Expertise

The Law of Armed Conflict and Emerging Technologies: Legal, Ethical and Strategic Perspectives[1]

CHRISTOPHE LEUENBERGER VERZASCONI

Abstract Die Konferenz zum Thema «Das Kriegsvölkerrecht und neue Technologien» verdeutlichte, wie geopolitischer Wettbewerb und rasante technologische Innovationen die Kriegsführung und die Anwendung des humanitären Völkerrechts (IHL) neu gestalten. Während Technologien wie Cyberfähigkeiten, Künstliche Intelligenz, autonome Systeme und Quantencomputing das Einsatzumfeld verändern, waren sich die Teilnehmer einig, dass die Kernprinzipien des humanitären Völkerrechts unverändert bleiben, auch wenn ihre Anwendung immer komplexer wird: Cyberoperationen verwischen Konfliktgrenzen und die Zuordnung von Verantwortlichkeiten, KI bietet sowohl Chancen für eine verbesserte Einhaltung der Vorschriften als auch Risiken, die mit Geschwindigkeit und Unsicherheit verbunden sind, Kritische Infrastrukturen wie Unterseekabel und Cloud-Systeme werfen neue regulatorische Fragen auf. Quantencomputing stellt ein zukünftiges systemisches Risiko dar, da es aktuelle Verschlüsselungsstandards potenziell untergraben könnte. Eine zentrale Schlussfolgerung der Konferenz war, dass die menschliche Verantwortung weiterhin im Mittelpunkt steht: Technologie mag die Entscheidungsfindung unterstützen, doch rechtliches Urteilsvermögen und die Rechenschaftspflicht müssen bei den menschlichen Akteuren bleiben. Die Gewährleistung der Einhaltung erfordert daher eine kontinuierliche rechtliche Überprüfung, die Integration des humanitären Völkerrechts in die technologische Gestaltung sowie eine engere Zusammenarbeit zwischen juristischen, militärischen und technischen Kreisen. Die Konferenz bekräftigte, dass die Achtung des humanitären Völkerrechts sowohl eine rechtliche Verpflichtung als auch ein strategischer Vorteil ist, der für Legitimität, Vertrauen und langfristige Stabilität unerlässlich ist, und dass seine Wahrung angesichts des technologischen Wandels eine gemeinsame Verantwortung darstellt.

Abstract

The conference on "The Law of Armed Conflict and Emerging Technologies" highlighted how geopolitical competition and rapid technological innovation are reshaping warfare and the application of international humanitarian law (IHL). While technologies such as cyber capabilities, artificial intelligence, autonomous systems and quantum computing are transforming the operational environment, participants agreed that the core principles of IHL remain unchanged, even as their application becomes more complex. Cyber operations blur conflict thresholds and attribution, AI offers both opportunities for improved compliance and risks linked to speed and uncertainty, and critical infrastructures such as undersea cables and cloud systems raise new regulatory questions. Quantum computing poses a future systemic risk by potentially undermining current encryption standards. A key conclusion was that human responsibility remains central: technology may support decision-making, but legal judgment and accountability must remain with human actors. Ensuring compliance therefore requires continuous legal review, integration of IHL into technological design and closer cooperation across legal, military and technical communities. The conference reaffirmed that respect for IHL is both a legal obligation and a strategic asset, essential for legitimacy, trust and long-term stability, and that safeguarding it in the face of technological change is a shared responsibility.

Schlüsselbegriffe Kriegsvölkerrecht; humanitäres Völkerrecht; neue Technologien; KI; menschliche Verantwortung
Keywords the law of armed conflicts; international humanitarian law; emerging; technologies; AI; human responsibility

COLONEL CHRISTOPHE LEUENBERGER VERZASCONI,
Attorney-at-Law, LL.M, is Commander of the IHL Detachment of the Swiss Armed Forces, Co-President of the Swiss Society for Military Law and the Law of War and a member of the International Institute of Humanitarian Law, San Remo
E-Mail: leve65@bluewin.ch

