CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

# Unnecessary Repetition: Russia's Latest Attempt at a New UN Convention on Cyberspace

Aleksi Kajander
Law Researcher, NATO CCDCOE

Parallel to the cyber front of Russia's illegal war of aggression in Ukraine, conflict brews within the discussions on the cyber aspects of international law at the United Nations Open-Ended Working Group (OEWG). Russia's latest proposal for a legally binding convention on ensuring international information security was submitted by Russia on the 29th of June after the fourth substantive session of the OEWG. It was conspicuous, despite it being ultimately largely ignored in the Progress Report. Even if ultimately unsuccessful, such proposals serve to direct the discussion and draw attention to the proposer's desired topics, hence they are an effective influencing tool. Russia has a long history of proposing new conventions and instruments at the United Nations, so this is nothing new; however, after its successful proposal for a UN convention on cybercrime, all such initiatives should be carefully examined. While seemingly innocuous on the surface, this proposal is akin to a Trojan horse filled with the proposer's own interests.

## 1. The Cart Before the Horse

The accepted consensus on international law and cyberspace is that the law applies in its entirety in cyberspace, although there may be gaps in the application of certain rules. However, Russia and a few other states caused a stir at the fourth substantive session of the OEWG by attempting to undermine the applicability of international humanitarian law (IHL) in the cyber context, claiming that it neither applies fully nor automatically. As expressed by the Swiss statement, this is a surprising, not to mention unfounded, claim. The applicability of international law, including IHL, in cyberspace has been repeatedly confirmed by numerous individual state positions and by various reports such as the UN Group of Governmental Experts' 2021 report and the 2022 OEWG Annual Progress Report.

The backtracking on this matter is thus remarkable, although perhaps not surprising in light of the convention proposal and the ongoing armed conflict in Ukraine. The justification for this backtracking is two-fold. Firstly, as IHL applies only during an armed conflict, it cannot be applied to peacetime cyber operations. While this is correct, it is the second part of the justification that is a misapplication of international law: Russia claims that there is 'no consensus' on qualifying malicious cyber operations as an 'armed attack' under the UN Charter's Article 51, which would enable a state to legitimately resort to self-defence as a

response to a cyber operation. Consequently, Russia considers that cyber operations cannot be assessed from an IHL perspective at all.

This latter claim, while creative, is a misrepresentation of the law. Application of IHL is not conditional upon the application of Article 51 of the UN Charter. IHL applies during a time of armed conflict, regardless of whether a belligerent is relying on Article 51 of the UN Charter for legitimate self-defence. IHL applies equally to all belligerents, regardless of whether they are legitimately defending themselves under Article 51 of the UN Charter or engaging in an illegal war of aggression, such as that of Russia in Ukraine. Consequently, from a purely IHL applicability perspective, whether Article 51 of the UN Charter is relied on is irrelevant: IHL will begin to apply from the moment an armed conflict exists. While there is no specific treaty on cyber warfare, the customary international law of IHL applies to all states during armed conflicts, regardless of whether the conflicts are fought physically in the trenches or cyberspace. Therefore, the argument that cyber operations cannot be assessed from an IHL perspective is inconceivable, for they can and must be assessed from an IHL perspective during an armed conflict.

The misapplication of existing international law has thus been used to create an artificial problem, in order to be able to propose a solution for it in the form of a new convention. This proposal has been met with considerable resistance from numerous states and organisations, such as Switzerland, Israel and the European Union, which all consider it imperative to first clarify how the existing rules apply before creating any new binding convention. The accepted consensus has been, and still is, that international law, including IHL, applies in cyberspace, although *how* exactly it applies remains to be clarified in problematic areas. The Swiss statement, that a convention would be premature before the application of the existing international law is clarified, exemplifies the prevailing majority sentiment. Therefore, the timing, circumstances and manner in which the convention proposal was presented not only represents putting the cart before the horse, but is additionally an unnecessary departure from the previously agreed consensus that international law applies in cyberspace.

## 2. Conventional Deception

### 2.1 Unnecessary Repetition

The primary justification put forward for the treaty proposal is the 'growing need' to 'conclude a legally binding' treaty. However, this 'growing need' is unfounded, or at the very least considerably exaggerated. The sources provided for this statement include three UN Documents (A/75/817, A/76/135 and A/RES/76/19) which do not stand up to closer scrutiny.

Proceeding in order, A/75/817, an OEWG report from 2021, recommends (paras 38-40) that states continue to provide their national views and assessments on how international law applies in order to construct a better understanding of the application of international law in the cyber context. The 'growing need' was only to be found within the Chair's summary, which mentioned that some states felt that a binding legal instrument might be required. However, a mere few paragraphs later it highlighted that the states proposed as a 'first key step' the clarification of a common understanding of how international law applies. While there were states which did feel that a legally binding instrument might be in order, this view did not make it into the recommendations of the report. Consequently, it cannot be elevated to an issue that warrants a convention before completing the agreed

first key step of establishing how the law applies. Similarly, the second document A/76/135, a GGE Report from 2021, in paragraph 72 repeats the sentiment that first clarifying the existing law through discussions and exchanges of views is crucial. This point is repeated in the recommendation section of the document in paragraph 95 (b). Furthermore, the third document, A/RES/76/19, merely mentions the possibility of having a binding legal instrument in the future 'if appropriate', while clearly emphasising the importance of first discussing how international law applies in the cyber context.

Therefore, the proposed convention is not actually addressing a 'growing need', at least not a need of the international community. The consensus is clearly for first finalising the discussions on how the current international law framework applies, before any binding legal instrument may follow, should it be deemed appropriate.

