتاج مختلف بالنسبة الى المتعاقدين والموظفين الذين ادمجوا ، لجميع الاغراض والمقاصد ، في القوات المسلحة لطرف في النزاع ، سواء اكان ذلك عبر اجراءات رسمية وفقا للقانون الوطني او بحكم الواقع ، من خلال تسليمهم وظيفة قتالية يستمرون في ادائها لفترة معينة، فبموجب القانون الدولي الانساني ، يصبح هؤلاء الموظفون اعضاء في قوات او جماعات او وحدات مسلحة منظمة ، تحت قيادة مسؤولة تابعة لاحد اطراف النزاع ، ولا يعودون يصنفون بالمدنيين لأغراض مبدأ التمييز))^(٦١) . وعليه فان المدني الذي يقوم بأعمال صيانة لشبكة الحواسيب العسكرية لا يعد مشارك في العمليات العسكرية ، على خلاف المتعاقد الذين يقوم بعمل عدائي يساهم بسببية في الهجمات الإلكترونية يعد مشارك مباشر في العمليات العسكرية.^(٦٢) وهناك صورة اخرى تتمثل في قيام المدني بالمشاركة في هجمات الإلكترونية من جانب واحد ، الغرض منها التداخل مع اجهزة الحاسوب وجمع المعلومات ، كما حدث في الهجمات الإلكترونية ضد جورجيا في ٢٠٠٨ ، المدني الذي يساهم من تلقاء نفسه في هجمات الإلكترونية بدون توجيه من طرف النزاع ، يعد مساهم مباشر في العمليات العدائية، فأى عمل يقوم به مثل هذا الشخص بقصد استهداف الشبكات الإلكترونية ، تعد مشاركة مباشرة بنفس الاسلوب اذا حصل في اطار العمليات العسكرية التقليدية ، لتدمير او احداث اضرار بهدف عسكري.^(٦٣)

المدني الذي يقوم بأعداد برامج حاسوبية خبيثة ويقدمها الى القوات المسلحة او لطرف في نزاع دون ان يقوم بتنفيذ ذلك البرنامج ، تلك الصورة تحاكي ما يعرف بصانع القنابل ، الشخص الذي يقوم بأعداد الية مدمرة ، دون ان يساهم بعمل ابعده من تصنيعها ، ذلك العمل لا يشكل مشاركة مباشرة في العمليات العدائية ، فهي تعد من الاعمال التحضيرية التي لا ترقى الى المشاركة المباشرة في العمليات العدائية .^(٦٤)

مبدأ التمييز في القانون الدولي الانساني كما سبق الإشارة اليه يتطلب من المقاتلين تمييز انفسهم عن المدنيين ، وبالتالي فان القانون الدولي الانساني عند تصنيفه المقاتلين راعى هذا المبدأ من خلال اشتراطه وجود العلامات الدالة على فئة المقاتلين ، فاللباس العسكري اشارة الى القوات المسلحة النظامية ، واشتراط وجود العلامة البارزة المرئية من بعيد لتصنيف الجماعات المسلحة، واخيراً رفع السلاح علناً في الهبة الجماعية ، فالسؤال المطروح هل يعد المهاجم الإلكتروني مقاتل وفق الاشتراطات التي وضعها القانون الدولي الانساني في اتفاقية جنيف الثالثة والبروتوكول الاضافي الاول ؟

اذا كان القانون الدولي الانساني يتطلب اللباس العسكري والشارة المميزة ورفع السلاح علناً ، الاشخاص الذين يقومون بالهجمات الإلكترونية غالباً ما يكونون بعيداً عن الهدف وبالتالي لا يمكن تمييزهم ، كما ان القيادة المسؤولة غالباً ما تختفي قراراتها في الهجمات الإلكترونية ، لان المهاجم الإلكتروني يتأخذ قرارات انية تتوافق مع المستجدات التي تحصل اثناء القيام بهجمات الكترونية ، تلك المستجدات التي لم يتوقعها من قام بإصدار الامر ، كما ان المهاجم الإلكتروني غالباً ما يخضع لإجراءات داخلية وليس لنظام قضائي عسكري ، حيث يكون اقرب في الخضوع للقوانين الجنائية .

في ضوء الهجمات الإلكترونية ، القواعد المقبولة القابلة للتطبيق على المقاتلين في القانون الدولي الانساني ، لا تتسجم مع طبيعة هذه الهجمات ، فالاشتراطات التقليدية المطلوبة في نظام المقاتلين ، لا تمت بصلة لمتطلبات الهجمات الإلكترونية .^(٦٥) كما ان هؤلاء يتجنبون الضربات الانتقامية الموجهة من الدولة المستهدفة ، بسبب بعدهم عن هدف الهجوم .^(٦٦)

هناك صعوبة في تطبيق تعريف القانون الدولي الانساني للمقاتلين على المقاتلين الإلكترونيين، صعوبة كبيرة في ضم هذه الفئة الى الهبة الجماعية ، تكمن الصعوبة في اشتراط رفع السلاح علناً في الهجمات الإلكترونية ، كما ان المقاتلين ملزمين بموجب القانون الدولي الانساني بالتقيد بمبادئه طيلة فترة النزاع ، وعدم التقيد لا يقود فقط الى فقدانهم امتيازات المقاتلين

في حالة القبض عليهم ، بل يمكن ان يتصف عملهم بالغدر ، وهو فعل محظور في القانون الدولي الانساني .^(٦٧)

الحرب الالكترونية الاحتمالية فيها اكبر من الحرب التقليدية ، ان يتجاهل المقاتلين مبدا التمييز ، ويوجهون ضربات الى الاهداف المحمية بالقانون الدولي الانساني ، عند قصف قوات الناتو لإذاعة سربينتس خلال الحملة على كوسوفو ، اذا تم عرض المسألة بصورة مختلفة باستخدام الاسلحة الالكترونية ، في ذلك الوقت بررت قوات الناتو الهجوم على الاذاعة بانها تستخدم في نطاق الدعاية الحربية ، كما انها تستخدم لأغراض الاتصالات العسكرية ، اثار ذلك الهجوم انتقادات كبيرة ، تمثلت في ان الميزة المتحققة من الهجوم لا ترتقي الى الميزة العسكرية كما انها فاقت الخسائر في صفوف المدنيين ، لو فرضنا استخدام الناتو للأسلحة الالكترونية في تلك الحالة ، يدعم حجج الناتو كما انه يقلل من الخسائر العرضية ، وبذلك لا يتم مناقشة المكاسب المتحققة من الهجوم ومقارنتها بالخسائر العرضية.^(٦٨) تبقى الحرب الإلكترونية اكثر الحروب ينتهك فيها المهاجمون لمبدا التمييز حيث يذهب احد الخبراء الى القول (تلك الهجمات مع نتائجها الملموسة بصورة محدودة ، مثل التداخل مع الانظمة المالية والاجتماعية ، او الكشف عن معلومات شخصية ، تشكل اضرار ضد الاشخاص الذين يحميهم القانون الدولي الانساني) في ضوء ذلك الهجمات المباشرة تمس الاهداف المدنية بواسطة الاسلحة الالكترونية اكثر من استخدام الاسلحة التقليدية ، علاوة على ما تشكله من جرائم حرب .^(٦٩)

المسألة الاكثر تعقيدا في الحرب الالكترونية ، تلك المتعلقة بالتمييز بين الاهداف العسكرية والاعيان المدنية ، الاعيان المدنية يقصد بها كل المنشآت التي لا تعتبر منشآت عسكرية ، وقد عرفت المادة ٥٢ من البرتوكول الاضافي الاول للمنشآت العسكرية بانها ((..... وتتحصر الاهداف العسكرية فيما يتعلق بالأعيان على تلك التي تسهم مساهمة فعالة في العمل العسكري سواء بطبيعتها ام بموقعها ام بغايتها ام باستخدامها ، والتي يحقق تدميرها التام او الجزئي او الاستيلاء عليها او تعطيلها في الظروف السائدة حينذاك ميزة عسكرية اكيدة)) .

