CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

A Tale of Two Draft Resolutions: A Report on the Polarising International Law Discussions at the 2023 OEWG Substantive Sessions

Aleksi Kajander
NATO Cooperative Cyber Defence Centre of Excellence

Tallinn 2023

About the authors

The author of this paper Aleksi Kajander is a law researcher at the NATO CCDCOE. Additionally he is a Ph.D. candidate and Early Stage Researcher at the Tallinn University of Technology for Law and Technology. He holds a Master's degree in Investment Treaty Arbitration from Uppsala University as well as a Master's degree in Law and Technology from the Tallinn University of Technology.

CCDCOE

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) is a NATO-accredited knowledge hub offering a unique interdisciplinary approach to the most relevant issues in cyber defence. The heart of the CCDCOE is a diverse group of international experts from military, government, academia, and industry, currently representing 39 nations.

The CCDCOE maintains its position as an internationally recognised cyber defence hub, a premier source of subject-matter expertise and a fundamental resource in the strategic, legal, operational, and technical aspects of cyber defence. The Centre offers thought leadership on the cutting edge of all aspects of cyber defence and provides a 360-degree view of the sector. The Centre encourages and supports the process of mainstreaming cybersecurity into NATO and national governance and capability, within its closely connected focus areas of technology, strategy, operations, and law.

The Tallinn Manual, prepared at the invitation of the CCDCOE, is the most comprehensive guide for policy advisers and legal experts on how international law applies to cyber operations carried out between and against states and non-state actors. Since 2010, the Centre has organised Locked Shields, the biggest and most complex technical live-fire cyber defence challenge in the world. Each year, Locked Shields gives cybersecurity experts the opportunity to enhance their skills in defending national IT-systems and critical infrastructure under real-time attacks. The focus is on realistic scenarios, cutting-edge technologies, and simulating the entire complexity of a massive cyber incident, including strategic decision-making and legal and communication aspects.

The CCDCOE hosts the International Conference on Cyber Conflict, CyCon, a unique annual event in Tallinn, bringing together key experts and decision makers from the global cyber defence community. The conference, which has taken place in Tallinn since 2009, attracts more than 600 participants each spring.

The CCDCOE is responsible for identifying and coordinating education and training solutions in the field of cyber defence operations for all NATO bodies across the Alliance. NATO-accredited centres of excellence are not part of the NATO Command Structure.

www.ccdcoe.org
publications@ccdcoe.org

Disclaimer

1. Table of Contents

2. Abstract 4
3. Best Laid Plans of Mice and States 5
4. The Fourth Substantive and Inter-sessional 7
   4.1 Sovereignty 7
   4.2 Non-Intervention and Sovereignty 8
5. The Fifth Substantive Session 11
6. Results of the Substantive Sessions 14
7. Conclusions 16

2. Abstract

The UN's Open-Ended Working Group (OEWG) had its Fourth and Fifth Substantive Sessions in 2023, which included intense discussions on the applicability of international law in cyberspace. However, the sessions were naturally overshadowed by Russia's illegal war of aggression in Ukraine which resulted in several heated exchanges and uses of the right to reply during the sessions.

The sessions themselves did not proceed as expected, as a proposal by Russia and several other states for a new binding convention, although ultimately largely ignored by the final report, significantly altered the direction of the discussions. Additionally, a statement by Russia which undermined the applicability of international humanitarian law (IHL) in cyberspace similarly caused a distraction. Ultimately, the Sessions, while undoubtedly making some progress, were partially derailed by the unexpected proposals and statements.

Furthermore, besides the final report, two draft resolutions were produced at the end of the Sessions, which contained significant differences on key issues. This outcome reflects the increasing polarisation that is present in the discussions themselves. This paper is a report on the discussions and outcomes of the Fourth and Fifth Substantive Sessions of the OEWG in 2023 which aims to analyse the discourse as well as implications of the outcomes of the discussions.

3. Best Laid Plans of Mice and States

The proposed focus for the 2023 OEWG international law discussions was considerably shaped by the proposal made by Canada and Switzerland at the end of 2022 containing four specific topics: how the UN Charter applies in cyberspace; the peaceful settlement of disputes; international humanitarian law (IHL); and state responsibility. However, in the provisional programme of work for the Fourth Substantive Session, IHL and state responsibility were replaced by the principle of sovereignty, sovereign equality and non-intervention in the internal affairs of other states.

