Granite Journal
The University of Aberdeen Postgraduate Interdisciplinary Journal

Crossing Borders: International Collaboration and Cooperation in Research

International Research Cooperation in The Tallinn Manual

Ian Clark, Department of Divinity, University of Aberdeen

Abstract: Contemporary military strategy exhibits a growing dependence on operations conducted within the domain of cyberspace. These operations are increasingly capable of inflicting tangible harm in the physical world, degrading essential infrastructure, and inducing widespread disruption. Nevertheless, a debate persists regarding the applicability of established international legal frameworks governing armed conflict to cyberwarfare. The *Tallinn Manual*, a non-binding academic study exploring the intersection of international law and cyberwarfare, plays a pivotal role in disentangling this complex debate by bridging international law, professional military ethics, and technical disciplines. In addition to being an indispensable guide to the legality of cyberwarfare operations, this paper argues that the *Tallinn Manual* represents a successful example of interdisciplinary collaboration and international cooperation, which may serve as a model for addressing a myriad of challenging legal and moral realities.

Keywords: cyberwarfare, international law, military ethics, *Tallinn Manual*, international cooperation

1 Introduction

Military history is a story of technological change. While the nature of war has remained a violent enterprise designed to compel political change, the methods and means of carrying out that violence have changed and evolved with time. Many written works of global military history, such as John Keegan's classic *A History of Warfare* (1993) or the *Cambridge History of Warfare* (2020), divide their analysis into historical epochs defined by particular technological advancements which transformed how war was waged. It is often true that the development and application of new military technologies and tactics are accompanied by significant debate over the lawfulness and morality of their usage, an interesting example being medieval attempts to prohibit the use of the crossbow in war (Clough and Stiltner, 2007, pp. 111-112). In the contemporary world, a new epoch may well be emerging defined by the ability of militaries to conduct operations within and through the domain of cyberspace. Exploiting information systems for military purposes not only presents a new way of fighting and exerting force but also presents unique challenges to existing international laws governing military wartime conduct. To meaningfully and proactively address these challenges, a resource known as the *Tallinn Manual* has emerged as an indispensable guide for legal advisors and scholars. In this paper, I will argue that the success of the *Tallinn Manual* can be attributed in no small part to the intentionally interdisciplinary and cross-cultural character of its development. Additionally, this article will suggest that three best practices in collaborative research can be extrapolated from the Tallinn Manual Project. These best practices are researcher diversity, end-user integration, and political neutrality.

2 Cyberwarfare and the challenge to International Humanitarian Law

Before commenting explicitly on the *Tallinn Manual* and the academic project that enabled it, it is important to contextualise the issues of international law and cyberwarfare. Given that these two topics are the subjects of the *Tallinn Manual*, it is necessary to offer some insight into each. International Humanitarian Law (IHL), also

called the Laws of Armed Conflict (LOAC), refers to a body of international laws and treaties governing military conduct in war. In a significant way, IHL has been shaped by the Just War Tradition (JWT), which emerged from historical Christian moral thought on wartime conduct (commonly referred to as *jus in bello* principles) (Alexander, 2015). As such, dominant themes in IHL relate to *jus in bello* criteria of noncombatant immunity (frequently referred to as the principle of discrimination), proportionality, and the protection of the legal rights of combatants and civilians (Clough and Stiltner, 2007, p. 59; International Committee of the Red Cross (ICRC), 2015). At the heart of IHL are the Geneva Conventions of 1949 and their Additional Protocols (ICRC, 2014). While IHL is intended to be enforced by individual states, various international tribunals and courts have been set up to work on behalf of the global community when they fail to do so (ICRC, 2010). Collectively, IHL works to regulate and restrict war and wartime conduct to facilitate harm reduction.

