UN General Assembly Cybercrime Treaty Negotiations - Short Overview

In January 2022 a two year process to create a new global convention on Cybercrime gets underway in New York under the aegis of the UN General Assembly: the Ad-Hoc Committee on Cybercrime ("AHC").[1]

Originally initiated primarily by Russia, it is seen by many Western democratic states as a vehicle for Russia to create a competitor agreement to the European Convention on Cybercrime (Budapest Convention), which Russia (and others) refuse to join but which global business has long supported[2]. The ostensible argument for a new treaty is that there is no expressly global treaty on cybercrime per se, and that the Budapest Convention is a European instrument, and a global instrument is needed - despite the fact that Budapest is open to any member-state that wants to join and many non-European states already have.

The timing of this initiative is not accidental; the parties to Budapest are in the final stages of adding a new protocol[3] to Budapest which industry has participated in drafting, and which considerably modernises and updates Budapest's provisions.

The AHC will have six meetings, three each in New York and Vienna and at the end requires only 60% of participating governments to support for it to be submitted to the UN General Assembly for adoption. There is a process for engagement by NGOs and industry though so far industry participation has been rather limited.

This is at once a geopolitical contest between Russia and its friends on the one side and the like-minded Western democratic states on the other and it carries significant risks as unlike the UNGA's work on cybersecurity, which requires consensus, this process does not.

- The objective is an outcome that doesn't exist at the global level but where the substance duplicates existing agreements that any UN member-state may already join.

[1] For an overview of the process and more detail please visit https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home.

[2] Sixty-six countries are already in Budapest; 11 more are in the process of joining. See the list here: https://www.coe.int/en/web/cybercrime/parties-observers.

[3] The "Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence," at https://rm.coe.int/0900001680a2aa1c.

- Since the expertise on cybercrime in the UN system is focused in Vienna at the UN Office on Drugs and Crime having this process overseen by the UN in New York carries risks that some member-states' officials will not have the substantive background to understand the potential negative consequences of provisions that might sound sensible to a diplomat without an extensive background in the subject - and most member-state delegations in New York don't have specialists in the subject available;

- The relatively low bar for the process to move to a conclusion means that political considerations and numbers of votes can allow genuinely harmful outcomes to move forward - a consensus-based process does not carry that same risk;

- Ultimate adoption is by the General Assembly which seeks to adopt outcomes by consensus but often votes on contentious issues - again making political considerations and deal-making across all the issues on the table at the time the outcome reaches the Assembly far more influential on the outcome than a subject like this deserves.

Russia has already tabled a draft treaty for consideration in January, a draft which has many provisions which would be profoundly negative for industry worldwide as well as the development of an open, permissionless-innovation-based Internet:

- Article 19 - making an offence of any suggestion anywhere online that a government of another state should be overthrown.
- Article 28 - creates very broad contributory liability
- Article 28 - on legal persons - also very broad.
- Article 33(1(a) - creates a very broad right for each state to "record" any information "transmitted by means of ICTs" in real time - this would effectively end all privacy online amongst other effects. (b) creates very broad obligations on service providers as well.
- Article 35 - obligations to hold "traffic data" "regardless of how many service providers were involved in the transmission of data" - so everyone from ISPs onwards would have to retain very broad amounts of information about what everyone, everywhere did and looked at online.

It is true that it is early in this process and this is only one proposal - but it does give a picture of what the main originating member-state has in mind. The relatively low threshold for the outcome of this process to lead to a treaty means

that industry needs to have a robust level of engagement with the member-states to ensure they understand what industry really needs and what the unanticipated negative consequences of provisions they are discussing really are. Civil society and many companies have recently voiced serious concerns about this process in a joint statement.

Industry also needs to participate actively to ensure friendly delegations keep our views in mind and have the information they need to help make the case for good outcomes - even if the best outcome turns out to be no new treaty.

The brief is provided by Nick Ashton-Hart who follows the cyber-related work of the UN General Assembly for ICC United Kingdom. He can be reached at nashtonhart@iccwbo.uk.