I T A L Y

ITALIAN POSITION PAPER ON
'INTERNATIONAL LAW AND CYBERSPACE'

TABLE OF CONTENTS

Introduction 3

I. The protection of sovereignty in cyberspace and violations of the principle of non-intervention .. 4

II. The application of the Law of States Responsibility to activities in the cyberspace 5
a) Attribution 5
b) Due diligence 6
c) Countermeasures 7

III. Cyber operations and the Use of Force 8
a) Cyber operations and Article 2(4) of the UN Charter 8
b) Cyber operations and the exercise of self-defence by States 9
c) Cyber operations and the application of International Humanitarian Law 9
d) Cyber operations and the law of neutrality 10

IV. Human rights in cyberspace 10

V. The role of private stakeholders in cyberspace 11

VI. International cooperation in the cybersecurity domain 11

Introduction

Italy deems that international law is applicable to cyberspace and considers it the existing legal discipline and a fundamental tool for assuring responsible State behaviour in cyberspace. This is in line with Italy's unyielding support to the rule of law both at the international and domestic levels, to a rules-based international order and cooperation and, more generally, to compliance with international law.

Italy thus concurs with the conclusions reached by the UN Group of Governmental Experts (GGE) and by the Open-ended Working Group (OEWG) that was established in 2019, according to which 'international law and in particular the Charter of the United Nations in its entirety, is applicable and is essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment'.[1] While the work of the GGE primarily addressed issues of international peace and security, Italy considers that the concept of international peace and security goes beyond a merely military connotation. Accordingly, Italy finds that the rules and principles of international law – be they customary or treaty-based – applicable to activities in cyberspace are not limited to those pertaining to the prohibition of the use of force in international relations.

While Italy has no doubt as to *whether* international law applies to the cyberspace, it is aware that *how* existing rules and principles of international law apply gives rise to significant difficulties inherent in the technical features of cyberspace. Such difficulties require responses that the international community is currently developing. Italy thus welcomes and supports the ongoing process of exchange of views, study and cooperation amongst States to that end.

In this paper[2], Italy presents its non-exhaustive views on a number of discrete issues concerning the application of international law to cyberspace. The following topics will be considered in turn: the protection of sovereignty in cyberspace and violations of the principle of non-intervention; the application of the law of the international responsibility of States to activities

[1] 2013 *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/68/98, 24 June 2013, para.20; 2015 *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/70/174, 22 July 2015, para. 24.; 2021 *Open-ended working group on developments in the field of information and telecommunications technologies in the context of international security*; UN Doc A/75/816, para 7.

[2] This paper has been prepared by the Ministry for Foreign Affairs and International Cooperation together with the Presidency of the Council of Ministers and the Ministry of Defence and has been completed in the month of September 2021.

carried out in cyberspace; cyber operations and the use of force; the application of international human rights law, the role of private stakeholders; and international cooperation in cyberspace.

With specific regard to the use of force, while reaffirming the general principles and validity of both *jus ad bellum and jus in bello* in cyberspace, Italy underlines that International Humanitarian Law (IHL) is restrictive as it aims at limiting the belligerents' conduct which negatively affects civilians and civilian objects in an armed conflict. Therefore, the recognition of its applicability to cyberspace does not amount to encouraging or allowing the use of force as an instrument of aggression and/or as a means for the settlement of international disputes.

I. The protection of sovereignty in cyberspace and violations of the principle of non-intervention

Italy attaches fundamental importance to the application of the principle of sovereignty to cyberspace, including its ancillary rules, such as the right to internal self-determination. Italy considers that both the internal and external aspects of sovereignty apply in cyberspace.

The principle of sovereignty is a primary rule of international law, the violation of which amounts to an internationally wrongful act. Italy considers that the principle in question prohibits a State from conducting cyber operations, which produce harmful effects on the territory of another State, irrespective of the physical location of the perpetrator. Italy finds that, according to the same principle, a State may not conduct cyber operations from the territory of another State without its express authorization. This is without prejudice to situations of distress where the state of necessity entails the applicability of a different discipline.

Each State's exclusive jurisdiction over the physical, social and logical layers of cyberspace located on its territory may be exercised within the limits imposed by international law, including international obligations deriving from diplomatic privileges and immunities and those arising from human rights obligations.

