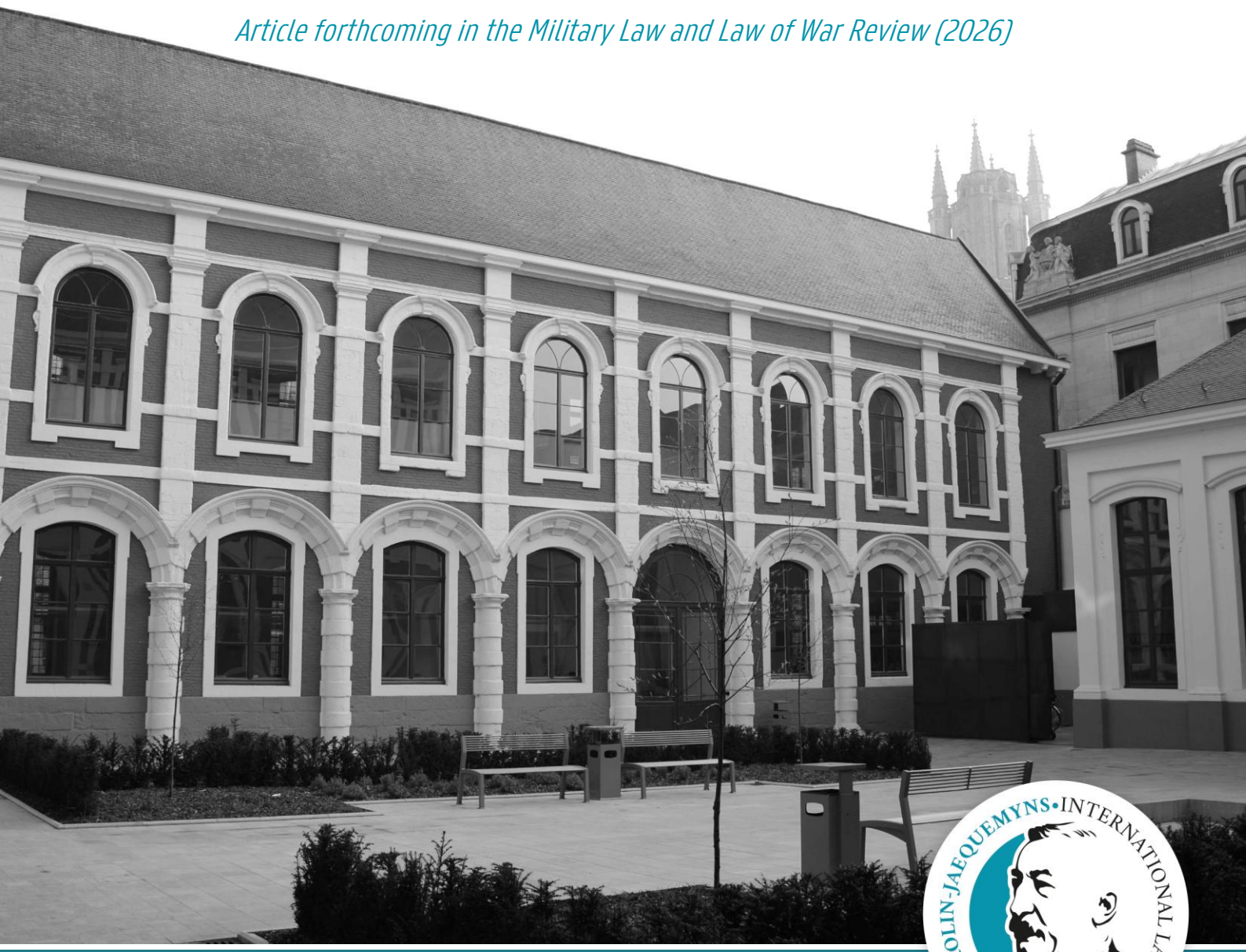
GRILI WORKING PAPER NO.16

Article forthcoming in the Military Law and Law of War Review (2026)



PREPARING EUROPE FOR CYBER WARFARE: APPLYING PEACETIME INTERNATIONAL HUMANITARIAN LAW TO THE EUROPEAN UNION'S READINESS 2030 INITIATIVE

January/2026

Quinten DeGroote

Ghent Rolin-Jaequemyns International Law Institute (GRILI), Ghent University

GHENT UNIVERSITY

Military Law and Law of War Review (2026)

PREPARING EUROPE FOR CYBER WARFARE: APPLYING PEACETIME INTERNATIONAL HUMANITARIAN LAW TO THE EUROPEAN UNION'S READINESS 2030 INITIATIVE

by Quinten DeGroote[1]

Abstract

This article examines the often-overlooked peacetime obligations under International Humanitarian Law (IHL) in the context of preparations for cyber warfare, using the European Union's (EU) Readiness 2030 initiative as a case study. Against the backdrop of intensive capacity building and the EU's explicit call to develop both defensive and offensive cyber capabilities, the article revisits the legal foundations, relevance, and contemporary urgency of peacetime IHL obligations, with a specific focus on their application to the cyber domain. The analysis concentrates on the three peacetime obligations related to the conduct of hostilities: the duty to disseminate IHL, the obligation to take passive precautions, and the requirement to conduct weapons reviews.

The article argues that the EU and its Member States have not yet adequately integrated these peacetime obligations into their preparations for cyber warfare, and that compliance with IHL during armed conflict necessarily presupposes concrete legal and institutional preparations undertaken in peacetime. On this basis, the research identifies key shortcomings in current EU practice and advances recommendations for strengthening the legal dimension of cyber readiness in order to ensure IHL compliance in future conflicts.

Keywords

international humanitarian law - peacetime obligations - cyber

[1] PhD researcher, Ghent Rolin-Jaequemyns International Law Institute (GRILI), Ghent University, Quinten.DeGroote@UGent.be.

1 Introduction

The European Union (EU) is increasingly adopting a wartime posture. These sharp words are appropriate, given Russia's invasion of Ukraine and the shifting US foreign policy under the second Trump administration, which have compelled the EU to take matters into its own hands. Through the *Readiness 2030* initiative, the EU seeks to strengthen the defence capacities of its Member States and achieve strategic autonomy by 2030.[2] This evolving security context provides an ideal backdrop to examine a long-neglected area of international humanitarian law (IHL): peacetime obligations. Although these obligations play a crucial role during defence planning and capacity building,[3] they have received limited scholarly attention. Yet, the current geopolitical climate makes it imperative to revisit even seemingly self-evident principles, particularly in light of the extensive defence preparations underway in the EU. The present study therefore aims to revive the idea that compliance with IHL in armed conflict already begins in peacetime.

This research will specifically focus on the application of peacetime obligations to the cyber domain for two reasons: (i) *Readiness 2030* emphasises preparation for cyber warfare, highlighting the need to develop both defensive and offensive cyber capabilities,[4] and (ii) peacetime obligations are often overlooked, especially when it comes to their application to a relatively new phenomenon like cyber. For practical and substantive reasons, the scope of this article is further limited to peacetime obligations related to the conduct of hostilities, which means it will not discuss those related to enforcement.[5] Practically, it is not feasible to analyse all peacetime obligations in the cyber context within the framework of this article. Substantively, obligations related to the conduct of hostilities are more interesting to examine, as preventing IHL violations in this domain comes before enforcement, and there is considerable scholarly debate concerning the conduct of hostilities in cyber. Building on these considerations, the central research question of this study will be: *how do peacetime obligations under international humanitarian law, specifically those related to the conduct of hostilities, apply to the European Union's Readiness 2030 initiative in the context of cyber*?

