SILENT LEGES INTER ARMA CONFERENCE VI

Report of the 'Silent Leges Inter Arma?' Conference VI held in Bruges (Belgium) from 19 to 22 September 2023

***Rapporteurs**: Yoren Beyens, Rafael Boeynaems, Hanna Bourgeois, Jan De Gols, Mathieu Fontaine, Saskia Lemeire, Sarah Letellier, Édouard Malcourant, Camille Martens, Karel Peeters, Adrien Van Kan (Legal Advisors at the Ministry of Defence, Belgium)*

***Editor**: Hanna Bourgeois (Legal Advisor at the Ministry of Defence, Belgium)*

TABLE OF CONTENTS

1 INTRODUCTION

From 19 to 22 September 2023, the Belgian Group of the International Society for Military Law and the Law of War (ISMLLW) held the sixth edition of the 'Silent Leges Inter Arma?' Conference. In line with the previous editions, this conference was hosted at the Grand Hotel Casselbergh in the historic centre of Bruges (Belgium). This conference was supported by the Baltic Defence College, the Italian Navy, the Kalshoven-Gieskes Forum on International Humanitarian Law at Leiden University, and the Lieber Institute for Law and Warfare at West Point. The conference aimed to bring together legal practitioners and academics from various countries who are active in the field of security and defence. Over 110 delegates attended the conference, which provided a platform to exchange ideas and discuss current legal developments and challenges within the domain of security and defence. This report summarises the main discussions held during six sessions.

2 CONFERENCE OVERVIEW

2.1 Tuesday 19 September 2023

On the evening of 19 September 2023, the delegates were officially welcomed by the **Mayor of Bruges, Mr. Dirk De fauw** in the magnificent gothic room of the City Hall of Bruges. Following this, the city of Bruges hosted a reception in the parlours of the City Hall, where guests were treated to local beers.

2.2 Wednesday 20 September 2023

2.2.1 Opening of the Conference

On 20 September 2023, **Mr. Ludwig Van Der Veken, President of the Belgian Group and Secretary-General of the ISMLLW**, kindly welcomed the participants of the 'Silent Leges Inter Arma?' Conference VI to Bruges. He then introduced Ambassador H.E. Ms. Ariadne Petridis, Head of the Permanent Representation of the Kingdom of Belgium to the North Atlantic Treaty Organization (NATO), as the keynote speaker.

2.2.2 Keynote Speech – NATO's Challenges after the Vilnius Summit

H.E. Ms. Ariadne Petridis, Ambassador and Head of the Permanent Representation of the Kingdom of Belgium to NATO, opened the conference with a keynote speech on the challenges NATO faced after the Vilnius Summit. Ms. Petridis reminded the audience of the significant decisions made at this Summit to adapt the alliance for the future.

The first major decision concerned Ukraine. Ms. Petridis stated that NATO's leaders aimed to convey a powerful message about the Alliance's unity and commitment to stand with Ukraine. She noted that Ukraine is now stronger and closer to NATO than ever been before. The Allies agreed on a package consisting of three components. The first element is a new and robust multi-year package of practical assistance, far beyond anything NATO has ever done before. With this first component, NATO intends to support the modernisation of Ukraine's security and defence sector and make Ukraine's armed forces fully interoperable with NATO. The second component involves strengthening political ties with Ukraine through the establishment of a new NATO-Ukraine Council. This Council will be a platform for consultations on security issues, including meetings at ministerial, ambassadorial, and technical levels. The third component pertains Ukraine's membership aspirations. The Allies agreed to remove the requirement for a 'Membership Action Plan' for Ukraine's membership of NATO, making the two-

step process a one-step process. In addition to NATO's package for Ukraine, the G7 issued a declaration creating an umbrella under which States can launch negotiations for bilateral arrangements for Ukraine's long-term security. Belgium has adhered to this declaration.

Moving on to the second major decision taken during the Vilnius Summit, Ms. Petridis explained that leaders agreed on the final building blocks of NATO's military adaptation trajectory for deterrence and defence against the two main threats to the Alliance: Russia and terrorism. Allied Heads of State and Government also endorsed a Defence Production Action Plan with a view to boosting defence industrial production and increasing interoperability and interchangeability.

Ms. Petridis also highlighted a number of other decisions taken at the Vilnius Summit. First of all, Allies pledged to invest a minimum of 2 percent of GDP annually on defence; they also committed to invest 20 percent of their defence budget in equipment and R&D; and they stressed the importance for NATO of maintaining its technological edge. Significant discussions were held with the European Union (EU) and Indo-pacific partners on cyber security, maritime security, and new technologies. Moreover, the Allies committed to strengthening the existing NATO framework in the field of resilience against hybrid threats and the protection of critical infrastructure.

After discussing the decisions taken at the Vilnius Summit, Ms. Petridis highlighted that the Western Balkans are high on NATO's agenda, prompting extensive cooperation between NATO and the EU regarding this region. Secondly, she mentioned NATO's work on China. China is not considered a threat to the Euro-Atlantic area, nor does NATO have plans to invite Asian countries to join the Alliance or the intention to be militarily present in the Indo-Pacific. However, Allies feel that China poses systemic challenges to Euro-Atlantic interests, values, and security. NATO also closely monitors the strategic partnership between China and Russia. At the same time, NATO remains in favor of constructive engagement with China, to build reciprocal transparency and trust.

Ms. Petridis concluded by stressing that NATO is an alliance that can adapt to new security challenges and will stand up for a free and sovereign Ukraine, as well as for an open world of rules and rights.

2.2.3 Session 1 – Post-conflict Accountability for Violations of International Humanitarian Law, in Historical and Contemporary Contexts

Chair: Prof. Dr. Steven Dewulf, Chair of Law, Royal Military Academy, Belgium

Speakers:

- Colonel Charles Barnett, Army Legal Services, British Army
  The Leipzig war crimes trials

- Sabrina Rewald, Research and Teaching Associate, International Humanitarian Law Clinic, Kalshoven-Gieskes Forum, University of Leiden
  Digitally derived evidence to prosecute perpetrators of international crimes

The first session of the 'Silent Leges Inter Arma' Conference VI delved into the critical matter of accountability for violations of international humanitarian law (IHL) in the aftermath of conflicts. The discussions spanned both historical and modern-day situations. The session was **chaired by Prof. Dr. Steven Dewulf, Chair of Law at the Belgian Royal Military Academy**. The Chairman initiated the discourse by elucidating that such violations could lead to accountability at two levels–State and individual. The concept of individual criminal responsibility has gained significant traction over recent

years, yet numerous facets remain unresolved. Some of these unresolved elements formed the crux of the ensuing presentations.

The **first speaker, Colonel Charles Barnett,** who serves as a **Legal Adviser of the United Kingdom's (UK) Army Legal Service**, shed light on the Leipzig war crime trials. Colonel Barnett initiated his discourse by highlighting the escalating discussions around military liability for specific actions committed within an operational context. The acceptance of extraterritorial application of human rights has significantly contributed to this development. However, the operational context often impedes the establishment of military liability due to violations of IHL and/or human rights law (HRL). For instance, during British operations in Iraq, the transition from the legal framework governing major combat to the one applicable during stability operations was complicated by factors such as terrorism, organised crime, lack of rule of law, extreme temperatures, long working days, and an ambiguous legal framework. This complexity understandably led to difficulties during investigations into the individual liability of British servicemen, underscoring the paramount importance of a clear legal framework during operations.

Colonel Barnett asserted that the Leipzig trials were a landmark event in the history of International Criminal Law (ICL). These trials, for the first time, established the cumulative liability of a commander and their subordinates for grave IHL violations. A total of 17 German servicemen were prosecuted for committing war crimes during World War I in these trials, which spanned from January 1921 to July 1922. Articles 227 to 230 of the Treaty of Versailles of 1919 intended for these cases to be heard by a specially constituted court. However, Germany proposed conducting the proceedings before the *Reichsgericht* in Leipzig. Germany was tasked with the conduct of the proceedings, while the Allies were responsible for providing the evidence. The *Reichsgericht*'s rulings in these cases were based on German criminal law and military criminal law, which posed challenges due to the scarcity of provisions related to serious IHL violations in German law. The few criminal provisions that did exist related to mistreatment of prisoners of war, destruction and looting of houses, and sinking of hospital ships, among others.

