

DOI 10.5817/MUJLT2025-2-7

GIVE REALISTIC CYBER PEACE A CHANCE *

by

DAN JERKER B. SVANTESSON †

The topic of Cyber peace is receiving surprisingly little attention. Having considered some characteristics of Cyberspace affecting the topic of Cyber peace and having considered whether we benefit from trying to strictly define what we mean by Cyber peace, the article proceeds to offer a defence for the role that law may play towards Cyber peace. Against this background, the article proposes a focus on the three criteria Alfred Nobel articulated for his famous Peace Prize: (1) advance fellowship among nations, (2) the abolition or reduction of standing armies, and (3) the establishment and promotion of peace congresses, as a suitable point of departure towards Cyber peace. The article concludes that to move towards Cyber peace we need specific, practical, and realistic actions rather than lofty proclamations. Thus, it calls for the establishment of a realistic "Cyber Peace Agenda" and introduces ongoing work towards such an Agenda under the custodianship of the Norwegian Nobel Institute.

KEY WORDS

Cyber Peace, Cyberwar, Cybersecurity, Information Conflict, Sovereignty

* This article was written during my time as a Fellow at the Norwegian Nobel Institute. I am grateful to all the members of the Institute, as well as the other Fellows I got to work with, for their friendliness and for being so welcoming. I also take this opportunity to thank those who attended, and provided feedback, on the presentations I gave on this topic at the Nobel Peace Center (April 2025) and at the Peace Research Institute Oslo (May 2025).

† Professor, Bond University. Fellow, Norwegian Nobel Institute. Senior Fellow, Social Cyber Institute. E-mail: dasvante@bond.edu.au

1. INTRODUCTION

Cyberspace plays a central role in society. While helpful in many respects, this also creates an unavoidable dependency on Cyberspace. In turn, this dependency is a vulnerability, and it creates an attack surface that hostile actors seek to exploit. Those hostile activities force States to respond by a range of measures aimed at mitigating the associated risks. Conflict – in different forms – is now a prevalent feature of Cyberspace. Against this background, "Cyber peace" is more important than ever. Yet, the topic of Cyber peace is getting limited attention.

This article explores some steps that we can take towards Cyber peace. Such a venture may adopt a range of different starting points and methods. To identify some key steps that we can take towards Cyber peace, I here adopt Alfred Nobel's approach to the Peace Prize as the point of departure. This choice will also guide the structure adopted to a great extent.

In his final will of 1895, Nobel pointed to three criteria for the Peace Prize. As commonly translated, they are: (1) advance fellowship among nations, (2) the abolition or reduction of standing armies, and (3) the establishment and promotion of peace congresses.¹ I will structure the discussion of Cyber peace around these three criteria for two reasons. First, there is obvious value in examining how these criteria may be understood in the modern context of Cyberspace; after all, they are guiding the way in which the Peace Prize is awarded, and the Nobel Peace Prize is doubtlessly impacting how we think about peace. Second, while, by no means suggesting that this is the only option, I do contend that these three criteria may provide a helpful structure for analysing what is involved in the idea of "Cyber peace", and this is my attempt at showing why I have reached that conclusion.

The discussions result in a proposal for a "Realistic Cyber Peace Agenda" to include a set of proposed actions we may take in the pursuit of Cyber peace, and some thoughts on how this Agenda may be structured, developed, and used.

However, to prepare the ground for these discussions, it is necessary to first make some rudimentary observations about the nature of Cyberspace and what Cyber peace – or peace in Cyberspace – means and may look like. It is what we can observe in those discussions that has prompted my call for us to all be realistic about what we may expect. Yet, inaction is, in my view, not an option. I also briefly discuss a line of criticism that has been directed at the role that law may play in securing Cyber peace. As my discussion is

¹ The Nobel Prize. (2025) *Full text of Alfred Nobel's will*. [online] Available from: <https://www.nobelprize.org/alfred-nobel/alfred-nobels-will/> [accessed 11 August 2025].

largely focused on the law, it is appropriate to advance some defences against such criticism.

To conclude these introductory remarks, I hasten to acknowledge that there is much that could be said about the various topics addressed within this article. Topics such as the principle of distinction, the concept of sovereignty, and the issue of attribution deserve – and have received – detailed treatment elsewhere. Adding substantially to that is, however, not the aim here. Nor do I aim to comprehensively and systematically restate what others have said on such topics. Here the aim is to provide more of an examples-driven "birds eye" view of the topic of Cyber peace via a small selection of useful illustrations so as to hopefully point to some possible paths for the important, more detailed, work that lies ahead on the road towards Cyber peace.

2. THE NATURE AND ROLES OF CYBERSPACE

To understand Cyber peace, we must first realise that Cyberspace is both (1) its own war-fighting domain, and (2) supporting all other war-fighting domains (land, sea, air, and space). The former is illustrated e.g., by cyberattacks. But, as is elaborated upon below, it is also reasonable to see the Cyberspace domain as something broader than such cybersecurity issues. For example, it also includes information and cognitive warfare.

The fact that Cyberspace is supporting all other war-fighting domains is apparent when we consider the role that Cyberspace plays in everything from communications and targeting to logistics, situational awareness, and Command and Control. Especially if we include Cyberspace supporting all other war-fighting domains when we discuss Cyber peace, it is clear that offline peace is a necessary, but not sufficient, condition for Cyber peace; that is, we cannot have Cyber peace without offline peace, but offline peace does not guarantee Cyber peace. In contrast, perhaps it is possible to argue that we may have offline peace despite not having Cyber peace. In the end, this obviously comes down to how we chose to delineate Cyber peace from offline peace, and perhaps that distinction does not serve us as well as may instinctively be assumed. We will have reason to return to that topic a little later.

To complete the picture, before we can progress further, it must also be noted that, even where we approach Cyberspace as its own distinct war-fighting domain, this domain is not entirely cut off from the "real" physical world; after all, a cyberattack will often have serious real-world implications. In severe cases they may e.g., involve shutting down a hospital or causing a dam to open and cause flooding. This connection

between Cyberspace and the offline world is not unique to Cyberspace as a war-fighting domain. We see this also in many other settings; for example, cyber bullying – that occurs online – affects real people in the real world. This interconnectedness between Cyberspace and the offline world must always be kept in mind in any discussion of Cyber peace.

At any rate, perhaps the most important observation we can make when discussing the nature and roles of Cyberspace, is that Cyberspace offers an alternative means to achieving strategic gains historically unattainable without physical war. This comes in many different forms but is perhaps best illustrated by the so-called cognitive warfare that commonly forms part of the Cyberspace domain. As noted in the 2024 edition of US Department of Defense's annual report on Military and Security Developments Involving the People's Republic of China. "PLA articles on CDO [cognitive domain operations] state that seizing mind dominance in the cognitive domain and subduing the enemy without fighting is the highest realm of warfare."²

Importantly, all this points to just how multifaceted is the Cyberspace domain. Most people may immediately think of cyberattacks, but the Cyberspace domain is also characterised e.g., by a strong emphasis on information war (or perhaps better expressed as "information conflict"), espionage, and Open-Source Intelligence (OSINT). This means that Cyber conflict and Cyber hostilities can take many different forms.

Another noteworthy aspect of the Cyberspace domain is that it often is part of what is commonly discussed as the "grey zone" or "hybrid warfare". Put simply, these concepts, when used properly, seek to highlight the fact that Cyberspace activities frequently are carried out in times without open hostilities, and below the threshold for what counts as an "armed attack" under United Nations Charter, Article 51 (which then limits the defenders options), yet in times of high tension and with potentially serious effects on the victim State. We will have reason to examine this matter in more detail below. However, before leaving this topic, it is important to emphasise that, while the Cyberspace domain often is discussed in terms of "grey zone" or "hybrid warfare", Cyber operations can, and do, occur independently of hybrid strategies.

Finally, before leaving the discussion of the nature and roles of Cyberspace, it is also relevant to make some observations about the special features, or characteristics, of Cyberspace that affect these roles. First, it

² U.S. Department of Defense (2024) *Military and Security Developments Involving the People's Republic of China 2024*. [online] Available from: <https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF> [accessed 11 August 2025].

is both common and useful to discuss the different "layers" of the Cyber domain. There is, of course, a physical layer made up of hardware in various forms such as the servers and cables that connect us. The significance of the physical layer from a Cyber defence perspective has been put on display lately with the large number of incidents in which ships from certain States have managed to accidentally, negligently, or intentionally, cut undersea communications cables e.g. in the Baltic Sea and around Taiwan.

