No. – 3 – 2023

USI Occasional Paper

Changing Operational Scenario and Evolving Rules of Engagement

Wg Cdr UC Jha and
Gp Capt Kishore Kumar Khera (Retd)

Backdrop

War is guided and orchestrated within defined boundaries, commonly called Rules of Engagement (ROE). ROE are the commander's rules for applying armed force, arrived at with the help of a military lawyer, and implemented by those who execute military missions. ROE are designed to provide boundaries and guidance on the use of force. With the changing operational scenario, mission-specific ROE must be framed, by competent authorities, which do not hamper military operations. This paper starts with definitional aspects of ROE and follows up with the depiction of a confluence of the political, military, and legal framework in the collation of ROE. This is followed by an explanation of various types of ROE. The next section covers the planning process of framing ROE. The last section covers four specific cases of framing ROE for cyber, special operations, space, and urban warfare that have become essential components of conflict in the current century.

ROE are the commander's rules for applying armed force, arrived at with the help of a military lawyer, and implemented by those who execute military missions. ROE are designed to provide boundaries and guidance on the use of force.

Defining Rules of Engagement

In their most basic form, ROE are instructions issued to commanders and troops regulating the use of force and offensive actions in hostilities or during an operation. ROE are authorised either by national authorities or by the governing body of an international organisation following its procedures and with national agreement. States have provided different definitions for ROE with varying degrees of similarities in their national handbooks or manuals.[1] For instance, The United States Army Operational Law Handbook defines ROE as "Directives issued by the competent military authority that delineate the circumstances and limitations under which US [naval, ground, air] forces will initiate and/or continue combat engagement with other forces encountered".[2] NATO's ROE doctrine has defined ROEs as: "Directives to military forces that define the circumstances, conditions, degree, and manner in which force, or actions which might be construed as provocative, may be applied".[3]

Canadian ROE are orders issued by the military authority that define the circumstances, conditions, degree, manner, and limitations within which force, or actions which might be construed as provocative, may be applied to achieve military objectives under the national policy and the law.[4] According to British Defence Doctrine, ROE defines the constraints placed upon military activities, as well as the freedoms permitted, and

they reflect the operational context in which it is envisaged that force may be used.[5] The UN Handbook on Multidimensional Peacekeeping operations also similarly describes ROE: "The ROE for the peacekeeping operation will clarify the different levels of force that can be used in various circumstances, how each level of force should be used and any authorisations that may need to be obtained from commanders".[6] At the centre of all the definitions, there is an agreement that ROE are to be used by commanders to control the use of force by persons under their command.

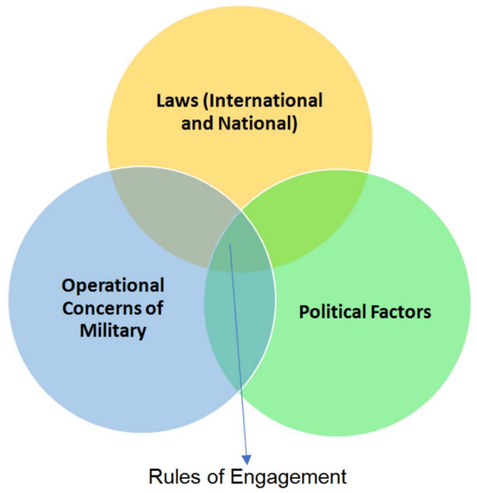
Components of ROE

The parts of ROE could be represented in a Venn diagram showing three circles, representing political factors, operational interests of the military, and relevant international and national laws, with ROE originating from the overlap in the middle of the three circles. Each of the constituent element influences the outcome of the ROE. The armed forces always serve a political goal and are deployed to attain political objectives. ROE are consequently approved by the political command authorities responsible for the operation in question. For instance, in the Falkland War, the geographical limitations on the area of operations of British forces around the Islands were imposed primarily for political reasons and not strictly required under the laws of naval warfare.[7]

Applicable Laws

The conduct of military operations is governed by international law, which includes the law of war or International Humanitarian Law (IHL), International Human Rights Law (IHRL), the UN Charter and national laws. The states and their forces are obliged to comply with international law that impacts military operations and need to train their forces accordingly. The core of the current IHL is formed by the four Geneva Conventions of 1949, the three Additional Protocols (AP) of 1977 and 2005, and a large number of weapon regulations / ban treaties. In addition to the treaties, IHL also consists of customary law. Regardless of the subject or object to which it is applied, IHL recognises and maintains a careful and delicate balance between military necessity, the reality of armed conflict and war, and humanitarian concerns.

