1st SINGAPORE INTERNATIONAL HUMANITARIAN LAW (IHL) ROUNDTABLE

WARFARE TECHNOLOGIES AND IHL

Day/Date	: Thursday, 15 September 2022
Place	: Lee Sheridan Room, Bukit Timah campus, National University of Singapore (NUS)
Time	: 0900 hrs - 1300 hrs
Moderator	: Mr. Jeffrey Chan Wah Teck, S.C., Adjunct Professor, Faculty of Law, NUS
Emcee	: Mr. Foo Hsien Weng, Singapore Red Cross (SRC)

INTRODUCTION

This inaugural Singapore Roundtable on International Humanitarian Law (IHL) was jointly organized by the Centre for International Law of the National University of Singapore (CIL-NUS), the International Committee of the Red Cross (ICRC), and the Singapore Red Cross Society (SRC) to increase understanding and awareness on how IHL applies to weapon technologies and the limits IHL places on the development and use of such technologies, as well as how these limits are interpreted and applied by states. Specifically, this roundtable aims to establish and maintain a regular platform for Singapore policymakers, academia, and think tanks for constructive dialogue.

The programme for this 1st Roundtable is attached as Annex A.

The list of speakers and their CVs is attached as Annex B.

30 participants from various agencies and law students participated in this 1st Roundtable which was moderated by Mr Jeffrey Chan Wah Teck, SC, Adjunct Professor, Faculty of Law, National University of Singapore with Mr Foo Hsien Wang, a member of SRC, as the emcee.

SUMMARY OF PROCEEDINGS

Welcoming Remarks (by Mr Benjamin Williams, Secretary-General of Singapore Red Cross)

This Roundtable is important given the many advances made in technologies that impact on armed conflicts. New weapon technologies and methods of warfare are new means of inflicting pain on other human beings during armed conflicts. These new developments have rendered outdated many norms of IHL. The response from the humanitarian community has not kept up with these developments. IHL need to remain relevant and develop new norms to address these new developments in technologies of warfare. There are numerous challenges here, especially in asymmetrical warfare. But there are positive aspects of new technologies in warfare, including more precise targeting and thus minimizing collateral damage. The discussions at this 1st Roundtable can provide more analysis and information on these issues.

Cyber Operations and IHL (by Benjamin Ang, S Rajaratnam School of Strategic Studies)

Cyber operations (Cyberops) are either computer network attacks (CNA) or computer network exploitation (CNE). They can occur within or outside armed conflicts. If outside armed conflicts, IHL does not apply. Many non-state actors engage in CNA. States at the recent UN Open-Ended Working Group (OEWG) on Cybersecurity unanimously agreed that UN Charter, IHL and International Human Rights law (IHRL) applies in the cyberspace. However, there were questions as to how IHL would apply. The issue was whether states can regulate CNAs and CNEs by non-state actors.

It was not disputed that Human Rights Law would apply to CNAs and the use of info-comm technologies. But the difficulty is how cyberops can be made subject to IHL. An example would be a CNA against a power plant which can result in outcomes similar to the plant being bombed. IHL prohibits attacks against power plants. But in a CNA, the target is not the physical plant as such but the data required to operate that plant. Can data be classified as an "object" protected by IHL against attacks in an armed conflict? Also, if the supply of power is disrupted by a CNA, i.e. a denial of service, is this "damage" as contemplated by IHL rules? This will determine if a commander who is responsible for a CNA can be held liable for breach of IHL. Would IHL be contravened if the denial of service by a CNA results in death of civilians.

There is also uncertainty over what is meant by "destroy" in a CNA. CNAs often results in disruption but the service disrupted can ultimately be restored. Can IHL apply where a CNA does not have permanent outcomes? Also what about CNAs carried out for a long time? When does such actions cross the threshold and become an armed conflict such that IHL applies?

- A related issue would be whether IT personnel who conduct or defend against CNAs are "combatants" and thus protected under IHL. The ripple effects of the international armed conflict in Ukraine on state interactions in the development of cyber norms were also

highlighted. While many ASEAN countries have been supportive of the processes in this area, the position of other countries have become more uncertain. Are the many hackers engaged in this cyberwar combatants under IHL, even though they are not in the territory where the armed conflict is taking place. Other difficult issues include:

- Would whether a "cyber army" of individuals launching or defending against cyber-attacks independent of State directions be treated as levee en masse and combatants?
- How and to what extent are tech companies and social media platforms responsible for the online misinformation, disinformation and hate speech that may perpetuate civilian harm?
- How much of a disruption needs to take place for CNA/CNE to amount to an attack and cross the threshold of causing civilian harm?
- Should any such law developed have a retrospective effect, considering cyber-attacks that pre-date current active conflicts?

Autonomous Weapon Systems (AWS) and Artificial Intelligence (AI) in Armed Conflicts (by Professor Simon Chesterman, Dean, Faculty of Law, National University of Singapore)
Three main challenges in the development of rules to regulate AI are:

- *Speed:* e.g. on 6 May 2010 Dow Jones crashed by 1000 points but fully recovered within 30 minutes, all wholly on account of AI. As AI and machines can now operate with such speed and are developing so rapidly, rules that apply to them could easily become impractical
- *Autonomy:* While AWS are not new (e.g., landmines, heat-seeking missiles) and machines have become more efficient in targeting and overcoming human weaknesses (e.g. biases, fatigue, anger, racism), the moral and ethical question that remains ultimately is whether machines should be left to decide human life and death
- *Opacity:* given increasing complexity of machines and systems, military commanders may not fully understand what the machine could do, even if they could understand the principles and underpinnings of IHL. Is it then fair to hold human commanders fully accountable when they do not fully understand the machines they use, or when the machine malfunctions in a way the user may not be aware of?