Colonel Barnett further explained that Belgium, France, and the UK brought the 12 cases before the *Reichsgericht*. Representatives from these three countries were sent to Leipzig to oversee the cases and report back to their respective governments. The first case, a Belgian one, resulted in the conviction of three German soldiers for looting in Belgium. The German legislation that criminalised these acts was a translation into national law of the provisions of Articles 28 and 47 of the Fourth Hague Convention of 1907, leading to prison sentences of 5, 4, and 2 years respectively. The subsequent three cases were British and involved aggravated assault and murder of prisoners of war, with the perpetrators receiving prison terms of 6 to 10 months. The fifth case, also British, was the most significant and involved the sinking of the HMHS Dover Castle. The German submarine's commander was acquitted due to the circumstances, as German intelligence indicated that British hospital ships were being used for illegal transportation of troops and ammunition. The commander had merely followed orders and allowed an hour and a half between the firing of two torpedoes for ship personnel to evacuate. Another Belgian case involved a member of the German secret police accused of torturing Belgian children for their potential involvement in sabotaging a German railroad.

The Allies were outraged by the light sentences and acquittals. In response, Belgium and France recalled their representatives. It was clear that a strong message needed to be sent. The case of the HMHS Llandovery Castle was selected to deliver this message. This hospital ship was also sunk by a submarine, and instead of being rescued, the drowning crew was fired upon by the submarine's crew. As the commander was in Gdansk (Poland), he was outside the jurisdiction of the *Reichsgericht*, leading

to a trial against his two highest-ranking subordinates. They were sentenced to four years in prison under Article 23(c) of the Hague Regulations on the Laws and Customs of War on Land, an Annex to the Fourth Hague Convention of 1907.

In conclusion, Colonel Barnett highlighted that despite the vast scale of World War I, the number of effective trials resulting in convictions for some of the atrocities was relatively small. However, these trials marked a significant advancement in ICL. Specifically, the case against the HMHS Llandovery Castle demonstrated for the first time that obedience to an order does not automatically absolve one of liability for certain actions. Furthermore, the Leipzig trials played a crucial role in the establishment of subsequent ad hoc tribunals, such as the Nuremberg Tribunal and the Tokyo Tribunal. Yet, even today, States remain reluctant towards the International Criminal Court (ICC), preferring to prosecute their nationals themselves.

Hereafter, the **second speaker, Sabrina Rewald, Research and Teaching Associate at the Kalshoven-Gieskes Forum's International Humanitarian Law Clinic of the University of Leiden**, gave a presentation on digitally derived evidence (DDE) to prosecute perpetrators of international crimes. In particular, she explained how new technology can help prosecutors to build their case.

In 2019, Dr. Emma Irving and Dr. Robert Heinsch, the Director of the Kalkhoven-Gieskes Forum on International Humanitarian Law, embarked on a research project on 'Digitally Derived Evidence'. The project aimed to scrutinise the different legal standards of evidence employed across various national and international accountability fora to prosecute international crimes. The researchers had observed that courts demonstrated inconsistent approaches towards DDE and that there was a lack of common international rules for DDE's collection, preservation, sharing, and treatment before accountability bodies. The aim of the project was to outline the ICL framework and derive standards applicable to DDE in domestic courts, fact-finding missions, and international courts and tribunals. The project culminated in the creation of a DDE Database (i.e., an online repository) and the Leiden Guidelines on the Use of DDE in International Criminal Courts and Tribunals.

Ms. Rewald further explained that DDE can be categorised into digital evidence or digitised evidence. Digital evidence refers to evidence that originates digitally, such as photos and videos, areal imaginary, satellite imaginary, or digital reconstruction technology. An example of this is Amnesty International's reconstruction of the Syrian Saydnaya military prison based on testimonies, among other things. Digitised evidence pertains to analogue material that is converted into a digital format. It concerns data that has been manipulated, stored, or communicated by or over a computer system. Examples of such evidence include radio broadcasts or intercepts transferred from cassette to digital audio file.

Ms. Rewald proceeded to discuss the key evidentiary advantages of DDE. These include: (i) the enhancement of unreliable witness statements through the use of DDE; (ii) the accessibility of DDE without the need to enter insecure or inaccessible areas or State territories; and (iii) the wealth of information and perspective provided by DDE, such as the ability to heat track a conflict via NASA Fire Data. However, DDE also presents several evidentiary challenges: (i) we are living in an era dominated by smartphones, the internet, and social media platforms like TikTok, as well as the emergence of deepfakes; (ii) the algorithms of online content companies often result in the removal of DDE material, as evidenced by the removal of footage from Syria on various online platforms; (iii) there is a reliance on private companies and the cooperation of governments; (iv) the sheer volume of potential evidence to sift through necessitates manual oversight, as demonstrated by the more than 400 million videos taken during the conflict in Syria; (v) there is a significant need for technical experts and literacy to scrutinise DDE; (vi) DDE can have a profound impact on fair trial rights; (vii) future

technologies will inevitably pose new challenges; and (viii) there is a lack of uniformity across and within accountability fora.

Ms. Rewald then discussed the potential application of the Leiden Guidelines. These Guidelines aim to provide a comprehensive outline of the key elements that legal practitioners should consider before submitting DDE to an international criminal court or tribunal. The Leiden Guidelines can be considered to support the sources of ICL and can serve to inform courts and tribunals accordingly (see, for example, Article 21 of the ICC Statute of 1998). According to the ICC, "*for an item to be admitted into evidence it must satisfy the three-part test under which it must (i) be relevant to the case; (ii) have probative value; and (iii) be sufficiently relevant and probative as to outweigh any prejudicial effect its admission may cause. Further, [the] determination on the admissibility into evidence of an item has no bearing on the final weight to be afforded to it, which will only be determined by the Chamber at the end of the case when assessing the evidence as a whole*".[1] In this regard, the Leiden Guidelines offer recommendations on how best to submit evidence (e.g., submit videos in their entirety instead of only excerpts), how to increase the probative value of evidence (i.e., the higher the probative value of evidence, the more it tends to prove an asserted fact), and what actions to take in the absence of corroborating evidence.

Ms. Rewald concluded her presentation by noting that the Leiden Guidelines are conservative in nature, as they are based on case law from a time when technology was not as advanced as it is today. However, they can prove to be an exceptionally useful tool for practice.

2.3 Thursday 21 September 2023

2.3.1 Session 2 – Evolutions in the Cyber Domain

Chair: Major-General Michel Van Strythem, Commander, Belgian Cyber Command

Speakers:

- Geert Baudewijns, General Director, Secutec
  Current trends

- Sarah Wiedemar, Researcher, Cyber Defence Project, Risk and Resilience Team, Center for Security Studies, ETH Zurich
  Cyber Defence and Article 5 of the North Atlantic Treaty

- Prof. Dr. Terry Gill, Emeritus Professor of Military Law, University of Amsterdam
  Cyber operations and the war in Ukraine

The second session of the conference delved into the developments in the cyber domain. This session was **chaired by Major-General Michel Van Strythem, Commander of the Belgian Cyber Command**. In his introductory remarks, Major-General Van Strythem provided some insights into the characteristics and evolution of threats in cyberspace.

[1] *Prosecutor v Bemba* (Decision on the admission into evidence of items deferred in the Chamber's "Decision on the Prosecution's Application for Admission of Materials into Evidence Pursuant to Article 64(9) of the Rome Statute" (ICC-01/05-01/08-2299)) ICC-01/05-01/08 (27 June 2013) TC [9].

The **first speaker, Sarah Wiedemar, Researcher at the Cyber Defence Project of the Center for Security Studies of the Swiss Federal Institute of Technology in Zurich (ETH Zurich)**, discussed the relation between cyber defence and Article 5 of the North Atlantic Treaty.

Ms. Wiedemar introduced the topic by citing the 2022 cyberattack against Albania as an example. This attack, attributed to Iran, prompted Albanian Prime Minister Rama to publicly contemplate invoking Article 5 of the North Atlantic Treaty of 1949 in response. Although no formal request was made within NATO, this marked the first public discussion about the possibility of invoking Article 5 in response to a cyberattack. This raises the question of how to apply the North Atlantic Treaty to today's cyberspace.

Cyber defence first appeared on NATO's agenda in 2002, but it wasn't until a series of cyberattacks against Estonia in 2007 that NATO adopted its first policy on the subject. The 2008 war between Russia and Georgia underscored the significant role cyber warfare can play in conventional warfare. The 2014 NATO Wales Summit Declaration acknowledged that a cyberattack could trigger Article 5 action. Notably, the Declaration did not specify a threshold and referred to a cyberattack in the singular form. This stance evolved in the 2021 NATO Brussels Summit Declaration, which shifted NATO's focus to 'cumulative cyber activities', reflecting NATO's growing understanding of the risk of cumulative effects in cyberspace.

