Proceedings of the Bruges Colloquium

Technological Challenges for the Humanitarian Legal Framework

11th Bruges Colloquium
21-22 October 2010

Actes du Colloque de Bruges

Les défis technologiques posés au cadre juridique humanitaire

11ème Colloque de Bruges
21-22 octobre 2010

Brugge
College of Europe
Collège d'Europe
Natolin

COMITE INTERNATIONAL GENEVE
CICR

Notice

The proceedings of this Colloquium have been written by the speakers or by the Delegation of the International Committee of the Red Cross (ICRC) in Brussels on the basis of audio recordings of the Colloquium. These texts were then reviewed by the speakers. The opinions expressed herein are not necessarily those of College of Europe nor the International Committee of the Red Cross.

Avertissement

Les Actes de ce Colloque ont été rédigés par les orateurs ou par la Délégation du Comité international de la Croix-Rouge (CICR) à Bruxelles sur base d'enregistrements audio du Colloque. Ces textes ont alors été revus par les orateurs et n'engagent que ces derniers. Tous droits réservés. Ils ne représentent pas nécessairement les vues ni du Collège d'Europe ni du Comité international de la Croix-Rouge.

Session 3
Remote-Controlled and Autonomous Weapons Systems

Chair person: **Stéphane Kolanowski**, *ICRC Brussels*

Session 4
Outer space – a new conflict theatre?

Chair person: **Marco Sassoli**, *University of Geneva*

Panel Discussion
How will technological development challenge IHL in the 21st century?

Chair person: **Eric David**, *Université Libre de Bruxelles*

Concluding Remarks and Closure

PROCEEDINGS OF THE BRUGES COLLOQUIUM
ACTES DU COLLOQUE DE BRUGES

Opening remarks

REMARQUES DE BIENVENUE

François Bellon
Chef de la délégation du CICR auprès du Royaume de Belgique, de l'Union européenne et de l'OTAN

Mesdames et Messieurs,

J'ai l'honneur et le plaisir, au nom du Comité international de la Croix-Rouge (CICR), de vous accueillir pour ce 11ème Colloque de Bruges, qui sera consacré à l'étude des défis que posent les avancées technologiques au cadre juridique humanitaire.

La collaboration qui s'est établie entre le Collège d'Europe et le CICR a déjà mené à de nombreux colloques de Bruges qui ont traité de sujets essentiels et d'actualité. Vous en avez la liste dans votre dossier de documentation. Le sujet qui nous occupera ces deux jours ne fait pas exception, preuve en est l'importance qu'y accorde un grand nombre d'analystes.

Le Colloque de Bruges est devenu, en un peu plus de dix ans, un événement annuel incontournable dans le domaine de la réflexion et la recherche en droit international humanitaire, et je m'en réjouis. Il est en effet très important de pouvoir discuter à un haut niveau d'expertise de sujets liés au droit international humanitaire qui est un droit vivant, en constante évolution et dont l'interprétation doit être adaptée à la réalité des conflits et des développements du monde moderne.

Alors que nous allons commencer nos travaux qui nous amèneront à discuter de «technologies», il ne faut pas perdre de vue que le cadre dans lequel ces technologies sont appelées à être utilisées est celui des conflits armés qui s'accompagnent de nombre de souffrances humaines. Il est essentiel de garder à l'esprit le but ultime du droit international humanitaire qui est de conserver un peu d'humanité dans ces conflits armés.

Ce Colloque de Bruges nous permettra d'examiner les nouvelles technologies présentes sur le champ de bataille et les défis qu'elles posent quant à la réglementation des méthodes et des moyens de combats. Nous aborderons ensuite le très vaste et difficile domaine de la guerre cybernétique. L'utilisation de l'espace cybernétique à des fins hostiles offre en effet un immense potentiel de nuisance dont il est difficile d'imaginer, aujourd'hui, tous les contours. Les armes télécommandées et automatiques seront ensuite abordées avant d'explorer dans quelle mesure l'espace extra-atmosphérique pourrait devenir un théâtre de conflit armé. Enfin nous conclurons ce Colloque par une table ronde dont le but sera de discuter de la manière dont ces nouvelles technologies vont défier le DIH dans les décennies à venir.

Les nouvelles technologies posent très certainement un bon nombre de défis que nous examinerons pendant ces deux jours, défis qui ne sont pas théoriques. On se souviendra, par exemple, du vol Iran Air 655 abattu par erreur le 3 juillet 1988. Alors que le système automatisé d'un navire de guerre croisant dans le Golf persique l'avait pris pour un chasseur F-14, le militaire responsable du système de détection a eu un doute sur la nature militaire de l'avion détecté, mais a malheureusement fait une confiance aveugle au système informatisé plutôt qu'à son jugement. 290 personnes ont péri dans cet incident.

Il faut souligner que le recours aux nouvelles technologies s'inscrit dans un cadre juridique existant. En effet, des règles plus ou moins précises ou laissant place à une interprétation évolutive sont contenues dans les instruments du DIH actuels.
Ainsi, par exemple, en ce qui concerne les armes nouvelles, le droit international humanitaire contient une clause intéressante qui exige que dans la mise au point, le développement ou l'acquisition d'armes nouvelles, les Etats s'assurent que leur emploi ne serait pas interdit dans certaines circonstances, ou en toutes circonstances. Il s'agit de l'article 36 du Protocole I de 1977 qui a, d'ailleurs, été examiné lors du 8ème Colloque de Bruges en 2007, dont vous trouverez les actes sur la table de documentation.

Par ailleurs, étant conscients de l'imprédictibilité des avancées de la science et de la technologie, des juristes spécialisés en droit international humanitaire ont élaboré une clause permettant d'anticiper ces développements tout en conservant un minimum de protection pour ces victimes. En effet, il y a déjà plus de cent ans, plus précisément en 1899, le Professeur Frédéric de Martens, délégué russe à la conférence de la paix à La Haye, a proposé une clause, aujourd'hui connue sous le nom de «clause de Martens» qui s'énonce comme suit: «En attendant qu'un code plus complet des lois de la guerre puisse être édicté, les Hautes Parties contractantes jugent opportun de constater que, dans les cas non compris dans les dispositions réglementaires adoptées par elles, les populations et les belligérants restent sous la sauvegarde et sous l'empire des principes du droit des gens, tels qu'ils résultent des usages établis entre nations civilisées, des lois de l'humanité et des exigences de la conscience publique». Cette clause est aujourd'hui reprise à l'article 1 du 1er Protocole additionnel aux Conventions de Genève.

Enfin, il est certain que toutes technologies, anciennes et nouvelles, doivent respecter les règles et principes établis du DIH tels que la distinction entre les combattants et les non-combattants ainsi qu'entre les objectifs militaires et ce qui n'en est pas. De même, les principes de proportionnalité et de précaution dans l'attaque s'imposent bien entendu sur le champ de bataille. Il n'est cependant pas toujours aisé d'appliquer ces principes à des technologies qui ne sont pas tout à fait maîtrisées ou dont les effets ne sont pas encore tout à fait connus.

Le CICR se doit de se poser régulièrement la question de l'adéquation et la pertinence du droit international humanitaire dans des contextes sans cesse changeants. C'est ce que le CICR a fait en 1864 avec l'élaboration de la première Convention de Genève et ensuite en 1899, en 1929 en 1949, en 1977 et c'est ce que nous faisons toujours aujourd'hui, aussi bien par le biais de réflexions internes que par des consultations avec des Etats, des acteurs non-étatiques ou encore des organisations régionales et internationales. En raison de son mandat, le CICR a toujours pris l'initiative de travailler au développement du droit international humanitaire, lorsque les conséquences des conflits armés le requéraient.

Ainsi, dans sa stratégie 2011-2014 le CICR réaffirme son rôle de catalyseur de la réflexion sur la clarification et le développement du droit international humanitaire. Il se doit de demeurer l'organisation de référence à cet égard, et de guider et d'encadrer le débat sur ces questions juridiques.

Aujourd'hui, nous sommes convaincus que le droit international humanitaire reste, dans son ensemble, tout à fait pertinent. Certaines notions méritent cependant d'être clarifiées voire, peut-être, développées. Dans le cadre d'une étude que le CICR a menée à l'interne depuis un peu plus de deux ans, nous avons identifié quatre domaines dans lesquels le DIH mériterait, éventuellement, d'être quelque peu développé. Ces domaines sont la protection des personnes privées de liberté, la mise en œuvre du droit international humanitaire et les réparations pour les victimes des conflits armés, la protection de l'environnement naturel ainsi que la protection des personnes déplacées. Nos réflexions internes seront tout prochainement présentées à un certains nombres d'États afin de recueillir leurs commentaires et avis et définir ainsi la suite éventuelle à donner à cette étude.

Les nouvelles technologies ne rentrent pas dans ces quatre domaines qui méritent une réflexion sur un éventuel développement du droit, du moins pas à ce stade.
Les nouvelles technologies s'intègrent peut-être sans grande difficulté dans l'ordre juridique actuel. Peut-être faudra-t-il cependant clarifier certains aspects du DIH? Peut-être certaines technologies exigeront que la Communauté internationale adopte de nouvelles conventions réglementant leur usage? Cela reste encore à explorer.

Si le CICR a décidé d'organiser un colloque sur ces thèmes particuliers, c'est parce que nous n'avons pas toutes les réponses aux questions que posent ces nouvelles technologies. Les nombreux experts que nous avons réunis sauront sans aucun doute nous éclairer et le CICR est impatient de vous écouter et de pouvoir échanger, avec vous, points de vue et idées sur cette problématique importante. C'est là tout l'intérêt de ce Colloque.

Je ne saurais terminer sans remercier les participants d'avoir été si nombreux à répondre favorablement à notre invitation à participer à ce 11ème Colloque de Bruges.

Mesdames et Messieurs,

Je me réjouis d'avance des débats que nous allons avoir pendant ces deux jours qui s'annoncent très stimulants et je vous remercie de votre attention.

KEYNOTE ADDRESS

Ms Christine Beerli
Vice-President, ICRC

Mesdames et Messieurs,

De tout temps, les nouvelles technologies ont révolutionné la manière de faire la guerre. Ces changements ont été parfois brusques, parfois graduels. Il suffit de penser à l'invention du chariot, de la poudre à canon, de l'aéronef, du radar ou encore de la fission nucléaire pour se rendre compte à quel point certaines inventions technologiques ont pu modifier le paysage des conflits armés. Il va de soi que tout effort sérieux d'alléger les souffrances causées par les conflits armés doit prendre en compte cette évolution constante. Les premiers rédacteurs du cadre juridique humanitaire ont, avec sagesse, donné à ce cadre une certaine flexibilité qui lui permet de s'adapter aux développements technologiques, y compris ceux que l'on ne pouvait, à l'époque, encore prévoir. De toute évidence, l'émergence de nouvelles technologies n'a rien d'inhabituel pour le droit international humanitaire, mais ces technologies apportent, cependant, toujours de nouveaux défis.

Although there can be no doubt that international humanitarian law (IHL) applies to novel weaponry and new developments, subsuming a new technology under pre-existing rules naturally raises the question whether this is sufficient in terms of legal clarity, in view of the new technology's specific characteristics and – above all – with regard to the humanitarian impact such technology may have. This year's colloquium will allow us to take a closer look and to discuss an array of new technologies that have only recently entered the battlefield or that are now being tested with a view to be used for military purposes in the course of an armed conflict.

The interest in legal issues raised by what is now often called 'cyber warfare' is currently particularly high and still increasing. The military potential of cyberspace is only starting to be fully explored. But cyber attacks of the recent past have already shown that cyberspace is becoming a new war fighting domain. States all over the world are taking the potential threats posed by cyber attacks very seriously. Clearly, cyber warfare is no longer perceived as science fiction but as a reality that needs to be dealt with. Naturally, a humanitarian organisation like the International Committee of the Red Cross (ICRC) must closely follow these developments and carefully assess their humanitarian impact.

Potentially, the humanitarian impact of cyber warfare could be enormous. Although the cyber attacks for example against Estonia in 2007 and Georgia in 2008, as well as most recently the so-called "Stuxnet" attacks against Iran, did not cause grave humanitarian consequences, cyber attacks against airport control and other transportation systems, dams or nuclear power plants, appear to be technically possible. Such attacks would most likely have large-scale humanitarian consequences. They could result in significant civilian casualties and damages. Of course, for the time being it is difficult to assess how likely cyber attacks of such gravity really are. We may hope that they never occur, but we should also prepare for the worst. Many technical experts at least, seem to be of the opinion that it is only a question of time until such cyber attacks occur.

It is for this reason that the ICRC currently devotes specific attention to the application of humanitarian rules in the context of cyber warfare. Notably, as early as in 2001, the ICRC published a paper on computer network attacks and their regulation by IHL on the ICRC webpage. Henceforth, the topic has gained more and more momentum. In the beginning of this year, the ICRC participated in a panel discussion devoted to cyber warfare during the annual meeting of the American Society of International Law in Washington. The panel discussion confirmed that a lot of questions still demand further research before conclusive answers can be given. But it also confirmed that there can be no doubt that fundamental humanitarian rules and principles apply to cyber operations. There is no legal vacuum in cyberspace.

Certainly, however, there is a need for further clarification of how established humanitarian rules apply and function in the cyber context. Against this background, the ICRC now actively participates in an expert process – sponsored by NATO's Cooperative Cyber Defence Centre of Excellence in Estonia – which aims to clarify the humanitarian legal rules applicable in the context of cyber warfare.

Another technological development that is currently of central interest are remote-controlled weapon systems, most importantly drones. Each new technology, from the bow and arrow via gunpowder to the bomber plane has moved soldiers farther and farther away from their enemies and the actual combat zone. In this sense, remote-controlled drones do not amount to an entirely new development. Rather, they form part of a continuous development of warfare technology.

Nevertheless, the issue is complex. On the one hand, advanced military technology can help belligerents to further minimize civilian casualties and damages; but on the other hand it may expand attack possibilities and put the civilian population at risk.

Remote-controlled drones are a conspicuous example in point. They have greatly enhanced aerial surveillance possibilities thereby enlarging the toolbox of precautionary measures that may be taken in advance of an attack. But remote-controlled weapon systems also involve great risks. First of all, various studies have shown how disconnecting a person, especially via distance (be it physical or emotional) makes killing easier and abuses and atrocities more likely. The military historian John Keegan has called this the "impersonalisation of battle"; Special Rapporteur Philip Alston – somewhat more bluntly and specifically with regard to the use of drones – spoke of a "play-station mentality".

Secondly, a particular concern of the ICRC is that remote-controlled drones have significantly increased the possibilities to carry out attacks. This entails the risk, that IHL's geographical scope of application is ever more expanded in the attempt to justify drone attacks, especially so-called targeted killings, in various corners of the world. In this context it must be borne in mind that IHL was specifically designed to regulate military violence and to mitigate the effects of armed conflict. Hence it must only be applied in places where an armed conflict exists.

As technological development continues, there may eventually also be shift from remote-controlled weapons systems towards more or even fully automated/autonomous weapons systems, i.e., robots. In fact, this development is also already upon us. Military robots have reportedly been deployed for example in Iraq and Afghanistan. Evidently, weapon systems without a man in the 'loop' raise a panoply of difficult moral and ethical questions. Undoubtedly, they will pose new challenges to the humanitarian legal framework.

Again there will be opportunities as well as risks. As political thinker Francis Fukuyama has pointed out, "science cannot by itself establish the ends to which it is put". In theory, a robot could be programmed to behave far more cautiously on the battlefield than a human being. After all, self-preservation is not an issue for a robot. At the same time, difficult legal questions abound. For example, how could it be ensured that an automated weapons system distinguishes between combatants and civilians? How could it be guaranteed that it conducts a correct proportionality assessment or that it takes into consideration that the value of a robot never weighs up to a human life? How well could a robot adapt to changing circumstances, e.g., when a combatant is rendered hors de combat? And what if it is simply not technically possible to reliably program an autonomous weapon system so as to ensure that it functions in accordance with IHL under battlefield conditions?

Evidently, it will take some time before conclusive answers can be given to these questions. For the ICRC, it is important to promote the discussion of these issues, to raise attention to the necessity to assess the humanitarian impact of this developing technology and above all to ensure that it is not prematurely employed under conditions where respect for IHL cannot be guaranteed.

As far as outer space technology is concerned, it must first of all be observed that there is currently very little discussion about the application of IHL in this context. This, of course, is first of all due to the fact that thus far no significant hostilities have been conducted in outer space. Certainly, the ICRC shares the hope that outer space will be used for no other than peaceful purposes. But it is indisputable that satellites are used for an ever increasing array of military purposes. In order to be prepared, we should start thinking about the humanitarian impact hostilities in outer space could have. Hopefully, this scenario remains hypothetical and our discussions will have been in vain – but if not, we will be prepared and we will have a better understanding of how to limit the humanitarian impact, should outer-space become a war fighting domain.

Mesdames et Messieurs,

Comme l'a dit Isaac Asimov, "la science acquiert des connaissances plus rapidement que la société n'acquiert de la sagesse". De la même manière, il est parfois dit que le droit international humanitaire (DIH) a une guerre de retard. En effet, il est difficile de réglementer l'usage de nouvelles technologies avant même que celles-ci ne soient utilisées. Les armes à laser aveuglantes sont un des rares exemples où cela a été possible.

Cependant, nous devons sans cesse nous efforcer de clarifier et de préciser l'application des règles de DIH pour nous assurer qu'elles correspondent aux nouveaux défis posés par les progrès technologiques. Il nous faut pouvoir discuter de certaines évolutions technologiques avant que leurs effets, potentiellement dramatiques, ne se fassent sentir. Les technologies dont nous allons discuter pendant ces deux jours de colloque sont celles qui vont modeler le paysage des conflits armés pour les décennies à venir.

Le Comité international de la Croix-Rouge suit l'impact que ces avancées technologiques ont sur les victimes des conflits armés et sur l'application du DIH. Il est également essentiel qu'un maximum d'acteurs soit impliqué dans ces discussions qui doivent être globales et universelles. Le Colloque de Bruges de cette année marque une étape importante dans cette direction et je tiens à vous remercier pour votre présence et votre intérêt pour ce Colloque qui sera, sans aucun doute, passionnant.

Session 1
New Technology on the Battlefield

Chair person: **Marten Zwanenburg,** *Ministry of Defence The Netherlands*

CURRENT CHALLENGES TO THE LEGAL REGULATION OF MEANS OF WARFARE

Jann K. Kleffner
Swedish National Defence College

Résumé

1. Introduction

Tout d'abord, il convient de noter que dans le cadre cette présentation, les termes « moyens de guerre » doivent être compris comme « armes » au sens large du terme, incluant les systèmes et plateformes d'armes, les projectiles et le matériel de guerre. D'autre part, la présente contribution complète celle de M. Boutruche sur les méthodes de guerre, et se propose d'adresser un certain nombre de défis relatifs aux moyens de guerre utilisant les nouvelles technologies en général, et non à un type d'armes en particulier.

2. Le défi conceptuel: qu'est-ce qu'un « moyen de guerre »?

Le droit des conflits armés ne prévoit pas de définition d'un « moyen de guerre », ni d'une « arme ». Or, l'émergence de nouvelles technologies pose un véritable défi en la matière, en particulier dans le cadre d'attaques contre les réseaux informatiques. Certains suggèrent de prendre la notion d'attaque comme point de départ: les moyens de guerre sont alors les instruments utilisés pour conduire une attaque. Reste à s'accorder sur ce qu'est une « attaque ». La neutralisation d'un objet constitue-t-il une attaque? Cette question se pose de manière générale à l'égard des armes non-létales et moins-létales. En effet, certaines armes emploient des mécanismes qui ne causent pas forcément la mort des victimes, ni même des blessures. Est-ce pour cette raison qu'elles ne doivent pas être considérées comme des « moyens de guerre » au regard du DIH? Si de telles armes ne sont pas des « moyens de guerre », cela implique qu'elles ne causent pas de "violence" et ne constituent donc pas une attaque au sens du DIH. En conséquence, l'interdiction d'attaquer directement les civils ne s'applique pas. Ainsi, il semble qu'une approche trop restrictive des « moyens de guerre » pourrait affaiblir certains préceptes fondamentaux du DIH. En revanche, il est bien entendu qu'une approche trop extensive ne serait ni satisfaisante, ni réaliste.

Le défi normatif: les règles de DIH relatives aux effets des armes qui ne se matérialisent qu'au bout d'un laps de temps prolongé

3. Le débat se concentre ici sur deux points.

Le premier est relatif aux effets de certaines armes. Quels effets ou types d'effet doivent être pris en compte dans l'application du DIH? Est-ce l'effet immédiat, celui qui a été souhaité? Ou bien aussi les effets non intentionnels? La réponse à cette interrogation permettra de clarifier plusieurs éléments. Par exemple, concernant l'interdiction d'attaques indiscriminées, certains moyens de combats ne permettent tout simplement pas d'en limiter les effets. Il est donc primordial d'évaluer le degré de contrôle et de « contrôlabilité » des effets des nouvelles armes. Eu égard au principe de proportionnalité, c'est la nature du dommage collatéral à mesurer avant toute attaque, qui permettra ensuite d'établir les mesures de précaution à prendre pour protéger les populations civiles. Enfin, concernant l'interdiction de causer des maux superflus et des souffrances inutiles, la réponse à la question de départ déterminera ce que sont juridiquement un « mal » et une « souffrance ».

*Le second point concerne le degré de certitude scientifique requis eu égard aux effets d'une arme. La règle n° 44 de l'étude sur le droit coutumier dispose, au sujet de l'environnement naturel, que «*l'absence de certitude scientifique quant aux effets sur l'environnement de certaines opérations militaires n'exonère pas une partie au conflit de son devoir de prendre de telles précautions *». Ainsi, il est essentiel de définir le concept de « certitude scientifique ». S'il est clair que les États ne peuvent pas connaître ce qui est inconnu, ils ne peuvent pas ignorer les risques potentiels d'un moyen de guerre donné.*

4. Le défi du désengagement moral

Les moyens de guerre tels que les armes moins létales, les armes automatiques ou contrôlées à distance, et les attaques contre les réseaux informatiques ont en commun une chose: elles donnent l'impression à celui qui les utilise que la violence qu'il inflige est moins directe, moins grave. Les conséquences peuvent être moins visibles et paraissent moins réelles, moins tangibles. Dans le cas d'armes automatiques par exemple, celui qui contrôle l'arme est souvent physiquement très loin du champ de bataille. Indépendamment de l'exactitude de cette perception, le défi majeur pour le DIH est la tendance des belligérants à utiliser très facilement ces armes. Puisque leur utilisation semble plus propre et plus acceptable, le seuil fixé pour utiliser ces armes est très souvent plus bas que pour des armes létales ordinaires.

1. Introduction

The present paper addresses current challenges to the legal regulation of means of warfare. In accordance with the general view in doctrine and practice, I will understand the terms 'means of warfare' to mean 'weapons' in the widest sense of the word, including weapons systems and platforms, projectiles and materials. Several other papers presented during this colloquium touch upon 'means of warfare' and address specific weapons and weapons systems. I have therefore taken my task to be to address a selected number of challenges that have given rise to debate and have the potential to affect our way of thinking about the legal regulation of weapons more generally. In order to avoid too much overlap, I will try to stay away as much as possible from those weapons and weapons systems that will be addressed in more detail over the course of this colloquium.

A second delineation of the present paper is *vis-à-vis* Théo Boutruche's paper on 'methods of warfare', that is to say, on the way in which weapons are being used. Clearly, the distinction between 'means' and 'methods' is somewhat ideal-typical. The advent of remotely-controlled and autonomous weapons systems – 'means of warfare' in the sense of the law of armed conflict,– is, for instance, part and parcel of the evolution of methods such as zero-casualty and 'long-distance warfare'. This is but one example that readily demonstrates that at least certain weapons and weapons systems are so intrinsically linked to specific methods that a separation between these two dimensions of conducting hostilities becomes at times somewhat artificial. Notwithstanding this, an attempt is made to limit the present paper as much as possible to a discussion of 'means of warfare' and the challenges that we are facing in their legal regulation.

More specifically, I will address the following challenges:

First, the conceptual challenge of what is meant by 'means of warfare' or 'weapons' in the broadest sense. Indeed, to clarify that notion is vital in determining the regulatory ambit of the law of armed conflict as it relates to 'means of warfare'.

Secondly, I will address a normative challenge, namely the regulation in the law of armed conflict of effects of weapons that may only materialise after a considerable lapse of time.

Thirdly, I will address the challenge to legal regulation that emanates from processes of moral disengagement induced by an increasing number of new technologies.

Two more brief introductory clarifications: first, I would like to clarify that I obviously do not think that these challenges are the only ones, but the time allotted to me and the other issues addressed during the colloquium have led me to the present selection. Secondly, the fact that

I limit myself to addressing 'challenges' should not be misunderstood to suggest that there are not also positive sides to developments in weapons technology from a law of armed conflict perspective. I would submit that improvements in the accuracy of missiles, for instance, and developments in the realm of non-lethal weapons are but two examples of developments that open new ways for parties to an armed conflict to better comply with their legal obligations in the realm of distinction and the prohibition of superfluous injury and unnecessary suffering. As lawyers, and particularly as academics, we have a certain tendency to focus on the problems rather than the solutions, but this analytical bias is not always entirely justified.

With these introductory remarks, let me now turn without further ado to the first of the challenges that I will be addressing.

2. The conceptual challenge: what are 'means of warfare' – what are 'weapons'?

As far as that challenge is concerned, the law of armed conflict does not provide a definition of what a 'means of warfare' or a 'weapon' is, in either treaty or custom. The recent Air and Missile Warfare Manual[1] suggests that 'means of warfare' are 'objects used to conduct attacks. They are the instruments used to cause, in the course of an armed conflict, (i) the death of, or injury to, individuals; or (ii) damage to, or destruction of, objects.' This definition takes the notion of 'attacks' as a starting point, defined in the Additional Protocol I (AP I) as 'acts of violence against the adversary, whether in offence or in defence'. 'Violence' in turn is equated with what results in death, injury, damage or destruction. Others have argued that the references in the definition of a military objective to neutralisation of an object as a possible result of an attack, suggests that it is not necessarily required that a given cause of action, or an instrument employed, causes death, injury, damage or destruction. Rather, the mere disabling of an object should be qualified as an attack as well and the instrument employed to achieve that disabling should also qualify as a 'means of warfare' and hence a weapon in the broad sense.

The debate between these two alternative approaches has primarily been conducted in the context of computer network operations. The debate amply illustrates a challenge that arises in the context of regulating new technologies, especially non-kinetic ones that do not necessarily inflict 'classical' types of injury, death and destruction that have dominated much of the warfare in the past. However, I submit that that challenge is not limited to computer network operations. Indeed, it reveals a problem that is highly significant in the context of 'means of warfare' more broadly and here in particular *vis-à-vis* what are referred to as 'non-lethal weapons' or, as some would prefer, 'less-lethal weapons'. Some of those 'weapons'

[1] Published by HPCR, May 2009.

employ mechanisms that do not necessarily cause death or injury, such as sticky foam, stink and sound bombs, for example. To the extent that they do cause death or injury, are they to be considered 'means of warfare' at all in the sense of the law of armed conflict? In answering that question, we should be careful what we wish for and be aware of the consequences of making the case for one position or the other: arguing that these mechanisms and instruments are not weapons would mean that their employment would not amount to 'violence' and hence not constitute an 'attack' in the meaning of the law of armed conflict. The consequential prohibitions of directly attacking civilians would not be triggered. Likewise, the generic prohibitions of employing *means* of warfare that cause superfluous injury or unnecessary suffering and of those causing widespread, long-term and severe damage to the natural environment would not apply, because such less-lethal instruments are not 'means of warfare'. The potential consequence of such a restrictive approach to what constitutes 'means of warfare' is that it erodes some of the fundamental precepts of the law of armed conflict.

On the other hand, it may not be convincing to qualify every mechanism that causes some form of inconvenience as a weapon. For one, States do not seem to be prepared to accept an overly expansive notion, which would bring too many things and matters that are part and parcel of military operations into the regulatory ambit of the law on weaponry.

I do not purport to make the case for one position or another here. Rather, my intention is merely to point to the fact that certain new technologies pose challenges to the regulation of means of warfare by raising the very basic question what a 'means' actually is and what should be regarded as one.

Let me then turn to a second challenge.

3. Regulation by the law of armed conflict of effects of weapons that may only materialise after a considerable lapse of time

This question is certainly not one that is limited to 'new technologies' or new weapons. Comparatively old weapons, such as nuclear weapons, raise identical issues. Indeed, the normative standards most at play when considering the effects of weapons – the principles of distinction, proportionality and precaution, the prohibition of superfluous injury and unnecessary suffering, as well as the rules protecting the natural environment – have long been part of conventional, and also to a large extent, of customary international law. However, relatively recent debates, in particular those surrounding cluster munitions, explosive remnants of war, and also depleted uranium ammunitions, have given new impetus for revisiting that question. The debate here essentially centers around the following two issues.

First, which effects enter the legal equations? Only the primary, perhaps even only the intended effects, or are the secondary, unintended effects equally relevant?
An answer to that question is relevant with respect to several rules of the law of armed conflict. As regards the prohibition of indiscriminate attacks in the form of attacks which employ a means of combat, the effects of which cannot be limited as required by the law of armed conflict, the answer determines the required *standard of control and controllability* of the effects of weapons. As regards the principle of proportionality, the answer determines what amounts to collateral damage, which has to be measured against the direct military advantage anticipated from an attack. The answer also naturally determines what precautionary measures need to be taken to spare the civilian population and to avoid, and in any event to minimise, collateral damage. Last but not least, as regards the prohibition of superfluous injury and unnecessary suffering, the answer determines what amounts to 'injury' and 'suffering' – is it only that caused by the weapon directly, or are more long-term consequences of having been targeted with, or otherwise exposed to, a weapon, also included?

