

Guide for operationalizing Article 36

Implementing legal review mechanisms for
new weapons, means, and methods of warfare



About DCAF – Geneva Centre for Security Sector Governance

DCAF – Geneva Centre for Security Sector Governance is dedicated to improving the security of states and their people within a framework of democratic governance, the rule of law, respect for human rights, and gender equality. Since its founding in 2000, DCAF has contributed to making peace and development more sustainable by assisting partner states, and international actors supporting these states, to improve the governance of their security sector through inclusive and participatory reforms. It creates innovative knowledge products, promotes norms and good practices, provides legal and policy advice, and supports capacity building of both state and non-state security sector stakeholders. DCAF's Foundation Council members represent over 40 countries and the Canton of Geneva. Active in over 60 countries, DCAF is internationally recognized as one of the world's leading centres of excellence for security sector governance (SSG) and security sector reform (SSR). DCAF is guided by the principles of neutrality, impartiality, local ownership, inclusive participation, and gender equality. For more information visit www.dcaf.ch and follow us on social media.



About the Responsible by Design Institute

The Responsible by Design Institute is a not-for-profit organization dedicated to promoting the responsible design, development, and governance of emerging military technologies, including artificial intelligence (AI) enhanced and autonomous weapon systems.

Acknowledgements

This Guide benefited greatly from the expertise and generosity of those who reviewed earlier drafts and shared their insights. Particular thanks are due to Damian Copeland (Responsible by Design Institute) and Stuart Casey-Maslen, whose expertise in international humanitarian law, weapons law, and national review practice shaped both the structure and the substance of the text. Patrick Masshardt and Philippe Lejeune contributed practitioner experience and insights drawn from current multilateral discussions concerning emerging technologies. The International Law Division of the Legal Support Department of the Ministry of Defence of Ukraine generously shared its national practice and gave detailed comments, ensuring that the Guide is grounded in implementation realities. Megan Bastick provided invaluable guidance on the integration of gender perspectives throughout the Guide, while Line Barabant and Anaïs Fiault contributed expertise on the business and security dimensions of capability development, including the role of industry and the governance of private military and security companies.

Special thanks are owed to Grazvydas Jasutis, whose support and guidance accompanied this project from its inception through to completion, and whose comments on the Guide's practitioner focus helped ensure that its methodology and tools remain practical and usable in day-to-day review work.

DCAF would like to thank the Federal Department of Defence, Civil Protection and Sport (DDPS) of the Swiss Confederation for its generous support in making this publication possible.

Author: Rebecca Petra Mikova

Reviewers: Line Barabant, Megan Bastick, Stuart Casey-Maslen, Damian Copeland, Anaïs Fiault, Grazvydas Jasutis, Philippe Lejeune, Patrick Masshardt, and the International Law Division of the Legal Support Department of the Ministry of Defence of Ukraine

Copy-editor: Alessandra Allen

Design and layout: Nadia Joubert

Cover photo: © dsheremeta / Adobe Stock

ISBN: 978-92-9222-836-1

Publisher

DCAF – Geneva Centre for Security Sector Governance
Maison de la Paix
Chemin Eugène-Rigot 2E
1202 Geneva, Switzerland



+41 22 730 94 00



info@dcaf.ch



www.dcaf.ch



Contents

List of abbreviations	4
Foreword	5
Introduction	7
1. Article 36 legal review obligation	11
Nature and function of the obligation	11
Scope of the obligation	12
Temporal dimension: 'Before use' and continuing obligation	13
Applicable legal framework	13
Standard of assessment	17
Responsibility of the reviewing state	18
2. Why legal reviews matter	19
3. Contemporary challenges	21
Establishing a national legal review mechanism	23
4. Legal and policy foundations	23
National implementation instruments	24
Core elements and design of implementing instruments	30
5. Institutional design of review mechanisms	33
Institutional embedding of the review function	33
Composition of review bodies	37
Roles and responsibilities	40
6. Integration into defence procurement processes and capability life cycle	42
7. Legal effect and outcomes of reviews	48
From conditional approval to operational practice	49
8. Governance, transparency, and system management	52
Record-keeping	52
Transparency and information sharing	53
Capacity building	56
Managing resource constraints	58

How to conduct an Article 36 legal review 65

9. Preliminary identification	68
Step 1: Preliminary assessment to establish whether the review is required	68
Step 2: Define the object under review and intended use	69
Step 3: Collect and verify the evidentiary basis	72
10. Legal assessment	74
Step 4: Assess specific prohibitions and restrictions	74
Step 5: Assess general prohibitions and restrictions	76
Step 6: Apply a functional review approach where appropriate	83
Step 7: Determine the outcome of the review	88
Step 8: Document the review and communicate implementation requirements	89

Practical tools for legal reviewers and committee members 91

11. Review process tools	91
Review trigger and screening matrix	92
Model review workflow	93
12. Reviewer analytical tools	95
Technical information request template	95
Core legal review checklist	109
Specific prohibitions and restrictions: Chronological reference table	117
Functional assessment matrix for AI-enabled, autonomous, cyber, software-defined, or multifunction systems	119
Operational context assessment tool	123
13. Institutional support tools	126
Review report template	126
Reassessment trigger matrix	129
14. Training framework	134

Annexes 145

Annex 1: Worked example completed review report (illustrative)	145
Annex 2: Example training programme – two-day practitioner course (illustrative)	148

List of abbreviations

AI	Artificial intelligence
AIRCW	Advisory Committee on International Law and Conventional Arms Use
CCW	Convention on Certain Conventional Weapons
CEJ	Commission d'évaluation juridique
DCDC	UK Ministry of Defence, Development, Concepts and Doctrine Centre
DDPS	Swiss Federal Department of Defence, Civil Protection and Sport
EW	Electronic warfare
GGE LAWS	UN Group of Governmental Experts on Lethal Autonomous Weapons Systems
ICRC	International Committee of the Red Cross
IHL	International humanitarian law
IIHL	International Institute of Humanitarian Law
ROE	Rules of engagement
SOP	Standard operating procedures



Foreword

Article 36 of Additional Protocol I asks something of states that sounds straightforward: before a new weapon, means, or method of warfare is studied, developed, acquired, or adopted, they must determine whether its use would be prohibited by international law. Building a national system that can do this reliably is a good deal harder. It requires institutions with a clear mandate and the resources to carry it out. It requires reviews to form part of how a state plans and buys its military capabilities, rather than being added at the end of that process. And it requires access to technical, operational, and medical expertise; records that remain usable as staff change and software is updated; and the ability to look at a capability again whenever it is modified during its years in service. These practical, institutional questions are what this Guide sets out to address.

DCAF – Geneva Centre for Security Sector Governance brings a particular perspective to the legal review of weapons. Article 36 is an obligation under international humanitarian law, but successful implementation also depends on how the security sector is governed. It concerns how responsibility is shared within defence institutions, how procurement is managed, what role private industry plays, how oversight and accountability are exercised, and how the officials involved are trained. Good security sector governance means, among other things, that armed forces are given only those means they can lawfully use, and that the processes ensuring this are properly established, adequately resourced, and open to scrutiny. A well-functioning Article 36 mechanism is one sign of a well-governed defence sector.

The Guide has been written with practitioners in mind. It describes the core elements of effective national mechanisms, drawing on the experience of states that already have them, and sets out a step-by-step method for conducting reviews. It also provides practical instruments – including screening matrices, information request templates, legal checklists, functional and operational assessment tools, reporting formats, reassessment triggers, and a modular training framework – that states can adapt to their own structures and procedures. Particular attention is given to the hardest capabilities to review using traditional approaches – AI-enabled, autonomous, cyber, and software-defined systems, whose legally relevant features may continue to change long after they enter service.

The Guide builds on the existing body of work on Article 36, and above all on the ICRC's 2006 'Guide to the Legal Review of New Weapons, Means and Methods of Warfare', which remains the authoritative reference on what the legal assessment must cover. It adds to that foundation by focusing on the institutions, procedures, and skills that states need in order to carry out the assessment in practice. It is offered in the belief that the humanitarian purpose of Article 36 is served not only by a clear understanding of the law, but also by institutions capable of applying it.

Darko Stančić

Head of Europe and Asia
DCAF – Geneva Centre for Security Sector Governance



Introduction

The development, acquisition, and use of new military technologies require states to assess how rules of international law apply to complex, evolving, and often software-dependent capabilities. Article 36 of Additional Protocol I provides the central legal mechanism for this assessment. It provides that '[i]n the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party'. This obligation has existed since the protocol's adoption in 1977. What has changed, however, is the technological and institutional context in which it must be applied. Capabilities are increasingly developed and acquired through complex procurement ecosystems involving defence institutions, private industry, software developers, research bodies, and multinational partners – often via iterative development cycles rather than linear acquisition processes. Contemporary capabilities may involve artificial intelligence (AI), autonomous functions, cyber effects, networked systems, data-driven decision-support tools, modular payloads, and software updates that alter performance over time. These characteristics make legal reviews more technically demanding, more dependent on interdisciplinary evidence, and more closely linked to procurement, testing, operational planning, and life-cycle management.

This Guide is intended to support states and defence institutions in implementing Article 36 through effective national review mechanisms. It does not, however, propose a single institutional model; international law requires a reliable determination of legality, but does not specify whether this must be conducted by an individual reviewer, legal office, commission, committee, or other review body. States retain discretion to design mechanisms that reflect their constitutional systems, defence structures, procurement processes, and operational needs. The purpose of this Guide is therefore to identify core elements of effective implementation and to provide practical tools that can be adapted to different national contexts. The Guide proceeds from the premise that an Article 36 review is more than simply a formal legal step at the end of the procurement process. To be effective, the review should be integrated into the full capability life cycle, from early concept and development through to acquisition, testing, introduction into service, modification, operational use, and reassessment. This is particularly important where the legality of a capability depends not only on its physical characteristics, but also on its software configuration, data inputs, operational environment, human-machine interaction, or conditions of use.

The Guide is intended primarily for legal advisers and other officials responsible for conducting, supporting, or strengthening national Article 36 review mechanisms. It may also be useful for procurement authorities, capability managers, operational planners, technical experts, testing authorities, policy officials, and trainers who support or interact with the legal review process. While the legal determination must remain with the reviewing state, an effective review depends on the structured participation of actors capable of providing the technical, operational, medical, environmental, cyber, AI, data, or other expertise required for a legally reliable assessment.

The Guide is organized into four main parts. The first part describes the obligation under Article 36, explains why legal reviews matter, and identifies contemporary challenges affecting implementation. The second part examines the establishment of national legal review mechanisms, including legal and policy foundations, institutional design, life-cycle integration, review outcomes, governance, transparency, and capacity building. The third part proposes a structured methodology for conducting Article 36 reviews, from preliminary screening and evidentiary collection through to substantive legal assessment, functional assessment, review outcomes, and implementation requirements. The final part provides practical tools for reviewers and review bodies, including screening, information collection, legal analysis, functional assessment, operational context assessment, reporting, reassessment, and training tools.

8

The tools included in this Guide are not intended to replace national procedures or create new legal obligations. Where states already have review forms, checklists, reporting templates, or decision-making processes, those instruments should remain the primary basis for national practice. The tools provided here may nevertheless assist states in developing, updating, or supplementing their own mechanisms, particularly where new technologies raise questions not fully addressed by existing procedures.

The Guide draws on several sources. These include the text and drafting history of Additional Protocol I; the International Committee of the Red Cross (ICRC) 2006 'Guide to the Legal Review of New Weapons, Means and Methods of Warfare'; publicly available national legislation, directives, military manuals, policy documents, and state statements; and expert reports, academic literature, and materials developed in recent discussions on autonomous weapons, AI-enabled military systems, cyber capabilities, and responsible military innovation. It also reflects insights from expert consultations, interviews with national practitioners, observations of review-related processes, and practical experience supporting the development of Article 36 review mechanisms.

The Guide does not claim to provide an exhaustive account of all state practice, much of which remains confidential or only partially public. Nor does it seek to resolve every contested question concerning the legality of particular technologies. Instead, it has a more practical aim: to assist states in building review systems that are legally grounded, institutionally workable, technically informed, and capable

of producing reliable determinations before new weapons, means, or methods of warfare are developed, acquired, adopted, or used.

The Guide's approach to unsettled questions of law is also worth clarifying. The Guide distinguishes between the requirements of Article 36 under existing law and what constitutes good implementation practice. Its statements of the legal baseline reflect existing law, anchored in the text and drafting history of Additional Protocol I and the ICRC's 2006 guide. Its operational recommendations, by contrast, go further: they not only describe how states with effective review systems structure their mechanisms, but also, in places, recommend measures that go beyond what the obligation, strictly construed, requires. This is intentional. A guide confined to the bare minimum would offer little to practitioners tasked with reviewing capabilities that the 1977 drafters could not have foreseen; however, readers should not mistake a recommendation of good practice for a binding obligation, and the Guide maintains this distinction throughout.

It is important to acknowledge three positions taken in this Guide, as they involve questions on which legal opinion is divided.

01

First, regarding the **relationship between weapons law and targeting law**, the classical view holds that the Article 36 review assesses a capability against the rules governing weapons themselves, while the rules on distinction, proportionality, and precautions apply to those who plan and decide on attacks. This Guide adopts the functional approach for systems that perform tasks governed by targeting rules – such as target identification, selection, or engagement recommendation – on the grounds that a review that ignores those functions cannot reliably determine whether the capability is able to be used lawfully; it acknowledges, however, that the extent to which Article 36 itself compels this remains debated.

02

Second, regarding **AI-enabled decision-support systems**, whether tools that inform, rather than apply, force fall within 'means or methods of warfare' is not settled. The Guide adopts an inclusive screening approach, under which such systems are assessed to determine whether they constitute or form part of a means or method of warfare, and recommends a review where their outputs foreseeably shape use-of-force decisions – a precautionary position presented as good practice rather than as an uncontested reading of the provision's scope.

03 Third, regarding the **use of reviews conducted by other states**, the traditional position, affirmed by this Guide, is that the Article 36 determination is non-transferable – another state's review cannot substitute for the reviewing state's own assessment, since obligations, interpretations, and intended uses differ. Where this Guide departs from conventional treatment is in what follows from this rule. Insisting on the principle while ignoring the realities of multinational procurement and interoperability – in which many states, particularly smaller ones, acquire capabilities already reviewed by allies and lack the resources to reconstruct every assessment from first principles – has in practice often resulted in no reviews at all, rather than more. The Guide therefore takes a deliberately pragmatic approach: it not only distinguishes the legal determination, which must remain national, from the evidentiary and analytical inputs that may legitimately inform this, but also identifies structured ways in which prior reviews, testing data, technical assessments, and partner methodologies can be used to make a national review feasible and proportionate rather than duplicative. This is presented as a means of enabling compliance, not diluting it.

For ease of reading, this Guide uses the term **'capability'** as shorthand for **'new weapon, means, or method of warfare'** within the meaning of Article 36, unless the context indicates otherwise. Likewise, references to 'new technologies' or 'emerging technologies' are descriptive: they do not alter the legal scope of Article 36, which attaches to weapons, means, and methods of warfare – not to the technologies themselves. Where a technology does not constitute, or form part of, a weapon, means, or method of warfare, it falls outside the scope of the obligation, although other legal assessment requirements may apply.

1. Article 36 legal review obligation

Nature and function of the obligation

Article 36 of Additional Protocol I requires that, ‘in the study, development, acquisition or adoption of a new weapon, means or method of warfare’, a state must determine whether its employment would, in some or all circumstances, be prohibited under international law.¹ A national determination under Article 36 does not create a new substantive prohibition against specific weapons or weapon types. Rather, it provides a concrete procedural expression of the broader duty to comply with international humanitarian law (IHL), as reflected in Common Article 1 of the Geneva Conventions, by requiring states to assess legality before using a capability in armed conflict.² In this sense, Article 36 functions as a preventive compliance mechanism, designed to ensure that unlawful capabilities do not enter operational use. The obligation is therefore best understood as a forward-looking legality assessment rather than a retrospective accountability mechanism. Article 36 does not itself prescribe the consequences that follow from a negative determination; instead, it is for each state to give effect to the determination within its national procurement and decision-making processes.

A central feature of Article 36 is that it imposes a substantive obligation of result, not a prescribed procedure.³ International law defines what must be assessed – namely compliance with IHL and other applicable rules – but does not prescribe how the review must be conducted institutionally or procedurally. States therefore retain discretion as to:

- institutional design (such as committee vs. single reviewer);
- methodology; and
- internal processes and documentation.

This discretion is not, however, unlimited. As a matter of general international law, and consistent with the principle of good faith in performing treaty obligations,⁴ the review must be capable of producing a legally reliable determination. A state cannot

¹ Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), adopted 8 June 1977, entered into force 7 December 1978, 1125 UNTS 3, art. 36.

² Common Article 1 refers to Article 1 of all four Geneva Conventions of 12 August 1949: Geneva Convention I (Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field), 75 UNTS 31; Geneva Convention II (Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea), 75 UNTS 85; Geneva Convention III (Treatment of Prisoners of War), 75 UNTS 135; Geneva Convention IV (Protection of Civilian Persons in Time of War), 75 UNTS 287. It establishes that the High Contracting Parties ‘undertake to respect and to ensure respect for the present Convention[s] in all circumstances’. In the context of weapons reviews, this imposes on states a binding, continuous obligation to ensure compliance, requiring proactive measures – such as Article 36 reviews – to ensure that any weapon, means, or method of warfare developed or acquired can be utilized lawfully under IHL before it ever enters operational deployment.

³ ICRC (International Committee of the Red Cross), ‘A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977’ (Geneva: ICRC, 2006), pp. 3, 5, 20.

⁴ See Vienna Convention on the Law of Treaties, adopted 23 May 1969, entered into force 27 January 1980, 1155 UNTS 331, art. 26.

invoke procedural discretion to justify a review process that is structurally incapable of properly assessing the legality of a weapon, means, or method of warfare.

The obligation is procedural in nature. Failure to conduct a review constitutes a breach of Article 36, but does not, of itself, render the weapon, means, or method of warfare concerned unlawful: legality is determined by the substantive rules applicable to the capability and its employment. Conversely, the conduct of a review confers no immunity – a favourable national determination does not affect the operation of the substantive rules by which the state is bound.

Scope of the obligation

The obligation applies broadly to weapons, means, and methods of warfare. These terms must be interpreted functionally rather than formally. The decisive question is whether the intended – or reasonably foreseeable – use of the capability is **to contribute to the application of force in armed conflict**.⁵ This includes:

- traditional kinetic weapons;
- non-kinetic systems (such as cyber capabilities whose foreseeable use would produce effects amounting to an application of force); and
- certain decision-support or AI-enabled systems, where they materially shape the application of force.

It also extends beyond entirely ‘new’ technologies to include:

- newly acquired systems;
- modified systems; and
- existing systems used in a new operational manner.

For the purposes of the review, the operative terms may be understood as follows. The term ‘weapons’ encompasses arms, munitions, weapon systems, and other devices designed, intended, or adapted to injure, kill, disable, or incapacitate persons, or to damage or destroy objects. ‘Means of warfare’ refers to the broader category of weapons, weapon systems, platforms, and associated materiel used in the conduct of hostilities. ‘Methods of warfare’ refers to the ways in which capabilities are employed – the tactics, techniques, and procedures by which hostilities are conducted. A capability is ‘new’ for the reviewing state where it has not previously been the subject of that state’s review, including where an existing

⁵ See Yves Sandoz, Christophe Swinarski, and Bruno Zimmermann, eds., ‘Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949’ (ICRC, Geneva, 1987), para. 1402, which notes that ‘the words “methods and means” include weapons in the widest sense, as well as the way in which they are used’, establishing that a weapon cannot be legally divorced from its operational method of deployment. See also ICRC, ‘A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977’ (Geneva: ICRC, 2006), p. 7, fn. 1, p. 9, which explicitly states that to ‘lighten the text’ and avoid burdensome or overly restrictive definitions, the term ‘weapons’ is used as universal shorthand for any tool or capability designed to be used in hostilities. The drafting history demonstrates that the tripartite formulation (‘weapons, means, or methods’) was intended to form a seamless, all-inclusive net rather than separate technical categories, meaning the threshold trigger for a review is simply whether a capability plays a meaningful role in the application of force.

capability is newly acquired, materially modified, or intended for a new operational use. These working formulations reflect the ICRC's 2006 guide and national guidance; states may refine them in national instruments, and the decisive question remains the functional one set out above.

Operational implication: The scope of the legal review must encompass all capabilities that materially shape the application of force, tracking them across their entire life cycle.

Temporal dimension: 'Before use' and continuing obligation

Article 36 requires that legality be determined before the capability is used in armed conflict. This establishes a strict temporal requirement: a new weapon, means, or method of warfare should not be employed unless its compliance with the reviewing state's applicable international law obligations has been determined. In addition, the obligation has a **continuing dimension**. States must reassess legality where:

- the capability is materially modified, in a manner capable of affecting its legal assessment;
- new information becomes available (such as operational performance data revealing unanticipated effects or reliability issues);
- the applicable legal framework evolves; or
- the method of use has been changed from that originally assessed.

Operational implication: Legal review is not a one-time certification, but an iterative process integrated into the life cycle of the capability.

Applicable legal framework

The legal review must assess compliance with all applicable international law, including:

A. Core IHL principles (customary and treaty law):

1. prohibition of superfluous injury or unnecessary suffering;
2. prohibition of inherently indiscriminate weapons;
3. rules on distinction, proportionality, and precautions in attack; and
4. environmental protection (widespread, long-term, severe damage).

B. Specific prohibitions and restrictions applicable to the reviewing state, as well as weapon-specific treaty and customary rules (including under disarmament law), in chronological order:

1. St Petersburg Declaration (1868): prohibits the use of explosive or inflammable projectiles below 400 g; its preamble articulates the foundational principle that weapons that uselessly aggravate the sufferings of disabled men exceed the legitimate object of war;
2. Hague Declaration (IV,3) (1899): prohibits the use of bullets that expand or flatten easily in the human body (dum-dum bullets) as a means of warfare;
3. Hague Regulations (1907), Article 23(a): prohibits the use of poison and poisoned weapons (also customary law);
4. Geneva Gas Protocol (1925): prohibits the use in war of asphyxiating, poisonous, or other gases, and of bacteriological methods of warfare;
5. Biological Weapons Convention (1972): prohibits the development, production, acquisition, transfer, stockpiling, and retention of biological and toxin weapons at all times;
6. Environmental Modification (ENMOD) Convention (1976): prohibits military or any other hostile use of environmental modification techniques having widespread, long-lasting, or severe effects;
7. Convention on Certain Conventional Weapons (CCW) (1980) and its Protocols: design-based and use-based constraints on non-detectable fragments (Protocol I, 1980), mines and booby traps (Protocol II, 1980, amended 1996), incendiary weapons (Protocol III, 1980), and blinding laser weapons (Protocol IV, 1995);
8. Chemical Weapons Convention (1993): prohibits the development, production, stockpiling, transfer, and use of chemical weapons at all times;
9. Anti-Personnel Mine Ban Convention (1997): prohibits the use, development, production, stockpiling, and transfer of anti-personnel mines at all times;
10. Convention on Cluster Munitions (2008): prohibits the use, development, production, stockpiling, and transfer of cluster munitions at all times; and
11. customary international law prohibitions and restrictions on specific weapons, as reflected in Rules 70-86 of the ICRC Customary IHL Study, which bind all states irrespective of treaty ratification.

C. Other applicable international law, including where relevant:

1. international human rights law;
2. international criminal law, insofar as weapons-related war crimes may inform the assessment; and
3. other regimes applicable to the capability's intended domain of use, such as the law of the sea, air law, or outer space law.

Box 1: Human rights law

International human rights law is not the primary focus of an Article 36 review. Article 36 concerns new weapons, means, and methods of warfare, with the core assessment typically conducted under IHL, including specific weapons treaties and the general rules governing the conduct of hostilities. Human rights law may nevertheless be relevant where a capability falling within the scope of Article 36 is also intended for use, or reasonably foreseeable use, in contexts where human rights obligations regulate the conduct of state agents.⁶ This may be particularly important for capabilities with both combat and law enforcement functions, or for systems used by armed forces in occupation, detention, internment, border security, facility guarding, crowd control, peace operations, or other situations in which state agents exercise authority or control over individuals.

The relevance of human rights law should be understood carefully. In most cases, the question is not whether human rights law prohibits the weapon, means, or method of warfare as such. Rather, the reviewing authority should consider whether the capability's intended or foreseeable uses, functions, or effects may require additional safeguards, restrictions, operational guidance, or a separate assessment under applicable human rights standards. This reflects the wording of Article 36 itself, which requires a review not only under Additional Protocol I, but also under 'any other rule of international law applicable' to the reviewing state.

For example, a biometric or AI-enabled surveillance function integrated into a military capability may fall within an Article 36 review if it materially supports targeting, attack planning, force protection, or another function connected to the conduct of hostilities. Its use may be compatible with IHL if it supports the lawful identification of military objectives and is subject to appropriate reliability, verification, and precautionary safeguards. The same function, however, may also engage human rights law when it collects, stores, analyses, or shares personal data about individuals, particularly in occupation, detention, border security, internal security, or other contexts involving state authority or control. In such circumstances, inadequate legal basis, excessive retention, indiscriminate collection, discriminatory profiling, or sharing of personal data without safeguards may raise issues concerning privacy and non-discrimination rights.

Similarly, a cyber capability that is reviewed as a means or method of warfare may raise human rights considerations if its foreseeable effects extend beyond the immediate conduct of hostilities. For instance, a cyber operation

⁶ See Casey-Maslen, Stuart, Neil Corney, and Abi Dymond-Bass, 'The Review of Weapons under International Humanitarian Law and Human Rights Law', in Stuart Casey-Maslen, ed., 'Weapons under International Human Rights Law' (Cambridge: Cambridge University Press, 2014), pp. 411–47, pp. 411–12 (in particular), 420–21.

that deletes, corrupts, or denies access to hospital data would first have to be assessed under IHL rules protecting medical services, civilian objects, proportionality, and precautions. Depending on the context, it may also raise human rights concerns, including those related to the rights to life and health, particularly when the affected persons are under the authority or control of the state or the operation is conducted outside active hostilities.

Where a capability is not materially connected to the conduct of hostilities, Article 36 may not apply as a strict treaty obligation. This may be the case for certain surveillance, data-processing, detention-management, border-control, or law enforcement technologies procured or used by military institutions but not intended as weapons, means, or methods of warfare. Such capabilities may nevertheless require legal assessment under human rights law, domestic law, data-protection law, operational law, or procurement rules. In practice, where no separate review mechanism exists, the national Article 36 review authority may be well placed to identify the need to coordinate or conduct such broader legality assessments, provided that the distinction between the Article 36 review and other forms of legal assessment is clearly recorded. This broader legality perspective is consistent with the wording and drafting history of Article 36, whose final text refers not only to Additional Protocol I but to ‘any other rule of international law applicable’ to the reviewing state.⁷

Where human rights issues are identified, the review should distinguish clearly between the Article 36 assessment of the capability as a weapon, means, or method of warfare and any additional human rights assessment required by national law, operational law, or other applicable international obligations. The Article 36 review report may record the need for additional safeguards, restrictions, operational guidance, or separate legal assessments, but it should not treat human rights law as a substitute for the IHL framework applicable to the conduct of hostilities.

The reference in Article 36 to ‘any other rule of international law applicable’ confirms that the legal review is not limited to the provisions of Additional Protocol I alone. The reviewing authority should also consider other treaty and customary rules that are binding upon the state, including specific weapons treaties, relevant disarmament obligations, customary IHL, and, where applicable, other bodies of international law such as international human rights law.⁸ This broader formulation is also relevant to the Martens Clause, reflected in Article 1(2) of Additional

⁷ See Casey-Maslen, Stuart, Neil Corney, and Abi Dymond-Bass, ‘The Review of Weapons under International Humanitarian Law and Human Rights Law’, in Stuart Casey-Maslen, ed., ‘Weapons under International Human Rights Law’ (Cambridge: Cambridge University Press, 2014), pp. 411-47, pp. 411-12, fn. 3, which notes that the final wording of Article 36 was broader than the earlier Dutch, Norwegian, and Swedish proposal, which referred to rules applicable in armed conflict. See also Lawand, Kathleen, ‘Reviewing the Legality of New Weapons, Means and Methods of Warfare’, *International Review of the Red Cross*, Vol. 88: No. 864, December 2006, pp. 925-30.

⁸ Sandoz, Yves, Christophe Swinarski, and Bruno Zimmermann, eds., ‘Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949’ (Geneva: ICRC/Martinus Nijhoff, 1987), para. 1472.

Protocol I, which may assist reviewers where a new weapon, means, or method of warfare raises concerns not fully addressed by specific treaty rules.⁹ (The role and legal effect of the Martens Clause in review practice are addressed in Box 10 – Step 5, Part 3.) The review should therefore remain grounded in binding legal obligations, while also identifying any residual concerns requiring safeguards, restrictions, policy considerations, or further assessment.

Operational implication: Review frameworks should ensure strong expertise in weapons law and IHL, while enabling access to additional legal expertise – including human rights, disarmament, environmental, data-protection, cyber, or procurement law – where the capability or its foreseeable use raises issues under those regimes.

Standard of assessment

The legal assessment is based on the normal or expected use of the capability and a reasonable foreseeability standard. This excludes purely hypothetical misuse, but includes foreseeable patterns of use based on the design, doctrine, and operational context. In many cases, weapons are not found to be unlawful per se. Their legality depends on how they are used and whether their effects can be controlled in accordance with IHL.¹⁰

The general prohibitions applicable at this stage – notably the prohibition of weapons which cause superfluous injury or unnecessary suffering and the prohibition of inherently indiscriminate weapons – set deliberately high thresholds, and findings of per se unlawfulness are correspondingly rare. The standards of assessment for these prohibitions, and the evidence needed to apply them, are addressed in detail in Step 5 of Part 3.

Operational implication: Legal reviews must integrate:

- technical data;
- operational doctrine; and
- realistic use scenarios.

⁹ ICRC, *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977* (Geneva: ICRC, 2006, p. 17.)

¹⁰ German practice articulates this expressly as a scenario-based test, under Zentrale Dienstvorschrift A-2146/1, Prüfung neuer Waffen, Mittel und Methoden der Kriegführung (Review of New Weapons, Means and Methods of Warfare) – Federal Ministry of Defence, nos. 602-603. The question of whether a new weapon, means, or method of warfare should be introduced is ultimately answered by asking whether there are sufficient conceivable scenarios in which a militarily meaningful and operationally feasible employment can be assessed as lawful. The regulation concludes that the legal review will frequently be unable to rest on technical and medical descriptions alone and must incorporate military-operational analysis (text of version 1 of 13 June 2016, published in Deutscher Bundestag, Drucksache 18/9191, annex; the operative version 2 of 10 January 2019 is not publicly available).

Responsibility of the reviewing state

The obligation under Article 36 is non-transferable. A state:

- must conduct its own legal review, even when acquiring weapons from another state; and
- cannot rely exclusively on prior reviews conducted by others.

This partly stems from the fact that states are not bound by identical obligations: treaty ratifications differ, and national law may define the scope of the review – including what is understood as a means of warfare – in different terms. An assessment conducted elsewhere therefore cannot substitute for a determination based on the reviewing state's own obligations, interpretations, doctrine, and intended use.

A state may take account of reviews, technical assessments, testing data, interoperability standards, or methodological guidance developed by weapon manufacturers, allies, or multinational partners. Such cooperation may be particularly valuable in NATO or other multinational procurement and capability development contexts, where states seek to standardize requirements, testing, and interoperability. Multinational standardization does not, however, replace the reviewing state's own Article 36 determination. The obligation remains with the state studying, developing, acquiring, or adopting the weapon, means, or method of warfare, and that state must exercise its own due diligence in determining whether its employment would be prohibited under the rules of international law applicable to it.¹¹

Operational implication: Procurement processes for new weapons, means, or methods of warfare should include a mandatory national legal review where Article 36 is triggered. Prior assessments by suppliers, allies, multinational bodies, or partner states may inform the review, but they cannot replace the reviewing state's own legal determination.

