الاحتياجات في الهجمات على شبكة الحاسوب والمسؤولية الجنائية للقادة والرؤساء

م . م سراب ثامر أحمد
كلية القانون – جامعة ذي قار
legalur@yahoo.com

المقدمة

من المعلوم ان الهجمات على شبكات الحاسوب التي لا يكون توجيهها لهدف عسكري محدد أو تلك التي لا يمكن الحد من آثارها طبقا" لما يقتضيه القانون الدولي الانساني تعد هجمات عشوائية محظورة الى جانب تلك الهجمات التي يتوقع ان تتسبب في الاصابات أو الاضرار العرضية للسكان المدنيين والاعيان المدنية بصورة مفرطة مقارنة بالميزة العسكرية المتوقعة والمباشرة مما يتوجب على الطرف المسؤول عن التخطيط لتلك الهجمات أو اتخاذ قرار بشأنها ان يتخذ الاحتياطات اللازمة اثناء الهجوم لتفادي مثل تلك الآثار، وبالمقابل ينبغي على المدافع اتخاذ كافة الاحتياطات الضرورية ضد الآثار التي يمكن ان تترتب عليها ، وبخلاف ذلك يتحمل كلا" من القائد العسكري أو المسؤول المدني المسؤولية الجنائية عن الأوامر العسكرية غير المشروعة ، ولدراسة ما تقدم ارتأينا تقسيم هذا البحث على مبحثين ، خصصنا المبحث الأول لتناول الاحتياطات في الهجمات على شبكات الحاسوب ، فيما خصصنا المبحث الثاني لتناول موضوع المسؤولية الجنائية للقادة والرؤساء في الهجمات على شبكات الحاسوب .

Abstract

This research deals with the precautions that must be taken during computer network Attacks . This issue raise different questions concerning the applicability of the laws of International Humanitarian law .Such as the precautions that must be taken by those. Who are planning or executing the CNA ? Are the commanders or other superiors responsible for the acts of their subordinates in conducting CNA ?

All these questions have been discussed throughout this research and the conclusion is that despite the newness of the technology of CNA , legal constraints apply to it , and it should be undertaken in a way which respects existing law and its related principles .

المبحث الاول
الاحتياطات في الهجمات على شبكات الحاسوب

يقتضي احترام مبدأ التميز ومبدأ التناسب ضرورة اتخاذ الاحتياطات التي تضمنتها المادة (٥٧) من البروتكول الإضافي الأول عند الهجوم ، وذلك من اجل تجنب التسبب بالخسائر المدنية العرضية او التقليل منها الى الحد الأدنى ورغبة في تجنب الاستهداف الخاطئ او التعسفي للأشخاص والاعيان المدنية .وعليه سنقسم هذا المبحث على مطلبين ، نخصص المطلب الاول لدراسة الاحتياطات اثناء الهجمات ، فيما نخصص المطلب الثاني لتناول الاحتياطات ضد آثار الهجمات .

المطلب الاول
الاحتياطات اثناء الهجمات

تكرس ممارسة الدول هذه القاعدة كإحدى قواعد القانون الدولي العرفي المنطبقة في النزاعات المسلحة الدولية وغير الدولية التي اشارت في الجزء الأول منها الى ضرورة بذل الرعاية المتواصلة في إدارة العمليات العسكرية لتفادي المدنيين من الأشخاص والاعيان وهذا ما أكدته الجمعية العامة للأمم المتحدة في قرارها المرقم ٢٦٧٥ على ((بذل كافة الجهود في إدارة العمليات العسكرية لتفادي معاناة السكان المدنيين ويلات الحرب واتخاذ جميع الاحتياطات الضرورية من اجل تجنب إيقاع الإصابات او الخسائر في صفوفهم او الاضرار بهم)) [١] هذه القاعدة العامة الواردة في الفقرة الأولى من المادة (٥٧) تشير الى مفهوم العمليات العدائية الذي يعد مفهوماً واسعاً بما يكفي لينطبق على العمليات على شبكات الحاسوب بما فيها الهجمات ، وذلك لأن واجب (بذل الرعاية المتواصلة) هو ذو طبيعة مستمرة وينطبق خلال جميع العمليات على شبكات الحاسوب ولا يقتصر على المرحلة التحضيرية فقط ويقع بالتالي على عاتق كل من ينخرط في تلك العمليات واجب تأدية هذا الالتزام وذلك لحماية المدنيين والاعيان المدنية [٢]

هذا وقد أشار دليل تالين للحرب السيبرانية في القواعد (٥٣ – ٥٩) منه الى ان من يخطط لهجوم على شبكات الحاسوب ويتخذ قراراً بشأنه ينبغي ان يتخذ جملة من الاحتياطات فيما يتعلق بذلك الهجوم ، بمعنى ان تلك الاحتياطات تتعلق بالهجمات على شبكات الحاسوب التي يمكن ان تحدث الموت او الإصابة للأشخاص والتلف او الدمار للاعيان وبصورة حصرية .

فالقاعدة (٥٣) من هذا الدليل اشارت الى ضرورة قيام من يخطط للهجمات على شبكات الحاسوب ببذل ما في طاقته عملياً للتحقق من ان الأهداف المقرر مهاجمتها ليست اشخاصاً مدنيين او اعياناً مدنية وانها غير مشمولة بحماية خاصة ، وانما هي اهداف عسكرية بالمعنى الذي اوردناه سابقاً [٣] .

وطبقاً لما ذهبت اليه اللجنة الدولية للصليب الأحمر وممارسة الدول ، فان الواجب في اتخاذ الاحتياطات (العملية) تقتصر على تلك الاحتياطات التي يمكن اجراؤها او الممكنة عملياً ، مع الاخذ بعين الاعتبار كافة الظروف السائدة في حينه ، بما في ذلك الاعتبارات الإنسانية والعسكرية [٤].

وعند التصديق على البروتكول الإضافي الأول ، أعلنت بعض الدول مثل سويسرا على ان الواجب الذي يفرضه المادة (٥٧ / ٢) منه على من يخطط لهجوم او يتخذ قراراً بشأنه في اتخاذ التدابير الاحتياطية المحددة والمنصوص عليها في هذه المادة يشكل التزاماً " للضباط القادة فقط على مستوى الكتيبة او الفوج وما فوق " ، وبذات المعنى ذهبت النمسا في المؤتمر الدبلوماسي ذاته الذي أدى الى اعتماد البروتكولين الاضافيين في انه " لا يمكن التوقع من العسكريين من أصحاب الرتب الدنيا اتخاذ جميع الاحتياطات المفروضة وعلى الأخص احترام مبدأ التناسب اثناء الهجوم " [٥]

الا ان ذلك لا يعني اعفاء أصحاب الرتب الدنيا بصورة كاملة من اتخاذ الاحتياطات المماثلة ، فعلى سبيل المثال ، اذا تم التخطيط للهجمات على شبكات الحاسوب مع اتخاذ كافة الاحتياطات الواجبة بما فيها تحديد كون الهدف ذو طبيعة عسكري ، فانه واثناء انتظار منفذ الهجوم للأوامر بالتنفيذ من القيادة العليا ، قد تظهر بعض التغيرات في البيئة الالكترونية بخصوص الهدف المعني يفرض واجب إبلاغه بأسرع وقت ممكن لمن يملك سلطة اصدار القرار بالهجوم ، وهذا يمثل جزءاً من تلك الاحتياطات [٦] .

ومن المسلم به ان جميع الهجمات على شبكات الحاسوب (على خلاف الهجمات العشوائية) تتطلب الالتزام بإجراء المسح والفحص الدقيق للنظم الالكترونية المستهدفة لتحديد الثغرات التي يمكن من خلالها اختراق ذلك النظام والنفاذ اليه ، وذلك من خلال عمليات استغلال شبكات الحاسوب التي تمثل الجانب الاستخباري لهذه العمليات ، هذا الالتزام لا يقتصر فقط على الأهداف التي تم اختيارها ، بل يمتد ايضاً ليشمل مصدر الهجمات المضادة الذي يمكن ان يشنه الطرف الخصم للتحقق من مصدره وتحديد طبيعة كونه هدفاً عسكرياً وليس مدنياً او مشمولاً بحماية خاصة ، وعلى الرغم من ان الاسناد الدقيق لمثل تلك الهجمات ينطوي على صعوبة ، وذلك

لتعمد المهاجم بتضليل الخصم باستخدام وسائل الكترونية ، الا ان ما يتوجب ملاحظته في هذا الشأن ان ذلك الخداع ينبغي ان لا يمتد ليخرق المادة (٥١ / ٧) من البروتكول الإضافي الأول عن طريق اطلاق تقارير استخبارية كاذبة لتضليل العدو ودفعة لمهاجمة اشخاص مدنيين او اعياناً مدنية بناءً على اعتقاد خاطئ بانها اهداف عسكرية [٧].