Three peacetime obligations are linked to the conduct of hostilities and will be examined in this research: the obligation to disseminate IHL, the obligation to take passive precautions, and the obligation to conduct weapons reviews. While their applicability in peacetime will be analysed later, it is appropriate to briefly explain here why they relate to the conduct of hostilities. Firstly, although dissemination is sometimes associated with enforcement and applies across all categories of IHL rules, this article will focus on how it prevents violations of the rules on the

[2] See European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 'Joint White Paper for European Defence Readiness 2030' (*European Defence Agency*, 19 March 2025) <https://eda.europa.eu/news-and-events/news/2025/03/19/joint-white-paper-for-european-defence-readiness-2030> all websites listed in the footnotes were last accessed on 4 November 2025.
[3] Marco Sassòli, *International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare* (Edward Elgar 2024) MN 5.136.
[4] European Commission and High Representative of the Union for Foreign Affairs and Security Policy (n 1) 7.
[5] For more information on the peacetime obligations related to enforcement, see Sassòli (n 2) MN 5.136-5.152.

conduct of hostilities. Secondly, passive precautions concern protecting civilians and civilian objects from the effects of the conduct of hostilities. Thirdly, weapons reviews aim to ensure weapons comply with the rules governing the conduct of hostilities. There is no need to distinguish between international and non-international armed conflicts for the purpose of this analysis, as all three obligations are the same in both contexts.[6]

Considering this study's focus on the application of IHL to cyber warfare, three preliminary comments must be made. Firstly, this author follows the majority view that IHL applies in the cyber context,[7] notwithstanding the existence of some opposing views.[8] Secondly, two key cyber-related terms used throughout this work require clarification. 'Cyber operation' refers to the use of cyber capabilities to achieve objectives in or through cyber, whereas 'cyber warfare' is understood more narrowly as the conduct of hostilities during armed conflict using cyber capabilities.[9] Thirdly, the cyber focus also affects the sources used in this research. As no treaty specifically governs IHL in the cyber context,[10] discussions centre on the application of existing IHL, whose non-cyber-specific nature leaves room for interpretation.[11] Consequently, this article regularly draws on the *Tallinn Manual 2.0*, a widely influential expert document on the application of international law in the cyber context,[12] as well as on position papers issued by States and international organisations that set out their views on how international law should apply in this domain.[13] Furthermore, as scholarly work on peacetime obligations in cyber remains limited, this research relies heavily on primary sources.

To answer the questions set out in the introduction, this article will proceed as follows. The second part will set the scene by introducing *Readiness 2030* and outlining the peacetime obligations of IHL, as they form the legal and conceptual foundation of this study. The third part will then turn to the core of the analysis, examining how the three aforementioned peacetime obligations apply in the cyber domain. As *Readiness 2030* does not explicitly address

---

[6] See Sassòli (n 2) MN 5.136.

[7] For more information, see Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford University Press 2014) 117. The EU also supports this view, see Council of the European Union, 'Declaration on a Common Understanding of International Law in Cyberspace' (*Counsil of the European Union*, 18 November 2024) <https://www.consilium.europa.eu/en/press/press-releases/2024/11/18/cyberspace-council-approves-declaration-to-promote-common-understanding-of-application-of-international-law/> 7.

[8] For example, China opposes applying IHL to cyber on the ground that it wishes to preserve cyberspace as a peaceful domain and avoid an arms race, though this position may also reflect concern over its comparatively limited military cyber capabilities vis-à-vis major Western powers. For more information, see Zhixiong Huang and Yaohui Ying, 'Chinese Approaches to Cyberspace Governance and International Law in Cyberspace' in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar 2021) 561-562.

[9] The narrowest notion 'cyber attack' is not relevant for the purpose of this article. Multiple definitions of all these terms exist. For an overview, see Roscini (n 6) 10-18.

[10] Most IHL treaties were drafted long before cyber was envisaged. See Roscini (n 6) 19-24.

[11] William H Boothby, 'Cyber Capabilities' in William H Boothby (ed), *New Technologies and the Law in War and Peace* (Cambridge University Press 2018) 88-89.

[12] Natalia Jevglevskaja, *International Law and Weapons Review: Emerging Military Technology under the Law of Armed Conflict* (Cambridge University Press 2021) 240-241.

[13] The CCDCOE maintains a database of all position papers. See CCDCOE, 'Cyber Law Toolkit' (*CCDCOE*, s.d.) <https://cyberlaw.ccdcoe.org>.

these obligations, this part will explore policy recommendations for the EU and its Member States to ensure that their preparations for cyber warfare comply with IHL.

2 Setting the scene

To contextualise the analysis that follows, this part starts by introducing the *Readiness 2030* initiative, explaining why it was launched and what priorities it sets. As the initiative was developed in peacetime, this part then examines IHL's peacetime obligations, outlining their role, relevance, and legal basis.

2.1 Readiness 2030

2.1.1 Background and context

Russia's war of aggression against Ukraine represents the most profound challenge to European security since the end of the Cold War. While the war itself has intensified perceptions of vulnerability across the continent, the decisive catalyst for the EU's recent change in defence policy lies elsewhere. In the early stages of the conflict, European States were able to rely on the financial and military support of the United States (US). This changed with a shift in US foreign policy under the second Trump administration, sparking a transatlantic security crisis and forcing Europe to confront a sobering reality: it could no longer rely solely on external partners for its security. European leaders realised that their own military spending and capabilities were inadequate to support Ukraine effectively and, more fundamentally, to defend themselves.[14]

'Europe faces an acute and growing threat. The only way we can ensure peace is to have the readiness to deter those who would do us harm.'[15] With these stark words, the EU introduces its response to this new reality. Initially baptised as *ReArm Europe*, the project was quickly renamed *Readiness 2030* following criticism from Italy and Spain. In their view, the name needed to reflect a broader approach than just military rearmament, for example by also addressing civilian preparedness, supply chain resilience, and energy infrastructure.[16]

In essence, *Readiness 2030* aims to strengthen the defence capacities of EU Member States and achieve strategic autonomy by 2030. The EU envisions itself in a supporting and coordinating role to help deliver this objective.[17] The initiative consists of two main elements: a financial package to support Member States' defence investments, and, most crucially for this article, the *White Paper for European Defence*, which sets out the plan for rebuilding military strength.[18]

---

[14] Gregorio Sorgi, Jacopo Barigazzi and Giovanna Faggionato, 'EU slams the door on US in colossal defense plan' (*POLITICO*, 19 March 2025) <https://www.politico.eu/article/eu-freeze-us-multi-billion-defense-plan-arm-makers/>.
[15] European Commission and High Representative of the Union for Foreign Affairs and Security Policy (n 1) 1.
[16] Jorge Liboreiro, 'Brussels rebrands 'Rearm Europe' plan after backlash from leaders of Italy and Spain' (*Euronews*, 21 March 2025) <https://www.euronews.com/my-europe/2025/03/21/brussels-confirms-rearm-europe-rebrand-after-backlash-from-italy-and-spain>.
[17] European Commission and High Representative of the Union for Foreign Affairs and Security Policy (n 1) 5.
[18] ibid 16-19.

2.1.2 Focus on cyber

Readiness 2030 addresses a broad scope of issues, ranging from continued support for Ukraine to the establishment of an EU-wide market for defence equipment and the closing of critical capability gaps. Within this latter category, the initiative identifies seven priority areas. Most relate to conventional defence needs, such as ammunition and air defence systems, but the initiative also places particular emphasis on cyber. One of the listed priorities is to 'protect the freedom to operate in cyberspace and ensure unhindered access to cyber capabilities'. Notably, the text goes beyond a purely defensive approach to cyber: it explicitly acknowledges the need to develop offensive cyber capabilities as a component of credible deterrence.[19]

It is significant that the EU has named cyber as one of its priorities, as this recognises its pivotal role in both modern and future warfare. Since the late 2000s, experts have consistently warned about the growing risks posed by cyber warfare. Cyber incidents such as those in Estonia (2007) and Georgia (2008), allegedly conducted by Russia, as well as the deployment of the Stuxnet malware (2010), have underscored these concerns.[20] Nonetheless, Rickli and Mantellassi argue that the war in Ukraine has demonstrated a more limited impact of cyber operations than previously expected. Despite Russia's known cyber capabilities, its cyber operations in Ukraine have mostly been minor actions in support of conventional warfare rather than large-scale attacks.[21] In the context of *Readiness 2030*, this observation is of limited relevance for two reasons. Firstly, although Rickli and Mantellassi note that past cyber operations have had minimal effects, they still acknowledge that cyber will remain a key domain of modern warfare.[22] Secondly, as Liff convincingly puts it: 'the fact that we have not yet seen a cyber-incident as shocking as Pearl Harbor or 9/11 is not a cogent justification […] to neglect the topic'.[23]