¹¹ Both the 1987 ICRC commentary and the 2006 ICRC guide make clear that a purchasing state must conduct its own review and cannot simply rely on the assessment of the seller, manufacturer, or another state. The Commentary states that the purchaser 'should not blindly depend on the attitude of the seller or the manufacturer' but should conduct its own evaluation of the weapon against Additional Protocol I and other applicable rules of international law. The ICRC guide similarly states that the purchasing state 'is under an obligation to conduct its own review' and 'cannot simply rely on the vendor or manufacturer's position as to the legality of the weapon, nor on another State's evaluation'. See Sandoz, Yves, Christophe Swinarski, and Bruno Zimmermann, eds., 'Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949' (Geneva: ICRC/Martinus Nijhoff, 1987), para. 1473; ICRC, *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977* (Geneva: ICRC, 2006), p. 24.

2. Why legal reviews matter

Legal reviews are a binding legal obligation for states party to Additional Protocol I; as such, they are not merely a matter of good practice or policy preference, but a concrete obligation to ensure compliance with IHL and other applicable international law. For states party to Additional Protocol I, this obligation is explicit. More broadly, conducting legal reviews may also be seen as fulfilling the duty under Common Article 1 of the Geneva Conventions to respect and ensure respect for IHL.¹² Beyond their formal legal basis, legal reviews serve a critical preventive and operational function – ensuring that weapons are both lawful and used in a lawful way. The reviews make sure that unlawful capabilities are identified and excluded before they are acquired and enter operational use, while translating abstract IHL rules into concrete constraints, conditions, and guidance governing how a capability may be lawfully employed. In this sense, legal reviews act as a bridge between legal norms and military practice, enabling compliance to be embedded within decision-making processes rather than assessed retrospectively. Legal reviews also facilitate the systematic integration of legal considerations throughout the entire capability life cycle. They ensure that questions of legality are addressed not just at the point of deployment, but throughout research and development, acquisition, testing, and operational planning. This is particularly important in contemporary defence environments, where technological development is often driven by complex interactions between military institutions, industry actors, and scientific communities.

In addition, legal reviews contribute to cost-efficiency and more effective procurement planning. By identifying legal constraints at an early stage, states can communicate clear requirements to industry during the development phase and avoid investing in capabilities that would ultimately be unlawful or unusable, or require significant modification. The same logic applies in procurement contexts, where early legal assessment reduces the risk of acquiring systems that cannot be lawfully employed under the state's international obligations.

From an operational perspective, legal reviews support commanders and personnel in conducting military operations. While the responsibility to comply with IHL ultimately rests with those who plan and execute operations, legal reviews provide them with defined parameters and guidance that facilitate lawful decision-making in complex and time-sensitive environments. In this way, the review process contributes directly to the practical ability of armed forces to comply with the law when they are in the field.

Furthermore, legal reviews play an important role in reinforcing the credibility and legitimacy of state conduct. In an international system characterized by limited transparency and the absence of formal verification mechanisms, the existence of

¹² See ICRC, 'Bringing IHL Home: Guidelines on the National Implementation of International Humanitarian Law' (ICRC: Geneva, 2021), p. 21, which states that reviews 'flow from the obligation to ensure respect for IHL'.

a structured and credible legal review process demonstrates good faith compliance and supports confidence building among states. This reputational dimension, while not determinative of legality, remains an important element in the broader functioning of the international legal order.

Finally, the growing prominence of Article 36 reviews in contemporary debates on emerging technologies – such as autonomous weapon systems, AI-based decision-support systems, and advanced drone capabilities – is not coincidental. These technologies are characterized by increasing technical complexity, opacity in functioning, and reliance on probabilistic or data-driven processes, which complicate the assessment of their practical effects. As a result, the application of core IHL principles – such as distinction, proportionality, and the prohibition of indiscriminate weapons – becomes more uncertain and context-dependent. In parallel, existing weapons law remains fragmented and largely reactive, with many emerging capabilities falling outside clearly defined treaty regimes. In this context, Article 36 reviews assume an expanded role. Rather than merely verifying compliance with established rules, they operate as a mechanism for managing legal and operational uncertainty, requiring states to interpret and apply general principles of international law to novel technological configurations. Article 36 therefore functions not only as a preventive compliance tool, but also as a form of anticipatory regulation, enabling states to impose constraints, conditions, and risk mitigation measures in situations where the legality of a capability cannot be determined solely by reference to existing prohibitions. This dynamic is particularly significant for technologies whose behaviour, effects, or interaction with human operators may not be fully predictable at the point of acquisition or deployment.



3. Contemporary challenges

The effective implementation of Article 36 legal reviews is increasingly shaped by a range of contemporary developments that affect both the nature of the technologies being assessed and the institutional context in which reviews are conducted. While these challenges do not alter the substance of the legal obligation, they complicate its interpretation and practical application. In particular, they raise questions as to how existing legal frameworks can be applied to novel capabilities, how legal reviewers can meaningfully assess increasingly complex systems, and how states can organize review processes in evolving defence and procurement environments.

From a legal and normative perspective, a first set of challenges concerns the application of existing frameworks to new types of capabilities. The absence of transparency in state practice, combined with the lack of formal verification mechanisms, makes it difficult to identify shared standards and best practices, thereby limiting the development of consistent approaches. At the same time, the increasing prevalence of dual-use technologies blurs the distinction between civilian and military applications, complicating the threshold question of whether a given capability qualifies as a ‘weapon, means, or method of warfare’ subject to review. These difficulties are further compounded by the emergence of software-based and non-kinetic capabilities, including cyber tools, which do not fit easily within traditional, weapon-centric understandings of Article 36 and instead require a more functional, effects-based approach to legal assessment.

A second set of challenges arises from the technological characteristics of contemporary military systems. Rapid technological development compresses the timelines between design, acquisition, and deployment, making it more difficult to conduct thorough and iterative legal reviews. At the same time, the increasing technical complexity of systems – particularly those involving software, machine learning, or autonomous functions – can exceed the capacity of legal reviewers to fully understand and evaluate their effects without extensive interdisciplinary input. The emergence of AI-enabled and autonomous systems raises additional concerns related to predictability and reliability, as well as the extent to which compliance with international law can be assessed on the basis of reasonably foreseeable use. These issues are further exacerbated by the modularity of, along with the ability to update, many modern systems, particularly through software updates, which complicates the temporal dimension of legal reviews and necessitates continuous or iterative reassessment.

Finally, a third set of challenges relates to institutional and operational factors that shape the conduct of legal reviews. The growing role of private industry in developing military technologies creates information asymmetries and requires states to rely on external actors for essential technical data. This dynamic is further intensified by the emergence of non-traditional defence actors, including start-ups and technology companies operating outside the traditional defence-

industrial base, which alters established procurement relationships and makes it more difficult to ensure that legal requirements are integrated at early stages of development. At the same time, resource constraints – particularly in situations of active conflict or urgent procurement – may create pressure to streamline or prioritize reviews, raising the risk that procedural expediency could undermine the substantive legal standard required by Article 36.



Establishing a national legal review mechanism

While the substantive content of the Article 36 obligation is defined by IHL and other applicable legal regimes, its institutional and procedural implementation is left to states. As a result, national legal review mechanisms vary considerably in their legal basis, structure, and operation. This section examines how states may operationalize Article 36 in practice by establishing a national review mechanism that is legally grounded, institutionally coherent, and effectively integrated into defence acquisition processes. State practice relating to the implementation of Article 36 remains diverse, uneven, and often only partially transparent. While a number of states have developed relatively detailed legal and institutional frameworks, others rely on less formalized arrangements, and publicly available information is often limited. This section does not seek to provide an exhaustive account of all existing models; rather, it identifies and analyses recurring elements found in current practice, alongside approaches that appear particularly effective in ensuring compliance with international law. The aim is to distil from this practice the elements most capable of supporting effective, consistent, and legally sound implementation of Article 36, while allowing for adaptation to different national legal systems, institutional arrangements, and operational contexts.

4. Legal and policy foundations

The obligation under Article 36 of Additional Protocol I is implemented domestically through a range of legal and policy instruments embedded within states' defence governance and acquisition frameworks. While state practice reveals considerable diversity in the form and terminology of these instruments, this variation does not reflect fundamentally different approaches in substance. Instead, Article 36 implementation is typically structured as a multi-layered system, combining general legal authority with increasingly specific operational guidance.

States use different types of instruments to implement Article 36, and an instrument's title does not always indicate how the review mechanism operates in practice. Known mechanisms have been established through government ordinances, ministerial directives, defence instructions, general orders, military manuals, or internal administrative procedures. Comparative analysis should therefore look beyond the instrument's formal label and examine its function within the national system: whether it makes review mandatory, identifies the responsible authority, defines review triggers, sets out the applicable legal framework, ensures access to technical and operational information, provides for expert participation, and determines the effect of the review outcome.

At the highest normative level, Article 36 implementation is anchored in the state's broader constitutional and legal framework governing the relationship between international law and the domestic legal order, as well as in legislative provisions regulating defence and military activities. Article 36 is rarely implemented through a standalone statute. Instead, its domestic effect derives from general constitutional commitments to comply with international law and from legislative frameworks that define the organization and responsibilities of the armed forces. As a procedural obligation requiring the establishment of review mechanisms, Article 36 cannot be implemented through the direct application of treaty norms alone. Even where Additional Protocol I forms part of domestic law, states must adopt specific institutional and administrative arrangements to operationalize the obligation.

In practice, this foundational layer performs three essential functions: affirming the binding nature of IHL within the domestic legal order; allocating institutional competence within the defence structure; and providing the legal authority for the adoption of more specific implementing measures. The detailed conduct of legal reviews is almost invariably regulated at lower normative levels, through instruments adopted within defence institutions.

National implementation instruments

The table below illustrates how these elements are operationalized in practice across selected states. It identifies the principal legal and policy instruments governing Article 36 implementation and highlights their respective functions within national systems.¹³

¹³ The Asia-Pacific Institute for Law and Security's 'Legal Review of Weapons Portal' offers a valuable and regularly updated compilation of national legal review frameworks, including the original texts of many of the instruments discussed in this section (accessed 31 July 2026). Practitioners seeking the full documentation of a particular state's review mechanism may find this a useful starting point.

Table 1: National implementation instruments

States	Legal and/or policy instrument	Function in relation to Article 36
Australia	Defence Instruction (General) OPS 44-1: Legal Review of New Weapons – Department of Defence, 2005	Establishes the formal Article 36 review procedure and assigns responsibility for reviews early in acquisition. Superseded in practice by the 2024 Australia Defence Force (ADF) guide (below).
	<u>ADDP 06.4 Law of Armed Conflict</u> – Department of Defence, 2006	Provides doctrinal law of armed conflict framework, including the need to review weapons before use.
	<u>ADF Guide to the Legal Review of New Weapons, Means or Methods of Warfare</u> – ADF/ Department of Defence, 2024	Provides detailed review methodology; covers materially modified capabilities and adds functional review for AI/ autonomous systems.
Belgium	Ordre général J/836 – Defence Staff/Chief of Defence structure, 2002	Original instrument establishing Belgium's standing legal review commission (Commission d'évaluation juridique, CEJ) within the Belgian Defence: plays a legal advisory role to the Chief of Defence. Repealed and replaced by the 2018 Specific Procedure (DGJUR-SPS-CJBCEJ-CXX-001), which retains 18 July 2002 as the benchmark date for determining whether a weapon, means, or method of warfare is 'new'.
	<u>Ministerial Decree on Determining the Weapons and Ammunition Forming Part of the Prescribed Equipment for Members of the Armed Forces and Establishing the Specific Provisions Relating to the Acquisition, Possession, Safekeeping, Carrying, Use and Transfer of These Weapons and Ammunition</u> – Minister of Defence, 2018	Establishes (art. 13) the CEJ within the Ministry of Defence responsible for evaluating new weapons and new means or methods of warfare against the law applicable in armed conflict, and prescribes its composition (jurists from the Ministry of Defence legal services serving as chair and secretary; representatives of operations and strategy, a technical expert, and a military physician) – with procedures governed by internal defence regulations.
	<u>Specific Procedure (Commission d'Evaluation Juridique des nouvelles armes, des nouveaux moyens et des nouvelles méthodes de guerre)</u> DGJUR-SPS-CJBCEJ-CXX-001/LEGAD-Int – Directorate General Legal Support, 2018	Implements Article 13 of the 2018 Ministerial Decree by setting out the mandate, composition, and procedure of the CEJ: review is mandatory at the earliest possible stage and in any event before acquisition or adoption; the CEJ delivers a reasoned advisory opinion, adopted unanimously by its permanent members, to the Chief of Defence via the Directorate General Legal Support; re-evaluation is required where new information emerges or the capability is substantially modified. Replaces General Order J/836 of 18 July 2002.

States	Legal and/or policy instrument	Function in relation to Article 36
Canada	<u>National Defence Act (R.S.C., 1985, c. N-5) – Parliament, 1985/last amended 2025</u>	Provides statutory basis for Judge Advocate General legal advisory role.
	<u>LOAC Manual B-GJ-005-104/FP-021 – Chief of Defence Staff/Office of the Judge Advocate General, 2001</u>	States Canada's Article 36 position and review obligation for new weapons, means and methods (para. 530), while framing the standard of review by reference to the law of armed conflict rather than the full 'any other rule of international law'.
	<u>DAOD 3002-0 Series: Ammunition and Explosives – Department of National Defence, 2016</u>	Structures certification of ammunition and explosives across the capability life cycle – from capability development or acquisition through to design and modification and completion before introduction into use – with validation criteria drawing on Canadian law and international agreements. The Director Ammunition and Explosives Regulation reports annually to the Deputy Minister and the Chief of the Defence Staff.
	<u>Directive for Article 36 Legal Review of Weapons – Deputy Minister/Chief of the Defence Staff, 2025, restricted</u>	Reportedly formalizes timing and process for Article 36 reviews.
Finland	<u>Act on the Defence Forces (551/2007), s. 4 – Parliament, 2007</u>	Requires that the military force employed by the Defence Forces complies with Finland's binding international obligations.
	<u>Ministry of Defence Decree on Legal Review of New Weapons, Means and Methods of Warfare – Ministry of Defence, 2012</u>	Establishes review mechanism and assigns responsibility within defence structures. ¹⁴
France	<u>Code de la défense, arts. L1141-1 and R*3121-1 – Parliament/Government</u>	Provides the general statutory basis for ensuring military capabilities comply with international obligations.
	<u>Directive 1618/ARM/CAB on the conduct of armament operations – Ministry for the Armed Forces, 2019</u>	Integrates legal review into procurement/project management.
	<u>Directive 6255/ARM/CAB – Ministry for the Armed Forces, 2019</u>	Establishes review process and responsibilities.

¹⁴ See also Government Bill HE 56/2025 vp (sec. 1.5), which quotes Section 4 of Act on the Defence Forces 551/2007 and describes the national Article 36 procedure in Section 9, and Foreign Affairs Committee Report UaVM 4/2025 vp (13 June 2025).

States	Legal and/or policy instrument	Function in relation to Article 36
Germany	<u>Zentrale Dienstvorschrift (ZDv) 15/10: Kriegsvölkerrecht: Leitfaden für den Unterricht, Teil 7: Allgemeine Bestimmungen des Kriegsführungsrechts und Landkriegsrecht</u> (Law of Armed Conflict: Guidelines for Teaching, Part 7: General Legal Provisions relating to the Conduct of Hostilities and War on Land) – Federal Ministry of Defence, 1961	Teaching manual dating back to 1961 on the law of armed conflict: addresses, in Part 7, the legal rules governing the means and methods of warfare – illustrating German engagement with weapons law conformity decades before Additional Protocol I.
	Joint Service Regulation A-2146/1: Review of New Weapons, Means and Methods of Warfare – Federal Ministry of Defence, 2016/2019	Binding regulation implementing Article 36, Additional Protocol I: vests responsibility for legal reviews in the Ministry of Defence legal directorate (R I 3), supported by an interdepartmental steering group; embeds reviews in the procurement process, to be completed before in-service use; ensures the definition of ‘new’ includes substantially modified capabilities; requires documented review results.
	<u>ZDv A-1500/3 Project-based Procurement and In-Service Use</u> – Federal Ministry of Defence, 2024	General regulation governing project-based procurement and in-service use: embeds the A-2146/1 review requirement as a mandatory task in the analysis and realization phases and, during in-service use, in the management of product modifications – taking into account Article 36 considerations throughout the capability life cycle.
Netherlands	<u>Ministerial Decision of 18 June 2014 establishing the Advisory Committee on International Law and Conventional Weapons Use (AIRCW), Staatscourant 2014, No. 16746</u> – Minister of Defence, 2014	Establishes the standing advisory committee that conducts Article 36 reviews. The AIRCW advises the Minister of Defence, on request or on its own initiative, regarding the compatibility of the acquisition, possession, and use of conventional weapons and munitions (expressly excluding nuclear weapons), as well as methods of warfare, with current and developing international law – in particular IHL. Improvements to previously approved capabilities are considered new, and the approval decision rests with the minister. This mechanism has been in place since 1978; the 2014 decision replaced its 2007 predecessor, which in turn revoked the original decision of 5 May 1978.

States	Legal and/or policy instrument	Function in relation to Article 36
New Zealand	<u>Geneva Conventions Act 1958 – Parliament</u>	Incorporates the Geneva law framework domestically.
	<u>Defence Act 1990 – Parliament</u>	Provides defence institutional authority.
	<u>Manual of Armed Forces Law, Vol. 4 – New Zealand Defence Force, 2017/2019</u>	Sets doctrinal basis for law of armed conflict compliance and weapons review.
Norway	<u>Directive on the Legal Review of Weapons, Methods and Means of Warfare – Ministry of Defence, 2003, restricted</u>	Establishes national Article 36 review mechanism.
	<u>Guidelines on International Law Review of New Weapons, Methods and Means of Warfare in the Defence Sector – Ministry of Defence, 2023, restricted</u>	Modernizes review practice and life-cycle approach.
	<u>Manual i krigens folkerett (Manual of the Law of Armed Conflict) – Norwegian Armed Forces, 2025 edition</u>	Armed forces manual restating the requirement for legal review of new weapons, methods, and means of warfare and setting out the substantive weapons law rules (prohibited weapons, weapons subject to restrictions, and clearance obligations): the only published Norwegian instrument articulating the review obligation, complementing the restricted 2003 Directive and 2023 Guidelines.
Sweden	<u>Förordning (1994:536) om folkrättslig granskning av vapenprojekt (Ordinance SFS 1994:536 on International Law Review of Weapons Projects) – Government, 1994</u>	Establishes formal review system and review body.
	<u>Förordning (2007:936) om folkrättslig granskning av vapenprojekt (Ordinance SFS 2007:936 on International Law Review of Weapons Projects) – Government, 2007</u>	Current framework requiring review of weapons projects and establishing the delegation.
Switzerland	<u>Materialverordnung VBS (Material Ordinance of the DDPS), 26 March 2018 (SR 514.20) – Federal Department of Defence, Civil Protection and Sport (DDPS)</u>	Establishes an obligation to review weapons for compliance with international law. Article 11 defines the scope; requires review for acquisition, modification, and new uses; mandates involvement of the competent authority; conditions procurement progress on a positive legality determination.

States	Legal and/or policy instrument	Function in relation to Article 36
	Weisungen über die Zusammenarbeit der Departementsbereiche Verteidigung und armasuisse (ZUVA), 28 March 2018 – Chief of the Armed Forces/ armasuisse	Embeds legal review into procurement and approval workflows. Annex 6 operationalizes the review within life-cycle processes and inter-agency coordination.
Ukraine	Temporary Review Algorithm – approved by resolution of a deputy minister of defence (interim, in force); Draft Order on Comprehensive Assessment of New Weapons, Means and Methods of Warfare – Ministry of Defence, 2025 draft	Interim instrument establishing the current review procedure, pending adoption of the draft order creating a national Article 36-style comprehensive assessment system.
	Draft Instruction Manual – Ministry of Defence, 2025 draft	Defines the procedure, scope, participants, objects of review, and legal criteria.
	Draft Checklist/Assessment Forms – Ministry of Defence, 2025 draft	Provides detailed technical/legal data collection tool, including AI and autonomy questions.
United Kingdom	JSP 383 Joint Service Manual of the Law of Armed Conflict – Ministry of Defence, 2004	States the UK obligation/practice of reviewing new weapons.
	Instruction 2009DIN04-217: Legal Review of Newly Acquired or Developed Weapons and Associated Equipment – Ministry of Defence, Development, Concepts and Doctrine Centre (DCDC) Legal, 2009, internal	Directs that legal reviews be conducted by the joint three-service legal team at DCDC at ‘initial gate’, ‘main gate’, and before entry into service, including for urgent operational requirements; defines ‘new’ as including modified versions and systems acquired from other states, and ‘means or methods’ as including sighting, target-acquisition, and targeting software; specifies the technical, effects, reliability, and environmental data required; precludes reliance on another state’s review; requires legal reviews to be retained permanently with the project records.
	UK Weapon Reviews policy paper – Ministry of Defence, 2016	Public explanation of UK review practice.
	JSP 936 Dependable Artificial Intelligence in Defence, Part 1: Directive, V1.0 – Ministry of Defence, 2024	Adds AI assurance framework relevant to legal review of AI-enabled capabilities.

States	Legal and/or policy instrument	Function in relation to Article 36
United States of America	<u>DoD Directive 2311.01: DoD Law of War Program</u> – Secretary of Defense, 2020	Establishes Department of Defense-wide law of war compliance framework.
	<u>DoD Law of War Manual</u> – Office of General Counsel, updated 2023	Provides interpretive legal framework for law of war compliance and weapons review.
	<u>Army Regulation 27-53: Legal Review of Weapons and Weapon Systems</u> – Department of the Army, 2019 (originally from 1979)	Establishes service-specific weapon review procedure.
	<u>AFI 51-401: The Law of War, Part 2</u> – Department of the Air Force, 2018 (superseding AFI 51-402)	Establishes service-specific legal review process for weapons (para. 2.1.2).
	<u>SECNAVINST 5000.2G</u> – Department of the Navy, 2022	Integrates legal review into US Navy acquisition system.
	<u>DoD Directive 3000.09: Autonomy in Weapon Systems</u> – Secretary of Defense, 2023	Establishes specific policy and review safeguards for autonomous weapon systems.

Core elements and design of implementing instruments

This comparative overview demonstrates that, despite variations in legal form and institutional context, national implementation of Article 36 is characterized by a high degree of convergence in the content of governing legal and policy instruments. Across jurisdictions, these instruments do not merely restate the obligation to conduct legal reviews; rather, they define the parameters within which this obligation is applied in practice. Several recurring elements can be identified, reflecting how states translate Article 36 into regulatory terms:

- **Multi-layered structuring of instruments:** State practice consistently reflects the use of multiple instruments operating at different levels of abstraction. Higher-level instruments typically establish the existence and legal basis of the review obligation – for example, through defence legislation or binding ordinances requiring compliance with international law and mandating the review of new capabilities. These are complemented by framework or directive-level instruments, often adopted within ministries of defence, which define the scope of application, identify responsible actors, and link the review obligation to regulated processes such as procurement or capability development. At a more detailed level, procedural instruments – such as internal instructions or guidance documents – specify how the obligation is to be implemented in practice, including timing, required inputs, and coordination among actors. This layered structure allows core obligations to be anchored in binding frameworks, while more specific elements are regulated through adaptable policy or administrative instruments.

Operational implication: Implementing frameworks should distribute regulatory content across instruments of different levels, distinguishing clearly between foundational provisions, framework rules, and detailed implementing guidance.

- **Regulation of scope within instruments:** Implementing instruments typically define the material scope of Article 36 by specifying which capabilities are subject to review. This commonly includes newly developed weapons, means, and methods of warfare; modifications to capabilities already in service; new or previously unassessed uses of an existing capability; and, in many national frameworks, capabilities acquired from external sources – including foreign military sales, commercial off-the-shelf procurement, donation, and in-kind assistance. The express inclusion of acquired capabilities matters because acquisition and adoption engage Article 36 independently of study or development, and a review conducted by the supplying state does not discharge the acquiring state's own obligation.¹⁵ While the level of specificity varies, the presence of an explicit scope provision is a consistent feature.

Operational implication: Instruments should explicitly define the scope of application, ensuring that the obligation is framed in sufficiently clear terms to be applied consistently.

31

- **Incorporation of life cycle-based triggers:** A recurring feature of implementing instruments is the inclusion of provisions specifying when the review must be conducted, often referencing stages of the capability life cycle. Rather than relying on open-ended obligations, instruments frequently tie review requirements to existing capability acquisition processes such as development, acquisition, or modification.

Operational implication: Instruments should include clearly defined trigger points linked to recognized processes, rather than leaving the timing of review to discretionary practice.

- **Allocation of responsibilities:** Implementing instruments commonly regulate the allocation of responsibilities by identifying the actors involved in the review process and their respective roles. While the level of detail varies, instruments typically distinguish between those responsible for initiating the review, those conducting the assessment, and those required to provide supporting information.

¹⁵ For example, the UK Ministry of Defence 'Legal Review of Newly Acquired or Developed Weapons and Associated Equipment' (2009DIN04-217) (October 2009, para. 14) specifies that where the United Kingdom acquires equipment already in service with another state's armed forces, it remains legally obliged to conduct its own review and cannot rely on the supplying state's.

Operational implication: Instruments should explicitly assign responsibilities to relevant actors, ensuring that the obligation is implemented through clearly defined roles rather than implicit practices.

- **Specification of applicable legal standards:** Most implementing instruments identify, either directly or by reference, the legal framework against which assessments must be conducted. This generally includes IHL, applicable treaty obligations, and customary international law. In some cases, instruments further articulate specific principles or categories of prohibition.

Operational implication: Instruments should clearly indicate the applicable legal framework, even where detailed analytical methodologies are developed elsewhere.

- **Integration clauses within instruments:** A number of systems include provisions that explicitly link Article 36 reviews to other regulated processes, particularly procurement and capability development. These provisions do not regulate these processes themselves, but require that legal reviews be incorporated into them.

Operational implication: Instruments should include provisions that connect legal review obligations to existing regulatory or administrative processes, ensuring that the obligation is embedded rather than isolated.

- **Delimitation of regulatory detail:** An important feature of state practice is that implementing instruments generally define the framework of the obligation without specifying the detailed methodology. Technical assessment criteria, analytical steps, and data requirements are typically addressed in separate internal guidance materials rather than in binding or formal policy instruments.

Operational implication: Instruments should establish the structure and parameters of review while allowing methodological details to be developed through flexible, non-binding tools.

5. Institutional design of review mechanisms

States organize Article 36 review mechanisms through different institutional arrangements. These arrangements determine where the review function is embedded, whether the assessment is conducted by an individual authority or a collective body, and how legal, technical, and operational expertise is incorporated into the process. This section focuses on three elements of institutional design: first, the institutional embedding of the review authority; second, the composition of review bodies; and third, the allocation of responsibilities among the actors involved in initiating, conducting, and implementing reviews.

Institutional embedding of the review function

The review function under Article 36 is, in almost all documented systems, embedded within the ministry of defence or an equivalent authority responsible for the development and acquisition of military capabilities. This reflects both the operational context of the obligation – linked to the conduct of hostilities – and the institutional reality that defence authorities exercise primary control over capability development and procurement.

Within this defence-centred framework, state practice reveals a limited number of recurring models concerning the institutional location and organization of the review function. While these arrangements differ in form, they can broadly be understood by reference to whether responsibility for conducting legal reviews is assigned to a designated authority or to a collective body.

33

Table 2: Authority or entity responsible for Article 36 reviews

State	Review authority/entity	Institutional location and model
Australia	Directorate of Operations and International Law, Defence Legal (Military Legal Service), Department of Defence	Department of Defence, designated legal authority model
Belgium	Commission d'évaluation juridique des nouvelles armes, moyens et méthodes de guerre	Ministry of Defence, standing commission model
Canada	Office of the Judge Advocate General, Directorate of International Law	Canadian Armed Forces legal service, designated legal authority model
Finland	Legal Department, Defence Command Finland	Defence-based legal authority with supporting expertise
France	Direction des affaires juridiques (Department of Legal Affairs), Ministry for the Armed Forces	Central legal authority within the Ministry of Defence

State	Review authority/entity	Institutional location and model
Germany	Federal Ministry of Defence legal structures under Joint Service Regulations	Defence ministry-based legal authority model
Netherlands	Advisory Committee on International Law and Conventional Arms Use (AIRCW)	Ministry of Defence, advisory committee model
New Zealand	New Zealand Defence Force legal authorities	Defence Force-based legal review function
Norway	Defence sector legal authorities; escalation to Ministry of Defence	Hybrid model within defence sector
Sweden	Delegation for International Law Monitoring of Weapons Projects	Government-established delegation under the Ministry of Defence framework reporting to the government
Switzerland	Law of Armed Conflict Section under the DDPS	Centralized legal authority model with internal independence
Ukraine	Comprehensive Assessment Commission (currently operating on an ad hoc basis; formalization proposed)	Ministry of Defence, central commission model
United Kingdom	Military lawyers within the DCDC, operating under Defence Futures, on behalf of Ministry of Defence Central Legal Services	Defence-based legal authority model embedded in a tri-service doctrine and futures organization, functionally independent from single-service chains of command
United States of America	Service-level legal review authorities (Army, Navy, Air Force) under Department of Defense framework	Distributed service-based model

The comparative overview indicates that, while Article 36 review functions are almost invariably situated within defence institutions, states adopt different approaches to how this function is institutionally embedded. These approaches can be grouped into three broad models, depending on whether the review function is assigned to an existing legal authority, entrusted to a dedicated collective body, or distributed across multiple entities:

- Designated legal authority model:** In this model, responsibility for conducting legal reviews is assigned to an existing legal service or a designated legal authority within the ministry of defence or armed forces. No separate institutional body is created specifically for Article 36; instead, the function is integrated into the mandate of an established legal office. Reviews are conducted under the authority of legally qualified personnel, typically within central legal services, with technical and operational input provided as required.

This model is reflected in a number of states. In Canada, the review function is carried out by the Office of the Judge Advocate General, a statutory legal authority within the Canadian Armed Forces. Switzerland similarly assigns the function to a designated authority, the Law of Armed Conflict Section, without creating a separate review body. In Australia, the function is exercised by the legal directorate responsible for operations and international law within the Department of Defence. These arrangements typically rely on existing institutional structures, with the review function incorporated into broader legal advisory roles.

Operational implication: States may implement Article 36 without establishing a new body by formally assigning responsibility to an existing legal authority – provided that this authority has a clear mandate, sufficient expertise, and access to relevant information.

- **Collective body model:** In this model, the review function is entrusted to a dedicated institutional body – such as a commission, committee, delegation, or working group – established specifically to conduct Article 36 reviews. These bodies are typically created through ministerial or governmental instruments, which define their mandate, structure, and relationship to the defence establishment. They may be permanent or standing bodies, or structured as recurring working groups, depending on the system.

This model can be found in several states. In France, responsibility lies with a committee comprising representatives of the Joint General Staff (État-major des armées), the General Procurement Agency (Direction générale de l'armement), and the Department of Legal Affairs (Direction des affaires juridiques) – convened when a preliminary review determines that a formal legality review is required. In Belgium, a standing legal review commission, established within Defence by ministerial decree and governed by internal defence regulations, provides recommendations to the Chief of Defence. In the Netherlands, the Advisory Committee on International Law and Conventional Arms Use (AIRCW) functions as an expert body under the Ministry of Defence. In Sweden, the Delegation for International Law Monitoring of Weapons Projects is established by government ordinance within the defence framework and reports to the government. Finland follows a similar approach: the review function is carried out through a mechanism established by a Ministry of Defence decree, involving a structured, multi-actor process rather than a single designated reviewer. The proposed Ukrainian framework similarly establishes a central commission under the Ministry of Defence, chaired by a senior-level official and supported by multiple departments. A defining feature of this model is the creation of a dedicated institutional structure with an explicit Article 36 mandate, often formalized through a founding instrument.