على ان مدى المعرفة المتوقعة من القادة العسكريين في تقييمهم للأهداف المحتملة والتحقق من طبيعتها ، قد تعد مشكلة تثير الاهتمام ، وهذا يفرض على أولئك القادة او الأشخاص الآخرين المسؤولين عن التخطيط للهجمات او اتخاذ قرار بشأنها ، ضرورة التوصل الى تلك القرارات بناءً على تقييمهم للمعلومات المتوفرة من كافة المصادر المتاحة لهم في ذلك الحين ، وبما ان القادة او المسؤولين من الأشخاص الاخرين ، لا يمتلكون المعرفة الشخصية عن كل هدف للهجوم ، فعليهم تبعاً لذلك الاعتماد على التقارير الاستخبارية للتزود بمثل تلك المعلومات ، ويتحقق ذلك بالحصول على افضل الاستخبارات الممكنة ، بما في ذلك المعلومات بشأن تجمع الأشخاص المدنيين والاعيان المدنية المهمة وبخاصة الاعيان المحمية والبيئة الطبيعية والمحيط المدني للأهداف العسكرية ، وهذا ما أكدته المحكمة الجنائية الدولية ليوغسلافيا السابقة عندما ذهبت الى ان :

" على القائد العسكري ان يؤسس لنظام فعال لجمع وتقييم المعلومات الاستخبارية المتعلقة بالأهداف المحتملة ، وعليه يقع واجب توجيه قواته العسكرية لاستخدام الوسائل التقنية لتحديد الأهداف بصورة صحيحة خلال العمليات العسكرية " [٨]

والامر ذاته ينطبق في سياق الهجمات على شبكات الحاسوب ، من حيث ضرورة توافر المعلومات الموثوقة بشأن الأهداف المحتملة وهذه تدخل ضمن مهام فريق خبراء الحاسوب وذلك لأنه وكما ذهب الكاتب (Michael N. Schmitt) الى ان " موازنة التلف والأذى العرضي المصاحب للهجوم مقابل الميزة العسكرية المتوقعة منه يصعب تقيمها دون معرفة كيفية عمل نظام الحاسب الآلي الداخلة في العملية ومدى اتصالها بالنظم الالكترونية الأخرى، وهذا يقتضي ضرورة وجود أولئك الخبراء من ذوي الاختصاص لتقييم مثل تلك الآثار " [٩] .

وتبعاً لما تقدم فان الاحتياطات المستطاعة في السياق الالكتروني أي في سياق الهجمات على شبكات الحاسوب تتضمن جمع المعلومات الاستخبارية عن الشبكة الالكترونية من خلال وضع خريطة لتلك الشبكة المستهدفة ، على ان الإجراءات غير المستطاعة لا تدخل ضمن هذا الالتزام ، فاذا لم يكن بالإمكان وضع مخطط لشبكة النظام الالكتروني مثلاً لأن القيام بذلك يؤدي الى كشف العملية العسكرية المرتقبة وبالتالي يمكن للإجراءات الدفاعية الالكترونية للطرف الخصم التصدي لها فأن ذلك الالتزام لا يعد واجباً، اما عند عدم إمكانية المهاجم من جمع المعلومات الموثوقة بشأن طبيعة ذلك الهدف ، فان على القائد العسكري او المسؤول عن اتخاذ القرار الالتزام بتقييد نطاق الهجوم على أجزاء النظام الالكتروني الذي تتوافر بشأنه المعلومات الكافية[١٠].

الالتزام الآخر الذي يقع على عاتق من يخطط الهجمات على شبكات الحاسوب او يتخذ قراراً بشأنها وأن يتخذ جميع الاحتياطات المستطاعة عند اختيار وسائل وأساليب الهجوم من اجل تجنب احداث خسائر في أرواح المدنيين او الحاق الإصابة بهم او الاضرار بالأعيان المدنية وذلك بصفة عرضية وعلى أي الأحوال حصر ذلك في اضيق نطاق ، وفي ذات المعنى ذهبت القاعدة (٥٤) من دليل تالين للحرب السيبرانية[١١] .

وقد ذهب الكاتب (Kalshoven) الى ان الالتزام الرئيس بموجب هذه الفقرة " يتمثل بتجنب احداث الخسائر بين السكان المدنيين او اصابتهم او الحاق الضرر بالأعيان المدنية ، اما الالتزام بالتقليل من تلك الآثار وحصرها في نطاق ضيق فانه يلعب دوراً عند عدم الاستطاعة في تجنب احداث النتائج المترتبة على الالتزام الرئيسي"[١٢].

هذه الخصائص تعزز من استخدام الهجمات على شبكات الحاسوب كإحدى وسائل الحرب التي قد لا تعرض ـ في اكثر الأحيان ـ حياة السكان المدنيين او الأعيان المدنية للخطر او الدمار قياساً بالوسائل القتالية التقليدية وهذا ما اكده الكاتب (Michael N. Schmitt) من انه " حتى اذا كان الهدف المختار هدفاً مشروعاً والهجوم المزمع القيام به متناسباً ، يظل على القائمين بالهجوم الالتزام باختيار أساليب ووسائل الحرب التي من شأنها ان تحدث اقل دمار مصاحب او اذى عرضي في حالة تساوي العوامل الأخرى مثل المخاطرة بالقوة التي تقوم بالهجوم ، واحتمال النجاح ومخزون السلاح ..... الخ " [١٣]

وكما اشرنا سابقاً ، فان قضية تداعيات الهجمات على شبكات الحاسوب وآثارها غير المباشرة تعد على جانب كبير من الأهمية وذلك للتداخل والترابط بين النظم الالكترونية العسكرية والمدنية ، مما يعني معه ضرورة اعتبار الآثار غير المباشرة لمثل تلك الهجمات بمثابة اضرار عرضية ، وهذا بدوره يلقي على عاتق القائد العسكري او غيره من الأشخاص المسؤولين عن التخطيط لتلك الهجمات باتخاذ كل الاحتياطات المستطاعة لتلافي او على الأقل لتقليل الاضرار العرضية المباشرة وغير المباشرة للهجمات على شبكات الحاسوب [١٤] .

جيم / أوردت المادة (٥٧ / ٢ / ب) من البروتكول الإضافي الأول والقاعدة (٥٧) من دليل تالين للحرب السيبرانية التزاماً يقضي بوجوب القيام بكل ما هو مستطاع لإلغاء او تعليق الهجوم على شبكات الحاسوب في الأحوال التالية : ـ

١ـ اذا تبين ان الهدف ليس هدفاً عسكرياً او انه مشمول بحماية خاصة

٢- او ان الهجوم قد يتوقع منه ان يحدث خسائر في أرواح المدنيين او الحاق الإصابة بهم او الاضرار بالأعيان المدنية او ان يحدث خلطاً من هذه الخسائر والاضرار وذلك بصفة عرضية ، تفرط في تجاوز ما ينتظر ان يسفر عنه ذلك الهجوم من ميزة عسكرية ملموسة ومباشرة [١٥] .

هذا الالتزام ينطبق في سياق الهجمات على شبكات الحاسوب ، في الأحوال التي تتخذ فيها الاحتياطات الضرورية من قبل أولئك الذين يخططون للهجوم او ينفذونه ، الا ان ظهور معلومات جديدة يحتمل معها ان يؤدي الهجوم الذي تم التخطيط له مسبقاً الى وقوع خسائر واضرار عرضية مفرطة بالقياس للميزة العسكرية الملموسة والمباشرة تتطلب الغاء الهجوم او تعليقه .