With this in mind, what kind of cyber operations should the EU be preparing for? Cyber capabilities can be used for espionage or to tamper with software and data, which could lead to the malfunctioning of computer-operated physical infrastructures.[24] In Ukraine, for example, the world has witnessed cyber operations targeting power grids and communication systems.[25] However, although this has not yet happened in practice, the potential of cyber operations extends far beyond this. In theory, they could cause aircraft to crash, disable weapons, or even redirect

---

[19] ibid 2-7.
[20] For a more detailed overview of previous cyber operations and efforts to bring cyber issues onto the international agenda, see Roscini (n 6) 2-9.
[21] Jean-Marc Rickli and Federico Mantellassi, 'The War in Ukraine: Reality Check for Emerging Technologies and the Future of Warfare' (*GCSP*, 5 April 2024) <https://www.gcsp.ch/publications/war-ukraine-reality-check-emerging-technologies-and-future-warfare> 22-25.
[22] ibid 25.
[23] Adam P Liff, 'Cyberwar: A New "Absolute Weapon"? The Proliferation of Cyberwarfare Capabilities and Interstate War' (2012) 35 *Journal of Strategic Studies* 401, 404.
[24] Roscini (n 6) 2.
[25] For the cyber operation targeting power grids, see Joe Tidy, 'Ukrainian power grid "lucky" to withstand Russian cyber-attack' (*BBC*, 12 April 2022) <https://www.bbc.com/news/technology-61085480>. For the cyber operation targeting communication systems, see Tom Balmforth, 'Exclusive: Russian hackers were inside Ukraine telecoms giant for months' (*Reuters*, 5 January 2024) <https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/>.

missiles toward their origin.[26] Moreover, cyber operations are relatively inexpensive to develop, operate, and maintain, and most can be deployed rapidly.[27]

In conclusion, given the evolving nature of cyber threats, it is positive that *Readiness 2030* focuses on preparing for cyber warfare. As cyber weapons proliferate and our dependence on digital infrastructures and services grows,[28] cyber is becoming firmly entrenched alongside land, sea, air, and space as a domain of military operations. A clear indication of this trend is the establishment of dedicated cyber units within the armed forces of countries such as the US, Germany, and many others.[29]

[26] Roscini (n 6) 2.
[27] Jevglevskaja (n 11) 8.
[28] ibid 1-2.
[29] Boothby (n 10) 85-86.

2.2 IHL in peacetime

2.2.1 Role and relevance

For the purpose of this article, it is important to emphasise that *Readiness 2030* is launched during peacetime. IHL, however, generally applies only in situations of armed conflict.[30] This means that, as the EU is currently not engaged in an armed conflict with Russia,[31] the full set of obligations under IHL does not yet apply to its Member States and, by extension, to this initiative. Nonetheless, IHL also sets out a number of obligations that already apply in peacetime. States engaged in defence planning and capability-building, such as *Readiness 2030*, provide a clear example of when peacetime obligations must be taken into account.[32]

According to Sassòli, these peacetime obligations are essential to facilitate respect for IHL during armed conflict. They serve both a preventive and preparatory function by encouraging the integration of IHL into policymaking before hostilities begin. This early integration is crucial, as the chaos of armed conflict hinders focusing on IHL compliance.[33] Accordingly, mere ratification of the Geneva Conventions is insufficient: compliance with IHL on the battlefield requires substantial legal and operational preparations well in advance. Government authorities, military personnel, and the general population must be familiarised with IHL, and the necessary legal frameworks and processes must be put in place.[34]

Gallino and Vité rightly highlight an additional concern. When powerful States prepare for potential conflicts, they possess the means to acquire weapons of mass destruction, develop new technologies, and access vast resources. These factors increase the likelihood that any ensuing conflict will be massive in intensity, scale, and humanitarian consequences. This reality amplifies the responsibility of such powerful States to take IHL peacetime obligations seriously.[35] The concern is particularly relevant to the EU's preparations for a potential conflict with Russia, given the substantial capabilities of both sides.

In light of this crucial role of peacetime obligations, it is striking that *Readiness 2030* makes no reference to them. This omission underscores the relevance and urgency of this research: what guidance do IHL's peacetime obligations

[30] GCs 1949, Common Article 2; Sassòli (n 2) MN 6.01.
[31] An international armed conflict requires an act of violence between States, which has not yet occurred between Russia and any EU Member State. See Sassòli (n 2) MN 6.04-6.12.
[32] Sassòli (n 2) MN 5.136.
[33] ibid.
[34] Isabelle Gallino and Sylvain Vité, 'Complying with IHL in Large-Scale Conflicts: Key Preparedness Measures' (*ICRC Humanitarian Law & Policy Blog*, 3 April 2025) <https://blogs.icrc.org/law-and-policy/2025/04/03/complying-with-ihl-in-large-scale-conflicts-key-preparedness-measures/>.
[35] ibid.

provide regarding the EU's defence planning and capacity building, particularly in relation to the preparations for cyber warfare?

2.2.2 Legal basis

IHL does not contain an explicit provision regulating peacetime obligations. Nevertheless, the International Committee of the Red Cross (ICRC) maintains that the obligation to act in peacetime can be derived from Common Article 1 of the Geneva Conventions, which requires States to 'respect and ensure respect' for IHL. A closer reading of the Updated Commentary to GC IV suggests that this argument rests on two grounds. Firstly, a textual argument: Common Article 1 expressly stipulates that the obligation to respect and ensure respect applies 'in all circumstances', a phrase that naturally includes peacetime.[36] Secondly, a teleological argument: in order for States to respect IHL during armed conflict, they must have undertaken the necessary preparations in advance.[37] Although the Updated Commentary to GC IV is unequivocal on this point, the idea that Common Article 1 functions as an umbrella provision for peacetime obligations is not widely reflected in scholarly writing.[38] At the same time, this research has not identified any scholar who denies that Common Article 1 functions as the legal basis for peacetime obligations. As previously noted, this author considers it valuable to restate even seemingly self-evident principles, especially in a geopolitical climate where large-scale preparations for conflict are bringing peacetime IHL to the fore.

Moreover, beyond this overarching obligation to act in peacetime, IHL contains a number of provisions that implicitly or explicitly prescribe that they already apply in peacetime. These specific provisions flesh out the general obligation, offering clearer guidance as to the preparatory measures that States must undertake. One example is the obligation to criminalise grave breaches in national law and establish universal jurisdiction over them.[39] To avoid violating the principle of *nulla poena sine lege* ('no crime without law'), States must enact these criminal provisions before the armed conflict arises.[40]

[36] ICRC, *Updated Commentary on the Fourth Geneva Convention* (2025) para. 201.
[37] ibid para. 216.
[38] For example, however, it can be found in Gallino and Vité (n 33).
[39] GC I–IV, Arts. 48, 49, 128, 145; AP I, Art. 84.
[40] Sassòli (n 2) MN 5.147.

3 Peacetime obligations and cyber

This article now turns to the application of peacetime obligations in the cyber context. It focuses exclusively on peacetime obligations related to the conduct of hostilities, namely dissemination, passive precautions, and weapons review. Each obligation is briefly introduced before a detailed analysis of its relevance and application in the cyber domain. Where appropriate, attention is paid to how the EU and its Member States are implementing these obligations in their cyber preparations, and where further improvements are required.