Second, the debate is about the level of scientific certainty required as to the effects of a given weapon. Rule 44, 3rd sentence of the ICRC Customary Law Study posits, for instance, that 'lack of scientific certainty as to the effects on the environment of certain military operations does not absolve a party to the conflict from taking [all feasible precautions].' The Rule imports the precautionary principle, well established in international environmental law, into the corpus of the law of armed conflict. I will leave aside for the purpose of this presentation the question of whether and to what extent the Study is correct in asserting that such a rule has attained customary status and will just recall that Rule 44, 3rd sentence, is amongst the more contested ones. However, assuming for the purposes of my presentation that a customary rule to that effect has indeed evolved, it is vital to determine more precisely the contours of what is meant by 'scientific certainty'. In fact, to clarify the notion is not only relevant in the specific context of Rule 44, but also raises the broader point as to what the requirements are to conduct weapons reviews under Article 36 of AP I with a view to ensure that means of warfare comply with the law of armed conflict. Clearly, the long-term effects of weapons are not easily determined, nor are secondary 'knock-on' effects. The debate surrounding depleted uranium ammunition readily comes to mind here. Evidently, States cannot be expected to know the unknown. At the same time, they cannot simply ignore potential risks that a given means of warfare may entail. The question hence is what they have to do in order to satisfy the precautionary standards in the law, such as those suggested by Rule 44, 3rd sentence.

4. The challenge of moral disengagement

The third challenge is perhaps the most fundamental of the challenges that I am addressing. When we consider the developments in weapons technologies, a certain trend is identifiable that is conducive to weapons operators and decision-makers to morally disengage from the actual employment of weapons and the consequences of such weapons. Means of warfare such as less-lethal, automated and remotely-controlled weapons, precision ammunition, as well as cyber network operations have the following in common: they create the perception in those who inflict the death, injury or destruction by operating such weapons and weapons systems that the violence that is being inflicted is less severe or direct, or at least less visible and real, than aiming an assault rifle at an adversary, pulling the trigger and seeing the person go down in front of one's eyes, for instance. In the case of less-lethal weapons, that perception is created by the very notion that they incapacitate or repel personnel with a low probability of fatality or permanent injury, or disable equipment with minimal undesired damage or impact on the environment. In the case of automated and remotely-controlled weapons, the human operator is often far removed from the actual battlefield. As far as precision ammunition is concerned, the suggested accuracy of such weapons is conducive to the perception that unintended consequences, and in particular incidental loss of life of, or injury to civilians and damage to civilian objects are being minimised. In the context of cyber network operations, the causal remoteness between implanting malicious code and the actual materialisation of death, injury or destruction is such that those developing and implanting the code are oftentimes not confronted with the consequences of their actions in a direct and tangible way.

Irrespective of the accuracy or otherwise of these perceptions, the main challenge that they create for the law of armed conflict is that they have a tendency of lowering the threshold for using such weapons and weapons systems. The perceptions make their use more acceptable. Weapons operators may be more readily inclined to use less-lethal weapons than 'ordinarily' lethal weapons in the expectation that the injury and damage will be less. Likewise, they may be more readily prepared to launch a precision-guided missile than an ordinary 'dumb' bomb. It is very plausible that the legal requirements such as the obligation to do everything feasible to verify that targets are military objectives will in turn be interpreted more loosely when employing less-lethal weapons or precision-guided ammunition, with the consequential risk of erroneous targeting decisions. In a similar vein, the use of automated and remotely-controlled weapons takes place in a semi-virtual world whose visualisation for the operators resemble more computer games than actual real-life combat. The screen that is placed between the operator and the target makes 'pulling the trigger' easier, or, in the case of fully automated weapons systems, the decision to kill is being delegated to a machine. The non-kinetic modes of inflicting injury, death and destruction employed in computer network operations replaces the trigger with the keyboard of a computer whose operation is in many ways no different from the most ordinary, every-day business of using a computer, except for its consequences.

Processes of moral disengagement, in turn, have been shown in historical, sociological and psychological studies to be one of the causes for violations of the law of armed conflict. It appears reasonable to assume that the processes of moral disengagement induced by the weapons and weapons systems that I am referring to lead to the same result.

5. Concluding observations

In summing up, I will not try to offer any 'conclusions'. Rather, I hope that my observations on the three selected challenges can inform our discussions in the next one and a half days.

CURRENT CHALLENGES IN THE LEGAL REGULATION OF THE METHODS OF WARFARE

Dr. Théo Boutruche

Consultant in International Human Rights and Humanitarian Law

Résumé

L'exposé qui va suivre traite des défis que posent les développements technologiques aux règles de DIH relatives aux méthodes de guerre. Plus précisément, il s'agit d'examiner si la technologie créé de nouvelles obligations pour les belligérants, si elle conduit à de nouvelles interprétations du DIH, et si un développement normatif apparaît nécessaire en matière de méthodes de guerre.

Les défis technologiques relatifs à la protection des personnes civiles et des objets à caractère civil

Un des principes fondamentaux du DIH est le principe de distinction entre civil et combattant, objectif militaire et objet à caractère civil. Plusieurs règles en découlent: la définition d'un objectif militaire spécifique, l'interdiction de prendre un objet civil comme cible d'une attaque, l'interdiction de mener des attaques indiscriminées, l'obligation de prendre des mesures de précautions pour limiter les éventuels dommages collatéraux. Si l'évolution de la technologie peut, dans une certaine mesure, conduire à un meilleur respect du DIH – par exemple, une meilleure précision pour une discrimination accrue – plusieurs problèmes se posent. L'utilisation croissante de drones dans les opérations militaires est particulièrement problématique. En effet, en l'absence d'un pilote à bord, qui est responsable en cas de violation du DIH? Il semble qu'au cœur de cette problématique se trouve la question du degré d'autonomie des drones et de l'implication de l'être humain dans l'identification de la cible, la vérification de la cible, et/ou le déclenchement de l'arme. Différentes situations peuvent se présenter:

- *une personne identifie une cible et évalue les critères requis en vertu du DIH sur la base d'informations fournies par des drones. Se pose alors la question de la fiabilité de telles informations.*
- *un drone sélectionne lui-même sa cible, sans intervention de l'être humain. Si les capacités de discrimination des drones sont fiables et justes, reste le problème de l'évaluation du principe de proportionnalité et des dommages collatéraux potentiels.*
- *le drone décide lui-même de tirer. Cette option est la plus controversée et semble peu compatible avec le DIH. Les règles de DIH ont été écrites par des humains pour des humains, et se fondent pour certaines d'entre elles sur l'évaluation d'un commandant responsable.*

Les défis technologiques relatifs à la protection des combattants

Les défis relatifs à la protection des combattants concernent l'interdiction pour les parties d'utiliser des méthodes susceptibles de causer des maux superflus ou des souffrances inutiles, l'interdiction d'ordonner qu'il ne sera pas fait de quartier, et la protection des personnes hors de combat. Dans ce domaine, l'apparition des armes non-létales ou moins létales pose quelques questions. En particulier, l'utilisation de telles armes peut avoir un impact sur la notion de "personne hors de combat". En vertu du DIH, une personne hors de combat ne peut pas faire l'objet d'attaques. Cependant, certaines armes moins létales ont la capacité d'immobiliser ou d'invalider temporairement une personne. La détermination du statut "hors de combat" est alors plus délicate. En outre, les belligérants pourraient être tentés d'utiliser des armes moins létales pour mieux utiliser une arme létale après. Si la personne est considérée "hors de combat", c'est une violation du DIH.

L'impact des nouvelles technologies sur le recours à de nouvelles tactiques

Un autre défi est celui mis en exergue par le déséquilibre entre les parties à un conflit armé ayant à leur disposition une technologie de pointe, et celles dites "désavantagées". Ce cas de figure se retrouve par exemple dans le conflit en Afghanistan vis-à-vis d'acteurs non étatiques, qui utilisent des méthodes de guerre contraires au DIH pour compenser leur infériorité technologique.

Ébauche de réponses à certains des défis contemporains

L'évocation des différents défis ne conduit pas à la conclusion que le DIH existant est obsolète et que de nouvelles règles sont forcément nécessaires. En revanche, des avancées technologiques telles que les drones peuvent remettre en cause certaines définitions et concepts, et appeler à la clarification dans l'interprétation de règles données. A ce stade, l'article 36 du Protocole additionnel I aux Conventions de Genève reste sans doute le cadre juridique pertinent.

I would like to start by thanking the College of Europe and the International Committee of the Red Cross for inviting me to participate in this Colloquium. I also wish to stress how honoured I feel to be addressing such a distinguished audience.

Introduction

As indicated in the programme, I have been tasked with addressing current challenges to the legal regulation of methods of warfare. Unsurprisingly, and as pointed out by Jann Kleffner earlier, the somewhat difficult distinction between means and methods of warfare has also impacted on my approach to this presentation. It is striking that in coordinating for the preparation of this Panel, Mr Kleffner and I exchanged our speeches and it turned out that we had addressed some similar issues in our respective presentations, while having apparently two different topics to deal with. It may have made me wish I had spoken first. But most importantly, it demonstrates that although recent military manuals, such as the US military manual, insist on differentiating between means and methods, the challenge (the first of a long list) is actually when it comes to applying international humanitarian law (IHL) norms on means and methods of warfare to specific cases. One way to look at this issue would be to rely on the IHL rules as a starting point. The expression 'means and methods of warfare' can be found in several IHL norms, meaning that there are common rules to both the means and the methods. On the other hand, State practice and scholars also refer to particular rules on specific methods of conducting warfare when considering the methods of warfare. There would then be a wider understanding of what methods encompass, beyond the mere relation to weapons.

It is necessary to recall that the term 'methods' includes a broader array of rules depending on the definition retained. If an IHL rule regulates both the means and the methods, such as the prohibition of superfluous injury or unnecessary suffering, it has a broader scope than if it concerned only weapons. On the other hand, it does not mean that States and practitioners always grasp what the reference to methods implies. When adopting Article 35 (2) of the Additional Protocol I (AP I) during the Diplomatic Conference on the prohibition of unnecessary suffering, only Australia objected to the addition of the term 'methods', arguing that it was unclear what was meant by this term and how it would affect the scope of the rule.

Without overlapping with what was said by Mr. Kleffner, I must also try from the outset to clarify what is understood by 'methods'. Traditionally, the 'means' encompass weapons and weapons system or platforms, whereas the 'methods' designate the way weapons are used. Under this understanding, weapons may not be unlawful by nature but may be considered unlawful in some of the manners in which they are used. However, referring to the recent Manual on International Law Applicable to Air and Missile Warfare, the concept of method of warfare also comprises any specific way of conducting hostilities, whether tactical or strategic in manner, to outweigh and weaken the adversary, not particularly related to weapons, and includes the specific tactics used for attack. Consequently, 'methods of warfare' encompass a much broader category of activities and tactics, beyond the mere manner of using weapons, relating to almost every facet of hostilities. The expression comprises specific ways of conducting hostilities and concerns particular rules of IHL such as the prohibitions of perfidy or of the denial of quarter, the prohibitions of indiscriminate attacks, or of the destruction of property. It is argued that methods of warfare have played, and often still play, a more critical role than means of warfare. This is particularly true in the present theatres of conflict, which are often characterised by an asymmetry between the opponents in terms of means, power, organisation and time.

For the purpose of this presentation, 'methods of warfare' will then encompass both definitions (ways of using a weapon and specific ways of conducting hostilities). Consequently, if methods of warfare are understood in a broad sense, the current challenges to legal regulation refer to numerous issues. Due to time constraints, a selection of the challenges is called for. I am also aware that some of the questions that I address will be discussed in greater detail later during this colloquium, so I will limit some of my remarks to the minimum.

While it is not possible to restate here the existing IHL norms and definitions pertaining to our topic, it still seems appropriate to review some of those current challenges based on the various rules related to the methods of warfare. Furthermore, given the broad definition of methods of warfare, it is also interesting to discuss the wider implications, in terms of new military doctrine and strategies for example, and impact of technology on the behaviour and methods of the opponents.

As noted by Mr. Kleffner, it is obvious that technological developments may also ensure better compliance with IHL, but this presentation focuses on technological developments that raise challenges to IHL. However, challenges regarding existing IHL norms also relate to whether technology is not creating greater obligations for parties to a conflict which have advanced technology in their arsenal. Technological challenges to legal regulation, like for other changing areas covered by IHL, exert pressure on existing norms on methods of warfare by leading to new or conflicting interpretations of IHL norms or questioning whether new law is needed.

I. Some technological challenges to the legal regulation of methods of warfare related to the protection of the civilian population and of civilian objects

Most of the current legal challenges arising from technological developments under IHL relate to the norms protecting the civilian population and civilian objects. One of the fundamental tenets of IHL is the principle of distinction, prescribing parties to the conflict to distinguish between the civilian population and combatants and between civilian objects and military objectives at all times (Art. 48 of 1977 AP I). Accepted as a restatement of customary international law even by non-parties to the Protocol, this principle is set out by different specific rules such as the ones defining military objectives, the prohibition of making civilians objects of attacks, the prohibition of indiscriminate attacks or the rules on precautionary measures.

Advances in technology, notably in respect of precision, unquestionably lead to an improvement in the ability to respect those norms. On the other hand, technology also raises several issues in this regard.

The development of electronic warfare, such as computer network attacks (CNA), while not involving kinetic force, may have just as destructive effects as common warfare. This particular field raises a key issue at the heart of the legal regime protecting civilians and civilian objects under IHL. Computer warfare triggered debates on the way relevant IHL norms are framed and articulated, notably regarding the definition of attack. As this was already addressed by Mr. Kleffner, I will only stress the fact that the challenge here is one of conflicting interpretation of existing rules.

The increasing resort to Unmanned Combat Aerial Vehicles (UCAVs) for military operations in Afghanistan, Pakistan or Yemen raise serious issues for the legal regulation of methods of warfare, in particular the rules related to targeting and the protection of civilians. UCAVs are defined by the Manual on International Law Applicable to Air and Missile Warfare as 'unmanned military aircrafts of any size which carry and launch a weapon, or which can use on-board technology to direct such a weapon to a target'. Under military considerations, the use of such aircrafts provides significant advantage with regard to the safety of military personnel, an element which is put forward in State practice as part of the military advantage to be taken into consideration when launching an attack. It has been suggested, however, that the pilot's absence from the cockpit in UCAVs constitutes a challenge under IHL norms, including the question of assigning responsibility in case of violations. The key issue lies in the degree of autonomy (remotely-controlled, semi-autonomous, or completely autonomous designs) the UCAVs have over battle operations and whether or not a human element remains either in remotely piloting, in the identification and verification of targets, and/or the decision to release weapons. At this stage, current designs still include an element of human control (a 'man in the loop'), at least through the authorisation of weapons release by a ground controller.

Among the problematic implications of the use of such methods under IHL, one may consider the following. In cases of remotely piloted UCAVs, the aircraft uses a communications link with a manned control station, dictating the vehicle's flight path and operation. Additionally, imagery from the UCAV's sensors is transmitted to the control station, enabling the human operator to locate, identify, and engage enemy targets. Such devices still raise the issue, in the absence of human eyes on board, of the requirements of IHL related to the definition of military objectives, the compliance with the principle of distinction and precautionary measures to be taken. On the other hand, it is argued that through high technology systems, a drone will ensure better (better than human) target discrimination and that the factor of stress experienced by soldiers will be avoided. In addition, it is not proven that a pilot in the cockpit would have better sight of the battlefield than a human operator away from the target. In the absence of fully autonomous UCAVs, one issue however lies in the ability of human operators to base the identification of targets on information and intelligence gathered though UCAV's systems, miles away from the field of operations, and consequently to assess IHL legal parameters based on this information. Another issue relates to the reliability of such information.

Debates also concern the case of UCAVs selecting their own targets, with no human sense of what might be unusual or out of place on the ground. It remains to be proven that the discriminative capability of UCAV computers is reliable and accurate, let alone the capability to assess potential collateral damage under the principle of proportionality.

Leaving the decision of releasing a weapon to the UCAV's computers also triggers debate. While so far it has been left to a human operator, this prospect is problematic. A complete reliance on computers to consider all the aspects of an attack, gives rise to great doubts in terms of capacity to respect and assess legal requirements. This is so even where it is proven that a drone would use the same caution that a human being would use when deciding to employ a weapon. There would be an intrinsic issue with removing the human factor, with the potential sense of hesitation that a human being can have, compared to a machine. There are both ethical and legal considerations at stake here but ultimately this reluctance could come from the fact that IHL rules are drafted by human beings for commanders and soldiers. Some of those rules are based on assessments by a reasonable commander such as the requirement on precautionary measures.

Let me now turn to the issue of whether technologically advantaged States have greater obligations under IHL than disadvantaged ones.

A first case relates to the debate whether States have an obligation to either acquire precision-guided munitions or to use such weapons when they possess them in their arsenal. While it is difficult to make a case for an obligation to acquire, which depends more on policy and moral grounds, there has been debate regarding the obligation to use precision-guided weapons when they are available. This derives from the reference in IHL norms on precautionary measures to the obligation to 'take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimising, incidental loss or civilian life, injury to civilians and damage to civilian objects' (Art. 57(2)(a)(ii) AP I). However, the existence of an obligation has been contested on the basis that IHL norms merely set up a good faith and contextual standard which depend on circumstances and what is expected from a reasonable commander in the choice of methods of warfare.

The level of technology available may also impact on the assessment of an attack 'which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, which would be excessive in relation to the concrete and direct military advantage anticipated'. This codification of the principle of proportionality entails a determination of the expected effects of an attack on civilians and on civilian objects. A Party to a conflict having advanced technological capabilities regarding information gathering would have a better ability to evaluate more precisely those expected effects.

II. Some technological challenges to the legal regulation of methods of warfare related to the protection of combatants

IHL regulating methods of warfare naturally also relate to the protection of combatants such as the prohibition of methods causing superfluous injury or unnecessary suffering, the prohibition of the denial of quarter, or the protection of persons who are *hors de combat*.

One revolutionary aspect is the increasing resort to non-lethal or 'less than lethal' technology in the context of situations covered by IHL. There are potential implications of such developments for some of the key rules on methods of warfare. Such weapons are defined as 'those which are intended to incapacitate or immobilise a person without intending to cause death or serious injury to that person'. One may consider then that such technology would change the perception one has of what the primary purpose of a weapon is. Such weapons are not designed to be substituted for lethal weapons, but are to be used in combination with the latter. 'Less than lethal' weapons potentially have an impact on the notion of 'hors de combat'. Under IHL a person who is recognised or who, in the circumstances, should be recognised to be 'hors de combat' shall not be made the object of attack (Article 41,AP I). This immunity from attack is also a norm of customary law. Under IHL a person is considered hors de combat in different cases, notably when rendered unconscious or otherwise incapacitated by wounds or sickness, and therefore is incapable of defending himself; provided that in any of these cases he abstains from any hostile act and does not attempt to escape. While these criteria may be difficult to apply in practice, the use of antipersonnel 'less than lethal' weapons may complicate such determination in that they are designed to have temporary effects. There may be an incentive for combatants to also use lethal weapons once a person has been incapacitated temporarily by 'less than lethal' weapons. However, this would be seen a violation of the above mentioned rule as the person is already *hors de combat*.

The technological improvements in methods of warfare can also have implications on the broader issue of the legal requirements limiting the type of actions to be undertaken against combatants. It has been acknowledged that at this stage there is no obligation 'to shoot to injure' and that the way to use weapons against legitimate targets is not regulated in the same manner as under human rights law. IHL does not expressly regulate the kind and degree of force that may be used against legitimate targets. There is however controversy on whether the IHL general principle limiting the kind and amount of force used in a military operation to what is militarily necessary imposes legal requirements on the way lethal force is used. The argument could also be based on the principle prohibiting superfluous injury or unnecessary suffering. The gradual approach in the use of lethal force was primarily discussed with regard to the issue of civilians directly participating in hostilities but there is no reason why this should not be discussed when considering attacks against combatants. Technological improvements in information gathering and in 'less than lethal' weapons may lead to a normative evolution in regard to some standards of gradual use of force against legitimate targets.

III. The impact of technology on the recourse to new tactics of warfare

The challenges posed by technological developments to IHL norms regulating methods of warfare are not limited to issues arising from technologically advantaged States. There has been an increasing asymmetrical gap created by high technology capabilities between such States and disadvantaged States or parties to a conflict. This is particularly the case with regard to non-state actors in Afghanistan or Iraq who, in response to sophisticated technology in warfare and methods of combat, adopted new methods of combat stressing or violating IHL norms.

Among those new measures are the use of booby-traps in dead and wounded bodies, moving the battlefield to urban or other built-up areas, the use of civilians as human shields, or mingling with the civilian population. Such methods may violate the rules protecting civilians and civilian objects. They also pose great challenges for the opponent to respect IHL in its own operations.

IV. Perspectives on responses to some of the current challenges

The challenges discussed earlier regarding the legal regulation of methods of warfare do not mean that by definition relevant IHL norms are obsolete and that new rules are needed. The situation is of course more nuanced. Technological advances such as UCAVs or CNA question existing definitions and concepts pertaining to IHL norms on methods of warfare calling for clarification in interpretations of the law. This can take the form of the adoption by States using UCAVs of rules of engagement that duly take into account the various challenges posed by the use of this type of aircraft.

Under IHL, the reference to the Article 36 AP I seems to be an appropriate framework to address issues raised by some of the new methods of warfare. The obligation of review covers both the means and the methods. Furthermore the reference to the words ‘in some or all circumstances’ in this provision requires that States contextualise the review in order to properly assess the lawfulness of weapons and methods of warfare. This includes reviewing the way weapons are planned to be used. In this regard, the technological advances also impact on the context in which weapons are used.

Finally, a key question is whether it is possible to comply with IHL rules on methods of warfare without having any human intervention. How can a machine determine when a soldier offers to surrender for example? However, the critical issue of human involvement seems also to be a matter of principle. If IHL rules are based on a balance between humanitarian imperatives and military considerations, that balance could only be assessed by human beings.

I thank you for your attention.

PANEL 1 – NEW TECHNOLOGY ON THE BATTLEFIELD DISCUSSIONS

During the debate following the presentations of the first panel, the audience raised five main issues:

1. The accuracy of weapons and the prohibition of rendering 'death inevitable' (St Petersburg declaration)

As mentioned during the session, technological developments on the battlefield include a better accuracy of weapons. Such weapons allow targeting alleged military objectives with very high accuracy but are also more likely to hit and kill the people targeted. On the other hand, Paragraph 4 of the Preamble of the St Petersburg Declaration[1] makes unlawful the use of weapons that 'render death inevitable'. Are these weapons compatible with the St Petersburg declaration? If the panellists seem to agree that there might be a problem when looking at the abstract rule, no State practice would support the interpretation that the use of excessive force violates the rule of superfluous injury and unnecessary suffering. One suggestion was to consider whether the killing effect is systematic or not. Even if a weapon is accurate, there might not be a systematic effect of killing instantly the people targeted. On a more general level, it was noted that the St Petersburg Declaration states that 'the progress of civilisation should have the effect of alleviating as much as possible the calamities of war'. Indeed, even if some weapons are explicitly developed to decrease collateral damage and designed to better respect international humanitarian law (IHL), they could pose, nonetheless, a challenge to the prohibition of causing superfluous injury, unnecessary suffering or of rendering death inevitable.

2. A quantitative or a qualitative change in the applicability of IHL?

With respect to the impact of new technologies on the applicability of IHL, the question was raised whether the change needed would be simply quantitative or also qualitative. According to the panellists, it seems that there is no technological revolution taking place in the battlefield but rather gradual developments. Therefore, most of the changes would be quantitative. However, one area might be new: the use of non-kinetic force, like computer network opera-

[1] Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight, St Petersburg, 29 November / 11 December 1868.

tions. As IHL was based on the assumption that attacks use kinetic force, there might be a qualitative change in this particular area.

3. Precautions in attack and precision-guided munitions

IHL rules on precautions in attack include the limitation of collateral damage. In this respect, the question of precision-guided munitions arises. Indeed, such weapons allow better accuracy to hit the intended target and could therefore be used to reduce collateral damage. It was argued that such high-technology material, if available to a belligerent party, should be used when carrying out attacks that may cause collateral casualties or damage. This would be part of the parties' obligation to take precautions in attack.

4. Autonomous weapon systems?

According to military specialists, there is at present no autonomous weapon system. Would there ever be one? Indeed, there is always a person behind an action, for example the commander who commands to press the button. For the commander, there is a necessity to use these types of weapons only when it is certain that it will hit a legitimate military objective and that no disproportionate collateral damage will occur. Beyond the legal obligations, there are also strategic obligations for commanders to be sure that the weapons will be used in the right way.

Session 2
Cyber Warfare

Chair person: **Knut Doermann,** *ICRC Geneva*

THE TECHNOLOGY OF OFFENSIVE CYBER OPERATIONS[1]

Herbert Lin
US National Research Council

Résumé

Technologie et autres éléments pouvant avoir un effet : *une opération offensive, qu'il s'agisse d'une attaque ou d'une exploitation, requiert trois éléments: un accès (à distance ou fermé), une vulnérabilité, et une charge utile (*payload*).*

Les différents types d'offensives cybernétiques : *une attaque cybernétique est destinée à provoquer: (1) une perte directe d'intégrité, en ce qu'elle peut altérer/transformer un programme ou des données informatiques; (2) une perte d'authenticité qui induit le destinataire d'un message en erreur quant à son expéditeur; (3) une perte de disponibilité d'un réseau ou système. En outre, des effets indirects peuvent intervenir sur d'autres systèmes ou appareils reliés, ou sur les usagers du système ou réseau informatique attaqué. Une cyberexploitation vise la confidentialité de l'information stockée sur un système ou un réseau, qui est normalement accessible uniquement aux parties autorisées. A l'inverse d'une cyberattaque, une cyberexploitation n'est pas destructive par nature. Une cyberexploitation est furtive et conduite une intervention minimum. Elle ne perturbe pas le fonctionnement normal du système.*

Caractéristiques des offensives cybernétiques : *en générale, les offensives peuvent être conduites sous couvert de déni plausible, dans la mesure où la preuve de l'implication d'un acteur dans une telle opération est souvent difficile à obtenir. La technologie en question est relativement peu coûteuse, largement disponible et facilement accessible. Ainsi de nombreux acteurs non étatiques, qu'ils soient des compagnies privées, des hackers ou des terroristes, peuvent y*

[1] This paper is based almost entirely on material drawn from National Research Council (William A. Owens, Kenneth W. Dam and Herbert S. Lin, editors), *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (National Academies Press, Washington DC) 2009. The project responsible for this publication was supported by the MacArthur Foundation and the Microsoft Corporation, although the views reflected in this article and in the referenced publication do not necessarily reflect the views of either of these sponsors.

avoir recours, et avoir la même influence, dans l'espace cybernétique, que des acteurs étatiques. Toutefois, un État gardera toujours un avantage grâce aux renseignements considérables dont il dispose à l'appui d'une opération. Concernant les effets d'une offensive cybernétique, les effets indirects d'une attaque cybernétique sont presque plus importants que les effets directs. Ils peuvent être différés par rapport au moment de l'attaque, et de magnitudes très diverses. Les opérations cybernétiques peuvent être sélectives ou non. Les attaques sont particulièrement compliquées à planifier et à exécuter. La réussite d'une opération dépend donc en grande partie de la quantité et de la qualité des renseignements à disposition.

***Considérations opérationnelles :** en vue d'une opération cybernétique, la partie responsable doit: (1) identifier la cible, (2) planifier l'opération, (3) exécuter l'opération, (4) évaluer le résultat. Une attaque peut être utilisable une ou plusieurs fois; elle peut avoir des effets limités dans le temps et dans l'espace. En outre, il est important de noter que la plupart des cyberattaques sont certes techniquement rapides, mais elles sont lentes d'un point de vue opérationnel du fait du temps de préparation qui peut être très long.*

***Objectifs éventuels d'une offensive cybernétique :** une attaque cybernétique peut avoir pour objectif (1) de détruire des données dans un ordinateur, (2) de devenir un membre actif d'un réseau et générer ainsi de faux emails par exemple, (3) transformer clandestinement des données stockées sur un réseau, (4) de dégrader ou détruire un service sur un réseau donné. Une exploitation cybernétique peut viser à (1) obtenir des informations sur les intentions ou capacités d'un adversaire, (2) observer la topologie et le trafic d'un réseau.*

***Quelques ambiguïtés relatives au DIH :** certains problèmes se posent au regard du DIH. Par exemple, d'un point de vue technique, il n'est pas évident de distinguer préalablement à l'opération si celle-ci a pour objectif l'exploitation ou l'attaque d'un système ou serveur donné. Or, en droit international, l'espionnage est légal alors que l'utilisation de la force ne l'est pas.*
Une infrastructure à double usage civil et militaire constitue-t-elle un objectif militaire légitime? Quelle est la responsabilité des États pour des opérations cybernétiques conduites par des acteurs non-étatiques sur leur territoire?

***Réponse à quelques questions fondamentales:** En matière d'opérations cybernétiques militaires, il est possible de distinguer une cible militaire d'une cible civile, mais seulement dans une certaine mesure et à l'aide d'une quantité importante de renseignements. Les dommages collatéraux peuvent être limités grâce à des renseignements efficaces, une bonne compréhension technique de la cible, et une haute capacité de sélection.*

1. Introduction – A canonical example in the news

A recent example of an offensive cyber operation discussed in the news is Stuxnet. The Stuxnet incident, still ongoing at the time of writing (February 2011), involves malware directed against industrial control systems. The malware has been dubbed Stuxnet, and reportedly performs both cyber attack and cyber exploitation functions. The attack function reprograms industrial control systems of a particular kind so that the machinery controlled by those systems is destroyed. The exploitation function exfiltrates sensitive data to those controlling Stuxnet.

To gain access to the targeted systems, Stuxnet takes advantage of previously unknown vulnerabilities in certain Windows operating systems. The physical mechanism for introducing Stuxnet into the targeted systems is not known, though speculation has centered on an initial introduction through an infected USB drive inserted into a computer attached to the internal network controlling the systems. Once inside the network, Stuxnet replicates itself, taking advantage of poorly configured internal security systems (e.g., knowledge of default passwords) and forged digital certificates of identity (thus tricking the system into believing that it is from a trustworthy source).

Stuxnet attacks only a specific configuration of hardware (in other cases, it is dormant), and the sophistication of the attack requires a detailed knowledge of the industrial processes involved.