فعلى سبيل المثال ، قد تعمد الدولة (أ) الى القيام بوضع قنبلة منطقية في احد أجزاء شبكة الاتصالات العسكرية للدولة (ب) قبل بدء الاعمال العدائية ، وعند الشروع بتلك الاعمال يتعين على الدولة (أ) القيام بتفعيل تلك القنبلة ، الا انها قد تتمكن من الحصول على معلومات تفيد بقيام الدولة (ب) مؤخراً بربط النظام الالكتروني لخدمات الطوارئ المدنية بشبكتها العسكرية (المستهدفة بالهجوم)، مما يعني التزام الدولة (أ) ، تطبيقاً لمبدأ التناسب ، تعليق ذلك الهجوم والقيام بالاستطلاعات الإضافية للتأكد من طبيعة الاضرار التي يمكن ان تلحق بالسكان المدنيين عند استهداف نظام الطوارئ وتعطله [١٦] .

إضافة لما تقدم ، يلتزم من يخطط للهجمات على شبكات الحاسوب او يتخذ قراراً بشأنها ، ان يقوم بتوجيه انذار مسبق وفعال قبل تلك الهجمات التي يحتمل ان تمس السكان المدنيين وبوسائل مجدية حسبما اشارت اليه القاعدة (٥٨) من دليل تالين ما لم تحل الظروف دون ذلك[١٧].

هذا وتعد الوسائل الالكترونية ، وسائل مجدية للإنذار فيما يتعلق بالهجمات على شبكات الحاسوب ، بل وحتى في الهجمات التقليدية ، على ان مدى فعالية ذلك الإنذار يتوقف على الظروف القائمة ، فمثلاً لا يعد الإنذار مطلوباً عندما لا تسمح الظروف بذلك ، وعندما يكون عنصر المفاجأة مثلاً اساسياً لنجاح العملية او لأمن القوات المهاجمة او عندما لا يكون هنالك مدنيين في المنطقة المزمع مهاجمتها ، كما ان فعالية الإنذار تعني مدى إمكانية المتلقي من استقباله والاستجابة له في الوقت المناسب وبالسرعة الضرورية .

وقد ذهبت الولايات المتحدة الامريكية انه لا حاجة لأن يكون الإنذار محدداً ، بل يمكن ان يكون عاماً ، حتى لا يعرض القوات المهاجمة او نجاح عمليتها للخطر ، إضافة الى ان مثل هذا الإنذار العام يمكن ان يكون شاملاً يوجه بثاً على موجات الاثير وينصح السكان المدنيين بالبقاء بعيداً عن الأهداف العسكرية [١٨].

وفي سياق الهجمات على شبكات الحاسوب فان مثل هذا الإنذار يمكن اما ان يوجه عن طريق العدو نفسه الذي يقوم بدوره بإنذار السكان المدنيين ، فمثلاً اذا كان من المزمع شن تلك الهجمات على اعيان ذات استخدام مزدوج ، فان الطرف المهاجم بوجه انذاراً للعدو بذلك الهجوم على افتراض قيام العدو بإبلاغ سكانه المدنيين بذلك لغرض العمل على تقليل الدمار العرضي الذي قد يلحق لهم .

او ان يقوم المهاجم بتوجيه الإنذار بنفسه وبصورة مباشرة الى السكان المدنيين عندما تدعو الظروف الى الاعتقاد بعدم قيام الخصم بإبلاغ سكانه المدنيين بذلك الهجوم رغبة منه في استخدامهم كدروع بشرية مثلاً ، وقد يكون هذا الإنذار عبر وسائل اعلام العدو او القيام بارسال رسائل نصية (SMS) الى كل مستخدم مدني [١٩] .

وكما اشرنا في أعلاه فان فاعلية الإنذار تتوقف على الظروف القائمة حينها ، فقد تتطلب الهجمات على شبكات الحاسوب عنصر المفاجأة الذي يعد ضرورياً للتأكد من قيام الطرف الخصم باستخدام وسائل الدفاع الالكترونية ضد الهجوم ، وقد يكون عنصر المفاجأة ضرورياً لأمن وحماية الطرف المهاجم ، فالإنذار في مثل هذه الحالة لا يعد مطلوباً لأنه قد يسمح للعدو وبمراقبة تلك الهجمات وردها على المهاجم .

وبالمثل فان الهجمات على شبكات الحاسوب قد تكون جزءاً من عملية عسكرية واسعة والانذار يمكن ان يؤدي الى كشف القوات وتعريضها للخطر ، هذا وان الإنذار بخصوص تلك الهجمات يمكن ان يكون عاماً وليس محدداً مثال ذلك توجيه إنذار يقضي بان الهجمات على شبكات الحاسوب ستشن ضد معدات توليد الطاقة الكهربائية (مزدوجة الاستخدام) في كافة إقليم العدو دون تحديد الهدف على وجه الدقة [٢٠].

الالتزام الآخر الذي يقع على عاتق من يخطط للهجمات على شبكات الحاسوب او يتخذ قراراً بشأنها ، يتمثل بضرورة اختيار الهدف العسكري الذي يتوقع ان يسفر الهجوم عليه عن احداث اقل قدر من الاخطار على أرواح المدنيين والاعيان المدنية ، من بين عدة اهداف تقدم ذات الميزة العسكرية ، اذا كان ذلك الخيار ممكناً هذا الالتزام ينحدر من المادة (٥٧ /٣) من البروتكول الإضافي الأول ، وبذات المعنى ذهبت القاعدة (٥٦) من دليل تالين للحرب السيبرانية[٢١] .

فكلما كان هناك فرصة للاختيار بين الأهداف العسكرية التي يمكن ان يحقق الهجوم عليها النتائج المرغوبة ، ينبغي اختيار الهدف الذي يحقق مخاطر اقل من الدمار المصاحب و الأذى العرضي ، وهذا ما جسدته اللجنة الدولية للصليب الأحمر في

تعليقها على البروتكول الإضافي الأول من انه ((يتوجب قذف خطوط السكك الحديدية بالقنابل بدلاً من ضرب محطاتها المتمركزة في المناطق المأهولة بالسكان المدنيين والاعيان المدنية)) [٢٢].

فلا يشترط وجود التماثل من الناحية الكمية والنوعية بين الأهداف ، طالما ان هناك مماثلة في الحصول على ذات الميزة العسكرية المتمثلة بالتفوق العسكري الملموس والمباشر .

لذلك ، تزيد إمكانية الهجمات على شبكات الحاسوب من فرص الاختيار فيما يتعلق بتقليل الدمار المصاحب او الأذى العرضي ، وكما ذهب الكاتب (Michael N. Schmitt) الى ان " التدمير المادي كان ضرورياً في الماضي لتعطيل مساهمة احد الأهداف في جهود العدو ، يمكن الان ببساطة أطفاء الهدف ، وبدلاً من القاء القنابل على احد المطارات على سبيل المثال ، يمكن قطع التحكم في المرور الجوي ، الشيء نفسه صحيح بالنسبة لإنتاج الطاقة ونظم التوزيع والاتصالات والمصانع وهكذا ، اذ يتعين على من يخططون وينفذون هذه العمليات ان يظلوا حريصين على التقليل من الدمار المصاحب والأذى العرضي والتقليل من تداعيات الضرب (نأخذ في الاعتبار مثال محطة الكهرباء العراقية التي ذكرناها آنفاً) ، وتقل المخاطر المرتبطة بالحرب الحركية التقليدية كثيراً في حالة الهجمات على شبكات الحاسوب ، حيث انه يمكن ببساطة ـ حسب النتيجة المرجوة ــ قطع التشغيل عن المنشأة المستهدفة ، وقد يكون هذا التكتيك مفيداً على وجه الخصوص في حالة الأهداف المزدوجة الاستخدام ، ففي حالة محطات الكهرباء مثلاً ، ربما يكون ضرورياً من الناحية العسكرية اغلاق النظام لفترة قصيرة ، كأن تكون قبيل الهجوم واثناءه ، ثم يمكن اعادته للعمل بعد انتهاء الحاجة الملحة لتوقفه وبذلك يمكن الحد من الاثار السلبية على سكان المدنيين من جانب ، ثم لن يكون هنالك حاجة لإعادة الإصلاح والبناء نظراً لعدم تحقق الدمار المادي للأهداف من جانب آخر ، مما يعمل على تسهيل عودة السكان المدنيين الى الحياة الطبيعية بعد انتهاء النزاع)) [٢٣] .