The redundancy of the convention is amply reflected in the number of suggested provisions that are already either encompassed or derived from the UN Charter. Under Section III of the proposed convention, these include Article 3, the prohibition on the use of force (UN Charter 2(4)), Article 5 prohibiting already prohibited interventions, and Article 7 on the obligation for the peaceful settlement of disputes (UN Charter Articles 2(3) and 33). There is simply no need to restate such provisions, as they are encompassed in the UN Charter and the Charter constitutes customary law applicable to all states. To re-encompass them in a treaty would actually be both unnecessary and technically a downgrade in terms of coverage, as a treaty only binds those states that are party to it, whereas customary international law applies to all states.

## 2.2. Imposing Sanctions on Sanctions

The real purpose of the proposed convention arguably lies beneath the repetition of many of the UN Charter's obligations: it is to elicit changes favourable to the proposer under the guise of objectivity and concern for international peace and stability. Section III Article 6 of the proposal is perhaps the most flagrant example of this: to summarise, in effect, the Article would make it considerably more difficult for states to respond to cyber operations via sanctions.

Firstly, the legality of imposing sanctions on trade between states for any reason is well-established.[1] A state is legally able to terminate trade relations with another state at any time, without any justification. Therefore, states have no general obligation to state the reasons or justify sanctions they impose, for example as a response to a breach of international law by the sanctioned state. Consequently, alongside other unfriendly, but entirely legal, means of influencing other states' behaviour, sanctions have become common responses to undesirable or illegal behaviour by other states such as malicious cyber operations. Therefore, a state is, in principle, free to legitimately decide to impose sanctions on any other state as a response to a cyber operation, without justification. Thus, the proposal to restrict this ability to impose sanctions for states that do not have contrary legal obligations would be an entirely unwarranted restriction on the freedom of sovereign states to choose their trading partners.

Only in the case where a state has entered into a treaty or other binding legal arrangement that contains a contrary legal obligation, which imposing sanctions would breach, is a state required to justify or excuse its imposition of sanctions. In this latter case, the sanctions

[1] See International Court of Justice (1986), *Nicaragua v. United States of* America, paragraph 276.

could be classified as countermeasures, as their imposition would be illegitimate, due to the existence of a contrary legal obligation, were it not for the fact that they are imposed as a response to a breach of international law by another state, in order to make that other state cease its breach of its (international) legal obligations. Moreover, besides countermeasures, alternative grounds exist under established international law for excusing the imposition of sanctions (or other measures), such as necessity. Therefore, international law already regulates the imposition of measures that would otherwise be unlawful were it not for the existence of certain circumstances, and thus, it is unnecessary to restate this in a new convention.

Furthermore, sanctions that must be justified or excused under international law, such as countermeasures, are strictly limited in the time for which they may be imposed, such as the duration of the other state's breach of its obligations. By contrast, sanctions by states which have no contrary legal obligations, that are launched in response to, for example, a cyber operation, may remain in place long after the cyber operation has ended and, thereby, have a considerably higher deterring effect. Therefore, the effect of depriving victim states of legitimate and effective means of responses that do not need justification or an excuse under international law, such as sanctions, would in effect significantly hamper their ability to legitimately respond to unlawful and hostile cyber operations. The only beneficiaries of such provisions would be the states that conduct malicious cyber operations, while states which are frequently targeted would suffer.

## 2.3. Frustrating Attribution

Similarly, the net beneficiary of provisions that would both introduce an unreasonable evidentiary standard for attribution and require a state to publicly disclose evidence, especially technical evidence, would also be the perpetrator state(s). This may seem surprising at first, as on the surface an obligation to publicly substantiate the attribution of a cyber operation seems like a reasonable proposition intended to improve transparency and reliability of attributions. However, underneath the façade of transparency lurks a surreptitious ulterior motive for these provisions.

One of the primary reasons why states are reluctant and frequently hold back details of exactly how they attributed a cyber operation is simple. In doing so, the attributing state risks revealing its technical capabilities and the methods it uses to attribute cyber operations, as well as other sources of intelligence to which it may have access. This information is worth its weight in gold to the perpetrators of malicious cyber operations, as they can use this information to adjust their operations in order to reduce the chance of future successful attributions. Therefore, a legally binding obligation that would deprive states of the ability to decide on a case-by-case basis what evidence they would disclose would significantly benefit the perpetrators of such malicious cyber operations.

It is prudence, rather than intentional obfuscation, when attributing states decide not to publicly share the full details of how exactly they attributed the operation. Therefore, the freedom of states to decide on which evidence to share publicly must be preserved. No other actor besides the attributing state can reasonably be claimed to be in a better position to assess what should and should not be shared in order to prevent the information from benefitting malicious third parties. Moreover, the effects of the proposal's provisions on attribution cannot be examined in isolation without considering the other provisions. In particular, the proposed restriction of the ability to impose sanctions as discussed previously, in combination with the proposed attribution requirements, would together serve

to considerably incentivise illegal cyber operations, as the imposition of legitimate responses would be made considerably more difficult.

## 3. Conclusions

The proposal for a binding treaty on ensuring international information security is arguably an example of placing the cart before the horse in the realm of international law. Currently, as many states have pointed out, the focus on the cyber aspects of international law is on determining how it applies and identifying any gaps. It is both premature and illogical to make any proposal for a binding treaty when the gaps such a treaty should fill are yet to be fully identified. However, it is evident from the proposal that other concerns and agendas are the main reasons for a new treaty. The proposal itself does little besides re-stating already applicable customary international law, except for the provisions that attempt to introduce insidious changes into international law. These include the attempt to undermine and restrict the ability of states to impose sanctions on other states and the obligation to 'substantiate' the attribution of cyber operations publicly. What both of these proposed changes have in common is their negative effect on states victimised by cyber operations while benefitting the perpetrators of cyber operations that breach international law. Consequently, the proposal should be rejected, as it would not benefit either the international community or international law.