Figure 1: Components of Rules of Engagement



The UN has been a pioneer in human rights protection since its establishment. There are certain rights included in constitutions as well as in international treaties which may not be derogated under any circumstances, including war or public emergency threatening the life of the nation. There are nine core IHRL treaties and the states ratifying a treaty undertakes the obligation to introduce it to its internal legal order and implement it in good faith, without the principle of reciprocity.[8] Certain human rights which are protected under all circumstances are – the right to life, the prohibition of torture, the prohibition of slavery, and the non-retroactivity of criminal offences. Only those IHL and IHRL treaties to which a state is a party should be considered while formulating ROE. The actual contents of the ROE are classified at the same level as the OP-ORDER and remain subject to official state secrets. Any divulgence of the details of the ROE could lead to mission failure and/or place the lives of military personnel in danger unnecessarily. ROE may authorise the initiative in the use of force and become applicable only after a political decision has been taken to deploy the armed forces. They do not regulate such political decisions themselves.

During the Vietnam War (Operation Rolling Thunder), the ROE issued by the US imposed serious restrictions on the operational effectiveness of the air force. Besides making flying less effective, the ROE gave the enemy many advantages. In ROE, the targets were assigned in a strict time frame. The targets could not be attacked outside that time frame even if weather conditions precluded attacks within the time allowed.

Operational Aspects

ROE must not be too restrictive. During the Vietnam War (Operation Rolling Thunder), the ROE issued by the US imposed serious restrictions on the operational effectiveness of the air force. Besides making flying less effective, the ROE gave the enemy many advantages. In ROE, the targets were assigned in a strict time frame. The targets could not be attacked outside that time frame even if weather conditions precluded attacks within the time allowed. Once attacked, targets could not be re-attacked without prior permission even if the initial attack had not been successful or if the target had been repaired or rebuilt. In addition, targets were assigned without taking into account connections between them, meaning that multiple targets belonging to the same target category, such as the enemy's power supply or logistic supply lines, were frequently assigned at different intervals, allowing the North Vietnamese to redistribute their use of such assets to the elements which had not been attacked. Also, some targets were assigned at regular intervals even though they had previously been destroyed. This allowed the North Vietnamese to increase air defence systems around such targets, thus, increasing the risk to the US air force.[9]

Closer home, ROE on the India-China border have been framed to avoid the use of firearms. While both sides have troops amassed on the respective sides of the Line of Actual Control (LAC) in the region for nearly three years, the situation remains tense but has not aggravated into a conflict.

Kinds of ROE

The ROE may be issued at different levels of hierarchy and may appear in a variety of forms in military manuals. There may be standing ROE and mission-specific ROE. They may be included in operational plans or orders. The US military forces operate under three types of ROE. First, the Standing Rules of Engagement (SROE) empower commanders at all levels to protect their forces from hostile acts and demonstrations of hostile intent. Unit commanders always retain the inherent right to exercise unit self-defence in response to a hostile act or demonstrated hostile intent, whether in peace or a state of armed conflict.[10] Second, the Supplemental

ROE (mission-specific ROE) are mission-specific and does not restrict the appropriate use of force in self-defence. Supplemental ROE may be used to elaborate on how the SROE should be interpreted in situations likely to occur during a specific mission. Supplemental ROE are an important focus of mission planning which defines specific objectives, establishes lists of targets to be attacked to achieve those objectives, and develops courses of action and options for attacking each target.[11] Finally, the Standing Rules for the Use of Force (SRUF), govern military actions inside the US.[12]

Self-Defence

A specific feature of ROE is that the right of self-defence may authorise actions not covered in ROE. The sovereign right to self-defence is a fundamental principle under international law.[13] An attack in self-defence must be necessary, proportional, and triggered by an imminent or ongoing attack. The right to individual self-defence is an element of customary international law recognised by treaty bodies, tribunals, and international organisations. Soldiers must also be authorised to fire on more ambiguous threats where they see an individual engaged in what is interpreted as a 'hostile act' (attack) or demonstrating 'hostile intent' (threat of imminent attack). Military higher authorities or the force commander must guide, as how to respond to harassment that falls short of an attack (a hostile act). Subject to any limitations promulgated in ROE, all necessary and proportional means and actions may be used in self-defence.