Geopolitical challenges and their implications for Switzerland

In his keynote, **Dr. Markus Mäder,** State Secretary at the State Secretariat for Security Policy (SEPOS) in the Federal Department of Defence, Civil Protection and Sport, underscored that Switzerland faces a rapidly deteriorating security environment shaped by power politics, weakening international law, and growing geopolitical rivalry, particularly involving Russia, China and the United States. He emphasised that Switzerland must respond to this environment through a comprehensive security approach built on resilience, protection and defence, while maintaining neutrality and strengthening international cooperation. Dr. Mäder underlined that Switzerland aims to maintain the ability to defend itself independently while preparing for cooperation with partners if necessary, without compromising neutrality. In this context, interoperability, particularly with NATO standards, plays a key role. As highlighted by the State Secretary, security today is interconnected across military, civilian, technological and societal domains, and therefore requires collective responses. Technological advances such as AI and cyber capabilities are transforming warfare, increasing vulnerabilities and challenging existing legal frameworks. Dr. Mäder highlighted that Switzerland's core strengths – federalism, direct democracy, economic integration and neutrality – enhance its resilience but also expose it to hybrid threats such as disinformation, espionage and economic coercion. In response, Switzerland should pursue a comprehensive security approach that integrates civilian and military instruments and places strong emphasis on international cooperation.

Global Security in a changing world order

In the first panel, **Dr. Gorana Grgic** (Head of the Global Security Team, Centre for Security Studies, ETH Zürich) described in her statement a global order increasingly defined by contestation rather than coherence, resembling a "mosaic" of overlapping structures rather than a single unified system. She argued that major powers such as the United States, China and Russia are reasserting spheres of influence, not primarily through territorial control, but through economic, technological and institutional means that create dependencies and shape regional dynamics. Regions have thus become the main arenas of competition, with their insti-

Figure 1: The participants of the ISMLLW conference in front of the AAL in Lucerne. (Source: Author)

tutional strength determining whether they can resist external pressure or become conduits for influence. Dr. Grgic highlighted different forms of regionalism, ranging from the EU's regulatory and defensive capacity to more instrumental or flexible models seen in China's Belt and Road Initiative or ASEAN. The global system, she suggested, is governed simultaneously by logics of cooperation, autonomy and control. This fragmentation creates risks such as escalation, regulatory fragmentation and institutional paralysis, which she addressed through the concept of "negotiated pluralism" as a way to preserve cooperation despite diverging norms. On technology, Dr. Grgic emphasised that while it is a powerful driver of change, it is not deterministic. Warfare is evolving toward "intelligentization", marked by multidomain operations, AI-enabled systems and increased precision, but technological change alone does not constitute a military revolution; its impact depends on how it is integrated into strategy and organisation.

In the panel discussion with **Dr. Markus Mäder** and **Dr. Tobias Vestner** (Director of the Research and Policy Advice Department at the Geneva Centre for Security Policy), participants stressed the high degree of uncertainty surrounding future developments and the limits of prediction. They underscored the need for scenario-based thinking, flexible strategies that serve as a "compass", and greater interdisciplinary cooperation. The discussion also highlighted the growing role of middle powers, which can shape outcomes through coalitions and shared interests, with countries like Switzerland demonstrating that power today extends beyond territory to technological, financial and regulatory influence. Overall, the exchange pointed to a fragmented and technologically driven global order that requires adaptive strategies, resilient institutions and sustained cooperation to manage its risks and opportunities.

Is a lower threshold for the application of international humanitarian law emerging?

The second panel, chaired by **Prof. Dr. Marco Sassoli** (University of Geneva) and featuring **Dr. Julia Grignon** (Associate Professor at the University of Panthéon-Assas, Paris) and **Dr. Antonio Coco** (Associate Professor at the University of Essex), examined whether modern technologies are leading to a lowering of the threshold for the application of IHL. The discussion highlighted that developments such as drones, cyber operations and information warfare challenge traditional understandings of when an armed conflict arises. In this context, attribution remains a central issue, as identifying the actor responsible for an attack is essential for determining whether a situation qualifies as an international or non-international armed conflict. Where attribution is unclear, legal classification becomes more difficult. Nevertheless, the panel stressed that IHL considerations must continue to guide the planning and conduct of operations, even in situations where the precise classification of the conflict remains uncertain.

Several grey areas were discussed in the panel. Cyber operations may qualify as armed conflict only where their effects are comparable to those of kinetic attacks,

while disruptions such as temporary internet outages remain legally unsettled. Violations of due diligence obligations by states, on their own, generally do not meet the threshold for armed conflict. Similarly, the mere presence or use of drones does not automatically amount to an "attack" or use of force; rather, the context and concrete effects are decisive. Even the use of armed drones may not constitute an attack, depending on how they are employed. With regard to targeted killings and extraterritorial operations, IHL may apply when members of armed groups are targeted abroad, but targetability depends on functional roles rather than formal status and may also intersect with domestic legal frameworks. The panel further noted that disinformation alone does not constitute a use of force, although it may indirectly lead to violence that could trigger an armed conflict, while emerging concepts such as cognitive warfare remain legally and practically underdeveloped.