In today's world, which is increasingly characterised by – and reliant upon – digital technologies, cyberspace is emerging as a conflict zone in military operations, both inside and outside of conventional armed conflict. For instance, in the ongoing conflict between Ukraine and Russia, cyber weapons have been deployed alongside conventional weapons and tactics (Clark, 2023). Likewise, cyber weapons have been deployed in isolation apart from conventional military engagement, as was the case with the notable Stuxnet attack against the Iranian nuclear program in 2010 (Lindsay, 2013). While there have been limited examples to date of cyber-attacks directly resulting in physical destruction or death, evidence suggests that cyber operations are being used in some modern conflicts in a manner that seeks to expand the lethality of war, rather than minimise it (Clark, 2023). In addition, a growing body of evidence suggests that critical infrastructure, including essential civilian infrastructure, are both vulnerable to attack and being actively targeted. For instance, in testimony delivered before a select committee of the United States House of Representatives in 2024, Christopher Wray, the Director of the Federal Bureau of Investigation (FBI), noted that:

"*China's hackers are positioning on [sic] American infrastructure in preparation to wreak havoc and cause real-world harm to American citizens and communities*" (Wray, 2024).

Such harm could take the form of degraded essential utilities and electrical grids and could, theoretically, result in physical destruction and death, particularly in a scenario such as an attack on control systems for critical passenger infrastructure like railways or aircraft.

IHL's scope is generally limited to military operations carried out in the context of armed conflict (Sassòli, 2019). Herein lies the first significant challenge that military cyber operations pose to IHL: operations taken in cyberspace often blur the once conspicuous boundaries between war and non-war, especially when cyber operations are carried out apart from conventional warfare. Determining if IHL applies to a particular act or set of acts is typically dependent on whether the event in question occurred in the context of armed conflict. It is not universally apparent whether a clear "yes" or "no" could be declared in the context of a standalone cyber-attack. Returning to the Stuxnet attack, one might note that while the cyber-attack itself was destructive, no nation was formally at war with Iran at the time: no troops were engaging in kinetic violence, and nobody was killed or injured in the attack. All of which indicates that the attack was highly discriminate (Lucas, 2017, p. 59). In another prominent example, the Baltic nation of Estonia experienced a series of sustained cyber-attacks in the spring of 2007, widely believed to have been attributable to Russia (Schmitt, 2017b, p. 376). While these attacks had a significant and disruptive impact on Estonia's financial and political institutions, they were not understood by the North Atlantic Treaty Organisation (NATO) to have been acts of war due to their lack of physical destruction. As such, the attacks did not cause the military alliance to trigger its Article Five mutual defence mandates (McGuinness, 2017). Nevertheless, one advisor to the President of the United States noted:

"*Estonia has built their future on having a high-tech government and economy, and they've basically been brought to their knees because of these attacks*" (Herzog, 2011, p. 52).

The Estonian attack would serve as the catalyst for what would become the Tallinn Manual Project.

As Article 51 of the United Nations (UN) Charter indicates, member states are authorised to utilise military force against another state or party "if an armed attack occurs against" that nation (UN Charter, 1945, Article 51). The question of whether a cyber-attack can represent an "armed attack," and if so, on what grounds, can pose a significant challenge to existing bodies of international law. Thomas Rid (2013) has notably suggested that cyber operations generally fail to meet the threshold of an armed attack because they are generally non-destructive (Rid, 2013, p. 1). By contrast, Clark and Knake laid out cases where cyber operations could result in death and destruction on a significant scale. For instance, in the case of attacks against air traffic and railroad control systems, fuel pipelines, dams, satellites, and other high-impact targets (Clark and Knake, 2010, pp. 64-68).

While these questions present unique challenges to international law, their existence should not be understood as implying that current international law does not apply to military activity taken in cyberspace or that the law is silent concerning the domain of cyberspace. The view that the law does not apply to operations in cyberspace was widely considered in the 1990s and early 2000s when the Internet was beginning to become more widely integrated into households, businesses, and military affairs. For instance, in a 1996 speech titled *Declaration of Independence of Cyberspace*, delivered at the World Economic Forum, John Barrow, a notable cyber-activist, called cyberspace a domain where "legal concepts of property, expression, identity, movement, and context do not apply" (Barlow, 1996, p. 3). As the Internet, and society's relationship to it, has matured so too has thinking relating to the intersection of international law and conduct in the domain of cyberspace. Today, it is generally no longer disputed that conduct in cyberspace is subject to international law, a fact which has been affirmed and reaffirmed consistently (Tsagourias, 2021, p. 9). Today's question is not "Does international law apply to military conduct in cyberspace?" but rather, "How does international law apply to military conduct in cyberspace?" The *Tallinn Manual*, a scholarly assessment of the relationship between IHL and cyberwarfare, seeks to answer that question and, in so doing, serves as a guide to governments, militaries, and international institutions.