A specific feature of ROE is that the right of self-defence may authorise actions not covered in ROE. The sovereign right to self-defence is a fundamental principle under international law.

Planning Rules of Engagement

Ideally, an ROE Planning Cell is a necessity before any operation. This Cell should be led by operational staff and include legal advisers, policy advisers, and officers with specialist expertise in land, air, maritime, special operations, outer space, and cyberspace operations, as appropriate. ROE should be assessed continually by tactical, operational, and strategic level commanders to ensure that appropriate adjustments can be made as missions or phases of the operation develop. New measures should be implemented, as necessary, to ensure the ROE remain consistent with the mission, threat situation, and law.

The Role of Judge Advocate

The legal sources that provide the foundation for ROE are complex and include customary and treaty law principles from IHL and IHRL. As a result, Judge Advocates (JA) must participate significantly in the preparation, dissemination, and training of ROE. JA should play an important role in ensuring the troops (soldiers, staff, and unit leaders) understand the mission-specific ROE and can apply the rules reflected therein. Commanders and targeting personnel must seek advice from the JA for ROE restrictions (including collateral damage) before mission execution. JA should be trained, operationally oriented, and readily accessible to assist commanders/ planners/ operators on ROE or related issues. Despite the important role of the JA, commanders are ultimately responsible for the ROE.

Judge Advocates (JA) must participate significantly in the preparation, dissemination, and training of ROE. JA should play an important role in ensuring the troops (soldiers, staff, and unit leaders) understand the mission-specific ROE and can apply the rules reflected therein.

Effectiveness of ROE

ROE should be as direct as any other order issued by the commander. Drafter should use separate sentences or subparagraphs to assure clarity of expression. ROE cards must be issued to soldiers containing a summary or extract of mission-specific ROE. In case the ROE is changed during an operation, the colour of the new card must be changed and old cards collected and destroyed. Every ROE card must have an 'as of' date on it. This will ensure that the soldiers are operating with the current ROE. To be effective, ROE must have the following features:

- Expressed in plain language, clear, and lawful.
- Reflect operational reality.
- Not to be overly restrictive.
- Common understanding between the drafter and field commander.
- To be continuously reviewed.

One of the most effective ROE was in the 1999 Kargil conflict wherein the then Prime Minister of India, Shri Atal Bihari Vajpayee allowed use of air power in evicting Pakistani intruders from the Kargil sector but with a restriction that aircraft need to operate within the Indian air space only. On the strategic front, this restrictive ROE paved the way for a resounding victory.

To be effective, ROE must have the following features:

- **Expressed in plain language, clear, and lawful.**
- **Reflect operational reality.**
- **Not to be overly restrictive.**
- **Common understanding between the drafter and field commander.**
- **To be continuously reviewed.**

ROE in Changing Operational Scenario

Greater hybridisation of conflict, expansion of battlespace, compression of timeframe for acting/ reacting, and widespread availability of devastating kinetic and non-kinetic tools with states and non-state actors has transformed the threat matrix. In this changing operational scenario, drafting ROE becomes a key activity with certain inbuilt precautions. Cyber, special operations, space and urban warfare are critical constituents of modern-day war. ROE for these four cases are discussed in subsequent paragraphs.

Cyber Warfare

The cyber-attack in Estonia in 2007, which lasted for a week, did not cripple the country but the ease with which they were executed created fear in cyber-dependent countries. In 2010, Stuxnet, a malware designed to interfere with Siemens Industrial Control Systems, was discovered in Iran, Indonesia, and elsewhere, leading to speculation that it was a government cyber weapon aimed at the Iranian nuclear programme. These cyber-attacks forced the governments to acknowledge that the cyber threat was real and since then, there has been a spate of attacks on defence and other critical national infrastructures around the world. The militarisation of the internet, could evolve into a more dangerous situation bringing critical infrastructures (water, nuclear power stations etc) to a halt or rendering military command and control systems inoperable. The threat potential is even more sinister when one considers that, unlike nuclear weapons, cyber-attack may not cost more than a few thousand rupees. The existing treaties of the laws of war cannot be extended to the internet.

