PANEL DISCUSSION

POSSIBLE HUMAN COST OF CYBER WARFARE

11 SEPTEMBER 2018

INSTITUTE FOR DEFENCE STUDIES AND ANALYSES, NEW DELHI

REPORT

JOINTLY ORGANISED BY
INSTITUTE FOR DEFENCE STUDIES AND ANALYSES (IDSA)
INTERNATIONAL COMMITTEE OF THE RED CROSS (ICRC)

idsa | ICRC

WELCOME ADDRESS

Yves Heller

Deputy Head of Regional Delegation, ICRC

Yves Heller opened the panel discussion thanking the Institute for Defence Studies and Analyses (IDSA) for providing a platform for discussing modern technology and warfare. Calling the ICRC the guardians of International Humanitarian Law (IHL), he said that IHL looks at modern issues like autonomous weapon systems (AWS), cyber warfare and nuclear weapons and their relationship with the principles of IHL, especially proportionality and distinction. Citing instances of software attacks on equipment and services, he stated that till today cyber attacks have not been used in the context of armed conflicts. However, he added that India sees the third highest number of cyber threats and stands second in terms of targetted cyber attacks. He stated that if critical infrastructures of States are hit by cyber attacks, civilians may be deprived of potable water, electricity, medication, education and food. Civilian casualties too may see an increase as a result of GPS systems being targetted and computer reliant structures like dams, nuclear plants may also get affected.

ICRC's interests lie in ensuring application of IHL to cyber operations in order to avoid or limit the potential damage and humanitarian consequences. It urges both state and non-state armed groups to act in accordance with international law, particularly IHL, while involved in cyber operations. He assured that the ICRC would continue to develop its expertise in IHL and protection of civilians in order to address these challenges. Even though cyberspace is an unchartered territory, the possible human cost must be understood, as in the case of AWS. He posed the following questions:

1. Given the interconnectedness of cyberspace, what structures can be constructed to protect essential civilian infrastructures?
2. Do dams and nuclear plants receive the same protection under IHL even in cyberspace?
3. What measures can States take to protect civilians and civilian objects from the hostilities taking place in cyberspace?

He stated that in the times of humanitarian needs, where laws are being systematically violated, technological innovation is an essential component of response and this cannot be impeded as a result of cyber warfare. He reiterated the critical need to exchange information in an important country like India which has an expert audience.

OPENING REMARKS BY THE CHAIR

Maj Gen Alok Deb (Retd)

Deputy Director General, IDSA

Maj Gen Deb welcomed the participants and stated that the collaboration between IDSA and the ICRC has been a fruitful one. He highlighted the need for security professionals to understand the advances in cyber warfare to work in accordance with IHL. Turning to the issue at hand, he emphasised that the cyber domain affects all aspects of civil and military operations. He raised the question of distinguishing between military and civilian domain on account of their interconnectedness. Quoting the NATO Tallinn Manual, he stated that a cyber offensive or defensive, which is reasonably expected to cause injury, death, damage or destruction to an object could also be construed as an armed conflict. He explained that cyber conflict can be viewed in two ways: cyber conflict as direct warfare and cyber conflict which is just short of war. As newer technologies like blockchain, AI and machine learning are developed, the scope of cyber warfare too, will expand.

CYBER OPERATIONS ATTACK AND WARFARE: MEANING AND SCOPE

Umesh Kadam

Consultant, ICRC

Umesh Kadam began by explaining the key terminologies within IHL which can apply to cyber conflicts. He noted that there does not exist any internationally binding legal document on cyber warfare and that current discussions are taking place in defence forums, humanitarian organisations and the United Nations. He shared that he would rely on the Tallinn Manual which describes cyber operations as "the deployment of cyber capabilities to achieve objectives in cyber space" and cyber space as "the environment for physical and non-physical components to store, modify and exchange data using computer networks". The manual also mentions cyber attack as "any operation, whether it is offensive or defensive, that is reasonably expected to cause injury or death to persons or damage, destruction of objects". Hence, cyber operations which lead to injury or death, damage or destruction are cyber attacks. He clarified that only when cyber attacks happen in the context of an armed conflict does IHL apply. Cyber warfare on the other hand, is any hostile measure against any "enemy" which is designed to discover, destroy, disrupt or transfer or store data through a computer. Traditionally, whenever armed forces of two or more States engage, it qualifies as an international armed conflict (IAC). However, in the context of cyber operations, this has been debated.

