SEMINAR REPORT ON

CONTEMPORARY CHALLENGES IN INTERNATIONAL HUMANITARIAN LAW (IHL)

RELATED TO NEW TECHNOLOGIES

06 NOV 2015

Centre for Land Warfare Studies
New Delhi

Vij Books India Pvt Ltd
New Delhi

Report Compiled by   :   Gp Capt Puneet Bhalla

CONTENTS

CENTRE FOR LAND WARFARE STUDIES (CLAWS)

AND

INTERNATIONAL COMMITTEE OF THE RED CROSS (ICRC)

Panel Discussion on

"Contemporary Challenges in International Humanitarian Law (IHL)

Related to New Technologies"

06 Nov 2015

EXECUTIVE SUMMARY

➢ International Humanitarian Law (IHL) aims at more civilised war that seeks to avoid civilian casualties. It is relevant to 'application of armed force' in 'Armed Conflict' only.

➢ Fundamental IHL Principles are based on:

- Distinction - Between Civilians and Combatants

- Proportionality - Of Harm and Benefit.

- Precautions in Attack - minimise, to the greatest extent possible, the use of lethal force.

➢ States have to be encouraged to examine the threats and challenges arising from the development and deployment of new technologies of modern warfare.

➢ Towards new technologies, Article 36 of the API defines that states are "under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the state."

Armed UAVs

➤ Technically, if a UAV strike is launched against a legitimate military objective by using a weapon that does not cause unnecessary suffering of combatants, and the attack does not harm civilians to a degree that makes the action disproportionate, the attack complies with IHL. Any transgressions are not attributable to the characteristics or shortcomings of the technology itself but to its application by the human planners and operators involved.

Cyber Warfare

➤ Cyber Warfare is the means and methods of warfare that consist of cyber operations amounting to, or conducted in the context of, an armed conflict within the meaning of IHL.

➤ Cyber is a new domain of warfare that is challenging the current international laws of armed conflict as it is difficult to link attacks to armed conflict, they do not follow geographical boundaries and are difficult to attribute.

➤ IHL is based on assumption of resort to armed force and of resultant violent effects whereas cyber warfare might involve isolated computer operations without kinetic operation and those that might not create direct physical damage.

Autonomous Weapon Systems

➤ Categories: (i) Human-controlled (ii) Human-supervised (iii) Fully Autonomous

➤ No technology in the foreseeable future could equal human capability towards the principles of distinction, proportionality and precautions and of targeting. Therefore, a human operator would be a part of weapon systems for the foreseeable future.

➤ The interaction between technology and legal regime is a two way process. There has to be creation of legal regime to respond to technology and the technology creation itself should adhere to the legal regime.

DETAILED REPORT

Background

Technological advances are leading to unprecedented methods of warfare that present humanitarian and legal challenges. The right to choose means and methods of warfare is not unlimited. They are limited by the General rules of IHL and rules of conduct of hostility that prohibit indiscriminate attacks against civilians and limits the choice of weapon or warfare that would cause excessive suffering of combatants. Concerns are being raised regarding the legality of some forms of attack as also of attributions of responsibility of such attacks that employ new technologies. IHL rules were framed decades ago when these technologies and their employment was not contemplated. However, their development and employment in armed conflict does not occur in a legal vacuum and states have to be encouraged to examine the threats and challenges arising from these. The panel discussion brought together experts in various fields to debate and discuss relevant issues to ensure informed decisions on legal and ethical dynamics that emerge as also the relevance and evolution of the IHL to keep up with the technological challenges.

The panellists who took part in the discussion were:

- Lt Gen Davinder Kumar, PVSM VSM** (Retd) Former SO in C (Chair)

- Ms Mary Werntz, Head of Regional Delegation, ICRC, New Delhi

- Ms Supriya Rao, Legal Advisor, ICRC, New Delhi

- Gp Capt Puneet Bhalla, Senior Fellow, CLAWS

- Dr Can Akdogan, ICRC, New Delhi

- Dr Dinesh Kumar Yadavendra, Scientific Advisor to CIDS

The panel discussion was successful in initiating a debate on the challenges being faced due to the emerging technologies in relation to the International Humanitarian Law. The Panel Discussion sought to focus on three emerging technologies and came up with some important issues and recommendations.