3.1 Dissemination

3.1.1 Legal basis, content, and applicability in peacetime

The obligation to disseminate IHL, meaning that States must ensure their population is familiar with this body of law, is anchored in multiple treaty sources.[41] Additionally, because States consistently carry out dissemination activities in practice and consider themselves legally bound to do so, this obligation has attained the status of customary international law.[42]

The *ratio legis* of this obligation is the belief that widespread knowledge of IHL is a prerequisite for its effective application.[43] Such a rationale is notable for a branch of public international law, as most rules in this field can be implemented by States even if only a small group of specialised officials is familiar with them. This does not apply to IHL: in armed conflict, all individuals have rights and duties.[44] However, empirical research by the ICRC shows that merely spreading knowledge of IHL alone, for example by making the texts of the Geneva Conventions and their Additional Protocols available, is insufficient to change the behaviour of people. While knowledge will remain an essential first step, true internalisation of IHL requires States to go further by providing systematic training and fostering expertise.[45]

How should this be put into practice? The ICRC emphasises that spreading knowledge of IHL among civilians is as important as within the armed forces, but acknowledges that States have more discretion in how they do so regarding civilians.[46] For the armed forces, IHL should be fully integrated into all levels of military training, both theoretically in the classroom and practically through manoeuvres and exercises, in order to ensure that compliance with IHL

[41] See, for example, GC I–IV, Arts. 47, 48, 127, 144; AP I, Arts. 6, 82, 83; AP II, Art. 19.
[42] ICRC, *Customary IHL Study* (2005) Rules 142 and 143.
[43] ICRC (n 35) para. 6491; Gallino and Vité (n 33).
[44] Sassòli (n 2) MN 5.137.
[45] ICRC (n 35) para. 6492; Philip Spoerri, 'From Dissemination Towards Integration. An ICRC Perspective' (2013) 52 *Military Law and Law of War Review* 113-114.
[46] ICRC, *The Obligation to Disseminate International Humanitarian Law* (2003) 2.

becomes a reflex.[47] States are also required to appoint legal advisors within the armed forces who are trained to assist commanders in applying IHL during operations.[48] Moreover, armed forces must integrate IHL into rules of engagement, which they should do by developing military manuals containing their interpretation of IHL.[49] As for civilians, IHL should also be disseminated 'as widely as possible'.[50] This includes incorporating IHL into the curricula of law schools and even secondary education, as well as targeting professional groups such as the medical corps and the media.[51]

Finally, the applicability of this obligation in peacetime is evident, as the provisions explicitly state that it applies 'in time of peace as in time of war'. This guarantees that the dissemination begins well before armed conflict, as teaching IHL in peacetime allows for tailored education and training and gives audiences time to become familiar with the law over the long term.[52]

3.1.2 Cyber-specific relevance and application

At the outset, it is important to observe that neither the *Tallinn Manual 2.0* nor the position papers of the EU and its Member States provide guidance on how the obligation to disseminate IHL relates to cyber.[53] Nevertheless, to demonstrate the particular relevance of this obligation in the cyber context, this article again distinguishes between dissemination within the armed forces and dissemination among the civilian population.

3.1.2.1 Armed forces

Several aspects of disseminating IHL to the armed forces require particular emphasis in the cyber context. To begin with, both the theoretical and practical military training must incorporate the ongoing debate on IHL and cyber. Unlike traditional warfare, cyber warfare is not governed by specific rules; instead, existing IHL norms must be interpreted and applied in this domain.[54] Grasping this is crucial for all branches of the armed forces, as cyber capabilities have become so pervasive that even conventional ground forces may encounter cyber-related challenges in their

[47] ICRC (n 35) para. 6495-6496; Spoerri (n 44) 113-114. Additionally, while a detailed analysis is beyond the scope of this article, Sassòli argues that the reality of modern conflicts urges armed forces to integrate international human rights law (IHRL) considerations into their training. For example, the increasing use of armed forces in law enforcement operations blurs the line between such operations and the conduct of hostilities. For more information, see Sassòli (n 2) MN 5.139.
[48] AP I, Art. 82. According to the ICRC, this obligation further specifies the general obligation to disseminate IHL, see ICRC (n 45) 1.
[49] ICRC (n 35) para. 6495; Spoerri (n 44) 115-118.
[50] ICRC (n 35) para. 6497.
[51] ICRC (n 45) 2.
[52] ICRC (n 35) para. 6484-6485.
[53] Regarding the *Tallinn Manual 2.0*, see Michael N Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge University Press 2017). Regarding the position papers of the EU and its Member States, see, for example, Council of the European Union (n 6); France, *International Law Applied to Operations in Cyberspace* (2019); Germany, *On the Application of International Law in Cyberspace* (2021); Ireland, *Position Paper on the Application of International Law in Cyberspace* (2023); Italy, *Italian Position Paper on 'International Law and Cyberspace'* (2021); Poland, *The Republic of Poland's Position on the Application of International Law in Cyberspace* (2022).
[54] Boothby (n 10) 88-89.

operations. For example, in the Ukraine-Russia war, Ukrainian ground forces have deployed drones embedded with malware. If these drones are captured and connected to Russian computers, they can compromise and damage their networks.[55] Although the ground forces may not be responsible for embedding malware into the drones, they are nonetheless the ones deploying them. As such, they must be aware of the obligations under IHL related to their use. Determining whether armed forces provide cyber-specific IHL training to their soldiers is challenging, given the limited publicly available information on how such training is implemented in practice.[56]

Beyond general IHL training for all soldiers, it has been outlined above that States must also provide their armed forces with qualified legal advisors.[57] In the cyber domain, this requires advisors with specific expertise in applying IHL to cyber operations. Therefore, at a minimum, States should ensure that their armed forces have access to external civilian experts or assign military lawyers with such expertise to their land, sea, air, and space units. If a State's resources permit, this author argues that the most effective way to meet this obligation is to establish dedicated cyber units supported by legal advisors with specialised cyber expertise.[58] However, traditional legal advisors alone are not sufficient for highly technical matters such as cyber. Effective advice necessitates combining legal expertise with an understanding of the underlying technology. This can be achieved by ensuring that legal advisors either develop sufficient technological knowledge themselves, or work closely with technical experts.[59] Examining whether armed forces comply with these recommendations is difficult, as little is known about the training and expertise of legal advisors. Research indicates that nearly half of EU Member States have established dedicated cyber units,[60] but it remains unclear whether legal advisors in general possess cyber-specific expertise, have sufficient technological knowledge, or receive support from technical experts.[61]

Lastly, armed forces should explicitly address cyber operations in their military manuals, especially when such operations constitute a significant component of their overall activities. The manual should set out how the armed forces interpret the application of IHL in the cyber context and specify the measures they will take to ensure

---

[55] Vikram Mittal, 'Russians Capture Ukrainian Drones Which Infect Their Systems With Malware' (*Forbes*, 2 April 2025) <https://www.forbes.com/sites/vikrammittal/2025/04/02/russians-capture-ukrainian-drones-which-infect-their-systems-with-malware/?.com>.

[56] For instance, the French military manual considers it 'a priority to provide appropriate education' but does not elaborate on concrete implementation measures. See France, *Manual of the Law of Military Operations* (2022) 308. Similarly, the US military manual provides an overview of the treaties that contain an obligation to disseminate IHL but does not specify how they implement these obligations in practice. See US, *Department of Defense Law of War Manual* (2015, updated July 2023) 18.6.

[57] AP I, Art. 82; ICRC (n 41) Rule 142.

[58] Concentrating all cyber operations within a single unit allows expertise to accumulate, thereby promoting a more consistent and accurate application of IHL to such operations.

[59] For example, these experts should understand how networks, servers, and data work, as well as how cyber tools such as malware and denial-of-service attacks function.

[60] See Aleksander Olech and Damjan Štrucl, *The Evolution of Cyber Forces in NATO Countries* (CCDCOE 2025). This study only covers NATO members and therefore excludes EU Member States outside NATO, namely Austria, Cyprus, Ireland, and Malta.

[61] For instance, both the US and French military manuals underline the essential role of legal advisors, yet they do not specify whether these advisors have cyber-specific expertise, technological knowledge, or support from technical experts. See France (n 55) 307; US (n 55) 18.5.1.

compliance during cyber operations. While this can be achieved by referencing cyber operations where relevant throughout the text, the clearest and most practical approach is to include a dedicated section on the subject. Two examples of good practice already exist within the EU: the French and Norwegian armed forces have included a dedicated cyber section in their military manuals.[62] Most EU Member States, however, have not followed suit. Germany's manual, for example, addresses cyber only in a single paragraph,[63] while Denmark limits its discussion to a few context-specific references.[64] Although the United Kingdom (UK) is no longer a Member State of the EU, it is notable that such a major military power does not mention cyber operations at all in its manual.[65] It is difficult to pinpoint why some manuals include dedicated cyber sections and others do not, but this article assumes that publication dates may help explain the differences. France's newer manual (2022) was drafted after extensive scholarship on IHL and cyber had emerged, whereas the German (2013) and Danish (2016) manuals appeared just after cyber had entered the international agenda, and the UK's (2004) was even released before that.[66] Nonetheless, publication dates cannot constitute an excuse: the armed forces of EU Member States should update their military manuals to reflect the growing importance of cyber warfare.