The panel also explored the temporal dimension of IHL, noting that preparatory acts, such as deploying cyber capabilities or dormant malware, do not necessarily trigger armed conflict but must still comply with IHL obligations in anticipation of potential use. The relevance of obligations to review weapons under Article 36 of Additional Protocol I to the Geneva Conventions was also noted, though their customary status remains debated. Overall, the panel concluded that while technological developments are testing the boundaries of existing legal frameworks, they have not fundamentally lowered the threshold for the application of IHL. Instead, they expose ambiguities and the need for clearer interpretation and possibly further normative development, particularly in the cyber and information domains.

Cyber warfare and international humanitarian law

Panel 3, bringing together Ambassador **Sandra Lendenmann Winterberg** (Vice-Director, Directorate of International Law, Swiss Federal Department of Foreign Affairs), Lieutenant Colonel **Nick Wobma** (Deputy Head, Law Branch, NATO Cooperative Cyber Defence Centre of Excellence) and **Dr. Heather Harrison Dinniss** (Senior Lecturer, Centre for International and Operational Law, Swedish Defence University), examined how existing legal frameworks apply in the cyber domain. A central issue discussed was the qualification of cyber operations as "attacks." While operations causing physical damage or injury clearly fall within this category, more complex questions arise in cases involving non-physical effects, such as data deletion or the disruption of functionality. The panel noted that cyber operations may still qualify as attacks where they directly impair the functioning of systems, depending on their severity and consequences.

The discussion highlighted the increasing relevance of cyber operations for critical civilian systems, including healthcare, financial networks, and digital infrastructure such as cloud services and communication backbones. Even without physical destruction, such operations can produce significant cascading effects, complicating their assessment under IHL. In this context, the classification of military objectives becomes more difficult, as cyber infrastructure is often interconnected and dual-use in nature. Nevertheless, the principle of distinction remains fundamental, even if its application is more complex in practice. Where a cyber operation qualifies as an attack, the full set of IHL rules applies, including proportionality and precaution. Even where this threshold is not met, actors remain bound by obligations of constant care, requiring them to consider foreseeable consequences and minimise harm. The panel also underscored that certain types of data, particularly medical data and healthcare-related databases, benefit from specific protection under IHL.

Emerging technologies such as AI add further complexity by increasing interdependencies, accelerating operational tempo and making outcomes harder to predict. This raises concerns about maintaining compliance with IHL in high-speed decision-making environments. At the same time, the panel clarified that misinformation and disinformation may qualify as lawful ruses of war, provided they do not cross into prohibited conduct such as perfidy. Overall, the discussion emphasised the need for robust legal reviews of cyber capabilities, the development of clear national positions to strengthen state practice, and enhanced education and training for operators. Despite the challenges posed by technological developments, the panel concluded that IHL remains fully applicable and relevant but requires careful interpretation and practical implemen-

tation in an increasingly complex and fast-evolving environment.

Autonomous weapon systems & artificial intelligence

Panel 4, chaired by **Reto Wollenmann** (Deputy Head Section Arms Control, Disarmament and Cybersecurity, Swiss Federal Department of Foreign Affairs) with contributions from **Joe Boucher** (Research Assistant, Swiss Centre for Drones and Robotics, armasuisse Science and Technology, Swiss Federal Office for Defence Procurement), **Dr. Jessica Dorsey** (Assistant Professor of International and European Law, Utrecht University) and Colonel **Inna Zavorotko** (Head of International Humanitarian Law, Ministry of Defence, Ukraine), examined how AI is rapidly transforming warfare and what this means for compliance with IHL. The discussion highlighted that AI is already deeply embedded in modern military operations, from intelligence analysis and battle management systems to AI-enabled drones and counter-drone technologies. While fully autonomous systems remain limited, there is a clear trend toward delegating specific functions to AI, sometimes reducing direct human involvement in parts of the decision-making process.

A central insight was the dual nature of AI. On the one hand, AI offers significant potential to enhance IHL compliance by improving target identification, supporting distinction, proportionality and precaution, and enabling more accurate assessments of collateral damage through the processing of large datasets. On the other hand, serious risks persist, including misidentification due to flawed or biased data, system vulnerabilities, the accelerating speed and scale of operations, and the danger of overreliance on AI outputs. The panel stressed that AI itself bears no responsibility; legal accountability remains firmly with human operators and commanders. Maintaining meaningful human control was therefore identified as essential. AI should assist, but not replace, human judgment, and operators must understand the systems they employ, including their limitations. This becomes increasingly challenging as operational tempo accelerates.