Operational implication: States may choose to establish a dedicated review body where there is a need to formalize multi-disciplinary input, enhance visibility of the review function, or reinforce its institutional autonomy.

- **Distributed service-based model:** In a third, less common model, responsibility for Article 36 reviews is distributed across multiple entities, typically corresponding to different branches of the armed forces. Rather than centralizing the function within a single authority or body, each service maintains its own review arrangements within a broader defence framework.

The principal example is the United States of America, where responsibility for conducting legal reviews is allocated across the military services (Army, Navy, Air Force), each of which operates under its own implementing regulations. Within each service, however, the review function is itself centralized and assigned to a designated legal authority within the service's legal structure, such as the Office of the Judge Advocate General or an equivalent legal directorate. These service-level legal authorities conduct reviews in accordance with Department of Defense policy and law of war obligations, while maintaining their own procedures and practices. As a result, the US system combines inter-service distribution with intra-service centralization. There is no single defence-wide review authority, nor is the function decentralized in an ad hoc manner; rather, it is replicated across services through parallel legal authority structures.

Operational implication: A distributed model may be adopted in systems with decentralized defence structures, but requires clear overarching guidance and consistency mechanisms. Even in such systems, it remains necessary to designate a specific reviewing authority within each entity responsible for conducting the legal assessment.

These models are not mutually exclusive in practice, and hybrid arrangements are common. For example, systems based on a designated legal authority may involve structured consultation with technical experts, while collective bodies rely on legal expertise to guide their assessments. The United Kingdom represents a distinctive hybrid, where the review function is exercised by legal personnel within a doctrine and futures organization (DCDC, now operating under Defence Futures), combining elements of centralization, cross-service integration, and functional independence.

Across all models, the decisive factor is not the institutional form chosen, but whether the review function is clearly assigned, appropriately embedded within defence structures, and capable of producing independent and legally reliable assessments.

Operational implication: The choice between assigning the function to an existing authority, creating a dedicated body, or distributing responsibilities across entities should be guided by institutional context. In all cases, the key requirement is that reviewing entity is formally designated, operationally integrated, and functionally capable of exercising independent legal judgement.

Box 2: What about entities with military functions outside the ministry of defence?

Although Article 36 is framed in functional terms, national implementation is overwhelmingly embedded within ministries of defence. In practice, states rarely establish separate review mechanisms for other entities that may possess military or quasi-military capabilities, such as law enforcement bodies, national guards, or intelligence services.

Instead, where such entities are involved in the development or acquisition of relevant capabilities, states tend to extend an existing defence-based mechanism rather than creating parallel systems. Sweden provides a clear example: the Delegation for International Law Monitoring of Weapons Projects operates as a centralized review body and receives notifications not only from the armed forces and procurement authorities, but also from other relevant government agencies. This reflects a functionally broad, government-level approach, under which the Article 36 review is triggered by the nature of the activity rather than the institutional identity of the actor.

Where no such extension exists, activities of non-defence entities are generally considered to fall outside the scope of Article 36, insofar as they are not linked to the conduct of hostilities and are instead governed by other legal frameworks, including law enforcement and human rights regimes.

Composition of review bodies

The composition of Article 36 review mechanisms reflects the need to conduct a legal assessment that is informed by an accurate understanding of the technical characteristics and operational use of a capability. While institutional arrangements differ, state practice consistently shows that reviews are carried out either by a designated legal authority supported by consultation or by a collective body bringing together multiple forms of expertise. In both cases, the composition of the mechanism is designed to ensure that the legal determination is based on sufficiently reliable technical and operational information. Across state practice, three categories of expertise are consistently involved in the review process. Legal expertise is central, as the review ultimately involves determining whether a

capability complies with international law, including IHL. This legal determination is informed by technical and, where relevant, medical expertise – such as engineers, weapons specialists, or medical practitioners who assess the design, functioning, and effects of the capability – and by operational or military expertise, which offers insights into intended use and deployment scenarios. The role of technical and operational expertise is therefore to support and enable the legal assessment, rather than to replace it.

This structure is reflected across systems. For example, in Australia, defence legal officers conduct legal reviews on the basis of technical documentation and input from capability managers. In Switzerland, the review is carried out by a specialized legal authority, the Law of Armed Conflict Section, which consults technical, medical, or other experts depending on the characteristics of the system under review.

Operational implication: Review mechanisms must ensure that legal decision-makers have structured access to the technical and operational expertise necessary to support a legally sound assessment.

State practice demonstrates two principal approaches to organizing this expertise. In systems with a designated legal authority, the review is conducted by an individual legal reviewer or a specialized legal unit within defence legal services. Multidisciplinary input is obtained through consultation rather than embedded in a formal body. This approach is followed, for example, in Switzerland and Australia, where the review function is integrated into existing legal structures, with additional expertise brought in as required.

In contrast, collective models institutionalize multidisciplinary expertise within a formally constituted body, such as a commission, committee, or delegation. These bodies are typically established through ministerial or governmental instruments and operate as standing or semi-standing entities. Examples include Belgium, where a legal review commission (CEJ) provides recommendations to the Chief of Defence; the Netherlands, where the AIRCW conducts reviews under the Ministry of Defence; and Sweden, where the Delegation for International Law Monitoring of Weapons Projects is established by government ordinance as a dedicated review body. In such systems, the responsibility for the assessment is formally attributed to the collective body, even though legal expertise remains central to the determination.

Where review is conducted by a collective body, these entities are typically relatively small and functionally focused, rather than large inter-agency committees. In most documented systems, such bodies consist of a core group of members, often drawn from legal, technical, and operational domains, with the possibility of involving additional experts as required. This allows the body to maintain continuity and efficiency while retaining access to specialized expertise. For example, Sweden's Delegation is a formal body with appointed members and a defined

mandate, while the Dutch AIRCW operates as a specialized advisory committee composed of experts in international law and related fields. In Belgium, the review commission functions as a standing body within the defence structure, ensuring continuity in the assessment process. Although the exact number of members is not always publicly specified, these bodies are generally structured to remain manageable in size, allowing for effective deliberation and timely review.

Collective bodies may have fixed membership or mechanisms allowing for flexible participation depending on the capability under review. Standing membership supports consistency and institutional memory, while flexible participation allows the inclusion of specialized expertise where needed. In practice, many systems combine these approaches, maintaining a core membership while drawing on additional experts for specific reviews.

Even in systems based on designated legal authorities, similar flexibility is observed. For example, in Switzerland, the reviewing authority may consult external experts, including technical or medical specialists, depending on the characteristics of the system. This reflects a broader pattern in which flexibility is achieved either through institutional design (collective bodies) or through consultative practices (individual authority models). Reliance on external expertise also raises questions about independence and conflicts of interest. Where external expertise is drawn from the developer, manufacturer, or supplier of the capability under review, the review body should ensure that commercial interests are disclosed, that supplier representatives do not participate in the legal determination itself, and that, wherever practicable, supplier-provided technical claims can be independently verified. Access to independent testing or evaluation capacity is essential for a reliable review.

Operational implication: Review mechanisms should ensure continuity of expertise while also enabling the incorporation of specialized knowledge as required by the characteristics of the capability.

Beyond the core categories of legal, technical, and operational expertise, some systems provide for the inclusion of additional forms of expertise where relevant. This may include medical, environmental, or safety specialists, particularly where the effects of a capability raise specific concerns in these areas, as well as expertise in assessing differential impacts on different groups of the civilian population – including gender expertise and expertise in identifying and analysing data-bias risks. For example, Swiss practice allows for the consultation of medical and environmental expertise in assessing weapon effects, while some national frameworks envisage the involvement of scientific or testing institutions as part of the review process.

This reflects the increasing complexity of modern military technologies, which may require assessment across a broader range of disciplines. Such expertise is, however, typically incorporated on a case-by-case basis, rather than forming part of the permanent composition of the review body.

Operational implication: Review frameworks should allow for the inclusion of specialized expertise beyond core categories, without over-institutionalizing the composition of the review body.

Roles and responsibilities

Institutional arrangements for Article 36 reviews typically distinguish between several core functions, which are allocated across different actors within the defence structure. First, responsibility for initiating the review is generally assigned to the entity responsible for the development, acquisition, or modification of the capability. This may include programme managers, procurement authorities, or other units within the defence organization. For example, in France, actors responsible for armament programmes are required to notify the legal affairs directorate when a legal review is required. In the proposed framework for Ukraine, developers or procuring entities are responsible for submitting the necessary documentation to the review commission.

Second, responsibility for conducting the legal assessment is assigned either to a designated reviewing authority or to a collective body. In systems such as those of Canada and Australia, this function is exercised by a designated legal office within the defence structure, whereas in Belgium, Finland, the Netherlands, and the proposed framework for Ukraine, it is carried out by a commission or working group established for that purpose.

Third, technical and operational actors are responsible for providing the information necessary to support the assessment. This includes data on the design, performance, and intended use of the capability, as well as relevant operational concepts. In practice, much of this information is held by private-sector actors external to the state – such as the developer, manufacturer, or supplier of the capability – who increasingly also operate, maintain, or sustain fielded systems under contract. Where the review relies on such actors, their role and responsibilities in supplying information should be clearly identified, and safeguards to ensure the independence of the assessment (see the discussion of composition and expertise above) should be applied.

Fourth, responsibility for decision-making or endorsement may be distinct from the body conducting the review. In some systems, the review body issues a recommendation or legal opinion that is submitted to a higher authority for

approval. For example, in Belgium, the commission provides advice to the Chief of Defence. In the proposed framework for Ukraine, the conclusions of the commission are adopted at the senior ministerial level.

Finally, the review outcome must be implemented within military practice. This involves integrating it into procurement decisions, incorporating any legal constraints into doctrine or operational guidance, and making sure it is applied by commanders and operational personnel, who remain responsible for ensuring compliance with international law in the conduct of operations.

6. Integration into defence procurement processes and capability life cycle

State practice demonstrates that the Article 36 review is not conducted as a single, isolated assessment, but is increasingly integrated across the capability life cycle, from initial concept and development through to acquisition, introduction into service, and subsequent modification or change of use. This reflects the practical reality that the legality of a capability cannot always be determined definitively at a single point in time, particularly where systems evolve during development or are adapted to new operational contexts.

The integration of legal review across the capability life cycle can be illustrated through a simplified model reflecting state practice. In systems such as those of Switzerland and Australia, legal reviews are conducted at multiple stages of the procurement process, from initial concept through to development and introduction into service. The model below abstracts this approach, illustrating how legal review operates as a staged and iterative process, aligned with key decision points within the procurement cycle. During these stages, legal assessment may function as a control gate, informing and, where necessary, conditioning the decisions made to progress a capability to subsequent phases, thereby ensuring that legal considerations are addressed before key investment and deployment decisions are made. This staged approach allows preliminary assessments to be conducted on the basis of available information in the early stages, while enabling more detailed analysis as technical specifications and operational concepts become clearer over time. The model also includes the possibility of reassessment where a capability is modified or used in a new operational context.

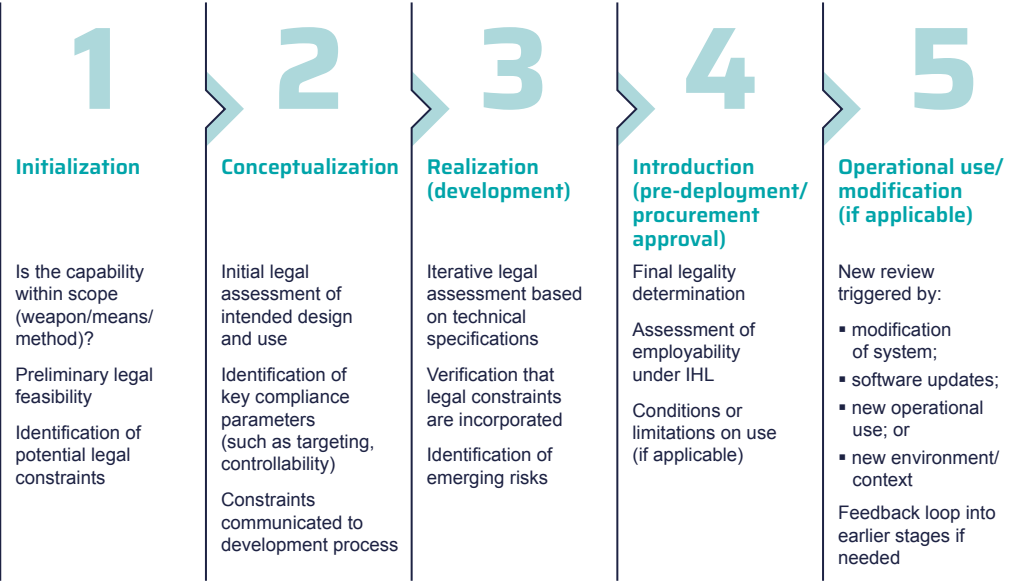


Figure 1. Steps for integrating an Article 36 review across the capability life cycle

The integration of legal review into life-cycle processes also serves a governance function by linking the assessment to decision-making points within procurement and capability development frameworks. While the precise legal effect of review outcomes varies across states, practice suggests that the legal review functions as a control mechanism within procurement governance, ensuring that the process for capabilities that raise unresolved legal concerns does not advance to the next phase without further assessment or modification. In some systems, this is reflected in requirements that the legal review be completed before a project can proceed to key approval stages, while in others this takes the form of advisory opinions that inform decision-making by competent authorities.

Beyond ensuring compliance, the integration of legal reviews into procurement processes also serves a risk management and cost-efficiency function. By identifying potential legal constraints at an early stage, states can avoid investing in capabilities that may later prove unlawful or unusable, or require substantial modification. Early integration of legal assessments therefore contributes to a more efficient allocation of resources and supports more predictable and legally compliant capability development.

Importantly, the life-cycle approach continues beyond the introduction of a capability into service. A legal review may need to be revisited if a capability undergoes significant modification, is assigned a new operational function, or is deployed in a substantially different context than originally assessed. This is particularly relevant for modern systems characterized by iterative development, software updates, or adaptive behaviour. In such cases, the initial review may no longer be sufficient to ensure compliance, and additional assessment may be required. More broadly, states may treat post-fielding monitoring – including the structured collection and analysis of data on operational performance and civilian harm – as part of the review system's feedback loop. If this data reveals unanticipated effects, including possible indiscriminate effects or differentiated impacts on particular groups of the civilian population, this should trigger a reassessment of the original determination. This introduces an element of feedback and reassessment into the review process, transforming it from a one-time approval mechanism into a more dynamic form of legal oversight across the life cycle of the capability.

Operational implication: Review mechanisms should be integrated across the full capability life cycle, including post-adoption phases, and should be linked to decision-making processes in a manner that allows legal assessments to influence and, where necessary, constrain the development, acquisition, and continued use of military capabilities.

Box 3: Communicating legal review criteria to industry

While the obligation under Article 36 rests exclusively with the state, its effective implementation increasingly depends on how legal requirements are translated into technical and development processes, particularly where capabilities are designed and produced by external actors. In contemporary defence ecosystems, this includes not only traditional defence contractors, but also smaller companies and start-ups that may develop enabling technologies without prior engagement with military legal frameworks.

In practice, an Article 36 review is often conducted after key design decisions have been made, which can limit the reviewing authority's ability to influence the technical characteristics of a system. This creates both legal and economic inefficiencies, as capabilities may require modification or may ultimately prove unusable if they are found to be incompatible with applicable legal constraints. These challenges are amplified where industry actors lack familiarity with IHL or do not possess established compliance structures.

A forward-looking approach to Article 36 implementation would therefore involve the systematic communication of relevant legal criteria and constraints – such as requirements concerning the principle of distinction and the extent to which new weapons, means, and methods of warfare can be controlled, and their effects limited – to procurement authorities and, where appropriate, to industry actors at early stages of development. This does not entail delegating the legal assessment itself, which remains the responsibility of the state, but rather ensuring that developers are aware of the parameters within which a capability must operate in order to be lawfully employed.

This logic is reflected in emerging policy approaches such as the 'Lawful by Design'¹⁶ initiative developed by Article 36 Legal, which seeks to promote the integration of legal, ethical, engineering, and safety considerations into the development of military technologies from the outset. While such initiatives do not constitute binding legal standards, they demonstrate a growing recognition that compliance with IHL cannot be ensured solely through ex post review, but must also be embedded within design and development processes.

Such an approach can contribute to cost-efficiency by reducing the risk of investing in capabilities that require substantial redesign or cannot be approved for use. It also supports more effective integration of legal considerations into innovation processes, particularly in sectors where technological development is driven by actors outside traditional defence-industrial structures. For smaller and emerging companies, which may lack the expertise or capacity to integrate IHL and ethical compliance into

¹⁶ Lawful by Design Initiative, 'Bridging the Gap between Industry Led Innovation and National Legal Review Processes'.

design and development processes, one practical approach is to embed legal and ethical considerations directly into investment policies and funding opportunities to ensure they are considered at an early stage of company or product development.

In practice, this approach may be implemented through procurement conditions and contractual requirements. States may take the following four steps: (1) require suppliers to provide the technical, testing, data quality, and human control information needed for legal review – including, for AI-enabled systems, information on training data sufficient to assess bias; (2) include enforceable contractual obligations relating to transparency, monitoring, incident reporting, and continuous testing; (3) apply evaluation criteria that reward demonstrable IHL-compliance engineering and, where relevant, gender-responsive safeguards; and (4) provide for suspension or termination if material non-compliance is identified. Model questions for industry engagement – addressing bias mitigation, data set representation, impact assessment, and levels of human oversight – support consistent practice. Comparable approaches have been developed in other domains, such as contract guidance for private military and security services.¹⁷

Operational implication: States should consider how to translate legal review criteria into clear, accessible requirements within procurement and development processes, enabling industry actors – including start-ups – to design capabilities that are compatible with applicable international legal constraints from the outset.

The mechanisms described above depend on the state being party to a structured acquisition relationship – a tender it can shape, a contract through which conditions can be imposed, and a developer with whom requirements can be discussed before design decisions are finalized. Not all capabilities reach the armed forces through this route. If they arrive via donations, unit-level purchases, or changes in the field, the connection to the review system must be made at the point of entry into service rather than at the point of design.

¹⁷ See DCAF, 'A Contract Guidance Tool for Private Military and Security Services: Promoting Accountability and Respect for Human Rights and International Humanitarian Law' (Geneva: DCAF, 2017), which sets out selection criteria weighted according to respect for IHL and human rights law rather than lowest price, and a model contract addressing rules of conduct, monitoring, and non-compliance, building on the non-binding good practices in Part Two of the Montreux Document (2008). The mechanics are transposable, although both instruments concern the contracting of military and security services rather than the development or acquisition of a weapon.

Box 4: Article 36 review in the context of decentralized procurement

In contemporary practice – especially in states engaged in large-scale armed conflict, including Ukraine – capabilities increasingly enter service outside the central procurement pipeline: through direct purchases by individual services or units, donations and international assistance, crowdfunded and volunteer-supplied equipment, framework and urgent operational procurement, and rapid front-line adaptation of commercial systems (for example, the fitting of alternative munitions or payloads to commercially sourced unmanned systems). The volume and pace of such acquisition can exceed what a single central review channel was designed to absorb.

Decentralization of purchasing does not, however, decentralize the obligation. Article 36 applies to the state itself, and is engaged by the study, development, acquisition, or adoption of a new weapon, means, or method of warfare through any channel – including donation and in-kind assistance. A state therefore needs mechanisms that connect every acquisition channel to its review system. Modalities that can be applied in this regard include:

- type-based or generic reviews assessing classes of capabilities – for example, categories of unmanned systems or munitions – against a defined technical envelope so that individual acquisitions within an approved envelope require only confirmation-level screening;
- a centralized register of reviewed types and envelopes, accessible to procuring entities, the services, and – where appropriate – donation acceptance bodies;
- expedited or limited review pathways for commercial off-the-shelf items and minor variants, with clearly defined triggers for escalation to a full review – for example, a new payload or warhead; a new guidance, autonomy, or target-recognition function; or a new operational use;
- delegated screening at the service or unit level – exercised under the authority of, and with mandatory reach-back to, the central reviewing authority – should major triggers for escalation be identified;
- integration of screening into the administrative channels through which decentralized acquisitions already pass, such as donation acceptance, safety or airworthiness certification, codification, and introduction-into-service decisions;
- reliance, where appropriate, on Article 36 reviews already conducted by the country of origin or by other states operating the same system, which can inform and expedite – though not substitute for – the receiving state's own review, since applicable treaty obligations and intended methods of employment may differ between states; and

- record-keeping arrangements ensuring that decentralized acquisitions and unit-level modifications are captured in the central review archive.

Unit-level modifications deserve particular attention: the adaptation of payloads, software, or methods of employment at the edge may produce a 'new' weapon or means of warfare requiring review. Screening duties should therefore be embedded in the approval process for modifications, not just acquisitions. In situations of urgent operational necessity, expedited procedures – rather than waived review – preserve both compliance and the operational record. Where equipment has entered use without review, the appropriate course is regularization: prompt screening – drawing, where available, on the review conducted by the country of origin; any necessary conditions on use; and documentation of the determination.

Operational implication: The reviewing authority should map every channel through which capabilities and modifications enter service and ensure that each is connected to the review system through proportionate screening, escalation, and record-keeping mechanisms.

7. Legal effect and outcomes of reviews

The outcome of an Article 36 review is a legal assessment of whether a weapon, means, or method of warfare may be employed in compliance with applicable international law. While the obligation to conduct such a review is binding, international law does not prescribe the legal status of the outcome within domestic systems. As a result, states differ in whether review conclusions are considered binding determinations or advisory legal opinions within defence decision-making structures.

In a number of systems, the review outcome constitutes a binding or determinative legal conclusion, at least within the defence establishment. In such cases, the reviewing authority is responsible for determining legality, and its conclusion directly governs whether a capability may proceed to procurement, introduction into service, or operational use. This approach is typically associated with systems in which the review function is assigned to a designated legal authority within the defence structure. For example, in Switzerland, the Law of Armed Conflict Section, as the competent authority conducts the legal review and issues a formal legal assessment that informs and, in practice, defines the conditions for procurement and deployment decisions. Similarly, in systems such as that of Australia, legal reviews conducted by defence legal authorities form part of formal approval processes for the development, acquisition, modification, or introduction into service of military capabilities.

In other systems, the review outcome is formulated as an advisory legal opinion, which is then considered by another authority responsible for making the final decision on procurement or deployment. This is particularly evident in systems based on collective bodies. For example, in Belgium, the legal review commission provides recommendations to the Chief of Defence, rather than issuing a formally binding determination. Likewise, in the Netherlands, the AIRCW provides expert advice to the Ministry of Defence, which retains responsibility for final decision-making.

Despite this formal distinction, the practical difference between binding and advisory outcomes is often less pronounced than it may appear. Even where review conclusions are framed as advisory, they typically carry significant weight within defence decision-making, and it is rare for a capability to proceed in the face of unresolved legal concerns. Conversely, in systems where legal authorities issue determinations, these are often embedded within broader procurement processes, meaning that legal conclusions operate alongside, rather than entirely independently from, political and operational considerations.

A further dimension of review outcomes concerns their substantive content. Rather than resulting in a simple binary conclusion (lawful/unlawful), legal reviews frequently produce conditional assessments, identifying the circumstances under which a capability may be lawfully employed. These may include limitations on use, operational constraints, or requirements for additional safeguards. In this sense, the review outcome does not merely determine whether a capability may be used, but also shapes how it may be used in practice.

Operational implication: States should define clearly, within their implementing frameworks, the legal status of review outcomes and their relationship to procurement and operational decision-making processes. Whether formulated as binding determinations or advisory opinions, review conclusions must be capable of effectively influencing decisions on the development, acquisition, and use of military capabilities.

From conditional approval to operational practice

A central – yet often under-theorized – dimension of Article 36 practice lies not in the adoption of legality determinations, but in their translation into operationally binding norms governing use. Legality is frequently contingent: weapons are not simply ‘lawful’ or ‘unlawful’, but lawful only under certain conditions of use, which must be concretized within military practice. Conditional approval reflects the structure of IHL itself. Many prohibitions are tied not to the weapon per se, but to its foreseeable effects in context. Review authorities may therefore approve a capability subject to restrictions on use, impose operational parameters (such as target type, distance, or environment), or require technical or procedural safeguards prior to deployment. These conditions must be translated into operational frameworks if the review is to have practical effect.

This process often requires developing weapon – or capability-specific normative instruments, which define the conditions under which a system may be lawfully employed. The Swiss system provides a particularly clear illustration of this approach. The legal review is conducted in multiple stages: an initial assessment at the procurement intent stage, a second review once a specific system has been identified, and a third review when the operational regulation governing the weapon is drafted. During this process, the reviewing authority specifies the legal conditions for approval – including requirements relating to weapon characteristics, testing, and permissible use – and works in coordination with procurement authorities to ensure that these conditions are reflected in the design and implementation of the system. While comparable approaches may exist in other systems, available information remains limited. Nevertheless, this model illustrates a coherent and structured method for translating legal assessments into operational practice and provides a useful reference for states seeking to implement Article 36 obligations.

The outcome of this process is typically formalized in military weapon regulations and manuals, which constitute the primary instruments through which legal constraints are operationalized. Such regulations define how the weapon may be used in practice, including parameters such as permissible targets, engagement distances, safety requirements, and other operational limitations. They serve as binding reference documents within the armed forces and are used for training and instruction, thereby ensuring that operators understand and internalize legal constraints.

Other instruments, such as manuals or technical guidance, may complement this framework by providing additional detail or interpretation, although they may not always have the same binding status. Similarly, rules of engagement (ROE) play an important role, but their function is more limited and context specific. ROE regulate the use of force within a particular operation and may incorporate or reflect constraints identified during legal reviews; however, they typically operate within the parameters already established by weapon-specific regulations, rather than defining those parameters themselves. In this sense, ROE and operational directives impose legal constraints in specific operational contexts, but do not replace the underlying normative framework governing the lawful use of the capability.

The translation of conditional approval into practice is further reinforced through training and operational preparation. Weapon regulations and associated constraints are incorporated into training programmes, simulation environments, and certification processes, ensuring that operators understand not only how a system functions, but also the legal conditions under which it may be used. In this way, legal constraints become part of operational practice rather than abstract assessments.

This model highlights a broader structural point: the legality of a weapon is not determined at the moment of review, but by the extent to which the conditions identified in that review are embedded in doctrine, regulation, and practice. The effectiveness of Article 36 therefore depends not only on the quality of the legal assessment, but also on the integrity of the mechanisms through which its conclusions are operationalized.

At the same time, translating conditions of approval into stable regulatory instruments becomes more complex in the context of emerging and digital technologies. Where system behaviour is adaptive, or where effects depend on evolving operational environments, it may be more difficult to stabilize conditions of lawful use within fixed regulatory instruments. This may require more flexible approaches, including iterative review, closer integration between legal and technical actors, and the development of dynamic operational constraints.

The addressees of review conditions are not always military personnel, reachable through weapon regulations, doctrine, and training. States increasingly contract private military and security companies and other private actors to operate, maintain, update, or sustain military capabilities – functions that may bring contractor personnel close to direct participation in hostilities and create oversight gaps that facilitate misuse or unlawful use if left unaddressed. Where a capability is to be operated or maintained, entirely or partially, by private contractors, the approval conditions of must be integrated into the contract governing the service: contractual clauses should specify the conditions of lawful use, impose obligations to report deviations and incidents, and preserve the state's ability to remove particular contractor personnel or to terminate the contract in the event of violations or non-compliance. The Montreux Document's good practices – on contractual clauses and performance requirements ensuring respect for IHL, on rules of

conduct (including the use of force), and on control arrangements over contractor personnel during contract performance – provide some transposable guidance. Addressing these questions as part of the legal review helps identify appropriate safeguards early and reduces the risk of future legal gaps.

Operational implication: Conditional approval should not be treated as the endpoint of the legal review, but as the starting point for its operationalization. States should ensure that the conditions attached to legal approval are systematically translated into binding or authoritative instruments governing the use of the capability, communicated effectively to public and private operators, and, as appropriate, embedded in contractual arrangements, training, and operational practice. The legality of a capability ultimately depends on whether these conditions are not only identified, but also implemented and enforced in practice.

8. Governance, transparency, and system management

Article 36 implementation depends on more than the existence of a review authority or the conduct of individual assessments. It also requires governance arrangements capable of ensuring consistency, institutional memory, accountability, and continuity over time. Because weapons reviews often involve sensitive technical and operational information, governance of the review system must balance confidentiality with the need for record-keeping, internal traceability, and appropriate transparency. This section therefore examines four system management functions: record-keeping, transparency and information sharing, capacity building, and the management of resource constraints.

Record-keeping

Record-keeping is a core governance function of an Article 36 review mechanism. Legal reviews should not exist only as isolated opinions attached to individual procurement files. Instead, they should form part of a structured institutional archive, enabling the reviewing authority to track prior determinations, conditions attached to approvals, the technical assumptions relied upon, and later modifications or changes in use.

The ICRC guide emphasizes record-keeping as important for consistency and institutional memory, particularly where a later review concerns a modified version of a previously reviewed weapon. It notes that some states require permanent files of legal reviews and that at least one state is subject to general archival obligations. Australia provides a concrete example: a review management team is responsible for tracking review progress and maintaining records, while the legal reviewer's work is subject to secondary review before approval.

Record-keeping also supports life-cycle governance. Where a capability is modified, used in a new operational context, or raises concerns after deployment, earlier review files allow the state to identify what was previously assessed and whether the factual basis of the original determination remains valid.

Operational implication: Review mechanisms should maintain a secure and searchable archive of review requests, supporting documentation, legal determinations, conditions of approval, and subsequent modifications or reassessments.

Transparency and information sharing

Transparency and information sharing in the context of Article 36 implementation are characterized by a notable absence of formalized obligations or institutionalized mechanisms. Unlike other areas of arms control or disarmament law, states are not required to report on their review processes, share outcomes, or participate in peer review. As a result, transparency has developed in practice through a combination of informal, decentralized, and practice-driven mechanisms.

A useful distinction may be drawn between the transparency of procedures and the transparency of outcomes. In relation to procedures, Article 84 of Additional Protocol I provides a limited basis for information sharing, requiring states parties to communicate their implementation measures to one another upon request. In practice, however, systematic exchanges are rare, and no centralized repository of national review frameworks exists. Instead, knowledge sharing has emerged through a dispersed set of platforms and initiatives.

Multilateral expert discussions provide one such avenue. In particular, the UN Group of Governmental Experts (GGE) on Lethal Autonomous Weapons Systems (LAWS) has served as a recurring forum in which states set out national positions and, at times, refer to their Article 36 review practices. Although these discussions do not focus exclusively on weapons reviews, they contribute to a gradual convergence of views on how existing legal obligations apply to emerging technologies.¹⁸

A second channel is constituted by expert-led and practice-oriented initiatives. In the absence of formal intergovernmental coordination, organizations such as Article 36 Legal have played an important role in facilitating exchanges among government lawyers, technical experts, and industry actors.¹⁹ Initiatives such as the ‘Lawful by Design’ and ‘Responsible by Design’ processes provide platforms for discussing how legal requirements can be integrated into the development and review of military technologies, particularly in relation to AI-enabled systems and dual-use innovation. These processes are notable for extending the discussion beyond purely legal analysis to include technical and industrial perspectives. An analogous institutional model exists in the field of private military and security regulation: the Montreux Document Forum provides a standing venue in which national regulatory authorities of participating states share implementation experience and exchange good practice – a precedent that could inform future arrangements for structured exchange among weapons review authorities.