2. Technology and other effectors

An offensive operation, which may be either an attack or an exploitation, requires three components:

- *Access*. Access refers to how the commander of the operation gets at the network/system of interest. Access comes in two categories:
  - *Remote access* (e.g., over the Internet, through a dial-up modem attached to it, through penetration of the wireless network to which it is connected). Examples include denial-of-service attacks and malware found on web pages that victims visit.
  - *Close access*, in which an operation takes place through the local installation of hardware or software functionality by friendly parties (e.g., covert agents acting as operators or service technicians, vendors) in close proximity to the computer or network of interest. Close access is a possibility anywhere in the supply chain (e.g., during chip fabrication, assembly, loading of system software, during shipping to the customer, during operation). Examples include use of USB keys in operation and opening the box and replacing software while in transit.
- *Vulnerability*. A vulnerability is an aspect of the system that can be used to compromise it. Such weaknesses may be accidentally introduced through a design or implementation

flaw. They may also be introduced intentionally (see 'close access' above). An unintentionally introduced defect ('bug') may open the door for opportunistic use of the vulnerability by an adversary.

- *Payload*. Payload is the term used to describe the mechanism for affecting the target system once an attacker has been able to take advantage of a vulnerability. For example, once a software agent (such as a virus) has entered a given computer, its payload can be programmed to do many things—reproducing and retransmitting itself, destroying files on the system, altering files.

  Payloads can be designed to do more than one thing, or to act at different times. If a communications channel is available, payloads can be remotely updated.

The discussion above is cast largely in technological terms. But people also interact with information technology, and social operations can be used to target the human element. Social operations may involve tricking, bribing, blackmailing, extorting someone to take action that works to the advantage of the perpetrator. Technical and social operations are often combined for greater effect.

3. Types of offensive cyber operation

There are two types of offensive cyber operation. Cyber attacks (as opposed to cyber exploitations) are directed at causing a loss of:

- *Integrity*. Compromising integrity entails altering information (a computer program, data, or both) so that under circumstances selected by the attacker, the computer system does something it should not do.
- *Authenticity*. A message whose authenticity has been compromised will fool a recipient into thinking it was properly sent by the asserted originator.
- *Availability*. Compromising availability means that the functionality provided by the target system or network is not available to the user when needed—when the computer controls a physical process, physical destruction may result.

The compromises above can also result in indirect effects, which are effects on the systems and/or devices that the attacked computer system or network controls or interacts with, or on the people that use or rely on the attacked computer system or network. Because virtually anything can be connected to a computer system, the scope and nature of effects resulting from a cyber attack can span an enormous range. Both direct and indirect effects must be taken into account in ascertaining the significance of a cyber attack.

Cyber exploitations target the confidentiality of information stored on or passing through a system or a network. Under normal circumstances, such information should be available only to authorised parties. A successful cyber exploitation compromises the confidentiality of such information and makes the information available to the adversary.

Cyber attacks are destructive in nature and cause adversary computer systems and networks to become unavailable or untrustworthy and therefore less useful to the adversary. Cyber exploitations are non-destructive, as they seek to obtain information resident on or transiting through an adversary's computer systems or networks, information that would otherwise be kept confidential. Cyber exploitations are stealthy and are conducted with the smallest possible intervention that still allows extraction of the information sought. Stealthiness is required to reduce the likelihood that the victim will take countermeasures and to enable, from one penetration of an adversary's computer, multiple exfiltrations of data. Cyber exploitations do not disturb the normal functioning of a system, and the best cyber exploitation is one that a user never notices.

4. Key characteristics of offensive cyber operations

In general, offensive operations can be conducted with plausible deniability, as definitive proof of a particular actor's involvement is hard to obtain. (However, remember that it is possible for an attacker to make mistakes that leave clues as to his identity.)

Offensive technology is relatively inexpensive, widely available and easy to obtain. Thus, many non-state actors (companies, patriotic hackers, terrorists) can have influence and may be able to cause some of the same kinds of effects in cyberspace as State actors. However, State actors have many advantages, such as the availability of considerable intelligence resources to support an offensive operation.

On the other hand, a resource-poor attacker may nonetheless have significant leverage, through the theft of computing and financial resources and the use of automation to reduce personnel and skill requirements.

The indirect effects of cyber attacks are almost always more consequential than the direct effects of the attack – 'indirect' does not mean 'not primary'. Furthermore, the collective effects can span an enormous range, and thus a cyber attack is not of lesser consequence because it 'only' targets a computer. The effects of a cyber attack may be significantly delayed in time from moment of insertion, and the time and spatial scales of a cyber attack can span many orders of magnitude.

Cyber operations can be selective or non-selective in targeting. High selectivity implies long lead time to collect a lot of intelligence and specialised skills to attack just the target of interest – and thus implies higher cost. Cyber operations (especially attacks) are also very complex to plan and execute, as they involve both a larger range of options than most traditional military operations and many possible outcome paths, whose analysis often requires highly specialised knowledge.

The success of a cyber operation depends heavily on good, detailed and timely intelligence:

- Small details of configuration matter a lot and can change easily.
- Cascading effects are hard to predict.
- Collateral damage is hard to estimate.
- Damage assessment is hard to perform.

5. Operational considerations

To conduct a cyber operation, the responsible party must:

- Perform target identification (often a manual, time intensive process);
- Plan the operation (gain access, determine vulnerabilities, specify the effects sought and plan to limit collateral damage);
- Execute the operation (which may take place sometime long after obtaining access/vulnerability during which defences/configuration of the target may have changed);
- Assess the effects/results (distinguish between real success and faked success—an apparently successful exploitation may have obtained misinformation, an apparently successful attack may be successful in appearance only).

A cyber attack may be usable only once or a few times (the victim may take countermeasures after the initial attack), limited temporally in effect (victim may recover quickly and prevent similar future attacks) and limited in scope (if highly targeted). Most importantly, many cyber attacks are technically fast but operationally slow (all of the preparation steps above take a lot of time)—hence they may be most suitable in non-time-urgent operational scenarios (e.g., early use). Technically, they may operate at the 'speed of light'. In practice, cyber attacks may operate at the speed of law/thought/analysis/policy.

6. Possible goals of an offensive cyber operation

A cyber attacker might seek to:

- Destroy data on a computer, targeting the information on it or something connected to it (e.g., a power plant controlled by the computer).
- Be an active member of a network and generate bogus traffic. For example, an attacker might issue phony orders to its adversary or pass faked intelligence information.

- Clandestinely alter data in a database stored on the network. For example, the attacker corrupts a database that controls logistics deployment for the adversary.
- Degrade or deny service on a network. An attacker might try to degrade the quality of service available to network users by flooding communications channels with large amounts of bogus traffic, thereby delaying communications or making communications more vulnerable to interception.

A cyber exploitation might seek to:

- Obtain information on an adversary's intentions and capabilities.
- Be a passive observer of a network's topology and traffic (e.g., map the network and make inferences about important and less important nodes).
- Obtain information from a company's network in another country in order to benefit a domestic competitor of that company.

7. Some IHL ambiguities

Cyber operations pose many problematic cases under present international humanitarian law (IHL). For example:

- Is a given cyber operation an attack or an exploitation? The target of an operation may not be able to distinguish a cyber operation for attack purposes from one for exploitation purposes, as these operations are very similar from a technical point of view. But under international law, exploitation (that is, espionage) is not forbidden, whereas uses of force are forbidden.
- Are cyber attacks on dual-use infrastructure permissible? For example, modern military forces increasingly communicate using capabilities provided by nominally civilian infrastructure. Does this fact make civilian infrastructure a legitimate military target?
- Cyber attacks are inherently clandestine and based on deception. How do such characteristics comport with the intent underlying present-day IHL?
- How and to what extent should nations be responsible for the cyber operations conducted by non-state actors within their territories or otherwise under their jurisdiction?
- Given the possibility of a long delay between the insertion of an attack agent and the moment it is activated, at what moment in time should 'a use of force' be recognised?

8. Some fundamental questions

The sponsors of this talk posed several questions for me to answer. These follow below, with short answers provided by me.

- Is it possible (feasible) to distinguish civilian and military targets in military cyber operations?

Answer: Yes, to a limited extent, but only with a significant amount of intelligence on the target and/or cooperation from target.

- How can collateral damage be minimised?

  Answer: Only with good intelligence and technical understanding of the target complex, and a very selective targeting capability for an attack.

- How can exploitation operations and destructive intrusions be distinguished?

  Answer: As a general rule, this is a very difficult task. The software code responsible for the operation or intrusion can be analysed, but it often takes a lot of time to perform a definitive analysis. If the software code can be remotely upgraded (i.e., changed), the task is essentially impossible, since the analyst has no idea what new code may be uploaded in the future. However, after the code has been activated, the results may be easy to see, in which case intent may become easier to ascertain.

I also posed a number of other questions that I regard as fundamental to understanding this domain.

- What can or should a nation do in cyberspace in conditions short of avowed armed conflict or in response to actions that fall short of armed attack or uses of force?
- How (if at all) should an attacking nation enable adversaries to differentiate between exploitation and attack?
- In light of limited law enforcement response capabilities, how and to what extent, if any, should private entities be allowed to shoot back or investigate? Does private shoot-back increase or decrease likelihood that a private entity will be attacked?
- How, if at all, are existing international legal regimes (e.g., the laws of armed conflict, the Geneva Conventions) adequate to manage cyber conflict?
- What is the role of international cooperation and agreements in managing cyber conflict?

9. Concluding Thoughts

Offensive cyber operations – both cyber attacks and cyber exploitations – pose many challenges for the interpretation of IHL. A cyber dimension of conflict in the future is virtually inevitable, and policy makers must understand the legal landscape *before* such a conflict occurs. A central recommendation of the National Research Council report, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* is to develop a knowledge base and expertise that policy makers will find helpful if and when such conflict occurs, and the International Committee of the Red Cross has a vital role to play in this regard.

CYBER WARFARE AS ARMED CONFLICT

Noam Lubell[1]
National University of Ireland, Galway

Résumé

Une guerre cybernétique peut-elle être qualifiée de conflit armé au sens du DIH? La réponse à cette question conditionne l'application ou non du DIH, et en ce sens, est essentielle.

Dans un premier temps, il convient de s'interroger sur la notion de "champ de bataille" dans le cadre d'une guerre cybernétique. Une guerre cybernétique est-elle une guerre qui se déroule dans le cyberespace? Le cyberespace est parfois décrit comme le réseau interconnectant ordinateurs, informations, télécommunications et services. En ce sens, il ne s'agit pas d'un espace physique. En revanche, la stratégie de défense nationale américaine considère le cyberespace comme une théâtre d'opérations, au même titre que l'air, la terre ou l'espace.

Une définition qui limiterait la guerre cybernétique à une guerre se déroulant dans le cyberespace n'est pas satisfaisante. En effet, ce qui importe sont les effets de la sphère cybernétique dans la sphère physique. Une guerre cybernétique remplit-elle les critères d'un conflit armé? Le fait que des opérations cybernétiques soient conduites par des forces armées n'est pas suffisant. Il faut avant tout établir l'existence d'un conflit armé. Un élément est essentiel: il faut déterminer quelles sont les parties au conflit. Or, cet aspect peut représenter un défi majeur en cas d'attaque anonyme, l'auteur ou la provenance d'une attaque cybernétique étant techniquement difficile voir impossible à identifier. Cet élément est toutefois essentiel pour (1) déterminer l'existence d'un conflit, (2) appliquer les règles de DIH et (3) établir une responsabilité.

*Si l'implication de deux ou plusieurs parties, États ou groupes armés organisés, est avérée, il faut ensuite établir qu'elles utilisent la force armée entre elles. A noter que dans le cadre d'un conflit armé non international, le critère traditionnel est une "*violence armée prolongée*" (CIJ,* Tadic, *Arrêt de la Chambre d'appel du 2 Octobre 1995). A ce stade, il peut être utile de se référer au* ius ad bellum. *L'interdiction de l'usage de la force à l'article 2(4) de la Charte des Nations unies est souvent interprétée comme étant l'usage de la force physique. Selon la Cour Internationale de Justice (CIJ) dans l'arrêt* Nicaragua, *la notion de "*force*" au sens de la Charte peut également inclure des actes qui sont en dessous du seuil requis pour une "*attaque armée*". Une attaque*

[1] The following is an approximate transcript of the spoken presentation. The author is currently working on a detailed publication in the area. The publication will include in-depth analysis of these issues, and details on sources used in this presentation.

armée requiert un élément armé. Toutefois, si les conséquences d'une attaque cybernétique sont similaires à celles d'une attaque classique – qui a un caractère cinétique – par des forces armées, on pourrait alors certainement soutenir que celle-ci constitue une attaque armée, au sens juridique du terme.

Si une attaque cybernétique peut constituer une violation de l'interdiction de l'usage de la force, selon sa nature et ses conséquences, il n'est pas sûr pour autant qu'une telle attaque atteigne le seuil requis d'un conflit armé en vertu du DIH. En effet, le DIH distingue "hostilités" et "attaques", les "attaques" intervenant le plus souvent dans le cadre d'"hostilités" plus larges. Une attaque est donc traditionnellement considérée comme un élément de la violence armée. On peut alors supposer que l'élément important dans la définition d'une "attaque" est l'intention de causer un dommage, qu'il soit humain et/ou matériel. Il pourrait être allégué que si une guerre cybernétique a les mêmes effets qu'une guerre classique, le type de violence qu'elle implique devrait être considérée comme équivalente à celle envisagée par le ius in bello.

Ainsi, on peut caractériser une guerre cybernétique par rapport à un conflit armé de trois manières:

(1) Les opérations cybernétiques ne remplissent pas en elles-mêmes les critères nécessaires pour être considérées comme constitutives d'un conflit armé. Le DIH ne s'applique pas.

(2) Certains types d'opérations cybernétiques peuvent être équivalentes à des attaques traditionnelles du fait de leurs conséquences en terme de victimes et de destruction. L'intensité d'une telle violence doit alors être évaluée, en particulier dans le cadre d'un conflit armé non international.

(3) Scénario le plus probable: les opérations cybernétiques ne constituent pas la preuve d'un conflit armé, mais elles peuvent être utilisées en soutien à la force armée traditionnelle. Il faut alors déterminer si ces opérations cybernétiques font partie des hostilités en cours. Si ces opérations sont conduites par les forces armées d'un État, la question est relativement facile. Si, à l'inverse, c'est un civil qui mène une telle opération, cela signifie-t-il qu'il participe directement aux hostilités?

The focus of this presentation is to examine whether cyber war can be categorised as armed conflict, because if not, international humanitarian law (IHL) might not apply in the first place. The rhetoric of war is not enough in order to determine an armed conflict. We are familiar with the controversies surrounding the 'war on terror' and whether this is an armed conflict as defined by international law. Even more so, the phrases 'war on drugs' and 'war on poverty' are further evidence that simply calling something a 'war', does not mean this is a *bona fide* armed conflict. Accordingly, one cannot assume that cyber war is indeed a war at all.

Cyberspace

To start with, we may wish to determine the battleground. Are we looking for a geographical area in which cyber war hostilities take place? Alternatively, is there a new type of battlefield, in other words, does cyber war take place in cyberspace? The phrase 'cyberspace' is associated with science fiction literature (and films) in past decades, referring to networks linking all people, machines, and information. This does sound a little futuristic, especially the part about connected humans, although the US Defence Advanced Research Projects Agency (DARPA) is funding a 'Human-Assisted Neural Devices Program'. In fact, there is research into brain-machine interfacing, which allows a pilot to 'become the plane'. The cyberspace network linking everyone to everything is therefore perhaps not as far removed from reality as initially thought. Cyberspace has been defined by a 2001 Report for Congress as the 'total interconnectedness of human beings through computers and telecommunication without regard to physical geography'. For now, however, we will leave brain-machines out of the picture, and focus, in the current context, on a form of network linking machines, information, telecommunications, and services.

Cyberspace is sometimes described as the space between the machines. In that sense, it is not a physical area. The networks and links crisscross the globe with no regard for State borders. Cyberspace is described as a theatre of operations in the US National Defence Strategy. Is this then an actual location in which war can take place? It certainly is increasingly referred to in a manner similar to the accepted physical domains of conflict. Indeed, the mission of the US Air Force is to 'to fly and fight in Air, Space, and Cyberspace'.

Cyber warfare

Is cyber warfare a war in cyberspace? This would not be a satisfying definition, since it disregards the effect in the physical realm. Cyberspace links the information realm and the physical realm, and it is the effect of the former on the latter that is at the centre of attention in cyber warfare.

In the context of international law, one of the pressing questions is whether cyber warfare fulfils the definition of armed conflict. For the purpose of clarity, the following examination of this question will focus upon circumstances encompassing cyber warfare alone, and not in conjunction with kinetic attacks. Taken alone, would the following examples be considered as armed conflicts?

- NATO had allegedly planned to compromise Serbia's air defences (but decided against because might have caused it to target civilians).
- The US is said to have planned to damage the Iraqi financial system (but didn't go through because of possibility of effect flowing into international financial system).

- Estonian critical services sites were subjected to 2,000 visits a second. Russia was blamed, but this was unproven.
- Russia was alleged to have been responsible for denial-of-service attacks against Georgian websites.
- The Stuxnet worm, a computer virus designed to attack particular systems, was used against Iran's Bushehr nuclear power plant, with alleged Israeli involvement.

One reason we often think of cyber operations in context of war is the military involvement. Clearly, the military nowadays plays a vital role in these operations. The US, for example, appointed a four-star general to head the new Cyber Command, with the objective to 'direct the operations and defence of specified Department of Defence information networks [involving some 90,000 military personnel] and prepare to, when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, [to] ensure US allied freedom of action in cyberspace and deny the same to our adversaries.'

If operations are carried out by the military, is that enough to call it armed conflict? The answer is negative. Not everything done by the military is viewed as an armed conflict – for example, some militaries engage in humanitarian aid missions such as search and rescue after earthquakes. The need remains to identify the existence of an armed conflict. This is a technical legal term with requirements that must be fulfilled. It goes beyond the rhetoric of 'war', and is based primarily on the existence of particular factual circumstances.

Unquestionably, there need to be parties to the conflict. For an international armed conflict, these must be States. Here we already have one of the greatest challenges arising from cyber warfare - anonymous attacks. In many cases, there are plenty of allegations of State involvement (e.g., the cases of alleged Russian involvement in cyber attacks on Estonia or Georgia, and alleged Israeli responsibility for the Stuxnet worm). On traditional battlegrounds, we can see who is fighting; even the source of missiles from a distance can usually be traced. But if we have no knowledge of the source of a cyber attack, then we may be obstructed from determining the conflict, from applying the rules, and most importantly, from having any form of accountability.

Nonetheless, if State involvement is confirmed, we then still need to identify the existence of force between States, which is usually understood to mean armed force. The question of 'force' will be returned to shortly. For a non-international armed conflict the traditional requirement is 'protracted armed violence between governmental authorities and organised armed groups or between such groups within a State'.

The existence of force is therefore a prerequisite for the existence of armed conflict. There are various areas of international law that deal with force. They are all designed to answer different questions, not only about the existence of armed conflict, but perhaps one can learn from them even if only by analogy. In particular, in the context of cyber attacks, it is useful to also mention the *ius ad bellum*. The prohibition of force in Article 2(4) of the UN Charter is usually understood to include an element of physical force, though there is a possibility that this could include indirect force. Following the *Nicaragua case*[2], 'force' under Article 2(4) might include acts that are of a lower threshold than an 'armed attack', although this has proved a source of controversy An armed attack would seemingly require an armed element, but if the consequences of a cyber attack would be of a similar nature and scale as a kinetic attack by armed forces, there would be a strong case for it to be considered an armed attack. There may also be acts which do not amount to force at all, but would constitute unlawful intervention.

Depending on their precise nature and consequences, cyber attacks may fit some of these descriptions and be a violation of the prohibition on use of force or of non-intervention, but this may be too low a threshold to necessarily determine existence of armed conflict. Consequently, a single act which violates *ius ad bellum* might not necessarily reach the threshold of force required to determine the existence of an armed conflict.

Moving on to the *ius in bello*, the law makes reference to 'hostilities' and to 'attacks'. Hostilities can encompass more than single acts of violence, but the latter are usually expected to be part of the situation. As for 'attacks', these are traditionally understood to include an element of armed violence. However, it seems fair to assume that the primary focus was on the fact that the attacks were acts designed to cause physical harm, whether human casualties or physical damage and destruction. As such, it could be argued that cyber warfare which has these same effects, could be considered as equivalent to the type of violence envisaged to exist under the *ius in bello*.

Conclusions

There are three possible ways to categorise cyber warfare with reference to armed conflict:

1. That cyber operations do not meet the requirements to be recognised as armed conflict. In this case, it is not IHL that should be regulating them at all.

However, there are two other possibilities through which IHL may be applicable:

2. Certain types of cyber operations would be equivalent to 'traditional' attacks due to their consequences of casualties and destruction. There may still be a question of intensity

[2] *Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America)*, ICJ Rep. 1986, p.14.

– there is the argument that minor border incidents do not amount to armed attacks or armed conflict. By analogy, a single cyber incident with physical but minor harm, might not qualify as an armed conflict. Consequently, for it to be an armed conflict in the absence of anything other than cyber warfare, one may need to see sustained attacks causing physical harm. For non-international armed conflict, this is even more difficult as there is a higher threshold of intensity. Moreover, cyber operations may present a significant difficulty in identifying the parties.

3. Most likely scenario: unless satisfying the above in terms of consequences, cyber operations do not themselves constitute evidence of armed conflict; however, there may be traditional (kinetic) armed force occurring at the same time. If we already have an armed conflict regardless of the cyber operations, the question now is where the cyber element fits in. In this case, it should be noted that not all conduct during an armed conflict is part of the hostilities. The question then is whether the cyber operations meet the criteria to be considered as hostilities. This is less relevant if the attacker carrying out the cyber operations is a member of armed forces and this is an international armed conflict. However, if this is a civilian in any type of armed conflict or a member of an armed group in a non-international armed conflict, does this mean that the individual is directly participating in hostilities and has therefore lost protection? This will be a case-by-case test, as outlined by the criteria for direct participation, and the subject of a whole new debate.

THE LEGAL REGULATION OF CYBER ATTACKS IN TIMES OF ARMED CONFLICT

Robin Geiß[1]
Geneva ICRC

Résumé

I. Introduction

Bien que le potentiel militaire de l'espace cybernétique (ou cyberespace) commence seulement à être exploré, les États prennent très au sérieux les potentielles menaces que pourraient représenter des attaques cybernétiques. En terme humanitaire, une guerre cybernétique pourrait avoir des conséquences désastreuses, et notamment causer de nombreuses victimes et dommages civils. Techniquement, on peut en effet envisager des attaques sur des systèmes de contrôle aérien, ou sur des centrales nucléaires.

II. L'espace cybernétique, un nouveau champ de bataille

La découverte et l'exploitation de l'espace cybernétique ont ouvert un nouveau champ de bataille. Cet espace est homogène et permet une interconnectivité sans limites ni frontières. Or, les attributs de cette interconnectivité peuvent facilement être exploitées par des cyber-criminels, à des fins d'espionnages, ou pour conduire des hostilités dans le cadre d'un conflit armé. Dans un contexte de guerre, cela signifie que tout ce qui a une interface avec Internet peut être attaqué de n'importe quel endroit de la planète. En outre, les effets d'une attaque cybernétique ne peuvent être limités à sa cible première, mais se répercuteront sur d'autres systèmes ou réseaux, potentiellement civils. A l'heure actuelle, les réseaux militaires dépendent très largement des infrastructures commerciales. L'anonymat qu'offre l'espace cybernétique, grâce à la digitalisation, complique l'attribution d'un acte à un Etat ou à un acteur non-étatique et rend difficile la distinction entre les acteurs.

III. Les contraintes juridiques à la conduite des hostilités dans l'espace cybernétique

En dépit de l'absence de dispositions spécifiques, les règles et principes du DIH existant s'appliquent aux opérations cybernétiques. Cette position est celle établie par le CICR et est largement acceptée. Cependant, il est essentiel de s'assurer qu'aucun vide juridique ne sera laissé. Cette

[1] Robin Geiß is legal advisor at the Legal Division of the International Committee of the Red Cross. The views expressed in this article reflect the author's opinion and not necessarily those of the ICRC.

tâche est rendue particulièrement difficile du fait du manque de pratique des États en matière d'opérations militaires cybernétiques. Il est, en effet, vraisemblable que le potentiel militaire, de même que les impacts humanitaires, ne seront véritablement connus qu'â travers des conflits armés futurs. Néanmoins, les États doivent d'ores et déjà se pencher sur la question de savoir quel seuil devra atteindre une attaque cybernétique pour déclencher un conflit armé. Quel type d'opération militaire cybernétique peut être qualifié « d'attaque » au sens du DIH? Ce débat est crucial, puisque une « attaque » au sens de l'article 49 du Protocole Additionnel I aux Conventions de Genève (PAI) entraîne l'application de différentes règles, en particulier relatives au principe de distinction. La question est alors la suivante: de quelles conséquences le DIH protège-t-il la population civile? Il est admis qu'une attaque cybernétique qui provoquerait la mort ou causerait des blessures ou encore des dommages matériels, est une attaque au sens du DIH. Cependant, il a également été suggéré que le dommage physique inhérent à la notion d'attaque soit étendu à la perte définitive d'avoirs, d'argent, ou d'actions. Des opérations qui auraient des effets de ce type devraient alors respecter le principe de distinction et ne viser que des objectifs militaires légitimes. Il peut être suffisant que de telles conséquences soient prévisibles. Reste les opérations qui ont des conséquences moins tangibles, telle que l'interruption temporaire d'un service en ligne ou d'un réseau. Si le déni de service n'est pas considéré comme une attaque au sens juridique du terme, alors de telles opérations pourraient être conduites de manière indiscriminées, et également à l'encontre d'installations civiles.

De même que toute opération militaire n'est pas considérée par le DIH comme une attaque, toute opération cybernétique ne constitue pas automatiquement une « attaque » au sens du DIH. En revanche, dans le cadre spécifique d'opérations cybernétiques, il convient de porter une attention particulière à l'article 52 PAI, selon lequel la neutralisation d'un objet résultant d'une attaque, peut constituer une « attaque ». La question de savoir si cette neutralisation est réversible ou non pourra alors être décisive.

IV. Conclusion

De manière générale, le DIH s'applique à l'espace cybernétique. Le DIH n'interdit ni n'autorise les attaques sur des réseaux informatiques, mais impose certaines limites relatives à la conduite des hostilités dans ou à travers l'espace cybernétique. L'attaque d'un objectif militaire spécifique, la prise de précautions dans le choix des méthodes et moyens de guerre en vue de limiter les dommages civils collatéraux, sont autant de règles qui doivent être respectées. Néanmoins, il convient de garder à l'esprit que le potentiel militaire de l'espace cybernétique et la pratique des États en la matière n'en sont qu'à leurs débuts. Il n'est pas exclu que des développements futurs révèlent un besoin en terme de réglementation au regard de caractéristiques particulières des opérations et de l'espace cybernétique.

I. Introduction

The interest in legal issues raised by 'cyber warfare' is currently particularly high and still increasing. Cyber warfare and cyber security in general are making headlines in the international media on a weekly basis.[2] The so-called 'Stuxnet' attack against Iranian nuclear installations is merely the most recent example.[3] The military potential of cyberspace is only now starting to be fully explored. States all over the world are taking the potential threats (and possibilities) posed by cyber attacks very seriously. For example, the US Quadrennial Defence Review Report of February 2010 states that:

> *"[C]yberspace is now as relevant a domain for DoD [Department of Defence] activities as the naturally occurring domains of land, sea, air, and space. There is no exaggerating our dependence on DoD's information networks for command and control of our forces, the intelligence and logistics on which they depend, and the weapons technologies we develop in the field. In the 21st century, modern armed forces simply cannot conduct high-tempo, effective operations without resilient, reliable information and communication networks and assured access to cyberspace."*[4]

Clearly, cyber warfare is no longer perceived as science fiction but as a reality that needs to be dealt with. Potentially, the humanitarian impact of cyber warfare could be enormous. Although the cyber attacks against Estonia in 2007 and Georgia in 2008 did not cause grave humanitarian consequences,[5] technically, cyber attacks against airport control and other transportation systems, dams or nuclear power plants appear to be possible. Such attacks would most likely have large-scale humanitarian consequences. They could result in significant civilian casualties and damages. Technical experts seem to be of the opinion that it is only a question of time until such cyber attacks occur. Naturally, a humanitarian organisation like the Interna-

[2] See , 'War in the fifth domain – Are the mouse and keyboard the new weapons of conflict?', The Economist , 1 July 2010. To be found at: http://www.economist.com/node/16478792?story_id=16478792 (last accessed: October 2010).

[3] In October 2010, a new generation of a highly potential computer virus that selectively targets industrial plants built by Siemens was discovered in Iranian Nuclear power installations. It is not yet fully clear what the virus can do or who built it but it is clear that the 'Stuxnet-virus' amounts to a very advanced weapon technology; 'A silent attack, but not a subtle one', New York Times, 26 September 2010. To be found at: http://www.nytimes.com/2010/09/27/technology/27virus.html (last accessed: October 2010).

[4] *Quadrennial Defence Review Report* (February 2010) p. 37. To be found at: http://www.defense.gov/qdr/.

[5] The cyber attacks on Estonia refer to a series of cyber attacks that began April 27, 2007 and swamped websites of Estonian organisations, including the Estonian parliament, banks, ministries, newspapers and broadcasters. The 2008 attacks against Georgia caused certain governmental websites in Georgia to malfunction. See Alex Rodriguez, *Attacks on Estonia Move to New Front*, CHI. TRIB., May 29, 2007; 'Estonia and Russia: A Cyber-Riot', The Economist, May 12, 2007. To be found at: http://www.economist.com/node/9163598

tional Committee of the Red Cross (ICRC) must closely follow these developments and carefully assess the potential humanitarian impact of cyber warfare.