> Armed Unmanned Aerial Vehicles – An evolution of existing systems

> Cyber Warfare - A new domain of fighting

> Autonomous Weapon Systems

International Humanitarian Law and New Technologies

International Humanitarian Law aims at more civilised war that seeks to avoid civilian casualties. It consists of four Geneva Conventions of 1949 and the first and second Additional Protocols of 1977. It does not seek to prevent armed conflicts or to confine them territorially but, rather, to regulate them whenever and wherever they occur.

IHL is applicable to application of armed force in 'Armed Conflict' only. Common Article 2 of the Geneva Conventions defines International Armed Conflict (IAC) as any "declared war or any other armed conflict which may arise between two or more States even if the state of war is not recognized by one of them." International Criminal Tribunal for the former Yugoslavia (ICTY) says that an international armed conflict exists "whenever there is a resort to armed force between States." Criteria considered for existence of IAC is Organisation of combatants, intensity of conflict and control of territory.

Besides this specific limitations or prohibitions exist against specific weapons based on treaty law and custom. In case no treaty or rule is applicable, principles of humanity & dictates of public conscience are to be applied (Martens Clause).

Fundamental IHL Principles

➢ **Distinction** - Distinction between Civilians and Combatants and between civilian objects and military objectives. As spectrum of conflict becomes predominantly sub conventional, there are challenges to this distinction even as there are increasing instances of civilians participating to a varying extent in combat without being legally permitted to do so. There are issues regarding dual purpose installations and even factories/ buildings and offices that develop the weapons that might have military objectives or those establishments that might not be developing objects solely for military purposes.

➢ **Proportionality** - Proportionality of Harm and Benefit. Any attack which may be expected to cause incidental loss of civilian life, injury to civilians, damages to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage expected to result from the attack is prohibited. This depends on anticipated goals and the assessment made by commanders.

➢ **Precautions** - All security operations must be planned, organized and controlled so as to minimise, to the greatest extent possible, the use of lethal force. Incidental effects on innocent bystanders as also the recourse to lethal force against the targeted individuals themselves should be minimised. Even post launch, constant re-evaluation is required in light of the evolving circumstances so that required adjustments can be made to avoid or minimise the expected infliction of death, injury and destruction.

Adherence to these principles depends on a number of factors. The prime among them is the perceived or evaluated security risks which additional precautionary measures may entail for the attacking forces or the civilian population.

New Technologies. Towards new technologies, Article 36 of the API defines "In the Study, development, acquisition or adoption of a new

weapon, means or method of warfare a High Contracting Party (HCP) is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the HCP." Also, all new weapons, means and methods of warfare should be subject to rigorous and multidisciplinary review.

ICRC's approach to New Technologies:

➤ Not calling for a ban

➤ Calling upon States to thoroughly reflect on whether such technologies can comply with the norms of IHL and

➤ Fix limits in the critical functions of these weapon systems so that they can be used in accordance with IHL

At present there is no legal definition for the three relatively novel systems being discussed. None of the three technologies have been specifically mentioned in weapon treaties or other legal instruments of IHL and there is no general prohibition or restriction on the development or use of these technologies.

Armed UAVs

There is an increasing employment of armed drones because of the advantages they offer –

➤ they are not restricted by human limitations, thereby providing persistent presence capability

➤ allow cheaper operations

➤ reduced combat pressure and elimination of risk of life of combatants

➤ best used for missions that are dull, dangerous or dirty

Technological enhancements have allowed development and deployment of Hunter-Killer systems that reduce the sensor to shooter cycle, providing time critical targeting. Integration of UAV technology into modern

military strategy and tactics is already a reality. Design elements and aerial refuelling are adding to endurance and operational reach of UAVs. UAV usage is only going to increase and they will be employed by more number of nations, totally replacing manned aircraft in the future.