استهداف الاهداف العسكرية الصرفة ، لا يشكل انتهاك لمبدا التمييز ، وبمفهوم المخالفة ، اذا وجهت الهجمات الإلكترونية بصورة عمدية لاستهداف منشآت ، وينتج عن ذلك الاستهداف خسائر في الارواح في صفوف المدنيين والممتلكات المدنية ، مثل هذه الهجمات بدون شك غير شرعية وفق قانون الحرب ، الذي يلزم اطراف النزاع عند توجيه الهجمات ، التأكد من عدم حدوث خسائر عرضية تفوق الميزة العسكرية المتوقعة من الهجوم (المادة ٥٧ الفقرة ثالثا) من البرتوكول الاضافي الاول .

الهجمات الإلكترونية التي تستهدف المدنيين تكون أكثر ازعاجاً لأنها تهدد الحياة والطمأنينة ، فعلى سبيل المثال ، في عام ٢٠٠٨ ، اثناء التوتر بين جورجيا وروسيا بسبب الانفصاليين في ابخازيا وجنوب استونيا ، ذلك التوتر قاد الى نزاع مسلح بين الطرفين في اب ٢٠٠٨ . قامت روسيا اثناء النزاع بتوجيه هجمات الكترونية ، استهدفت اجهزة الخدمة الالكترونية ، لشبكات السي ان ان والبي بي سي العاملة في جورجيا ، مما منع الوصول الى الاخبار الدولية ، مثل هذا الهجوم جعل المدنيين في حالة من التشويش ، مع ذلك ، الهجمات الإلكترونية كانت لتحقيق غرض معين هو احداث نوع من الازعاج المؤقت ، الا ان اثار الهجمات امتدت لتهدد المدنيين علاوة على تدمير ممتلكات مدنية ، تلك الهجمات تعتبر غير قانونية .^(٧٠)

المسألة الأخرى القابلة للنقاش ومرتبطة باستهداف المنشآت العسكرية ، وحظر استهداف الأعيان المدنية ، تلك المتعلقة بالأهداف مزدوجة الاستخدام ، قواعد القانون الدولي الانساني وضعت لتحد من العمليات العسكرية ، وتوجيهها نحو هدف واحد ، هو تحقيق الميزة العسكرية اي اضعاف قدرة العدو على المواصلة في القتال . فالصعوبة تكمن في العمليات الالكترونية التي تستهدف انظمة ، كما هو الحال باستهداف منشأة تخصيب اليورانيوم الايرانية ، او تستهدف انظمة مزدوجة الاستخدام ، تخدم المدنيين والعسكريين على حد سواء .^(٧١)

الهجمات الإلكترونية ضد الاهداف المزدوجة الاستخدام ، تؤدي الى خسائر عرضية كبيرة بالمقارنة مع الميزة العسكرية المتحققة ، يرسم الاستاذ Richard Clark صورة قاتمة حول هذه المسألة (عندما تقوم دولة بتوجيه هجمات الكترونية واسعة الانتشار الى البنى التحتية الحساسة ، مثل شبكات الكهرباء ، انظمة السيطرة على الملاحة الجوية ، مراكز المعلومات المصرفية) ، مع ذلك فاذا حصل التداخل بين الانظمة ذات الاستخدام المدني والعسكري ، مثل تداخل الاتصالات العسكرية الجوية مع انظمة السيطرة الملاحية الجوية ، او اعتماد القوات العسكرية على شبكات الكهرباء ، تلك تعتبر اهداف مشروعة للاستهداف .^(٧٢) الوسيلة الوحيدة لحماية غير المقاتلين من الهجمات الموجهة ضد الشبكات مزدوجة الاستخدام ، هي عزل الاستخدامات العسكرية من الانظمة والشبكات المدنية .

مدى مشروعية القرار بتوجيه الهجمات الإلكترونية ضد الاهداف المزدوجة الاستخدام ، يعتمد على القصد من وراء الهجمات ، الهجمات الإلكترونية تكون مشروعة اذا استهدفت منشأة مزدوجة الاستخدام لتحقيق ميزة عسكرية ، وبالعكس يكون غير مشروع اذا كان الهدف من وراء الهجوم تقويض الدعم السياسي لطرف النزاع ، وليس لتحقيق الميزة العسكرية .^(٧٣)

السؤال الذي يطرح نفسه ، هل تستطيع الهجمات الالكترونية ان تتجنب الهجمات العشوائية ؟ . القانون الدولي الانساني يحظر الهجمات العشوائية ، وذلك استنادا الى المادة ٥١ الفقرة ١ من البروتوكول الاضافي الاول التي تنص على ((.....٤- تحظر الهجمات العشوائية ، وتعتبر هجمات عشوائية : ا- تلك التي لا توجه الى هدف عسكري محدد ب- او تلك التي تستخدم طريقة او وسيلة للقتال لا يمكن ان توجه الى هدف عسكري محدد ج- او تلك التي تستخدم طريقة او وسيلة للقتال لا يمكن حصر اثارها على النحو الذي يتطلبه هذا البروتوكول ، ومن ثم فان من شأنها ان تصيب ، في كل حالة كهذه ، الاهداف العسكرية والاشخاص المدنيين او الاعيان المدنية دون تمييز)) . في ضوء متطلبات المادة ٥١ ، هل تستوفي الهجمات الالكترونية تلك المتطلبات ؟ فلو فرضنا ، ان تقوم الدولة بتوجيه هجمات الكترونية من خلال ادخال الفيروسات الى انظمة الحواسيب للدولة المستهدفة ، فاذا استطاعت ان تحدد النظام الالكتروني العسكري ، فان هذا الهجوم لا يعد عشوائيا ، ولكن اذا تسرب هذا الفيروس فأصاب اجهزة حواسيب مدنية ، نتيجة للتداخل بين الشبكات ، مما قد يصيب حواسيب تتعلق بالنظام الصحي او حركة الملاحة الجوية ، فان مثل هذا الهجوم يعد عشوائيا ، وعليه فان من الصعوبة بمكان ان تكون الهجمات الالكترونية غير عشوائية ، وذلك لطبيعة الانظمة الالكترونية المتداخلة مع بعضها .^(٧٤)

القانون الدولي الانساني يفرض التزامات على الطرف المهاجم والطرف المدافع ، تلك الالتزامات وردت في المادة ٥٧ والمادة ٥٨ من البروتوكول الاضافي الاول . السؤال المطروح الى اي مدى يمكن للحرب الالكترونية ان تستوفي متطلبات المادة ٥٧ والمادة ٥٨ ؟