¹⁸ Legal reviews have featured prominently in the GGE LAWS process. In the chair’s summary of the first 2026 session, legal reviews are included as a specific element in Box IV of the rolling text, alongside voluntary exchange of relevant practices between states. The summary also records broad support for the paragraph on legal reviews and the voluntary exchange of best practices. See ‘Chair’s Summary – First 2026 Session of the GGE on LAWS, CCW/GGE.1/2026/WP.2’, 1 April 2026, paras. 58 , 61.

¹⁹ See Copeland, Damian and Rain Liivoja, ‘Progressing the Legal Review of Autonomous Weapon Systems: Report of an Expert Meeting (Geneva, 10–11 March 2025)’ (Asia-Pacific Institute for Law and Security, September 2025).

A third, and particularly influential, mechanism is the development of guidance and soft-law instruments. The ICRC's 2006 *Guide to the Legal Review of New Weapons* remains the principal reference point for states, providing a common analytical framework for conducting reviews. Work is currently underway to update this guidance in light of developments in emerging technologies. While such instruments are not legally binding, they play a significant role in shaping expectations of good practice and in promoting a degree of functional convergence across otherwise diverse national systems.

Taken together, these mechanisms illustrate a broader structural feature of Article 36 implementation: transparency operates through an informal ecosystem of information sharing, rather than through formalized or institutionalized arrangements. This facilitates the exchange of experience and the gradual development of common approaches, but does not ensure consistency, comparability, or accountability across states.

Transparency in relation to review outcomes remains considerably more limited. In most systems, the results of legal reviews are treated as confidential, reflecting the sensitivity of the technical, operational, and commercial information involved. Against this background, the Netherlands provides a rare example of partial transparency in practice.

Box 5: The Netherlands – a model of transparency in Article 36 implementation

The Netherlands provides one of the most developed examples of transparency and information sharing in relation to Article 36 reviews. This is achieved through the work of the AIRCW, whose recommendations are, in part, made publicly available.

The AIRCW is a high-level advisory body within the Ministry of Defence, composed of senior representatives of the defence establishment – including the Commander of the Armed Forces (chair), the Director of Legal Affairs, and senior policy, materiel, and medical officials. It is supported by a multidisciplinary working group drawing on operational commands and technical expertise. The committee assesses whether new means and methods of warfare – understood broadly to include both lethal and non-lethal capabilities, as well as modifications of existing systems – comply with international law. The final decision on approval rests with the Minister of Defence, who may authorize use with or without conditions.

A distinctive feature of the Dutch system is the publication of selected AIRCW recommendations in accordance with the Public Information Act (Wet openbaarheid van bestuur, Wob). To date, at least 27 advisory opinions have been made publicly available, covering a wide range of capabilities – including non-lethal weapons (such as tasers and acoustic devices),

small arms ammunition, precision-guided munitions, artillery systems, and specialized equipment.²⁰

The published material reveals a dual approach to transparency, combining both capability-specific reviews and framework-level recommendations. Most published opinions relate to specific weapons or systems and include structured legal assessments addressing technical characteristics, intended use, applicable legal frameworks, medical and environmental considerations, and comparative analysis. These opinions frequently impose conditions or limitations on use, providing insight into how legal conclusions are translated into operational constraints.

The AIRCW has also issued framework recommendations addressing broader categories of means and methods of warfare – including, for example, cyber capabilities and loitering munitions. These do not assess a single system, but instead set out general legal considerations, applicable principles, and parameters for future reviews. This approach enables the sharing of legal reasoning and interpretative frameworks without disclosing sensitive technical or operational details.

An additional feature of the Dutch approach is the systematic omission of personal identifiers, including the names, signatures, and contact details of individual reviewers or officials involved in the assessment process. In a number of published opinions, this appears to be the primary or sole form of redaction, with the substantive legal reasoning, structure of the analysis, and overall conclusions remaining largely intact. This measure reflects a deliberate effort to balance transparency with confidentiality: while institutional roles, legal reasoning, and review outcomes are disclosed to a significant extent, individual attribution is withheld. Such an approach helps protect personnel, preserves space for internal deliberation, and reduces potential external pressure on reviewers, while ensuring that transparency is tied to the system rather than to individual decision-makers.

Taken together, the two elements produce a balanced form of transparency. Capability-specific opinions provide concrete examples of how legal reviews are conducted in practice, while framework recommendations offer a higher level of abstraction that can guide interpretation in emerging or sensitive domains. At the same time, the system preserves confidentiality through the redaction of commercially or operationally sensitive information, as well as through the discretionary selection of opinions for publication. The result is a structured but incomplete form of transparency, which balances openness with security considerations.

²⁰ Ministerie van Defensie, 2026. 'Adviescommissie Internationaal Recht en Conventioneel Wapengebruik (AIRCW)', Rijksoverheid, accessed 5 May 2026.

From a policy perspective, the Dutch approach demonstrates that meaningful transparency in Article 36 implementation is feasible without creating undue security risks. In particular, combining detailed but partially redacted opinions with higher-level framework recommendations provides a practical method for sharing legal approaches while protecting sensitive information. This model may therefore serve as a useful reference for states seeking to enhance information sharing and confidence building in the implementation of Article 36, while maintaining control over sensitive capabilities.

Publication material of this kind remains exceptional, and the sensitivity of review material will preclude most states from following this approach. A state can, however, be open about how it conducts reviews without being disclosing what it decides. Even where outcomes must stay confidential, the framework – including the legal basis, the responsible body, the triggers for review, and the procedural steps – can be published with redactions where necessary to protect national security and commercial confidentiality. Accountability may also be pursued through reporting to parliamentary bodies on the functioning of the review system rather than on individual determinations. Parliamentary oversight is largely absent from current Article 36 practice, but combining the publication of redacted applicable regulations and procedures with oversight by parliamentary bodies, including through annual reporting, is well established in the regimes governing private military and security services, and merits consideration in the governance of national review systems.

Capacity building

Effective implementation of Article 36 requires not only a formal review mechanism, but also the availability of personnel capable of conducting legally and technically reliable assessments. This includes expertise in IHL, as well as the ability to engage with complex technical information and to understand operational contexts in which capabilities are developed and used. Capacity building is therefore a core enabling condition for the functioning of national review systems.

At the national level, publicly available examples of structured capacity building remain limited. Australia provides one of the clearest illustrations, where the Department of Defence, through the Directorate of Operations and International Law, has introduced a certification course for military legal officers responsible for conducting Article 36 reviews. Launched in 2023, this programme takes the form of a one-day training course, structured around both legal and practical components.²¹ It combines instruction with practical exercises and assessment to

²¹ Goussac, Netta et al, 'Enhancing the Legal Review of Autonomous Weapon Systems: Report of an Expert Meeting (Sydney, 28–30 March 2023)' (Brisbane: Law and the Future of War Research Group, University of Queensland, May 2023), p. 6.

ensure competence in conducting legal reviews. This reflects a broader emphasis on developing applied, practice-oriented expertise, rather than purely theoretical knowledge, in order to enable legal reviewers to operate effectively within procurement and operational contexts.

In practice, capacity building in this area is not organized through a single institutional framework but operates through a distributed ecosystem of expert-led initiatives. Training programmes are delivered through a combination of international organizations, academic institutions, specialized organizations, and governmental partners. Notably, institutions such as the International Institute of Humanitarian Law (IIHL), as well as academic partners, host dedicated courses on weapons law and Article 36 review. The Geneva Centre for Security Policy (GCSP) has previously played a significant role in this area through executive-level training programmes, while more recent initiatives increasingly involve collaboration across institutions and expert networks.

Within this ecosystem, specialized organizations – such as Article 36 Legal – deliver targeted training courses, workshops, and expert roundtables focused specifically on Article 36 implementation, engaging with both governmental and non-governmental stakeholders. More recent initiatives, such as the ‘Five-Eyes Article 36 Legal Review Course’ – delivered in collaboration with governmental partners, further reflect a growing emphasis on interoperability and shared practice among states.

Across these initiatives, several common functions can be identified. First, they provide foundational knowledge of weapons law, including the applicable treaty framework, customary international law principles, and the scope of the Article 36 obligation. Second, they develop practical skills for conducting legal reviews, including analysing weapon effects, meeting evidentiary requirements, and preparing review reports. Third, they address emerging challenges, including the review of AI-enabled systems, cyber capabilities, and other new technologies. Finally, they facilitate peer exchange and convergence of practice, allowing participants to compare national approaches and develop shared understandings of review methodologies.

The emphasis across these initiatives is consistently practice-oriented. Training typically combines lectures with case studies, scenario-based exercises, and group work, enabling participants to apply legal principles to concrete technical and operational contexts. This reflects the nature of Article 36 review as a function operating at the intersection of law, technology, and military operations, and therefore impossible to implement effectively through doctrinal knowledge alone.

At the same time, capacity building is not limited to those directly responsible for conducting legal reviews. Procurement officials, engineers, testing authorities, and operational personnel require sufficient awareness of Article 36 obligations to identify when a review is required, provide relevant information, and implement any conditions attached to legal approval. Without such broader institutional awareness, even well-designed review mechanisms may fail to operate effectively in practice.

Operational implication: States should approach capacity building as a systemic requirement, combining specialized training for legal reviewers with broader awareness raising across procurement, technical, and operational actors. Engagement with the wider ecosystem of training initiatives –including those led by specialized organizations such as Article 36 Legal and institutions such as IIHL – may provide an effective means of developing capacity, particularly where national programmes are not yet fully established.

Managing resource constraints

Resource limitations are a recurring challenge in the implementation of Article 36 review mechanisms, particularly for states with limited technical infrastructure, small legal services, rapidly expanding procurement portfolios, or ongoing operational pressures. These challenges may be especially acute in the context of emerging technologies, where legal reviews increasingly require access to specialized technical expertise, testing infrastructure, and interdisciplinary assessment capabilities. At the same time, resource constraints do not remove or diminish the obligation under Article 36. Rather, they require states to adopt organizational and procedural approaches that allow available resources to be used efficiently while preserving the reliability and independence of legal assessments. In practice, state experience and expert guidance suggest that resource management should focus not on lowering legal standards, but on improving prioritization, workflow integration, institutional cooperation, and access to expertise. Several practical approaches may assist states in managing resource constraints while maintaining effective review systems.

Structuring and prioritizing the review process

- **Risk-based and differentiated approaches to review pathways:** States may adopt differentiated approaches to review pathways depending on the characteristics and legal risk profile of the capability under assessment. Not every review requires the same depth of analysis of all possible legal issues. The scope and intensity of assessment should depend on the nature of the capability, its intended operational use and foreseeable effects, and the legal questions it raises. For example, certain ammunition types may primarily require analysis under the prohibition of superfluous injury or unnecessary suffering, whereas autonomous or AI-enabled systems may necessitate a broader assessment relating to predictability, controllability, distinction, proportionality, or human supervision. Resource allocation and review intensity may therefore legitimately differ depending on the complexity, novelty, and legal risk profile of the capability concerned.

- **Escalation and reassessment mechanisms:** States adopting simplified or accelerated review pathways should also establish mechanisms requiring the review to be escalated to a more comprehensive assessment where relevant circumstances change. This may include software or functionality updates, operational modifications, integration into new systems, deployment in different operational environments, emergence of new evidence, or situations in which uncertainty remains following the preliminary assessment. Such mechanisms may be particularly important for software-modifiable, AI-enabled, or adaptive systems whose behaviour may evolve over time.
- **Prioritization and sequencing of reviews:** Where review demand exceeds available institutional capacity, states may prioritize assessments according to operational urgency, deployment timelines, procurement schedules, or the potential humanitarian and legal risks associated with the capability. Such prioritization may assist in allocating limited resources more effectively, provided that no capability proceeds to operational use prior to completion of the required legal assessment.

Box 6: Reliance on prior reviews conducted by other states

Prior legal reviews conducted by other states may provide useful supporting information and reduce unnecessary duplication of technical testing or analytical work within national Article 36 processes. This may be particularly relevant where capabilities are acquired through transfer, multinational procurement, coalition cooperation, licensed production, or foreign military assistance programmes. Depending on the circumstances, prior reviews may assist by providing:

- technical weapon data and testing results;
- information regarding weapon effects and operational characteristics;
- legal analysis and interpretation;
- testing methodologies and evidentiary standards;
- conditions or limitations attached to prior approval; or
- examples of review structure and methodology.

At the same time, Article 36 obligations remain the obligations of the reviewing state itself. A prior foreign review may inform but cannot replace an independent national legal determination conducted by the receiving state. The receiving state must therefore independently assess whether the capability would be prohibited under international law in the context of its own intended acquisition, integration, and use. This is particularly important because legality assessments may depend not only on the characteristics of the capability itself, but also on national doctrine, intended operational use, operational environment, technical configuration, system integration, and national interpretations of international law.

Accordingly, where a state takes into account prior foreign reviews, it should, at a minimum, independently determine:

- whether the capability being acquired corresponds to the version previously reviewed, including hardware configuration, software version, subsequent modifications, and integrated components;
- whether the technical information underlying the prior review is sufficiently complete, accessible, and independently verifiable;
- whether testing data, methodologies, and operational assumptions remain reliable and relevant for the receiving state's intended use;
- whether the capability has been modified, adapted, or integrated into new operational systems in a manner that could affect the legal assessment;
- whether the intended operational use differs from the context considered in the original review;
- whether any conditions, limitations, or restrictions attached to the original approval have been fully communicated and can be implemented nationally;
- whether additional national testing, technical analysis, or operational evaluation is required;
- whether the receiving state's treaty obligations, ROE, operational doctrine, or interpretations of international law differ in ways that could affect the legality assessment.

Where the legal review depends on technical examination or weapons testing, the receiving state should not rely solely on another state's testing conclusions without independent verification. While prior testing data and methodologies may provide valuable support, the reviewing state should ensure that any technical testing necessary for its own legal assessment is conducted, supervised, validated, or otherwise independently evaluated as part of the national review process.

Particular caution may be required where the prior review is unavailable in full, the underlying technical or testing data cannot be accessed, or the legal reasoning supporting the original conclusion cannot be independently evaluated. Similarly, greater caution may be needed for AI-enabled systems, software-modifiable capabilities, cyber tools, or integrated multi-component systems, where functionality may evolve over time or depend heavily on operational context, data inputs, or system integration. In such cases, reliance solely on prior foreign legal conclusions without access to underlying technical information or independent verification may create significant legal and operational risks.

Prior foreign reviews should therefore be understood as supporting material within a broader national assessment process. While these reviews may reduce duplication of technical testing or analytical work and assist states in accessing expertise or information that would otherwise be difficult to obtain independently, they cannot substitute for the receiving state's own responsibility to determine whether the capability would be prohibited under international law in the circumstances of its intended use.

Capacity, expertise, and institutional cooperation

Expansion of institutional expertise: Resource constraints may be mitigated by expanding the number of personnel capable of supporting the review process. While legal advisers remain central to the conduct of Article 36 reviews, effective implementation also depends on the awareness and participation of procurement officials, engineers, operational planners, testing authorities, cyber specialists, AI experts, and technical personnel. Capacity building may therefore include modular training programmes, practical exercises, online learning tools, and interdisciplinary workshops.

- **Flexible use of multidisciplinary expertise:** Effective legal reviews require access to multidisciplinary expertise, including legal, technical, operational, medical, cyber, or environmental specialists – depending on the nature of the capability under assessment. Resource-efficient systems do not necessarily require all experts to participate in every review, however. In practice, many review mechanisms operate through a core review structure supplemented by ad hoc consultation with additional specialists where particular legal or technical issues arise. A flexible model such as this may reduce administrative burdens while still ensuring that relevant expertise is available when required. States with limited permanent staffing may also consider regional or inter-institutional expert-sharing arrangements, enabling access to specialized expertise without maintaining large standing review bodies.
- **Use of external expertise and institutional support:** External actors may assist states in strengthening review capacity, including by providing technical analysis, legal advisory support, training programmes, templates and checklists, or methodological guidance. Relevant actors may include partner states, universities, specialized technical laboratories, international organizations, and institutions such as IIHL, DCAF – Geneva Centre for Security Sector Governance, Article 36 Legal, the Responsible by Design Institute, or the ICRC. Such organizations offer capacity-building training that may help develop or strengthen national legal review processes. This type of cooperation may enhance institutional resilience and facilitate access to expertise that may not exist domestically. The final legal determination must, however, remain with the reviewing state.

- **Pooling technical infrastructure and testing resources:** Certain forms of legal review require highly specialized technical testing or evaluation that may exceed national institutional capacity. States may therefore benefit from shared testing facilities, pooled technical infrastructure, regional cooperation arrangements, or accredited external laboratories and technical centres. Such cooperation may be particularly useful for blast and fragmentation testing, AI reliability and predictability assessments, cyber resilience evaluations, environmental impact analysis, or the testing of autonomous systems. Even where testing is conducted externally, the reviewing state should retain oversight of the testing methodology, operational assumptions, interpretation of data, and legal conclusions ultimately drawn from the results.

Integration with procurement and capability development

- **Early-stage legal filtering and acquisition guidance:** Integrating legal reviews into procurement and capability development processes from the outset can significantly reduce problems later on. Legal screening during concept development, acquisition planning, or technical specification phases can prevent investment in legally problematic systems and reduce the need for costly redesigns or reassessments at later stages. This may include the use of standardized information requirements, the provision of legal guidance for procurement authorities, and the early identification of capability categories likely to raise heightened legal concerns. Engaging with the private sector developing military technology in order to communicate the legal requirements and information necessary to conduct a legal review may also form part of these efforts.
- **Ensuring review-relevant information from developers:** States and procurement authorities should, to the extent possible, communicate relevant IHL and international law review requirements to developers, suppliers, and industry partners at an early stage. The aim is not to require capabilities to be designed for legal review, but to ensure that developers understand what information the reviewing authority will need to assess legality. This may include technical specifications, intended and reasonably foreseeable uses, testing and validation data, performance limitations, failure modes, update history, version control, audit logs, human control features, explainability or interpretability information, and safeguards affecting operational behaviour. Identifying these information requirements at an early stage can not only help developers generate and preserve review-relevant evidence, but also reduce uncertainty, delay, and duplication during the legal review or reassessment. This is particularly important for AI-enabled, software-defined, cyber, networked, or adaptive systems, where legality may depend on functionality, testing, updates, constraints, and operational configuration.

Standardization, workflow management, and information systems

- **Standardized documentation and review templates:** Administrative burdens may be reduced through the use of standardized review templates, structured questionnaires, common reporting formats, and predefined information requirements. Such tools may improve consistency, reduce duplication, facilitate peer review, and support continuity despite personnel rotation or long procurement cycles. At the same time, templates should remain sufficiently flexible to accommodate differing levels of technical complexity and legal risk.
- **Digital workflow systems and review databases:** Digital workflow and record-management systems may significantly improve the efficiency and resilience of review mechanisms. Such systems can facilitate the submission and tracking of review requests, management of supporting documentation, coordination among participating actors, storage of legal opinions and technical testing data, and identification of systems requiring reassessment following modification or software updates. Searchable databases of prior reviews may also support institutional memory, promote consistency across assessments, and reduce duplication of analysis where similar capabilities are reviewed over time. This may be particularly important where procurement cycles extend over many years, systems undergo iterative modification, or personnel rotate frequently within defence institutions.

How to conduct an Article 36 legal review

Available state practice demonstrates a significant degree of convergence in the overall structure of Article 36 review processes. While states employ different institutional arrangements, terminology, and levels of procedural formalization, review processes generally follow a series of identifiable phases: determining whether review is required; defining the object and scope of assessment; collecting and analysing relevant information; applying the applicable legal framework; determining the outcome of the review; and translating any conditions or limitations into operational practice.

State practice from countries such as Australia, France, Switzerland, and Ukraine illustrates the various ways in which these stages may be organized in practice. Australia's 2024 guidance provides one of the clearest examples of a structured review methodology, with the following distinct steps: preliminary assessment; information gathering; assessment of specific and general prohibitions; consideration of policy factors; and an additional functional review for AI-enabled or autonomous systems. France similarly adopts a staged approach, beginning with preliminary screening to determine whether a capability falls within the scope of Article 36 review, followed by a more detailed legal assessment where required. Switzerland likewise follows a staged review process integrated across successive procurement and acquisition stages. The Swiss system begins with a preliminary assessment identifying whether a review is required and which legal questions are potentially concerned, followed by subsequent review stages linked to the identification of a specific product, technical testing, drafting of weapon regulations, and final approval decisions. Ukraine's emerging framework similarly reflects a structured and sequential approach, incorporating a preliminary assessment of whether a weapon falls within the scope of review, the collection of technical and operational information through standardized questionnaires, an additional functional assessment for autonomous systems, and formalized documentation of review outcomes through a dedicated information and communication system.

Taken together, these approaches suggest several common features of contemporary Article 36 practice. First, the legal review is increasingly structured as a sequential process rather than a single isolated legal opinion, with different forms of assessment taking place at different stages of acquisition, testing, integration, and operational preparation. Second, effective review processes increasingly integrate legal analysis into technical and operational assessments, recognizing that determining the legality of many capabilities requires not only abstract legal interpretation but also an understanding of the capability's design, effects, reliability, and intended use in practice. Finally, emerging technologies – including AI-enabled, autonomous, software-based, and multifunction systems – have led a number of states to supplement traditional weapon-based assessments with more granular functional analysis directed at specific system capabilities or operational functions. The following section proposes a structured approach for conducting Article 36 reviews based on common elements found in available state practice and expert guidance.

Box 7: The functional approach – from presumption of lawful use to demonstrated compliance

A functional approach is an analytical method for reviewing complex military capabilities whose legal significance cannot be adequately assessed by examining the system only as a single, integrated platform. It is particularly relevant for AI-enabled, autonomous, cyber, software-defined, networked, adaptive, or multifunction systems, where different functions may perform distinct operational roles and raise different legal questions.²² The approach has been developed most explicitly in relation to autonomous weapon systems. Damian Copeland argues that the traditional legal review process focuses primarily on the legality of the weapon per se and may be insufficient in cases where an autonomous system performs functions governed by IHL targeting rules. Where a system is designed to interpret data, interact with its environment, or make decisions or recommendations relevant to the use of force, the review must assess whether those functions can be performed in accordance with the reviewing state's international legal obligations.²³

A functional approach does not establish a separate legal regime for emerging technologies. Nor does it replace the ordinary Article 36 review. Instead, it is a way of applying existing international law more precisely. The reviewing authority must still assess the capability against specific prohibitions, general IHL rules, and any other applicable international law. The functional approach assists the reviewer in identifying which functions are legally relevant, what evidence is required, what operational context must be considered, and

²² See Boulanin, Vincent, 'Implementing Article 36 Weapon Reviews in the Light of Increasing Autonomy in Weapon Systems', Stockholm International Peace Research Institute (SIPRI) Insights on Peace and Security No. 2015/1 (Stockholm: SIPRI, November 2015), p. 9.

²³ See Copeland, Damian, 'A Functional Approach to the Legal Review of Autonomous Weapon Systems', *International Humanitarian Law Series*, Vol. 72, Brill/Nijhoff (2024), ch 7.

whether particular safeguards, human control requirements, use restrictions, or reassessment triggers are necessary.

In practical terms, the approach may assist the reviewing authority in determining whether the capability as a whole requires review, or whether the legally significant issue lies in a particular function, subsystem, software capability, operational mode, or use case. It may also help distinguish legally relevant functions from administrative, logistical, maintenance, or support functions that do not independently affect the conduct of hostilities.

The functional approach should therefore be understood as a cross-cutting method within the Article 36 review. It may inform preliminary screening, the definition of the object and scope of review, evidentiary collection, substantive legal assessments, operational context assessments, and life-cycle reassessments. It is most relevant where a capability contains functions that directly affect targeting, attack planning, application of force, cyber effects, or other legally significant aspects of military operations.

The analytical foundation of the functional approach rests on the same presumption as that of traditional weapon reviews: that a human operator will use the weapon lawfully. Based on that presumption, the review concentrates on the legality of the weapon per se – weapons law – and does not determine compliance with the rules governing the conduct of particular attacks – that is, targeting law, which addresses distinction, proportionality, and precautions in attack. Compliance with these rules remains the responsibility of commanders and operators at the point of use. Some national systems accordingly limit the formal Article 36 assessment to weapons law requirements, addressing compliance with targeting law through separate operational, doctrinal, and training processes.

For autonomous and AI-enabled capabilities, this presumption does not apply to any function the system performs that is governed by IHL. Where a system, rather than its operator, identifies, classifies, selects, or engages targets – or materially shapes those judgements – lawful use can no longer simply be presumed and left to the point of employment. For such functions, the review must determine, rather than presume, that the system can perform the function in compliance with the applicable targeting rules within the operational contexts for which it is intended.

The functional review in Step 6 gives effect to this shift: for IHL-relevant functions, it examines demonstrated performance – reliability, predictability, controllability, and the quality of human control – rather than extending the presumption of lawful use to machine-executed judgements. Seen in this light, the functional approach is not an optional addition but the logical consequence of the Article 36 obligation when applied to systems that take decisions previously made by human operators.

9. Preliminary identification

The first phase of the review process involves determining whether review is required, identifying the object under review, and establishing the factual and technical basis necessary for the legal assessment. These preliminary stages are particularly important because they shape the scope, depth, and focus of the subsequent legal analysis.

Step 1: Preliminary assessment to establish whether the review is required

The first stage of the review process involves determining whether the capability in question falls within the scope of Article 36 of Additional Protocol I and thus requires a legal review. This preliminary determination is essential because not all military-related technologies, systems, or equipment necessarily constitute ‘weapons, means, or methods of warfare’ within the meaning of Article 36. The reviewing authority must therefore identify whether the capability is sufficiently connected to the conduct of hostilities to trigger the obligation of review.

At this stage, the focus is not on legality but on whether the capability is subject to review. The determination should be guided by the national definition of ‘new weapons, means, or methods of warfare’, if one exists, which often reflects the capability’s intended military purpose and foreseeable operational use, as well as how it relates to the application of force or other hostile effects during armed conflict. In practice, this involves asking two questions: whether the capability constitutes a weapon, means, or method of warfare; and whether it is ‘new’ for the reviewing state (including through acquisition, material modification, or proposed new operational use). Identifying the norms of reference – the rules by which the reviewing state is bound – at this stage frames the subsequent assessment.

The reviewing authority may therefore consider questions such as:

- Is the capability intended for use in the conduct of hostilities?
- Is it capable of causing injury, death, destruction, disruption, or other operational effects during armed conflict?
- Is the capability designed to support, facilitate, or directly influence attacks or other military operations?
- Does the capability constitute a weapon, means, or method of warfare under the reviewing state’s interpretation of Article 36?
- Is the capability dual-use in nature and, if so, does its military application nevertheless require review?

- Does the capability merely provide administrative or logistical support, or does it affect operational military functions relevant to hostilities?
- Is the capability new, newly acquired, materially modified, or proposed for a new operational use that may alter its legal assessment?

In practice, this stage may be particularly significant for cyber capabilities, AI-enabled systems, software-defined technologies, and multifunction platforms, where the boundaries between civilian, commercial, and military functions can be less apparent than in traditional weapon systems. The review authority should therefore adopt a sufficiently flexible and technologically neutral approach capable of accommodating emerging technologies while remaining anchored in the object and purpose of Article 36.

State practice demonstrates different ways in which this preliminary filtering function may be operationalized. Australia treats the initial determination of whether review is required as a threshold assessment conducted on a case-by-case basis by the Directorate of Operations and International Law. France similarly applies a preliminary screening stage examining whether the capability qualifies as a weapon, means, or method of warfare; whether it is new; and whether it is intended for use in armed conflict. Switzerland likewise incorporates an initial assessment stage to determine whether a review is required and which legal questions are potentially concerned by the capability under consideration. Ukraine's draft framework also contains a preliminary determination stage, during which the Comprehensive Assessment Commission assesses whether the weapon sample requires a comprehensive assessment under Article 36 obligations and whether a full assessment is mandatory, unnecessary, or recommended.

Step 2: Define the object under review and intended use

After establishing that a capability falls within the scope of Article 36, the reviewing authority must define the object under review and identify the capability's intended and foreseeable operational uses. This stage establishes the analytical framework for the remainder of the review process and is particularly important for emerging technologies whose architecture, software configuration, or operational effects may evolve over time.

The object under review should be defined with sufficient precision to allow meaningful legal assessment. Depending on the nature of the capability, the object under review may be an individual weapon, platform, software capability, subsystem, operational module, or broader military system. The reviewing authority should avoid definitions that are either excessively narrow, thereby overlooking important legal aspects, or excessively broad, thereby obscuring the specific functions giving rise to legal concerns. While Article 36 does not prescribe how the object under review is to be framed, defining it carefully is good practice to ensure the assessment addresses the legally relevant functions and uses.

For certain complex, modular, software-defined, AI-enabled, or autonomous systems, the object under review may not necessarily encompass the entire platform or system. In some circumstances, the legally relevant element may instead be a specific function, subsystem, software capability, or operational use case. Functional identification at this stage may therefore assist reviewers in distinguishing between components or functions that directly affect the conduct of hostilities and those that do not require equivalent legal assessment.

The reviewing authority should also identify the capability's intended operational purpose as well as reasonably foreseeable uses and misuses, including its intended targets, operational environment, anticipated effects, foreseeable operational limitations, and reasonably foreseeable misuse risks. Such considerations may significantly affect the subsequent legality assessment, particularly where the capability's effects, reliability, or controllability vary depending on the context in which it is used. This assessment is important because the legality of many technologies depends on not only their technical characteristics, but also the manner in which they are expected to be employed during military operations. That includes considering who will operate, maintain, and sustain the capability: private actors are involved both upstream (in the development, production, and commercialization of new capabilities) and, increasingly, downstream (in the operation and maintenance of fielded systems). The definition of foreseeable operational use should reflect any such delegation.

The review may therefore consider questions such as:

- What precisely constitutes the object under review?
- Is the review directed at an entire system, a subsystem, a software capability, or a specific operational function?
- What military purpose is the capability intended to serve? (for example, to defeat personnel, disable materiel, protect forces, identify or track targets, support attack planning, disrupt communications, deny access, or produce crowd control/force protection effects)
- What targets is the capability intended or expected to engage? (for example, enemy personnel, armoured vehicles, drones, aircraft, vessels, command-and-control systems, communications infrastructure, weapon systems, sensors, buildings, or cyber infrastructure)
- In what operational environments is the capability expected to operate?
- What effects is the capability designed or expected to produce?
- Under what operational conditions is the capability expected to be used? (for example, open terrain, urban areas, maritime or air environments, contested electromagnetic spectrum, degraded communications, low visibility, adverse

weather, proximity to civilians or civilian objects, protected sites, or mobile/ time-sensitive targets)

- Does the capability possess autonomous, adaptive, modular, or multifunction characteristics?
- How will the capability achieve its intended effect?
- Are there foreseeable operational uses beyond those originally intended?
- Are there foreseeable operational limitations affecting reliability or controllability?
- Are there reasonably foreseeable misuse scenarios or unintended operational consequences?
- Could degraded operational conditions alter system behaviour or legal risk?
- Could future software modifications, updates, or integration with other systems alter the capability's legal assessment?
- Does the capability depend upon interaction with external data, networks, sensors, or third-party systems?
- Will the capability be operated, maintained, or updated – entirely or partially – by private military and security contractors? If so, will contractor personnel perform functions of legal significance – for example, target recognition, mission-planning support, model retraining, or operation of the weapon system itself – with the attendant implications for state oversight and for the status of those personnel under IHL?

This stage is particularly important for emerging technologies because many contemporary military systems no longer operate as static or self-contained platforms. They may instead involve evolving software architectures, machine-learning components, distributed networks, cloud-based processing, or integration across multiple systems and operators. Clearly defining the object and intended use of the review is therefore essential to ensure that subsequent legal analysis remains both technically accurate and operationally meaningful.