ROE for the cyber-space operation have received growing attention in the recent past and it is possible to achieve military objectives through cyber-operations. The formulation of ROE for cyber weapons, unlike kinetic weapons, would be a complicated and cyber-specific process. It would need the expertise of civilian experts in the field. To neutralise a cyber-attack, the states need to incorporate cyber weapons in their arsenal. As regards self-defence, a cyber operator would not face any personal threat to life similar to that of a soldier who is engaged in combat on a battlefield.

The *Tallinn Manual on the International Law Applicable to Cyber Warfare* provides certain guidelines in the formulation of ROE against cyber-attacks.[14] According to *Tallinn Manual,* a cyber operation, like any operation, resulting in damage, destruction, injury, or death is to be considered a use of force. A state injured by an internationally wrongful act may resort to proportionate countermeasures, including cyber countermeasures, against the responsible state. A state that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence.[15]

ROE for the cyber-space operation have received growing attention in the recent past and it is possible to achieve military objectives through cyber-operations. The formulation of ROE for cyber weapons, unlike kinetic weapons, would be a complicated and cyber-specific process.

In a first kinetic response to a cyber-attack, the Israeli Defence Forces (IDF) attacked in May 2019 by bombing a building believed to be the Hamas cyber unit's headquarters. Again, in May 2021, the IDF claimed that it bombed two objectives in the Gaza Strip that housed centres for Hamas cyber operations".[16] A cyber operation that constitutes a threat, or use, of force against the territorial integrity or political independence of any state, or that is in any other manner inconsistent with the purposes of the UN, is unlawful. In addition, medical and religious personnel, medical units, and medical transports must be respected and protected and, in particular, may not be made the object of cyber-attack. ROE drafters must consider the following important points while drafting ROE for Cyber Warfare:

- Waiting and merely enduring each cyber-attack could lead to a point where armed forces are no longer able to cope with the attacks and backup systems go beyond the point of restoration.
- ROE must preserve the right of combatants at the point of impact to defend either in retaliation to a cyber-attack or when an attack is imminent.
- The principles of 'distinction' and 'proportionality' applies to cyber-attacks.
- The following persons may be made the object of cyber-attacks: (i) members of the armed forces; (ii) members of organised armed groups; (iii) civilians taking direct part in hostilities; and (iv) in an international armed conflict, participants in a *levée en masse*.
- Once identified, a kinetic response to a cyber-attack could be authorised by the political authorities.

Special Force Operations

The political and military utility of special military operations has increased and today several states have their Special Forces (SFs) to execute difficult tasks in grey-zone conflicts. With an increased focus on the employment of SFs, the ROE governing special operations be drafted succinctly since the success or failure of these operations must contribute to the success or failure of national policy. Take the case of the US invasion of Panama in 1989. The US Navy SEAL raid on Paitilla airfield (Panama) in December 1989 during Operation Just Cause was a unilateral US action. To avoid domestic and international criticism, the planner desired minimum collateral damage.[17] It has been reported that in this operation, overly restrictive ROE reduced the tactical success of the operation and caused much higher casualties than expected. The higher-than-anticipated casualties sustained on this operation occurred not only because of the written ROE given to the SEALs but also because of the inferred and implicit ROE. Inferred ROE resulted from the interpretation and translation of the written ROE by the various levels of command and was influenced by the great concern at all levels for the minimisation of collateral damage.[18]

Special Forces, undertaking unexpected operations, provide the military planner flexibility and a measure of cost-effectiveness in many situations. As a force multiplier, they can have great effects against enemy forces and installations.