Responses to violations of sovereignty should be assessed on a case-by-case basis taking into account the nature and consequences of each violation.

Italy believes that cyber operations constitutes a violation of the customary principle of non-intervention in the internal affairs of other States when a State employs coercive means to

compel another State to undertake or desist from a specific action, in matters falling under its domain réservé.

The accelerating pace of technological change, the unpredictable effects of its applications, as well as the difficulty to measure the coercive impact of influence activities, which are on the rise, cannot be overlooked. Therefore, Italy sees merit in continuing to deepen the study of possible violations of the principle of non-intervention in cyberspace. That is particularly the case with regard to influence activities aimed, for instance, at undermining a State's ability to safeguard public health during a pandemic, or at manipulating voting behaviour.

II. The application of the Law of States Responsibility to activities in the cyberspace

a) Attribution

Attributing responsibility of cyber activities is a complex matter which has led to different approaches across the international community. Italy sees merit in contributing to the international law debate on the matter.

Italy deems that attribution is a national sovereign prerogative and so is the decision to make it public or not, on a case-by-case basis.

Italy is aware that attribution entails technical, legal and political considerations. With regard to the attribution of cyber wrongful acts by States, Italy considers that any attribution should be based on a sufficient level of confidence on the source of the cyber activities in question and on the identity of the actor(s) responsible. Although under international law there is no general obligation thereto, Italy stresses the importance of transparency: attribution of cyber wrongful activities should therefore be reasonable and credibly based on factual elements related to relevant circumstances of the case. This would be especially required should attribution become part of international courts and/or arbitration proceedings, with the exception of States' classified information.

Italy concurs with the view that attribution of cyber wrongful acts from one State to another is governed by the general rules of international law on the attribution of State conduct as codified by the International Law Commission (ILC) Articles on the Responsibility of States for

Internationally Wrongful Acts (ARSIWA)[3]. Still, Italy acknowledges the difficulties of applying the ARSIWA in a peculiar environment such as cyberspace.

Finally, and in the spirit of cooperation and of national contribution to study how international law applies to cyberspace that informs this document, Italy considers that further dialogue on the matter could be conducive to a better understanding of attribution.

b) Due diligence

Italy considers that due diligence obligations apply in cyberspace as defined in the *Corfu Channel* case by the International Court of Justice (ICJ), according to which every State is under an 'obligation not to knowingly allow its territory to be used for acts contrary to the right of other States'.[4] Hence, due diligence requires States to take all reasonable measures concerning activities in cyberspace falling under their jurisdiction in order to prevent, eliminate or mitigate potentially significant harm to legally protected interests of another State, or of the international community as a whole. Italy deems that the due diligence obligation in question also encompasses, *inter alia*, human rights protection and the protection of international peace and security.

States are thus under the obligation not to allow their territory, or their Information and Communication Technology (ICT) infrastructure to be used for the conduct of wrongful cyber activities by State or non-State actors. State actors include governmental institutions as well as individuals or groups acting on behalf of or under the control of a State. The principle has been further developed over the years in different fields of international law, most prominently with regard to transboundary natural resources,[5] the protection of the environment[6] and human rights.[7]

In case of wrongful cyber activities that cause harm to another State, the State of origin is required to make its best efforts to prevent, eliminate, or mitigate all acts of wrongdoing.

[3] *Responsibility of States for internationally wrongful acts*, UN Doc. A/RES/56/83, 28 January 2002.
[4] *Corfu Channel Case*, Judgment of April 9th, 1949: I.C.J. Reports 1949, p. 4, at 18.
[5] ILC, "Draft Articles on Prevention of Transboundary Harm from Hazardous Activities", in *Yearbook of the International Law Commission*, 2001, vol. II, Part 2, p. 148.
[6] *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, I.C.J. Reports 1996, p. 226, para. 241-242.
[7] CESCR, "General Comment No. 3: The Nature of States Parties' Obligations (Art. 2, Para. 1, of the Covenant)", UN Doc. E/1991/23. 14 December 1990.

Although there is no general international obligation to do so, the State of origin should share any relevant information with the victim-State.