Furthermore, like the best-laid plans of mice and men, the discussions at the substantive session did not proceed as planned due to Russia's statement that IHL is not applicable in a cyber context and their submission of a concept for a new UN convention on cyberspace. The statement derailed the discussions, with numerous states voicing their surprise and opposition to the claim. Therefore, the progress that could have been achieved with substantive sessions focused on pre-defined issues of international law was hindered by Russia's statement.

The effect of the proposal was noticeable, as 12 states[1] expressed their views on the possibility of a binding convention during the Fourth Substantive Session. Despite an overwhelming majority of nine states[2] rejecting the need for a new convention, the damage resulted from the time used to consider and reject the proposal instead of using it for the agreed topics. The clear majority view was that a treaty is premature as the gaps in the existing international law must be identified first before even deciding on whether a new treaty is needed. As Australia eloquently put it, a treaty now would be like 'sending a patient to surgery without first determining if that person is even ill'.

A similar effect resulted from the attempt to undermine the applicability of IHL to cyberspace with states re-iterating that consensus on the topic had already been reached on an international level such as in the UN Group of Governmental Experts 2021 Report and the 2022 Annual Progress Report (APR) of the OEWG, both of which were endorsed by the General Assembly. A more in-depth analysis of the effects of the proposed convention and the claims intended to undermine the applicability of IHL is available at the CCDCOE library.

Despite the additional time and effort spent on rejecting these proposals, the OEWG did discuss the intended topics. But the shadow of what could have been and the

[1] See statements of: Australia, New Zealand, Romania, Switzerland, South Africa, Czechia, Israel, Netherlands, Cuba, Iran, Russia, Pakistan.
[2] See statements of: Australia, New Zealand, Romania, Switzerland, South Africa, Czechia, Israel and the Netherlands.

progress that may have been made absent the distractions will continue to mar the legacy of the Fourth and Fifth Substantive sessions.

4. The Fourth Substantive and Inter-sessional

4.1 Sovereignty

On the bright side, the Fourth and Fifth Substantive Sessions reaffirmed the consensus that the UN Charter applies both online and offline. While all of the UN Charter is considered applicable, the obligations to settle disputes peacefully (Articles 2(3) and 33(1)) and the prohibition on the use of force (Article 2(4)) were emphasised both during the discussions and the resulting 2023 APR. However, this is hardly a new development the General Assembly confirmed its applicability as far back as 2015. In light of the sudden U-turn on the applicability of IHL by statements made at the Fourth Substantive Session, it is perhaps to be appreciated that at least the approach to the UN Charter's applicability remains the same.

However, the principle of sovereignty and its implications for cyberspace remains a contested issue. On the surface, the wording of the APR which reaffirmed 'the principles of State sovereignty […] and the international norms and principles that flow from sovereignty' appears to convey a consensus. However, there remain unresolved conflicts. As the Swiss statement aptly summarised, internal sovereignty refers to the state's right to define, apply and enforce its own legal order in its territory. External sovereignty refers to the equality of states, which is to say no state should have any precedence or preference over another. In the cyber context, issues arise both on how to define the scope of sovereignty in cyberspace and whether or not violations of sovereignty are internationally wrongful acts.

El Salvador's statement during the intersessional discussion provides an excellent starting point for characterising the application of sovereignty to cyberspace. The statement refers to the Tallinn Manual's three-layered cyberspace consisting of the physical (hardware), the logical (data, software and anything else that connects network devices) and the social (individuals and groups engaging in cyber activities).[3] El Salvador contends that a state's sovereignty applies to the first and third levels. This interpretation departs from the Tallinn Manual's approach under which all three layers are subject to the sovereignty of a state.[4] By contrast, for example, Colombia stated that states exercise sovereignty over 'cyber infrastructure' within their territory, which could be argued to include only the first layer, subject naturally to the definition of 'cyber infrastructure' being used. This may lead to misunderstandings and miscommunications as different states may have differing views on which 'layers' of cyberspace are included in their definition for 'cyber infrastructure' and so such a statement could be interpreted differently by each state.

[3] Tallinn Manual 2.0 p.12.
[4] Ibid.

