BRILL
NIJHOFF

NORDIC JOURNAL OF INTERNATIONAL LAW
92 (2023) 446–455

NORDIC JOURNAL OF INTERNATIONAL LAW
brill.com/nord

# Denmark's Position Paper on the Application of International Law in Cyberspace

## *Introduction*

*Jeppe Mejer Kjelgaard*
Ministry of Foreign Affairs of Denmark, Copenhagen, Denmark
*jepkje@um.dk*

*Ulf Melgaard*
Ministry of Foreign Affairs of Denmark, Copenhagen, Denmark
*ulfmel@um.dk*

Published online: 4 July 2023

A number of States have published national position papers on the application of international law in cyberspace to further the common understanding of the interpretation of international law in this domain. Denmark fully supports these efforts and is pleased to now share its own paper.

The focus of the Danish position paper is on cyberspace in the broad context of international law, including issues pertaining to state sovereignty, non-intervention, the prohibition on the use of force and international humanitarian law. The position paper supplements Denmark's views already expressed in the UN Open-ended Working Group on Information and Communication Technologies and through the annual reporting to the UN Secretary General.

*May, 2023*

# Denmark's Position Paper on the Application of International Law in Cyberspace

## 1 Introduction

The UN General Assembly has endorsed the conclusions set out in the reports from the Group of Governmental Experts (GGE) and the Open-ended Working Group on Information and Communication Technologies (OEWG) affirming that international law, including the UN Charter, applies in cyberspace. Denmark is an unwavering supporter of this view and continues to support efforts to develop the rules, norms and principles of responsible State behaviour in cyberspace. As a strong proponent of the rules based international order Denmark is fully committed to international law as the fundamental framework for responsible state behaviour in cyberspace. With a view to contributing to clarifying that framework this paper sets out Denmark's official position on selected issues of international law in relation to cyberspace. The aim of the paper is to strengthen the interpretation of international law in relation to cyberspace and to clarify the basis upon which Denmark will respond to unlawful acts from other States and non-State actors in cyberspace.

It is the view of Denmark that the application of international law does not depend on the particular technological means employed. Treaty obligations, customary law, and general principles of law apply across domains, which includes operations conducted in cyberspace.

However, unanswered questions remain regarding the precise interpretation of international law with respect to cyberspace operations. This lack of clarity stems from general issues of interpretation of international law, from limited State practice in cyberspace, and from the unique characteristics of cyberspace. Consequently, the understanding of how international law applies to cyberspace is, and will continue to be, a complex and evolving process.

The focus of this paper is on cyberspace in the broad context of international peace and security and general issues of international law such as state sovereignty, use of force, countermeasures and international humanitarian law (IHL). Denmark subscribes to the general view that also human rights obligations apply in cyberspace, but for the sake of brevity this paper does not elaborate further on that topic. In addition, the paper does not deal with sector specific issues such as law enforcement cooperation, intelligence gathering and telecommunications law, nor does it address the many treaty obligations that Denmark is subject to, and which would necessarily be part of a legal analysis of any particular cyber operation.

It should also be noted that international law does not regulate all cross border cyber activities undertaken by States. Some cyber acts might be unfriendly, or even hostile, but not as such regulated by international law and will accordingly be subject to policy considerations.

## 2 Sovereignty

Sovereignty denotes each State's authority to exercise within its territory the functions of a State, to the exclusion of any other State. Denmark is of the view that sovereignty is not only a principle but a primary rule of international law a breach of which amounts to an internationally wrongful act and if attributable to a State it may give rise to State responsibility.

Denmark shares the view that sovereignty applies to States' cyber activities as has been widely endorsed by other States who have voiced their national positions on international law in cyberspace.

Sovereignty has both an internal and external dimension. Internal sovereignty signifies the independent right of a State to exercise the functions of a State in regard to a given territory to the exclusion of any other State. It pertains to a State's jurisdiction over all persons, entities, and objects within its territory and some manifestations of the State outside its territory.

It follows that all States may exercise sovereignty over any cyber infrastructure located on their territory and all activities associated with that infrastructure – irrespective of whether such infrastructure or activity is of a public or private character. In the exercise of governmental authority, the State may promulgate and enforce domestic laws or protect cyber infrastructure and cyber activity located or taking place in its territory unless prohibited from doing so by its international legal obligations such as the limitations set out in international human rights conventions and international law on State and diplomatic immunity. A State's internal sovereignty also encompasses an obligation for the State not to allow its territory to be used for acts contrary to the rights of other States (as further elaborated under section 6 on due diligence).