The Tallinn Manual Project is an ongoing effort that has published two editions of the *Tallinn Manual* to date. The first edition of the Tallinn Manual (Tallinn 1.0) was "limited to international law on the use of force and international humanitarian law" (Koenders, 2017, p. xxvi). Yet, in the second version of the Tallinn Manual (Tallinn 2.0), it was acknowledged that such a restricted scope failed to comprehensively engage the issue of military cyber operations, most of which occur outside the context of war as it has been conventionally understood. As a result, Tallinn 2.0 was expanded to include "international law governing cyber activities occurring in peacetime" (Ilves, 2017, p. xxiii). The resulting document represents a comprehensive assessment of the application of international law to militarily significant cyber operations occurring both in times of war and non-war. The in-development third version of the Tallinn Manual (Tallinn 3.0) will revise and update existing chapters and integrate new ones relating to the actions and statements of both international bodies and individual states (CCDCOE, 2024).

3 Developing The *Tallinn Manual*

The strength of the *Tallinn Manual* rests in its acknowledgement that cyberwarfare is a complex phenomenon and that an accurate and practical assessment of it requires a broad range of skill sets, including legal scholars, cyber security experts, military professionals, computer scientists, human rights experts, and others. Michael Schmitt, director of the Tallinn Manual Projects, commented that: "The 154 black letter rules of the *Tallinn Manual 2.0* reflect the consensus of our diverse, experienced and global group of experts" (Atlantic Council, 2017). With significant intentionality, the International Group of Experts was selected not merely for each member's robust and applicable experience but also for their diversity. The same could be said of those chosen as contributors, peer reviewers, and legal researchers. This diversity reflects nationality, gender, age, language, types of institutions served (i.e., traditional universities and military universities, as well as public and private institutions), military experience, and scholarly specialisations (Schmitt, 2017c, p xii-xviii).

The second and most current version of the *Tallinn Manual* (Tallinn 2.0) was prepared by an International Group of Experts comprised of 21 specialists,

supplemented by nine additional contributors. The work was supported by 16 legal researchers and reviewed by 58 legal and two technical peer reviewers. In this article, I have sought to analyse the backgrounds and associations of the International Group of Experts members, as well as the contributors, researchers, and reviewers who supported the project. To do so, I examined publicly available resources related to the individuals named within the *Tallinn Manual* who had contributed to the project, successfully locating and identifying information for each named contributor. In most cases, comprehensive biographical information was readily available for the individuals, often through the institutions they serve, or through media reporting. Information about the gender identity of individual contributors was based on the pronouns utilised within their publicly available biographical information. Military status (active duty or veteran) was also determined based on available biographical information or through official military titles (such as a military rank identifier). Institutional information (such as the physical location of a university) was determined based on publicly available information about that institution. In other cases, institutional information was based on national identifiers (such as the Netherlands Defence Academy, Royal Military College of Canada, or United States Air Force).

It is worth noting that as my analysis is based exclusively on publicly available biographical information, there is a possibility that data may be incomplete. For instance, it is conceivable that biographical information for a scholar may not include prior military experience or that a scholar affiliated with an institution based in the United Kingdom may undertake their work in a different nation. Due to these potentially limiting factors, the data below is presented with the intention of providing a high-level demographic overview of the Tallinn Manual Project team.