Other related legal and ethical points include automation bias vs meaningful human control; psychological impacts of the current use of drones, the absence of human judgement of societal value of military action etc.

Use of AWS and AI in armed conflicts can be seen as the outsourcing of command decisions and responsibility to machines and the software that run them. General rule here is that governmental functions cannot be outsourced to private entities. Likewise the use of force should

not be outsourced to machines. Decisions as as targeting should not be outsourced to AWS reliant on AI.

Legal aspects of the use of biological agents in armed conflicts (by Ms Danielle Yeow, Senior Fellow, Centre for International Law, National University of Singapore)
While the law regulating biological weapons are settled in terms of the Biological Weapons Convention (BWC), it is time to consider the relevance and validity of its undertakings in view of recent scientific advancements and technological developments as the BWC allows. This review should consider and clarify the following questions:

- Should the prohibition in Article 1 BWC also cover the use of biological agents and weapons?
- Should and, if yes, how should the BWC - initially designed for bioweapons disarmament - address the humanitarian impacts and concerns of bioweapons such as relating to human health, food safety and security, the environment, and biodiversity, in its interpretation?

It was highlighted that the BWC review conferences have attempted to address some of these questions, but discussion outcomes have been unclear and limited to impacts on human health only. The review should take into consideration the Environment Modification Convention (ENMOD) (e.g. in reference to article 2) to ensure complementarity in the reading of both treaties, as well as the environmental damage that are caused by bioweapons. At the same time, domestic implementing law and policy framework such as the Biological Agents and Toxins Act (Singapore) should also be aligned with the developments at the global processes.

ICRC perspectives on weapon technologies in discussion (by Ms Sahar Haroon, Regional Legal Advisor, International Committee of the Red Cross)
The ICRC's concerns with these weapon technologies were highlighted. The human and societal cost of cyber operations, including in the targeting of humanitarian data, for example are already visible. The ICRC's position regarding AWS were recently refined to cover ethical considerations, i.e., unpredictable AWS and those that target humans should be prohibited, while all other types of AWS should be strictly regulated. These rules may be reflected in a new instrument or in any other mechanism that states may further agree on, e.g., additional protocol to the Conventional Weapons Convention (CCW). Response to this position among CCW States so far are divided. Fundamentally, AI including those linked to AWS should be used to augment, not substitute, human decision-making in civilian protection and respect for IHL on the battlefield. As the climate crisis exacerbate vulnerabilities of conflict-affected populations and local communities, the ICRC's positions and recommendations to states are now reflected in the 2020 Updated Guidelines on the Protection of Natural Environment in Armed Conflict – in complementarity with parallel UN International Law Commission work.

Open Discussion

The following are the key reflections during this segment of the roundtable:

- While the many overlapping issues exacerbate concerns, they still present opportunities for multi-stakeholder action and cooperation
- The Tallinn Manual on the International Law Applicable to Cyber Warfare ("Tallinn Manual"), soon in its version 3.0, would remain a useful guide and reference as an international effort comparable to the Oxford Process on International Law Applicable in Cyberspace. But further development of this Manual is still needed to provide for recent situations. Criticisms of the Tallinn Manual including that it was not formulated by a representative multilateral process and thus cannot be considered as setting out legal principles should also be addressed.
- On the question of how much of human intervention should there be to overcome the legal and ethical issues relating to AI/AWS, it was agreed that the human intervention must be meaningful, i.e., not necessarily in terms of military advantage and reducing casualties but in ensuring that wars are fought more humanely (e.g., by making killing difficult, efficiently addressing human flaws like bias and fatigue)
- Concerns over biases in AI systems demonstrate the need to regulate programmes to preserve societal values, and to assess how much military commanders and decision makers understand the moral and ethical questions involved in developing weapon technologies
- On whether the scope and applicability of IHL and international criminal law should be expanded to address accountability of private actors involved in hostilities (e.g. through cyber operations), it was suggested that reference to other areas of law should be considered – for example, the UN International Law Commission (ILC) draft principles on the protection of the environment in relation to armed conflicts are already addressing the liability of business enterprises

Concluding remarks

The discussion reflected the continuing relevance of IHL in addressing some key questions on the morality and perhaps, like those previously relating to the "global war on terror", on the definition of the battlefield when it comes to warfare technologies. Concerns over new technologies in warfare fundamentally remain linked to fast, disruptive, and dangerous technologies. The challenge is how to best ensure respect for the principle of humanity in armed conflicts. To overcome these challenges, ensuring good global governance and optimizing existing legal frameworks beyond IHL are key. With this in mind, the next roundtable should be framed to develop – and not merely continue – the discussion of this 1st Roundtable A record of thanks was finally expressed to everyone's valuable participation and inputs in this successful 1st Singapore Roundtable on IHL.

***** End of report *****