In addition to that physical layer, we can distinguish between the logic layer consisting of software and applications, the data layer made up of the data that in many ways is the "lifeblood" of the Cyber landscape,³ and the social, persona, or cognitive layer made up of persons, real or fake, who act in one way or another online. All these layers, not just the physical layer, can be subject to various forms of attacks and they all need to be defended.

The second special feature of Cyberspace that I want to mention is its so-called "borderlessness". While we are used to our physical world being divided by various types of borders, whether they are between different States or within States, those legal constructs do not naturally map onto any of the mentioned layers apart from (to a degree) the physical layer. For example, data can generally flow easily across the legal constructs we call State borders, and different communities in the social layer may be organised e.g., according to interests rather than geographical locations.

A consequence of the noted "borderlessness" is that the Internet caters for a completely different degree of interconnectedness between people in different States than we are used to from the offline world. Many positive consequences can flow from this increased cross-border interaction. However, it also means that it is easier for people in one State to cause harm in another State.

A third characteristic of Cyberspace that must be noted when we discuss Cyber peace is the low threshold for engagement in conflicts. While there are private defence organisations also in the physical world, it is generally difficult for private individuals and organisations to take part in military conflicts; at the minimum they need to be physically present where the conflict takes place, and they need expensive equipment to be effective. In Cyberspace, neither of these thresholds apply. An individual can engage in a conflict from anywhere in the world and with the help of a relatively cheap computer or even a smart phone. Furthermore, the private sector, such as the major Internet companies, plays a significant role in the Cyberspace domain. This means that there is a potentially large number of types of actors that

³ The "data layer" is not always included in the discussions of the layers, but I think it is important to address it separately.

must be taken into account when discussing Cyber peace. As is elaborated upon in the below, this may both be an asset and source of risks.

Fourth, Cyberspace, just like dynamite – the invention that, beyond others, built Alfred Nobel's wealth – is an excellent example of what has been termed dual-use technologies; that is, technologies that may serve both civilian and military purposes. Beyond Cyberspace itself, most of its components and aspects of the online world are also examples of dual-use technology. Cyberspace may be used for peace, and it may serve the aims of war. The same is true about cloud computing, blockchain, emails, social media, websites, and the like.

The fifth characteristic of Cyberspace that must be kept in mind when working towards Cyber peace is that cyberattacks typically involve significant preparatory work. While that does not distinguish cyberattacks from kinetic attacks per se, the difference is found in where the preparatory work takes place. While exceptions certainly can be found, most kinetic attack will be prepared from the attacker's territory. In contrast, preparations or cyberattacks involves work in the intended victim's system. While a State may have a right to express concerns about the buildup of hostile troops in a neighbouring State, until an attack takes place, the current role of laws is often limited. But already the preparatory work prior to a cyberattack may well be argued to violate international law and would certainly contravene domestic laws in most cases.

Turning to the sixth characteristic of note for Cyberspace, perhaps it might be said that, while website technology made us all potentially worldwide publishers, social media truly facilitated the opportunity to "go viral". But social media also did something else. The content we published on our websites would be found and consumed primarily based on its relevance in relation to the searches of other users. In contrast, when it comes to social media, it is well-known that content that sparks strong emotional responses typically gets a far wider reach and greater engagement. It is not a particularly big step to take to imagine that these peculiar dynamics have shaped online behaviour, and in this regard, the social media platforms – and the choices they have made in the algorithms they adopt – have a lot to answer for.

Finally, and this has perhaps already been alluded to in the above, Cyberspace is now entwined into just about every aspect of life. This sets it apart from other areas in relation to which there are international efforts to create regulation. Contrast, for example, the important ongoing work by the United Nations Committee on the Peaceful Uses of Outer Space. Would it even be possible to start imagining a United Nations Committee

on the Peaceful Uses of Cyberspace? I think not as such a committee would be tasked with discussing almost every aspect of human life outside war. Agreement between States seems an impossibility. On the other hand, perhaps such a committee is just what we need to avoid the "siloing" that currently undermines progress in Cyberspace governance?

3. CAN WE DEFINE REALISTIC CYBER PEACE?

Can Cyberspace ever be at peace? The answer to that question doubtlessly depends on how we define peace. It also depends on how we define Cyberspace. The discussion above should have provided some guidance as to how I here approach the concept of Cyberspace. However, it is necessary to also say a few words about how we may best understand the word "peace" in the Cyberspace context.

While not speaking specifically about Cyberspace, it is rather telling that the Swedish Prime Minister, in January 2025 observed: *"Sweden is not at war, but not at peace either"*.⁴ It may safely be assumed that Sweden is not the only State that perceives the current international climate this way. But a particularly interesting aspect of this statement is that it challenges the traditional binary distinction between war and peace. Are we now in a period where this longstanding binary distinction no longer reflects reality? After all, States rarely declare war these days, "cyberwar" is difficult to define,⁵ and intense competition and conflict now takes place much more frequently below the threshold for war, than it does above that threshold. All this complicates any attempt to define Cyber peace.

Nevertheless, there are, unsurprisingly, several definitions around, and it has, for example, been noted that:

"An early use of the word "peace" in the context of cyberspace and the Internet is a 2008 forward [sic] written by the former Costa Rican president and Nobel laureate, Óscar Arias Sánchez, for the International Telecommunications Union's (ITU) report on the ITU's role in cybersecurity. He referred to the need to promote "peace and safety in the virtual world" as "an ever more essential part of peace and safety in our everyday lives" and the urgency of creating a "global framework" to provide cybersecurity. He implied that this safe place within cyberspace can be implemented

⁴ The Brussels Times (2025) Sweden is 'not at war' but not at peace either, says PM Kristersson. [online] Available from: <https://www.brusselstimes.com/1389724/sweden-is-not-at-war-but-not-at-peace-either-according-to-pm-kristersson> [accessed 11 August 2025].

⁵ Téllez Carvajal, E. and González Hernández, J. (2022) Reflections on the Concept of Cyberwar and the Contributions of the International Community in the Peaceful Use of Cyberspace, *Opinión Jurídica*, 21(46) Special Edition, pp. 1-23.

through intergovernmental coordination around cybersecurity practices.”⁶ (Internal references omitted)

Some definitions are relatively brief, such as Roff observing that “Cyber peace is the end state of cybersecurity. Yet it is not a mere absence of attacks, rather it is a more robust notion about the very conditions for security.”⁷ Others are more elaborate such as the definition provided by Shackelford, Douzet, and Ankersen in the Introduction to their seminal edited volume on Cyber peace:

“a positive cyber peace is defined here as a polycentric system that (1) respects human rights and freedoms, (2) spreads Internet access along with cybersecurity best practices, (3) strengthens governance mechanisms by fostering multistakeholder collaboration, and (4) promotes stability and relatedly sustainable development.”⁸ (Footnotes omitted)

Commenting on these four pillars, Marlin-Bennett has referred to Diehl’s observation that “some positive peace concepts muddle the distinction between the definitional aspects of peace and the causal conditions needed to produce peaceful outcomes.”⁹ Drawing upon this, she concludes that “the four cyber peace pillars may fall prey to this lack of conceptual clarity and, perhaps, to a sort of tautology.”¹⁰

Furthermore, while most people no doubt would happily endorse the ambitions expressed in the definition offered to us by Shackelford, Douzet, and Ankersen, it may be argued that not all what they include is absolutely needed to achieve what we may call Cyber peace. For example, could we not have positive Cyber peace¹¹ – that is, Cyber peace that involves “relations that are just, sustainable, and conducive human flourishing in multiple ways”¹² – in the absence of “multistakeholder collaboration”? And if there was no further spread of Internet access beyond what we have today, would that mean that

⁶ Marlin-Bennett, R. (2022) Cyber Peace: Is that a Thing? In: Shackelford, S., Douzet, F., & Ankersen C. (eds) *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*. Cambridge: Cambridge University Press, pp. 3–21, at 5.