Ms. Wiedemar delved into two recent instances of cyberattacks. In 2021, a Russian group launched a ransomware attack on the IT system of the Colonial Pipeline in the United States (US), leading to a significant shutdown that impacted critical infrastructure. This incident had diplomatic repercussions: a month after the attack, during a meeting, President Biden presented President Putin with a list of critical infrastructure in the US that should be off-limits to cyberattacks. Another example discussed was the Viasat Hack, executed just hours before Russia's invasion of Ukraine in February 2022. It is believed that Russia targeted the global satellite company Viasat, disabling thousands of modems relied upon by the Ukrainian State and military. The attack also had collateral effects on other countries (NATO members), causing extensive damage beyond Ukraine.

Cyberattacks present several challenges to Article 5. Firstly, what is the threshold that a cyberattack must meet to qualify as an armed attack and trigger Article 5? It was long believed that a cyberattack should be equivalent to a conventional attack to meet the required threshold, but the effects of a cyberattack are more intricate than those of a conventional attack. Secondly, attribution is a challenge. It is difficult to attribute a cyberattack, and it may not be possible to do so with sufficient certainty. Lastly, how should one appropriately retaliate against a cyberattack? This question is much harder to answer than retaliation for a conventional attack.

During a press conference on 25 February 2022, NATO Secretary General Jens Stoltenberg stated: "*On cyber, well we have stated that cyberattacks can trigger Article 5. But we have never gone into the position where we give a potential adversary the privilege of defining exactly when we trigger Article 5*". This statement reflects NATO's current approach to cyberattacks, which is one of strategic ambiguity. The exact circumstances under which a cyberattack can trigger Article 5 remain unclear, both for adversaries and for NATO members.

The **second speaker, Prof. Dr. Terry Gill, Emeritus Professor of Military Law at the University of Amsterdam**, addressed the application of international law in cyberspace and cyberwarfare. Prof. Gill began his presentation by explaining why international law is applicable in cyberspace. While this is now largely accepted, as evidenced by resolutions of the United Nations (UN), it was not a given during the early stages of cyber activities. Initially, the question of whether or not international law applies to the cyber domain was an undecided issue and it was clear that international law needed to be

adapted to cyberspace. The initial discussions centred around the threshold for a cyberattack to constitute a use of force under Article 2(4) of the UN Charter of 1945 and when a cyberattack would constitute an armed attack so that Article 51 UN Charter could be invoked, in other words, when a cyberattack crosses the threshold of the 'threat or use of force'. The vast majority of the first version of the Tallinn Manual focused on how the rules of the *jus ad bellum* (threshold for a use of force and the right to self-defence) and rules of IHL would apply to cyber acts. This Manual allowed for the application of a treaty in a domain for which it was not originally developed. However, cyber interferences and cyber sabotages often fall below the threshold of an armed attack or the use of force.

The Tallinn Manual 2.0 aimed to expand its scope by incorporating rules for peacetime cyber activities that fall short of an armed attack. This included rules on non-intervention, sovereignty, and to some degree, human rights (e.g., privacy). A significant development was the initiation of the Hague Process by the Netherlands, which followed the Tallinn Manual 2.0. This process offered a platform for States to express their own questions and concerns about cyber activities, with over 50 States taking part. Although these discussions were confidential, they provided a crucial platform for States to voice their perspectives on cyber issues.

The UN Charter's rules and principles were declared to be applicable to cyber activities. As a natural outcome of this declaration, IHL is also considered applicable to cyberattacks. Presently, discussions are underway about the Tallinn Manual 3.0, which is focused on how States have adopted rules and policies in relation to harmful or intrusive cyber activity. There seems to be a general agreement that a cyberattack resulting in death, destruction, or significant other physical harm, could activate Articles 2(4) and 51 of the UN Charter. However, the debate about the threshold continues, despite some resolutions of the UN and State practice. Several States have a policy stance on where the threshold should be, but these are not always disclosed, as States do not want to give adversaries the opportunity to launch cyberattacks that would just fall below the threshold. Conversely, it is crucial to ensure that there is no excessive ambiguity.

The speaker concluded that, apart from events occurring in an ongoing armed conflict involving kinetic actions, there have been very few incidents that have resulted in material incidents of death. Economic losses and/or intellectual property losses amounting to millions of dollars are indeed common, but not death, injury, or significant material damage. This does not mean it is impossible, but it has seemingly not happened yet. However, we live in an era where sabotage, espionage, and interference occur daily. While international legal scholars initially thought the focus would be on the application of *jus in bello* to cyberattacks, current practice suggests that most cyber activities occur below the threshold of an armed attack and largely outside the context of armed conflict. Future research should focus on cyber acts below the threshold of an armed attack that qualify as 'unfriendly acts'. This is where the significant action is currently.

The **third speaker, Geert Baudewijns, General Director at Secutec**, focused on the current trends in the cyber domain. Mr. Baudewijns first clarified that there is a distinction between the 'clear web', which accounts for about 4% of the internet, and the 'deep web', which accounts for 96% of the internet. For ordinary internet users, the 'deep web', and even more so the 'dark web', is untraceable. Mr. Baudewijns demonstrated live on-screen how hackers operate and how to screen for hacker attacks. He displayed several websites used by hackers that reveal the vulnerabilities of companies. For any organisation, it is important to monitor its 'attack factor' (vulnerabilities), as well as the 'attack factor' of companies that work for it and could expose the organisation. To ensure one's security, it is important to be aware of the vulnerabilities and suppliers will at some point create vulnerabilities by not being up-to-date. Mr. Baudewijns' company registers about 97% commercial hackers and 3% State hackers.

Hackers can usually be identified by the mistakes they make. In the cybersecurity sector, it is important to have the right tools (everyone uses the same tools) and to combine them. Artificial intelligence is expected to play a significant role in this.

2.3.2 Session 3 – Military Activities and Presence in Outer Space

Chair: Prof. Dr. Valeria Eboli, Italian Naval Academy

Speakers:

- Jean-François Mayence, LLM, Legal Unit 'International Relations', Federal Science Policy, Belgium
  The space law framework and current concerns

- Major General (Air Force) Hongbo Xing, Academy of Military Sciences, PLA, China
  A Chinese perspective: Strengthening global governance on outer space jointly to ensure space security

- Pauline Warnotte, Senior Legal Advisor, ICRC delegation to the EU, NATO and the Kingdom of Belgium; Lecturer, Faculty of Law, University of Namur
  The ICRC's perspective

The third session of the conference addressed the topic of military activities and presence in outer space. This session was **chaired by Prof. Dr. Valeria Eboli** from **the Italian Naval Academy**. Prof. Eboli opened the session with a few words about the rapid development of new technology and its escalating utilisation in outer space. Consequently, we are facing new challenges, particularly regarding the military use of outer space. To our knowledge, no weapons are yet deployed in outer space, but some States aspire to do so. Therefore, persistent efforts are required to improve the legal framework for the military use of outer space.

As regards the most recent novelties in the field, Prof. Eboli mentioned the McGill Manual on International Law Applicable to Military Uses of Outer Space (MILAMOS), which clarifies the existing rules applicable to military uses of outer space by both States and non-State actors in peacetime, while underlining the limitations international law places on the threat or use of force in outer space. MILAMOS could become an important term of reference for operators and policymakers in this field.

The **first speaker, Mr. Jean-François Mayence**, who works at **the Legal Unit 'International Relations' of the Federal Science Policy in Belgium**, presented an overview of the space law framework and current concerns related to military activities in outer space. He began by outlining the existing regulations for the use of outer space, which are incorporated in the five UN Outer Space Treaties. These include the Outer Space Treaty of 1967 and the Moon Agreement of 1979, the Partial Nuclear Test Ban Treaty (PTBT) of 1963, and the Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques (ENMOD) of 1977. While the Outer Space Treaty and the Moon Agreement provide general principles for State activities in the exploration and use of outer space, including the moon and other celestial bodies, the PTBT and ENMOD treaties specifically prohibit any nuclear weapon test explosion in outer space and any military or other hostile use of environmental modification techniques that could have long-lasting or severe environmental effects.

Mr. Mayence delved deeper into the specifics of what is explicitly or implicitly prohibited in outer space and what actions are not prohibited (though not necessarily authorised) under the outer space treaties. For instance, the placement or testing of a weapon of mass destruction is explicitly prohibited, while the placement and use of conventional weapons in a non-aggressive manner is not. Furthermore, a military manoeuvre or the placing of military infrastructure on celestial bodies is explicitly prohibited by the UN Outer Space Treaties, as well as the destruction or capture of a foreign-registered space object which is implicitly prohibited by the Outer Space Treaty of 1967. However, research and development for military purposes and applications are not prohibited. Mr. Mayence emphasised that his discussion was limited to the outer space treaties and that other regulations might still impose restrictions. Nonetheless, based on the principle of freedom of outer space, every State has the right to explore and use outer space.