3.1.2.2 Civilian population

Just as the cyber context compels States to rethink how they disseminate IHL within the armed forces, it also demands greater focus on dissemination among the general public. Cyber brings the battlefield closer to civilians than ever before, as anyone with a computer can access it. Consequently, civilians can conduct cyber operations without setting foot on a traditional battlefield or confronting opposing forces directly.[67]

Under IHL, civilians lose their protection against attack when their conduct meets the criteria for direct participation in hostilities (DPH).[68] It is therefore crucial to disseminate IHL so that civilians recognise when their cyber activities

[62] Regarding the French military manual, see France (n 55) 285-300. Regarding the Norwegian military manual, see Norway, *Manual i krigens folkerett* (2025) 291-310. The US, although not an EU Member State, is among the few other States with a dedicated cyber section, see US (n 55) 16.
[63] Germany, *Law of Armed Conflict Manual* (2013) para. 486.
[64] For example, the manual highlights that cyber weapons cannot be used if they cause superfluous injury or unnecessary suffering. See Denmark, *Military Manual* (2016) 363.
[65] UK, *The Joint Service Manual of the Law of Armed Conflict* (2004).
[66] Cyber got on the international agenda due to the cyber incidents in Estonia (2007) and Georgia (2008), as well as Stuxnet malware (2010). For more information, see Roscini (n 6) 2-9.
[67] Matthew T King, 'High-Tech Civilians, Participation in Hostilities, and Criminal Liability' in Ronald TP Alcala and Eric Talbot Jensen (eds), *The Impact of Emerging Technologies on the Law of Armed Conflict* (Oxford University Press 2019) 182-183.
[68] The three criteria are threshold of harm, direct causation, and belligerent nexus. See ICRC, *Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law* (2009) Recommendation V and VII.

make them lawful targets,[69] and to ensure that they themselves comply with IHL when conducting cyber operations.[70] Recent examples from the Ukraine-Russia war, such as civilian hackers and civilian intelligence apps,[71] illustrate the urgent need for such awareness and guidance.

In this context, dissemination of IHL should also extend to private technology companies. These actors should be made aware that providing cyber-related services to clients who are, or may become, involved in armed conflict entails significant risks, as discussed above. In addition, it is important to show private technology companies that they can play a crucial role in fulfilling the obligation to take precautions against the effects of attacks.[72] The role that such companies can play, as well as the concrete measures they can adopt to fulfil this obligation, will be examined in greater detail in the following chapter on passive precautions.

With regard to *Readiness 2030*, the EU and its Member States should prioritise educating civilians on these issues and actively involve private technology companies in this process. However, there is no evidence that any such measures have been undertaken.

[69] However, there is ongoing debate regarding the application of DPH to cyber. For a humanitarian view, see Kubo Mačák, 'Will the Centre Hold? Countering the Erosion of the Principle of Distinction on the Digital Battlefield' (2023) 105 *International Review of the Red Cross* 965, 970-978. For a more strict view, see Michael N Schmitt and William Biggerstaff, 'Ukraine Symposium – Are Civilians Reporting With Cell Phones Directly Participating in Hostilities?' (*Lieber Institute West Point*, 2 November 2022) <https://lieber.westpoint.edu/civilians-reporting-cell-phones-direct-participation-hostilities/>.

[70] See Tilman Rodenhäuser and Mauro Vignati, '8 Rules for "Civilian Hackers" During War, and 4 Obligations for States to Restrain Them' (*ICRC Humanitarian Law & Policy Blog*, 4 October 2023) <https://blogs.icrc.org/law-and-policy/2023/10/04/8-rules-civilian-hackers-war-4-obligations-states-restrain-them/>.

[71] Regarding the civilian hackers, see Rodenhäuser and Vignati (n 69). Regarding the civilian intelligence apps, see Quinten DeGroote, 'Learning Lessons From Ukraine: State Obligations and Legal Challenges of Civilian Intelligence Apps Under International Humanitarian Law' (*Opinio Juris*, 30 June 2025) <https://opiniojuris.org/2025/06/30/learning-lessons-from-ukraine-state-obligations-and-legal-challenges-of-civilian-intelligence-apps-under-international-humanitarian-law/>.

[72] 34th International Conference of the Red Cross and Red Crescent, *Resolution 2: Protecting civilians and other protected persons and objects against the potential human cost of ICT activities during armed conflict* (2024) para. 11.

3.2 Passive precautions

3.2.1 Legal basis, content, and applicability in peacetime

A fundamental duty under IHL is the obligation for States to take precautions against the effects of attacks, commonly referred to as 'passive precautions', which is enshrined in multiple treaty provisions and has attained customary international law status.[73] It requires States to avoid locating military objectives within or near densely populated areas and to remove civilians and civilian objects under their control from the vicinity of such objectives.[74] In addition, it imposes a broader catch-all duty to protect civilians and civilian objects against the effects of attacks.[75] Importantly, however, the obligation to take passive precautions is not absolute: States are only required to take measures 'to the maximum extent feasible', which affords them considerable discretion by taking into account the circumstances ruling at the time.[76]

Although the provisions on passive precautions do not explicitly state that these obligations apply in peacetime, the Commentary to AP I indicates an implicit applicability prior to the outbreak of hostilities. Because these measures are preventive in nature, they necessarily require States to act in advance, before an armed conflict erupts.[77]

3.2.2 Cyber-specific relevance and application

The obligation to take passive precautions in the cyber domain is confirmed by Rule 121 of the *Tallinn Manual 2.0*, but the text only refers to the catch-all obligation. The contributing experts have stated that this wording was chosen because it encompasses the full scope of the duty to take passive precautions, making reference to the other components unnecessary. They further clarify that this omission should not be interpreted as reducing or limiting the obligation in the cyber context.[78] In addition to the *Tallinn Manual 2.0*, the EU and some of its Member States' position papers on the application of international law in the cyber context also affirm that passive precautions extend to this domain, yet they provide no interpretative guidance on how this should be applied in practice.[79]

---

[73] The general obligation to take passive precautions is laid down in AP I, Art. 58(a)–(c). Additionally, several provisions impose context-specific duties to take particular passive precautions, such as GC I, Art. 19(2); GC IV, Art. 18(5); and AP I, Arts. 12(4) and 56(5). Regarding its customary international law status, see ICRC (n 41) Rules 22-24.

[74] AP I, Art. 58(a)-(b); ICRC (n 41) Rules 23-24.

[75] AP I, Art. 58(c); ICRC (n 41) Rule 22.

[76] See, for example, US (n 55) 5.2.3.2.

[77] ICRC, *Commentary on Additional Protocol I* (1987) para. 2244.

[78] Schmitt (n 52) 487-488.

[79] See, for example, Council of the European Union (n 6) 7; France (n 52) 9-10. However, some guidance and specific measures can be found in the position papers of non-EU States and the publications of international organisations. See, for example, Costa Rica, *Costa Rica's Position on the Application of International Law in Cyberspace* (2023) para. 54; ICRC, *Avoiding Civilian Harm from Military Cyber Operations During Armed Conflicts* (2020) 27-28.

Against this backdrop, two characteristics of cyber underscore the particular importance of the duty to take passive precautions: (i) its dual-use nature, and (ii) its pervasiveness.