وقد أشار دليل تالين للحرب السيبرانية الى ضرورة ان تكون الميزة العسكرية المتحققة تمثل التفوق الذي يمكن ان يتم الحصول عليه كنتيجة للهجوم بأكمله وليس من ذلك الجزء المتمثل بالهجوم ، فاذا لم يتحقق ذلك من خلال اختيار هدف اخر من بين عدة اهداف ، يتوجب العدول عن القيام بذلك لأنه لن يحقق الغرض العسكري للهجوم بأكمله وان كان ذلك الجزء من العملية يؤدي الى تقليل من الأذى العرضي ، فعلى سبيل المثال ، الهجمات على شبكات الحاسوب التي تستهدف تعطيل نظام القيادة والسيطرة التابع للعدو ، يطرح امام المهاجم خيارات عدة ، تتمثل احداها باستهداف أجزاء من شبكة الامداد بالطاقة الكهربائية (ذات الاستخدام المزدوج) التي يعتمد عليها نظام الاتصالات للعدو مع إمكانية وقوع الإصابة والاذى العرضي في صفوف المدنيين ، بينما يتمثل الخيار الاخر باستهداف شبكة القيادة والسيطرة التابعة للعدو بصورة مباشرة فان الخيار الأخير هو المرجح اذا كان من شأنه ان يقلل من الأذى العرضي الذي يمكن ان يلحق بالمدنيين ، شريطة ان يؤدي الى الحصول على ذات الميزة العسكرية ، التي كان من المفترض تحققها في حالة الخيار الأول ، وان تكون تلك الميزة في ضوء العملية العسكرية بأكملها [٢٤] .

على ان واجب الاختيار بين الأهداف ليس واجباً مطلقاً وانما يطبق فقط " حين يكون الخيار ممكناً " بحسب نص المادة (٥٧ / ٣) من البروتكول الإضافي الأول ، لذلك ينبغي على المهاجم الالتزام به اذا كان ممكناً ـ وفي سياق الهجمات على شبكات الحاسوب ، يتوقف ذلك على إمكانية النفاذ الى شبكة الالكترونية للعدو ، او القدرة على تحديد الاثار المترتبة على تحييد أجزاء محددة من تلك الشبكة وعلى مدى إمكانية ضرب الهدف في الوقت المحدد للعملية العسكرية ، ومدى إمكانية الحصول على ذات الميزة العسكرية ، بمعنى اخر ، ان كل ذلك يتوقف على تحقيق المهمة والمجازفة المسموح بها والا تعين على المهاجم ان يخلص الى ان اتخاذ مثل ذلك القرار يعد مستحيلاً [٢٥] .

المطلب الثاني

الاحتياطات ضد آثار الهجمات

اشارت القاعدة (٥٩) من دليل تالين للحرب السيبرانية الى أنه " ينبغي على اطراف النزاع قدر المستطاع ، اتخاذ الاحتياطات الضرورية لحماية السكان المدنيين والاعيان المدنية الموجودة تحت سيطرتها ضد الاخطار الناجمة عن الهجمات على شبكات الحاسوب " .

هذه القاعدة تنحدر من المادة (٥٨ / ج) من البروتكول الإضافي الأول ، حيث تعد قاعدة من قواعد القانون الدولي الإنساني العرفي المنطبقة في النزاعات المسلحة الدولية وغير الدولية .

والقواعد التي اشرنا اليها في القاعدة (٥٧) من الدليل و(٥٧) من البروتكول الاضافي الأول ، انما تمثل الاحتياطات التي تقع على عاتق المهاجم اثناء الهجوم ، في حين ان هذه القاعدة تتعلق بالاحتياطات الواجبة من قبل المدافع ضد آثار تلك الهجمات [٢٦] .

هذا وقد أشار ، تعليق اللجنة الدولية للصليب الأحمر على البروتكول الإضافي الأول الى ان " القيام ببناء الملاجئ ، وحفر الخنادق ، نشر المعلومات ، توجيه التحذيرات ، تنظيم المرور ، حراسة الممتلكات المدنية ، تعبئة منظمات الدفاع المدني هي تدابير يمكن اتخاذها لتفادي اثار تلك الهجمات على ما تحت سيطرة ذلك الطرف من سكان مدنيين او اعيان مدنية " [٢٧] .

انما في سياق الهجمات على شبكات الحاسوب فتتمثل بعزل البنى التحتية الالكترونية العسكرية عن المدنية وفصل نظم الحاسب الآلي التي تعتمد عليها تلك البنى التحتية الأساسية عن شبكة الانترنيت ، عدم استخدام شبكة الاتصالات المدنية للأغراض العسكرية ، دعم البيانات المدنية الرقمية بنسخ احتياطية ، استخدام الإجراءات المضادة لفايروسات الحاسوب لحماية النظم المدنية الى جانب ضرورة القيام بالإجراءات اللازمة لإصلاح نظم الحاسب الآلي المهمة بصورة مستمرة مما قد يلحق بها من الدمار بسبب الهجمات على شبكات الحاسوب القيام بتوزيع البرامجيات الواقية ، مراقبة النظم والشبكات الالكترونية وتطوير قدرات رد الفعل لمنع التسلل من قبل الخصم للنظم الالكترونية المدنية [٢٨] .

الا ان تلك الاحتياطات المستطاعة ضد اثار الهجمات تقتصر على الاحتياطات التي يمكن القيام بها او الممكنة عملياً ، مع الاخذ بعين الاعتبار جميع الظروف السائدة في حينه بما فيها الاعتبارات الإنسانية والعسكرية ، حسبما ذهبت اليه اللجنة الدولية للصليب الأحمر في تفسيرها للبروتكول الإضافي الأول " ان من الواضح ان تلك الاحتياطات تمثل واجب اطراف النزاعات المسلحة الدولية وغير الدولية ، وبالقدر المستطاع ، نقل ما تحت سيطرتها من اشخاص مدنيين واعيان مدنية بعيداً عن المناطق المجاورة للأهداف العسكرية " [٢٩].

لذلك قد لا يكون من المستطاع عملياً قيام اطراف النزاع بفصل او عزل الأهداف العسكرية عن الأهداف المدنية كمحطة توليد الطاقة الكهربائية ، او مركز التحكم في الحركة الجوية التي تعد اعياناً مزدوجة الاستخدام من قبل كل من العسكريين والمدنيين ، مما يعني احتمال وجود الاعيان المدنية والأشخاص المدنية في مثل هذه المواقع التي تعد اهدافاً مشروعة للهجوم ، وبالمثل قد يستحيل فصل الوظائف العسكرية عن الوظائف المدنية لتلك البنى التحتية الالكترونية بما يتفق مع هذا الالتزام ، لكن استحالة القيام بتلك الإجراءات الاحتياطية ضد اثار الهجمات على شبكات الحاسوب ، لا تعفي اطراف النزاع من الالتزام بضرورة توفير الحد الأقصى المستطاع من الإجراءات الأخرى لحماية المدنيين وباحترام مبدأ التناسب ، وهذا الالتزام باتخاذ الاحتياطات ضد اثار الهجمات على شبكات الحاسوب ، حسب ما اجمع عليه في دليل تالين ، تمتد لتشمل البنى التحتية الالكترونية المدنية والأنشطة المرتبطة بها والواقعة تحت سيطرة طرف في النزاع سواء كانت قائمة في اقليمه او تلك الواقعة في الجزء المحتل من إقليم العدو من قبل هذا الطرف ، فمتى تمكن ذلك الطرف من التحكم في عمليات نظم الحاسب الآلي المدنية فإنها تكون خاضعة لسيطرته ويلتزم بتوفير تلك الاحتياطات الدفاعية ضد آثار الهجمات لغرض توفير الحماية لها، الا ان تلك الحماية لا تمتد مثلاً لتشمل حماية المدنيين ضد اثار الهجمات على شبكات الحاسوب التي تتمثل بعدم قدرتهم على النفاذ الى الموقع الالكتروني بصورة مؤقته ، انما الالتزام بتوفير الحماية يكون في مواجهة الاثار التي تسببها تلك الهجمات والمتمثلة بالإصابة او الموت للأشخاص او التلف والدمار للاعيان وبصورة عرضية [٣٠] .