Mr. Mayence concluded his presentation by discussing some trends and issues. He spoke about the growing tension between States and the shift towards a national response (rather than a purely international one) due to emerging national legislation and policies that promote the development of national surveillance capacities. He also described the 'arsenalisation' of orbital space, highlighting the trend to expand military space capabilities and the race for lunar resources as crucial for establishing long-term infrastructure on the moon. He also addressed the issue of private actors being directly and (pro)actively involved in international conflicts. The implications of applying treaties aimed at States and not private entities remain unclear. The integration of space and defence is an ongoing and accelerating process that poses challenges to international cooperation, national and regional policies and regulations, and existing international space law. Therefore, Mr. Mayence stressed, we must rephrase the same basic principles with different words and maintain peace through new means.

The **second speaker, Major General (Air Force) Hongbo Xing** who is affiliated with the **Chinese Academy of Military Sciences**, discussed China's stance on military activities and presence in outer space. He highlighted China's active participation, mentioning that China has entered into over 130 space cooperation agreements and Memorandum of Understandings (MOUs).

In April 2023, the European Space Agency (ESA) launched the JUICE mission towards Jupiter and its moons, and in August 2023, India launched the Chandrayaan-3 past the moon's south pole. While current technology provides unprecedented opportunities for peaceful exploration and use of space, it also poses challenges due to the ongoing arms race in space. For this reason, Major General Xing emphasised the need for all States to collaborate to ensure peace and security in space, advocating for the use of space for economic, scientific, technological, and cultural development for the benefit of all.

In May 2023, the UN released a report titled "*For all Humanity - The Future of Outer Space Governance*", underscoring the need for a new framework for international cooperation in space. Major General Xing argued against extending growing ideological and military divisions into space, advocating instead for international cooperation. He stressed that space should be peaceful, inclusive, and governed by all.

Major General Xing outlined several key points necessary for this vision to succeed. Firstly, a 'global governance' system for space must be established, ensuring equal rights for all countries in the peaceful use of space. Special consideration should be given to developing countries and those undertaking space missions for the first time, with technological support from other nations to ensure space accessibility for all. Secondly, space security must be maintained through proper coordination, considering the risks posed by the arms race in space and potential collisions between the large volume of objects in space. Good communication and coordination can mitigate these risks. Thirdly, an arms race in space should be avoided at all costs. As a relatively new domain with significant military value, the world's

superpowers are vying for military superiority in space, potentially compromising stability and security. Major General Xing argued that States should learn from history and understand that there are no winners in an international arms race. He emphasised that cooperation for the benefit of future generations should be the primary concern in space.

Key UN forums, such as the General Assembly First Committee and the Conference on Disarmament, serve as crucial venues for dialogue and coordination in the pursuit of global security. It is essential for States to actively back these platforms. Moreover, States should adhere to and implement the principles outlined in the UN Charter and other international law sources. When it comes to the peaceful utilisation of space, the principles of peaceful dispute resolution and the prohibition of force or threats between nations are of particular importance. States must also strictly comply with various space-related treaties, including the Outer Space Treaty of 1967, the Rescue Agreement of 1968, the Space Liability Convention of 1972, the Convention on Registration of Objects Launched into Outer Space of 1974, and the Moon Agreement of 1979. In Major General Xing's view, there is also a pressing need for a new treaty to prevent an arms race in space. In this regard, China and other States have proposed the 'Draft Treaty on the Prevention of the Placement of Weapons in Outer Space, the Threat or Use of Force against Outer Space Objects'. Currently, this is the sole proposed treaty addressing the issue of space arms race.

Lastly, Major General Xing emphasised the need to establish a global community focused on space, where the future of all humanity is the primary concern. In this endeavour, all States should have equal access to space. States with prior experience in space exploration and usage bear the responsibility to assist others. Space is a shared objective of humanity. In this context, we either all succeed or all fail. Therefore, States must consider the interests of future generations, not just immediate gains.

The **third speaker, Pauline Warnotte, Senior Legal Advisor at the International Committee of the Red Cross (ICRC) delegation to the EU, NATO, and the Kingdom of Belgium and Lecturer at the Faculty of Law of the University of Namur**, wrapped up the third session with a presentation on space law from a humanitarian perspective. Space and the technology it enables have become indispensable in civilian life, affecting many aspects such as weather forecasting, communication systems, navigation, and earth observation. Also the ICRC uses space technology on a daily basis: not only are satellites used to count buildings, to monitor cattle vaccination programs, to assess damage in crisis situations, but also satellite communication is of great importance.

However, the use of space systems in warfare has also increased. The ICRC is concerned about the potential human cost to civilians on earth from the use of weapons and other military operations in outer space during armed conflict. Military activities in or related to outer space are not legally unregulated and are indeed constrained. Existing restrictions can be found in pre-existing international law, such as the UN Charter, the Outer Space Treaty of 1967, IHL, and the law of neutrality. International law restricts the choice of weapons and means or methods of warfare. Moreover, Article 36 of the First Additional Protocol of 1977 to the Geneva Conventions of 1949 states that States are required to conduct a legal review of new weapons, means, or methods of warfare (including in space). IHL provides specific protection for certain objects and persons in armed conflicts, such as space systems necessary for the safety and functioning of objects indispensable to the survival of the civilian population, like medical units, vehicles, and other transport, or installations containing dangerous forces. IHL also obligates States to take all feasible precautions to protect civilians and civilian objects, supported by the ever-applicable principles.

Given the unique characteristics of space, the ICRC encourages States to work towards a shared understanding of the application of IHL in outer space. This is with the aim of protecting civilians and

civilian objects from the effects of military space operations. The concept of an 'attack' under IHL and military operations against space systems should consider all foreseeable direct and indirect actions. However, a universally accepted definition does not exist for the term 'space debris', which could have a significant impact on life on Earth. Another area where interpretation varies greatly is the dual use of space objects, where the military use of a space object affects its civilian character. These differences in interpretation pose challenges for the application of IHL.

In January 2023, the ICRC presented a working paper to the UN General Assembly's Open-Ended Working Group on "*Reducing space threats through norms, rules, and principles of responsible behaviours*". The paper included five preliminary recommendations focusing on norms to minimise the risk of harm to civilians. Firstly, States are urged not to conduct or support any military operation or other activity designed or expected to disrupt, damage, destroy, or disable space systems necessary for the provision of essential civilian services and for the protection and functioning of persons and objects specifically protected under international law. Secondly, States are encouraged to separate the military use of space systems from their civilian use, whenever feasible, particularly with regard to systems necessary for the provision of essential civilian services and for the protection and functioning of persons and objects specifically protected under international law. Thirdly, States should identify, register, mark, announce, and/or otherwise indicate those space systems within their jurisdiction or control that are to be spared from the effects of military space operations. Fourthly, States are urged not to develop, test, or use kinetic counter-space capabilities or conduct other harmful operations against space systems that are designed or expected to create space debris. Fifthly, States are urged to cooperate to increase the resilience of satellite services for humanitarian relief and emergency response in times of armed conflict and other emergencies. With these recommendations, which are necessary to minimise the risk of harm to civilians, Ms. Warnotte concluded her presentation, thereby ending the third session.

2.3.3 Session 4 – International Humanitarian Law vs. Counter-terrorism Legislation

Chair: Gert-Jan van Hegelsom, Former Head of the Legal Service of the European External Action Service

Speakers:

- Jelena Pejic, Former ICRC Senior Legal Advisor
  International level legislation on counter-terrorism

- Thomas Van Poecke, PhD Fellow, Research Foundation Flanders
  The armed conflict exclusion clause: a comparative perspective

- Liesbet Masschelein, Federal Magistrate, IHL Section, Office of the Federal Prosecutor, Belgium
  The Belgian legal framework regarding the 'armed conflict exclusion clause' and cumulative prosecution for terrorist crimes and IHL crimes: current legal challenges

The fourth session, which focused on the relationship between IHL and counter-terrorism law, was **chaired by Mr. Gert-Jan van Hegelsom, Former Head of the Legal Service of the European External Action Service**. Mr. van Hegelsom initiated the session with a brief overview of the intricate relationship between IHL and counter-terrorism legislation, followed by a warm welcome to the three speakers.

The **first speaker, Ms. Jelena Pejic, Former ICRC Senior Legal Advisor**, gave a presentation on IHL and counter-terrorism legislation at the international level (not including domestic legislation). During her presentation, she identified several points of friction between IHL and the global counter-terrorism framework. She began by outlining the general relationship between the two legal frameworks, then moved on to discuss the impact of counter-terrorism laws on non-international armed conflicts (NIACs) and international armed conflicts (IACs).