⁷ Roff, H. M. (2016) *Cyber Peace: Cybersecurity Through the Lens of Positive Peace*. [online] Available from: https://static.newamerica.org/attachments/12554-cyber-peace/FOR%20PRINTING-Cyber_Peace_Roff.2fbbb0b16b69482e8b6312937607ad66.pdf

⁸ Shackelford, S. Douzet, F., & Ankersen, C. (2022) Introduction. In: Shackelford, S., Douzet, F., & Ankersen C. (eds.) *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*. Cambridge: Cambridge University Press, pp.19 – 31, at 24.

⁹ Diehl, P. (2019). Peace: A Conceptual Survey. In: *Oxford Research Encyclopedia of International Studies*. Oxford University Press.

¹⁰ Marlin-Bennett, R. (2022) Cyber Peace: Is that a Thing? In: Shackelford, S., Douzet, F., & Ankersen C. (eds) *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*. Cambridge: Cambridge University Press, pp. 3–21, at 14.

¹¹ Contrast to “negative peace”, understood as the mere absence of violence in a relationship.

¹² Marlin-Bennett, R. (2022) Cyber Peace: Is that a Thing? In: Shackelford, S., Douzet, F., & Ankersen C. (eds) *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*. Cambridge: Cambridge University Press, pp. 3–21, at 13.

we can never reach Cyber peace? Perhaps I am misunderstanding their definition, but at the very least, it seems to me that we must acknowledge that these pillars are all matters of degree and that the definition might have benefited from expressly addressing how that impacts the definition.

At any rate, we may here pause to make two observations. First, it seems clear that Cyber peace is something more than the mere absence of Cyber war and cyberattacks. This is a point with which I fully agree. Second, definitions of Cyber peace have so far been heavily focused on cybersecurity. However, as I have hinted at above, Cyber conflict takes many forms such as cognitive warfare, information warfare, and espionage. This, I think, needs to be reflected in any definition of Cyber peace. Put differently, we will not reach Cyber peace merely by focusing on cybersecurity; also this obviously complicates the task of achieving Cyber peace.

In the end, it may well be the case that academics, and not least legal academics (myself included), are overly concerned with definitions. Perhaps we should not seek to specifically define Cyber peace? After all, when it comes to a concept like Cyber peace, a definition is only useful if it: (1) helps encourage and guide our actions in the pursuit of that we seek to define (here, Cyber peace), and at the same time (2) it does not limit, exclude, or discourage actions that may help the pursuit of that we seek to define (here, Cyber peace).

With that in mind, I certainly endorse the view that the term Cyber peace cannot, and should not, be defined precisely, and that we rather should use the term to orient the mind toward the right choices, and that consequently *“it must remain somewhat open-ended. The definition cannot be watertight, but must be rather intuitive, and incremental in its list of ingredients.”*¹³

Against this background, we may now turn to the three criteria that Nobel included in his will in relation to the Peace Prize. Guided by those three criteria we can examine what may be done in the pursuit of Cyber peace even in the absence of a strict definition of Cyber peace. First, however, a few observations may usefully be made in defence of the role that law may play in the pursuit of Cyber peace.

¹³ Wegener, H. (2011) A Concept of Cyber Peace. In: International Telecommunication Union, *The Quest for Cyber Peace*. Available from: https://www.itu.int/dms_pub/itu-s/opb/gen/s-gen-wfs.01-1-2011-pdf-e.pdf, pp. 77-85, at 78.

4. IN DEFENCE OF "CYBER LEGALISM"

I see law as playing a major role in achieving Cyber peace. Indeed, it may well be the case that I, in this article, expose myself to legitimate criticism of having overlooked a range of other important mechanisms. Others will be better placed to add any such mechanisms to complete the picture.

The view that the law is central to Cyber peace is widely, but not universally, shared. Some commentators have sought to point out the inadequacy of international law as a tool to address hostilities in Cyberspace. This is healthy. We must always be prepared to discuss and evaluate the value of the tools on which we rely.

Here, I will seek to defend the role of the law. It must be understood, however, that I am *not* necessarily defending the structure and application of *current* law. Indeed, the article should make clear that I see a strong and widespread need for legal reform, but I do maintain a conviction that law must play a significant part in creating Cyber peace.

A particularly interesting and engaging discussion may be found in Kello's recent book "Striking Back". There he goes to great lengths to demonstrate that "Cyber legalism" – the doctrine that stresses the importance of existing international institutions and legal frameworks – fails and that we therefore must focus on a harsher, more aggressive, strategic doctrine instead. He argues that "*Until and unless the legal system is equipped with instruments to limit technological acts of unpeace [his term], policymakers must find a solution to problems of cyber conflict prevention elsewhere - in the realm of strategies to deter aggression by rational means*".¹⁴

In more detail, he advocates what he calls "punctured deterrence" which the reader late in his book finds out is retaliation carried out as a single action wherever and whenever best fits the victim's interest and capacities, in a manner of the victim's choosing, and that may be in response to a series of actions for their cumulative effect.¹⁵ We may, of course, question how many States in the world have the option to effectively adopt this punctured deterrence. Would, for example, Estonia in 2007 been able to, and well served by, adopting this doctrine in response to the Russian cyberattacks? Personally, I doubt it. Kello acknowledges the problem but unless his aim is simply to support the spreading "might makes right" doctrine, he could have done much more to explore alternatives for the vast majority of States that are not well positioned to rely on striking back as their response to cyber incidents.

¹⁴ Kello, L. (2022) *Striking Back: The End of Peace in Cyberspace – and How to Restore it*, New Haven: Yale University Press, p. 61.

¹⁵ Kello, L. (2022) *op. cit.*, pp. 143-144, p. 148.

At any rate, the main thrust of Kello's attack on "Cyber legalism" is built on two significant misunderstandings. First, he is, of course, correct to point out the aspects of legalism that do not work well, and doing so is important. But it is entirely misguided to see this as a question of either Cyber legalism or strategic doctrine. As they are not mutually exclusive, we must work via both as both may serve the goal of Cyber defence and ultimately Cyber peace.

The second main misunderstanding underpinning his attack on Cyber legalism relates to the war-peace distinction and has two parts. One frequently sees claims such as Kello's claim that "*cyber conflict often occurs along a spectrum between the poles of war and peace.*"¹⁶ At the same time, Kello complains that the "*existing legal framework reinforces the traditional war-peace binary that underpins Western strategic doctrine.*"¹⁷ This latter point is indeed a major issue, and – as discussed – we can probably all agree that the line between war and peace is not as clear in practice as it may be portrayed in theory. But the two claims Kello make are irreconcilable and thus, to the extent that this is meant to be a criticism of law, it lacks sting. If the existing legal framework is binary, there clearly cannot be any "spectrum between the poles of war and peace".

The second part of this misunderstanding relates to its focus. Any talk of hybrid war, grey zone war, or indeed a spectrum between the poles of war and peace leads the mind astray. What we do have, and what really is the concern, is hostile activities that are perceived as severe, perhaps even "war-like", but that nevertheless fall beneath the relevant key thresholds; in particular the Article 51 threshold for an "armed attack" found in the UN Charter.¹⁸ As hostile actors deliberately structure their attacks (and campaigns) so as to fit below the Article 51 threshold, they successfully cause damage without running the risk of a significant lawful response from the victim State. This must be seen as a flaw in the current legal structure and should be remedied.

Thus, the cure to this unfortunate, but from a historical perspective understandable, situation is found in: (a) international instruments acknowledging some right to respond also for attacks beneath the Article 51 threshold, or (b) State practice to evolve showing that States see such

¹⁶ Kello, L. (2022) *op. cit.*, p. 45.

¹⁷ *ibid.*

¹⁸ For a detailed discussion see e.g.: Haataja, S. (2019) *Cyber Attacks and International Law on the Use of Force The Turn to Information Ethics*, [online], CCDCOE, Available from: <https://cyberlaw.ccdcoe.org/wiki/Self-defence> [accessed 11 August 2025] and Pangrazzi S. (2021), *Self-Defence against Cyberattacks? Digital and Kinetic Defence*. In: ICT for Peace Foundation. *Self-Defence Against Cyberattacks?*, Geneva. Available from: <https://ict4peace.org/wp-content/uploads/2021/03/ICT4Peace-2021-Cyberattacks-and-Article51-1.pdf> [accessed 11 August 2025].

additional right as existing. The latter is, of course, a more uncertain and dangerous path.