هذا وقد اشارت ممارسة الدول الى ان المهاجم ليس ممنوعاً من مهاجمة الأهداف العسكرية اذا قصر المدافع في اتخاذ الاحتياطات المناسبة ضد اثار الهجمات على شبكات الحاسوب ، مع ضرورة التزام المهاجم بالقواعد التي تغطي الهجمات وبخاصة مبدأ التمييز ومبدأ التناسب وضرورة اتخاذ الاحتياطات اثناء الهجوم الوارد في المادة (٥٧) من البروتكول الأول [٣١] .

المبحث الثاني

المسؤولية الجنائية للقادة والرؤساء في الهجمات على شبكات الحاسوب

تكتسب المسؤولية أهمية خاصة نظراً لما يترتب على انتهاك الالتزامات التي يفرضها القانون الدولي الانساني والمساس او الاخلال بالمبادئ الانسانية التي يرتكز عليها من خسائر فادحة مما يؤدي بالنتيجة الى افراغ تلك القواعد من مضمونها الفعلي . وما يميز النظام العسكري هو وجوب طاعة الاوامر وضرورة الانصياع لها وهذا ما تنص عليه التشريعات العسكرية ،الا ان هناك بعض المشاكل التي قد تثور بصدد الاوامر العسكرية والرئاسية غير المشروعة ،والتي تمثل انتهاكاً لقوانين الحرب [٣٢] . وعليه ارتأينا دراسة هذا المبحث في مطلبين ، نتناول في المطلب الاول المسؤولية عن الاوامر العسكرية والرئاسية غير المشروعة ، فيما نخصص المطلب الثاني لدراسة المسؤولية في حالة العلم اليقيني أو التقديري .

المطلب الاول
المسؤولية عن الاوامر العسكرية والرئاسية غير المشروعة

ومن المعلوم ان اهم قواعد واسس العمل العسكري ، ان ايه معركة لا تبدا الا اذا توافرت التقارير الاستخبارية المتمثلة بمجموعه المعلومات المتعلقة بقوة العدو العسكرية والاقتصادية ومراكز تجمعاته والخرائط المتعلقة بذلك .
هذا كله يلقي على عاتق جميع العاملين العسكريين في مراكز العمليات التحوط من اجل تفادي الحاق الاذى بالسكان المدنيين او الاعيان المدنية .
وعليه يلتزم كل قائد عسكري يخطط للهجوم او يتخذ قراراً بشأنه ان يضع في حسابه جميع الاحتياطات التي اشارت اليها المادة (٥٧) من البروتكول الإضافي الأول سالفة الذكر .
ومن ذلك مثلا الامتناع من اتخاذ أي قرار بشن هجوم قد يتوقع منه احداث خسائر في صفوف المدنيين او الحاق الضرر بالأعيان المدنية بصورة عرضية [٣٣] .
وفي سياق الهجمات على شبكات الحاسوب ،أورد دليل تالين قاعدة عامة بشأن المسؤولية الجنائية للقادة والرؤساء في حالة اعطاءهم الأوامر للقيام بتلك الهجمات التي ترقي الى جرائم حرب أولاً وحالة أن يكون القائد العسكري قد علم او كان يفترض به ان يكون قد علم بسبب الظروف السائدة في ذلك الحين ، بان القوات ترتكب او تكون على وشك ارتكاب هذه الجرائم ولم يتخذ جميع الإجراءات والتدابير اللازمة والمعقولة في حدود سلطته لمنع او قمع ارتكاب هذه الجرائم او لعرض المسألة على السلطات المختصة للتحقيق والمقاضاة [٣٤].

هذه القاعدة تمثل تأكيداً للقانون الدولي الاتفاقي والعرفي بشأن عدم تمكن القادة والرؤساء من الإفلات من المسؤولية الجنائية بحجة عدم قيامهم شخصياً بارتكاب تلك الافعال التي تكون جرائم حرب . فالقادة والأشخاص الارفع مقاماً مسؤولون جزائياً عن الجرائم التي يرتكبها مرؤوسيهم ، في حالة معرفتهم ان مرؤوسيهم كانوا على وشك ارتكاب مثل تلك الأفعال أو كانوا يقومون بارتكابها ، وهذه المسؤولية تقوم على اساس تقصير القادة في اتخاذ تدابير لمنع أو معاقبة مرتكبيها سواء في النزاعات المسلحة الدولية أو غير ذات الطابع الدولي[٣٥] فضلا عن ان هذه القاعدة تفرض المسؤولية الجنائية على أي قائد عسكري أو رئيس مدني، عن اصدار الاوامر لتنفيذ مثل تلك الهجمات على شبكات الحاسوب والمثال على ذلك هو اصدار أمر بشن هذه الهجمات ضد المدنيين الذين لم ينخرطوا بصورة مباشرة في القتال ، كالتلاعب بالمعلومات الطبية لأحد المدنيين والمخزنة في قاعدة البيانات أو اعطاء الاوامر بشن الهجمات على شبكات الحاسوب بصورة عشوائية وغير تمييزية مثال ذلك توظيف البرمجيات الخبيثة كالفايروسات في تلك الهجمات الذي يؤدي الى انتشارها على نحو عشوائي في النظم الالكترونية المدنية ، مما يثير المسؤولية الجنائية بغض النظر عن اشتراك القائد العسكري أو الرئيس المدني أو عدم اشتراكه بصورة شخصية في تنفيذ ذلك الهجوم [٣٦] .
على أن مثل هذه المسؤولية الجنائية تمتد لسلسلة القيادة والسيطرة ، فعلى سبيل المثال فان القائد الادنى درجة الذي يصدر أمراً لقوات تحت إمرته تنفيذاً لأمر صدر اليه من قائده الاعلى لأجل القيام بفعل يشكل جريمة حرب ، أو قيامه بإصدار مثل تلك الأوامر للقيام بهجمات على شبكات الحاسوب ضد نظم الحاسب الآلي الخاص بأعيان مدنية تتمتع بالحماية طبقاً لقواعد القانون الدولي الانساني ، فان هذا القائد يتحمل بالمثل المسؤولية الجنائية لإصداره مثل ذلك الأمر.

فالقادة والأشخاص الآخرون الارفع مقاماً مسؤولون عن جرائم الحرب المرتكبة تبعاً لأوامرهم ، بدليل ما ورد مثلاً في الفقرة الثانية من المادة (٥٠) من اتفاقية جنيف الثانية التي اشارت الى ضرورة اتخاذ أي إجراء تشريعي يلزم لفرض عقوبات جزائية فعالة على الاشخاص الذين يقترفون أو يأمرون باقتراف **الإنتهاكات** الجسيمة لهذه الاتفاقية [٣٧] .

وقد قضت السوابق القضائية الدولية انه في حال عدم وجود علاقة رسمية لرئيس بمرؤوس فأن (اعطاء الامر) يعني ضمناً وعلى الاقل وجود تلك العلاقة كأمر واقع . وفي هذا الصدد يتعين التمييز بين ثلاث حالات فيما يتعلق بالأفعال التي يقوم بها المرؤوسون وفقاً للأوامر بارتكاب جرائم حرب هي : -

أ - في حال ارتكبت جرائم حرب بشكل فعلي ، فالممارسات الدولية واضحة بوجود مسؤولية للقيادة.

ب - في حال لم ترتكب جرائم حرب بشكل فعلي وإنما كانت هناك محاولات لارتكابها فقط فان الممارسات الدولية تشير الى قيام مسؤولية القيادة وهذا ما اشارت إليه المحكمة الجنائية الدولية في نظامها الأساسي من أن مسؤولية القيادة تتحقق عن إعطاء الأوامر بارتكاب جرائم حرب عندما تحدث بشكل فعلي او عندما تجري محاولات لذلك [٣٨] .