II. Cyberspace as a new war fighting domain

Clearly, as far as computer network attacks, and more generally the conduct of hostilities in and via cyberspace, is concerned, we are not simply discussing the nascence of a new weapon. Cyberspace is opening up an entirely novel war fighting domain; a new man-made theatre of war that is interlinked with the naturally occurring theatres of land, air, sea and outer space.[6] Cyberspace is a homogenous space that provides worldwide interconnectivity without borders. Above all, it is designed for convenience and reliability and it is easily accessible in all quarters of the world.

Notwithstanding their utility, these features can easily be exploited by cyber criminals, for the purposes of espionage or in order to conduct hostilities in the course of an armed conflict.[7] In times of war, interconnectivity means that anything that has an interface with the internet can be attacked from anywhere in the world. In cyberspace launch-to-impact time is reduced to seconds. A cyber attack could be launched from nothing more than a simple cell-phone. Interconnectivity also means that the effects of an attack may not be confined to the actual target. Rather, a cyber attack may have repercussions on various other systems including civilian systems and networks. At least for the time being, military networks remain heavily dependent on commercial infrastructure. In addition, the digitalisation on which cyberspace is built ensures anonymity and thus complicates not only the attribution of conduct to a certain State or non-state actor but also the distinction of actors. In cyber operations, concealing one's identity is the rule, not the exception. Identifying the source, i.e., the machine that is at the origin of a given attack, is difficult and, if certainty is desired, time-consuming.[8] Identifying the fingers on the keyboard, i.e., the person who executed the attack, without additional intelligence, is often impossible. Already in light of this short overview, it appears that reconciling the emergence of cyberspace as a new war-fighting domain with the established humanitarian legal framework is a challenging task.

[6] *Quadrennial Defence Review Report* (February 2010) p. 37. To be found at: http://www.defense.gov/qdr/.

[7] Generally, see Symantec, *Symantec Global Internet Security Threat Report – Trends for 2009* (Volume XV, April 2010). To be found at: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf

[8] Generally see Howard F. Lipson, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues (CERT Coordination Centre, November 2002). To be found at: www.cert.org/archive/pdf/02sr009.pdf (last accessed: October 2010).

III. Legal constraints on the waging of war in cyberspace

As with any new technology, international humanitarian law (IHL) applies to warfare in and via cyberspace despite the fact that the established humanitarian legal framework entails no specific rules dealing with cyber warfare. The law of armed conflict is flexible enough to accommodate new technological developments.[9] This was envisaged already by the so-called Martens Clause, it is implied by Article 36 of Additional Protocol I (AP I), and it has been confirmed by the International Court of Justice when it considered the legality of Nuclear Weapons.[10] The various rules and prohibitions arising, for example, out of the principle of distinction do not depend on the type of weapon or the specific method used. This is the established position of the ICRC and as far as can be seen, this opinion is widely accepted.[11] There should thus be no doubt that fundamental humanitarian rules and principles apply to cyber operations.

However, all that this means is that in times of armed conflict there is no legal vacuum in cyberspace. Whether humanitarian rules need to be adapted to the specific technological features of cyberspace; whether cyber technology can realistically be reconciled with the presumptions underlying the humanitarian legal framework and whether the application of traditional rules sufficiently mitigates the humanitarian impact of new technology remains to be seen. Naturally, if distinction was technically impossible in cyberspace, a legal rule prescribing distinction would be meaningless. Technical experts, however, confirm that distinction, albeit difficult, is also possible in cyberspace.[12] The main problem with the assessment of military cyber operations is that, at least for the time being, visible or readily discernible (State) practice is still scarce. The vast majority of what are colloquially called 'cyber attacks' are network exploitation attacks that are being carried out for purposes of information gathering and espionage. These cyber operations occur outside the context of an armed conflict and they are most effective when they remain unnoticed. In fact, these operations are inherently clandestine and although everyone knows that a great number of such attacks occur on any given day, it is difficult to assess their precise impact and features. However, as far as an overt conduct of hostilities in or via cyberspace with destructive 'real-world' or virtual effects is concerned, hardly any attributable State practice can be discerned thus far. Neither the events in Estonia in 2007 nor the events in Georgia in 2008 were qualified as an armed conflict. Thus, it remains to be seen above

[9] ICRC Commentary, AP I, para.1476.

[10] *Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion)*, ICJ Rep., 1996, p. 226.

[11] See Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework" in: Colum. J. Transnat'l L., Vol. 37, 1999, p.885 atp.890; Michael N. Schmitt "Wired Warfare: Computer Network Attack and *Jus in Bello*" in: *Int'l Rev. Red Cross*, Vol. 84, 2002, p.365 at 365. To be found at: http://www.icrc.org/web/eng/siteeng0.nsf/htmlall/ 5c5d5c?opendocument.

[12] See contribution from Herb Lin in this issue.

which threshold States will consider 'cyber-attacks' as triggering an armed conflict. Most likely, the full military potential and the humanitarian impact of cyber operations will only become visible in the context of a future armed conflict. For the time being it is difficult to assess how realistic or likely the theoretical worst-case scenarios that are contemplated in the literature, e.g., the manipulation of a nuclear power plant via cyberspace, really are.

Computer network attacks, unlike most conventional kinetic attacks, can be designed in a way to only temporarily disable or modify their targets rather than physically destroying them. Temporarily shutting down an electrical power grid via the internet is certainly of lesser impact than bombing it. This has sparked debate about targeting possibilities in and via cyberspace. More significantly, the discussion as to which kind of military cyber operations would qualify as an 'attack' in the humanitarian legal sense is a controversial one, but one of crucial importance. Under IHL only an 'attack' in the sense of Article 49 AP I triggers the various rules that give effect to the principle of distinction, such as Articles 51(2), (4), (5), (6); 52(1), (2) AP I. Therefore, heightening the threshold of what amounts to an 'attack' under IHL automatically curtails the protective scope of these provisions and the principle of distinction in general.[13]

In essence, the discussion about the notion of attack boils down to the question against which consequences of military operations IHL aims to protect the civilian population. It is undisputed that computer network attacks that result in death or injury (including mental suffering) to persons or physical damage to objects qualify as attacks in the sense of IHL.[14] It has also been suggested that – as far as cyber operations are concerned – the concept of physical damage inherent in the notion of 'attack' should be extended to comprise the permanent loss of assets, money, or stock.[15] Operations which may have such effects must comply with the principle of distinction and must only be directed against legitimate military targets. There also seems to be widespread agreement that it is sufficient if the consequences are foreseeable, i.e., they need not necessarily materialise for a certain act to qualify as an attack. Thus, the laying of a landmine already amounts to an 'attack' even if the mine has not yet detonated. What is at issue, however, are operations with less tangible consequences, such as the temporary disruption of certain networks and online services. If such denial-of-service attacks

[13] Notably, the basic rule laid out in Article 48 AP I is broader. It provides that 'in order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.'

[14] Knut Dörmann, *Applicability of the Additional Protocols to Computer Network Attacks*, p. 4. To be found at: http://www.icrc.org/Web/eng/siteeng0.nsf/htmlall/68LG92/$File/ApplicabilityofIHLtoCNA.pdf (last visited October 2010); Michel N. Schmitt, 'Wired Warfare…' *op cit*. n.10 at p.374.

[15] Michel N. Schmitt, *ibid*.

would not amount to an 'attack' in the legal sense, they could be carried out indiscriminately and could arguably also be directed against civilian installations.

Of course, IHL does not rule out each and every adverse effect on the civilian population as a consequence of military operations. Furthermore, not every military operation qualifies as an 'attack'. In times of war, this would simply be unrealistic. The setting up of military checkpoints or even roadblocks, for example, does not constitute an 'attack', even though it causes inconveniences for the civilian population. Economic embargos, espionage and psychological operations including propaganda, the incitement of the enemy population to revolt against its government, ruses of war and the spreading of false rumours or misleading information, are also not considered to amount to an 'attack'.[16] The same holds true with regard to military cyber operations, i.e., not each and every cyber operation automatically constitutes an attack. However, this being said, it can be inferred from Article 52 AP I, the wording of which is not disputed and which explicitly refers to the 'neutralisation' of an object as a possible result of an attack, that the disabling ('neutralisation') of an object is comprised by the notion of 'attack'.[17] Whether the neutralisation of an object would be reversible or permanent can hardly be decisive in this context. Two months without electricity, water or accessible financial assets have dire humanitarian consequences, irrespective of whether the disruption is ultimately reversible or not.

IV. Conclusion

Certainly, various other humanitarian law prescriptions will need to be carefully assessed in view of cyberspace's specific features. On the whole, however, it can be concluded that existing IHL applies in cyberspace. IHL neither prohibits nor endorses computer network attacks *per se* but imposes certain constraints with regard to the conduct of hostilities in and via cyberspace. Parties to an armed conflict are prohibited from employing a method or means of combat which cannot be directed at a specific military objective and they are under an obligation to take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimising, incidental loss of civilian life, injury to civilians and damage to civilian objects. But this being said, it must be noted that the military potential of cyberspace, as well as corresponding State practice, is only starting to emerge. It may well be that future developments will reveal a necessity to devise a set of new humanitarian rules that are specifically tailored towards the particular characteristics of cyberspace and military cyber operations.

[16] Stefan Oeter, in: D. Fleck (ed.), *The Handbook of International Humanitarian Law* (2nd ed.), p. 231.

[17] Knut Dörmann, op cit. n.13 at p. 4.; Michael Bothe, Karl Josef Partsch, Waldemar A. Solf, *New Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949* (1982), p.289.

PANEL 2 – CYBER WARFARE DISCUSSIONS

Rich discussions followed the second panel and focused on the following issues:

1. Geographical application of international humanitarian law

A lawyer from the audience proposed rethinking the question of direct participation in hostilities (DPH) and geographical relevance in the context of cyber warfare. What is the geographical field of application of international humanitarian law (IHL)? For regular warfare, it seems that the concept of 'battlefield' is not a requirement under IHL anymore. Would it be relevant for cyber warfare? To answer the question, several experts agreed to draw a distinction between international armed conflicts (IAC) and non-international armed conflicts (NIAC). One of them argued that, in the context of an IAC, IHL would apply wherever the parties to the armed conflict meet, and serves to regulate the relationship between those parties, and those two parties alone. In this expert's view, there is a need to regulate the relationship between States with IHL wherever they meet because States are such powerful actors. . This also explains why the threshold for IAC is low. On the contrary, the situation and the kind of actors in NIAC are very different. According to him, IHL applies where it is not realistic to apply higher standards. In NIAC, law enforcement would be sufficient to regulate the relationship of the parties to a NIAC outside the battlefield by mere intervention of police force. Therefore, in the context of cyber warfare, IHL would only apply to NIAC geographically, where geographic hostilities occur. Another expert gave a slightly different explanation about the distinction between IAC and NIAC, which related to the area of war. In IAC, parties can conduct military operations on the territory of the warring parties, including territorial waters, air space and the high seas. This territorial limitation is also relevant for cyber warfare. For NIAC, although there has been less doctrine and research on the subject, the *Tadic*[1] case gives us some indications about territorial limitation, that is to say, the territory under the parties' control. This, according to this view, would be the geographical application of IHL. Therefore, if a person launching a cyber attack hides in Belgium, for instance, the question would be: is Belgium a party to the armed conflict? If the answer is yes, IHL would apply in Belgium.

However, another panellist presented a different reasoning: IHL should apply to every person directly participating in hostilities wherever the person is geographically located. Indeed, the question of where a person can or cannot be targeted is a question of jus ad bellum and does

[1] ICTY, The Prosecutor v. Tadic, IT-94-1-AR72, Appeals Chamber, Decision, 2 October 1995

not depend on the type of conflict. Therefore, the geographical location does not make any difference.

In relation to this, the issue of neutrality in the framework of a cyber attack was also raised. For instance, would a computer operation passing through the network of different countries potentially violate the rule of neutrality? If no answer was suggested, the question will surely have to be considered.

Additionally, the response to cyber attacks seems to require clarification. If a cyber attack is not an armed attack, States are prohibited from responding with armed force. However, could they respond with a cyber attack? In this respect, it was emphasized that NATO is currently considering whether a cyber attack could be an armed attack triggering the exercise of the self-defence under Article 5 of the NATO treaty.

2. Are the existing rules of IHL applicable to cyber warfare?

In particular, the principle of proportionality and the principle of distinction were challenged: is it physically possible to apply these principles in a cyber warfare context, and if so, would it make sense? In the view of one of the panellists, there is, for the time being, no other option than applying the existing rules. If the rules are not realistic, then there might be a need to develop the law. However, States are gradually changing the law and we therefore need to wait until State practice with regard to cyber operations in an armed conflict emerges. Another position was to suggest that other branches of international law, such as the international law of telecommunications, might apply to cyber warfare. The aim of IHL is not to regulate as much as possible but to regulate conducts during armed conflicts.

3. Is a cyber attack an armed attack within the meaning of IHL?

On a similar topic, an expert also warned of the danger of considering that a cyber attack is equivalent to armed attack. He argued that IHL was made by the States at a time of physical confrontation and that cyber attacks were not contemplated. He recalled that the mere use of the term ‘warfare’ in ’cyber warfare’ does not necessarily mean that there is an armed conflict within the meaning of IHL. The same question arose with respect to so-called ‘economic war’. When the UN Charter was being drafted, Brazil proposed an amendment to include economic measures in the concept of armed attack. In the end, this broad interpretation of armed attack was not accepted. In the view of the same expert, a similar reasoning applies by analogy to cyber operations: whilst it may have very serious consequences,it is not an armed conflict. This type of ‘warfare’ would not be beyond the law but is not within the framework of IHL, as there is no armed conflict. Another member of the audience added that State practice does not support the application of IHL to cyber warfare. Even in the case of the cyber-attack in Estonia, States did not support the conclusion that it was an armed attack. However, it seems that the existence of an armed conflict depends on the violence of the consequences resulting from the attack. Therefore, the answer might be different if someone takes control of the missile defence of a country and turns it against a country.

4. Destruction of property

A participant expressed concerns about the shift in the definition of the notion of property. In IHL, is the concept of digital objects and intellectual property recognised as 'objects' that can be destroyed? Indeed, intellectual property and digital objects tend to have a growing role and it is important that they are covered by IHL. It seems that there is scope in the Additional Protocols for interpreting more broadly the notion of property to include, in addition to buildings or houses, digital property. However, experts agreed that this issue needs to be thought about.

5. Identifying and marking computers and perfidy

Technically, it would be possible mark computers or other cyber objects, but it appears that there is no obligation to mark military or civilian computers, even if it would certainly help. However, according to one of the panellists, it raises another important issue concerning cyber attacks as perfidy. For example, a cyber attack could be used to wrongly identify, to hide behind, or make something look like it is protected, and then be used to engage in a lethal attack. In this case, the cyber operation might violate the perfidy prohibition.

Session 3
Remote-Controlled and Autonomous Weapons Systems

Chair person: **Stéphane Kolanowski,** *ICRC Brussels*

REMOTE-CONTROLLED WEAPONS SYSTEMS AND THE APPLICATION OF IHL

Jack Beard
University of California, Los Angeles

Résumé

Les systèmes d'armement commandés à distance et l'application du Droit international humanitaire (DIH)

En moins de dix ans, les systèmes d'armements commandés à distance ont dépassé le stade expérimental pour faire aujourd'hui partie intégrante des opérations militaires modernes. Or, cette évolution technologique modifie la conduite des opérations militaires, le fonctionnement des institutions militaires, et même les objectifs des conflits armés. Partant de ce constat, l'orateur a choisi de se concentrer, dans sa présentation, sur les questions fondamentales qui se posent alors au regard du DIH.

*L'utilisation croissante de Véhicules aériens non-pilotés (UAV) pour des assassinats ciblés suscite de nombreuses critiques. Le conseiller juridique du Département d'État des États-Unis, Harold Koh, a eu l'occasion de se défendre sur le sujet lors de la conférence annuelle de la Société américaine du Droit international (ASIL) le 25 mars 2010. Dans son allocution, il met en avant quatre séries objections qui reflètent bien le débat juridique autour de ces nouvelles capacités. Ces objections concernent: (1) le ciblage de leaders spécifiques, (2) les assassinats illégaux et extrajudiciaires, (3) la violation de l'interdiction américaine d'assassinat (*US assassination ban*), et (4) l'utilisation d'armes de haute technologie de manière générale.*

Dans ses remarques, Herald Koh souligne en particulier l'importance fondamentale de respecter les principes de discrimination et de proportionnalité. Or, c'est dans ce contexte que la "surveillance continue" rendue possible par les UAV devient cruciale pour le DIH. Ces nouvelles capacités permettent en effet un contrôle renforcé de la mise en oeuvre de ces principes, et une veille plus systématique des dommages humains dans les conflits armés actuels, notamment en Afghanistan. Elles offrent une plus grande transparence et donc des possibilités plus grandes d'engager la responsabilité des individus dans les opérations de ciblage.

En outre, les systèmes commandés à distance peuvent être utilisés en vue d'affaiblir, voire d'éliminer, certains éléments souvent avancés pour justifier des dommages civils collatéraux, tels que l'absence de craintes concernant la sécurité des équipages lors du lancement d'une attaque, les capacités de ciblage rendues possibles par l'environnement virtuel dans lequel opèrent les UAV, ou encore les capacités des UAV de tourner autour d'une cible pendant une longue période.

Cependant, la sécurité des personnes qui contrôlent ces systèmes peut poser certains défis au jus ad bellum. *En particulier, l'absence de risques pour le pilote et son équipage soulève quelques inquiétudes quant à l'allègement des restrictions auxquelles un État est confronté dans sa décision d'engager ou non la force armée. Par ailleurs, si ces systèmes offrent de sérieuses perspectives d'un meilleur respect des principes clés du DIH, leur prolifération au sein des acteurs étatiques, mais aussi non-étatiques, risque d'avoir des conséquences importantes pour les conflits armés futurs, de même que pour le DIH. Ainsi, à l'instar de tous les systèmes d'armement, le développement de systèmes commandés à distance génère certes de nouvelles capacités, mais également de nouvelles vulnérabilités, tout en plaçant une demande accrue sur les biens dans l'espace extra atmosphérique et cybernétique.*

Les capacités limitées en terme de bande passante, ainsi que le progrès constant des systèmes d'intelligence artificielle, sont également susceptibles d'augmenter la pression sur les États. Cela pourrait les conduire à réduire au maximum leur dépendance à l'égard de nombreux systèmes d'armement commandés à distance, au profit de systèmes entièrement autonomes. Une telle évolution soulèverait alors une série de nouvelles considérations juridiques.

In less than just one decade, remote-controlled weapons systems have moved from limited or experimental applications to become an integral part of modern military operations. These so-called 'unmanned' (or more accurately 'uninhabited') systems, especially unmanned aerial vehicles (UAV), are refashioning the conduct of military operations, the functioning of military institutions, and even the objectives of armed conflicts themselves. As they continue to evolve and variants multiply, unmanned systems are allowing military forces to project power on an unprecedented scale and have introduced a new era of remote-controlled killing. In so doing, they are raising profound questions for international humanitarian law. However, these technologies may also be unexpectedly and somewhat ironically giving unprecedented traction, transparency and relevance to *venerable jus in bello* principles protecting civilians from the effects of hostilities – and may ultimately force States and individuals to confront revitalised and new duties to avoid causing harm to civilian populations.

The use of increasingly sophisticated UAVs for the 'targeted killing' of individuals has prompted much debate and criticism, including a recent report by the United Nations Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions that was highly critical of US policies in this area. In a much-awaited speech on March 25 at the 2010 Annual Meeting of the American Society of International law addressing, *inter alia*, the status of armed UAVs and targeting killing under international law, Mr. Harold Koh, the Legal Adviser at the US Department of State outlined and discussed four sets of 'objections' to the US targeting practices made possible by UAVs. His remarks are a useful starting point for reviewing the legal implications of new, unprecedented, remote-controlled or 'virtual' targeting capabilities. While not suggesting that a comprehensive review of the legal issues raised here can be conducted in my brief remarks, I would nonetheless like to restate the questions that form the framework for this continuing debate, beginning with the four raised by the US Legal Adviser:

- Objections regarding the targeting of particular leaders;
- Objections to 'unlawful, extra-judicial killing';
- Objections based on violation of US ban on assassination;
- Objections to the use of high-tech weapons generally.

These questions were answered in fairly short order by Mr. Koh in his remarks on March 25. Several important subsidiary or related questions were not *directly* addressed by Mr. Koh, although some answers to those questions were suggested or implied by his descriptions of relevant US. policies. These subsidiary or related questions include:

What is the nature of the conflict with Al Qaeda and can attacks on a transnational terrorist network be justified on the basis of self-defence?

Where may attacks take place? Are there any boundaries or geographic limits to these attacks?

If the conflict with Al Qaeda is an 'armed conflict' for purposes of international humanitarian law, what is the legal status of Al Qaeda 'members'?

What is the legal status of those who provide 'material support' to Al Qaeda? If this is an armed conflict, what constitutes 'direct participation in hostilities'? How are these questions answered for purposes of targeting? How are names of targeted persons vetted?

What answers or approaches to these questions are suggested by US. courts construing relevant US statutes? (Note in particular the recent decision of the US Circuit Court of Appeals for the District of Columbia in Al-Bihani v. Obama.) What, if any, tensions with international law may be generated by these USapproaches?

Finally, who is allowed to pilot the UAVs used in attacks and what is their status?

In his remarks, Mr. Koh correctly noted the overarching importance of observing the principles of discrimination and proportionality. He stated 'In my experience, the principles of distinction and proportionality that the United States applies are not just recited at meetings. They are implemented rigorously throughout the planning and execution of lethal operations to ensure that such operations are conducted in accordance with all applicable law.' In concurring with Mr. Koh's remarks, I cannot overemphasise the importance of ongoing changes in the military legal profession in the United States. Since the Persian Gulf conflict in 1991, Judge Advocate General (JAG) officers have been achieving greater and greater relevance to every aspect of the conduct USmilitary operations.

It is in the context of serious legal oversight of the observance of discrimination and proportionality and the heightened scrutiny of civilian casualties in current armed conflicts (particularly in the ongoing conflict in Afghanistan) that the 'persistent surveillance' made possible by UAVs becomes so important for international humanitarian law. These capabilities offer the possibility of more transparency and accountability in targeting operations than ever before. For example, video data from unmanned systems can now indicate the presence of civilians at a target *before* an attack, show their presence *during* an attack, and then leave a record of the performance of military personal to be reviewed *after* the attack. It is thus not surprising that such data was cited in a recent US military report that found the military personnel operating a UAV were at fault in failing to properly communicate information to the ground force commander about the presence of civilians in a convoy that was attacked by US forces in Uruzgan Province in Afghanistan. Based in part on the UAV-generated 'full-motion video' record of the attack, the report concluded that the UAV operators had 'deprived the ground force commander of vital information' which indicated the presence of civilians in the convoy.

In addition to the transparency that comes with the persistent surveillance provided by unmanned systems, many of the factors that have been cited as excuses or justifications for incidental civilian casualties in the past are profoundly affected or even eliminated by these systems. These factors include the absence of any concerns regarding the safety of air crews in launching attacks, the improved targeting capabilities made possible by the virtual environment in which UAV personnel operate (as opposed to the constraints confronting human aircrews in conventional aircraft), and the extra-human capabilities of UAVs to loiter over targets for a long period of time.

The safety of the humans who operate unmanned systems may, however, present challenges for international law in regulating recourse to force. In particular, the absence of any threat to human pilots and aircrews raises concerns about the diminished restraints States may face in deciding to engage in the use of force – and fears that these developments may undermine the meaningful application of the *jus ad bellum*. In addition, while these systems offer serious prospects for improved compliance with key principles of the *jus in bello*, the proliferation of these weapons among both States and non-state actors is likely to have important consequences for both future armed conflicts and international humanitarian law. As with all weapons systems, unmanned systems are generating not only new capabilities but also new vulnerabilities, while placing more demands on assets in outer space and cyber space. Limited bandwidth capacities, combined with continuing advances in artificial intelligence systems, are also likely to place increasing pressure on States to decrease their reliance on many remote-controlled weapons systems in favour of fully autonomous ones, raising a new set of legal considerations.

ROBOTS IN THE BATTLEFIELD: ARMED AUTONOMOUS SYSTEMS AND ETHICAL BEHAVIOUR

Ronald Arkin
Georgia Institute of Technology

Résumé

Tout d'abord, il convient de noter que, en matière de robotique militaire, non seulement les systèmes commandés à distance continueront à être utilisés, mais des systèmes autonomes vont inévitablement se développer. La technologie est d'ailleurs déjà très avancée. Un « système autonome », dans un contexte militaire, est un système capable de choisir et de désigner une cible, d'engager le combat et même éventuellement d'évaluer les dommages potentiels. L'utilisation croissante de cette technologie à des fins militaires montre bien qu'il est essentiel de réfléchir aux moyens de rendre ces machines capables de se comporter de manière éthique. Théoriquement, une alternative serait d'interdire cette technologie, mais un tel scénario ne semble pas réaliste.

La première question qui se pose alors est la suivante : quelle peut-être et doit être l'utilisation de la robotique dans le cadre d'un conflit armé ? Le monde militaire voit dans cette technologie plusieurs avantages et recherche, entre autres, un plus grand rendement et une meilleure efficacité tout en mobilisant un minimum de soldats. Comment accroître les capacités d'un combattant ? Comment faire en sorte qu'un soldat puisse voir et tirer plus loin tout en étant mieux protégé ? Un autre aspect est celui de la protection des non-combattants et des objets à caractère civil. L'armée, en particulier américaine mais pas seulement, va très loin dans sa réflexion quant à l'utilisation de cette technologie. La question qui se posera ensuite sera celle de savoir si le droit existant est applicable au développement de ces systèmes. Est-il pertinent ? Étant donné le rythme d'avancement de cette technologie, il est essentiel que les spécialistes se penchent dès à présent sur le sujet.

Dans le cadre d'un projet de recherche, l'auteur a été amené à examiner les capacités de performance des robots. Par exemple, des robots pourraient ils être plus performants que des êtres humains en matière de dommages collatéraux résultant d'une attaque ? Étant donné qu'ils sont déjà plus forts, plus rapides et plus habiles, ils pourraient potentiellement se comporter de manières plus humaines que des humains ? Il apparaît également que, techniquement, des robots pourraient rapporter des informations sur le comportement éthique ou non des soldats sur le champ de bataille, ce qui pourrait avoir un effet positif général sur l'attitude des soldats. Un des objectifs du prototype de logiciel réalisé dans le cadre du projet était d'incorporer dans

le système certaines règles d'engagement et principes de droit international humanitaire (DIH), tels que la nécessité militaire, la proportionnalité, et la distinction. Selon l'auteur, des robots autonomes pourraient mieux se conduire sur un champ de bataille que des êtres humains, s'ils sont correctement programmés. En effet, ils sont, par exemple, capables d'agir avec retenue, ou d'attendre véritablement le moment où l'intention hostile est déclarée avant d'engager la force. En outre, la colère et la frustration sont des caractéristiques propres aux humains qui sont absentes de ces systèmes. Ainsi, il apparaît qu'un système autonome pourrait avoir un effet positif sur la conduite des hostilités et le respect du DIH.

En revanche, il est évident que ces systèmes ne doivent pas être utilisés dans tous les cas de figure. S'ils peuvent sembler adaptés à des conflits inter-étatiques et dans le cadre de missions spéciales, ils sont par exemple inappropriés pour des opérations de contre-insurrection. En aucun cas de tels systèmes autonomes ne doivent remplacer le soldat; ils doivent plutôt l'assister dans des missions bien spécifiques comme des opérations contre des snipers.

*Le développement de l'autonomie est bien sûr loin de faire l'unanimité. Un des arguments les plus sérieux formulé par certains à l'encontre contre cette évolution technologique est celui de l'établissement de la responsabilité. Les êtres humains sont responsables devant la loi, pas les robots. Cela signifie que des soldats ou des commandants devraient être responsables pour le déploiement de ces machines. Un autre argument est celui d'une guerre sans risque (*risk free warfare*), au moins pour l'une des parties au conflit. En outre, la prolifération est un problème de taille, de même que la question des dérives potentielles dans l'utilisation des systèmes autonomes.*

To some extent, we are here to ask for help. Hopefully, you will see why by the end of this talk. I do not have the answers but I surely have a lot of questions about what is coming downstream in military robotics. Another thing I will try to convince you of is that, not only will remote-control systems continue to be used, but autonomous systems are inevitable. Some will contend that it is not necessarily a bad thing, and I am one of these. I will also explain why.

There are two solutions: one is finding ways to make autonomous systems behave ethically as we move forward, the other is to consider banning them. Recently, I was in a meeting organised by the International Committee of Robot Arms Control, which decided to request a ban on this technology. I am not sure it is advisable or needed, but it should be considered. Additionally, what exactly a ban would mean is another thing to look at.

I have been a roboticist for 25 years. I do not only do military work, and if I do, then only unclassified research. This is why I can speak freely with you today about anything and everything that I do. I have been working on autonomy and autonomous systems since my Ph.D. for a variety of programmes, defence projects, agencies, etc. Currently, I am working under the Army Research Laboratory Program and Navy Program, studying how teams of robots can collectively work together, for example, to build surveillance reconnaissance working with small crawlers and flyers. You would be surprised to learn what the military is exploring in this particular case. And it is only the unclassified work that is going on in my lab.

What I will report today is the result of the smallest grant I ever received from the Department of Defence (DoD). The army research organisation in the DoD granted me a three year program to study the application of ethics in these autonomous systems. In my view, this is probably one of the most controversial, and will potentially have the greatest impact, of all the research projects I have conduced. This is what I will be talking about today.

I share with you the view that we should not have wars, but we do nonetheless. Assuming that wars will continue, the question is therefore the following: what, if anything, is the appropriate use of robotics technology in this particular space? There are many reasons why the military is exploring it. One is force multiplication: how can we do more with fewer soldiers? Another thing is extending the battle space, finding how we can fight over much larger areas than we did before. This means also larger areas literally, such as coast lines with Broad Area Maritime Surveillance (BAMS). A third reason concerns individual war fighters: how can we provide them with the ability to see and strike further? How, for example, can they look around the corner without putting themselves at risk while around the corner? Robotics technology is one mechanism by which it can be done. Last but not least, the notion of reducing casualties is also important. But how can we potentially use technology to protect non-combatants and non-combatants' property?