Use of armed UAVs is increasing by countries seeking zero casualty war. However, saving military lives might come at the expense of civilian lives. Concerns regarding armed UAVs emanate from their availability allowing conduct of signature strikes of pre-selected individuals in the territory of other States and in areas marked by weakened public authority. Such strikes are increasingly being seen as a precise and effective tool with minimal downsides or collateral impacts that is best used against non state actors who otherwise cannot be contained through traditional law enforcement measures. While law of armed conflict does not require providing warning to enemy combatants before targeting them, there has been criticism regarding the subjectivity in assessment of targets.

Armed UAVs are similar in roles and employment to the manned aircraft, the only difference being in their being remotely controlled by an operator, who is expected to take decisions with due concerns for the law of armed conflict and Rules Of Engagement, including those related to distinction, proportionality and precautions. The UAV as a weapon carrying platform adheres to IHL as long as it does not carry any prohibited payload and any transgressions on its employment would be attributed to the man behind the machine and not the technology itself.

Use of remote weapons that removes combatants from combat has been criticised for making war remote with disassociation leading to dehumanising and lack of remorse. Operators of armed UAVs being operated from distant locations have been accused of PlayStation Mentality – seeing the war as a video game. Disassociation is also blamed for taking away the ability of the attacking forces to remain receptive to a declaration of surrender. Disassociation, however, is not unique to modern systems but is inherent in all long range weapons. On the contrary, slow moving UAVs might provide better capability to abort an attack on surrendering persons.

Availability of armed UAVs along with development of weapons that are increasingly becoming smaller, more precise and lethal, however, do provide concerns of quicker and increased use of force by nations. This would result from the lower risk to the life or well-being of one's own soldiers, the smaller footprint that it allows as also the lower costs, all contributing to greater political acceptability of armed conflict.

UAVs have been accused of carrying privacy invasive technologies, such as thermal imaging, communication intercepting and location tracking equipment. While these are not exclusive to UAVs, their persistent presence is known to cause adverse psychological effects on targeted civilians.

While attribution is not a concern, there are issues regarding accountability and transparency in their employment and in targeting. However, these again are not unique to the platform and depend on the human intentions and decisions.

Proponents of UAVs emphasise that:

➢ Operators have greater access to information - from both onboard sensors + Off-board information for deciding on the targets.

➢ Extended loiter time provides uninterrupted intelligence picture for better decision-making, extensive verification of targets and assessment of likelihood of collateral harm.

➢ There is reduced pressure on operating crew which is displaced from actual combat and such crew is less likely to take decisions under emotional impact. Such crew can be supervised for adherence to procedures and practices.

Cyber Warfare

Cyber Warfare is the means and methods of warfare that consist of cyber operations amounting to, or conducted in the context of, an armed conflict within the meaning of IHL. Tallinn Manual, an academic, non-binding study on how international law (in particular the jus ad bellum and IHL) applies to cyber conflicts and cyber warfare is a useful contribution. It

defines a cyber attack as a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.

Cyber is a new domain of warfare that is challenging the current international laws of armed conflict.

➢ Most cyber attacks cannot be directly linked to an armed conflict, or be necessarily conducted in an armed conflict.

➢ Cyber warfare is not limited by geographical limits.

➢ IHL assumes parties to the conflict are known, whereas anonymity is inherent to most cyber operations and attribution to a state is difficult and can be denied.

➢ Applicability of law is not possible in case of involvement of virtual organisations.

➢ IHL is based on assumption of resort to armed force and of resultant violent effects whereas cyber warfare might involve isolated computer operations without kinetic operation and those that might not create direct physical damage.

Distinction, Proportionality and Precaution - ICRC position is that impairing functionality constitutes damage. However, this aspect becomes debatable due to the distinction challenges related to dual use objects and services and interconnectivity of civilian and military systems. For effective implementation of the law, there is a need to understand the technology and intricacies of the cyber world and build situational awareness capacities. Adherence would require mission planners to have, where feasible, appropriate technical experts available to assist them in determining whether appropriate precautionary measures have been taken.