ج - في حال لم ترتكب جرائم حرب ولم تجر محاولات لارتكابها ، فان قلة من الدول تنسب مسؤولية جزائية الى القائد لمجرد اعطاء ذلك الامر ، على ان الغالبية لا تشير الى المسؤولية الجزائية للقيادة ، لكن من الواضح من ان وجود قاعدة تتضمن حظراً بإعطاء امر معين ، كحظر الامر بعدم الإبقاء على احياء ، تثير مسؤولية القائد العسكري حتى ولو لم ينفذ الامر[٣٩] .

المطلب الثاني

المسؤولية في حالة العلم اليقيني او التقديري

أشار دليل تالين للحرب السيبرانية الى ان المسؤولية تتحقق اذا كان القادة او الأشخاص الآخرين الارفع مقاماً قد علموا او كان بوسعهم ان يعلموا ان مرؤوسيهم على وشك ان يرتكبوا أو كانوا يقومون بارتكاب مثل هذه الجرائم ولم يتخذوا التدابير اللازمة التي تخولها لهم سلطتهم لمنع ارتكابها او معاقبة مرتكبيها ممن يقعون تحت سلطتهم وسيطرتهم الفعلتين ، سواء كان ذلك في نزاع مسلح دولي او غير دولي .

فالممارسات الدولية تؤكد ان مسؤولية القادة لا تقتصر على الأوضاع التي يكون فيها القائد أو الارفع مقاماً على علم فعلي بالجرائم المرتكبة أو التي على وشك ان ترتكب من قبل مرؤوسيه ، بل أن المعرفة التقديرية كافية لإثارة المسؤولية ويعبر عن ذلك بتعبير (يُفترض أن يعلم) [٤٠] وكذلك تعبير (كانت لديه معلومات تمكنه (القائد أو الارفع مقاماً) من الاستنتاج في تلك الظروف) [٤١] .

أو استخدام عبارة (كان القائد او الارفع مقاماً مسؤولاً عن تقصيره في الحصول على هذه المعلومات) و(كان القائد او الارفع مقاماً متهاوناً جزائياً في عدم معرفته) كل هذه الصيغ تغطي مفهوم المعرفة التقديرية[٤٢].

ويعد هذا التوسع في شأن اثارة المسؤولية الجنائية للقائد العسكري أو الرئيس المدني الذي يعلم وكان يفترض به أن يعلم بتلك الأفعال المكونة بجريمة الحرب تكتسب ذات الأهمية في سياق الهجمات على شبكات الحاسوب[٤٣].

وأشار دليل تالين الى ان تفادي المسؤولية الجنائية من قبل القادة والرؤساء عن الافعال التي يقوم بها من هم تحت امرتهم وسلطتهم الفعلية ، يوجب عليهم اتخاذ الخطوات المناسبة لمعرفة العمليات التي نفذت من قبل وحداتهم من اجل فهم تفاصيل تلك العمليات والعواقب التي يمكن ان تترتب عليها واتخاذ التدابير اللازمة والمعقولة بشأنها .

وقد فسرت المحكمة الجنائية الدولية ليوغسلافيا السابقة في قضية ديلاليتش عام ١٩٩٨ عبارة (التدابير اللازمة والمعقولة) على انها (تقتصر على التدابير الممكنة ضمن سلطة الشخص ، اذ لا يمكن ارغام احد على القيام بما هو مستحيل) . وفيما يتعلق بالتدابير اللازمة والمعقولة لتأمين معاقبة المشتبه بهم كمجرمي حرب، قضت المحكمة في قضية كنوتشكا في العام ٢٠٠١ ، بان " ليس بالضرورة على الارفع مقاماً ان يضع العقوبة موضع التنفيذ ، بل ان يتخذ خطوة هامة في عملية الانضباط " ، وفي حكم لها في قضية Blaskic في العام ٢٠٠٠ ، رأت المحكمة ان (القائد وتحت وطأة ظروف معينة يمكن ان يتحرر من واجبه بمنع او قمع جريمة الحرب وذلك برفعه تقرير بالمسألة الى السلطات المختصة وبخلافه يترتب على القائد مسؤولية التقصير في إجراء التحقيق

ورفع التقارير الى السلطات المختصة لاتخاذ الإجراءات اللازمة لقمع المرؤوسين الذين يرتكبون جرائم الحرب ، وكما اشرنا فان المسؤولية في هذا الصدد تمتد الى كل من القائد العسكري أو الرئيس المدني ومثال ذلك الرئيس المدني في دوائر الامن او الاستخبارات المدنية الذي يتحمل المسؤولية الجنائية عن الهجمات على شبكات الحاسوب التي ترقى الى جرائم حرب في سياق النزاع المسلح الدولي وغير الدولي ، ويتحقق ذلك على الرغم من ان العمليات على شبكات الحاسوب تتميز بالتعقيد التكنلوجي الذي يصعب معه إمكانية علم القادة بتلك الافعال مقارنة بالعمليات العسكرية التقليدية ، الا ان ذلك لا يخفف من مسؤوليتهم في مباشرة السيطرة على فاعليهم ، فالجهل بمثل تلك العمليات لا يعد عذراً ، لأن القانون يفترض في كل قائد عسكري تمتعه بدرجة من العلم الذي يتمتع به الرجل المعتاد بذات المستوى القيادي وفي سياق عمليات مماثلة وبما يعد كافياً لتمكنهم من القيام بواجبهم وعلى نحو معقول لغرض تشخيص أو منع أو ايقاف ارتكاب جرائم الحرب المعلوماتية (السيبرانية) [٤٤].

هذا وأن بعض الكتاب ومنهم Michael N. Schmitt ذهب الى ان النزاع المسلح الذي يشتمل على الهجمات على شبكات الحاسوب يشن عبر الفضاء الافتراضي بعيداً عن الحدود التقليدية ، الا ان الآثار المترتبة على مثل تلك الهجمات على الأشخاص او الاعيان والممتلكات هي التي تفرض الالتزامات وتولد المسؤولية طبقاً لقواعد القانون الدولي الإنساني ، وفي هذا المعنى ذهبت المحكمة الجنائية الدولية ليوغسلافيا السابقة بانه : " ليس بالضرورة وجود ارتباط بين المكان الفعلي لوقوع الاعمال العدائية وبين الوصول الجغرافي لقوانين الحرب، لأن الأخيرة تنطبق على كافة أقاليم الدول المتحاربة في النزاع الدولي ، وعلى الإقليم الذي يخضع لسيطرة طرف في النزاع غير الدولي ، بغض النظر عن وقوع او عدم وقوع الاعمال العدائية فيه ، القانون الدولي الإنساني يستمر بالانطباق على كافة الإقليم حتى تتم التسوية السلمية بين الأطراف لذلك فمن البديهي ان يتم خرق قواعد واعراف الحرب في أجزاء أخرى من الإقليم ذاته وان لم يقع فيها العمل القتالي الفعلي ، لان المطلوب ان تكون الأفعال المنسوبة للمتهم وثيقة الصلة بالنزاع المسلح ، ولن ينفيها كونها بعيدة جغرافياً او زمنياً عن الموقع الفعلي
للقتال ، حيث يكفي مثلاً تحقق الارتباط الوثيق بين الجرائم المرتكبة والاعمال العدائية التي تقع على أجزاء أخرى من الإقليم الواقع تحت سيطرة اطراف النزاع " [٤٥] .

وبناءً على ذلك ، فإن اية دولة او مجموعة مسلحة تجد نفسها منخرطة في نزاع مسلح يشتمل على استخدام الهجمات على شبكات الحاسوب ، فان المطلوب منها الالتزام بتطبيق القانون الدولي الإنساني على كافة إقليم الدولة في النزاع الدولي وعلى كافة الإقليم الخاضع لسيطرة المجموعة المسلحة المنظمة في النزاع غير الدولي طبقاً لوجهة النظر التقليدية ، بما في ذلك البحر الاقليمي والمجال الجوي الذي تقع فيه ذلك النزاع .