Table 1: Analysis of Tallinn Manual Project participants (excluding legal researchers)

	International Group of Experts		Other Contributors		Peer Reviewers	
	Number	%	Number	%	Number	%
Total Number	21		9		60	
Number of Institutions Represented	24		9		49	
Male	19	90.50%	9	100.00%	48	80.00%
Female	2	9.50%	0	0.00%	12	20.00%
Military Experience (Active Duty of Veteran)	5	23.80%	4	44.40%	17	28.30%

As indicated in Table 1, of the 21 individuals comprising the International Group of Experts, 24 different institutions were represented (some scholars represented multiple institutions). The represented institutions are based in the United Kingdom, the United States, the Netherlands, Israel, Japan, China, Germany, Australia, and Kazakhstan. Nations represented by the nine additional contributors to the project include Sweden and Canada.

Analysis of the above data indicates significant involvement in the Tallinn Manual Project from a broad and global consortium of specialists. The considerable percentage of project participants who possessed military experience (either through active or prior service) demonstrates an intentional focus on the part of the project to ensure that the manual would be relevant to end users. Of notable concern, however, is the small number of women included within the project team, especially within the International Group of Experts and "Other Contributors" elements. While it should be noted that the managing editor of the Tallinn Manual 2.0 project is female, the imbalance overall between male and female project participants represents an important gap within the project's otherwise highly diverse and intersectional approach.

To enhance the international collaboration present within the drafting of Tallinn 2.0, the Netherlands Ministry of Foreign Affairs convened the Hague Process, which gathered delegations from over 50 nations and international organisations to provide additional feedback on the working drafts of the *Manual*, including representatives from the five

permanent members of the UN Security Council (Schmitt, 2018, p. 6). This element of the drafting process, which was not a component part of the first version of the Manual, enabled greater diversity in perspectives. It also allowed the International Group of Experts and collaborators to refine their work based on feedback from governmental and military personnel, as well as that of peacekeeping and humanitarian organisations such as the UN and the Red Cross, thus gaining buy-in from participating states and agencies. This integration of end users and stakeholders helped to refine Tallin 2.0, ensuring it would be a beneficial product for those who would eventually use it.

An additional benefit to the drafting process of the *Tallinn Manual* is its approach to independence and neutrality. While a wide range of individuals contributed to the project, the *Tallinn Manual* is an independent publication that does not reflect the official views of any state, military force, or agency, including the project's sponsors and facilitators (such as NATO), and the states which participated in the Hague Process. The *Tallinn Manual*, then, only officially represents the views of the International Group of Experts, who were acting in their individual capacities as subject matter experts. The text of the Manual also makes clear that contributors employed by their nation's armed forces or otherwise serving in government do not necessarily represent the views of their nations. Additionally, while NATO convened the Tallinn Manual Project, the resource was published by Oxford University Press and not by NATO or any other governmental body. This allows the *Tallinn Manual* to be treated as a relatively neutral source. To assist in this effort, the wording of the Tallinn Rules takes care to express only *lex lata* (the law as it is) as opposed to *lex ferenda* (the law as it should be) (Schmitt, 2017a, p. 3).

While the *Tallinn Manual*'s development represents a remarkable global collaboration on a complex topic, there is scope for criticism and growth. Most conspicuously, no faculty members serving universities in the Global South were represented within the International Group of Experts. Furthermore, the limited number of women in the International Group of Experts leaves scope for greater gender parity in drafting subsequent versions of the manual. From the perspective of expertise, it also appears that academic ethicists were generally excluded from the drafting process, potentially resulting in the loss of a useful perspective that may have enhanced the moral clarity of the Manual's analysis, especially in contexts where legal ambiguity

existed. Such exclusion may have been driven by a concern that the integration of ethicists into the project may have shifted the project towards a *lex ferenda* orientation. However, the perspective of academic ethicists may have enhanced and nuanced some of Tallinn Rules, especially those dealing with cyberwar's impacts on noncombatants.