This highlights an important aspect of the discussions; that there is considerable room for miscommunication and misunderstandings that may result from ambiguous wordings. For example, Iran's view that they have the right to exercise sovereignty over 'their cyberspace' is likely to be subject to differing interpretations as to the limits of 'their' cyberspace. During the Sessions, most states did not discuss in nearly as much detail as El Salvador to what layers of cyberspace their sovereignty extends, with many merely writing a few lines stating that the principle of sovereignty applies. While it is the prerogative of states to remain as ambiguous as they desire, it would be helpful if more states would make their views known in a similar level of detail as El Salvador to facilitate a common understanding of the limits of sovereignty in cyberspace. Presently, there remains a risk of mismatched expectations and miscommunications on, for example, which layers of cyberspace are encompassed by the principle of sovereignty.

The question of whether violations of sovereignty amount to an international wrongful act also looms large. Needless to say, the implications of the controversy are considerable; the lack of a uniform understanding of what constitutes internationally wrongful acts may result in exploitable loopholes that enable harmful cyber operations to occur with impunity. This discussion is perhaps best approached from the apparent minority position that violations of sovereignty do not amount to internationally wrongful acts. The United Kingdom outlined its position whereby in essence they are not convinced that a sovereignty-based prohibition that would be separate from the principle of non-intervention exists. The UK does not contest the existence of sovereignty as a 'fundamental concept' of international law but argues that there does not arise a separate prohibition to the principle of non-intervention.

4.2 Non-Intervention and Sovereignty

The principle of non-intervention is characterised by two criteria: the intervention must pertain to something that the state may freely decide over (*domaine reserve*); and there is coercion. The first criterion is therefore intrinsically linked to sovereignty, as (internal) sovereignty is essentially the state's right to decide on its own matters freely within its own borders, through for example its own laws. As a result, no state has a right to intervene on the territory of another by, for example, enforcing its own legal order on the territory of another state. Hence, it is clear how a general principle of sovereignty is already encompassed within the principle of non-intervention through its first criteria. The difference boils down to those states that believe that violations of sovereignty are possible on their own versus those that believe that sovereignty is already protected by the principle of non-intervention and therefore it cannot be separately violated by a state's conduct.

The alternative approach where sovereignty can be violated by a state's conduct is equally understandable. This is perhaps best explained through the high threshold set by the second criterion that a cyber operation must meet to qualify as a prohibited

intervention, coercion. Coercion is not defined in international law[5] and remains ambiguous, which is partially acknowledged even in the UK's statement that states its definition of coercion and its evolution in its courts.

A traditional interpretation of coercion requires that the state is entirely deprived of options and therefore loses control over something over which it should have free reign. This therefore sets a very high threshold for the application of non-intervention. The UK appears to acknowledge the rigidity of this criteria by highlighting the possibility of cyber behaviour being coercive even if it is not possible to identify a single decision that the state has been forced to take. Nevertheless, it is unavoidable that there is a possibility that cyber operations could fall below the rigid definition and threshold of a prohibited intervention, especially due to the coercion requirement, into a legal blind spot. As a result, many states recognize that violations of sovereignty may occur in order to close the potential loophole of cyber operations falling below the prohibited intervention threshold.

As highlighted by the Fourth Substantive and intersessional discussion, the UK and Australia are of a similar opinion that violations of sovereignty are not possible. However, numerous other states such as Switzerland, Estonia and the Netherlands are of the opposite view. However, it is difficult to discern the opinion of many other states on this topic, as many, perhaps purposefully, do not provide detailed views and have left the question ambiguous while others like Iran believe that the issue is controversial and requires further discussion. The Colombian statement, for example, is carefully worded to not provide any definitive indication of toward which side of the discussion they lean. The Colombian position recognises the "international norms and principle flowing from sovereignty" but does not elaborate what those norms and principles are, thereby not committing to either interpretation.

Moreover, the language used at the OEWG when discussing sovereignty was noticeably different from that used in the state positions that discuss sovereignty. In state positions, the view that a violation of sovereignty is an internationally wrongful act is commonly compressed to a statement of 'sovereignty as a rule' or simply that sovereignty is a standalone rule.[6] This succinctly conveys the dichotomy between principles and rules under international law under which the violation of a principle is not internationally wrongful, unlike the violation of a rule, which if violated amounts to an internationally wrongful act. Consequently, it is surprising that only New Zealand referred to the 'standalone rule' of sovereignty. While seemingly a minor point, its implications are not insignificant.