In broad terms, significant differences exist between IHL and the global counter-terrorism framework. IHL is unique among bodies of international law in its bifurcated approach to violence–it permits violence against combatants and military objectives, but also regulates and restricts it in relation to civilians and civilian objects. In contrast, counter-terrorism legislation does not adopt a bifurcated approach to violence. An act of terrorism is invariably a criminal act and is always unlawful. Furthermore, under IHL, there is no formal reciprocity, but *de facto* reciprocity plays an important role. Civilians, civilian objects, and persons *hors de combat* must always be equally protected by all sides to an armed conflict. There is no similar principle of equality of rights and obligations of the parties in the treaties dealing with acts of terrorism. Also, IHL prohibits certain acts of terrorism. For instance, during hostilities, it is prohibited to commit acts of violence primarily intended to spread terror among the population. Acts considered terrorism during peacetime are already and always forbidden under IHL. According to Ms. Pejic, this leads us to the following questions: What value does the recent blurring of lines between IHL and counter-terrorism bring? Why is there a need to add a counter-terrorism layer to acts committed in armed conflict which are already prohibited under IHL?

Prior to the 9/11 attacks, there were over half a dozen conventions that centred on counter-terrorism, containing exclusion clauses for acts governed by IHL when the prohibited acts could also be committed in armed conflict. For instance, the International Convention against the Taking of Hostages of 1979 includes a distinct exclusion clause for acts governed by IHL. The UN Draft Comprehensive Convention on Counter-Terrorism of 2000 also has an exclusion clause. However, the 9/11 attacks brought an end to multilateral negotiations. In the aftermath of 9/11, the UN Security Council began adopting resolutions under Chapter VII of the UN Charter. These resolutions, such as the first one, Resolution 1373 of the UN Security Council, did not reference interplay with other bodies of international law, while later ones paid lip service to this issue. They also left it to individual States to define what constitutes an act of terrorism and what constitutes a terrorist organisation. This ambiguity in terminology has had a detrimental impact on IHL. As a result of the global war on terror, the number of non-State armed groups placed on terrorist lists regionally and globally has surged. It is worth noting that the identification of organisations to be included on these lists is always left to individual States. It is extremely difficult to be removed from such a list, and there is no oversight over this process (an Ombudsman was appointed at the UN with an oversight role only after several years).

Regarding the effects of counter-terrorism legislation on NIACs. Firstly, most non-State groups that are parties to a NIAC are on a terrorist list. While a non-State armed group is not prohibited from attacking legitimate military objectives if such an attack aligns with IHL, these acts are, of course, prohibited under domestic law. This interaction between IHL and domestic criminal law has already had a skewed effect on non-State entities. What is the added value of adding a counter-terrorism layer on top of this already skewed relationship? It is driven by political and emotive reasons. States have proven eager to criminalise under domestic law, based on the legal framework developed by the UN Security Council, acts that would not be prohibited by IHL, rendering compliance by armed groups with the latter essentially futile. Secondly, there is a provision encouraging amnesty in the IHL of NIAC, which aims to incentivise non-State armed groups to comply with IHL. However, if the acts of non-State armed groups are always criminalised under domestic law, particularly under terrorism legislation, the chances

of amnesty for those who have fought in accordance with IHL is slim, even though amnesties will often be a necessary prelude to peace negotiations. For instance, after the EU brokered a deal between the Ethiopian government and Tigray armed groups, in March 2023, the Ethiopian government had to vote on removing the relevant group(s) from the national terrorist list.

As regards the effects of counter-terrorism legislation on IACs. Firstly, in recent years, especially following the start of the Russia-Ukraine conflict, we have seen a new evolution whereby States are denominated as 'terrorist States' or 'State-sponsors of terrorism'. Some time ago, the US put the Iranian Revolutionary Guard on their list of foreign terrorist organisations. Iran reciprocated by putting the US' Central Command on their terrorism list. This raises a number of questions: What would happen if there were an IAC between these States and combatants were captured and became prisoners of war on both sides? If national courts are faced with a choice between applying the relevant IHL rules (which they are not very familiar with) and domestic (terrorism) legislation, which body of rules would they be likely to rely on? What would be the effect of disregarding the protections due to prisoners of war under IHL? Secondly, in 2022, the EU Parliament declared Russia a State-sponsor of terrorism. Every act listed for which Russia is named a State-sponsor is in fact a war crime. NATO and the parliaments of several EU nations have made similar designations. What is their value and potential legal effect? Despite pressure on EU executive bodies and the Biden administration to designate Russia as a 'terrorist' State, this has not yet happened. In Ms. Pejic's view it should not, due to the possible undermining of central tenets of IHL in case of conflict. As another illustration of the issue: Earlier this year, Russia prosecuted several members of the Ukrainian Azov brigade, charging them–among others–with participation in a terrorist organisation, all for acts falling within the conduct of hostilities/IHL. If States want their militaries to be treated in accordance with IHL, legal frameworks should not be blurred. In addition, as in a NIAC, terrorist designations would render possible negotiations much more difficult.

In conclusion, the impact of counter-terrorism legislation on NIACs is substantial. As of now, counter-terrorism legislation has not significantly affected IACs in the same way, with the Ukraine-Russia conflict being a notable exception. This is likely because the trend of designating States as terrorist organisations has not yet escalated, but it could change in the future. It is in the self-interest of States and their armed forces to be cautious of this development.

The **second speaker, Thomas Van Poecke, PhD Fellow at the KU Leuven (and funded by the Research Foundation Flanders)**, discussed the armed conflict exclusion clause. Mr. Van Poecke started his presentation by clarifying that armed conflict exclusion clauses are present in international, regional, and national criminal law instruments on terrorism, and they exclude certain activities from the purview of such instruments. It is important to highlight that an exclusion clause is not the same as saving or non-prejudice clauses. While exclusion clauses prevent the application of criminal law instruments on terrorism to certain activities, saving or non-prejudice clauses leave the application of criminal law instruments on terrorism intact. Moreover, armed conflict exclusion clauses primarily focus on the activities of armed actors, not humanitarian exemptions.

Mr. Van Poecke further explained that he scrutinised both international conventions and regional instruments for armed conflict exclusion clauses (hereby leaving out the International Convention against the Taking of Hostages of 1979). Exclusion clauses are not necessarily uniformly drafted and read, for example, as follows:

- "*does not apply to activities of armed forces that are governed by IHL*", as included in the Terrorist Bombing Convention of 1997 (and a number of other international conventions, as well as the draft Comprehensive Convention on International Terrorism) and in the 2002/2017

EU Framework Decision/Directive on Combating Terrorism and the Council of Europe Convention on the Prevention of Terrorism of 2005;

- "*does not apply to activities that are in accordance with IHL*", as included in the Terrorist Financing Convention of 1999;
- "*does not apply to liberation struggles or struggles against occupation*", as included in the Arab Convention of 1998, the OIC Convention of 1999, the (O)AU Convention of 1999, as well as the AU Model Anti-Terrorism Law of 2011 and the Malabo Protocol of 2014; and
- "*does not apply to acts covered by IHL, committed by government forces or members of organized armed groups*", as included in the AU Model Anti-Terrorism Law of 2011 and the Malabo Protocol of 2014.

Mr. Van Poecke also drew a typology of instruments at the national level that include an armed conflict exclusion clause. The vast majority of national laws do not provide for an armed conflict exclusion clause, as this is not mandatory. Those national laws that do, include the following formulations:

- "*does not apply to activities that are in accordance with IHL*", as found in the national laws of the US and Ireland and this for specific offenses, as well as in Belgian national legislation, yet as part of the general scope of the law in question. However, as was further discussed by Ms. Liesbet Masschelein in the subsequent presentation, Belgium is currently in the process of revisioning the armed conflict exclusion clause.
- "*does not apply to activities of armed forces that are governed by IHL*", as included in the national laws of Switzerland for specific offenses (and of the Gambia and Mali, although the effects of the clauses in question are not clear), as well as in the national laws of Canada and New-Zealand, yet as part of the general scope of the law in question.
- "*does not apply to liberal struggles or struggles against occupation*", as included in South African legislation until 2022, after which it was removed despite pressure by the ICRC not to do so.

Mr. Van Poecke concluded that while armed conflict exclusion clauses are prevalent at the international level, they are less so at the regional level and even less so at the national level. There is currently also a trend not to adopt new exclusion clauses and to restrict the scope of existing clauses or to delete them. As such, criminal law instruments on terrorism are expanding from the realm of peace to that of armed conflict. Hence, there is a pressing need to preserve integrity and enforcement of IHL.