Special Forces, undertaking unexpected operations, provide the military planner flexibility and a measure of cost-effectiveness in many situations. As a force multiplier, they can have great effects against enemy forces and installations. At the tactical level, SFs conduct purely offensive operations using initiative, movement, and surprise attacks. In nearly all missions, special operations forces conduct offensive missions against defended positions with enemy troops in a defensive posture. To execute a successful special operation, SFs must follow six essential principles: simplicity, security, repetition, surprise, speed, and purpose. Each of these principles can be affected by the ROE that either political or military leaders impose on SFs, in the conduct of their missions. Because the ROE affect these fundamental principles of SFs, they in turn affect SFs ability to achieve a decisive advantage and to meet military and political objectives necessary for mission success. While drafting ROE for special operations, the following points must be kept in mind:

- The operational environment in which special operations are conducted is permeated by the fog of war.
- SFs members may have to take quick personal judgment assisted only by what their memory retains regarding the directed ROE for the mission.
- At the tactical level, SFs must have the flexibility to apply maximum force to succeed.
- SFs staff need to be associated in the process of translating broad political and strategic military objectives into appropriate tactical level ROE.

Any attempt to fine-tune a special operation, which by nature is a limited collateral damage option, can result in tactical failure or an increase in casualties. SFs personnel are mature, well-trained soldiers who possess exceptional judgment. In times of crisis, their training and judgment must be trusted to a greater extent than conventional forces.[19]

Space Warfare

Today, space is the ultimate military high ground, with particular importance to communications, intelligence, and missile-warning surveillance operations. Militaries around the world are preparing for future wars with assets located in space and developing counter-space technologies. After Persian Gulf War, the weaponisation of outer space is continuing rapidly. An increasing number of countries around the world are attempting exploration of space and its militarisation.[20] These countries are looking to use space to enhance their military capabilities and national security by developing a broad range of defensive and offensive dual-use technologies. In addition to

active investments in counter-space programmes by France, India, Iran, Japan, and North Korea, dominant players such as China, Russia, and the United States lead in the research, development, testing, and systems and weapons operationalisation domains, enhancing the risk of future conflicts in space. Space weapons[21] could be classified into six categories:

- Kinetic and non-kinetic Earth-to-space weapons like projectiles or jammers, dazzlers, and cyberattacks
- Kinetic and non-kinetic space-to-space weapons like on-orbit projectiles or microwaves
- Kinetic and non-kinetic space-to-Earth weapons like jammers, lasers, or projectiles down from orbit. [22]

In addition to active investments in counter-space programmes by France, India, Iran, Japan, and North Korea, dominant players such as China, Russia, and the United States lead in the research, development, testing, and systems and weapons operationalisation domains, enhancing the risk of future conflicts in space.

The existing international treaties governing outer space, which came into force in the 1960s and 70s, are vague on the prospects of military outer space activities and any armed confrontation in space.[23] Currently, no agreement or treaty bans placing conventional weapons into outer space but multilateral discussions regarding the peaceful uses of outer space are a recurring issue at the UN Conference on Disarmament in Geneva. The core laws of war principles of distinction between civilians and combatants or civilian objects and military objectives, proportionality, and necessity, constitute an established benchmark for assessing the legality of *jus in bello* conduct. IHL allows the states to resort to armed force only in cases of self-defence or aggression, requiring that parties to the conflict distinguish between civilian objects and military objectives and use proportional force. These principles impose the requisite limits on the use of force in traditional warfare but are inadequate for implementation in inter-state conflicts extending beyond the terrestrial realm.

International law permits states to resort to armed force in cases of self-defence. States intending to attack the satellite infrastructure of other states would need to balance the military advantages sought and the prospects of damage and civilian losses related to it. Legal controversy may arise when, it might become necessary to destroy a private civilian satellite system contracted by a state to achieve military objectives in an inter-state conflict. A civilian satellite system contracted to a military entity to advance its military objectives in an inter-state conflict ceases to be a civilian object and as such is no longer immune from an attack by adversarial armed forces. Threats to space assets, both direct and indirect, are increasing, making it increasingly necessary to deter potential adversaries. The armed forces of the states having stakes in space militarisation lack clear ROE for space warfare. The following issues are to be kept in mind while formulating ROE for Space Warfare:

- Should a non-state actor responsible for providing vital satellite infrastructure for both military and civilian use be regarded as an 'enemy' in space warfare?
- Should every enemy satellite infrastructure in space be regarded as a military objective?
- In case of an attack by a state actor on a non-state actor satellite infrastructure, what ought to constitute a proportional response?
- Will it be appropriate to extend IHL principles to conflicts in outer space?
- What are the international law limits on the means and methods used to wage war in space?