3.2.2.1 Dual-use

One of the biggest challenges of cyber is its dual-use nature.[80] While most servers, satellites, and fibre-optic cables are owned by private companies, they are also used by the military. Consequently, armed forces rely to a large extent on the same networks and cyber infrastructures as civilians.[81] This reality highlights the importance of the obligation for States to separate military objectives from civilians and civilian objects in the cyber domain.[82] Already in 2015, the ICRC emphasised the need for States to start 'segregating military from civilian cyber infrastructure and networks'.[83] Yet, to date, no State has taken concrete steps in this direction, largely due to the high financial costs and the risk of undermining the resilience of the networks.[84] Accordingly, States appeal to the discretion afforded by the obligation to take passive precautions, arguing that such separations are not feasible.[85]

Corn and Pascucci argue that the obligation to segregate military objectives from civilians and civilian objects is untranslatable to cyber, since the measures it requires are impracticable and the feasibility argument therefore always serves as an escape clause.[86] In the context of *Readiness 2030*, however, this line of argument is unconvincing. The EU is among the wealthiest regions in the world and increasingly profiles itself as a technological powerhouse.[87] Moreover, *Readiness 2030* provides a five-year implementation horizon, which gives some time to prepare. Given these circumstances, this article argues that a failure by the EU and its Member States to take steps toward separating military and civilian cyber infrastructure and networks could amount to a violation of the obligation to take passive precautions.[88]

---

[80] ICRC (n 78) 27. Although the present article focuses on the principle of precautions, cyber its dual-use nature also presents challenges regarding the principle of distinction. The military use 'contaminates' civilian objects, as it removes their protection against attack. For more information, see Laurent Gisel, Tilman Rodenhäuser and Knut Dörmann, 'Twenty Years on: International Humanitarian Law and the Protection of Civilians against the Effects of Cyber Operations during Armed Conflicts' (2020) 102 *International review of the Red Cross* 287, 321; Sassòli (n 2) MN 8.312.

[81] ICRC (n 78) 27; Roscini (n 6) 238.

[82] AP I, Article 58(a)-(b); ICRC (n 41) Rules 23-24.

[83] ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts* (2015) 43.

[84] Sassòli (n 2) MN 10.132.

[85] Roscini (n 6) 238.

[86] Gary P Corn and Peter P Pascucci, 'The Law of Armed Conflict Implications of Covered or Concealed Cyber Operations: Perfidy, Ruses, and the Principle of Passive Distinction' in Ronald TP Alcala and Eric Talbot Jensen (eds), *The Impact of Emerging Technologies on the Law of Armed Conflict* (Oxford University Press 2019) 298-300.

[87] Regarding the EU's technological aspirations, see Atli Stannard, Pauline Agius and Bart Szewczyk, 'What Does the New European Commission Mean for EU Tech Policy?' (*Global Policy Watch*, 28 January 2025) <https://www.globalpolicywatch.com/2025/01/what-does-the-new-european-commission-mean-for-eu-tech-policy/>.

[88] For completeness, it should be noted that less demanding measures than complete separation have been proposed. Nevertheless, given humanitarian considerations and confidence in the EU's capacity, this article advocates for full separation. For alternative approaches, see Simon McKenzie and Eve Massingham, 'Taking Care Against the Computer: Precautions Against Military Operations on Digital Infrastructure' (2021) 12 *Journal of International Humanitarian Legal Studies* 224, 246-248.

3.2.2.2 Pervasiveness

As noted earlier in this research, cyber is highly pervasive: it is accessible to anyone with a computer, and society's reliance on it continues to grow.[89] This ubiquity emphasises the need to protect civilians and civilian objects in the cyber context, making the obligation of States to take 'other necessary precautions' against the effects of attacks particularly relevant in the cyber domain.[90] Such precautions should contribute to building a strong culture of cyber resilience by increasing public awareness of cyber-related risks.[91]

The question then arises: what measures can States take to comply with this obligation? Roscini convincingly characterises such measures as 'cyber defences and standard measures of cyber hygiene',[92] such as making backups of important civilian data, issuing warnings of impending or ongoing attacks, using antivirus tools, distributing protective software, monitoring networks and systems, and ensuring the timely repair of networks and cyber infrastructure.[93] A potential obstacle to the effective implementation of these measures lies in the earlier-discussed indispensable role of the private sector in the cyber context. Cooperation with private actors will be unavoidable, which may raise concerns regarding sensitive business information and the right to privacy.[94]

The EU and its Member States have already taken steps to fulfil their obligations to adopt 'other necessary precautions'. Notably, one week after the launch of *Readiness 2030*, the EU introduced its *Preparedness Union Strategy*. This initiative aims to 'enhance the EU's civilian and military preparedness and readiness for future crises', with a particular focus on cybersecurity. More specifically, the strategy seeks to 'improve early warning systems' and 'increase awareness about risks and threats'.[95] Another measure in this regard is the establishment of a Computer Emergency Response Team (CERT) in each EU Member State.[96] These teams provide assistance to actual and potential victims of cyber operations, deliver initial emergency response aid, monitor malicious cyber activities, and train experts to address cybersecurity threats.[97] Furthermore, the EU's 2023 *Cyber Defence Policy* envisions stronger cooperation between these national CERTs through the creation of an EU-wide network.[98] Taken together, while a

---

[89] See Jevglevskaja (n 11) 1-2; King (n 66) 182-183.
[90] AP I, Article 58(c); ICRC (n 41) Rule 22.
[91] ICRC (n 78) 27.
[92] Roscini (n 6) 238-239.
[93] See ICRC (n 82) 43; Roscini (n 6) 238-239; Schmitt (n 52) 488-491. A notable caveat is the debate about qualifying data as a civilian object, which is pertinent as it determines its protection under the obligation to take passive precautions. For discussion, see Gisel, Rodenhäuser and Dörmann (n 79) 318-320.
[94] Roscini (n 6) 239.
[95] European Commission, 'EU Preparedness Union Strategy' (*European Commission*, 26 March 2025) <https://commission.europa.eu/topics/preparedness_en>.
[96] The EU even has its own CERT for its institutions, agencies and bodies. ENISA maintains a database of all CERTs in the EU, see ENISA, 'CSIRTs by Country' (*ENISA*, 31 January 2024) <https://tools.enisa.europa.eu/topics/incident-response/csirt-inventory/certs-by-country-interactive-map>.
[97] Schmitt (n 52) 563.
[98] European Commission, 'EU Cyber Defence Policy' (*European Commission*, 22 May 2023) <https://www.consilium.europa.eu/en/policies/cyber-defence/#defence>.

comprehensive overview of all the adopted measures lies beyond the scope of this article, it is clear that the EU and its Member States are undertaking efforts to implement precautions to protect civilians and civilian objects from the effects of cyber operations.

3.3 Weapons review

3.3.1 Legal basis, content, and applicability in peacetime

The final peacetime obligation addressed in this article is the duty to conduct a weapons review, which requires States to determine, during the study, development, acquisition, or adoption of a new weapon, means, or method of warfare, whether its use would be prohibited under IHL or any other applicable rule of international law. This obligation is embedded in Article 36 of AP I (hereinafter Article 36), though its customary international law status remains disputed.[99] It has not yet been included in the ICRC's study on customary IHL,[100] and some States, such as the US, have consistently objected to its recognition as such.[101] Nonetheless, the ICRC persuasively argues that the obligation applies to *all* States, as it flows directly from their substantive IHL obligations.[102]

The debate on the customary international law status is of limited relevance to the present research, as all EU Member States are Parties to AP I and therefore bound by Article 36.[103] However, the ICRC reported in 2006 that only nine States worldwide confirmed having a weapons review mechanism, five of which are EU Member States: Belgium, Germany, France, the Netherlands, and Sweden.[104] More recent research suggests that other EU Member States, namely Austria, Denmark, and Finland, also undertake efforts to comply with Article 36.[105] While the secrecy surrounding weapons reviews makes it difficult to draw strong conclusions, it appears likely that not all 27 EU Member States have a review system. In the context of *Readiness 2030*, the EU should therefore leverage its intended supporting and coordinating role by urging Member States to comply with Article 36.