It is easy to relate to the frustration Kello expresses in relation to international law, the disdain and hypocrisy with which it is treated by a growing number of States, and the weakness, or indeed lack, of its enforcement. However, international law plays several roles, and I wish to conclude this section defending international law by outlining what those roles are.

Combining the works of Hart¹⁹, Koskenniemi²⁰ and Svantesson²¹ one can argue that international law fulfills at least four different roles. International law is (1) a tool to decide legal disputes; (2) a tool to provide a framework to control, to guide, and to plan life out of court; (3) a tool to express and communicate the values of those who created the law; and (4) a tool – a surface or a playing board – on which political adversaries recognise each other as such and pursue their adversity in terms of something shared. Acknowledging these quite diverse roles of international law, it is difficult to maintain the argument that Cyber legalism's current inadequacies are fatal to law as a tool for Cyber peace, and at least to me, it seems clear beyond intelligent dispute that law must continue to play a role in the pursuit of Cyber peace.

5. THE FIRST CRITERIA: ADVANCE FELLOWSHIP AMONG NATIONS

If we are to understand how the first of Nobel's criteria applies in the context of Cyber peace, it is important to first recognise that the standard translation focused on advancing "fellowship among nations" amounts to a simplification of the Swedish original. The phrase used by Nobel in the Swedish original text of the will is "*folkens förbrödrande*". While it is not incorrect to translate the word "*folkens*" by referring to nations, "*folkens*" also means "the peoples". Thus, it is certainly proper to view Nobel's aim to be fellowship among people also within a domestic context, not merely on the level of the relationship between nations.

This fuller picture allows matters such as civil cyber war, and the suppression of online human rights within a State by the government of that State, to fall within the scope of what we here discuss as Cyber peace. Indeed, it may be argued that the conventional translation focusing on fellowship

¹⁹ Hart, H.L.A. (2012) *The Concept of Law*, 3rd ed. Oxford: Oxford University Press.

²⁰ Koskenniemi, M. (2011) *The Politics of International Law*, Hart Publishing.

²¹ Svantesson, D. (2015) A Jurisprudential Justification for Extraterritoriality in (Private) International Law. *Santa Clara Journal of International Law*, 13, p. 517.

among *nations* does not fully capture this and that a better translation would be "advancing fellowship among peoples" or "advancing fellowship among, and within, nations".²²

Importantly, the understanding of Nobel's first criteria advanced here is also a better fit with how the Committee awarding the Peace Prize actually has acted over the years. After all, on many occasions, the Nobel Peace Prize has been awarded to persons or organisations engaged in important conflicts-related human rights work rather than more directly in peace efforts specifically. Indeed, former chair of the Norwegian Nobel Committee, Berit Reiss-Andersen, has noted that "*The fraternity [fellowship] criteria covers, among others, human rights contributions to peace.*"²³ Against this background, it may be the case that those who have expressed criticism against the Peace Prize being awarded for important conflicts-related human rights work simply have read the text of the will too narrowly.

When discussing the criteria of advancing fellowship among (and within) nations, the first thing to note is that Cyberspace itself is a tool with a remarkable potential to do just that; advance fellowship among (and within) nations. As is commonly noted, Cyberspace has an unprecedented ability to connect people across national borders, and at least if we hold a generally optimistic view of humanity, it seems reasonable to expect that such increased connectivity between peoples ought to advance fellowship among (and within) nations.²⁴ However, we have reason to pause to consider whether this so far has brought us closer to, or further from, peace.

First of all, we may ask whether the world today is characterised by a higher degree of fellowship among nations than was the case in the pre-Cyberspace world. Exact criteria for such an assessment may be lacking, but it seems fair to say that there is a widespread and credible view that we are now considerably closer to World War III than we were in the early 90's when Cyberspace started to become an important aspect of society. Additionally, it may be argued that there is a higher degree of tension also

²² Critics of such a more expansive translation may argue that the peace movement at the time of Nobel's will was centered on nations. At the same time, however, it could be argued that there must have been a reason why Nobel chose the term "folkens" instead of alternatives explicitly limited to "nations".

²³ The Nobel Prize. (2025) *Behind the scenes of the Nobel Peace Prize*. [online] Available from: <https://www.nobelprize.org/behind-the-scenes-of-the-nobel-peace-prize/> [accessed 11 August 2025].

²⁴ Admittedly, it is also possible to take the opposite view and assume that increased contact between people automatically lead to a greater increase in friction and conflict rather than to advance fellowship among them. Much could be said about this, but the end conclusion of such a view is presumably that we are all better off not having any contact at all with each other and that we should make haste to dismantle the Internet and any other tools for communication. If so, this article is probably pointless.

among States that (at least currently) are unlikely to go to war against each other. Finally, one may point to the "Doomsday Clock" provided by the Bulletin of the Atomic Scientists' Science and Security Board as an indication of how close humanity is to self-annihilation. In the latest update (January 2025) it points to 89 seconds to midnight. The international situation as deteriorated considerably since then and yet that was the closest it has ever been to "midnight". In 1990, it was 10 minutes to midnight.

I hasten to acknowledge that the rather sad state in which we find international relations today is not only a result of our increasing dependence on Cyberspace. Thus, no definitive conclusions should be drawn. Yet, there are things we may point to – such as the propensity by some to use short messages on social media as an alternative to more classical diplomacy – that reasonably seem to be contributing to a deteriorating international relations landscape. Consequently, the reality of the world situation we face today does call into question any assertion that Cyberspace so far has advanced fellowship among nations.

Additionally, if we turn our attention to fellowship *within* nations as the discussion above suggested we ought to do as well, we can arguably also see how Cyberspace has led to a deterioration in "fellowship". In this respect, Cyberspace – and in particular social media – has had a devastating impact. Many societies are now more divided than ever before and the "filter bubbles" that ensure that our online exposure is restricted to content that tends to confirm our existing views have been a driving force in this. Work towards social cohesion is crucial, and social media must play a more responsible role in the fight against harmful social division.

If we were to try to summarise the above, perhaps it may be said that the ability of Cyberspace to create connections among nations (and their peoples), has not yet resulted in the desirable fellowship among nations (and their peoples) that it has the potential to create. This should, however, not be seen as any criticism against Cyberspace. Cyberspace, as such, is neutral – it can be used for good, and it can be used for bad. Rather, the failure here lies in the governance of Cyberspace.

It was entirely predictable that Cyberspace would reflect human behaviour generally. As e.g., there are child abuse materials in the physical world, there was always going to be child abuse materials in Cyberspace. And as States seek to compete with each other in the physical world, they were bound to do so also online. We have not dealt with this well, and it may be said that law/regulation/governance has so far failed Cyberspace. Recognising the harm caused by certain uses of Cyberspace (e.g the content filter bubbles in social media), it is not enough to curse the private companies

that operate social media. The law must respond and set clear boundaries. Importantly, law has failed the promise offered by Cyberspace both by being overly intrusive and creating an environment of complex partly overlapping laws, and by being too passive not sufficiently addressing harmful content and practices online.

In all this, it must be remembered that Cyberspace is neither the problem, nor is it the cause of the problem. Rather, unless it is adequately protected, Cyberspace risks becoming the victim of how it is used and regulated. The question is then what we can do to shape the Cyberspace environment in a manner that helps it achieve its potential to advance fellowship among (and within) nations. The answer to such a question is clearly that there is much to be done; there are many issues that could be considered under the label of advancing fellowship among (and within) nations in the pursuit of Cyber peace. Here, however, I will limit myself to focusing on three illustrative examples of the types of issues we should consider in this context, namely: Internet openness and inclusiveness, delineation of jurisdiction, and the role of sovereignty. And given the space limitations associated with a journal article, I merely seek to showcase how addressing these issues may take us some steps towards Cyber peace.

5.1. INTERNET OPENNESS AND INCLUSIVENESS

While, as was acknowledged above, Cyberspace has not yet lived up to its potential to advance fellowship among (and within) nations, we should not give up. Cyberspace pioneers have given the world a wonderful tool. Now it is time for the legal community to "tame" it and make it serve humanity and peace via openness and inclusiveness.