نصت المادة ٥٧ (الاحتياطات اثناء الهجوم) على العديد من التدابير التي يجب ان يتقيد بها من يقوم بالتخطيط لهجوم او يتخذ قرار بشأنه . فالمهاجم الالكتروني عليه ان يوجه هجماته للعناصر الالكترونية للأهداف العسكرية ، بما ينسجم مع متطلبات مبدأ التناسب ، الا انه من الناحية العملية هناك صعوبة في التنبؤ بالخسائر العرضية ، في حالة اللجوء الى الهجمات الالكترونية ، عن الهجمات التقليدية

اما فيما يتعلق بالمادة ٥٨ (الاحتياطات ضد اثار الهجوم) ، عند تطبيق المادة ٥٨ على الحرب الإلكترونية ، من المهم ان نلاحظ ان الوفود المشاركة في المؤتمر الدبلوماسي ، بينوا ان مصطلح (قدر المستطاع) الذي ورد في بداية المادة ، يلزم الاطراف بتوفير الحماية وفق قدرات الطرف في النزاع المسلح وليسما يفوق قدراته ، يذهب احد المختصين في مجال الحرب الإلكترونية ، الى القول انه من الصعب تأمين الحماية للشبكات الالكترونية على مدار الوقت ،

ونتيجة لذلك يذهب اتجاه اخر الى ان الحماية توفر للمنشآت الاكثر حيوية لتنفيذ متطلبات المادة ٥٨. (٧٥)

المضمون الثاني في المادة ٥٨ يتعلق باتخاذ الاحتياطات ما تحت سيطرتها من سكان مدنيين وممتلكات مدنية ، لو اخذنا مثال لا يتعلق بالحرب الالكترونية لتفسير ذلك الالتزام ، اذا المدنيين او الممتلكات المدنية تقع تحت سيطرة ميناء عسكري، ينشا التزام على قادة ذلك الميناء باتخاذ الاجراءات التي تحمي المدنيين والممتلكات المدنية من نتائج العمليات العسكرية ، بضمنها الهجمات من طرف العدو ، بالتشابه اي جهاز حاسوب ، شبكة انترنت ، انظمة الكترونية ، اجهزة ارسال ، اجهزة اتصال في الفنادق ، تحت سيطرة الحكومة يستتبعه تنفيذ ذلك الالتزام ، ويكون تنفيذ الالتزام خلال الهجمات الالكترونية من قبل العدو ، بقيام الحكومة باتخاذ اجراءات تراها ضرورية ، للسيطرة على شبكة الحواسيب ، لضمان استمرار اعمال الحكومة ، تلك الشبكة تبقى مدنية مع بقاء الاتصالات العسكرية هدف مشروع للاستهداف .

الخاتمة

بعد ان جف حبر القلم ، وانتهت صفحات بحثنا ، قد وصلنا الى جادة الخاتمة ، فنعرض لما توصلنا إليه ، بعد رحلة في وريقات المصادر ، علنا نخرج بنتيجة تفيد القارئ ومن يبحث بعدنا .

شكلت الحرب الالكترونية تحديا خطيرا للسلم والأمن الدوليين ، وازدادت الهجمات الالكترونية كما ونوعا لتهدد المفاصل الحيوية المدنية وغيرها من شبكات المعلومات التي تؤدي خدمة الى المجتمع . وهذا الاندفاع من قبل الدول نحو استخدام الحرب الالكترونية ، يرجع بالدرجة الأولى الى القيمة الرخيصة في توجيه الهجمات حيث ان هذه الهجمات غالبا ما تنتج عن فيروسات او برامج خبيثة الكترونية ، يمكن تصنيعها بقيمة رخيصة ، علاوة على الاحتجاج من قبل الدول التي تملك مثل هذه القدرات ، بان استخدام الأسلحة الالكترونية فيه ضمانة لعدم انتهاك القانون الدولي الإنساني .

وبعد المقدمة أعلاه نصل الى استنتاجاتنا في موضوع الحرب الالكترونية.

اولا - الحرب الالكترونية تتطوي على أعمال عنف ، وتندرج هذه الأعمال في تعريف القانون الدولي الإنساني للهجمات بأنها أعمال هجومية ودفاعية ، والغاية من توجيه هذه الهجمات في الحرب التقليدية تحقيق الميزة العسكرية ، وهذا ما يحصل في حالة قيام دولة بتوجيه فيروس الى أجهزة المراقبة الجوية ، فان ذلك سيؤدي الى تعطيل ذلك النظام ، مما يسمح بتوجيه ضربات محددة الى الأهداف التي بضرها تتحقق الميزة العسكرية ، ويبقى تحديد وجود او عدم وجود النزاع المسلح ، حتى يمكن تطبيق القانون الدولي الإنساني في الحرب الالكترونية مسألة قابلة للنقاش خارج حدود القانون الدولي الإنساني التقليدية . النزاع المسلح لتحديد وجوده يجب ان لا نكتفي بتحديد بالاعتماد على المعايير الموضوعية فقط ، لان من شان ذلك خروج الكثير من النزاعات المسلحة من دائرة القانون الدولي الإنساني ، ومنها الحرب الالكترونية التي لا نجد فيها انتشار لقوات مسلحة او تبادل لإطلاق النار عبر الحدود ، والتي تعد معايير موضوعية لوجود النزاع ، بل يتم الاعتماد على طبيعة الأهداف المتوخاه من الهجمات وكثافة الهجمات وما تخلفه من نتائج ، اي بالاعتماد على نية المهاجم من وراء توجيه الضربة الالكترونية ، سواء كانت الخسائر مادية او بدنية فكلا الأثرين نتيجة لأعمال العنف التي يعتبرها القانون الدولي الإنساني قاعدة للهجوم ، فكلا غياب القواعد في القانون الدولي الإنساني المنطبقة على الحرب

الالكترونية ، لا يجرّد هذه الحرب من القيود القانونية فيمكن ان تخضع لشرط مارتنز ولقواعد حقوق الإنسان ، وغياب هذه القواعد يمكن ان يكون حافزا للدول على أعداد اتفاقية خاصة بتنظيم وتقييد الحرب الالكترونية .

ثانيا - الحرب الالكترونية وسيلة من وسائل القتال ، بدأت الدول التي تلجا إليها في النزاعات الحديثة ، وبالتالي تخضع للمادة ٣٦ من البرتوكول الإضافي الأول ، وعليه فان الدول ملزمة بمراجعة قانونية لمثل هذه الوسائل ، ومدى مطابقتها لمعايير القانون الدولي الإنساني ، ولا يجوز الدفع بان الوسائل المستخدمة في الحرب الالكترونية غير خاضعة لتلك المعايير ، بحجة غياب القواعد المنظمة للحرب الالكترونية ، فذلك الغياب لا يبرر عدم مراجعة تلك الوسائل .

ثالثا- الأشخاص الذين يساهمون في الحرب الالكترونية ، يعدون مدنيين فاقدى للحماية طيلة مشاركتهم في تلك الهجمات ، بشرط استيفاءهم لمتطلبات المشاركة المباشرة ، ولا يجوز للدول ضمهم الى القوات المسلحة .

رابعا - تبقى الهجمات الالكترونية مقيدة بعدم توجيهها الا الى الأهداف العسكرية ، وحظر توجيهها الى الأهداف المدنية ، وحظر توجيه الهجمات الى المنشآت ذات الاستخدام المزدوج ، الا في حالة تحقيق ميزة عسكرية ، كما ان الحرب الالكترونية مقيدة بعدم توجيهها عشوائيا .