State practice further illustrates the importance of defining both the object and the operational context of review. Switzerland distinguishes between reviews of entire systems and more limited reviews focused on specific components, such as ammunition, thereby tailoring the scope of the assessment to the capability under consideration. Australia similarly requires reviewers to assess the capability's functions, intended uses, anticipated effects, damage mechanisms, and targeting characteristics, as well as evidence demonstrating that the capability functions accurately and effectively under expected operational conditions.

Step 3: Collect and verify the evidentiary basis

An effective legal review depends upon the availability of sufficient factual, technical, operational, and legal information concerning the capability under assessment. The reviewing authority must therefore establish and verify an adequate evidentiary basis capable of supporting informed legal analysis. Without reliable information regarding the capability's characteristics, functioning, operational environment, and foreseeable effects, the review risks becoming purely abstract or speculative.

The information required will vary depending on the nature and complexity of the capability under review. In many cases, the review authority may need to obtain technical documentation, manufacturer or developer information, testing results, operational concepts, engineering assessments, risk analyses, and expert input from military operators, engineers, scientists, medical personnel, or external specialists. Information regarding comparable or previously reviewed systems may also assist reviewers in contextualizing the assessment, particularly where the capability represents a modification or evolution of an existing technology.

The evidentiary basis may therefore include:

- technical descriptions and design documentation;
- manufacturer, developer, or supplier information;
- testing data and performance evaluations;
- operational concepts and intended patterns of use;
- information regarding comparable systems or previously reviewed capabilities;
- safety and reliability assessments;
- input from medical, environmental, technical, or scientific experts where relevant;
- information regarding software architecture, autonomy functions, or data-processing systems; and
- classification, security, proprietary, or confidentiality considerations relevant to information handling.

For AI-enabled,²⁴ autonomous, cyber, or multifunction systems, the evidentiary basis may also need to be collected and assessed on a function-specific basis. Different operational functions may raise distinct legal concerns and therefore require separate technical evaluation, testing, or operational analysis. In such

²⁴ Boothby identifies a detailed set of information likely to be required for the legal review of AI-enabled or AI-enhanced weapons, means, or methods of warfare. This includes the following: the technical characteristics and intended effects of the system; the radius of effect, wounding mechanism, intended circumstances, and method of use; testing results concerning accuracy, reliability, performance, wounds, and failure rates; environmental impact; the exact role and functions of AI in the system; the reliability and accuracy with which AI performs those functions; the testing applied to the AI, including whether testing reflects all intended circumstances of use; the transparency of AI processes to the user; robustness against external interference and cyber vulnerabilities; whether the system uses machine learning or deep learning; whether the lessons available for the AI to learn are constrained; whether those constraints support compliance with targeting law; and whether relevant risks and vulnerabilities have been sufficiently addressed to ensure proper system performance. See Boothby, Bill, 'AI Warfare and the Law', *International Law Studies*, Vol. 104, Stockton Center for International Law, U.S. Naval War College (2025), pp. 136-38.

cases, reviewers may need information regarding specific software functions, autonomy parameters, training data (including the provenance, representativeness, and quality of data – which needs to be sufficient to enable the assessment of bias risks), human-supervision mechanisms, reliability metrics, fail-safe measures, cybersecurity vulnerabilities, or operational constraints relevant to the legally significant function under assessment.

The review may therefore require information regarding:

- which functions are capable of affecting targeting or attack decisions;
- levels of autonomy or automation associated with specific functions;
- predictability and reliability under operational conditions;
- human supervision, intervention, or override mechanisms;
- testing methodologies and operational validation procedures;
- software modification, retraining, or update processes;
- cybersecurity vulnerabilities or adversarial manipulation risks;
- foreseeable failure modes and safeguard mechanisms; and
- expected effects on military objectives, civilians, civilian objects, or the environment.

At this stage, the reviewing authority should also assess whether the available information is reliable, adequate, and of sufficient quality. Where uncertainty remains substantial, additional testing, operational evaluation, or expert consultation may be necessary before proceeding further. This is particularly important for technologies whose behaviour may vary depending on the operational context, data inputs, interaction with external systems, or environmental conditions.

State practice further demonstrates the importance of structured evidentiary collection within the review process. Australia's guidance explicitly emphasizes that the quality of the legal review depends upon the relevance, quality, and quantity of information provided to reviewers. It places responsibility on the requesting authority to provide all relevant available information necessary to conduct the assessment. Ukraine's emerging framework similarly operationalizes this stage through structured questionnaires addressing technical characteristics, target type, accuracy, safeguards, autonomy functions, civilian risk mitigation measures, health effects, and environmental impacts.

10. Legal assessment

Once the capability has been identified, the object and scope of review defined, and the evidentiary basis collected, the reviewing authority must proceed to the substantive legal assessment. The purpose of this phase is to determine whether the capability would be prohibited under applicable international law, either inherently or in relation to its normal or reasonably foreseeable use.

State practice demonstrates different ways in which this stage may be structured. In some systems, particularly where the capability raises relatively limited or clearly identifiable legal concerns, the review may focus only on the specific legal questions raised by the capability. For example, certain ammunition types may primarily require assessment under the prohibitions relating to superfluous injury or unnecessary suffering, non-detectable fragments, or expanding bullets, without necessitating extensive analysis of broader targeting-related rules. Switzerland's staged review process illustrates this more targeted approach, where preliminary review phases may identify the principal legal questions raised by the capability at an early stage and focus subsequent analysis accordingly.

At the same time, available state practice also demonstrates the importance of maintaining a sufficiently structured and systematic methodology, particularly for more complex, multifunctional, or emerging technologies. Australia's 2024 guidance provides one of the clearest examples of such an approach, structuring the substantive assessment around three principal layers of analysis: first, an assessment of specific prohibitions and restrictions applicable to the capability; second, an assessment under the general prohibitions and principles of IHL; and third, consideration of broader policy, soft-law, and national constraints. This layered approach is particularly useful for ensuring that the review remains comprehensive without becoming mechanically over-inclusive.

The following section therefore proposes a structured approach to substantive legal assessment based on converging elements found in available state practice and expert guidance. While the depth and sequencing of analysis may vary depending on the characteristics of the capability under review, the framework below reflects a coherent methodology capable of accommodating both traditional weapon systems and emerging technologies.

Step 4: Assess specific prohibitions and restrictions

The first stage of substantive legal analysis should determine whether the capability falls within the scope of any existing regime specifically prohibiting or restricting particular categories of weapons, means, or methods of warfare. The purpose of this stage is to identify capabilities that are already expressly prohibited or specifically regulated under international law before proceeding to a broader

assessment under the general principles of IHL. This stage therefore functions as a threshold legal screening to determine whether the capability corresponds to a specifically regulated category of weapon, means, or method of warfare. In many cases, this assessment may be relatively straightforward and may allow the reviewing authority to reach conclusions without requiring more extensive analysis under the general rules governing the conduct of hostilities. The sequence is not prescribed: some national systems assess the general prohibitions and principles (Step 5) first and then turn to specific regimes; what matters is that both stages of analysis are completed.

The review may therefore consider questions such as:

- Does the capability fall within the scope of a treaty prohibiting or restricting a specific category of weapon, means, or method of warfare?
- Is the reviewing state party to the relevant treaty regime? (This will normally have been established when identifying the applicable norms in Step 1.)
- Has the reviewing state made any reservations, interpretative declarations, or national implementation modifications relevant to the application of the treaty?
- Does the capability contain prohibited or specifically regulated components, payloads, or effects?
- Are there restrictions relating to development, acquisition, stockpiling, transfer, deployment, or use?
- Are there operational restrictions that apply only in particular circumstances or to certain categories of targets?
- Does the capability require compliance with specific technical requirements established under international law?
- Are there relevant customary international law rules that may prohibit or restrict the capability or its expected use?

Relevant treaty frameworks and specific prohibitions applicable at this stage are discussed in the ‘Applicable legal framework’ section in Part 1 and summarized chronologically in the reference table in Part 4.

For emerging technologies, this stage may not always yield definitive answers because many contemporary capabilities do not correspond neatly to pre-existing categories established in treaty law. Nevertheless, conducting this threshold assessment remains important because it allows clearly prohibited capabilities to be identified at an early stage of the review process and ensures that the subsequent analysis under general principles remains analytically structured.

In practice, some states may also take into account relevant national policy positions, military doctrine, non-binding international instruments, or public statements concerning emerging technologies when conducting Article 36 reviews.

This may be particularly relevant in areas such as autonomous weapon systems, AI-enabled capabilities, or cyber operations, where states have increasingly expressed positions on issues such as human control, predictability, reliability, accountability, or responsible military use of AI in international fora. While such considerations do not independently determine legality under IHL, they may nevertheless influence national review practice, operational limitations, procurement decisions, or conditions attached to approval.

Step 5: Assess general prohibitions and restrictions

Where the capability is not specifically prohibited or restricted under a dedicated treaty regime, the reviewing authority should proceed to assess whether the capability's normal or reasonably foreseeable use would nevertheless be prohibited under the general rules and principles of IHL governing the conduct of hostilities. This stage constitutes the core substantive legality assessment within most Article 36 review processes. The assessment is conducted based on the normal or planned use of the capability in foreseeable and ordinary operational scenarios – in all circumstances or in specific cases – including its intended doctrine of use. Unlike the previous stage, which focuses on specifically regulated categories of weapons, means, or methods of warfare, this assessment examines whether the capability's characteristics, effects, or foreseeable operational use align with the broader principles and rules governing the conduct of hostilities. In many cases, the legality of a capability will depend not only on its technical design, but also on the manner in which it is expected to function in operational practice.

This stage may be structured around the following questions, each anchored in the rule or rules indicated:

- Is the capability of a nature to cause superfluous injury or unnecessary suffering? (Additional Protocol I, Article 35(2); Customary IHL Rule 70)

Box 8: Superfluous injury and unnecessary suffering

Article 35(2) of Additional Protocol I prohibits the use of ‘weapons, projectiles and material and methods of warfare of a nature to cause superfluous injury or unnecessary suffering’. The rule is customary (Rule 70) and has been identified by the International Court of Justice as one of the ‘cardinal’ principles of IHL.²⁵ It is one of the few rules of IHL that shields combatants, the protection of civilians being addressed by the principle of distinction and the rules covered in the questions below.²⁶ The test is objective and focused on the capability’s normal or expected use and design characteristics: it prohibits weapons whose innate characteristics would inflict injury or suffering beyond what is necessary to render an adversary hors de combat – in the court’s formulation, ‘a harm greater than that unavoidable to achieve legitimate military objectives’. The assessment therefore weighs the nature and severity of foreseeable injury against the military utility the weapon is designed to achieve. Relevant evidential factors include the mechanism of injury; wound severity and treatability; the inevitability of serious permanent disability or death; and comparison with existing lawful weapons with comparable military effects.²⁷ Both ‘superfluous’ and ‘unnecessary’ are comparative rather than absolute concepts,²⁸ and the comparison is most naturally made with the weapon or means the capability is intended to replace: does the new capability foreseeably inflict graver injury – such as larger or less treatable wounds, higher mortality, or a greater incidence of permanent disability – without a corresponding gain in military effectiveness?

Findings of per se unlawfulness on this basis are rare,²⁹ and the rule has historically operated as the driver of specific treaty prohibitions – for example, on weapons causing injury by non-detectable fragments and on blinding laser

²⁵ Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), adopted 8 June 1977, entered into force 7 December 1978, 1125 UNTS 3, art. 35(2); Henckaerts, Jean-Marie and Louise Doswald-Beck, eds., ‘Customary International Humanitarian Law, Volume I: Rules’ (Cambridge: ICRC/Cambridge University Press, 2005), Rule 70; ICJ (International Court of Justice), ‘Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion’, ICJ Reports (1996), para. 78, which describes the prohibition as one of the ‘cardinal principles’ of IHL and defines unnecessary suffering as ‘a harm greater than that unavoidable to achieve legitimate military objectives’.

²⁶ Casey-Maslen, Stuart and Steven Haines, ‘Hague Law Interpreted: The Conduct of Hostilities under the Law of Armed Conflict’ (Oxford: Hart Publishing, 2018), pp. 22, 208; Bellal, Annysa and Stuart Casey-Maslen, ‘The Additional Protocols to the Geneva Conventions in Context’ (Oxford: Oxford University Press, 2022), para. 12.13.

²⁷ See ICRC, ‘Customary International Humanitarian Law’ commentary on Rule 70, which identifies ‘the inevitability of serious permanent disability’ among the relevant factors; ICRC, A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977 (Geneva: ICRC, 2006), pp. 17–18.

²⁸ Boothby, Bill, ‘Weapons and the Law of Armed Conflict’ (Oxford: Oxford University Press, 2009), p. 62 (‘both adjectives, “unnecessary” and “superfluous”, are comparative, not absolute, concepts’). See also United Kingdom Ministry of Defence, ‘Joint Service Manual of the Law of Armed Conflict’, Joint Service Publication 383 (2004), para. 6.2: the criterion is whether use of a weapon ‘is of a nature to cause injury or suffering greater than that required for its military purpose’.

²⁹ Kalshoven, Fritz and Liesbeth Zegveld, ‘Constraints on the Waging of War: An Introduction to International Humanitarian Law’, 3rd edn. (Geneva: ICRC, 2001), pp. 41–42, which describes the rule as ‘too vague to produce by itself a great many practical results’; Bellal, Annysa and Stuart Casey-Maslen, ‘The Additional Protocols to the Geneva Conventions in Context’ (Oxford: Oxford University Press, 2022), para. 12.13, which notes the absence of consensus among states and commentators as to which weapons the rule prohibits.

weapons.³⁰ It does not follow that the question carries little practical weight in review. Because Article 36 applies precisely to capabilities for which no specific regime yet exists, this is the rule most likely to be engaged by a genuinely novel wounding mechanism, and the design stage is the point at which the question can still be acted upon. In practice, the rule generally leads to design constraints, information requirements, or conditions on use rather than a finding of unlawfulness. Medical and wound-ballistics expertise will often be required to apply it reliably, and the review report should record the evidential basis on which any conclusion rests.³¹

The ICRC SIrUS project and medical effects criteria: Confronted with the difficulty of determining which weapons are of a nature to cause superfluous injury or unnecessary suffering, in the mid-1990s the ICRC convened the SIrUS project, which proposed four alternative evidence-based criteria drawn from field data on weapon effects: (1) specific disease, specific abnormal physiological or psychological state, specific and permanent disability, or specific disfigurement; (2) field mortality of more than 25 per cent or hospital mortality of more than 5 per cent; (3) 'Grade 3' wounds as measured by the ICRC wound classification (large wounds); or (4) effects for which there is no well-recognized and proven treatment.³²

The project was criticized – in particular for omitting the military use aspect of the legal equation – and was withdrawn by the ICRC in 2001.³³ The SIrUS criteria therefore do not reflect the legal test. They do, however, remain a useful reference for structuring the collection and assessment of medical and wound-ballistics evidence in review practice, provided any conclusion is reached by applying the legal standard – which balances foreseeable injury against military utility – rather than the criteria alone.

- Are the capability's effects inherently indiscriminate? (Additional Protocol I , Article 51(4); Customary IHL Rules 11-13)
- Can the capability be directed at a lawful military objective? (Additional Protocol I, Articles 48 and 52(2); Customary IHL Rules 1 and 7)

³⁰ Protocol on Non-Detectable Fragments (Protocol I to the CCW), adopted at Geneva, 10 October 1980, entered into force 2 December 1983; Protocol on Blinding Laser Weapons (Protocol IV to the CCW), adopted at Vienna, 13 October 1995, entered into force 30 July 1998. On the derivation of the blinding laser prohibition from the superfluous injury rule, see ICRC, 'Customary International Humanitarian Law', commentary on Rule 70.

³¹ ICRC, 'A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977' (Geneva: ICRC, 2006), pp. 17-18.

³² Coupland, R. M., ed., 'The SIrUS Project: Towards a Determination of Which Weapons Cause 'Superfluous Injury or Unnecessary Suffering'' (Geneva: ICRC, 1997), p. 23.

³³ The principal criticism – that the criteria addressed injury and suffering to the near exclusion of military utility – was raised at the ICRC Meeting of Experts on the SIrUS Project, Geneva, 10–11 May 1999; the ICRC announced the withdrawal of the project in January 2001. See Daoist, Isabelle, 'ICRC Expert Meeting on Legal Reviews of Weapons and the SIrUS Project', *International Review of the Red Cross*, Vol. 83: No. 842 (June 2001), pp. 539-42; Bellal, Annysa and Stuart Casey-Maslen, 'The Additional Protocols to the Geneva Conventions in Context' (Oxford: Oxford University Press, 2022), paras. 12.20-12.23.

Box 9: Inherently indiscriminate weapons

Article 51(4)(b) and (c) of Additional Protocol I prohibits as indiscriminate attacks employing a method or means of combat that ‘cannot be directed at a specific military objective’ or whose effects ‘cannot be limited’ as required by the protocol, and which are consequently ‘of a nature to strike military objectives and civilians or civilian objects without distinction’. A weapon that systematically breaches either prohibition is inherently indiscriminate and may not be used; the prohibition is customary (Rule 71) and derives from the principle of distinction.³⁴ The first part concerns the ability to direct the weapon at a specific military objective with sufficient reliability (the ‘accuracy’ limb); the second concerns effects that, once the weapon is directed, cannot be adequately limited (the ‘effects’ limb – for example, due to the uncontrollable spread of fire, disease, or malicious code).

Here, too, the threshold is high, and the assessment is contextual: a weapon need not be capable of pinpoint accuracy to be lawful.³⁵ A capability that can be directed at specific military objectives in some circumstances – for example, area targets such as troop concentrations in open terrain – is not inherently indiscriminate, even if particular uses (such as employment against point targets in populated areas, or firing at the extreme of range) would be indiscriminate and unlawful. The distinction is illustrated, albeit imperfectly, by the International Criminal Tribunal for the former Yugoslavia’s treatment of the M-87 Orkan multiple rocket launcher in *Martić*: fired into Zagreb from the extreme of its range, the weapon was held incapable of hitting specific targets in those circumstances, and the Appeals Chamber clarified that the Trial Chamber had concluded that the Orkan ‘was used as an indiscriminate weapon’. The case is therefore better interpreted as a finding about the weapon’s employment at that range than as a ruling that the weapon was unlawful per se in all uses.³⁶

International law sets no fixed numerical accuracy standard;³⁷ dispersion or circular-error-probable data must be assessed against intended target sets, engagement ranges, and operational environments. Where lawful employment is possible only within a defined envelope, the appropriate outcome will usually be conditional approval, confining use to that envelope, rather than a finding of unlawfulness per se.

³⁴ Additional Protocol I, art. 51(4)(b) and (c); Henckaerts, Jean-Marie and Louise Doswald-Beck, eds., ‘Customary International Humanitarian Law, Volume I: Rules’ (Cambridge: ICRC/Cambridge University Press, 2005), Rule 71.

³⁵ US Department of Defense, ‘Law of War Manual’, Washington, DC (June 2015, updated December 2016), para. 6.7.2: ‘[I]f the weapon could be directed at specific areas [that constitute military objectives], it would be unlikely that the weapon would be considered inherently indiscriminate.’

³⁶ Prosecutor v. Milan Martić, Case No. IT-95-11-T, Judgement (Trial Chamber I), 12 June 2007, paras. 462-63; Prosecutor v. Milan Martić, Case No. IT-95-11-A, Judgement (Appeals Chamber), 8 October 2008, paras. 247-48.

³⁷ Bellal, Annyssa and Stuart Casey-Maslen, ‘The Additional Protocols to the Geneva Conventions in Context’ (Oxford: Oxford University Press, 2022), para. 12.25, which notes ‘a particular lack of clarity as to how inaccurate a weapon must be before its use is always unlawful’ and that military manuals offer little guidance; United Kingdom Ministry of Defence, ‘Joint Service Manual of the Law of Armed Conflict’, Joint Service Publication 383 (2004), para. 6.4.

- Can the capability's effects be sufficiently limited in time, geography, and scale? (Additional Protocol I, Articles 51(4)-(5); Customary IHL Rules 11-13)
- Does foreseeable use create unreasonable risks of civilian harm or damage to civilian objects? (Additional Protocol I, Articles 51 and 57; Customary IHL Rules 14-24)
- Could the capability foreseeably cause widespread, long-term, and severe damage to the natural environment? (Additional Protocol I, Articles 35(3) and 55; Customary IHL Rules 43-45)
- Does the capability remain sufficiently predictable, reliable, and controllable under expected operational conditions? (derived from the obligation to comply with distinction, proportionality, and precautions in attack)
- Can operators understand, supervise, and appropriately manage the capability's functioning during use? (derived from the obligation to ensure compliance with distinction, proportionality, and precautions in attack)
- Do foreseeable operational conditions create unacceptable risks of malfunction, escalation, or unintended effects? (derived from customary obligations relating to precautions and indiscriminate attacks)
- Could interaction with external systems, degraded environments, or adversarial interference compromise lawful use? (derived from obligations relating to distinction, precautions, and control of effects)
- Will the capability be operated by private actors and, if so, have sufficient safeguards and appropriate restrictions been established to ensure effective state oversight and to prevent misuse? (derived from the state's obligation to respect and ensure respect for IHL; delegating operation to private contractors may otherwise create oversight gaps – see the Montreux Document)

This assessment should focus on the capability's normal or reasonably foreseeable use rather than on purely hypothetical or abusive uses detached from operational reality. At the same time, the reviewing authority should take into account foreseeable misuse risks, technical limitations, operational stress, degraded environments, and other circumstances that may realistically affect the capability's behaviour during military operations.

Foreseeable effects should also be assessed carefully to examine how they are distributed across the civilian population. The effects of certain weapons differ between women and men– documented, for example, in relation to chemical, biological, nuclear, and explosive weapons, including effects on pregnant women – and impacts on civilians and civilian objects differ according to gendered patterns of life; reverberating effects may likewise be gendered. Sex – and age-

disaggregated data, where available, strengthens the reliability of the assessment of foreseeable effects and of civilian harm.³⁸

The rules considered at this stage, together with the specific prohibitions examined in Step 4, will resolve most reviews. Where a capability raises concerns that those rules do not fully capture, the reviewing authority may also need to consider the Martens Clause.

Box 10: Martens Clause

The Martens Clause provides that, in cases not covered by specific treaty rules, civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, the principles of humanity, and the dictates of public conscience. In its contemporary form, the clause is reflected in Article 1(2) of Additional Protocol I.³⁹ In an Article 36 review, the Martens Clause should not be treated as a substitute for the ordinary legal assessment required under specific weapons treaties and general IHL rules. The reviewing authority must first assess whether the capability is prohibited or restricted by applicable treaty law, customary international law, or the general prohibitions.

The Martens Clause is nevertheless relevant where a new weapon, means, or method of warfare raises concerns that are not fully addressed by existing specific rules. Its precise legal effect is debated: it may be understood narrowly, as an interpretive aid in applying existing rules, or more broadly, as a source of normative guidance in cases where positive law is incomplete or uncertain.⁴⁰ For this reason, the clause should be applied carefully and transparently in legal review practice.

In practical terms, the Martens Clause may assist the reviewing authority in identifying residual concerns arising under the principles of humanity or the dictates of public conscience, interpreting existing rules in light of their protective object and purpose, and determining whether additional safeguards, operational restrictions, senior-level review, or national policy limitations are required. Its relevance may be particularly important for novel technologies or

³⁸ See, for example, Tengroth, Cecilia, 'Should Gender Considerations Impact the Legal Review of New Weapons?', in Cecilia Tengroth and Kristina Lindvall, eds., 'IHL and Gender' (Stockholm: Swedish Red Cross, 2015), p. 115 ff; UNIDIR (United Nations Institute for Disarmament Research), 'Missing Links: Understanding Sex – and Gender-Related Impacts of Chemical and Biological Weapons', (Geneva: UNIDIR, 2021); UNIDIR, 'Gender and Ionizing Radiation: Towards a New Research Agenda Addressing Disproportionate Harm' (Geneva: UNIDIR, 2024); ICRC, 'Explosive Weapons with Wide Area Effects: A Deadly Choice in Populated Areas' (25 January 2022).

³⁹ Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), adopted 8 June 1977, entered into force 7 December 1978, art. 1(2). See also ICRC, 'A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977' (Geneva: ICRC, 2006), p. 17.

⁴⁰ ICJ (International Court of Justice), 'Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion', ICJ Reports (1996), paras. 78, 84, 87.

methods of warfare whose effects or modes of operation were not specifically anticipated when existing weapons rules were developed.

Where the Martens Clause is considered, the review report should distinguish clearly between conclusions based on binding treaty or customary law and any additional considerations based on the principles of humanity, the dictates of public conscience, national policy, or emerging legal developments. This distinction is important to preserve the legal discipline of the review and to avoid presenting contested or policy-based considerations as if they were settled prohibitions under international law.⁴¹

For emerging technologies, this stage may raise particularly complex questions relating to predictability, reliability, explainability, human-machine interaction, software adaptation, autonomy, or operational control. In the context of AI-enabled or autonomous systems, the review may therefore need to assess not only physical effects, but also the capability's decision-making functions, supervision mechanisms, operational constraints, and ability to function lawfully in realistic operational environments.

Similarly, cyber capabilities may raise questions concerning indirect, delayed, reverberating, or geographically dispersed effects, including effects on civilian infrastructure or interconnected systems extending beyond the immediate operational target environment.

Step 6: Apply a functional review approach where appropriate

Certain technologies may require the reviewing authority to supplement traditional system-level assessments with more granular functional analyses. This may be particularly relevant for AI-enabled systems, autonomous systems, cyber capabilities, software-defined technologies, multifunction platforms, or highly modular systems whose legality depends not solely on the capability as a whole but on the behaviour, interaction, or operational role of specific functions.

Traditional Article 36 review methodologies were primarily developed in relation to relatively discrete weapon systems whose effects could largely be assessed through their physical characteristics and expected operational effects. Emerging technologies increasingly challenge this assumption. Many contemporary systems operate through distributed software architectures, adaptive algorithms, data-driven processes, networked interactions, or modular subsystems that may perform legally

⁴¹ See expert concerns about the inclusion of the Martens Clause and non-legal considerations in legal reviews in Goussac, Netta et al, 'Enhancing the Legal Review of Autonomous Weapon Systems: Report of an Expert Meeting' (Sydney, 28–30 March 2023) (Brisbane: Law and the Future of War Research Group, University of Queensland, May 2023), p. 13.

distinct functions within the same broader capability. In such cases, reviewing the system solely as a single integrated capability may fail to capture the functions that are legally relevant to the conduct of hostilities. A functional approach therefore seeks to identify and assess those specific functions that directly affect the application of force, targeting processes, attack planning, operational decision-making, or other legally significant aspects of military operations.

The purpose of a functional approach is not to create a separate legal regime for emerging technologies, but rather to ensure that existing international legal obligations can be meaningfully applied to technologies whose operational behaviour may depend upon specific software functions, autonomy parameters, data-processing systems, or interactions between human operators and machine processes.

A functional approach may therefore be particularly relevant where:

- the capability contains autonomous or semi-autonomous functions;
- different subsystems perform legally distinct operational roles;
- the system relies upon AI-enabled decision-support functions;
- the capability performs targeting, classification, prioritization, or attack planning functions;
- software updates or retraining may alter operational behaviour over time;
- the capability depends upon external data, sensor fusion, cloud-based processing, or networked interaction;
- the system's legality depends heavily on the context of use or operational configuration;
- different operational modes create different legal risks; or
- interaction between subsystems may generate emergent or unpredictable effects.

Under a functional approach, the reviewing authority may therefore assess not only the capability as a whole, but also specific operational functions relevant to compliance with international law in the context of particular operational scenarios.

The review may therefore consider questions such as:

- Which functions directly affect the conduct of hostilities?
- Which functions influence targeting, attack decisions, or the application of force?
- Can legally relevant functions be distinguished from administrative or logistical functions?
- Do different functions raise different legal risks?
- Does lawful operation depend upon specific safeguards, constraints, or human supervision?

- Could software adaptation, retraining, or updates alter legally relevant behaviour?
- Could interactions between subsystems produce unintended or insufficiently predictable effects?
- Are operators capable of understanding, supervising, and controlling legally relevant functions under realistic operational conditions?

Not all systems incorporating AI, software automation, or digital functionality necessarily require a full functional review. In many cases, administrative, logistical, maintenance, or support functions may not independently raise legal concerns under Article 36. Conversely, functions directly affecting targeting, attack planning, force application, or operational decision-making may require particularly detailed scrutiny even where they form only one component of a larger system. A functional approach may therefore assist reviewing authorities in avoiding both under-inclusive and excessively broad assessments by focusing analysis on those functions that are legally relevant to the conduct of hostilities.

Where a functional review is undertaken for an autonomous or AI-enabled capability, its focus is the software – including any AI models – that interprets data and enables the system’s autonomous functionality. Given the centrality of that software to the lawful operation of the weapon, the functional review may precede the traditional review steps; alternatively, where an existing weapon is enhanced by AI, the functional review will be the primary focus of the reassessment, drawing on the review completed when the weapon was originally acquired.

A structured functional review may proceed through eight elements. For each IHL-relevant function, the reviewing authority should:

- identify the governing IHL rule(s);
- identify the standard of compliance required;
- identify the operational context(s) in which the function will be performed;
- obtain the technical, functional, and performance data;
- conduct a legal risk analysis across realistic use scenarios;
- determine the appropriate level of human control;
- confirm lines of human responsibility; and
- assess trust, by determining reliability, predictability, and explainability.

The analytical tools in Part 4 – in particular the functional assessment matrix, the operational context assessment tool, and the technical information request template – support each of these elements.⁴²

⁴² The eight-element functional review methodology reflects the approach proposed by Damian Copeland in his expert review of this Guide (2026); see also Boulanin, Vincent, ‘Implementing Article 36 Weapon Reviews in the Light of Increasing Autonomy in Weapon Systems’, Stockholm International Peace Research Institute (SIPRI) Insights on Peace and Security No. 2015/1 (Stockholm: SIPRI, November 2015).

For AI-enabled and software-defined capabilities, reviewing authorities need not generate all of this evidence themselves. Emerging AI assurance methodologies – including risk management and life-cycle frameworks, as well as system – or assurance-card approaches under which developers and defence institutions jointly document evidence of legal compliance, performance under realistic and contested conditions, known system limits, and supply-chain integrity in a single auditable record – can provide much of the structured evidence on which a functional review depends. Such frameworks complement rather than replace the legal review: they do not make the legal determination but define what evidence is needed, in what form, and who should have access to it, including legal advisers and future reviewers. Reviewing authorities may specify this type of assurance documentation as part of their standing information requirements, and consider validation against worst-case and contested operational conditions – rather than performance in controlled testing – as the relevant evidentiary benchmark.⁴³

This approach may be particularly important for AI-enabled decision-support systems, autonomous targeting functions, cyber capabilities, and multifunction systems whose legality cannot be assessed solely through traditional platform-based analysis. State practice increasingly reflects this development. Australia's 2024 guidance expressly incorporates additional functional assessments for AI-enabled and autonomous systems, while Ukraine's emerging review framework similarly includes dedicated assessment forms addressing autonomy-related functions within complex and software-enabled capabilities.