4 The *Tallinn Manual*: Providing Clarity and Direction

In cases where the law is silent or ambiguous as it pertains to military conduct in cyberspace, the *Tallinn Manual* serves to provide clarity, rooted in the scholarly judgement of a diverse cross-section of professionals, around the application of international laws related to the use of force in and through the domain of cyberspace. This involves what Dan Efrony and Yuval Shany have referred to as "the drawing of analogies between kinetic (physical) and cybernetic domains" (2018, p. 584). Efrony and Shany note that this is possible because cyber attacks can generate military outcomes comparable to kinetic attacks and often occur across borders. In addition, these scholars state that analogies can be drawn "between state sovereignty or state control over land, sea, and airspace to state sovereignty or state control over parts of the infrastructure that comprises cyberspace," amongst other points of comparison (Efrony and Shany, 2018, p. 584). While applying this approach to cyberwarfare is novel to the *Tallinn Manual*, several other manuals in this area have been created for similarly contentious and challenging legal issues in the past. Examples include the *San Remo Manual* on International Law Applicable to Armed Conflicts at Sea (adopted 1994) and the *Manual on International Law Applicable to Air and Missile Warfare* (adopted 2009). The primary intended audience for legal manuals, including the *Tallinn Manual*, is governmental and military legal advisors, though the manuals are also of interest to academics and policymakers.

Tallinn 2.0 offers 154 rules divided across 20 subject areas. While these rules are not legally binding on their own, they represent a scholarly consensus of the ways in which binding international law applies to conduct in cyberspace, both in times of war and non-war. These subject areas and the number of corresponding rules are as follows:

	SUBJECT AREA	NUMBER OF RULES
1	Sovereignty	5
2	Due diligence	2
3	Jurisdiction	6
4	Law of international responsibility	11
5	Cyber operations not *per se* regulated by international law	2
6	International human rights law	5
7	Diplomatic and consular law	6
8	Law of the sea	9
9	Air law	3
10	Space law	3
11	International telecommunication law	4
12	Peaceful settlement	1
13	Prohibition of intervention	2
14	The use of force	12
15	Collective security	4
16	The law of armed conflict generally	6
17	Conduct of hostilities	44
18	Certain persons, objectives, and activities	15
19	Occupation	4
20	Neutrality	5

As non-binding scholarly assessments, measuring the success of the Tallinn Rules or the more expansive Tallinn Manual Project is challenging. The Tallinn Rules are not legal rulings to be formally adopted, but insights that enable richer topical dialogue and may eventually shape or help refine international law. Likewise, given the covert nature of most military cyber operations, it is likely not possible to meaningfully assess compliance with the rules while relying exclusively on open-source information. On this point, Efrony and Shany note that:

"*The uneasy "fit" between traditional international law principles governing the exercise of state power inside and outside its territory, and the regulation of a*

deterritorialized cyberspace, provides one explanation for the preference given by some states involved in cyber operation to retaining silence and maintaining ambiguity in relation to their legal position" (2018, p. 654).

In short, assessing the Tallinn Rules' operational impact on cyberwarfare in practice is challenging.

There is, however, good reason to celebrate the development of the *Tallinn Manual*. The Manual has spurred significant scholarly dialogue on the intersection of cyberwarfare and international law, thus elevating the issue to a more central position in the field. Likewise, within their published defence and cyber strategies, nations are increasingly making note of their commitment to conduct operations in cyberspace in line with international law. For instance, the 2022 National Cyber Strategy for the United Kingdom notes a commitment to the

"[...] *responsible use of our offensive cyber capabilities, consistent with both UK and international law and our publicly stated positions, in contrast with the indiscriminate activities of some of our adversaries*" (HM Government, 2022, p. 23).

Similar sentiments have been expressed by the United States (White House, 2023, p. 29). International bodies, notably the UN, have debated the regulation of military cyber operations numerous times in recent years, demonstrating the prioritisation of the issue within the international community and that it represents a worthy pursuit for international cooperation. In these efforts, the *Tallinn Manual* plays an important role by serving as a point of reference, reflecting the scholarly consensus of specialists in international law, technology, and warfare (Efrony and Shany, 2018, p. 648).