خامسا - يجب على الدولة المهاجمة والمدافعة في الحرب الالكترونية ، اتخاذ الاحتياطات اللازمة التي وردت في المادة ٥٧ والمادة ٥٨ من البرتوكول الإضافي الأول ، فعلى المهاجم اتخاذ جميع الاحتياطات الممكنة عند اختياره لوسائل وأساليب الهجوم من اجل تفادي الخسائر والإضرار المدنية العرضية والحد منها في جميع الأحوال . وقد تكون الخسائر والإضرار المدنية العرضية الناجمة عن العمليات الالكترونية في بعض الحالات اقل من الخسائر في الحرب التقليدية .

سادسا - تبقى الحرب الالكترونية مفتوحة لكثير من المناقشات القانونية ، فالدول التي تستخدم مثل هذه الوسائل تدافع عن استخدامها بأنها تستجيب لمتطلبات القانون الدولي الإنساني ، وبصفة خاصة مبدأ التمييز ، وتدفع الدول المتضررة بان تلك الأسلحة لا تراعي مبدأ التمييز . رأينا ان الحرب الالكترونية ، بوسائلها المتعددة لا تستوفي مبدأ التمييز بل تتطوي الهجمات الالكترونية في اغلب الأحيان على الهجمات العشوائية ، وتبقى الدول التي لا تملك القدرات

الالكترونية في وضع سيئ ، كما ان المهاجم الالكتروني شخص لا يمكن الوصول إليه في اغلب الأحيان ، مما يجعله مهاجم يلجا الى الغدر كوسيلة قتالية ، وهو محظور في القانون الدولي الإنساني . الحرب الالكترونية نتائجها اكبر من نتائج الحرب التقليدية ، مما يتطلب قواعد عالمية تحظر او تقييد اللجوء إلى الحرب الالكترونية.

المصادر

باللغة العربية .

- الكتب

- ١- جون -ماريهنكرتس ولويز دوزوالد- بك ، القانون الدولي الإنساني العرفي - المجلد الأول : القواعد ، اللجنة الدولية للصليب الاحمر ، القاهرة ، ٢٠٠٧ .
- ٢- د . صلاح الدين عامر ، التفرقة بين المقاتلين وغير المقاتلين ، دراسات في القانون الدولي الإنساني ، دار المستقبل العربي ، القاهرة ، ٢٠٠٠ .
- ٣- د . عبد الغني عبد الحميد محمود ، حماية ضحايا النزاعات المسلحة في القانون الدولي الإنساني والشريعة الإسلامية ، بعثة اللجنة الدولية للصليب الأحمر - القاهرة ، الطبعة الرابعة ٢٠٠٩ .

- البحوث

- ١- جستين ماك كلياند ، استعراض الاسلحة وفقا للمادة ٣٦ من البرتوكول الاضافي الاول ، المجلة الدولية للصليب الاحمر ، العدد ٨٥٠ ، ٢٠٠٣ .
- ٢- مايكل ن . شميث ، الحرب بواسطة شبكات الاتصال الهجوم على شبكات الكمبيوتر (الحاسوب) والقانون في الحرب ، المجلة الدولية للصليب الاحمر ، مختارات من اعداد ٢٠٠٢ .

- الوثائق

- دليل تفسيري لمفهوم المشاركة المباشرة في العمليات العدائية وفق القانون الدولي الانساني ، اللجنة الدولية للصليب الاحمر ، القاهرة ، ٢٠١٠ .
- الاسلحة الحديثة ، منشور قسم الخدمات الاستشارية للقانون الدولي الانساني ، اللجنة الدولية للصليب الاحمر .

BOOKS

1- Jean Pictet ,commentary on rhe Additional Protocols of 8 ١٦
June 1977 to the Geneva Conventions of 12 August 1949
,international committee of the Red Coss ,Geneva 1987.

2- Jean Pictet , commentary : Geneva convention III Relative to
the treatment of prisoners of war , international committee of the
red cross ,1960.

3- Jean-Marie Henckaerts and Louis Doswald – Beck ٤٥
,customary international humanitarian law – practices ,
,٢٠٠٥international committee of red cross, Cambridge,

DOCUMENTS

AGuide to the Legal of New Weapons , Means and Methods of ١٥
Warfare ;Measures to Implement Article 36 of Additional Protocol
of 1977,international committee of the red cross Geneva,January
2006.reportes and documents ,international review of the red
cross ,volume 88number 864 December 2008

REASRCHS

1 Isabelle Daoust ,Robeincoupland and Rikkelshoey ,new wars, new ٢٤
weapons ? the obligation of states to assess the legality of means and
methods of warfare , review of international red cross ,Vol.
.84,N.846,June ,2002.

- 2 Kathleen Lawand, Reviewing , the legality of new weapons , mans 20 and methods of warfare , international review of the red cross , volume .88 number 864 December 2006.
- 3 Daphne Richmond – Barak , Nonstate Actors in Armed Conflicts : issues of Distinction and Reciprocity .
- 4 Dieter Fleck , technological challenges in armed conflicts and areas of regulation.
- 5 Emily Crawford , virtual battlegrounds : direct participation in cyber warfare , Sydney law school, legal studies research paper , NO.12/10, February 2012.
- 6 Eric Talbot Jensen , cyber warfare and precautions against the effects .of attacks, Texas Law Review , VOL.88:1533, 2010.
- 7 James Fallows Tierney , threshold constraints and laws of wars , .university of Chicago, lawschool, 2011.
- 8 Jeffrey T.G.Kelsey , Hacking into international humanitarian law the principles of distinction and neutrality in the age of cyber warfare , Michigan law review, VOL.106:1427, 2008.
- 9 Johann – Christoph Woltag , Computer Network Operations Below the Level of Armed Force , European Society of international law , conference paper series , conference paper NO.1/2011, 2011.
- 10 John Richardson , Stuxnet as cyberwarfare : Applying the law of war to the Virtual Battlefield , JMR Portfolio Intelligence, 2011.
- 11 Katherine Del Mar , the requirement of belonging under international humanitarian law , the European journal of international law , VOL.21 NO.1, 2010.

12 Knut Dormann, applicability of the additional protocols to computer network attacks,2004.

13 Konstantin Meljnik and Stefan Weiss, conference report – 30 years additional protocols to the 1949 :past , present and future , German Law . Journal ,VOL.09 NO.10 ,2008.

14 LTC Bryan W.Ellis , the international legal implication and limitations of information warfare : what are our options ? , usawc strategy research project ,u.s. army war college.

15 Marco Alberto Velasquez – Ruiz , the principles of distinction and proportionality under the framework of international criminal responsibility .–content and issues–,int.law.Rev.colomb,n14,2009,

16 Marco Roscini , world wide warfare – jus ad bellum and the use of cyber force,Maxplanck yearbook of united nations law,vol.14,2010.

17 Marco Roscini , World Wide Warfare – Jus ad bellum and the use of cyber Force , Max Planck Yearbook of United Nations Law , .VOL.14,2010.

18 Max Blumenthal , international humanitarian law for cyber–warfare ,School of international Service the American university ,2011..