The **third speaker, Ms. Liesbet Masschelein, Federal Magistrate at the IHL Section of the Belgian Office of the Federal Prosecutor**, gave a presentation on the current legal challenges related to the Belgian legal framework regarding the 'armed conflict exclusion clause' and cumulative prosecution for terrorist crimes and IHL crimes.

The current Belgian legal framework regarding the 'armed conflict exclusion clause' and cumulative prosecution for terrorist crimes and IHL crimes presents difficulties for the Belgian Federal Prosecutor's Office in a number of cases. The current Article 141bis of the Belgian Criminal Code reads as follows: "*This title shall not apply to acts of armed forces during armed conflict as defined in and subject to international humanitarian law, nor to the acts of the armed forces of a State in the exercise of their official duties, to the extent that such acts are subject to other provisions of international law*". Until recently, this article was interpreted in a complex manner in court cases. It was interpreted as excluding prosecution of all terrorist crimes in the case of crimes committed during an armed conflict by a group recognised as both a terrorist group and a party to the armed conflict (for example, IS in Syria).

In certain cases, this interpretation (potentially) led to impunity. Ms. Masschelein illustrated this with three examples of acts committed by a group recognised as both a terrorist group and a non-State armed group (for instance, IS in Syria):

- An attack by IS on a village followed by the execution of civilians: Under Article 141bis of the Belgian Criminal Code, prosecution for war crimes is possible because the act is not in accordance with IHL, but prosecution for a terrorist crime is not possible.
- An attack by IS on a military base resulting in the death of several soldiers: Under Article 141bis of the Belgian Criminal Code, prosecution for war crimes is only possible if the act is not in accordance with IHL, and prosecution for a terrorist crime is not possible.
- Financing IS: according to Article 141bis of the Belgian Criminal Code, prosecution for war crimes is not possible because the act falls outside the scope of IHL and prosecution for a terrorist crime is not possible.

In response to this situation, the Interministerial Commission for Humanitarian Law adopted a new interpretation of Article 141bis of the Belgian Criminal Code whereby the definitions of 'terrorist group' and 'armed forces' were considered autonomous. Recently, the Federal Prosecutor's Office also applied this new interpretation to criminal cases. Most of this new interpretation is accepted by case law (and in particular that the definition of a 'terrorist group' and 'armed forces' are autonomous and that IS in Syria is considered a terrorist group and, at least since 2014, an armed force). However, jurisprudence has struggled with the concept of 'acts within the scope of IHL' and case law does not consistently uphold the distinction between an act that is or is not in compliance with IHL. Examples have shown that the attempt to better interpret Article 141bis of the Belgian Criminal Code has not improved the situation. Therefore, a proposal to reformulate Article 141bis is being discussed.

The Federal Prosecutor's office currently has around 20 cases under investigation for cumulative offences (both terrorist crimes and IHL offences, i.e., war crimes, crimes against genocide, etc.). According to Ms. Masschelein, the evolving interpretation and/or text of article 141bis of the Belgian Criminal Code will play a significant role in the current and future prosecution of such cases.

2.3.4 Session 5 – The Right to Life of a Soldier in Combat

Chair: Emmanuel Jacob, President, EUROMIL

Speakers:

- Prof. Dr. Valeria Eboli, Italian Naval Academy
  The Right to Life of a Soldier in Combat

- Dr. Jan Arno Hessbruegge, Visiting Professor, University for Peace, Costa Rica & Human Rights Officer, United Nations
  The Soldier's Human Right to Life in Combat: Analytical Framework based on International Human Rights Law

The fifth session of the 'Silent Legal Inter Arma?' VI Conference dealt with the right to life of a soldier in combat. This session was **chaired by Mr. Emmanuel Jacob, President of EUROMIL**. Mr. Jacob initiated the session by outlining EUROMIL's activities and objectives. EUROMIL, the European Organisation of Military Associations and Trade Unions, serves as the voice of European soldiers at the international level. Its primary mission is to advocate for the professional and social interests of European soldiers, as well as their fundamental rights and freedoms. EUROMIL addresses a wide range

of topics related to EU and international law, such as suicide, the right to organise, human rights within and by the armed forces, and the social rights of military personnel. It also facilitates the exchange of information, experiences, and best practices among its member associations. Although EUROMIL operates independently, notably from the EU and NATO, it maintains strong connections with other organisations within Europe, such as the Council of Europe, particularly concerning human rights. The right to life, the main topic of this session, is one such area of focus. EUROMIL sends observers to the UN and the European Parliament. It strives to protect and promote the human rights, fundamental freedoms, and socio-professional interests of the military, endorsing the concept of the 'Citizen in Uniform'. In this regard, a soldier is entitled to the same rights and obligations as any other citizen.

The first speaker, **Prof. Dr. Valeria Eboli from the Italian Naval Academy**, furthered the discussion with a presentation on the right to life of military personnel, as stipulated in Article 2 of the European Convention on Human Rights (ECHR) of 1950. She started her presentation with highlighting the differences in application between IHL and HRL. IHL provides protection for those who are not actively participating in hostilities, mainly through the limitation on means and methods of warfare. It also outlines measures to protect combatants when they are actively involved in hostilities. IHL is, however, silent about the obligation of States to respect the right to life of its own combatants.

HRL is another body of law that applies during armed conflict. It has its own scope of application, which differs from other bodies of law. HRL has an extraterritorial application, meaning that a State has jurisdiction outside its own territory when it has control over a certain territory or over certain individuals, irrespective of nationality. This was exemplified in several cases of the European Court of Human Rights (ECtHR) (e.g., Banković et al. vs. Belgium et al, Ilaşcu et al. vs. Moldova and Russia, Al-Jedda vs. the United Kingdom, and Al-Skeini et al. vs. the United Kingdom). Furthermore, HRL applies both in peacetime and wartime and its applicability is not automatically suspended in armed conflicts. In such cases, IHL and HRL interplay, and when there are conflicts between the two, IHL is considered *lex specialis*, or the law governing the specific subject matter.

Hereafter, Prof. Eboli turned to the right to life of military personnel. She explained that the right to life, as for example foreseen in Article 2 of the ECHR as well as Article 6 of the International Covenant on Civil and Political Rights (ICCPR) of 1966, is non-derogable in nature. This does not mean that there are no exceptions to be made. Some limitations are provided. Article 2 of the ECHR foresees, for example, that the deprivation of life shall not be regarded as inflicted in contravention of Article 2 when it results from the use of force which is no more than absolutely necessary: "(a) *in defence of any person from unlawful violence; (b) in order to effect a lawful arrest or to prevent the escape of a person lawfully detained; (c) in action lawfully taken for the purpose of quelling a riot or insurrection*". Article 6 of the ICCPR foresees that "*Every human being has the inherent right to life. This right shall be protected by law. No one shall be arbitrarily deprived of his life*". Under certain circumstances, the right to life can also be suspended, yet this does not happen automatically but must instead be invoked by the State in question. Principally, Article 15 ECHR prohibits derogation from the right to life in time of emergency, but it allows for an exception in the case of deaths resulting from lawful acts of war.

The right to life involves a dual obligation: a negative and a positive one. The negative obligation prevents States from interfering (i.e., refraining from violating the right), while the positive obligation requires States to take reasonable and suitable measures to protect individuals' rights effectively. Those steps and actions consist of all reasonable and suitable measures a national authority could take to protect the effective, rather than the theoretical, enjoyment of rights (see also Golder vs. United Kingdom, 1975 and Airey vs. Ireland, 1979). When it comes to the protection of a soldier's right to life in combat, there are several potential positive obligations that military authorities must fulfil. Firstly,

States must ensure that military training, the planning of operations, and the equipment used do not unnecessarily endanger the lives of servicepersons. Secondly, States must ensure that members of the armed forces have proper access to healthcare when their lives are at risk. Thirdly, in the event of a death, there is an obligation to carry out an investigation to ascertain the circumstances leading to the person's death.

Case law, such as the Smith case by the UK House of Lords, also confirms that when the right to life is violated, HRL is the main body of law that applies. For instance, in the context of conflicts in Afghanistan or Iraq, families of soldiers have argued that their loved ones were exposed to avoidable risk and that the government did not provide sufficient protection.

In conclusion, while the issue is not specifically regulated, conclusions can be drawn by jointly considering HRL and IHL and referring to the relevant provisions. This approach ensures that the right to life, even in the complex context of combat, is upheld and protected.