Box 11: Data quality, bias, and intersectional risks in AI-enabled systems

For AI-enabled, autonomous, and data-driven military systems, the legality of a capability may depend not only on its intended effects, but also on the quality, representativeness, reliability, and operational relevance of the data and models on which the system relies. In such systems, flaws in data sets, modelling assumptions, training environments, or algorithmic processes may directly affect compliance with IHL. Bias in AI-enabled systems may arise when the data used is incomplete, unrepresentative, historically skewed, or lacking sufficient context. Such risks may be particularly acute where systems rely upon pattern recognition, behavioural profiling, target identification, threat classification, civilian harm estimation, or decision-support functions. Particular risks may also arise where data sets or operational models insufficiently account for differentiated patterns of civilian presence and vulnerability, including those relating to sex, gender, age, disability, ethnicity, language, or child-specific patterns of life. Bias may further evolve over time

⁴³ Muhammedally, Sahr, 'The Preparation Gap: IHL, Human–Machine Teaming and Assurance in Military AI Systems' (Geneva: ICRC, 2026), pp. 1–33, which proposes a 'Human–Machine Teaming Assurance Card' integrating legal, technical, operational, and civilian-harm considerations into a single evidentiary standard across the AI life cycle, and surveying the NIST AI Risk Management Framework, the IEEE Autonomous and Intelligent Systems life-cycle framework, and the Alan Turing Institute's Defence AI Assurance methodology as structural reference points.

through operational deployment, retraining, software updates, or interaction with changing operational environments.⁴⁴

From an Article 36 perspective, these issues are legally relevant where they affect the ability of the system to comply with obligations relating to distinction, proportionality, precautions in attack, or meaningful human judgement and control. For example, biased data sets or flawed modelling assumptions may contribute to:

- systematic over-identification of certain demographic groups as combatants;
- failure to detect civilians or civilian objects;
- inaccurate estimation of civilian harm;
- discriminatory or disproportionate targeting outcomes;
- unreliable identification of protected persons;
- increased risks of false positives or false negatives;
- degraded system performance in unfamiliar operational environments; or
- erosion of meaningful human supervision through automation bias.

Experts have specifically warned that AI-enabled systems may reproduce or amplify existing societal and operational biases – including gender-related bias – particularly where demographic proxies or incomplete data sets shape assessments of civilian presence, patterns of life, or anticipated harm.⁴⁵ Concerns have also been raised regarding the over-identification of military-aged men as combatants, the failure to account for culturally specific civilian behaviour, or the invisibility of certain civilian populations within operational data sets.

Special consideration may additionally be required regarding the effects of AI-enabled systems on children. Expert discussions have highlighted that many civilian harm assessment methodologies remain calibrated primarily around adult populations and may inadequately account for the differentiated physical, developmental, psychological, and reverberating effects of military operations on children.⁴⁶ Age-insensitive data, along with behavioural proxies and target-identification models, may fail to adequately recognize child-specific patterns of life, civilian activities, or vulnerabilities. This may be particularly relevant in relation to systems used for target identification, behavioural analysis, pattern-of-life assessments, urban operations, or estimations of civilian

⁴⁴ DCAF, 'Operationalising IHL in AI-Enabled and Autonomous Military Systems: Gender and WPS as Enablers of Lawful Use' (Geneva: DCAF and Canadian Red Cross, 2026).

⁴⁵ Chandler, Katherine, 'Does Military AI Have Gender? Understanding Bias and Promoting Ethical Approaches in Military Applications of AI' (Geneva: UNIDIR, 2021).

⁴⁶ See, for example, Hazelwood, Jessica and Nicoll, Claire 'Not Mini-Civilians: The Legal Obligations towards Children as Children in Armed Conflict', *International Review of the Red Cross* (2026), pp. 1-49, p. 30, which notes that AI models are generally trained on adult-oriented data sets and may therefore misidentify children as adults or fail to recognize their civilian status.

harm. Reviewing authorities may therefore need to assess whether relevant systems appropriately account for child-specific risks, including through age-disaggregated data, contextual operational testing, and safeguards against the misidentification or invisibility of children within operational data sets.

Reviewing authorities should therefore consider whether the capability is based on:

- sufficiently representative, contextually relevant, and operationally validated data sets, including sex-, age-, and context-disaggregated information where relevant;
- transparent or sufficiently explainable model architecture and decision-making processes;
- verifiable testing, validation, and red-teaming procedures;
- mechanisms to identify, monitor, and mitigate bias;
- safeguards against automation bias and over-reliance on system outputs;
- safeguards against discriminatory or systematically skewed targeting outcomes affecting particular demographic groups, including women, men, children, minorities, or other vulnerable populations;
- meaningful human supervision, override, contextual assessment, and operational challenge mechanisms; and
- feedback, reassessment, and operational learning mechanisms following deployment and use.

Particular attention may be required where systems are expected to operate in complex civilian environments, including densely populated urban areas, non-international armed conflicts, or contexts where civilian and combatant status may be difficult to distinguish. The legality of such systems may depend heavily on context-specific reliability, predictability, explainability, and quality of human oversight.

A gender-responsive and intersectional approach does not create new legal obligations under IHL. Instead, it may assist reviewing authorities in identifying foreseeable operational risks, improving civilian harm assessments, strengthening precautionary measures, and ensuring that AI-enabled systems can realistically be used in compliance with existing international legal obligations.

Step 7: Determine the outcome of the review

At the conclusion of the legal assessment, the reviewing authority should determine whether the capability may be lawfully developed, acquired, adopted, or used under applicable international law. The review outcome should be clearly documented and communicated to the relevant procurement, development, and operational actors. In the majority of national systems (such as that of France), the review concludes with a finding of conformity (closing the examination), partial conformity (requiring modification of part of the system or its doctrine of use), or non-conformity.

Possible review outcomes may include:

- lawful/approved;
- lawful subject to conditions or limitations;
- approval subject to additional testing or information;
- approval subject to technical modification or safeguards;
- restricted to specified operational contexts or methods of use;
- temporary suspension pending reassessment; or
- unlawful/not approved.

Where the legality of a capability is subject to conditions of use, the reviewing authority should specify those conditions with sufficient precision to enable their operational implementation.

Such conditions may relate to:

- permissible targets;
- operational environments;
- levels of human supervision or control;
- technical safeguards;
- reliability thresholds;
- software configuration;
- data limitations;
- civilian harm mitigation measures;
- testing or certification requirements; or
- restrictions on autonomous functions or operational modes.

For AI-enabled, autonomous, software-defined, or adaptive systems, the reviewing authority should also determine whether future software updates, retraining, integration into other systems, or changes in operational context may require reassessment prior to continued use.

Operational implication: Review outcomes should be formulated in a way that allows direct operational implementation and integration into procurement, doctrine, training, and operational planning processes.

Step 8: Document the review and communicate implementation requirements

The review process and its conclusions should be formally documented in order to ensure traceability, institutional memory, accountability, and effective implementation of the review outcome.

Review documentation should normally include:

- identification of the capability reviewed;
- scope and object of the review;
- intended and foreseeable operational use;
- technical and evidentiary basis;
- testing and evaluation data;
- applicable legal framework;
- legal analysis and reasoning;
- assumptions and operational limitations relied upon;
- identified risks and uncertainties;
- conclusions and review outcome;
- conditions or restrictions attached to approval; and
- requirements for reassessment or further review.

Where relevant, the reviewing authority should also communicate implementation requirements to the relevant authorities responsible for procurement, doctrine, training, testing, and operational use.

Implementation measures may include:

- incorporation of legal limitations into weapon regulations;
- operational restrictions or concepts of employment;
- training and certification requirements;
- technical safeguards or system constraints;
- procurement conditions and contractual requirements;
- testing, monitoring, or validation obligations;
- procedures for software updates or modification approval; and
- triggers for reassessment following modification, operational feedback, or new use.



Practical tools for legal reviewers and committee members

This section provides practical tools to support the conduct of Article 36 legal reviews in a structured, consistent, and practical manner. The tools are intended for legal reviewers, members of review bodies, and supporting technical, operational, medical, environmental, procurement, and testing personnel involved in the assessment of new weapons, means, or methods of warfare. They translate the methodology set out in the preceding section into usable instruments for screening, information collection, legal analysis, functional assessments, documentation, reassessments, and training.

The tools do not create a separate legal standard and should not be applied mechanically. They are instead designed to assist reviewers in identifying the scope and depth of assessment required in a particular case to ensure that relevant evidence is collected, that legal questions are addressed systematically, and that any conditions attached to approval are communicated in a form capable of implementation. Depending on the nature of the capability under review, some tools may be used in full, while others may be applied only in part. A limited review, full review, reassessment, or full review including functional assessment all remain forms of Article 36 legal review; the difference lies in the focus, evidentiary requirements, and analytical depth required to reach a legally reliable determination.

11. Review process tools

The following tools support the initial organization and routing of Article 36 reviews. They are designed to help reviewing authorities determine whether a capability should enter the review process, identify the appropriate review pathway, and situate the assessment within the broader capability life cycle. These tools should be used before substantive legal analysis begins, and revisited where new information, modifications, or changes in intended use affect the scope of review.

Review trigger and screening matrix

The decision tree below assists reviewers in determining whether a capability falls within the scope of Article 36 review and, if so, which review pathway is appropriate. It should be applied at the earliest feasible stage of study, development, acquisition, adoption, modification, integration, or proposed new use. The screening outcome should be recorded, including for cases where the conclusion is that no review is required or that a previous review remains sufficient.

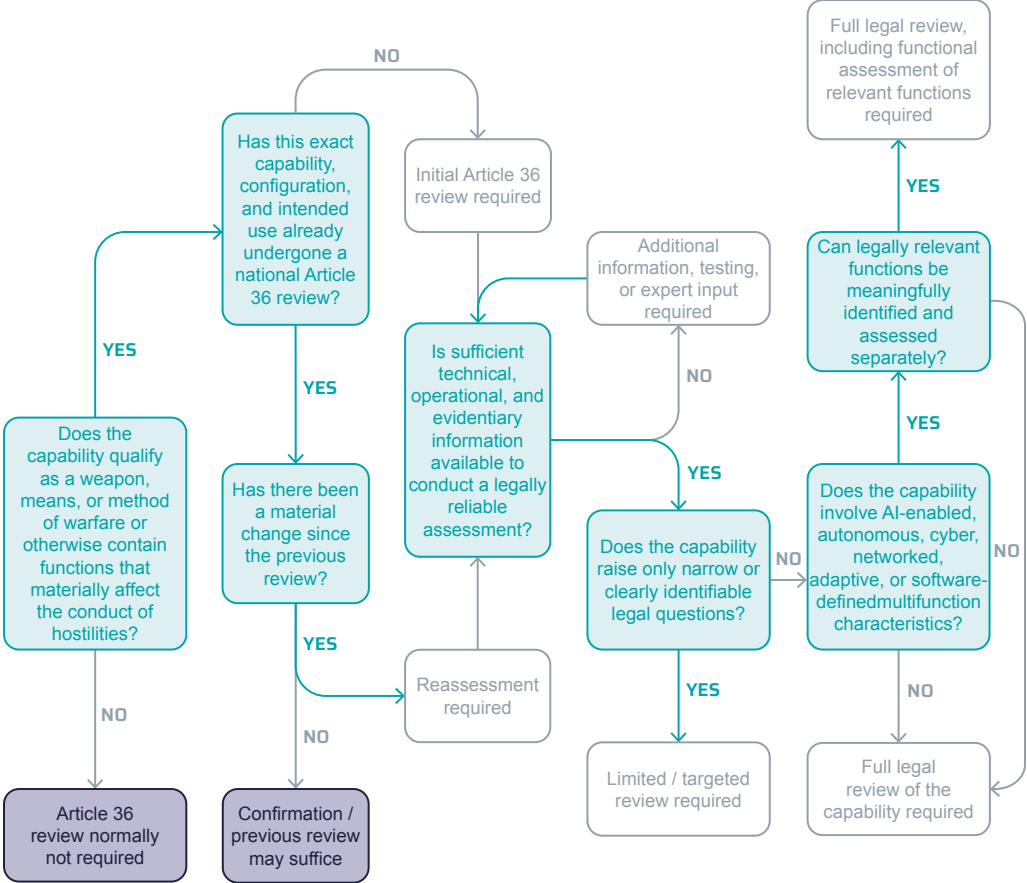


Figure 2: Screening decision tree

The screening outcome should guide which tools are used next. The pathways do not create different legal standards; rather, they indicate which practical tools are most relevant to the scope, complexity, and evidentiary needs of the review.

Table 3: Screening outcomes and relevant tools

Screening outcome	Tools to use next
Article 36 review normally not required	Record the screening conclusion and rationale.
Confirmation/previous review may suffice	Review prior legal assessment; use the reassessment trigger matrix to confirm that no material change has occurred.
Initial Article 36 review required	Use the technical information request template, then proceed to the relevant legal review checklist.
Reassessment required	Use the reassessment trigger matrix, technical information request template, and review report template.
Additional information, testing, or expert input required	Use the technical information request template; where relevant, request expert input on technical, medical, environmental, cyber, AI/autonomy, or operational issues.
Limited/targeted review required	Use the core legal review checklist only for the specific legal issues identified; document the limited scope in the review report template.
Full legal review of the capability required	Use the technical information request template, core legal review checklist, operational context assessment tool, and review report template.
Full legal review, including functional assessment of relevant functions, required	Use the technical information request template, functional assessment matrix, operational context assessment tool, core legal review checklist, reassessment trigger matrix, and review report template.

Model review workflow

The model review workflow illustrates the sequence of steps an Article 36 review may follow once a capability has entered the review process. It situates the screening decision within a broader process of information collection, technical and operational assessment, legal analysis, outcome formulation, implementation, and reassessment. While the workflow should be adapted to the institutional structure of the reviewing state, the sequence below reflects the core stages identified in the review methodology set out in this Guide.

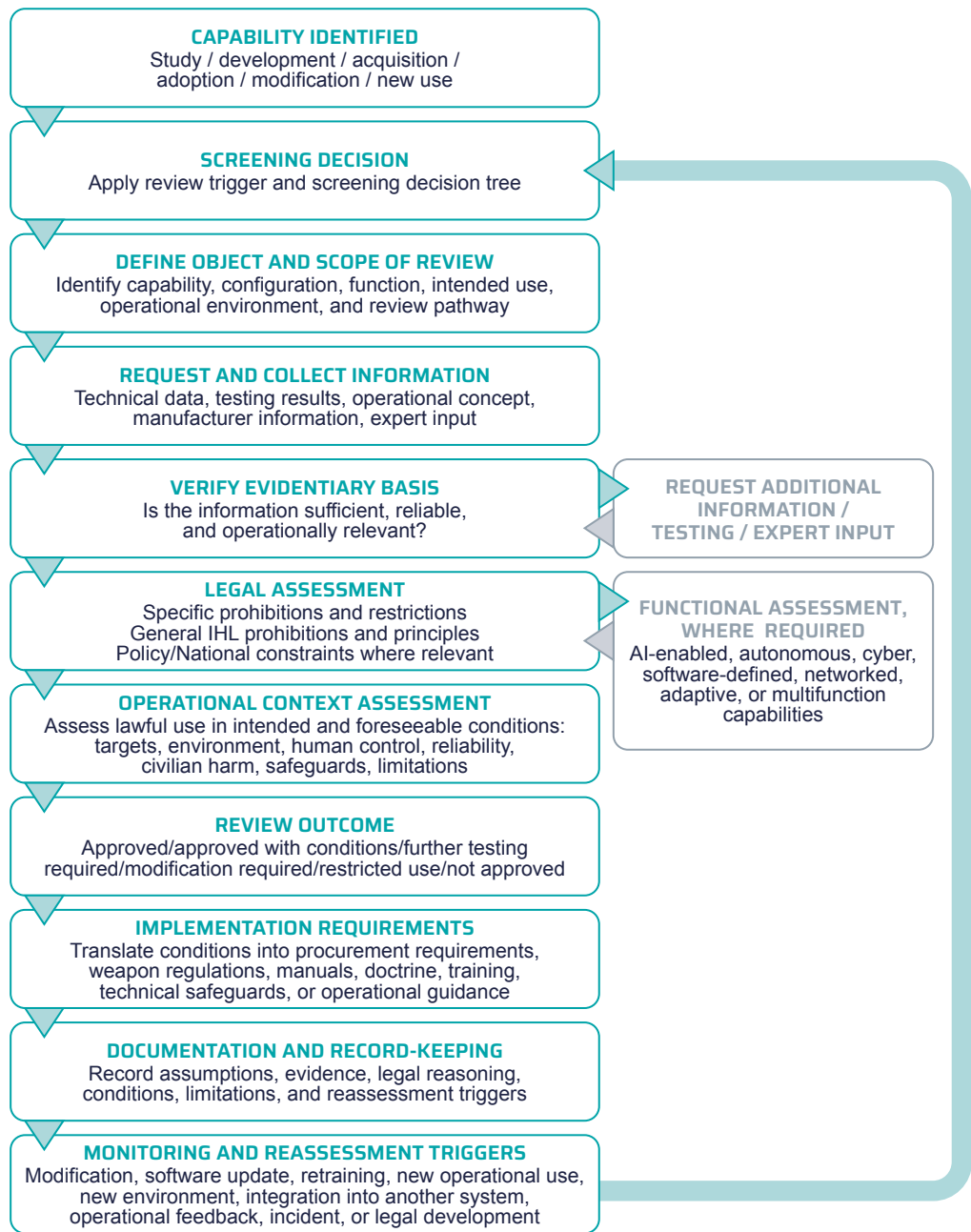


Figure 3: Model review workflow

The workflow should not be interpreted as strictly linear. In practice, an Article 36 review may move iteratively between information collection, technical assessment, legal analysis, functional assessment, and operational context assessment. Following monitoring and reassessment triggers, a capability may return to the screening stage for confirmation, limited reassessment, full review, or full review including functional assessment.

12. Reviewer analytical tools

The following tools support the substantive analysis carried out during an Article 36 review. They are intended to help reviewers define the object of assessment, collect relevant technical and operational information, identify applicable legal questions, assess compliance with specific and general prohibitions, and determine whether additional functional or operational context analysis is required. The tools may be used in full or selectively depending on whether the screening stage has identified a limited review, full review, or full review including functional assessment.

Technical information request template

This template is intended to support the collection of technical, operational, and evidentiary information necessary for an Article 36 legal review. It should be completed by the requesting authority, procurement body, developer, manufacturer, or relevant technical personnel before the substantive legal assessment begins. The level of detail required will depend on the nature and complexity of the capability under review. Only the sections and fields relevant to the capability under review need to be completed. Where information is unavailable, incomplete, classified, commercially sensitive, or subject to further testing, this should be clearly indicated. Completion of this template does not determine legality. It provides the factual and technical basis on which the reviewing authority conducts the legal assessment.

Table 4: Technical information request template

Information requested	Response/evidence provided	Supporting documents/ reviewer notes
A. Basic identification of the capability		
Name or designation of the capability		
Type or category of capability	<i>For example, weapon, munition, platform, software capability, cyber capability, AI-enabled system, subsystem, component, or method of use.</i>	
Manufacturer, developer, supplier, or originating authority		
Country of origin		
Requesting authority, unit, or procurement body		

Information requested	Response/evidence provided	Supporting documents/ reviewer notes
Stage of development, acquisition, adoption, or use	<i>For example, concept, prototype, testing, procurement, pre-deployment, modification, or operational use.</i>	
Is the capability new, newly acquired, materially modified, or proposed for a new operational use?		
Has the capability previously undergone national Article 36 review?	<i>If yes, provide reference and indicate whether this is the same configuration and intended use.</i>	
Has the capability previously undergone review, testing, or approval by another state or organization?	<i>If yes, provide available documentation, but note that this does not replace a national review.</i>	
Are comparable systems already in service or have they been previously reviewed?		
B. Object and scope of review		
What precisely is being submitted for review?	<i>Identify whether the review concerns an entire system, component, munition, payload, software function, subsystem, operational module, or method of use.</i>	
What configuration, version, model, or software build is being reviewed?		
Is the capability part of a larger integrated system?	<i>If yes, identify relevant interfaces, dependencies, and other components.</i>	
Are different variants, configurations, payloads, or modes of operation available?		
Are future modifications, software updates, payload changes, or integration options anticipated?		

Information requested	Response/evidence provided	Supporting documents/ reviewer notes
Are there functions or components that may require a separate assessment?	<i>For example, target recognition, navigation, targeting support, autonomous tracking, payload delivery, cyber effects, or decision-support functions.</i>	
Are there functions that are purely administrative, logistical, maintenance-related, or otherwise not relevant to the conduct of hostilities?		
C. Intended use and operational context		
What military purpose is the capability intended to serve?	<i>For example, engaging personnel, disabling vehicles, suppressing enemy fire, destroying materiel, neutralizing explosive threats, disrupting communications, protecting forces, supporting targeting, conducting surveillance, or denying access to an area.</i>	
Who is expected to operate or use the capability?	<i>For example, infantry, artillery, air force, naval units, special forces, cyber units, remote operators, private military, and security contractors – including where the capability may be operated, managed, stored, or transferred by private actors.</i>	
What targets is the capability intended or expected to affect?	<i>For example, personnel, vehicles, aircraft, vessels, infrastructure, electronic systems, networks, sensors, data, or objects.</i>	
Is the capability intended for offensive, defensive, support, ISR, targeting, force application, cyber, electronic warfare (EW), or other functions?		

Information requested	Response/evidence provided	Supporting documents/ reviewer notes
In what operational environments is the capability expected to be used?	<i>For example, open terrain, urban areas, maritime environment, airspace, cyber environment, contested electromagnetic environment, or populated areas.</i>	
Is the capability expected to be used near civilians or civilian objects?		
Is the capability expected to operate in environments where civilian and military objects/persons may be difficult to distinguish?		
What are the expected range, duration, and conditions of use?		
Are there foreseeable alternative uses beyond the intended use?		
Are there reasonably foreseeable misuse risks or unintended operational consequences?		
Could degraded operational conditions affect performance or legal risk?	<i>For example, weather, darkness, smoke, dust, GPS denial, electronic interference, communications loss, or cyber interference.</i>	
D. Technical characteristics and performance		
Provide a technical description of the capability.	<i>Describe the design, components, operating principles, materials, and main technical parameters.</i>	
What is the mechanism of effect, damage, disruption, injury, or destruction?		
What is the range of the capability?		

Information requested	Response/evidence provided	Supporting documents/ reviewer notes
What is the speed, trajectory, endurance, or duration of operation, where relevant?		
What payload, munition, effect, or output does the capability deliver?		
What is the expected area of effect or radius of impact?		
What is the accuracy or error rate under expected conditions of use?		
What guidance, navigation, targeting, sensor, or control mechanisms are used?		
What materials, fragments, substances, or other physical elements are produced or dispersed during normal use?		
What fragments or remnants may be generated, and are they detectable by X-ray where relevant?		
What is the expected reliability rate under normal operational conditions?		
What is the expected failure rate, malfunction rate, or abnormal operation risk?		
What residual hazards may remain after use?	<i>For example, unexploded ordnance, contamination, persistent cyber effects, unexploded submunitions, or hazardous debris.</i>	
How does the capability perform under degraded or contested conditions?		
What testing or evaluation has been conducted to assess performance?		

Information requested	Response/evidence provided	Supporting documents/ reviewer notes
E. Targeting, effects, and controllability		
Can the capability be directed at a specific military objective?		
How are targets detected, selected, classified, tracked, prioritized, or engaged?		
Can the capability distinguish between intended targets and civilians/civilian objects under expected operational conditions?		
Can the effects of the capability be limited in time, space, and scale?		
Can the attack, effect, or operation be cancelled, suspended, redirected, deactivated, or aborted after activation?		
Are there mechanisms to prevent or reduce unintended effects on civilians or civilian objects?		
Are there safeguards to prevent unauthorized use, seizure, misuse, or activation by third parties?		
What happens if the capability fails, malfunctions, loses communication, loses GPS, or behaves abnormally?		
Are fail-safe, self-destruct, self-neutralization, deactivation, or recovery mechanisms available?		
Are effects reversible, temporary, persistent, or permanent?		

Information requested	Response/evidence provided	Supporting documents/ reviewer notes
What collateral damage or incidental effects are foreseeable during normal or expected use?		
Can the capability create secondary or cascading effects?	<i>For example, fire, explosions, environmental contamination, infrastructure failure, network disruption, or reverberating cyber effects.</i>	
F. AI, autonomy, software, cyber, data, and bias-related information		
Does the capability rely on AI, machine learning, automated classification, pattern recognition, decision-support, autonomous functions, cyber effects, or adaptive software?		
Which functions are automated, AI-enabled, autonomous, cyber-enabled, or software-defined?		
Does the system detect, classify, prioritize, recommend, track, select, or engage targets?		
What level of human supervision, confirmation, intervention, or override exists for each relevant function?		
Can the operator understand the basis of system outputs or recommendations sufficiently to exercise meaningful judgement?		
Can the operator override, cancel, suspend, or modify system action in real time?		

Information requested	Response/evidence provided	Supporting documents/ reviewer notes
What data does the system rely on during training, testing, validation, or operation?		
Are data sets representative of the intended operational environment?		
Have data sets been assessed for demographic, geographic, cultural, age-related, sex-related, gender-related, or other relevant bias?		
Does the system rely on demographic, behavioural, biometric, pattern-of-life, or other proxy indicators?		
Could proxy indicators increase the risk of misidentifying civilians, children, protected persons, or particular demographic groups?		
Has the system been tested for false positives and false negatives across different operational environments and population groups?		
Are there mechanisms to detect, monitor, mitigate, or correct bias during development, testing, deployment, or retraining?		
Does the system use confidence scores, thresholds, uncertainty indicators, or warnings to users?		
Can software updates, model retraining, new data sets, or configuration changes alter legally relevant behaviour?		

Information requested	Response/evidence provided	Supporting documents/ reviewer notes
How are software versions, model updates, data sets, and configuration changes tracked and documented?		
Is the system vulnerable to spoofing, jamming, data poisoning, cyber compromise, adversarial manipulation, or other interference?		
Does the system depend on external networks, cloud services, third-party infrastructure, external sensors, or live data feeds?		
Could loss, degradation, or manipulation of external data or connectivity affect lawful use?		
Are cybersecurity, software integrity, access control, audit logs, and system-monitoring mechanisms in place?		
G. Risk mitigation and safeguards		
What technical safeguards are built into the capability?		
What operational safeguards are required for lawful use?		
What additional safeguards or restrictions are required for lawful use where the capability is operated by private contractors?		
Are there geofencing, time-limitation, target-limitation, payload-limitation, or environment-limitation mechanisms?		

Information requested	Response/evidence provided	Supporting documents/ reviewer notes
Are there restrictions on use in populated areas, urban environments, civilian infrastructure, or other high-risk contexts?		
Are there restrictions on target type, distance, altitude, range, operational mode, or level of autonomy?		
Are there training, certification, or operator-qualification requirements?		
Are there procedures for monitoring system performance during use?		
Are there procedures for monitoring the use of the capability by private operators and for reporting misuse?		
Are there reporting procedures for malfunction, unexpected effects, civilian harm, or operational incidents?		
Are reassessment triggers defined?	<i>For example, software update, new payload, new operational environment, retraining, integration into another system, incident, or new evidence.</i>	
H. Human health effects		
Describe the expected medical effect on the human body when used as intended or reasonably foreseeably.		
What is the expected wound or injury profile?	<i>Specify the effects by target type, distance, munition, operational mode, or environment where relevant.</i>	

Information requested	Response/evidence provided	Supporting documents/ reviewer notes
What is the expected short-term mortality rate, including with and without prompt medical care?		
What is the expected long-term mortality rate where treatment is available?		
What is the likelihood of full or partial recovery?		
Could the capability cause anatomical disability, disfigurement, severe burns, permanent blindness, poisoning, psychological trauma, or other long-term harm?		
Are the injuries expected to be more severe, more painful, or more difficult to treat than those caused by comparable weapons?		
Can injuries be treated under field conditions and in reasonably equipped medical facilities?		
Does the capability produce effects unfamiliar to medical personnel?		
Does the capability use projectiles or munitions that expand, flatten, explode, burn, poison, or fragment in the human body?		
Does the capability produce fragments that are not detectable by X-ray?		
Are medical studies, expert assessments, test results, or comparative data available?		

Information requested	Response/evidence provided	Supporting documents/ reviewer notes
I. Environmental effects		
What materials, substances, chemicals, fuels, batteries, metals, explosives, or toxic components are used?		
Could the capability cause direct environmental damage during normal use?	<i>Describe the immediate environmental effects expected from normal or intended use, including damage to land, water, air, vegetation, wildlife, soil, or ecosystems. Specify the type, expected scale, and duration of damage, and whether it is inherent to the capability's normal effects.</i>	
Could the capability cause indirect or reverberating environmental effects?	<i>Describe the foreseeable secondary environmental effects arising from use of the capability, including fires, release of hazardous substances, contamination of water or soil, damage to industrial facilities, unexploded ordnance, disruption of infrastructure, or cascading effects on ecosystems or civilian resources.</i>	
Could the capability cause widespread, long-term, or severe damage to the natural environment?	<i>Assess whether the environmental damage could reach the threshold of being widespread, long-term, or severe. Explain the likely geographic extent, duration, seriousness, and reversibility of damage, and available scientific or testing evidence. Indicate any uncertainties or assumptions.</i>	
Could environmental harm affect the health or survival of the civilian population?	<i>Describe whether the capability could contaminate water, soil, air, crops, livestock, food supplies, medical infrastructure, housing, or other resources necessary for civilian health or survival.</i>	

Information requested	Response/evidence provided	Supporting documents/ reviewer notes
Is the capability designed specifically to damage the environment or manipulate natural processes?		
Could weather, wind, rain, groundwater, soil, terrain, water, or climate conditions spread hazardous substances or increase environmental harm?		
Could the capability create contamination, fires, unexploded ordnance, hazardous remnants, or long-term ecological damage?		
Can environmental damage be mitigated, neutralized, remediated, or reversed?		
Have environmental impact studies or expert assessments been conducted?		
Are alternative materials, configurations, or methods available to reduce environmental or health risks?		
J. Testing, validation, and supporting evidence		
What tests, trials, simulations, or evaluations have been conducted?		
Who conducted the testing?	<i>For example, manufacturer, state testing body, independent laboratory, foreign authority, or operational unit.</i>	
What testing methodology was used?		
Were test conditions representative of expected operational use?		

Information requested	Response/evidence provided	Supporting documents/ reviewer notes
Were degraded, contested, urban, civilian-dense, cyber, electromagnetic, weather, or other challenging conditions tested?		
Are test results available to the reviewing authority?		
Are testing limitations, uncertainties, assumptions, or unresolved issues identified?		
Are further tests planned or required?		
Are manufacturer claims independently verified?		
Are foreign testing data, prior operational use reports, or comparative assessments available?		
Are relevant experts available to explain the test results to the reviewing authority?		
K. Documents and attachments		
Technical specifications		
Operating manuals or user instructions		
Safety documentation		
Testing reports and validation data		
Operational concept or concept of employment		
Training materials		
Manufacturer or developer documentation		

Information requested	Response/evidence provided	Supporting documents/ reviewer notes
Software documentation, version history, update logs, or model cards where relevant		
Data documentation, data set descriptions, validation reports, or bias assessments where relevant		
Medical, environmental, technical, cyber, AI/ autonomy, or operational expert reports		
Prior national review, foreign review, or comparable assessment if available		
Proposed restrictions, safeguards, operating conditions, or draft weapon regulation/manual provisions		

The reviewing authority should assess whether the information provided is sufficient, reliable, and operationally relevant for the legal assessment. Where essential information is missing, uncertain, classified, commercially withheld, or based solely on manufacturer assertion, the reviewing authority should request clarification, independent testing, or expert input before proceeding. For complex, AI-enabled, autonomous, cyber, software-defined, or multifunction capabilities, information may need to be provided separately for each legally relevant function. Completion of this template does not determine legality. It establishes the evidentiary basis for the subsequent legal review checklist, functional assessment matrix, and operational context assessment tool, as applicable.

Core legal review checklist

This checklist supports the substantive legal assessment of a weapon, means, or method of warfare under Article 36. It should be used after the reviewing authority has defined the object and intended use of the review and collected the necessary technical, operational, and evidentiary information. The checklist is not intended to be applied mechanically. Reviewers should focus on the legal questions actually raised by the capability, while ensuring that the assessment remains sufficiently comprehensive to support a legally reliable determination.