19 Michael Gerais,cyber attacks and the law of war , yale university – law school ,October 1,2011.

20 Michael N.Schmit , Attack and jus in bello, irrc june, Vol.84 wired warfare computernetwork,N.846,2002.

21 Nikhil D`Souze , cyber warfare and state responsibility : development in international law , university of Mysore ,2011.

22 Noelle Quenivet , the war on terror and the principle of distinction ٥٠
،٢٠١٠ in international humanitarian law,ACDI,Bogota ,

23 PapanastasionAfroditi , Application of international law in cyber
Warfare Operations, university of Leicester – faculty of law ,2010.

24 Sean Watts , combatant status and computer network attack
.,Virginia journal of international law,VOL.50:2,2010.

25 Susan W.Brenner and Leo L.Clarke , conscription and cyber conflict
legal issues,international conference on cyber conflict
,Tallinn,Estonia,2011..

26 Trevor A. Keck,The Principle of Distinction, the Question of Direct
Participation in Hostilities and Evolving Restraints on the Use of Force in
Warfare ,From the Selected Works of Trevor Keck,2011.

الهوامش

**1 PapanastasionAfroditi , Application of international law in cyber
Warfare Operations, university of Leicester – faculty of law
,2010,p7**

**2 Max Blumenthal , international humanitarian law for cyber–
warfare ,School of international Service the American university
,2011,p2.**

٣- قال مسؤولون حكوميون، وأجانب في استونيا إن مواقع حكومية ومواقع خاصة بمصارف وشركات اتصالات ومؤسسات اخبارية في استونيا، ظلت تتعرض على مدى الأسابيع الأخيرة لهجمات سايبيرية هائلة ومنظمة. ويصف خبراء في أمن شبكات الكمبيوتر في استونيا هذه الهجمات بأنها هائلة وغير مسبوقه تستهدف البنية التحتية الالكترونية للدولة على المستويين العام والخاص. ويقول هؤلاء الخبراء ان روسيا هي مصدر هذه المشكلة بسبب تغييرها موقع

نصب تذكاري حربي من الحقبة السوفياتية. إلا ان مسؤولين روسا نفوا ان تكون للحكومة الروسية أية صلة بهذه الهجمات. حلف شمال الاطلسي (الناتو) والاتحاد الأوروبي، سارعا من جانبها بإرسال خبراء في تكنولوجيا المعلومات الى استونيا للمراقبة وتقديم المساعدات اللازمة، خلال الهجمات التي تسببت في تعطيل شبكات البريد الالكتروني الحكومية، وأدت الى وقف المؤسسات المالية التعاملات المصرفية التي تجرى عادة عبر شبكة الانترنت. ويخشى خبراء من ان يلجأ الأعداء خلال الحروب الى إصابة هذه الشبكات بالشلل في ظل اعتماد المجتمعات بصورة متزايدة على شبكات الكمبيوتر العابرة للحدود. وكانت وزارة الأمن الداخلي الاميركية، قد نبهت الى ضرورة حماية شبكات الكمبيوتر الأميركية ضد هجمات الهاكرز التابعين لتنظيم «القاعدة». ويرى محللون ان تجربة استونيا تعتبر فرصة نادرة للوقوف على طبيعة ومدى هذه الهجمات. من جانبه قال جاك أفيكسو، وزير دفاع استونيا، ان الهجمات التي تعرضت لها مواقع وشبكات الانترنت الحكومية والخاصة ببعض المؤسسات كانت هائلة ومنظمة وموجهة بعناية. وأضاف قائلاً، انه لا يمكن النظر اليها فقط في سياق كونها «رد فعل تلقائي للاستياء العام تجاه سلطات استونيا، فيما يتعلق بإزالة النصب التذكاري الحربي السوفياتي، مؤكدا على ضرورة مناقشتها ايضا في سياق كونها هجمات منظمة تستهدف بنيات تحتية حديثة. لم تتهم حكومة استونيا الحكومة الروسية بصورة مباشرة وصريحة بتنظيم هذه الهجمات .

4-Johann – ChrstophWoltag ,Computer Network Operations Below the Level of Armed Force ,European Society of international law , conference paper series , conference paper NO.1/2011,2011,P3-5.

٥-حادث جورجيا يعد الاول من نوعه يحدث خلال عمليات عسكرية ، حيث حدث اثناء النزاع الروسي الجورجي عام ٢٠٠٨ ، العمليات المستخدمة كانت تضم تشويه شبكات الانترنت الذي استخدم في الهجمات على استونيا ، وينتج عن تشويه شبكات DDoS وكذلك استخدام الانترنت تغير في المحتويات ،لمحتوى والمظهر المرئي منه، في هذه الحالة شملت تغيير العديد من المواقع الحكومية الرسمية لعرض الصور من الحكام المستبدين في القرن ٢٠ واصطفت بجانب صورة الرئيس الجورجي ساكاشفيلي، مع آثار واضحة. في العديد من المواقع متوفرة للتحميل DDoS المتاحة للجمهور، وكانت البرامج والتعليمات اللازمة لتنفيذ هجمات ' ، صراحة على www.stopgeorgia.ru إلى أي شخص. تم إنشاء هذه المواقع، مثل ' السماح لعدد كبير من الناس لتنفيذ هجمات على مواقع الحكومة الجورجية. كما تم توفير كافة البرامج والتعليمات والأهداف، وأصبحت الهجمات متاح لأي شخص القيام بها.

وكان من أجل إتاحة المواقع الجورجية الرسمية، ونقل المحتويات إلى خوادم تقع خارج جورجيا، بما في ذلك الولايات المتحدة الأمريكية وبولندا واستونيا. نقلت الحكومة الجورجية استضافة للموقع من رئيس جورجيا والتابعة لوزارة الدفاع إلى ملقحات على أراضي الولايات المتحدة. ساعد خبراء الكمبيوتر من استونيا الذين كانوا قادرين على الاستفادة من خبراتهم التي أدلى بها في حادث ٢٠٠٧.

ibid.p6.

اول اكتشاف لهذا الفيروس كان في عام ٢٠١٠ من قبل شركة امنية Stuxnet ٦- متخصصة بالبرمجيات في بلا روسيا ، في ٢٥ ايلول اكتشفت ايران ان ما يقارب ٣٠ الف نظام معلومات اصيب بهذا الفيروس ، وبين السيد محمود لالي المسؤول عن مجلس نظم المعلومات التابع الى وزارة الصناعة والتعدين الايراني ، ان هذا الفيروس مصمم لنقل المعلومات من المعامل الصناعية الى اماكن خارج ايران ، ادى اختراق الفيروس الى تعطيل المشاريع السرية لإيران ، واستنادا الى احدى المؤسسات المعنية بتصنيع برامج الحماية الالكترونية ان الفيروس ابتداء ضرب داخل ايران ولكن في ذات الوقت وجد في الهند وإندونيسيا وعدد من الدول ، وتبين عدم تأثيره الكبير في هذه الدول نتيجة للعمل الذي نتج عنه في ايران ، وبين احصائية وضعها المركز الدول التي تأثرت من هذا الفيروس في اب ٢٠١٠ ب ٦٢،٨٦٧ الف جهاز حاسوب في ايران ، ١٣،٣٣٦ الف في إندونيسيا ، ٦،٥٥٢ الف في الهند ، ٢،٩١٣ الف في الولايات المتحدة الامريكية .

7-John Richardson , Stuxnet as cyberwarfare : Applying the law of war to the Virtual Battlefield ,JMR Portfolio Intelligence,2011,p9.