I realise, of course, that my statement above may be highly offensive to those who still adhere to the mindset held by the early Cyber-libertarians. However, it is no longer – if it ever was – realistic to call for Cyberspace to be unaffected by law. That position, although recycled to a degree by the blockchain community, was conclusively defeated by reality and we need not revisit that debate here. It is sufficient to note that even with the role that the law has played so far, Cyberspace is not delivering on its potential to create fellowship among (and within) nations, and that we would be in an even worse position if we had adopted the Cyber-libertarian ideals; after all, we need e.g., international humanitarian law and human rights law as much online as we do offline.

An open and inclusive Cyberspace helps connect the world with the potential to foster cross-border trade, exchange of ideas, and scientific discoveries, as well as a sense of world community. We need legal structures

that support diversity and freedoms, that nevertheless facilitate societal cohesion instead of constantly amplifies divisions. All this can clearly favour peace both in a general sense and Cyber peace specifically.

5.2. DELINEATION OF JURISDICTION

To ensure that States can coexist in a peaceful manner, we need predictable and accepted rules for the allocation of each State's rights and duties; both to each other on a bilateral or e.g., regional level, and as members of a global community. We must reverse the emerging trend in which foreign laws are treated as merely a form of "trade barriers". That trend is harmful on multiple levels and shows a decreasing respect for the rule of law, and for each other among nations – the opposite of Nobel's first mentioned criteria for the Peace Prize.

In this context, jurisdiction is, and will remain, a key concept and an important tool both under public - and private international law. Put simply, we need rules for delineating legal authority and we get that in the form of jurisdictional rules. Indeed, if we examine how the regulation of Cyberspace has worked to-date, we find that, while there are some areas of harmonisation and coordination (such as in relation to the domain name system), the main tool is our rules regarding jurisdiction and applicable law; done well, they are tools to avoid conflict and promote peace, even though they – particularly from a private international law perspective – too rarely are discussed as tools for peace.

A key issue when it comes to applying jurisdictional rules in Cyberspace is that they are traditionally viewed as anchored in territoriality – not least when it comes to public international law – and it is widely acknowledged that territoriality is a poor fit for the online environment. Anchoring jurisdictional rules in territoriality is inappropriate and often requires arbitrary decisions about "where" various events take place; decisions that may spark unnecessary tensions. Thus, it frequently generates poor and unfair outcomes, and in a range of cases, territoriality simply cannot provide the answers needed; after all, if you are regulating processes occurring in a virtual world, location is always going to be no more than a manipulable legal fiction. These are sufficiently serious flaws to justify a search for better alternatives,²⁵ and by not relying on the ill-fitted concept of territoriality, we can devise jurisdictional rules that cause less international friction. This serves the goal of advancing fellowship among nations and ultimately the goal of Cyber peace.

²⁵ See e.g.: Svantesson, D. (2015) A New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft, *American Journal of International Law Unbound*, 109, pp. 69-74.

5.3. THE ROLE OF SOVEREIGNTY

Sovereignty is a crucial concept for how States coexist,²⁶ and leading commentators have noted that sovereignty is one of the most politically loaded terms in the discussions of State behaviour in Cyberspace.²⁷ Indeed, it could be said that our ability to address some of the most pressing challenges facing humanity – such as the diverse areas of international conflict, the disinformation-driven decline in trust in society, human rights abuses, and threats to the environment – depends, in no small part, on how well we can work with sovereignty.

Perhaps due to its centrality in international law, the concept of "sovereignty" has spawned a large number of "newer" concepts, such as "digital sovereignty", "data sovereignty", and "information sovereignty", with dubious connection to the concept of sovereignty found in international law. In my view, these newer concepts are nothing but "a shoal of red herrings" detracting from the underlying reality that (a) the international law concept of sovereignty applies in Cyberspace, and (b) we need to find a way to make that concept work appropriately in Cyberspace.

Additionally, it seems that the increased use of the term "sovereignty" is resulting in an ever-lower level of shared understanding of what sovereignty is and what function(s) sovereignty fulfills. Such a lowering in the degree of shared understanding may be a conscious strategy by some States, but it is harmful and must be resisted. Nevertheless, it is also the case that the current mainstream thinking on sovereignty is ill-equipped for the modern world; not least in the Cyberspace environment.

To this may be added that sovereignty now is under threat on a level not seen since the end of World War II. At the January 2025 edition of the annual "Folk och Försvar"²⁸ conference in Sweden, esteemed Russia expert – Dr. Gudrun Persson of the Swedish Defence Research Agency – observed that:

*"The Russian view of the world order is largely based on a particular view of sovereignty and the multipolar world. According to this view, only a great power can be sovereign and decide for itself. Small states cannot do that. They are vassals or satellites to the great power and must bow [to the great powers]. According to this view, the world order must be based on a number of poles; Russia, USA, China, Brazil, India and so on. And now Putin is making great power claims."*²⁹

²⁶ See e.g.: *Ibid.*

²⁷ Osula, A. M. Kasper, A. and Kajander, A. (2022) EU Common Position on International Law and Cyberspace. *Masaryk University Journal of Law and Technology*, 16 (1), p. 95.

²⁸ Translates roughly as "Society and defence".

²⁹ Original Swedish: "Den ryska bilden av världsordningen bygger i hög grad på en särskild syn på suveränitet och den multipolära världen. Bara en stormakt kan enligt denna syn vara suverän och

Recently, the Trump administration has made a range of statements e.g., relating to Greenland, Panama, Gaza, and Ukraine, indicating that also the US – under the current regime – shares these troubling attitudes towards sovereignty. To this may be added China's longstanding aggressive attempts to impose dominance in the South China Sea, in the Pacific, and elsewhere, as well as its constant threat to occupy democratic Taiwan by force.

Our thinking on sovereignty must show awareness of this type of attitudes and the threat to peace to which they amount. Indeed, I argue that, in order to remain a valuable tool to serve the aim of peace, our work on defining sovereignty must seek to actively counter these attitudes – it must aim to equip the concept of sovereignty to serve as a shield against these attitudes. Doing so is not a case of so-called "lawfare", it is about fair laws. We must advocate the best version – or understanding – of sovereignty possible, not content ourselves with repeating (partially) obsolete mantras articulated over the past 100 years or so in a handful of cases. This represents an opportunity to also explore a conception of sovereignty that is not anchored in territoriality and thus would be more easily applied in the Cyberspace environment; all in the pursuit of Cyber peace.

6. THE SECOND CRITERIA: ABOLITION OR REDUCTION OF STANDING ARMIES

The idea of the abolition or reduction of standing armies may look different in Cyberspace compared to how it looks offline, and leading commentators such as Tzagourias and Biggio have pointed to the difficulties associated with discussing cyber-disarmament.³⁰

There are presently comparatively little by way of standing armies, in a traditional sense, in the Cyberspace environment, although Cyberspace forces are rapidly increasing in size. The dynamics of Cyberspace are such that a State does not require a large standing army to constitute a serious threat to other States. However, States do require a large standing army of cybersecurity expertise to minimise and mitigate the threats, including those posed by other States in Cyberspace. Such capabilities almost always overlap with civilian – private sector – cybersecurity capabilities, and it is not always

bestämma själv. Små Stater kan inte det. Dom är vasaller eller satelliter till stormakten och ska böja sig. Världsordningen ska enligt denna syn bygga på ett antal poler; Ryssland, USA, Kina, Brasilien, Indien och så vidare. Och nu gör Putin stormaktsanspråk." See Persson, G. (2025) "Vi vet vad Ryssland vill" - Gudrun Persson, docent Försvarsmakten [online video] Available from: https://youtu.be/H5RdtHiCE1o?si=_pLb7rOZ-zvWSol1 [accessed 11 August 2025].

³⁰ Tzagourias, N. and Biggio, G. (2021) Cyber-peacekeeping and international law. In: Tzagourias, N. and Buchan, R. (eds.) *Research handbook on international law and cyberspace*, 2nd ed., Northampton, Massachusetts. Edward Elgar Publishing, pp. 345-365.

possible, or meaningful, to distinguish between civilian and military when it comes to cybersecurity and cyber defence.

