CIHOL International Law Brief

Czech Republic publishes position paper on the application of international law in cyberspace

The Czech Republic has joined a host of nations and organisations pronouncing on the applicability of international law in cyberspace (see here for the various positions). On 27 February, the Ministry of Foreign Affairs of the Czech Republic formally published its Position Paper on the Application of International Law in Cyberspace. The position paper, developed in cooperation with the Ministry of Defence and the National Cyber and Information Security Agency, highlights the official position of the Czech Republic on eleven key issues: state sovereignty, the prohibition of intervention; peaceful settlement of disputes; the use of force; the law of neutrality; international humanitarian law; international human rights law; State responsibility and attribution; retorsion; and circumstances precluding wrongfulness.

Key takeaways:

Sovereignty

The Czech Republic considers that the principles of sovereignty and sovereign equality of States applies equally to cyberspace. Sovereignty may be exercised over a State's territory and includes information and communication technologies (ICTs) located within that territory. Cyber activities which do not amount to prohibited intervention or prohibited use of force may nevertheless amount to a violation of a State's sovereignty. Consequently, such activities would be considered an internationally wrongful act under the Draft Articles on State Responsibility for Internationally Wrongful Acts.

The position paper does however list three instances when the Czech Republic considers a violation of sovereignty. Cyber operations violate sovereignty when they:

- Cause significant physical damage, death or injury to persons
- Damage or disrupt cyber or other infrastructure which significantly impacts on national security, economy public health, public safety or the environment (such as a power outage affecting thousands of homes)
- Interferes and thereby disrupts data or services essential for the exercise of inherently governmental functions (such as an operation which disrupts the payment of retirement or social benefits)

Prohibition of intervention

The Czech Republic views the prohibition of intervention applying only between States. In situations where intervention is conducted by individuals or non-state actors, such intervention is prohibited when it is attributable to States. Cyber activities may violate the prohibition of intervention if they are 'comparable in scale and effect to intervention in non-cyber contexts.' Two conditions of such interventions are detailed: the cyber activity tampers with the internal or external affairs of the State; and, the cyber activity must be coercive in nature. However, no definition of coercion is provided. One specific example given of the violation of the prohibition

of intervention is when cyber activities target election systems to manipulate the outcomes of an election.

Interestingly, the Czech Republic does not consider cyber activities described as 'propaganda' as a violation of the prohibition (as long as they do not violate other rules of international law). Similarly, the Czech Republic does not view 'influencing, criticism or persuasion' as violations either (*cf* the positions of Costa Rica and Switzerland).

Due Diligence
The Czech Republic considers that the obligation of due diligence on States extends to cyberspace; States therefore have an obligation to take 'reasonable and feasible measures' to prevent, eliminate or mitigate potentially significant harm to legally protected interests of other States. In this case, the Czech Republic considers that harm need not be limited to physical damage or injury but that other serious non-physical harm may trigger the due diligence obligation.

Use of Force
The prohibition of the threat or use of force in Article 2(4) of the UN Charter applies equally to cyberspace. Cyber activities may amount to a use of force when the effects of a cyber operation are 'comparable to those of a conventional character.' While the term 'use of force' is not defined by the UN Charter, the Czech Republic considers factors provided for in the Tallinn Manual 2.0 important criteria when characterizing a cyber act as an unlawful use of force. These factors include among others, severity, immediacy, directness, invasiveness, and measurability of effects.

Similar to other position papers, the Czech Republic views cyber operations attributable to States as potentially constituting armed attacks under Article 51 of the UN Charter, thereby giving rise to the right of individual and collective self-defence (see *inter alia* the positions of Australia; the African Union; Finland; Italy; the United Kingdom). It did not however take any explicit position on whether self-defence can be permitted against a solely non-State actor. Few States have gone this far in their positions papers (see for example Denmark and Germany who have stated that non-state actors could mount armed attacks to which self-defence may apply; France on the other hand has rejected such an assertion). Cyber operations 'comparable in its scale and effect to an attack by convention means (kinetic operations) in terms of gravity, such as fatalities, damage and destruction' may be considered armed attacks.

Importantly, the Czech Republic indicates that self-defence may be used 'if an armed attack occurs' suggesting it does not support pre-emptive, anticipatory or preventive self-defence (similar positions are held by the African Union, Brazil; cf France). In addition, while a response in self-defence must be necessary and proportionate, such a response is not limited to the cyber domain. The Czech Republic also affirms its position that collective self-defence in response to an armed attack can only be exercised 'at the request of the victim State and within the scope of such a request.'

Neutrality
The Czech Republic considers that cyber infrastructure located within a neutral State is protected by both territorial integrity and the rules of international humanitarian law. Such

infrastructure is protected regardless of public or private ownership or the nationality of the owners, so long as it is not used by the parties to an international armed conflict for the exercise of belligerent rights.

The Czech Republic further views that the use of a public, internationally and openly accessible network by for military purposes does not violate the law of neutrality 'even if it or its components are located on the territory of a neutral State, provided that doing so does not have any harmful effects on that State'. The Czech Republic considers that neutral States are obliged to take all feasible measures to terminate an abuse of cyber infrastructure within its territory by a party to an international armed conflict.

International Humanitarian Law

The Czech Republic considers that the rules of international humanitarian law (IHL) apply to cyber operations both in international and non-international armed conflicts. Cyber operations during an armed conflict attributable to a State may constitute an 'attack' under IHL if its effects are 'comparable to those conducted by conventional means or methods of warfare'. IHL provides the same protections to persons and objects in conventional warfare as it does in cyberspace.

State Responsibility and Attribution

The Czech Republic considers that state responsibility as reflected in the International Law Commission`s Draft Articles on Responsibility of States for Internationally Wrongful Acts applies to State behaviour in cyberspace.

The Czech Republic is of the view that cyber activities are attributable to a State if perpetrated by organs of States, or persons or entities exercising elements of governmental authority and acting in that capacity in the particular instance, or organs placed at the disposal of a State by another State. Importantly, the Czech Republic also considers state responsibility for international wrongful acts conducted by 'cyber means and perpetrated by nonstate actors if such an actor in fact acts on the instruction of, or under the direction or control of that State in carrying out the conduct in question.'

Countermeasures

In case of cyber-related violations of international law attributable to other States, both in the form of actions or omissions, the Czech Republic reserves its right to respond by undertaking countermeasures to induce the wrongdoing State to comply with its international obligations. This response can be carried out using traditional forms of countermeasures (such as trade embargoes and financial sanctions) or via cyber means.