Urban Warfare

Most recent armed conflicts have occurred in cities, not in the field. The wars in Iraq, Syria, Libya, and Yemen have actually been mainly fought inside cities. The Russia-Ukraine conflict serves as another example of the urban nature of contemporary war. Urban warfare could be defined as military operations planned and conducted on, or against, objectives on a topographical complex and its adjacent natural terrain, where manmade construction or the density of population are the dominant features. The military operations in cities are now inevitable and operations in and around cities are one of the greatest challenges the forces face.[24] These operations are conducted amongst civilians and against various threats including hybrid threats, conventional or regular forces, irregular forces, terrorists, foreign fighters, and, criminal elements. Additionally, buildings can obscure the line of sight to adversaries and conceal their position. Hidden obstacles and tunnels are other threats as they can conceal the enemy. The British Army has developed some excellent tactical urban doctrine and training and has operated successfully in many urban environments across the globe.[25]

The urban war zone has always been challenging to military tactics, communications, and weaponry. It is associated with low performance and high - cost resulting in excessive collateral damage.

The urban war zone has always been challenging to military tactics, communications, and weaponry. It is associated with low performance and high - cost resulting in excessive collateral damage. Urban ROE, by their very nature, are normally constraints on military operations, but they may contain instructions to use force to defend or protect civilians, critical infrastructure or sites of historical/religious importance. While drafting ROE for urban warfare, the following should be kept in mind:

- The enemy may exploit politically sensitive places such as schools, religious places, government offices, and factory complexes.
- Restrictions on the use of explosive warheads in densely populated areas where there is a likely impact on essential services (electricity, gas, water, sewage, health etc.) on which the civilian population relies.
- Military objective to be achieved with minimum damage to civilian property.
- Guidance for non-lethal engagements in addition to those involving lethal force.
- Precautionary measures since the enemy may be tempted to employ prohibited chemical or biological weapons.
- Limited communications jamming so that humanitarian communications continue and regular pauses in military operations to allow humanitarian aid to reach impacted civilians; and creation of humanitarian corridors for evacuation of civilians from conflict areas.
- Humanitarian and relief agencies must be treated with respect and kept informed and cooperated with to avoid negative publicity.

Conclusion

Rules of engagement are based on the three pillars of national policy, the military's operational requirements, and law. These are guidance to unit commanders and individual soldiers in the form of a control mechanism to ensure that the use of military force complies with political and military aims. With the change in operational scenario,

development of modern technologies and grey-zone conflict, battlefields have become immensely complex demanding precise regulations. ROE are a major tool for ensuring that a commander's actions stay within the bounds of international law. The domestic laws of both the states, the one conducting operations and of the state in whose territory the operations are being conducted, may also impact ROE. These are to be drafted by experts in keeping with the demands of changing operational scenarios at each level: national self-defence, unit self-defence and individual self-defence. ROE must leave considerable room for personal judgment on the part of the military personnel to make a situation-specific evaluation of the necessity and proportionality to use force in any given situation.

End Notes

1 The states have used different words to describe how ROE are intended to be used, for instance, whether ROE define, authorise, delineate, regulate, specify or clarify circumstances for, help tailor or guide the use of force; all the definitions and descriptions indicate that ROE are to be used by commanders to somehow influence the use of force by persons under their command. Cooper, Camilla G., Rules of Engagement Demystified: A Study of the History, Development and Use of ROE, Military Law and the Law of War Review, Vol. 53/1 (2014): 53.

2 US Department of Defence Joint Publication 1-02, Dictionary of Military and Associated Terms.

3 NATO ROE, MC 362/1, 23 July 2003, definition as cited in NATO Legal Desk-book (2010): 254.

4 Canadian Forces Joint Publication CFJP-5.1, "Use of Force for CF Operations" (August 2008): 2-3.

5 UK Ministry of Defence, JDP 0-01: British Defence Doctrine (2011): 1-24.

6 UN Department of Peacekeeping Operations (DPKO), *Handbook on Multidimensional Peacekeeping Operations* (New York, United Nations, 2003), p. 57.