The second speaker, **Dr. Jan Arno Hessbruegge, Human Rights Officer at the United Nations, but speaking in an academic capacity as Visiting Professor at the University for Peace (Costa Rica)**, wrapped up the day's fifth and final session by laying out an analytical framework of a soldier's right to life in combat grounded in the jurisprudence of the UN Human Rights Committee and other United Nations human rights mechanisms. States have a duty to respect the lives of their soldiers by not exposing them to risk unlawfully or arbitrarily. While there are inherent limitations due to the nature of military life and soldiers can be exposed to risks of being killed in combat, States must seek to limit such risks with due diligence, investigate any potential violations, and provide effective remedies.

Dr. Hessbruegge further explored the right to life, reiterating Prof. Eboli's point that the right to life fully applies in armed conflict and wherever a State has effective control or power over a territory or individuals (hence also in relation to the deployment of their soldiers abroad). This right encompasses both actual loss of life and potential risks to life. While States do create risks to life by sending military personnel into combat, these risks must not be unlawful, discriminatory, unnecessary, or disproportionate. Firstly, for a risk assigned to a soldier's life to be lawful, it must have a legal basis. If there is no clear basis in national law or the national law is not followed, the assignment of risk would be a violation (e.g., if conscripts are deployed in combat operations abroad contrary to national law). Risk cannot be assigned as a form of punishment (e.g., by sending soldiers who protest against conditions to the frontline) or to conduct a war of aggression, as the latter ipso facto violates the rights to life of anyone killed by it as per the UN Human Rights Committee's jurisprudence. Secondly, the allocation of risks must be free from discrimination. This means that factors such as skin colour, gender, or belonging to a politically vulnerable minority group must not influence these decisions (e.g., because the lives of soldiers of an ethnic minority are considered politically more 'expendable' than others). Additionally, any substantial deviation in the approach to risk between different units or front sectors that lacks military justification would be deemed discriminatory. Thirdly, any assigned risk that lacks a military purpose (e.g., to be ordered not to surrender for the sole purpose of protecting their 'honour') or for which a less risky and equally effective alternative exists, is considered unnecessary and is therefore also prohibited. Risks must always be mitigated with reasonable precautions, such as providing adequate equipment and training, avoiding overly restrictive rules of engagement (notably by not denying soldiers' their right to self-defence), and ensuring the ability to organise casualty evacuations and medical care, as also required by IHL. Fourthly, the assignment of risks to life must not be disproportionate, and the level of risk to soldiers should be weighed against the importance of the mission and its protective impact. The level of self-assumed risk can vary among members of the armed forces (e.g., between conscripts and voluntarily enlisted soldiers) and should be considered,

along with military effectiveness considerations. In the proportionality analysis, it must be heavily factored in to what extent different operational choices increase or decrease the risk of incidental civilian losses (e.g., a State may not conduct a bombing campaign with disproportional civilian losses to protect soldiers from any risks inherent to ground operations).

Dr. Hessbruegge concluded his presentation by briefly discussing effective remedies for violations of the right to life. He explained that States have a duty to investigate potentially unlawful deaths in combat by conducting post-operation assessments, as also laid out by the UN's revised Minnesota Protocol. States must provide soldiers (or their families) effective remedies in case of apparent violations, including reasonable access to justice (with courts showing a certain level of deference in the review of battlefield decisions), and the possibility of compensation and satisfaction. Soldiers have the right to disobey manifestly unlawful orders to deploy if the risk to their life or physical integrity appears severe and irreparable (e.g., an order to fight in a war of aggression). This is a logical corollary of the duty under ICL to disobey manifestly unlawful orders. Indeed, soldiers cannot be expected to disobey manifestly unlawful orders that violate other persons' right to life, but diligently follow manifestly unlawful orders that violate their own right to life.

2.4 Friday 22 September 2023

2.4.1 Session 6 – Hybrid Threats

Chair: Mr. Olavi Jänes, Legal Advisor, Baltic Defence College

Speakers:

- Eto Buziashvili, Research Associate, Digital Forensic Research Lab, Atlantic Council
  Russian disinformation and influence operations

- Brigadier Keith Eble, Head Operational Law, British Army
  A British military-legal perspective on hybrid threats

- Andres Munoz Mosquera, Director, Office of Legal Affairs, ACO, NATO
  Lawfare – SHAPE OLA's approach

The sixth session of the conference delved into hybrid threats. This session was **chaired by Mr. Olavi Jänes, Legal Advisor at the Baltic Defence College**. Mr. Jänes initiated the discussion by referring to the definition of hybrid threats provided by the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). Hybrid CoE characterises hybrid threats as:

- "*Coordinated and synchronized action that deliberately targets democratic states' and institutions' systemic vulnerabilities through a wide range of means.*
- *Activities that exploit the thresholds of detection and attribution, as well as the different interfaces (war-peace, internal-external security, local-state, and national-international); and*
- *Activities aimed at influencing different forms of decision-making at the local (regional), state, or institutional level, and designed to further and/or fulfil the agent's strategic goals while undermining and/or hurting the target*."

Mr. Jänes then introduced the first speaker, **Eto Buziashvili, Research Associate at the Atlantic Council's Digital Forensic Research Lab**, who gave a presentation on Russian disinformation and influence operations. She began by elucidating that hybrid operations employ a wide range of tactics,

targeting democratic States by exploiting their vulnerabilities. A key goal is often to influence the decision-making at the State and local levels. The classification of such operations, however, poses a challenge.

Turning to the Russia-Ukraine war, Russia has been employing a strategic approach in the information space. The goals are twofold: domestically, the aim is to maintain and increase support for the war, while internationally, the objective is to influence public opinion about the war, justify the re-invasion, and decrease support for Ukraine. The audiences targeted by these efforts are diverse, including domestic audiences (through censorship and propaganda), Ukrainians (with the aim of demoralisation), the West (with the intent to tarnish Ukraine's reputation and undermine support for the country), and the 'Global South' (Latin America and Africa, where the goal is to associate the West with colonialism).

The central question in 2021 was whether Russia would further invade Ukraine. The Atlantic Council's Digital Forensic Research Lab examined disinformation and propaganda to predict Russia's actions, focusing on narratives propagated by 10 Russian State-controlled outlets that claimed Ukraine was planning to start a war. In November 2021, articles suggested that Kyiv was violating the ceasefire agreement and that Ukraine might attack the Donbas. In December 2021, outlets blamed the US for training extremists to attack the Donbas, and in January 2022, the outlets suggested that Ukraine might stage a chemical attack in Donbas and blame it on the separatist authorities. By January 2022, there was a 50% increase in messages about a potential Ukrainian invasion of Russia in the near future, leading analysts to suspect that something was afoot.

The Kremlin and Russian news outlets justified a war of aggression against Ukraine through narrative warfare. These narratives are not new and have been observed since at least 2014. Various techniques and modus operandi have been identified, including the control and weaponization of the comment sections of Western media, the theft of Western media logos, the creation of fake fact-checking pages/websites, the establishment of fake Facebook/Instagram profiles, the hijacking of protests in EU capitals, the use of the Internet Research Agency (IRA) (a troll factory owned by Prigozhin that focuses on creating misleading and fake content online), and the use of deepfake technology to create, for example, false images of Ukrainian President Zelensky to undermine Ukraine's partnership with Türkiye.

Ms. Buziashvili concluded her talk by noting that censorship measures have also been intensified in Russia, including the blocking of Western platforms, the enactment of laws on fake news related to the Russian army, control over search engines, the domestic replacement of YouTube and Wikipedia, and the blocking of VPNs. A significant increase in censorship was observed in Russia following the re-invasion of Ukraine. Surveillance measures, such as the use of the Oculus system, have also been employed.

The second speaker, **Brigadier Keith Eble, Head of Operational Law in the British Army**, delivered a talk on the British military-legal perspective on hybrid threats. He began by defining 'hybrid', referring to the work of the Multinational Capability Development Campaign, which is backed by 14 nations, including the UK. This campaign, through its Countering Hybrid Warfare project, has been striving to define 'hybrid' as a concept. In 2017, they recognised that the concept of 'hybrid warfare' was not well understood, but was agreed by all, including NATO and the EU, to be a problem. By 2019, they had defined 'hybrid warfare' as the synchronised use of multiple instruments of power, tailored to specific vulnerabilities across societal functions to achieve synergistic effects. According to the UK, to counter such threats, a comprehensive government approach is needed. NATO currently views 'hybrid' as referring to threats from State and non-State actors to political institutions, with the aim of influencing public opinion and undermining NATO security. This involves the use of both covert and overt methods

of propaganda, deception, sabotage, and other non-military tactics, sometimes in coordination with military operations. An example of this is the Russian Federation's operations against Ukraine in 2014. NATO acknowledges that other States use malicious cyber operations, confrontational rhetoric, disinformation, and economic power to create dependencies and influence, thereby challenging the rules-based international order and democratic values. Technology has amplified the speed and reach of State and non-State actors in hybrid operations. NATO's strategy is to prepare, deter, and defend its members against such threats. Hybrid threats could trigger UN Charter provisions and an Article V NATO response, or lesser State actions such as lawful countermeasures.