A central element in connection with AI and autonomous systems is the role of training and preparation. While AI can help in operations to shorten decision cycles and increase operational speed, that time saving is generally "purchased" beforehand – through thorough training, systematic testing and iterative adaptation to ensure reliable and responsible use. As was emphasised in the panel, the effective use of AI-supported systems requires months, if not years, of intensive preparation. Systems must be trained in realistic scenarios, their performance tested under different conditions, and their limitations continually understood. Only then can it be ensured that they function reliably in operations and that their results are interpreted correctly.

The war in Ukraine once again provides a particularly illustrative example: in the run-up to the so-called Operation "Spider Web," AI-enabled drone systems were specifically trained to identify particular Russian strategic bombers. To do so, developers used, among other things, real reference objects, such as aircraft exhibited in museums, in order to train visual recognition models. This tailor-made, context-specific training enabled the systems to operate reliably even under difficult conditions. Even when no communication link was available, they were able to recognise and pursue their targets autonomously. The example makes clear that the actual performance of AI in operations is inseparably linked to the quality of its data and training. Operational speed arises not primarily from spontaneous automation, but from prior and longer-term investment in data, modelling and practical, iterative testing.

Drawing on operational experience, particularly from Ukraine, the discussion concluded that compliance with IHL does not necessarily hinder military effectiveness and can even provide strategic advantages, especially in a transparent battlefield environment. Colonel Inna Zavorotko underscored in particular the importance of conducting hostilities in full compliance with IHL, describing IHL as a "golden tool" for enabling a return to normal life after conflict. Ultimately, while AI increases the complexity of applying existing rules, it does not alter the fundamental principles of IHL. Rather, it reinforces the need for careful governance, continuous oversight and a balanced approach that aligns military effectiveness with humanitarian protection.

Ensuring compliance with IHL requires a comprehensive lifecycle approach, from design and testing to deployment and continuous adaptation. Legal reviews under Additional Protocol I to the Geneva Conventions,

particularly Article 36, remain crucial but must evolve into ongoing processes given the dynamic nature of machine learning systems. The panel also underscored governance challenges, especially the growing influence of private technology companies in AI development. It emphasised that states must retain control and ensure that military applications of AI align with legal and ethical standards. Bridging the gap between legal, technical and military communities was seen as critical, requiring shared understanding, integration of IHL principles into system design and enhanced training.

Maritime warfare in a digital age

Panel 5, chaired by **Prof. (em.) Dr. Wolff Heintschel von Heinegg** (President of the Society & Europa-Universität Viadrina Frankfurt (Oder) and featuring **Prof. Dr. Anna Petrig** (Chair of International and Public Law, University of Basel) and **Abby Zeith** (Legal Advisor, International Committee of the Red Cross) explored how technological developments are reshaping the legal framework governing naval operations, particularly with regard to critical infrastructure such as undersea cables.

As outlined by Prof. Dr. Anna Petrig in her introductory statement and supported by the other panellists, the existing framework of naval warfare law is insufficiently equipped to safeguard vital infrastructures such as underwater communication cables in the digital age. First, submarine communication cables are of extraordinary importance for modern life. They carry around 99 per cent of global Internet traffic, form the backbone of the Internet, and are thus indispensable for civilian life as well as for military operations. Second, there is a high probability that such cables would be targeted in an armed conflict at sea. Cable cutting has a long history in naval warfare and is technically feasible, comparatively easy and difficult to detect. Third, the scale of harm resulting from damage to such cables would likely be far greater today than in earlier wars because their destruction could seriously disrupt communications, finance, health services and other essential systems. Fourth, the legal framework of naval warfare does not adequately reflect this new reality. The legal regulation of communication cables in armed conflict is highly incomplete. While peacetime protection of cables and pipelines has recently attracted greater attention, the wartime framework remains even less developed. Treaty law contains almost no relevant provisions. The only exception, Article 54 of the 1907 Hague Convention IV, is narrowly limited to outdated submarine telegraph cables and acts on land. Otherwise, neither treaty law nor customary international law provides a special regime for communication cables. In the absence of hard law, attention shifts to soft law, in particular to Rule 37 of the San Remo Manual, which is replicated, with some nuances, in Rule 69 of the Oslo Manual. Yet this rule is also unsatisfactory. First, it treats all cables and pipelines alike, although pipelines, power cables and fibre-optic communication cables differ significantly in function and importance. Second, it rests on an outdated understanding of communication cables as bipolar point-to-point systems, whereas modern submarine cables form part of a dense global network in which data takes unpredictable routes. Third, the geographical scope of this single rule is limited and only covers some parts of the ocean. Fourth, its precise meaning remains contested and, fifth, it does not sufficiently reflect the centrality of communication cables in the digital age. However, the absence of a special regime does not mean that belligerents are free to target cables without restraint. Rather, the general targeting rules of international humanitarian law continue to apply, especially the principles of distinction, proportionality and precaution. But their application raises difficult questions, including whether cyber operations qualify as attacks, when a cable amounts to a military objective, and how proportionality should be assessed where civilian harm may consist in indirect, second-order effects.