In the light of the above, as far as Cyberspace is concerned, the second criteria on which Nobel placed emphasis – the abolition or reduction of standing armies – should in my view be understood to be predominantly, if not exclusively, focused on offensive capabilities; indeed, offensive capabilities whether in the form of standing armies, or otherwise. Such offensive capabilities may be a concern also if produced on an *ad hoc* basis as frequently is the case where certain authoritarian States utilise non-State actors such as Cyber criminal groups.

There are several distinct aspects of the Cyberspace domain that could be highlighted when we discuss the criteria of abolition or reduction of standing armies. Below I briefly discuss three examples of such aspects, namely (1) recalibrating the positions of attackers and defenders, (2) abandoning the hidden use of non-State actors, and (3) Cyberspace as an alternative to the use of kinetic weapons. All three of those topics warrant extensive discussions and I am here constrained to merely introduce them superficially as illustrations without making any attempt to link into the literature engaging with the more intricate issues within each topic.

6.1. RECALIBRATING THE POSITIONS OF ATTACKERS AND DEFENDERS

Arguably the best way to apply the criteria of the abolition or reduction of standing armies to Cyberspace is to see it as a call to recalibrate the balance between attackers and defenders. We need to facilitate an environment capable of abolition or reducing the "attacker advantage" that currently is prevalent in the Cyberspace domain.

In the AI arms race, for example, we see a clear illustration of one aspect of the "attacker advantage". It is true that AI can be used in support of both offensive and defensive cyber measures. However, for an aggressor, AI technology can be seen as a success if it proves effective at least some of the times it is being used. In contrast, for a defender using AI technology, that technology must prove effective in nearly all cases to be of value. Imagine, for example, that a State is using AI technology both in its offensive capabilities and in its defensive capabilities. Imagine further that the technology in each task is effective at a rate of 50%. In such an instance, an evaluation would presumably conclude that the AI technology is highly effective in its offensive application, but ineffective to the degree of being useless in the defensive role.

The dynamics created by the "attacker advantage" may lead to a vicious circle where States view increased offensive capabilities as the

only meaningful response due to the inefficiency of defensive capabilities. Breaking such a chain of events is crucial for the abolition or reduction of standing armies in Cyberspace.

A central challenge for the defenders in Cyberspace is found in the lack of available personnel. This is often discussed in relation to cybersecurity experts, but it is an issue more broadly also impacting e.g., information conflicts. One obvious way to address this issue and help rebalance the comparative situation between attackers and defenders is found in education. We need more high-level cybersecurity experts, but we also need to work to increase the base-level cybersecurity knowledge in the public. This increase in capability will serve cyber defence, the fight against cyber crime, and ultimately Cyber peace.

In addition, we need to develop defender "surge capacity" via Cyber reserve forces and structures for promoting and harnessing volunteer capabilities. Admittedly, it may seem counterintuitive to call for an increase of the number of people engaged in Cyber defence as part of a move to abolish or reduce standing armies. However, such a view misses the point made above distinguishing between offensive and defensive capabilities. Cyberspace is a whole-of-society resource, and it requires a whole-of-society defence. Increasing society's capabilities to defend a vital resource such as the Cyberspace environment can, thus, not be contrary to Nobel's goal of the abolition or reduction of standing armies.

A related way to support defenders over attackers in the Cyberspace environment would involve refining the "principle of distinction"; that is, the principle requiring that parties to an armed conflict at all times distinguish between civilians and combatants and between civilian objects and military objectives.³¹ While the principle of distinction remains of central importance for guiding the behaviour of those engaging in cyberattacks, when attacks on a State's Cyberspace environment, as noted, is a whole-of-society matter, it is hard to see how the cyber defence could be anything but a whole-of-society matter. Thus, calls to keep civilians out of the cyber defence are unrealistic and yet such civilians need to be appropriately protected. In a sense, what I am proposing involves using a reformed version of the principle of distinction to give the defender an advantage by essentially limiting the principle's application to attackers only. Similar steps could be taken in relation to some other legal principles regulating conflicts.

³¹ ICRC. (2023) *The Principle of Distinction*. [online] Available from: https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/03_distinction-0.pdf [Accessed 11 August 2025].

Another key step towards countering the attacker's advantage in Cyberspace could be taken if we can improve the attribution of cyberattacks and other hostilities, including mis- and dis-information campaigns. Current attribution challenges strongly favour the attacker, and they provide plausible deniability. Attribution is often technically difficult but that should only be seen as a sign that we need to put even more resources into developing better attribution techniques.³²

Finally, scholars such as Housen-Couriel have pointed to the role that information sharing can play in addressing the "attacker advantage": *"Typical informational asymmetries that have characterized cyber hostilities to the advantage of the attacker are addressed by the sharing of data."*³³ Also this may help rebalancing the positions of attackers and defenders in a manner favourable to Cyber peace, and such information sharing is not only useful in the context of cybersecurity, but obviously information sharing is at least equally important when it comes to information conflicts. Indeed, sharing of information e.g., relating to ongoing threats, may be crucial in the fight against mis- and dis-information.

In this context, we may also point to the importance of solidarity with the States that currently are less advanced in their use, and regulation, of the online environment. Information sharing with such States is important and should be supplemented by training and the sharing of practises. But it cannot just be a focus on "best practises" from the point of view of the more advanced States as too often is the case. The "best practises" from the advanced States must be adjusted to the specific context of the developing States and made to be useful in their specific environment; this is an important point often missed in various "bench-marking" studies.

6.2. ABANDONING THE HIDDEN USE OF NON-STATE ACTORS

Perhaps the greatest risk of unwanted escalation through Cyberspace activities stems from the fact that several States actively "outsource" a range of questionable, or directly illegal, activities to non-State actors. The reason States do this is obvious; it gives them plausible deniability. However, the risks are great as these non-State actors may not be as tightly controlled as regular Cyberspace forces, and may of course, have agendas of their own.

As argued above, cyber volunteers may be a useful addition for cyber defences, but peace and security in Cyberspace would be enhanced greatly

³² *Ibid.*

³³ Housen-Couriel, D. (2022) Information Sharing as a Critical Best Practice for the Sustainability of Cyber Peace. In: Shackelford, S., Douzet, F., & Ankersen C. (eds.) *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*. Cambridge: Cambridge University Press, pp. 39–63, at 53.

if we could prevent the use of such actors in offensive activities online, and, perhaps even more importantly, if we could ensure transparency in their use. In other words, States should agree to abandon the hidden use of non-State actors.

6.3. CYBERSPACE AS AN ALTERNATIVE TO KINETIC WEAPONS

While the risk of Cyberspace activities leading to conflict-escalation are commonly emphasised, several leading experts have also noted that Cyberspace activities may be used to de-escalate conflicts; the Cyberspace domain may be used as a much-needed off-ramp in serious conflict situations. In the words of Valeriano and Jensen: “*Cyber operations are not clear paths to peace, but in the context of more dramatic options digital technologies can lead us down a road away from war.*”³⁴ In this context, a commonly used example is found in the well-known Stuxnet operation attributed to Israel and the US resulting in a serious disruption of Iran’s ability to develop nuclear weapons.³⁵ The planting of the code that caused the harm may obviously be seen as a form of cyberattack – an aggression. Yet, it is easy to see that any kinetic alternative – such as an air strike, or less likely, a special forces raid, not to mention a full-scale military invasion – would have (a) caused collateral damage not caused via the cyberattack, and (b) involved a considerably higher risk of escalation.

With examples like this in mind, it seems clear that we ought to consider in more detail the circumstances under which we may be willing to sacrifice some Cyber peace in order to maintain peace in the offline world. Doing so clearly has the potential to support Nobel’s goal of abolishing, or at least reducing, standing armies as a whole. Indeed, if all international competition and conflict was limited to expressions in Cyberspace, there would be almost no need at all for standing armies in a traditional sense.

³⁴ Valeriano, B. and Jensen, B. (2022) De-escalation Pathways and Disruptive Technology. In: Shackelford, S., Douzet, F., & Ankersen C. (eds.) *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*. Cambridge: Cambridge University Press, 64–93, at 66.

³⁵ See e.g.: *Ibid.* and Marlin-Bennett, R. (2022) Cyber Peace: Is that a Thing? In: Shackelford, S., Douzet, F., & Ankersen C. (eds.) *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*. Cambridge: Cambridge University Press, pp. 3–21.