Mr. Eble subsequently explained that the UK's defence strategy is steered by an integrated review and focuses on enhancing readiness and future transformation of the UK army through Operation MOBILISE. The strategy includes deterring Russian aggression, preventing war, and lawfully addressing hybrid threats in collaboration with other government departments. The UK armed forces operate under operational law, encompassing IHL and other international laws, UK laws, and human rights law applicable to military operations. At present, the UK army is supporting Ukraine's self-defence and lawful response to aggression, learning tactical and operational lessons about Large Scale Combat Operations (LSCO) and the use of strategic tools such as cyber, space, and special operations. When engaged in hybrid operations, almost all areas of law are relevant, including not only the UN Charter provisions, *jus ad bellum*, IHL (if above the threshold of armed conflict), but also HRL, data protection law, copyright law, defamation, tort, contract, national security laws, and political agreements between friendly States about the conduct of armed forces in other States. Legal training and advice are crucial, emphasising that there is no grey zone in the law. Legal advice must be unambiguous and simple, with legal advisers available to address questions of legal risk. This supports the rule of law and democratic control of the army.

Mr. Eble then discussed potential options for States to respond to threats. Firstly, while diplomatic and economic actions are the primary responses, technical activities related to cyber attribution and offensive cyber operations also play an important role. The UK and its allies have, for instance, publicly attributed cyber hacking to the Chinese State in 2018 and 2021, calling for an end to such actions. The UK has also used strategic offensive cyber tools in coordinated operations by the Government Communications Headquarters (GCHQ) against Daesh/ISIS. Secondly, NATO' Office of Legal Affairs (OLA) of the Allied Command Operations (ACO) does remarkable work in analysing threats and identifying legal State craft practices. This includes identifying both legitimate and spurious uses of courts and tribunals. State interventions in litigation are increasingly being used as collective State action against non-compliers and aggressors (see e.g. International Court of Justice (ICJ) Case on Allegations of Genocide under the Convention on the Prevention and Punishment of the Crime of Genocide (Ukraine vs. Russian Federation) (2022); the ECtHR case on Ukraine vs. Russia (re Crimea) concerning Ukraine's allegations of a pattern ('administrative practice') of violations of the ECHR by the Russian Federation in Crimea beginning in February 2014 (App. Nos 20958/14 and 38334/18)). Thirdly, States are increasingly using their domestic (criminal) law to deal with hybrid threats. The UK's National Security Act 2023 is an example of a clear intent to tackle these threats. In February 2022, the ICC Prosecutor, Karim Khan King's Counsel, reminded the parties involved in the war in Ukraine of their obligations under the law of armed conflict/international humanitarian law. In March 2022, the situation in Ukraine was referred to the ICC Prosecutor by multiple State applications, with States cooperating on evidence gathering.

Mr. Eble concluded his presentation by highlighting several potential legal issues associated with emerging technologies. Firstly, in terms of cybersecurity, the UK's National Cyber Force (NCF), a joint initiative of GCHQ, operates under a policy called "*Responsible Cyber Power in Practice*" that was

published in April 2023. This policy outlines the operational principles for cyber operations, emphasising accountability, precision, and calibration to ensure compliance with both policy and law. Secondly, concerning artificial intelligence (AI), there are ongoing practical considerations about how AI might be utilised in military operations. AI has the potential to be used more broadly by the armed forces, including in hybrid operations. The rise of automated systems and the use of deep fake technology could significantly influence hybrid operations conducted by potential adversaries. In response to these challenges, NATO has committed to using facts and truth, a strategy that must be as effective and lawful as possible.

The third speaker, **Andres Munoz Mosquera, Director at the Office of Legal Affairs, ACO, NATO**, gave a presentation on the Supreme Headquarters Allied Powers Europe (SHAPE) OLA's approach to lawfare. He pointed out that 'hybrid warfare' is not a new concept; it is as ancient as warfare itself. The term 'hybrid' warfare and threats, which are difficult to define, originated from the Israeli Defence Forces' (IDF) characterisation of Hezbollah's activities in 2006. It essentially refers to a comprehensive, 360-degree approach to conflict, utilising all available power instruments. Russia and China are recognised for their employment of hybrid threats. In a 1999 publication, two officers from the People's Liberation Army, Qiao Liang and Wang Xiangsui, argued that the highest form of warfare is to defeat the enemy without engaging in combat.

Hybrid threats can manifest in various ways. They can be legal or non-legal, kinetic or non-kinetic, and may or may not cross the threshold of an armed attack and/or the application IHL. Consequently, lawfare is a type of hybrid warfare. While there is no universally accepted definition for lawfare, it can be described as the (mis)use of legal systems and institutions to achieve political objectives. Lawfare can be employed to legally prepare the battlefield and seems to play a crucial role in establishing internal (within the State) and external (international) legitimacy. Currently, national law appears to be the primary source of lawfare aimed at establishing legitimacy.

Mr. Mosquera reminded the audience that international law is primarily based on good faith among its actors. It has been noted that Russia, as part of its lawfare operations, has been exploiting this good faith and attempting to shift the paradigm of international law usage. For instance, Russia has granted its constitutional court the authority to nullify any treaty it has signed, thereby undermining other actors' confidence in their international agreements with Russia. Russia has also been altering its national law to shape the international landscape, exploiting international warranty systems such as international courts and tribunals, and setting up a sham investigation commission for the war crimes committed in Bucha.

To conclude, Mr. Mosquera posed the question of how NATO should respond to lawfare, how it should anticipate lawfare, and how it should categorise such actions. He reminded the audience that in previous NATO/Western military operations, policy standards were maintained that exceeded the requirements of the law. For example, when NATO declared a zero-CIVCAS policy in Afghanistan, the Taliban began to position civilians around military objectives. These should not be regarded as legal precedents for any future actions NATO undertakes. To counter such actions, SHAPE OLA has developed a tool to identify malign lawfare against NATO. This tool determines the extent and consequences of the malign lawfare and assigns the officer of primary responsibility to counter the lawfare.

2.4.2 Award Ceremony

Mr. Alfons Vanheusden, Assistant Secretary-General of the ISMLLW, has been honoured with the prestigious Serge Lazareff Prize for his exceptional service. This international accolade, presented by Mr. Mosquera, is bestowed upon both civilians and military personnel under the auspices of SHAPE

OLA. The prize is a recognition of significant contributions in the realm of legal affairs pertaining to NATO's operations. The certificate of recognition that Mr. Vanheusden received stands as a testament to his unwavering dedication and remarkable contributions. We extend our hearty congratulations to Mr. Vanheusden on this well-deserved honour.

2.4.3 Closing Ceremony

The conference was officially concluded by **Mr. Ludwig Van Der Veken, who serves as the President of the Belgian Group and the Secretary-General of the ISMLLW**. He underscored the importance of law as an ethical benchmark and expressed his confidence in applying or referring to it, particularly when it is in line with international law, including HRL. This confidence is rooted in the understanding that the existing international legal framework is a product of ethical deliberations and lessons drawn from tragic historical events such as World War II and the Holocaust.

Key legal instruments like the UN Charter of 1945, the four Geneva Conventions of 1949, and the ECHR of 1950 were established in the wake of these events. However, the potent collective resolve of 'never again' seems to be diminishing over time. In 2022, 141 UN Member States vehemently condemned the aggression by a Permanent Member of the UN Security Council against Ukraine, a breach of Article 2(4) of the UN Charter.

Despite this, there have been numerous instances of horrific acts by armed forces and groups who disregard the Geneva Conventions and IHL. In recent times, there have also been criticisms against the protections offered by HRL, often justified in the name of national security or efficiency. Hence, it is of paramount importance to cherish, elucidate, and defend the rules-based order. This implies choosing to abide by the law, even when under attack, to prevent ourselves from becoming a monster in the process of defeating one.

As the event concluded, Mr. Van Der Veken extended his gratitude to the conference partners, including the Baltic Defence College, the University of Leiden, the Lieber Institute for Law and Warfare, and the UK's Army Legal Services. He also thanked the chairs and speakers for their insightful presentations and responses, all participants for their interest, questions, and comments, the staff of the Grand Hotel Casselbergh, and Mr. Hans Vranken and Mr. Geert Maes for their support. Special thanks were given to the program director, Mr. Alfons Vanheusden, for his commendable work. Lastly, he announced that the Belgian Group of the ISMLLW plans to host the 'Silent Leges Inter Arma' Conference VII around the same time next year, and invitations will be sent out in due course.