There are many existing platforms:

- The South Korean robot, which is already the second generation, is intended for deployment in the demilitarised zone (DMZ) and has a fully autonomous capability. It provides either an autonomous lethal or a non-lethal response with an automatic mode capable of making the decision on its own.
- The Roomba maker (iRobot) provides Packbots, which are typically used for explosive ordnance disposal and not threatening tasks, but have also been equipped with tasers, less-than-lethal weapons, as well as with the MetalStorm system, which is one of the more lethal systems in the 'short near' space.

- The SWORDS platforms, one of the middle platforms, have recently been replaced by a system called MAARS which has been designed from the bottom up to have major weapons developments on the ground.

Other countries such as Israel are leaders in the area as well. China, Russia and a number of other nations have also programmes, unmanned aerial vehicles and unmanned systems. Not all systems are armed but there is a logical progression, which leads to the eventual deployment of these things.

The military is very far thinking in their use of this technology. The US DoD has an Unmanned Systems Integrated Roadmap which goes from 2009 to 2034, and is starting to get traction with the ethical argument. The Roadmap says that *'the decision to fire will not likely be fully automated until legal rules of engagement and safety concerns have all been thoroughly examined and resolved'*. However, it does not say that there will never be fully autonomous engagement of targets. At this point, it is important to note that, by autonomous systems, I mean the ability of a system to choose, designate, engage, and even do battle damage assessment afterwards without human confirmation. I am not talking about moral agency or free will. This is a working military definition. From the US Air Force, the Unmanned Aircraft Systems Flight Plan (2009-2047) states that: *'authorising a machine to make lethal combat decisions is contingent upon political and military leaders, resolving legal and ethical questions... Ethical discussions and policy decisions must take place in the near term rather than allowing the development to take its own path apart from this critical guidance'.* This is important. To me, this is asking for help. I am trying, with many of my colleagues, to engage international discussions on this particular topic. Does existing law fit and govern the development of these systems? Maybe it does, maybe it does not, but it would surely be useful to find out before it is too late, especially when looking at the trajectory of these systems.

This is my conclusion: lethal autonomy is not only inevitable, it is already here. We talked about cruise missiles, there is also the Navy Phalanx system, which automatically engages when in automode operation and is on the Aegis-class Cruisers. It has recently been deployed in the Greenzone in Bagdad, Iraq, to protect against mortar shells as these come in. Turn it on and it will strive to shoot them out of the sky. Patriot missiles, fire-and-forget systems and even landmines fit a definition of autonomous robotics to some degree. Anti-personnel landmines are considered illegal or at least immoral depending upon whether you are a signatory of the Ottawa Convention, because they do not discriminate effectively. But the point is that certain systems, such as anti-tank mines which can listen acoustically and/or recognise a visual signature, are discriminatory. If you place them out there, they can engage fully autonomously. They are robots by most roboticists' definition, even though they may not be mobile.

The notion of a human in a loop is also changing. The Air Force is now referring to 'humans on the loop' rather than 'in the loop'. The Army refers to it as a 'leader in the loop'. In any case, one thing remains clear: there will always be someone in the command structure deploying the system. One of the aspects that makes autonomy inevitable, is the tempo of warfare which is increasing so dramatically that human decision making is no longer feasible in many situations. Things happen too fast and that forces autonomy towards the 'tip of the spear'. Imagine a UAV radio link breaks down. What is the system supposed to do? Right now, it just goes around in a circle or returns to base, hoping to try to recover a link, but the mission is aborted. In other circumstances, the system will have to have autonomy to be able to complete the mission, given an enemy that may be more effective in disrupting battlefield communication. The only possible prevention is by international treaty or prohibition. I am not saying you should do this, but you should definitely talk about it.

The premise of the research I was asked to do was to explore whether robots could outperform soldiers with respect to collateral damage. Could they be ultimately more human than humans? Robots are already stronger, faster and smarter than us in many cases. The International Committee of the Red Cross (ICRC), more than any other organisation, should know that we do not treat each other well in the battlefield. Therefore, it is, in my opinion, a relatively low bar to create autonomous systems that can perform more ethically in the battlefield. Part of this research program was to program a robot for the right of refusal of an order. The military was not particularly happy about that. But it can also provide on-the-ground reporting on the ethical behaviour of soldiers which may have the ability to cause human soldiers to behave better. What we tried to do in our prototype software was to incorporate international humanitarian law and rules of engagement which are required to be consistent with that.

How can we make the systems comply with the laws of war and the rules of engagement? To convince you again of the weaknesses of human soldiers, there is a survey from 2006 on mental heath of soldiers returning from Operation Iraqi Freedom (2005-2007). The statistics are really disturbing. For example, 17% of soldiers and marines strongly agreed that all non-combatants should be treated as insurgents, over a third of reported torture should be allowed, etc. The numbers are very significant. It is hard to examine the intent of a particular human being. We have troops now in Afghanistan that have been accused of deliberately killing civilians for sport and trophy-taking, which are war crimes. But atrocities happen in all wars and conflicts.

These are some of the reasons, and I believe that an autonomous system can avoid much of the associated difficulties.

This is the question I ask my colleagues: how can we use technology to reduce the impact on non-combatants through the use of autonomous systems? One answer is not to use them at all, which, if otherwise left unchecked, cause me to seriously worry about the consequences. How can we ultimately make ethical robotic autonomy occur? This is my underlying thesis: the key word is 'ultimately'. It may take 10, 20, 30 years to get to this particular state, but it will require a sustained research effort by a very large community to address the extreme difficulty of discrimination and recognition of *hors de combat* in many sets of mission circumstances. However, if we establish the benchmark as human performance in the battlefield, and we exceed that, then that translates into saving non-combatant lives and civilian property. I do not make any claim that these systems can be perfectly ethical and will perform correctly in each and every set of circumstances. However, I do believe it could be beneficial and feasible in a number of situations our soldiers are confronted with. These are indeed situations which no human being has ever been designed to function in, and it is progressively becoming worse as the battlefield tempo increases. Better behaviour in humans does not always occur by providing them with abstract rules and ethical training, especially in stressful combat situations.

I also believe that these systems should not be used for all sets of circumstances. For example, I do not believe that they should be used in counter-insurgency operations, but rather for interstate warfare, and only for use in specialised missions. These are not one-on-one replacements for soldiers, but rather highly specialised devices to conduct special types of missions, working alongside soldiers more like dogs or mules, for example in building clearing or room clearing operations, counter-sniper operation, etc. They should serve alongside war fighters, not as a replacement. From the military point of view, this deals with the notion of what is called the 'war fighter ethos' and is why people sign up to join the military in the first place.

I do believe that future autonomous robots may be able to perform better that human under battlefield conditions for several reasons, which includes their ability to act conservatively. They can assume risks on behalf of non-combatants. Indeed, soldiers are supposed to do this. It is an easy thing to say but a very hard thing for people to do. Robots can do this. They can wait to make certain that either hostile intent or hostility is exhibited. Ultimately, they will be able to see in the battlefield much better than a human can. We can also remove anger and frustration from their performance. The scenario fulfilment problem can also be avoided with the advent of network-centric warfare and the global information grid. More information will be available from an 'internetted' battlefield than any human being could possibly digest. As such, if it is processed correctly and appropriately, I believe better decisions can be made by computers. This is why we use them for strategic planning. Conceivably, these can be moved down to lower levels as well. Additionally, and as mentioned before, they can affect the behaviour of individual human soldiers in the battlefield.

You might imagine that there are a few people who think that it is a very bad idea. There are several arguments against autonomy:

- One of the most serious arguments is the establishment of responsibility. Human beings are responsible, not robots. We work with human soldiers or commanders to accept the responsibility for the deployment of these things. But it is still a daunting problem, especially as autonomy moves more and more forward.
- There is also the *jus ad bellum* argument, which reflects the lowering of the threshold for entering into warfare. But to me, this is in common with any asymmetric advances in technology and not only with regard to autonomous systems. The answer would be to freeze military technology where it stands, and I do not think this is going to happen.
- The notion of risk-free warfare also advocates against autonomy. Is it unjust? Not much discussion has been given to it yet, and the ICRC is surely an interesting body to discuss this capability.
- The effect of squad cohesion, which is the 'band of brothers' effect. You put a tattletale in the middle of your squad, and you may behave differently and affect the way the system performs.
- The notion of 'winning hearts and minds', which translates into the following question: if your parents were killed by a robot, how would you react?
- Proliferation is a serious concern. An admiral at one of the meetings at the Royal United Services Institute (RUSI) expressed concerns about the proliferation of autonomous systems for the London Olympics. Going to RadioShack and mounting a cell phone on a model R/C aircraft and packing it with explosives potentially has very dangerous uses. UAVs with explosives were also used by Hezbollah in one of the Israeli conflicts.
- Finally, the notion of mission creep is sometimes mentioned. It refers to systems being used for things other than the one they were intended to be or were designed for.

What we chose to represent in the system are the hallmark characteristics of the Geneva Conventions and Just War theory: military necessity, making sure that they do not inflict unnecessary suffering, proportionality and the ability to deal with discrimination.

We have used action-based machine ethics, which is a branch of the Artificial Intelligence (AI) community dealing with obligations, prohibitions and permissions. It translates, in a bounded morality sense for the particular situation at hand, the applicable laws of war and rules of engagement, not the entire Geneva Conventions. You have to be concerned with what you are dealing with at any particular point in time. There are different things I am addressing in this research, such as the design of software architecture for intelligent machines. We can show that there is never intent to target a non-combatant. We try to follow and set up the principle of double effect, which is the toleration of the evil associated with the killing of civilians and destruction of civilian property, as a consequence of a military good. The principle of double intention is pursued above and beyond that which actually says that we have to actively pursue the minimisation of collateral damage and I am confident that a robotic system may be able to better calculate, specifically regarding proportionality. The bottom line is: you can take a position where these systems can 'first do no harm' as opposed to a 'shoot first ask questions later' under this set of circumstances.

Before I conclude, I would like to go through four important scenarios.

(1) In the first scenario, the American military recognised, with an armed predator, that there were 190 Taliban at a cemetery, in range of attack. Hellfire missiles could have been engaged. They called lawyers at the Pentagon, who eventually told them not to do it, as the rules of engagement provide, in short, that a cemetery should not be targeted, unless there is a manifest hostility. This is technically extremely easy to do. You can establish GPS coordinates for the locations of cemeteries and program the systems to engage only if, for example, the Taliban start shooting at the system.

(2) The second scenario deals with legitimate targets and *hors de combat* status. Insurgents were planting roadside improvised explosive devices. Near the end of the scenario, there is a wounded man lying beside the truck. The gunner recognised that this target was *hors de combat*, but he was commanded to move the cross airs back, despite his intention to try to destroy the war materiel, which was a legitimate target. Eventually, he did shoot this wounded man. The real thing I would like to point out is the distance aspect which is fundamentally different than if someone has commanded the individual to walk up and shoot him in the head. This is a manned system. I asked a Judge Advocate General (JAG) lawyer if he would want a robot to take that shot and he said no. I would like to be able to create systems that can refuse those particular orders better than a human in this situation.

(3) The Samsung Techwin system is developed and deployed in the demilitarized zonein Korea. In this third scenario, there is a military demarcation line, it is marked for civilians to stay away and it says that if you cross the line you will be shot. They have created a robot that detects people five or three kilometres away (day and night). But we would also like to be able to encourage and recognise people to surrender under such circumstances if possible, unless they happen to be conceivably the North Korean army coming across the DMZ.

(4) Finally, I would like to test counter-sniper operations. There are robots in Afghanistan and in Iraq which have sensors which can localise a target, slough a gun through a particular window, can also do muzzle detection, and point the weapon right where a sniper happens to be. A human being has to push a button correctly to allow that to occur; either the human being will not pay attention and just push the button or the sniper

> will move in the meantime. That person is on the hook for negligence if it happens to be a non-combatant in those circumstances. There are likely to be better ways to address this problem.

These are the a few examples of things that push autonomy forward, and we have implemented many scenarios in our software system. But there are far more questions than there are answers. This is also not to say that it will be fielded anytime soon. The real question is whether research in and deployment of lethal autonomous systems should be pursued or not.

The last thing I would like to put to you relates to the Martens clause. On the ICRC website, it says that weapons which violate dictates of the public conscience may also be prohibited on that basis alone. In fact, no weapons have ever been prohibited on this basis. Therefore, there are two options: either you remove it or you try to prove it. The point is that many people find it abhorrent to think that an autonomous system could be fielded and take human lives. If you are going to consider a ban, this might be an appropriate strategy. Technically it might however provide greater persistence and other military-relevant capabilities. The problem, however, faced by humanitarian lawyers is that there is no accepted interpretation of the Martens clause. If you cannot use it, why is it there?

In conclusion, I would like to say we have to be made aware of the potential and current use of this emerging technology. Let's be proactive. You did it with blinding lasers. You came up with policies for that. So why stop there?

AUTONOMOUS WEAPONS SYSTEMS AND THE APPLICATION OF IHL[1]

Daniel Reisner

Formerly Israel Defence Force (IDF) International Law Department

Résumé

*Après avoir présenté trois anecdotes professionnelles relatives aux systèmes (d'armes) autonomes, l'orateur s'est concentré sur le concept du ciblage en DIH ("*targeting*"). Les règles de DIH existantes sont-elles applicables à des robots en matière de* targeting *? Afin de répondre à cette question, il convient de déterminer, d'une part, les règles applicables aux systèmes autonomes et, d'autre part, qui est responsable en cas de violation ?*

Lors de la conduite d'une attaque, trois règles fondamentales doivent être observées : (1) la licéité de l'arme utilisée, (2) la licéité de la cible, et (3) la proportionnalité entre l'avantage militaire escompté et les dommages collatéraux potentiels. Concernant la responsabilité des commandants, trois principes doivent être soulignés : (1) celui qui agit est responsable de ses actes, (2) il n'y a pas de défense d'ordres supérieurs, (3) il existe un concept de responsabilité des commandants en sus de la responsabilité de l'auteur. Ces règles ont été développées sur la base de plusieurs hypothèses, et notamment en fonction (1) d'une certaine éthique ou morale, (2) de la reconnaissance des capacités et faiblesses de l'être humain, (3) de la limite des équipements militaires, ainsi que (4) de l'existence de standards minimum requis par les organisations militaires en terme de formation, d'exécution et de supervision. Cependant, aucune de ces hypothèses de départ n'est pertinente en matière de systèmes d'armes autonomes. En effet, l'appréhension d'une situation de même que les capacités d'analyse d'un robot sont différentes de celles d'un être humain. En outre, il est probable que le commandant d'un robot n'aura aucune idée des capacités exactes de celui-ci.

Face à ce constat, la solution est de tenter de rendre ces systèmes autonomes techniquement compatibles avec les principes de DIH susmentionnés. A cette fin, il est essentiel de comprendre la manière dont les humains prennent les décisions. Si on considère le principe de distinction, trois caractéristiques permettent de distinguer un combattant ennemi d'un non-combattant : un élément physique tel que le port d'un uniforme et d'une arme, un élément comportemental, et un élément géographique relatif à sa situation par rapport à l'objectif militaire. Malgré le défi technologique que cela représente, il apparaît que des machines pourraient être programmées afin de respecter ses trois caractéristiques. Reste à savoir s'il y aura la volonté de le faire, étant

[1] This contribution has been written on the basis of the audio recording of the Colloquium and has not been revised by the speaker.

donné le coût et la complexité de la manoeuvre. Si on examine à présent le principe de proportionnalité, il est nécessaire d'établir une formule permettant d'évaluer la proportionnalité entre l'avantage militaire et les dommages collatéraux, et ce afin de pouvoir programmer le robot. Ainsi, le robot qui interviendra directement sur le champ de bataille devra être capable de distinguer et d'appliquer le principe de proportionnalité. Quant au principe de la responsabilité des commandants, les difficultés s'annoncent nombreuses. Qui engagera sa responsabilité si la machine est défaillante ? Le commandant, bien qu'il ait respecté toutes les instructions du manuel du robot ? Le fabriquant du robot ?

A cet égard, l'auteur a souhaité apporter une suggestion. Il s'agirait de créer une classification pour les systèmes d'armes autonomes. Catégorie A serait, par exemple, un système muni de capacités sensorielles restreintes et de capacités de prise de décision limitées. Ces robots ne seraient pas capables de réellement distinguer et ne pourraient donc être déployées que dans certaines situations, par exemple dans des zones de combat où il n'y a pas de civils. En revanche, la catégorie C serait une combinaison de capteurs sensoriels innovants et du meilleur cerveau qui pourrait être introduit dans un système. Un tel robot dépasserait les capacités humaines sensorielles et de prise de décision. La catégorie B se situerait entre les deux. Ainsi, si un robot était déployé dans une zone de combat autre que celle prévue initialement et conformément à sa catégorie, son déploiement constituerait une violation du droit. En effet, comment engager la responsabilité des commandants pour le déploiement d'un système dont il ne connaît pas les limites ? Si, en revanche, celui-ci est formé aux classifications, alors il devient plus facile d'engager sa responsabilité pour une mauvaise utilisation de la machine dans une mauvaise situation. Si cette proposition n'est qu'une ébauche, l'auteur souligne qu'il est urgent de se pencher sur ces questions : il est vital de s'assurer des règles pertinentes avant que ces équipements autonomes ne soient déployés sur le champ de bataille.

I want to start with three short anecdotes:

(1) When I was a military lawyer, I participated in a business mission in Germany. One of my colleagues on the mission did not pay their entire hotel bill. Back in Israel, I received a letter from the hotel saying that one of the persons in the group failed to pay the extras. The letter ended with the following sentence: *'This is an automatic letter sent by the computer of the hotel. If you pay now, we will not inform our management. Otherwise, we will inform the management, but lawyers will be involved and the price will go up'.* I suddenly realised that if the computer had, for example, made this public, it could have committed an act of liability. It would then have been interesting to figure out who would be responsible for this act.

(2) During one of the Israeli operations in Lebanon in 1996, there was an unbelievably unfortunate tragedy: Israeli, firing back at Hezbollah positions, hit the UN position in Qana. There were a few hundred civilian refugees in the Qana camp and about 90 were killed during the counter-battery fire. The UN set up a committee to find out if the fire was intentional or not. The UN camp commander had claimed that it was intentional because the Hezbollah squad ran toward his base after firing, to take refuge. The commander led them into the base and hid them there. When the firing started and hit the base, he thought that the Israelis must have seen Hezbollah running into the base, and therefore attacked it on purpose. His proof was that there was an Israeli unmanned aerial vehicle (UAV) flying above the area all the time. The reasoning of the UN commander was that, because of the UAV, the Israelis had seen the UN base, therefore they knew, and because they knew, the attack was intentional. What they did not know is that UAVs cannot see anything. They have very limited vision capability, especially that particular model of UAVs although this has improved. We actually discovered that the UAV operator first saw the base only one and a half hours later, after being told to *'search for the fire, search for the fire'.*

(3) 27 years ago, I was an infantry soldier in the Israel Defence Forces (IDF) and went to Lebanon during the first Lebanon war. My job was to guard a base at night, and during the day, I had to check Lebanese workers going to Israel to make sure that they were not terrorists. After two weeks, they asked me to take responsibility for the squad in the base and I became commander of the squad. One night, the landline rings. The landline is the real military line, and it never rang before. The general commander on the line informs me that there is a suicide squad on their way to the base. What do I do? I had not been trained to defend a base against suicide squad in the middle of the night in Lebanon. I woke up all the guards; we took all the ammunitions from the bunker, doubled on every position, prepared everything possible for an attack and waited. We waited for hours and hours. At some point, a Lebanese car stops. Four Lebanese men get out of the car and say that there is a pregnant woman in the car who is about to give birth. They knew that I had an ambulance and wanted me to evacuate her to a hospital in Israel. I had two options: humanitarian situation or suicide squad. That night, I took two decisions. First, I was too scared to send them away. Second, I had to send someone across the killing zone to look closely, to check the people and the car and to make sure that the woman was pregnant. I went myself, with my own rifle on automatic. She was pregnant. The reason I am telling you this is that today I represent companies which, instead of sending soldiers, develop robots to do the job of protecting bases. What would do a robot in that situation? I do not know the answer and will therefore not address this issue in my presentation.

Instead, I will address the simpler situation of targeting. Targeting is the simplest situation on the battlefield because it has clear rules and clear algorithm for decision-making. What

I want to discuss is the following: can we take the rules of IHL and apply them to robots in the battlefield?

You have heard about the different types of systems, and I know that there are a few other kinds. We already have autonomous systems, which are usually semi-autonomous, or remote-controlled systems with a module that will allow them to turn autonomous in certain situations. For example, some of the missiles or UAVs have a self-destruct function so that if you lose control, they will explode. This is to prevent the technology falling into the hands of the enemy. What they do not have is a mechanism to ensure that, when they self-destruct, they do not kill civilians. We have not developed it yet, but we know that it is a problem. We also talked about the mines. Naval mines are today obviously autonomous systems. They wait for an acoustic signature and they attack. Once you put them in place, you can forget about them. They also have a self-destruct mechanism. What I would really like to talk about is the system Mr. Arkin mentioned previously: systems which are deployed from Day 1. They would go out to the battlefield, do something and come back later to report. There are two questions: (1) what rules apply to these systems? (2) If something goes wrong, who will be responsible?

Let's talk about targeting specifically. There are three basic rules we need to respect to be able to lawfully target under IHL: a lawful weapon, a lawful target, and an assessment of proportionality. Indeed, when you target, you have to make sure that you minimise the collateral damage. What about command responsibility? There are again three points: the actor is responsible for their actions, there is no defence of superior orders and there is a concept of command responsibility in addition to actor's responsibility. These rules were developed by humans for humans and they are based on certain assumptions. The first assumption is that there is acceptable and unacceptable human behaviour. This is morality or ethics. The second assumption is the recognition of human capabilities and fallibilities. Humans have sensory and cognitive capabilities. They can make mistakes, but they can see, feel and understand certain types of things. The third assumption is to understand the limitation of equipment, such as its accuracy or its percentage of failure, for example. The fourth assumption is that there are minimum standards of training, enforcement and supervision which are required from a military organisation.

These basic assumptions are challenged when confronted with autonomous weapon systems (AWS):

1. The situational awareness of a robot is different from a human. It is not necessarily better, but it is different, depending on what you put into it.
2. The analytical capabilities of a robot are different.

3. The commander of robots, with a high level of certainty, will have absolutely no idea of what the capabilities of the robot are. Do you know why your laptop does 95% of what it does? Do you understand any of this? Do you have any idea why your laptop sometimes sends emails to a number of people when you did not even press the button? I do not, and I assume that the commander of a robot will know even less. He will be given the menu, he will be trained, but that is all. Computers and humans do not compete together anymore; computers win.

For these three reasons, the basic assumptions are no longer valid. So what do we do?

Option 1 is to say : *We are in trouble, so do not develop AWS*. Option 2 is to try to make sure that the principles and the system will work together. For this, we need to understand how humans make decisions. Let us take the principle of distinction. How do we distinguish between an enemy and a non-combatant? There are three primary characteristics which automatically come to mind. There is the physical element, such as the uniform and whether they are carrying a weapon. Then there are the behaviour characteristics, which is the type of movement (moving towards you, moving low, moving high, running...). The geographical characteristics comes next: where are they in relation to the military target? You could train a machine to learn these three characteristics. It is a technological challenge, but it can be done. In order for the robots to be able to do this, they will need to have a situational awareness capability, i.e. sensory capabilities and decision-making capacities, which is again a challenge but technologically feasible. However, the question is whether it will be done or not, because it will cost a lot of money and it will be very complicated. It might also create a situation where robot makers may have more information than they want to. It could be that they do not want to know so much about their weapon systems on the battlefield, because then, they could be liable. Therefore, robot makers are not necessarily interested in making those systems comply with what I just said.

Let us now consider the principle of proportionality. If you break it down, it is actually composed of two principles. The first is again distinction: look at all the targets and find the non-combatants. Second is the balance between military advantage and collateral damage. I have done it for years and I still do not know the formula. If we want to teach a robot, we will have to develop a formula or a system for them to mimic our decision-making process. Therefore, in order to have a robot which is able to apply the principle of proportionality, we will need a robot capable of distinguishing and with a formula for proportionality. These are things that we have been working on for fifty years and we are not there yet.

Now, I would like to move to command responsibility. I will go through three scenarios. Two of them already exist.

In the middle of the fighting, there is a house. There is an enemy squad in the house, but you also suspect that there are civilians. Your first option is to send your special forces to clean the house. They are trained to look, room after room, for certain characteristics,. Then they identify who is a civilian and who is a combatant, kill one and save the other. Your second option is to send an animal, such as a dog, trained for this. They are very good and can identify combatants.
Robots could also do this job. In Gaza, for example, we used to send robots. They were not firing robots but reconnaissance robots to go through the house. You threw them through the window; they then open up and can move anywhere. The next generation of these robots could be armed and do the cleaning operations quite efficiently.

What happens if, at the end of one of these scenarios, the family ends up dead? If it is a Special Forces team, the military will launch an investigation and decide if they made a reasonable mistake depending on the difficulty of the situation. If it is a dog, there is no rule in international law, although they have been used for years. However, if it is a robot which killed everyone, who will be blamed? The commander who sent the robot? What if the manual did not say that the robot could break the rules? Will we go to the manufacturers?

I am presenting this situation to you because I would like to recommend that we take a particular direction. First, we must recognise that we are already there. We do not have the option of waiting. It is therefore extremely important to have rules ready before the equipment is fielded. Then, I suggest that we think about categories of AWS. Category A would be a system with limited sensory capabilities and possibly limited decision-making capabilities. We employ a lot of these already. You place a machine gun with a sensor; when it sees someone moving, it can fire at it. It becomes a robot once you take the man out of the loop. It is a decision, not a technological question. Although the technology is now advanced, it still cannot really distinguish. Therefore, a Category A robot can only be allowed to be deployed in situations where it will not be required to distinguish, for example in a combat zone where there are no civilians. Category C (Category B would be in the middle) would be a combination of innovative sensors and the best brain we can put into a system. These robots may surpass the decision-making and the sensory capability of a human being. That robot may be fielded in combat situations, and we will have to decide where this is possible. If we have this classification, we can also say that fielding a Category A robot in a situation where only Category C would be capable is a violation. We will also be able to go to the army and require that all their manufacturers certify the robots according to a classification system. So that we know which category it is, and where it is allowed to be used. This is an example of how this issue could be addressed. The principles would remain the same but we would create a procedure so that when these things come out, we would be ready.

I am concerned about moving the responsibility away from the commander. If we accept the idea that a commander is responsible, we have to figure out how we can make him responsible for a system of which he does not understand the limitation. However, if he is trained on classifications and knows where he is allowed to field Category A, B and C robots, then it becomes easier to hold him responsible if he uses the wrong system in the wrong location. These are initial thoughts, which would require much more thought and elaboration, as well as more cooperation between the technical and the legal field. However, we are heading very quickly in this direction and we need solutions now.

Thank you.

PANEL 3 – REMOTE-CONTROLLED AND AUTONOMOUS WEAPONS SYSTEMS DISCUSSIONS

The issue of command responsibility with respect to the use of robots in armed conflicts (1) and the introduction of robots on the battlefield (2) dominated the discussions following the third panel.

1. Command responsibility

With the introduction of robots in the landscape of armed conflicts, there was a consensus among the experts that there is a clear need to redefine responsibility. Indeed, a participant presented the following fictional scenario: a machine, which is used on the battlefield, was programmed not to kill civilians but did. The commander does not know and is not able to understand why the machine failed and killed civilians. What would then happen? Who would bear responsibility? The same participant further developed that, when a human soldier has psychological problems or 'goes crazy', the commander is not necessarily responsible anymore. For example, if soldier's training was perfect and his behaviour is completely unexpected, the chain of causality may be broken. With robots, the lack of causality could be much easier to prove. How do we then deal with this issue of responsibility?

In relation to the issue of command responsibility, a military from the audience added that there is another aspect besides prevention, which is sanction. As a commander, if you do not take measures after a violation of international humanitarian law (IHL), you would be responsible, because it can happen again in the future. According to him, the same could apply to robots. It is possible to follow up on the situation, to make sure that there will be an investigation and that the failure does not happen in the future. This is how a commander would be able to fulfil the obligations flowing from their command responsibility. This, however, would also lead to the question of how to sanction robots, which could be tricky. Should the memory be erased? Should it be destroyed?

2. Robots on the battlefield

In the potential scenario where robots fight other robots, would it raise further questions? For example, would these robots be combatants within the meaning of IHL? Technical experts answered that the military is concerned about the issue of systems conceivably fighting each other. Indeed, specialists are working on the question of restricting the use of autonomous systems to attacks against existing weapon systems, and prohibiting targeting of human beings. This, in principle, would be a good thing but does not fully address the issue of the person standing in the vicinity of the weapon systems. Another issue would then be: how would robots with ethical constraint to respect IHL perform against robots which do not have this ethical constraint? Additionally, the risk exists that the situation could evolve into an arms race, with counter measures being developed. This could require control by treaties.

Session 4
Outer space – a new conflict theatre?

Chair person: **Marco Sassoli,** *University of Geneva*

UNDERSTANDING THE PHYSICS OF SPACE SECURITY

Luca del Monte
European Space Agency

Résumé

Dans la présente contribution, l'orateur se propose de discuter des questions militaires et techniques relatives à l'utilisation de l'espace extra-atmosphérique: quelles sont les capacités des armes dans l'espace? Quelles sont les capacités des armes anti-satellitaires? Ces capacités sont-elles uniques? Quel est leur coût? Quelles options ont les États pour contrer de telles capacités?

En vue d'évaluer les différents systèmes militaires proposés, il est important de distinguer les différents types de contraintes: financières, technologiques, physiques. La technologie existante pose certaines limites aux systèmes réalisables pour un État donné; ces limites peuvent toutefois évoluer avec le temps. En revanche, la physique pose des limites fondamentales et immuables aux opérations spatiales. C'est la raison pour laquelle les informations techniques sont cruciales pour toute personne impliquée dans le débat sur la sécurité dans l'Espace.