Due diligence is an obligation of conduct, not one of result. Accordingly, as long as it makes its best efforts, a State cannot be held liable if ultimately unable to prevent, mitigate, or terminate wrongful cyber activities launched from or in transit through its territory.

In addition, when considering whether a State is in breach of its due diligence obligations, due regard should be paid to the technological/financial resources and overall capabilities of the State in question.

Further discussions on thresholds and scenarios of cyber operations (not necessarily resulting in physical damage of property), that amount to a breach of due diligence obligations in cyberspace, could be conducive to a clearer understanding of the matter.

c) Countermeasures

Italy is of the view that when a State is victim of an international wrongful act perpetrated by another State, it may take countermeasures in response.[8]

Italy deems that countermeasures are adequate responses to cyber operations that constitute an international wrongful act[9] below the threshold of an armed attack. This is without prejudice to the inherent right of States to self-defence.

The adoption of countermeasures against the State that may be held responsible, directly or indirectly, for unlawful cyber acts may be problematic due to, *inter alia*, difficulties of: traceability, assessment of breach in relation with the threshold of the diligence due, significance of the harm suffered.

The victim-State is generally required to call upon the State of origin to discontinue the wrongful act and to notify it of its intention to take countermeasures in response to wrongful cyber operations. However, in conformity with international law, this requirement may not

[8] Under customary international law, as stated by the ARSIWA and corroborated by the ICJ case law (Gabćikovo-Nagymaros Project, Judgment, paras 83-85), the lawfulness of countermeasures is subject to the following conditions: (i) They may be taken in response to a previous international wrongful act of another State and must be directed against that State; (ii) The injured State must have called upon the State committing the wrongful act to discontinue its wrongful conduct or to make reparations for it; (iii) The effects of a countermeasure must be commensurate with the injury suffered, in accordance with the principle of proportionality.

[9] Responsibility of States for internationally wrongful acts, UN Doc. A/RES/56/83, 28 January 2002, Articles 49-54.

apply if immediate action is needed to enforce the rights of the injured State and to prevent further damage.

The response to a wrongful cyber operation may be in kind (but not necessarily, as per relevant international law), on the condition that the response is commensurate with the harm suffered and is limited to the purpose of ensuring compliance with breached obligations, thus taking into account the seriousness of the initial violation and the rights in question. In any case, countermeasures must not amount to a threat, or use, of force and must be consistent with other peremptory norms, as well as with human rights and humanitarian law.

III. Cyber Operations and the Use of Force

a) Cyber operations and Article 2(4) of the UN Charter

There is no established definition or threshold of hostile cyber operations falling within the scope of the prohibition of the 'use of force' in the sense of article 2(4) of the UN Charter. Such assessment will be determined on a case-by-case basis depending on the consequences of any given cyber operation.

Italy considers a cyber operation conducted by a State against another State as a use of force, when its scale and effects are comparable to those of a conventional use of force, resulting in physical damage of property, human injury or loss of life.

While it is generally accepted that cyber operations resulting in material damage can constitute a use of force, we consider the qualification of cyber operations which merely cause loss of functionality a controversial one. The inclusion of such operations in the scope of the prohibition of the use of force, however, could be justified if one considers that, because of the reliance of modern societies on computers, computer systems and networks, cyber technologies have enabled States to cause the interruption of essential services without the need of physical damage.

b) Cyber operations and the exercise of self-defence by states

In line with the conclusions reached by the ICJ in the *Nicaragua v. United States* case, Italy considers that the gravest form of use of force constitutes an armed attack[10]. There is no established definition or threshold of hostile cyber operations falling within 'armed attack' in the sense of article 51 of the UN Charter[11]. Such assessment will be determined on a case-by-case basis depending on the consequences of any given cyber operation.

Italy deems that wrongful cyber operations conducted by State or non-State actors may constitute an armed attack when their scale and effects are comparable to those resulting from conventional armed attacks, resulting in significant physical damage of property, human injury and loss of life, or disruption in the functioning of critical infrastructure.