Although verifying whether new weapons comply with IHL may appear straightforward,[106] it merits closer analysis of how States are expected to implement this obligation. The review must be conducted through a mechanism within the domestic system, making it a national rather than international responsibility.[107] However, Article 36 affords States considerable discretion regarding how weapons reviews are organised, as its broad wording does not prescribe specific requirements.[108] This makes it challenging to verify when a State has complied with its obligations under

[99] Jevglevskaja (n 11) 164-166.
[100] See ICRC (n 41).
[101] The US has a weapons review system in place, which demonstrates State practice, but it considers this a matter of 'good policy' rather than a legal obligation under Art. 36, and thus there is no *opinio juris*. See Jevglevskaja (n 11) 186-187; US (n 55) 6.2.3.
[102] ICRC, *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare* (2006) 4.
[103] Additionally, none of the EU Member States has made a reservation to Art. 36. See ICRC, 'State Parties to Additional Protocol I' (*ICRC International Humanitarian Law Databases*, s.d.) <https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/state-parties>.
[104] ICRC (n 101) 5.
[105] Jevglevskaja (n 11) 4-5.
[106] ibid 144-146.
[107] Consequently, these reviews are embedded in secrecy. Therefore, the establishment of an international review mechanisms would be desirable, but this proposal was rejected during the negotiations. See Jevglevskaja (n 11) 124-126; Sassòli (n 2) MN 8.389.
[108] Additionally, the ICRC has not indicated in its supporting documents that there is a specific manner in which weapons reviews must be conducted to comply with Art. 36. See ICRC (n 76); ICRC (n 101).

Article 36. While many aspects could be explored when setting up these processes,[109] the most important factor is the people conducting the review. States with established review mechanisms generally follow one of two main approaches: the individual model, in which a legal (military) officer is primarily responsible for the review and consults other experts if necessary (for example, to discuss a weapon's performance in practice); and the committee model, where the legal officer is joined by a multidisciplinary team that may include military, technological, medical, and other relevant experts.[110]

Finally, for the purpose of this research, it is necessary to establish that Article 36 applies in peacetime. At first glance, neither the text of the provision nor its commentaries explicitly confirm such applicability. Nevertheless, the wording of Article 36 refers to 'High Contracting Part[ies]' rather than to parties to an armed conflict, which suggests that the obligation is not limited to situations of armed conflict. Beyond the textual interpretation, the underlying logic of Article 36 likewise supports its application in peacetime. The obligation to conduct weapons reviews stems from the duty to 'respect and ensure respect' in Common Article 1 of the Geneva Conventions.[111] As discussed above, this duty requires States to act in peacetime: in order to respect IHL during armed conflict, they must make the necessary preparations in advance.[112] Therefore, since the study, development, acquisition, and adoption of weapons occur continuously in peacetime, it is essential that Article 36 applies at that stage as well.[113]

3.3.2 Cyber-specific relevance and application

First and foremost, as Article 36 only applies to weapons, means, and methods of warfare, it is necessary to determine when cyber capabilities can be classified as such. According to the commentary to Rule 103 of the *Tallinn Manual 2.0*, 'cyber weapons' are defined as 'cyber means of warfare that are used, designed, or intended to be used to cause injury to, or death of, persons or damage to, or destruction of, objects, that is, that result in the consequences required for qualification of a cyber operation as an attack'.[114] Two comments should be made regarding this definition. Firstly, this author considers it too narrow because it limits cyber weapons to those causing physical damage akin to conventional weapons.[115] While this is not the majority view, this article advocates for the EU and its Member States to adopt a broader approach that also includes the loss of functionality,[116] as it better serves humanitarian interests by ensuring that a wider range of cyber capabilities is subjected to review.[117] Secondly, cyber weapons must be distinguished from

[109] For a comprehensive discussion, see Jevglevskaja (n 11) 122-162.
[110] ibid 135-137.
[111] Nicholas Tsagourias and Giacomo Biggio, 'The Regulation of Cyber Weapons' in Eric Myjer and Thilo Marauhn (eds), *Research Handbook on International Arms Control Law* (Edward Elgar 2022) 442.
[112] ICRC (n 35) para. 216.
[113] That is why the ICRC has also confirmed that Article 36 enjoys a 'very broad' temporal scope of application, see ICRC (n 101) 23-24. This is also supported by State practice, see SIPRI, *SIPRI Compendium on Article 36 Reviews* (2017).
[114] Schmitt (n 52) 452.
[115] See Roscini (n 6) 168-169.
[116] The EU's position paper leaves this question unresolved, see Council of the European Union (n 6) 7.
[117] The humanitarian consequences of the narrow approach are illustrated by this example: while a conventional warhead destroying a single house (causing physical damage) would be subject to review, a cyber weapon disrupting an electrical grid supplying thousands

cyber infrastructure, such as the internet, which does not constitute a means of warfare. Cyber infrastructure lies outside the control of the attacking party and functions solely to connect the cyber weapon to its target.[118]

That being said, cyber weapons are a textbook example of why Article 36 was established: to ensure that new technologies are assessed for compliance with IHL.[119] However, among EU Member States, only the German and Belgian position papers emphasise the importance of legally reviewing cyber weapons.[120] The applicability of Article 36 to cyber is nonetheless confirmed in Rule 110 of the *Tallinn Manual 2.0*.[121] To reach the conclusion that the general rules governing the legality of weapons likewise determine the permissibility of cyber weapons, the experts contributing to the manual referred to the *Nuclear Weapons Advisory Opinion* of the International Court of Justice (ICJ), which states that 'the established principles and rules of humanitarian law […] appl[y] to all forms of warfare, and to all kinds of weapons, those of the past, those of the present and those of the future'.[122]

When this is combined with *Readiness 2030*'s call to develop 'offensive cyber capabilities as credible deterrence',[123] the importance of Article 36 to this article becomes evident. This study identifies two aspects that require careful examination when applying the weapons review obligation to cyber weapons: (i) tailoring the review process to the characteristics of cyber, and (ii) addressing the ongoing legal debate concerning the application of IHL to cyber, which has an impact on the outcome of the review.

3.3.2.1 Form

Each type of weapon has distinct characteristics, meaning that a one-size-fits-all review process cannot satisfy the requirements of Article 36. While States enjoy considerable discretion in deciding on the format of weapons reviews, experts emphasise that the (technological) complexity of new technologies like cyber obliges States to adapt the process to this context to ensure the effectiveness of the reviews.[124] However, since these mechanisms are embedded in secrecy, this research is confined to advancing recommendations and cannot evaluate the extent to which they are observed in practice.

The most important measure a reviewing State can take is to include knowledgeable experts in the review. While assessing common ammunition may be a routine exercise, analysing complex weapon systems requires input from

---

of people (causing only a loss of functionality) would not. See Cordula Droege, 'Get off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians' (2012) 94 *International Review of the Red Cross* 533, 558-559.

[118] Schmitt (n 52) 453.

[119] The ICRC had already underscored the importance of legally reviewing cyber capabilities in 2015, see ICRC (n 82) 43-44. See also ICRC (n 76) para. 1476.

[120] Regarding the German position paper, see Germany (n 52) 10. Regarding the Belgian position paper, see Belgium, *The National Position of Belgium on International Law Applicable to Cyberspace* (2025) 10.

[121] Schmitt (n 52) 464-465.

[122] ICJ, *Legality of the Threat or Use of Nuclear Weapons* [1996] I.C.J. Rep 226, 259, para. 86.

[123] European Commission and High Representative of the Union for Foreign Affairs and Security Policy (n 1) 7.

[124] Gisel, Rodenhäuser and Dörmann (n 79) 331; Jevglevskaja (n 11) 140.

multiple stakeholders. For cyber weapons, this means at least involving a technical cyber expert, as an effective review depends on understanding the weapon's capabilities and foreseeing its effects.[125] The reviewing team should also include military personnel, preferably coming from dedicated cyber units if the armed forces have them, as well as experts in health and environment.[126] In conclusion, because the review of cyber weapons demands the involvement of many experts, this article argues that the only appropriate approach is the committee model, where a multidisciplinary team works together rather than leaving the process primarily to a (military) lawyer.[127]

Besides the people involved, several other elements must be considered when adapting the review process to cyber weapons. Firstly, given that most cyber weapons are designed for specific missions, the review obligation will likely arise more frequently than for mass-produced weapons. Whenever a cyber weapon is reused in a new operational environment, the initial review may become obsolete and must be repeated.[128] The rapidly evolving cyber technology even raises the question of whether continuous or real-time monitoring is necessary, though the practical feasibility of this remains uncertain.[129] Secondly, the networks on which cyber weapons operate constantly change and there is often limited information about the targeted systems. This limits the value of modelling and simulation exercises during reviews, making it imperative to devise appropriate testing methods and reliable technical standards.[130] Thirdly, the development and operation of cyber weapons will often involve the private sector, whose data, networks, and servers are essential for the weapon's use. This raises questions about the scope of the review and the sharing of sensitive information,[131] which may require EU-level legislation obliging private companies to comply.