Quelques éléments sur les orbites satellitaires

La vitesse d'un satellite est déterminée par son orbite et liée à son altitude. L'orbite d'un satellite ne dépend pas de sa masse mais de sa vélocité (vitesse et direction) à un moment donné dans l'espace. Plus un satellite est proche de la Terre, plus il se déplace rapidement. L'altitude qui permet aux satellites d'être en orbite au même rythme que la Terre est 36 000 km. Ces satellites sont appelés "géo-synchrone". Une fois placés sur orbite, un satellite utilise de petits moteurs fusées pour manœuvrer. Une orbite satellitaire se trouve sur un plan qui passe par le centre de la Terre. L'angle entre le plan de l'orbite et celui de l'Équateur est "l'inclinaison orbitale". Un satellite sur orbite polaire (c'est-à-dire qui passe par les deux pôles) passe régulièrement au-dessus de tous les points de la surface de la Terre; un satellite sur orbite équatoriale passe régulièrement au-dessus des points de l'Équateur. Les satellites peuvent se situer sur une orbite entre ces deux extrêmes. Les satellites sur orbite équatoriale qui ont une période orbitale de 24h restent fixes et sont appelés "géostationnaires". Ils sont utiles pour héberger des satellites de communication

et de diffusion. Les satellites qui ne sont pas géostationnaires se déplacent par rapport au sol, et la couverture constante d'un endroit spécifique requiert une constellation de satellites. Pour prendre des images haute résolution d'un endroit spécifique, ou encore conduire une attaque, un satellite doit être situé sur une orbite proche de la Terre, ce qui le rend plus vulnérable aux interférences avec des méthodes d'attaques au sol.

Manoeuvrer dans l'espace

Modifier la trajectoire ou la vitesse d'un satellite peut nécessiter une dépense importante d'énergie. En effet, la force de propulsion dont un satellite a besoin pour changer sa vélocité augmente de manière exponentielle en fonction de la grandeur de la vélocité. Ainsi, la difficulté et le coût de telles manipulations limitent les manœuvres des satellites. La propulsion utilisant les nouvelles technologies permet un changement de vitesse plus important par quantité de combustible que les propulseurs chimiques conventionnels. Cependant, ces nouvelles technologies de propulsion ne sont pas efficaces pour des manœuvres rapides, ce qui limite alors leur utilité tactique.

Les interférences entre systèmes satellitaires

Les interférences peuvent avoir des conséquences temporaires et réversibles mais aussi provoquer la paralysie ou la destruction du satellite. Plusieurs méthodes peuvent être utilisées: interférence électronique des systèmes de communication, interférence laser à l'aide de capteurs, collision avec un autre objet, explosions nucléaires, etc. De par leur nature, les satellites sont vulnérables aux attaques. Néanmoins, s'il est facile de brouiller des systèmes satellitaires non protégés, tels ceux utilisés pour la communication commerciale, il est techniquement très difficile d'altérer ceux qui sont utilisés pour la communication militaire. De plus, l'efficacité d'attaques anti-satellitaires est difficile à prévoir. Par exemple, le déploiement d'armes anti-satellitaires en vue d'attaques conduites depuis l'espace, peut difficilement se faire secrètement. En revanche, une fois déployés, aucun pays ne peut prétendre être capable de détecter ou d'identifier des dispositifs anti-satellitaires. Et quand bien même, cela ne signifie pas que ce pays peut se défendre contre ces armes anti-satellitaires. A noter que les conséquences d'une attaque contre un satellite dans le système peuvent être réduites par une conception intelligente, telle que l'ajout de systèmes de sauvegarde et de pièces de rechange, et le développement de moyens alternatifs pour effectuer certaines fonctions vitales.

Introduction

Recent interest in new types of weapons has spawned an emerging international debate. Key topics include whether the deployment of space-based weapons and anti-satellite weapons (ASAT) is inevitable, what military utility such weapons would have, how their deployment would affect the security of the owner nation and the wider international community, whether their deployment and use would interfere with other military and civilian uses of space, and what normative and legal constraints on the use of space could be agreed upon and enforced.

Addressing these issues requires an assessment of a wide range of political, diplomatic, military and technical issues. This report is limited to a discussion and analysis of the technical and military issues and focuses on a number of key questions: What capabilities could anti-satellite weapons and weapons in space realistically provide? Would these capabilities be unique? How do they compare with alternatives? What would they cost? What options would be available to nations seeking to counter these capabilities? The answers depend on technical realities that must be considered in any policy analysis of space weapons and anti-satellite weapons. In evaluating proposed military systems, it is important to distinguish between constraints imposed by financial cost, by technology and by physics.

Available technology places important limits on what systems are currently feasible for a given country, but those limits can change over time and do not represent fundamental limitations. The space-based laser, for example, has so far achieved power levels well below what is required for a usable weapon, but there do not appear to be fundamental limits to increasing its power over time. Physics, on the other hand, places fundamental limits on space operations that will not change with time. An example of a fundamental limit posed by physics is the fact that satellites in low orbits cannot remain stationary over a given location on Earth, so multiple satellites are required to ensure that one is always near that location. It is thus important to provide information on a range of technical issues related to space systems critical for anyone involved in the debate over space security to understand.

Basics of Satellite Orbits

The speed of a satellite is not arbitrary: it is determined by the satellite's orbit and is closely tied to the satellite's altitude. A satellite's orbit does not depend on its mass. All objects with the same velocity (speed and direction) at a given point in space follow the same orbit. Satellites close to the Earth move faster than those at higher altitudes and, when viewed from the ground, cross the sky faster. Satellites in low earth orbits (hundreds of kilometres above the Earth) move rapidly relative to the Earth, completing an orbit in 1.5 to 2 hours. Satellites in higher orbits move at slower speeds than those in lower orbits and the distance they travel in one orbit is longer. As a result, the time required for a satellite to orbit (the orbital period) increases with altitude. Only one altitude (36,000 km) permits satellites to orbit at the same rate at which the Earth rotates; such satellites are called geosynchronous. Once in orbit, a satellite does not need constant powering to remain in flight, as airplanes do. Satellites use small onboard rocket engines to manoeuver in space.

A satellite's orbit always lies in a plane that passes through the centre of the Earth. The angle between that plane and the plane of the equator is called the orbit's inclination. Because the Earth rotates underneath the satellite as it orbits, a satellite in a polar orbit (an orbit that passes over both poles) travels directly over every point on Earth. Satellites in equatorial orbits only travel directly over the equator. Satellites may be in orbits with inclinations between these two extremes; in such cases, the satellite travels directly over points on the Earth with a latitude equal to or less than the satellite's inclination angle. Satellites that are in equatorial orbits and that have an orbital period of 24 hours stay fixed over a point on the equator; they are called geostationary. While geostationary orbit is useful for hosting communications and broadcasting satellites, it is not well suited to such missions as high-resolution imagery or ground attacks, because such an orbit requires a very high altitude (36,000 km). Furthermore, because geostationary satellites travel only in the equatorial plane, they have difficulty communicating with the Earth's polar regions. Satellites that are not in geostationary orbit move with respect to the ground, and so constant coverage of a particular location on the Earth requires a constellation of satellites. Satellites at high altitudes can see more of the Earth's surface at one time than can satellites at lower altitudes. Satellites that need to be close to the Earth to perform specific missions, for example, to take high-resolution images of the ground, must be located in low earth orbits. Being closer to the Earth's surface makes these satellites more vulnerable to interference from ground-based methods of attack.

Manoeuvring in Space

Manoeuvring a satellite, which requires changing the speed of the satellite or its direction of travel, can require a large expense of energy. The mass of propellant a satellite needs to change its velocity increases exponentially with the amount of velocity change. The difficulty and cost of placing large amounts of propellant in space therefore limit how much manoeuvring satellites can do. Manoeuvres to change the satellite's orbital plane can require large changes in the satellite's velocity and can therefore require large amounts of propellant. By contrast, manoeuvres that alter the shape or altitude of the orbit but that do not change the orbital plane generally require much less propellant, especially if the satellite moves between low earth orbits.

Propulsion using new technologies can generate substantially more velocity change per unit mass of fuel than conventional chemical propellants do. This reduces the mass of fuel a satellite needs to carry to perform a given manoeuvre. While more efficient, the new propulsion technologies that will be available in the foreseeable future cannot be used to carry out manoeuvres quickly, which limits the tactical utility of these technologies.

Overview of Interfering with Satellite Systems

Interference can range from temporary or reversible effects to permanent disabling or destruction of the satellite. Many methods can be used to interfere with satellites, including electronic interference with communication systems, laser interference with imaging sensors, laser heating of the satellite body, high-power microwave interference with electrical components, collision with another object (kinetic-kill) and nuclear explosions.

Because satellites can be tracked and their trajectories can be predicted, they are inherently vulnerable to attack. However, a satellite's vulnerability to ASAT attack does not guarantee the effects of an attack will be predictable or verifiable, and this may limit the ASAT attack's usefulness. Jamming satellite ground stations (the downlinks) and the satellite's receivers (the uplinks) is relatively simple to do on unprotected systems such as commercial communications satellites. Jamming protected systems, such as military communications satellites, is much harder. An adversary need not be technologically advanced to attempt a jamming attack. Ground-based lasers can dazzle the sensors of high-resolution reconnaissance satellites and inhibit observation of regions on the Earth that are kilometres in size. With high enough power, ground- and space-based lasers can partially blind a satellite, damaging relatively small sections of the satellite's sensor. A high-power laser can physically damage a satellite if its beam can be held on the satellite for long enough to deposit sufficient energy. This can result in overheating the satellite or damaging its structure. High-power microwave weapons can disrupt or damage the electrical systems of a satellite if enough of their energy enters these systems. Such attacks would be conducted from space rather than from the ground. Microwave attacks could attempt to enter the satellite through its antennae (a front-door attack) or through other routes, such as seams in the satellite's casing (a back-door attack). The effectiveness of both types of attack would be difficult to predict. Satellites in low earth orbits can be attacked by kinetic-kill ASATs carried on short-range missiles launched from the ground. ASATs stationed on the ground or in low earth orbits can be designed to reach targets at higher altitudes in a matter of hours. A nuclear explosion at an altitude of several hundred kilometres would create an intense electromagnetic pulse that would likely destroy all unshielded satellites that are in low earth orbit and in the line of sight of the explosion. In addition, persistent radiation created by the explosion would slowly damage unshielded satellites at altitudes near that of the detonation.

Space-based ASATs are likely to be deployed in one of four ways: co-orbital with and a short distance behind the target satellite (a trailing ASAT); attached to the target (sometimes called a parasitic ASAT); in a distant part of the same orbit, requiring a manoeuver to approach and attack the target; or in a crossing orbit, keeping its distance from the target until the time of engagement. Different interference methods would be suited to different deployment configurations. To be covert, a space-based ASAT must elude detection and/or identification during launch, during deployment manoeuvres and while in orbit. No country could assume its deployment of a space-based ASAT would remain covert. At the same time, no country can assume it would be able to detect or identify a space-based ASAT deployed by another country. Detecting a covert weapon may allow the targeted country to publicly protest its presence and to prepare tactical alternatives to the targeted satellite, but may not guarantee the country's ability to defend against the ASAT. A simple anti-satellite weapon that could be used by an attacker with relatively low technical sophistication is a cloud of pellets lofted into the path of a satellite by a short- or medium-range ballistic missile. The effectiveness of such an attack would depend on the attacker's ability to determine the path of the target satellite with precision and to control its missile accurately. Unless the attacker can do both, such an ASAT would have limited effectiveness. Many systems that rely on satellites can be made to withstand interference that disrupts an individual satellite. The consequences of an attack on a satellite in the system can be reduced by smart design, including building in redundancy, adding backup systems and spares and developing alternative means to perform vital functions.

Reference and further reading

- David Wright, Laura Grego, and Lisbeth Gronlund *The Physics of Space Security- a reference manual.*
- Report of the Commission to Assess United States National Security, *Space Management and Organization* January 11, 2001. To be found at: http://www.fas.org/spp/military/commission/report.htm, accessed February 8, 2005,
- Air Force Space Command, *Strategic Master Plan: FY06 and Beyond*, October 1, 2003. To be found at: http://www.peterson.af.mil/hqafspc/news/images/FY06%20Beyond%20Strategic%20Master%20Plan.pdf, accessed February 8, 2005.

LEGAL REGULATION OF THE MILITARY USE OF OUTER SPACE – WHAT ROLE FOR INTERNATIONAL HUMANITARIAN LAW?

Steven Freeland[1]

University of Western Sydney and University of Copenhagen

Résumé

Cadre général de la réglementation de l'espace extra-atmosphérique

Il existe un corps de règles internationales relatif à l'utilisation et l'exploration de l'espace extra-atmosphérique. Pour la plupart, ces règles trouvent leur source dans les traités, les résolutions de l'Assemblée générale des Nations unies, le droit et la jurisprudence nationale, les accords bilatéraux, et les décisions des Organisations internationales. On relèvera cinq traités conclus sous les auspices des Nations unies : (1) le Traité de l'espace de 1967, (2) l'Accord sur le sauvetage des spationautes, le retour des spationautes et la restitution des objets lancés dans l'espace extra-atmosphérique de 1968, (3) la Convention sur la responsabilité internationale pour les dommages causés par des objets spatiaux de 1972, (4) la Convention sur l'immatriculation des objets lancés dans l'espace extra-atmosphérique de 1975, et (5) l'Accord régissant les activités des États sur la Lune et les autres corps célestes de 1979. Entre autres, ces traités affirment que l'espace extra-atmosphérique doit être considéré comme un domaine global commun, à l'instar, en partie, de la haute mer. Son utilisation et son exploration se feront exclusivement à des fins pacifiques. Outre ces traités, l'Assemblée générale des Nations unies a adopté six séries de principes, non contraignants, qui traitent d'utilisations spécifiques de l'espace et de la question impérieuse des débris.

Le Traité de l'espace prévoit un certain nombre de règles destinées à limiter l'utilisation militaire de l'espace extra-atmosphérique, notamment en ce qu'il impose que les activités relatives à l'utilisation et à l'exploration de l'espace extra-atmosphérique s'effectuent « conformement au droit international, y compris la Charte des Nations unies ». *Si l'article 51 de la Charte, qui confère aux parties un droit à la légitime défense, s'applique également à l'espace extra-atmosphérique, l'État qui y aurait recours resterait soumis au* jus in bello.

[1] This paper was written in October 2010.

La pertinence des principes du DIH dans l'espace extra-atmosphérique

Ainsi, les principes existants du DIH sont applicables à l'utilisation militaire de l'espace extra-atmosphérique. Il n'y a pas de limite territoriale spécifique à l'application du DIH : il s'applique dans les zones de combats et dans celles affectées par les conflits armés. Toute activité militaire dans l'espace extra-atmosphérique est donc soumise au DIH, qu'il s'agisse de l'action en elle-même ou de ses effets, par exemple sur Terre. Toutefois, ces règles sont-elles pertinentes en matière d'activités dans l'espace extra-atmosphérique ? En effet, l'espace extra-atmosphérique est de plus en plus fréquemment utilisé dans le cadre de la conduite des hostilités. Par exemple, des informations sont collectées depuis l'espace pour la planification d'opérations militaires sur Terre. Plus préoccupante est l'utilisation d'engins spatiaux pour diriger des activités militaires. Dans ce cas de figure, l'espace extra-atmosphérique fait alors partie intégrante de l'infrastructure militaire des parties au conflit. Le développement de systèmes défensifs est en même temps le résultat et le moteur d'une course globale à l'armement. Les États-Unis, l'Union européenne, la Russie, et la Chine, entre autres, considèrent l'espace extra-atmosphérique comme une composante essentielle de leurs infrastructures militaires. On note également l'utilisation croissante de la technologie spatiale dans les interventions militaires de l'OTAN en Serbie, puis au Kosovo et en Afghanistan. En outre, l'avènement de la Chine en tant que puissance spatiale majeure suscite des craintes quant à l'utilisation de l'espace à des fins stratégiques que ne respecterait pas nécessairement les principes de coopération des Traités de l'espace. En effet, on a récemment observé que les États-Unis et la Chine détruisaient volontairement des satellites à l'aide de leurs systèmes de missiles terrestres respectifs.

*Si, comme le suggèrent certains spécialistes, une guerre spatiale venait à éclater, il est certain que le DIH serait applicable. Son application in concreto, en revanche, est moins évidente. Une partie importante du patrimoine spatial utilisé à des fins militaires étant à double usage (civil et militaire), une question fondamentale est, par exemple, de savoir si, et dans quelles circonstances, un tel satellite peut être considéré comme une cible légitime. En effet, l'application des principes de distinction, de proportionnalité, de même que l'évaluation des précautions que doivent prendre les parties pour protéger les populations civiles, est problématique. En effet, la destruction d'un satellite ne cause pas de forcément de dommages civils immédiats, mais pourra potentiellement affecter la vie et les moyens de subsistance de millions de personnes, anéantir des économies et détruire des services essentiels. Si de telles conséquences sont difficiles à prévoir, on peut penser qu'elles seraient considérées comme de l'imprudence (recklessness). Reste que le test de l'imprudence (*recklessness test*) paraît lui aussi difficile à appliquer à une telle situation.*

Ainsi, étant donné la nature spécifique de l'espace extra-atmosphérique, les principes de DIH ne sont probablement ni suffisamment spécifiques, ni complètement appropriés à l'action militaire *dans un tel contexte. Tous les efforts doivent bien sûr être faits pour appliquer le plus directement possible les principes existants, toutefois il semble que des règles plus spécifiques devront être établies en vue de protéger l'humanité des conséquences potentielles d'une guerre dans l'espace extra-atmosphérique.*

The General Framework for the Legal Regulation of Outer Space

On October 4, 1957, a Soviet space object, Sputnik I, was launched and subsequently orbited the Earth over 1,400 times during the following three-month period. This milestone heralded the dawn of the space age, the space race (between the USSR and the United States), and the legal regulation of the use and exploration of outer space. Since then, laws have developed that significantly improve the standard of living for all humanity, through, for example, the facilitation of public services such as satellite telecommunications, global positioning systems, remote sensing technology for weather forecasting and disaster management, and television broadcast from satellites. The prospects for the future use of outer space offers both tremendous opportunities and challenges for humankind, and law will continue to play a crucial role in this regard.

The journey of Sputnik I immediately gave rise to difficult and controversial legal questions, involving previously undetermined concepts. Although the USSR had not sought the permission of other States to undertake this mission, there were no significant protests that this artificial satellite had infringed on any country's sovereignty as it circled the Earth. This international (in)action confirmed that this new frontier of human activity – outer space - did not possess the elements of sovereignty that had already been well established under international law regulating land, sea and air space on Earth.

There is now a substantial body of law dealing with many aspects of the use and exploration of outer space, mainly codified in and evidenced by Treaties, United Nations General Assembly resolutions, national legislation, decisions of national courts, bilateral arrangements and determinations by Intergovernmental Organisations.

Five important multilateral treaties have been finalised through the auspices of the United Nations Committee on the Peaceful Uses of Outer Space (UNCOPUOS), the principal multilateral body involved in the development of international space law.[2] These are:

[2] UNCOPUOS was established by the United Nations General Assembly in 1959, shortly after the advent of the 'space age' brought on by the successful launch of Sputnik 1: see United Nations General Assembly Resolution 1472 (XIV) on International co-operation in the peaceful uses of outer space (1959).

(i) 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and other Celestial Bodies (Outer Space Treaty);[3]

(ii) 1968 Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space;[4]

(iii) 1972 Convention on International Liability for Damage Caused by Space Objects;[5]

(iv) 1975 Convention on Registration of Objects Launched into Outer Space;[6]

(v) 1979 Agreement Governing the Activities of States on the Moon and other Celestial Bodies (Moon Agreement).[7]

Among other important principles, these Treaties confirm that outer space is to be regarded as a 'global common' area, with similarities in this regard to the high seas. The use and exploration of outer space is to be for 'peaceful purposes', although this principle has been highly controversial - arguments still persist as to whether this refers to 'non-military' or 'non-aggressive' activities. The Treaties were formulated in the Cold War era, when only a small number of countries had space-faring capability. The international law of outer space thus, at least partially, reflects the political pressures imposed by the superpowers at that time. Indeed, even the question of where air space ends and outer space begins has not been definitively determined from a legal viewpoint, although more recently a consensus as to a demarcation point (100 kilometres above mean sea level) is beginning to emerge.

The United Nations General Assembly has also adopted six sets of Principles. These largely 'soft law' guidelines supplement the Treaties and deal with various specific uses of outer space, as well as the increasingly urgent issue of space debris. Yet, it is clear that the existing legal and regulatory regime has not kept pace with the remarkable technological and commercial progress of space activities since 1957. This represents a major challenge, all the more in view of the strategic and military potential of outer space in an era of globalisation. The Outer Space Treaty does provide a number of general principles that are intended to restrict the military uses of outer space, including the requirement that space activities shall be carried out 'in accordance with international law, including the Charter of the United Nations'.[8] One of the

[3] 610 U.N.T.S. 205.

[4] 672 U.N.T.S. 119.

[5] 961 U.N.T.S. 187.

[6] 1023 U.N.T.S. 15.

[7] 1363 U.N.T.S. 3.

[8] Article III, Outer Space Treaty. Article 2 of the Moon Agreement extends these sentiments by referring to 'the Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, adopted by the General Assembly on 25 October 1970'.

primary reasons for the inclusion of this provision was the concern among many States at the time that outer space would become a new arena for international conflict.

Moreover, Article 51 of the United Nations Charter – which confirms the 'inherent right' of self-defence 'if an armed attack occurs'- is also applicable to the legal regulation of outer space. Under the principles of public international law, this right remains subject to express legal limitations – the requirements of necessity and proportionality.[9] Even where the right of self-defence is lawfully exercised, the State so acting will remain subject to the *jus in bello* principles. Whilst this is, in theory, uncontroversial, the difficulty is to determine precisely whether (and how) the fundamental principles of international humanitarian law can be applied to the unique legal and technological context of outer space.

This is particularly relevant given that the use of satellite technology already represents an integral part of the military strategy and the conduct of many armed conflicts. As this technology continues to develop, the armed conflicts of the 21st century and beyond will increasingly involve the utilisation of outer space. In this regard, the United Nations is anxious to avoid a 'weaponisation' of outer space.[10] However, the current momentum does, unfortunately, appear to be directed towards a greater incorporation of satellite technology and outer space within the course of warfare.

In this context, if one were to adopt a hard-line pragmatic view, it seems that the 'non-military v non-aggressive' debate is a redundant argument, even though it represents an extremely important issue of interpretation of the strict principles of international space law. In one sense, this assumes that the militarisation of space is a given, as much as it pains international and space lawyers to admit this. This is highly troubling and flies in the face of the principles of the Outer Space Treaty. Yet, it would be naive to ignore the realities – rather it is important both to understand what (and how) existing legal principles apply to any military activities involving outer space and to determine what needs to be done to provide, at least from a regulatory perspective, an appropriate framework to protect humankind in the future.

[9] See *The Caroline Case* 29 B.F.S.P. 1137-1138; 30 B.F.S.P. 195-196, which also referred to a requirement of immediacy, although this was not mentioned in the more recent decision of the International Court of Justice in *Oil Platforms (Merits) (Iran v. United States)* ICJ Rep. 2003, p.161.

[10] Refer to the numerous United Nations General Assembly Resolutions, beginning with Resolution 36/97C, 9 December 1981, which have been directed towards the 'Prevention of an arms race in outer space.'

The Relevance of the Principles of International Humanitarian Law to Outer Space

As noted, the existing principles of international humanitarian law, as an integral part of international law, are, in theory, applicable to the military use of outer space. There is no specific 'territorial' limitation to the laws and customs of war, which apply both to the area where the hostilities actually take place, as well as to other areas affected by those hostilities. If, for example, direct military action takes place in one area, but the effects of that action impact on civilians elsewhere, that represents a relevant consideration in determining whether such action is consistent with, for example, the principle of proportionality. As a consequence, any military activity that takes place in outer space will be subject to the *jus in bello* in relation not only to that direct action, but also as to its effects elsewhere, including on Earth.

Having reached this conclusion, it is then necessary to determine whether this is just an issue of academic curiosity or, alternately, that the rules of war are 'relevant' to activities in outer space. The answer, unfortunately, appears self-evident. Just as States have for a long time been undertaking in outer space what might euphemistically be termed 'passive' military activities, outer space is now increasingly being used as part of the 'active' conduct of armed conflict. Not only is the information gathered from outer space – through, for example, the use of remote satellite technology and communications satellites – used to plan military engagement on Earth, but space assets now also direct military activity, and thus represent an integral part of the military hardware of the major powers.

It was during the Gulf War in 1990 that the military value of space assets for the conduct of warfare was first utilised to a significant degree. Indeed, 'Operation Desert Storm' is regarded as 'the first space war'.[11] It was recognised that the use of space technology would create an 'integrated battle platform' to aid in the implementation of military strategy.[12] Following the attacks of 11 September 2001, the United States Administration issued a landmark policy paper,[13] in which it emphasised the need to maintain technological supremacy, so as to 'dominate the space dimension of military operations'.[14] This necessitates having 'the ability to defend the homeland, conduct information operations, ensure US access to distant theaters,

[11] Jackson Maogoto and Steven Freeland, 'Space Weaponization and the United Nations Charter: A Thick Legal Fog or a Receding Mist?' in: *The International Lawyer* Vol. 41, No. 4, 2007p.1091 at p.1107.

[12] Ibid.

[13] The White House, *The National Security of the United States of America*, September 2002 at p.30. To be found at: http://www.whitehouse.gov/nsc/nss.html (accessed 20 July 2006).

[14] See Sa'id Mosteshar, 'Militarization of Outer Space: Legality and Implications for the Future of Space Law' in: *Proceedings of the Colloquium on the Law of Outer Space*, 47, 2004 at footnotes 1 and 2.

and protect critical US infrastructure and assets in outer space.'[15] Although the Obama Administration has more recently issued an updated space policy that emphasises co-operation to a far greater degree, these sentiments still represent the approach of the United States military.

Ballistic missiles play an increasingly important role in any sophisticated national security structure, and the development of defensive systems 'is both a result of and additional factor driving' a global arms race.[16] In 2001, a commission headed by former United States Secretary of Defence, Donald Rumsfeld, suggested that an 'attack on elements of US space systems during a crisis or conflict should not be considered an improbable act.'[17] The Report went on to (in)famously warn of the possibility of a 'Space Pearl Harbor' – a surprise attack on the space assets of the United States. The European Union has recently identified outer space as 'a key component for its European Defence and Security Policy',[18] and Russia and China also regard space as a vital part of their military infrastructure. Even for smaller countries such as Australia, the political landscape of national space policy highlights military and national security concerns.[19]

In an effort to consolidate its policy of 'space control', the United States has pursued its national missile defence system (NMD), the development and testing of which led to its withdrawal in 2002 from the 1972 Anti-Ballistic Missile Treaty.[20] Space technology played an increasingly important role in the military actions by NATO in Serbia and Kosovo in 1999 and by the 'Coalition of the Willing' forces in Afghanistan in 2001. During the invasion of Iraq in 2003, the United States used GPS satellite technology to direct so-called 'smart bombs' to their designated targets.

[15] See White House, n.13 above.

[16] Regina Hagen and Jürgen Scheffran, 'International Space Law and Space Security – Expectations and Criteria for a Sustainable and Peaceful Use of Outer Space' in: Marietta Benkö and Kai-Uwe Schrogl, *Space Law: Current Problems and Perspectives for Future Regulation* (Eleven International Publishing, The Netherlands, 2005) p.273, 273.

[17] United States Department of Defence, *Report of the Commission to Assess United States National Security Space Management and Organization* 11 January 2001. To be found at: http://www.defenselink.mil/pubs/spaceintro.pdf (accessed 12 March 2006), p.8.

[18] Hagen and Scheffran, n.16 above, p.281-282.

[19] For a discussion of Australia's Space Policy, see Steven Freeland, 'Difficulties of Implementing National Space Legislation Exemplified by the Australian Approach' in Stephan Hobe, Bernhard Schmidt-Tedd and Kai-Uwe Schrogl (eds), *'Project 2001 Plus' - Global and European Challenges for Air and Space Law at the Edge of the 21^{s}t Century*, (Carl Heymanns Verlag, Köln, 2006) p.65.

[20] Treaty on the Limitation of Anti-Ballistic Missile Systems (ABM Treaty), 23 U.S.T. 3435. Article V(1) of the ABM Treaty provided that '[e]ach Party undertakes not to develop, test or deploy ABM systems or components which are sea-based, air-based, space-based, or mobile land-based'.

In addition, the advent of China as a major space power – symbolised not only by becoming, in 2003, the third country to successfully send a man into space, but also by its ambitious plans for missions both to the Moon and Mars – have given rise to increasing concerns about the use of outer space for strategic purposes not necessarily in keeping with the underlying co-operative principles of the space Treaties. Both China and the United States have, in recent years, deliberately destroyed satellites through their respective land based missile systems, thereby further raising the tensions associated with a potential arms race in space.[21]

In this context, several commentators have gone even further and opined that space warfare is, in fact, inevitable and cannot be avoided.[22] If these assertions turn out to reflect reality, the principles of the laws of war should be applied. However, it is not clear how this will be done in practice and what consequences will follow. Given that an important group of space assets used for military purposes are 'dual-use' satellites, one is also drawn to the question of whether, and in what circumstances, such a satellite can (ever) be regarded a legitimate target of war.

The answer will depend upon a number of fundamental principles of international law. Clearly, the physical destruction of a satellite constitutes a use of force. Apart from a consideration of the principles in the space Treaties, one would have to determine whether such an action represented a legitimate (at law) use of force, with the only possible justification being Article 51 of the United Nations Charter. This would necessarily involve a consideration of the necessity and proportionality – measured against the armed attack and threat of further attacks – of the act of self-defence. Even if the action did not violate these *jus ad bellum* principles, one would then need to consider the principles of international humanitarian law.