5 A Model for Future Research Projects

Drawing on the example of the Tallinn Manual Project, researchers engaging with similarly complex global issues may benefit from adopting and applying some of the best practices in international, interdisciplinary, and inter-organisational research exhibited by the International Group of Experts and colleagues. In particular, based on my assessment of the Tallinn Manual Project in section 3 of this article, I have identified three foundational elements that may resonate broadly with researchers. These include

the *Tallinn Manual's* (1) intentional use of a diverse pool of international researchers, (2) the integration of end users and stakeholders into the drafting process, and (3) the project's intentional efforts to pursue political and national neutrality.

1) Including an intentionally diverse pool of researchers: complex international challenges require a response that proactively integrates a diverse and global body of experts. Such intentionality helps avoid a colonial mindset, helping to ensure that the end product more fully reflects the international audience it intends to impact. Care should be taken, as it was with the Tallinn Manual Project, to fully integrate specialists from across the landscape of applicable disciplines. We may also learn from some of the *Tallinn Manual's* gaps by suggesting that future projects should include scholars from institutions in the Global South more intentionally, and ensure that the voices and perspectives of female scholars and professionals are fairly represented. Despite its gaps, the intentional use of a diverse body of researchers and experts is an important contribution of the *Tallinn Manual*. As Sue Silverman notes in no uncertain terms, "International law suffers from a lack of diversity," especially regarding race, gender, and the perspectives of Third World nations (Silverman, 2024, p. 81). While the Tallinn Manual Project may employ diversity imperfectly, it does so seriously. Future collaborative research projects, especially those addressing international law, may be able to build on the model used by the Tallinn Manual Project in their own efforts to ensure greater representation.

2) Soliciting practical feedback from the intended target audience during the drafting phase: projects like the *Tallinn Manual* may be academic in nature, but they also recognise that their intended audience is beyond the academy. When this is the case, the Tallinn Manual Project – particularly through its integration of the Hague Process – offers a timely reminder of the importance of collaborating with end users of the research. This helps establish buy-in from those end users but also helps to ensure that the end product is useful, addresses operational concerns, and is free from obvious political, cultural, or national bias. The *Tallinn Manual* is a product of scholarly work, however, it clearly recognises that its impacts are broad and of distinct interest to legal bodies, militaries, governments, and international organisations. By integrating these end users into the drafting and review process, the Tallinn Manual Project produced a

manual that was well-received and widely considered to be helpful for both scholarly and practical purposes. Stakeholder engagement is an often underutilised tool in international law scholarship, though it is used widely in other research areas, such as in the study of corporate social responsibility (CSR) (Aversano et al., 2022, pp. 1-6). Such an approach is increasingly being recognised as a best practice within international law-related work, as Joost Pauwelyn has noted. For instance, Pauwelyn points to efforts related to pandemic treaties following the global Covid-19 pandemic (2023, pp. 51-65). The *Tallinn Manual*'s embrace of such a practice may serve to broaden the ways that stakeholders and end users can be meaningfully integrated into the drafting of scholarship related to issues in international law.

3) Neutrality: internationally oriented research projects are likely to be more widely embraced by a global audience when they are seen as genuinely objective research as opposed to political instruments aligned with the interests of a particular state or international organisation. Achieving this necessitates that care be taken to clarify that research participants are acting in their individual capacity as experts within a given field (as opposed to representatives of a state or organisation), publishing the work through a non-politically aligned publisher, ensuring that the research content and outcomes have broad applicability, and inviting broad input which transcends known political divides. In the case of the Tallinn Manual Project, deliberate care was taken to avoid aligning the work with any nation, political ideology, or policy. In this endeavour, the *Tallinn Manual's* efforts to sustain political and national neutrality within the project will likely have several benefits for end users. As scholars like Peter Triantafillou have noted, "an ethos of neutrality," especially in research related to public administration, may assist in creating policies that help to curb abuses while minimising other economic, strategic, and political risks, and helping civil servants to craft and execute impartial and enduring strategies (Triantafillou, 2015, pp. 174).