He explained that if cyber operations are conducted in the course of an already existing IAC, these operations will be regulated by IHL. Whether cyber operations in themselves can lead to an IAC is a question that is often raised. It is also possible that cyber operations alone may lead to an IAC regulated by IHL and that there could be a non-international cyber armed conflict which would also be regulated by IHL. He cited an example of the United Kingdom carrying out cyber operations against ISIS within the backdrop of a pre-existing non-international armed conflict (NIAC). Lastly, there can be cyber operations conducted outside the context of an armed conflict where IHL is not applicable. Such instances will be governed by human rights law, laws relating to State responsibility, laws relating to counter-measures and due diligence obligations of States. He acknowledged that humanitarian consequences of cyber operations outside the framework of an armed conflict are also possible and noted that there is an agreement among experts that additional rules might be needed as the existing humanitarian rules are not adequate to deal with all that is occurring in the context of cyber operations.

REMARKS BY THE CHAIR

The Chair summarised that only cyber operations which cause direct or indirect death or injury to people can be considered armed conflict where IHL would apply. He finished by stating that much work is needed for parties to come to mutually acceptable terms worldwide.

PROTECTION OFFERED BY IHL AGAINST HUMAN COST OF WARFARE

Supriya Rao

Legal Adviser, ICRC

Supriya Rao stated that her talk would focus on IHL treaties and their role in regulating cyber warfare. Stating examples of cyber attacks from media reports, she said military potential of cyberspace is only in the nascent stage. She pointed out that the human cost of these incidents are imaginable even if not specifically highlighted. Talking about regulations under IHL treaties, she explained the difference between *jus ad bellum* and *jus in bello* underlining that the aim of IHL is to mitigate suffering by protecting those who are not or no longer participating in the hostilities and by restricting the means and method of warfare. Although IHL does not refer to

cyber warfare, it still applies. The legal basis for this is rooted in the ICJ Advisory Opinion in the Nuclear Weapons case as per which the established rules of IHL apply to all forms of warfare, including those of the future and Article 36 of the Additional Protocol I (AP I) which stipulates the obligation on States to undertake a legal review of weapons which might be prohibited by IHL.

Rao alluded to the ICRC Guide on Legal Reviews of Weapons in line with the Article 36 obligation. She also spoke about the 2013 and 2015 report by the UN Group of Governmental Experts (GGE) for Development in the field of Information and Telecommunications in the context of international security, where India too participated. The GGE found that International Law, in particular the UN Charter applies to cyber warfare along with the established principles of humanity, necessity, proportionality and distinction. The 2018 Commonwealth Head of Governments meeting also adopted a declaration on cyber security expressing commitment to forward discussions on application of IHL to cyberspace.

Talking about the limits that IHL places on cyber warfare, Rao stated that IHL allows the use of lethal weapons but at the same time it aims to protect civilians and civilian objects through the rules of distinction, proportionality and precautions in attack known as the rules on the conduct of hostilities. She then highlighted how the application of IHL to cyber warfare raises some challanges for the rules on the conduct of hostilities. The principle of distinction is applicable in a cyber attack in an armed conflict. Indiscriminate attacks are those which cannot be directed at a specific military objective or the effects of which cannot be limited to a specific military objective. This then raises the issue of whether malware can be used to target a specific military objective. Disproportionate attacks are defined as those where the expected incidental loss or injury of civilian life and object is excessive to the direct military advantage. This directs one towards foreseeable military planning to ensure that the proportionality obligation may be upheld. The need to apply IHL to cyber warfare arises from the concerns to safeguard essential civilian infrastructure. Objects like dams and nuclear plants enjoy special protection. The work of hospitals cannot be interfered with, hence, a cyber attack on the information system of a hospital also violates IHL.

On the question of interconnectedness of cyberspace and the challenge it places on the rules of proportionality and distinction, she stated that since there is only one cyberspace, it is difficult to distinguish military objects from civilian cyber infrastructure. Secondly, it is difficult to foresee the incidental harm to civilians and civilian objects as it needs to be assessed in relation to obligations under IHL rules of conduct of hostilities. Thirdly, the definition of an "attack" under Article 49 of AP I as acts of violence against the adversary in offence or defence raises the issue of physical damage. Can the loss of functionality be included in that? For the ICRC, as long as an object has been damaged, it doesn't matter if it occurred through physical means or in any other way. A narrow definition of what constitutes an attack would not align with the object and purpose of IHL which is to protect civilians and civilian objects from harm to the greatest extent possible. Finally, as there exists anonymity in cyberspace, it is difficult to attribute acts to the perpetrator and if a perpetrator cannot be identified it would be difficult to know if IHL is applicable or not.