External sovereignty pertains to the international equal rights and duties of a State in its relations to other States. It derives from the principle of sovereign equality of States as recognized in article 2(1) of the UN Charter and requires all States to respect the territorial integrity and political independence of other States. Other principles and rules of international law such as the prohibition of the use of force, the prohibition on intervention, and the right of self-defence are based on this principle.

As sovereignty is a primary rule under international law States are obliged to respect the sovereignty of other States and must not conduct activities that

violate another State's sovereignty. Whether or not a given act in cyberspace is done in violation of another State's sovereignty requires a case-by-case assessment of all relevant factors, in particular the nature of and the effects caused by the cyber operation. Denmark supports the view that the lawfulness of a cyber operation should be assessed based on two different bases: the degree of infringement upon the target State's territorial integrity, and whether there has been an interference with or usurpation of inherently governmental functions. Unlike the prohibition on intervention, a breach of sovereignty is not contingent on a coercion element.

With respect to infringements on a State's territory Denmark generally shares the view that cyber operations which result in physical damage or injury constitute a violation of a State's sovereignty and may also violate the principle of non-intervention, or the prohibition of the use of force, cf. section 3 and 4. In addition to physical damage or injury loss of functionality may also, depending on its nature, scale, and effects, constitute such a violation. Cyber operations that alter or delete data without necessarily resulting in physical damage or loss of functionality may also, based on a case-by-case assessment of the nature, scale, and effects of the operation in question, constitute a violation. Cyber activities causing negligible physical effects or loss of functionality would generally not be considered a violation of sovereignty.

Furthermore, interference with or usurpation of a State's inherently governmental functions may constitute a violation of a State's sovereignty or prohibited intervention. This assessment is not contingent on whether physical damage, injury, or loss of functionality have occurred, but rather if a cyber operation has interfered with data or services necessary for the exercise of inherently governmental functions. This applies irrespective of whether such inherently government functions are performed by the State itself (either by central, regional or local government) or have been delegated to non-governmental entities.

## 3 Non-intervention

The principle of non-intervention is a fundamental principle of international law. It is a corollary of the principle of sovereignty, and more specifically the aspect that provides for the sovereign equality of States as set forth in article 2(1) of the UN Charter.

Denmark is of the view that the prohibition of intervention is a rule of international law forming part of customary international law. This was established by the ICJ in the *Nicaragua* v. *United States of America* case where the Court

held that States are prohibited from intervening directly or indirectly in internal or external affairs of other States.[1]

In order for an action to qualify as an unlawful intervention it must qualify as an intervention in matters that are the sovereign prerogative of a State, the so-called *domaine réservé*, and it must involve an element of coercion.[2]

The scope of activities falling within the *domaine réservé* include but are not limited to " (…) the choice of a political, economic, social, and cultural system, and the formulation of foreign policy."[3] The range of activities covered by the non-intervention rule largely overlap with the activities reserved to States under the rule of sovereignty.

The term coercion is not defined in either treaty law or customary international law. Denmark takes the view that an act may be considered of a coercive nature when the act of interference has a potential for compelling the target State to engage in an action that it would otherwise not take. However, a distinction must be drawn between activities that merely involve influencing, as opposed to compelling, the voluntary actions of a target State. Acts of influence, such as persuasion, criticism, and public diplomacy are insufficient to qualify as an intervention. To be coercive the effort to intervene must be designed to have a decisive impact on outcomes or conduct with respect to a matter reserved to the target State. As emphasized by the Court in the Nicaragua judgment coercive acts involving the use of force are particularly obvious examples of unlawful interventions.[4] Denmark considers that coercion is not limited to means of direct or indirect use of force and that also measures below this threshold may constitute coercion. Cyber activities that do not amount to use of force can therefore also be coercive.

An example of unlawful intervention in the cyber domain could be where a State coercively interferes in the internal political process of another. In the cyber context this could potentially occur by using cyber technology to alter electronic ballots and thereby affecting the results of a political election.

## 4 Use of force and self-defence

Cyber operations may violate the prohibition on the threat or use of force, which primarily depends on the physical scale and effects of the cyber operation in question. It requires an individual assessment of the specific circumstances

1 Military and Paramilitary Activities in and against Nicaragua (*Nicaragua* v. *United States of America* case). Merits, Judgment. ICJ Reports 1986, p. 14, para. 205.

2 *Ibid.*

3 *Ibid.*

4 *Ibid.*

in each case to determine whether the scale and effects of a cyber operation correspond to what would qualify as use of force had they resulted from conventional weapons.