Consider for example the Dutch statement on sovereignty in which the first paragraph states that sovereignty is one of the 'fundamental principles' of international law, which is later followed up on in the closing paragraphs with a contradictory statement that

[5] Tallinn Manual 2.0 p.317.

[6] Sovereignty - International cyber law: interactive toolkit (ccdcoe.org)

establishes an obligation for states to 'refrain from activities that constitute a violation of other countries' sovereignty'. While the Dutch statement enables the attentive reader with prior expert knowledge to deduce that the last paragraph conveys that the Netherlands considers sovereignty as a rule, the wording is arguably needlessly complex and subtle for what is being conveyed. This is especially evident when considering the Dutch National Position which clearly uses the wording 'standalone rule', something which leaves little room for misinterpretation or ambiguity. The needless subtlety of the statement used to convey the same position at the OEWG is striking and carries with it an unnecessary risk of miscommunication.

Therefore, the publishing of detailed national positions on international law and cyberspace, which was encouraged by numerous states at the OEWG[7], is a crucial step in reaching a common understanding of how existing international law applies in cyberspace and what gaps exist. An example of good practice in this regard is the Swiss statement at the intersessional which explicitly stated that for more details, the national position paper should be consulted. Such papers are invaluable in discussions such as those at the OEWG where time is limited as they not only reduce the chance of misinterpretation, but also the need for states to continuously re-state their definitions of contentious concepts in-depth, using up valuable time.

Similarly, the existence of state positions reduces the possibility of unfounded claims on 'majority positions' such as those put forward by Russia concerning the automatic applicability of international law, particularly IHL, to cyberspace as it will be readily evident from state positions where the majority truly lies. However, until more states release their national position papers, such arguments will retain a distracting power as demonstrated by the UN Convention proposal at the Fourth and Fifth substantive sessions at the OEWG, which used up the precious time and effort of the actual majority to invalidate it. Consequently, the role that national position papers play in the background during discussions on the applicability of international law is significant, and as the APR stated, the release of such position papers should be encouraged.

[7] See e.g. the statements of Czechia and EU at the May 2023 inter-sessional and Paragraph 31 b) of the 28 July 2023 Draft APR

5. The Fifth Substantive Session

The Fifth Substantive Session brought with it the second round of discussions on the proposal for a UN Convention on cyberspace that was received overwhelmingly negatively at the Fourth Substantive Session. Accusations that the OEWG was violating its mandate were also expressed. As a result, the Fifth Session was very much a continuation of the Fourth.

Seemingly undeterred by the negative feedback at the Fourth Substantive Session, Belarus and nine other states issued three joint statements that *inter alia* protested the treatment of the convention proposal in the draft report and accused the OEWG from straying from its mandate as encompassed in UNGA Resolution 75/240. Of this group, Russia went the furthest by increasing the audacity of its claim challenging the 'full and automatic' applicability of international law at the Fourth Substantive Session. Russia changed its argument by going even further in stating that 'most states do not share the opinion on the full and automatic applicability of international law to the use of ICTs'. Flying in the face of reality and the extensive debunking at the Fourth Substantive Session of the more cautiously worded initial argument, Russia went all in with the new version. Instead of questioning the applicability of IHL in the cyber context, the new wording no longer contained any limitation to IHL but rather questioned the applicability of the whole of international law to cyberspace. The resulting argument is inconceivable in the light of the consensus that has been consistently developed for the better part of a decade with numerous UN instruments clearly stating that international law applies to cyberspace.

Out of the 13 available statements on the UNODA website[8] that Russia made alone, nine mentioned the UN Convention proposal. It would appear that Russia attempted to undermine even the application of the UN Charter to cyberspace during the Fifth Substantive Session. This is evident from Russia's statement that the APR draft missed an 'essential element of a longstanding compromise' which, according to Russia, is the 'need for [the] progressive development of international law [… through the] development of new norms of a legally binding nature'. Thus, it would appear that the underlying 'logic' is that the UN Charter, as well as other international law, applies to cyberspace only insofar as it is 'confirmed' through new legally binding instruments which Russia, among others, is conveniently proposing.