The occurrence of an armed attack triggers the right to self-defence, and the victim-State may resort to all necessary and proportionate means to end the aggression. The decision as to when a cyber operation amounting to armed attack would lead to collective self-defence will be taken on a case-by-case basis.

c) Cyber operations and the application of International Humanitarian Law

IHL applies in cyberspace in the context of an international or non-international armed conflict. The definition of 'armed conflict' in this regard has been formulated by the Appeals Chamber in the *Prosecutor v Tadić* case Jurisdiction Decision, according to which '…an armed conflict exists whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organised crime groups or between such groups within a State'[12].

In line with the definition of 'attack' under Article 49(1) of the 1977 Protocol I Additional to the Geneva Conventions of 12 August 1949[13], Italy qualifies cyber operations as 'attacks' under IHL if they constitute an act of violence resulting in more than minimal physical damage of

[10]Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits, International Court of Justice (ICJ), 27 June 1986.
[11] United Nations, Charter of the United Nations, 24 October 1945.
[12]ICTY, Prosecutor v Tadić, Case No IT-94-1, Decision on the Defence Motion for Interlocutory Appeals on Jurisdiction, 2 October 1995, para. 70.
[13]International Committee of the Red Cross (ICRC), Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.

property or disruption in the functioning of critical infrastructure, or human injury and loss of life.

Furthermore, a State may not carry out attacks against targets located within the territory of a non-belligerent State without the express consent of the latter, unless otherwise allowed by *jus ad bellum* rules for the purposes of self-defence or under the authorization of the UN Security Council. Finally, the law of neutrality must also be taken into account as a possible limit in international armed conflicts.

d) Cyber operations and the law of neutrality

The law of neutrality applies in cyberspace in the context of an international armed conflict on the basis of existing international customary law[14]. According to the law of neutrality, parties to an international armed conflict may not launch wrongful cyber operations from ICT infrastructure located in the territory or under the exclusive control of a neutral State.

Within an armed conflict, any action taken by a neutral State should be applied equally to all belligerents. For instance, a State may not provide or deny access to its ICT infrastructure to one party but not to the other(s). In addition, neutral States must abide by the rules and recommendations taken by the UNSC. They may thus not invoke their neutrality to refrain from adopting such measures against the wrongdoer(s).

IV. Human rights in cyberspace

Italy finds that international human rights law applies in cyberspace in the same way as it applies to the analogue world. In particular, each State is bound to protect human rights both on-line and off-line, protecting individuals from possible violations of those rights, including but not limited to freedom of opinion and expression, the right to access to information, and the right to privacy.

[14] International Conferences (The Hague), Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, 18 October 1907; The Hague Convention XIII of 1907 Concerning the Rights and Duties of Neutral Powers in Naval War. Washington, D.C., The Endowment.

Respect for human rights obligations must be upheld at all times, including when preventing, mitigating or responding to cyber incidents.

V. The role of private stakeholders in cyberspace

Given the fundamental role of the private sector in the cyberspace, Italy considers public-private cooperation as key to guaranteeing cybersecurity and effective capacity-building.

Wrongful activities in cyberspace can also affect private stakeholders, both as individuals and as partners/members of public-private partnership running ICT infrastructures.

Italy also acknowledges the accountability of the private sector regarding human rights in cyberspace, in line with UN Guiding Principles on Business and Human Rights.[15]

VI. International cooperation in the cybersecurity domain

Italy promotes international cooperation to improve cyber resilience and international stability. Italy wishes to stress the relevance of confidence building as a means to foster cooperation and the necessity to operationalise capacity building and information sharing activities.

Italy considers that, within such a cooperation context, best practices may be taken stock of and shared, building upon initiatives of this kind within regional organizations.

Italy deems that capacity building should be demand-driven, tailored to specific needs and contexts, evidence-based, results-oriented, transparent, accountable, gender sensitive and supported by public-private partnerships in line with the Busan Principles.[16]

In addition to its firm support for global cooperation, Italy believes regional and bilateral cooperation to be very well suited to foster cyber resilience at the present stage. Regional forums such as the European Union (EU), the Organization for Security and Co-operation in Europe (OSCE), the Council of Europe (CoE), the Association of Southeast Asian States (ASEAN) and the Organization of American States (OAS) have so far made valuable contributions in this regard.

---

[15] UN, *Guiding Principles on Business and Human Rights*, UN Doc. HR/PUB/11/04, 2011.
[16] OECD, *Busan Partnership for effective co-operation in support of international development*, 1 December 2011.