الخاتمة

أن احترام مبادئ التميز والتناسب تتطلب ضرورة اتخاذ الاحتياطات اللازمة سواء اثناء الهجوم من قبل من يخطط للهجمات على شبكات الحاسوب أو يتخذ قراراً بشأنها طبقاً للمادة (٥٧) من البروتكول الاضافي الاول أو الاحتياطات ضد آثار تلك الهجمات طبقاً (٥٨) من البروتكول ذاته هذا يعني أن على من يخطط للهجمات على شبكات الحاسوب أن يتخذ جملة من الاحتياطات بشأن الآثار التي يمكن أن تحدثها تلك الهجمات سواء للأشخاص أو الاعيان ، على أن مثل تلك الاحتياطات يكفي أن تكون مستطاعه وعملية للتأكد من أن تلك الاهداف ليست محمية ، وذلك من خلال المسح والفحص الدقيق للنظم الالكترونية المستهدفة وتقيم المعلومات المتوافرة من كافة المصادر المتاحة ومنها فريق خبراء الحاسوب على أن مثل تلك الاحتياطات تمتد الى اختيار وسائل واساليب الهجمات على الحاسوب لأجل تجنب احداث خسائر بين صفوف المدنيين أو الاضرار بالأعيان المدنية مع ضرورة تعليق الهجمات أو الغاءها أذا تبين أن الاهداف لا تعد مشروعة للهجمات وعند خرق الالتزامات المتقدمة ، فأن المسؤولية الجنائية للقادة والرؤساء المدنيين يمكن إثارتها بخصوص الهجمات على شبكات الحاسوب التي ترقى الى مستوى جرائم الحرب جراء مخالفتها للقيود والمبادئ التي اوردها القانون الدولي الانساني ، إلا أنه وعلى الرغم من أن القانون الدولي الإنساني في شكله الحالي يكفي بشكل عام لحماية من يسعى لحمايتهم من آثار الهجمات على شبكات الحاسوب إلا أن هناك أوجه قصور كبيرة ينبغي تلافيها عبر توصيات يمكن أن تأخذ مجالها للتطبيق منها :

١- ينبغي العمل على تحديث قوانين النزاع المسلح بما يراعي الأخطار الجديدة ، لأن الافتقار إلى إطار قانوني يمكن أن يتم تفسيره على أنه يتضمن موافقة قانونية على شن مثل تلك الهجمات .
٢- ينبغي أن يلتزم كل بلد بالتعاون مع غيره من البلدان ضمن إطار دولي للتعاون لضمان السلام في الفضاء الافتراضي المعلوماتي .
٣- ينبغي للحكومات التي تشارك بفاعلية في جهود الأمم المتحدة التي ترمي إلى النهوض بالأمن في الفضاء المعلوماتي وتحقيق السلام .
٤- ينبغي وضع استراتيجية عالمية لتيسير بناء القدرات البحرية والمؤسسية من أجل تعريف الخبرة في مجال الأمن المعلوماتي وادراك المخاطر المحتملة في هذا الفضاء لأجل الاستفادة من تكنولوجيا المعلومات والاتصالات بصورة آمنة .

الهوامش

(1)GA. Res 2675 (XXV) Basic Principles for the protection of civilian population in Armed conflict , UNGAOR , 25th sess. , sup. No. 28 – 76 UNDoc . A/8028 (1971) .

(٢)نصت المادة (٥٧ / ١) من البروتكول الإضافي الأول على ان " تبذل رعاية متواصلة في إدارة العمليات العسكرية ، من اجل تفادي السكان المدنيين والأشخاص والاعيان المدنية " .

انظر ايضاً . ICRC Additional protocols commentary , paras . 2191 , 1875

(٣) انظر المادة (٥٧ / ٢ / أ / اولاً) من البروتكول الإضافي الأول ١٩٧٧ .

(٤) يعرف البروتكول الثاني من الاتفاقية بشأن الأسلحة تقليدية معينة في المادة (٣ / ٤) منه .

وكذلك البروتكول الثالث من الاتفاقية بشأن أسلحة تقليدية معينة في المادة (١ / ٥) منه الاحتياطات المستطاعه بانها :

" تلك الاحتياطات القابلة للاتخاذ او الممكنة عملياً مع مراعاة جميع الظروف القائمة في حينها ، بما في ذلك الاعتبارات الإنسانية والعسكرية " .

(5)ICRC Customary IHL study , commentary accompanying Rule 15 .

(6)Tallinn Manual on international law applicable to cyber warfare , the international group of experts and the invitation of the Nato cooperative cyber defence center of excellence , cambrige university , 2013, Rule 53 (1 – 5) , p138 – 139 .

(٧)نصت المادة (٥١ / ٧) من البروتكول الإضافي الأول الى انه " لا يجوز التوسل بوجود السكان المدنيين او الأشخاص المدنيين او تحركاتهم في حماية نقاط او مناطق معينة ضد العمليات العسكرية ولا سيما في محاولة درء الهجوم عن الأهداف العسكرية او تغطية او تحييد او إعاقة العمليات العسكرية ..... " .

(8) ICTY , Final Report to the prosecutor , para . 29 .

انظر كذلك Heather Harrison ,cyber warfare and the law of war ,cambridge university , 2012, p211 – 212 .

(9)Michael N. Schmitt , Wired warfare , computer network attack and jus in bello , international review of the red cross , p 109 .

انظر كذلك Tallinn Manual ,opcit , Rule 53 (5) , p140 .

(10)Tallinn Manual , Rule 53 (6) , p140 .

(١١)هذا الالتزام يجد أساسه في المادة (٥٧ / ٢ / أ / ثانياً) من البروتكول الإضافي الأول ١٩٧٧ ، والذي تكرسه ممارسة الدول كإحدى قواعد القانون الدولي العرفي المنطبقة في النزاعات المسلحة الدولية وغير الدولية .

انظر ماري هنكرتسولويزدوزوالدبك ، القانون الدولي الإنساني العرفي ، المصدر السابق ، ص ٥٠ – ٥١.

(12)Heather Harrison , op. cit , p213 .

(13)Michael N. Schmitt , Wired warfare , ibid , p110 .

(14)Tallinn Manual , Rule 54 (1 – 6) , and Rule 55 (1 – 3) , p 140 – 141 .

(١٥)انظر المادة (٥٧ / ٢ / ب) من البروتكول الإضافي الأول ١٩٧٧ .

Tallinn Manual , Rule 57 , p143 .

(16)Tallinn Manual , Rule 57 (1 – 8) , p143 – 144 .

(١٧) نصت لائحة لاهاي المتعلقة بقوانين واعراف الحرب البرية ، المادة (٢٦) على انه " يتعين على قائد الوحدات المهاجمة قبل الشروع في القصف ان يبذل قصارى جهده لتحذير السلطات ..... " .

انظر المادة (٥٧ / ٢ / ج) من البروتكول الثاني لاتفاقية لاهاي الخاص بحماية الممتلكات الثقافية في حالة النزاع المسلح ، آذار ١٩٩٩ .

(١٨) انظر ماري هنكرتس و لويزدوزوالديك ، القانون الدولي الإنساني العرفي ، اللجنة الدولية للصليب الاحمر ، القاهرة ، ٢٠٠٧ ، ص٥٨ .

(19)Tallinn Manual , Rule 58 (1 – 8) , p145 .

(20)Tallinn Manual , Rule 58 (8 – 10) , p146 .

(٢١)نصت المادة (٥٧ / ٣) من البروتكول الإضافي الأول الى انه " ينبغي ان يكون الهدف الواجب اختياره حين يكون الخيار ممكناً بين عدة اهداف عسكرية للحصول على ميزة عسكرية مماثلة ، هو ذلك الهدف الذي يتوقع ان يسفر الهجوم عليه عن احداث اقل قدر من الاخطار على أرواح المدنيين والاعيان المدنية " .

(22) ICRC , Additional protocols commentary , paras . 2227 – 2228 .

(23)Michael N. Schmitt , Wired warfare , op.cit , p110 .

(24)Tallinn Manual , Rule 56 (1 – 8) , p142 -143 .

(25)Tallinn Manual , Rule 56 (5) , p142 .

- ICRC Customary IHL study ,op. cit Rule 21 .

(٢٦)نصت المادة (٥٨ / ج) من البروتكول الإضافي الأول الى ان " تقوم اطراف النزاع قدر المستطاع باتخاذ الاحتياطات الأخرى اللازمة لحماية ما تحت سيطرتها من سكان مدنيين وافراد واعيان مدنية من الاخطار الناجمة عن العمليات العسكرية " .