7. THE THIRD CRITERIA: ESTABLISHMENT AND PROMOTION OF PEACE CONGRESSES

Peace congresses of the kind that were common around the time when Nobel finalised his will at the end of the 1800s are no longer taking place. Thus, not least in the Cyberspace context, it may be worthwhile to read the criteria of establishing and promoting peace congresses broadly. And when doing so, there are numerous examples of attempts to coordinate and promote global peace efforts that may be noted. For example, to mention a few arbitrary examples we may note:

- The Paris Call for Trust and Security in Cyberspace;
- The various UN Groups of Governmental Experts (UNGA Res. 73/266 (Dec. 5, 2018)) and Open-Ended Working Groups (UNGA Res. 73/27 (Dec. 22, 2018));
- The Global Commission on the Stability of Cyberspace (GCSC), including its Norms of Responsible Behaviour in Cyberspace and Call to Protect the Public Core of the Internet;
- The Erice Declaration on Principles for Cyber Stability and Cyber Peace;
- The International Telecommunication Union's five principles for cyber peace; and
- The EU Institute for Security Studies' Advancing the Cyber Programme of Action (PoA).

All these initiatives are commendable, and there are of course others. In addition, there is also a wide range of more general attempts to coordinate Internet governance that have a more indirect, or indeed implicit, peace focus:

- Internet Governance Forum;
- The NETMundial Multistakeholder Statement;
- The Hague Charter for Accountability in the Digital Age;
- Internet & Jurisdiction Policy Network; and
- The UN's High-Level Panel on Digital Cooperation.

It is not my ambition here to discuss any of these initiatives. They were selected as illustrations only, and others have already discussed them in detail. For example, Douzet, Géry and Delerue expertly describe the history of several important developments with a particular emphasis on the complicated Cyber peace building dynamics within the various processes that have taken place within the United Nations' structures. Published

in 2022, they note that: *“the renewed strategic competition and exacerbated geopolitical tensions have led states to engage not only in a cyber arms race, but also in a competition for normative influence.”*³⁶ That was no doubt a correct assessment at that time. But the world has already changed considerably since then. Arguably the new environment in which we are now may lead to one of two outcomes. The first – and perhaps most likely – option is that the continued hardening of the strategic competition and exacerbated geopolitical tensions will lead to an even more intense cyber arms race and competition for normative influence. The second alternative is that the US continues to withdraw from the international community. That second option may well include increased, or at least a continued, cyber arms race but result in less competition for normative influence as there may no longer be any shared norms at all. Much is uncertain at the time of writing, and it is easy to agree with the claim that *“The road to cyber peace is paved with malicious intentions.”*³⁷

7.1. ESTABLISHING A REALISTIC CYBER PEACE AGENDA

Guided by the criteria of establishing and promoting peace congresses, I have called for what we may refer to as a “Realistic Cyber Peace Agenda” that brings together many of the points raised above throughout the article.³⁸ Part of the idea was that, at least when it comes to Cyber peace, we need specific, practical, and realistic actions more than we need lofty proclamations. In other words, drawing upon the observations about possible actions in the pursuit of Cyber peace that we have been able to tease out above via the three criteria included in Nobel’s will, we may start to form a sort of action plan for Cyber peace. While more work is needed to identify suitable agenda items, in the light of the above, some potential action items for such a Cyber Peace Agenda could, for example, include:

- Reforming the rules regarding jurisdiction;
- Reforming the rules regarding sovereignty;
- Improved tools for attribution; and
- Ban on the hidden use of non-State actors in Cyberspace.

³⁶ Douzet, F. Géry, A. and Delerue, F. (2022) Building Cyber Peace While Preparing for Cyber War. In: Shackelford, S. Douzet, F. & Ankersen C. (eds.) *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*. Cambridge: Cambridge University Press, pp. 170–193, at 191.

³⁷ Douzet, F. Géry, A. and Delerue, F. (2022) *Op. cit.* p. 171.

³⁸ The idea was first presented at a talk titled *Give (Realistic) Cyber Peace a Chance* held on 30 April 2025 at the Nobel Peace Center in Oslo, Norway. See Svantesson, D. (2025) Give (Realistic) Cyber Peace a Chance. In: Nobel Peace Center. [online] Available from: <https://www.nobelpeacecenter.org/en/events/give-realistic-cyber-peace-a-chance> [accessed 11 August 2025].

Already this short list of examples is ambitious. Yet it is obviously illustrative rather than exhaustive. My aim has been to point to *some* potential actions that would address some of the more obvious obstacles to Cyber peace highlighted above. There is clearly a range of other actions – such as clearer rules regarding cyberespionage, and a ban on attacks on undersea communications cables – that have not been discussed above but that could be added to this "Realistic Cyber Peace Agenda". Consequently, this must be treated as a "living document" and I invite suggestions of proposed actions to add.

Obviously, there are also many practical issues to be worked out. For example, it must be acknowledged that different persons will have different views of what is sufficiently "peace-related" and what is sufficiently "cyber-related" to be included on a Cyber Peace Agenda. Such matters must be discussed in the context of the Agenda as it may be unhelpful for the Agenda to become unnecessarily broad.

At any rate, it must be understood that each Agenda Item stands "on its own legs"; that is, while some connections may be found, they are all generally intended to be pursued as individual goals, not as a package. Thus, there is no need to seek agreement on a large number of Agenda Items at once. Rather, the path towards Cyber peace is made up of a number of independent Agenda Items each of which will take us closer to Cyber peace if achieved.

Moving forward with the Cyber Peace Agenda in a credible manner requires a leading peace-promoting institution with a strong international reputation becoming its custodian, and the Norwegian Nobel Institute has assumed this role. The Cyber Peace Agenda will be published in 2026. This is a major and crucial step. However, much work is needed before a credible Cyber Peace Agenda can be presented and diverse input is needed and will be sought as part of the work on the Agenda.

Apart from its potential to be agenda-setting by mapping out tangible steps that may be taken towards Cyber peace, and to raise the profile of Cyber peace work generally, the Cyber Peace Agenda will be a nice way to showcase the enduring relevance of Alfred Nobel's peace initiative, and to place that peace initiative in the Cyberspace environment that now is so central to humanity.

8. CONCLUDING REMARKS

This article has focused on the topic of Cyber peace. To set the scene, it highlighted certain aspect of Cyberspace that must be considered in this context. Furthermore, it discussed the extent to which defining Cyber peace is a fruitful exercise and concluded against doing so. It also addressed some criticism directed as the role that law may play in the Cyberspace domain. The discussion then turned to focus on the application of Nobel's three criteria for the world-famous, and much coveted, Peace Prize. Drawing upon a range of admittedly arbitrary examples, it was argued that a focus on Nobel's three criteria allows us to identify action items that may usefully be pursued with the aim of reaching Cyber peace.

This is important because peace cannot be taken for granted. Rather, we need to actively work for peace, and it is in uncertain times, such as those we are in now, that we must devote even more of our attention towards peace. This applies at least as much online as it does offline. On that note, we may pause to question whether it makes sense to work for Cyber peace specifically or whether it is better to just view such work as an aspect of peace work in general; after all, the text above has more than once highlighted the degree to which Cyber is entwined in the "real" world.

I argue that it, at least currently, is useful to focus specifically on Cyber peace. Doing so can bring attention to the work that needs to get done and may help raise the profile of peace work aimed at Cyberspace. So, for now, it remains relevant to speak of "cyberattacks", "cyberwar", "cyber peacekeeping",³⁹ and "Cyber peace" despite the fact that no sharp lines can be drawn between what is Cyber and what is not.

Cyber peace has only gained limited academic attention, and while there are plenty of civil society groups in the field of Cyberspace, only a comparatively small number of them have been engaging in explicit Cyber peace work. Perhaps this is linked, in some way, to the fact that there also does not seem to be much of a grassroots movement in favour of Cyber peace. Perhaps the general public perceives the Cyber risks as too technical and too abstract for such a movement to arise? The Cyber Peace Agenda under the custodianship of the Norwegian Nobel Institute can serve as a much-needed tool to raise the profile of Cyber peace.

Alfred Nobel's approach to peace was obviously coloured by the peace discussions of his time. Looking beyond his will, Nobel appears to have seen great potential in deterrence. Indeed, the Swedish historian Tägil notes that: *"In 1891, he commented on his dynamite factories by saying to the countess*

³⁹ Kleffner, J. and Harrison Dinniss, H. (2013) Keeping the Cyber Peace: International Legal Aspects of Cyber Activities in Peace Operations. *International Law Studies*, 89, p. 512.