This claim is entirely baseless as the applicability of international law and the UN Charter have been highlighted numerous times in UN General Assembly Resolutions, such as the 2015 Resolution A/RES/70/237 and the 2018 A/RES/73/27. The restatement of the same claim in a more audacious form at the Fifth Substantive Session is difficult to reconcile with good faith argumentation considering the extensive

[8] See Fifth Substantive Session statements by Russia (13) available at the Meetings.unoda.org website.

consensus on the matter as evidenced by the UN Resolutions which Russia must have been aware of considering Russia itself cited Resolution A/RES/73/27 at the Fourth Substantive Session. The Resolution explicitly confirms the applicability of both international law and the UN Charter.

Nevertheless, in the end, despite the protestations of Russia, Belarus and others, the proposal for the Convention was largely ignored by the final report with only a few passing mentions being included. The report stated that 'important proposals were put forward' that were not 'necessarily agreed by all States, including the possibility of additionally legally binding obligations'.[9] As can be seen from the wording, it does not reference any specific proposal by name, nor give any appreciable detail. Similarly, in Paragraph 32 the possibility of 'additional binding obligations, if appropriate' was noted. This reflects the actual majority position whereby a convention for cyberspace with legally binding obligations could be considered in the future, but only after the gaps in the current application of international law are identified. Consequently, the main accomplishment of the treaty proposal by its defenders would appear to be the distraction it provided from the main topics of the international law discussion.

Secondly, Belarus *et al.* in their joint statement made an accusation which was later echoed by Russia, that the OEWG had strayed from its mandate at the Fifth Substantive Session. In essence, the argument stated that the OEWG had failed to comply with its mandate as outlined in UN Resolutions A/RES/75/240 and A/RES/76/19. As outlined in A/RES/75/240, the OEWG has a twofold mandate: to 'further develop the rules, norms, and principles' and oversee 'their implementation, and, **if necessary**, to introduce changes to them or elaborate additional rules of behaviour' (emphasis added).[10] The accusation contends that the OEWG is ignoring the first part of the mandate for further development and only focusing on implementation. This argument is tenuous at best considering the wording of the Resolution itself states that changes should only be introduced 'if necessary', which must therefore imply that the need for such changes be first identified. This concurs with the opinions of states opposing the current treaty proposal, which argue that such gaps must first be identified to determine if it is necessary to introduce new rules or changes such as through a convention.

Moreover, the wording of the first part of the mandate, which supposedly is being ignored by the OEWG, is clearly broad enough to encompass its current activities and discussions. For the current discussions on establishing *how* the current laws apply in cyberspace progresses the understanding and application of said laws, which, therefore, 'further develops' the 'rules, norms, and principle' as required by the first part of the mandate. It would appear that the states proposing a new UN treaty have fixated on the idea that the only further development in the meaning of the mandate is a new

[9] Paragraph 29(b)(i).
[10] A/RES/75/240.

binding treaty. This is in clear contradiction to the original mandate that makes it clear that any changes should be made only 'if necessary', which therefore explicitly provides for the possibility that no changes would be made and the mandate would still be fulfilled. Consequently, the argument put forth by Belarus *et al.* is without substance to the extent that one could wonder whether it was made in good faith. This persistent unfounded argumentation was ignored by the final version of the APR and its lasting influence is to be found primarily in the time it consumed at the Fifth Substantive Session.

6. Results of the Substantive Sessions

After the Fourth and Fifth Substantive Sessions two separate draft resolutions were put forward, 'L.11' tabled by Russia and 'L.60/Rev.1' by Colombia, France and the United States. While broadly similar to the extent that many states voted in favour of both, there are key underlying differences between them. Unsurprisingly the main differences relate to the same points of disagreement that were raised during the Substantive Sessions.

First and foremost, the wordings differs when it comes to the possibility of binding legal instruments in the future. L.60/Rev.1 leaves the door open for legally binding instruments in the future by "'noting the possibility of future elaboration of additional binding obligations, if appropriate'. The wording clearly reflects an uncommitted position with 'possibility' and 'if appropriate' that leaves the issue to the discretion of the states in the future. By contrast, the wording in L.11 is rather more definite, with the draft noting 'the need to further consider the development of additional legally binding obligations'. The use of 'need' implies an existing and underlying demand for such an obligation, which is in line with Russia's rhetoric during the Sessions.