Where the checklist identifies unresolved factual issues, function-specific risks, operational context dependencies, possible conditions of approval, or reassessment triggers, these should be addressed through the relevant accompanying tool: the technical information request template; the functional assessment matrix; the operational context assessment tool; the review report template; or the reassessment trigger matrix.

Table 5: Core legal review checklist

Legal issue	Reviewer questions	Evidence to consider	Notes/possible implications
A. Specific prohibitions and restrictions			
Specific treaty prohibitions or restrictions	Does the capability fall within the scope of a treaty prohibiting or restricting a specific category of weapon, means, or method of warfare?	Applicable treaty obligations; technical description; payload; munition type; mechanism of effect; national reservations or declarations.	If prohibited, the capability must not be approved. If restricted, further assessment should verify compliance with treaty conditions.
State party status and national implementation	Is the reviewing state party to the relevant treaty regime? Has it made reservations, interpretative declarations, or national implementing rules relevant to the assessment?	Treaty ratification status; national legislation; military manuals; implementing regulations; prior legal opinions.	Identify whether the restriction applies as treaty law, customary law, national law, or policy.
Prohibited or regulated components, payloads, or effects	Does the capability contain or produce specifically prohibited or regulated components, payloads, substances, fragments, effects, or delivery mechanisms?	Technical specifications; munition composition; test data; manufacturer documentation; expert reports.	May require prohibition, modification, technical certification, or operational restriction.
Development, acquisition, transfer, stockpiling, or use restrictions	Are there restrictions relating not only to use, but also to development, acquisition, possession, transfer, stockpiling, or deployment?	Applicable weapons treaties; procurement documents; transfer agreements; stockpile arrangements.	Procurement or adoption may be prohibited even before operational use.

Legal issue	Reviewer questions	Evidence to consider	Notes/possible implications
Technical compliance requirements	Does the capability need to satisfy specific technical requirements under international law?	Testing reports; design features; detectability, self-deactivation, marking, recording, or other technical standards where applicable.	May require technical modification, certification, or additional testing.
B. Superfluous injury or unnecessary suffering			
Nature of injury	Is the capability of a nature to cause superfluous injury or unnecessary suffering?	Medical effects; wound profile; mechanism of injury; ballistic testing; medical expert input; comparison with existing lawful weapons.	Requires assessment by reference to intended, normal, or reasonably foreseeable use.
Severity and treatability of injury	Are expected injuries unusually severe, painful, difficult to treat, permanently disabling, disfiguring, or unfamiliar to medical personnel?	Medical studies; field treatment data; hospital treatment data; expert medical assessment; long-term effects.	May require medical expert review, modification, or restrictions on use.
Detectability of fragments	Does the capability generate fragments that cannot be detected by X-ray in the human body?	Fragmentation testing; material composition; X-ray detectability data; medical testing reports.	The prohibition (CCW Protocol I) applies to weapons whose primary effect is to injure by fragments which, in the human body, escape detection by X-rays; incidental production of undetectable fragments does not, of itself, engage the prohibition.

Legal issue	Reviewer questions	Evidence to consider	Notes/possible implications
Projectile behaviour in the body	Does the munition expand, flatten, explode, fragment, tumble, yaw, or otherwise behave in a way that raises weapons law concerns?	Ballistic testing; gelatin testing; projectile design; wound ballistics; expert reports.	May require additional testing or approval limited to lawful ammunition types or configurations. Expanding or flattening behaviour engages the 1899 Hague Declaration prohibition (as a means of warfare); exploding behaviour in anti-personnel use may engage the 1868 St Petersburg Declaration. Such tpreclude approval for anti-personnel use rather than merely requiring further testing.

C. Inherently indiscriminate effects

Ability to be directed	Can the capability be directed at a specific lawful military objective?	Targeting mechanism; accuracy data; guidance system; operator control; sensor performance; intended target set. Note that international law sets no fixed numerical accuracy standard; the question is whether, in its intended use and environment, the capability can be directed at a specific military objective with sufficient reliability. Dispersion/Circular Error Probability data should be assessed against intended target sets and engagement ranges.	May be inherently indiscriminate if it cannot be directed at lawful military objectives.
------------------------	---	---	--

Legal issue	Reviewer questions	Evidence to consider	Notes/possible implications
Limitation of effects	Can the effects of the capability be limited in time, space, and scale?	Area of effect; blast radius; cyber propagation limits; persistence; residual hazards; safeguards; abort/deactivation mechanisms.	May require restrictions on environment, target type, quantity, mode, or conditions of use.
Reliability and predictability	Are the effects sufficiently predictable and reliable under expected operational conditions?	Testing under realistic conditions; failure rates; environmental sensitivity; cyber/EW vulnerability; software behaviour; operational validation.	Significant uncertainty may require further testing, operational limits, or reassessment.
Residual or persistent effects	Does the capability create residual hazards after the military purpose has been served?	Unexploded ordnance risk; mines/submunitions/remnants; contamination; persistent cyber effects; continuing autonomous behaviour.	May require self-neutralization, clearance, monitoring, or restrictions on use.

D. Distinction and targetability

Target discrimination	Can the capability distinguish, or be used by operators to distinguish, lawful military objectives from civilians and civilian objects?	Sensor data; targeting process; operator role; classification system; human confirmation; operational context.	If distinction cannot be reliably maintained, approval may need to be denied or limited to specific contexts.
Target type	Is the capability intended for use against personnel, objects, infrastructure, networks, vehicles, vessels, aircraft, or mixed environments?	Intended use; target profile; concept of employment; operational doctrine.	Conditions may need to specify permissible target categories.
Civilian presence	Is the capability expected to be used in environments where civilians or civilian objects are present or difficult to distinguish?	Operational context; civilian-density assumptions; urban use; pattern-of-life data; intelligence dependencies.	May require restrictions on use in populated areas or heightened human control requirements.

Legal issue	Reviewer questions	Evidence to consider	Notes/possible implications
Data-driven classification	If the capability classifies persons, objects, behaviour, or environments, are the criteria legally and operationally reliable?	AI/model documentation; training data; confidence thresholds; false-positive/false-negative rates; bias testing.	May require functional assessment and data/bias review.
E. Proportionality and foreseeable civilian harm			
Foreseeable incidental harm	What civilian death, injury, damage to civilian objects, or reverberating effects may foreseeably result from intended, normal, or reasonably foreseeable use?	Collateral damage estimates; blast/effects modelling; operational scenarios; civilian infrastructure dependencies; expert input.	May require use limitations, target restrictions, or additional mitigation measures.
Reverberating effects	Could the capability cause indirect or cascading civilian harm beyond the immediate target?	Infrastructure interdependence; cyber/network effects; environmental effects; fire, flood, or industrial risk; medical, water, energy, or communications systems.	Conditions may need to restrict use against or near certain infrastructure.
Civilian harm estimation	Are available tools or models sufficient to estimate civilian harm in expected operational contexts?	Testing data; modelling assumptions; AI outputs; operational validation; uncertainty analysis.	Uncertainty should be documented and may require conservative restrictions.
F. Precautions and controllability			
Feasible precautions	Can users take feasible precautions in the choice and use of the capability to avoid or minimize civilian harm?	Operator procedures; targeting cycle; warning/cancellation mechanisms; available alternatives; safeguards.	May require doctrine, training, technical safeguards, or operational procedures.
Cancellation or suspension	Can use be cancelled, suspended, redirected, deactivated, or aborted if circumstances change?	Human control; communication links; abort mechanisms; fail-safe modes; operator interface.	Lack of cancellation capacity may require restrictions on use or operational environment.

Legal issue	Reviewer questions	Evidence to consider	Notes/possible implications
Human supervision and control	Is the level of human supervision adequate for the function performed and the operational risk involved?	Human-machine interface; operator workload; decision timelines; autonomy level; override capacity.	May require specific human control conditions or prohibition of certain modes.
Safeguards against misuse or malfunction	Are there safeguards against unauthorized use, seizure, spoofing, jamming, cyber compromise, malfunction, or unintended operation?	Cybersecurity assessment; access controls; fail-safes; technical safeguards; operational procedures.	May require technical modification, certification, or restricted deployment.
G. Environmental harm			
Direct environmental damage	Could the capability cause direct environmental damage during intended, normal, or reasonably foreseeable use?	Environmental testing; munition composition; blast/fire effects; contamination; terrain and ecosystem impact.	May require environmental restrictions or mitigation measures.
Indirect or reverberating environmental effects	Could use of the capability cause secondary environmental harm through interaction with the target or environment?	Target environment: dams, industrial sites, fuel depots, chemical facilities, water systems, forests, or agricultural land.	Conditions may restrict use near environmentally sensitive or hazardous objects.
Widespread, long-term, and severe damage	Could direct or indirect effects reach the threshold of widespread, long-term, and severe damage to the natural environment?	Geographic extent; duration; severity; reversibility; scientific evidence; cumulative use; environmental expert input.	If such risk exists, approval may need to be denied or heavily restricted.
Civilian survival resources	Could environmental harm affect water, food, agriculture, sanitation, healthcare, housing, or other resources necessary for civilian health or survival?	Environmental and civilian infrastructure analysis; contamination modelling; public health assessment.	Relevant to precautions, proportionality, and protection of objects indispensable to civilian survival.

Legal issue	Reviewer questions	Evidence to consider	Notes/possible implications
H. Martens Clause – principles of humanity and dictates of public conscience			
Residual humanitarian concerns	Even if not specifically prohibited, does the capability raise serious concerns under principles of humanity or dictates of public conscience?	Nature of effects; degree of suffering; autonomy in force application; public/legal positions; expert debate; humanitarian impact.	May inform interpretation, policy restrictions, or decision not to approve.
Novel or ethically sensitive effects	Does the capability create effects that are unusually cruel, uncontrollable, dehumanizing, or incompatible with recognized humanitarian considerations?	Technical effects; mode of operation; human control arrangements; foreseeable harm; expert views.	May require senior-level review, policy consideration, or additional safeguards.
I. AI, autonomy, software, cyber, and complex systems			
Legally relevant functions	Does the capability include functions that affect targeting, attack planning, force application, cyber effects, or operational decision-making?	Functional decomposition; system architecture; software documentation; concept of employment.	If yes, use the functional assessment matrix.
Predictability and explainability	Are system outputs and behaviour sufficiently predictable, understandable, and explainable for lawful use?	Testing data; model documentation; confidence scores; operator interface; validation reports.	May require restrictions, safeguards, or reassessment after updates.
Data quality and bias	Could data sets, model assumptions, or proxy indicators produce legally relevant errors or discriminatory effects?	Data set documentation; bias testing; false-positive/false-negative rates; demographic and contextual validation.	May require bias mitigation, operational restrictions, or prohibition of certain functions.
Software updates and model changes	Could updates, retraining, configuration changes, or integration alter legally relevant behaviour?	Version logs; update procedures; retraining process; configuration control; audit logs.	Reassessment triggers should be considered in the report and reassessment matrix.

Legal issue	Reviewer questions	Evidence to consider	Notes/possible implications
Cyber effects and vulnerabilities	Could the capability create cyber effects, be compromised by cyber means, or affect interconnected civilian systems?	Cybersecurity assessment; network mapping; propagation limits; adversarial manipulation testing.	May require cyber-specific safeguards and operational context limits.
J. Policy, national constraints, and non-binding commitments			
National policy positions	Has the state adopted national positions, policy commitments, doctrine, or public statements relevant to this capability?	National AI, autonomy, or cyber positions; military doctrine; ministerial policy; public statements.	May influence conditions, procurement decisions, or approval even where not independently legally determinative.
Non-binding instruments and emerging standards	Are there relevant non-binding instruments, political declarations, soft-law standards, or emerging normative processes?	CCW/GGE statements; responsible military AI commitments; NATO/coalition standards; national guidance.	May inform risk management, interpretation, or approval conditions.
Procurement and export-control constraints	Are there procurement, transfer, export-control, end-use, or arms control policies relevant to the capability?	Procurement rules; export-control regimes; end-user certificates; arms control policy.	May affect acquisition or deployment even if IHL approval is possible.

Findings from this checklist should be carried forward into the review report template. Where the assessment identifies conditions of lawful use or future changes that may affect legality, these should be recorded in the review report and, where appropriate, in the reassessment trigger matrix.

Specific prohibitions and restrictions: Chronological reference table

The table below consolidates, in chronological order, the principal weapon-specific prohibitions and restrictions relevant at Step 4 of the review methodology. While it summarizes the applicable instruments, whether a given rule binds the reviewing state depends on ratification status, reservations, and customary international law, which should be confirmed at the outset of the review. The table may therefore need to be adapted to reflect the reviewing state's own obligations.

Table 6: Chronological reference table

Instrument (year)	Weapon type/subject	Nature of prohibition or restriction
St Petersburg Declaration (1868)	Explosive or inflammable projectiles below 400 g	Prohibits use as a means of warfare; preamble articulates the prohibition of arms that uselessly aggravate suffering.
Hague Declaration (IV,3) (1899)	Expanding ('dum-dum') bullets	Prohibits use, as a means of warfare, of bullets that expand or flatten easily in the human body.
Hague Regulations (art. 23(a)) (1907)	Poison and poisoned weapons	Prohibits employment; customary in all armed conflicts.
Geneva Gas Protocol (1925)	Asphyxiating, poisonous, or other gases; bacteriological methods of warfare	Prohibits use in war.
Biological Weapons Convention (1972)	Biological and toxin weapons	Prohibits development, production, acquisition, transfer, stockpiling, and retention at all times.
ENMOD Convention (1976)	Environmental modification techniques	Prohibits military or any other hostile use having widespread, long-lasting, or severe effects.
CCW Protocol I (1980)	Non-detectable fragments	Prohibits use of weapons whose primary effect is to injure by fragments that escape detection by X-rays.
CCW Protocol II (1980; amended 1996)	Mines, booby traps and other devices	Restricts use; prohibits certain types and uses.
CCW Protocol III (1980)	Incendiary weapons	Restricts use, in particular against or in proximity to concentrations of civilians.
Chemical Weapons Convention (1993)	Chemical weapons	Prohibits development, production, stockpiling, transfer, and use at all times.
CCW Protocol IV (1995)	Blinding laser weapons	Prohibits use and transfer of laser weapons specifically designed to cause permanent blindness to unenhanced vision.
Anti-Personnel Mine Ban Convention (1997)	Anti-personnel mines	Prohibits use, development, production, stockpiling, and transfer at all times.
Convention on Cluster Munitions (2008)	Cluster munitions	Prohibits use, development, production, stockpiling, and transfer at all times.
Customary international law	Weapon-specific customary rules	ICRC 'Customary IHL Study', Rules 70-86; binding on all states irrespective of treaty ratification.

Functional assessment matrix for AI-enabled, autonomous, cyber, software-defined, or multifunction systems

This matrix supports the functional assessment of complex, AI-enabled, autonomous, cyber, software-defined, networked, adaptive, or multifunction capabilities. It should be used where the legality of a capability cannot be assessed solely by examining the system as a whole, because specific functions may affect targeting, attack planning, force application, cyber effects, operational decision-making, or other legally significant military operations.

This functional assessment does not replace the Article 36 legal review. It is an analytical method within the review process that helps identify which functions require legal scrutiny, what evidence is needed for each function, and what safeguards, restrictions, or reassessment triggers may be required. Where legally relevant functions cannot be meaningfully separated, the capability should be assessed as a whole through the core legal review checklist.

Table 7: Functional assessment matrix

Function/system component	Operational role	Legal relevance	Evidence required	Risks/uncertainties	Safeguards/conditions
Target detection	Identifies potential persons, objects, signals, systems, or locations of interest.	May affect distinction, precautions, and risk of misidentification.	Sensor specifications; detection criteria; training/testing data; false-positive/false-negative rates; performance in realistic environments.	Misidentification of civilians, civilian objects, protected persons, or non-target objects; poor performance in degraded conditions.	Human confirmation; confidence thresholds; restricted use environments; additional validation; exclusion of high-risk target categories.
Target classification	Classifies detected entities as military objectives, civilians, civilian objects, hostile systems, or other categories.	Directly relevant to distinction and targetability.	Classification model; rules/criteria; data set documentation; bias testing; validation across target types and environments.	Over-classification of civilians as combatants; reliance on proxies; demographic, cultural, age, sex, or gender bias.	Mandatory human review; prohibition on sole reliance on automated classification; bias mitigation; context-specific testing.

Function/system component	Operational role	Legal relevance	Evidence required	Risks/uncertainties	Safeguards/conditions
Target prioritization/ranking	Ranks or prioritizes potential targets for operator attention or engagement.	May affect proportionality, precautions, and targeting decisions.	Prioritization criteria; weighting factors; operator interface; audit logs; testing of ranking outputs.	Automation bias; over-reliance by operators; prioritization based on legally irrelevant or unreliable factors.	Explainability requirements; display of confidence/uncertainty; operator training; review of prioritization criteria.
Attack recommendation/decision-support	Recommends whether, when, or how a target should be engaged.	Highly relevant to distinction, proportionality, precautions, and human judgement.	Recommendation logic; human-machine interface; decision timelines; uncertainty indicators; testing in operational scenarios.	Erosion of meaningful human judgement; compressed decision-making; overtrust in system outputs.	Human decision authority; minimum review time; requirement to display basis for recommendation; operational limits.
Autonomous navigation/route planning	Determines movement route, path, loitering area, or approach to target area.	Relevant where navigation affects civilian risk, target environment, or ability to control effects.	Navigation algorithms; geofencing data; obstacle avoidance; map dependencies; GPS/EW performance; fail-safe modes.	Entry into prohibited or civilian-dense areas; GPS spoofing; loss of communication; collision risks.	Geofencing; no-go zones; return-to-base function; human override; degraded-mode restrictions.
Target tracking	Continuously follows a target after detection or designation.	Relevant to distinction, precautions, cancellation/suspension, and risk of target status change.	Tracking reliability; sensor fusion data; loss-of-track behaviour; reacquisition rules; operator alerts.	Tracking wrong object; failure to recognize civilian intermingling; target status changes.	Human confirmation before engagement; loss-of-track abort; periodic revalidation; target status alerts.
Engagement/force application	Delivers kinetic, electronic, cyber, or other operational effect against a target.	Directly relevant to all core IHL rules governing attack.	Payload/effect data; accuracy; area of effect; timing; abort capacity; collateral effects modelling.	Indiscriminate effects; excessive civilian harm; inability to cancel or suspend; uncontrolled propagation.	Human authorization; abort/deactivation mechanisms; target/environment restrictions; collateral damage limits.

Function/system component	Operational role	Legal relevance	Evidence required	Risks/uncertainties	Safeguards/conditions
Cyber access/persistence	Gains or maintains access to a target system or network.	Relevant where access may impact civilian systems, sovereignty, protected objects, or later effects.	Network mapping; access method; propagation controls; privilege level; persistence mechanism.	Spread to civilian systems; unintended data alteration; loss of control; discovery by adversary.	Strict target boundaries; propagation limits; monitoring; reversible access; legal review of subsequent payloads.
Cyber payload/effect delivery	Disrupts, degrades, denies, manipulates, destroys, or otherwise affects data, systems, or networks.	Relevant to classification as means/method, distinction, proportionality, precautions, and reverberating effects.	Payload description; intended effects; reversibility; propagation limits; dependency mapping; test environment results.	Cascading effects on civilian infrastructure; delayed or geographically dispersed harm; difficulty predicting effects.	Effects limitation; sandbox testing; exclusion of critical civilian systems; reversible design; monitoring and termination mechanisms.
Sensor fusion/data integration	Combines data from multiple sensors, databases, intelligence feeds, or external sources.	Relevant to reliability, target identification, and quality of human decision-making.	Data sources; fusion logic; data provenance; error handling; confidence scoring; validation reports.	Conflicting data; outdated data; biased data; false confidence; adversarial manipulation.	Data provenance controls; uncertainty indicators; cross-checking requirements; human validation.
Data ingestion/live data feeds	Uses external, real-time, or third-party data during operation.	Relevant to foreseeability, reliability, and operational control.	Data source documentation; update frequency; quality controls; access dependencies; failure modes.	Corrupted, incomplete, manipulated, or non-representative data; dependency on civilian infrastructure.	Data validation; fallback modes; restrictions if data quality falls below threshold; audit logs.
Learning/adaptation/retraining	Modifies model behaviour through updates, retraining, reinforcement learning, or operational feedback.	Relevant to continuing validity of review and reassessment triggers.	Update process; model governance; training data; validation before deployment; version control.	Behaviour changes after review; unvalidated model drift; new errors or bias.	Pre-deployment validation; configuration control; mandatory reassessment after material updates; version lock for approved configurations.

Function/system component	Operational role	Legal relevance	Evidence required	Risks/uncertainties	Safeguards/conditions
Swarm coordination/ multi-system interaction	Coordinates multiple systems or agents operating together.	Relevant to predictability, control, distinction, precautions, and cumulative effects.	Coordination logic; communication architecture; deconfliction mechanisms; emergent behaviour testing.	Emergent effects; loss of human control; cumulative civilian harm; unpredictable target engagement.	Limits on swarm size, environment, target type, or autonomy level; human supervision; abort command; simulation and field testing.
Human-machine interface	Presents information, alerts, recommendations, or controls to the operator.	Relevant to meaningful human judgement, precautions, and ability to cancel/suspend.	Interface design; operator workload testing; explainability features; alert hierarchy; training requirements.	Automation bias; confusion; information overload; inability to challenge system output.	Operator training; clear uncertainty display; mandatory confirmation steps; interface testing under stress.
Fail-safe/abort/ override function	Allows interruption, deactivation, return, self-neutralization, or termination of effects.	Relevant to precautions, controllability, and limitation of effects.	Abort mechanism; response time; reliability; communication dependencies; degraded-mode testing.	Failure to stop effects; loss of communication; unsafe default behaviour.	Independent abort channel; automatic safe mode; self-neutralization; mandatory testing and certification.
Logging/audit/ traceability	Records system inputs, outputs, operator actions, decisions, and configuration changes.	Relevant to accountability, reassessment, incident review, and verification of lawful use.	Audit logs; storage policy; tamper resistance; version records; event reconstruction capacity.	Inability to reconstruct incidents; loss of institutional learning; difficulty identifying malfunction or misuse.	Mandatory logging; secure retention; review after incidents; linkage to reassessment trigger matrix.

Reviewers should adapt this matrix to the capability under assessment. Not every function will be relevant in every case, and additional rows may be required for specific systems. The purpose of the matrix is to identify legally relevant functions, to determine whether sufficient evidence exists to assess them, and to record any function-specific safeguards, operational restrictions, or reassessment triggers that should be carried forward into the review report.

Operational context assessment tool

This tool assists reviewers in assessing whether a capability can be used lawfully in its intended and reasonably foreseeable operational contexts. It is particularly useful where legality depends not only on the capability's technical characteristics, but also on target type, environment, civilian presence, system reliability, human control, connectivity, or foreseeable indirect effects. The tool should be used to identify operational conditions that may require restrictions, safeguards, additional testing, or reassessment.

Table 8: Operational context assessment tool

Operational factor	Questions to assess	Legal relevance	Risk rating	Possible restrictions/mitigation
Target environment	Is the capability intended for use against isolated military objectives, mixed civilian-military environments, dual-use infrastructure, personnel, vehicles, networks, or area targets?	Distinction; proportionality; precautions.	Low; medium; high; information required.	Restrict permissible target types; require higher-level approval for dual-use targets; require additional target verification.
Civilian presence	Are civilians, civilian objects, protected persons, children, medical units, humanitarian actors, or cultural property likely to be present?	Distinction; proportionality; precautions; protected objects/persons.	Low; medium; high; information required.	Restrict use in civilian-dense areas; require enhanced verification; prohibit use where civilian presence cannot be assessed.
Urban or populated environments	Is use foreseeable in urban, peri-urban, or densely populated areas? Can effects be contained in such environments?	Distinction; proportionality; precautions; reverberating effects.	Low; medium; high; information required.	Limit use to open areas; require collateral damage assessment; impose minimum distance from civilian objects.
Operational environment and terrain	Could terrain, weather, vegetation, water, mountains, tunnels, or confined spaces affect performance or effects?	Predictability; reliability; precautions.	Low; medium; high; information required.	Require environment-specific testing; restrict use under certain weather, terrain, or visibility conditions.

Operational factor	Questions to assess	Legal relevance	Risk rating	Possible restrictions/mitigation
Electromagnetic, cyber, or GPS-contested conditions	Could jamming, spoofing, cyber compromise, loss of GPS, communications degradation, or adversarial manipulation affect lawful use?	Reliability; controllability; precautions; indiscriminate effects.	Low; medium; high; information required.	Require degraded-mode testing; restrict use in contested environments; require fail-safe or abort mechanisms.
Connectivity and external dependencies	Does lawful use depend on external networks, cloud services, sensors, data feeds, third-party infrastructure, or communication links?	Predictability; control; distinction; precautions.	Low; medium; high; information required.	Require fallback modes; prohibit use if data/connectivity quality falls below threshold; require data validation.
Human supervision and decision time	Can operators meaningfully supervise, verify, challenge, override, or cancel system outputs under realistic operational tempo?	Precautions; human judgement; accountability; distinction.	Low, medium, high, or information required.	Require human confirmation; impose time thresholds; restrict autonomous modes; require training/certification.
Reliability in realistic conditions	Has the capability been tested under conditions resembling intended use, including stress, degraded environments, civilian presence, or adversarial interference?	Predictability; precautions; indiscriminate effects.	Low; medium; high; information required.	Require additional testing; limit use to tested environments; require conservative operating parameters.
Indirect or reverberating effects	Could use cause cascading effects on civilian infrastructure, the environment, healthcare, water, energy, food systems, or communications?	Proportionality; precautions; environmental protection; civilian survival resources.	Low; medium; high; information required.	Prohibit or restrict use against or near critical infrastructure; require reverberating effects assessment.
Scale and cumulative use	Could repeated, simultaneous, or large-scale use increase civilian harm, environmental harm, or loss of control?	Proportionality; precautions; environmental harm; cumulative effects.	Low; medium; high; information required.	Limit quantity, duration, area, or frequency of use; require cumulative-impact assessment.
Target status change	Could the status of the target change between detection, tracking, decision, and engagement?	Distinction; precautions; cancellation/suspension.	Low; medium; high; information required.	Require target revalidation; require abort mechanism; impose maximum time between identification and engagement.

Operational factor	Questions to assess	Legal relevance	Risk rating	Possible restrictions/mitigation
Data quality and contextual validity	Are data, models, maps, intelligence feeds, or pattern-of-life assumptions valid for the specific operational context?	Distinction; proportionality; precautions; bias risk.	Low; medium; high; information required.	Require context-specific validation; prohibit use where data is outdated, incomplete, biased, or non-representative.
Differentiated civilian risk factors	Could women, men, children, older persons, persons with disabilities, displaced persons, or minority groups be misidentified, undercounted, or affected differently?	Distinction; proportionality; precautions; civilian harm mitigation.	Low; medium; high; information required.	Require age-/sex-/context-sensitive assessment; adjust civilian harm estimates; require additional safeguards in civilian environments.
Environmental sensitivity	Is use expected near forests, agricultural land, water sources, protected areas, industrial sites, dams, chemical facilities, or fuel depots?	Environmental protection; proportionality; precautions; civilian survival resources.	Low; medium; high; information required.	Restrict use near sensitive sites; require environmental assessment; require mitigation or alternative means.
Operational constraints necessary for lawful use	Are lawful use conditions clear, technically feasible, and capable of being communicated to operators?	Implementation of review outcome; precautions; training.	Low; medium; high; information required.	Translate restrictions into weapon regulations, manuals, training, ROE, technical locks, or procurement requirements.

The risk rating should not be treated as a legal conclusion. It is a practical indicator used to identify where additional evidence, safeguards, operational restrictions, or reassessment may be required. Where a high-risk operational context cannot be sufficiently mitigated, the reviewing authority should consider limiting approval to specific environments, targets, modes of use, or technical configurations.

13. Institutional support tools

The following tools support documentation, institutional memory, and life-cycle management of Article 36 reviews. They are intended to ensure that review conclusions, evidentiary assumptions, conditions of approval, and reassessment triggers are recorded in a consistent and usable form. These tools should be used after a substantive legal assessment has been completed and, where relevant, must be updated during the capability life cycle if new information, modifications, software updates, operational incidents, or changes in use arise.

Review report template

This template provides a standard structure for recording the outcome of an Article 36 legal review. It is intended to ensure that review conclusions are documented in a clear, consistent, and traceable form. The report should identify the capability reviewed, the scope of assessment, the evidentiary basis, the applicable legal framework, the legal reasoning, any conditions or restrictions attached to approval, and any triggers requiring future reassessment. The level of detail should be proportionate to the complexity and legal risk profile of the capability under review.

If the screening decision tree indicates that an Article 36 review is not generally required, the reviewing authority does not need to complete the full review report template. In such cases, a shorter screening note may be sufficient, recording the capability assessed, the reason it falls outside the scope of Article 36, the authority making the determination, the date, and any circumstances that would require renewed screening if the capability’s use or configuration changes.

Table 9: Review report template

Section	Information to include
1. Review identification	Note the review reference number, the date, the reviewing authority or review body, the requesting authority, the classification level, the version/control number, and the responsible reviewer or committee.
2. Capability reviewed	Note the name or designation of the capability; the type or category; the manufacturer, developer, or supplier; the configuration, version, or software build; the stage of development, acquisition, or use; and whether the review concerns a new capability, acquisition, modification, integration, or new operational use.
3. Scope and object under review	Define precisely what is being reviewed: whole system, component, munition, payload, software function, subsystem, operational mode, or method of use. Identify what falls outside the scope of the review.
4. Review pathway	Indicate whether this is a limited/targeted review, full legal review, full legal review including functional assessment, confirmation review, or reassessment. Briefly state why this pathway was selected.

Section	Information to include
5. Intended and reasonably foreseeable use	Describe the military purpose, intended users, intended targets, expected operational environments, normal/expected use, and reasonably foreseeable uses or limitations considered in the review.
6. Evidentiary basis	List technical documents; manufacturer information; testing reports; operational concepts; expert reports; medical, environmental, cyber, or AI assessments; prior reviews; and other materials relied upon. Identify any classified, missing, unavailable, or commercially restricted information.
7. Assumptions and limitations	Record factual, technical, operational, or legal assumptions on which the review depends. Identify uncertainties, limitations of testing, reliance on manufacturer claims, or conditions that could affect the validity of the conclusion.
8. Applicable legal framework considered	Identify the principal legal framework applied in the review, including relevant treaty obligations, customary international law, specific weapons treaties, national implementing rules, and any relevant policy or non-binding commitments. This section should be concise and cross-refer to the detailed analysis in Sections 9 and 10.
9. Assessment of specific prohibitions and restrictions	Summarize whether the capability falls within any specific prohibition or restriction applicable to the state – including treaty or customary prohibitions, technical requirements, or restrictions on development, acquisition, transfer, stockpiling, deployment, or use.
10. Assessment under general IHL prohibitions and principles	Summarize the analysis of superfluous injury or unnecessary suffering, inherently indiscriminate effects, distinction, proportionality, precautions, controllability of effects, environmental harm, and any considerations related to the Martens Clause.
11. Functional assessment, where applicable	For AI-enabled, autonomous, cyber, software-defined, adaptive, networked, or multifunction systems, identify the legally relevant functions assessed and summarize conclusions on reliability, predictability, human supervision, data quality, bias, cyber vulnerabilities, software updates, and function-specific safeguards.
12. Operational context assessment	Identify operational environments, target types, civilian risk factors, environmental sensitivities, connectivity dependencies, degraded conditions, and foreseeable indirect or reverberating effects relevant to lawful use.
13. Expert input	Identify any technical, operational, medical, environmental, cyber, AI/data, or other expert input obtained during the review, including any unresolved disagreement or uncertainty relevant to the legal assessment.
14. Review conclusion	State the review outcome clearly: lawful/approved; lawful subject to conditions; approval subject to additional information or testing; modification required; restricted to specified uses; temporary suspension pending reassessment; or unlawful/not approved.