REMARKS BY THE CHAIR

The Chair highlighted challenges like the question of defining proportionality, the scope of cyber warfare in relation to information operations, accountability of corporations under IHL and the peacetime use of social cyberspace which is inimical to civilian concern.

CYBER OPERATIONS DURING ARMED CONFLICT: CURRENT MILITARY DOCTRINES AND FUTURE DEVELOPMENT

Brig Ashish Chhibbar

Senior Fellow, IDSA

Brig Chhibbar began his session by highlighting two cybercrime incidents. The first occurred in North Korea which raised the issue of movement of malware from one system to another, backdoor propagation of virus which

need not be clicked and the targetting of specific systems which did not have a particular domain name. Over 200,000 computers in over 150 countries, including India, were made redundant and the data destroyed. The second incident resulted in the payment of ransom money and destruction of data affecting Merck, a global shipping company. He stated that these cases highlight the difficulty of attributing an attack, the cascading effect of the same, the question of linkages between multinational companies and the intelligence community and the ease of undertaking an attack. Referring to the Army Manual of USA, he listed the three categories of cyberspace:

1. Physical layer
2. Logical layer
3. Cyber persona

He stated that cyberspace will always be in favour of an attacker since it wasn't created with security in mind. The three layers of cyberspace listed above can be attacked from the outside. On the question of the existing international legal mechanism, he stated that one should not expect justice where there is no binding law.

He compared the cyberspace doctrines of USA, China and Russia. In USA, the use of cyberspace for offensive operation has been acknowledged as a strategy. China's challenge is to assure that cyberspace remains available to critical infrastructure through indigenisation, to build a strategic network of power and better international governance of cyberspace which they currently view as being tilted in the favor of the West. Russia, on the other hand, is interested in the psychological aspects of cyberspace. Their national security doctrines perceive that cyberspace is used to manipulate the minds of its citizens.

He stated that in cyberspace 2.0, governmental control will increase and the access to Internet will be curtailed. He went on to state that a common global document is difficult to perceive, although bilateral and multilateral arrangements might be concluded. There will be an increased accountability of ICT companies to the government as they become party to national security concerns and disclosure of collaboration with other governments will be mandatory. He ended on the thought that weapons will become even more sophisticated, but the decision to eliminate human life will not rest with AI.

REMARKS BY THE CHAIR

The Chair stated that on one side, there is universal application of law, while on the other, there is the reality of how nations behave. Technical jargons, he believed, need to be understood by common persons as they are active users of the cyberspace. He remarked that application of IHL to the cyber

Participants attend a presentation at the panel discussion.

domain needs to be relooked continuously. He highlighted the issues of accountability and attribution and concluded that countries do come together in times of crisis but creating a preventive framework still remains a challenge.

EVOLUTION AND FUTURE OUTLOOK OF CYBER ATTACKS DIRECTED AGAINST ESSENTIAL SERVICES AND INFRASTRUCTURE

Dr Manmohan Chaturvedi

IIT Delhi

Dr Chaturvedi focussed on the evolution of critical infrastructure due to technology and India's response to the same. He stated that critical infrastructures (CI) like water, electricity etc. have an underpinning of critical information infrastructure (CII) which in turn depends on basic information technology (IT) and industrial control systems (ICS). Section 70 of the Indian IT Act, 2008 (Amendment) defines CII as "computer resources, the incapacitation or destruction of which shall have debilitating impact on the national security, economy, public health and safety". When systems are too secure, usability is limited, however, security is also essential. The four kinds of threats to national security in the cyberspace are, cyber war, cyber terrorism, cyber espionage and cyber crime. The rise in next generation networks (NGN) has increased the likelihood of cyber attacks and attacks on CI and the surface area on which cyber attacks may take place is also on the increase. Infrastructures are greatly interconnected and interdependent which leads to a cascading effect, evident in the case of natural disasters. He highlighted the various incidents of recent attacks on CI and stated that risk assessment is an immediate need. India's governance system needs to match the speed of technological advancement as regulation of critical infrastructure is essential. Under the IT Act, the National Critical Information Infrastructure Protection Centre has been formed and is the key body under the Indian regulatory system which is supposed to undertake numerous activities, such as identification of critical sub sectors, issuance of alerts, malware analysis, cyber forensic activities, awareness and training helpdesk service etc.