Available at www.assrn.com/abstract=1892888.

٨- الهجمات على شبكات الحاسوب ، سواء التي قد تصل الى مستوى حرب المعلومات او التي تكون مجرد عمليات معلوماتية عبارة عن عمليات لا يقاع الفوضى في المعلومات الموجودة في اجهزة الحاسوب او شبكات الحاسوب او الاجهزة او الشبكات نفسها او نفيها او الانتقاص من شأنها او تدميرها وجوهر الهجمات على شبكات الحاسوب بغض النظر عن الاطار الذي تجري فيه ، انها تعتمد على تيار من البيانات لتنفيذ الهجوم .وهكذا فان الوسائل المستخدمة تفصل الهجوم على شبكات الحاسوب عن جميع اشكال العمليات المعلوماتية الاخرى ، وتختلف هذه الوسائل اختلافا كبيرا ، وتشمل عدة اشكال من بينها الحصول على امكانية الدخول الى احد انظمة الحاسوب واكتساب القدرة على التحكم فيه ،ونقل فيروسات لتدميره ، او تغيير البيانات ، واستخدام قنابل منطقية تظل كامنة في النظام حتى تنطلق عند

حدوث شيء معين او في وقت محدد ،وتشمل الوسائل ادخال ديدان تتكاثر لدى دخولها الى احد الانظمة وبذلك تعمل على افراط تحميل الشبكة .

٩-مايكل ن . شميث ، الحرب بواسطة شبكات الاتصال الهجوم على شبكات الكمبيوتر (الحاسوب) والقانون في الحرب ، المجلة الدولية للصليب الاحمر ، مختارات من اعداد ٢٠٠٢ ،
Nikhil D`Souze , cyber warfare and state responsibility : development in international law , university of Mysore ,2011.p2.

7Susan W.Brenner and Leo L.Clarke , conscription and cyber conflict legal issues,international conference on cyber conflict ,Tallinn,Estonia,2011,p1.

١٠-القانون الدولي الانساني وتحديات النزاعات المسلحة المعاصرة ، التقرير الحادي والثلاثين ، ٢٠١١ ،
لاتفاقية هي أول معاهدة دولية بشأن الجرائم التي ترتكب عبر شبكة الانترنت وشبكات الكمبيوتر الأخرى، والتعامل بشكل خاص مع التعدي على حق المؤلف ، ذات الصلة بالحاسوب الاحتيال، و المواد الإباحية ، جرائم الكراهية [٦] وانتهاكات أمن الشبكة . كما أنه يحتوي على سلسلة من الصلاحيات والإجراءات مثل بحثا عن شبكات الكمبيوتر و الاعتراض المشروع هدفها الرئيسي، المنصوص عليها في الديباجة، هو السعي الى سياسة مشتركة الجنائية التي تهدف إلى حماية المجتمع من الجريمة الإلكترونية، وخصوصا من خلال اعتماد التشريعات المناسبة وتعزيز التعاون الدولي. الاتفاقية تهدف أساسا إلى: المواءمة بين العناصر المحلية الجنائية القانون الموضوعي من الجرائم والأحكام المتصلة في مجال الجرائم الإلكترونية التي تنص على القوى المحلية الجنائية قانون الإجراءات اللازمة للتحقيق والملاحقة القضائية لهذه الجرائم، فضلا عن غيرها من الجرائم المرتكبة عن طريق نظام الكمبيوتر أو أدلة فيما يتعلق الذي هو في شكل الكتروني ،إنشاء نظام سريع وفعال للتعاون الدولي.

وتعرف الجرائم التالية بموجب الاتفاقية: وصول غير قانوني، اعتراض غير قانوني، تدخل البيانات، وتدخل النظام، وإساءة استخدام أجهزة والتزوير المتعلقة بالكمبيوتر والاحتيال المتعلقة بالكمبيوتر، والجرائم المتصلة المواد الإباحية والجرائم ذات الصلة بحقوق المؤلف والمجاورة. كما يحدد هذا القانون القضايا الإجرائية مثل الحفاظ على التعجيل من البيانات المخزنة، والحفاظ المعجل والكشف الجزئي للبيانات حركة المرور، ونظام الانتاج والبحث

والمصادرة من بيانات الكمبيوتر، في الوقت الحقيقي جمع بيانات حركة المرور، واعتراض بيانات المحتوى. وبالإضافة إلى ذلك، فإن الاتفاقية تتضمن حكماً على نوع معين من الوصول إلى البيانات عبر الحدود الكمبيوتر المخزنة والتي لا تتطلب المساعدة المتبادلة (مع موافقة أو حيثما كان ذلك متاحاً للجمهور)، وينص على إقامة شبكة ٧/٢٤ لضمان توفير المساعدة السريعة بين الأطراف الموقعة.

Michael Gerais, cyber attacks and the law of war , yale university – law school ,October 1,2011,p7.

11– Jeffrey T.G.Kelsey , Hacking into international humanitarian law the principles of distinction and neutrality in the age of cyber warfare ,Michigan law review,VOL.106P1434–1435

12–LTC Bryan W.Ellis , the international legal implication and limitations of information warfare : what are our options ? , usawc strategy research project ,u.s. army war college ,p3–4.

١٣ – كتيب تطبيق القانون الدولي على الحرب الجوية والصاروخية الذي تم تبنيه من مركز أبحاث النزاعات في جامعة هارفرد في عام ٢٠٠٩ أشار إلى أن الهجوم يمكن أن يستهدف أجهزة الحاسوب الشخصية ، كما أن عمليات الانتهاك تتركز في جانب الدفاع والهجوم .

Marco Roscint , World Wide Warfare – *Jus ad bellum* and the use of cyber Force , Max Planck Yearbook of United Nations Law , VOL.14,2010,p95.

Attack and *jus in bello*, irrcline, Vol.84 ,N.846,2002p,368.Michael

N.Schmit , wired warfare computernetwork

NO LEGAL VACUUM IN CYBER SPACE , 2011, WWW.ICRC.ORG ,P2.

Dieter Fleck , technological challenges in armed conflicts and areas of regulation ,p5

Konstantin Meljnik and Stefan Weiss, conference report – 30 years additional protocols to the 1949 :past , present and future , German Law Journal ,VOL.09 NO.10 ,2008.p1363 .

**Marco Roscini , world wide warfare – jus ad bellum and the use of
cyber force,Maxplanck yearbook of united nations
law,vol.14,2010p114**

منظمة الامم المتحدة للاتصالات والمعلومات ، بذلت جهود على الصعيد الدولي لتنظيم الفضاء الإلكتروني ، وبدا سكرتير المنظمة الدكتور حمدون تورا جهود لتفعيل دور المنظمة ، لتلعب دورا محوريا في عقد اتفاقية سلام خاصة بالحرب الالكترونية ، ذلك كان السبب لتقديم المعاهدة الالكترونية ، المعاهدة التي اعلنت ان الحرب الالكترونية ليست قانونية ، الاتحاد الاوربي نجح في عقد اتفاقية الجرائم الالكترونية التي تعد نموذج لاتفاقية دولية للحرب الالكترونية ، اتفاقية الجرائم الالكترونية تطبق في اوربا ودول مثل الولايات المتحدة الامريكية واليابان ، اعترفت الاتفاقية بانها لا تسعى الى منع صناعة الاسلحة الالكترونية ، ولكنها تفرض قيود على الاستخدام فاذا كان الاستخدام لاغراض عدائية ، فان المستخدم يتعرض للمساءلة القانونية .