Section	Information to include
15. Conditions, restrictions, or safeguards	Specify any conditions of lawful use with operational precision. These may concern permissible targets, environments, range, distance, altitude, operational mode, autonomy level, human supervision, data requirements, software configuration, safety mechanisms, training, certification, authorized operators, or approval authority.
16. Implementation requirements	Identify how the review outcome must be translated into practice: procurement conditions, technical modifications, weapon regulations, manuals, doctrine, standard operating procedures (SOPs), training, ROE, certification, technical locks, monitoring, or reporting procedures.
17. Reassessment triggers	Identify future events requiring reassessment: software update, model retraining, configuration change, new payload, munition, effect or operational function, integration into another system, new operational use, new operational environment, operational incident, unexpected effects, new evidence, or legal development.
18. Record-keeping and distribution	Identify where the review report and supporting materials will be stored, who may access them, classification restrictions, and which authorities must receive the conclusion or implementation requirements.
19. Approval/ signature/ endorsement	Record the reviewing authority's determination, the signature or endorsement process, the date of approval, and any higher-level approval required under national procedures.

Table 10: Optional annexes

Annex	Content
Annex A: Technical information request	Completed technical information request template and supporting documents.
Annex B: Legal review checklist	Completed core legal review checklist or issue-specific checklist.
Annex C: Functional assessment matrix	Completed matrix for AI-enabled, autonomous, cyber, software-defined, or multifunction capabilities.
Annex D: Operational context assessment	Completed operational context assessment tool.
Annex E: Testing and expert reports	Technical testing, medical, environmental, cyber, AI/autonomy, or operational expert assessments.
Annex F: Reassessment trigger matrix	Identified reassessment triggers and responsible authority.

The review report should be sufficiently detailed to allow the reviewing authority, procurement actors, commanders, trainers, and future reviewers to understand the basis of the determination. Where approval is conditional, the conditions should be formulated in a way that enables direct implementation. Where the report relies on factual assumptions, technical configurations, software versions, operational contexts, or safeguards, these should be clearly recorded so that future modifications or changes in use can be assessed against the original basis of approval.

A worked example demonstrating how the review report template may be completed in practice is set out in Annex 1. The example concerns a fictitious capability and state – all designations, figures, and findings are invented for illustrative purposes and carry no factual or legal weight – and follows the numbered sections of the template.

Reassessment trigger matrix

This matrix supports life-cycle management of Article 36 reviews by identifying changes that may require renewed screening, limited reassessment, full reassessment, or functional assessment. It should be used after a capability has already undergone a legal review and throughout its development, procurement, deployment, modification, and operational use.

A reassessment trigger does not automatically mean that the original approval is invalid, but rather that the reviewing authority should determine whether the factual, technical, operational, or legal basis of the previous review remains valid. Where the change affects the capability's legally relevant characteristics, intended use, operational context, safeguards, or applicable legal framework, reassessment should be conducted before continued use.

For adaptive systems in particular, the effectiveness of these triggers depends on monitoring arrangements established at the time of approval: unless actual system performance, incidents, software and model changes, and material changes in operational conditions are recorded and reported back to the reviewing authority, trigger events may pass unnoticed. Recent practice-oriented analysis accordingly argues that for systems capable of learning or adaptation in use, the review function must extend into the deployment phase and treat assurance documentation as a living instrument to be updated with evidence of actual performance, rather than closed at the point of approval.⁴⁷

⁴⁷ McFarland, Tim and Zena Assaad, 'Legal Reviews of In Situ Learning in Autonomous Weapons', *Ethics and Information Technology*, Vol. 25: No. 9 (2023), which argue that the review of AI-enabled weapons capable of in situ learning must extend beyond conventional pre-deployment review to post-deployment review for IHL compliance); see also Muhammedally, Sahr, 'The Preparation Gap: IHL, Human–Machine Teaming and Assurance in Military AI Systems', *International Review of the Red Cross* (2026), pp. 1–33.

Table 11: Reassessment trigger matrix

Trigger	Questions to assess	Possible reassessment pathway	Notes/action required
1. Hardware modification	Has the physical design, structure, mechanism, platform, sensor, guidance system, propulsion, range, accuracy, or control mechanism changed?	Limited reassessment or full legal review	Determine whether the modification impacts effects, targetability, reliability, controllability, or injury/damage profile.
2. New munition, payload, effect, or output	Has the system been fitted with a new warhead, munition, explosive charge, sensor, electronic effect, cyber payload, smoke, incendiary, fragmentation, or other effect-producing component?	Limited reassessment, full legal review, or functional assessment	Assess whether the new effect changes applicable legal questions, specific prohibitions, injury profile, environmental risk, or operational restrictions.
3. Software update or configuration change	Has software been updated, patched, reconfigured, or modified in a way that may affect performance, targeting, navigation, control, safety, or effects?	Limited reassessment or functional assessment	Verify version control and determine whether approved configuration remains unchanged.
4. AI model update, retraining, or data change	Has the system been retrained, updated with new data sets, adjusted through machine learning, or modified through model replacement?	Functional assessment required	Assess whether behaviour, reliability, bias profile, false-positive/false-negative rates, or explainability has changed.
5. Change in autonomy or automation level	Has the level of autonomous or automated operation increased or changed? Has human supervision, confirmation, override, or intervention been reduced?	Functional assessment or full legal review	Review implications for distinction, precautions, human judgement, predictability, and control.
6. Integration into another system	Has the capability been integrated into a larger platform, command system, sensor network, weapon system, data architecture, or multi-system environment?	Full legal review or functional assessment	Assess interaction effects, system dependencies, new functions, emergent behaviour, and operator control.

Trigger	Questions to assess	Possible reassessment pathway	Notes/action required
7. New operational use or method of employment	Is the capability proposed for a new use, tactic, doctrine, method of employment, target set, or operational role not considered in the original review?	Limited reassessment or full legal review	Determine whether the previous review covered the new method of use.
8. New operational environment	Is the capability proposed for use in a different environment, such as urban areas, populated areas, maritime settings, cyber environments, dense civilian infrastructure, GPS-denied areas, or contested electromagnetic environments?	Operational context assessment; limited or full reassessment	Assess whether reliability, controllability, civilian risk, reverberating effects, or environmental effects differ materially.
9. Change in intended targets	Are new target types proposed, including personnel, vehicles, infrastructure, networks, dual-use objects, civilian-adjacent systems, or protected objects?	Limited reassessment or full legal review	Reassess distinction, targetability, proportionality, precautions, and specific restrictions.
10. Change in scale, quantity, or pattern of use	Will the capability be used in greater numbers, over a larger area, more frequently, simultaneously, or in cumulative ways not considered in the original review?	Operational context assessment; limited or full reassessment	Assess cumulative effects, environmental harm, civilian harm, loss of control, or saturation risks.
11. New testing data or technical information	Has new testing, field data, manufacturer information, foreign assessment, scientific study, or expert opinion become available?	Confirmation review, limited reassessment, or full reassessment	Determine whether new evidence confirms or undermines original assumptions.

Trigger	Questions to assess	Possible reassessment pathway	Notes/action required
12. Operational incident or unexpected effect	Has the capability malfunctioned, caused unexpected harm, behaved unpredictably, failed safeguards, caused civilian harm, or produced effects beyond those assessed? Does post-fielding monitoring – including civilian harm data, disaggregated where available – indicate unanticipated or differentiated impacts?	Reassessment	Suspend or restrict use where necessary pending reassessment.
13. Reliability or performance degradation	Has operational use shown reduced reliability, accuracy, controllability, safety, cybersecurity, or predictability compared with the original review?	Limited reassessment or functional assessment	Assess whether lawful use remains possible under approved conditions.
14. Cybersecurity vulnerability or adversarial manipulation	Has the capability been compromised, spoofed, jammed, manipulated, data-poisoned, or shown to be vulnerable to cyber or electronic interference?	Functional assessment or operational context reassessment	Review safeguards, fail-safe modes, resilience, and restrictions in contested environments.
15. Change in data quality or operational data set	Has the data used for operation, classification, targeting, navigation, or decision-support changed? Are data sets outdated, incomplete, biased, corrupted, or no longer contextually valid?	Functional assessment	Reassess distinction, reliability, bias risk, predictability, and human supervision.
16. Change in human supervision or operator training	Has the operator role changed? Has training, certification, interface design, workload, decision time, or human override capacity changed?	Limited reassessment or functional assessment	Assess whether human judgement and feasible precautions remain effective.

Trigger	Questions to assess	Possible reassessment pathway	Notes/action required
17. Change in safeguards or operating restrictions	Have technical safeguards, geofencing, abort mechanisms, target limitations, operational restrictions, or safety procedures been removed, weakened, bypassed, or changed?	Reassessment	Determine whether prior approval depended on those safeguards or restrictions.
18. Medical, humanitarian, or environmental evidence	Has new evidence emerged concerning wound effects, treatability, long-term health effects, environmental harm, contamination, or civilian survival impacts?	Limited reassessment or full legal review	Reassess superfluous injury/unnecessary suffering, environmental harm, proportionality, and precautions.
19. Legal development	Has there been a relevant treaty change, new customary law assessment, judicial decision, national legal interpretation, policy change, or international commitment affecting the capability?	Legal reassessment	Determine whether the applicable legal framework or national position has changed.
20. Change in prior foreign review relied upon	If the original national review relied partly on foreign testing or a prior foreign review, has new information emerged about that review, version, testing methodology, assumptions, or conditions?	Confirmation review or reassessment	Verify whether reliance remains appropriate and whether independent national assessment remains valid.

The matrix should be used to preserve the continuing validity of the original legal determination. Where a trigger is identified, the reviewing authority should return to the screening decision tree to determine whether a confirmation, limited reassessment, full legal review, or full legal review including a functional assessment is required. Reassessment should be completed before continuing use where the change may affect the legal basis, factual assumptions, technical configuration, operational context, or conditions on which the original approval depended.

14. Training framework

The training framework below is intended as a guide for states, defence institutions, training providers, and review authorities seeking to build or strengthen capacity for Article 36 legal reviews. It draws on existing weapons law and legal review courses. These courses typically combine doctrinal instruction on weapons law and Article 36 with practical exercises on review methodology, and are increasingly incorporating emerging technologies such as cyber and AI-enabled systems. While integrating these established elements, the framework adapts the training model to the good practices and practical tools presented in this Guide. It therefore places particular emphasis on review triggers, evidentiary collection, use of the technical information request template, application of the core legal review checklist, operational context assessment, functional assessment for complex systems, conditional approvals, implementation requirements, and reassessment. The objective is not only to teach weapons law as a body of substantive rules, but to train participants to conduct, support, document, and operationalize legal reviews in practice.

The framework is modular. The level of depth of each model may vary depending on the audience, available time, institutional maturity, and the role of participants in the review process. It may therefore be adapted into a short briefing, a half-day workshop, a one-day induction, a two-day thematic training, or a multi-day practitioner course. The three levels below should be understood as levels of depth rather than fixed course formats.

Introductory training provides orientation to Article 36 reviews for participants who do not conduct reviews themselves but need to understand when a review may be required and how to support the process. This may include commanders, procurement officials, capability managers, operational planners, policy staff, technical personnel, and new members of review bodies. Depending on the audience, introductory training may range from a short briefing to a half-day or one-day session. It should focus on the purpose of Article 36, review triggers, basic legal issues, information requirements, and the implementation of review outcomes. Short vignette-based exercises are useful at this level, especially to help participants recognize when a capability should be referred for review.

Professional training provides the core practical course for personnel who conduct, coordinate, support, or participate directly in Article 36 reviews. It is designed primarily for legal advisers, review body members, review secretariat staff, procurement or legal focal points, and personnel responsible for coordinating review inputs. It may also be used as a training-of-trainers course for national personnel who will subsequently deliver introductory or institutional training. A professional course would normally require three to four days if delivered in full, but selected modules may also be adapted into shorter one – or two-day formats. It should combine lectures, case studies, group work, and

practical exercises using the tools in this Guide. Participants should practise applying the screening decision tree, completing technical information requests, using the core legal review checklist, identifying conditions of approval, and preparing elements of a review report.

Advanced training does not necessarily follow a single fixed curriculum. It should be understood as a set of advanced modules that may be selected and expanded depending on the needs of the audience. It is particularly relevant for experienced legal reviewers, trainers, senior review body members, and personnel working on complex or emerging technologies. Specific modules may also be delivered to AI, cyber, data, engineering, testing, medical, environmental, or operational experts where their expertise is needed to support legal review. The advanced level may be provided as a one – or two-day add-on to basic training, or as separate thematic modules. Advanced training should include scenario-based exercises requiring participants to identify legally relevant functions, evidence gaps, safeguards, conditions of approval, and reassessment requirements.

Training should be delivered by a multidisciplinary team. At a minimum, trainers should include experts in IHL and weapons law, personnel with practical experience in Article 36 or equivalent weapons review processes, and technical or operational experts capable of explaining weapon effects, testing, system performance, AI/autonomy, cyber, environmental, medical, data-bias, or gender-differentiated impact issues where relevant. Where possible, national practitioners should be involved so that participants can connect the general methodology to their own institutional procedures, procurement structures, classification rules, and operational realities. This is particularly important for training-of-trainers formats, where the objective is not only to transfer knowledge but also to create sustainable national capacity.

Table 12: Training framework

Module	Introduction level 2 hours-1 day	Professional level 1-4 days total	Advanced level approx. 1-2 day thematic add-on
1. Article 36 obligation, scope, and standard of review	Content: Introduce Article 36 of Additional Protocol I, the preventive function of legal reviews, and the basic meaning of 'weapons, means, and methods of warfare'. Explain that a review may be required for newly developed, acquired, modified, or newly used capabilities.	Content: Detailed treatment of Article 36's operative terms: the study, development, acquisition, or adoption of a 'new' weapons, means, or method of warfare; normal or expected use; reasonable foreseeability; timing before use; continuing reassessment; and the non-transferable responsibility of the reviewing state.	Content: Difficult scope questions: dual-use technologies, software-enabled systems, cyber capabilities, AI-enabled decision-support systems, modular systems, foreign-procured capabilities, and functions that affect hostilities without themselves producing direct physical effects.
	Exercise: Short vignette: participants decide whether selected capabilities potentially fall within Article 36.	Exercise: Participants classify examples: small-calibre ammunition, off-the-shelf drone, AI decision-support system, cyber capability, modified munition, and foreign-procured weapon.	Exercise: Borderline case exercise: participants decide whether each capability requires no review or a limited review, full review, reassessment, or full review including functional assessment.

Module	Introduction level 2 hours-1 day	Professional level 1-4 days total	Advanced level approx. 1-2 day thematic add-on
2. Weapons law and applicable legal framework	Content: Provide an overview of weapons law sources and the basic distinction between specific treaty prohibitions/restrictions and general IHL principles applicable to all weapons, means, and methods. Introduce superfluous injury/unnecessary suffering, inherently indiscriminate weapons, distinction, proportionality, precautions, environmental protection, and the Martens Clause.	Content: Doctrinal core of the training covering: A. Sources of weapons law – treaty law, customary IHL, national implementation, policy, and non-binding commitments. B. Specific prohibitions and restrictions – chemical and biological weapons, anti-personnel mines, cluster munitions, CCW and Protocols, non-detectable fragments, mines/booby traps, incendiary weapons, blinding lasers, expanding bullets, poison/poisoned weapons, and environmental modification techniques. C. General IHL prohibitions and principles – superfluous injury/unnecessary suffering, inherently indiscriminate weapons, distinction; proportionality, precautions, and ability to direct and limit effects. D. Environmental protection – widespread, long-term, and severe damage and environmental effects relevant to civilian harm and civilian survival. E. Martens Clause, humanity, public conscience, and policy considerations.	Content: Difficult legal assessments: technologies not specifically regulated by treaty, interaction between specific weapons regimes and general IHL, context-dependent legality, uncertain or novel effects, environmental and reverberating effects, cyber and AI-enabled capabilities under existing law, and Martens Clause arguments and policy commitments without overstating their legal status.

Module	Introduction level 2 hours-1 day	Professional level 1-4 days total	Advanced level approx. 1-2 day thematic add-on
		F. Other relevant international law and national constraints, where applicable.	
	Exercise: Participants match legal issues to capability examples.	Exercise: Participants apply the core legal review checklist to a conventional munition and identify which legal issues are actually raised.	Exercise: Participants assess a capability that is not prohibited per se but may be lawful only under certain conditions.
3. Legal review process, pathways, and life-cycle management	Content: Introduce the structure of a review mechanism and the basic review pathways: no review required, confirmation/no further review, limited/targeted review, full review, full review including functional assessment, or reassessment. Introduce the screening decision tree and model review workflow.	Content: Explanation of the full review process: screening, defining the object and scope, collecting information, verifying evidence, applying legal analysis, conducting a functional assessment where required, carrying out an operational context assessment, formulating the outcome, ensuring implementation, providing documentation, and conducting a reassessment. Clarify the role of different actors: legal reviewers, review bodies, procurement authorities, technical experts, operational personnel, testing authorities, and commanders.	Content: Complex process management: urgent procurement, wartime acquisition, foreign reviews, multinational systems, classified/proprietary information, iterative development, software updates, and life-cycle governance.
	Exercise: Participants apply the screening tree to two short examples.	Exercise: Participants apply the decision tree to multiple examples and identify which tools should be used next.	Exercise: Participants design a review pathway for a rapidly acquired capability involving foreign testing data, software updates, and a proposed new operational use.

Module	Introduction level 2 hours-1 day	Professional level 1-4 days total	Advanced level approx. 1-2 day thematic add-on
4. Evidentiary basis, technical information, and weapons effects	Content: Explain why legal review depends on reliable technical and operational information. Introduce the technical information request template and the need for technical, medical, environmental, cyber, AI/data, and operational input where relevant.	Content: Detailed training on the information required for legal review: system description, intended use, target type, operational environment, technical performance, accuracy, reliability, failure modes, testing data, manufacturer information, health and injury effects, environmental effects, cyber/software/data dependencies, safeguards, and supporting documents. Include how to assess whether evidence is sufficient, reliable, and operationally relevant.	Content: Evidence challenges in complex systems: manufacturer assertions, black-box systems, incomplete testing, classified data, independent verification, AI model validation, data set quality, cyber vulnerabilities, adversarial manipulation, X-ray detectability, wound ballistics, environmental modelling, and indirect environmental harm.
	Exercise: Participants identify missing information in a short fictional procurement file.	Exercise: Participants complete or critique a technical information request template for a selected capability and identify what expert input is needed.	Exercise: Participants decide whether the evidentiary basis is sufficient to proceed, and what additional testing or expert input must be requested.

Module	Introduction level 2 hours-1 day	Professional level 1-4 days total	Advanced level approx. 1-2 day thematic add-on
5. Operational context, conditional approval, and implementation	Content: Introduce the idea that many capabilities are not inherently lawful or unlawful; legality may depend on target type, environment, human control, safeguards, and conditions of use. Introduce the operational context assessment tool.	Content: Intended and foreseeable use; operational environments; civilian presence; urban and populated areas; dual-use infrastructure; degraded environments; electromagnetic/cyber/GPS-contested conditions; human supervision; indirect/reverberating effects; civilian harm; environmental sensitivities; and conditions of lawful use. Include how review outcomes are translated into weapon regulations, manuals, SOPs, ROE, training, procurement clauses, technical safeguards, monitoring, and operator certification.	Content: Complex conditional approvals for AI-enabled, autonomous, cyber, software-defined or networked systems. Cover dynamic operational constraints, connectivity dependencies, data quality thresholds, human supervision requirements, software configuration limits, geofencing, confidence thresholds, and monitoring obligations.
	Exercise: Participants identify possible use restrictions for a simple capability.	Exercise: Participants draft conditions of approval and implementation requirements for a capability approved only under specified operational constraints.	Exercise: Participants convert legal findings into operational restrictions, technical safeguards, training requirements, and reassessment triggers.

Module	Introduction level 2 hours-1 day	Professional level 1-4 days total	Advanced level approx. 1-2 day thematic add-on
6. Functional assessment for complex and emerging technologies	Content: Introduce why certain systems require an assessment of legally relevant functions rather than only the capability as a whole. Explain examples: AI-enabled decision-support systems, autonomous functions, cyber effects, software-defined capabilities, networked systems, and multifunction platforms.	Content: Use the functional assessment matrix. Cover target detection, classification, prioritization, recommendation, tracking, engagement, cyber access/effects, data ingestion, sensor fusion, learning/adaptation, human-machine interface, fail-safe/abort functions, audit logs, and reassessment triggers. Include data quality, bias, and differentiated civilian risk questions where relevant.	Content: Module can serve as the main advanced add-on. Suggested subsections: A. Functional decomposition of complex systems – identifying legally relevant functions and separating them from support functions. B. AI-enabled and autonomous functions – detection, classification, prioritization, tracking, recommendation, engagement, and human supervision. C. Cyber and software-defined capabilities – access, payload/effects, propagation, cascading effects, system dependencies, software updates, and configuration changes. D. Data quality, bias, and differentiated civilian risk assessment – representativeness; false positives/false negatives; demographic and behavioural proxies; gender, age, children, disability, displacement, and automation bias; and undercounting civilians.

Module	Introduction level 2 hours-1 day	Professional level 1-4 days total	Advanced level approx. 1-2 day thematic add-on
			E. Testing, validation, explainability, and assurance – model drift, red-teaming, auditability, confidence scores, version control, and operational validation. F. Function-specific safeguards and reassessment triggers – human override, geofencing, use restrictions, confidence thresholds, retraining triggers, and incident reporting.
	Exercise: Participants identify legally relevant functions in a simple system diagram.	Exercise: Participants complete a functional assessment matrix for an AI-enabled, autonomous, cyber-enabled, or software-defined capability.	Exercise: Participants conduct a full functional assessment of a complex system and identify legal risks, evidence gaps, safeguards, conditions of use, and reassessment triggers.

Module	Introduction level 2 hours-1 day	Professional level 1-4 days total	Advanced level approx. 1-2 day thematic add-on
7. Capstone practical exercise	Content: Short consolidation exercise covering the essential logic of the review system.	Content: Full syndicate exercise applying the Guide's tools from screening to report drafting. Participants should use the screening decision tree, technical information request template, core legal review checklist, operational context assessment tool, and review report template.	Content: Advanced scenario involving a complex AI/autonomous/cyber/software-defined system with incomplete evidence, data quality concerns, operational constraints, software update risks, and reassessment triggers.
	Exercise: Participants decide whether a review is required, identify the likely pathway, and list the information required for the next phase.	Exercise: Participants conduct a review of a selected conventional or emerging capability and present findings, including conditions of approval where relevant.	Exercise: Participants produce a functional assessment, an operational context assessment, recommended conditions of approval, and a reassessment trigger analysis.

The matrix should be adapted to the institutional framework, review procedure, and training needs of the state or organization concerned. Where national review forms, checklists, reporting templates, or decision-making procedures already exist, training should be built around those instruments. Where they do not, the tools provided in this Guide may be used as reference materials or adapted for national use. In all cases, training should include practical exercises that require participants to apply the relevant legal standards to realistic capability scenarios; identify evidentiary gaps; formulate review outcomes; and consider how any conditions of approval would be implemented in practice.

An example programme illustrating how the modular training framework may be assembled into a two-day practitioner course – at the professional level, for legal advisers and review body members – is set out in Annex 2. Timing is indicative, and the programme should be adapted to national procedures and, where they exist, national review instruments and forms.



Annexes

Annex 1: Worked example completed review report (illustrative)

The following worked example illustrates how the review report template may be completed in practice. It concerns a fictitious capability and state: all designations, figures, and findings are invented for illustrative purposes and carry no factual or legal weight. The example is deliberately concise; an actual report would normally annex the underlying technical, testing, and validation material. The example follows the numbered sections of the review report template above.

Table A1: Example review report

Section	Example content (illustrative)
1. Review identification	Review ref. A36-2026-014; 15 March 2026; reviewing authority: Directorate of International and Operational Law, Ministry of Defence; requesting authority: Land Systems Procurement Office; classification: RESTRICTED [fictitious example]; Version 1.0; reviewer: [name withheld].
2. Capability reviewed	'LM-120' loitering munition with automated target recognition (ATR) and operator-confirmed engagement; manufacturer: [fictitious]; software build 4.2; warhead: 2.5 kg shaped charge; endurance: 45 min; stage: acquisition (procurement of an in-production system), with national software configuration.
3. Scope and object under review	Object: the LM-120 system comprising air vehicle, warhead, ATR function (vehicle-class recognition), datalink, and operator station. The ATR function and the engagement-authorization chain are assessed functionally. Out of scope: the launcher vehicle; training simulators.
4. Review pathway	Full legal review including functional assessment: first national acquisition of the type; ATR constitutes an IHL-relevant function (target identification support). Pathway selected per the screening matrix.

Section	Example content (illustrative)
5. Intended and reasonably foreseeable use	Engagement of armoured vehicles and artillery systems in land operations. Operator confirms each engagement (human-in-the-loop); the ATR proposes and prioritizes candidate objects. Foreseeable environments include mixed rural/peri-urban terrain and degraded communications conditions. Foreseeable variation: employment against defensive fortifications.
6. Evidentiary basis	Manufacturer technical description and safety case; national acceptance-testing report (120 sorties); ATR validation report (data set composition, per-class detection, and false-recognition rates under defined conditions); data link loss behaviour specification; warhead arena-test data; operator-station human factors assessment; prior review by exporting state (informative only).
7. Assumptions and limitations	ATR performance figures assume the tested sensor configuration and environmental envelope; performance in dense urban clutter not fully characterized; reliance on manufacturer data for warhead fragmentation at extreme temperatures; assumed doctrine restricts engagement to operator-confirmed targets.
8. Applicable legal framework considered	Additional Protocol I, Articles 35(2), 36, 48, 51, 57; Customary IHL Rules 1, 7, 11-24, 70-71; CCW framework (no specific protocol directly applicable to the system as configured); national implementing directive D-2019/4.
9. Assessment of specific prohibitions and restrictions	The system is not a mine, booby trap, incendiary, or blinding laser weapon; warhead fragments are X-ray-detectable; no toxic or biological payload. Not within any specific treaty prohibition or restriction applicable to the state.
10. Assessment under general IHL prohibitions and principles	Warhead effects are comparable to lawful anti-armour munitions; no design characteristic of a nature to cause superfluous injury or unnecessary suffering. The system can be directed at specific military objectives (guidance plus operator confirmation), and its effects are limited in space and time; loiter-abort and self-destruct functions further limit effects on datalink loss. Not inherently indiscriminate. Predictability and controllability acceptable within the tested envelope.
11. Functional assessment	Function assessed: ATR (detection/classification/prioritization of vehicle classes). Governing rules: distinction; precautions in attack. Standard: support to human judgement – the operator must be able to make the distinction determination. Findings: per-class recognition reliability within envelope is adequate for decision support; false-recognition rate rises materially in visually cluttered environments; automation bias risk identified in high-tempo operation. Human control: engagement requires positive operator confirmation with imagery of adequate resolution; no autonomous engagement mode is enabled in the national configuration. Responsibility lines confirmed through command and operator certification.

Section	Example content (illustrative)
12. Operational context assessment	Approved envelope: open and mixed terrain; engagement in populated areas only where target identification is confirmed by an independent source in addition to ATR; employment prohibited where datalink conditions prevent operator confirmation imagery of specified resolution.
13. Expert input	Weapons-effects engineer (warhead data); ATR validation team (data set and performance); operational user representative; military medical officer (wound-profile comparison); no unresolved expert disagreement.
14. Review conclusion	Lawful subject to conditions: acquisition and introduction into service approved, subject to the conditions in section 15.
15. Conditions, restrictions, or safeguards	(a) autonomous engagement mode shall remain disabled; (b) engagement requires positive operator confirmation based on imagery meeting the specified resolution standard; (c) employment in populated areas requires independent corroboration of target identification; (d) ATR software updates or retraining require reassessment prior to fielding; (e) operator certification per the approved training package.
16. Implementation requirements	Conditions (a)-c) to be incorporated in the weapon regulation and operator manual; procurement contract to require notification of software or data set changes and delivery of updated validation data; conditions reflected in pre-deployment training and ROE annexes.
17. Reassessment triggers	ATR model update or retraining; new warhead or payload; integration on a new platform; employment doctrine extending to autonomous engagement; operational incident indicating unexpected behaviour or civilian harm; material change in operating environment.
18. Record-keeping and distribution	Report and annexes stored in the central review archive (ref. A36-2026-014); distribution: procurement office, force headquarters, training command; classification review after five years.
19. Approval/ signature/ endorsement	Determination signed by the Director, International and Operational Law; endorsed by the Legal Adviser to the Chief of Defence; date 15 March 2026.

Annex 2: Example training programme – two-day practitioner course (illustrative)

The following example programme illustrates how the modular training framework may be assembled into a two-day professional-level practitioner course for legal advisers and review body members. Timings are indicative. The programme assumes pre-course reading of Parts 1 and 3 of this Guide and should be adapted to national procedures and, where they exist, national review instruments and forms. Delivery should follow the multidisciplinary trainer requirements set out above.

Table A2: Example training programme

Session	Focus and content	Framework module
Day 1		
Session 1 (09:00–10:30)	The Article 36 obligation: sources, operative terms (study, development, acquisition, adoption; ‘new’; weapons, means, and methods), standard of review, temporal dimension, and the non-transferable responsibility of the reviewing state. Short vignette: Which capabilities potentially fall within Article 36?	Module 1 (professional level)
Session 2 (10:45–12:30)	Weapons law I – specific prohibitions and restrictions: chronological treaty framework and customary rules; use of chronological reference table. Exercise: classify sample capabilities against specific regimes.	Module 2 (professional level)
Session 3 (13:30–15:15)	Weapons law II – general prohibitions and principles: superfluous injury or unnecessary suffering; inherently indiscriminate weapons; distinction, proportionality, and precautions; environmental protection; Martens Clause. Exercise: Apply the core legal review checklist to a conventional munition.	Module 2 (professional level)
Session 4 (15:30–17:00)	The review process: screening decision tree, review pathways, model workflow, roles and responsibilities, life-cycle integration. Exercise: Apply the screening tree to two capabilities and select pathways.	Module 3 (professional level)

Session	Focus and content	Framework module
Day 2		
Session 1 (09:00–10:30)	Evidence and technical information: the technical information request template; assessing sufficiency and reliability; testing data; manufacturer information; health and environmental effects. Exercise: Identify gaps in a fictional procurement file.	Module 4 (professional level)
Session 2 (10:45–12:30)	Operational context and conditional approval: the operational context assessment tool; drafting conditions of use and implementation requirements; translating outcomes into weapon regulations, training, and ROE. Exercise: Draft conditions of approval for a capability lawful only under constraints.	Module 5 (professional level)
Session 3 (13:30–15:15)	Functional assessment for AI-enabled and autonomous systems: the eight-element functional methodology; data quality and bias, including differentiated civilian risk assessment; human control and responsibility. Exercise: Functional assessment of an ATR-equipped loitering munition using the functional assessment matrix.	Module 6 (professional level, with advanced elements)
Session 4 (15:30–17:00)	Capstone syndicate exercise: full review from screening to report, end-to-end use of the Guide's tools; syndicate presentations and instructor feedback; course assessment and certification.	Module 7 (professional level)



DCAF Geneva Centre
for Security Sector
Governance

Maison de la Paix

Chemin Eugène-Rigot 2E
1202 Geneva, Switzerland

 +41 (0) 22 730 94 00

 info@dcaf.ch

 www.dcaf.ch