REMARKS BY THE CHAIR

The Chair summarised the challenge to the Indian system as one of governance versus technology. After taking into consideration the legal, military and industrial perspectives, the task comes down to bringing about an egalitarian and transparent cyber governance scheme.

Q&A SESSION

Questions related to international consensus on cyber warfare laws, trade like protectionism, precision guided system, the application of IHL on non state armed groups when they use cyber warfare and terming disabling of systems and data destruction as armed conflict.

Rao stated that there are pre-existing obligations under IHL and those not party to the Geneva Conventions will be expected to abide by Customary International Law. The ICRC does not make laws and the actual respect for the law needs to be brought at a domestic level and incorporated into military doctrine and practice. Kadam added that after some progress in 2015, the GGE received a setback in 2017 as States failed to reach a consensus on the applicability of IHL to cyber law.

On the question of precision guided systems, Rao stated that anticipating reverberating effects of an attack in the cyberspace were difficult, however, protecting civilian objects and demarcating them separately is a long standing obligation under IHL. Dr Chaturvedi explained that even though the principle of proportionality is difficult, it is a goal worth pursuing.

Brig Chhibbar pointed out that the Fourth GGE, came to the conclusion that nations would not attack critical infrastructure of other nations, they will also not attack cyber emergency response teams and they will collaborate if a territorial connect can be found between a cyber attack and a territory.

On the question of non-state armed groups, Kadam explained that IHL will continue to apply on crimes such as recruitment of child soldiers even if it takes place in the cyberspace. State are under the obligation to make sure

that cyberspace is not used to cause harm to another State under the principle of State responsibility, however, enforceability remains a challenge.

Rao explained that the ICRC has considered the act of "disabling" an attack and whether disabling a system alone, as part of the cyber operation, triggers IHL. The ICRC's commentary on Common Article 2 and 3 states that disabling alone may not be sufficient to reach the threshold. In the case of NIAC, both the criteria of intensity and organisation need to be fulfilled and if they do fulfill the criteria, an armed attack may be construed. On the question of data, she stated that if destruction of data causes harm to civilian objects, it would come under the purview of IHL.

CLOSING REMARKS

Maj Gen Alok Deb (Retd)

Deputy Director General, IDSA

Maj Gen Deb stated that we cannot wait for a catastrophe to engage in the topic of cyber warfare. He acknowledged that the work of the ICRC is difficult but governments around the world are working on these concerns. The only solution is for both to meet on common grounds. He underscored that the way forward would be to broaden the scope of interaction and include citizens of all ages.

VOTE OF THANKS

Maj Gen Sajiv Jetley (Retd)

Head of Department, Armed and Security Forces, ICRC

Maj Gen Jetley thanked everyone present at the panel discussion. He stated that the session brought forth important issues regarding cyber warfare and that these discussions needed to be followed up further with such gatherings. He thanked Maj Gen Deb and his team at IDSA, the panellists, the participants and members of the ICRC for putting together the event.

A group photograph featuring all the participants.

WHO WE ARE

The International Committee of the Red Cross (ICRC) is an independent and non-political organisation with a large scope of strictly humanitarian activities which it undertakes through its presence in over 80 countries around the world. It has a universally recognised responsibility to promote International Humanitarian Law (IHL) and to respond to the needs of people affected by situations of humanitarian concern, in particular armed conflict and violence.

Working in partnership with National Red Cross and Red Crescent Societies, local authorities and others, the ICRC provides humanitarian aid and expertise in areas such as: international humanitarian law, emergency response, health and rehabilitative services, water and habitat, livelihood support, humanitarian forensics, detention management and the restoration of family links.

The ICRC has a proven record and long history in Asia and works by engaging with all parties concerned through a unique approach based on confidential dialogue, transparent activities, sharing of expertise and partnerships in order to be able to reach and meet the needs of vulnerable persons.

@ICRC_nd
blogs.icrc.org/new-delhi

International Committee of the Red Cross
Regional Delegation for India, Nepal, Bhutan and the Maldives
C-6/6, Safdarjung Development Area
New Delhi - 110016
T: +91 11 42211000 | F: +91 11 42211068
Email: newdelhi@icrc.org | www.icrc.org/in

ICRC