Max Blumenthal , op.cit,p1875 .

اتفاقية لاهاي لعام ١٩٠٧ واتفاقية حظر استحداث وانتاج وتخزين البكتريولوجية والتكسينية وتدمير تلك الاسلحة ١٩٧٢ واتفاقية حظر استخدام تقنيات التغيير في البيئة لاغراض عسكرية او لاية اغراض عدائية اخرى ١٩٧٦ واتفاقية حظر او تقييد استعمال اسلحة تقليدية معينة يمكن اعتبارها مفرطة الضرر او عشوائية الاثر والبروتكول الخامس الملحق باتفاقية حظر او تقييد استعمال اسلحة تقليديه معينة يمكن اعتبارها مفرطة الضرر او عشوائية الاثر . ٢٠٠٣

21AGuide to the Legal of New Weapons , Means and Methods of Warfare ;Measures to Implement Article 36 of Additional Protocol of 1977,international committee of the red cross Geneva,January 2006.reportes and documents ,international review of the red cross ,volume 88number 864 December 2008,p932.

22 Jean Pictet ,commentary on rhe Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 ,international committee of the Red Coss ,Geneva 1987 ,p390

ظهرت الحاجة الى وجود ترابط بين المبادئ الموجودة في المادة ٣٥ وقيود الحظر والتقيد على الاسلحة التي تسبب الالام غير المبررة او التأثيرات العشوائية ، وجدت بعض الوفود الحاجة لقواعد خاصة تؤسس لجهاز خاص ، لجنة مسؤولة لتحديد الاسلحة واساليب القتال التي تستخدم والتي يمكن ان تقع في دائرة المحظورات ، تلك اللجنة شكلت بموجب البروتوكول . وان تكون تلك الاجراءات الغاية منها ضمان نصوص المادة ، وعقدت مؤتمرات متخصصة لغرض توقيع اتفاقيات خاصة في هذا المجال بموجب القانون الدولي الانساني .

ibid,p421-422

قراءة المادة ٣٦ تبين ان الدول الأطراف عليها التزام بتقييم الاسلحة الجديدة ووسائل وأساليب القتال في ضوءالبروتوكول الإضافي الأول وغيرها من القواعد القانونية القابلة للتطبيق في القانون الدولي ، إشارة الى تعليق اللجنة الدولية للصليب الأحمر على البروتوكولالإضافيالأول، المادة ٣٦ تتضمن التزام بتبني إجراءات داخلية لتحديد قانونية الاسلحة الجديدة وأساليب القتال.

AGuide to the Legal of New Weapons , op.cit,p933-934.

المادة ٣٥ (ان حق اطراف أي نزاع مسلح في اختيار اساليب ووسائل القتال ليس حقا لا تقيده قيود ٢- يحظر استخدام الاسلحة والقدائف والمواد ووسائل القتال التي من شأنها احدثت اصابات او الام لا مبرر لها ٣- يحظر استخدام وسائل واساليب للقتال ، يقصد بها او قد يتوقع منها ان تلحق بالبيئة الطبيعية اضرارا بالغة واسعة الانتشار وطويلة الامد) .

26 Jean Pictet, op.cit,p424

ان عبارة أسلحة ووسائل الحرب لم يوضع لها تعريف ، ومن ثم لا بد من تفسيرها تفسيراً معقولاً . وتحديد ما اذا كانت إحدى المعدات تعتبر سلاحاً ام لا عملية مباشرة نسبياً ، اذ يفيد التعبير ضمناً القدرة الهجومية التي يمكن ان تطبق على هدف عسكري او مقاتل من الأعداء . أما الصعوبة الأكبر فتكمن في تحديد تعبير وسائل وأساليب الحرب . وقد اقترح ان عبارة أساليب الحرب تعني الطريقة التي تستخدم بها الاسلحة . كما ذكر أيضاً انه من غير الواضح وجه الاختلاف بين كلمة أسلحة ووسائل الحرب . ومن المسلم ب هان مصطلحات وسائل وأساليب الحرب يمكن من الناحية العملية ان تقررا معا . وبذلك تشمل تلك البنود المعدات التي قد لا تشكل سلاحاً بالمعنى المفهوم ، ولكن لها اثر مباشر على القدرة الهجومية للقوات التي تملكها . ومن الأمثلة على ذلك عربة تطهير الألغام ، وربما لا تخضع سماتها للجدل من المنظور القانوني ، ولكن ربما يكون من المعقول ان تدرج في نطاق وسائل وأساليب الحرب لأنها تقدم أسهاماً مباشراً في القدرة الهجومية للقوات العسكرية . على انه من الضروري ان نفرق بين

المعدات واستخدامها وبين التكتيكات ، والتقنيات ، والإجراءات التي تتبعها القوات المسلحة .
اذ تغطي هذه الجوانب نطاقا كبيرا من المجالات لا تتعلق كلها باستخدام الأسلحة او وسائل
الحرب . وهي في الواقع توفر أطارا للعمل تجري من خلاله العمليات التي صممت للعدد الهائل
من الظروف التي تواجهها القوات في الميدان ، وهي لا تقضي نطاق المادة ٣٦. ويصدق هذه
أيضا على الرقابة على استخدام السلاح في أطار قواعد الاشتباك ، فهي لا تشكل جزءا من
عملية المراجعة القانونية ، بل تخص بالضرورة العمليات تحديدا ، ولا يمكن التكهن بها في
الأعداد للمراجعة القانونية لسلاح او لوسيلة او أسلوب للحرب .

جستين ماك كلياند ، استعراض الاسلحة وفقا للمادة ٣٦ من البرتوكول الاضافي الاول ،
المجلة الدولية للصليب الاحمر ، العدد ٨٥٠ ، ٢٠٠٣ ، ص ٨ .

ان عبارة اسلحة ووسائل واساليب الحرب لم يوضع لها تعريف ، ومن ثم لا بد من تفسيرها
تفسيرا معقولا وتحديد ما اذا كانت احدى المعدات تعتبر سلاحا ام لا عملية مباشرة نسبيا ، اذ
يفيد التعبير ضمنا القدرة الهجومية التي يمكن ان تطبق على هدف عسكري او مقاتل من
الاعداء ، اما الصعوبة الاكبر فتكمن في تحديد تعبير وسائل واساليب الحرب . وقد اقترح ان
عبارة اساليب الحرب تعني الطريقة التي تستخدم بها الاسلحة . كما ذكر ايضا انه من غير
الواضح وجه الاختلاف بين كلمة اسلحة ووسائل الحرب ، ومن المسلم به ان مصطلحات
وسائل واساليب الحرب يمكن من الناحية العملية ان تقرا معا ، وبذلك تشمل تلك البنود
المعدات التي لا تشكل سلاحا بالمعنى المفهوم ، ولكن لها اثر مباشر على القدرة الهجومية
للقوات التي تملكها ، ومن الامثلة على ذلك عربة تطهير الالغام ، فربما لا تخضع سماتها
للجدل من المنظور القانوني ، ولكن ربما يكون من المعقول ان تدرج في نطاق وسائل
واساليب الحرب لأنها تقدم اسهاما مباشرا في القدرة الهجومية للقوات العسكرية ، مع الاخذ
بنظر الاعتبار ان التكتيكات العسكرية لا تقع في نطاق المادة ٣٦ . نفس المصدر ، ص ١٠ -
. ١١

الاسلحة الحديثة ، منشور قسم الخدمات الاستشارية للقانون الدولي الانساني ، اللجنة
الدولية للصليب الاحمر .