In the case of the *Tallinn Manual*, an ethos of neutrality also supports the Manual's ambition to offer a *lex lata* interpretative framework of international law. It must be noted, however, that there is a close connection between international law governing armed conflict and the ethics of warfare. The pursuit of neutrality in documents such as the *Tallinn Manual* and related projects may degrade the ability of such projects to offer

ethical guidance (though, admittedly, this is not the intent of the manual). Future research projects, especially those with a broad or international audience, may wish to consider employing all or some of *Tallinn Manual's* neutrality procedures.

6 Conclusion

Cyberwarfare represents an emerging tool of warfare and disruption in the contemporary world. As a comparatively new military technology, policymakers and scholars are actively engaging with open and pressing questions about the legal parameters of military operations conducted in cyberspace. While some manifestations of cyber operations overlap with existing law, cyberwarfare raises novel questions in international law. The non-binding *Tallinn Manual* represents an important tool for addressing many of those questions and has served as a catalyst for political, academic, and humanitarian engagement with the issue of how cyber operations intersect with existing international law. In this article, I have argued that the *Tallinn Manual* represents a significant step forward in guiding and shaping discussions and thoughts on applying international law to cyberwarfare. I have further argued that the success of the *Tallinn Manual* is a product of its intentionally international, interdisciplinary & inter-organisational approach to preparing, reviewing, and editing the document. Finally, drawing on the example of the Tallinn Manual Project, I have suggested that three best practices in international research collaboration and cooperation – diversity, target audience inclusion, and neutrality – have enhanced *the Tallinn Manual* and may serve similar research projects positively.

7 References

1. Alexander, A. (2015) 'A Short History of International Humanitarian Law', *European Journal of International Law* [Online], 26 (1), pp. 109–138.
2. Atlantic Council (2017) Tallinn Manual 2.0 Clarifies How International Law Applies to Cyber Operations. The Atlantic Council (Press Release). https://www.atlanticcouncil.org/news/press-releases/tallinn-manual-2-0-clarifies-how-international-law-applies-to-cyber-operations/ (Accessed 16 May 2024).
3. Aversano, N., Sannino, G., Aversano, N., Sannino, G., Polcini, P. T., & Nicolò, G. (2022) *Corporate Social Responsibility, Stakeholder Engagement, and Universities*. MDPI - Multidisciplinary Digital Publishing Institute.
4. Barlow, J. P. (1996) *A Declaration of The Independence of Cyberspace*. World Economic Forum. https://www.weforum.org/agenda/2018/02/a-declaration-of-the-independence-of-cyberspace/ (Accessed 1 June 2024).
5. Clark, I. A. (2023) 'The Ethical Character of Russia's Offensive Cyber Operations in Ukraine: Testing the Principle of Double Effect', *Journal of Advanced Military Studies* [Online], 14 (2), pp. 88–101.
6. Clough, D. L., & Stiltner, B. (2007) *Faith and Force: A Christian Debate about War*, Washington: Georgetown University Press. Available from: ProQuest Ebook Central (Accessed 17 May 2024).
7. Efrony, D. & Shany, Y. (2018) 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice', *The American Journal of International Law* [Online], 112 (4), pp. 583–657.
8. Herzog, S. (2011) 'Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses', *Journal of Strategic Security* [Online], 4 (2), pp. 49–60.
9. HM Government (2022) *National Cyber Strategy 2022: Pioneering a cyber future with the whole of the UK*. HM Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf (Accessed 23 April 2024).