Considering any hostile cyber operation that affects functioning of objects as a resort to armed force and consequent triggering of IHL is considered to be too broad a definition to be effective. Cyber attacks in themselves might never breach the intensity threshold for existence of IAC/

NIAC and most assessments would depend on post attack consequences. However, cyber attacks do have the potential to trigger an international armed conflict and this requires definition by States.

For determination of applicability of law, a combination analysis on the severity of effect, the means used, involvement of military or other government agency and whether the target was military or not can be applied.

Autonomous Weapon Systems

Autonomous Weapon Systems are weapons which have the capability to operate without any external control and independently select and attack targets (with or without human oversight).

Categories:

➢ Human-controlled ("human-in-the-loop") - Autonomy with human oversight. Programmed to attack a particular target following a predetermined path (Cruise missiles), while humans select the target.

➢ Human-supervised ("human-on-the-loop") - Targeting and weapon release are remote controlled by the human operator. This is the current state of military robotics (Predator, Reaper, X-47 B UCAVs). The limitations of such systems are that the machines lack the flexibility to adapt to changing situations and very little reaction time is available for human intervention.

➢ Fully Autonomous ("human-out-of-the-loop") - Autonomy with no human oversight. In such machines, software algorithm enables continuous self learning and they have both Artificial Intelligence and cognitive abilities. They make independent detection, targeting and firing decision.

Defensive Autonomous Systems that can autonomously search, detect, evaluate, track, engage and kill have already been employed.

Offensive Autonomous Systems are potential killer machines. They are being used as robotic sentries in South Korea and Israel but these cannot fire without human command.

Drivers for Autonomous Weapon Systems:

➢ Decreased Personnel Requirement

➢ Reduced Reliance on Communication Links, thereby reduced system vulnerability

➢ Increased Performance And Speed Of Decision Making

Requirements for autonomous weapon systems to perform critical functions of acquiring, tracking, selecting and attacking targets:

➢ Highly accurate and discriminative sensing and vision systems

➢ Autonomous target identification and selection

➢ Situational Awareness and Flexibility

➢ Time critical decision making algorithms that incorporate the mission goals, applicable law as well as the underlying military and humanitarian values.

Distinction. Determination of target's nature based on pre-programmed characteristics such as shape and dimensions is mechanical - based on quantitative data. However this could lead to an unacceptable degree of ambiguity. It would also be difficult to distinguish combatants that are no longer in contact or are surrendering.

Proportionality. This requires Qualitative Evaluation that might lead to different conclusions in different situations, thereby requiring evaluation on case to case basis. Such subjective assessments would also require adaptability to changing circumstances as military advantage of a particular target is contextual and can rapidly change based upon battlefield developments.

While coding could take care of requirements of physical verification of the target and choose the means of attack to avoid or minimise collateral damage, it is the inherent value judgment involved in attack which is the biggest challenge for autonomous weapon systems in terms of compliance. It is debatable whether it would ever be feasible to encode quantitative and qualitative judgment, equivalent to those of the humans, into the machines.

Proponents say that coding and algorithms would allow evolving towards more acceptable form of human control or automation, wherein the machines' Rules of Engagement could be programmed in accordance with IHL. They also highlight that human moral performance and judgement is not sterile and is dependent on environmental factors.

Concerns are also being voiced regarding maintenance of effective control over self-learning robots as such machines could develop in directions and behaviour not anticipated.

Conclusion

No technology in the foreseeable future could equal human capability towards the principles of distinction, proportionality and precautions and of targeting. Artificial Intelligence will not be universal as is the case with Human Intelligence but will remain context–specific, based on the coding. Therefore, even though human control would continue to reduce, a human operator would continue to be a part of weapon systems for the foreseeable future.

The interaction between technology and legal regime is a two way process. There has to be creation of legal regime to respond to technology and the technology creation itself should adhere to the legal regime. Efforts have to be made to debate and discuss the need for new norms or evolution of the existing regime to take into account the specific characteristics of these newer technologies and their foreseeable humanitarian consequences.