The panel concluded that the current law is not fit for the digital age. It therefore calls for renewed discussion of possible regulatory options, including an outright prohibition on attacking communication cables, a higher threshold such as “absolute military necessity”, additional steps after the proportionality assessment, and additional warning or mitigation requirements.

Cloud and Quantum computing in armed conflict

Panel 6, chaired by **Ann Väljataga** (International Law Researcher, NATO Cooperative Cyber Defence Centre of Excellence) and featuring Major **David Quayat** (Directorate of Cyber Operations Law, Office of the Judge Advocate General, Canada) and **Dr. Heike Riel** (IBM Fellow, Head of Science and

Technology, Lead of IBM Research Quantum EMEA) examined how emerging digital infrastructures are reshaping both warfare and its legal framework. The discussion emphasised the growing strategic importance of cloud and quantum computing systems, which underpin both civilian and military operations and are often operated by private actors across multiple jurisdictions. This creates complex legal challenges related to sovereignty, attribution, and the classification of such infrastructure as potential military objectives. A central focus was the transformative impact of quantum computing. Once sufficiently advanced, quantum technologies could break current encryption systems that protect military communications, critical infrastructure and financial networks. This creates an urgent need for a transition to quantum-resistant cryptography, as data intercepted today could be decrypted in the future. Ensuring that systems become "quantum safe" was therefore identified as a key strategic priority. Looking ahead, quantum technologies are likely to have far-reaching implications for the conduct of hostilities. They may undermine confidentiality, enhance detection capabilities through advanced sensing and accelerate decision-making processes, particularly when combined with artificial intelligence. At the same time, they could significantly expand both offensive and defensive cyber capabilities. These developments will further complicate the application of IHL, particularly with regard to attribution, distinction, proportionality and precaution as the interconnection between civilian and military systems deepens.

Overall, the panel concluded that quantum and cloud technologies are not only transforming the technical environment of conflict but also exposing systemic vulnerabilities, requiring early adaptation, stronger cooperation between states and private actors and continued efforts to clarify and apply existing legal frameworks in a rapidly evolving technological landscape.

In closing, the conference reaffirmed that although emerging technologies are rapidly transforming warfare, the *core principles of IHL remain unchanged*. Participants stressed that IHL is not only a legal framework but also a strategic and moral compass, essential for maintaining legitimacy, trust and long-term stability, particularly in an increasingly transparent battlefield environment. A central conclusion was that *human responsibility must remain at the core of decision-making*: while technologies such as AI can support operations, legal judgment and accountability cannot be delegated. Ensuring compliance with IHL therefore requires closer cooperation between legal, military and technical communities, as well as adaptive governance approaches. At the same time, new challenges, such as quantum computing, underscore the need for proactive adaptation. Ultimately, the conference highlighted that *safeguarding IHL is a collective responsibility* and that its enduring strength depends on the continued commitment of those who uphold it, ensuring the protection of human dignity even in times of profound technological change. ◆

Endnotes

1 This article draws on discussions held in Lucerne, Switzerland, in March 2026 during an international conference organised by the International Society for Military Law and the Law of War (ISMLLW) with the support of the Federal Department of Defence, Civil Protection and Sport (DDPS) and the Swiss Group of the International Society for Military Law and the Law of War. The author writes in his personal capacity; the contents do not necessarily reflect the positions of the institutions or states to which the contributors are associated. The author thanks Prof. Anna Petrig for her substantive contribution regarding the protection of underwater communication cables.