10. ICRC (International Committee of the Red Cross) (2010) *International Criminal Jurisdiction*. International Committee of the Red Cross. https://www.icrc.org/en/document/international-criminal-jurisdiction (Accessed 25 April 2024).
11. ICRC (International Committee of the Red Cross) (2014) *The Geneva Conventions of 1949 and their Additional Protocols*. International Committee of the Red Cross. https://www.icrc.org/en/document/geneva-conventions-1949-additional-protocols (Accessed 18 April 2024).
12. ICRC (International Committee of the Red Cross) (2015) *What is IHL?*. International Committee of the Red Cross. https://www.icrc.org/en/document/what-ihl#:~:text=It%20is%20a%20branch%20of%20public%20international%20law,and%20to%20restrict%20means%20and%20methods%20of%20warfare. (Accessed 12 April 2024).
13. Ilves, T.H. & Schmitt, M.N. (2017) 'Foreword', in Schmitt, M. N. (ed.) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, pp. xxiii–xxiv.
14. Koenders, B. & Schmitt, M.N. (2017) 'Foreword', in Schmitt, M. N. (ed.) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, pp. xxv–xxvii.
15. Lindsay, J. R. (2013) 'Stuxnet and the Limits of Cyber Warfare', *Security Studies* [Online], 22 (3), pp. 365–404.
16. Lucas, G. (2017) *Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare*. 1st edition [Online]. New York: Oxford University Press.
17. McGuinness, D. (2017) 'How a Cyber Attack Transformed Estonia', *BBC News*. https://www.bbc.co.uk/news/39655415 (Accessed 7 May 2024).
18. NATO, Cooperative Cyber Defence Centre of Excellence (CCDCOE) (2024) *The Tallinn Manual, Research*. North Atlantic Treaty Organization (NATO) https://ccdcoe.org/research/tallinn-manual/ (Accessed 13 May 2024).
19. Pauwelyn, J. (2023) 'Taking Stakeholder Engagement in International Policy-Making Seriously: Is the WTO Finally Opening Up?', *Journal of International Economic Law*, 26(1), pp. 51–65.

20. Rid, T. (2013) *Cyber War Will Not Take Place*. 1st edition. New York: Oxford University Press.
21. Sassòli, M. (2019) 'Scope of Application: When Does IHL Apply?' in Sassòli, M. (ed.) *International Humanitarian Law*. [Online]. United Kingdom: Edward Elgar Publishing Limited. pp. 158-174.
22. Schmitt, M.N. (2019) 'Wired warfare 3.0: Protecting the civilian population during cyber operations', *International Review of the Red Cross*, 101(910), pp. 333–355.
23. Schmitt, M.N. (2017a) 'Introduction', in Schmitt, M.N. (ed.) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, pp. 1–8.
24. Schmitt, M.N. (2017b) 'The law of armed conflict generally', in Schmitt, M. N. (ed.) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, pp. 375–400.
25. Schmitt, M.N. (2017c) 'Tallinn Manual 2.0 International Group of Experts and Other Participants', in Schmitt, M. N. (ed.) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, pp. xii–xviii.
    - Please note that the statistics related to the International Group of Experts I presented in Section 4 have been compiled based on information in this chapter of the Tallinn Manual version 2.0.
26. Silverman, S. (2024) 'Examining the Society in Which We Are Educated: Applying Critical Approaches to International Law Research', *Legal Reference Services Quarterly*, 43(1–2), pp. 81–103.
27. Triantafillou, P. (2015) 'The Politics of Neutrality and the Changing Role of Expertise in Public Administration', *Administrative Theory & Praxis*, 37(3), pp. 174–187.
28. Tsagourias, N.K. (2021) 'The legal status of cyberspace: sovereignty redux?,' in Tsagourias, N.K. & Buchan, R. (eds.) *Research Handbook on International Law and Cyberspace*. 2nd edition. Cheltenham, UK: Edward Elgar Publishing Limited, pp. 9-31.

29. United Nations (1945) *Charter of the United Nations*. https://treaties.un.org/doc/Publication/UNTS/No%20Volume/Part/un_charter.pdf (Accessed 2 May 2024).
30. White House (2023) *National Cybersecurity Strategy*. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf (Accessed 2 June 2024).
31. Wray, C. (2024) *Director Wray's Opening Statement to the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party*. Federal Bureau of Investigation (FBI). https://www.fbi.gov/news/speeches/director-wrays-opening-statement-to-the-house-select-committee-on-the-chinese-communist-party (Accessed 2 June 2024).