[Bertha von Suttner]: “Perhaps my factories will put an end to war sooner than your congresses, on the day that two army corps can mutually annihilate each other in a second, all civilised nations will surely recoil with horror and disband their troops.”⁴⁰ To this Tägil adds that “Nobel did not live long enough to experience the First World War and to see how wrong his conception was.” But perhaps Nobel was not wrong at all. After all, he referred to “all civilised nations”. Perhaps it is just the case that nations are not yet sufficiently “civilised”? And we may wonder whether they ever will be. With that doubt in mind, deterrence may have its limitations.

Today, Nobel might have expressed his criteria slightly differently. However, it seems to me that we can continue to draw inspiration, and indeed guidance, from the three criteria articulated in his will, signed by him in its final form 130 years ago, and referred to extensively above. Indeed, I would argue that the discussion above highlights the enduring value of Nobel’s thinking about the criteria for the Peace Prize and more broadly, what is needed for peace.

In the context of Cyber peace specifically, and in relation to the aim of giving realistic Cyber peace a chance, this article has noted the initiative to establish a Cyber Peace Agenda that may help focus our attention at specific proposed actions in the pursuit of this otherwise quite abstract goal. The Agenda should be a living document and no doubt develop over time.

Perhaps the most significant observation that may be made from the above is that our pursuit of Cyber peace must be an ongoing sustained effort taking the form of many small steps, and hopefully some larger steps. It is a task for anyone who wants to contribute and as many of us as possible ought to implement, at least a subtle, “peace focus” in our daily work; that is, we need not necessarily change what we work on, but we ought to pause frequently and evaluate our work through the lens of Cyber peace. We must be realistic yet determined. That way, we can give Cyber peace a chance.

⁴⁰ The Nobel Prize. (2025) *Alfred Nobel’s thoughts about war and peace*. [online] Available from: <https://www.nobelprize.org/alfred-nobel/alfred-nobels-thoughts-about-war-and-peace/> [accessed 11 August 2025].

LIST OF REFERENCES

- [1] CCDCOE. *Self-Defence*. [online] Available from: <https://cyberlaw.ccdcoe.org/wiki/Self-defence> [accessed 11 August 2025]
- [2] Diehl, P. (2019). *Peace: A Conceptual Survey*. In: *Oxford Research Encyclopedia of International Studies*. Oxford University Press.
- [3] Douzet, F. G ry, A. and Delerue, F. (2022) Building Cyber Peace While Preparing for Cyber War. In: Shackelford, S., Douzet, F. & Ankersen C. (eds.) *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*. Cambridge: Cambridge University Press, pp. 170–193.
- [4] Haataja, S. (2019) *Cyber Attacks and International Law on the Use of Force The Turn to Information Ethics*, [online], CCDCOE, Available from: <https://cyberlaw.ccdcoe.org/wiki/Self-defence> [accessed 11 August 2025]
- [5] Hart, H.L.A. (2012) *The Concept of Law*, 3rd ed. Oxford: Oxford University Press.
- [6] Housen-Couriel, D. (2022) Information Sharing as a Critical Best Practice for the Sustainability of Cyber Peace. In: Shackelford, S., Douzet, F., & Ankersen C. (eds.) *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*. Cambridge: Cambridge University Press, pp. 39–63
- [7] ICRC. (2023) *The Principle of Distinction*. [online] Available from: https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/03_distinction-0.pdf [Accessed 11 August 2025].
- [8] Kello, L. (2022) *Striking Back: The End of Peace in Cyberspace – and How to Restore it*, New Haven: Yale University Press.
- [9] Kleffner, J. and Harrison Dinniss, H. (2013) Keeping the Cyber Peace: International Legal Aspects of Cyber Activities in Peace Operations. *International Law Studies*, 89.
- [10] Koskenniemi, M. (2011) *The Politics of International Law*, Hart Publishing.
- [11] Marlin-Bennett, R. (2022) Cyber Peace: Is that a Thing? In: Shackelford, S., Douzet, F., & Ankersen C. (eds.) *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*. Cambridge: Cambridge University Press, pp. 3–21.
- [12] Michael N. Schmitt (Gen. ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge, Cambridge University Press, 2017
- [13] Osula, A. M. Kasper, A. and Kajander, A. (2022) EU Common Position on International Law and Cyberspace. *Masaryk University Journal of Law and Technology*, 16 (1)
- [14] Pangrazzi S. (2021), Self-Defence against Cyberattacks? Digital and Kinetic Defence. In: ICT for Peace Foundation. *Self-Defence Against Cyberattacks?*, Geneva. Available from: <https://ict4peace.org/wp-content/upload>

- s/2021/03/ICT4Peace-2021-Cyberattacks-and-Article51-1.pdf [accessed 11 August 2025].
- [15] Roff, H. M. (2016) *Cyber Peace: Cybersecurity Through the Lens of Positive Peace*. [online] Available from: https://static.newamerica.org/attachments/12554-cyber-peace/FOR\%20PRINTING-Cyber_Peace_Roff.2fbfb0b16b69482e8b6312937607ad66.pdf
 - [16] Shackelford, S. Douzet, F., & Ankersen, C. (2022) Introduction. In: Shackelford, S., Douzet, F., & Ankersen C. (eds.) *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*. Cambridge: Cambridge University Press, pp. 19 – 31
 - [17] Svantesson, D. (2015) A Jurisprudential Justification for Extraterritoriality in (Private) International Law. *Santa Clara Journal of International Law*, 13, p. 517.
 - [18] Svantesson, D. (2015) A New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft, *American Journal of International Law Unbound*, 109, pp. 69-74.
 - [19] Svantesson, D. et al. (2023) On sovereignty. *Masaryk University Journal of Law and Technology*. 17 (1), pp. 33–85
 - [20] Téllez Carvajal, E. and González Hernández, J. (2022) Reflections on the Concept of Cyberwar and the Contributions of the International Community in the Peaceful Use of Cyberspace, *Opinión Jurídica*, 21(46) Special Edition, pp. 1-23.
 - [21] The Brussels Times (2025) *Sweden is 'not at war' but not at peace either, says PM Kristersson*. [online] Available from: <https://www.brusselstimes.com/1389724/sweden-is-not-at-war-but-not-at-peace-either-according-to-pm-kristersson> [accessed 11 August 2025].
 - [22] The Nobel Prize. (2025) *Alfred Nobel's thoughts about war and peace*. [online] Available from: <https://www.nobelprize.org/alfred-nobel/alfred-nobels-thoughts-about-war-and-peace/> [accessed 11 August 2025].
 - [23] The Nobel Prize. (2025) *Behind the scenes of the Nobel Peace Prize*. [online] Available from: <https://www.nobelprize.org/behind-the-scenes-of-the-nobel-peace-prize/> [accessed 11 August 2025].
 - [24] The Nobel Prize. (2025) *Full text of Alfred Nobel's will*. [online] Available from: <https://www.nobelprize.org/alfred-nobel/alfred-nobels-will/> [accessed 11 August 2025].
 - [25] Tsagourias, N. and Biggio, G. (2021) Cyber-peacekeeping and international law. In: Tsagourias, N. and Buchan, R. (eds.) *Research handbook on international*

law and cyberspace, 2nd ed., Northampton, Massachusetts. Edward Elgar Publishing, pp. 345-365.

- [26] U.S. Department of Defense (2024) *Military and Security Developments Involving the People's Republic of China 2024*. [online] Available from: <https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF> [accessed 11 August 2025].
- [27] United Nations Charter, Article 51.
- [28] Valeriano, B. and Jensen, B. (2022) De-escalation Pathways and Disruptive Technology. In: Shackelford, S., Douzet, F., & Ankersen C. (eds.) *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*. Cambridge: Cambridge University Press, 64–93.
- [29] Wegener, H. (2011) A Concept of Cyber Peace. In: International Telecommunication Union, *The Quest for Cyber Peace*. Available from: https://www.itu.int/dms_pub/itu-s/opb/gen/s-gen-wfs.01-1-2011-pdf-e.pdf, pp. 77-85.