Assume, for example, that a combatant regards a dual-use satellite – for example, a GPS or remote sensing satellite – as representing a legitimate military objective in accordance with the principles of distinction and military advantage. Even if this were a correct assessment, the principle of proportionality would also apply. Moreover, one could argue that, implicit in the principle of distinction is the obligation on the parties to a conflict to take 'all feasible precautions' to protect civilians from the effects of an attack.[23]

[21] For further details, see Jackson Maogoto and Steven Freeland, 'From Star Wars to Space Wars - The Next Strategic Frontier: Paradigms to Anchor Space Security' in: *Air and Space Law* Vol.33, 2008p.10.

[22] See, for example, Iole M De Angelis, 'Legal and Political Implications of Offensives Actions from and against the Space Segment' in: *Proceedings of the Colloquium on the Law of Outer Space*, 45, 2002,p.197.

[23] Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law – Volume 1: Rules*, (Cambridge University Press, United Kingdom, 2005) p.70. There would also be adverse environmental consequences (including significant space debris) resulting from the destruction of a satellite, and various international environmental law principles would also therefore be applicable in these circumstances.

One can certainly envisage that the deliberate destruction of such a satellite, even if it does not result in any immediate civilian casualties, could have a devastating impact on communities, countries or even regions of the world. Millions of lives and livelihoods could, potentially, be affected, economies destroyed and essential services incapacitated. Obviously, some of the consequences of such an attack may be difficult to foresee, but it would, one could argue, be regarded at the least as reckless. However, there is likely to be some uncertainty as to whether and how a 'recklessness' test is to be applied in such a situation.[24]

Overall, given the unique nature of outer space, the principles of international humanitarian law – developed to regulate *terrestrial* warfare and armed conflict – are probably neither sufficiently specific nor entirely appropriate for military action in outer space. Even though every effort should be made to apply the existing principles as directly as possible, the largely unprecedented nature of such circumstances means that more specific rules will almost certainly be required, if they are to provide a comprehensive framework to properly protect humanity from the otherwise disastrous consequences of outer space (potentially) becoming another theatre of warfare.

Concluding Remarks – some suggestions as to what needs to be done

This necessarily brief discussion gives rise to several conclusions: first, present indications suggest that there is an increasing likelihood that outer space will not only be used to facilitate armed conflict (as it already is) but may ultimately become a theatre of war. The tendency of the major powers to increasingly rely on space technology may spiral a space weapons race, despite the efforts of the international community. Even though the United States may currently claim space superiority, it can only be a matter of time before other space-faring countries – including Russia, China and India – will have access to equally sophisticated (and potentially devastating) space weapons technology.

Secondly, the development of such technology and the increasing range of military uses of outer space heighten the dangers of a space war, as frightening as that prospect is. The proliferation of crucial military space assets means that, from a military and strategic viewpoint, the disabling or destruction of satellites used by another country may be perceived as giving rise to very significant advantages. The fact that it has not happened in the past is no reason to assume that we will never see a space conflict.

[24] For a discussion of the difficulties of applying the proportionality principle in the case of the 'high altitude bombing' during the NATO military action in Serbia and Kosovo in 1999, see Steven Freeland, 'The Bombing of Kosovo and the Milosevic Trial: Reflections on Some Legal Issues' in: *Australian International Law Journal*, 2002,p.150 atpp.165-168.

Thirdly, the countries of the world are highly dependent on space technology to maintain and improve their livelihood and standard of living. The non-military uses of space have become vital aspects of any community's survival. At the same time, however, many of the satellites providing these civilian services are dual-use, in that they are also utilised for military and strategic purposes. This raises difficult questions about the 'status' of such assets under the rules of war – particularly as to whether they may, under certain circumstances, be regarded as legitimate military objectives.

Fourthly, the Outer Space Treaty, which also reflects customary international law, specifies that the rules of international law apply to the use and exploration of outer space. These include not only the *jus ad bellum* principles regulating the use of force, but also the *jus in bello* principles. Respect for these rules is absolutely vital for the safety and security of humankind, as well as the interests of future generations. However, with the exception of those Treaties that seek to ban the use and testing of certain types of weapons, there are many uncertainties that arise when one seeks to apply, in particular, the principles of international humanitarian law to a (at this stage hypothetical) space conflict. The consequences of a space war are potentially so enormous and unknown that one cannot be sure as to exactly how these existing rules are to apply.

Fifthly, if we are to avoid 'grey areas' in the law, it is therefore necessary to develop specific and clear rules and standards that categorically prohibit the weaponisation of space, as well as any form of conflict in the region of space and against space assets. The Outer Space Treaty, as well as the other space Treaties, does not currently provide stringent rules or incentives to prevent an arms race in outer space, let alone a conflict involving (and perhaps 'in') space. This may, therefore, require additional specific legal regulation of outer space that is directly applicable to armed conflict involving the use of space technology. The position is, of course, further complicated by the applicability of the right of self-defence, a right that States will never abandon. As part of these new rules, clear definitions must be developed for concepts such as 'space weapons', 'peaceful purposes' and 'military uses'. Moreover, the fundamental issue of 'where space begins' should be definitively resolved, so as to counter any arguments that outer space is, in fact, an area akin to the territory of a State for the purposes of national security.

Sixthly, at the same time, careful consideration must be given to the application of the principles of international humanitarian law to this new paradigm of warfare. Whilst, of course, there already exist very well established fundamental rules regulating terrestrial warfare, it is not clear whether these are entirely appropriate, relevant and sufficient to protect humanity from the exigencies and consequences of any future 'space wars'.

Finally and most significantly, in developing all of these new rules, we must at all times adhere to the fundamental sentiment of ‘humanity’ that underpins both space law and international humanitarian law, in order to avoid the possibility of alternate scenarios that are too frightening to contemplate.

PANEL 4 - OUTER-SPACE – A NEW CONFLICT THEATRE? DISCUSSIONS

Both technical and legal questions followed the fourth panel.

1. Number of satellites

Asked about the number of satellites in outer space, the technical expert made a distinction between active satellites, which are controlled, operable and operated, and other space objects. The expert estimated the number of active satellites at roughly 1000. This number, however, does not include the classified satellites, which represent a huge portion of the satellites in space. In addition, it is important to bear in mind that even if nothing can be hidden in space, tools might be required to be able to see. On this matter, the EU seems to lack this capability and is strongly dependant on the US. There are also technologies to develop stealth satellites, which are less visible.

With respect to the total number of objects in space, no expert can answer. The only possible to guess is to limit the size of the objects: there are about 20 000 registered objects bigger than 1cm. However, even the smallest objects can be very destructive.

The deployment of satellites for a specific theatre, for example, for the purpose of surveillance in Afghanistan, is a very new concept. A lot of satellites already in operation are used for crises and conflicts, specifically in Afghanistan, but they were not deployed just for this purpose. However, while this practice is emerging, but remains rare and very expensive. Indeed, in addition to the material itself, the launch of a satellite is very expensive.

2. Is it possible to clean up the debris?

When a collision of satellites occurs, kinetic energy radiation is released by the impact. There is an evident need to clean up the debris. According to the experts, the basic technology is available. It is called '*rendez-vous and docking*', which involves of coming close to an object, turning around it and docking. However, it is a dual-use technology: the exact same technology might indeed be used to destroy a satellite, to tamper the information a satellite is transmitting to earth, or to transmit false information. Therefore, no one really wants to enter this domain. It is technically possible to allocate responsibility for cleaning up the debris, but it does not seem politically and financially feasible. However, the issue of debris remains incredibly important, say the experts. It is indeed noteworthy that there are, at the United Nations, voluntary guidelines for debris mitigation.

3. The 2008 Russia/China draft treaty

In 2008, China and Russia submitted a draft treaty to the Conference on Disarmament in Geneva, which purported to ban space weapons. The draft treaty was relatively comprehensive, although it did not ban all weapons. It provided very useful definitions, such as the definition of space and space weapons. The draft treaty was rejected by the United States but the legal expert of the panel is still confident that it will come to light.

4. Rules of liability and responsibility for falling objects

According to an expert, there are specific rules about responsibility and liability. The Outer Space Treaty provides that states are responsible for all national activities in space, including for private activities. It imposes international liability for damages caused by space objects. Additionally, the Convention on International Liability for Damage Caused by Space Objects ('Liability Convention') sets up a specific liability regime. The expert added that the reality is that space objects fall to Earth causing damage. Although it has not happened yet, cases could potentially be brought before the ICJ in the future.

5. Enforcement of IHL in space

One participant expressed concerns about the enforcement of IHL in outer space: is there a realistic chance to have any sort of control, as the possibility for organisations such as the ICRC or for a fact-finding commission to go to outer space seems to be very limited. One of the panellists replied that states are reluctant to agree on binding mechanisms and recalled that there is no way to hide. Data is available on Earth. In theory, investigations could be undertaken. The problem is rather a lack of political will. As of the possible establishment of a space court within ICJ, the legal expert considers such a development very likely. At the EU level, another panellist explained the technical problems of control activities in space. Systems are available, for example, one developed by a French company and operated by French air force. However, it is not perfect and there is a need to federate efforts. Whilst it works well within the EU, the US is not very willing to cooperate in terms of information exchange.

6. Can space be modified?

More specifically, a member of the audience raised the question of the applicability of a convention such as the Environmental Modification Conventions (ENMOD Convention). The experts agreed that it can be modified and that we are already modifying it by polluting it, for instance. However, it was added that most of the space treaties were adopted before the environmental movement, which dates back to the 1970s, so that there are very few provisions in the relevant treaties dealing with this specific issue. The only provision to be mentioned would be Article 9 of the Outer Space Treaty avoiding contamination in and from outer space. It should also be noted that a Moon Agreement was adopted, which intends to regulate the commercial exploitation of natural resources from the moon. With respect to the applicability of the precautionary approach to these issues, it was argued that it could discourage entrepreneurs and private enterprises which currently hold the technology , by making it too expensive. However, the political will might again be lacking.

Panel Discussion
How will technological development challenge IHL in the 21st century?

Chair person: **Eric David,** *Université Libre de Bruxelles*

Professor Marco SASSOLI

University of Geneva

After this day and a half, I have a great admiration for persons who are not represented here: the Taliban. Despite all these space capacities, robots etc., these people who do not have any of these technologies have succeeded to resist, for nine years, against those who have such capacities. If the Taliban did not exist, I would have said that it is no longer possible to conduct an armed conflict against States with such capacities, because he or she would automatically and immediately lose.

Over the course of the Colloquium, there were many questions and fewer conclusions. This is understandable because it is difficult for human spirits, at least for non-experts, to come to conclusions. However, it is important to raise our awareness and to honestly consider the different aspects.

We have heard that the rules must be adapted in light of the technology. Here, I think about the enemy. The enemy also wants to adapt the rules to the technology it has available. If an enemy has only suicide bombers available, should we adapt the rule? A war is always a relationship between two parties and we need to be careful not to adapt the law to the technology that is only available to one party. I think international humanitarian law (IHL) no longer serves its purposes when the law is realistic for one party only. This is why it probably has to remain at a certain level of abstraction. Rules apply according to their text, as understood according to their object, purpose and context, including to new phenomena not foreseen at the time of drafting, until new law is adopted. There, customary law complicates the issue. But we cannot simply say that because three or five states do certain things, a new customary law which derogates from the old rules has entered into force.

I am a little sceptical about the difference between rules and principles. For me, people who say that they will only comply with principles are always suspected of not wanting to comply with the rules.

The greatest challenge is probably the issue of the geographic field of application. There, I do not know the right answer. IHL applies where there is an armed conflict and it is the belligerents who decide where there is an armed conflict, subject to jus ad bellum. Therefore, IHL does not say where there may be an armed conflict but it simply applies if there is an armed conflict in a certain place. But if IHL is seen as a basis for justifying certain things, then there is a problem. Some may say that we need IHL even if, for example, someone, for any reason, e.g., in self-defence, launches a missile to destroy a house in Brussels. They might say that we need IHL because it is essential that, even in such a situation, whether justified or not, the principles of proportionality, distinction, precautions for civilian population are applied. If these principles are respected, then IHL is not violated. This, however, does not become a lawful act. There are plenty of other rules in international law. Therefore, I think that we need IHL but we should not use it to legitimise a use of force. It is not because it is allowed under IHL, that it is legitimate or lawful. It remains prohibited by international law, even if it is not by IHL.

I understand the difficulty in some modern forms of warfare, when we do not know who perpetrated a specific action. But this too could probably be brought back under the old rules. Indeed, it is also possible in ‘old’ warfare that we do not know who did it. What counts is the effect of attacks on people. I agree that there are some new problems when there is use of non-kinetic force because the rules were made in view of use of kinetic force. But we do not have to rethink the rules; we can interpret them to apply them to the new reality.

On robots, I am not sure if it is easier to programme humans than robots or machines, because humans have a moral choice which can also go against the respect of the law. A robot can fail but it will never be its decision not to follow the rules and this can be an advantage.

As a conclusion, I would say that the same rules should be applied to and interpreted in view of the new phenomenon. New technology is governed by existing rules, but the new technology may bring us to adopt new rules. To give an example, if tomorrow technology enables us to drive 500 km per hour with a car, no one will say that the traffic code is no longer adapted to this new technology. We would say that you can not use this technology for the time being, until we have developed the technology up to the point where it is able to comply with the rules.

Professor Jack BEARD
University of California, Los Angeles

Preliminary note: Please note that Professor Beard's comments were illustrated by a power point presentation which is not reproduced in the following, but is explained whenever necessary.

I, of course, agree that we are not here to throw out international humanitarian law (IHL) in the face of new technological developments. Instead, we are required to look for the deeper meaning of fundamental IHL principles and their appropriate application in these new, dynamic circumstances. I do, however, think that there are some serious risks presented by the undisciplined application of IHL to all manners of unfriendly or hostile actions in cyberspace. In particular, it seems unwise to diminish the high threshold established by Article 51 of the UN Charter for 'armed attacks' in this area. Such an approach could dramatically widen the scope of armed conflicts and encompass far too many ambiguous acts involving fingers pressing the keyboards of computers. With respect to remote-controlled weapons, the ability of States to conduct attacks from afar with no accompanying risk to human operators continues to raise the question of whether such weapons will ultimately diminish restraints on States going to war. Finally, I believe that certain types of advanced autonomous weapons will present serious challenges to IHL and will highlight implicit requirements for human judgement and control, particularly in applying the principles of distinction and proportionality in complex situations where the risk of civilian casualties is high.

At this point, I would also like you to look for a moment at some of the new technologies surrounding us and take a slightly larger view of the subjects that we have been discussing. First, it is the supreme arrogance of States to believe that newly-developed weapon systems and military technologies will always belong only to them - history instead teaches that such systems and technologies ultimately find their way into the arsenals of other States and even into the hands of non-state actors. The original military system designed to ensure communications between nuclear missile silos – which grew into what is now the internet – is today ironically perhaps Al-Qaida's most useful weapon. While transnational terrorist groups may not have access to many sophisticated weapon systems, the internet enables them to engage in decentralised communication, recruiting, fundraising and many activities that were once unimaginable for a non-state actor. Such capabilities set the stage for new forms of 'information warfare', including attempts by Al-Qaeda, the Taliban and other groups to use powerful images of civilian casualties as examples of IHL violations by allied military forces. In fact, there seems to be increasingly few information technologies which now benefit States exclusively.

Even in outer space, commercial satellites now allow non-state actors to present their side of many events with revealing imagery.

The extensive use of information technologies by non-state actors in both civil and 'non-civil' society is only part of a larger picture in which new technological capabilities are changing the way in which wars are waged in the information age. These developments often appear to outpace critical legal analysis. While we may initially be amazed with new technological devices in our personal lives, there is a tendency to quickly become unable to imagine our existence without them while at the same time failing to seriously reflect on the broader, long-term implications of these new technologies for society. The same phenomenon appears to be occurring with respect to the introduction of new information technologies into the world of armed conflict and the failure to fully assess their possible long-term impact on the observance of IHL.

As I indicated in my previous presentation, the vast new surveillance capabilities made possible by unmanned aerial vehicles (UAVs) and other new remote-controlled military technologies are clearly affecting the planning and conduct of military operations, sometimes in unexpected ways. States also appear increasingly willing to use imagery made possible by these new technologies to document their version of events in various conflict situations. For example, when there is a report of an air strike that has caused extensive civilian casualties, the US has on some occasions made surveillance videos available and essentially said: 'this is what happened, this is what we saw'. But if a state frequently engages in this sort of conduct, other governments, non-governmental organisations and media representatives may come to expect such information whenever facts in similar situations are in dispute. As I have documented, it is becoming more common for news organisations to ask governments – especially the US government – for videos or other imagery related to such controversial incidents involving the use of force.

We thus increasingly encounter situations in which States, aided by new technologies (especially remote-controlled systems), seek to provide their own video coverage of international incidents involving the use of force and various actions by their military forces. To illustrate this, you can see on the power point presentation these pictures taken by a UAV hovering over a boat that was hijacked by pirates during a recent incident off the coast of Somalia. The UAV was launched from a nearby US military vessel. Viewers at home could see the pirates holding hostages as the UAV recorded the unfolding scene from above. In this way, these new technologies are contributing to a sort of 'virtual courtroom of public opinion' that may significantly affect the way States conduct many military operations.

To conclude, it is indeed a new era, but it is not one that means international law has to be redesigned or ignored – instead its core concepts must be thoughtfully applied in the context of new technologies. It is thus worthwhile to pause and evaluate what these developments mean for promoting IHL and better ensuring compliance in the still-unfolding information age. New technologies may not only challenge IHL, but in some cases may also give it more traction than ever before.

Knut DÖRMANN
ICRC Geneva

As a starting point, we all would agree that when assessing technology from the perspective of international humanitarian law (IHL), it is without a value judgement on whether it is good or bad. We have seen throughout the discussions that there are some positive elements, such as better intelligence, better implementation of the principle of precaution, etc. But we have also heard about less legal problems that may arise: the 'play-station mentality', the bigger distance from the killings and therefore perhaps a lower threshold for the use of lethal force. All these elements need to be taken into account whenever we analyse the challenges posed by technology.

Therefore, I would take the same starting point as Professor Sassoli: any new technology must comply with existing IHL. Otherwise, how can we have a preventive approach towards avoiding civilian casualty or damage to civilian objects? If we try to make distinctions between rules and principles, it certainly creates more ambiguity and duplication of the law than it serves the law's protective value. We know how long it takes to develop specific rules for certain weapons, and the longer you allow ambiguities and duplications to develop, the more likely it is that civilians or civilian objects will be harmed.

When assessing the challenges to IHL posed by the technologies described, it is essential to first assess what the general rules mean for this specific weapon. You must go rule by rule, and see what it means for the new weapon. When there is an agreement as to what the exact meaning is, then we can have a better idea whether new rules will be required to address the specificities of new weapons. When it comes to the hard rules, for example distinction, I would always argue that, if it is technically not feasible, then you do not do it. On the other hand, I found what Herb Lin mentioned earlier very interesting, namely that, although it is complex and would involve a lot of planning, you can probably do distinction.

This very much echoes the conference organised by the International Committee of the Red Cross and Switzerland for the 60th anniversary of the Geneva Conventions, where there was a specific panel on new means and weapons. Indeed, one of the conclusions was that new technology does not change the law; rather it must be bound by the law.

However, the statement that the existing rules apply to new technologies is a good starting point but it is certainly not sufficient. We need to ask the question whether the existing law is sufficiently precise and relevant to ensure that humanitarian consequences that may be created by these new technologies are efficiently prevented. My point would be to always build on what exists and then see how to respond to particular humanitarian problems that may be caused. Computer network attacks (CNA) and cyber warfare are probably examples of where future thinking is necessary, because of certain characteristics that have been mentioned: the difficulty to identify who is behind an attack and perhaps also the likelihood of immense casualties and damages that can be caused by CNA.

When assessing what kind of new rules might be necessary, we have two options: restrictions, as we have in the context of the Convention on certain conventional weapons, or prohibitions, like we had in discussions on anti-personnel (AP) landmines and cluster munitions. Restrictions may be a solution. Daniel Reisner has mentioned this about automatic weapons, where you can define specific scenarios. I do not know if is it likely that IHL will go into these scenarios, but I do not think that we have precedents. Concerning the restrictions that we had initially in the field of landmines, one quickly came to the conclusion that they were not sufficiently precise and detailed in order to react to the humanitarian consequences of the use of AP landmines. There, perhaps, public conscience played a role when it came to new prohibitions. Indeed, the conviction arose that the most likely use of AP landmines, based on what we observed in reality, led to civilian casualties. Despite the fact that there might be lawful uses of AP landmines, fully in compliance with the principles of IHL in a minority of cases (i.e., placing AP landmines where there are no civilians), the international community can certainly take the approach of a complete ban for the benefit of protecting civilians. Is any of the technology that we have discussed so far going in this direction? For the time being and based on what we affirmed, I am not sure, but we certainly have to see clearer what CNA can cause in terms of problems.

In any case, it would be useful, if you go down the road of restriction on the use, that you have a clear determination in the treaties of how existing rules would apply to certain technology, and at least to have the same starting point as with AP landmines. If you remember, there were initially debates on planting landmines. Is it already an attack? Is it at the moment where it explodes?

With regard to drones, there is no particular need for special regulation so far. But certainly you have to assess on a case-by-case basis and see what kind of humanitarian consequences will be caused.

On automatic weapons, there will be more discussions needed regarding possible scenarios, and whether they can be better used. I would therefore reserve judgement on this issue. When it concerns truly autonomous weapons, such as artificial intelligence, it is not clear to me what is really achievable. At the conference for the 60th anniversary of the Geneva Conventions, most participants said that it is too futurist and that there is no interest for the military. This, however, needs to be observed.

The final point I would make is that, when looking at technology and interpreting existing rules, the more you try to fiddle around with different thresholds, the more likely it is, that the rules will be weakened and will lose their impact on weapons that are not specifically regulated. In particular, for CNAs, you will have to look at the definition of attack. For me, it would be a very dangerous development to exclude denial-of-service attacks from the definition of an armed attack. It would certainly render void part of the definition of a military objective which says that it may be linked to neutralisation of an object. This should be borne in mind before allowing CNA against civilian objects which almost shut down these objects. I would be interested to know how those who advocate that shutting down is not really an attack make a distinction between shutting down Wall Street and shutting down TV stations like in Belgrade. Some people would argue that it would have been fine to attack a Belgrade TV station by CNA because it is not really an attack.

Daniel REISNER[1]

Former Israel Defence Force (IDF) International Law Department

First, I would like to recall that international humanitarian law (IHL) is not biblical. It was written by men for men. It has not been written by States either, because States are virtual entities that we invented. In the end, people are responsible for drafting the Treaties and people make mistakes. Now, if you want to compare Hugo Grotius' public international law with public international law from the 19th century and with the one of now, they are very different. And in the 22nd century, we will laugh at what we once thought of international law. So, we are not absolutely right. We are just right for 2010, but please let us remain limited in our expectation of where we are.

Now, let us take it in context. We have rules and I absolutely agree that we should comply with and enforce the existing rules. There is no other way to do it. On the other hand, we have to remember that IHL is very slow, sometimes 100 years too late (I am thinking of unexploded ordnance that we were dealing with during WWI). It is also conservative with a natural tendency not to change. This is reasonable behaviour. We have international law, and we cannot break it. There is no alternative. There is no real natural law of humanity to fall back on. If we break international law, we have chaos. Therefore, we obviously have to maintain it and keep it as robust as possible.

The problem is that parts of IHL are not crystal clear and are sometimes strange. My least favourite example concerns the law of lawful weapons. It is always repeated: it is a very bad law with very inaccurate technologically and very bad logic. There is no logic behind a 398 gram projectile creating fire being unlawful and a 401 gram projectile being lawful. There is also no logic for a flechette to be unlawful but a bayonet to be lawful. It is just random choice, depending on what conventions were brought about at a certain period of time. There is a general rule of not causing unnecessary sufferings which one really does not understand how to apply. As illustrated, it is not sufficient to have the rule. It has to be clear enough to be able to advise, in real time, with yes or no answers. Many of our rules do not fill this criterion. We have to not only comply with and apply these rules, but we also constantly have to look at these rules to see which one is not clear enough so that we have make sure that people can actually live and work and die with and by them.

[1] This contribution has been written on the basis of the audio recording of the Colloquium and has not been revised by the speaker.

To this, we add the complexity that, over the last 15 years, we decided that some of these activities will lead to criminal responsibility. In all legal systems the level of clarity required in criminal proceedings is much higher than the standard level. Most of public international law lacks this level of clarity. If you look at the rulings of the international criminal tribunal for Rwanda, or for Former Yugoslavia, you will see that they are trying to fill in holes. Every single decision invents new rules for holes which they identified and for which they have no answers. All of these are challenges that we have to keep working on, taking the existing rules and clarifying them. We have to make sure that we similarly understand the same rule in different countries.

How do we address these challenges? I think for the challenges which are in evolution and not revolution, we focus on clarity. You take the existing rule and make sure that its application to this new variation is clear to everyone. I think drones fall into that category. It raised some complex questions but there is no need to change the rule. However, when you recognise that there is a potential of being revolutionary, like in my view, cybernetic warfare and automatic weapon systems, then we need to look at the rules and principles and see whether they can work in this reality. I am not saying that we have to change the rules; I am just saying that we should start by looking at them.

Another thing in international law is that there is a basic principle that not everything is prohibited. It is not like in national systems where the State is in principle only allowed to do what the laws allows it to do. In international law, it is almost generally the opposite. States can do everything they want unless it is prohibited, because international law does not put a total umbrella on States. Therefore, one of my problems is that if we do not have clear rules, and there are no clear prohibitions, sometimes as a lawyer I am able to say: *"I don't think we should be using this but there is no rule against it"*. There, the Martens Clause is not very useful. No one would accept a general statement written a long time ago with obvious ambiguity and lack of clarity as a legal basis to say that a certain new technology cannot be used, specifically after billions have been spent on developing it.

I will leave you with two thoughts. We are now talking about technological challenges of today, but what about tomorrow? The new technology which is now coming out for toys is thought-controlled toys. They have managed to understand which parts of the brain gives order and have managed to create toys for children, which you control by using thoughts with mind-readers.

The technology is already there and it has a huge potential for the military. We are talking about kinetic moving to cybernetic, but the world has already moved to the next level and is now talking about controlling thought process. Do you think that the existing rules of international law deal with this? I am not comfortable in saying this, but the technology is there.

My final point concerns the concept of international law. This is a case I give to my students: Assume that aliens come to visit our planet and think we are food. Are we obligated to apply our rules when we fight them? I asked this question because I wanted to understand the boundaries when we think that our rules apply. I am using this to show you that we have a scope, which we look at all the time, and put it in the right context.

Concluding Remarks and Closure

CONCLUSIONS DU COLLOQUE DE BRUGES 2010

Christine Beerli
Vice-Présidente du CICR

Mesdames et Messieurs,

Nous voici arrivés à la fin de nos travaux. Il m'appartient maintenant de conclure ce Colloque qui a été particulièrement riche en débats et en échanges, et d'essayer d'en résumer l'essentiel, ce qui n'est pas chose aisée au vu de la densité et la qualité des discussions.

The first session was dedicated to the new technologies on the battlefield and the challenges that they pose to the legal regulation of the means and methods of warfare. IHL has to face challenges due to the use of new means and consequently of new methods of warfare. The first challenge identified is a conceptual one as one need to understand first if new technological means can be a weapon with which an attack, in the meaning of IHL, is possible. We are also facing a normative challenge when we need to assess the principles of proportionality and precaution in attack. This assessment is even more difficult to make when the effects of the new technologies can, sometimes, appear long after the "attack" has been carried out. A third challenge, which is certainly an essential one, is the challenge of moral disengagement. Indeed the violence engaged can appear less brutal to the user of the technological system than shooting with an assault rifles in an eye-to-eye contact. This might put the limits further than it should. The asymmetry between the sophistication of enemies might also lead the less technologically advanced party to adopt methods of warfare which violate IHL, this effect being the outcome of the use of the new technologies.

The second panel raised a number of fundamental issues with respect to cyber warfare. Technical clarifications on the technology of offensive cyber operations gave us a clearer idea of possible threats but also of the technical limits of new technology. A rich discussion on the definition of the concept of cyber warfare showed us to the legal challenges related to these issues.

The most important challenge which has been identified is the question of who are the parties to a potential armed conflict – the problem of identification is key.
We heard that cyber warfare in itself does not meet the definition of armed conflict but that cyber attacks can of course be conducted during an armed conflict or in the context of wider

hostilities. Consequently the issue of what rules are applicable remains to be decided on a case by case basis.

Important questions were raised such as whether pre-existing IHL is applicable to new technologies. Is the current legal framework sufficient? Is there enough legal clarity? And is the existing IHL framework sufficiently developed to limit the humanitarian consequences of the use of new technologies?
We had a debate on the geographical field of application discussing the question of what is the conflict theatre. Is it a geographical area, or is cyberspace something different? The uncertainty concerning the answers to be given to these questions make the principle of command responsibility more difficult to handle.

The third session was focusing on the remote-controlled and autonomous weapons systems and was supported by numerous practical examples. The emphasis was put on the fact that behind every remote-controlled or autonomous weapons system there is, indeed, a human being handling it, to which the command responsibility can be applied. It was also underlined that new technologies offer not only new capabilities, with both positive and negative effects, but also new types of vulnerabilities for those using them. For example, the videos produced by "uninhabited" vehicles not only give essential information before and during an attack, but also after an attack. This will probably lead to an important change in the way investigations and prosecutions are conducted. It was underlined that a long series of legal questions related to the possibilities offered by new technologies are to be answered. This will definitely be a challenge for the lawyers.

We had a stimulating presentation on the role robots can take on the battlefield and the qualitative advantage they can have on human beings by being programmed to respect certain rules and not be influenced by emotions. Evidence was presented that indeed "human soldiers" recognize not to behave in conformity with the law in a certain number of difficult situations, which would not be the case of robots programmed to react in a certain way. Ethical consideration can therefore be taken into consideration when designing, producing and programming robots.
It was stressed that the use of autonomous weapons system is, in itself, a challenge to usual military training as it brings a whole change in the capacities to analyse situations. Additionally, the understanding of how autonomous weapons systems are working is generally very poor which also poses challenges to the commander. From these assumptions we could either conclude just to refuse using them, which is not a realistic stand, or trying to make sure that principles and systems are compatible. Principles like proportionality, distinction and commander responsibility are here to be seriously considered. A recommendation was made to

maybe have categories of autonomous weapons system that could be used in specific situations in order to be able to apply principles, like the command responsibility of using one or the other weapons system. The speakers have also underlined on many occasions that we are not discussing on what could become reality, but we are already there and a serious consideration of these points is definitely required.