7 Hastings, M. and Jenkins, S., *The Battle for the Falklands* (London, Pan Books, 1997): 173-177.

8 (i) The International Convention on the Prevention and Punishment of the Crime of Genocide (1948); (ii) the International Convention on the Elimination of All forms of Racial Discrimination (1965); (iii) International Covenant on Civil and Political Rights (1966); (iv) International Covenant on Economic, Social and Cultural Rights (1966); (v) Convention on the Elimination of all forms of Discrimination Against Women (1979); (vi) Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (1984); (vii) UN Convention on the Rights of Child (1989); (viii) International Convention for the Protection of All Persons from Enforced Disappearance (2006), and (ix) Convention on the Rights of Persons with Disabilities (2006).

9 Drake Major Ricky J., *The Rules of Defeat: The Impact of Aerial Rules of Engagement on USAF Operations in North Vietnam, 1965 – 1968*, Thesis, the Air University, United States Air Force (Alabama, May 1992): 49.

10 The SROE allow a US commander to use all necessary means available and to take all appropriate actions in self-defence, provided these actions do not violate the laws of war or IHL requirements of necessity and proportionality. However, they allow only those immediate actions minimally required (concerning nature, duration, and scope of force) to end the immediate threat. Some weapons and tactics require specific approval from the President or Secretary of Defence before they can be used (for instance, only the President can authorize the use of nuclear weapons).

11 For example, a given mission might call for deployed forces to interact with civilians. If such interactions are unfriendly (for instance, an encounter with an unarmed mob), the risk of escalating a conflict may be high, and so a supplemental ROE might direct that the unit should withdraw or use smoke to camouflage itself, but should not use its weapons on the mob. Some supplemental ROE permit a specific tactic, weapon, or operation; whereas others clarify action allowed under the SROE.

12 Such actions may include aid to civil authorities, search & rescue operations, humanitarian aid delivery, and law enforcement/security measures at government installations. SRUF are inherently restrictive: unless specific weapons and tactics are explicitly approved, they cannot be used without the authorization of the Secretary of Defence. Kehler C. Robert, Herbert Lin and Michael Sulmeyer, Rules of engagement for cyberspace operations: a view from the USA, *Journal of Cybersecurity*, Vol. 3, No. 1 (2017): 69-80.

13 In ROE, self-defence is addressed at two levels, the unit level (or unit self-defence) and the national level (or national self-defence.). See: MN Schmitt, 'Responding to Transnational Terrorism under the Jus ad Bellum: A Normative Framework' in MN Schmitt and J Pejic (eds), *International Law and Armed Conflict: Exploring the Faultline—Essays in Honour of Yoram Dinstein* (Martinus Nijhoff, 2007), 157-169.

14 Schmitt Michael N. (Ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, UK: Cambridge University Press, 2013, pp. 282. Tallinn Manual 2.0 (2017) expands the first edition by extending its coverage of the international law governing cyber warfare to peacetime legal regimes. The Tallinn Manual projects reflect a minority opinion. Only NATO nations were involved in writing the Tallinn Manuals, and countries like China, Russia, Israel, Iran, and North Korea, which have significant cyber-war capabilities did not participate. The NATO countries may think that a particular interpretation of the Geneva Conventions is valid in cyberspace, but if their adversaries there do not see the same rules as applying, then it's not clear how useful the Tallinn Manuals are.

15 According to Article 51 of the United Nations Charter, 'nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations until the Security Council has taken the measures necessary to maintain international peace and security'. This Article recognizes and reflects the customary right of self-defence.

16 Available at: https://therecord.media/israel-bombed-two-hamas-cyber-targets.

17 According to the US Secretary of State Baker, Article 51 of the United Nations Charter and Article 21 of the Organization of American States Charter supported the US's decision to use appropriate measures in defence of US citizens and facilities.