(27)ICRC , Additional protocols commentary , paras , 2257 – 2258 .

انظر ايضاً . ICRC Customary IHL study ,cairo , 2005 , commentary accompanying Rule 22

(28)Tallinn Manual , Rule 59 (1 – 6) , p147 .

(٢٩) ذكر مقرر مجموعة العمل في المؤتمر الدبلوماسي الذي أدى الى اعتماد البروتكولين الاضافيين انه جرى الاتفاق بسرعة بعد ادخال عبارة " الى اقصى حد مستطاع " لتحديد جميع الفقرات الفرعية في المادة (٥٨) وقد عكس هذا التعديل قلق البلدان الصغيرة المكتظة بالسكان والتي يصعب عليها ان تفصل السكان المدنيين والاعيان المدنية عن الأهداف العسكرية وحتى البلدان الكبيرة التي

يصعب عليها القيام بذلك الفصل في حالات كثيرة ، وكما ذكرت النمسا وسويسرا ، عند التصديق على البروتكول الإضافي الأول ، ان هذا الواجب يطبق بحسب متطلبات الدفاع عن الأراضي الوطنية ، انظر :

Diplomatic conference leading to the Adoption of the Additional protocols , Report to committee III on the working Group ICRC Customary IHL study , خحز ؤهف , p63.

- ICRC Additional protocols commentary , para .2245 .

(30)ICRC Additional protocols commentary , para . 2239 .

-Tallinn Manual , Rule 59 (6 – 13) , p148 .

(31)Tallinn Manual , Rule 59 (14) , p149 .

(٣٢) الانتهاكات على نوعين : -

أ - الانتهاكات الجسيمة لقواعد القانون الدولي الانساني والتي تعد من قبل جرائم الحرب تعرف بموجب النظام الأساسي للمحكمة الجنائية الدولية في المادة الثامنة منها بأنها : - " الانتهاكات الخطيرة للقوانين والأعراف السارية على النزاعات الدولية المسلحة " و "الانتهاكات الخطيرة للقوانين والاعراف السارية على النزاعات المسلحة غير ذات الطابع الدولي "

انظر النظام الاساسي للمحكمة الجنائية الدولية ١٩٩٨ ، المادة (٨)

ب - الانتهاكات غير الجسيمة وهي " جميع الافعال المنافية لاتفاقيات جنيف وبروتكولها الأول وتتخذ حيالها تدابير تأديبه من قبل الاطراف المتعاقدة "

انظر المواد (٤٩ - ٥٤) من اتفاقية جنيف الأولى ١٩٤٩ .

انظر المواد (٥٠ - ٥٣) من اتفاقية جنيف الثانية ١٩٤٩ .

انظر المواد (١٢٩ - ١٣٢) من اتفاقية جنيف الثالثة ١٩٤٩ .

انظر المواد (١٤٦ - ١٤٩) من اتفاقية جنيف الرابعة ١٩٤٩ .

(٣٣) انظر المادة (٥٧) من البروتكول الإضافي الأول الملحق باتفاقيات جنيف ١٩٧٧ .

(34)Tallinn Manual , Ch III , Rule 24 , p80 .

(٣٥) رأت المحكمة الجنائية الدولية ليوغسلافيا السابقة أن مبدأ مسؤولية القادة كمبدأ في القانون الدولي العرفي ، ينطبق ايضاً في ما يتعلق بالنزاعات المسلحة غير الدولية وجرى التأكيد عليها في قضايا عديدة رفعت امام المحكمة الجنائية ومنها قضية (Hadzihasanovic) .

- ICTY , Hadzihasanovic and other case , No. IT- 01-47 AR72 , 16 July , 2003 .
- Geneva convention I , art , 49 .
- Geneva convention III ,art . 50 .
- Geneva convention III, art . 129 .
- Additional protocol I, arts . 86 - 87 .

عرف دليل الحرب للولايات المتحدة (US . Army manual) بأن " جريمة الحرب هي أي انتهاك لقانون الحرب من جانب أي شخص أو الاشخاص من العسكريين أو المدنيين " .

Us . Army Manual , 1956 , para 499 .

انظر المادة (٢٨ / ٢) من النظام الاساسي للمحكمة الجنائية الدولية .

(٣٦) انظر المادة ٥٠ من اتفاقية جنيف لتحسين حال الجرحى ومرضى وغرقى القوات المسلحة في البحار .

وبذات المعنى انظر المادة (٤٩) من اتفاقية جنيف الاولى ، المادة (١٢٩) من اتفاقية جنيف الثالثة ، والمادة (١٤٦) من اتفاقية جنيف الرابعة ١٩٤٩ ، والمادة (٢٨) من اتفاقية لاهاي لحماية الممتلكات الثقافية ١٩٥٤ .

(٣٧) انظر النظام الأساسي للمحكمة الجنائية الدولية ،المادة (٢٥ / ٣ / ب) .

(٣٨) انظر النظام الاساسي للمحكمة الجنائية الدولية في المادة (٨ / ٢ / ب / ١٢) .

انظر ايضا: البروتكول الاضافي الأول الملحق باتفاقيات جنيف في المادة (٤٠) .

(٣٩) انظر النظام الأساسي للمحكمة الجنائية الدولية ليوغسلافيا السابقة ، في المادة (٧ / ٣) .
ـ انظر النظام الأساسي للمحكمة الجنائية الدولية لرواندا في المادة (٦ / ٣) .
(٤٠) انظر البروتكول الإضافي الملحق باتفاقيات جنيف في المادة (٨٦ / ٢) والتي تنص على : ـ
(لا يعفى قيام أي مرؤوس بانتهاك الاتفاقيات أو هذا اللحق (البروتكول) رؤساءه من المسؤولية الجنائية او التأديبيه حسب الاحوال ، اذا علموا ، او كانت لديهم معلومات تتيح لهم في تلك الظروف ، أن يخلصوا الى انه كان يرتكب ، أو انه في سبيله لارتكاب مثل هذا الانتهاك ، ولم يتخذوا كل ما في وسعهم من إجراءات مستطاعة لمنع أو قمع هذا الانتهاك) .
(٤١) بالنسبة لمن هم ارفع مقاماً من غير القادة العسكريين ، يستخدم النظام الأساسي للمحكمة الدولية صيغة (اذا الرئيس تجاهل عن وعي أي معلومات تبين بوضوح) وقد استخدم هذا المعيار من قبل المحكمة الجنائية الدولية لرواندا في قضية كايشيما عام ١٩٩٩ لوصف معنى عبارة (يفترض أن يكون قد علم بالنسبة للقادة من غير العسكريين .
انظر النظام الأساسي للمحكمة الجنائية الدولية من المادة (٢٨ / ب / ١) .
انظر كذلك . ICTR , Kayishema and Ruzindana case , 1999 , para 703

(42)Tallinn Manual , ch III , Rule 24 , para . 7 - 8 .
(43) -Tallinn Manual , ch III , Rule 24 , para 8 - 8 .
ICTY , Delalic case , 1998 , para . 707 .
ICTY , Kvoka case , 2001 , para . 714 .
ICTY , Blaskic case , 2000 , para . 757 .
د. صلاح الدين عامر ، تطور مفهوم جرائم حرب ، بحث منشور ضمن مجموعة بحوث في (المحكمة الجنائية الدولية المواءمات الدستورية والتشريعية ، اعداد شريف عتلم ، اللجنة الدولية للصليب الاحمر ، القاهرة ، ٢٠٠٦ ، ص ١٠٤ ـ ١٤٧ .
(44)ICTY , prosecutor vs. DragoliubKunarac et al. 2002 , case no IT -96 -23 and 23/1 , para 57 .
تنص المادة (٤٩ / ٢) من البروتكول الإضافي الأول الملحق باتفاقيات جنيف لعام ١٩٧٧ ذلك بالاتي : ـ
" تنطبق احكام هذا اللحق (البروتكول) المتعلقة بالهجمات على كافة الهجمات في أي إقليم تشن منه بما في ذلك الإقليم الوطني لاحد اطراف النزاع والواقع تحت سيطرة الخصم " .