I will not recall what has been discussed during the last panel discussion as the debates are still fresh in your mind. But I will briefly come back on the first morning session that was devoted to the outer-space as, potentially, a new conflict theatre. The first speaker has brilliantly explained us the orbital mechanics and peculiarities of the space flight and the constraints that this does pose for space activities, including e.g. for obtaining images from a specific location. We learned how fragile the satellites are and the consequences that the destruction a few satellites can have on an entire orbit that could be easily rendered useless. We discussed legal regulations and it was underlined that even there is a lot of space law today, more work remains to be done, especially on the military activities carried out from space, or maybe, one day, in space, if space becomes a conflict theatre as such. Some particular weapons are forbidden in space, like the nuclear weapons and other weapons of mass destruction. But other weapons can indeed be legally deployed in space, raising more and more concern about a space arms race. From the discussions we had, there seems to be nothing restricting the application of *jus in bello* in space both for "passive" military activities as well as if space become an active theatre of warfare, and there is indeed an increasing likelihood that it will be the case sooner or later. Here too, more thinking on the concrete application of existing IHL to space activities is needed.

Mesdames et Messieurs,

Le CICR a bien entendu l'appel des scientifiques demandant instamment que des études sérieuses soient menées sur les questions soulevées lors de ce colloque. Nous sommes attentifs à ces préoccupations et allons certainement pousser la réflexion plus loin. Nous avons été, en effet, particulièrement frappés par l'ampleur des possibilités que les nouvelles technologies peuvent apporter pour améliorer le respect du DIH, mais également des risques que les développements de ces technologies peuvent engendrer dans le cadre de conflits armés ou d'autres situations de violence organisée.

Je vous remercie de votre attention et vous invite d'ores et déjà au 12ème Colloque de Bruges qui aura lieu la troisième semaine d'octobre 2011.

PARTICIPANTS LIST
LISTE DES PARTICIPANTS

- **AGTEN Toon**
  K.U. Leuven
- **ARKIN Ronald**
  Georgia Institute of Technology, College of Computing
- **ATTAHERI Mimoun**
  Faculte Pluridisciplinaire/ NADOR/MAROC
- **BAETENS Freya**
  Leiden University, Grotius Centre for International Legal Studies
- **BARTELS Rogier**
  Netherlands Defence Academy/District Court of Rotterdam
- **BEARD Jack**
  University of California
- **BEERLI Christine**
  ICRC
- **BEHLOUL Agnès**
  Paris X Nanterre / UMPF Grenoble
- **BELLON François**
  ICRC
- **BERGHEN Esmeralda**
  Royal Military Academy – Belgium
- **BIAUMET Gilles**
  GRAPAX (CReSPo/FUSL)
- **BOEVA Antoaneta**
  NATO
- **BOUTRUCHE Theo**
- **BRANDAO Caroline**
  Croix-Rouge française
- **BREHM Maya**
  UNIDIR
- **BRESLIN Andrea**
  National University of Ireland, Galway
- **CAMUS Emilie**
  ICRC

- **CASIER Frédéric**
  Croix-Rouge de Belgique (Fr)
- **CLOUVEL Matthieu**
  Ministère des affaires étrangères, Direction des affaires juridiques - France
- **COLLIENNE Fleur**
  Université de Liège
- **CREVECOEUR Dominique**
  Défense – Direction générale Appui juridique et Médiation – Belgique
- **CUYCKENS Hanne**
  Institute for International law, K.U. Leuven
- **DANAU Marcel**
  Centre d'Etude de Droit militaire et de Droit de la Guerre - Belgique
- **DASKALOVA Ana**
  Council of the European Union
- **DAVID Eric**
  Université Libre de Bruxelles (ULB)
- **DE TANT Hans**
  Royal Military Academy - Belgium
- **DE VIDTS Baldwin**
  San Remo Institute
- **DECKMYN Annelies**
  College of Europe
- **DEL MONTE Luca**
  European Space Agency
- **DEMEYERE Bruno**
  Leuven Centre for Global Governance Studies, Katholieke Universiteit Leuven
- **DESCH Thomas**
  Ministry of Defence – Austria
- **DOERMANN Knut**
  ICRC
- **DOUCET Ghislaine**
  CICR
- **DRYBOOMS Eric**
  Royal Military Academy, Belgium
- **DUCHEINE Paul**
  Netherlands Defence College / Faculty Military Sciences
- **DURHIN Nathalie**
  Ministère de la défense français – direction des affaires juridiques

- **FREELAND Steven**
  University of Western Sydney and University of Copenhagen
- **GALLANT Johan**
  Royal Military Academy - Belgium
- **GARNIER Paul**
  Mission suisse auprès de l'OTAN
- **GEISBACHEROVA Daniela**
  Ministry of Defence – Slovakia
- **GEISS Robin**
  ICRC
- **GERMOND Thierry**
  ex CICR
- **GOES Benjamin**
  SPF Chancellerie du Premier Ministre – Belgique
- **GOSSELIN Caroline**
  ICRC
- **HANF Dominik**
  College of Europe
- **HECTOR Mireille**
  Ministry of Foreign Affairs, The Netherlands
- **HEINSCH Robert**
  Leiden University
- **HELINCK Pauline**
  Université de Liège
- **HENNEAUX Benoit**
  Ministère de la Défense – Belgique
- **HUYGHE Patrick**
  Ecole Royale Militaire – Belgique
- **JULLIEN Gaelle**
  Université de Liège
- **KACPERSKA Agnieszka**
  Ministry of Foreign Affairs, Poland
- **KELDERS Jeroen**
  Royal Military Academy - Belgium
- **KLEFFNER Jann K.**
  Swedish National Defence College
- **KODAR Erki**
  Estonian Ministry of Defence

- **KOLANOWSKI Stéphane**
  ICRC

- **KOOYMAN Elke**
  Chartis

- **KOZIK Andrei**
  International Institute of Labour and Social Relations – Minsk

- **LELIEVRE Chloe**
  Université Paris Ouest Nanterre La Défense

- **LIN Herb**
  US National Research Council of the National Academies, Computer Science and Telecommunications Board

- **LINGAAS Carola**
  Norwegian Red Cross

- **LORIAUX Gérard**
  Centre d'Etude de Droit militaire et de Droit de la Guerre – Belgique

- **LUBELL Noam**
  National University of Ireland, Galway

- **MAGLIA Laura**
  NATO

- **MAKRIS Vasileios**
  HELLENIC NATIONAL DEFENCE GENERAL STAFF

- **MASCIA Roberto**
  NATO Joint Force Command Brunssum HQ

- **MASSCHELEIN Liesbet**
  FOD Kanselarij van de Eerste Minister – Belgium

- **MILLET-DEVALLE Anne**
  UFR IDPD UNIVERSITÉ DE NICE

- **MONTENEGRO Pedro**
  Mission of Brazil to the European Union

- **MULVEIN Helen**
  Foreign & Commonwealth Office, UK

- **NEYRINCK Roeland**
  Belgian Red Cross – Flanders

- **NOOTENS Laureline**
  Croix-Rouge de Belgique (Fr)

- **OCHMANNOVA Petra**
  Ministry of Defence – Czech Rep.

- **PARREIN Pieter-Jan**
  Royal High Institute for Defence

- **PÉRILLAT-PIRATOINE Xavier**
  Armée de l'Air, France
- **PIETERS Boukje**
  Netherlands Red Cross
- **POUW Eric**
  Netherlands Defence Academy
- **RAINNE Juha**
  Mission of Finland to NATO
- **REISNER Daniel**
  Formerly Israel Defence Force
- **ROELAND Geert**
  Defense Belge
- **ROSSELLO Stephanie**
  K.U. Leuven
- **SAGON Hilde**
  ICRC
- **SASSOLI Marco**
  University of Geneva
- **SCHAUMANS Charlotte**
  KULeuven
- **SCHMIDT Martin**
  German Permanent Delegation to NATO, Brussels
- **SCHWENDIMANN Felix**
  Directorate of International Law - Swiss DFAE
- **SOUSA Alejandro**
  Ambassade du Mexique auprès de l'UE
- **STELMASZEWSKI Jessica**
  Université de Liège
- **STOCKBROECKX Sanne**
  K.U. Leuven
- **STOIBER Benedikt**
  NATO Headquarters
- **SWINKELS Nicoline**
  NATO
- **VAN DAMME Steven**
  Oxfam Belgium
- **VANDECASTEELE Jean-Pierre h.a.**
  Belgian Defense

- **VANDEN DRIESSCHE Thomas**
  ICRC
- **VERMEER Arjen**
  Netherlands Red Cross
- **VINKOVIĆ Zoran**
  The District Attorney’s Office - Croatia
- **WALDT Adrianne**
  Belgian Red Cross Flanders
- **WALTHER Pernille**
  Danish Red Cross
- **WARNOTTE Pauline**
  SPF Justice – Belgique
- **ZWANENBURG Marten**
  Ministry of Defense, Netherlands

PROGRAMME: TECHNOLOGICAL CHALLENGES FOR THE HUMANITARIAN LEGAL FRAMEWORK
PROGRAMME : LES DÉFIS TECHNOLOGIQUES POSÉS AU CADRE JURIDIQUE HUMANITAIRE

11th Bruges Colloquium – 21st-22nd October 2010
11ème Colloque de Bruges, 21-22 octobre 2010

Simultaneous translation into French and English will be provided
Traduction simultanée anglais/français

DAY 1: Thursday, 21st October

9:00-9:30	Registration and Coffee
9:30-9:40	Welcome address by **Prof. Dominik Hanf,** Professor at the College of Europe
9:40-9:50	Welcome address by **Mr. François Bellon**, Head of the ICRC Delegation to the Kingdom of Belgium, the EU and NATO
9:50-10:10	Keynote address by **Ms. Christine Beerli,** Vice-President of the ICRC
10:10-10:30	Coffee break

Session One: New Technology on the Battlefield

Chair person: **Marten Zwanenburg**, Ministry of Defence, The Netherlands

10:50-11:10	CURRENT CHALLENGES IN THE LEGAL REGULATION OF THE MEANS OF WARFARE Speaker: **Jann Kleffner**, Swedish National Defence College
11:10-1:30	CURRENT CHALLENGES IN THE LEGAL REGULATION OF THE METHODS OF WARFARE Speaker: **Théo Boutruche**, Consultant in international human rights and humanitarian law
11:30-12:30	Discussion
12:30-14:00	Sandwich lunch

Session Two: Cyber Warfare

Chair person: **Knut Doermann**, ICRC Geneva

14:00-14:20 TECHNOLOGY: WHAT IS POSSIBLE IN TERMS OF ATTACK?
Speaker: **Herb Lin**, Computer Science and Telecommunications Board, National Research Council of the National Academies, USA

14:20-14:40 BETWEEN CYBER CRIME, CYBER TERRORISM AND CYBER WARFARE. WHERE TO DRAW THE LINE?
Speaker: **Noam Lubell**, National University of Ireland, Galway

14:40-15:00 THE LEGAL REGULATION OF CYBER ATTACKS IN TIMES OF ARMED CONFLICT
Speaker: **Robin Geiss**, ICRC Geneva

15:00-15:45 Discussion

15:45-16:00 Coffee break

Session Three: Remote-controlled and Autonomous Weapons Systems

Chair person: **Stéphane Kolanowski**, ICRC Brussels

16.00-16.20 REMOTE-CONTROLLED WEAPONS SYSTEMS AND THE APPLICATION OF IHL
Speaker: **Jack Beard**, University of California, Los Angeles

16:20-16:40 ROBOTS ON THE BATTLEFIELD
Speaker: **Ronald Arkin**, Georgia Institute of Technology

16:40-17:00 AUTONOMOUS WEAPONS SYSTEMS AND THE APPLICATION OF IHL
Speaker: **Daniel Reisner**, Formerly Israel Defence Force (IDF) International Law Department

17:00-18:00 Discussion

19:30-22:30 Dinner

DAY 2: Friday, 22nd October

Session Four: Outer Space – A New Conflict Theatre?

Chair person: **Marco Sassoli**, University of Geneva

9:00-9:20 SPACE WEAPONS – WHAT'S POSSIBLE, WHAT'S NOT?
Speaker: **Luca Del Monte**, Space Security Office, European Space Agency, France

9:20-9:40 LEGAL REGULATION OF THE MILITARY USE OF OUTER SPACE
Speaker: **Steven Freeland**, University of Western Sydney and University of Copenhagen

9:40-10:10 Discussion

10:10-10:40 Coffee break

Panel Discussion: How Will Technological Development Challenge IHL in the 21st Century?

Chair person: **Eric David**, Université Libre de Bruxelles

10.40-12.30 Panelists
Marco Sassoli, University of Geneva
Jack Beard, University of California, Los Angeles
Knut Doermann, ICRC Geneva
Daniel Reisner, Former Israel Defence Force (IDF) International Law Department

Concluding Remarks and Closure

12.30-13.00 **Concluding remarks**
Ms. Christine Beerli, Vice-President of the ICRC

SPEAKERS' BIOS
CURRICULUM VITAE DES ORATEURS

Opening Session/Session d'introduction

Dominik Hanf is Professor of European Law at the College of Europe since 2002. He teaches the Constitutional Law of the European Union in Bruges (European Legal Studies Programme) and the Substantive Law of the European Union in Natolin/Warsaw (European Interdisciplinary Studies Programme). Dominik Hanf received his Law Degree (*Erstes juristisches Staatsexamen*) and passed the Bar Exam (*Zweites juristisches Staatsexamen*) in Germany. He holds a Ph.D (*Doctor iuris*) in Comparative Constitutional Law from the Johannes-Gutenberg-Universität Mainz and a Ph.D (*Docteur en droit*) in European Law from the Université de Liège where he served as a Senior Researcher (*Chargé de recherches*) before joining the College of Europe. Dominik held several visiting professorships in Europe and abroad. Areas of research are constitutional and Substantive Law of the European Union; Comparative Constitutional Law; External relations of the EU; Differentiation in EU Law.

François Bellon is the Head of the ICRC Delegation to the Kingdom of Belgium, the European Union and NATO in Brussels since August 2010. Mr Bellon joined the ICRC in 1984, and has occupied numerous positions within the ICRC. Prior to Brussels, he has been the Head of ICRC Regional Delegation for the Russian Federation (2006-2010), the Head of Delegation in Israël (2002-2005), in Georgia (1999-2002), in Budapest (1997-99), and in the Federal Republic of Yougoslavia (1994-97). Before that, Mr Bellon did several ICRC field missions in Azerbaijan (Nagorni Karabakh), Moldova, Bosnia-Herzegovina, Sri Lanka, Pakistan, Iraq and Lebanon. He also served at the ICRC Headquarters at the Middle East and North Africa Desk as well as in the Legal Division. He holds a Master in Law from the Lausanne University in Switzerland and completed a Postgraduate course in conflict management and emergency response at the Complutense University in Madrid.

Christine Beerli, Vice-President of the International Committee of the Red Cross, was born in 1953. A member of a law firm in Biel, Ms Beerli began her political career on that city's municipal council, where she served from 1980 to 1983. From 1986 to 1991 she was a member of the legislative assembly of the Canton of Bern. In 1991 she was elected to the upper house of the Swiss parliament, where she remained until 2003, chairing the foreign affairs committee (1998-99) and the committee for social security and health (2000-01). Ms Beerli chaired the caucus of the Free Democratic Party in Switzerland's federal assembly from 1996 to 2003. She also served on committees dealing with security policy and economic and legal affairs. She retired from politics in 2003. Since 1 January 2006, she has headed Swissmedic, the Swiss supervisory authority for therapeutic products. She is former director of the School of Engineering and Information Technology at Bern University of Applied Sciences.

Session One/1ère session

Marten Zwanenburg is a senior legal advisor with the Directorate of Legal Affairs, International and Legal Policy Affairs Section of the Ministry of Defense of the Netherlands, where he advises primarily on international law and military operational law issues. He also teaches a course on UN peacekeeping in the Master of Advanced Studies in International Public Law program at Leiden University. Marten has published widely on International Humanitarian Law and collective security law. His PhD dissertation 'Accountability of Peace Support Operations' was published by Brill publishers in 2005, and received several prizes including the 2006 Paul Reuter prize of the International Committee of the Red Cross. Marten is an editor of the Military Law and the Law of War Review.

Jann Kleffner is the Head of the International Law Center and an Associate Professor of International Law at the Swedish National Defence College. He holds a LLM degree in International law and a PhD from the University of Amsterdam. In the past, Mr Kleffner has been working with the International Tribunal for Former Yugoslavia and the International Criminal Court. He has also been an Assistant Professor and a Visiting Professor in numerous academic institutions and universities, and a general rapporteur to the International Society of Military Law and the Law of War (2000-2003). More recently, Jann has been an Advisor with the UN Interregional Crime and Justice Research Institute (UNICRI) on the ICC Judicial Summaries Project, and an Expert on a project to develop Manual on the International Law Applicable in Cyber Warfare with Durham University Law School and the Cooperative Cyber Defence Center of Excellence. Mr. Kleffner is a member of several Law societies and has published widely.

Theo Boutruche holds a PhD in Law from the Graduate Institute of International and Development Studies (Geneva) and from the Aix-Marseille Faculty of Law (France). He is currently a consultant in international human rights and humanitarian law. He worked previously as a Teaching and Research Assistant at the Public International Law Department of the Faculty of Law in Geneva and as an Associate Human Rights Officer within the UN High Commissioner for Human Rights. More recently, he worked as the IHL/Human Rights Expert of the Independent International Fact-Finding Mission on the Conflict in Georgia created by the European Union. He published several articles in law reviews and contributions to books on international law related issues, including a number of publications on the regulation of means and methods of warfare under IHL. His PhD thesis on "The Prohibition of Superfluous Injury or Unnecessary Suffering in International Humanitarian Law" was recently awarded the 2009 ICRC Paul Reuter Prize for international humanitarian law.

Session Two/2ème session

Knut Dörmann is Head of the Legal Division of the International Committee of the Red Cross (ICRC) since December 2007. He had been Deputy Head of the Legal Division between June 2004 and November 2007 and Legal Adviser at the Legal Division between December 1998 and May 2004. He was a member of the ICRC Delegation to the Preparatory Commission of the International Criminal Court. He holds a Doctor of Laws (Dr. Iur.) from the University of Bochum in Germany (2001). He was Managing Editor of Humanitäres Völkerrecht - Informationsschriften (1991-1997). Prior to joining the ICRC, he was Research Assistant (1988-1993) and Research Associate (1993-1997) at the Institute for International Law of Peace and Armed Conflict, University of Bochum. Dr. Dörmann is and has been a member of several groups of experts working on the current challenges of international humanitarian law. He has extensively presented and published on international law of peace, international humanitarian law and international criminal law. He received the 2005 Certificate of Merit of the American Society of International Law for his book *Elements of War Crimes under the Rome Statute of the International Criminal Court*, published by Cambridge University Press.

Herbert Lin is chief scientist at the Computer Science and Telecommunications Board, National Research Council of the National Academies, where he has been study director of major projects on public policy and information technology. These studies include a study on national cryptography, a study on the future of computer science, a study of Defense Department systems for command, control, communications, computing, and intelligence, a study on workforce issues in high-technology, a study on protecting kids from Internet pornography and sexual exploitation, a study on aspects of the FBI's information technology modernization program, a study on electronic voting, a study on computational biology, a study on privacy and information technology, a study on cybersecurity research, a study on healthcare informatics, and a study on offensive information warfare. Prior to his NRC service, he was a professional staff member and staff scientist for the House Armed Services Committee (1986-1990), where his portfolio included defense policy and arms control issues. He received his doctorate in physics from MIT. Apart from his CSTB work, he is published in cognitive science, science education, biophysics, and arms control and defense policy.

Noam Lubell is a Lecturer in international law at the Irish Centre for Human Rights, National University of Ireland, Galway. In previous years he was the Co-Director of an International Law Amicus Curiae Clinic at the Concord Research Centre in Israel, a Visiting Research Fellow at the Hebrew University, Jerusalem, and prior to that he was a Senior Researcher at the Human Rights Centre at the University of Essex. He has taught courses on international human rights law and the laws of armed conflict in a number of academic institutions, including the University of Essex, Oxford University, and as a Visiting Professor at Case Western Reserve

University in the US. Alongside his academic work Dr. Lubell has worked with various human rights NGOs dealing with the Israeli/Palestinian conflict. He is also a member of the Executive Committee of Amnesty International (Ireland). He has provided consultancies and training in human rights law and the laws of armed conflict, for international bodies such as Amnesty International, various government bodies, and the BBC.

Robin Geiß is Legal Adviser for the International Committee of the Red Cross (ICRC) in Geneva. He completed his First and Second State Exam in Law in Germany and was conferred his doctorate for a thesis on "Failed States" in 2003. He also holds an LL.M. degree in "International Legal Studies" from New York University. Before joining the Legal Division of the ICRC in 2007 Robin Geiß worked as a Research Fellow at the Walther Schücking Institute for International Law in Kiel, New York University and the Bucerius Law School in Hamburg. He has published in a wide range of scholarly journals and regularly lectures on human rights law and international humanitarian law.

Session Three/3ème session

Stéphane Kolanowski holds a Law Degree and a Master in Laws (LL.M.) in Public International Law. He joined the ICRC Legal Division (Geneva) in 1997, where he worked on different issues, such as Human Rights, impunity and reparation, as well as on some arms related issues. In 1999, he participated in the build-up of the ICRC Delegation to the EU and NATO, a Delegation in which he is still working today as a Legal Adviser. He is responsible for following relevant legal developments in EU and NATO policies and operations and for promoting and disseminating International Humanitarian Law for several audiences. In 1999, he also initiated the cooperation with the College of Europe, leading to the organisation of the yearly Bruges Colloquium.

Jack M. Beard has served as a professorial lecturer and scholar-in-residence at the UCLA School of Law since 2005. He previously held the position of Associate Deputy General Counsel (International Affairs) in the Office of the Secretary of Defense, from 1990 to 2004. In addition to holding senior civilian legal positions in the U.S. Government, he also served as an officer in the Judge Advocate General's Corps and is a retired Lieutenant Colonel in the U.S. Army. He received a B.S. degree *magna cum laude* from Georgetown University, a J.D. *magna cum laude* from the University of Michigan Law School, and an LL.M. in International and Comparative Law from Georgetown Law. Professor Beard has written articles on international law and the use of force, the law of war, terrorism, and international efforts to prevent the proliferation of weapons of mass destruction. His recent article in the American Journal of International Law entitled "Law and War in the Virtual Era" examines the implications for modern armed conflicts and international humanitarian law of remote-controlled or "virtual" weapons systems. He is currently working on a book under contract with Oxford University Press entitled “Modern Technology and the Law of Armed Conflict.”

Ronald C. Arkin is Regents’ Professor, Associate Dean for Research, and the Director of the Mobile Robot Laboratory in the College of Computing at the Georgia Institute of Technology. Professor Arkin served as STINT visiting Professor at the Centre for Autonomous Systems at the Royal Institute of Technology (KTH) in Stockholm, held a Sabbatical Chair at the Sony Intelligence Dynamics Laboratory in Tokyo and then served as a member of the Robotics and Artificial Intelligence Group at LAAS/CNRS in Toulouse. Dr. Arkin’s research interests include behavior-based reactive control, hybrid deliberative/reactive software architectures, robot survivability, multiagent robotic systems, biorobotics, human-robot interaction, robot ethics, and learning in autonomous systems. He has over 170 technical publications in these areas. Books Prof. Arkin has written include *Behavior-Based Robotics, Robot Colonies and Governing Lethal Behavior in Autonomous Robots.* Dr. Arkin is the Series Editor for the MIT Press book series Intelligent Robotics and Autonomous Agents. He serves on the Board of Governors of the IEEE Society on Social Implications of Technology, served on the Administrative Committee of the IEEE Robotics and Automation Society, served as a founding co-chair of the IEEE RAS Technical Committee on Robot Ethics and co-chairs of the Society’s Human Rights and Ethics Committee. He was elected a Fellow of the IEEE in 2003.

Daniel Reisner is one of Israel’s leading public international law practitioners, a result of his 20 year career in government in this field, including 10 years as head of the Israel Defense Force’s International Law Department. His areas of expertise are extensive, and include laws of war, human rights, legal aspects of counter-terrorism, peacekeeping, border disputes, transboundary natural resources, maritime law and many others. In parallel to the above, from 1994 onwards, Daniel Reisner served as a senior member of Israel’s peace delegations with both Jordan and the Palestinians, working in the triple role of negotiator, legal advisor and drafter. In this capacity, he has advised Prime Ministers Rabin, Peres, Netanyahu, Barak, Sharon and Olmert, and participated in most of the negotiation sessions and summits, including those in Amman, Wye River, Camp David and Taba. Today, Daniel Reisner is the International Law, Defense and Homeland Security partner at Herzog, Fox & Neeman, Israel’s leading law firm. As part of his practice, Reisner advises governments and leading international corporations on wide variety of international law, defense and homeland security related issues, including policy, commercial and regulatory aspects. His clients include some of the world’s leading technological leaders in the defense and homeland security fields. Parallel to his professional career, Daniel has also pursued an active academic career. He teaches in three of Israel’s leading academic institutions, has published articles on a variety of issues and is a highly sought after lecturer and panellist, both in Israel and abroad. Concurrently, he continues to advise the senior members of the Israeli government on a variety of issues relating to the Middle East peace process and security issues. Most recently, Daniel Reisner has been requested by Prime Minister Netanyahu to serve as his Special Advisor for International Affairs, in support of Netanyahu's peace talks with the Palestinians.

Session Four/4ème session

Marco Sassòli is professor of international law and director of the Department of international law and international organization at the University of Geneva. From 2001-2003, he has been professor of international law at the Université du Québec à Montreal (Canada), where he remains associate professor. He is also associate professor at the University Laval (Canada). He chairs the board of Geneva Call, an NGO with the objective to engage armed non-State actors to adhere to humanitarian norms. He is also Vice-Chair of the board of the International Council of Human Rights Policy. He graduated as doctor of laws at the University of Basel (Switzerland) and is member of the Swiss bar. He has worked from 1985-1997 for the International Committee of the Red Cross (ICRC) at the headquarters, *inter alia* as deputy head of its legal division, and in the field, *inter alia* as legal adviser of the ICRC delegation in Israel and the Occupied Territories, as head of the ICRC delegations in Jordan and Syria and as protection coordinator for the former Yugoslavia. Marco Sassòli's publications and research are dedicated to international humanitarian law, human rights law, international criminal law, the sources of international law and the responsibility of States and non-State actors.

Luca del Monte was hired by the rocket propulsion department of former Daimler-Benz Aerospace (now EADS) in Germany, after graduating in aeronautics and aerospace engineering at the University of Rome "La Sapienza". In 1998, he joined the Rome-based company Telespazio where he was appointed project manager in the satellite navigation business unit. In 2000, he completed a full year assignment by the European Patent Office in The Hague (the Netherlands) and, later, moved to the Italian Space Agency representing the Italian government at the ESA Ariane launcher Programme Board, the ESA Navigation Programme Board, the ESA Council and at several other international organisations. In 2002 he was hired by Paris-based ESA in the strategy department and he later moved to the Director General's Policy Office - Security Strategy and Partnership Development Office, in charge of promoting the role of ESA in the domain of the security and defence activities, as well as of launching new initiatives and programmes in this area. In particular, he was responsible for the setting up of the new European Space Situational Awareness programme, and he is now responsible for the preparation of a new space coordination framework supporting European crisis management by responsive space. Mr. del Monte is author of more than 30 scientific publications. He regularly teaches at the Rome's University Master in Space Platforms and Satellites and, in 2008 and 2009, he attended the 45th Session of the French National Defence Procurement College (CHEAr).

Steven Freeland is Professor of International Law at the University of Western Sydney, Australia, where he teaches both postgraduate and undergraduate students in International Criminal Law, Commercial Aspects of Space Law, Public International Law and Human Rights Law. He is also Associate Head of School (Research) and coordinator of the School's International Law Mooting Program. He is a Visiting Professor in International Law at the University of Copenhagen, Denmark and a Member of Faculty of the London Institute of Space Policy and Law, and has taught courses and presented guest lectures at Universities in The Netherlands, Austria, Italy, Germany, Bulgaria, United Kingdom, New Zealand, Denmark, United States, Australia and Singapore. He has also been a Visiting Professional within the Appeals Chamber at the International Criminal Court, The Hague, a member of the Australian delegation to the United Nations Committee on the Peaceful Uses of Outer Space, Vienna, and a Special Advisor to the Danish Foreign Ministry in matters related to the International Criminal Court. Among other appointments, he is a member of the Space Law Committee of the London-based International Law Association, a member of the Directorate of Studies of the Paris-based International Institute of Space Law, a member of the Australian and New Zealand Society of International Law and a Fellow of the Tim Fischer Centre for Global Trade and Finance. He sits on the Editorial Board of the *Australian Journal of Human Rights*, the *Australian International Law Journal and the China-based Space Law Review*, as well as a series of books entitled *Studies in Space Law*. He is also actively involved in the publication of a series of casebooks annotating the jurisprudence of the International Criminal Court, the International Criminal Tribunals for the former Yugoslavia and for Rwanda, the Special Court for Sierra Leone and the Special Panels for Serious Crimes in East Timor. He has published extensively on various aspects of International Law and is a frequent speaker at national and international conferences.

Panel Discussion/Table ronde

Eric David est Professeur émérite de l'Université Libre de Bruxelles (ULB) depuis le 1er octobre 2009. A l'ULB, il continue à enseigner le droit des conflits armés, domaine dans lequel ses différentes publications font autorité. Président du Centre de droit international et de la Commission consultative de DIH de la section francophone de la Croix-Rouge de Belgique, il est membre de la Commission internationale d'établissement des faits (1er PA aux CG de 1949, art. 90) et pratique le droit international comme conseil dans des affaires soumises à la Cour internationale de justice.