Moreover, the L.11 draft also mentions 'specific proposals of States on establishing an international legal regime' thereby indirectly highlighting and drawing attention to the proposed concept for a legally binding treaty that was submitted during the Sessions. Consequently, while the differences are fairly subtle, L.11 tacitly and delicately serves to reinforce the rhetoric and arguments Russia made during the Sessions. As a result, it would not be a surprise if Russia returns to the fact that 112 states voted in favour of L.11 in its future argumentation as evidence that the 'need' for a treaty exists.

A second key difference was the focus on prohibited interventions and the duty of states to refrain from 'any defamatory campaign, vilification or hostile propaganda' that would interfere in the internal affairs of states, which was present in L.11 but not in L.60/Rev.1. This 'duty' seemingly seeks to limit the ability of states to legitimately criticise the actions of other states, which is presently specifically excluded from being considered a prohibited intervention[11].

The word 'vilification' in particular is so broad that it can easily be used to encompass almost any criticism, legitimate or not, including ironically the type of rhetoric which was used by Russia itself in its right to reply during the substantive session where it accused NATO countries of being criminal accomplices and having in their hands the blood of civilians.

Moreover, the reason 'coercion' is a requirement in the definition of a prohibited intervention is to set a high threshold to limit its application to only the most serious

[11] See Tallinn Manual 2.0 pp.318-319.

cases where due to the direct intervention of another state the victim state is made unable to govern freely. As such it is absurd to suggest a state would no longer be able to govern its own affairs after being subject to mere criticism of its policies. The attempt by L.11 to include criticism in the concept of a prohibited intervention is a dangerous development because, if left unchecked and unopposed, it could lead to a world order where censorship would become an international norm and criticism an internationally wrongful act.

Nevertheless, by the votes L.60/Rev.1 proved to be the more popular draft with 158 states in favour and only 10 against, whereas L.11 received significantly more opposition with 52 states opposing and 112 in favour. However, it is concerning that the trend started by the split into two separate working groups in 2018 (the OEWG and the Group of Governmental Experts) is continuing with two differing draft resolutions being the final product of the Fourth and Fifth Substantive Sessions. Given that the contents of the two were broadly similar, the devil definitely lies in the details, whereby the implications of L.11 could serve to fuel the polarisation already witnessed for years to come.

7. Conclusions

The Fourth and Fifth Substantive Sessions of the OEWG were certainly colourful and memorable events with surprising proposals, statements and even accusations against the OEWG itself. This represents a concerning development as such actions could derail the OEWG discussions entirely from the agreed focus for sessions. Moreover, in the case of the Fourth and Fifth Substantive Sessions, some of the arguments and accusations were arguably so far-fetched and unfounded as to raise serious questions on whether they were truly the product of good faith discourse. The final report's decision to largely ignore these unwelcome developments was both prudent and practical as it denies them any further influence or official recognition, thus limiting the damage to the time wasted in listening to and refuting such claims.

Nevertheless, the Sessions did highlight important aspects related to the applicability of international law in cyberspace. In particular, despite Russia's attempts, the reaffirmation of the UN Charter's applicability in the final report further solidifies its well-established position in regulating cyberspace. However, it was frustrating that the discussions on sovereignty did not have the depth required to truly discuss the existing alternative interpretations of its applicability in cyberspace. This shortcoming highlights the importance of the recommended next step in paragraph 34 of the APR, which is for states to publish their national positions on the applicability of international law in cyberspace, which would not only help establish a solid baseline for discussions but also reduce the chance for misinterpretation and miscommunication in the discussions. Consequently, it is evident that the discussions at the OEWG still have a long road ahead of them and it is important that the process is continued and any attempts at derailing the discussions as seen in the Fourth and Fifth Sessions are reacted to appropriately.

Moreover, the draft resolutions reflect the increasing polarisation at the OEWG. This is evidenced not only by their content but by the very fact that there are two of them. Despite the broadly similar content, L.11, in particular, is sowing the seeds for further discord by subtly and implicitly legitimising the arguments that were so vocally rejected during the Sessions.