Article 2(4) of the UN Charter sets out that all Member States shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations. Numerous other international documents and State practice contribute to the understanding of the principle of the non-use of force. It is, however, fair to assert that there are still significant grey areas and divergent views among States as to the precise content of the law.

Generally, Denmark subscribes to the notion that where a cyber operation results in injury, death, or significant physical damage, this prima facie qualifies as use of force.

With regard to the precise interpretation of the term force and the question as to whether economic or political coercion can qualify as use of force, Denmark considers that it generally cannot be ruled out that acts of economic or political coercion can fall within the purview of Article 2(4) of the UN Charter if, for example, a cyber operation resulting in the malfunctioning of a State's financial system leads to significant economic damage.

It has been suggested that States should apply the following non-exhaustive factors for determining if a cyber operation reaches the level of use of force: Severity, immediacy, directness, invasiveness, measurability of effects, military character, State involvement, presumptive legality.[5] While few States in their public positions have endorsed these particular factors, Denmark is of the view that these factors are useful reference points for further understanding and discussing the definition of use of force in cyberspace.

In certain instances, use of force may due to its scale and effects reach the level of an armed attack and thus give rise to a right to self-defence of the target State, cf. article 51 of the UN Charter. In its Nicaragua judgment the ICJ defined an armed attack as the most grave form of the use of force.[6] Denmark subscribes to the understanding that not all illegal use of force under article 2(4) of the UN Charter necessarily amounts to an armed attack under article 51 of the Charter.

Denmark takes the view that a cyber attack may qualify as an armed attack under article 51 of the UN Charter if the effects generated are comparable to

5 M. N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable To Cyber Operations*, (Cambridge University Press, 2017), pp. 334-336.

6 *Nicaragua* v. *United States of America* case, *supra* note 1, para. 191.

effects resulting from an action, which would otherwise qualify as an armed attack. Thus, Denmark considers that a cyber operation, which e.g. leads to serious injury or death, or which causes significant physical damage, may qualify as an armed attack. This could be the case if a cyber attack leads to the disabling of an air traffic control system which causes planes to crash or an interference with the operating system of a power station, which causes serious physical damage.

Certain States take the view that an armed attack can only be undertaken by State actors or entities acting under the control or instruction of States, and thus no right to self-defense exists against an armed attack by a non-State actor. Denmark does not share this view, but contends that State practice supports that a State might in some instances and under certain conditions be permitted to exercise self-defence against an armed attack by a non-State actor.

## 5 State responsibility

Denmark is of the view that the general rules of State responsibility apply in cyberspace. A State bears international responsibility if it breaches an international obligation owed to another State. A State may be responsible under international law for acts undertaken by an organ of the State or by actors exercising government authority on behalf of that State. Acts by a non-State actor may be attributable to a State where the non-State actor carries out a cyber operation under the instruction of, or under the direction or control of that State, or where the State actor acknowledges and adopts the operations carried out by the non-State actor as its own.

Each State may decide whether to publicly attribute cyber acts to other States or not. There is no obligation under international law for States to share documentation or other evidence supporting an attribution. The application of international law and State responsibility does not depend on public attribution.

## 6 Due diligence

Denmark is of the view that a State may bear international responsibility where a State fails to take adequate measures against a non-State actor - or third State - that conducts harmful cyber operations against another State from its territory or other cyber infrastructure under its effective control.

As the ICJ Stated in the *Corfu Channel* Case[7], States are under an "obligation not to knowingly allow its territory to be used for acts contrary to the right of other States". This obligation is a natural corollary of a State's sovereignty over persons and cyber infrastructure on its territory.

As a general rule due diligence requires States to take all reasonable measures to prevent, eliminate and mitigate potentially significant harm to legally protected interests of another State, or the international community as a whole. The general principle of due diligence has developed with some variation in different fields of international law, including international environmental law, transboundary harm, and human rights. Similarly, Denmark believes that the precise contours of the due diligence obligation in cyberspace will continue to develop and crystalize in the coming years. It is, however, possible to set out some key features.

Due diligence is an obligation of conduct, not of result. A State is obliged to take all reasonable measures to stop or prevent a given cyber act from occurring. Not all harmful cyber operations emanating from another State's territory entail due diligence obligations and corresponding rights of the target State. While there is still scope for State practice to clarify the precise threshold, Denmark subscribes to the view that the harm suffered must be significant and not merely amount to inconveniences or minor disruptions.

The lack of compliance with a State's due diligence obligations may lead another State to take countermeasures if the conditions set out below in section 7 are fulfilled.