18 Operational Order 1-90 (OPORD 1-90) was released by General Thurman on 30 October 1989. It contained a very specific ROE for the use of military force during the intervention. The OPORD ROE were divided into two sections. The first section included the usual generic ROE, such as the direction to conduct military operations in accordance with international law of armed conflict, the soldiers' inherent right to self-defence, and the treatment of prisoners. The second section contained specific ROE for the intervention. The decision to use Riot control agents (RCA) could not be made by commanders below the rank of Lieutenant Colonel or Commander. Further, commanders were to ensure that troops used the minimal force necessary to accomplish military objectives.

19 Reilly Michael S., Rules of Engagement in the Conduct of Special Operations, Thesis, Naval Postgraduate School (California, December 1996): 223.

20 Today there are two different processes taking place in space: The militarization of space refers to the use of space-based technology (communication, remote sensing and navigation) to support military operations, and the weaponization of space refers to the introduction of weapons into space, such as anti-satellite weapons, satellites capable of damaging other satellites, and weapons operating from space aimed at Earth. Shapira Zeev and Gil Baram, The Space Arms Race: Global Trends and State Interests, *Cyber, Intelligence, and Security*, Volume 3, No. 2 (October 2019), pp. 3-21.

21 According to US Congressional Research Service, China and Russia are pursuing non-destructive and destructive counter-space weapon capabilities, such as jammers, lasers, kinetic-kill or anti-satellite (ASAT) systems, and cyber-attack capabilities. Stephen M. McCall, Space as a Warfighting Domain: Issues for Congress, Congressional Research Service, August 10, 2021, pp. 2.

22 This classification has been suggested by Todd Harrison, director of CSIS's Aerospace Security Project. This does not include Counterspace weapons or weapons that are based on Earth and affect other systems on Earth as well as in orbit. For instance: weapons like cruise missiles or cyberattacks that hit satellite ground stations.

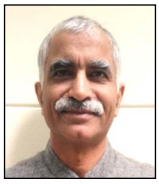
23 The United Nations General Assembly adopted the Outer Space Treaty, or the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, in October 1967. It was followed by the 1972 Liability Convention or the "Convention on International Liability for Damage Caused by Space Objects, and the 1979 Moon Agreement or the Agreement Governing the Activities of States on the Moon and Other Celestial Bodies.

24 Urban Warfare, Headquarters, Department of Army and United States Marine Corps, ATP 3-06, July 2022.

25 Sternberg Richard, Urban Operations, *British Army Review*, Special Report, Vol. 1 (Winter 2018): 4.

About the Authors

Wg Cdr UC Jha, a military veteran, did his PhD in Law and Governance from Jawaharlal Nehru University. His research focuses on the military legal system, international humanitarian law and human rights law and their impact on the functioning of the armed forces. His work comprises 30 books and over 150 articles published in various Journals and newspapers. His recent books include *Chinese Military Legal System;Biological Weapons: Coronavirus, Weapon of Mass Destruction? Human Rights in the Indian Armed Forces: An Analysis of Article 33; Modern Non-Lethal Weapons: Concepts, Application, Legal and Moral Perspective; and Nuclear Weapons: Untangling the Societal Enigma.*



Gp Capt Kishore Kumar Khera (Retd) is an independent analyst. He served as a fighter pilot in the Indian Air Force for 33 years. He was a pioneer member of Composite Battle Response and Analysis (COBRA) Group and headed the Operational Planning and Analysis Group at Air Headquarters. His recent books include *Chinese Military Legal System; Combat Aviation: Flight Path 1968-2018; Modern Non-Lethal Weapons: Concepts, Application, Legal and Moral Perspective; and Nuclear Weapons: Untangling the Societal Enigma.*

About the USI

The United Service Institution of India was founded in 1870 by a soldier scholar, Colonel (late Major General) Sir Charles MacGregor 'for the furtherance of interest and knowledge in the Art, Science and Literature of National Security in general and Defence Services, in particular'. It commenced publishing its Journal in 1871. USI also publishes reports of its research scholars as books/monographs and occasional papers (pertaining to security matters) by its members. The present Director General is Major General BK Sharma, AVSM, SM & Bar (Retd).

United Service Institution of India (USI)

Rao Tula Ram Marg, Opposite Signals Enclave, New Delhi-110057
Tele: 2086 2316/ Fax: 2086 2315, E-mail: dde@usiofindia.org

Price: ₹ 250.00