Jean Pictet, op.cit,p426-427 30

31 Isabelle Daoust ,Robeincoupland and Rikkelshoey ,new wars,
new weapons ? the obligation of states to assess the legality of
means and methods of warfare , review of international red cross
,Vol. 84,N.846,June ,2002.p350-351.

32 Kathleen Lawand, Reviewing , the legality of new weapons ,
mans and methods of warfare , international review of the red
cross , volume 88 number 864 December 2006, p926-927.

ibid .p927 33

34 Kathleen Lawand , op.cit, p354.

35 Isabelle Daoust , Robeincoupland and
Rikkelshoey, op.cit, p354-356

ibid, p362. 36

جستين ماك كليلاند ، مصدر سابق ، ص ١٠.

Knut Dormann, applicability of the additional protocols to computer
network attacks, 2004, p2

واضح ان النهي عن قتال هؤلاء ليس لكونهم عاجزين عن القتال الفعلي ولكن لعدم اشتراكهم
في القتال ، ومن ثم فان قتل من هؤلاء في حروب المسلمين كان بسبب اشتراكه في
الأعمال العدائية ضد المسلمين .

د . عبد الغني عبد الحميد محمود ، حماية ضحايا النزاعات المسلحة في القانون الدولي
الإنساني والشريعة الإسلامية ، بعثة اللجنة الدولية للصليب الأحمر - القاهرة ، الطبعة الرابعة
٢٠٠٩ ، ص ٥٤ .

والواقع ان بورتاليس كان يردد حرفيا الفقه الذي قال به جان جاك روسو في كتابه ذائع الصيت
العقد الاجتماعي والذي وضع أساسا فقهيا للترقية بين المقاتلين وغير المقاتلين ، وعندما قرر
ان الحرب علاقة بين الدول وليست علاقة عداء بين المواطنين المدنيين الا بصفة عرضية .
الاستاذ الدكتور صلاح الدين عامر ، التفرقة بين المقاتلين وغير المقاتلين ، دراسات في
القانون الدولي الإنساني ، دار المستقبل العربي ، القاهرة ، ٢٠٠٠ ، ص ٩٧ .

جون -ماريهنكرتس ولويز دوزوالد- بك ، القانون الدولي الإنساني العرفي - المجلد الأول :
القواعد ، اللجنة الدولية للصليب الاحمر ، القاهرة ، ٢٠٠٧ ، ص ٣ .

القاعدة الأساسية في الحماية والتمييز تجسدت في نص المادة ٤٨ ، والتي أسست لتدوين
قواعد وأعراف الحرب ، السكان المدنيين والأعيان المدنية يجب أن تكون محمية ومحترمة
أثناء النزاعات المسلحة ، ولذلك الغرض لا بد من تمييزهم عن المقاتلين والأهداف العسكرية
هذا النظام تأسيس في لاهاي عام ١٨٩٩ و ١٩٠٧ وفي جنيف من عام ١٨٦٤ الى
١٩٧٧ والتي أصبحت قاعدة عرفية ، مع ملاحظة ان نص المادة تم تبنيه بصورة ضمنية في

إعلان سان بطرسورغفي ١٨٨٦ ، والتي أكدت على ان الهدف الرئيسي التي تسعى أطراف النزاع تحقيقه هو منع الخصم من مواصلة القتال ، ونتيجة لذلك يمنع توجيه ضربات من شأنها أحداثاآلام غير مبررة . في اتفاقيات لاهاي شأنها شأن اتفاقيات جنيف تم قبول هذا المبدأ كقاعدة قانونية .

Jean Pictet, op.cit,p 598.

جون -ماريهنكرتس ولويز دوزوالد ، مصدر سابق ، ص٥ - ص٧ .
شكلت تلك المادة القاعدة الاساسية (مبدا التمييز) الذي يميز بين السكان المدنيين والمقاتلين من ناحية ، وبين الاهداف العسكرية والمدنية من ناحية اخرى ، وتم الاتفاق على المبدأ مع اعتراض جاء فيه (تطبيق القاعدة مرهون بقدرات وممارسات كل طرف على حدة ، قدرة الاطراف على التمييز يعتمد على الوسائل المتاحة لكل طرف بصورة عامة ، وعليه فان المادة لا تطلب من الاطراف القيام بعمل ليس في مقدورهم القيام به) . الا ان البروتكول يلزم الدول الاطراف بتهيئة مستلزمات احترام قواعده ، ولذلك من المفيد على الدول الاطراف امتلاك تلك المستلزمات .

0Jean Pictet, op.cit,p 60

45Jean-Marie Henckaerts and Louis Doswald – Beck ,customary international humanitarian law – practices , international committee of red cross,Cambridge,2005,p12

ibid .p600 46

47Marco Alberto Velasquez – Ruiz , the principles of distinction and proportionality under the framework of international criminal responsibility –content and issues– ,int.law.Rev.colomb,n14,2009,p30–31.

48Daphne Richemond – Barak , Nonstate Actors in Armed Conflicts : issues of Distinction and Reciprocity , p118

49Trevor A. Keck,The Principle of Distinction, the Question of Direct Participation in

Hostilities and Evolving Restraints on the Use of Force in Warfare,From the SelectedWorks of Trevor Keck,2011,p13–14

50 Noelle Quenivet , the war on terror and the principle of distinction in international humanitarian law,ACDI,Bogota ,2010,p162

51Jean Pictet , commentary : Geneva convention III Relative to the treatment of prisoners of war , international committee of the red cross ,1960,p51

52kKatherine Del Mar , the requirement of belonging under international humanitarian law , the European journal of international law ,VOL.21 NO.1,2010,p123

Michael Gerais , op.cit, p34.

Ibid ,p34.

Sean Watts , combatant status and computer network attack ,Virginia journal of international law,VOL.50:2,2010p424.

Ibid ,p425

James Fallows Tierney , threshold constraints and laws of wars , university of Chicago,lawschool,2011,p31.

Ibid,p32

Emily Crawford , virtual battlegrounds : direct participation in cyber warfare , Sydney law school, legal studies research paper , NO.12/10,February 2012,p15.

دليل تفسيري لمفهوم المشاركة المباشرة في العمليات العدائية وفق القانون الدولي الانساني ،اللجنة الدولية للصليب الاحمر ،القاهرة، ٢٠١٠، ص ٣٩ .

. Emily Crawford,op.cit,p16.

Ibid,p17.

Ibid,p18

..Sean Watts,op.cit,p446-447.

John Richardson, op.cit,p27.

PapanastasionAfroditi,op.cit,p26.

, 0Jeffrey T.G.Kelsey,op.cit,p144.

ibid,p144.

Michael Gerais,op.cit,p35–36

James Fallows Tierney,op.cit,p28.

ibid,p29.

Michael Gerais,op.cit,p36

Knut Dormann,op.cit,p10. 73

74 Eric Talbot Jensen , cyber warfare and precautions against the effects of attacks,Texas Law Review , VOL.88:1533,2010,p1553.