3.3.2.2 Outcome

To determine whether a weapon complies with IHL logically presupposes that the reviewing entity has a clear understanding of how IHL applies to the weapon in question. While interpretative debates exist within IHL more broadly, they are particularly acute in the cyber context due to the absence of specific treaty provisions governing cyber operations. Therefore, as several scholars rightly observe, a legal review of a cyber weapon is impossible without first clarifying the reviewing entity's position on how IHL applies to cyber, since this ultimately determines

[125] Jevglevskaja (n 11) 268-269.
[126] Sassòli (n 2) MN 8.391.
[127] This approach also has challenges. If codes for cyber weapons are developed in the heat of battle, a formal review involving all relevant experts may be impossible. In such circumstances, the advice of an operational lawyer may be the only practical option. Nevertheless, it should be emphasised that operational exigencies do not relieve States of their obligations under international law. See Jeffrey T Biller and Michael N Schmitt, 'Classification of Cyber Capabilities and Operations as Weapons, Means, or Methods of Warfare' (2019) 95 *International Law Studies* 178, 221; Jevglevskaja (n 11) 270.
[128] However, scholars argue that minor modifications do not automatically trigger a new Article 36 review. Requiring a full review for every code change would be impractical given the frequency of such updates. Where the degree of change is minimal, an operational review may suffice. See Jevglevskaja (n 11) 267; Tsagourias and Biggio (n 110) 442-443.
[129] Jevglevskaja (n 11) 269.
[130] Jevglevskaja (n 11) 268-269; Tsagourias and Biggio (n 110) 447.
[131] Tsagourias and Biggio (n 110) 447.

whether a weapon is approved or rejected.[132] Some States and international organisations have publicly issued position papers outlining their views,[133] while others may have adopted internal positions without disclosing them. In this author's view, publication is preferable, as such transparency contributes to shaping international law in the complex and contested domain of cyber.[134]

The most pertinent rules for assessing the legality of a weapon are those governing the conduct of hostilities, namely distinction, proportionality, and precaution.[135] Significant debate remains as to how these three principles should be interpreted in the context of cyber,[136] making it essential for a reviewing entity to address them when formulating its position. For issues where the law remains unsettled, States and international organisations should adopt a cautious stance to avoid hindsight claims that their cyber weapon should have been deemed unlawful.[137]

However, the EU's position paper does not even adopt a cautious stance, as it leaves most, if not all, interpretative questions concerning the conduct of hostilities unanswered.[138] The majority of EU Member States' position papers suffer the same shortcoming, merely confirming that the rules on the conduct of hostilities apply in the cyber context without explaining how.[139] Although Germany and France provide a more detailed application of distinction and precaution to cyber, they still offer insufficient clarification regarding proportionality.[140] As a result, the EU and its Member States lack the clarity required to conduct a proper weapons review of cyber weapons, though it bears repeating that internal documents may be more detailed. Given the EU's intention to play a supporting and coordinating role in the context of *Readiness 2030*,[141] it should issue a more comprehensive position paper and assist its Member States in developing their own.[142]

---

[132] Gisel, Rodenhäuser and Dörmann (n 79) 330; Jevglevskaja (n 11) 241.
[133] See CCDCOE (n 12).
[134] Henning Lahmann, 'State Behaviour in Cyberspace: Normative Development and Points of Contention' (2023) 16 *Zeitschrift für Außen- und Sicherheitspolitik* 31, 34.
[135] Given that Article 36 obliges States to determine whether a weapon is prohibited by 'any other rule of international law', additional bodies of law must also be considered, such as arms control treaties and rules on environmental protection. While the broad wording of Article 36 could be read as encompassing IHRL, in practice this is rarely done, which ultimately ties back to the debate on *lex specialis*. For discussion, see Jevglevskaja (n 11) 261-266; Tsagourias and Biggio (n 110) 444-447.
[136] A comprehensive analysis of this debate goes beyond the scope of this article. For more information, see Roscini (n 6) 182-239.
[137] Gisel, Rodenhäuser and Dörmann (n 79) 330.
[138] For example, the position paper does not clarify when a definite military advantage arises in cyberspace, nor does it explain whether the proportionality analysis considers only physical damage or also includes loss of functionality. See Council of the European Union (n 6) 7.
[139] See, for example, Ireland (n 52) 7-8; Italy (n 52) 9-10; Poland (n 52) 7.
[140] France (n 52) 13-16; Germany (n 52) 7-10.
[141] European Commission and High Representative of the Union for Foreign Affairs and Security Policy (n 1) 5.
[142] A useful source in that regard is the recent handbook by Mačák, Dias, and Kasper, which provides guidance for States to develop position papers. See Kubo Mačák, Talita Dias and Ágnes Kasper, *Handbook on Developing a National Position on International Law and Cyber Activities* (CCDCOE 2025).

4 Conclusion

As the EU accelerates its preparations for cyber warfare under the *Readiness 2030* banner, this article has emphasised that military readiness must go hand in hand with legal readiness. By analysing the three IHL peacetime obligations related to the conduct of hostilities, it has shown how these duties should inform the EU's push towards strengthening its cyber (defence) capacities. Across all three obligations, one lesson stood out: compliance with IHL during cyber warfare already begins in peacetime.

Firstly, regarding the obligation to disseminate IHL, the analysis demonstrated that teaching and internalising IHL in peacetime is indispensable for its application during armed conflict. In the cyber domain, dissemination requires tailored and sustained efforts: members of the armed forces must be trained not only in general IHL principles, but also in the specificities and legal uncertainties concerning their application to cyber operations. States need to appoint technically knowledgeable legal advisors, ideally embedded within cyber units, and update their military manuals to include comprehensive cyber-specific guidance. Assessing compliance with these recommendations remains challenging, however, due to the scarcity of publicly available information on how States disseminate IHL within their armed forces. At the civilian level, the accessibility of cyber makes it essential to ensure that civilians understand when their conduct may amount to direct participation in hostilities and how they should comply with IHL when conducting such cyber activities. Yet, to date, there is no evidence that the EU and its Member States are engaging in such IHL-focused cyber education of civilians.

Secondly, this study highlighted that two characteristics of cyber render the obligation to take passive precautions particularly important in this domain. Its dual-use nature underscores the need to separate military and civilian networks and cyber infrastructure. Although States often invoke feasibility constraints to avoid action in that regard, this article argued that the EU's wealth and technological capacity, combined with a five-year implementation horizon under *Readiness 2030*, make such claims less convincing. At the same time, the pervasiveness of cyber urges States to take measures aimed at general resilience, such as making backups of important civilian data, distributing protective software, and establishing monitoring and warning systems. Encouragingly, the EU's *Preparedness Union Strategy* and the presence of Computer Emergency Response Teams across all Member States indicate steps in this direction.

Thirdly, the obligation to conduct weapons reviews was highly relevant to this research given *Readiness 2030*'s explicit call to develop offensive cyber capabilities. However, the secrecy surrounding weapons reviews made it difficult to verify which EU Member States have such mechanisms in place, let alone whether they are being adequately adapted to reviewing cyber weapons. Effective cyber-specific reviews require multidisciplinary committees that include cyber-technical experts. They also depend on the ability to revisit reviews as operational environments evolve, the implementation of appropriate testing methods and technical standards, and the

involvement of the private sector. Furthermore, due to the ongoing discussions on the application of IHL to cyber, a review of a cyber weapon can only take place if the reviewing entity has established its position on the matter. In that regard, the current position papers of the EU and its Member States are too generic to guide reviews, though it is possible that internal documents provide more detail. Still, the EU should issue a more comprehensive position paper and assist its Member States in developing their own.

Looking ahead, future research could contribute by conducting qualitative empirical work, such as interviews with government officials, to explore how States are actually implementing peacetime IHL obligations in the cyber context. It could, for instance, examine how the application of IHL to cyber is disseminated within the armed forces, how military legal advisors interact with technical personnel, how the private sector is involved in carrying out passive precautions, and how Article 36 reviews of cyber weapons are conducted behind the scenes. Such research would help to identify the practical obstacles States face and bridge the current gap between formal commitments and operational reality.