## 7 Countermeasures

States may be subject to unfriendly or hostile cyber acts or omissions that do not rise to the level of illegality under international law. These may be met with responses of a diplomatic, economic, or political nature intended to deter and hold accountable such States, irrespective of the fact that those acts are not illegal under international law. Such responses are generally termed retorsions. However, where one State breaches its obligations under international law towards another State, the victim State may respond with countermeasures. A State injured by an internationally wrongful act may be justified in taking non-forcible countermeasures in order to procure the cessation of the wrongful act and to achieve reparation for the injury.

7 *United Kingdom of Great Britain and Northern Ireland* v. *Albania* (merits), p. 22.

Breaches of international obligations, whether cyber or non-cyber in nature, may be responded to by both cyber and non-cyber countermeasures. Countermeasures must be necessary and proportionate. Thus, countermeasures may not go beyond what is necessary to bring the illegal conduct to an end. Countermeasures must be taken with the intention of compelling the offending State to change its behaviour. That being the case countermeasures may only be taken for the period where the other State continues its illegal acts. To the extent possible countermeasures should be reversible although the precise meaning of this concept in a cyber-context is not clear.

Countermeasures may only be taken in response to an internationally wrongful act. That raises the question of when such an act may be considered to have been completed and whether a target State may, for example, take countermeasures in response to an unsuccessful cyber operation that has not been completed e.g. due to defensive mechanisms from the target State. It is the view of Denmark that States cannot be presumed to have to suffer actual harm before taking countermeasures.

Denmark accepts the existence of general procedural requirements when taking countermeasures including an obligation to notify, but also supports the view put forward by a number of States that observance of these obligations may not be feasible in all circumstances in a cyber-context.

Countermeasures must be directed against State organs or other entities acting on behalf of, or whose acts are attributable to, a State as it is the State that is in breach of its obligations vis-à-vis the target State. This, however, does not necessarily exclude that actions may in some circumstances be directed against non-State actor as part of countermeasures.

The question of collective countermeasures does not seem to have been fully settled in state practice and needs careful consideration. As a general observation Denmark finds that there may be instances where one State suffers a violation of an obligation owed to the international community as a whole, and where the victim State may request the assistance of other States in applying proportionate and necessary countermeasures in collective response hereto.

## 8 International humanitarian law and cyber operations

Denmark concurs with the view put forward by a number of States that international humanitarian law (IHL) applies to cyber operations undertaken in the context of armed conflict. This is the case regardless of whether the cyber operation takes place during an international or a non-international armed conflict.

With regard to the application of IHL in the cyber domain one key issue concerns the definition of attack and under which circumstances a cyber operation can amount to an attack.

Denmark is a party to the four Geneva Conventions and Additional Protocols and defines cyber-attack within the meaning of Article 49 of Additional Protocol I. Denmark takes the view that a cyber operation may be considered an attack in the context of an armed conflict where it produces effects akin to those of a kinetic attack. Consequently, a cyber operation will constitute an attack if it can be reasonably expected to cause injury, death, or physical damage to individuals or objects. This definition also includes activity where substantial destruction is caused as a foreseeable secondary effect. For instance, if a military air traffic control system through a cyber operation is taken out of operation which causes foreseeable loss of human life or substantial damage to or destruction of physical objects.

Although digital data cannot generally in and of itself be considered an object under IHL, the destruction of data may have such adverse secondary effects on individuals or physical objects that the operation may nonetheless qualify as an attack. This may be the case where the destruction of data foreseeably results in injury, death or physical damage, in which case the objects or individuals subject hereto can be considered the object of the attack. Similarly, an operation targeting data upon which the functionality of an object relies could qualify as an attack depending on the nature and scale of the damage foreseeably resulting from the operation in question.

Where a cyber operation amounts to an attack it is subject to the same rules and requirements as those applicable to attacks conducted in the physical domain. These include, inter alia, the principles of military necessity, distinction, proportionality, and humanity.

In situations where a cyber operation does not amount to an attack the relevant rules of IHL that address conducts or effects falling below the threshold of an attack nevertheless apply. This includes but is not limited to the obligation of constant care by which States are required to take all reasonable precautions to spare the civilian population as well as civilian individuals and objects, including essential civilian infrastructure, services, and data, when planning or conducting cyber operations in the context of hostilities.

## Note from the publisher

The authors mentioned at the start of this article, Jeppe Mejer Kjelgaard and Ulf Melgaard, are only responsible for the introduction to this position paper. The position paper is a product of the government of Denmark.